User Manual

Original Instructions

Allen-Bradley

VersaVirtual Appliance

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

Allen-Bradley • Rockwell Software

Rockwell Automation

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

Chapter 1

Features

Chapter 2

Install and Start the VersaVirtual Appliance

Chapter 3

Integrate the Network

Chapter 4

Manage the System

Chapter 5

System Shutdown and Startup

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
AD	Active Directory
BMC	Baseboard Management Controller
CMC	Chassis Management Controller
DCUI	Direct Console User Interface
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HA	Host Address
HCL	Hardware Compatibility List
HDD	Hard Disk Drive
HSRP	Hot Standby Router Protocol
LDAP	Lightweight Directory Access Protocol

Abbr	Meaning
NAT	Network Address Translation
NM	Network (I/O) Module
NTP	Network Time Protocol
OVF	Open Virtualization Format
SSH	Secure Shell
SSO	Single Sign-on
VA	Virtualization Appliance
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
VSE	Virtual Support Engineer

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.

Chapter 1

Features

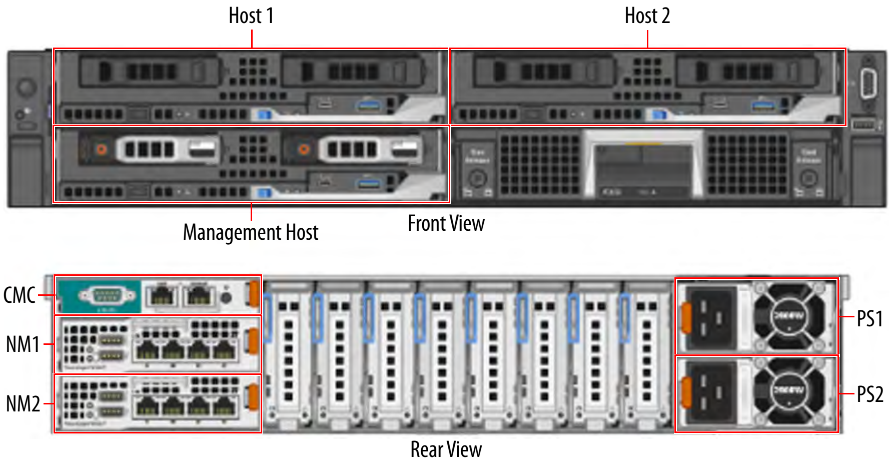
Overview

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:

Chapter **2**

Install and Start the VersaVirtual Appliance

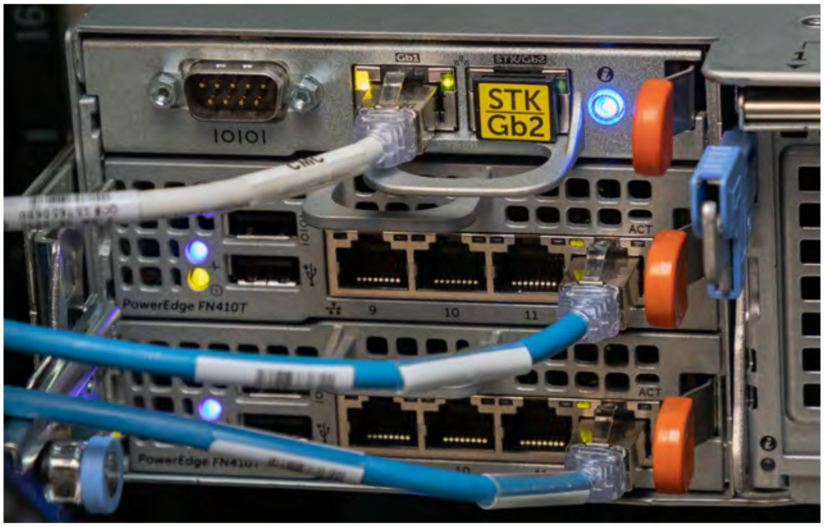
The VersaVirtual™ Appliance must be installed in a rack mount. After you install the VersaVirtual Appliance in a rack mount and connect peripherals, you must install the front bezel, which is included.

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.

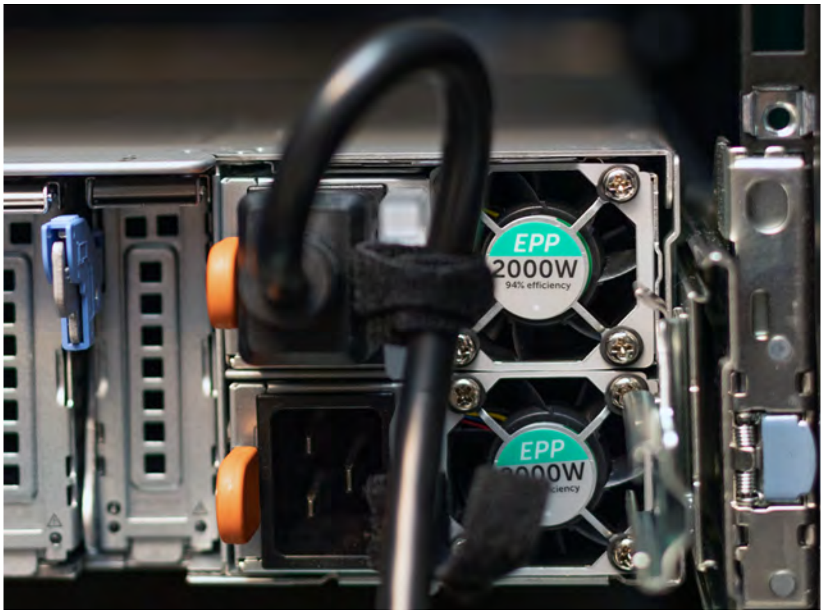


CMC cable

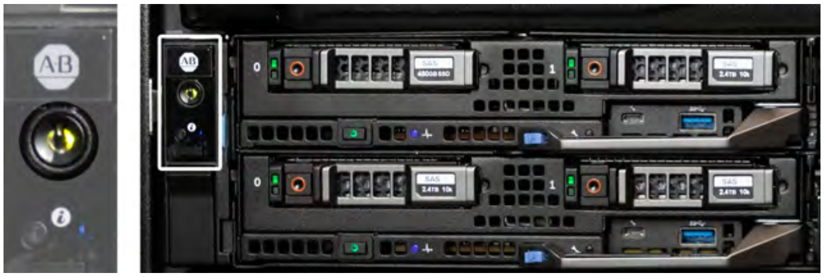
I/O module cables (connect each to port 12)

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.

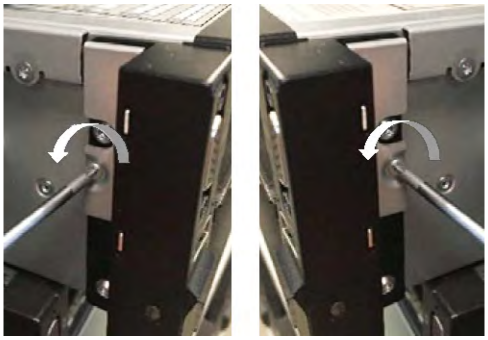


Install the Bezel

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

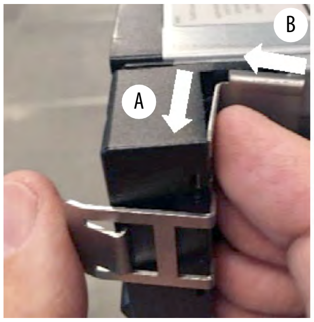
TIP To perform the following steps, you need a T8 Torx screwdriver.

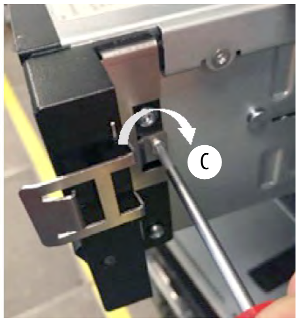
1. Locate and remove the screw on each side and near the front of the appliance.



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

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

IMPORTANT	To integrate your VersaVirtual Appliance into your network, you need the following connections. For chassis management: • An Ethernet connection at least1 Gb speed For application and hypervisor traffic: • 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.

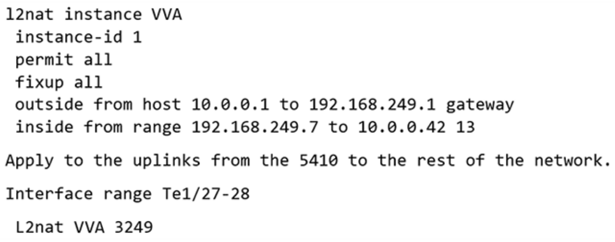
     ```
     switch#config term
     switch#config terminal
     switch(config)#vlan 3249
     switch(config-vlan)#name VersaVirtual
     switch(config)#interface Tel/1
     switch(config-if)#switchport mode access
     switch(config-if)#switchport access vlan 3249
     switch(config-if)#interface range 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.

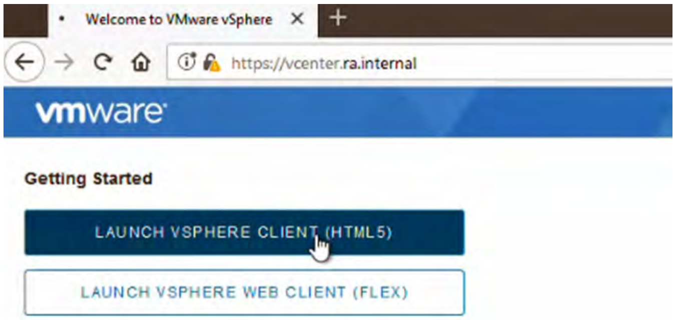
192.168.249.7	nm1.ra.internal	nm1	#FN410T	Network I/O Module
192.168.249.8	nm2.ra.internal	nm2	#FN410T	Network I/O Module
192.168.249.9	cmc.ra.internal	cmc	#FX2	Chassis Management Controller
192.168.249.10	management-bmc.ra.internal	management-bmc	#FC640	Service Baseboard Management Controller
192.168.249.11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

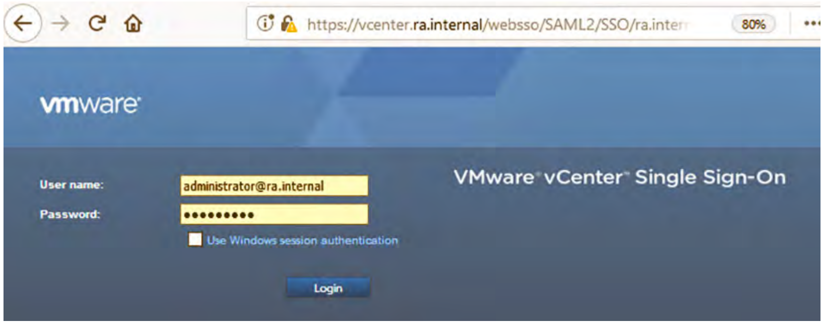
Put the vSAN Hosts in Maintenance Mode

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).


Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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


https://vcenter.ra.internal/websso/SAML2/SSO/ra.inter
80%
vmware
VMware vCenter Single Sign-On
Login

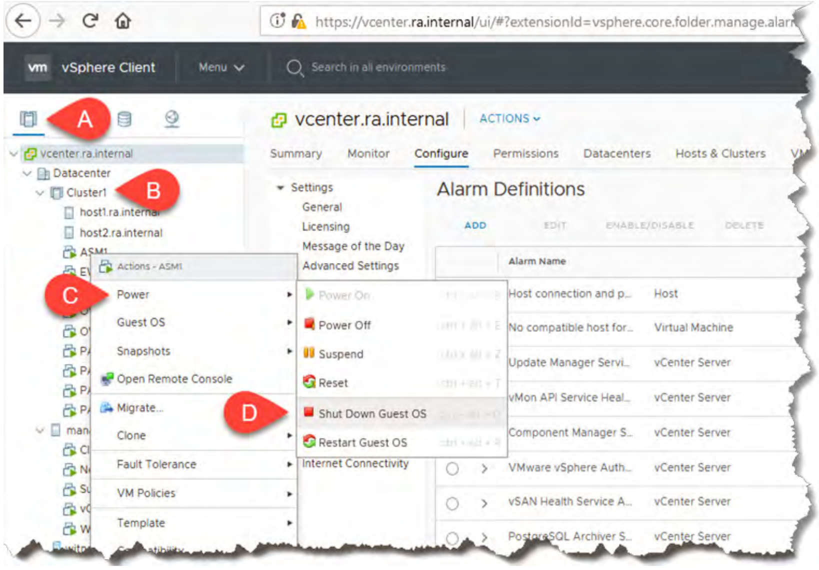
User name: administrator@ra.internal

Password: •••••••••

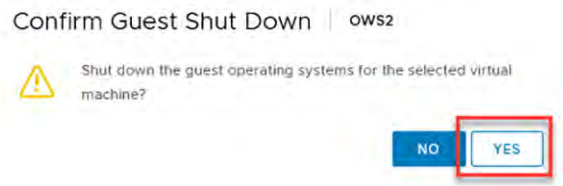
□ Use Windows session authentication

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.



Confirm Guest Shut Down | OWS2

Shut down the guest operating systems for the selected virtual machine?

NO YES

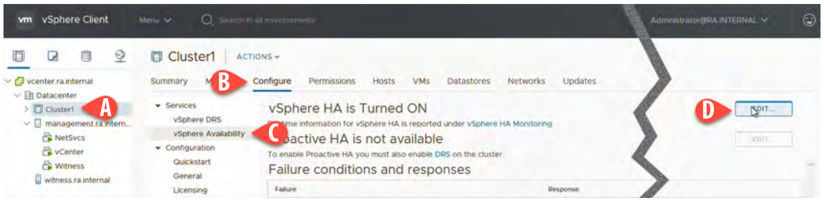
6. On the main Navigation pane, highlight Cluster1 (A).

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).



vSphere HA is Turned ON

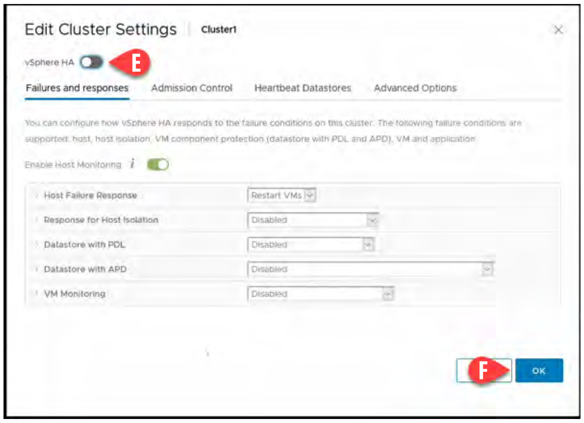
Runtime information for vSphere HA is reported under vSphere HA Monitoring

Proactive HA is not available

To enable Proactive HA you must also enable DRS on the cluster.

Failure conditions and responses

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



Edit Cluster Settings | Cluster1

vSphere HA

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application

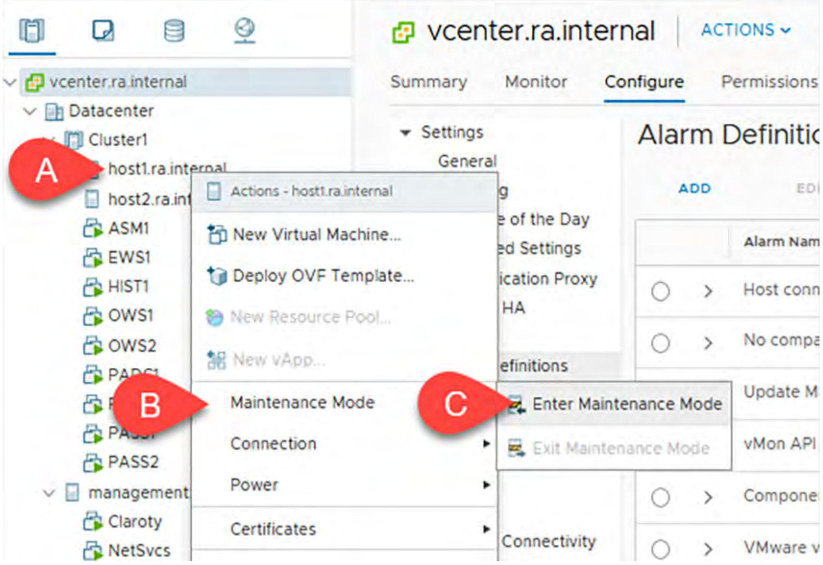
Enable Host Monitoring

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	Disabled

Click OK (F).

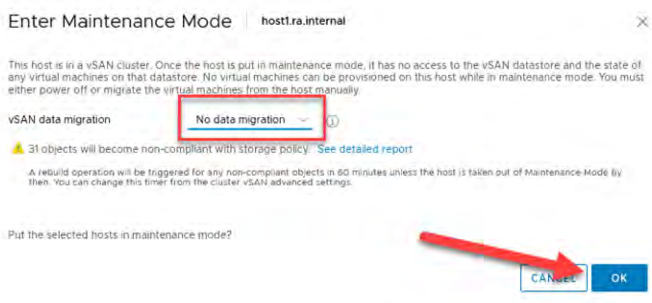
12. Right-click on host1.ra.internal (A).

Select Maintenance mode (B) > Enter Maintenance Mode (C).



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

Click OK.



Enter Maintenance Mode | host1.ra.internal

This host is in a vSAN cluster. Once the host is put in maintenance mode, it has no access to the vSAN datastore and the state of any virtual machines on that datastore. No virtual machines can be provisioned on this host while in maintenance mode. You must either power off or migrate the virtual machines from the host manually.

vSAN data migration: No data migration

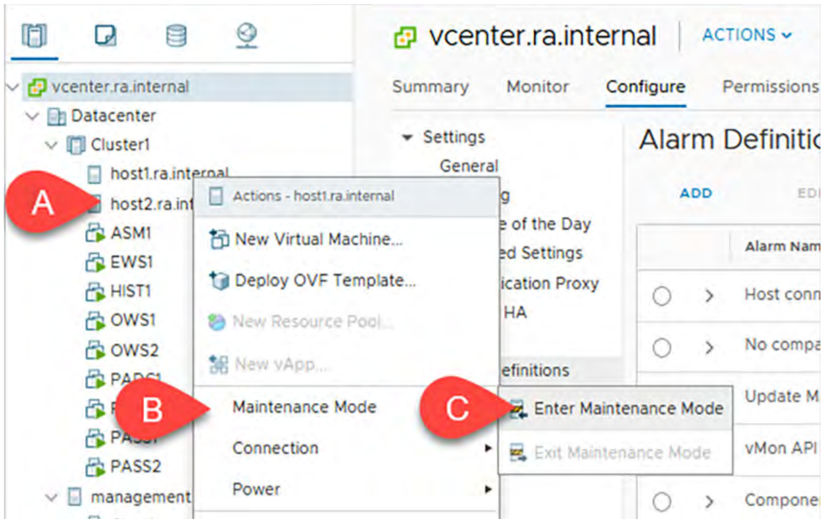
31 objects will become non-compliant with storage policy. See detailed report

A rebuild operation will be triggered for any non-compliant objects in 60 minutes unless the host is taken out of Maintenance Mode by then. You can change this timer from the cluster vSAN advanced settings.

Put the selected hosts in maintenance mode?

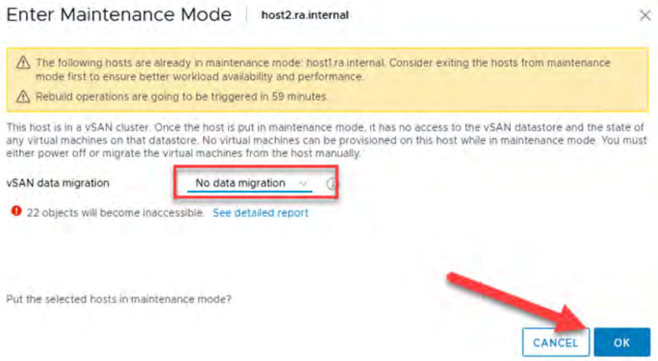
14. Right-click on host2.ra.internal (A).

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.



Enter Maintenance Mode | host2.ra.internal

⚠ The following hosts are already in maintenance mode: host1.ra.internal. Consider exiting the hosts from maintenance mode first to ensure better workload availability and performance.

⚠ Rebuild operations are going to be triggered in 59 minutes.

This host is in a vSAN cluster. Once the host is put in maintenance mode, it has no access to the vSAN datastore and the state of any virtual machines on that datastore. No virtual machines can be provisioned on this host while in maintenance mode. You must either power off or migrate the virtual machines from the host manually.

vSAN data migration: No data migration

22 objects will become inaccessible. See detailed report

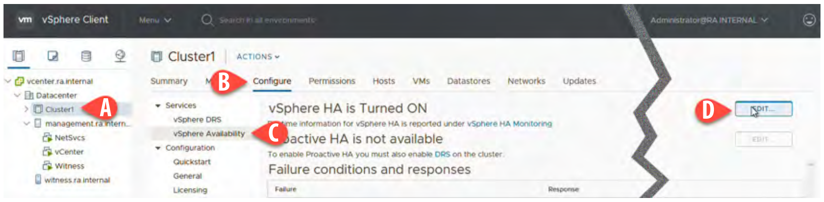
Put the selected hosts in maintenance mode?

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).



vSphere HA is Turned ON

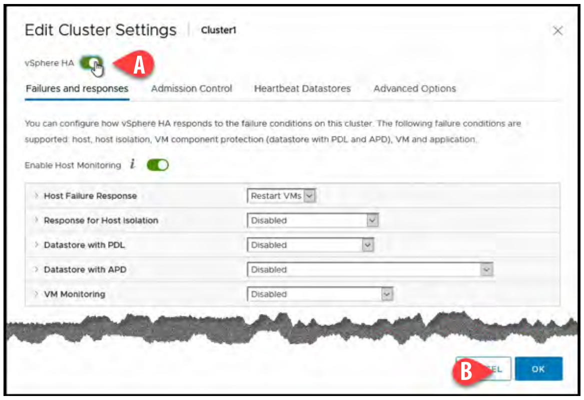
...time information for vSphere HA is reported under vSphere HA Monitoring

...active HA is not available

To enable Proactive HA you must also enable DRS on the cluster.

Failure conditions and responses

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



You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	Disabled

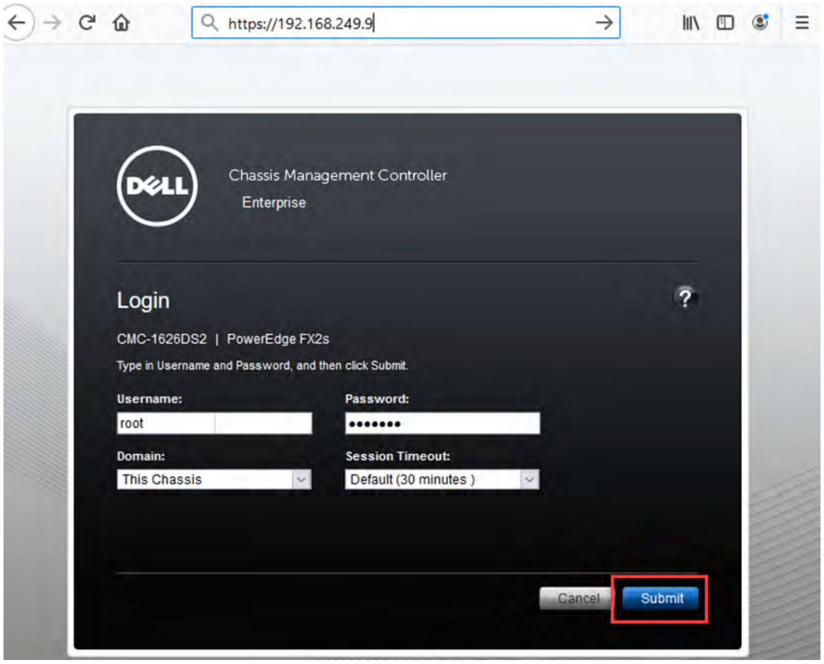
Click OK (B).

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.



CMC-1626DS2 | PowerEdge FX2s

Type in Username and Password, and then click Submit.

Username: root

Password: •••••••

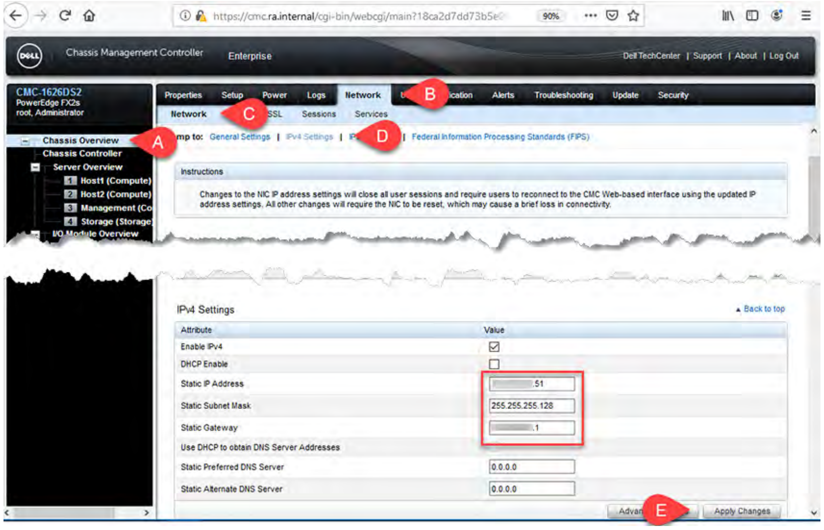
Domain: This Chassis

Session Timeout: Default (30 minutes)

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).



Instructions

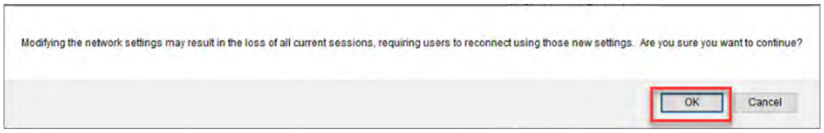
Changes to the NIC IP address settings will close all user sessions and require users to reconnect to the CMC Web-based interface using the updated IP address settings. All other changes will require the NIC to be reset, which may cause a brief loss in connectivity.

IPv4 Settings

Attribute	Value
Enable IPv4	☑
DHCP Enable	□
Static IP Address	[redacted].51
Static Subnet Mask	255.255.255.128
Static Gateway	[redacted].1
Use DHCP to obtain DNS Server Addresses	
Static Preferred DNS Server	0.0.0.0
Static Alternate DNS Server	0.0.0.0

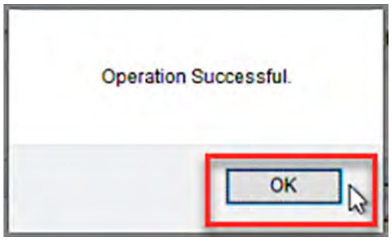
You subsequently lose connectivity to the CMC.

3. Click OK to the current sessions warning.



Modifying the network settings may result in the loss of all current sessions, requiring users to reconnect using those new settings. Are you sure you want to continue?

4. Click OK to the Operation Successful window.

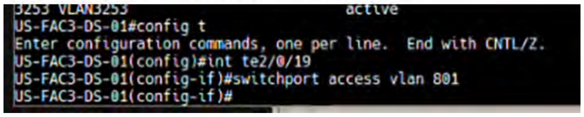


Operation Successful.

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.

