

Table of Contents

Lab Overview - HOL-2010-01-SDC - Virtualization 101: Introduction to vSphere	2
Virtualization	3
Lab Guidance	14
Module 1 - Introduction to Management with vCenter Server (60 Min).....	20
Introduction.....	21
Hands-on Labs Interactive Simulation: ESXi Installation and Configuration	22
ESXi Host Client	23
vCenter 6 Overview	31
vCenter Server and Creating a Virtual Machine	37
Cloning Virtual Machines and Using Templates	70
Using Tagging and Search to Find Objects Quickly	84
Understanding vSphere Availability and Distributed Resource Scheduler (DRS)....	98
vSphere 6 Fault Tolerance Provides Continuous Availability	115
Monitoring Events and Creating Alarms	118
Configure Shares and Resources.....	140
Migrating Virtual Machines with VMware vMotion	147
vSphere Monitoring and Performance	158
Introduction to vSphere Platinum.....	173
Module 2 - Introduction to vSphere Networking and Security (60 Min).....	176
Introduction.....	177
Adding and Configuring vSphere Standard Switch	181
Working with the vSphere Distributed Switch	214
Using Host Lockdown Mode	258
User Access and Authentication Roles	282
Understanding Single Sign On	297
Adding an ESXi Host to Active Directory	317
Module 3 - Introduction to vSphere Storage (60 Min)	325
vSphere Storage Overview.....	326
Creating and Configuring vSphere Datastores	330
Storage vMotion	371
Managing Virtual Machine Disks	380
Working with Virtual Machine Snapshots	391
vSphere Datastore Cluster	407

Lab Overview - HOL-2010-01-SDC - Virtualization 101: Introduction to vSphere

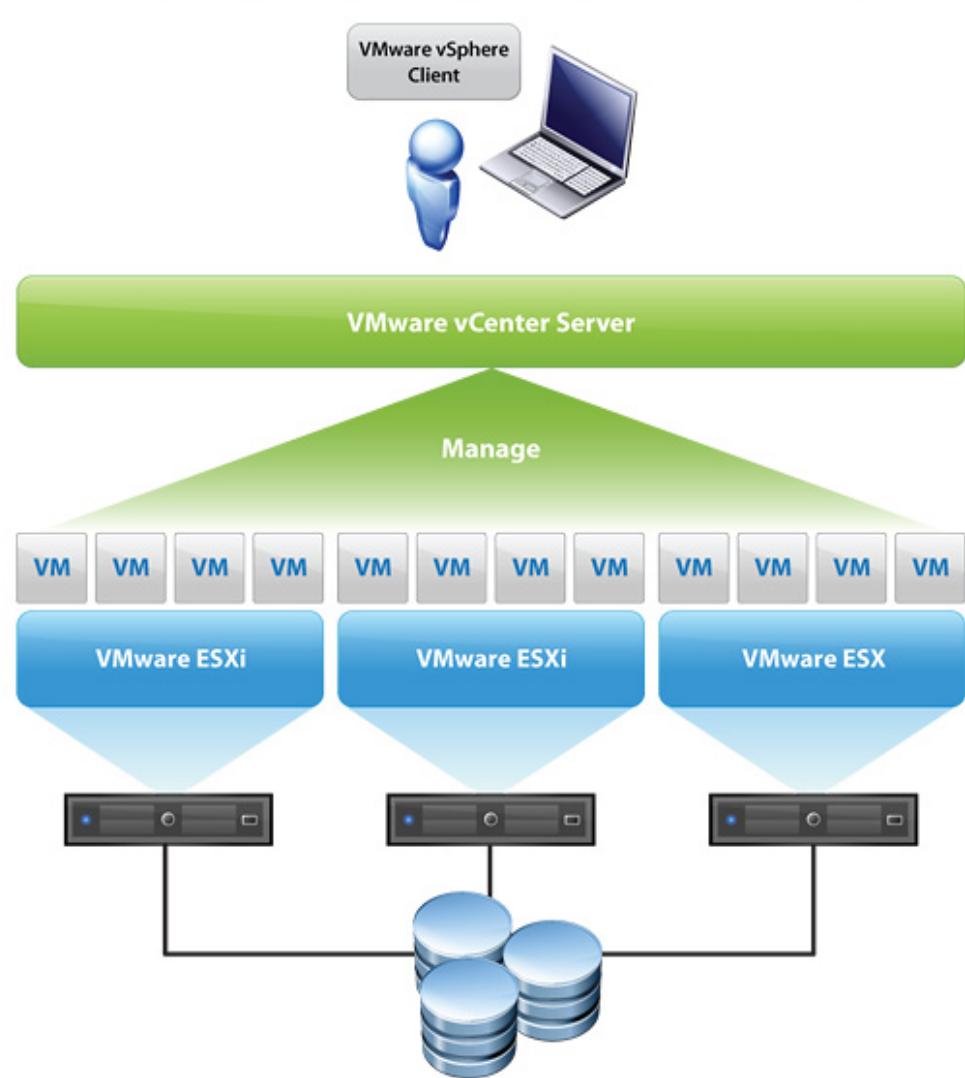
Virtualization

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 the [Lab Guidance](#) section.

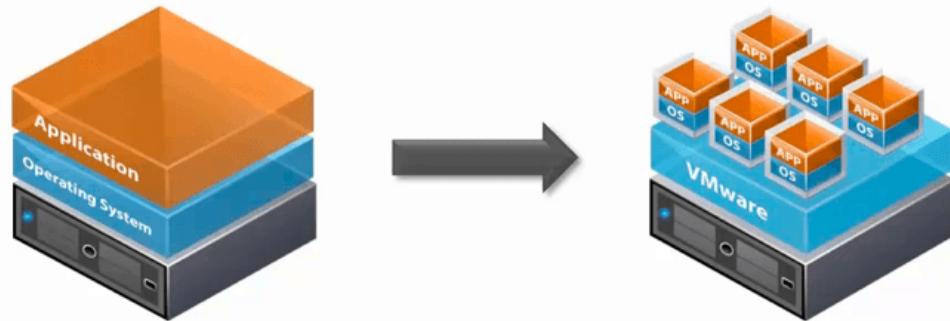
What is Virtualization:

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 Defined



Traditional Architecture

- Single operating system
- Single application

Virtual Architecture

- Virtualize many VMs using VMware Hypervisor

vmware

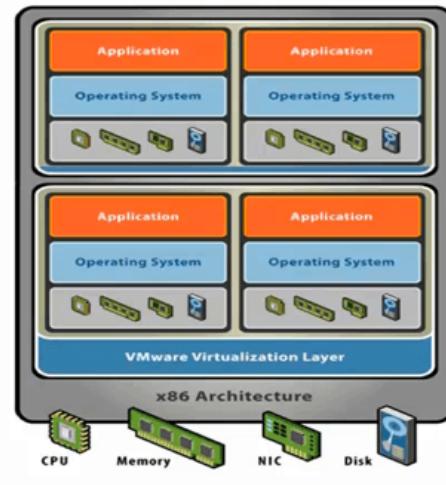
Virtualization is placing an additional layer of software called a hypervisor on top of your physical server. The hypervisor enables you to install multiple operating systems and applications on a single server.

Separation

Virtualization Defined

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

vmware®

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

Isolation

Key Properties of Virtual Machines: Continued



Isolation

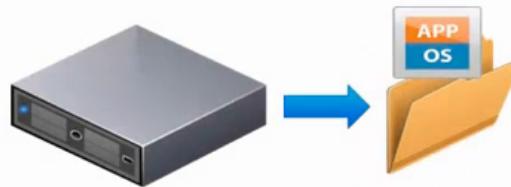
- Fault and security isolation at the hardware level
- Advanced resource controls preserve performance



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

Key Properties of Virtual Machines: Continued



Encapsulation

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

vmware

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

Hardware Independence

Key Properties of Virtual Machines: Continued



Hardware Independence

- Provision or migrate any virtual machine to any similar or different physical server

vmware®

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

Benefits

How Do I Get Those 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

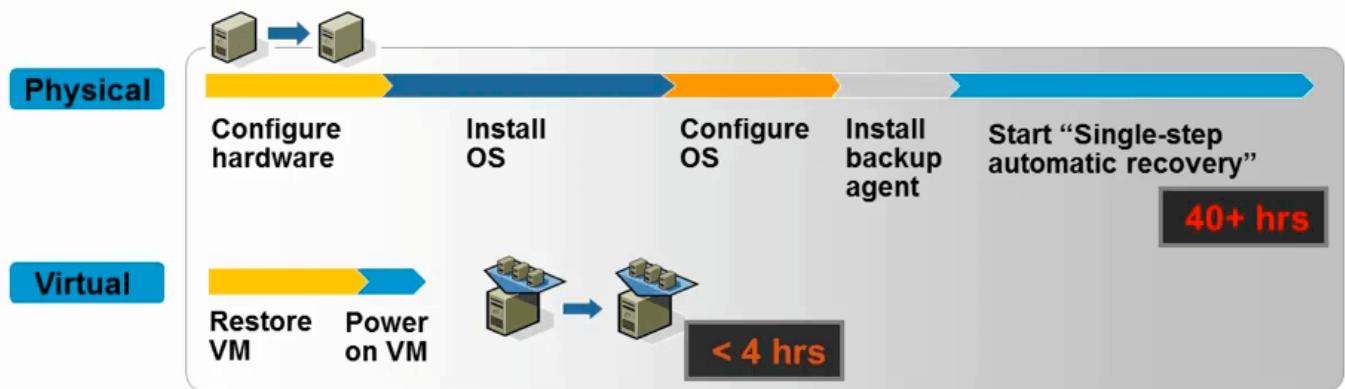
...there are many more benefits of virtualization

The VMware logo, consisting of the word "vmware" in a white, lowercase, sans-serif font, with a small registered trademark symbol (®) to the right.

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

Simplify Recovery

Save Time During Disaster Recovery



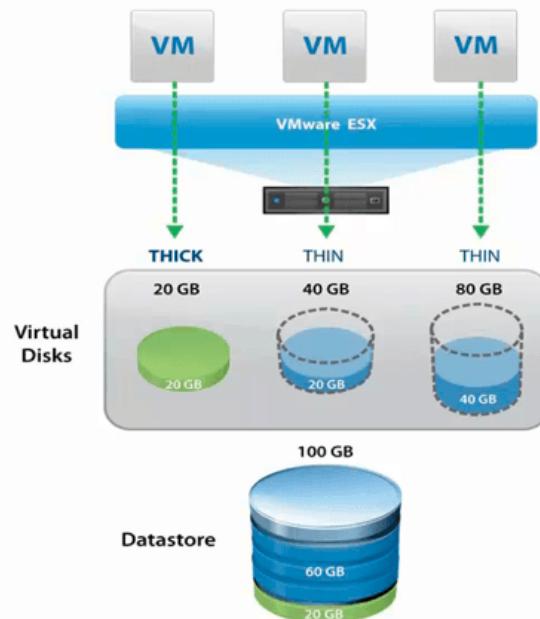
- Eliminate recovery steps
- Standardize recovery process

vmware

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

vmware®

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

The CapEx Story: Better use of existing infrastructure

Before VMware



More applications per machine = less machines

After VMware



Servers	10
Utilization	8%
Annual cost per server	\$4,000
Total Cost	\$40,000

Servers	3
Utilization	80%
Annual cost per server	\$4,000
Total Cost	\$12,000

\$28,000 in cost avoidance

Source: IT Business Edge, "The Business Value of Server Virtualization" – cost for average a 2 x CPU server in three-year amortized hardware purchase, and annual support and maintenance contract costs 9/07

vmware

Lab Guidance

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.

- [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, Dave Rollins, A.J. Ciampa

A copy of this manual can be downloaded in PDF format:

http://docs.hol.vmware.com/HOL-2020/hol-2010-01-sdc_pdf_en.pdf

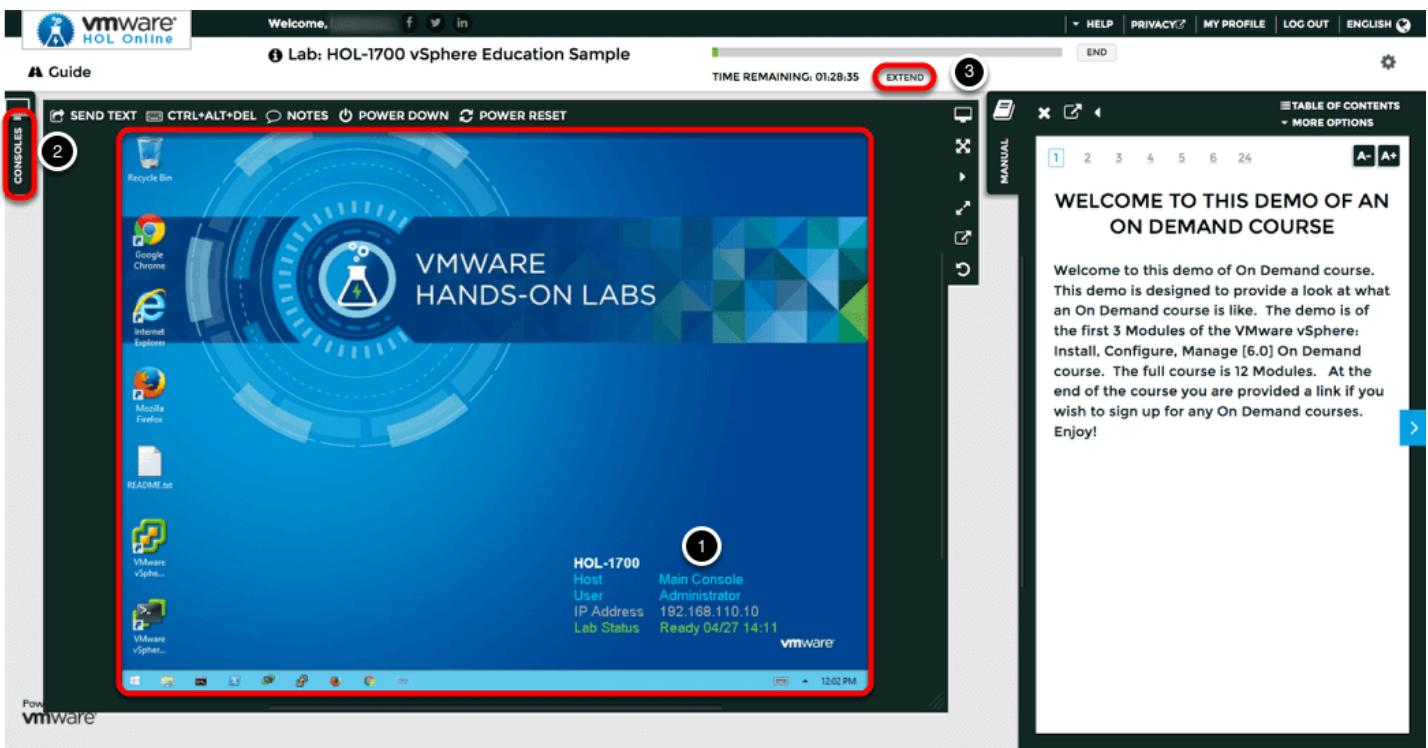
or viewed in HTML:

http://docs.hol.vmware.com/HOL-2020/hol-2010-01-sdc_html_en/

This lab may be localized. To see if this lab has been localized in your language and how to change your preferences to see it, you may review this PDF:

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

Location of the Main Console



1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for 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

During this module, 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

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.

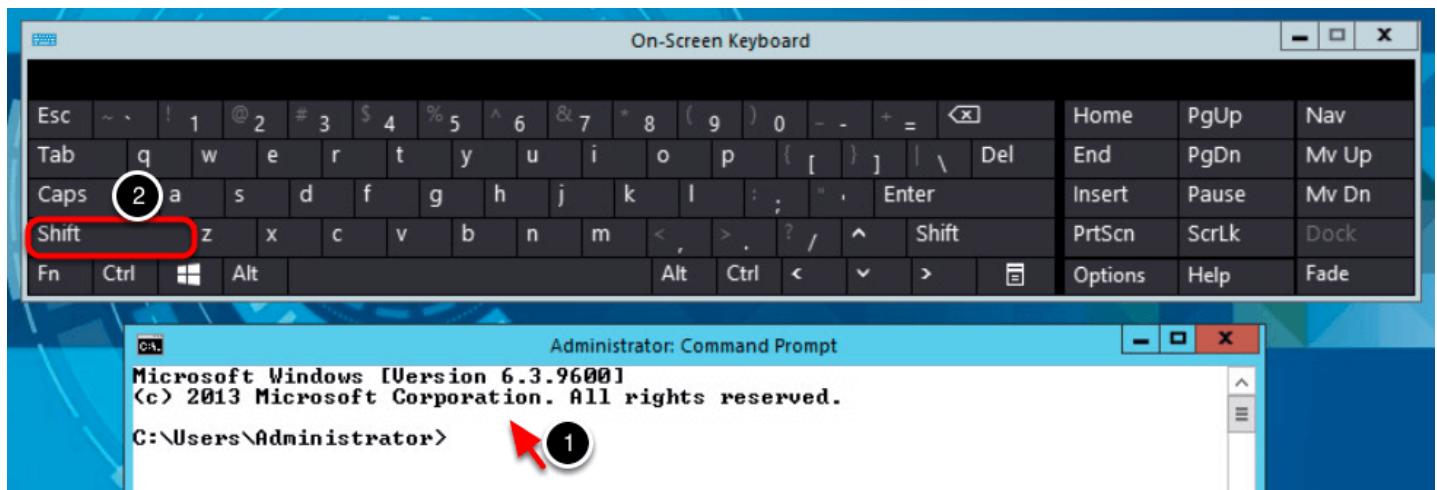
Accessing the Online International Keyboard



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.

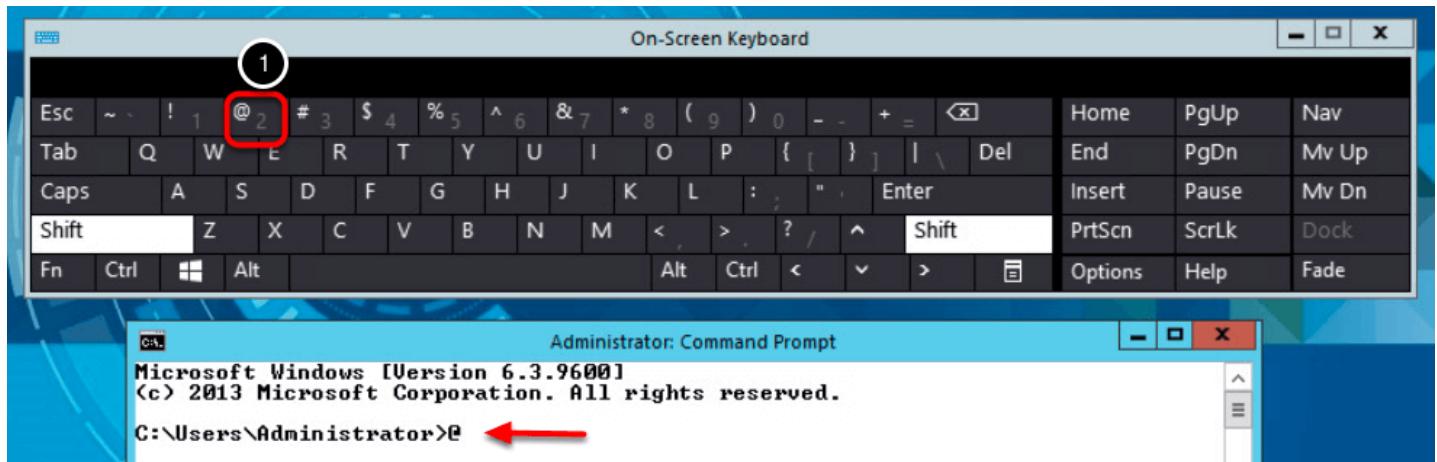
Click once in active console window



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.

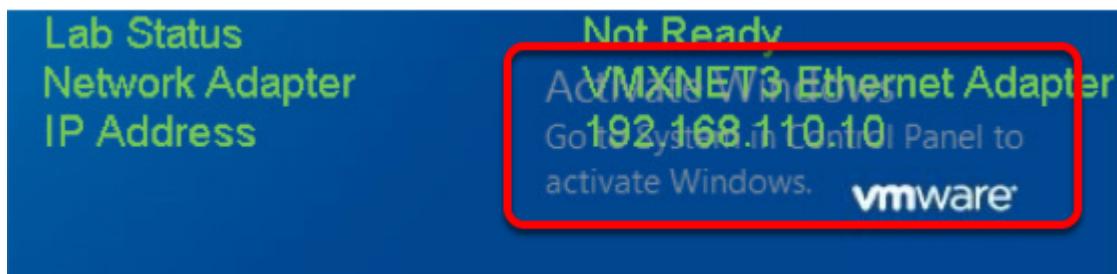
Click on the @ key



1. Click on the "@" key.

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark



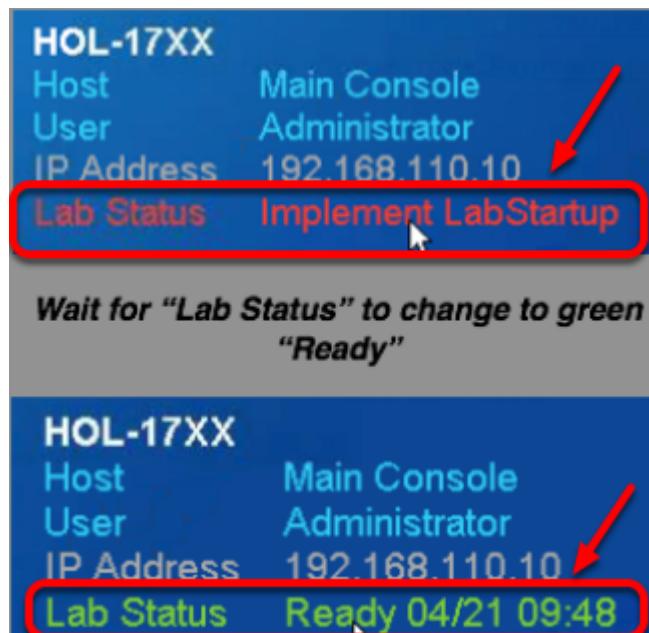
When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the 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, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen



Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes.

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

Introduction

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

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

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

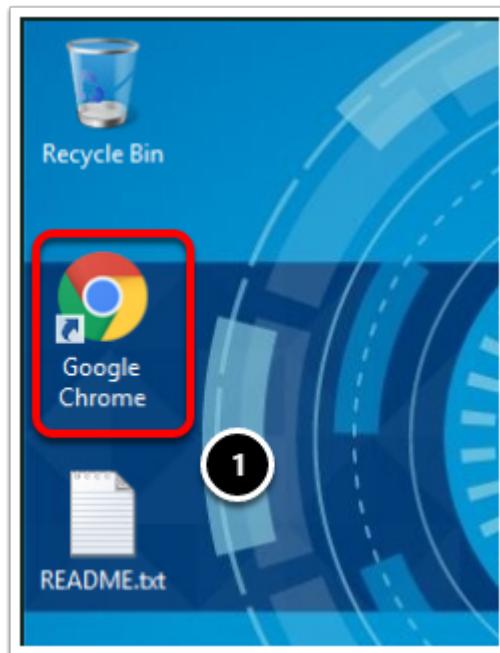
You can use the VMware Host Client to perform administrative and basic troubleshooting tasks, as well as advanced administrative tasks on your target ESXi host. You can also use the VMware Host Client to conduct emergency management when vCenter Server is not available.

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/6.7/vsphere-html-host-client-125-guide.pdf>)

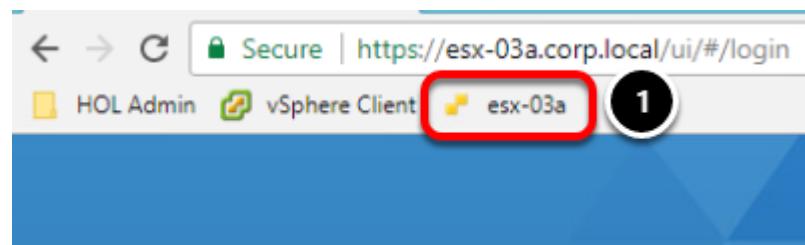
This lesson will walk through some of the most frequently used features in the ESXi Host Client.

Launch Chrome



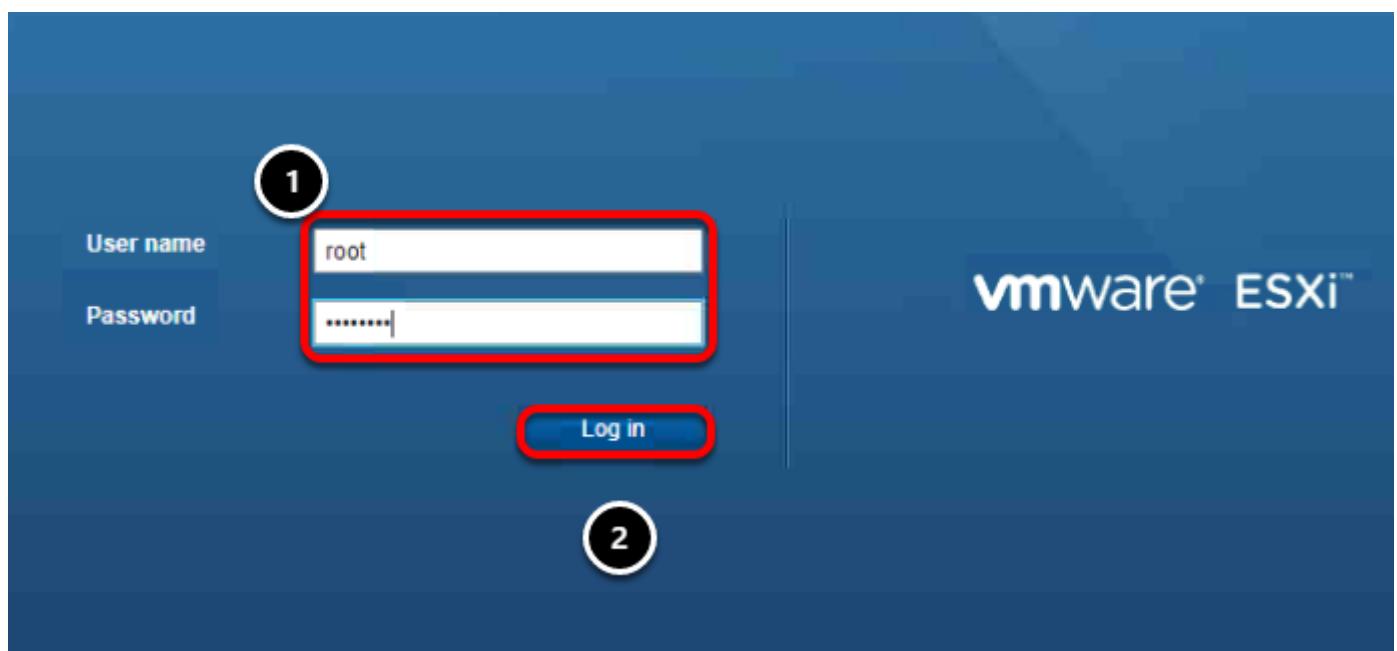
1. Launch **Google Chrome** from the desktop.

Select esx-03a



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

Login

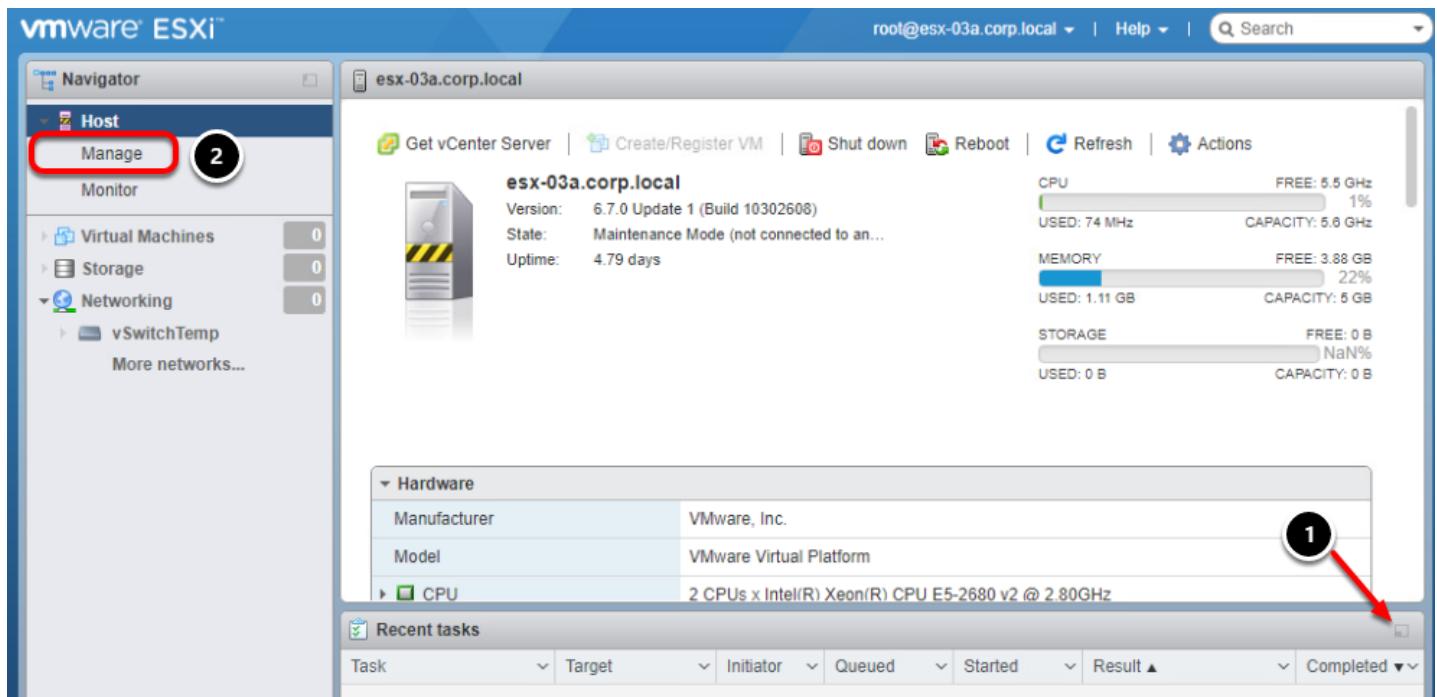


1. Login with the following credentials:

- **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 current in Maintenance Mode, which will be discussed in a future lesson.

1. Click to minimize the Recent tasks interface to gain more room.
2. Click on **Manage**.

System

esx-03a.corp.local - Manage

System **Hardware** Licensing Packages Services Security & users

Advanced settings

Autostart Swap Time & date

Annotations.WelcomeMessage: A welcome message in...
BufferCache.FlushInterval: Flush at this interval (m...
BufferCache.HardMaxDirty: Block writers if this ma...

Quick filters... 1059 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.

1. Click on the **Hardware** tab.

Hardware

esx-03a.corp.local - Manage

System Hardware Licensing Packages **Services** Security & users

PCI Devices **Power Management**

Change policy Refresh

Technology	Unknown
Active Policy	Balanced

1. Click **Power Management**.

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

2. Click the **Services** tab.

Services

The screenshot shows the 'Services' tab in the vSphere Web Client. The tab bar includes 'System', 'Hardware', 'Licensing', 'Packages', 'Services', and 'Security & users'. The 'Security & users' tab is highlighted with a red box and a circled '1'. Below the tabs is a toolbar with buttons for 'Start', 'Stop', 'Restart', 'Refresh', and 'Actions'. The main area is a table with columns: 'Name', 'Description', 'Status', 'Source', and 'Firewall rules'. The table lists several services: DCUI (Running), lbtd (Stopped), lwsmd (Stopped), and ntpd (Running). A search bar and a '12 items' link are at the bottom right.

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

1. Click on **Security and Users**.

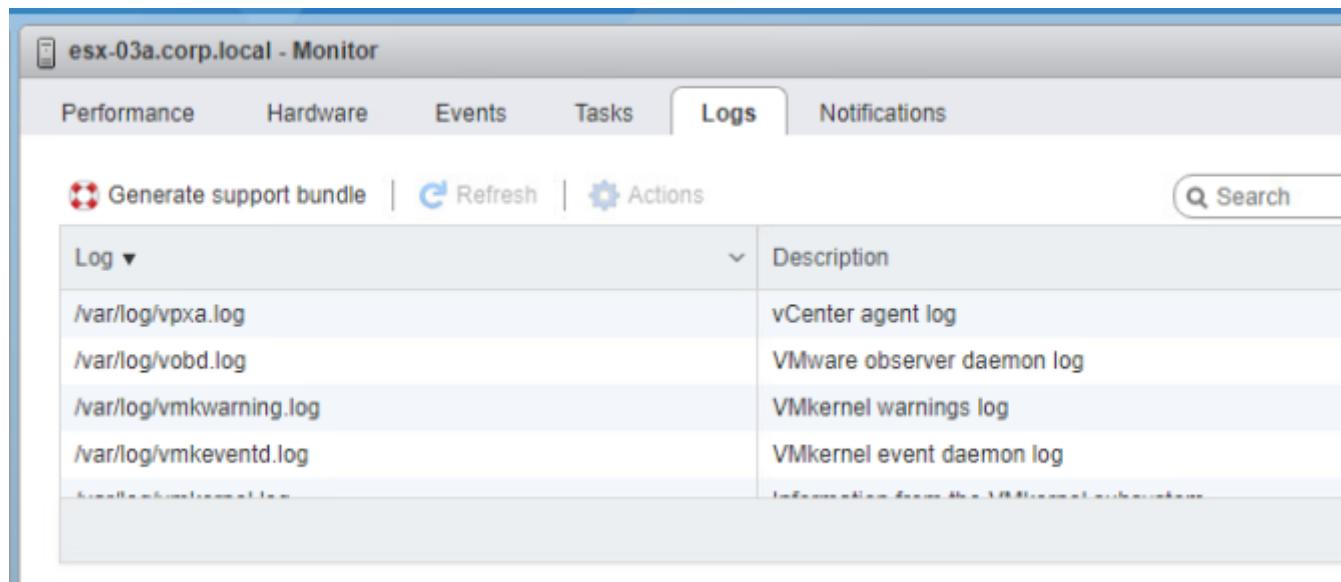
Security & Users

The screenshot shows the 'Manage' tab in the vSphere Web Client. The tab bar includes 'System', 'Hardware', 'Licensing', 'Packages', 'Services', and 'Security & users'. The 'Security & users' tab is selected. On the left, a 'Navigator' sidebar shows 'Host' with 'Manage' selected, and 'Monitor' is highlighted with a red box and a circled '1'. Other options in the sidebar include 'Virtual Machines', 'Storage', 'Networking', and 'vSwitchTemp'. The main content area shows 'Acceptance level' with 'Authentication', 'Certificates', 'Users', 'Roles', and 'Lockdown mode' listed. There are 'Edit settings' and 'Refresh' buttons at the top of this section.

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 setup to use Single Sign-on which makes account management much easier. This will be reviewed in the lessons that follow.

1. Click on **Monitor**.

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

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

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.

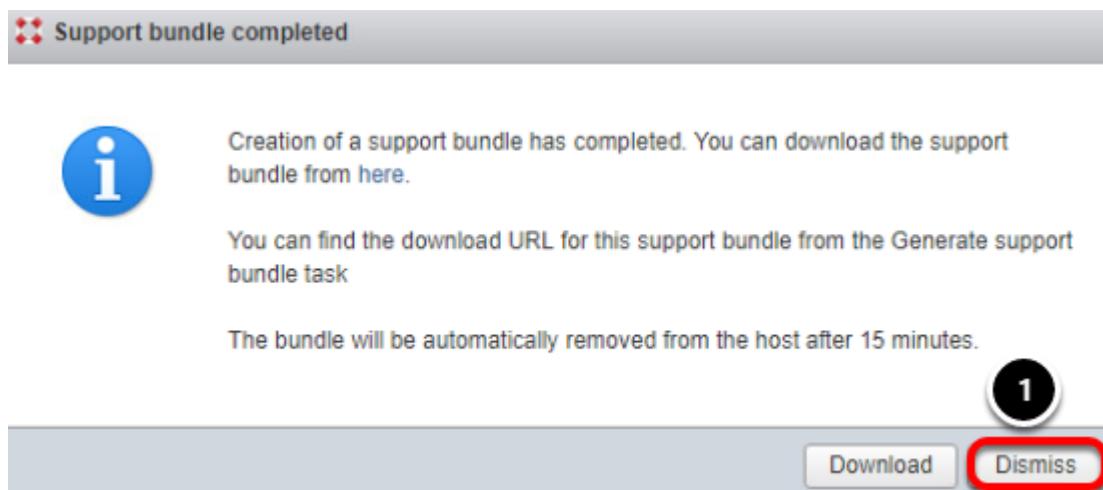
2. Click the **Generate Support Bundle** button. This operation will take a minute or two to complete.

Credentials?

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

- User name: root
- Password: VMware1!

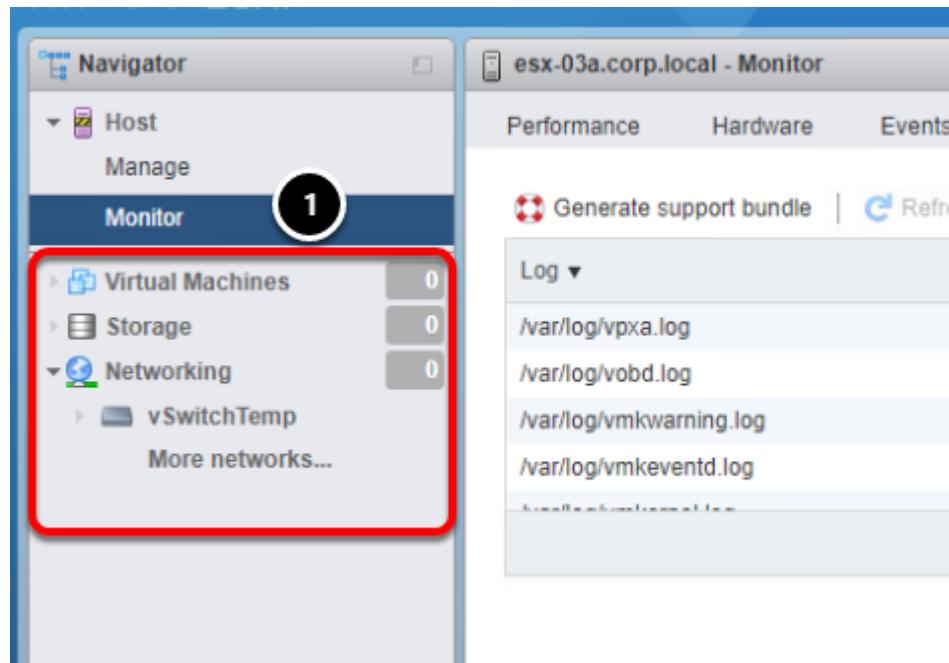
Support Bundle Completed



1. Click the Dismiss button.

Note that the bundle will be deleted after 15 minutes.

VMs, Storage and Networking



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

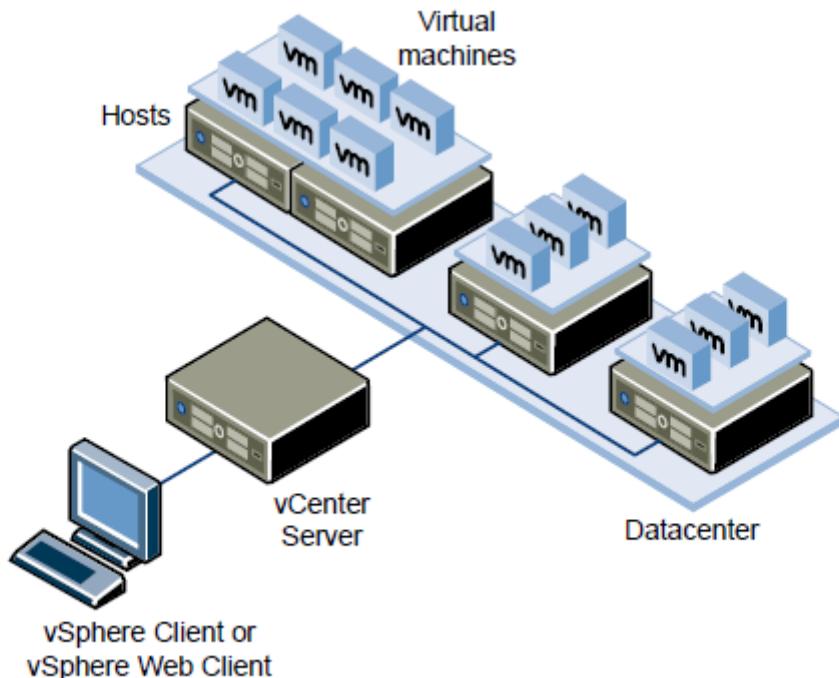
Since these features will be covered throughout the lab and the actions performed are identical, just at the vCenter Server level, we will not be reviewing them here.

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 6 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.

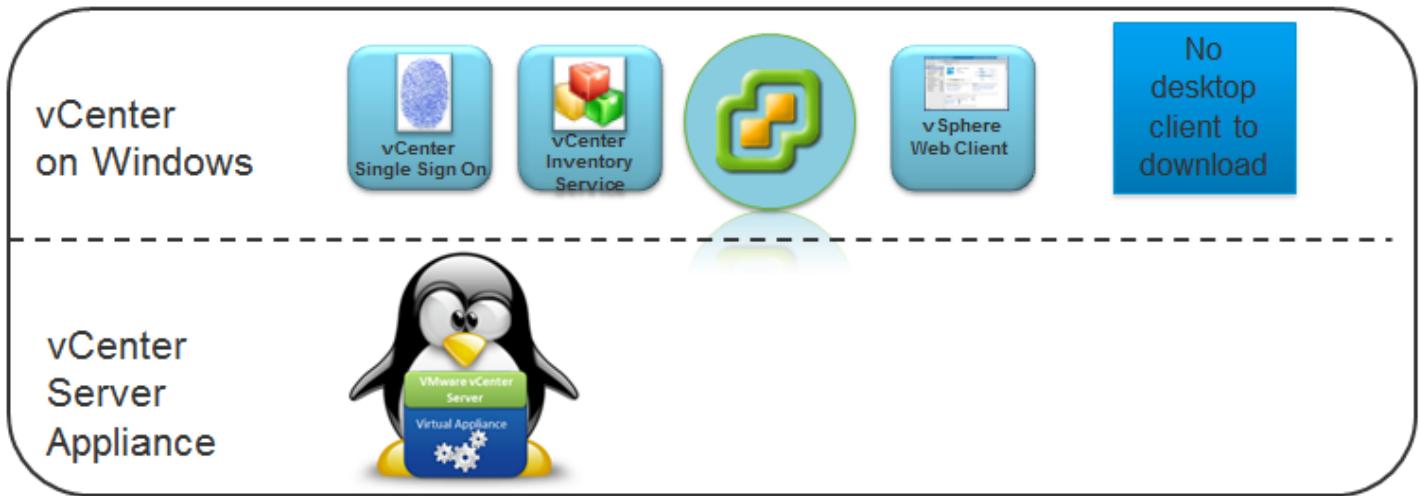
vSphere v6 Components



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 6 Components

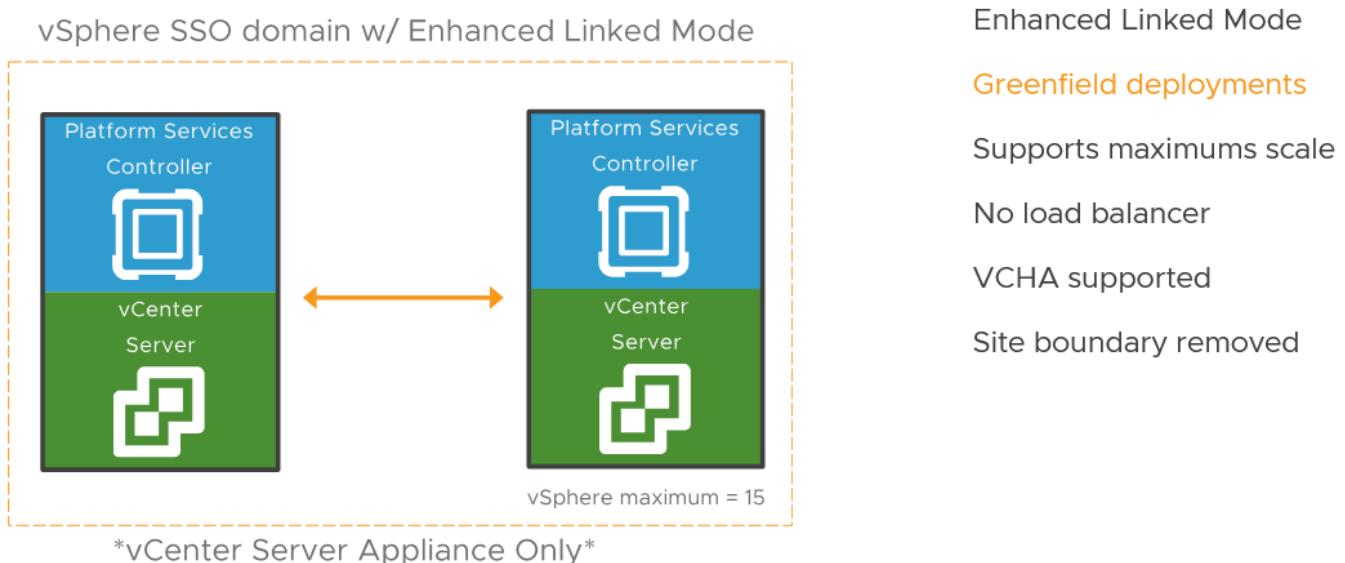


Starting with vSphere 5.1 there are two methods to deploy vCenter. The first method is a Windows installation. With the Windows method, you can install vCenter Single Sign On, Inventory Service, and vCenter Server on the same host machine (as with vCenter Simple Install) or on different virtual machines.

The other method is a virtual appliance. 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)

vCenter Server with Embedded PSC and ELM Simplified Architecture



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:

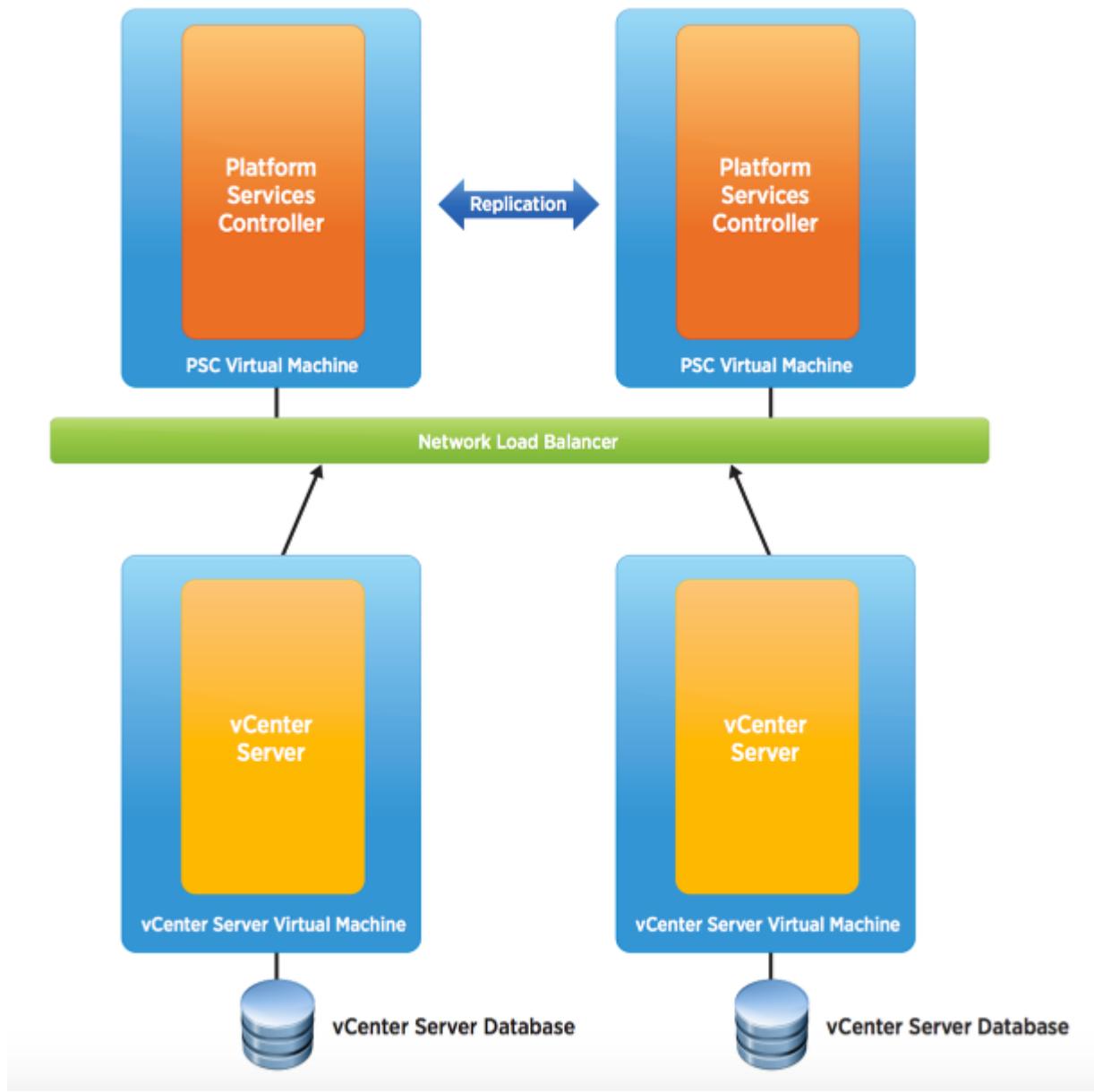
- The PSC removes services from vCenter and makes them centralized across the vCloud Suite.
- This gives customers a single point to manage all their vSphere roles and permissions along with licensing.
- Reducing vCenter Server installation complexity allows customers to install or upgrade to vSphere 6 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

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

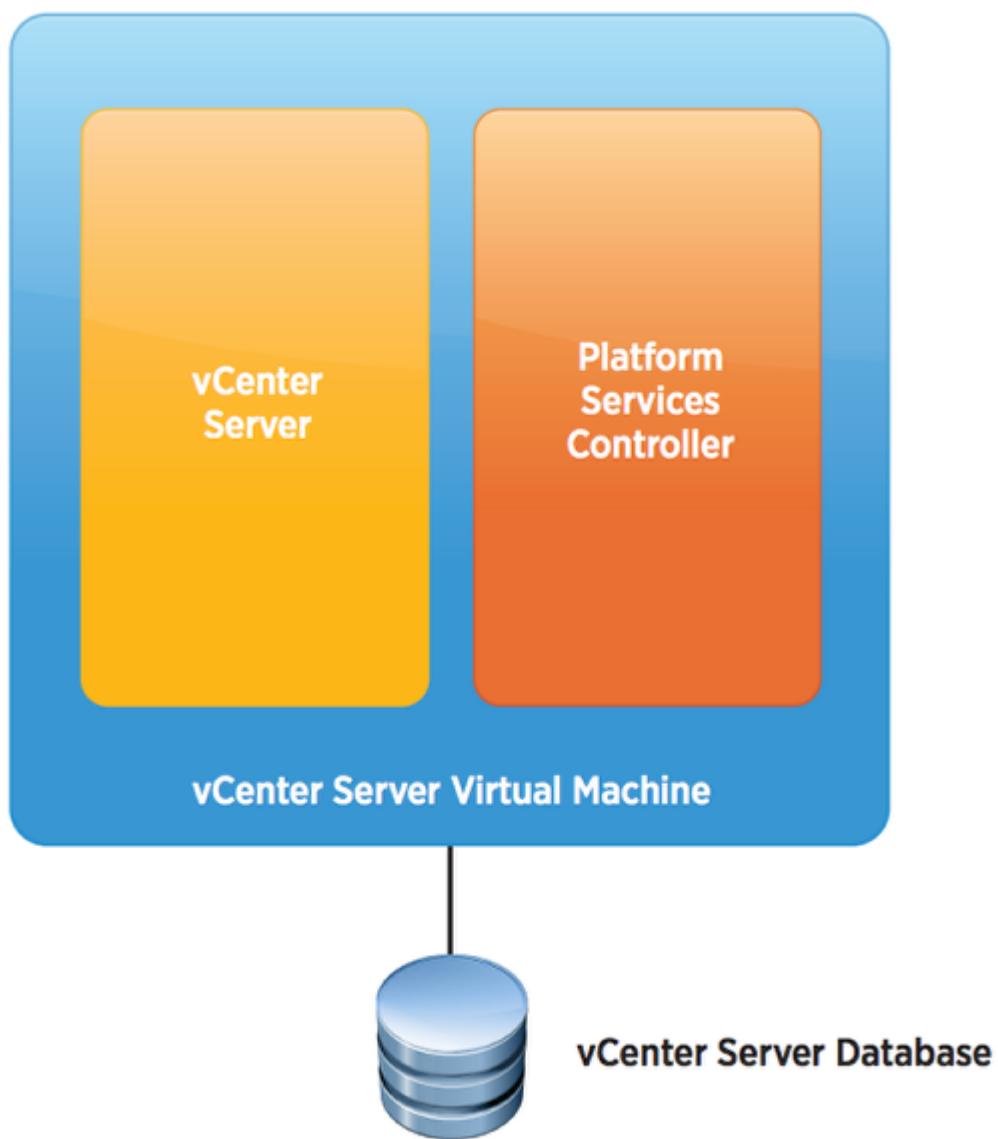


Starting with version 5.1, vSphere includes a vCenter Single Sign-On service as part of the vCenter Server management infrastructure.

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. Both Windows and the vCSA can participate in this 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 6 Deployment Guide for more in-depth requirements and considerations for SSO architecture in vCenter 6:

<http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server6-deployment-guide.pdf>

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

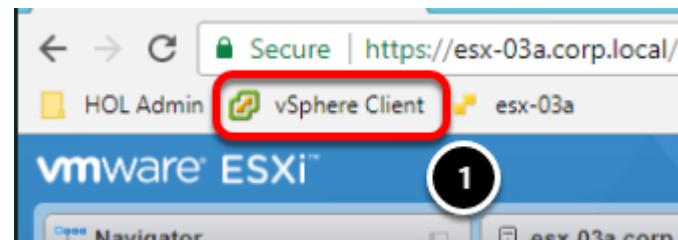
You can extend vSphere in different ways to create a solution for your unique IT infrastructure. You can extend the vSphere Client with additional GUI features to support these new capabilities, with which you can manage and monitor your unique vSphere environment.

Launch Chrome



If you are not already in Chrome, double click the **Google Chrome**.

Select vSphere Client



1. Click the **vSphere Client** bookmark.

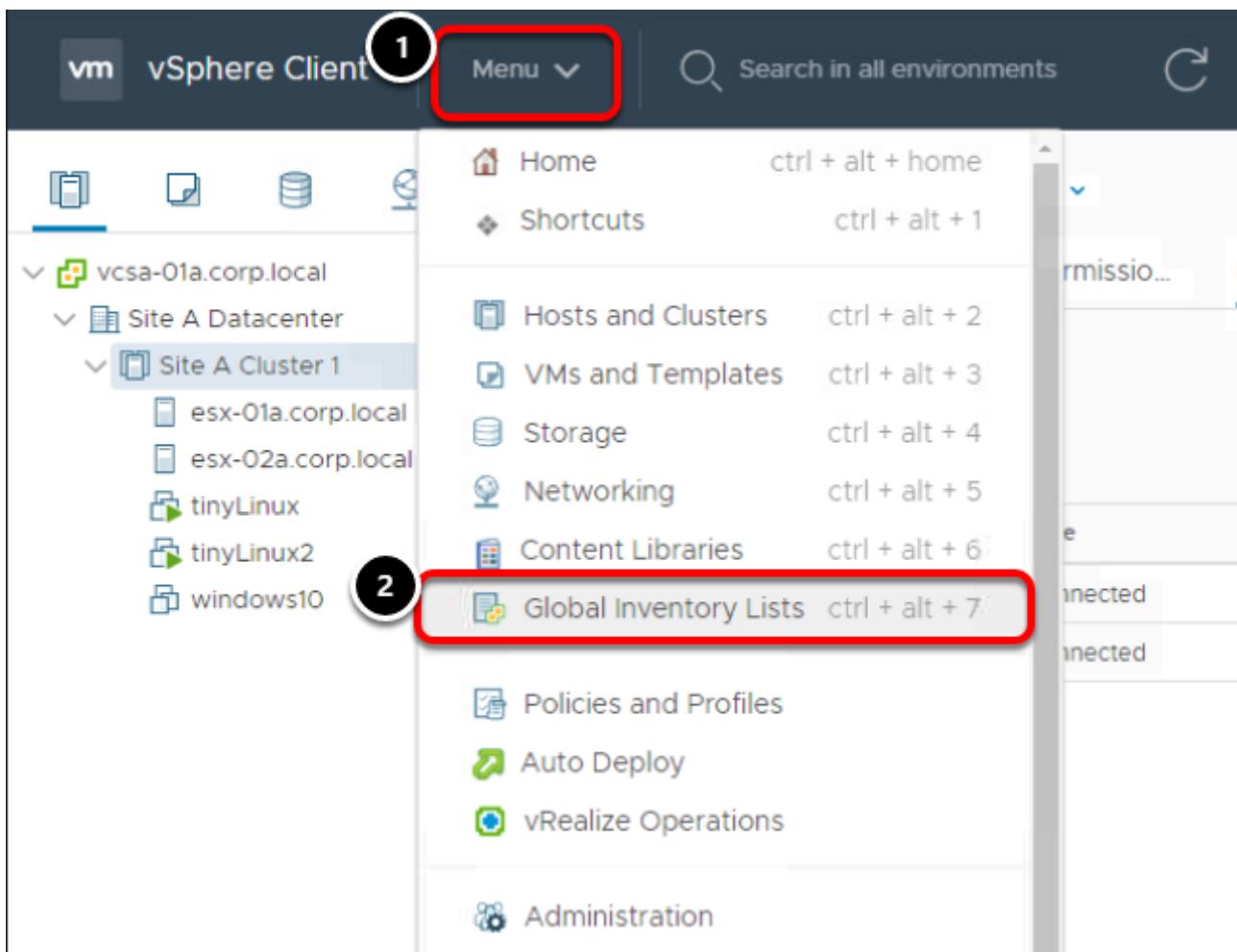
Login to vCenter



Log in using the following method:

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

vCenter Inventory

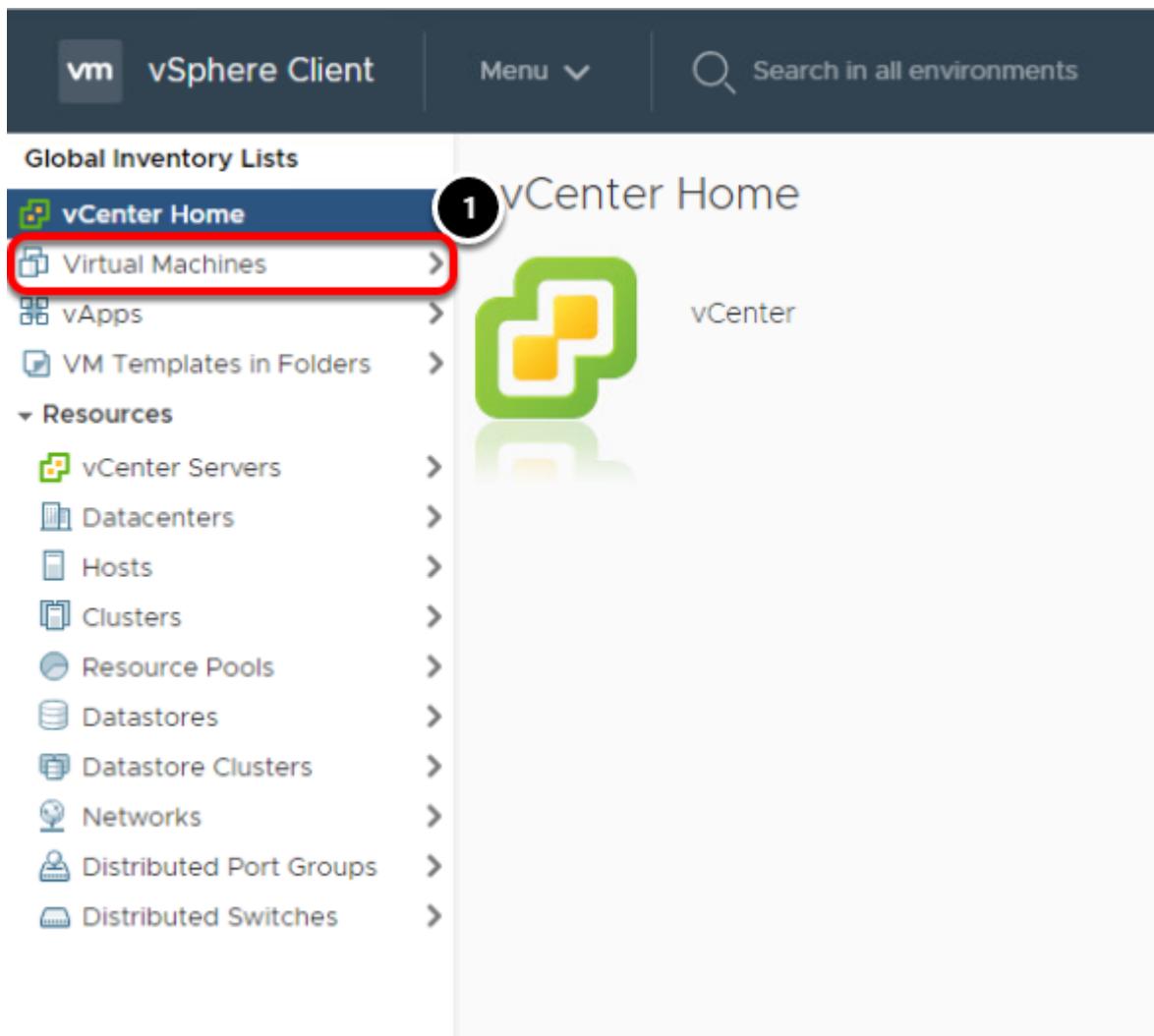


By default, you are brought to a view that shows the Hosts and Clusters attached to vCenter. Get a more complete look by viewing the Global Inventory Lists.

