



HOL-2210-01-SDC
Virtualization 101:
Introduction to vSphere

Table of contents

Lab Overview - HOL-2210-01-SDC - Virtualization 101: Introduction to vSphere	4
Virtualization.....	4
Lab Guidance	15
Module 1 - Introduction to Management with vCenter Server (60 Min)	19
Introduction.....	19
Hands-on Labs Interactive Simulation: ESXi Installation and Configuration.....	19
ESXi Host Client.....	19
vCenter 7 Overview	28
vCenter Server and Creating a Virtual Machine	36
Cloning Virtual Machines and Using Templates	75
Using Tagging and Search to Find Objects Quickly.....	89
Understanding vSphere Availability and Distributed Resource Scheduler (DRS).....	104
vSphere 7 Fault Tolerance Provides Continuous Availability.....	122
Monitoring Events and Creating Alarms.....	124
Configure Shares and Resources.....	145
Migrating Virtual Machines with VMware vMotion	152
vSphere Monitoring and Performance	165
Introduction to vSphere with Tanzu	185
ESXi Install and Configure.....	187
Certification Path	188
Module 2 - Introduction to vSphere Networking and Security (60 Min)...	191
Introduction.....	191
Adding and Configuring vSphere Standard Switch	195
Working with the vSphere Distributed Switch	232
Adding and Configuring a vSphere Distributed Switch.....	283
Using Host Lockdown Mode	326
Configuring the Host Services and Firewall	355
User Access and Authentication Roles.....	356
Understanding Single Sign On	373
Adding an ESXi Host to Active Directory.....	395
Certification Path	406

Module 3 - Introduction to vSphere Storage (60 Min)	409
vSphere Storage Overview	409
Creating and Configuring vSphere Datastores	412
Storage vMotion	461
Managing Virtual Machine Disks.....	471
Working with Virtual Machine Snapshots.....	481
vSphere Datastore Cluster	501
Certification Path	510
Conclusion	513
For More Information.....	513
Appendix	525
Hands-on Labs Interface	525

Lab Overview - HOL-2210-01-SDC - Virtualization 101: Introduction to vSphere

Virtualization

[2]

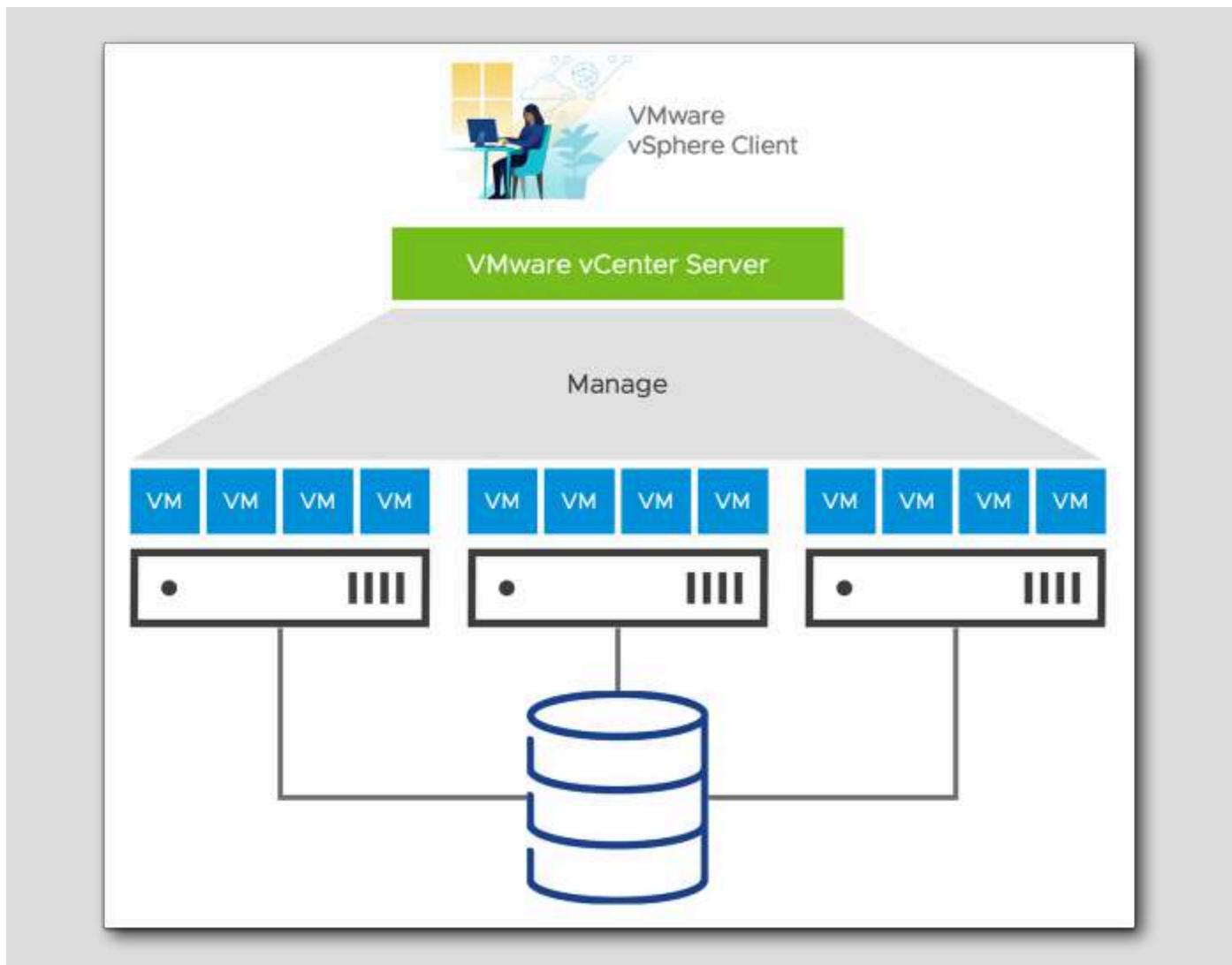
If you are not familiar with Virtualization, this lesson will give you an introduction to it.

If you are familiar with virtualization or have taken this lab previously, you can jump ahead to [Module 1 - Introduction to management with vCenter Server](#).

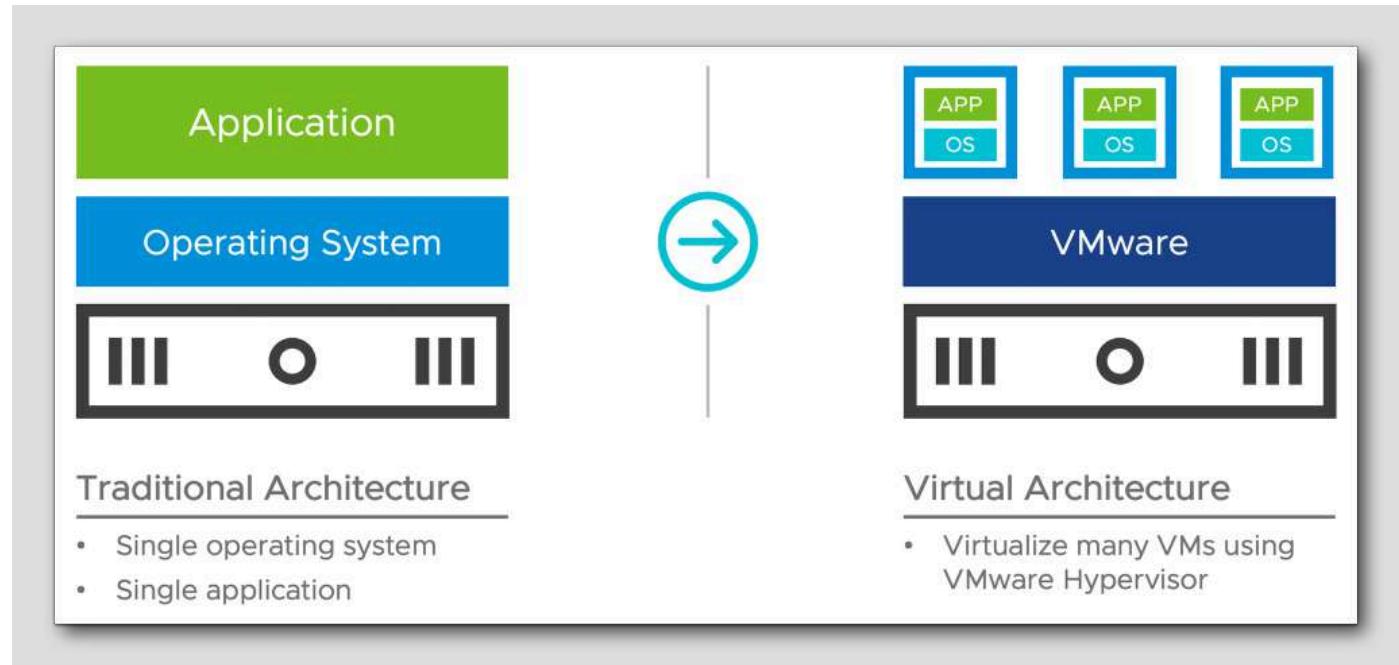
What is Virtualization:

[3]

Today's x86 computer hardware was designed to run a single operating system and a single application, leaving most machines vastly underutilized. Virtualization lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer.



Virtualization Defined

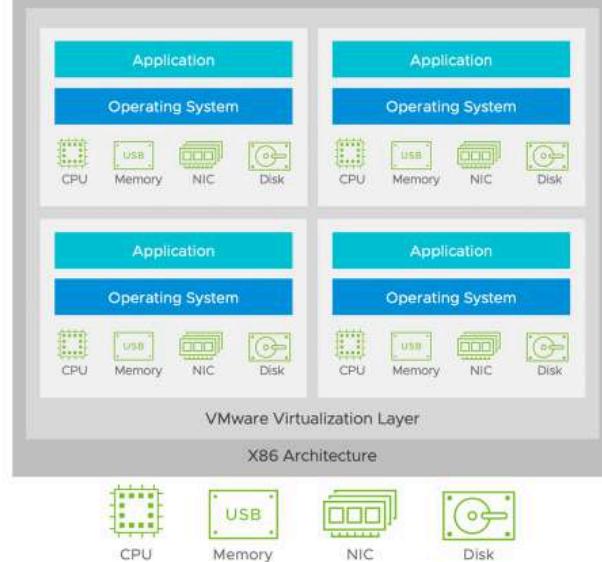


Virtualization is placing an additional layer of software called a hypervisor on top of your physical server. The hypervisor enables you to install multiple operating systems and applications on a single server.

Separation

Server virtualization is separating the OS from the Hardware ...

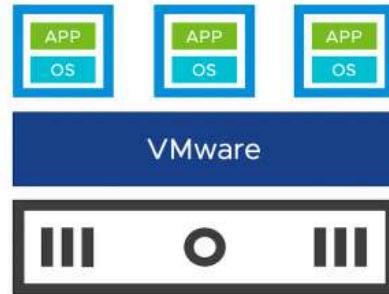
... by presenting a complete x86 platform to the OS



By isolating the operating system from the hardware, you can create a virtualization-based x86 platform. VMware's hypervisor-based virtualization products and solutions provide you the fundamental technology for x86 virtualization.

Partitioning

Key Properties of Virtual Machines



Partitioning

- Run multiple operating systems on one physical machine
- Divide system resources between virtual machines

In this screen, you can see how partitioning helps improve utilization.

Isolation

Isolation

- Fault and security isolation at the hardware level
- Advanced resource controls preserve performance

You can isolate a VM to find and fix bugs and faults without affecting other VMs and operating systems. Once fixed, an entire VM Restore can be performed in minutes.

Encapsulation

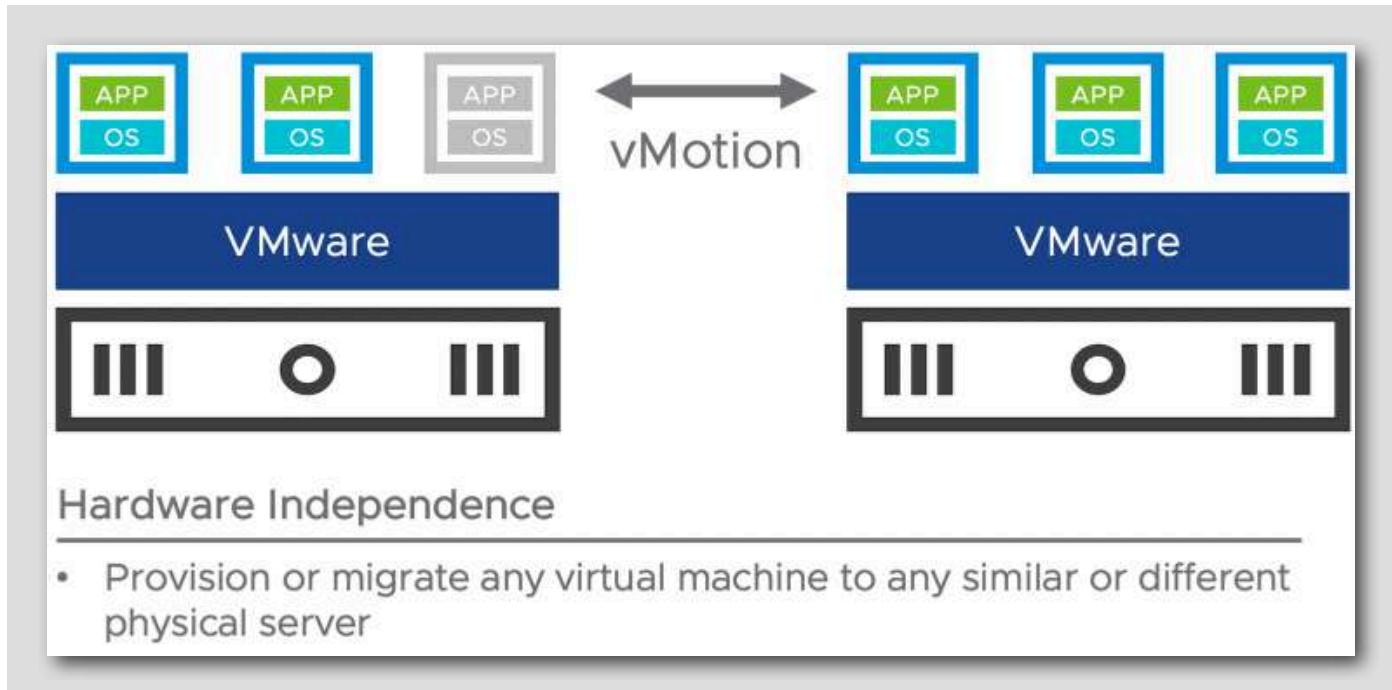


Encapsulation

- Entire state of the virtual machine as a set of files
- Move and copy virtual machines easily

Encapsulation simplifies management by helping you copy, move and restore VMs by treating entire VMs as files.

Hardware Independence



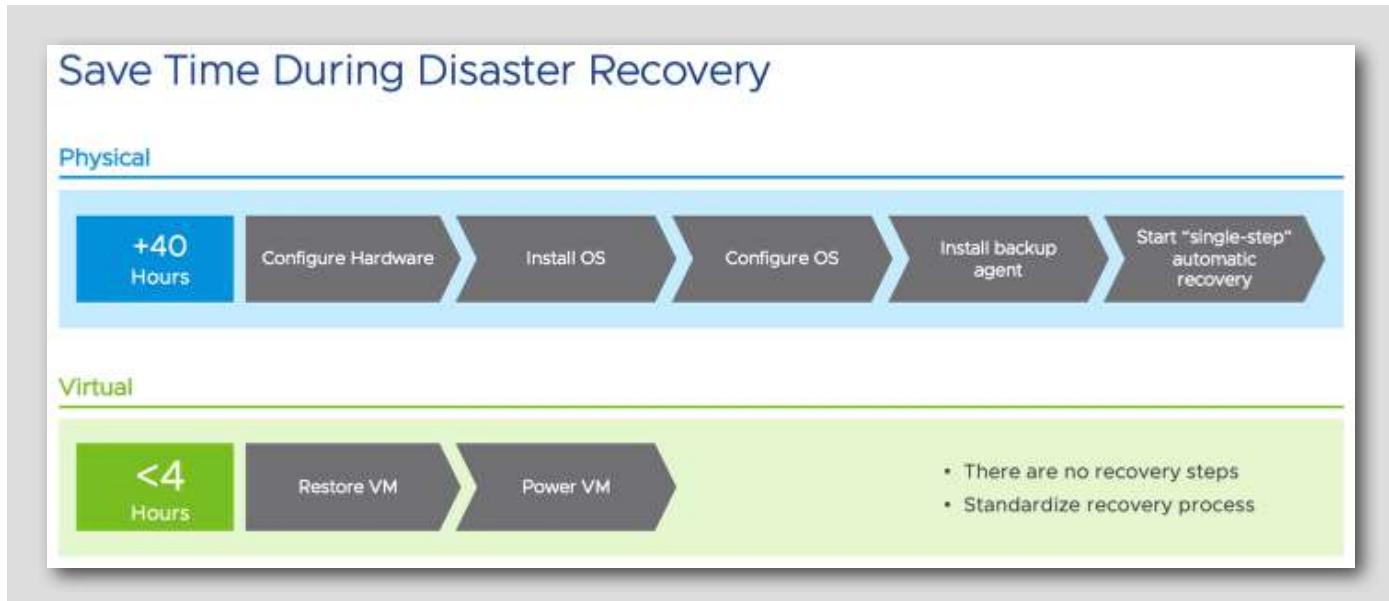
VMs are not dependent on any physical hardware or vendor, making your IT more flexible and scalable.

Benefits

Consolidation		One-time event that moves existing applications onto a fewer number of servers
Containment		An ongoing effort to virtualize new applications and manage growth of existing ones
Availability		Introducing virtualization to increase application availability and data recoverability
There are many more benefits of virtualization		

Virtualization enables you to consolidate servers and contain applications, resulting in high availability and scalability of critical applications.

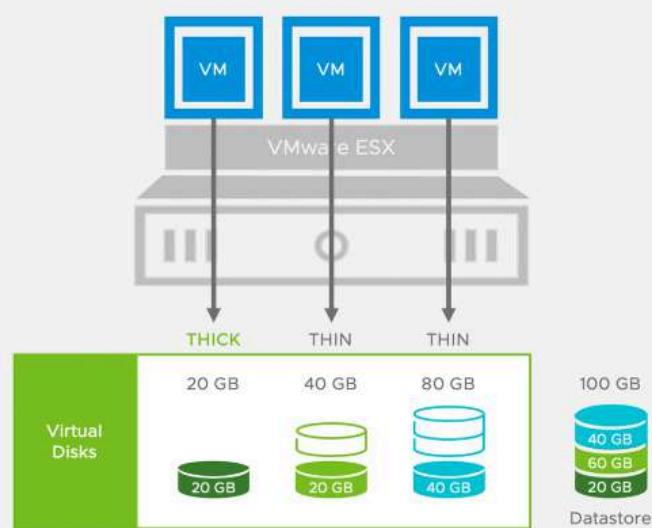
Simplify Recovery



Virtualization eliminates the need for any hardware configuration, OS reinstallation and configuration, or backup agents. A simple restore can recover an entire VM.

Reduce Storage Costs

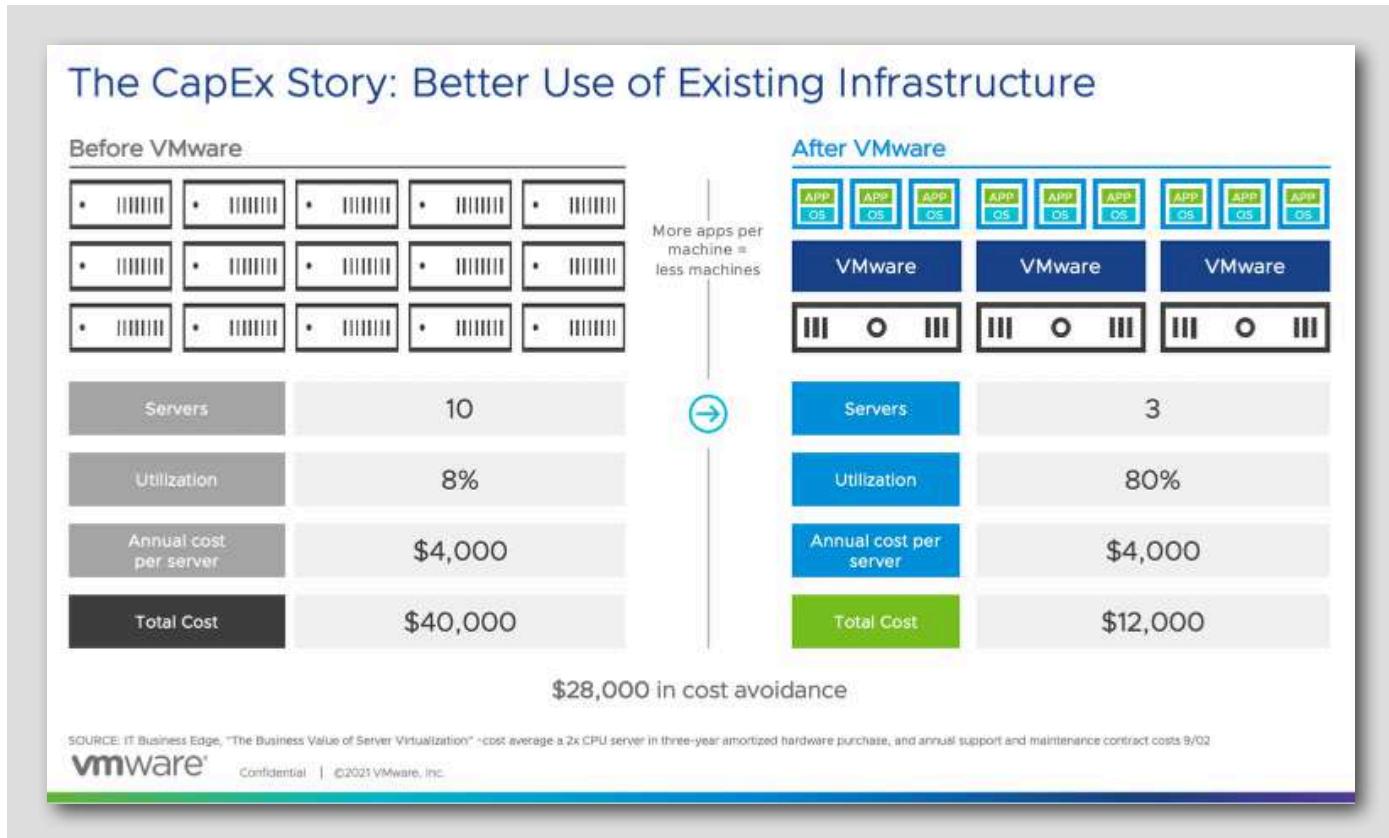
Better Storage Utilization and Efficiency



- Provisioning storage only based on what is needed now and can grow over time
- Drastically save on storage costs

A technology called thin provisioning helps you optimize space utilization and reduce storage costs. It provides storage to VMs when it's needed, and shares space with other VMs.

Cost Avoidance



Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You may only finish 2-3 of the modules during your time. However, you may take this lab as many times as you want. The modules are independent of each other so you can start at the beginning of any module and proceed from there. Use the Table of Contents to access any module in the lab. The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

This introductory lab demonstrates the core features and functions of vSphere and vCenter. This is an excellent place to begin your Virtualization 101 experience.

This lab will walk you through the core features of vSphere and vCenter, including storage and networking. The lab is broken into 3 Modules and the Modules can be taken in any order.

Lab Module List:

- Module 1 - An Introduction to Management with vCenter Server (60 Minutes)
- Module 2 - An Introduction to vSphere Networking and Security (60 Minutes)
- Module 3 - An Introduction to vSphere Storage (60 Minutes)

Each Module will take approximately 60-90 minutes to complete, but based on your experience this could take more or less time.

We have included videos throughout the modules. To get the most out of these videos, it is recommended that you have headphones to hear the audio. The timing of each video is noted next to the title. In some cases, videos are included for tasks we are unable to show in a lab environment, while others are there to provide additional information. Some of these videos may contain an earlier edition of vSphere, however, the steps and concepts are primarily the same.

Lab Captains:

- Doug Baer, Staff Architect, USA
- Dave Rollins, Staff Architect, USA
- Dave Cook, Sr. Technical Marketing Architect USA
- Sandy Visoso, Content Architect, USA
- Milena Chen, Associate Content Architect, Costa Rica

This lab manual can be downloaded from the Hands-on Labs document site found here:

<http://docs.hol.vmware.com>

This lab may be available in other languages. To set your language preference and view a localized manual deployed with your lab, utilize this document to guide you through the process:

<http://docs.hol.vmware.com/announcements/nee-default-language.pdf>

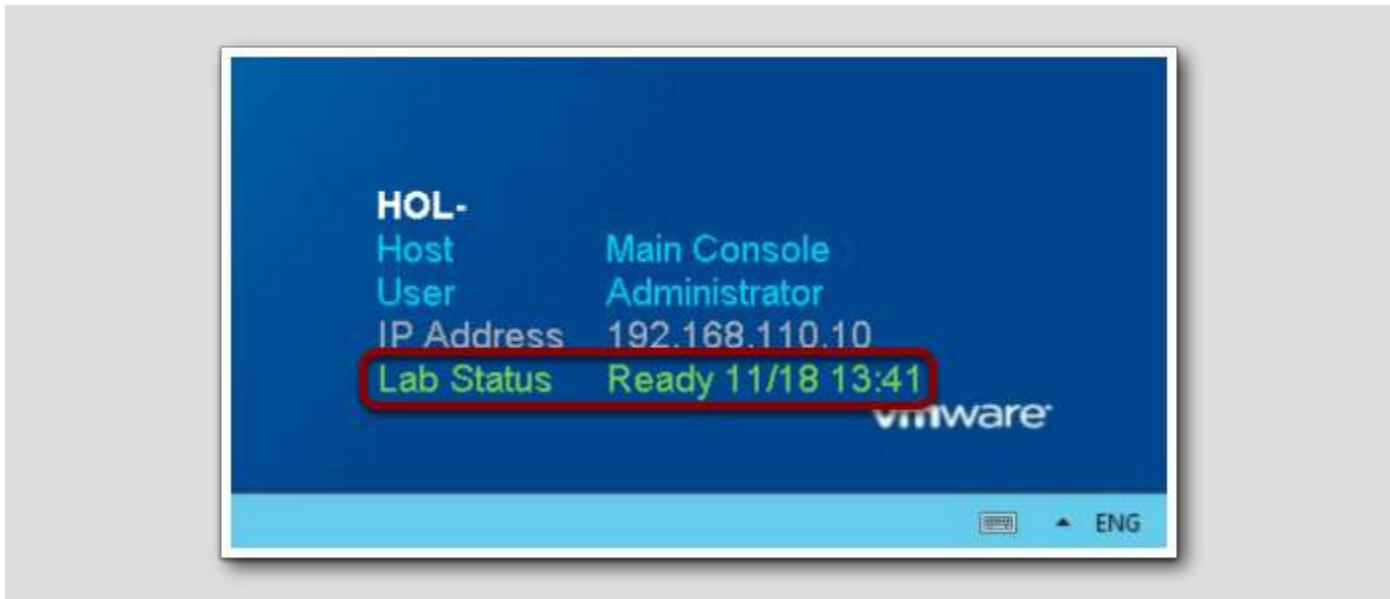
First time using Hands-on Labs?

The screenshot shows the VMware Hands-on Labs interface. At the top, there's a navigation bar with links for HELP, PRIVACY, MY PROFILE, LOG OUT, and ENGLISH. Below the bar, a toolbar includes a timer (28:35), an EXTEND button, and a settings gear icon. A sidebar on the left features a blue and green geometric pattern and a vertical menu with icons for monitor, crosshairs, arrows, and a circular arrow, with 'MANUAL' selected. The main content area has a title 'WELCOME TO THIS DEMO OF AN ON DEMAND COURSE'. Below the title is a welcome message: 'Welcome to this demo of On Demand course. This demo is designed to provide a look at what an On Demand course is like. The demo is of the first 3 Modules of the VMware vSphere: Install, Configure, Manage [6.0] On Demand course. The full course is 12 Modules. At the end of the course you are provided a link if you wish to sign up for any On Demand courses. Enjoy!'. The 'TABLE OF CONTENTS' button in the top right is highlighted with a red circle. There are also 'MORE OPTIONS', page numbers (1, 2, 3, 4, 5, 6, 24), and font size adjustment buttons (A-, A+).

Welcome! If this is your first time taking a lab navigate to the [Appendix](#) in the Table of Contents to review the interface and features before proceeding.

For returning users, feel free to start your lab by clicking next in the manual.

You are ready....is your lab?



Please verify that your lab has finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.

Module 1 - Introduction to Management with vCenter Server (60 Min)

Introduction

[18]

This module will start with an interactive simulation of an ESXi installation. ESXi is the foundation of vSphere and is sometimes referred to as the host. After the installation, the ESXi Host Client will be reviewed. It is a web-based management tool that allows you to manage a single ESXi host at a time.

The remainder of the module will focus on using the vSphere Client to access vCenter Server and manage your entire virtual infrastructure using one interface. Virtual machines will be created, with more details covered on how to manage and monitor the environment. Lastly, you will be introduced to vSphere Platinum, which provides advanced security capabilities in vSphere in combination with VMware AppDefense.

Hands-on Labs Interactive Simulation: ESXi Installation and Configuration

[19]

This part of the lab is presented as a **Hands-on Labs Interactive Simulation**. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.

ESXi Host Client

[20]

The VMware Host Client is an HTML5-based client that is used to connect to and manage single ESXi hosts.

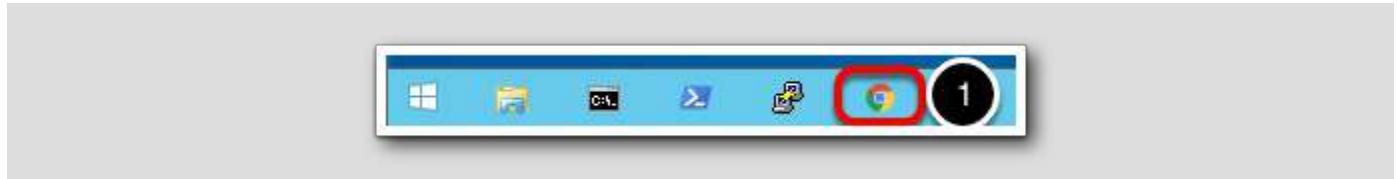
You can use the VMware Host Client to perform administrative and basic troubleshooting tasks, as well as advanced administrative tasks on your target ESXi host. You can also use the VMware Host Client to conduct emergency management when vCenter Server is not available.

It is important to know that the VMware Host Client is different from the vSphere Web Client, regardless of their similar user interfaces. You use the vSphere Web Client to connect to vCenter Server and manage multiple ESXi hosts, whereas you use the VMware Host Client to manage a single ESXi host.

For additional details on the VMware Host Client, please see this PDF (<https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-host-client-1344-guide.pdf>)

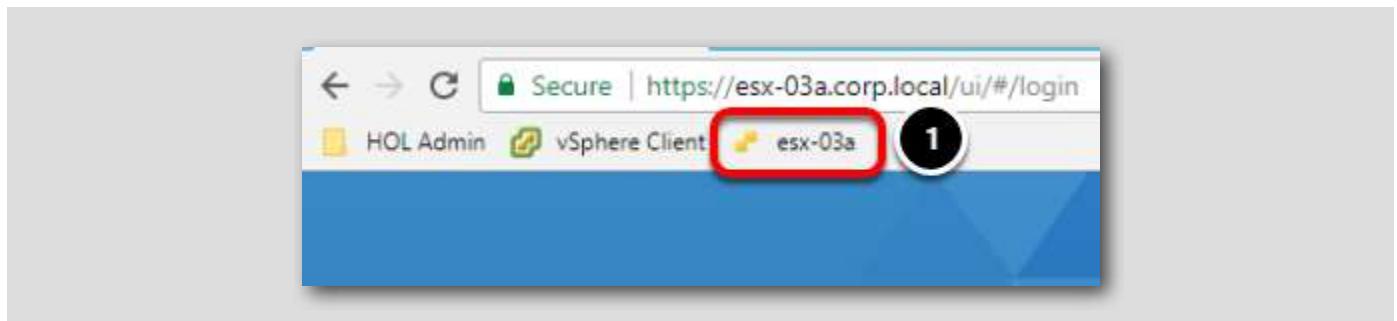
This lesson will walk through some of the most frequently used features in the ESXi Host Client.

Launch Chrome



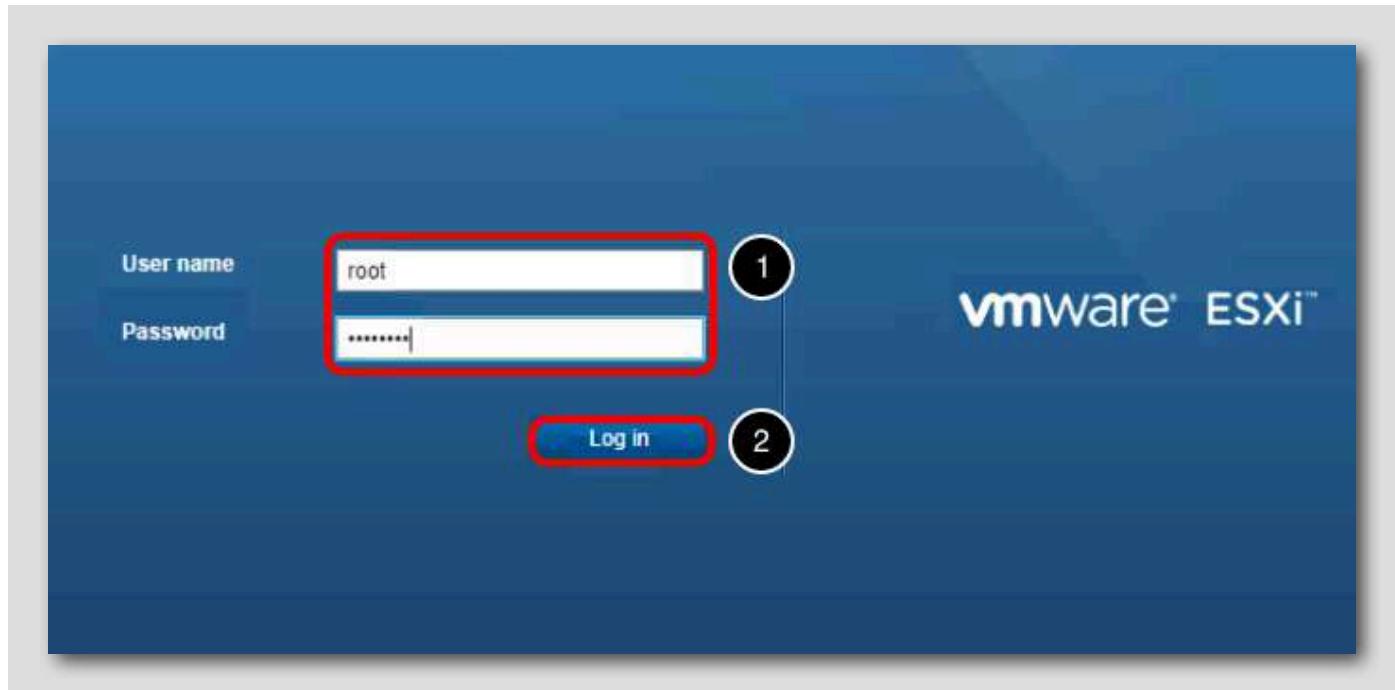
1. Click on the Chrome Icon on the Windows Quick Launch Task Bar

Select esx-03a



1. From the Bookmarks bar, select esx-03a

Login

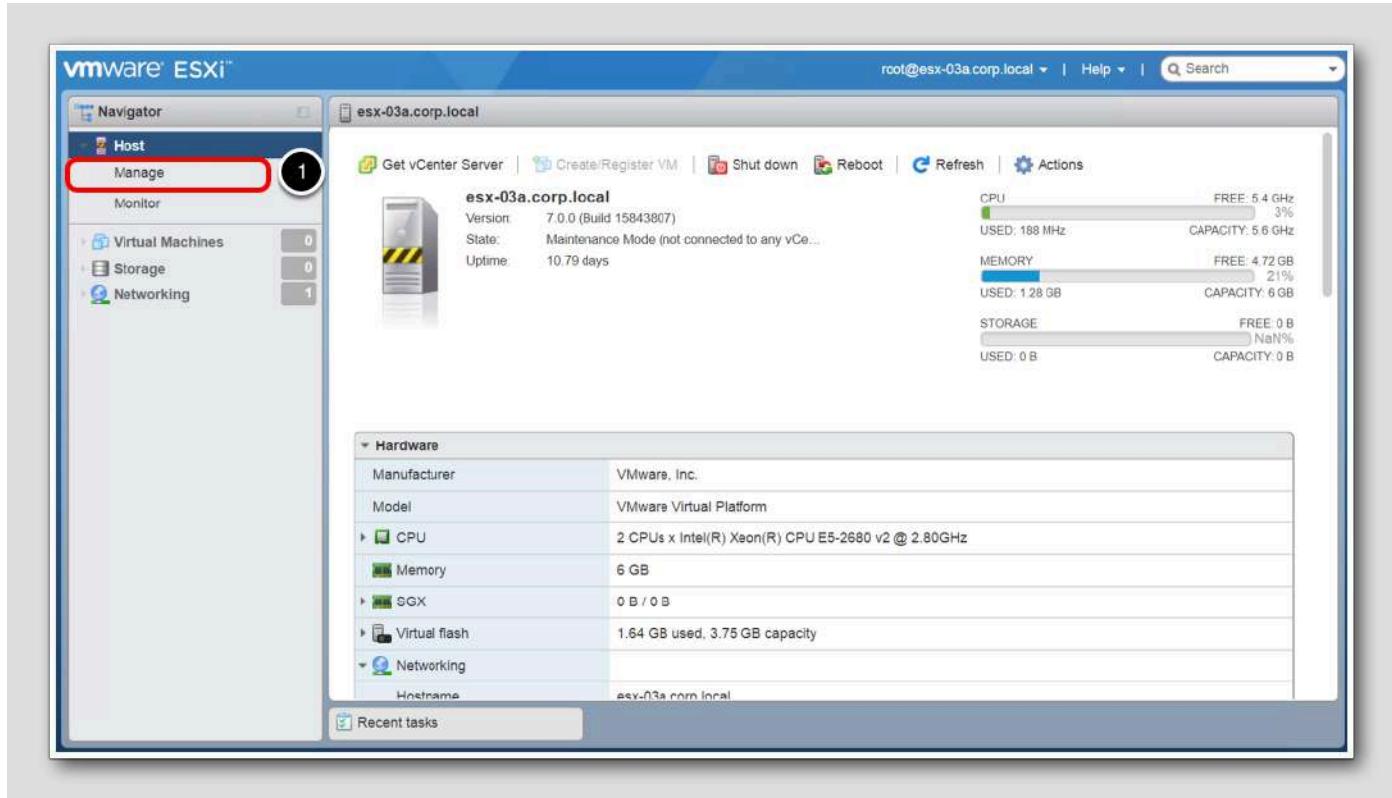


1. Login with the following credentials:

- User name: root
- Password: VMware1!

2. Click the Log in button

ESXi Host Client



The ESXi Host, in this case, **esx-03a**, can now be directly managed. This can be useful in test/dev environments where a vCenter Server is not present or in a production environment where the vCenter Server is not reachable.

The initial screen shows high-level details and recent tasks. There are also various power options for the host and an Actions menu for the most common tasks. Note that the server is currently in Maintenance Mode, which will be discussed in a future lesson. Click to minimize the Recent tasks interface to gain more room.

1. Click on **Manage**

System

Key	Name	Value	Default	Overl...
Annotations.WelcomeMessage	A welcome message in the initial scre...			False
BufferCache.FlushInterval	Flush at this interval (milliseconds)	30000	30000	False
BufferCache.HardMaxDirty	Block writers if this many buffers are ...	95	95	False
BufferCache.ParallelHardMaxDirty	Block writers if this many buffers of a...	50	50	False

1138 items

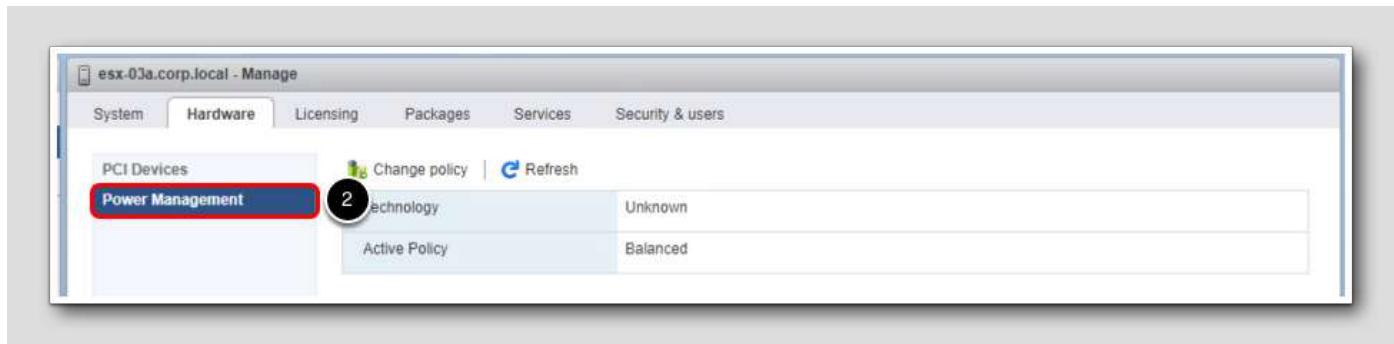
On the System tab, the most common options set here are the date and time for the host. It can be set and synchronized with an NTP server or set manually. In addition, Autostart settings for the host can be configured here as well.

Hardware

Address	Description	SR-IOV	Passth...	Hardw...

45 items

1. Click on the Hardware tab

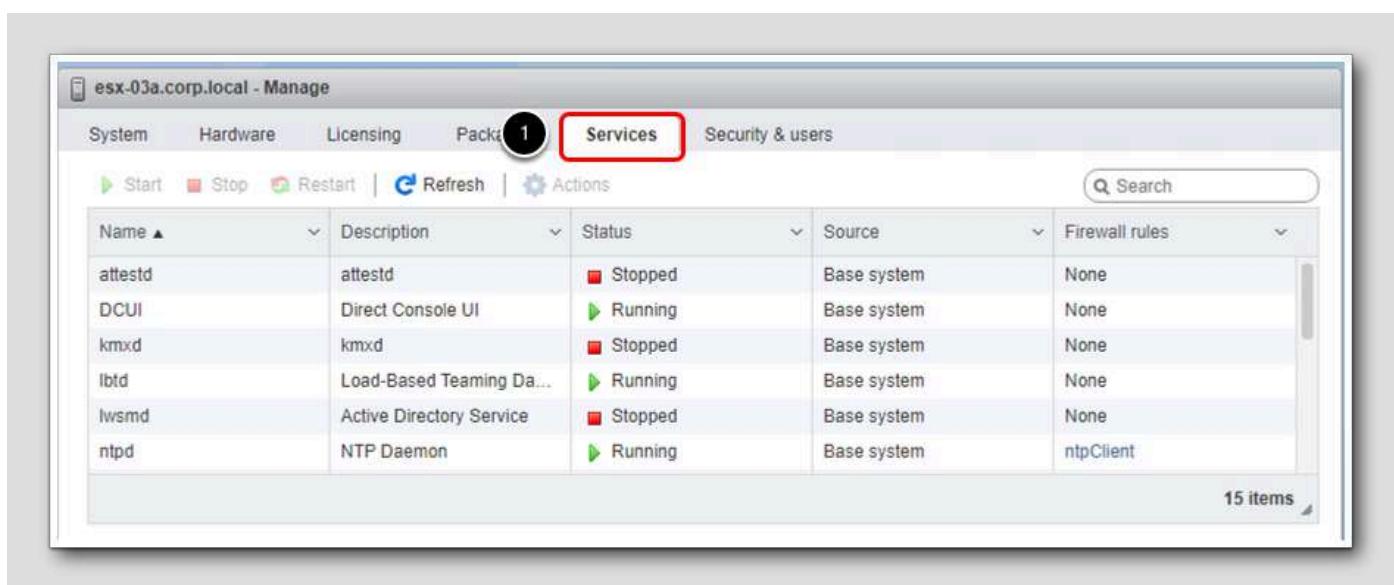


2. Click Power Management

This is where power management policies can be set for the host.

Services

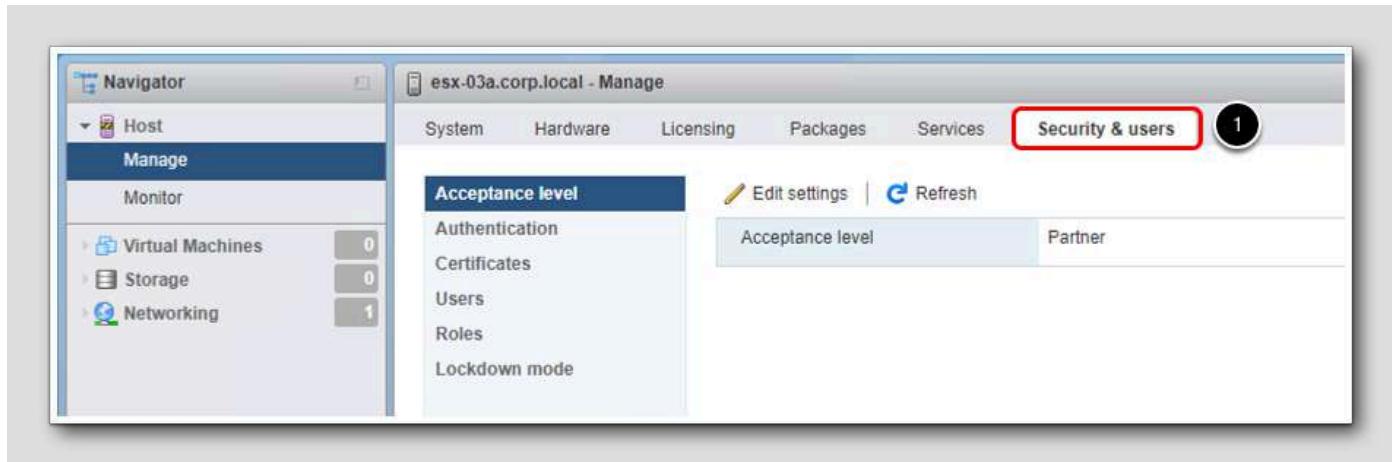
[27]



1. Click the Services tab

Services like SSH access and the Direct Console UI can be stopped and started from this screen.

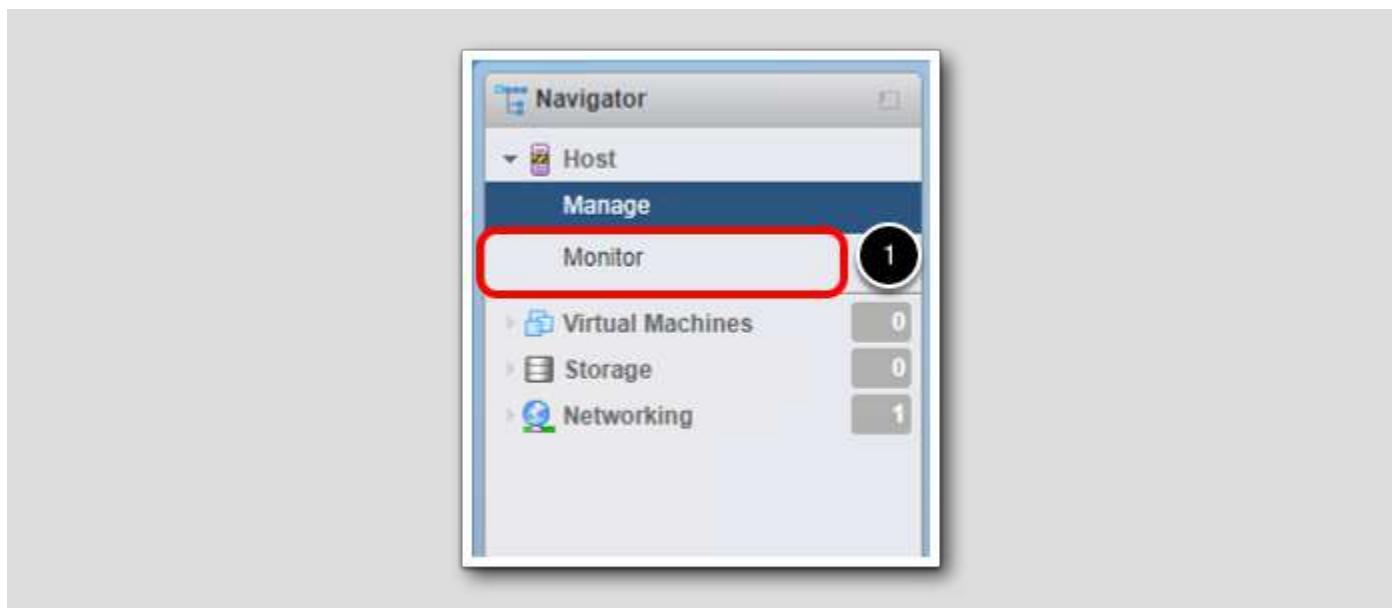
Security and Users



On the Security & Users tab, security options such as authentication to Active Directory and Certificates can be set here. There is also the ability to create additional roles and user accounts for the host itself. This option uses accounts that are local only to the host and not shared with any other hosts or vCenter Server. vCenter Server is set up to use single sign-on which makes account management much easier. This will be reviewed in the lessons that follow.

1. Click on **Security & users**

Monitor



The Monitor section includes Performance Charts, Hardware monitoring, an event log and other useful monitoring information.

1. Click on **Monitor**

Log	Description
/var/log/vpxa.log	vCenter agent log
/var/log/vobd.log	VMware observer daemon log
/var/log/vmkwarning.log	VMkernel warnings log
/var/log/vmkeventd.log	VMkernel event daemon log

1. Click the **Logs** tab

On the Logs tab, a support bundle can be created that includes log files and system information that can be helpful in troubleshooting issues.

Generate Support Bundle

[30]

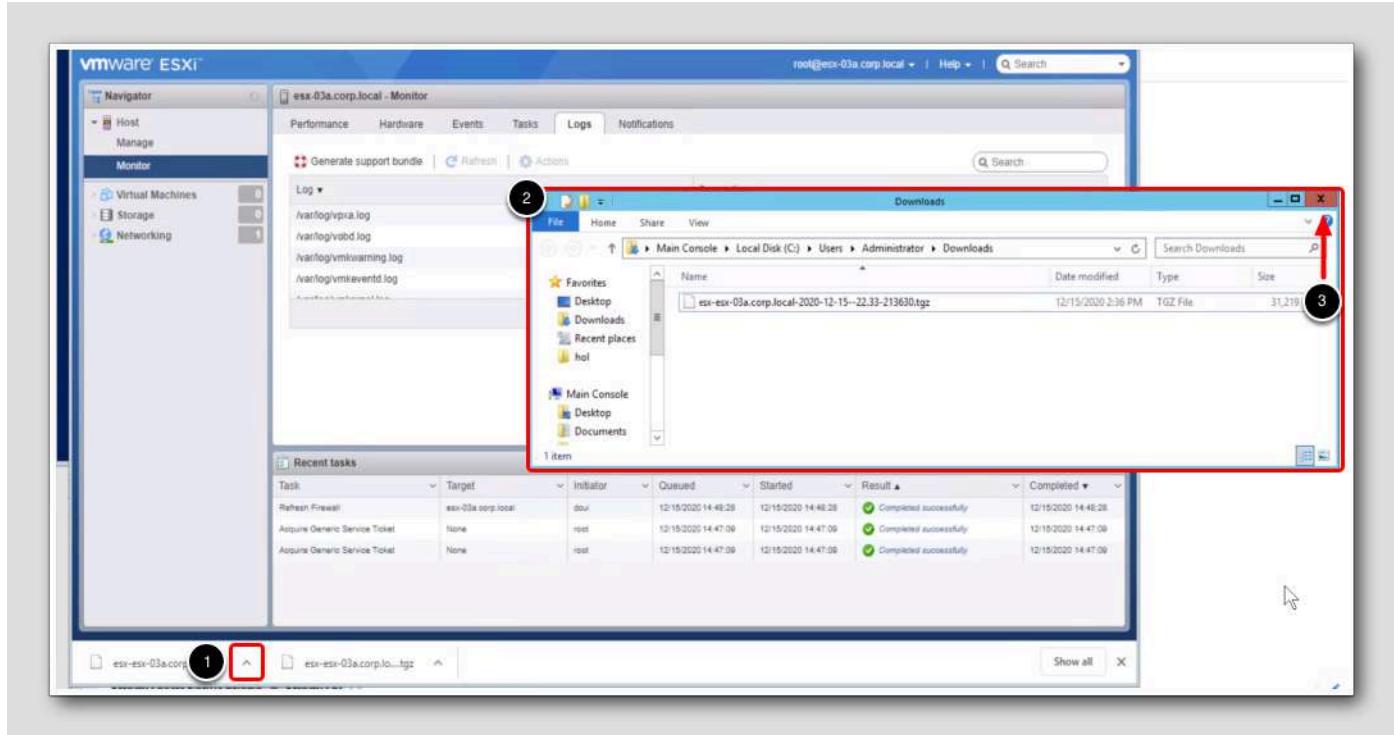
Log	Description
/var/log/vpxa.log	vCenter agent log
/var/log/vobd.log	VMware observer daemon log
/var/log/vmkwarning.log	VMkernel warnings log
/var/log/vmkeventd.log	VMkernel event daemon log

- Click the Generate Support Bundle button

This operation will automatically download the support file. It will take a couple of minutes.

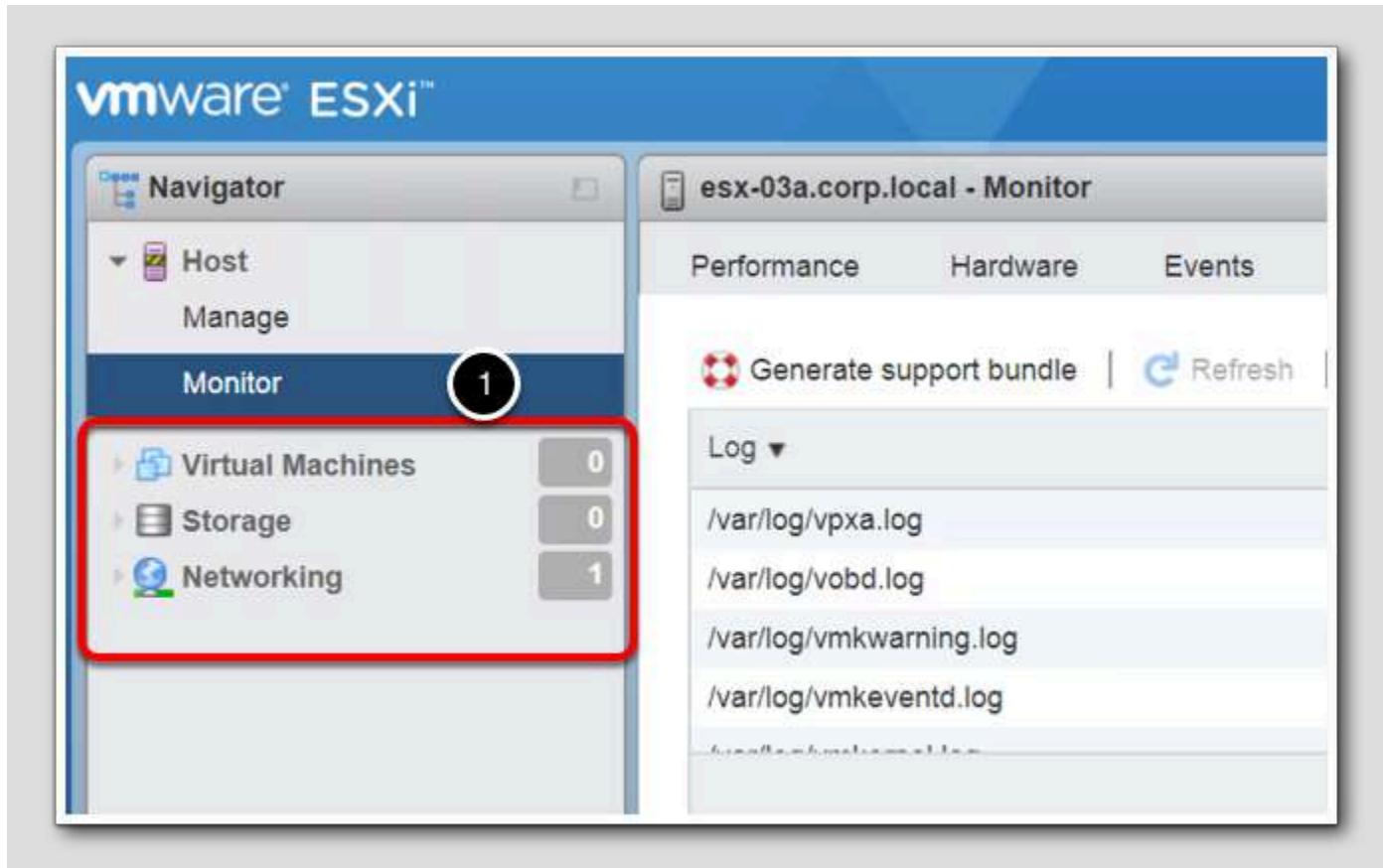
You may be asked to provide credentials. Use the same information you used to log in:

- Username: root
- Password: VMware1!



- Click on the arrow on the downloaded file and select Show in folder.
- A pop-up window will appear with the downloaded support file. Review file if needed.
- Close window when finished.

VMs, Storage and Networking



1. In addition to managing and monitoring the host, Virtual Machines can be created, Storage and Networking can be configured at the host level.

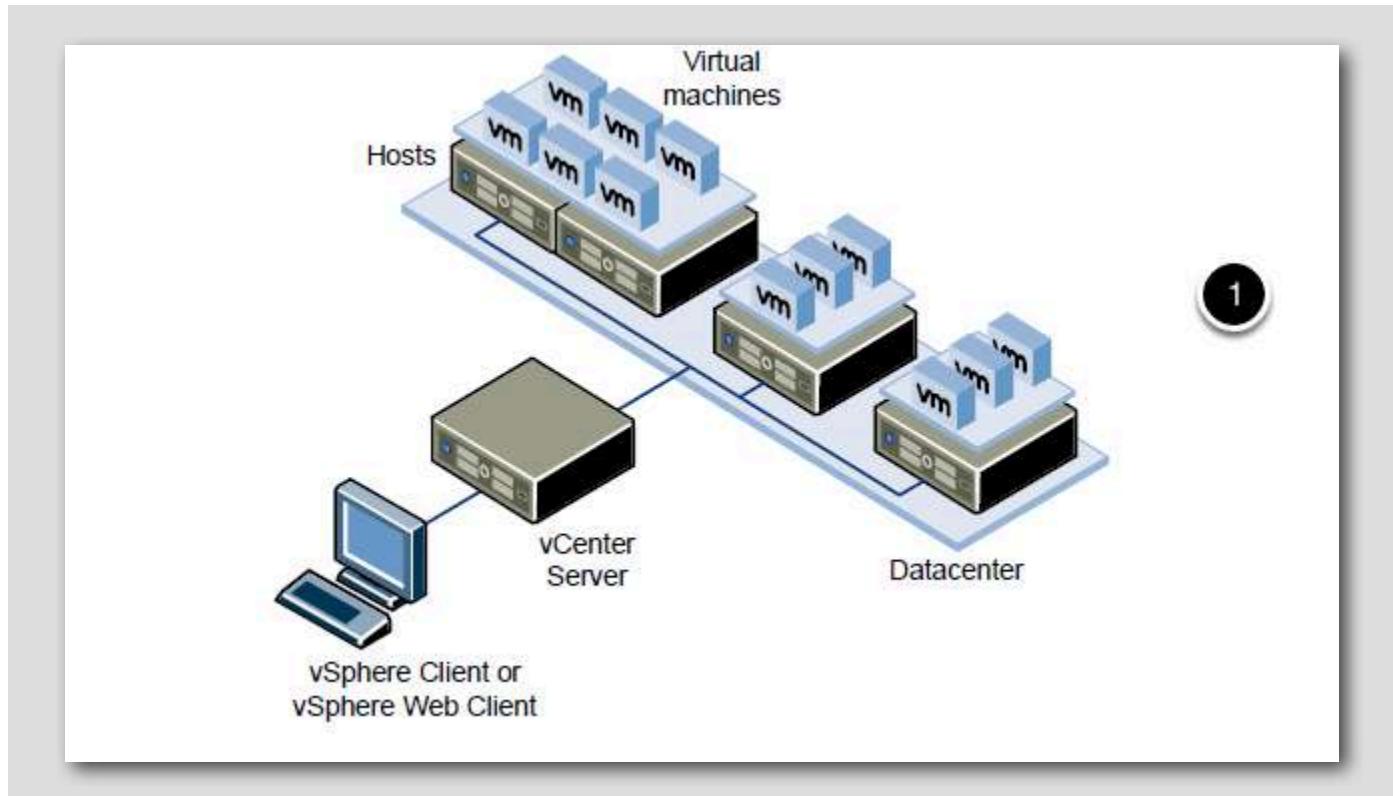
Since these features will be covered throughout the lab and the actions performed are identical, just at the vCenter Server level, we will not be reviewing them here.

The ESXi Host Client can be very useful in situations where a vCenter Server is not present to manage the host. However, when a vCenter Server is present, it is the preferred option and provides better tools to manage your infrastructure as a whole.

vCenter 7 Overview

vCenter Server unifies resources from individual hosts so that those resources can be shared among virtual machines in the entire datacenter. It accomplishes this by managing the assignment of virtual machines to the hosts and the assignment of resources to the virtual machines within a given host based on the policies that the system administrator sets.

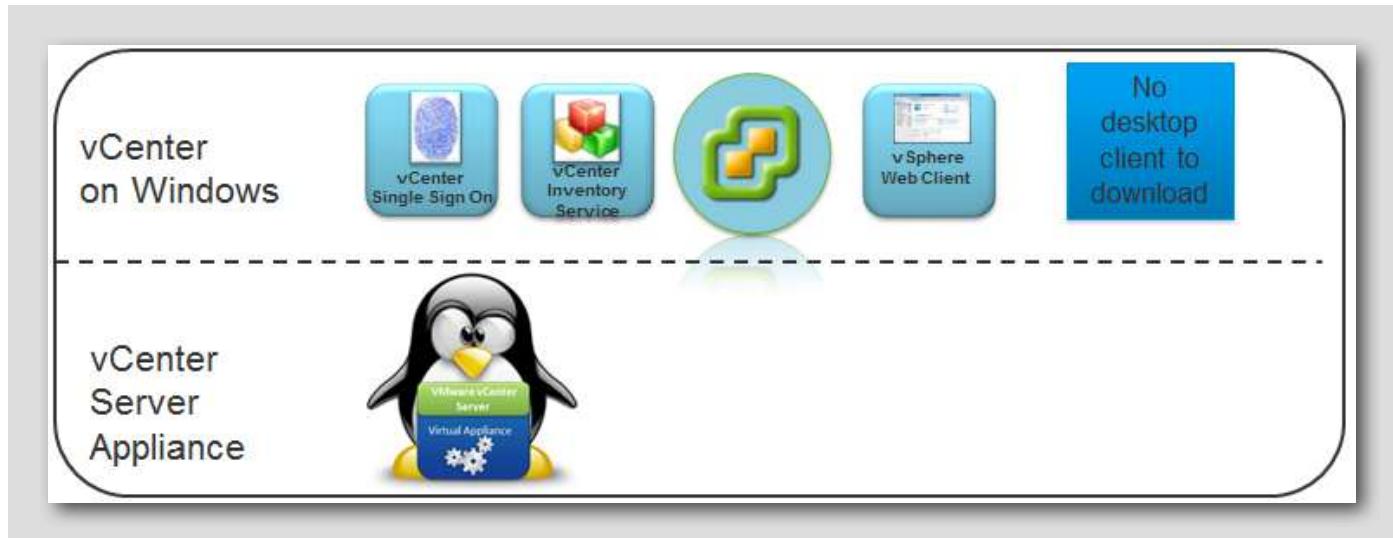
vSphere Components



The above diagram shows how vCenter fits in the vSphere stack. With vCenter installed, you have a central point of management. vCenter Server allows the use of advanced vSphere features such as vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), vSphere vMotion, and vSphere Storage vMotion.

The other component is the vSphere Web Client. The vSphere Web Client is the interface to vCenter Server and multi-host environments. It also provides console access to virtual machines. The vSphere Web Client lets you perform all administrative tasks by using an in-browser interface.

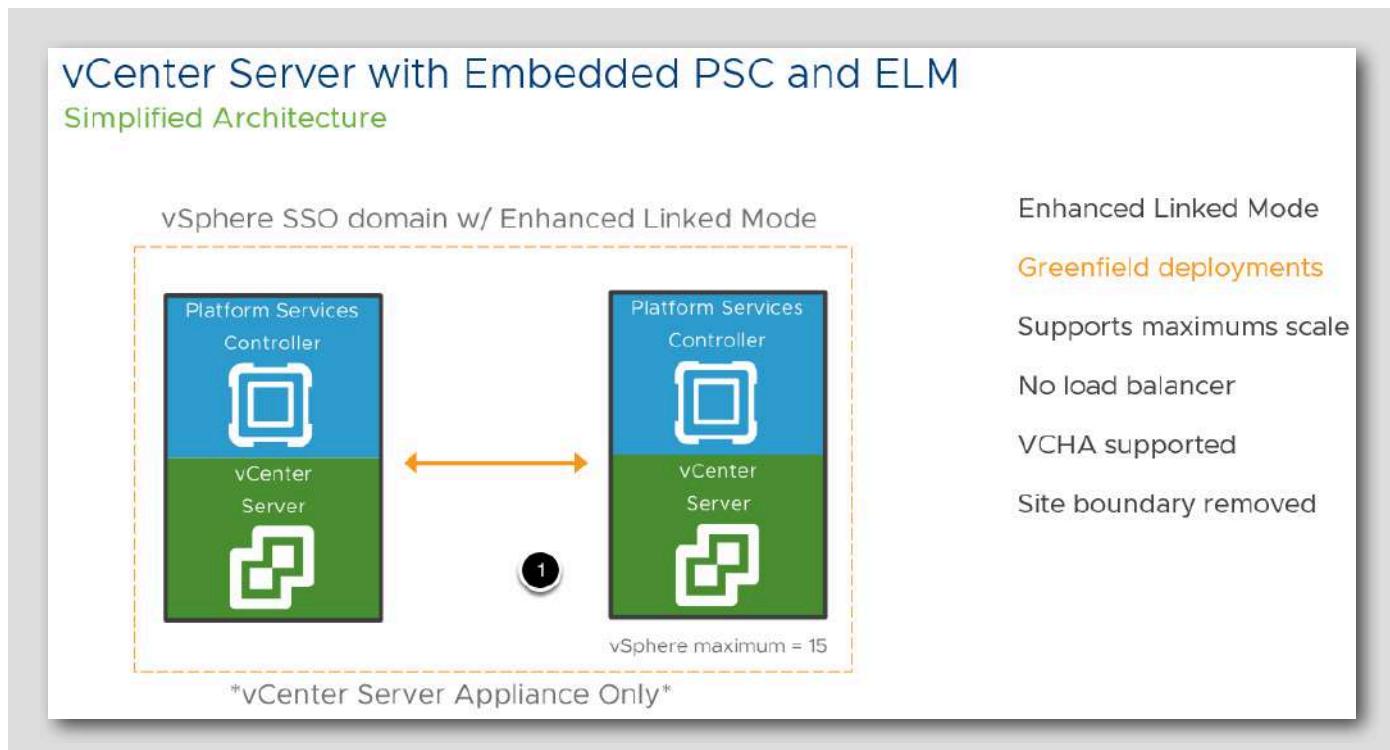
vCenter 7 Components



Starting with vSphere 5.1 there are two methods to deploy vCenter. The first method is a Windows installation. With the Windows method, you can install vCenter Single Sign-On, Inventory Service, and vCenter Server on the same host machine (as with vCenter Simple Install) or on different virtual machines.

The vCenter Server Appliance (vCSA) is a single preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

Platform Services Controller (PSC)



The Platform Services Controller (PSC) includes common services that are used across the suite. These include Single Sign-On (SSO), Licensing, and the VMware Certificate Authority (VMCA). You will learn more about SSO and the VMCA in the following pages.

The PSC is the first piece that is either installed or upgraded. When upgrading an SSO instance becomes a PSC. There are two models of deployment, embedded and centralized.

- Embedded means the PSC and vCenter Server are installed on a single virtual machine. – Embedded is recommended for sites with a single SSO solution such as a single vCenter.
- Centralized means the PSC and vCenter Server are installed on different virtual machines. – Centralized is recommended for sites with two or more SSO solutions such as multiple vCenter Servers, vRealize Automation, etc. When deploying in the centralized model it is recommended to make the PSC highly available as to not have a single point of failure, in addition to utilizing vSphere HA a load balancer can be placed in front of two or more PSC's to create a highly available PSC architecture.

The PSC and vCenter servers can be mixed and matched, meaning you can deploy Appliance PSC's along with Windows PSC's with Windows and appliance-based vCenter Servers. Any combination uses the PSC's built-in replication.

Use Case:

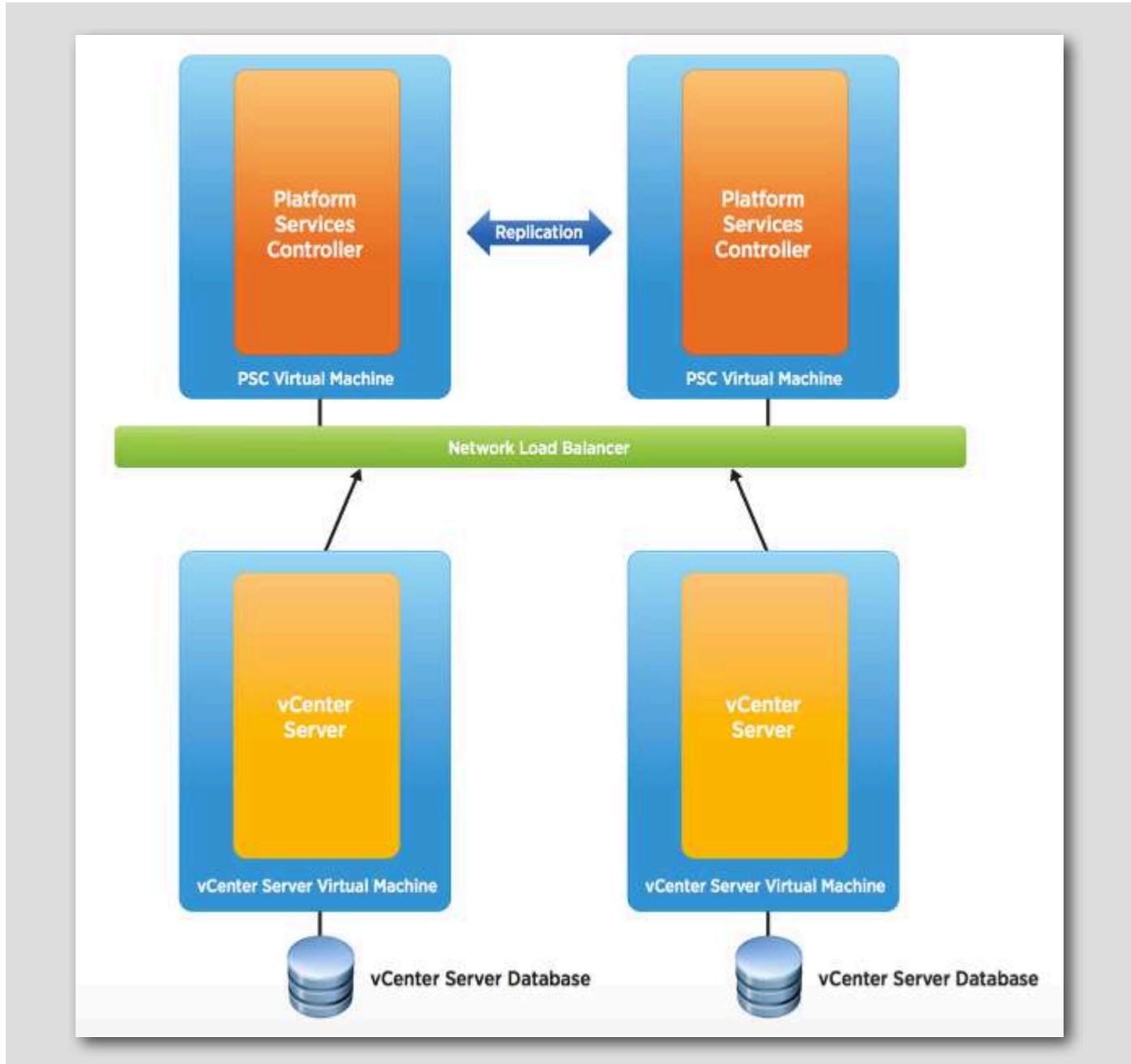
- The PSC removes services from vCenter and makes them centralized across the vCloud Suite.
- This gives customers a single point to manage all their vSphere roles and permissions along with licensing.
- Reducing vCenter Server installation complexity allows customers to install or upgrade to vSphere 7 faster.
- There are only two installs options:
 - Embedded PSC which installs all components on a single virtual machine.
 - Centralized, the customer must install the PSC and vCenter Server separately.
- In either installation model, all vCenter Server services are installed on the vCenter Server reducing the complexity of planning and installing vCenter Server.

vCenter Single Sign On

[36]

vSphere 5.1 introduced vCenter Single Sign On (SSO) as part of the vCenter Server management infrastructure. This change affects the vCenter Server installation, upgrading, and operation. Authentication by vCenter Single Sign On makes the VMware cloud infrastructure platform more secure by allowing the vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

vCenter Single Sign On - Typical Deployment

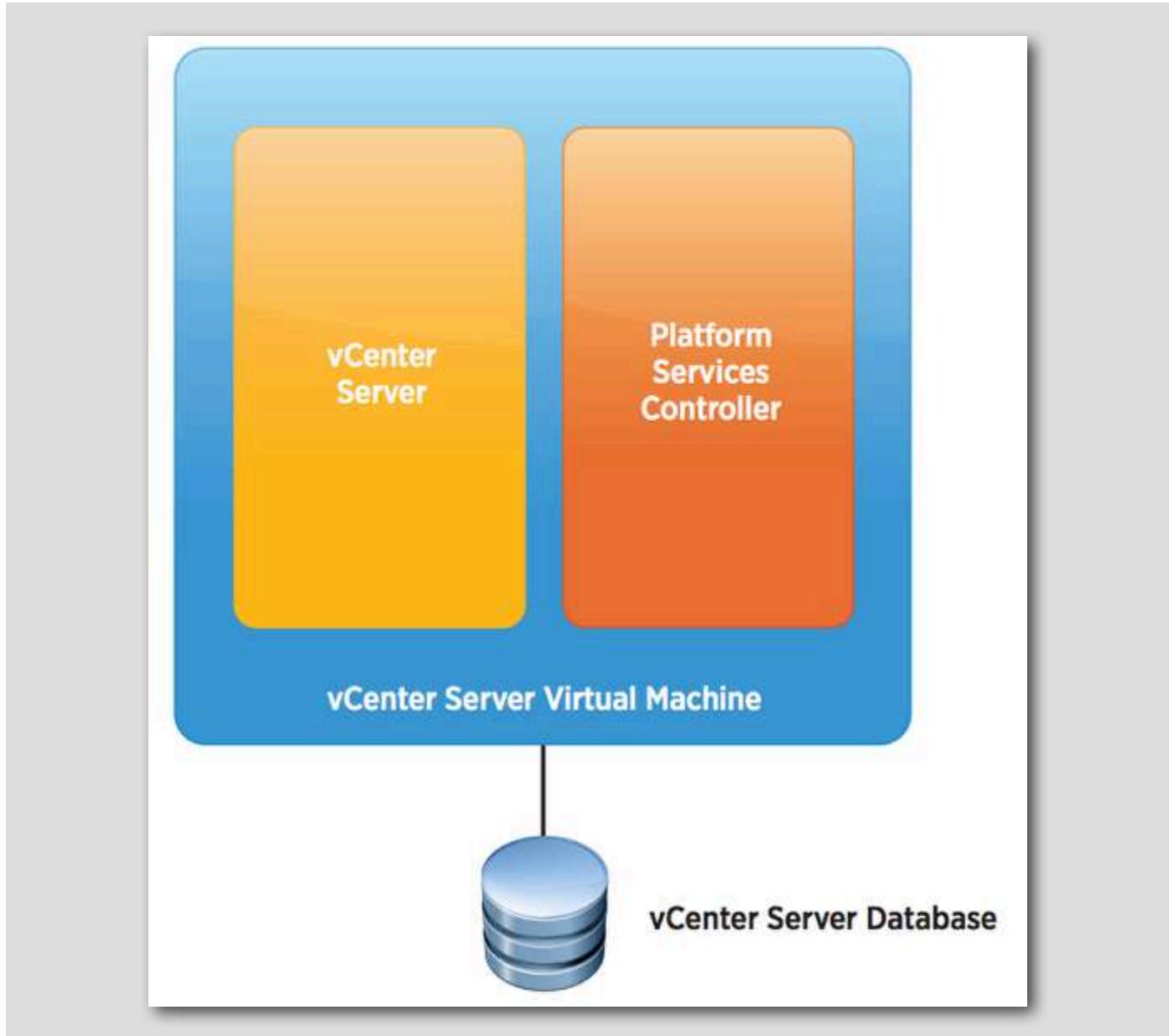


Starting with version 5.1, vSphere includes a vCenter Single Sign-On service as part of the vCenter Server management infrastructure.

Authentication with vCenter Single Sign-On makes vSphere more secure because the vSphere software components communicate with each other by using a secure token exchange mechanism, and all other users also authenticate with vCenter Single Sign-On.

Starting with vSphere 6.0, vCenter Single Sign-On is either included in an embedded deployment or part of the Platform Services Controller. The Platform Services Controller contains all of the services that are necessary for the communication between vSphere components including vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service, and the licensing service. For example, in the image above, SSO resides within the Platform Services Controller as part of this multi-vCenter topology.

vCenter Single Sign On - Single vCenter



In a single vCenter topology, the PSC (along with all of its associated services) can run on a single machine, also called the embedded deployment. This single machine could be a physical Windows server, a Windows VM, or the vCSA.

While vCenter Server requires a database, as shown above, SSO itself does not have such a requirement.

More Information on Single Sign On

The second Module in this lab, Introduction to vSphere Networking and Security covers SSO in more detail.

However, you can also refer to the [vCenter 7 Deployment Guide](#) for more in-depth requirements and considerations for SSO architecture in vCenter 7.

vCenter Server and Creating a Virtual Machine

The previous lesson reviewed the ESXi Host Client, which can be used to manage one ESXi host at a time. This lesson will introduce the vSphere Client which is used to connect to vCenter Server to manage your collective infrastructure as a whole. In addition, the process of creating a virtual machine will also be covered.

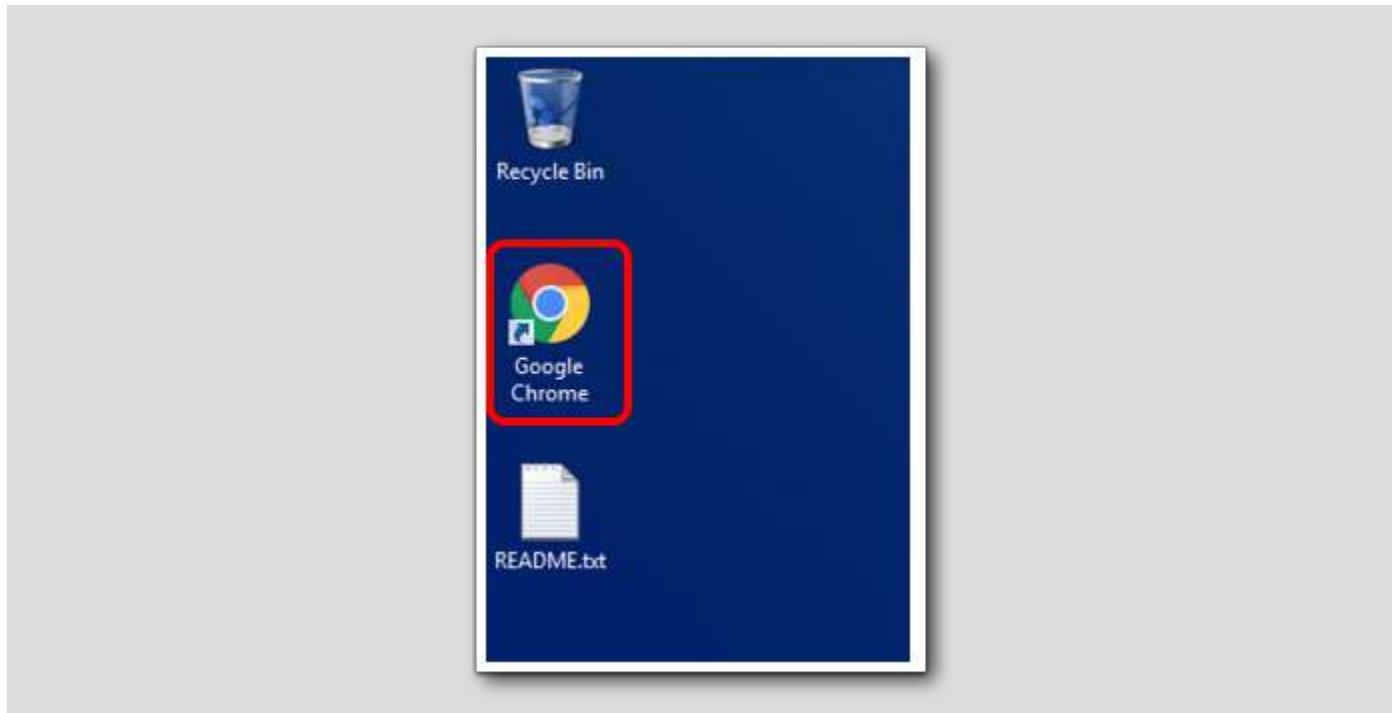
The vSphere Client is the primary method for system administrators and end-users to interact with the virtual data center environment created by VMware vSphere. vSphere manages a collection of objects that make up the virtual data center, including hosts, clusters, virtual machines, data storage, and networking resources.

The vSphere Client is a Web browser-based application that you can use to manage, monitor, and administer the objects that make up your virtualized data center. You can use the vSphere Client to observe and modify the vSphere environment in the following ways.

- Viewing health, status, and performance information on vSphere objects
- Issuing management and administration commands to vSphere objects
- Creating, configuring, provisioning, or deleting vSphere objects

You can extend vSphere in different ways to create a solution for your unique IT infrastructure. You can extend the vSphere Client with additional GUI features to support these new capabilities, with which you can manage and monitor your unique vSphere environment.

Launch Chrome



If you are not already in Chrome, double click on Google Chrome on your desktop. If you are already in Google Chrome, open a new tab.

Select vSphere Client



1. Click the vSphere Web Client bookmark.

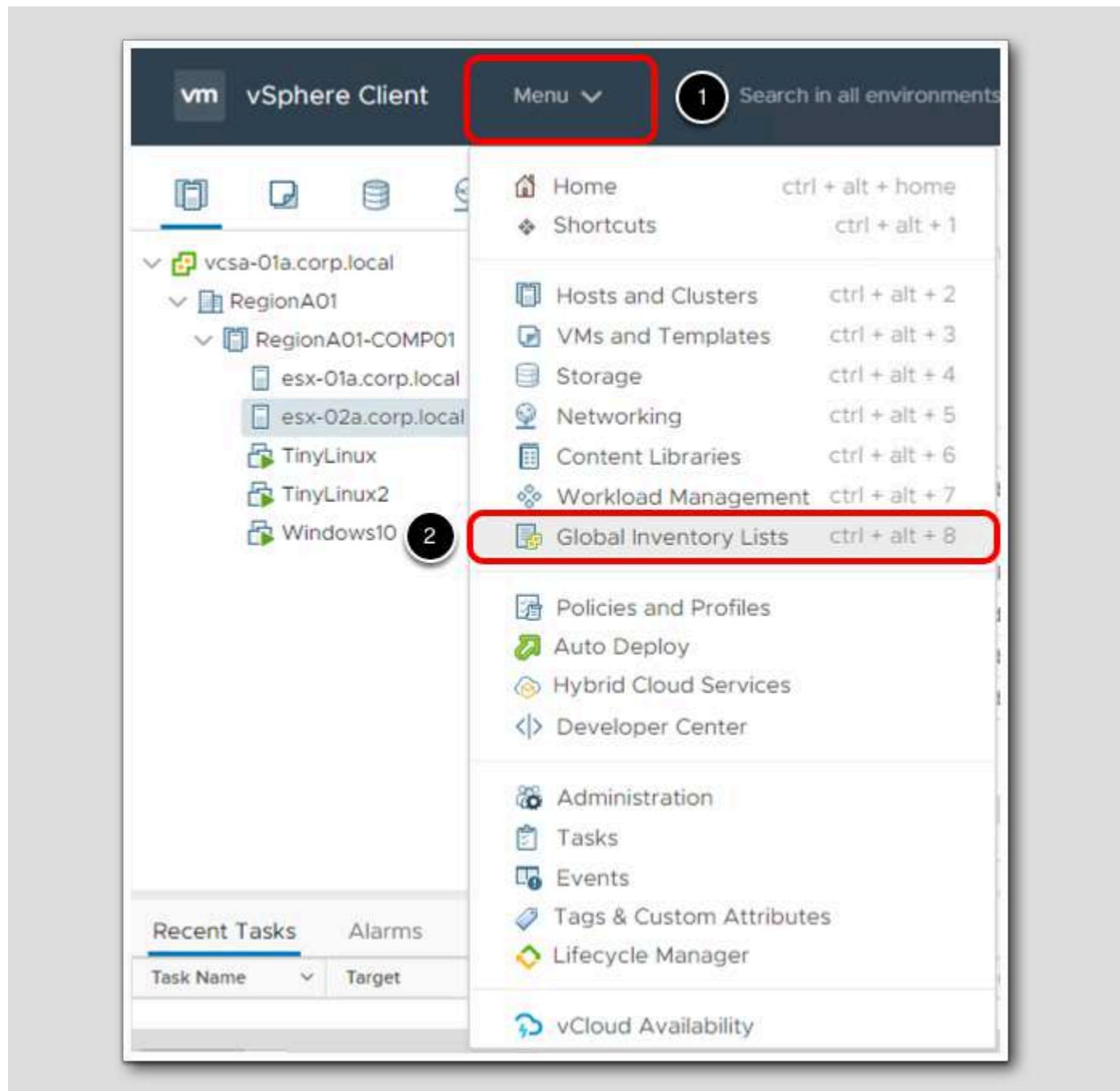
Login to vCenter



Log in using the following method:

1. Click the "Use Windows session authentication" check box.
2. Click the "Login" button.

vCenter Inventory

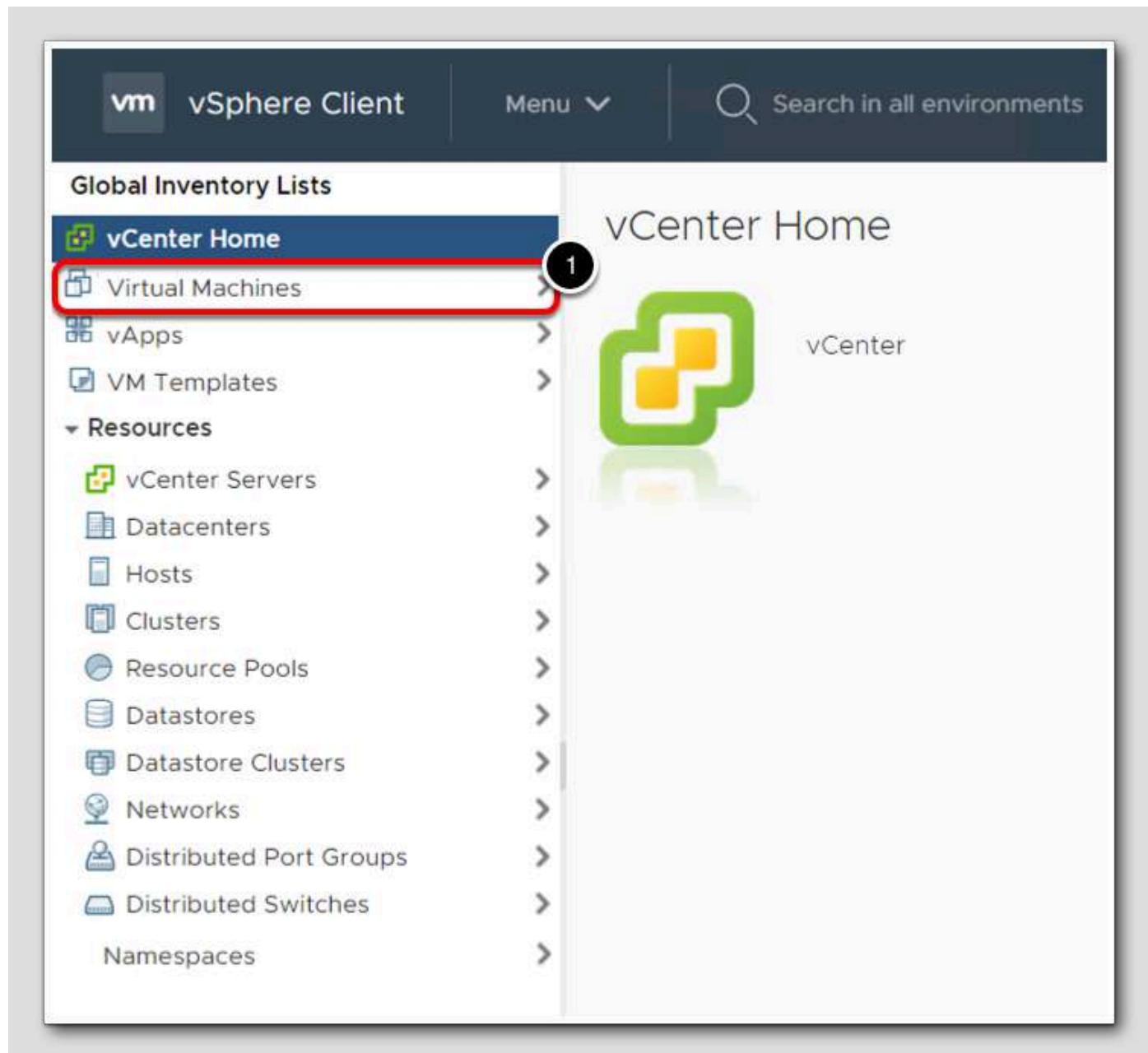


By default, you are brought to a view that shows the Hosts and Clusters attached to vCenter. Get a more complete look by viewing the Global Inventory Lists.

1. Click on the **Menu** drop-down list and select **Global Inventory Lists**.

Clicking Global Inventory Lists will take you to the inventory page where you find all the objects associated with vCenter Server systems such as data centers, hosts, clusters, networking, storage, and virtual machines.

Child objects, Data Centers, and Hosts



1. Click the "Virtual Machines" inventory item. By selecting this inventory item, you are presented with a list of the VMs which are located in this environment.

Virtual Machine Summary

The screenshot shows the vSphere Client interface. In the left sidebar, under 'Virtual Machines', there are three entries: 'TinyLinux', 'TinyLinux2', and 'Windows10'. The 'Windows10' entry is highlighted with a red oval and has a black circle with the number '1' above it. The main content area is titled 'Windows10' and shows the 'Summary' tab selected (indicated by a red oval and a black circle with '2'). Below the tab bar, there's a thumbnail image of the Windows desktop. To the right of the image, detailed information about the VM is listed:

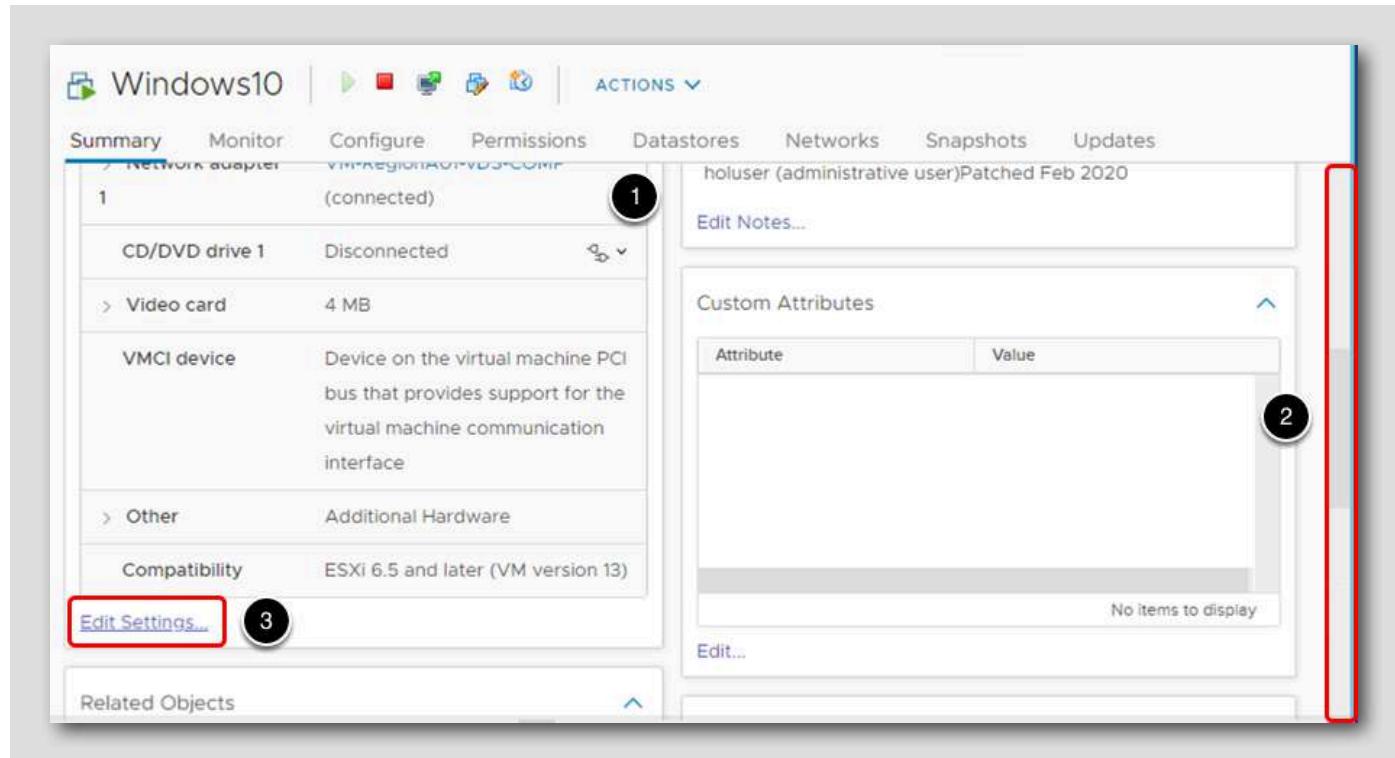
Guest OS:	Microsoft Windows 10 (64-bit)
Compatibility:	ESXi 6.5 and later (VM version 13)
VMware Tools:	Running, version:11297 (Current) More info
DNS Name:	Windows10.corp.local
IP Addresses:	192.168.120.53 View all 2 IP addresses
Host:	esx-02a.corp.local

Below this, there are two links: 'Launch Web Console' and 'Launch Remote Console'. On the far right, there's a 'Notes' section with a list of items and an 'Edit Notes' link. A red oval and a black circle with '3' are highlighting the upward-pointing arrow icon in the notes section.

Here are all the virtual machines associated with this vCenter instance.

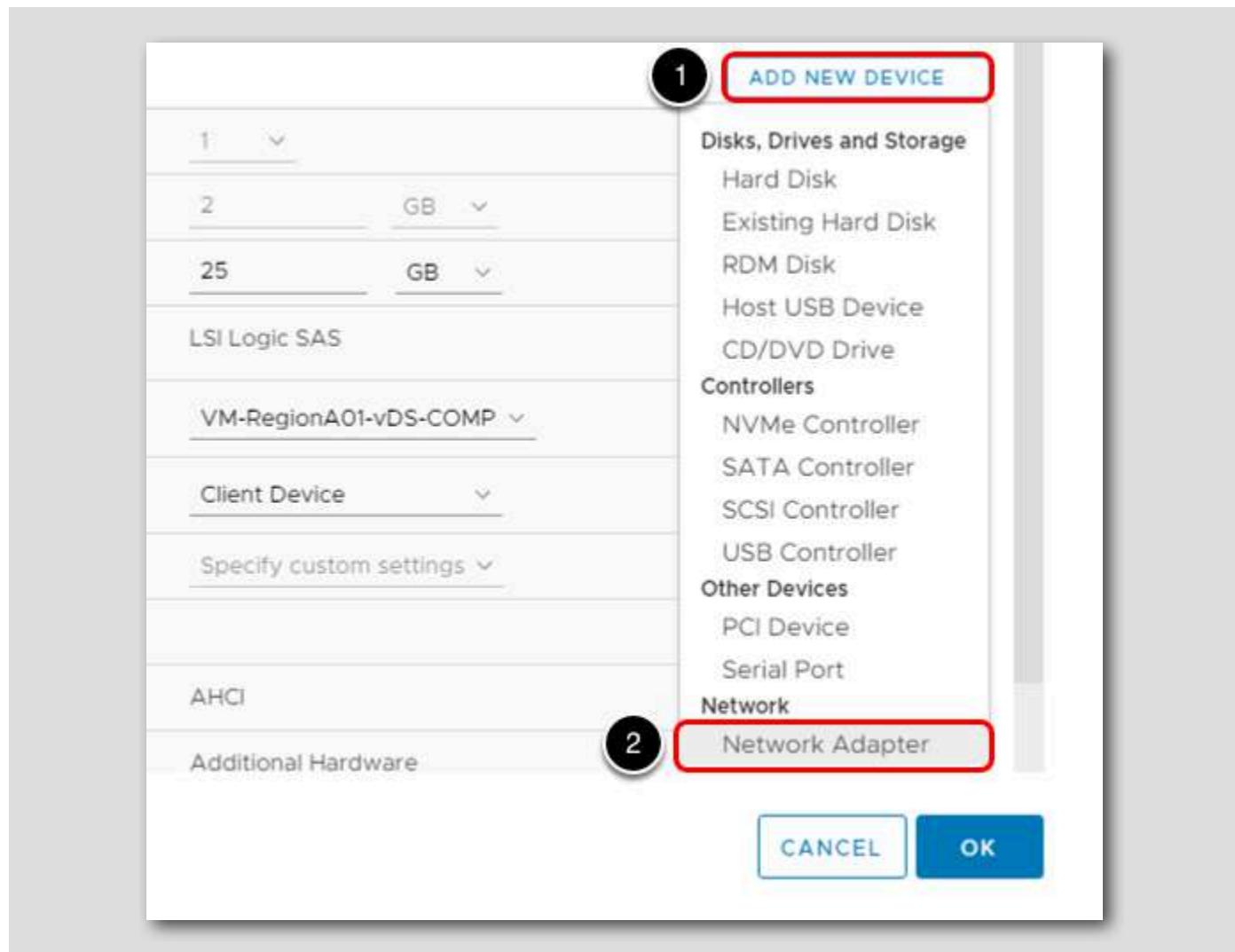
1. Click the "Windows10" virtual machine.
2. Click the "Summary" Tab for that virtual machine. On this page, you are able to see all the details regarding the virtual machine. There is an "Edit Settings" link as well to modify the settings of the virtual machine.
3. Expand the VM Hardware section.

Edit the settings of a virtual machine.



1. Review the VM Hardware for the windows10 virtual machine. Note that there is currently only one network adapter.
2. Use the scroll bar to move to the bottom of the VM Hardware section.
3. Click "Edit Settings" so a second network adapter can be added to the virtual machine.

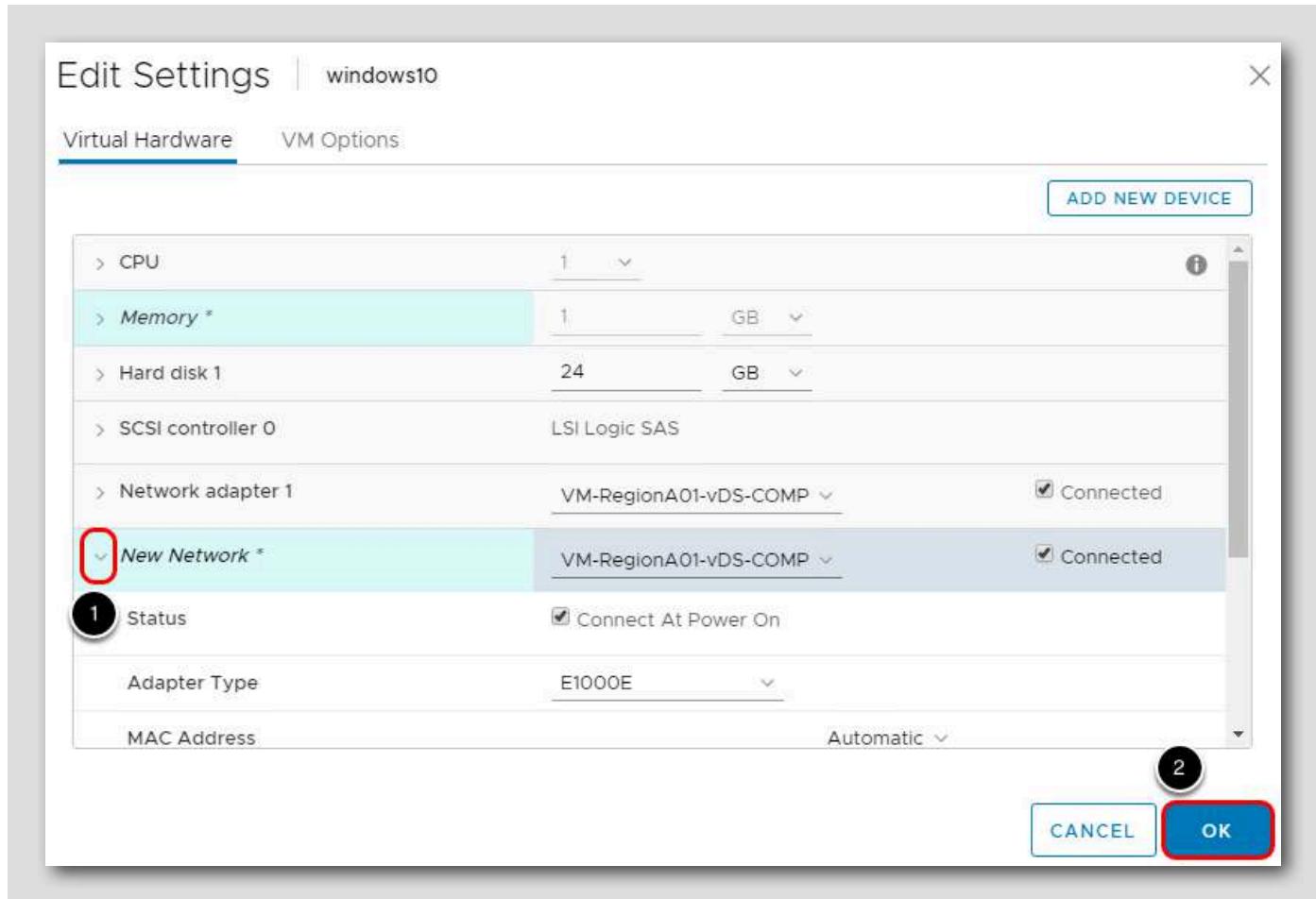
Add a second network adapter



Add another network adapter to the windows10 machine.

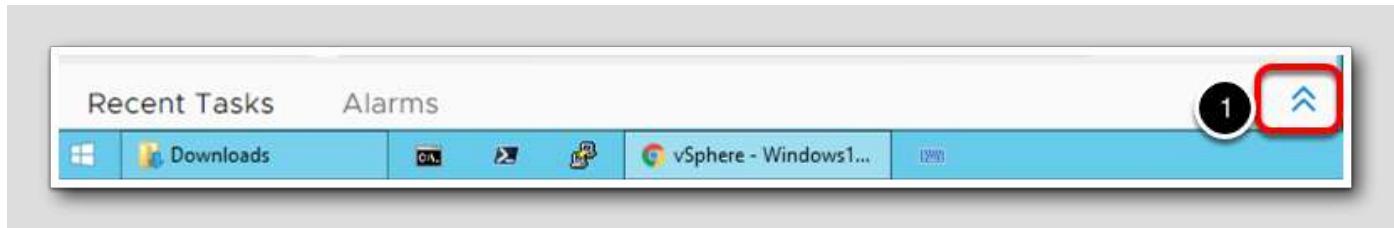
1. In the Edit Setting window, click the Add New Device button.
2. Select Network Adapter from the drop-down list.

Configure the Second Network Card.



1. Click the arrow next to the New Network card to expand and view its settings. Notice that the MAC address is blank at this point. A new MAC address will be generated once this NIC is added or we are able to specify (with some rules) our own MAC address.
2. Click "OK" to add the device to the VM. When you select "OK" a new task is created.

Recent Tasks List



Click on the Arrows to view the Recent Tasks to watch the task's progress.

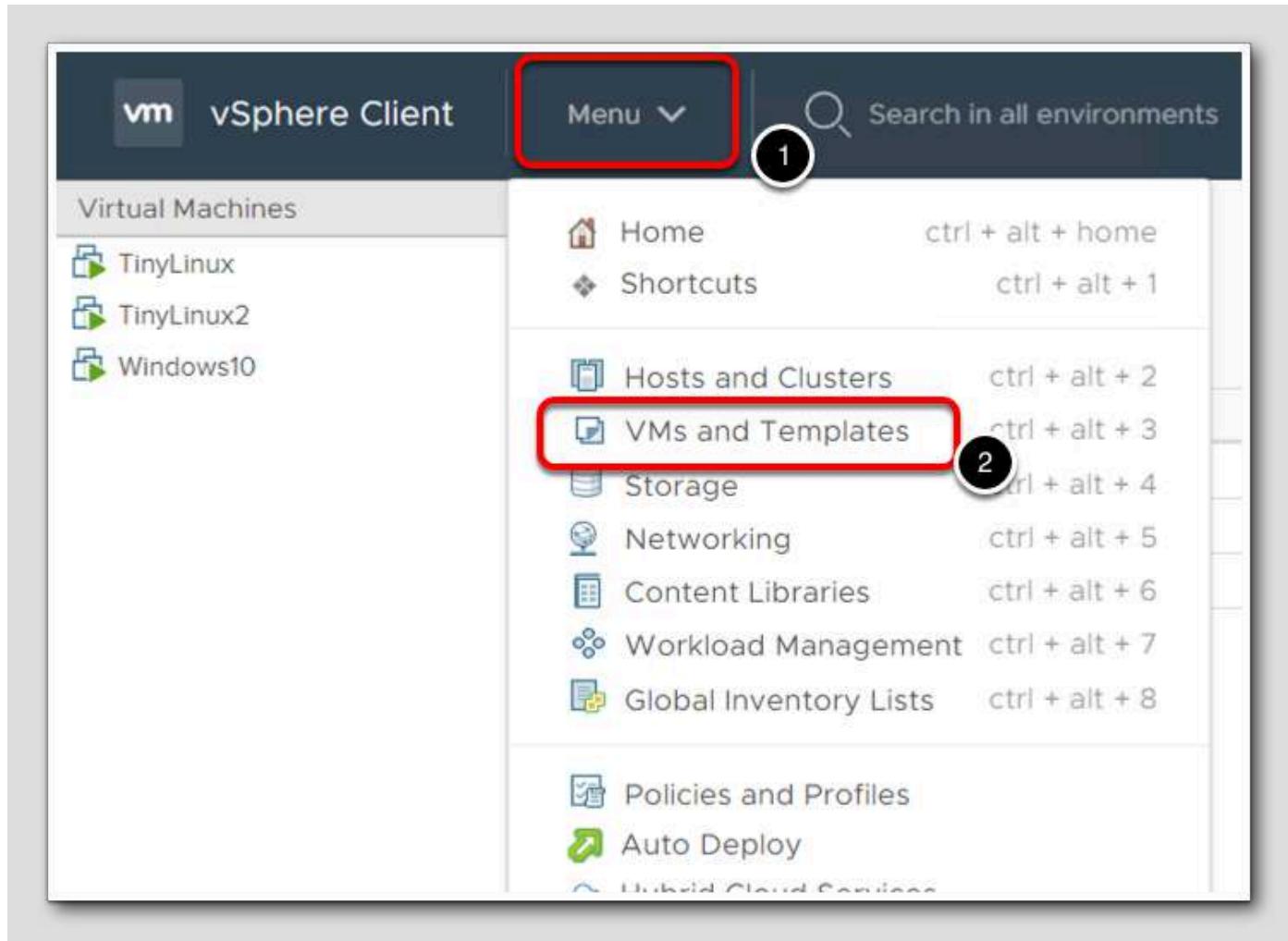
Recent Tasks List

Recent Tasks											Alarms
Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server			▼
Reconfigure virtual machine	Windows10	Completed	Reconfiguring Virtual Machine on destination host	CORP\Administrator	9 ms	12/22/2020, 9:20:28 AM	12/22/2020, 9:20:31 AM	vcsa-Qta.corp.local			▼

Review the "Recent Tasks" list. Once the task is complete, a second Network Adapter should be shown in the "VM Hardware" section. Note the networks are in a disconnected state because the VM is powered off.

Once you are done viewing the Recent Tasks list, click the down-arrows to minimize it.

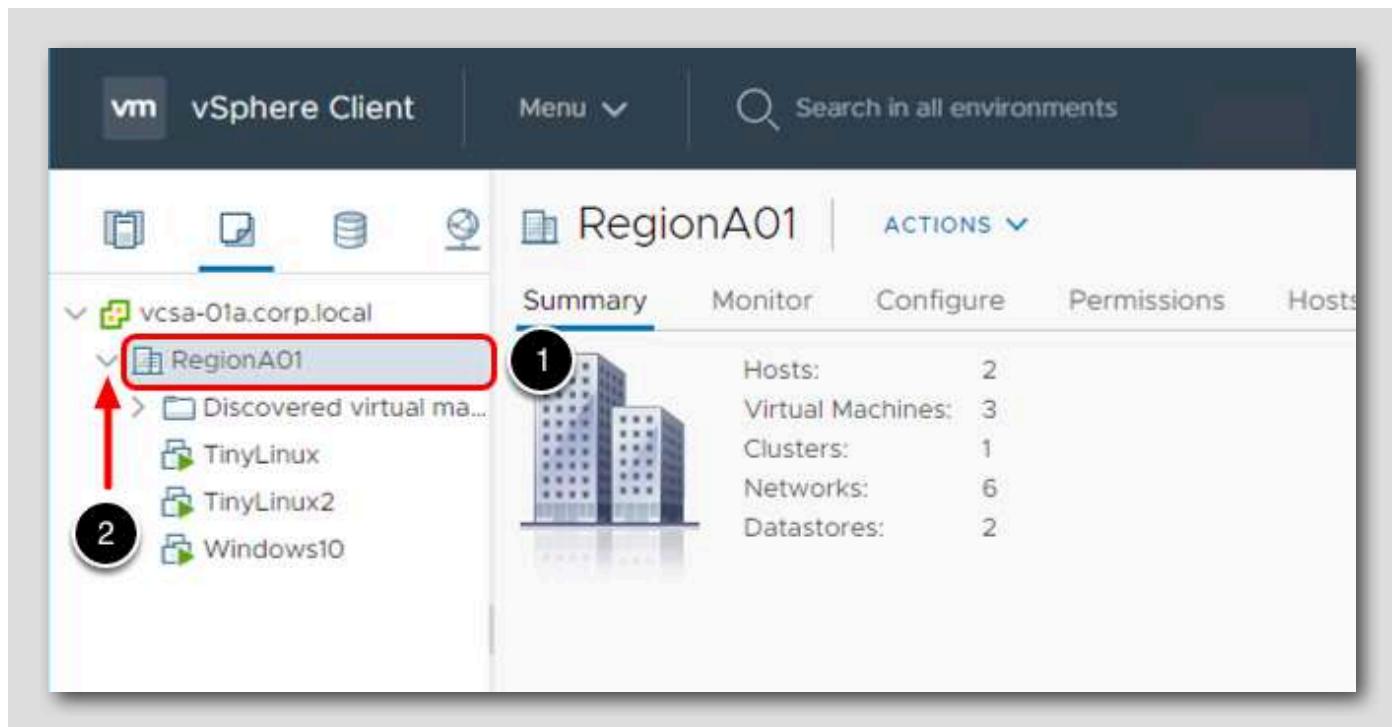
Create a Virtual Machine



In the next steps, we will create a virtual machine and then, install an operating system.

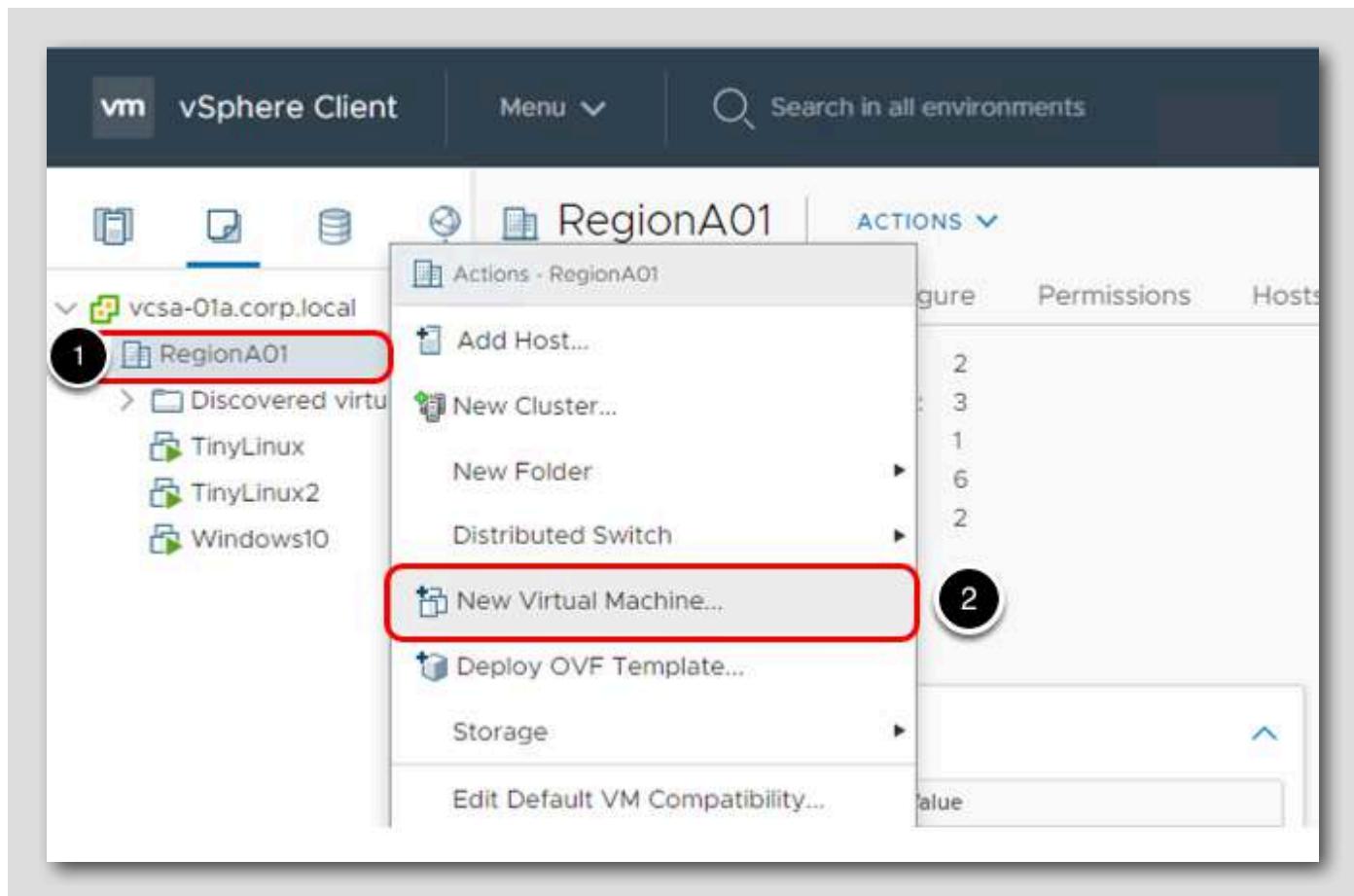
1. To return to the VMs and Templates view, click on Menu.
2. Select VMs and Templates.

Select and Expand Datacenter



1. Click on RegionA01 Datacenter.
2. Expand RegionA01 Datacenter so the virtual machines under it can be seen.

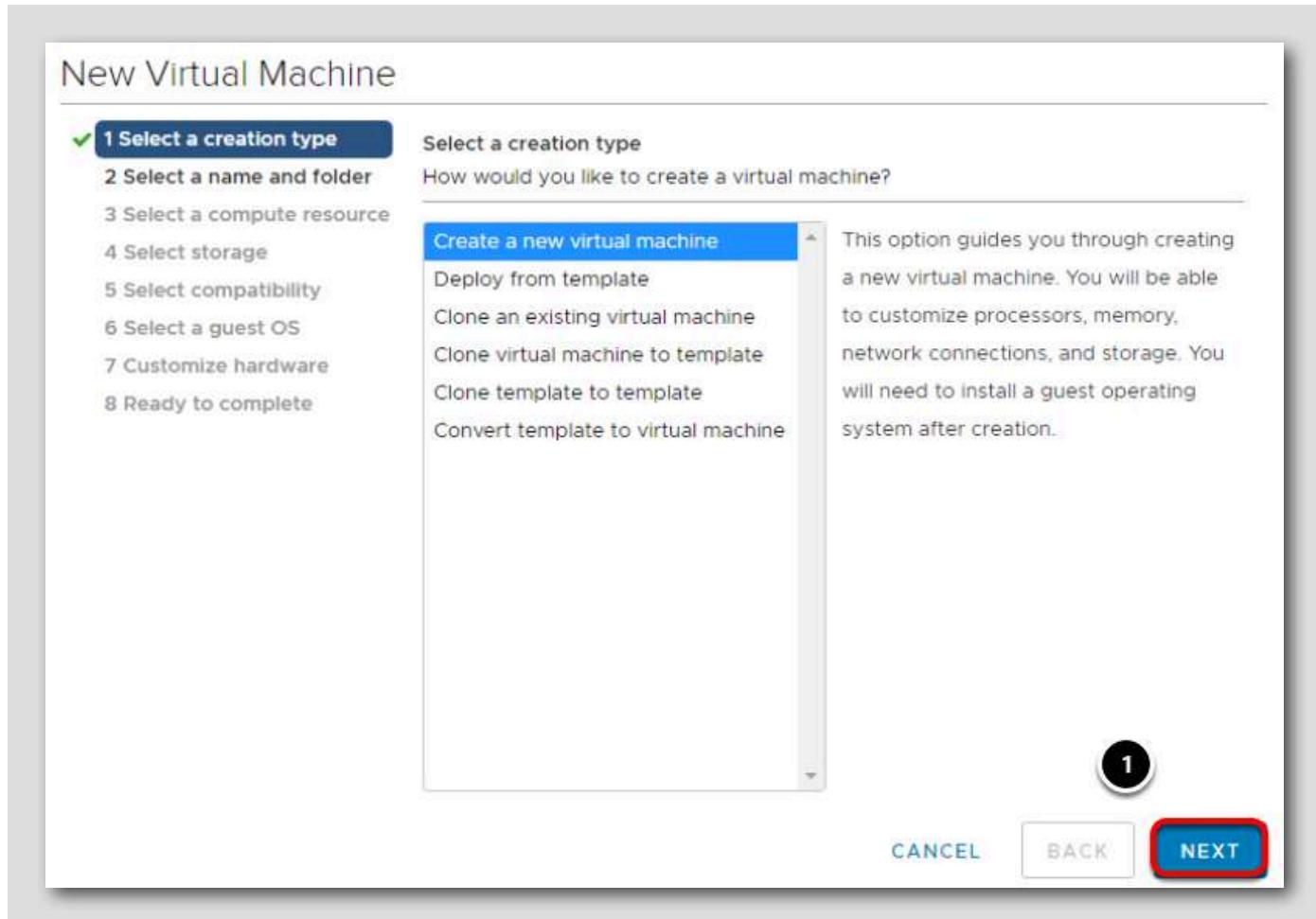
Start the New Virtual Machine Wizard



1. Right-click on RegionA01 Datacenter.
2. Click New Virtual Machine to start the new virtual machine wizard.

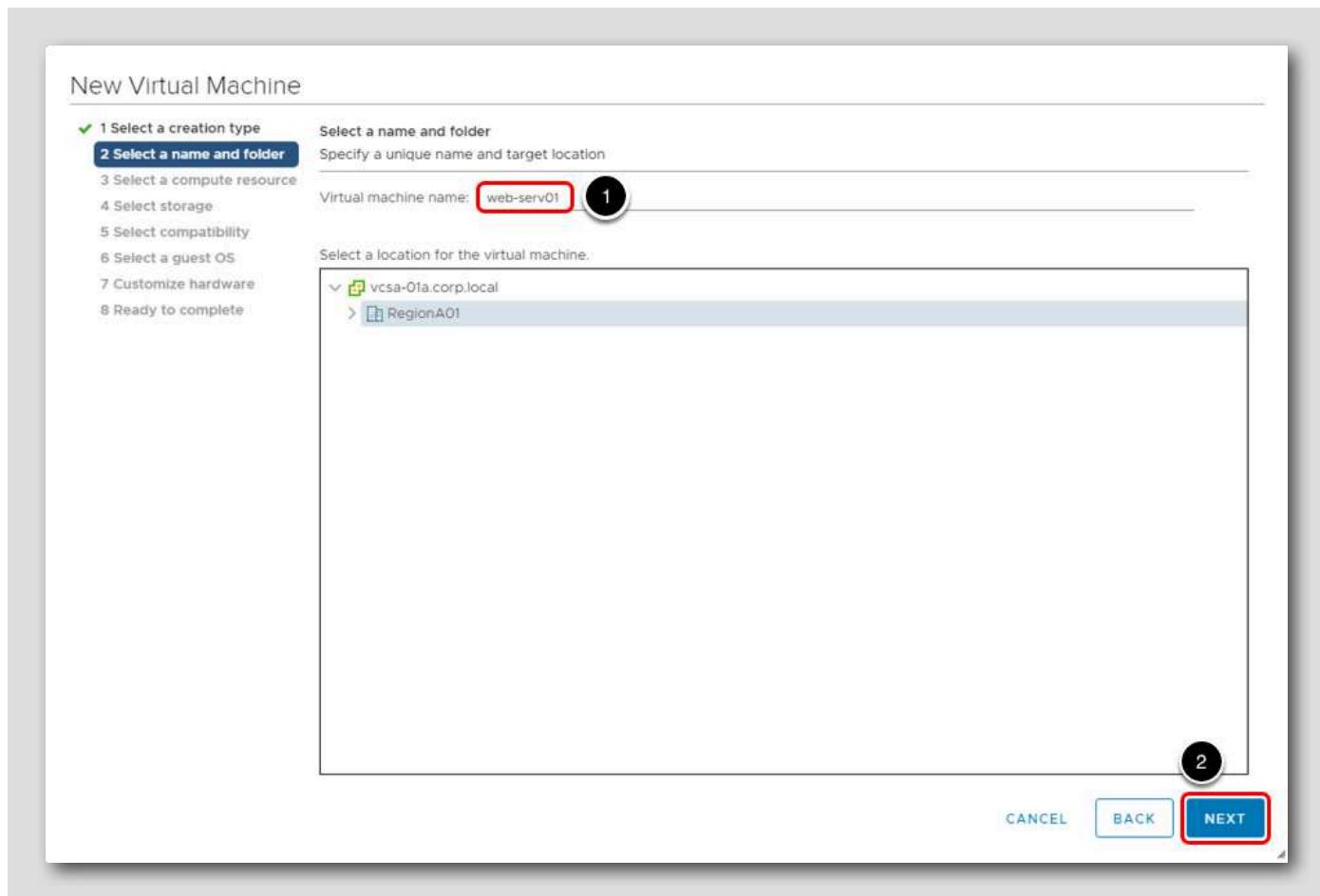
This wizard is used to create a new Virtual Machine and place it in the vSphere inventory.

Virtual Machine wizard



1. Since the Create a new virtual machine wizard is highlighted, just click Next.

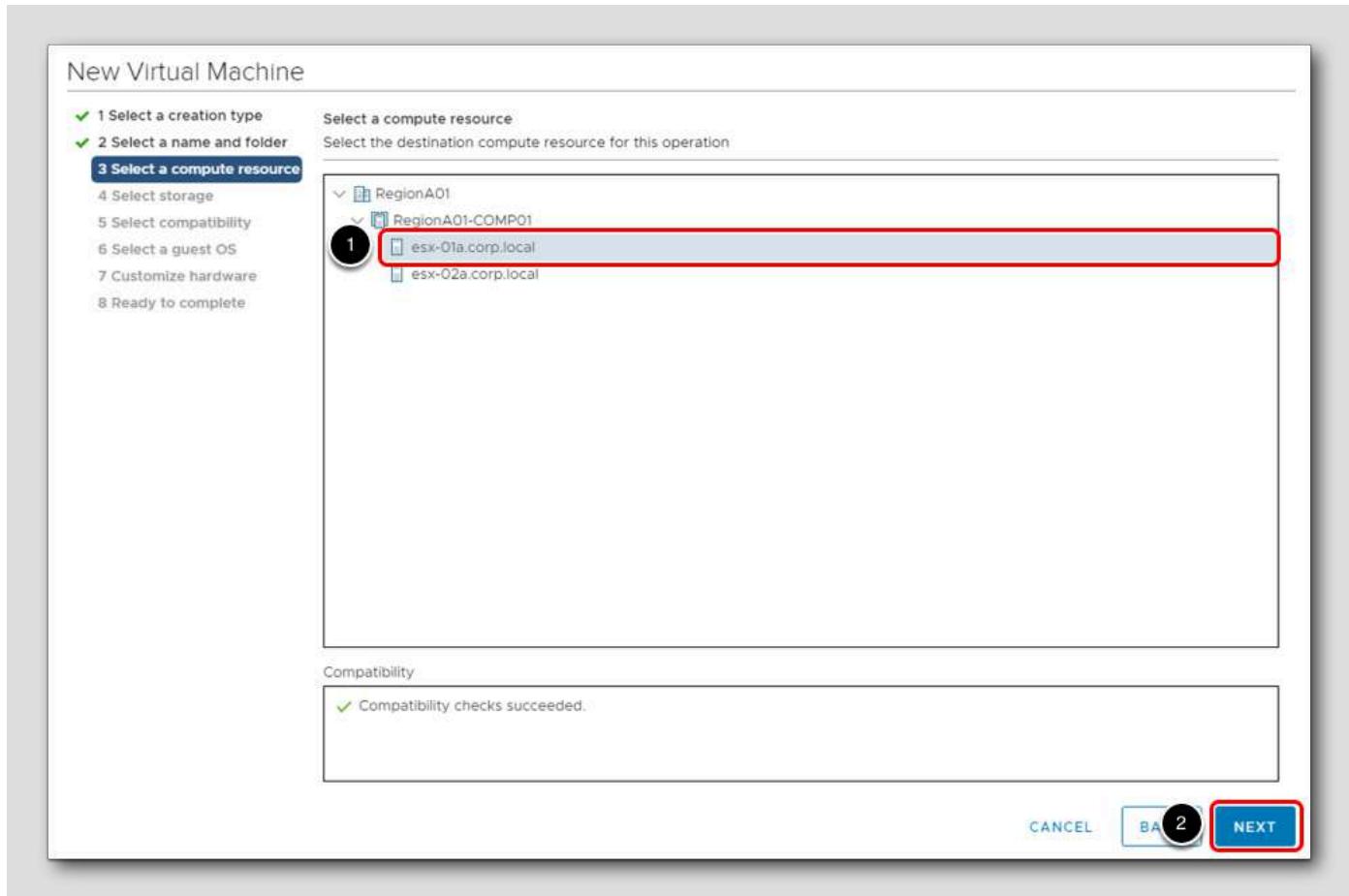
Name the Virtual Machine



1. Enter **web-serv01** for the name of the new virtual machine.

2. Click **Next**.

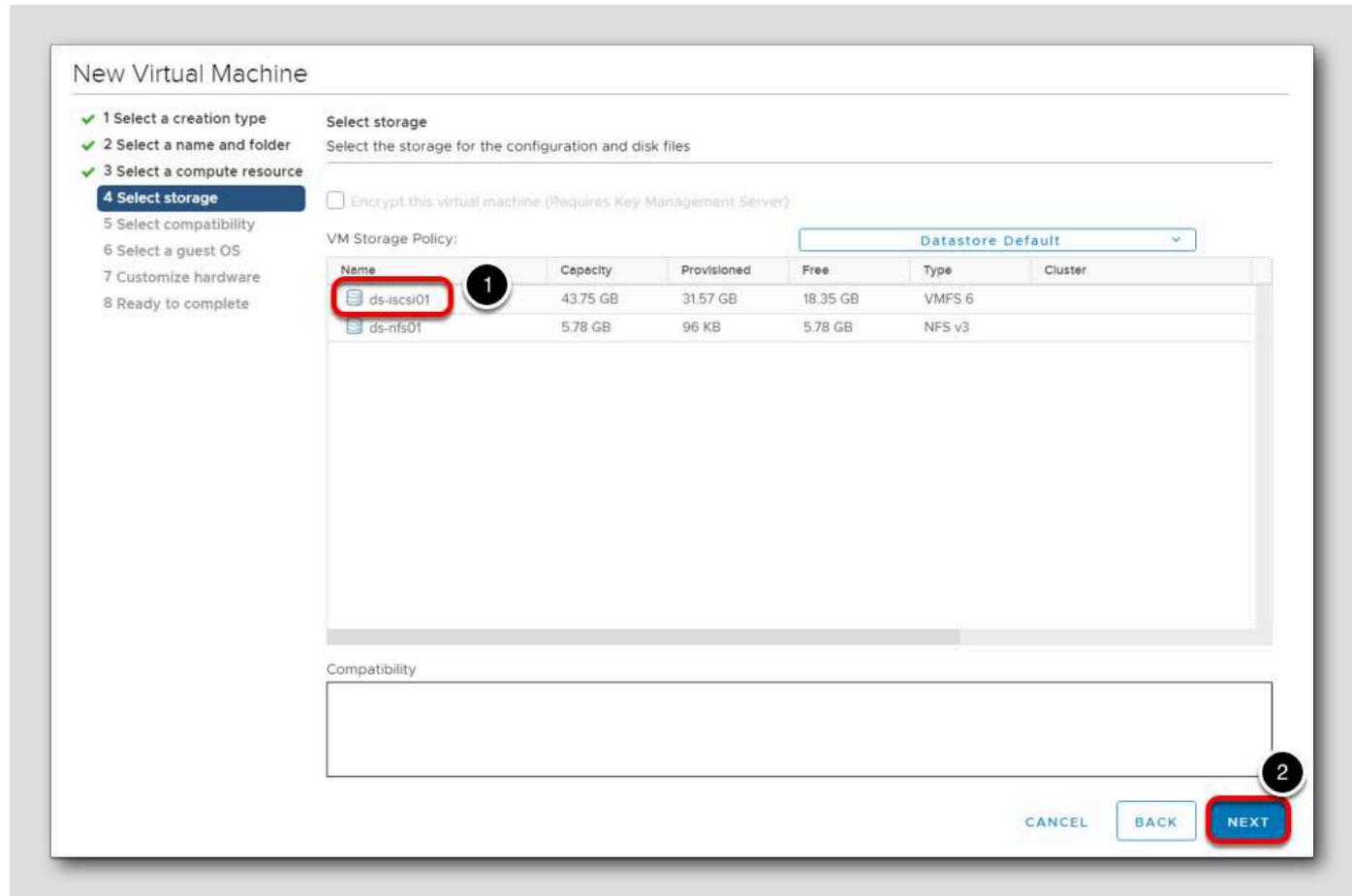
Virtual Machine Placement



Because Distributed Resource Scheduler (DRS) is not enabled, you just have to select a host to use for the VM. More details on DRS will be covered later in this module.

1. Click **esx-01a.corp.local**.
2. Click **Next**.

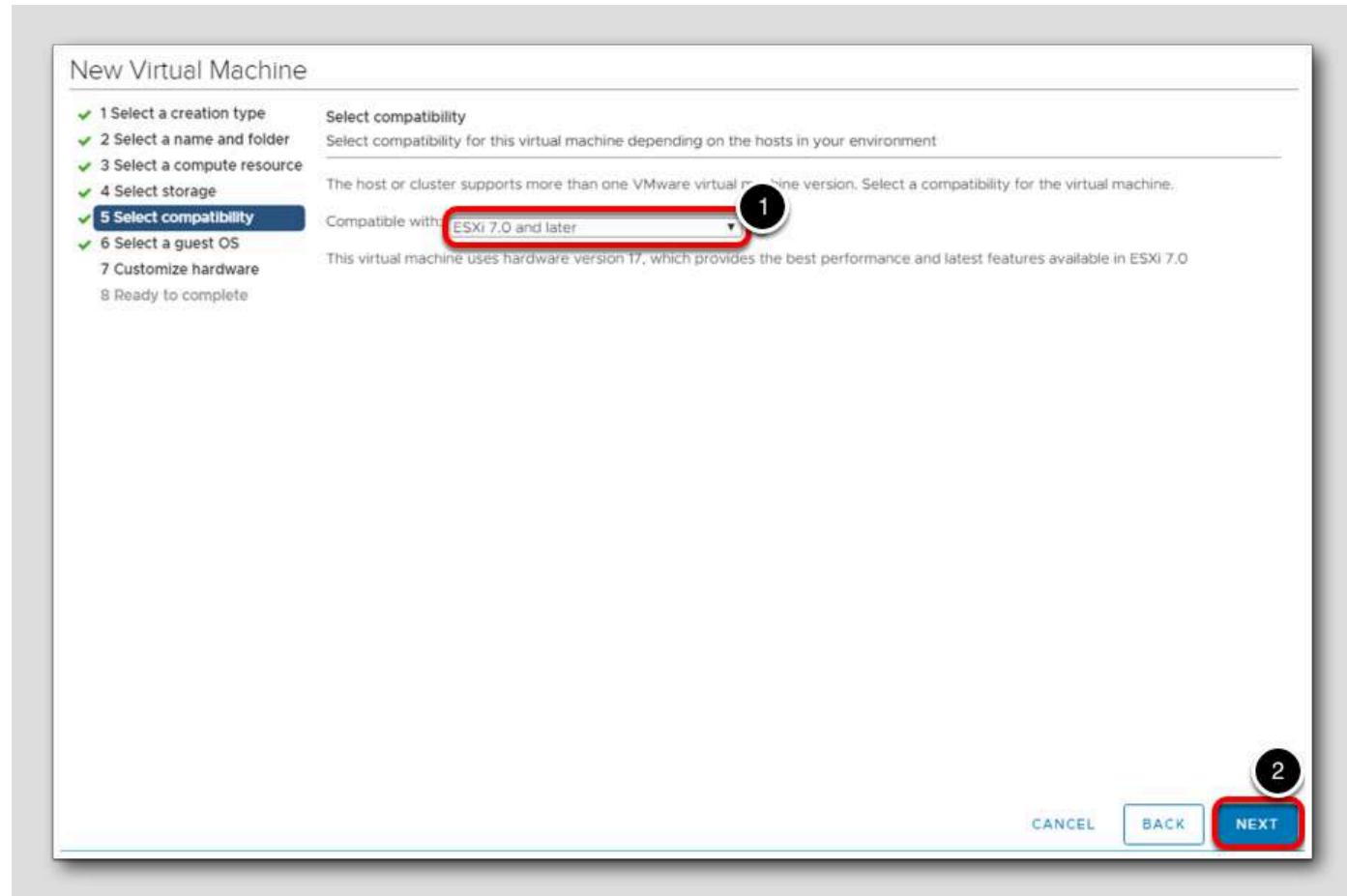
Select Storage



1. Ensure the **ds-iscsi01** datastore is selected.

2. Click **Next**.

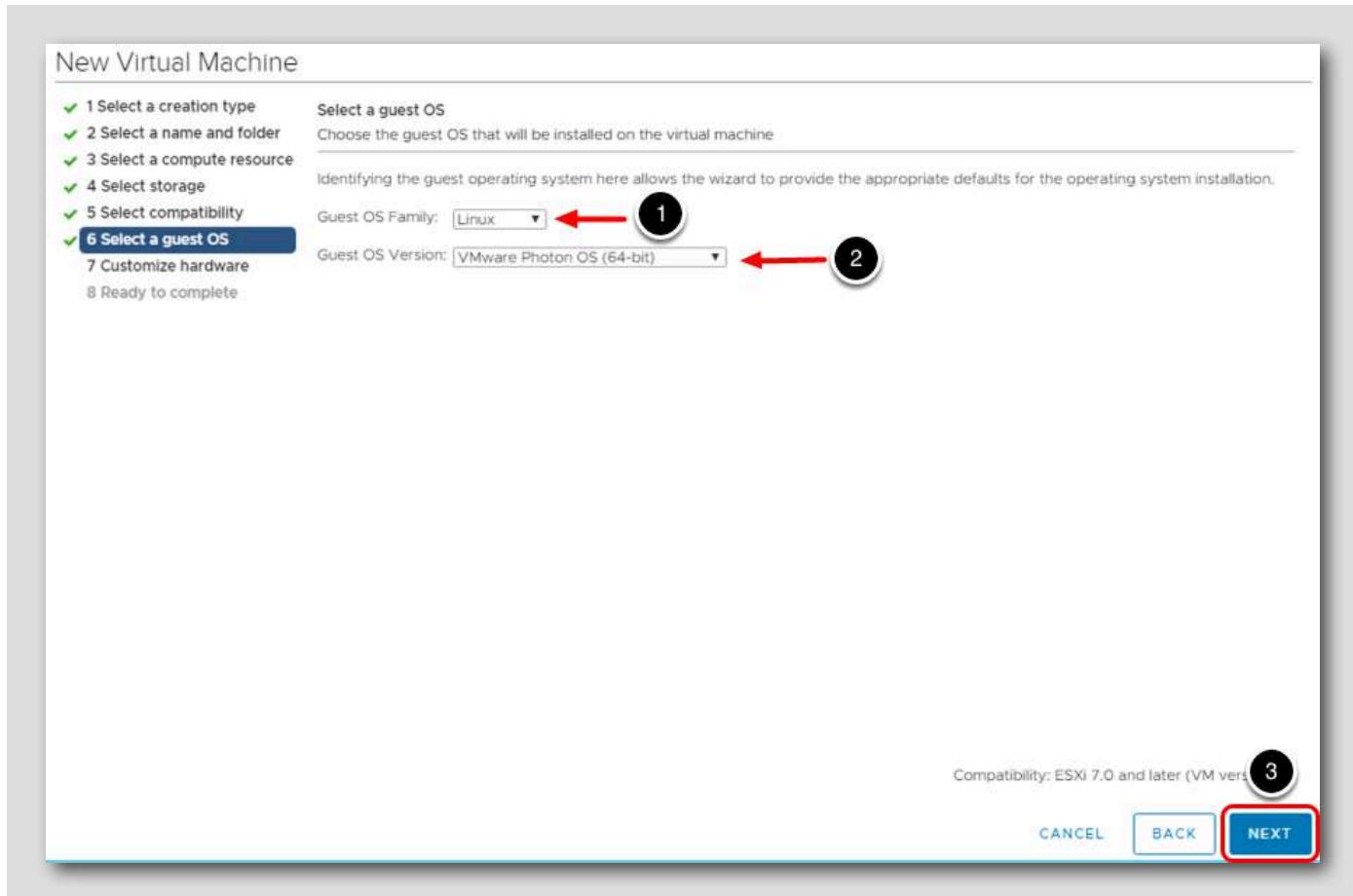
Compatibility



1. Select ESXi 7.0 and later.

2. Click **Next** to accept.

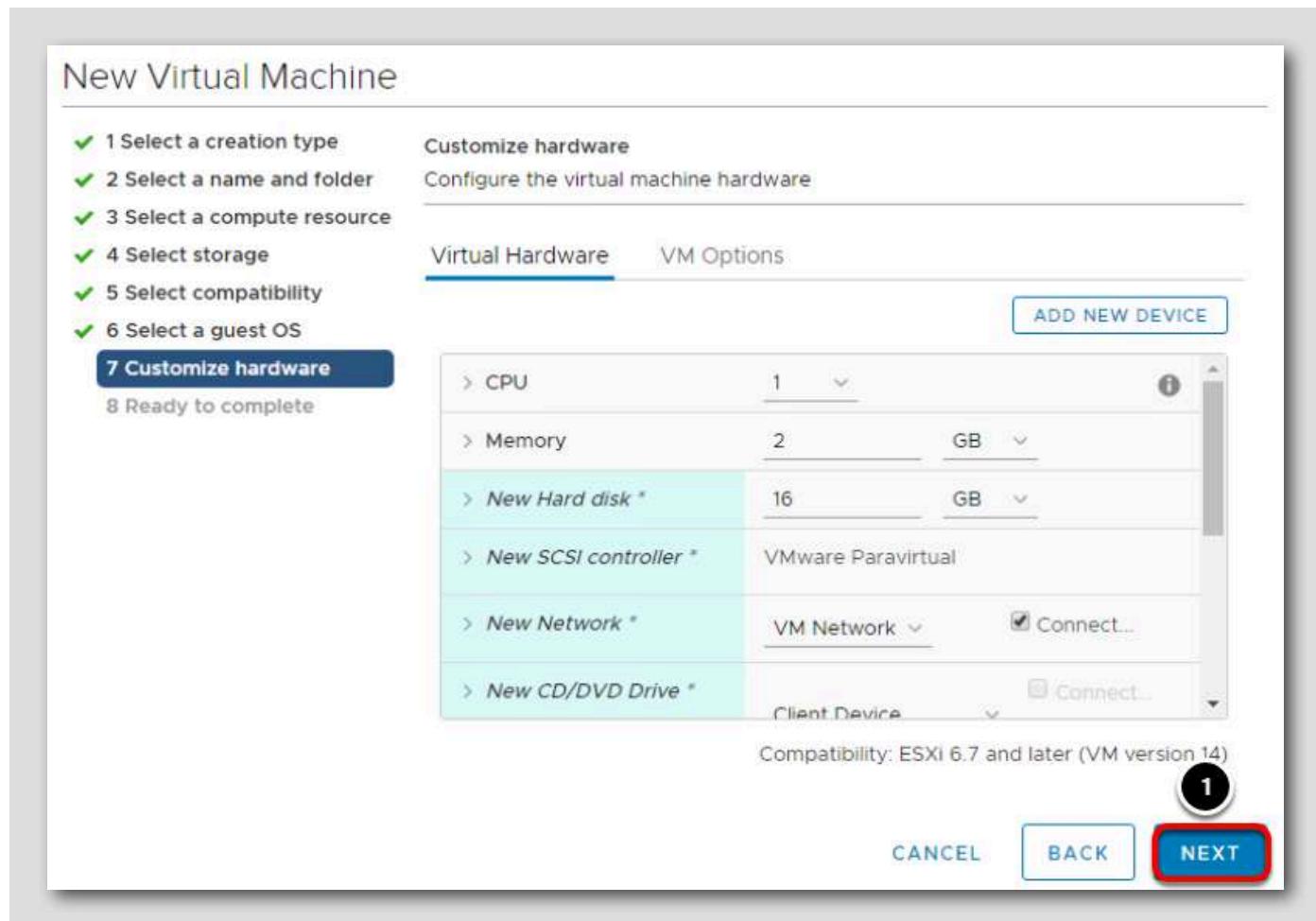
Guest OS



In this step, we will be selecting what operating system we will be installing. When we select the operating system, the supported virtual hardware and recommended configuration is used to create the virtual machine. Keep in mind this does not create a virtual machine with the operating system installed, but rather creates a virtual machine that is tuned appropriately for the operating system you have selected.

1. For the Guest OS Family, select Linux from the drop-down menu.
2. For the Guest OS Version, select VMware Photon OS (64-bit).
3. Click **Next** to continue.

Change Virtual Disk Size.



The recommended virtual hardware settings are shown as the default. These can be modified if needed.

1. Leave the default settings and click Next.

Ready to complete

New Virtual Machine

✓ 1 Select a creation type Ready to complete
✓ 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

Virtual machine name: web-serv01
Folder: RegionA01
Host: esx-01a.corp.local
Datastore: ds-iscsi01
Guest OS name: VMware Photon OS (64-bit)
Virtualization Based Security: Disabled
CPUs: 1
Memory: 2 GB
NICs: 1
NIC 1 network: VM Network
NIC 1 type: VMXNET 3
SCSI controller 1: VMware Paravirtual
Create hard disk 1: New virtual disk
Capacity: 16 GB
Datastore: ds-iscsi01

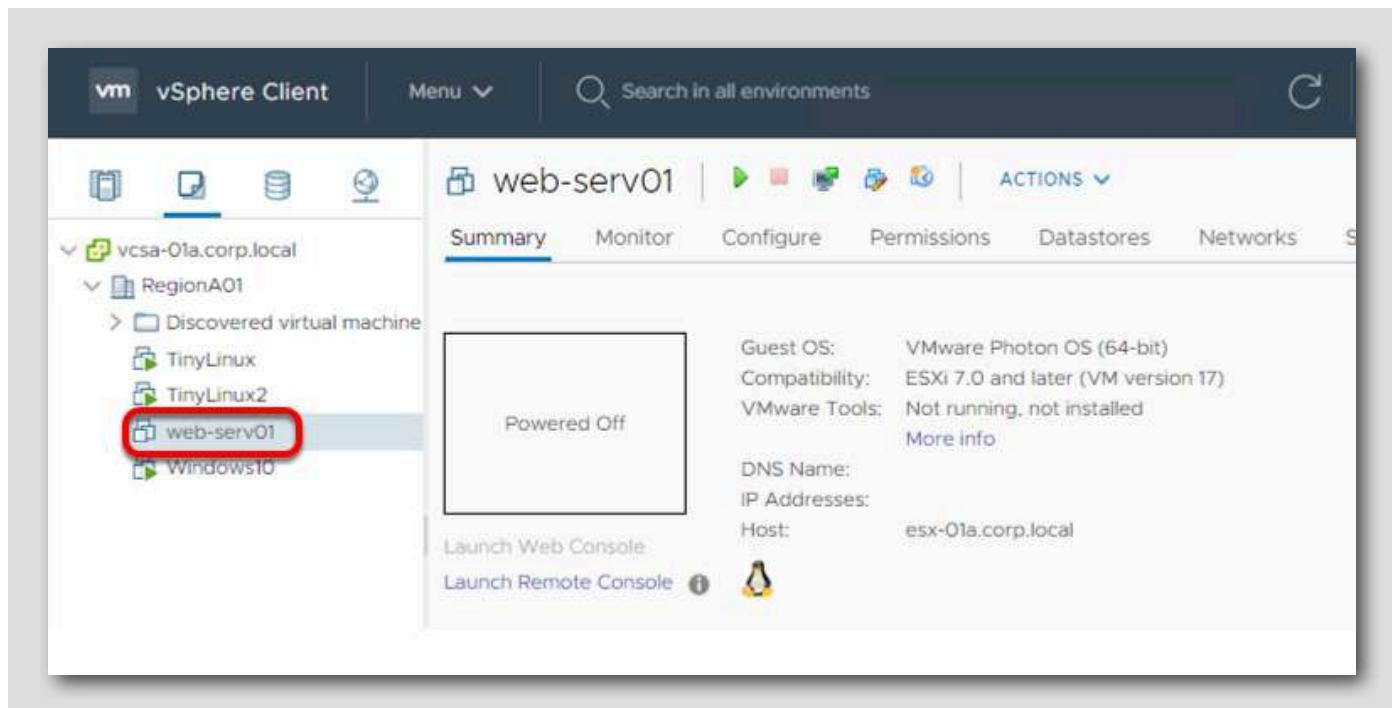
Virtual machine ready. **FINISH** 1

CANCEL BACK FINISH

The settings for the virtual machine can be verified prior to it being created.

1. Click **Finish** to create the virtual machine.

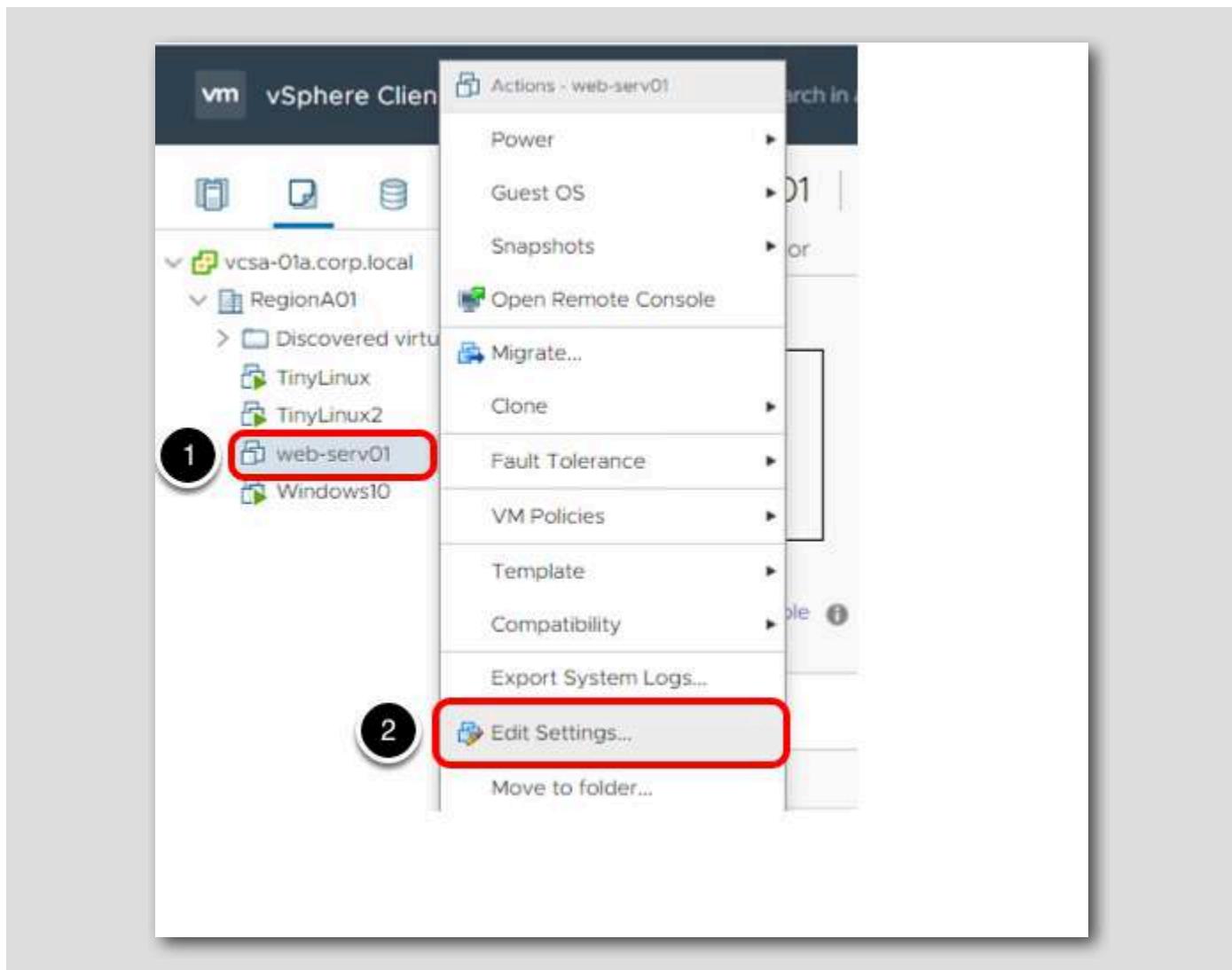
Newly created virtual machine



Congratulations on creating your first virtual machine **web-serv01**!

In the next steps, Photon OS will be installed on the virtual machine.

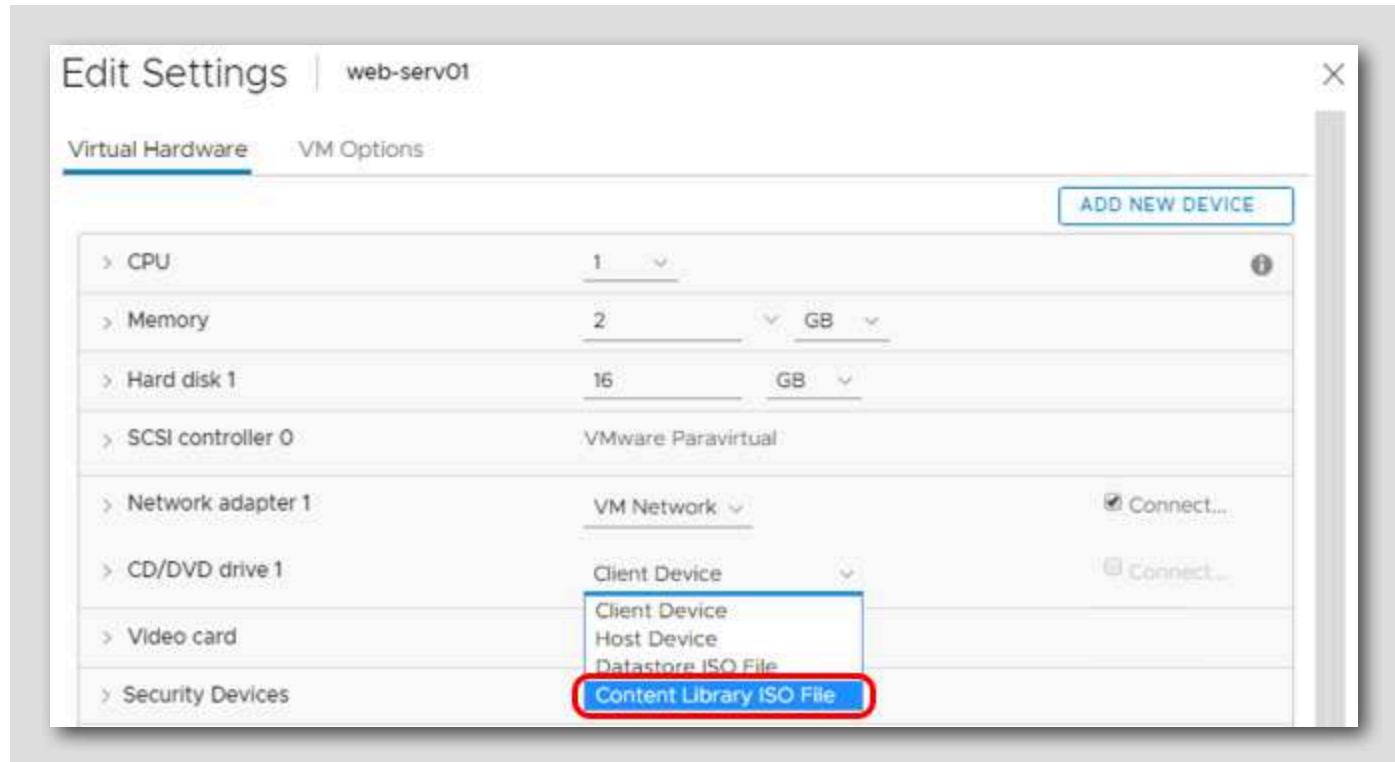
Attaching an ISO to a Virtual Machine



To make it easier to install operating systems on virtual machines, ISO images can be used. These can be kept in the same storage used for virtual machines. In addition, vCenter offers a Content Library as a repository. Content Libraries can then be synchronized to ensure every location is using the same versions.

1. To attach an ISO image to the virtual machine we just created, make sure **web-serv01** is selected.
2. Right-click on **web-serv01** and select **Edit Settings...**

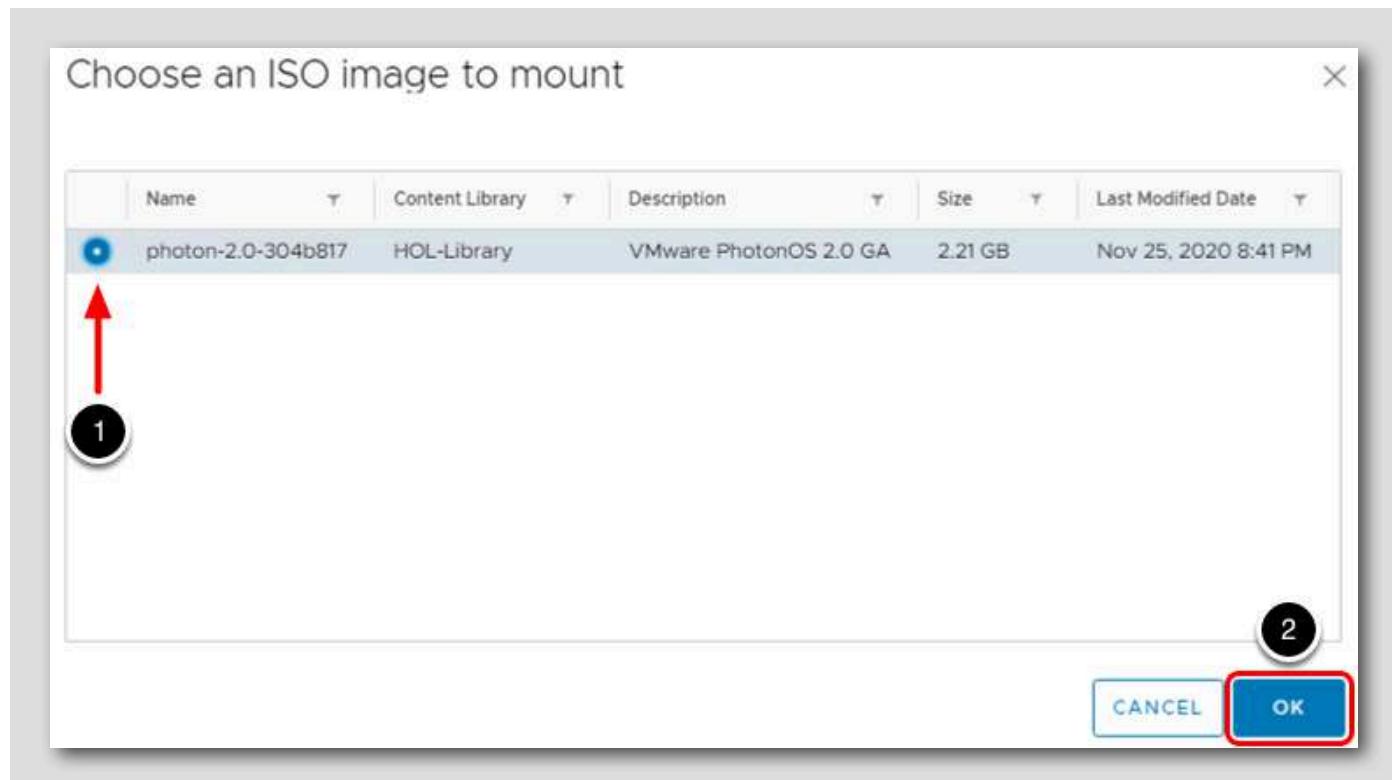
Content Library ISO File



1. From the CD/DVD drive 1 drop-down menu, select Content Library ISO File.

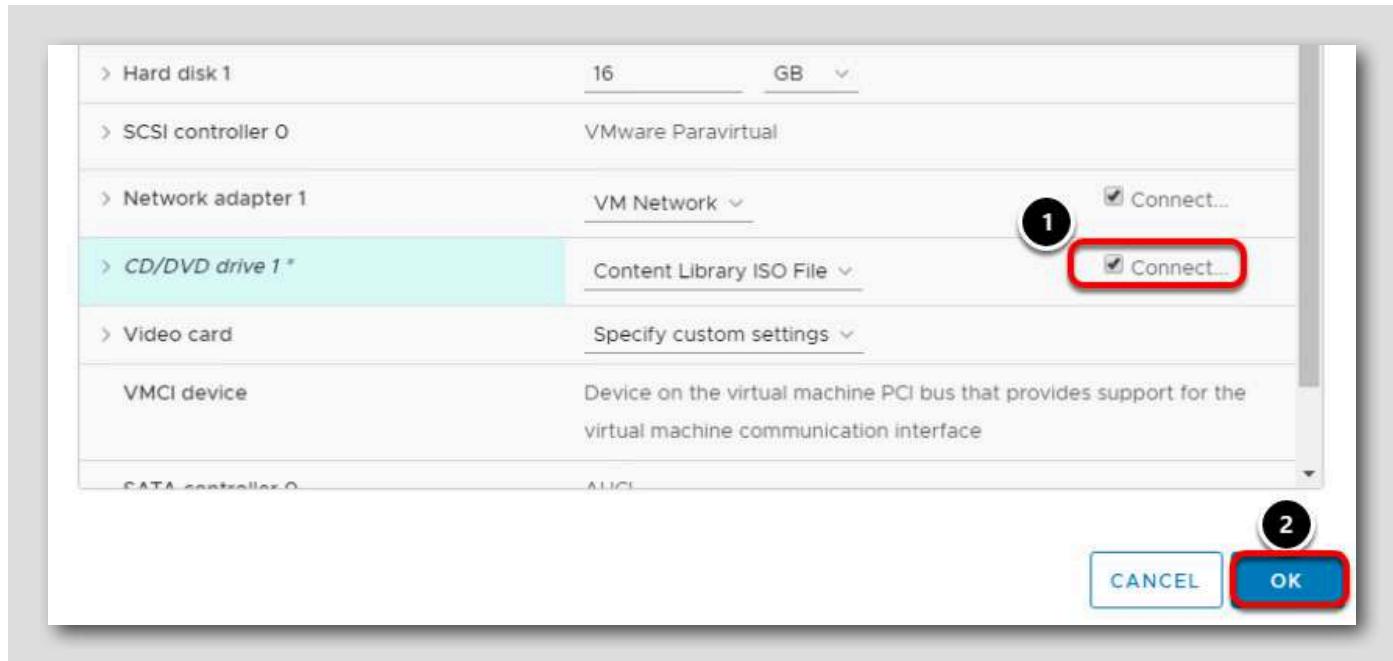
This will open a file explorer to select that file.

Select Photon



1. Click the radio button next to photon-2.0-304b817.
2. Click OK.

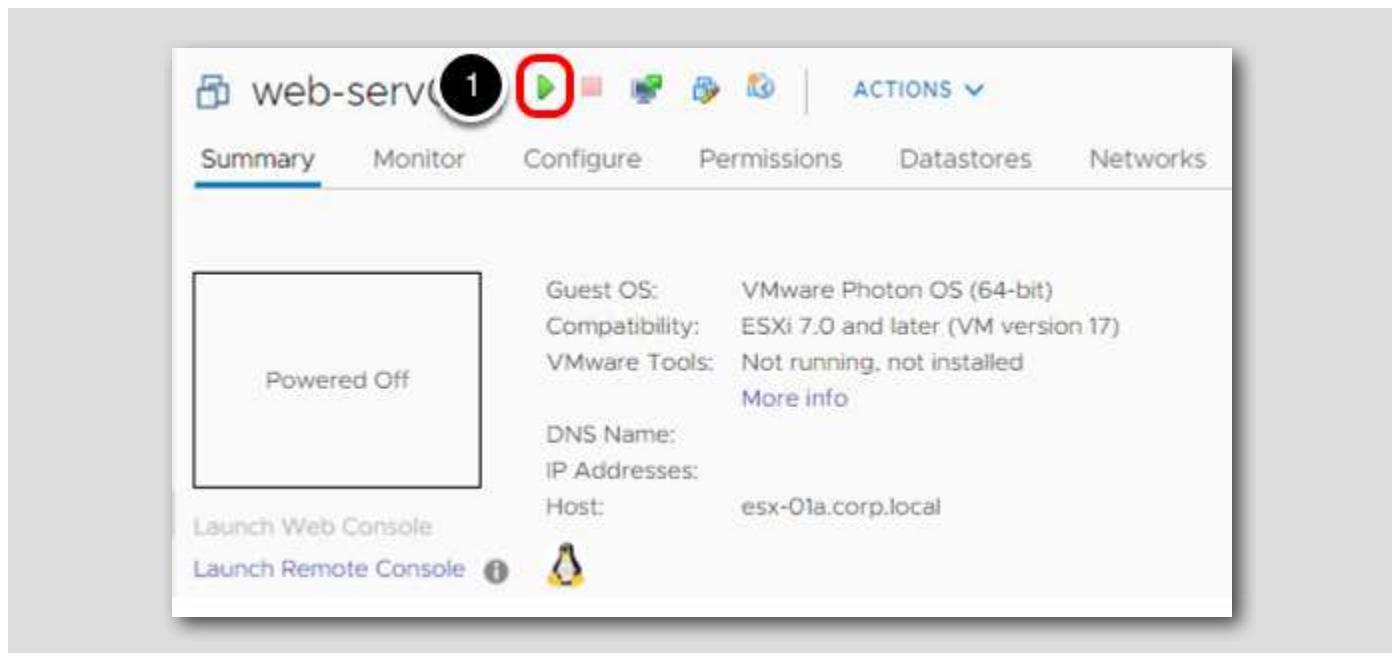
Connect the drive



Finally, we want to attach or connect the ISO image to the virtual machine.

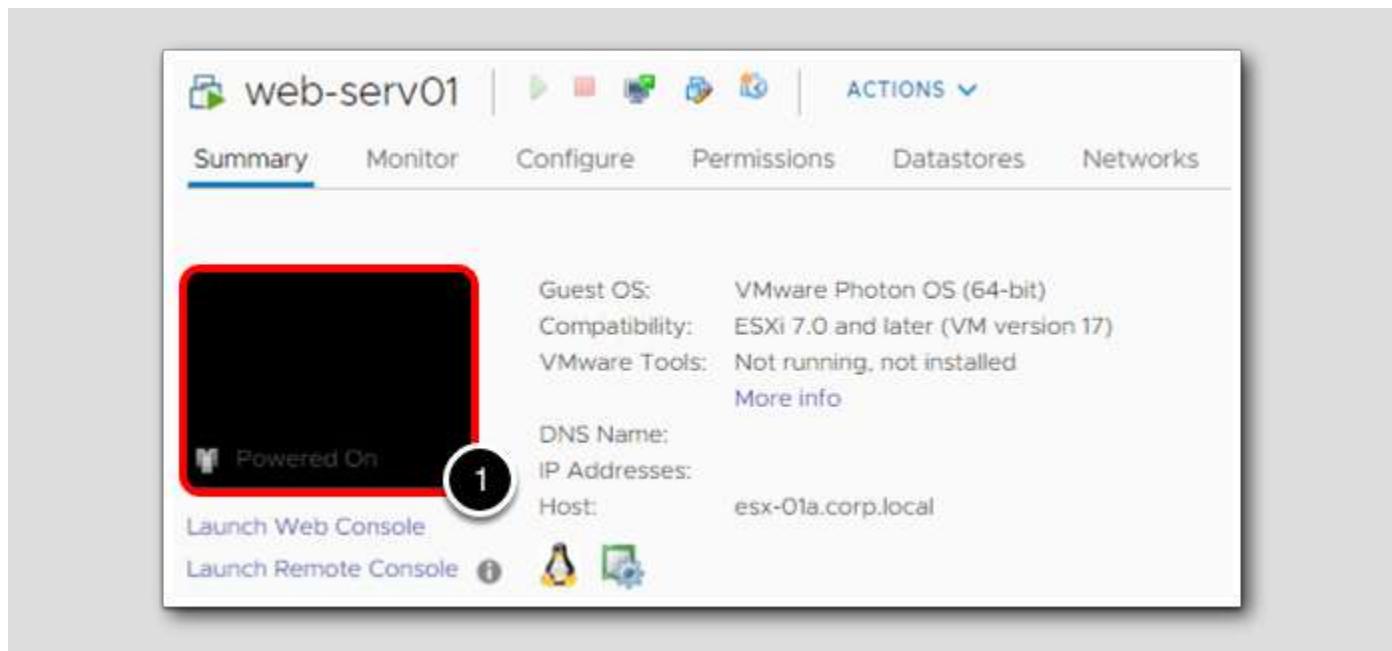
1. Click the Connected check box next to CD/DVD drive 1.
2. Click OK.

Power on web-serv01



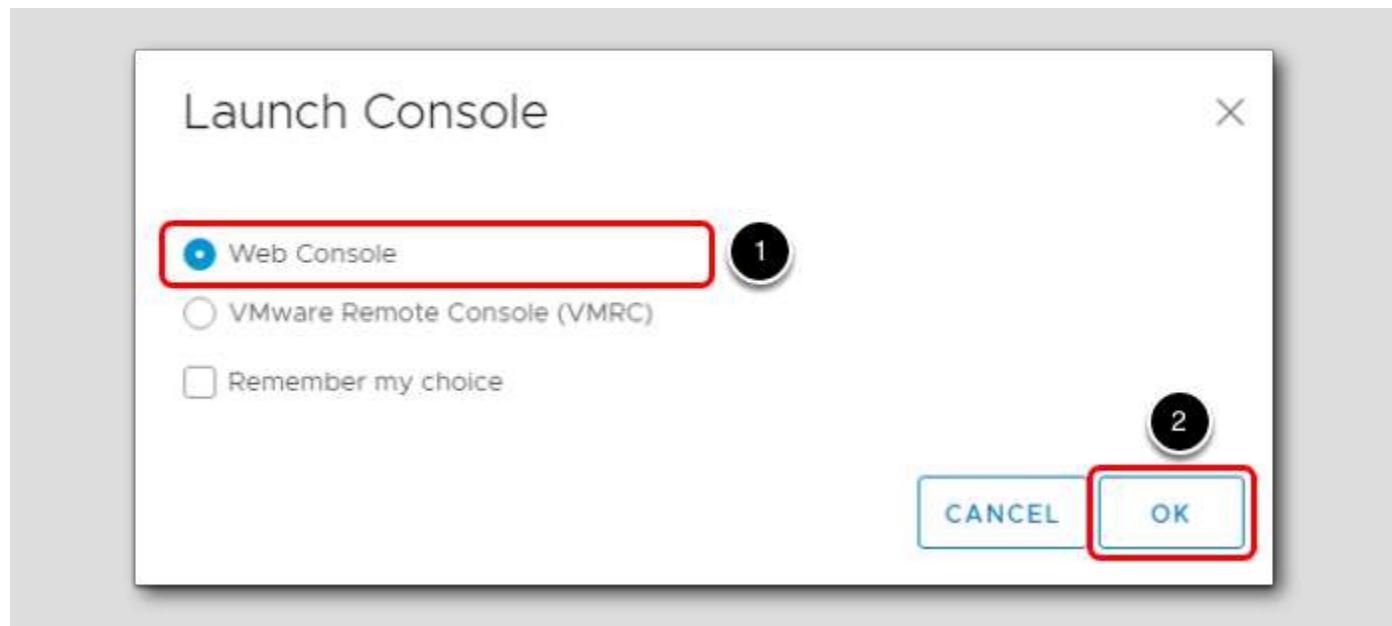
1. Click the green play button to power on the virtual machine and start the installation.

Launch Console



1. To launch the console window, click anywhere in the console window screen.

Web Console

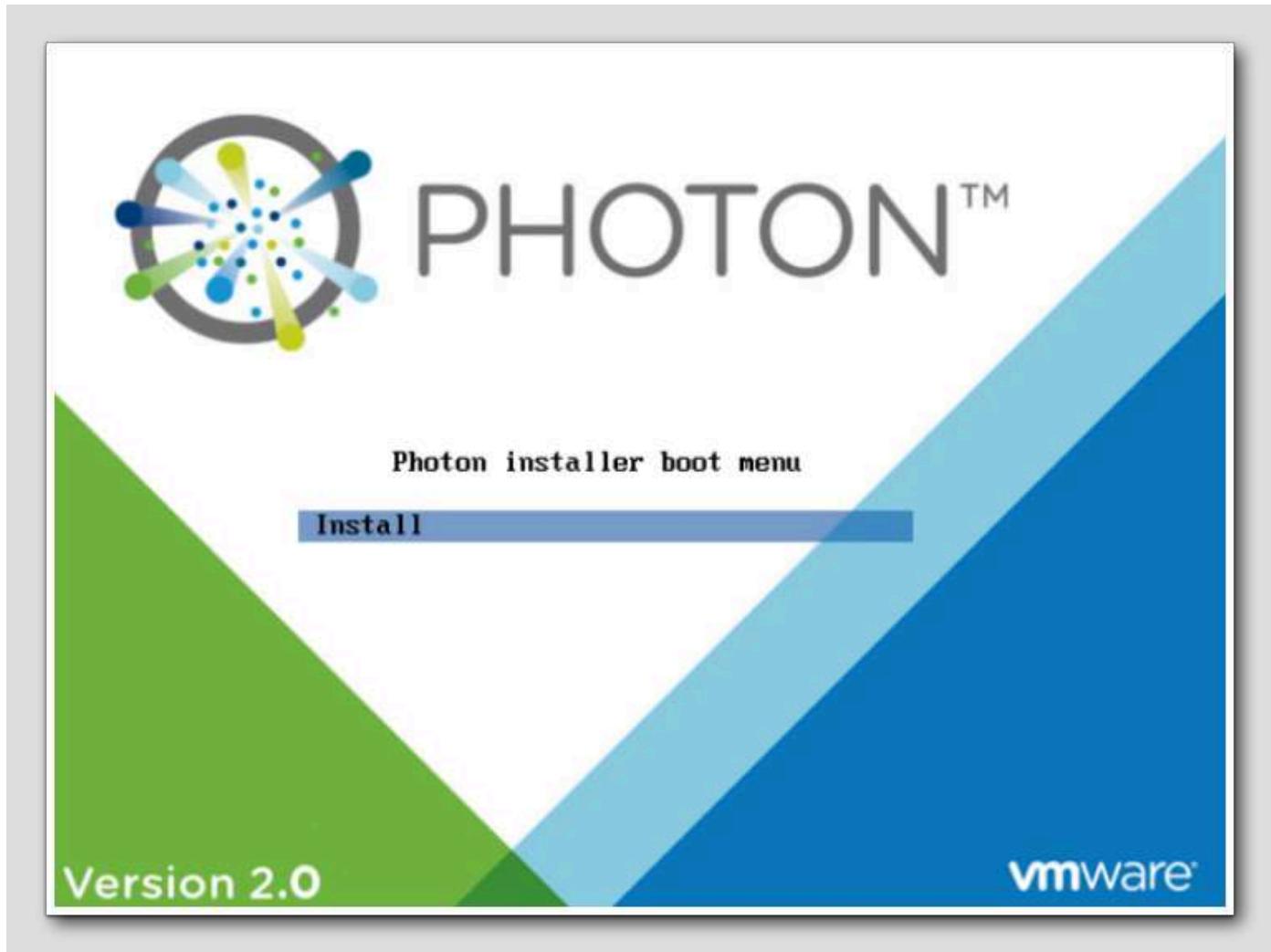


1. Select the **Web Console**.

2. Click **OK**.

Note you also have the option of using the VMware Remote Console (VMRC). This console is a separate application that needs to be installed on your local device as opposed to the Web Console which will launch in a new browser tab. The VMRC can be useful in certain situations when you need more capabilities, like attaching devices or power cycling options.

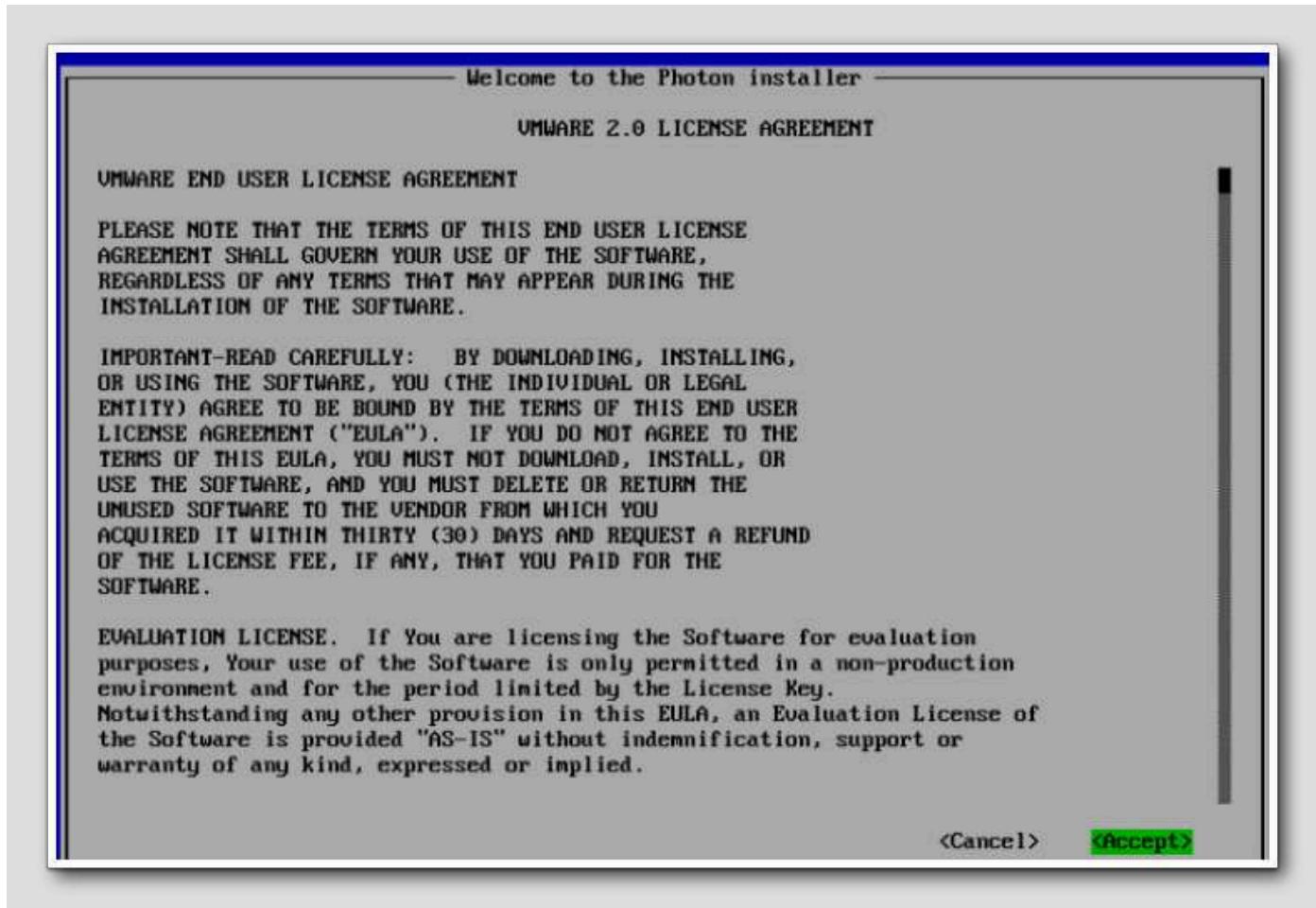
Photon Boot Screen



A new tab will open and you will be presented with the Photon OS boot screen.

1. Press the **Enter** key to start the installation process.

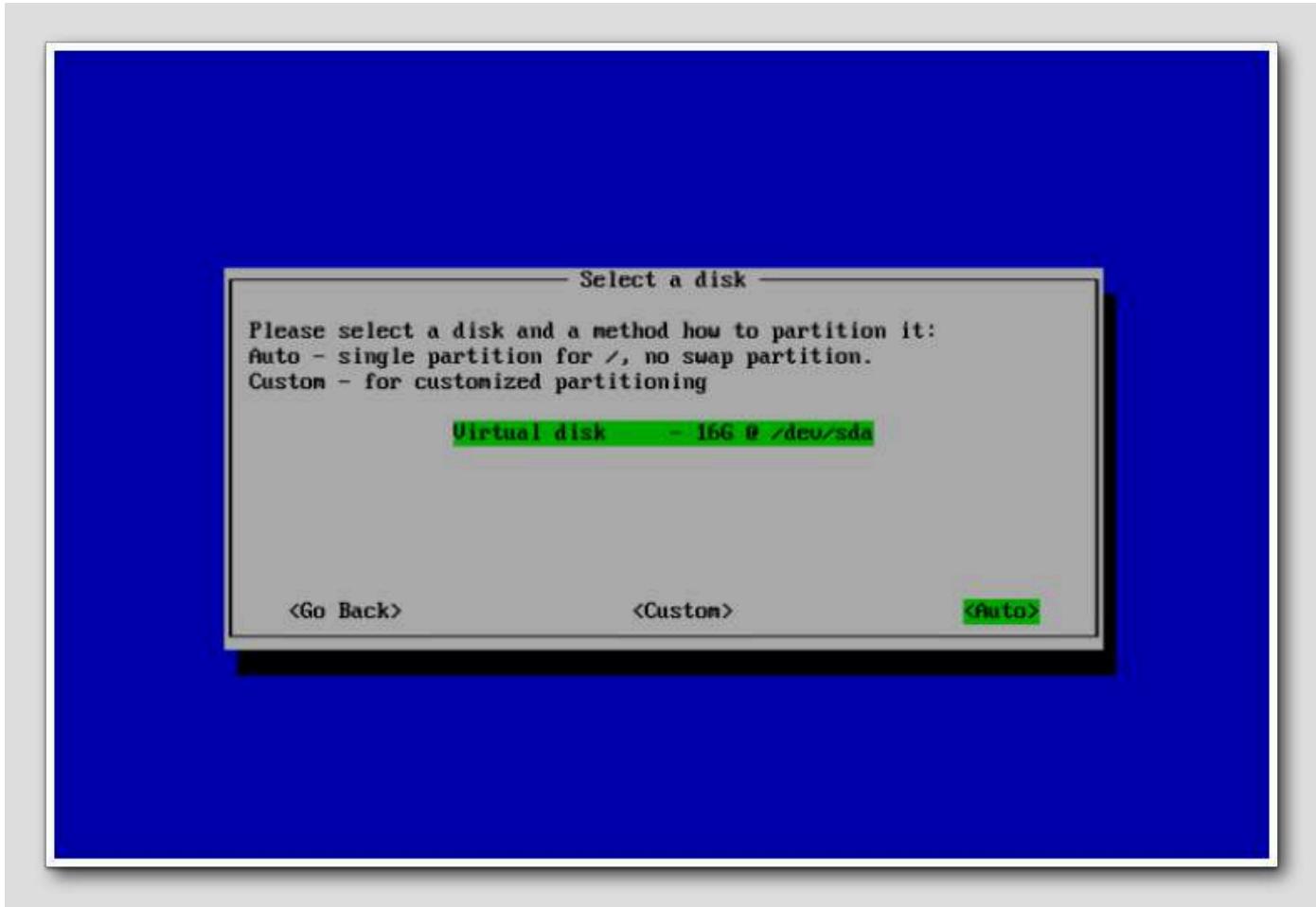
License Agreement



After the boot process is complete, you will be presented with a license agreement.