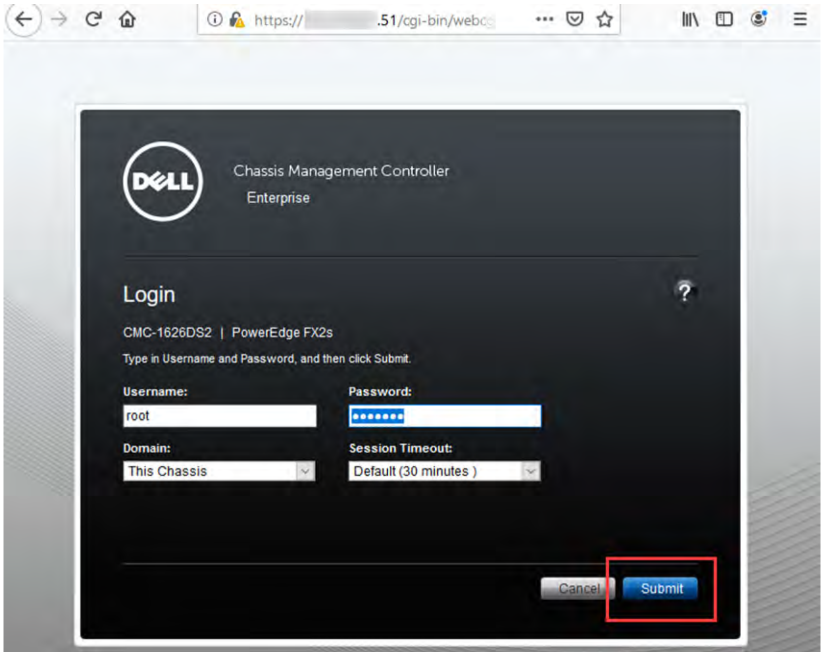
```
config t
int te2/0/19
switchport access vlan 801
```



```
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.



https://[redacted].51/cgi-bin/webc

Chassis Management Controller
Enterprise

Login

CMC-1626DS2 | PowerEdge FX2s

Type in Username and Password, and then click Submit.

Username: root

Password: •••••••

Domain: This Chassis

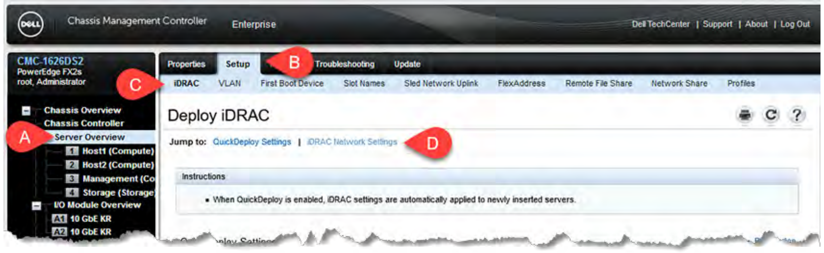
Session Timeout: Default (30 minutes)

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).



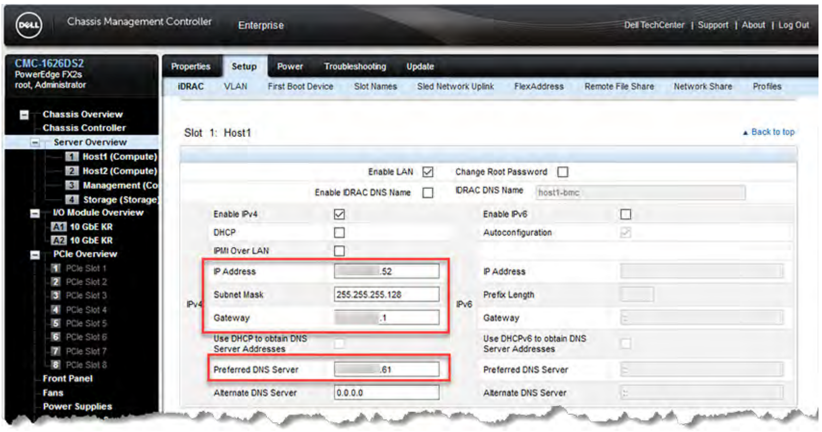
Deploy iDRAC

Jump to: QuickDeploy Settings | iDRAC Network Settings

Instructions

- When QuickDeploy is enabled, iDRAC settings are automatically applied to newly inserted servers.

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).



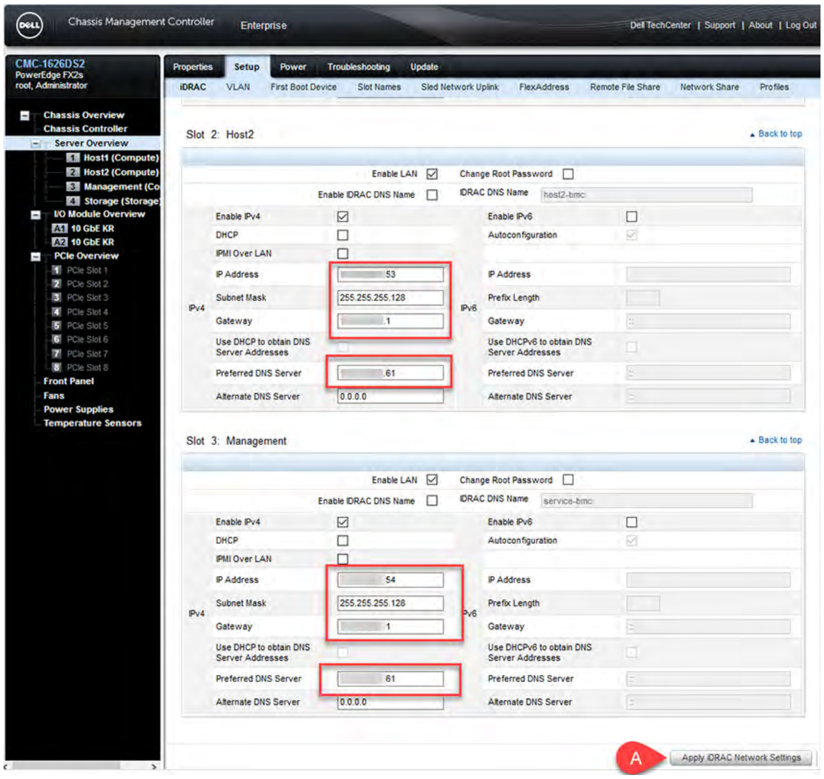
Slot 1: Host1

Enable LAN ☑ Change Root Password ☐
Enable IDRAC DNS Name ☐ IDRAC DNS Name host1-bmc

IPv4	Enable IPv4	☑	Enable IPv6	☐
	DHCP	☐	Autoconfiguration	☑
	IPMI Over LAN	☐		
	IP Address	[redacted].52	IP Address	
	Subnet Mask	255.255.255.128	Prefix Length	
	Gateway	[redacted].1	Gateway	
	Use DHCP to obtain DNS Server Addresses	☐	Use DHCPv6 to obtain DNS Server Addresses	☐
	Preferred DNS Server	[redacted].61	Preferred DNS Server	
	Alternate DNS Server	0.0.0.0	Alternate DNS Server	

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).



Slot 2: Host2

Enable LAN ☑ Change Root Password ☐
Enable IDRAC DNS Name ☐ IDRAC DNS Name host2-bmc

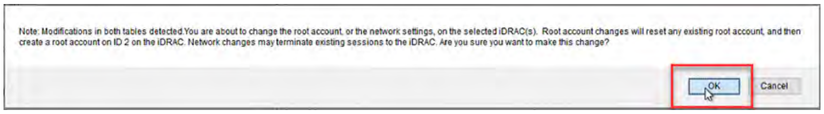
IPv4	Enable IPv4	☑	Enable IPv6	☐
	DHCP	☐	Autoconfiguration	☑
	IPMI Over LAN	☐		
	IP Address	[redacted].53	IP Address	
	Subnet Mask	255.255.255.128	Prefix Length	
	Gateway	[redacted].1	Gateway	
	Use DHCP to obtain DNS Server Addresses	☐	Use DHCPv6 to obtain DNS Server Addresses	☐
	Preferred DNS Server	[redacted].61	Preferred DNS Server	
	Alternate DNS Server	0.0.0.0	Alternate DNS Server	

Slot 3: Management

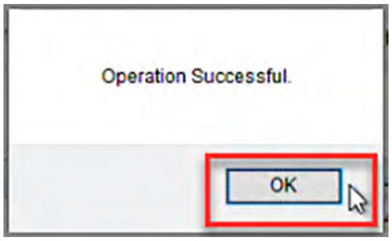
Enable LAN ☑ Change Root Password ☐
Enable IDRAC DNS Name ☐ IDRAC DNS Name service-bmc

IPv4	Enable IPv4	☑	Enable IPv6	☐
	DHCP	☐	Autoconfiguration	☑
	IPMI Over LAN	☐		
	IP Address	[redacted].54	IP Address	
	Subnet Mask	255.255.255.128	Prefix Length	
	Gateway	[redacted].1	Gateway	
	Use DHCP to obtain DNS Server Addresses	☐	Use DHCPv6 to obtain DNS Server Addresses	☐
	Preferred DNS Server	[redacted].61	Preferred DNS Server	
	Alternate DNS Server	0.0.0.0	Alternate DNS Server	

5. At the warning, click OK.


Note: Modifications in both tables detected.You are about to change the root account, or the network settings, on the selected iDRAC(s). Root account changes will reset any existing root account, and then create a root account on ID 2 on the iDRAC. Network changes may terminate existing sessions to the iDRAC. Are you sure you want to make this change?

6. Click OK to the Operation Successful window.



Operation Successful.

Network Modules

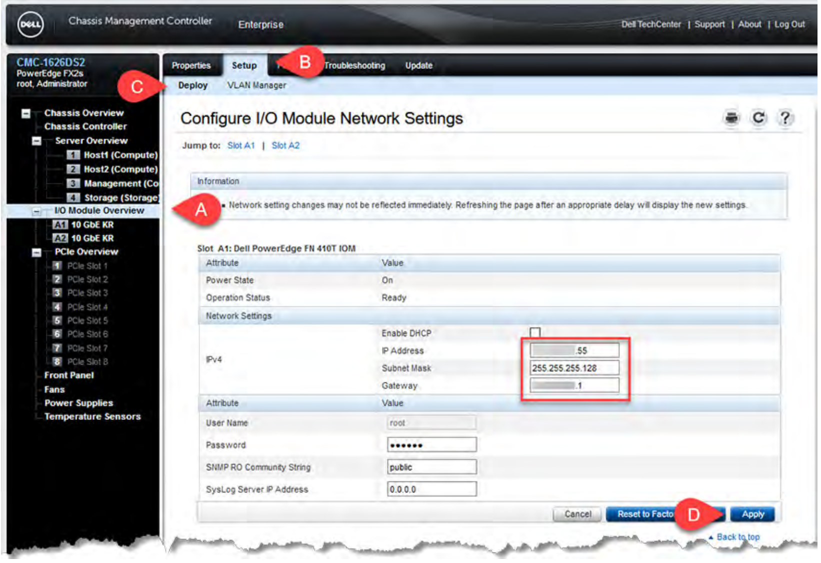
1. If you are not already there, access the Chassis Management Controller (CMC) through a browser.

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

2. Once inside the CMC, navigate to 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).



Configure I/O Module Network Settings

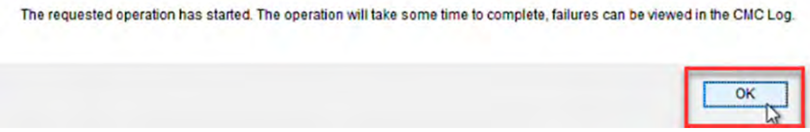
Information

- Network setting changes may not be reflected immediately. Refreshing the page after an appropriate delay will display the new settings.

Slot A1: Dell PowerEdge FN 410T IOM

Attribute	Value	
Power State	On	
Operation Status	Ready	
Network Settings		
IPv4	Enable DHCP	□
	IP Address	[redacted].55
	Subnet Mask	255.255.255.128
	Gateway	[redacted].1
Attribute	**Value**	
User Name	root	
Password	•••••••	
SNMP RO Community String	public	
SysLog Server IP Address	0.0.0.0	

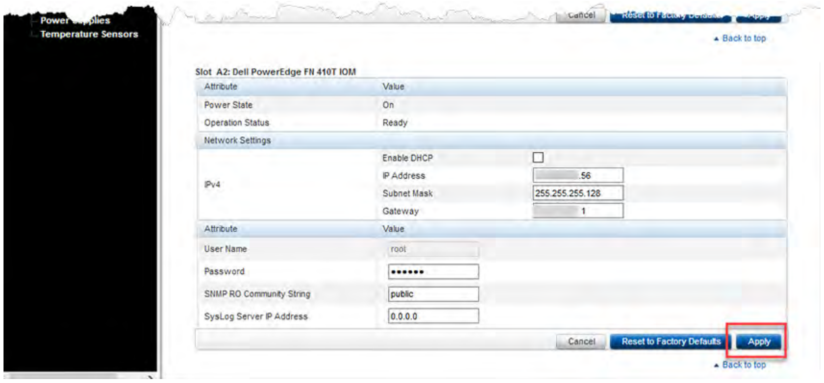
3. At the operation status, click OK.



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.

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

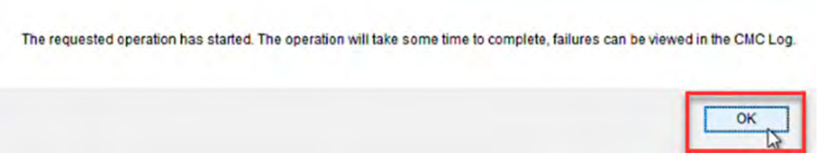


Slot A2: Dell PowerEdge FN 410T IOM

Attribute	Value	
Power State	On	
Operation Status	Ready	
Network Settings		
IPv4	Enable DHCP	□
	IP Address	[redacted].56
	Subnet Mask	255.255.255.128
	Gateway	[redacted]1

Attribute	Value
User Name	root
Password	••••••
SNMP RO Community String	public
SysLog Server IP Address	0.0.0.0

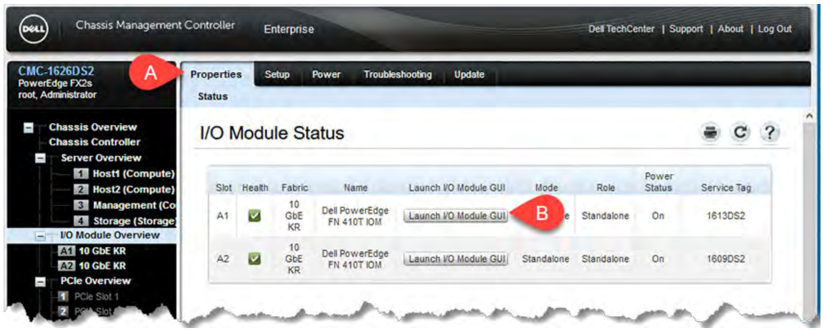
5. At the operation status, click OK.



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

6. Navigate to the Properties tab of the I/O Module Overview (A).

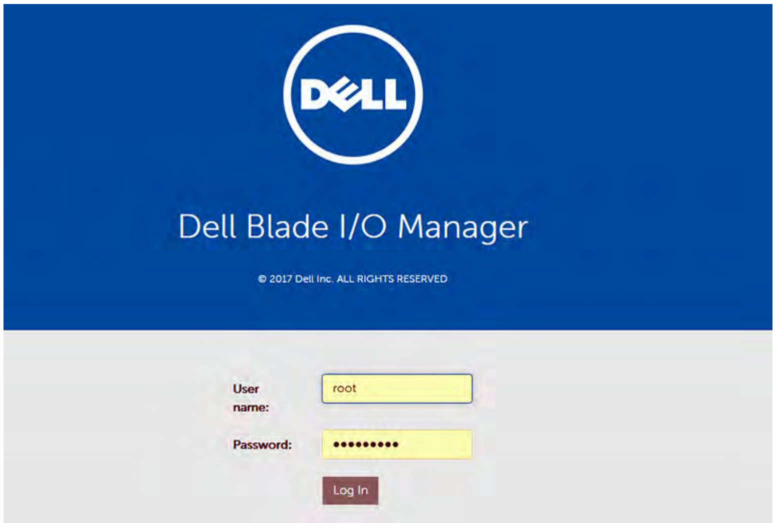
For Slot A1, click Launch I/O Module GUI (B).



I/O Module Status

Slot	Health	Fabric	Name	Launch I/O Module GUI	Mode	Role	Power Status	Service Tag
A1	✓	10 GbE KR	Dell PowerEdge FN 410T IOM	Launch I/O Module GUI	e	Standalone	On	1613DS2
A2	✓	10 GbE KR	Dell PowerEdge FN 410T IOM	Launch I/O Module GUI	Standalone	Standalone	On	1609DS2

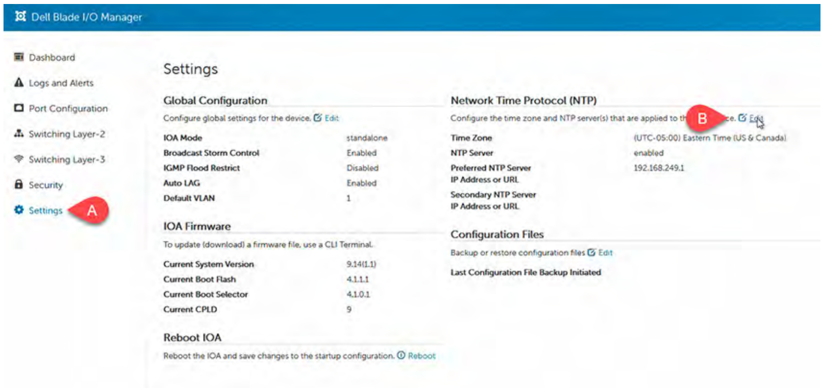
7. On the Dell Blade I/O Manager, log in as root with the system-wide password.



User name: root

Password: •••••••••

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



Settings

Global Configuration

Configure global settings for the device. Edit

IOA Mode	standalone
Broadcast Storm Control	Enabled
IGMP Flood Restrict	Disabled
Auto LAG	Enabled
Default VLAN	1

IOA Firmware

To update (download) a firmware file, use a CLI Terminal.

Current System Version	9.14(1.1)
Current Boot Flash	4.1.1.1
Current Boot Selector	4.1.0.1
Current CPLD	9

Reboot IOA

Reboot the IOA and save changes to the startup configuration. Reboot

Network Time Protocol (NTP)

Configure the time zone and NTP server(s) that are applied to th ce. Edit

Time Zone	(UTC-05:00) Eastern Time (US & Canada)
NTP Server	enabled
Preferred NTP Server IP Address or URL	192.168.249.1
Secondary NTP Server IP Address or URL	

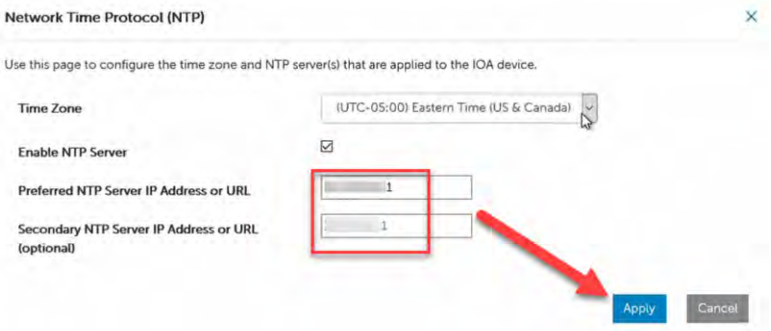
Configuration Files

Backup or restore configuration files Edit

Last Configuration File Backup Initiated

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

   Click Apply.



Network Time Protocol (NTP)

Use this page to configure the time zone and NTP server(s) that are applied to the IOA device.

Time Zone	(UTC-05:00) Eastern Time (US & Canada)
Enable NTP Server	☑
Preferred NTP Server IP Address or URL	[redacted]1
Secondary NTP Server IP Address or URL (optional)	[redacted]1

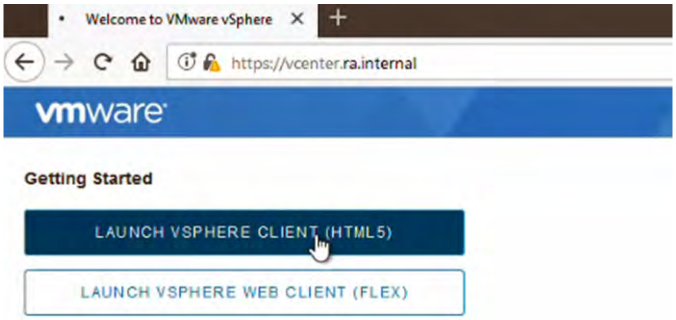
10. For I/O module 2, repeat step 2...step 8.

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.

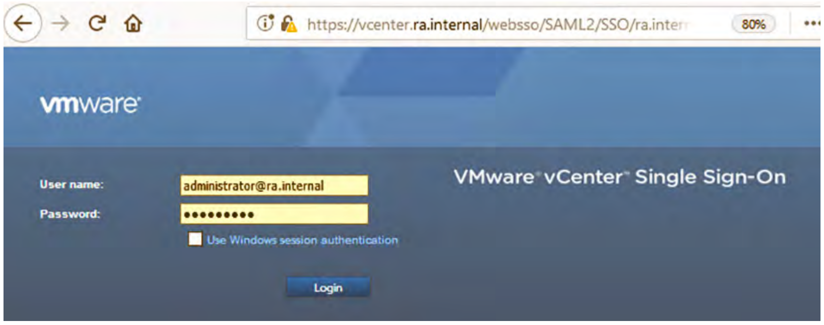
1. Access the VMware® vSphere® website: https://vcenter.ra.internal.
2. Under Getting Started, click Launch vSphere Client (HTML5).


Welcome to VMware vSphere
vmware
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

https://vcenter.ra.internal

Getting Started

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



https://vcenter.ra.internal/websso/SAML2/SSO/ra.inter

User name: administrator@ra.internal

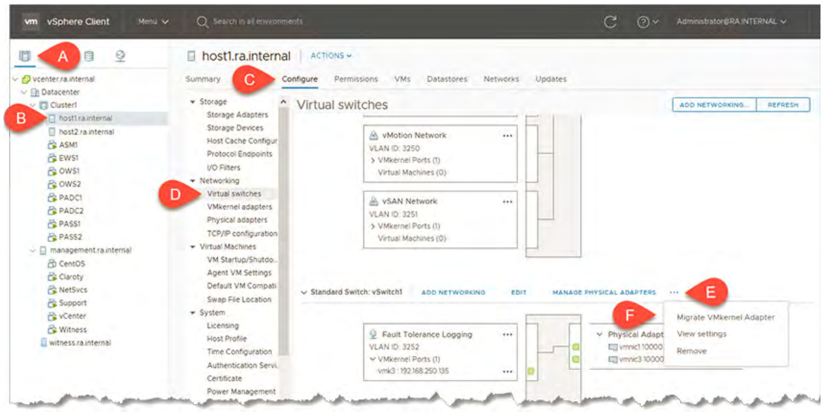
Password: ●●●●●●●●●

□ Use Windows session authentication

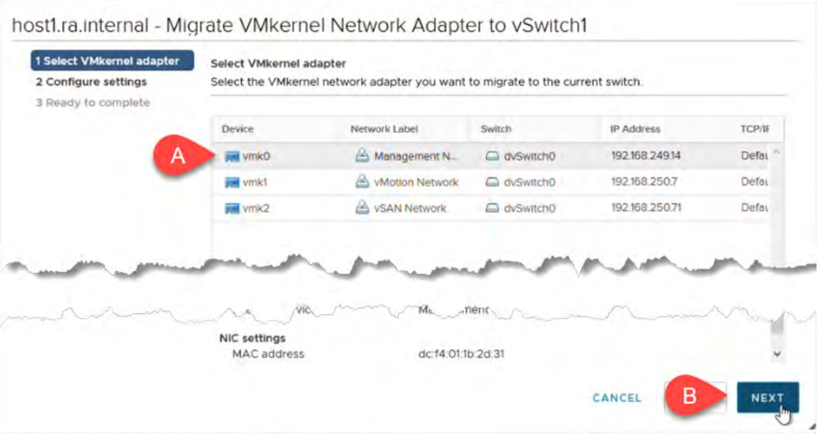
4. Navigate to the Hosts and Clusters tab (A).

   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 VMkernal Adapter.



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



host1.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

1 Select VMkernel adapter
2 Configure settings
3 Ready to complete

Select VMkernel adapter

Select the VMkernel network adapter you want to migrate to the current switch.

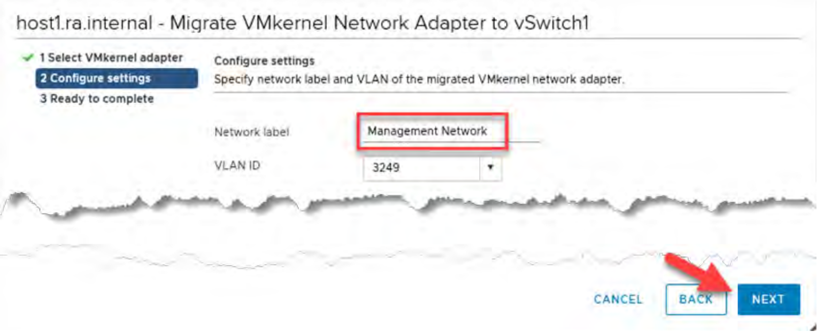
Device	Network Label	Switch	IP Address	TCP/IF
vmk0	Management N...	dvSwitch0	192.168.249.14	Defau
vmk1	vMotion Network	dvSwitch0	192.168.250.7	Defau
vmk2	vSAN Network	dvSwitch0	192.168.250.71	Defau

NIC settings
MAC address dc:f4:01:1b:2d:31

6. Name the Network Label “Management Network”.

IMPORTANT Don’t change the VLAN ID yet.

Click Next.



host1.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

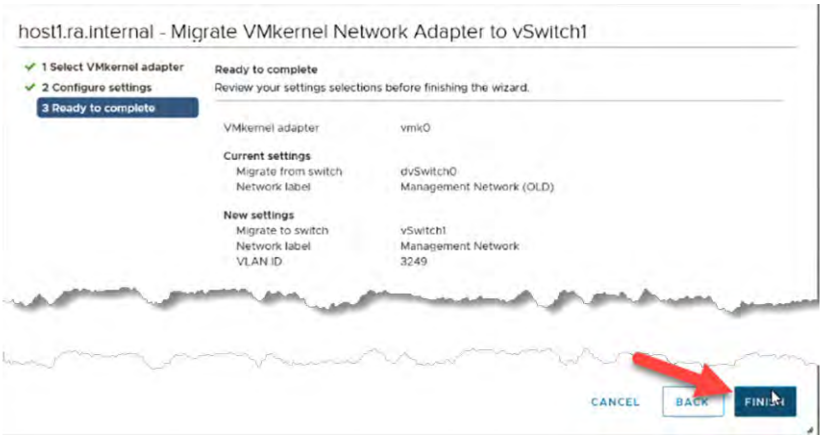
Configure settings

Specify network label and VLAN of the migrated VMkernel network adapter.

Network label: Management Network

VLAN ID: 3249

7. Review your settings and click Finish.



host1.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

Ready to complete

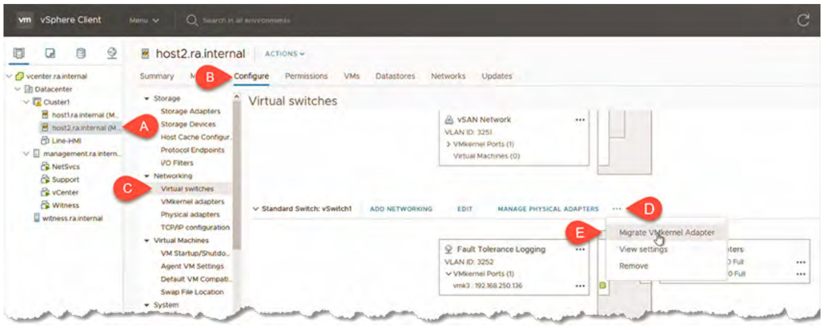
Review your settings selections before finishing the wizard.

VMkernel adapter	vmk0
Current settings	
Migrate from switch	dvSwitch0
Network label	Management Network (OLD)
New settings	
Migrate to switch	vSwitch1
Network label	Management Network
VLAN ID	3249

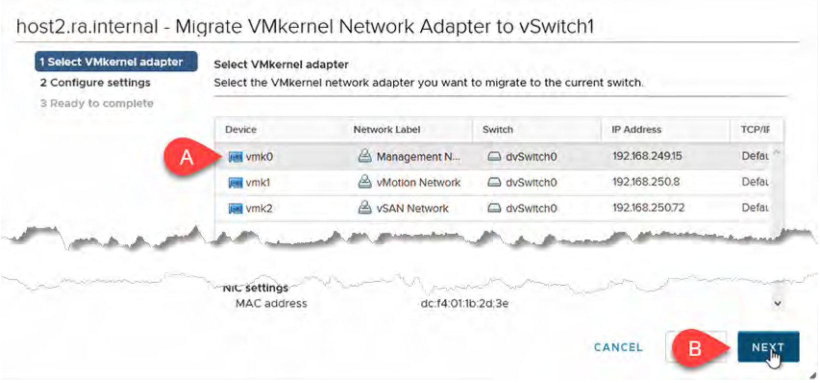
8. Repeat the process for Host2.

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).



host2.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

1 Select VMkernel adapter
2 Configure settings
3 Ready to complete

Select VMkernel adapter
Select the VMkernel network adapter you want to migrate to the current switch.

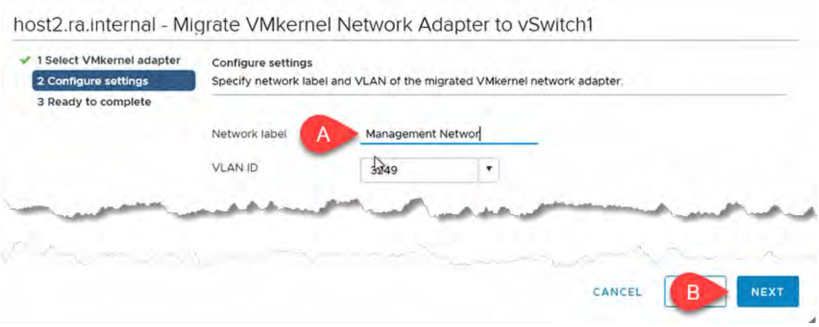
Device	Network Label	Switch	IP Address	TCP/IF
vmk0	Management N...	dvSwitch0	192.168.249.15	Defau
vmk1	vMotion Network	dvSwitch0	192.168.250.8	Defau
vmk2	vSAN Network	dvSwitch0	192.168.250.72	Defau

NIC settings
MAC address dc:f4:01:1b:2d:3e

10. Name the Network Label “Management Network” (A).

IMPORTANT Don’t change the VLAN ID yet.

Click Next (B).



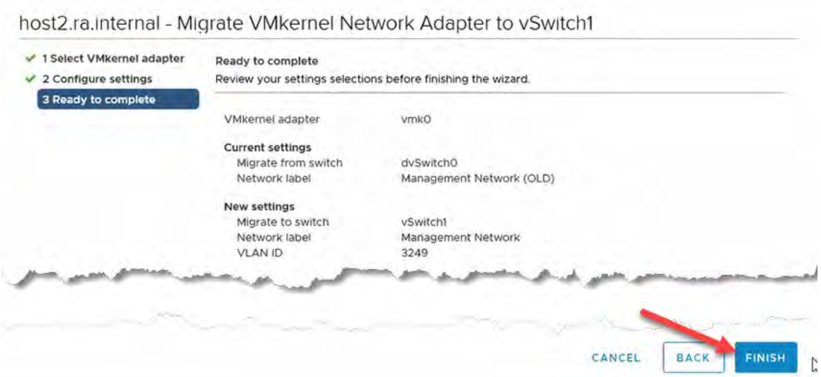
host2.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

✓ 1 Select VMkernel adapter
2 Configure settings
3 Ready to complete

Configure settings
Specify network label and VLAN of the migrated VMkernel network adapter.

Network label: Management Networ
VLAN ID: 3249

11. Review your settings and click Finish.



host2.ra.internal - Migrate VMkernel Network Adapter to vSwitch1

✓ 1 Select VMkernel adapter
✓ 2 Configure settings
3 Ready to complete

Ready to complete
Review your settings selections before finishing the wizard.

VMkernel adapter: vmk0

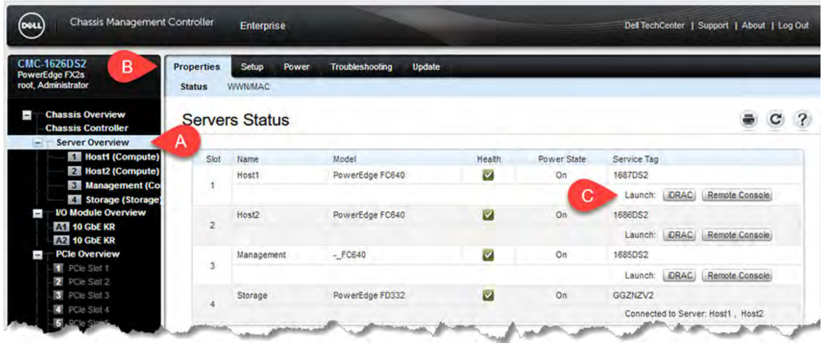
Current settings
Migrate from switch: dvSwitch0
Network label: Management Network (OLD)

New settings
Migrate to switch: vSwitch1
Network label: Management Network
VLAN ID: 3249

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.



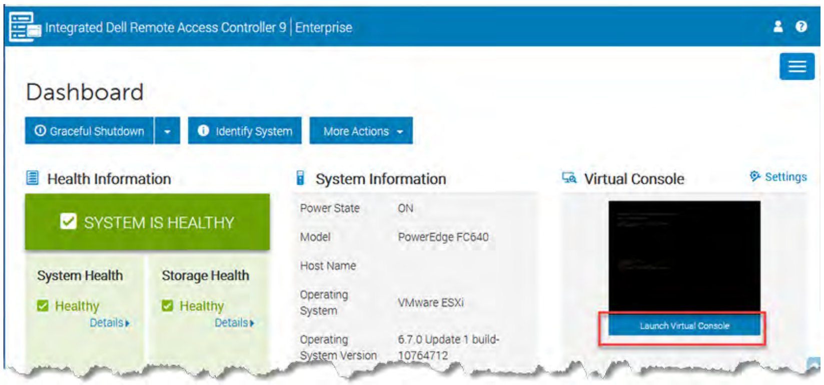
Servers Status

Slot	Name	Model	Health	Power State	Service Tag
1	Host1	PowerEdge FC640	☑	On	1687DS2 Launch: iDRAC Remote Console
2	Host2	PowerEdge FC640	☑	On	1686DS2 Launch: iDRAC Remote Console
3	Management	-_FC640	☑	On	1685DS2 Launch: iDRAC Remote Console
4	Storage	PowerEdge FD332	☑	On	GGZNZV2 Connected to Server: Host1 , Host2

   The Remote Access Controller opens in a separate tabbed browser.

   TIP If prompted, disable your popup blocker.

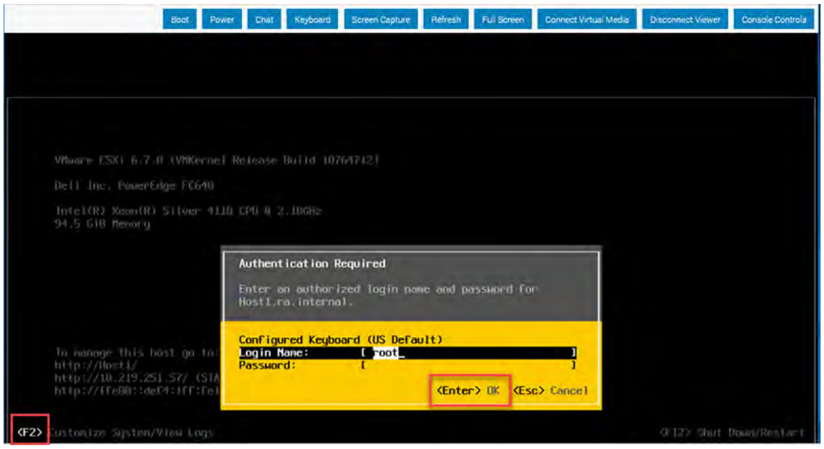
2. Click Launch Virtual Console.



Power State	ON
Model	PowerEdge FC640
Host Name	
Operating System	VMware ESXi
Operating System Version	6.7.0 Update 1 build-10764712

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

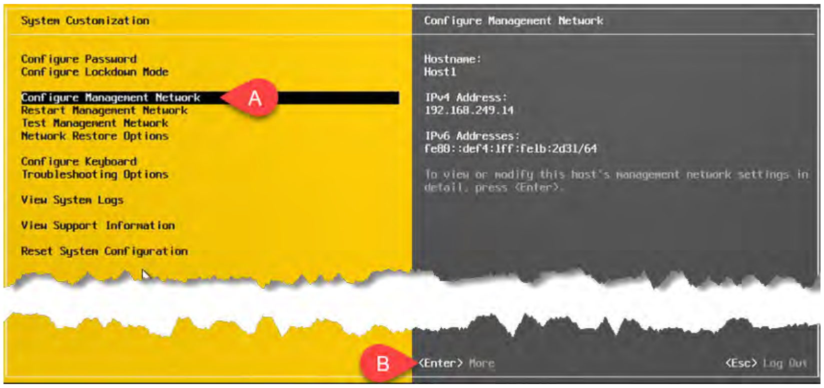
   Log in with root and system password, and then press Enter.



```
VMware ESXi 6.7.0 (VMKernel Release Build 10764712)

Dell Inc. PowerEdge FC640

Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
94.5 GiB Memory

Authentication Required

Enter an authorized login name and password for
Host1.ra.internal.

Configured Keyboard (US Default)
Login Name:          [ root_                    ]
Password:            [                          ]

                         <Enter> OK  <Esc> Cancel

To manage this host go to:
http://Host1/
http://10.219.251.57/ (STA
http://[fe80::def4:ff:fe

<F2> Customize System/View Logs                  <F12> Shut Down/Restart
```

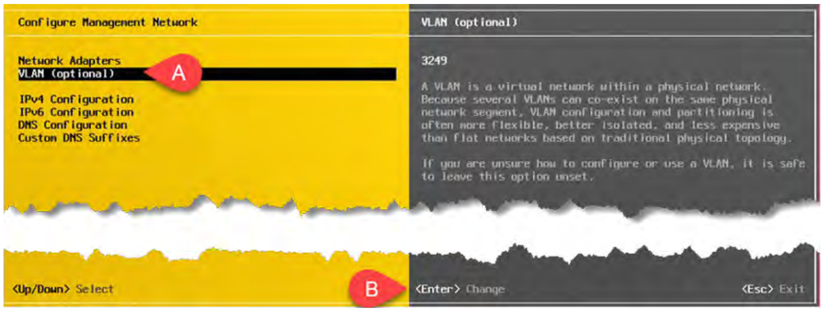
4. In the ESXi Direct Console User Interface (DCUI), navigate to Configure Management Network (A) and press Enter (B).

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



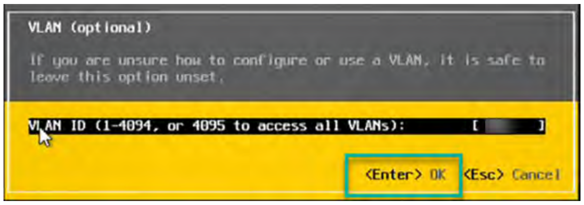
```
System Customization                        Configure Management Network

Configure Password                          Hostname:
Configure Lockdown Mode                     Host1

Configure Management Network                IPv4 Address:
Restart Management Network                  192.168.249.14
Test Management Network
Network Restore Options                     IPv6 Addresses:
                                            fe80::def4:1ff:fe1b:2d31/64
Configure Keyboard
Troubleshooting Options                     To view or modify this host's management network settings in
                                            detail, press <Enter>.
View System Logs

View Support Information

Reset System Configuration

                                            <Enter> More                          <Esc> Log Out
```

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



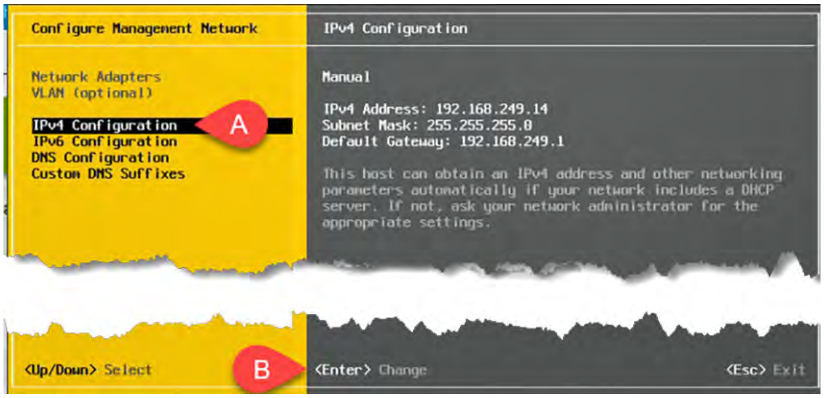
```
Configure Management Network                VLAN (optional)

Network Adapters                            3249
VLAN (optional)
                                            A VLAN is a virtual network within a physical network.
IPv4 Configuration                          Because several VLANs can co-exist on the same physical
IPv6 Configuration                          network segment, VLAN configuration and partitioning is
DNS Configuration                           often more flexible, better isolated, and less expensive
Custom DNS Suffixes                         than flat networks based on traditional physical topology.

                                            If you are unsure how to configure or use a VLAN, it is safe
                                            to leave this option unset.

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

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



```
VLAN (optional)

If you are unsure how to configure or use a VLAN, it is safe to
leave this option unset.

VLAN ID (1-4094, or 4095 to access all VLANs):       [ [redacted] ]

                                      <Enter> OK  <Esc> Cancel
```

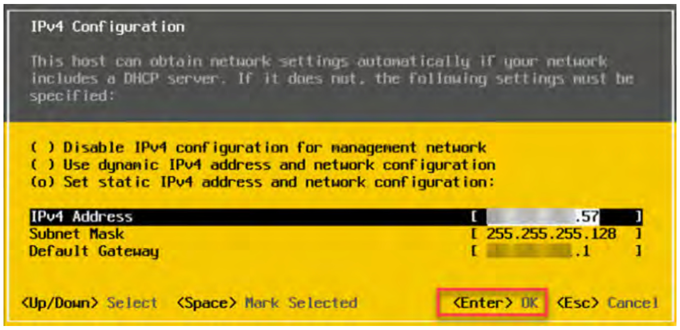
7. Select IPv4 Configuration (A) and press Enter (B).



```
Configure Management Network       IPv4 Configuration

Network Adapters                   Manual
VLAN (optional)
                                   IPv4 Address: 192.168.249.14
IPv4 Configuration                 Subnet Mask: 255.255.255.0
IPv6 Configuration                 Default Gateway: 192.168.249.1
DNS Configuration
Custom DNS Suffixes                This host can obtain an IPv4 address and other networking
                                   parameters automatically if your network includes a DHCP
                                   server. If not, ask your network administrator for the
                                   appropriate settings.

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

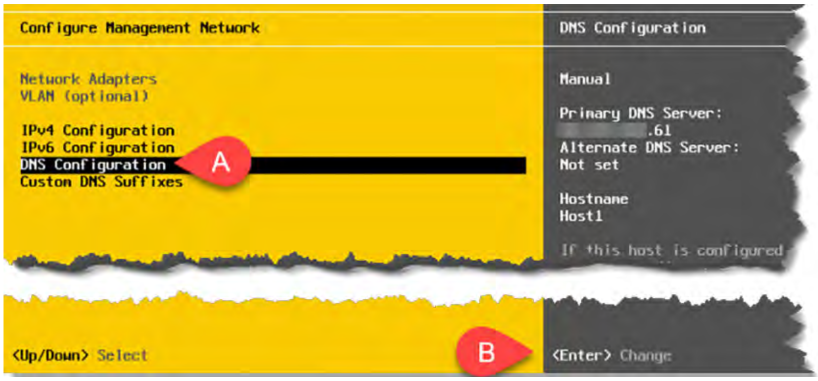
8. With the Up and Down arrow keys, change the IPv4 settings to the desired configuration.

   Press Enter when complete.



```
IPv4 Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Disable IPv4 configuration for management network
( ) Use dynamic IPv4 address and network configuration
(o) Set static IPv4 address and network configuration:

IPv4 Address                                    [ [redacted].57    ]
Subnet Mask                                     [ 255.255.255.128  ]
Default Gateway                                 [ [redacted].1     ]

<Up/Down> Select   <Space> Mark Selected        <Enter> OK  <Esc> Cancel
```

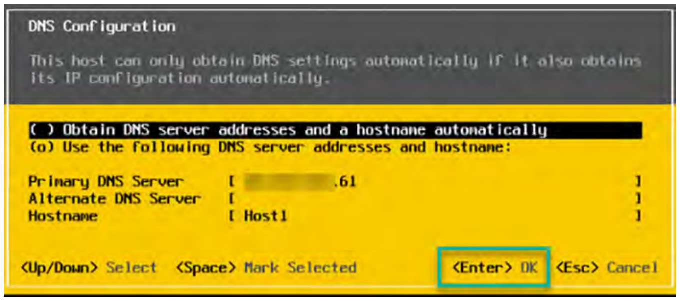
9. Select DNS configuration (A) and press Enter (B).



```
Configure Management Network                    DNS Configuration

Network Adapters                                Manual
VLAN (optional)
                                                Primary DNS Server:
IPv4 Configuration                              [redacted].61
IPv6 Configuration                              Alternate DNS Server:
DNS Configuration                               Not set
Custom DNS Suffixes
                                                Hostname
                                                Host1

                                                If this host is configured

<Up/Down> Select                                <Enter> Change
```

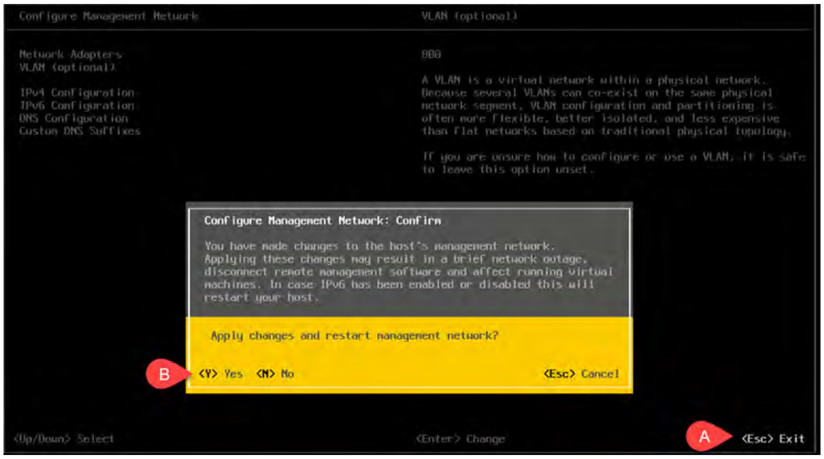
10. Enter the new IP address of the NetSvcs (DNS).

    When completed, press Enter.



```
DNS Configuration

This host can only obtain DNS settings automatically if it also obtains
its IP configuration automatically.

( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:

Primary DNS Server      [ [redacted].61                              ]
Alternate DNS Server    [                                            ]
Hostname                [ Host1                                      ]

<Up/Down> Select   <Space> Mark Selected        <Enter> OK  <Esc> Cancel
```

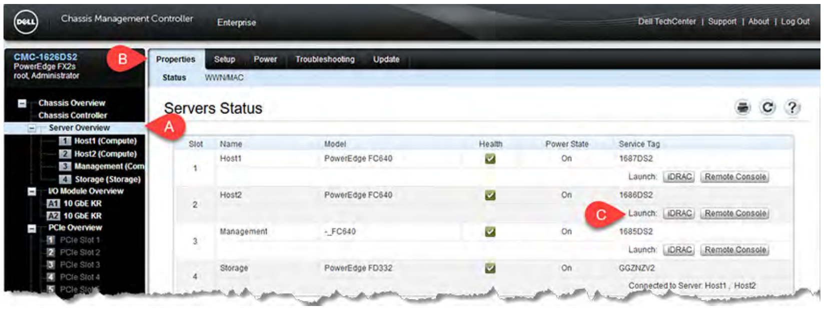
11. To exit, press the Esc key (A) and then press Y (B) to confirm your changes.



```
Configure Management Network                    VLAN (optional)

Network Adapters                                808
VLAN (optional)
                                                A VLAN is a virtual network within a physical network.
IPv4 Configuration                              Because several VLANs can co-exist on the same physical
IPv6 Configuration                              network segment, VLAN configuration and partitioning is
DNS Configuration                               often more flexible, better isolated, and less expensive
Custom DNS Suffixes                             than flat networks based on traditional physical topology.

                                                If you are unsure how to configure or use a VLAN, it is safe
                                                to leave this option unset.

          Configure Management Network: Confirm

          You have made changes to the host's management network.
          Applying these changes may result in a brief network outage,
          disconnect remote management software and affect running virtual
          machines. In case IPv6 has been enabled or disabled this will
          restart your host.

           Apply changes and restart management network?

          <Y> Yes  <N> No                                <Esc> Cancel

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

12. Switch to the CMC, navigate to Server Overview (A) > Properties (B).

On Servers Status, click Launch: iDRAC (C) for Host2.



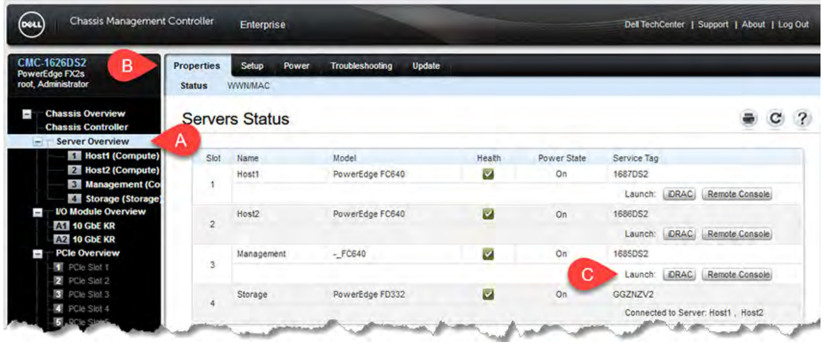
Servers Status

Slot	Name	Model	Health	Power State	Service Tag
1	Host1	PowerEdge FC640	✓	On	1687DS2 Launch: iDRAC Remote Console
2	Host2	PowerEdge FC640	✓	On	1686DS2 Launch: iDRAC Remote Console
3	Management	-_FC640	✓	On	1685DS2 Launch: iDRAC Remote Console
4	Storage	PowerEdge FD332	✓	On	GGZNZV2 Connected to Server: Host1 , 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.



Servers Status

Slot	Name	Model	Health	Power State	Service Tag
1	Host1	PowerEdge FC640	✓	On	1687DS2 Launch: iDRAC Remote Console
2	Host2	PowerEdge FC640	✓	On	1686DS2 Launch: iDRAC Remote Console
3	Management	-_FC640	✓	On	1685DS2 Launch: iDRAC Remote Console
4	Storage	PowerEdge FD332	✓	On	GGZNZV2 Connected to Server: Host1 , Host2

15. Starting on page 32, repeat step 2... step 11 for Management.

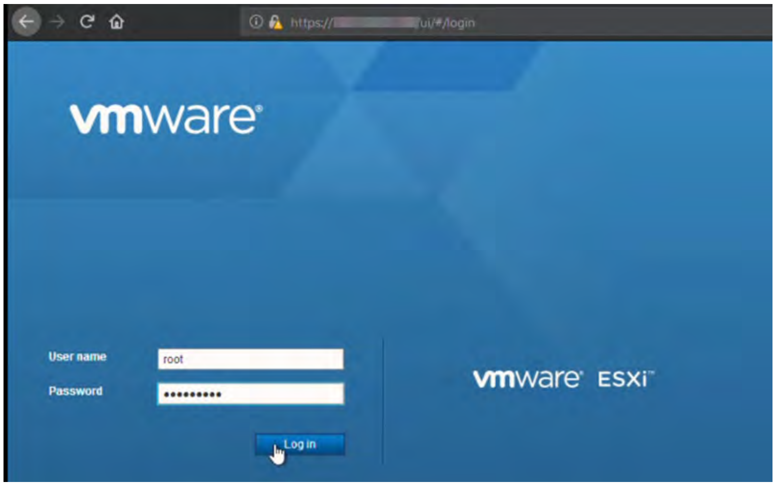
IMPORTANT Because the Management host uses a Standard vSwitch, it is not necessary to access vCenter.

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.



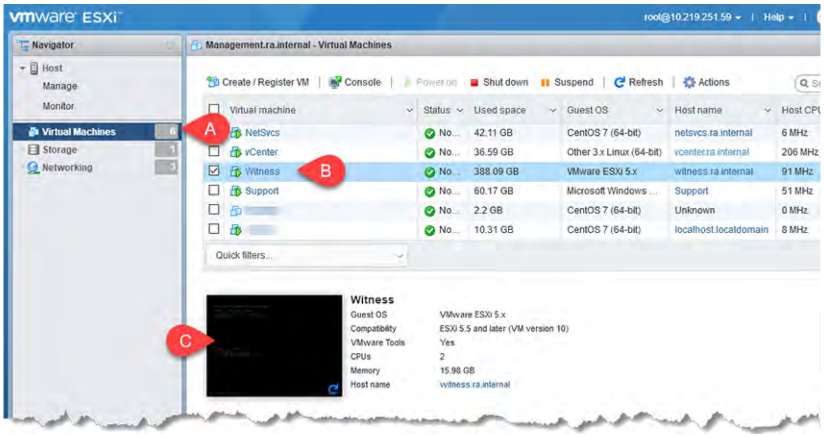
https://[redacted]/ui/#/login

User name: root

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.



root@10.219.251.59

Management.ra.internal - Virtual Machines

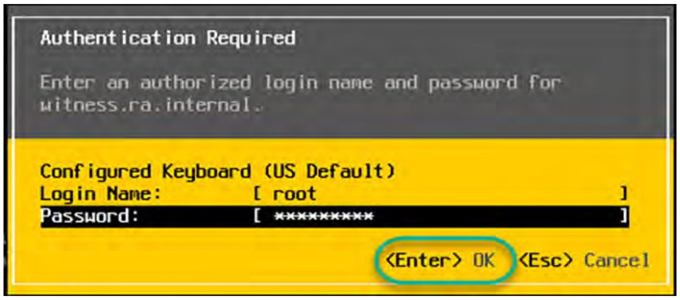
☐	Virtual machine	Status	Used space	Guest OS	Host name	Host CPU
☐	NetSvcs	No...	42.11 GB	CentOS 7 (64-bit)	netsvcs.ra.internal	6 MHz
☐	vCenter	No...	36.59 GB	Other 3.x Linux (64-bit)	vcenter.ra.internal	206 MHz
☑	Witness	No...	388.09 GB	VMware ESXi 5.x	witness.ra.internal	91 MHz
☐	Support	No...	60.17 GB	Microsoft Windows ...	Support	51 MHz
☐	[redacted]	No...	2.2 GB	CentOS 7 (64-bit)	Unknown	0 MHz
☐	[redacted]	No...	10.31 GB	CentOS 7 (64-bit)	localhost.localdomain	8 MHz

Witness

Guest OS	VMware ESXi 5.x
Compatibility	ESXi 5.5 and later (VM version 10)
VMware Tools	Yes
CPUs	2
Memory	15.98 GB
Host name	witness.ra.internal

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

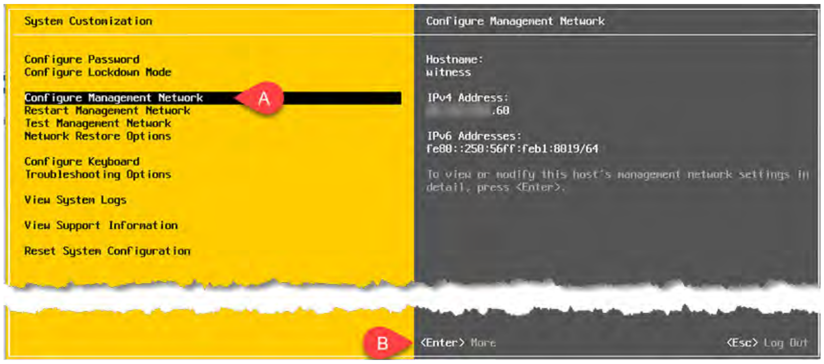
   Log in with root and the system password, and then press Enter.



```
Authentication Required

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

Configured Keyboard (US Default)
Login Name:          [ root                    ]
Password:            [ **********              ]

                              <Enter> OK  <Esc> Cancel
```

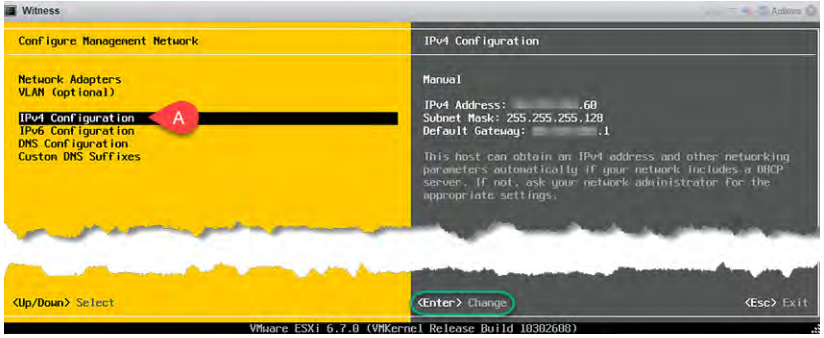
4. In the ESXi DCUI, navigate to Configure Management Network (A) and press Enter (B).