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.

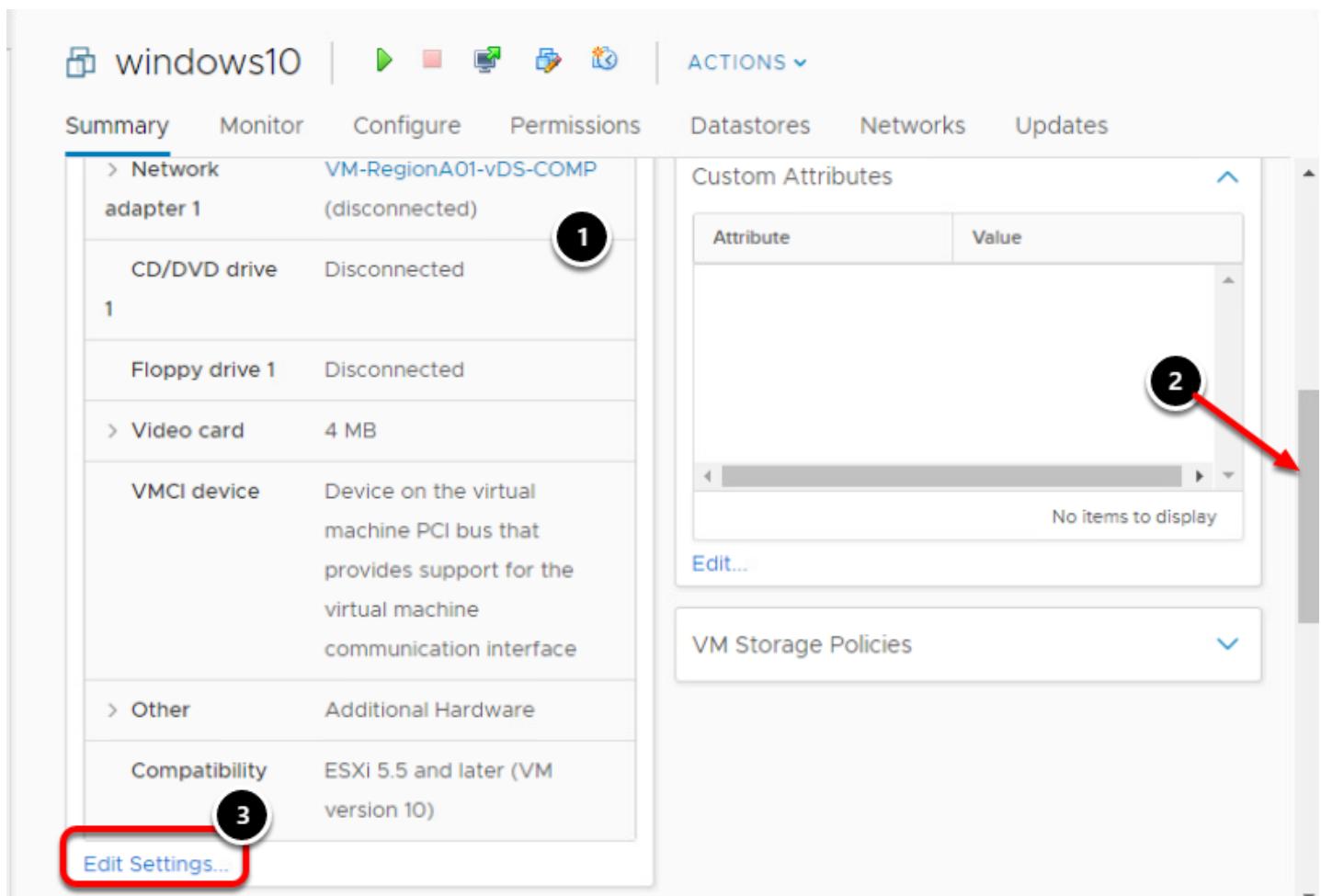
Virtual Machine Summary

The screenshot shows the vSphere Client interface. On the left, a list of virtual machines includes 'tinyLinux', 'tinyLinux2', and 'windows10' (which is circled with a red box labeled '1'). The main pane displays the 'Summary' tab for the selected 'windows10' VM. The VM is 'Powered Off'. On the right, detailed information is shown: Guest OS: Microsoft Windows 10 (32-bit), Compatibility: ESXi 5.5 and later (VM version), VMware Tools: Not running, version:10338 (with a 'More info' link), DNS Name: windows10, IP Addresses: (empty), and Host: esx-02a.corp.local. Below this, there are 'Launch Web Console' and 'Launch Remote Console' buttons. The 'VM Hardware' section is expanded, showing: CPU (1 CPU(s)), Memory (1 GB, 0 GB memory active), Hard disk 1 (24 GB), and Network (VM-RegionA01-vDS-COMP). A red box labeled '3' highlights the 'Edit Settings' link next to the Network entry. A 'Notes' panel on the right contains a note about vCD showing W unavailable, MSDN 1511 build, and DHCP, NTP, and access enable, with an 'Edit Notes...' link.

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 a "Edit Settings" link as well to modify the settings of the virtual machine.
3. Expand the **VM Hardware** section.

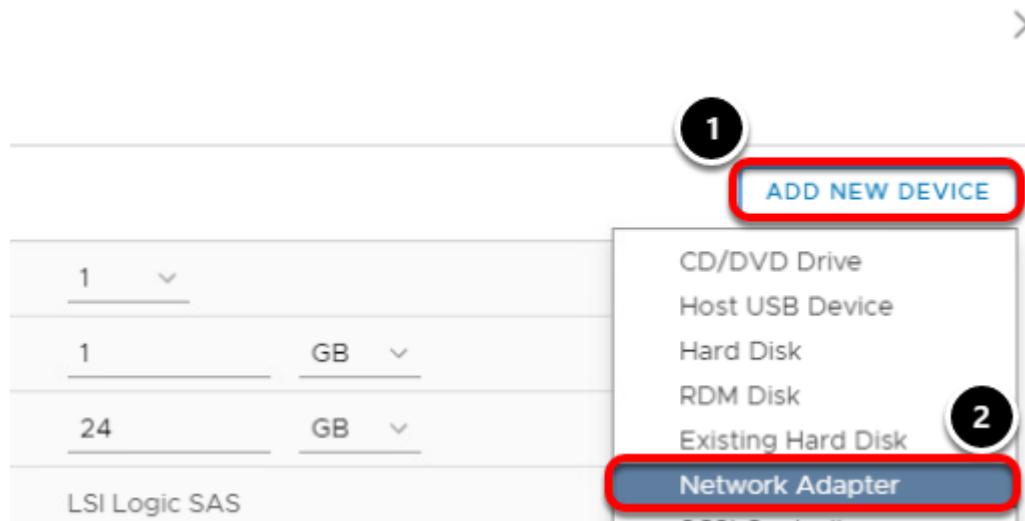
Edit the settings of a virtual machine.



The screenshot shows the vSphere Web Client interface for a virtual machine named "windows10". The "Edit Settings..." button is highlighted with a red box and labeled with a black circle containing the number 3. A scroll bar on the right side of the window is labeled with a black circle containing the number 2, with a red arrow pointing towards it. The "Edit Settings..." button is located at the bottom left of the main content area.

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.

Edit Settings | windows10 X

Virtual Hardware VM Options

ADD NEW DEVICE

> CPU	1	▼	i
> Memory *	1	GB	▼
> Hard disk 1	24	GB	▼
> SCSI controller 0	LSI Logic SAS		
> Network adapter 1	VM-RegionA01-vDS-COMP	▼	<input checked="" type="checkbox"/> Connected
New Network *	VM-RegionA01-vDS-COMP	▼	<input checked="" type="checkbox"/> Connected
Status	<input checked="" type="checkbox"/> Connect At Power On		
Adapter Type	E1000E		
MAC Address	Automatic		

CANCEL
OK

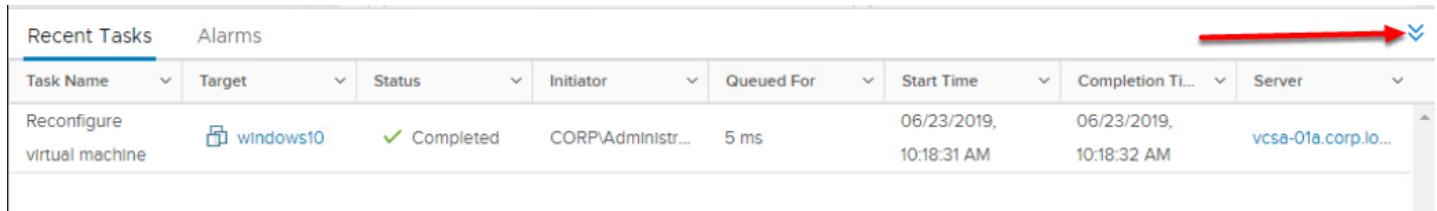
1. Click the arrow next to the New Network card to expand and view its settings. Notice that the MAC address is blank at this point. A new MAC address will be generated once this NIC is added or we are able to specify (with some rules) our own MAC address.
2. Click "OK" to add the device to the VM. When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

Recent Tasks List

Recent Tasks
Alarms

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

Recent Tasks List

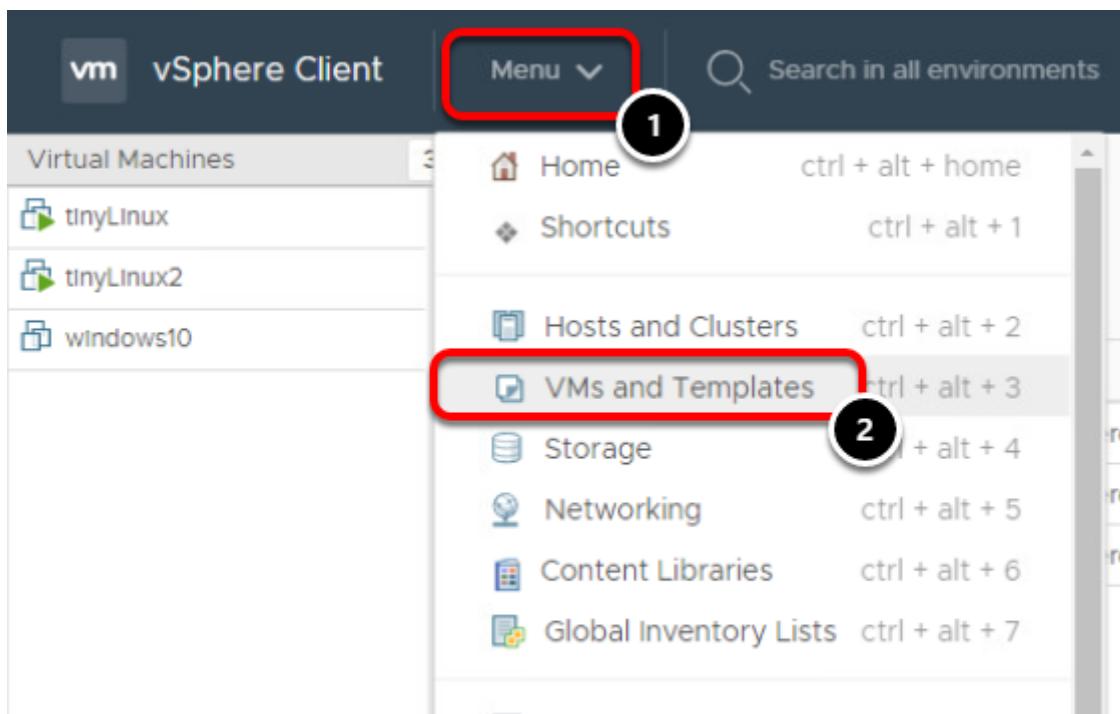


Recent Tasks		Alarms						
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Ti...	Server	
Reconfigure virtual machine	Windows10	Completed	CORP\Administr...	5 ms	06/23/2019, 10:18:31 AM	06/23/2019, 10:18:32 AM	vcsa-01a.corp.lo...	

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.

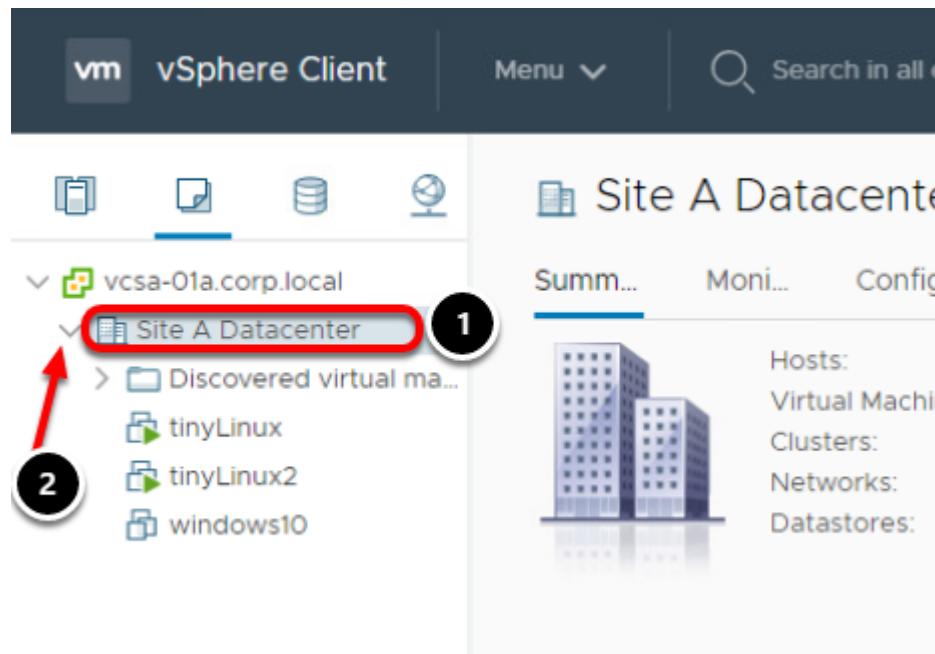
Create a Virtual Machine



In the next steps, we will walk through the process of creating a virtual machine and then installing an operating system.

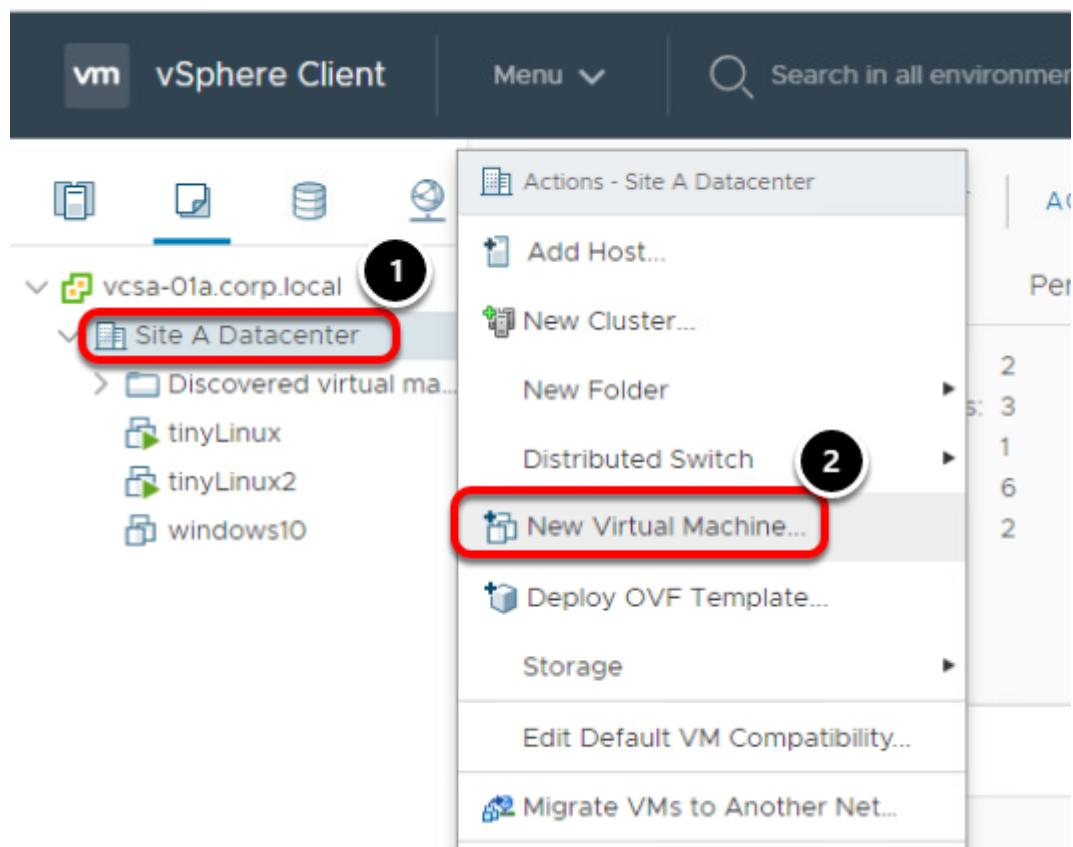
1. To return to the VMs and Templates view, click on **Menu**.
2. Select **VMs and Templates**

Select and Expand Datacenter



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

Start the New Virtual Machine Wizard



1. Right click on **Site A 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

New Virtual Machine

The screenshot shows the 'Select a creation type' step of the 'New Virtual Machine' wizard. On the left, a vertical list of steps is shown: 1 Select a creation type (highlighted with a green checkmark), 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, and 8 Ready to complete. The main panel shows the 'Select a creation type' step with the question 'How would you like to create a virtual machine?'. A list of options is displayed: 'Create a new virtual machine' (highlighted in blue), 'Deploy from template', 'Clone an existing virtual machine', 'Clone virtual machine to template', 'Clone template to template', and 'Convert template to virtual machine'. To the right of the list is a description: 'This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.' At the bottom right are three buttons: 'CANCEL', 'BACK', and 'NEXT' (which is highlighted with a red circle).

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

Name the Virtual Machine

New Virtual Machine

✓ 1 Select a creation type

2 Select a name and folder

3 Select a compute resource

4 Select storage

5 Select compatibility

6 Select a guest OS

7 Customize hardware

8 Ready to complete

Select a name and folder

Specify a unique name and target location

1

Virtual machine **web-serv01**

name:

Select a location for the virtual machine.

vcsa-01a.corp.local
Site A Datacenter

2

CANCEL

BACK

NEXT

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

Virtual Machine Placement

New Virtual Machine

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

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

1

2

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Because Distributed Resource Scheduler (DRS) is enabled, you just have to select a cluster and DRS will determine which host to use for the VM. More details on DRS will be covered later in this module.

1. Click **Site A Cluster 1**
2. Click **Next**

Select Storage

New Virtual Machine

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

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine

VM Storage Policy: Datastore Default

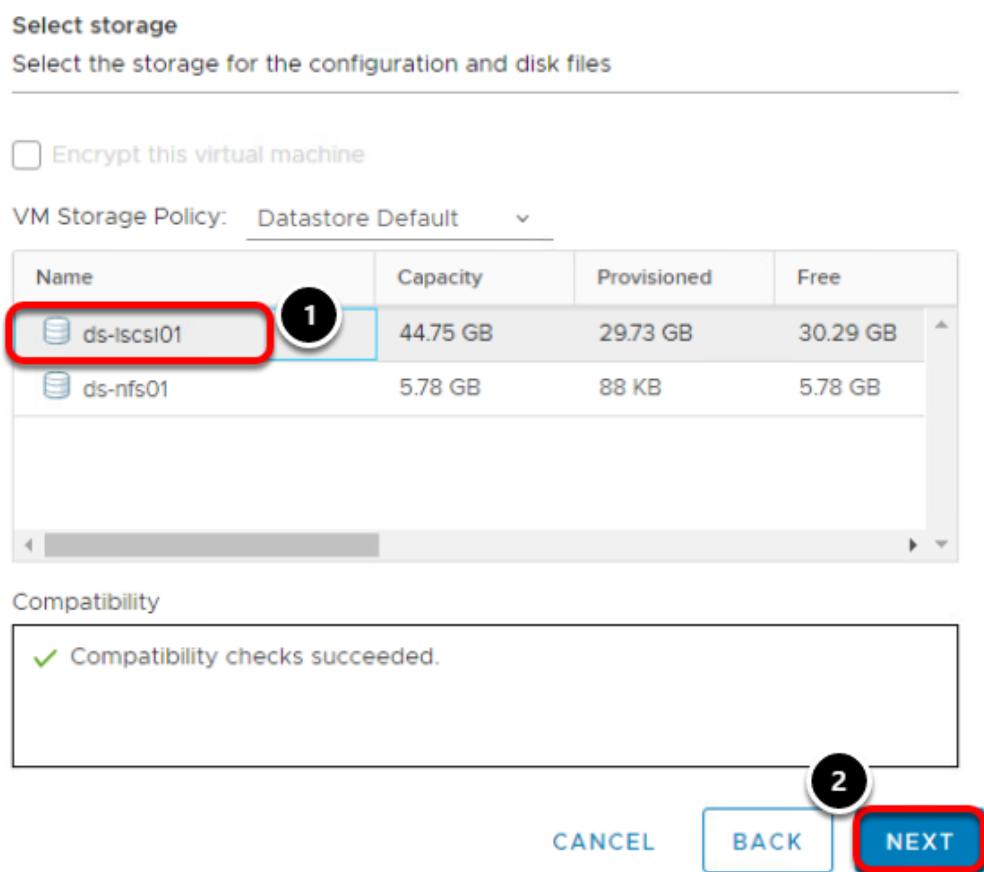
Name	Capacity	Provisioned	Free
ds-iscsi01	44.75 GB	29.73 GB	30.29 GB
ds-nfs01	5.78 GB	88 KB	5.78 GB

Compatibility

✓ Compatibility checks succeeded.

1 2

CANCEL BACK **NEXT**



1. Ensure the **ds-iscsi01** datastore is selected
2. Click **Next**

Compatibility

New Virtual Machine

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

Select compatibility

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

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

Compatible with: **ESXi 6.7 and later**  

This virtual machine uses hardware version 14, which provides the best performance and latest features available in ESXi 6.7.

CANCEL

BACK

NEXT

1

1. Click **Next** to accept the default **ESXi 6.7 and later**

Guest OS

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- 6 Select a guest OS**

7 Customize hardware
8 Ready to complete

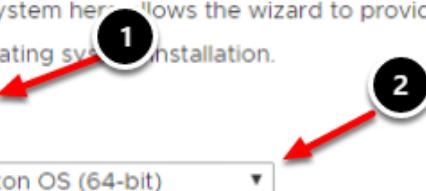
Select a guest OS

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

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

Guest OS Family: **Linux**

Guest OS Version: **VMware Photon OS (64-bit)**



Compatibility: ESXi 6.7 and later (VM vers 3)

CANCEL

BACK

NEXT

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.

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS

7 Customize hardware

8 Ready to complete

Customize hardware
Configure the virtual machine hardware

Virtual Hardware VM Options

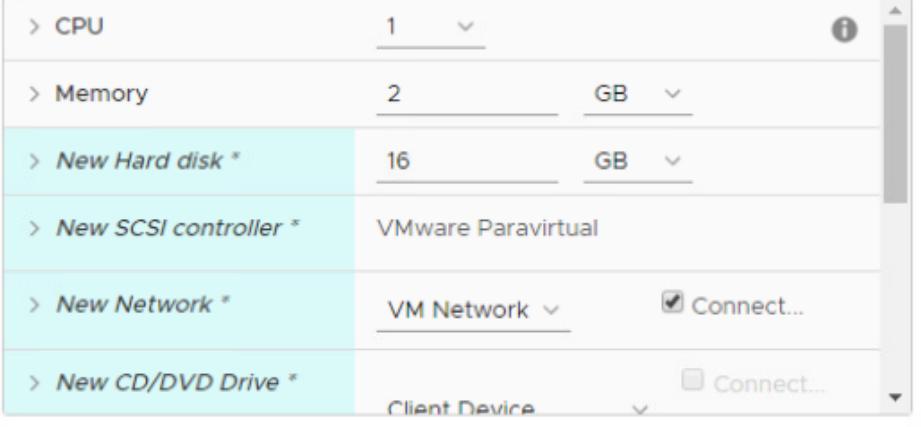
ADD NEW DEVICE

> CPU	1	▼	i
> Memory	2	GB	▼
> New Hard disk *	16	GB	▼
> New SCSI controller *	VMware Paravirtual		
> New Network *	VM Network	▼	<input checked="" type="checkbox"/> Connect...
> New CD/DVD Drive *	Client Device		

Compatibility: ESXi 6.7 and later (VM version 14)

1

CANCEL **BACK** **NEXT**



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
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- ✓ 7 Customize hardware

8 Ready to complete

Ready to complete
Click Finish to start creation.

Provisioning type	Create a new virtual machine
Virtual machine name	web-serv01
Folder	Site A Datacenter
Cluster	Site A Cluster 1
Datastore	ds-iscsi01
Guest OS name	VMware Photon OS (64-bit)
Virtualization Based Security	Disabled
CPUs	1
Memory	2 GB

Compatibility: ESXi 6.7 and later (VM version 14)

CANCEL

BACK

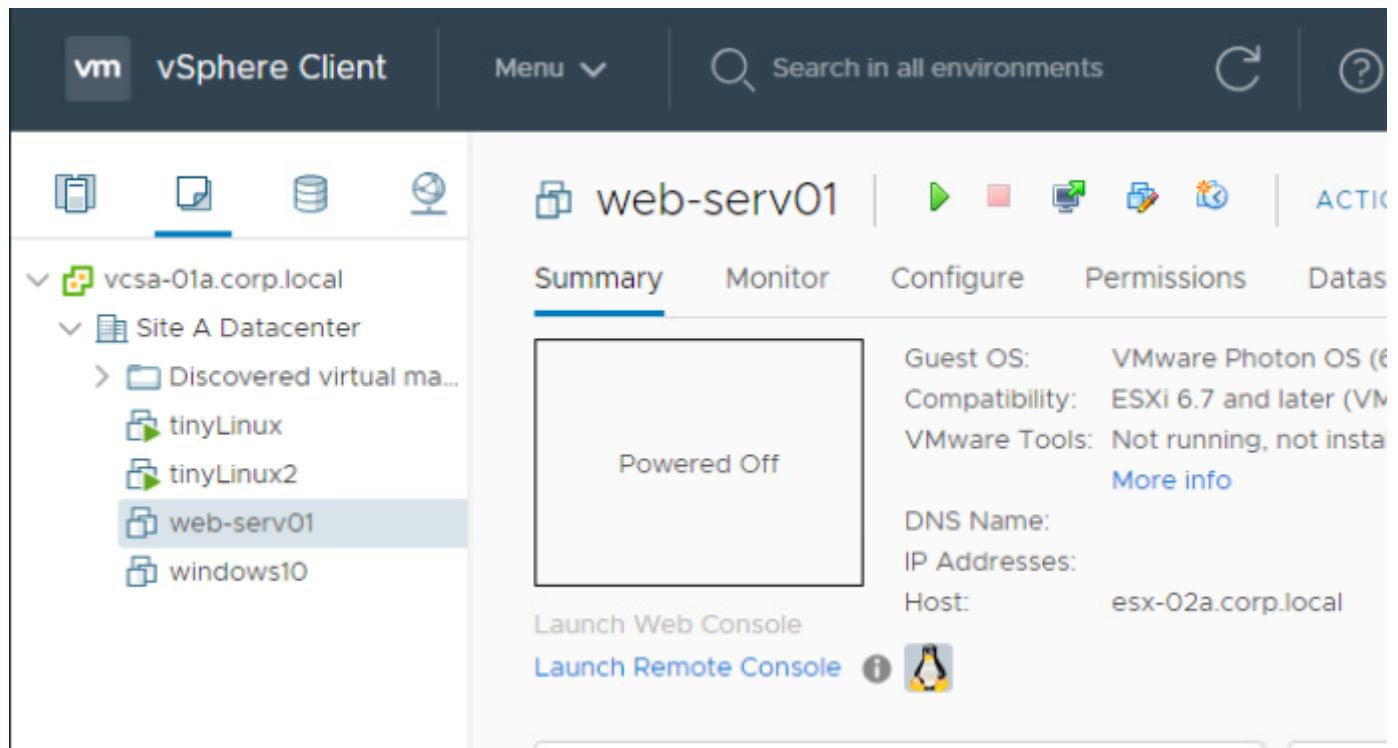
FINISH

1

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

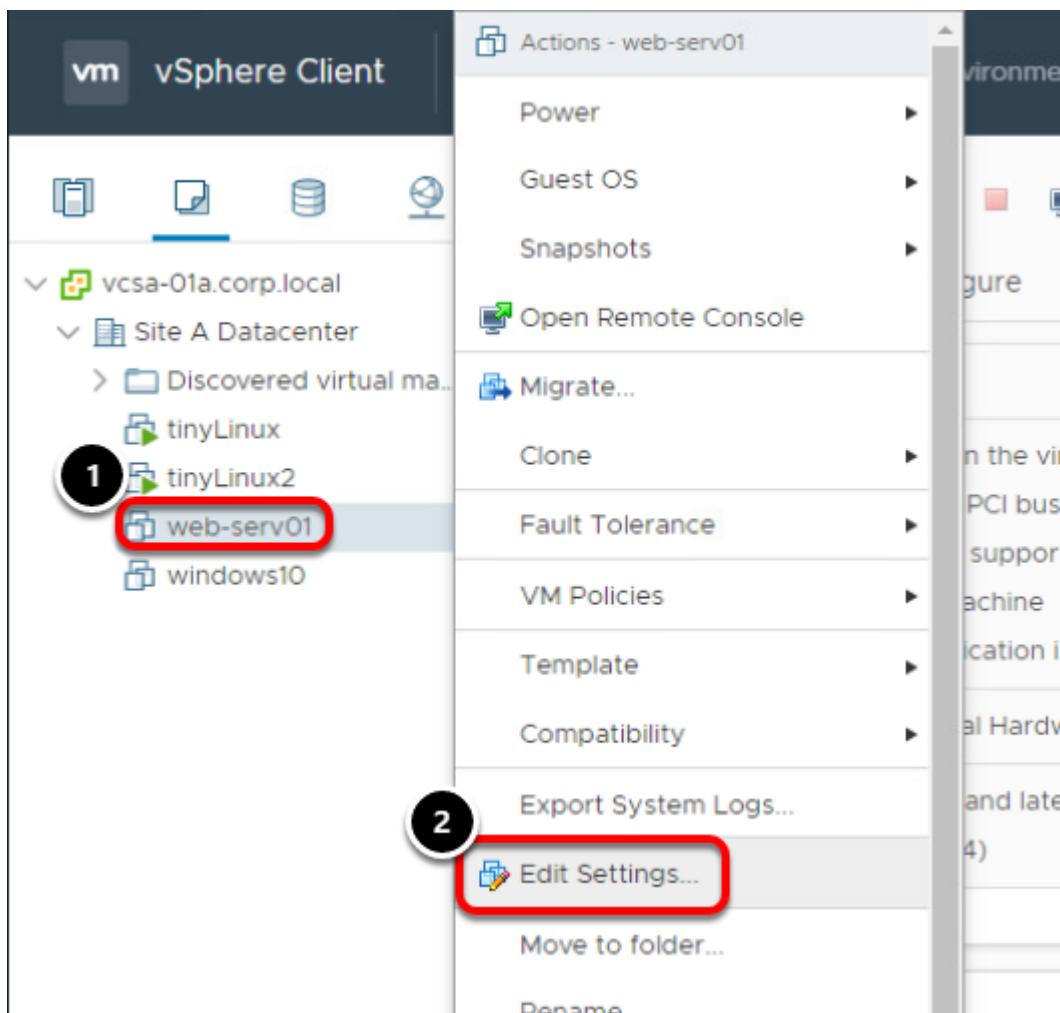


The screenshot shows the vSphere Client interface. In the left sidebar, under the 'vSphere Client' tab, the navigation tree shows 'vcsa-01a.corp.local' and 'Site A Datacenter'. Inside 'Site A Datacenter', there are several virtual machines: 'tinyLinux', 'tinyLinux2', 'web-serv01' (which is selected and highlighted in blue), and 'windows10'. The main pane displays the 'Summary' tab for the selected VM, 'web-serv01'. The status is 'Powered Off'. On the right, detailed information is provided: Guest OS: VMware Photon OS (64-bit), Compatibility: ESXi 6.7 and later (VMware Photon OS), VMware Tools: Not running, not installed, and a 'More info' link. The DNS Name is listed as 'web-serv01'. The IP Addresses and Host are listed as 'esx-02a.corp.local'. Below the summary, there are links to 'Launch Web Console' and 'Launch Remote Console'.

Congratulations on creating your first virtual machine!

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.

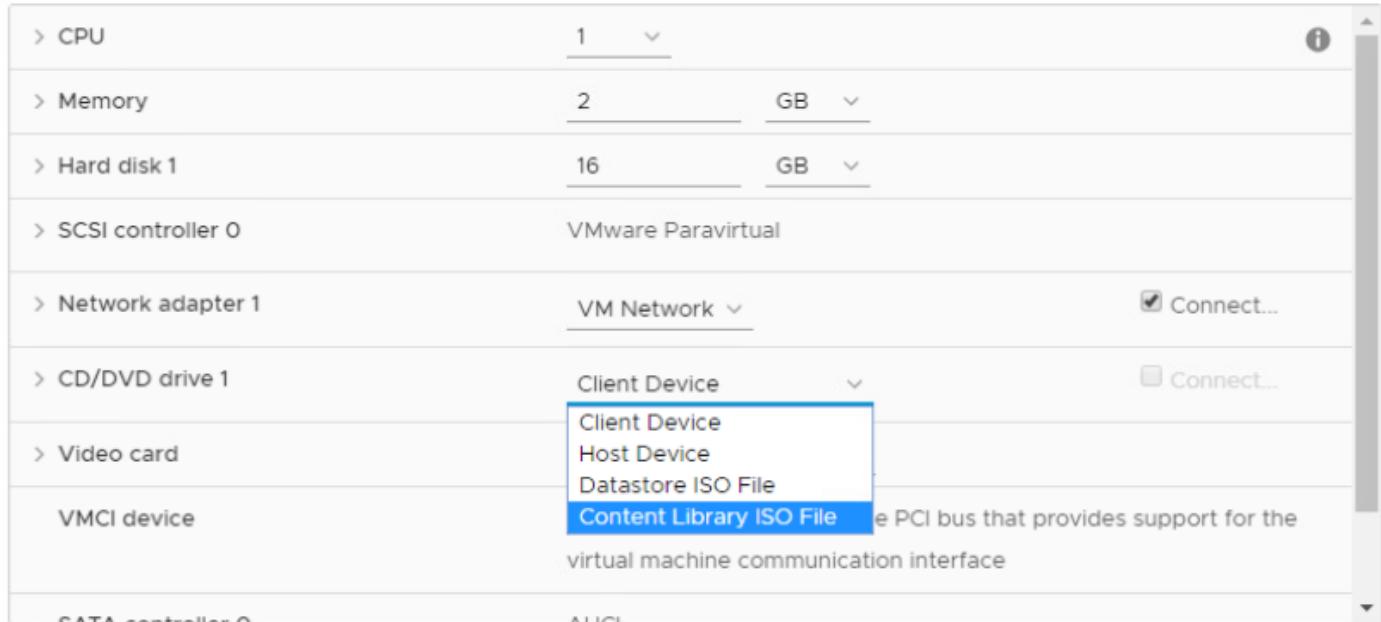
1. To attach an ISO image to the virtual machine we just created, make sure **web-serv01** is selected
2. Right click on **web-serv01** and select **Edit Settings...**

Content Library ISO File

Edit Settings | web-serv01 X

Virtual Hardware VM Options

ADD NEW DEVICE



> CPU	1	▼	i
> Memory	2	GB	▼
> Hard disk 1	16	GB	▼
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VM Network	▼	<input checked="" type="checkbox"/> Connect...
> CD/DVD drive 1	Client Device	▼	<input type="checkbox"/> Connect...
> Video card	Client Device		
VMCI device	Host Device		
	Datastore ISO File		
	Content Library ISO File		e PCI bus that provides support for the virtual machine communication interface
ATA controller 0	ALeT		

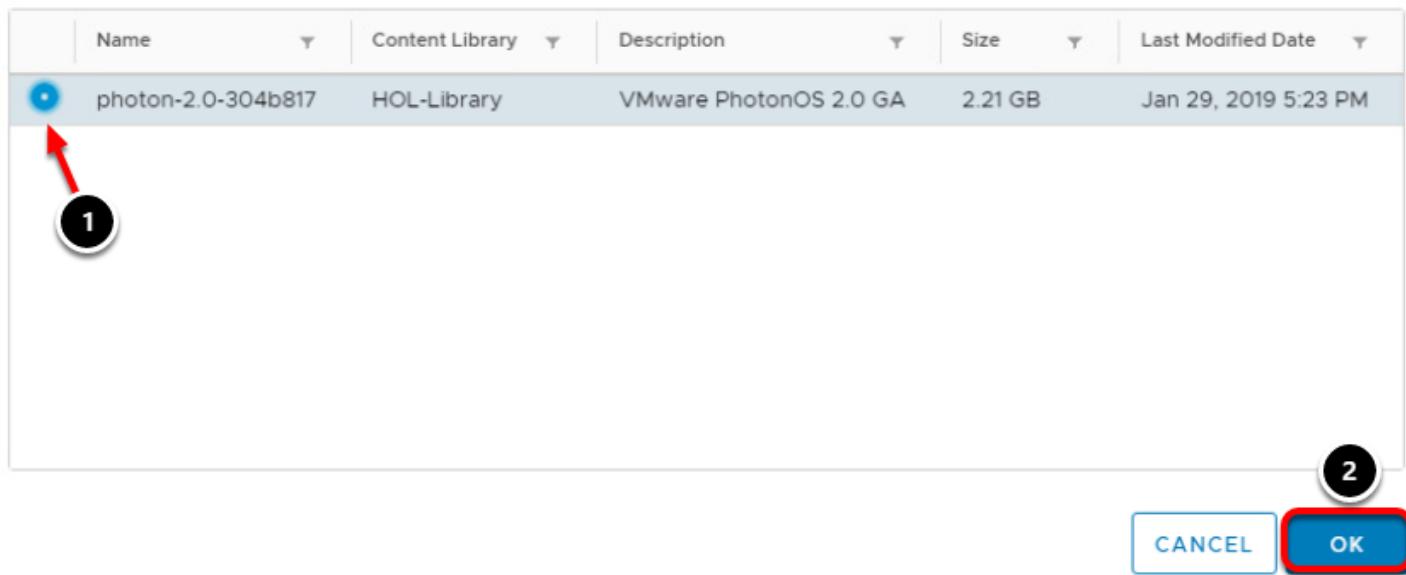
1. From the **CD/DVD drive 1** drop-down menu, select **Content Library ISO File**.

This will open a file explorer to select that file.

Select Photon

Choose an ISO image to mount

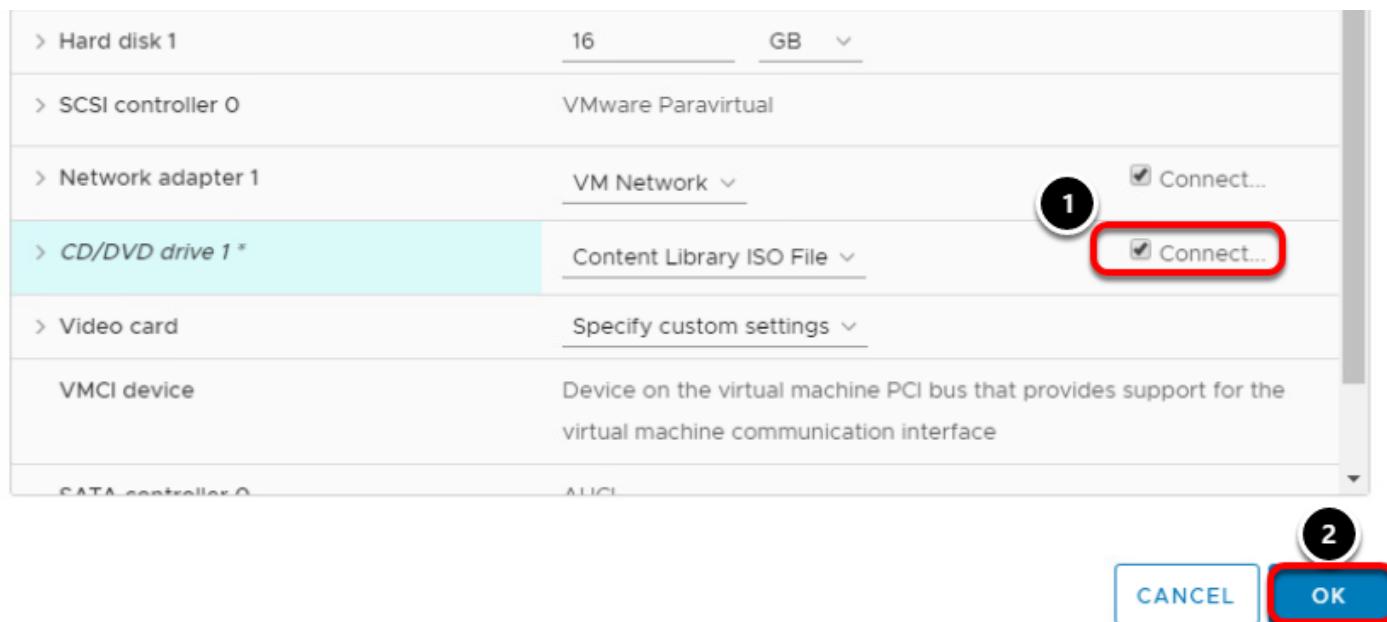
X



A screenshot of a file selection dialog. The table header includes columns for Name, Content Library, Description, Size, and Last Modified Date. A single row is selected, highlighted with a blue background. The row contains the following data: Name: photon-2.0-304b817, Content Library: HOL-Library, Description: VMware PhotonOS 2.0 GA, Size: 2.21 GB, and Last Modified Date: Jan 29, 2019 5:23 PM. A red arrow points to the radio button next to the selected file name. A red circle with the number '1' is placed over the selected file row. A red circle with the number '2' is placed over the 'OK' button, which is highlighted with a red border.

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

Connect the drive

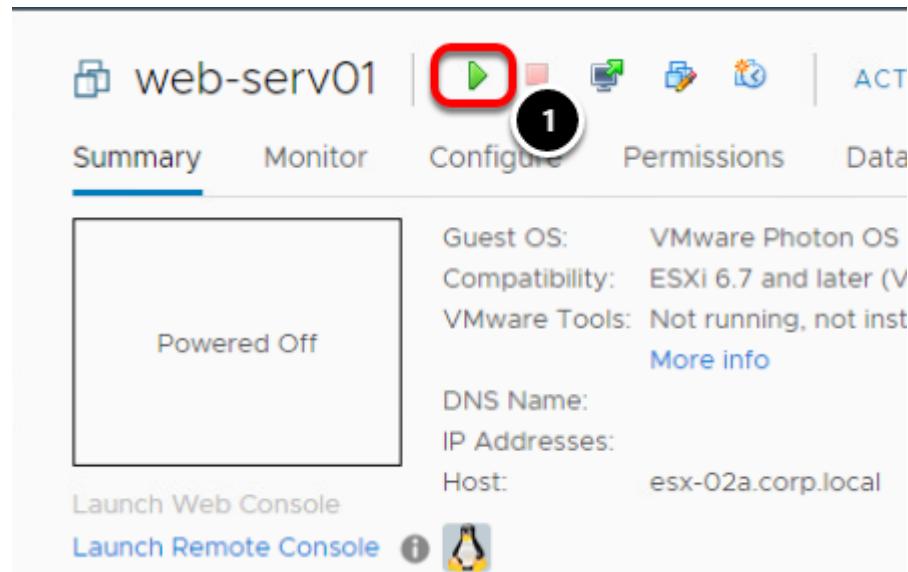


A screenshot of the 'Connect the drive' configuration dialog. The dialog lists various virtual machine components and their settings. The 'CD/DVD drive 1' section is highlighted with a light green background. The 'Content Library ISO File' dropdown is set to 'Content Library ISO File'. To the right of this dropdown, a red box highlights the 'Connect...' checkbox, which is checked. A red circle with the number '1' is placed over this checkbox. A red circle with the number '2' is placed over the 'OK' button, which is highlighted with a red border.

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

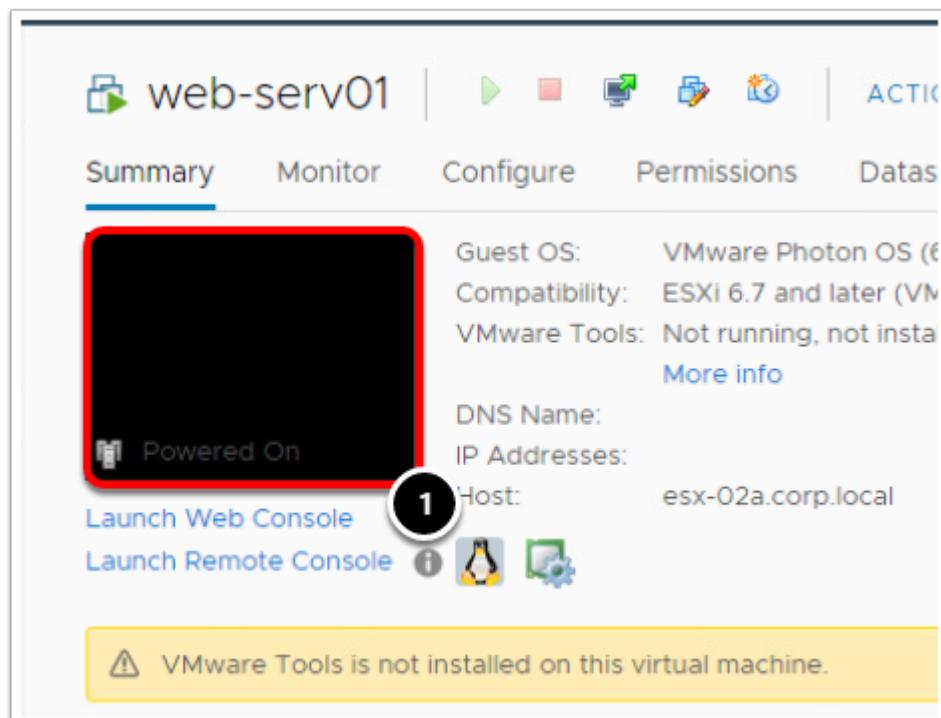
1. Click the **Connected** check box next to **CD/DVD drive 1**.
2. Click **OK**.

Power on web-serv01



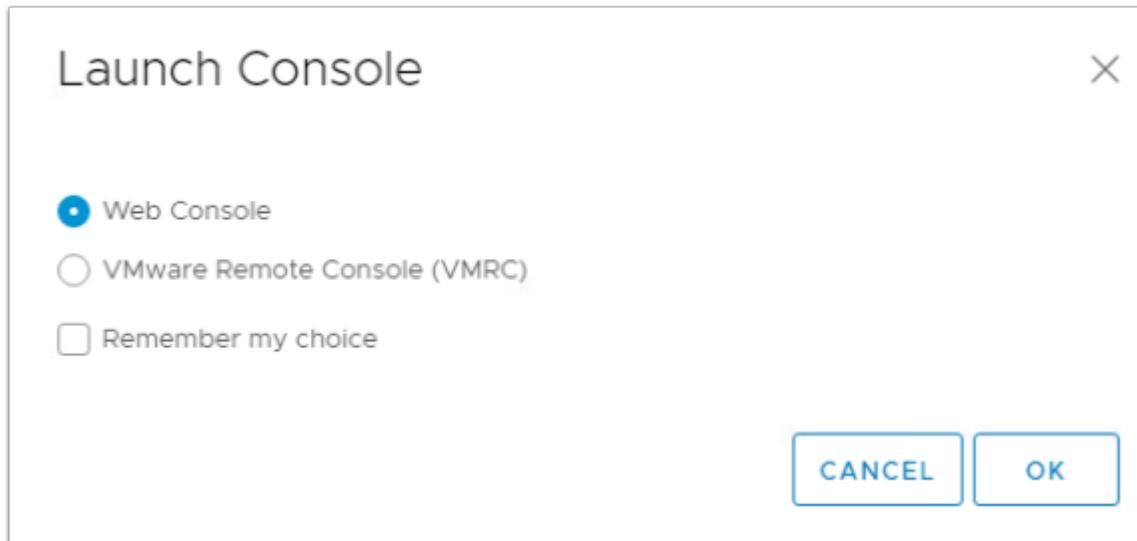
1. Click the **green play button** to power on the virtual machine and start the installation.

Launch Console



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

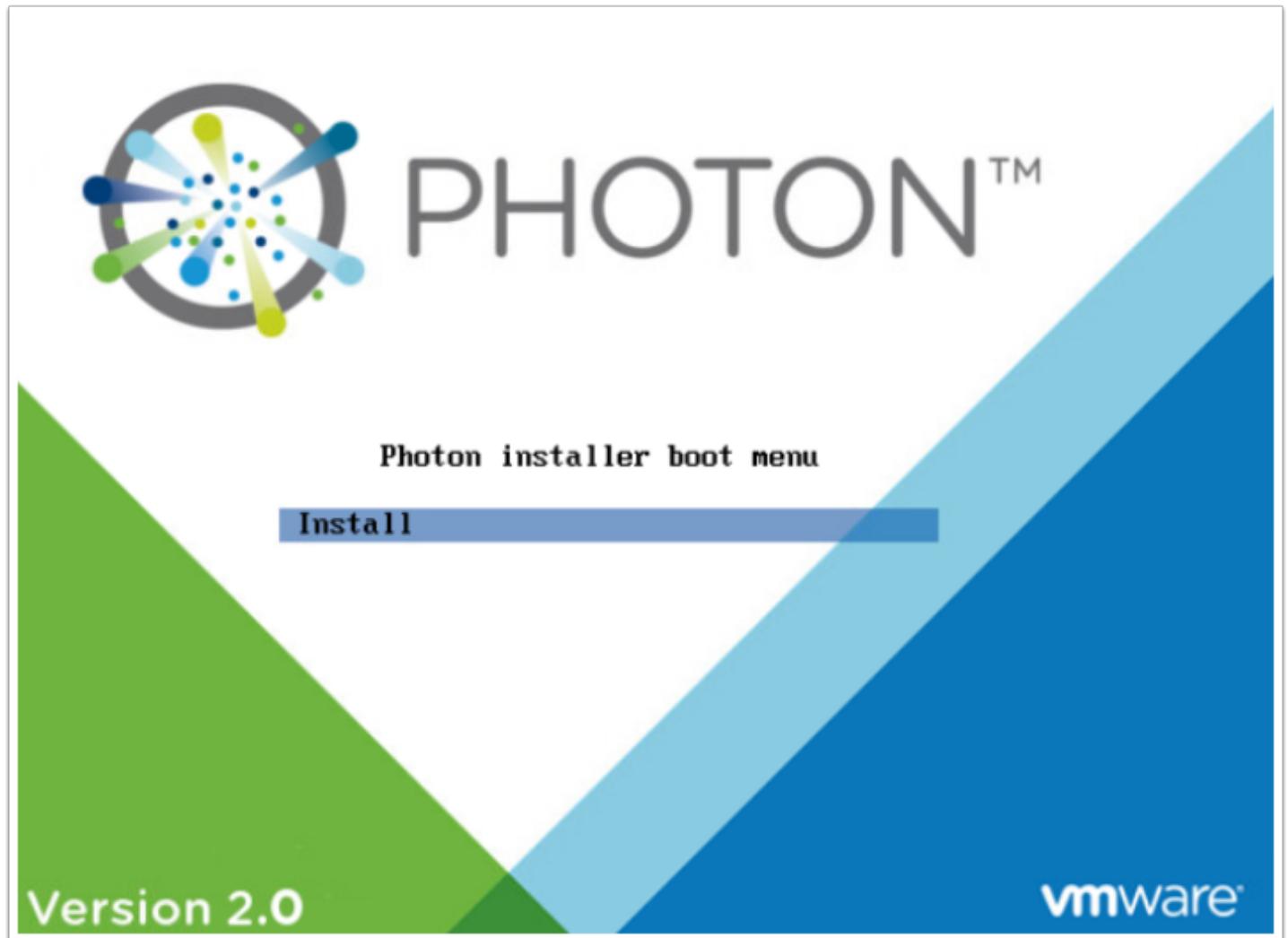
Web Console



1. Select the **Web Console**
2. Click **OK**

Note you also have the option of using the VMware Remote Console (VMRC). This 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.

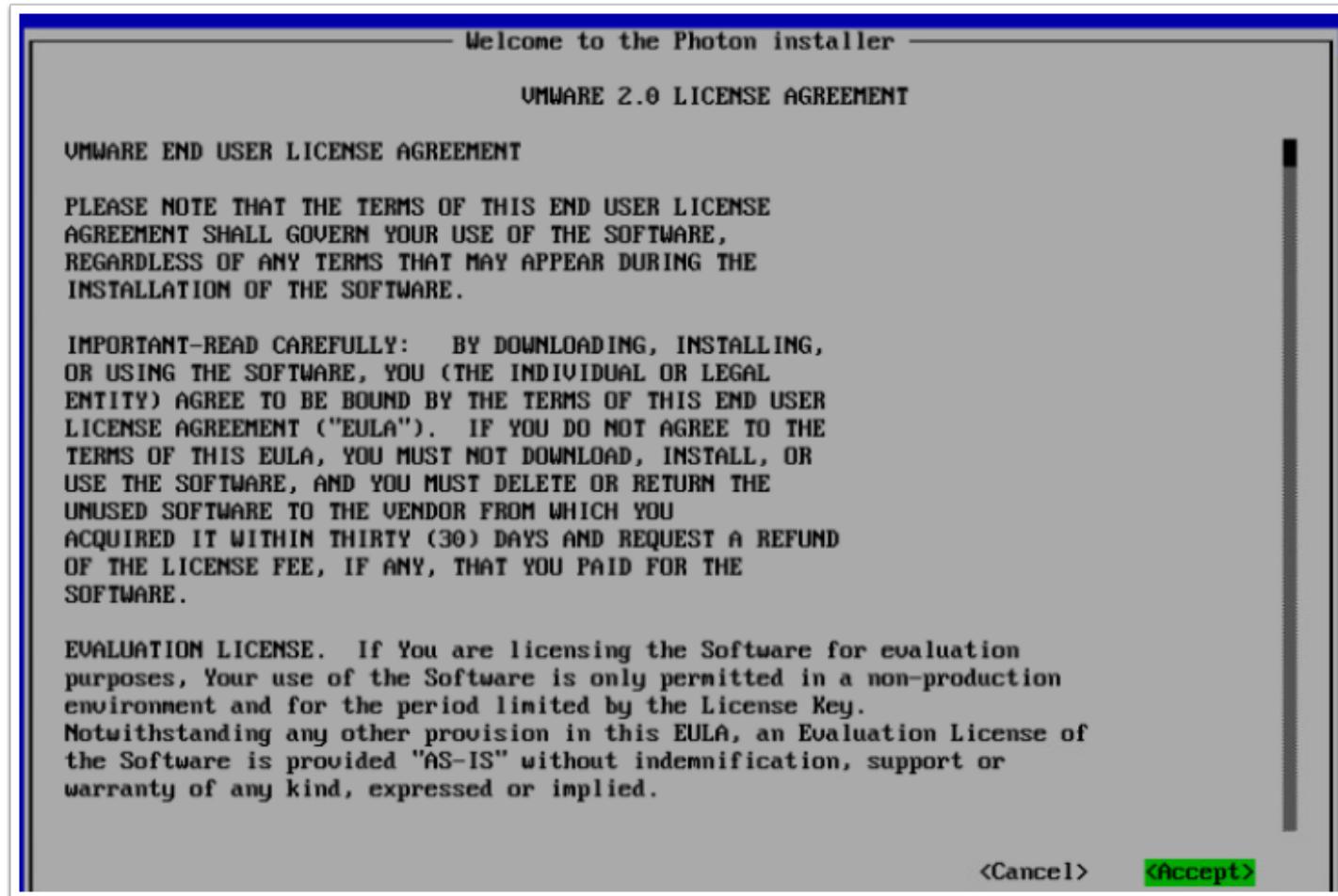
Photon Boot Screen



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.

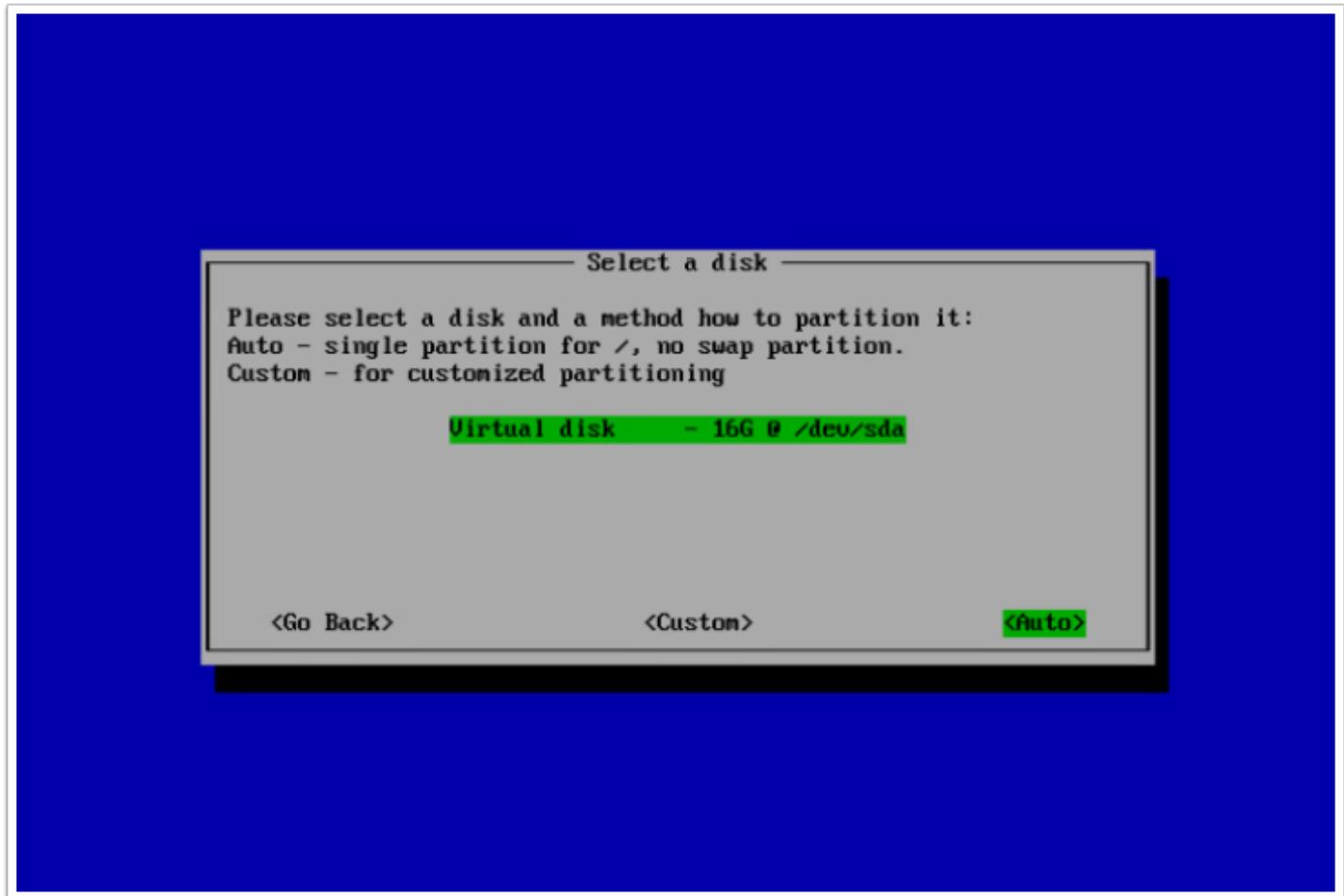
License Agreement



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

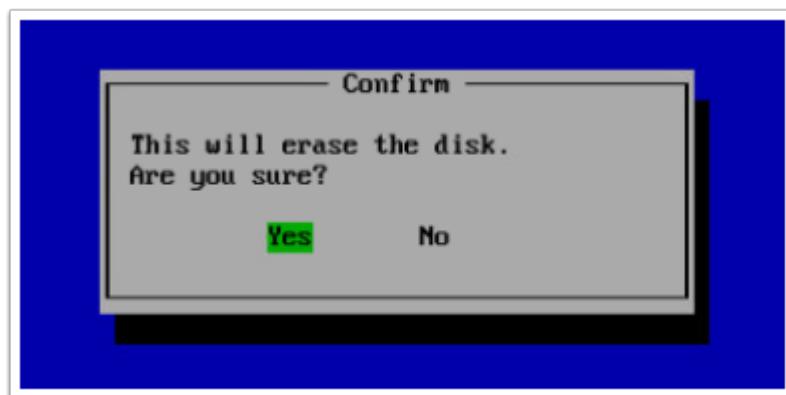
1. Press **Enter** to accept

Select Disk



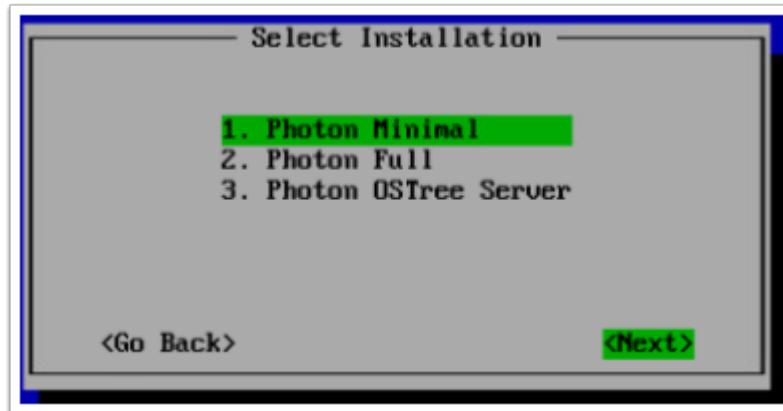
1. Press **Enter** to accept the selected disk and use the auto partitioning option.