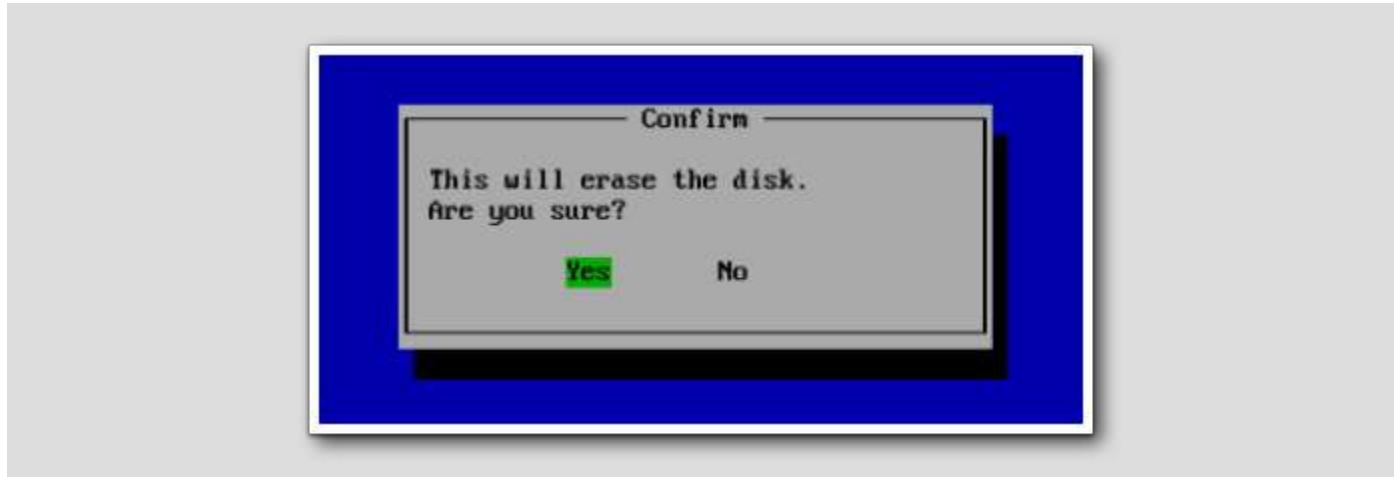
1. Press Enter to accept.

Select Disk



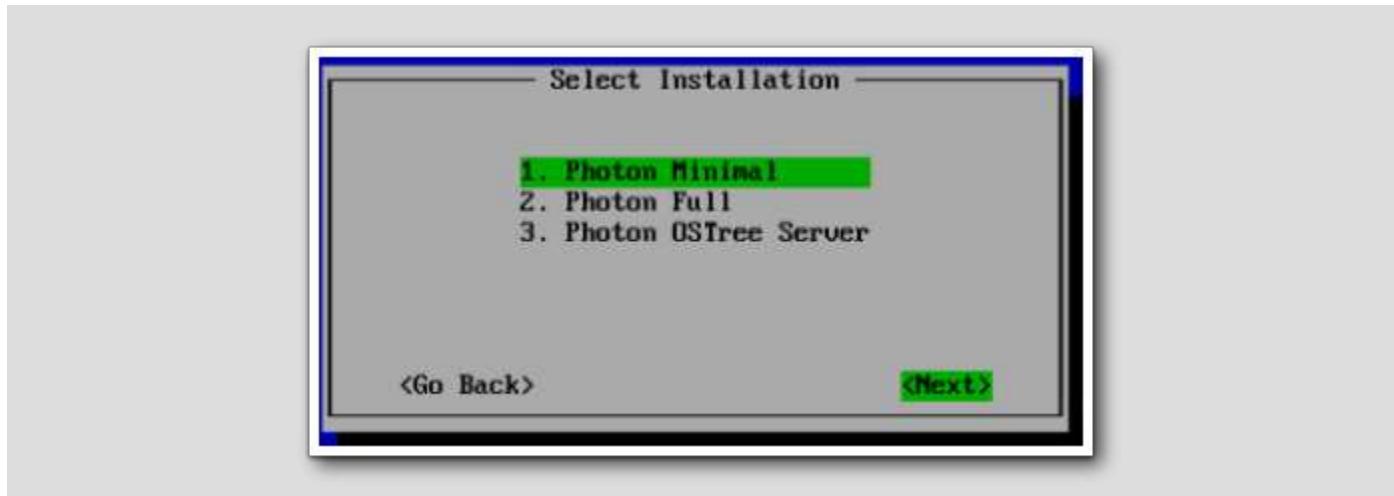
1. Press Enter to accept the selected disk and use the auto partitioning option.

Confirm



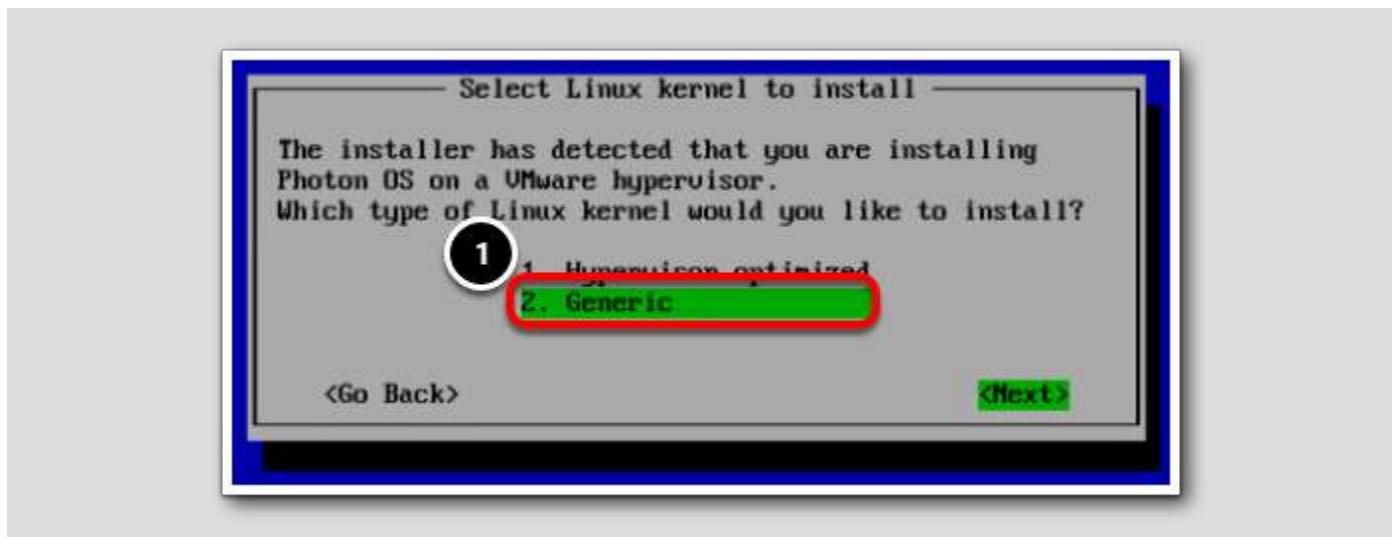
1. Press **Enter** confirm the disk should be erased.

Select Installation



1. At the Select Installation screen, make sure the default option of 1. Photon Minimal is selected.
2. Press the **Enter** key.

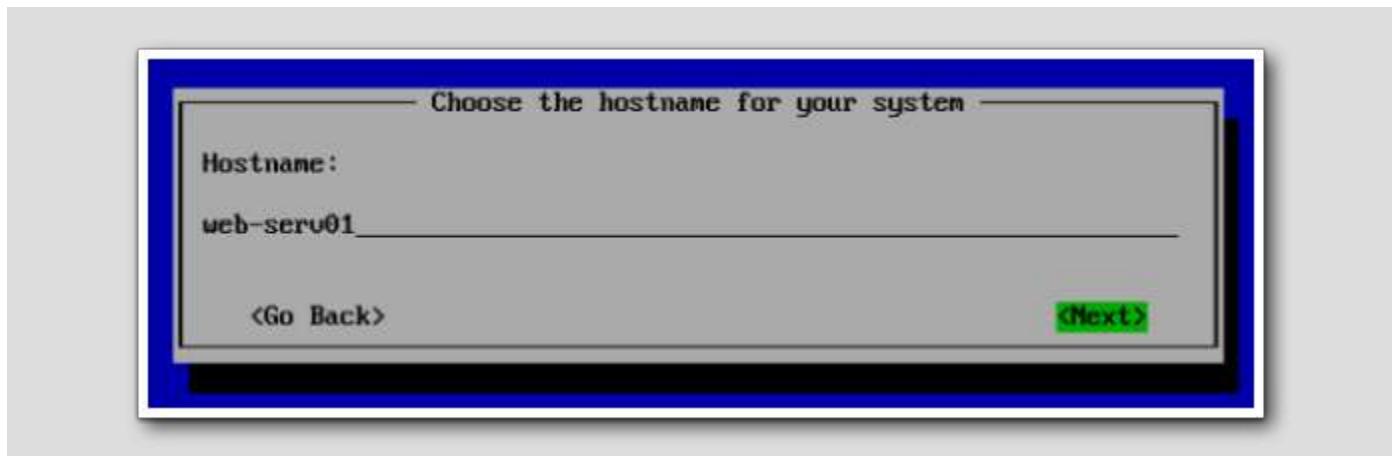
Linux Kernel



1. Use the arrow key to select 2. Generic.
2. Press the Enter key.

NOTE: If 1. Hypervisor optimized is selected, the virtual machine will not boot. This is due to the unique environment the Hands-on Labs are running in.

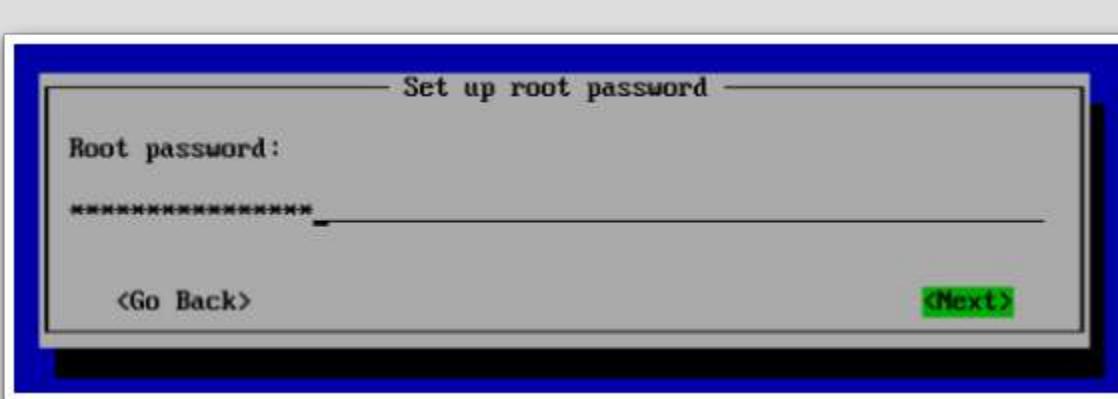
Rename Host



1. Use the Backspace key to remove the default hostname.
2. Type **web-serv01**.
3. Press the **Enter** key.

Password

[78]

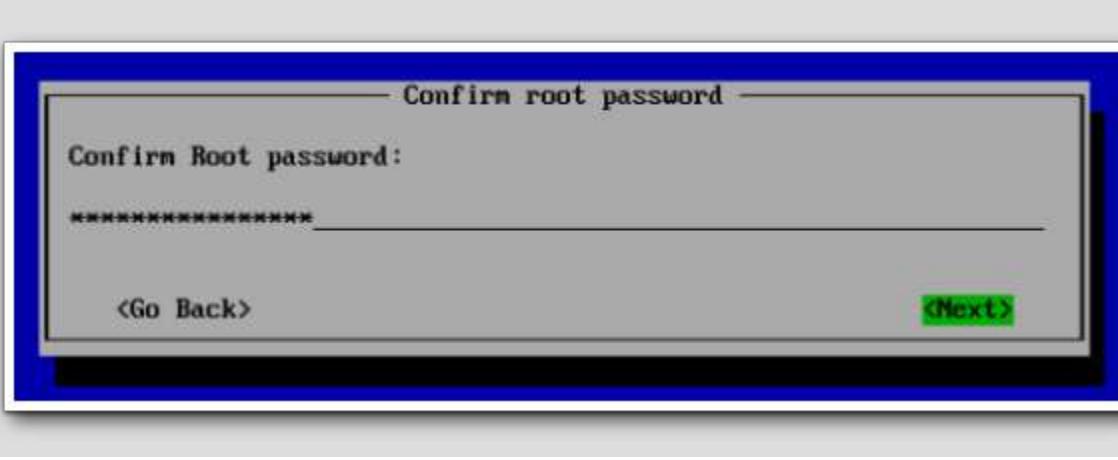


1. For the password, use **VMware1!VMware1!**

Note that Photon requires a complex, non-dictionary password, which is why the typical password is being repeated.

Confirm Password

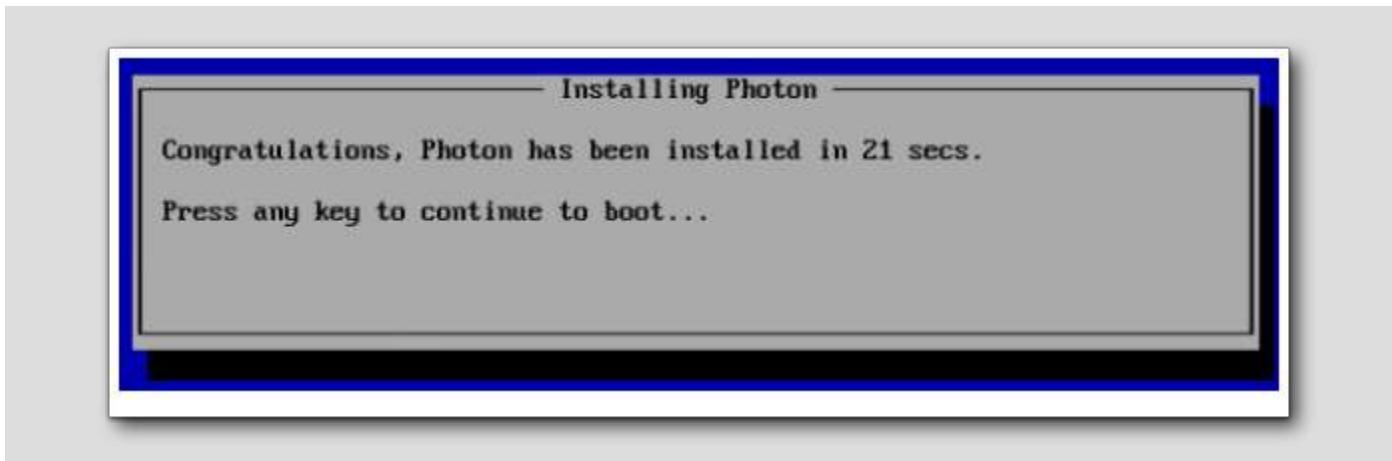
[79]



1. Type VMware1!VMware1! again to confirm the password.
2. Press the Enter key.

Installation Complete

[80]

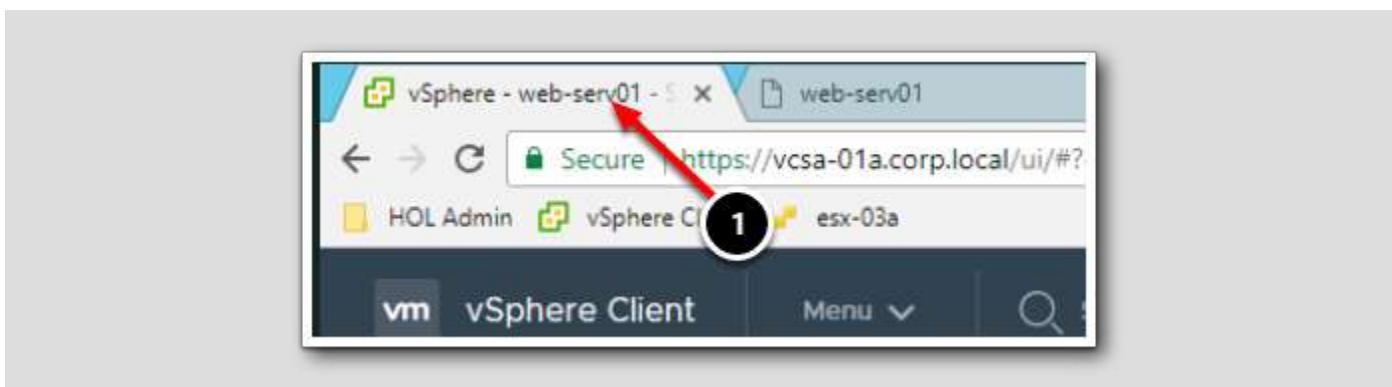


After a minute or two, the installation will be complete.

Press a key to reboot the virtual machine. After a minute or two, the system should boot the login prompt.

vSphere Tab

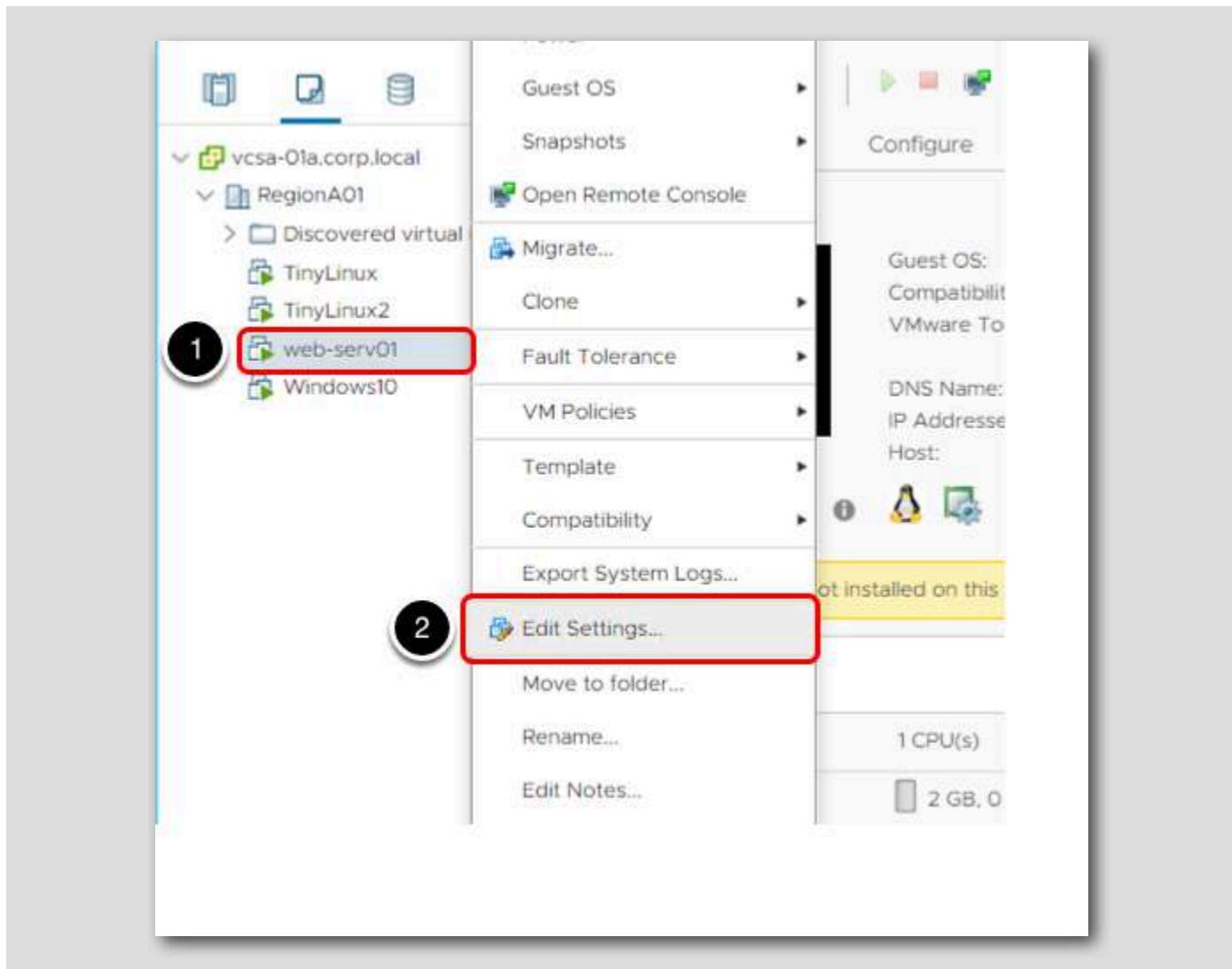
[81]



Now that the operating system has been installed and is up and running, the ISO image needs to be disconnected from the virtual machine.

1. Select the vSphere- web-serv01 tab.

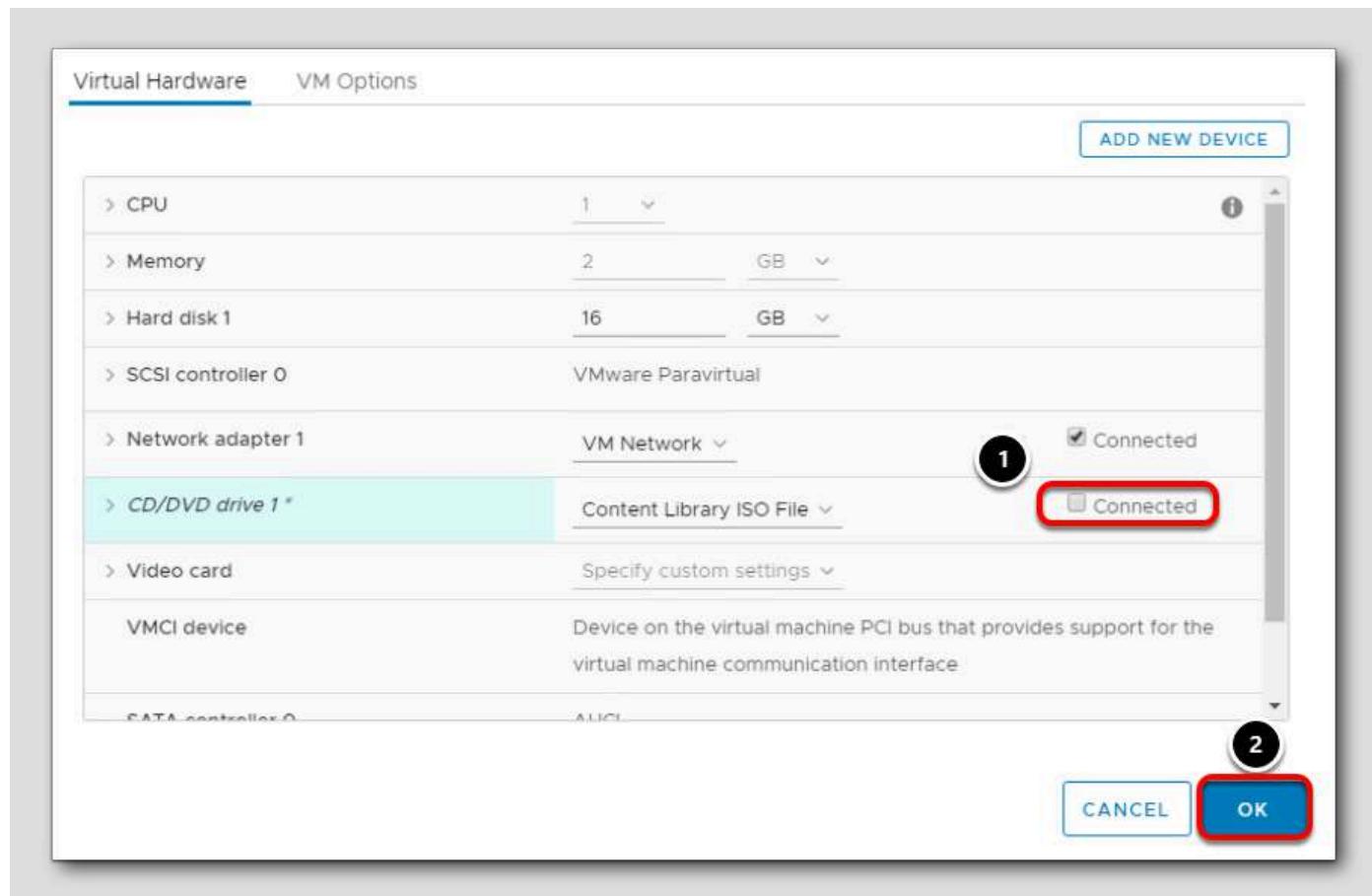
Edit Settings



Make sure **web-serv01** is still highlighted.

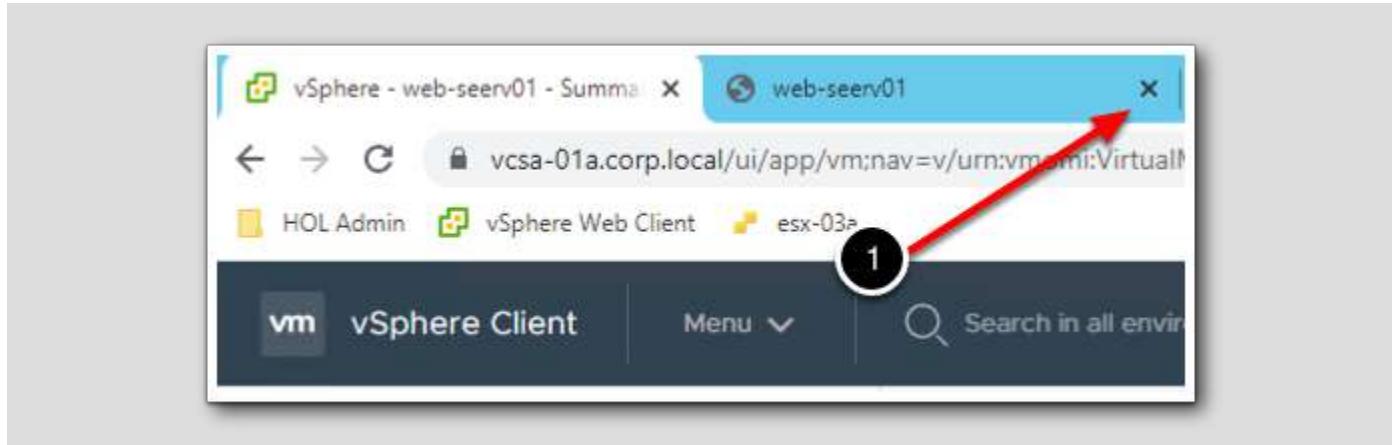
1. Right-click on **web-serv01**.
2. Select **Edit Settings...**

Disconnect CD/DVD



1. Uncheck the Connected box next to CD/DVD drive 1.

web-serv01 Console



1. Click the 'X' to close the console window for web-serv01.

Cloning Virtual Machines and Using Templates

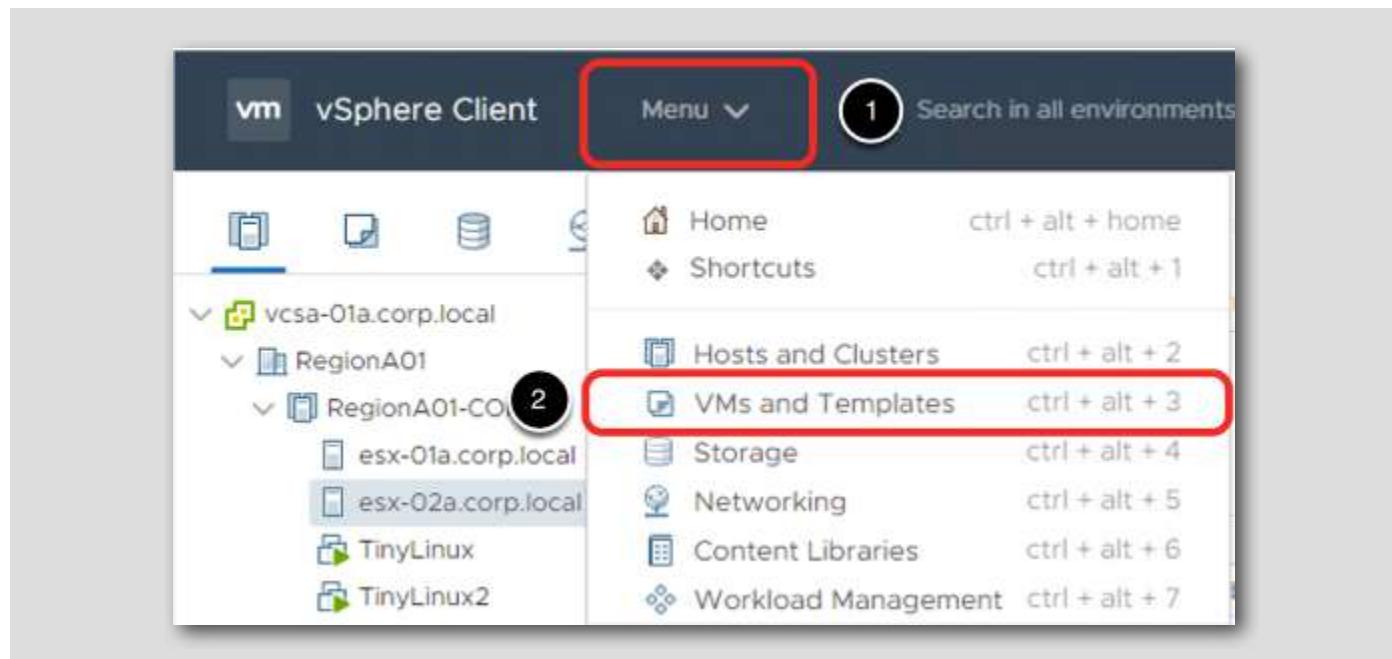
VMware provides several ways to provision vSphere virtual machines. In the last lesson, you saw how to create a virtual machine and manually install the operating system.

The virtual machine that was created can then be used as a base image from which to clone other virtual machines. Cloning a virtual machine can save time if you are deploying many similar virtual machines. You can create, configure, and install software on a single virtual machine. You can clone it multiple times, rather than creating and configuring each virtual machine individually.

Another provisioning method is to clone a virtual machine to a template. A template is a master copy of a virtual machine that you can use to create and provision virtual machines. Creating a template can be useful when you need to deploy multiple virtual machines from a single baseline but want to customize each system independently of the next. A common value point for using templates is to save time. If you have a virtual machine that you will clone frequently, make that virtual machine a template, and deploy your virtual machines from that template.

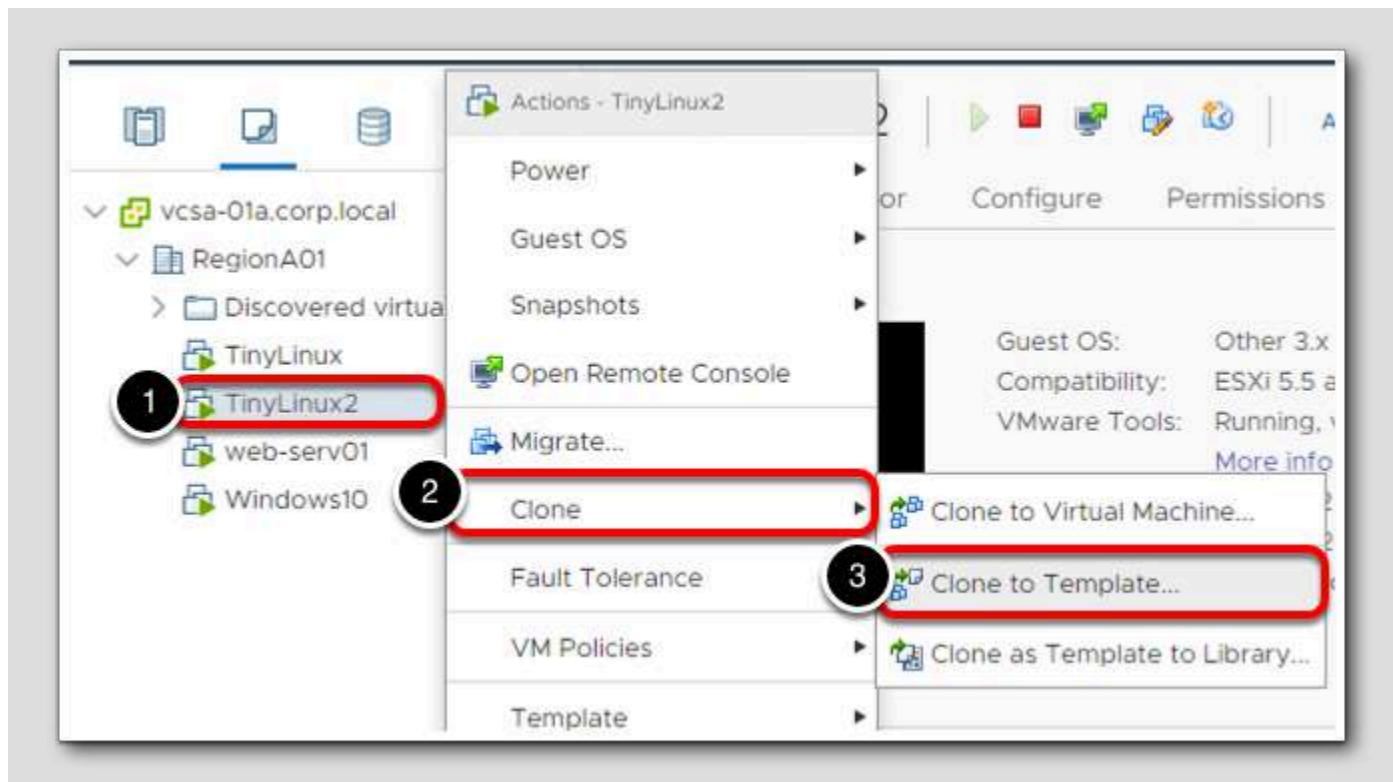
In this lesson, you will clone an existing Virtual Machine to a Template and deploy a new Virtual Machine from that Template.

Navigate to the VMs and Templates management pane



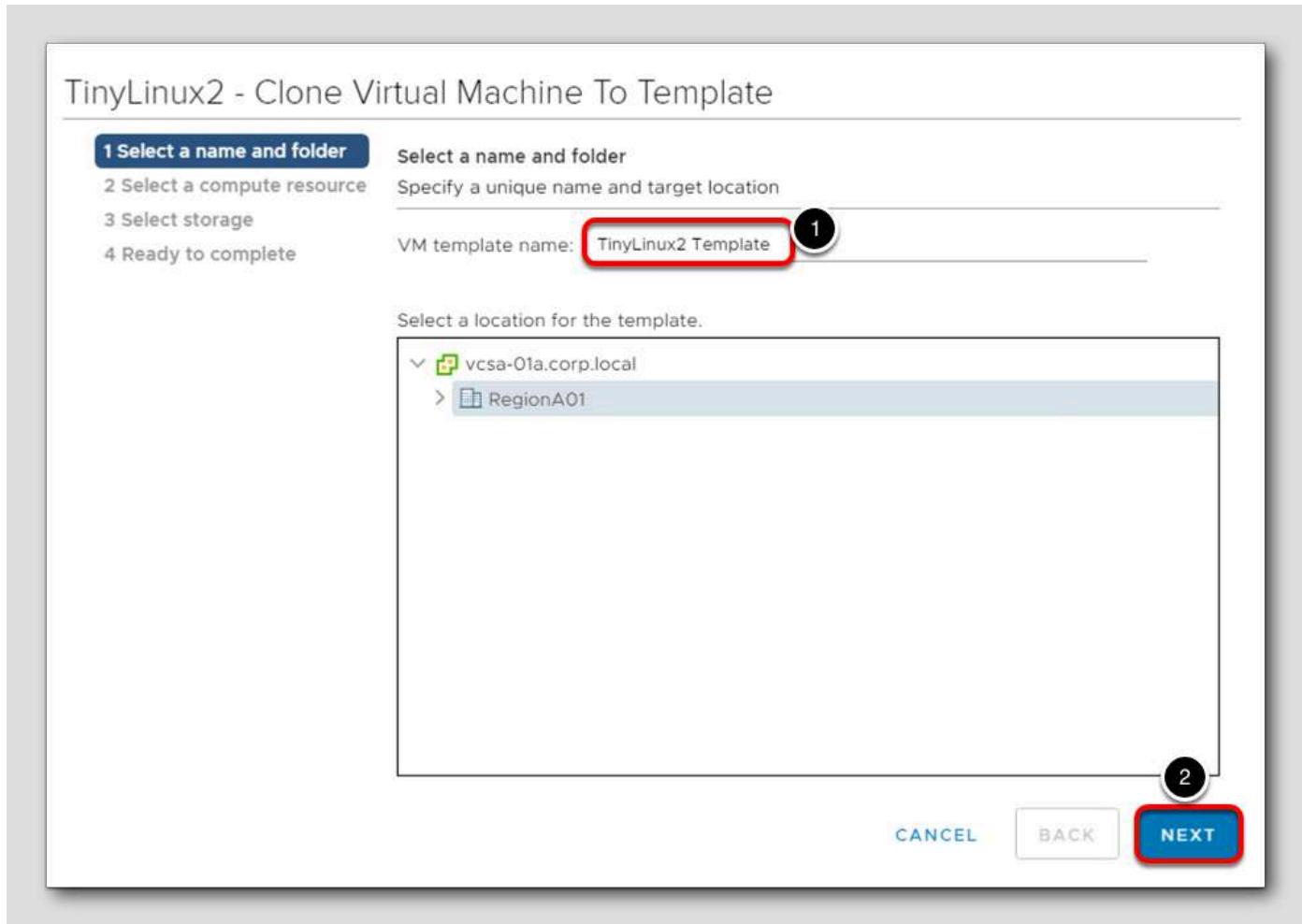
1. Click on **Menu**.
2. Select **VMs and Templates**.

Launch the Clone Virtual Machine to Template wizard



1. Right-click the Virtual Machine **TinyLinux2**.
2. Select **Clone**.
3. Select **Clone to Template...**

Select a name and folder

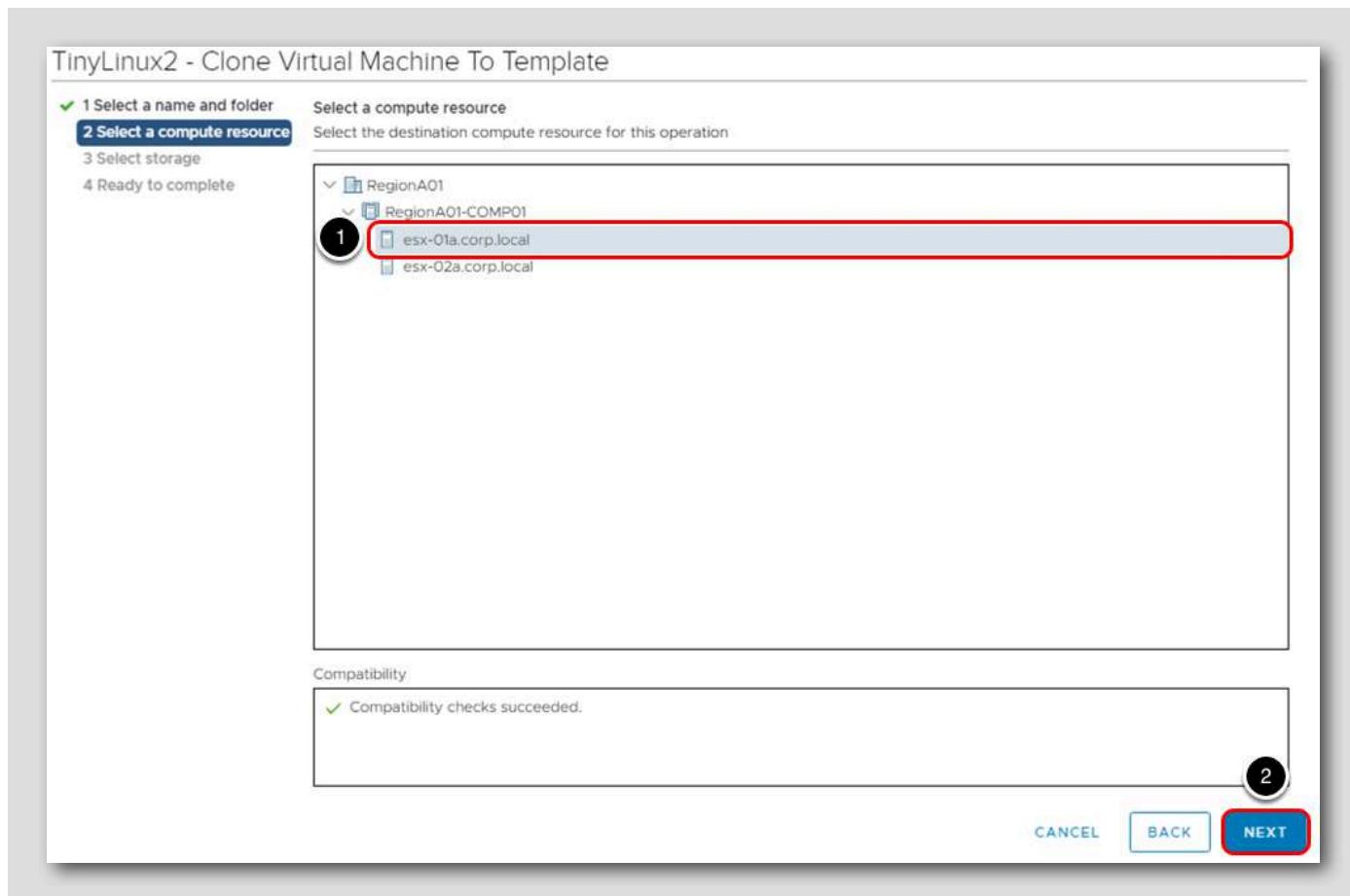


1. In the Clone Virtual Machine to Template wizard, provide a name for the Template - TinyLinux2 Template

Please leave the location as RegionA01 for this lab.

2. Click Next

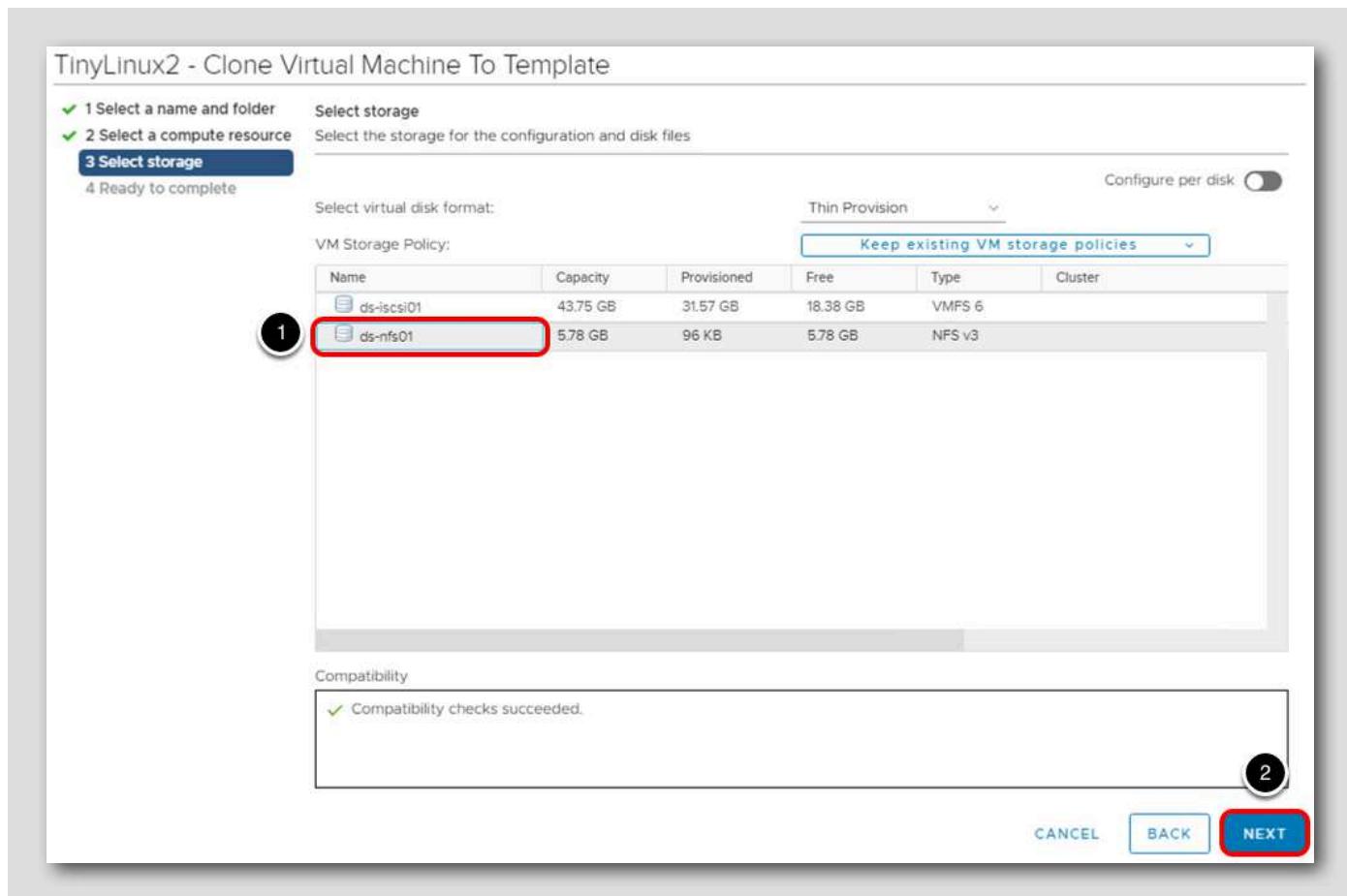
Select Compute Resource



Select a compute resource:

1. Choose **esx-01a.corp.local**.
2. Click **Next**.

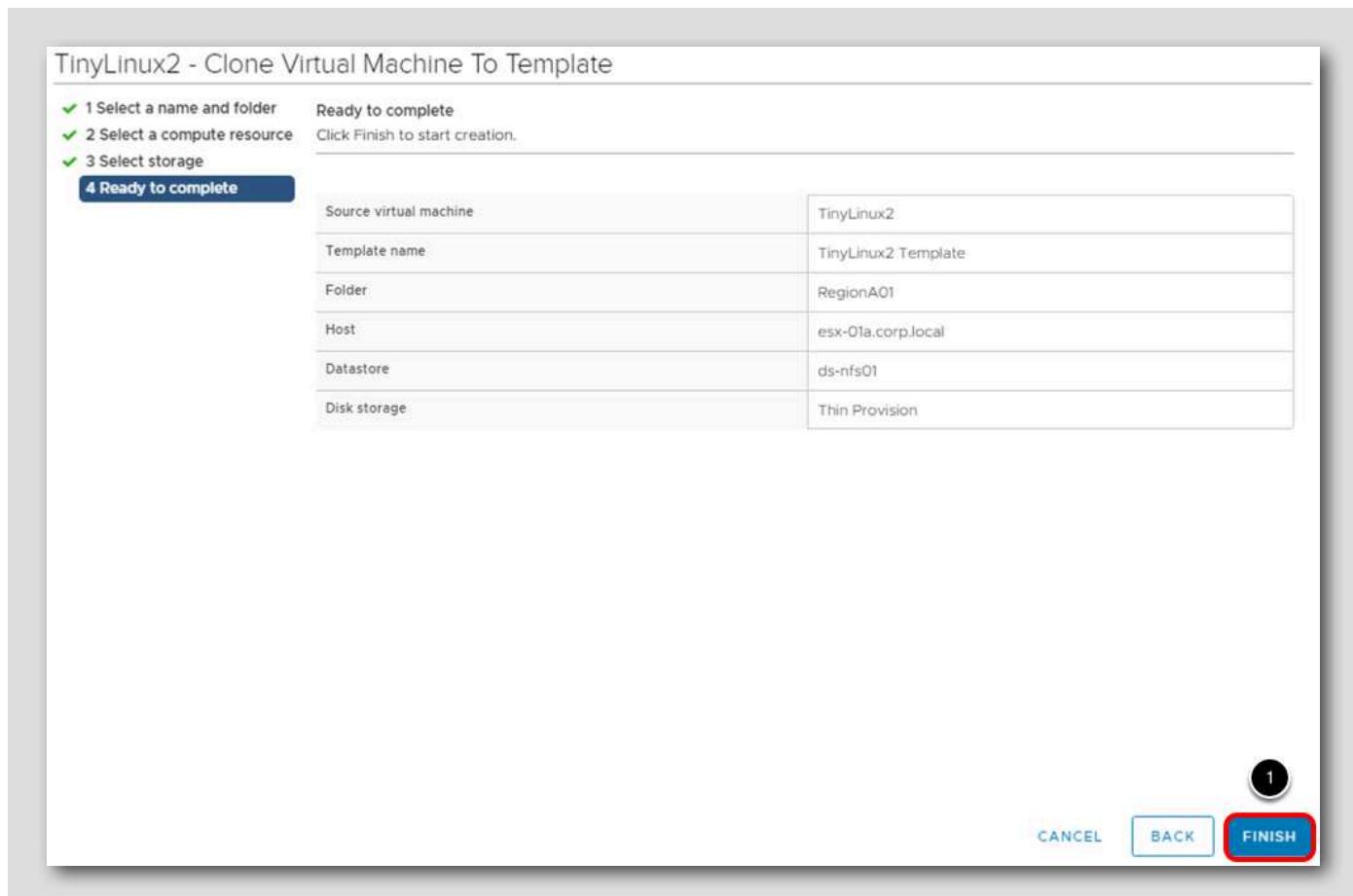
Select Storage



1. Select ds-nfs01 as the datastore.

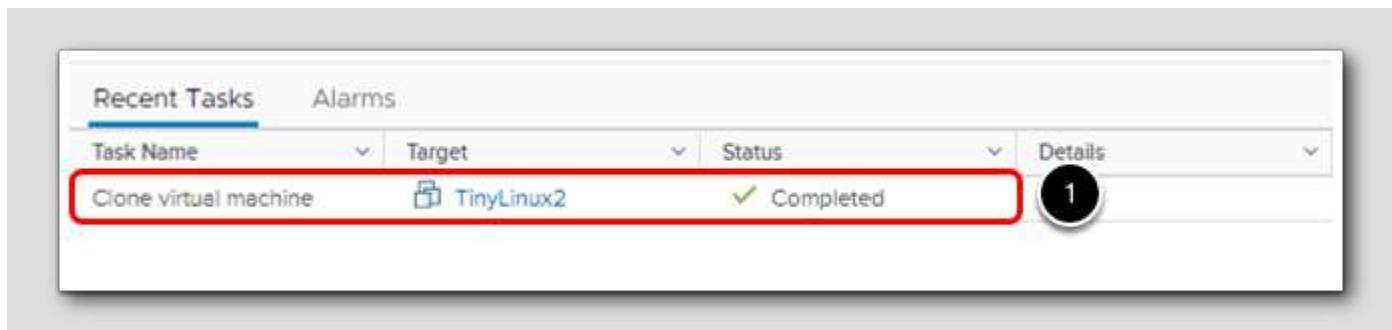
2. Press the Next button.

Review the VM Template Settings



1. Review the VM Template settings and press the Finish button.

Monitor task progress

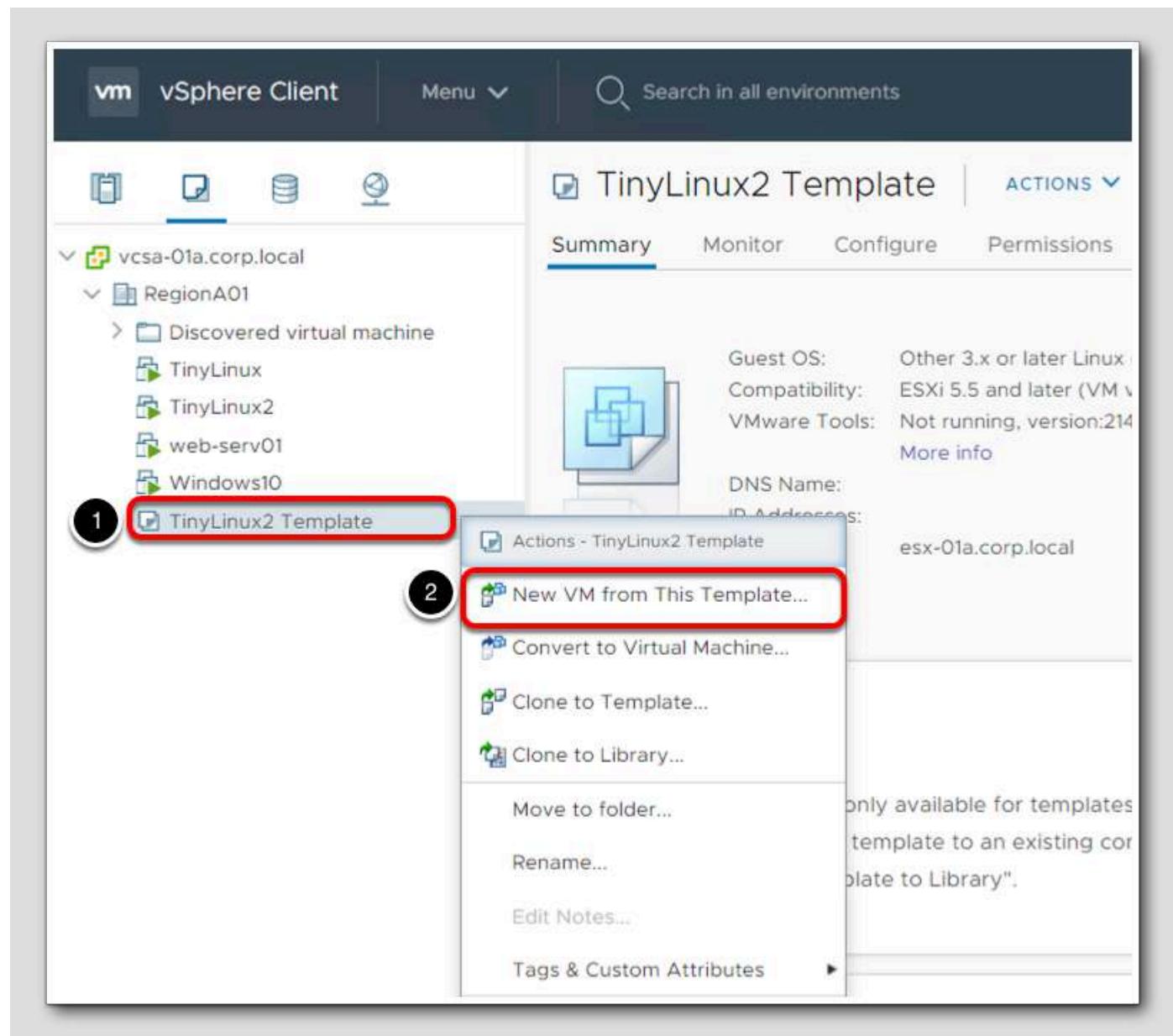


1. You can monitor the progress in the recent task window.

A screenshot of the vSphere Client interface showing the inventory pane. On the left, there's a tree view of the vSphere environment. A red box highlights the 'VM and Templates' icon (represented by a blue square with a white icon) and the '1' notification badge above it. Below the tree, a red box highlights the 'TinyLinux2 Template' object under the 'RegionA01' folder. On the right, the details for the 'TinyLinux2 Template' are shown in a card. The card includes sections for Summary, Monitor, Configure, Permissions, Datastores, and Versioning. The 'Summary' section shows the template's configuration: Guest OS: Other 3.x or later Linux (32-bit), Compatibility: ESXi 5.5 and later (VM version 10), VMware Tools: Not running, version:2147483647 (Guest Managed), DNS Name:, IP Addresses:, Host: esx-01a.corp.local. Below the summary is a 'Versioning' section with a note: 'Versioning information is only available for templates in a Published or Local Content Library. To add a template to an existing content library, select a VM and select "Clone as Template to Library".'

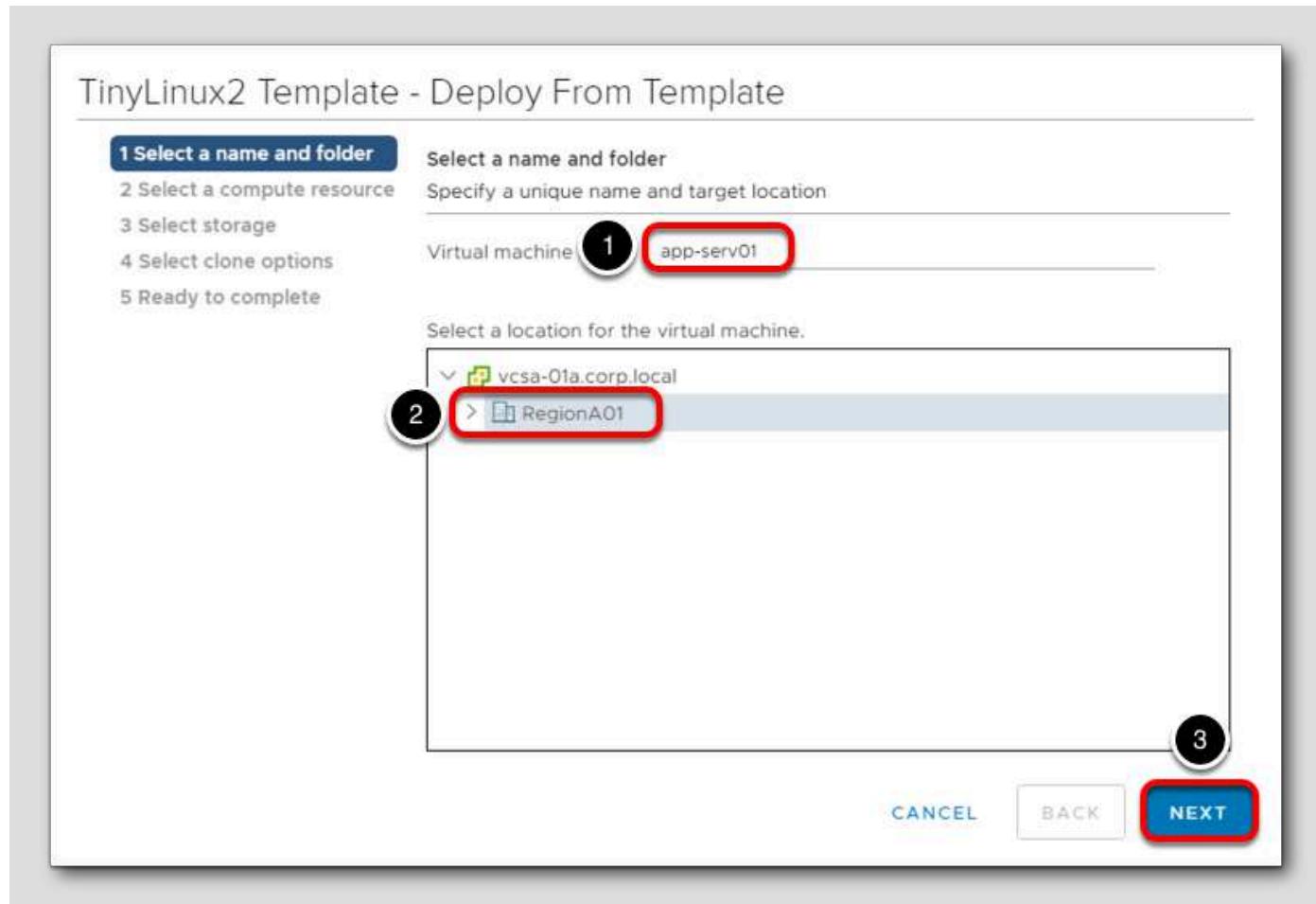
1. Once the task has been completed, click on the VM and Templates icon. **TinyLinux 2 Template** object should be on the inventory pane.

Launch the Deploy From Template wizard



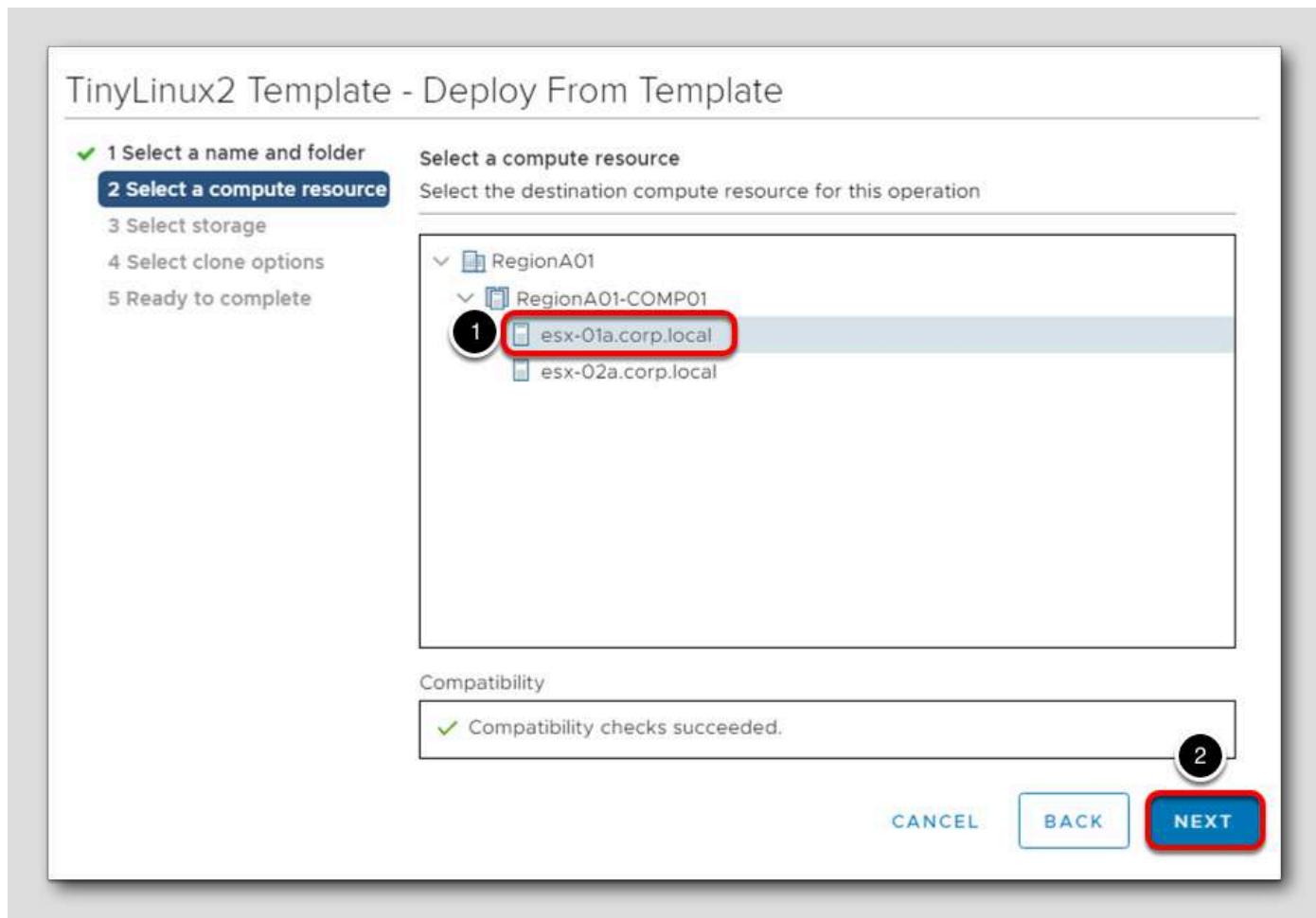
1. Select the Template, TinyLinux2 Template
2. Right click on TinyLinux2 Template and select New VM from This Template.

Select a name and folder



1. Enter **app-serv01** for the name of the new virtual machine.
2. Leave the default location of **RegionA01** Datacenter.
3. Click the **NEXT** button.

Select compute resource



1. Select esx-01a.corp.local.

2. Click **Next**.

Select storage

TinyLinux2 Template - Deploy From Template

✓ 1 Select a name and folder
✓ 2 Select a compute resource
3 Select storage
4 Select clone options
5 Ready to complete

Select storage
Select the storage for the configuration and disk files

Configure per disk

Select virtual disk format: Same format as source

VM Storage Policy: Keep existing VM storage poli... ▾

Name	Capacity	Provisioned	Free
ds-iscsi01	43.75 GB	49.65 GB	2.27 GB
ds-nfs01	5.78 GB	742.2 MB	5.76 GB

Compatibility

✓ Compatibility checks succeeded.

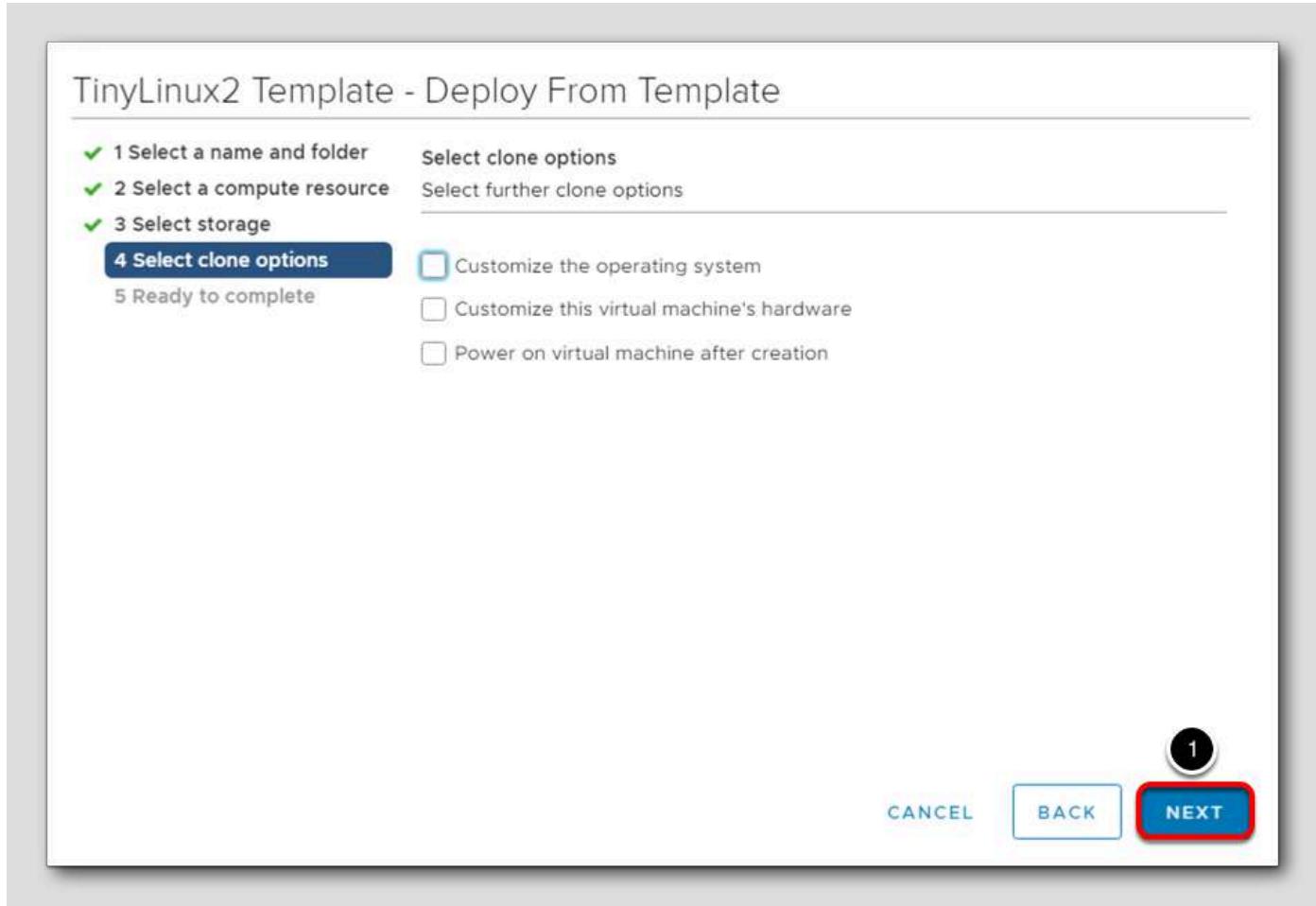
1 2

CANCEL BACK **NEXT**

1. Leave the default datastore selected, **ds-iscsi01**.

2. Click **Next**.

Select clone options



When cloning a virtual machine from a template, the guest operating system and virtual hardware can be modified. For this example, we will not customize the operating system or hardware.

1. Click **Next**.

Ready to complete

TinyLinux2 Template - Deploy From Template

✓ 1 Select a name and folder Ready to complete
✓ 2 Select a compute resource
✓ 3 Select storage
✓ 4 Select clone options
5 Ready to complete

Click Finish to start creation.

Source template	TinyLinux2 Template
Virtual machine name	app-serv01
Folder	RegionA01
Host	esx-01a.corp.local
Datastore	ds-iscsi01
Disk storage	Same format as source

1

CANCEL BACK FINISH

1. Review the deployment options and then click Finish.

Monitor task progress

The screenshot shows the vSphere Client interface. On the left, the inventory pane displays a tree structure of vCenter servers and datacenters. A red circle labeled '2' highlights the 'app-serv01' virtual machine under the 'RegionA01' datacenter. In the center, the 'Summary' tab for 'app-serv01' is selected, showing details like Guest OS (Other 3.x or later Linux (32-bit)), Compatibility (ESXi 5.5 and later (VM version 10.0.0.0)), and Host (esx-01a.corp.local). Below the summary, there are 'Launch Web Console' and 'Launch Remote Console' buttons. On the right, the 'Recent Tasks' window is open, showing a table of completed tasks. A red circle labeled '1' highlights the first task: 'Clone virtual machine' from 'TinyLinux2 Template' to 'app-serv01' was completed successfully by 'CORP\Administrator'. The table has columns for Task Name, Target, Status, Details, and Initiator.

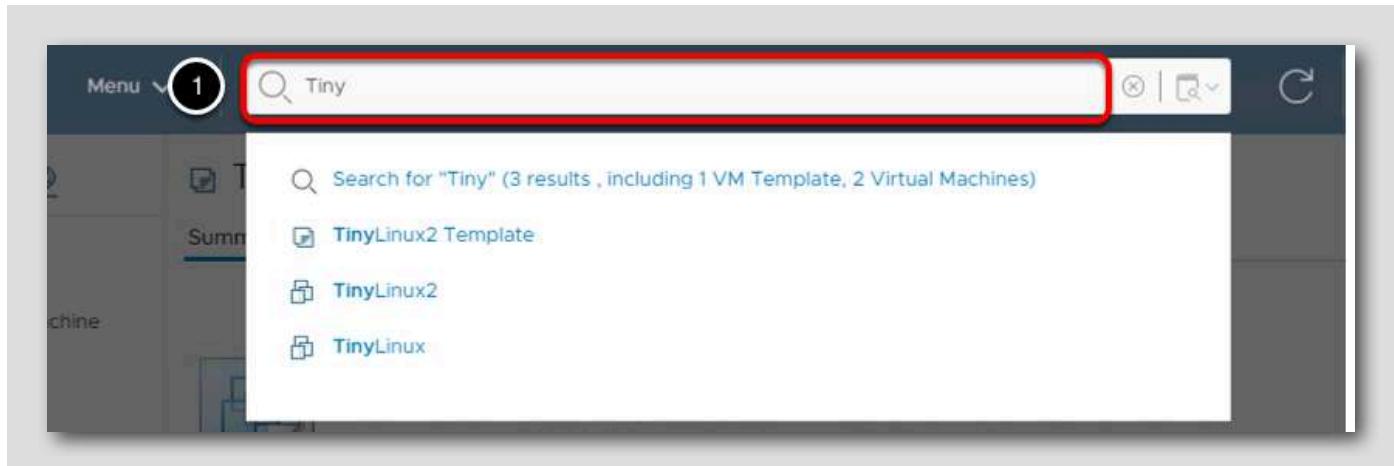
Task Name	Target	Status	Details	Initiator
Clone virtual machine	TinyLinux2 Te...	Completed	Copying Virtual Machine Configuration	CORP\Administrator

1. You can view the Recent Tasks window to monitor the virtual machine being created from the template.
2. When the task is complete, you will see the app-serv01 virtual machine in the inventory pane.

Using Tagging and Search to Find Objects Quickly

The vSphere Client provides some powerful search options. This lesson will guide you through the different search options to find the inventory of interest quickly. Also, the vCenter Inventory Service enables users to create custom defined tags that can be categorized and added to any inventory objects in the environment. These tags are searchable metadata and reduce the time to find inventory object information. This lab will cover how to create tags and use the tags for a search.

Search for Virtual Machines



At the top of the vSphere Client is a search bar that can be used to find objects quickly. This can be an object's name, like app-serv01 or an ESXi host. Tags can also be attached to objects and the search feature can be used to find them as well.

1. Click on the search bar at the top of the screen and type Tiny.

You can see all of the objects that contain the word tiny.

2. Press the **Enter** key.

Search Results

Search results for: "Tiny"

All Results (3)

Virtual Machines (3) 1

> Tags

> Custom Attributes

> Alert Status

Virtual Machines (3)

- TinyLinux2
- TinyLinux2 Template
- TinyLinux

[VIEW ALL](#)

On this page, you can see all the results for objects that contain the word **tiny**. If you have a large inventory, the results can be narrowed down further by selecting the object type you are looking for. Tags or Custom Attributes could be used to narrow the search results down. Selecting the object type can help you quickly find the object you are looking for.

1. Click on **Virtual Machines**.

Filter Results

The screenshot shows the vSphere Web Client interface. On the left, a sidebar titled 'Filter Results' is open, showing various filtering options. Under 'Power state', two checkboxes are selected: 'Powered off' and 'Suspended'. Both of these checkboxes are highlighted with a red border, and a large black circle with the number '1' is positioned next to them, indicating the step to follow. On the right, the search results for 'Tiny' are displayed in a table. The table has a header row with 'Name ↑' and a single data row for 'TinyLinux2 Template'.

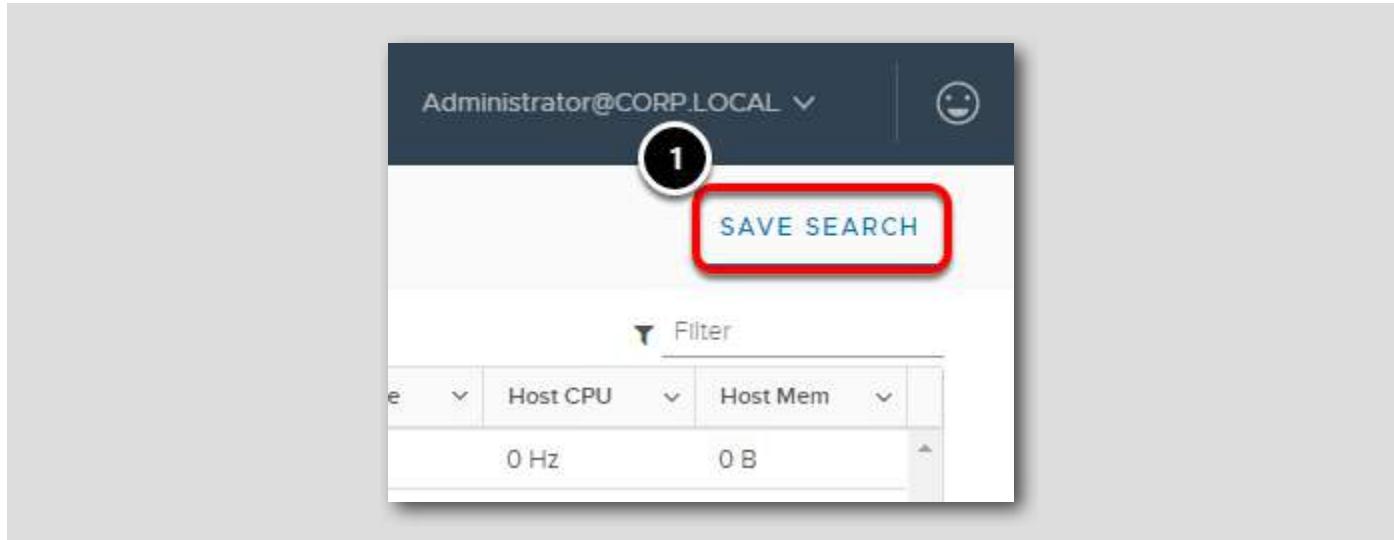
You can then filter the results down even further by specifying:

- The Power state of the virtual machine
- What operating system is running in the virtual machine
- What Host, Cluster or Datacenter to search in

1. Tick the box next to Powered Off and Suspended.

The search field is updated with the results.

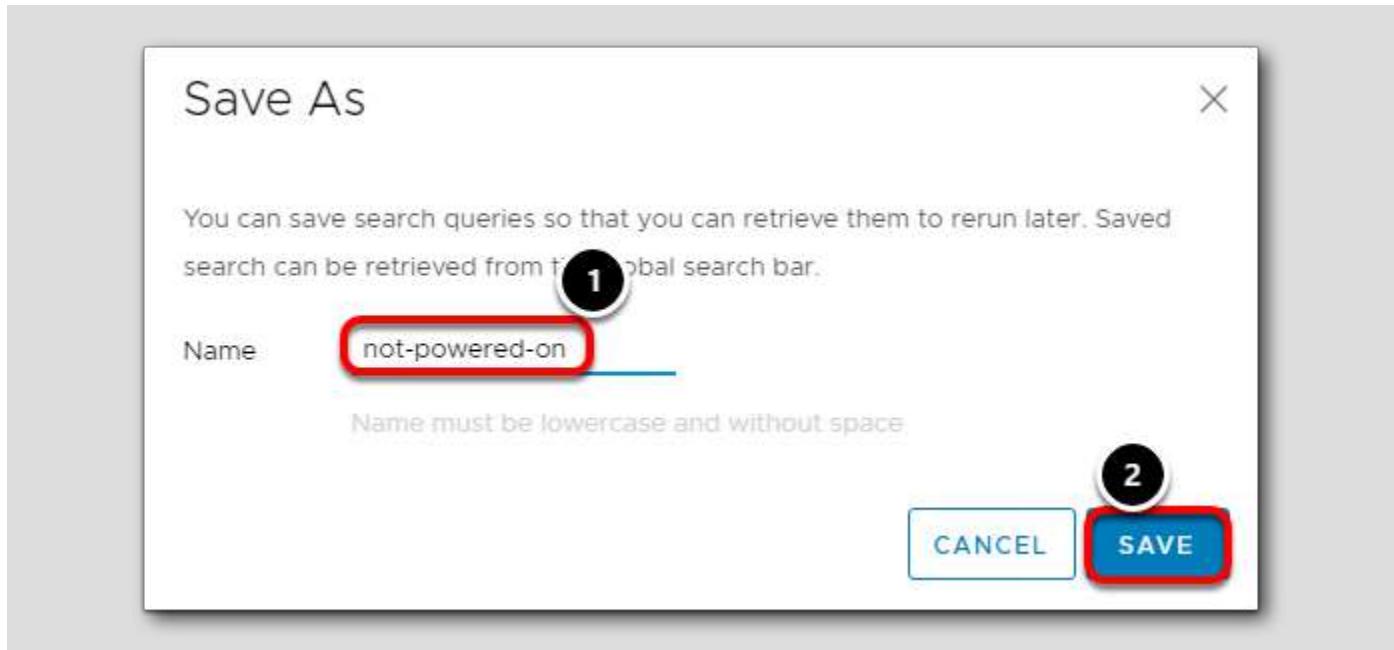
Save the Search



If this is a frequently used search, it can be saved for use in the future.

1. Click the **Save Search** button.

Name Search



1. Name the search **not-powered-on**

2. Click the **Save** button.

Note that the name must be in lowercase with no spaces between words.

View Saved Search



1. To view a saved search, click in the Search field.
2. Click on the drop-down arrow to see the previously saved search results.
3. Click on #not-powered-on.

Not-Powered-On-VMs

[107]

Saved Search: "#not-powered-on"

Search results for: "Tiny"

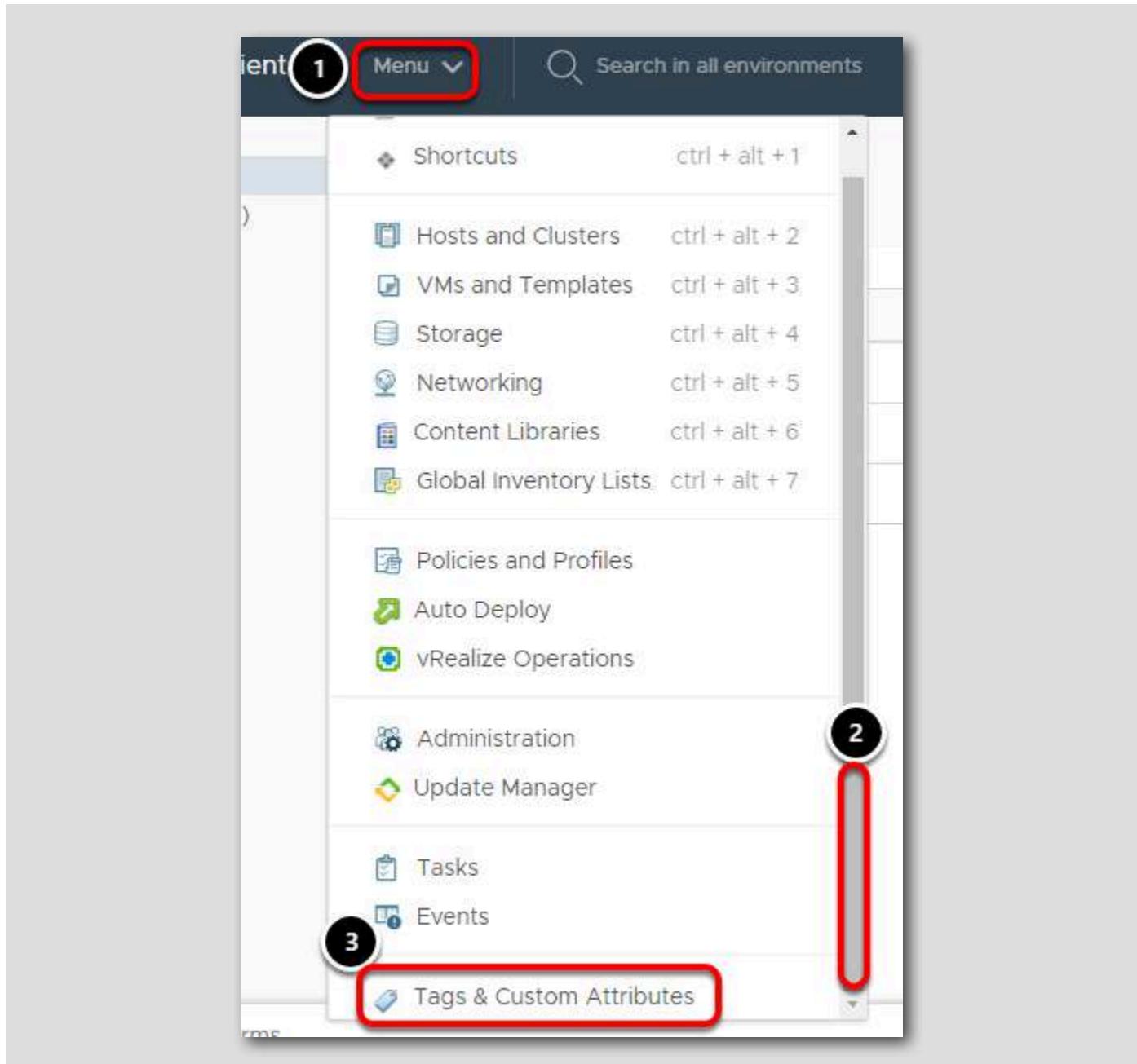
Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Memory
TinyLinux2 Template	Powered Off	Normal	734.24 MB	5.31 MB	0 Hz	0

ACTIONS

- Save as
- Rename
- Delete

1. Note that in the Actions menu, this search can be saved as another name and modified. It can also be renamed or deleted.

Tags and Custom Attributes

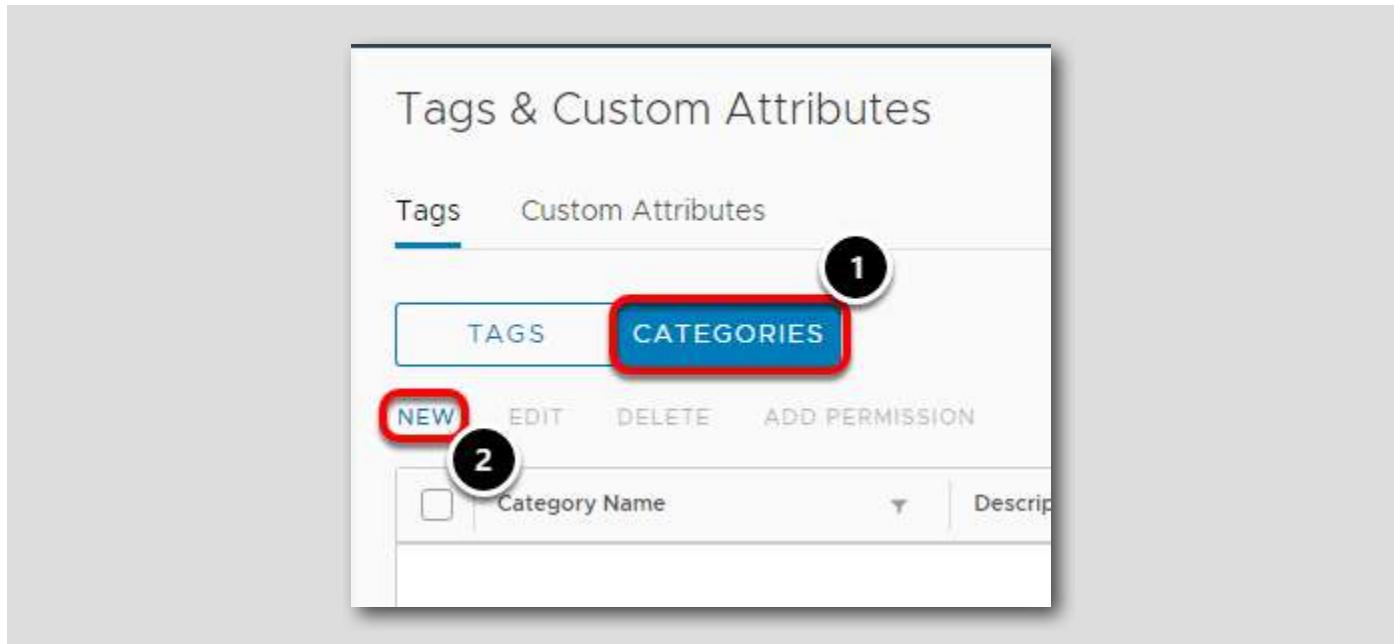


You use tags to add metadata to inventory objects. You can record information about your inventory objects in tags and use the tags in searches.

1. Click **Menu**
2. Use the scroll bar to scroll to the bottom of the list.
3. Select "Tags and Custom Attributes"

Creating Tag Categories

[109]

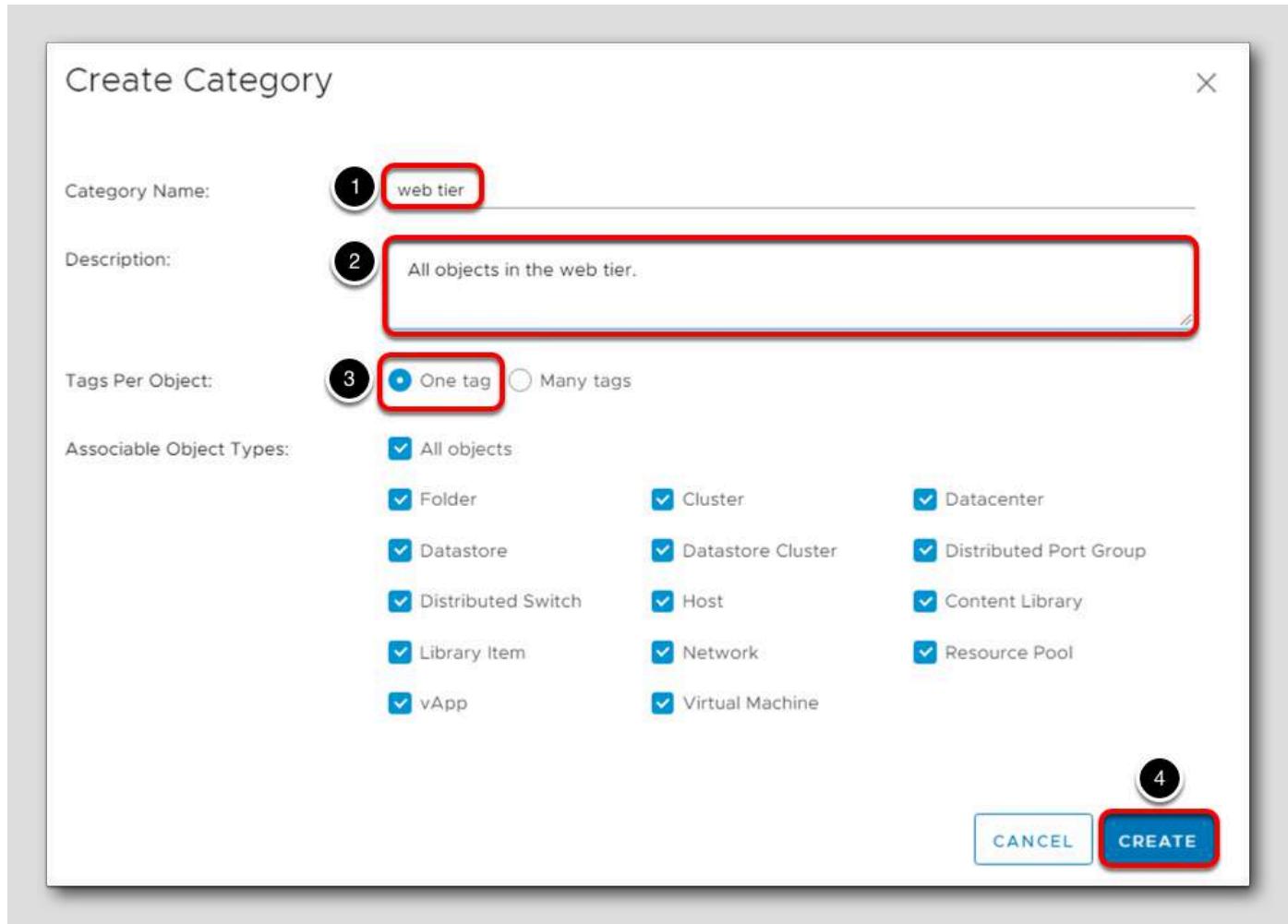


You use categories to group tags together and define how tags can be applied to objects.

Every tag must belong to one and only one category. You must create at least one category before creating any tags.

1. Click the **Categories** tab.
2. Click **New**.

New Category



Associable Object Types: We will use the default which states that the new tag in this category can be assigned to all objects. The other option is you can specify a specific object, such as virtual machines or datastores.

1. Enter "web tier" for the Category Name.
2. For a description, type All objects in the web tier.
3. Keep the default "One tag" tags per object
4. Click "Create"

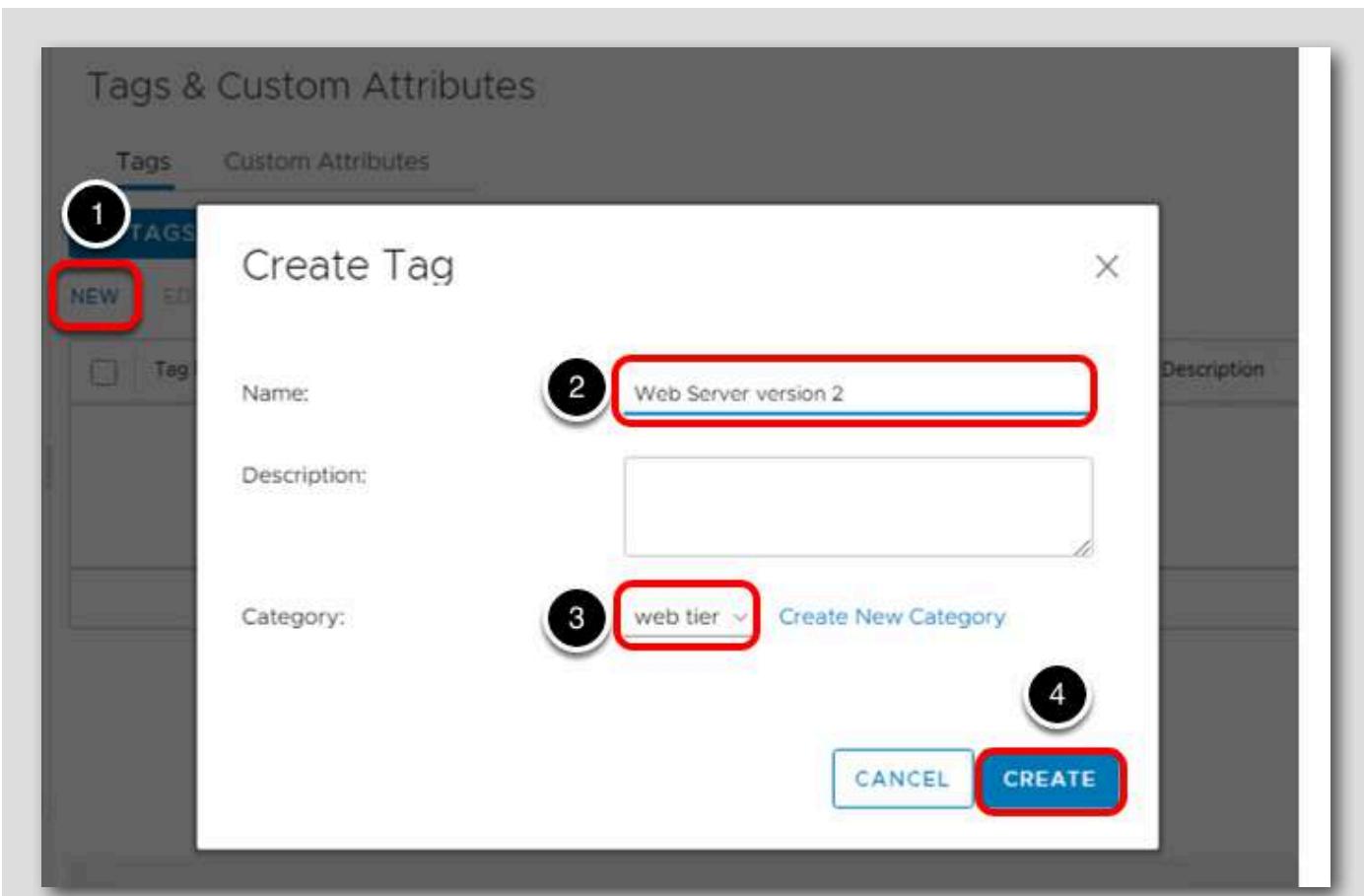
Create a New Tag

The screenshot shows the 'Tags & Custom Attributes' interface. The 'Tags' tab is selected, indicated by a red box and the number '2'. Below the tabs, there are buttons for 'NEW', 'EDIT', 'DELETE', and 'ADD PERMISSION'. A table lists categories. The first row has a checkbox, a category name input field containing 'Category Name' with a red box and the number '1', and a description field containing 'All objects in the web tier.'. The second row is partially visible.

	Category Name	Description
<input type="checkbox"/>	web tier	All objects in the web tier.
<input type="checkbox"/>		
<input type="checkbox"/>		

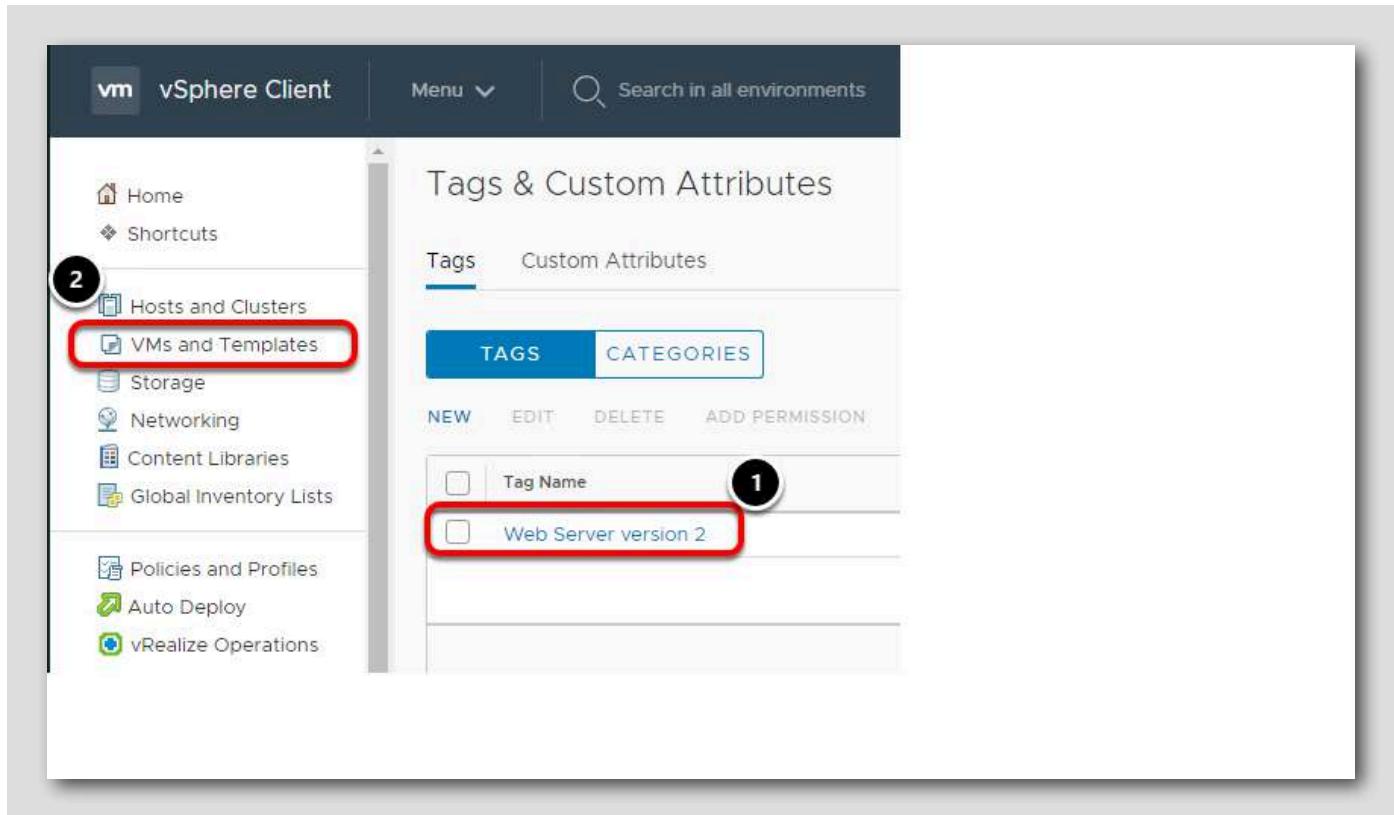
1. The new category has been created.
2. Click the **Tags** tab to create a new a Tag.

Add Tag



1. Click New
2. Name the tag Web Server version 2
3. Click the tag category **web tier** in the drop-down box.
4. Select Create

New Tag

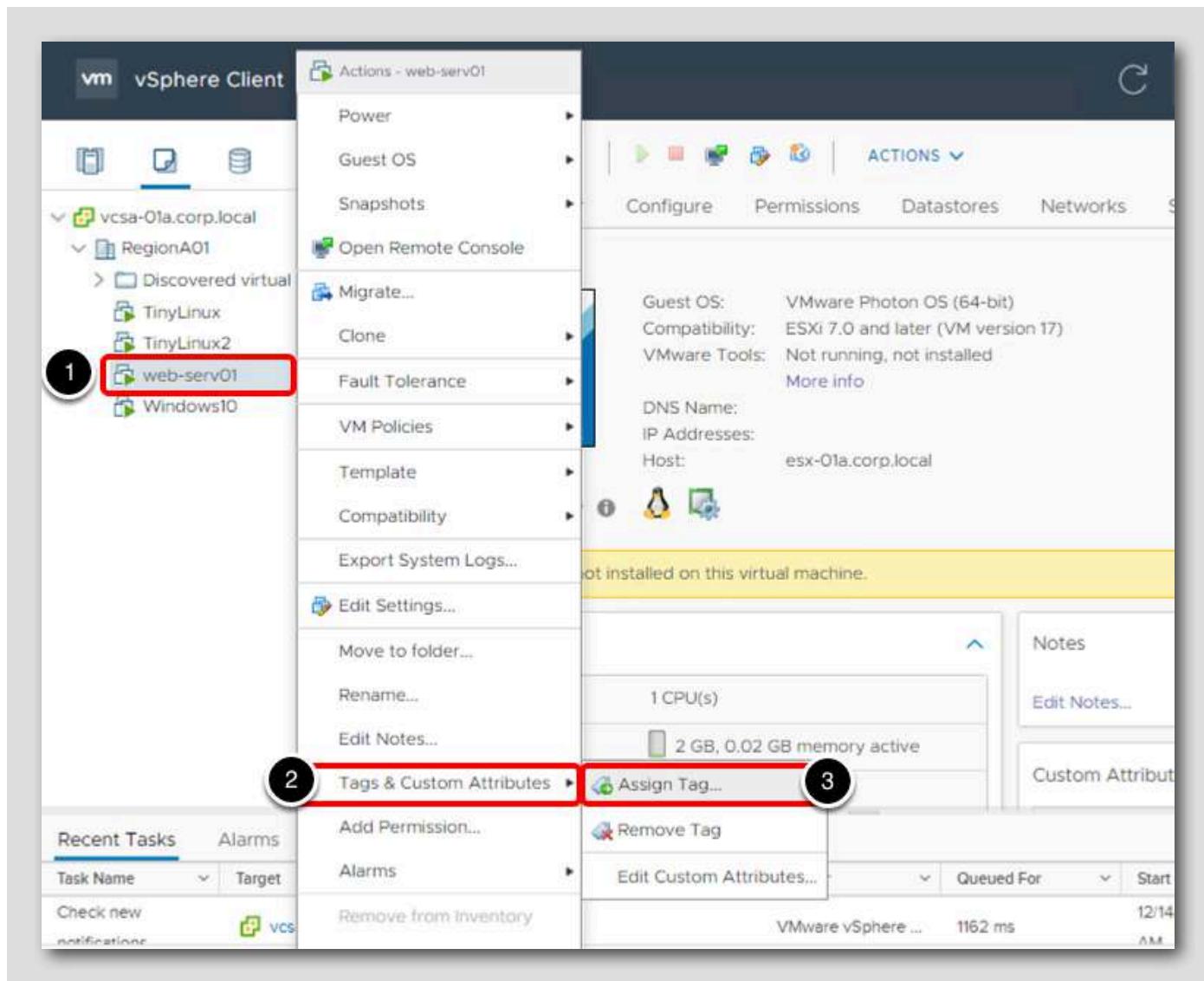


1. The newly created tag has now been added.

In order for these tags to be useful, they need to be assigned to objects. In the next steps, the tag will be assigned to virtual machines.

2. Click on VMs and Templates.

Select a Virtual Machine

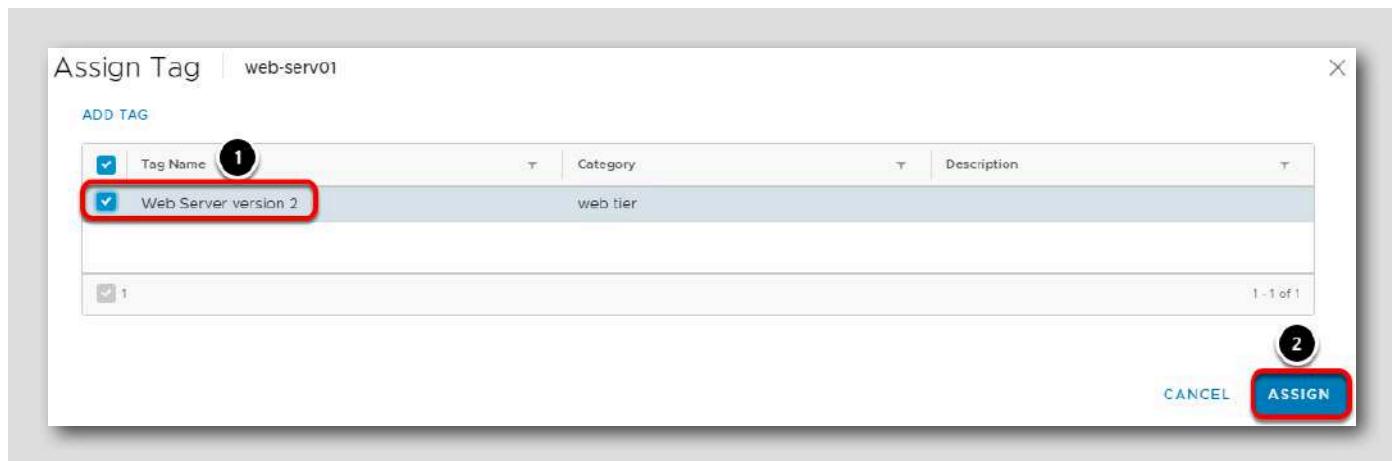


1. Right-click the virtual machine **web-serv01**.

2. Find **Tags & Custom Attributes**

3. Click **Assign Tag...**

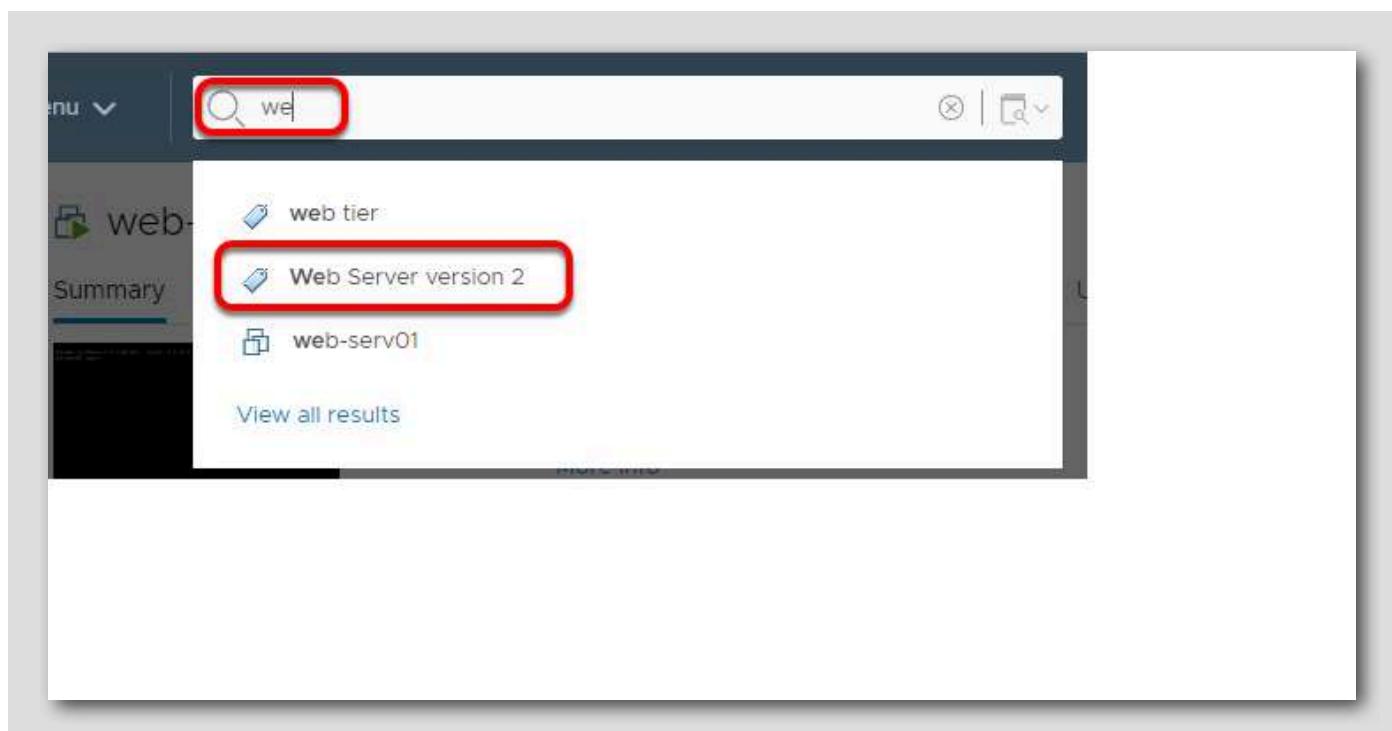
Assign Tag



1. Click the Web Server version 2 tag.

2. Click Assign.

Search Using Tags



1. In the Search field enter "we".
2. Select the Tag Web Server version 2.

Search Results

[117]

The screenshot shows a search results page for 'Web Server version 2'. At the top, there are tabs for 'Permissions' and 'Objects', with 'Objects' being the active tab and highlighted by a red box. To the right of the tabs, a circular badge contains the number '1'. Below the tabs is a table with a single row. The table has a header 'Name ↑' and a single entry 'web-serv01' with a small icon to its left.

Name ↑
web-serv01

1. Click on the Objects tab to find the list of objects which have been assigned the Web-serv01 tag.

Understanding vSphere Availability and Distributed Resource Scheduler (DRS)

[118]

This lab shows how to use the VMware vSphere web client to enable and configure vSphere Availability and Dynamic Resource Scheduling (DRS). HA protects from down time by automating recovery in the event of a host failure. DRS ensures performance by balancing virtual machine workloads across hosts a cluster.

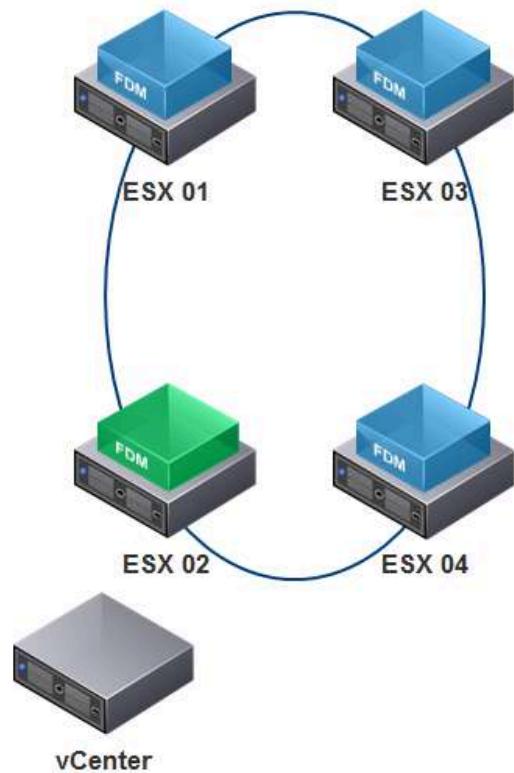
What is vSphere Availability?

vSphere Availability provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

When you create a vSphere Availability cluster, a single host is automatically elected as the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of the slave hosts. Different types of host failures are possible, and the master host must detect and appropriately deal with the failure. The master host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The master host uses network and datastore heartbeating to determine the type of failure. Also note that vSphere Availability is a host function which means there is not a dependency on vCenter in order to effectively fail over VMs to other hosts in the cluster.

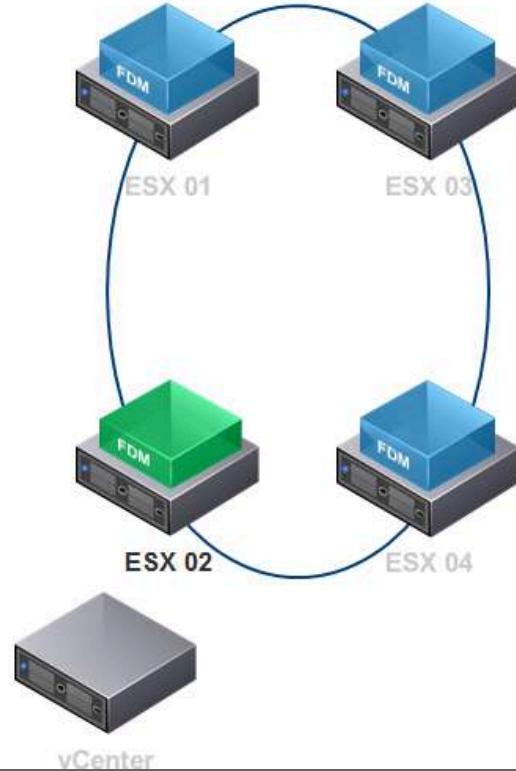
vSphere Availability Primary Components

- **Every host runs an agent.**
 - Referred to as 'FDM' or Fault Domain Manager
 - One of the agents within the cluster is chosen to assume the role of the Master
 - There is only one Master per cluster during normal operations
 - All other agents assume the role of Slaves
- **There is no more Primary/Secondary concept with vSphere HA**



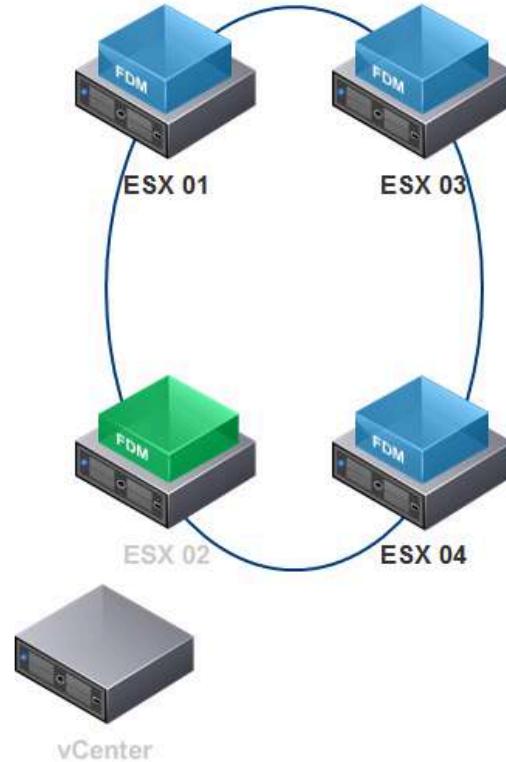
The Master Role

- **An FDM master monitors:**
 - ESX hosts and Virtual Machine availability.
 - All Slave hosts. Upon a Slave host failure, protected VMs on that host will be restarted.
 - The power state of all the protected VMs. Upon failure of a protected VM, the Master will restart it.
- **An FDM master manages:**
 - The list of hosts that are members of the cluster, updating this list as hosts are added or removed from the cluster.
 - The list of protected VMs. The Master updates this list after each user-initiated power on or power off.



The Slave Role

- A Slave monitors the runtime state of its locally running VMs and forwards any significant state changes to the Master.
- It implements vSphere HA features that do not require central coordination, most notably VM Health Monitoring.
- It monitors the health of the Master. If the Master should fail, it participates in the election process for a new master.
- Maintains list of powered on VMs.

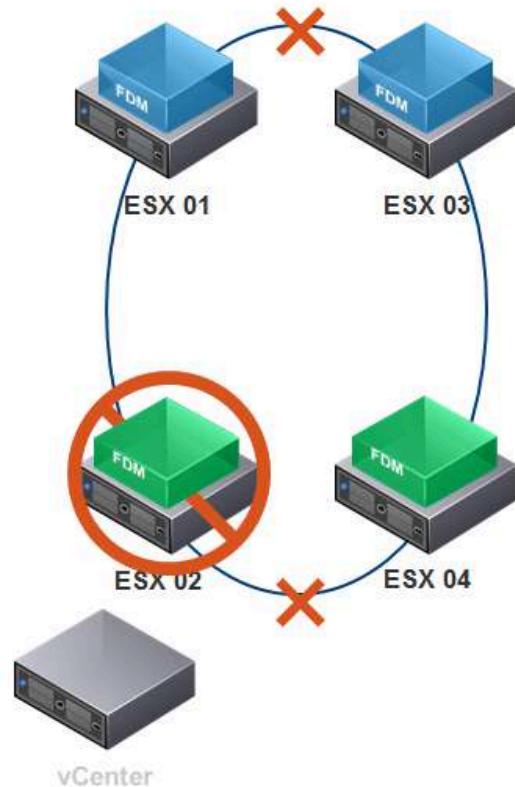


The Master Election Process

- The Master is determined through a election process.

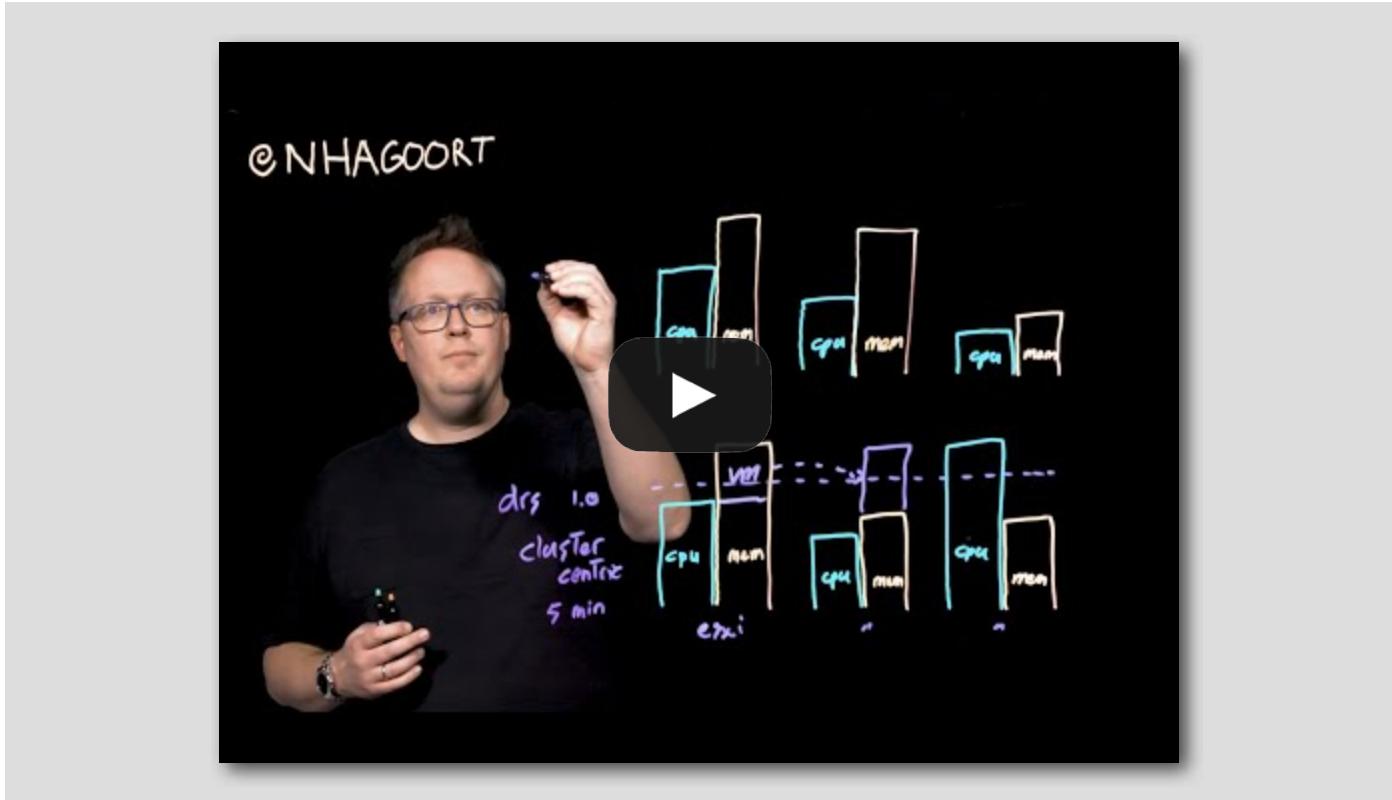
- A election occurs when:

- vSphere HA is enabled.
- A master host fails, is shutdown, or is placed in maintenance mode.
- A management network partition occurs.

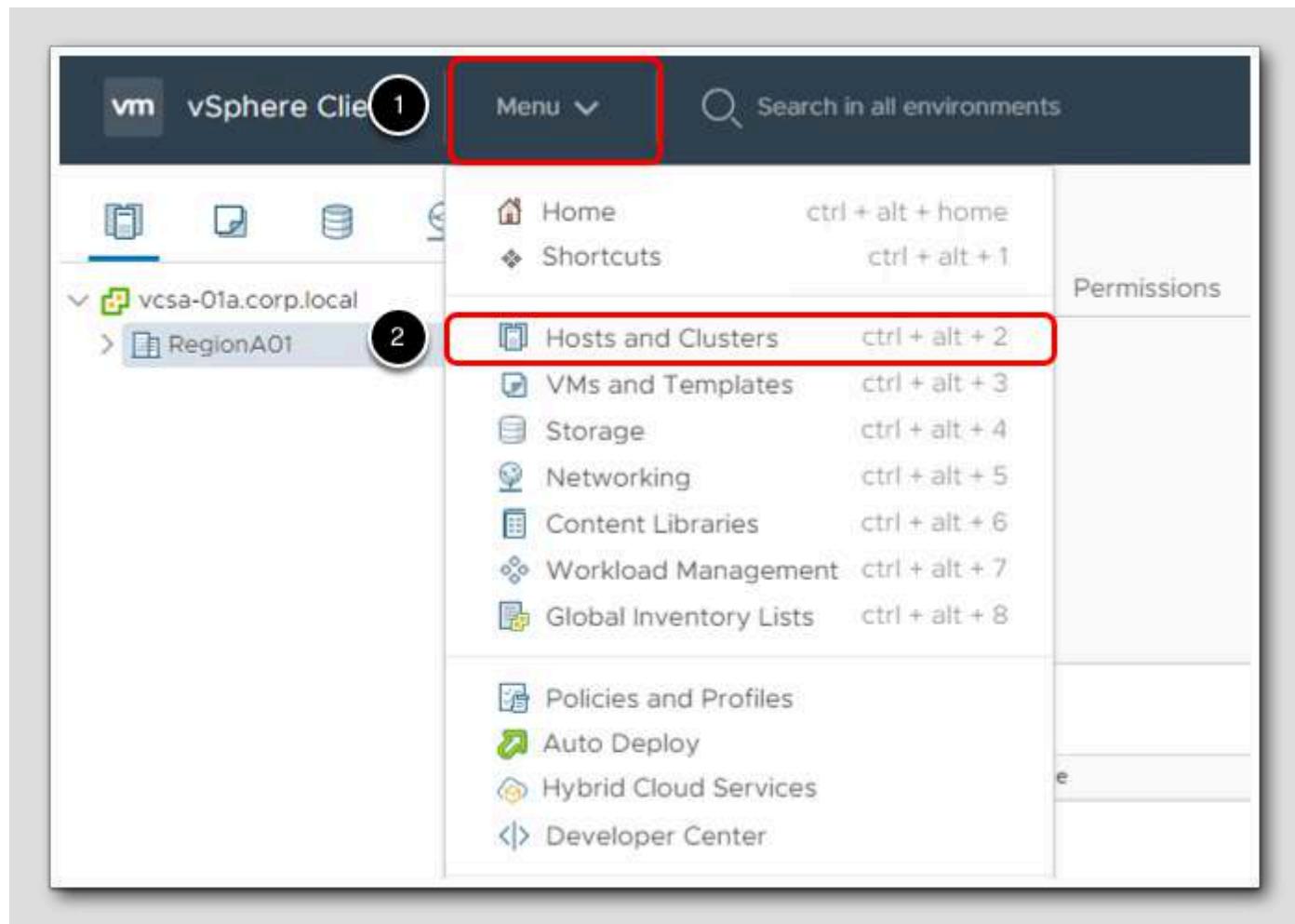


What's New with DRS in vSphere 7 (5:47)

<https://www.youtube.com/watch?v=vnuUzW7Yffo>

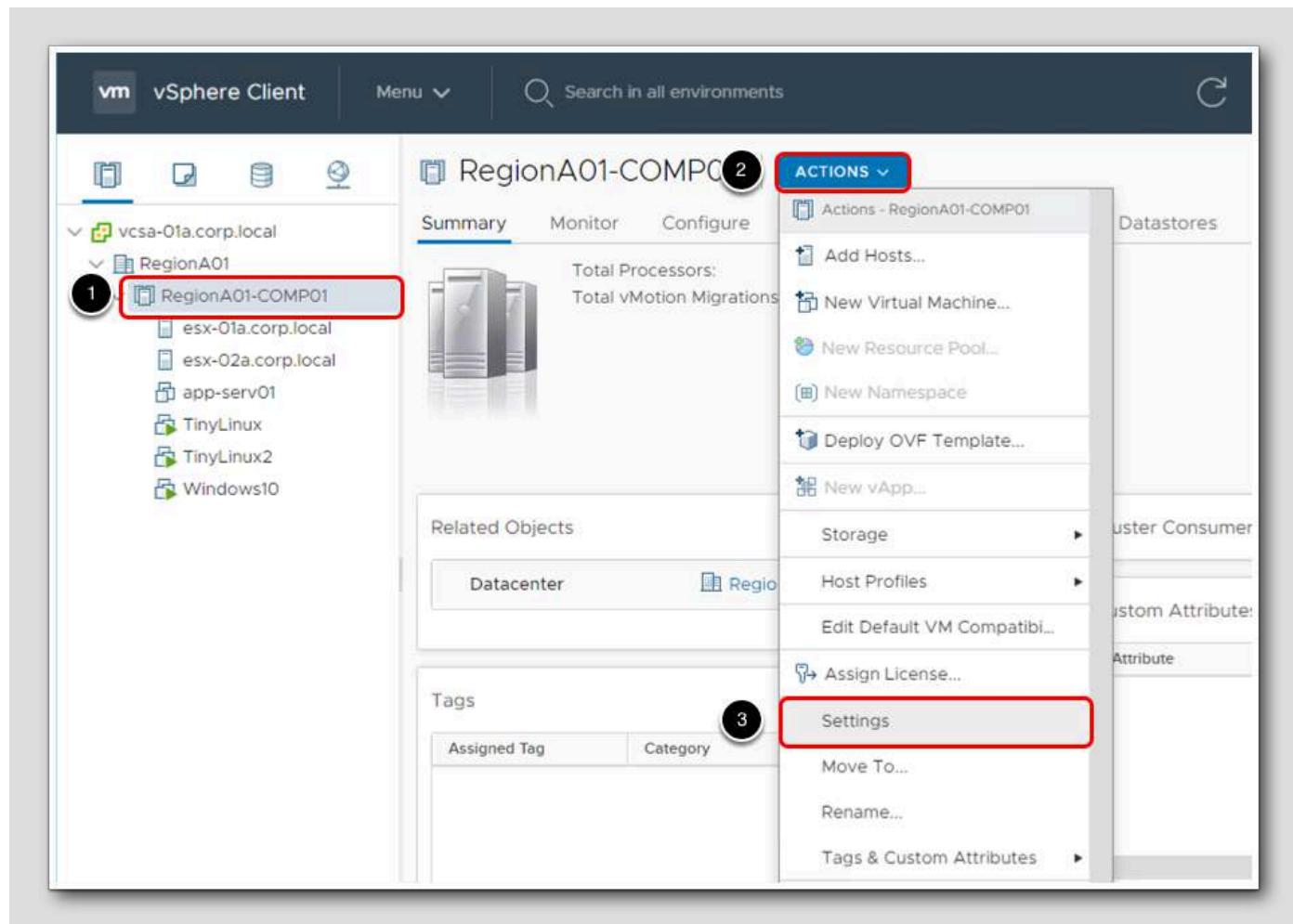


Enable and Configure vSphere Availability



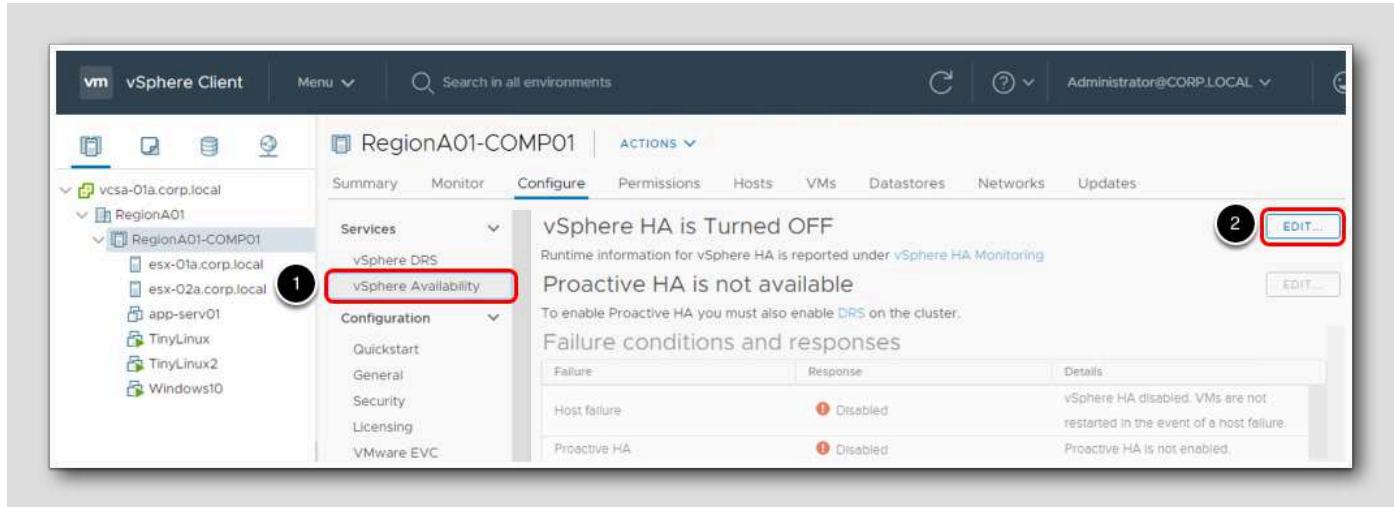
1. First, click on Menu
2. Select Hosts and Clusters

Settings for vSphere Availability



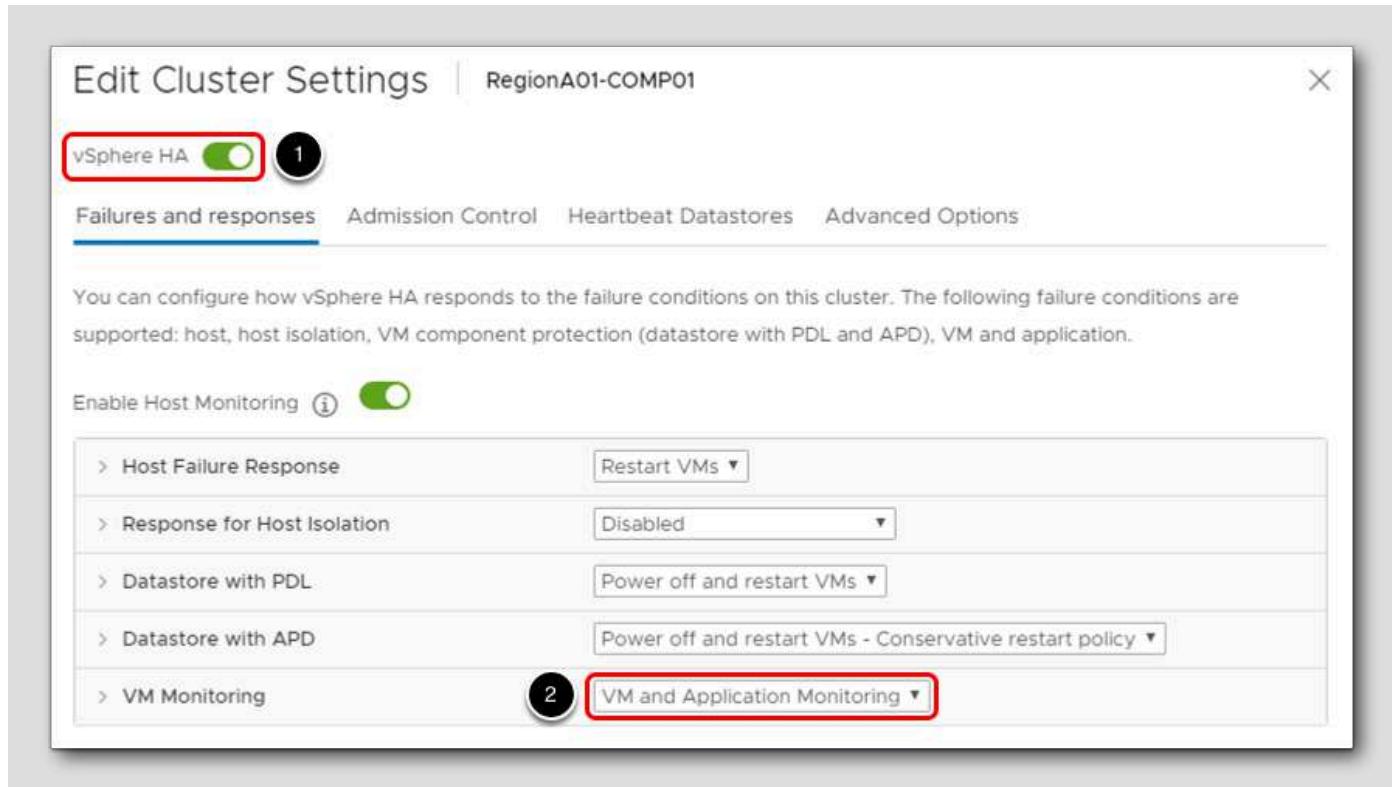
1. Click RegionA01 Cluster.
2. Click Actions to bring up the drop down-menu.
3. Click Settings.

Cluster Settings



1. Click **vSphere Availability** under **Services** to bring up the settings for high availability. Note that you may need to scroll to the top of the list.
2. Click the **Edit** button next to **vSphere HA is Turned OFF**.

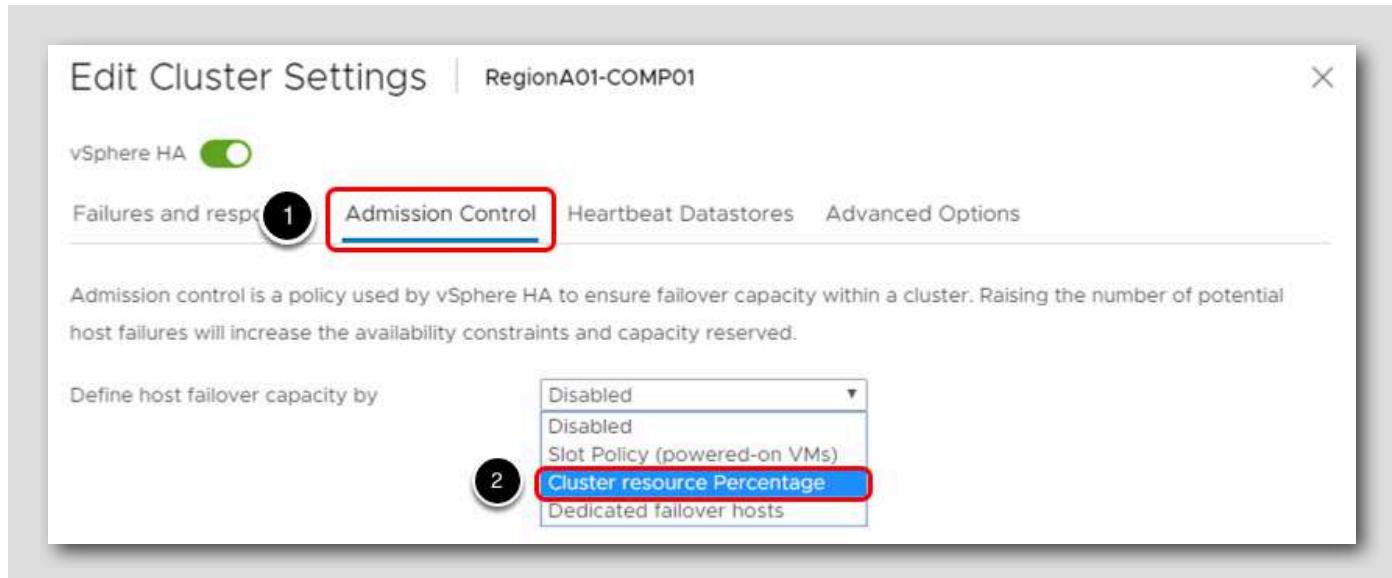
Enable vSphere HA



1. Click the toggle next to vSphere HA to enable it.
2. From the VM Monitoring drop-down list, select VM and Application Monitoring.

By selecting VM and Application Monitoring, a VM will be restarted if heartbeats are not received within a set time, the default is 30 seconds.

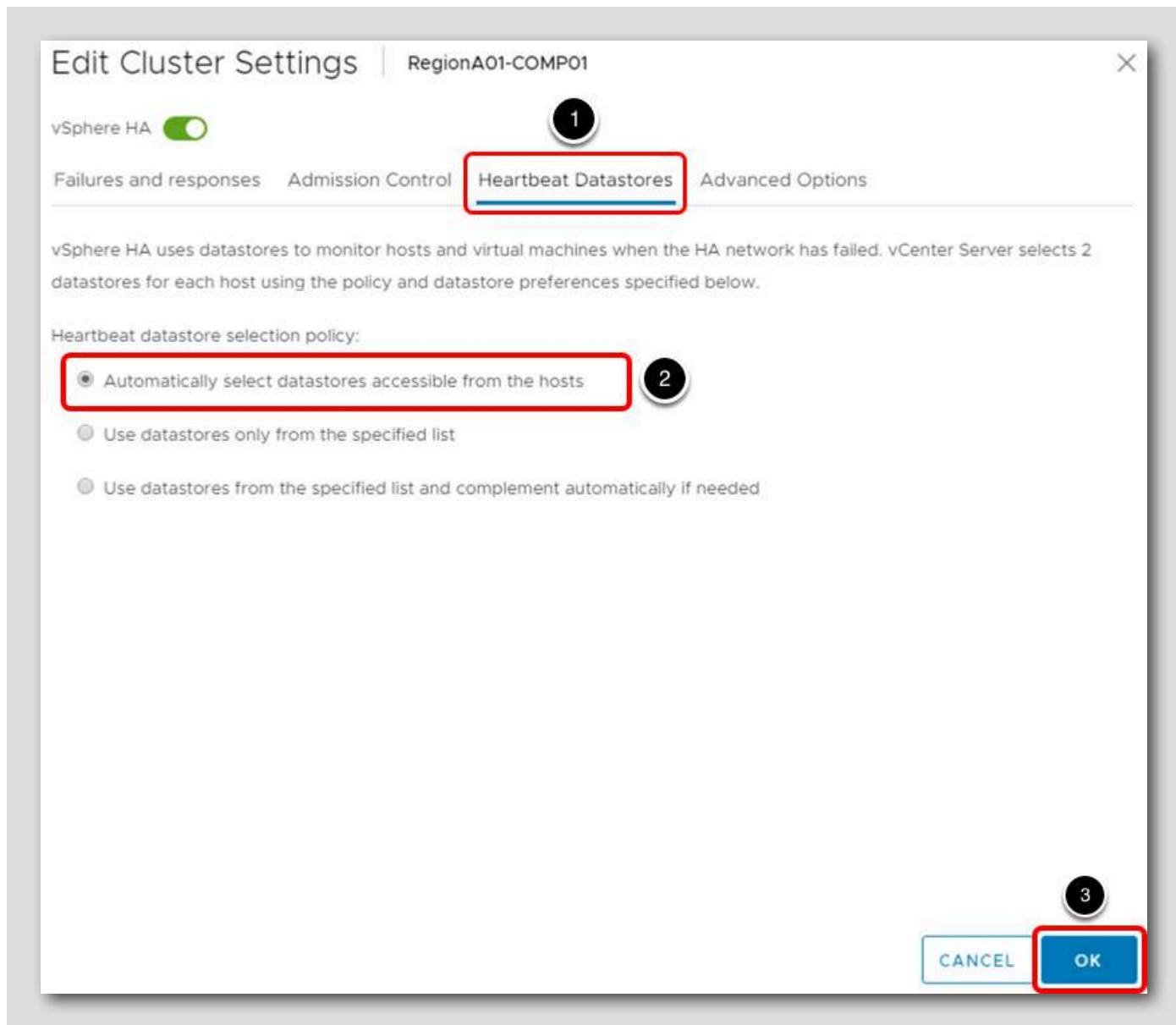
Admission Control



1. Click the **Admission Control** tab.
2. In the **Define host failover capacity by** drop-down menu, select **Cluster resource Percentage**.

We are setting aside a certain percentage of CPU and Memory resources to be used for failover, in the above case 25% for each.

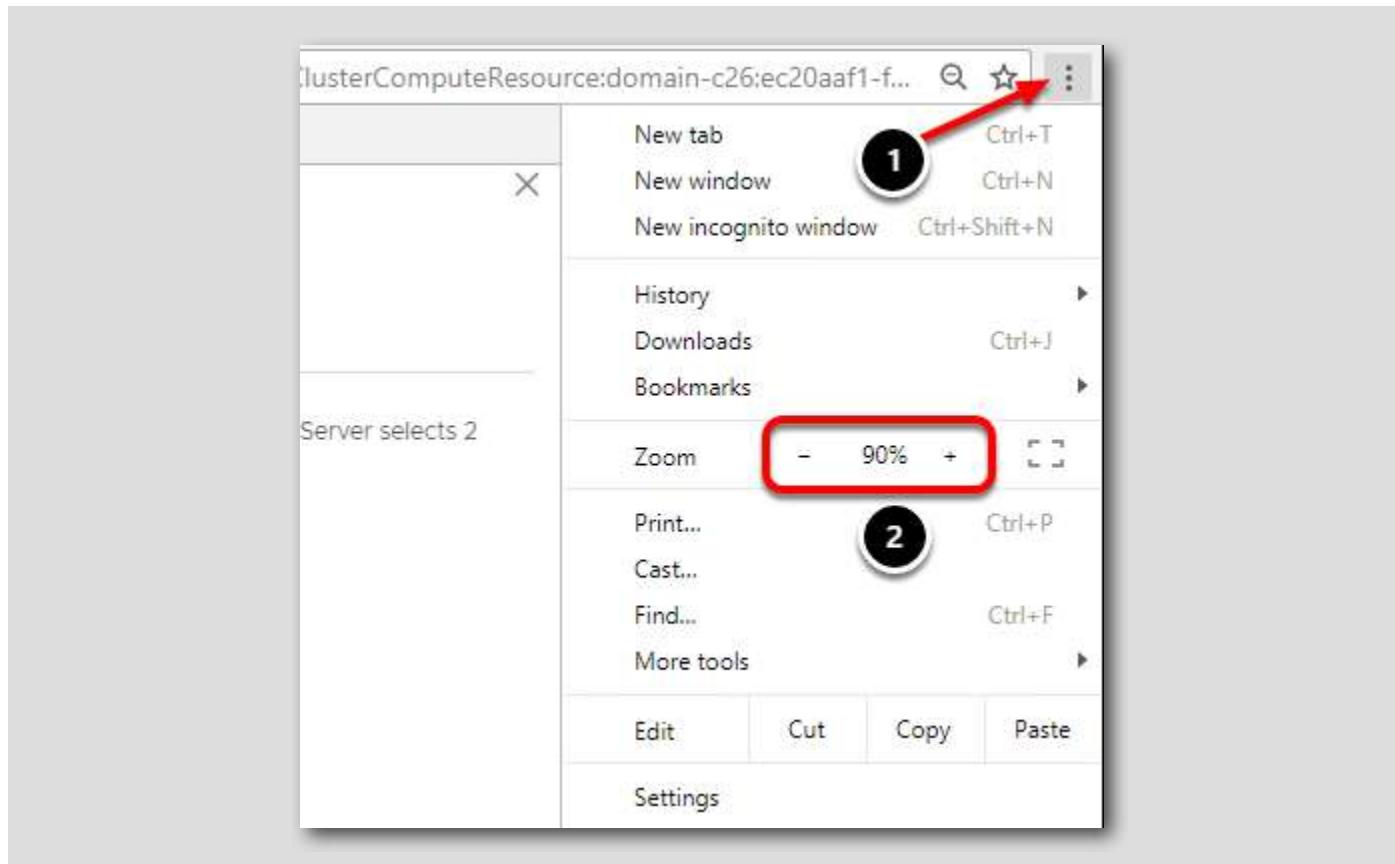
Heartbeat Datastores



1. Click Heartbeat Datastores.
2. Select Automatically select datastores accessible from the hosts.

This is another layer of protection. Heartbeat Datastores allows vSphere HA to monitor hosts when a management network partition occurs and to continue to respond to failures that occur.

2. Click OK to enable vSphere HA.



Note: If you do not see the OK button, you may need to zoom out on the web browser to see it.

Monitor the task

[131]

A screenshot of the vSphere Client interface showing the 'Recent Tasks' window. It displays two tasks: 'Configuring vSphere HA' on 'esx-01a.corp.local' and 'Configuring vSphere HA' on 'esx-02a.corp.local', both at 6% completion. The table includes columns for Task Name, Target, Status, Details, Initiator, Queued For, Start Time, Completion Time, and Server.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Configuring vSphere HA	esx-01a.corp.local	6%	Installing vSphere HA agent on esx-01a.corp.local	System	6 ms	01/07/2021, 6:21:16 AM		vcsa-01a.corp.local
Configuring vSphere HA	esx-02a.corp.local	6%	Installing vSphere HA agent on esx-02a.corp.local	System	15 ms	01/07/2021, 6:21:16 AM		vcsa-01a.corp.local

It will take a minute or two to configure vSphere HA. You can monitor the progress in the Recent Tasks window.

The screenshot shows the 'Recent Tasks' section of the vSphere Client interface. It displays a table with columns: Task Name, Target, Status, Details, and Initiator. There are two entries:

Task Name	Target	Status	Details	Initiator
Configuring vSphere HA	esx-01a.corp.l...	✓ Completed	Waiting for cluster election to complete	System
Configuring vSphere HA	esx-02a.corp.l...	✓ Completed	Waiting for cluster election to complete	System

Once the three tasks have been completed, you can move on to the next step.

Use the Summary Tab to Verify that HA Is Enabled

The screenshot shows the vSphere Web Client interface for a host named 'RegionA01-COMP01'. The 'Summary' tab is selected, indicated by a red box and a red border around the tab itself. A red circle with the number '1' is positioned above the 'Datacenter' link, pointing to a tooltip that says 'RegionA01'. Another red circle with the number '2' is positioned above the 'vSphere HA' panel, pointing to a tooltip that says 'Protected'. The 'vSphere HA' panel is expanded and has a red border around it. It displays resource usage and configuration details:

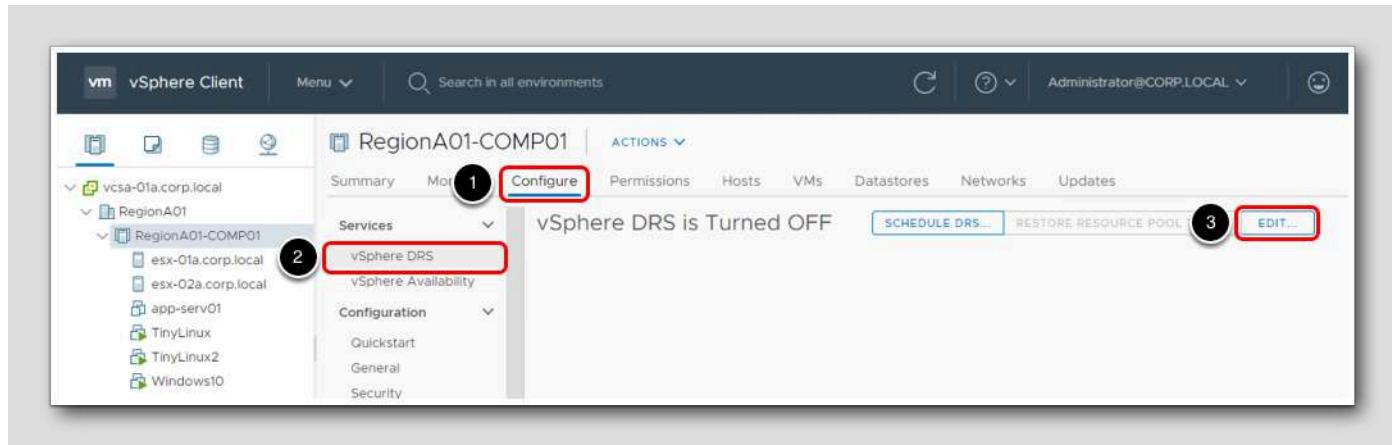
vSphere HA	
Protected	
CPU	0% - 50% - 100%
Memory	0% - 50% - 100%
CPU reserved for failover:	50 %
Memory reserved for failover:	50 %
Proactive HA:	Disabled
Host Monitoring:	Enabled
VM Monitoring:	VM and Application Monitoring

1. Click the **Summary** tab
2. Locate and expand the **vSphere HA** panel in the data area: click on the ">" to the right of the panel's name to expand it.

If vSphere HA does not show **Protected** and the tasks completed successfully, you may need to click the refresh button.

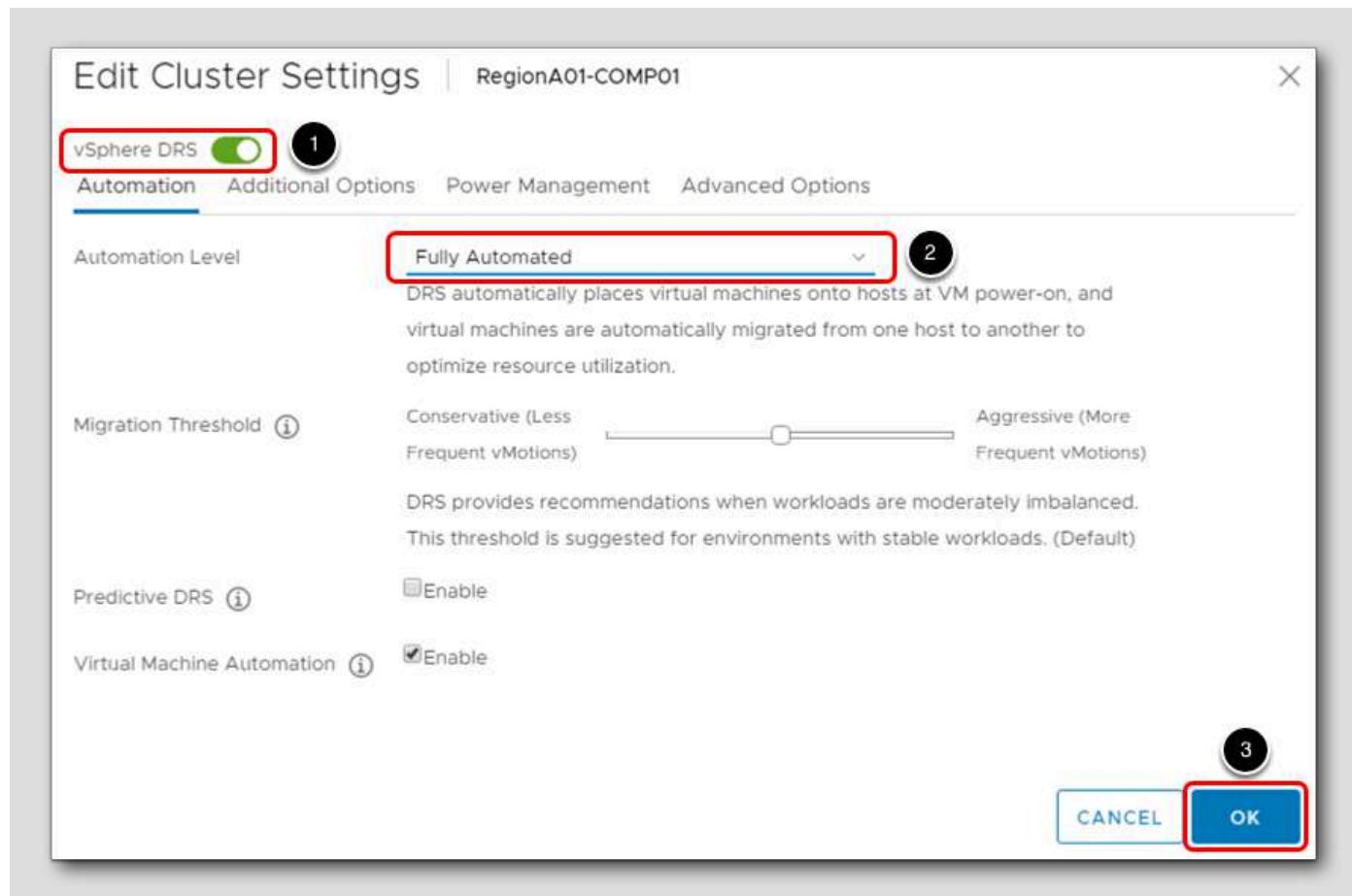
Notice the bars that display resource usage in blue, protected capacity in light gray, and reserve capacity using stripes.

Enable Distributed Resource Scheduler (DRS)



1. Click on the Configure tab to start the process of enabling Distributed Resource Scheduler.
2. Click vSphere DRS.
3. Click on the Edit button to modify the DRS settings.

Enable Distributed Resource Scheduler (DRS)



1. Verify that vSphere DRS is enabled. If not, click the vSphere DRS to enable.
2. Click the drop-down box and select Fully Automated.
3. Click OK.

Automation Levels

Automation Level	Action
Manual	<ul style="list-style-type: none"> ■ Initial placement: Recommended host(s) is displayed. ■ Migration: Recommendation is displayed.
Partially Automated	<ul style="list-style-type: none"> ■ Initial placement: Automatic. ■ Migration: Recommendation is displayed.
Fully Automated	<ul style="list-style-type: none"> ■ Initial placement: Automatic. ■ Migration: Recommendation is executed automatically.

The chart shown above is showing how DRS affects placement and migration according to the setting Manual, Partially Automated or Fully Automated.

Use the Cluster's Summary Tab to Check Cluster Balance

RegionA01-COMP01

ACTIONS ▾

Summary Monitor Configure Permissions Hosts VMs Datastores Networks Updates

Cluster Consumers Cluster Resources

Custom Attributes

Attribute	Value
No items to display	

Edit...

vSphere DRS

Cluster DRS Score ⓘ

VM DRS Score ⓘ

59%

Range	Count
0-20%	0 VMs
20-40%	1 VM
40-60%	0 VMs
60-80%	1 VM
80-100%	1 VM

DRS recommendations: 0

DRS faults: 0

[VIEW DRS SETTINGS](#) [VIEW ALL VMs](#)

1. Click the **Summary** tab to display the current status of the cluster.
2. The **Summary** tab of the Cluster RegionA01-COMP01 shows the current balance of the cluster. Also shown in the DRS section is how many recommendations or faults that have occurred with the cluster. (You may have to scroll down to see the vSphere DRS widget).

vSphere 7 Fault Tolerance Provides Continuous Availability

[137]

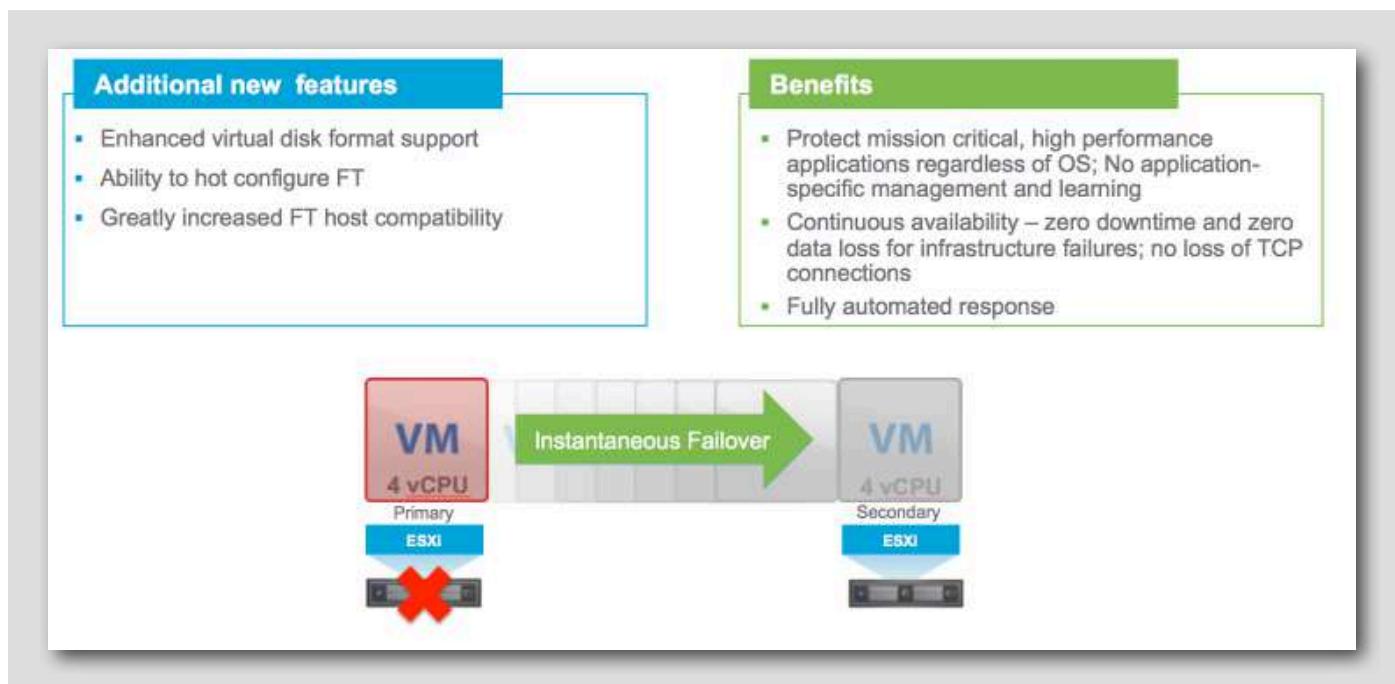
You can use vSphere Fault Tolerance for your virtual machines to ensure continuity with higher levels of availability and data protection. Fault Tolerance is built on the ESXi host platform, and it provides availability by having identical Virtual Machines (VM) run on separate hosts.

vSphere Fault Tolerance (FT) provides continuous availability by creating and maintaining the states of a Primary and Secondary VMs identical. In the event of a failover situation, the Secondary VM will be executed and it will replace the Primary VM (the protected virtual machine). The duplicate virtual machine, the Secondary VM, is created and runs on another host. The primary VM is continuously replicated to the secondary VM so that the secondary VM can take over at any point, thereby providing Fault Tolerant protection. The Primary and Secondary VMs continuously monitor the status of one another to ensure that Fault Tolerance is maintained.

Fault Tolerance avoids "split-brain" situations, which can lead to two active copies of a virtual machine after recovery from a failure. Atomic file locking on shared storage is used to coordinate failover so that only one side continues running as the Primary VM and a new Secondary VM is respawned automatically. vSphere Fault Tolerance can accommodate symmetric multiprocessor (SMP) virtual machines with up to four vCPUs. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.

VMware vSphere Fault Tolerance

[138]



The benefits of Fault Tolerance are:

- Protect mission critical, high performance applications regardless of OS
- Continuous availability - Zero downtime, zero data loss for infrastructure failures
- Fully automated response

Several typical situations can benefit from the use of vSphere Fault Tolerance. Fault Tolerance provides a higher level of business continuity than vSphere HA. When a Secondary VM is called upon to replace its Primary VM counterpart, the Secondary VM immediately takes over the Primary VM's role with the entire state of the virtual machine preserved. Applications are already running, and data stored in memory does not need to be reentered or reloaded. Failover provided by vSphere HA restarts the virtual machines affected by a failure.

This higher level of continuity and the added protection of state information and data provides the following use cases where you would want to implement Fault Tolerance:

- Applications which must always be available, especially applications that have long-lasting client connections that users want to maintain during hardware failure.
- Custom applications that have no other way of doing clustering.
- Cases where high availability might be provided through custom clustering solutions, which are too complicated to configure and maintain.

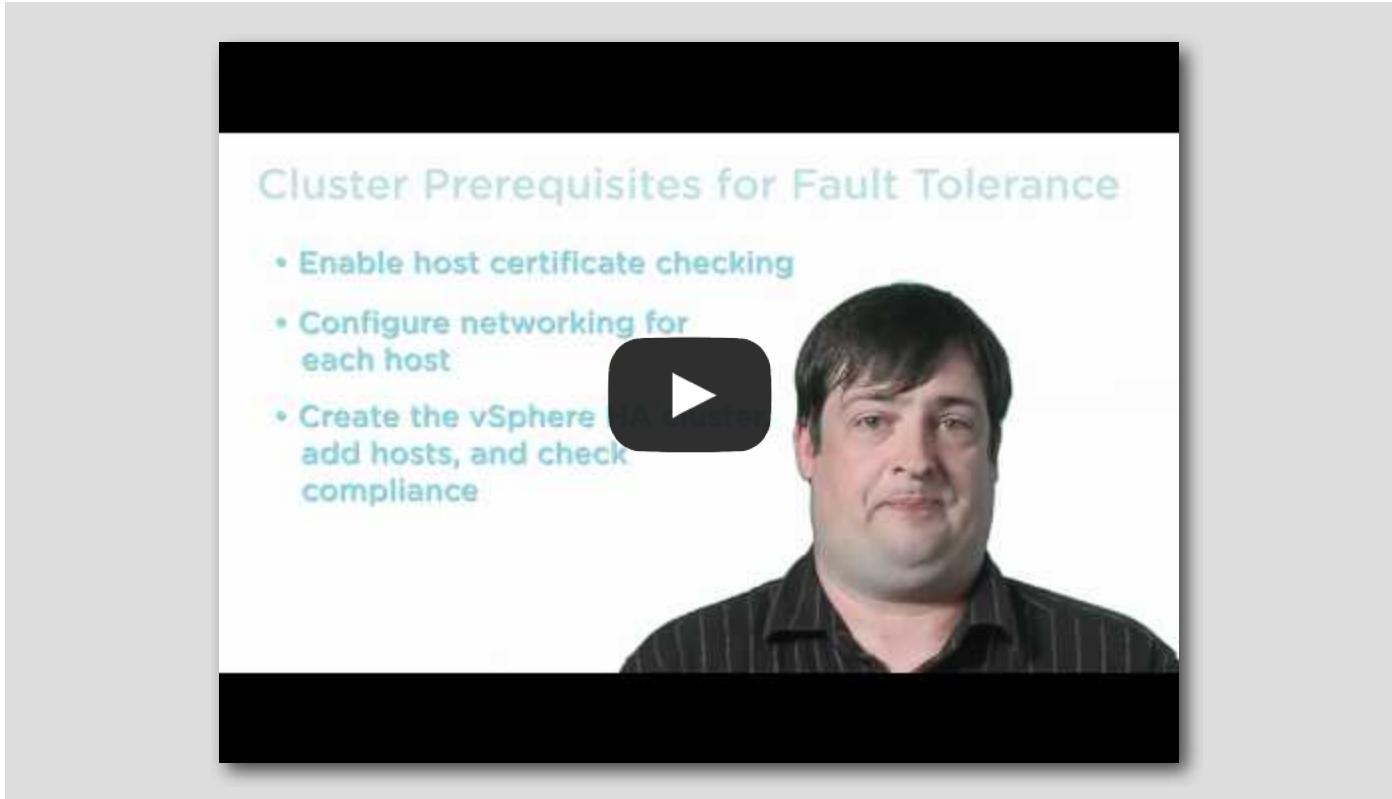
Another key use case for protecting a virtual machine with Fault Tolerance can be described as On-Demand Fault Tolerance. In this case, a virtual machine is adequately protected with vSphere HA during normal operation. During certain critical periods, you might want to enhance the protection of the virtual machine. For example, you might be running a quarter-end report which, if interrupted, might delay the availability of critical information. With vSphere Fault Tolerance, you can protect this virtual machine before running this report and then turn off or suspend Fault Tolerance after the report has been produced. You can use On-Demand Fault Tolerance to protect the virtual machine during a critical time period and return the resources to normal during non-critical operation. See the [Performance Best Practices for VMware vSphere](#) and [vSphere 7.0 Availability](#) for more information.

Video: Protecting Virtual Machines with FT (3:52)

[139]

This video shows how to protect virtual machines with VMware Fault Tolerance (FT). Due to resource constraints in the Hands-on Labs environment we are unable to demonstrate this live for you.

https://www.youtube.com/watch?v=dqDGGZ_fGrA



Monitoring Events and Creating Alarms

[140]

vSphere includes a user-configurable events and alarms subsystem. This subsystem tracks events happening throughout vSphere and stores the data in log files and the vCenter Server database. This subsystem also enables you to specify the conditions under which alarms are triggered. Alarms can change state from mild warnings to more serious alerts as system conditions change and can trigger automated alarm actions. This functionality is useful when you want to be informed, or take immediate action, when certain events or conditions occur for a specific inventory object, or group of objects.

Events are records of user actions or system actions that occur on objects in vCenter Server or on a host. Actions that might be reordered as events include, but are not limited to, the following examples:

- A license key expires
- A virtual machine is powered on
- A user logs in to a virtual machine
- A host connection is lost

Event data includes details about the event such as who generated it, when it occurred, and what type of event.

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. An alarm definition consists of the following elements:

- Name and description - Provides an identifying label and description.
- Alarm type - Defines the type of object that will be monitored.
- Triggers - Defines the event, condition, or state that will trigger the alarm and defines the notification severity.
- Tolerance thresholds (Reporting) - Provides additional restrictions on condition and state triggers thresholds that must be exceeded before the alarm is triggered.
- Actions - Defines operations that occur in response to triggered alarms. VMware provides sets of predefined actions that are specific to inventory object types.

Alarms have the following severity levels:

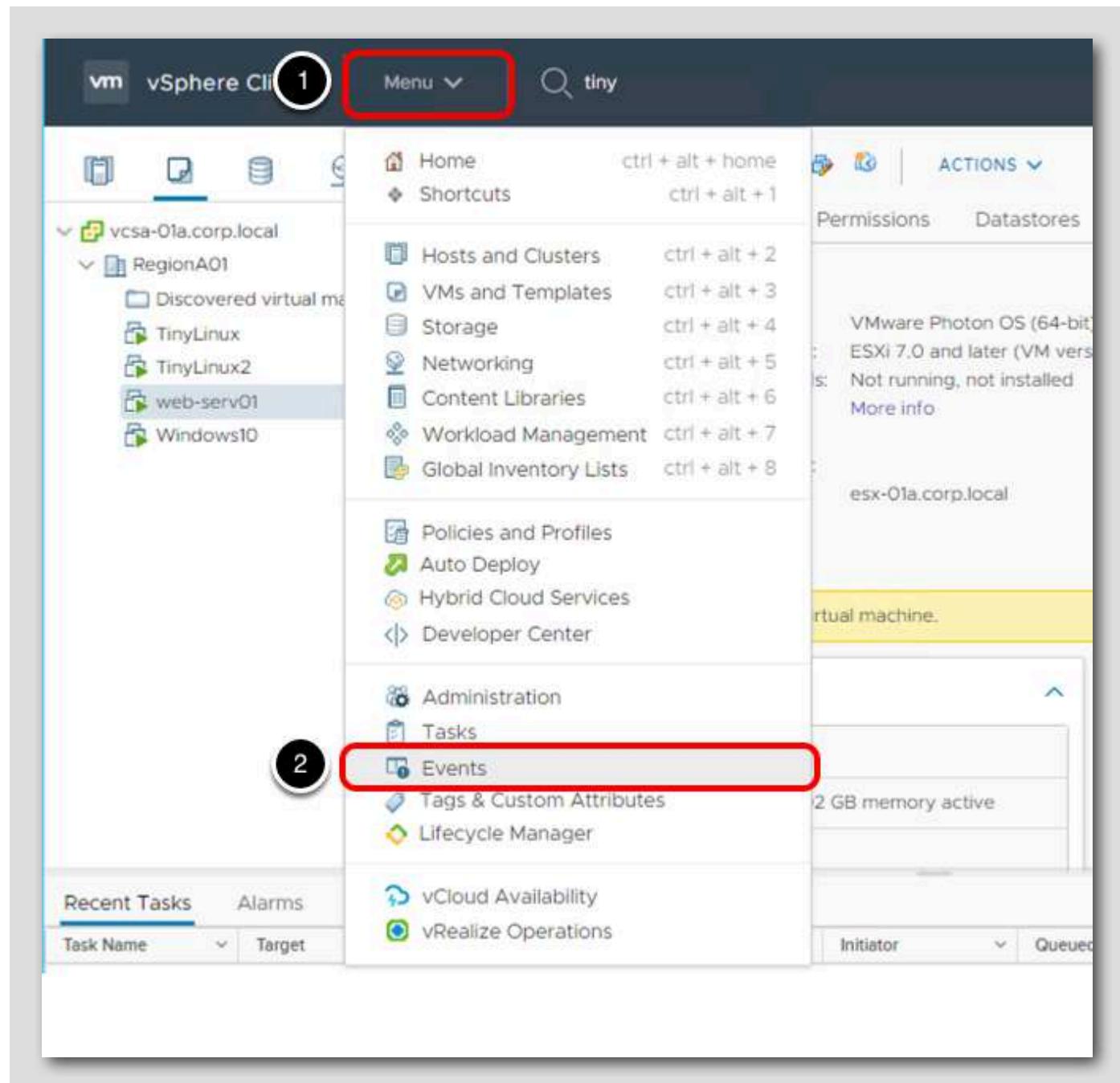
- Normal – green
- Warning – yellow
- Alert – red

Alarm definitions are associated with the object selected in the inventory. An alarm monitors the type of inventory objects specified in its definition.

For example, you might want to monitor the CPU usage of all virtual machines in a specific host cluster. You can select the cluster in the inventory and add a virtual machine alarm to it. When enabled, that alarm will monitor all virtual machines running in the cluster and will trigger when any one of them meets the criteria defined in the alarm. If you want to monitor a specific virtual machine in the cluster, but not others, you would select that virtual machine in the inventory and add an alarm to it. One easy way to apply the same alarms to a group of objects is to place those objects in a folder and define the alarm on the folder.

In this lab, you will learn how to create an alarm and review the events that have occurred.

Review default alerts



1. Click Menu
2. Click on Events menu item

Event Console

Event Console

Description	Type	Date Time	Task	Target	User	Event Type ID
User VSPHERE.L...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.UserLogout...
vCenter Update ...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter ESXi Du...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Log File ...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Image B...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Diagnos...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Autodep...	Information	12/11/2020, 3:10:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Boot File...	Information	12/11/2020, 3:10:57 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Root File...	Information	12/11/2020, 3:10:57 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Core dn...	Information	12/11/2020, 3:10:57 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
vCenter Stats, ev...	Information	12/11/2020, 3:10:57 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.ResourceE...
User VSPHERE.L...	Information	12/11/2020, 3:10:57 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.UserLoginS...
User VSPHERE.L...	Information	12/11/2020, 3:08:58 PM		VSPHERE.LOCAL\me...	VSPHERE.LOCAL\me...	vim.event.UserLogout...

100 items

Date Time: 12/11/2020, 3:10:58 PM Type: Information 2

User: VSPHERE.LOCAL\machine-d8d3462b-58da-49b3-9f5a-478d5175...

Description:

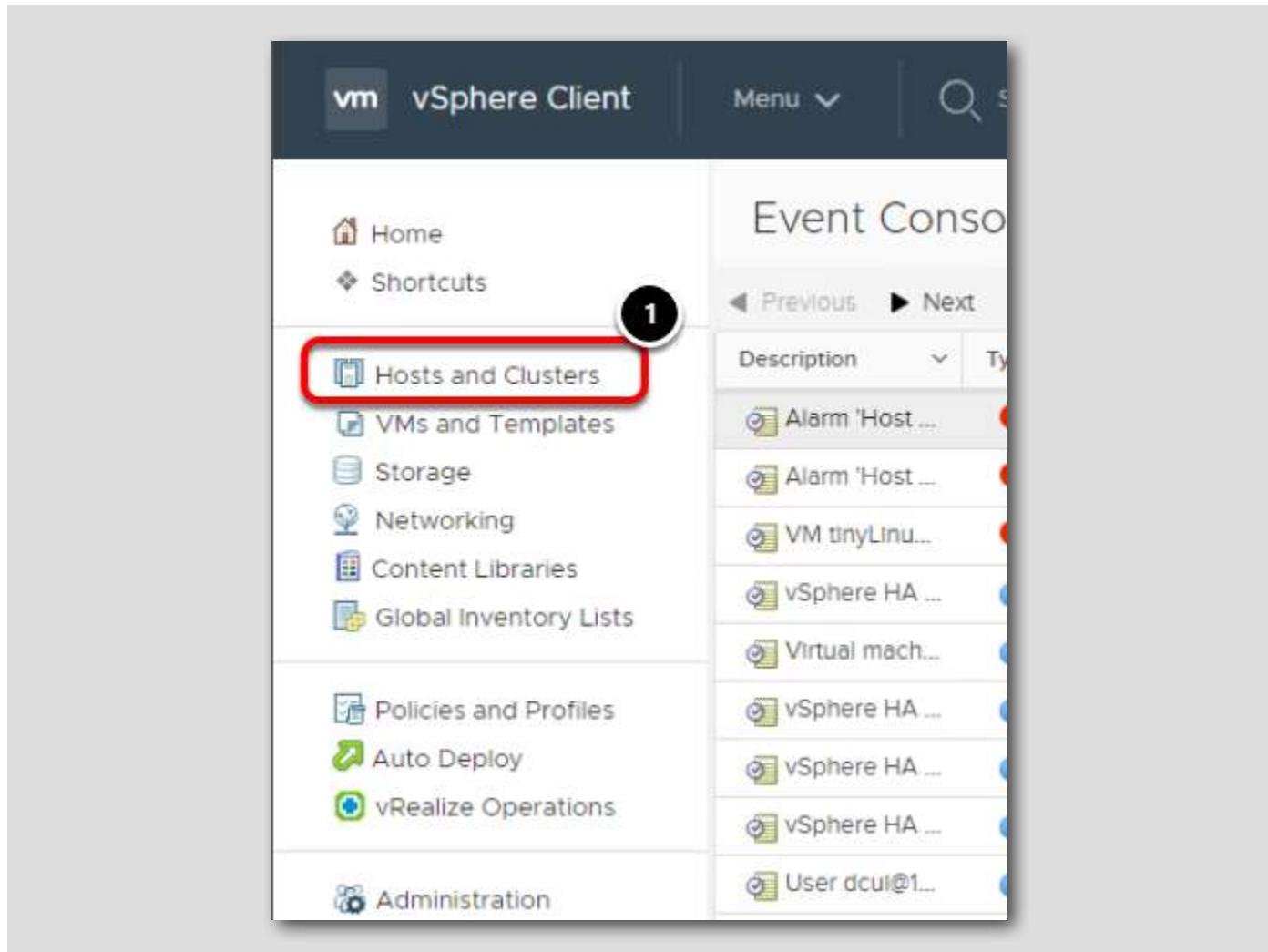
```
12/11/2020, 3:10:58 PM User VSPHERE.LOCAL\machine-d8d3462b-58da-49b3-9f5a-478d5175@127.0.0.1 logged out (login time: Friday, December 11, 2020 11:10:57 PM UTC; number of API invocations: 34; user agent: pyvmoni Python/3.7.5 (Linux; 4.19.84-t.ph3; x86_64))
```

Related events:

There are no related events.

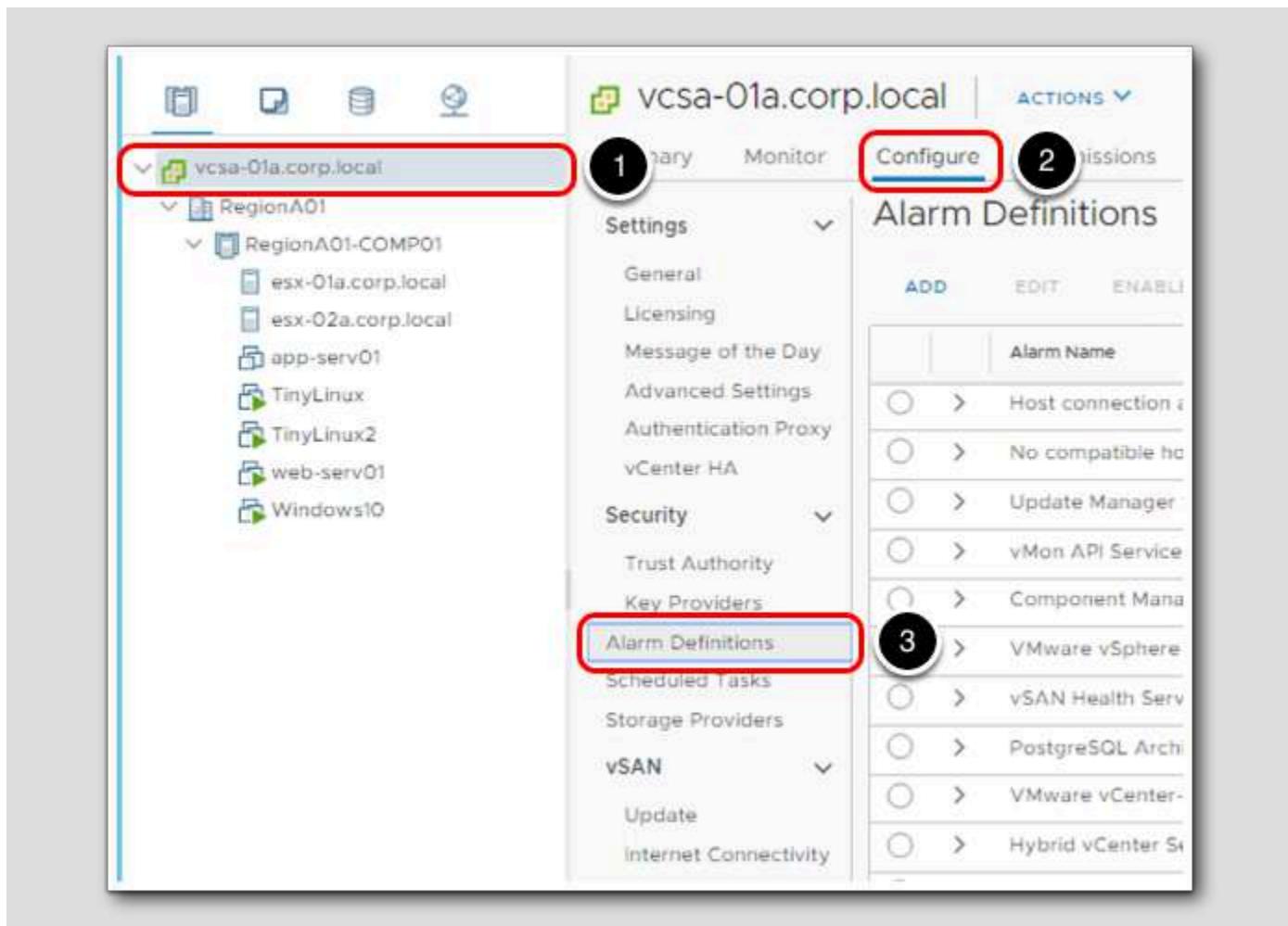
1. Click on the Type column to sort by level of severity.
2. Select an event to review the details of the event.

Setup notifications



1. Click Hosts and Clusters.

Setup Notifications



1. Select the vCenter - vcsa-01a.corp.local
2. Click the Configure tab
3. Click on Alarm Definitions. The default alarm definitions are shown.

Alarms can be defined at different levels. In the case of the highlighted alarm, you can see it is defined at the top level. Alarms that are defined at the top level are then inherited by the objects below.

Alarm Definitions

	Alarm Name	Object type	Defined in	Enabled	Last run
<input type="radio"/>	> Host connection and ...	Host	This Object	Disabled	04/24/2018
<input type="radio"/>	> No compatible host f...	Virtual Machine	This Object	Enabled	04/24/2018
<input type="radio"/>	> Update Manager Ser...	vCenter Server	This Object	Enabled	04/24/2018
<input type="radio"/>	> vMon API Service He...	vCenter Server	This Object	Enabled	04/24/2018
<input type="radio"/>	> Component Manager ...	vCenter Server	This Object	Enabled	04/24/2018
<input type="radio"/>	> VMware vSphere Aut...	vCenter Server	This Object	Enabled	04/24/2018
<input type="radio"/>	> vSAN Health Service ...	vCenter Server	This Object	Enabled	04/24/2018
<input type="radio"/>	> PostgreSQL Archiver ...	vCenter Server	This Object	Enabled	04/24/2018
<input checked="" type="radio"/>	> VMware vCenter-Ser...	vCenter Server	This Object	Enabled	04/24/2018

Alarms can be defined at different levels. In the case of the highlighted alarm, you can see it is defined at the top level (vCenter Server). Alarms that are defined at the top level are then inherited by the objects below.