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



```
System Customization                     Configure Management Network

Configure Password                       Hostname:
Configure Lockdown Mode                  witness

Configure Management Network             IPv4 Address:
Restart Management Network               [redacted].60
Test Management Network
Network Restore Options                  IPv6 Addresses:
                                         fe80::250:56ff:feb1:8019/64
Configure Keyboard
Troubleshooting Options                  To view or modify this host's management network settings in
                                         detail, press <Enter>.
View System Logs

View Support Information

Reset System Configuration

                                         <Enter> More                         <Esc> Log Out
```

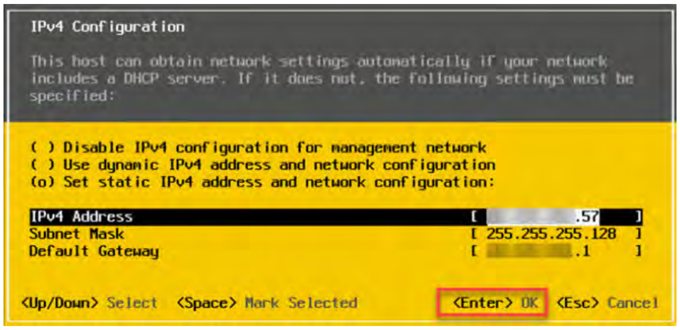
5. Select IPv4 Configuration, and press Enter.



```
Witness                                                                      Actions

Configure Management Network             IPv4 Configuration

Network Adapters                         Manual
VLAN (optional)
                                         IPv4 Address: [redacted].60
IPv4 Configuration                       Subnet Mask: 255.255.255.128
IPv6 Configuration                       Default Gateway: [redacted].1
DNS Configuration
Custom DNS Suffixes                      This host can obtain an IPv4 address and other networking
                                         parameters automatically if your network includes a DHCP
                                         server. If not, ask your network administrator for the
                                         appropriate settings.

<Up/Down> Select                         <Enter> Change                       <Esc> Exit
                   VMware ESXi 6.7.0 (VMKernel Release Build 10302608)
```

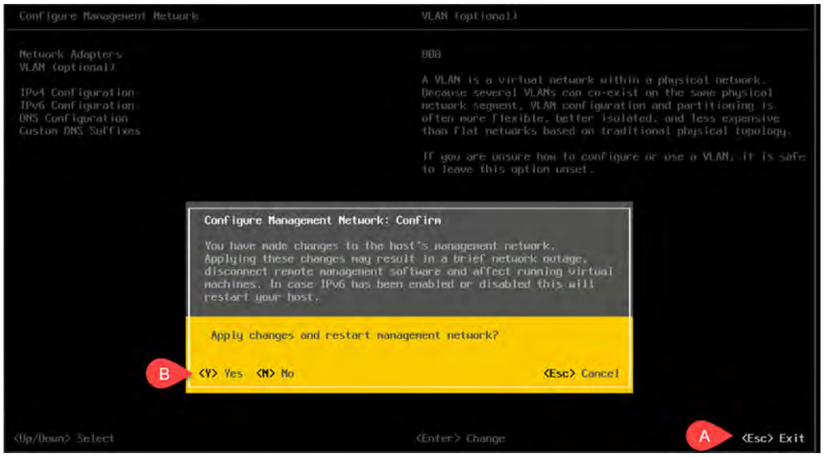
6. With the Up and Down arrow keys, change the IPv4 settings to the desired configuration.

   When completed, press Enter.



```
IPv4 Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Disable IPv4 configuration for management network
( ) Use dynamic IPv4 address and network configuration
(o) Set static IPv4 address and network configuration:

IPv4 Address                                      [ [redacted].57     ]
Subnet Mask                                       [ 255.255.255.128   ]
Default Gateway                                   [ [redacted].1      ]

<Up/Down> Select   <Space> Mark Selected          <Enter> OK  <Esc> Cancel
```

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

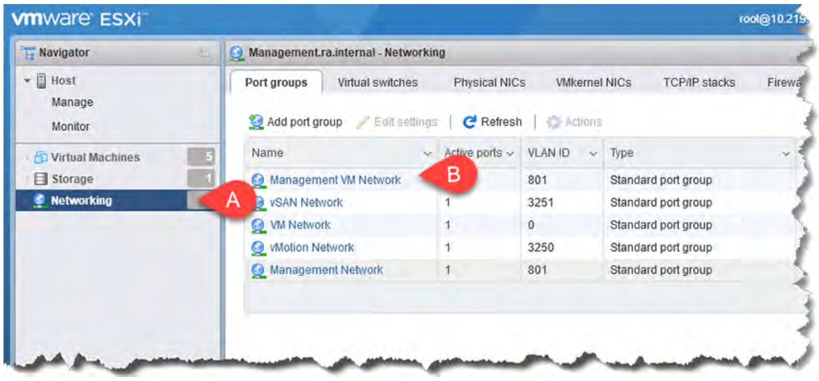


```
Configure Management Network                     VLAN (optional)

Network Adapters                                 800
VLAN (optional)
                                                 A VLAN is a virtual network within a physical network.
IPv4 Configuration                               Because several VLANs can co-exist on the same physical
IPv6 Configuration                               network segment, VLAN configuration and partitioning is
DNS Configuration                                often more flexible, better isolated, and less expensive
Custom DNS Suffixes                              than flat networks based on traditional physical topology.

                                                 If you are unsure how to configure or use a VLAN, it is safe
                                                 to leave this option unset.

          Configure Management Network: Confirm

          You have made changes to the host's management network.
          Applying these changes may result in a brief network outage,
          disconnect remote management software and affect running virtual
          machines. In case IPv6 has been enabled or disabled this will
          restart your host.

           Apply changes and restart management network?

          <Y> Yes  <N> No                                   <Esc> Cancel

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

8. Close the Web Console.

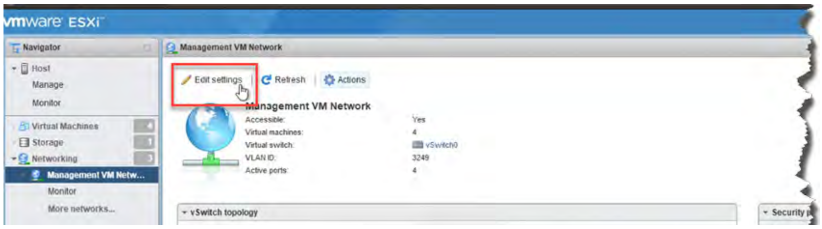
   You must change the VLAN ID of the Witness host in the ESXi Web GUI.

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



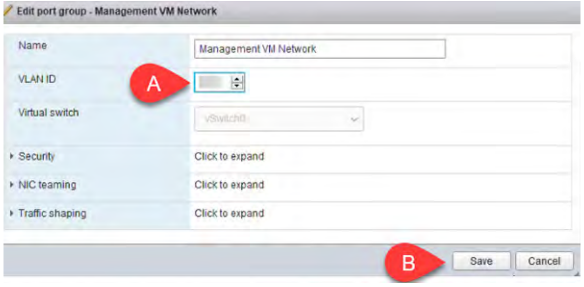
Name	Active ports	VLAN ID	Type
Management VM Network		801	Standard port group
vSAN Network	1	3251	Standard port group
VM Network	1	0	Standard port group
vMotion Network	1	3250	Standard port group
Management Network	1	801	Standard port group

10. Click Edit settings.



Management VM Network
Accessible: Yes
Virtual machines: 4
Virtual switch: vSwitch0
VLAN ID: 3249
Active ports: 4

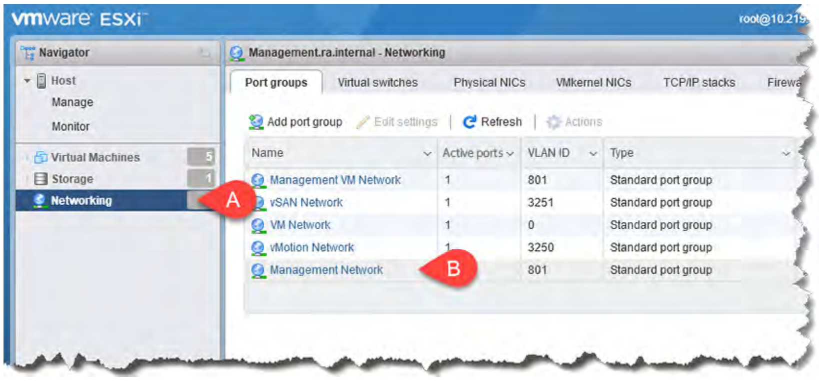
11. Change the VLAN ID (A) to the desired value, and then click Save (B).



Edit port group - Management VM Network

Name: Management VM Network
VLAN ID:
Virtual switch: vSwitch0
Security: Click to expand
NIC teaming: Click to expand
Traffic shaping: Click to expand

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

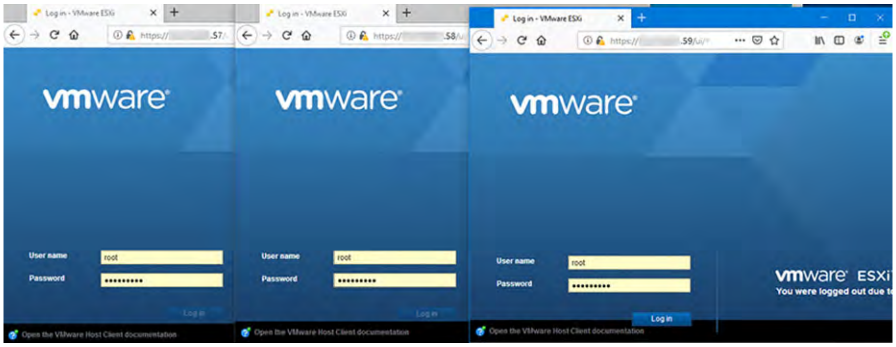


Name	Active ports	VLAN ID	Type
Management VM Network	1	801	Standard port group
vSAN Network	1	3251	Standard port group
VM Network	1	0	Standard port group
vMotion Network	1	3250	Standard port group
Management Network		801	Standard port group

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.


Log in - VMware ESXi
vmware
Log in
Open the VMware Host Client documentation
vmware ESXi
You were logged out due t

User name root
Password ••••••••••

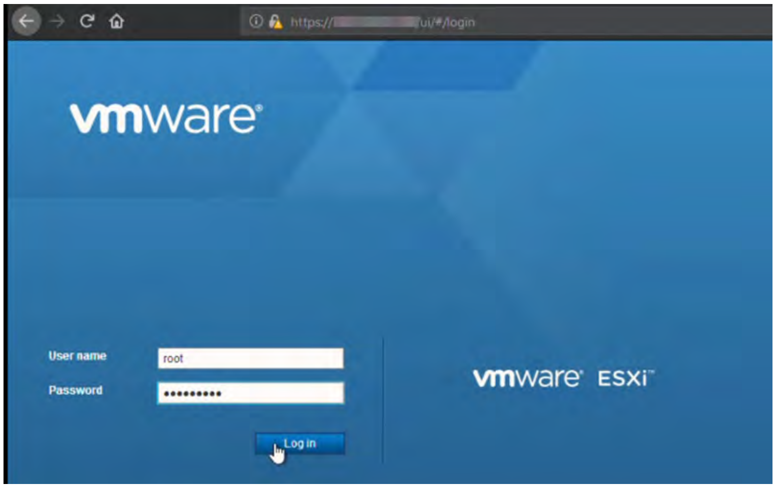
Modify the Virtual Machine IP Addresses

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.

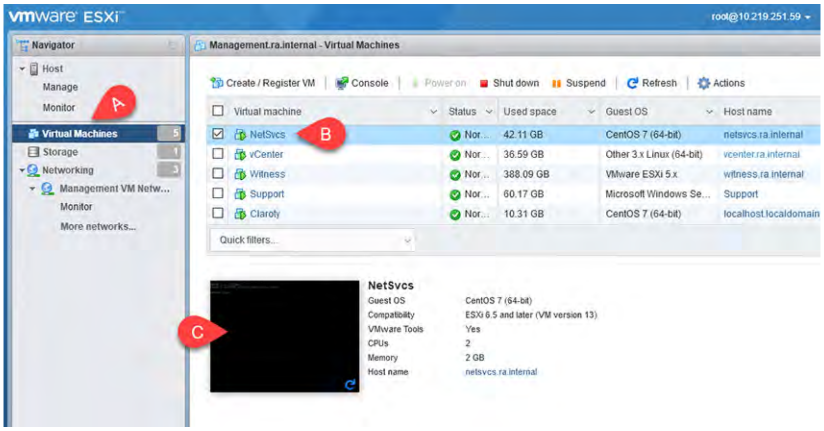
   Log in with root and the system-wide password.



User name root
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).

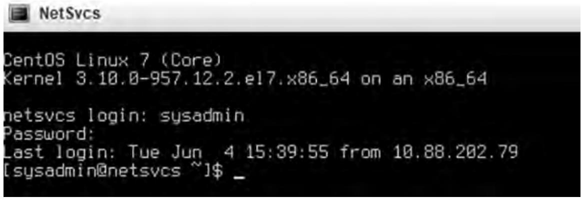


	Virtual machine	Status	Used space	Guest OS	Host name
☑	NetSvcs	Nor...	42.11 GB	CentOS 7 (64-bit)	netsvcs.ra.internal
□	vCenter	Nor...	36.59 GB	Other 3.x Linux (64-bit)	vcenter.ra.internal
□	Witness	Nor...	388.09 GB	VMware ESXi 5.x	witness.ra.internal
□	Support	Nor...	60.17 GB	Microsoft Windows Se...	Support
□	Claroty	Nor...	10.31 GB	CentOS 7 (64-bit)	localhost.localdomain

NetSvcs

Guest OS	CentOS 7 (64-bit)
Compatibility	ESXi 6.5 and later (VM version 13)
VMware Tools	Yes
CPUs	2
Memory	2 GB
Host name	netsvcs.ra.internal

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

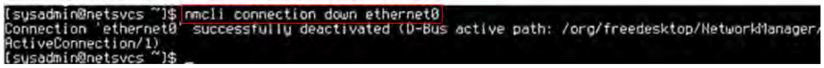


NetSvcs

```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.12.2.el7.x86_64 on an x86_64

netsvcs login: sysadmin
Password:
Last login: Tue Jun  4 15:39:55 from 10.88.202.79
[sysadmin@netsvcs ~]$ _
```

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

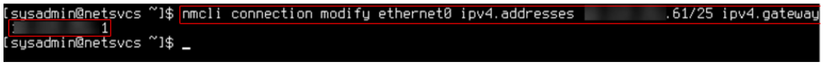
   ```
   nmcli connection down ethernet0
   ```



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

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

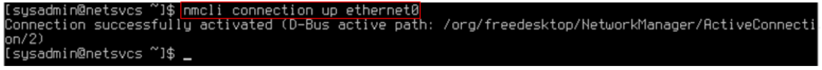
   ```
   nmcli connection modify ethernet0 ipv4.addresses xx.xx.xx.xx/
   25 ipv4.gateway xx.xx.xx.xx
   ```



```
[sysadmin@netsvcs ~]$ nmcli connection modify ethernet0 ipv4.addresses [redacted].61/25 ipv4.gateway
[redacted]1
[sysadmin@netsvcs ~]$ _
```

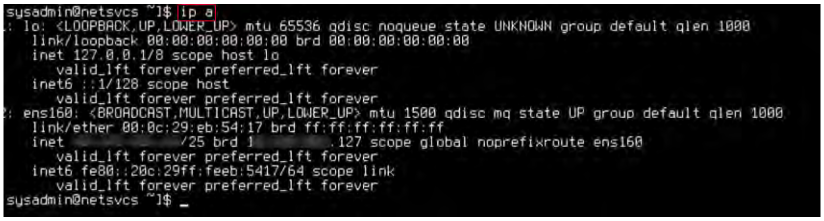
6. Activate the following interface:

   ```
   nmcli connection up ethernet0
   ```



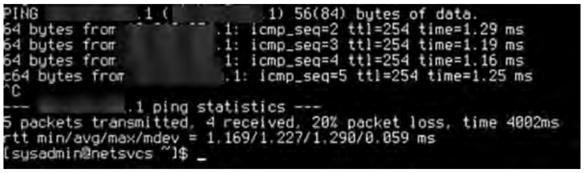
```
[sysadmin@netsvcs ~]$ nmcli connection up ethernet0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnecti
on/2)
[sysadmin@netsvcs ~]$ _
```

7. Verify that the IP address changed by typing: ip a



```
sysadmin@netsvcs ~]$ ip a
: 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
: 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 [redacted]/25 brd [redacted].127 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 ~]$ _
```

8. Test (ping) your connection to the gateway.

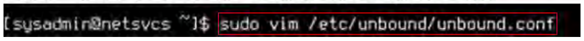


```
PING [redacted].1 ([redacted].1) 56(84) bytes of data.
64 bytes from [redacted].1: icmp_seq=2 ttl=254 time=1.29 ms
64 bytes from [redacted].1: icmp_seq=3 ttl=254 time=1.19 ms
64 bytes from [redacted] 1: icmp_seq=4 ttl=254 time=1.16 ms
c64 bytes from [redacted].1: icmp_seq=5 ttl=254 time=1.25 ms
^C
--- [redacted].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

1. While still in the NetSvcs VM, type the following command:

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



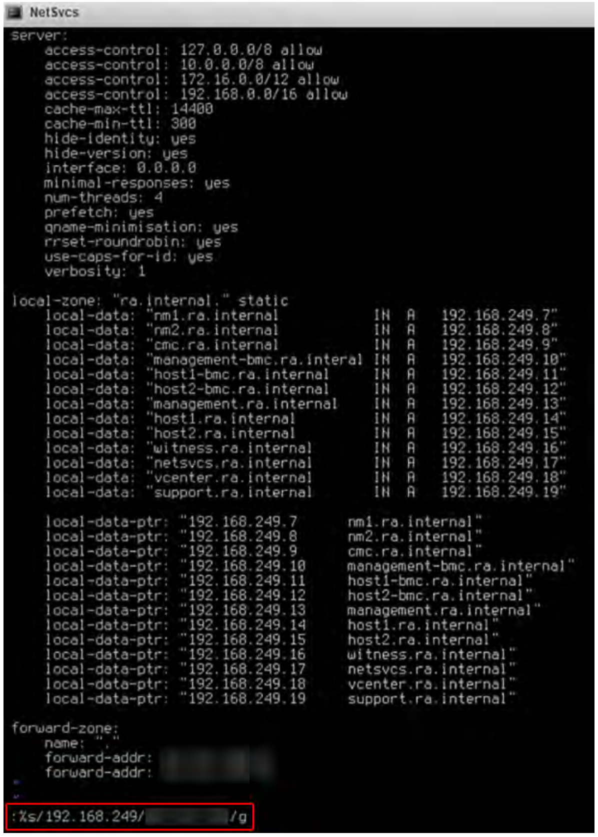
```
[sysadmin@netsvcs ~]$ sudo vim /etc/unbound/unbound.conf
```

2. 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
    rrset-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.interal  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: [redacted]
    forward-addr:
~
~
:%s/192.168.249/[redacted]/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.

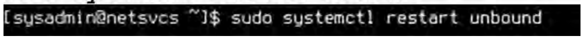
   TIP Sites that reuse an existing Windows Active Directory or are deployed without a Windows Active Directory on the Operational Technology network require that the forward-addr field change to the upstream DNS server.

6. Type:wq

7. Press Enter afterwards to write and then quit.

8. Enter the following command:

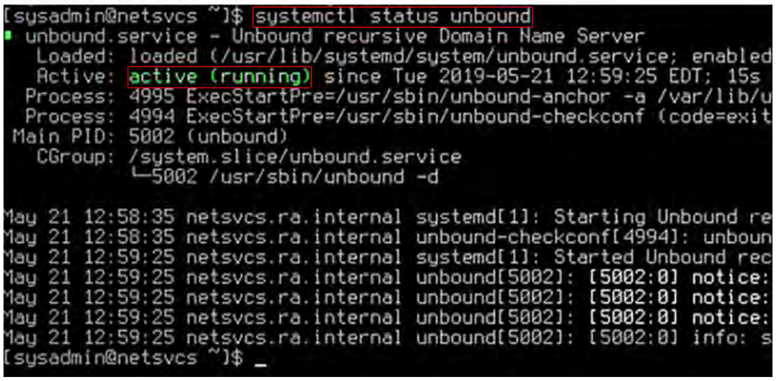
```
sudo systemctl restart unbound
```



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

   No feedback is returned if the services restart successfully.

9. 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: 4995 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]: unboun
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.

10. Type:Logout

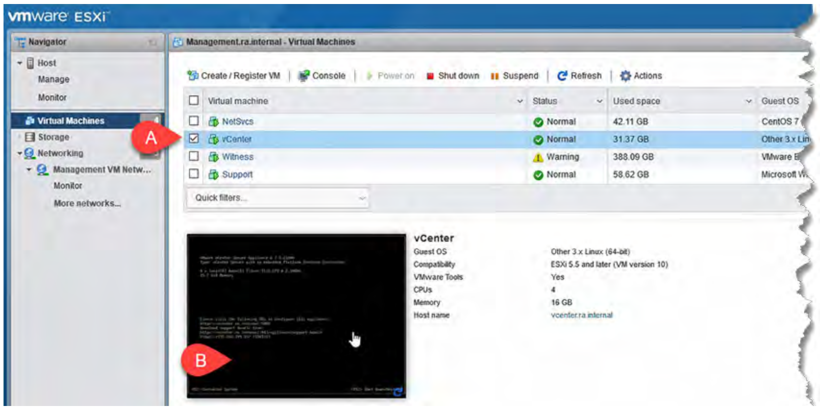
11. Press Enter to close the NetSvcs DCUI.

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.

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



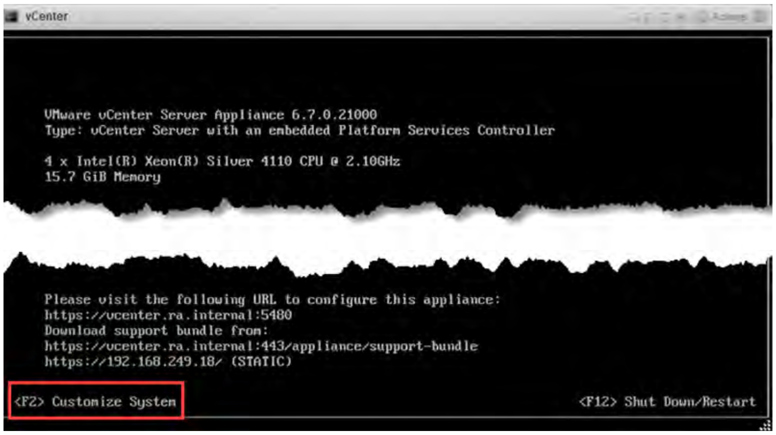
Management.ra.internal - Virtual Machines

☐	Virtual machine	Status	Used space	Guest OS
☐	NetSvcs	Normal	42.11 GB	CentOS 7
☑	vCenter	Normal	31.37 GB	Other 3.x Lin
☐	Witness	Warning	388.09 GB	VMware E
☐	Support	Normal	58.62 GB	Microsoft W

vCenter

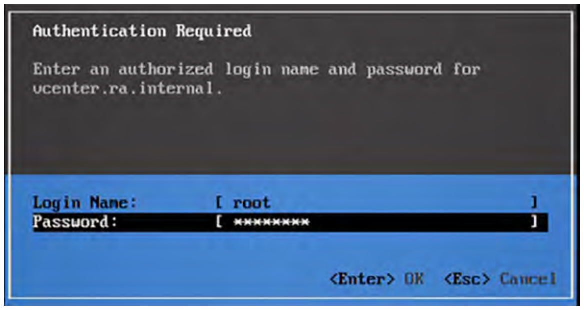
Guest OS: Other 3.x Linux (64-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Yes
CPUs: 4
Memory: 16 GB
Host name: vcenter.ra.internal

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



```
vCenter

  VMware vCenter Server Appliance 6.7.0.21000
  Type: vCenter Server with an embedded Platform Services Controller

  4 x Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
  15.7 GiB Memory

  Please visit the following URL to configure this appliance:
  https://vcenter.ra.internal:5480
  Download support bundle from:
  https://vcenter.ra.internal:443/appliance/support-bundle
  https://192.168.249.18/ (STATIC)

<F2> Customize System                                    <F12> Shut Down/Restart
```

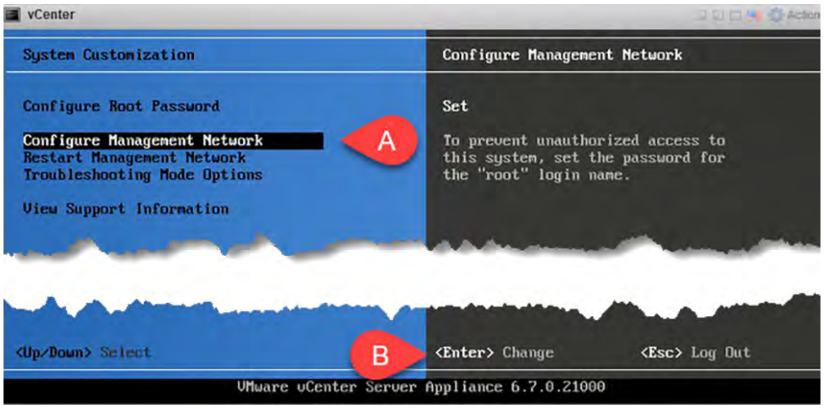
Log in with root and the system password, and then press Enter.



```
Authentication Required

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


Login Name:        [ root                  ]
Password:          [ ********              ]

                                 <Enter> OK  <Esc> Cancel
```

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

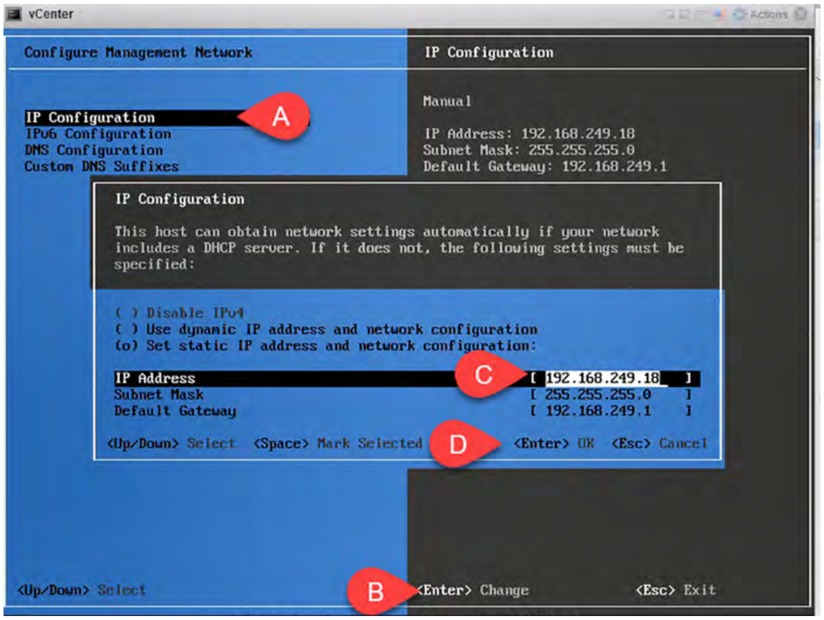
TIP Your mouse does not work in the vCenter console. You must navigate entirely with your keyboard.



```
vCenter
System Customization                    Configure Management Network

Configure Root Password                 Set

Configure Management Network            To prevent unauthorized access to
Restart Management Network              this system, set the password for
Troubleshooting Mode Options            the "root" login name.

View Support Information

<Up/Down> Select                        <Enter> Change          <Esc> Log Out
                    VMware vCenter Server Appliance 6.7.0.21000
```

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).



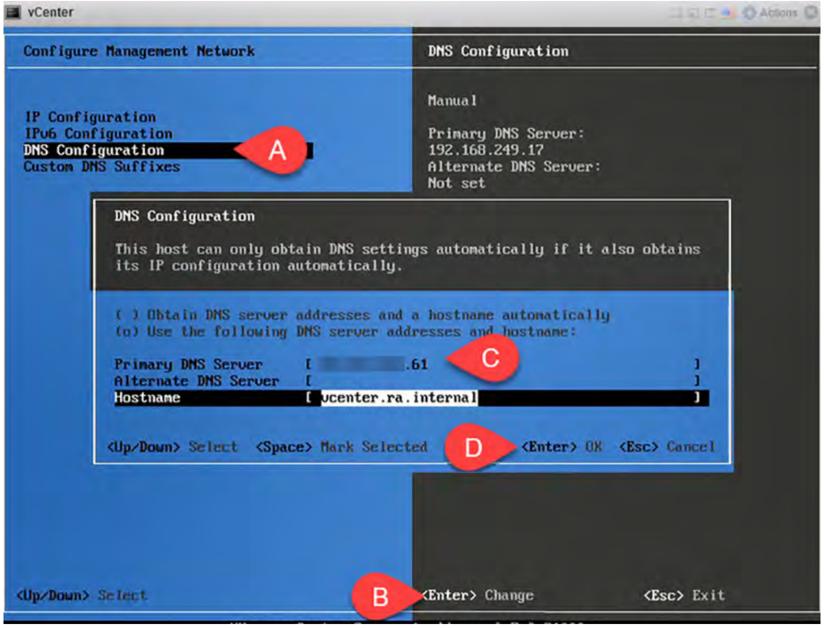
```
Configure Management Network          IP Configuration

                                      Manual
IP Configuration
IPv6 Configuration                    IP Address: 192.168.249.18
DNS Configuration                     Subnet Mask: 255.255.255.0
Custom DNS Suffixes                   Default Gateway: 192.168.249.1

     IP Configuration

     This host can obtain network settings automatically if your network
     includes a DHCP server. If it does not, the following settings must be
     specified:

     ( ) Disable IPv4
     ( ) Use dynamic IP address and network configuration
     (o) Set static IP address and network configuration:

     IP Address                                    [ 192.168.249.18  ]
     Subnet Mask                                   [ 255.255.255.0   ]
     Default Gateway                               [ 192.168.249.1   ]

    <Up/Down> Select  <Space> Mark Selected       <Enter> OK  <Esc> Cancel

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

6. Select DNS Configuration (A) and press Enter (B).

   Change the Primary DNS Server to your desired setting (C).

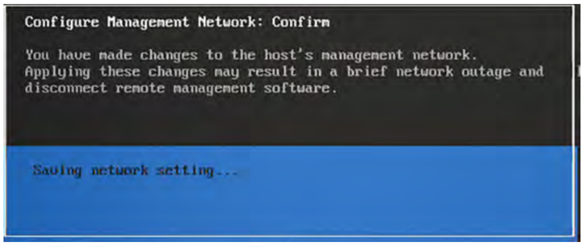
IMPORTANT Do not change the host name.

When completed, press Enter (D).



```
Configure Management Network          DNS Configuration

                                      Manual
IP Configuration
IPv6 Configuration                    Primary DNS Server:
DNS Configuration                     192.168.249.17
Custom DNS Suffixes                   Alternate DNS Server:
                                      Not set

     DNS Configuration

     This host can only obtain DNS settings automatically if it also obtains
     its IP configuration automatically.

     ( ) Obtain DNS server addresses and a hostname automatically
     (o) Use the following DNS server addresses and hostname:

     Primary DNS Server     [ [redacted].61                          ]
     Alternate DNS Server   [                                        ]
     Hostname               [ vcenter.ra.internal                    ]

    <Up/Down> Select  <Space> Mark Selected       <Enter> OK  <Esc> Cancel

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

7. To save network settings, press Y.

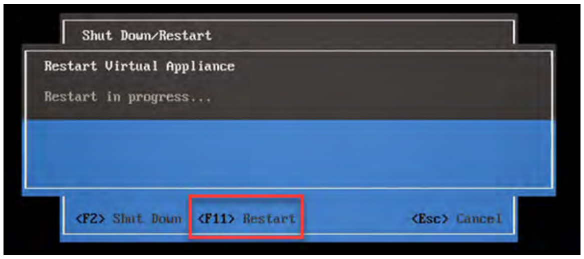


```
Configure Management Network: Confirm

You have made changes to the host's management network.
Applying these changes may result in a brief network outage and
disconnect remote management software.

Saving network setting...
```

8. To log off, press Esc .

9. To restart vCenter, press F12. You need to authenticate.

10. To restart, press F11.



```
Shut Down/Restart
Restart Virtual Appliance

Restart in progress...

<F2> Shut Down  <F11> Restart          <Esc> Cancel
```

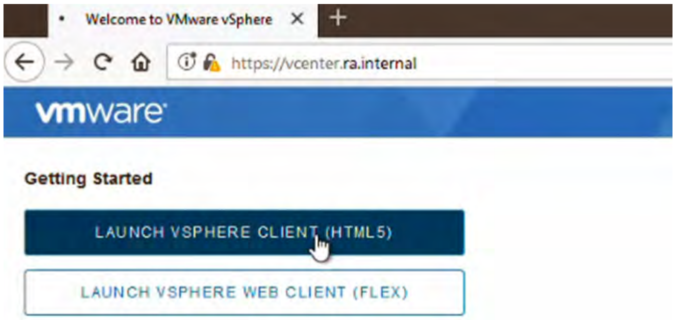
The restart process typically takes 10…15 minutes.

Migrate the Kernel Back to vdSwitch0

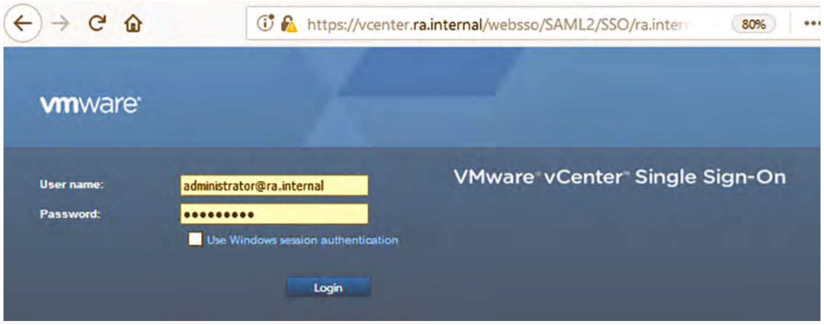
IMPORTANT To complete the following steps, vcenter.ra.internal must be resolvable to the current IP address of the VMware vCenter Server® at each step of the process. The easiest way to do so is to modify the hosts file, which is explained in Modify the Hosts File on page 66.

1. Access the following VMware® website: https://vcenter.ra.internal.

2. Under Getting Started, click Launch vSphere Client (HTML5).


Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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

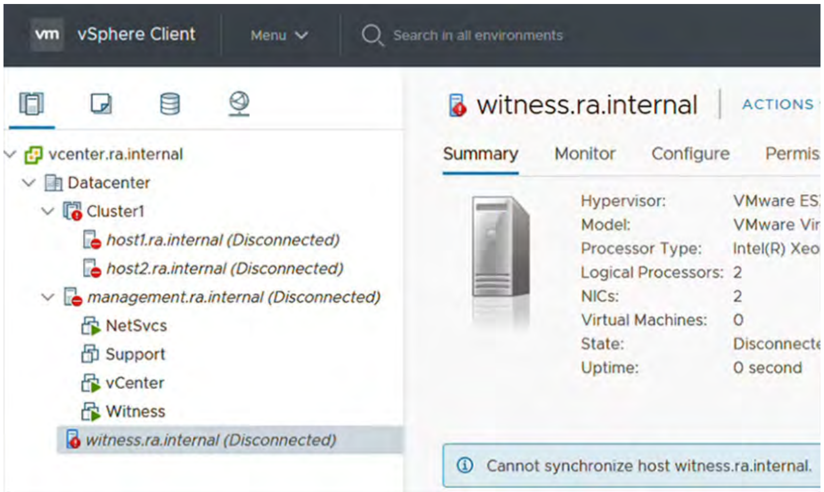

https://vcenter.ra.internal/websso/SAML2/SSO/ra.inter
80%
vmware
VMware vCenter Single Sign-On
Login

User name: administrator@ra.internal

Password: •••••••••

□ Use Windows session authentication

You will notice that the hosts have become disconnected.


vm vSphere Client
Menu
Search in all environments
vcenter.ra.internal
Datacenter
Cluster1
host1.ra.internal (Disconnected)
host2.ra.internal (Disconnected)
management.ra.internal (Disconnected)
NetSvcs
Support
vCenter
Witness
witness.ra.internal (Disconnected)
witness.ra.internal
ACTIONS
Summary
Monitor
Configure
Permis

Hypervisor: VMware ES

Model: VMware Vir

Processor Type: Intel(R) Xeo

Logical Processors: 2

NICs: 2

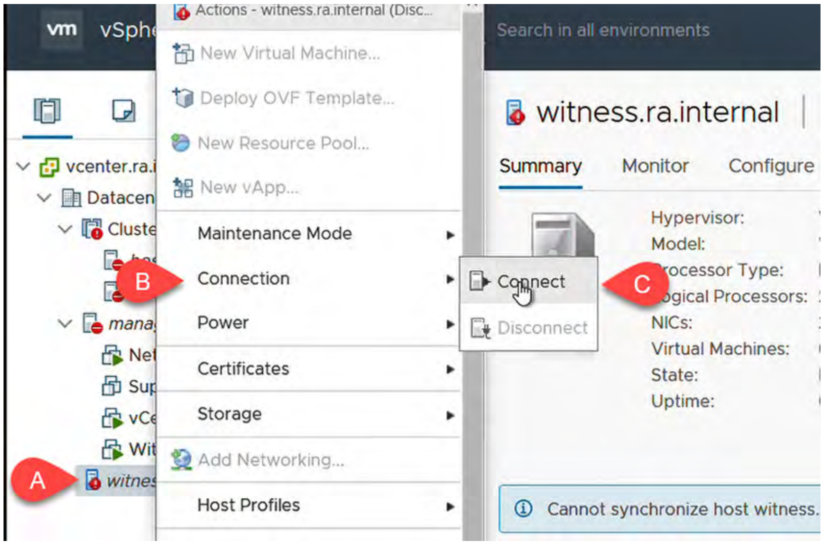
Virtual Machines: 0

State: Disconnecte

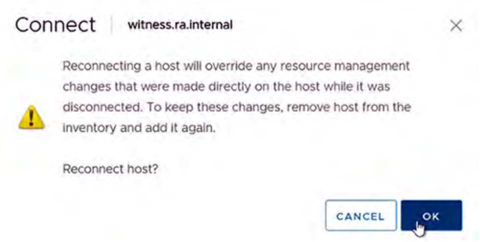
Uptime: 0 second

ⓘ Cannot synchronize host witness.ra.internal.

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



5. A connection alert box appears. Click OK.

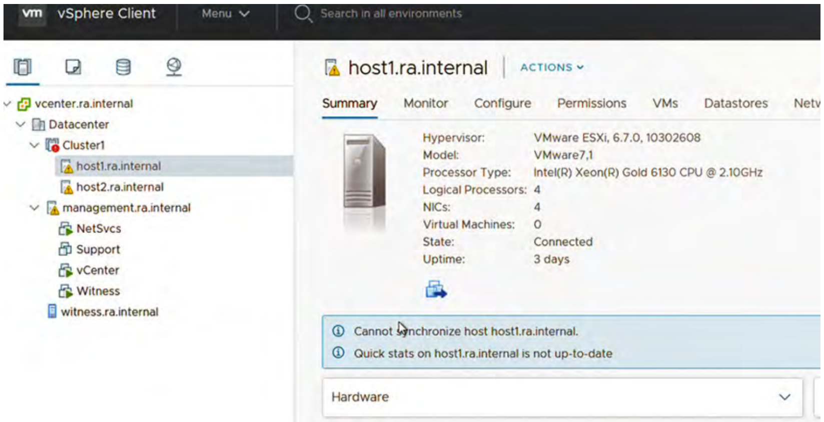


Connect | witness.ra.internal

Reconnecting a host will override any resource management changes that were made directly on the host while it was disconnected. To keep these changes, remove host from the inventory and add it again.

Reconnect host?

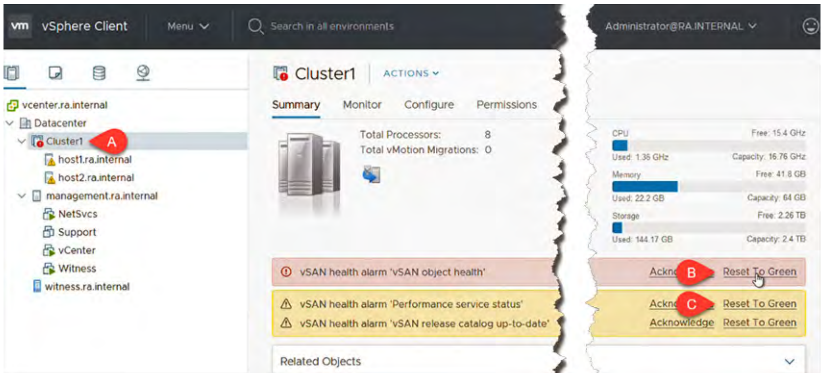
6. Please repeat the connection process for the Management host and hosts 1 and 2 until all hosts are properly connected.