Confirm



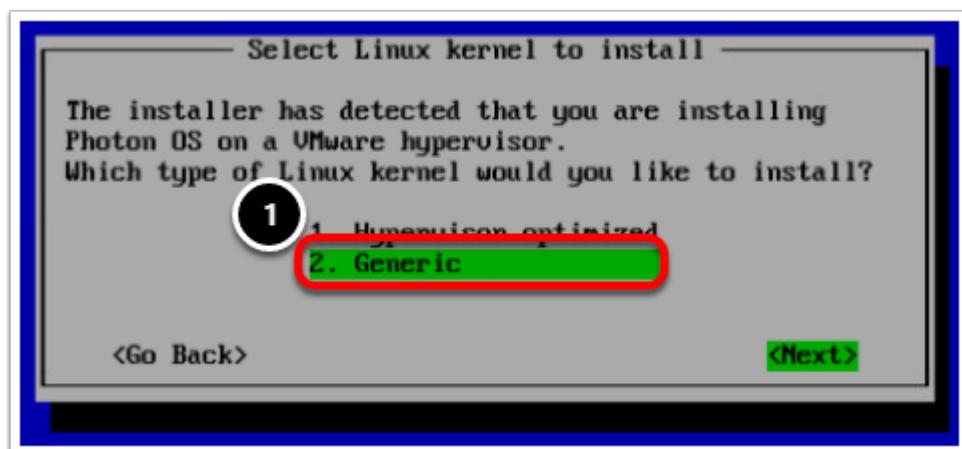
1. Press **Enter** confirm the disk should be erased

Select Installation



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

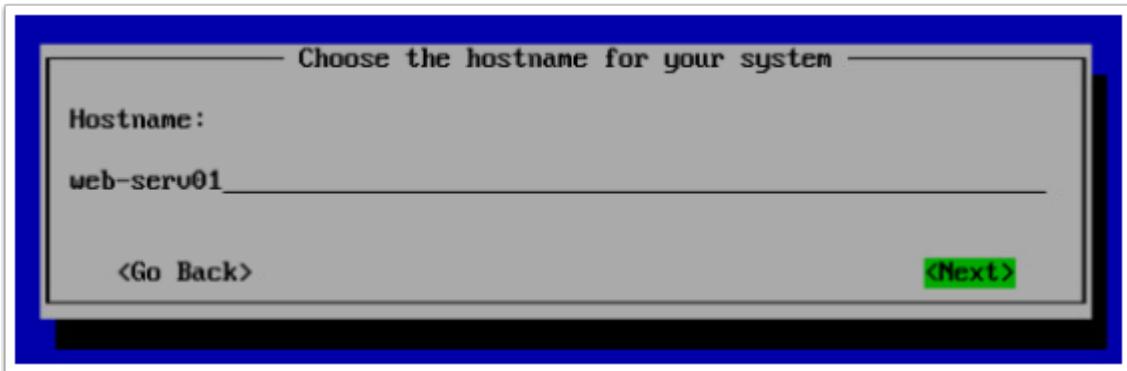
Linux Kernel



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

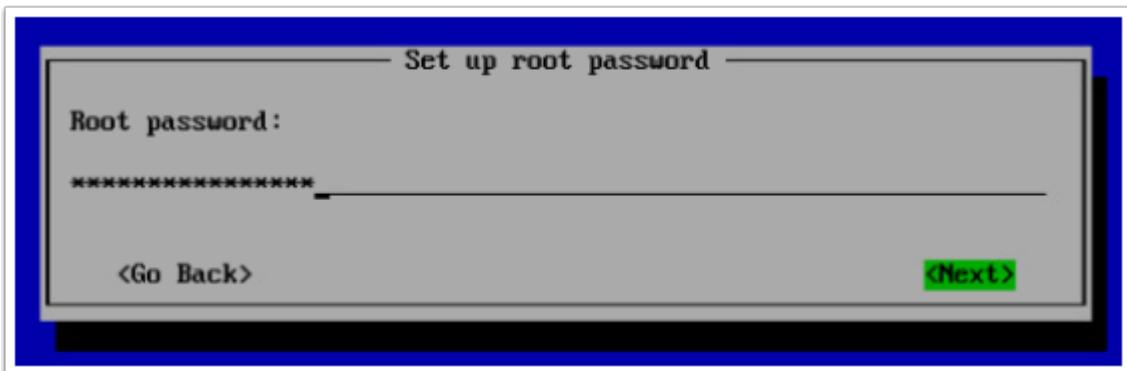
NOTE: If 1. Hypervisor optimized is selected, the virtual machine will not boot. This is due to the unique environment the Hands-on Labs are running in.

Rename Host



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

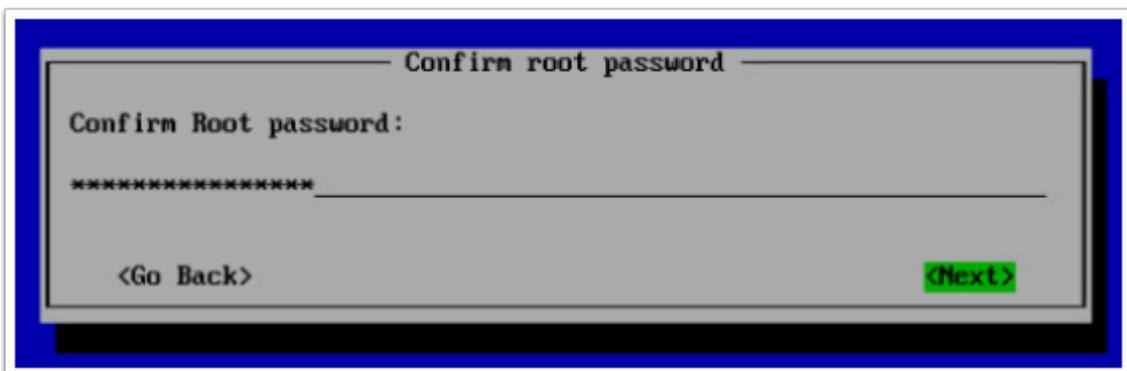
Password



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

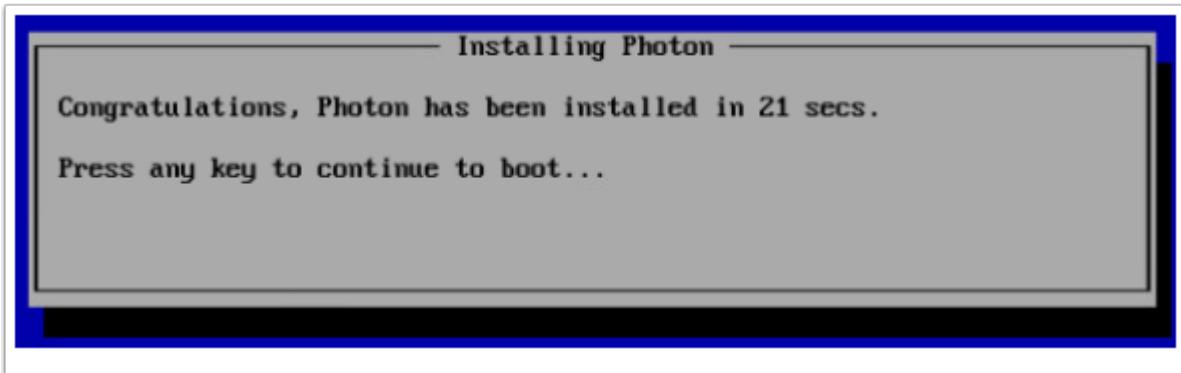
Note that Photon requires a complex, non-dictionary password, which is why the typical password is being repeated.

Confirm Password



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

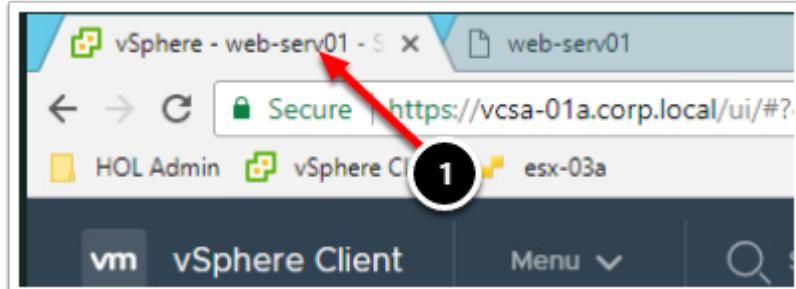
Installation Complete



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 log in prompt.

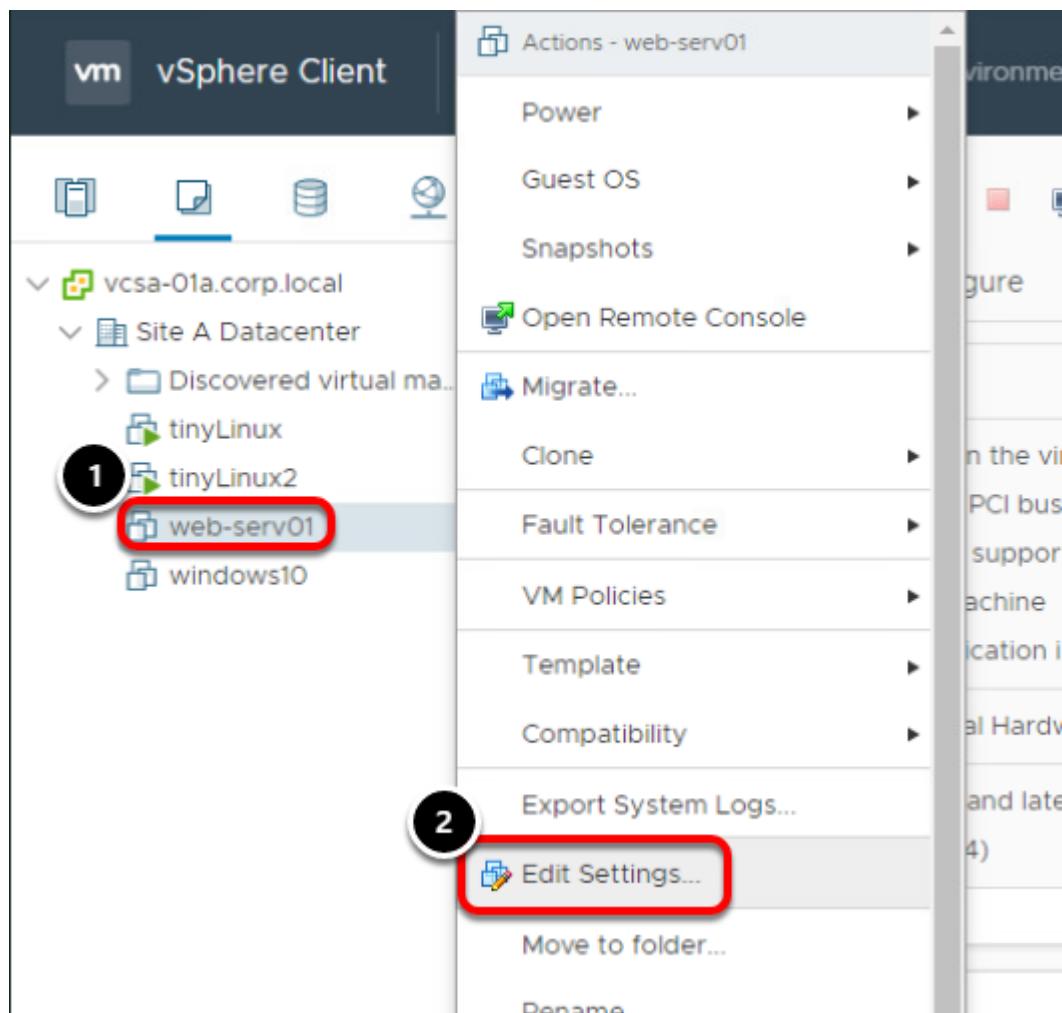
vSphere Tab



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.

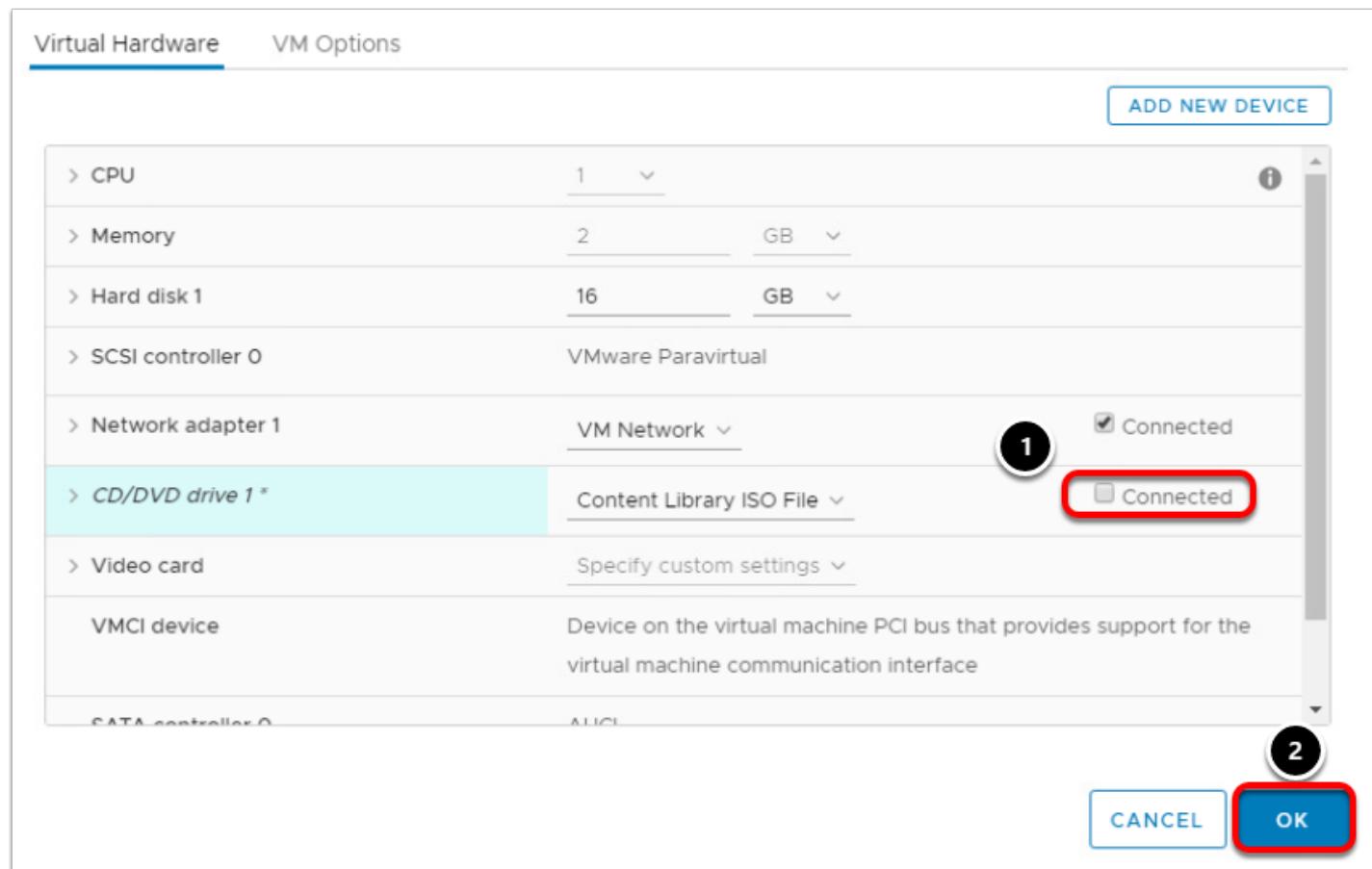
Edit Settings



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

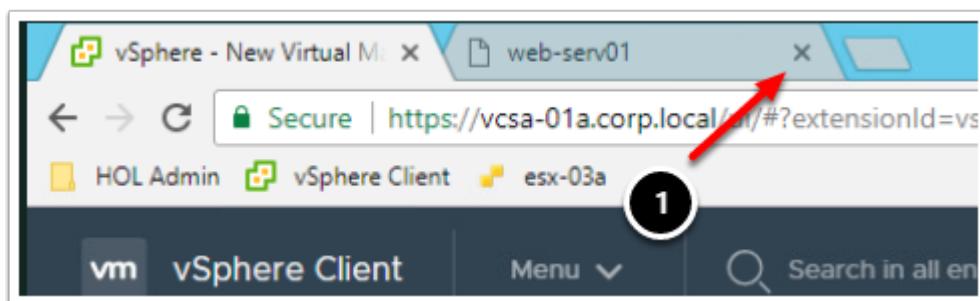
1. Right click on **web-serv01**
2. Select **Edit Settings...**

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

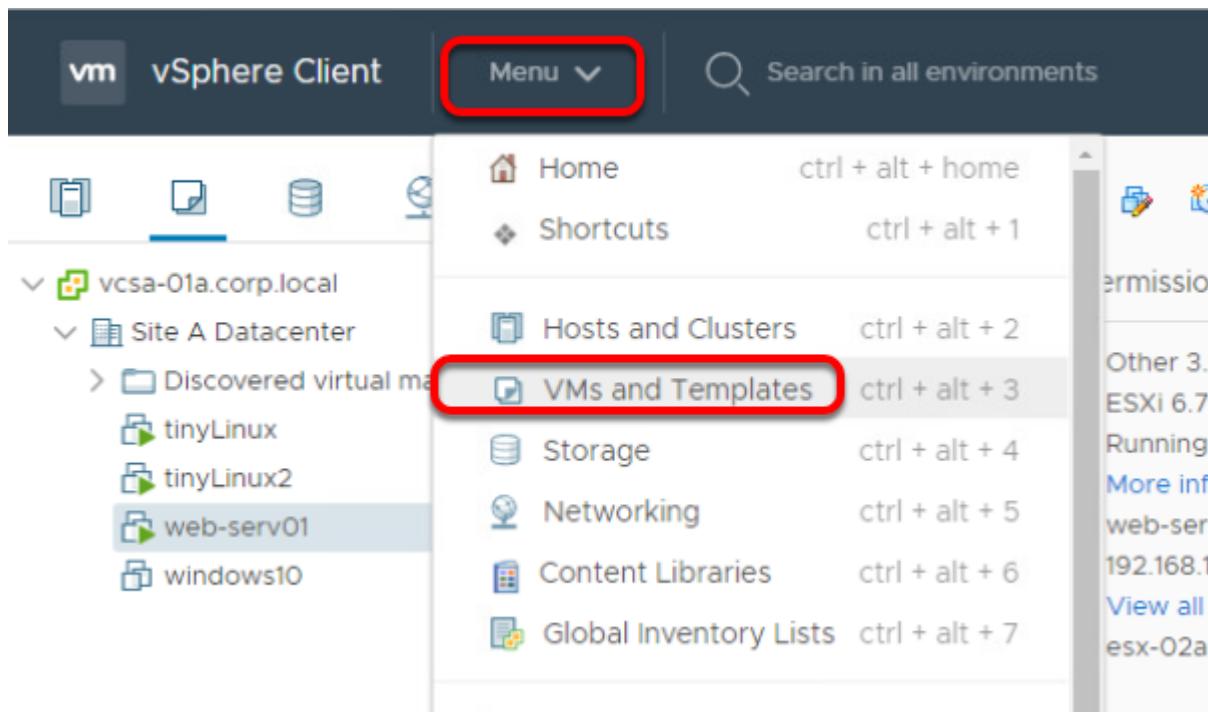
VMware provides several ways to provision vSphere virtual machines. In the last lesson, you saw how to create a virtual machine and manually install the operating system.

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.

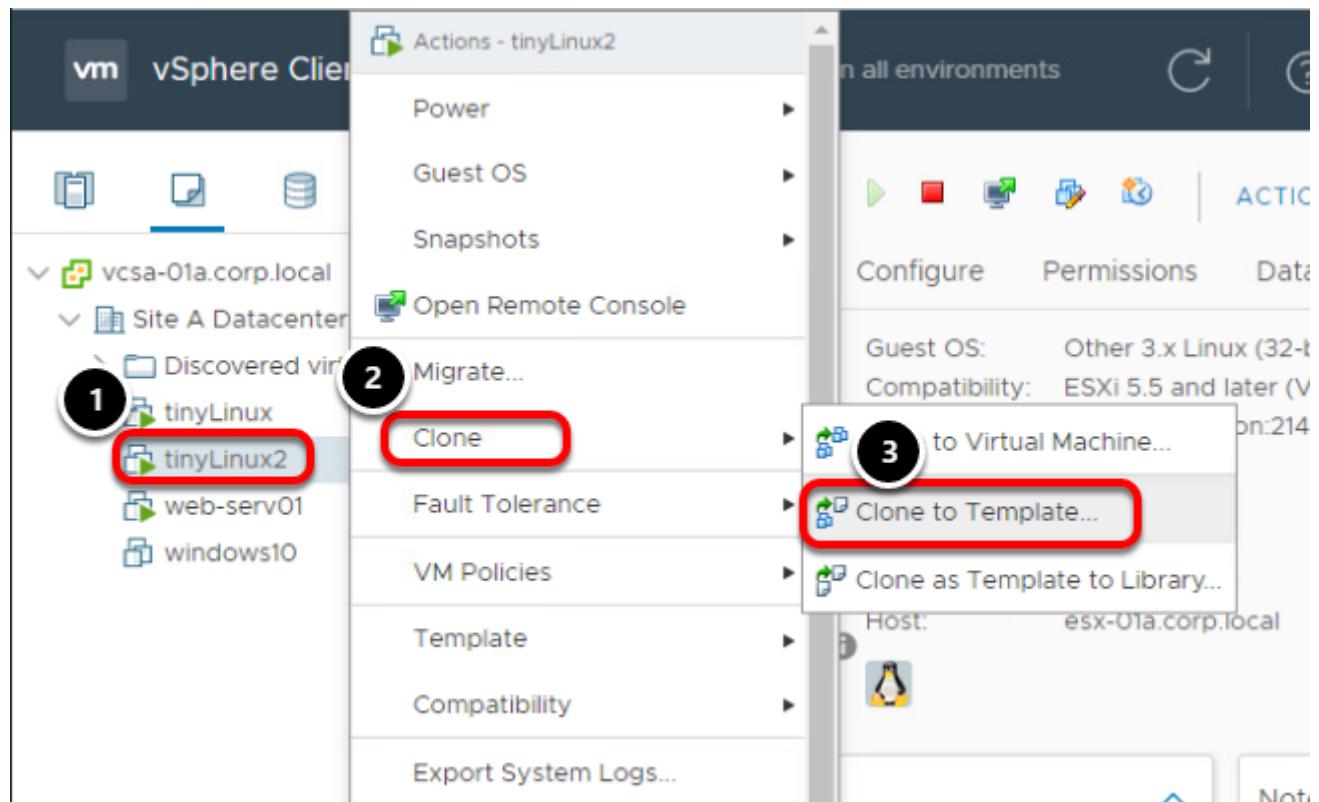
In this lesson, you will clone an existing Virtual Machine to a Template and deploy a new Virtual Machine from that Template.

Navigate to the VMs and Templates management pane



1. Select **VMs and Templates** from the **Menu**.

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

tinyLinux2 - Clone Virtual Machine To Template

1 Select a name and folder 2 Select a compute resource 3 Select storage 4 Ready to complete

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

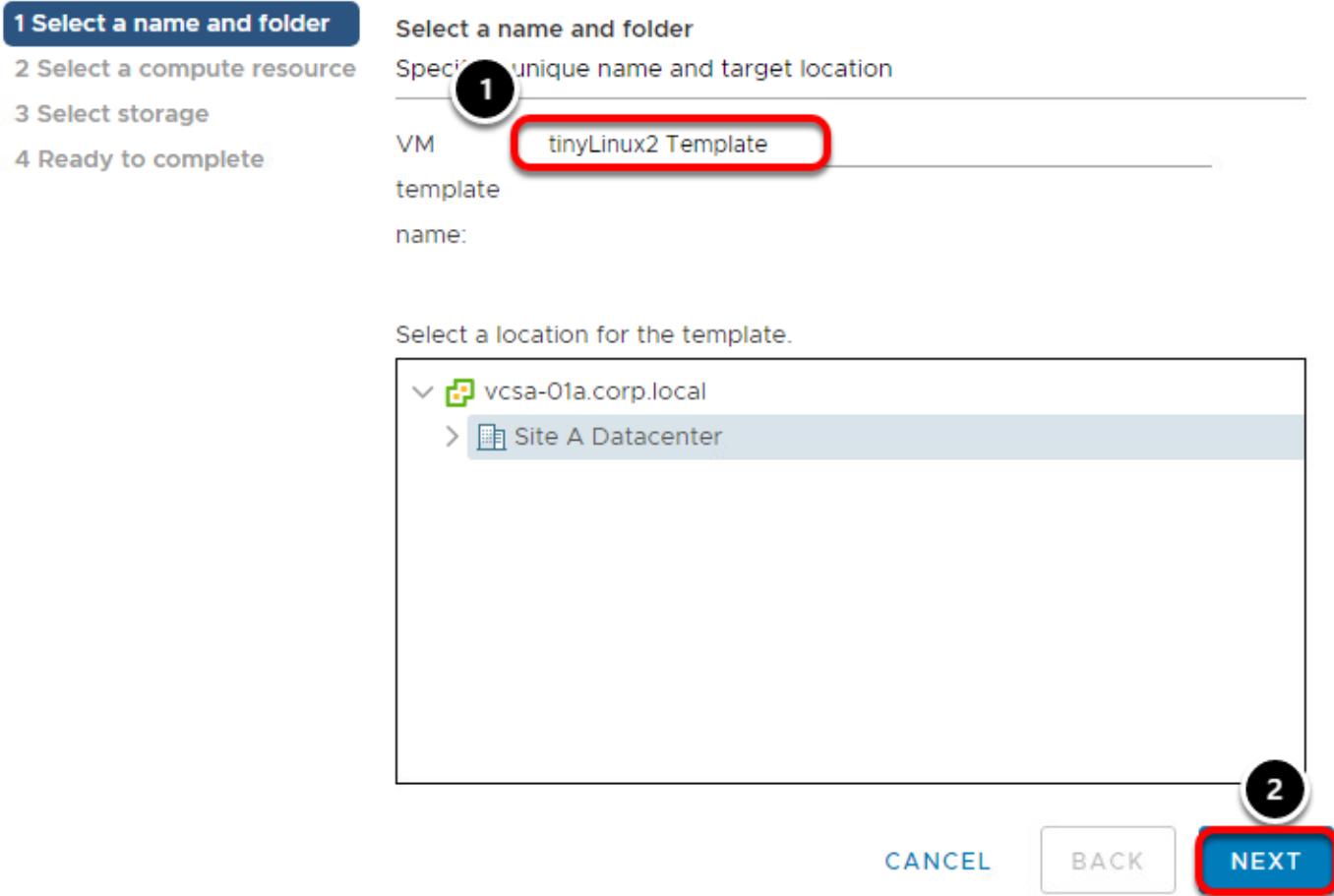
VM template name: **tinyLinux2 Template**

Select a location for the template.

vcsa-01a.corp.local
Site A Datacenter

2

CANCEL BACK **NEXT**



1. In the Clone Virtual Machine to Template wizard, provide a name for the Template - **tinyLinux2 Template**

Please leave the location as **Site A Datacenter** for this lab.

2. Click **Next**

Select Compute Resource

tinyLinux2 - Clone Virtual Machine To Template

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

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

1 Site A Datacenter
2 Site A Cluster 1

Compatibility
✓ Compatibility checks succeeded.

2 CANCEL BACK **NEXT**

Select a compute resource:

1. Choose **Site A Cluster 1**
2. Click **Next**

Select Storage

tinyLinux2 - Clone Virtual Machine To Template

- ✓ 1 Select a name and folder
- ✓ 2 Select a compute resource
- 3 Select storage**
- 4 Ready to complete

Select storage
Select the storage for the configuration and disk files

Configure per disk

Select virtual disk format: **Thin Provision**

VM Storage Policy: **Keep existing VM storage policies**

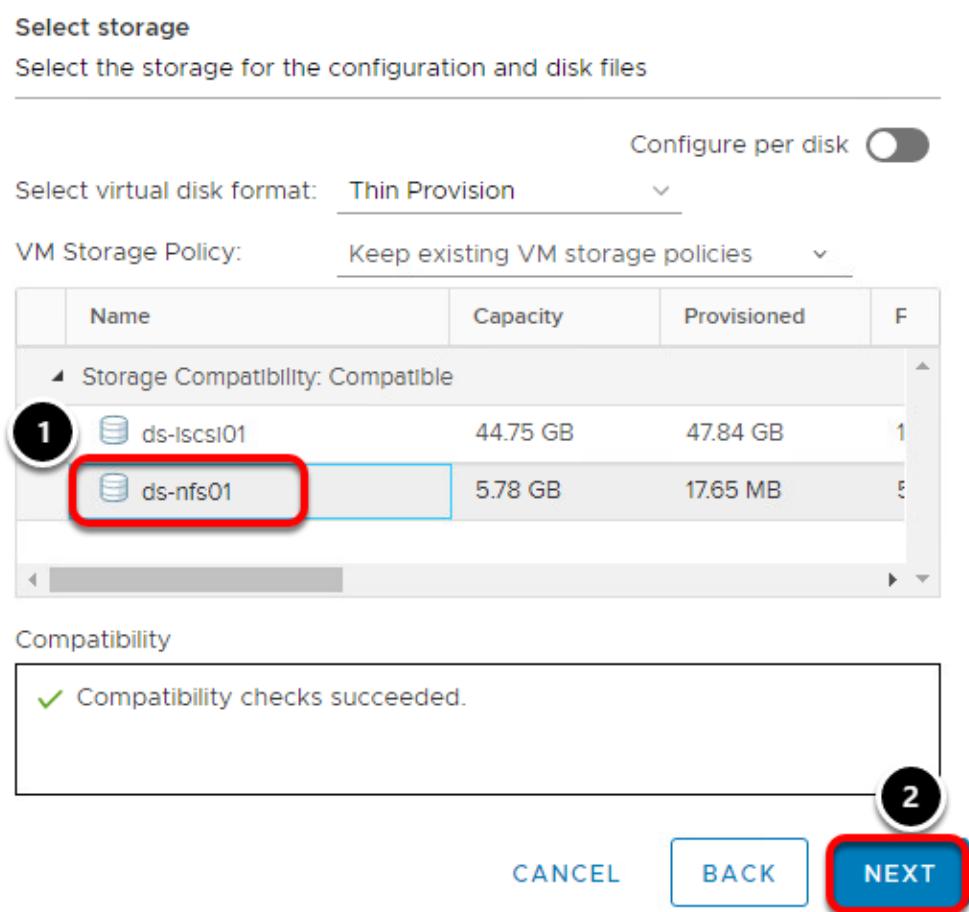
	Name	Capacity	Provisioned	F
▲ Storage Compatibility: Compatible				
1	ds-iscsi01	44.75 GB	47.84 GB	1
	ds-nfs01	5.78 GB	17.65 MB	5

Compatibility

✓ Compatibility checks succeeded.

2

CANCEL **BACK** **NEXT**



1. Select **ds-nfs01** for the datastore
2. Press the **Next** button.

Review the VM Template Settings

tinyLinux2 - Clone Virtual Machine To Template

- ✓ 1 Select a name and folder
- ✓ 2 Select a compute resource
- ✓ 3 Select storage
- 4 Ready to complete**

Ready to complete
Click Finish to start creation.

Provisioning type	Clone virtual machine to template
Source virtual machine	tinyLinux2
Template name	tinyLinux2 Template
Folder	Site A Datacenter
Cluster	Site A Cluster 1
Datastore	ds-nfs01
Disk storage	Thin Provision

CANCEL

BACK

FINISH

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

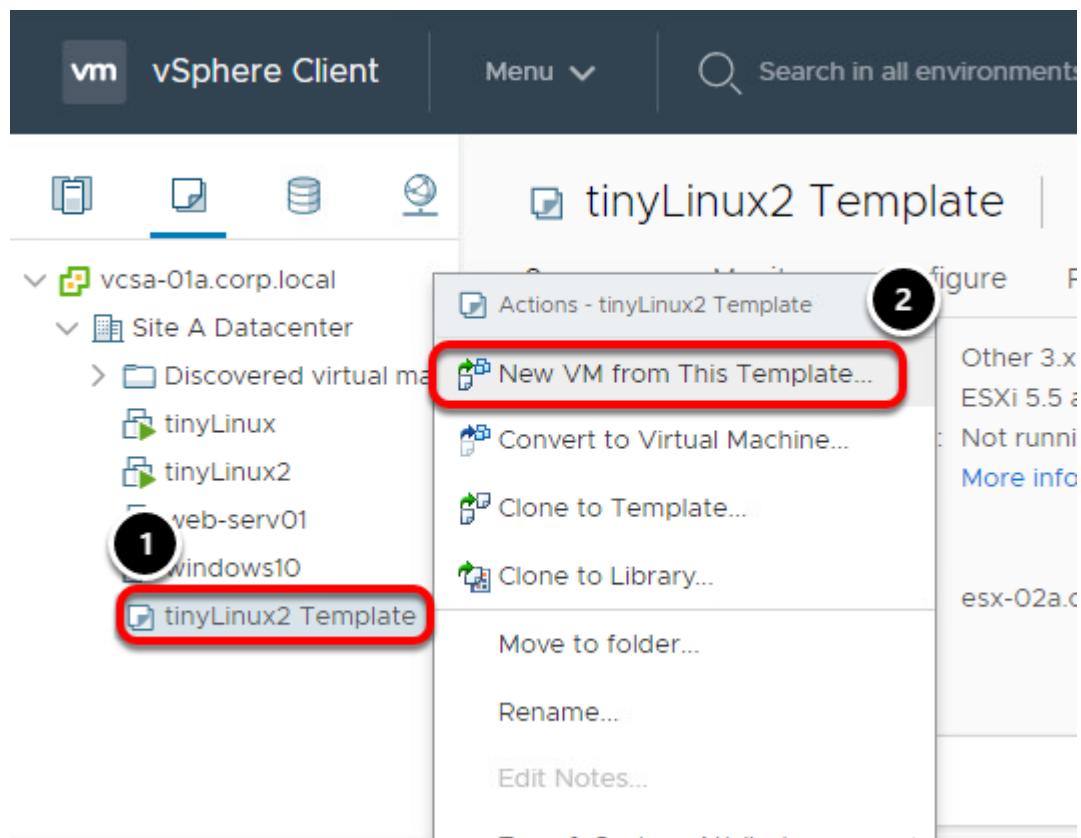
Monitor task progress

The screenshot shows the vSphere Client interface. The inventory pane on the left displays a tree structure of datacenters, hosts, and VMs. A red box highlights the 'tinyLinux2 Template' item under the 'tinyLinux2' folder, with a circled '2' above it. The main pane on the right shows the 'Summary' tab for the 'tinyLinux2' VM, with a red box highlighting the 'Powered On' status and the 'Launch Web Console' and 'Launch Remote Console' buttons. The 'Recent Tasks' table at the bottom shows a completed task: 'Clone virtual machine' with target 'tinyLinux2' and status 'Completed', with a circled '1' above it.

Task Name	Target	Status	Initiator
Clone virtual machine	tinyLinux2	Completed	CORPV

1. Once the task has been completed, you will see the new **tinyLinux2 Template** object in 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

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 a name and folder
Specify a unique name and target location

Virtual machine name: **app-serv01**

Select a location for the virtual machine.

2 vcsa-01a.corp.local
Site A Datacenter

3 CANCEL BACK NEXT

The screenshot shows the 'Select a name and folder' step of a VM deployment wizard. Step 1: The 'Virtual machine name' field contains 'app-serv01', which is highlighted with a red box. Step 2: The 'Select a location for the virtual machine' dropdown shows 'vcsa-01a.corp.local' and 'Site A Datacenter', with 'Site A Datacenter' also highlighted with a red box. Step 3: At the bottom are three buttons: 'CANCEL', 'BACK', and 'NEXT', with 'NEXT' being the only one highlighted with a red box.

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

Select compute resource

tinyLinux2 Template - Deploy From Template

✓ 1 Select a name and folder

2 Select a compute resource

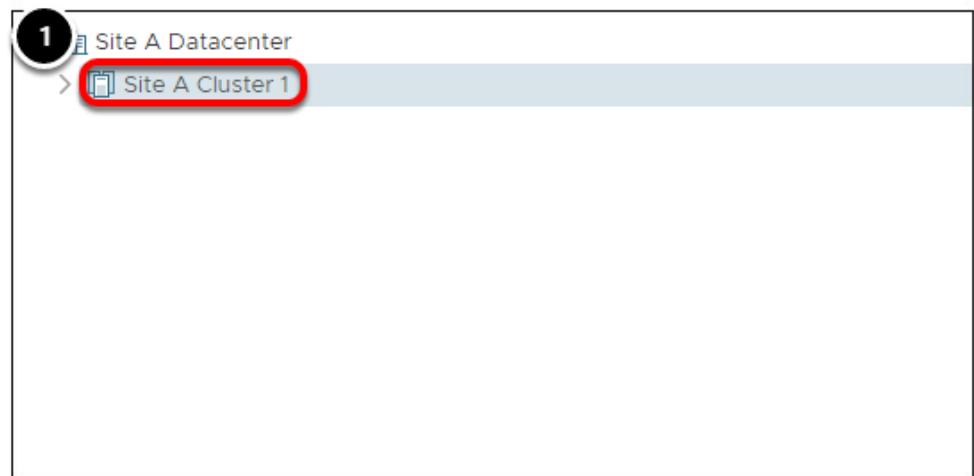
3 Select storage

4 Select clone options

5 Ready to complete

Select a compute resource

Select the destination compute resource for this operation



1 Site A Datacenter
Site A Cluster 1

Compatibility

✓ Compatibility checks succeeded.

2

CANCEL

BACK

NEXT

1. Select **Site A Cluster 1**.
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 policies**

	Name	Capacity	Provisioned	Free
Storage Compatibility: Compatible				
1	ds-iscsi01	44.75 GB	47.84 GB	12.18 GB
	ds-nfs01	5.78 GB	550.3 MB	5.78 GB

Compatibility

✓ Compatibility checks succeeded.

2

CANCEL

BACK

NEXT

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

Select clone options

tinyLinux2 Template - Deploy From Template

- ✓ 1 Select a name and folder
- ✓ 2 Select a compute resource
- ✓ 3 Select storage

Select clone options

Select further clone options

4 Select clone options

5 Ready to complete

Customize the operating system

Customize this virtual machine's hardware

Power on virtual machine after creation



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
- ✓ 2 Select a compute resource
- ✓ 3 Select storage
- ✓ 4 Select clone options

5 Ready to complete

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Source template	tinyLinux2 Template
Virtual machine name	app-serv01
Folder	Site A Datacenter
Cluster	Site A Cluster 1
Datastore	ds-iscsi01
Disk storage	Same format as source



1. Review the deployment options and then click **Finish**.

Monitor task progress

The screenshot shows the vSphere Web Client interface. On the left, the inventory pane displays a tree structure with 'vcsa-01a.corp.local' expanded, showing 'Site A Datacenter', 'Discovered VMs', and several VMs: 'app-serv01' (circled with number 2), 'tinyLinux', 'tinyLinux2', 'web-serv01', 'windows10', and 'tinyLinux2 Template'. The 'tinyLinux2 Template' is highlighted. On the right, the 'Summary' tab for 'tinyLinux2 Template' is selected, showing details like Guest OS: 'Other 3.x Linux (32-bit)', Compatibility: 'ESXi 5.5 and later (VM v', and Host: 'esx-02a.corp.local'. Below the summary is a 'VM Hardware' section. At the bottom, the 'Recent Tasks' window is open, showing a table with columns 'Task Name', 'Target', 'Status', and 'Initiator'. A task named 'Clone virtual machine' is listed, with 'tinyLinux2 Templ...' as the target, a green checkmark in the status column, and 'CORP\Administrator' as the initiator. This task is also circled with number 1.

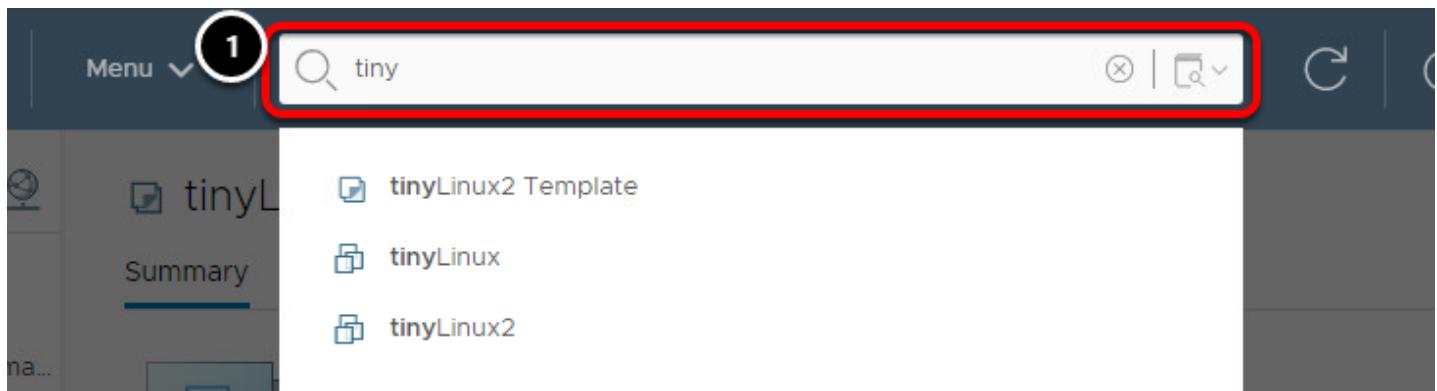
Task Name	Target	Status	Initiator
Clone virtual machine	tinyLinux2 Templ...	✓ Completed	CORP\Administrator

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



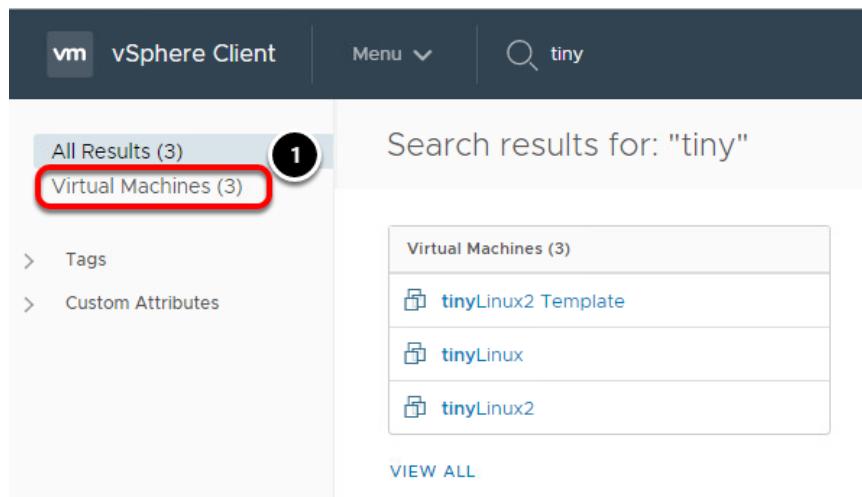
At the top of the vSphere Client is a search bar that can be used to find objects quickly. This can be an object's name, like app-serv01 or an ESXi host. Tags can also be attached to objects and the search feature can be used to find them as well.

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



The screenshot shows the vSphere Client interface with a search query of "tiny" entered in the search bar. The search results are displayed in a central pane, with a total of 3 results. A red box highlights the "Virtual Machines (3)" link in the search results list. The left sidebar shows navigation options: "All Results (3)" (selected), "Virtual Machines (3)" (highlighted with a red box and a circled '1' indicating new items), "Tags", and "Custom Attributes".

Virtual Machines (3)
 tinyLinux2 Template
 tinyLinux
 tinyLinux2

[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

Search results for: "tiny"

Name ↑	State
tinyLinux2 Template	Powered Off

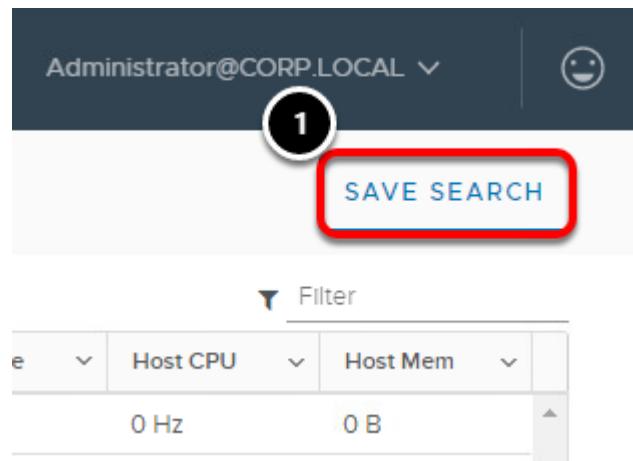
You can then filter the results down even further by specifying:

- 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.

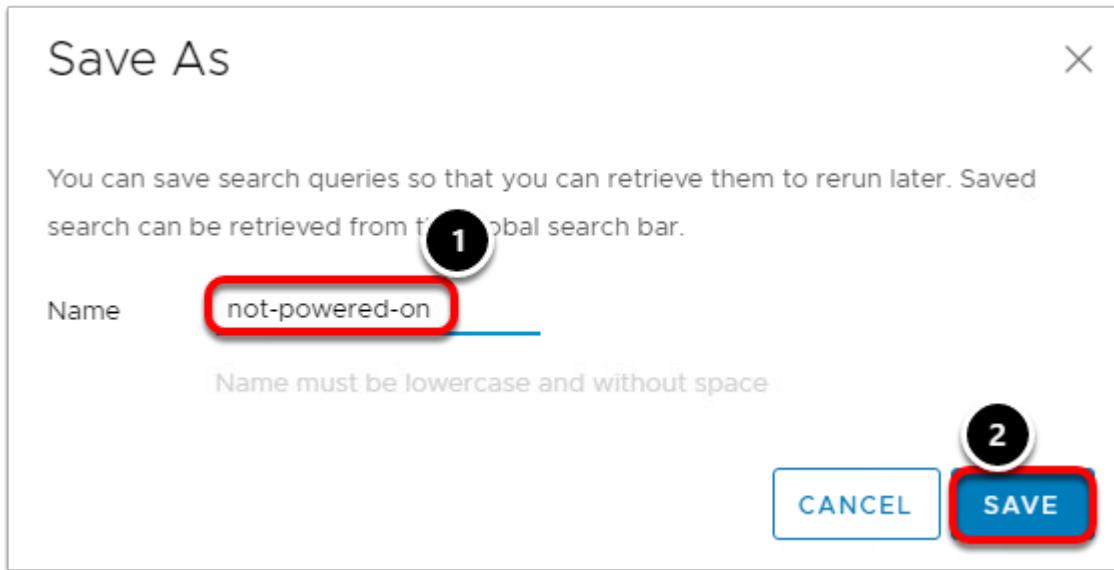
Save the Search



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

The screenshot shows the vSphere Web Client interface. At the top, there is a search bar with the placeholder "Search in all environments" (circled 1). To the right of the search bar is a magnifying glass icon with a drop-down arrow (circled 2). A tooltip is displayed, showing two saved search results: "#tiny-vms" and "#not-powered-on". A red arrow points from the text "#tiny-vms" in the tooltip to the "#tiny-vms" entry in the list. Below the search bar, the text "Search: '#not-powered-on'" and "Search results for: 'tiny'" is displayed. The main table shows a single row for "tinyLinux2 Template" with the following details: State: Powered Off, Status: Normal, Provisioned Space: 550.22 MB, Used Space: 2 KB. The table has columns for Name, State, Status, Provisioned Space, and Used Space.

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 **#tiny-vms**

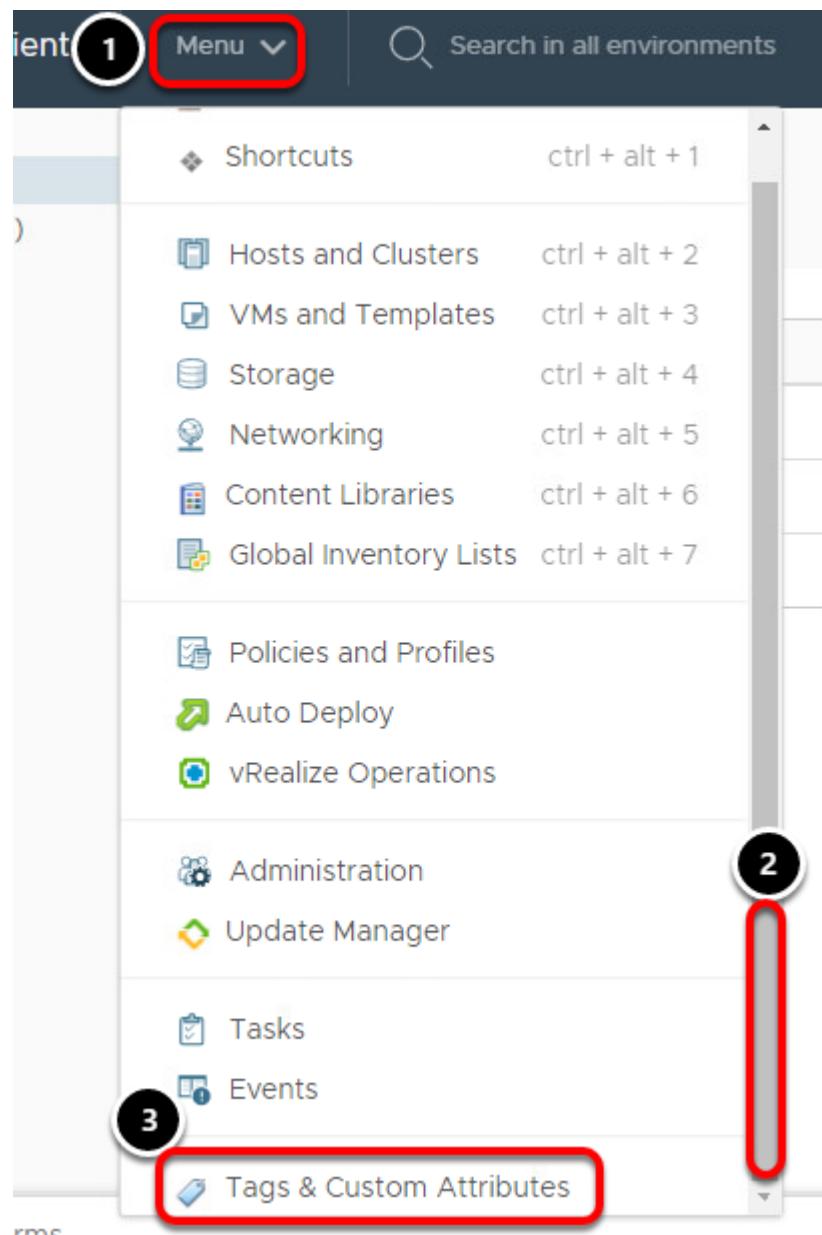
Tiny-VMs

The screenshot shows the results of the saved search "#tiny-vms". At the top, it displays "Saved Search: '#tiny-vms'" and "Search results for: 'tiny'". The main content area shows a table titled "Virtual Machines (3)" with three entries: "tinyLinux2 Template", "tinyLinux", and "tinyLinux2". Each entry has a small icon to its left. At the bottom left, there is a "VIEW ALL" link. On the right side, there is a "ACTIONS" menu (circled 1) with options: "Save as", "Rename", and "Delete". The "Actions" menu is highlighted with a red box.

This was a previously created saved search and shows the results for objects that contain **tiny**.

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

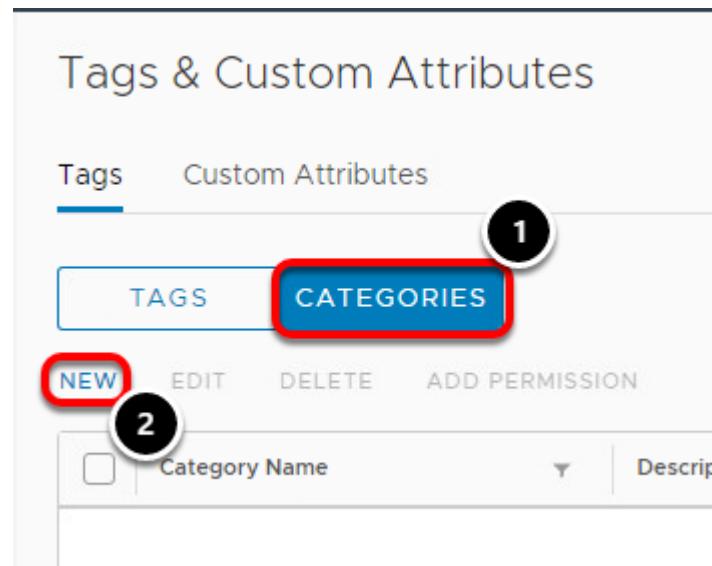
Tags and Custom Attributes



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



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

Add Category

Category Name: **1**

Description: **2**

Tags Per Object: **3** One tag Many tags

Associable Object Types:

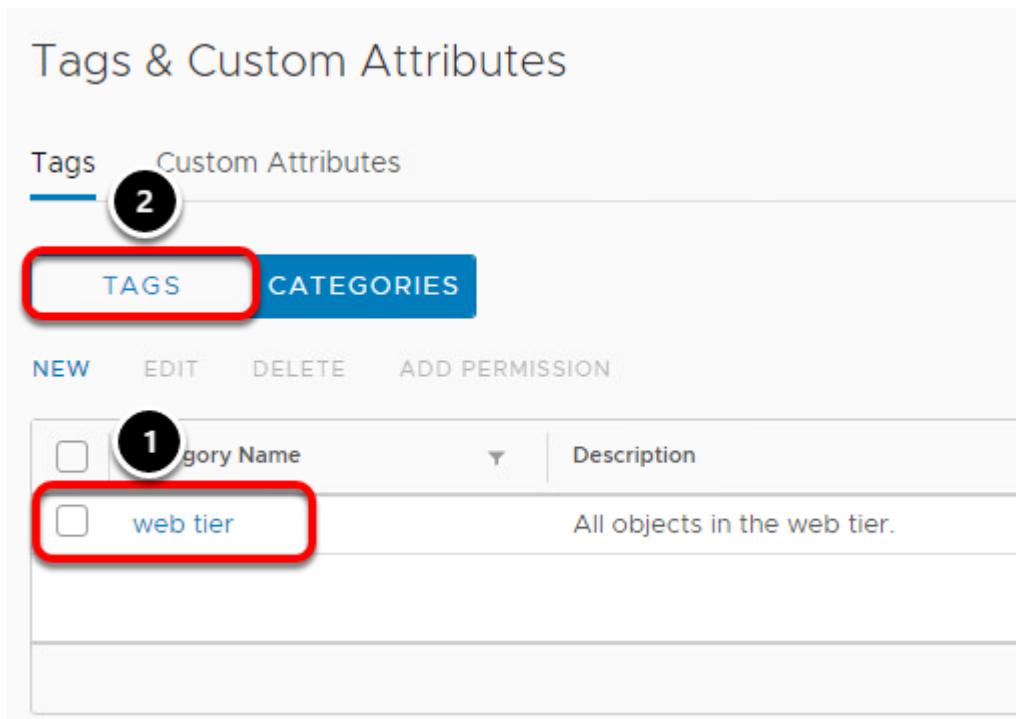
<input checked="" type="checkbox"/> All objects	<input checked="" type="checkbox"/> Cluster	<input checked="" type="checkbox"/> Datacenter
<input checked="" type="checkbox"/> Folder	<input checked="" type="checkbox"/> Datastore Cluster	<input checked="" type="checkbox"/> Distributed Port Group
<input checked="" type="checkbox"/> Datastore	<input checked="" type="checkbox"/> Host	<input checked="" type="checkbox"/> Content Library
<input checked="" type="checkbox"/> Distributed Switch	<input checked="" type="checkbox"/> Network	<input checked="" type="checkbox"/> Resource Pool
<input checked="" type="checkbox"/> Library Item	<input checked="" type="checkbox"/> Virtual Machine	
<input checked="" type="checkbox"/> vApp		

4

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 per object**"
4. Click "**OK**"

Create a New Tag



Tags & Custom Attributes

Tags Custom Attributes **2**

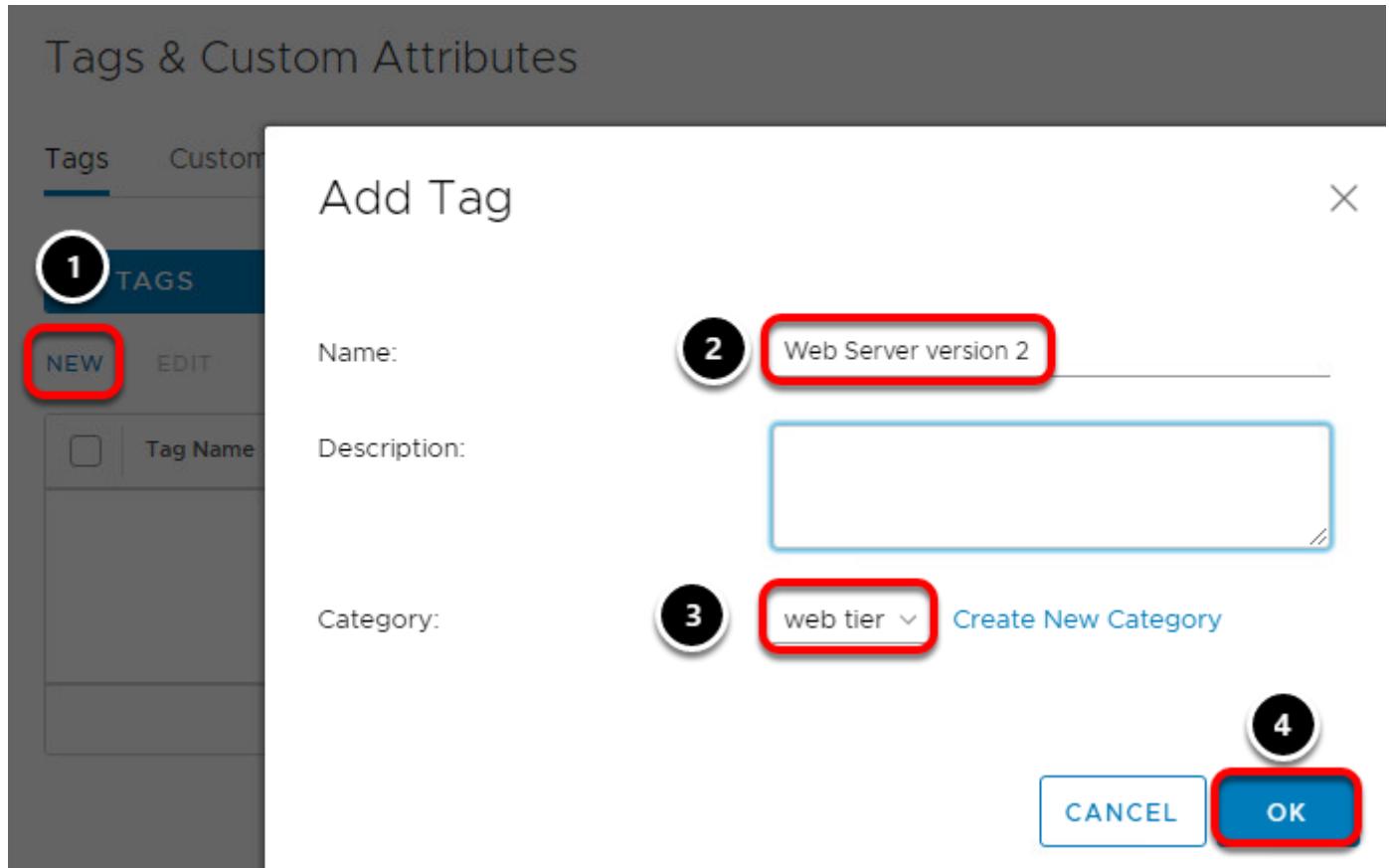
TAGS **CATEGORIES**

NEW EDIT DELETE ADD PERMISSION

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

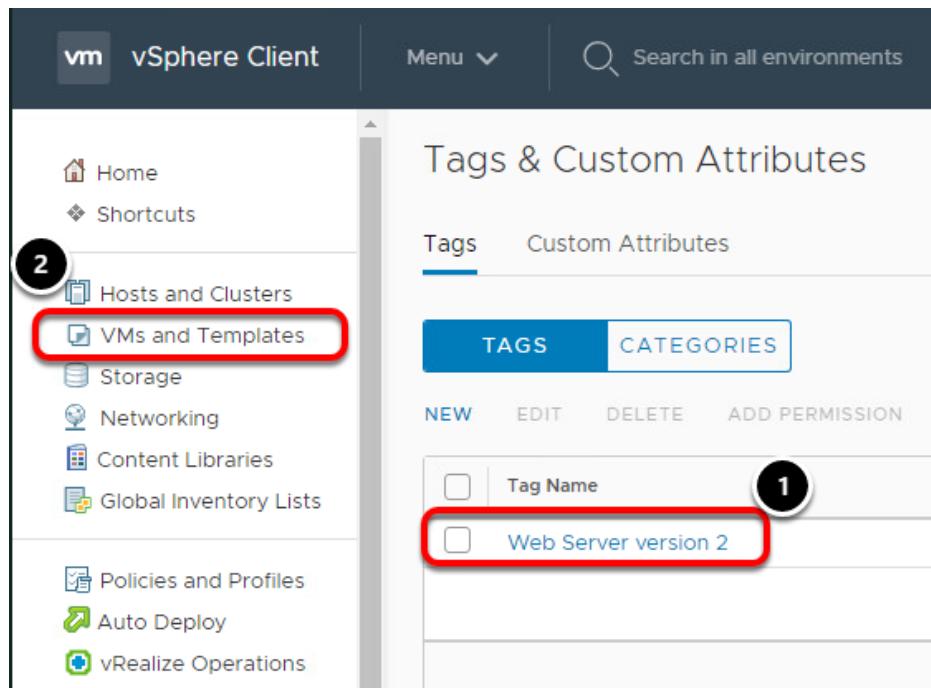
1. The new category has been created.
2. Click the **Tags** tab to create a new a Tag.