Defining an Alarm

The screenshot shows the 'Alarm Definitions' screen in vSphere. At the top, there are buttons for 'ADD', 'EDIT' (which is highlighted with a red box), 'DISABLE', and 'DELETE'. Below the buttons is a table with columns: 'Alarm Name', 'Object type', and 'Defined In'. The table contains four rows of data:

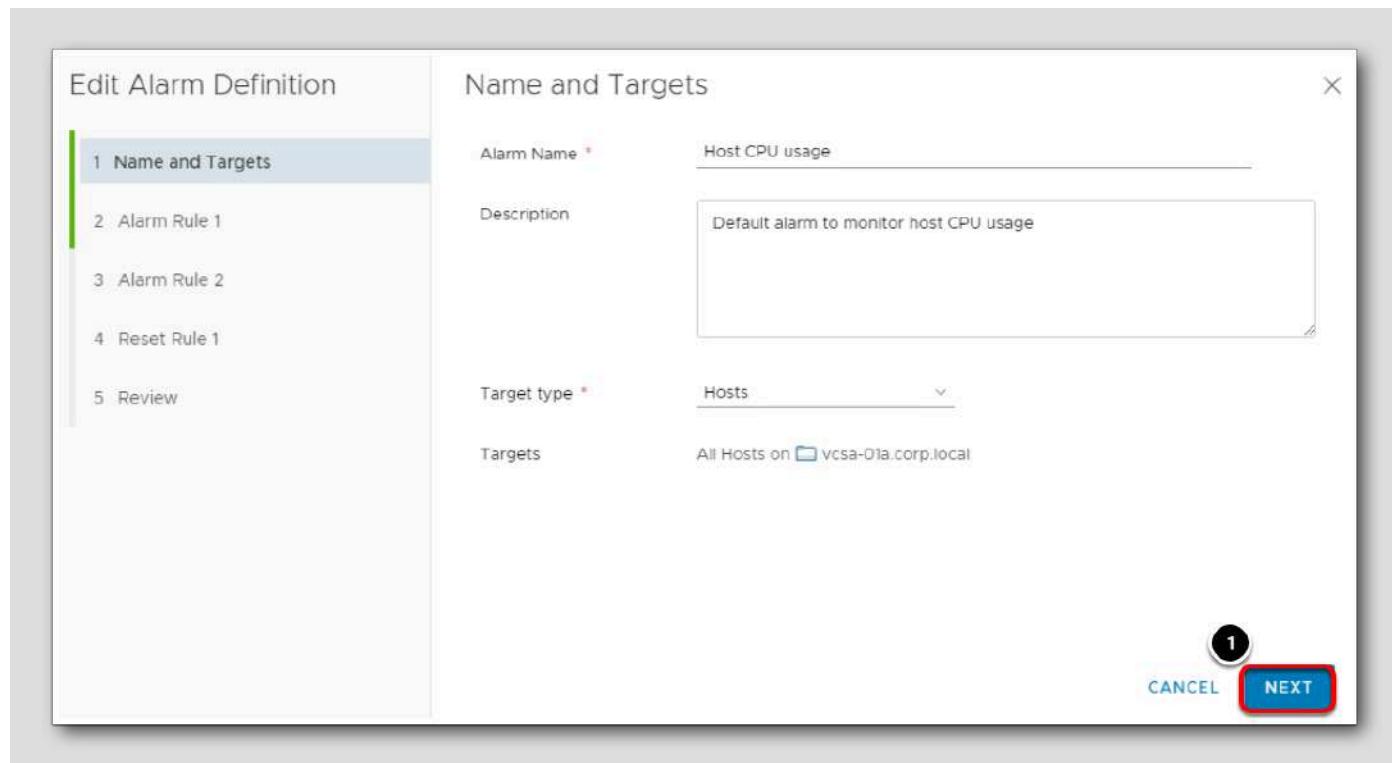
Alarm Name	Object type	Defined In
vCenter Server	vCenter Server	This Object
Cluster	Cluster	This Object
Host CPU usage	Host	This Object
Virtual machine CPU ...	Virtual Machine	This Object

Three numbered circles with arrows point to specific elements:

- Circle 1 points to the 'CPU' search term in the 'Alarm Name' filter field.
- Circle 2 points to the 'Host CPU usage' row in the table.
- Circle 3 points to the 'EDIT' button at the top of the screen.

1. Click on the Alarm Name filter field and type cpu in the search field.
2. Select the Host CPU usage alarm
3. Click the Edit button

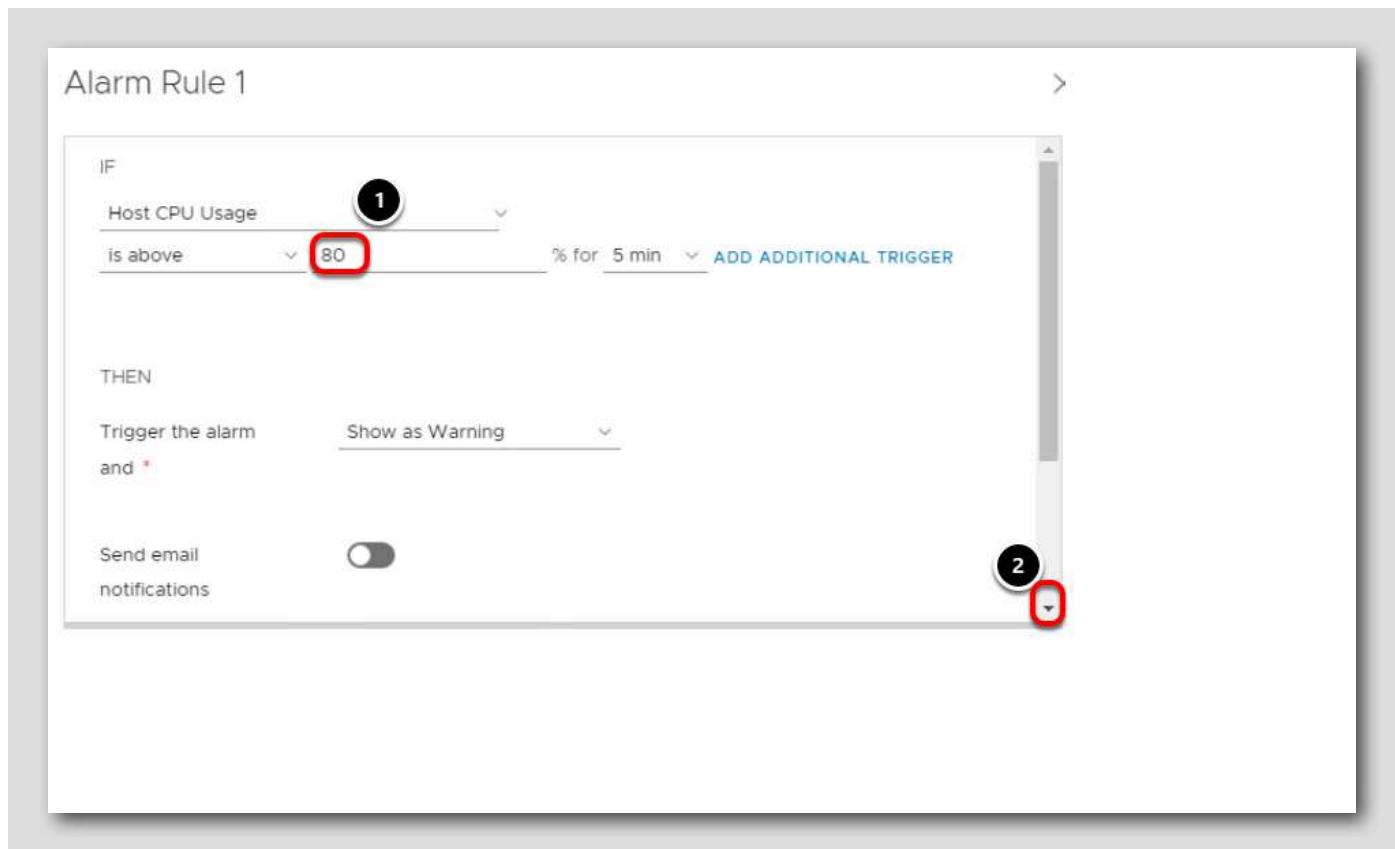
Name and Targets



The Name and Targets screen defines the name of the alarm (Host CPU usage), what object it applies to (Hosts) and where the objects are located.

1. Click **Next**.

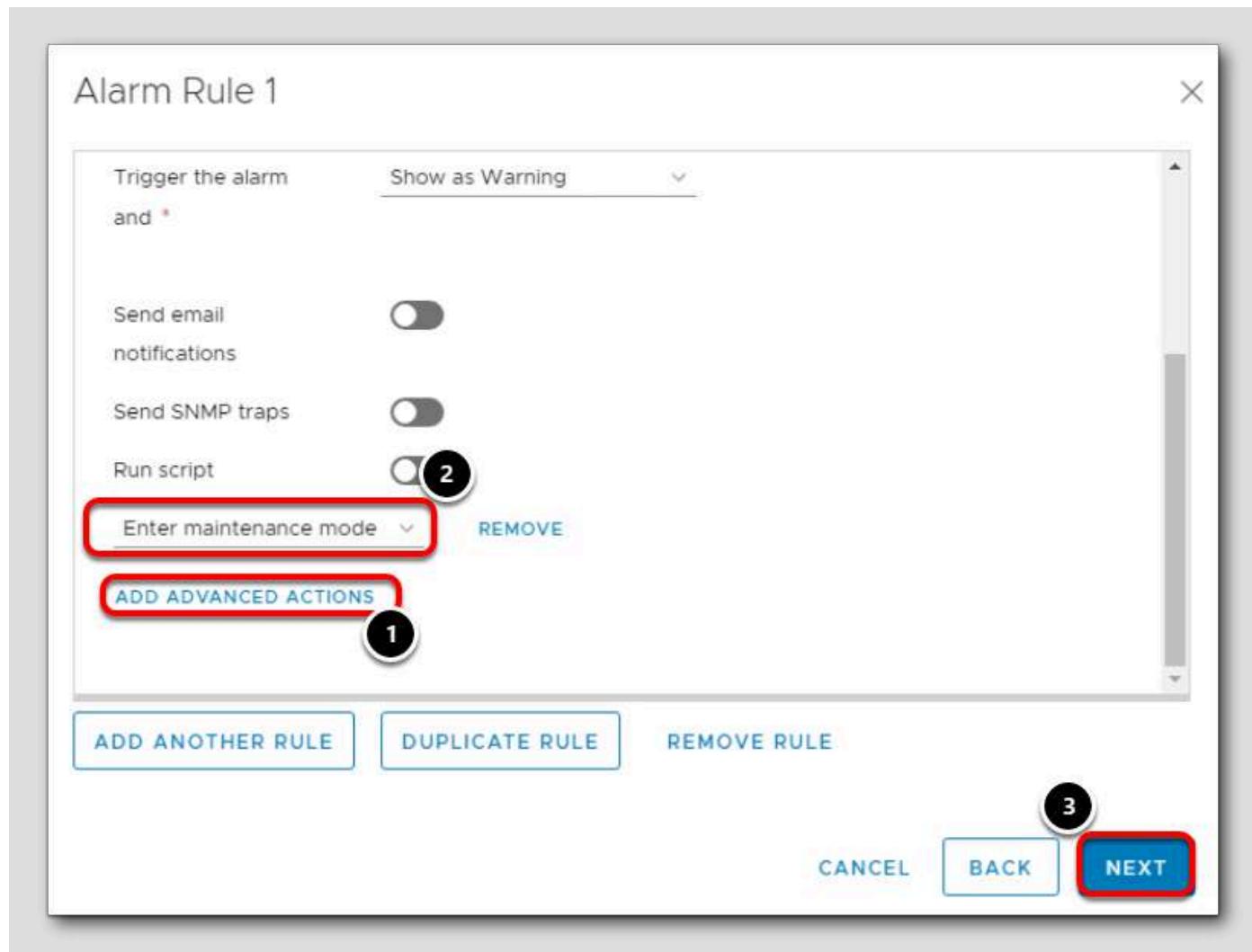
Alarm Rule 1



1. Change the percentage of 75% to 80%.
2. Use the scroll bar to scroll to the bottom.

Notice this will trigger a Warning alarm.

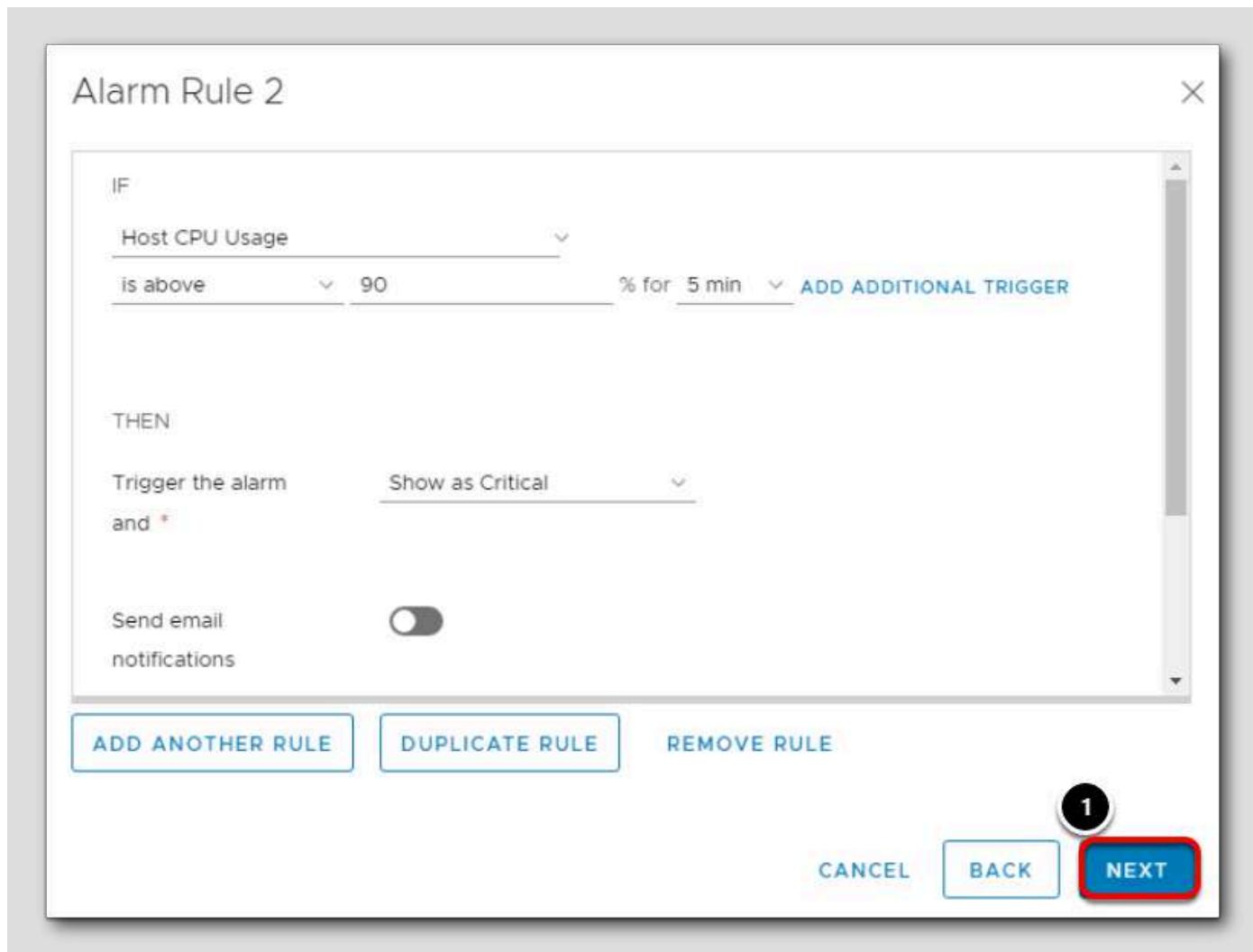
Add Advanced Action



1. Click on Add Advanced Action.
2. From the drop-down menu (Select an advanced action), select Enter maintenance mode.
3. Click Next

When a Host's CPU runs at or above 80% for more than 5 minutes, a Warning alarm will be triggered, and the Host will be put in Maintenance mode. Maintenance mode is covered in Module 3, but when a host is in this state, it is taken offline and any virtual machines that are running on it will be moved to other hosts in the cluster. This lets maintenance be performed on hosts without suffering downtime.

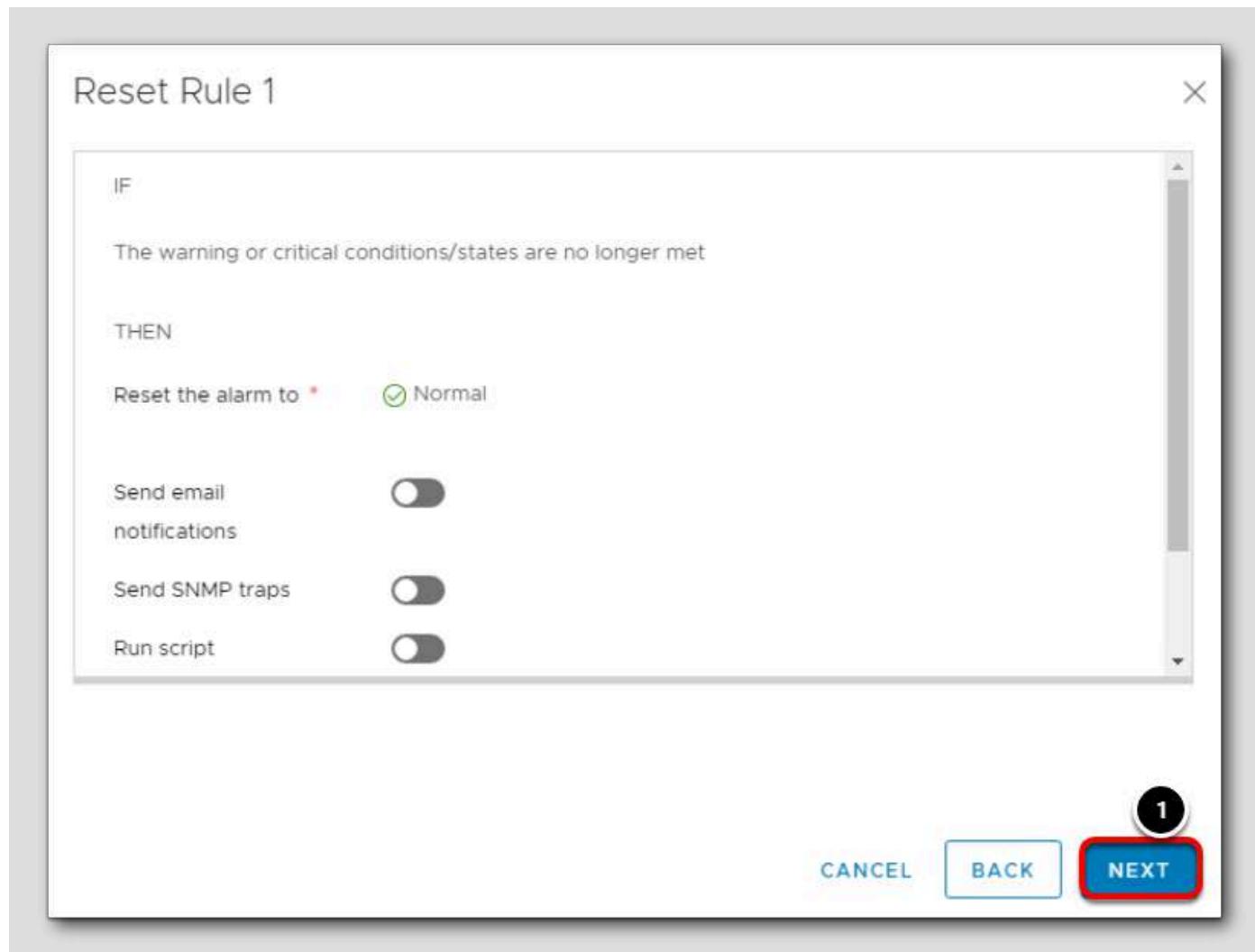
Alarm Rule 2



On this screen we can set additional actions based on when a Host's CPU is about 90% for 5 minutes. In this case, it would trigger a Critical alarm. Additional actions could be taken when a Host is in this state.

1. Click **Next**.

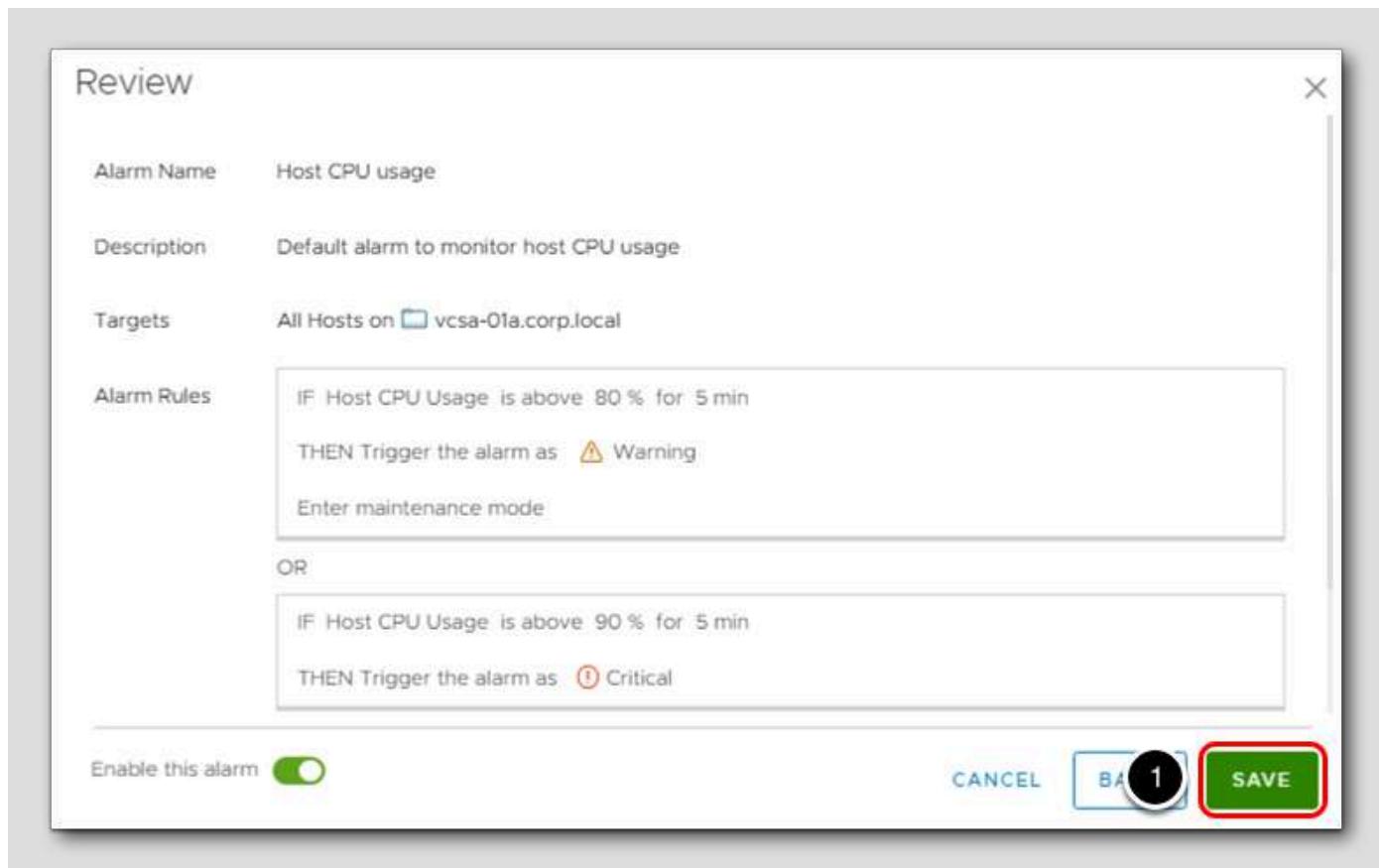
Reset Rule 1



If the conditions that originally triggered the alarm are no longer present, additional actions can take place. As an example, once a Host's CPU is no longer at 80% for more than 5 minutes, an email notification could be sent.

1. Click **Next**.

Review



The Review screen shows what was configured.

1. Click **Save** to keep the changes made to the Alarm.

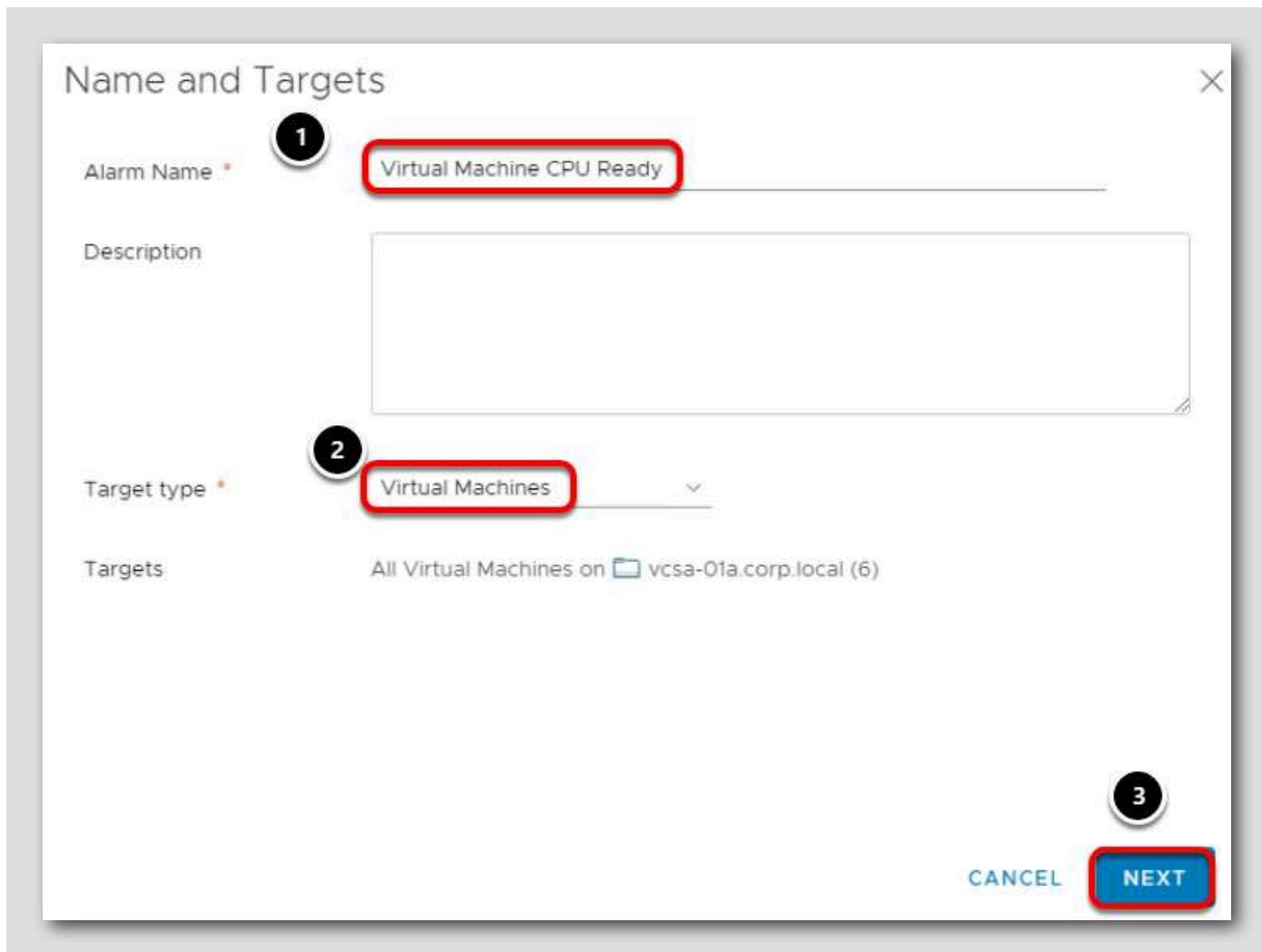
Create New Alarm

The screenshot shows the vSphere Client interface for managing alarms. The left sidebar has sections for Settings (General, Licensing, Message of the Day, Advanced Settings, Authentication Proxy, vCenter HA), More (Alarm Definitions, Scheduled Tasks, Key Management Serv..., Storage Providers), and vSAN (Update, Internet Connectivity). The 'More' section has 'Alarm Definitions' selected. The main pane is titled 'Alarm Definitions' and shows a table with four rows. The first row has an 'ADD' button highlighted with a red circle and the number '1'. The table columns are 'Alarm Name', 'Object type', and 'Definition'. The rows show: 'CPU Exhaustion on v...', 'vCenter Server'; 'vSAN health alarm 'C...', 'Cluster'; 'Host CPU usage', 'Host'; and 'Virtual machine CPU ...', 'Virtual Machine'. Each row has a circular icon with a right-pointing arrow.

	Alarm Name	Object type	Definition
○ >	CPU Exhaustion on v...	vCenter Server	TH
○ >	vSAN health alarm 'C...	Cluster	TH
○ >	Host CPU usage	Host	TH
○ >	Virtual machine CPU ...	Virtual Machine	TH

1. To add a new alarm, click Add.

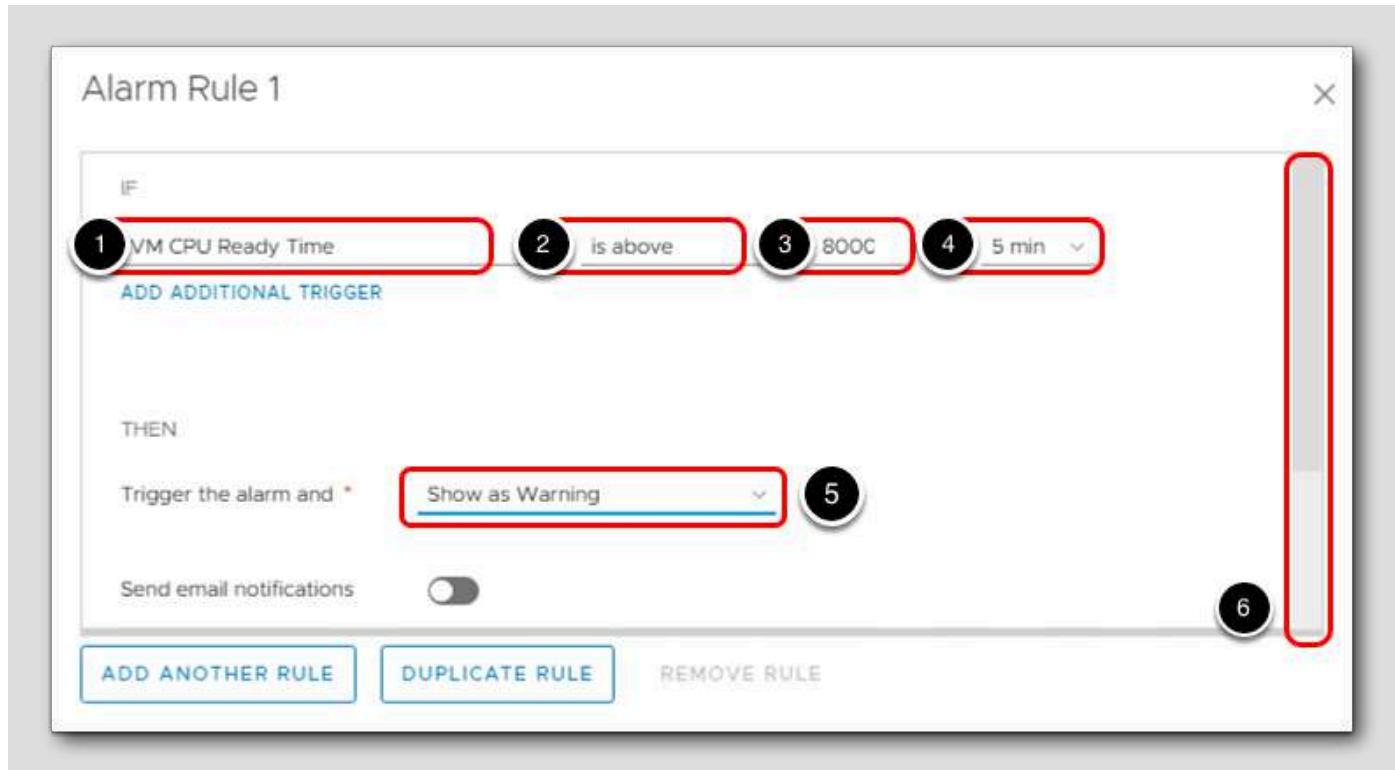
New Alarm Definition



We will be creating an alarm that will migrate a VM if CPU Ready exceeds an average of 8000ms over the course of 5 minutes.

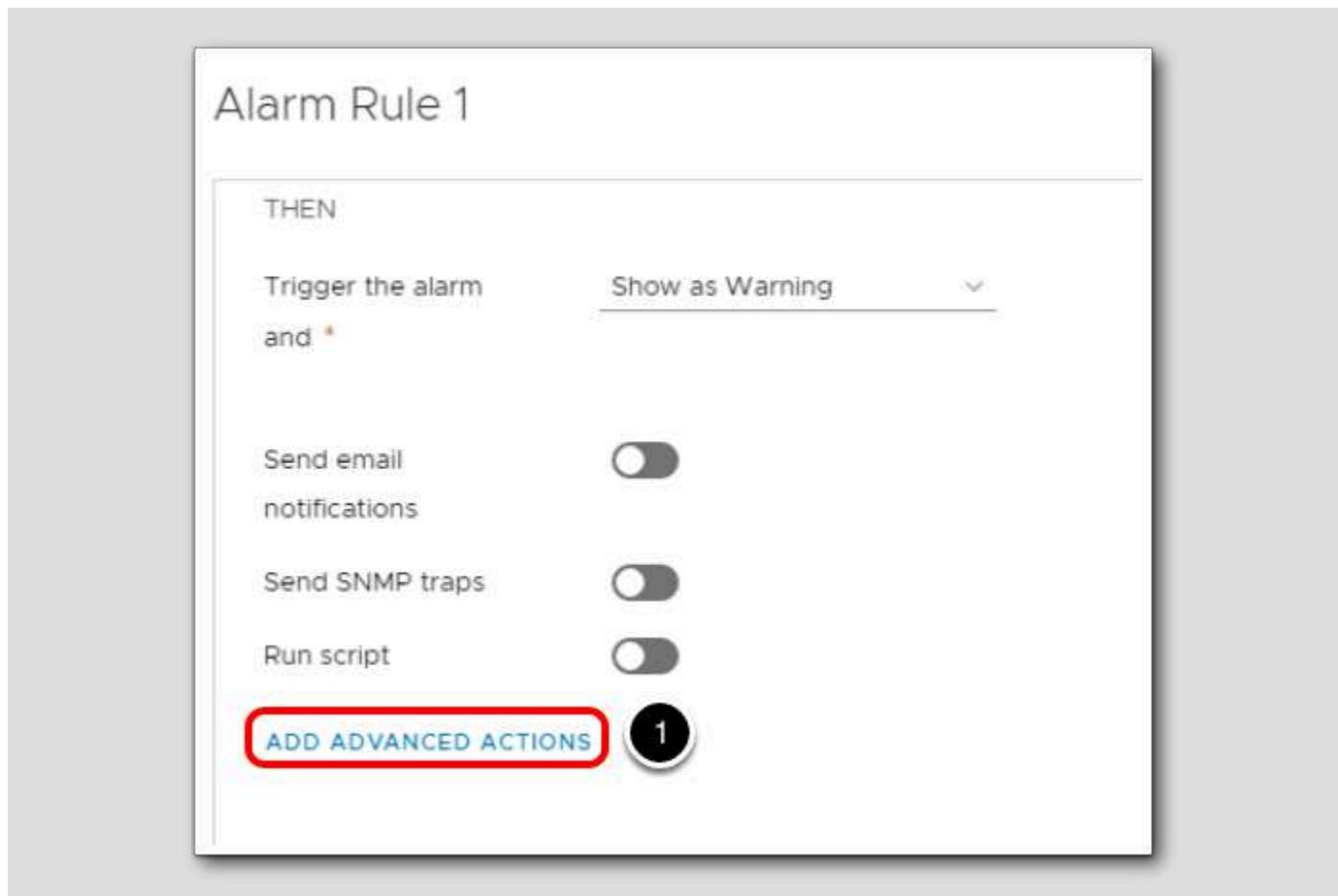
1. Enter Virtual Machine CPU Ready for the Alarm name.
2. Change Monitor from vCenter Server to Virtual Machines
3. Click **Next** to move to the Alarm Rule 1 screen.

Define CPU Ready Time



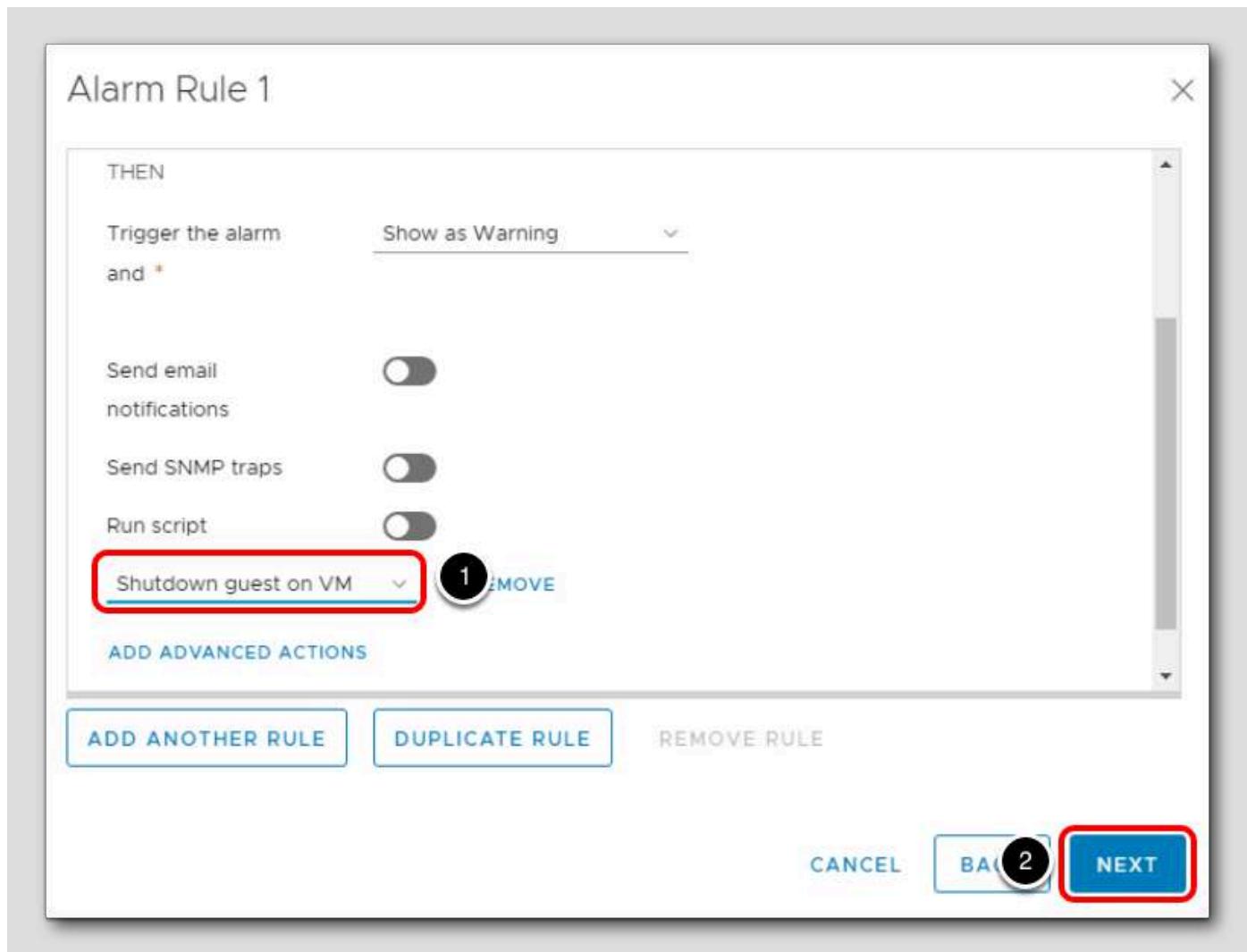
1. Click in the field under IF and select VM CPU Ready Time.
2. Change the select an operator filed to is above.
3. Type 8000 in the ms field
4. Use the drop-down menu to select 5 min.
5. Select Show as Warning in the Trigger the alarm menu.
6. Use the scroll bar to scroll to the Add advanced actions section.

Add Advanced Action



1. Click Add Advanced Actions

Migrate VM

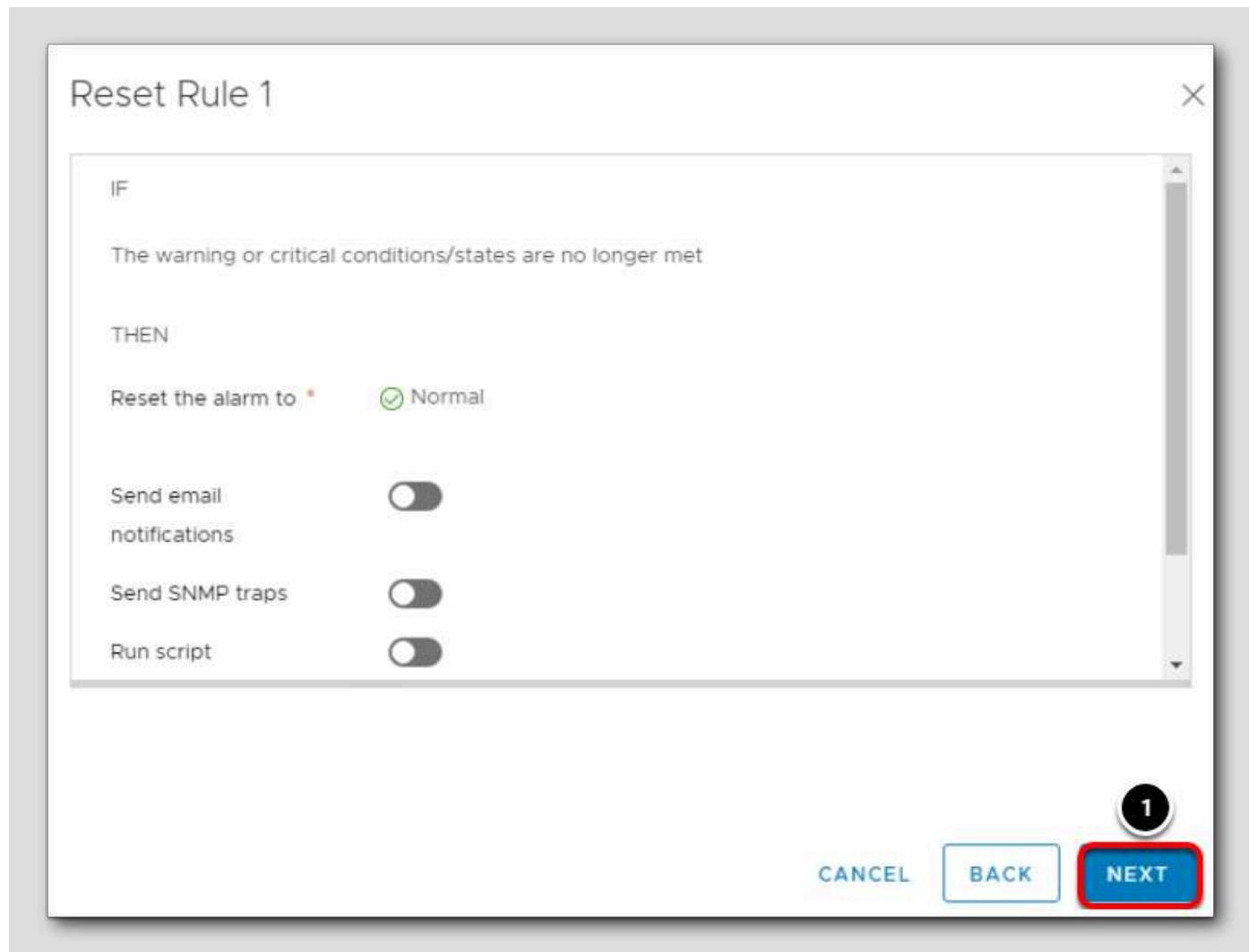


1. From the drop-down menu, select Shutdown guest on VM.

This will gracefully shutdown the virtual machine rather than just powering it off.

2. Click **Next**.

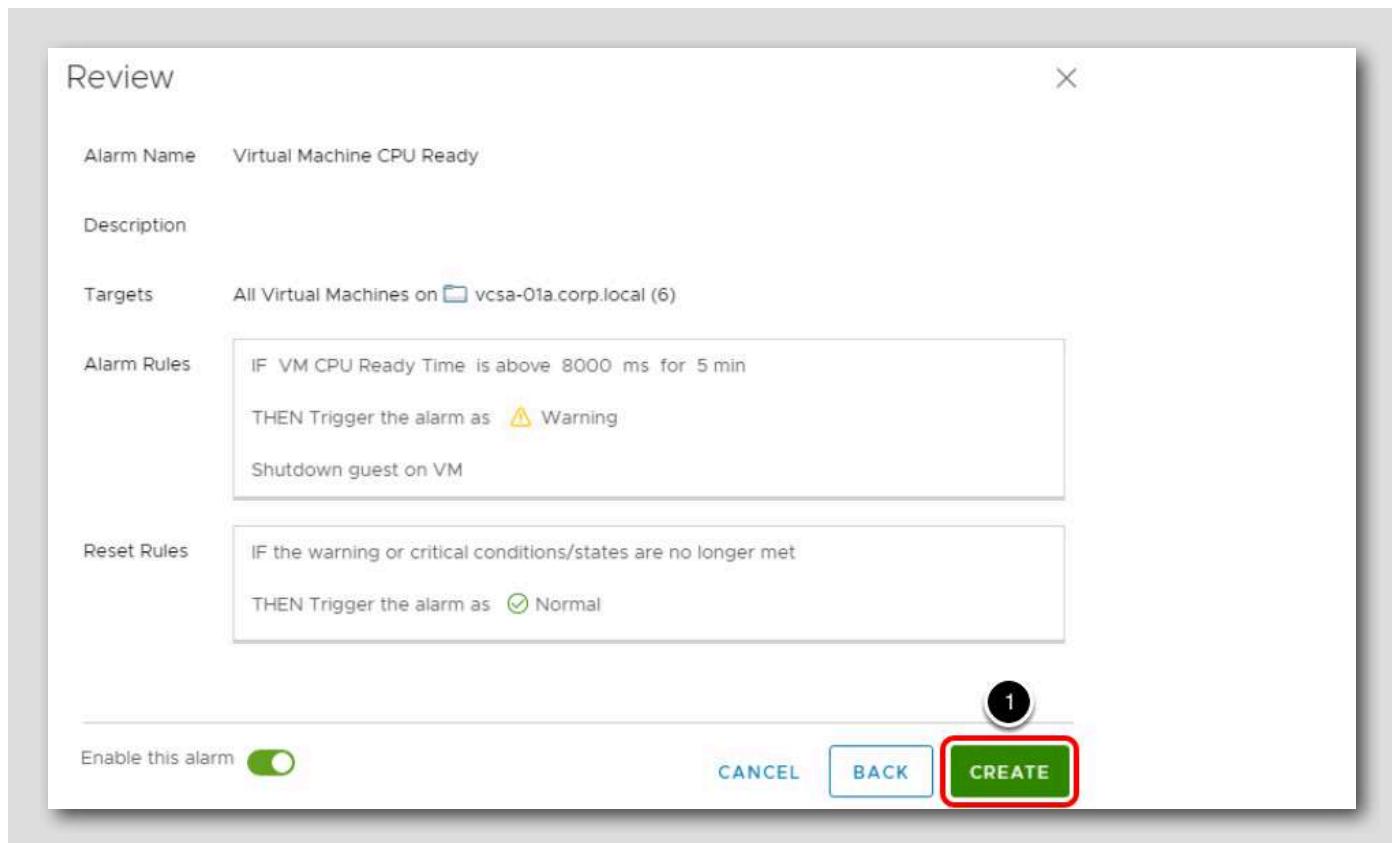
Reset Rule 1



Additional options could be specified once the conditions are clear.

1. Click **Next**

Review



The Review screen shows the details of what was configured for the new alarm.

1. Click Create.

New Alarm Created

Alarm Definitions

	Alarm Name	Object type	Defined In	
<input type="radio"/>	CPU Exhaustion on vcsa-01a	vCenter Server	 This Object	E
<input type="radio"/>	vSAN health alarm 'CPU AES-NI is disabled on ...	Cluster	 This Object	E
<input type="radio"/>	Host CPU usage	Host	 This Object	E
<input type="radio"/>	Virtual Machine CPU Ready	Virtual Machine	 This Object	E
<input type="radio"/>	Virtual machine CPU usage	Virtual Machine	 This Object	E

If the Alarm Name field is still filtering by "cpu", the newly created alarm is displayed. If not, simply click on the Alarm Name field and type cpu ready to see it.

Configure Shares and Resources

[161]

Shares specify the relative importance of a virtual machine (or resource pool). If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources. This lab starts with a video walking you through the process of working with shares and resources. The remainder of this module walks you through making the changes to a VM's resources.

Shares are typically specified as High, Normal, or Low

Video: DRS with Scalable Shares in vSphere 7 (4:17)

[162]

This video explains how scalable shares are and how they are used in order to effectively distribute compute and memory resources among virtual machines.

<https://www.youtube.com/watch?v=jkp25I4R0R8>



Shares, Limits and Reservations

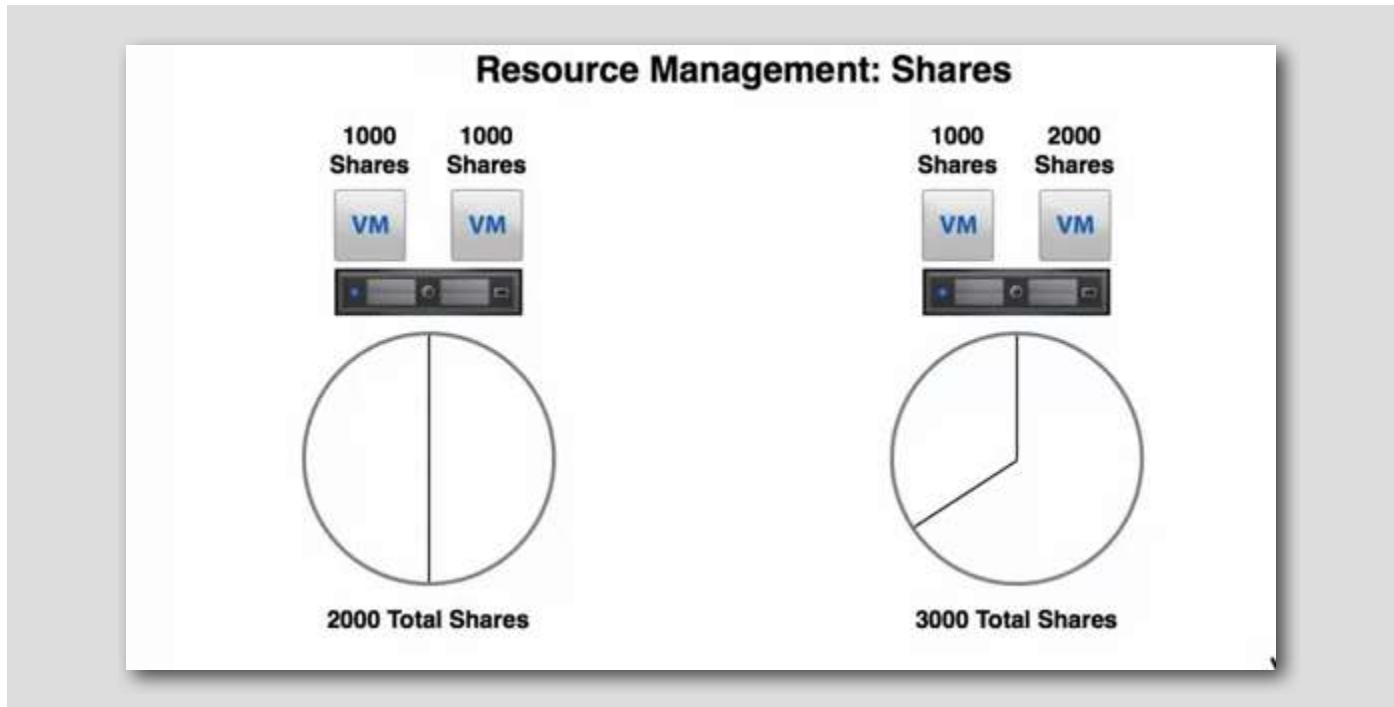
Resource Management

Shares: relative importance of a virtual machine (VM)

Reservation: guaranteed minimum allocation for a VM

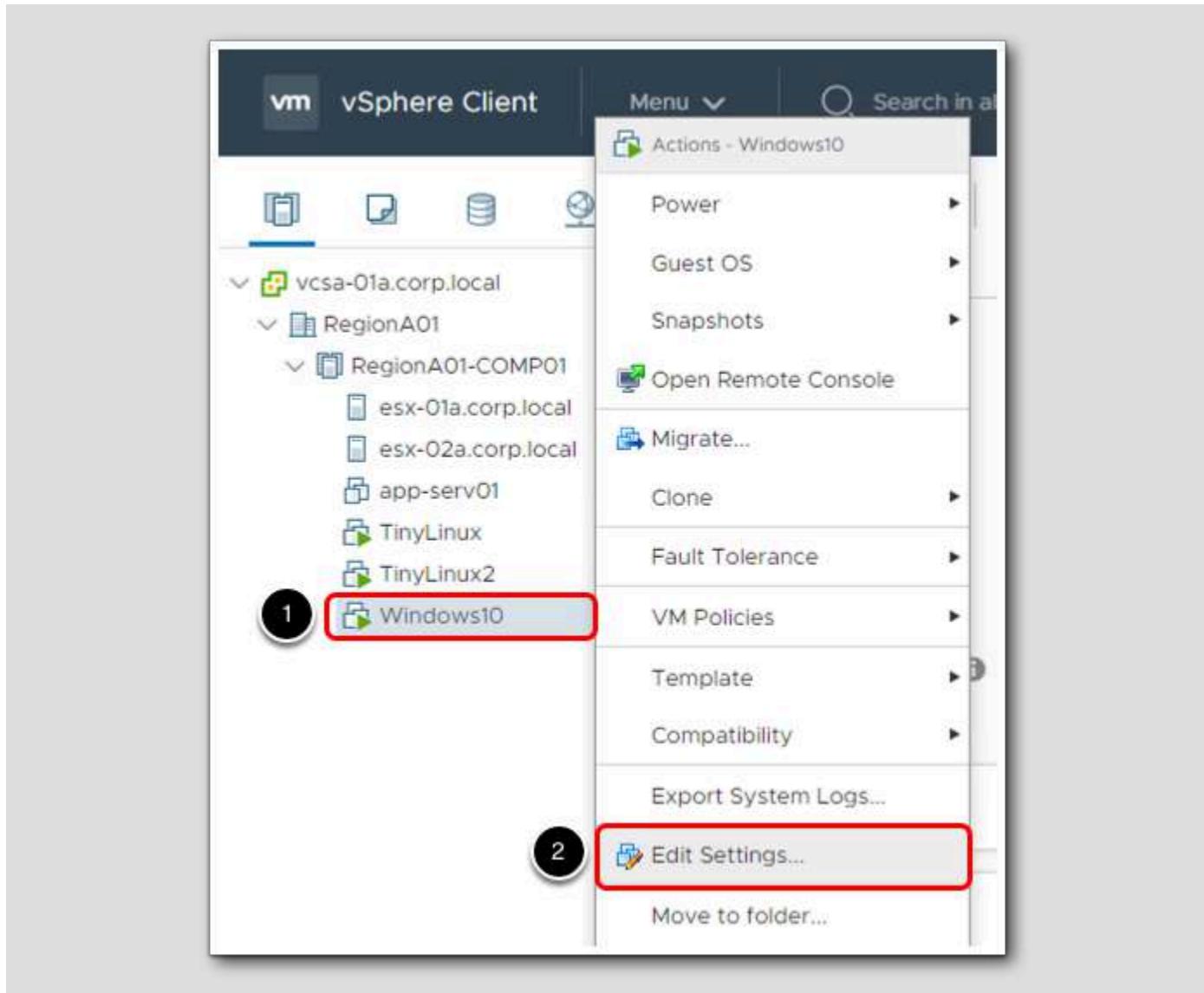
Limit: upper bound of resource that can be allocated to a VM

Understanding Shares



The above example shows 2 VM's, one a development VM and the other a Production VM. On the left-hand side of the diagram, you can see the CPU shares are equal. We want to make sure the Production VM gets the majority of the CPU resources when there is contention for those resources in the environment. Changing the shares for the production VM from 1000 shares to 2000 shares accomplishes this goal. The new settings are shown on the right side of the diagram.

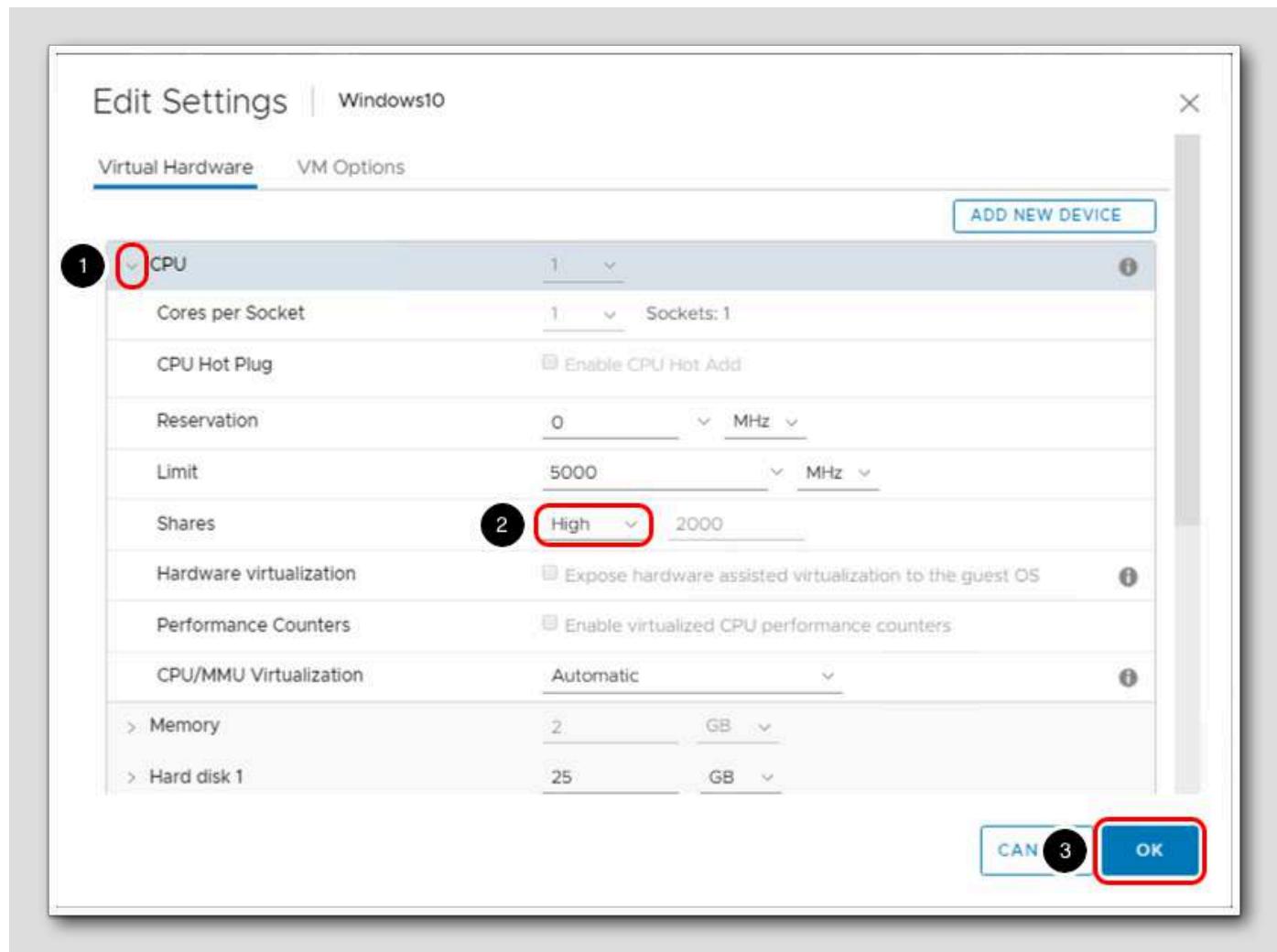
Review CPU settings



1. Right click the windows10 virtual machine.

2. Select Edit Settings...

Changing Resource Allocation of CPU shares.



Note the current setting for **Shares** is set to 1000.

1. Expand the CPU section of the settings.
2. From the Shares drop down box, Click **High** to change the setting of the CPU shares.
3. Click **OK**

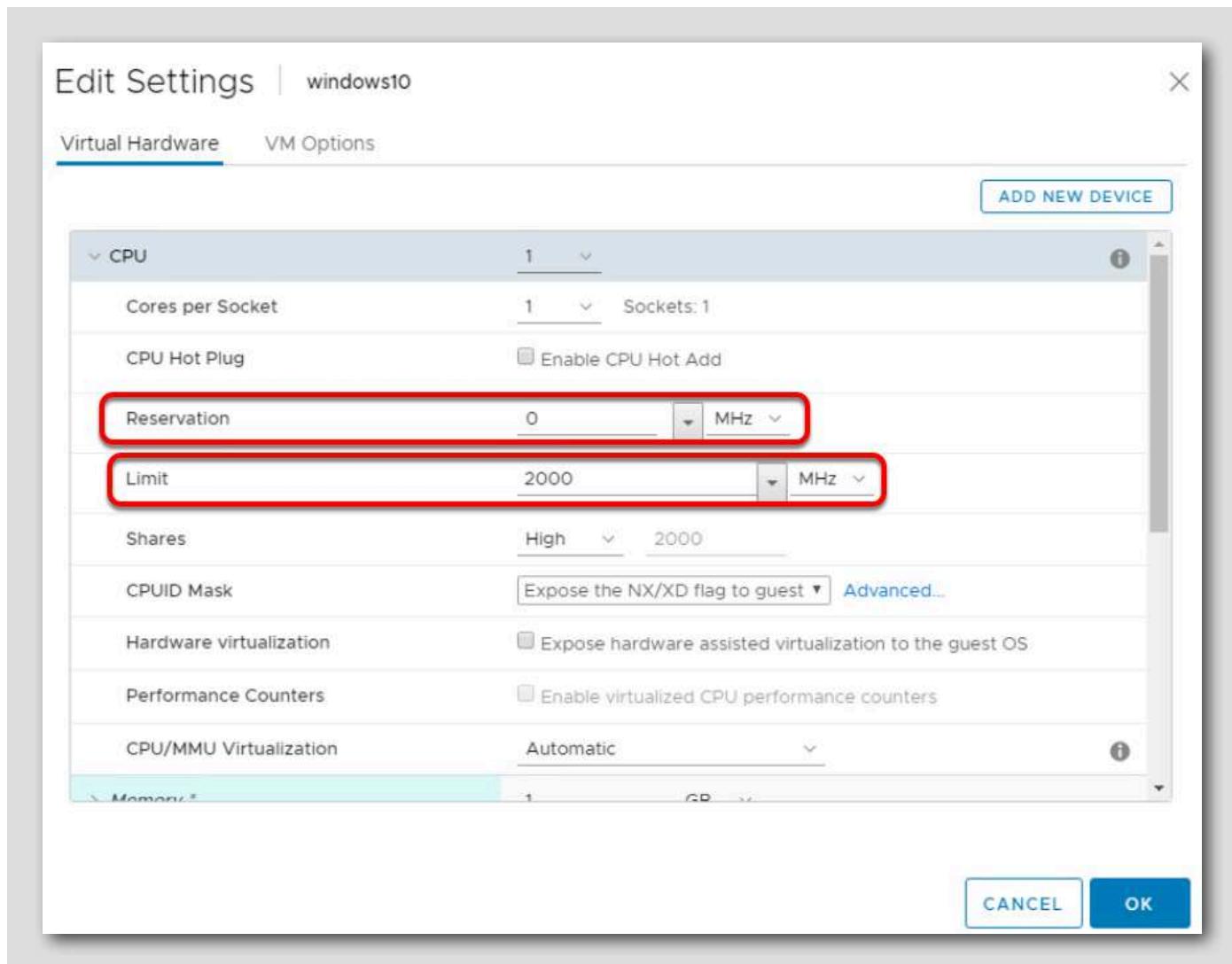
Review Settings

The screenshot shows the vSphere Web Client interface for a VM named "Windows10". The "Summary" tab is selected. In the "Hardware" section, the "CPU" row is expanded, revealing settings for Utilization, Reservation, Limit, and Hardware. The "Shares" setting is highlighted with a red circle and a red border, indicating it has been modified. The original value of 2000 (High) is circled with a black marker.

Setting	Value
Utilization	1 CPU(s), 140 MHz used
Shares	2000 (High)
Reservation	0 MHz
Limit	5000 MHz
Hardware	Disabled

1. The new Shares setting of 2000 is now shown in the VM Hardware section.
2. You may have to expand the VM Hardware section to see it.

Settings for Limits and Reservations.



Limits and Reservations are set with the same procedure. When you click on the "edit" settings for a VM, you will find the ability to set the Limit and Reservations. Limit restricts a VM from using more than the limit setting. Reservations guarantee a minimum amount of a resource be available for the virtual machine. Try out some settings for Limits and Reservations. One note is that if you try to reserve more of a resource such as memory or CPU than is available, the VM may not power on.

Migrating Virtual Machines with VMware vMotion

Planned downtime typically accounts for over 80% of datacenter downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule downtime windows.

The vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers without service interruption. Administrators can perform faster and completely transparent maintenance operations, without being forced to schedule inconvenient maintenance windows. With vSphere vMotion, organizations can:

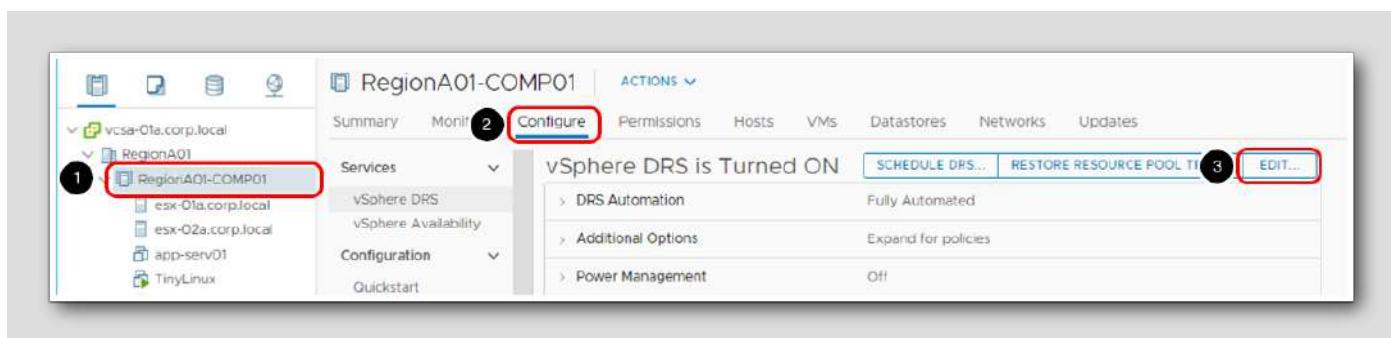
- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

Another feature of vSphere, Storage vMotion allows a virtual machine to be migrated to different storage devices with zero downtime. This technology is covered in more detail in Module 3.

In this lesson, you will learn how to work with vMotion and move virtual machines to different hosts within the cluster.

Edit Cluster Settings

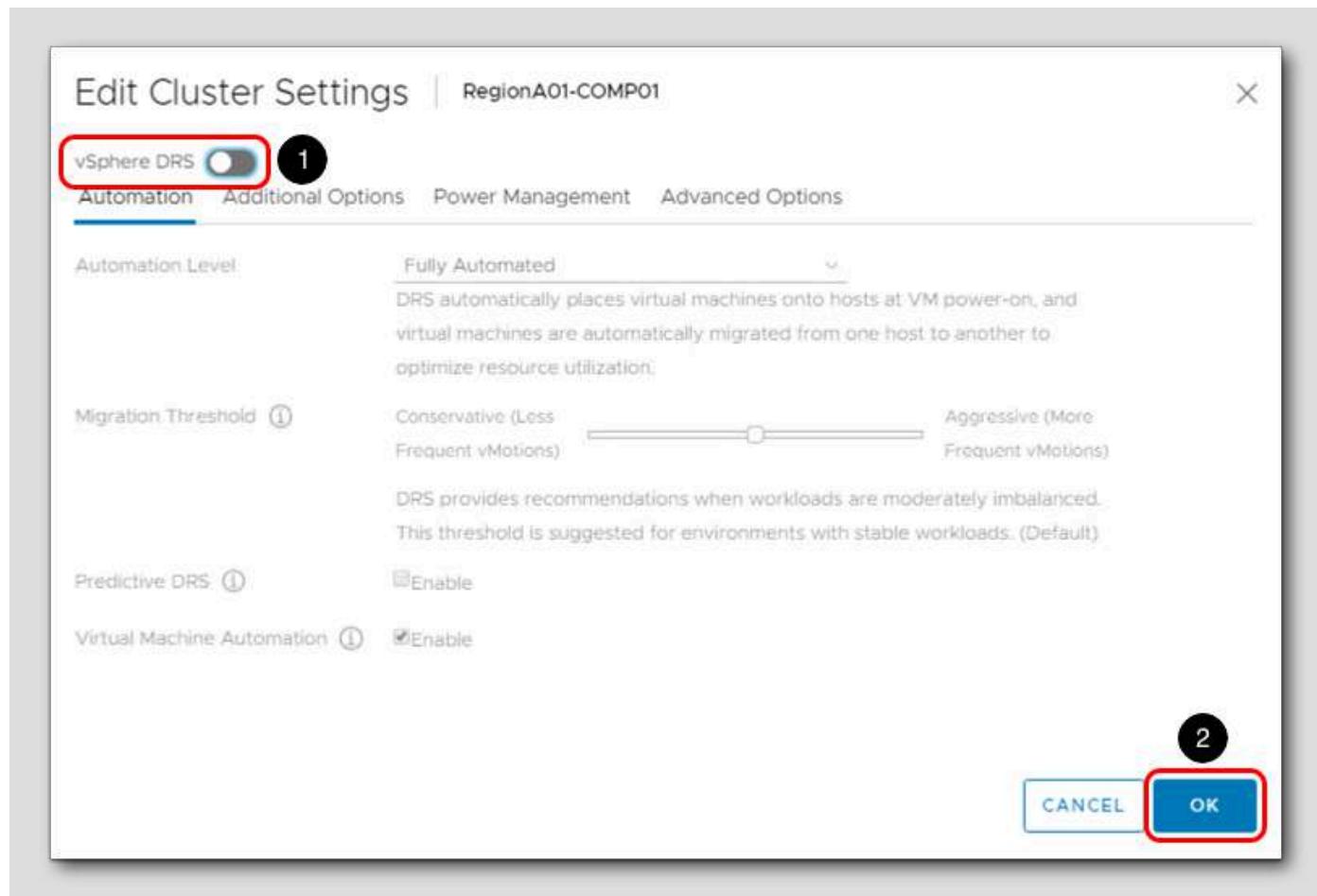
[170]



We will disable DRS and then migrate all of the virtual machines esx-02a.corp.local hosts over to esx-01a.corp.local. This will also help prepare us for the next lesson on Performance.

1. Select RegionA01-COMP01
2. Click the Configure tab
3. Click the Edit button

Disable DRS



1. Flip the switch to disable vSphere DRS.

2. Click OK

By disabling DRS, this will prevent the virtual machines from being migrated back to esx-01a.corp.local.

esx-02a.corp.local

The screenshot shows the vSphere Client interface. On the left, the navigation tree is expanded to show 'vcsa-01a.corp.local' and its subfolders 'RegionA01' and 'RegionA01-COMP01'. Within 'RegionA01-COMP01', the folder 'esx-01a.corp.local' is selected, highlighted with a red box and labeled '1'. On the right, the main content area displays the 'VMs' tab, which is also highlighted with a red box and labeled '2'. Below the tabs, there is a table listing four virtual machines:

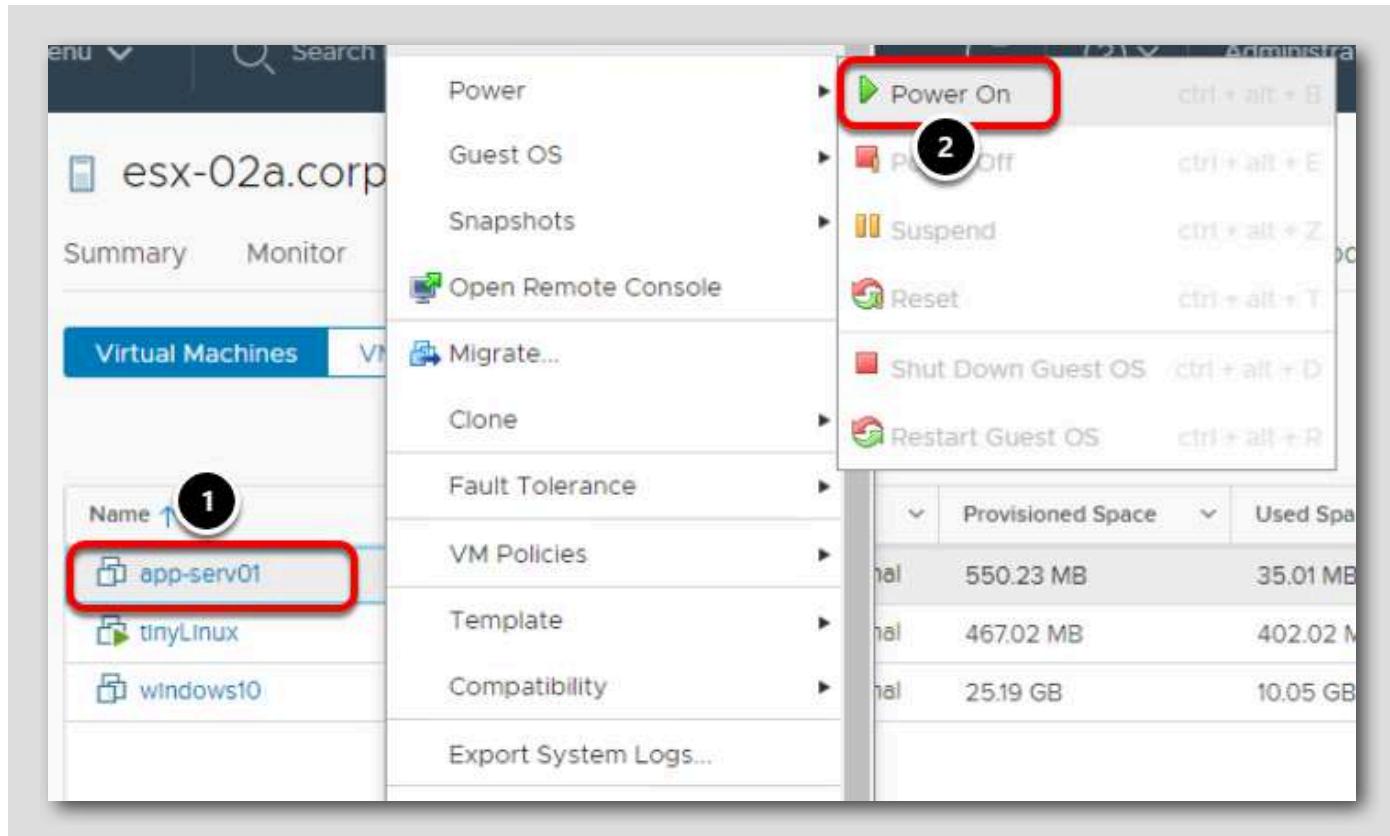
Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
app-serv01	Powered Off	Normal	734.25 MB	35.01 MB	0 Hz	0 B
TinyLinux2	Powered On	Normal	436.84 MB	371.84 MB	0 Hz	155 MB
web-serv01	Powered On	Normal	18.08 GB	18.08 GB	0 Hz	101 GB

1. Select esx-01a.corp.local

2. Click the VMs tab

Depending on what other modules you have taken, you may see more VMs.

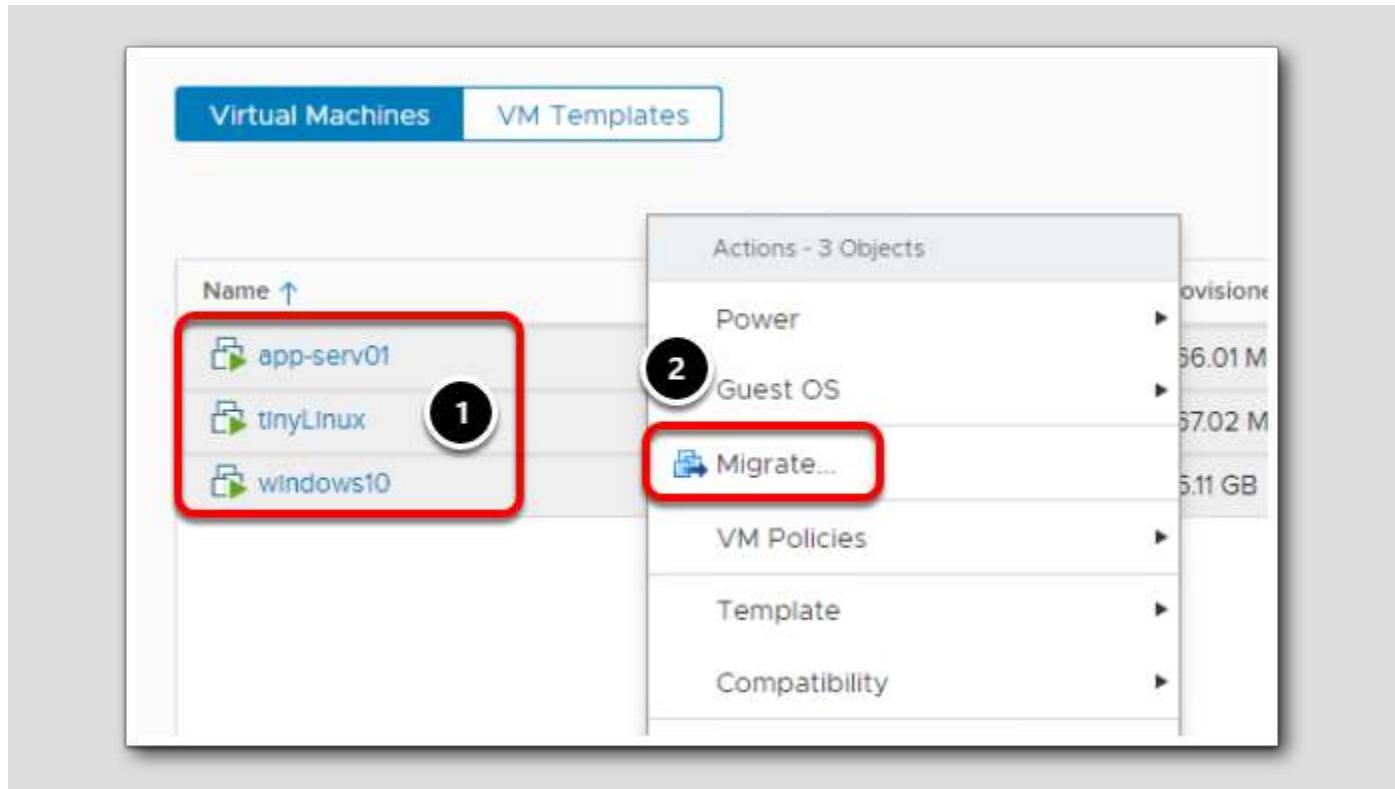
Power on VMs



1. Look for any virtual machines that are Powered Off and select them. Multiple virtual machines can be selected by holding the Ctrl key and clicking on them.
2. Right click and select Power/Power On

Do this for every powered off virtual machine, otherwise the next step will fail.

Migrate VMs



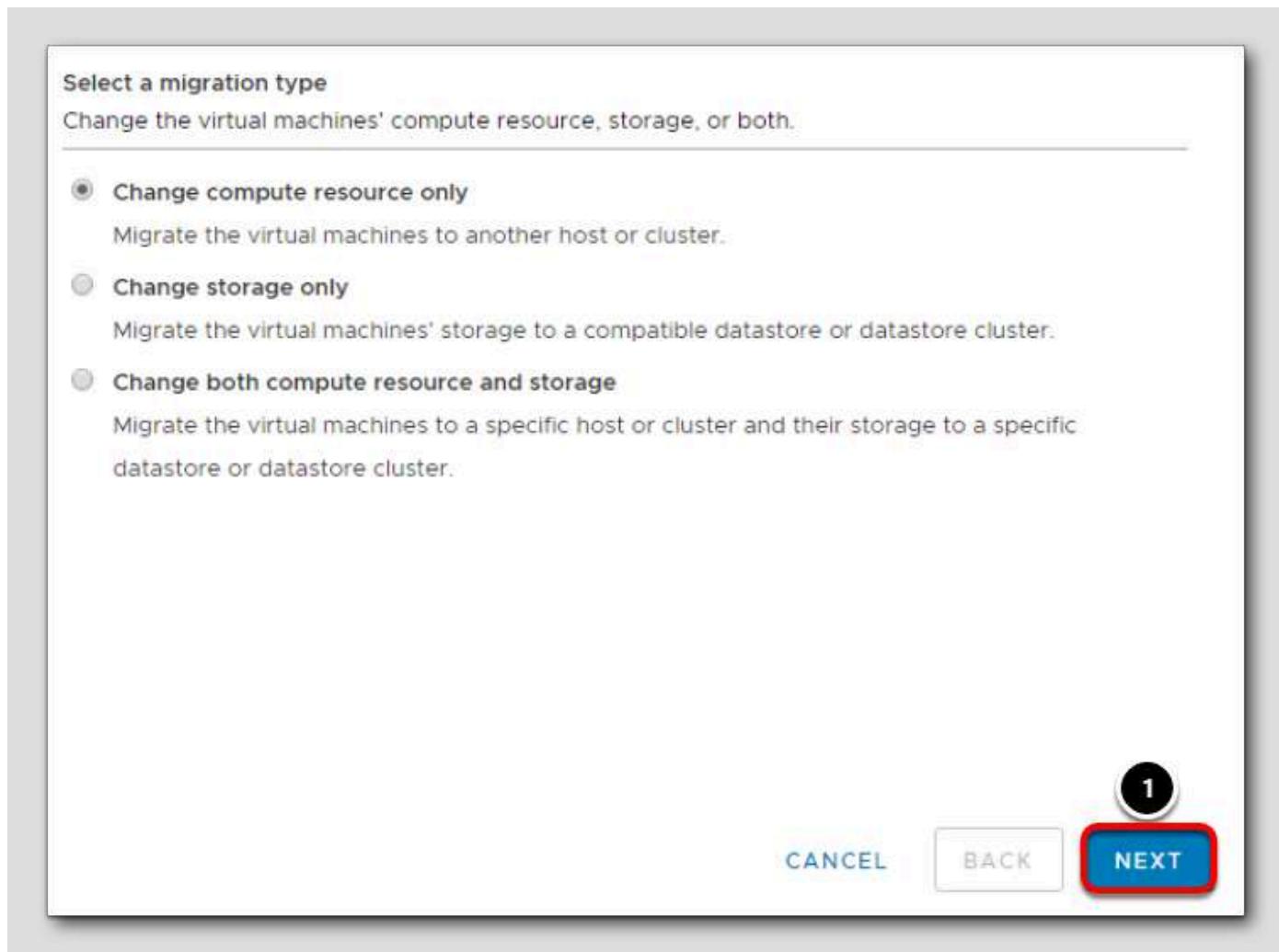
1. Select all the virtual machines (click the first one on the list, hold the shift key, click the last one on the list).
2. Right click and select **Migrate...**

Migrate



Click **Yes** to start the migration process.

Migration Type



1. Leave the default setting and click Next

In addition to changing what ESXi host the virtual machine will run on (using compute resources), the virtual machine can be moved to different datastores (storage) if needed. A virtual machine can also be moved to a different host and storage at the same time. More on migrating to different storage is covered in Module 3, in the Storage vMotion lesson.

Compute Resource

3 Virtual Machines - Migrate

✓ 1 Select a migration type
2 **Select a compute resource**

3 Select networks
4 Select vMotion priority
5 Ready to complete

Select a compute resource
Select a cluster, host, vApp or resource pool to run the virtual machines.

Hosts Clusters Resource Pools vApps

Name ↑ State Status Cluster

1 esx-02a.corp.local Connected ✓ Normal RegionA01-CO...

Filter 2 Items

Compatibility

app-serv01
esx-02a.corp.local
⚠ No guest OS heartbeats are being received. Either the guest OS is not responding or VMware Tools is not configured correctly.

CANCEL BA 2 NEXT

1. Select esx-02a.corp.local

2. Click Next

Since we want to move all the virtual machines to esx-02a.corp.local, we are selecting a specific host. We could also place it in a Cluster and let DRS decide the best host to move it to.

Networks

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
VM-RegionA01-vDS-COMP	2 VMs / 2 Network adapters	VM-RegionA01-vDS-COMP
VM Network	2 VMs / 2 Network adapters	VM Network

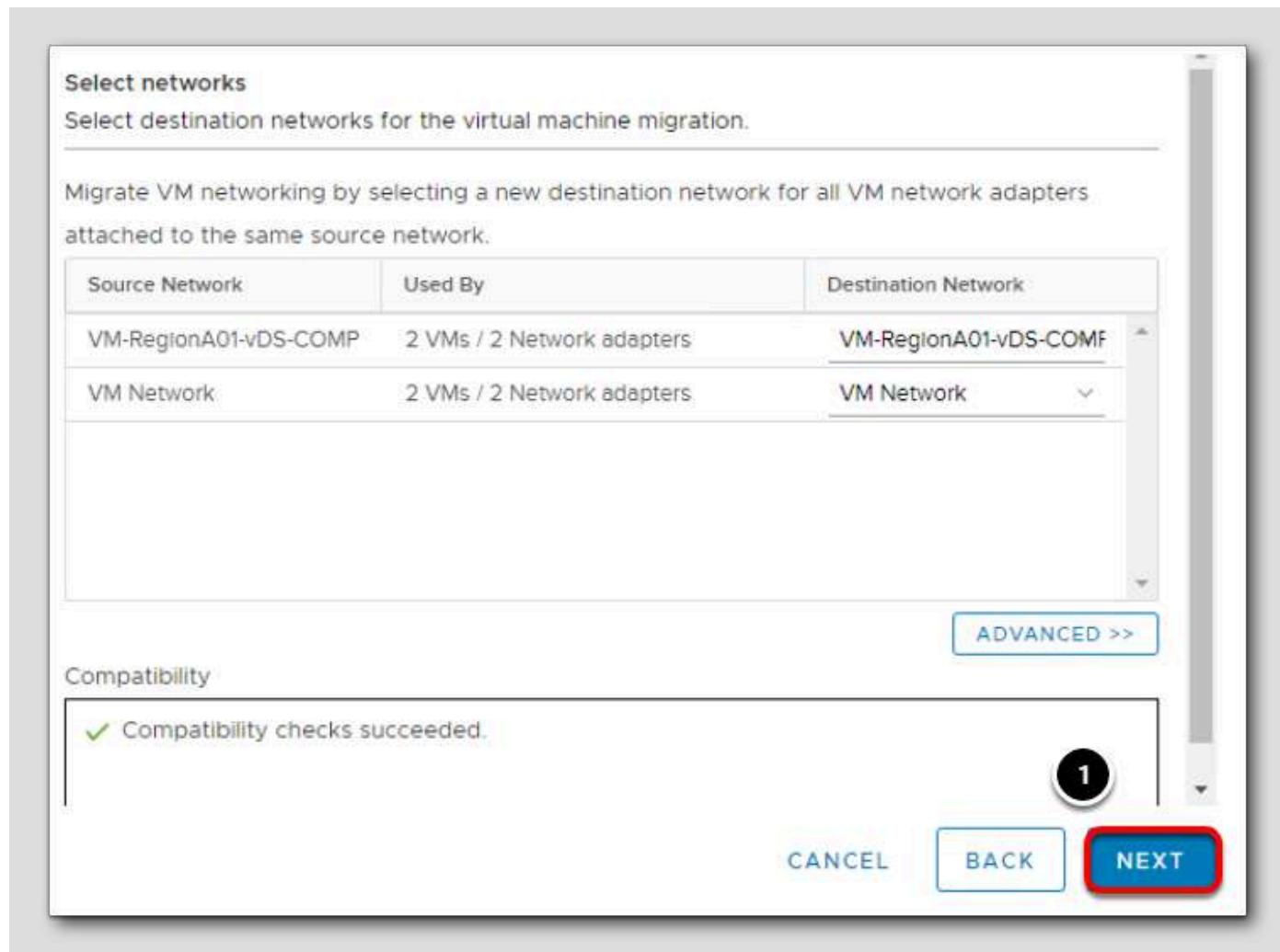
[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

1

CANCEL BACK NEXT



In most cases, the network adapter will not need to be changed.

1. Click **Next**.

vMotion Priority

Select vMotion priority

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

Schedule vMotion with high priority (recommended)

vMotion receives higher CPU scheduling preference relative to normal priority migrations.
vMotion might complete more quickly.

Schedule normal vMotion

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

1 **NEXT**

A priority can be set for the vMotion task. In most cases, the default option is OK.

1. Leave the default setting and click Next.

Ready to Complete

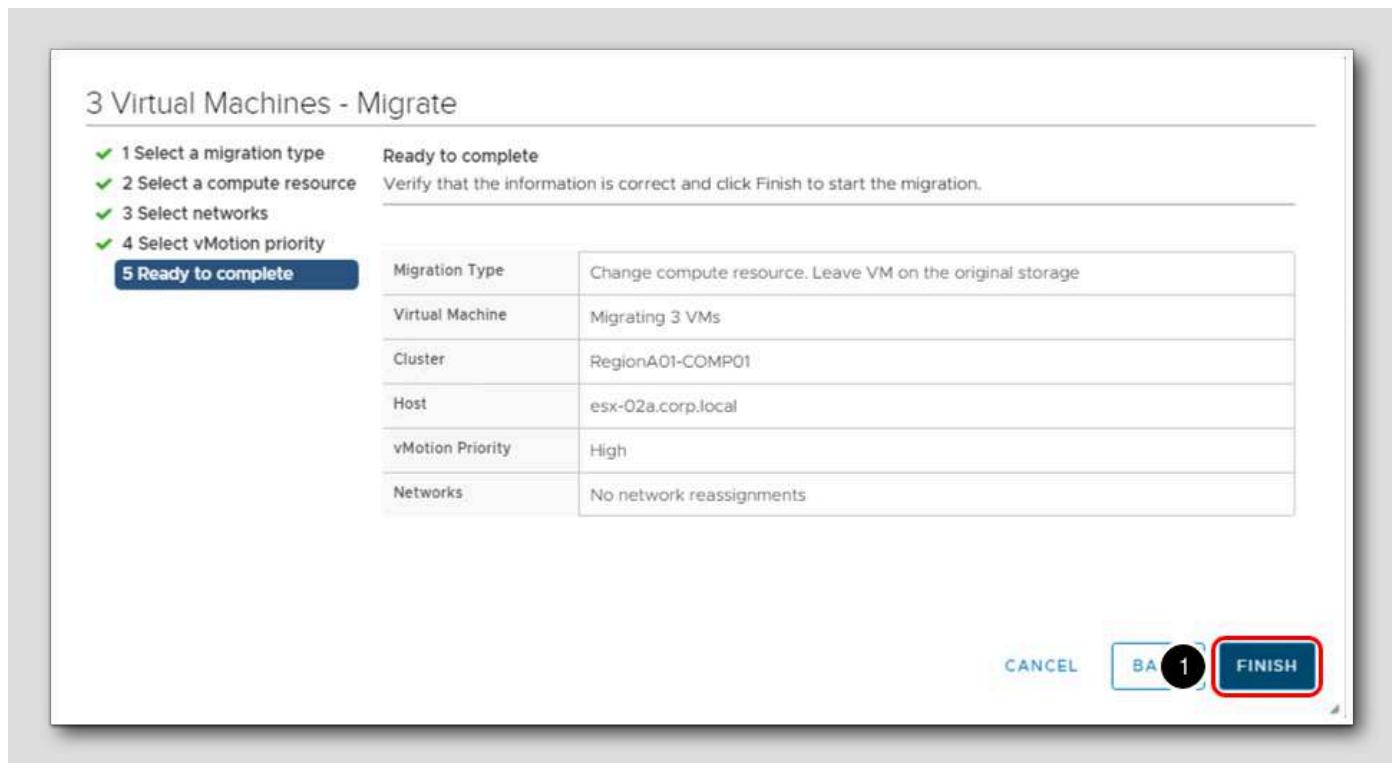
3 Virtual Machines - Migrate

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

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

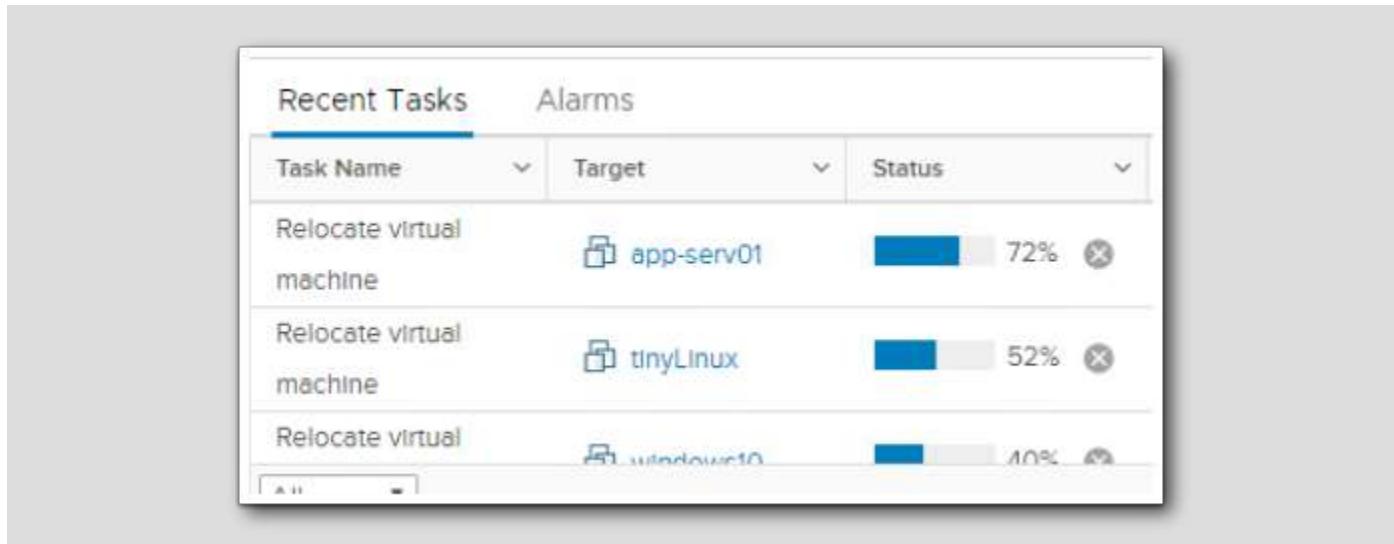
Migration Type	Change compute resource. Leave VM on the original storage
Virtual Machine	Migrating 3 VMs
Cluster	RegionA01-COMP01
Host	esx-02a.corp.local
vMotion Priority	High
Networks	No network reassignments

CANCEL BA 1 FINISH



Review the settings and click Finish to migrate the virtual machines to esx-01a.corp.local.

Monitor Progress



You can monitor progress using Recent Tasks.

Migration Complete

Name	State	Status	Provisioned Space	Used Space
app-serv01	Powered On	Normal	436.19 MB	371.19 MB
TinyLinux	Powered On	Normal	436.83 MB	371.83 MB
TinyLinux2	Powered On	Normal	436.81 MB	371.81 MB
web-serv01	Powered On	Normal	18.08 GB	18.08 GB
Windows10	Powered On	Normal	27.08 GB	20.56 GB

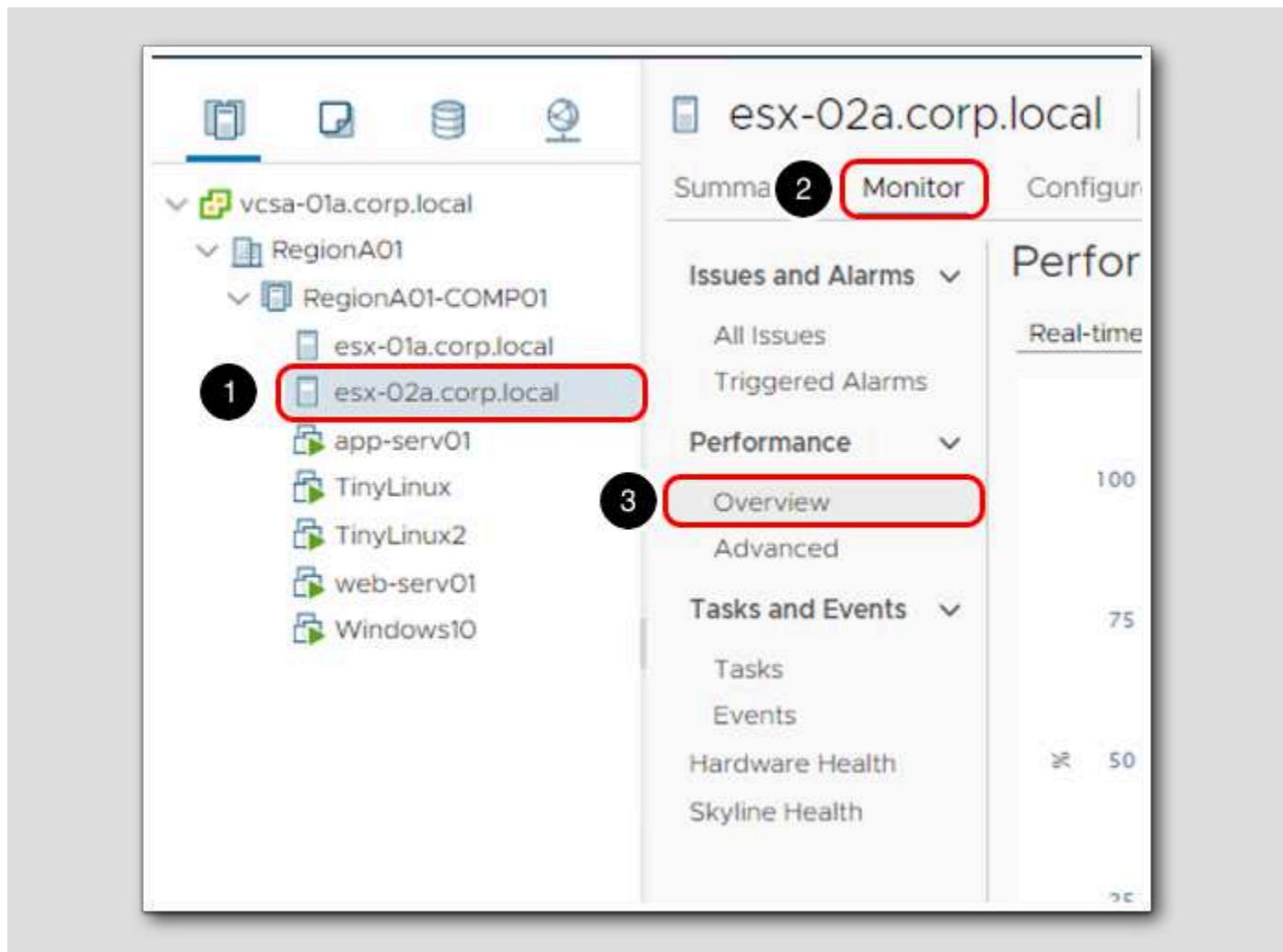
When the task has been completed successfully, you should see all of the virtual machines moved over to esx-02a.corp.local.

vSphere Monitoring and Performance

VMware provides several tools to help you monitor your virtual environment and to locate the source of potential issues and current problems. This lesson will walk through using the performance charts and graphs in the vSphere Client.

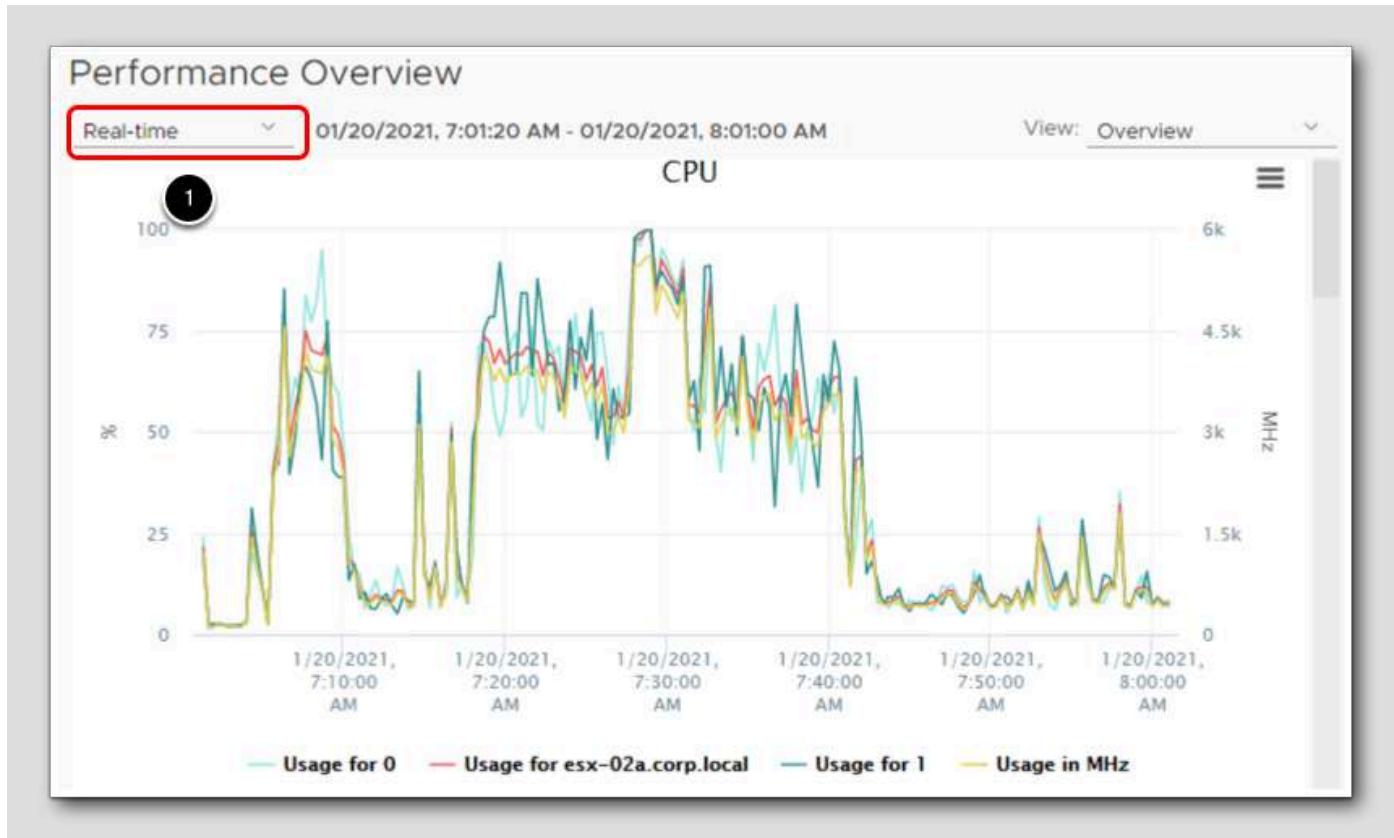
For a more advanced look at monitoring and performance, consider taking one of the vRealize Operations Hands-on Labs. vRealize Operations provides a more dynamic, proactive approach to monitoring your virtual infrastructure.

Select esx-02a



1. Select esx-02a.corp.local
2. Click the Monitor tab
3. Click Overview under the Performance section.

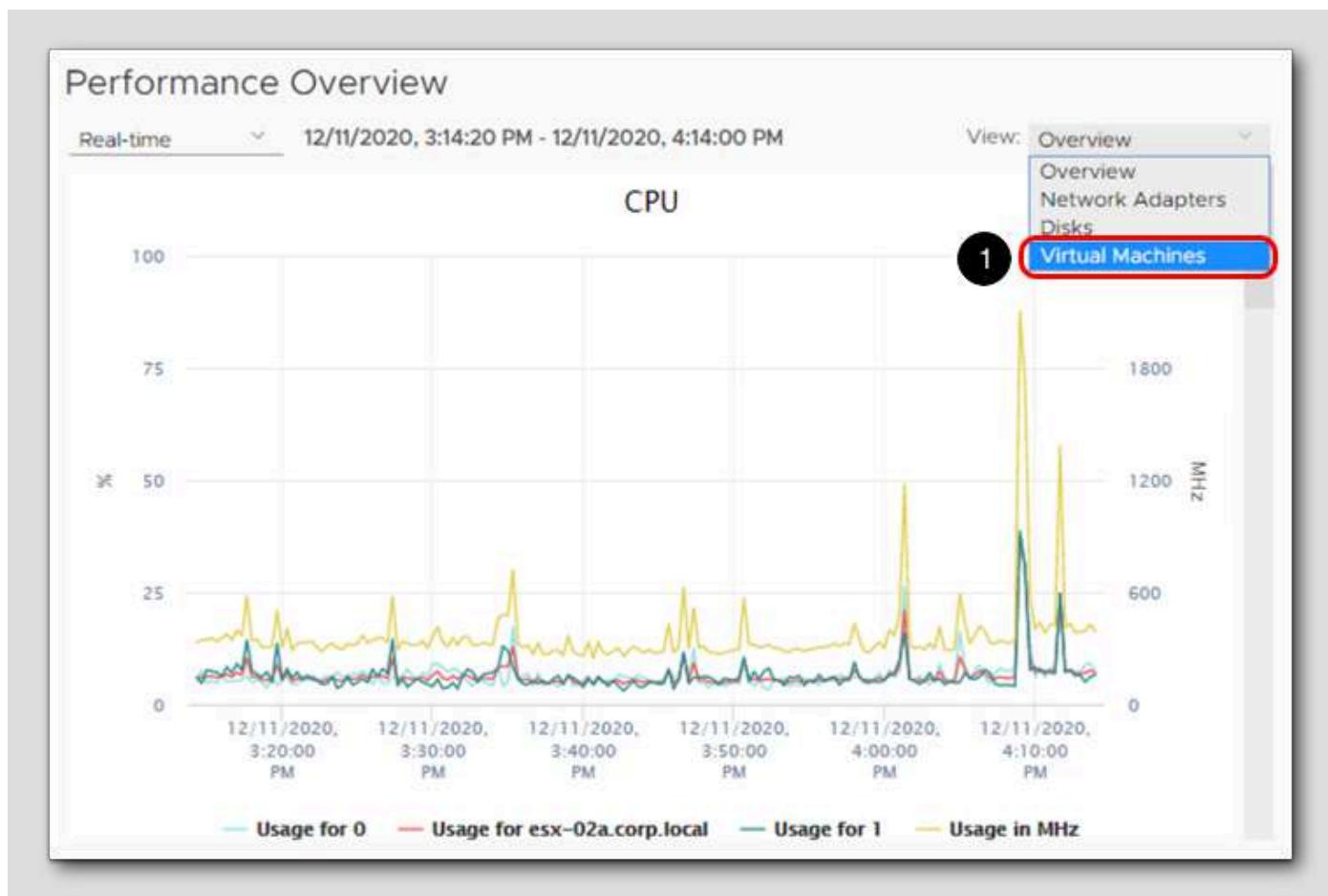
Host CPU Usage



1. Ensure Real-time has been selected from the Time Range drop-down menu.

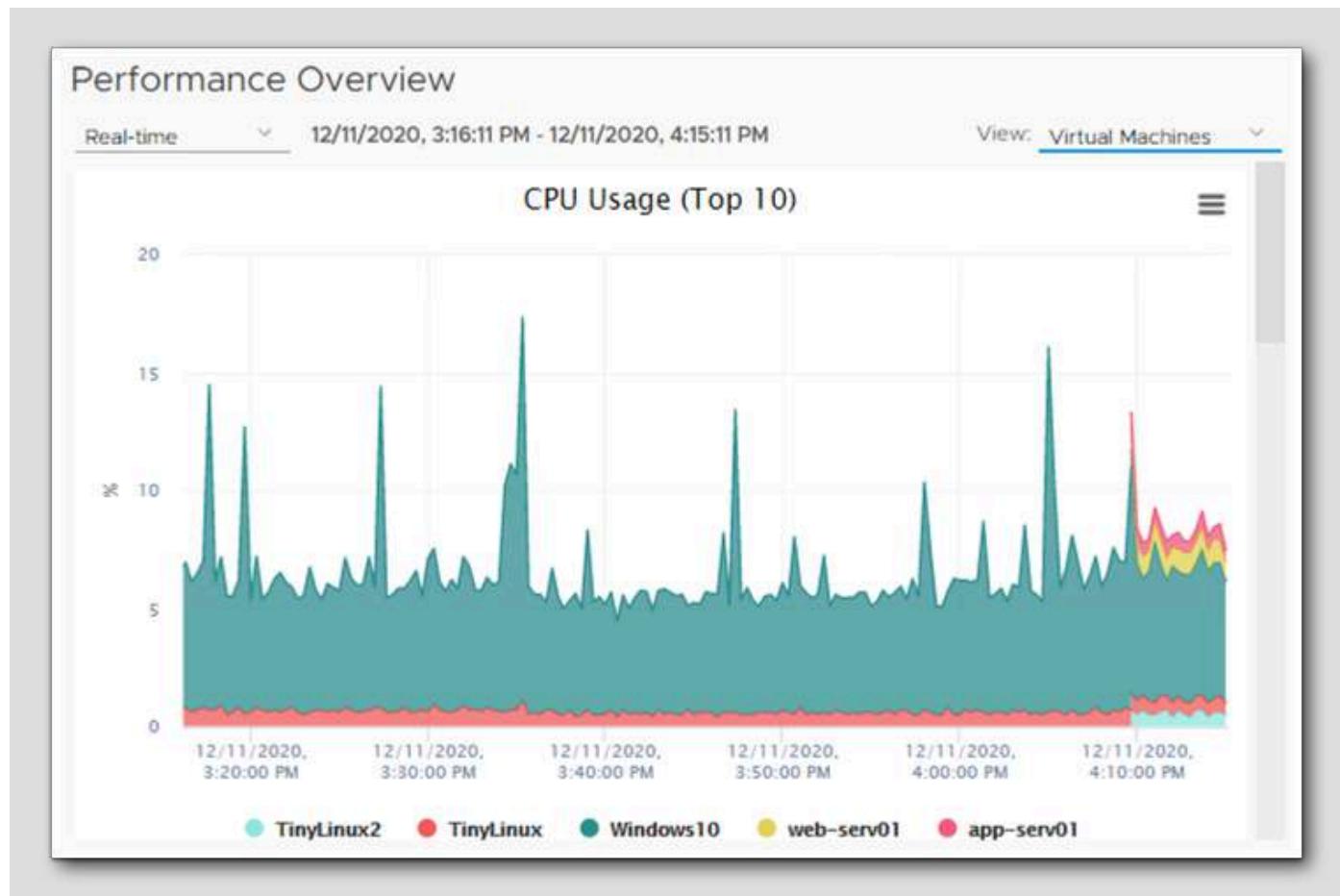
Here we can see in real time the CPU usage in percent for esx-02a.corp.local. By default, the chart will refresh every 20 seconds. The amount of data you see will depend on how long you have been taking the lab.

Virtual Machine CPU Usage



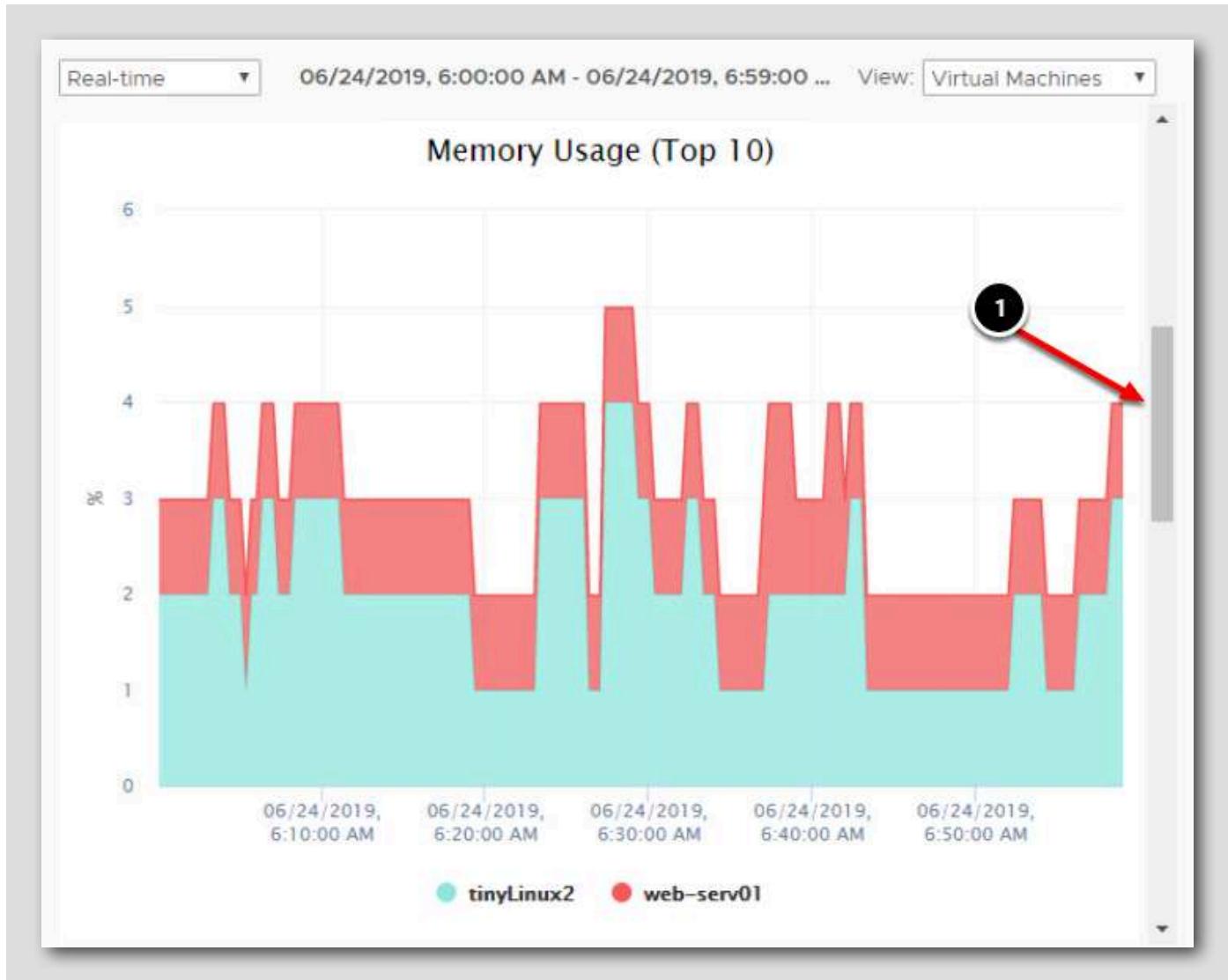
1. Now click the View drop-down box and select Virtual Machines.

Combined CPU Usage



This chart shows the real-time CPU usage of each virtual machine. Each VM is represented by a different color in the graph and you can see at the bottom, which VM is represented by what color. Combined, they give you an idea of overall CPU usage on the host.

Other Available Graphs



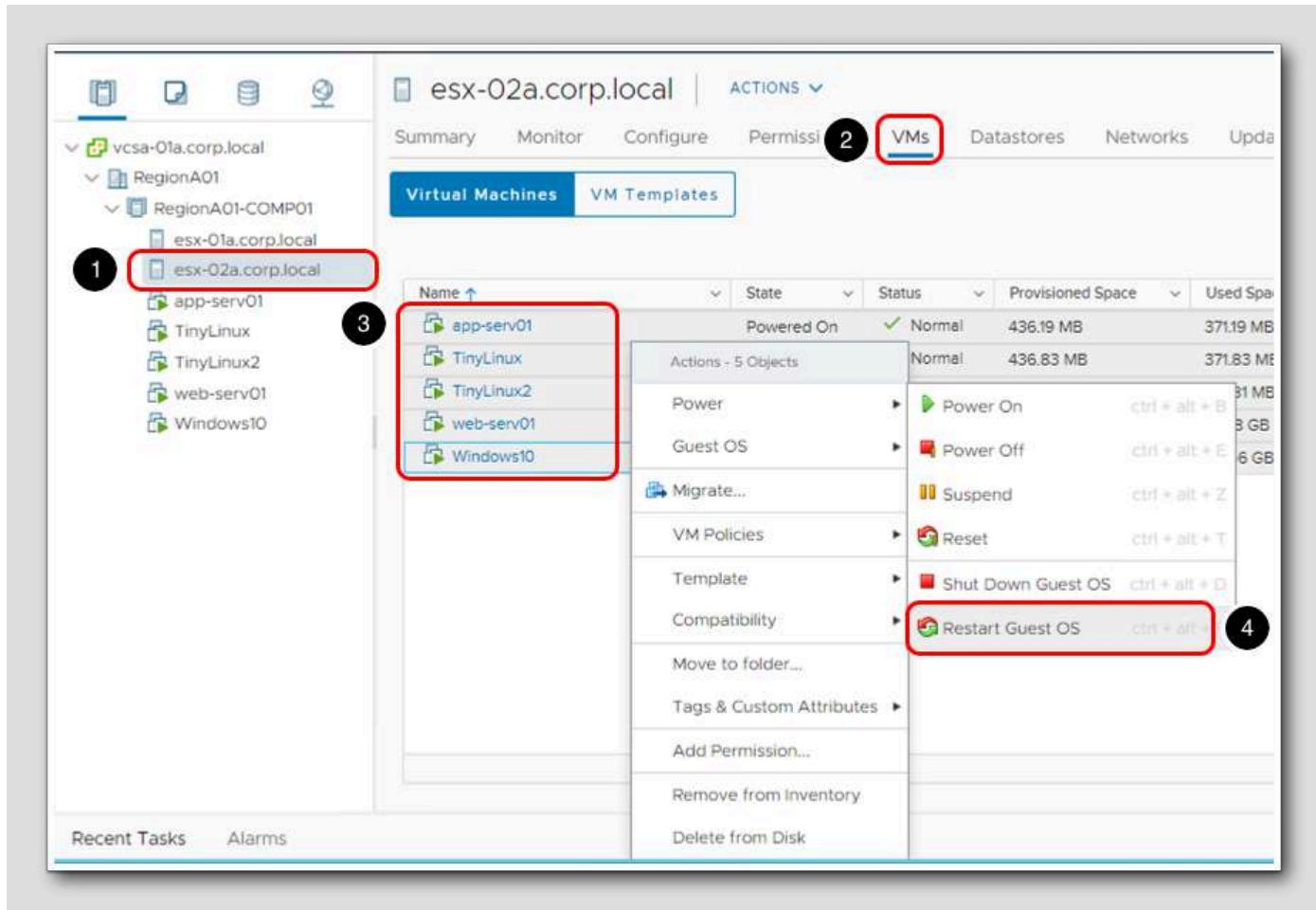
There are other graphs available to show host and virtual machine memory usage, network (Mbps) and disk (KBps).

1. Use the scroll bars to access the additional charts.

The graphs we have looked at so far will give you an overview of the four main components, CPU, memory, disk and storage. The advanced graphs will give you more detailed information on each of these.

Before we look at these charts, let's generate some CPU activity on esx-01a.corp.local by restarting all of the virtual machines it hosts.

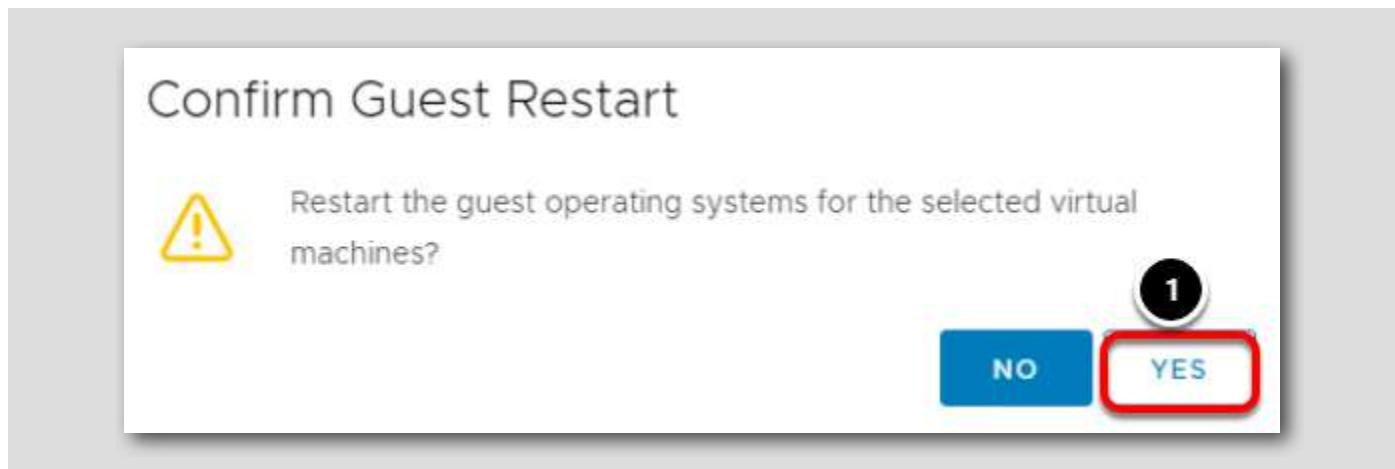
Select the VMs to be Restarted



To generate some activity on esx-02a.corp.local, the virtual machines will be rebooted.

1. Select esx-02a.corp.local
2. Click on the VMs tab
3. Click on the first VM that is listed, hold down the Shift key and select the last VM on the list
4. Select Power and click the Restart Guest OS button

Confirm Restart



1. Click Yes to continue.

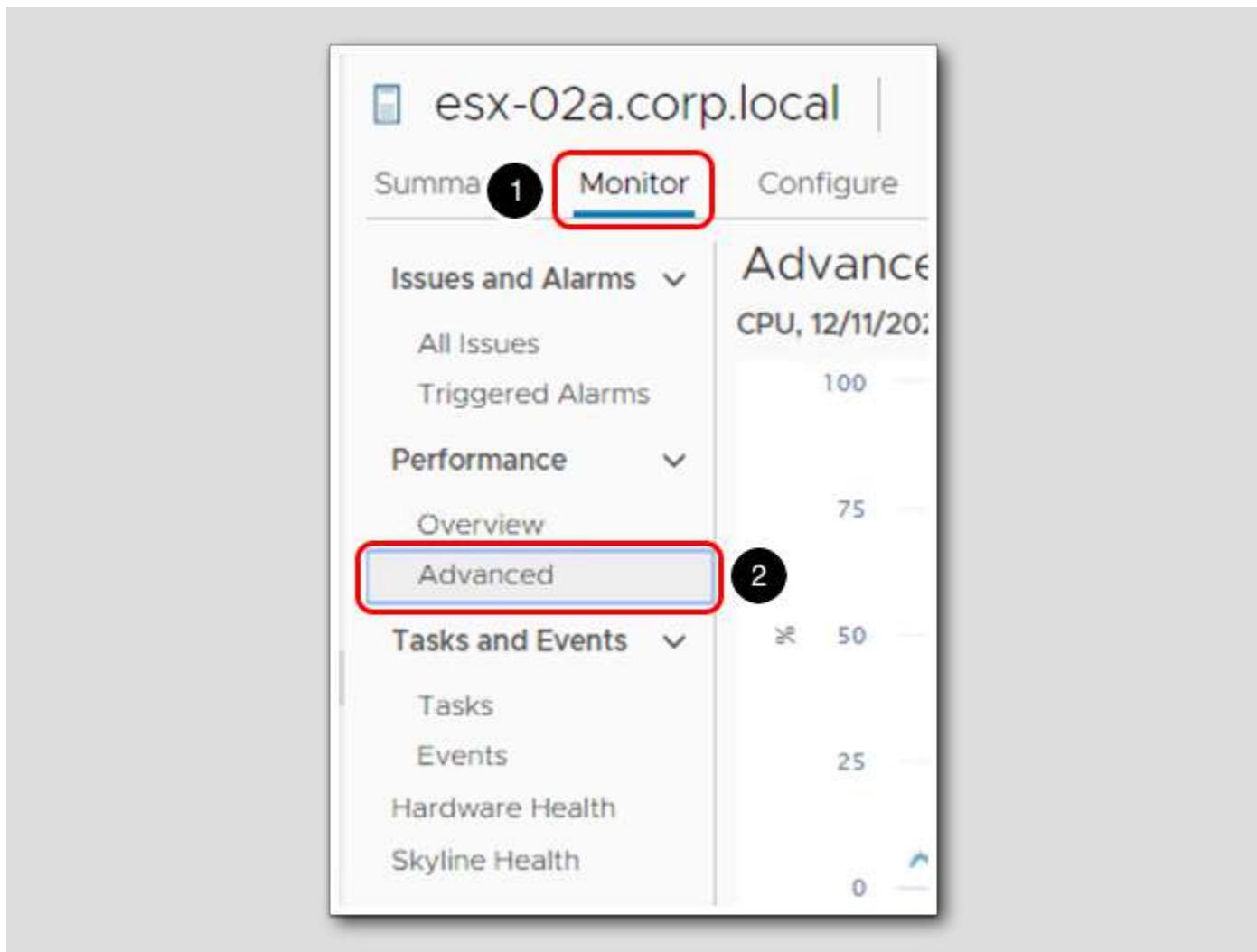
Note: You may also receive a warning that only X of X virtual machines will be restarted. This depend on what other modules and/or lessons have been completed in the lab previously.

Manually Start VMs

The screenshot shows the vSphere Web Client interface for the host `esx-02a.corp.local`. The `VMs` tab is selected. In the main list, three virtual machines are listed as `Powered Off`: `app-serv01`, `TinyLinux`, and `TinyLinux2`. A red box highlights these three entries. A context menu is open over these three VMs, with the `Power On` option highlighted by another red box. Other options in the menu include `Power Off`, `Suspend`, `Reset`, `Shut Down Guest OS`, and `Restart Guest OS`.

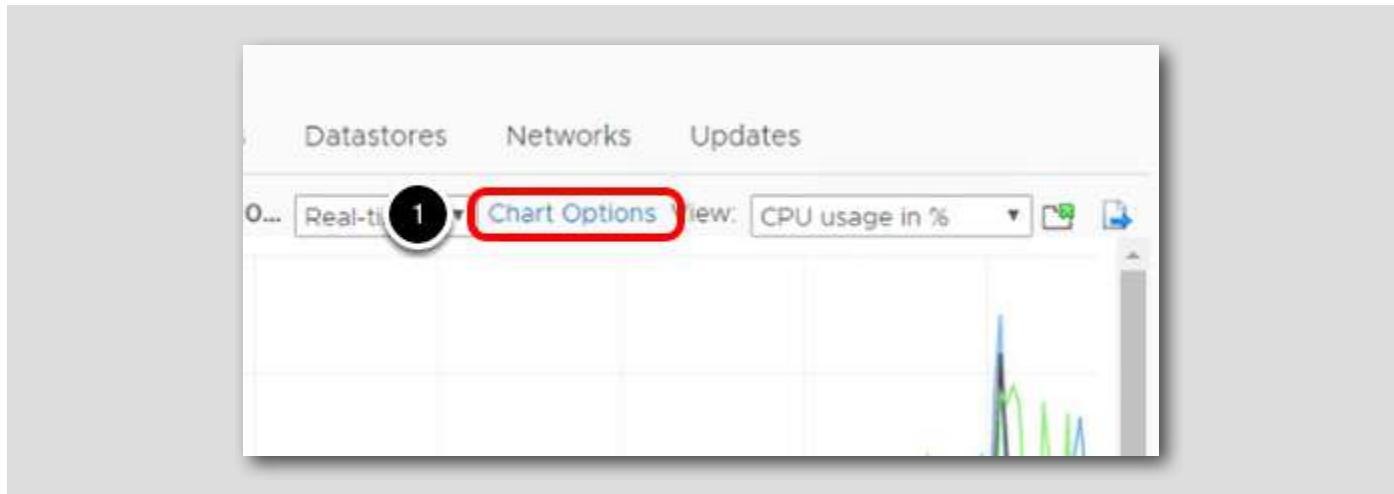
1. If `TinyLinux`, `TinyLinux2`, or `app-serv01` did not restart, but instead shut down.
2. Select all and power them on manually.

Monitor Performance



1. Click on the Monitor tab.
2. Click Advanced in the Performance section.

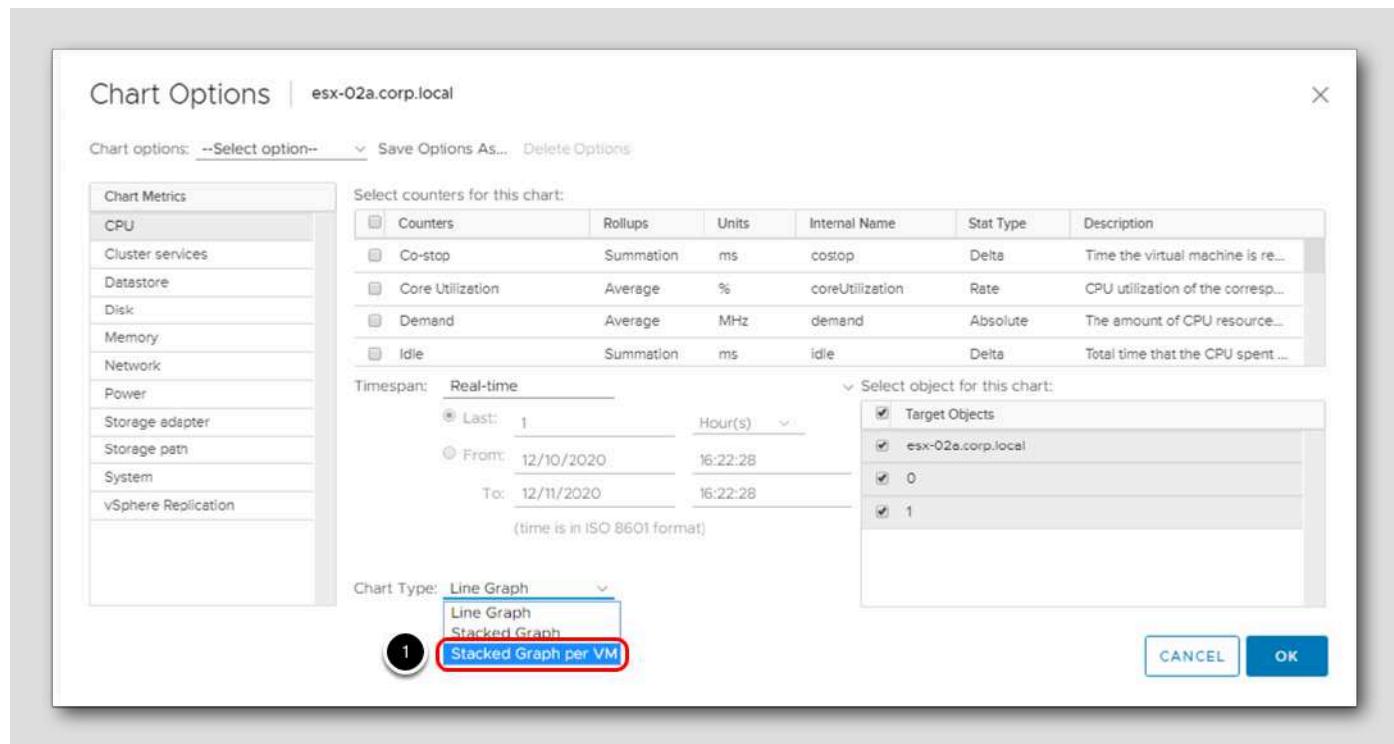
Chart Options



1. Click the Chart Options link.

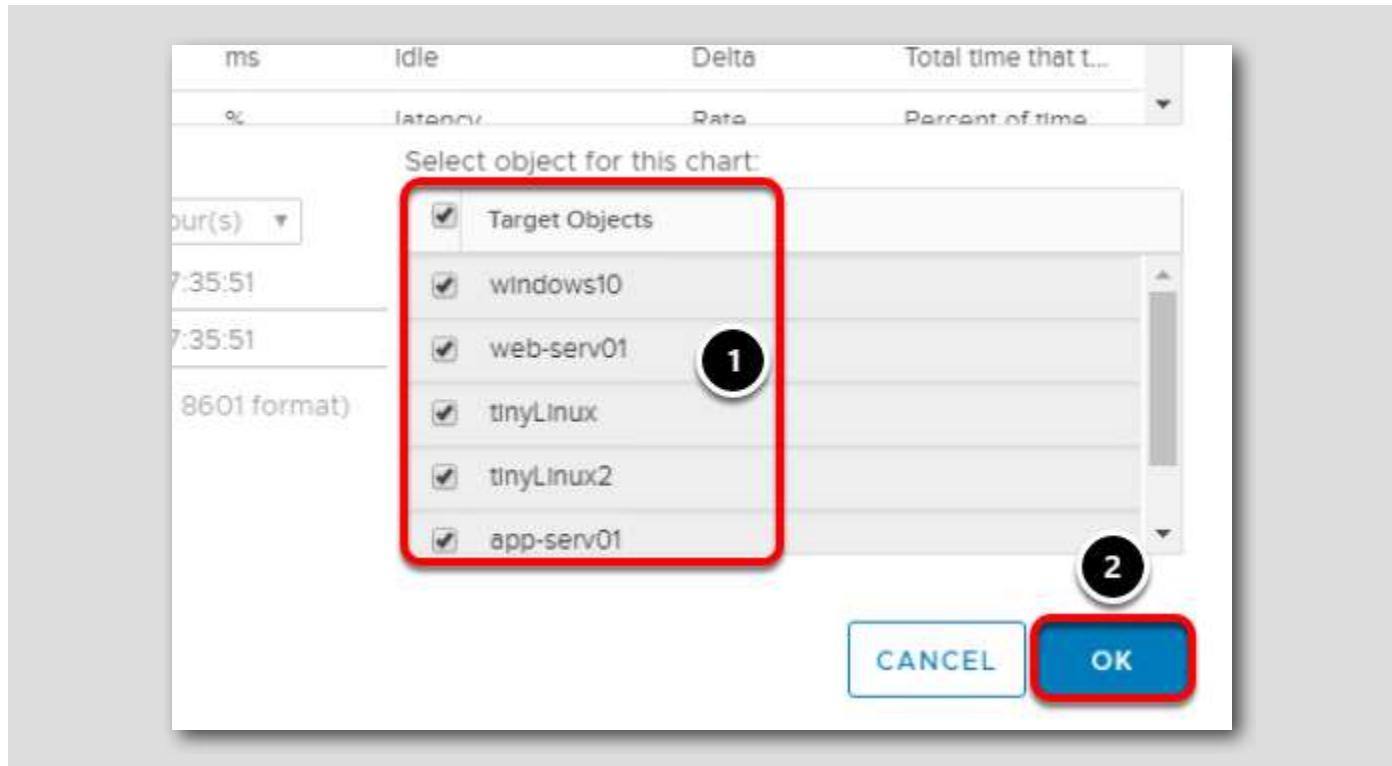
This will bring up options to customize the chart.

Stacked Graph per VM



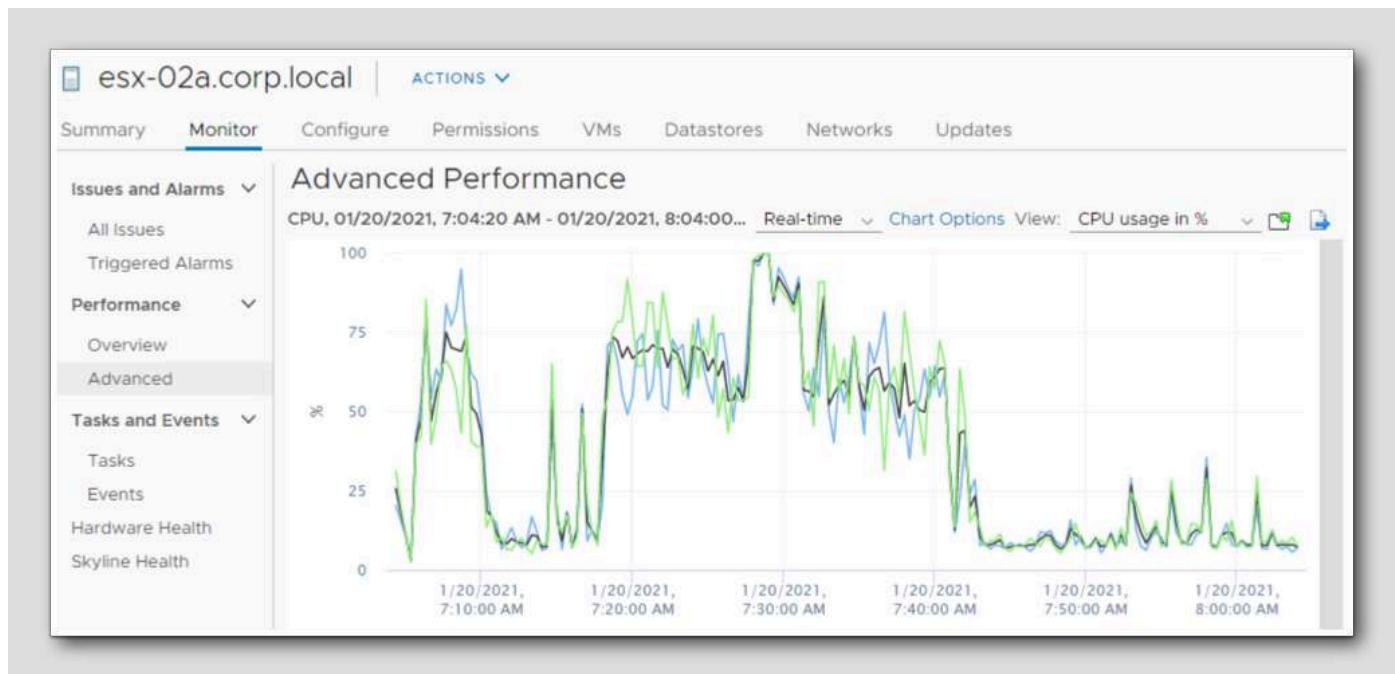
1. From the Chart Type drop-down menu, select Stacked Graph per VM.

Select Objects



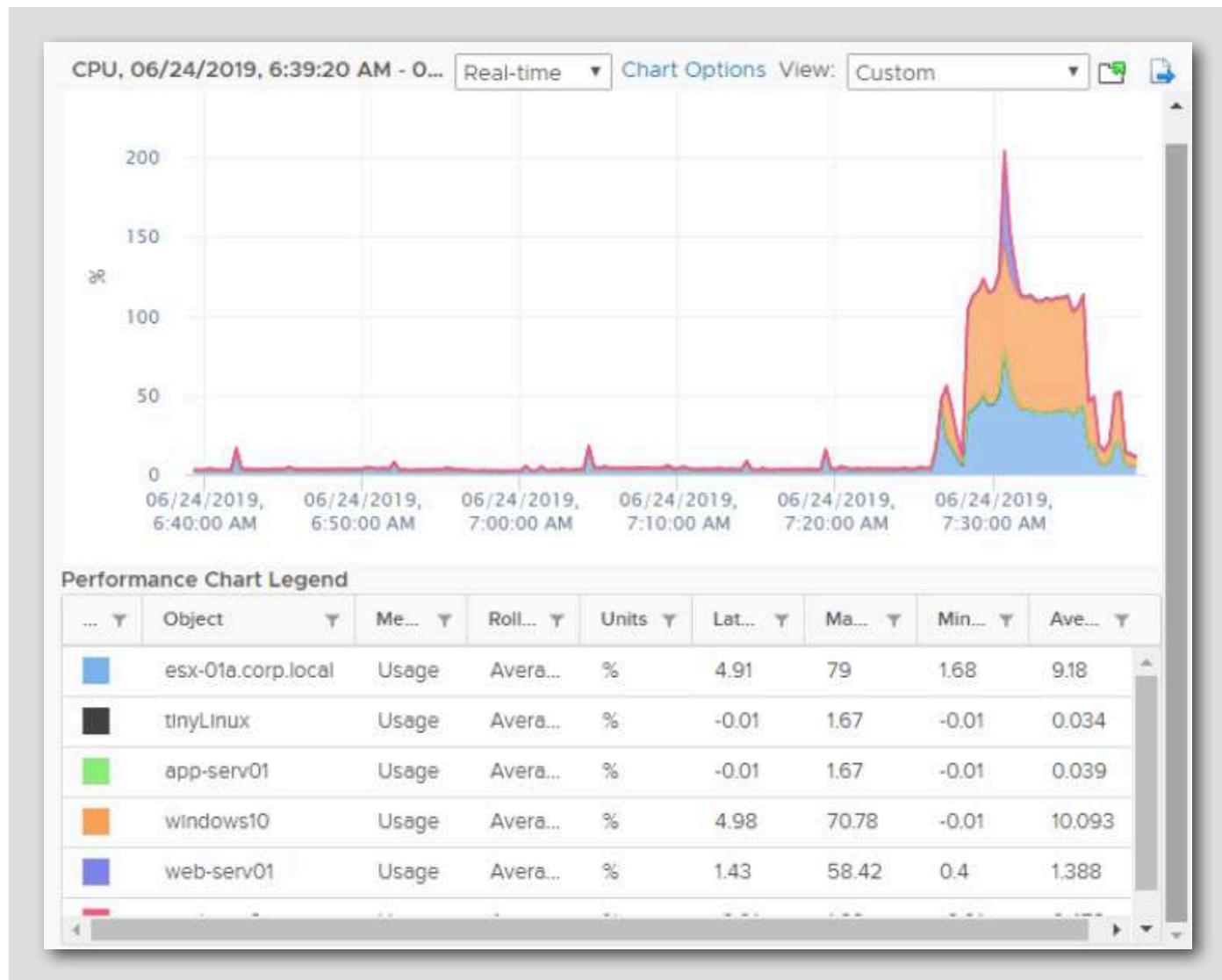
1. Under the Select objects for this chart box, verify all the virtual machines are selected.
2. Click the OK button to see the newly customized chart.

CPU Usage in Real-time



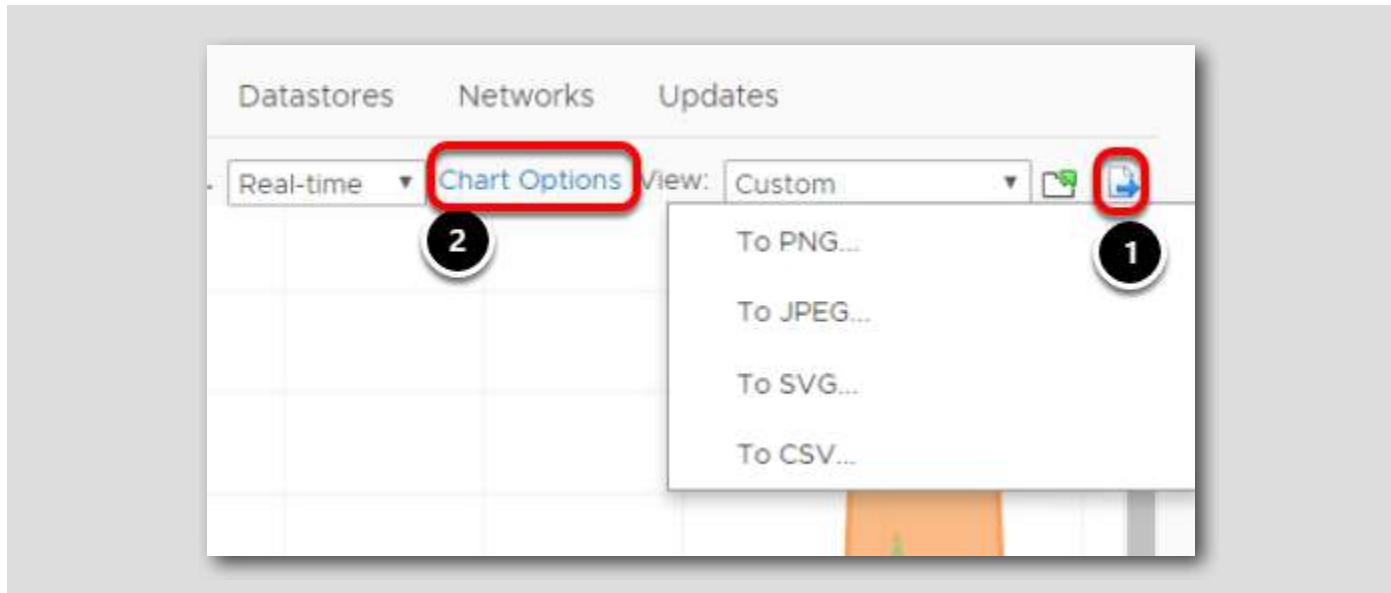
Here we can see the CPU usage of each virtual machine and esx-02a.corp.local.

Performance Chart Legend



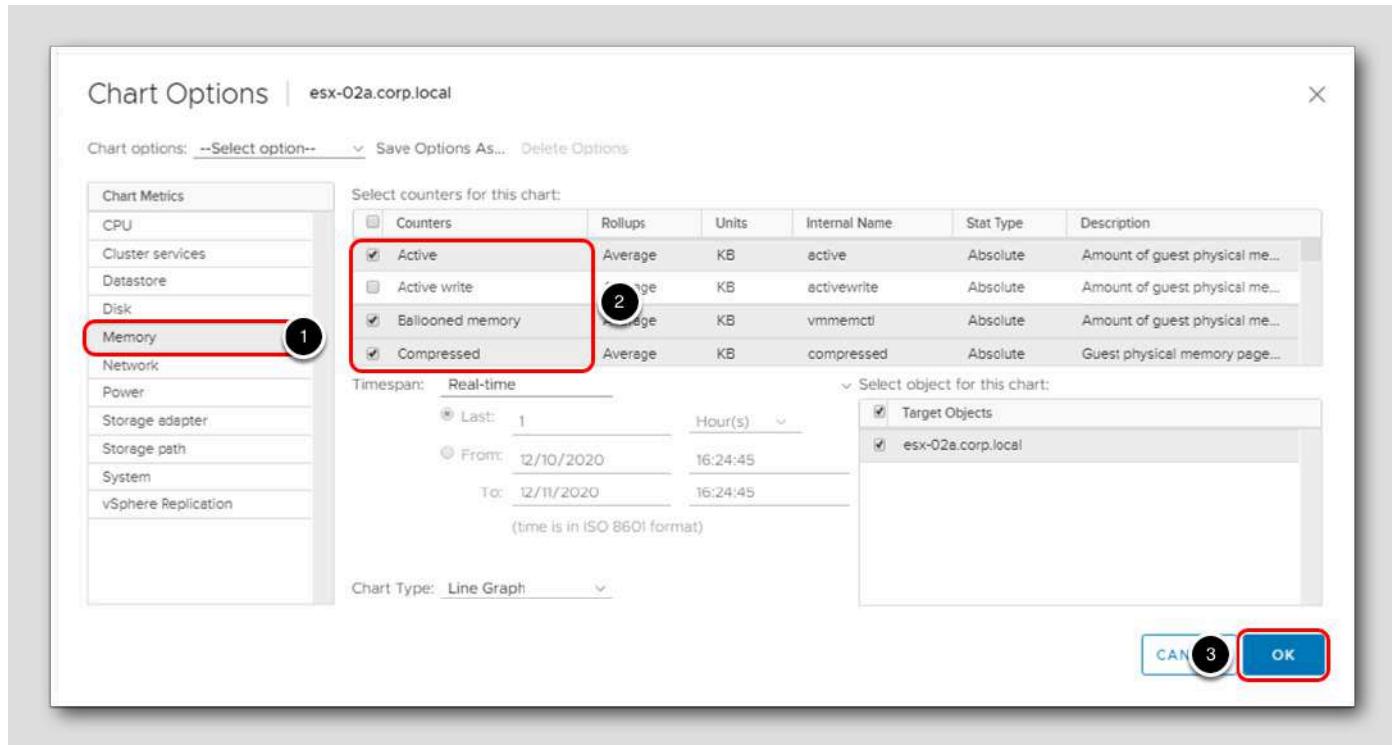
Scroll down and you will see the Performance Chart Legend. You can click on any of the virtual machines or esx-01a.corp.local to highlight it on the chart.

Exporting a Chart Image



1. You can export the chart in multiple formats, either as a graphic or CSV file by clicking the Export button.
2. Click the Chart Options link

Chart Metrics

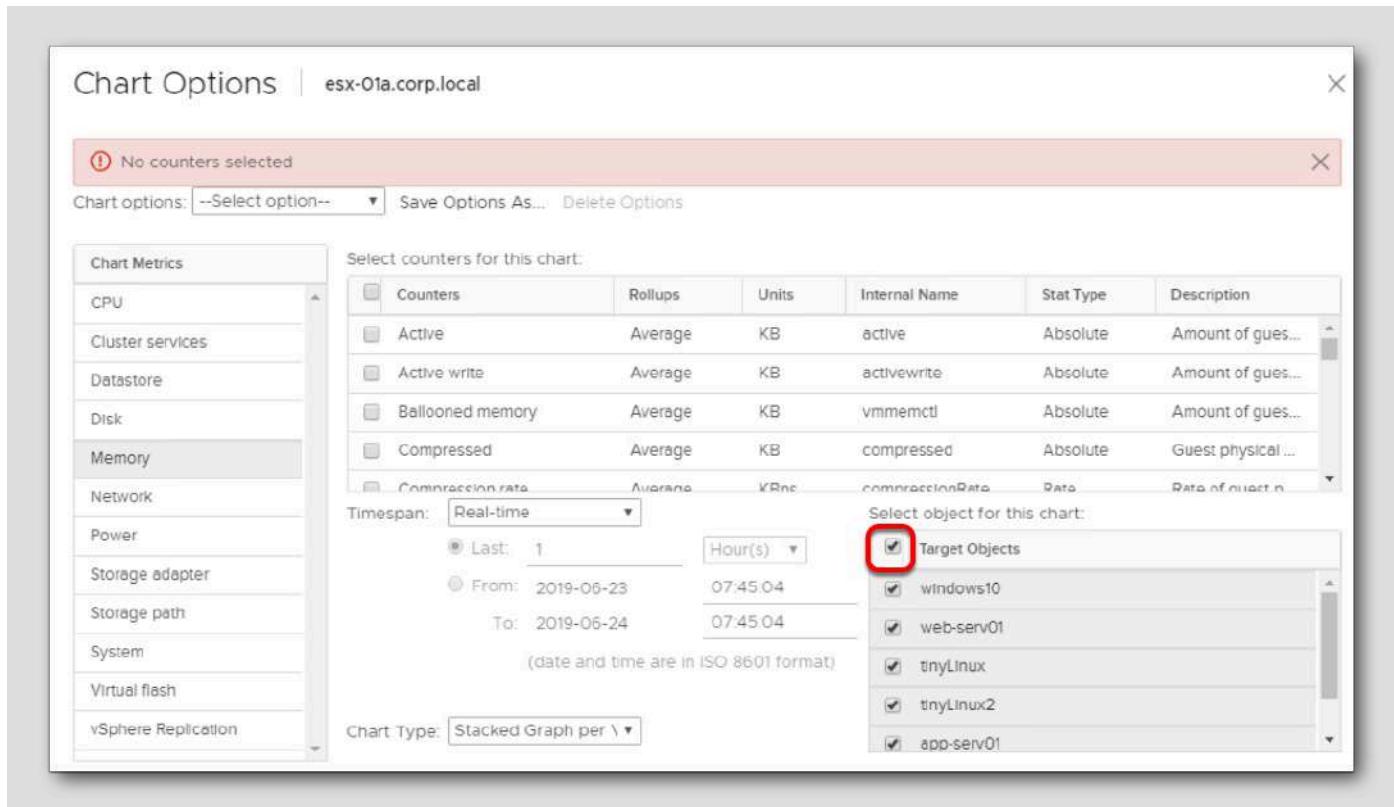


On the left-hand side, you will see a list of all the available chart metrics that can be viewed. The counters will update based on what metric you select.

1. Select **Memory** under Chart metrics.
2. Select **Active**, **Ballooned memory**, and **Compressed** for Counters to add.

Notice the counters section updates and now we have additional counters to view for this chart.

3. Click **OK**.



Note: If you receive an error that No Counter were selected, uncheck and check Target Objects, then click OK.

Memory Real-time



This chart shows the memory counters relative to memory for esx-02a.corp.local. Scroll down the Performance Chart Legend to see the counter each line represents.

Feel free to explore the various chart options and/or continue to the next step.

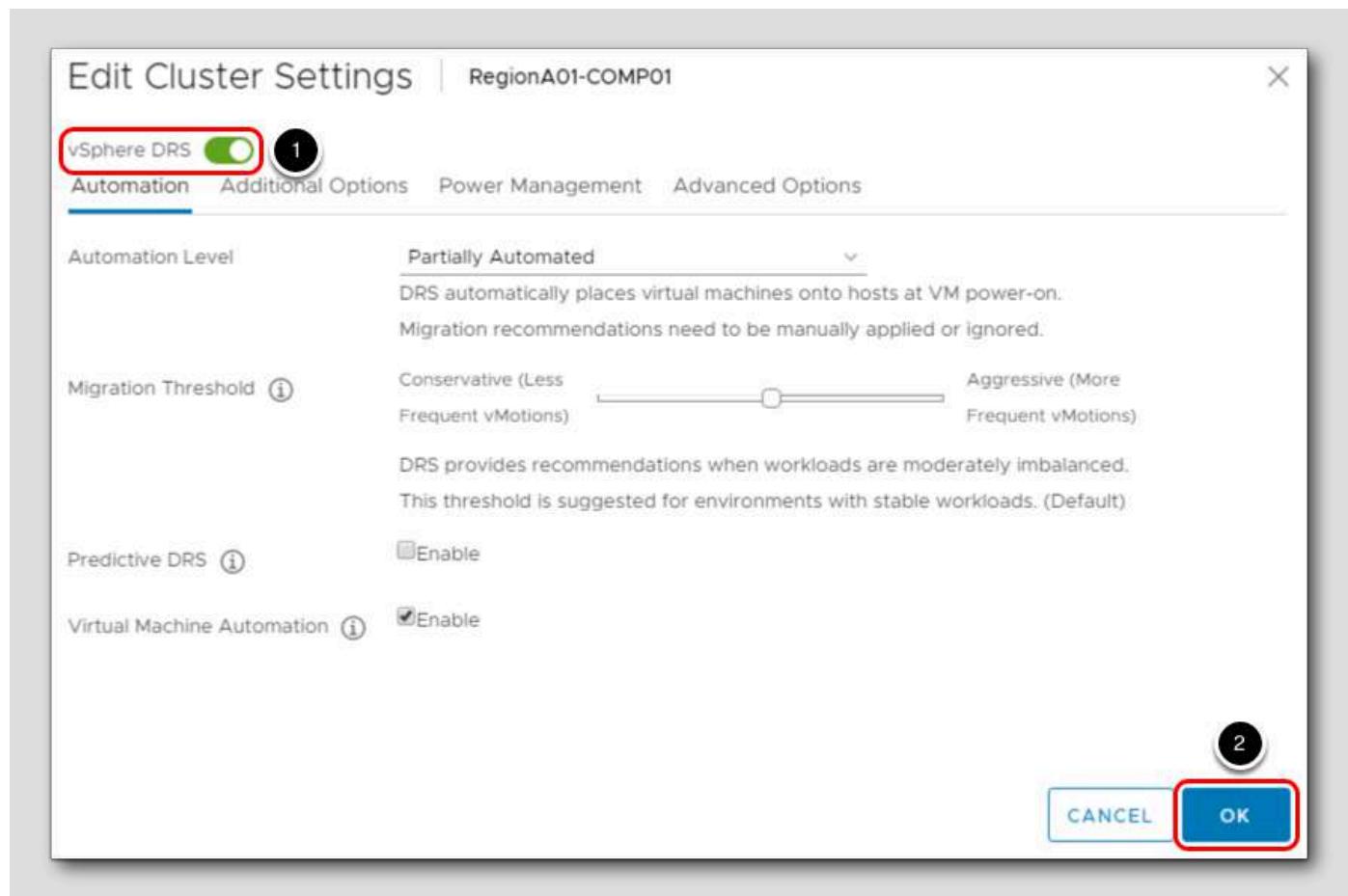
Enable DRS

Once you have finished viewing the charts, DRS needs to be enabled again.

1. Select RegionA01-COMP01.
2. Click the Configure tab.
3. Click on vSphere DRS.
4. Click the Edit button.

Turn ON vSphere DRS

[202]



1. Check the Turn ON vSphere DRS box to enable DRS.
2. Click OK.

Further Information

For more information on performance charts, you can view the [vSphere Monitoring and Performance](#) guide.

Introduction to vSphere with Tanzu

vSphere 7 is the biggest release of vSphere in over a decade and delivers these innovations and the rearchitecting of vSphere with native Kubernetes that we introduced at VMworld 2019 as Project Pacific.

Common Platform for Running both Kubernetes/Containerized Workloads and VMs

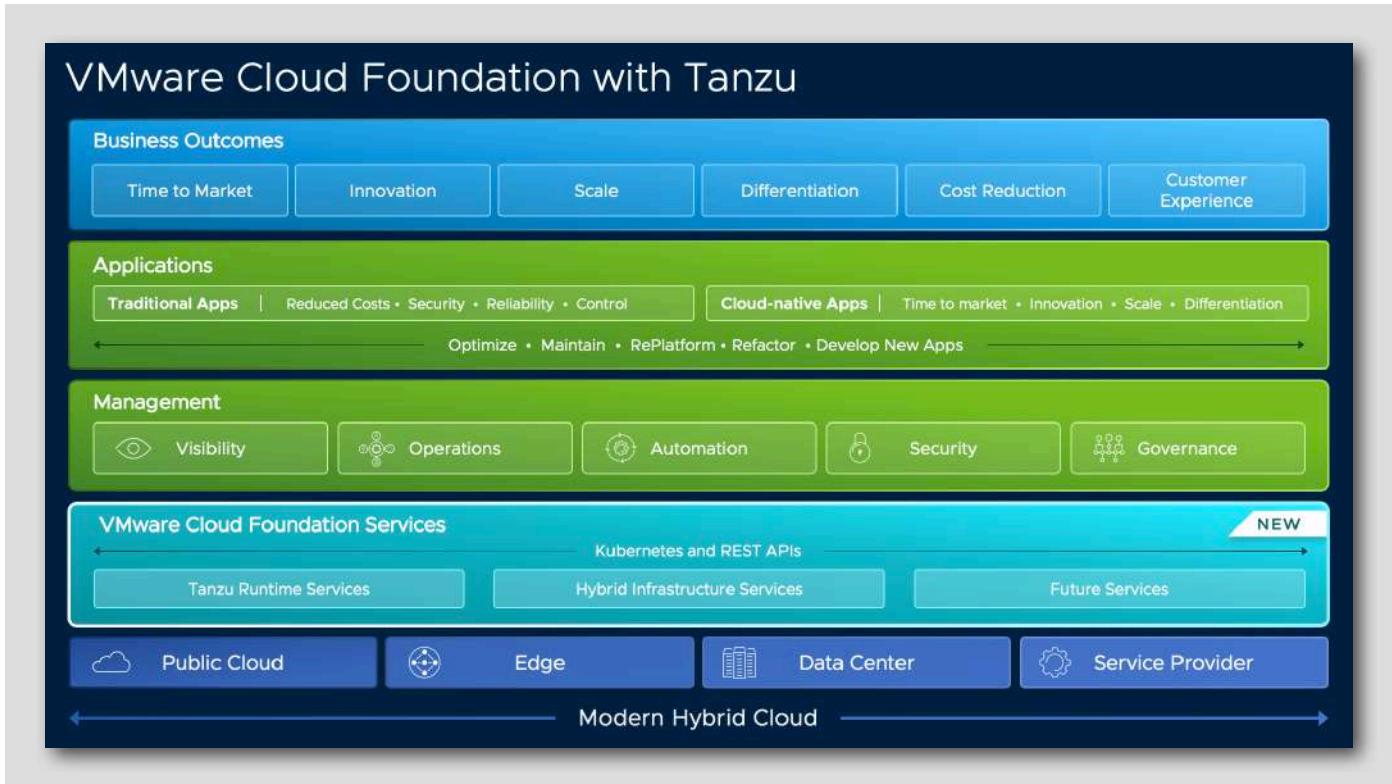
Kubernetes is now built into vSphere which allows developers to continue using the same industry-standard tools and interfaces they've been using to create modern applications. vSphere Admins also benefit because they can help manage the Kubernetes infrastructure using the same tools and skills they have developed around vSphere. To help bridge these two worlds we've introduced a new vSphere construct called Namespaces, allowing vSphere Admins to create a logical set of resources, permissions, and policies that enable an application-centric approach.

Agile Operations for Kubernetes Applications

We are introducing a lot of value in vSphere with Tanzu for the VI admin. We deliver a new way to manage infrastructure, called ‘application-focused management’ for containerized applications. This enables admins to apply policies to an entire group of objects and organize multiple objects into a logical group and then apply policies to the entire group. For example, an administrator can apply security policies and storage limits to a group of containers and Kubernetes clusters that represent an application, rather than to each of the objects individually. This helps improve productivity and reduce errors that can be costly to identify and correct.

VMware Cloud Foundation Services

vSphere with Tanzu is available through VMware Cloud Foundation 4 with Tanzu. One key innovation available only in VMware Cloud Foundation is a set of developer-facing services and a Kubernetes API surface that IT can provision, called VMware Cloud Foundation Services.



It consists of two families of services: Tanzu Runtime Services and Hybrid Infrastructure Services.

- **Tanzu Runtime Services** – deliver core Kubernetes development services, including an up-to-date distribution of:
 - **Tanzu Kubernetes Grid Service** – which allows developers to manage consistent, compliant, and conformant Kubernetes clusters to build their modern applications.
- **Hybrid Infrastructure Services** – include full Kubernetes and REST API access that spans creating and manipulating virtual machines, containers, storage, networking, and other core capabilities. It includes the following services today:
 - *vSphere Pod Service* – extends Kubernetes with the ability to run pods directly on the hypervisor. When developers deploy containers using the vSphere Pod Service, they get the same level of security isolation, performance guarantees, and management capabilities that VMs enjoy.
 - *Storage service* – allows developers to manage persistent disks for use with containers, Kubernetes, and virtual machines.
 - *Network service* – allows developers to manage Virtual Routers, Load Balancers, and Firewall Rules.
 - *Registry service* – allows developers to store, manage, and better secure Docker and OCI images using Harbor.

Conclusion

VMware vSphere 7 is the efficient and secure platform for the hybrid cloud. It provides a powerful, flexible, and secure foundation for business agility that accelerates the digital transformation to the hybrid cloud as well as success in the digital economy.

Here are the other vSphere labs to take to get familiar with the lastest vSphere 7 release:

- HOL-2111-01-SDC - VMware vSphere - What's New
- HOL-2113-01-SDC - vSphere with Tanzu

ESXi Install and Configure

Due to the environment the Hands on Labs are running in and the high I/O it would cause, we are not able to install software. Please use the following videos to walk through the process.

Video: Installing and Configuring vSphere (4:36)

The following video will walk through the process of installing and configuring vSphere.

<https://www.youtube.com/watch?v=naK5opxyKWA>



Video: Overview of the DCUI (4:58)

This video will walk you through the Direct Console User Interface (DCUI).

<https://www.youtube.com/watch?v=CPsX3Sx7XpI>



Certification Path

Learn and Practice with Hands-On Labs to help prepare for several VMware Certifications.

vmware[®]

CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

This Lab can help you study for the industry-recognized VCAP-DCV Deploy 2021 Deploy certification which validates that you know how to deploy and optimize VMware vSphere infrastructures.

Learn More Here https://via.vmw.com/dcv_deploy

vmware[®]
CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

Module 2 - Introduction to vSphere Networking and Security (60 Min)...

Introduction

[214]

The ability to connect virtual machines through a logical switch that is part of the vSphere hypervisor is a necessity for operating systems and applications to communicate on the physical network. Traditionally this was done through a Standard vSwitch, configured individually at each ESXi host in the datacenter.

Since its introduction, the vSphere Distributed Switch quickly became the recommended type of virtual switch to use for most if not all types of network traffic in and out of the ESXi host. This is due mostly in part to its ability to be created and managed centrally through vCenter, as well as the advanced networking features it provides.

Let's spend some time reviewing the similarities and differences between the two types of switches.

Types of virtual switches

[215]

There are two types of virtual switches in ESXi/ESX 4.x, ESXi 5.x, and ESXi 6.x, vNetwork Standard Switch and vNetwork Distributed Switch (vDS).

vNetwork Standard Switch (vSwitch, vSS)

[216]

As in VMware Infrastructure 3, the configuration of each vSwitch resides on the specific ESXi/ESX host. The VI administrators have to manually maintain consistency of the vSwitch configuration across all ESXi/ESX hosts to ensure that they can perform operations such as vMotion.

vSwitches are configured on each ESXi/ESX host.

vNetwork Distributed Switch (dvSwitch, vDS)

[217]

The configuration of vDS is centralized to vCenter Server. The ESXi/ESX 4.x, ESXi 5.x, and ESXi 6.x hosts that belong to a dvSwitch do not need further configuration to be compliant.

Distributed switches provide similar functionality to vSwitches. dvPortgroups is a set of dvPorts. The vDS equivalent of portgroups is a set of ports in a vSwitch. Configuration is inherited from dvSwitch to dvPortgroup, just as from vSwitch to Portgroup.

Virtual machines, Service Console interfaces (vswif), and VMKernel interfaces can be connected to dvPortgroups just as they could be connected to portgroups in vSwitches.

Comparing vNetwork Standard Switch with vNetwork Distributed Switch

These features are available with both types of virtual switches:

- Can forward L2 frames
- Can segment traffic into VLANs
- Can use and understand 802.1q VLAN encapsulation
- Can have more than one uplink (NIC Teaming)
- Can have traffic shaping for the outbound (TX) traffic

These features are available only with a Distributed Switch:

- Can shape inbound (RX) traffic
- Has a central unified management interface through vCenter Server
- Supports Private VLANs (PVLANS)
- Provides potential customization of Data and Control Planes

vSphere 5.x provides these improvements to Distributed Switch functionality:

- Increased visibility of inter-virtual machine traffic through Netflow.
- Improved monitoring through port mirroring (dvMirror).
- Support for LLDP (Link Layer Discovery Protocol), a vendor-neutral protocol.
- The enhanced link aggregation feature provides choice in hashing algorithms and also increases the limit on number of link aggregation groups.
- Additional port security is enabled through traffic filtering support.
- Improved single-root I/O virtualization (SR-IOV) support and 40GB NIC support.

vSphere 6.x provides these improvements to Distributed Switch functionality:

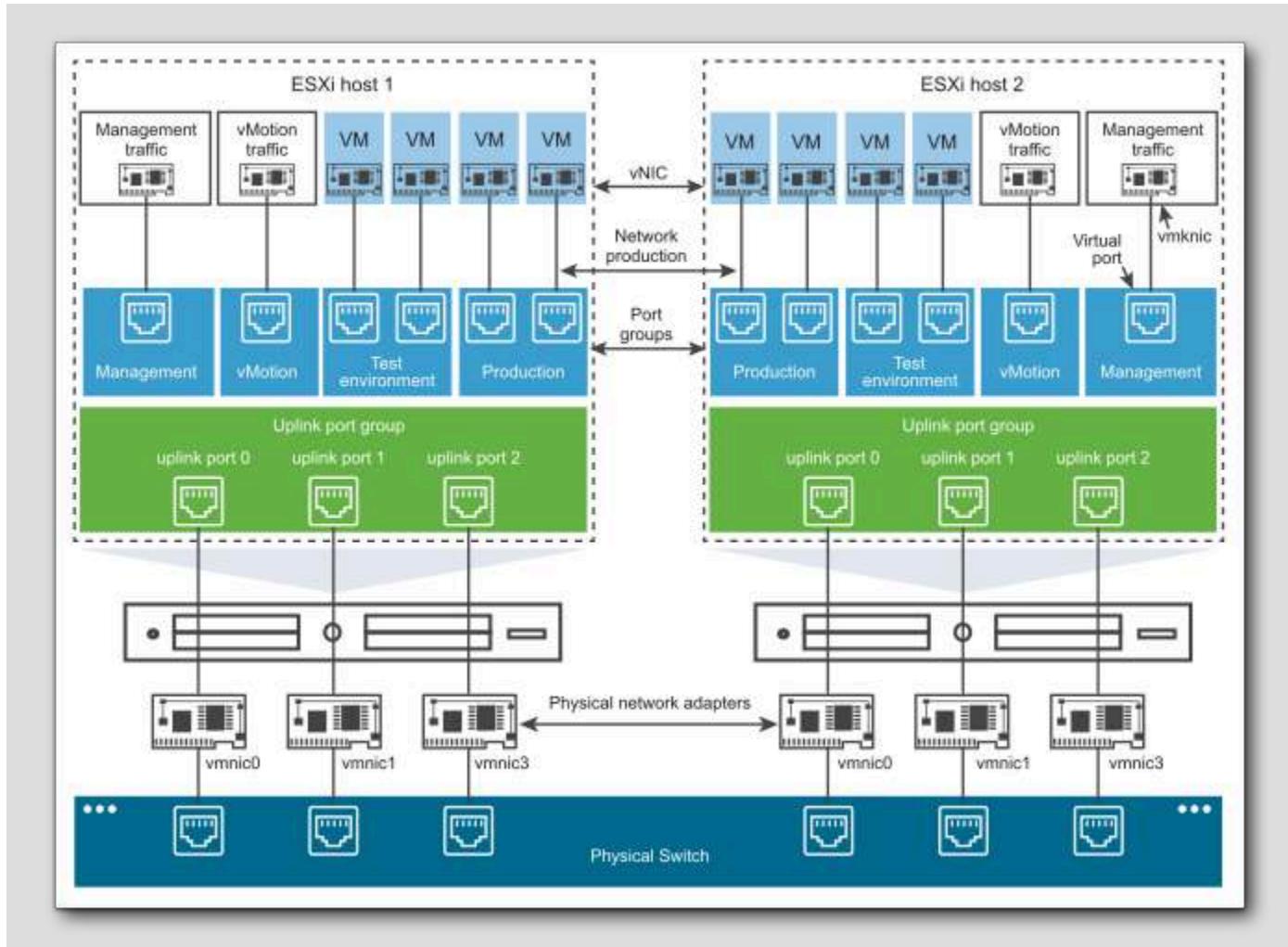
- Network IO Control - New support for per virtual machine Distributed vSwitch bandwidth reservations to guarantee isolation and enforce limits on bandwidth.
- Multicast Snooping - Supports IGMP snooping for IPv4 packet and MLD snooping for IPv6 packets in VDS. Improves performance and scale with multicast traffic.
- Multiple TCP/IP Stack for vMotion - Allows vMotion traffic a dedicated networking stack. Simplifies IP address management with a dedicated default gateway for vMotion traffic.

vSS vs vDS architecture

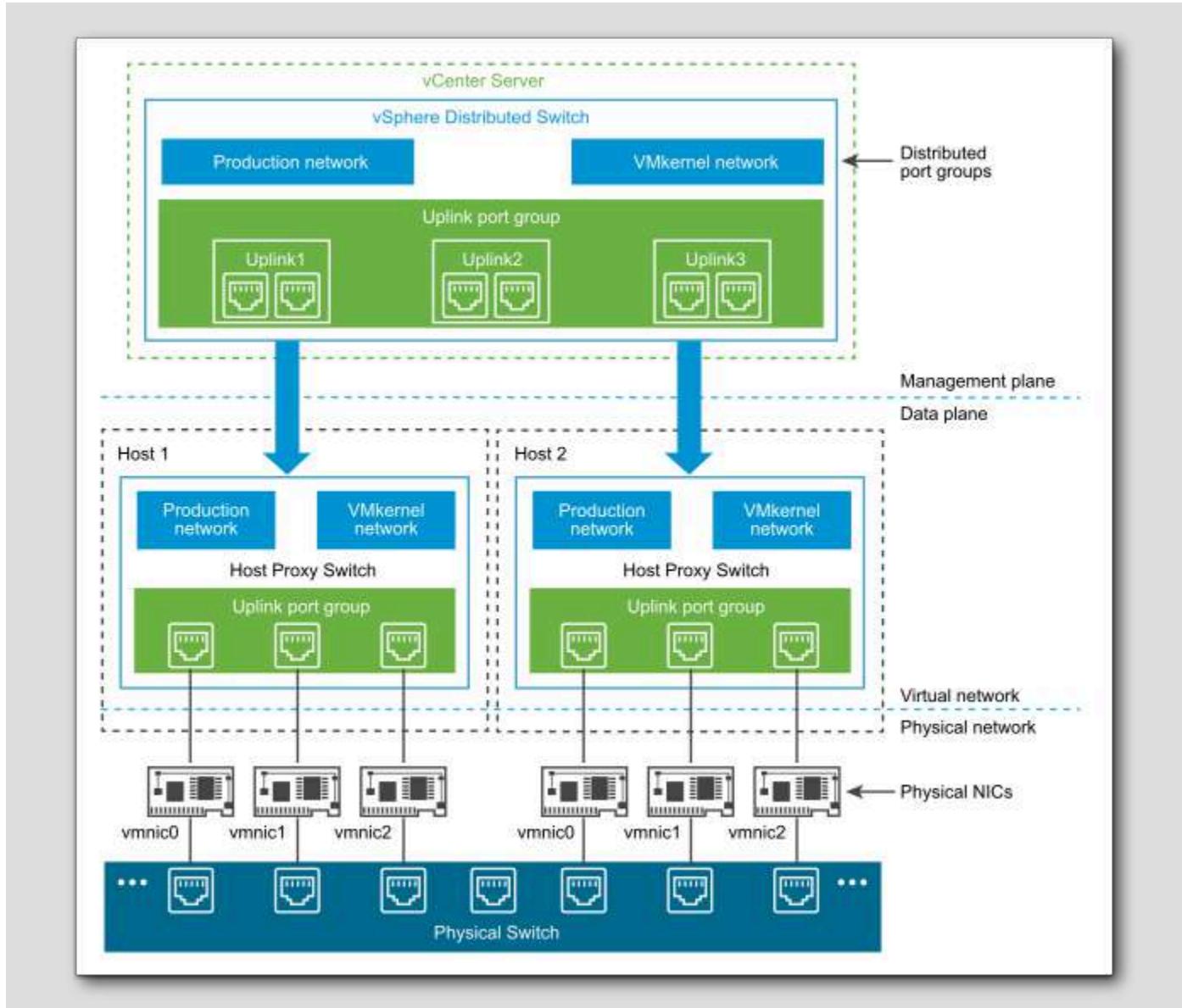
Spend a few minutes reviewing the differences between the *Standard vSwitch* and *Distributed vSwitch* architectures.

Pay special attention to how the port groups and uplinks are designed.

vSphere Standard Switch Architecture



vSphere Distributed Switch Architecture



Let's get started!

[222]

Now that we have a better understanding of what a Distributed vSwitch is and why we would want to use it, let's spend a little time exploring an example of one.

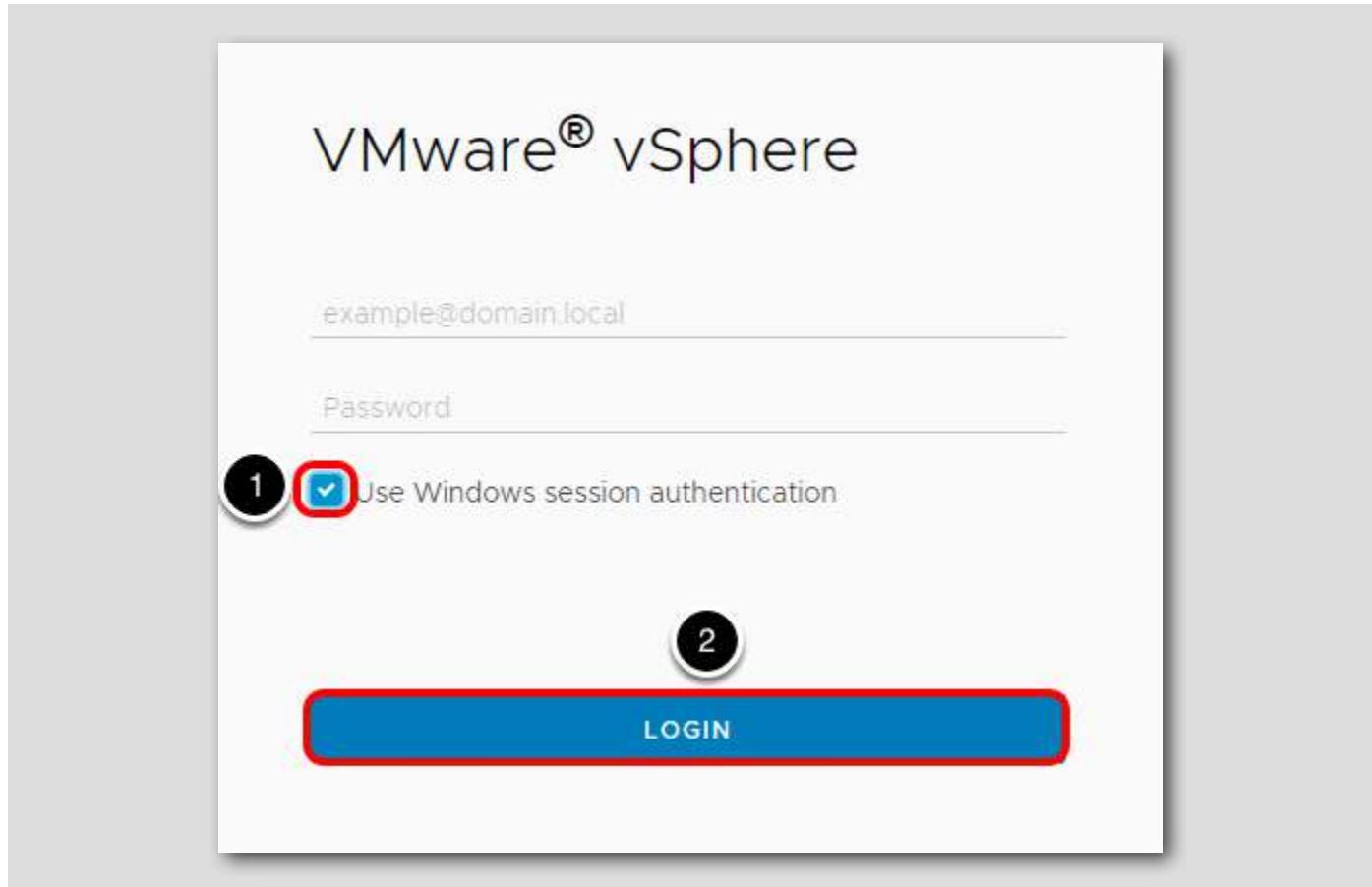
Adding and Configuring vSphere Standard Switch

[223]

The following lesson will walk you through the process of creating and configuring the vSphere Standard Switch.

Adding a Virtual Machine Port Group with the vSphere Client

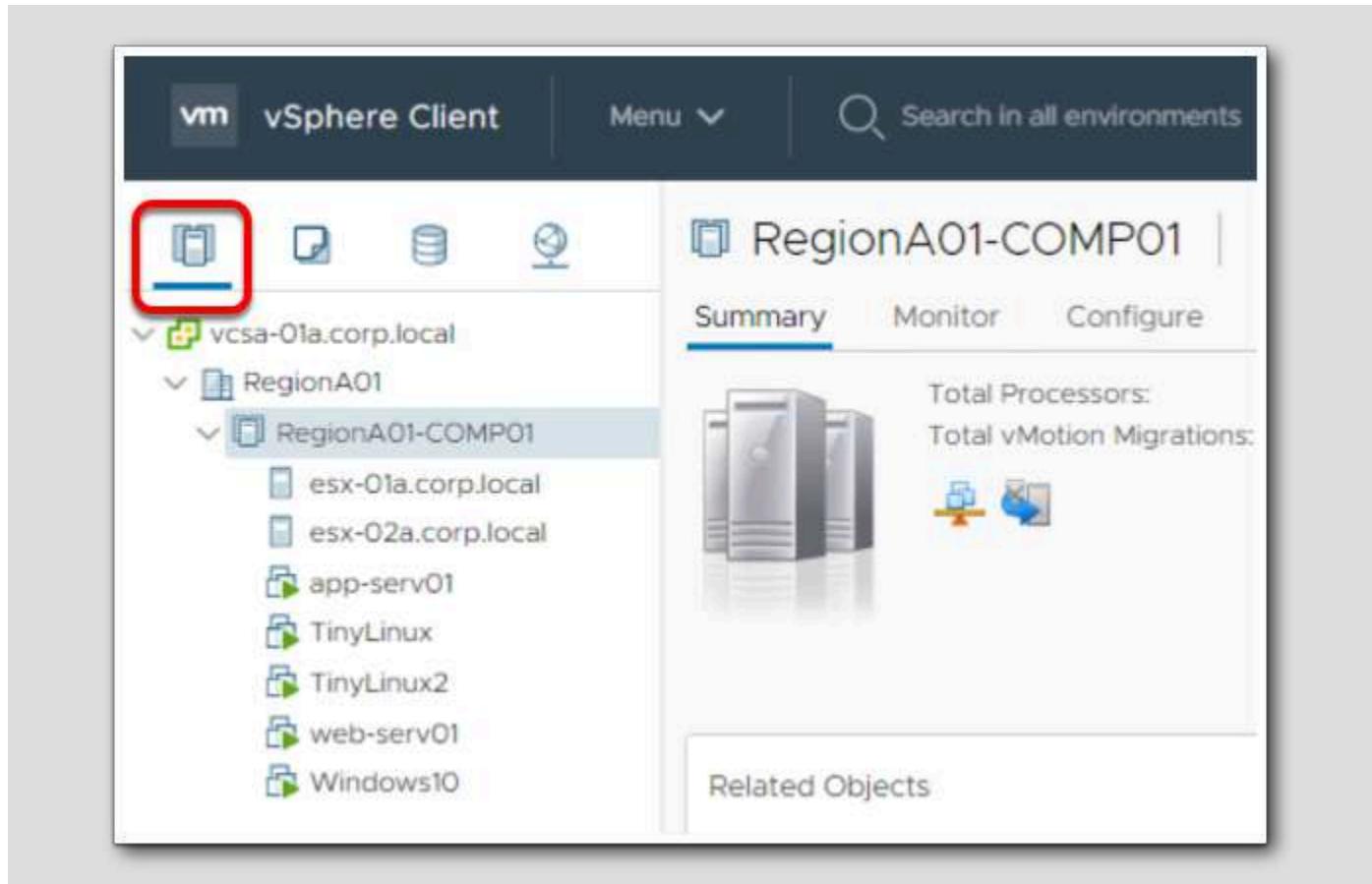
[224]



If you are not already logged in, launch the Chrome browser from the desktop and log in to the vSphere Web Client.