Hypervisor: VMware ESXi, 6.7.0, 10302608
Model: VMware7,1
Processor Type: Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
Logical Processors: 4
NICs: 4
Virtual Machines: 0
State: Connected
Uptime: 3 days

Cannot synchronize host host1.ra.internal.
Quick stats on host1.ra.internal is not up-to-date

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



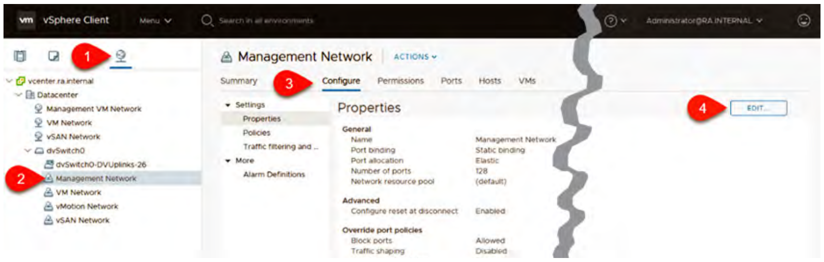
Total Processors: 8
Total vMotion Migrations: 0

CPU Free: 15.4 GHz
Used: 1.36 GHz Capacity: 16.76 GHz
Memory Free: 41.8 GB
Used: 22.2 GB Capacity: 64 GB
Storage Free: 2.26 TB
Used: 144.17 GB Capacity: 2.4 TB

vSAN health alarm 'vSAN object health'
vSAN health alarm 'Performance service status'
vSAN health alarm 'vSAN release catalog up-to-date'

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

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



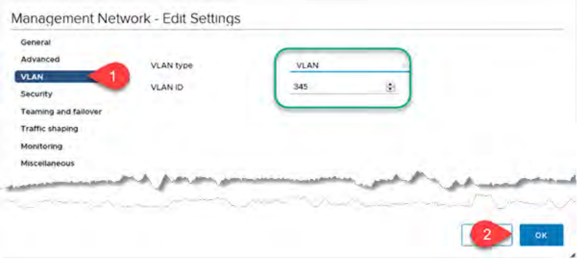
Properties

General
Name Management Network
Port binding Static binding
Port allocation Elastic
Number of ports 128
Network resource pool (default)

Advanced
Configure reset at disconnect Enabled

Override port policies
Block ports Allowed
Traffic shaping Disabled

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



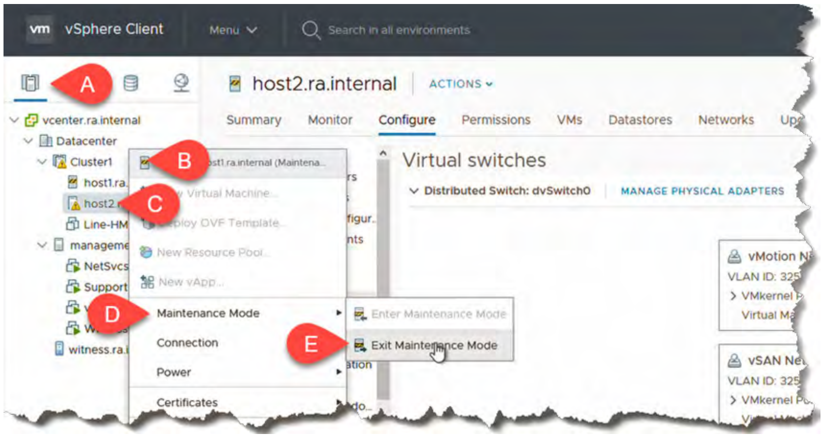
VLAN type: VLAN

VLAN ID: 345

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

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

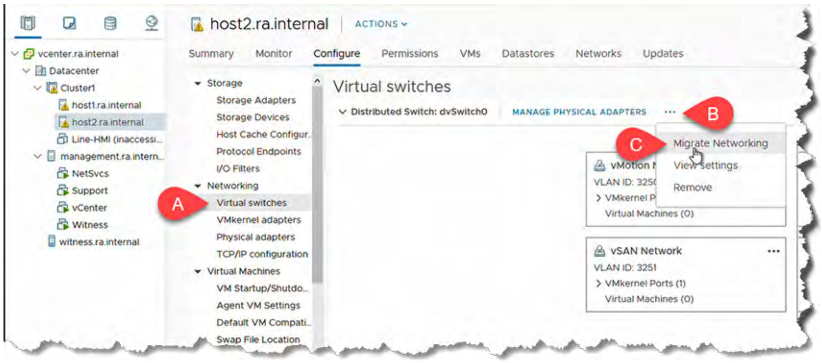
Right-click on host2 (C) > Maintenance Mode (D) > Exit Maintenance Mode (E).



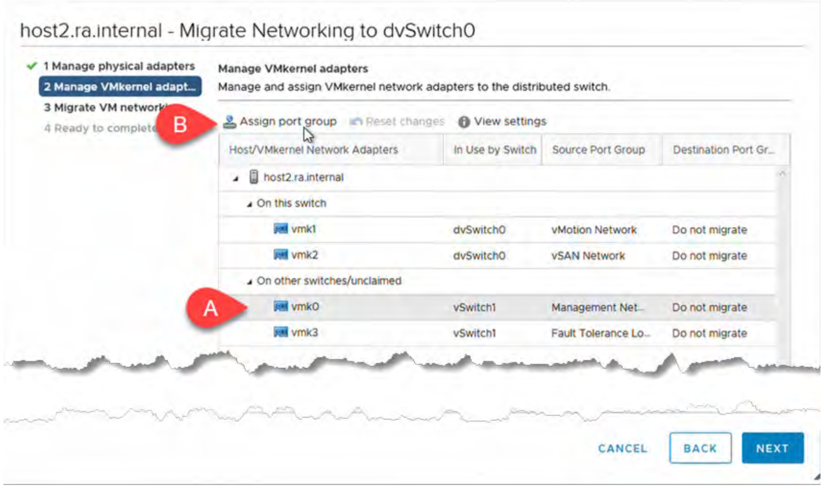
12. Repeat step for host1.

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

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



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



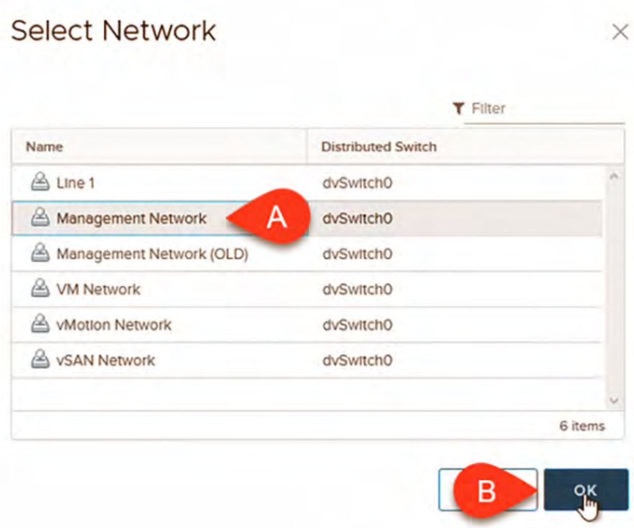
host2.ra.internal - Migrate Networking to dvSwitch0

Manage VMkernel adapters

Manage and assign VMkernel network adapters to the distributed switch.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Gr...
host2.ra.internal			
On this switch			
vmk1	dvSwitch0	vMotion Network	Do not migrate
vmk2	dvSwitch0	vSAN Network	Do not migrate
On other switches/unclaimed			
vmk0	vSwitch1	Management Net...	Do not migrate
vmk3	vSwitch1	Fault Tolerance Lo...	Do not migrate

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

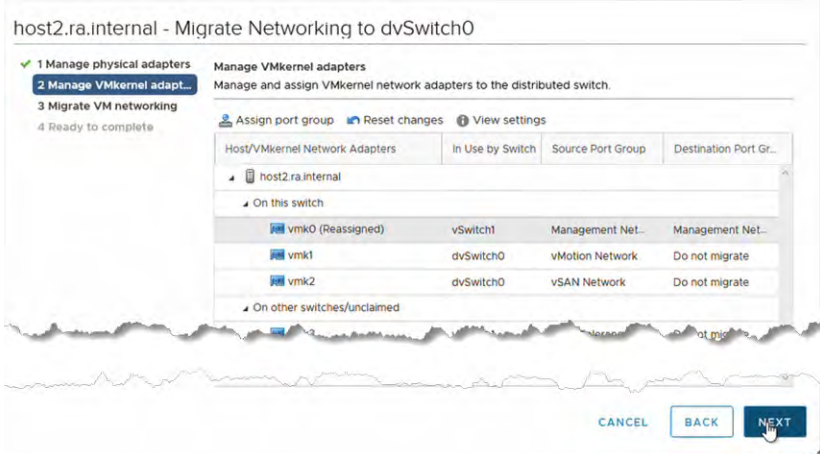


Select Network

Name	Distributed Switch
Line 1	dvSwitch0
Management Network	dvSwitch0
Management Network (OLD)	dvSwitch0
VM Network	dvSwitch0
vMotion Network	dvSwitch0
vSAN Network	dvSwitch0

6 items

16. Click Next.



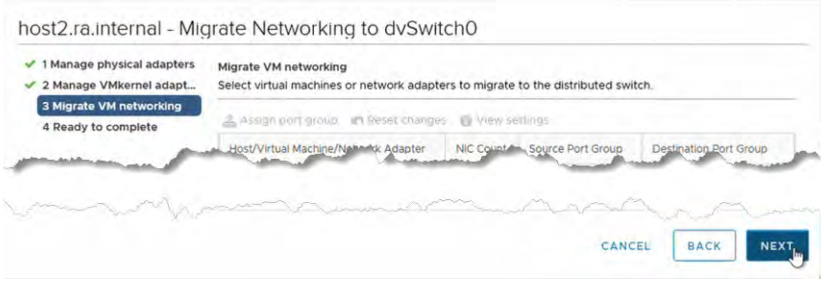
host2.ra.internal - Migrate Networking to dvSwitch0

Manage VMkernel adapters

Manage and assign VMkernel network adapters to the distributed switch.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Gr...
host2.ra.internal			
On this switch			
vmk0 (Reassigned)	vSwitch1	Management Net...	Management Net...
vmk1	dvSwitch0	vMotion Network	Do not migrate
vmk2	dvSwitch0	vSAN Network	Do not migrate
On other switches/unclaimed			

17. On step 3, click Next.

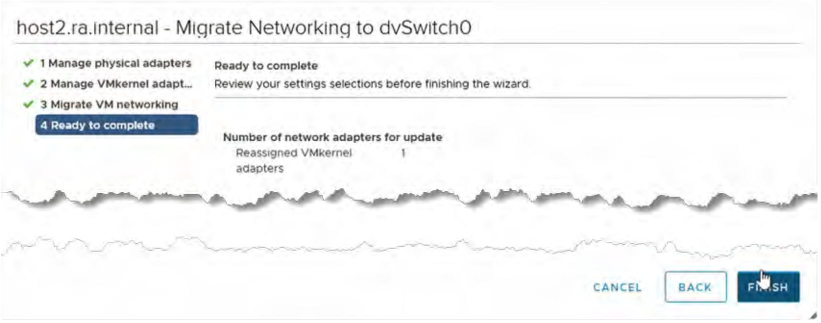


host2.ra.internal - Migrate Networking to dvSwitch0

Migrate VM networking

Select virtual machines or network adapters to migrate to the distributed switch.

18. On step 4, click Finish.



host2.ra.internal - Migrate Networking to dvSwitch0

Ready to complete

Review your settings selections before finishing the wizard.

Number of network adapters for update

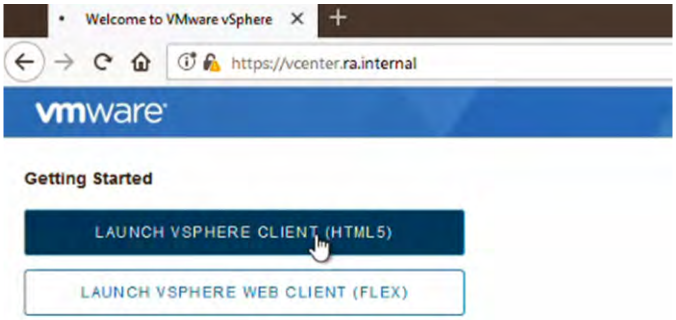
Reassigned VMkernel adapters	1

✓ 1 Manage physical adapters
✓ 2 Manage VMkernel adapt...
✓ 3 Migrate VM networking
4 Ready to complete
CANCEL
BACK
FINISH

19. Repeat step 13...step 18 to migrate the kernel on host1.

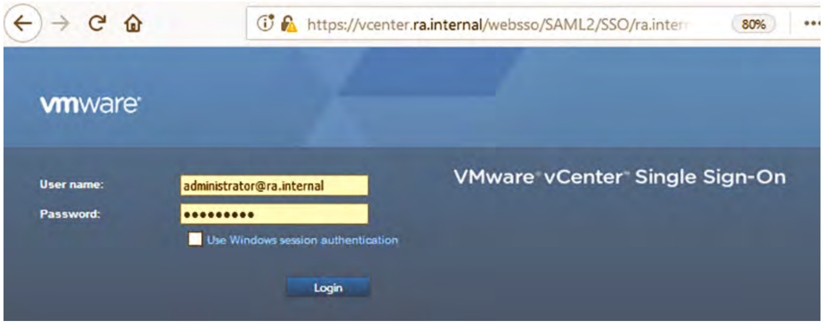
Change the Host Address (HA) Isolation Addresses

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



Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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

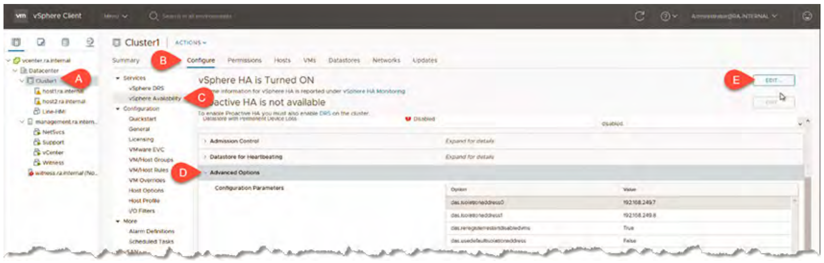


User name: administrator@ra.internal

Password: •••••••••

https://vcenter.ra.internal/websso/SAML2/SSO/ra.inter
80%
vmware
VMware vCenter Single Sign-On
□ Use Windows session authentication
Login

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



vSphere HA is Turned ON

Proactive HA is not available

Admission Control — Expand for details

Datastore for Heartbeating — Expand for details

Advanced Options

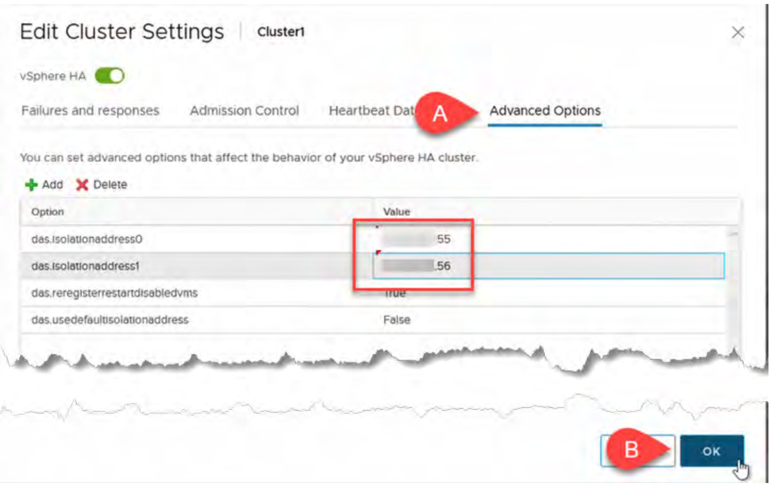
Configuration Parameters

Option	Value
das.isolationaddress0	192.168.249.7
das.isolationaddress1	192.168.249.8
das.reregisterrestartdisabledvms	True
das.usedefaultisolationaddress	False

5. Go to the Advanced Options tab (A).

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

Click OK (B).

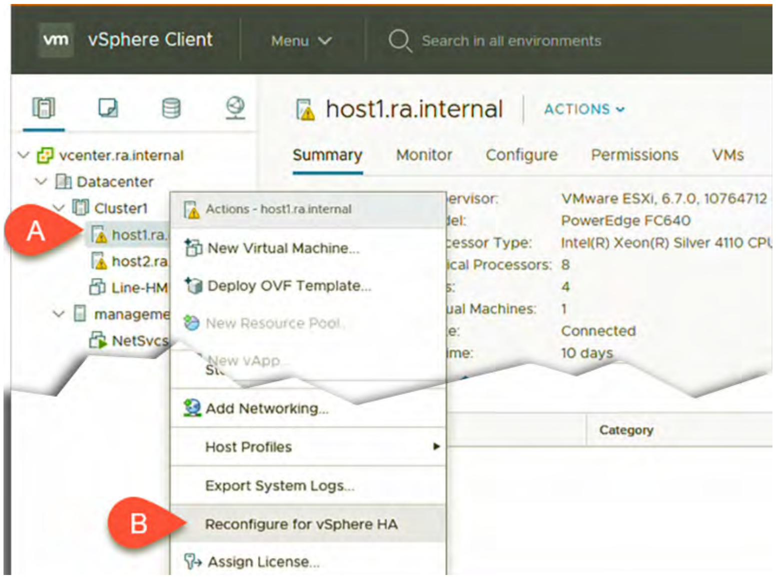


You can set advanced options that affect the behavior of your vSphere HA cluster.

Option	Value
das.isolationaddress0	[redacted].55
das.isolationaddress1	[redacted].56
das.reregisterrestartdisabledvms	True
das.usedefaultisolationaddress	False

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

After a moment, the warning clears.

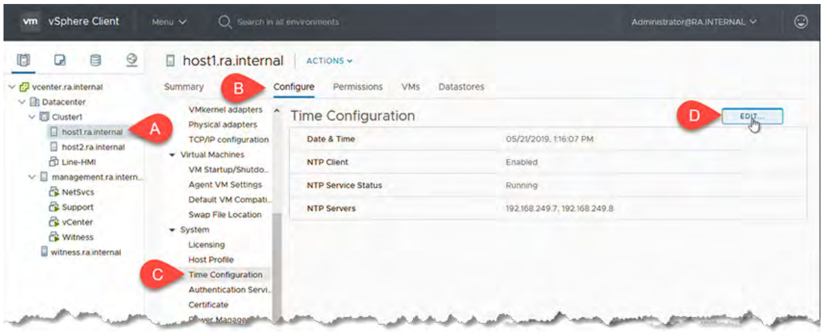


ervisor: VMware ESXi, 6.7.0, 10764712
del: PowerEdge FC640
cessor Type: Intel(R) Xeon(R) Silver 4110 CPU
ical Processors: 8
s: 4
ual Machines: 1
e: Connected
me: 10 days

7. 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).

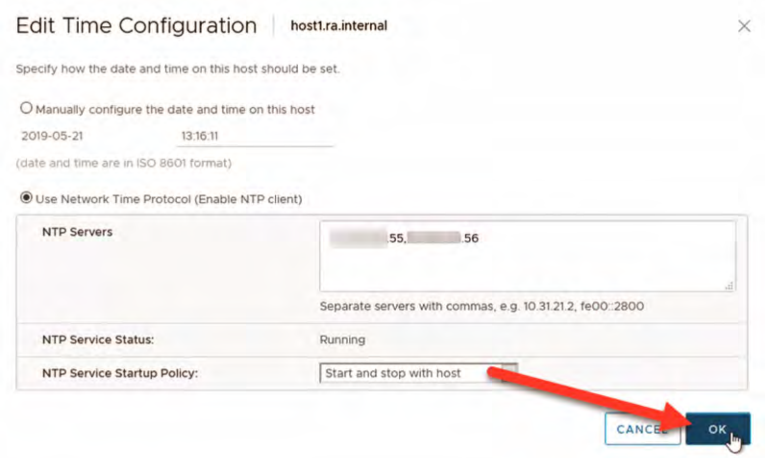


Time Configuration

Date & Time	05/21/2019, 1:16:07 PM
NTP Client	Enabled
NTP Service Status	Running
NTP Servers	192.168.249.7, 192.168.249.8

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

   Click OK.



Edit Time Configuration | host1.ra.internal

Specify how the date and time on this host should be set.

○ Manually configure the date and time on this host

2019-05-21 13:16:11

(date and time are in ISO 8601 format)

● Use Network Time Protocol (Enable NTP client)

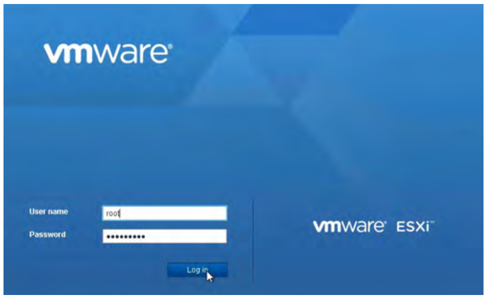
NTP Servers	[redacted].55,[redacted].56 Separate servers with commas, e.g. 10.31.21.2, fe00::2800
NTP Service Status:	Running
NTP Service Startup Policy:	Start and stop with host

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.

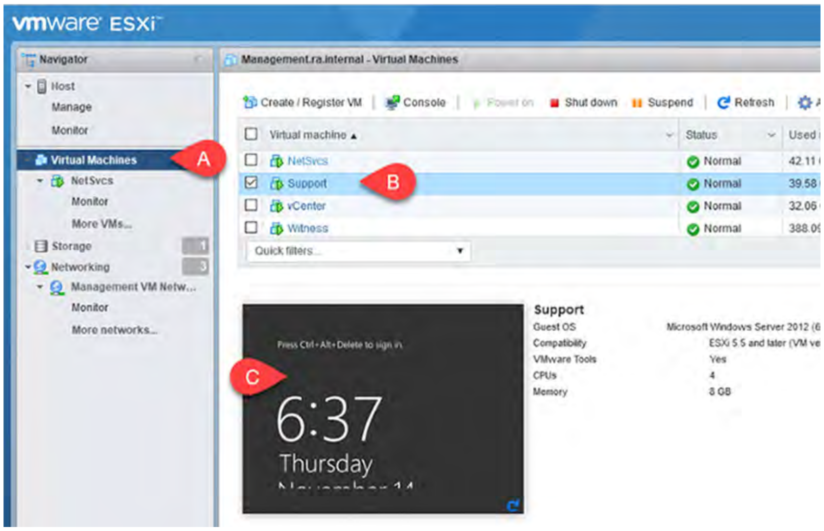


User name: root

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.

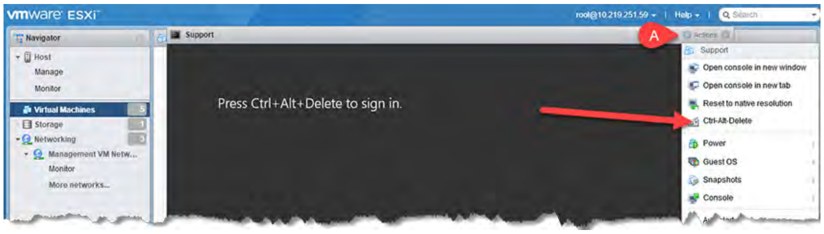


	Virtual machine ▲	Status	Used
□	NetSvcs	Normal	42.11
☑	Support	Normal	39.58
□	vCenter	Normal	32.06
□	Witness	Normal	388.0

Support

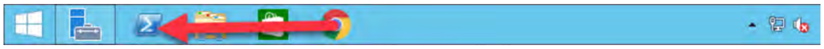
Guest OS	Microsoft Windows Server 2012 (6
Compatibility	ESXi 5.5 and later (VM ve
VMware Tools	Yes
CPUs	4
Memory	8 GB

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



Press Ctrl+Alt+Delete to sign in.

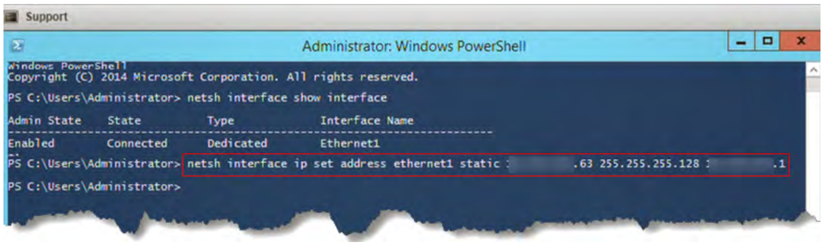
5. Launch the Microsoft® PowerShell application from the task bar.



6. 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.



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> netsh interface show interface

Admin State    State          Type             Interface Name
-------------------------------------------------------------------------
Enabled        Connected      Dedicated        Ethernet1

PS C:\Users\Administrator> netsh interface ip set address ethernet1 static [redacted].63 255.255.255.128 [redacted].1

PS C:\Users\Administrator>
```

7. Set the DNS server by typing the following command:

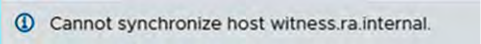
```
Netsh interface ip set dnsservers ethernet1 static x.x.x.x
```

   Where x is the IP address of the NetSvcs VM.

8. Sign out of the Support VM.

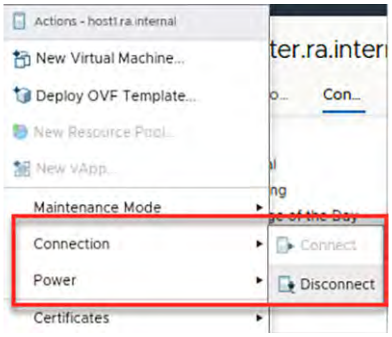
Disconnect Hosts

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

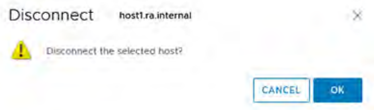


Cannot synchronize host witness.ra.internal.

1. Right click host1. Go to Connection > Disconnect.



2. To disconnect the host, click OK.

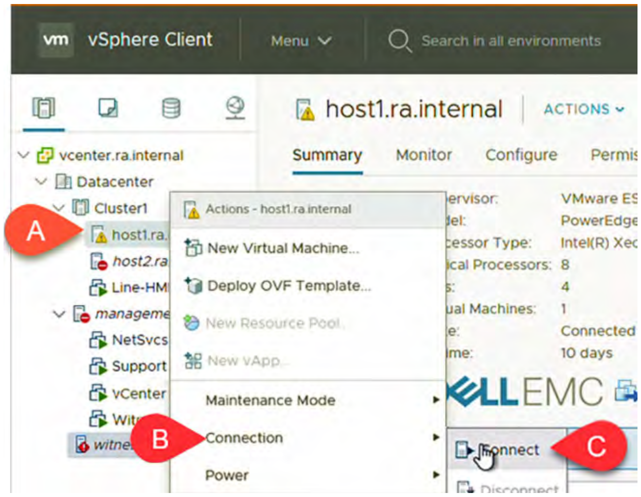


Disconnect host1.ra.internal

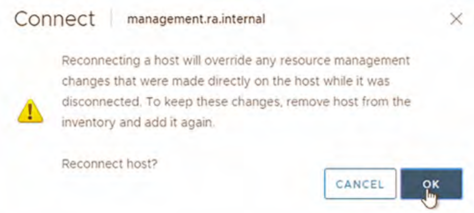
Disconnect the selected host?

3. 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.



Connect | management.ra.internal

Reconnecting a host will override any resource management changes that were made directly on the host while it was disconnected. To keep these changes, remove host from the inventory and add it again.

Reconnect host?

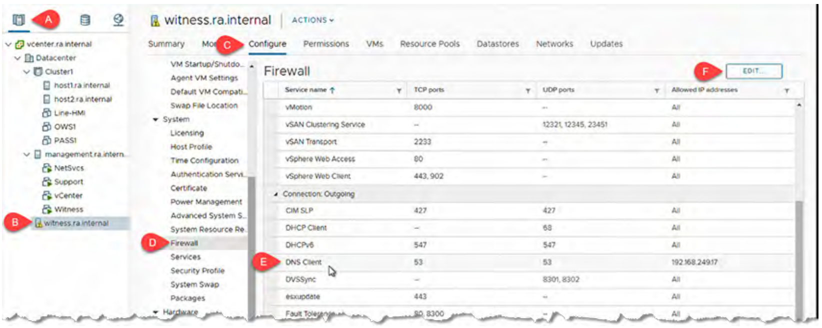
6. Repeat step 4 and step 5 for all four hosts.

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).



witness.ra.internal

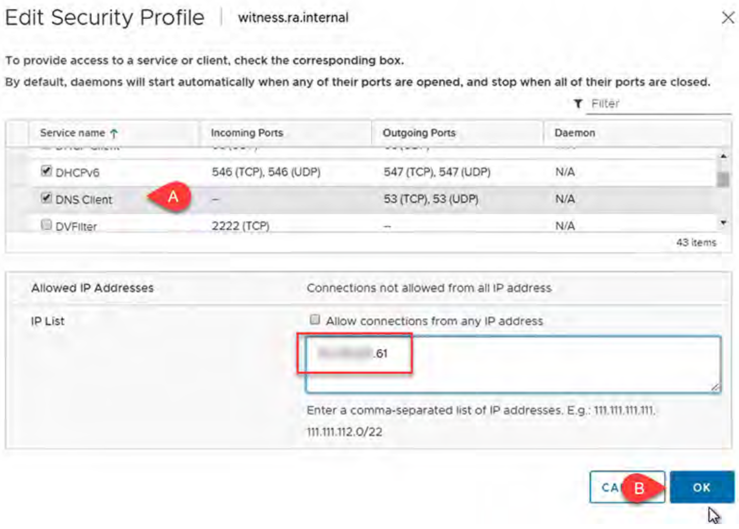
Firewall

Service name	TCP ports	UDP ports	Allowed IP addresses
vMotion	8000	--	All
vSAN Clustering Service	--	12321, 12345, 23451	All
vSAN Transport	2233	--	All
vSphere Web Access	80	--	All
vSphere Web Client	443, 902	--	All
Connection: Outgoing			
CIM SLP	427	427	All
DHCP Client	--	68	All
DHCPv6	547	547	All
DNS Client	53	53	192.168.249.17
DVSSync	--	8301, 8302	All
esxupdate	443	--	All
Fault Tolerance	80, 8300	--	All

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).



Edit Security Profile | witness.ra.internal

To provide access to a service or client, check the corresponding box.

By default, daemons will start automatically when any of their ports are opened, and stop when all of their ports are closed.

	Service name	Incoming Ports	Outgoing Ports	Daemon
☑	DHCPV6	546 (TCP), 546 (UDP)	547 (TCP), 547 (UDP)	N/A
☑	DNS Client	--	53 (TCP), 53 (UDP)	N/A
□	DVFilter	2222 (TCP)	--	N/A

43 items

Allowed IP Addresses — Connections not allowed from all IP address

IP List — □ Allow connections from any IP address

[redacted].61

Enter a comma-separated list of IP addresses. E.g.: 111.111.111.111, 111.111.112.0/22

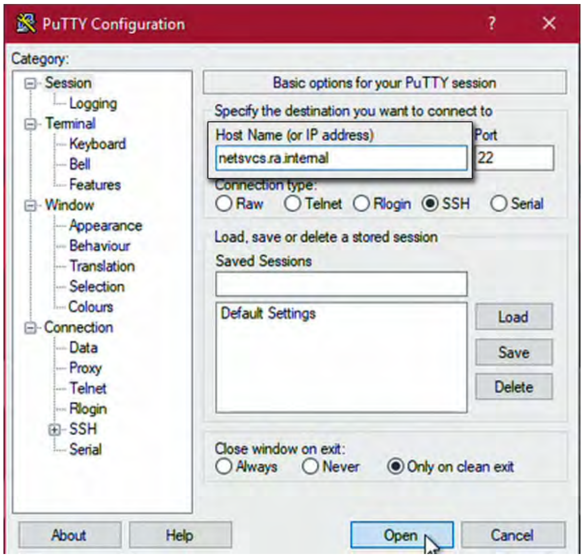
3. Repeat steps 1 and 2 for the other three hosts.

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.

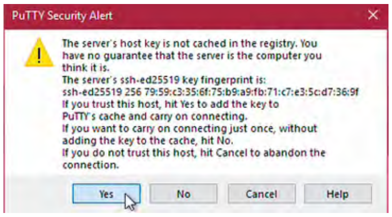
1. Open the application on your personal computer.
2. On the PuTTY configuration screen, add netsvcs.ra.internal as the host name.



Host Name (or IP address): netsvcs.ra.internal
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

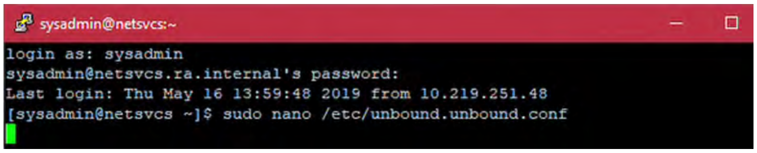
3. Click Open.

   A security alert appears.



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 256 79:59:c3:35:6f:75:b9:a9:fb:71:c7:e3:5c:d7:36:9f
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

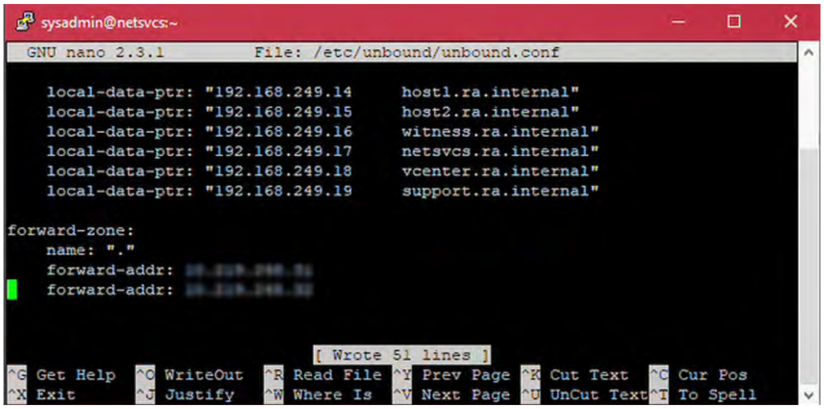
4. Click Yes.
5. On the PuTTY log in screen, type the following.
   - For login: sysadmin [Enter]
   - For password: <system specific password> [Enter]
   - For the $ prompt: sudo nano/etc/unbound/unbound.conf [Enter]



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

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.



```
  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     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: [redacted]
    forward-addr: [redacted]

                                [ Wrote 51 lines ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

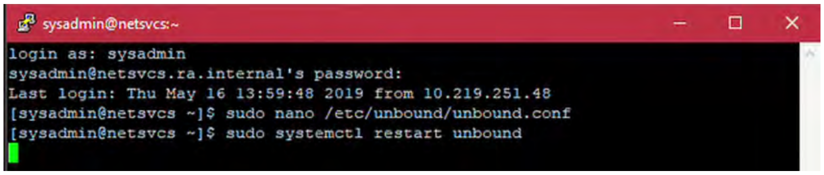
TIP If there are additional DNS servers on the network, additional 'forward-addr:' lines can be added.

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.

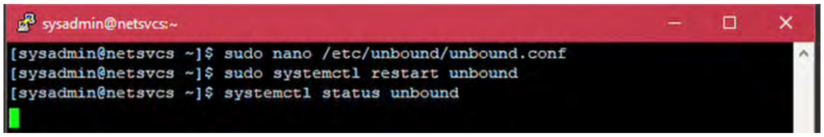
10. At the $ prompt, type sudo systemctl restart unbound [Enter].



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

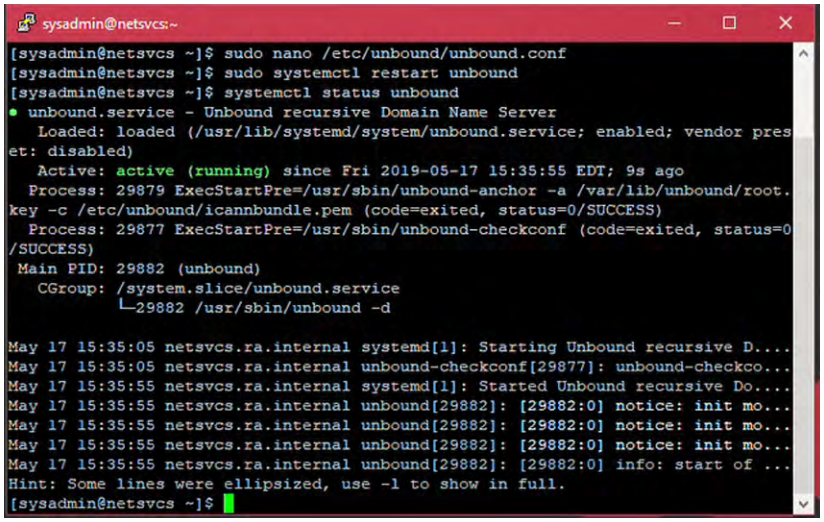
   The command restarts the system.

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



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

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



```
[sysadmin@netsvcs ~]$ sudo nano /etc/unbound/unbound.conf
[sysadmin@netsvcs ~]$ sudo systemctl restart unbound
[sysadmin@netsvcs ~]$ systemctl status unbound
● unbound.service - Unbound recursive Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled; vendor pres
et: 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 netsvcs.ra.internal systemd[1]: Starting Unbound recursive D....
May 17 15:35:05 netsvcs.ra.internal unbound-checkconf[29877]: unbound-checkco...
May 17 15:35:55 netsvcs.ra.internal systemd[1]: Started Unbound recursive Do....
May 17 15:35:55 netsvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...
May 17 15:35:55 netsvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...
May 17 15:35:55 netsvcs.ra.internal unbound[29882]: [29882:0] notice: init mo...
May 17 15:35:55 netsvcs.ra.internal unbound[29882]: [29882:0] info: start of ...
Hint: Some lines were ellipsized, use -l to show in full.
[sysadmin@netsvcs ~]$
```

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

Manage the System

Domain Name System (DNS) Requirements

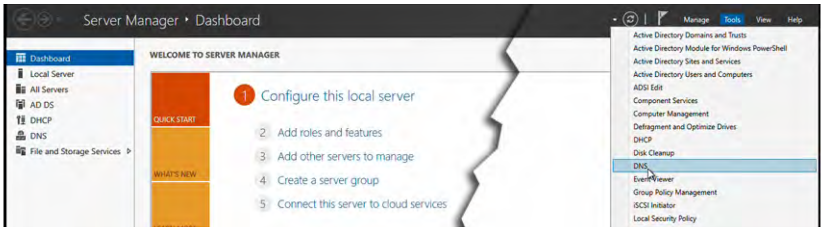
Proper DNS configuration affects access to the VMware vSphere® web client in VersaVirtual, or how you integrate the system with an existing or new Active Directory environment. To access the VMware vSphere web client, one of the following must be completed.

- 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.

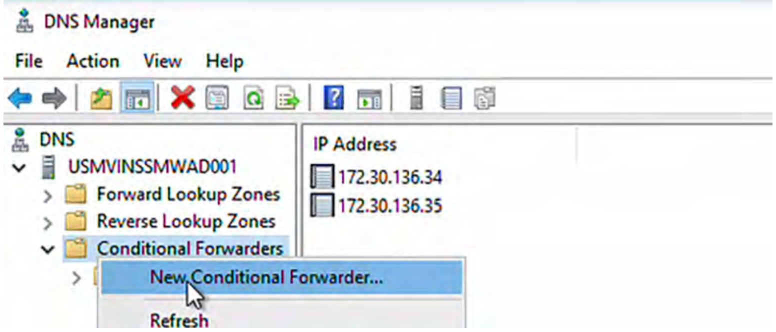
Forward DNS Requests

To add DNS conditional forwarders, perform the following steps.

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

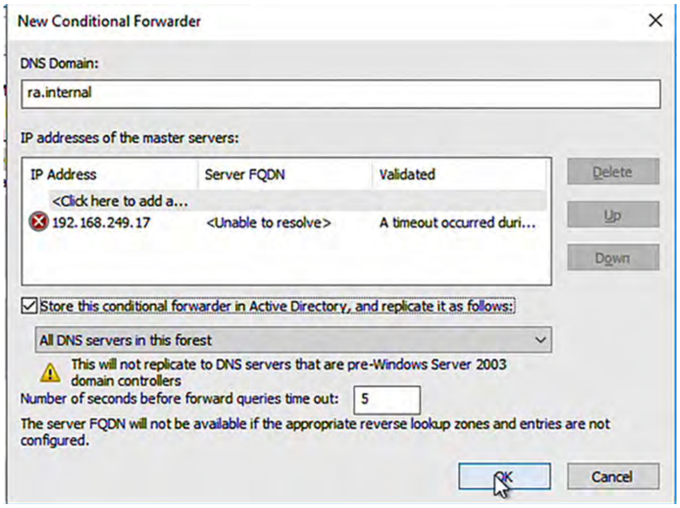

Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy

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.


New Conditional Forwarder

DNS Domain:

ra.internal

IP addresses of the master servers:

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

☑ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

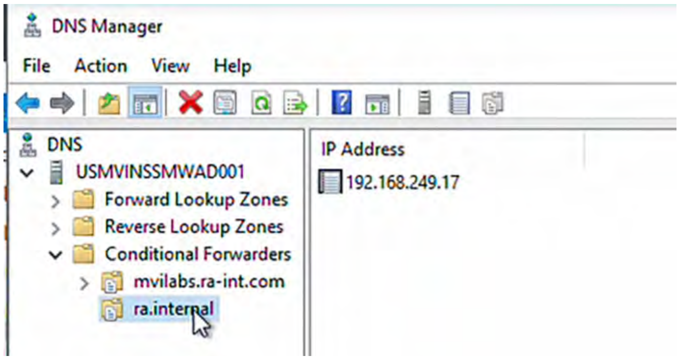
⚠ This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers

Number of seconds before forward queries time out: 5

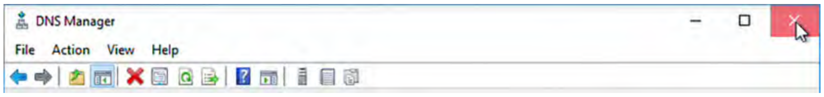
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

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.