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 **OK**

New Tag



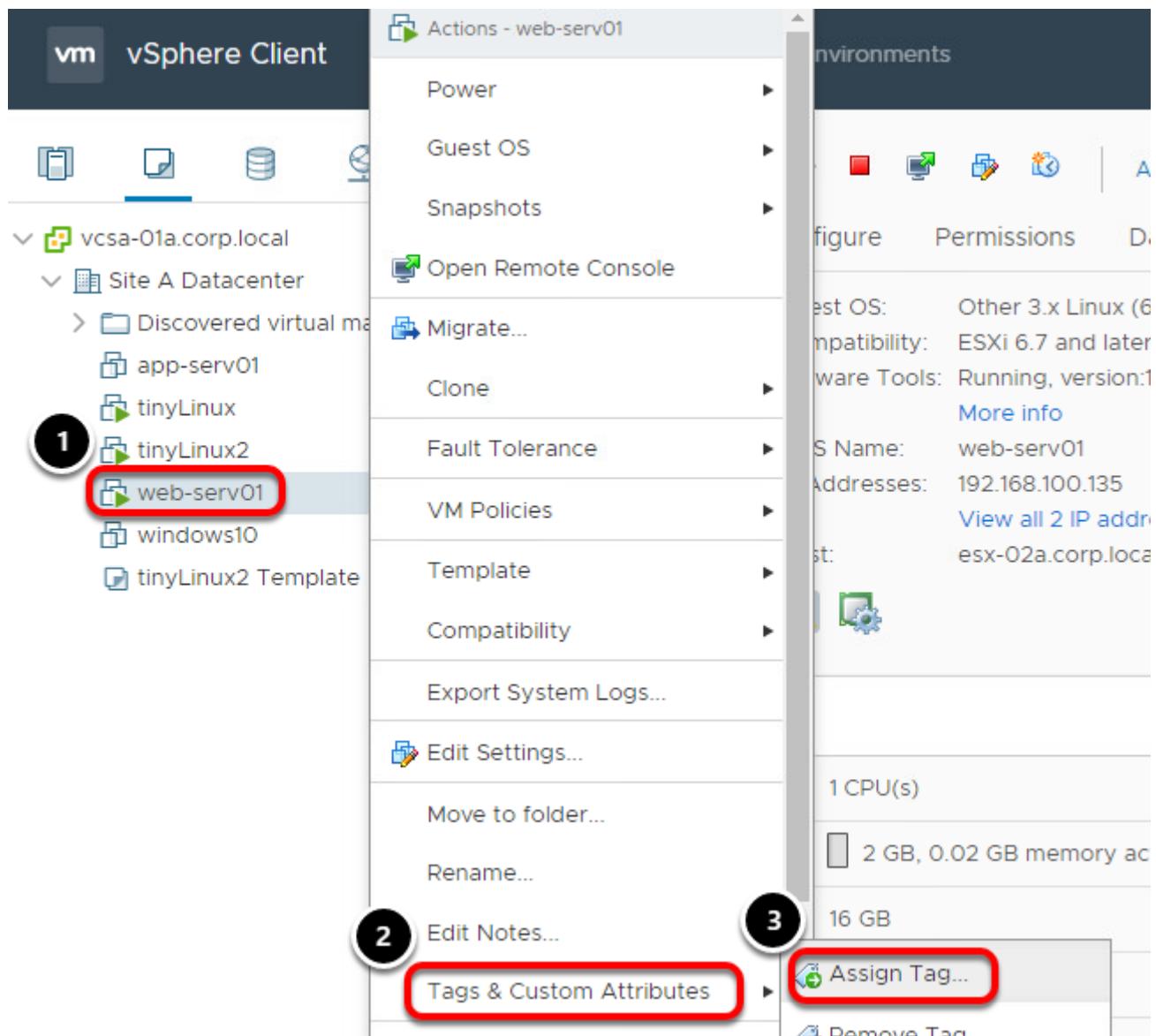
The screenshot shows the vSphere Client interface. The left sidebar has a 'VMs and Templates' item highlighted with a red box and a circled '2'. The main content area is titled 'Tags & Custom Attributes' and shows the 'Tags' tab selected. A table lists a single tag: 'Web Server version 2', which is also highlighted with a red box and a circled '1'.

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

Assign Tag | web-serv01

ADD TAG

Tag Name	Category	Description
<input checked="" type="checkbox"/> Web Server version 2	web tier	

1 of 1 1 - 1 of 1

2 CANCEL ASSIGN

1. Click the **Web Server version 2** tag.
2. Click **Assign**.

Search Using Tags

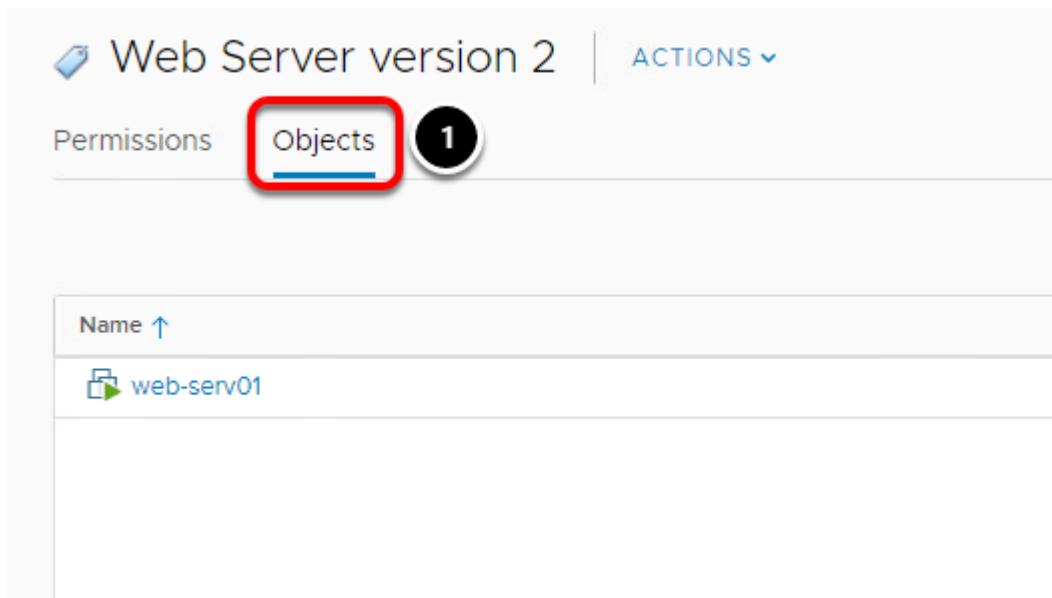
Search: we

- web tier
- Web Server version 2
- web-serv01

[View all results](#)

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

Search Results



Web Server version 2 | ACTIONS ▾

Permissions Objects 1

Name ↑

web-serv01

1. Click on the **Objects** tab to find the list of objects which have been assigned the **Web Server version 2** tag.

Understanding vSphere Availability and Distributed Resource Scheduler (DRS)

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.

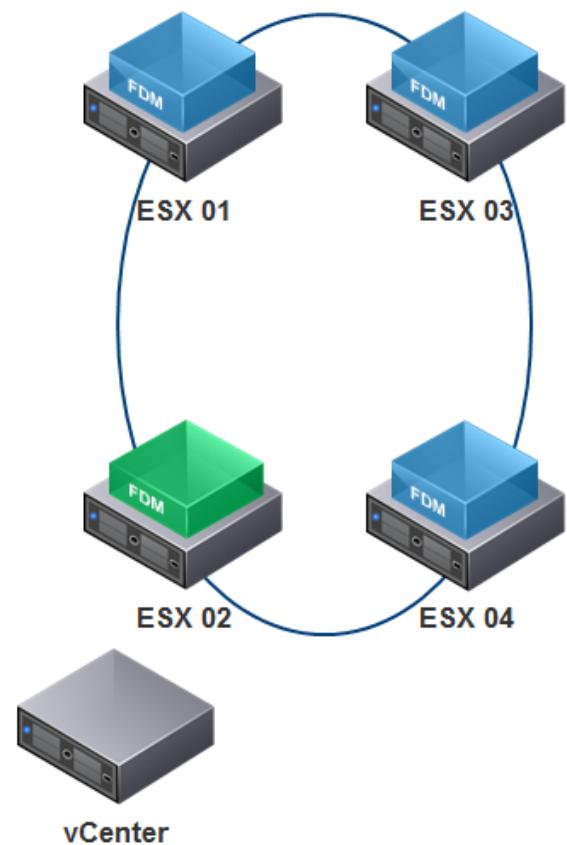
What is vSphere Availability?

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.

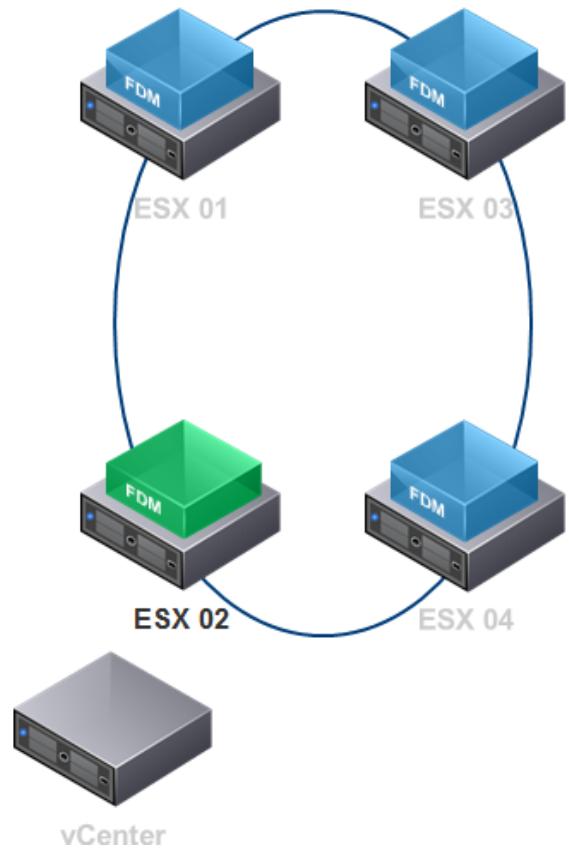
vSphere Availability Primary Components

- **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**



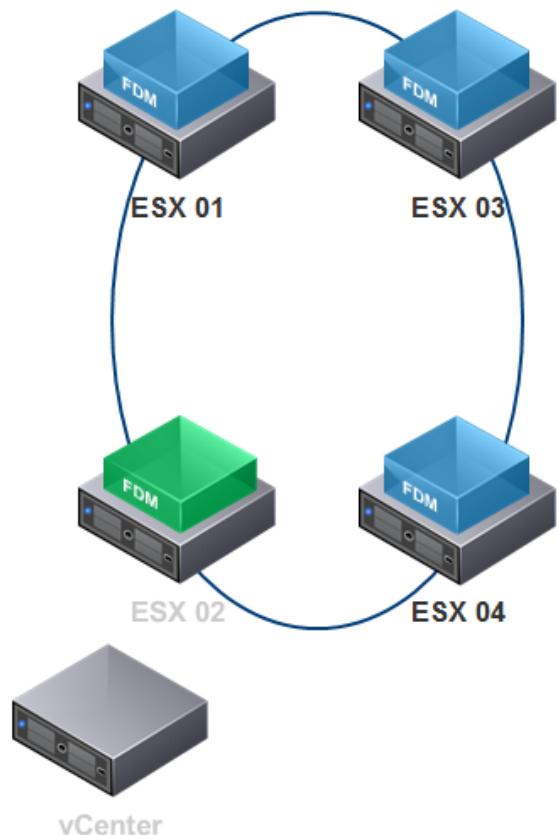
The Master Role

- **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.



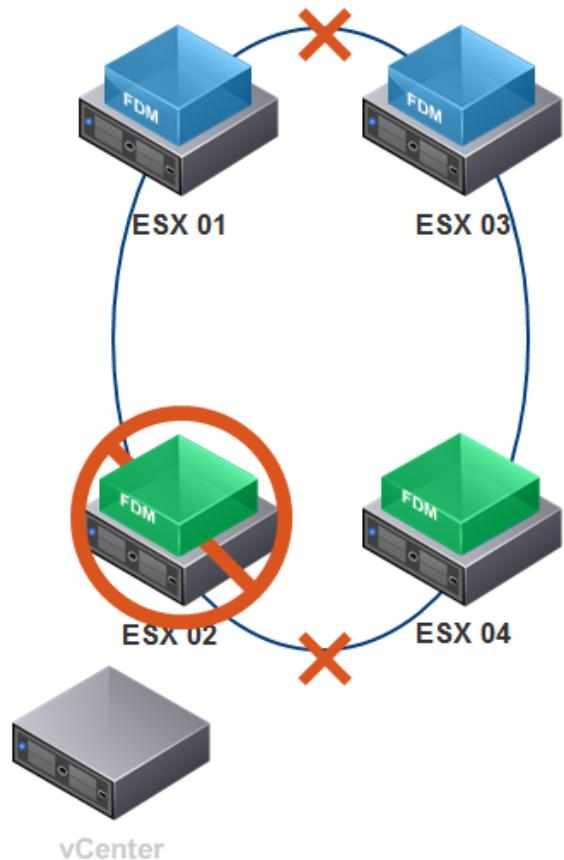
The Slave Role

- 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.

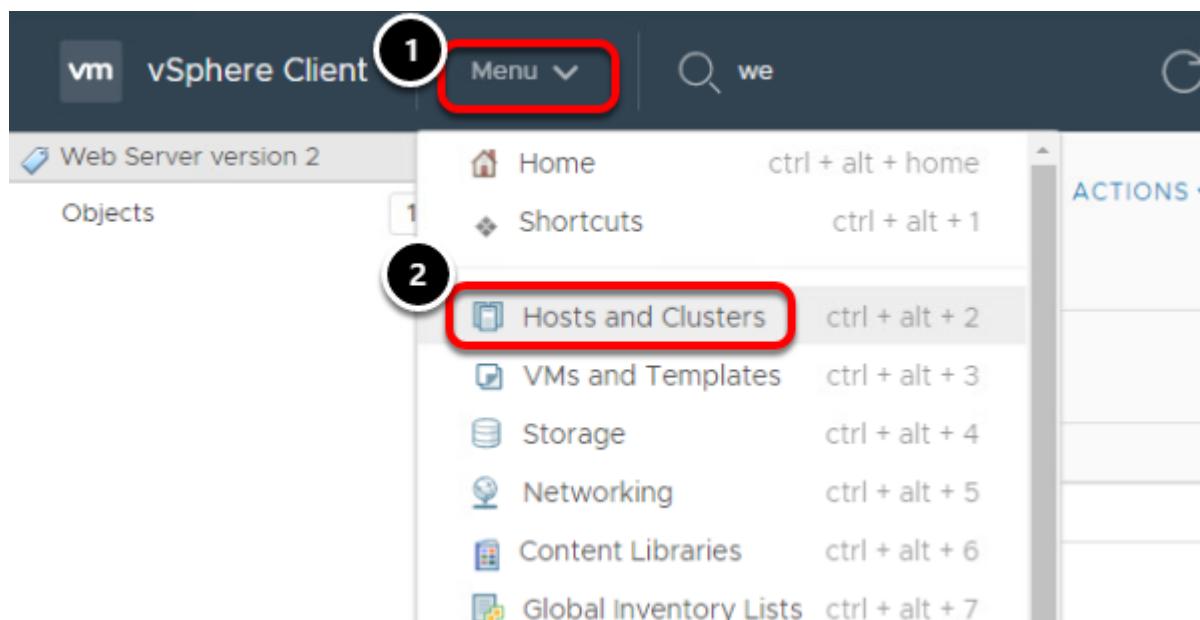


The Master Election Process

- 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.

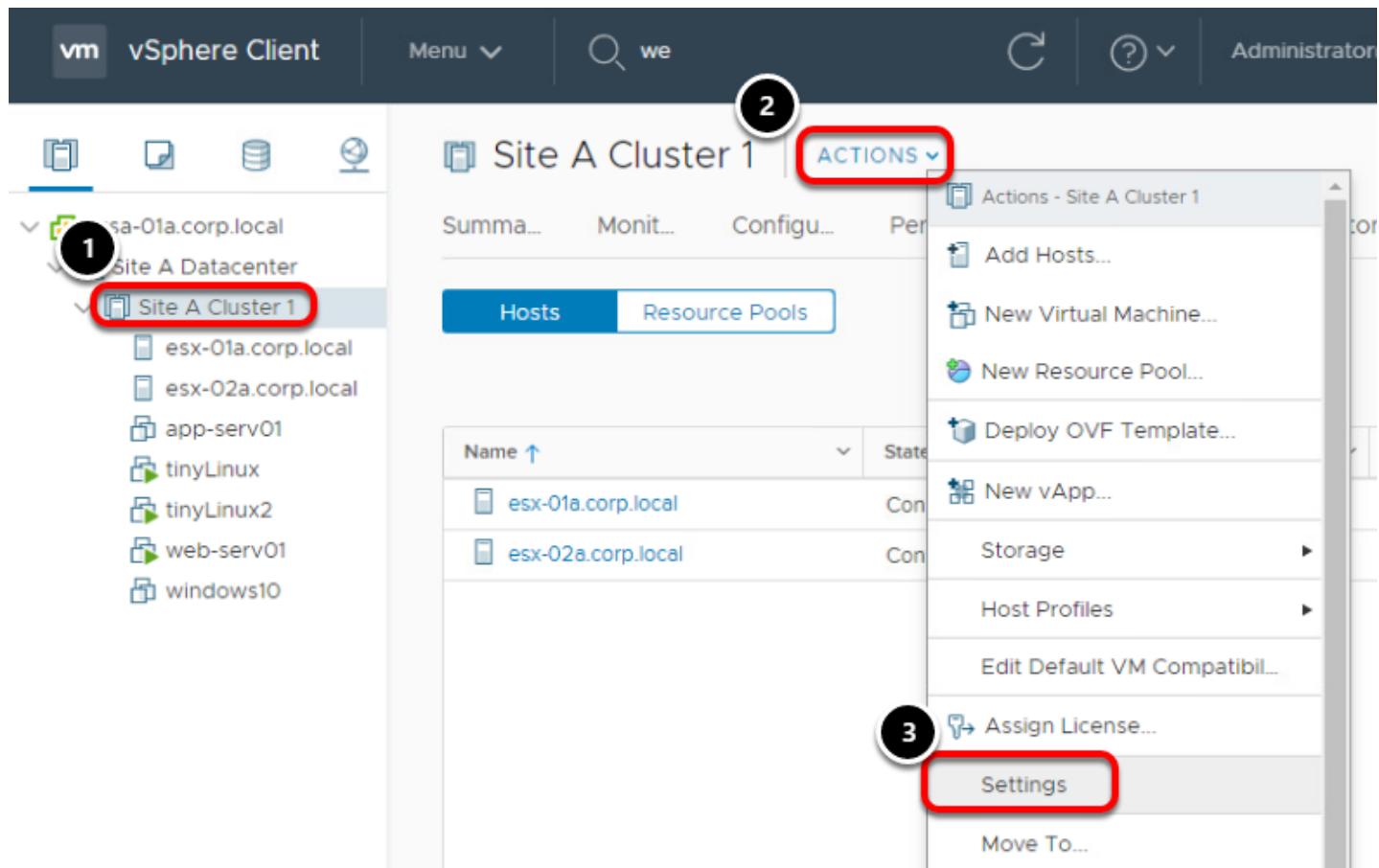


Enable and Configure vSphere Availability



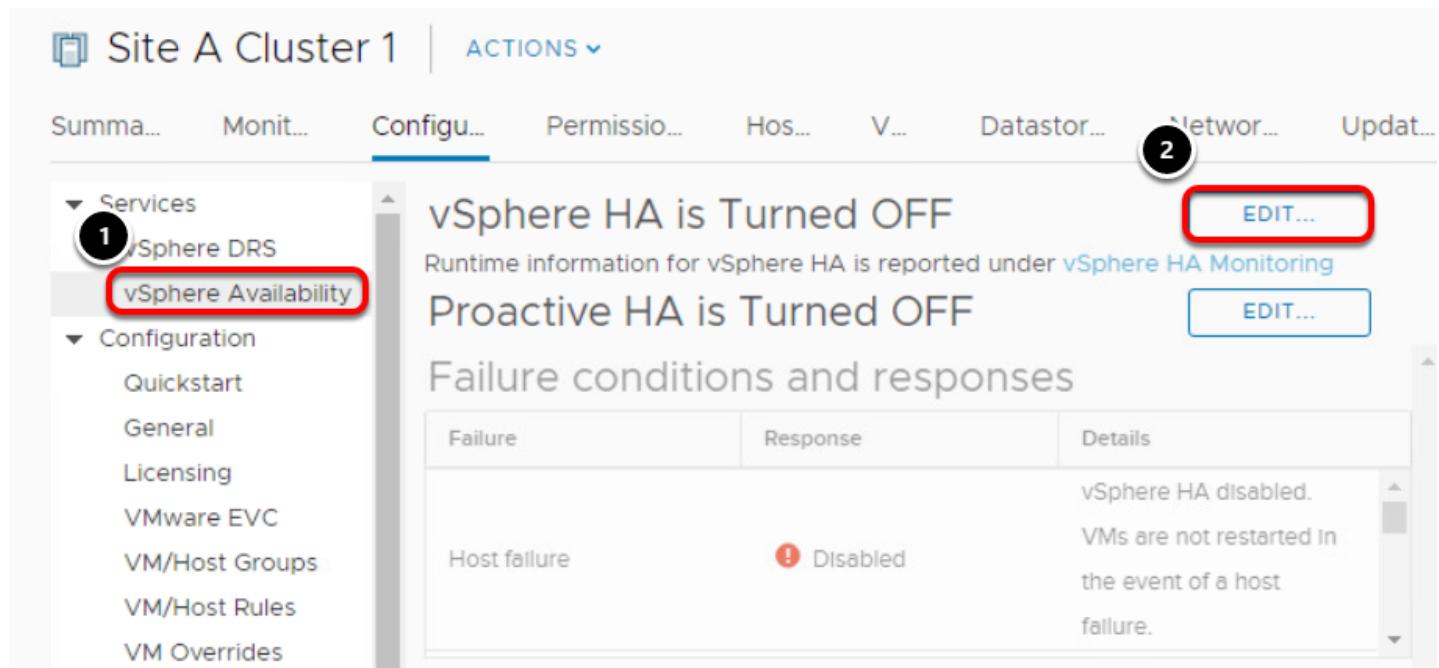
1. First, click on **Menu**
2. Select **Hosts and Clusters**

Settings for vSphere Availability



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

Cluster Settings



Site A Cluster 1 | ACTIONS ▾

Summa... Monit... Configu... Permissio... Hos... V... Datastor... Networ... Updat...

1 Services

- vSphere DRS
- vSphere Availability**

Configuration

- Quickstart
- General
- Licensing
- VMware EVC
- VM/Host Groups
- VM/Host Rules
- VM Overrides

vSphere HA is Turned OFF

Runtime information for vSphere HA is reported under [vSphere HA Monitoring](#)

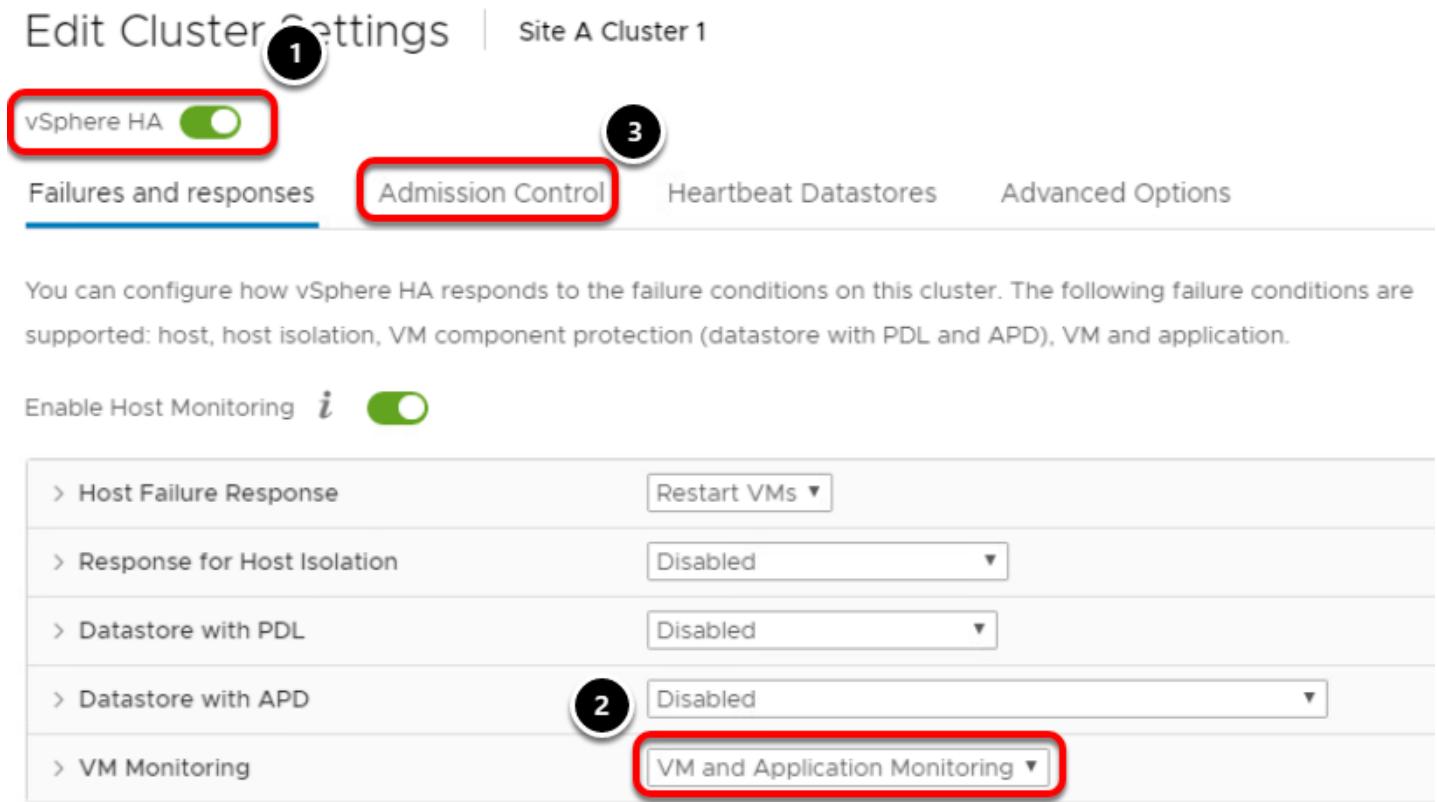
Proactive HA is Turned OFF

Failure conditions and responses

Failure	Response	Details
Host failure	! Disabled	vSphere HA disabled. VMs are not restarted in the event of a host failure.

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

2

3

Failure and responses Admission Control Heartbeat Datastores Advanced Options

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

Enable Host Monitoring *i*

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Disabled ▾
> Datastore with APD	Disabled ▾
> VM Monitoring	VM and Application Monitoring ▾

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.

3. Click the **Admission Control** tab.

Admission Control

Edit Cluster Settings | Site A Cluster 1

vSphere HA 

Failures and responses

Admission Control

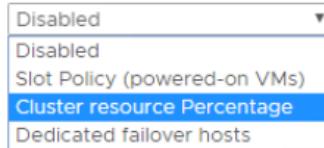
Heartbeat Datastores

Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Define host failover capacity by

1



1. In the **Define host failover capacity by** drop-down menu, select **Cluster resource percentage**.

Host failures cluster tolerates 1
Maximum is one less than number of hosts in cluster.

Define host failover capacity by Cluster resource Percentage ▾

Override calculated failover capacity.

Reserved failover CPU capacity: 0 % CPU

Reserved failover Memory capacity: 0 % Memory

Performance degradation VMs tolerate 100 %
Percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure. 0% - Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart. 100% - Warning is disabled.

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

2. Click '**Heartbeat Datastores**'.

Heartbeat Datastores

Edit Cluster Settings | Site A Cluster 1 | X

vSphere HA

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

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 2 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

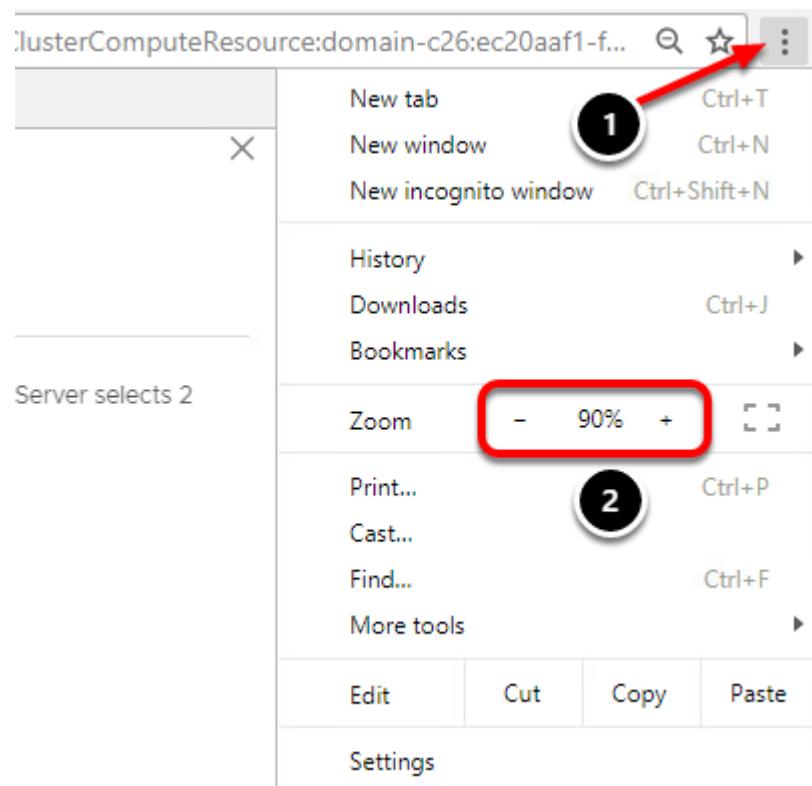
- Automatically select datastores accessible from the hosts 1
- Use datastores only from the specified list
- Use datastores from the specified list and complement automatically if needed

2
CANCEL OK

1. Select **Automatically select datastores accessible from the hosts**.

This is another layer of protection. Datastore heartbeating 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

Recent Tasks		Alarms		
Task Name	Target	Status	Initiator	
Configuring vSphere HA	esx-01a.corp.l...	6%	System	
Configuring vSphere HA	esx-02a.corp.l...	6%	System	
Reconfigure cluster	Site A Cluster 1	Completed	CORP1 Administrator	

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

Recent Tasks		Alarms	
Task Name	Target	Status	Initiator
Configuring vSphere HA	 esx-01a.corp.l...	✓ Completed	System
Configuring vSphere HA	 esx-02a.corp.l...	✓ Completed	System
Reconfigure cluster	 Site A Cluster 1	✓ Completed	CORPLAdministrator

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

1

Summary Monitor Configure Permissions Hosts VMs Datas

Total Processors: 4
Total vMotion Migrations: 0

Related Objects

Datacenter Site A Datacenter

vSphere HA

Protected

CPU

Memory

0% 50% 100%

CPU reserved for failover: 50 %

vSphere DRS

Cluster Consum

Custom Attribu

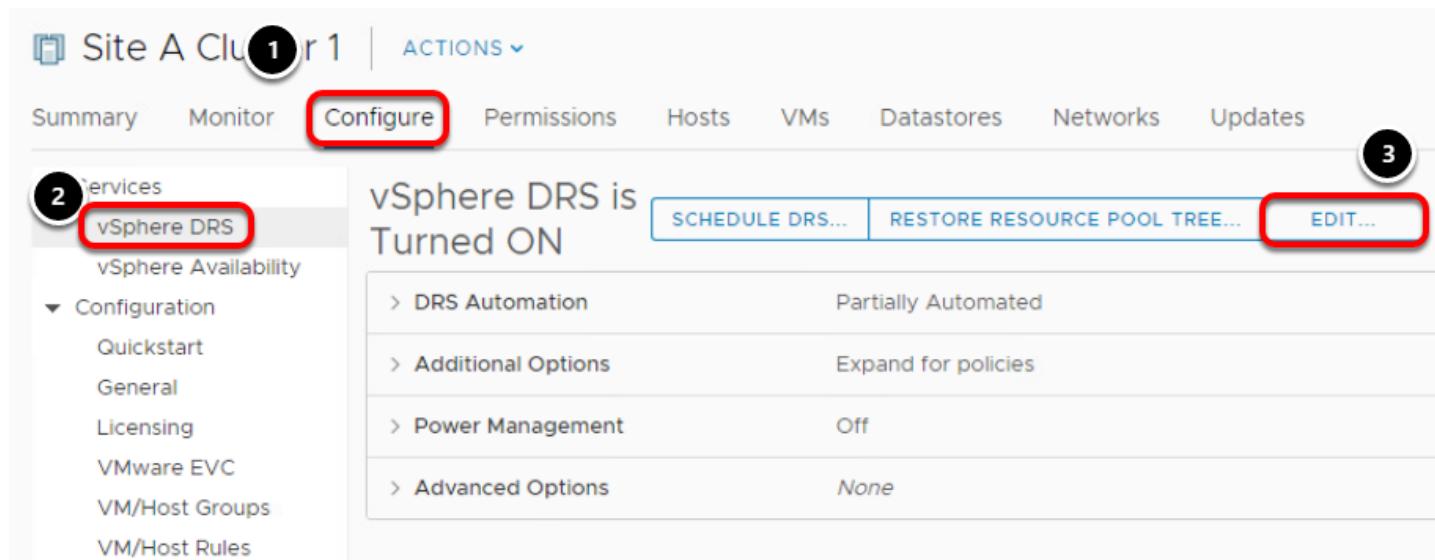
Update Manag

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)



Site A Cluster 1 | ACTIONS ▾

Summary Monitor **Configure** Permissions Hosts VMs Datastores Networks Updates

2 Services

2 vSphere DRS

vSphere Availability

Configuration

- Quickstart
- General
- Licensing
- VMware EVC
- VM/Host Groups
- VM/Host Rules

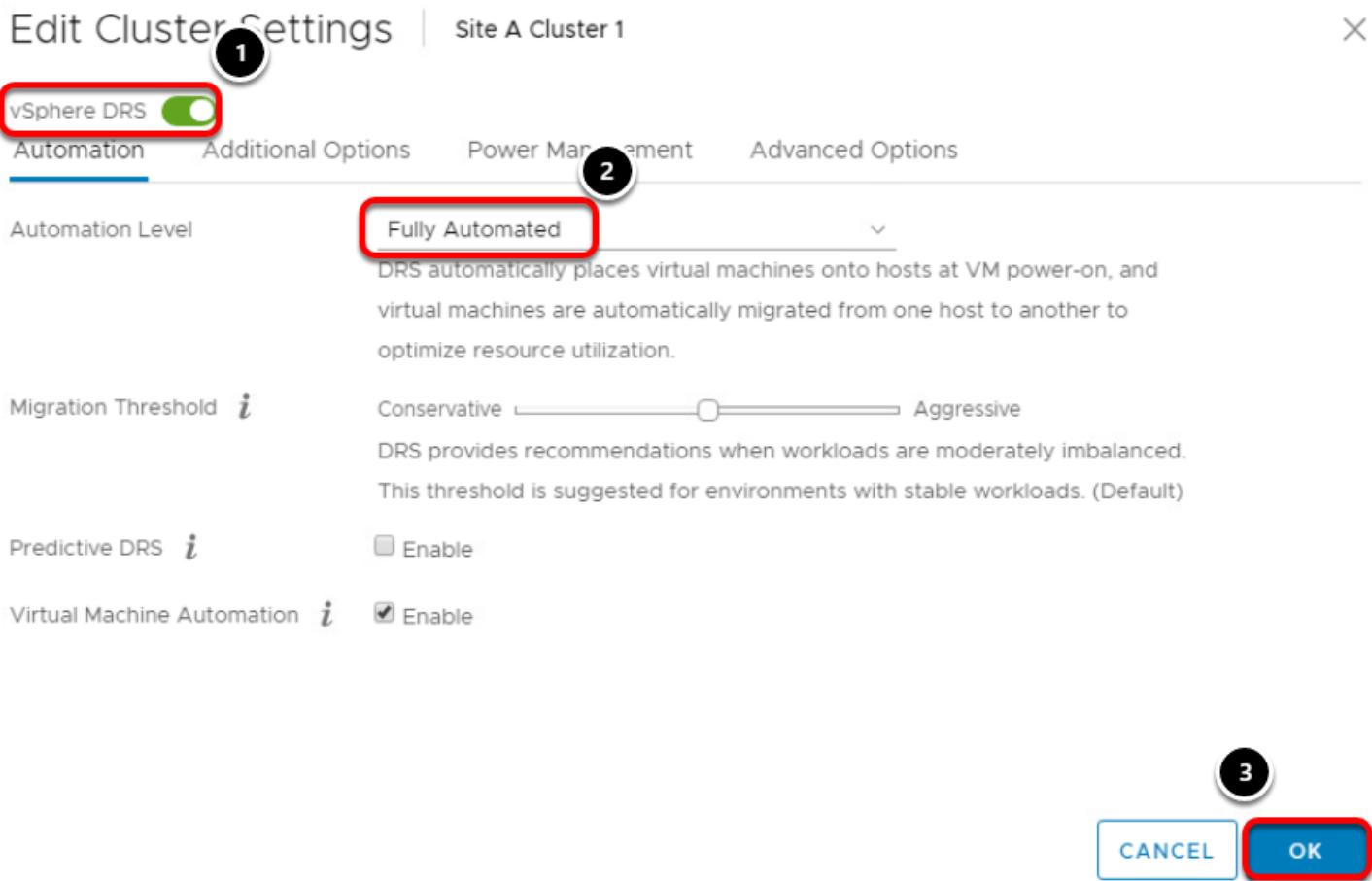
vSphere DRS is Turned ON

SCHEDULE DRS... RESTORE RESOURCE POOL TREE... **3** EDIT...

> DRS Automation	Partially Automated
> Additional Options	Expand for policies
> Power Management	Off
> Advanced Options	None

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. -- note that this is already enabled in the lab
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

The screenshot shows the vSphere Web Client interface for Site A Cluster 1. The top navigation bar includes Site A Cluster 1, ACTIONS, Summary (highlighted with a red box and a circled '1'), Monitor, Configure, Permissions, Hosts, VMs, Datastores, Networks, and Updates.

Summary Section:

- Total Processors: 4
- Total vMotion Migrations: 0
- Icons for vSphere HA and vSphere DRS

vSphere DRS Section (highlighted with a red box and a circled '2'):

vSphere DRS

Balanced (indicated by a green bar)

Migration automation level:	Fully Automated
Migration threshold:	Apply priority 1, priority 2, and priority 3 recommendations.
Power management automation level:	Off
DRS recommendations:	0
DRS faults:	0

Related Objects:

- Datacenter: Site A Datacenter

vSphere HA:

Protected (indicated by a grey bar)

CPU	0%	50%	100%
Memory	0%	50%	100%

CPU recovered for failure: 50 %

1. Click the **Summary** tab to display the current status of the cluster.
2. The Summary tab of the Cluster Site A 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 6 Fault Tolerance Provides Continuous Availability

vSphere 6 HA provides a base level of protection for your virtual machines by restarting virtual machines in the event of a host failure. vSphere 6 Fault Tolerance provides a higher level of availability, allowing users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.

Fault Tolerance provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in the instruction execution of the virtual machine. This is done using the VMware vLockstep technology on the ESXi host platform. vLockstep accomplishes this by having the Primary and Secondary VMs execute identical sequences of x86 instructions. The Primary VM captures all inputs and events (from the processor to virtual I/O devices) and replays them on the Secondary VM. The Secondary VM executes the same series of instructions as the Primary VM, while only a single virtual machine image (the Primary VM) executes the workload.

If the host running the Primary VM fails, an immediate and transparent failover occurs. The functioning ESXi host seamlessly becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. After a transparent failover occurs, a new Secondary VM is respawned and redundancy is re-established. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.

VMware vSphere Fault Tolerance

vSphere 6.0 VMware Fault Tolerance

Additional new features	Benefits
<ul style="list-style-type: none"> Enhanced virtual disk format support Ability to hot configure FT Greatly increased FT host compatibility 	<ul style="list-style-type: none"> Protect mission critical, high performance applications regardless of OS; No application-specific management and learning Continuous availability – zero downtime and zero data loss for infrastructure failures; no loss of TCP connections Fully automated response



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

Use cases

Any workload that has up to 4 vCPUs and 64GB Memory that is not latency sensitive (e.g. VOIP & High-Frequency trading are not good candidates for FT). Note that vSphere 6.0 introduces the capability to use FT to protect VMs with more than 1 vCPU. In vSphere 5.5 and prior versions, only VMs with 1 vCPU could be protected by FT. For vSphere v6.5 the Standard and Enterprise editions allow for up to 2 vCPUs, where the Enterprise Plus edition allow for up to 4 vCPUs.

There is VM/Application overhead to using FT and that will depend on a number of factors like the application, number of vCPUs, number of FT protected VMs on a host, Host processor type, etc. See the [Performance Best Practices for VMware vSphere](#) for more information.

The new version of Fault Tolerance greatly expands the use cases for FT to approximately 90% of workloads.

The new technology used by FT is called Fast Checkpointing and is basically a heavily modified version of an vMotion that never ends and executes many more checkpoints (multiple/sec). Also note that in versions prior to 6.0, FT required shared storage where both the Primary and Secondary copies of the FT-protected VM would share the same VMDK files. However, in vSphere 6.0 in order to add additional protection to the FT-protected VM, the Primary & Secondary VM use unique VMDK's.

FT logging (traffic between hosts where primary and secondary are running) is very bandwidth intensive and is recommended that a dedicated 10G NIC is used on each host. This isn't required, but highly recommended as at a minimum an FT protected VM will consume more bandwidth . Slower NICs on the ESXi hosts will impact performance on the secondary VM.

Video: Protecting Virtual Machines with FT (2:51)

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.

Monitoring Events and Creating Alarms

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

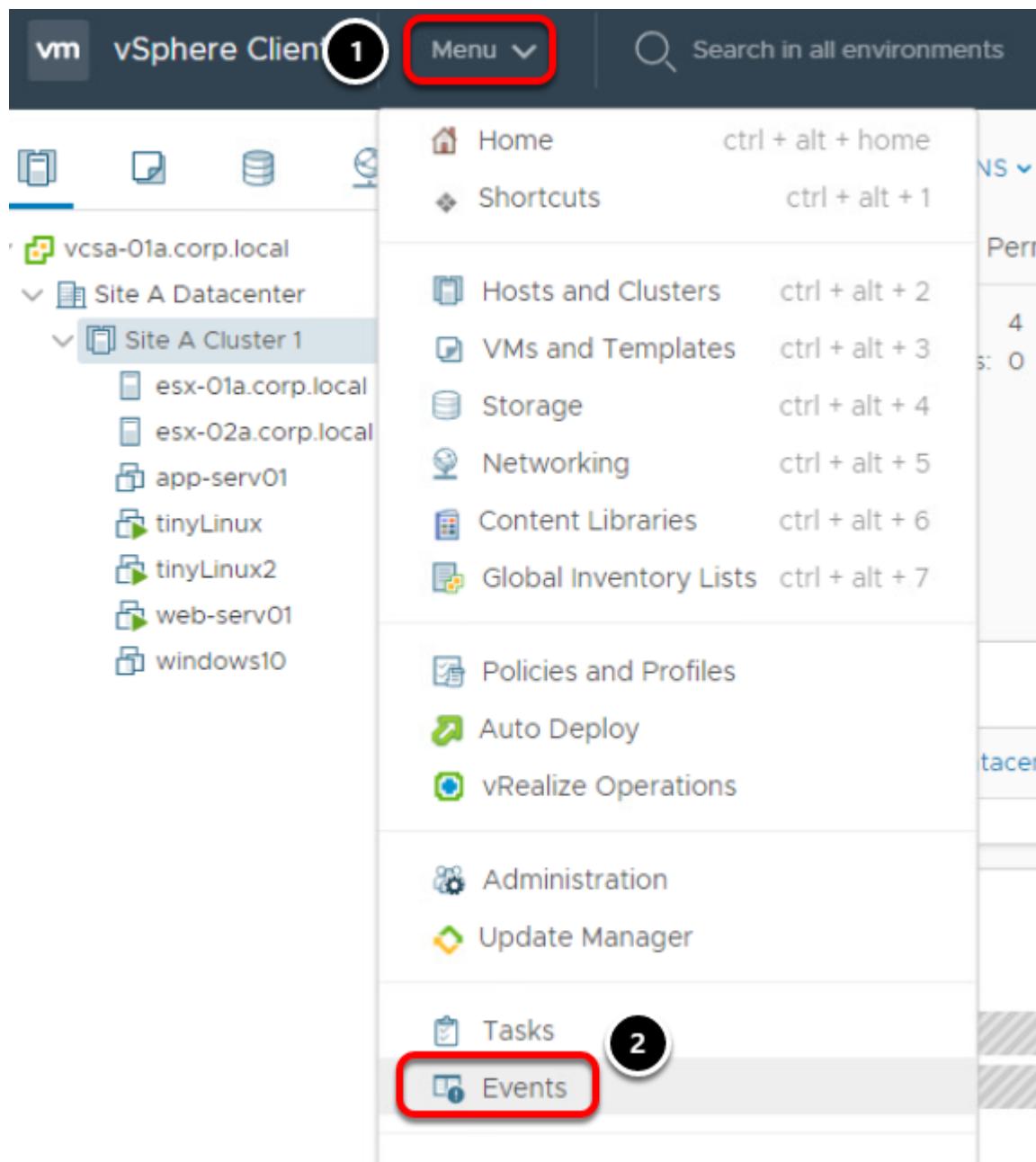
■ Alert – red

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

◀ Previous ▶ Next 1

Description	Type	Date Time	Task	Target	User	Event Type ID
Alarm 'Host ...	! Error	06/24/2019, 5:2...		esx-01a.cor...		com.vmware.vc.S...
Alarm 'Host ...	! Error	06/24/2019, 5:2...		esx-02a.cor...		com.vmware.vc.S...
VM tinyLinu...	! Error	06/24/2019, 4:5...		tinyLinux2 T...	CORP\Administr...	com.vmware.vc.v...
vSphere HA ...	Information	06/24/2019, 5:2...		Site A Clust...	CORP\Administr...	vim.event.DasAd...
Virtual mach...	Information	06/24/2019, 5:2...		tinyLinux		com.vmware.vc....
vSphere HA ...	Information	06/24/2019, 5:2...		esx-02a.cor...		vim.event.HostD...
vSphere HA ...	Information	06/24/2019, 5:2...		esx-01a.cor...		vim.event.HostD...
vSphere HA ...	Information	06/24/2019, 5:2...		esx-02a.cor...		com.vmware.vc....
User dcui@1...	Information	06/24/2019, 5:2...		esx-02a.cor...	dcui	vim.event.UserL...

100 items

Date Time: 06/24/2019, 5:29:08 AM 2 Type: Error

Target: esx-01a.corp.local

Description:

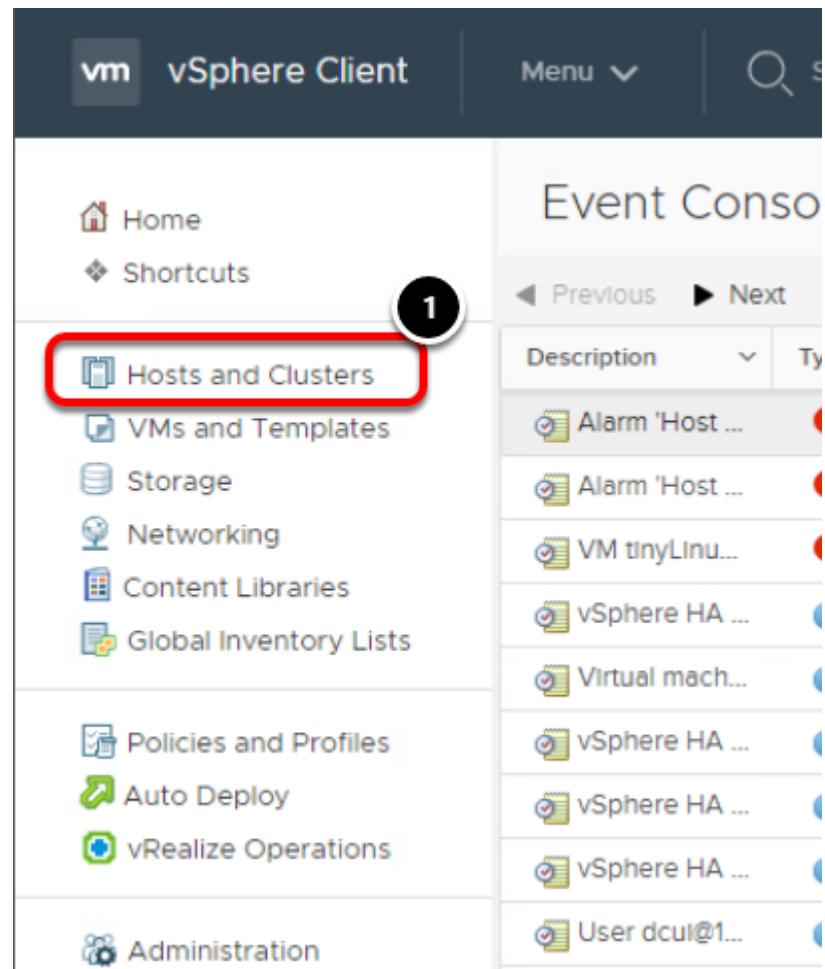
06/24/2019, 5:29:08 AM Alarm 'Host error' on esx-01a.corp.local triggered by event 9971 'Issue detected on esx-01a.corp.local in Site A Datacenter: Attempting to install an image profile bypassing signing and acceptance level verification. This may pose a large security (2019-06-24T12:28:59.687Z cpu0:2113463)'

Related events:

There are no related events.

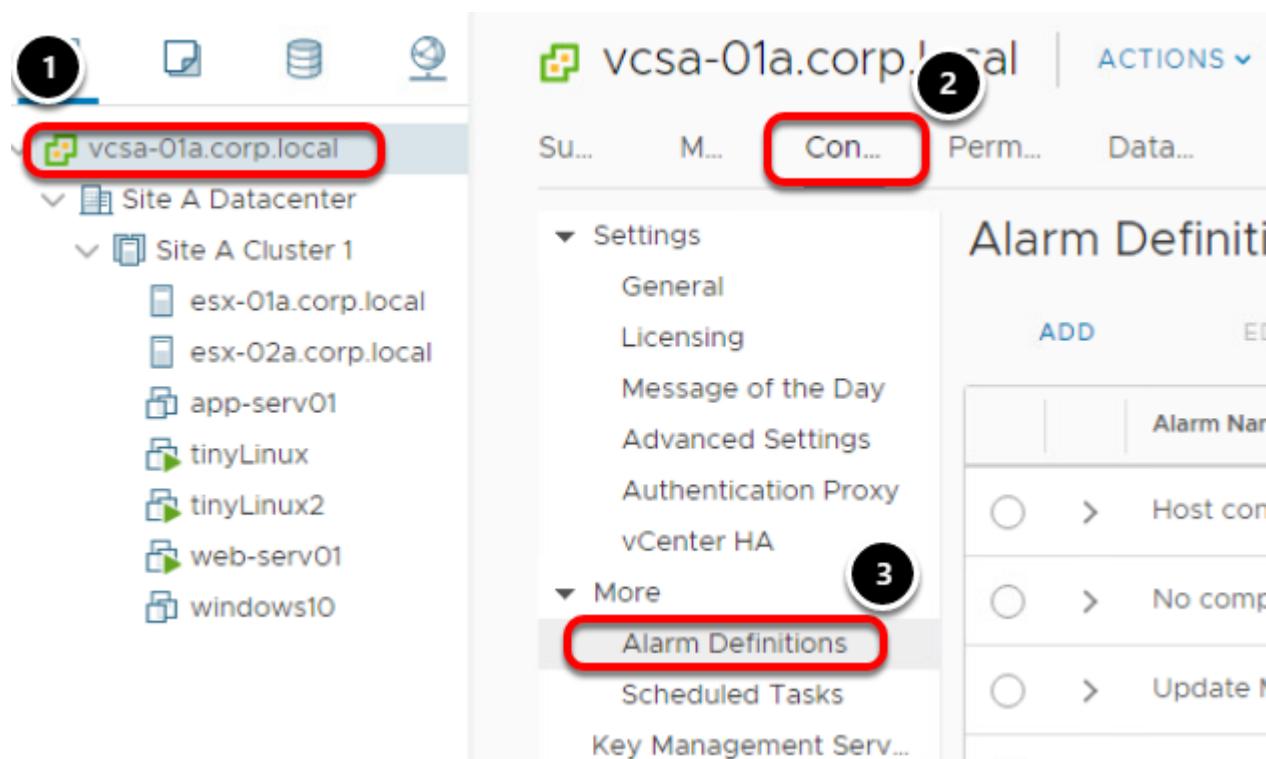
1. Click on the **Type** column to sort by level of severity.
2. Select an event to review the details of the event.

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.

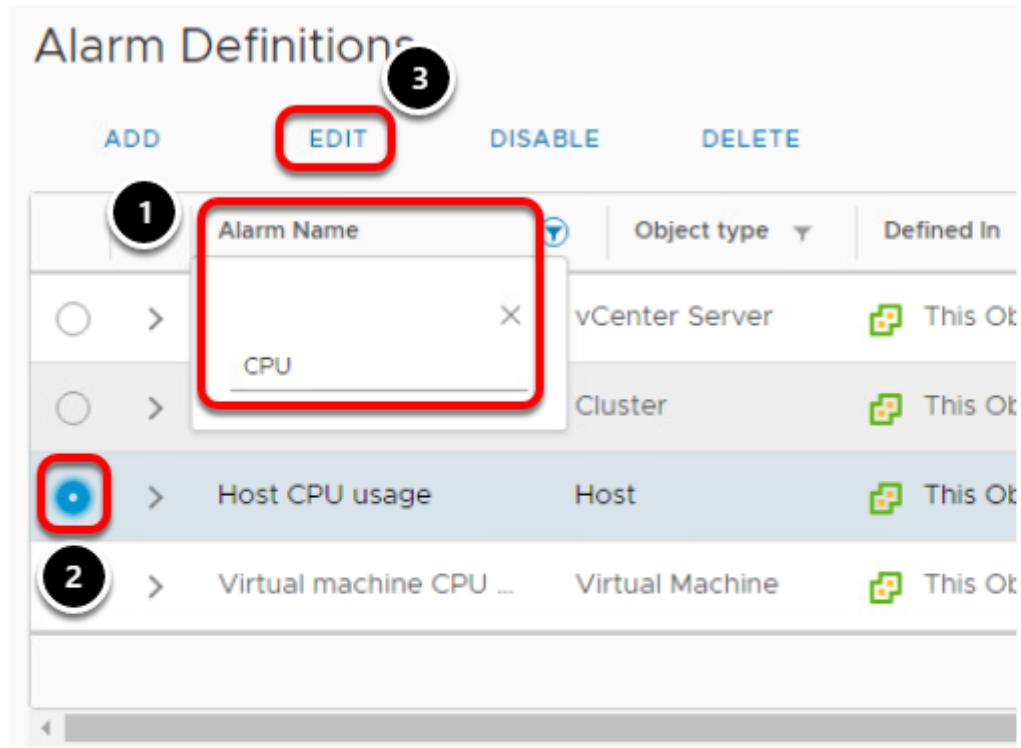
Alarm Definitions

Alarm Definitions

	Alarm Name	Object type	Defined In	Enabled	Last r...
<input type="radio"/>	Host connection and ...	Host	This Object	Disabled	04/24/2013
<input type="radio"/>	No compatible host f...	Virtual Machine	This Object	Enabled	04/24/2013
<input type="radio"/>	Update Manager Ser...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	vMon API Service He...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	Component Manager ...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	VMware vSphere Aut...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	vSAN Health Service ...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	PostgreSQL Archiver ...	vCenter Server	This Object	Enabled	04/24/2013
<input type="radio"/>	VMware vCenter-Ser...	vCenter Server	This Object	Enabled	04/24/2013

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' page in the vSphere Web Client. At the top, there are buttons for 'ADD', 'EDIT' (which is highlighted with a red box), 'DISABLE', and 'DELETE'. Below these are three rows of alarm definitions. The first row, step 1, shows an 'Alarm Name' search field with 'CPU' typed into it, also highlighted with a red box. The second row, step 2, shows the 'Host CPU usage' alarm, which is selected and highlighted with a red box. The third row shows the 'Virtual machine CPU ...' alarm. The columns from left to right are: 'Object type' (vCenter Server, Cluster, Host, Virtual Machine), 'Defined In' (This Object, This Object, This Object, This Object), and the alarm names.