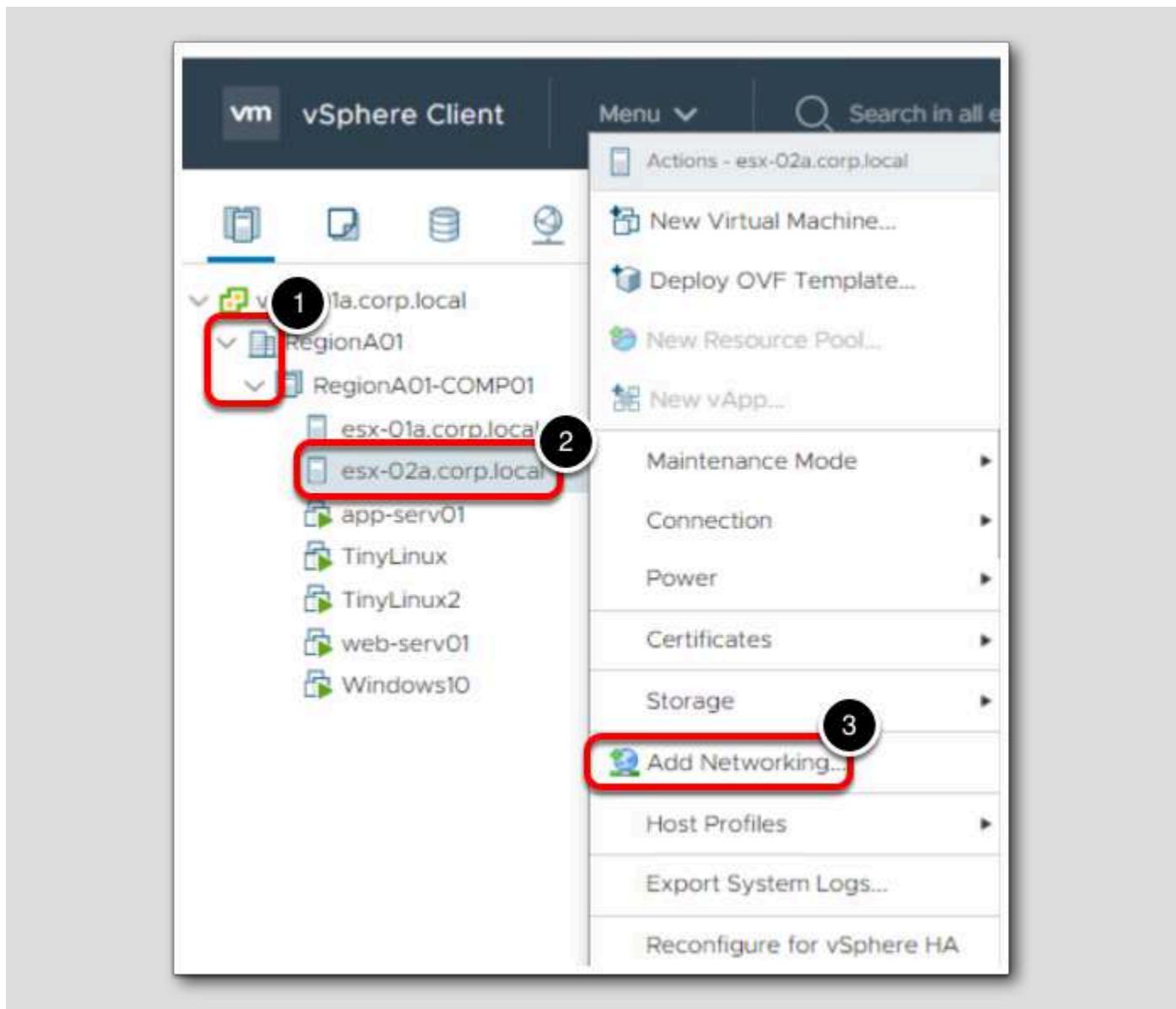
1. Click the "Use Windows session authentication" check box
2. Click "Login"

Select Hosts and Clusters



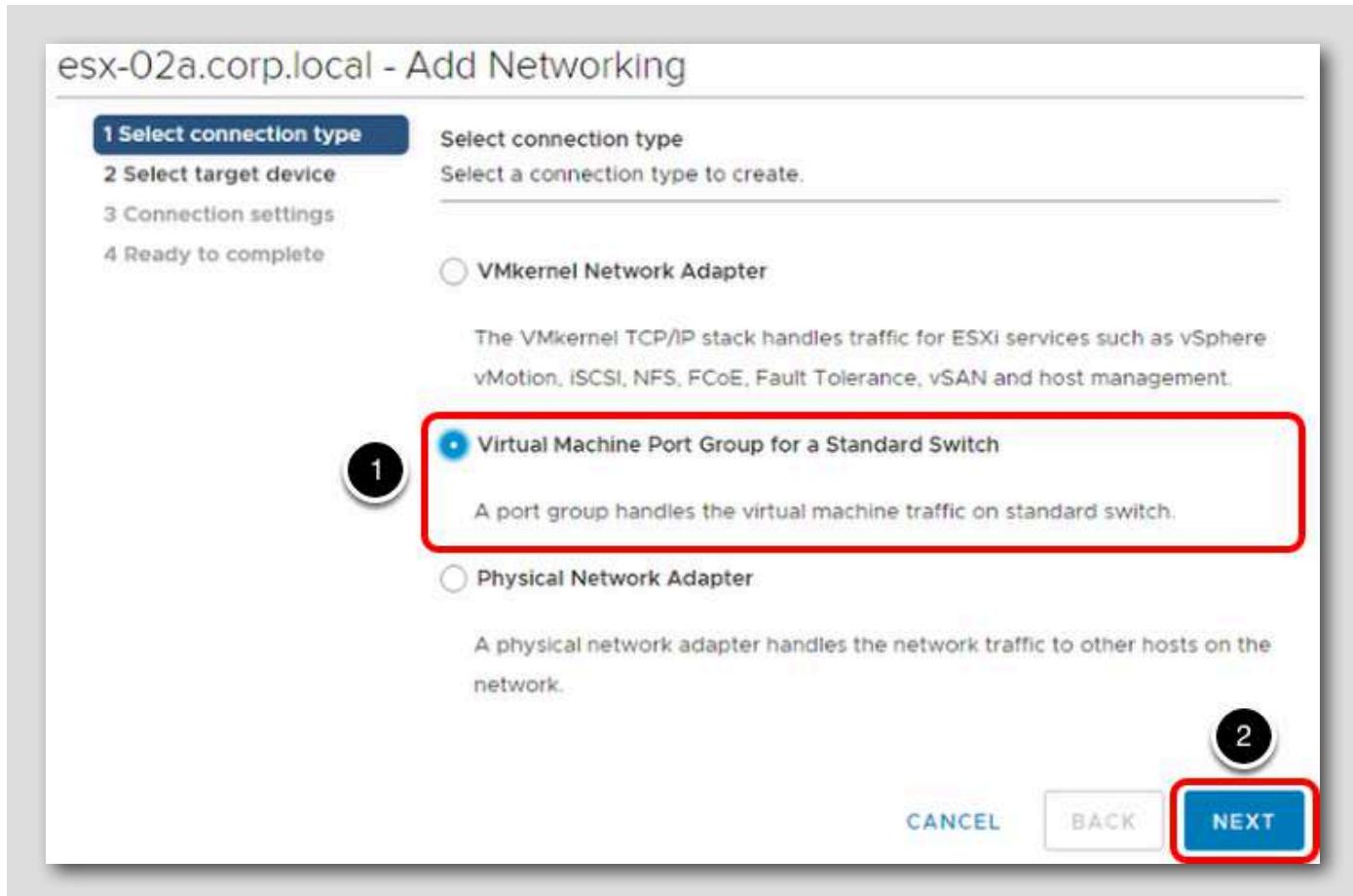
If you are not directed to "Hosts and Clusters", click the icon for it.

Add Networking



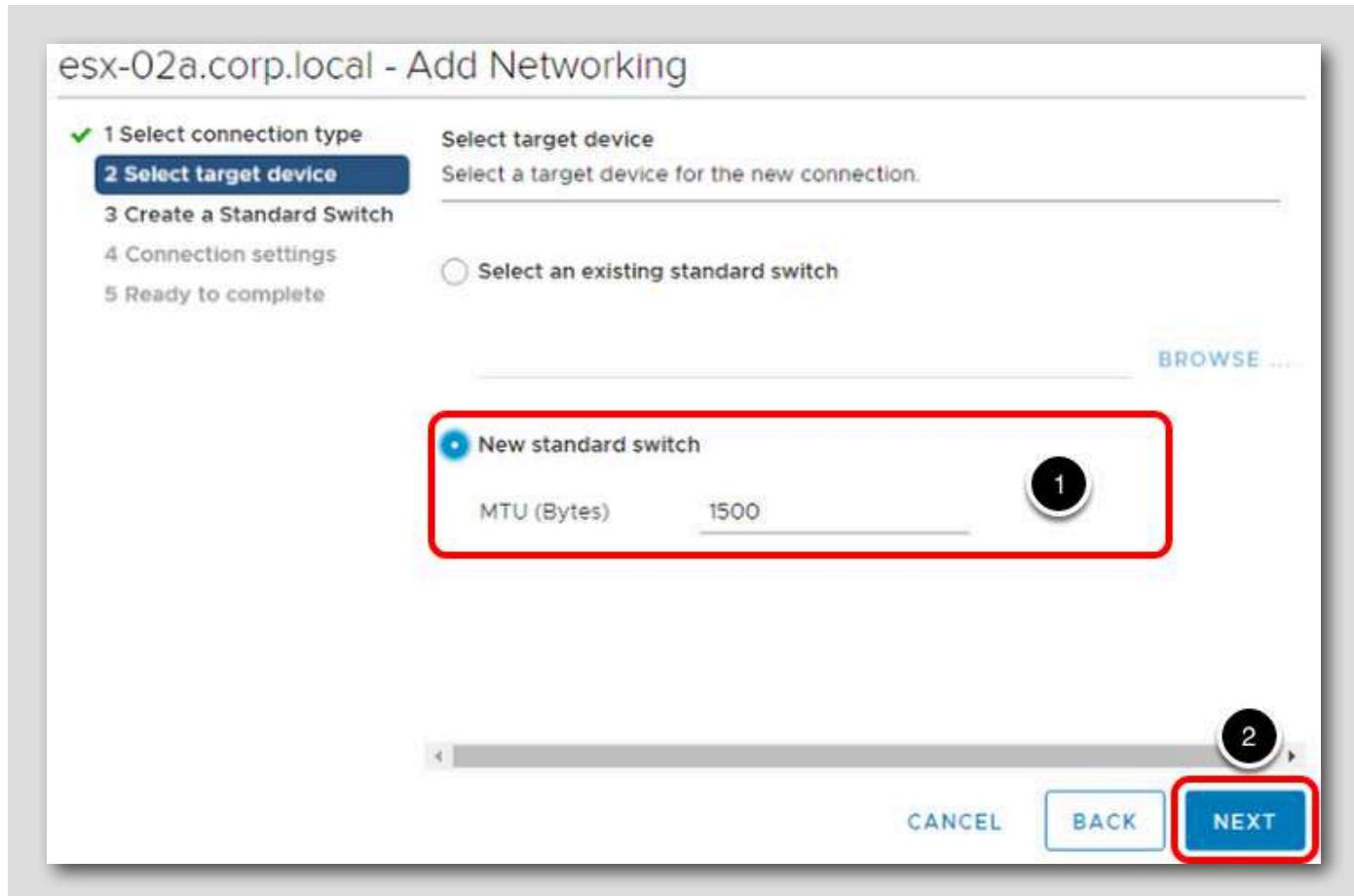
1. Under vcsa-01a.corp.local, expand RegionA01 and then RegionA01-COMP01.
2. Next, right-click on esx-02a.corp.local in the Navigator.
3. Select Add Networking....

Connection Type



1. When asked to select connection type, choose Virtual Machine Port Group for a Standard Switch.
2. Click **Next**.

Target Device



1. When asked to select a target device, choose New Standard Switch. Note that a larger MTU size can be specified if needed.
2. Click Next.

Create a Standard Switch

esx-02a.corp.local - Add Networking

✓ 1 Select connection type
✓ 2 Select target device
3 Create a Standard Switch
4 Connection settings
5 Ready to complete

Create a Standard Switch
Assign free physical network adapters to the new switch.

Assigned adapters

1

+

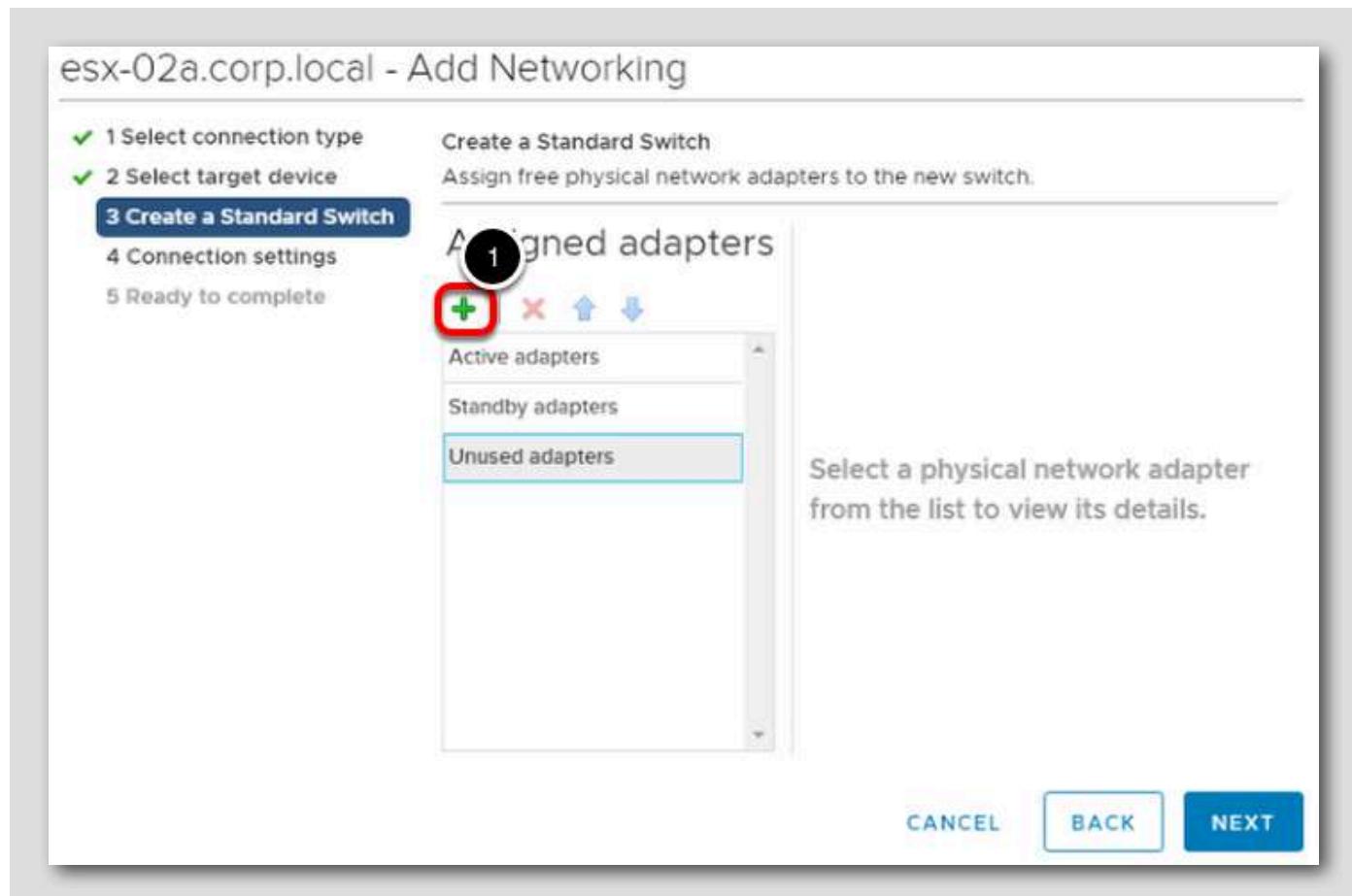
Active adapters

Standby adapters

Unused adapters

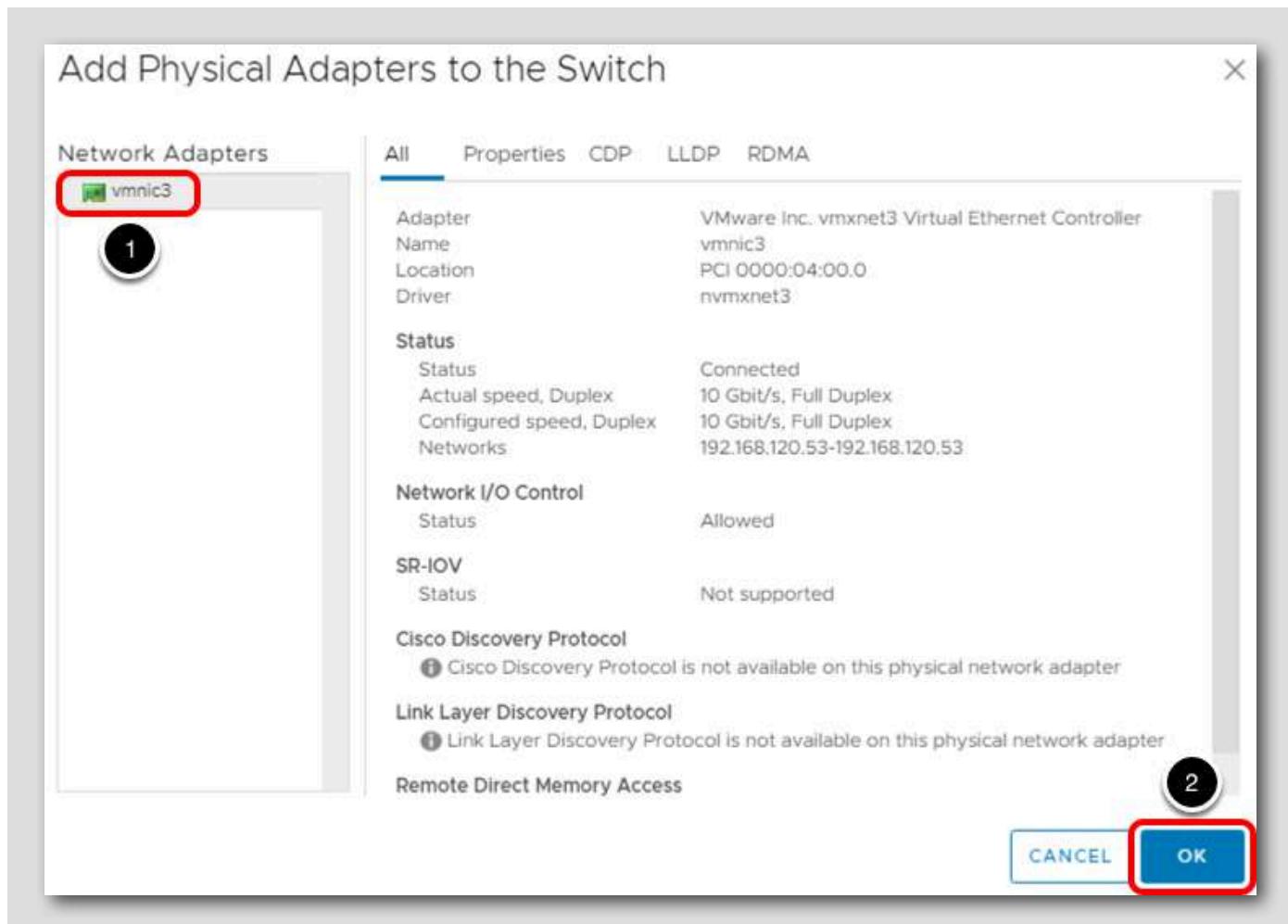
Select a physical network adapter from the list to view its details.

CANCEL BACK NEXT



1. Click the '+' button.

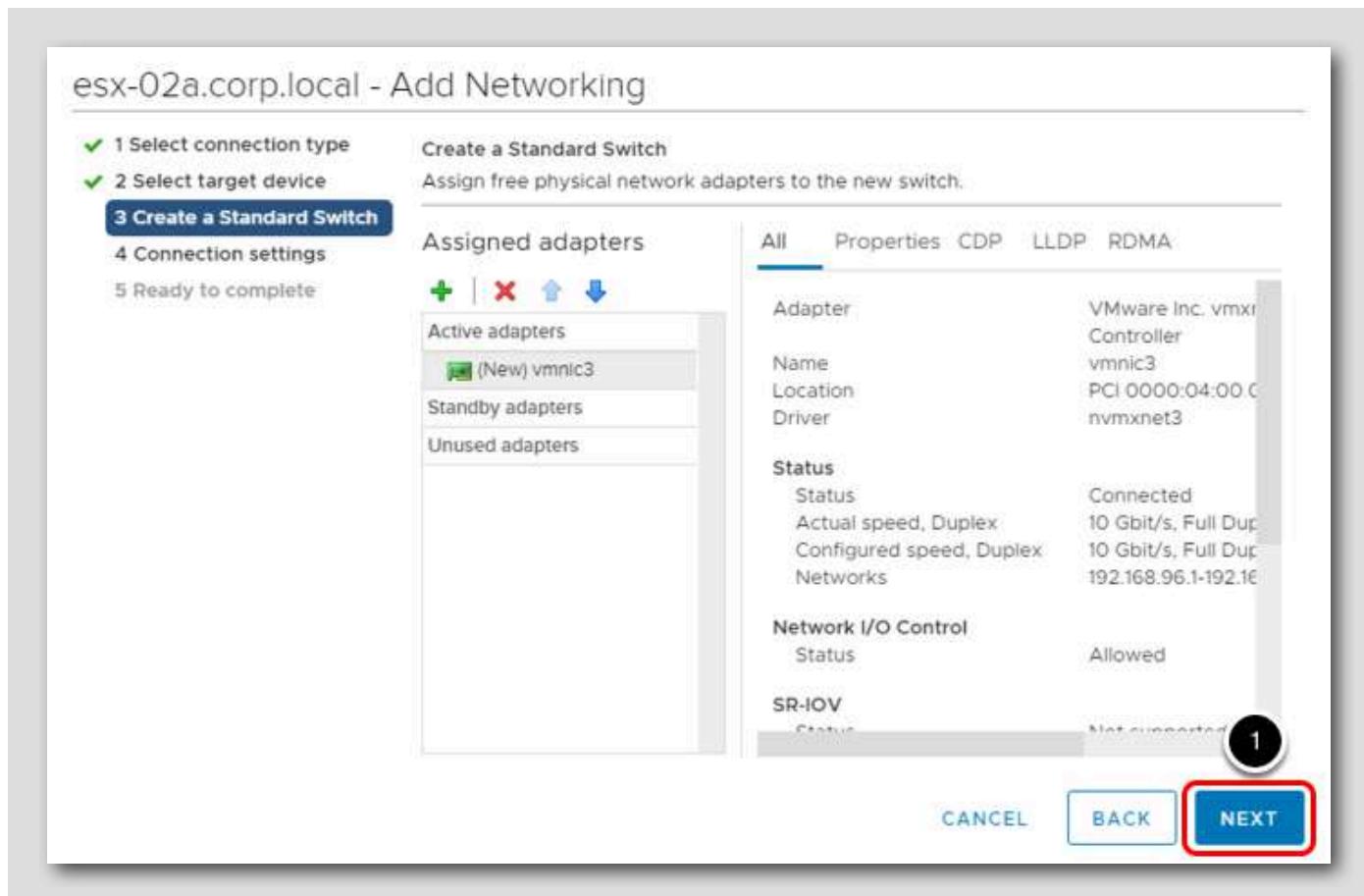
Add Physical Adapter



1. Select vmnic3 under Network Adapters

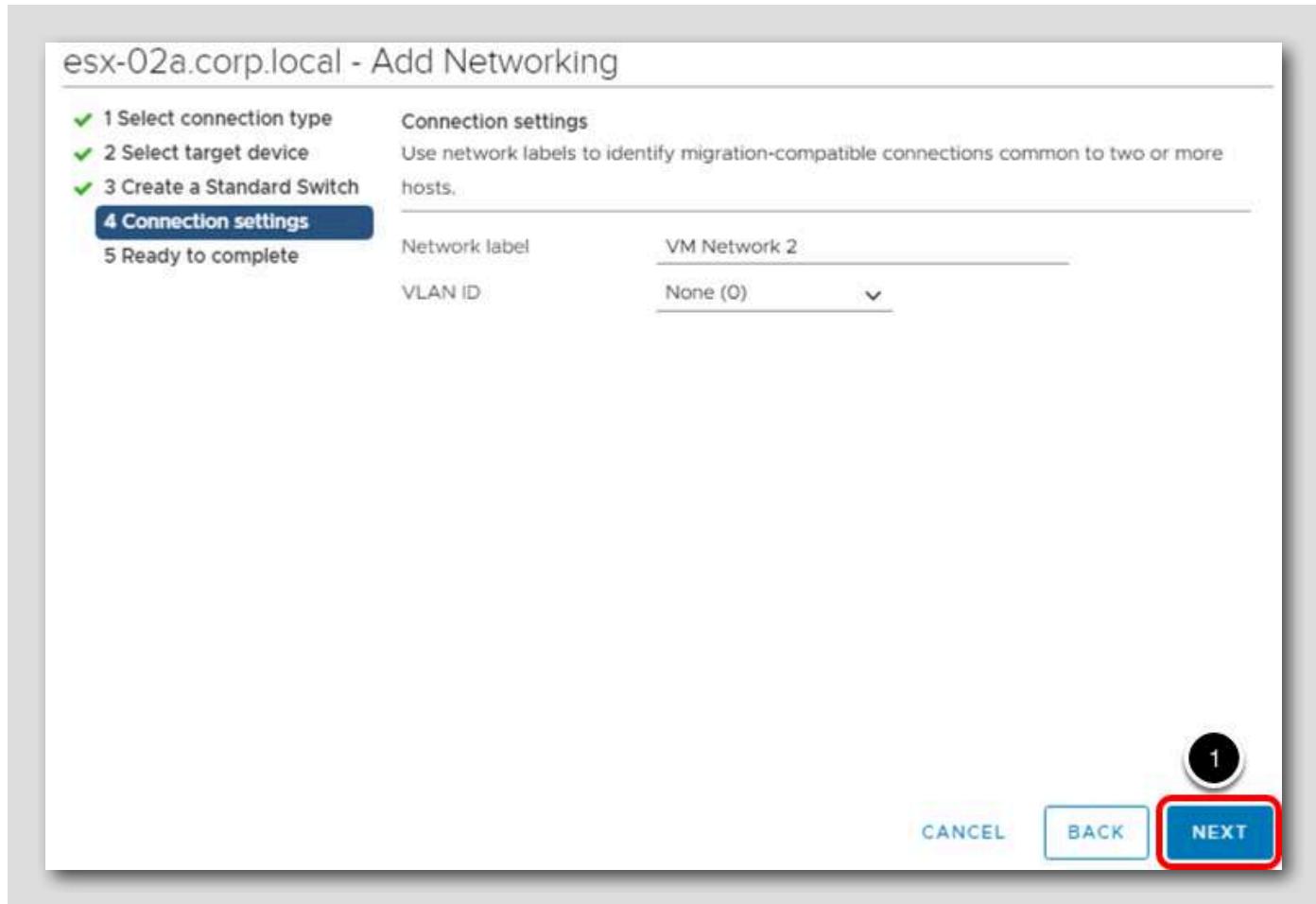
2. Click OK.

Add Physical Adapter



1. Click **Next** to continue.

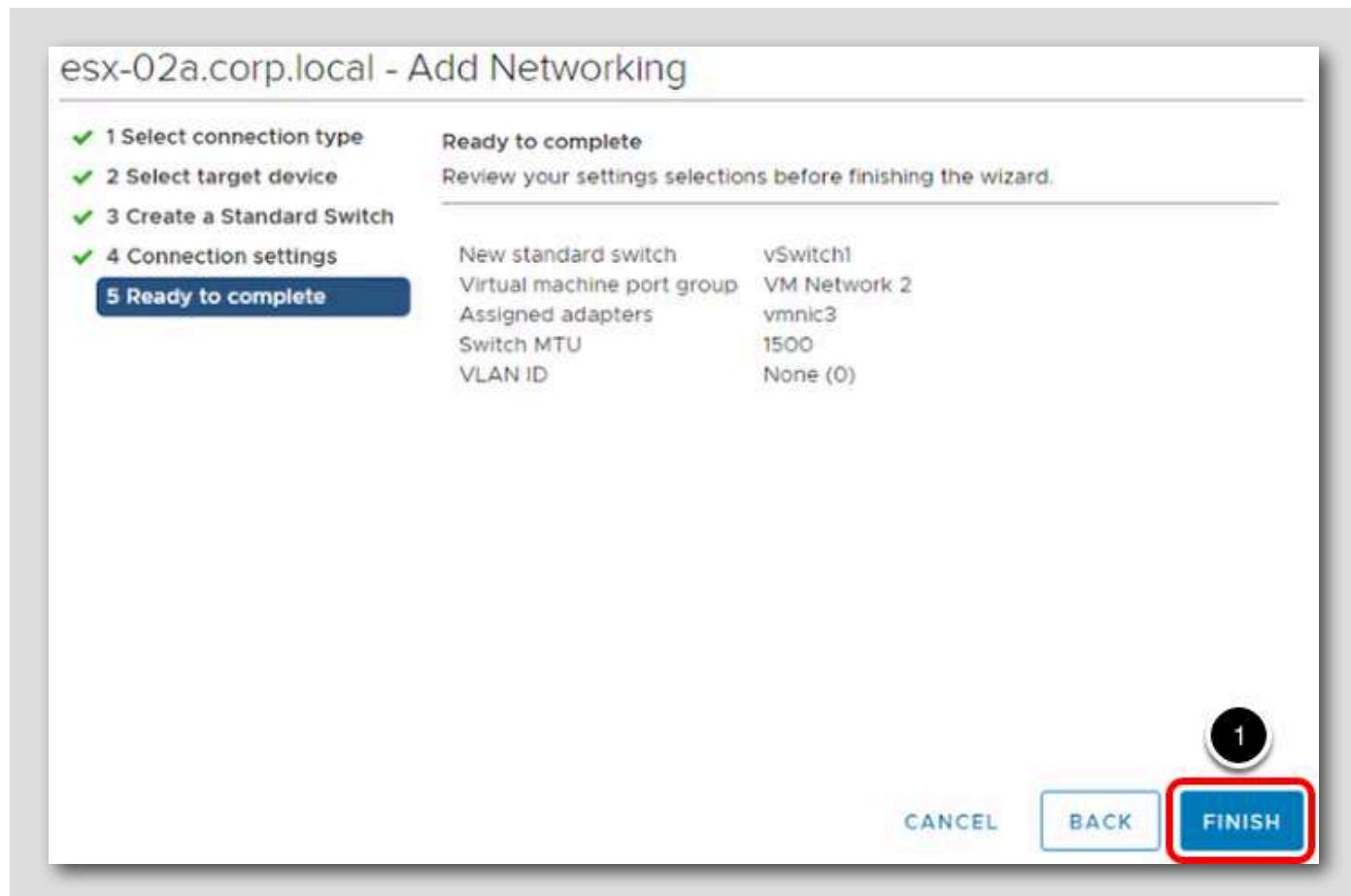
Connection Settings



At the Connection settings step of the wizard, for Network label, leave the default name of VM Network 2.

Do not change the VLAN ID; leave this set to None (0).

Complete the Wizard



1. Review the port group settings in Ready to complete and click Finish.

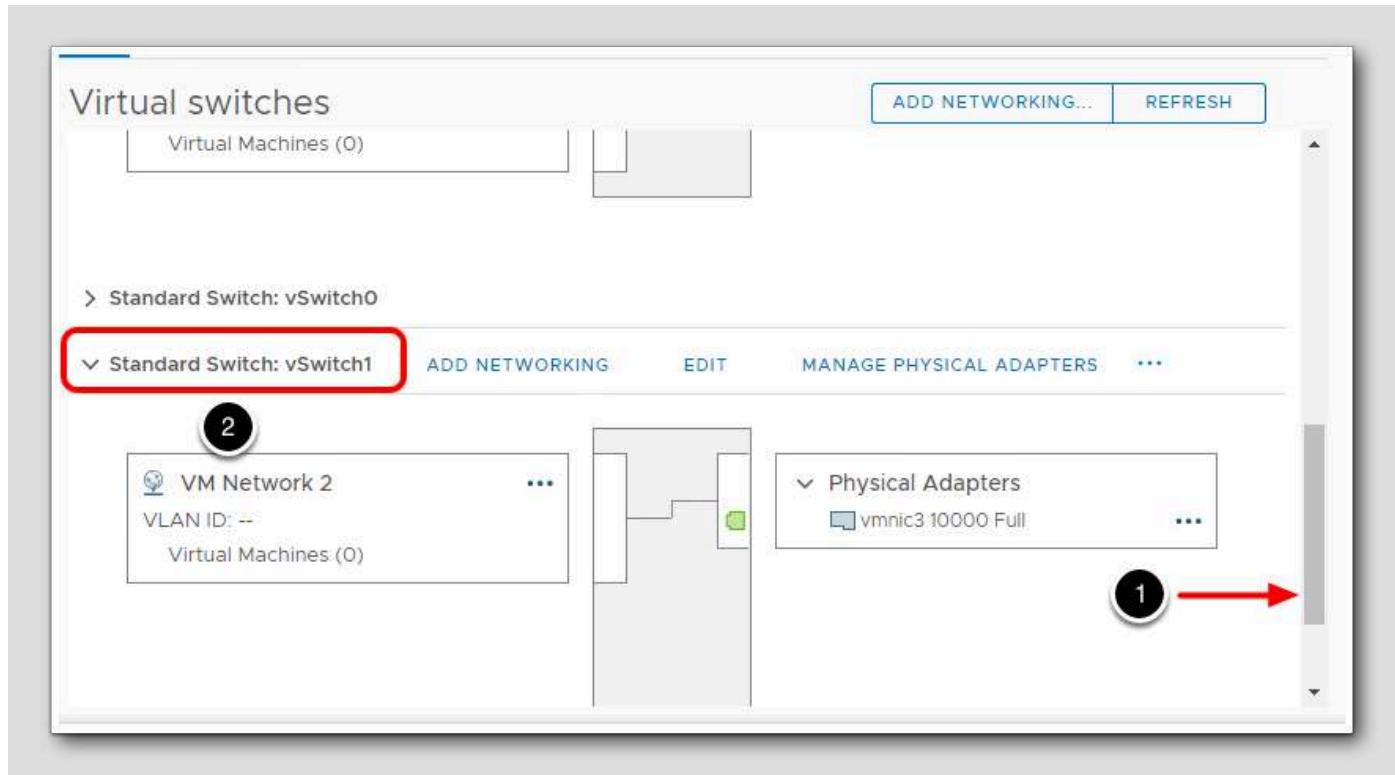
Virtual Switches



Next, we will verify the switch has been created.

1. Click Configure.
2. Click on Virtual Switches.

Standard Switch: vSwitch1



1. Scroll down until you see Standard Switch: vSwitch1.

2. If needed, expand the section.

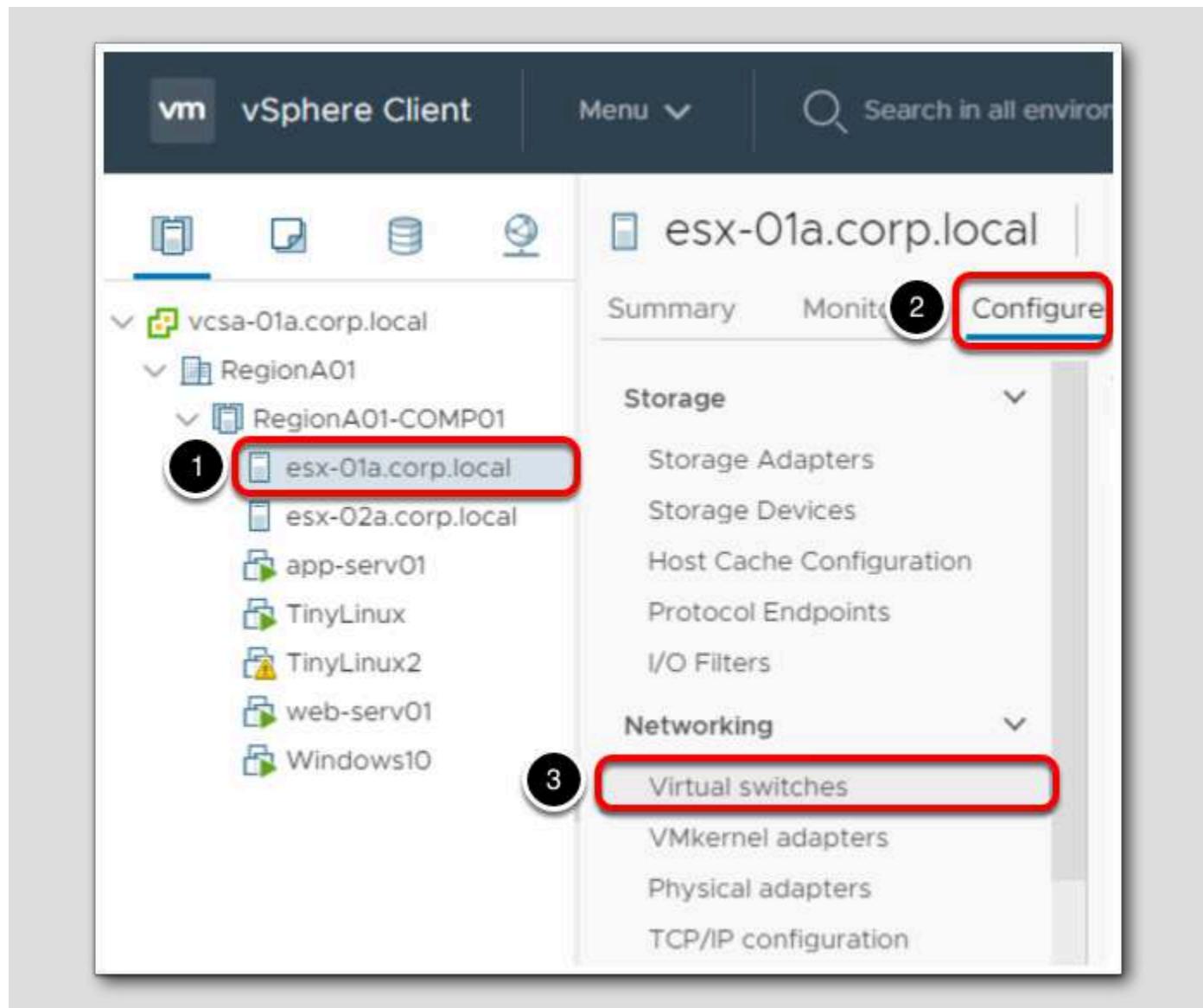
You should see the above diagram showing a virtual port group (VM Network 2) that is on vSwitch1 and it is using vmnic3 as an uplink.

Editing a Standard Switch in the vSphere Web Client

In this lesson, we will review the various properties of a Standard Switch.

vSphere Standard Switch settings control switch-wide defaults and switch properties such as the uplink configuration.

Select esxi-01a.corp.local



1. Select esxi-01a.corp.local.
2. Ensure the Configure tab is selected.
3. Click Virtual switches.

Select vSwitch0

The screenshot shows the 'Virtual switches' interface in the vSphere Web Client. At the top, there is a header with 'Virtual switches' and 'ADD NETWORKING...', 'REFRESH' buttons. Below the header, there is a list of existing virtual switches:

- vMotion-RegionA01-vDS-COMP ... (VLAN ID: --, VMkernel Ports (1), Virtual Machines (0))
- Standard Switch: vSwitch0** (VLAN ID: --, Virtual Machines (4))

Below the list, there are buttons for 'ADD NETWORKING', 'EDIT', 'MANAGE PHYSICAL ADAPTERS', and three dots. To the right of the list, there is a vertical scroll bar highlighted with a red rectangle. The 'Standard Switch: vSwitch0' section is also highlighted with a red rectangle and has a circled '2' above it. A circled '1' is located near the bottom right corner of the scroll bar area.

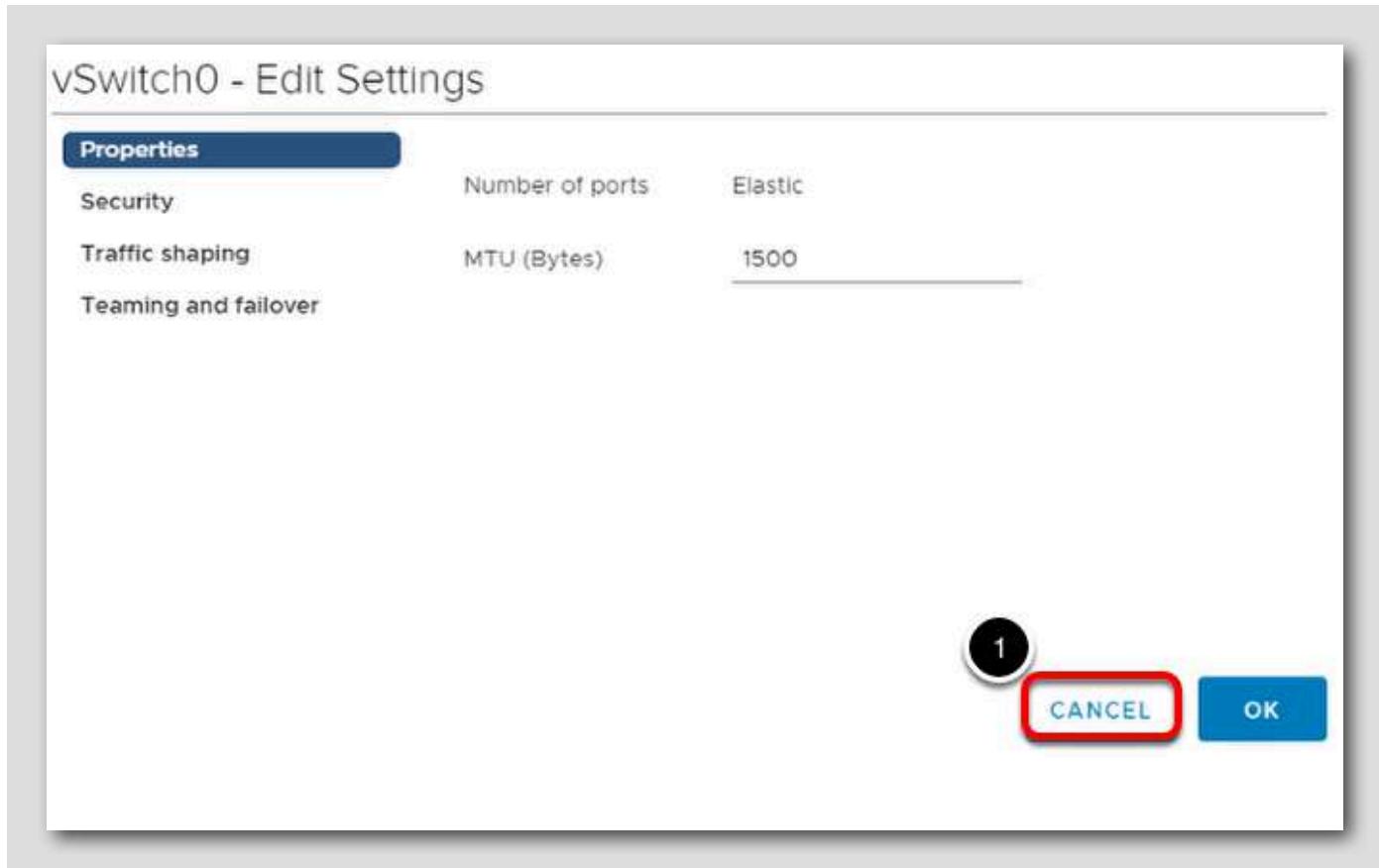
1. You will need to scroll down until you reach the Standard Switch: vSwitch0 section.
2. Expand the section to view the layout of the switch.

Edit vSwitch1

The screenshot shows the vSphere Web Client interface for managing networking. The left sidebar has 'Networking' expanded, with 'Virtual switches' selected. The main pane displays 'Virtual switches' with two entries: 'Distributed Switch: RegionA01-vDS-COMP' and 'Standard Switch: vSwitch0'. Below each entry are 'ADD NETWORKING...', 'EDIT' (which is circled with a red box and has a circled '1' above it), 'MANAGE PHYSICAL ADAPTERS', and more options. Under 'vSwitch0', there's a 'VM Network' card showing 'VLAN ID: --' and 'Virtual Machines (4)'. To the right is a network topology diagram and a 'Physical Adapters' section listing 'vmnic2 10000 Full'.

1. Click Edit.

Properties (MTU Setting)



If you are using jumbo frames in your environment and want to leverage this on a vSphere Standard Switch, you can change the MTU setting here.

You can change the size of the maximum transmission unit (MTU) on a vSphere Standard Switch to increase the amount of payload data transmitted with a single packet, that is, enabling jumbo frames. Be sure to check with your Networking team prior to making any modifications here. To realize the benefit of this setting and prevent performance issues, compatible MTU settings are required across all virtual and physical switches and end devices such as hosts and storage arrays.

You will also notice the Security, Traffic shaping, and Team and Failover options. This is where the default settings for the virtual switch would be set. As you will see later, these defaults may be overridden at the port group level as required.

1. Click the Cancel button.

Next, an additional uplink will be added to the switch and the other options will be reviewed.

Add Uplink Adapters in the vSphere Web Client

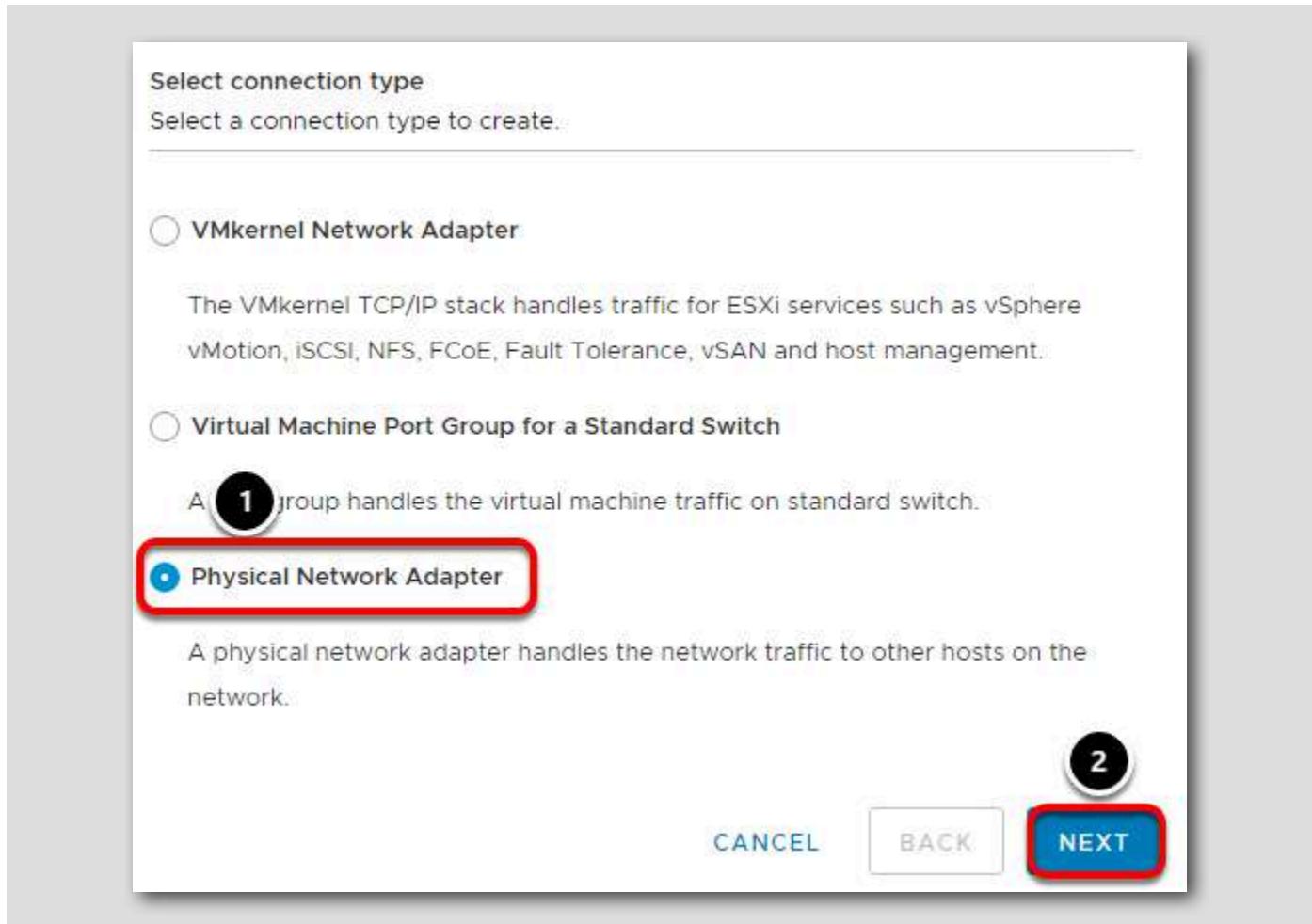
You can associate multiple adapters to a single vSphere standard switch to increase throughput and provide redundancy should a link fail. This is known as "NIC Teaming."

Select Virtual switches

The screenshot shows the 'Virtual switches' section of the vSphere Web Client. At the top, there is a header with 'Virtual switches' and an 'ADD NETWORKING...' button. Below the header, there is a list of switches. The first item is 'Standard Switch: vSwitch0', which has an 'ADD NETWORKING...' button next to it, highlighted with a red box. There are also 'EDIT' and 'MANAGE' buttons for this switch. To the right of the switch list, there is a diagram showing a network topology. On the left, there is a box labeled 'VM Network' with 'VLAN ID: --' and 'Virtual Machines (1)'. In the center, there is a standard switch icon with two ports. One port is connected to a green square representing a physical adapter, and the other port is connected to a white square representing another virtual machine or adapter. To the right, there is a box labeled 'Physical' with 'vmni'.

1. Click Add Networking

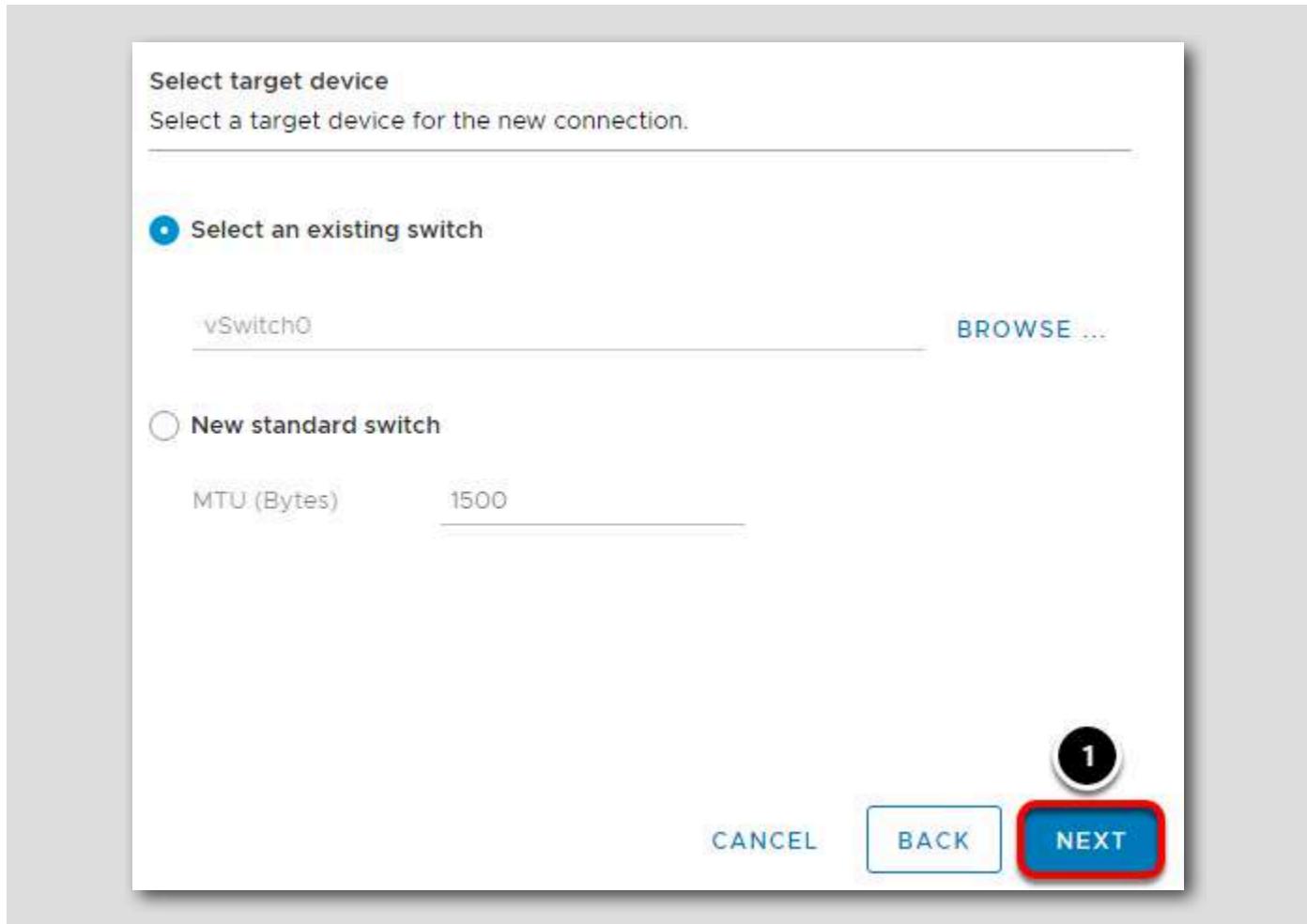
Select Connection Type



1. Select Physical Network Adapter.

2. Click Next.

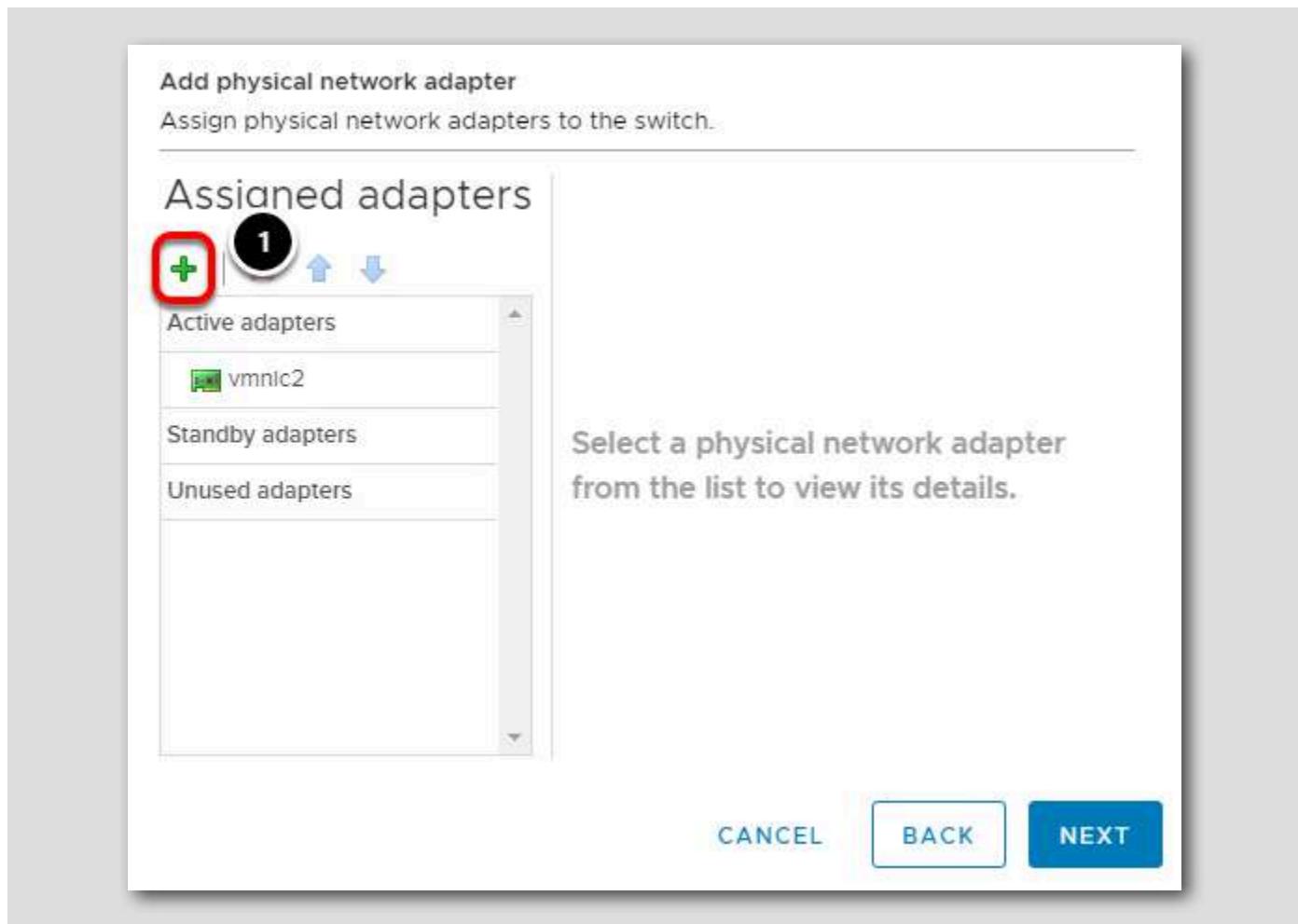
Select Target Device



Since a new network connect will be added to vSwitch0, no changes are needed.

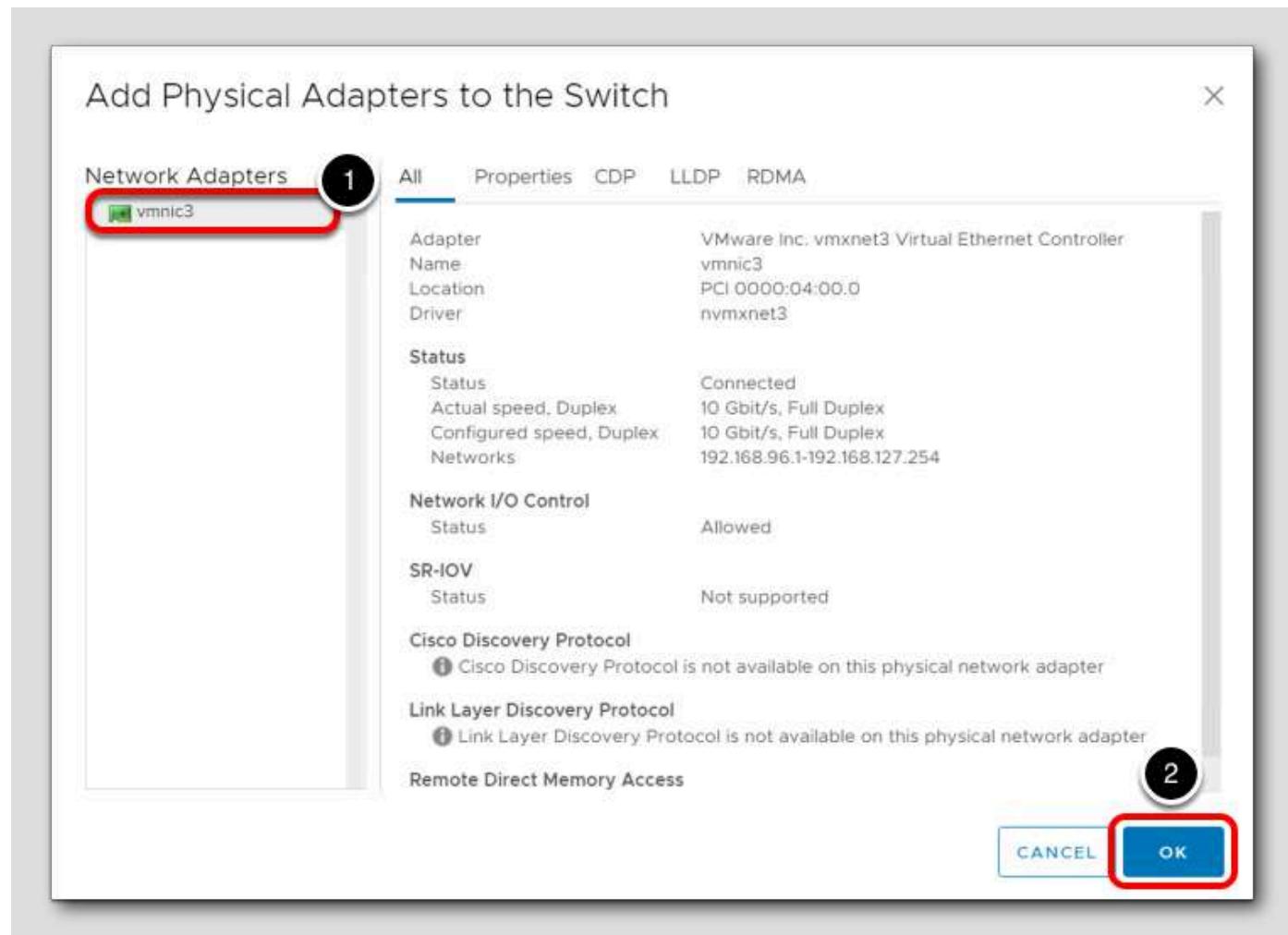
1. Click **Next**.

Add Networking



1. Click the green '+' to add the adapter.

Add vmnic3



1. Click on vmnic3

2. Click OK

Assigned Adapters

esx-01a.corp.local - Add Networking

✓ 1 Select connection type
✓ 2 Select target device
3 Add physical network ad...
4 Ready to complete

Add physical network adapter
Assign physical network adapters to the switch.

Adapter	
Name	VMware Inc. v
Location	Controller
Driver	vmnic3
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full
Configured speed, Duplex	10 Gbit/s, Full
Networks	192.168.96.1-19

Network I/O Control

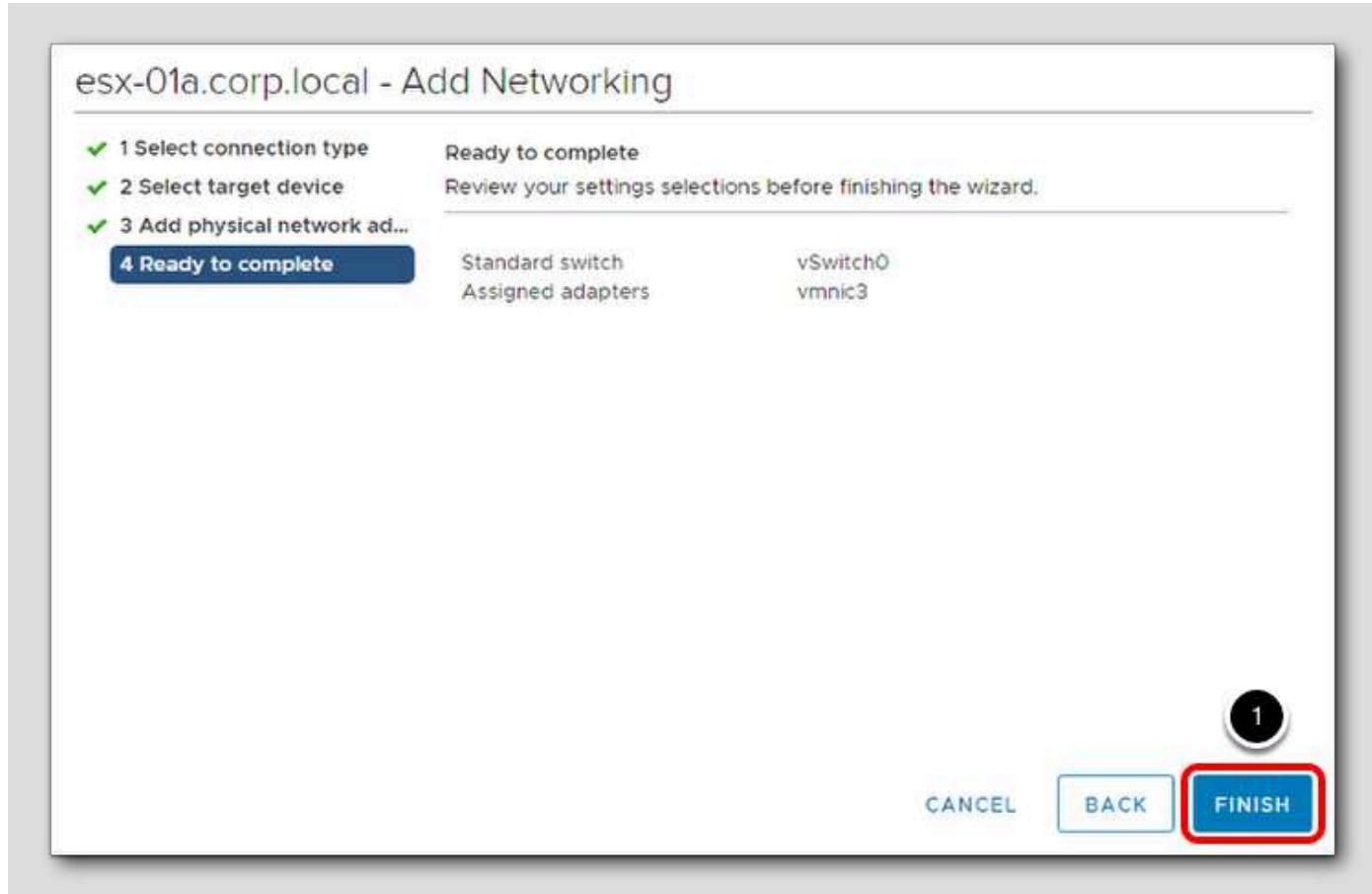
Status	Allowed

CANCEL BACK **NEXT**

The new adapter has been added in the Active Adapters section. An adapter could also be moved to the Standby Adapters section to be used for failover. The Unused Adapters section can be used when there are multiple portgroups on a switch and you would like the ability to control what traffic flows through which physical adapter. It can be used to segment traffic or be used for individual VLAN traffic.

1. Click **Next**.

Ready to Complete

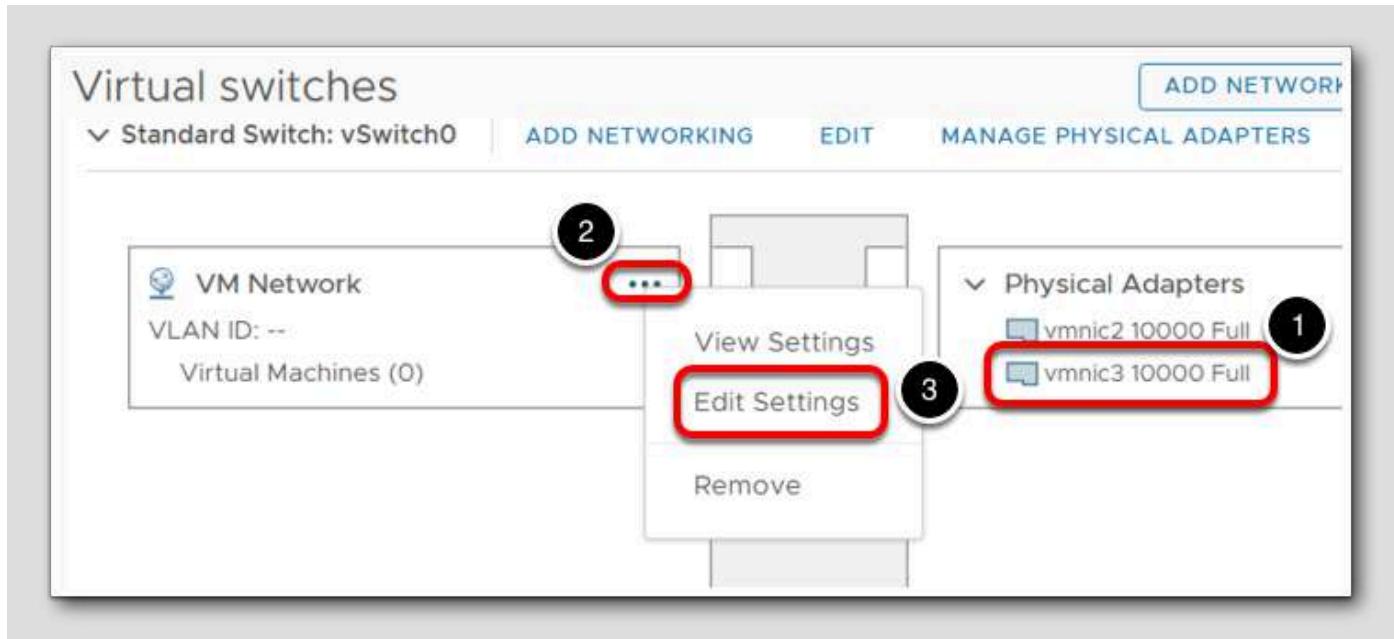


Click **Finish** to add vmnic3 to vSwitch0.

Editing a Standard Switch Port Group

Once the vSwitch has been configured and its defaults have been set, the port group can be configured. The port group is the construct that is connected to virtual machine NICs and usually represents a VLAN or physical network partition such as Production, Development, Desktop or DMZ.

New vmnic Added

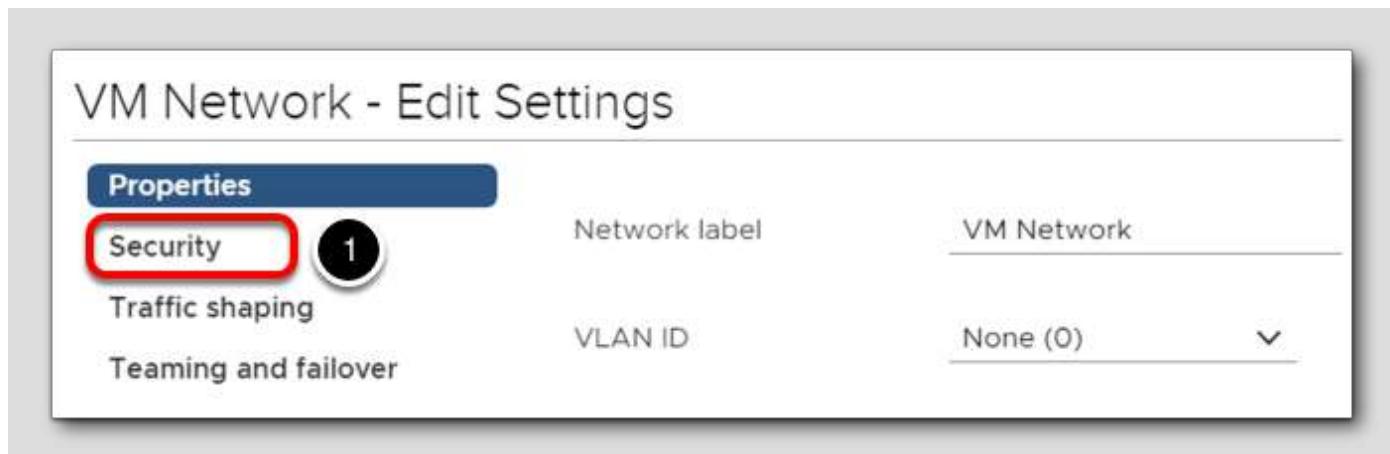


1. In the Physical Adapters section, vmnic3 has been added to the switch.

Now we will look at some of the options that can be selected at the port group level of a Standard Switch.

2. Click on the drop-down menu for the **VM Network** port group.
3. Select **Edit Settings**.

Port Group Properties

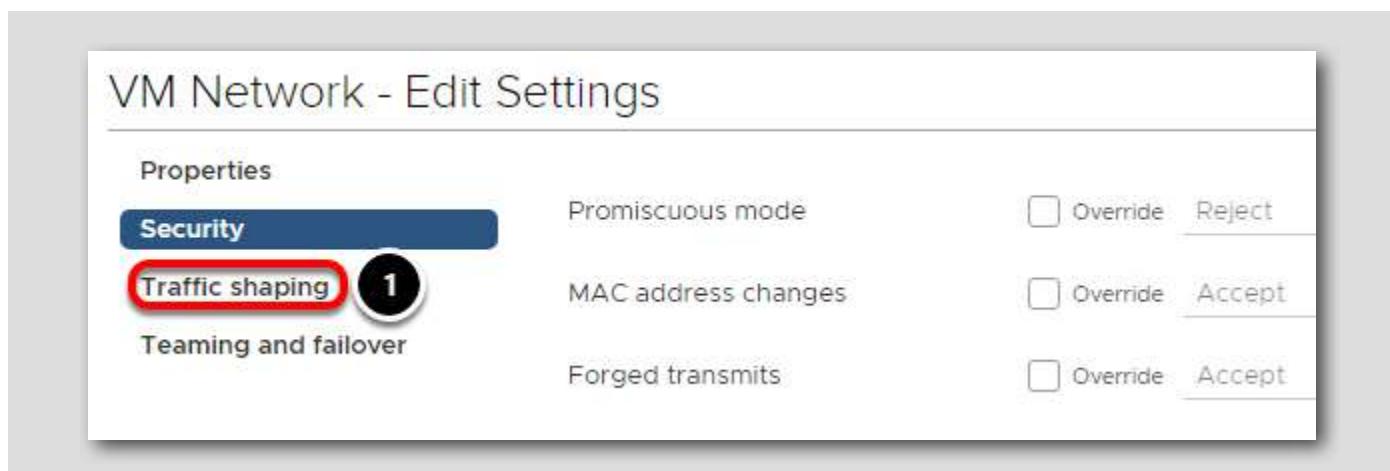


The Properties setting section is where the name or VLAN ID of the port group can be modified.

There is no need to modify these settings for this part of the lab.

1. Click **Security**.

Port Group Security



By ticking the Override box, you can override the default setting of the Standard Switch for just this port group.

In this section, you can configure the following:

Promiscuous Mode

- Reject — Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter.
- Accept — Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the vSphere standard switch that are allowed under the VLAN policy for the port group that the adapter is connected to.

MAC Address Changes

- Reject — If you set the MAC Address Changes to Reject and the guest operating system changes the MAC address of the adapter to anything other than what is in the .vmx configuration file, all inbound frames are dropped. If the Guest OS changes the MAC address back to match the MAC address in the .vmx configuration file, inbound frames are passed again.
- Accept — Changing the MAC address from the Guest OS has the intended effect: frames sent to the altered MAC address are received by the virtual machine.

Forged Transmits

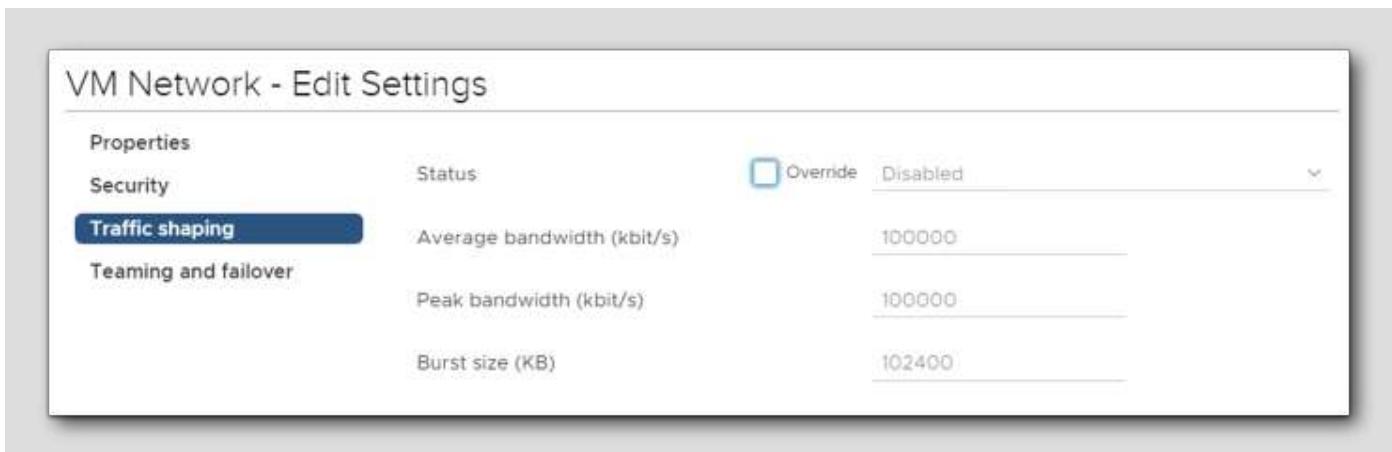
- Reject — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped.
- Accept — No filtering is performed and all outbound frames are passed.

No changes are needed here.

1. Click **Traffic shaping**.

Traffic Shaping

[253]



Just like in the Security settings, you can override the default policy set at the switch level to apply to just this port group.

A traffic shaping policy is defined by average bandwidth, peak bandwidth, and burst size. You can establish a traffic shaping policy for each port group.

ESXi shapes outbound network traffic on standard switches. Traffic shaping restricts the network bandwidth available on a port, but can also be configured to allow bursts of traffic to flow through at higher speeds.

Average Bandwidth

- Establishes the number of bits per second to allow across a port, averaged over time. This number is the allowed average load.

Peak Bandwidth

- Maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This number limits the bandwidth that a port uses when it is using its burst bonus.

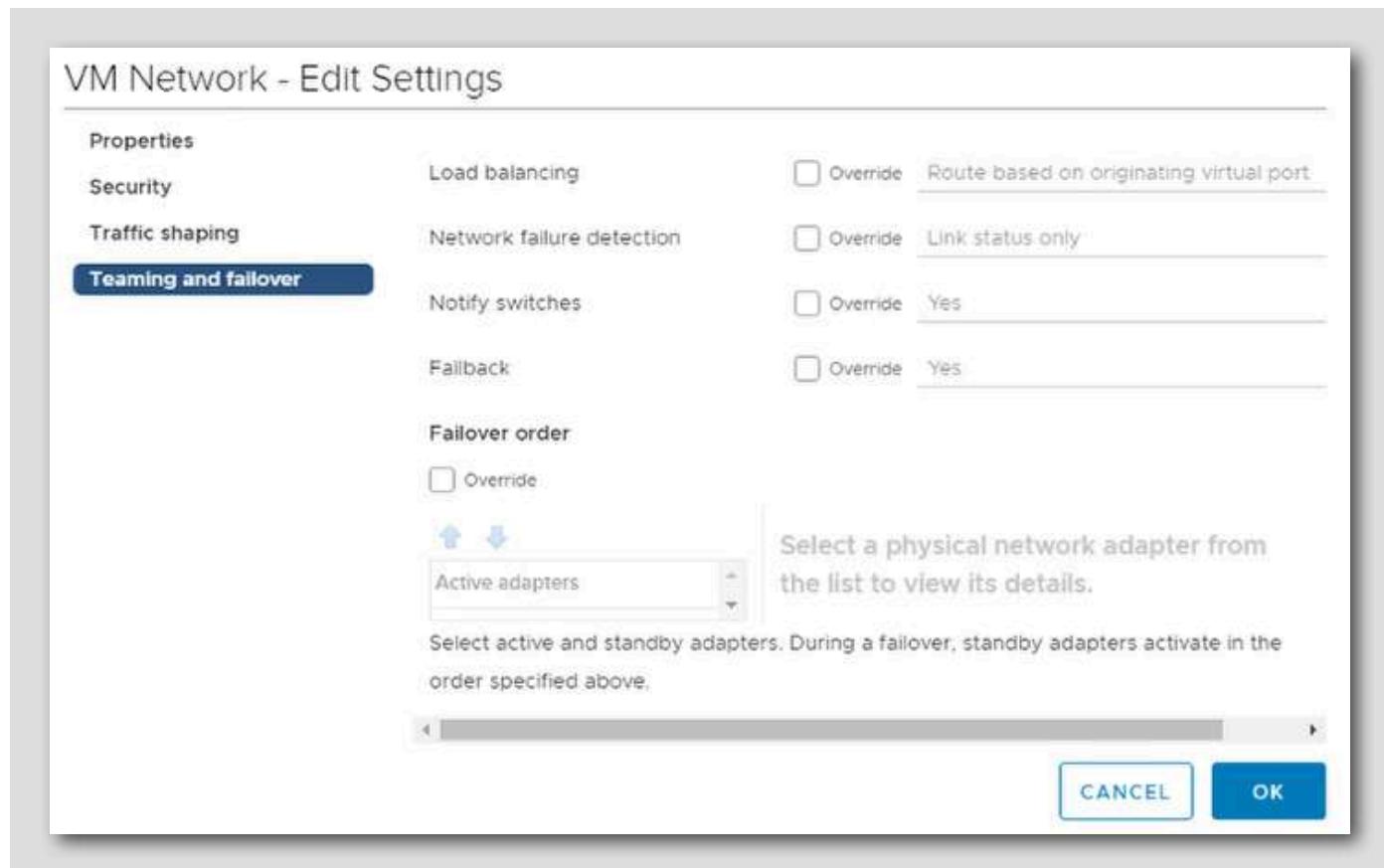
Burst Size

- Maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus if it does not use all its allocated bandwidth. When the port needs more bandwidth than specified by the average bandwidth, it might be allowed to temporarily transmit data at a higher speed if a burst bonus is available. This parameter limits the number of bytes that have accumulated in the burst bonus and transfers traffic at a higher speed.

No changes are needed here.

1. Clicking Teaming and failover.

Teaming and Failover



Again, we have the option to override the default virtual switch settings.

Load Balancing Policy - The Load Balancing policy determines how network traffic is distributed between the network adapters in a NIC team. vSphere virtual switches load balance only the outgoing traffic. Incoming traffic is controlled by the load balancing policy on the physical switch.

- Route based on the originating virtual port - Select an uplink based on the virtual port IDs on the switch. After the virtual switch selects an uplink for a virtual machine or a VMkernel adapter, it always forwards traffic through the same uplink for this virtual machine or VMkernel adapter.
- Route based on IP hash - Select an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, the switch uses the data at those fields to compute the hash. IP-based teaming requires that the physical switch is configured with EtherChannel.
- Route based on source MAC hash - Select an uplink based on a hash of the source Ethernet.
- Route based on physical NIC load - Available for distributed port groups or distributed ports. Select an uplink based on the current load of the physical network adapters connected to the port group or port. If an uplink remains busy at 75 percent or higher for 30 seconds, the host proxy switch moves a part of the virtual machine traffic to a physical adapter that has free capacity.
- Use explicit failover order - From the list of active adapters, always use the highest order uplink that passes failover detection criteria. No actual load balancing is performed with this option.

Network Failure Detection - The method the virtual switch will use for failover detection.

- Link Status only - Relies only on the link status that the network adapter provides. This option detects failures such as removed cables and physical switch power failures.
- Beacon Probing - Sends out and listens for beacon probes on all NICs in the team, and uses this information, in addition to link status, to determine link failure. ESXi sends beacon packets every second. The NICs must be in an active/active or active/standby configuration because the NICs in an unused state do not participate in beacon probing.

Notify Switches - specifies whether the virtual switch notifies the physical switch in case of a failover.

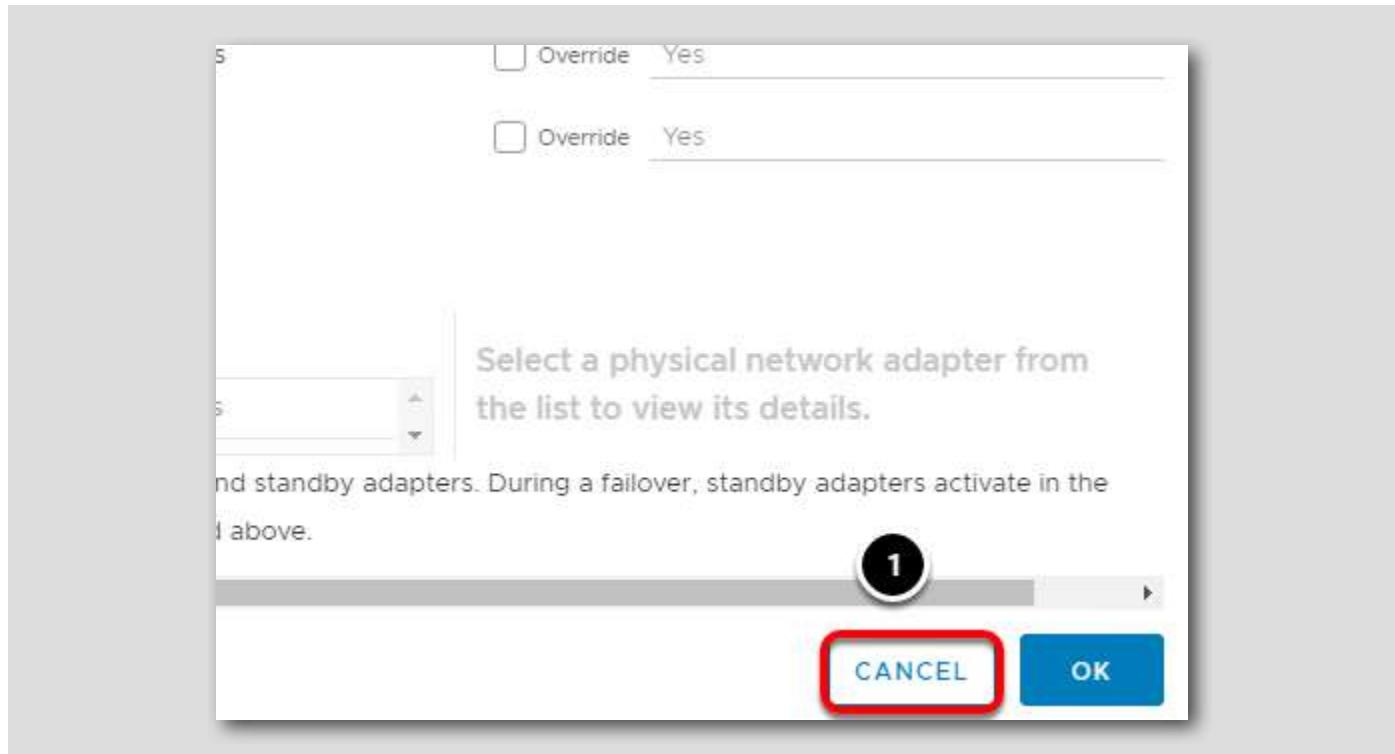
Failover - specifies whether a physical adapter is returned to active status after recovering from a failure.

- If failback is set to Yes, the default selection, the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any.
- If failback is set to No for a standard port, a failed adapter is left inactive after recovery until another currently active adapter fails and must be replaced.

You can also override the default virtual switch setting for the Failover order of the physical adapters.

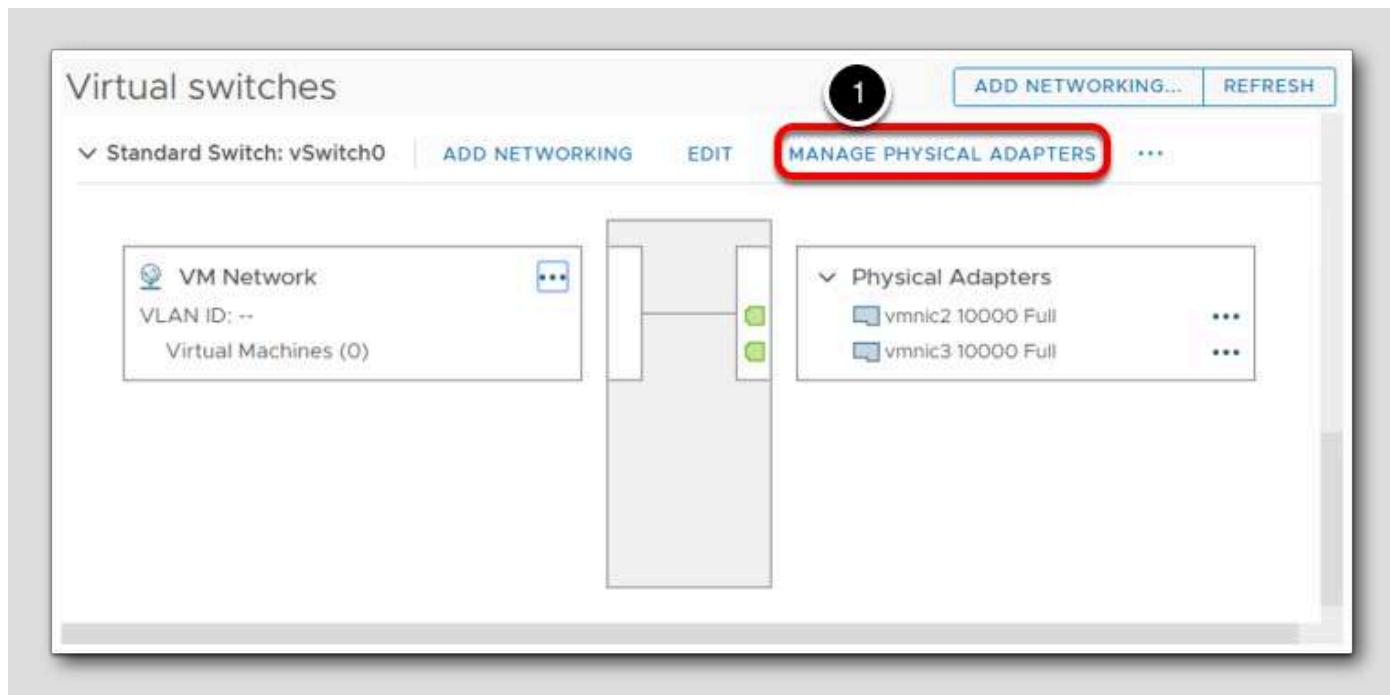
No changes are needed here and you may proceed to the next step.

Cancel the Changes



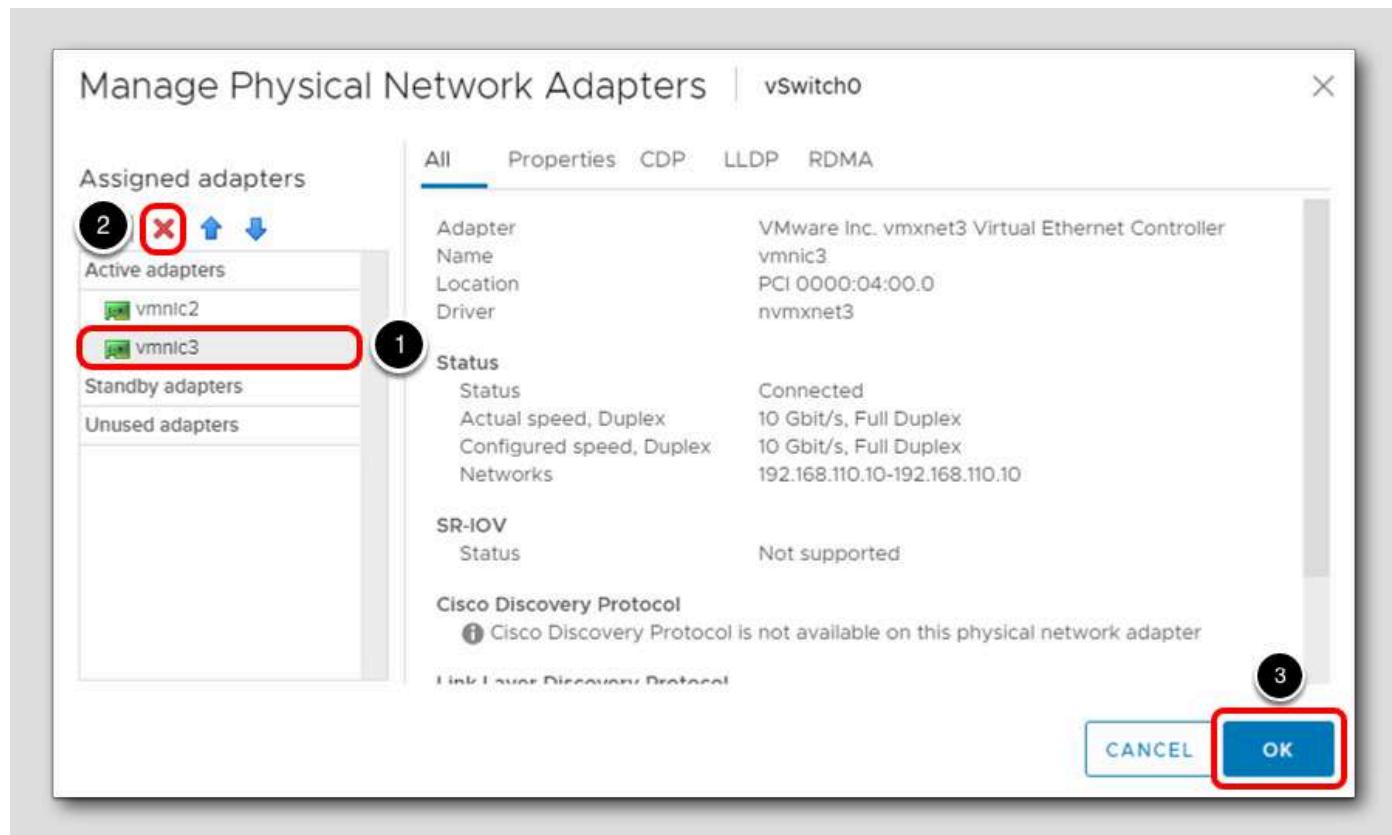
Since we don't want to make any changes to the port group, click the Cancel button.

Removing a Physical Adapter



1. Click Manager Physical Adapters for vSwitch0.

Remove vmnic3



1. Click on vmnic3.
2. Click the red 'X' to remove the adapter from the switch.
3. Click OK.

Adapter Removed

[258]

The screenshot shows the 'Virtual switches' interface in the vSphere Web Client. On the left, there's a tree view with 'VM Network' selected. In the center, there's a network diagram. On the right, under 'Physical Adapters', a list shows 'vmnic2 10000 Full'. A red box highlights this list.

1. The adapter, vmnic3 has been removed from the list of physical adapters.

Clear Alerts

[259]

The screenshot shows the 'Summary' tab for the host 'esx-01a.corp.local'. At the top, there are tabs for Summary (highlighted with a red box), Monitor, Configure, Permissions, VMs, Datastores, Networks, and Updates. Below the tabs, there's a summary table and resource usage charts. At the bottom, a red box highlights a warning message: 'Network uplink redundancy lost'. To the right of the message, there are 'Acknowledge' and 'Reset To Green' buttons, with the 'Reset To Green' button highlighted by a red box.

Since vmnic3 was removed from vSwitch0, you may receive an alert that network connectivity and/or redundancy has been lost.

1. To view these alerts, click on the Summary tab.
2. Click n Reset To Green to clear each alert.

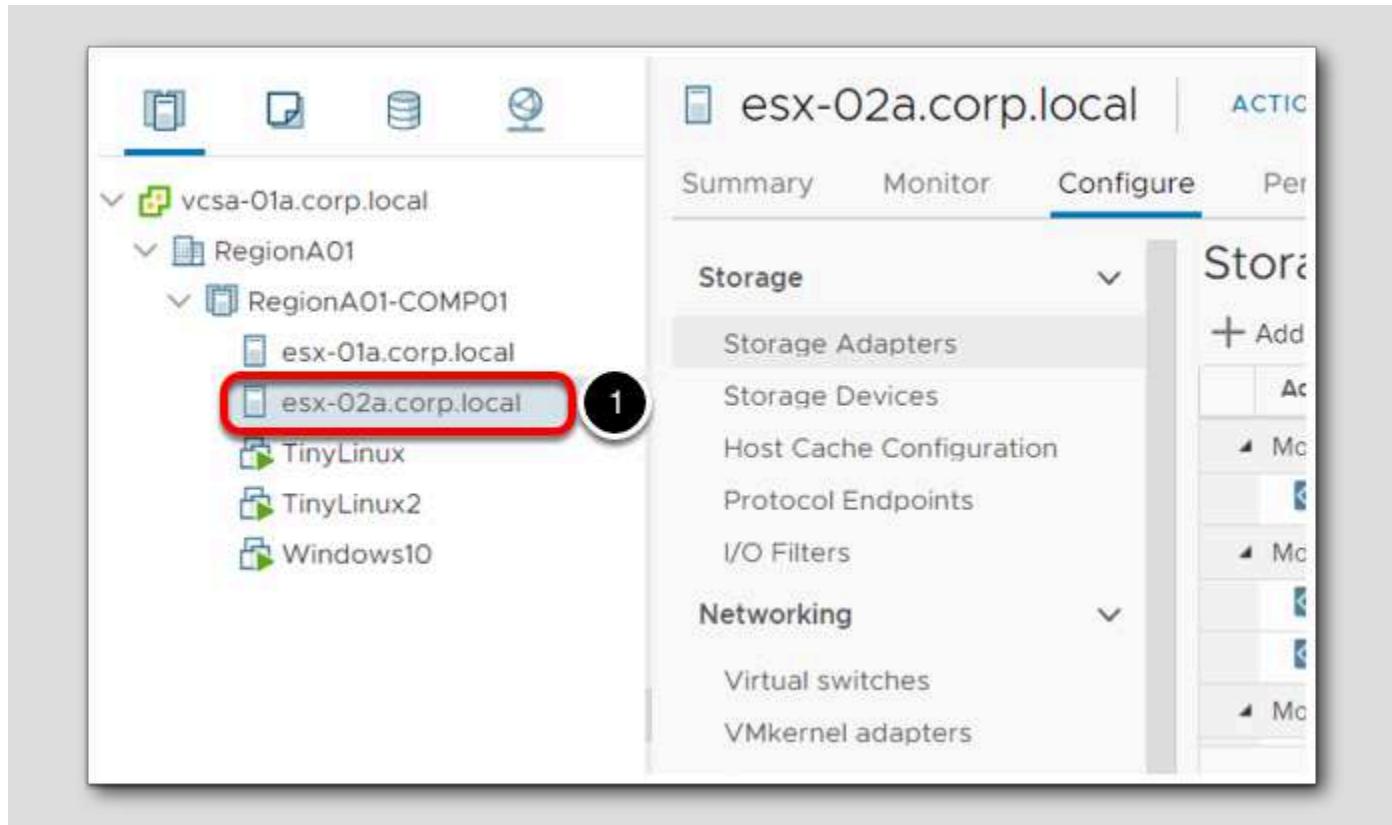
The screenshot shows the vSphere Client interface. The left sidebar displays a tree structure of hosts and clusters under 'vcsa-01a.corp.local'. The 'RegionA01-COMP01' cluster is expanded, showing hosts 'esx-01a.corp.local', 'esx-02a.corp.local', and several VMs: 'app-serv01', 'TinyLinux', 'TinyLinux2', and 'Windows10'. The 'esx-01a.corp.local' host is selected and highlighted with a blue border. The right panel is the 'Summary' tab for this host. It includes a summary card with the host's name, a server icon, and various status metrics. Below the card is a table of detailed information:

	Value	
Hypervisor:	VMware ESXi, 7.0.1	
Model:	VMware Virtual Plat	
Processor Type:	Intel(R) Xeon(R) CP	
Logical Processors:	2	
NICs:	4	
Virtual Machines:	2	
State:	Connected	
Uptime:	2 hours	

Below the table is a small 'Reset To Green' button icon.

You should no longer see the red exclamation point next to esx-01a.corp.local.

Deleting a Standard Switch



1. Click on esx-02a.corp.local

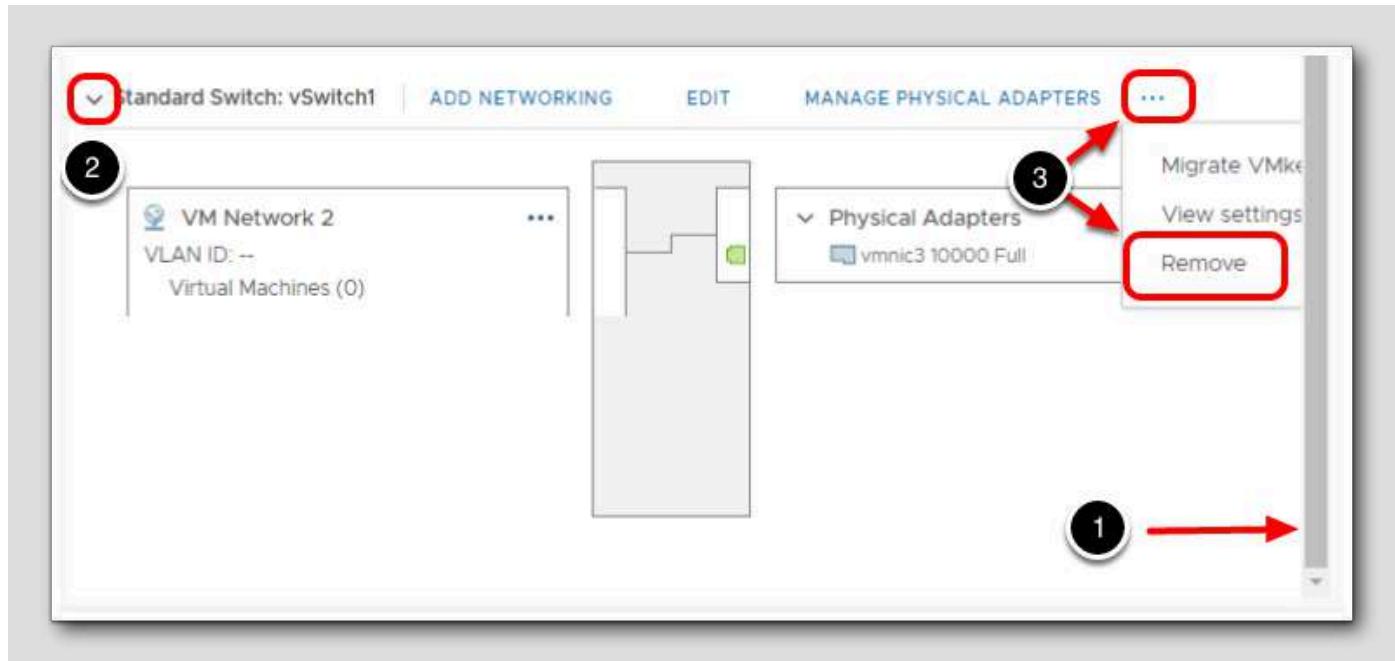
Virtual Switches



In preparation for the next lesson, we will delete the Standard Switch we created on esx-02a.corp.local.

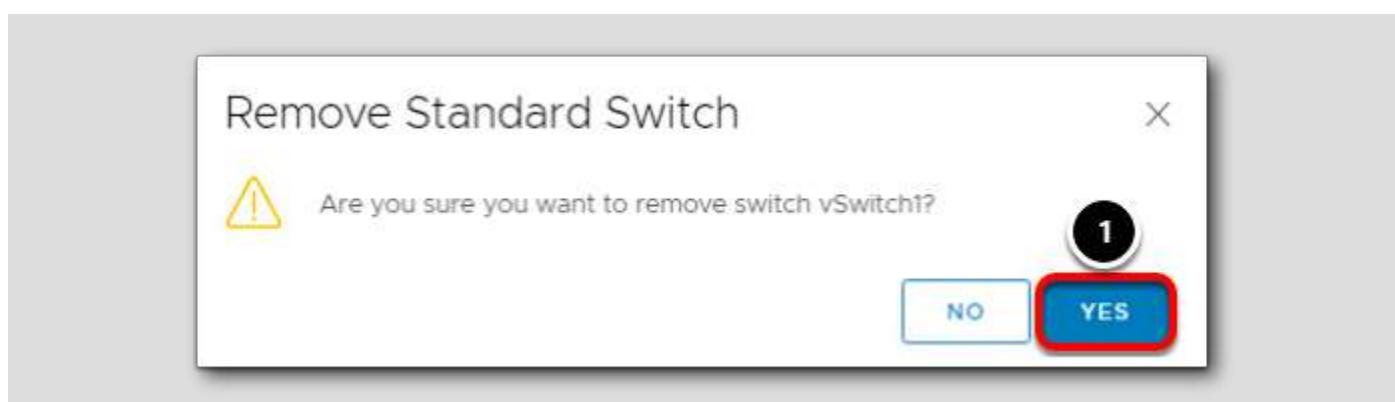
1. Click the Configure tab.
2. Select Virtual switches in the Networking section.

Standard Switch: vSwitch1



1. Scroll down until you see the Standard Switch: vSwitch1 section
2. Expand the section, if needed.
3. Click the '...' menu and select Remove

Remove Standard Switch



1. Click Yes to remove vSwitch1.

Conclusion

The vSphere Standard Switch is a simple virtual switch configured and managed at the host level. This switch provides access, traffic aggregation and fault tolerance by allowing multiple physical adapters to be bound to each virtual switch.

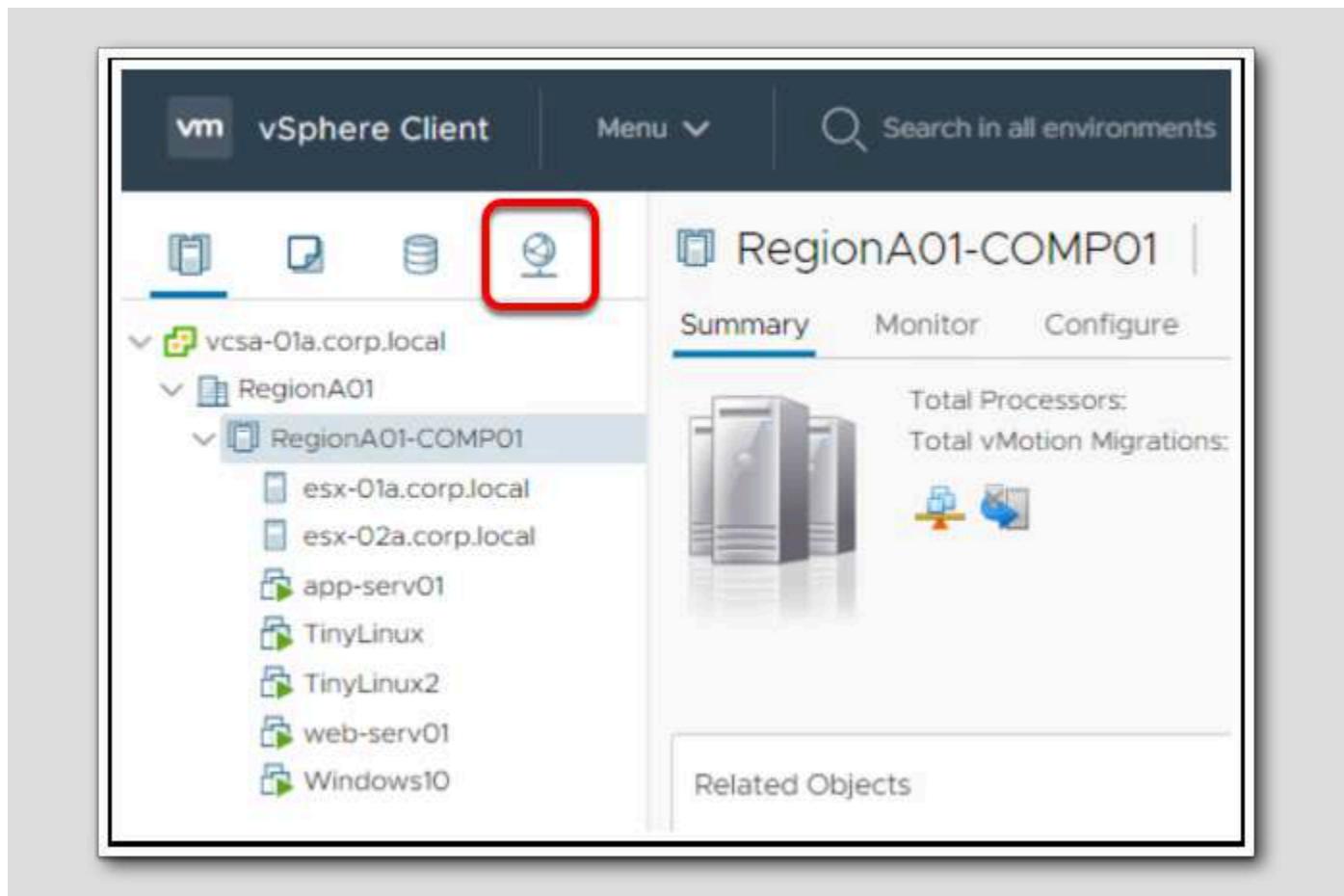
The VMWare vSphere Distributed Switch builds on the capabilities of the vSS and simplifies management in large deployments by appearing as a single switch spanning multiple associated hosts. This allows changes to be made once and propagated to every host that is a member of the switch.

Working with the vSphere Distributed Switch

Before we walk through the process of building our own Distributed vSwitch, let's take a minute to explore an existing vDS.

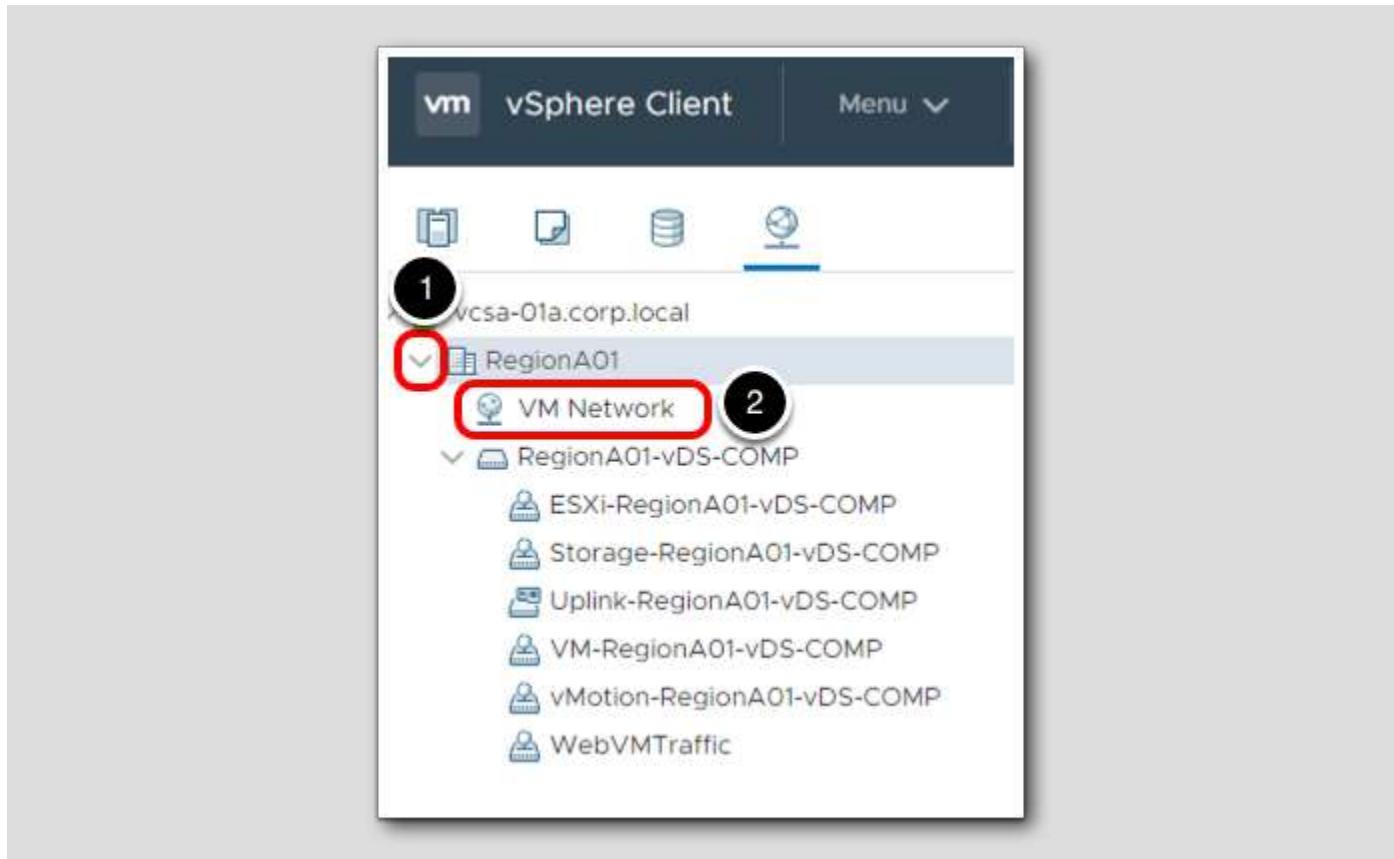
In this lab we will see how a Distributed vSwitch compares to a Standard vSwitch, how it is configured, and how it is connected to a running virtual machine.

Navigate to networking



1. Click on the Networking icon

View Standard vSwitch



1. Expand RegionA01
2. Select VM Network

VM Network

The screenshot shows the 'VM Network' interface in vSphere. At the top, there are tabs for 'Summary', 'Monitor', 'Permissions', 'Hosts', and 'VMs'. The 'VMs' tab is highlighted with a red box and has a circular badge with the number '1' next to it. Below the tabs, there are two buttons: 'Virtual Machines' (which is currently selected) and 'VM Templates'. The main area displays a table of virtual machines:

Name ↑	State	Status	Provisioned Space
app-serv01	Powered On	Normal	436.45 MB
TinyLinux2	Powered On	Normal	436.86 MB
web-serv01	Powered On	Normal	18.08 GB

1. Click on VMs tab

Take note of the virtual machines that are connected to this vSwitch. You should see a VM called TinyLinux2.

Note: You may see different results based on what lessons or modules you have already completed.

Hosts

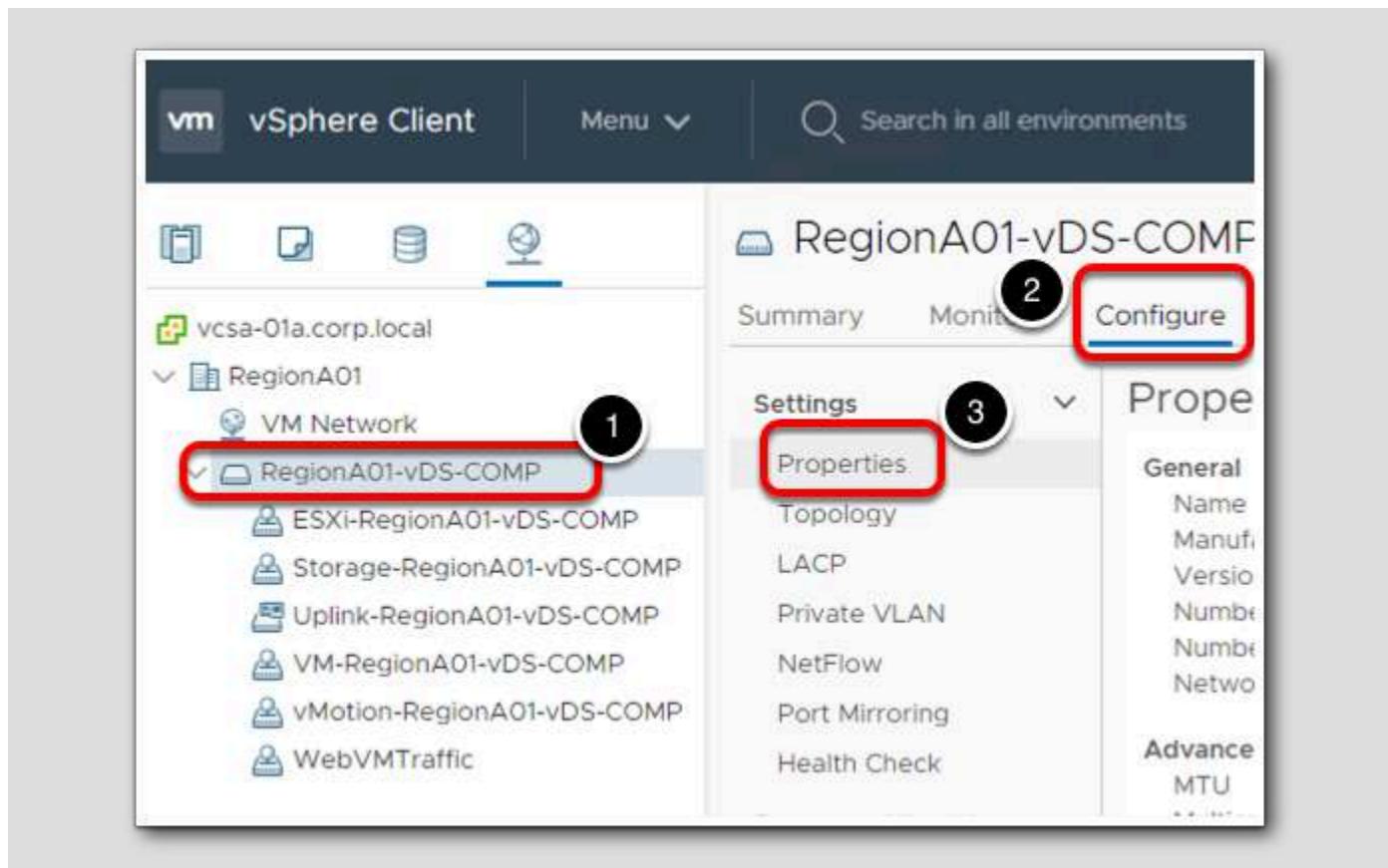
The screenshot shows the 'VM Network' interface in vSphere Web Client. At the top, there are tabs: 'Summary', 'Monitor', 'Permissions', 'Hosts' (which is highlighted with a red box and has a black circle with the number '1' above it), and 'VMs'. Below the tabs is a table with the following data:

Name	State	Status	Cluster
esx-01a.corp.local	Connected	Normal	RegionA01-CO...
esx-02a.corp.local	Connected	Normal	RegionA01-CO...

1. Click on Hosts tab

Take note of the hosts connected to the VM Network vSwitch. You should see esx-01a.corp.local and esx-02a.corp.local.

View Distributed Switch



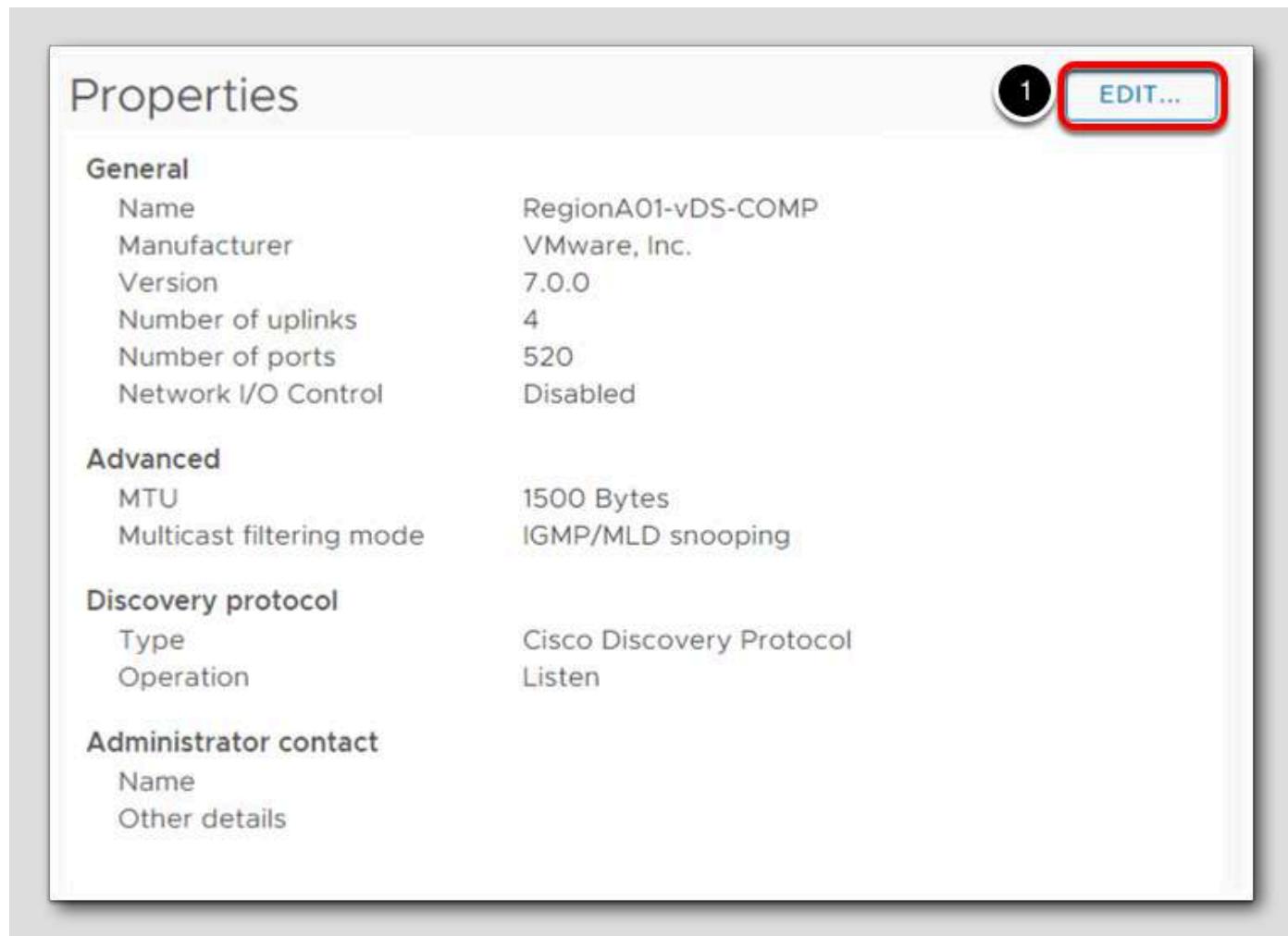
1. Click on RegionA01-vDS-COMP
2. Select the Configure tab
3. Select Properties

Review vDS configuration

General	
Name	RegionA01-vDS-COMP
Manufacturer	VMware, Inc.
Version	7.0.0
Number of uplinks	4
Number of ports	520
Network I/O Control	Disabled
Advanced	
MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping
Discovery protocol	
Type	Cisco Discovery Protocol
Operation	Listen
Administrator contact	
Name	
Other details	

Basic settings of Distributed Switch are displayed. Such as MTU settings, the version of the switch and discovery protocol being used.

Edit the switch properties



The screenshot shows the 'Properties' dialog box for a switch. At the top right, there is a circular icon with the number '1' and a blue 'EDIT...' button, which is highlighted with a red rectangular border. The dialog box contains several sections with configuration details:

General	
Name	RegionA01-vDS-COMP
Manufacturer	VMware, Inc.
Version	7.0.0
Number of uplinks	4
Number of ports	520
Network I/O Control	Disabled

Advanced	
MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

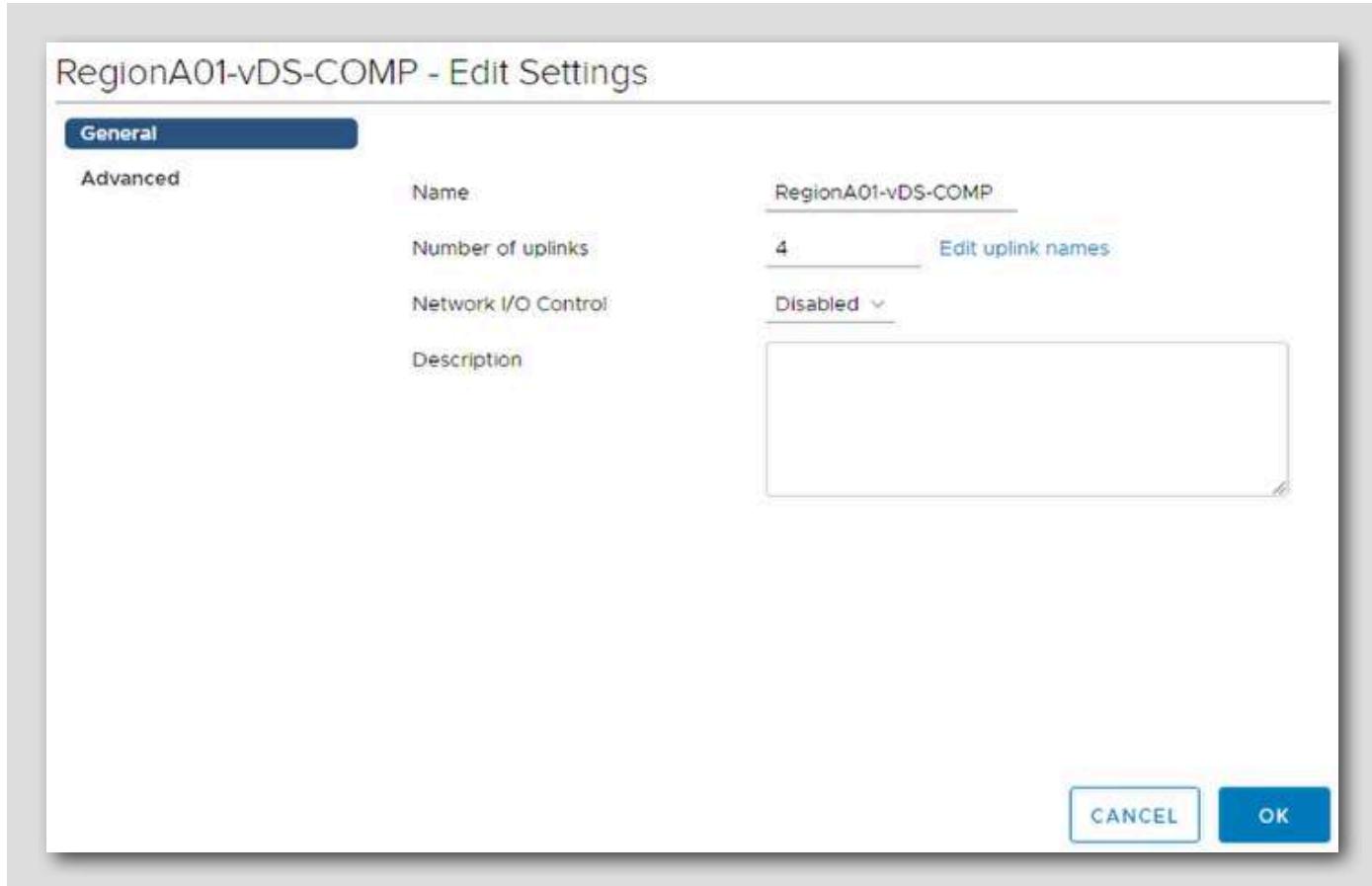
Discovery protocol	
Type	Cisco Discovery Protocol
Operation	Listen

Administrator contact	
Name	
Other details	

Next, we will explore the various properties of the switch.

1. Click Edit

General Settings



Click General to view the vSphere distributed switch settings. Here you can modify the following:

Name: You can modify the name of your distributed switch.

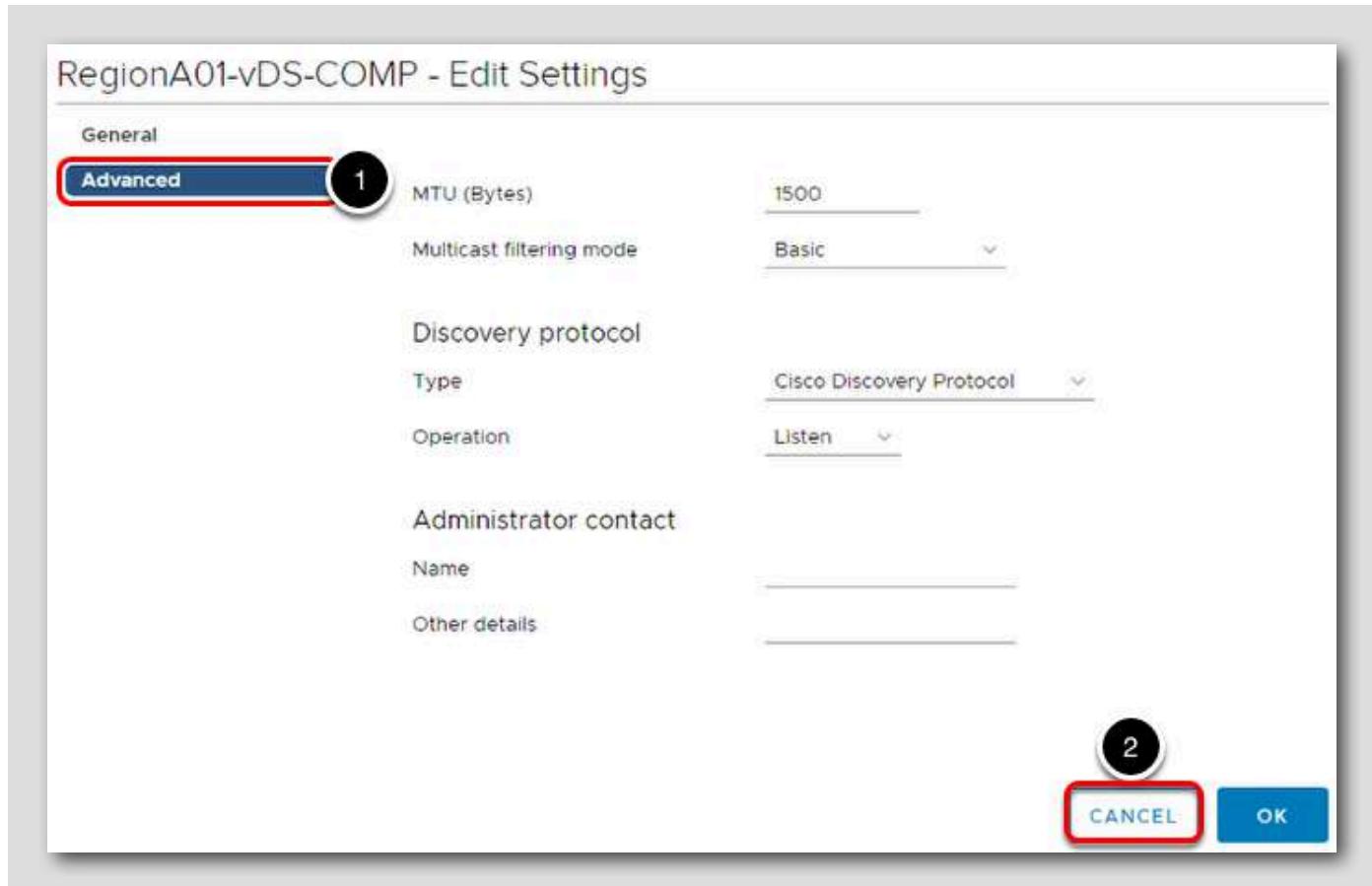
Number of Uplinks: Increase or decrease the number uplink ports attached to the distributed switch. Note that you can also click the Edit uplink names button to give the uplinks meaningful names.

Number of Ports: This setting cannot be modified. The port count will dynamically be scaled up or down by default.

Network I/O Control: You can use the drop-down menu to enable or disable Network I/O Control on the switch.

Description: You can use this field to give a meaningful description of the switch.

Advanced Settings



1. Click **Advanced** to view the vSphere distributed switch settings. Here you will find the following advanced settings for the switch:

MTU (Bytes): Maximum MTU size for the vSphere Distributed Switch. To enable jumbo frames, set a value greater than 1500 bytes. Make sure you check with your Networking team prior to modifying this setting in your environment.

Multicast filtering mode

- Basic - The distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group.
- IGMP/MLD snooping - The distributed switch forwards multicast traffic to virtual machines according to the IPv4 and IPv6 addresses of subscribed multicast groups by using membership messages defined by the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery protocol.

Discovery Protocol

- Type - Cisco Discovery Protocol, Link Layer Discovery Protocol, or disabled.
- Operation - to Listen, Advertise, or Both.

Administrator Contact: Type the name and other details of the administrator for the distributed switch.

2. We don't want to make any changes here, just click **Cancel**.

Enable or Disable vSphere Distributed Switch Health Check in the vSphere Web Client

The screenshot shows the vSphere Web Client interface for managing a vSphere Distributed Switch named "RegionA01-vDS-COMP". The "Configure" tab is active. On the left, a sidebar lists various configuration options: Properties, Topology, LACP, Private VLAN, NetFlow, Port Mirroring, and Health Check. The "Health Check" option is highlighted with a red box and a circled '1'. In the main pane, the "Health Check" section displays two items: "VLAN and MTU" and "Teaming and failover", both of which are currently set to "Disabled". In the top right corner of the main pane, there is an "EDIT..." button with a circled '2', indicating where to click to enable the health check.

The Distributed Switch Health Check monitors for changes in vSphere Distributed Switch configurations. You must enable vSphere Distributed Switch Health Check to perform checks on Distributed Switch configurations.

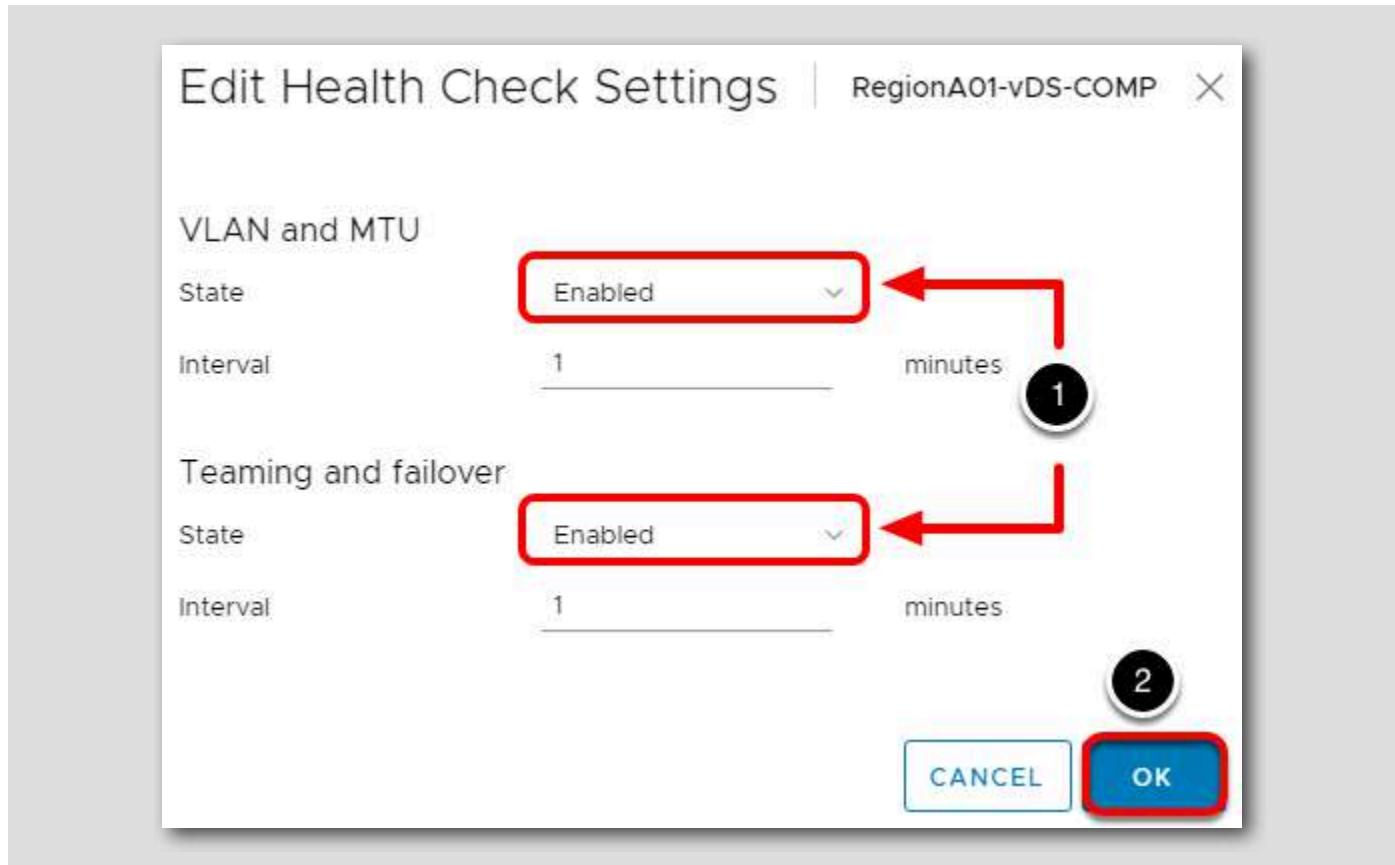
Health Check is available on ESXi 5.1 Distributed Switches and higher.

1. Click on the **Health check** tab for Distributed Switch

We can see that Health check is disabled for VLAN and MTU as well as Teaming and failover.

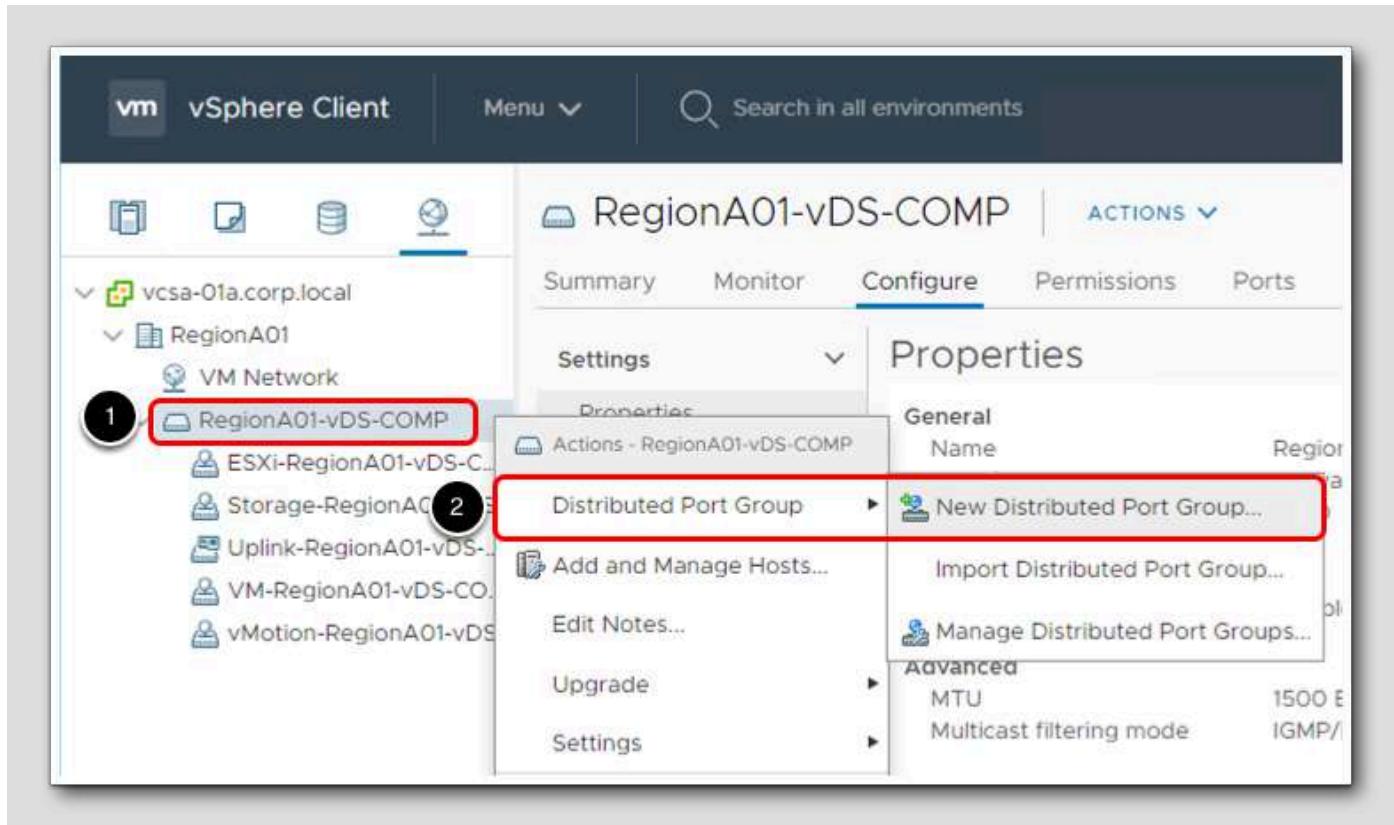
2. Click the **Edit** button

Edit Health Check Settings



1. Select Enabled for both and click OK
2. Click OK button

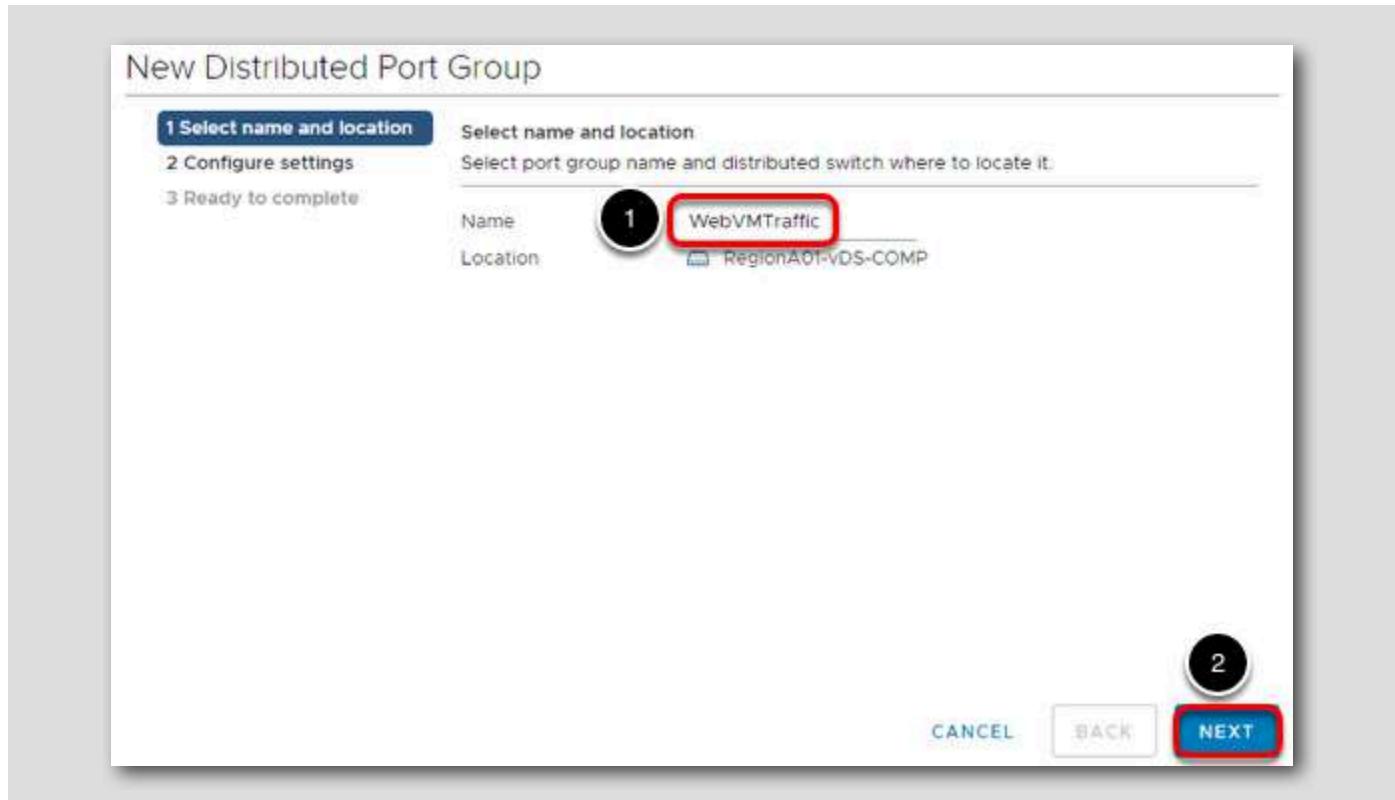
Distributed Port Groups



A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

1. Right-click RegionA01-vDS-COMP in the navigator
2. Select Distributed Port Group and then New Distributed Port Group...

Select name and location section



1. Name the new port group **WebVMTraffic**

2. Click **Next**

Configure settings

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

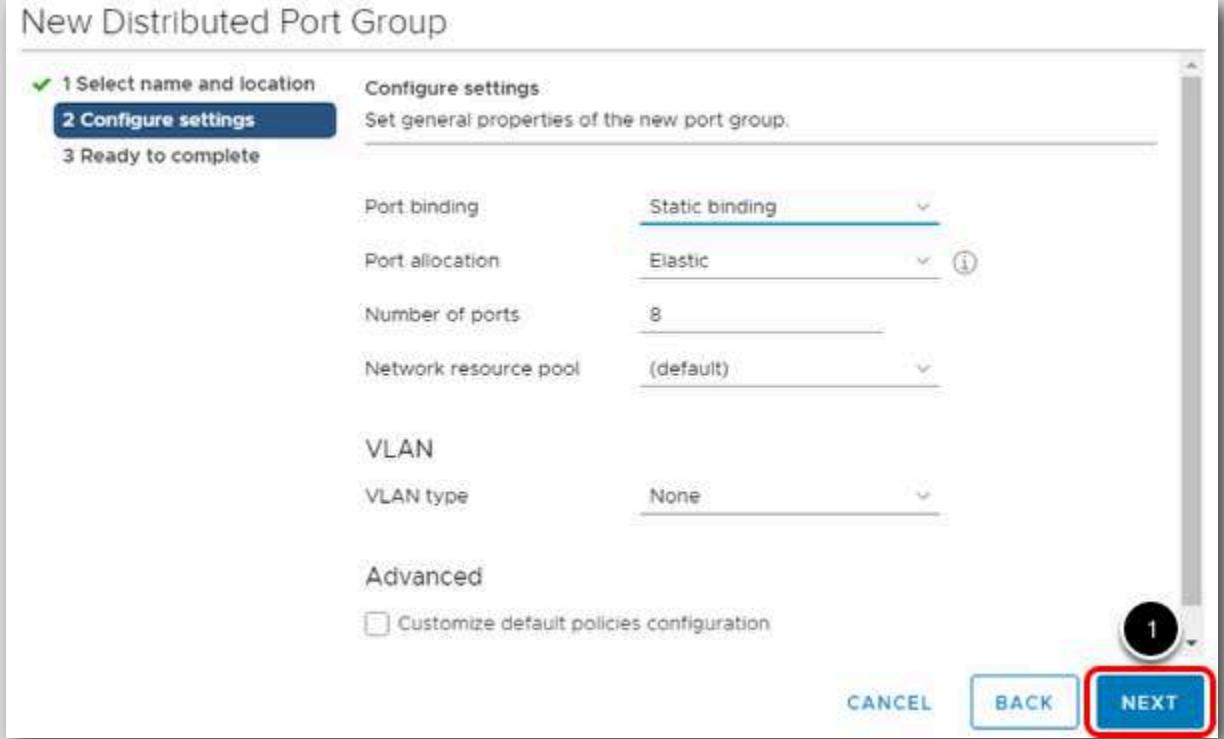
VLAN type	None
-----------	------

Advanced

Customize default policies configuration

1

CANCEL BACK NEXT



When creating a Distributed Port Group, you have the following options available:

Port binding - Choose when ports are assigned to virtual machines connected to this distributed port group.

- Static binding - Assign a port to a virtual machine when the virtual machine connects to the distributed port group.
- Ephemeral - No port binding. You can assign a virtual machine to a distributed port group with ephemeral port binding also when connected to the host.

Port allocation

- Elastic - The default number of ports is eight. When all ports are assigned, a new set of eight ports is created. This is the default.
- Fixed - The default number of ports is set to eight. No additional ports are created when all ports are assigned.

Number of ports: Enter the number of ports on the distributed port group.

Network resource pool: If you have created network pool to help control network traffic, you can select it here.

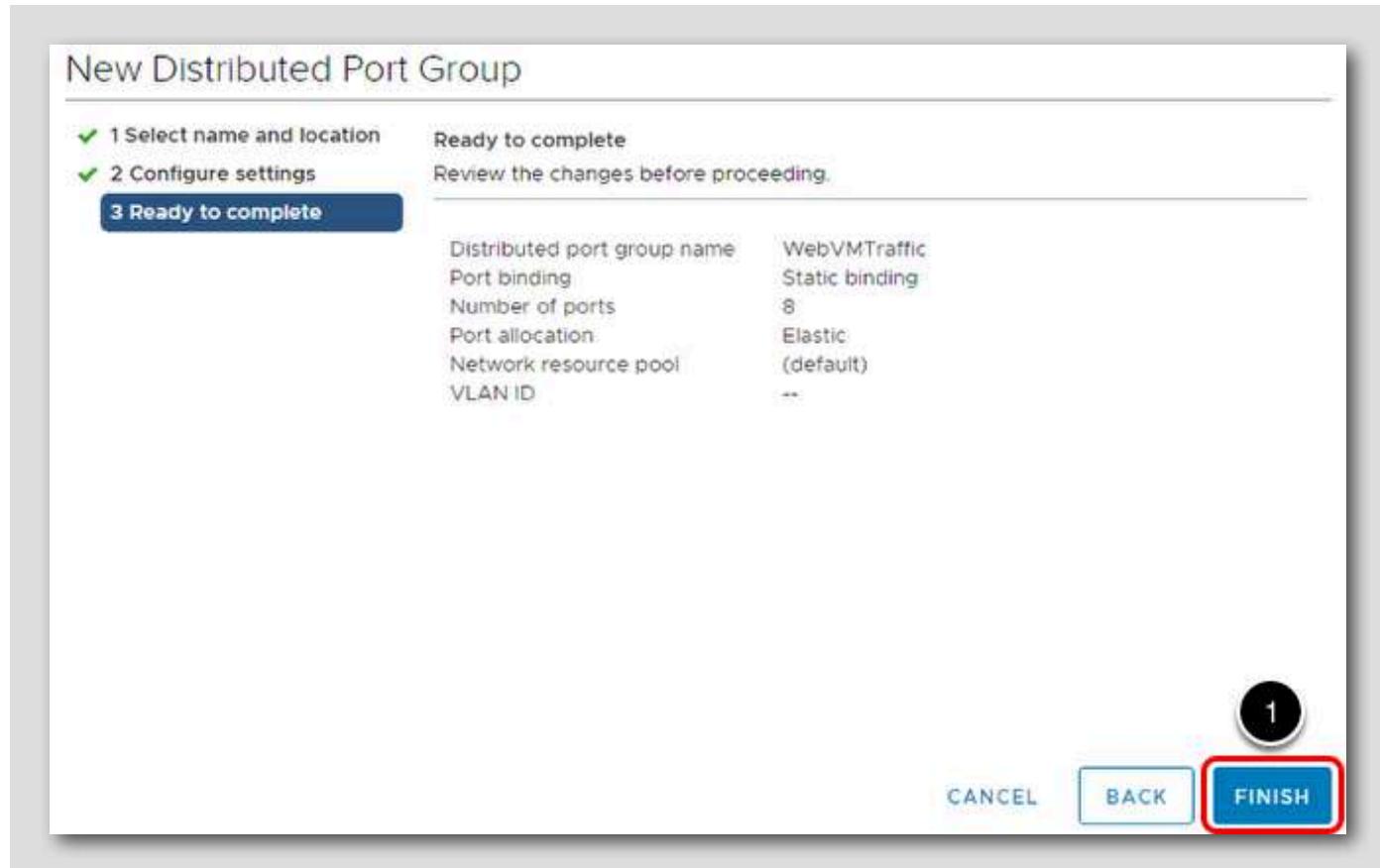
VLAN: Use the Type drop-down menu to select VLAN options:

- None - Do not use VLAN.
- VLAN - In the VLAN ID field, enter a number between 1 and 4094.
- VLAN Trunking - Enter a VLAN trunk range.
- Private VLAN - Select a private VLAN entry. If you did not create any private VLANs, this menu is empty.

Advanced: Select this check box to customize the policy configurations for the new distributed port group.

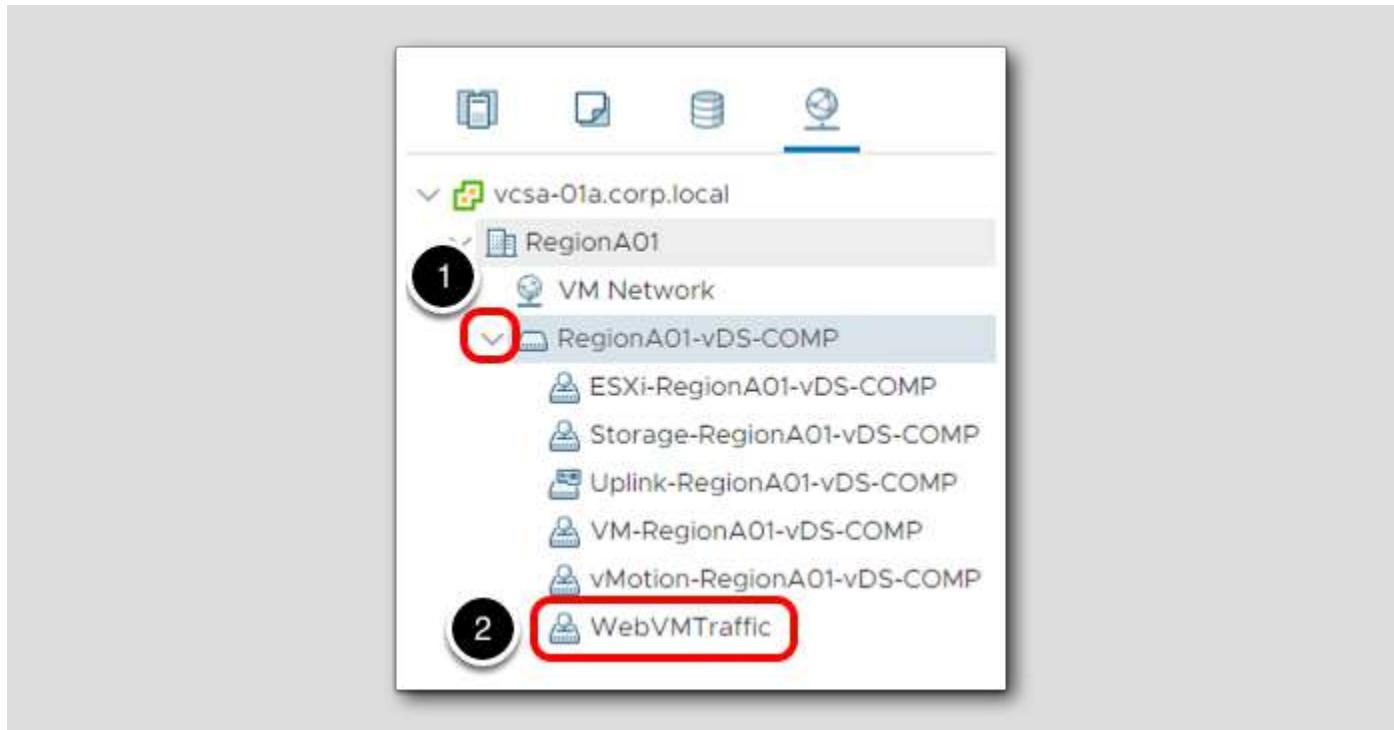
1. Just accept the defaults and click Next to continue.

Ready to complete



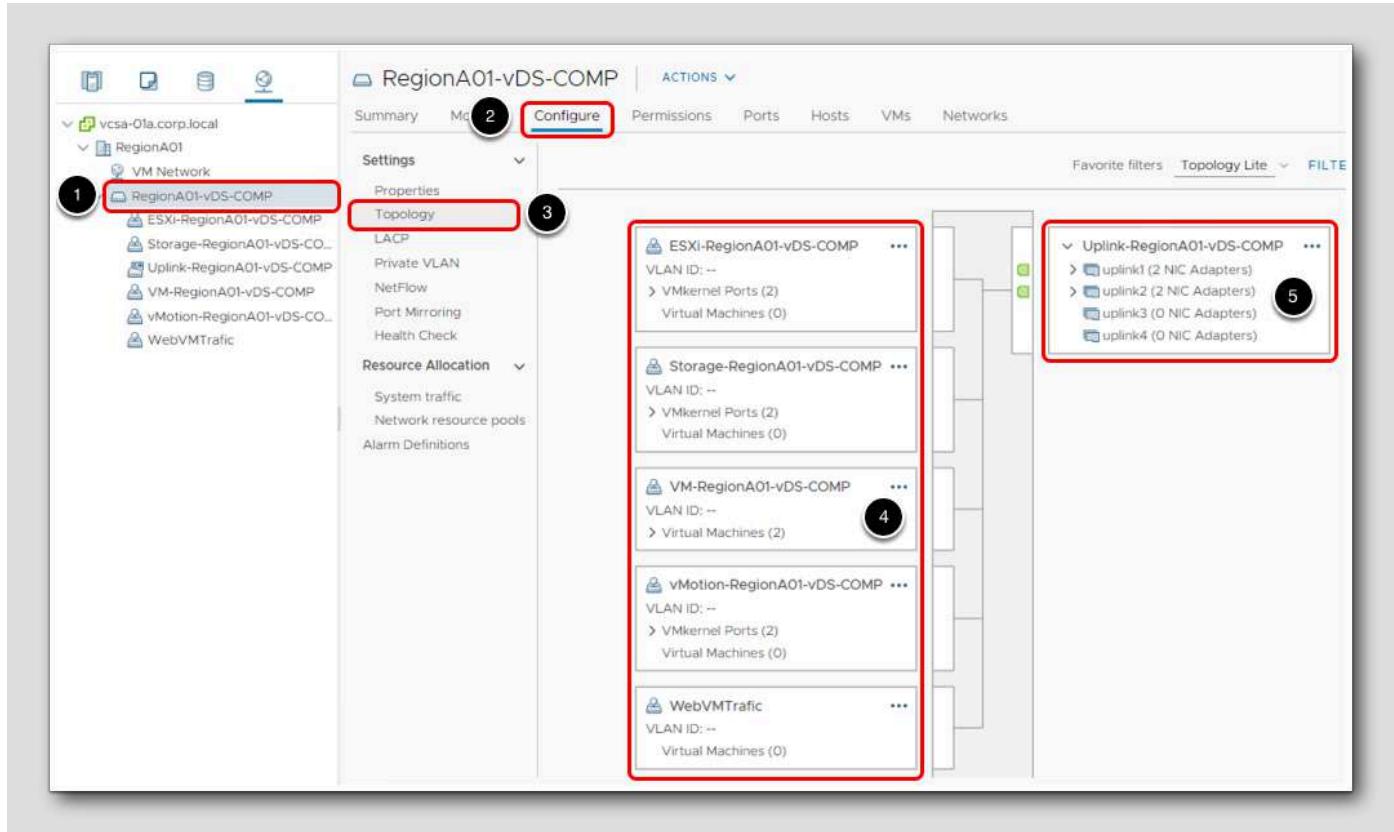
1. Review your settings and click Finish

View the new Distributed Port Group



1. In the Navigator, expand out RegionA01-vDS-COMP
2. The newly created WebVMTraffic Distributed Port Group has been created

Topology



1. Click on RegionA01-vDS-COMP
2. Select Configure
3. Click on Topology
4. On the left side of the diagram you will see the ports groups associated with the distributed switch RegionA01-vDS-COMP. These port groups are how the virtual machines and kernel ports are connected to the vDS. Note how there are VMkernel ports for Management, Storage and vMotion. This is very similar to the configuration you would see on a Standard vSwitch, except that these are defined and configured in one central location instead of individually at each host.
5. On the right you will see the uplinks associated with this vDS. These are used to connect the vDS directly to the physical NICs on the hosts that are tied to this Distributed vSwitch.

VM Port Group

RegionA01-vDS-COMP | ACTIONS ▾

Summary Monitor Configure Permissions Ports Hosts VMs

Settings Topology LACP Private VLAN NetFlow Port Mirroring Health Check Resource Allocation System traffic Network resource pools Alarm Definitions

Favorite filters

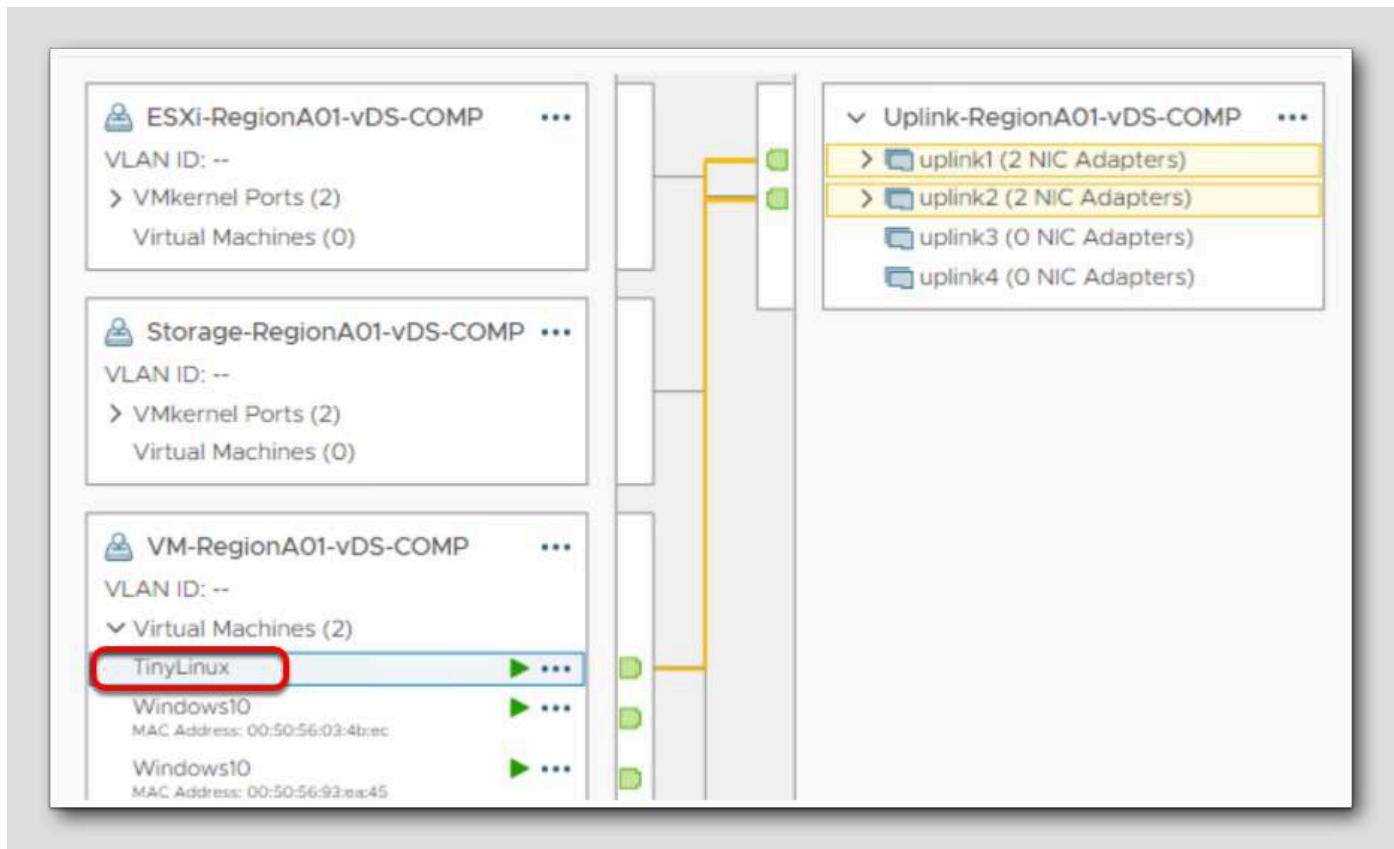
ESXi-RegionA01-vDS-COMP ... VLAN ID: -- VMkernel Ports (2) Virtual Machines (0)
Storage-RegionA01-vDS-COMP ... VLAN ID: -- VMkernel Ports (2) Virtual Machines (0)
VM-RegionA01-vDS-COMP ... VLAN ID: -- <input checked="" type="checkbox"/> Virtual Machines (2) TinyLinux Windows10 MAC Address: 00:50:56:03:4b:ec Windows10 MAC Address: 00:50:56:93:ea:45

1. Expand Virtual Machines on the VM-RegionA01-vDS-COMP port group

Again, note how there are virtual machines tied to this distributed port group just like you would see in a port group on a standard vSwitch.

Path to Uplinks

[284]



1. Click on **TinyLinux**

Note that a path to an uplink is drawn out and highlighted in orange to show the uplinks, hosts and vmnics it is associated with.

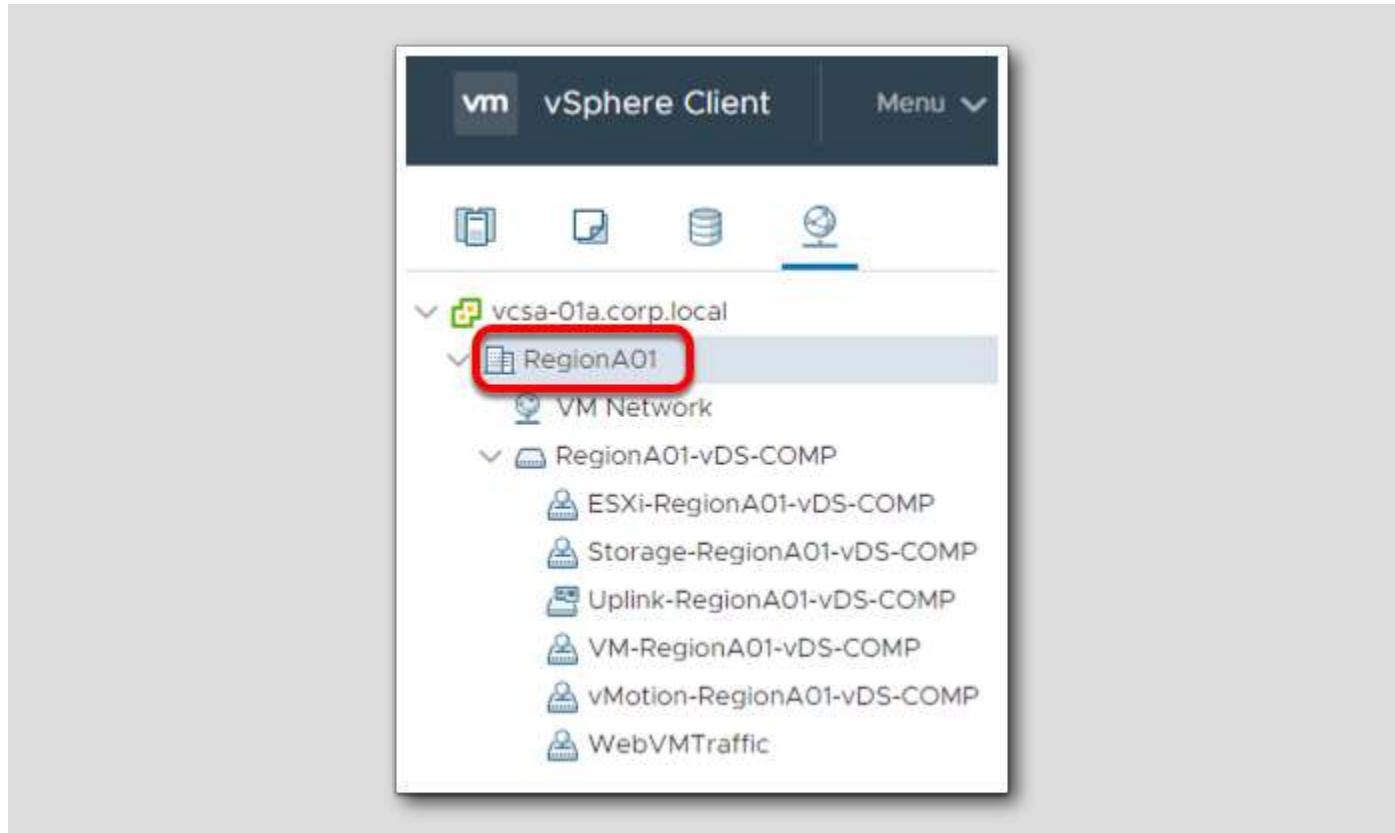
Creating a new Distributed Switch

[285]

Now that we have had a chance to explore an existing vDS, let's build one of our own.

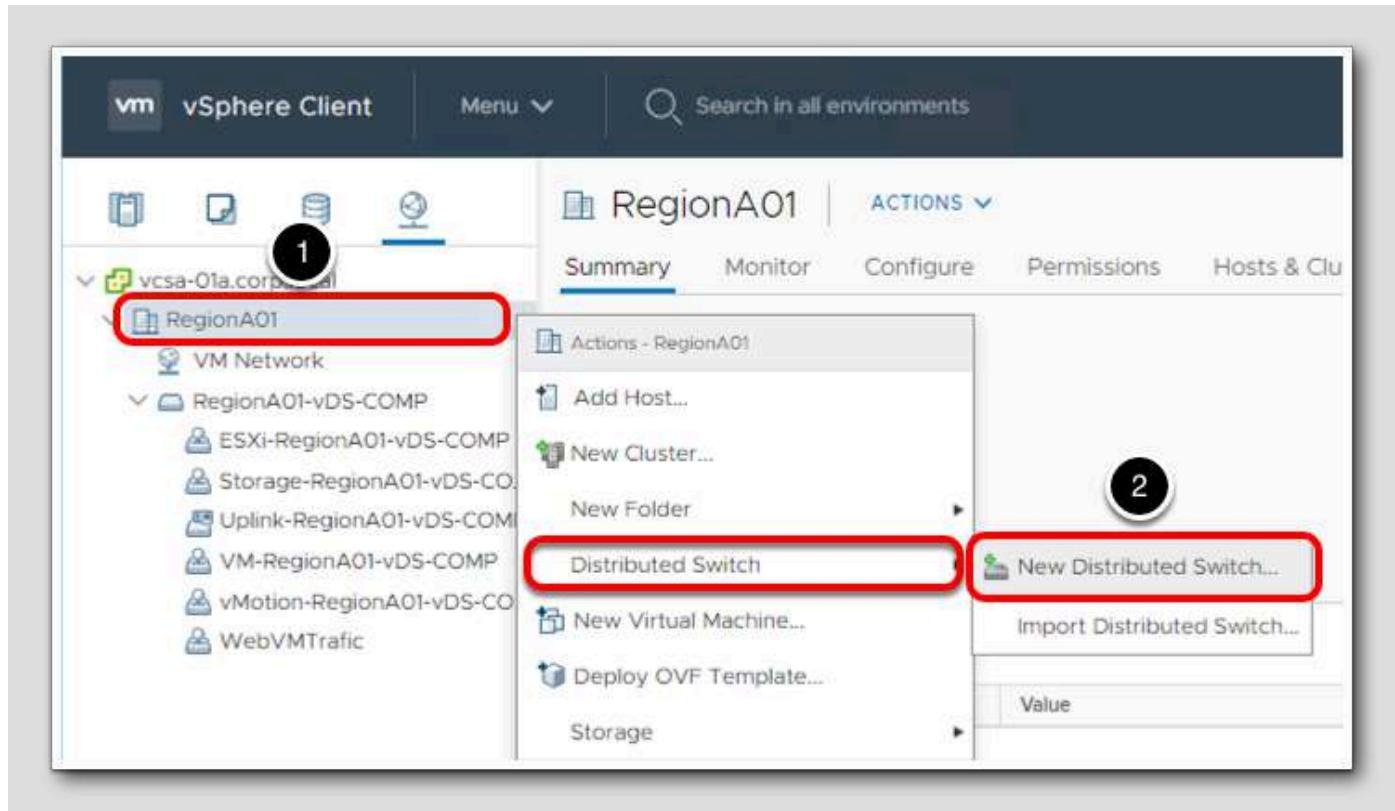
In this lab we will create a new Distributed vSwitch, add ESXi hosts to it, build port groups and connect them to uplinks so that we can use it to forward virtual machine traffic on to the physical network.

Navigate to RegionA01 Datacenter



1. In the vSphere Web Client, click on RegionA01

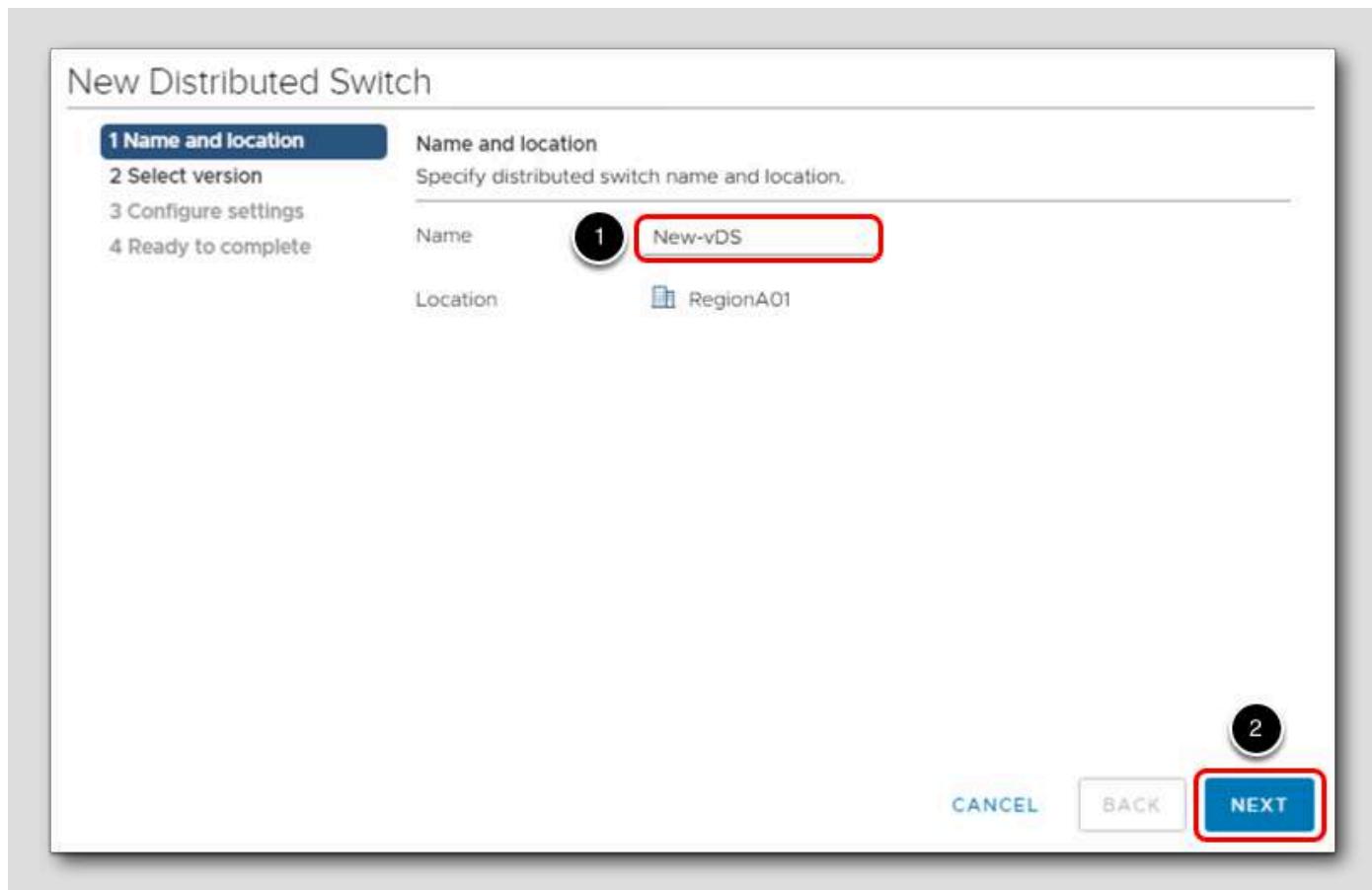
Create a new Distributed Switch



1. In the navigator, right-click the RegionA01
2. Select Distributed Switch and then New Distributed Switch

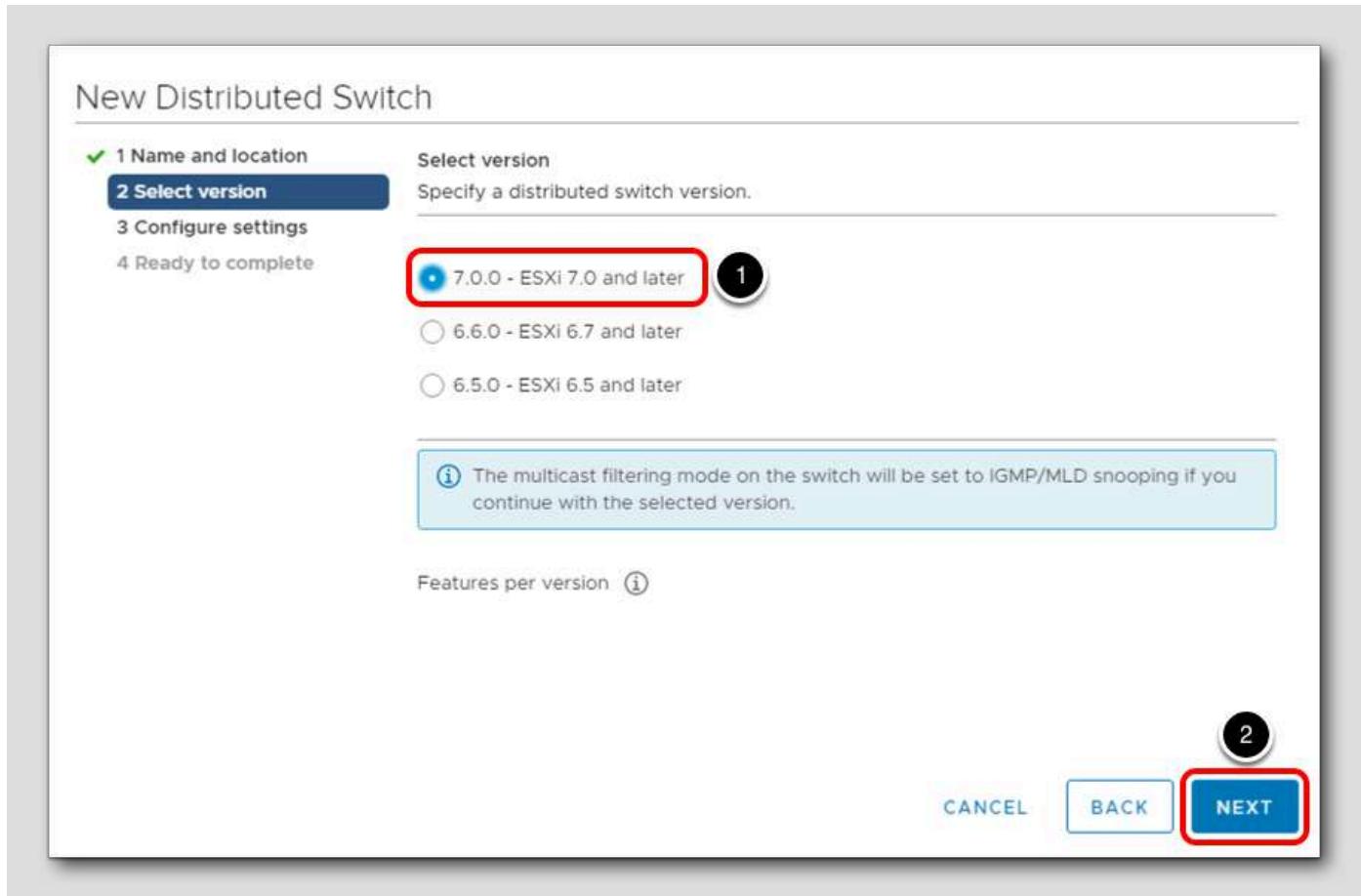
This will open the New Distributed Switch wizard.