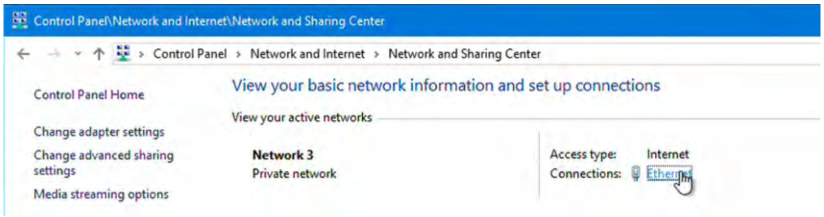


Ra.internal has been added as a DNS conditional forwarder.

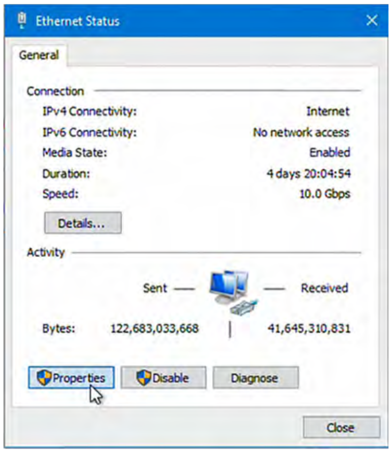
Configure the Management Computer

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.


Control Panel\Network and Internet\Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options
View your basic network information and set up connections
View your active networks
Network 3
Private network
Access type: Internet
Connections: Ethernet

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



Ethernet Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

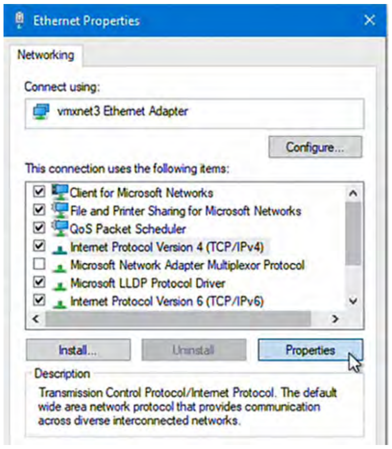
Duration: 4 days 20:04:54

Speed: 10.0 Gbps

Activity

Bytes: Sent 122,683,033,668 | Received 41,645,310,831

5. On the Networking tab, click Properties.



Ethernet Properties

Networking

Connect using:

vmxnet3 Ethernet Adapter

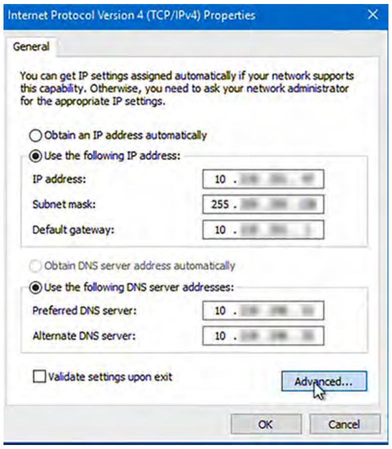
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

6. On the General tab, click Advanced.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . [redacted]

Subnet mask: 255 . [redacted]

Default gateway: 10 . [redacted]

○ Obtain DNS server address automatically

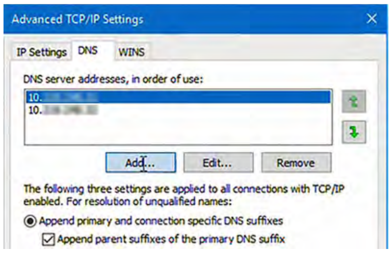
● Use the following DNS server addresses:

Preferred DNS server: 10 . [redacted]

Alternate DNS server: 10 . [redacted]

☐ Validate settings upon exit

7. On the DNS tab, click Add.



Advanced TCP/IP Settings

IP Settings | DNS | WINS

DNS server addresses, in order of use:

10.[redacted]
10.[redacted]

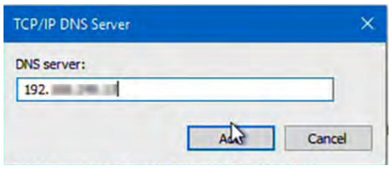
Add... | Edit... | Remove

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

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



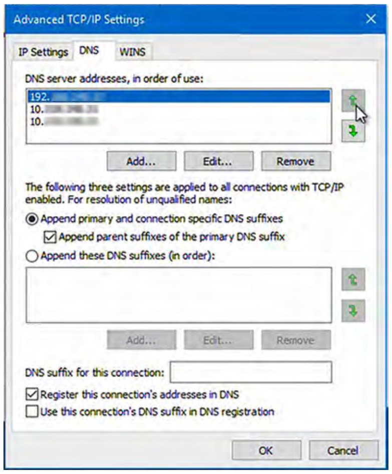
TCP/IP DNS Server

DNS server: 192.[redacted]

Add | Cancel

9. 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.



Advanced TCP/IP Settings

IP Settings | DNS | WINS

DNS server addresses, in order of use:

192.[redacted]
10.[redacted]
10.[redacted]

Add... | Edit... | Remove

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

Add... | Edit... | Remove

DNS suffix for this connection:

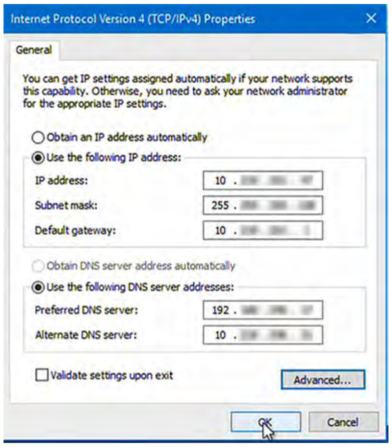
☑ Register this connection's addresses in DNS

□ Use this connection's DNS suffix in DNS registration

OK | Cancel

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

Click OK.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 .[redacted]

Subnet mask: 255 .[redacted]

Default gateway: 10 .[redacted]

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 .[redacted]

Alternate DNS server: 10 .[redacted]

□ Validate settings upon exit

Advanced...

OK | Cancel

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.

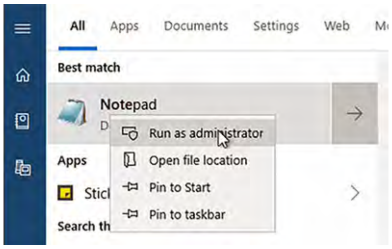
Modify the Hosts File

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.

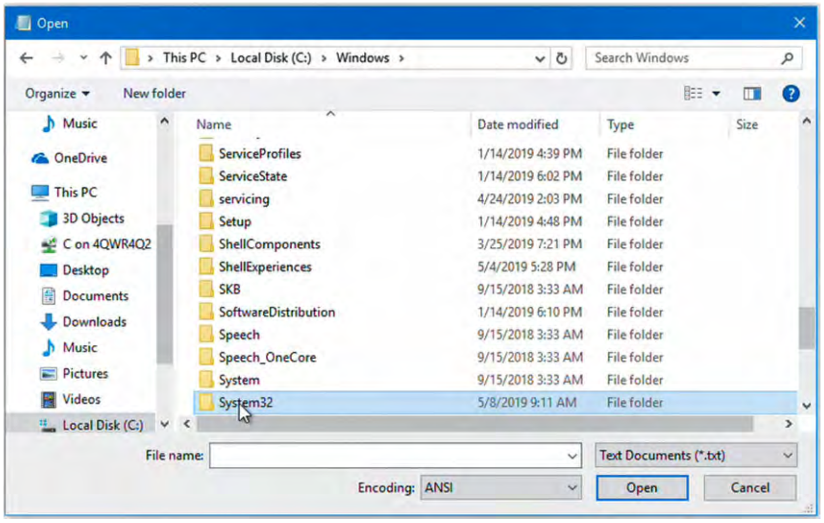
```
192.168.249.7   nm1.ra.internal             nm1             #FN410T  Network I/O Module
192.168.249.8   nm2.ra.internal             nm2             #FN410T  Network I/O Module
192.168.249.9   cmc.ra.internal             cmc             #FX2     Chassis Management Controller
192.168.249.10  management-bmc.ra.internal  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.



Name	Date modified	Type	Size
ServiceProfiles	1/14/2019 4:39 PM	File folder	
ServiceState	1/14/2019 6:02 PM	File folder	
servicing	4/24/2019 2:03 PM	File folder	
Setup	1/14/2019 4:48 PM	File folder	
ShellComponents	3/25/2019 7:21 PM	File folder	
ShellExperiences	5/4/2019 5:28 PM	File folder	
SKB	9/15/2018 3:33 AM	File folder	
SoftwareDistribution	1/14/2019 6:10 PM	File folder	
Speech	9/15/2018 3:33 AM	File folder	
Speech_OneCore	9/15/2018 3:33 AM	File folder	
System	9/15/2018 3:33 AM	File folder	
System32	5/8/2019 9:11 AM	File folder	

File name:

Text Documents (*.txt)

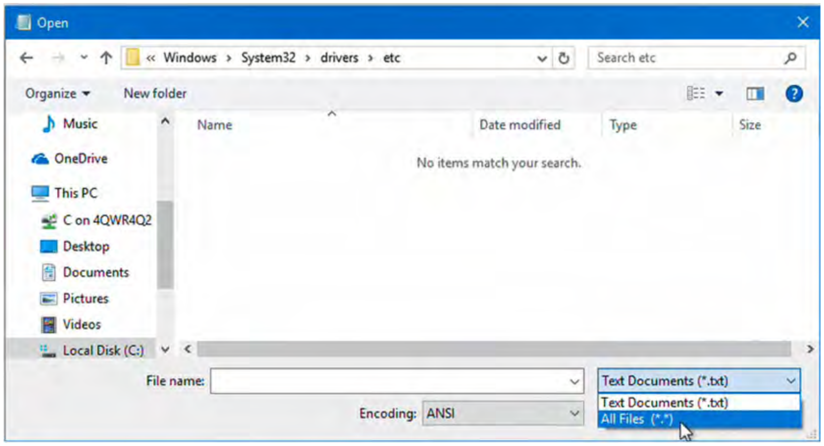
Encoding: ANSI

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.



No items match your search.

File name:

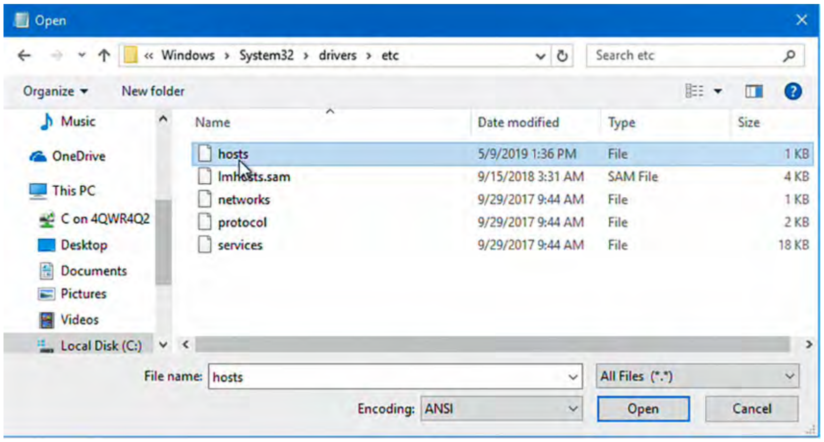
Text Documents (*.txt)

Text Documents (*.txt)

All Files (*.*)

Encoding: ANSI

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



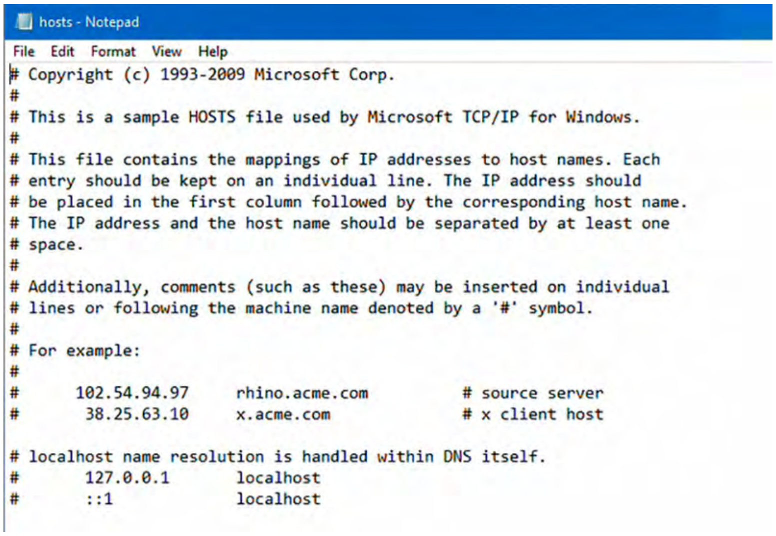
Name	Date modified	Type	Size
hosts	5/9/2019 1:36 PM	File	1 KB
lmhosts.sam	9/15/2018 3:31 AM	SAM File	4 KB
networks	9/29/2017 9:44 AM	File	1 KB
protocol	9/29/2017 9:44 AM	File	2 KB
services	9/29/2017 9:44 AM	File	18 KB

File name: hosts

All Files (*.*)

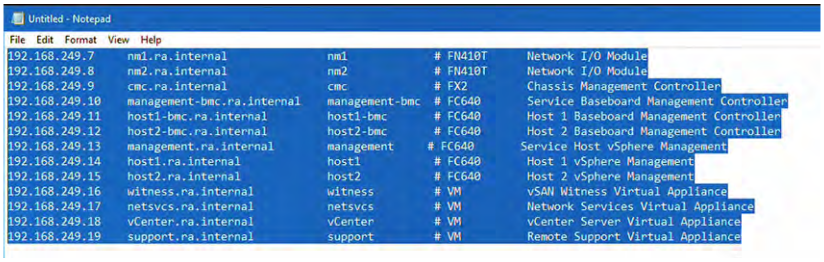
Encoding: ANSI

The hosts file opens in the Notepad application.



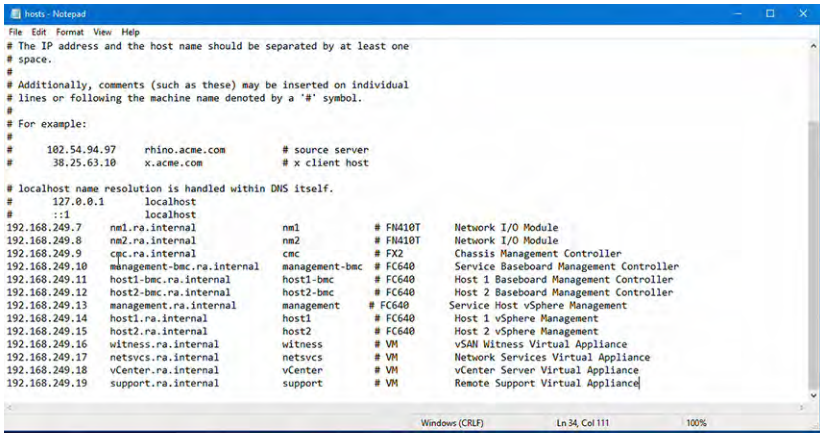
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the 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).



```
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
```

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



```
# 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             # 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
```

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.

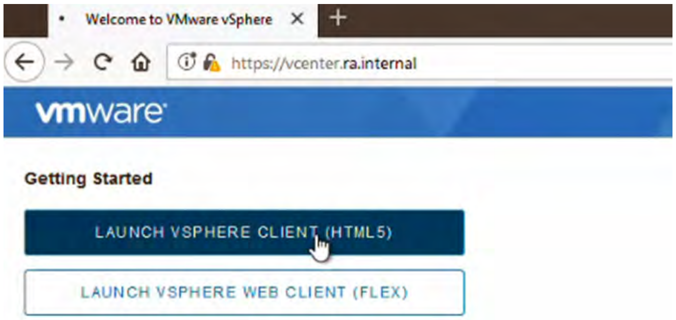
To install licenses after 90 days, search for instructions on the Rockwell Automation Knowledgebase site at https://www.rockwellautomation.com/en_NA/support/overview.page. Use VersaVirtual as your search criteria.

The following licenses are supplied.

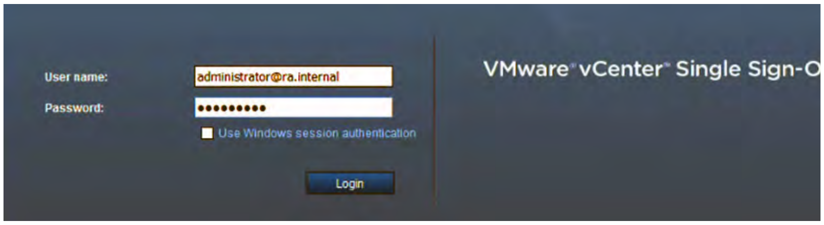
Application	Cat. Nos. 9300-VV1000EC, 9300-VV1000EN, 9300-VV1000RC, 9300-VV1000RN	Cat. Nos. 9300-VV2000EC, 9300-VV2000EN, 9300-VV2000RC, 9300-VV2000RN
VMware vCenter Server® Foundation	√	√
VMware vSphere® Standard	√	√
VMware vSAN™ Standard		√

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).


Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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

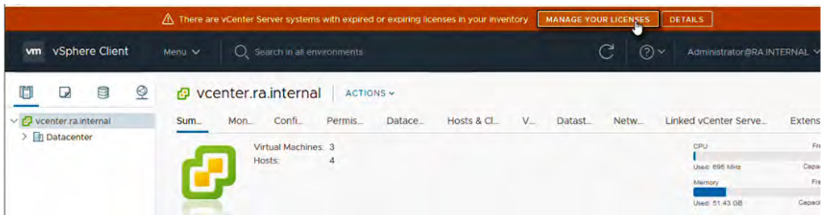

VMware vCenter Single Sign-O
User name:
Password:
Use Windows session authentication
Login

User name: administrator@ra.internal

Password: •••••••••

4. Click Login.

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

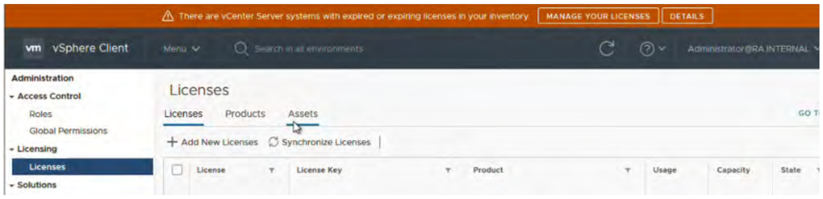


There are vCenter Server systems with expired or expiring licenses in your inventory

MANAGE YOUR LICENSES
DETAILS
vSphere Client
Menu
Search in all environments
Administrator@RA.INTERNAL
vcenter.ra.internal
ACTIONS
Datacenter
Sum... Mon... Confi... Permis... Datace... Hosts & Cl... V... Datast... Netw... Linked vCenter Serve... Extens

Virtual Machines: 3
Hosts: 4

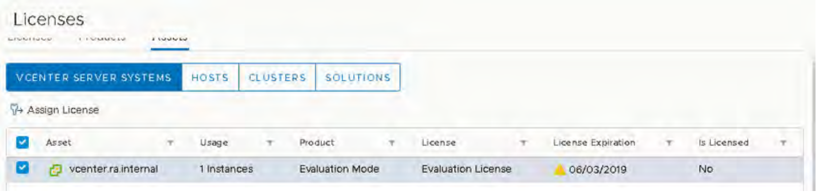
6. On Licenses, select the Assets tab.



There are vCenter Server systems with expired or expiring licenses in your inventory

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

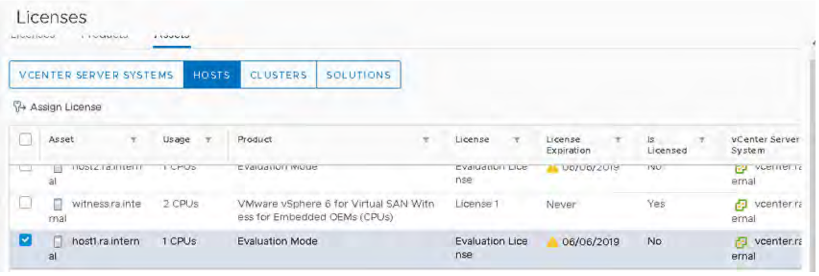
Verify that vcenter.ra.internal is checked and highlighted.



☑	Asset	Usage	Product	License	License Expiration	Is Licensed
☑	vcenter.ra.internal	1 Instances	Evaluation Mode	Evaluation License	⚠ 06/03/2019	No

8. Click Hosts.

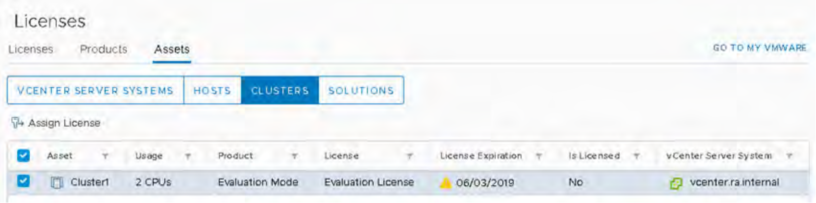
On Hosts, verify that host1.ra.internal is checked and highlighted.



□	Asset	Usage	Product	License	License Expiration	Is Licensed	vCenter Server System
□	host2.ra.internal	1 CPUs	Evaluation Mode	Evaluation License	⚠ 06/06/2019	No	vcenter.ra.internal
□	witness.ra.internal	2 CPUs	VMware vSphere 6 for Virtual SAN Witness for Embedded OEMs (CPUs)	License 1	Never	Yes	vcenter.ra.internal
☑	host1.ra.internal	1 CPUs	Evaluation Mode	Evaluation License	⚠ 06/06/2019	No	vcenter.ra.internal

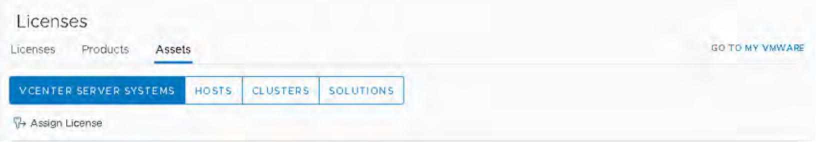
9. Click Clusters.

On Clusters, verify that Cluster1 is checked and highlighted.

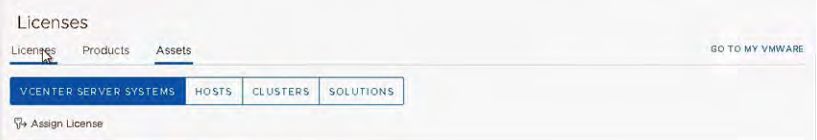


☑	Asset	Usage	Product	License	License Expiration	Is Licensed	vCenter Server System
☑	Cluster1	2 CPUs	Evaluation Mode	Evaluation License	⚠ 06/03/2019	No	vcenter.ra.internal

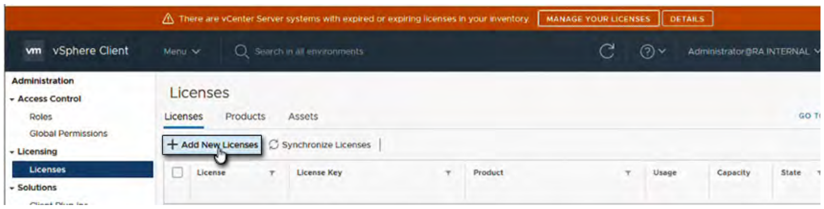
10. Click vCenter Server Systems.



11. On vCenter Server Systems, select the Licenses tab.

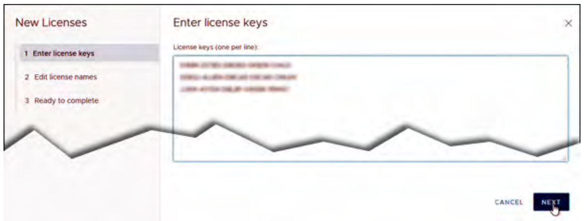


12. On Licenses, click Add New Licenses.



There are vCenter Server systems with expired or expiring licenses in your inventory

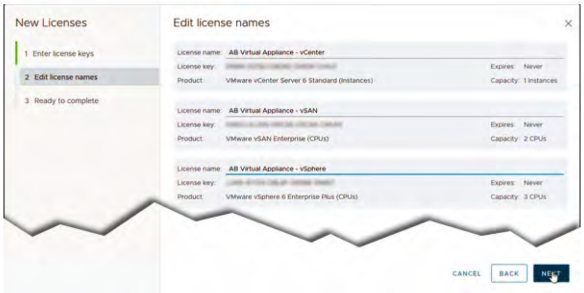
13. Enter the license keys that were supplied with your appliance purchase.



License keys (one per line):
[redacted]

After they are entered, click Next.

14. Rename each license key to a more suitable name.



License name: AB Virtual Appliance - vCenter
License key: [redacted] Expires: Never
Product: VMware vCenter Server 6 Standard (Instances) Capacity: 1 Instances

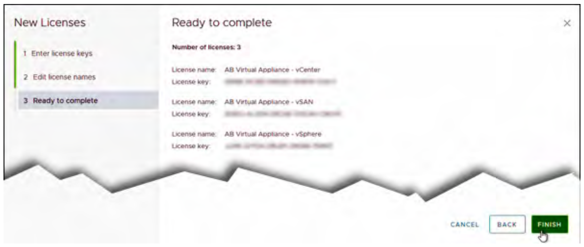
License name: AB Virtual Appliance - vSAN
License key: [redacted] Expires: Never
Product: VMware vSAN Enterprise (CPUs) Capacity: 2 CPUs

License name: AB Virtual Appliance - vSphere
License key: [redacted] Expires: Never
Product: VMware vSphere 6 Enterprise Plus (CPUs) Capacity: 3 CPUs

After you rename each key, click Next.

15. Verify that each license key has a suitable new name.

If any corrections are needed, then click Back and repeat step 14.



Number of licenses: 3

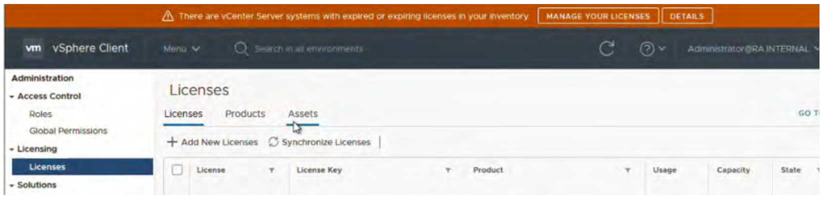
License name: AB Virtual Appliance - vCenter
License key: [redacted]

License name: AB Virtual Appliance - vSAN
License key: [redacted]

License name: AB Virtual Appliance - vSphere
License key: [redacted]

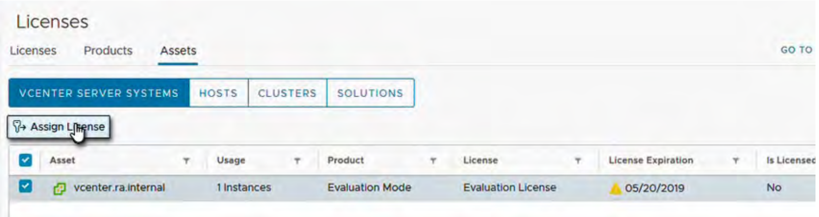
If the new license names are acceptable, then click Finish. You are returned to the Licenses page.

16. Select the Assets tab.



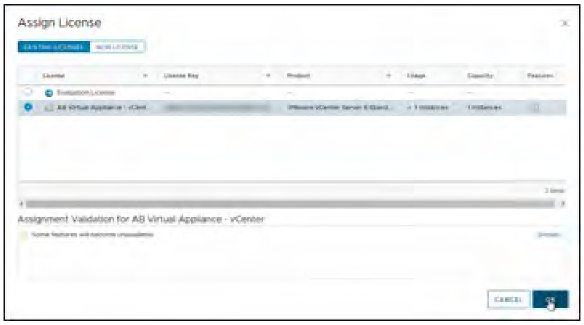
□	License	License Key	Product	Usage	Capacity	State

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



☑	Asset	Usage	Product	License	License Expiration	Is Licensed
☑	vcenter.ra.internal	1 Instances	Evaluation Mode	Evaluation License	⚠ 05/20/2019	No