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

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

Name and Targets

Edit Alarm Definition

1 Name and Targets

2 Alarm Rule 1

3 Alarm Rule 2

4 Reset Rule 1

5 Review

Name and Targets

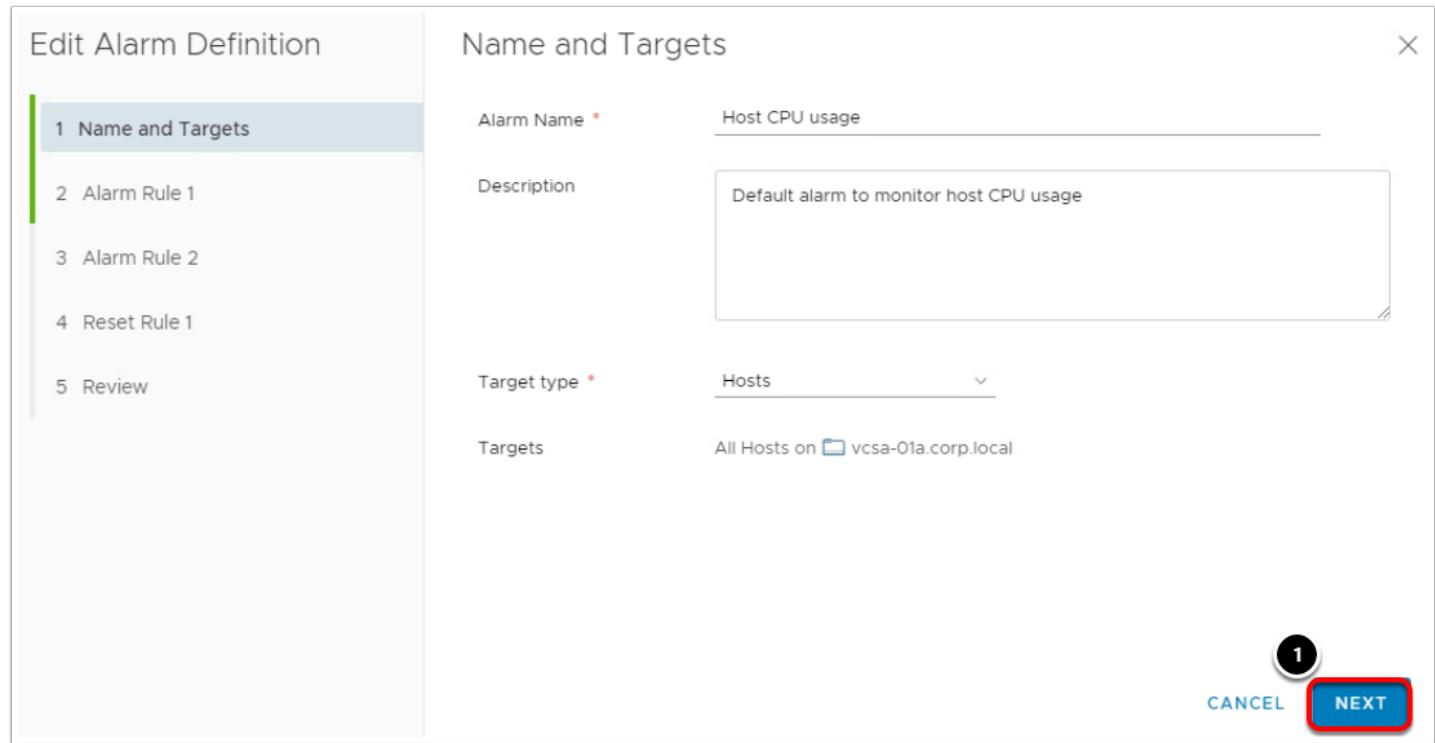
Alarm Name * Host CPU usage

Description Default alarm to monitor host CPU usage

Target type * Hosts

Targets All Hosts on vcsa-01a.corp.local

1 CANCEL NEXT



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

Alarm Rule 1



IF

Host CPU Usage

is above **80** % for 5 min [ADD ADDITIONAL TRIGGER](#)

THEN

Trigger the alarm [Show as Warning](#)

and *

Send email notifications

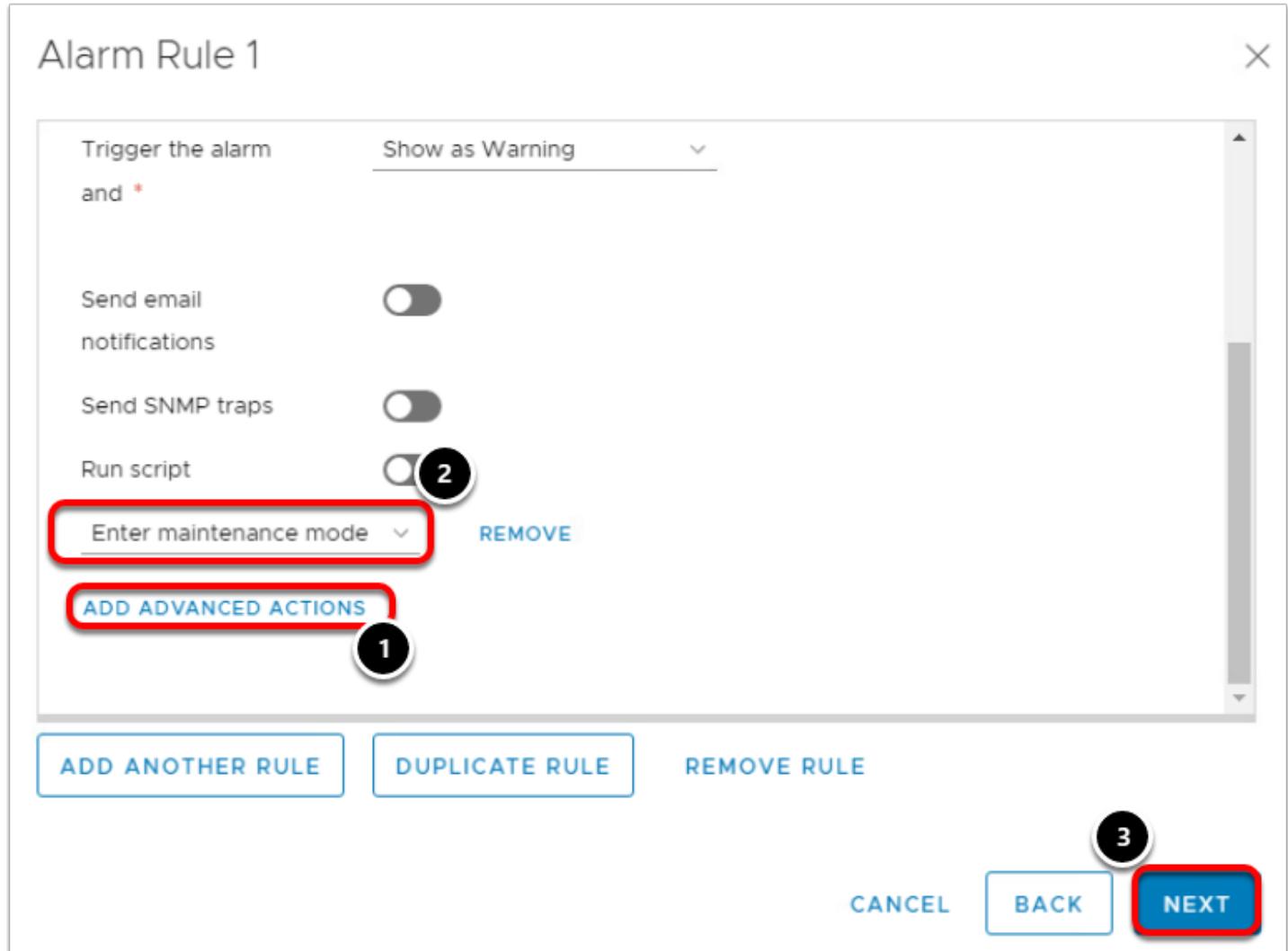
2

▼

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

Alarm Rule 2 X

IF

Host CPU Usage
is above % for ADD ADDITIONAL TRIGGER

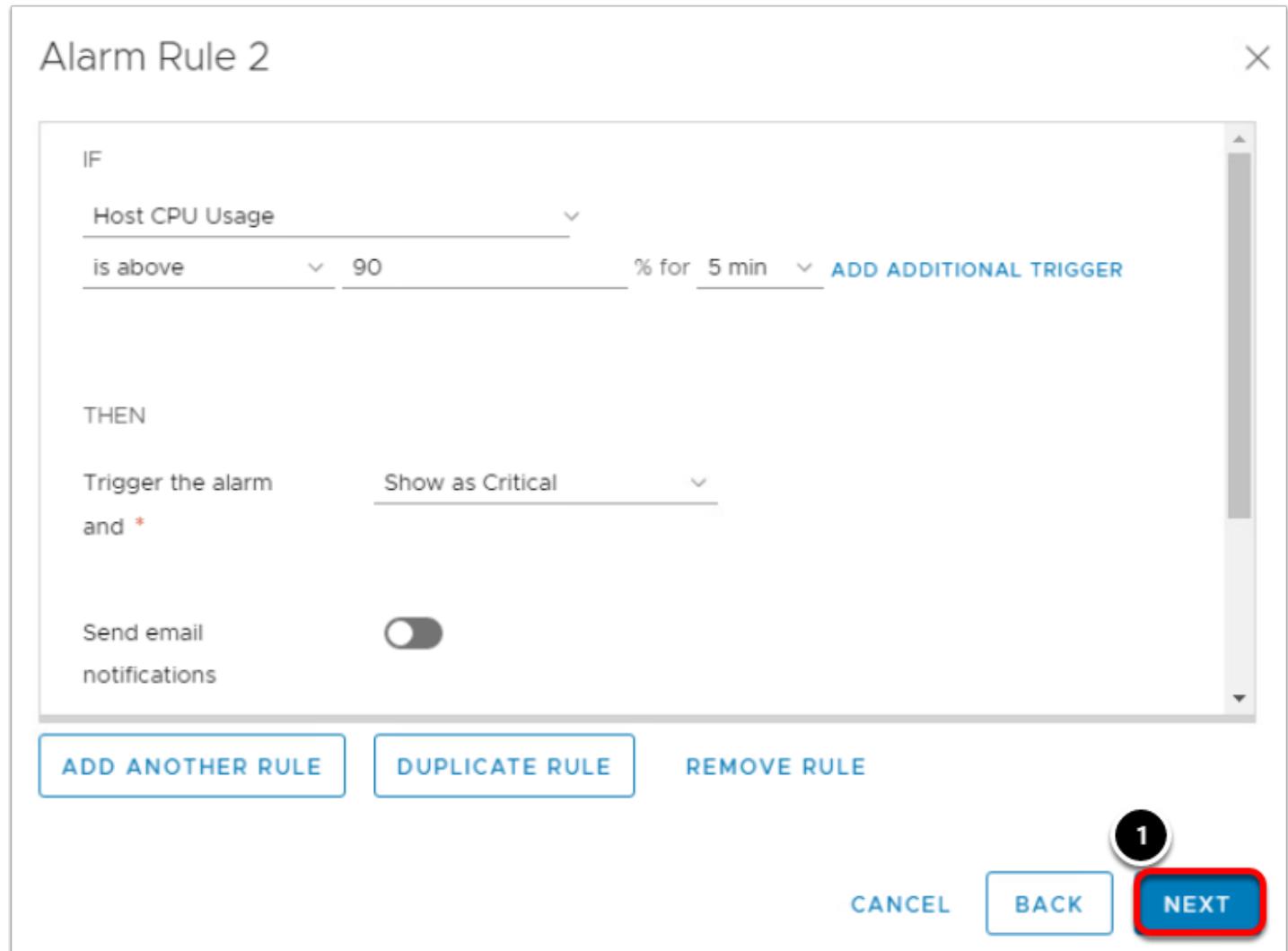
THEN

Trigger the alarm and *

Send email notifications

ADD ANOTHER RULE **DUPLICATE RULE** **REMOVE RULE**

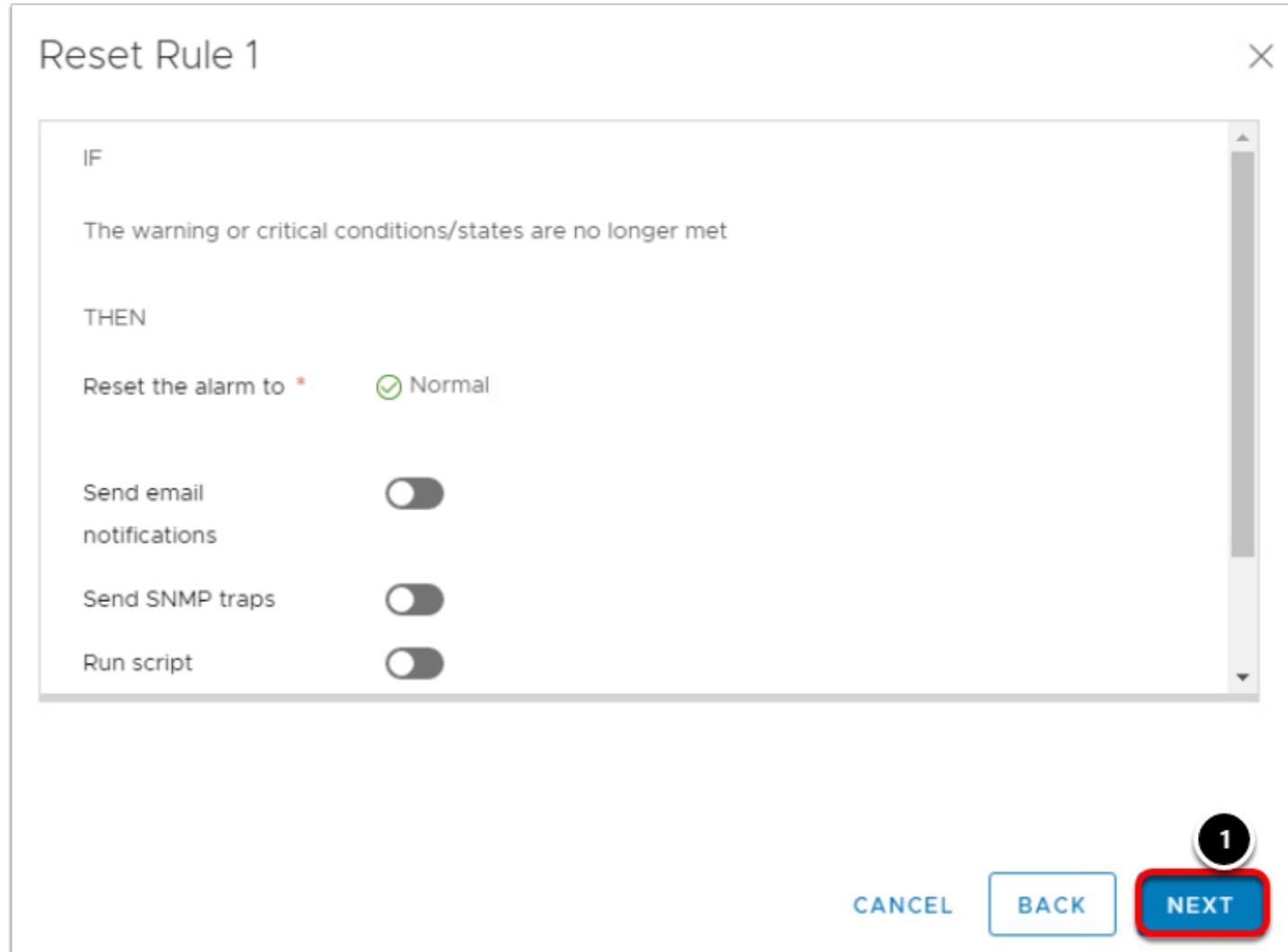
1 **NEXT** **BACK** **CANCEL**



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

Review

X

Alarm Name Host CPU usage

Description Default alarm to monitor host CPU usage

Targets All Hosts on  vcsa-01a.corp.local

Alarm Rules IF Host CPU Usage is above 80 % for 5 min

THEN Trigger the alarm as  Warning

Enter maintenance mode

OR

IF Host CPU Usage is above 90 % for 5 min

THEN Trigger the alarm as  Critical

Reset Rules

IF the warning or critical conditions/states are no longer met

1

Enable this alarm 

CANCEL

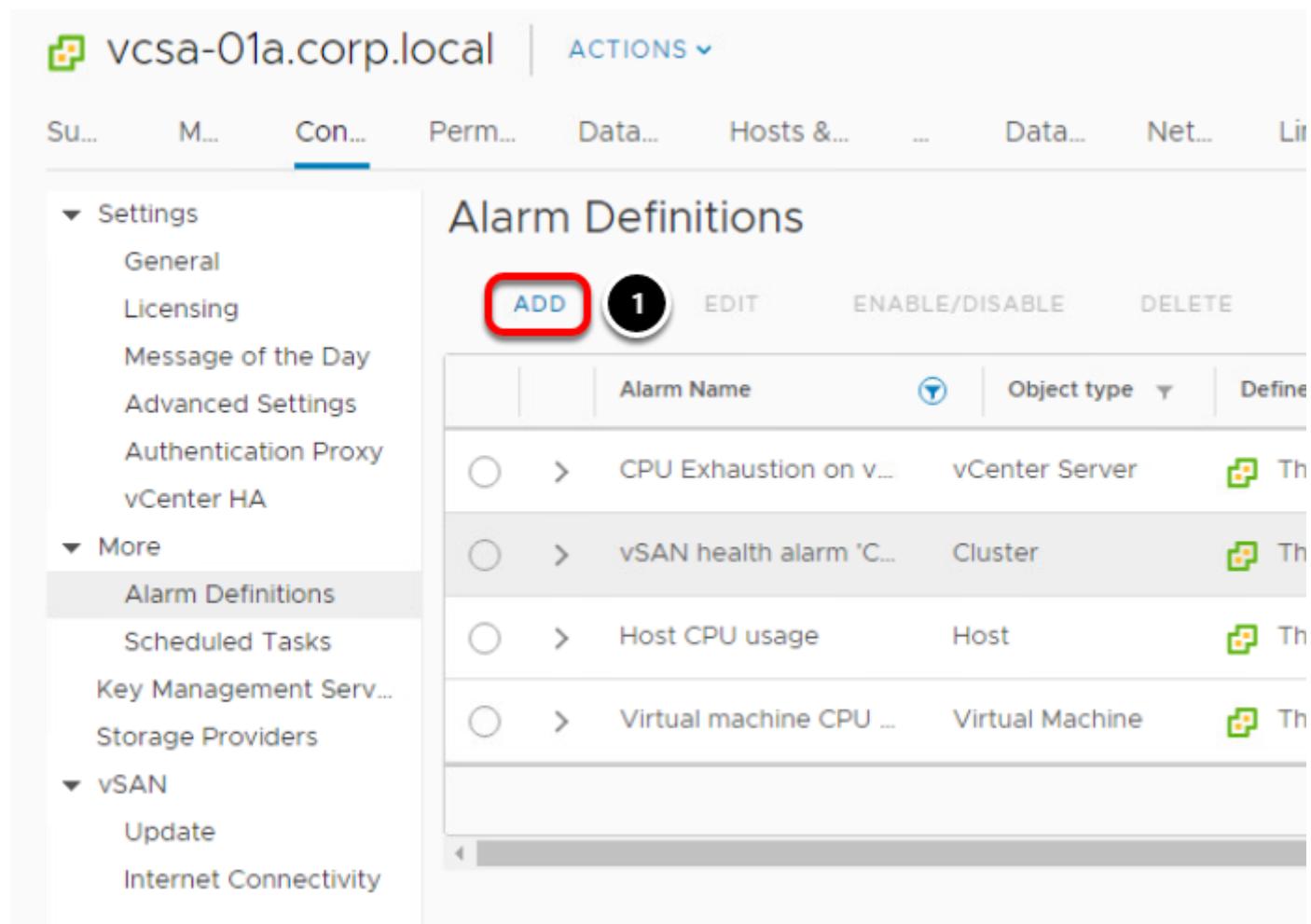
BACK

SAVE

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 'vcsa-01a.corp.local' interface. The 'Con...' tab is selected. The left sidebar shows 'Settings' (General, Licensing, Message of the Day, Advanced Settings, Authentication Proxy, vCenter HA) and 'More' (Alarm Definitions, Scheduled Tasks, Key Management Serv..., Storage Providers). The 'vSAN' section is collapsed. The main area is titled 'Alarm Definitions' and shows a table with four rows. The 'ADD' button is highlighted with a red circle and the number '1'. The table columns are: Alarm Name, Object type, and Define. The rows are: 1. CPU Exhaustion on vCenter Server (vCenter Server, Threshold icon). 2. vSAN health alarm 'C...' (Cluster, Threshold icon). 3. Host CPU usage (Host, Threshold icon). 4. Virtual machine CPU ... (Virtual Machine, Threshold icon).

	Alarm Name	Object type	Define
1	CPU Exhaustion on vCenter Server	vCenter Server	
2	vSAN health alarm 'C...	Cluster	
3	Host CPU usage	Host	
4	Virtual machine CPU ...	Virtual Machine	

1. To add a new alarm, click **Add**.

New Alarm Definition

Name and Targets

1 Alarm Name * Virtual Machine CPU Ready

2 Target type * Virtual Machines

Targets All Virtual Machines on vcsa-01a.corp.local (6)

3 CANCEL NEXT

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

Alarm Rule 1



1. Click in the field under IF and select **VM CPU Ready Time**.
2. Change the **select an operator** field to **is above**.
3. Type **8000** in the ms field
4. In the last field, use the drop-down menu to select **5 min**.
5. Use the scroll bar to scroll to the Add advanced actions section.

Add Advanced Action

Alarm Rule 1

THEN

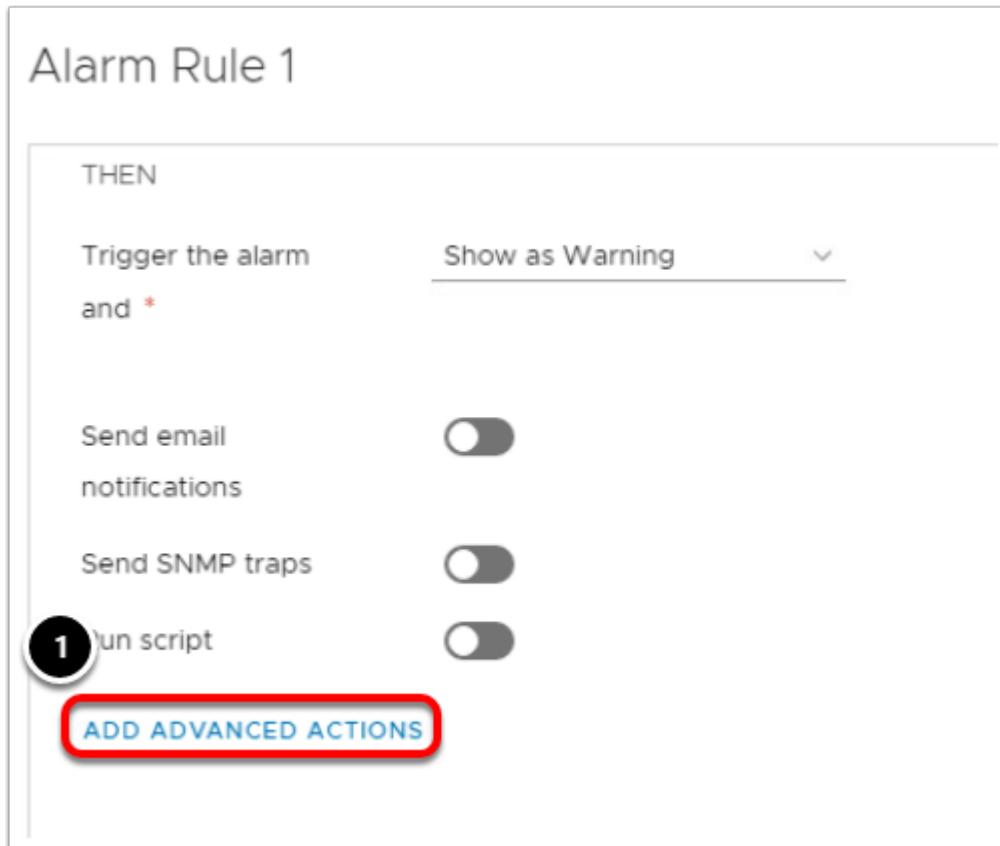
Trigger the alarm and *

Send email notifications

Send SNMP traps

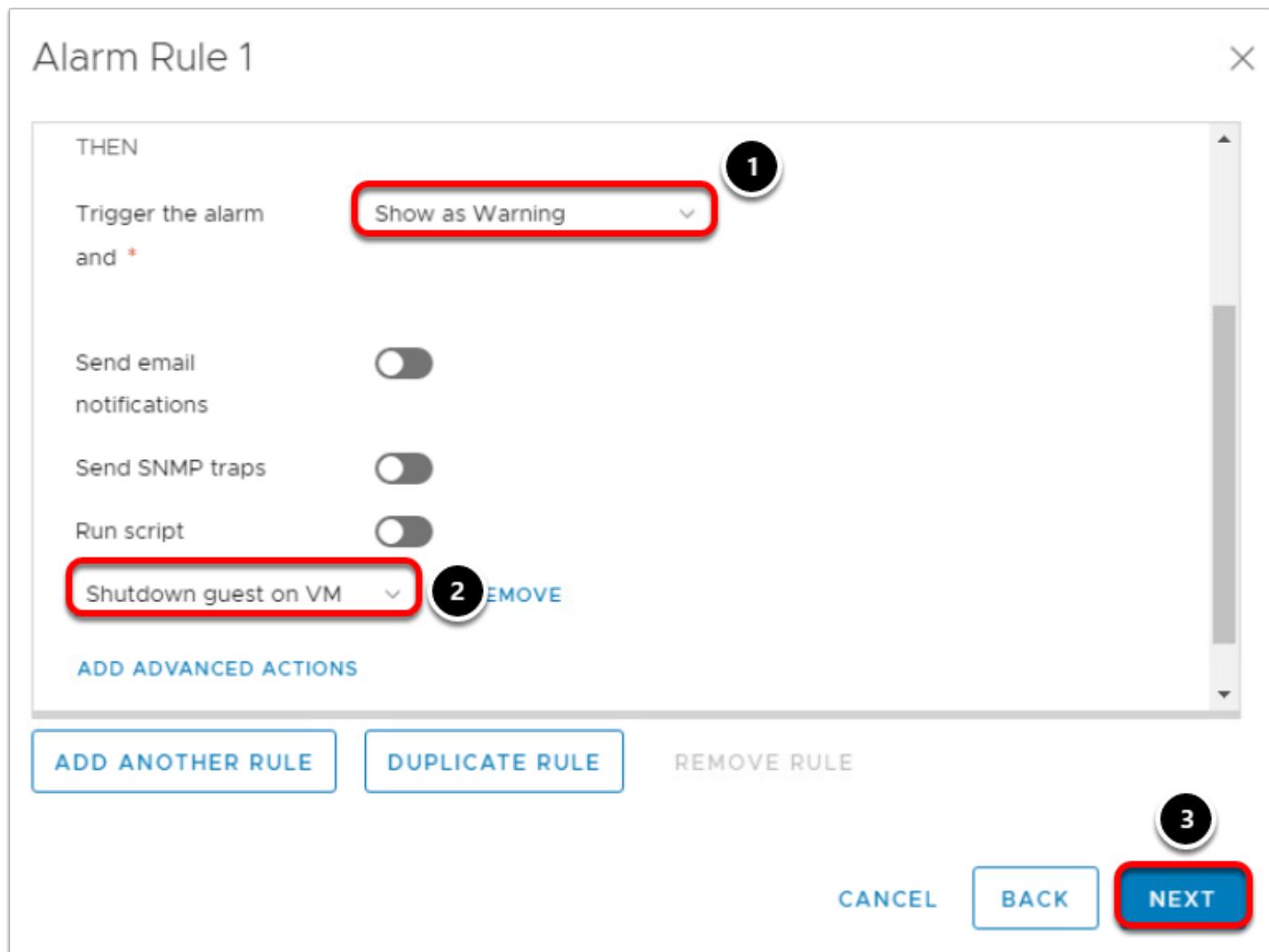
Run script

1 **ADD ADVANCED ACTIONS**



1. Click **Add Advanced Actions**

Migrate VM



1. Select **Show as Warning** in the Trigger the alarm menu
2. From the drop-down menu, select **Shutdown guest on VM**.

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

3. Click **Next**.

Reset Rule 1

Reset Rule 1 X

IF
The warning or critical conditions/states are no longer met

THEN

Reset the alarm to * Normal

Send email notifications

Send SNMP traps

Run script

1

CANCEL BACK NEXT

Additional options could be specified once the conditions are clear.

1. Click **Next**

Review

Review

Alarm Name Virtual Machine CPU Ready

Description

Targets All Virtual Machines on vcsa-01a.corp.local (6)

Alarm Rules

```
IF VM CPU Ready Time is above 8000 ms for 5 min
THEN Trigger the alarm as  Warning
Shutdown guest on VM
```

Reset Rules

```
IF the warning or critical conditions/states are no longer met
THEN Trigger the alarm as  Normal
```

Enable this alarm

[CANCEL](#)

[BACK](#)

[CREATE](#)

1

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		
<input type="radio"/>	vSAN health alarm 'CPU AES-NI is disabled on ...	Cluster	 This Object		
<input type="radio"/>	Host CPU usage	Host	 This Object		
<input type="radio"/>	Virtual Machine CPU Ready	Virtual Machine	 This Object		
<input type="radio"/>	Virtual machine CPU usage	Virtual Machine	 This Object		

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

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: Configuring Shares and Reservations (4:00)

This video shows how to use the VMware vSphere web client to configure shares, reservations, and limits in order to effectively distribute compute and memory resources among virtual machines.

Shares, Limits and Reservations

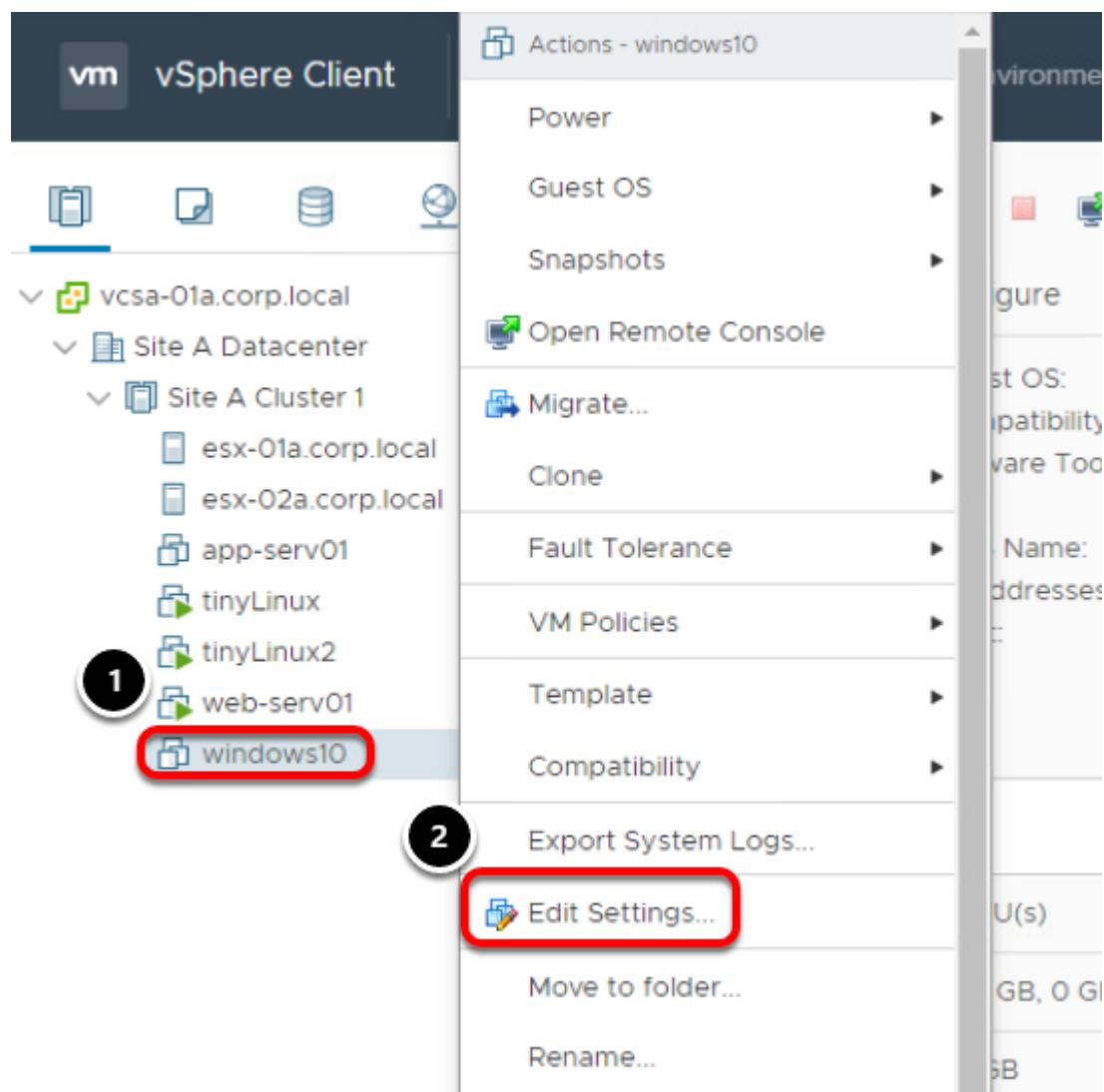
Resource Management

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

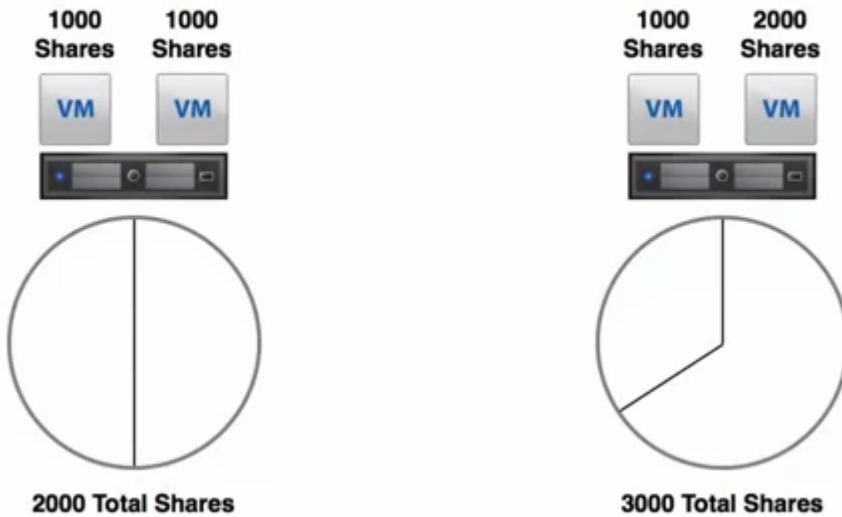
Review CPU settings



1. Right click the **windows10** virtual machine.
2. Select **Edit Settings...**

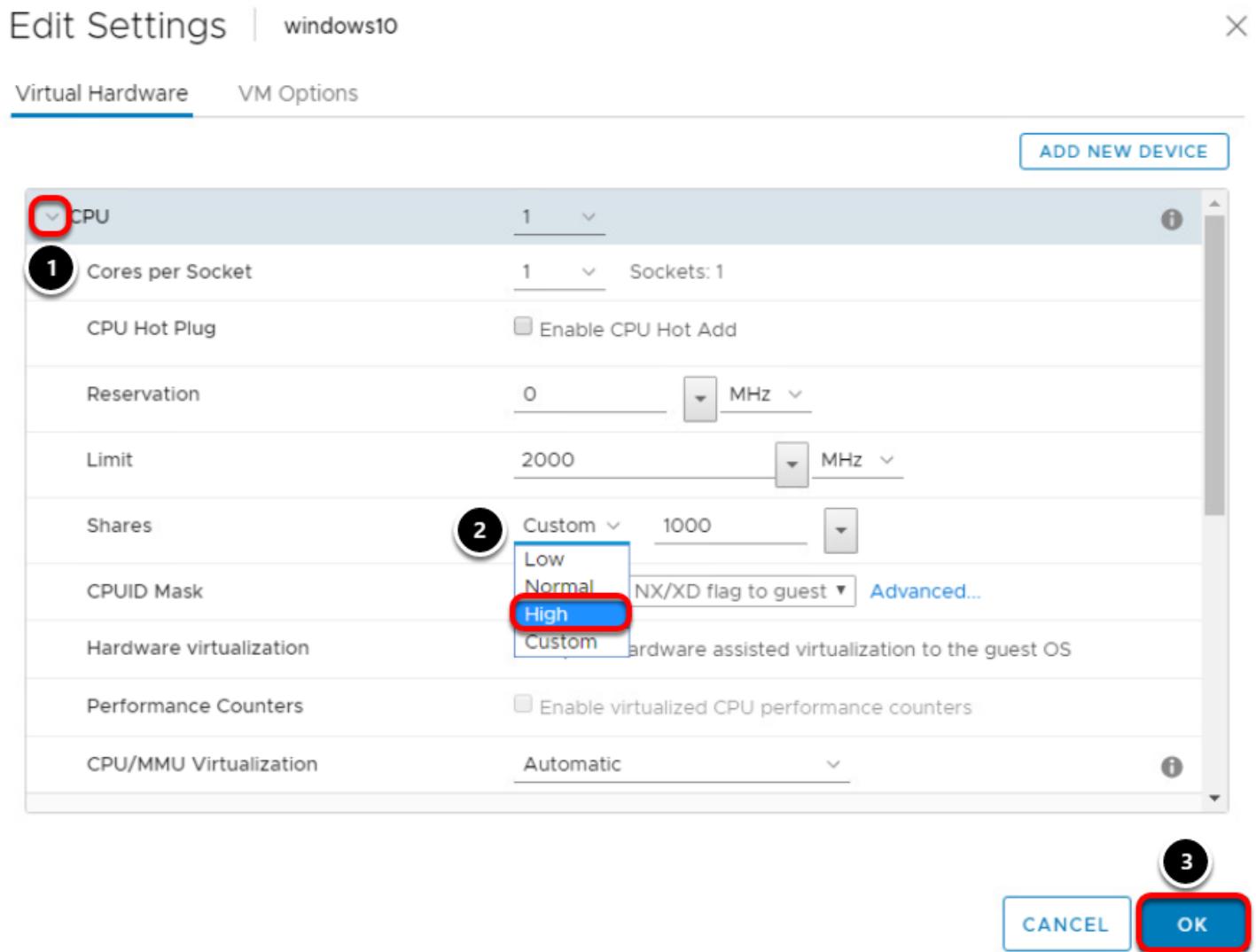
Understanding Shares

Resource Management: 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.

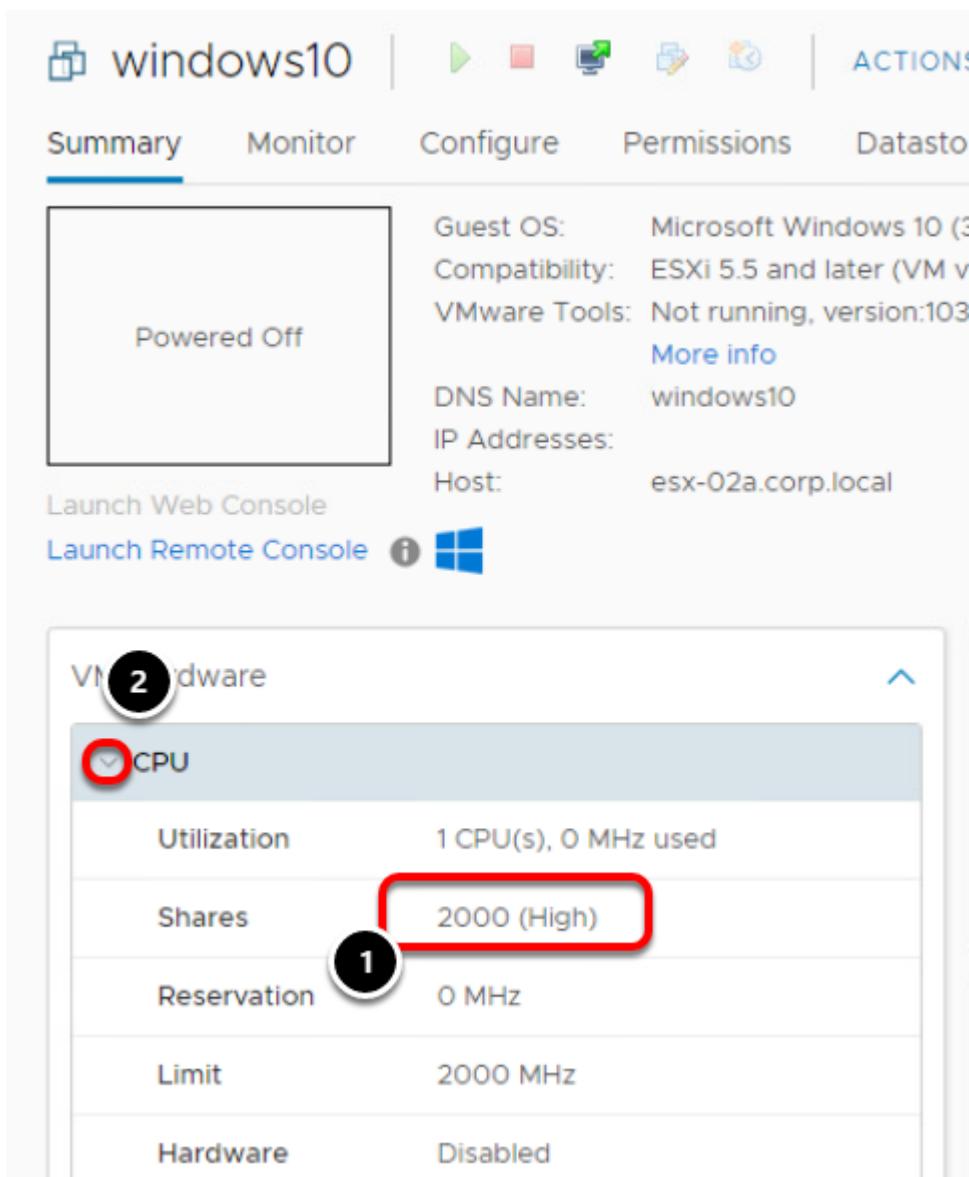
Changing Resource Allocation of CPU shares.



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



VMware

CPU

Utilization	1 CPU(s), 0 MHz used
Shares	2000 (High)
Reservation	0 MHz
Limit	2000 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.

Edit Settings | windows10 X

Virtual Hardware VM Options ADD NEW DEVICE

CPU

Cores per Socket	1	Sockets: 1
CPU Hot Plug	<input type="checkbox"/> Enable CPU Hot Add	
Reservation	0	MHz
Limit	2000	MHz
Shares	High	2000
CPUID Mask	Expose the NX/XD flag to guest Advanced...	
Hardware virtualization	<input type="checkbox"/> Expose hardware assisted virtualization to the guest OS	
Performance Counters	<input type="checkbox"/> Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic	

Memory

CANCEL **OK**

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

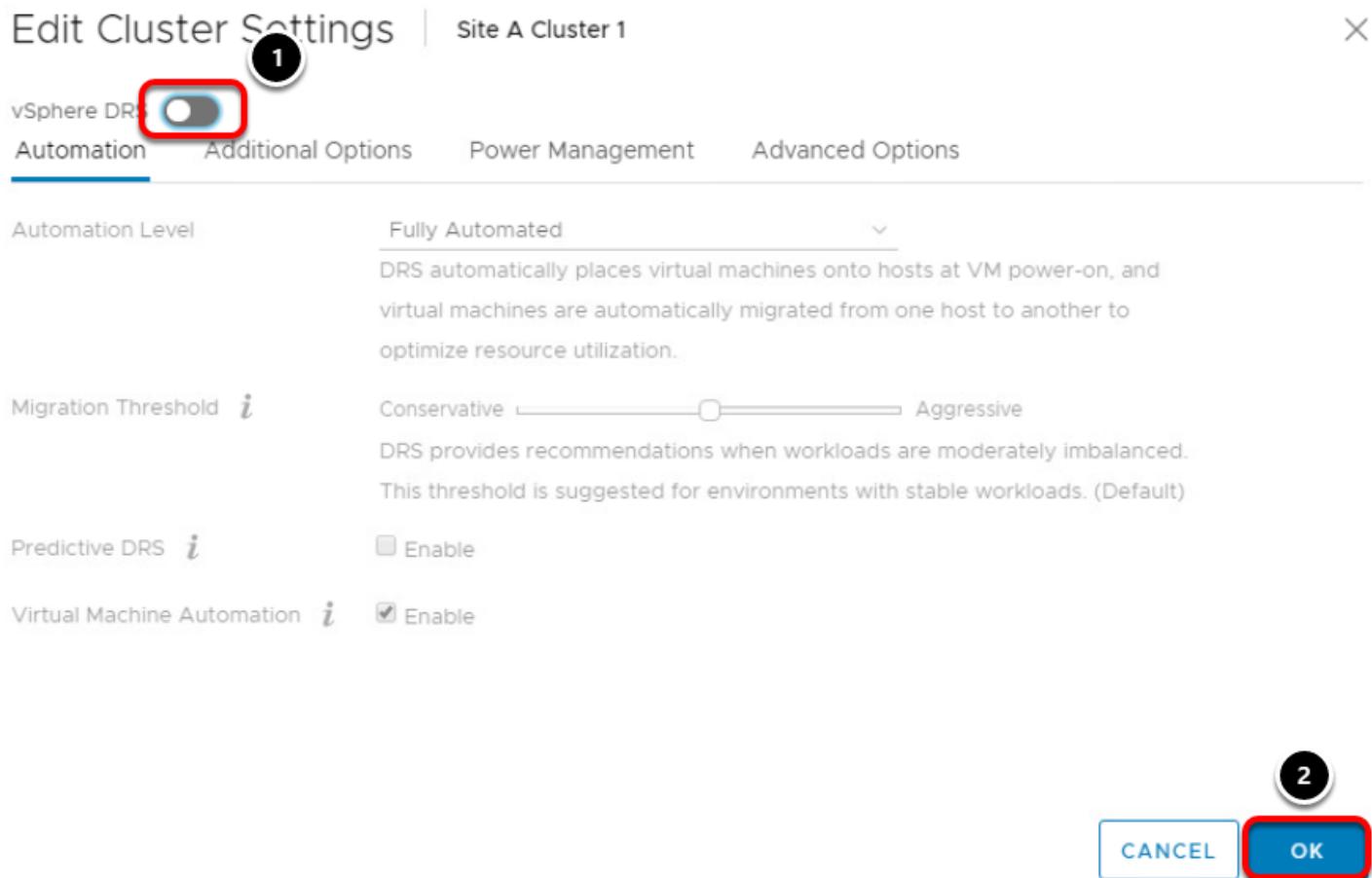
The screenshot shows the vSphere Web Client interface. The left sidebar shows a tree structure with 'vcsa-01a.corp.local' expanded, revealing 'Site A Datacenter' and 'Site A Cluster 1'. 'Site A Cluster 1' is selected and highlighted with a red box and a circled '1'. The top navigation bar has tabs: 'Summary', 'Monitor', 'Configure' (which is highlighted with a red box and circled '2'), 'Permissions', 'Hosts', 'VMs', 'Datastores', 'Networks', and 'Updates'. Below the navigation is a 'Site A Cluster 1' summary card. It displays 'vSphere DRS is Turned ON' with three buttons: 'SCHEDULE DRS...', 'RESTORE RESOURCE POOL TREE...', and 'EDIT...' (which is highlighted with a red box and circled '3'). The 'Configure' tab section shows 'Services' (with 'vSphere DRS' and 'vSphere Availability' sub-options) and 'Configuration' (with 'Quickstart', 'General', 'Licensing', and 'VMware EVC' sub-options). The 'vSphere DRS' section shows 'DRS Automation' as 'Fully Automated', 'Additional Options' as 'Expand for policies', 'Power Management' as 'Off', and 'Advanced Options' as 'None'.

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 **Site A Cluster 1**
2. Click the **Configure** tab

3. Click the **Edit** button

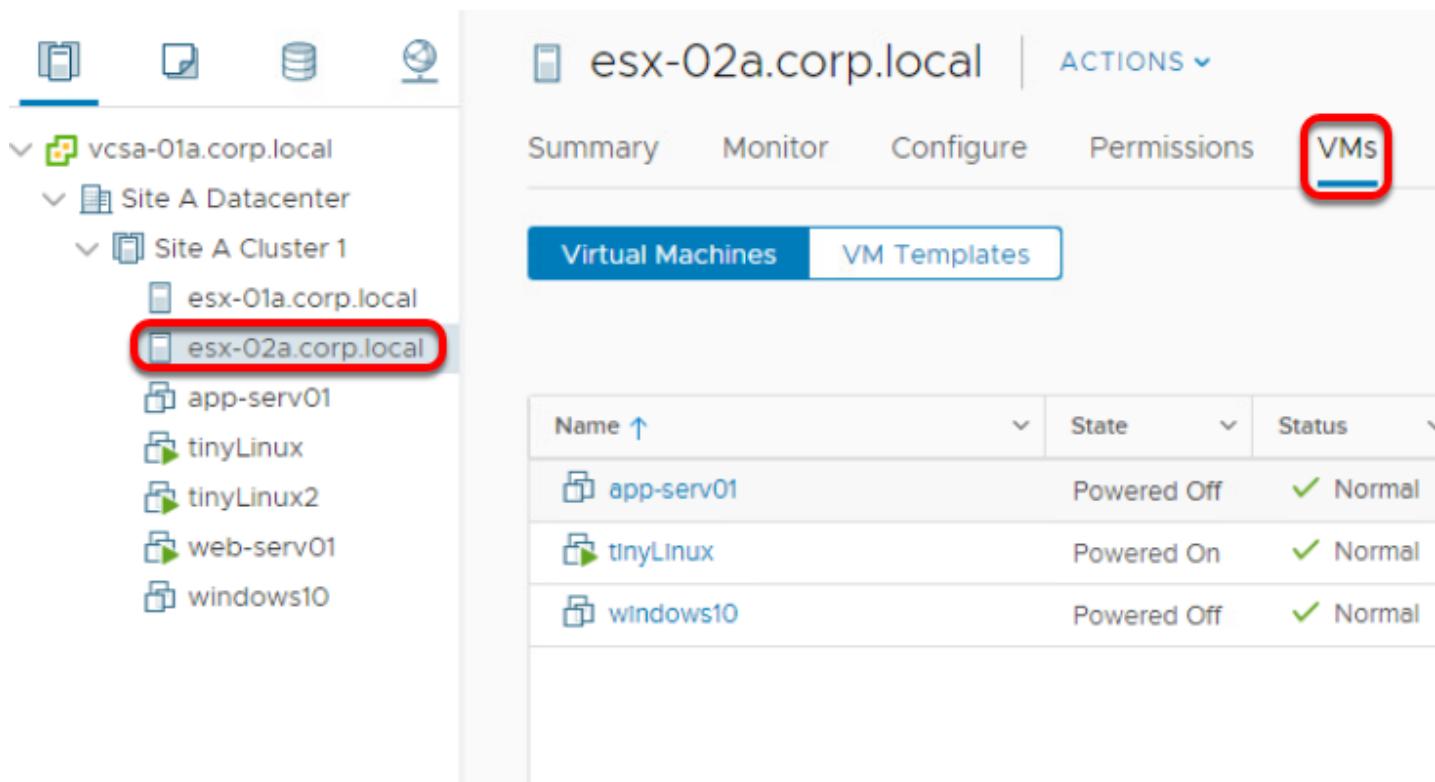
Disable DRS



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-02a.corp.local.

esx-02a.corp.local



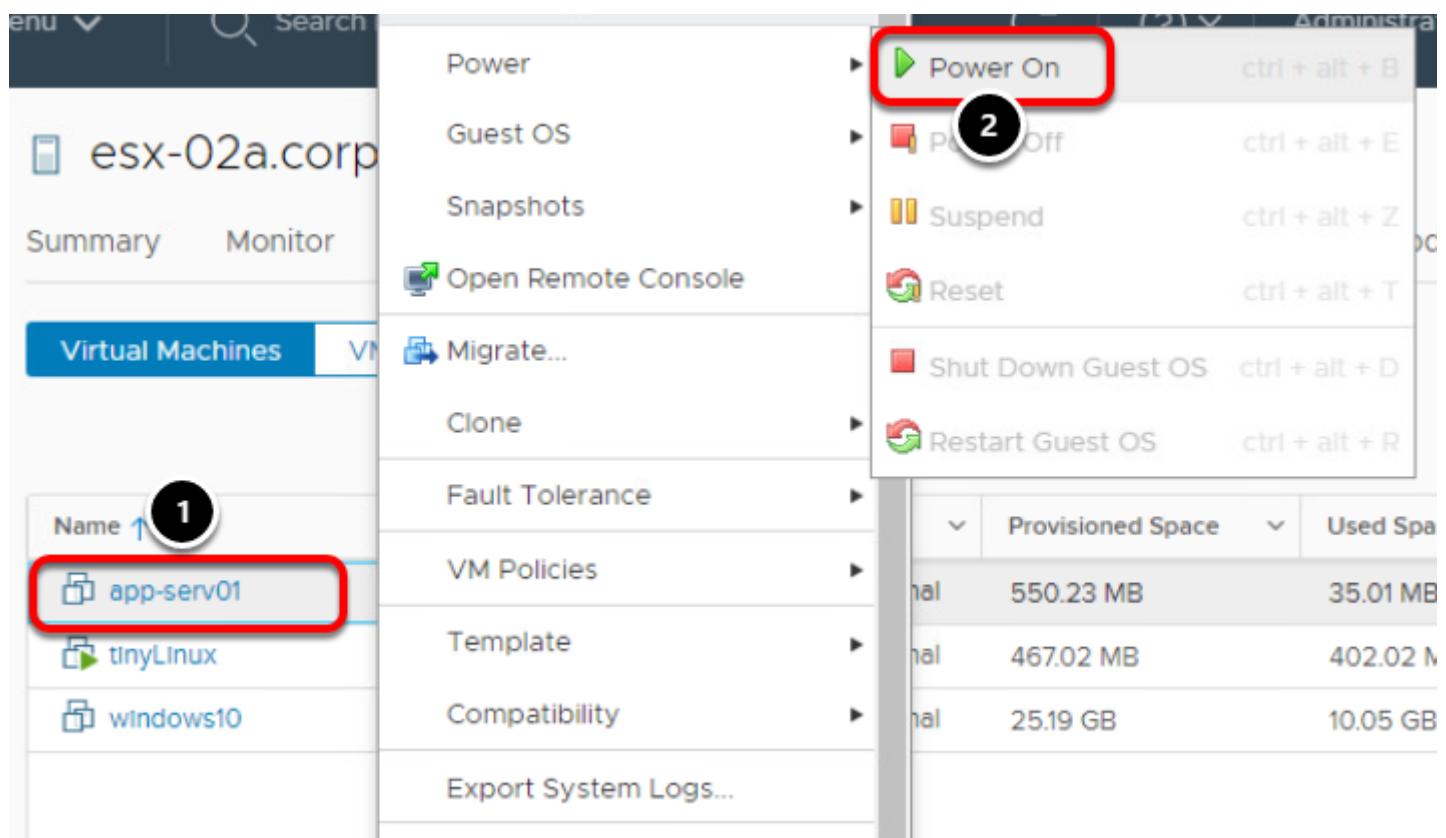
The screenshot shows the vSphere Web Client interface. On the left, a navigation tree displays the vCenter server 'vcsa-01a.corp.local' and its datacenter 'Site A Datacenter', which contains a cluster 'Site A Cluster 1'. Within this cluster, several virtual machines are listed: 'esx-01a.corp.local', 'esx-02a.corp.local' (which is highlighted with a red box), 'app-serv01', 'tinyLinux', 'tinyLinux2', 'web-serv01', and 'windows10'. On the right, the main content area is titled 'esx-02a.corp.local' and shows the 'VMs' tab selected. The 'VM Templates' tab is also visible. The 'VMs' table lists the following information:

Name	State	Status
app-serv01	Powered Off	Normal
tinyLinux	Powered On	Normal
windows10	Powered Off	Normal

1. Select **esx-02a.corp.local**
2. Click the **VMs** tab

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

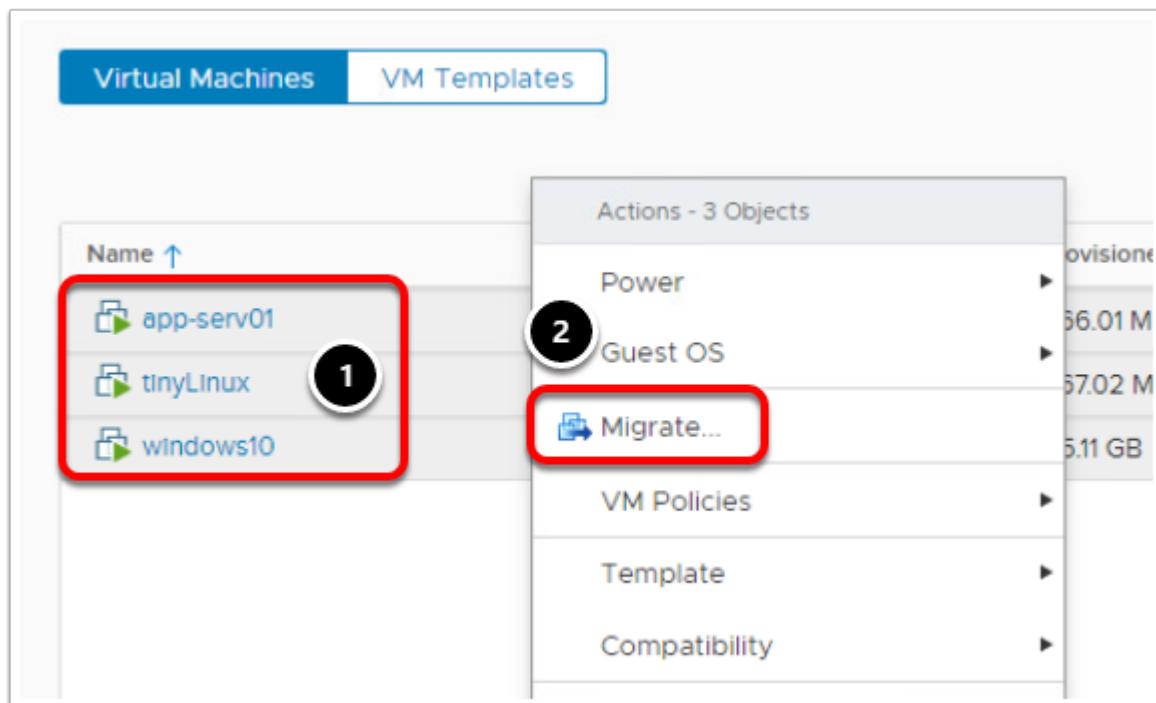
Power on VMs



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**

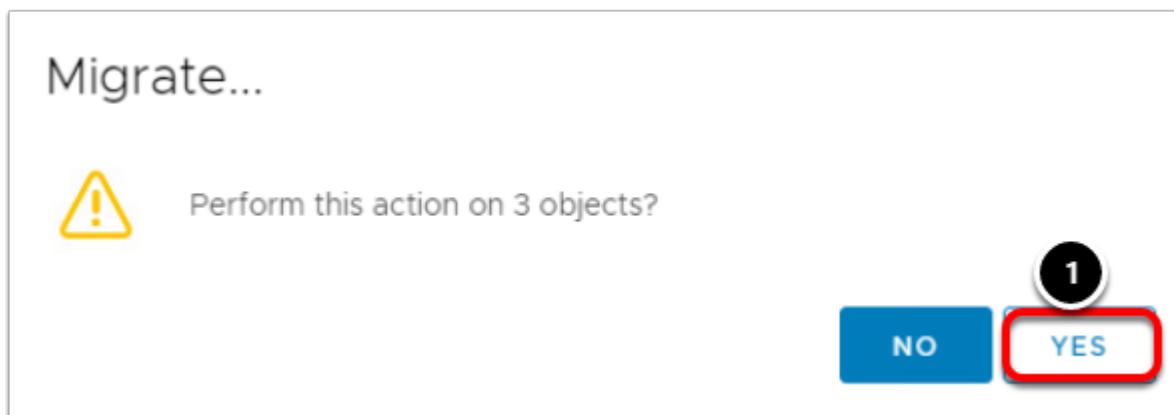
Do this for every powered off virtual machine, otherwise the next step will fail.

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

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

1

CANCEL

BACK

NEXT

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

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

Hosts Clusters Resource Pools vApps

Filter

Name	State	Status	Cluster
esx-01a.corp.local	Connected	Normal	Site A
esx-02a.corp.local	Connected	Normal	Site B

2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

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

Since we want to move all the virtual machines to esx-01a.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

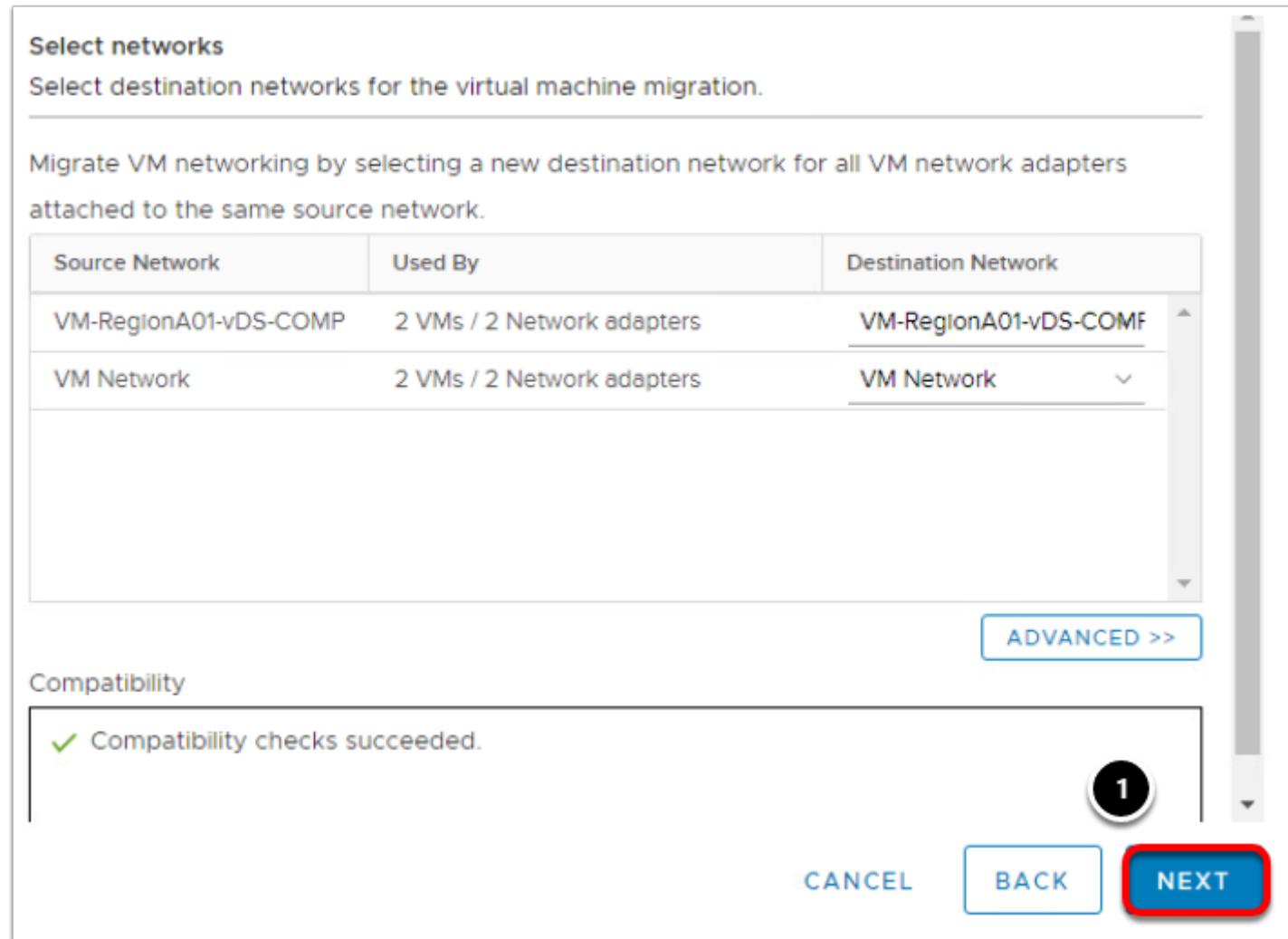
ADVANCED >>

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

CANCEL

BACK

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

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	Site A Cluster 1
Host	esx-01a.corp.local
vMotion Priority	High
Networks	No network reassignments

1

[CANCEL](#)[BACK](#)[FINISH](#)

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

Monitor Progress

Task Name	Target	Status
Relocate virtual machine	app-serv01	72%
Relocate virtual machine	tinyLinux	52%
Relocate virtual machine	windows10	10%

You can monitor progress using Recent Tasks.