Name the Distributed Switch



1. Type New-vDS in the Name field
2. Click Next

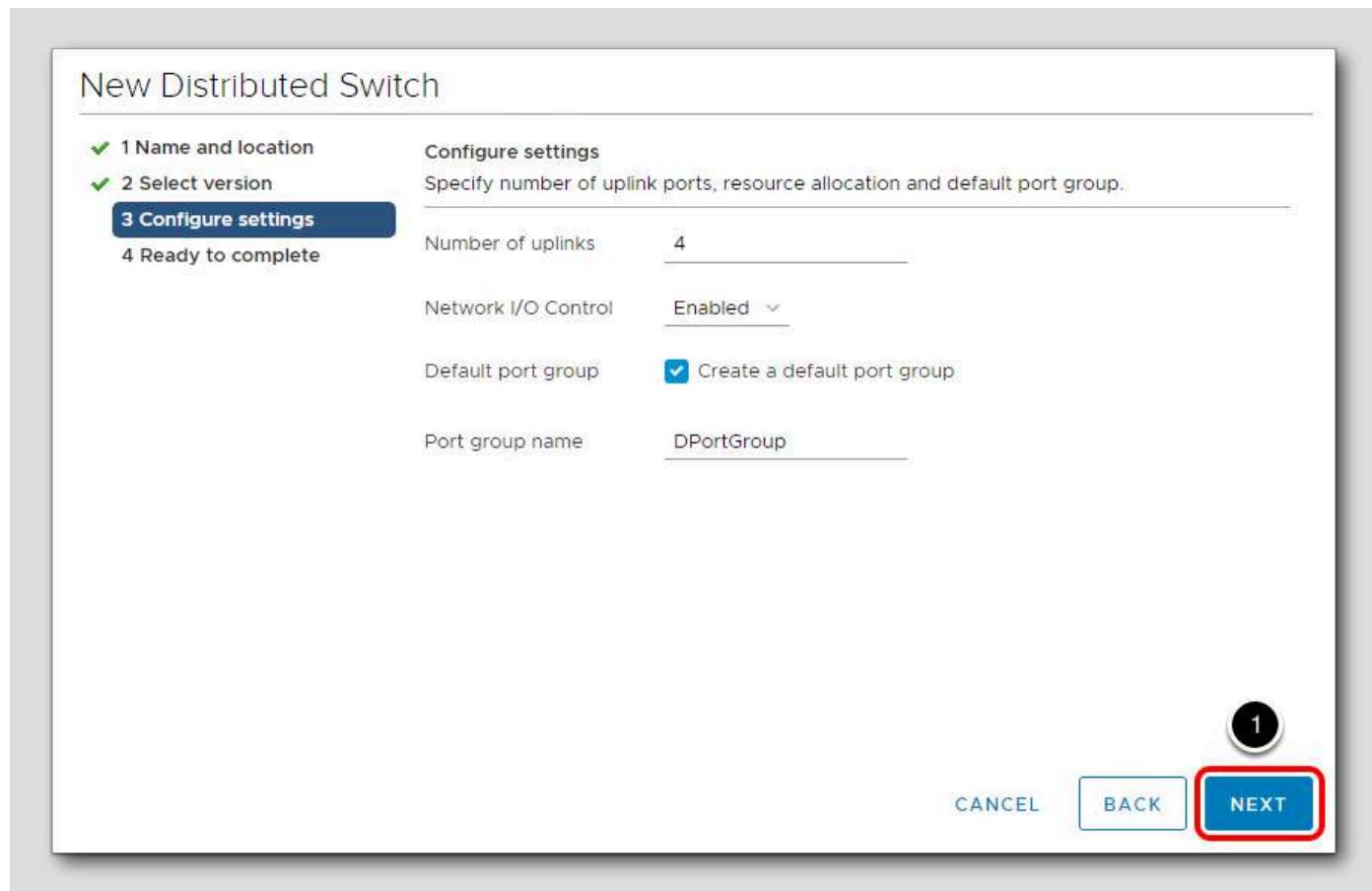
Select the version



1. Leave the default setting of 7.0.0 - ESXi 7.0 and later

2. Click **Next**

Configure settings



1. Leave the default options and click Next

Complete the build

New Distributed Switch

✓ 1 Name and location
✓ 2 Select version
✓ 3 Configure settings
4 Ready to complete

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

Name	New vDS
Version	7.0.0
Number of uplinks	4
Network I/O Control	Enabled
Default port group	DPortGroup

Suggested next actions

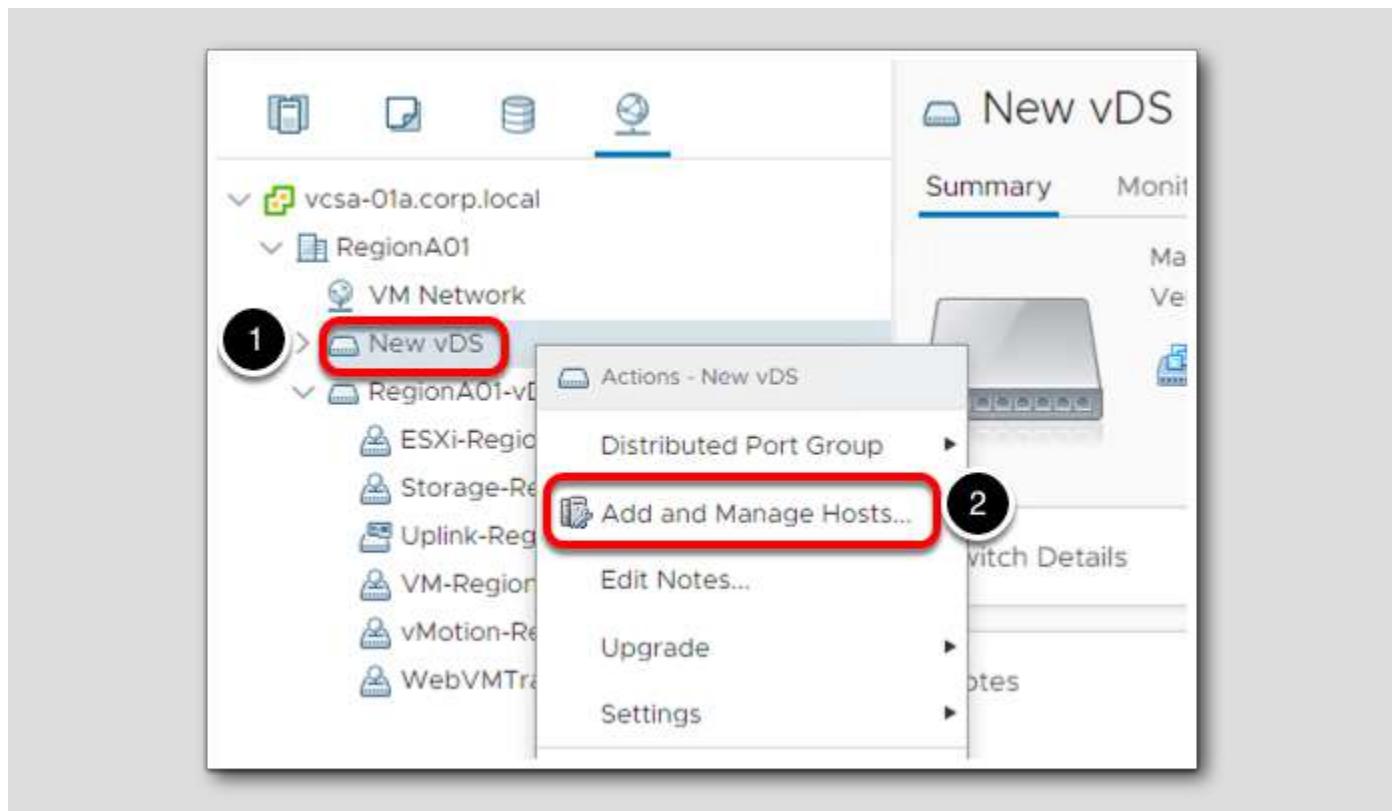
- New Distributed Port Group
- Add and Manage Hosts

ⓘ These actions will be available in the Actions menu of the new distributed switch.

1 CANCEL BACK FINISH

1. Review your settings and click Finish

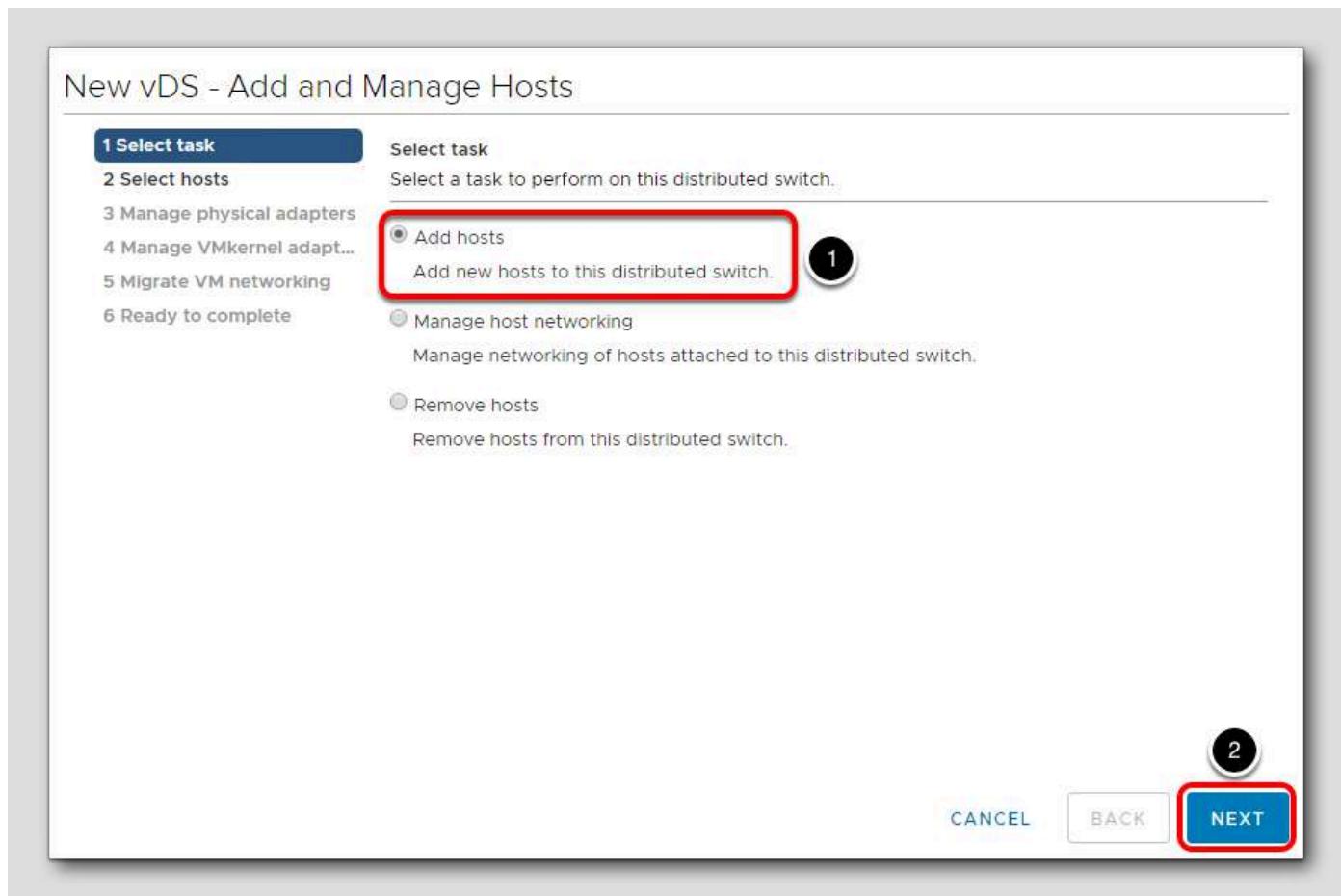
Add hosts to new Distributed Switch



1. Right-click on the newly created switch, **New vDS**

2. Select **Add and Manage Hosts**

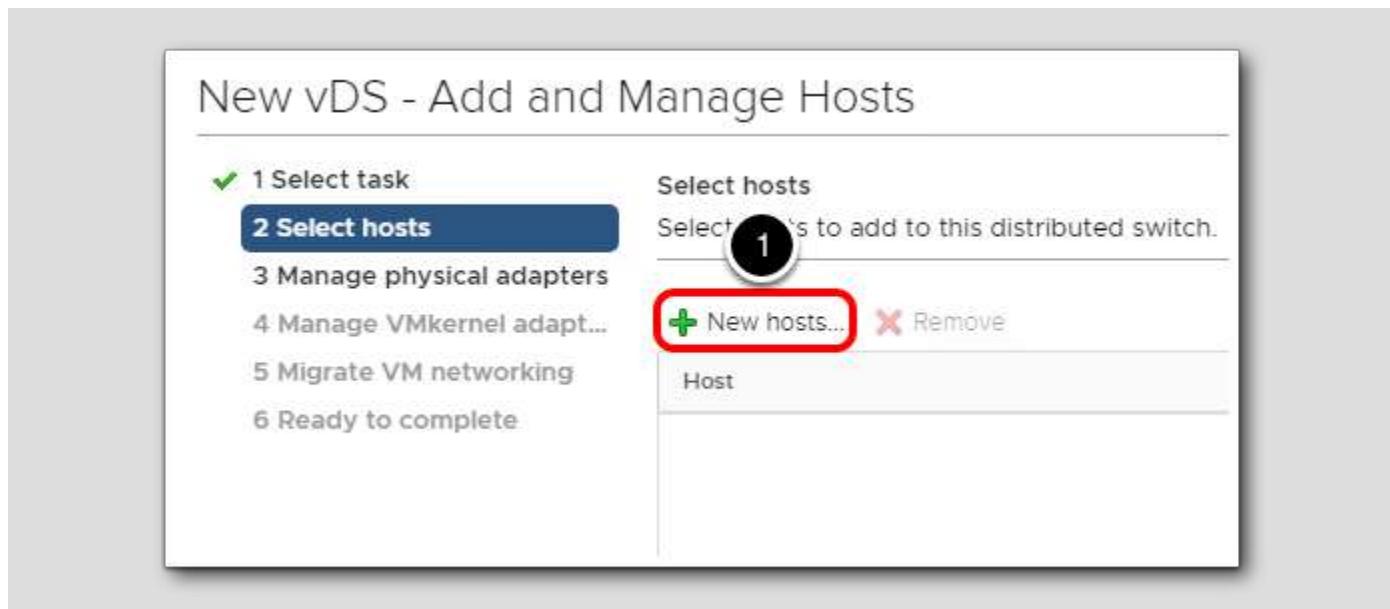
Select task



1. On the Select task page, select **Add hosts**

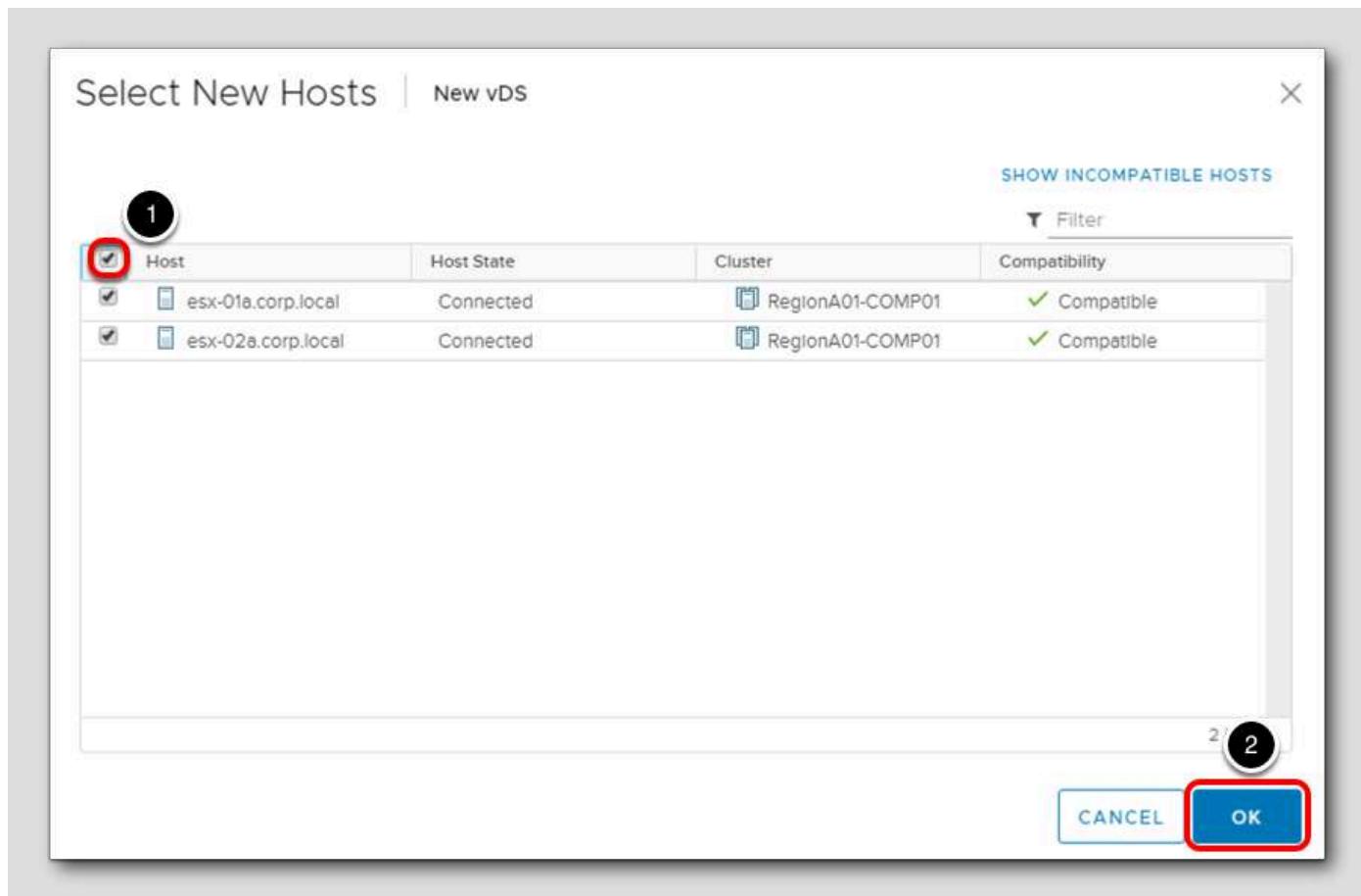
2. Click **Next**

Select hosts



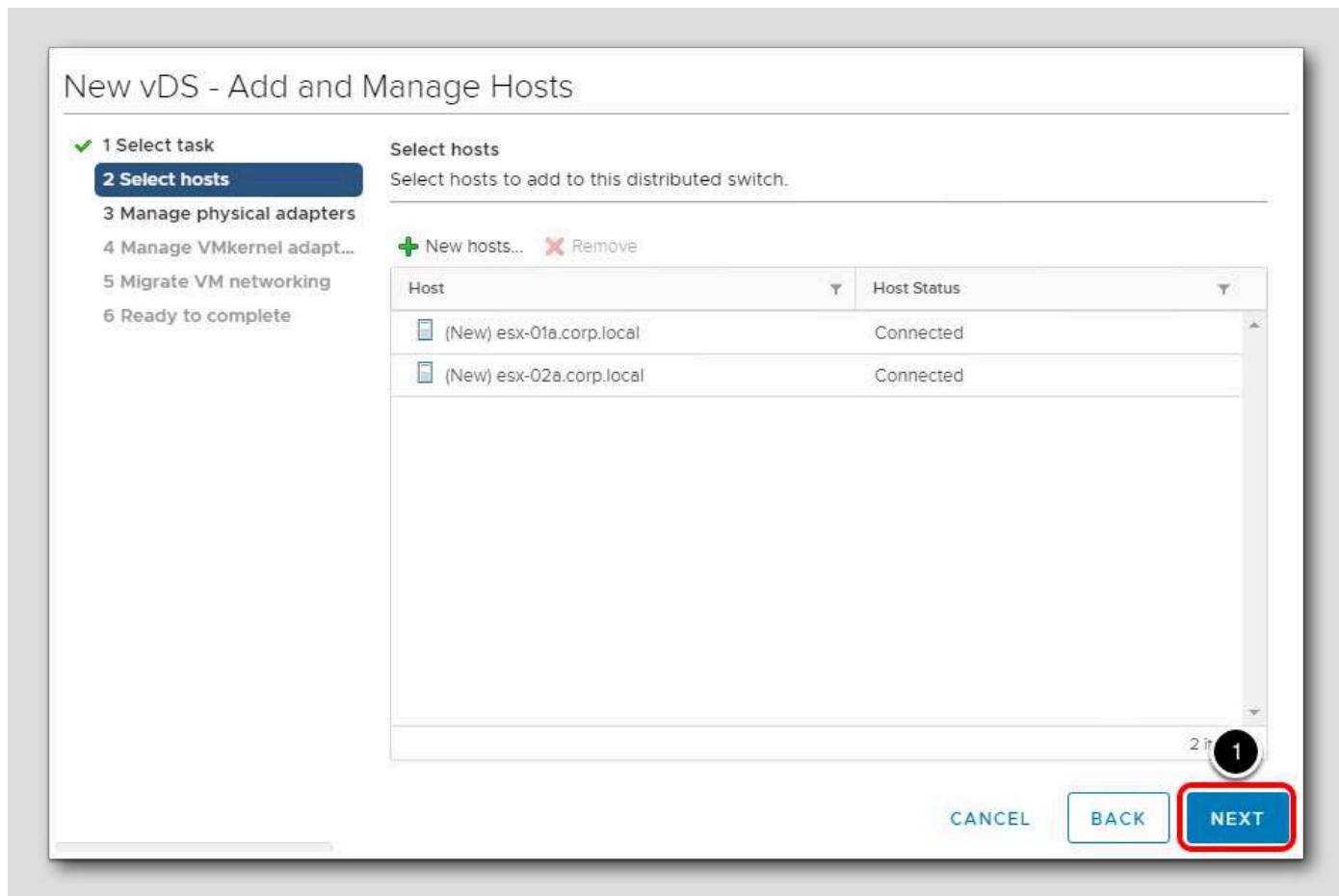
1. On the Select hosts page, click New hosts

Select New Hosts



1. Click the check box on the left to select both hosts in the datacenter
2. Click OK

Manage Hosts



1. Verify the two hosts are listed, then click **Next**

Assign physical adapters

New vDS - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Manage physical adapters
Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink
esx-01a.corp.local		
On this switch		
On other switches/unclaimed		
vmnic0	RegionA01-vDS-CO...	--
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--
vmnic3	--	--

Assign uplink **2** Assign adapter **1** View settings

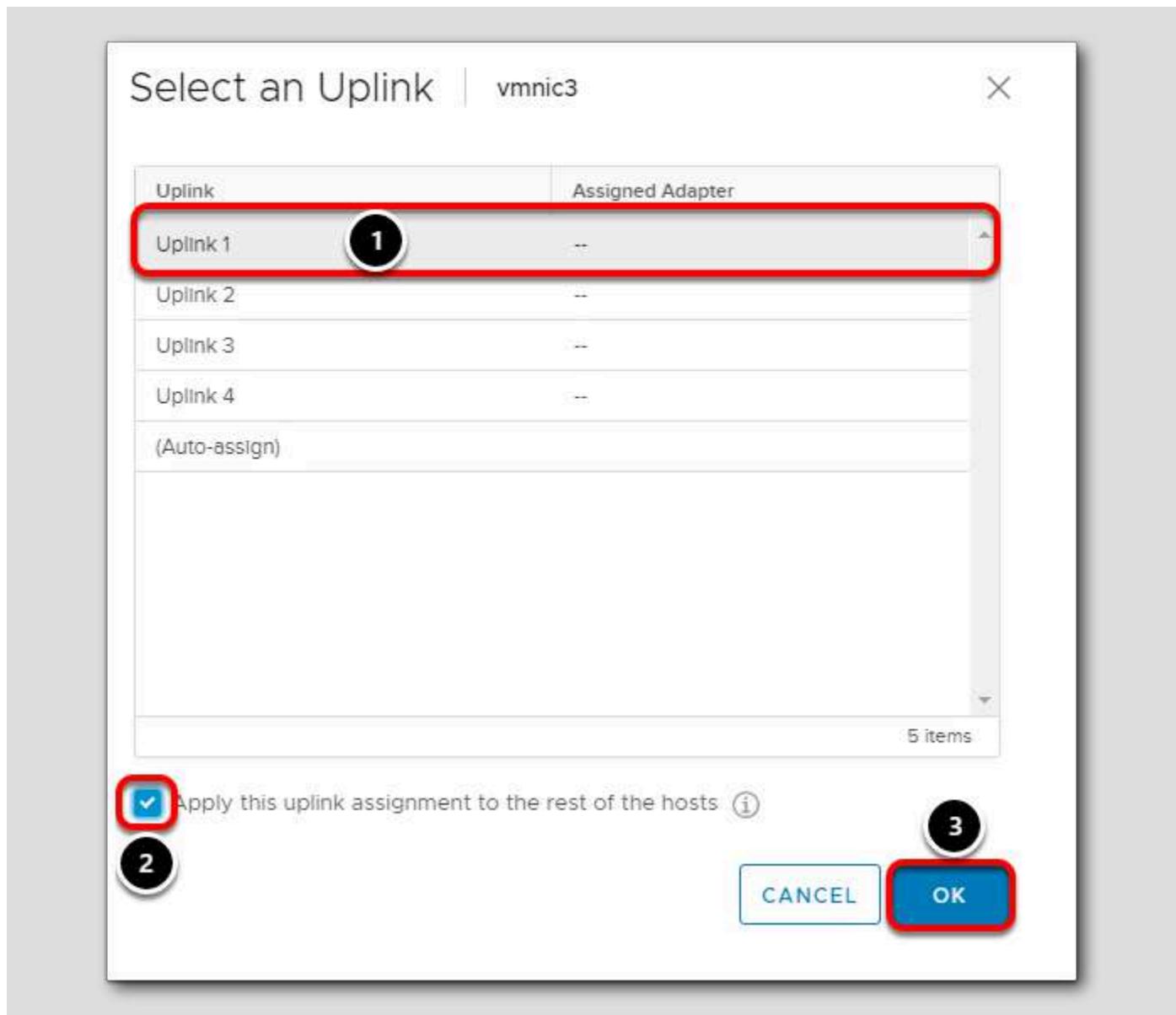
1. From the On other switches/unclaimed list, highlight vmnic3
2. Click Assign uplink



On the Manage physical network adapters page, we want to configure which physical NICs will be used on the distributed switch.

1. From the On other switches/unclaimed list, highlight vmnic3
2. Click Assign uplink

Assign uplinks to hosts



1. From the Select an Uplink page, select Uplink 1
2. Check the box next to Apply this uplink assignment to the rest of the hosts

This will automatically configure any other hosts that you are adding to this distributed switch with the same vmnic and uplink settings.

3. Click OK

Review settings

New vDS - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

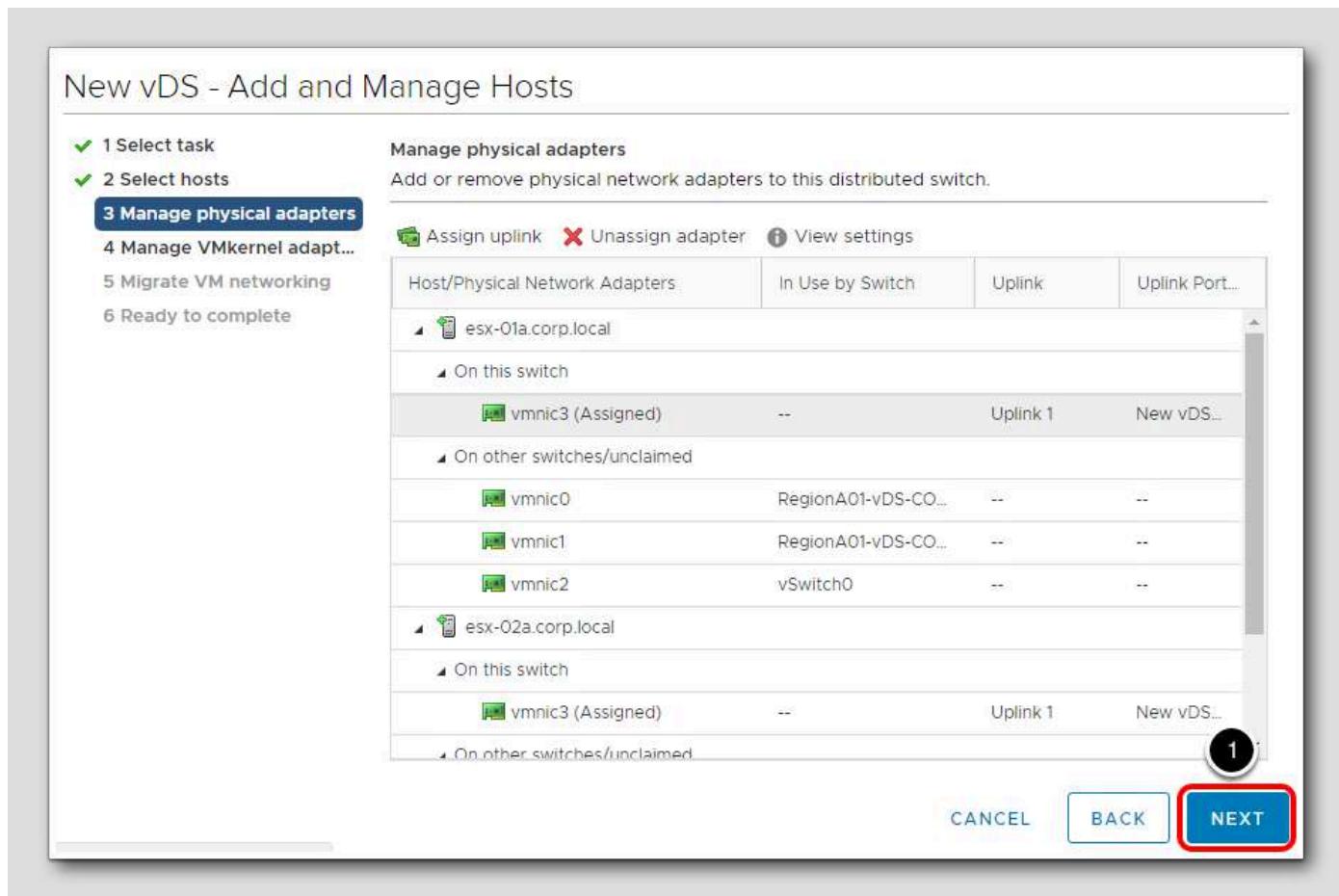
Manage physical adapters
Add or remove physical network adapters to this distributed switch.

Assign uplink Unassign adapter View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port...
esx-01a.corp.local			
On this switch			
vmnic3 (Assigned)	--	Uplink 1	New vDS...
On other switches/unclaimed			
vmnic0	RegionA01-vDS-CO...	--	--
vmnic1	RegionA01-vDS-CO...	--	--
vmnic2	vSwitch0	--	--
esx-02a.corp.local			
On this switch			
vmnic3 (Assigned)	--	Uplink 1	New vDS...
On other switches/unclaimed			

1

CANCEL BACK **NEXT**



1. Review vmnic and uplink settings for the hosts you are adding and click **Next**

Manage VMkernel adapters

New vDS - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
✓ 3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

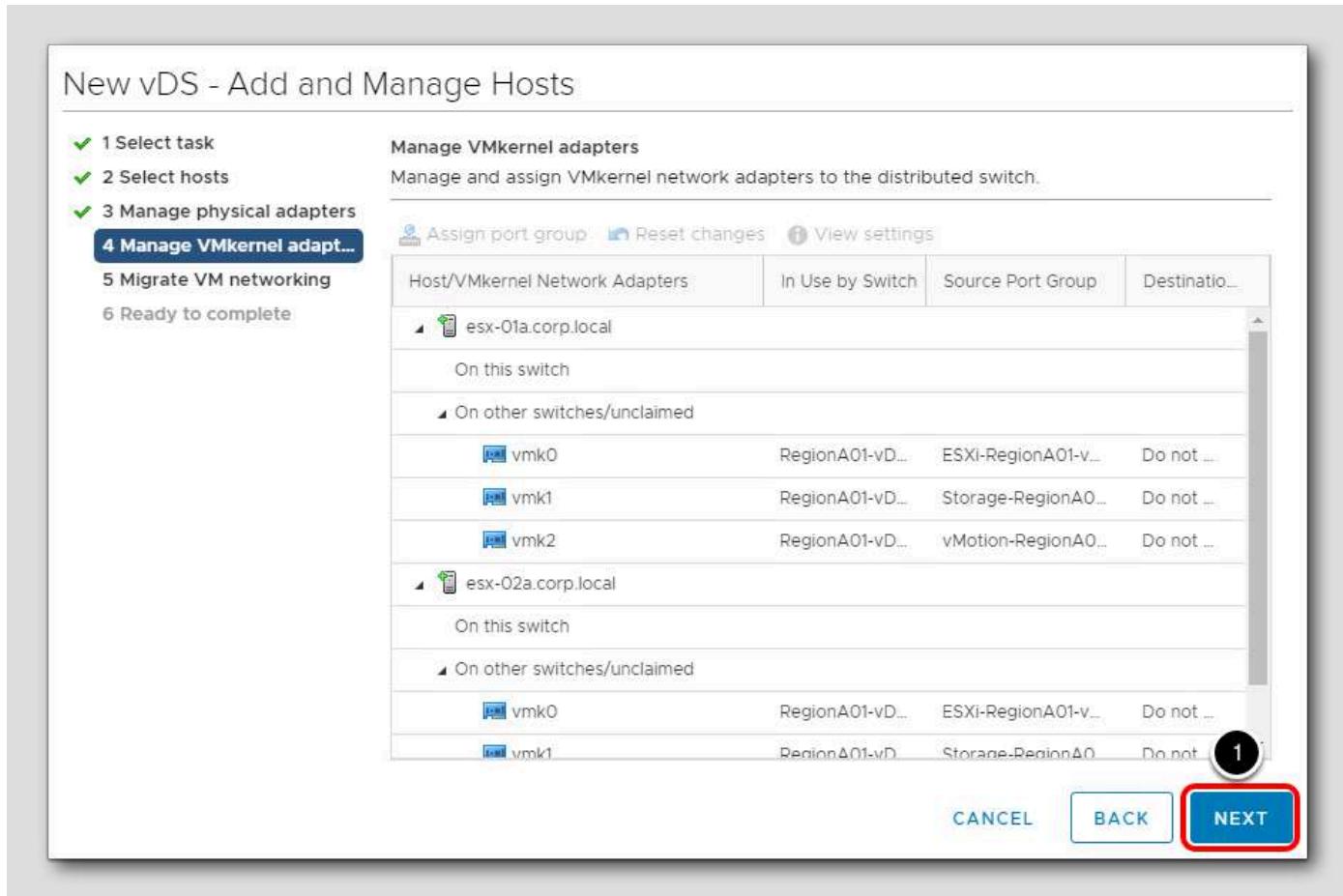
Manage VMkernel adapters
Manage and assign VMkernel network adapters to the distributed switch.

[Assign port group](#) [Reset changes](#) [View settings](#)

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destinatio...
▼ esx-01a.corp.local			
On this switch			
▼ On other switches/unclaimed			
vmk0	RegionA01-vD...	ESXI-RegionA01-v...	Do not ...
vmk1	RegionA01-vD...	Storage-RegionA0...	Do not ...
vmk2	RegionA01-vD...	vMotion-RegionA0...	Do not ...
▼ esx-02a.corp.local			
On this switch			
▼ On other switches/unclaimed			
vmk0	RegionA01-vD...	ESXI-RegionA01-v...	Do not ...
vmk1	RegionA01-vD...	Storage-RegionA0...	Do not ...

1

CANCEL BACK NEXT



1. Since we will not be using this distributed switch for any VMkernel functions, click **Next**

Migrate VM networking

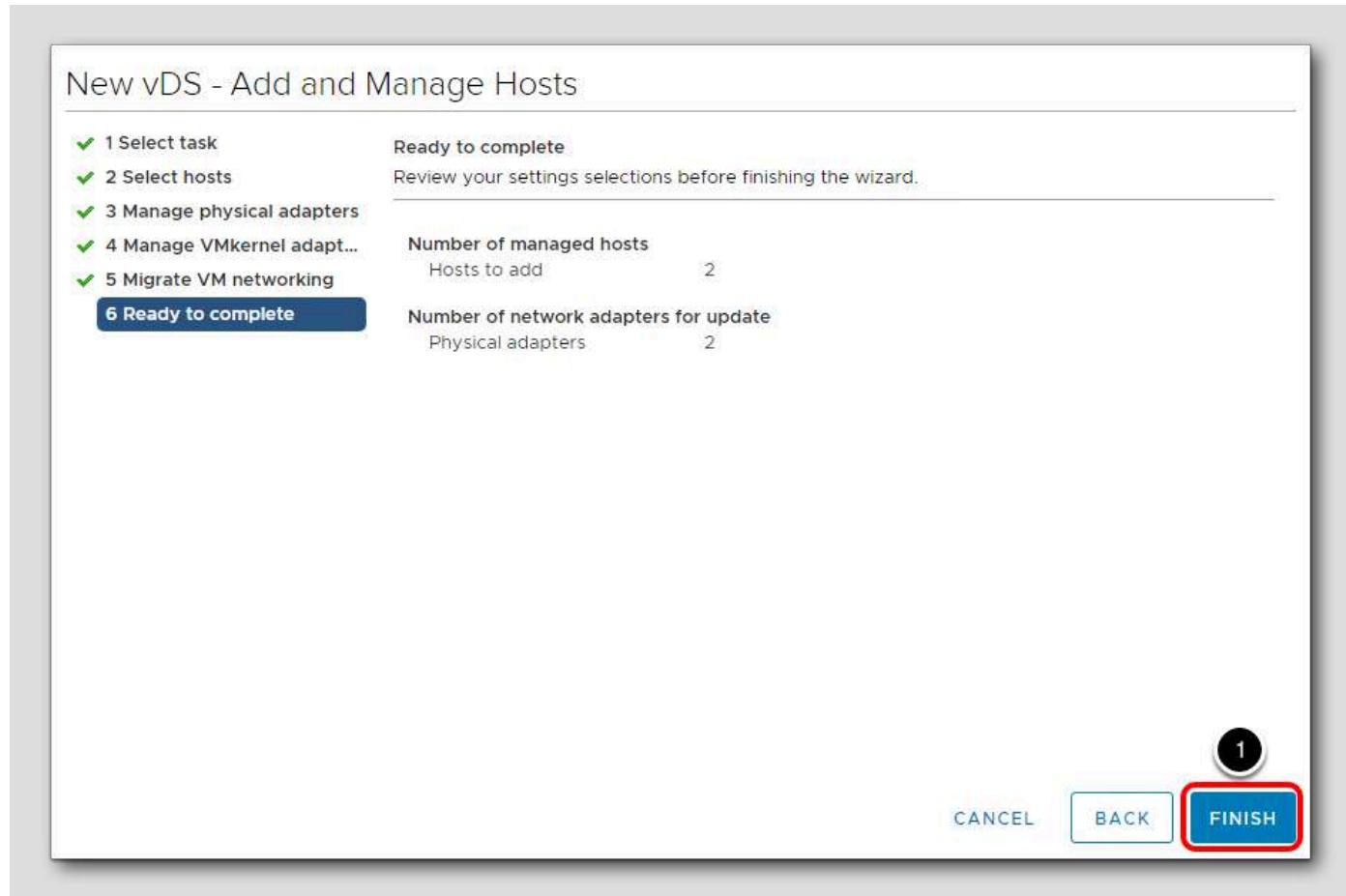
The screenshot shows the 'New vDS - Add and Manage Hosts' wizard. On the left, a vertical list of steps is shown: 1 Select task, 2 Select hosts, 3 Manage physical adapters, 4 Manage VMkernel adapt..., 5 Migrate VM networking (which is highlighted in blue), and 6 Ready to complete. The main pane is titled 'Migrate VM networking' and contains the instruction 'Select virtual machines or network adapters to migrate to the distributed switch.' Below this is a checkbox labeled 'Migrate virtual machine networking'. At the bottom of this section are three buttons: 'Assign port group', 'Reset changes', and 'View settings'. A table below this displays network adapter information, with the message 'No records to display'. At the bottom right of the main pane are 'CANCEL', 'BACK', and 'NEXT' buttons. The 'NEXT' button is circled in red. A small number '1' is circled in black at the top right of the main pane.

The add hosts wizard also gives us the ability to migrate VMs from one distributed switch to another on this page. While this action can be done here, we will be doing this in the next lesson.

1. Click **Next**

Also note that this wizard is not the typical place where you would migrate VMs from one virtual switch to another. The process we will be using later is the recommended method.

Complete the host add wizard



1. On the Ready to Complete page, click Finish

Explore your new vDS

New vDS | ACTIONS ▾

1

Hosts

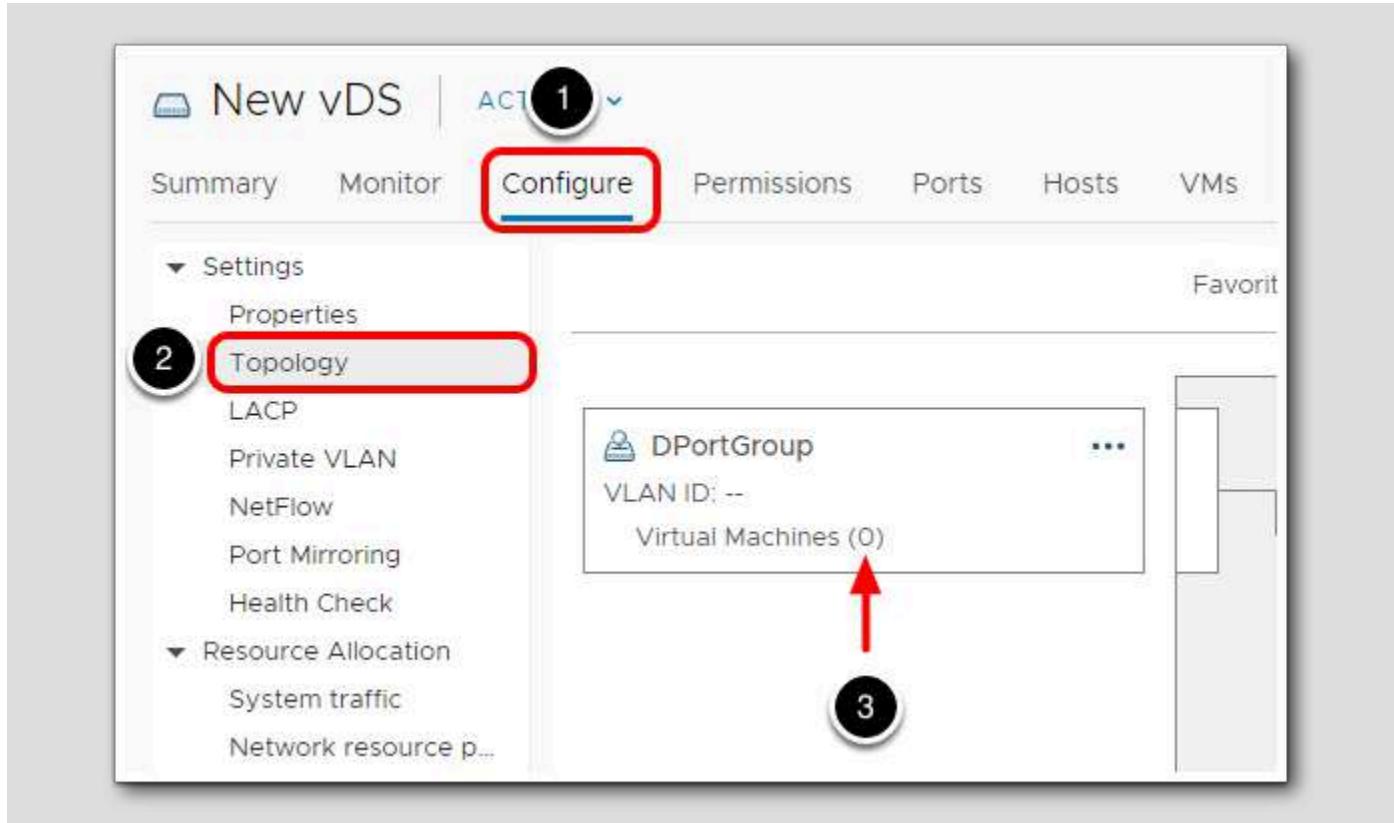
VMs Networks

Name ↑	State	Status	Cluster
esx-01a.corp.local	Connected	Normal	RegionA01-CO...
esx-02a.corp.local	Connected	Normal	RegionA01-CO...

With your new Distributed Switch highlighted, feel free to explore the associated tabs to get a feel for the setup and configuration.

1. Click on the Hosts tab to see the newly connected hosts

Topology



1. Click Configure

2. Click Topology

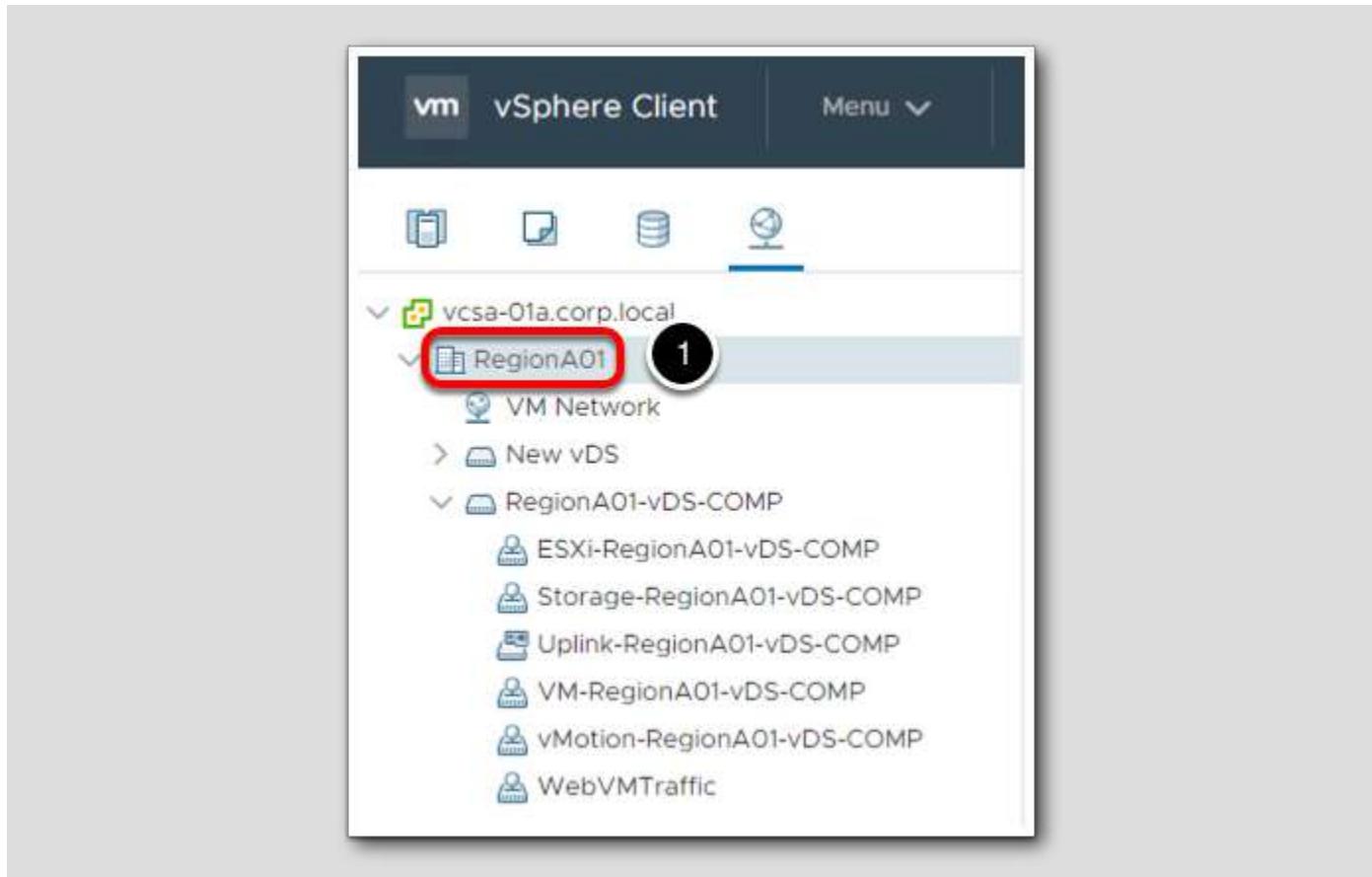
Note that your distributed port group DPortGroup does not have any VMs connected to it. The next lesson will walk through the process of migrating VMs to the new vDS.

Migrating VMs from vDS to vDS

Now that we have created a new vDS, we want to take advantage of its capabilities. In this lab we will migrate a running virtual machine from a virtual standard switch to the newly created distributed virtual switch.

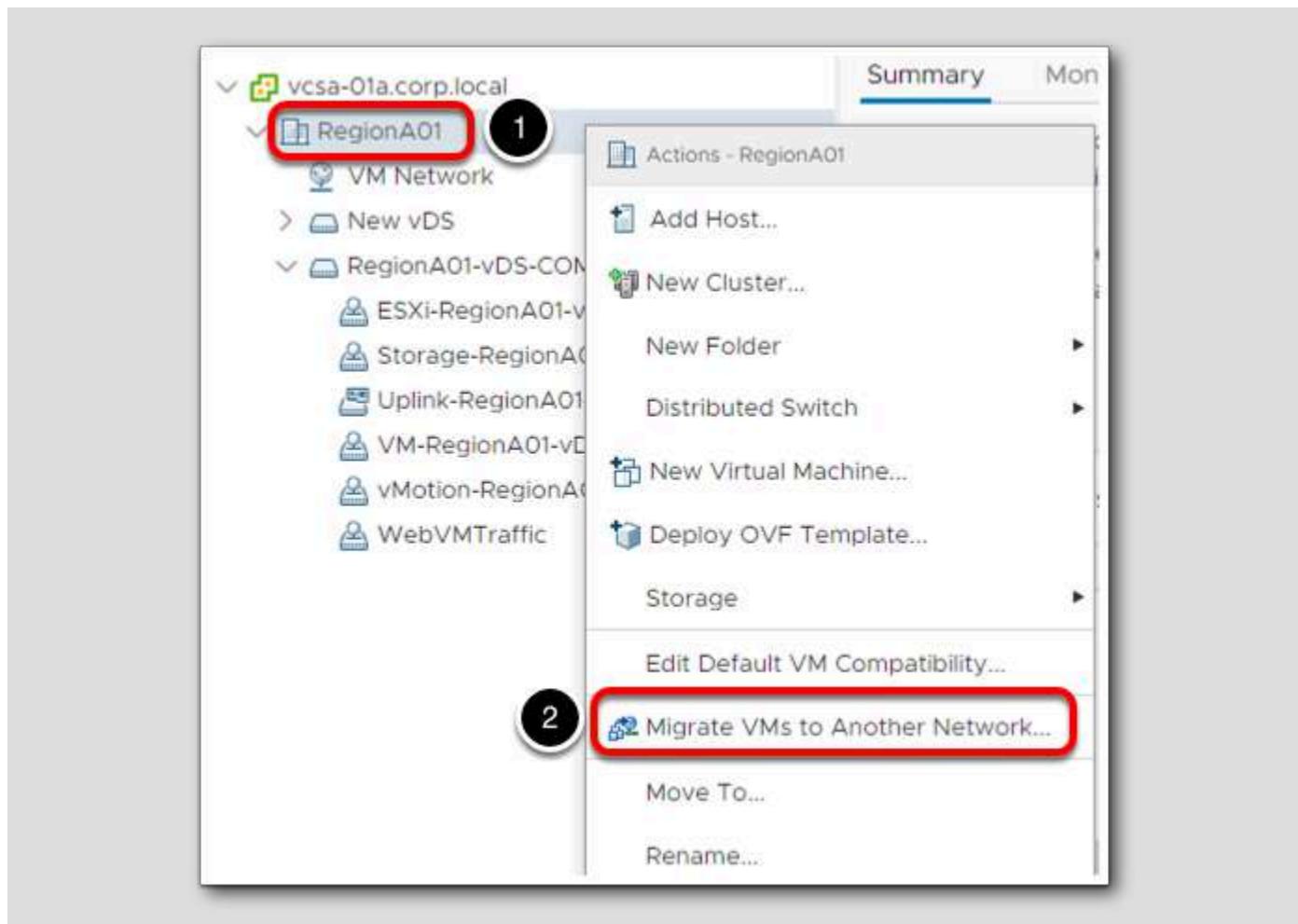
In the vSphere Client, there are numerous ways to accomplish the task of VM network migration. However, we will be walking through the procedures specifically outlined in the vSphere product documentation.

Navigate to your datacenter



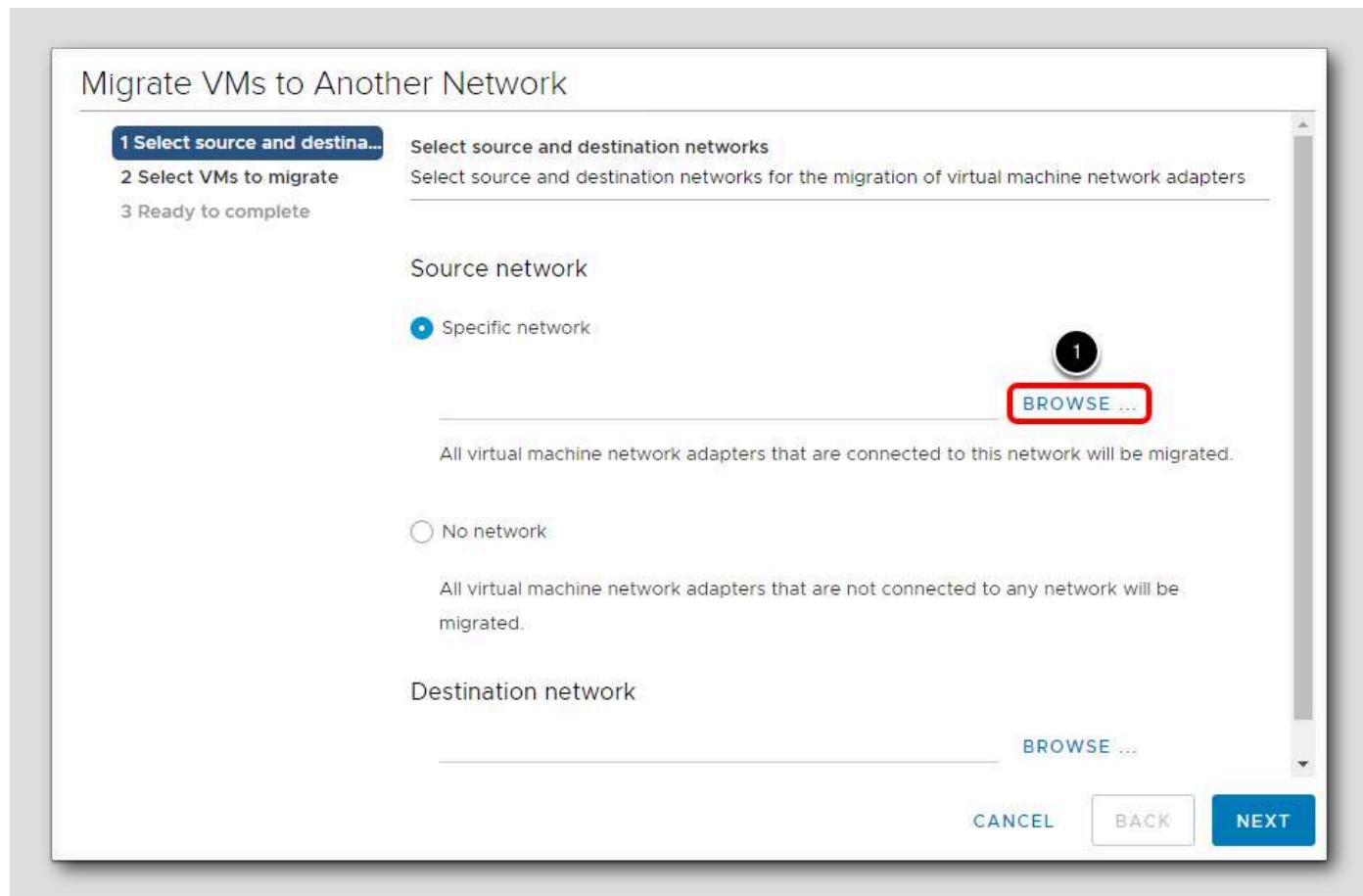
1. To get started, click on RegionA01

Migrate VMs



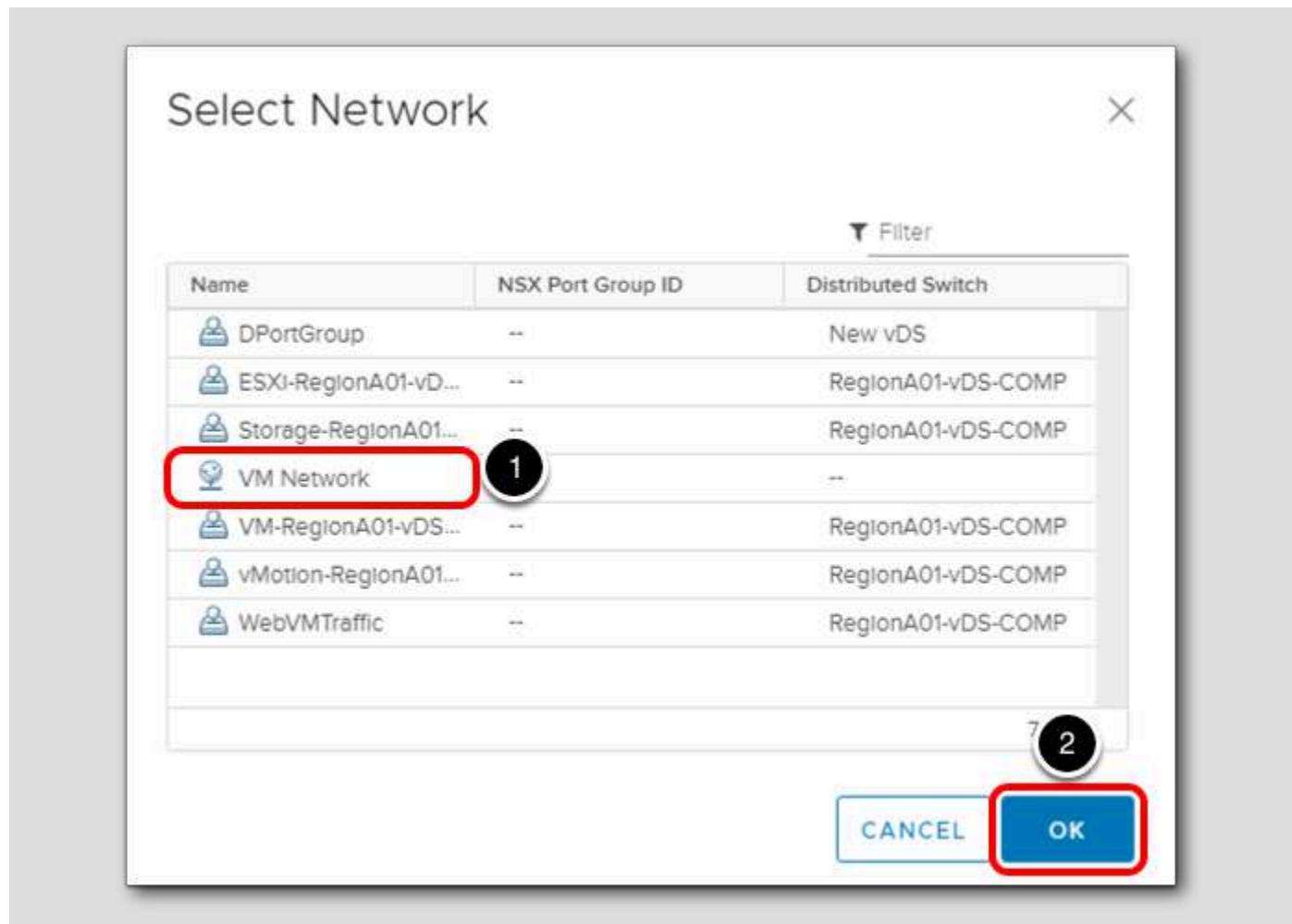
1. Right-click on RegionA01
2. Select Migrate VMs to Another Network

Select source network



1. Under Source network click on Browse

VM Network

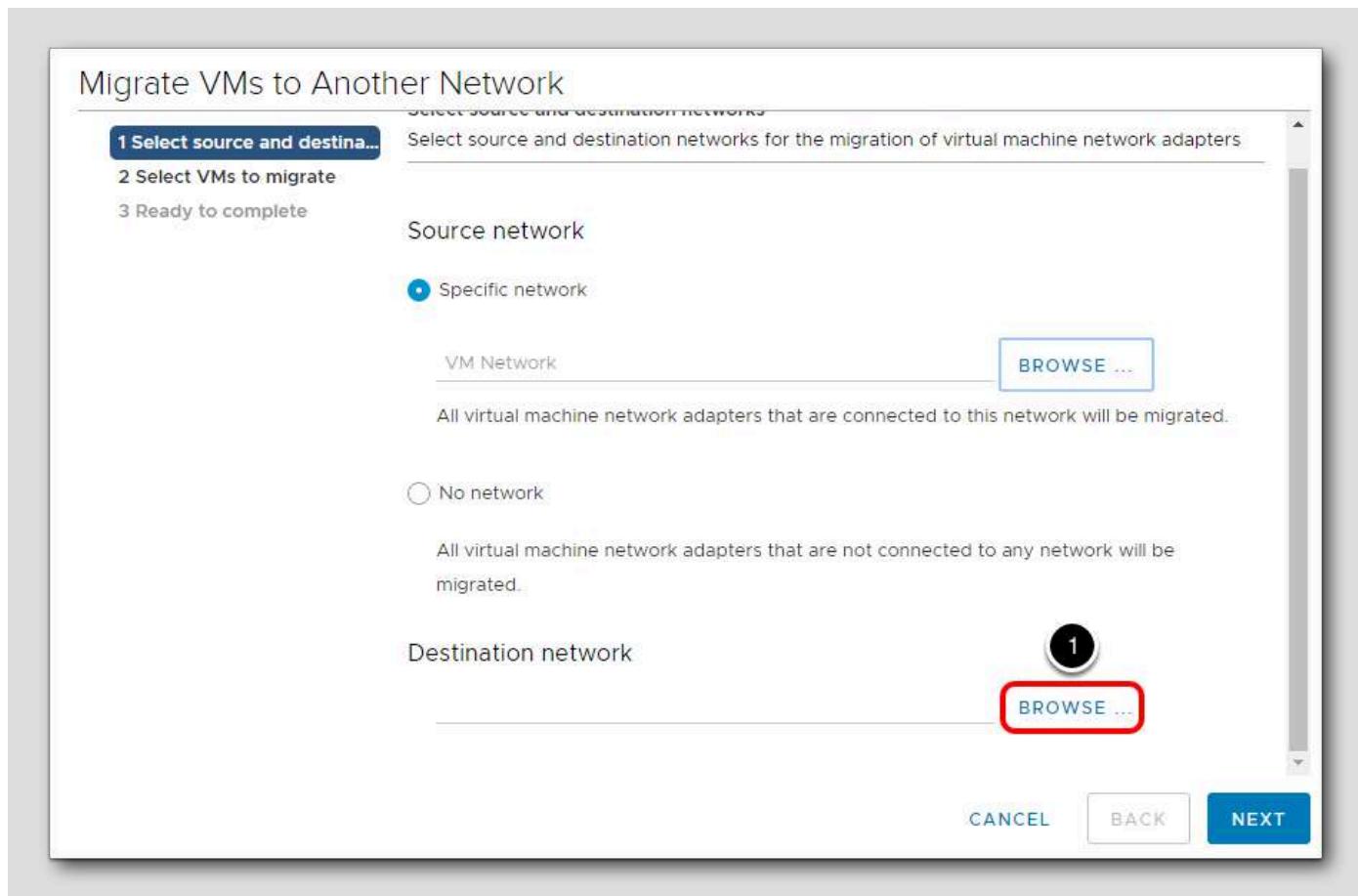


1. Select VM Network

2. Click OK

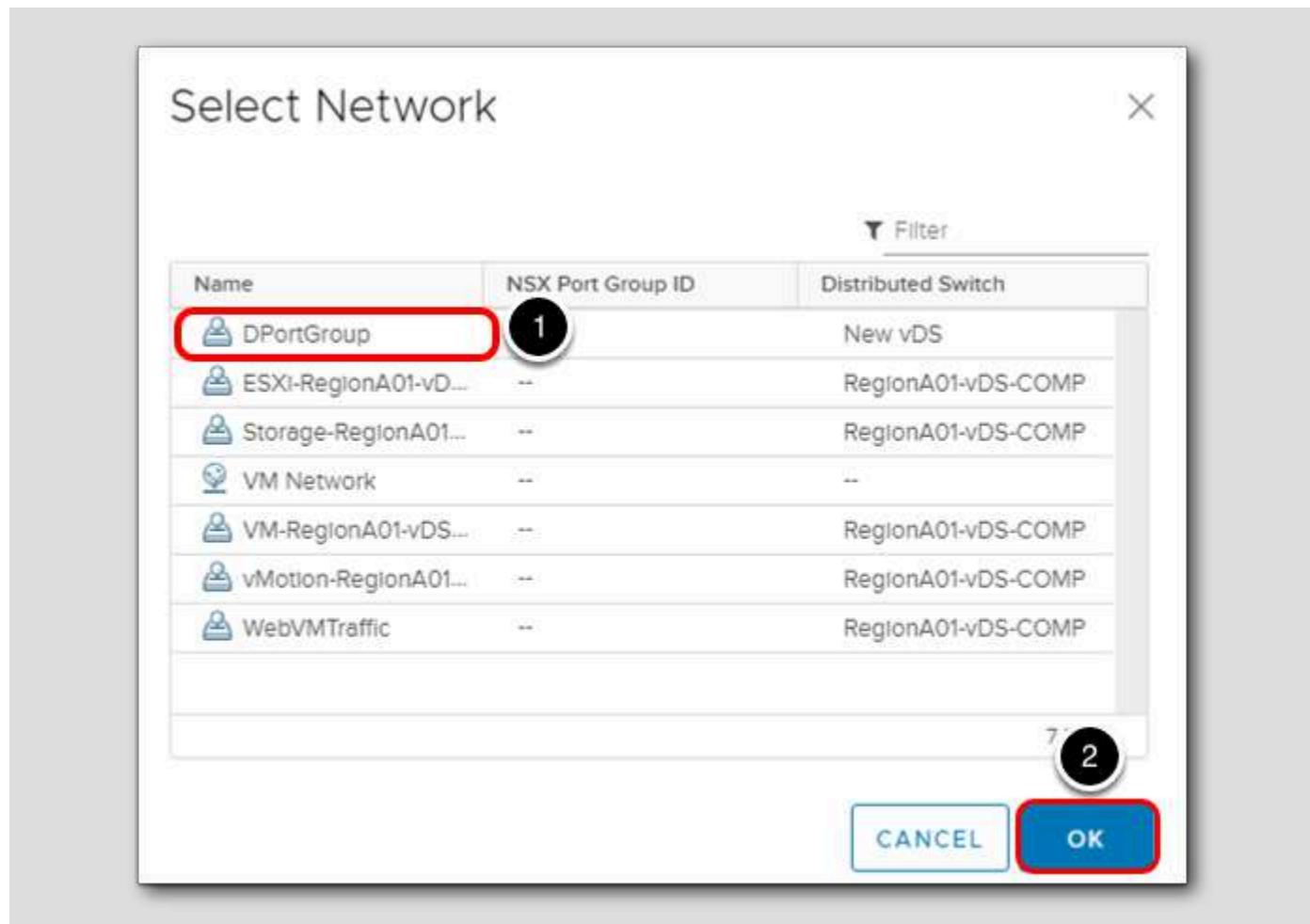
This is the network associated with the virtual standard switch where our VM is currently connected that we want to migrate.

Select destination network



1. Under Destination network select Browse

DPortGroup

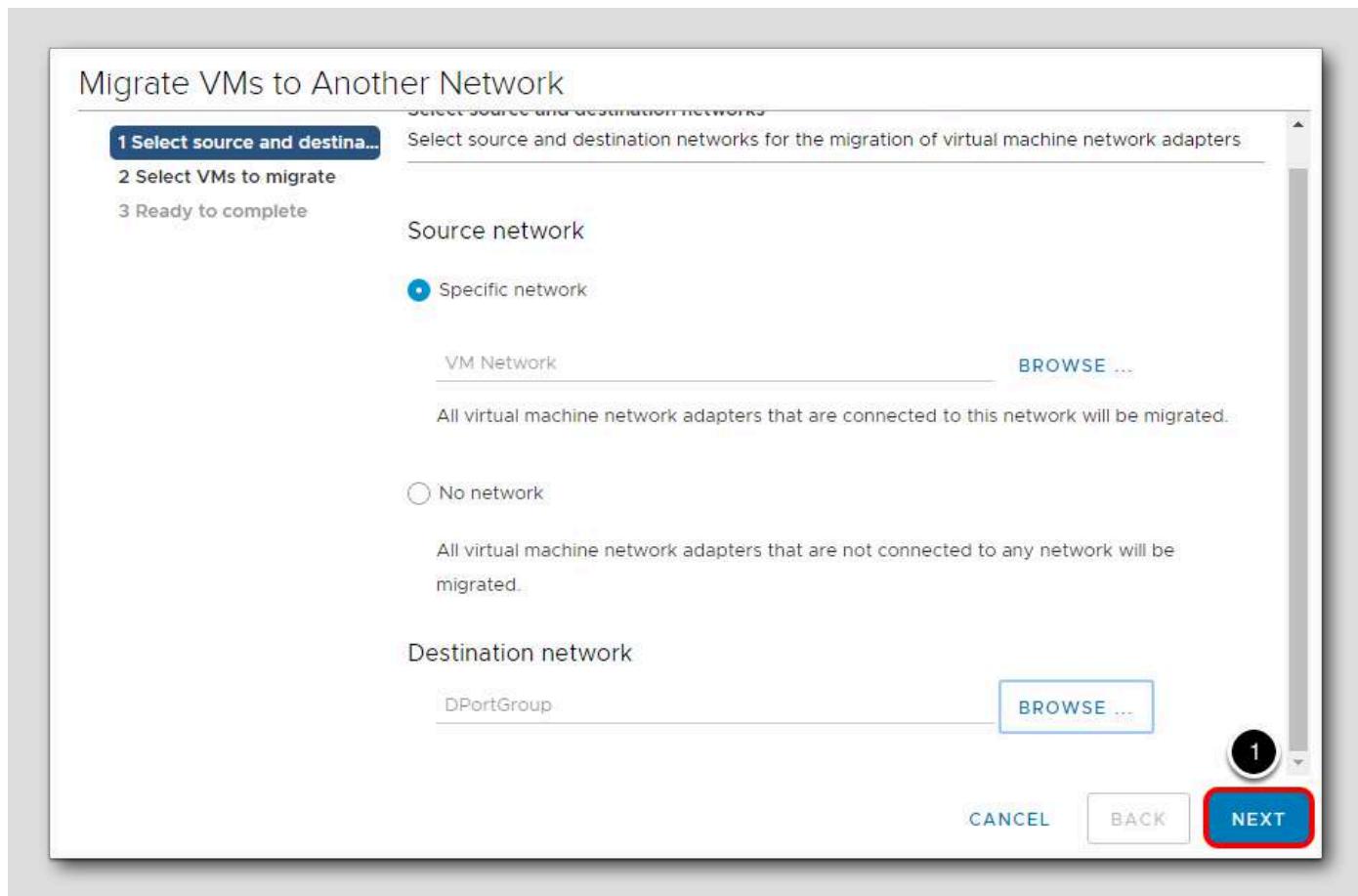


1. Select DPortGroup

2. Click OK

This is the port group on the new Distributed Switch that you created. This is the new port group that will be used to connect the VM being migrated to the network.

Migrate VMs



1. Click **Next**

Select VM to migrate

Migrate VMs to Another Network

1 Select source and destina... 2 Select VMs to migrate 3 Ready to complete

Select VMs to migrate
Select virtual machines to migrate to the destination network

Select virtual machines to migrate from VM Network to DPortGroup:

	Virtual Machine	Network Adapter	Host	Destination Network
1	<input checked="" type="checkbox"/> TinyLinux2	Network adapter 1	esx-01a.corp.local	Accessible

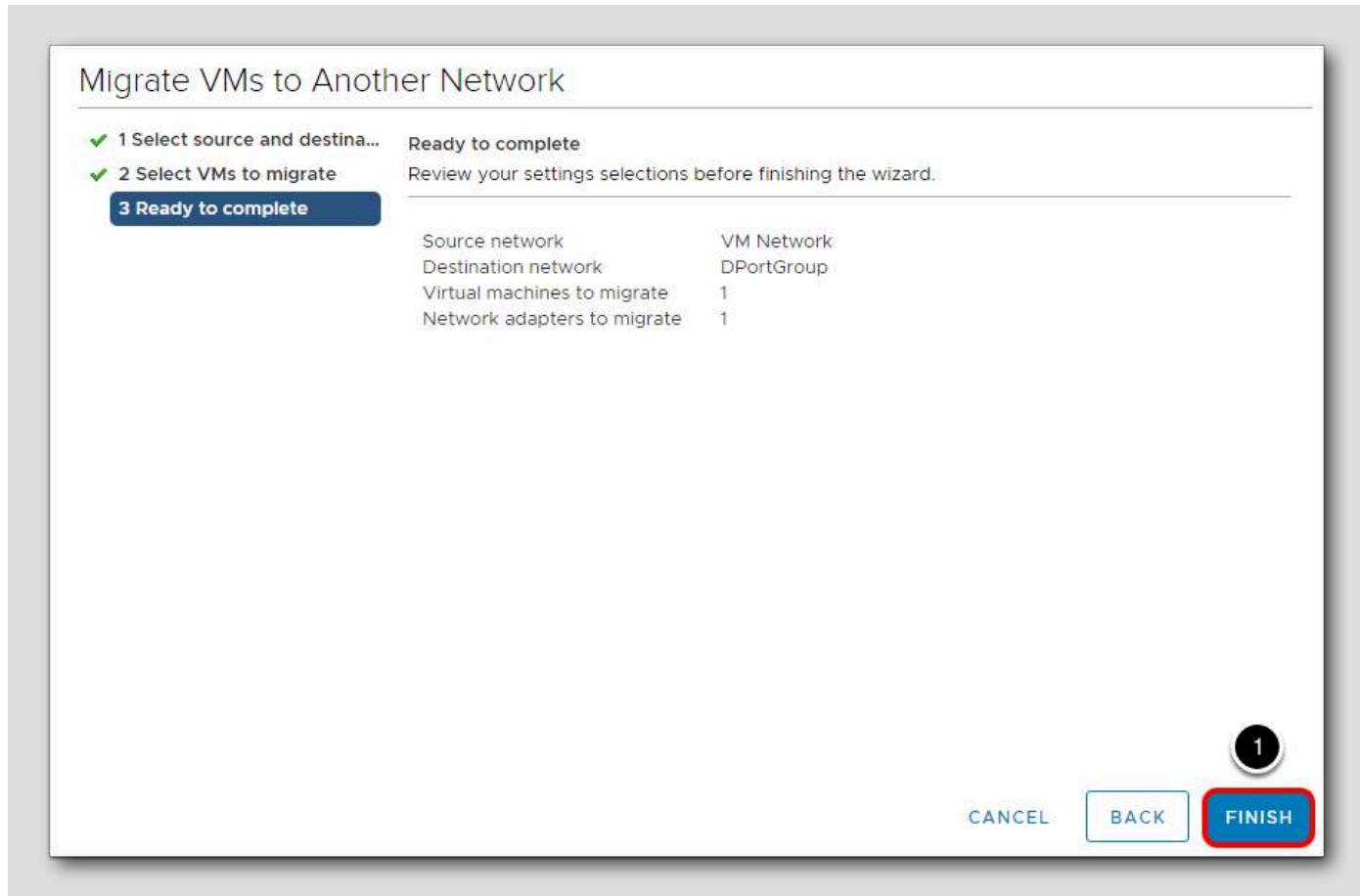
CANCEL BACK NEXT

1. Click on **TinyLinux2**

Note that there is only one adapter associated with this VM. If there was more than one, you would have the option of choosing which one you would want to connect to the new vDS.

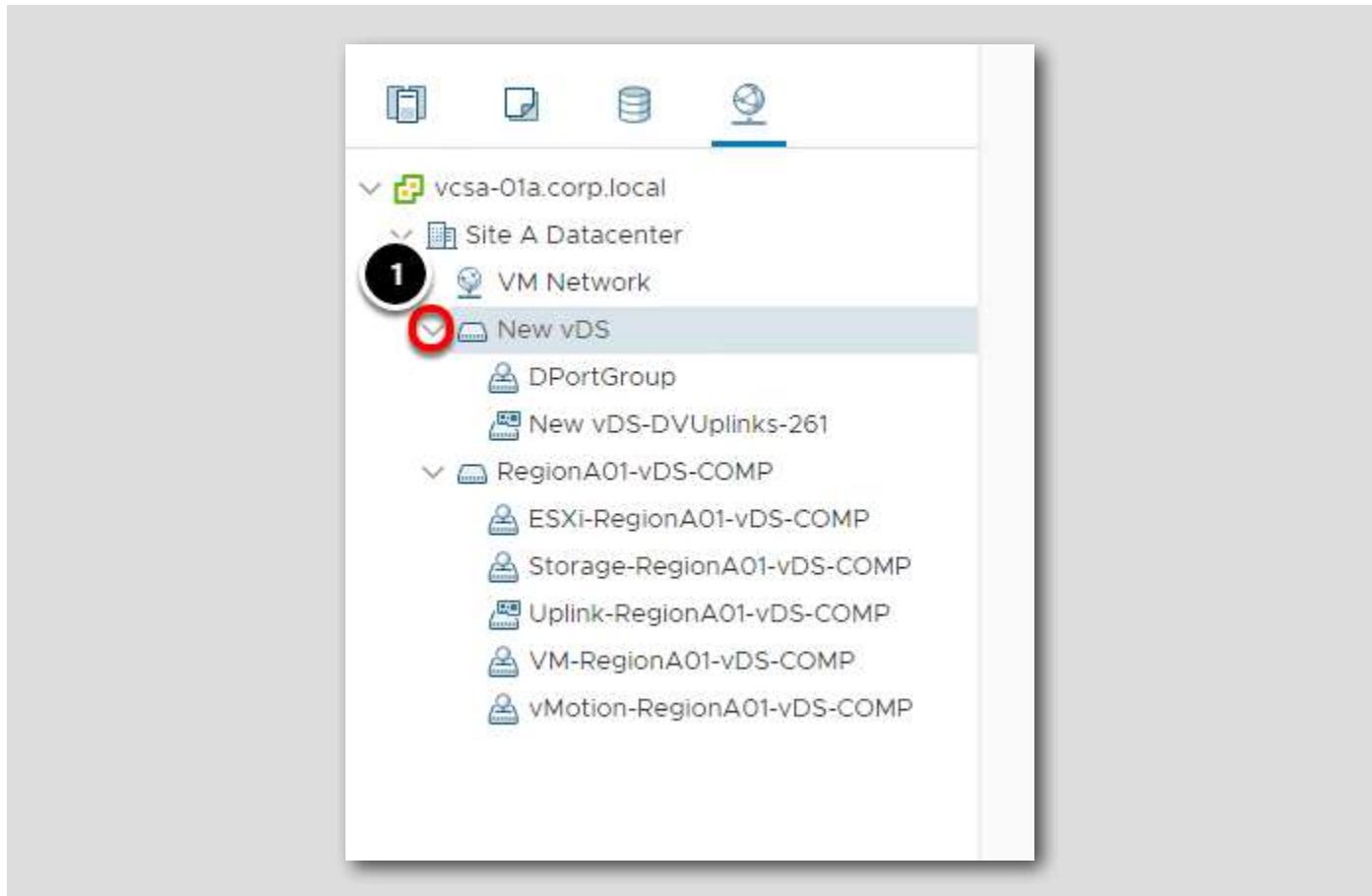
2. Click **Next**.

Ready to Complete



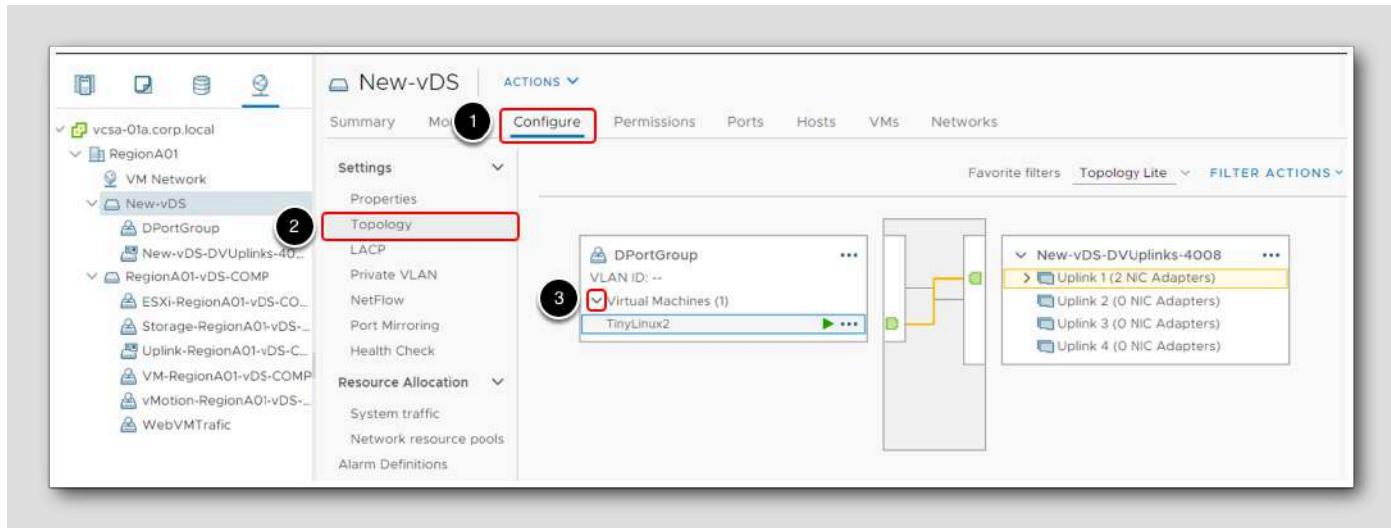
1. Click Finish to migrate the VM from a Standard Switch to the new Distributed Switch

Explore your changes



1. Click on the new Distributed Switch and expand it to see all associated port groups and uplink

New-vDS Topology Map



1. Click Configure
2. Click Topology
- 3.Under DPortGroup, click on the drop-down arrow to expand the view

Select the TinyLinux2 VM and note the highlighted path through the new vDS and Uplink.

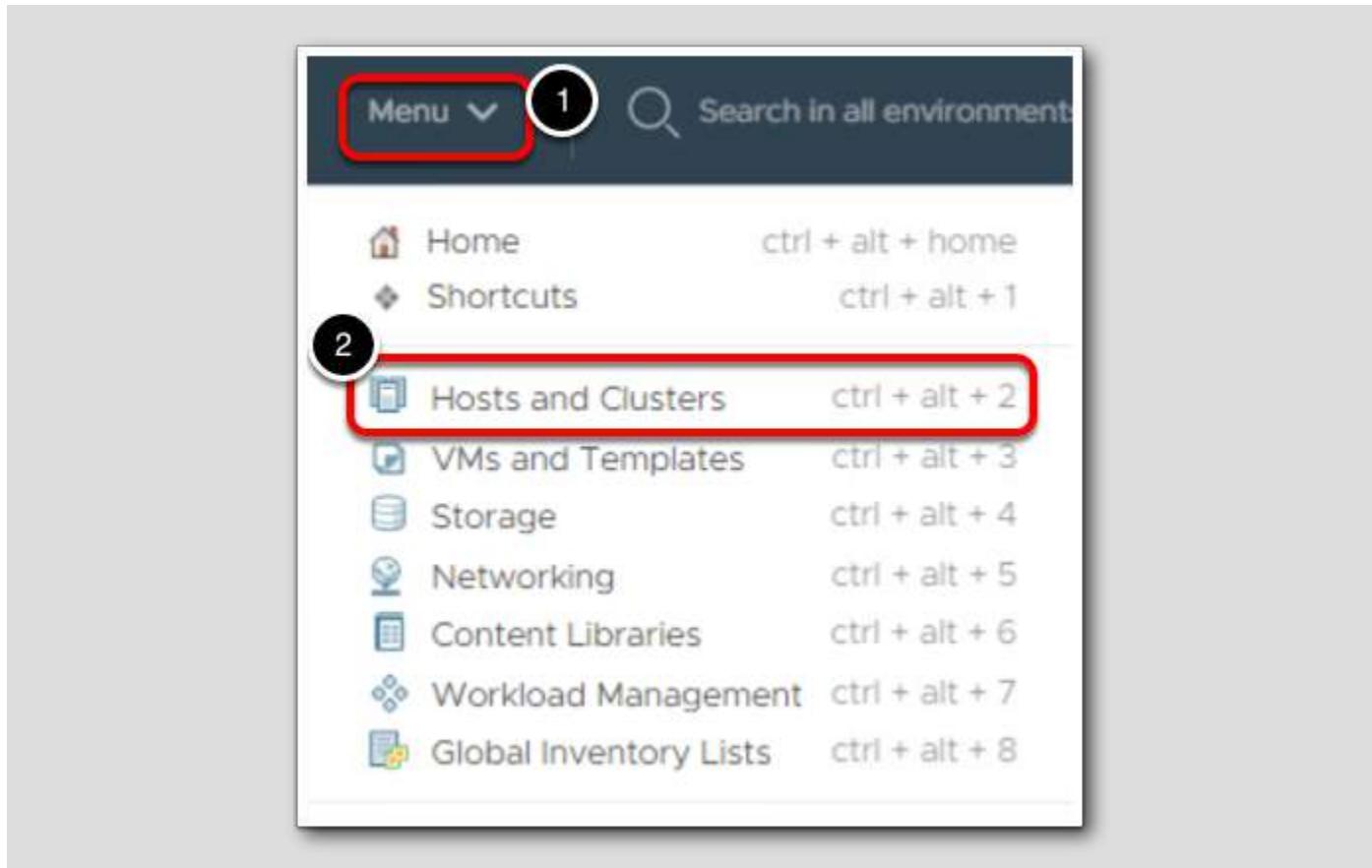
Adding and Configuring a vSphere Distributed Switch

This lesson will walk you through adding and configuring a Distributed Switch.

Create a vSphere Distributed Switch on a vSphere datacenter to handle networking traffic for all associated hosts in the datacenter. If your system has many hosts and complex port group requirements, creating distributed port groups rather than a standard port groups can go a long way towards easing the administrative burden.

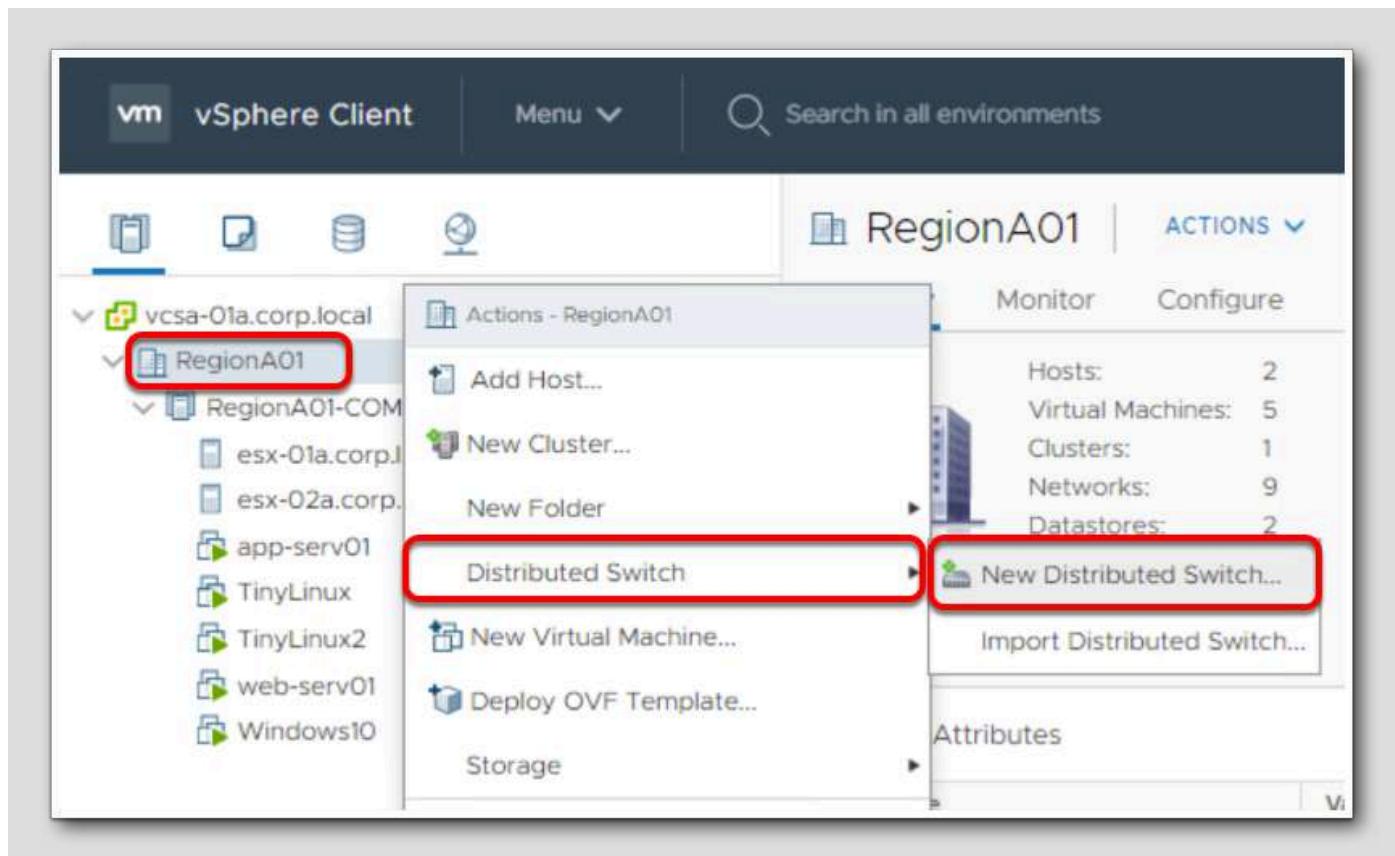
1. Keep the default values and click Next

Select Host and Clusters



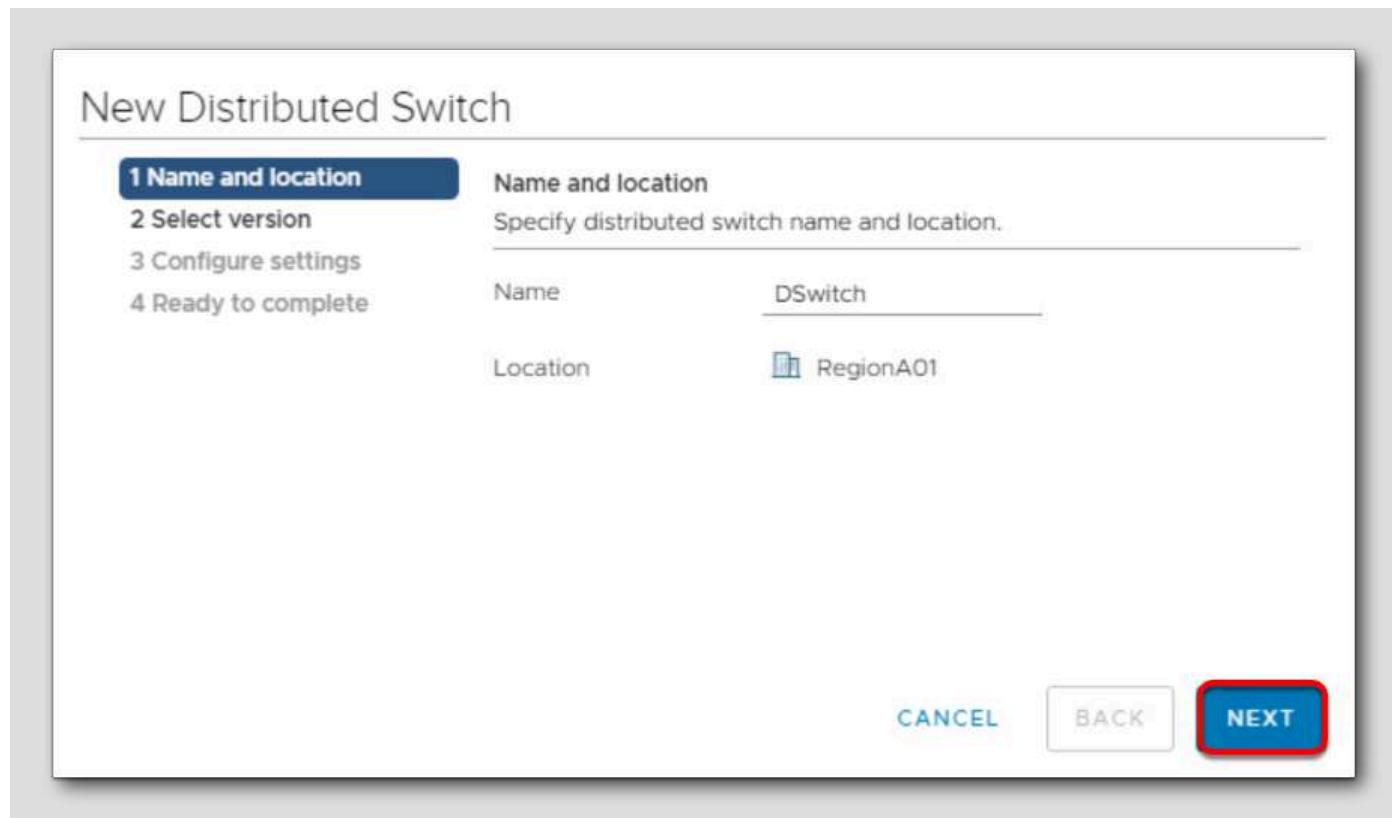
1. Click **Menu**
2. Click **Host and Clusters**

Add a vSphere Distributed Switch using the vSphere Web Client



1. Under vcsa-01a.corp.local, right-click RegionA01
2. Select Distributed Switch and then click New Distributed Switch

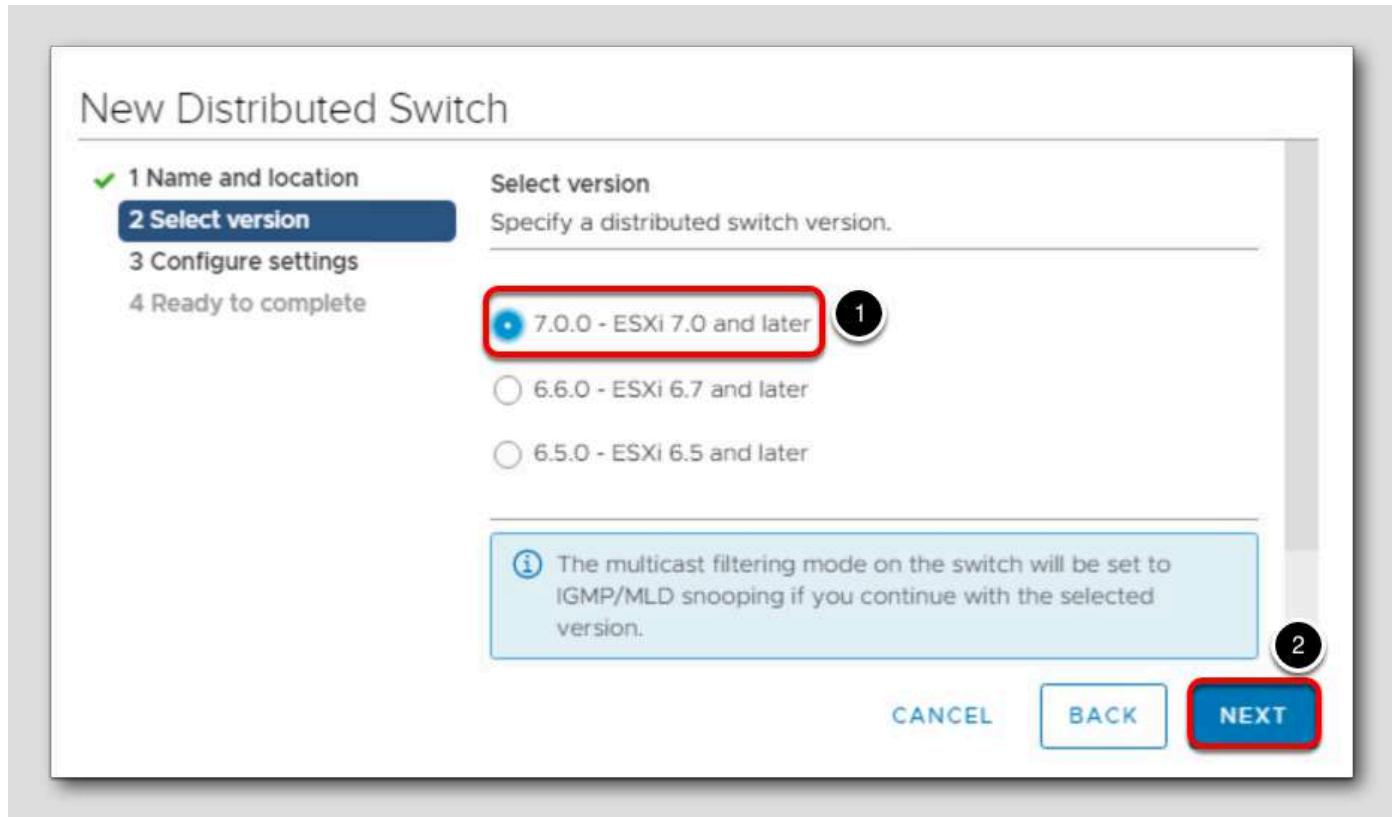
Name and Location



Keep the default name for the new distributed switch.

1. Click **Next**

Select version

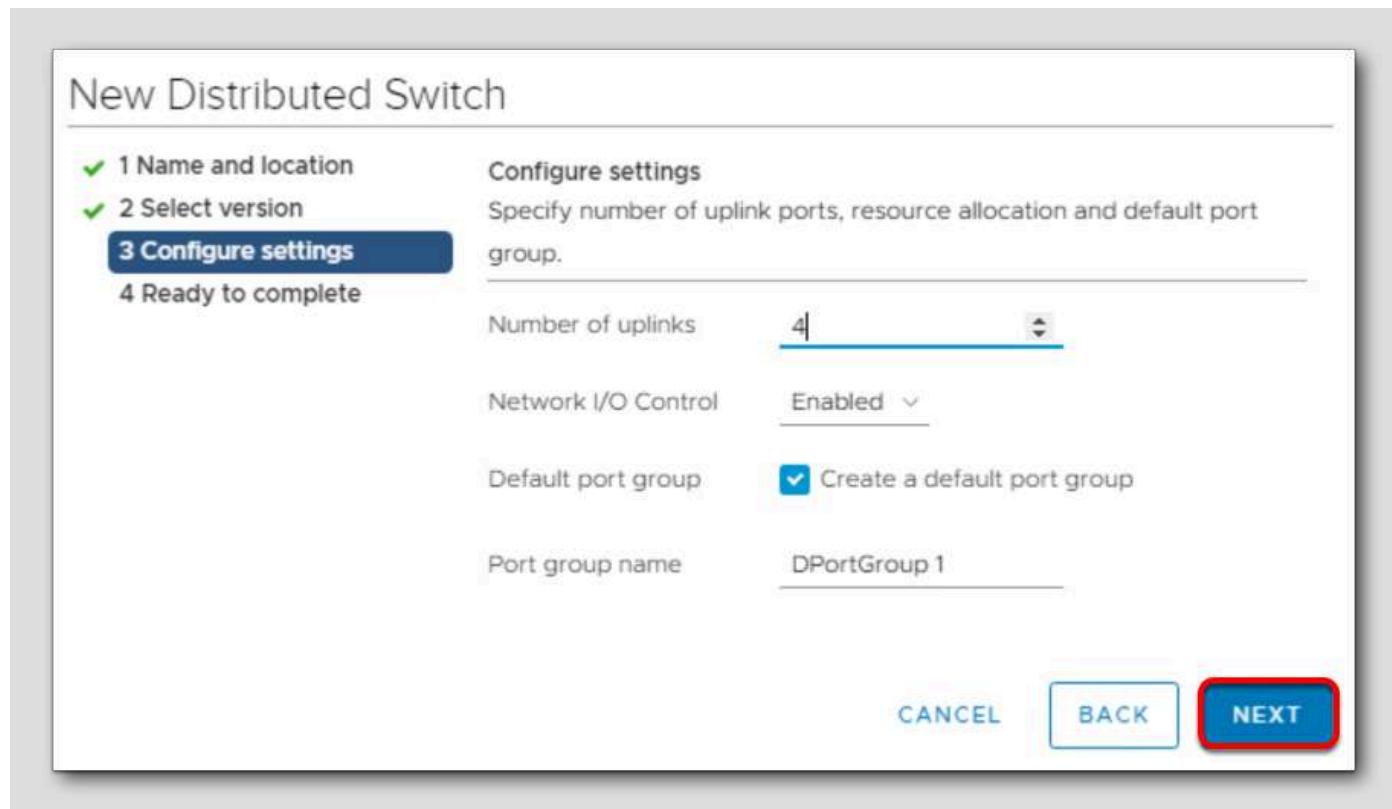


1. Leave the default setting of 7.0.0 - ESXi 7.0 and later

2. Click **Next**

Note that the version of the Distributed Switch determines which ESXi host versions are able to join the switch. Once all hosts that are a member of a Distributed Switch have been upgraded, the switch may be upgraded to the matching version.

Edit Settings



1. Leave the default options and click Next

Ready to complete

New Distributed Switch

✓ 1 Name and location
✓ 2 Select version
✓ 3 Configure settings
4 Ready to complete

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

Name	DSwitch
Version	7.0.0
Number of uplinks	4
Network I/O Control	Enabled
Default port group	DPortGroup 1

Suggested next actions

- New Distributed Port Group
- Add and Manage Hosts

ⓘ These actions will be available in the Actions menu of the new distributed switch.

CANCEL **BACK** **FINISH**

1. Review the settings and click **Finish**

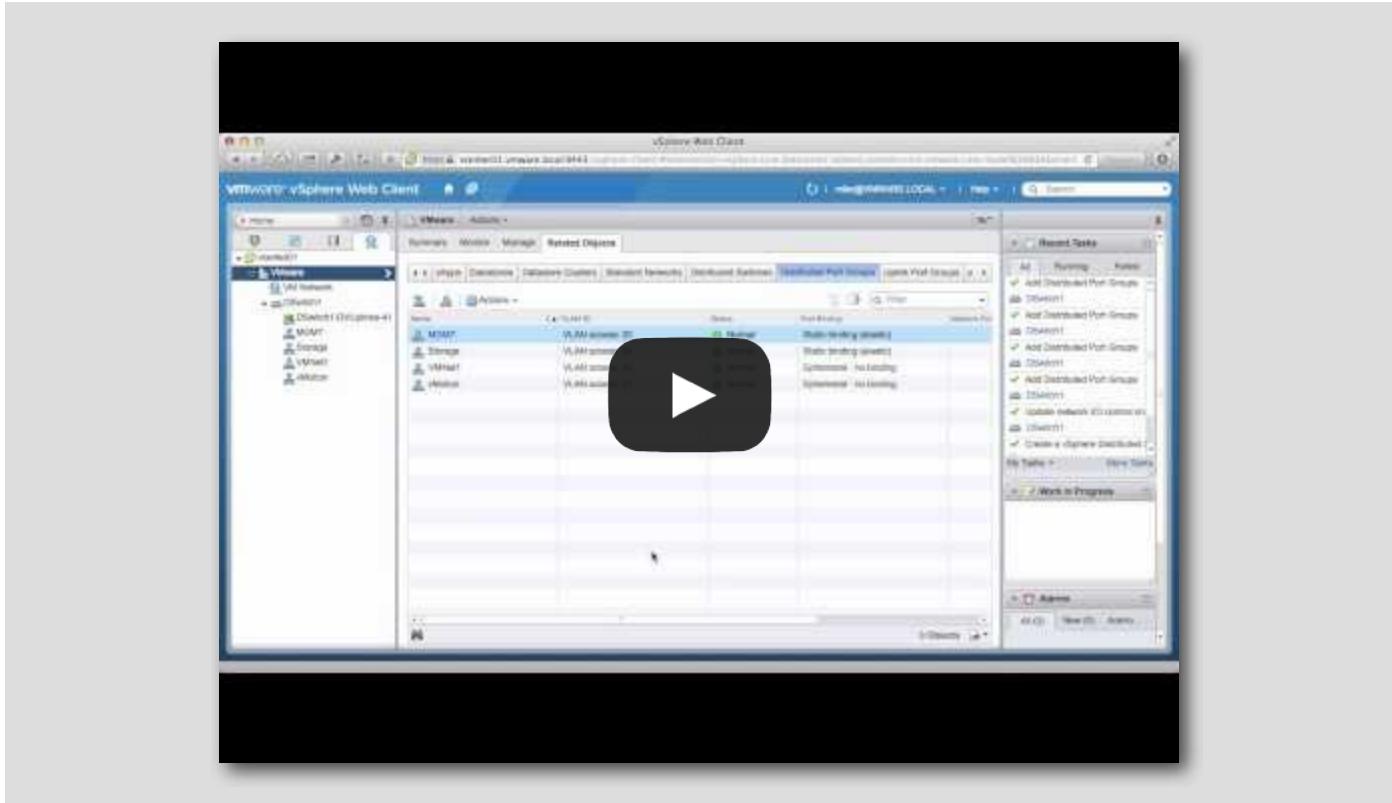
Notice the next suggested steps are to create Distributed Port Groups and adding Hosts.

(Optional) Video: Getting Starting with the VMware vSphere Distributed Switch - Part 1 (3:39)

[324]

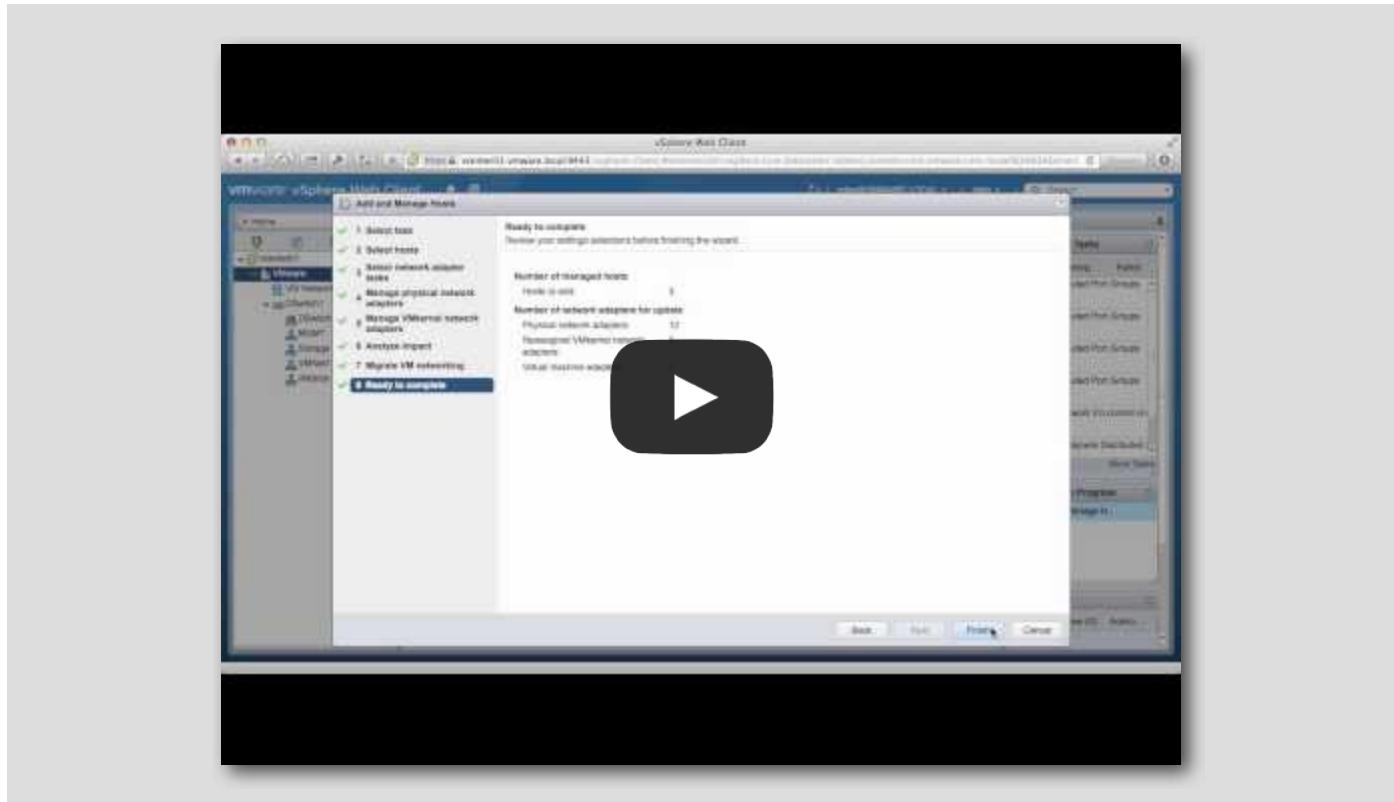
This video guides the user through creating a vSphere Distributed Switch and Port Groups.

<https://www.youtube.com/watch?v=NGQ5ejGfuDY>



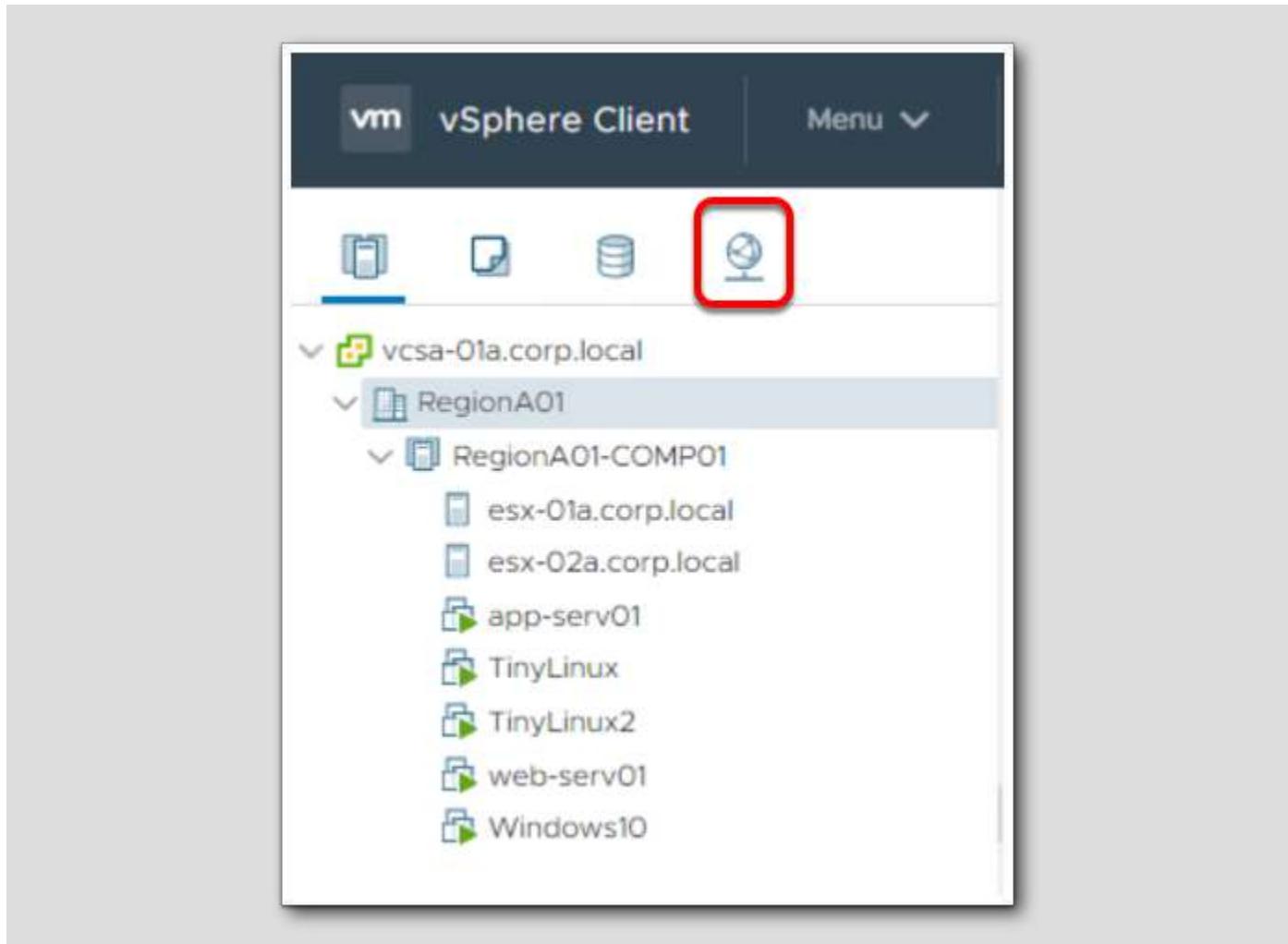
(Optional) Video: Getting Starting with the VMware vSphere Distributed Switch - Part 2 (3:38)

<https://www.youtube.com/watch?v=hiu8DLsIoAO>



This video guides the user through migrating hosts and VM's to the vSphere Distributed Switch.

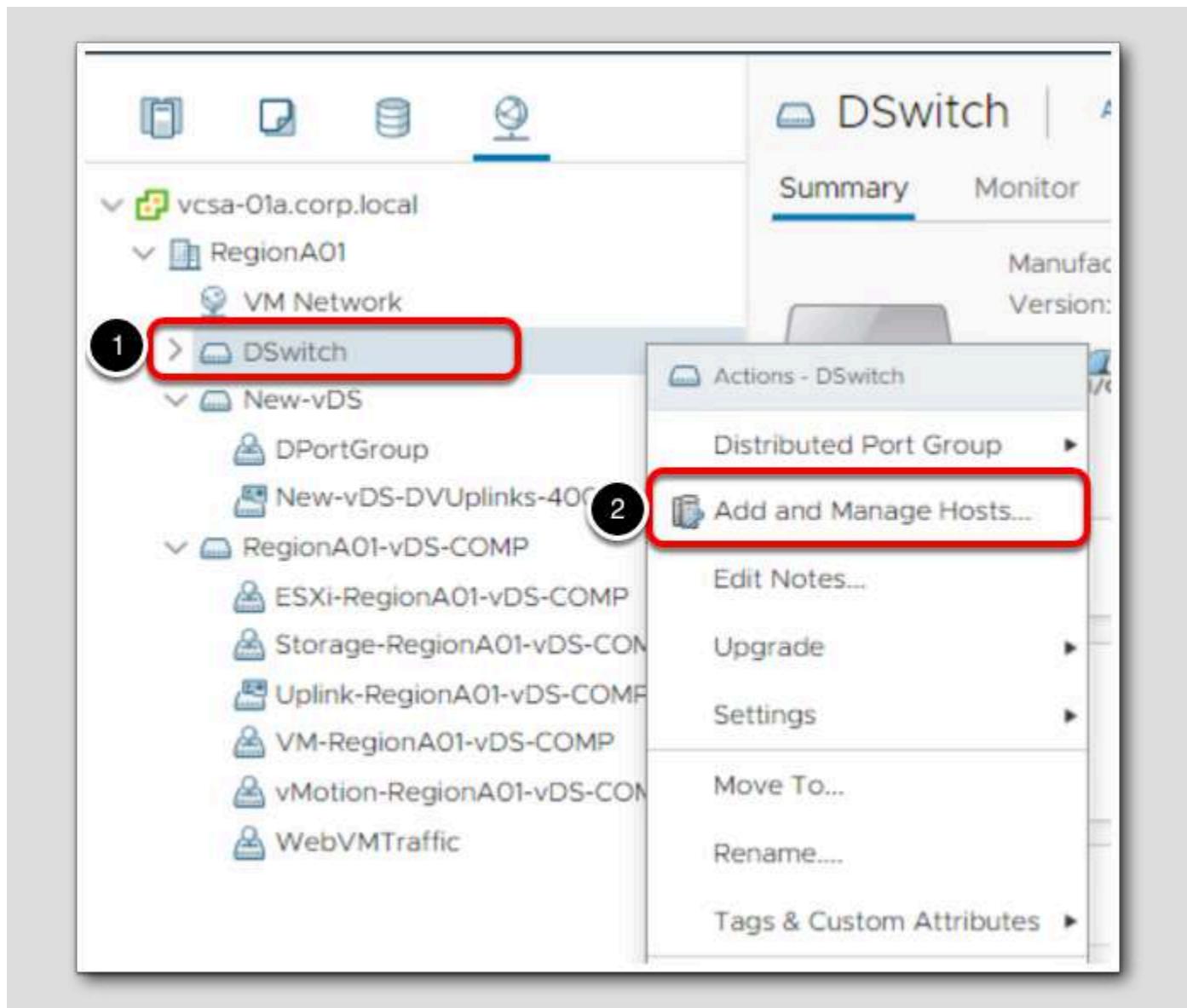
Add Hosts to a vSphere Distributed Switch in the vSphere Web Client



Now that we have created a vSphere distributed switch, let's add hosts and physical adapters to create a virtual network.

1. Click on the Networking icon

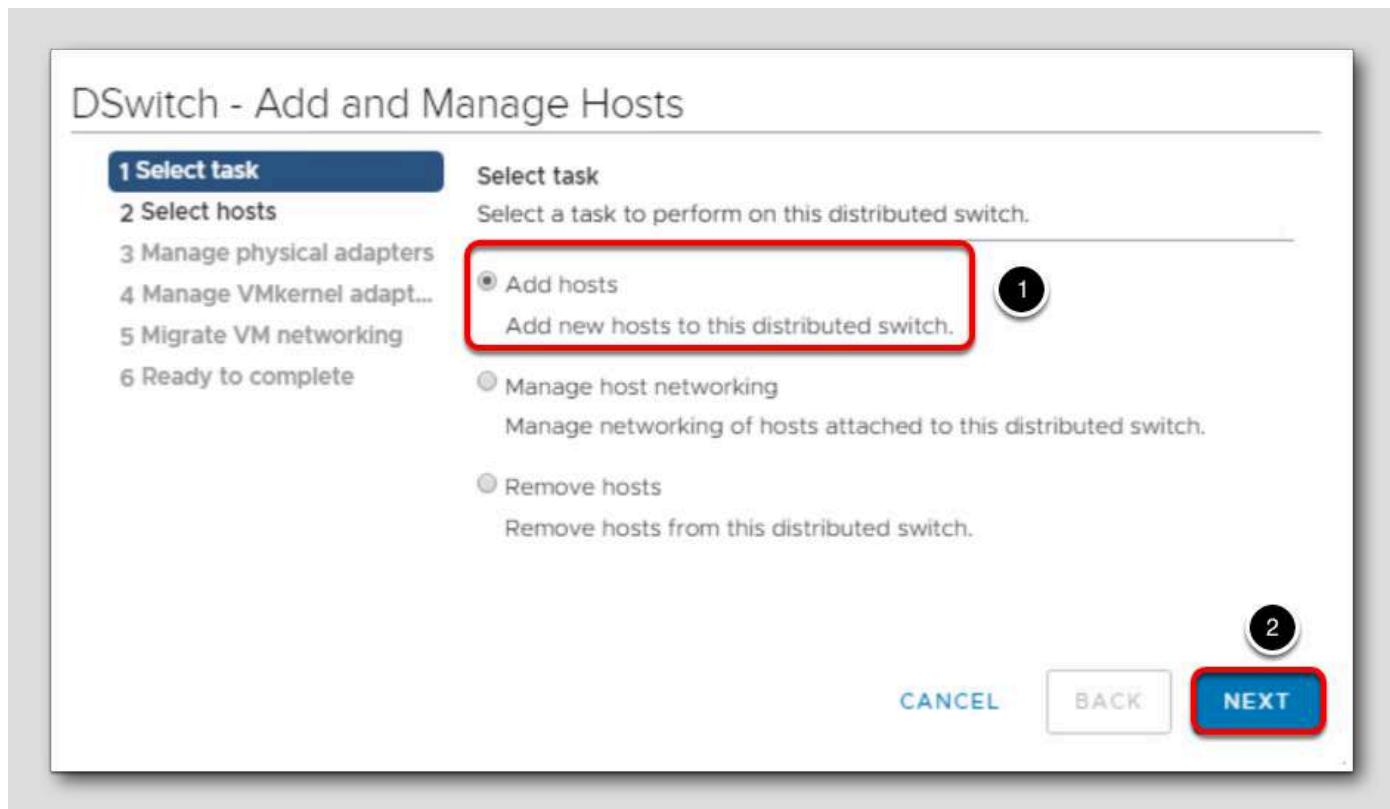
Add Hosts



Expand RegionA01 until you see the Distributed Switch we just created, DSwitch.

1. Right-click on DSwitch
2. Select Add and Manage Hosts

Select task



1. Select Add hosts

2. Click **Next**

Select hosts

To add hosts to the Distributed Switch, click the green '+'.

DSwitch - Add and Manage Hosts

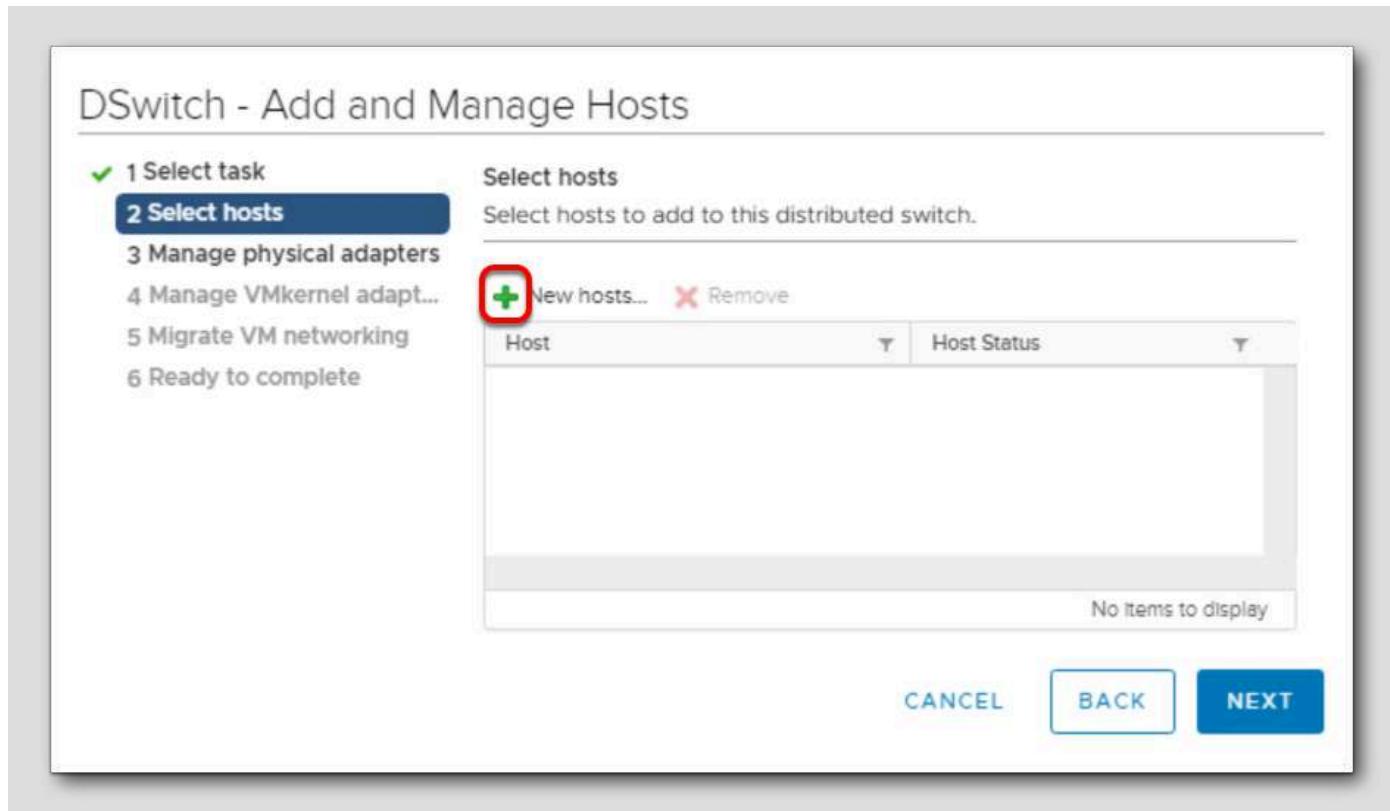
✓ 1 Select task
2 **Select hosts**
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Select hosts
Select hosts to add to this distributed switch.

 New hosts...  Remove

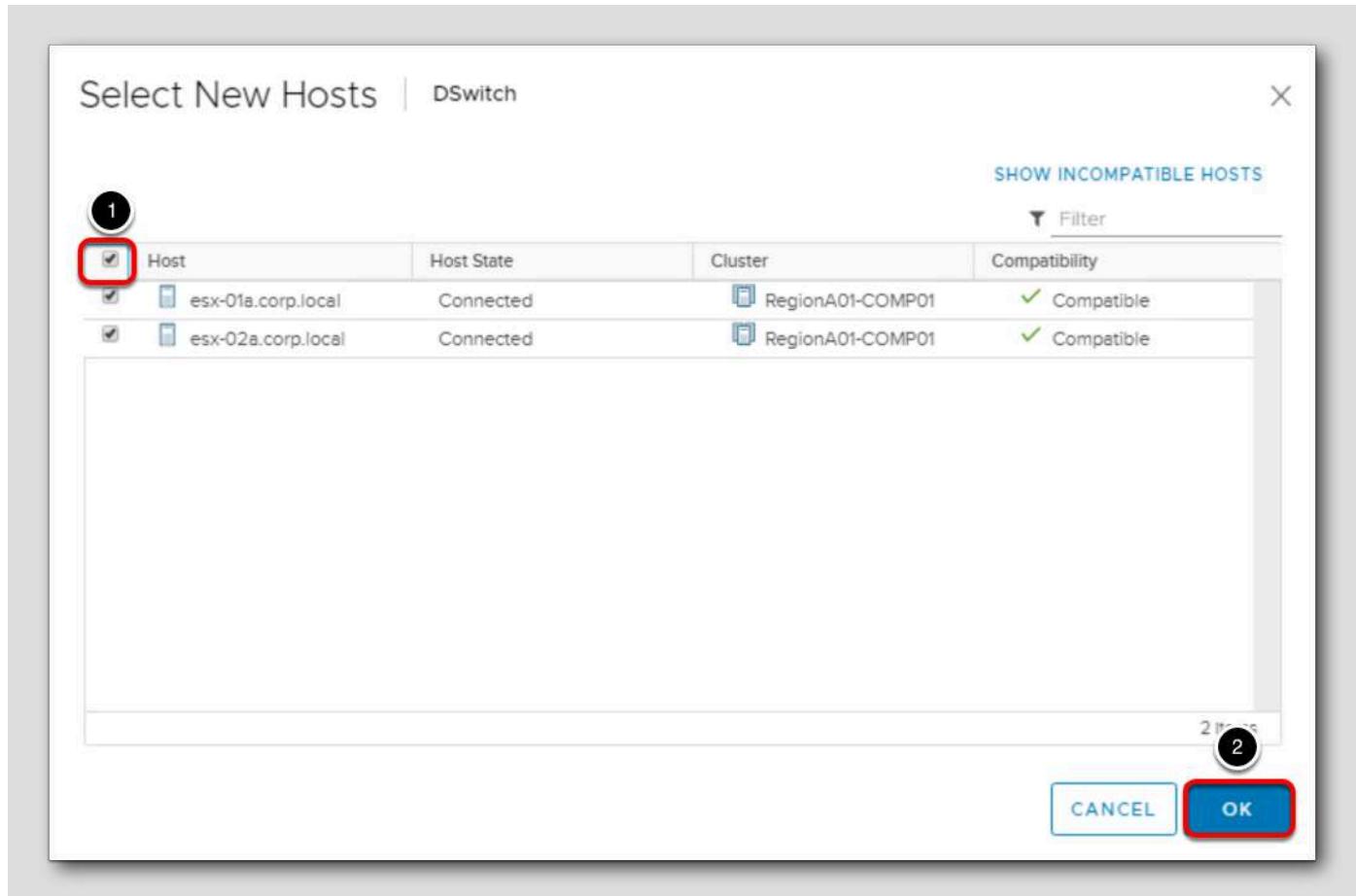
Host	Host Status
No items to display	

CANCEL BACK NEXT



1. Click New hosts

Select your Hosts



1. Select all ESXi hosts shown (esx-01a.corp.local and esx-02a.corp.local)

2. Click OK

Select hosts (cont.)

DSwitch - Add and Manage Hosts

✓ 1 Select task
2 **Select hosts**
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Select hosts
Select hosts to add to this distributed switch.

New hosts... Remove

Host	Host Status
(New) esx-01a.corp.local	Connected
(New) esx-02a.corp.local	Connected

2 items 1

CANCEL BACK NEXT

You should now see the hosts that will be added to the switch.

1. Click **Next**

Manage physical network adapters

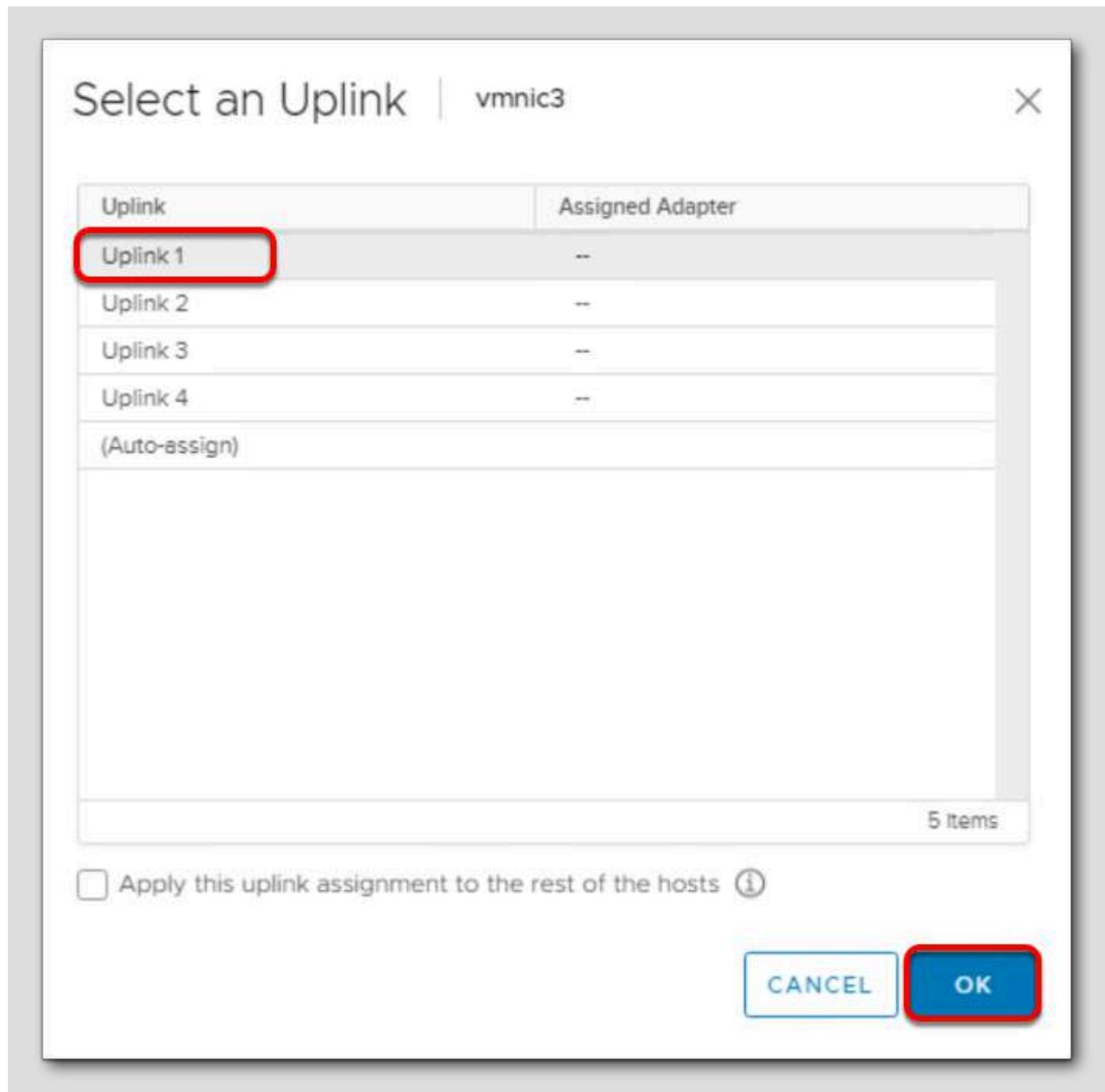
The screenshot shows the 'DSwitch - Add and Manage Hosts' interface. On the left, a sidebar lists steps: 1 Select task, 2 Select hosts, 3 Manage physical adapters (highlighted in blue), 4 Manage VMkernel adapt..., 5 Migrate VM networking, and 6 Ready to complete. The main area is titled 'Manage physical adapters' with the sub-instruction 'Add or remove physical network adapters to this distributed switch.' Below this is a table listing host/network adapter information. The table has columns: Host/Physical Network Adapters, In Use by Switch, Uplink, and more (partially visible). The table lists several entries, with 'vmnic3' being highlighted by a red box and circled with '1'. To the right of 'vmnic3' is the 'Assign uplink' button, which is also highlighted by a red box and circled with '2'. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Host/Physical Network Adapters	In Use by Switch	Uplink
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--
vmnic3	New-vDS	--
esx-02a.corp.local		
On this switch		
On other switches/unclaimed		
vmnic0	RegionA01-vDS-CO...	--
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--
vmnic3	New-vDS	--

Part of the "Add Host" process involves assigning one or more network adapters from each host to the Distributed Switch. The assigned adapters may not be shared with any other switch in the host.

1. Select vmnic3
2. Click Assign uplink

Select an Uplink for vmnic3



1. Select Uplink 1
2. Click OK

Confirm Addition

DSwitch - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Manage physical adapters
Add or remove physical network adapters to this distributed switch.

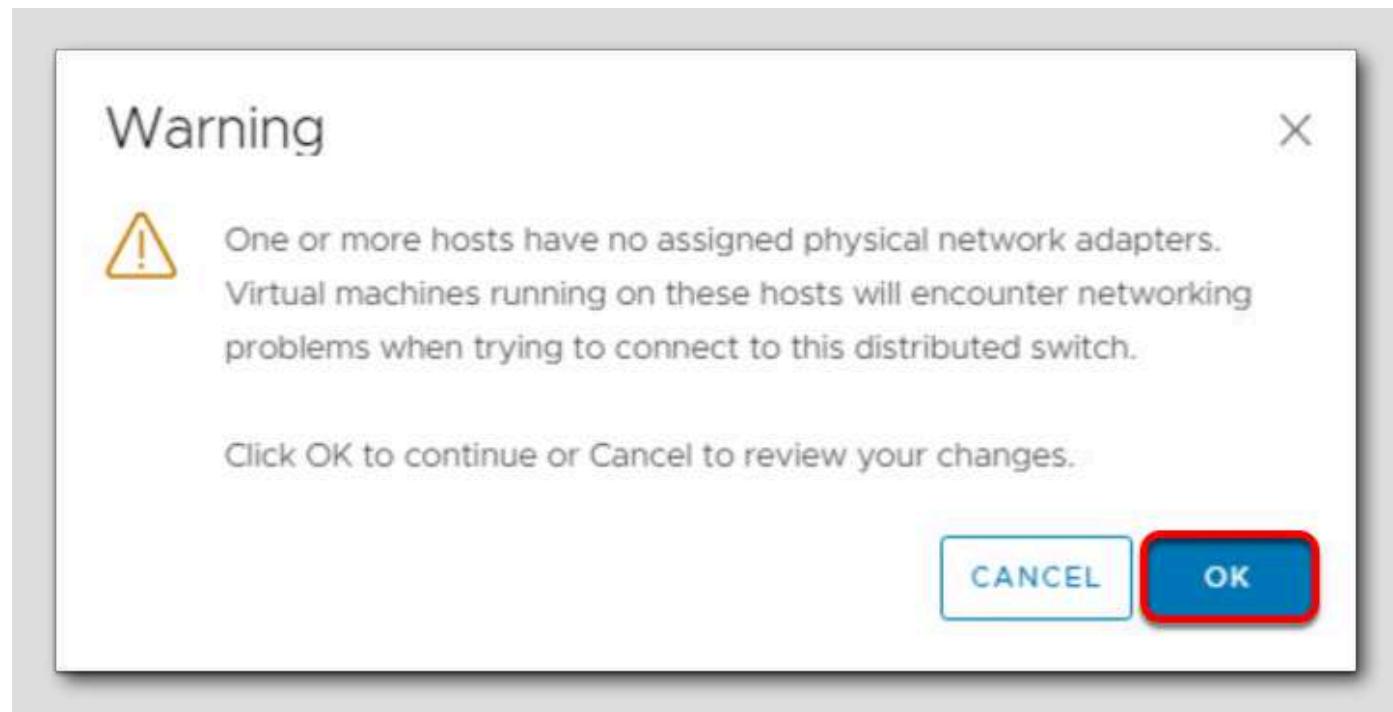
Assign uplink Unassign adapter View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	U...
esx-01a.corp.local			
On this switch			
vmnic3 (Assigned)	New-vDS	Uplink 1	D...
On other switches/unclaimed			
vmnic0	RegionA01-vDS-CO...	--	--
vmnic1	RegionA01-vDS-CO...	--	--
vmnic2	vSwitch0	--	--
esx-02a.corp.local			
On this switch			
On other switches/unclaimed			

CANCEL BACK **NEXT**

1. vmnic3 is assigned and click Next to continue

Warning message



If you did not add a vmnic from each ESXi host, you will receive this warning.

1. Click **OK** to continue

Manage virtual network adapters

DSwitch - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
✓ 3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Manage VMkernel adapters
Manage and assign VMkernel network adapters to the distributed switch.

Assign port group Reset changes View settings

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
esx-01a.corp.local			
On this switch			
On other switches/unclaimed			
vmk0	RegionA01-v...	ESXi-RegionA01-v...	Do not migrate
vmk1	RegionA01-v...	Storage-RegionA0...	Do not migrate
vmk2	RegionA01-v...	vMotion-RegionA0...	Do not migrate
esx-02a.corp.local			
On this switch			
On other switches/unclaimed			
vmk0	RegionA01-v...	ESXi-RegionA01-v...	Do not migrate
vmk1	RegionA01-v...	Storage-RegionA0...	Do not migrate

CANCEL BACK **NEXT**

In your environment, you may choose to migrate virtual network adapters from a vSphere Standard or Distributed switch to this new one. In this lab example, we won't move anything.

1. Click **Next** to continue

Migrate VM Networking

DSwitch - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
✓ 3 Manage physical adapters
✓ 4 Manage VMkernel adapt...
✓ 5 Migrate VM networking
6 Ready to complete

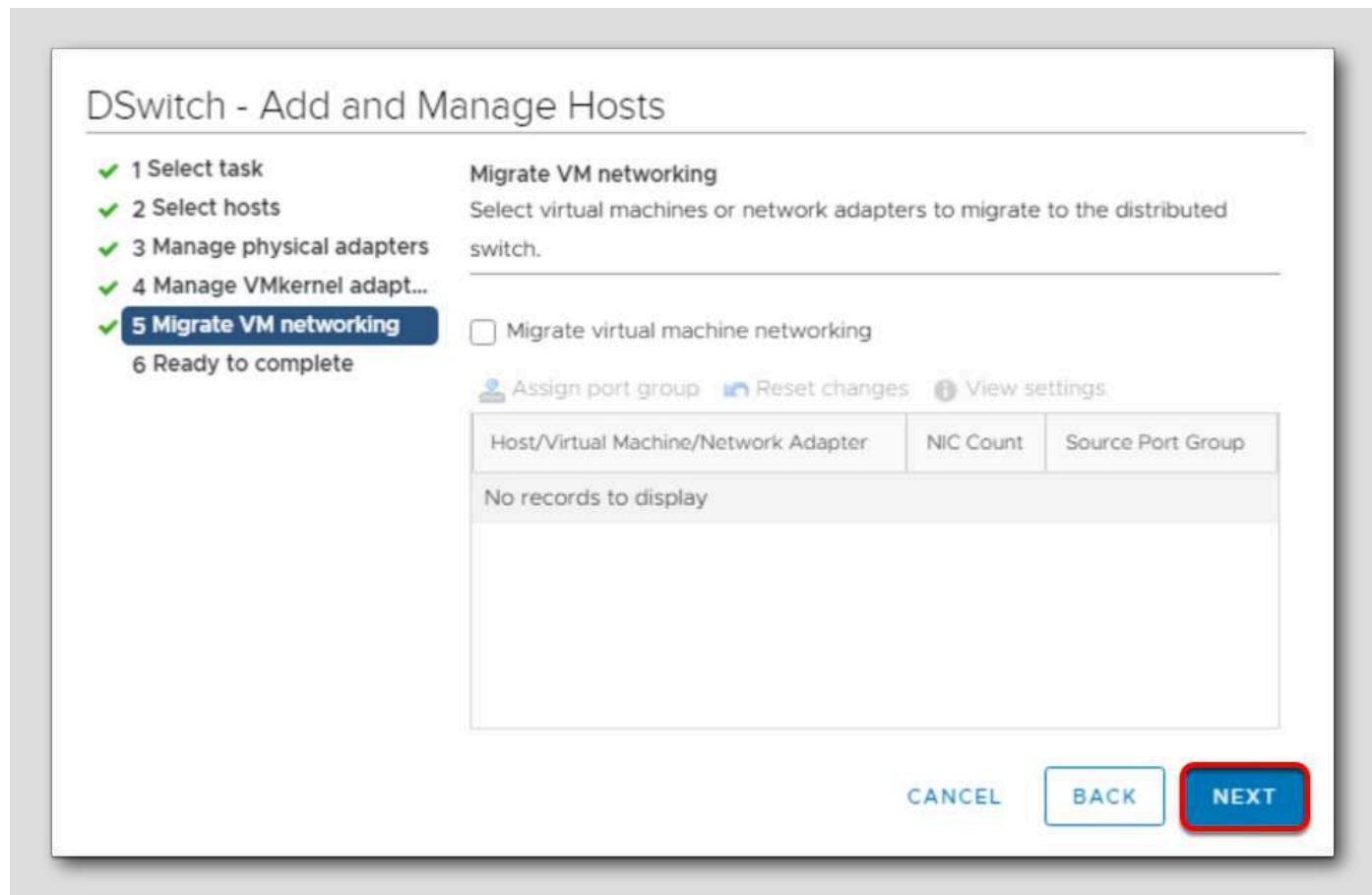
Migrate VM networking
Select virtual machines or network adapters to migrate to the distributed switch.

Migrate virtual machine networking

Assign port group Reset changes View settings

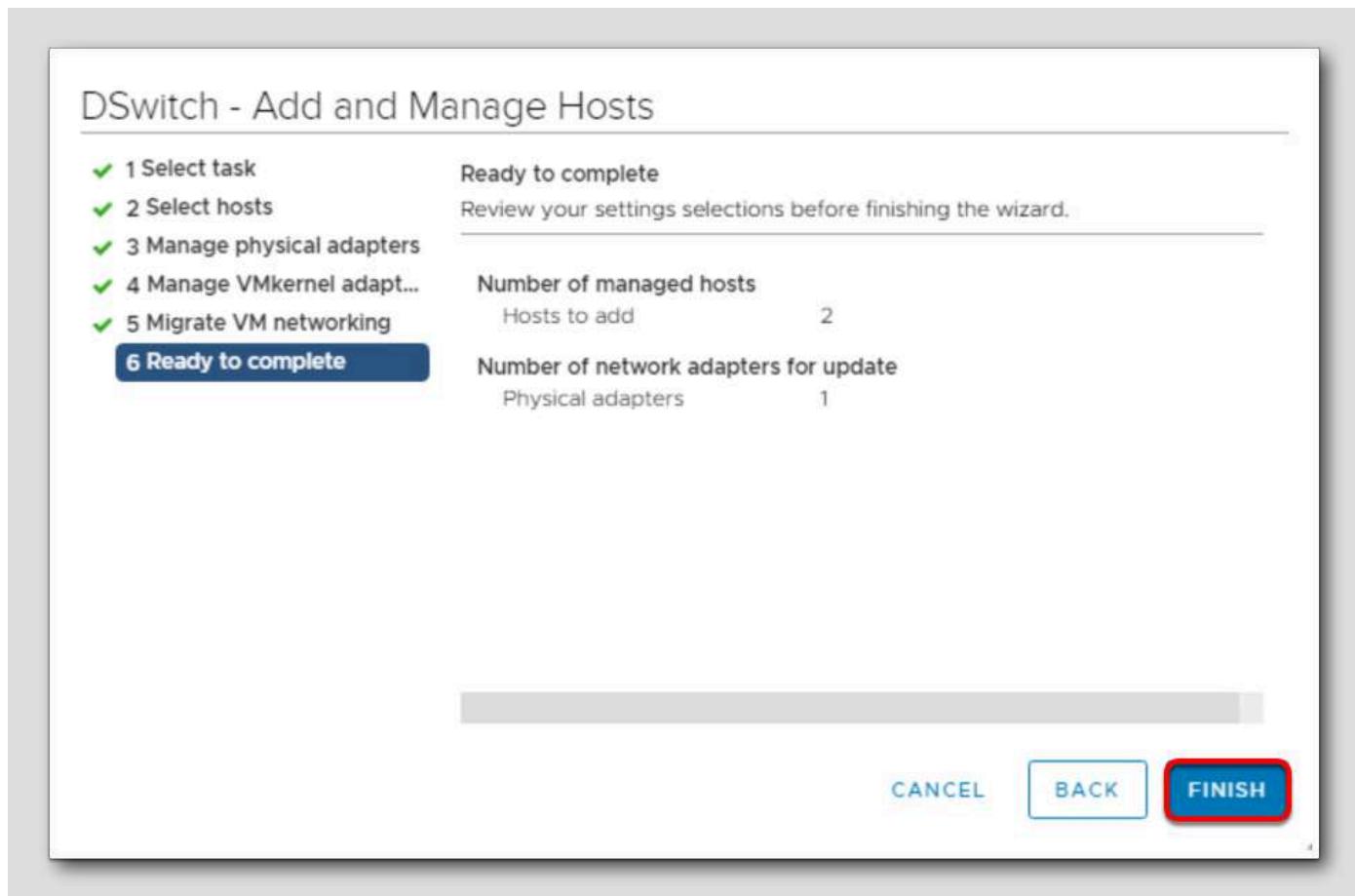
Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group
No records to display		

CANCEL BACK **NEXT**



1. Click **Next** to continue

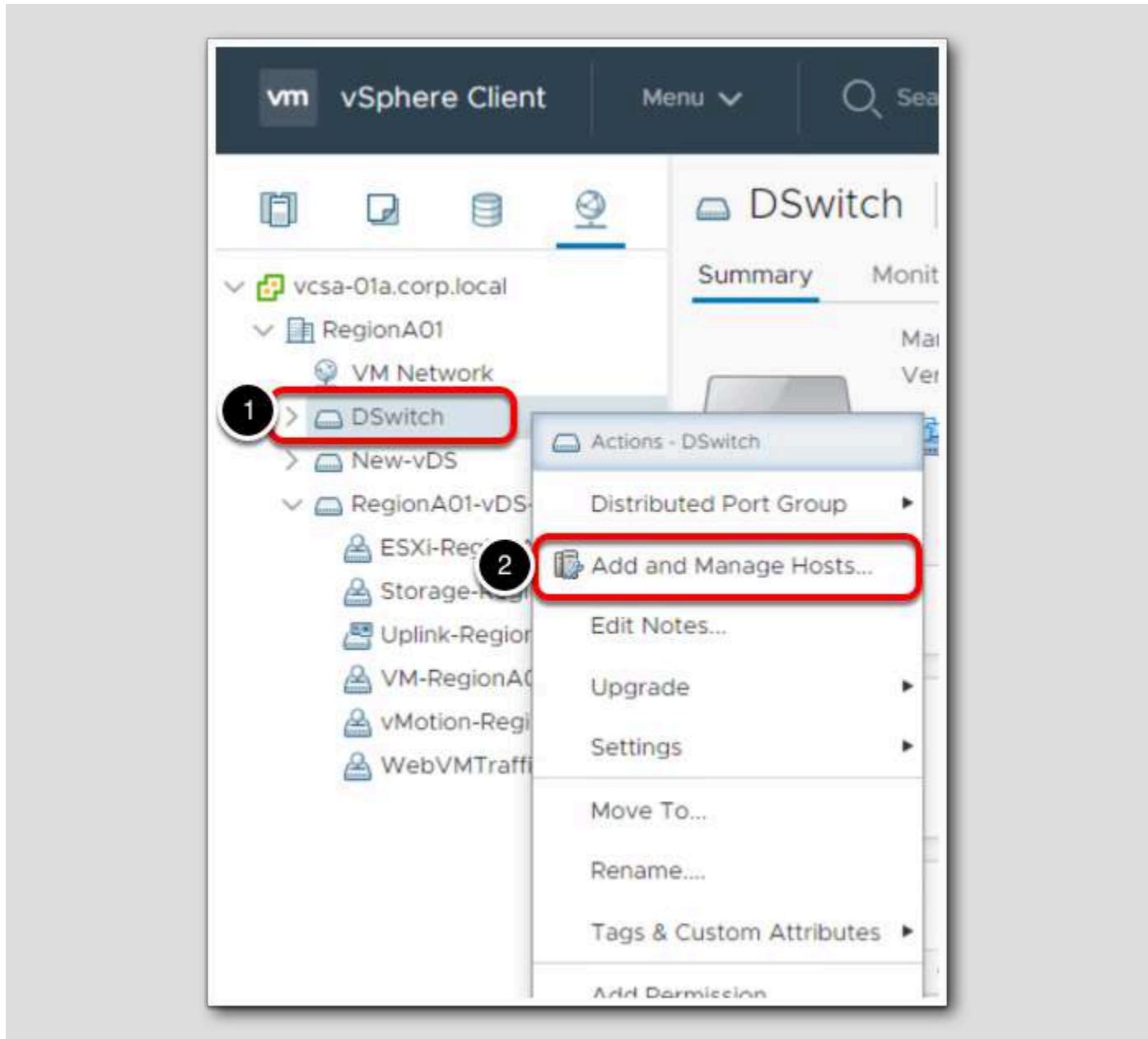
Ready to complete



You are now asked to verify the changes you are about to make.

1. Click Finish to commit the changes

Manage Hosts on a vSphere Distributed Switch in the vSphere Web Client



You can change the configuration for hosts and physical adapters on a vSphere Distributed Switch after they are added to the distributed switch.

1. Right-click DSwitch in the navigator
2. Select Add and Manage Hosts.

Select Task

DSwitch - Add and Manage Hosts

1 Select task

- 2 Select hosts
- 3 Manage physical adapters
- 4 Manage VMkernel adapt...
- 5 Migrate VM networking
- 6 Ready to complete

1

Select task
Select a task to perform on this distributed switch.

Add hosts
Add new hosts to this distributed switch.

Manage host networking
Manage networking of hosts attached to this distributed switch.

Remove hosts
Remove hosts from this distributed switch.

2

CANCEL BACK **NEXT**

The screenshot shows a software interface for managing a distributed switch. It consists of three main sections: a sidebar with a list of tasks, a detailed view of the selected task, and a footer with navigation buttons. The sidebar has six items: 'Select hosts', 'Manage physical adapters', 'Manage VMkernel adapt...', 'Migrate VM networking', 'Ready to complete', and 'Select task' (which is highlighted in blue). The 'Select task' section contains a sub-section titled 'Select task' with the instruction 'Select a task to perform on this distributed switch.' It lists three options: 'Add hosts', 'Manage host networking', and 'Remove hosts'. The 'Manage host networking' option is selected (indicated by a checked radio button) and is enclosed in a red box. Below it is a detailed description: 'Manage networking of hosts attached to this distributed switch.' At the bottom of the 'Select task' section are 'CANCEL' and 'BACK' buttons. In the center of the screen is a large 'NEXT' button, also enclosed in a red box. The number '1' is circled in black next to the 'Manage host networking' option, and the number '2' is circled in black next to the 'NEXT' button.

1. On the 'Select tasks' page, select **Manage host networking**

2. Click **Next**

Select hosts

DSwitch - Add and Manage Hosts

✓ 1 Select task
2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt
5 Migrate VM networking
6 Ready to complete

Select hosts
Select hosts to manage their networking on this distributed switch.

Attached hosts... ① Remove

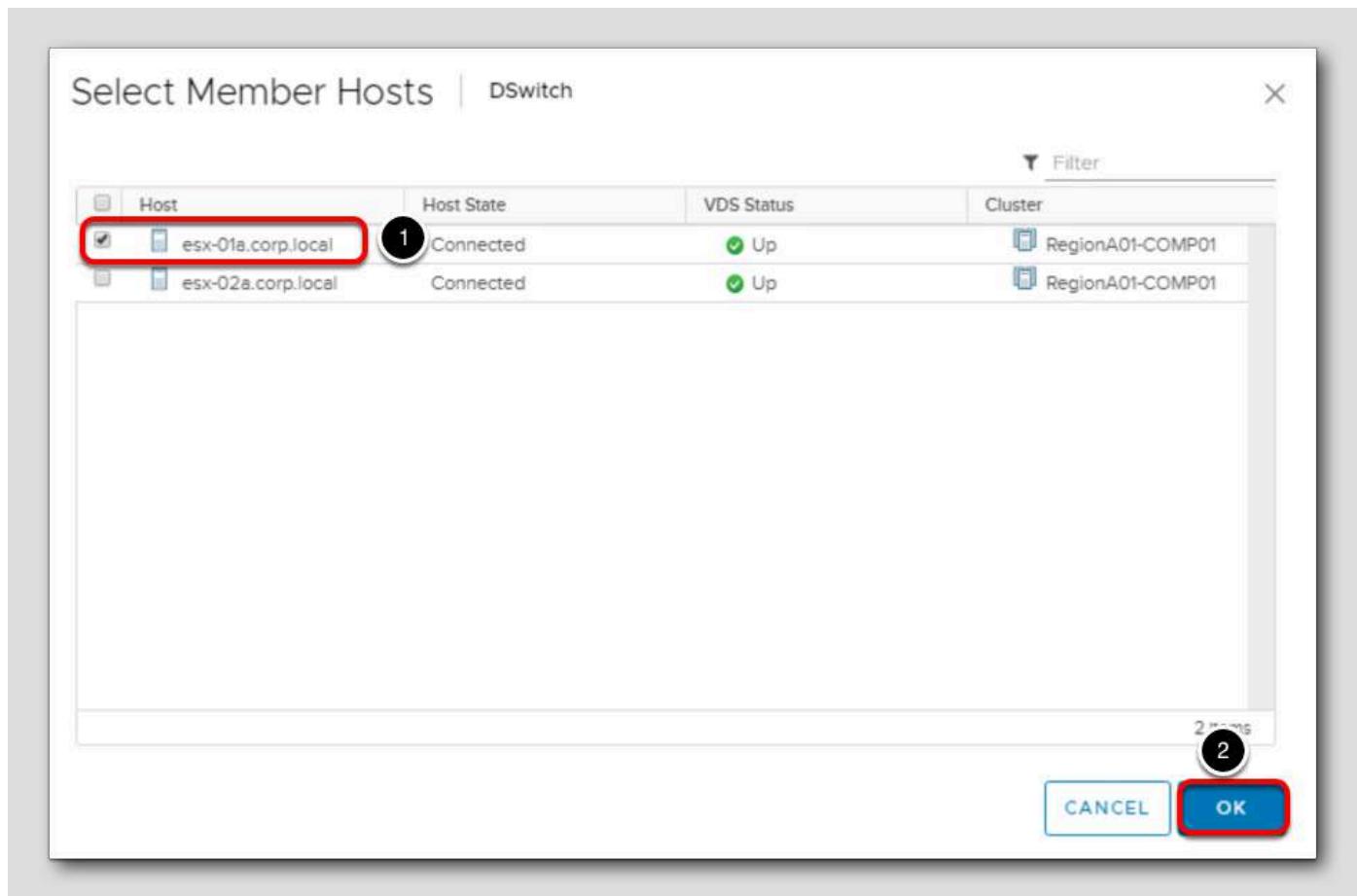
Host	Host Status
No items to display	

CANCEL BACK NEXT

The screenshot shows a step-by-step wizard titled 'DSwitch - Add and Manage Hosts'. Step 2, 'Select hosts', is active. A callout points to the green '+' icon next to 'Attached hosts...', which is circled in red with the number 1. Below the table, a note says 'No items to display'.

1. Click the green '+' to select the hosts to work with.

Select member hosts



1. On the "Select member hosts" page, select esx-01a.corp.local
2. Click OK

Select hosts (cont.)

DSwitch - Add and Manage Hosts

✓ 1 Select task
2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Select hosts
Select hosts to manage their networking on this distributed switch.

+ Attached hosts... X Remove

Host	Host Status
esx-01a.corp.local	Connected

1 esx-01a.corp.local
2

CANCEL BACK **NEXT**

1. You should now see **esx-01a.corp.local** added
2. Click **Next**

Manage physical network adapters

DSwitch - Add and Manage Hosts

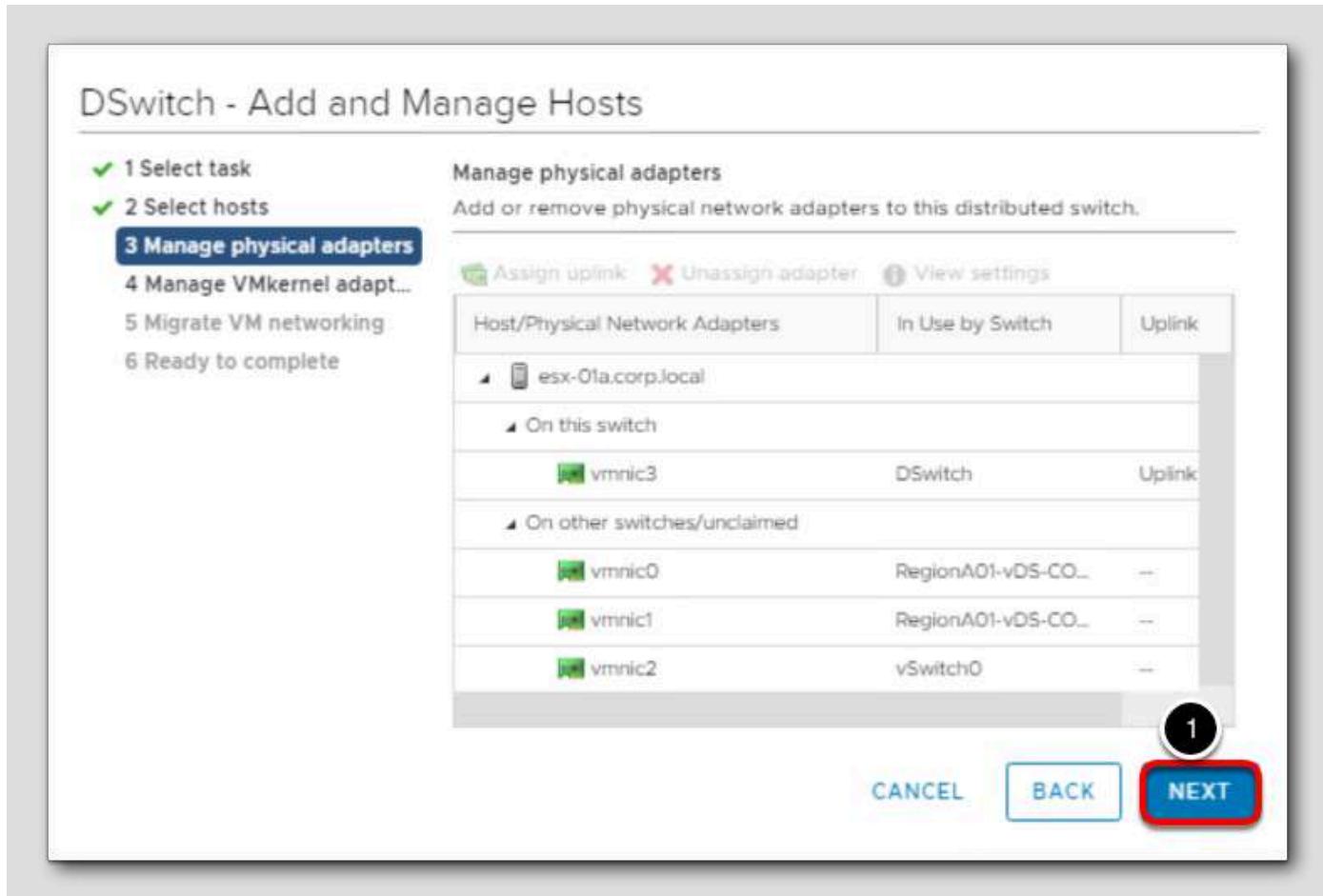
✓ 1 Select task
✓ 2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Manage physical adapters
Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink
esx-01a.corp.local		
On this switch		
vmnic3	DSwitch	Uplink
On other switches/unclaimed		
vmnic0	RegionA01-vDS-CO...	--
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--

1

CANCEL BACK **NEXT**



1. Click Next to continue

Manage VMKernel Adapters

DSwitch - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
✓ 3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

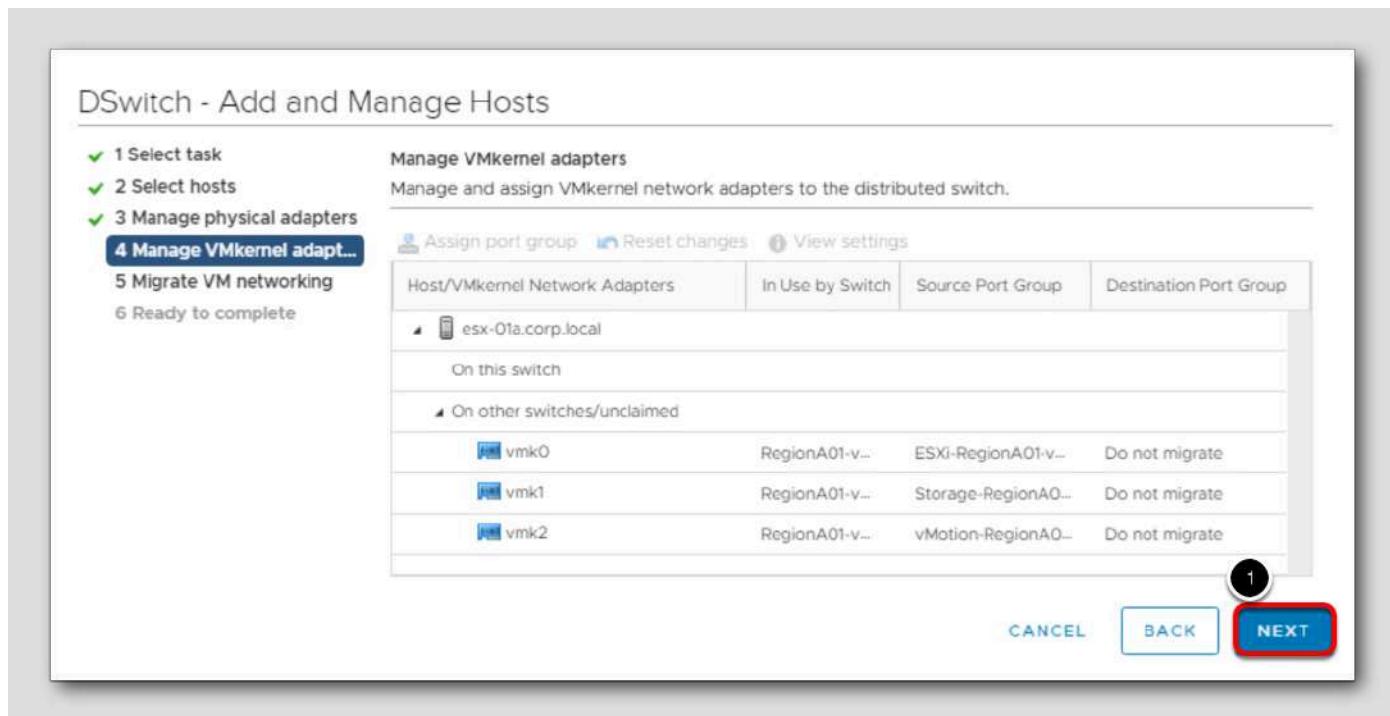
Manage VMkernel adapters
Manage and assign VMkernel network adapters to the distributed switch.

Assign port group Reset changes View settings

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
esx-01a.corp.local			
On this switch			
On other switches/unclaimed			
vmk0	RegionA01-v...	ESXi-RegionA01-v...	Do not migrate
vmk1	RegionA01-v...	Storage-RegionA0...	Do not migrate
vmk2	RegionA01-v...	vMotion-RegionA0...	Do not migrate

1

CANCEL BACK **NEXT**



Migrate VM Networking

DSwitch - Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
✓ 3 Manage physical adapters
✓ 4 Manage VMkernel adapt...
✓ 5 Migrate VM networking
6 Ready to complete

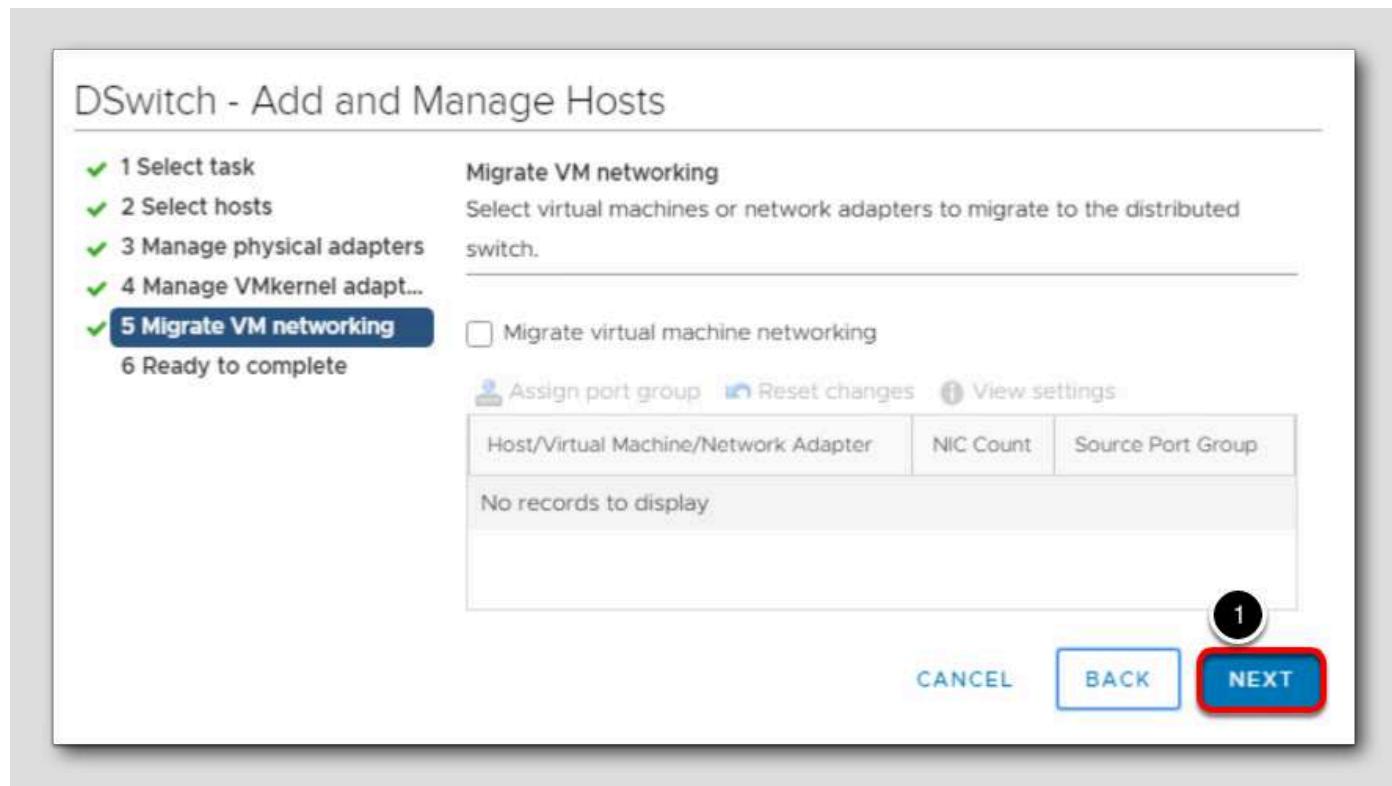
Migrate VM networking
Select virtual machines or network adapters to migrate to the distributed switch.

Migrate virtual machine networking

Assign port group Reset changes View settings

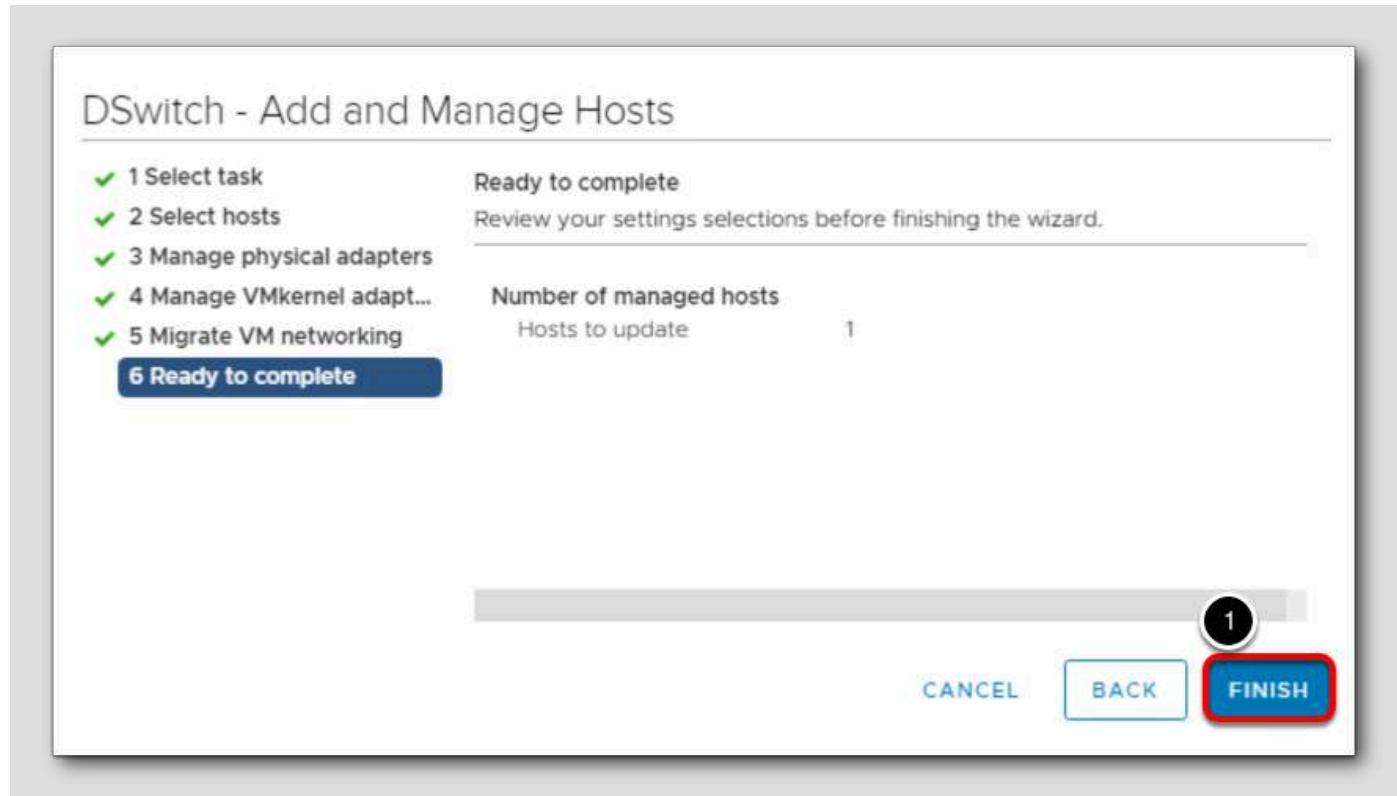
Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group
No records to display		

1 CANCEL BACK **NEXT**



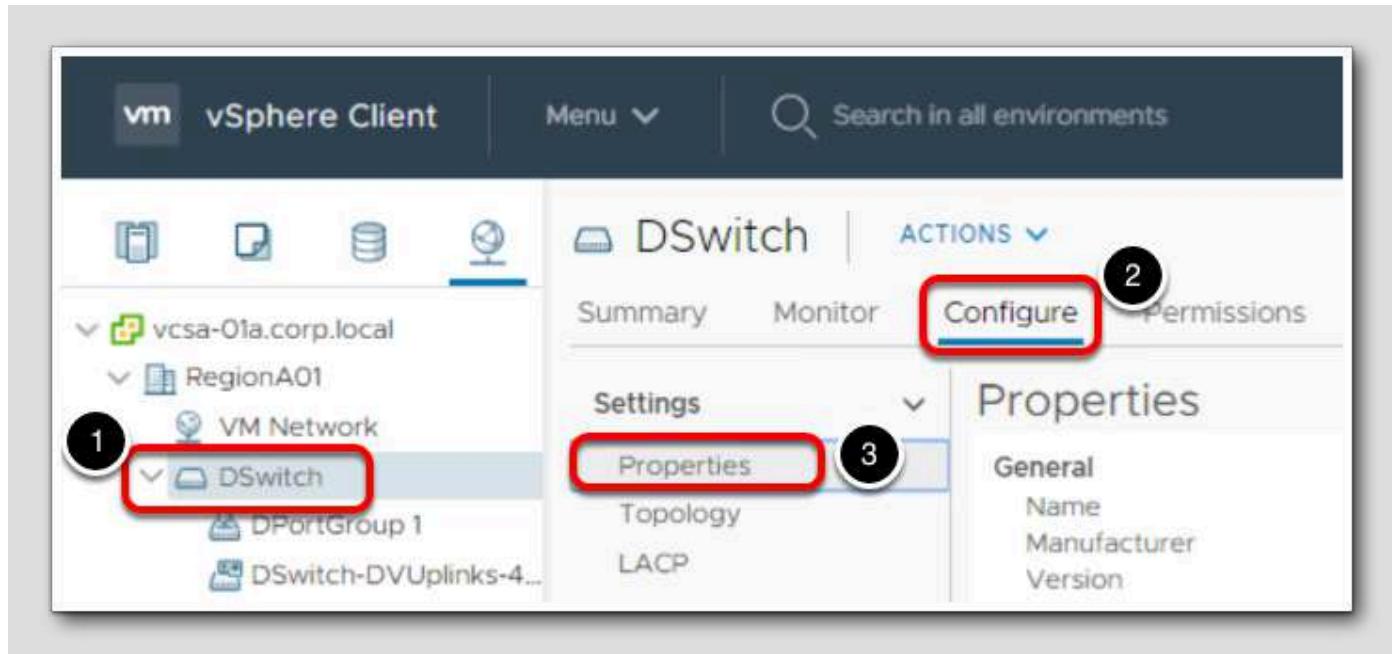
1. Click **Next** to continue

Ready to complete



1. Click Finish

Edit General and Advanced vSphere Distributed Switch Settings in the vSphere Web Client



General settings for a vSphere Distributed Switch include the distributed switch name and the number of uplink ports on the distributed switch. Advanced settings for a vSphere Distributed Switch include the Discovery Protocol configuration and the maximum MTU for the switch. Both general and advanced settings can be configured using the vSphere Web Client.

1. Make sure the DSwitch is selected under the Navigator pane
2. Click the Configure tab
3. Click Properties, under Settings

Edit the switch properties

The screenshot shows the vSphere Web Client interface for managing network switches. The main title is "DSwitch". The top navigation bar includes "Summary", "Monitor", "Configure" (which is underlined, indicating it's the active tab), "Permissions", "Ports", "Hosts", "VMs", and "Networks". On the left, a sidebar titled "Settings" has sections for "Properties" (which is selected and highlighted in grey), "Topology", "LACP", "Private VLAN", "NetFlow", "Port Mirroring", "Health Check", and "Resource Allocation" (which has sub-options like "System traffic", "Network resource pools", and "Alarm Definitions"). The main content area is titled "Properties" and contains three sections: "General", "Advanced", and "Discovery protocol". The "General" section includes fields for Name (DSwitch), Manufacturer (VMware, Inc.), Version (7.0.0), Number of uplinks (4), Number of ports (16), and Network I/O Control (Enabled). The "Advanced" section includes MTU (1500 Bytes) and Multicast filtering mode (IGMP/MLD snooping). The "Discovery protocol" section includes Type (Cisco Discovery Protocol) and Operation (Listen). A red box highlights the "Edit..." button in the top right corner of the properties table, with the number "1" above it.

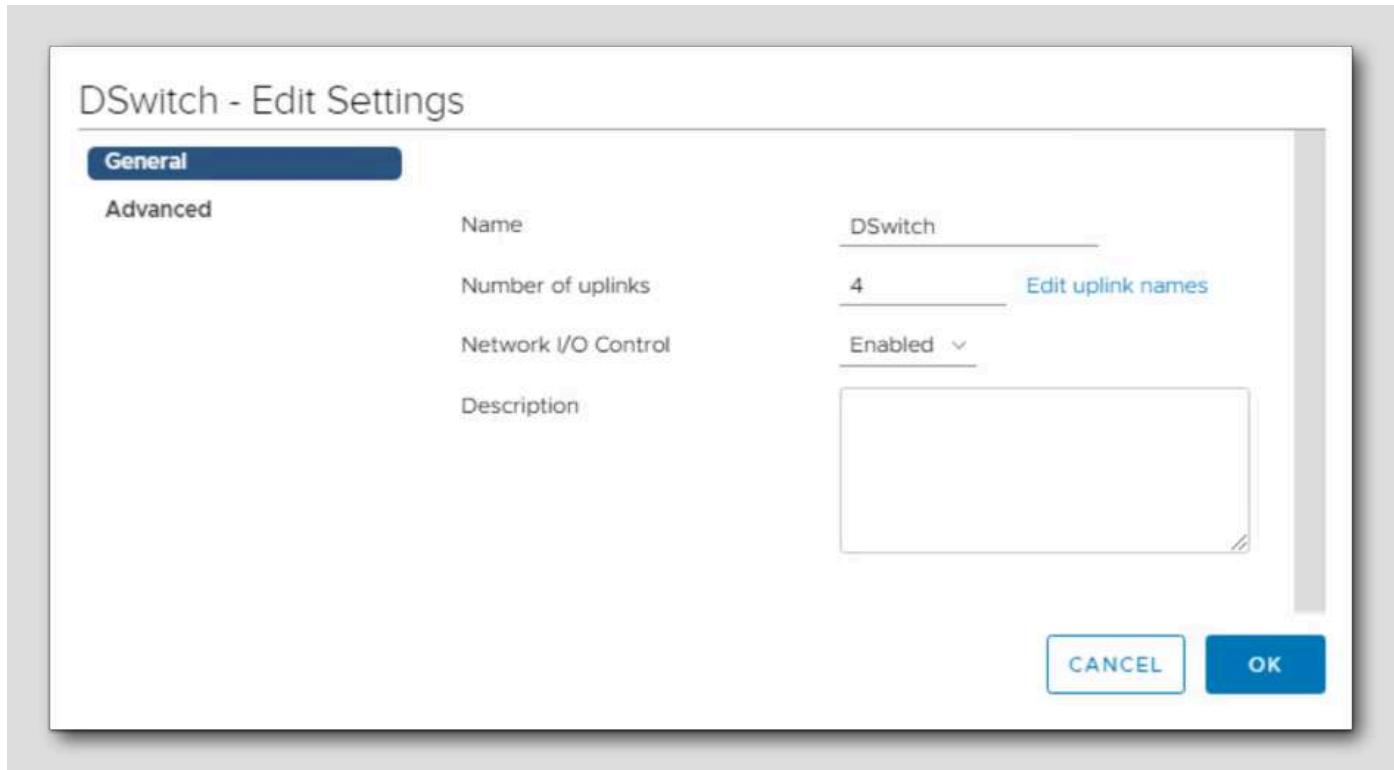
General	
Name	DSwitch
Manufacturer	VMware, Inc.
Version	7.0.0
Number of uplinks	4
Number of ports	16
Network I/O Control	Enabled

Advanced	
MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

Discovery protocol	
Type	Cisco Discovery Protocol
Operation	Listen

1. Click Edit

General Settings



Click General to view the vSphere distributed switch settings. Here you can modify the following:

Name: You can modify the name of your distributed switch.

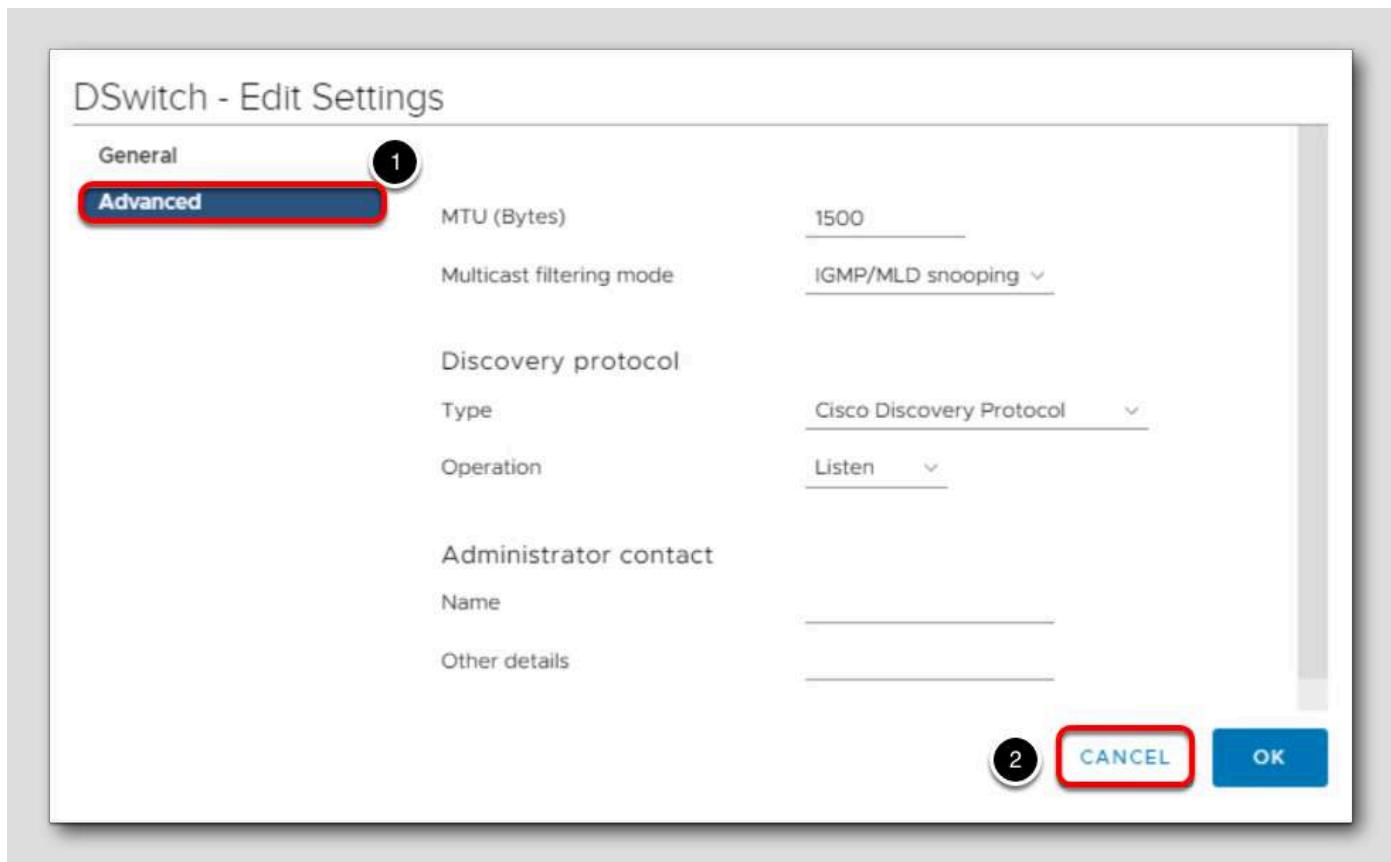
Number of Uplinks: Increase or decrease the number uplink ports attached to the distributed switch. Note that you can also click the Edit uplink names button to give the uplinks meaningful names.