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



Assignment Validation for AB Virtual Appliance - vCenter

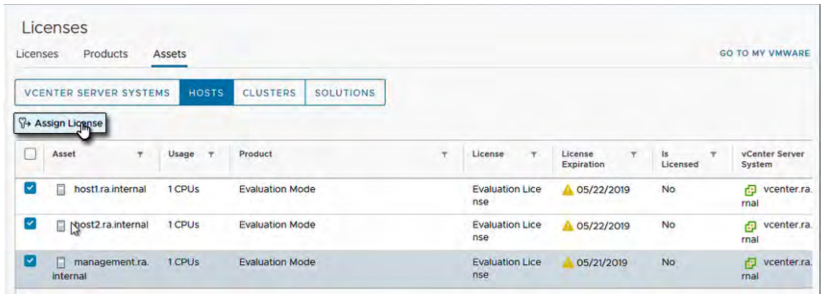
Click OK. You are returned to the Assets page.

19. Click Hosts.

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

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

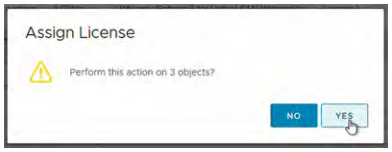
21. With the three assets selected, click Assign License.



□	Asset	Usage	Product	License	License Expiration	Is Licensed	vCenter Server System
☑	host1.ra.internal	1 CPUs	Evaluation Mode	Evaluation License	⚠ 05/22/2019	No	vcenter.ra.rnal
☑	host2.ra.internal	1 CPUs	Evaluation Mode	Evaluation License	⚠ 05/22/2019	No	vcenter.ra.rnal
☑	management.ra.internal	1 CPUs	Evaluation Mode	Evaluation License	⚠ 05/21/2019	No	vcenter.ra.rnal

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

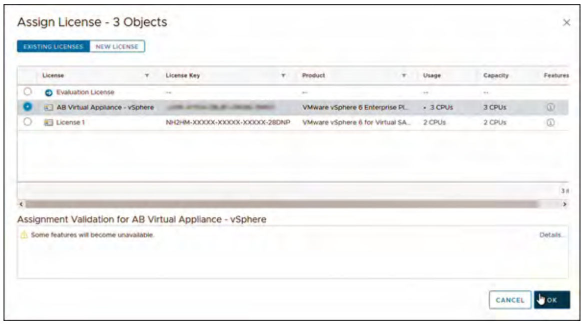
Click Yes.



Assign License

Perform this action on 3 objects?

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



Assign License - 3 Objects

	License	License Key	Product	Usage	Capacity	Features
○	Evaluation License	--	--	--	--	
●	AB Virtual Appliance - vSphere	[redacted]	VMware vSphere 6 Enterprise Pl...	• 3 CPUs	3 CPUs	ⓘ
○	License 1	NH2HM-XXXXX-XXXXX-XXXXX-28DNP	VMware vSphere 6 for Virtual SA...	2 CPUs	2 CPUs	ⓘ

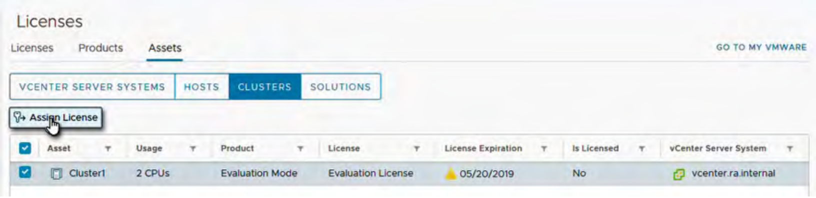
Assignment Validation for AB Virtual Appliance - vSphere

⚠ Some features will become unavailable.

Click OK. You are returned to the Hosts page.

24. Click Clusters.

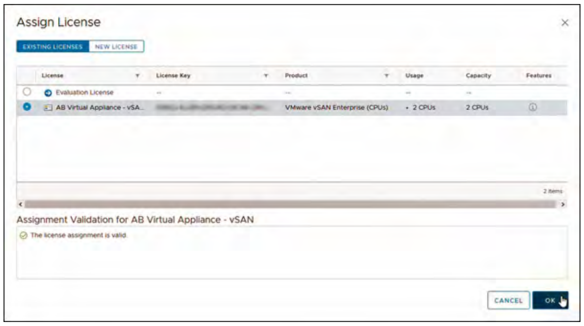
25. With the Cluster1 asset checked and highlighted, click Assign License.



Licenses

☑	Asset	Usage	Product	License	License Expiration	Is Licensed	vCenter Server System
☑	Cluster1	2 CPUs	Evaluation Mode	Evaluation License	⚠ 05/20/2019	No	vcenter.ra.internal

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



Assign License

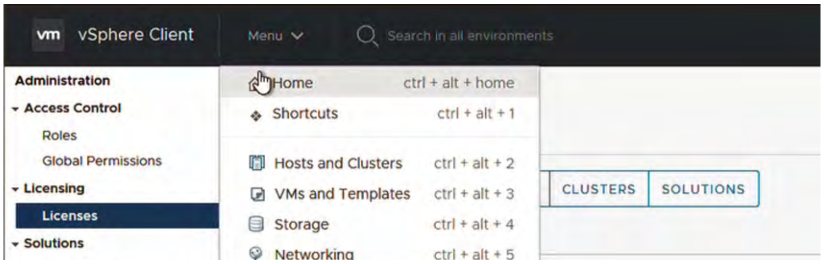
	License	License Key	Product	Usage	Capacity	Features
○	Evaluation License	--	--	--	--	
●	AB Virtual Appliance - vSA...	[redacted]	VMware vSAN Enterprise (CPUs)	• 2 CPUs	2 CPUs	ⓘ

Assignment Validation for AB Virtual Appliance - vSAN

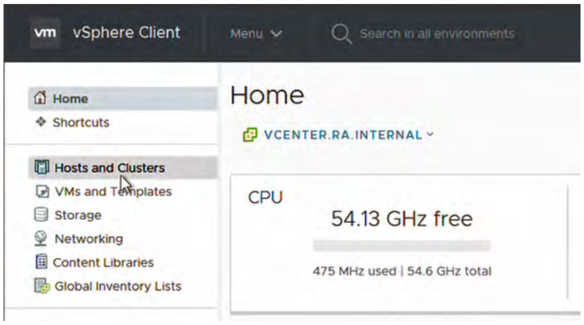
✓ The license assignment is valid.

Click OK. You are returned to the Clusters page.

27. Select Menu > Home.



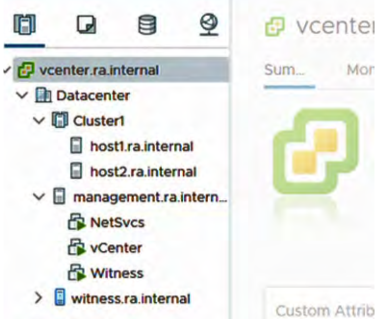
28. Under the Home navigation pane, select Hosts and Clusters.



CPU 54.13 GHz free

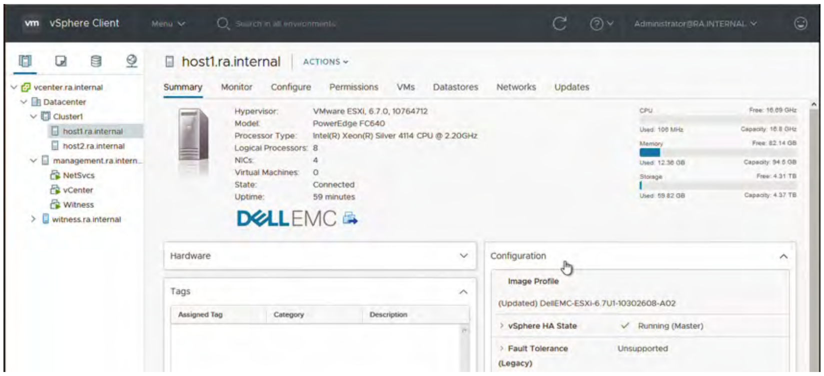
475 MHz used | 54.6 GHz total

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.



Hypervisor: VMware ESXi, 6.7.0, 10764712
Model: PowerEdge FC640
Processor Type: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Logical Processors: 8
NICs: 4
Virtual Machines: 0
State: Connected
Uptime: 59 minutes

CPU Free: 16.69 GHz
Used: 106 MHz Capacity: 16.8 GHz
Memory Free: 82.14 GB
Used: 12.36 GB Capacity: 94.5 GB
Storage Free: 4.31 TB
Used: 59.82 GB Capacity: 4.37 TB

Assigned Tag	Category	Description

Image Profile
(Updated) DellEMC-ESXi-6.7U1-10302608-A02
vSphere HA State ✓ Running (Master)
Fault Tolerance (Legacy) Unsupported

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

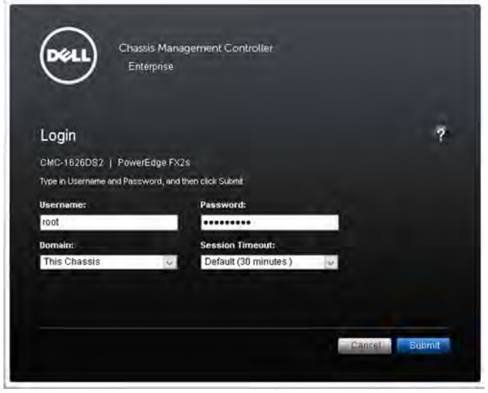
Change the Default Password

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>.



Login

CMC-1626DS2 | PowerEdge FX2s

Type in Username and Password, and then click Submit

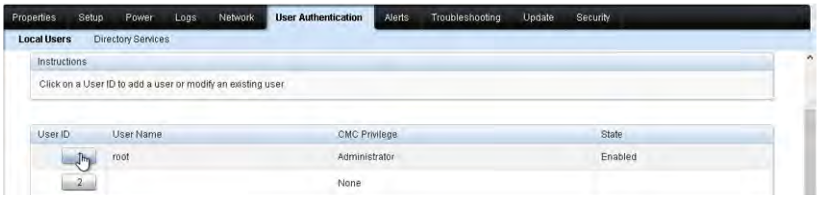
Username: root

Password: ●●●●●●●●●

Domain: This Chassis

Session Timeout: Default (30 minutes)

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

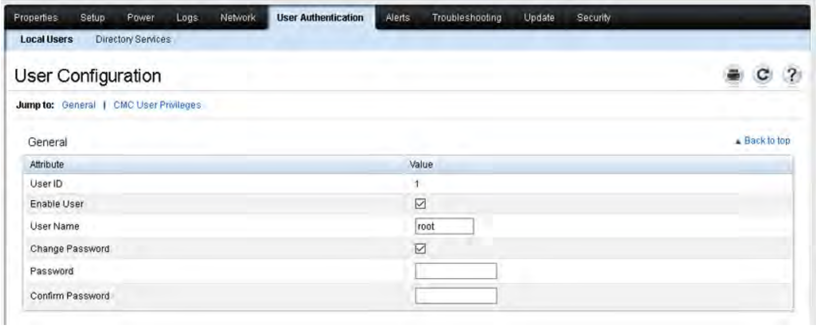


Instructions

Click on a User ID to add a user or modify an existing user

User ID	User Name	CMC Privilege	State
[illegible]	root	Administrator	Enabled
2		None	

5. Select the Change Password box.



User Configuration

General

Attribute	Value
User ID	1
Enable User	☑
User Name	root
Change Password	☑
Password	
Confirm Password	

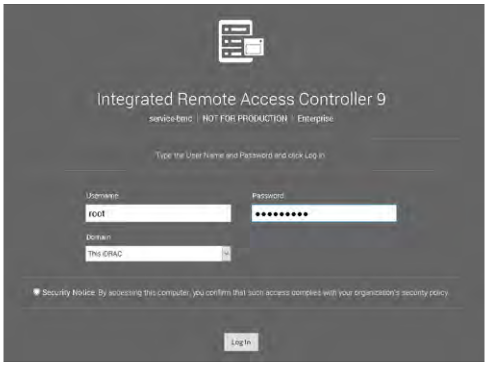
6. Enter the new password in the Password and Confirm Password fields.
7. Click Apply.
8. Log off from the CMC website, and verify that you can log in with the new password.

Baseboard Management Controller (BMC)

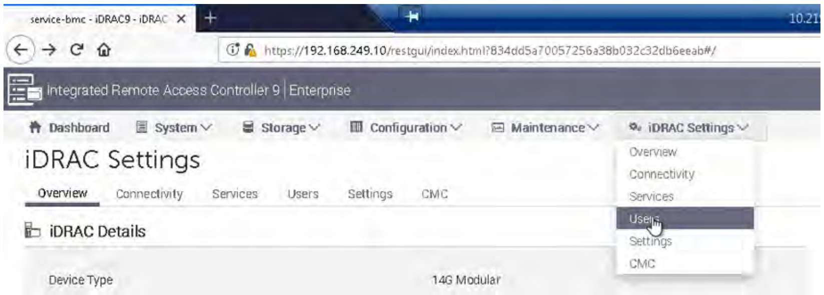
For the BMC, there is one service and two host management controllers with each appliance. To change the system password in each one, perform the following steps.

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>

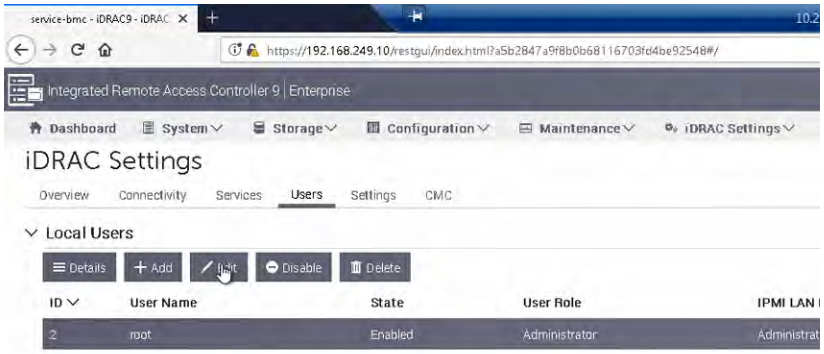

Integrated Remote Access Controller 9
service-bmc | NOT FOR PRODUCTION | Enterprise
Type the User Name and Password and click Log in
Username: root
Password: ••••••••••
Domain: This iDRAC
Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

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



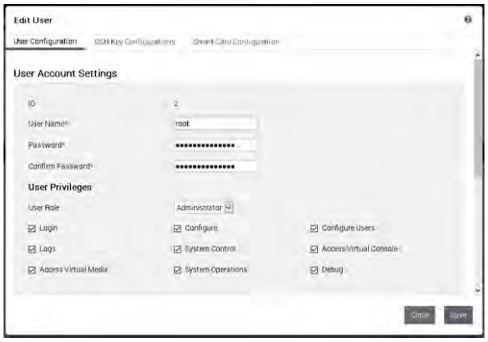
Device Type 14G Modular

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



ID	User Name	State	User Role	IPMI LAN I
2	root	Enabled	Administrator	Administrat

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



Edit User

User Account Settings

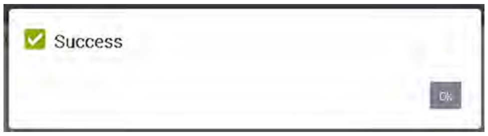
ID	2	
User Name*	root	
Password*	•••••••••••••••	
Confirm Password*	•••••••••••••••	

User Privileges

User Role	Administrator	
☑ Login	☑ Configure	☑ Configure Users
☑ Logs	☑ System Control	☑ Access Virtual Console
☑ Access Virtual Media	☑ System Operations	☑ Debug

5. When finished, click Save.

6. When the success window appears, click OK.



☑ Success

7. Log off from the BMC website, and verify that you can log in with the new password.

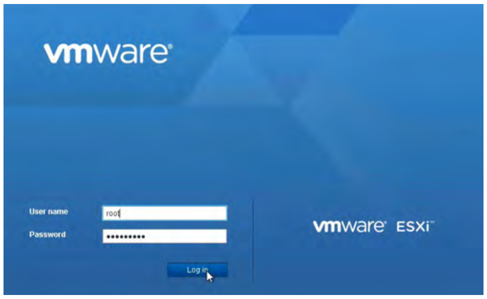
8. Repeat steps 1...7 for each of the two host management controllers. For step 1, use these URL addresses for each host controller:
   - Host 1: https://192.168.249.11
   - Host 2: https://192.168.249.12

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>

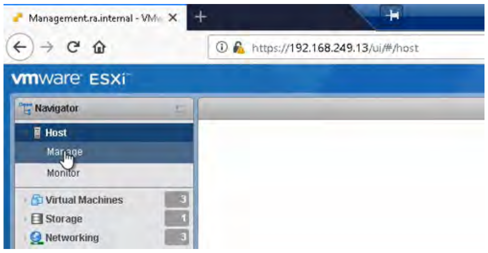


User name: root

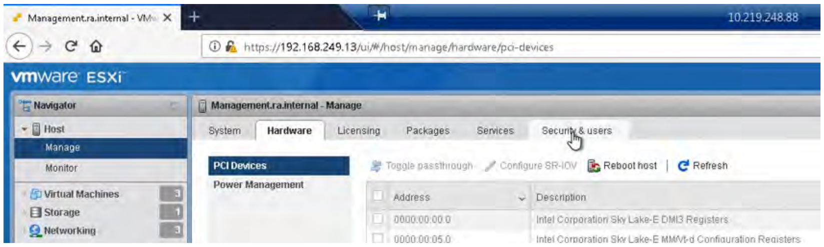
Password: •••••••••

2. Click Login.

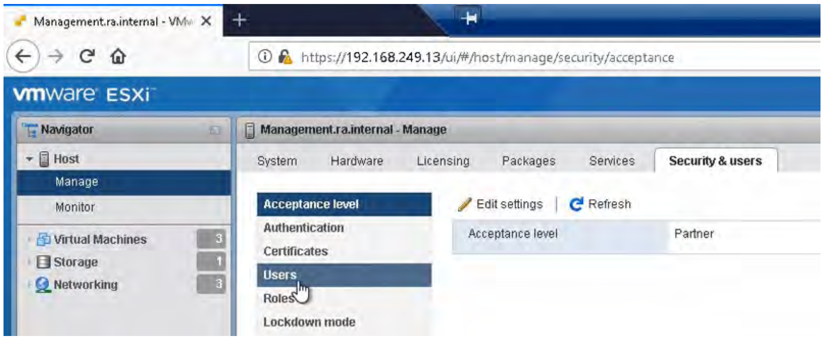
3. Under the Navigator pane, click Manage.



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

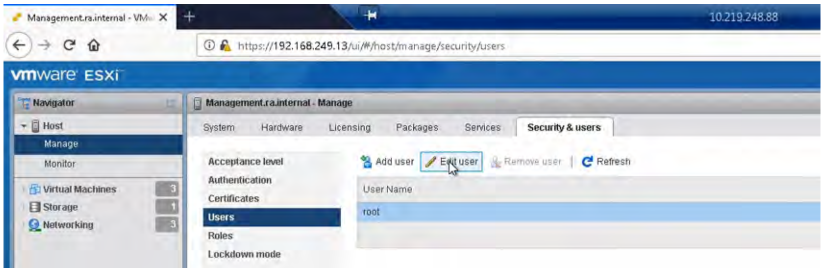


5. Under the Acceptance Level navigation pane, select Users.

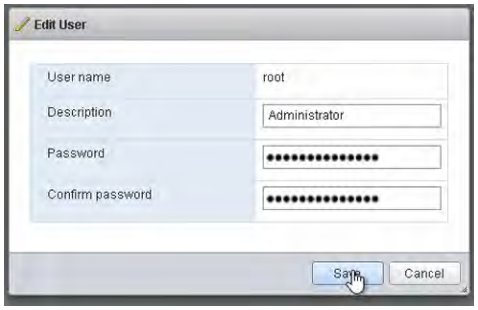


Acceptance level: Partner

6. Select 'root' and click Edit user.



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



User name	root
Description	Administrator
Password	•••••••••••••••
Confirm password	•••••••••••••••

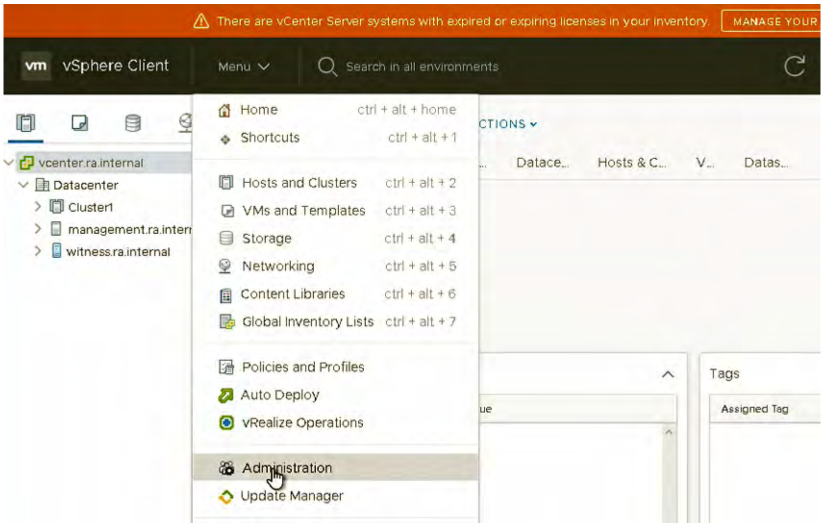
8. When finished, click Save.

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

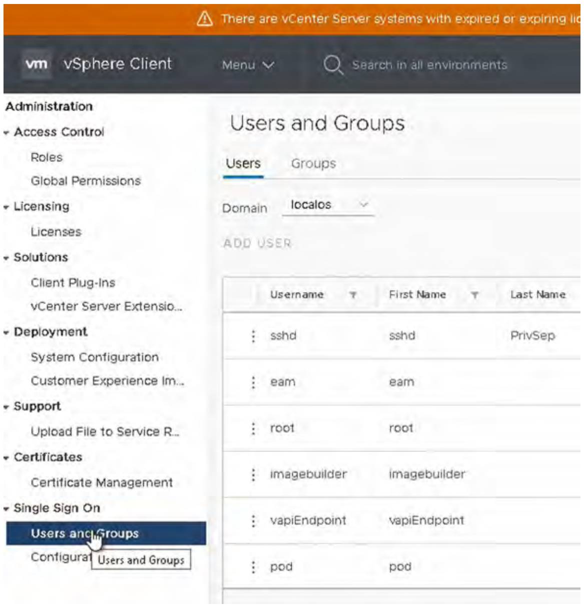
To change the password in vCenter, perform the following steps.

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.



There are vCenter Server systems with expired or expiring licenses in your inventory.

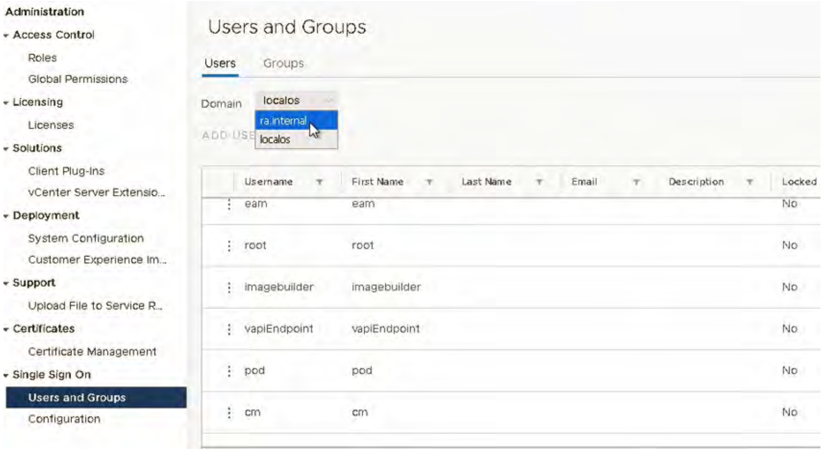
3. Under the Administration navigation pane, select Single Sign On > Users and Groups.



Domain localos

Username	First Name	Last Name
sshd	sshd	PrivSep
eam	eam	
root	root	
imagebuilder	imagebuilder	
vapiEndpoint	vapiEndpoint	
pod	pod	

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



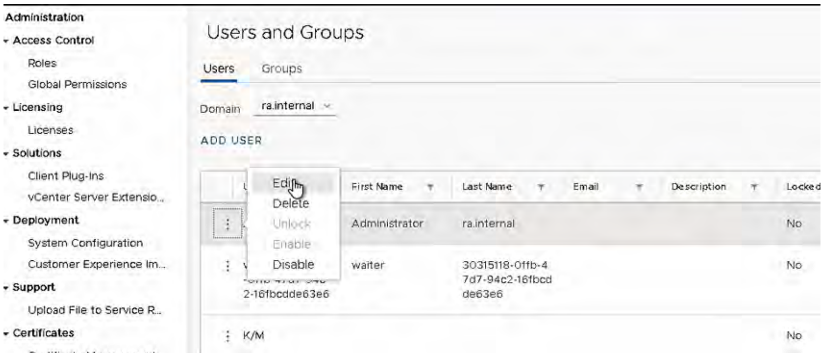
Domain localos

Username	First Name	Last Name	Email	Description	Locked
eam	eam				No
root	root				No
imagebuilder	imagebuilder				No
vapiEndpoint	vapiEndpoint				No
pod	pod				No
cm	cm				No

5. Under the ra.internal domain users, select the Administrator row.

6. Click the ellipsis next to the Administrator account.

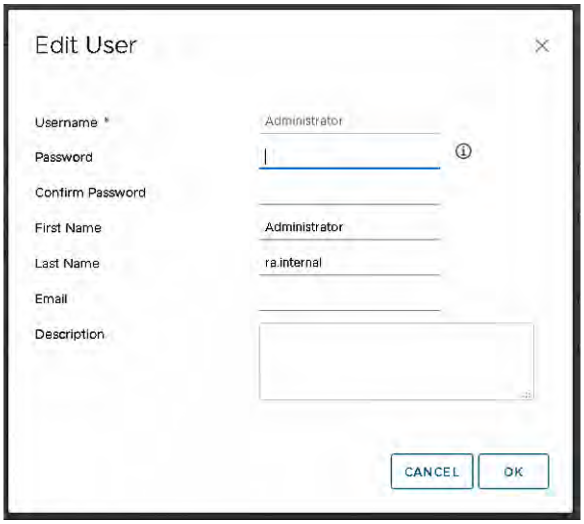
7. From the popup menu, select Edit.



Domain ra.internal

U	First Name	Last Name	Email	Description	Locked
	Administrator	ra.internal			No
v 2-16fbcdde63e6	waiter	30315118-0ffb-4 7d7-94c2-16fbcd de63e6			No
K/M					No

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



Edit User

Username * Administrator

Password

Confirm Password

First Name Administrator

Last Name ra.internal

Email

Description

9. When finished, click OK.

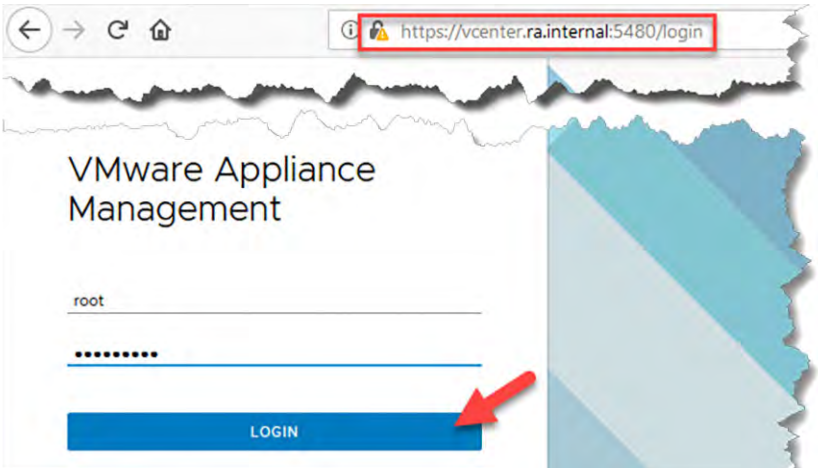
10. Log off from the vCenter website, and verify that you can log in with the new password.

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.



https://vcenter.ra.internal:5480/login

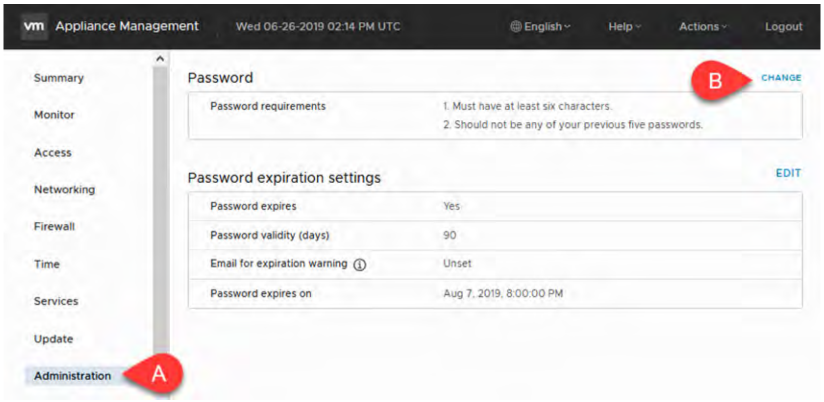
VMware Appliance Management

root

•••••••••

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).



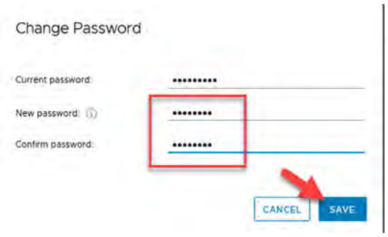
Password

Password requirements	1. Must have at least six characters. 2. Should not be any of your previous five passwords.

Password expiration settings

Password expires	Yes
Password validity (days)	90
Email for expiration warning ⓘ	Unset
Password expires on	Aug 7, 2019, 8:00:00 PM

5. Enter and confirm the New Password.


Change Password

Current password: ••••••••••

New password: ⓘ ••••••••

Confirm 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.

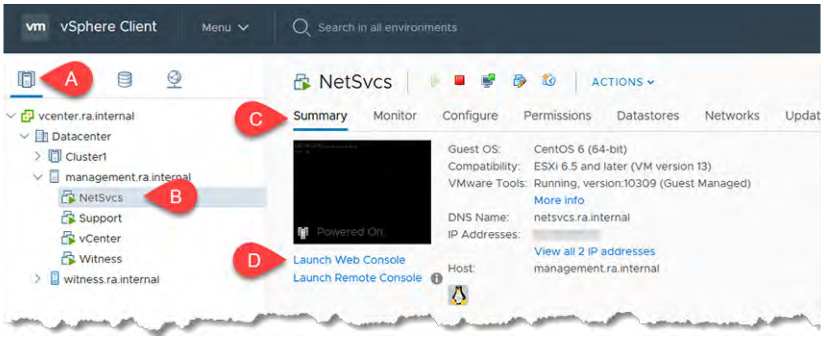
NetSvcs

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).

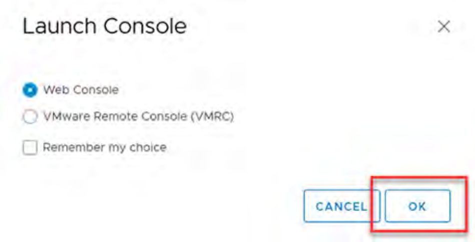
3. On the Summary tab (C), click Launch Web Console (D).



Guest OS: CentOS 6 (64-bit)
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Running, version:10309 (Guest Managed)
DNS Name: netsvcs.ra.internal
IP Addresses: [redacted]
Host: management.ra.internal

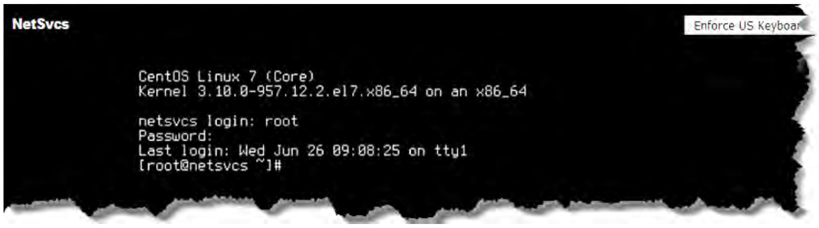
4. On Launch Console, click OK.

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



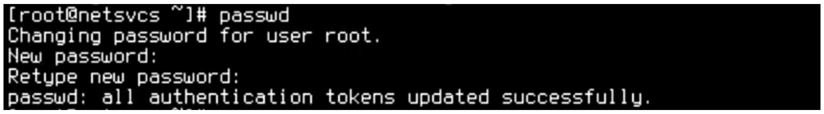
● Web Console
○ VMware Remote Console (VMRC)
□ Remember my choice

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