Migration Complete

Name	State	Status	Provisioned Space
app-serv01	Powered On	Normal	466.34 MB
tinyLinux	Powered On	Normal	467.19 MB
tinyLinux2	Powered On	Normal	466.8 MB
web-serv01	Powered On	Normal	18.11 GB
windows10	Powered On	Normal	25.11 GB

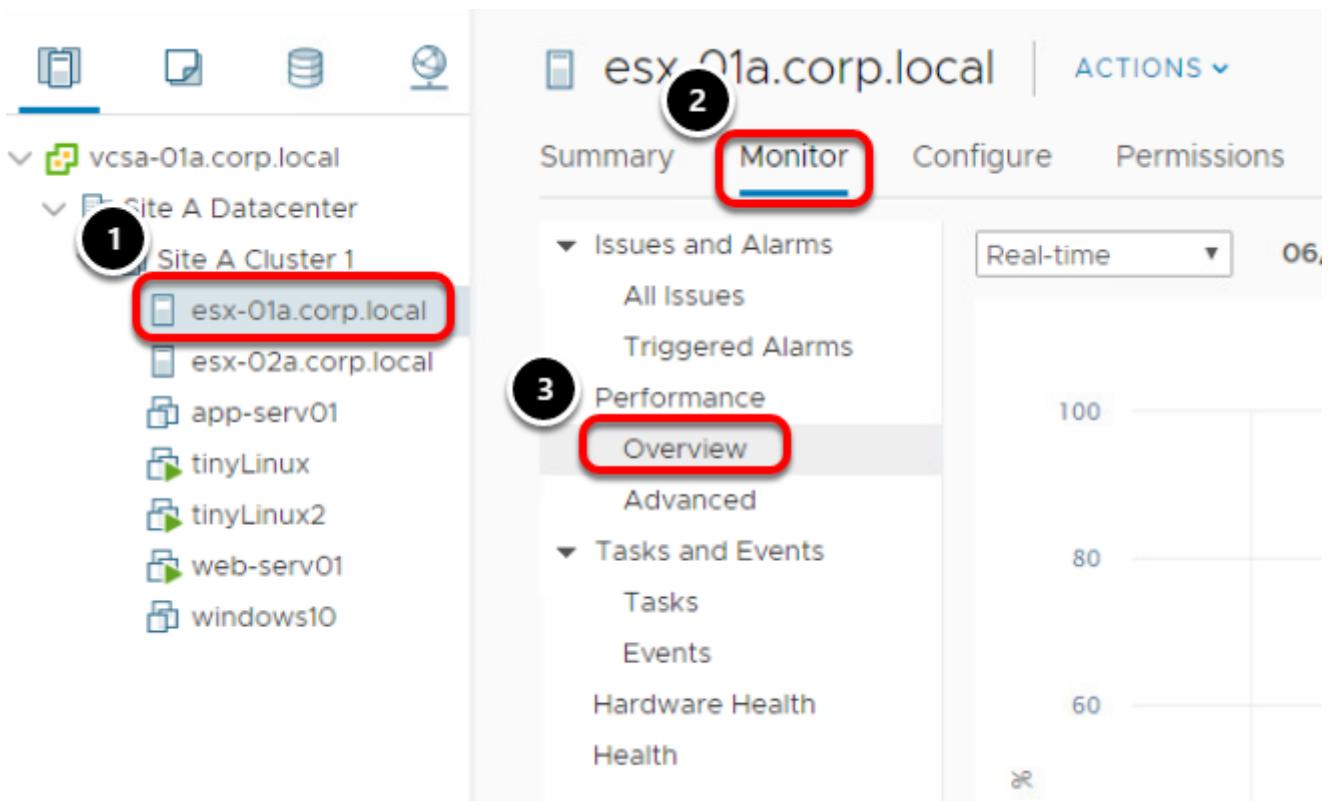
When the task has been completed successfully, you should see all of the virtual machines moved over to esx-01a.corp.local.

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.

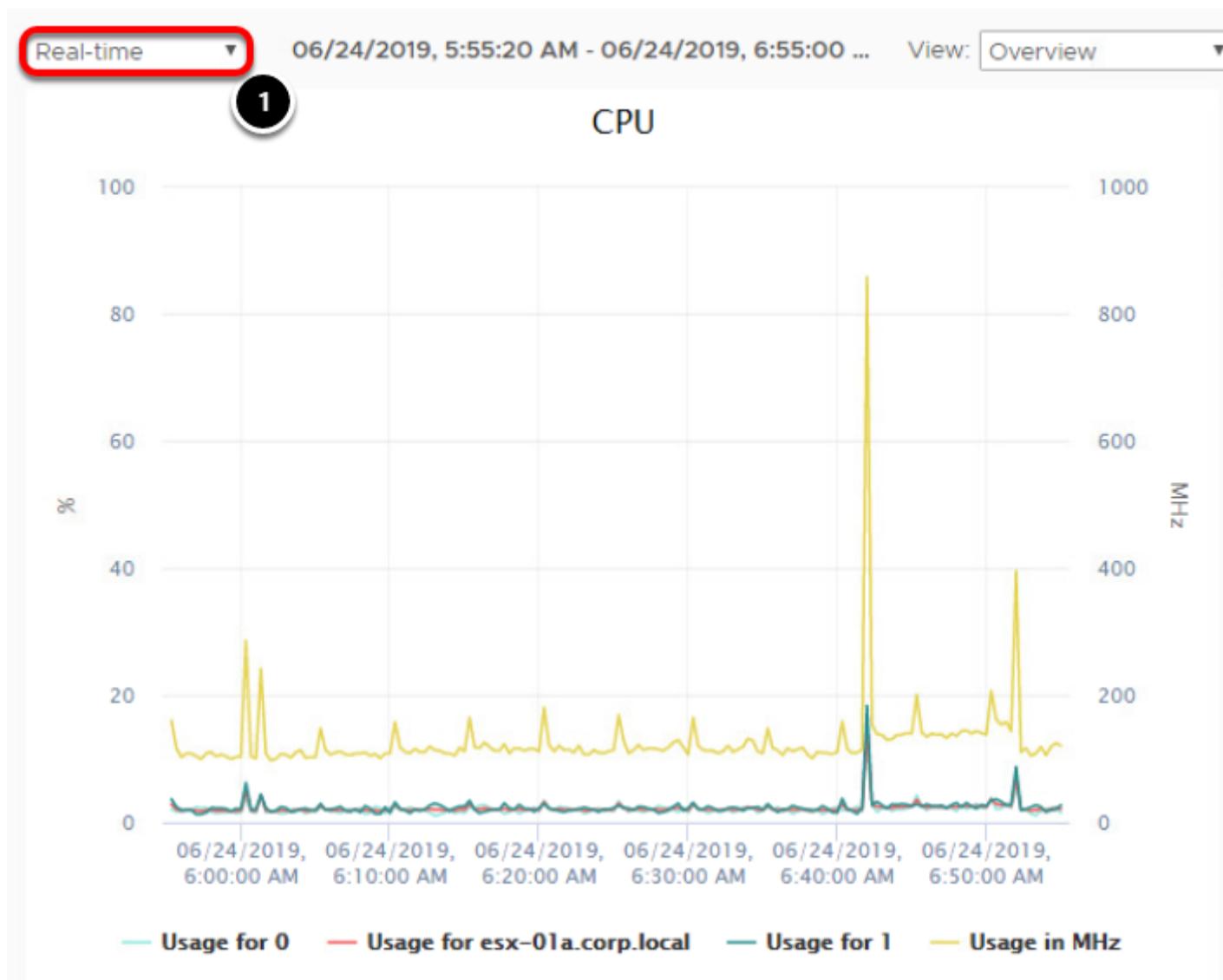
For a more advanced look at monitoring and performance, consider taking one of the vRealize Operations Hands-on Labs. vRealize Operations provides a more dynamic, proactive approach to monitoring your virtual infrastructure.

Select **esx-01a**



1. Select **esx-01a.corp.local**
2. Click the **Monitor** tab
3. Click **Overview** under the **Performance** section.

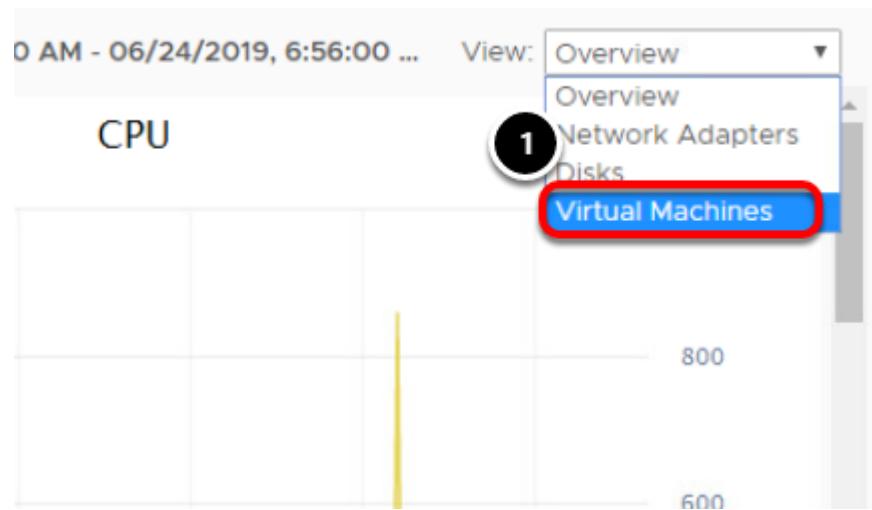
Host CPU Usage



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

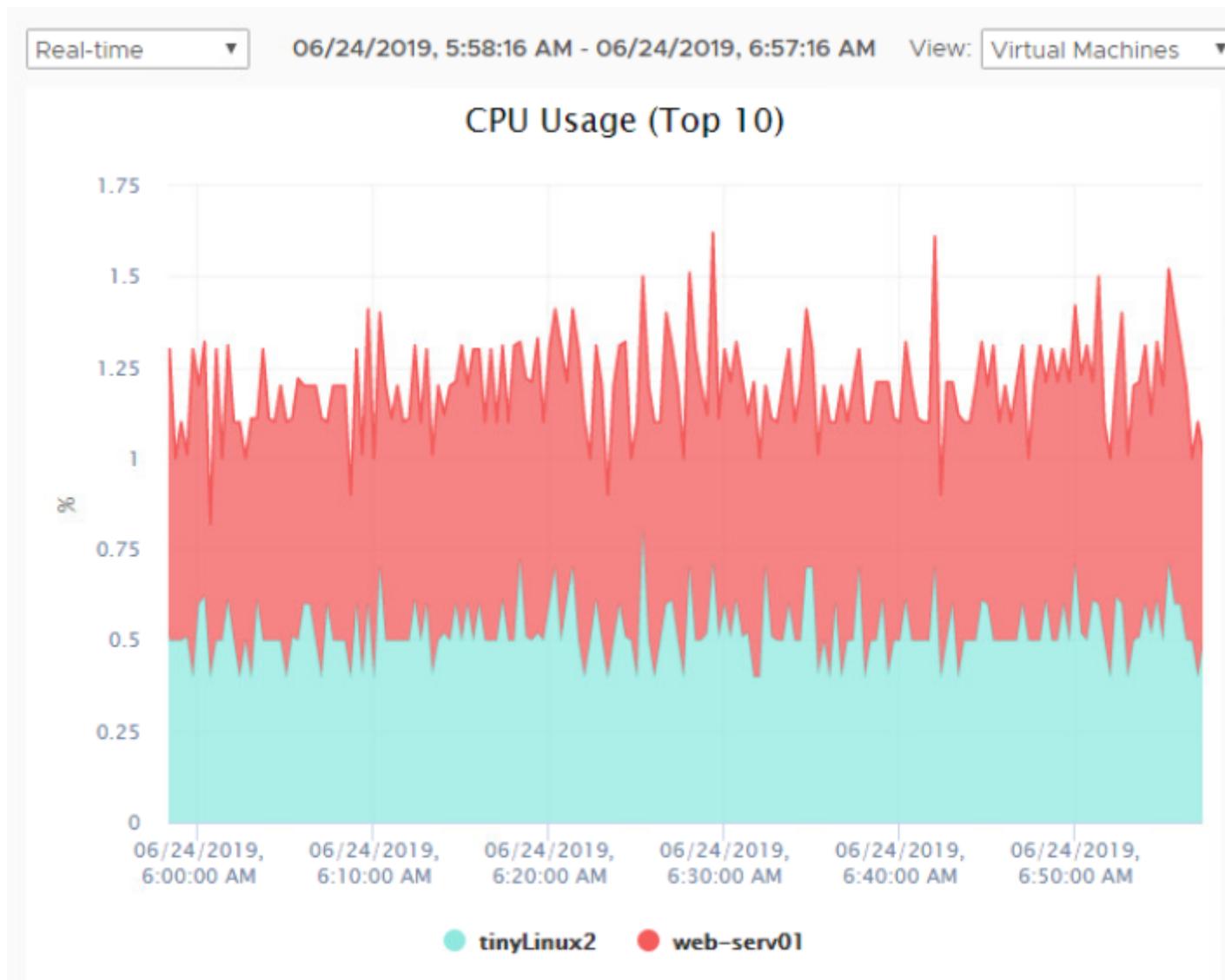
Here we can see in real time the CPU usage in percent for esx-01a.corp.local. By default, the chart will refresh every 20 seconds. The amount of data you see will depend on how long you have been taking the lab.

Virtual Machine CPU Usage



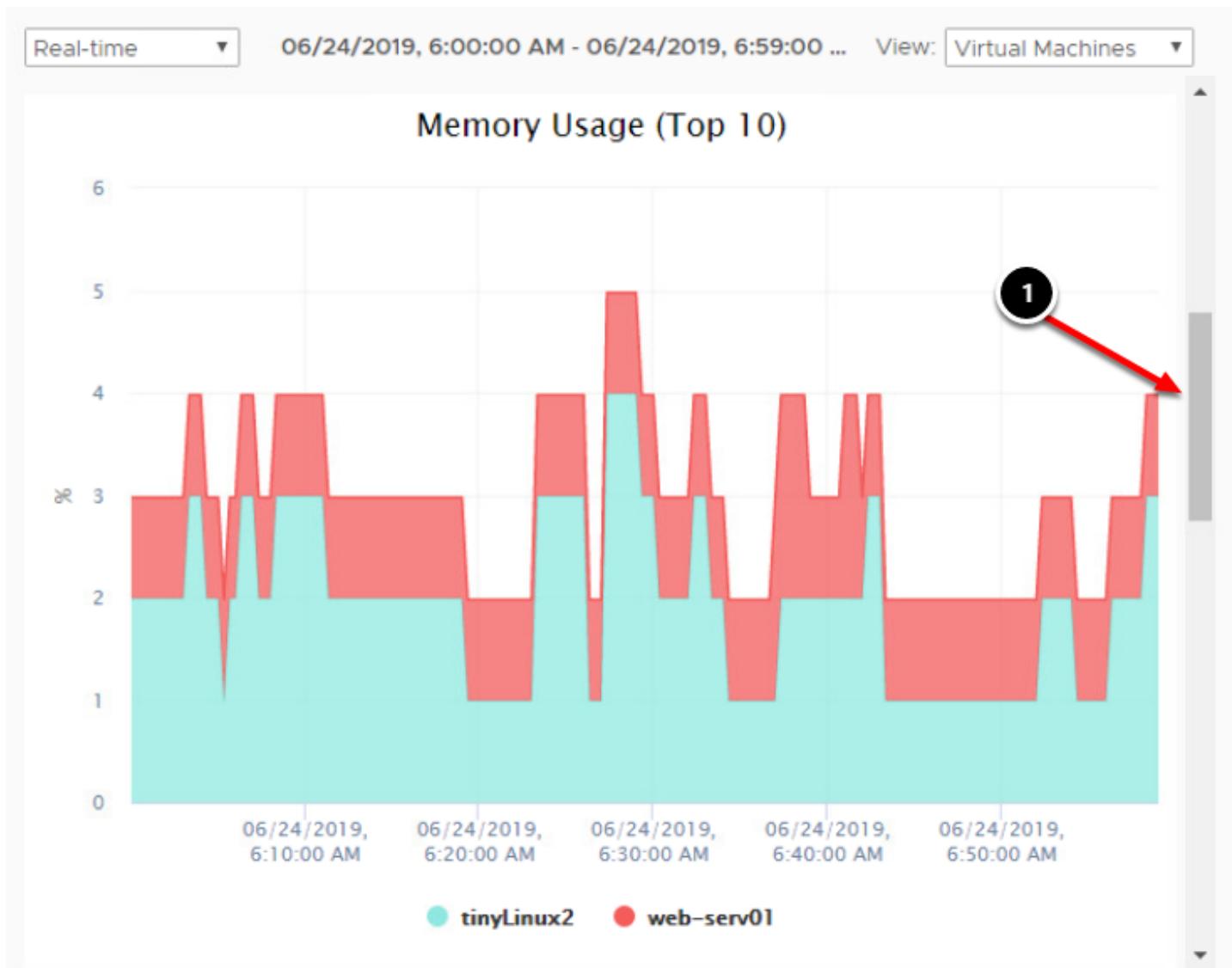
1. Now click the **View** drop-down box and select **Virtual Machines**.

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-01a.corp.local, the virtual machines will be rebooted.

1. Select **esx-01a.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. Click the **Restart** button

Confirm Restart

Confirm Guest Restart



Restart the guest operating systems for the selected virtual machines?



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

esx-01a.corp.local | ACTIONS ▾

VMs

Virtual Machines VM Templates

Name ↑

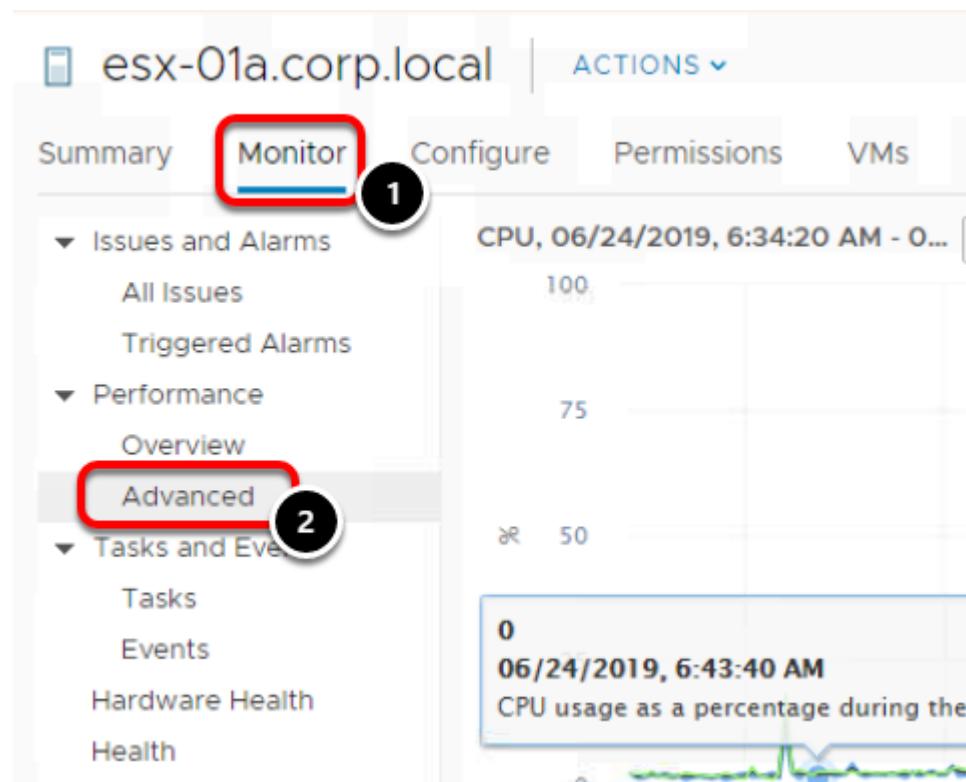
- app-serv01
- tinyLinux
- tinyLinux2
- web-serv01
- windows10

Actions - 3 Objects

- Power
- Guest OS
- Migrate...
- VM Policies
- Template

If tinyLinux, tinyLinux2, or app-serv01 did not restart, but instead shut down, select all and power them on manually.

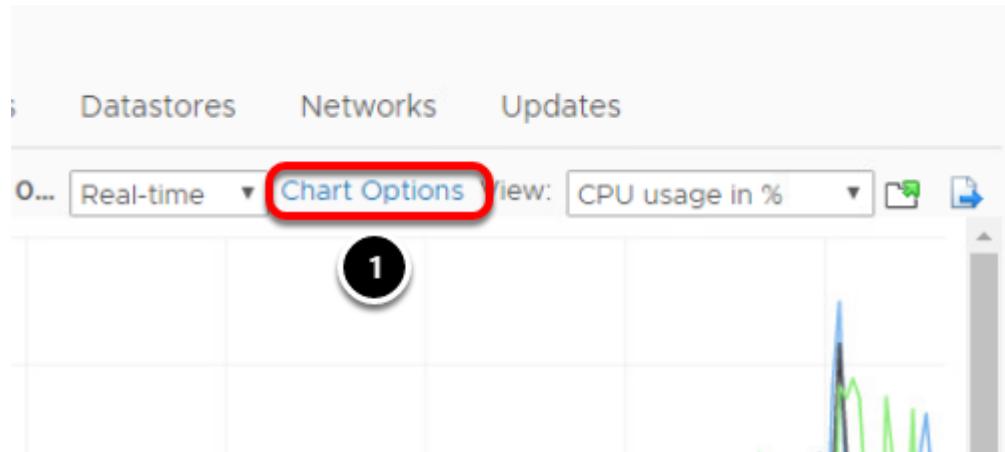
Monitor Performance



The screenshot shows the vSphere Web Client interface for a host named 'esx-01a.corp.local'. The 'Monitor' tab is selected, indicated by a red box and a circled '1'. In the 'Performance' section, the 'Advanced' link is highlighted with a red box and a circled '2'. The main content area displays a CPU usage chart for the date 06/24/2019, 6:34:20 AM, with a value of 0. A tooltip for the chart shows '0 06/24/2019, 6:43:40 AM CPU usage as a percentage during the last 10 minutes'.

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

esx-01a.corp.local X

- ▼ Save Options As... Delete Options

Select counters for this chart:

Counters	Rollups	Units	Internal Name	Stat Type	Description
Co-stop	Summation	ms	costop	Delta	Time the virtual ...
Core Utilization	Average	%	coreUtilization	Rate	CPU utilization ...
Demand	Average	MHz	demand	Absolute	The amount of ...
Idle	Summation	ms	idle	Delta	Total time that t...
Latency	Average	%	latency	Rate	Percent of time

Timespan: Real-time ▼

Last: Hour(s) ▼
 From:
 To:
(date and time are in ISO 8601 format)

Select object for this chart:

Target Objects
 esx-01a.corp.local
 0
 1

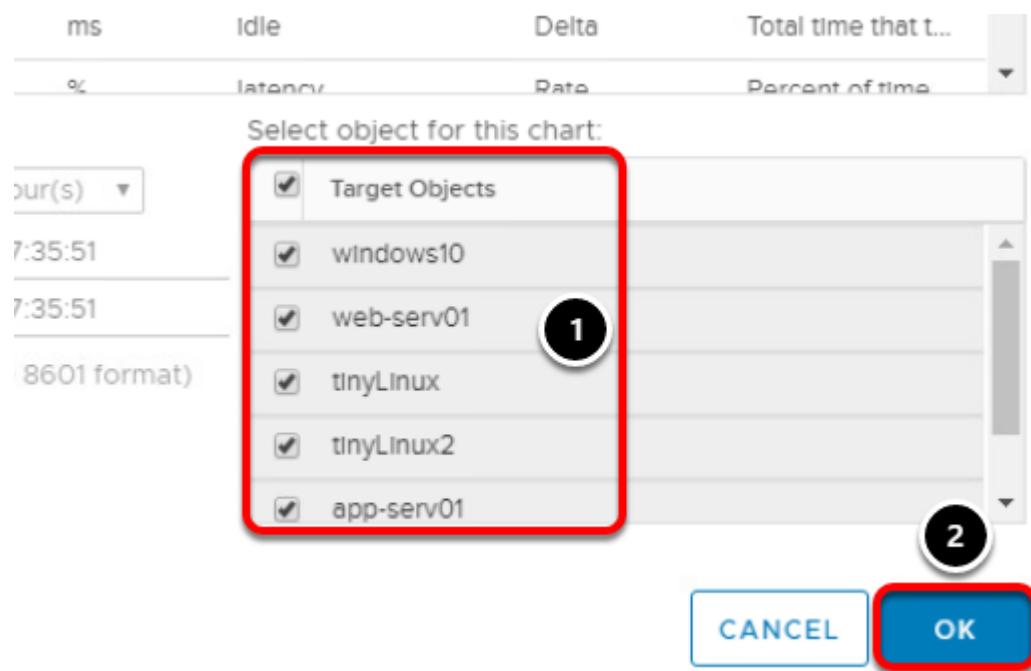
Chart Type: Line Graph ▼

Line Graph
Stacked Graph
Stacked Graph per VM

CANCEL OK

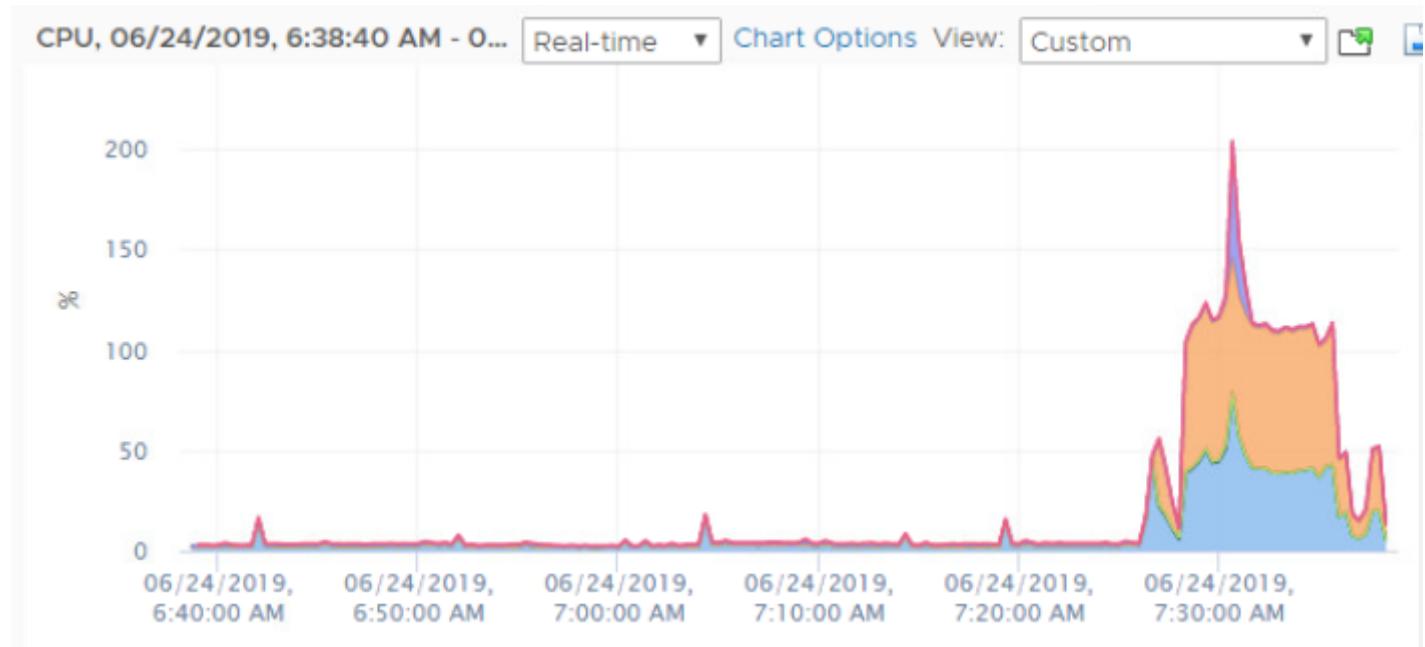
From the Chart Type drop-down menu, select **Stacked Graph per VM**.

Select Objects



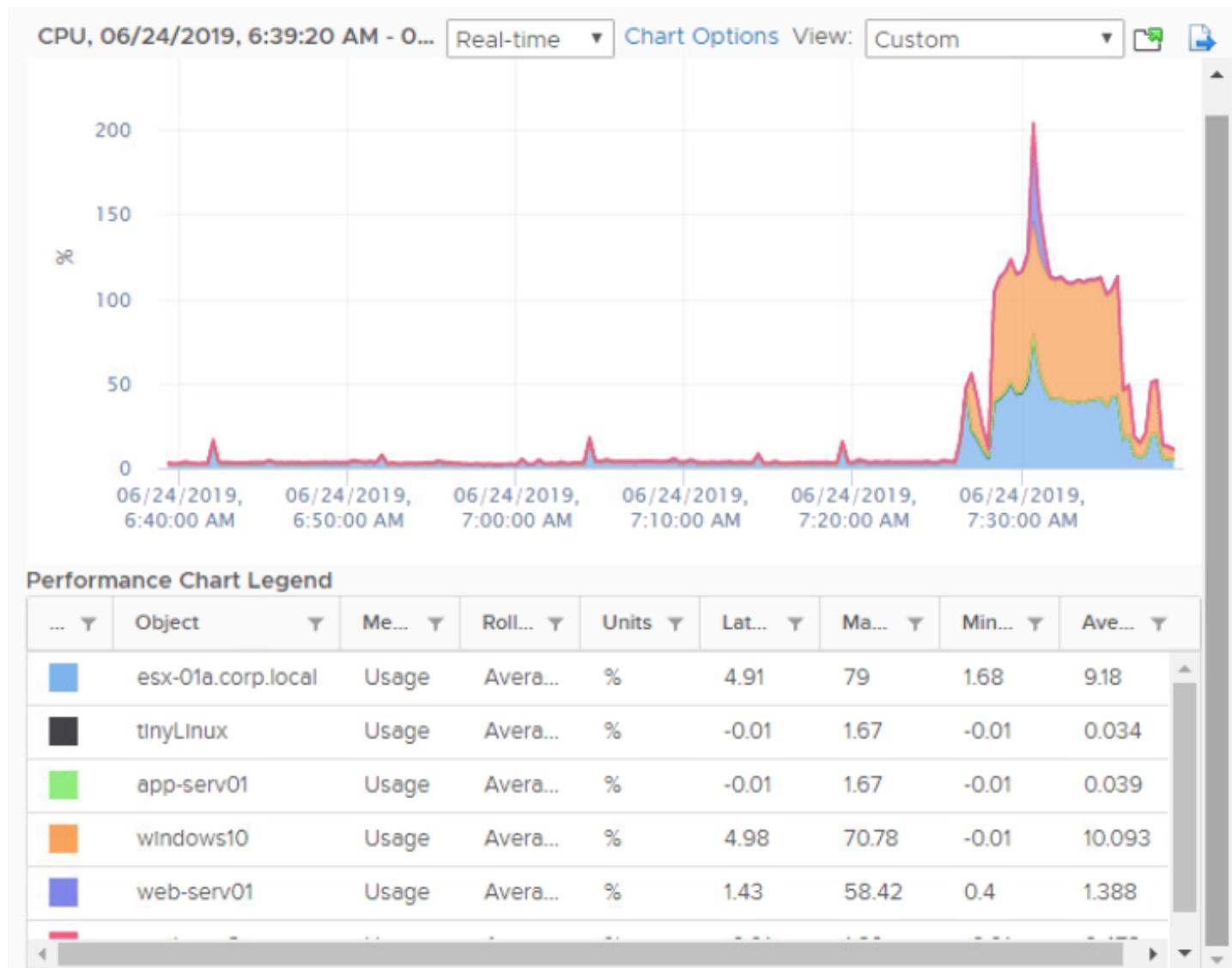
1. Under the Select objects for this chart box, verify all the virtual machines are selected.
2. Click the **OK** button to see the newly customized chart.

CPU Usage in Real-time



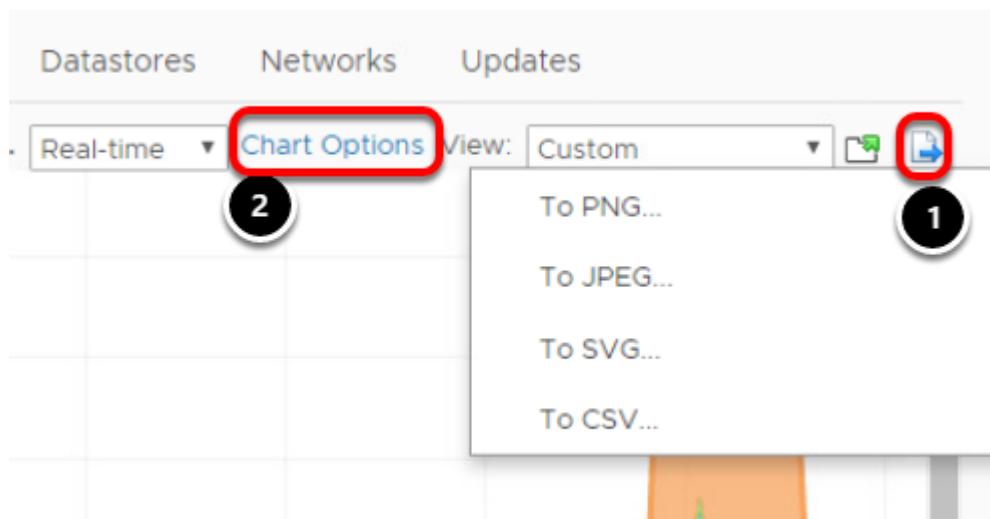
Here we can see the CPU usage of each virtual machine and esx-01a.corp.local.

Performance Chart Legend



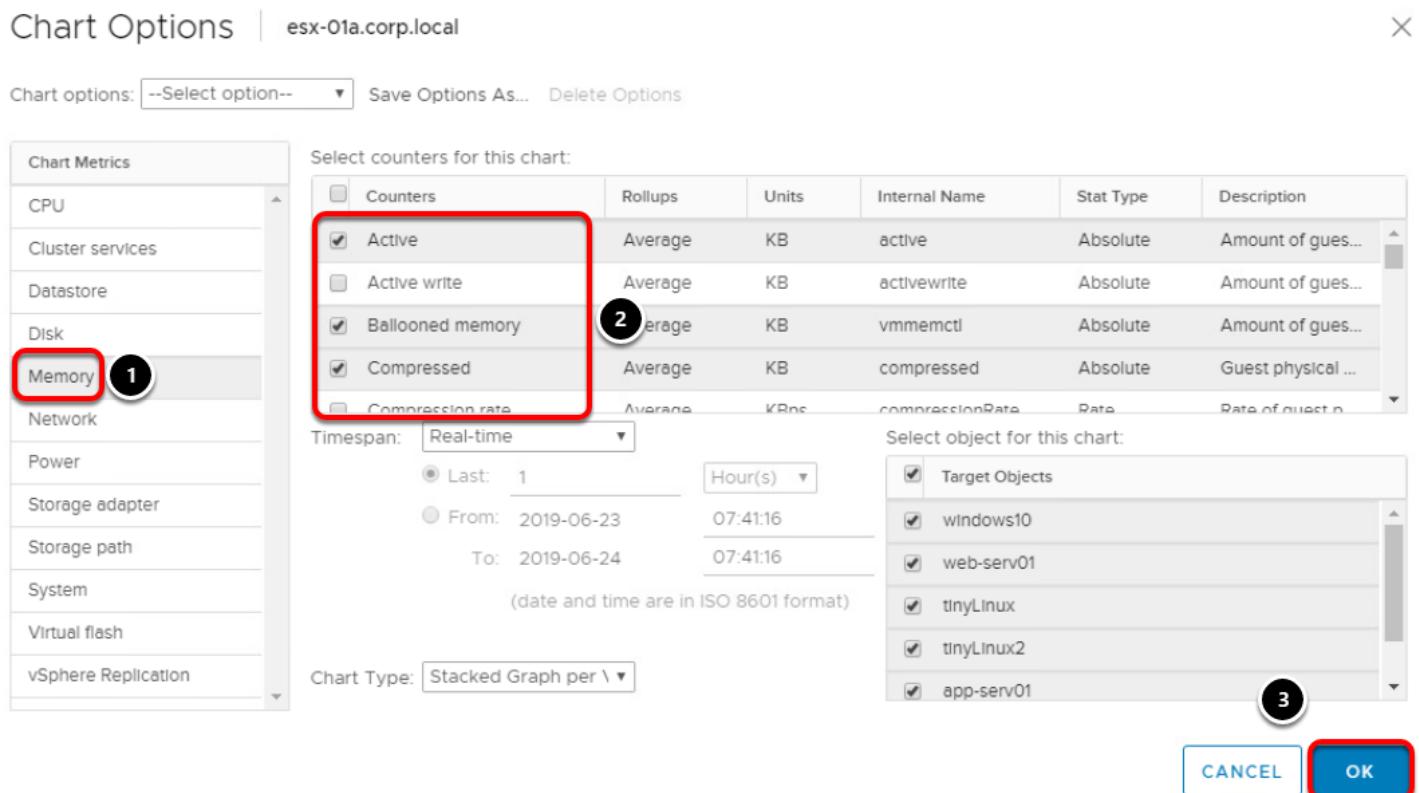
Scroll down and you will see the Performance Chart Legend. You can click on any of the virtual machines or esx-01a.corp.local to highlight it on the chart.

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**

Chart Options | esx-01a.corp.local X

! No counters selected

Chart options: Save Options As... Delete Options

Chart Metrics	Select counters for this chart:						
	Counters	Rollups	Units	Internal Name	Stat Type	Description	
CPU	<input type="checkbox"/>	Active	Average	KB	active	Absolute	Amount of gues...
Cluster services	<input type="checkbox"/>	Active write	Average	KB	activewrite	Absolute	Amount of gues...
Datastore	<input type="checkbox"/>	Ballooned memory	Average	KB	vmmemctl	Absolute	Amount of gues...
Disk	<input type="checkbox"/>	Compressed	Average	KB	compressed	Absolute	Guest physical ...
Memory	<input type="checkbox"/>	Compression rate	Average	KBps	compressionRate	Rate	Rate of questio...
Network							
Power							
Storage adapter							
Storage path							
System							
Virtual flash							
vSphere Replication							

Timespan: ▼

Last: 1 Hour(s)

From: 2019-06-23 07:45:04

To: 2019-06-24 07:45:04

(date and time are in ISO 8601 format)

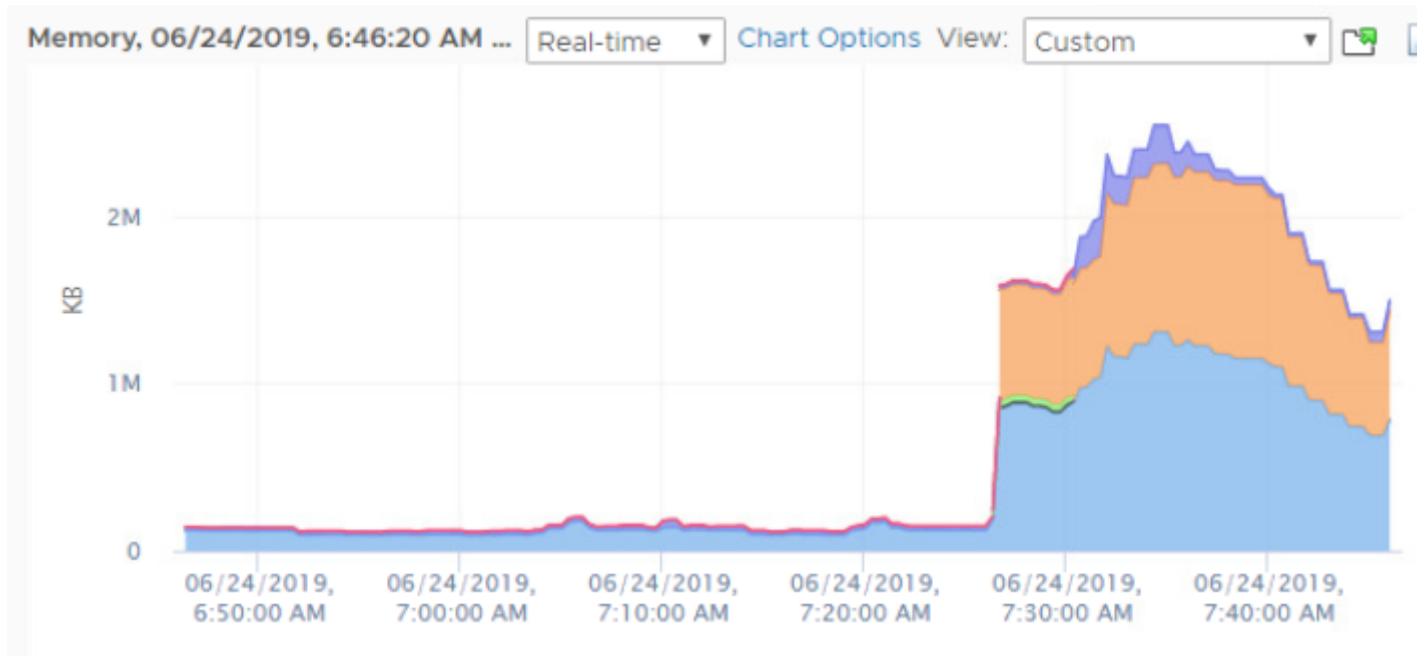
Chart Type:

Select object for this chart:

<input checked="" type="checkbox"/>	Target Objects
<input checked="" type="checkbox"/>	windows10
<input checked="" type="checkbox"/>	web-serv01
<input checked="" type="checkbox"/>	tinyLinux
<input checked="" type="checkbox"/>	tinyLinux2
<input checked="" type="checkbox"/>	app-serv01

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-01a.corp.local. Scroll down the Performance Chart Legend to see the counter each line represents.

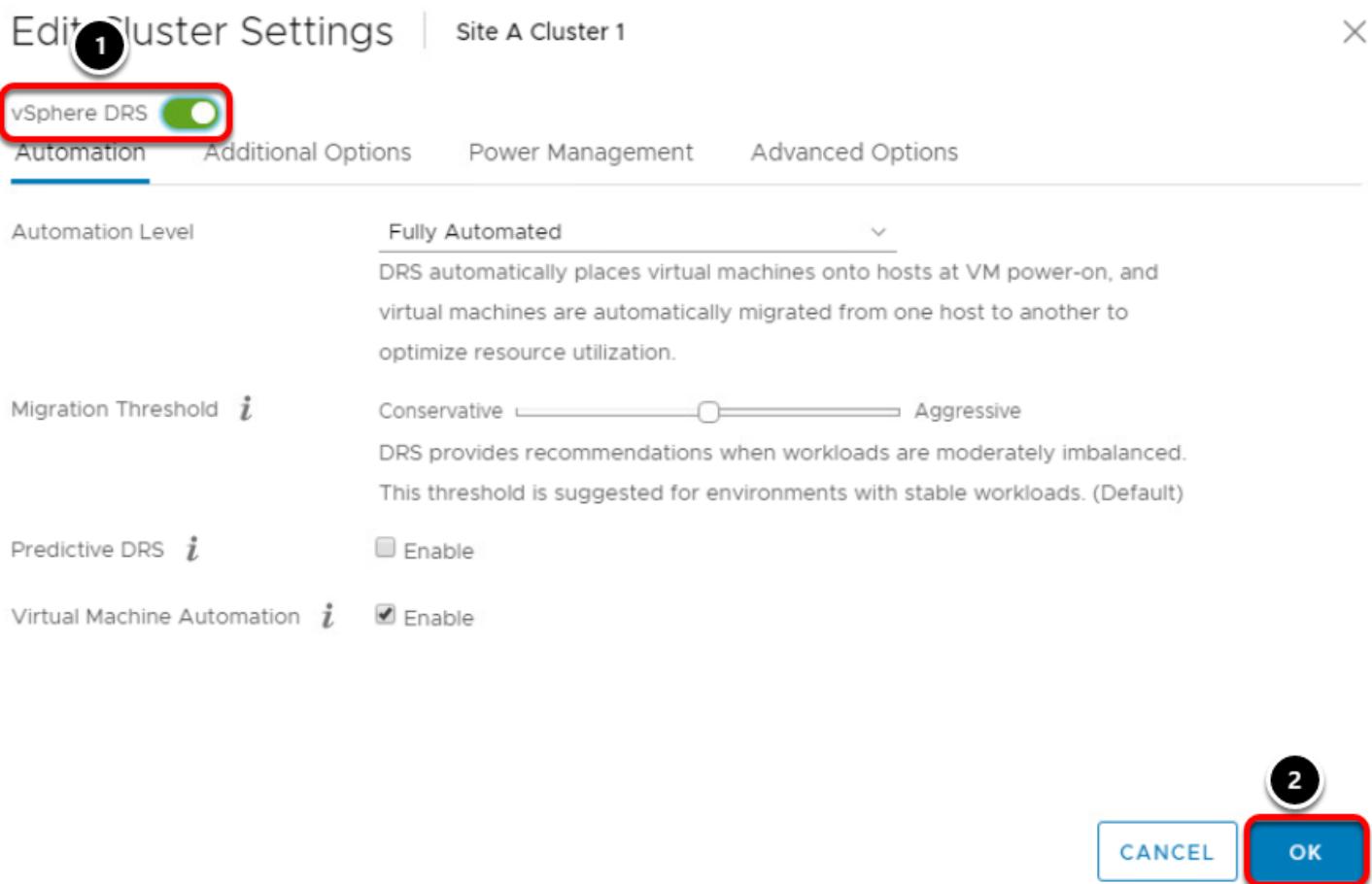
Feel free to explore the various chart options and/or continue to the next step.

Enable DRS

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

1. Select **Site A Cluster 1**
2. Click the **Configure** tab
3. Click on **vSphere DRS**
4. Click the **Edit** button

Turn ON vSphere DRS



1

2

Edit Cluster Settings | Site A Cluster 1

vSphere DRS

Automation Additional Options Power Management Advanced Options

Automation Level Fully Automated

Migration Threshold *i* Conservative Aggressive

Predictive DRS *i* Enable

Virtual Machine Automation *i* Enable

CANCEL OK

Check the **Turn ON vSphere DRS** box to enable DRS and click OK.

Further Information

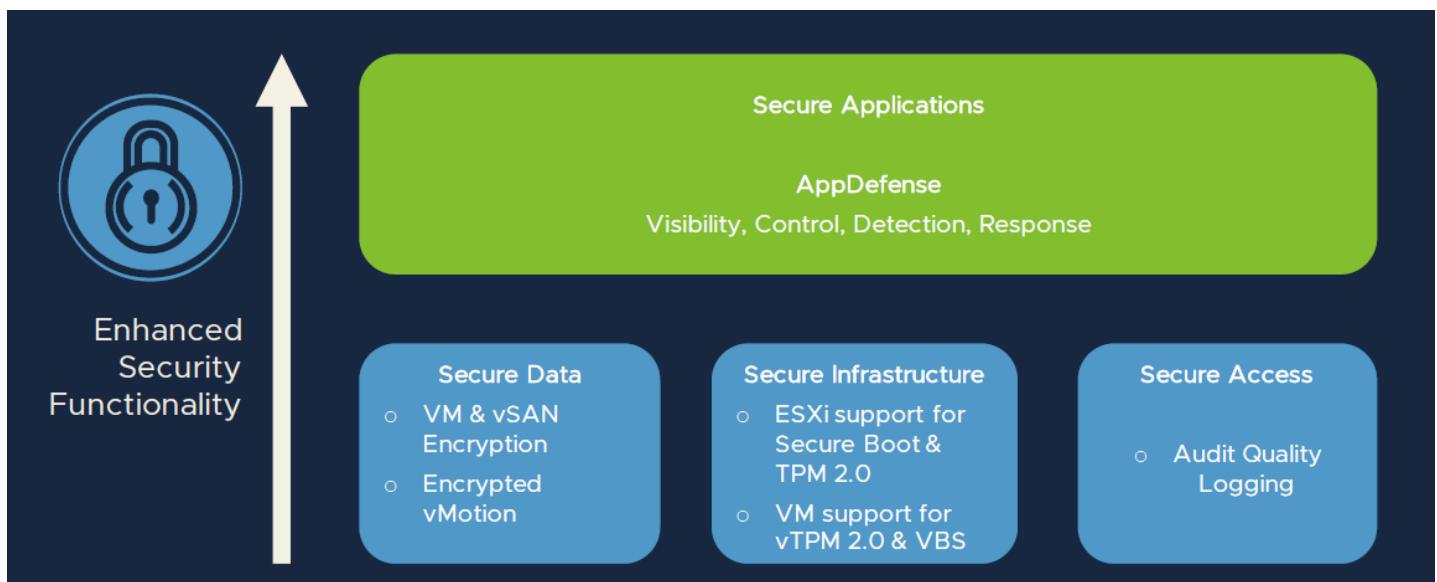
For more information on performance charts, you can view the [vSphere Monitoring and Performance](#) guide.

Introduction to vSphere Platinum

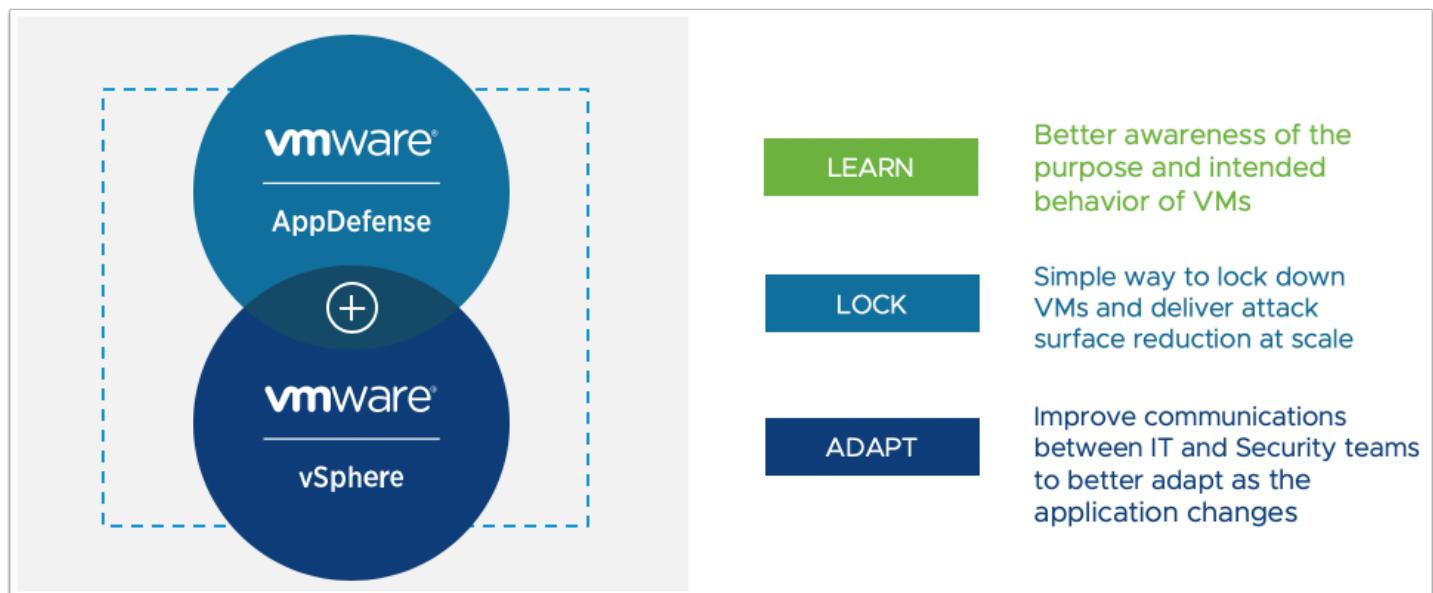
VMware vSphere Platinum delivers advanced security capabilities fully integrated into the world's leading hypervisor for complete data center protection. It combines vSphere and VMware AppDefense in a purpose-built, operationally simple solution with minimal overhead and performance impact.

AppDefense is a data center endpoint security solution that embeds threat detection and response into the virtualization layer and uses machine learning to ensure virtual machines (VMs) and applications are running in a known-good state.

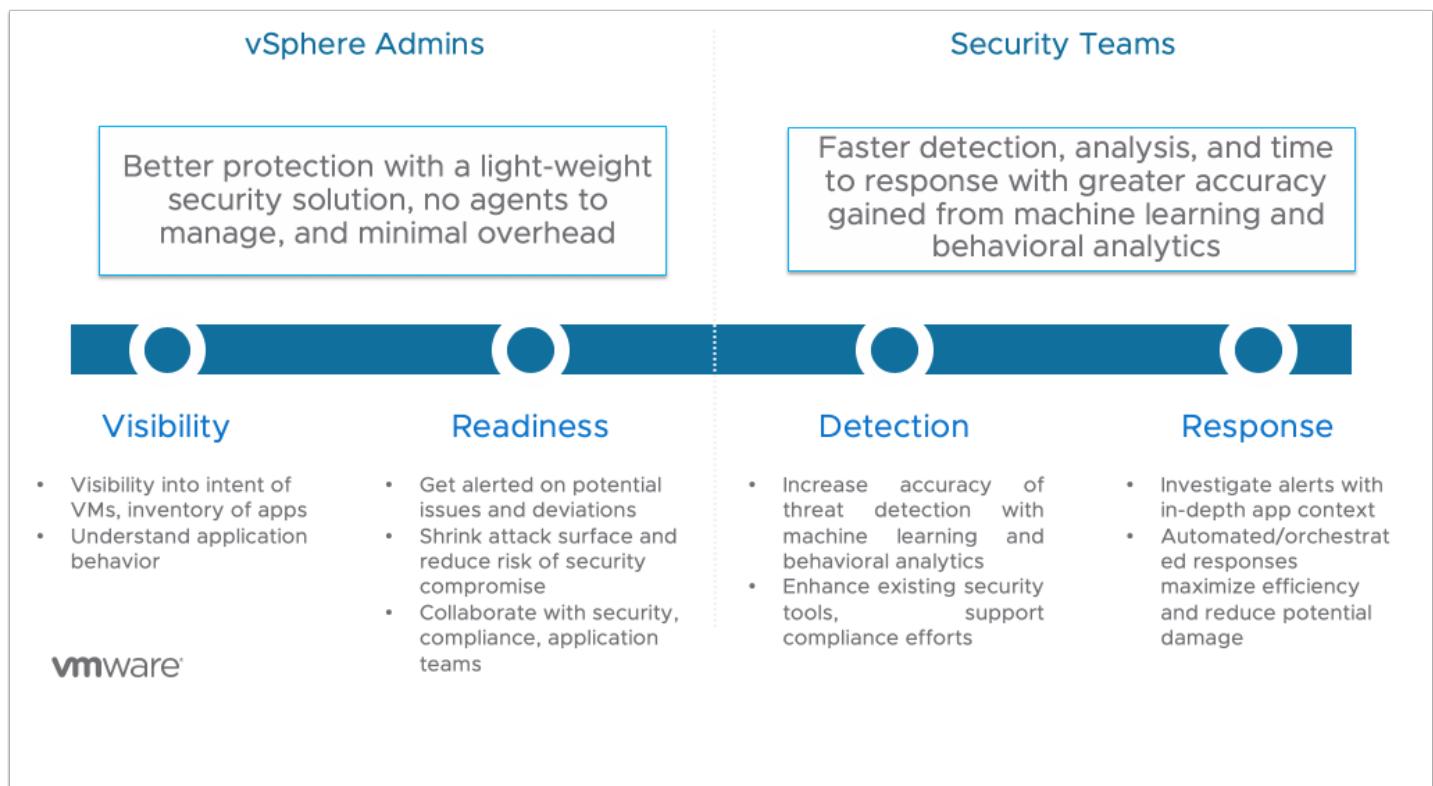
vSphere Platinum operates at the heart of the secure, software-defined data center (SDDC) where organizations house their most sensitive data and business-critical applications. It extends security from the IT architectural foundation across the entire environment to comprehensively secure applications, data, infrastructure, and access.



Introducing vSphere Platinum



VMware vSphere Platinum: Key Benefits



Video: vSphere Platinum (1:48)

This video gives a high-level overview of vSphere Platinum.

Hands-on Labs Interactive Simulation: vSphere Platinum

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.

Conclusion

This concludes Module 1 - Introduction to Management with vCenter Server. 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 Module to quickly jump to that content in the Manual.

- [Module 2 - An Introduction to vSphere Networking and Security \(60 Minutes\)](#)
- [Module 3 - An Introduction to vSphere Storage \(60 Minutes\)](#)

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

Introduction

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

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)

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)

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:

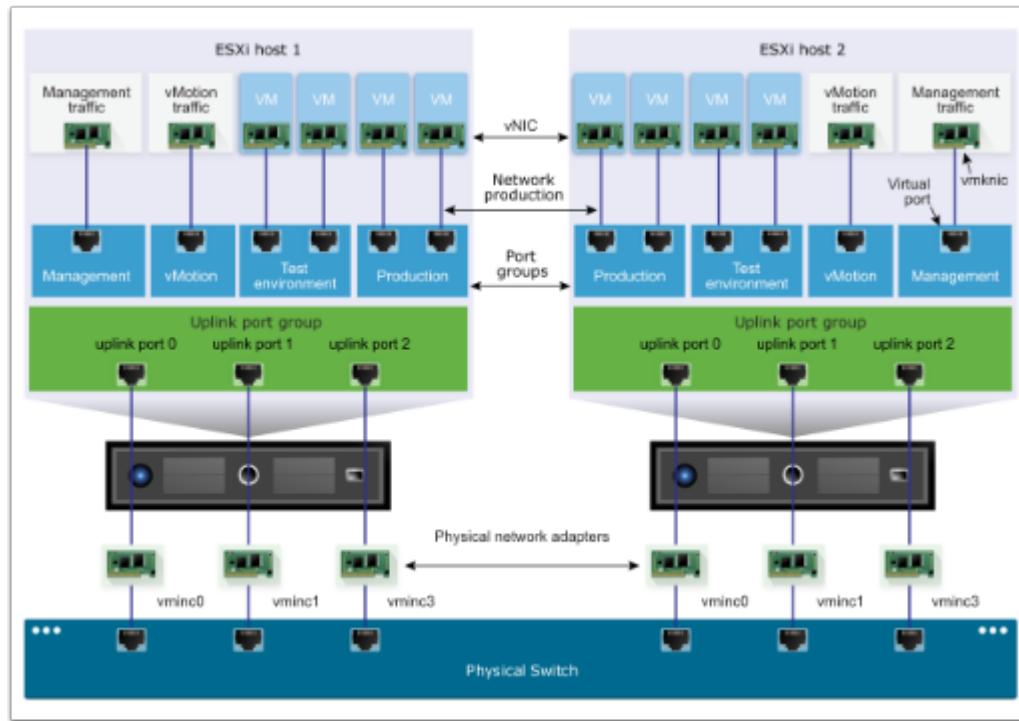
- Network IO Control New support for per virtual machine Distributed vSwitch bandwidth reservations to guarantee isolation and enforce limits on bandwidth.
- Multicast Snooping - Supports IGMP snooping for IPv4 packet and MLD snooping for IPv6 packets in VDS. Improves performance and scale with multicast 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

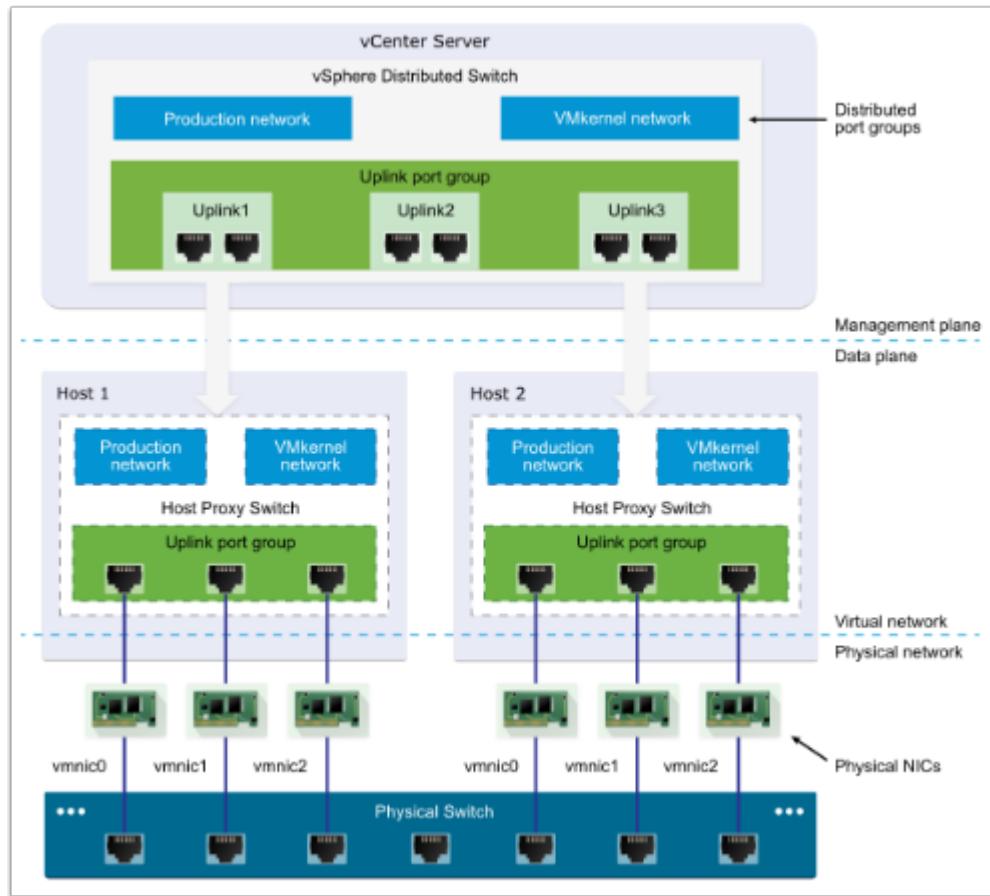
Spend a few minutes reviewing the differences between the Standard vSwitch and Distributed vSwitch architectures.