Number of Ports: This setting cannot be modified. The port count will dynamically be scaled up or down by default.

Network I/O Control: You can use the drop-down menu to enable or disable Network I/O Control on the switch.

Description: You can use this field to give a meaningful description of the switch.

Advanced Settings



1. Click Advanced to view the vSphere distributed switch settings. Here you will find the following advanced settings for the switch:

MTU (Bytes): Maximum MTU size for the vSphere Distributed Switch. To enable jumbo frames, set a value greater than 1500 bytes. Make sure you check with your Networking team prior to modifying this setting in your environment.

Multicast filtering mode

- Basic - The distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group.
- IGMP/MLD snooping - The distributed switch forwards multicast traffic to virtual machines according to the IPv4 and IPv6 addresses of subscribed multicast groups by using membership messages defined by the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery protocol.

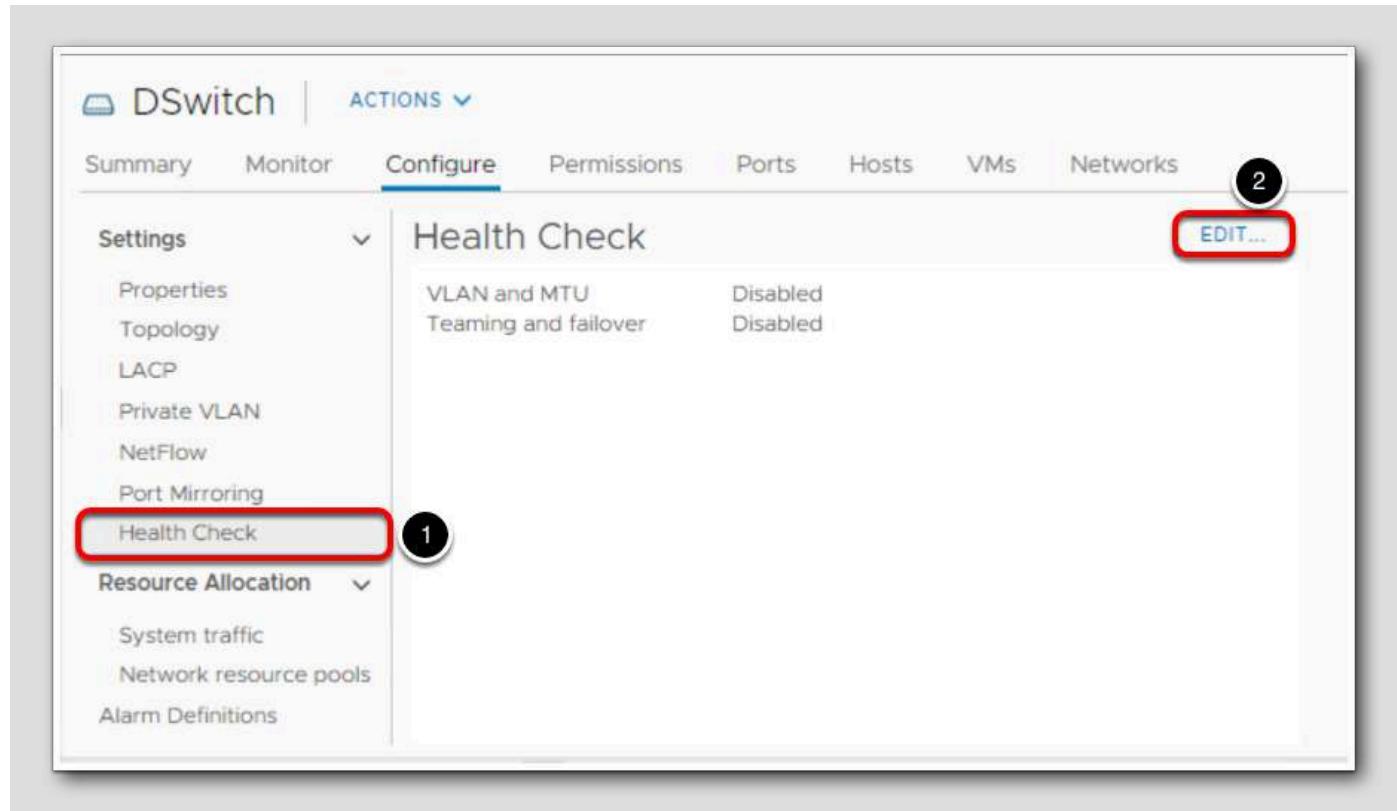
Discovery Protocol

- Type - Cisco Discovery Protocol, Link Layer Discovery Protocol, or disabled..
- Operation - to Listen, Advertise, or Both.

Administrator Contact: Type the name and other details of the administrator for the distributed switch.

1. We don't want to make any changes here, just click **Cancel**.

Enable or Disable vSphere Distributed Switch Health Check in the vSphere Web Client

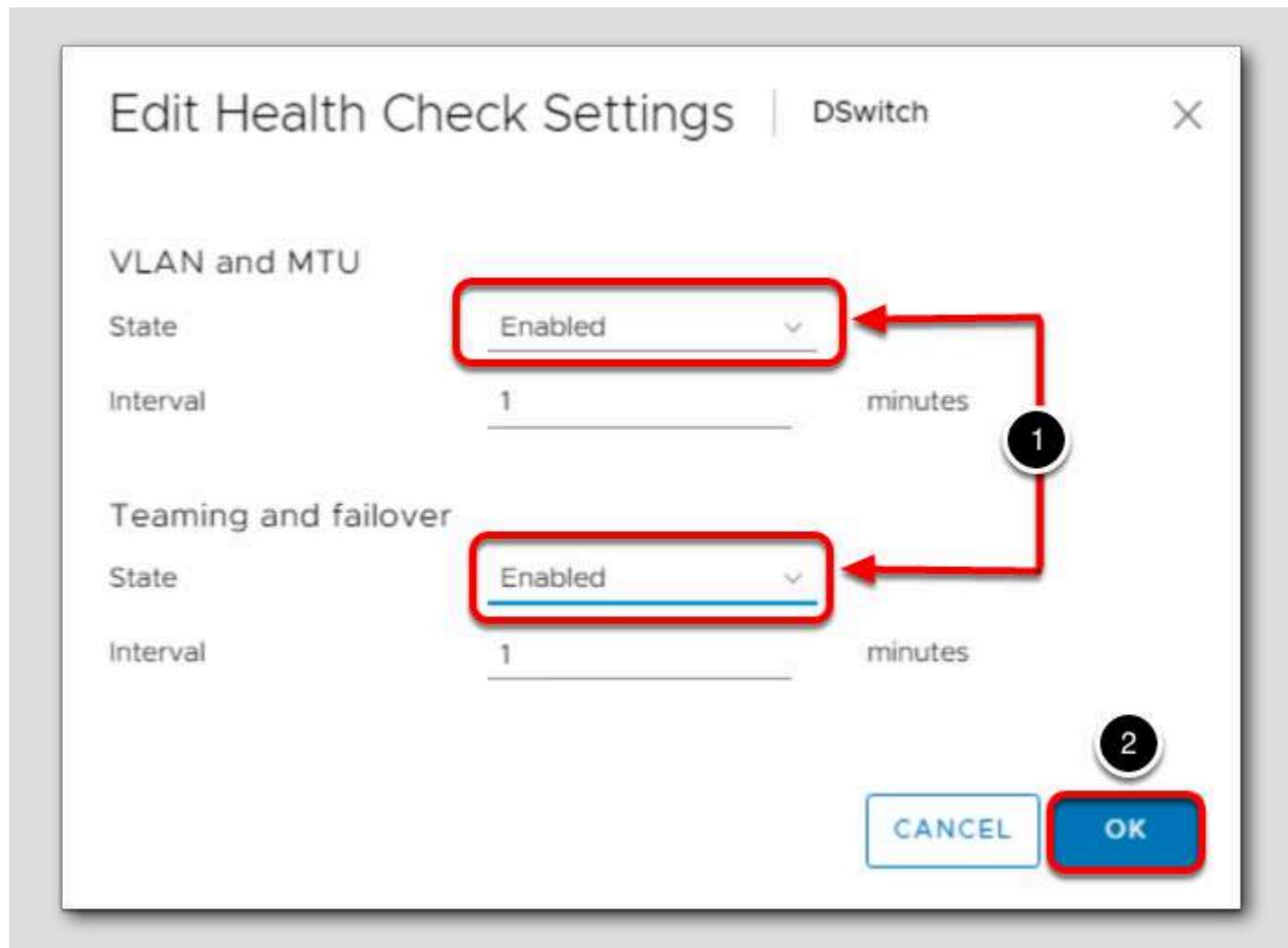


The Distributed Switch Health Check monitors for changes in vSphere Distributed Switch configurations. You must enable vSphere Distributed Switch Health Check to perform checks on Distributed Switch configurations.

Health Check is available on ESXi 5.1 Distributed Switches and higher. Also, you can only view Health Check information through the vSphere Web Client 5.1 or later.

1. Click on the Health check tab for DSwitch. We can see that Health check is disabled for VLAN and MTU as well as Teaming and failover.
2. Click the Edit button

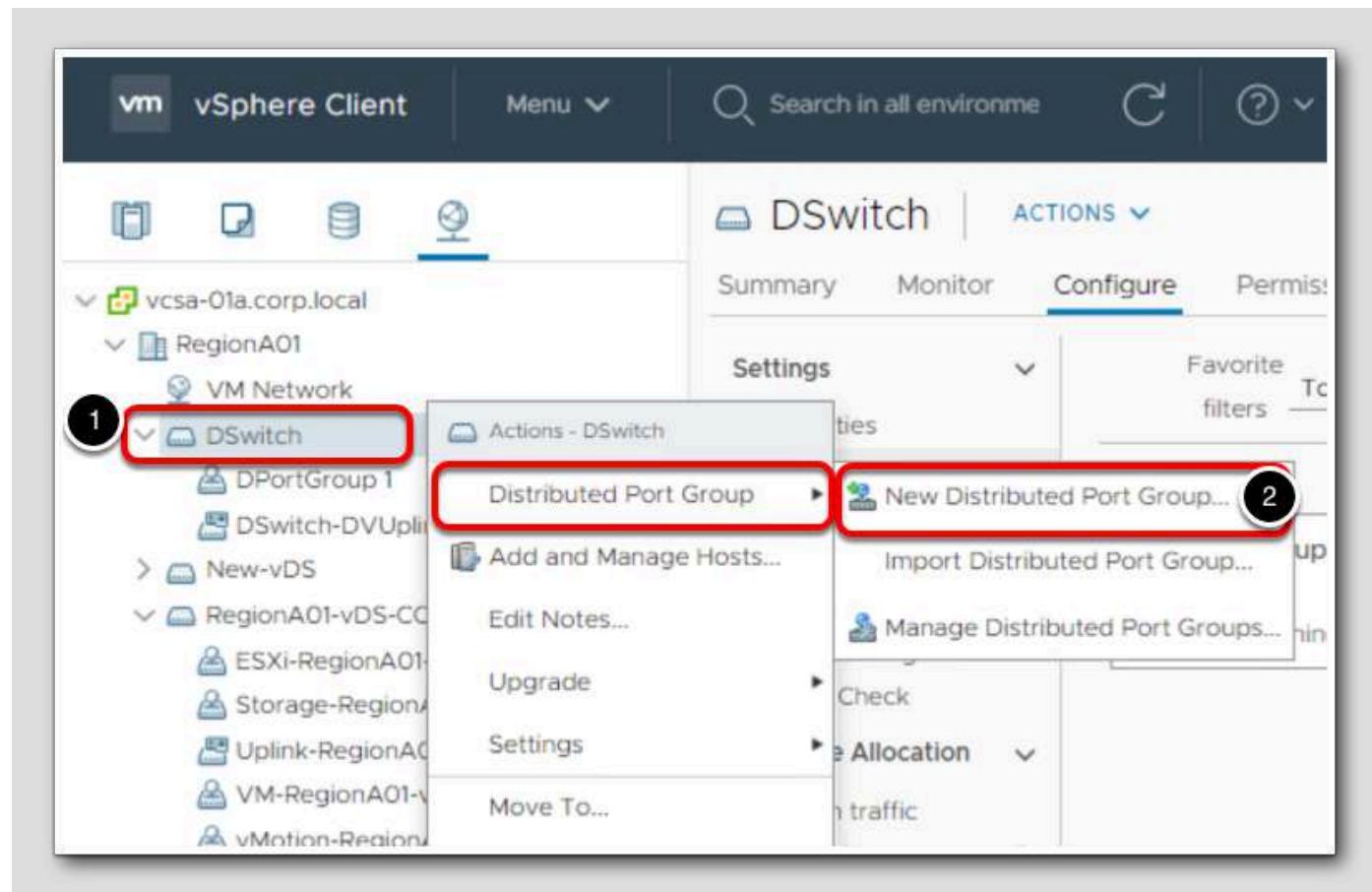
Edit Health Check Settings



1. Select Enabled for both

2. Click OK

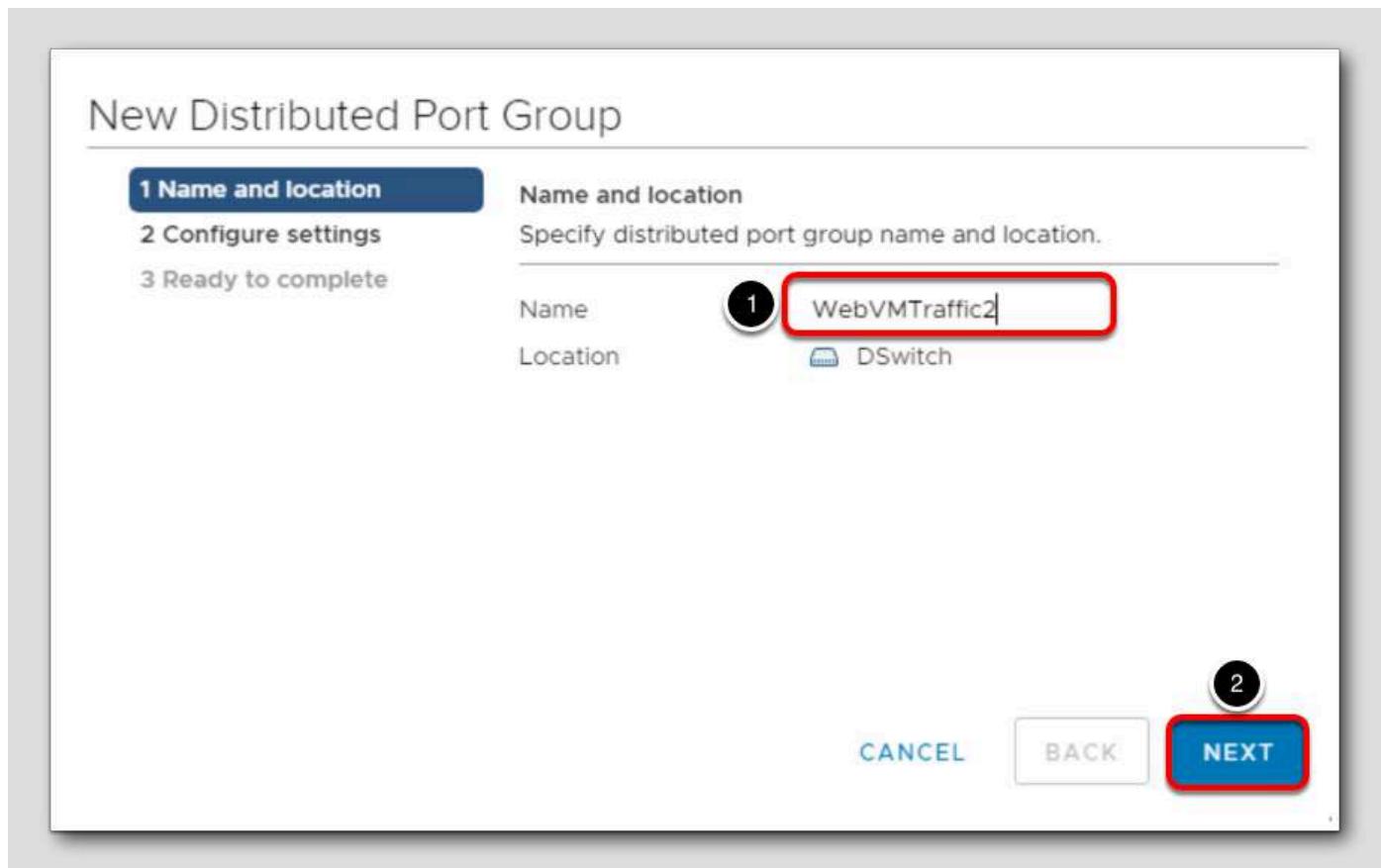
Distributed Port Groups



A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

1. Right-click the DSwitch in the navigator
2. Select Distributed Port Group and then click New Distributed Port Group

Select name and location section



1. Name the new port group **WebVMTraffic2**

2. Click **Next**

Configure settings

New Distributed Port Group

✓ 1 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 (i)
Number of ports	8
Network resource pool	(default)

VLAN

VLAN type	None
-----------	------

Advanced

Customize default policies configuration

1

CANCEL BACK **NEXT**

1. Keep default settings and click **Next**

When creating a Distributed Port Group, you have the following options available:

Port binding - Choose when ports are assigned to virtual machines connected to this distributed port group.

- Static binding - Assign a port to a virtual machine when the virtual machine connects to the distributed port group.
- Dynamic binding - Assign a port to a virtual machine the first time the virtual machine powers on after it is connected to the distributed port group. Dynamic binding has been deprecated since ESXi 5.0.
- Ephemeral - No port binding. You can assign a virtual machine to a distributed port group with ephemeral port binding also when connected to the host.

Port allocation

- Elastic - The default number of ports is eight. When all ports are assigned, a new set of eight ports is created. This is the default.
- Fixed - The default number of ports is set to eight. No additional ports are created when all ports are assigned.

Number of ports: Enter the number of ports on the distributed port group.

Network resource pool: If you have created network pool to help control network traffic, you can select it here.

VLAN: Use the Type drop-down menu to select VLAN options:

- None - Do not use VLAN.
- VLAN - In the VLAN ID field, enter a number between 1 and 4094.
- VLAN Trunking - Enter a VLAN trunk range.
- Private VLAN - Select a private VLAN entry. If you did not create any private VLANs, this menu is empty.

Advanced: Select this check box to customize the policy configurations for the new distributed port group.

Ready to complete

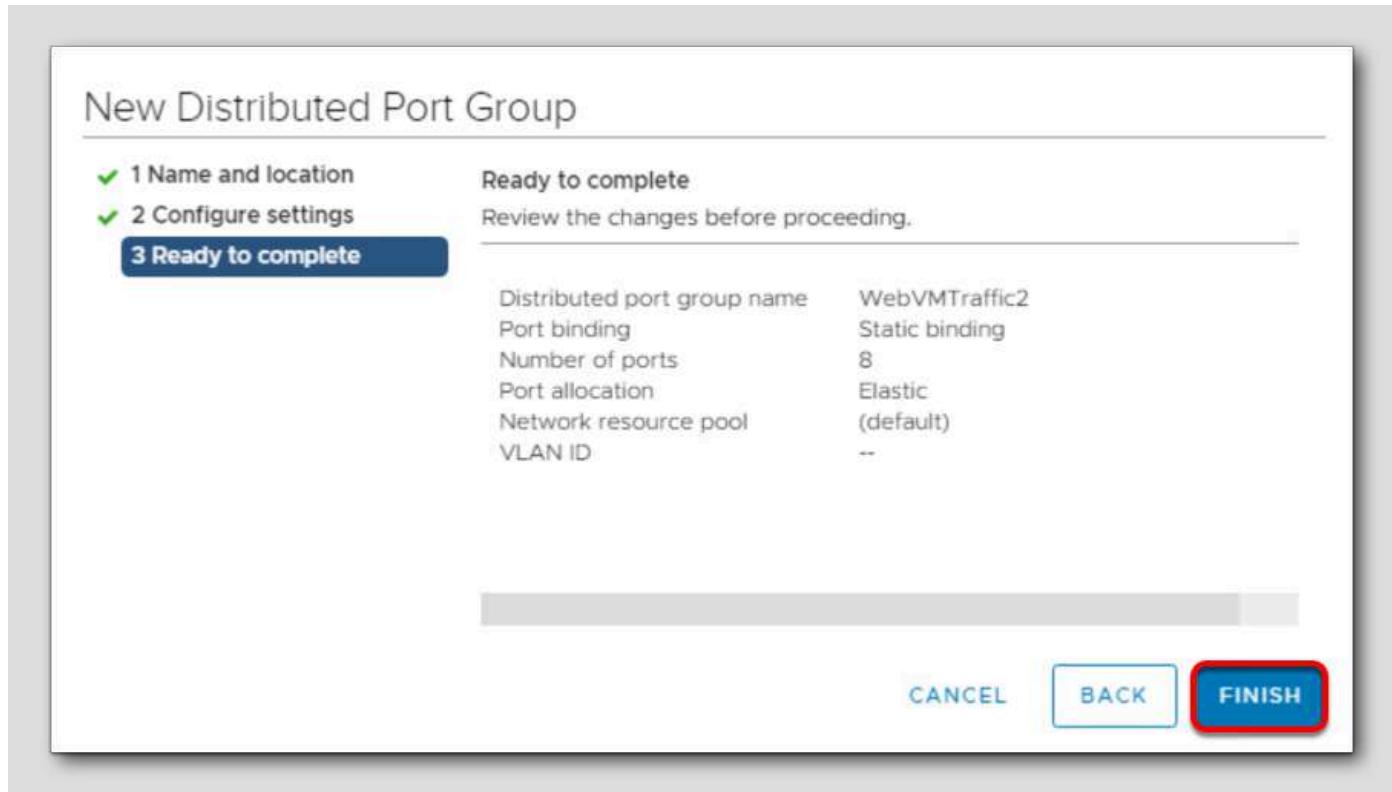
New Distributed Port Group

✓ 1 Name and location
✓ 2 Configure settings
3 Ready to complete

Ready to complete
Review the changes before proceeding.

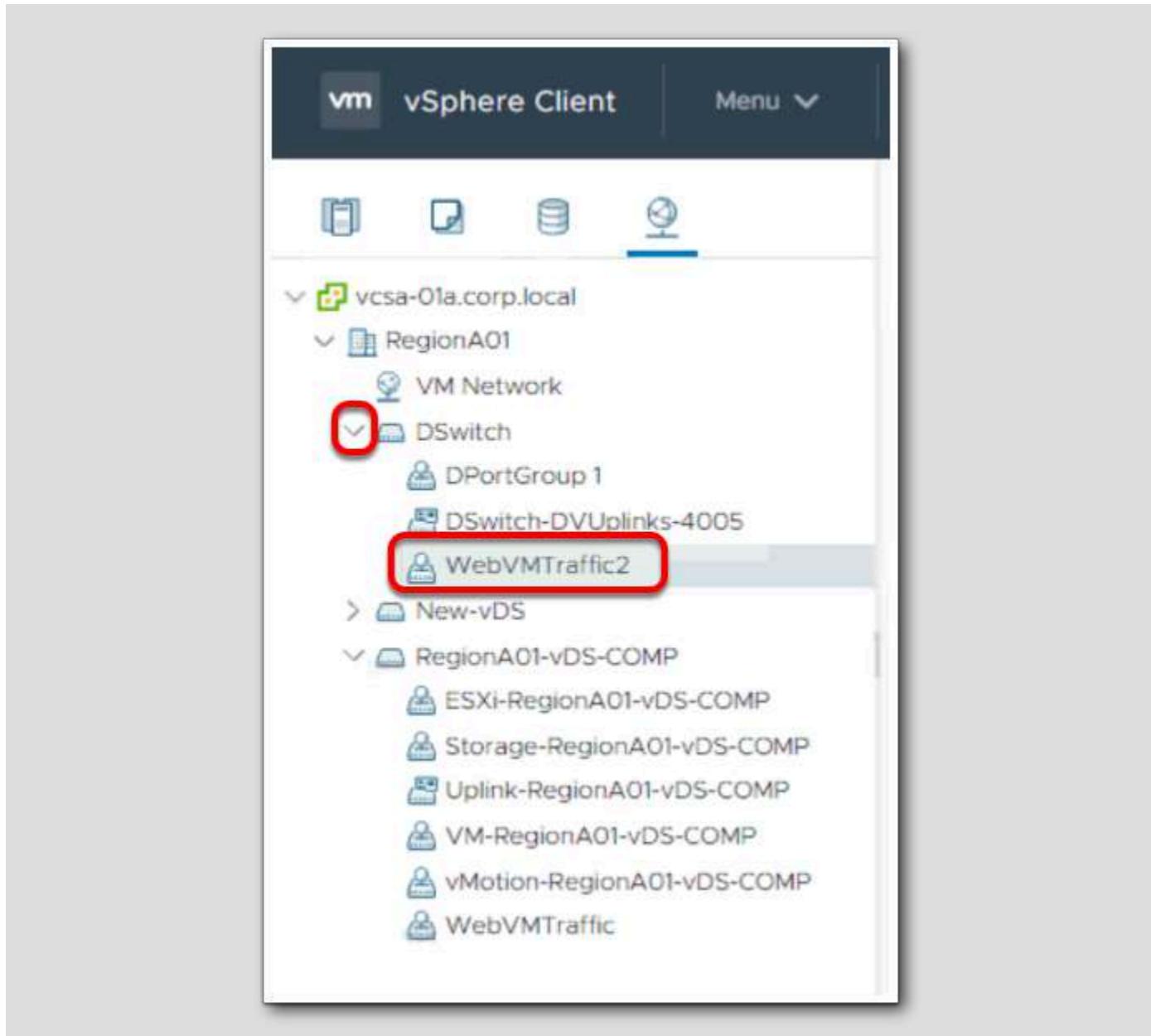
Distributed port group name	WebVMTraffic2
Port binding	Static binding
Number of ports	8
Port allocation	Elastic
Network resource pool	(default)
VLAN ID	--

CANCEL BACK FINISH



1. Review the settings and click **Finish**

View the new Distributed Port Group



In the Navigator, expand out DSwitch and you will see the newly created WebVMTraffic Distributed Port Group.

Using Host Lockdown Mode

To increase the security of your ESXi hosts, you can put them in lockdown mode.

When you enable lockdown mode, no users other than vpxuser have authentication permissions, nor can they perform operations against the host directly. Lockdown mode forces all operations to be performed through vCenter Server.

When a host is in lockdown mode, you cannot run vSphere CLI commands from an administration server, from a script or from vSphere Management Assistant (vMA) against the host. External software or management tools might not be able to retrieve or modify information from the ESXi host.

Lockdown mode is only available on ESXi hosts that have been added to vCenter Server. You can enable lockdown mode using the Add Host wizard to add a host to vCenter Server, using the vSphere Web Client to manage a host or using the Direct Console User Interface (DCUI).

NOTES:

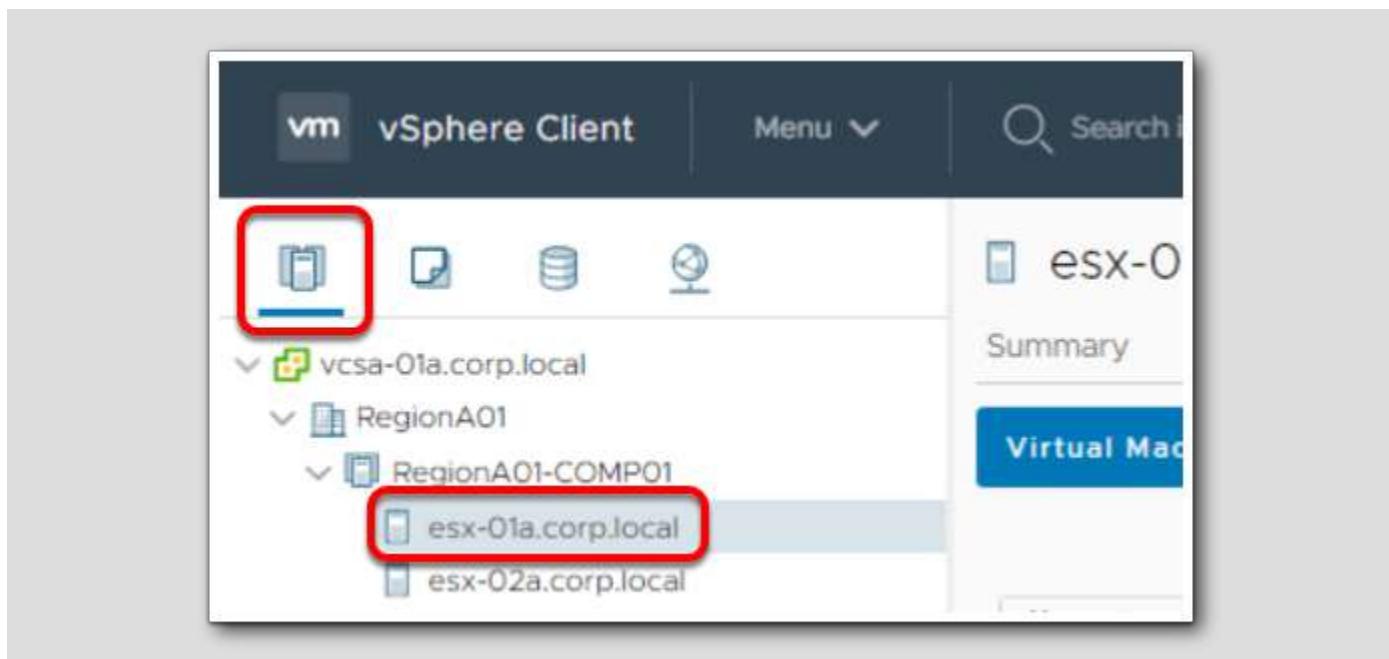
Users with the DCUI Access privilege are authorized to log in to the Direct Console User Interface (DCUI) when lockdown mode is enabled. When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host. The DCUI Access privilege is granted in Advanced Settings on the host.

If you enable or disable lockdown mode using the Direct Console User Interface (DCUI), permissions assigned to users and groups on the host are discarded. To preserve these permissions, you must enable and disable lockdown mode using the vSphere Client connected to vCenter Server.

Enabling or disabling lockdown mode affects which types of users are authorized to access host services, but it does not affect the availability of those services. In other words, if the ESXi Shell, SSH, or Direct Console User Interface (DCUI) services are enabled they will continue to run whether or not the host is in lockdown mode.

Select Hosts and Clusters

[360]



First, you will enable Host Lockdown Mode with the Normal setting on esx-01a.corp.local. This will mean the host will be accessible from vCenter and through the DCUI, but not remotely over SSH.

1. From the Navigator, select the Hosts and Clusters tab
2. Next, select esx-01a.corp.local

Security Profile

[361]

The screenshot shows the vSphere Web Client interface for the host esx-01a.corp.local. The top navigation bar includes tabs for Summary, Monitor, Configure (which is highlighted with a red box and has a circled '1' above it), Permissions, and VMS. A dropdown menu labeled 'PTIONS' is visible. The main content area is titled 'Services'. On the left, a sidebar lists various configuration options under 'System': Swap File Location, Licensing, Host Profile, Time Configuration, Authentication Servi.., Certificate, Power Management, Advanced System S..., vMotion Resource Re..., Firewall, Services (which is highlighted with a red box and has a circled '3' above it), Security Profile, System Swap, and Packages. The main pane displays a table of services with columns for Name, Restart, Start, and Stop. Services listed include Direct Console UI, ESXI Shell, SSH, Load-Based T...ing Daemon (with a circled '2' above it), Active Directory Service, NTP Daemon (highlighted with a red arrow), PC/SC Smart Card Daemon, CIM Server, and SNMP Server.

Before we configure Host Lockdown Mode, let's verify the SSH service is running on esx-01a.corp.local.

1. Clicking Configure tab
2. Scroll down until you find the **System** section
3. Click Services

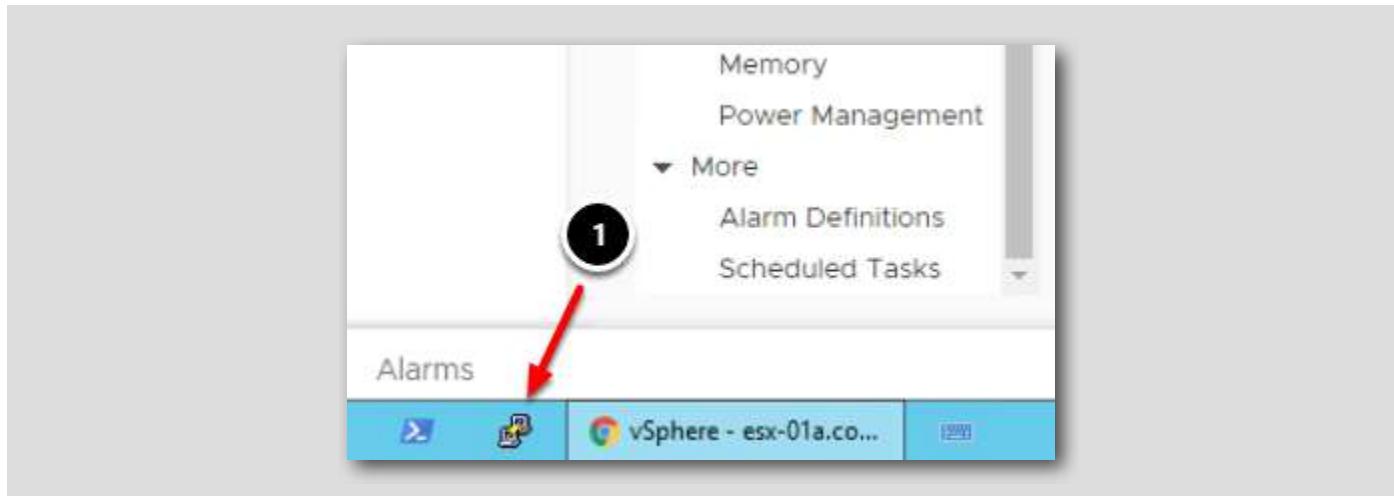
Verify SSH is Enabled

[362]

Name	Daemon	Startup Policy
Direct Console UI	Running	Start and stop with host
ESXI Shell	Stopped	Start and stop manually
SSH	Running	Start and stop with host
Load-Based Teaming Daemon	Running	Start and stop with host
Active Directory Service	Stopped	Start and stop manually
NTP Daemon	Running	Start and stop with host
PC/SC Smart Card Daemon	Stopped	Start and stop manually
CIM Server	Stopped	Start and stop with host
SNMP Server	Stopped	Start and stop with host
Syslog Server	Running	Start and stop with host
VMware vCenter Agent	Running	Start and stop with host
X.Org Server	Stopped	Start and stop with host

1. We can see that the SSH service is enabled and Running on esx-01a.corp.local

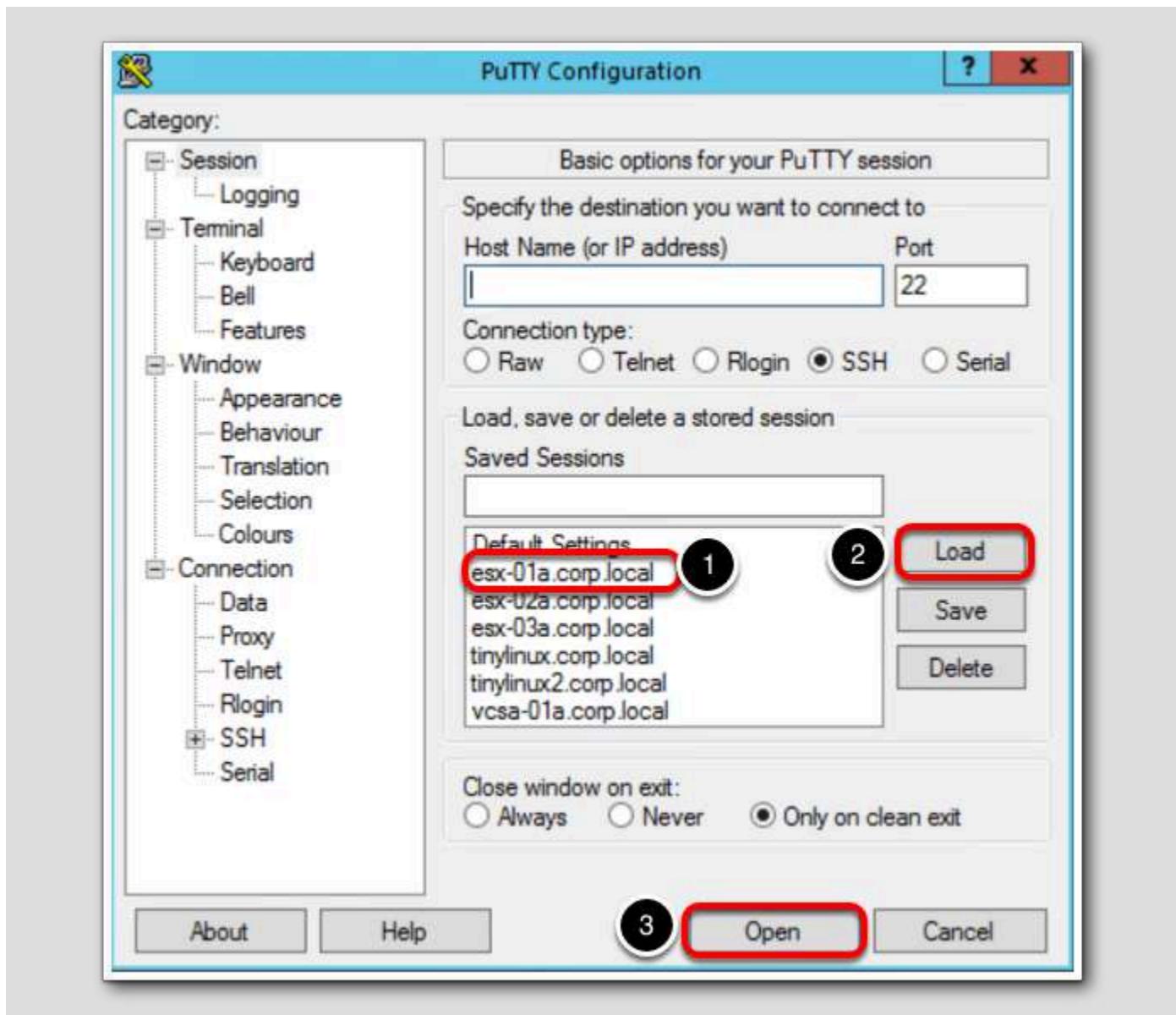
Open an SSH session to esx-01a



First, verify you can login to esx-01a using an SSH connection.

1. From the Windows Taskbar, click on the PuTTY icon

Connect to esx-01a



1. Under Saved Sessions, click on esx-01a.corp.local
2. Click Load
3. Click the Open button

Logged into esx-01a

The screenshot shows a PuTTY terminal window with the title bar 'esx-01a.corp.local - PuTTY'. The window contains the following text:

```
Using username "root".
Authenticating with public key "controlcenter" from agent
The time and date of this login have been sent to the system logs.

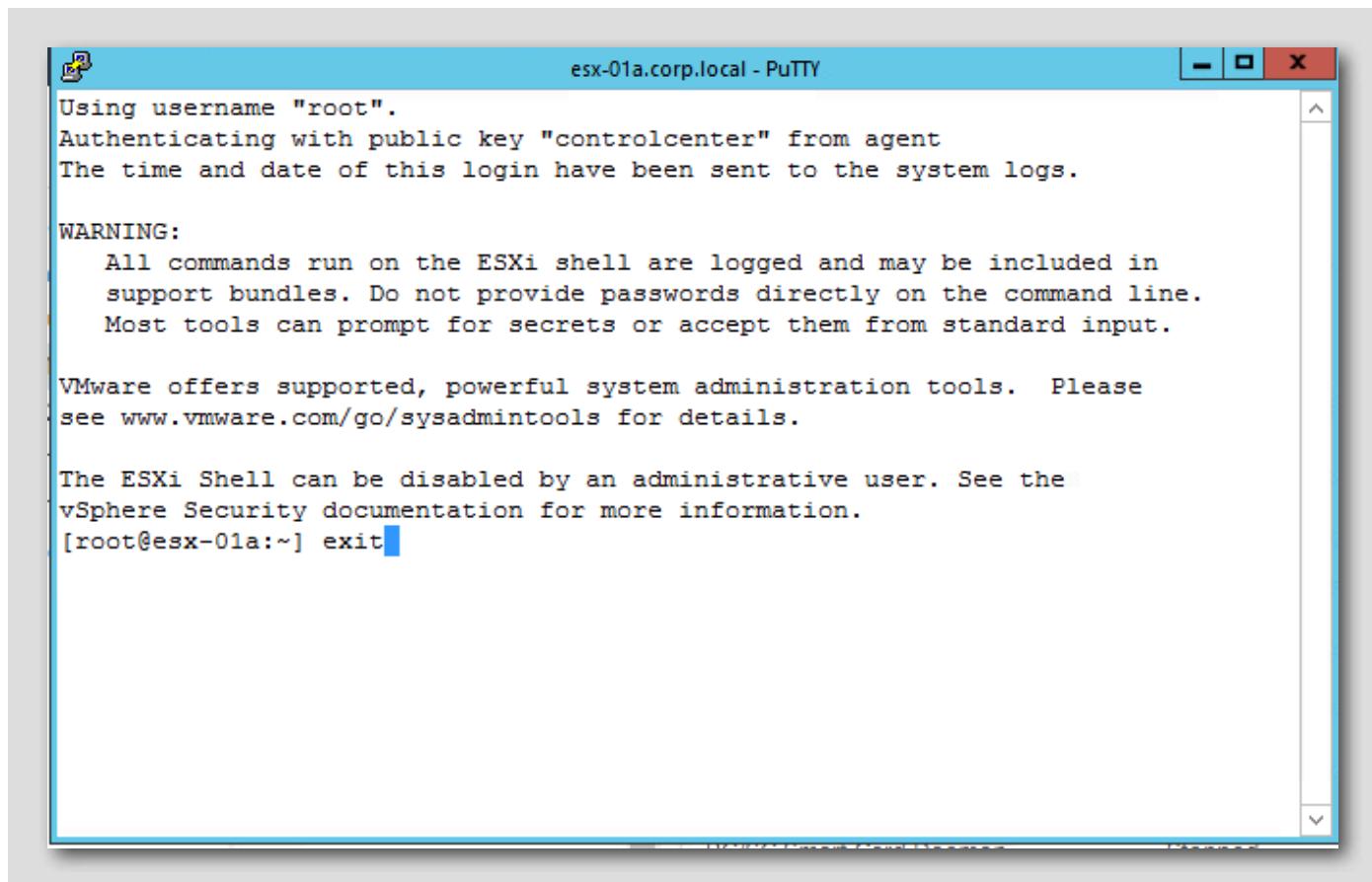
WARNING:
  All commands run on the ESXi shell are logged and may be included in
  support bundles. Do not provide passwords directly on the command line.
  Most tools can prompt for secrets or accept them from standard input.

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

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@esx-01a:~] 
```

You will be automatically logged in to esx-01a.corp.local because we have configured public-key authentication from the Main Console machine to the ESXi host.

Close the PuTTY Session



1. Close the PuTTY session by typing 'exit' and pressing Enter

Once you hit Enter, the PuTTY window will disappear.

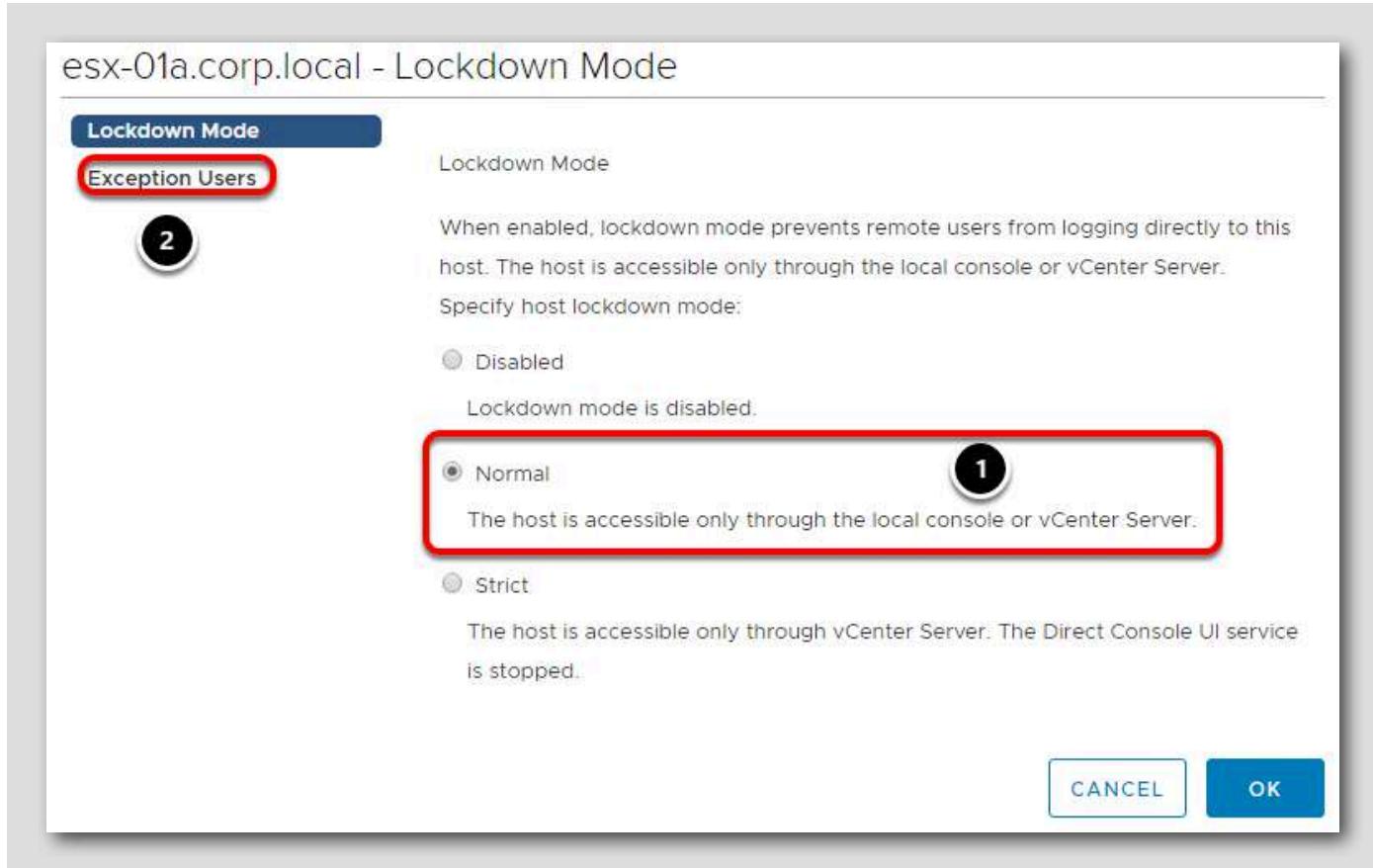
Enabling Lockdown Mode

The screenshot shows the vSphere Client interface for host 'esx-01a.corp.local'. The 'Configure' tab is selected. On the left, under 'System', the 'Security Profile' item is highlighted with a red box and a circled '1'. In the main pane, 'Lockdown Mode' is set to 'Disabled'. An 'EDIT...' button next to it is also highlighted with a red box and a circled '2'. Other sections visible include 'Host Image Profile Acceptance Level' and 'Host Encryption Mode'.

Go back to the vSphere Client

1. Click **Security Profile**
2. Click on the **Edit** button next to Lockdown Mode

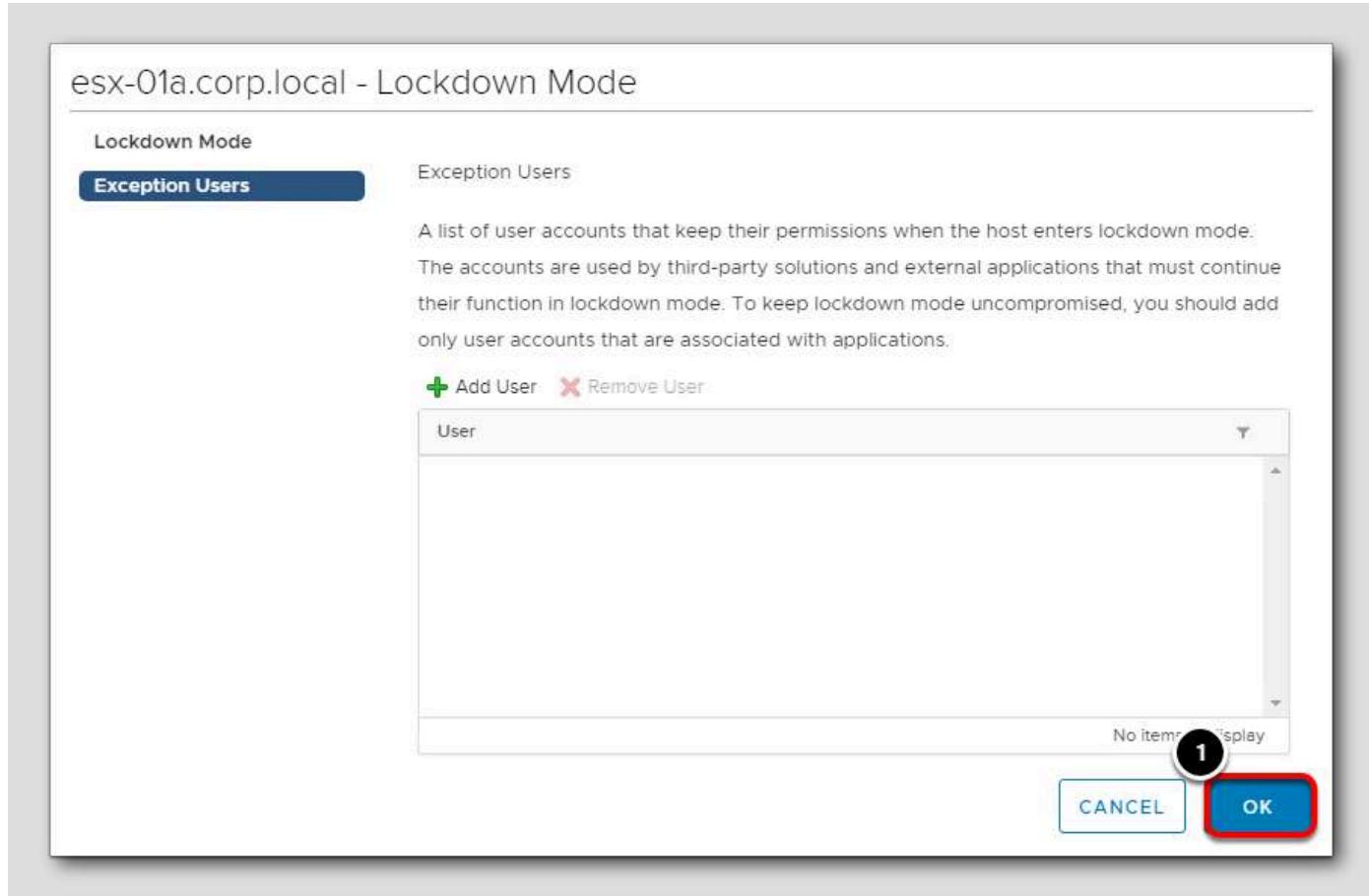
Lockdown Mode



Lockdown Mode is currently disabled. If we set it to Normal, we will not be able to access the host over SSH and only through vCenter or the local console (physically in front of the host). Lockdown Mode can also be set to Strict, meaning only vCenter can access the host and SSH and the local console are disabled.

1. Click the Normal radio button
2. Click on Exception Users

Exception Users



As previously noted, when Lockdown Mode is enabled, remote access to the host is disabled. Some third-party applications rely on this access and it can be granted by adding the accounts they use to the Exception List. This should not be a way for specific users to bypass security and should only be used for applications that require access.

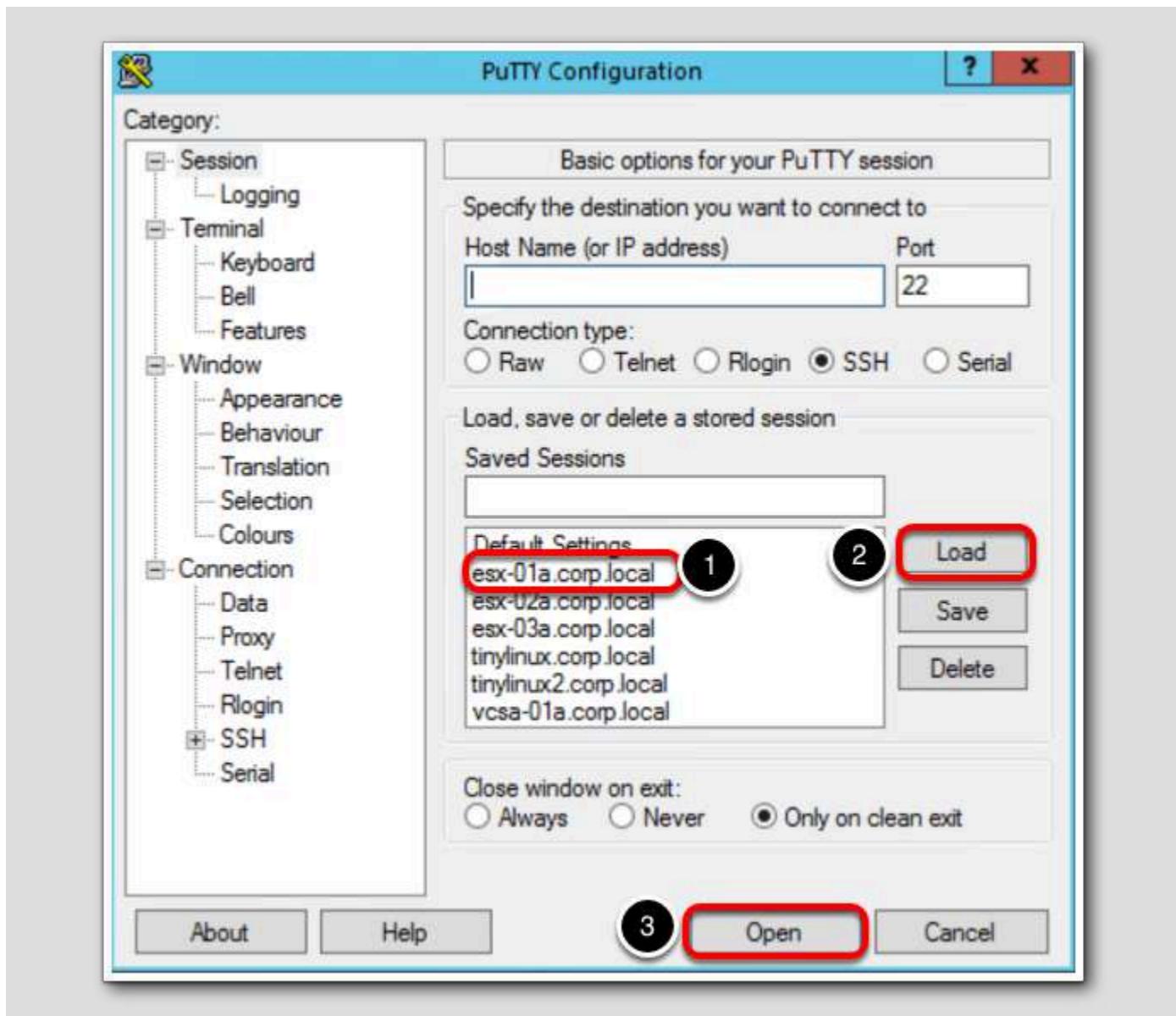
1. Click OK to enable Lockdown Mode

Lockdown Mode Enabled

The screenshot shows the vSphere Client interface for host `esx-01a.corp.local`. The navigation bar includes Summary, Monitor, Configure (selected), Permissions, VMs, Datastores, Networks, and Updates. The left sidebar under the System category lists Swap File Location, Licensing, Host Profile, Time Configuration, Authentication Servi..., Certificate, Power Management, Advanced System S..., System Resource Re..., Firewall, Services, Security Profile (which is selected), and System Swap. The main content area displays the **Lockdown Mode** section, which states: "When enabled, lockdown mode prevents remote users from logging directly into accessible through the local console or an authorized centralized management ap...". It shows "Lockdown Mode" set to "Enabled (Normal)" and "Exception Users". Below this are sections for Host Image Profile Acceptance Level (Acceptance Level: Partner Supported) and Host Encryption Mode.

Wait for the vSphere Client to refresh to see that Lockdown Mode has been enabled.

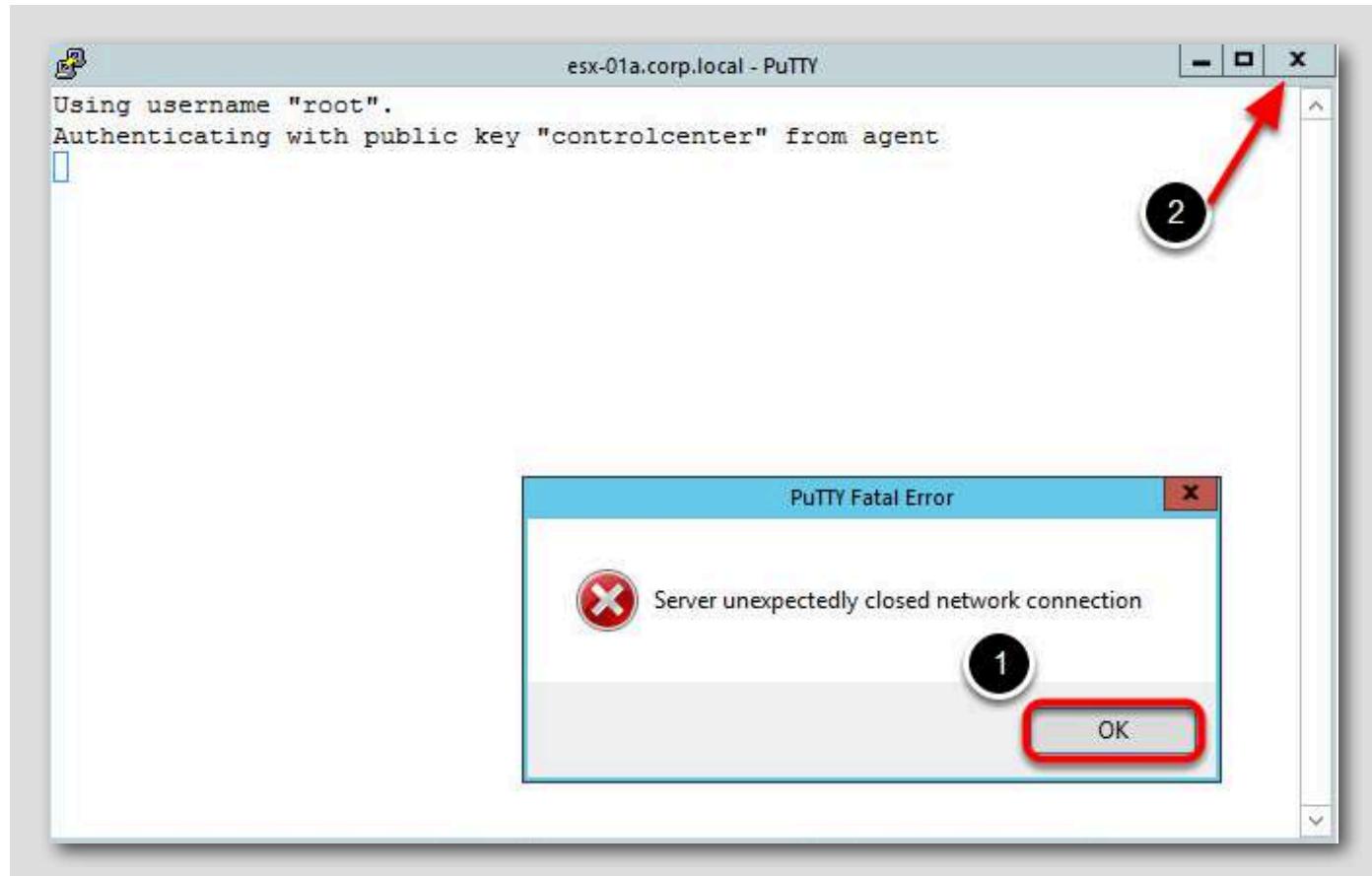
PuTTY Session to esx-01a



Using the same steps we used above, open the PuTTY application from the Windows Taskbar.

1. Click on esx-01a.corp.local under Saved Sessions
2. Click Load
3. Click Open

Denied!



You should receive an error when trying to connect to esx-01a.corp.local. The host has been configured with Host Lockdown Mode and will refuse any remote connections, unless those users were added to the Exception User list.

1. Click OK
2. Close PuTTY by clicking the 'X' in the top right-hand corner of the window

Disable Lockdown Mode

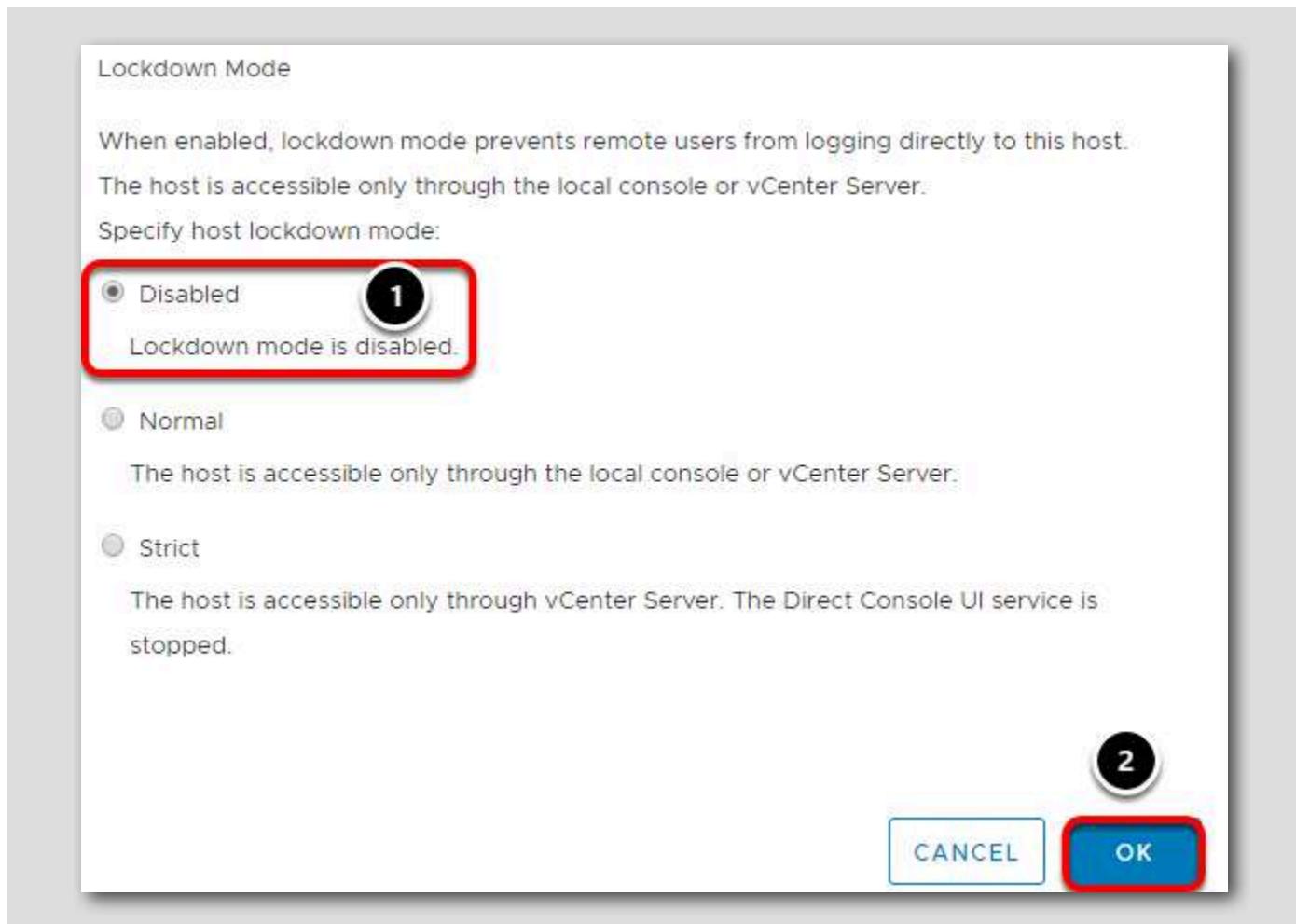
The screenshot shows the vSphere Client interface for a host named 'cal'. The top navigation bar includes 'Actions' and tabs for 'Configure', 'Permissions', 'VMs', 'Datastores', 'Networks', and 'Updates'. A red circle with the number '1' is positioned above the 'Edit...' button in the 'Lockdown Mode' section. The 'Lockdown Mode' section contains two rows: 'Lockdown Mode' set to 'Enabled (Normal)' and 'Exception Users'.

Lockdown Mode	Enabled (Normal)
Exception Users	

Go back to the vSphere Client.

1. Click on the Edit button again under Lockdown Mode

Lockdown Mode



1. Check the **Disabled** radio button

2. Click **OK** to continue

Host Lockdown Mode Disabled

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly accessible through the local console or an authorized centralized management system.

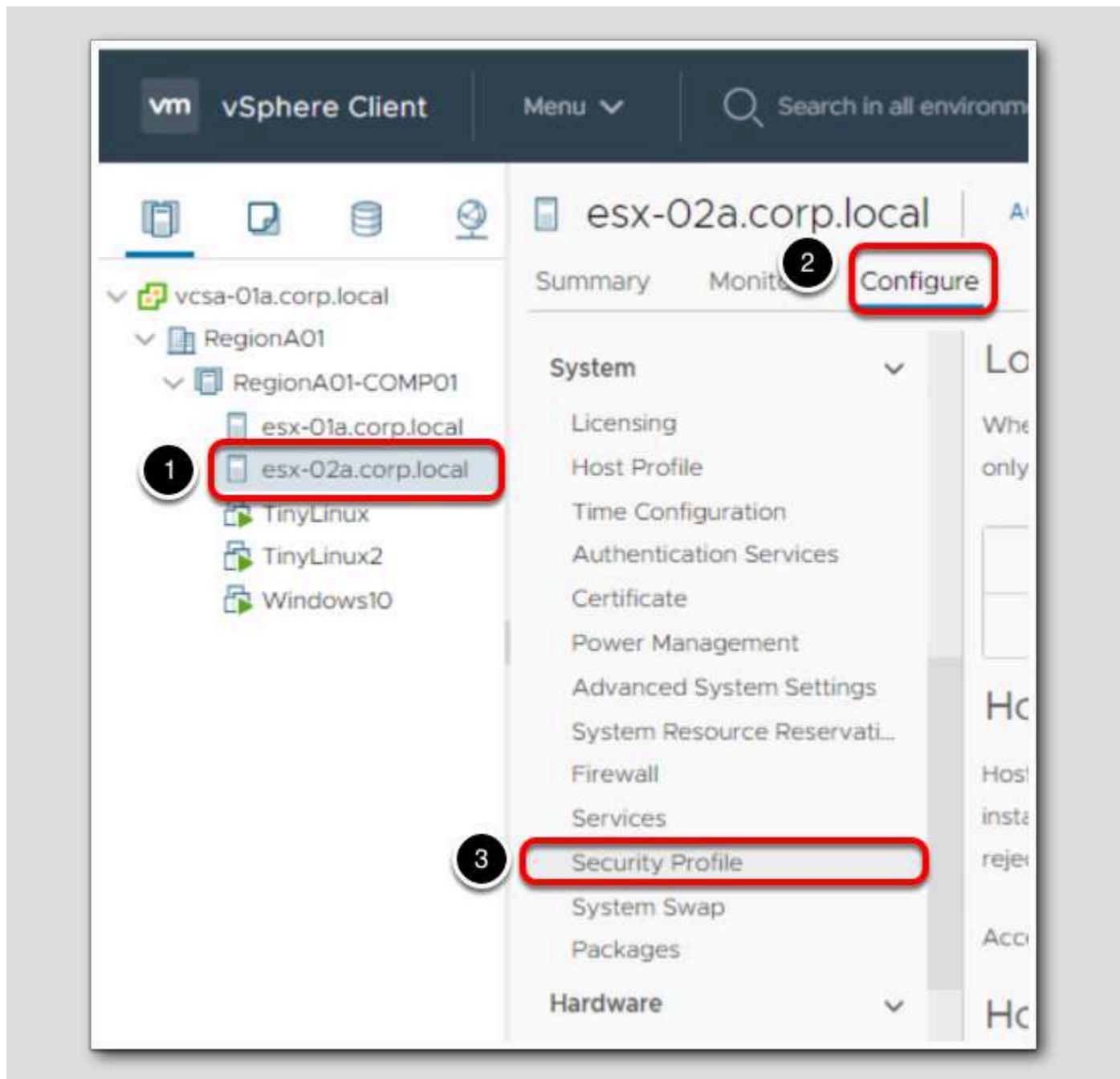
Lockdown Mode	Disabled
Exception Users	

Host Image Profile Acceptance Level

Lockdown Mode for the host should now be disabled.

Host Lockdown Mode provides an excellent way to further secure your vSphere hosts.

Strict Mode



Now you will set esx-02a.corp.local to use the Strict Mode of Host Lockdown. This means the host is only available through vCenter Server and access to the DCUI and SSH are disabled.

1. Click on **esx-02a.corp.local**.
2. Click the **Configure** tab, if it is not already selected
3. Click on **Security Profile** under the **System** section

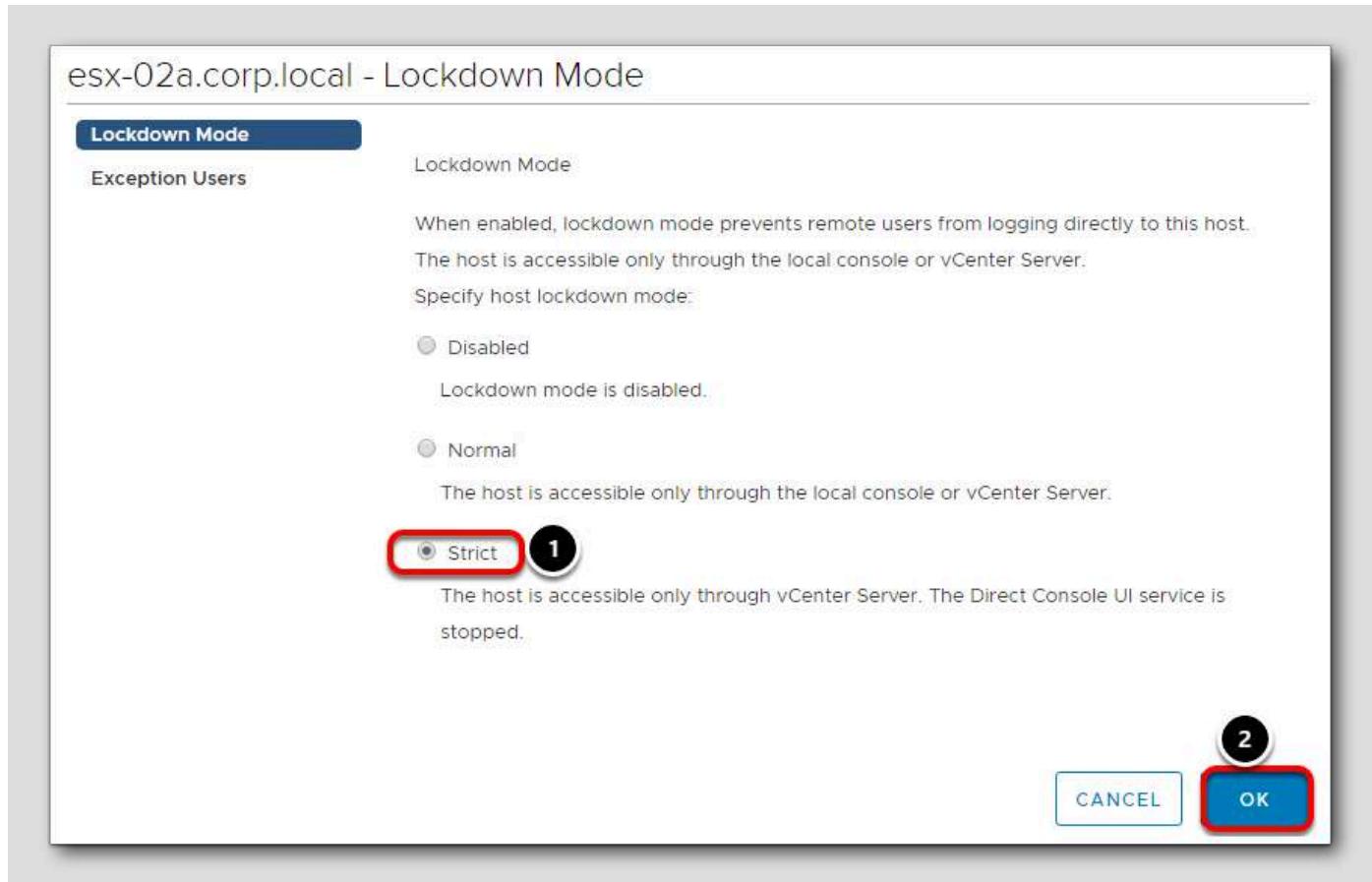
Enable Lockdown Mode

[377]

The screenshot shows the vSphere Web Client interface for host **esx-02a.corp.local**. The **Configure** tab is selected. In the left sidebar, under the **System** section, the **Security Profile** option is highlighted. On the right, the **Lockdown Mode** section is displayed, which includes a description and a table with two rows: **Lockdown Mode** (set to **Disabled**) and **Exception Users**. A red box highlights the **EDIT...** button next to the **Lockdown Mode** row. A circular callout with the number **1** is positioned above the **EDIT...** button.

1. Click on the **Edit** button

Lockdown Mode - Strict

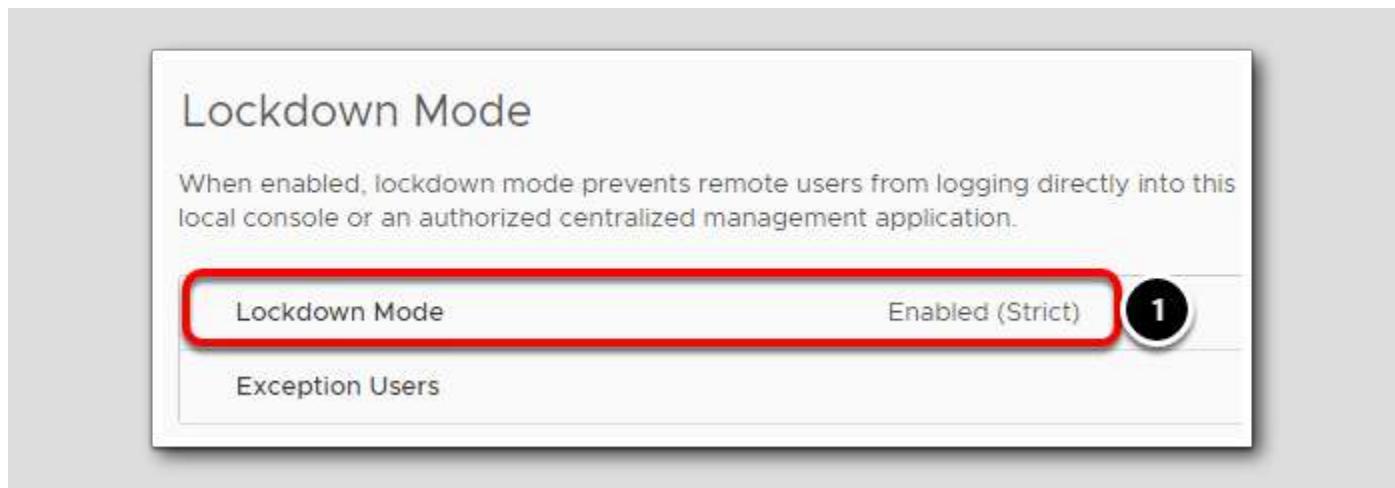


1. Click button next to **Strict**

2. Click **OK**

Again, note that users can be added to the exception list. This will only apply to SSH and not the DCUI.

Strict Mode - Enabled



1. Notice Lockdown Mode is now Enabled

Services

The screenshot shows the vSphere Web Client interface for host `esx-02a.corp.local`. The top navigation bar includes `esx-02a.corp.local`, `ACTIONS`, `Summary`, `Monitor`, `Configure` (which is underlined in blue), `Permissions`, `VMs`, `Datastores`, and `Networks`.

The left sidebar menu is expanded, showing:

- TCP/IP configuration**
- Virtual Machines**
 - VM Startup/Shutdown
 - Agent VM Settings
 - Default VM Compatibility
 - Swap File Location
- System**
 - Licensing
 - Host Profile
 - Time Configuration
 - Authentication Service
 - Certificate
 - Power Management
 - Advanced System Settings
 - System Resource Reservation
 - Firewall
 - Services** (highlighted with a red box and labeled 1)
 - Security Profile

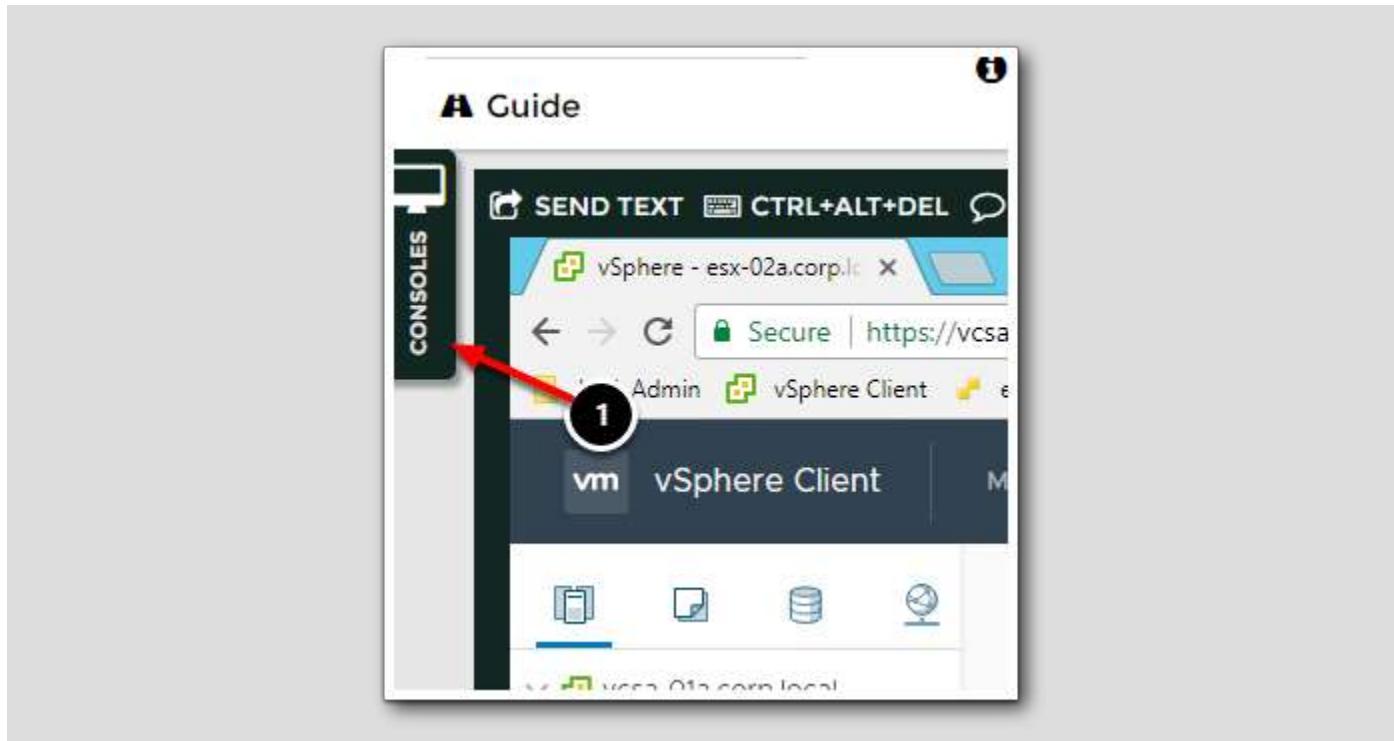
The main content area is titled **Services**. It contains a toolbar with `Restart`, `Start`, `Stop`, and `Edit Startup Policy...` buttons. Below the toolbar is a table listing services:

Name	Daemon
Direct Console UI	Stopped
ESXi Shell	Stopped
SSH	Running
Load-Based Teaming Daemon	Running
Active Directory Service	Stopped
NTP Daemon	Running
PC/SC Smart Card Daemon	Stopped
CIM Server	Stopped
SNMP Server	Stopped
Syslog Server	Running
VMware vCenter Agent	Running

1. Click on **Services**.

You can see the Direct Console UI (DCUI) service has been stopped. Note that the SSH service is still running in case users have been added to the Exception List.

DCUI Disabled

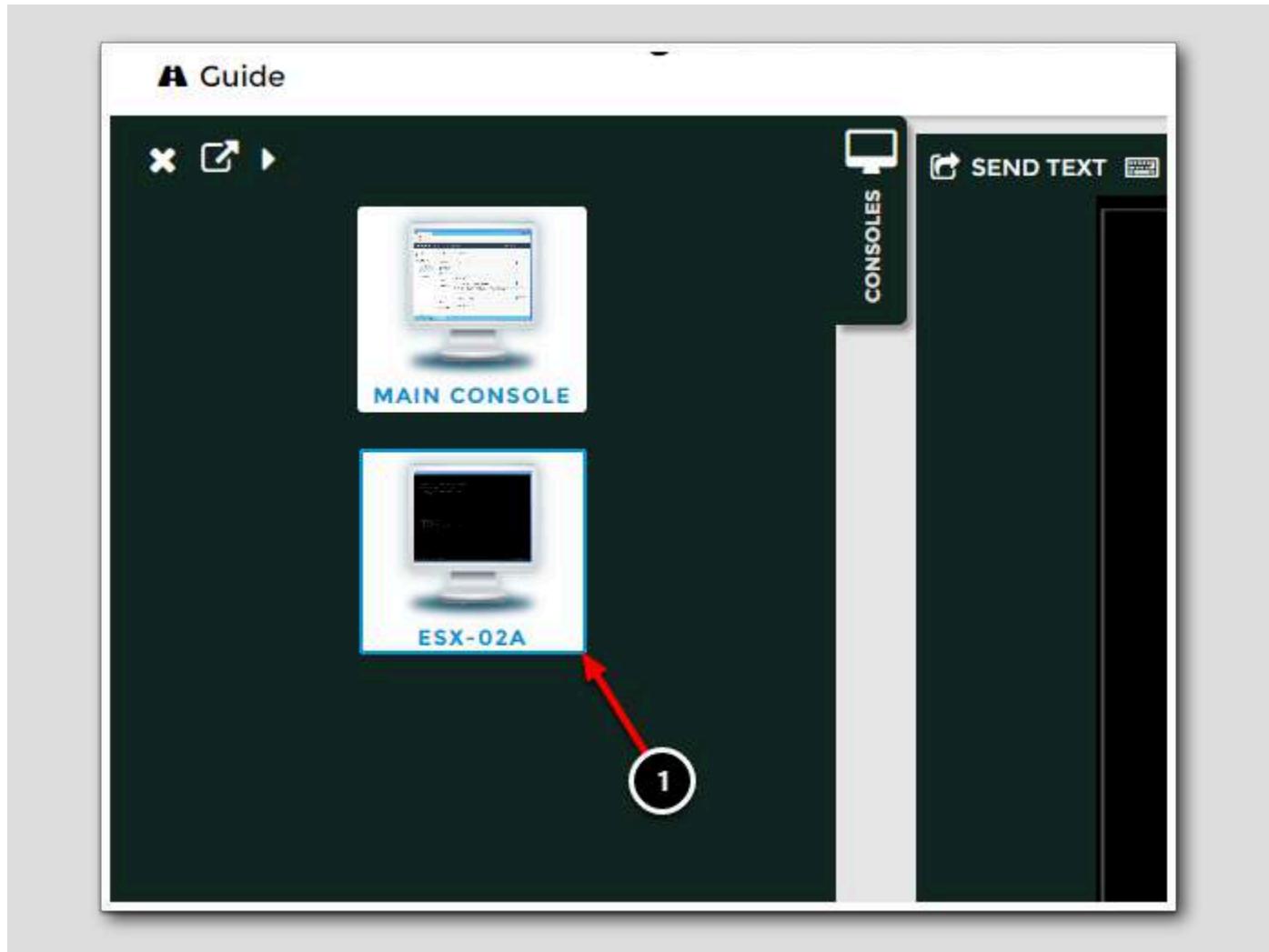


1. On the far, right-hand side of the web page, look for the Consoles tab and click on it.

This will give us access to the DCUI on esx-02a-corp.local.

Select ESX-02A

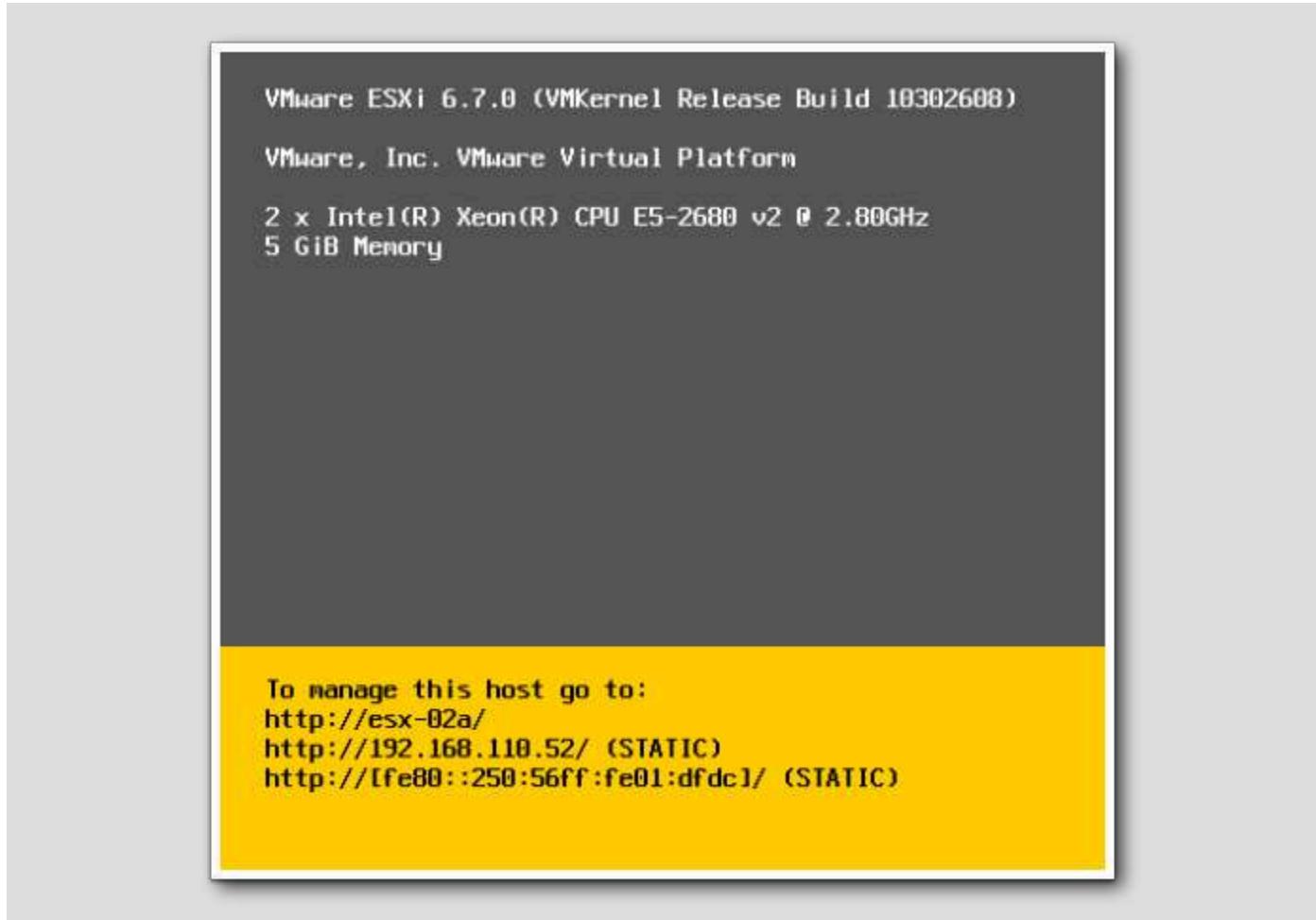
[382]



1. Click on the thumbnail for ESX-02A.

The console window will load the DCUI for esx-02a.corp.local.

Click in the Console



Click in the console and press the space bar to wake up the host.

Press F2

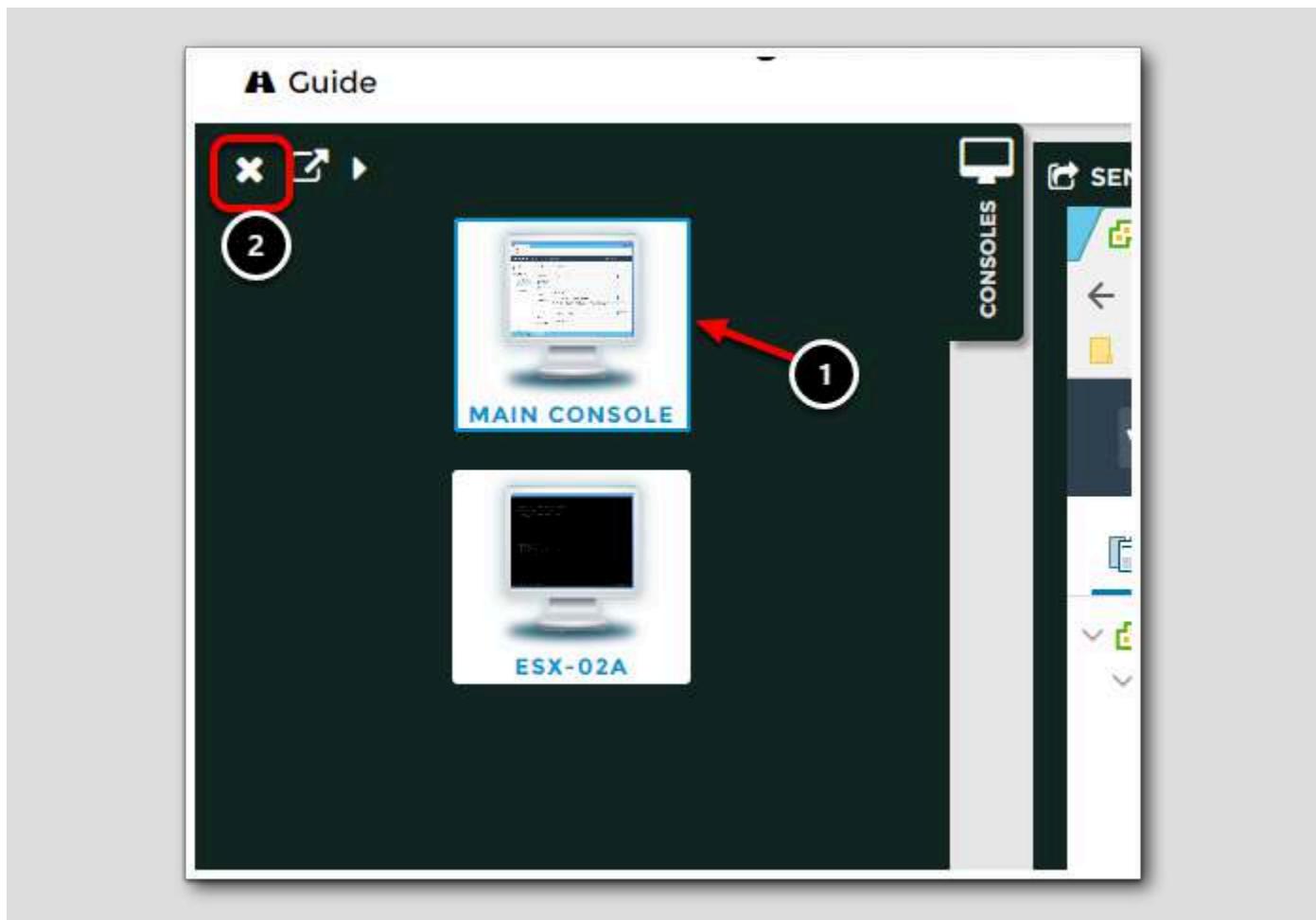


1. Now press the F2 key to log in to the DCUI.

You should receive an error that access to the DCUI has been disabled.

2. Press the Enter key to dismiss the message.

Main Console



1. Go back to the Console and click MAIN CONSOLE to return to the Windows desktop.
2. After the Main Console loads, click the X to close the Console panel.

Disable Lockdown Mode

esx-02a.corp.local | ACTIONS ▾

Primary Monitor Configure Permissions VMs Datastores Networks Updates

HOST PROFILE

- Time Configuration
- Authentication Servi...
- Certificate
- Power Management
- Advanced System S...
- System Resource Re...
- Firewall
- Services
- Security Profile** (1)
- System Swap

Lockdown Mode

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

Lockdown Mode	Enabled (Strict)
Exception Users	

Host Image Profile Acceptance Level

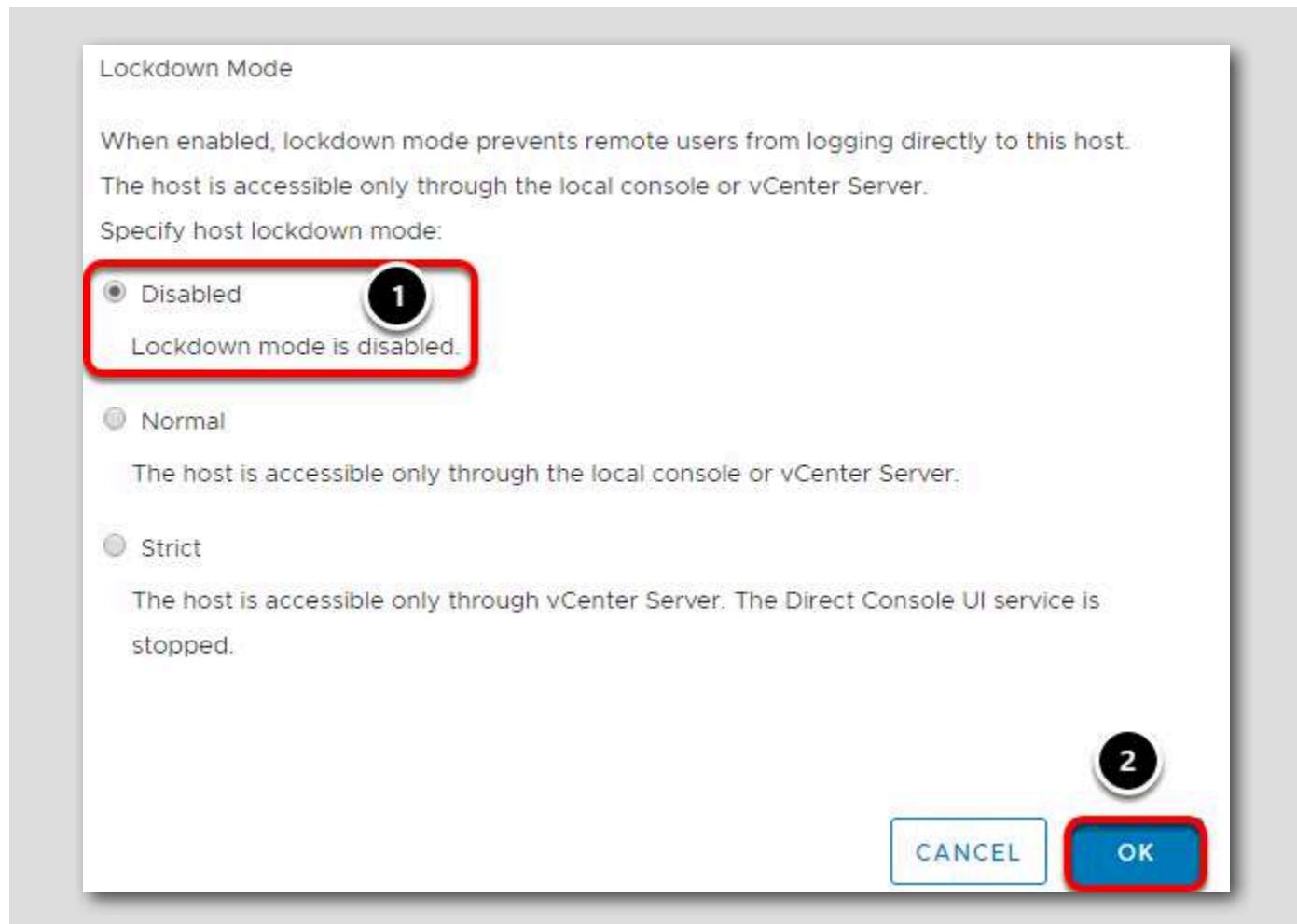
Host image profile acceptance level determines which vSphere installation bundles are accepted for installation.

EDIT... (2)

Go back to the vSphere Client.

1. Click on **Security Profile**.
2. Click on the **Edit** button again under Lockdown Mode.

Lockdown Mode



1. Check the **Disabled** radio button

2. Click **OK** to continue.

Host Lockdown Mode Disabled

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly accessible through the local console or an authorized centralized management system.

Lockdown Mode	Disabled
Exception Users	

Host Image Profile Acceptance Level

Lockdown Mode for the host should now be disabled.

Host Lockdown Mode provides an excellent way to further secure your vSphere hosts.

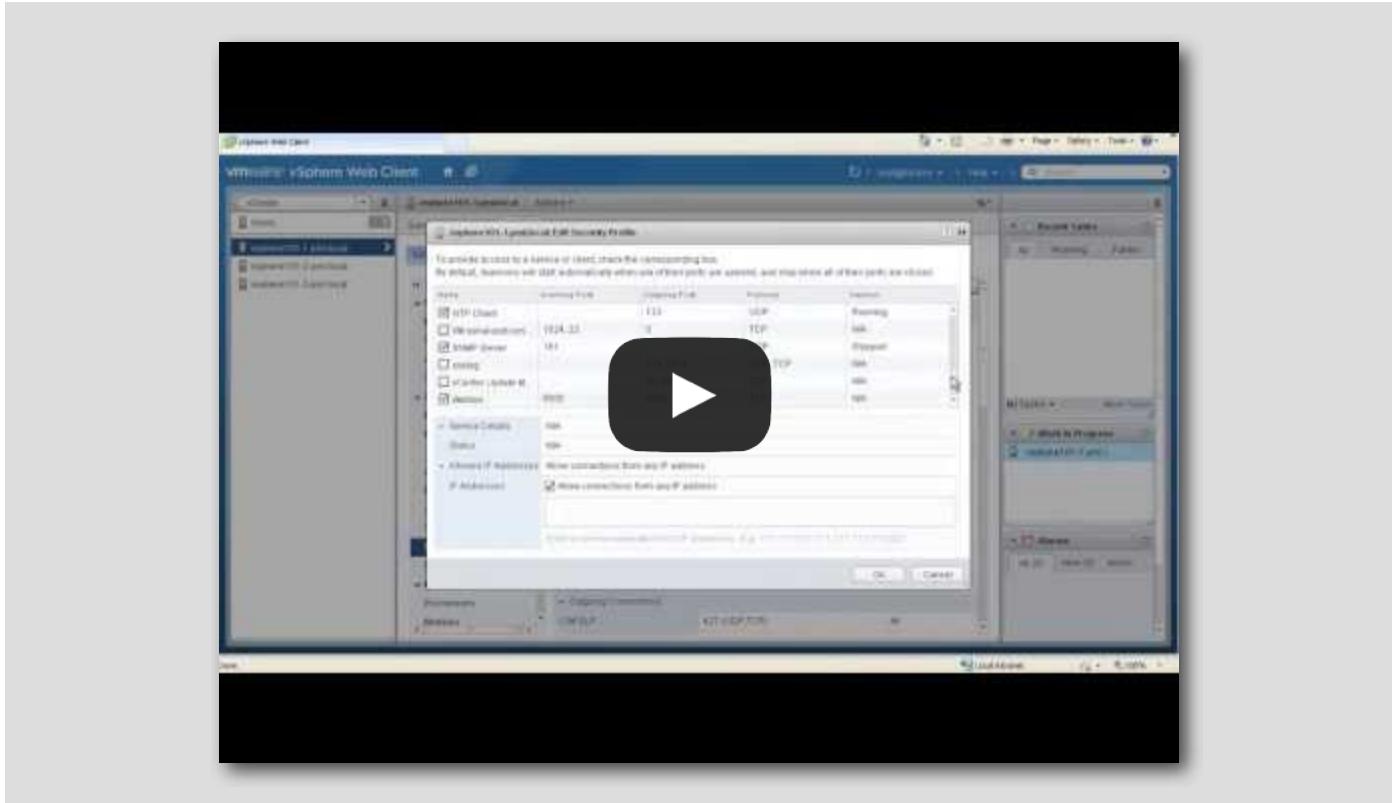
Configuring the Host Services and Firewall

This lesson includes a short video on how to use the VMware ESXi firewall.

Video: Configure vSphere Host Firewall for VMware vSphere (4:34)

This video shows how to use the VMware ESXi Firewall on the vSphere host to block incoming and outgoing communication and to manage the services running on the host.

<https://www.youtube.com/watch?v=bzjsjQdnTuk>



User Access and Authentication Roles

[391]

VMware recommends that you create roles to suit the access control needs of your environment. If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes that you make are propagated to all other vCenter Server systems in the group.

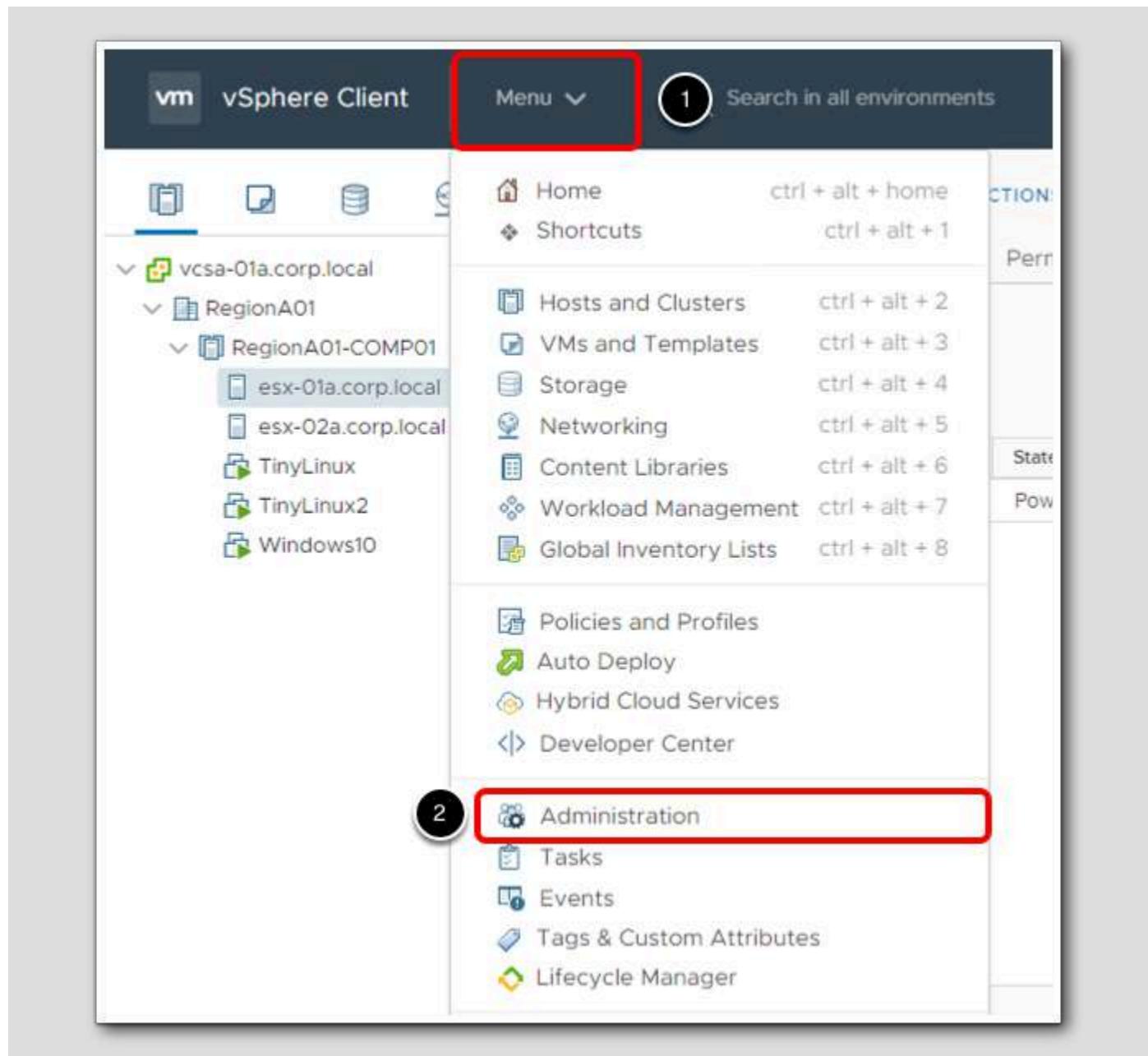
Linked Mode connects multiple vCenter Server systems together by using one or more Platform Services Controllers. It lets you view and search across all linked vCenter Servers and replicate roles, permissions, licenses, policies and tags.

Create a Role in the vSphere Client

[392]

In the following steps, we will create a role in the vSphere Client that we can assign rights for the role.

Administration



1. In the vSphere Client, click on **Menu**
2. Select **Administration**

Roles

The screenshot shows the vSphere Client interface. The top navigation bar includes the 'vm' icon, 'vSphere Client' title, 'Menu' dropdown, and a search bar. The left sidebar has a tree structure under 'Administration': 'Access Control' (selected, highlighted with a red box and a circled '1'), 'Licensing', 'Solutions' (with 'Client Plugins' and 'vCenter Server Extensions' listed), and 'Deployment'. The main content area is titled 'Roles' and displays a list of roles: 'Administrator', 'Read-only', 'No access', and 'AppdApplianceUser'. A '+' button and edit/cross icons are at the top of the list. The 'Roles provider:' field shows 'VSPHERE.LOCAL'. A status bar at the bottom indicates '1 item selected'.

1. Verify the **Roles** tab is selected

Roles Overview

The screenshot shows the vSphere Client interface with the 'Roles' section selected. The left sidebar has a tree view with various categories. The main pane displays a list of roles under 'VS SPHERE.LOCAL'. The 'DESCRIPTION' button is highlighted with a red border.

Role	Description
Administrator	Full access rights
Read-only	
No access	
AppdApplianceUser	
AutoUpdateUser	
Content library administrator (sample)	
Content Library Registry administrator (sample)	
Datastore consumer (sample)	
Network administrator (sample)	
No cryptography administrator	
No Trusted Infrastructure administrator	
NSX Administrator	
NSX Auditor	
NSX VI Administrator	

1. The "Roles" panel shows various roles that already exist or are provided as sample to use or create roles from
2. When a role is selected, information such as Description, Usage, and Privileges will be displayed by clicking the corresponding buttons

You can use one of the provided roles as a starting point to create your own or in some cases, it may make sense to create a new rule with zero permissions and only add the ones the role will need.

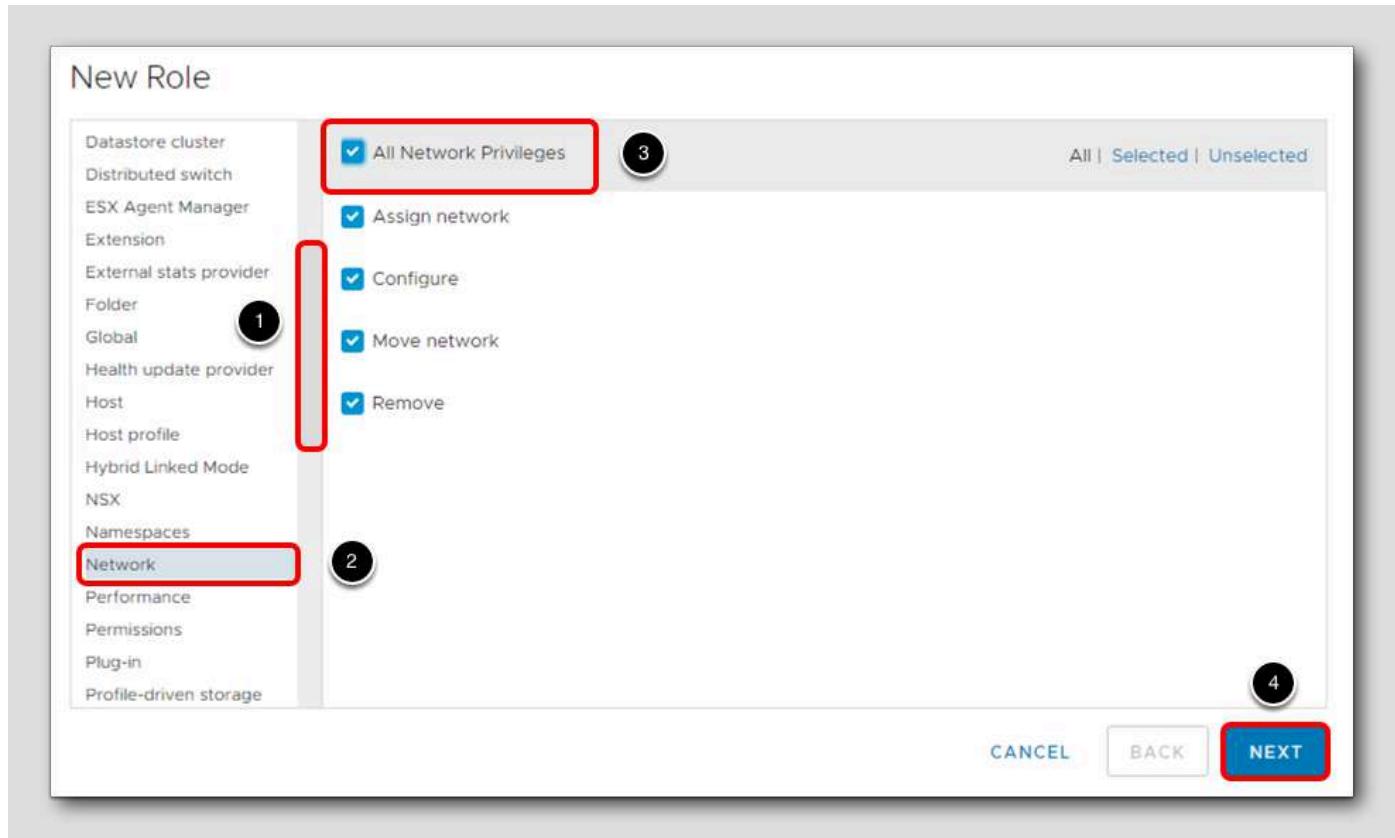
Add a Role

	DESCRIPTION
Administrator	This role entities
Read-only	
No access	
AppdApplianceUser	
AutoUpdateUser	

In this first example, a role will be created for a new contractor that will only be performing networking tasks.

1. Click on the '+' to add a new role

New Role



1. Use the scrollbar to scroll down until you see **Network**
2. Click **Network**
3. Tick the box for **All Network Privileges**
4. Click **Next**

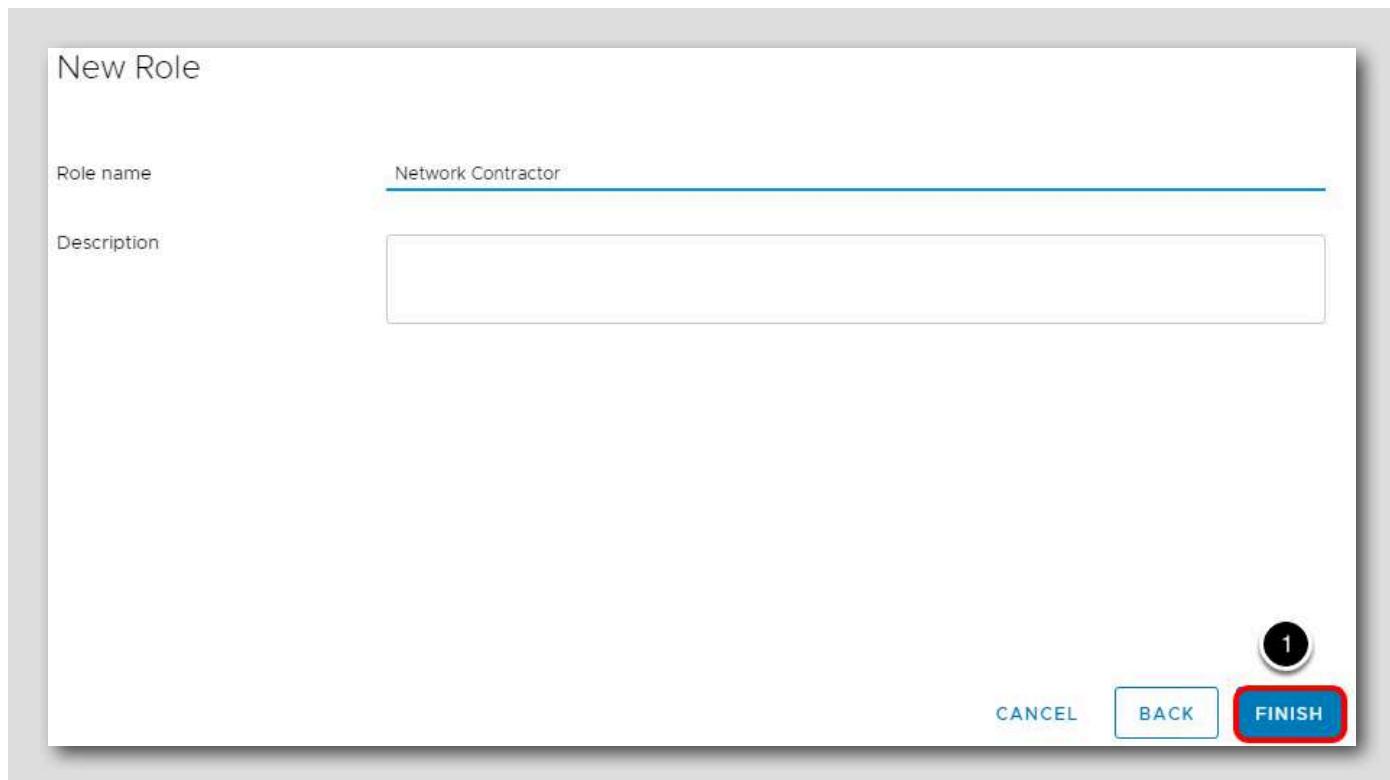
Role name

New Role

Role name	Network Contractor
Description	<input type="text"/>

1

CANCEL BACK FINISH



1. Name the role Network Contractor
2. Click the Finish button to create the new role

Edit a Role in the vSphere Client

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role. In Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. However, assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

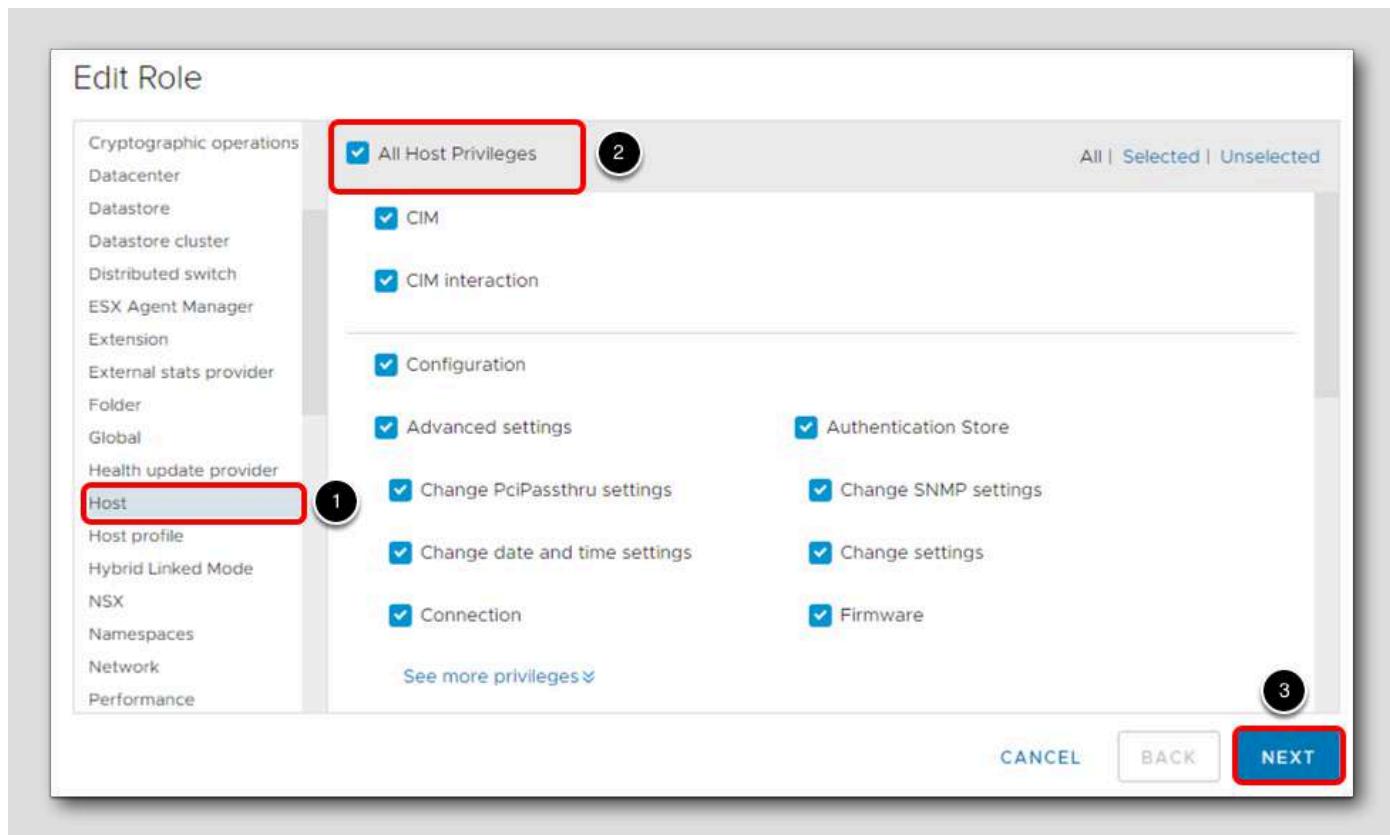
Edit Role

The screenshot shows the 'Roles' page in the vSphere Web Client. At the top, there is a search bar labeled 'Roles p...' and a dropdown menu 'VSPHERE.LOCAL'. Below the search bar are three icons: a plus sign, a document, and a pencil (highlighted with a red circle). To the right of these icons is a 'DESCRIPTION' button. The main area contains a list of roles, each with a small circular icon to its left. The 'Network Contractor' role is highlighted with a red box and has a circled '1' next to it. Other roles listed include: Content library administrator (sample), Content Library Registry administrator (sample), Datastore consumer (sample), Network administrator (sample), Network Contractor (highlighted with a red box and circled '1'), No cryptography administrator, No Trusted Infrastructure administrator, NSX Administrator, NSX Auditor, NSX VI AdminInistrator, Resource pool administrator (sample), SupervisorService Cluster Operator, SupervisorService Operator, and SupervisorService RootFolder Operator.

Sometimes a role may need to be updated for access to additional objects or tasks in vCenter. As an example, say the Network Contractor now needs access to the ESXi Hosts.

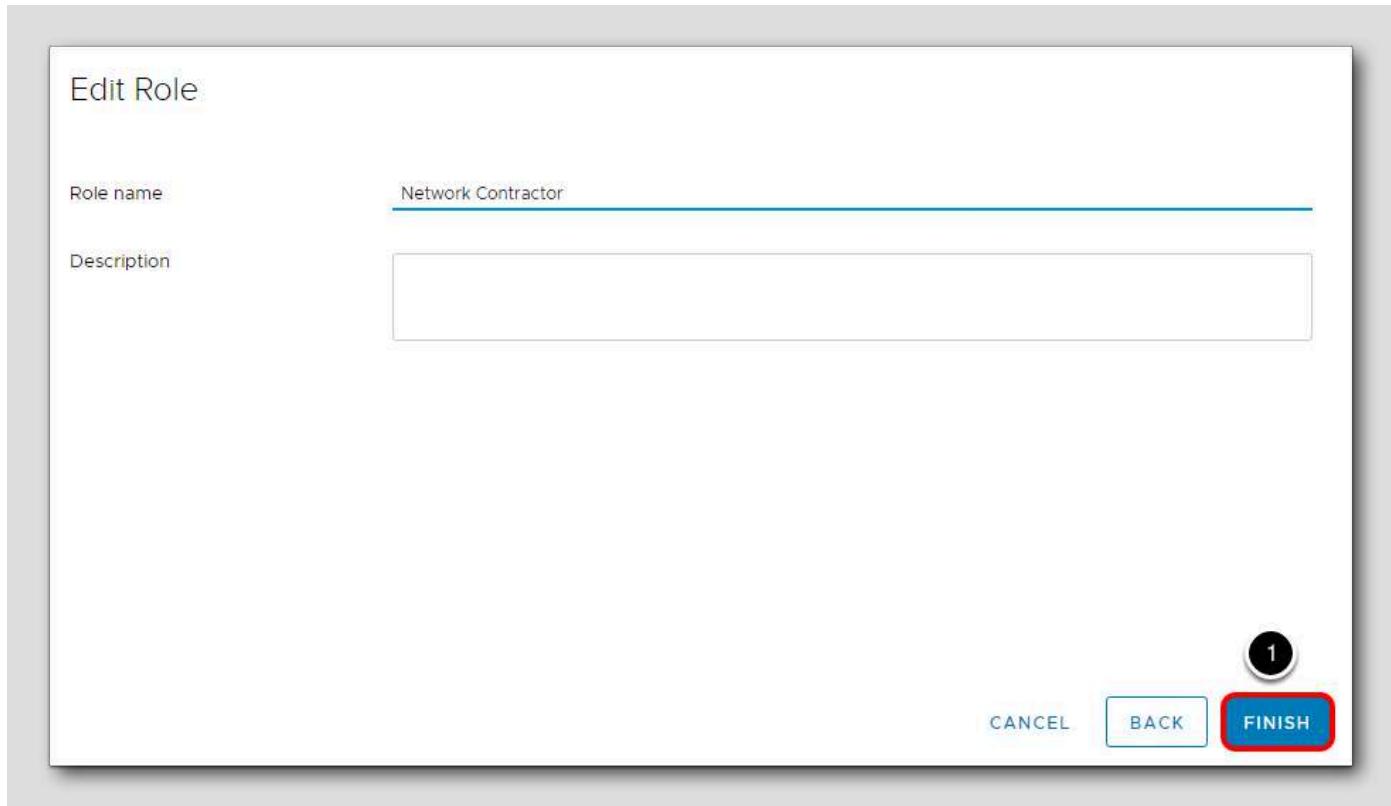
1. Scroll down if necessary, and click on the role Network Contractor
2. Click the pencil button to edit the role

Add Permissions



1. Click on Host
2. Tick the box next to All Host Privileges
3. Click Next

Edit Role



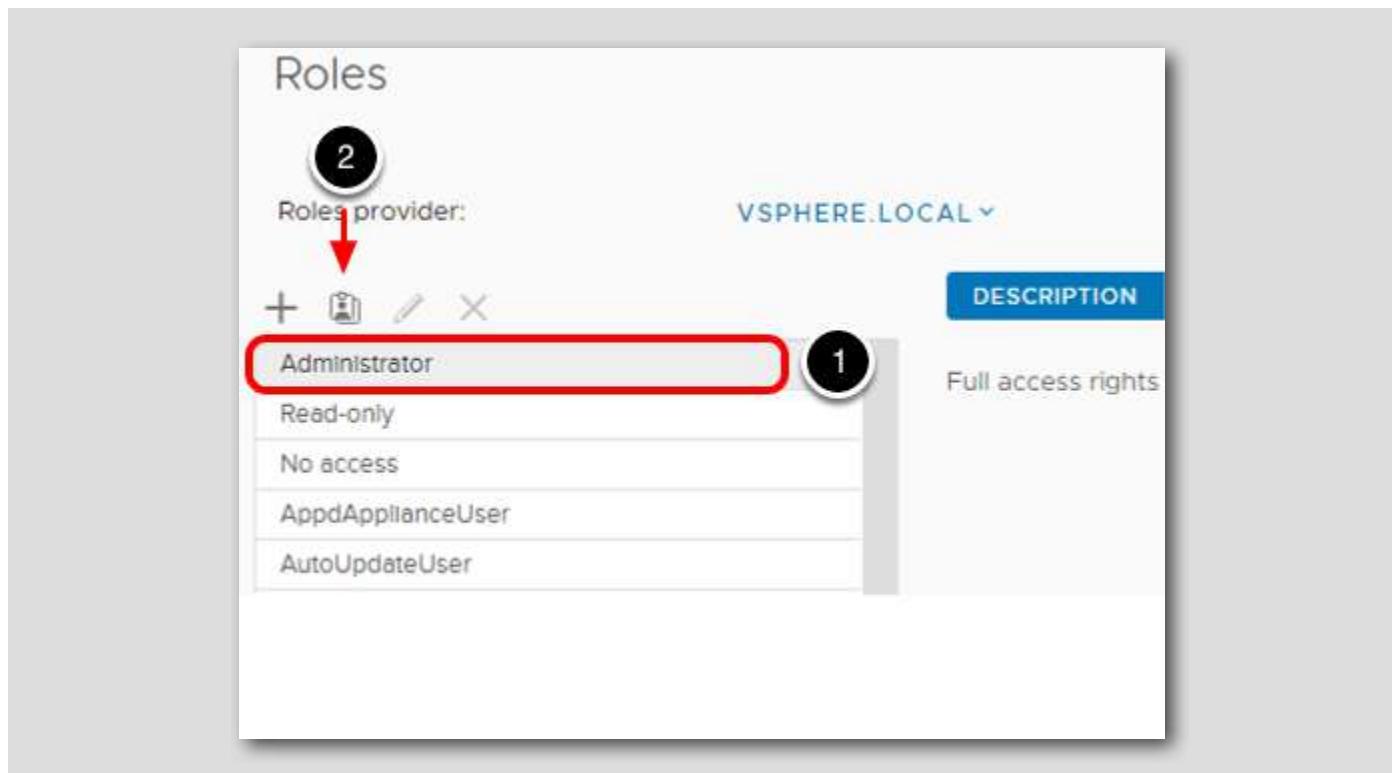
We will keep the same Role name.

1. Click Finish.

Clone a Role in the vSphere Client

You can make a copy of an existing role, rename it, and edit it. When you make a copy, the new role is not applied to any users, groups or objects -- it does not inherit anything from the parent except the settings. In Linked Mode, the changes are propagated to all other vCenter Server systems in the group, but assignments of roles to specific users and objects are not shared across linked vCenter Server systems.

Clone a Role



In this next example, the Administrator role will be cloned and the privileges that are not needed will be removed.

1. Click on the **Administrator** role
2. Click the **Clone** button

Clone Role



As an example, a new vSphere Admin is hired and they only need access to the compute and storage infrastructure, with no access to networking components.

1. For the Role name, type vSphere Administrator
2. In the Description field, type Full rights to all but Networking
3. Click OK

New Role Cloned

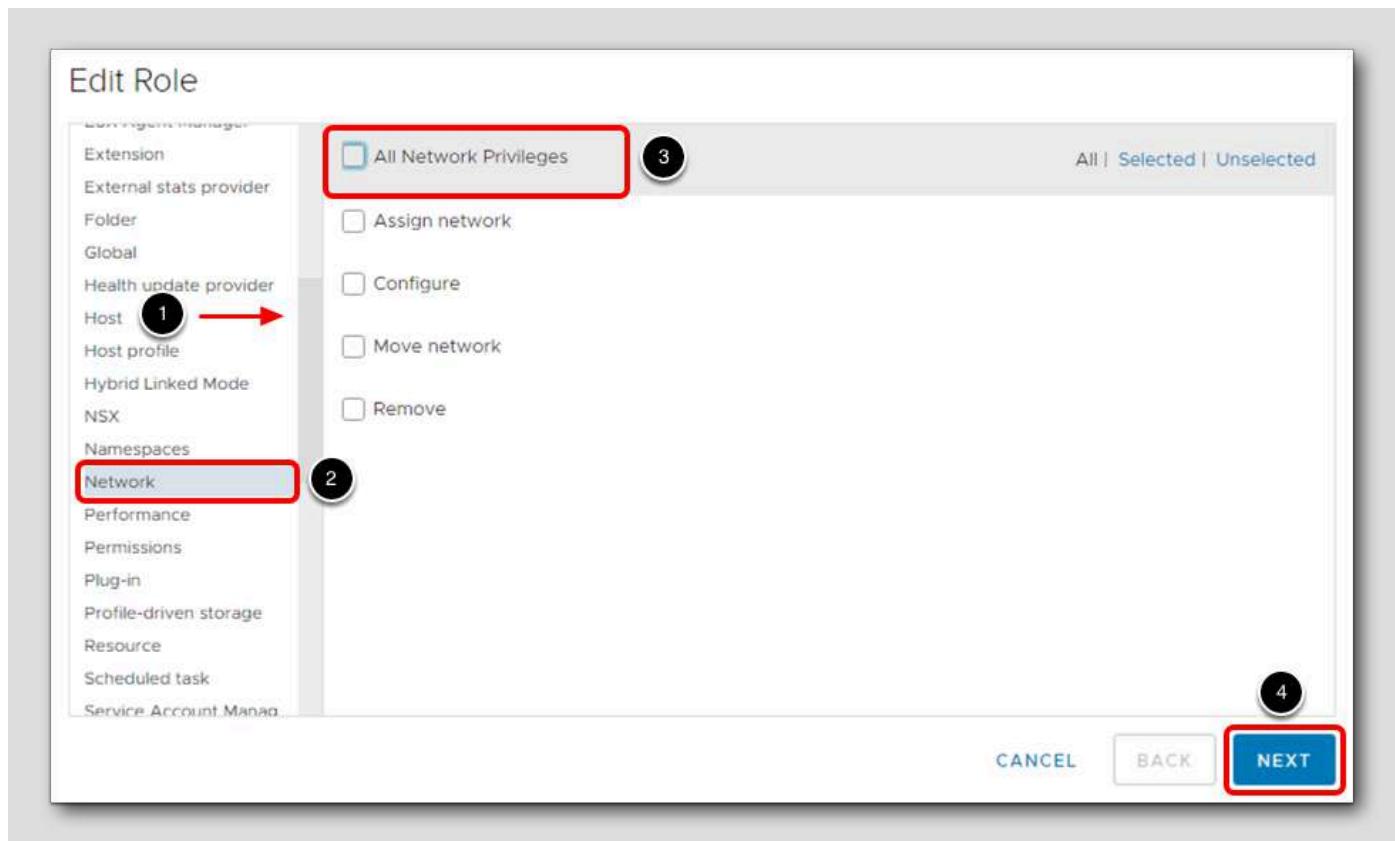
The screenshot shows the 'Roles' screen in the vSphere Client. The 'Roles provider' dropdown is set to 'VSphere.LOCAL'. The interface includes a toolbar with a '+' button (labeled 3), a pencil icon (labeled 2, indicating it's highlighted with a red box), and a 'X' button. Below the toolbar is a table with three columns: 'DESCRIPTION', 'USAGE', and 'PRIVILEGES'. A red arrow labeled 1 points from the bottom of the list to the 'vSphere Administrator' row. The 'vSphere Administrator' row is highlighted with a red box and has a pencil icon next to it (labeled 2). The table shows the following data:

	DESCRIPTION	USAGE	PRIVILEGES
Tagging Admin			
Trusted Infrastructure administrator			
Virtual Machine console user			
Virtual machine power user (sample)			
Virtual machine user (sample)			
VMOperator Controller			
VMOperator Controller Manager			
VMware Consolidated Backup user (sample)			
vSphere Administrator	Full rights to all but Networking.		
vSphere Client Solution User			
vSphere Kubernetes Manager			
vStatsAdmin			
vStatsUser			
Workload Storage Manager			

34 items

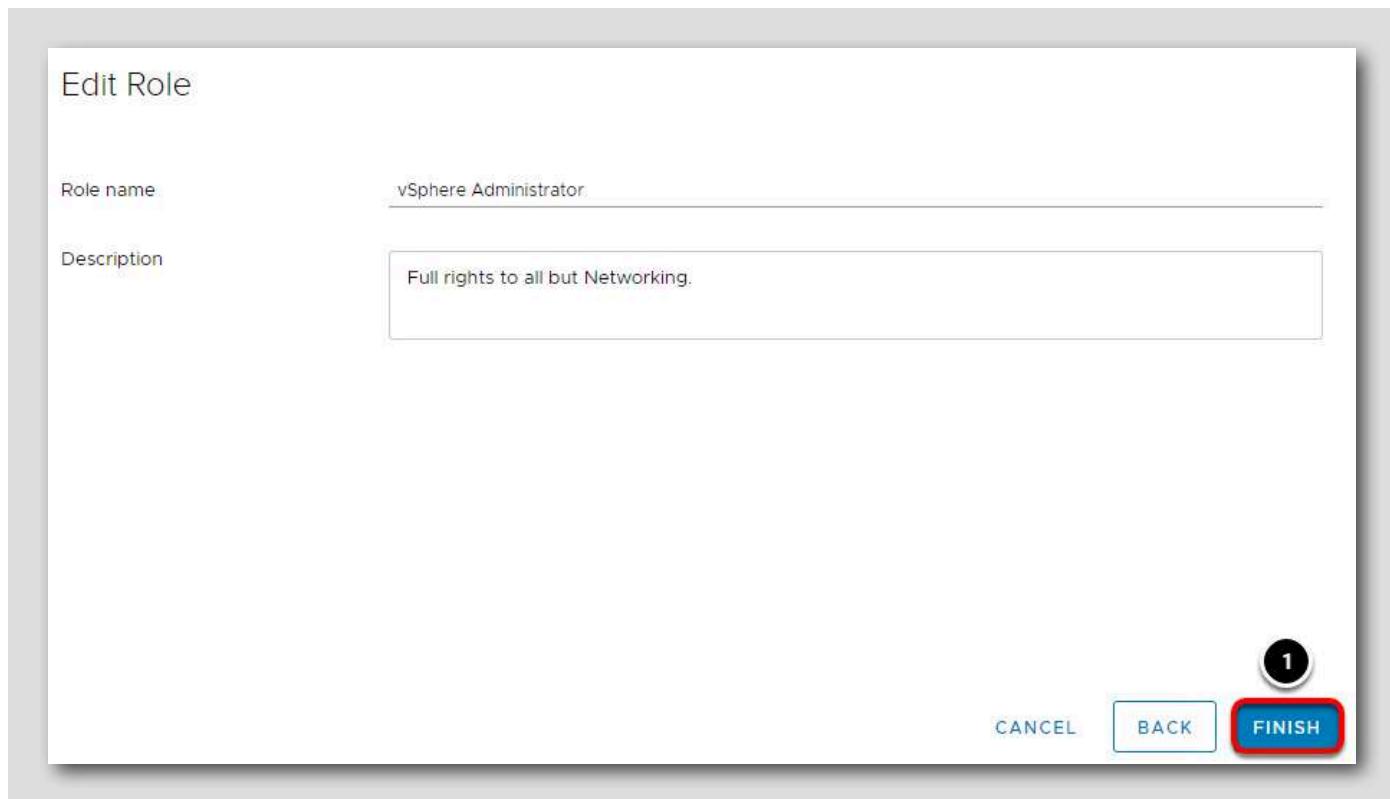
1. Scroll to the bottom of the list to find the newly created role
2. Click on vSphere Administrator
3. Click the pencil button to edit the role

Edit Role - Network



1. Scroll down until you see Network
2. Click on Network
3. Untick All Network Privileges
4. Click Next

Edit Role



1. Keep the same role name and click the **Finish** button

Remove a Role in the vSphere Client

When you remove a role that is not assigned to any users or groups, the definition of the role is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.

NOTE:

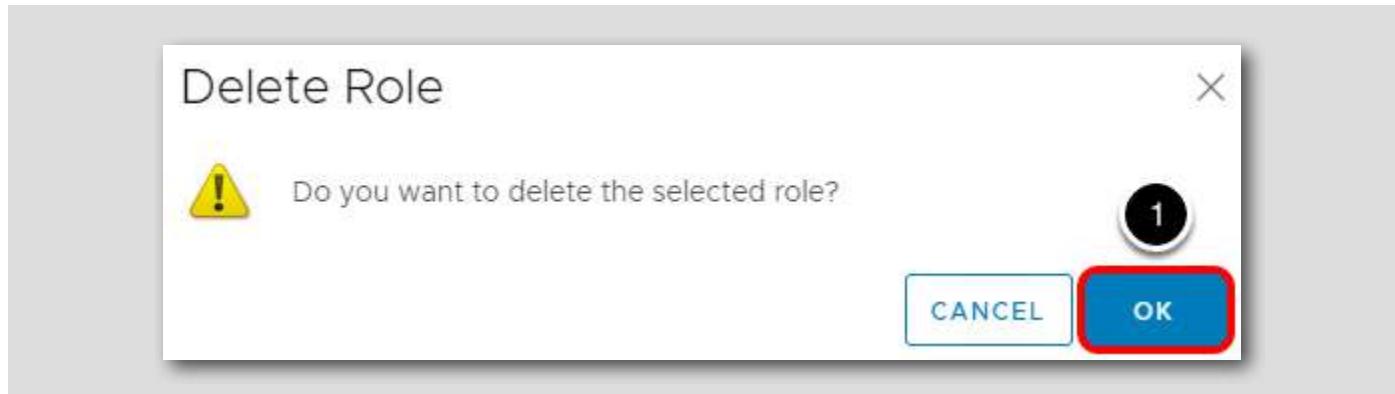
Before removing a role from a vCenter Server system that is part of a connected group in Linked Mode, check the use of that role on the other vCenter Server systems in the group. Removing a role from one vCenter Server system also removes that role from all other vCenter Server systems in the group, even if you reassign permissions to another role on the current vCenter Server system.

Delete Role

The screenshot shows the 'Roles' interface in vSphere. At the top, it displays 'Roles provider: VS SPHERE.LOCAL'. Below this are several icons: a plus sign, a document icon, a pencil icon, and a delete button (an 'X'). A circled '2' is placed over the delete button. The main area lists various roles, with 'Network Contractor' highlighted by a red box and a circled '1'. Other listed roles include: Content library administrator (sample), Content Library Registry administrator (sample), Datastore consumer (sample), Network administrator (sample), No cryptography administrator, No Trusted Infrastructure administrator, NSX Administrator, NSX Auditor, NSX VI Administrator, Resource pool administrator (sample), SupervisorService Cluster Operator, SupervisorService Operator, SupervisorService RootFolder Operator, and SyncUsers.

1. Click on the Network Contractor role to select it
2. Click the Delete button

Confirm Deletion



1. Click OK to confirm you want to delete this role

Role Deleted

The screenshot shows the 'Roles' interface in vSphere. At the top, it displays 'Roles provider: VSPHERE.LOCAL'. Below this is a toolbar with icons for adding (+), deleting (X), and editing (pencil). A table lists various roles, each with a 'DESCRIPTION' column. The roles listed are: Administrator (description: Full access rights), Read-only, No access, AppdApplianceUser, AutoUpdateUser, Content library administrator (sample), Content Library Registry administrator (sample), Datastore consumer (sample), Network administrator (sample), No cryptography administrator, No Trusted Infrastructure administrator, NSX Administrator, NSX Auditor, and NSX VI Administrator. A note at the bottom of the list states '...and many more'. A total count of '33 items' is shown at the bottom right of the list.

We can see that the role named Network Contractor has been deleted.

Creating unique and granular roles for users in your organization enables better security for your vSphere infrastructure.

Understanding Single Sign On

You use vCenter Single Sign-On to authenticate and manage vCenter Server users.

The Single Sign-On administrative interface is part of the vSphere Web Client. To configure Single Sign-On and manage Single Sign-On users and groups, you log in to the vSphere Web Client as a user with Single Sign-On administrator privileges. This might not be the same user as the vCenter Server administrator. Enter the credentials on the vSphere Web Client login page and upon authentication, you can access the Single Sign-On administration tool to create users and assign administrative permissions to other users.

In vSphere versions prior to 5.1, users were authenticated when vCenter Server validated their credentials against an Active Directory domain or the list of local operating system users. As of vSphere 5.1, users authenticate through vCenter Single Sign On. The default Single Sign-On administrator for vSphere 5.1 is admin@System-Domain and administrator@vsphere.local for vSphere 5.5 and higher. The password for this account is the one you specified at installation. These credentials are used to log in to the vSphere Web Client to access the Single Sign-On administration tool. You can then assign Single Sign-On administrator privileges to specific users who are allowed to manage the Single Sign-On server. These users might be different from the users that administer vCenter Server.

NOTE: Logging in to the vSphere Web Client with Windows session credentials is supported only for Active Directory users of the domain to which the Single Sign On system belongs.

Single Sign-On Identity Sources

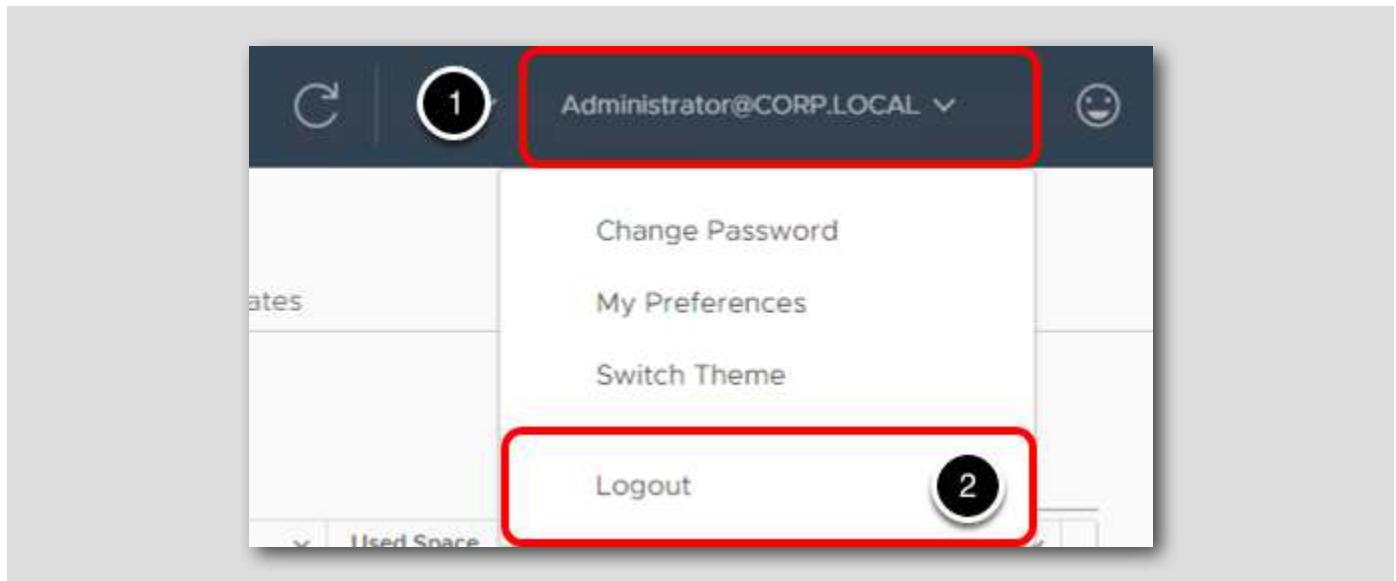
[414]

In most cases, vSphere SSO will be deployed to use an external Identity Source for primary authentication. In this lab environment, SSO has been integrated with Microsoft Active Directory so that users from the corp.local domain can log in to vSphere using their AD credentials.

In this section, we will look at the configured Identity Sources within Single Sign-on.

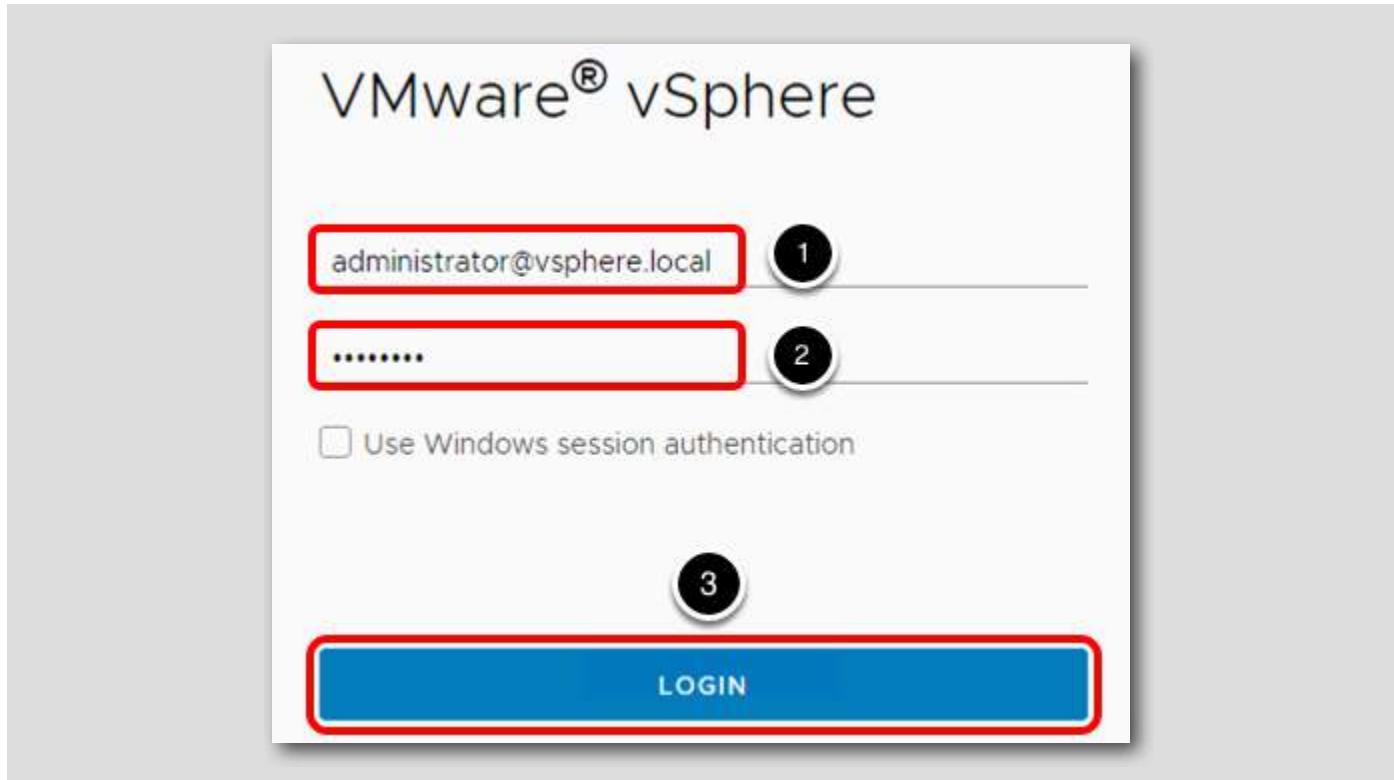
Log out as Administrator@CORP.LOCAL

[415]



1. If you are currently logged in to the vSphere Web Client, click on Administrator@CORP.LOCAL
2. Select Logout

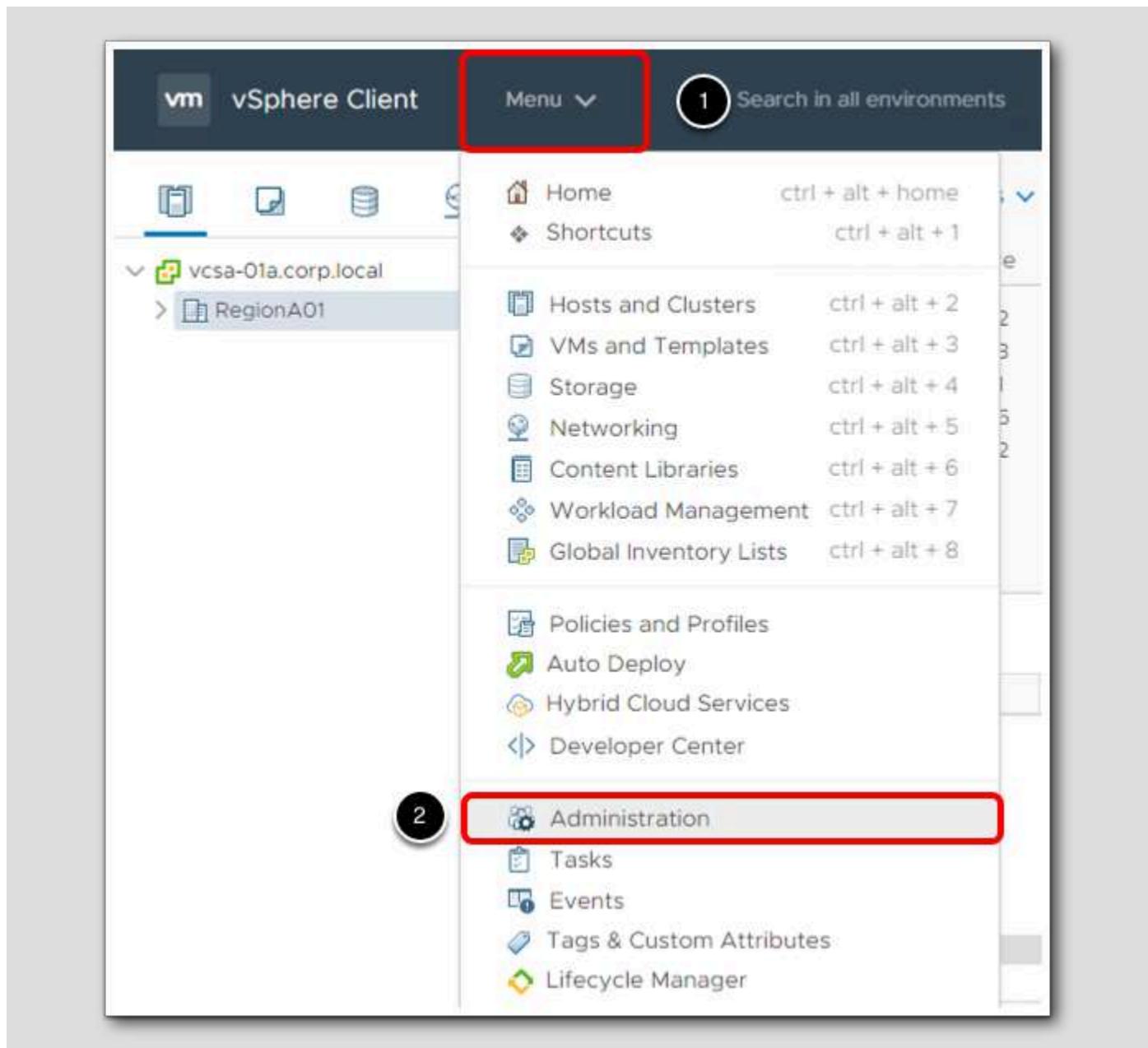
Log into vSphere Web Client as SSO Admin



Login to the vSphere Web Client with an account which has the SSO Admin privilege:

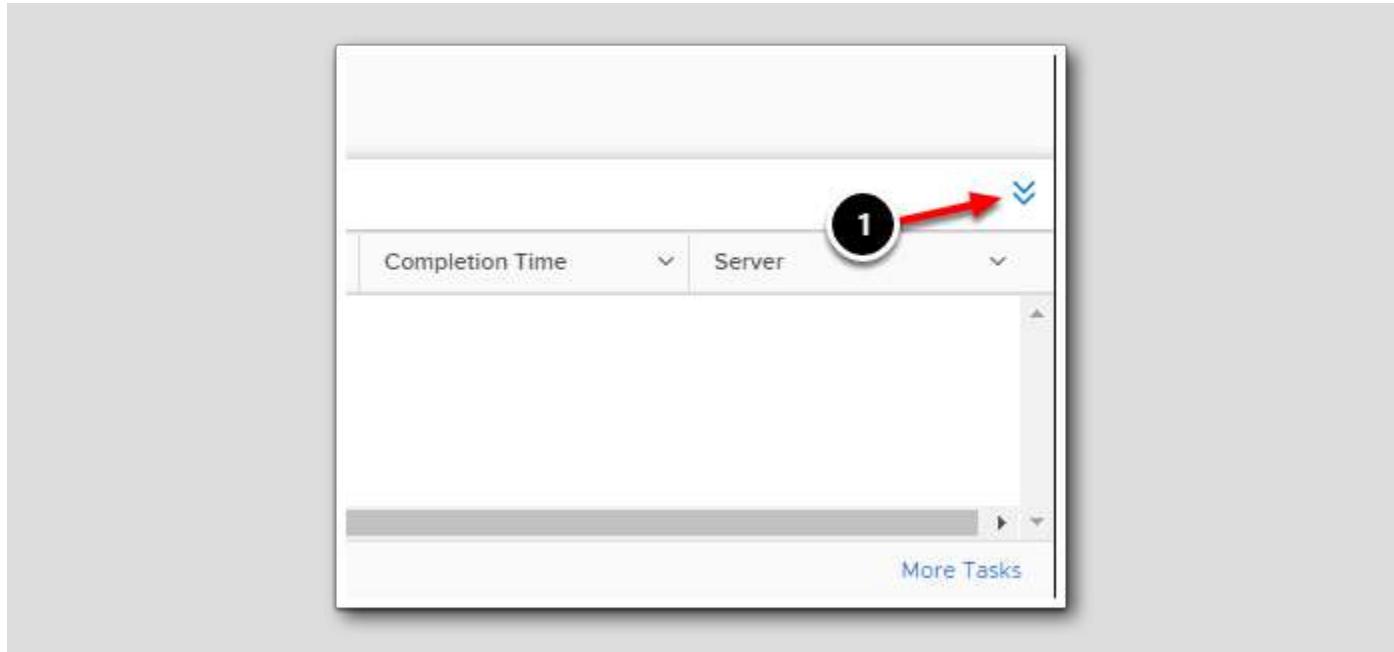
1. Username - administrator@vsphere.local
2. Password - VMware1!
3. Click Login

Navigate to Administration



1. Click **Menu**
2. Select **Administration**

Minimize Recent Tasks



1. To see more of the vSphere Client, minimize the Recent Tasks window by clicking the two down arrows.

vSphere Single Sign-on

The screenshot shows the vSphere Client interface with the title bar "vm vSphere Client" and a search bar "Search in all environments". The left sidebar under "Administration" has several collapsed sections: "Access Control", "Licensing", "Solutions", "Deployment", "Support", "Single Sign On" (which is expanded), and "Certificates". In the "Single Sign On" section, the "Configuration" item is highlighted with a red box and a circled "1". The main content area is titled "Configuration" and contains three tabs: "Identity Provider" (which is selected and highlighted with a blue underline), "Local Accounts", and "Login Message". Below the tabs is a table header with columns "Type", "Name", and "Server URL". Under the "Identity Provider" tab, there is a list of identity sources:

Type	Name	Server URL
Active Directory Domain	--	--
Smart Card Authentication	--	--
Identity Sources	corp.local	--

Two numbered callouts are present: a circled "2" points to the "Identity Sources" tab in the table, and a circled "1" points to the "Configuration" item in the sidebar.

When the machine with the Platform Services Controller (PSC), which runs the Single Sign-On component, is added to an Active Directory domain, the Identity Source for that domain is automatically added to SSO.

1. Click on Configuration in the Single Sign-On section of the Navigator
2. Click on the Identity Sources tab

Identity Sources

Name	Server URL	Type	Domain	Alias
--	--	System Domain	vsphere.local	--
--	--	Local OS (Default)	localos	--
corp.local		Active Directory (Integrated Windows Authentication)	corp.local	corp.local

1. Notice that the corp.local domain is listed as an Active Directory identity source

Users in the domains listed here can be granted permissions within vSphere.

Add a vCenter Single Sign On User with the vSphere Client

In the vSphere Client, users listed on the Users tab are internal to vCenter Single Sign On. These users are not the same as local operating system users, which are local to the operating system of the machine where Single Sign On is installed (for example, Windows). When you add a Single Sign On user with the Single Sign On administration tool, that user is stored in the Single Sign On database, which runs on the system where Single Sign On is installed. These users are part of the SSO domain, by default, "vsphere.local" -- or "System-Domain" for vSphere 5.1. Exactly one system identity source is associated with an installation of Single Sign On.

List Current Users and Add New User

The screenshot shows the vSphere Client interface. On the left, there's a navigation sidebar with various categories like Administration, Access Control, Licensing, Solutions, Deployment, Support, Single Sign On, Certificates, and Configuration. Under Single Sign On, the 'Users and Groups' link is highlighted with a red box and has a black circle with the number 1 over it. In the main content area, the 'Users and Groups' page is displayed. At the top, there are tabs for 'Users' and 'Groups', with 'Users' being the active tab. Below the tabs, there's a 'Domain' dropdown set to 'vsphere.local' with a black circle containing the number 2 over it. In the center, there's a large 'ADD USER' button with a black circle containing the number 3 over it. The main area lists users with columns for Username and First Name. There are four users listed:

	Username	First Name
1	K/M	
2	Administrator	Administrator
3	waiter-367012 18-4663-4a46 -983a-6a6def 5589bc	waiter
4	waiter-add44 5ef-1b5f-451d-	waiter

1. Click on **Users and Groups** under Single Sign-On
2. From the drop-down list, select **vsphere.local** for the Domain
3. On the Users tab, click the **Add User**

Enter Properties for New User

Add User

1

Username *	holadmin
Password *
Confirm Password *
First Name	HOL
Last Name	Admin
Email	holadmin@vsphere.local

Description

2

CANCEL ADD

1. Fill out the New User form as follows:

- Username: holadmin
- Password: VMware1!
- Confirm password: VMware1!
- First name: HOL
- Last name: Admin
- Email address: holadmin@vsphere.local

2. Click ADD to create the user

NOTE: You cannot change the user's name after you create the user. First and Last name are optional parameters.

New User Added

Users and Groups

Users Groups

Domain vsphere.local

ADD USER

	Username	First Name	Last Name
⋮	walter-367012 18-4663-4a46 -983a-6a6def 5589bc	waiter	36701218-4663-4a46-983a-6a6def5589bc
⋮	walter-add44 5ef-1b5f-451d- 9f93-1b42be9 3af69	waiter	add445ef-1b5f-451d-9f93-1b42be93af69
⋮	krbtgt/VSPHE RE.LOCAL		
⋮	holadmin	HOL	Admin
1			

Here we can see the new user has been added.

1. Clicking on the three dots next to the username, allows for editing, deleting or disabling the user.

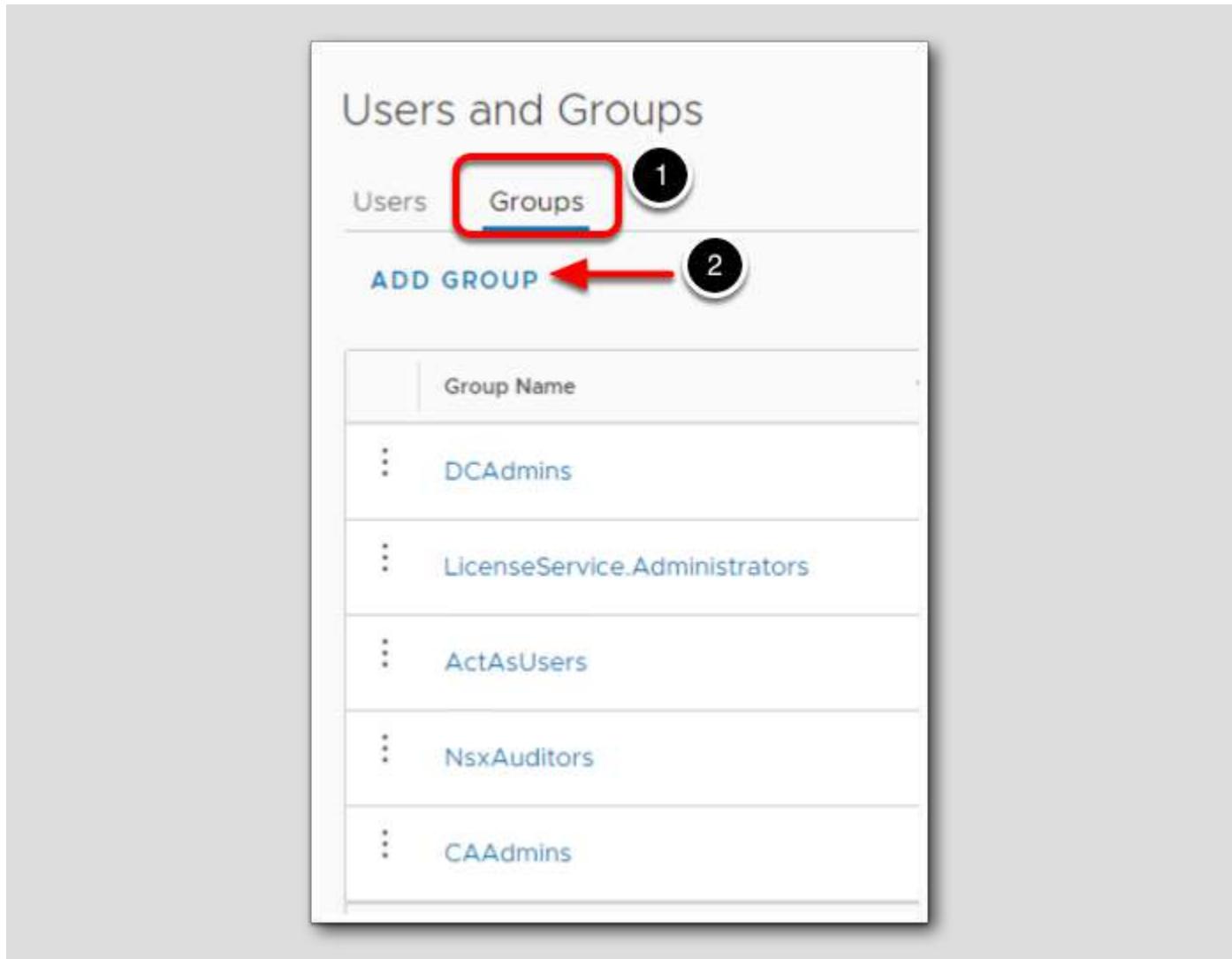
Add a vCenter Single Sign On Group with the vSphere Client

[425]

In the vSphere Client, groups listed on the Groups tab are internal to vCenter Single Sign On. A group lets you create a container for a collection of group members called principals. When you add a Single Sign On group with the Single Sign On administration tool, the group is stored in the Single Sign On database. The database runs on the system where Single Sign On is installed. These groups are part of the identity source domain vsphere.local (the default for vSphere 5.5 and higher), or System-Domain for vSphere 5.1.

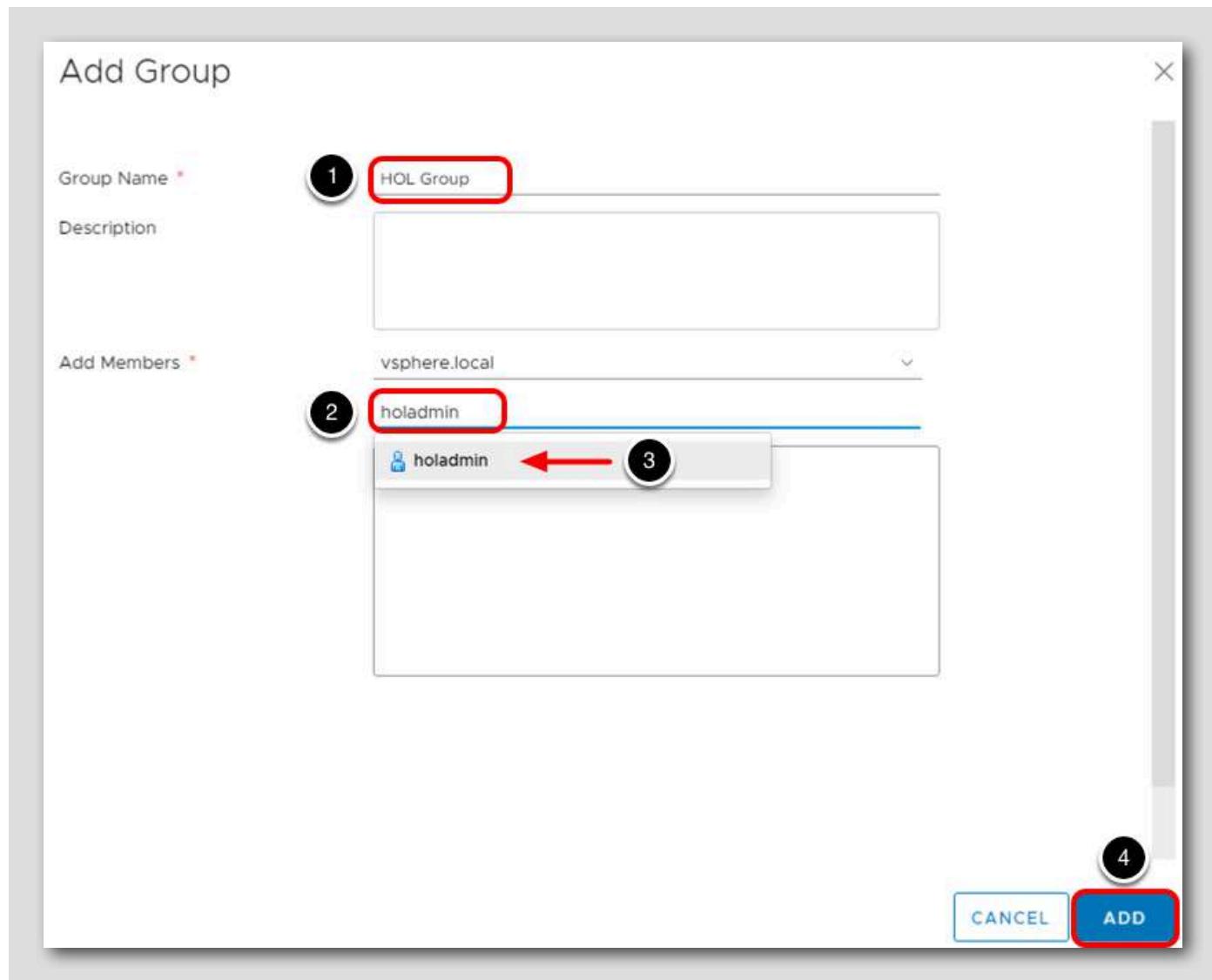
Group members can be users or other groups, and a group can contain members from across multiple identity sources. After you create a group and add principals, you apply permissions to the group. Members of the group inherit the group permissions.

Click Groups



1. Click Groups
2. Click Add Group

Create the new group



1. For the Group Name, type HOL Group
2. Add the user that was previously created by typing holadmin
3. Click **holadmin** from the drop-down list
4. Click the **ADD** button

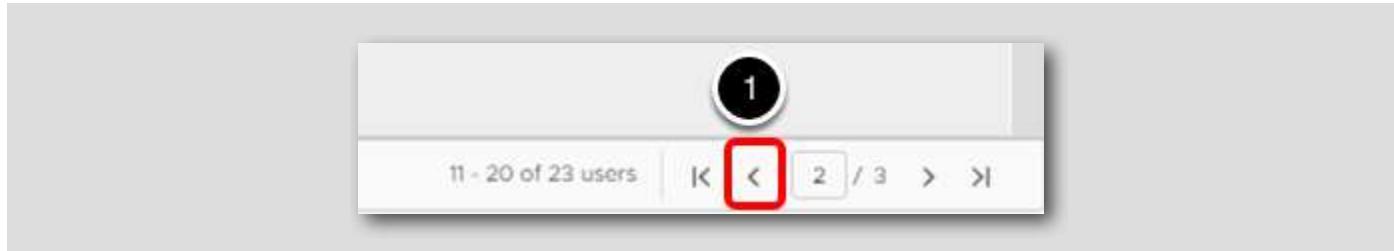
New Group Added

The screenshot shows the 'Users and Groups' interface in the vSphere Client. The 'Groups' tab is selected. At the top, there is an 'ADD GROUP' button. Below it, a table lists groups. The first group listed is 'SystemConfiguration.BashShellAdministrators' with the description 'Access bash shell and manage local users'. The second group listed is 'Users'. The third group listed is 'HOL Group', which is highlighted with a red rectangle and a black circle containing the number '2'. In the bottom right corner of the table area, there is a navigation bar with arrows and a page number '3 / 3', where the right arrow is also highlighted with a red rectangle and a black circle containing the number '1'.

1. Click on the arrow (→) to move to the third page of Groups
2. Here is the group, HOL Group that was just created

Add Members to a vCenter Single Sign On Group in the vSphere Client

Members of a vCenter Single Sign On group can be users or other groups from one or more identity sources. Members of a group are called principals. Groups listed on the Groups tab in the vSphere Client are internal to Single Sign On and are part of the identity source System-Domain. You can add group members from other domains to a local group. You can also nest groups.

[Return to Page 2](#)

1. Click on the left arrow (<) to return to the second page of Groups.

Add Members to Users and Groups

[431]

Group Name	Description
RegistryAdministrators	Allows members to manage the registry.
ComponentManager.Administrators	Component Manager Administrators
ServiceProviderUsers	Users allowed to manage WCP and VMC infrastructure.
AutoUpdate	Users allowed to perform update related operations
NsxViAdministrators	SSO group to manage NSX.
Administrators	1
DCClients	
SystemConfiguration.Administrators	Well-known configuration users' group which contains all configuration users as members.
vSphereClientSolutionUsers	vSphere Client Solution Users Group

1. Click on the Administrators group under the Group Names table

Note: You may need to scroll down to see it.

Add Members

The screenshot shows a user interface for managing administrators. At the top, the title 'Administrators' is displayed. Below it, there is a button labeled 'ADD MEMBERS' with a red rectangular border and a black circle containing the number '1'. A table lists two entries:

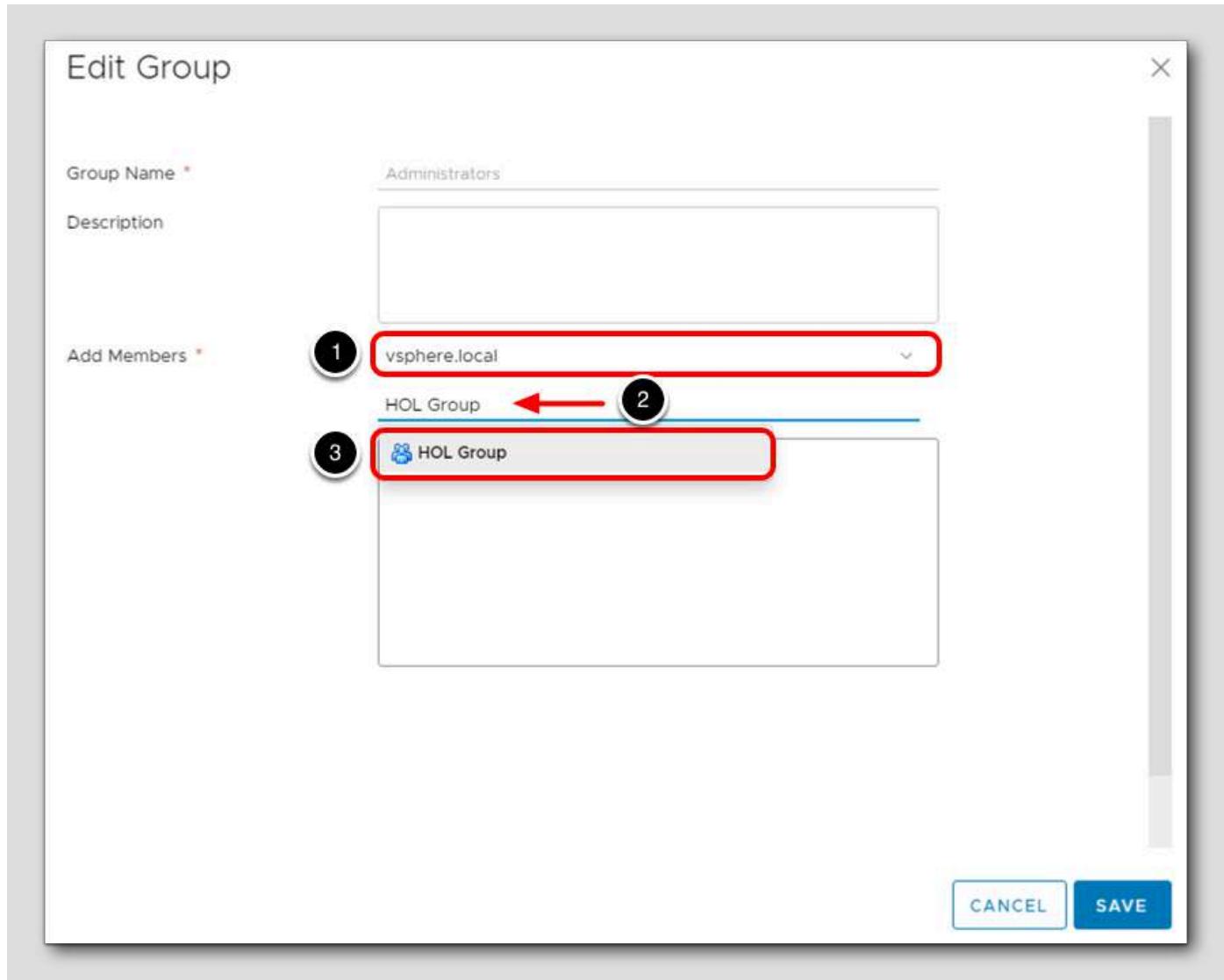
Member Name	Domain
Administrator	vsphere.local
Administrator	corp.local

At the bottom right of the table, the text '1 - 2 of 2 items' is visible.

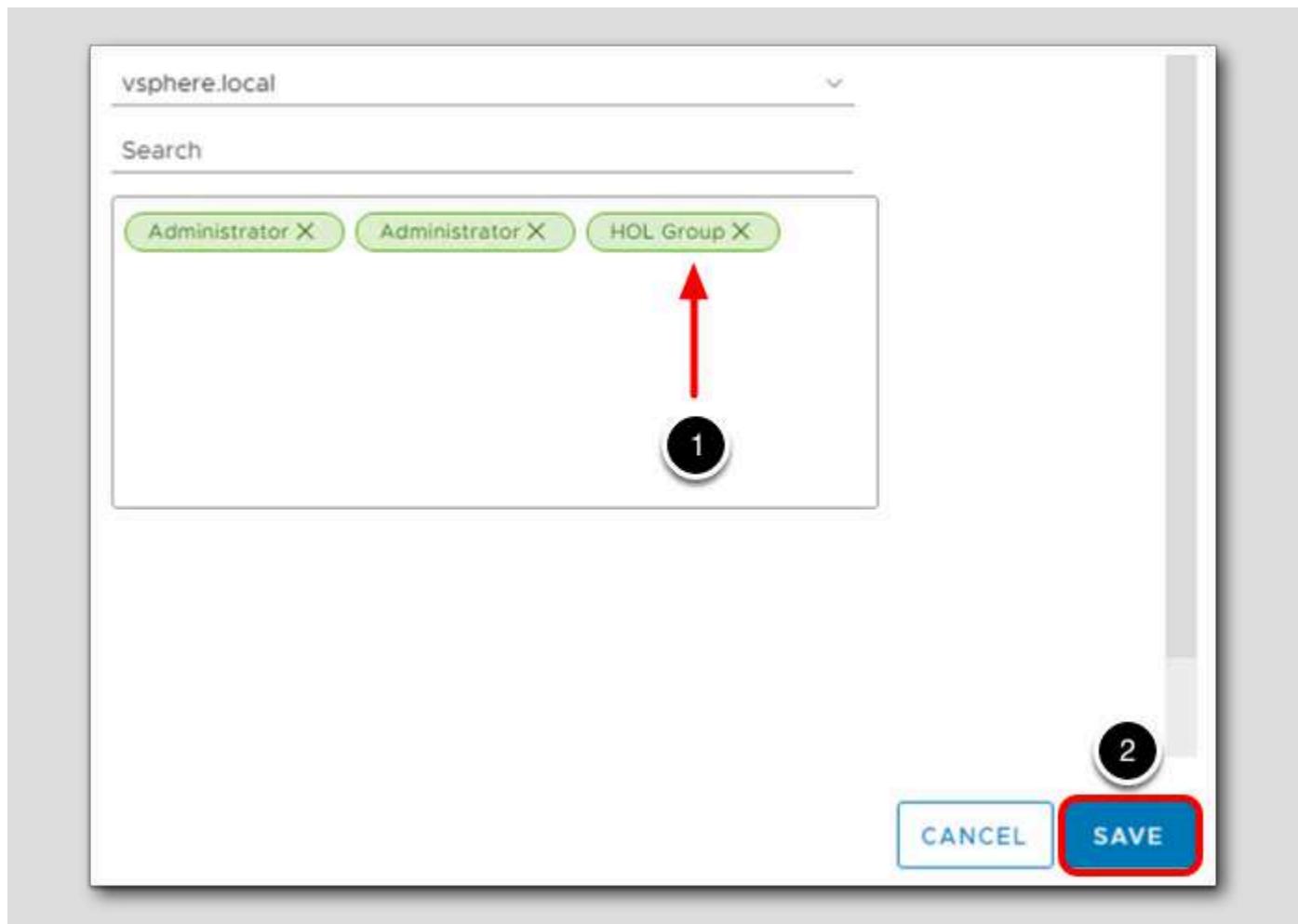
The Administrator account for the vsphere.local and corp.local domains are members.

1. Click Add Members

Edit Group



1. Make sure the domain selected is vsphere.local
2. Type HOL Group in the search box
3. Click on HOL Group to add it to the member list



1. You should see HOL Group added to the list.

2. Click Save.

New Member Added

Users and Groups

Groups

< ALL GROUPS

Administrators

ADD MEMBERS

Member Name	Domain
Administrator	vsphere.local
Administrator	corp.local
HOL Group	vsphere.local

1 - 3 of 3 items

The HOL Group has now been added to the Administrator group.

Assign Global Permissions

Once identity sources, users and groups have been configured, they must be assigned permissions in order to be useful in vSphere.

List Global Permissions

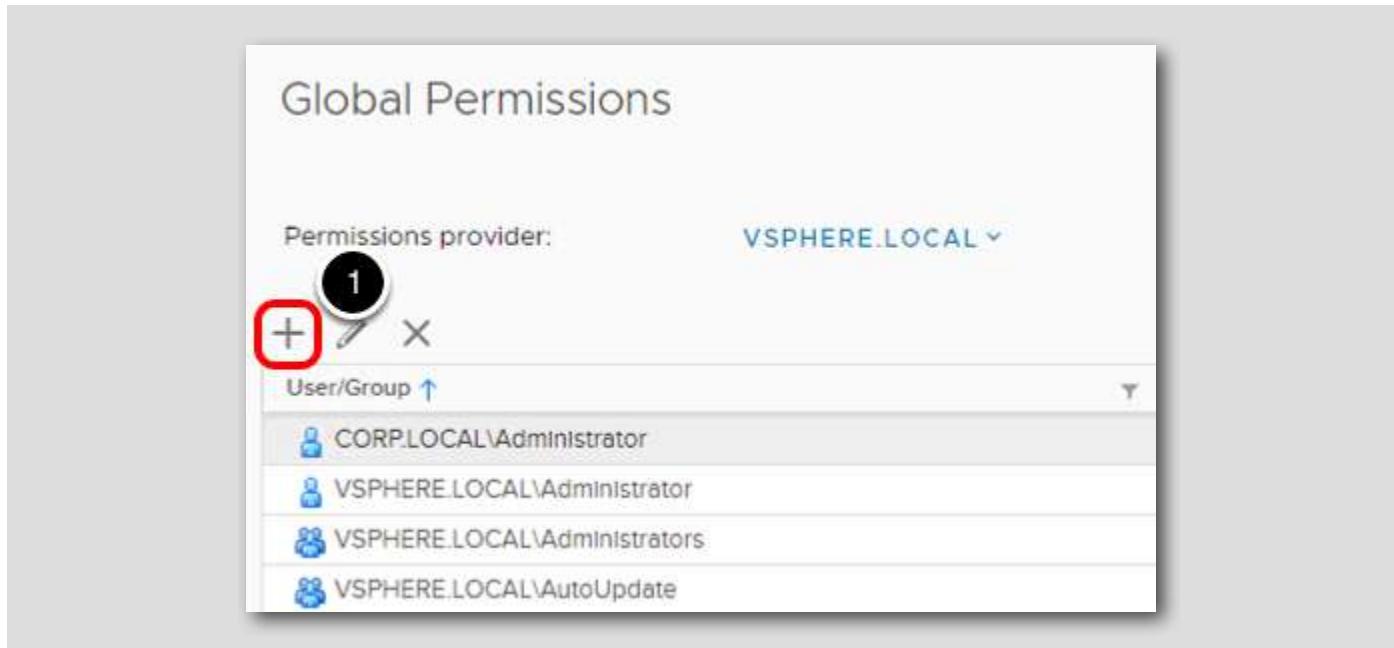
The screenshot shows the vSphere Client interface with the title bar "vSphere Client". The left sidebar has a "Administration" section with "Access Control" expanded, showing "Global Permissions" highlighted with a red box and a circled "1". Other sections include "Licensing", "Solutions", and "Deployment". The main pane is titled "Global Permissions" and shows a list of users and groups under "Permissions provider: VS SPHERE.LOCAL". The list includes:

User/Group
CORP.LOCAL\Administrator
VS SPHERE.LOCAL\Administrator
VS SPHERE.LOCAL\Administrators
VS SPHERE.LOCAL\AutoUpdate
VS SPHERE.LOCAL\NsxAdministrators

1. Click on the Global Permissions item under Access Control

SSO provides the ability to grant Global Permissions to an account by specifying the required access here. In the lab, this list represents the default permissions granted, with the exception of the CORP.LOCAL\Administrator user that we have added with Administrator permissions to the entire vSphere infrastructure.