```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.12.2.el7.x86_64 on an x86_64

netsvcs login: root
Password:
Last login: Wed Jun 26 09:08:25 on tty1
[root@netsvcs ~]#
```

6. Enter the new password and retype.



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

7. Log in as sysadmin and repeat step 5...step 7.

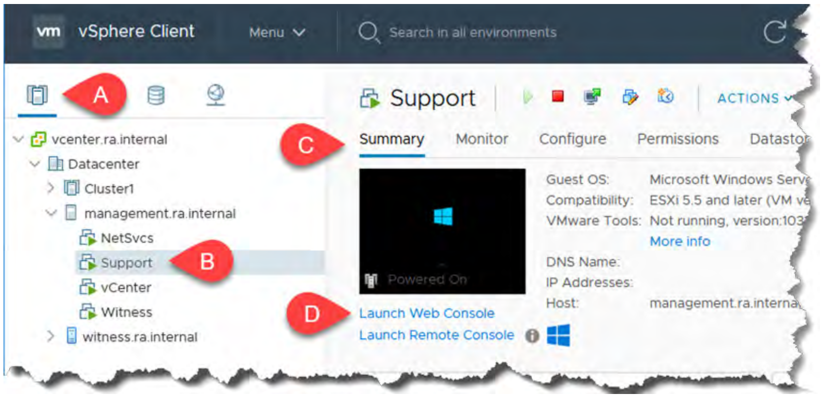
   CentOS prompts user for the current password.

8. When finished, enter log off or press Control+D.

Support

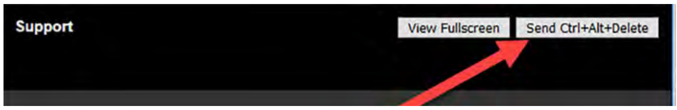
To change the password in the Support VM, perform the following steps.

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).

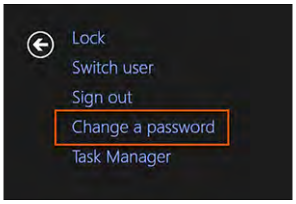


Guest OS: Microsoft Windows Serv
Compatibility: ESXi 5.5 and later (VM ve
VMware Tools: Not running, version:103
More info
DNS Name:
IP Addresses:
Host: management.ra.interna

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

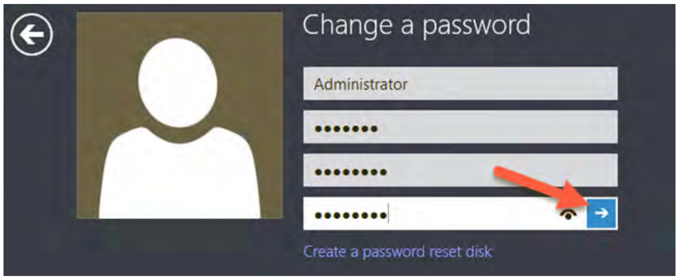


5. Once logged in, press Ctrl+Alt+Delete again, and then click Change a Password.



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

   When finished, click the blue arrow.



Administrator
•••••••
••••••••
••••••••

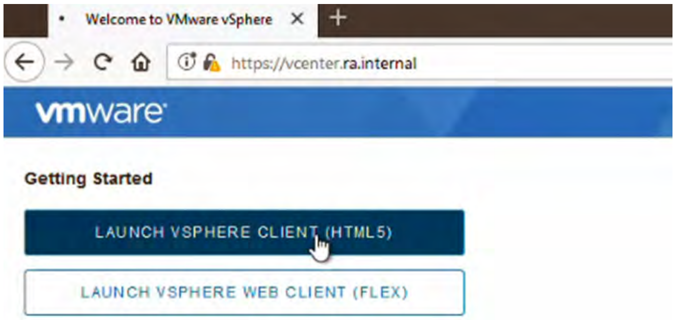
7. Log off Microsoft Windows, and verify that you can log in with the new password.

Configure Active Directory Authentication

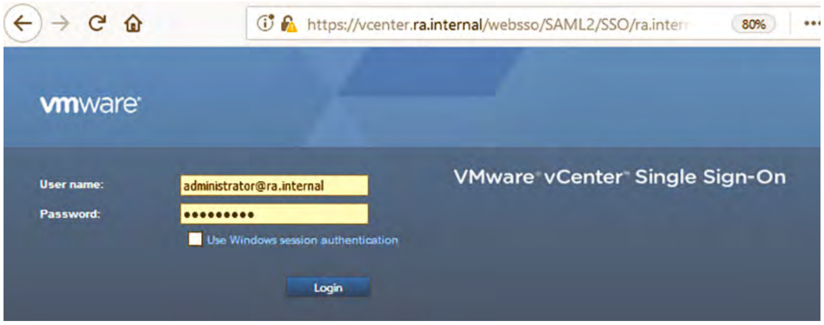
If you want to use domain users to manage VMware vCenter with Active Directory credentials, you can create a Lightweight Directory Access Protocol (LDAP) identity source to manage vCenter.

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).

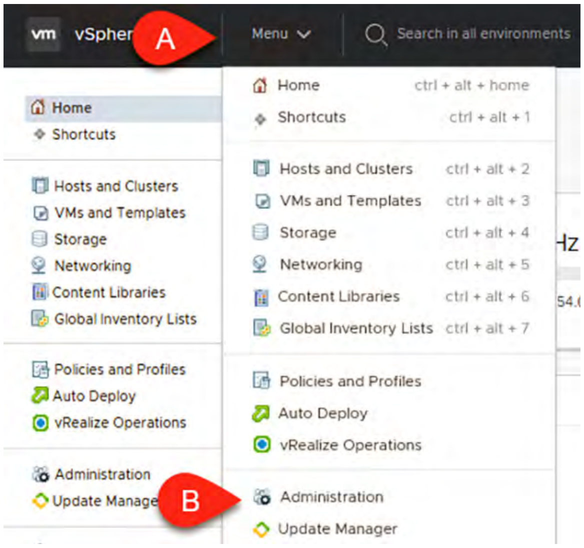

Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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

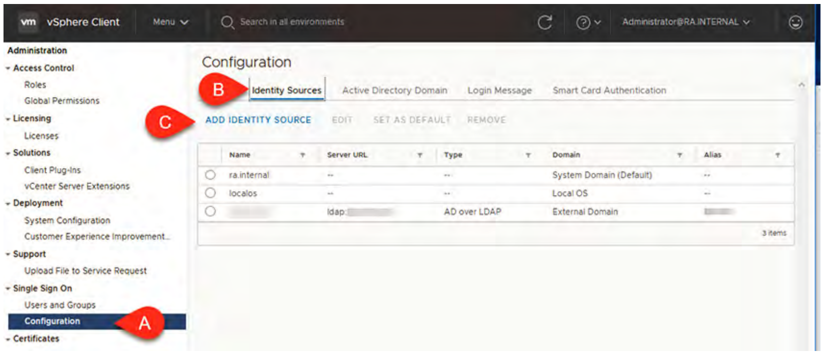

https://vcenter.ra.internal/websso/SAML2/SSO/ra.inter
80%
vmware
VMware vCenter Single Sign-On

User name: administrator@ra.internal
Password: •••••••••
□ Use Windows session authentication

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



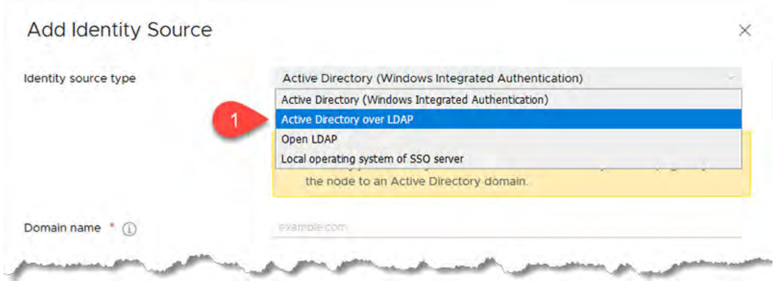
5. In the Administration navigation view, select Configuration (A).
   a. On Configuration, click the Identity Sources tab (B).
   b. On Identity Sources, click Add Identity Source (C).



	Name	Server URL	Type	Domain	Alias
○	ra.internal	--	--	System Domain (Default)	--
○	localos	--	--	Local OS	--
○	[redacted]	ldap:[redacted]	AD over LDAP	External Domain	[redacted]

3 items

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


Add Identity Source
×
1
Active Directory (Windows Integrated Authentication)
Active Directory over LDAP
Open LDAP
Local operating system of SSO server

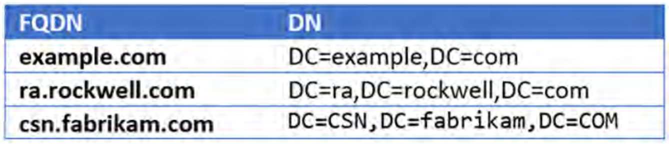
Identity source type: Active Directory (Windows Integrated Authentication)

the node to an Active Directory domain.

Domain name *: example.com

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'.

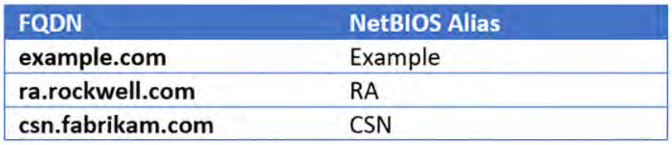


FQDN	DN
example.com	DC=example,DC=com
ra.rockwell.com	DC=ra,DC=rockwell,DC=com
csn.fabrikam.com	DC=CSN,DC=fabrikam,DC=COM

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

   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'.

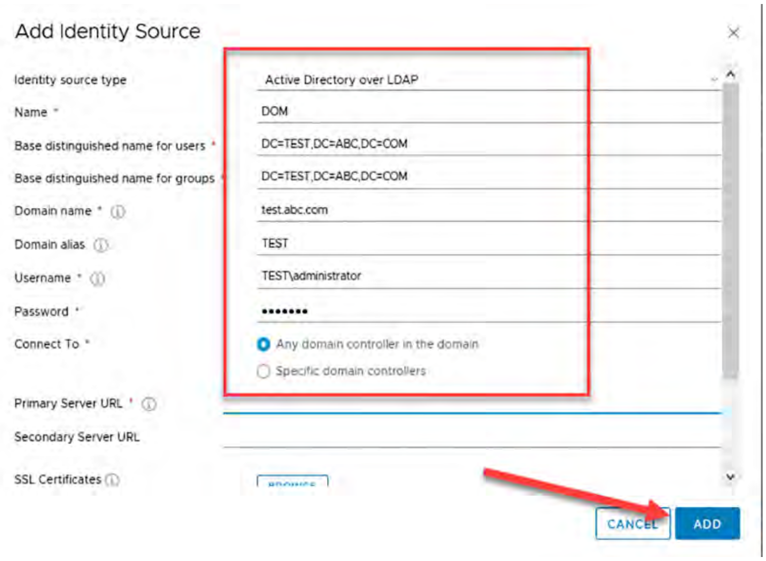


FQDN	NetBIOS Alias
example.com	Example
ra.rockwell.com	RA
csn.fabrikam.com	CSN

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.



Add Identity Source

Identity source type: Active Directory over LDAP

Name *: DOM

Base distinguished name for users *: DC=TEST,DC=ABC,DC=COM

Base distinguished name for groups *: DC=TEST,DC=ABC,DC=COM

Domain name *: test.abc.com

Domain alias: TEST

Username *: TEST\administrator

Password *: •••••••

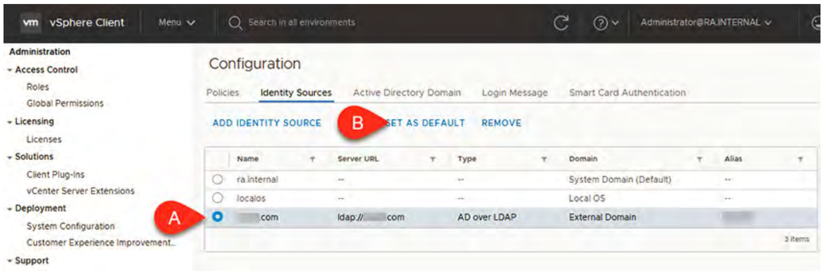
Connect To *: ● Any domain controller in the domain ○ Specific domain controllers

Primary Server URL *:

Secondary Server URL:

SSL Certificates:

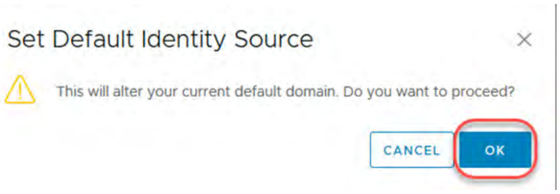
8. Select the newly created Identity Source (A), and then click Set as Default Domain (B).



	Name	Server URL	Type	Domain	Alias
○	ra.internal	--	--	System Domain (Default)	--
○	localos	--	--	Local OS	--
●	[redacted].com	ldap://[redacted].com	AD over LDAP	External Domain	[redacted]

3 items

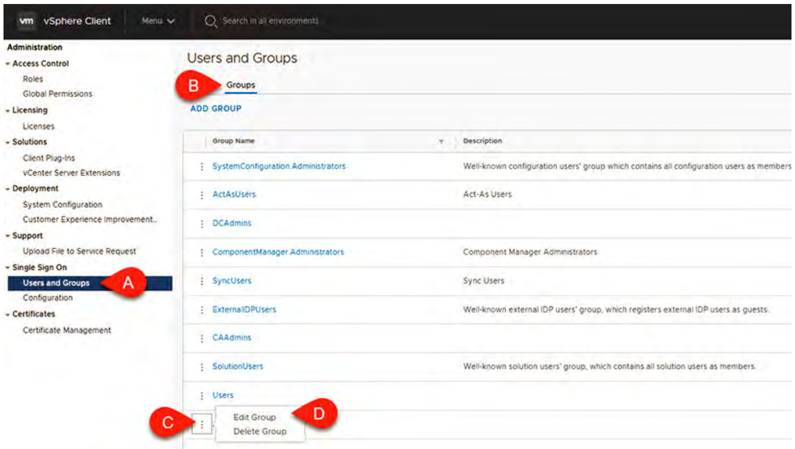
9. A warning appears; click OK.



Set Default Identity Source

This will alter your current default domain. Do you want to proceed?

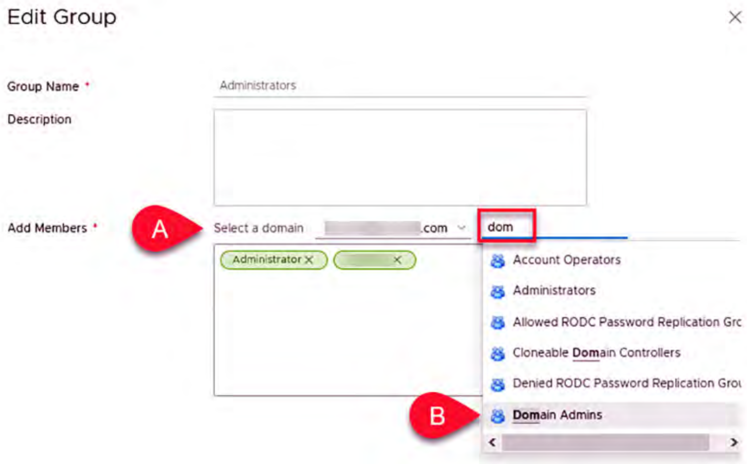
10. In the Administration navigation view, select Users and Groups (A).
    a. On Users and Groups, click the Groups tab (B).
    b. On Groups, click the ellipse next to the Administrators group (C).
    c. From the pull-down menu, select Edit Group (D).



Users and Groups

Group Name	Description
SystemConfiguration.Administrators	Well-known configuration users' group which contains all configuration users as members
ActAsUsers	Act-As Users
DCAdmins	
ComponentManager.Administrators	Component Manager Administrators
SyncUsers	Sync Users
ExternalIDPUsers	Well-known external IDP users' group, which registers external IDP users as guests.
CAAdmins	
SolutionUsers	Well-known solution users' group, which contains all solution users as members.
Users	

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).


×
A
B
Account Operators
Administrators
Allowed RODC Password Replication Grc
Cloneable Domain Controllers
Denied RODC Password Replication Grou
Domain Admins

Edit Group

Group Name * Administrators

Description

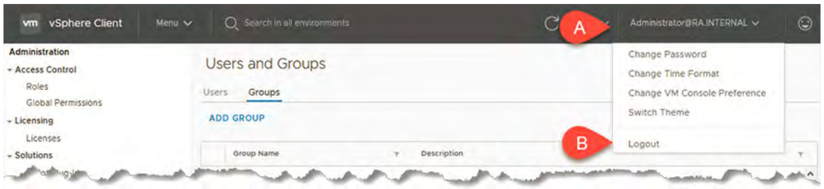
Add Members * Select a domain [redacted].com dom

Administrator × [redacted] ×

12. Click OK.

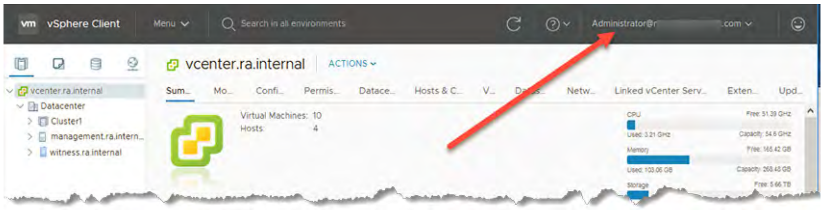
13. Click the user name in the top right of the window (A).

    From the pull-down menu, select Logout (B).



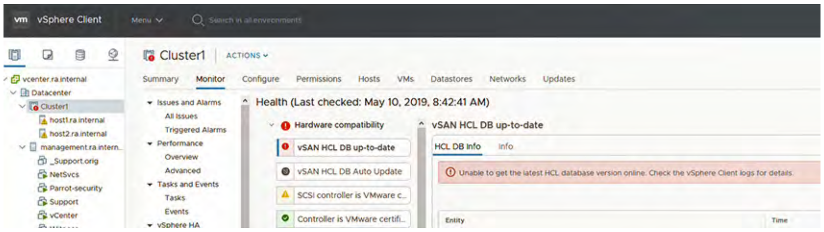
14. At the vSphere web client login prompt, use your new Domain Admin credentials to log in.

    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.

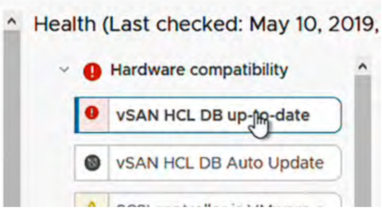


Health (Last checked: May 10, 2019, 8:42:41 AM)

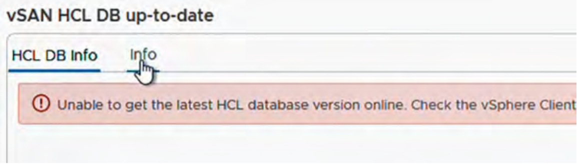
Unable to get the latest HCL database version online. Check the vSphere Client logs for details.

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

1. Click the alert about the outdated vSAN HCL DB.

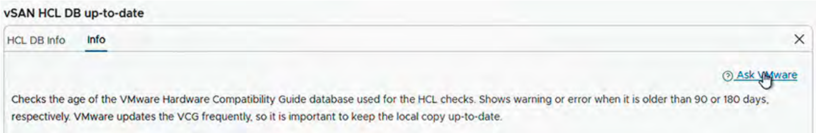


2. Click the Info tab.



Unable to get the latest HCL database version online. Check the vSphere Client

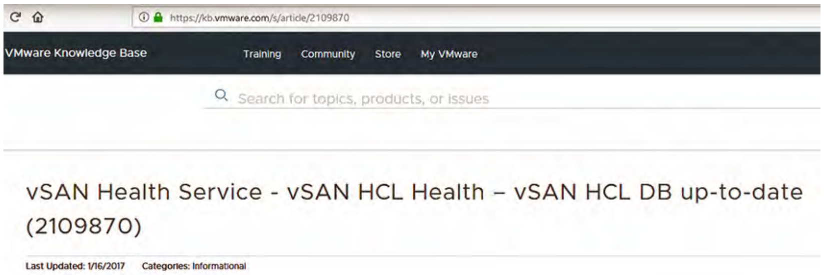
3. On Info, click Ask VMware.



Checks the age of the VMware Hardware Compatibility Guide database used for the HCL checks. Shows warning or error when it is older than 90 or 180 days, respectively. VMware updates the VCG frequently, so it is important to keep the local copy up-to-date.

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.


https://kb.vmware.com/s/article/2109870
VMware Knowledge Base
Training
Community
Store
My VMware
Search for topics, products, or issues

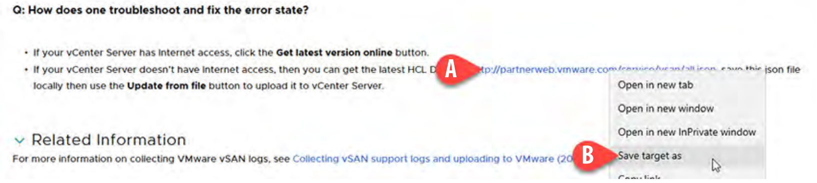
vSAN Health Service - vSAN HCL Health – vSAN HCL DB up-to-date (2109870)

Last Updated: 1/16/2017 Categories: Informational

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).



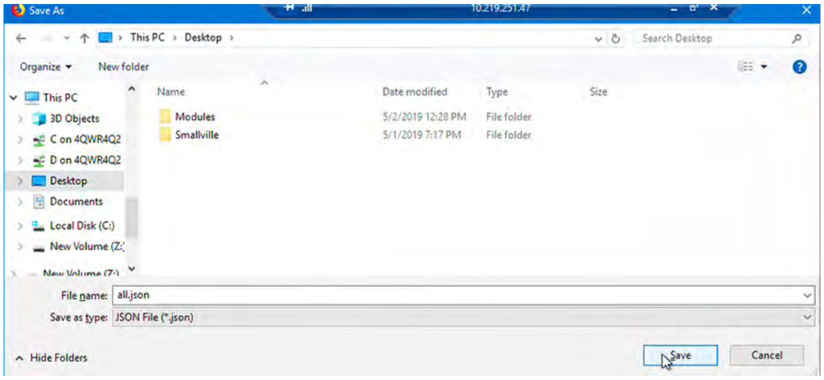
Q: How does one troubleshoot and fix the error state?

- If your vCenter Server has Internet access, click the **Get latest version online** button.
- If your vCenter Server doesn't have Internet access, then you can get the latest HCL D tp://partnerweb.vmware.com json file locally then use the **Update from file** button to upload it to vCenter Server.

Related Information

For more information on collecting VMware vSAN logs, see Collecting vSAN support logs and uploading to VMware (20

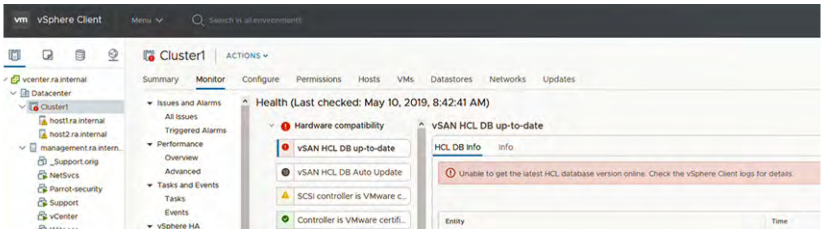
6. Navigate to your computer desktop and click Save.



File name: all.json

Save as type: JSON File (*.json)

7. Return to vSphere Client.

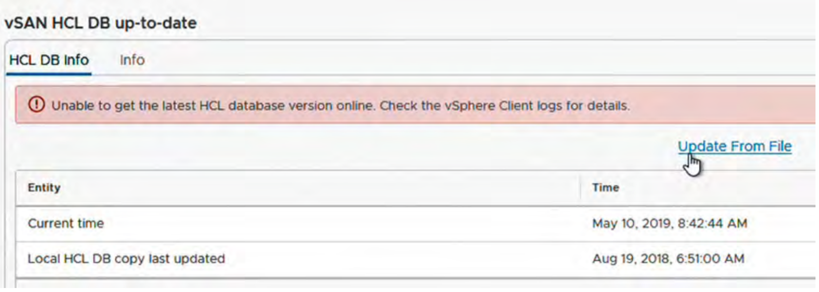


Health (Last checked: May 10, 2019, 8:42:41 AM)

Unable to get the latest HCL database version online. Check the vSphere Client logs for details.

8. Click the HCL DB Info tab.

9. On HCL DB Info, click Update from File.

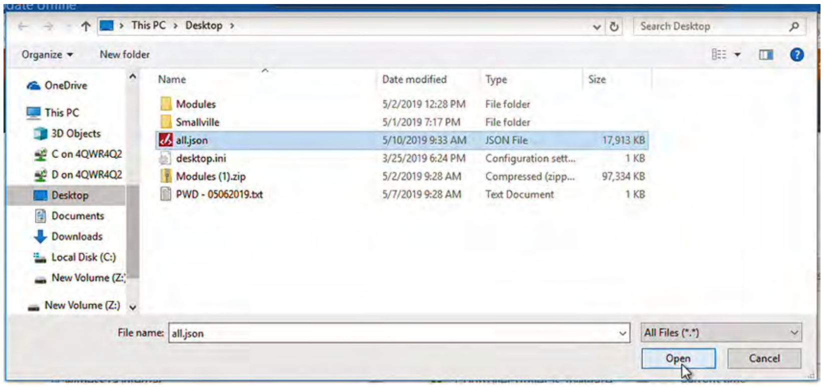


vSAN HCL DB up-to-date

ⓘ Unable to get the latest HCL database version online. Check the vSphere Client logs for details.

Entity	Time
Current time	May 10, 2019, 8:42:44 AM
Local HCL DB copy last updated	Aug 19, 2018, 6:51:00 AM

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

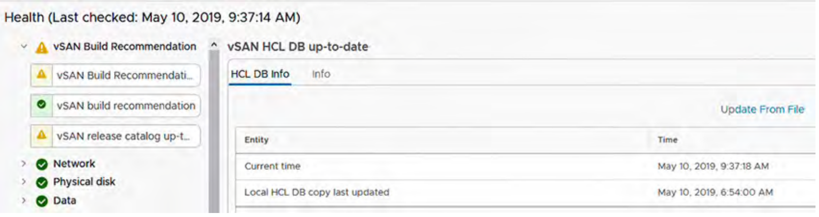


Name	Date modified	Type	Size
Modules	5/2/2019 12:28 PM	File folder	
Smallville	5/1/2019 7:17 PM	File folder	
all.json	5/10/2019 9:33 AM	JSON File	17,913 KB
desktop.ini	3/25/2019 6:24 PM	Configuration sett...	1 KB
Modules (1).zip	5/2/2019 9:28 AM	Compressed (zipp...	97,334 KB
PWD - 05062019.txt	5/7/2019 9:28 AM	Text Document	1 KB

File name: all.json

All Files (*.*)

Once updated, the Entity reflects the update.



Health (Last checked: May 10, 2019, 9:37:14 AM)

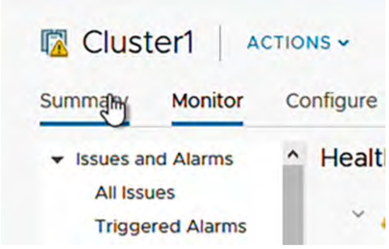
vSAN Build Recommendation
vSAN Build Recommendati...
vSAN build recommendation
vSAN release catalog up-t...
Network
Physical disk
Data

vSAN HCL DB up-to-date

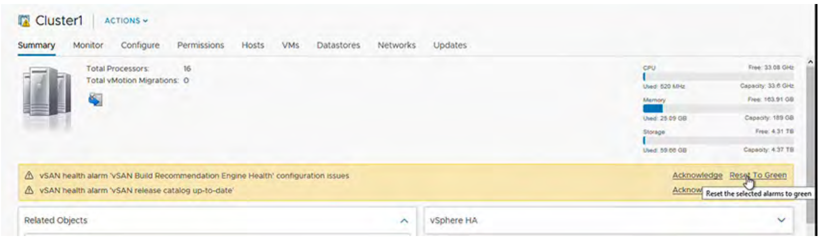
HCL DB Info
Info
Update From File

Entity	Time
Current time	May 10, 2019, 9:37:18 AM
Local HCL DB copy last updated	May 10, 2019, 6:54:00 AM

11. On Cluster1, click the Summary tab.



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



Total Processors: 16
Total vMotion Migrations: 0

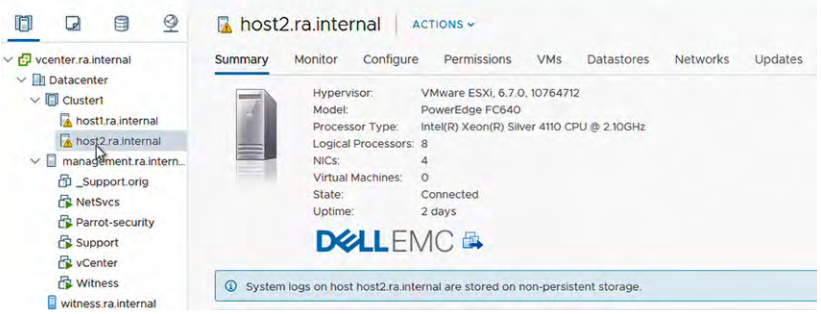
CPU Free: 33.08 GHz
Used: 520 MHz Capacity: 33.6 GHz
Memory Free: 163.91 GB
Used: 25.09 GB Capacity: 189 GB
Storage Free: 4.31 TB
Used: 59.66 GB Capacity: 4.37 TB

⚠ vSAN health alarm 'vSAN Build Recommendation Engine Health' configuration issues

⚠ vSAN health alarm 'vSAN release catalog up-to-date'

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.



Hypervisor: VMware ESXi, 6.7.0, 10764712
Model: PowerEdge FC640
Processor Type: Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
Logical Processors: 8
NICs: 4
Virtual Machines: 0
State: Connected
Uptime: 2 days

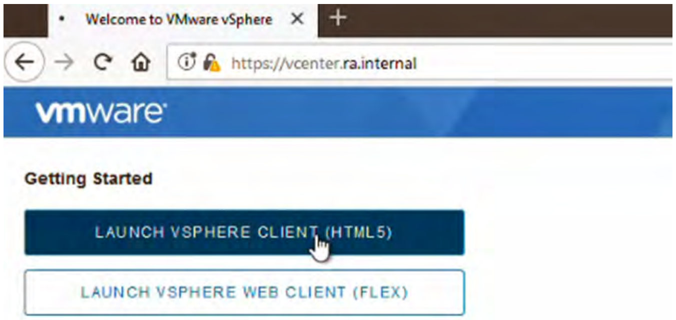
System logs on host host2.ra.internal are stored on non-persistent storage.

The VersaVirtual Appliance now has the most current HCL.

Add a Distributed Port Group

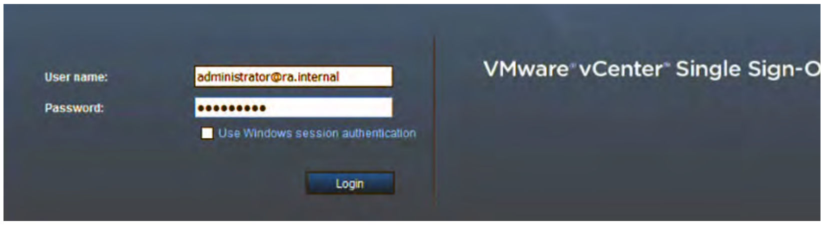
To add a distributed port group, perform the following steps.

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


Welcome to VMware vSphere
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

https://vcenter.ra.internal

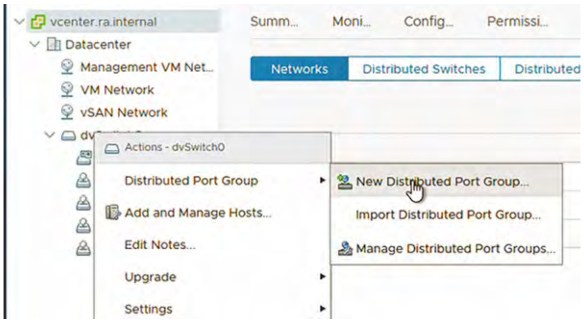
3. Log into https://192.168.249.18 with the following:
   - User name: administrator@ra.internal
   - Password: <system-specific password>


VMware vCenter Single Sign-O
Use Windows session authentication
Login

User name: administrator@ra.internal
Password: •••••••••

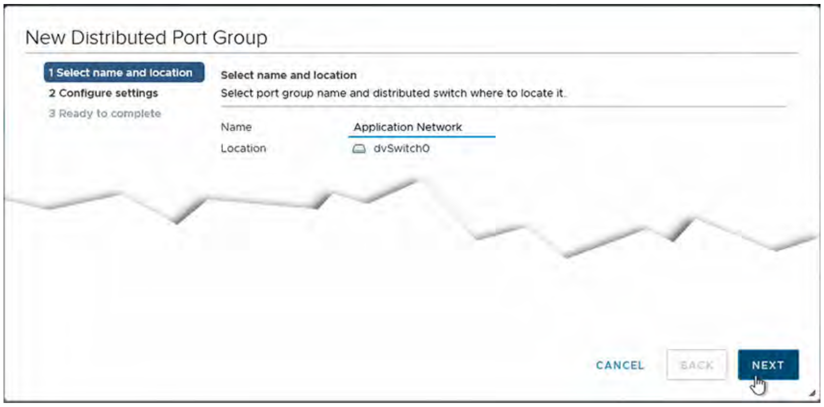
4. Click Login.

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



6. 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.



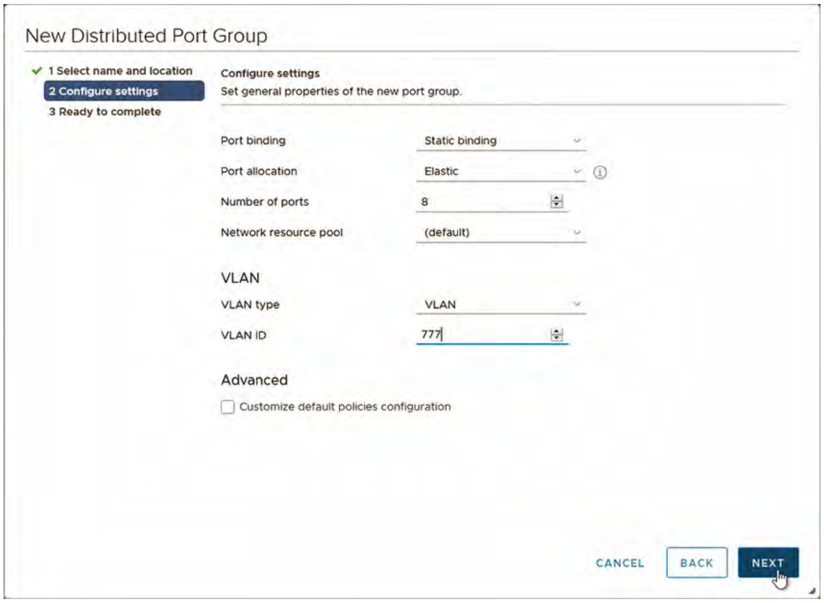
New Distributed Port Group

1 Select name and location
2 Configure settings
3 Ready to complete

Select name and location
Select port group name and distributed switch where to locate it.

Name: Application Network
Location: dvSwitch0

7. 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.



New Distributed Port Group

✓ 1 Select name and location
2 Configure settings
3 Ready to complete

Configure settings
Set general properties of the new port group.

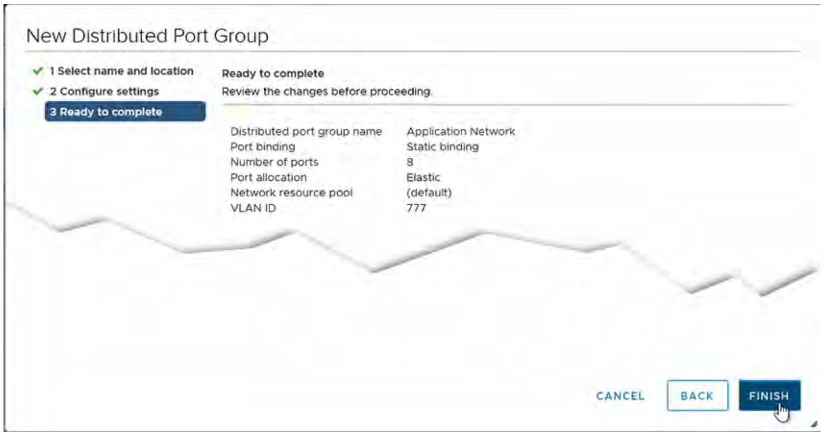
Port binding: Static binding
Port allocation: Elastic
Number of ports: 8
Network resource pool: (default)

VLAN
VLAN type: VLAN
VLAN ID: 777

Advanced
□ Customize default policies configuration

8. On step 3, review your additions and changes.

   If satisfied with your choices, click Finish.



New Distributed Port Group

- ✓ 1 Select name and location
- ✓ 2 Configure settings
- 3 Ready to complete

Ready to complete

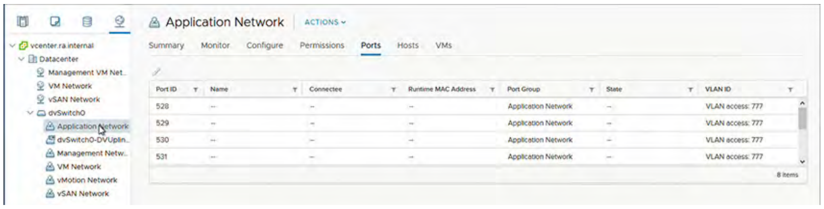
Review the changes before proceeding.

Distributed port group name	Application Network
Port binding	Static binding
Number of ports	8
Port allocation	Elastic
Network resource pool	(default)
VLAN ID	777

   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.

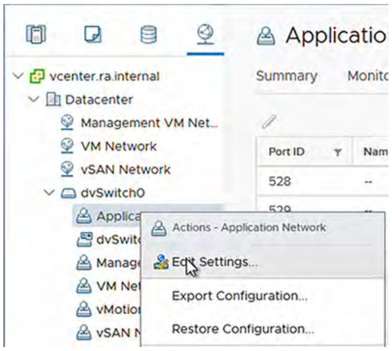


Port ID	Name	Connectee	Runtime MAC Address	Port Group	State	VLAN ID
528	--	--	--	Application Network	--	VLAN access: 777
529	--	--	--	Application Network	--	VLAN access: 777
530	--	--	--	Application Network	--	VLAN access: 777
531	--	--	--	Application Network	--	VLAN access: 777

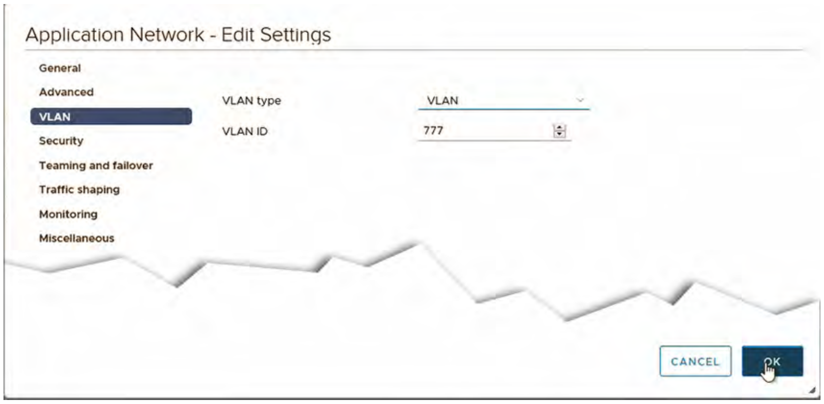
8 items

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.



12. Verify that the VLAN ID is the same as what you added in step 7 on page 93.



Application Network - Edit Settings

VLAN type: VLAN

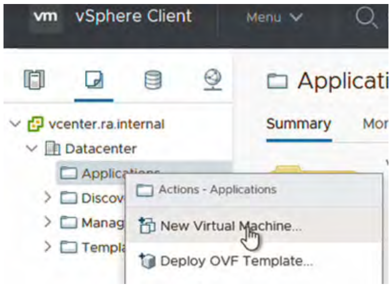
VLAN ID: 777

13. Click OK after the number is changed or verified.

Add a Virtual Machine

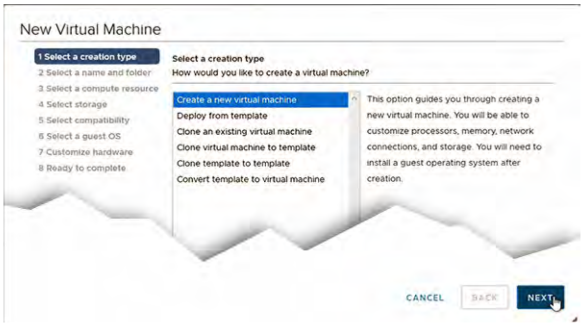
To add a virtual machine, perform the following steps.

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



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

   Click Next.



New Virtual Machine

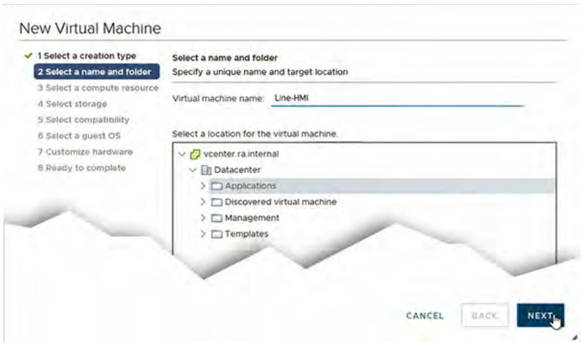
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine
CANCEL
BACK
NEXT

Select a creation type

How would you like to create a virtual machine?

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

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.



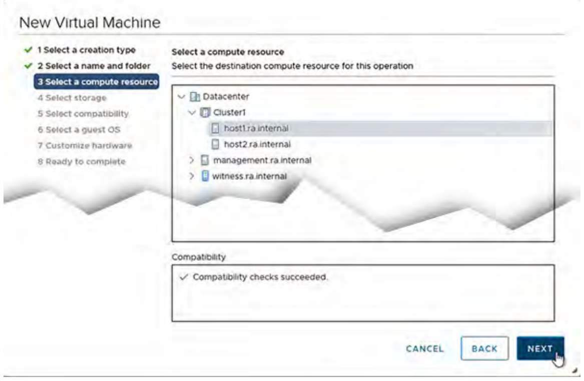
Select a name and folder
Specify a unique name and target location

Virtual machine name: Line-HMI

Select a location for the virtual machine.

- vcenter.ra.internal
  - Datacenter
    - Applications
    - Discovered virtual machine
    - Management
    - Templates

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.



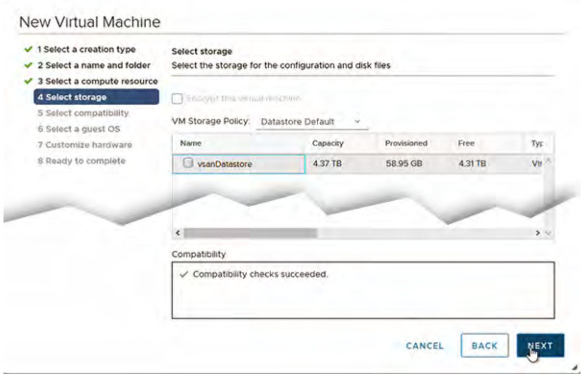
Select a compute resource
Select the destination compute resource for this operation

- Datacenter
  - Cluster1
    - host1.ra.internal
    - host2.ra.internal
  - management.ra.internal
  - witness.ra.internal

Compatibility

✓ Compatibility checks succeeded.

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.



Select storage
Select the storage for the configuration and disk files

□ Encrypt this virtual machine

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Ty
vsanDatastore	4.37 TB	58.95 GB	4.31 TB	Vi

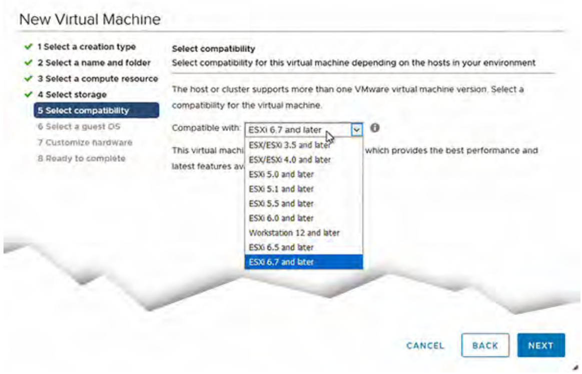
Compatibility

✓ Compatibility checks succeeded.

7. 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.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select compatibility
Select compatibility for this virtual machine depending on the hosts in your environment

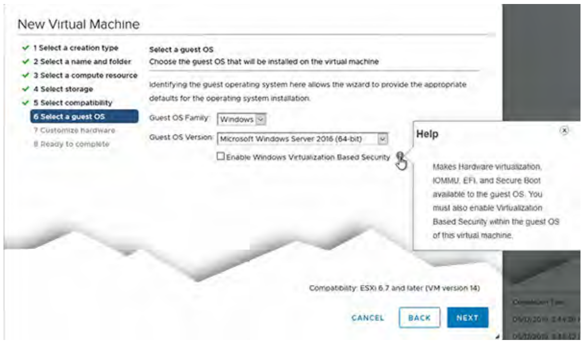
The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 6.7 and later

This virtual machi... which provides the best performance and latest features av...

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

   Click Next.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select a guest OS
Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Windows

Guest OS Version: Microsoft Windows Server 2016 (64-bit)

☐ Enable Windows Virtualization Based Security

Help

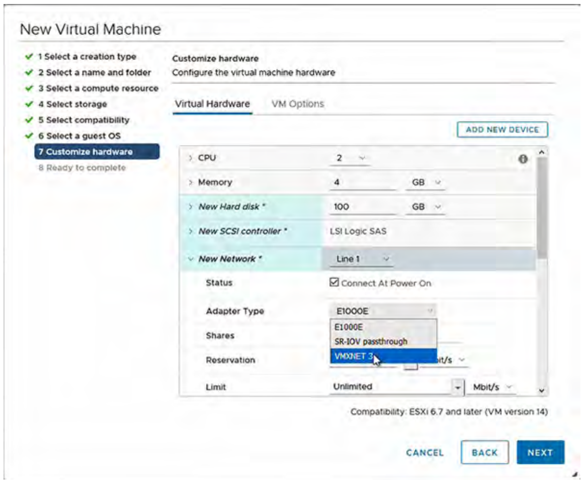
Makes Hardware virtualization, IOMMU, EFI, and Secure Boot available to the guest OS. You must also enable Virtualization Based Security within the guest OS of this virtual machine.

Compatibility: ESXi 6.7 and later (VM version 14)

9. 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.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

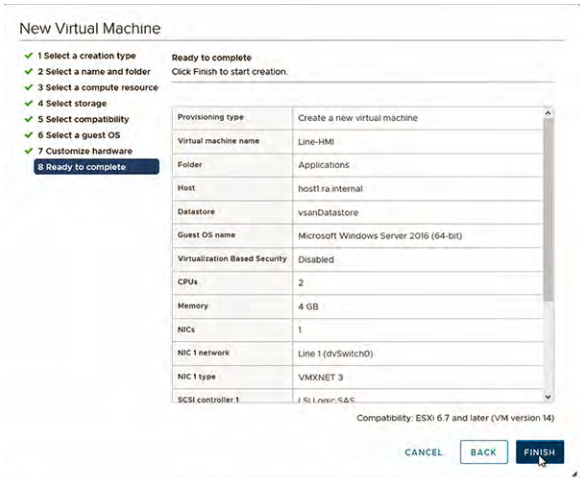
Customize hardware
Configure the virtual machine hardware

CPU	2	
Memory	4	GB
New Hard disk *	100	GB
New SCSI controller *	LSI Logic SAS	
New Network *	Line 1	
Status	☑ Connect At Power On	
Adapter Type	E1000E E1000E SR-IOV passthrough VMXNET 3	
Shares		
Reservation		...it/s
Limit	Unlimited	Mbit/s

Compatibility: ESXi 6.7 and later (VM version 14)

10. 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.



New Virtual Machine

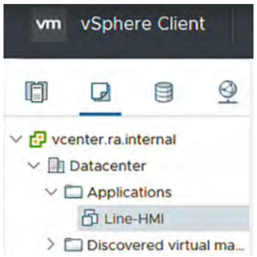
- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- ✓ 7 Customize hardware
- 8 Ready to complete

Ready to complete
Click Finish to start creation.

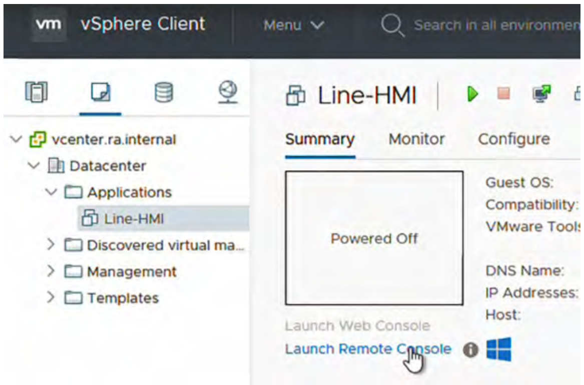
Provisioning type	Create a new virtual machine
Virtual machine name	Line-HMI
Folder	Applications
Host	host1.ra.internal
Datastore	vsanDatastore
Guest OS name	Microsoft Windows Server 2016 (64-bit)
Virtualization Based Security	Disabled
CPUs	2
Memory	4 GB
NICs	1
NIC 1 network	Line 1 (dvSwitch0)
NIC 1 type	VMXNET 3
SCSI controller 1	LSI Logic SAS

Compatibility: ESXi 6.7 and later (VM version 14)

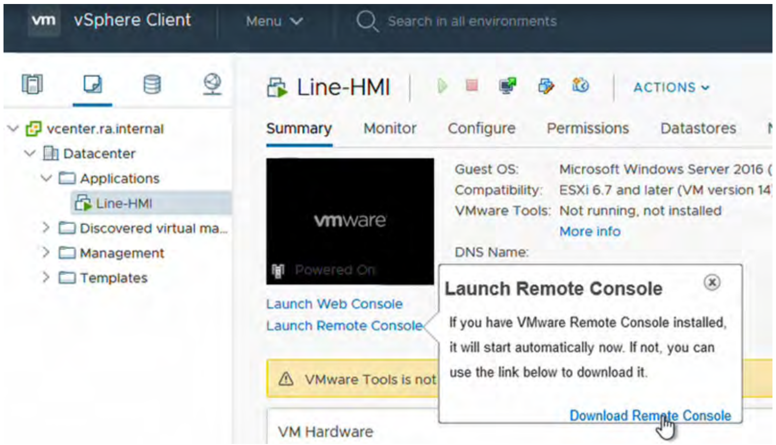
The new virtual machine is now visible under Applications in the Actions Navigation pane.



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



A popup window appears about the VMware Remote Console installation.



Guest OS: Microsoft Windows Server 2016 (
Compatibility: ESXi 6.7 and later (VM version 14
VMware Tools: Not running, not installed
More info
DNS Name:

Launch Remote Console

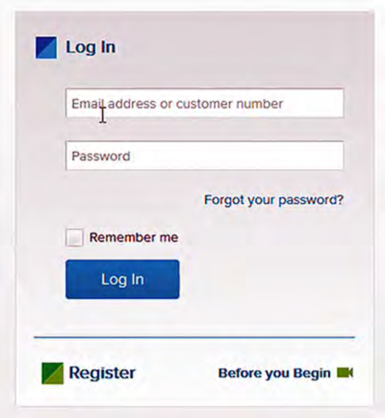
If you have VMware Remote Console installed, it will start automatically now. If not, you can use the link below to download it.

Download Remote Console

12. To install, click Download Remote Console.

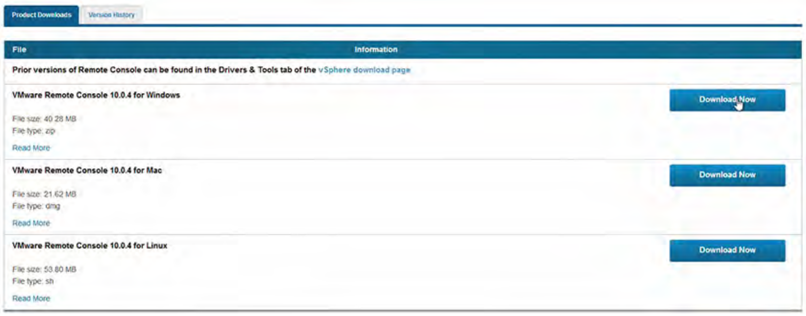
13. Log into VMware with your email address or customer number, and password.

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.



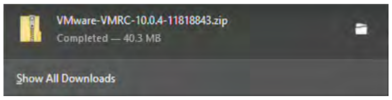
After you log in, you are automatically directed to the Remote Console Download page.

14. Click Download Now.



File	Information
Prior versions of Remote Console can be found in the Drivers & Tools tab of the vSphere download page	
VMware Remote Console 10.0.4 for Windows File size: 40.28 MB File type: zip Read More	Download Now
VMware Remote Console 10.0.4 for Mac File size: 21.62 MB File type: dmg Read More	Download Now
VMware Remote Console 10.0.4 for Linux File size: 53.80 MB File type: sh Read More	Download Now

The downloaded file is a WinZip file.

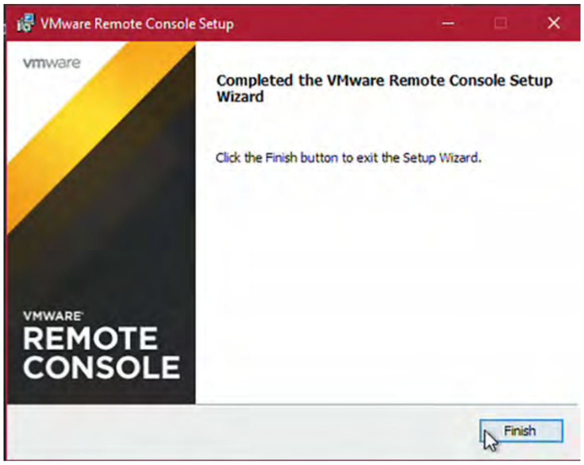

VMware-VMRC-10.0.4-11818843.zip
Completed — 40.3 MB

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.

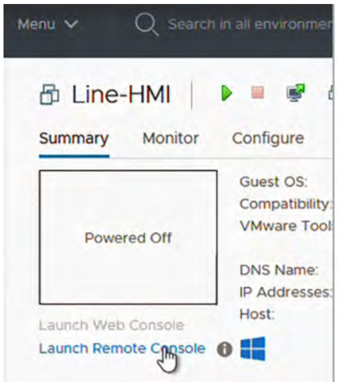
17. Click Finish when the installation is complete.


VMware Remote Console Setup

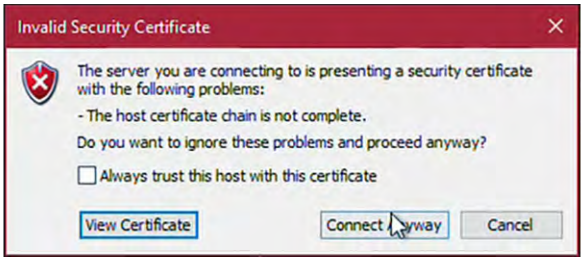
Completed the VMware Remote Console Setup Wizard

Click the Finish button to exit the Setup Wizard.

18. Launch the VMware Remote Console application.



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



Invalid Security Certificate

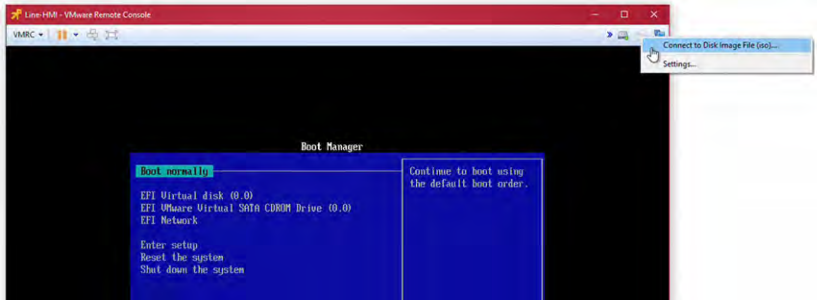
The server you are connecting to is presenting a security certificate with the following problems:

- The host certificate chain is not complete.

Do you want to ignore these problems and proceed anyway?

□ Always trust this host with this certificate

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

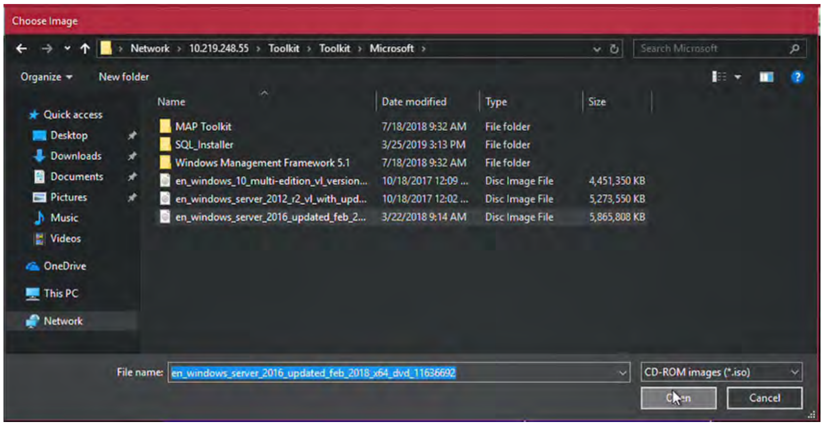


Line-HMI - VMware Remote Console
VMRC
Connect to Disk Image File (iso)...
Settings...

```
Boot Manager

Boot normally                         Continue to boot using
                                      the default boot order.
EFI Virtual disk (0.0)
EFI VMware Virtual SATA CDROM Drive (0.0)
EFI Network

Enter setup
Reset the system
Shut down the system
```

20. Navigate to the network address for available disk image files.

21. Highlight the most current disk image file and click Open.

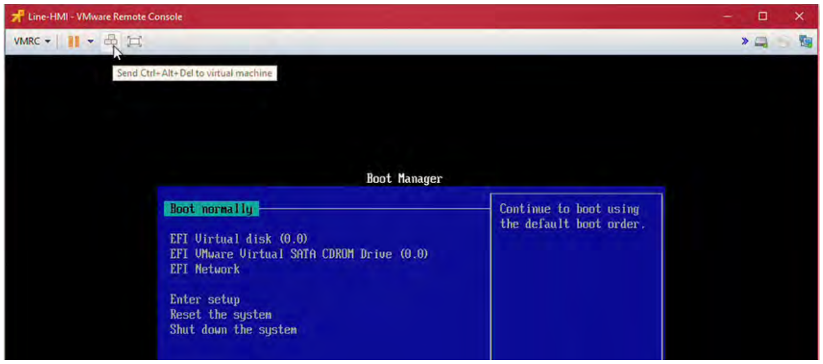


Name	Date modified	Type	Size
MAP Toolkit	7/18/2018 9:32 AM	File folder	
SQL_Installer	3/25/2019 3:13 PM	File folder	
Windows Management Framework 5.1	7/18/2018 9:32 AM	File folder	
en_windows_10_multi-edition_vl_version...	10/18/2017 12:09 ...	Disc Image File	4,451,350 KB
en_windows_server_2012_r2_vl_with_upd...	10/18/2017 12:02 ...	Disc Image File	5,273,550 KB
en_windows_server_2016_updated_feb_2...	3/22/2018 9:14 AM	Disc Image File	5,865,808 KB

File name: en_windows_server_2016_updated_feb_2018_x64_dvd_11636692

CD-ROM images (*.iso)

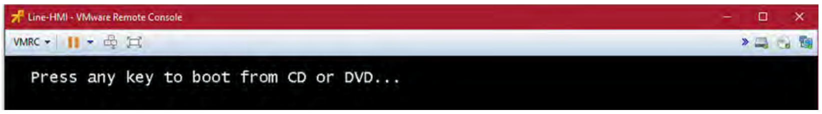
22. On the Boot Manager screen, click the Send Ctrl+Alt+Delete icon on the quick access toolbar.



Line-HMI - VMware Remote Console
VMRC
Send Ctrl+Alt+Del to virtual machine

```
Boot Manager

Boot normally                         Continue to boot using
                                      the default boot order.
EFI Virtual disk (0.0)
EFI VMware Virtual SATA CDROM Drive (0.0)
EFI Network

Enter setup
Reset the system
Shut down the system
```

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