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

vSphere Standard Switch Architecture



vSphere Distributed Switch Architecture



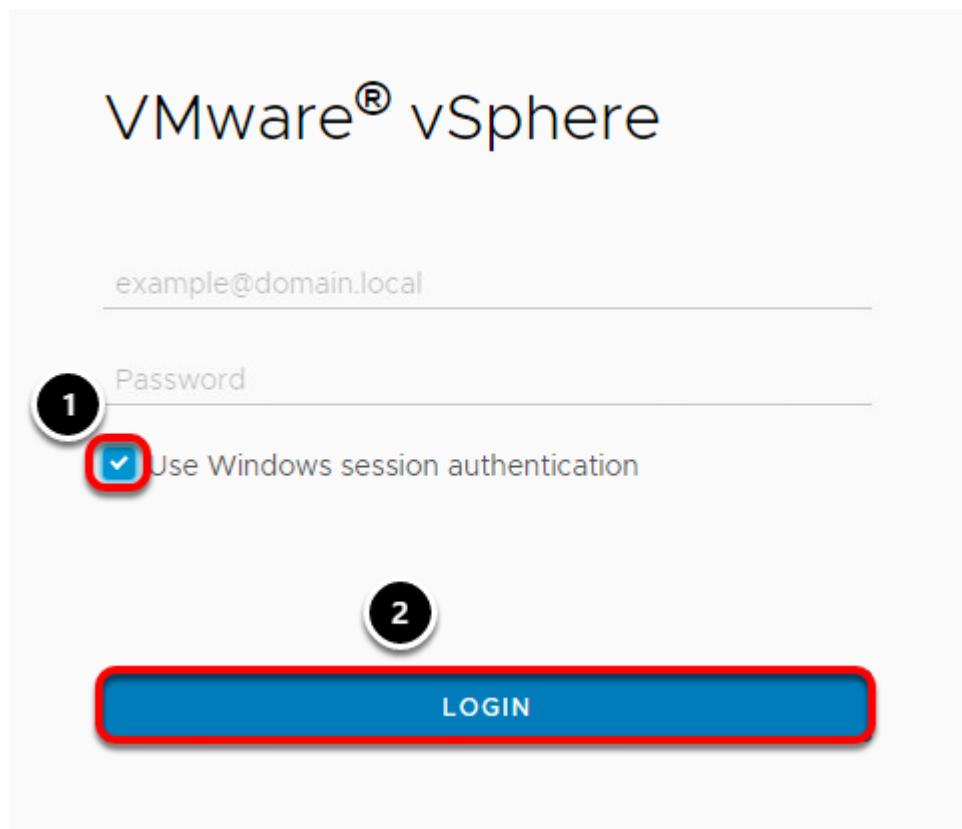
Let's get started!

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

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

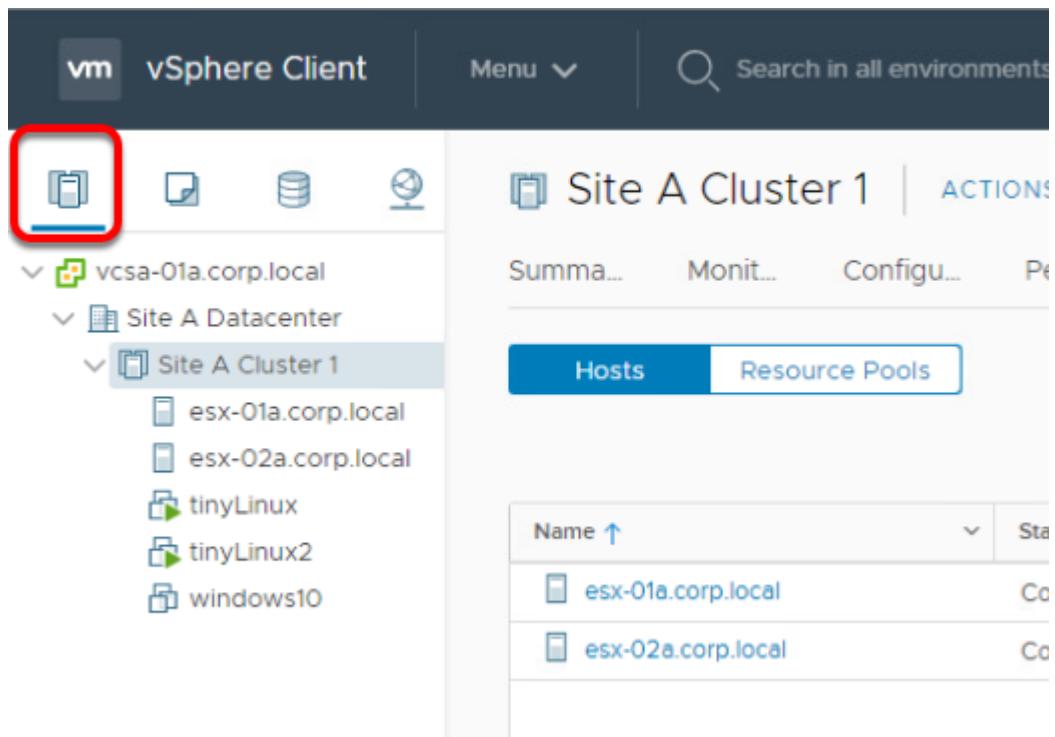
Adding a Virtual Machine Port Group with the vSphere Client



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

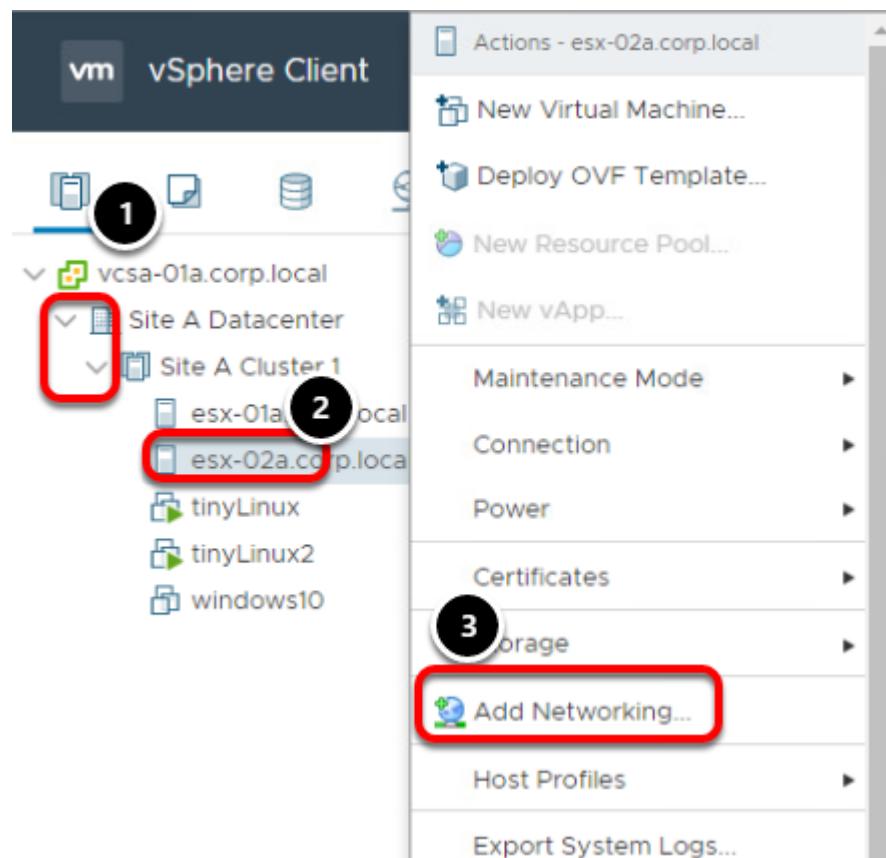


The screenshot shows the vSphere Client interface. The top navigation bar includes the 'vSphere Client' logo, a 'Menu' dropdown, and a search bar. The left sidebar is titled 'Hosts and Clusters' and shows a tree structure: 'vcsa-01a.corp.local' > 'Site A Datacenter' > 'Site A Cluster 1'. The 'Site A Cluster 1' node is selected. The right panel displays 'Site A Cluster 1' with tabs for 'Hosts' (selected) and 'Resource Pools'. Below the tabs is a table with columns 'Name' and 'Status'. Two hosts are listed: 'esx-01a.corp.local' and 'esx-02a.corp.local', both marked as 'Connected'.

Name	Status
esx-01a.corp.local	Connected
esx-02a.corp.local	Connected

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

Add Networking



1. Under vcsa-01a.corp.local, expand **Site A Datacenter** and then **Site A Cluster** **1**.
2. Next, right-click on **esx-02a.corp.local** in the Navigator.
3. Select **Add Networking....**

Connection Type

esx-02a.corp.local - Add Networking

1 Select connection type

2 Select target device

3 Connection settings

4 Ready to complete

Select connection type

Select a connection type to create.

VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

Virtual Machine Port Group for a Standard Switch

1

A port group handles the virtual machine traffic on standard switch.

Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

2

CANCEL

BACK

NEXT

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

Target Device

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

Select target device

Select a target device for the new connection.

Select an existing standard switch

New standard switch

MTU (Bytes)

1500

BROWSE ...

1

2

CANCEL

BACK

NEXT

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



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

CANCEL

BACK

NEXT

1. Click the '+' button.

Add Physical Adapter

Add Physical Adapters to the Switch X

Network Adapters

All	Properties	CDP	LLDP
vmnic3			
1			
Adapter Name	VMware Inc. vmxnet3 Virtual Ethernet Controller		
Location	PCI 0000:04:00.0		
Driver	nvmxnet3		
Status			
Status	Connected		
Actual speed, Duplex	10000 Mb, Full Duplex		
Configured speed, Duplex	10000 Mb, Full Duplex		
Networks	No networks		
Network I/O Control			
Status	Allowed		
SR-IOV			
Status	Not supported		
Cisco Discovery Protocol			
Cisco Discovery Protocol is not available on this physical network adapter			
Link Layer Discovery Protocol			
Link Layer Discovery Protocol is not available on this physical network adapter			
2			
CANCEL	OK		

1. Select **vmnic3** under Network Adapters
2. Click '**OK**'

Add Physical Adapter

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

All	Properties	CDP	LLDP
Adapter	VMware Inc		
Name	vmnic3		
Location	PCI 0000:0		
Driver	nvmxnet3		
Status			
Status	Connected		
Actual speed, Duplex	10000 Mb, Full		
Configured speed,			
Duplex			
Networks	No network		
Network I/O Control			
Status	Allowed		

+ | **×** **↑** **↓**

Active adapters

 (New) vmnic3

Standby adapters

Unused adapters

CANCEL

BACK

NEXT

1

1. Click **Next** to continue.

Connection Settings

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

Connection settings

Use network labels to identify migration-compatible connections common to two or more hosts.

Network label

VM Network 2

VLAN ID

None (0)



1

CANCEL

BACK

NEXT

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

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

Ready to complete

Review your settings selections before finishing the wizard.

New standard switch	vSwitch1
Virtual machine port group	VM Network 2
Assigned adapters	vmnic3
Switch MTU	1500
VLAN ID	None (0)

1

CANCEL

BACK

FINISH

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

Virtual Switches

esx-02a.corp.local | ACTIONS ▾

Summary Monitor **Configure** Permissions

Storage

- Storage Adapters
- Storage Devices
- Host Cache Configuration
- Protocol Endpoints
- I/O Filters

Networking

- Virtual switches** (highlighted with a red box and circled '1')
- VMkernel adapters

Virtual switches

- Distributed Switch: R**
- ESXi-RegionA
 - VLAN ID: --
 - VMkernel Ports
 - Virtual Machine

Next, we will verify the switch has been created.

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

Standard Switch: vSwitch1

Virtual switches

Virtual Machines (0) ADD NETWORKING... REFRESH

Standard Switch: vSwitch0 (2)

Standard Switch: vSwitch1 (highlighted with a red box and circled '2')

ADD NETWORKING EDIT MANAGE PHYSICAL ADAPTERS

VM Network 2

- VLAN ID: --
- Virtual Machines (0)

Physical Adapters

- vmnic3 10000 Full

1. Scroll down until you see **Standard Switch: vSwitch1**.
2. If needed, expand the section.

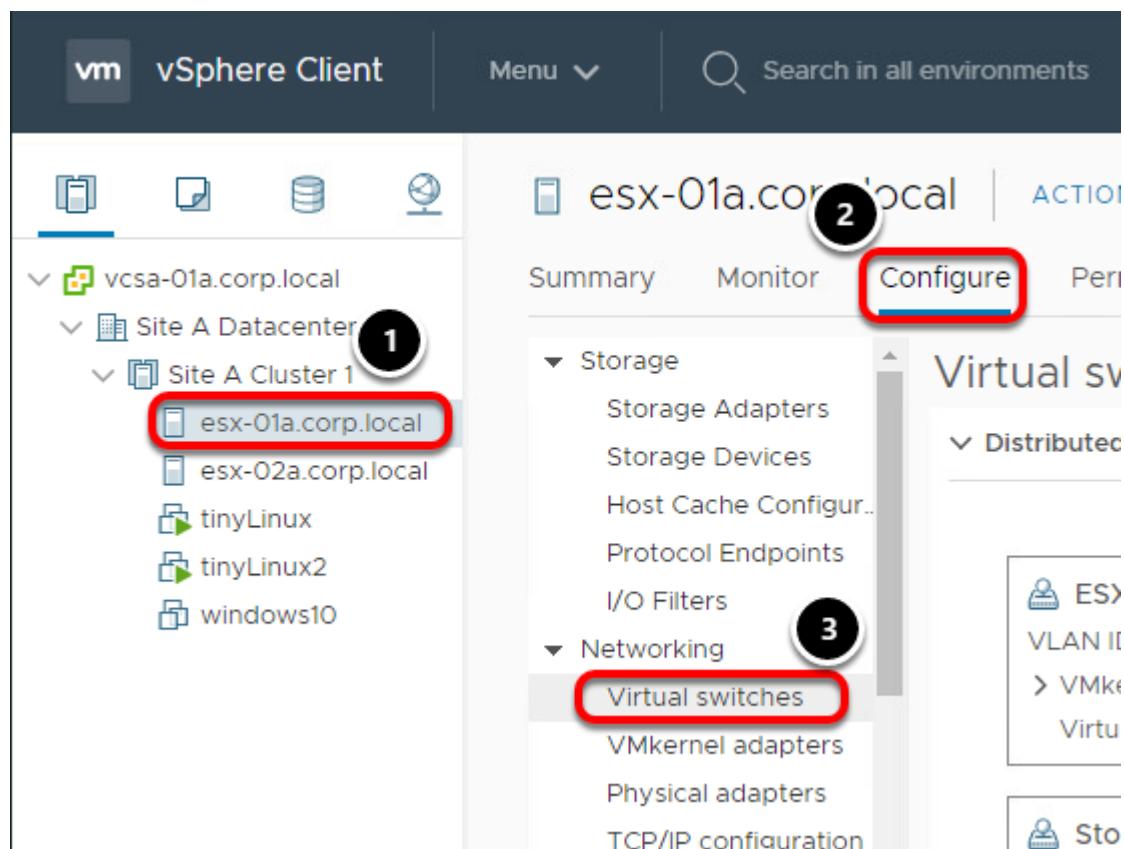
You should see the above diagram showing a virtual port group (VM Network 2) that is on vSwitch1 and it is using vmnic3 as an uplink.

Editing a Standard Switch in the vSphere Web Client

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

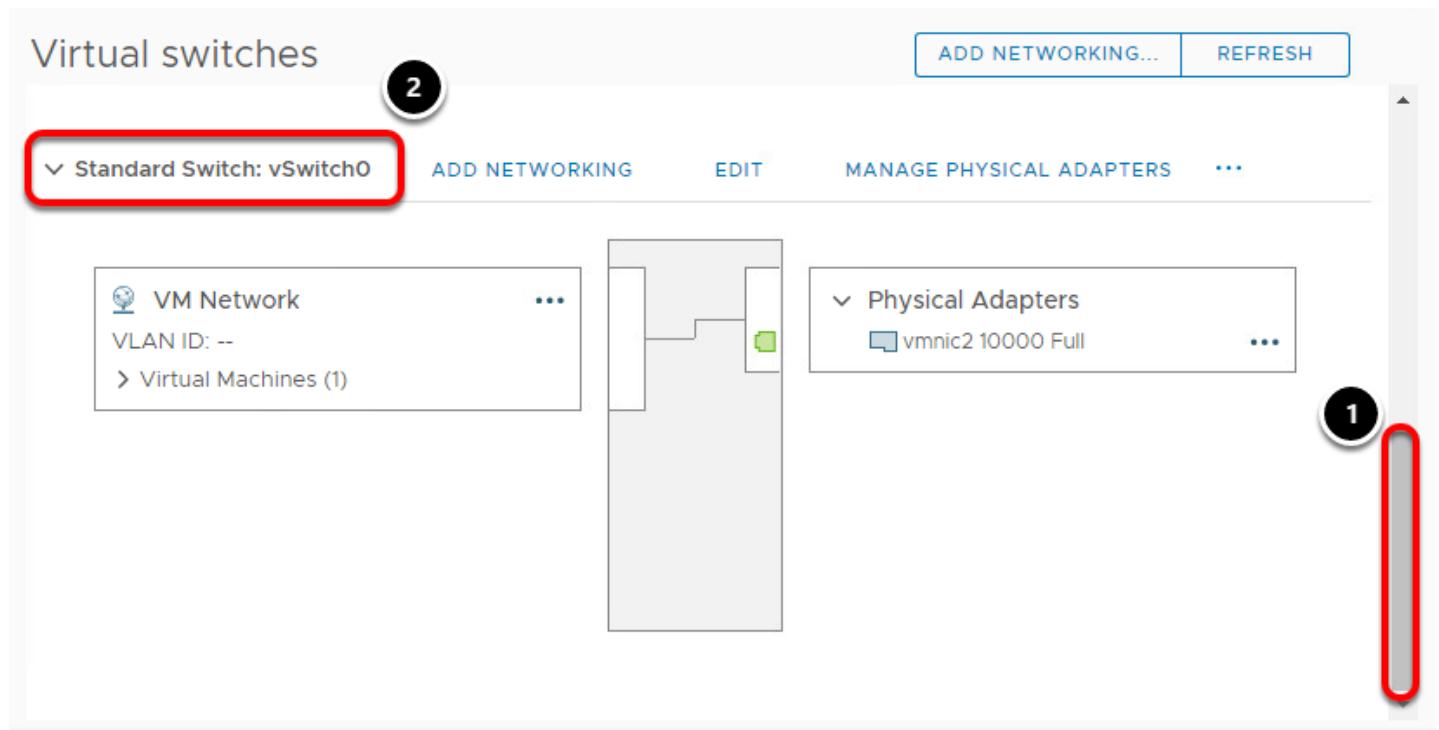
vSphere Standard Switch settings control switch-wide defaults and switch properties such as the uplink configuration.

Select **esxi-01a.corp.local**



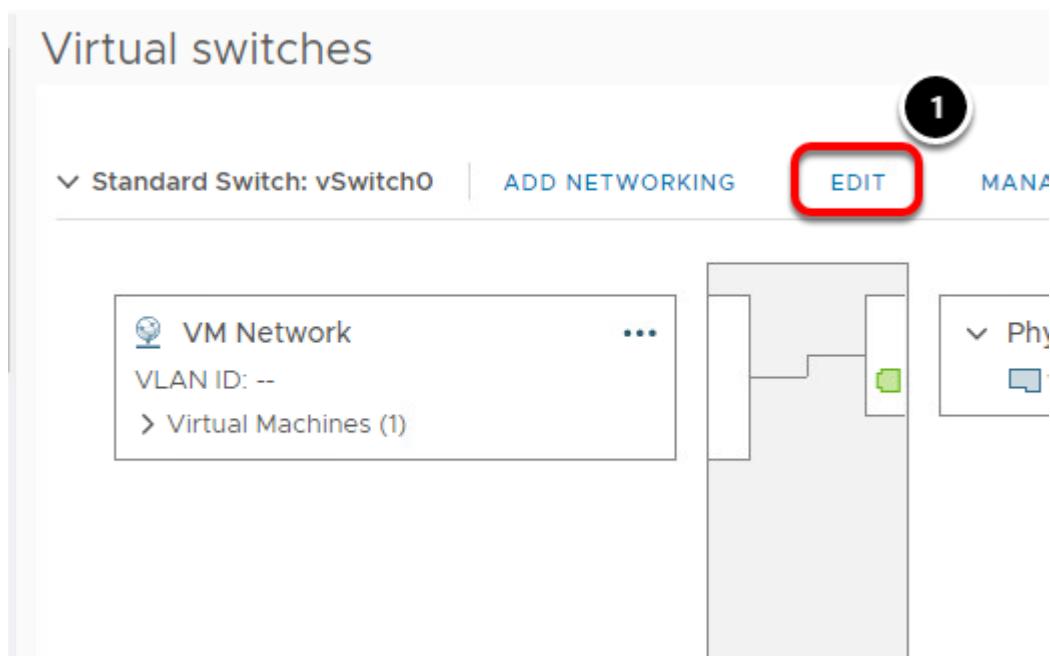
1. Select **esxi-01a.corp.local**.
2. Ensure the **Configure** tab is selected.
3. Click **Virtual switches**.

Select vSwitch0



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



1. Click **Edit**.

Properties (MTU Setting)

vSwitch0 - Edit Settings

Properties		
Security	Number of ports	Elastic
Traffic shaping	MTU (Bytes)	1500
Teaming and failover		



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.

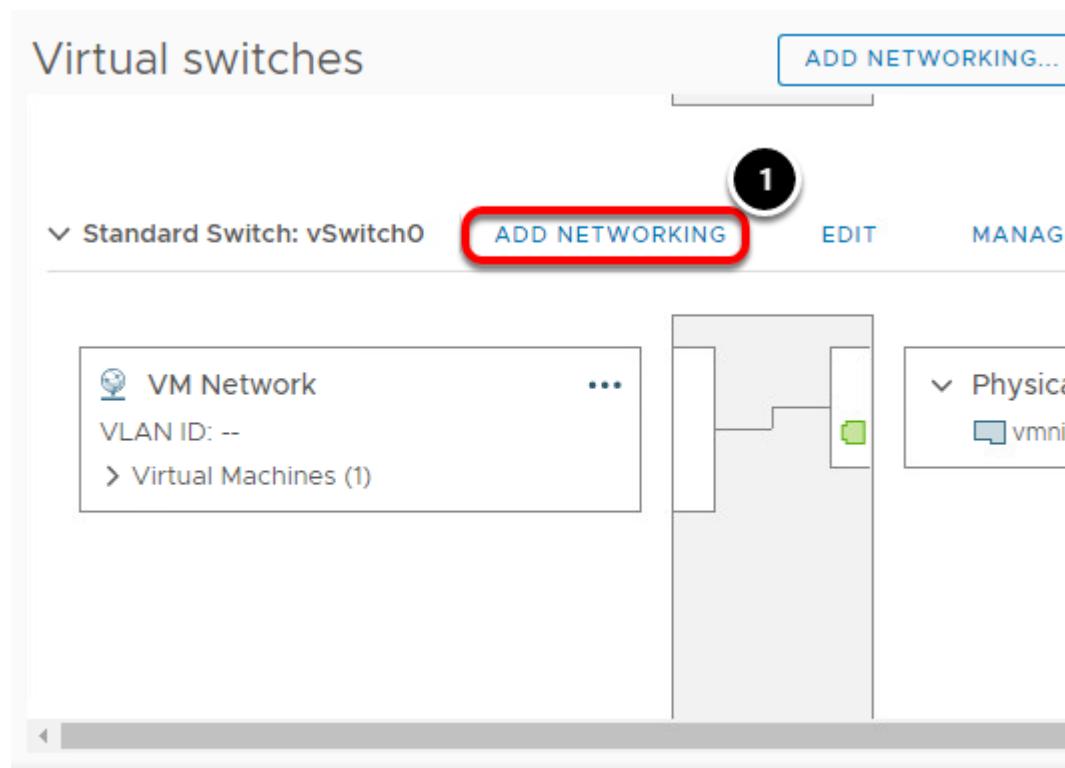
1. Click the **Cancel** button.

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



1. Click **Add Networking**

Select Connection Type

Select connection type

Select a connection type to create.

VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

Virtual Machine Port Group for a Standard Switch

A **1** group handles the virtual machine traffic on standard switch.

Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

CANCEL

BACK

NEXT

1. Select **Physical Network Adapter**.
2. Click **Next**.

Select Target Device

Select target device

Select a target device for the new connection.

Select an existing switch

vSwitch0

[BROWSE ...](#)

New standard switch

MTU (Bytes)

1500

1
[CANCEL](#) [BACK](#) [NEXT](#)

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

1. Click **Next**.

Add Networking

Add physical network adapter

Assign physical network adapters to the switch.

Assigned adapters

Active adapters

vmnic2

Standby adapters

Unused adapters

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

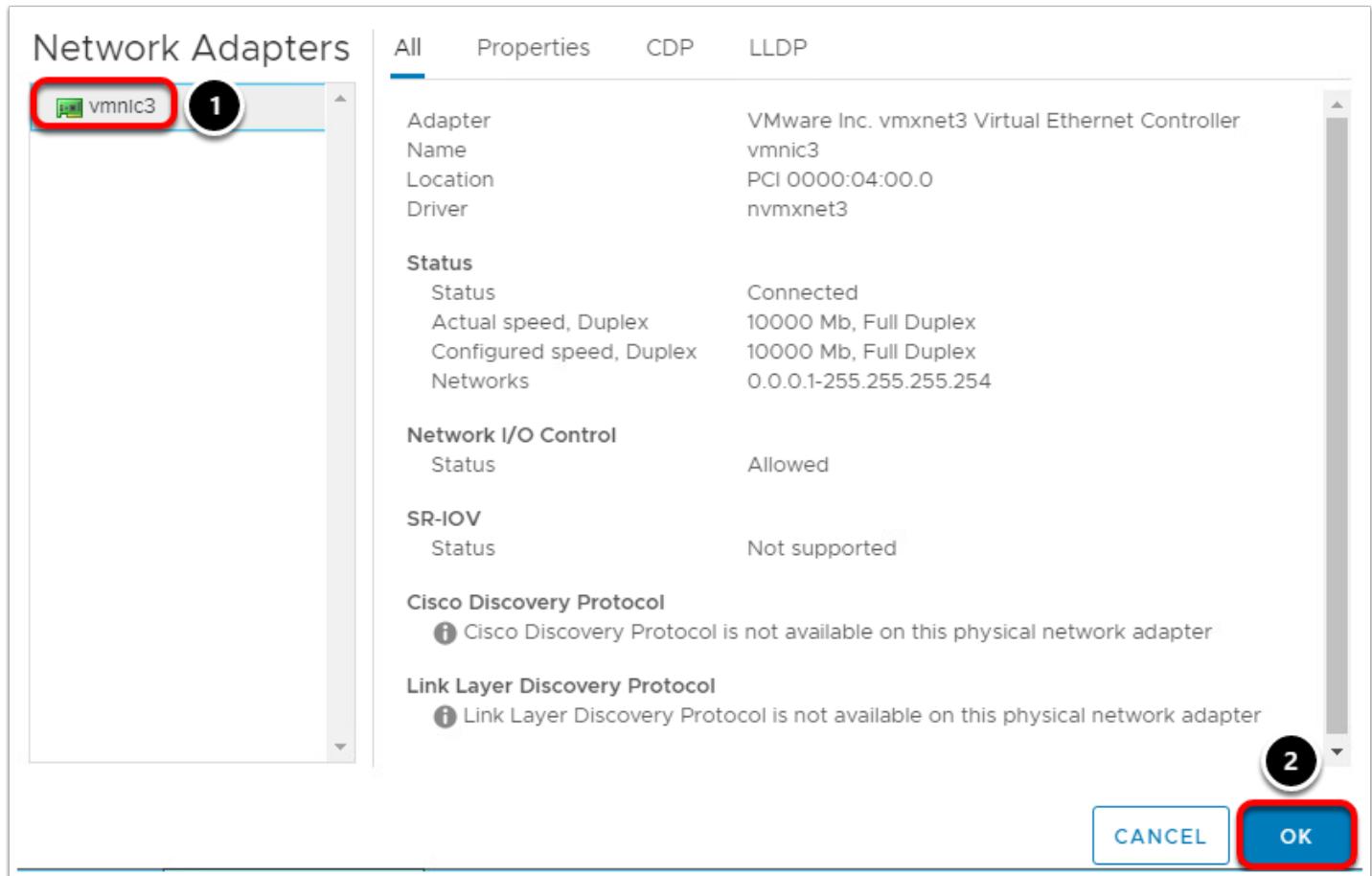
CANCEL

BACK

NEXT

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

Add vmnic3



Network Adapters

All Properties CDP LLDP

Adapter	VMware Inc. vmxnet3 Virtual Ethernet Controller
Name	vmnic3
Location	PCI 0000:04:00.0
Driver	nvmxnet3
Status	
Status	Connected
Actual speed, Duplex	10000 Mb, Full Duplex
Configured speed, Duplex	10000 Mb, Full Duplex
Networks	0.0.0.1-255.255.255.254
Network I/O Control	
Status	Allowed
SR-IOV	
Status	Not supported
Cisco Discovery Protocol	
Cisco Discovery Protocol is not available on this physical network adapter	
Link Layer Discovery Protocol	
Link Layer Discovery Protocol is not available on this physical network adapter	

CANCEL OK

1. Click on **vmnic3**
2. Click **OK**

Assigned Adapters

esx-01a.corp.local - Add Networking

✓ 1 Select connection type Add physical network adapter
 ✓ 2 Select target device Assign physical network adapters to the switch.

3 Add physical network ad...

4 Ready to complete

Assigned adapters

All	Properties	CDP	LLDP
Adapter	VMware In	Controller	
Name	vmnic3	PCI 0000:0	
Location		nvmxnet3	
Driver			
Status			
Status	Connected		
Actual speed, Duplex	10000 Mb,		
Configured speed, Duplex	10000 Mb,		
Networks	0.0.0.1-255		
Network I/O Control			
Status	Allowed		

Active adapters

- vmnic2
- (New) vmnic3

Standby adapters

Unused adapters

1

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

esx-01a.corp.local - Add Networking

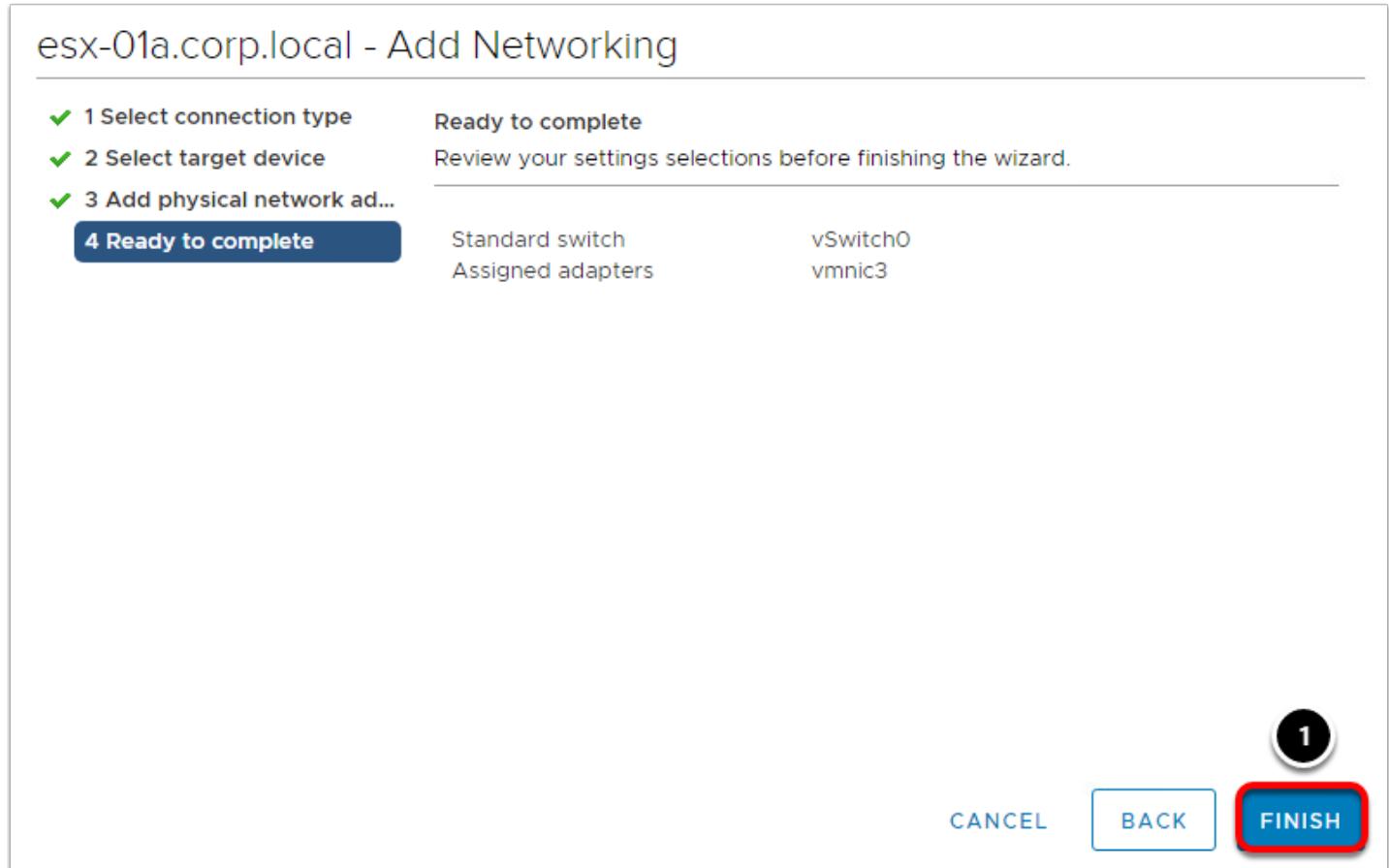
Ready to complete

Review your settings selections before finishing the wizard.

1 Select connection type	Standard switch	vSwitch0
2 Select target device	Assigned adapters	vmnic3
3 Add physical network ad...		
4 Ready to complete		

1

CANCEL BACK FINISH

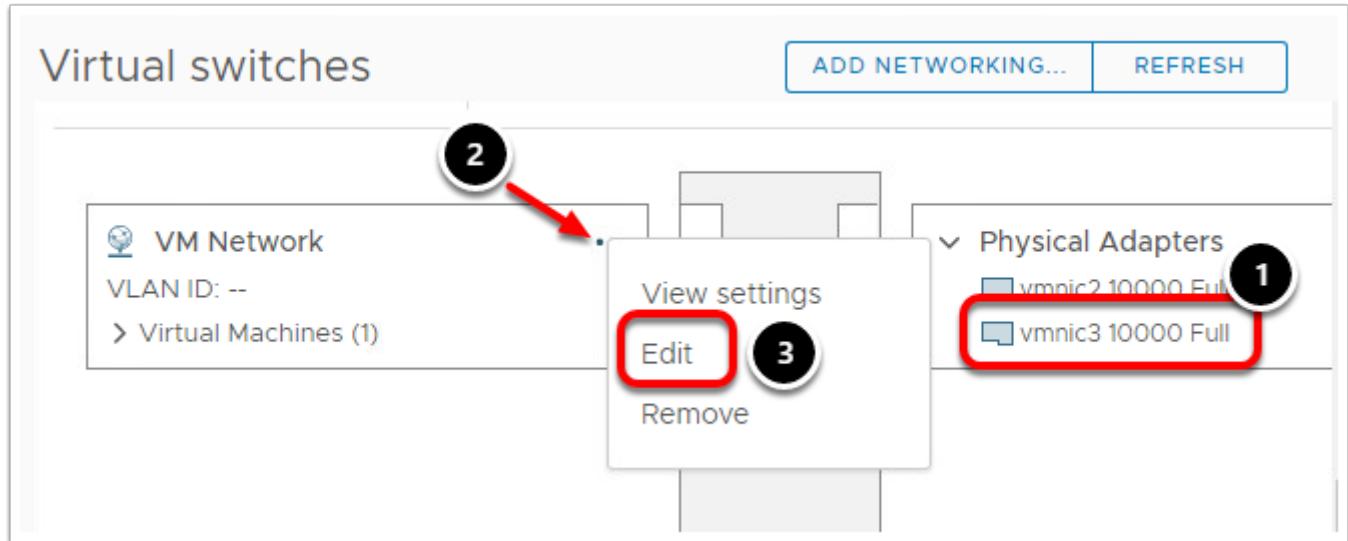


Click **Finish** to add vmnic3 to vSwitch0.

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



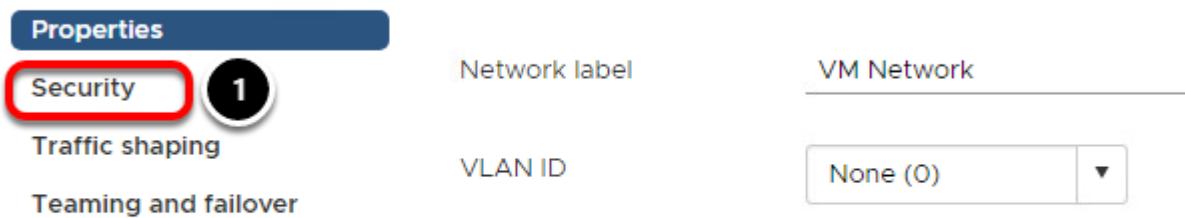
1. In the Physical Adapters section, vmnic3 has been added to the switch.

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**.

Port Group Properties

VM Network - Edit Settings



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

VM Network - Edit Settings

Properties			
Security	Promiscuous mode	<input type="checkbox"/>	Override Reject
Traffic shaping (1)	MAC address changes	<input type="checkbox"/>	Override Accept
Teaming and failover	Forged transmits	<input type="checkbox"/>	Override Accept

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.

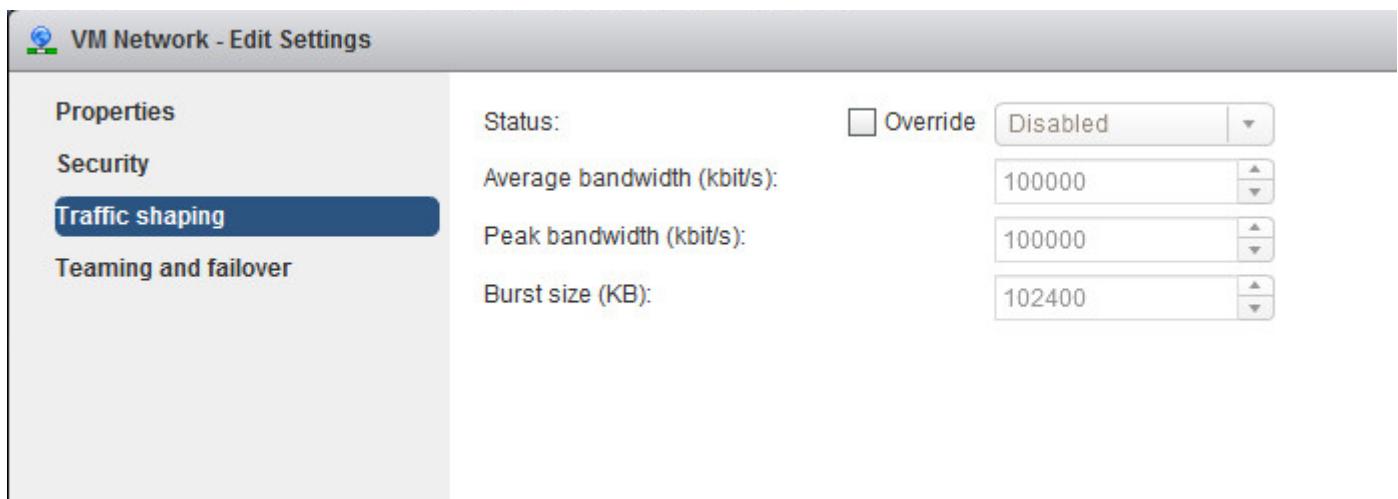
Forged Transmits

- 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



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.

- Clicking **Teaming and failover**.

Teaming and Failover

VM Network - Edit Settings

Properties

Security

Traffic shaping

Teaming and failover

Load balancing

Override Route based on originating virtual port

Network failure detection

Override Link status only

Notify switches

Override Yes

Fallback

Override Yes

Failover order

Override

Active adapters

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

Select active and standby adapters. During a failover, standby adapters activate in the order specified above.

CANCEL OK

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.

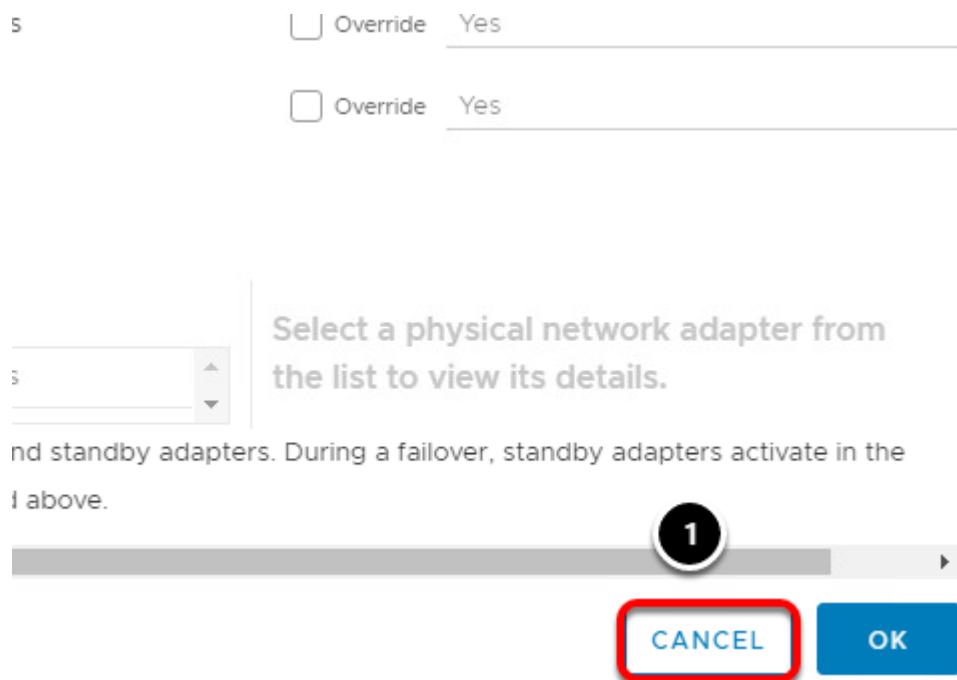
Failover - specifies whether a physical adapter is returned to active status after recovering from a failure.

- 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.

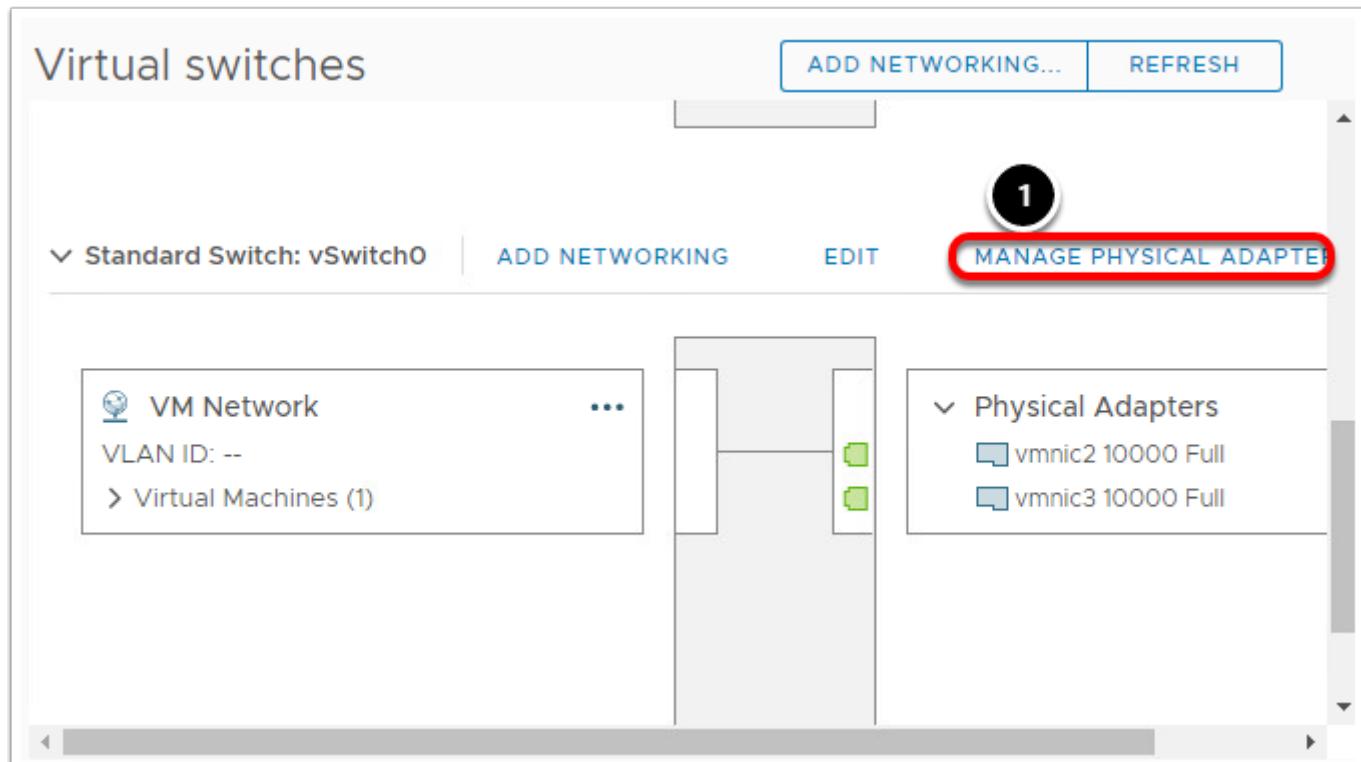
No changes are needed here and you may proceed to the next step.

Cancel the Changes



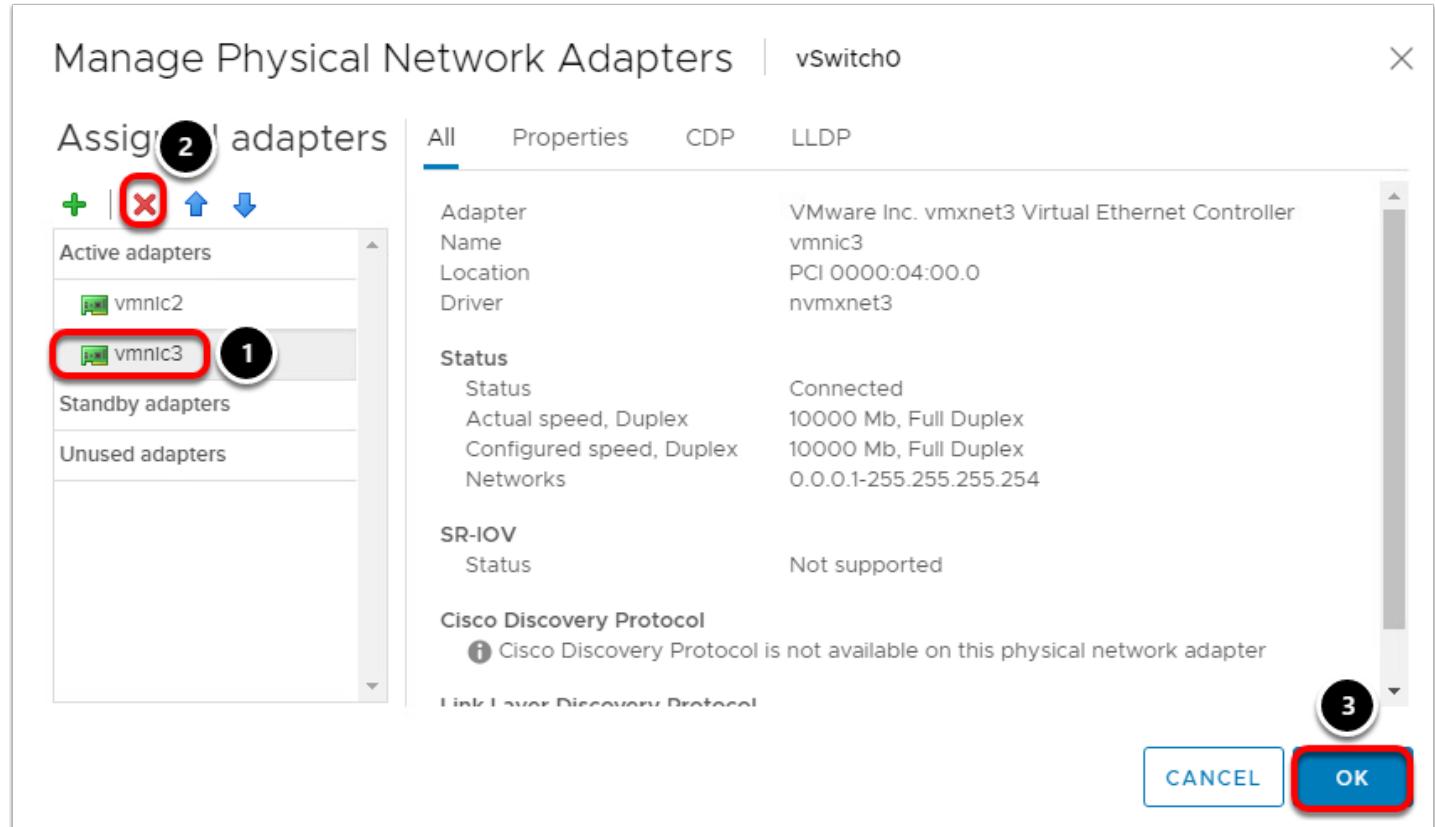
Since we don't want to make any changes to the port group, click the **Cancel** button.

Removing a Physical Adapter



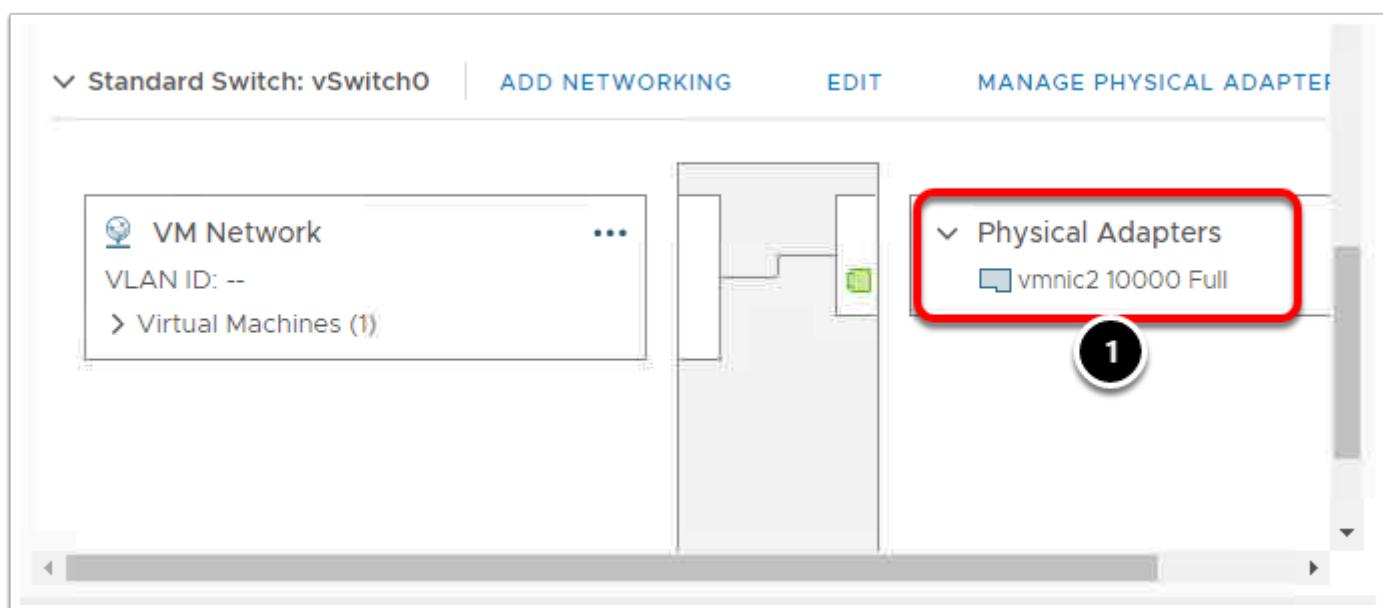
1. Click **Manager Physical Adapters** for vSwitch0.

Remove vmnic3



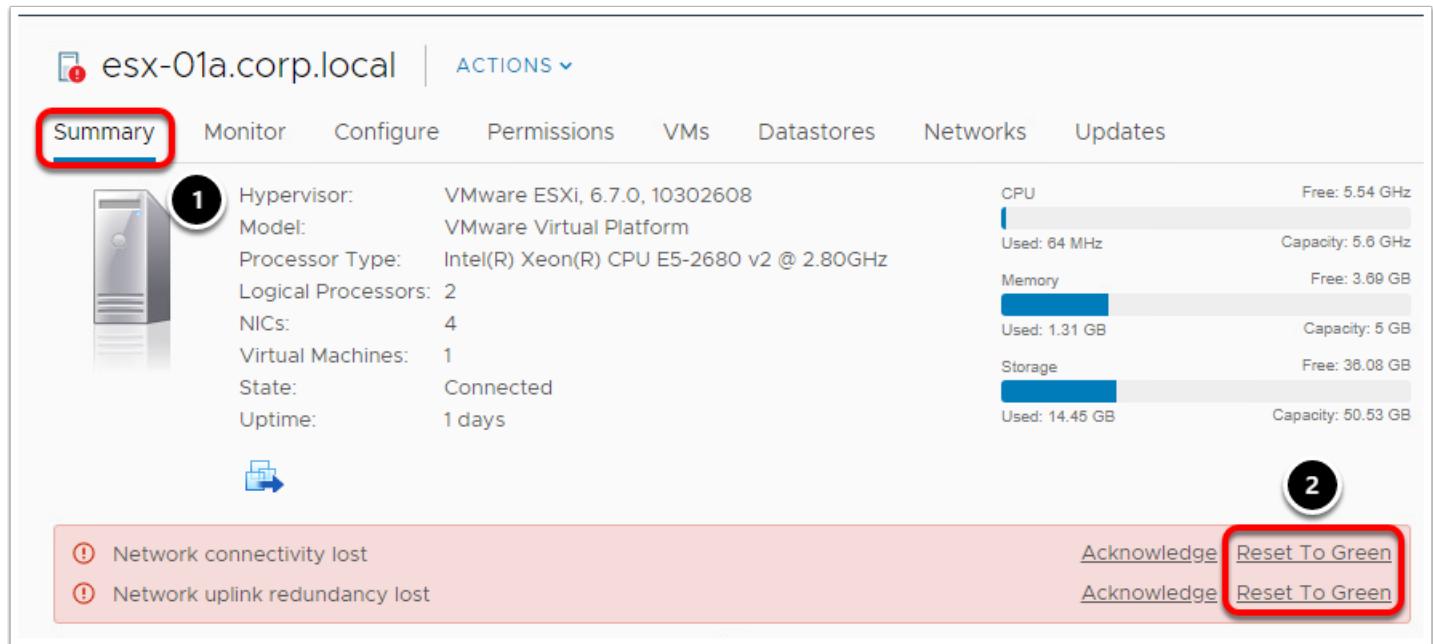
1. Click on **vmnic3**.
2. Click the red 'X' to remove the adapter from the switch.

Adapter Removed



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

Clear Alerts



esx-01a.corp.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

1

Hypervisor: VMware ESXi, 6.7.0, 10302608
 Model: VMware Virtual Platform
 Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
 Logical Processors: 2
 NICs: 4
 Virtual Machines: 1
 State: Connected
 Uptime: 1 days

2

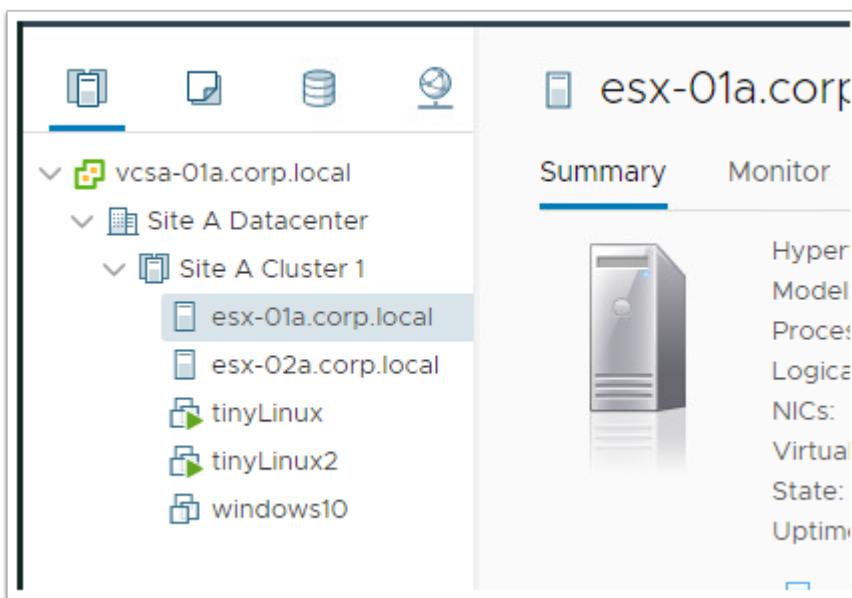
CPU Free: 5.54 GHz
 Used: 64 MHz Capacity: 5.6 GHz
 Memory Free: 3.69 GB
 Used: 1.31 GB Capacity: 5 GB
 Storage Free: 36.08 GB
 Used: 14.45 GB Capacity: 50.53 GB

Network connectivity lost
 Network uplink redundancy lost

[Acknowledge](#) [Reset To Green](#)
[Acknowledge](#) [Reset To Green](#)

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 on **Reset To Green** to clear each alert.



vcsa-01a.corp.local
 Site A Datacenter
 Site A Cluster 1
 esx-01a.corp.local
 esx-02a.corp.local
 tinyLinux
 tinyLinux2
 windows10

esx-01a.corp.local

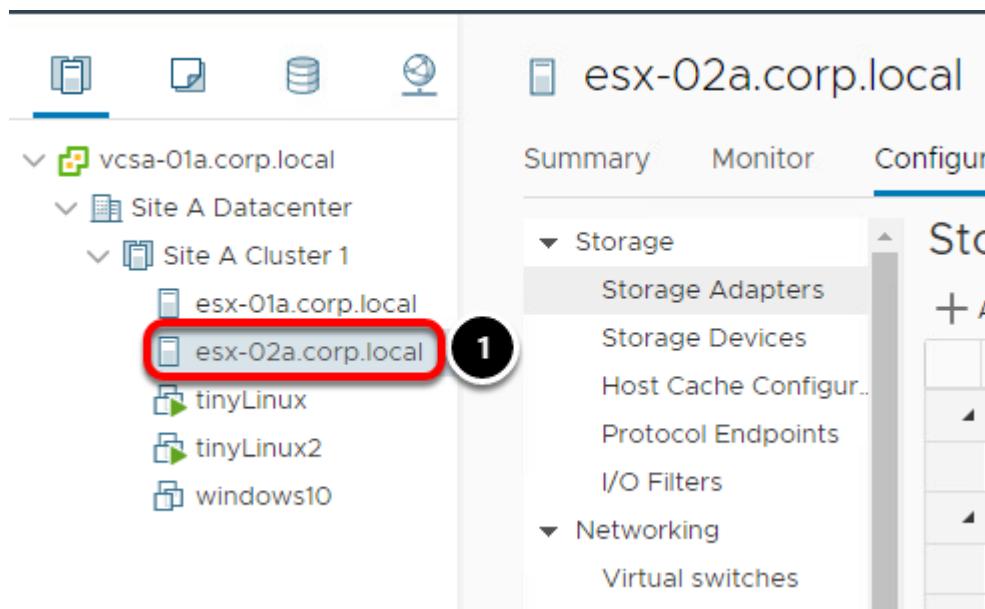
Summary Monitor

Hyper
 Model
 Processor
 Logical
 NICs:
 Virtual
 State:
 Uptime:

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

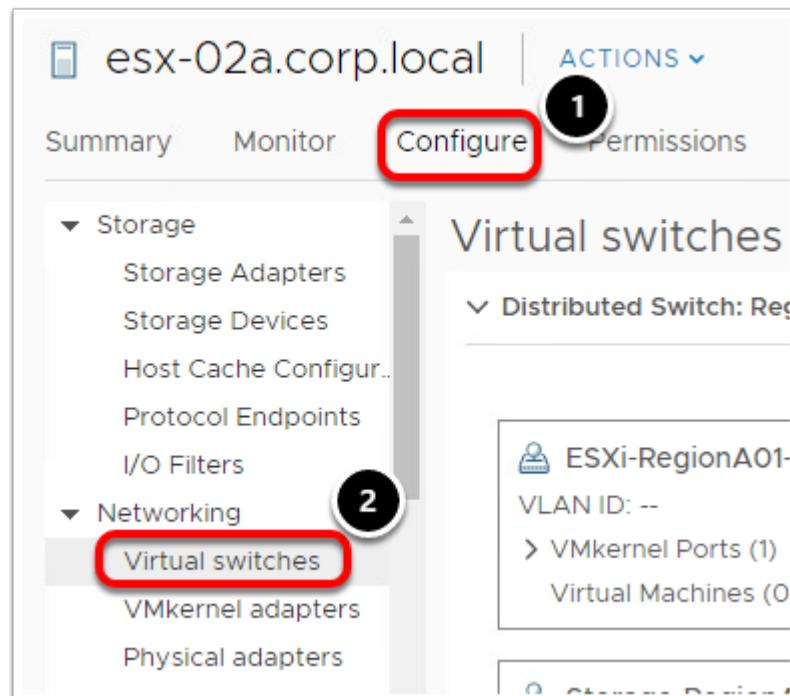
1. Click on **esx-02a.corp.local**.