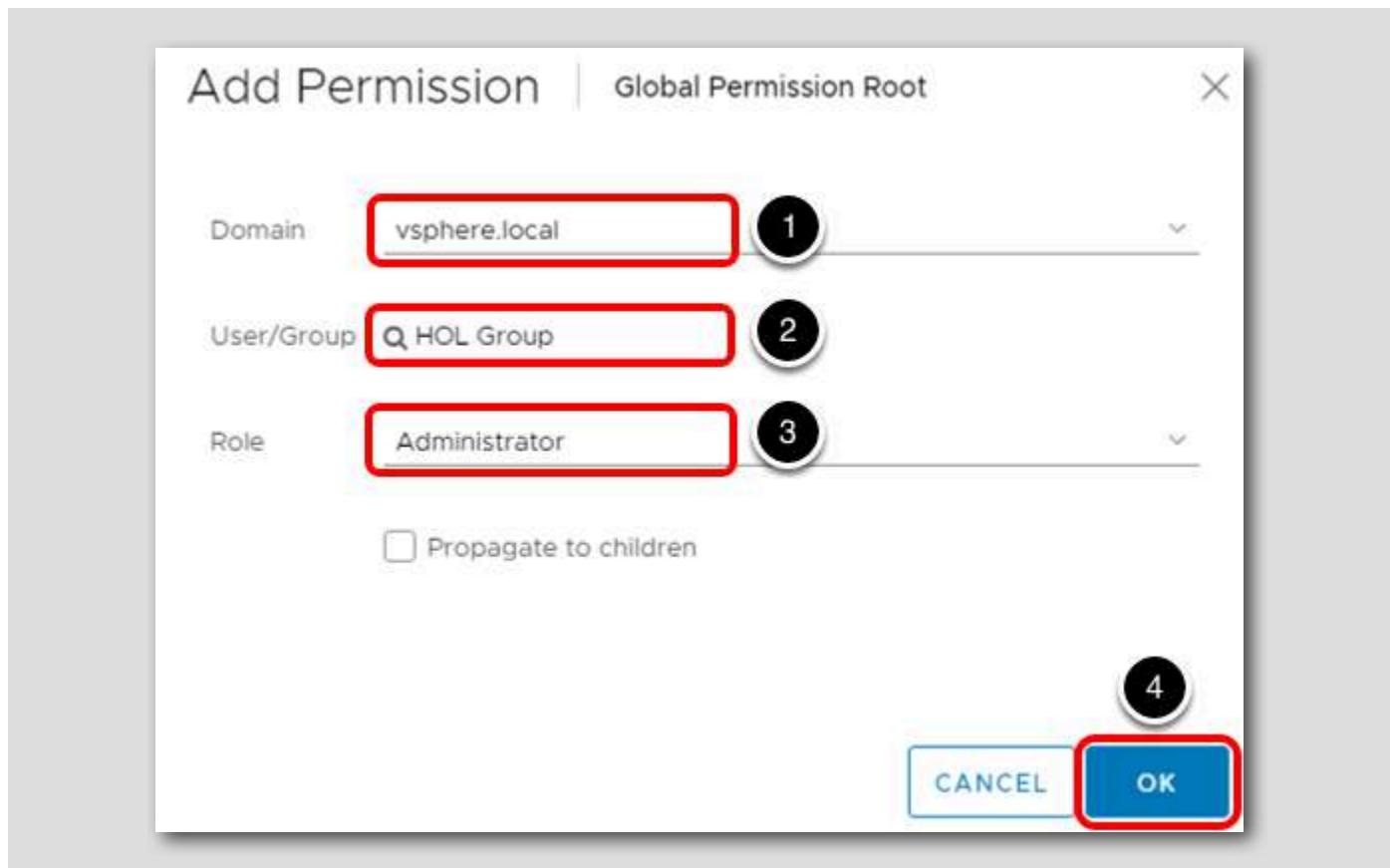
Add New Global Permission



The members of the HOL Group will need to manage all virtual machines in the environment, so we will configure permissions here.

1. Click the plus button (+) to open the Add New Permission window

Locate the HOL Group



1. Ensure that the **vsphere.local** domain is selected
2. Type **HOL Group** in the search field
3. For the Role, select the **Administrator** group
4. Click the **OK** button

New Global Permission

The screenshot shows the 'Global Permissions' interface in the vSphere Web Client. The permissions provider is set to 'VSphere.LOCAL'. A new entry has been added for the group 'VSphere.LOCAL\HOL Group', which is highlighted with a red box and a circled '1'.

User/Group	Role	Defined In
CORP.LOCAL\Administrator	Administrator	Global Permission
VSphere.LOCAL\Administrator	Administrator	Global Permission
VSphere.LOCAL\Administrators	Administrator	Global Permission
VSphere.LOCAL\AutoUpdate	AutoUpdateUser	Global Permission
VSphere.LOCAL\HOL Group	Administrator	Global Permission
VSphere.LOCAL\NsxAdministrators	NSX Administrator	Global Permission
VSphere.LOCAL\NsxAuditors	NSX Auditor	Global Permission

The newly created `vsphere.local` Global Permission has been created.

Conclusion

Typically, user accounts will not be managed naively within the SSO domain, but will be handled by an external directory source like Microsoft Active Directory or OpenLDAP. Understanding how SSO handles accounts and where to look for account-to-permission binding is useful for managing a vSphere implementation.

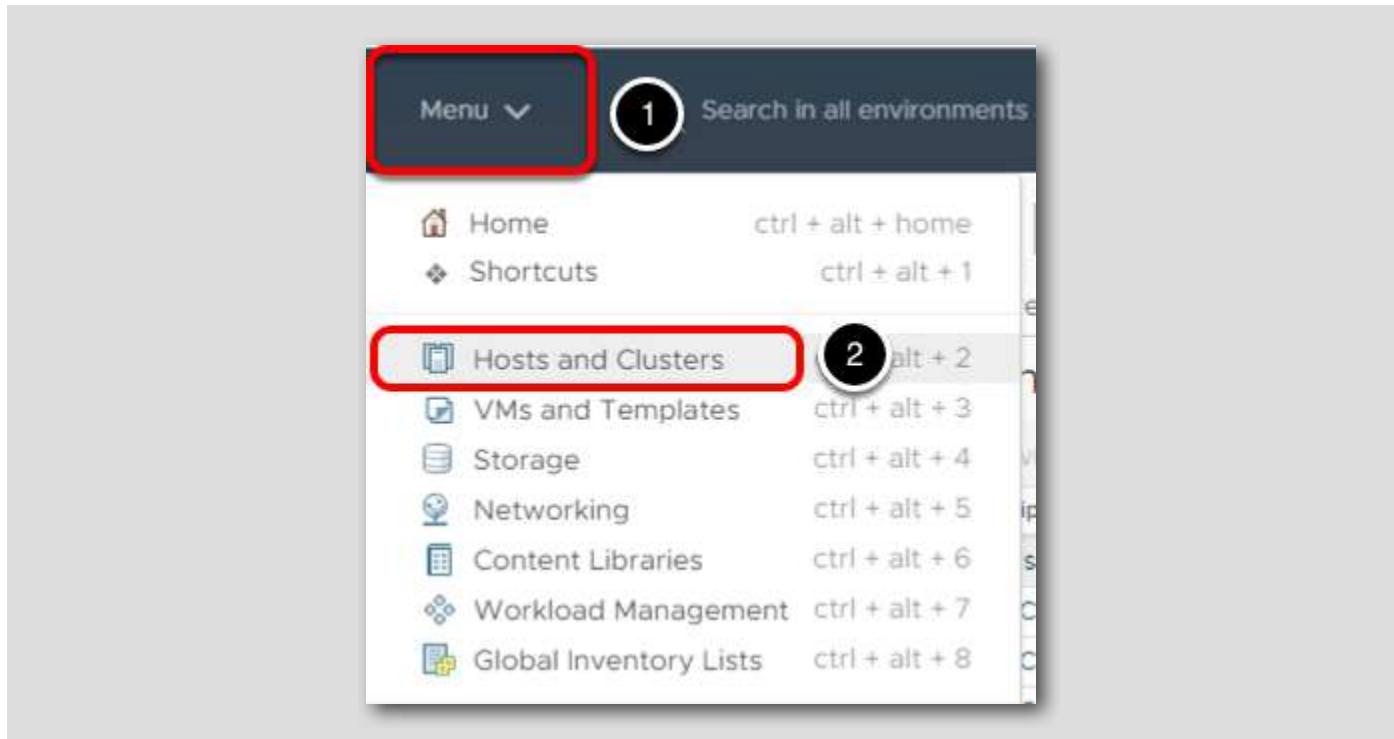
Adding an ESXi Host to Active Directory

In this lesson, we will walk through the process of adding an ESXi host to Active Directory.

Configure a Host to Use Active Directory in the vSphere Web Client

In this lesson, we walk through the process of adding a vSphere Host to authenticate against Active Directory.

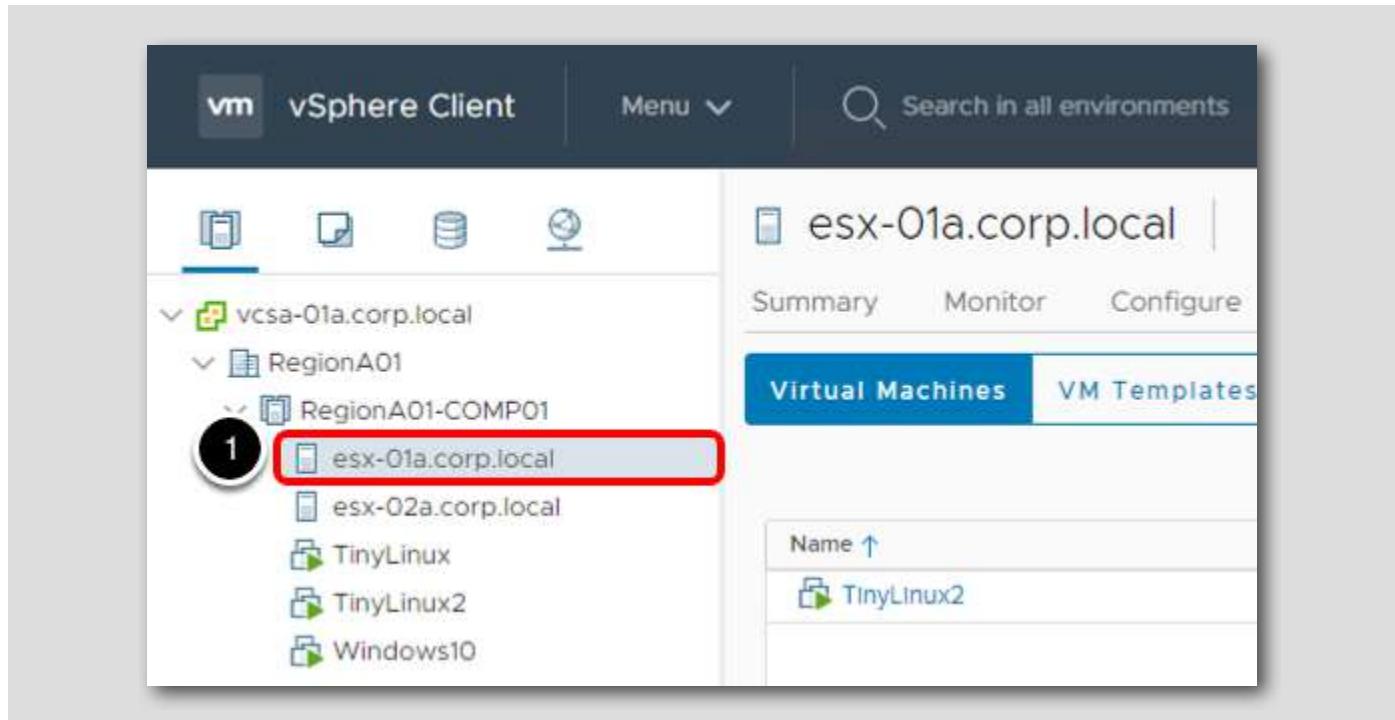
Hosts and Clusters



1. Click on **Menu**

2. Select **Hosts and Clusters**

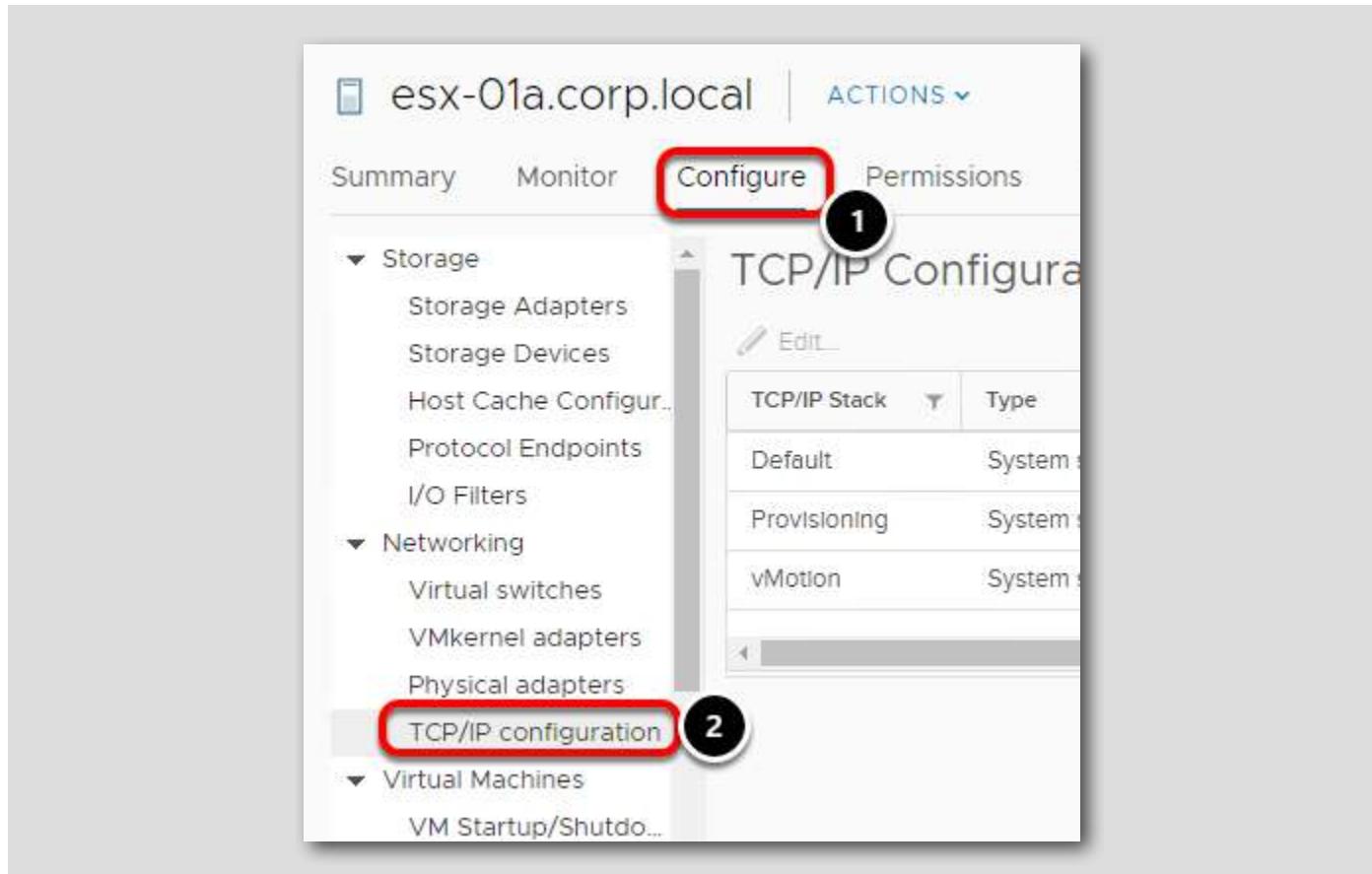
esx-01a.corp.local



1. Click on esx-01a.corp.local

Note: You may need to expand Site A Datacenter and/or Site A Cluster 1 to see the host.

TCP/IP Configuration



1. Click on the Configure tab
2. Select the TCP/IP configuration in the Networking section

Edit Default System Stack

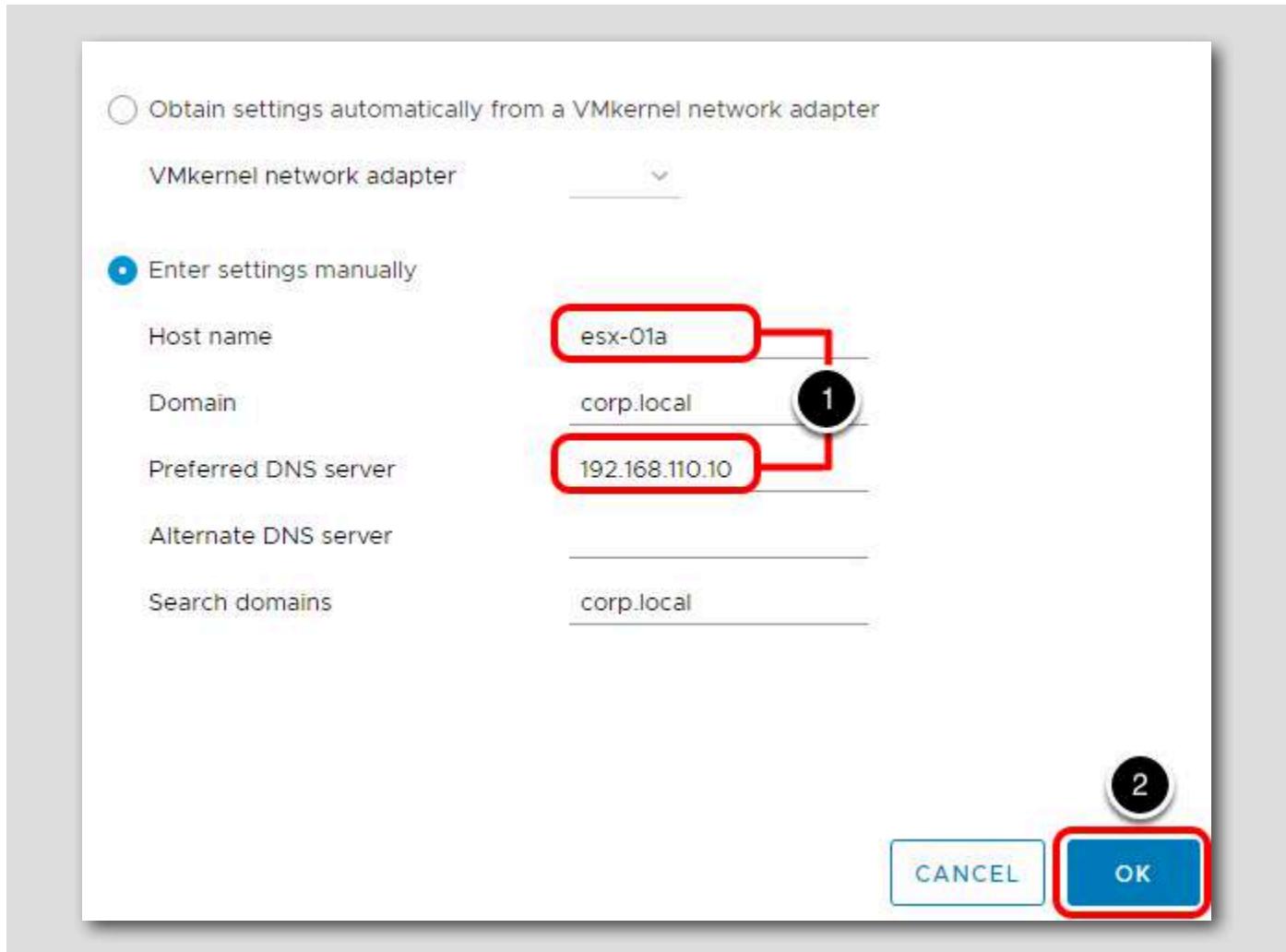
The screenshot shows the vSphere Web Client interface for managing system stacks. The host name is esx-01a.corp.local. The 'Configure' tab is selected. On the left, under 'Storage' and 'Networking', there are dropdown menus. Under 'Networking', 'TCP/IP configuration' is selected. On the right, the 'TCP/IP Configuration' section is displayed with the title 'TCP/IP Configuration'. It shows a table with three rows:

TCP/IP Stack	Type	VMkernel...
Default	System stack	2
Provisioning	System stack	0
vMotion	System stack	1

Row 1 ('Default') is highlighted with a red box. A black circle with the number '1' is on the left of the row. A red box highlights the 'Edit...' button next to the row. A black circle with the number '2' is on the left of the 'Edit...' button.

1. Click on Default under System stacks
2. Click the Pencil Icon to edit the stack

DNS configuration



1. Verify that the host name (esx-01a) and DNS server information (192.168.110.10) for the host are correct
2. Click OK

Add a Host to a Directory Service Domain in the vSphere Client

The screenshot shows the vSphere Client interface for a host named "esx-01a.corp.local". The "Configure" tab is selected. On the left, there is a navigation tree with categories like Storage, Networking, Virtual Machines, System, and Authentication Services. The "Authentication Services" item is highlighted with a red box and has a black circle with the number "1" above it. To the right of the navigation tree, there are several configuration panels: "Authentication" (with "Directory Services Configuration" and "Domain Settings" sections), "Smart Card Authentication" (with "When enabled, the S" text), "Smart Card Mode" (disabled), and "Certificates". At the bottom, there is a "NFS Kerberos" section with a "State" button.

Now that the network settings have been verified, the host will be added to Active Directory.

1. Click on **Authentication Services** under the System section

You may need to scroll down to see it

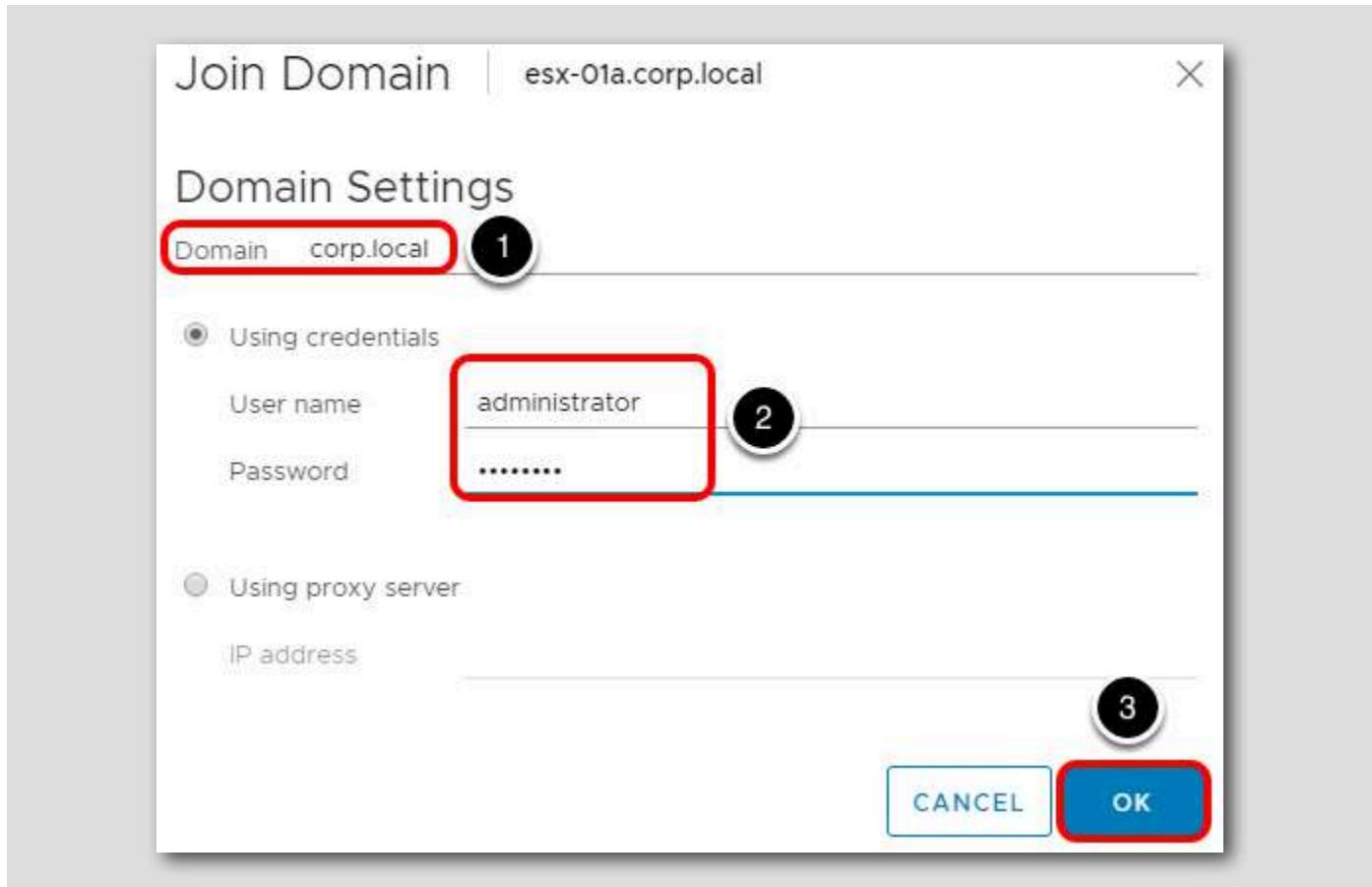
Join Domain

[449]

The screenshot shows the 'Authentication Services' configuration page in the vSphere Web Client. At the top, there are tabs for 'Configure', 'Permissions', 'VMs', 'Datastores', 'Networks', and 'Updates'. Below the tabs, the 'Authentication Services' section is displayed. On the right side of this section, there are two buttons: 'IMPORT CERTIFICATE...' and 'JOIN DOMAIN...'. A large red box surrounds the 'JOIN DOMAIN...' button, and a black circle with the number '1' is positioned above it, indicating the first step in the process. The 'JOIN DOMAIN...' button is blue with white text. The rest of the page contains configuration options for directory services and smart card authentication.

1. Click the Join Domain button.

Join Domain Settings



1. Enter **corp.local** for the Domain
2. In the Using Credentials section enter:
 - Username: **administrator**
 - Password: **VMware1!**
3. Click **OK**

Recent Tasks

Task Name	Target	Status	Details
List Smart Card Trust Anchors	esx-01a.corp.local	✓ Completed	
Join Windows Domain	esx-01a.corp.local	✓ Completed	
List Smart Card Trust Anchors	esx-01a.corp.local	✓ Completed	

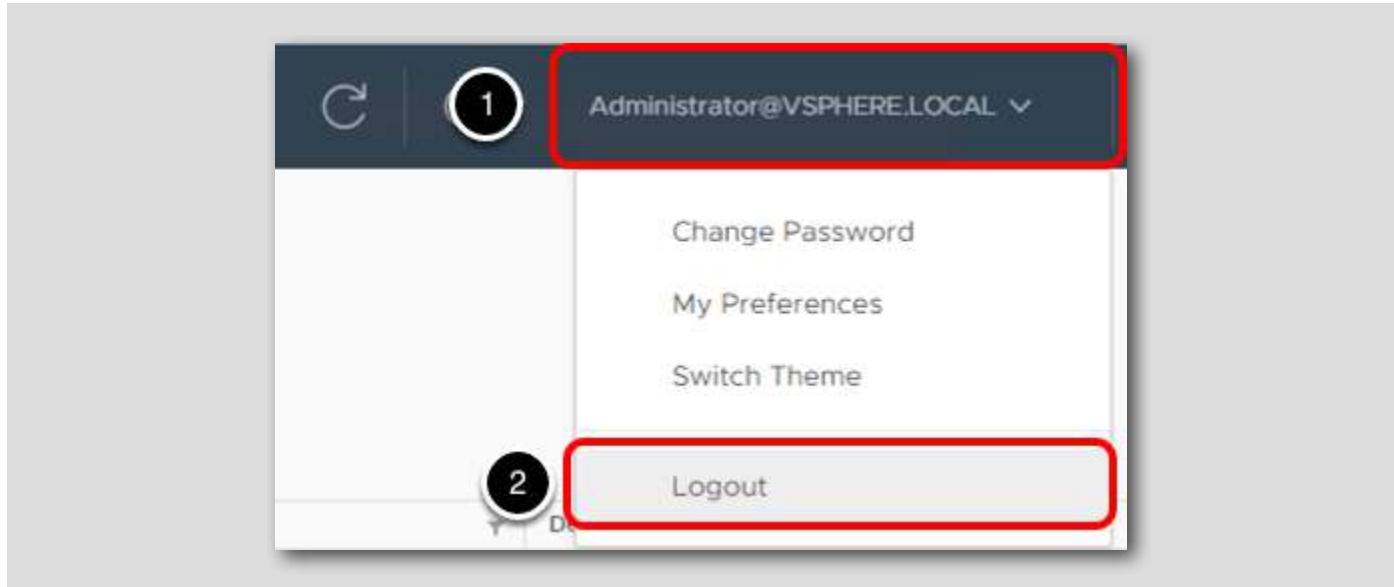
Progress can be monitored using the Recent Tasks window. It should take a minute or two to complete.

Added to Active Directory

The screenshot shows the vSphere Web Client interface for host `esx-01a.corp.local`. The `Configure` tab is selected. In the `Authentication Services` section, the `Directory Services Configuration` is set to `Active Directory`, and the `Domain Settings` show the domain as `CORP.LOCAL`. The `Smart Card Authentication` section indicates that Smart Card Mode is currently disabled.

Section	Setting	Value
Directory Services Configuration	Directory Services Type	Active Directory
Domain Settings	Domain	CORP.LOCAL
Smart Card Authentication	Smart Card Mode	Disabled

Once the task has been completed, the Authentication Services section will update to show the host is now connected to the Active Directory domain.

[Log out](#)

If you are continuing on to other modules in this lab, please log out as administrator@vsphere.local.

1. Click Administrator@VSPHERE.LOCAL
2. Click Logout

Conclusion

[454]

This concludes Module 2 - An Introduction to vSphere Networking and Security . We hope you have enjoyed taking this lab. Please remember to take the survey at the end.

If you have time remaining, here are the other Modules that are part of this lab, along with an estimated time to complete each one. Click on the Table of Contents button to quickly jump to that module in the manual.

- Module 1 - An Introduction to Management with vCenter Server (60 Minutes)
- Module 3 - An Introduction to vSphere Storage (60 Minutes)

Certification Path

[455]

Learn and Practice with Hands-On Labs to help prepare for several VMware Certifications.

vmware[®]

CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

This Lab can help you study for the industry-recognized VCAP-DCV Deploy 2021 Deploy certification which validates that you know how to deploy and optimize VMware vSphere infrastructures.

Learn More Here https://via.vmw.com/dcv_deploy

vmware[®]
CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

Module 3 - Introduction to vSphere Storage (60 Min)

vSphere Storage Overview

[457]

The following lesson provides an overview of the different types of storage available in vSphere.

The vSphere Hypervisor, ESXi, provides host-level storage virtualization, which logically abstracts the physical storage layer from virtual machines.

A vSphere virtual machine uses a virtual disk to store its operating system, program files, and other data associated with its activities. A virtual disk is a large physical file, or a set of files, that can be copied, moved, archived, and backed up as easily as any other file. You can configure virtual machines with multiple virtual disks.

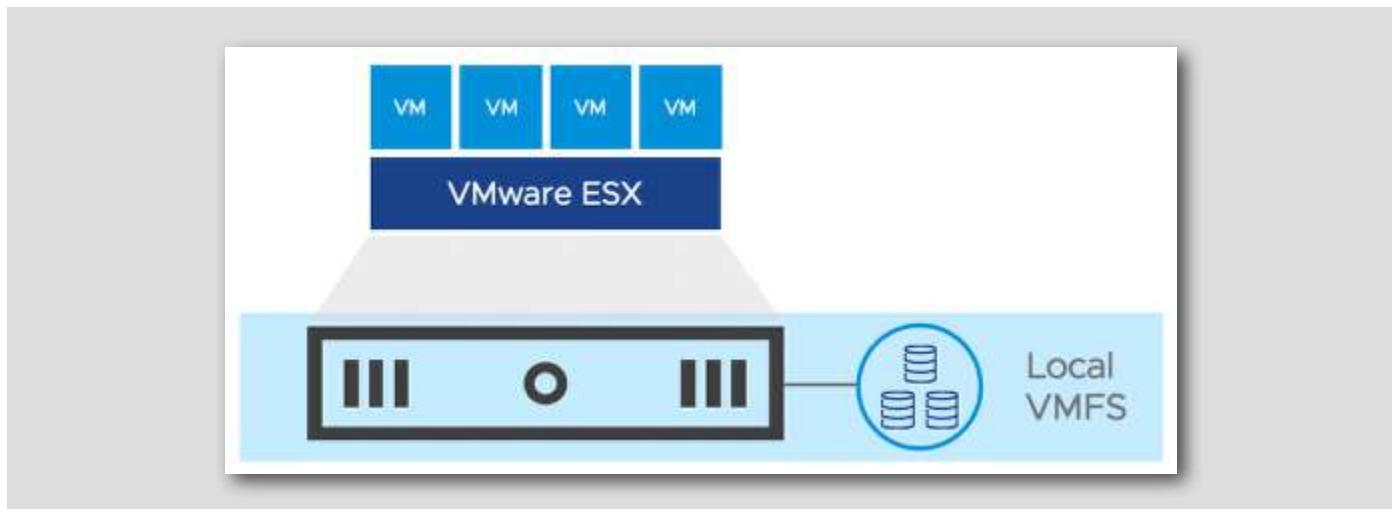
To access virtual disks, a virtual machine uses virtual SCSI controllers. These virtual controllers include BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. These controllers are the only types of SCSI controllers that a virtual machine can see and access.

Each virtual disk resides on a vSphere Virtual Machine File System (VMFS) datastore or an NFS-based datastore that are deployed on physical storage. From the standpoint of the virtual machine, each virtual disk appears as if it were a SCSI drive connected to a SCSI controller. Whether the actual physical storage device is being accessed through parallel SCSI, iSCSI, network, Fibre Channel, or FCoE adapters on the host is transparent to the guest operating system and to applications running on the virtual machine.

The vSphere storage management process starts with storage space that your storage administrator allocates on different storage systems prior to vSphere ESXi assignment. vSphere supports two types of storage - Local and Networked. Each type is detailed in the following lesson steps.

Local Storage

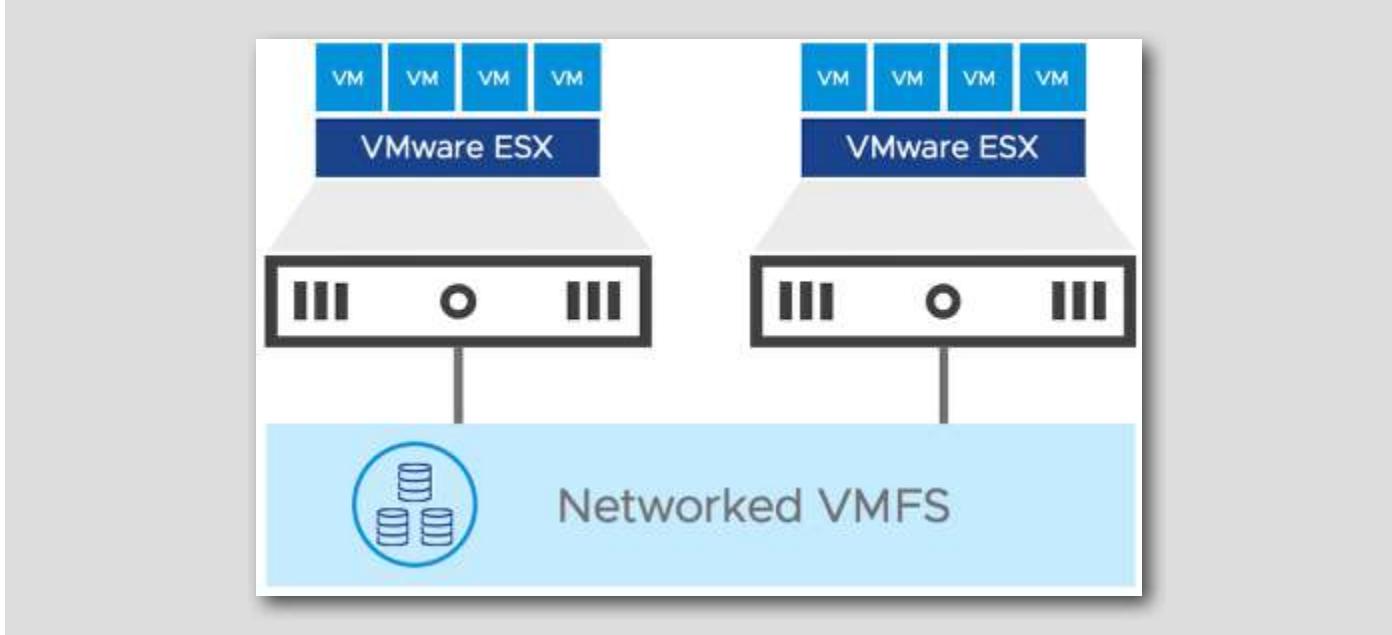
[458]



The illustration above depicts virtual machines using Local VMFS storage directly attached to a single ESXi host.

Local storage can be internal hard disks located inside your ESXi host, or it can be external storage systems located outside and connected to the host directly through protocols such as SAS or SATA.

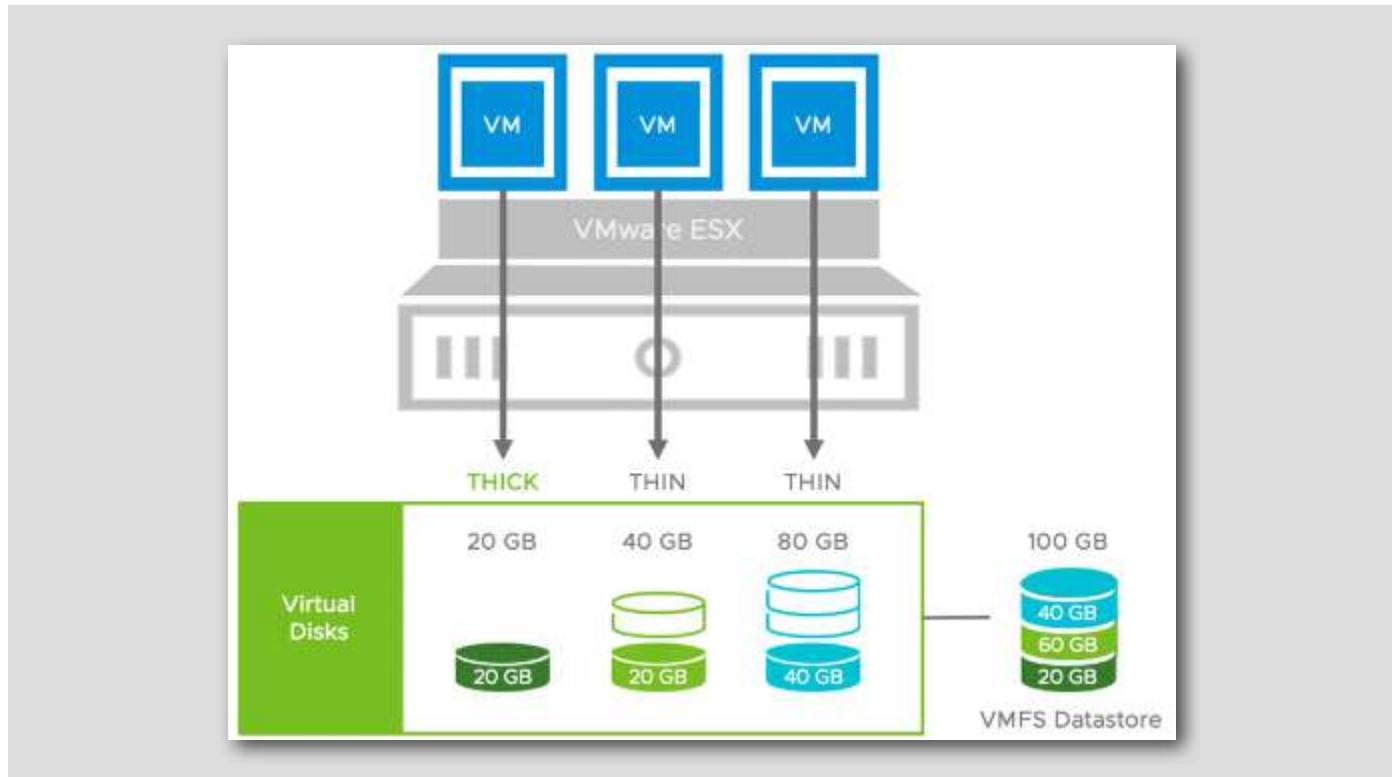
Networked Storage



The illustration above depicts virtual machines using networked VMFS storage presented to multiple ESXi hosts.

Networked storage consists of external storage systems that your ESXi host uses to store virtual machine files remotely. Typically, the host accesses these systems over a high-speed storage network. Networked storage devices are typically shared. Datastores on networked storage devices can be accessed by multiple hosts concurrently, and as a result, enable additional vSphere technologies such as High Availability host clustering, Distributed Resource Scheduling, vMotion and Virtual Machines configured with Fault Tolerance. ESXi supports several networked storage technologies - Fiber Channel, iSCSI, NFS, and Shared SAS.

Virtual Machine Disks



The illustration above depicts virtual machines using different types of virtual disk formats against a shared VMFS Datastore.

When you perform certain virtual machine management operations, such as creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine, you can specify a provisioning policy for the virtual disk file format. There are three types of virtual disk formats:

Thin Provision

Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

Thick Provision Lazy Zeroed

Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.

Using the thick-provision, lazy-zeroed format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space. You cannot convert a thick-provisioned, lazy-zeroed disk to a thin disk.

Thick Provision Eager Zeroed

A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick-provision, lazy-zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. In general, it takes much longer to create disks in this format than to create other types of disks.

Creating and Configuring vSphere Datastores

[461]

This lesson will walk you through creating and configuring an NFS, and an iSCSI vSphere Datastore. Also adding and configuring an iSCSI software adapter.

Launch Google Chrome web browser

[462]



1. Click on the Chrome Icon on the Windows Quick Launch Task Bar

Enter credentials and log in

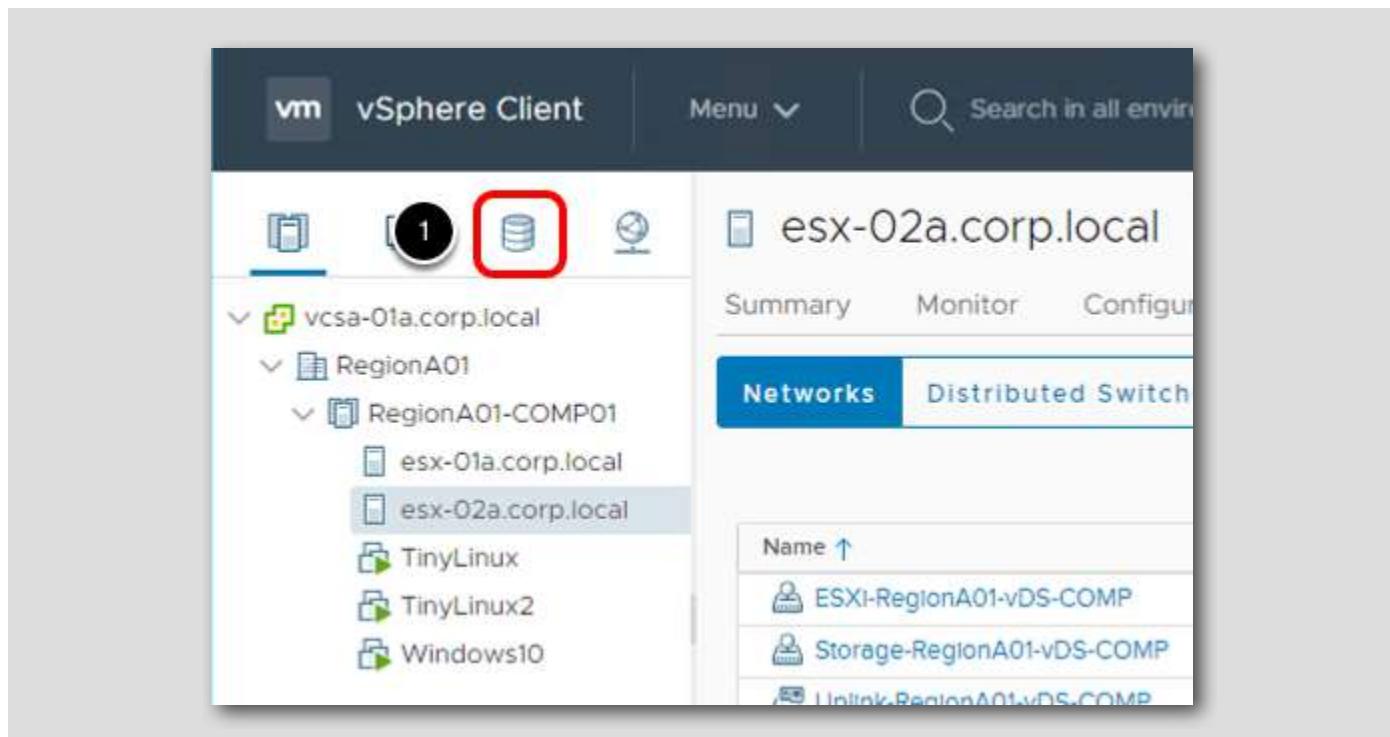


1. Select "Use Windows session authentication" check box
2. Select Login

If credentials aren't saved, use the following:

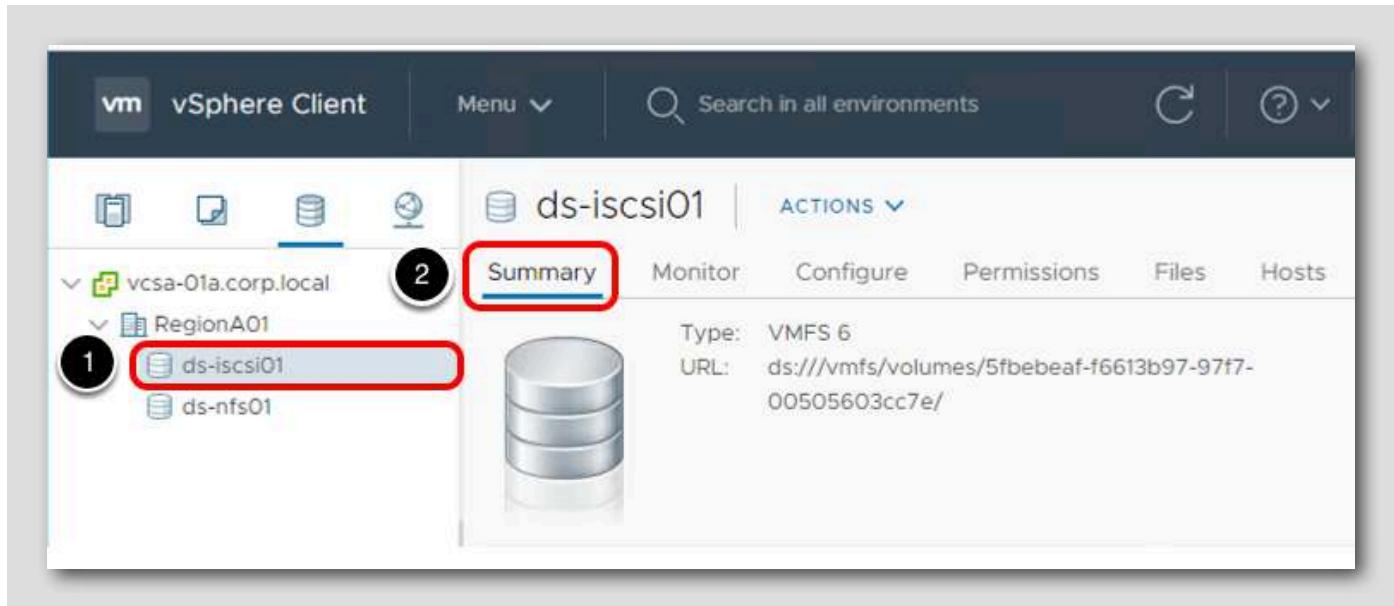
- username: administrator@corp.local
- password: VMware1!

Navigate to Storage Management



1. Select the Storage tab.

Expand RegionA01 Datacenter

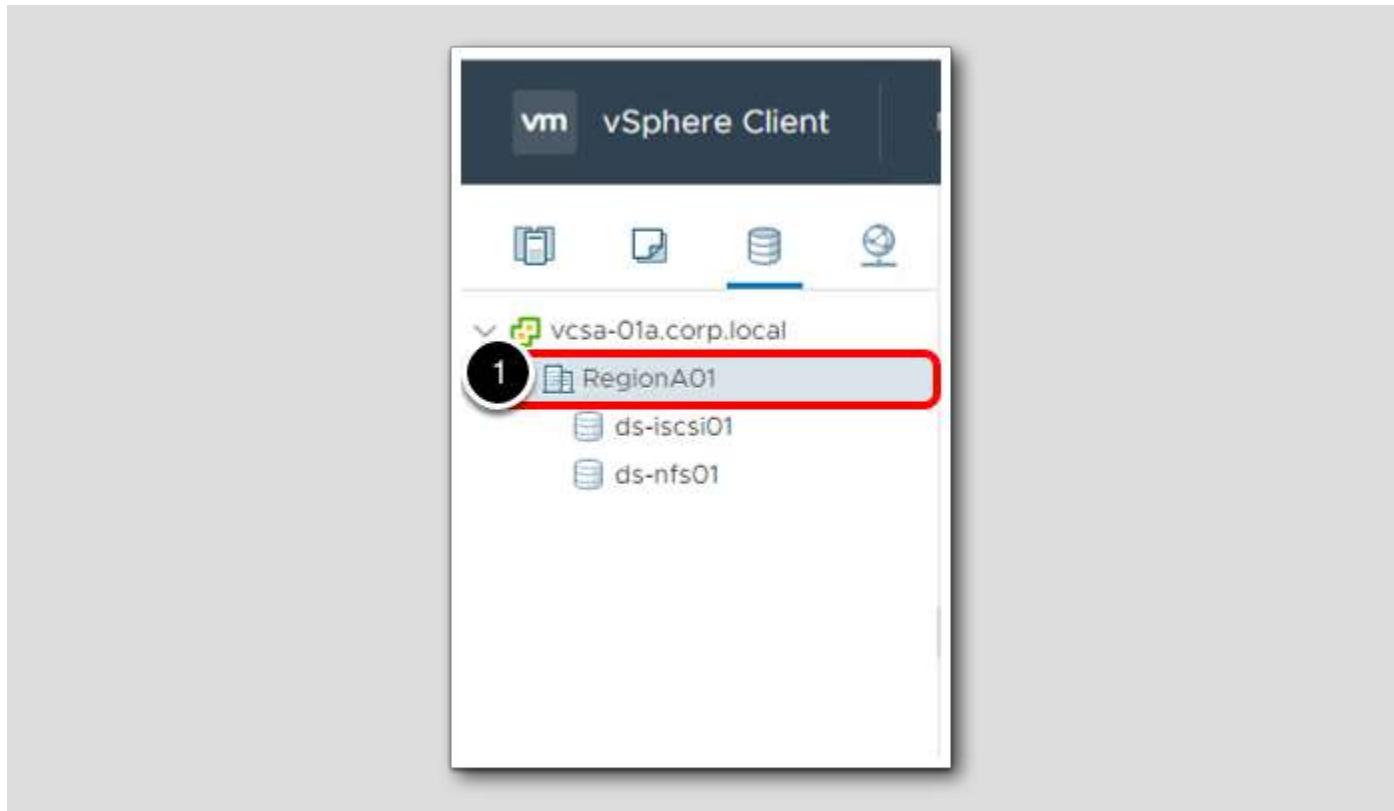


There are 2 storage datastores configured, an iSCSI datastore and an NFS datastore.

1. Select the **ds-iscsi01** datastore.
2. Click on **Summary** for summary details of the datastore.

Repeat the steps for the **ds-nfs01** datastore.

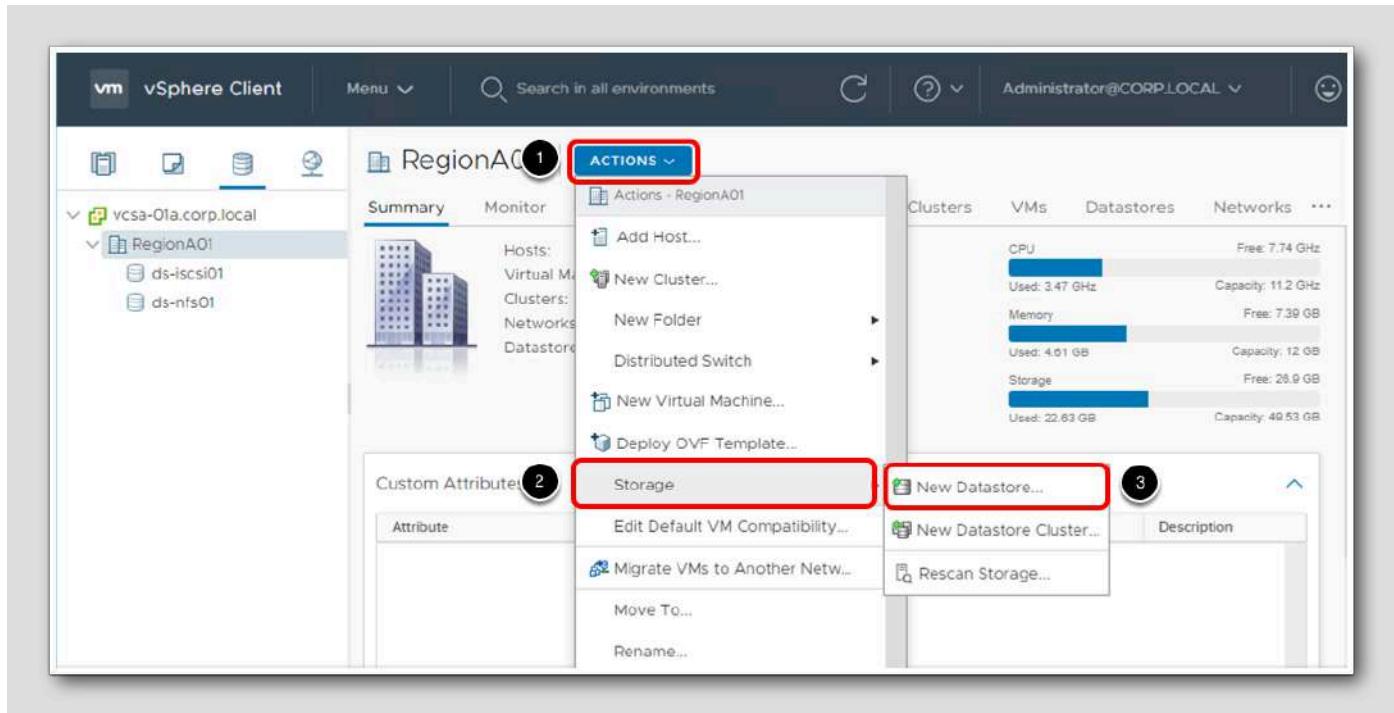
Create a vSphere NFS Datastore



In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select RegionA01 Datacenter.

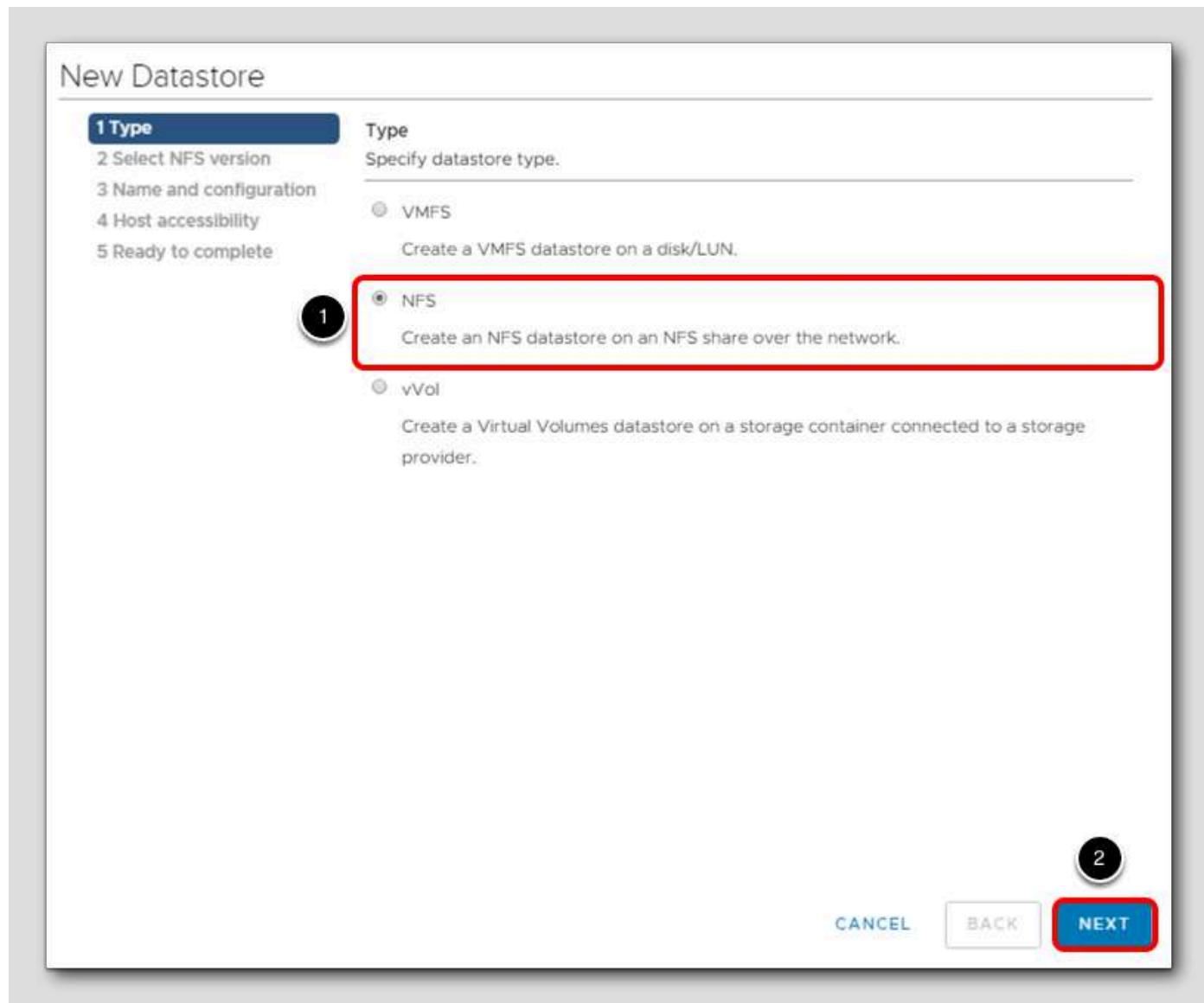
New Datastore



In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

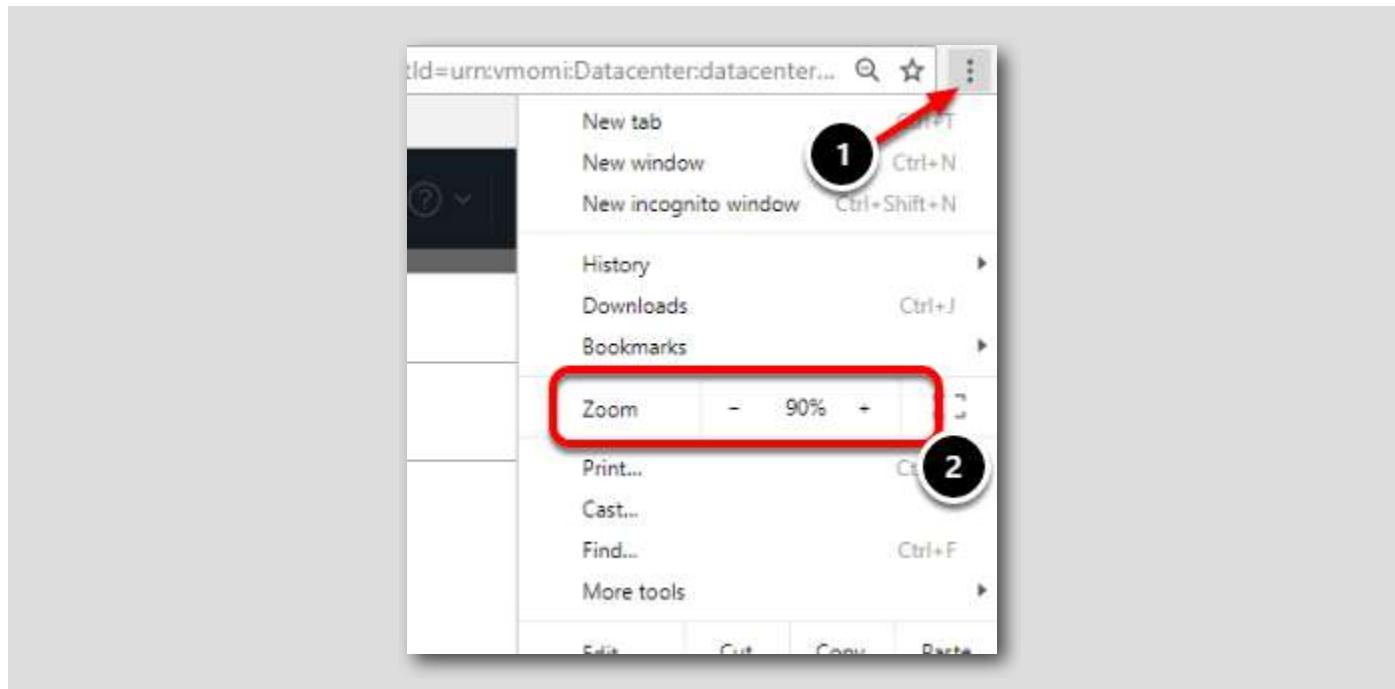
1. Select Actions.
2. Select Storage.
3. Select New Datastore.

New Datastore - Type



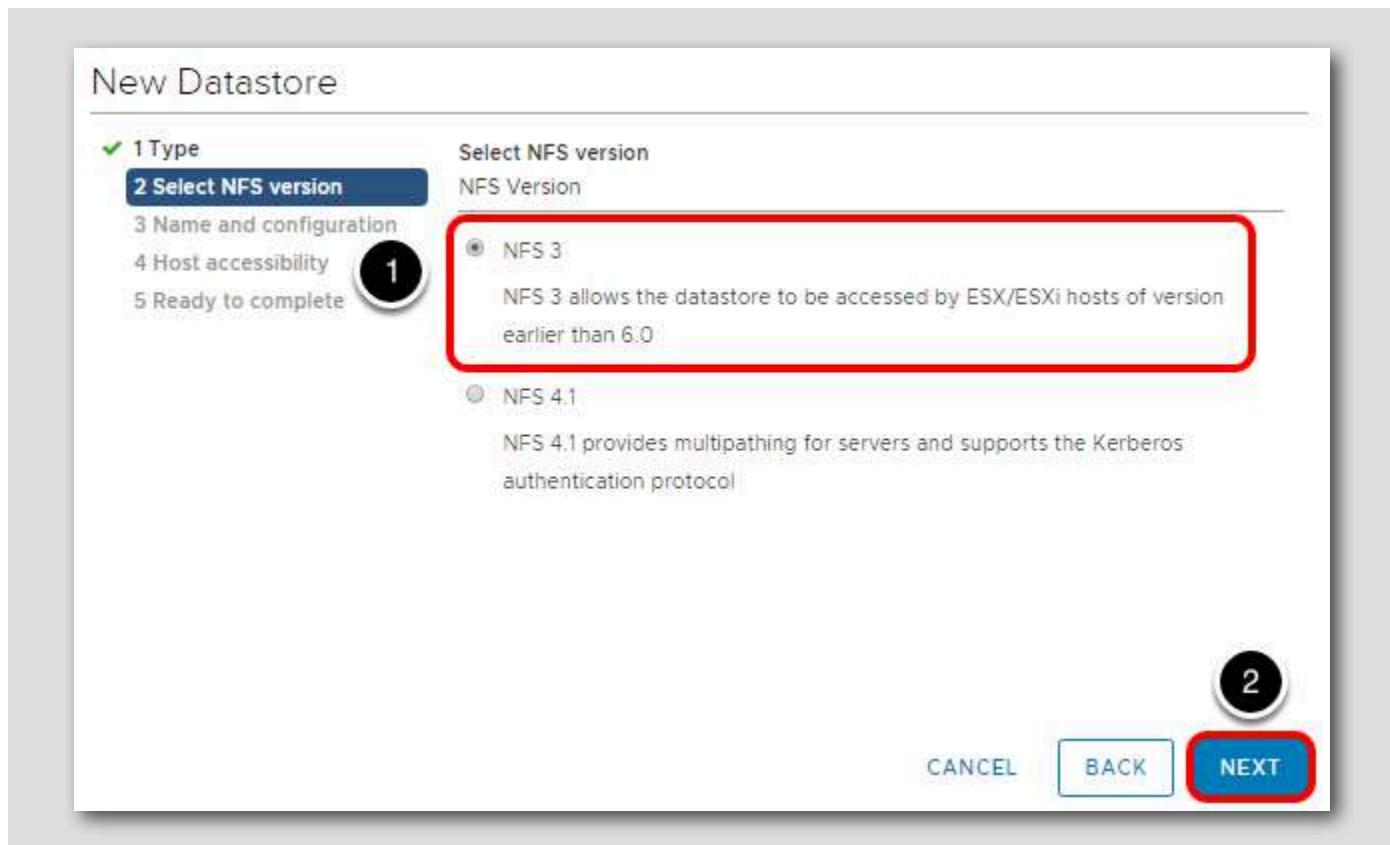
1. Select NFS for the new Datastore type

2. Click **Next**



Note: You may need to zoom out in order to see the Next button.

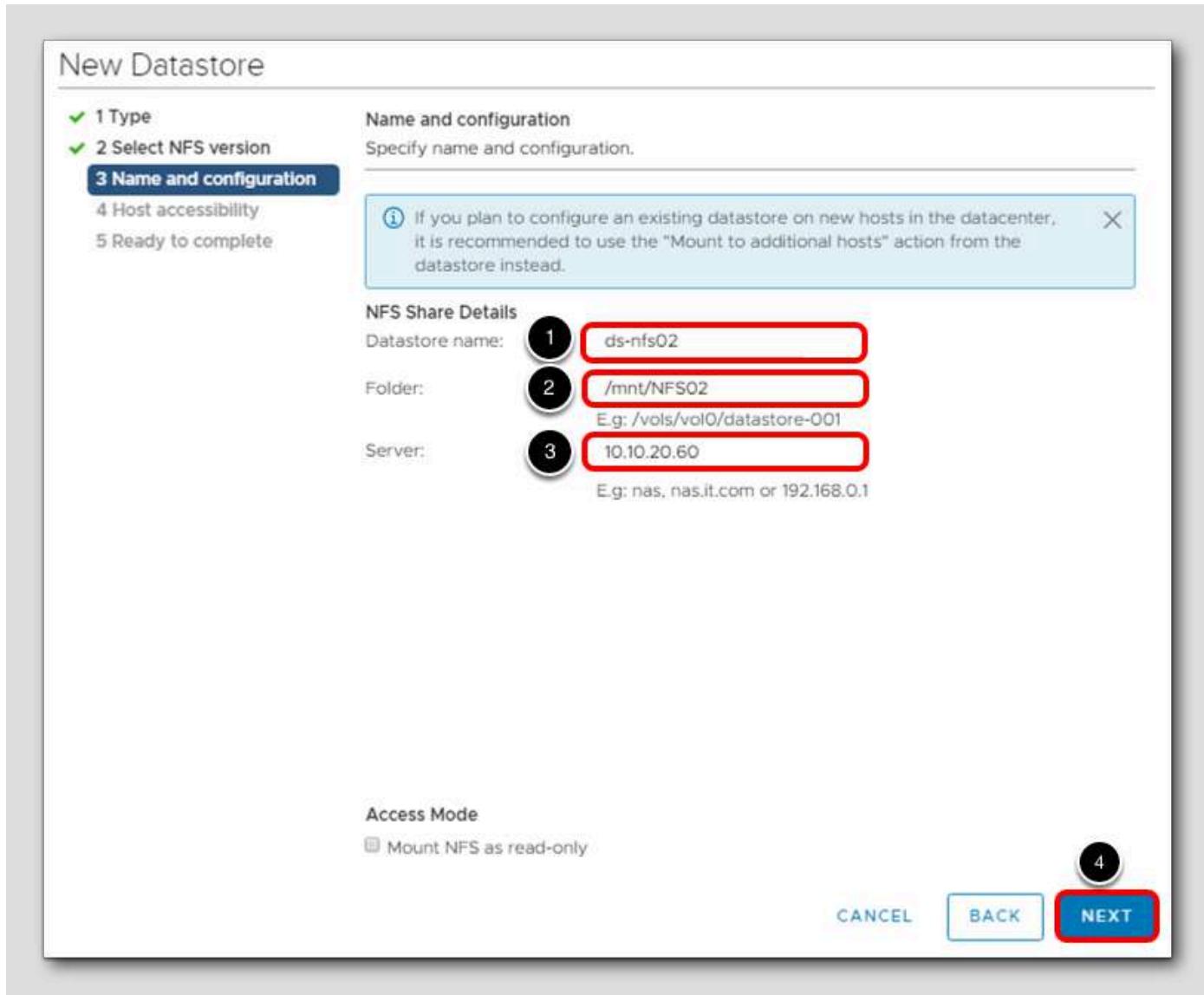
New Datastore - NFS Version



1. Verify NFS Version - NFS 3

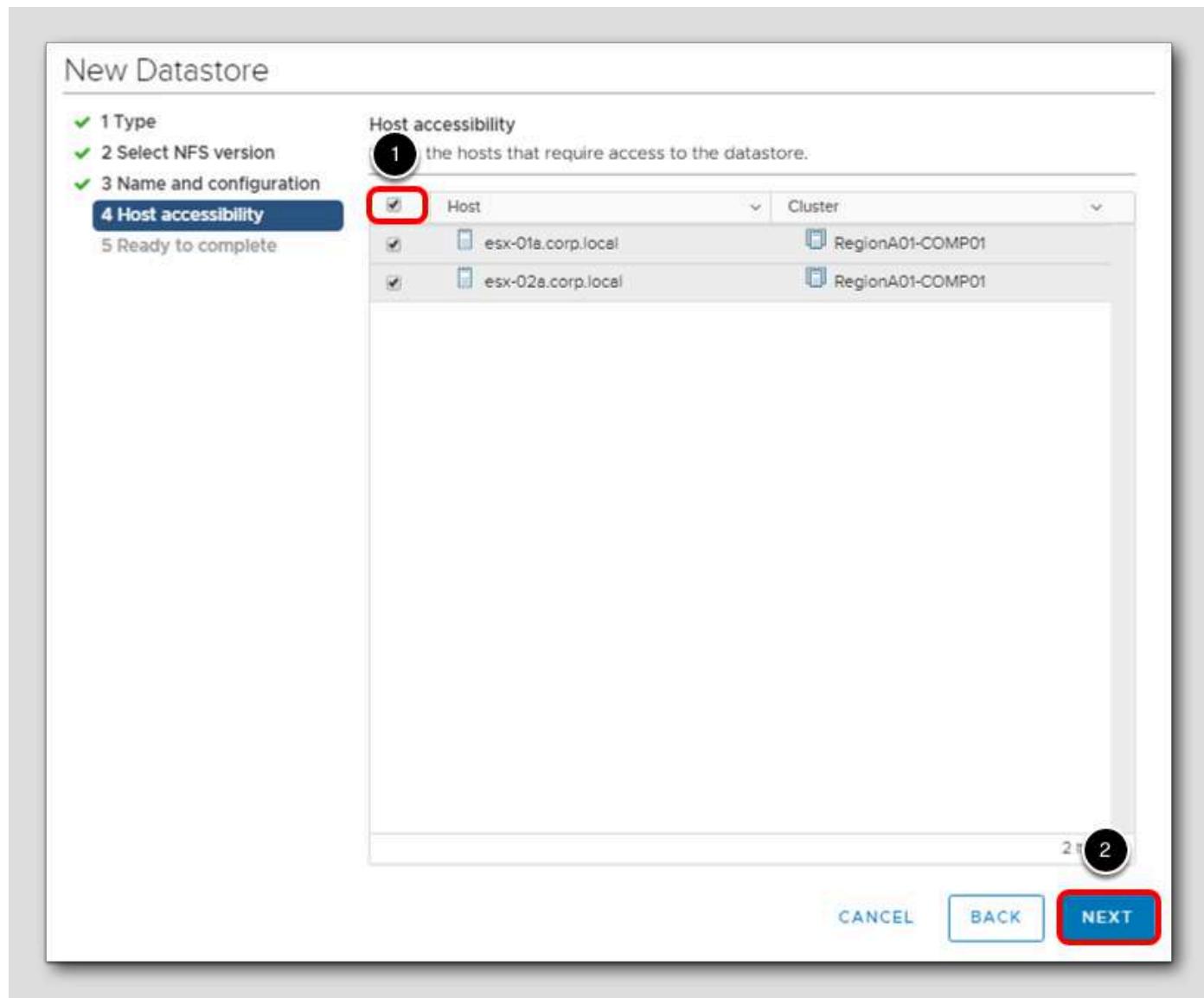
2. Click **Next**

New Datastore - Name and configuration



1. Give the new Datastore a name, ds-nfs02.
2. Enter the Folder /mnt/NFS02 in the NFS Share Details area.
3. Enter the Server 10.10.20.60 in the NFS Share Details area.
4. Click **Next**.

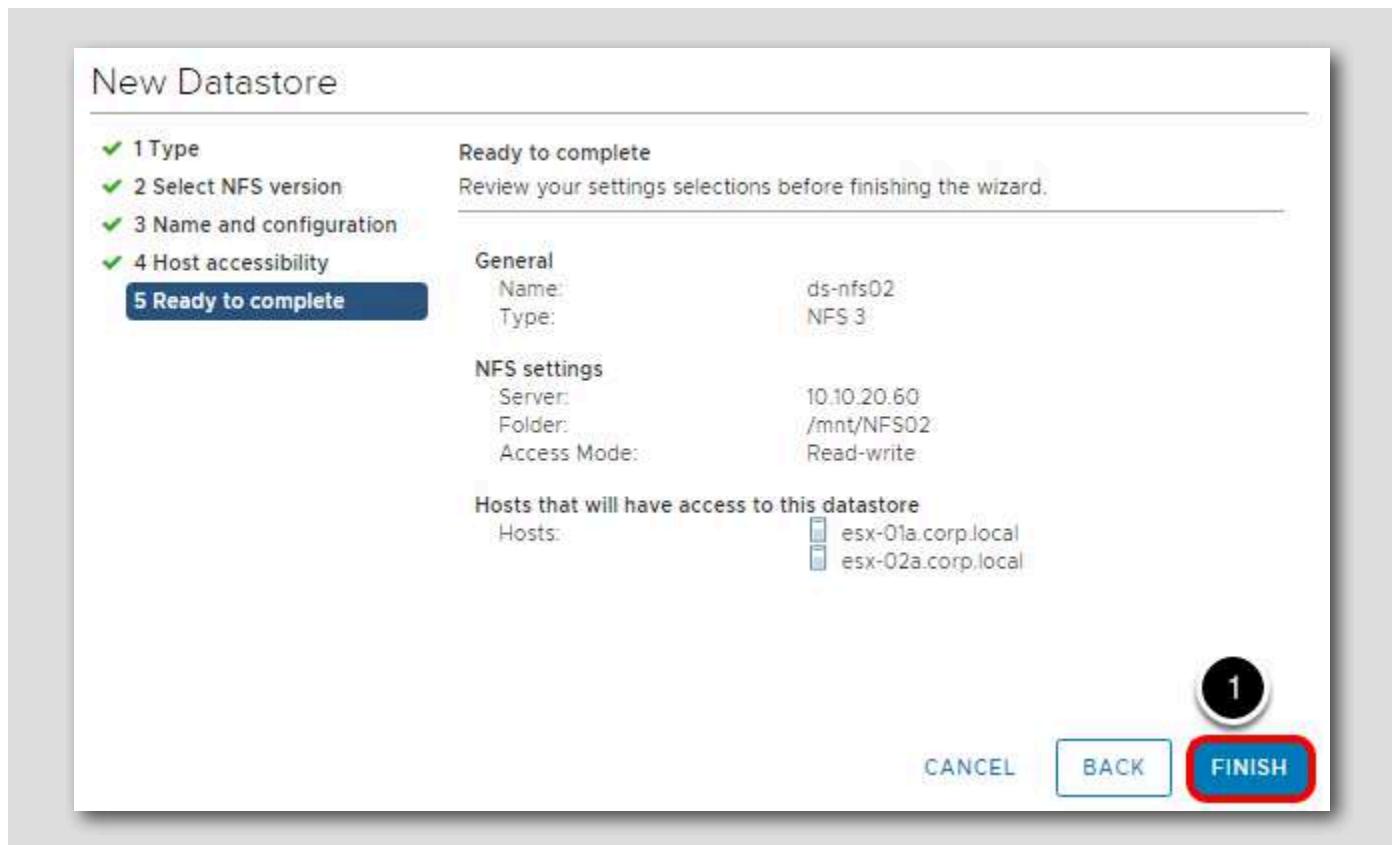
New Datastore - Host accessibility



1. Select the **check box** to include all hosts.

2. Click **Next**.

New Datastore - Ready to complete



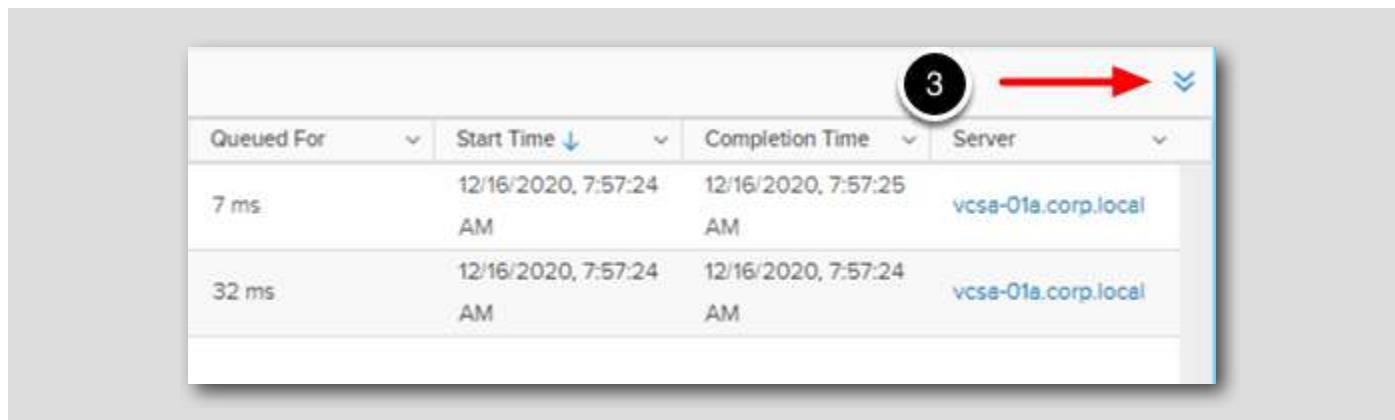
1. Review New Datastore configuration and click Finish.

Monitor task progress

The screenshot shows the vSphere Web Client interface. On the left, the navigation tree displays a folder named 'RegionA01' under 'vcsa-01a.corp.local'. A red arrow points from the number '2' to the 'ds-nfs02' item in this list. On the right, the 'Summary' tab for 'RegionA01' is selected, showing statistics: Hosts: 2, Virtual Machines: 3, Clusters: 1, Networks: 6, Datastores: 2. Below the summary, a 'Custom Attributes' section is visible. At the bottom, the 'Recent Tasks' tab is highlighted with a red box and the number '1' above it. The 'Recent Tasks' table lists two completed tasks:

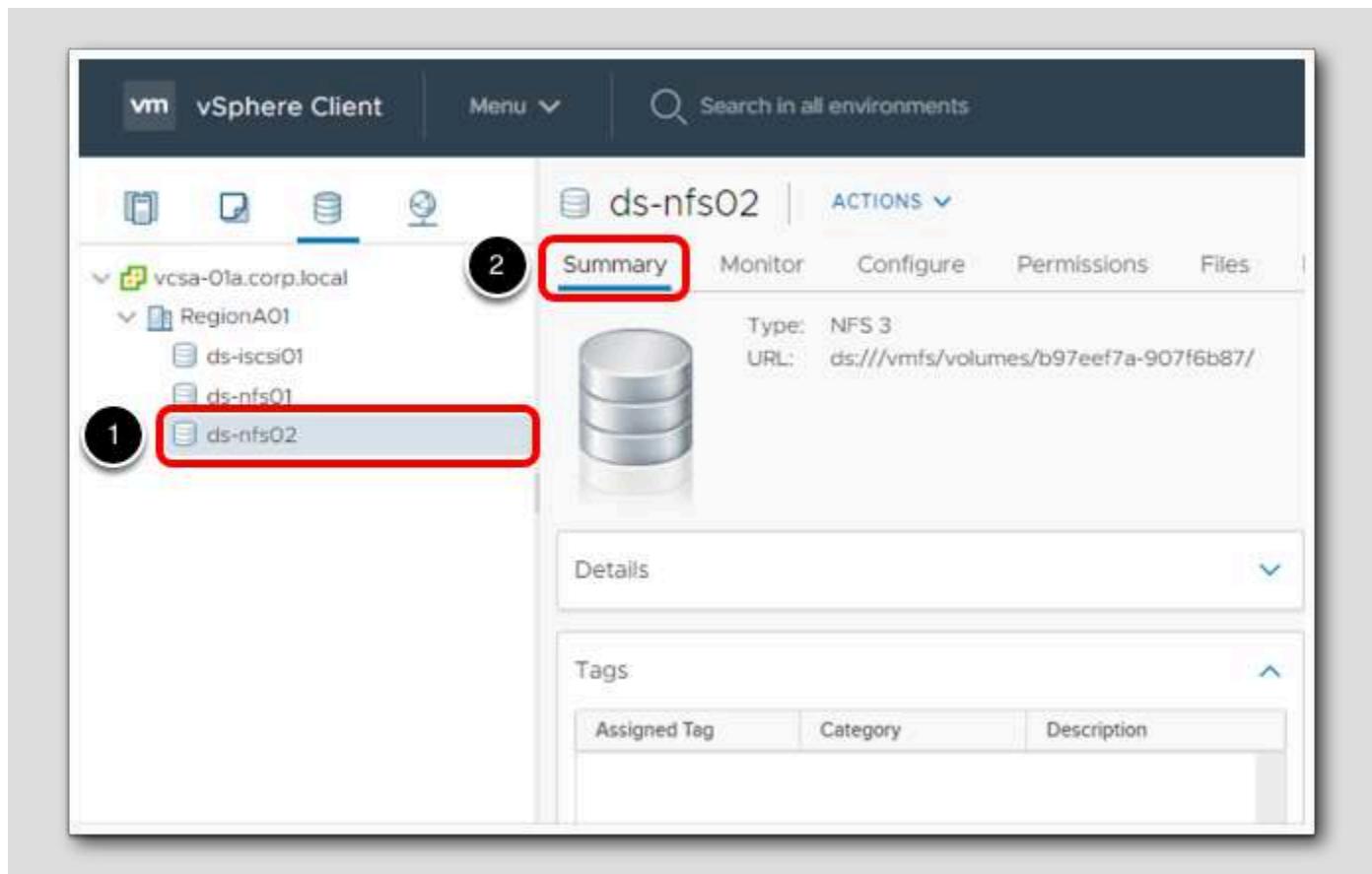
Task Name	Target	Status	Initiator
Create NAS datastore	esx-02a.corp.l...	Completed	CORP\Administrat...
Create NAS datastore	esx-01a.corp.l...	Completed	CORP\Administrat...

1. You can follow the progress in the Recent Tasks pane (by clicking on Recent Tasks)
2. When complete, you should see the new ds-nfs02 Datastore available for use



3. Minimize the Recent Tasks pane before continuing to the next step

Review new Datastore Settings



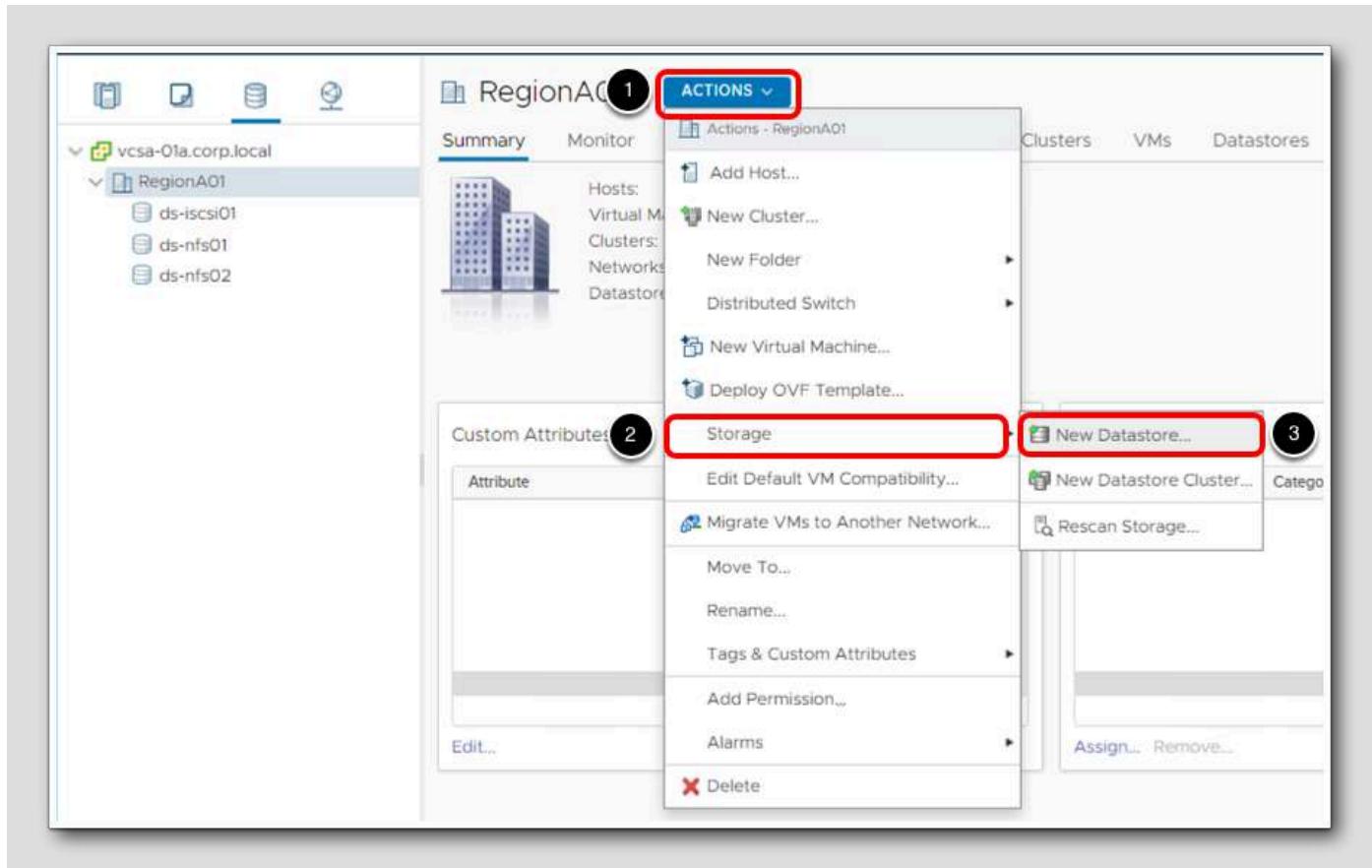
1. Select the datastore **ds-nfs02** from the inventory list
2. Select **Summary** to review capacity and configuration details

Create a vSphere iSCSI Datastore



1. Select RegionA01 Datacenter.

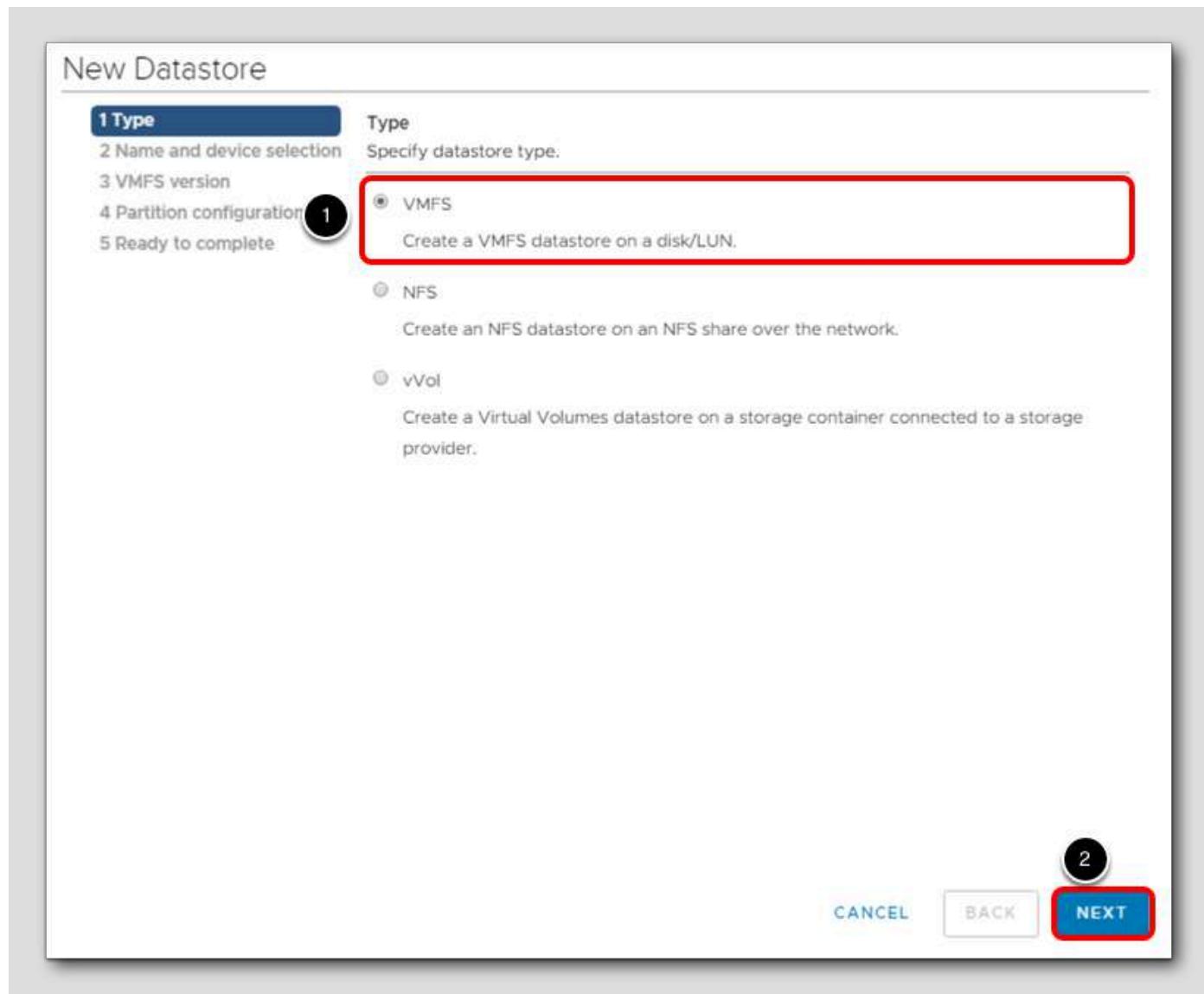
New Datastore



In this section, you will create a new vSphere iSCSI Datastore with a pre-provisioned iSCSI LUN.

1. Select Actions.
2. Select Storage.
3. Select New Datastore.

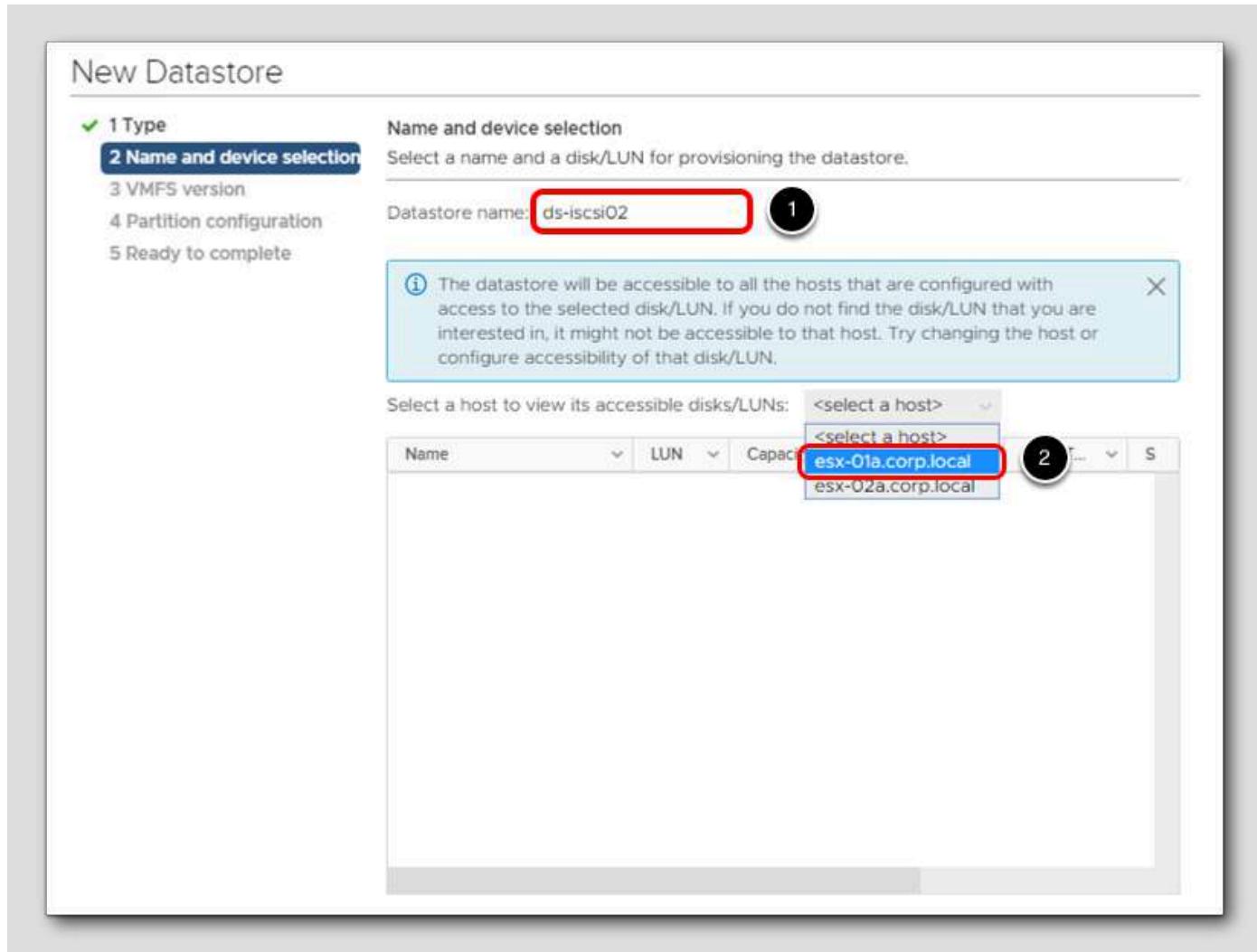
New Datastore - Type



1. Verify VMFS is selected.

2. Click **Next**.

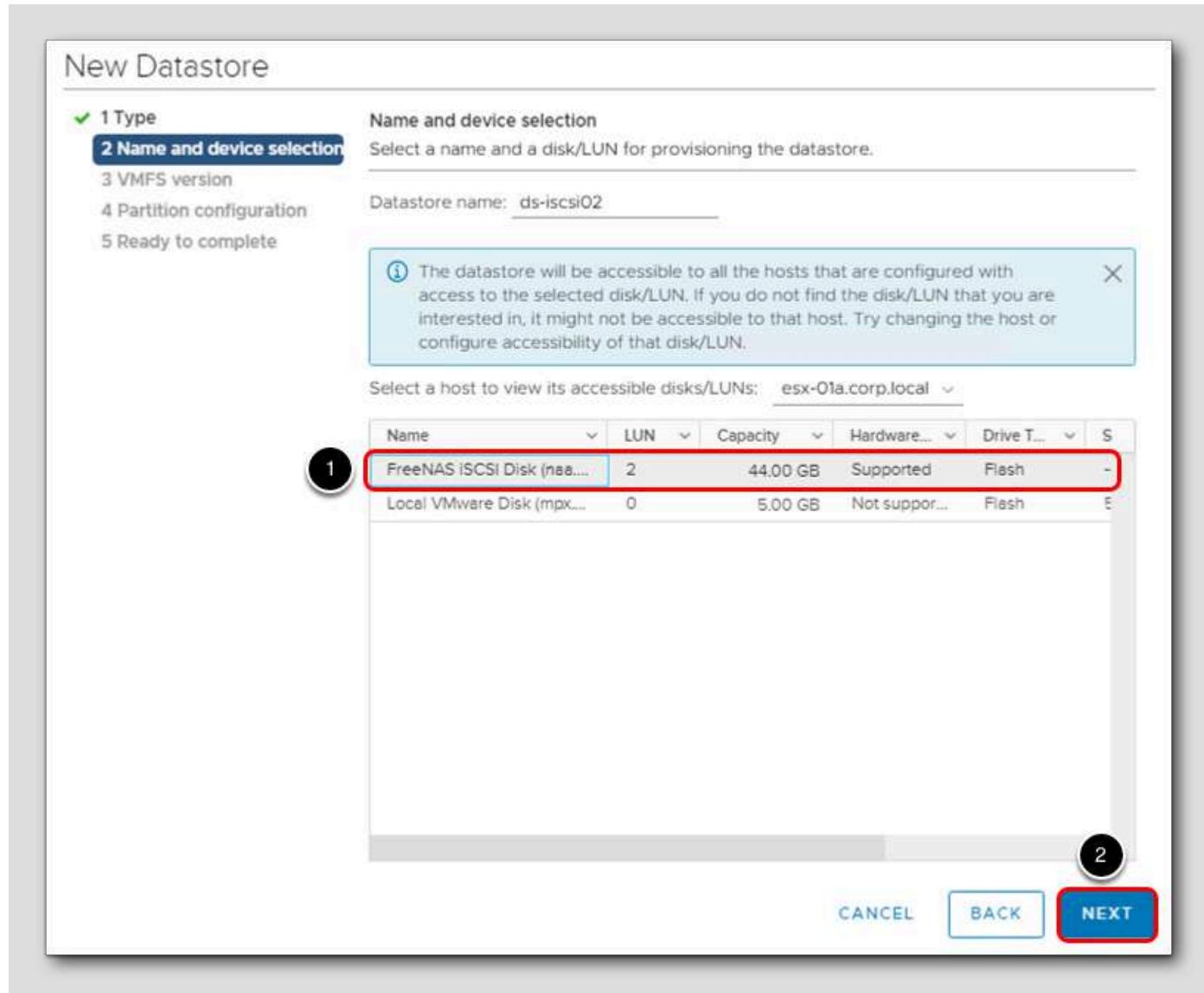
New Datastore - Name and Device configuration



1. Give the new Datastore the name ds-iscsi02.
2. Select a Host to view the accessible disks/LUNs and select esx-01a.corp.local in the drop-down box.

Note: Do not click Next just yet, proceed to the next step!

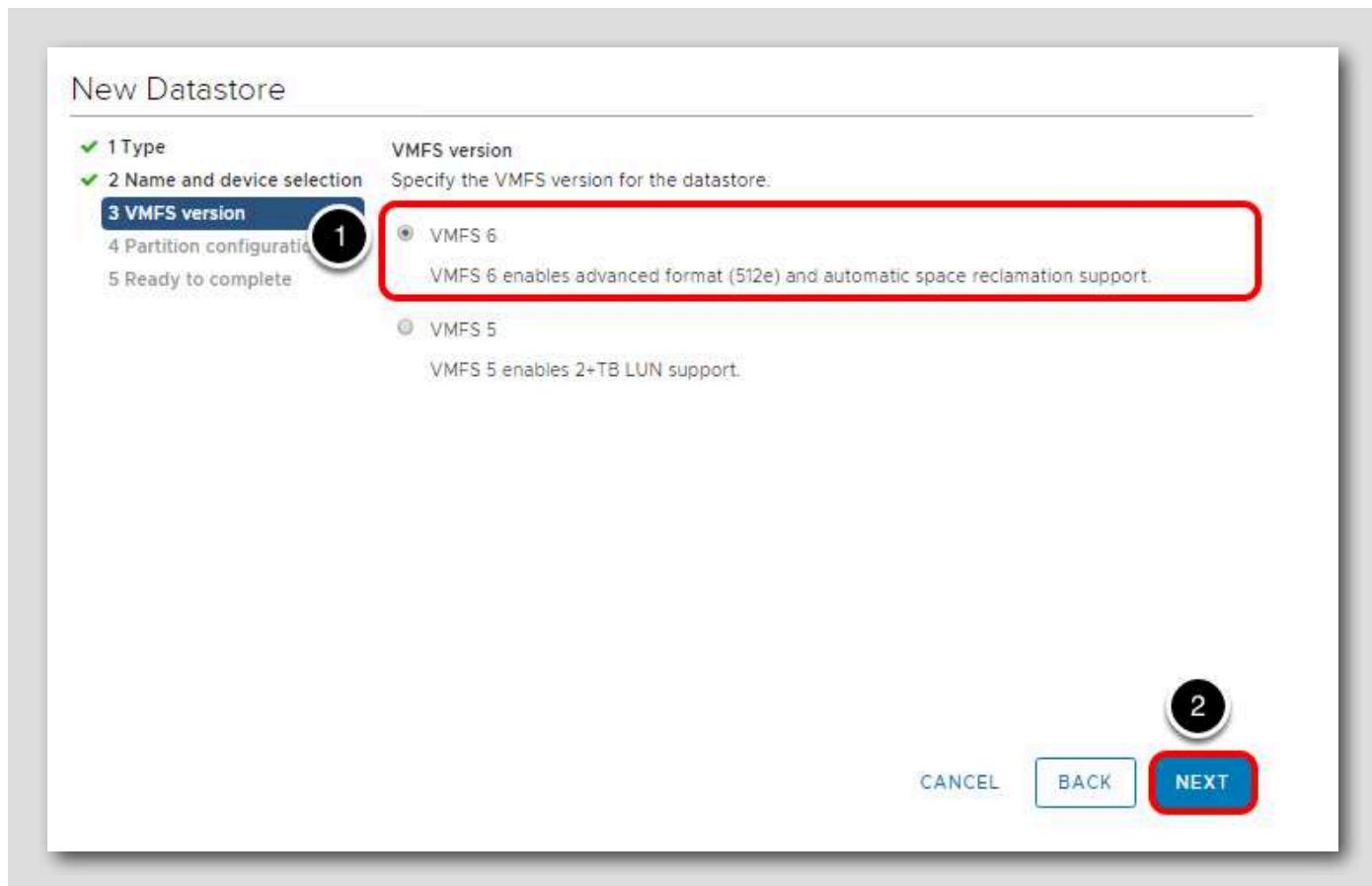
New Datastore - Name and device configuration (cont.)



From this view, we can see that there are existing datastores that can be presented to our vSphere environment.

1. Select the device with LUN ID 2. In this case, it should be the only device visible with a FreeNAS prefix.
2. Click **Next**.

New Datastore - VMFS Version



1. Leave the default of VMFS 6 selected.

2. Click **Next**.

New Datastore - Partition Configuration

New Datastore

✓ 1 Type Partition configuration
✓ 2 Name and device selection
✓ 3 VMFS version
4 Partition configuration
5 Ready to complete

Partition Configuration: Use all available partitions

Datastore Size: 44 GB

Block size: 1 MB

Space Reclamation Granularity: 1 MB

Space Reclamation Priority: Low: Deleted or unmapped blocks are reclaimed on the LUN at Low priority

Empty: 44.0 GB

1

CANCEL BACK **NEXT**

We can use all available capacity for this datastore or change the size if needed. The defaults are fine for this step.

1. Select Next.

New Datastore - Ready to complete

New Datastore

✓ 1 Type Ready to complete
✓ 2 Name and device selection
✓ 3 VMFS version
✓ 4 Partition configuration
5 Ready to complete

Review your settings selections before finishing the wizard.

General

Name:	ds-iscsi02
Type:	VMFS
Datastore size:	44.00 GB

Device and Formatting

Disk/LUN:	FreeNAS iSCSI Disk (naa.6589fc0000008bed872d58734fe67cb)
Partition Format:	GPT
VMFS Version:	VMFS 6
Block Size:	1 MB
Space Reclamation	1 MB
Granularity:	
Space Reclamation Priority	Low: Deleted or unmapped blocks are reclaimed on the LUN at low priority

1

CANCEL BACK **FINISH**

1. Review New Datastore configuration and click Finish.

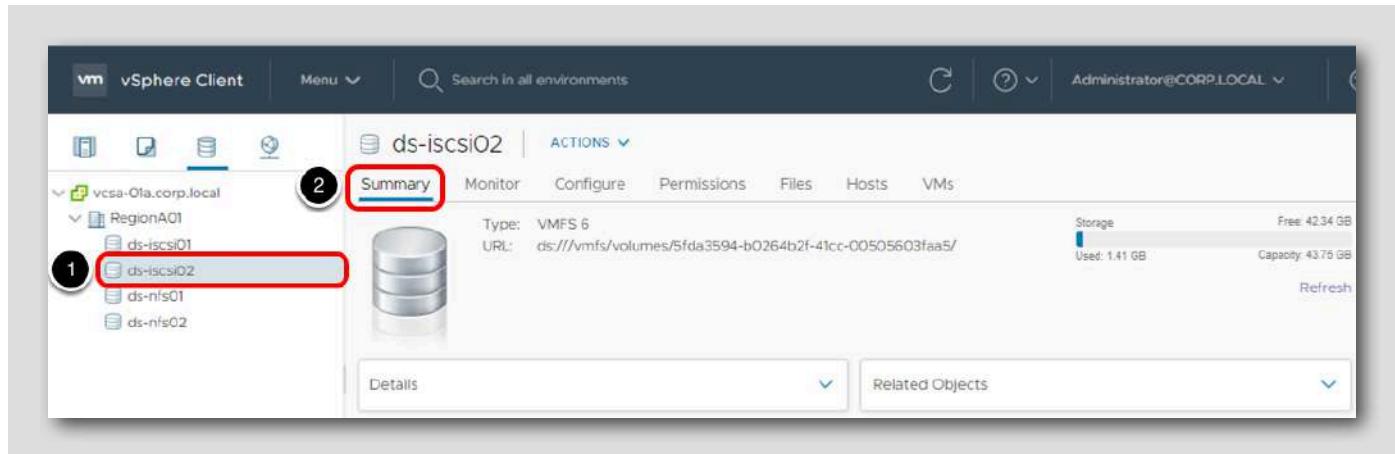
New Datastore - Monitor task progress

The screenshot shows the vSphere Client interface. On the left, a navigation tree displays a hierarchy: 'vcsa-01a.corp.local' > 'RegionA01' > 'ds-iscsi01' > 'ds-iscsi02'. A red circle labeled '2' is placed over the 'ds-iscsi02' item. On the right, the 'Summary' tab for 'ds-iscsi02' is selected, showing it is a 'VMFS 6' type datastore with URL 'ds://vmfs/volumes/5fda3594-b026'. A red circle labeled '1' is placed over the 'Recent Tasks' section. This section contains a table with three rows:

Task Name	Target	Status	Initiator
Process VMFS datastore updates	esx-02a.corp.l...	Completed	System
Create VMFS datastore	esx-01a.corp.l...	Completed	CORP\Administrat...
Compute disk partition information	esx-01a.corp.l...	Completed	CORP\Administrat...

1. Note the progress in the Recent Tasks pane
2. When complete, you should see the ds-iscsi02 Datastore available for use

New Datastore - Review Settings



1. Select the datastore **ds-iscsi02** from the inventory list
2. Select **Summary** to review capacity and configuration details

Add a new ESXi host

In this section, we will add a new ESXi host, `esx-03a.corp.local`, to the environment in RegionA01 and ensure that it has the appropriate storage configured so that it can become a productive member of the cluster.

Hosts and Clusters View

The screenshot shows the vSphere Hosts and Clusters View. The left sidebar has icons for Hosts and Clusters (highlighted with a red box and number 1), Datacenters, and Storage. A red box highlights the 'vcsa-01a.corp.local' datacenter under 'Datacenters'. A black circle with the number 2 highlights the 'RegionA01' cluster under 'vcsa-01a.corp.local'. The main pane displays the 'RegionA01' cluster summary, which includes:

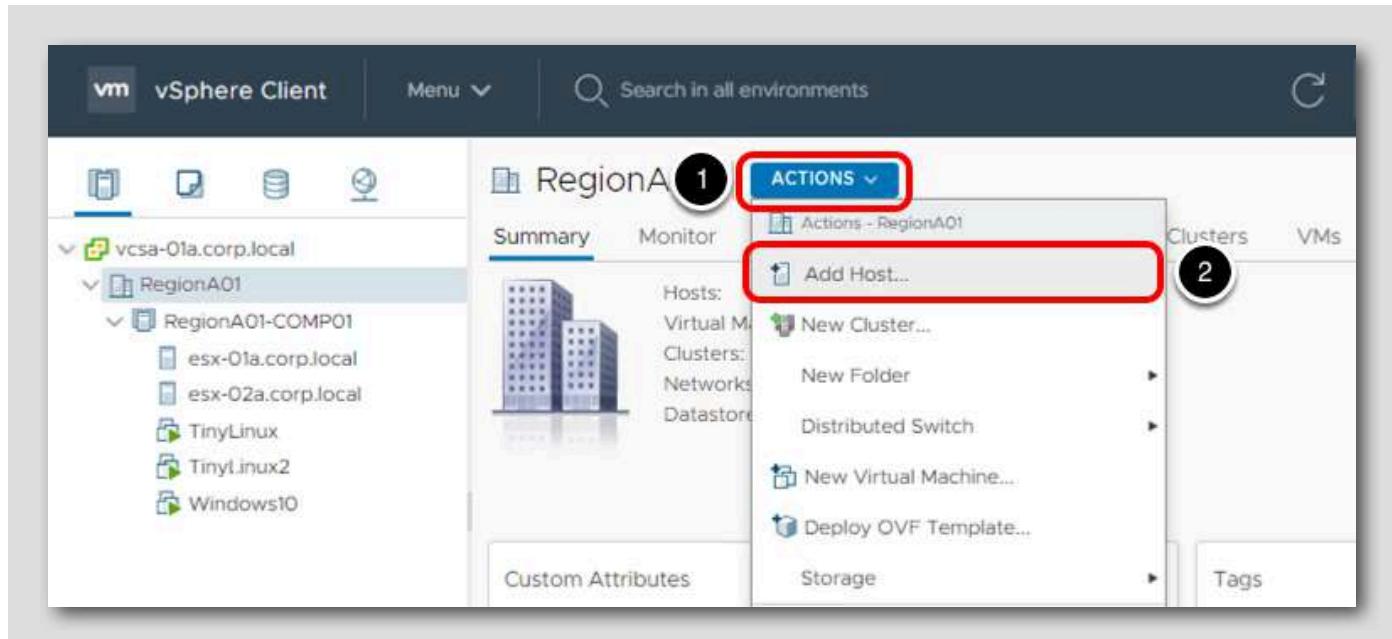
	Hosts:	2
Virtual Machines:	3	
Clusters:	1	
Networks:	6	
Datastores:	4	

A 'Custom Attributes' panel is open at the bottom right.

1. Click on the Hosts and Clusters icon to return to that Inventory view.
2. Select RegionA01 Datacenter.

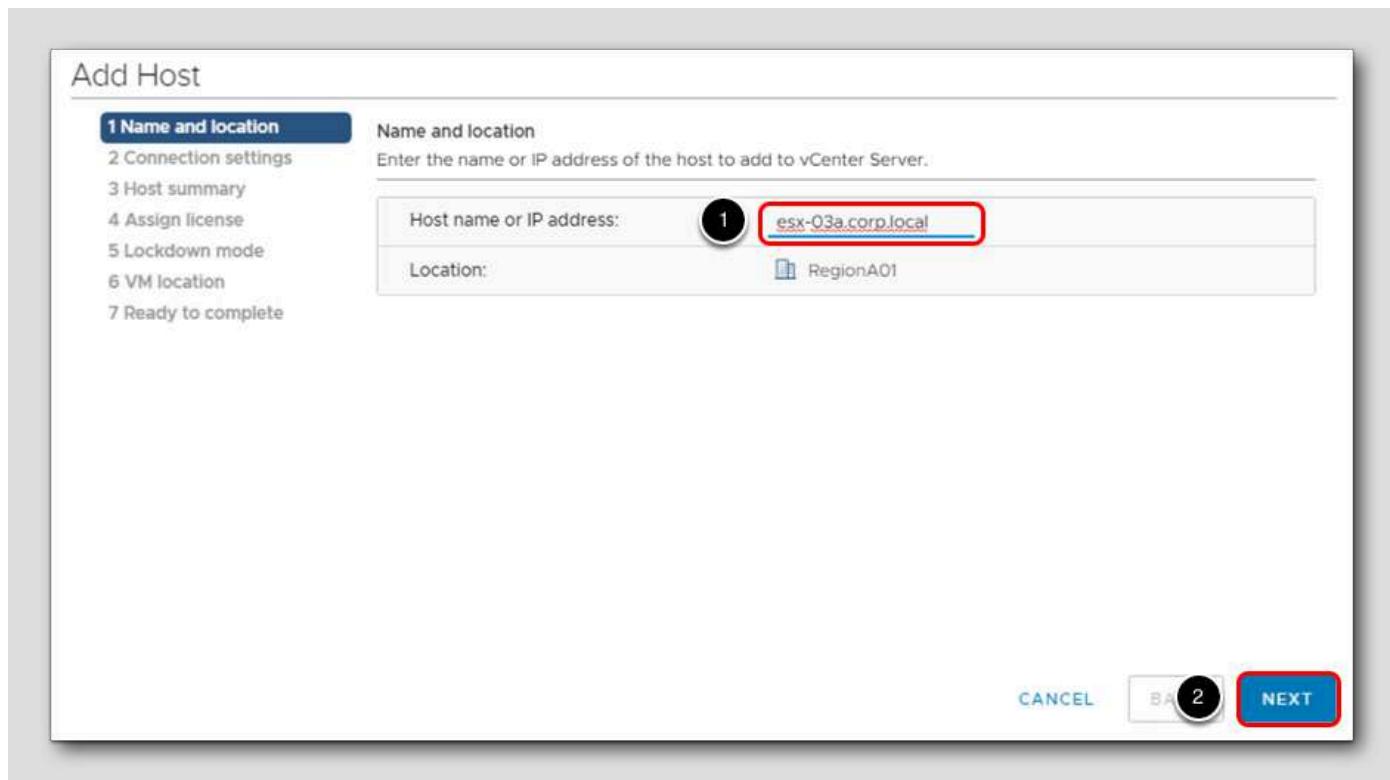
It is a best practice to bring hosts into a datacenter first before adding them to a cluster. If a host is added to a cluster first, by not having access to the cluster's storage volumes, it could impact High Availability (see Module 1 for more details on High Availability).

Begin the Add Host workflow



1. Go to the Actions menu.
2. Select Add Hosts...

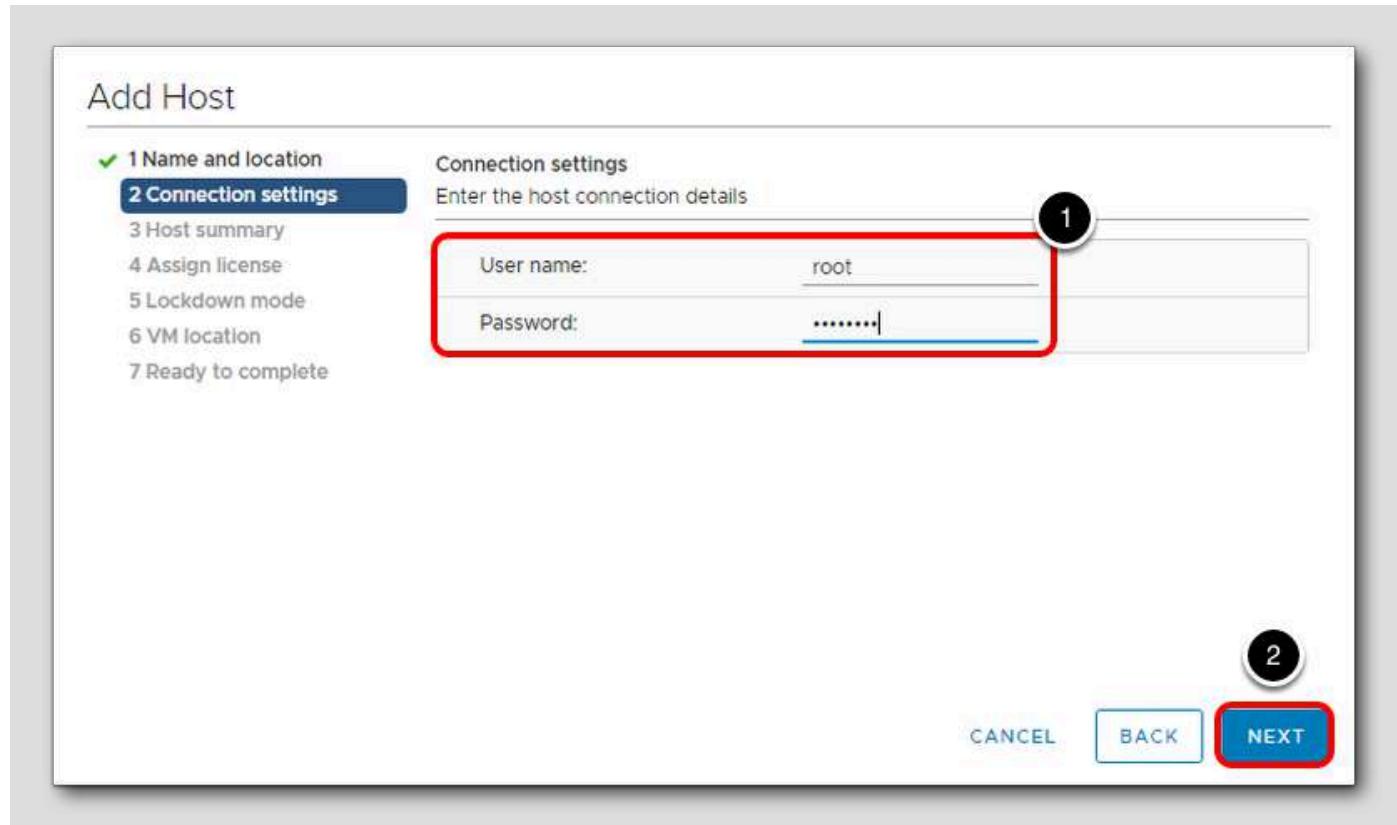
Enter the hostname



1. In the Host name or IP address, enter: esx-03a.corp.local

2. Click **Next**.

Connection Settings



1. Enter the following login details:

- User name: root
- Password: VMware1!

2. Click **Next**.

Host Summary

Add Host

Host summary
Review the summary for the host

Name	esx-03a.corp.local
Vendor	VMware, Inc.
Model	VMware Virtual Platform
Version	VMware ESXi 7.0.0 build-15843807
Virtual Machines	(Empty)

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

1

CANCEL BACK **NEXT**

This screen shows the details of the host.

1. Click **Next**.

Assign License

Add Host

4 Assign license

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

License	License Key	Product	Usage	Capacity
<input checked="" type="radio"/> FOR VMWARE HA...	XXXX-XXX	vSphere 7 Enterprise Pl...	• 3 CPUs ...	16 CPUs (...)
<input type="radio"/> Evaluation License	--	--	--	--

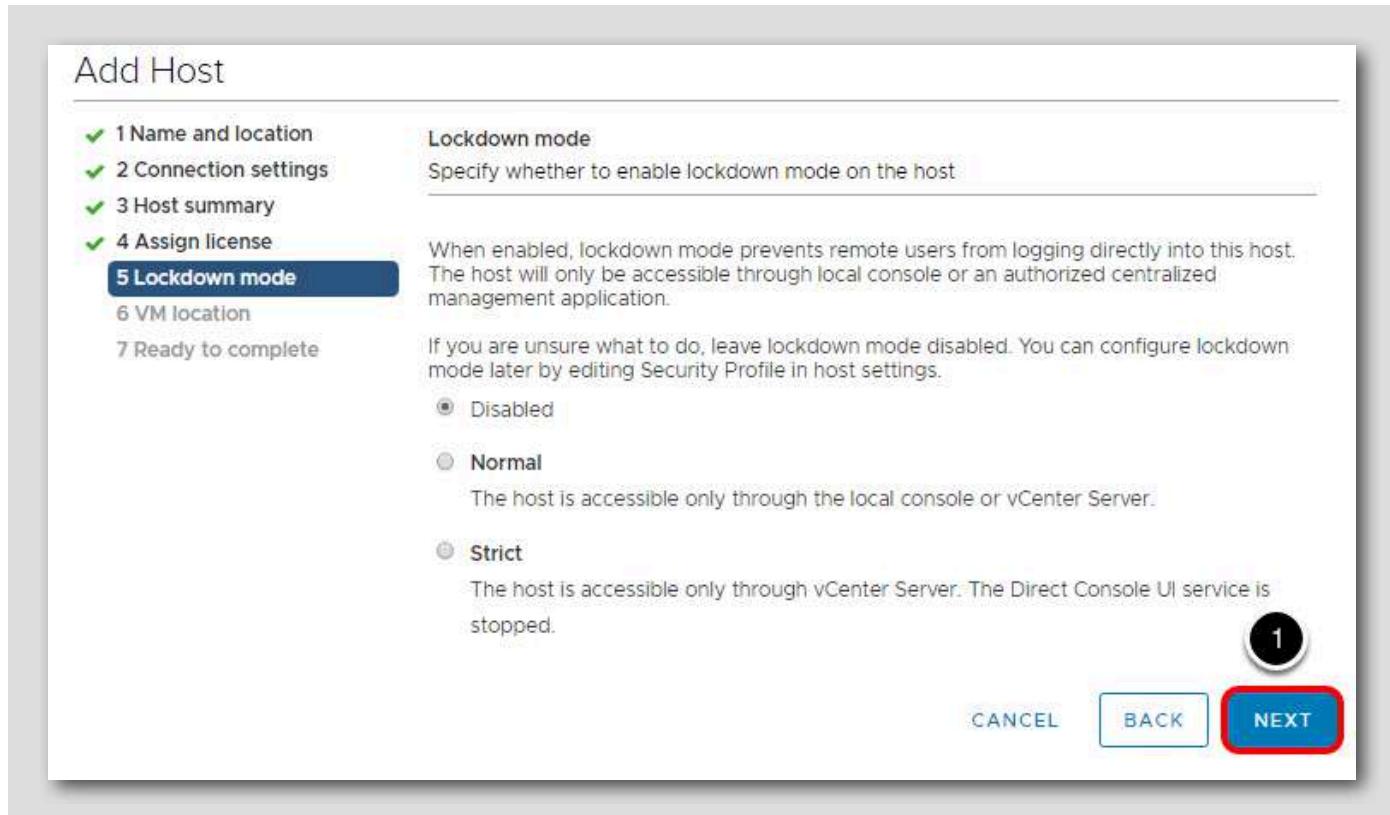
Assignment Validation for FOR VMWARE HANDS-ON LABS USE ONLY

The license assignment is valid.

CANCEL BACK NEXT

1. Leave the default license choice and click **Next**.

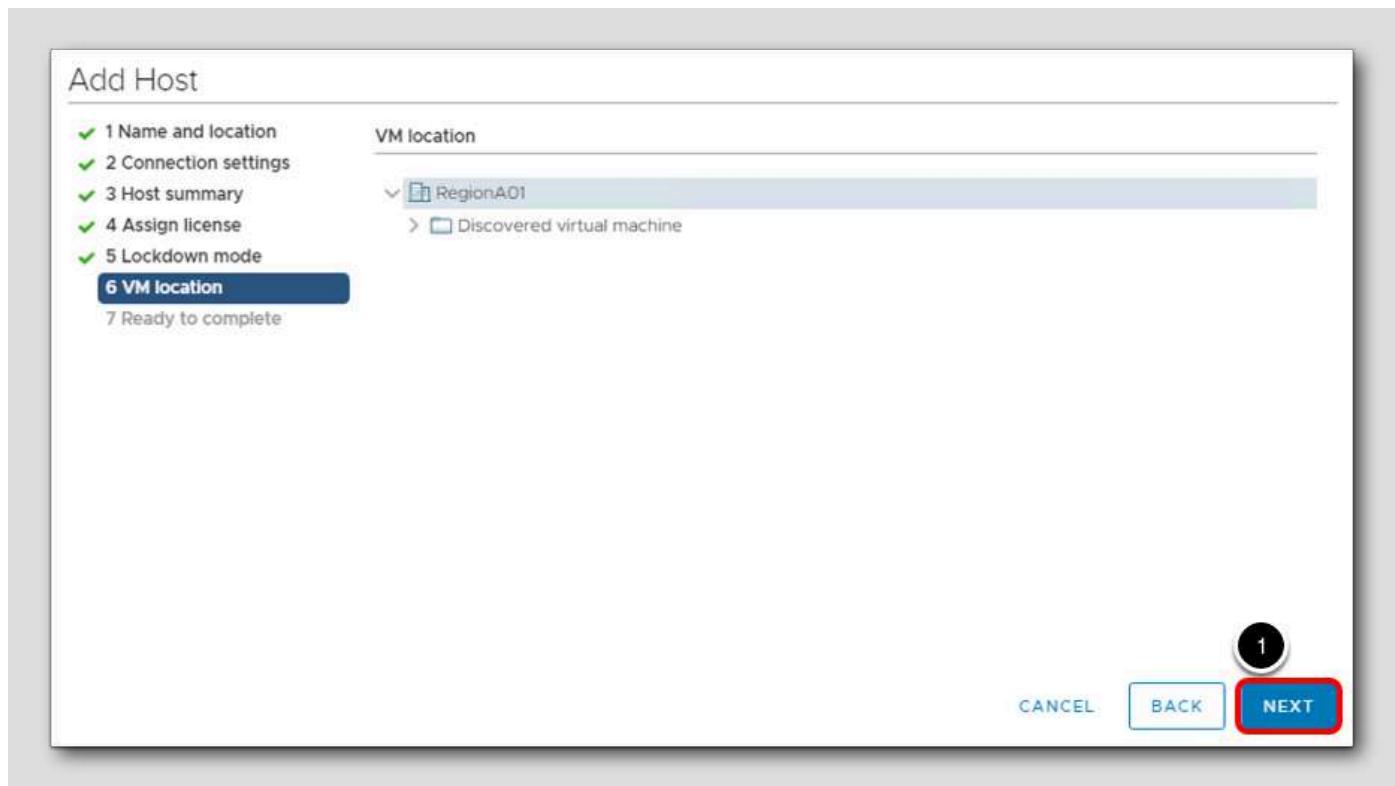
Lockdown Mode



When a host is being added to a Datacenter, it can be placed in what is called Lockdown mode. This can prevent unauthorized users from gaining access to the ESXi host either through local console access or remotely by way of SSH. If you are interested in Lockdown Mode, the details are covered in Module 1.

1. Leave the default setting and click Next.

VM Location



The virtual machines currently on the ESXi host being imported can be placed in either the Datacenter itself or in the default Discovered virtual machines folder.

1. Since there are no virtual machines on esx-03a.corp.local, leave the default setting and click **Next**.

Ready to Complete

Add Host

Ready to complete
Click Finish to add the host

Name	esx-03a.corp.local
Location	RegionA01
Version	VMware ESXi 7.0.0 build-15843807
License	FOR VMWARE HANDS-ON LABS USE ONLY
Networks	VM Network
Datastores	
Lockdown mode	Disabled
VM location	RegionA01

7 Ready to complete

CANCEL BACK FINISH

1. Review the settings and click **Finish** to add the esx-03a.corp.local to the datacenter.

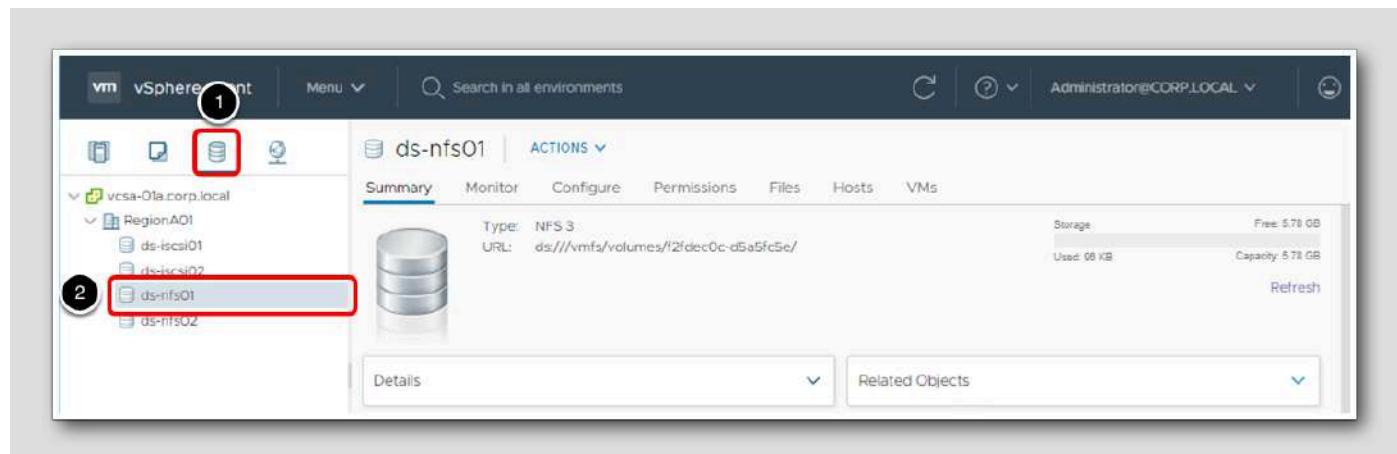
Host Added to Datacenter

The screenshot shows the vSphere Web Client interface. On the left, the navigation tree is visible with the path: vcsa-01a.corp.local > RegionA01 > RegionA01-COMP01. Under RegionA01-COMP01, several hosts are listed: esx-01a.corp.local, esx-02a.corp.local, TinyLinux, TinyLinux2, and esx-03a.corp.local. The entry for esx-03a.corp.local is highlighted with a red box. The main content area on the right is titled 'RegionA01' and contains the 'Summary' tab. The summary statistics are: Hosts: 2, Virtual Machines: 3, Clusters: 1, Networks: 6, Datastores: 4. Below the summary, there is a section for 'Custom Attributes' with a table and an 'Actions' dropdown menu.

Here you can see esx-03a.corp.local has been added to the datacenter and is in Maintenance Mode.

Maintenance Mode is used for hosts that service. A host could enter Maintenance Mode so that it can be brought offline in order for additional memory to be added to the physical host. In our case, it is in Maintenance Mode once it has been added to the datacenter so that we can verify its settings prior to bringing it online and potentially conflicting with other hosts in the environment.

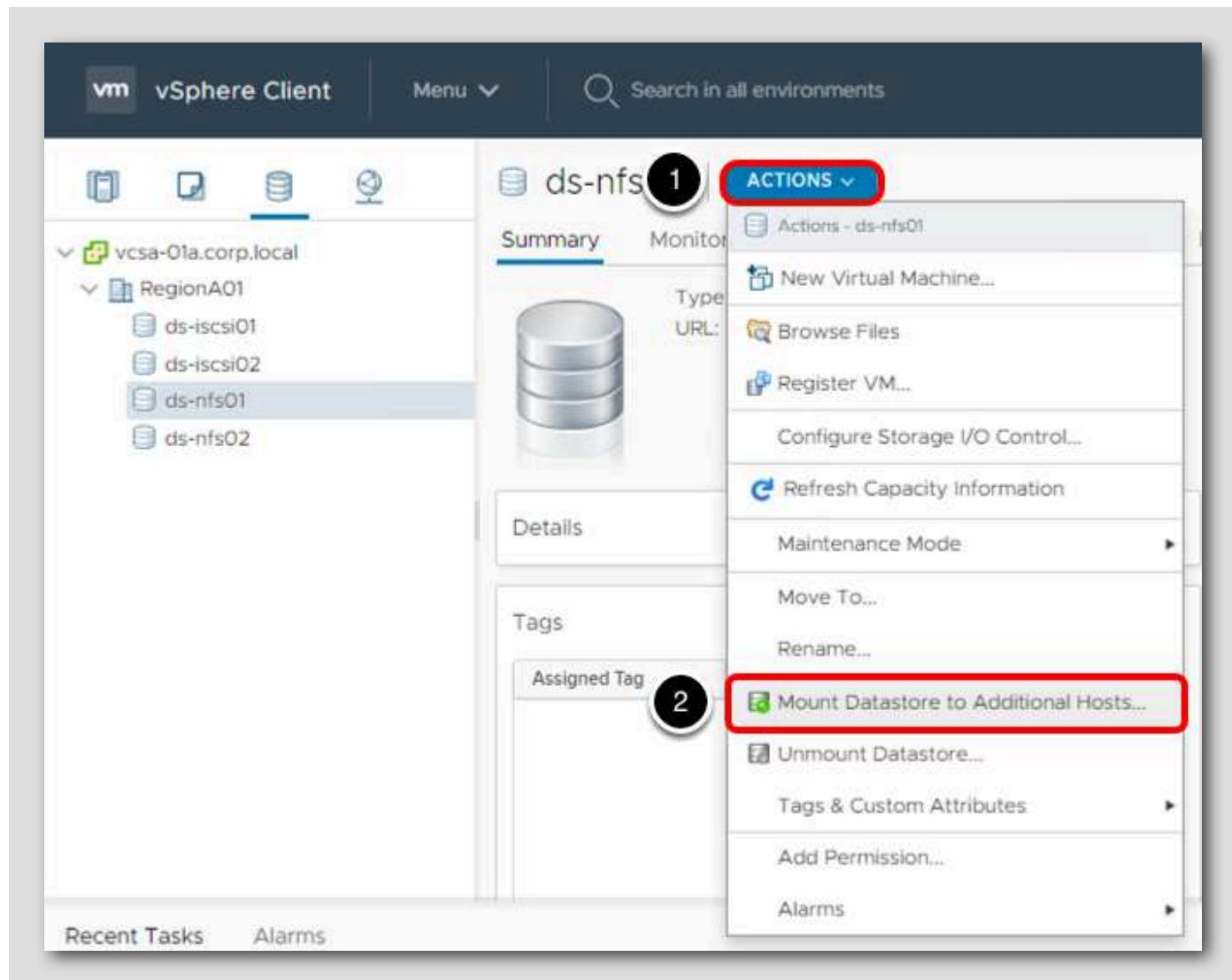
Datastore view



Prior to adding the new host to the cluster, an NFS datastore will be added to the host.

1. Click on the Datastore icon to switch to the Datastores view.
2. Select the **ds-nfs01** datastore in the Inventory.

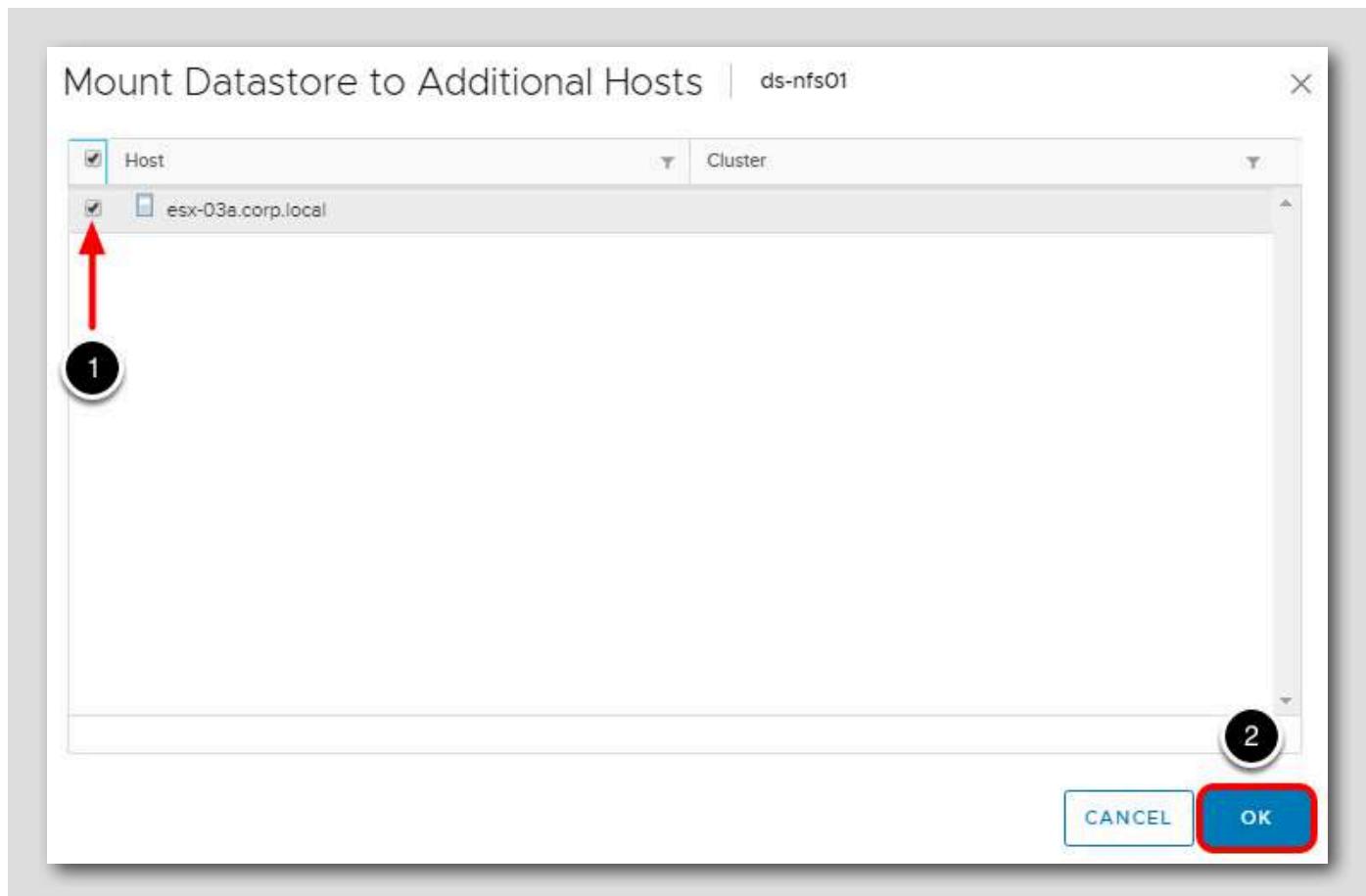
Mount NFS Datastore to New Host Wizard



In this case, there are two NFS datastores used by RegionA01 cluster. Adding an existing NFS datastore to a new host is a simple process.

1. Click on the Actions menu.
2. Select Mount Datastore to Additional Hosts...

Mount NFS Datastore - Select Host



1. Click the checkbox next to esx-03a.corp.local
2. Click OK.

Mount NFS Datastore - Monitor Task

The screenshot shows the vSphere Client interface. At the top, there's a navigation bar with 'vSphere Client', 'Menu', a search bar, and user information ('Administrator@CORP.LOCAL'). Below the navigation bar, the left sidebar shows a tree view of datastores: 'vcsa-01a.corp.local' (selected), 'RegionA01' (expanded) containing 'ds-iscsi01', 'ds-iscsi02', 'ds-nfs01' (selected), and 'ds-nfs02'. The main content area has tabs: 'Summary', 'Monitor', 'Configure', 'Permissions', 'Files', 'Hosts' (which is highlighted with a red box and has a circled '2' above it), and 'VMs'. Under 'Hosts', a table lists hosts: 'esx-01a.corp.local' (Connected, Normal, RegionA01-Cluster, 2% CPU, 22% Memory), 'esx-02a.corp.local' (Connected, Normal, RegionA01-Cluster, 7% CPU, 57% Memory), and 'esx-03a.corp.local' (Maintenance Mode, Normal, RegionA01-Cluster, 1% CPU, 19% Memory). At the bottom, there's a 'Recent Tasks' table with one entry: 'Create NAS datastore' (Completed, Target: esx-03a.corp.local, Initiator: CORP\Administrat..., Start Time: 12/16/2020, 9:58:36 AM, Completion Time: 12/16/2020, 9:58:36 AM, Server: vcsa-01a.corp.local). A circled '1' is above the 'Recent Tasks' tab.

1. The mount task can be monitored in Recent Tasks.
2. Once the mount completes, it can be verified by clicking on the Hosts tab.

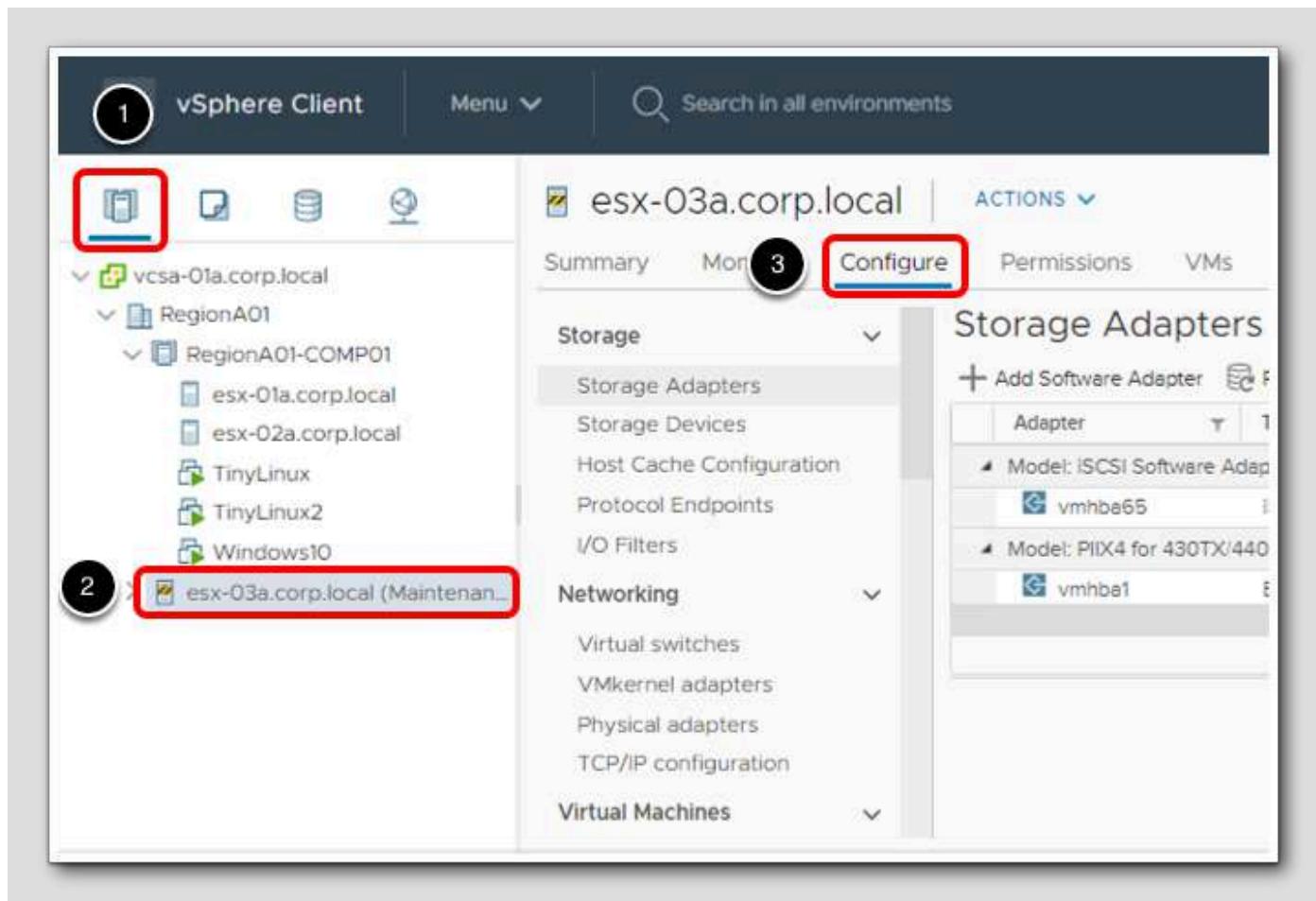
This will show all hosts in the inventory that have mounted this datastore.

For additional practice, perform the same steps to mount the other NFS datastore, ds-nfs02 to the esx-03a.corp.local host.

Add iSCSI Target to an ESXi host

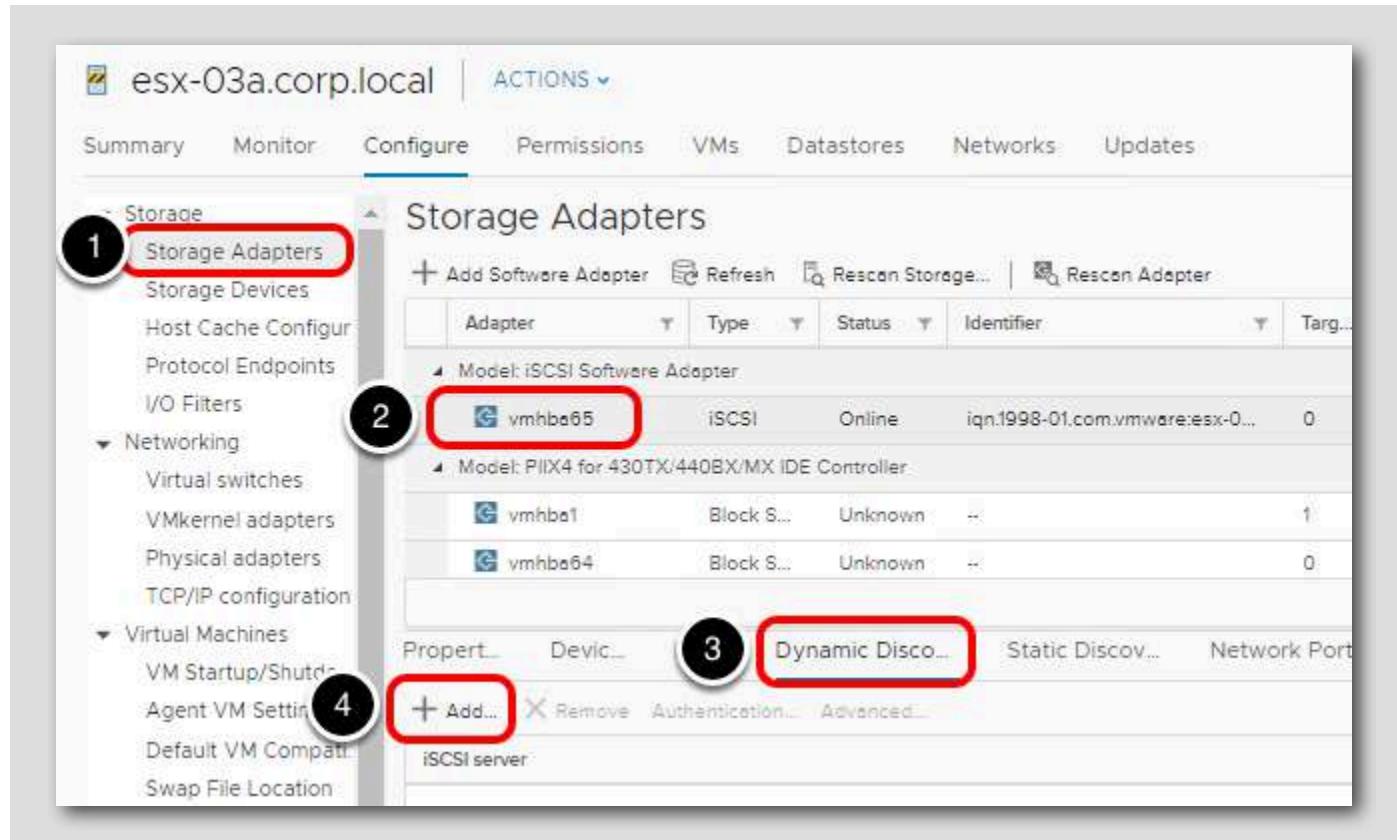
iSCSI devices are presented via an iSCSI Target. Think of this as the host for the iSCSI devices. The ESXi host needs to know where to look for the devices, so this section will go through the process of pointing the ESXi host at the iSCSI target and discovering which LUNs are available.

Select Hosts and Clusters



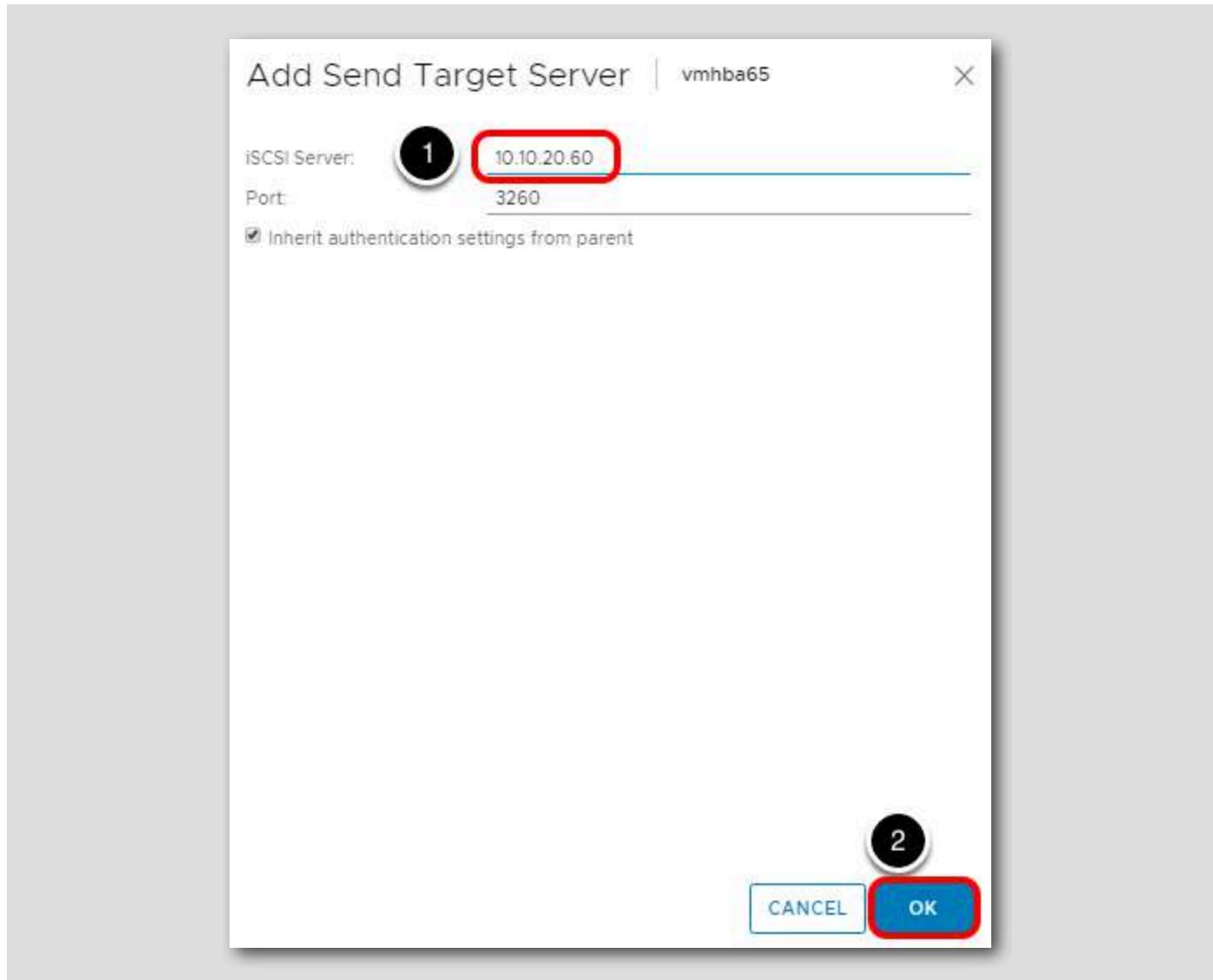
1. Select the Hosts and Clusters icon.
2. Click on esx-03a.corp.local (Maintenance Mode).
3. Click the Configure tab.

Perform Dynamic Discovery



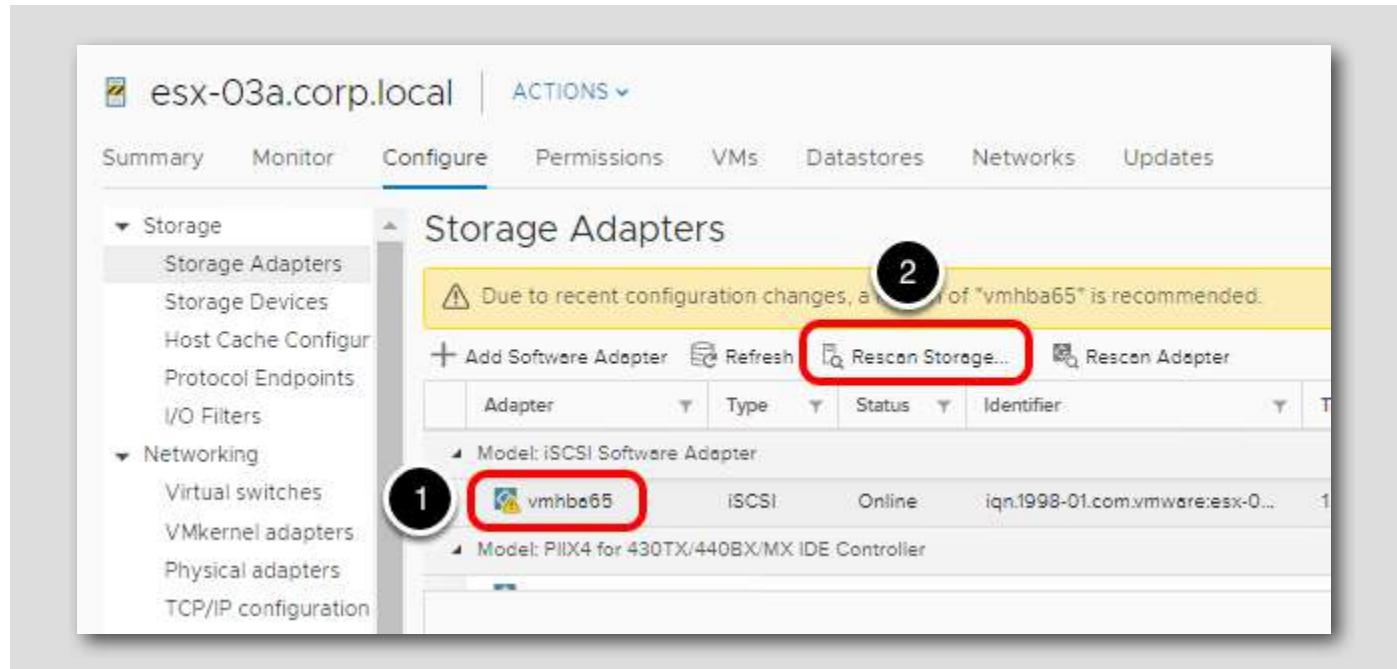
1. Select "Storage Adapters"
2. Select the "vmhba65" adapter in the iSCSI Software Adapter section.
3. Click on "Dynamic Discovery" - notice that the list of iSCSI Servers is currently empty.
4. Click "Add"

Add Send Target Server



1. Enter the iSCSI Server Address: 10.10.20.60
2. Select OK.

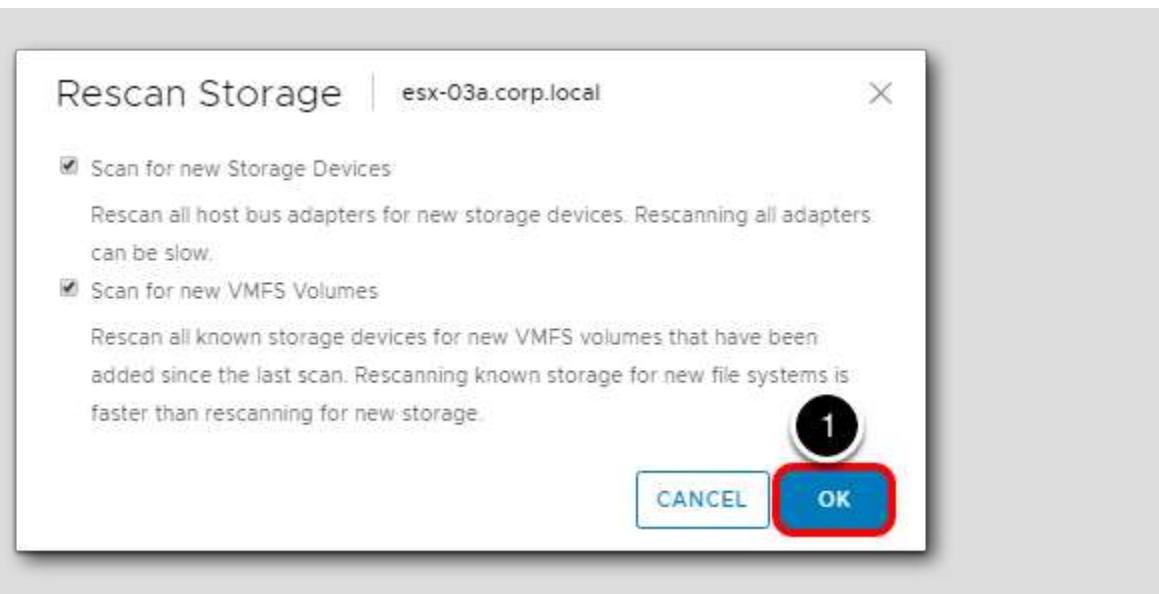
Rescan the iSCSI storage adapter



Once the new Target has been added, a message will appear in yellow to remind you of the need to tell the adapter to reach out and query the iSCSI Target.

1. Click on the vmhba65 iSCSI adapter to select it.
2. Click the Rescan Storage... icon to rescan.

Rescan Storage



1. Leave the default options selected and click OK.

Verify iSCSI Devices are Visible

The screenshot shows the vSphere Web Client interface for a host named esx-03a.corp.local. The 'Configure' tab is selected. In the left sidebar under 'Storage', the 'Storage Devices' item is highlighted with a red box and a circled '1'. The main content area displays a table of storage devices. Two entries are highlighted with a red box and a circled '2': 'FreeNAS iSCSI Disk (naa.6589fc0000008be...)' and 'FreeNAS iSCSI Disk (naa.6589fc000000e3f0f...)'. Both are listed as disk type with 44.00 GB capacity and are associated with Datastores 'ds-is...' and 'A'. Other entries include 'Local VMware Disk (mpx.vmhba0:C0:T0:L0)' and 'Local NECVMWar CD-ROM (mpx.vmhba1:C0:T0:L0)'. A message at the bottom right says 'No items selected'.

Name	Capacity	Type	Datastore	Host
Local VMware Disk (mpx.vmhba0:C0:T0:L0)	5.00 GB	disk	Not Cons...	A
FreeNAS iSCSI Disk (naa.6589fc0000008be...)	44.00 GB	disk	ds-is...	A
FreeNAS iSCSI Disk (naa.6589fc000000e3f0f...)	44.00 GB	disk	ds-is...	A
Local NECVMWar CD-ROM (mpx.vmhba1:C0:T0:L0)	0	cdrom	Not Cons...	A

1. Once the rescan is complete, Click on Storage Devices.
2. You should now see two iSCSI disks connected, both with 44GB of capacity.

Verify iSCSI Datastore Availability

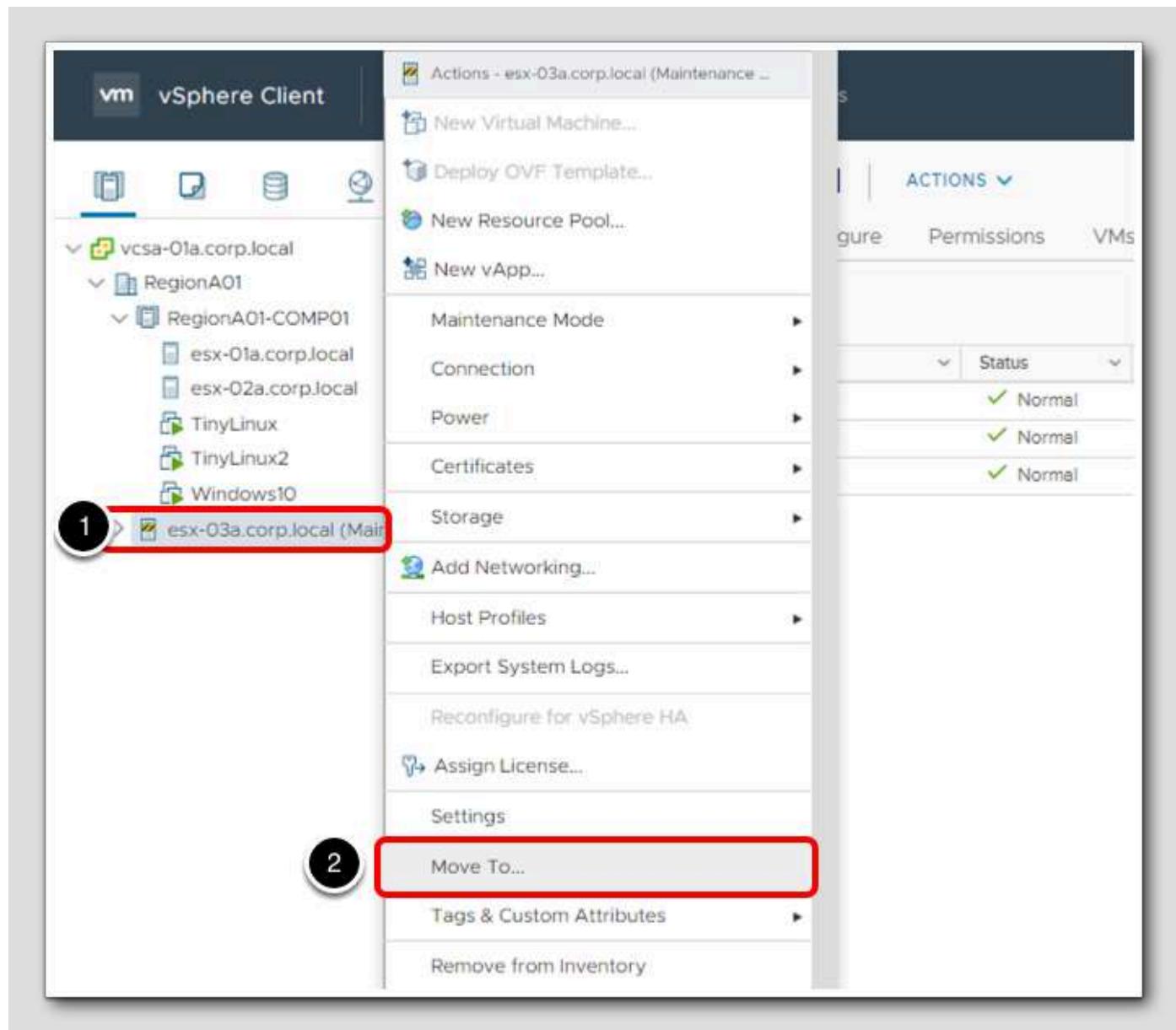
The screenshot shows the vSphere Web Client interface for the host `esx-03a.corp.local`. The top navigation bar includes `ACTIONS`, `Summary`, `Monitor`, `Configure`, `Permissions`, `VMs`, `Resource Pools`, `Datastores` (which is highlighted with a red box and has a circled '1' above it), `Networks`, and `Updates`. Below the navigation is a search bar labeled `Filter`. A table lists three datastores: `ds-iscsi01` (VMFS 6, 43.75 GB free), `ds-iscsi02` (VMFS 6, 43.75 GB free), and `ds-nfs01` (NFS 3, 5.78 GB free). The rows for `ds-iscsi01` and `ds-iscsi02` are also highlighted with red boxes.

Name	Status	Type	Capacity	Free
ds-iscsi01	Normal	VMFS 6	43.75 GB	18.83 GB
ds-iscsi02	Normal	VMFS 6	43.75 GB	42.34 GB
ds-nfs01	Normal	NFS 3	5.78 GB	5.78 GB

1. Click on the Datastores tab.

Notice that the two iSCSI datastores are now visible to the `esx-03a.corp.local` host.

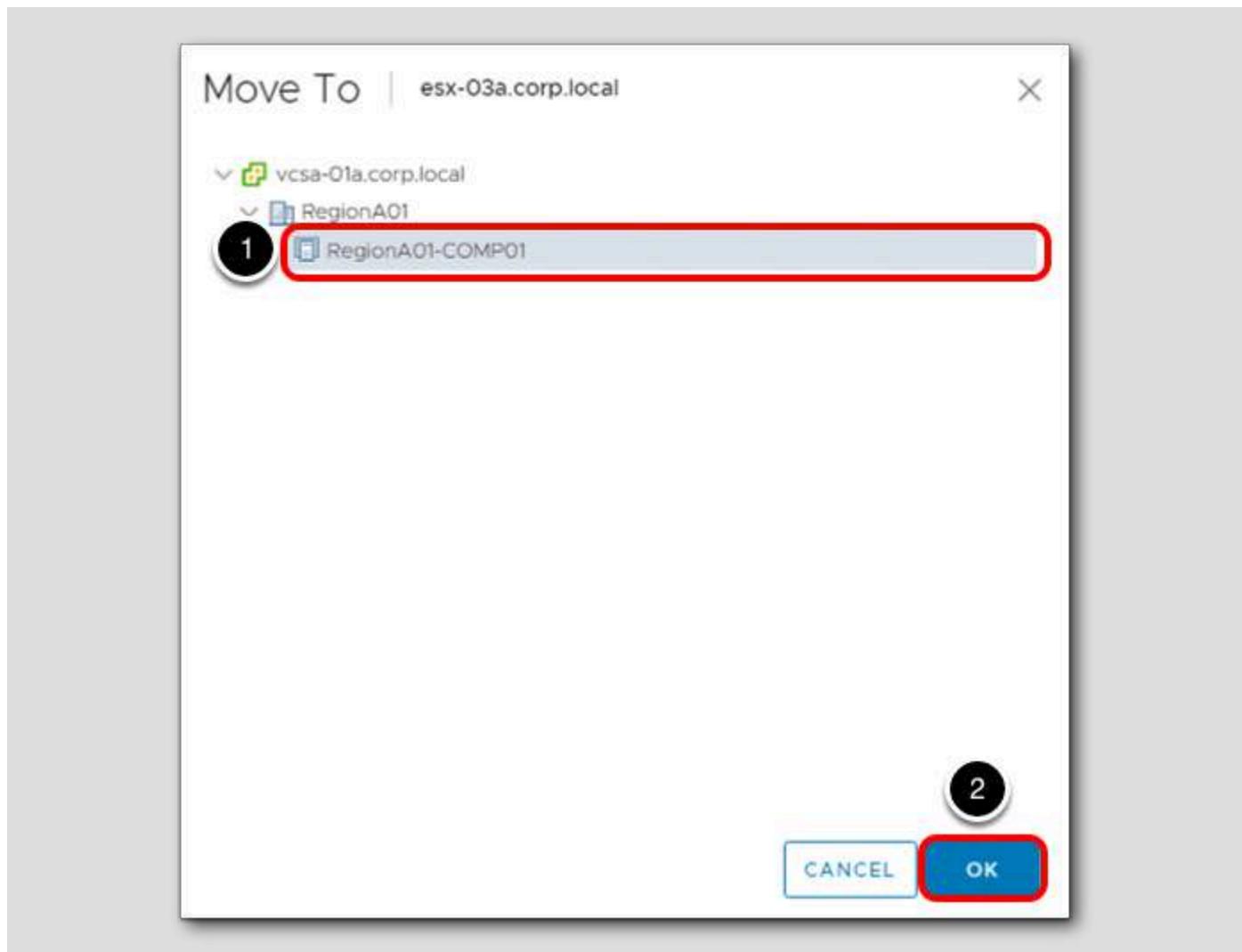
Move into the Cluster



Now that we have the storage configured, move the esx-03a.corp.local into RegionA01-COMP01.

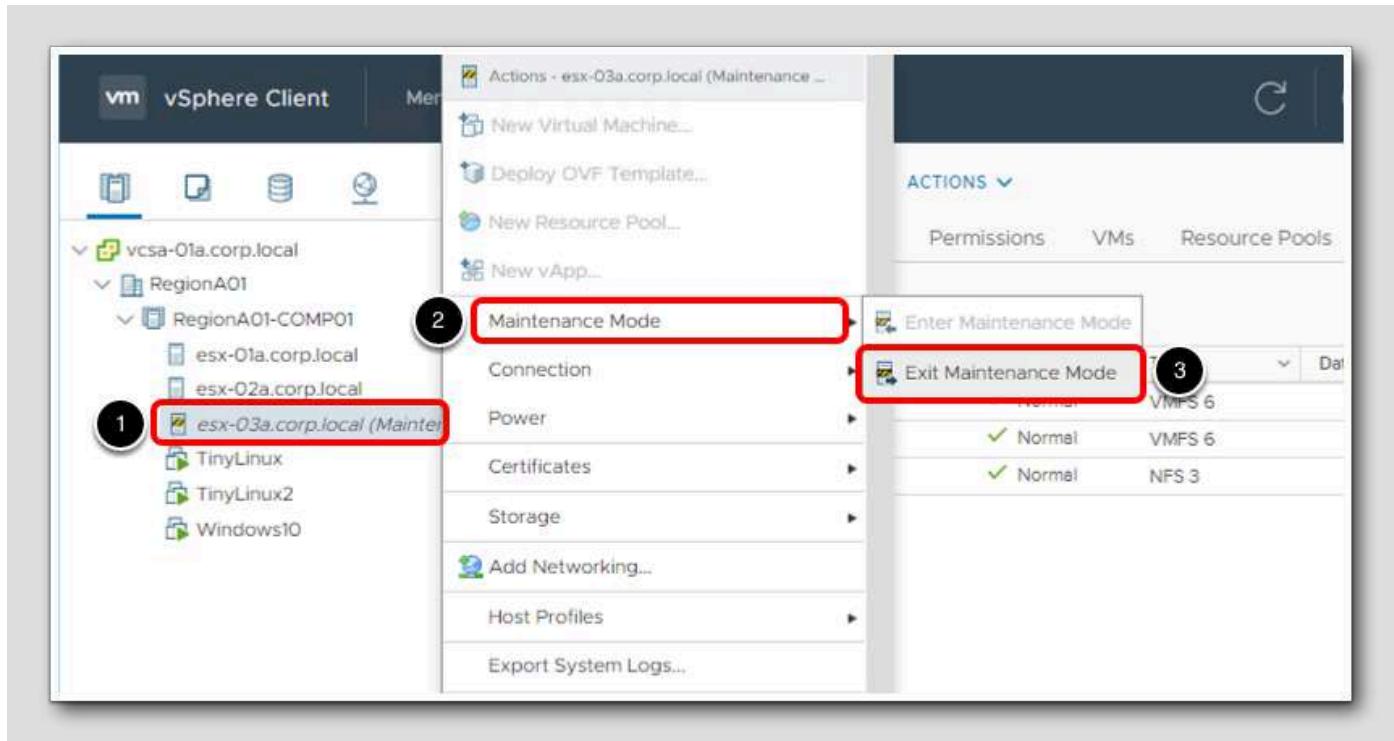
1. Right-click on esx-03a.corp.local
2. Select Move To...

Move To



1. Expand RegionA01 and select RegionA01-COMP01.
2. Click OK.

Exit Maintenance Mode



The host has been added to the cluster. Now it can exit Maintenance Mode and participate in the cluster.

1. Right-click on esx-03a.corp.local.
2. Select Maintenance Mode.
3. Click Exit Maintenance Mode.

Ready to Go

The screenshot shows the vSphere Client interface with the host **esx-03a.corp.local** selected. The host is part of the **vcse-01a.corp.local** cluster. The **Summary** tab is active, displaying the following host information:

- Hypervisor:** VMware ESXi, 7.0.0, 15843807
- Model:** VMware Virtual Platform
- Processor Type:** Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
- Logical Processors:** 2
- NICs:** 4
- Virtual Machines:** 0
- State:** Connected
- Uptime:** 3 hours

Resource usage summary:

Resource	Used	Capacity
CPU	100 MHz	5.5 GHz
Memory	1.24 GB	4.76 GB
Storage	20.32 GB	93.28 GB

Below the summary, there are two expandable sections: **Hardware** and **Configuration**.

After a minute or two, the host will exit Maintenance Mode. If you enabled vSphere HA on the cluster, the HA agent will be configured and started before the host shows a Status of Normal. The process occurs fairly quickly, so a refresh of the Web Client may be required to show the current state.

Note that basic networking for virtual machines, vMotion, and IP Storage have been preconfigured on this host for the purpose of this lab exercise. Adding the new host to a distributed switch would typically be done prior to taking the host out of Maintenance Mode, but is not required for this exercise. Feel free to migrate this switch to the vDS if you would like the practice.

This host is now able to handle workloads for the cluster.

Storage vMotion

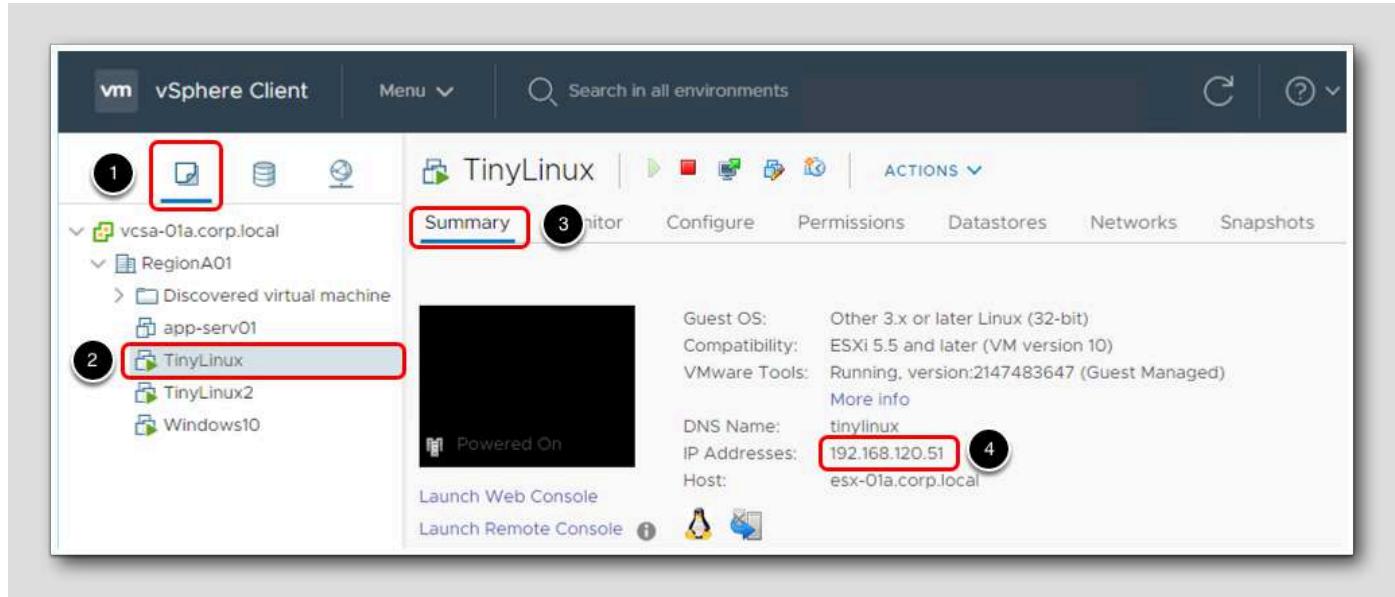
Planned downtime typically accounts for over 80% of datacenter downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule downtime windows.

The vMotion and Storage vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers or to different underlying storage without service interruption. Administrators can perform faster and completely transparent maintenance operations, without being forced to schedule inconvenient maintenance windows. With vSphere vMotion and Storage vMotion, organizations can:

- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

In this lesson, you will learn how to work with vMotion and move virtual machines to different hosts within the cluster.

Navigate to Virtual Machines and Templates



Before the Storage vMotion, we'll verify there is no downtime for the virtual machine by constantly ping it. To ping it, we will need the IP address of the virtual machine, TinyLinux-01.

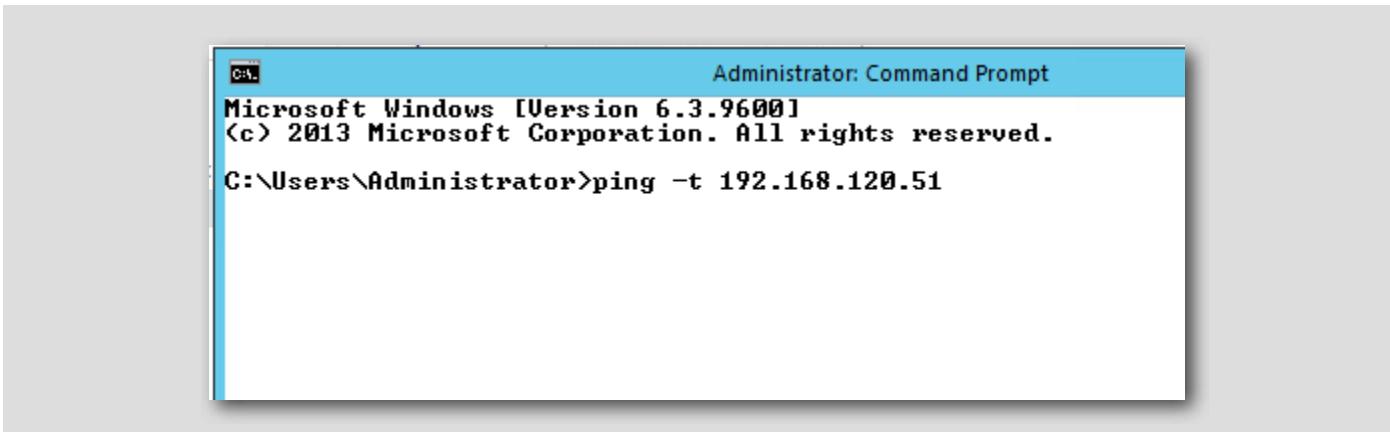
1. Click the VMs and Templates tab.
2. Select TinyLinux.
3. Ensure you are on the Summary tab.
4. Note the IP Address of TinyLinux, 192.168.120.51

Open a Command Prompt



1. Click on the icon to open a command prompt from the Windows Task Bar.

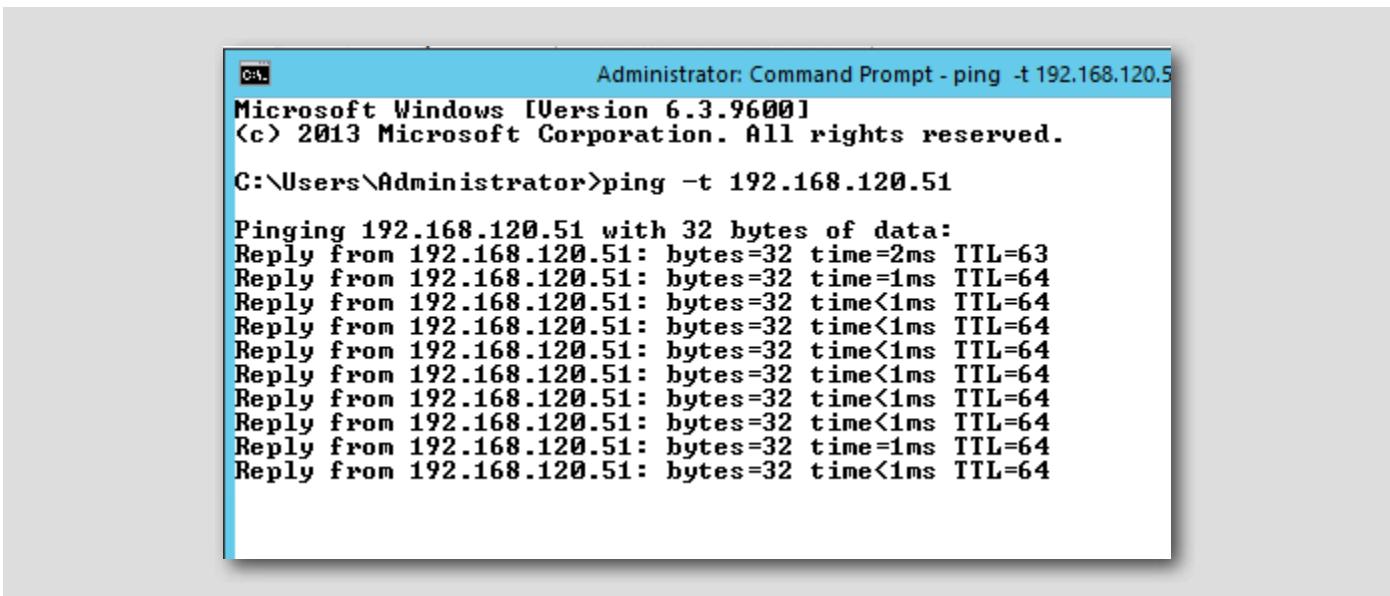
Ping TinyLinux-01



Issue the following in the command prompt and press the Enter key:

```
ping -t 192.168.120.51
```

Ping Results



You should now see a continuous ping to TinyLinux.

Storage View

The screenshot shows the vSphere Client interface with the 'Storage' icon highlighted (circled in red). The left sidebar shows a tree view of vCenter servers and datastores. The 'ds-nfs01' datastore is selected and highlighted in blue. The right panel displays the 'ds-nfs01' datastore details, including its hosts and VMs. The 'Hosts' tab is selected, showing three hosts connected to the datastore: esx-01a.corp.local, esx-02a.corp.local, and esx-03a.corp.local, all in a 'Connected' state with a 'Normal' status.