```
Press any key to boot from CD or DVD...
```

The setup screen appears for the chosen Windows OS.

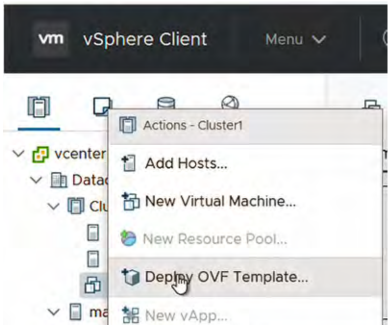
24. Follow the various screen prompts to install Windows.

The new virtual machine is successfully added to your network.

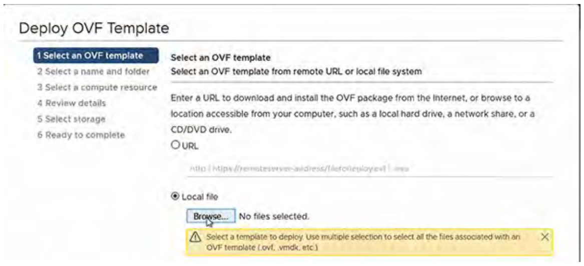
Import an OVA Template

To import an OVA template, perform the following steps.

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



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



Select an OVF template

Select an OVF template from remote URL or local file system

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

○ URL

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

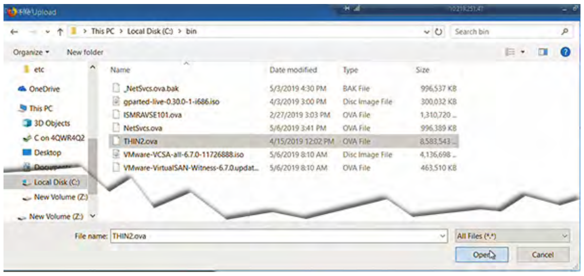
● Local file

Browse... No files selected.

Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

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

   Click Open.



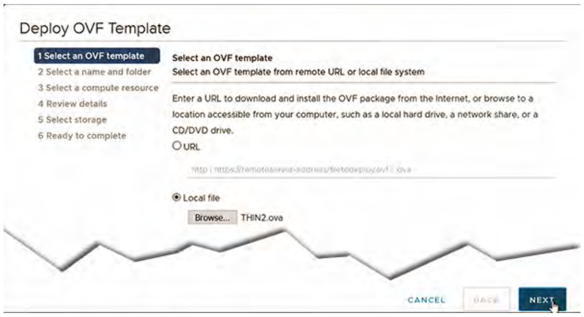
Name	Date modified	Type	Size
_NetSvcs.ova.bak	5/3/2019 4:30 PM	BAK File	996,537 KB
gparted-live-0.30.0-1-i686.iso	4/3/2019 3:00 PM	Disc Image File	300,032 KB
ISMRAVSE101.ova	2/27/2019 3:03 PM	OVA File	1,310,720 ...
NetSvcs.ova	5/6/2019 3:41 PM	OVA File	996,389 KB
THIN2.ova	4/15/2019 12:02 PM	OVA File	8,583,543 ...
VMware-VCSA-all-6.7.0-11726888.iso	5/6/2019 8:10 AM	Disc Image File	4,136,698 ...
VMware-VirtualSAN-Witness-6.7.0.updat...	5/6/2019 8:10 AM	OVA File	463,510 KB

File name: THIN2.ova

All Files (*.*)

5. The OVA file that you chose appears next to the Browse button.

   Click Next.



Deploy OVF Template

Select an OVF template

Select an OVF template from remote URL or local file system

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

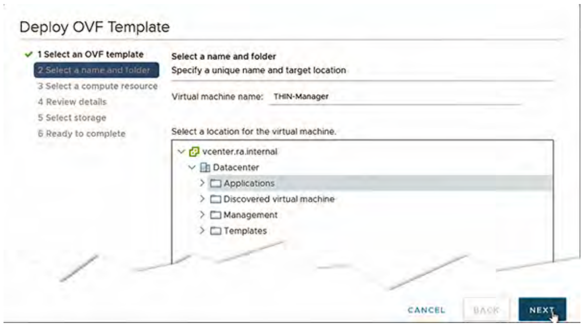
○ URL

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

● Local file

Browse... THIN2.ova

6. 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.



Deploy OVF Template

Select a name and folder

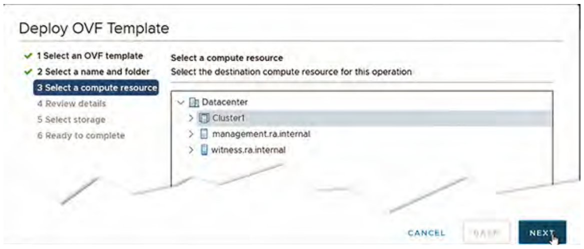
Specify a unique name and target location

Virtual machine name: THIN-Manager

Select a location for the virtual machine.

7. On step 3, select the resource for this operation.

   Click Next.



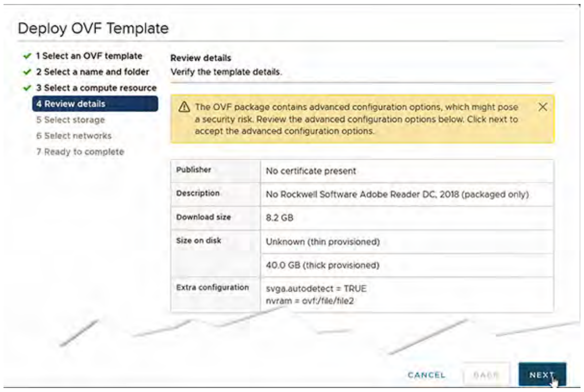
Deploy OVF Template

Select a compute resource

Select the destination compute resource for this operation

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

   Click Next.



Review details

Verify the template details.

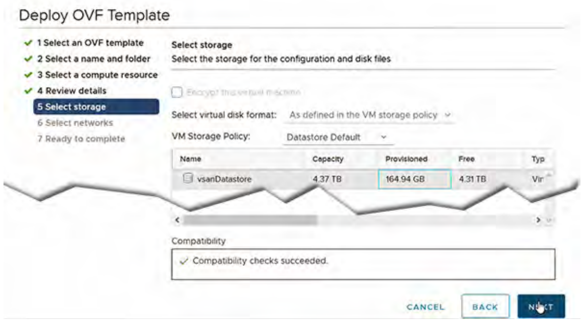
⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Description	No Rockwell Software Adobe Reader DC, 2018 (packaged only)
Download size	8.2 GB
Size on disk	Unknown (thin provisioned)
	40.0 GB (thick provisioned)

Extra configuration	svga.autodetect = TRUE
	nvram = ovf:/file/file2

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

   Click Next.



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine

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

VM Storage Policy: Datastore Default

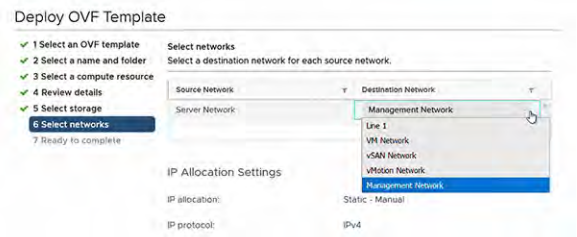
Name	Capacity	Provisioned	Free	Typ
vsanDatastore	4.37 TB	164.94 GB	4.31 TB	Vir

Compatibility

✓ Compatibility checks succeeded.

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

    Click Next.



Select networks

Select a destination network for each source network.

Source Network	Destination Network
Server Network	Management Network

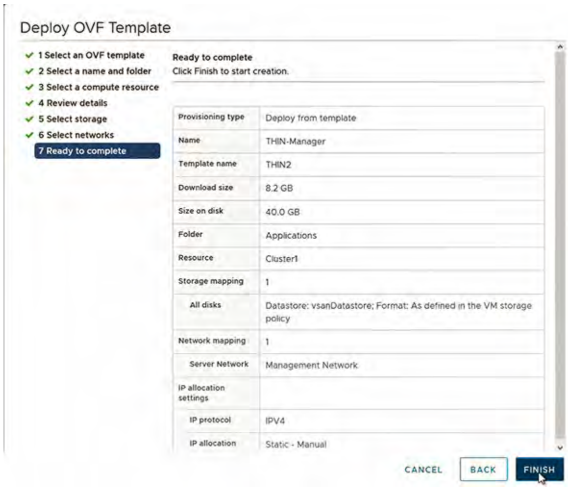
IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

11. 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.



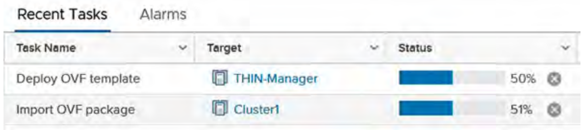
Deploy OVF Template

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

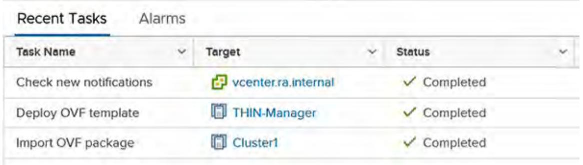
Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	THIN-Manager
Template name	THIN2
Download size	8.2 GB
Size on disk	40.0 GB
Folder	Applications
Resource	Cluster1
Storage mapping	1
All disks	Datastore: vsanDatastore; Format: As defined in the VM storage policy
Network mapping	1
Server Network	Management Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

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



Task Name	Target	Status
Deploy OVF template	THIN-Manager	50%
Import OVF package	Cluster1	51%

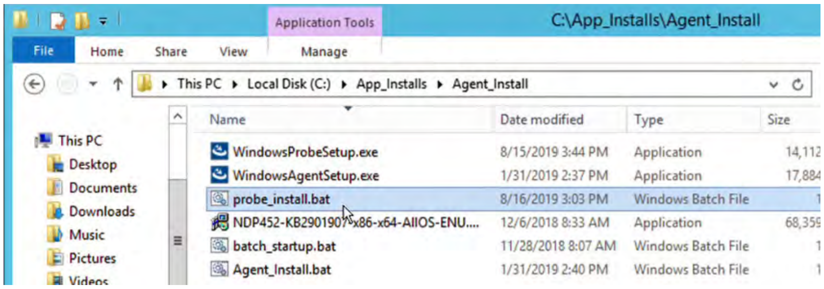


Task Name	Target	Status
Check new notifications	vcenter.ra.internal	✓ Completed
Deploy OVF template	THIN-Manager	✓ Completed
Import OVF package	Cluster1	✓ Completed

Install VSE Software

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

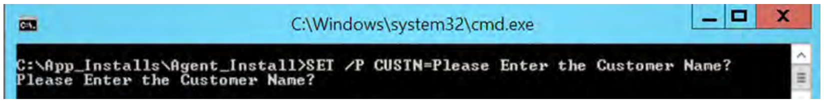
1. To access this software, follow step1…step 4 in Support on page 84.
2. Open Windows Explorer.
3. Navigate to C:\App_Installs\Agent_Install.
4. Locate the probe_install.bat file and double-click it.



Name	Date modified	Type	Size
WindowsProbeSetup.exe	8/15/2019 3:44 PM	Application	14,112
WindowsAgentSetup.exe	1/31/2019 2:37 PM	Application	17,884
probe_install.bat	8/16/2019 3:03 PM	Windows Batch File	1
NDP452-KB2901907-x86-x64-AllOS-ENU....	12/6/2018 8:33 AM	Application	68,359
batch_startup.bat	11/28/2018 8:07 AM	Windows Batch File	1
Agent_Install.bat	1/31/2019 2:40 PM	Windows Batch File	1

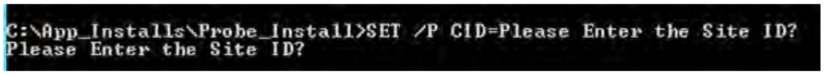
The batch file opens in the Windows Command Prompt program.

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



```
C:\App_Installs\Agent_Install>SET /P CUSTN=Please Enter the Customer Name?
Please Enter the Customer Name?
```

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

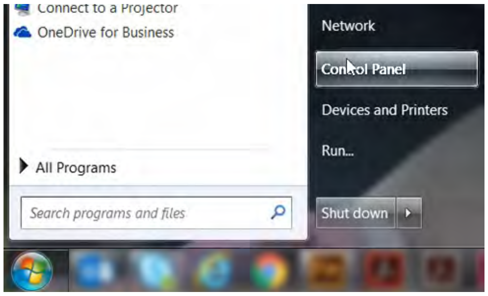


```
C:\App_Installs\Probe_Install>SET /P CID=Please Enter the Site ID?
Please Enter the Site ID?
```

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

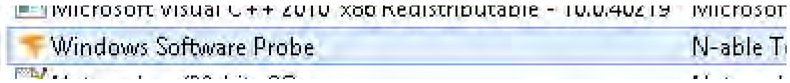
7. Verify that the installation was successful.

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.


Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 Microsof
Windows Software Probe N-able T

d. Close the window.

Chapter 5

System Shutdown and Startup

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.

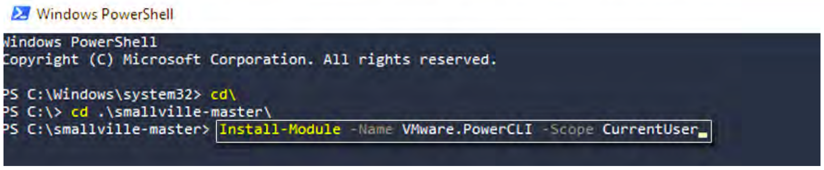
1. Download the latest shutdown script from the Rockwell Automation Knowledgebase site at https://www.rockwellautomation.com/en_NA/support/overview.page.

   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
   ```

   ```
   indows PowerShell
   opyright (C) Microsoft Corporation. All rights reserved.

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

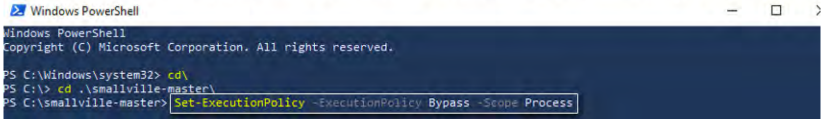
   Press Enter.

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.

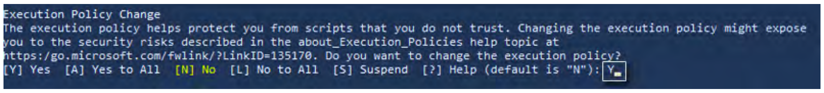
```
Set-Execution Policy  -Execution Policy Bypass  -Scope Process
```



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

PS C:\Windows\system32> cd\
PS C:\> cd .\smallville-master\
PS C:\smallville-master> Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
```

   An Execution Policy Change alert appears.

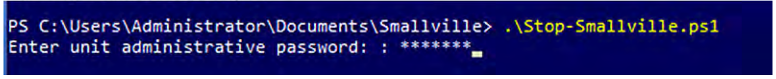
   b. To change the policy, press Y and then press Enter.



```
Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
```

5. At the PowerShell prompt, type the following:

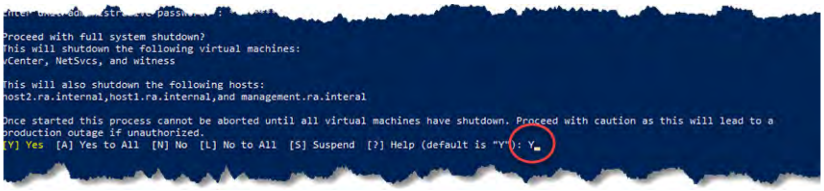
```
.\Stop-Smallville.ps1
```



```
PS C:\Users\Administrator\Documents\Smallville> .\Stop-Smallville.ps1
Enter unit administrative password: : *******
```

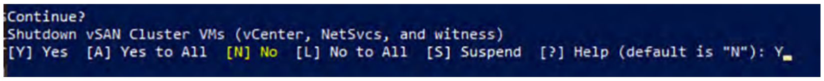
6. When prompted, enter the system-wide password.

7. When asked to proceed, type Y for Yes.



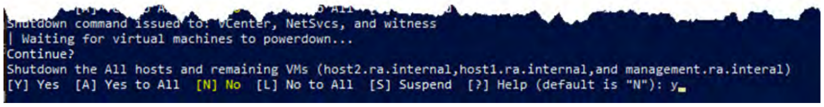
```
Enter unit administrative password : 

Proceed with full system shutdown?
This will shutdown the following virtual machines:
vCenter, NetSvcs, and witness

This will also shutdown the following hosts:
host2.ra.internal,host1.ra.internal,and management.ra.interal

Once started this process cannot be aborted until all virtual machines have shutdown. Proceed with caution as this will lead to a
production outage if unauthorized.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

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



```
Continue?
Shutdown vSAN Cluster VMs (vCenter, NetSvcs, and witness)
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
```

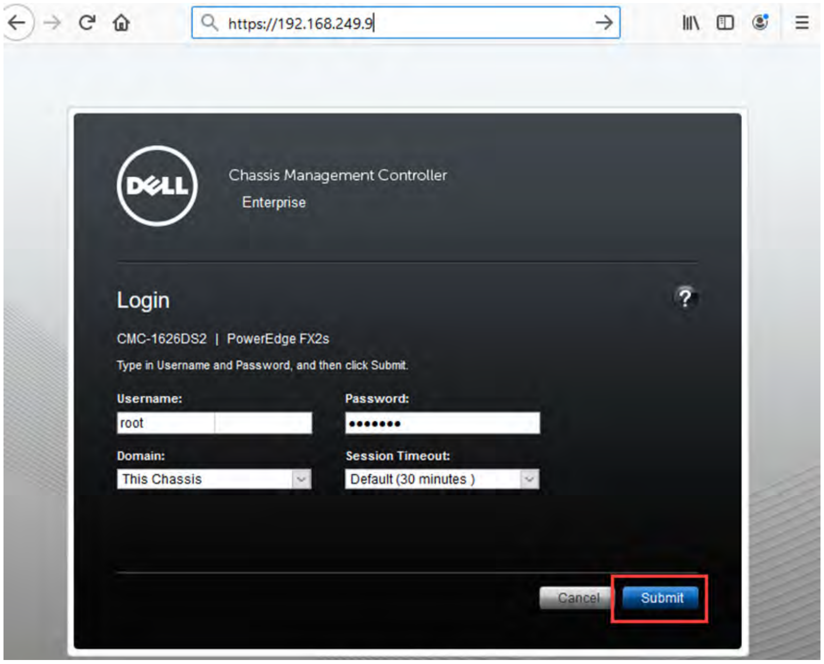
9. When prompted again to continue, type Y for Yes.



```
Shutdown command issued to: vCenter, NetSvcs, and witness
| Waiting for virtual machines to powerdown...
Continue?
Shutdown the All hosts and remaining VMs (host2.ra.internal,host1.ra.internal,and management.ra.interal)
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
```

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.



https://192.168.249.9

Chassis Management Controller
Enterprise

Login

CMC-1626DS2 | PowerEdge FX2s

Type in Username and Password, and then click Submit.

Username: root

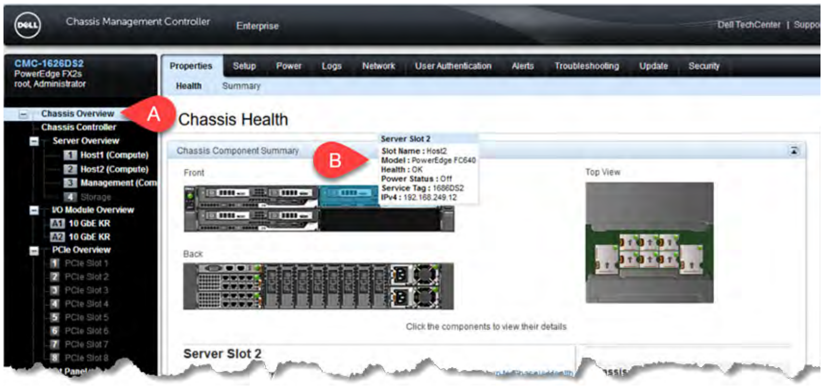
Password: •••••••

Domain: This Chassis

Session Timeout: Default (30 minutes)

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.



Chassis Health

Server Slot 2
Slot Name : Host2
Model : PowerEdge FC640
Health : OK
Power Status : Off
Service Tag : 1686DS2
IPv4 : 192.168.249.12

Click the components to view their details

Server Slot 2

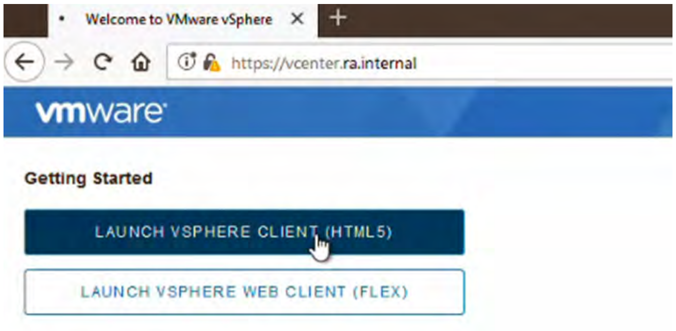
All virtual machines and hosts shut down.

Manual Shutdown

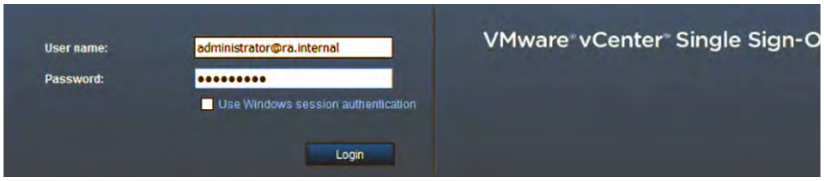
To shut down the VersaVirtual Appliance, perform the following steps.

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).


Welcome to VMware vSphere
https://vcenter.ra.internal
vmware
Getting Started
LAUNCH VSPHERE CLIENT (HTML5)
LAUNCH VSPHERE WEB CLIENT (FLEX)

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

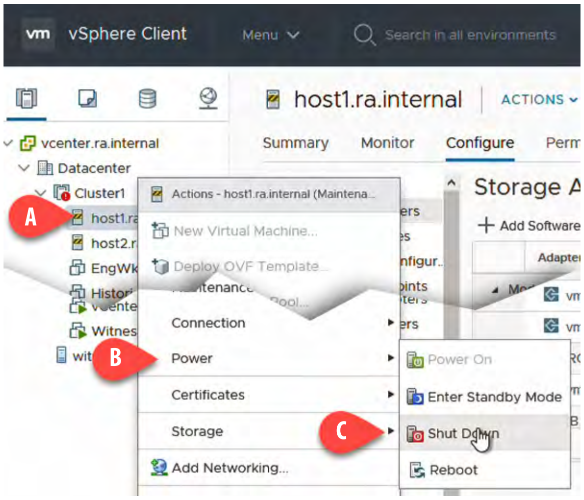


User name: administrator@ra.internal

Password: •••••••••

□ Use Windows session authentication

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).



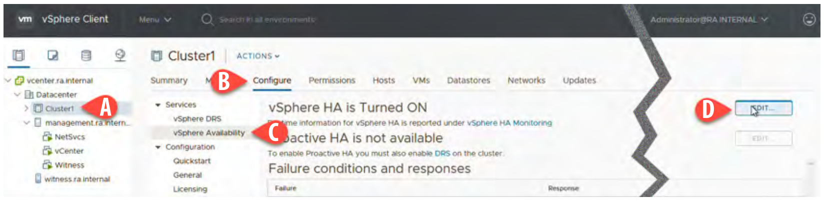
8. Repeat steps 6 and 7 for each virtual machine that is part of Cluster1.

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).



vSphere HA is Turned ON

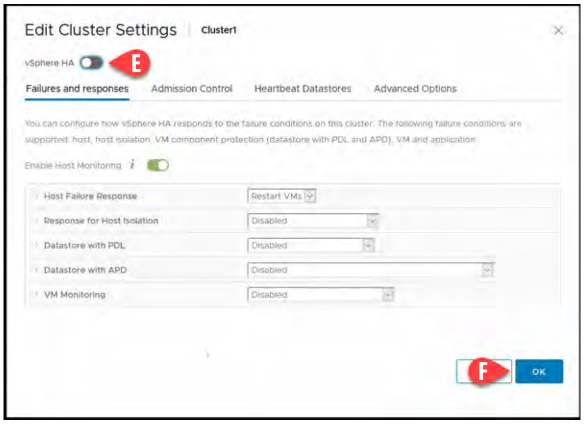
...time information for vSphere HA is reported under vSphere HA Monitoring

...active HA is not available

To enable Proactive HA you must also enable DRS on the cluster.

Failure conditions and responses

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



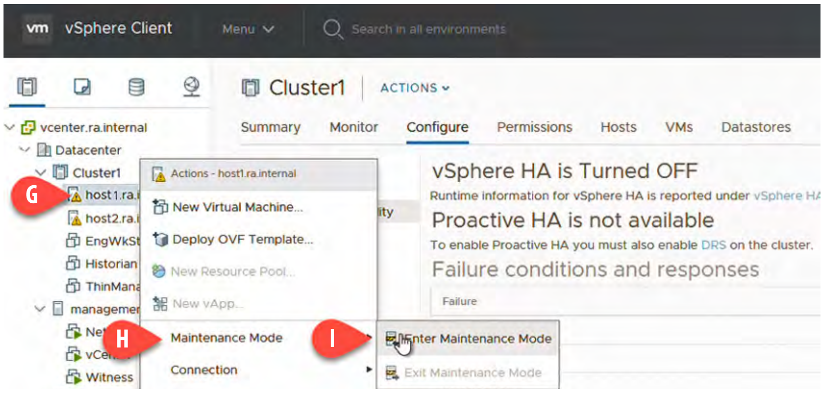
You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	Disabled

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).



vSphere HA is Turned OFF

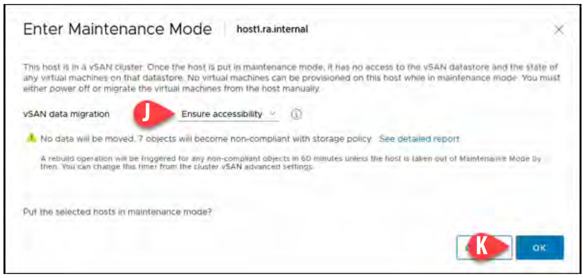
Runtime information for vSphere HA is reported under vSphere HA

Proactive HA is not available

To enable Proactive HA you must also enable DRS on the cluster.

Failure conditions and responses

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



Enter Maintenance Mode | host1.ra.internal

This host is in a vSAN cluster. Once the host is put in maintenance mode, it has no access to the vSAN datastore and the state of any virtual machines on that datastore. No virtual machines can be provisioned on this host while in maintenance mode. You must either power off or migrate the virtual machines from the host manually.

vSAN data migration: Ensure accessibility

No data will be moved. 7 objects will become non-compliant with storage policy. See detailed report

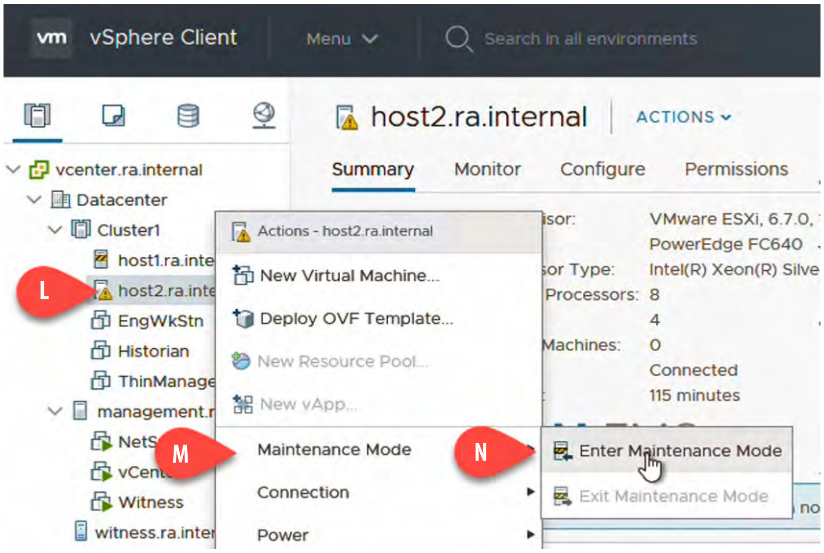
A rebuild operation will be triggered for any non-compliant objects in 60 minutes unless the host is taken out of Maintenance Mode by then. You can change this timer from the cluster vSAN advanced settings.

Put the selected hosts in maintenance mode?

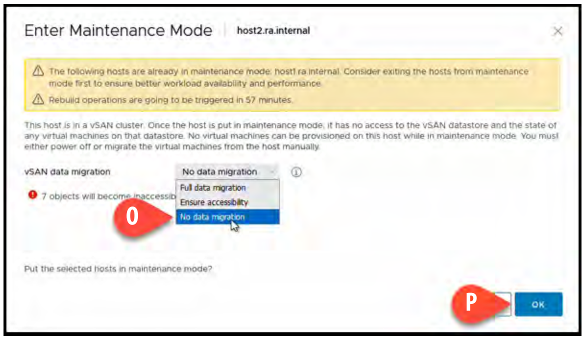
Click OK (K).

8. 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).



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



Enter Maintenance Mode | host2.ra.internal

The following hosts are already in maintenance mode: host1.ra.internal. Consider exiting the hosts from maintenance mode first to ensure better workload availability and performance.

Rebuild operations are going to be triggered in 57 minutes.

This host is in a vSAN cluster. Once the host is put in maintenance mode, it has no access to the vSAN datastore and the state of any virtual machines on that datastore. No virtual machines can be provisioned on this host while in maintenance mode. You must either power off or migrate the virtual machines from the host manually.

vSAN data migration: No data migration

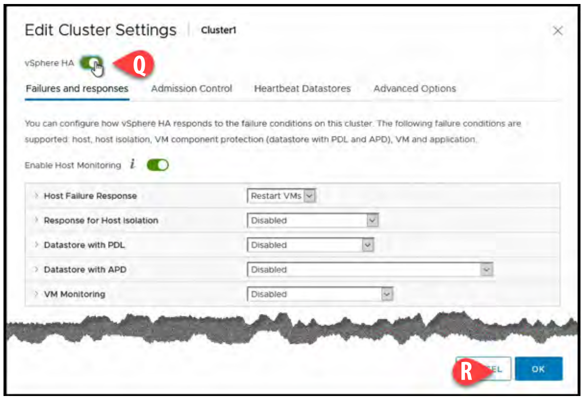
7 objects will become inaccessib

Put the selected hosts in maintenance mode?

Click OK (P).

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

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



You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

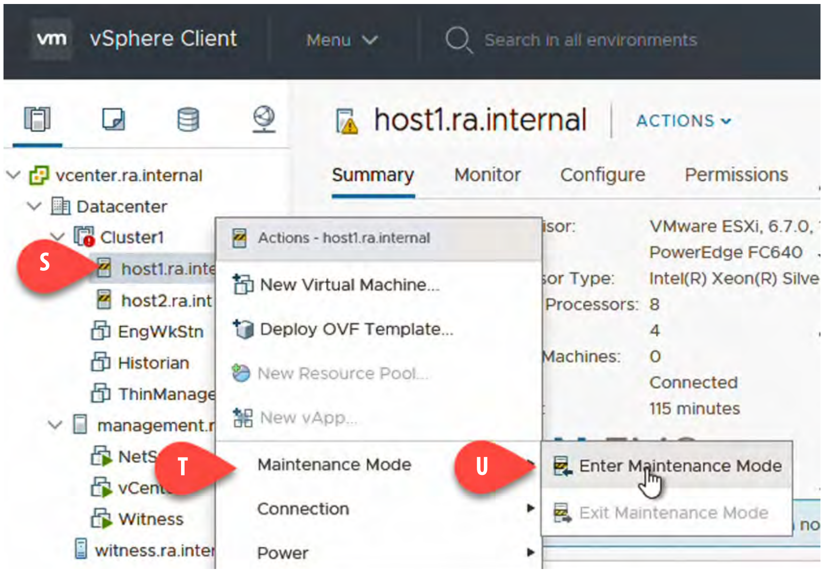
Enable Host Monitoring

Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Disabled
Datastore with APD	Disabled
VM Monitoring	Disabled

Click OK (R).

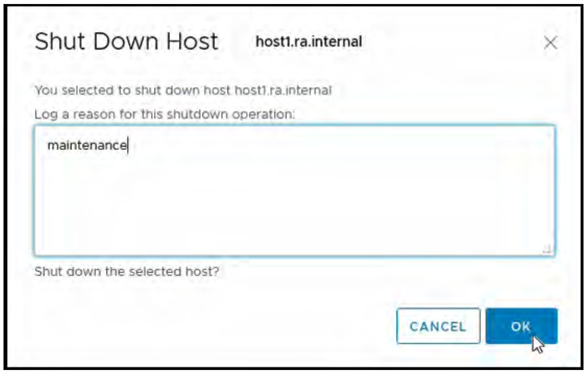
12. Under the expanded Cluster1 hierarchy of the main navigation pane, right-click host1.ra.internal (S).

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



isor: VMware ESXi, 6.7.0,
PowerEdge FC640
sor Type: Intel(R) Xeon(R) Silve
Processors: 8
4
Machines: 0
Connected
115 minutes

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



Shut Down Host host1.ra.internal

You selected to shut down host host1.ra.internal

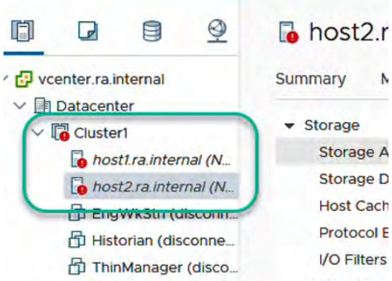
Log a reason for this shutdown operation:

maintenance

Shut down the selected host?

Click OK.

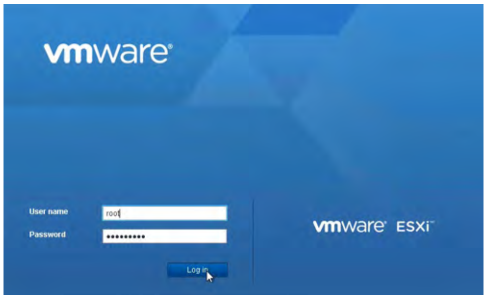
14. Repeat steps 12 and 13 for host2.ra.internal so both hosts are powered off.



Shut Down the vSphere Service Management Host

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

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



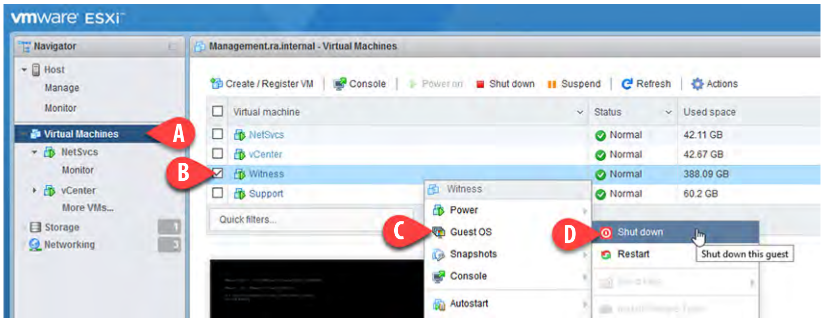
User name root

Password •••••••••

2. Click Login.

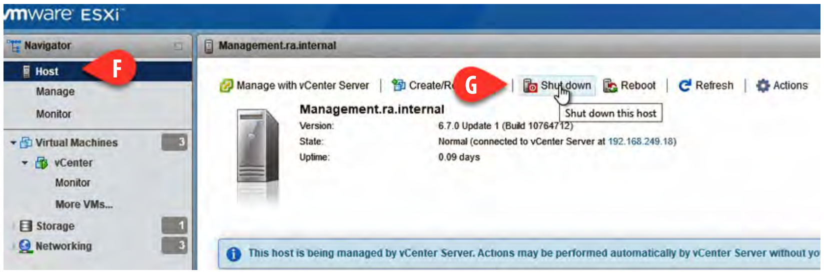
3. Under the main Navigator pane, click Virtual Machines (A).
4. On the Management pane, highlight the virtual machine Witness (B).
5. Right-click Witness.

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



Virtual machine	Status	Used space
NetSvcs	Normal	42.11 GB
vCenter	Normal	42.67 GB
Witness	Normal	388.09 GB
Support	Normal	60.2 GB

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



Management.ra.internal

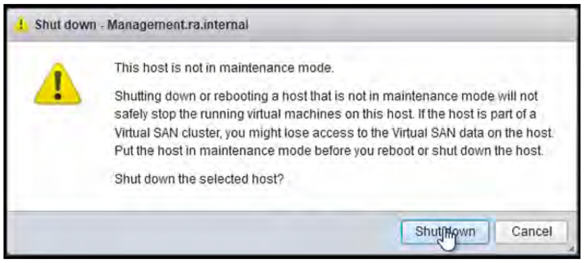
Version: 6.7.0 Update 1 (Build 10764712)

State: Normal (connected to vCenter Server at 192.168.249.18)

Uptime: 0.09 days

This host is being managed by vCenter Server. Actions may be performed automatically by vCenter Server without yo

8. A shutdown warning appears. Click Shutdown.



Shut down - Management.ra.internal

This host is not in maintenance mode.

Shutting down or rebooting a host that is not in maintenance mode will not safely stop the running virtual machines on this host. If the host is part of a Virtual SAN cluster, you might lose access to the Virtual SAN data on the host. Put the host in maintenance mode before you reboot or shut down the host.

Shut down the selected host?

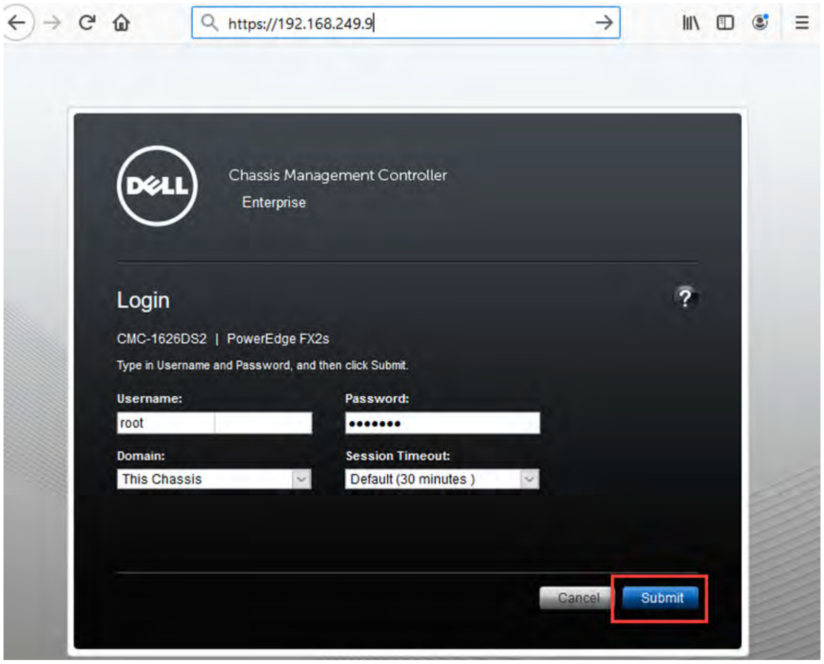
The service management host commences shutting down.

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.



Login

CMC-1626DS2 | PowerEdge FX2s

Type in Username and Password, and then click Submit.

Username: root

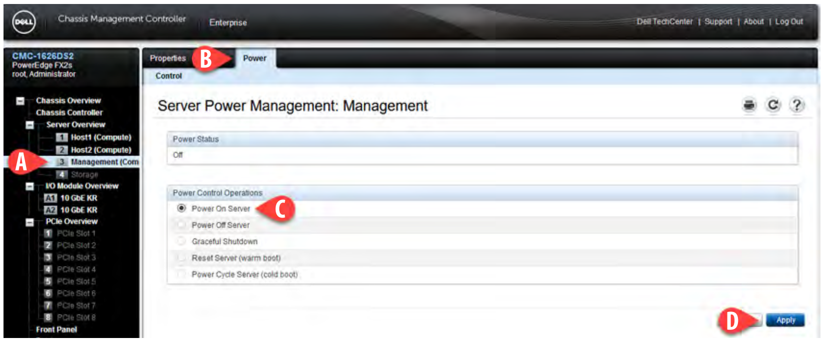
Password: •••••••

Domain: This Chassis

Session Timeout: Default (30 minutes)

   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).



Server Power Management: Management

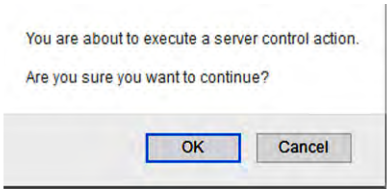
Power Status

Off

Power Control Operations

● Power On Server
○ Power Off Server
○ Graceful Shutdown
○ Reset Server (warm boot)
○ Power Cycle Server (cold boot)

6. An alert appears. Click OK.

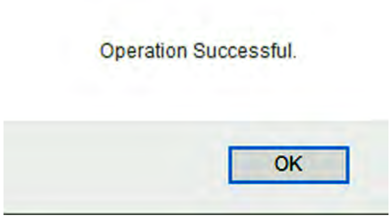


You are about to execute a server control action.

Are you sure you want to continue?

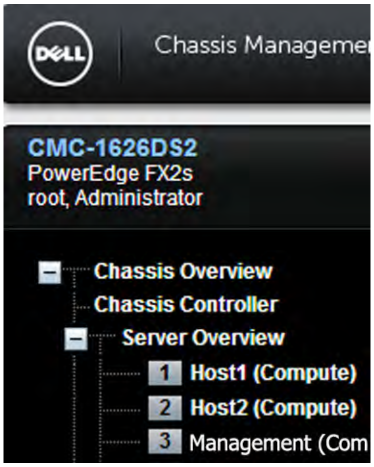
A confirmation appears when completed.

7. Click OK.



Operation Successful.

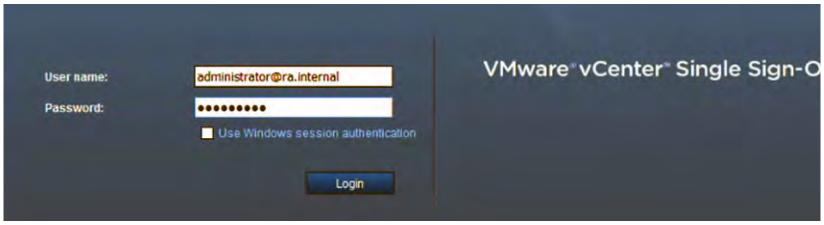
8. Repeat steps 3…7 for Host1 and Host2 under the Navigation pane.



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>



User name: administrator@ra.internal

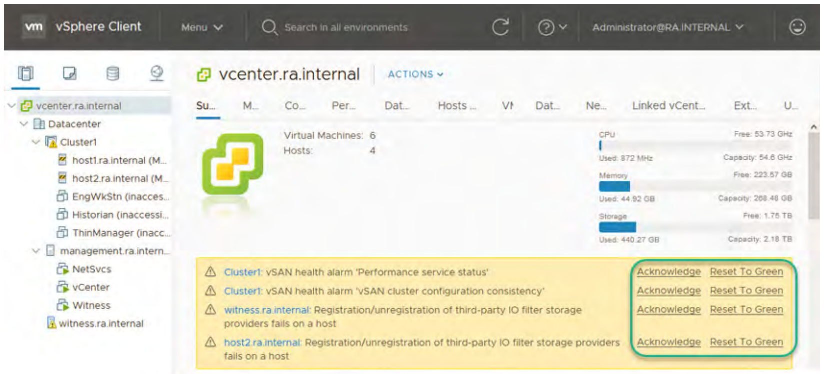
Password: •••••••••

□ Use Windows session authentication
Login
VMware vCenter Single Sign-O

11. Click Login.

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

12. For each warning, click Reset to Green.



Cluster1: vSAN health alarm 'Performance service status' Acknowledge Reset To Green

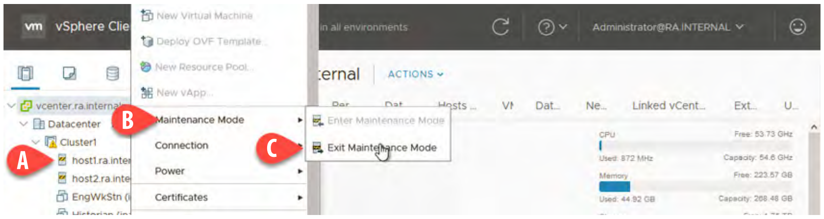
Cluster1: vSAN health alarm 'vSAN cluster configuration consistency' Acknowledge Reset To Green

witness.ra.internal: Registration/unregistration of third-party IO filter storage providers fails on a host Acknowledge Reset To Green

host2.ra.internal: Registration/unregistration of third-party IO filter storage providers fails on a host Acknowledge Reset To Green

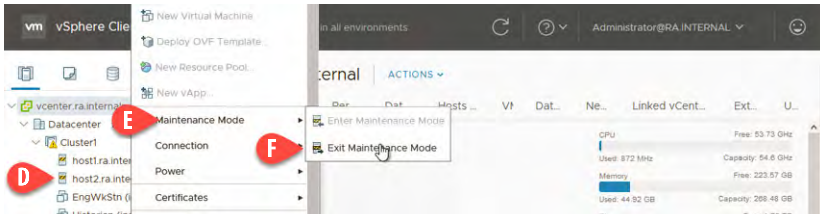
13. On the Navigation pane, click host1 (A).

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).

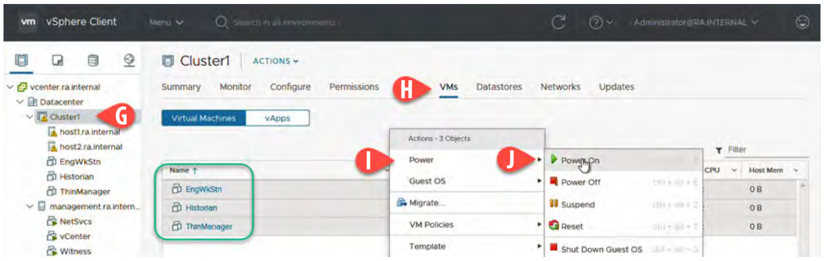


17. On the Navigation pane, click Cluster1 (G).

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-e.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.

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