1. Click the Storage icon.

List Virtual Machines on a Specified Datastore

The screenshot shows the vSphere Client interface with the 'Virtual Machine' icon highlighted (circled in red). The left sidebar shows a tree view of vCenter servers and datastores. The 'ds-iscsi01' datastore is selected and highlighted in blue. The right panel displays the 'Virtual Machines' section for the ds-iscsi01 datastore, showing three virtual machines: TinyLinux, TinyLinux2, and Windows10, all in a 'Powered On' state with a 'Normal' status. The 'VMs' tab is selected in the top navigation bar.

1. Click on the ds-iscsi01 datastore object in RegionA01 managed by the vcsa-01a.corp.local vCenter.

2. Click VMs.

3. Click the Virtual Machines tab.

You should now have a list of all virtual machines on the selected datastore.

Note: depending on which lessons you have completed, the available datastores and virtual machines may be different than the images.

Drag and Drop Storage vMotion

[519]

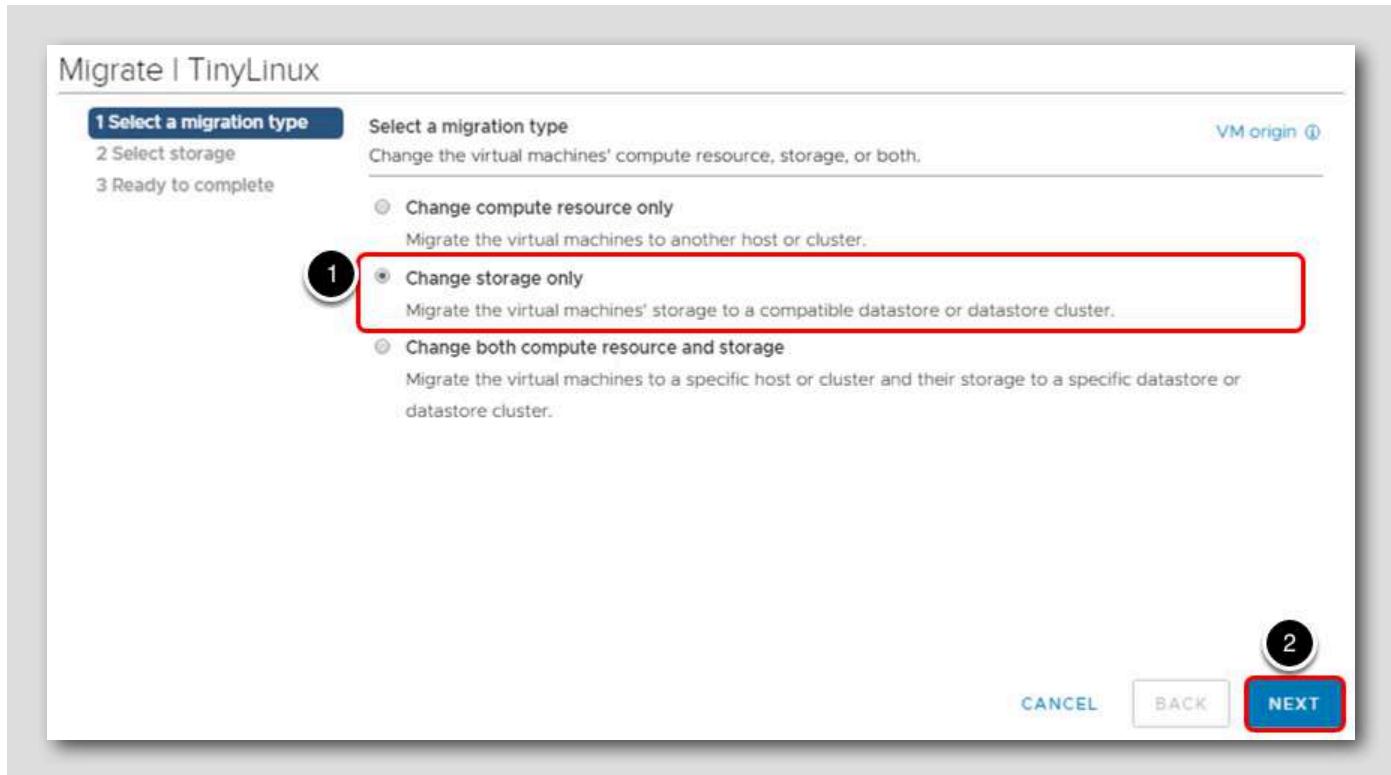
The screenshot shows the vSphere Client interface. On the left, the navigation tree shows a hierarchy: vcsa-01a.corp.local > RegionA01 > ds-iscsi01 (selected), ds-iscsi02, ds-nfs01 (highlighted with a red box and circled with a red number 1), and ds-nfs02. On the right, the 'Virtual Machines' tab is selected in the top navigation bar. The main area displays a table of virtual machines:

VM	State	Status	Provisioned Space	Used Space
TinyLinux	Powered On	Normal	436.83 MB	371.83 MB
TinyLinux2	Powered On	Normal	436.82 MB	371.82 MB
Windows10	Powered On	Normal	27.08 GB	20.56 GB

The VM TinyLinux is initially on ds-iscsi01 and needs to be moved to ds-nfs01.

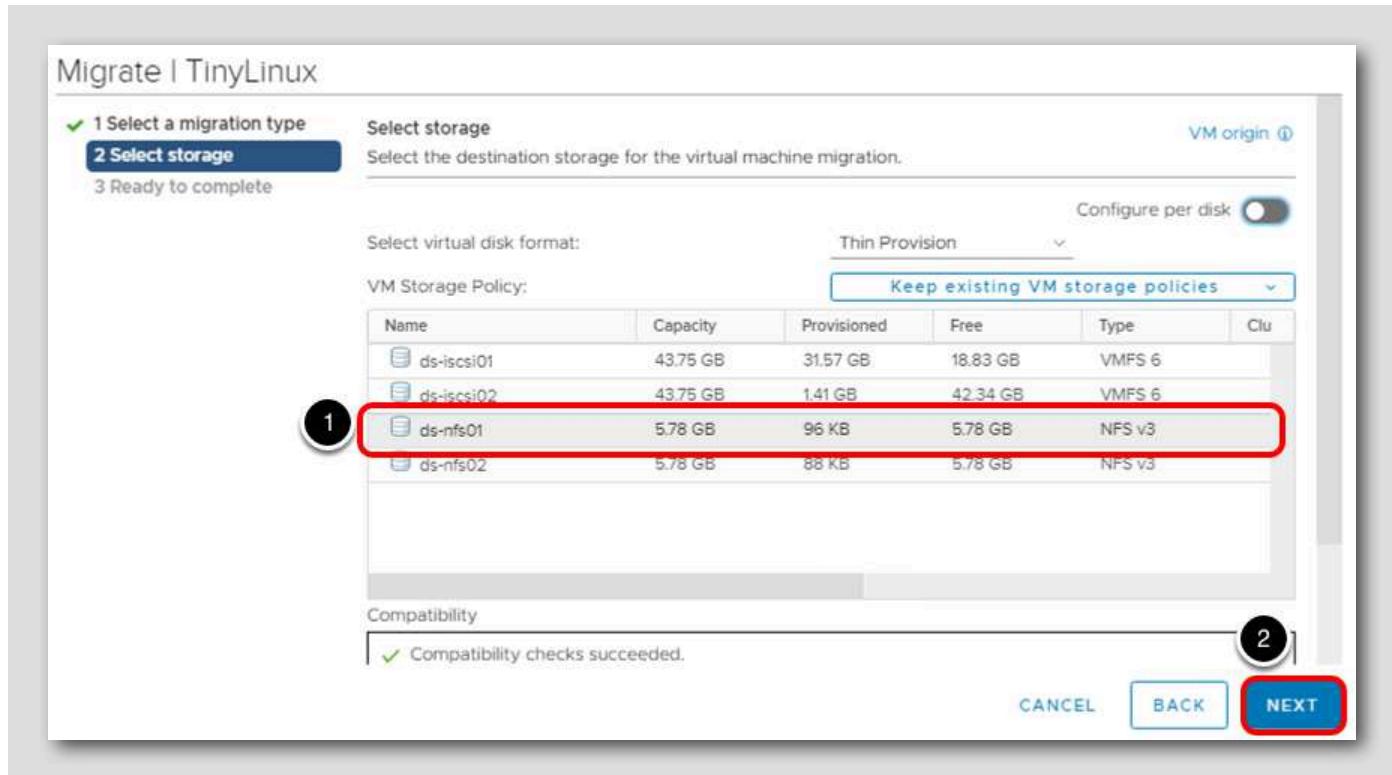
1. Click the TinyLinux VM and continue to hold the left mouse button while dragging the VM to the ds-nfs01 datastore object. A green + will appear near the mouse cursor (see picture) when it is pointing at objects which are suitable targets for the object being moved. Let go of the mouse button to drop the TinyLinux VM onto the ds-nfs01 object. The Migrate wizard will launch to complete the process.

Migrate Datastore



1. Select the radio button to **Change storage only**. Note that as of vSphere 6.5 (and higher) we do have the ability to change compute, network, and storage in the same vMotion operation.
2. Click **Next**.

Storage Policy



1. Note that the ds-nfs01 datastore is already selected because that is where the VM was dropped prior to starting the wizard.
2. Click **Next** to accept the settings for the storage move.

Ready to Complete

Migrate | TinyLinux

✓ 1 Select a migration type Ready to complete VM origin ⓘ

✓ 2 Select storage

3 Ready to complete

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

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	TinyLinux
Storage	ds-nfs01
Disk Format	Thin Provision

1

CANCEL BACK **FINISH**

1. Verify your selections on the Ready to complete screen and click **Finish** to start the migration.

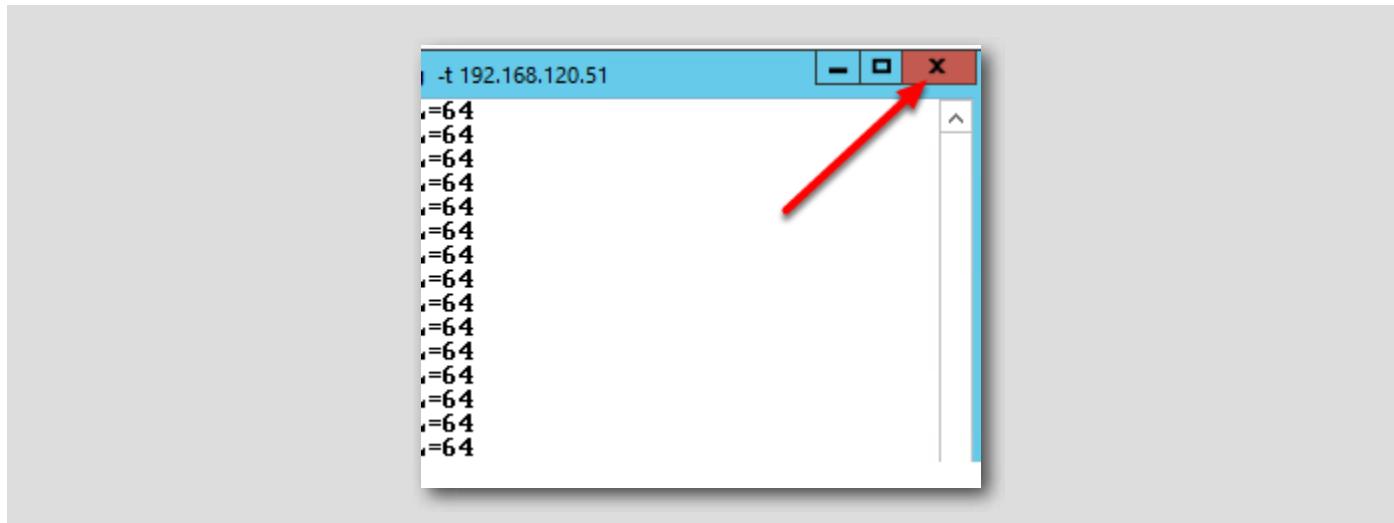
Feel free to monitor the operation within the Recent Tasks pane or move on to the next step.

Confirm no packets were dropped

Go back to the command prompt and review the results of the ping. You can use the scroll bar to see if there were any dropped packets.

You may see instances where the time field increases to 2ms, but otherwise no packets should have dropped.

Stop the ping



Click the 'X' to stop the ping and close the command window.

Confirm Storage vMotion

A screenshot of the vSphere Client interface. The left sidebar shows a tree view of hosts and datastores. A red circle labeled '1' is around the 'ds-nfs01' entry under the 'RegionA01' host. A red box highlights the 'ds-nfs01' entry. The main pane shows the 'VMs' tab selected. A red arrow points to the 'ds-nfs01' entry in the list of virtual machines. The list table has columns: Name, State, Status, and Provisioned Space. One row is visible: 'TinyLinux' (Powered On, Normal, 100.01 MB).

The Storage vMotion progress can be monitored in the Recent Tasks panel.

- Once complete, click on the **ds-nfs01** datastore and notice that the **TinyLinux** virtual machine is listed.

The virtual machine's storage has been migrated from iSCSI to NFS storage without the need to take the virtual machine offline.

Managing Virtual Machine Disks

[526]

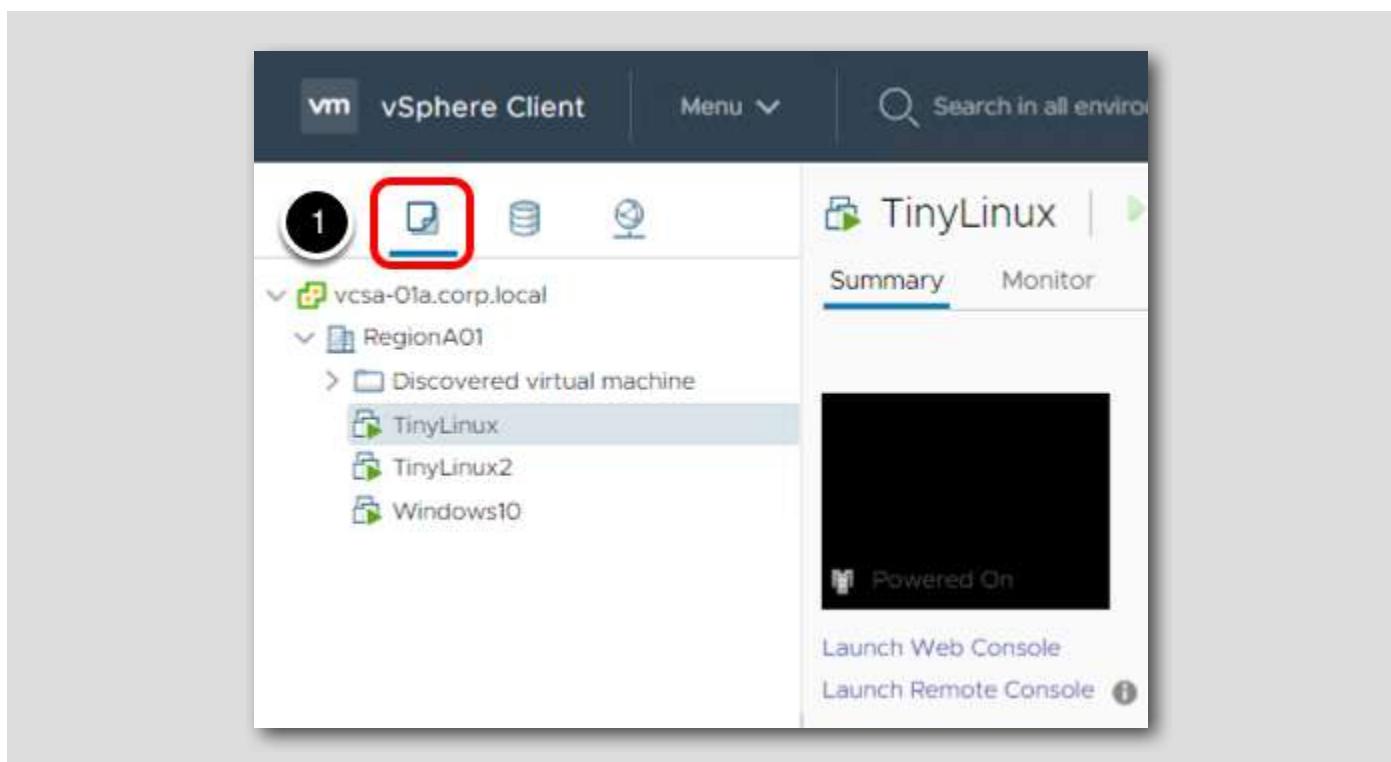
When working with Virtual Machines, you can create a virtual disk or use an existing virtual disk. A virtual disk comprises one or more files on the file system that appear as a single hard disk to the guest operating system. These disks are portable among hosts.

You use the "Create Virtual Machine" wizard to add virtual disks during virtual machine creation. However, in this lesson you will work with an existing Virtual Machine in the inventory.

This lesson will walk you through the process of adding a new virtual disk to an existing Virtual Machine. Additionally, you will extend the Virtual Machine's original disk to a larger capacity.

Navigate to the VMs and Templates management pane

[527]



- Select VMs and Templates.

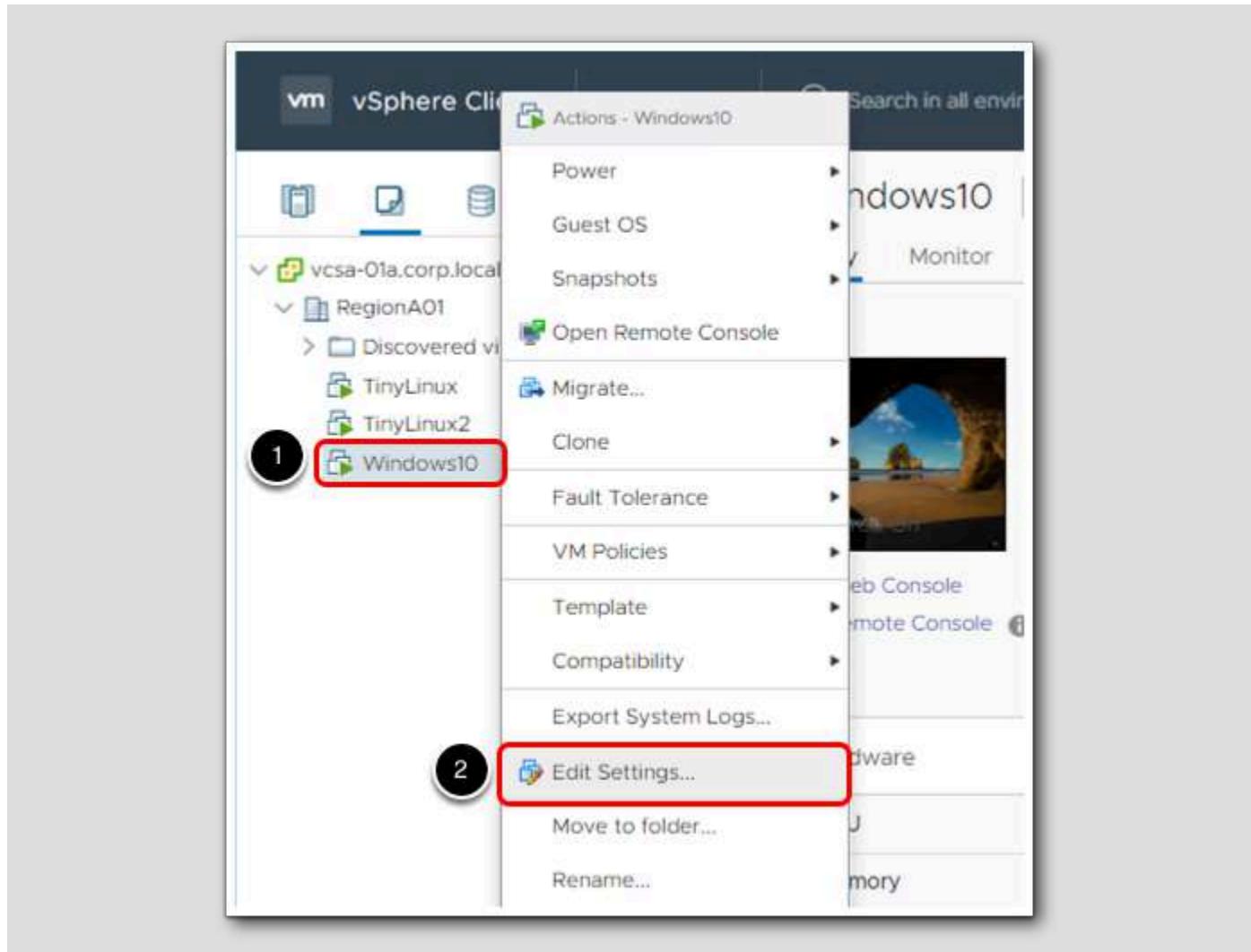
From this view, we can see that there are several existing Virtual Machines in our vSphere environment. In the next step, we will add a new virtual disk to the Windows10 Virtual Machine.

Verify windows10 Storage

The screenshot shows the vSphere Client interface. On the left, the inventory tree shows a folder named 'RegionA01' containing a 'Discovered virtual machine' folder with 'TinyLinux', 'TinyLinux2', and 'Windows10'. A red circle labeled '1' highlights the 'Windows10' entry. In the center, the 'Windows10' virtual machine summary tab is selected, showing its configuration details. A red circle labeled '2' highlights the power button icon. On the right, the 'VM Hardware' pane displays the VM's hardware components: CPU (1 CPU(s)), Memory (2 GB, 0.22 GB memory active), Hard disk 1 (25 GB), Network adapter 1 (VM-RegionA01-vDS-COMP connected), and CD/DVD drive 1 (Disconnected). A red circle labeled '3' highlights the 'Hard disk 1' entry. An arrow points from the 'Hard disk 1' entry in the hardware pane up towards the notes section on the right.

1. Select Virtual Machine Windows10 and click the Summary tab.
2. If w12-core is not powered on, click the power on button.
3. In the VM Hardware pane, note the original disk configuration - single hard disk with a capacity of 25.00 GB. You may need to expand the VM Hardware section to see it.

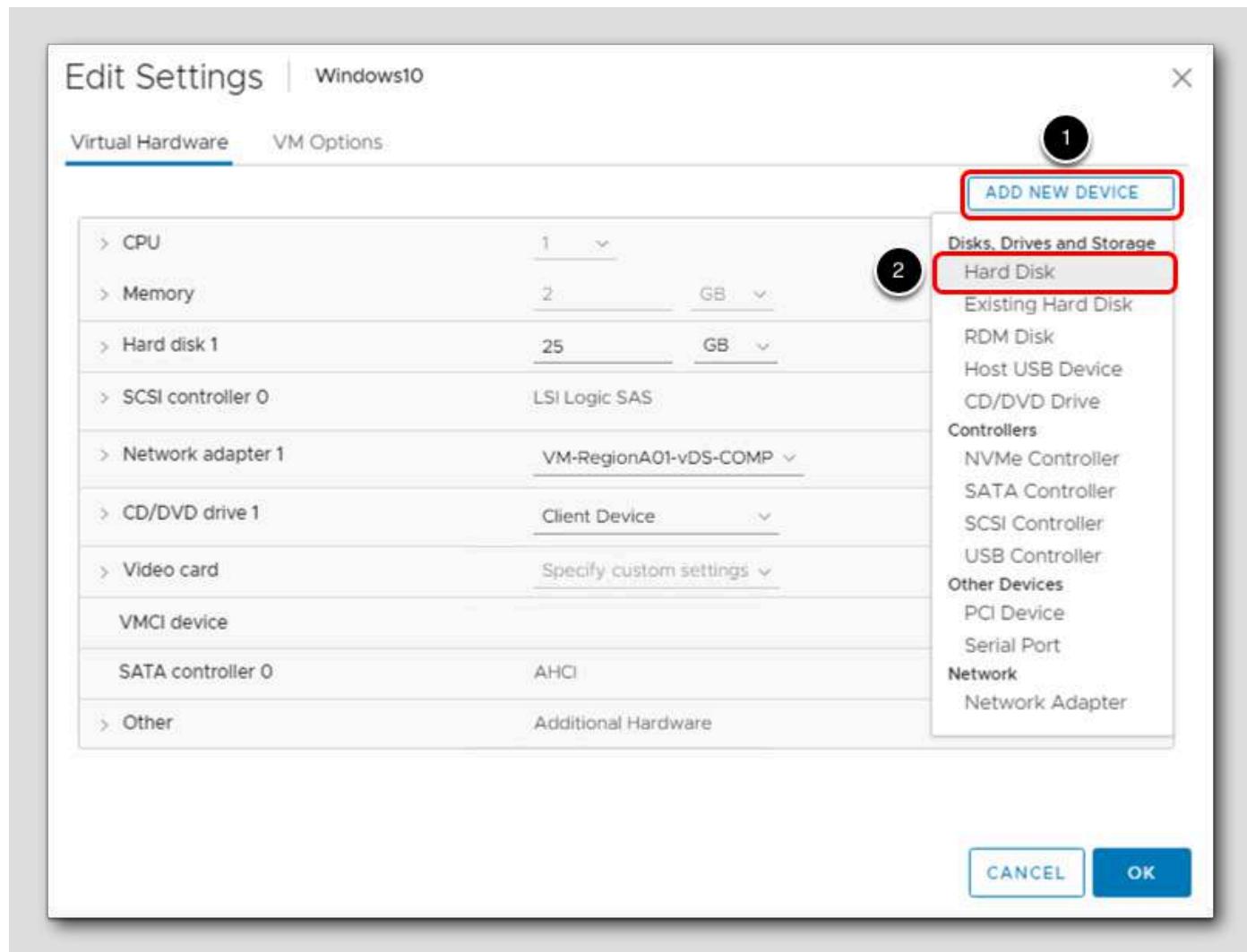
Edit VM Settings



1. Right-click on Windows10

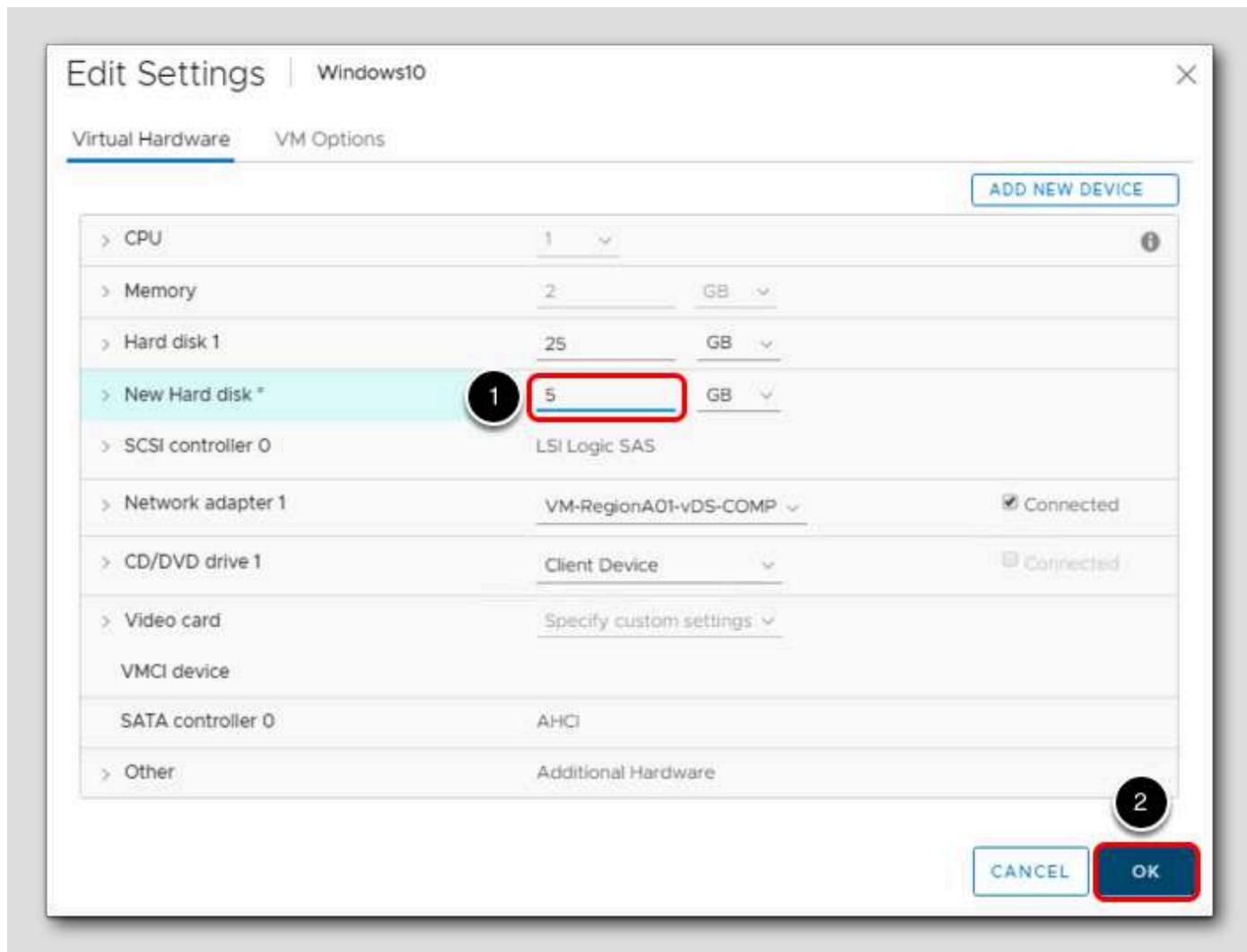
2. Select Edit Settings

Add New Device



1. Click the Add New Device button.
2. Click Hard Disk.

Configure Size and Provisioning settings



1. Decrease the size to 5 GB.
2. Click OK to create the new virtual disk.

Monitor task progress

The screenshot shows the vSphere Web Client interface. On the left, the navigation tree displays a folder structure under 'vcsa-01a.corp.local' with 'RegionA01' expanded, showing 'Discovered virtual machine' containing 'TinyLinux', 'TinyLinux2', and 'Windows10'. The 'Windows10' item is selected and highlighted with a blue border. The main pane shows the 'Windows10' summary card. The 'Summary' tab is active. The card displays the following details:

Guest OS:	Microsoft Windows 10
Compatibility:	ESXi 6.5 and later (V1)
VMware Tools:	Running, version:1129
More info	
DNS Name:	Windows10.corp.local
IP Addresses:	192.168.120.53
View all 2 IP addresses	
Host:	esx-02a.corp.local

Below the summary card is the 'VM Hardware' section, which lists the following components:

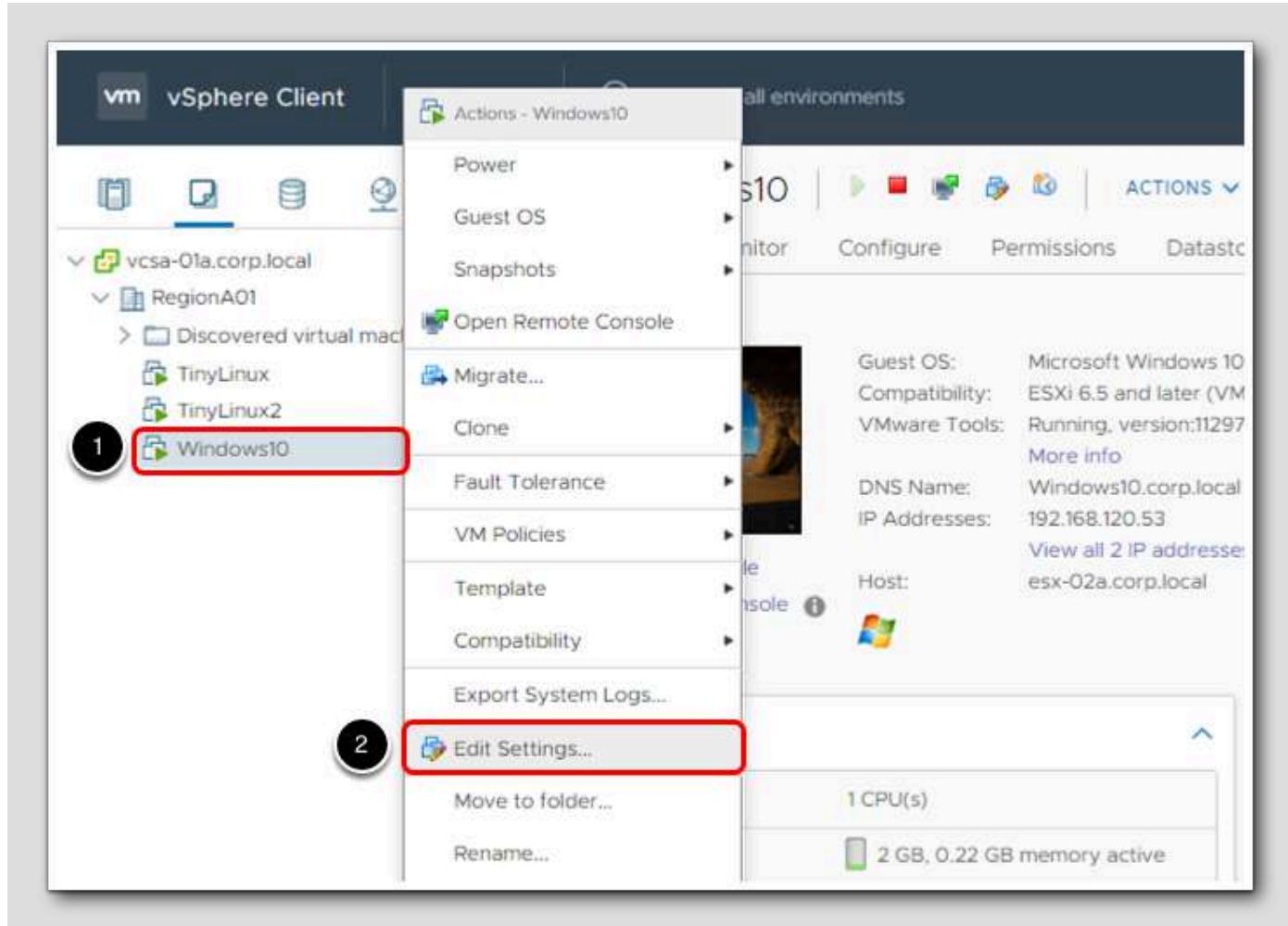
> CPU	1 CPU(s)
> Memory	2 GB, 0.22 GB memory active
> Hard disk 1	25 GB
> Hard disk 2	5 GB
> Network adapter 1	VM-RegionA01-vDS-COMP (connected)

A red box highlights the 'Hard disk 2' row, and a black circle with the number '1' is positioned to the left of the hardware list.

You can follow the progress in the Recent Tasks pane

1. You should now see Hard disk 2 with a capacity of 5 GB available to the Windows10 VM.

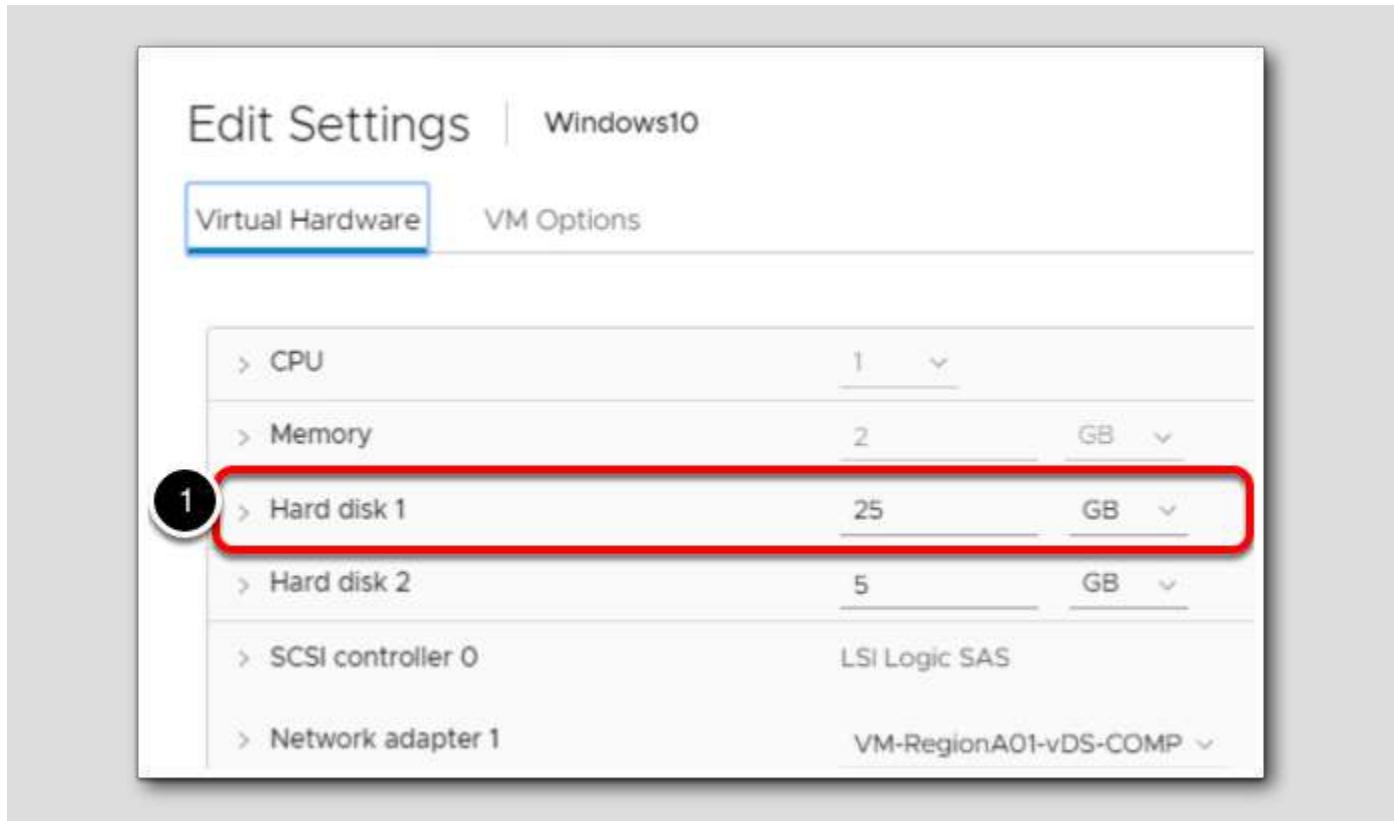
Extend an existing Virtual Disk



In this section, you will extend an existing Virtual Disk for a Virtual Machine.

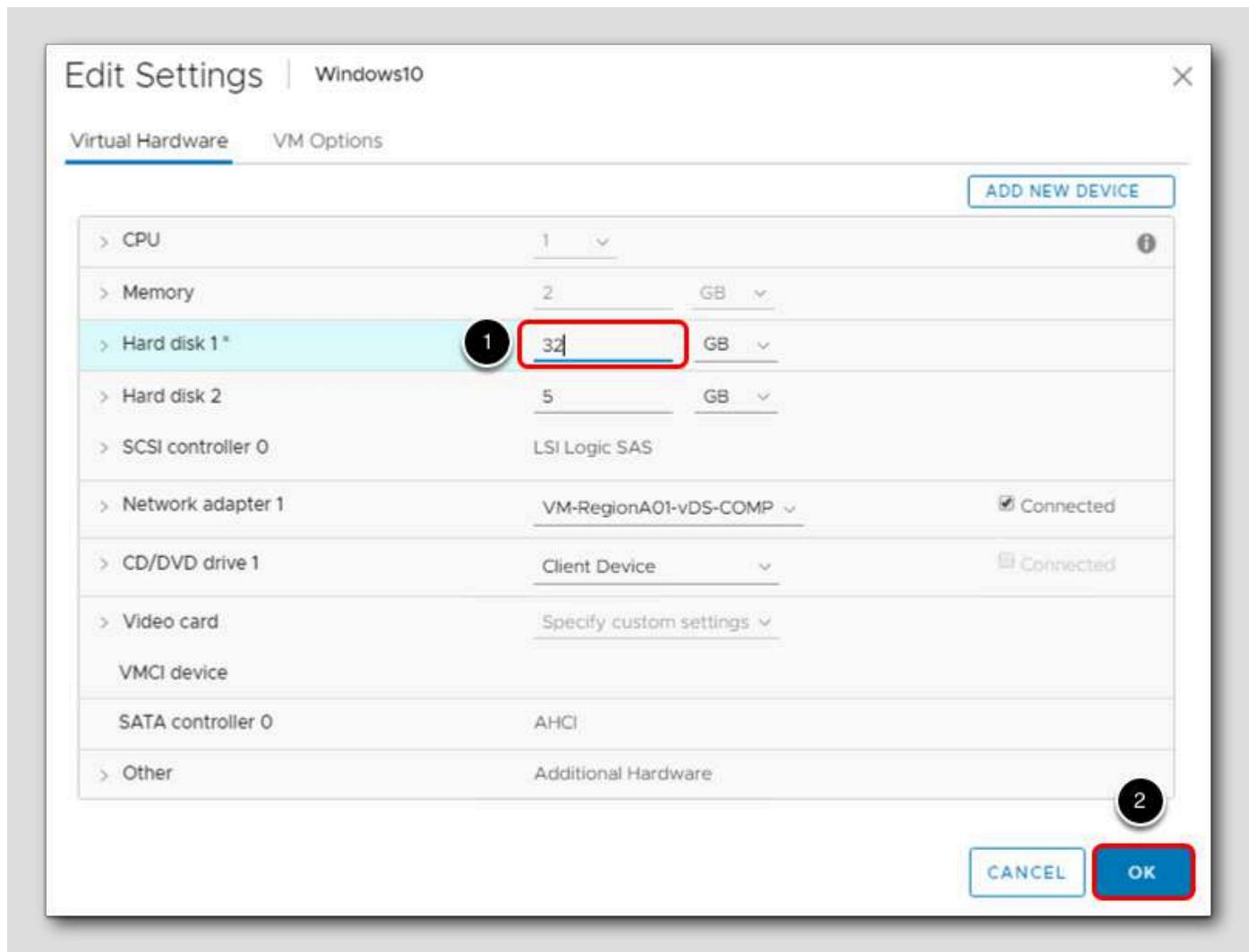
1. Right-click the Virtual Machine **Windows10**.
2. Select **Edit Settings...**.

Hard disk 1 settings



1. In the Edit Settings wizard, note the capacity for Hard disk 1 is 25 GB.

Extend Hard disk 1



1. Type 32 Hard disk 1 capacity field.
2. Click OK.

Monitor task progress

The screenshot shows the vSphere Client interface. On the left, the inventory tree shows a folder named 'RegionA01' containing several virtual machines: 'Discovered virtual machine', 'TinyLinux', 'TinyLinux2', and 'Windows10'. The 'Windows10' VM is selected and highlighted with a blue border. On the right, the 'Summary' tab is active for the 'Windows10' VM. The summary card displays the following information:

Guest OS:	Microsoft Windows 10 (0)
Compatibility:	ESXi 6.5 and later (VM)
VMware Tools:	Running, version:11297 (0)
More info	
DNS Name:	Windows10.corp.local
IP Addresses:	192.168.120.53 View all 2 IP addresses
Host:	esx-02a.corp.local

Below the summary card is a 'VM Hardware' section. It lists the following components:

CPU	1 CPU(s)
Memory	2 GB, 0.38 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB
Network adapter 1	VM-RegionA01-vDS-COMP (connected)

A red circle with the number '1' is drawn around the 'Hard disk 1' row in the VM Hardware list.

You can follow the progress in the Recent Tasks pane.

1. You should now see Hard disk 1 with a capacity of 32 GB available to the windows10 VM.

Review the Virtual Disk Configuration

The screenshot shows the vSphere Web Client interface for a virtual machine named 'Windows10'. The 'VM Hardware' section is expanded, displaying details about the CPU (1 CPU(s)), Memory (2 GB, 0.64 GB memory active), and two Hard disks (32 GB and 5 GB). The 'Notes' section contains system information and patch history. Two specific items are highlighted with red boxes and numbered circles: item 1 highlights the 'Hard disk 1' and 'Hard disk 2' entries in the VM Hardware list; item 2 highlights the 'MEMORY USAGE 655 MB' and 'STORAGE USAGE 23.28 GB' summary statistics.

1. Note each of the configured virtual disks and associated capacity.
2. Note that due to Thin Provisioning, the total consumed storage for the virtual disks is only using about half of the 32GB!

Working with Virtual Machine Snapshots

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines. You can also take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. The Snapshot Manager in the vSphere Web Client provides several operations for creating and managing virtual machine snapshots and snapshot trees. These operations let you create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more.

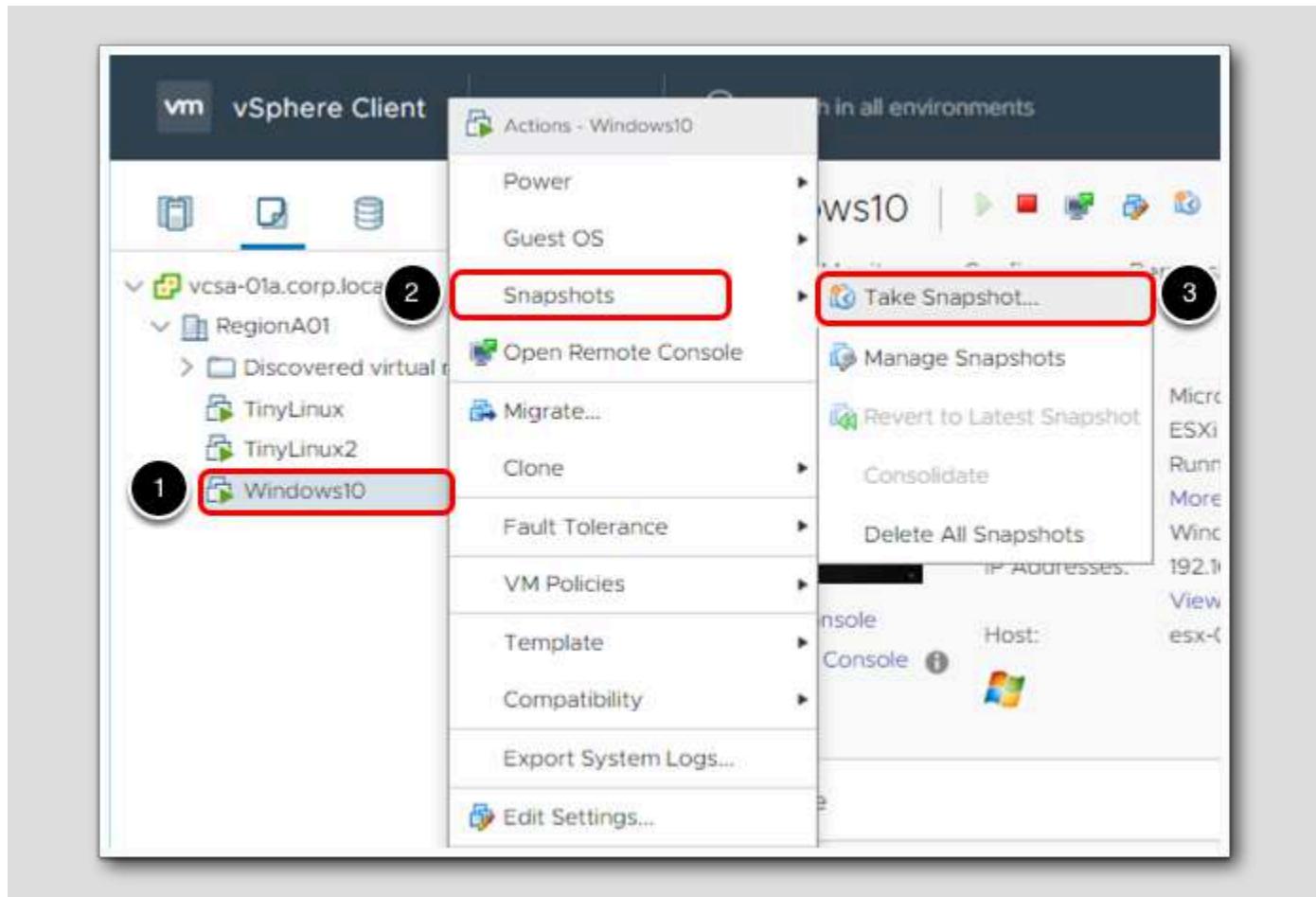
A Virtual Machine snapshot preserves the following information:

- **Virtual machine settings** - The virtual machine directory, which includes disks that were added or changed after you took the snapshot.
- **Power state** - The virtual machine can be powered on, powered off, or suspended.
- **Disk state** - State of all the virtual machine's virtual disks.
- **Memory state (optional)** - The contents of the virtual machine's memory.

In this section, you will create a Virtual Machine snapshot, make changes to the Virtual Machine's hardware and configuration state, and

then revert back to the original state of the Virtual Machine by leveraging the vSphere Web Client Snapshot Manager.

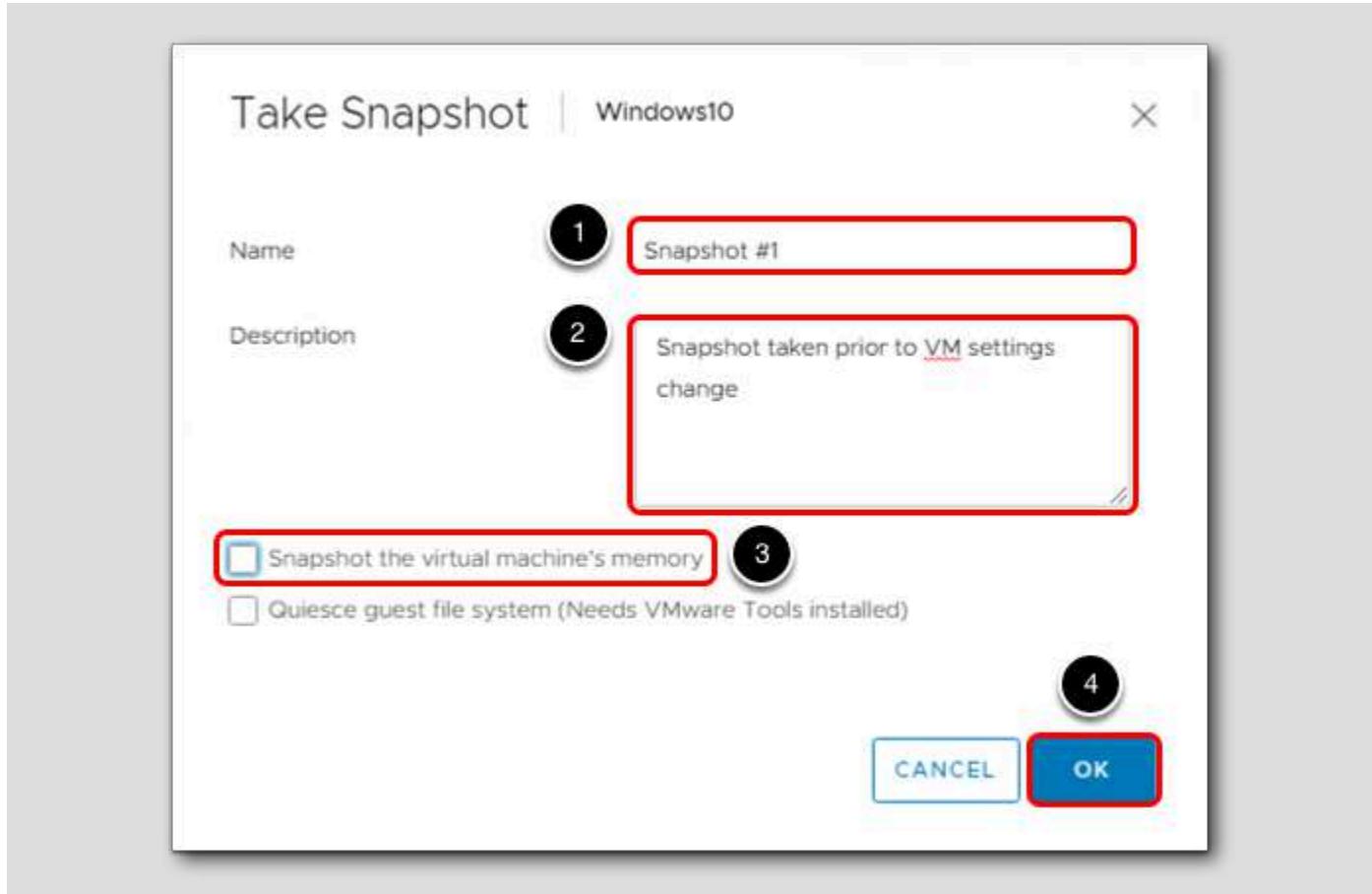
Take a Virtual Machine Snapshot



In this step, you'll take a Snapshot of a Virtual Machine.

1. Right-click windows10.
2. Select Snapshots.
3. Click Take Snapshot.

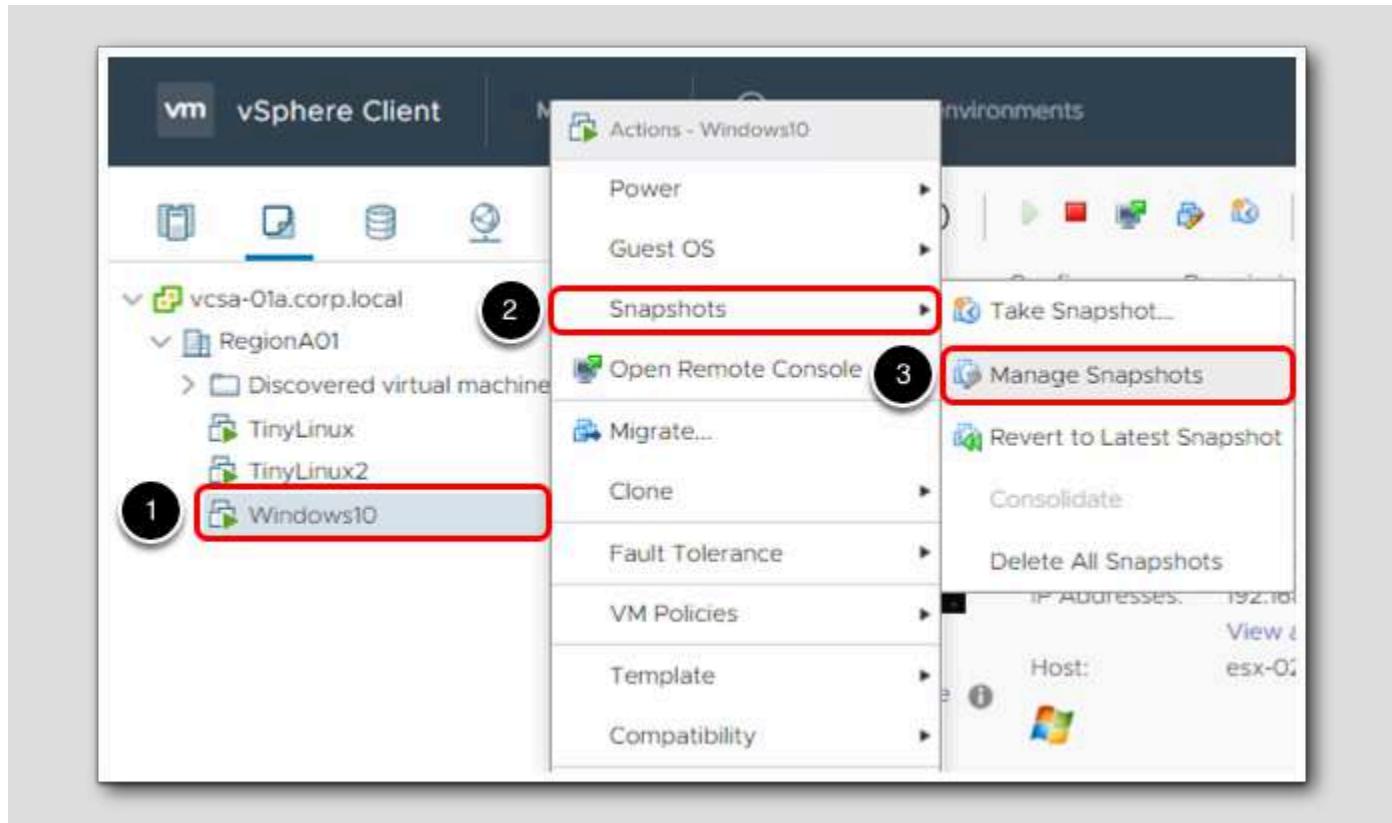
Enter a Name and Description for the VM Snapshot



1. In the Take Snapshot window, provide a name for the Snapshot point - **Snapshot #1**
2. Provide a description for the Snapshot point - **Snapshot taken prior to VM settings change**
3. Uncheck the **Snapshot the virtual machine's memory** box.
4. Click **OK**.

Note: When you take a snapshot of a powered-on virtual machine, you are given the option to capture the running VMs memory state. In our case, since we are in a lab environment, this will generate unneeded I/O.

Open the Snapshots tab



Note the progress in the Recent Tasks pane. Once the snapshot task is complete:

1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Snapshot Details

Manage Snapshots | Windows10

Windows10

Snapshot #1

You are here

Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	12/16/2020, 2:05:26 PM
Disk usage	23.48 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

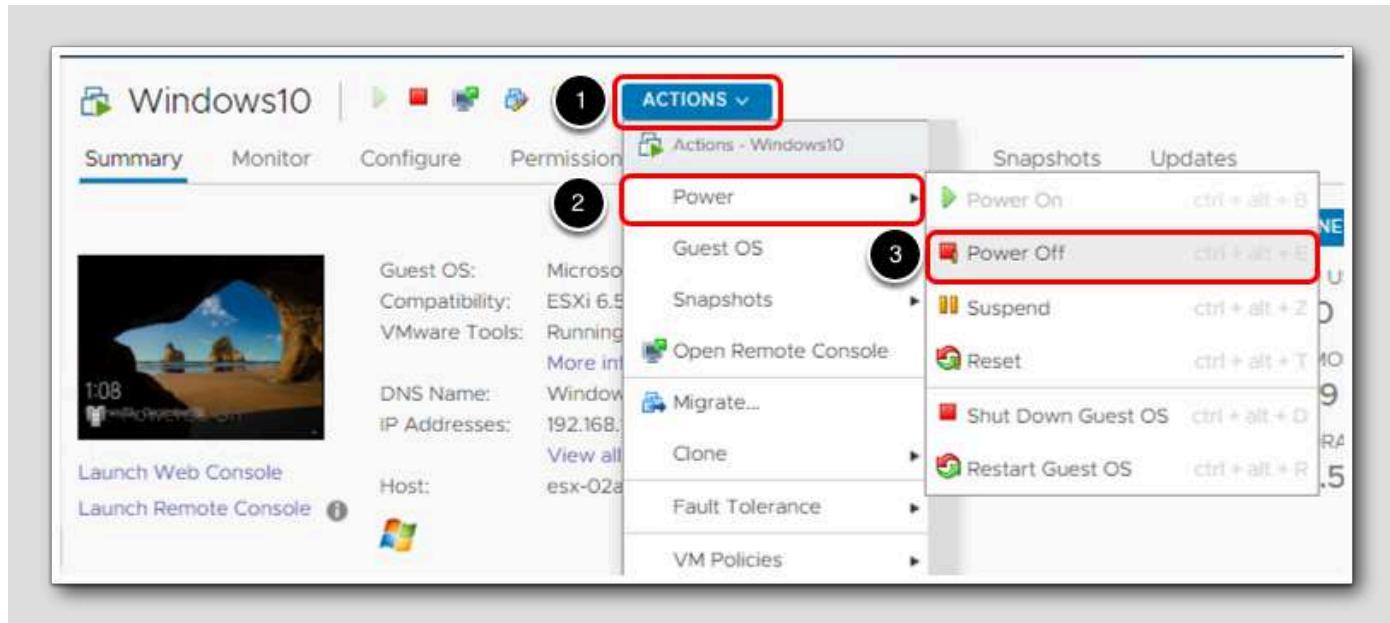
DELETE ALL DELETE REVERT TO EDIT DONE

1

Here you can view the details of the snapshot and verify it was taken.

1. Click Done when you are finished viewing the details.

Change the Virtual Machine Settings

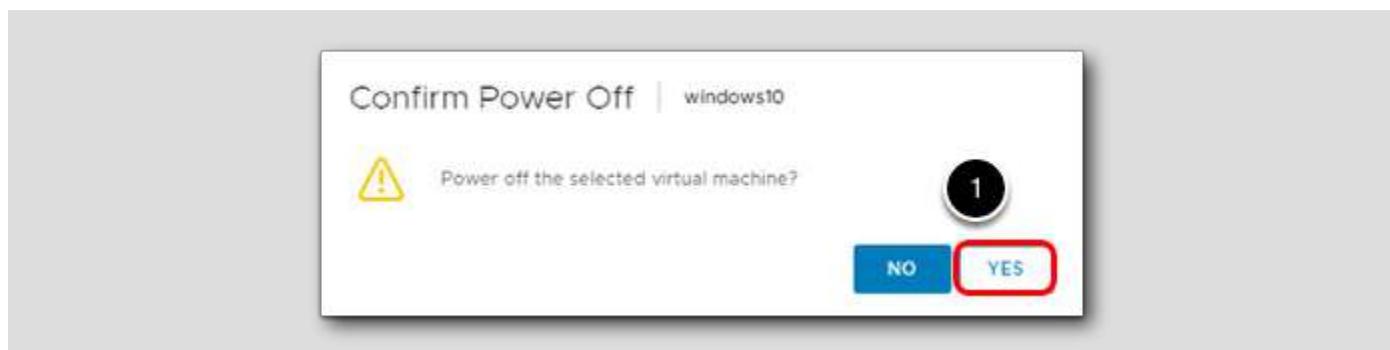


In this section, you will change the memory configuration for the Virtual Machine.

To change the memory configuration for Windows10, we will need to shut it down.

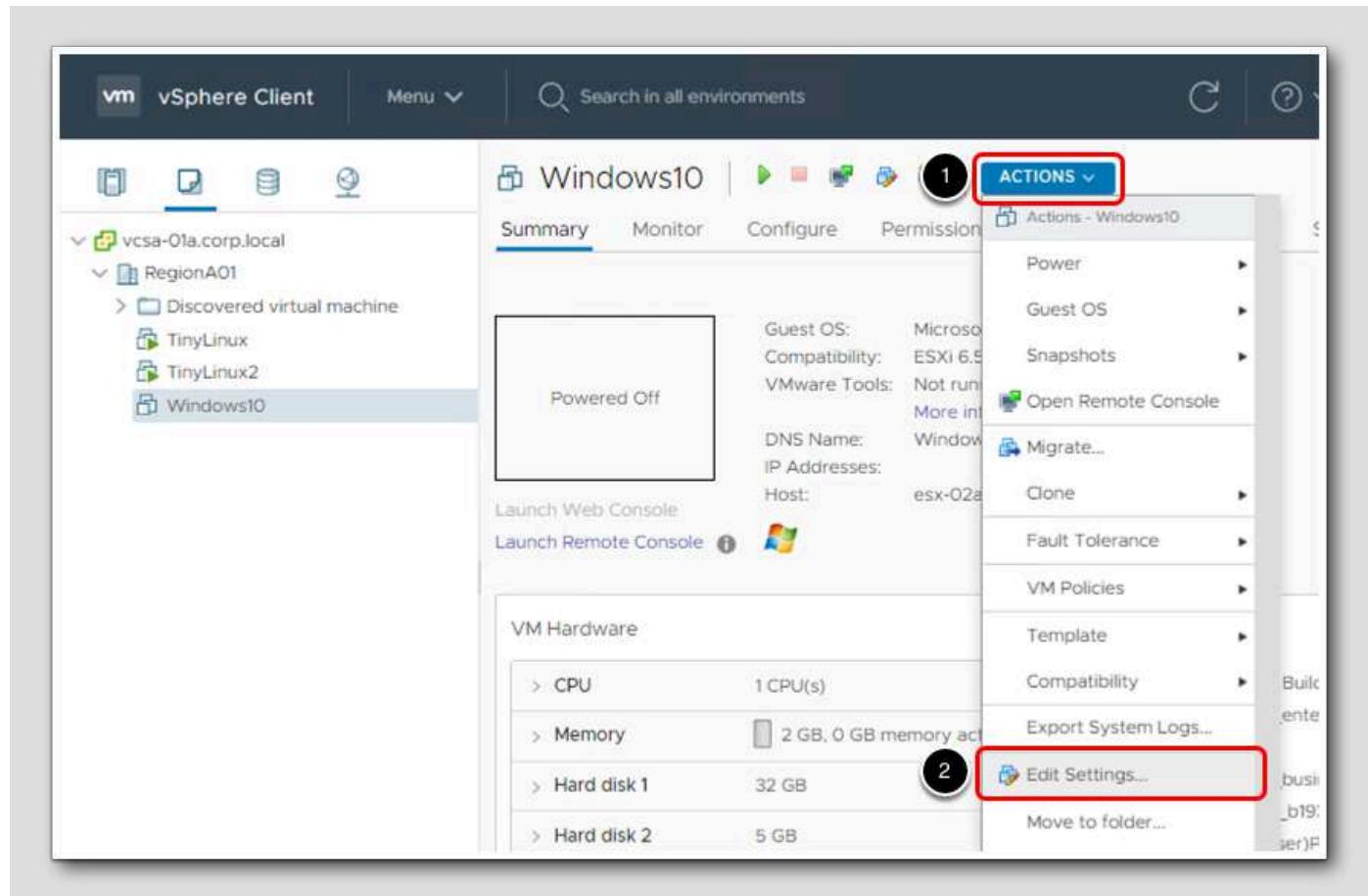
1. Click the Actions menu.
2. Select Power.
3. Click on Power Off.

NOTE: This is not the proper way to shut the VM down gracefully, but for our lab environment, it provides a quick way to power off a machine.



1. Click the Yes button to power off the virtual machine.

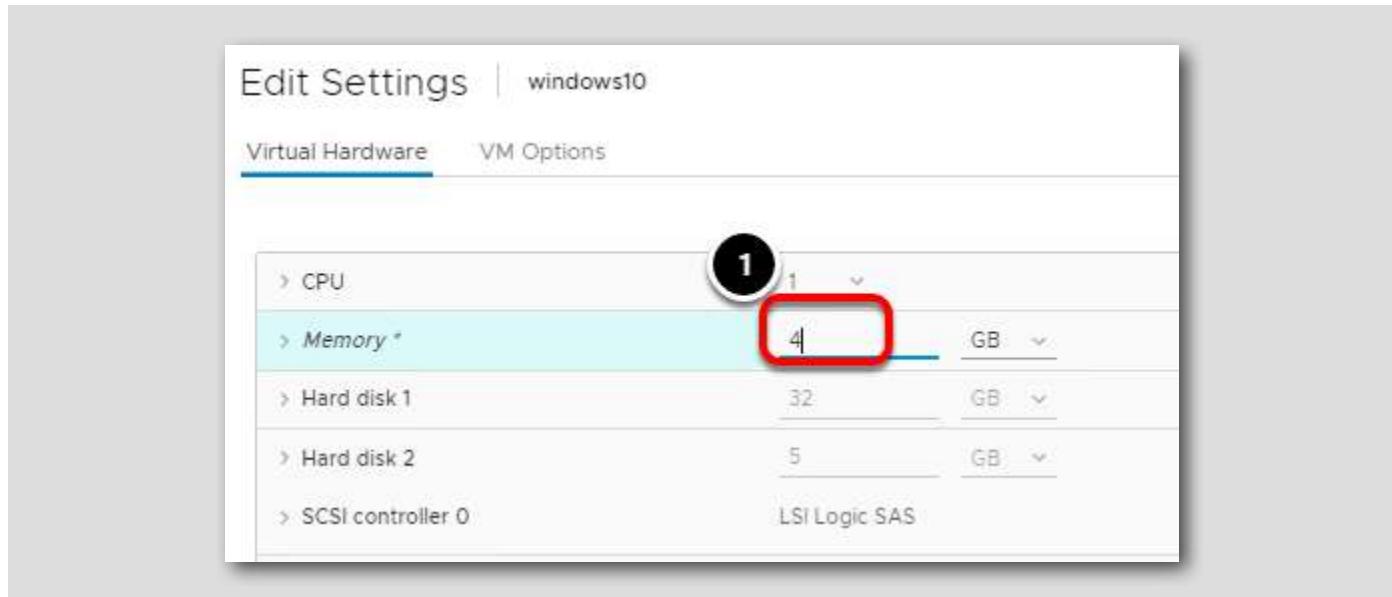
Launch the Edit Settings wizard



1. Click the "Actions" drop-down menu.

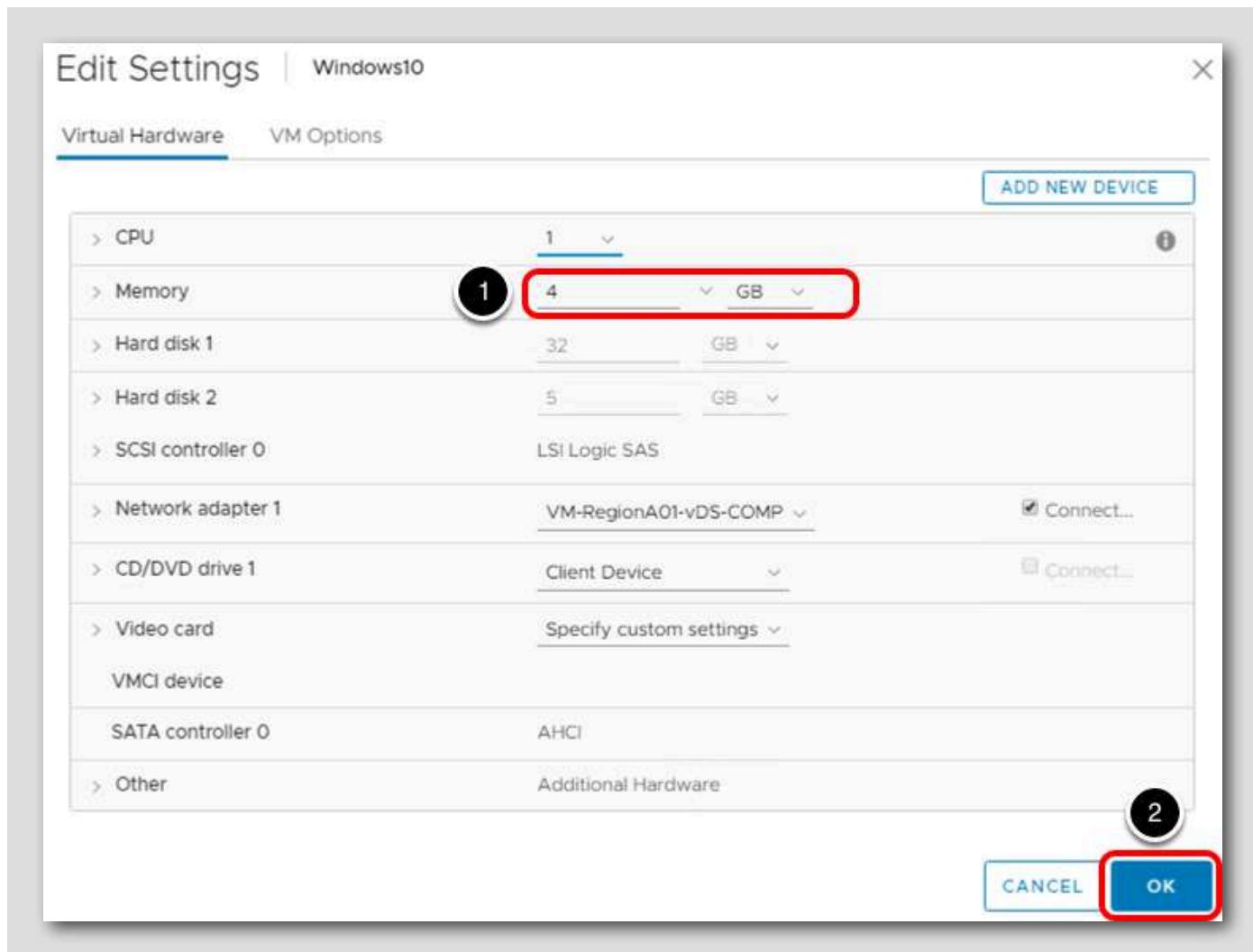
2. Select "Edit Settings..."

Change the Virtual Machine's settings



1. In the Memory field, change this setting to "4".

Review the Virtual Machine's new settings



1. Note the new Memory configuration.

2. Click OK to continue.

Summary tab

vSphere Client | Menu | Search in all environments

vcsa-01a.corp.local | RegionA01 | Discovered virtual machine | TinyLinux | TinyLinux2 | Windows10

Windows10 | ACTIONS

Summary Monitor Configure Permissions Data

Powered Off

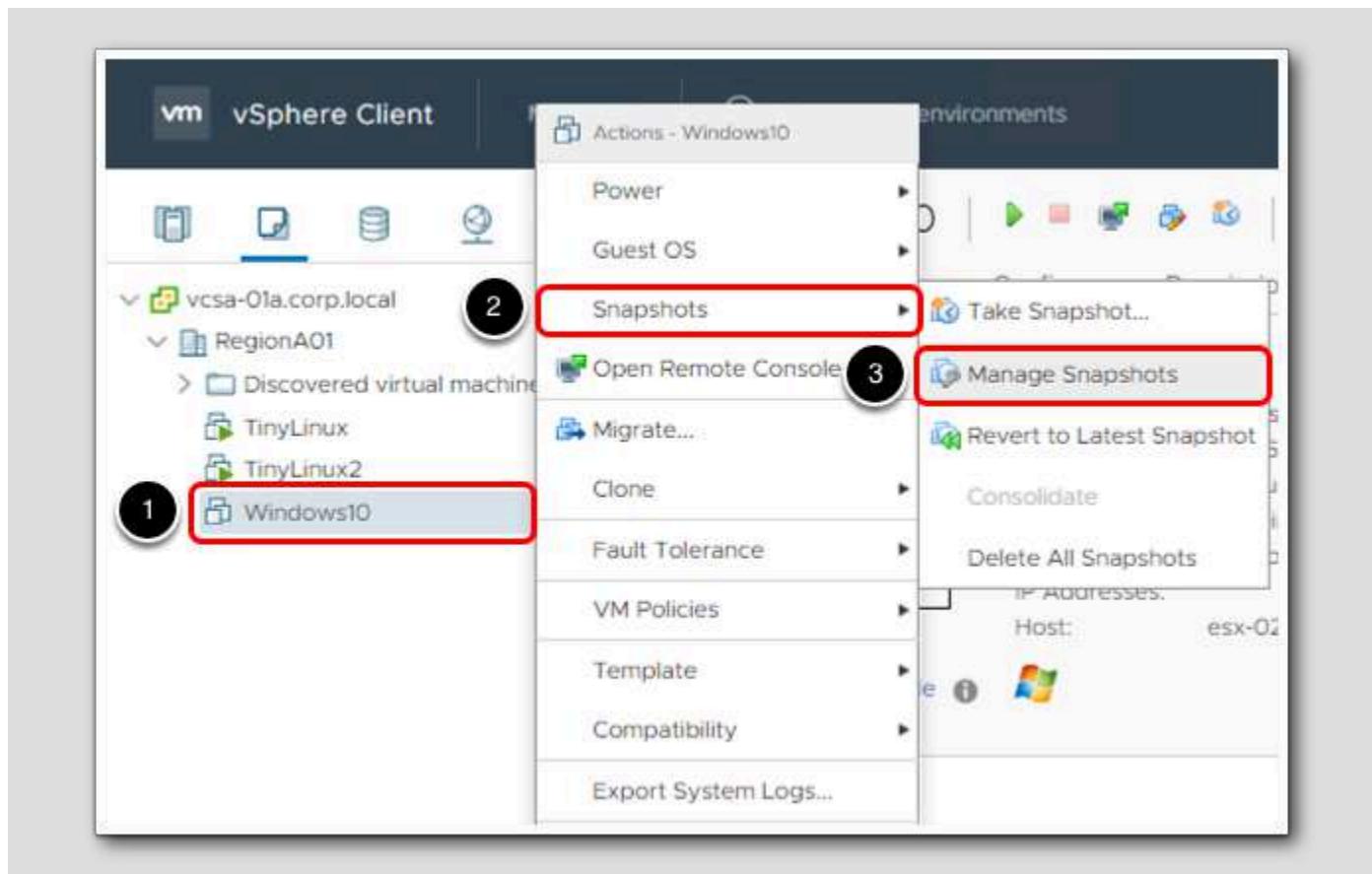
Launch Web Console | Launch Remote Console

VM Hardware

- CPU 1 CPU(s)
- Memory 4 GB, 0 GB memory active**
- Hard disk 1 32 GB
- Hard disk 2 5 GB

1. Make sure you are on the Summary tab for Windows10.
2. Verify the memory has been updated.

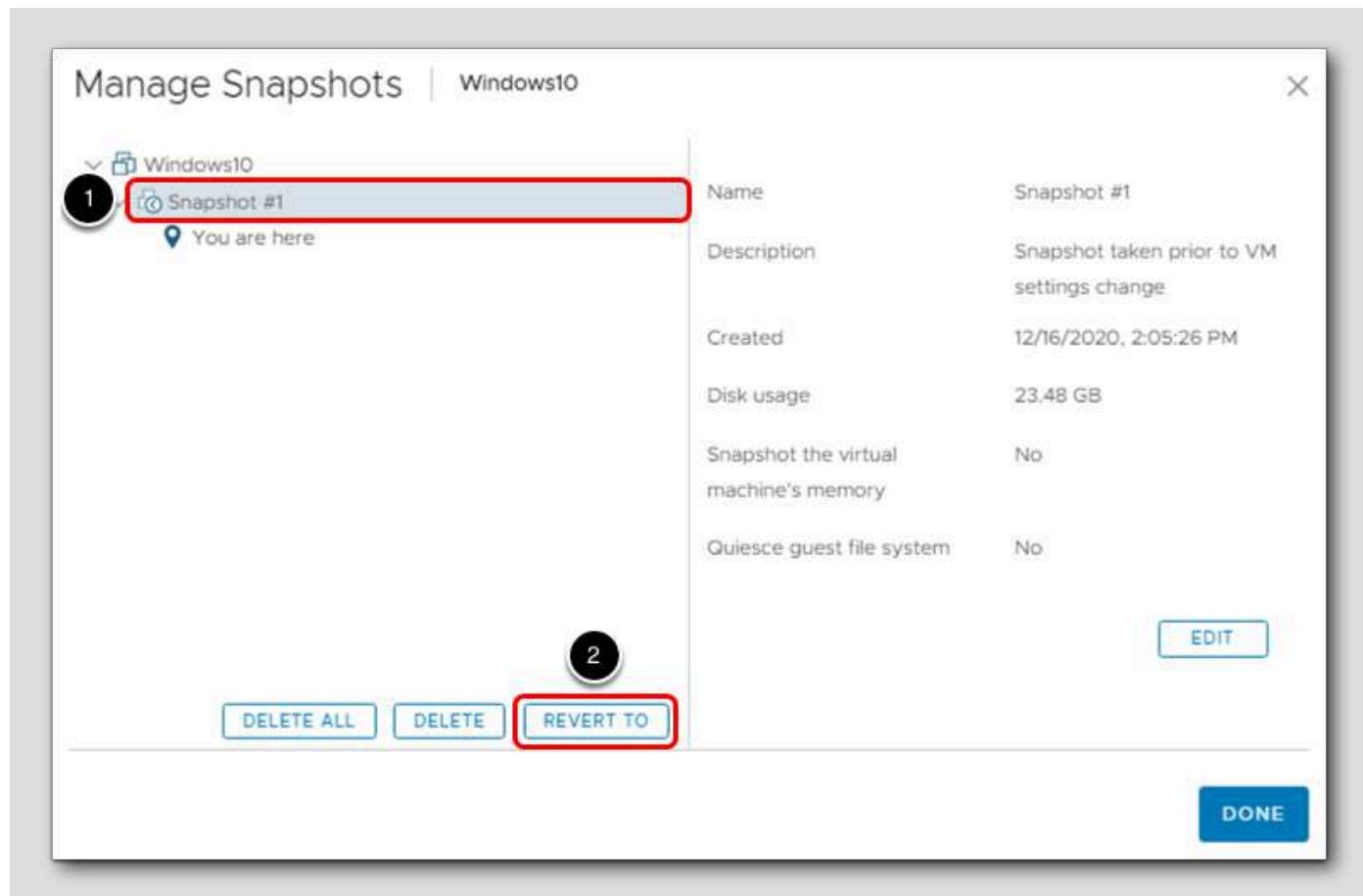
Revert Virtual Machine settings using the Snapshot Manager



In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

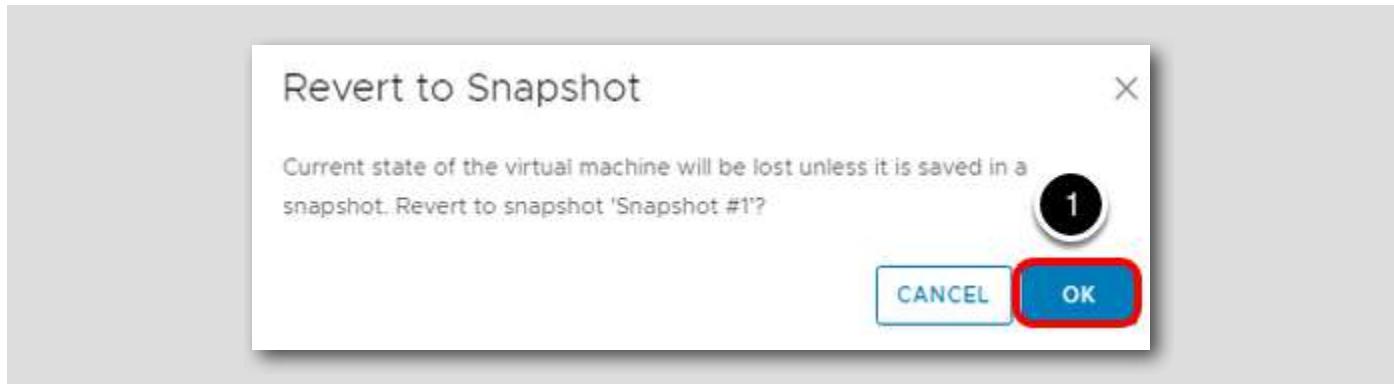
1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Select the VM Snapshot to Revert to



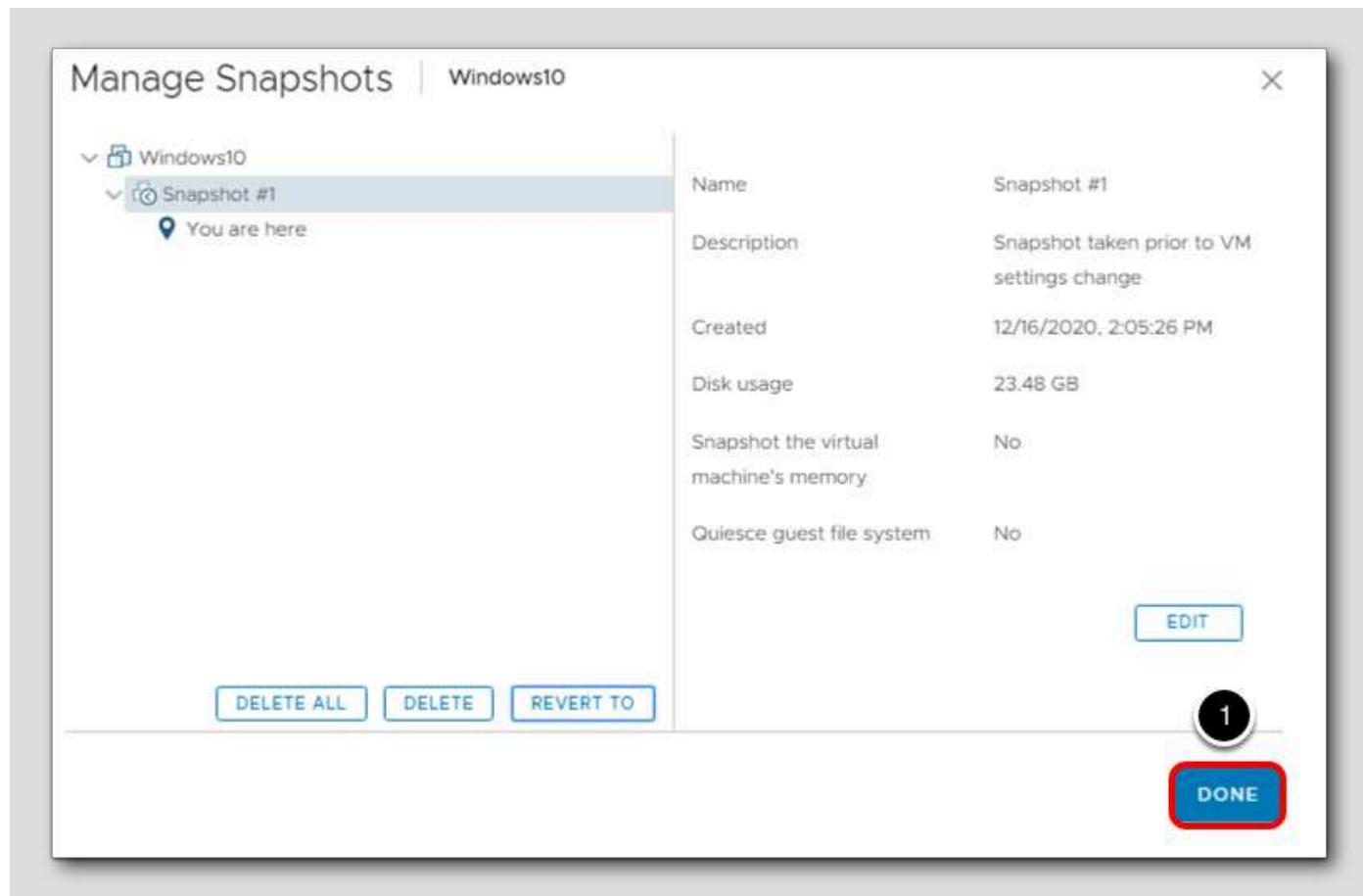
1. Make sure Snapshot #1 is selected.
2. Click the Revert To button.

Confirm Revert to Snapshot



1. Click OK to confirm action.

Close Snapshot Window



1. Click Done to close the Snapshot window.

Monitor task progress

vSphere Client | Menu | Search in all environments

vcsa-01a.corp.local | RegionA01 | Discovered virtual machine | TinyLinux | TinyLinux2 | Windows10

Windows10 | ACTIONS

Summary | Monitor | Configure | Permissions | Data

Powered Off

Guest OS: Microsoft Windows
Compatibility: ESXi 6.5 and later (VMware Tools: Not running, version 0.0.0)
More info
DNS Name: Windows10.corp.local
IP Addresses:
Host: esx-02a.corp.local

Launch Web Console | Launch Remote Console

VM Hardware

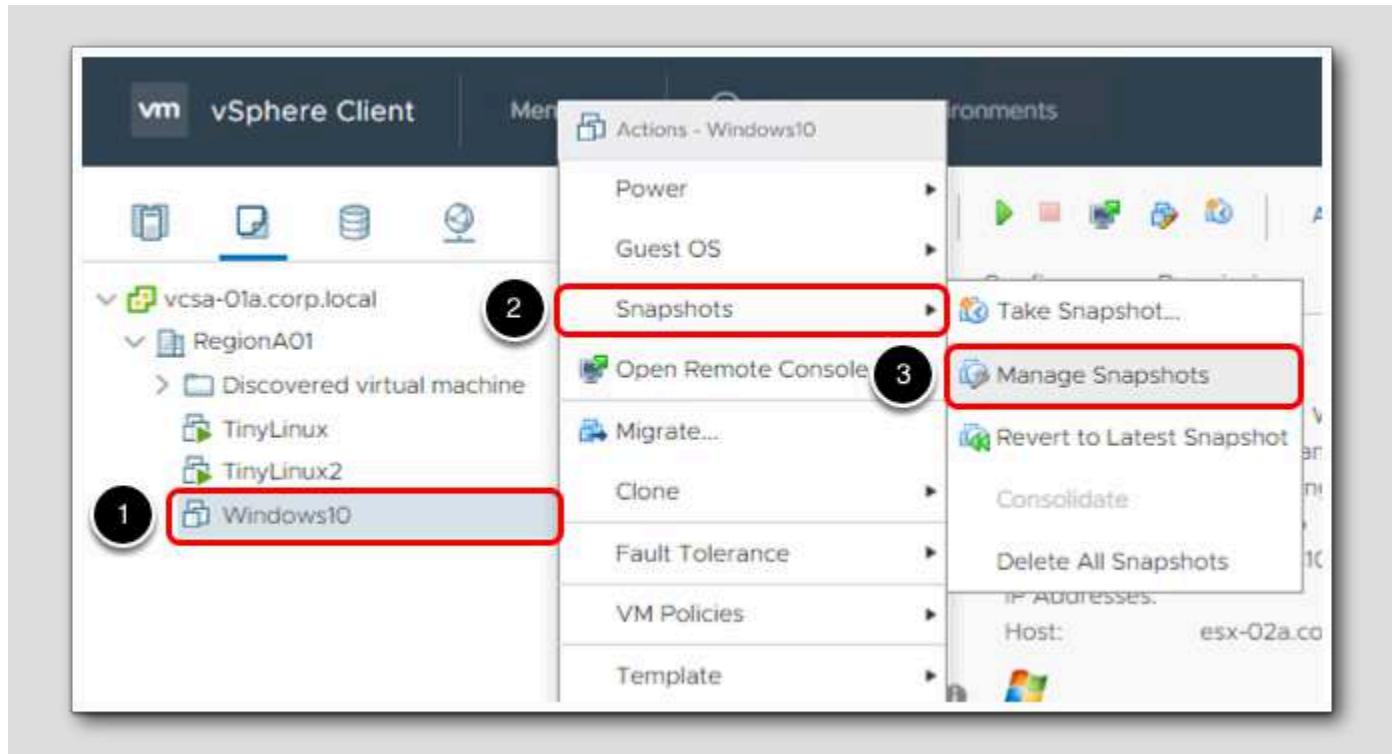
- CPU: 1 CPU(s)
- Memory: 2 GB, 0 GB memory active**
- Hard disk 1: 32 GB
- Hard disk 2: 5 GB

Recent Tasks | Alarms

Task Name	Target	Status	Details	Initiator	Queued
Revert snapshot	Windows10	Completed	Reconfiguring	Virtual Machine on CORP\Administrat...	6 ms

1. Note the progress in the Recent Tasks pane.
2. Note the Memory configuration has reverted back to 2 GB.

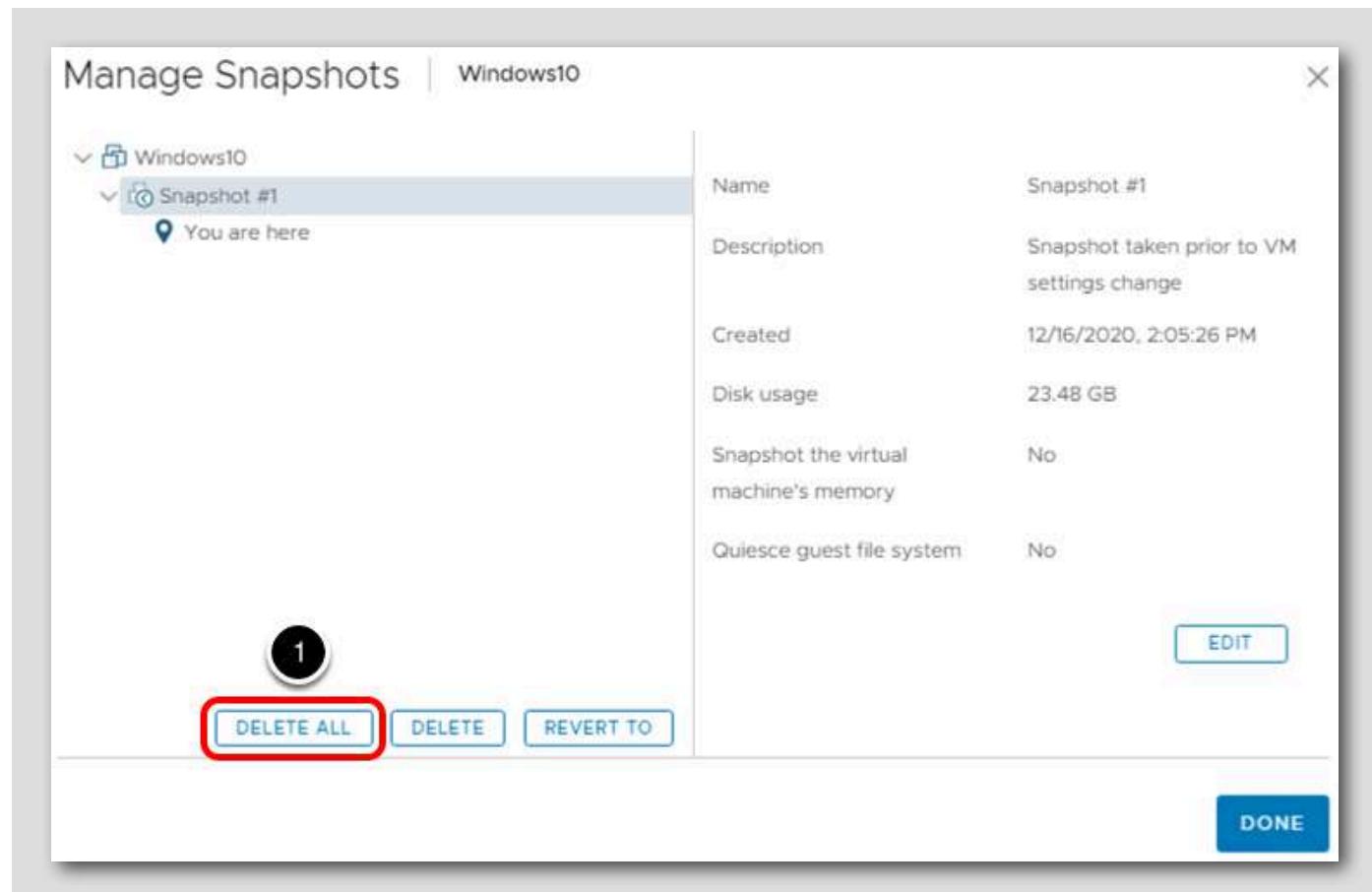
Delete Snapshot #1



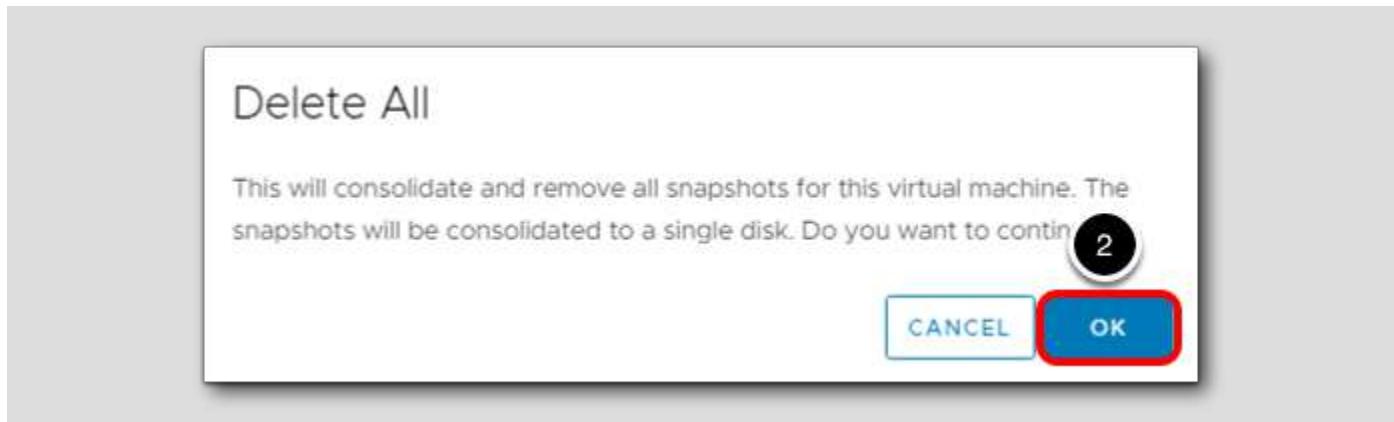
Here you can go and delete the taken snapshot.

1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Select the VM Snapshot to Delete All

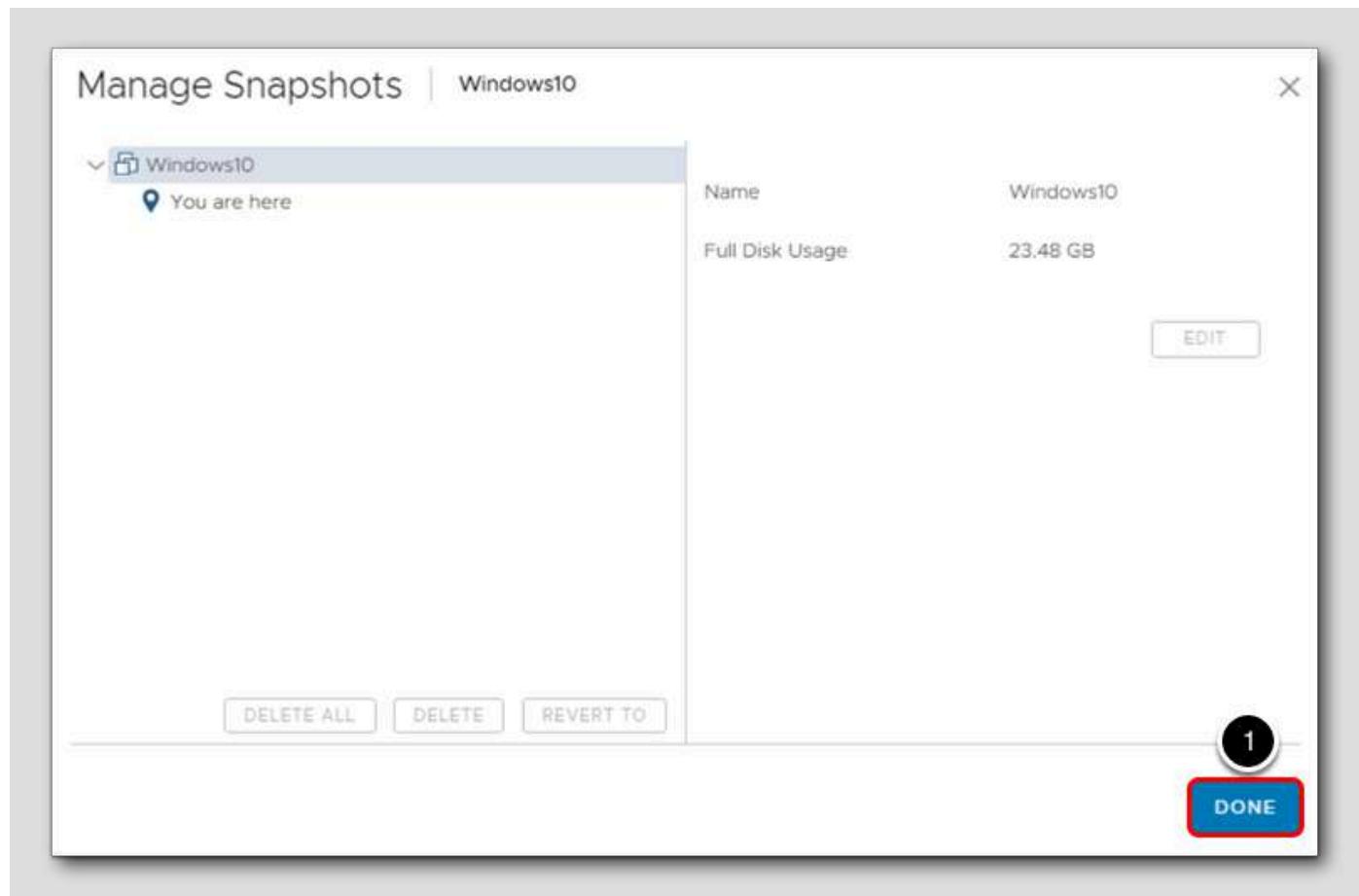


1. Click the **Delete All** button to remove the snapshot.



2. Click OK to confirm the deletion of all the snapshots.

Close Snapshot Window



1. Click Done to exit the manage snapshots window.

It is a best practice to delete virtual machine snapshots when they are no longer needed. Over time the snapshot delta can grow to be quite large which could result in issues consolidating the virtual machine files and lead to performance issues.

Snapshot Removed

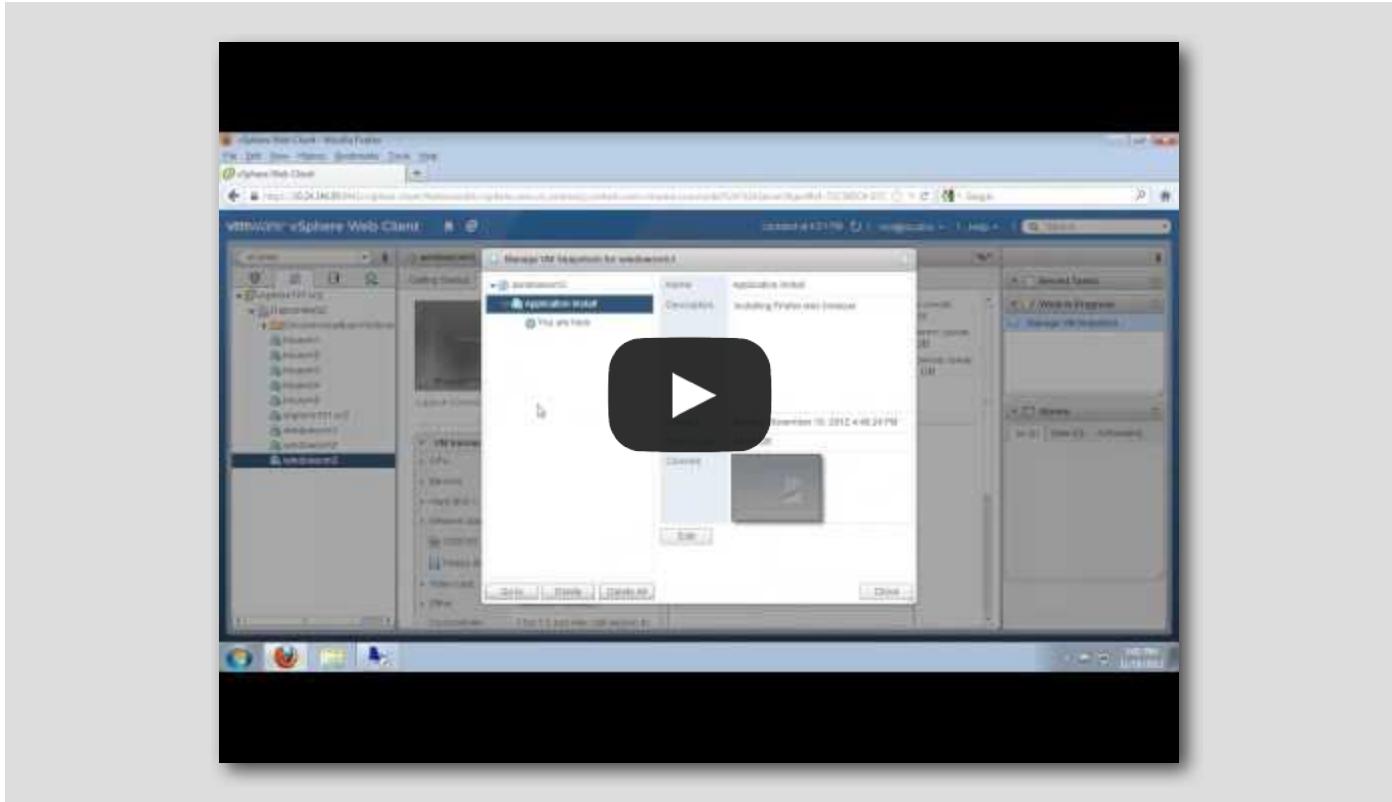
The screenshot shows the vSphere Client interface. On the left, the inventory tree shows a folder named 'RegionA01' containing several virtual machines. A red arrow points from the bottom-left towards the 'Windows10' entry in the tree. The main pane displays the 'Windows10' virtual machine details. The 'Summary' tab is selected, showing the VM is 'Powered Off'. To the right of the summary are various configuration details: Guest OS (Microsoft Windows 10), Compatibility (ESXi 6.5 and later (VM)), VMware Tools (Not running, version:112), DNS Name (Windows10.corp.local), IP Addresses, Host (esx-02a.corp.local), and a 'More info' link. Below the summary are 'Launch Web Console' and 'Launch Remote Console' buttons. The 'VM Hardware' section lists CPU (1 CPU(s)), Memory (2 GB, 0 GB memory active), Hard disk 1 (32 GB), and Hard disk 2 (5 GB). At the bottom, the 'Recent Tasks' table shows a completed task: 'Remove all snapshots' for 'Windows10' target, initiated by 'CORP\Administrat...' and queued for 10 ms.

Task Name	Target	Status	Initiator	Queued For
Remove all snapshots	Windows10	✓ Completed	CORP\Administrat...	10 ms

You can watch the progress of the snapshot being deleted in the Recent Tasks window.

Video: More on Virtual Machine Snapshots (2:33)

<https://www.youtube.com/watch?v=7AVIWifTEMM>



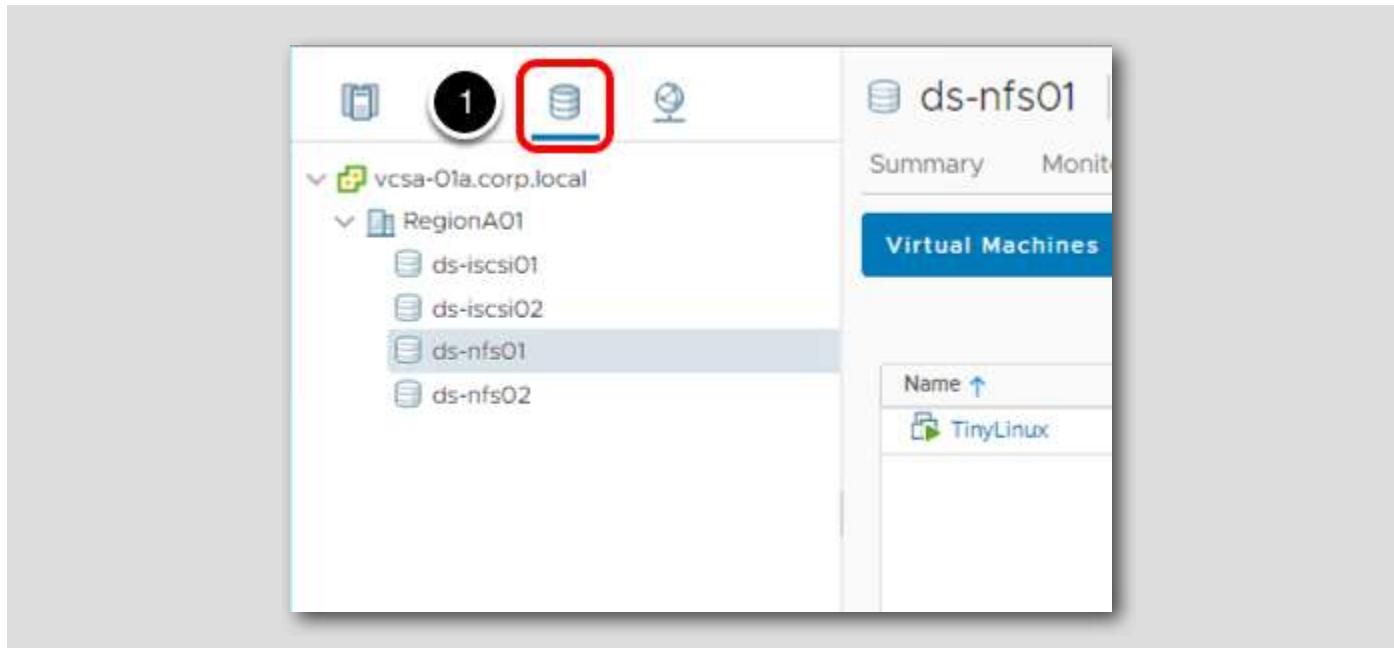
For more information on vSphere Virtual Machine Snapshots, be sure to check out this video.

vSphere Datastore Cluster

A vSphere Datastore Cluster balances I/O and storage capacity across a group of vSphere datastores. Depending on the level of automation desired, Storage Dynamic Resource Scheduler will place and migrate virtual machines in order to balance out datastore utilization across the Datastore Cluster.

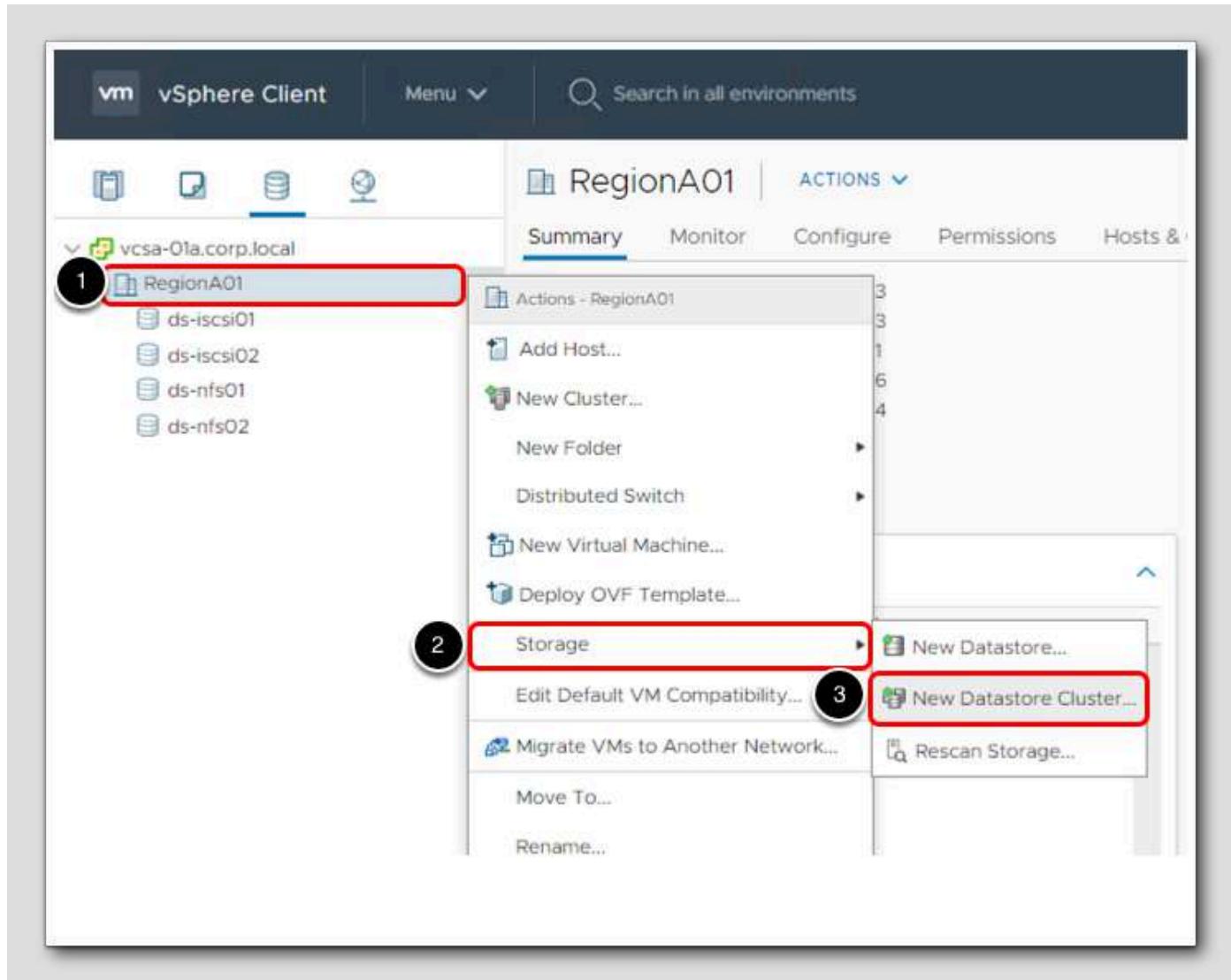
In this section, you will create a vSphere Datastore Cluster using two iSCSI datastores.

Navigate to Storage



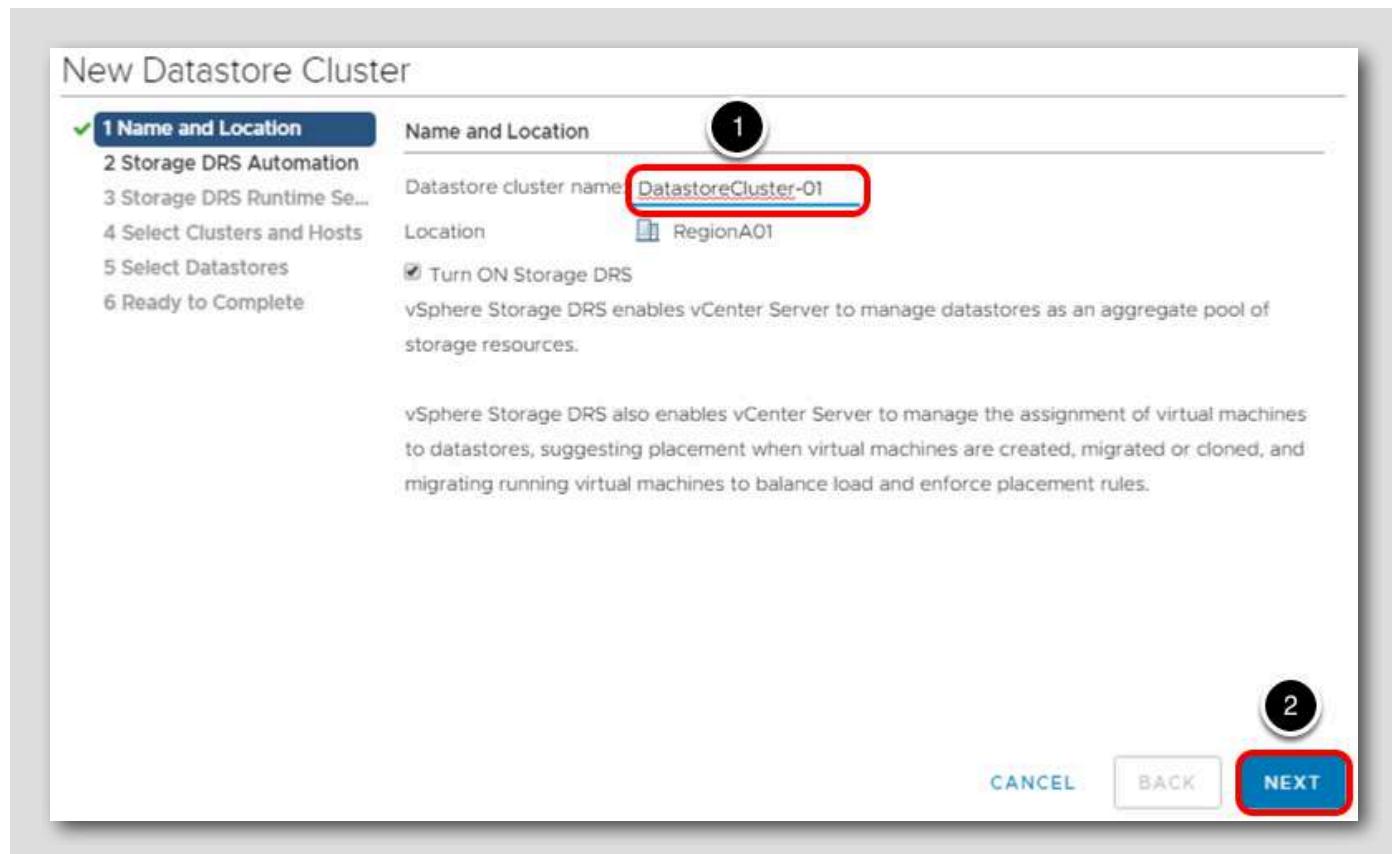
1. Click on the **Storage** icon

New Datastore Cluster



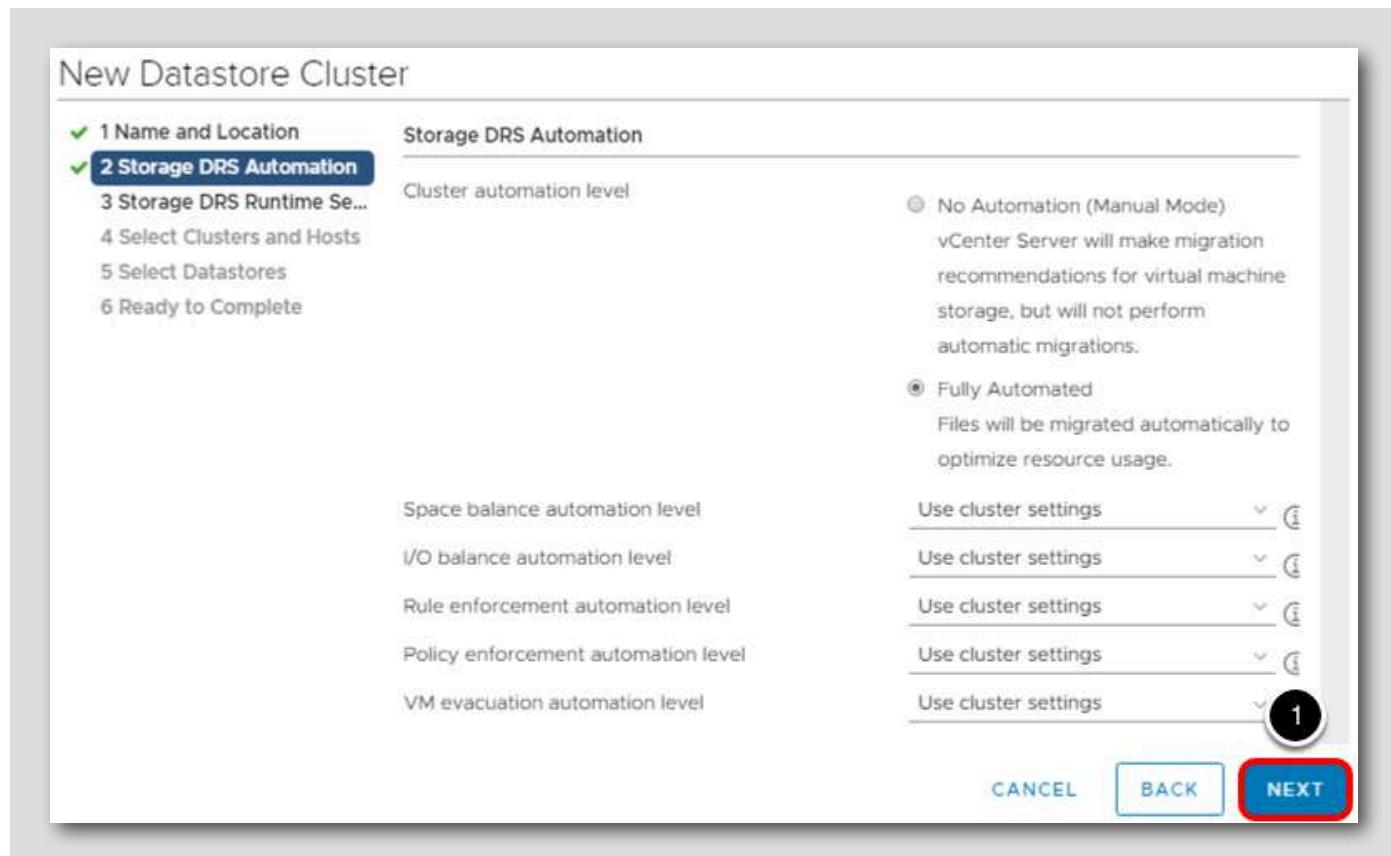
1. Right Click on RegionA01
2. Select Storage
3. Click New Datastore Cluster...

New Datastore Cluster - Name and Location



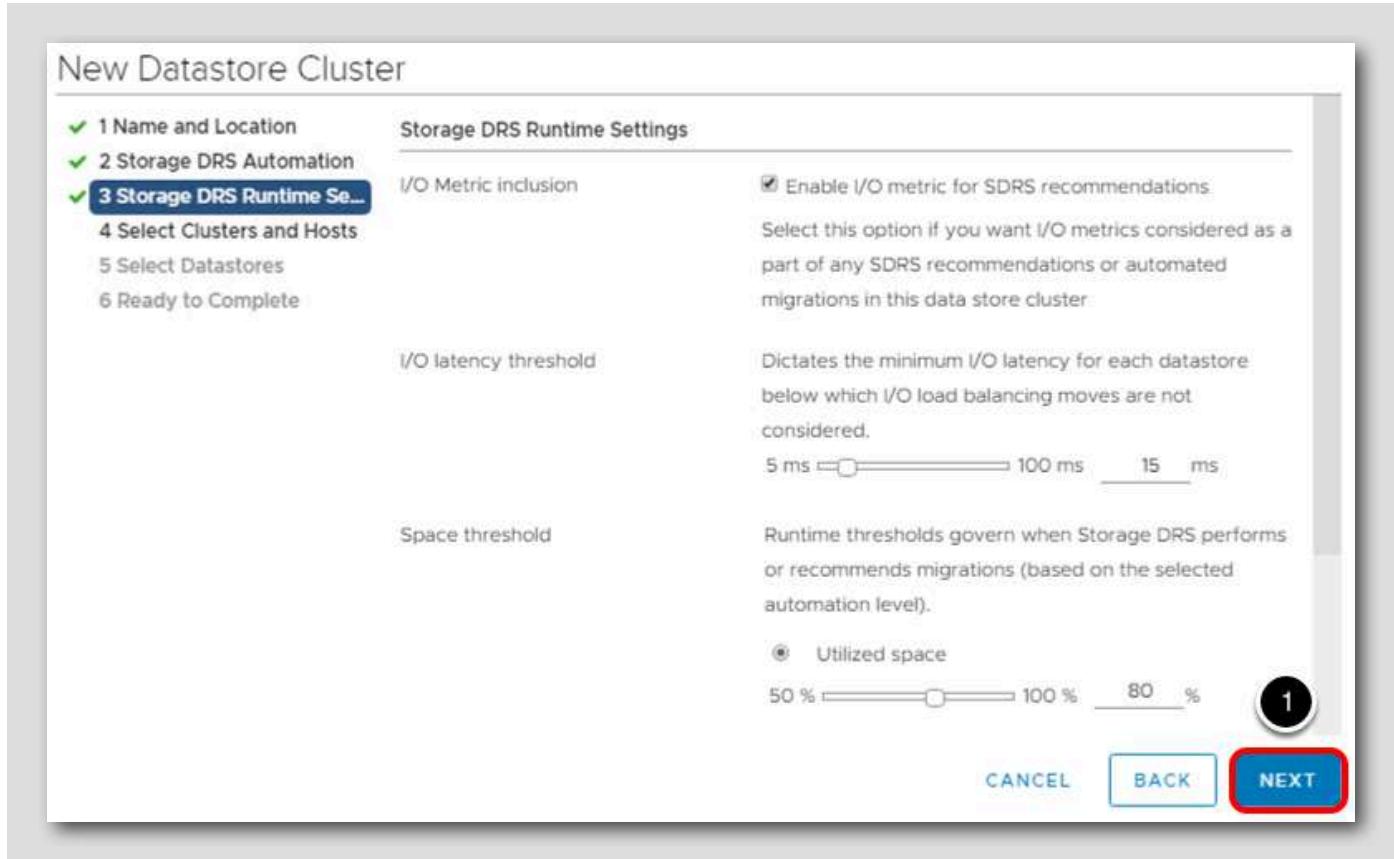
1. Enter DatastoreCluster-01 for the name
2. Select Next

New Datastore Cluster - Storage DRS Automation



1. Leave the defaults settings and select Next

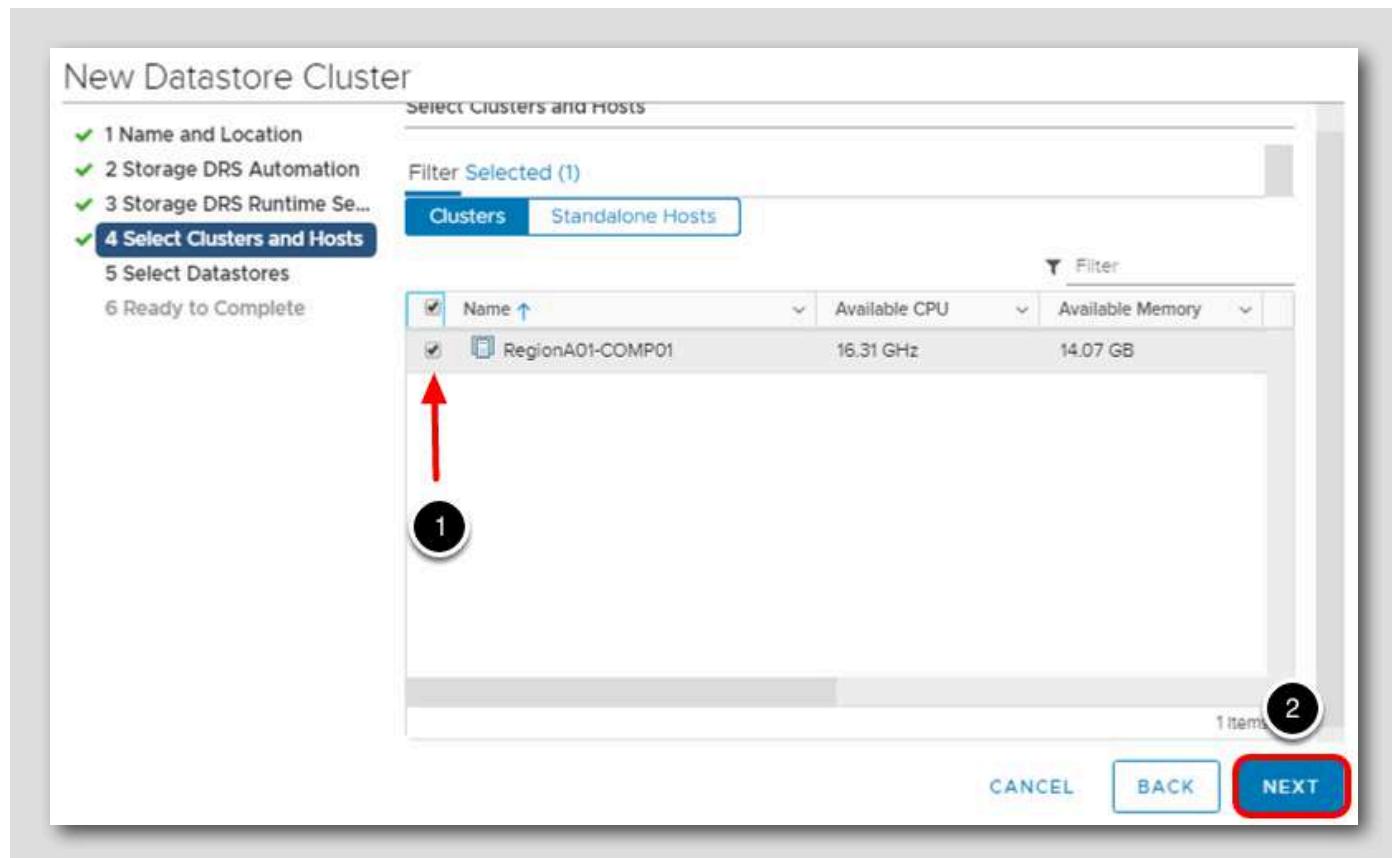
New Datastore Cluster - Storage DRS Runtime Settings



Storage DRS provides multiple options for tuning the sensitivity of storage cluster balancing.

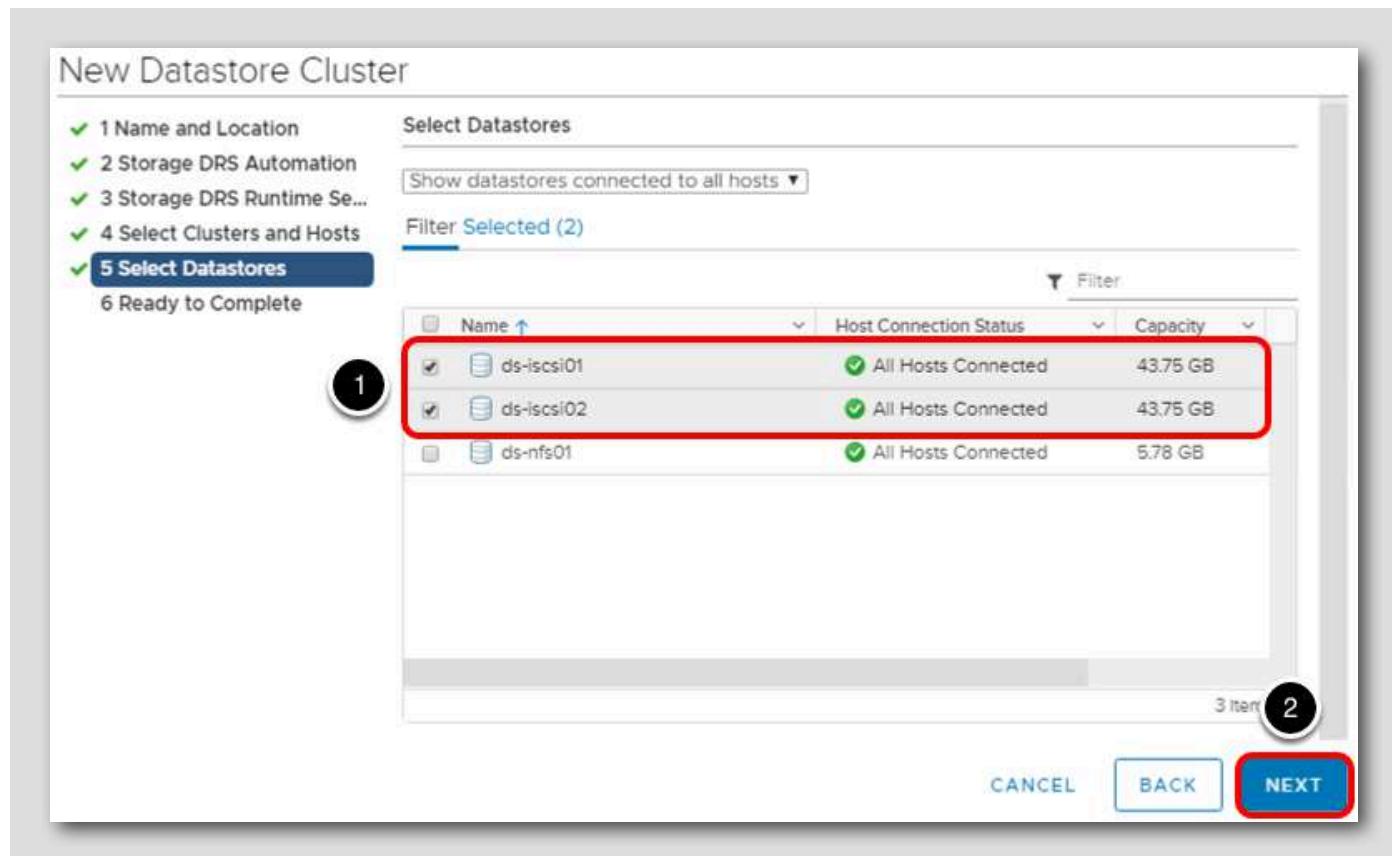
1. Leave the defaults for now and select Next

New Datastore Cluster - Select Clusters and Hosts



1. Because there are no standalone hosts, please select RegionA01-COMP01
2. Click the Next button

New Datastore Cluster - Select Datastores



1. Select the ds-iscsi01 and ds-iscsi02 datastores for the new Datastore Cluster
2. Click **Next**

New Datastore Cluster- Ready to Complete

New Datastore Cluster

Ready to Complete

✓ 1 Name and Location
✓ 2 Storage DRS Automation
✓ 3 Storage DRS Runtime Se...
✓ 4 Select Clusters and Hosts
✓ 5 Select Datastores
6 Ready to Complete

Name and Location
Datastore cluster name: DatastoreCluster-01
Storage DRS: Enabled

Storage DRS Automation
Cluster automation level: Fully Automated
Space balance automation level: Use cluster settings
I/O balance automation level: Use cluster settings
Rule enforcement automation level: Use cluster settings
Policy enforcement automation level: Use cluster settings
VM evacuation automation level: Use cluster settings

Storage DRS Runtime Settings
Storage I/O load balancing: Enabled
Space threshold: 80 % utilized space per datastore
I/O latency threshold: 15 ms

Datastores

Name	Capacity	Free Space	Type
ds-iscsi01	43.75 GB	16.25 GB	VMFS 6
ds-iscsi02	43.75 GB	42.34 GB	VMFS 6

CANCEL BACK FINISH

1

1. Review the Storage DRS settings and click the Finish button

New Datastore Cluster- Summary

The screenshot shows the vSphere Web Client interface for a Datastore Cluster named 'RegionA01'. The 'Summary' tab is selected. In the top right, resource usage is shown: CPU (Used: 415 MHz, Free: 16.8 GHz), Memory (Used: 3.93 GB, Free: 14.07 GB), and Storage (Used: 28.92 GB, Free: 70.14 GB, Capacity: 99.06 GB). Below this are sections for 'Custom Attributes' and 'Tags'. The bottom half of the screen is a table titled 'Recent Tasks' with columns: Task Name, Target, Status, Details, Initiator, Queued For, Start Time, Completion Time, and Server. Three tasks are listed: 'Move datastores into a datastore cluster' (Completed), 'Configure Storage DRS' (Completed), and 'Create a datastore cluster' (Completed). The 'Recent Tasks' table is highlighted with a red border.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Move datastores into a datastore cluster	DatastoreCluster-01	✓ Completed		CORP\Administrat...	6 ms	12/16/2020, 2:52:55 PM	12/16/2020, 2:52:55 PM	vcsa-01a.corp.local
Configure Storage DRS	DatastoreCluster-01	✓ Completed		CORP\Administrat...	29 ms	12/16/2020, 2:52:54 PM	12/16/2020, 2:52:54 PM	vcsa-01a.corp.local
Create a datastore cluster	RegionA01	✓ Completed		CORP\Administrat...	17 ms	12/16/2020, 2:52:53 PM	12/16/2020, 2:52:53 PM	vcsa-01a.corp.local

View the Recent Tasks to check the progress of the operation.

Conclusion

Leveraging vSphere Datastore Clusters in your vSphere environment can help to ensure datastores are filled evenly and I/O is spread out across the group of datastores in the cluster. Storage DRS can automate the initial placement of new virtual machines and adjust virtual machine placement to maintain an even distribution of I/O across the datastore cluster.

Certification Path

Learn and Practice with Hands-On Labs to help prepare for several VMware Certifications.

vmware[®]

CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

This Lab can help you study for the industry-recognized VCAP-DCV Deploy 2021 Deploy certification which validates that you know how to deploy and optimize VMware vSphere infrastructures.

Learn More Here https://via.vmw.com/dcv_deploy

vmware[®]
CERTIFIED

**ADVANCED
PROFESSIONAL**

Data Center
Virtualization Deploy
2021

Conclusion

For More Information....

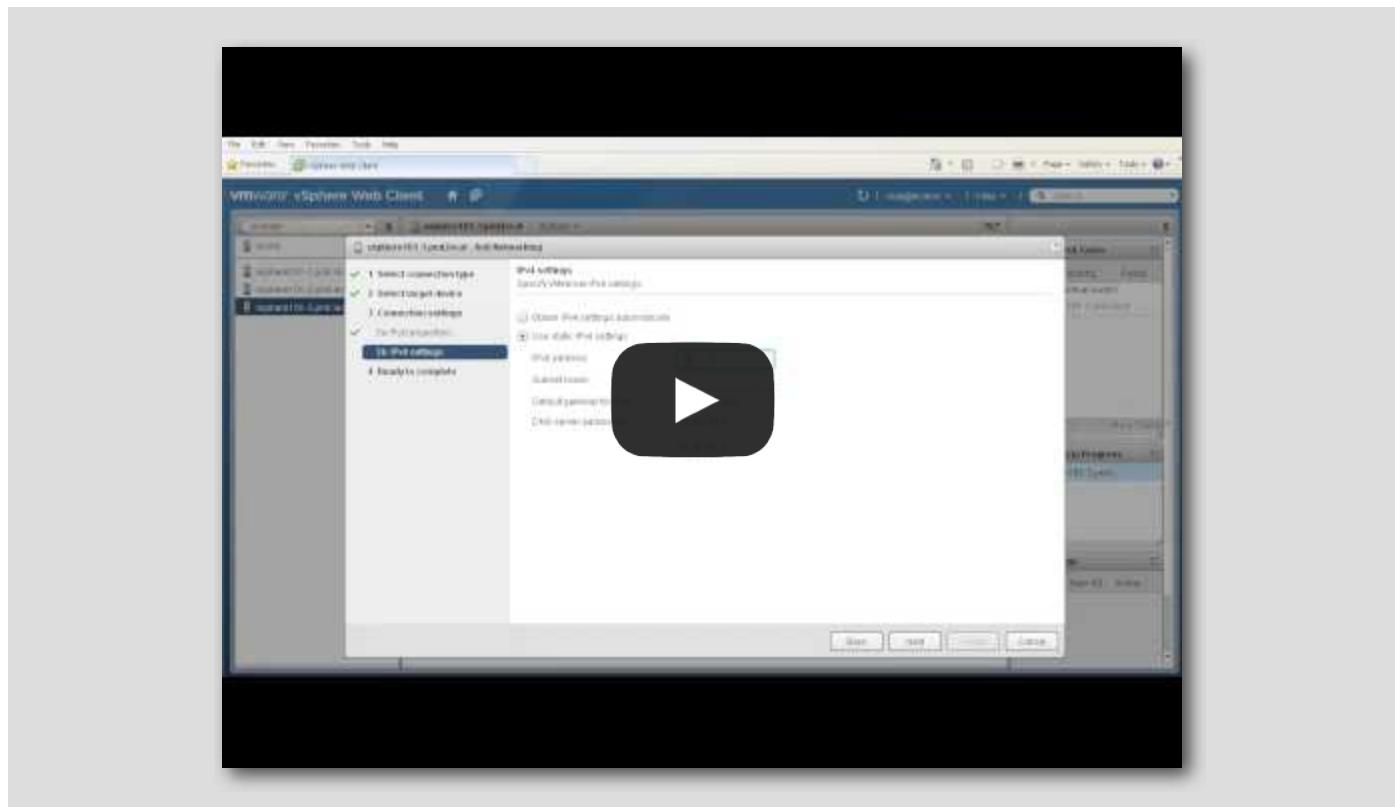
[571]

This section provides supplementary documentation and videos.

Video: How to Configure a vSphere Standard Switch (VSS) (4:22)

[572]

<https://www.youtube.com/watch?v=XpXuhKOc-f4>



This video shows how to use the VMware vSphere web client to configure basic networking for your vSphere hosts using the vSphere Standard Switch (VSS).

vSphere 7 - vCenter Server High Availability

<https://www.youtube.com/watch?v=XkP6QCutw9k>

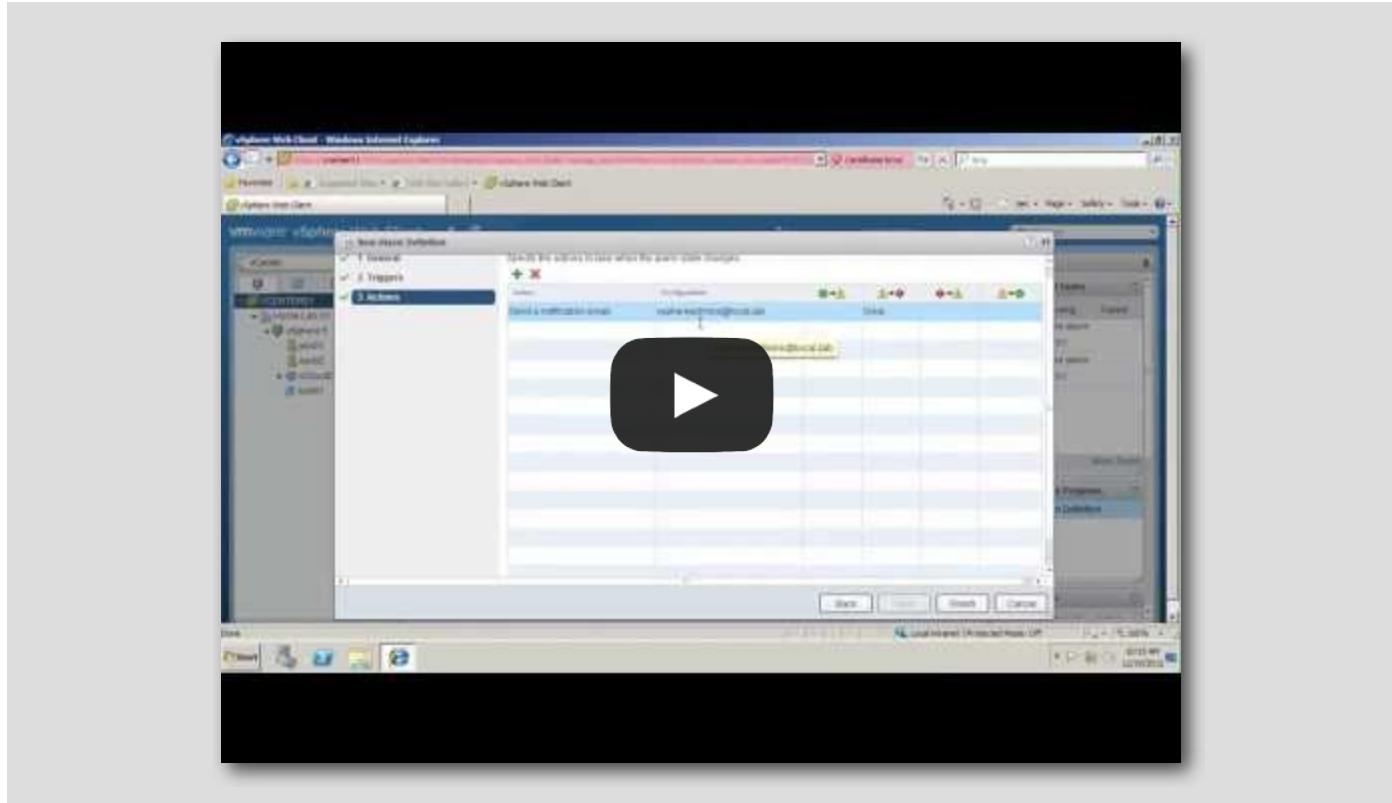


Lightboard illustration of the vCenter Server High Availability options for each deployment type.

Video: Configure Alarms and Notification for VMware vSphere (5:20)

This video shows how to use the VMware vSphere web client to configure vCenter Server alarms and alerts and how to enable email notification.

<https://www.youtube.com/watch?v=8vWNVBDPcu4>

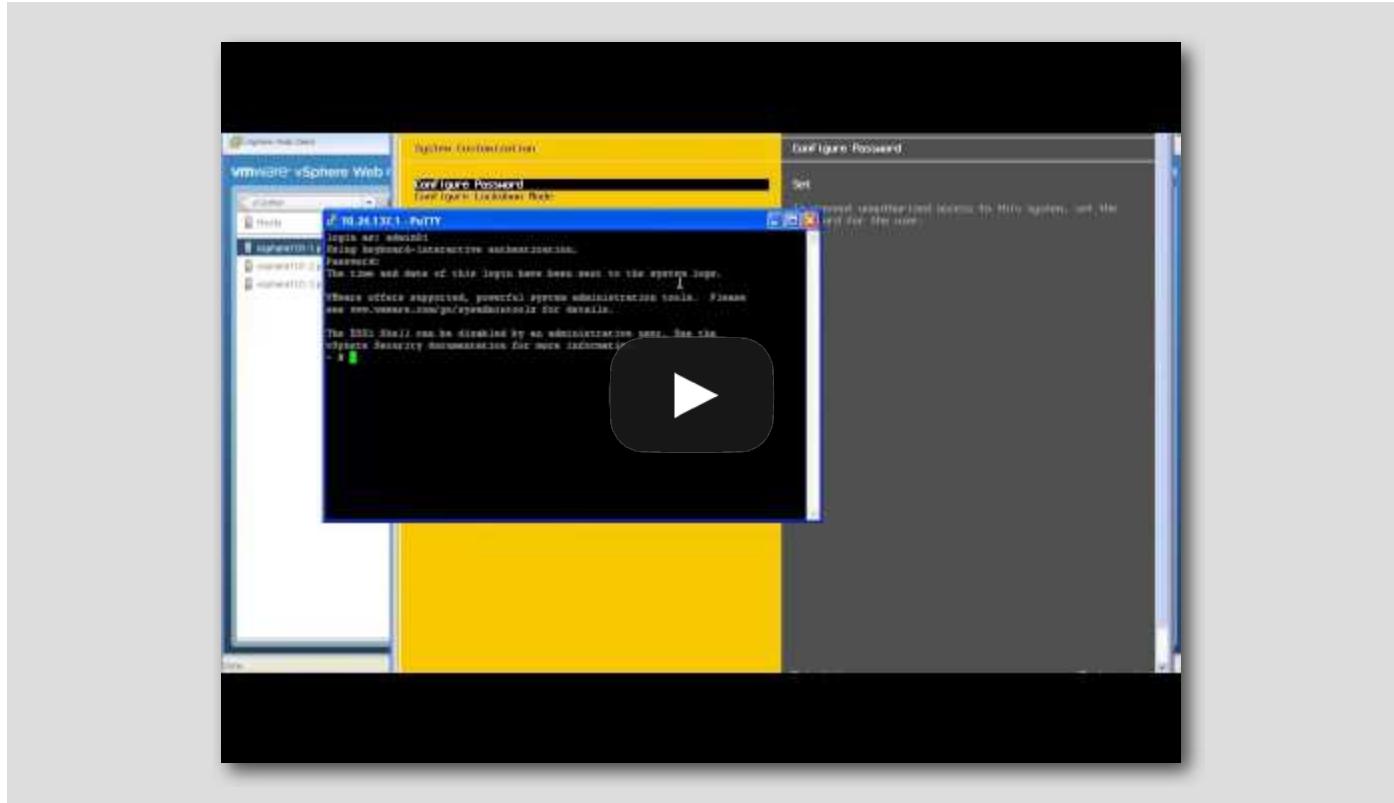


Video: Enable vSphere Host Lockdown Mode for VMware vSphere (4:48)

[575]

This video shows how to secure VMware vSphere hosts with Lockdown Mode in order to limit direct access to the host console and to require administrators manage hosts through vCenter Server.

<https://www.youtube.com/watch?v=gWlb2HHu3bE>

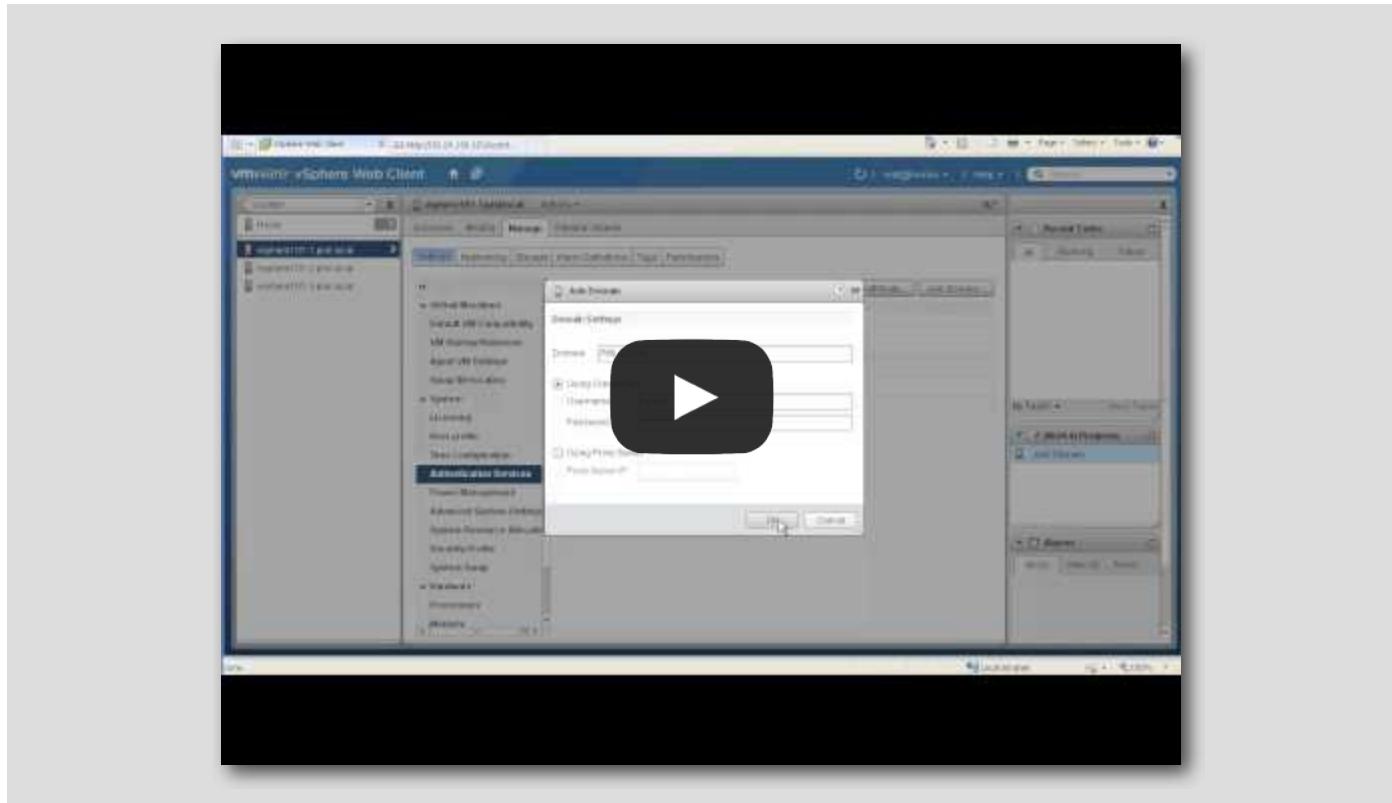


(Optional) Video: Add VMware vSphere Hosts to Active Directory (3:40)

[576]

This video shows how to join a VMware vSphere host to a Microsoft Active Directory (AD) domain in order to allow administrators to use their Active Directory credentials to access and manage hosts.

https://www.youtube.com/watch?v=H74M_Eshtw

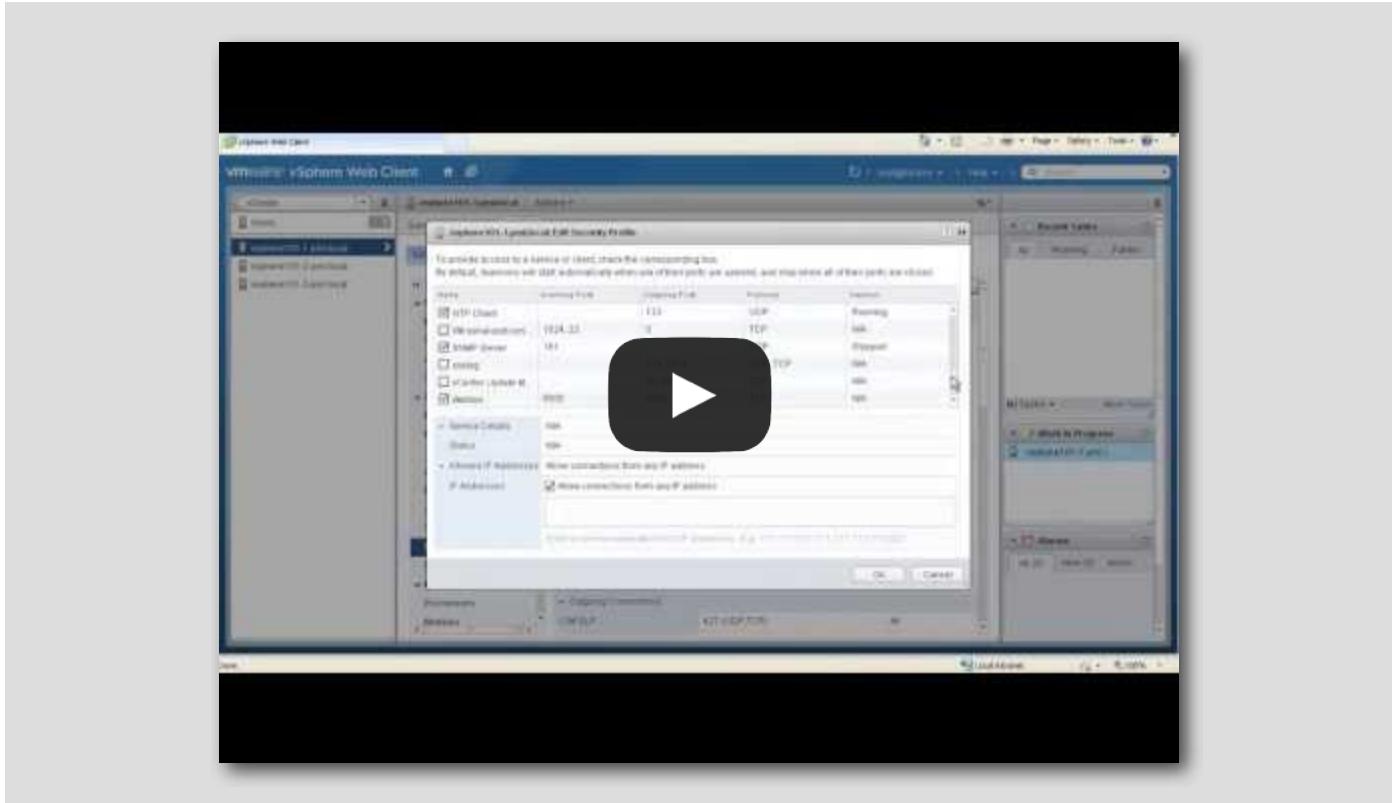


Video: Configure vSphere Host Firewall for VMware vSphere (4:34)

[577]

This video shows how to use the VMware ESXi Firewall on the vSphere host to block incoming and outgoing communication and to manage the services running on the host.

<https://www.youtube.com/watch?v=bzjsjQdnTuk>



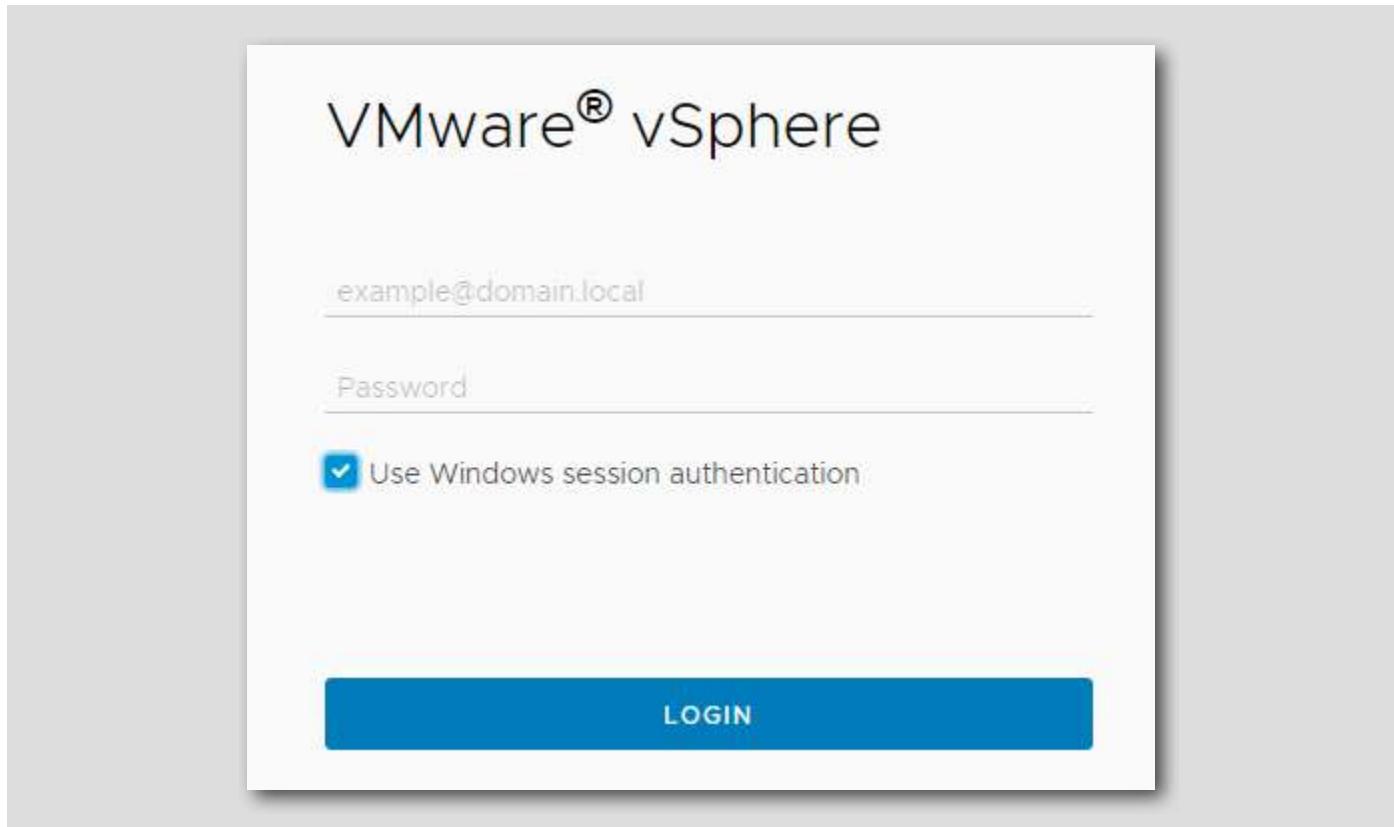
REFERENCE - Unlock vCenter Single Sign On Users in the vSphere Web Client

[578]

A vCenter Single Sign On user account might be locked when a user exceeds the allowed number of failed login attempts. After a user account is locked, the user cannot log in to the Single Sign On system until the account is unlocked, either manually or after a certain amount of time has elapsed.

You specify the conditions under which a user account is locked in the Single Sign On Lockout Policy. Locked user accounts appear on the Users and Groups administration page. Users with appropriate privileges can manually unlock Single Sign On user accounts before the specified amount of time has elapsed. You must be a member of the Single Sign On Administrators group to unlock a Single Sign On user.

Locked Out User



By default, after three failed login attempts, the Users' account is locked.

In the lab, this policy has been disabled in order to prevent login issues that frequently occur with non-US keyboards.

This section has been included for reference purposes only.

Unlocking a User

The screenshot shows the vSphere Client interface under the 'Administration' menu. The 'Users and Groups' option is selected (step 1). On the right, the 'Users' tab is active, displaying a list of users. The 'Locked' column header is highlighted with a red box (step 2). The 'sshd' user account is selected, indicated by a red box and a numbered callout (step 3). The table data is as follows:

	Username	First Name	Last Name	Email	Description	Locked
⋮	sshd	PrivSep				No
⋮	vstatsuser	vstatsuser				No
⋮	eam	eam				No
⋮	root	root				No
⋮	vdtc	VMware	vSphere Distributed Tracing Collector User			No

Login to the vSphere Web Client as a user with SSO Admin privileges and navigate Menu --> Administration.

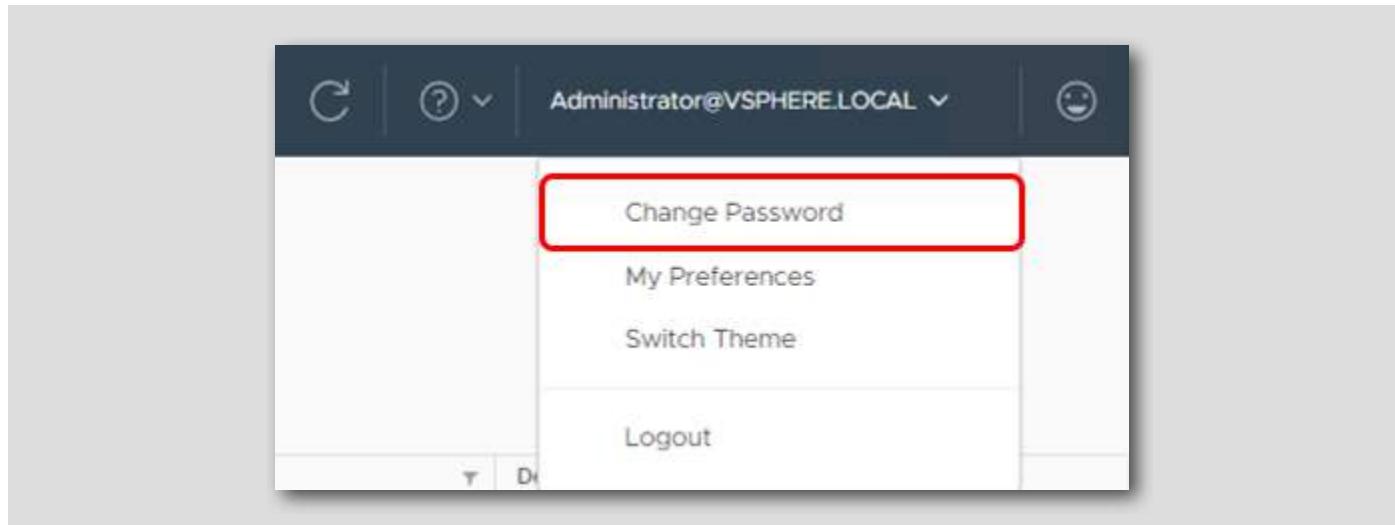
1. Click on Users and Groups
2. Locate the locked user account -- it will show as "Yes" in the "Locked" column if the user is locked
3. Click the tree dots on the left and select the unlock option

Log out of the Web Client.

Change Your Password in the vSphere Web Client

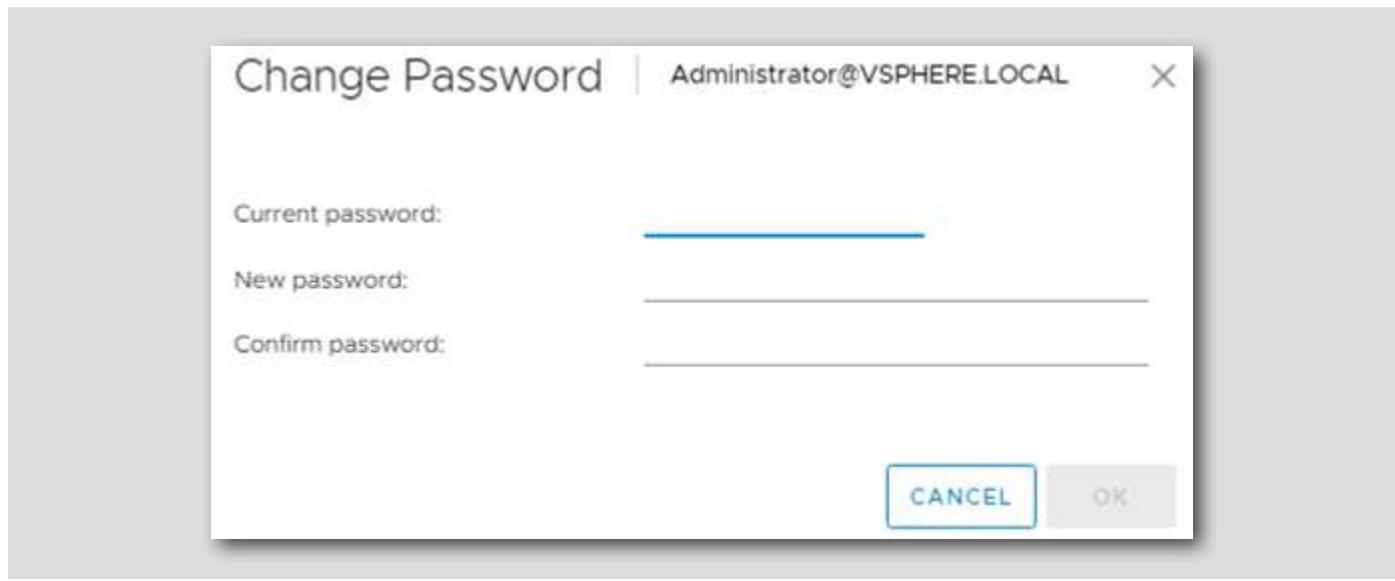
Depending on your vCenter Single Sign On privileges, you might not be able to view or edit your Single Sign On user profile. However, all users can change their Single Sign On passwords in the vSphere Web Client. The password policy defined in the vCenter Single Sign-On configuration tool determines when your password expires. By default, Single Sign-On passwords expire after 90 days in vSphere 6, but your system administrator might change this depending on the policy of your organization. If you choose to keep the defaults, remember to change the password for the administrator@vsphere.local account password every 90 days or it will lock out on day 91.

Change Password



In the upper navigation pane, click your user name to pull down the menu.

Change Password Dialog



Select Change Password and type your current password.

Enter a new password.

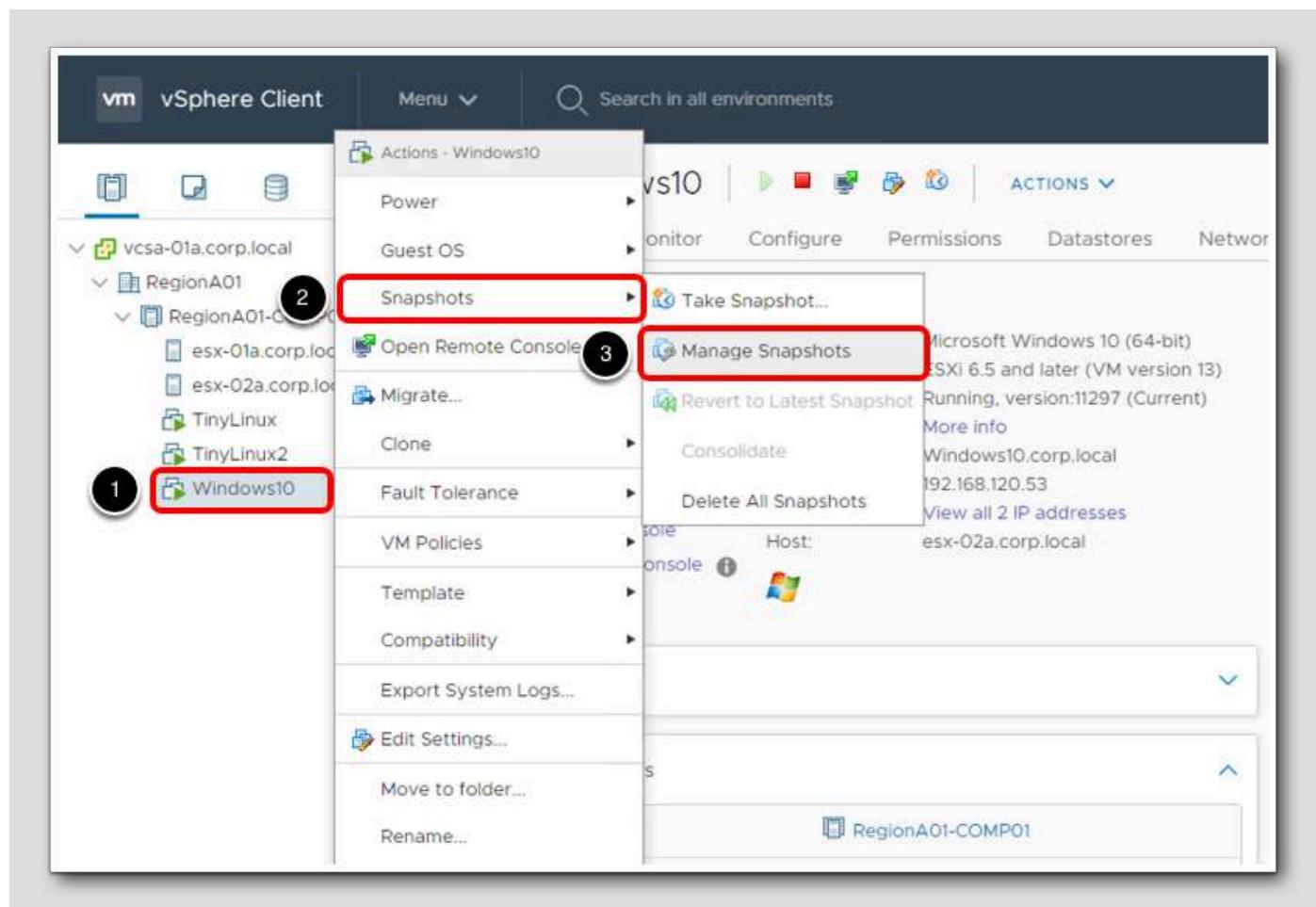
Type a new password and confirm it.

Click the OK button to make the change.

NOTE: If you do change the password, please make sure to remember it for other activities in the lab.

Snapshot Manager

[584]



In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

1. Right-click Windows10
2. Select Snapshots
3. Click Manage Snapshots

What is vSphere Storage DRS? (5:08)

[585]

<https://www.youtube.com/watch?v=z77xmaxoNec>



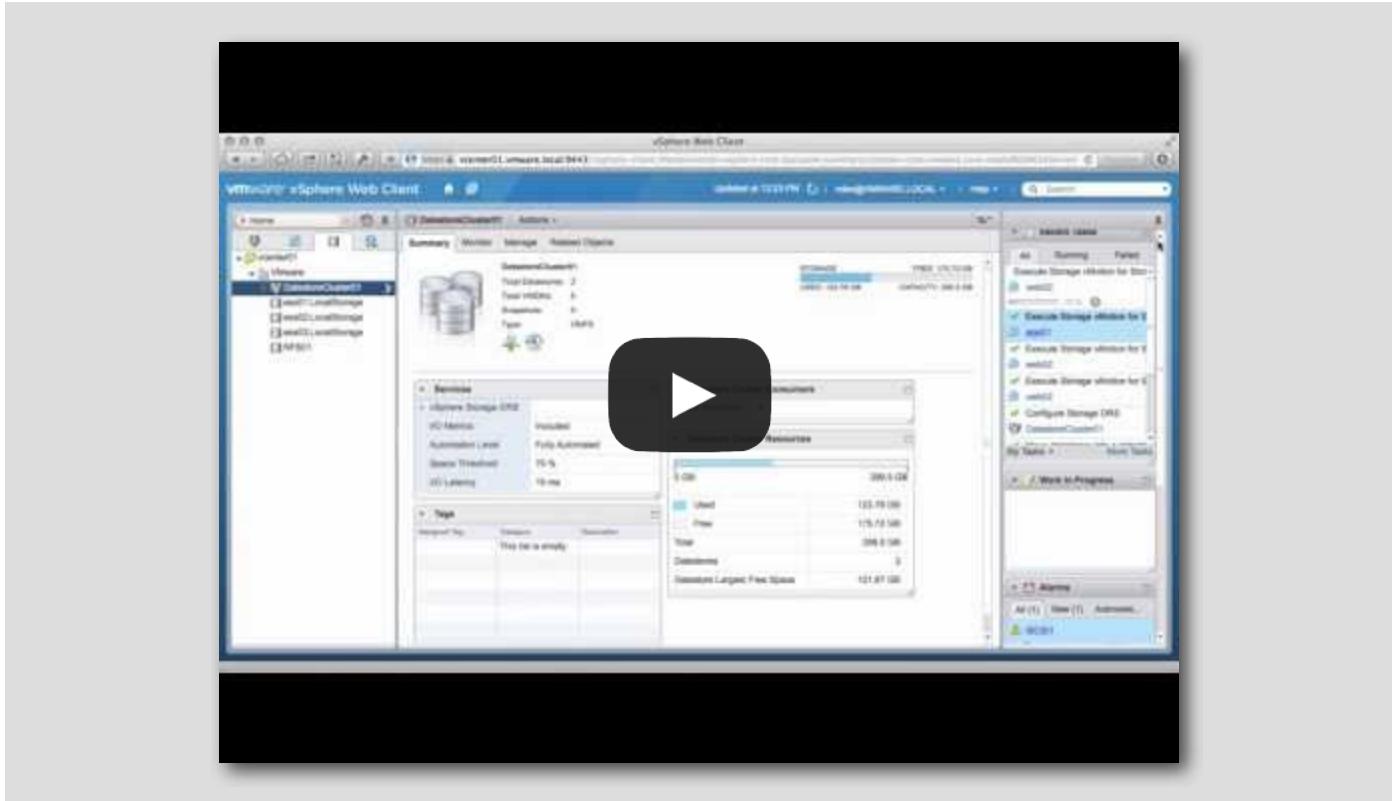
This animated video shows how VMware Storage DRS reduces the time and complexity of provisioning virtual machines by aggregating data stores into a single pool, called a datastore cluster, enabling rapid placement of virtual machines and virtual machine disks.

Creating a Datastore Cluster with Storage DRS (3:23)

[586]

This video reviews the process of creating and managing a datastore cluster in a vSphere environment.

<https://www.youtube.com/watch?v=gATLj6pUxnk>



Appendix

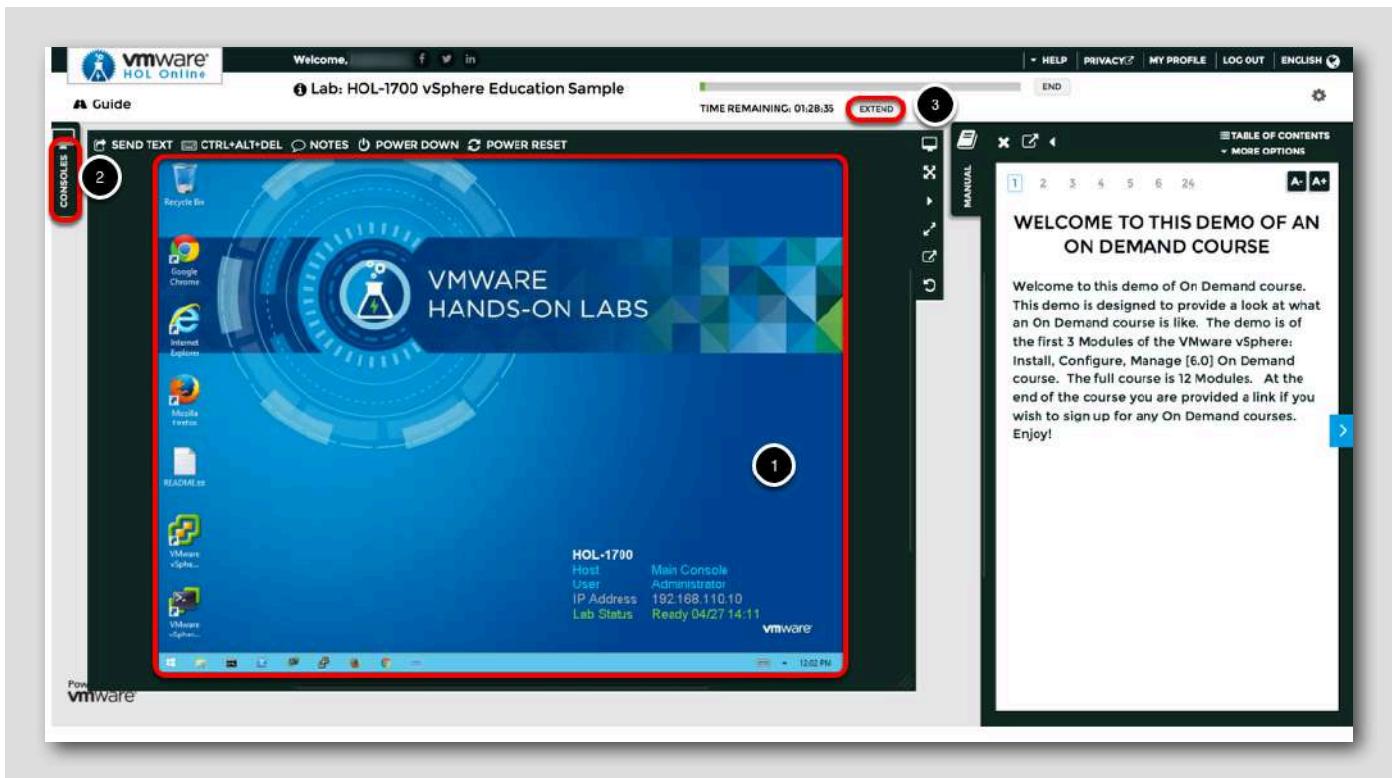
Hands-on Labs Interface

[588]

Welcome to Hands-on Labs! This overview of the interface and features will help you to get started quickly. Click next in the manual to explore the Main Console or use the Table of Contents to return to the Lab Overview page or another module.

Location of the Main Console

[589]



1. The area in the large RED box contains the Main Console. The Lab Manual is on the tab to the right of the Main Console.
2. Some labs have additional consoles found on separate tabs in the upper left. The lab manual will direct you to open another specific console if necessary.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. Your lab will end when the timer expires. Click the EXTEND button to increase the time allowed. If you are at a VMware event, you can extend your lab time twice up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

In this lab you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

<https://www.youtube.com/watch?v=xS07n6GzGuo>



You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

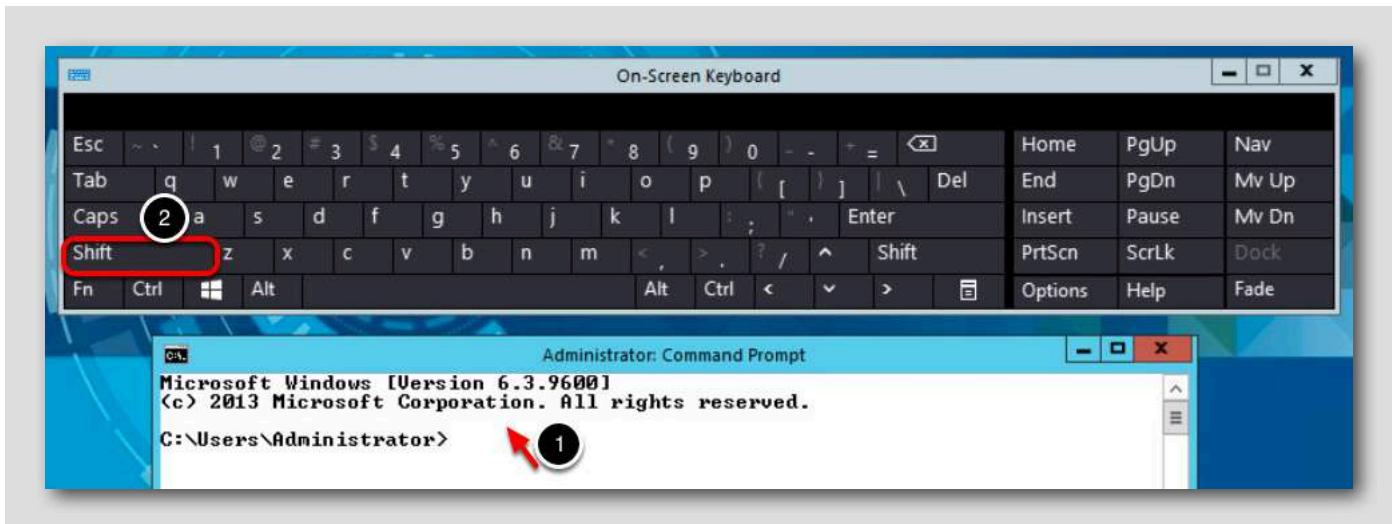


You can also use the Online International Keyboard found in the Main Console.

1. Click on the keyboard icon found on the Windows Quick Launch Task Bar.

Click once in active console window

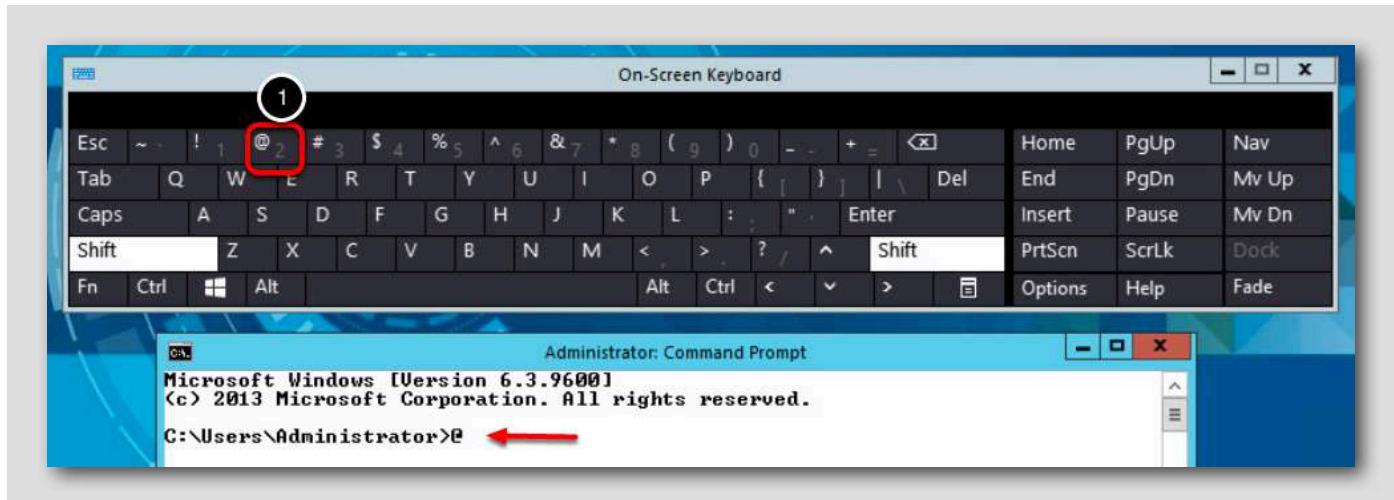
[593]



In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key



1. Click on the "@" key.

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark



When you first start your lab you may notice a watermark on the desktop indicating that Windows is not activated.

A major benefit of virtualization allows virtual machines to be moved and run on any platform. Hands-on Labs utilizes this benefit and hosts labs from multiple datacenters. However, these datacenters may not have identical processors which triggers a Microsoft activation check through the Internet.

Rest assured VMware and Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet. Without this, the Microsoft activation process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Return to Lab Guidance

[596]

Use the Table of Contents to return to the Lab Overview page or another module.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.
Copyright © 2021 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Lab SKU: HOL-2210-01-SDC Version: 2021122-183745