Deleting a Standard Switch



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

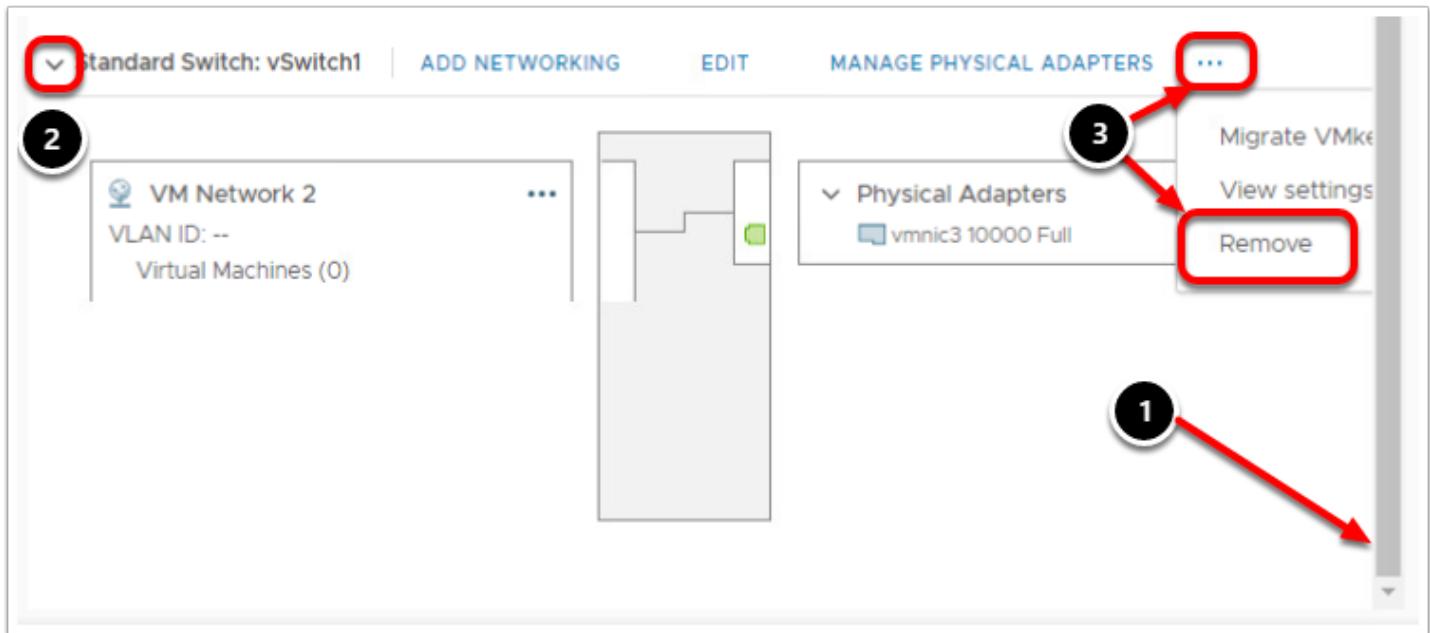
Virtual Switches



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

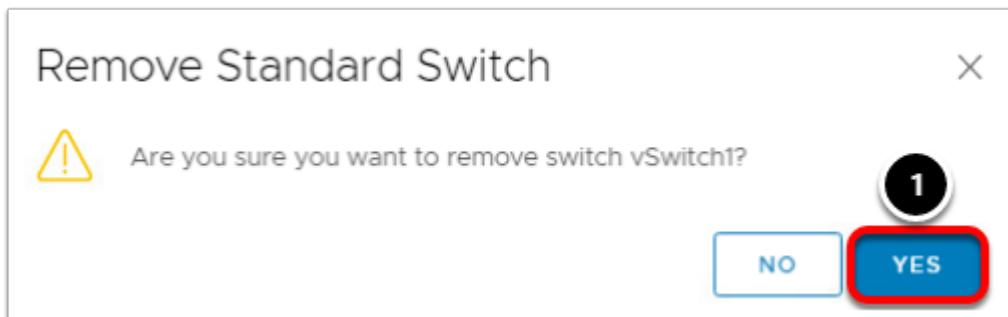
1. Click the **Configure** tab.
2. Select **Virtual switches** in the Networking section.

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

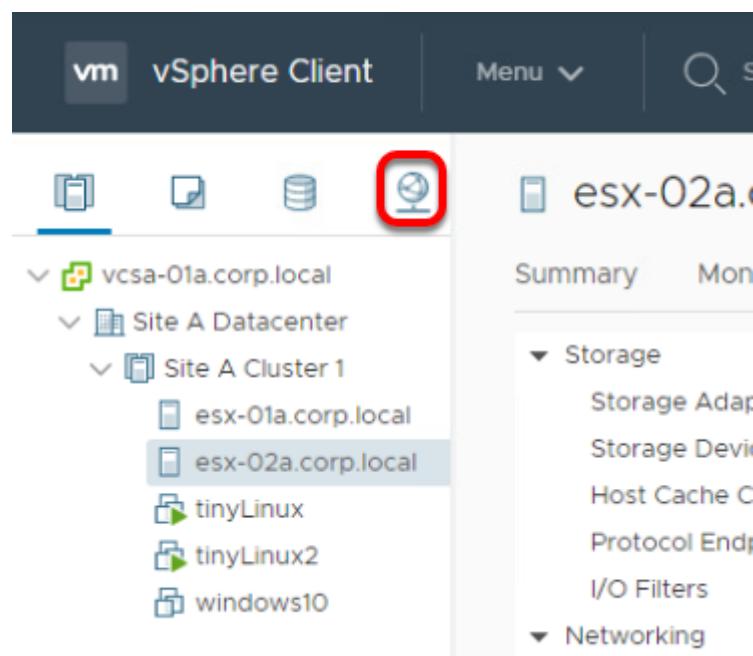
multiple associated hosts. This allows changes to be made once and propagated to every host that is a member of the switch.

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.

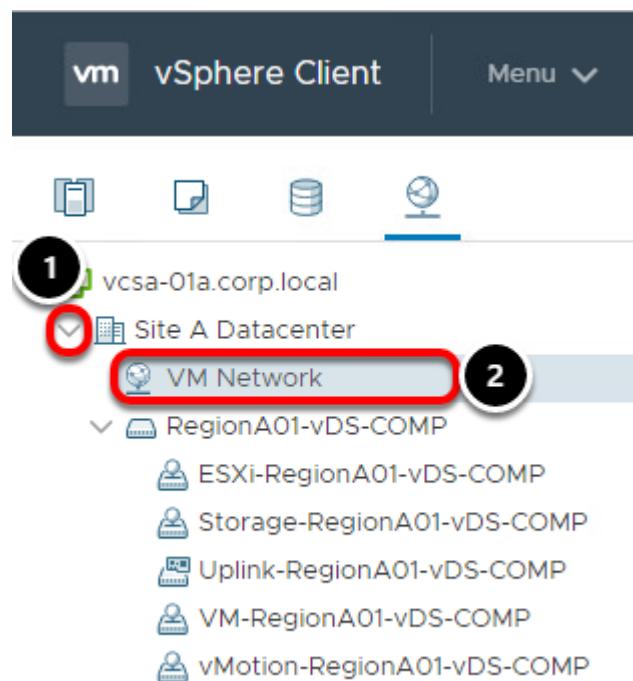
In this lab we will see how a Distributed vSwitch compares to a Standard vSwitch, how it is configured, and how it is connected to a running virtual machine.

Navigate to networking



1. Click on the **Networking** icon.

View Standard vSwitch



1. Expand **Site A Datacenter**.
2. Select **VM Network**.

VM Network

The screenshot shows the 'VM Network' details page with the following interface:

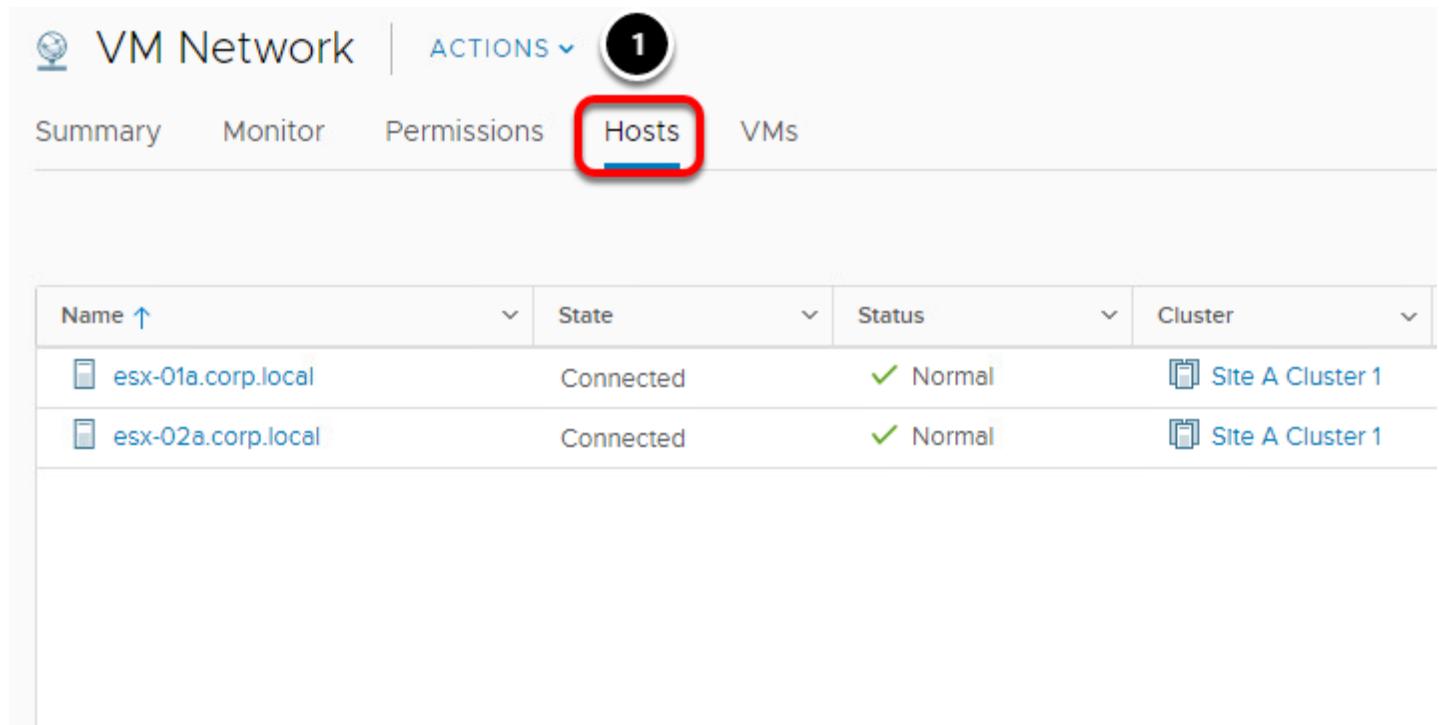
- Top bar: VM Network, ACTIONS
- Top navigation: Summary, Monitor, Permissions, Hosts, VMs (highlighted with a red box, circled with 1)
- Bottom navigation: Virtual Machines (highlighted with a red box)
- Table:
 | Name | State | Status | Provisioned Space |
| --- | --- | --- | --- |
| tinyLinux2 | Powered On | Normal | 466.78 MB |

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

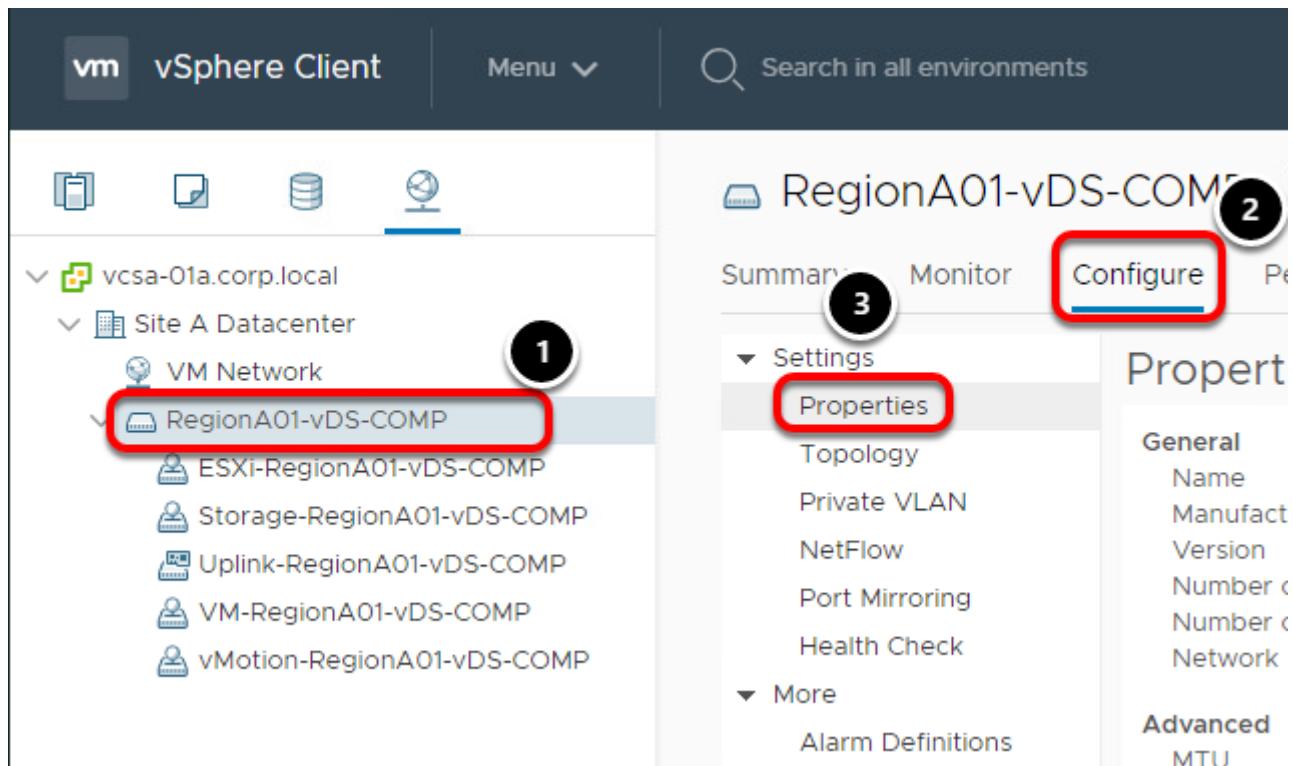


Name	State	Status	Cluster
esx-01a.corp.local	Connected	Normal	Site A Cluster 1
esx-02a.corp.local	Connected	Normal	Site A Cluster 1

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



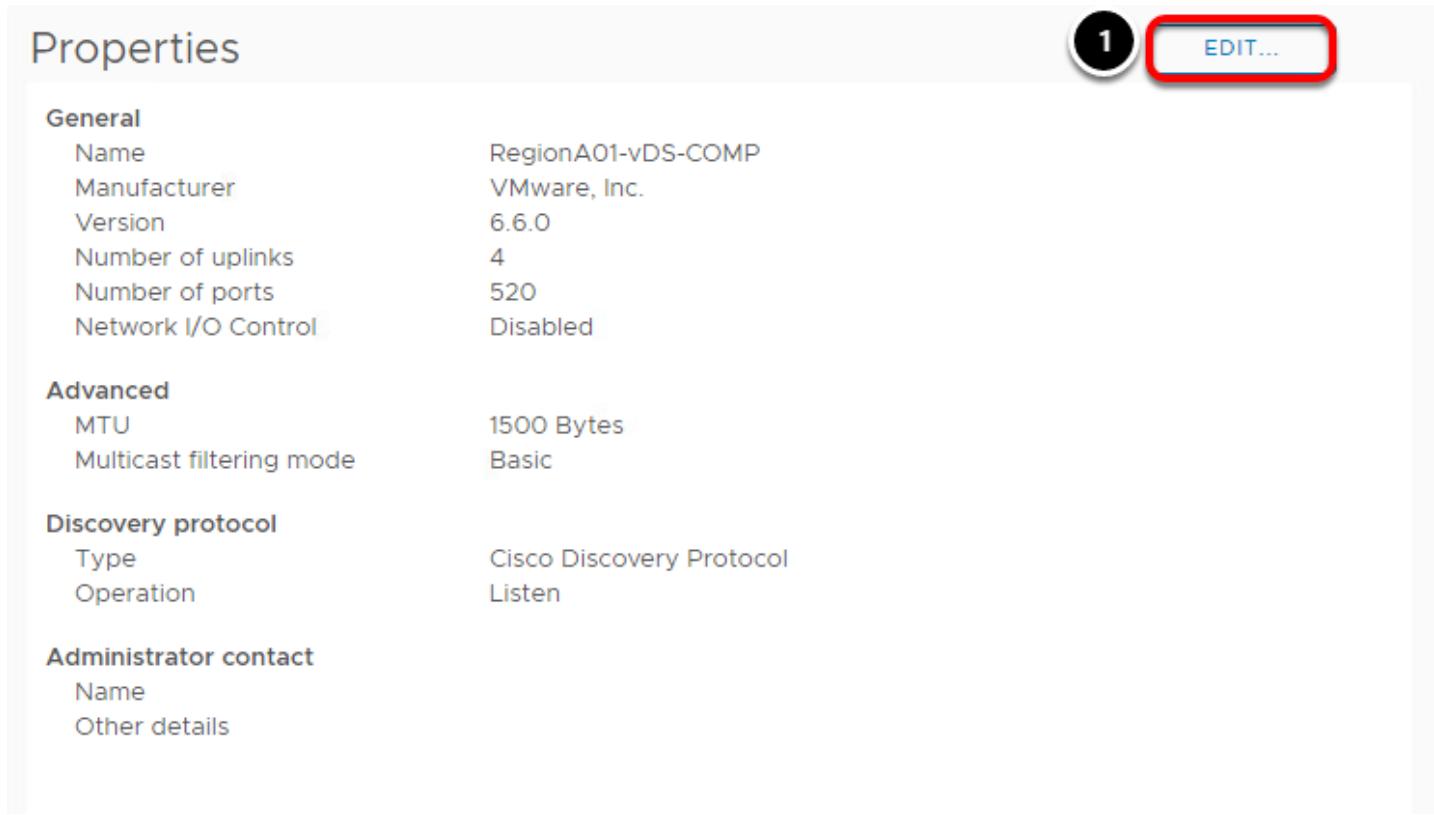
1. Click on **RegionA01-vDS-COMP**.
2. Select the **Configure** tab.
3. Select **Properties**.

Review vDS configuration

General	
Name	RegionA01-vDS-COMP
Manufacturer	VMware, Inc.
Version	6.6.0
Number of uplinks	4
Number of ports	520
Network I/O Control	Disabled
Advanced	
MTU	1500 Bytes
Multicast filtering mode	Basic
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



Properties

1 EDIT...

General	
Name	RegionA01-vDS-COMP
Manufacturer	VMware, Inc.
Version	6.6.0
Number of uplinks	4
Number of ports	520
Network I/O Control	Disabled
Advanced	
MTU	1500 Bytes
Multicast filtering mode	Basic
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

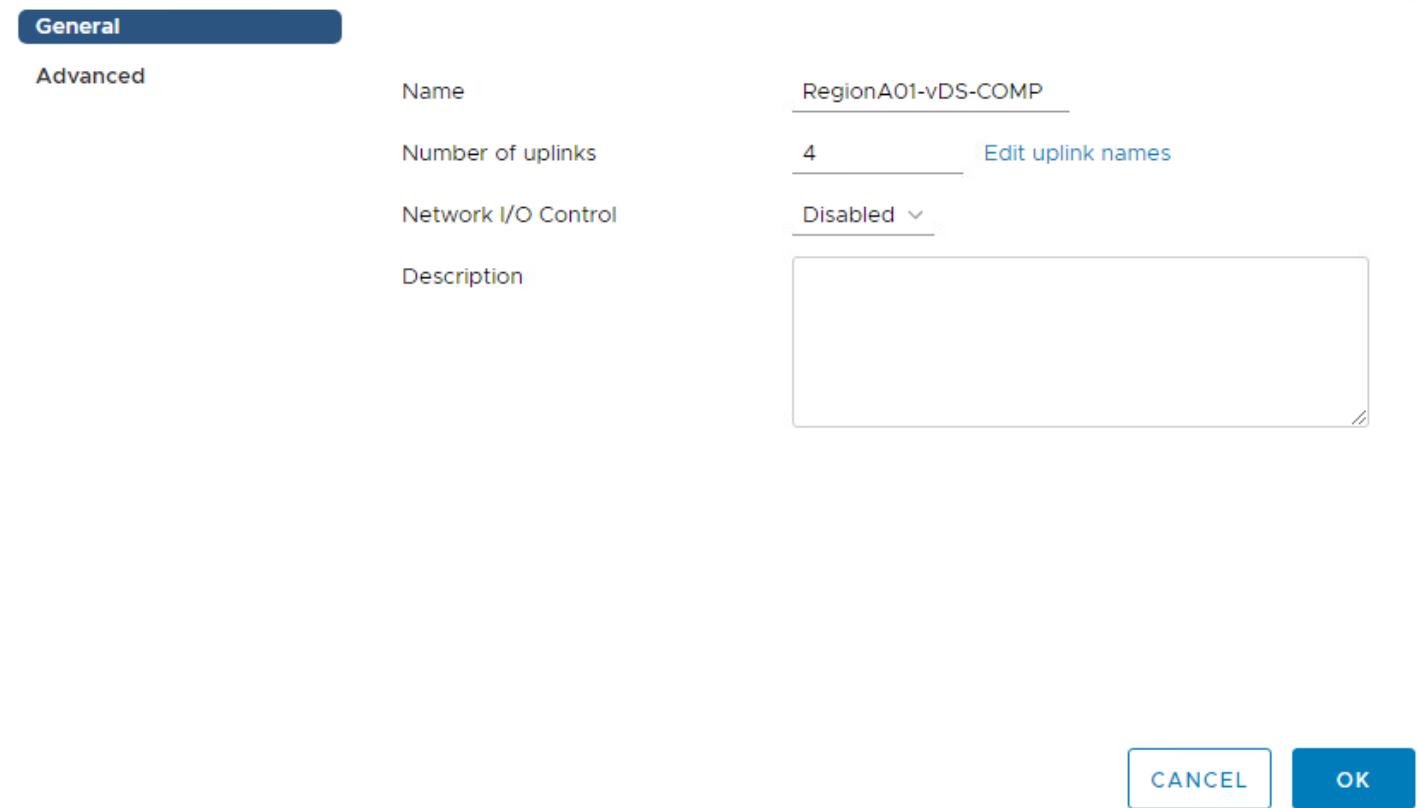
RegionA01-vDS-COMP - Edit Settings

General

Advanced

Name	RegionA01-vDS-COMP
Number of uplinks	4 Edit uplink names
Network I/O Control	Disabled
Description	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>

[CANCEL](#) [OK](#)



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

RegionA01-vDS-COMP - Edit Settings

General

Advanced 1

MTU (Bytes)	1500
Multicast filtering mode	Basic
Discovery protocol	
Type	Cisco Discovery Protocol
Operation	Listen
Administrator contact	
Name	
Other details	

2
CANCEL
OK

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 'Configure' tab selected in the vSphere Web Client. The left sidebar has a 'Health Check' section highlighted with a red box and number 1. The right panel shows the 'Health Check' configuration with two items: 'VLAN and MTU' and 'Teaming and failover', both set to 'Disabled'. The 'Edit...' button in the top right corner is highlighted with a red box and number 2.

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

Edit Health Check Settings | RegionA01-vDS-COMP X

VLAN and MTU

State: Enabled

Interval: 1 minutes

Teaming and failover

State: Enabled

Interval: 1 minutes



1

2

CANCEL

OK

Select **Enabled** for both and click **OK**.

Distributed Port Groups

RegionA01-vDS-COMP | ACTIONS ▾

Summary Monitor Configure Permissions Ports Host

Settings Properties

Health Check

VLAN and MTU	Enabled
Teaming and failover	Enabled

Actions - RegionA01-vDS-COMP

- Distributed Port Group
- Add and Manage Hosts...
- Edit Notes...
- Upgrade
- Settings

1

2

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

New Distributed Port Group

1 Select name and location

2 Configure settings

3 Ready to complete

Select name and location

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

Name: **WebVMTraffic** (1)

Location: RegionA01-vDS-COMP

2

CANCEL BACK NEXT

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 (i)
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	None
Advanced	
<input type="checkbox"/> 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

New Distributed Port Group

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

Ready to complete

Review the changes before proceeding.

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

CANCEL

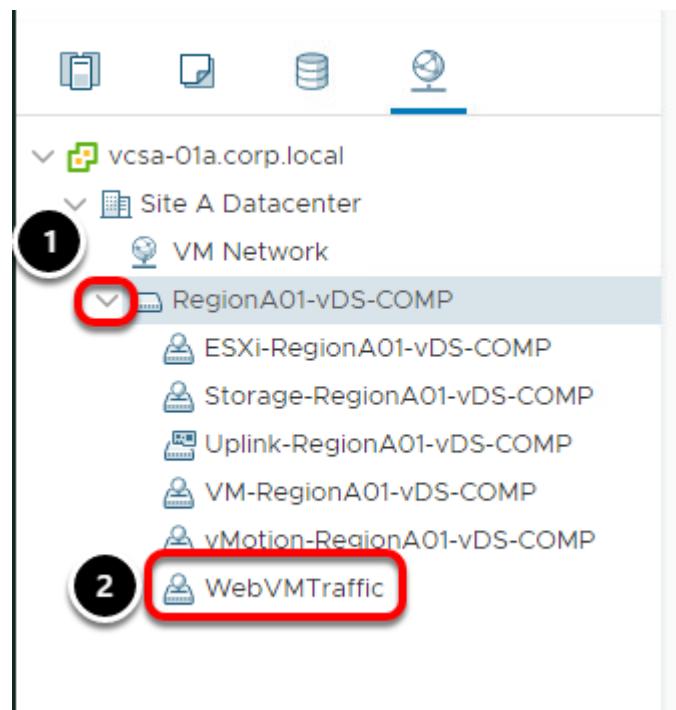
BACK

FINISH

1

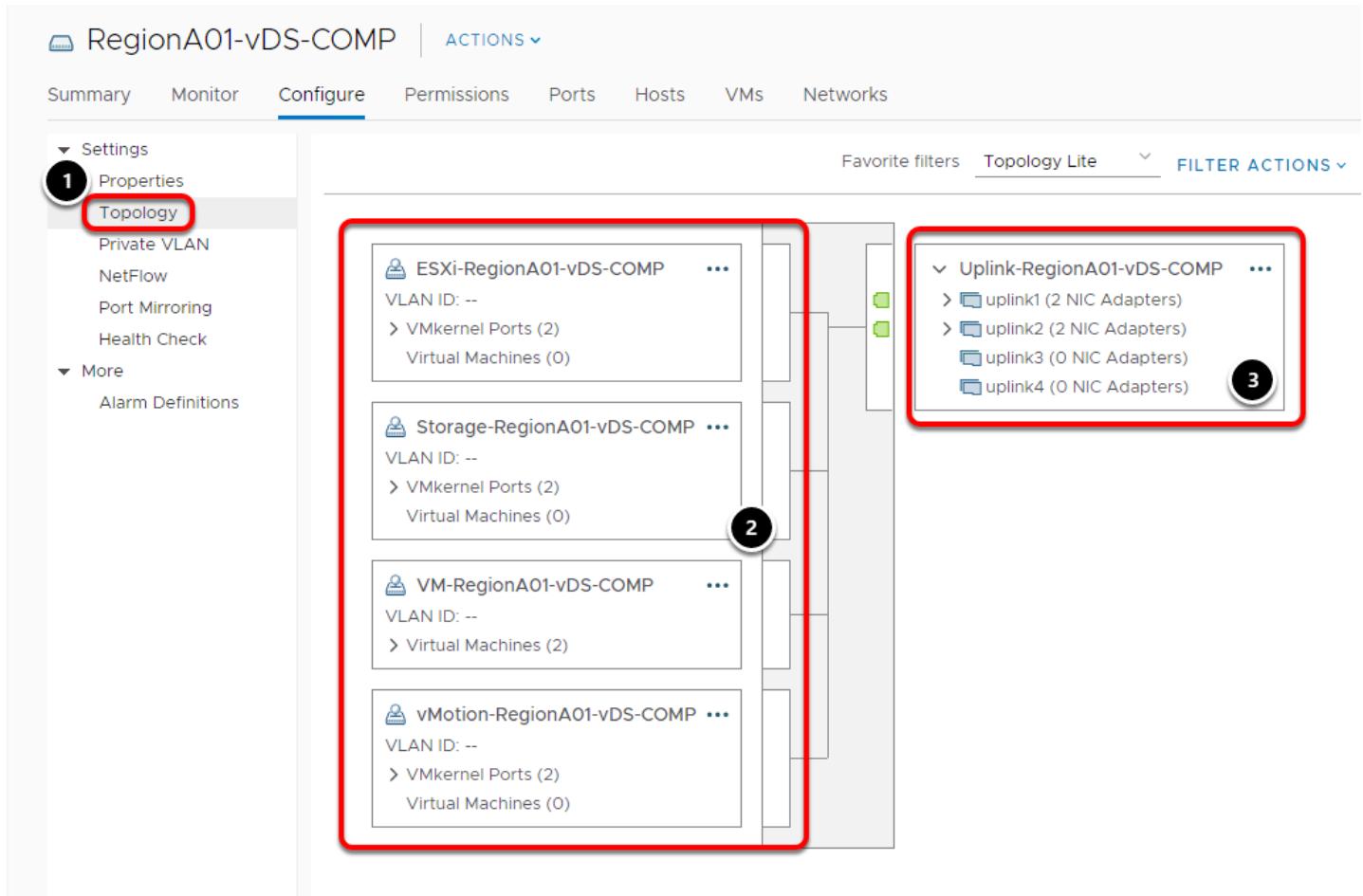
1. Review your settings and click **Finish** to create the Distributed Port Group.

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 **Topology**.
2. 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.
3. 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

Summary Monitor **Configure** Permissions Ports Hosts VM

▼ Settings

- Properties
- Topology**
- Private VLAN
- NetFlow
- Port Mirroring
- Health Check

▼ More

- Alarm Definitions

ESXi-RegionA01-vDS-COMP ...
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (0)

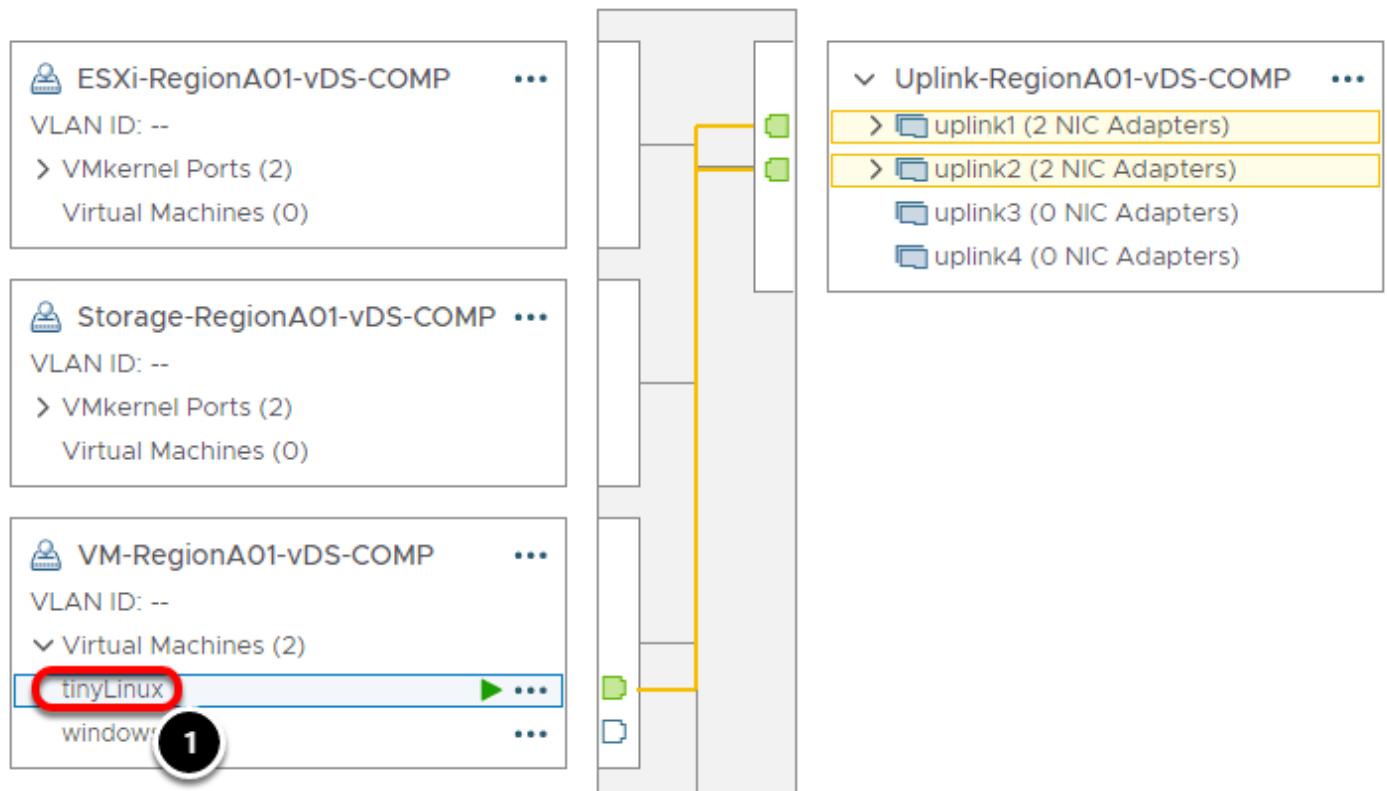
Storage-RegionA01-vDS-COMP ...
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (0)

1 VM-RegionA01-vDS-COMP ...
VLAN ID: --
Virtual Machines (2)
tinyLinux
windows10

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



1. Click on **tinyLinux**

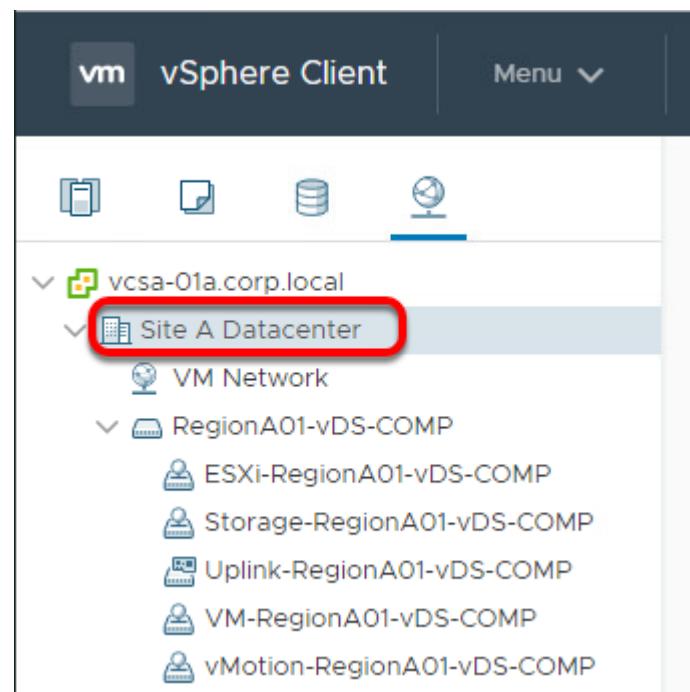
Note that a path to an uplink is drawn out and highlighted in orange to show the uplinks, hosts and vmnics it is associated with.

Creating a new Distributed Switch

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

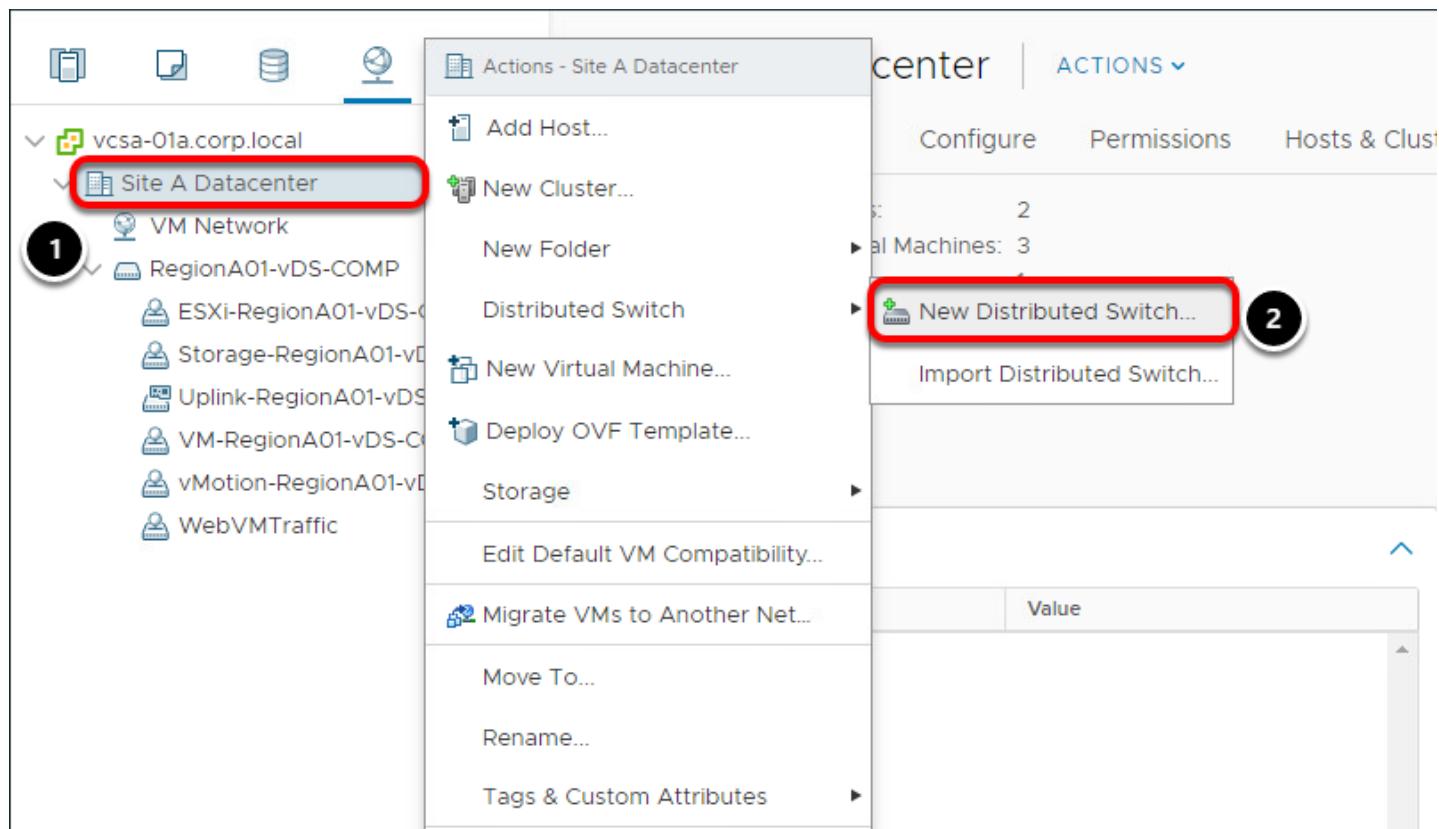
In this lab we will create a new Distributed vSwitch, add ESXi hosts to it, build port groups and connect them to uplinks so that we can use it to forward virtual machine traffic on to the physical network.

Navigate to Site A Datacenter



1. In the vSphere Web Client, click on **Site A Datacenter**.

Create a new Distributed Switch



1. In the navigator, right-click the **Site A Datacenter**.
2. Select **Distributed Switch > New Distributed Switch**.

This will open the New Distributed Switch wizard.

Name the Distributed Switch

New Distributed Switch

1 Name and location

2 Select version

3 Configure settings

4 Ready to complete

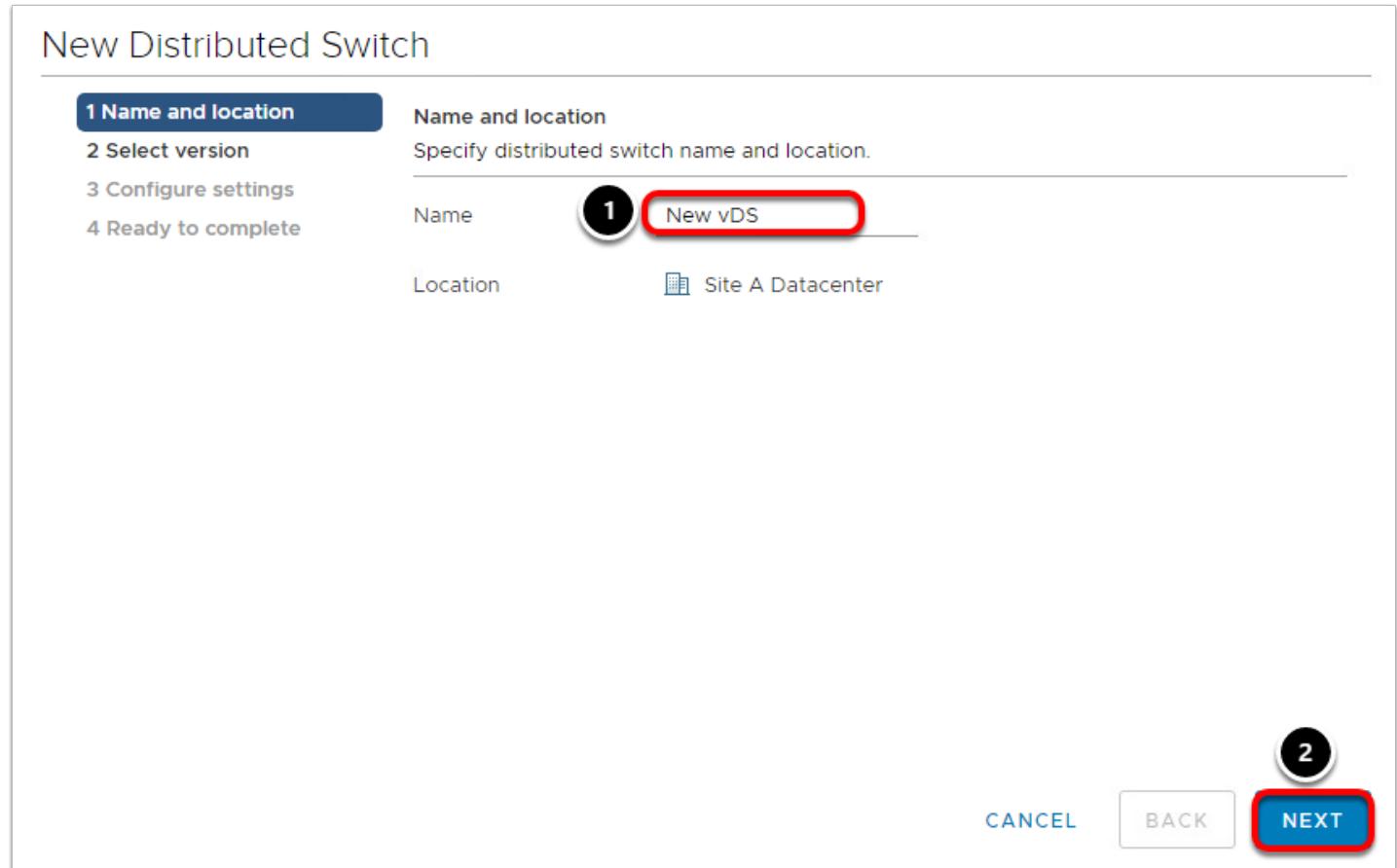
Name and location
Specify distributed switch name and location.

Name **1 New vDS**

Location  Site A Datacenter

2

CANCEL BACK **NEXT**



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

Select the version

New Distributed Switch

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

Select version
Specify a distributed switch version.

6.6.0 - ESXi 6.7 and later 1

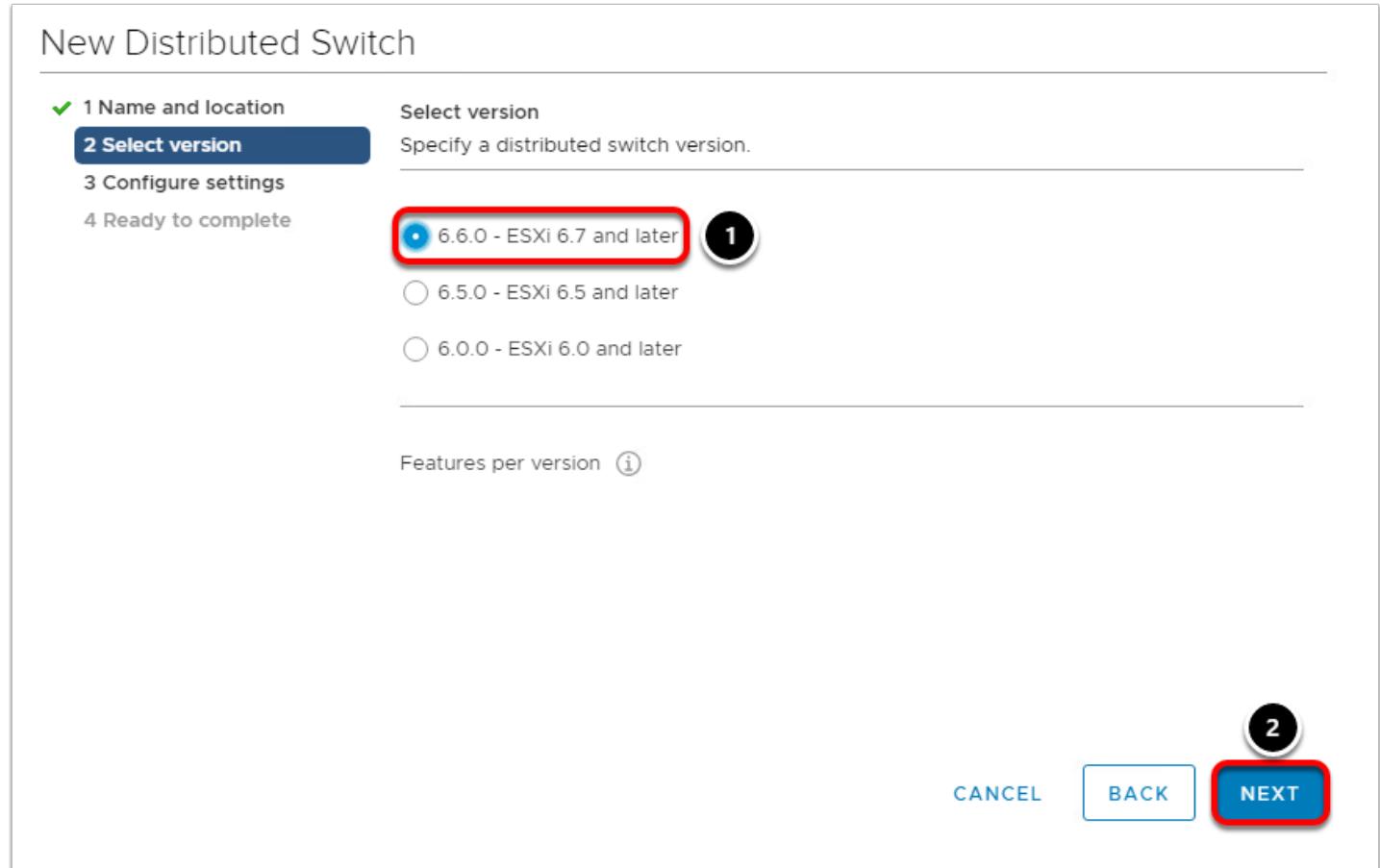
6.5.0 - ESXi 6.5 and later

6.0.0 - ESXi 6.0 and later

Features per version 1

2

CANCEL BACK NEXT



1. Leave the default setting of **6.6.0 - ESXi 6.7 and later**
2. Click **Next**.

Configure settings

New Distributed Switch

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

Configure settings
Specify number of uplink ports, resource allocation and default port group.

Number of uplinks	4
Network I/O Control	Enabled
Default port group	<input checked="" type="checkbox"/> Create a default port group
Port group name	DPortGroup

1

CANCEL BACK **NEXT**

1. On the Configure Settings page, leave the default options and click **Next**.

Complete the build

New Distributed Switch

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

Name	New vDS
Version	6.6.0
Number of uplinks	4
Network I/O Control	Enabled
Default port group	DPortGroup

Suggested next actions

-  [New Distributed Port Group](#)
-  [Add and Manage Hosts](#)

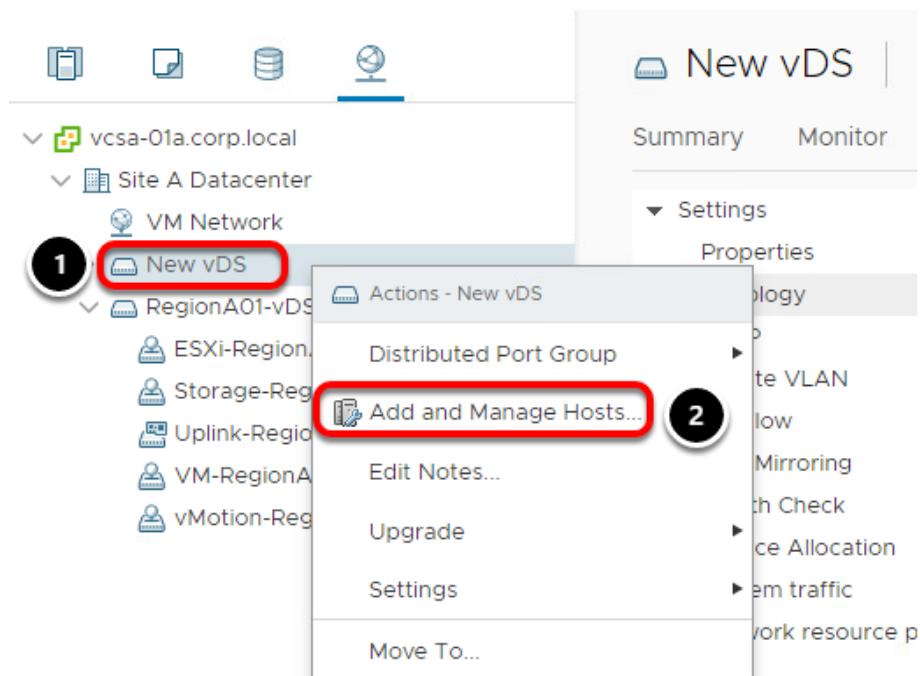
1 These actions will be available in the Actions menu of the new distributed switch.

1

[CANCEL](#) [BACK](#) [FINISH](#)

1. Review your settings on the Ready to Complete page and click **Finish** if everything looks good.

Add hosts to new Distributed Switch



1. Right click on the newly created switch, **New-vDS**.
2. Select **Add and Manage Hosts...**

Select task

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

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

Add hosts
Add new hosts to this distributed switch. **1**

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

Remove hosts
Remove hosts from this distributed switch.

2

CANCEL BACK **NEXT**

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

Select hosts

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

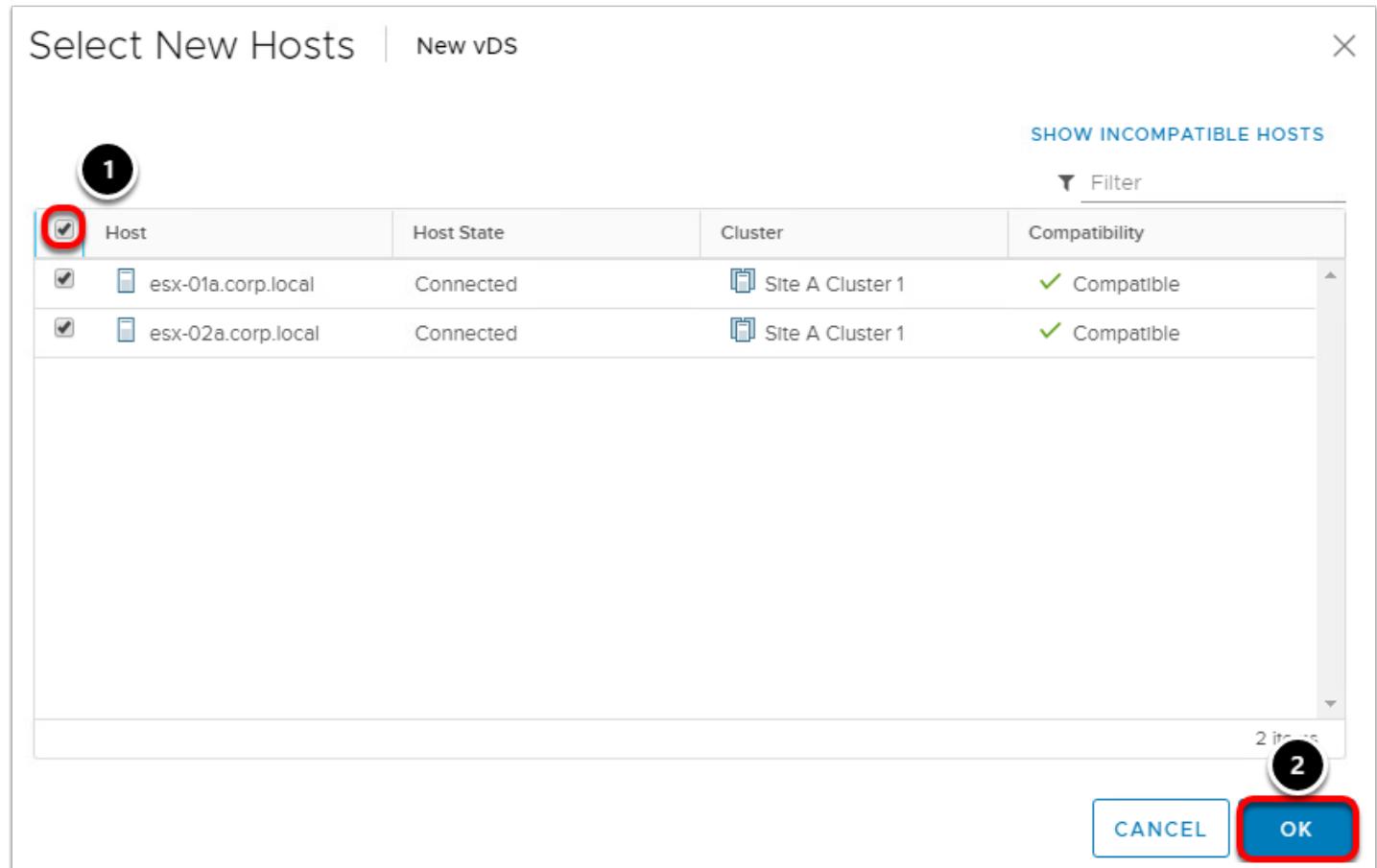
Select hosts
Select hosts to add to this distributed switch. **1**

+ New hosts... **X Remove**

Host

1. On the Select hosts page, click **New hosts**.

Select New Hosts



The screenshot shows the 'Select New Hosts' dialog box. At the top, there are tabs for 'Select New Hosts' and 'New vDS'. On the right, there are buttons for 'SHOW INCOMPATIBLE HOSTS' and 'Filter'. The main area is a table with the following columns: Host, Host State, Cluster, and Compatibility. Two hosts are listed: 'esx-01a.corp.local' and 'esx-02a.corp.local', both marked as 'Connected' and part of 'Site A Cluster 1'. Both hosts are marked as 'Compatible'. The 'Host' column header has a circled '1' above it, and the 'OK' button at the bottom right has a circled '2' above it. The 'OK' button is highlighted with a red box.

Host	Host State	Cluster	Compatibility
esx-01a.corp.local	Connected	Site A Cluster 1	Compatible
esx-02a.corp.local	Connected	Site A Cluster 1	Compatible

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

Manage Hosts

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

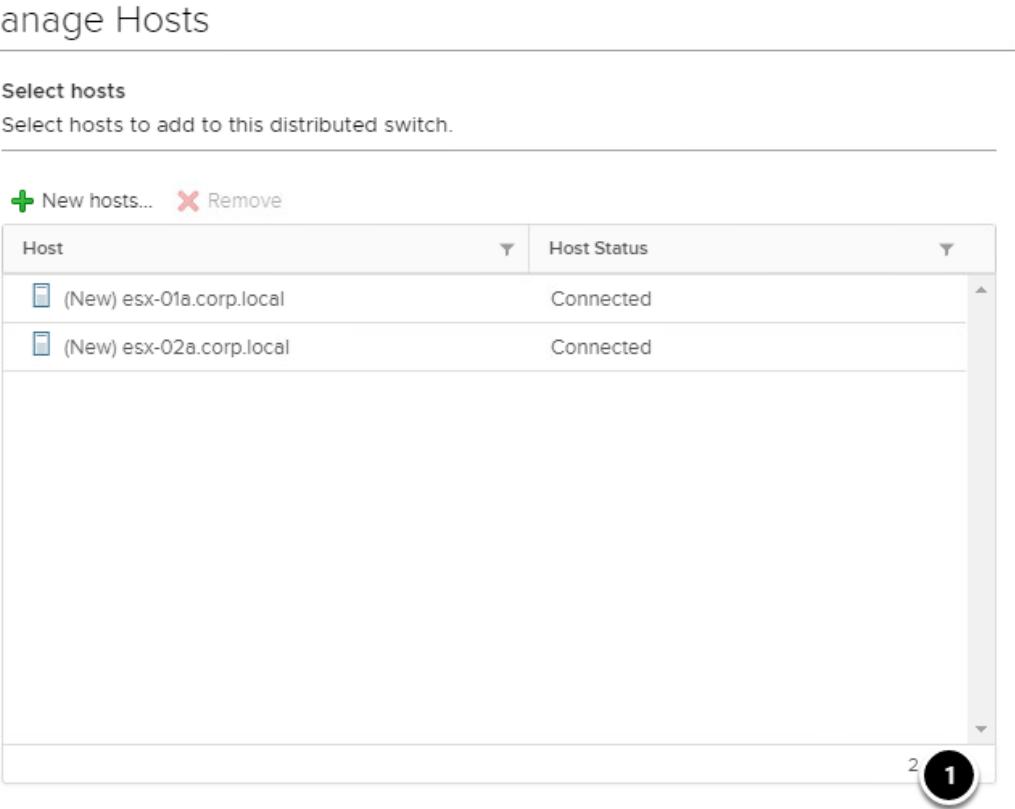
Select hosts
Select hosts to add to this distributed switch.

New hosts... **Remove**

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

2 **1**

CANCEL **BACK** **NEXT**



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.

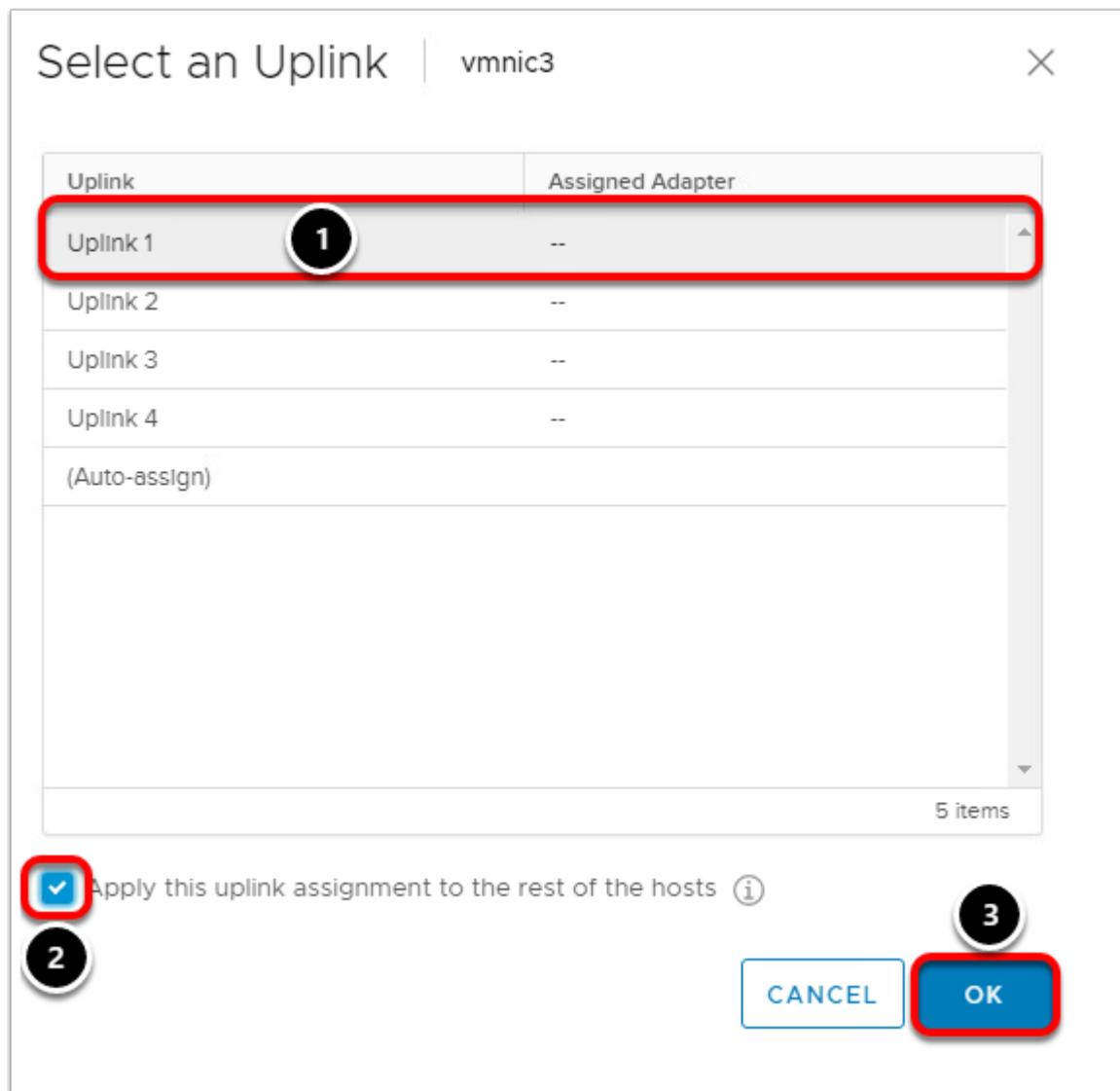
Host/Physical Network Adapters	In Use by Switch	Uplink
▲ esx-01a.corp.local		
On this switch		
▲ On other switches/unclaimed		
vmnic0	RegionA01-vDS-CO...	--
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--
vmnic3	--	--
▼ esx-02a.corp.local		

Assign uplink **Assign adapter** **View settings**

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.

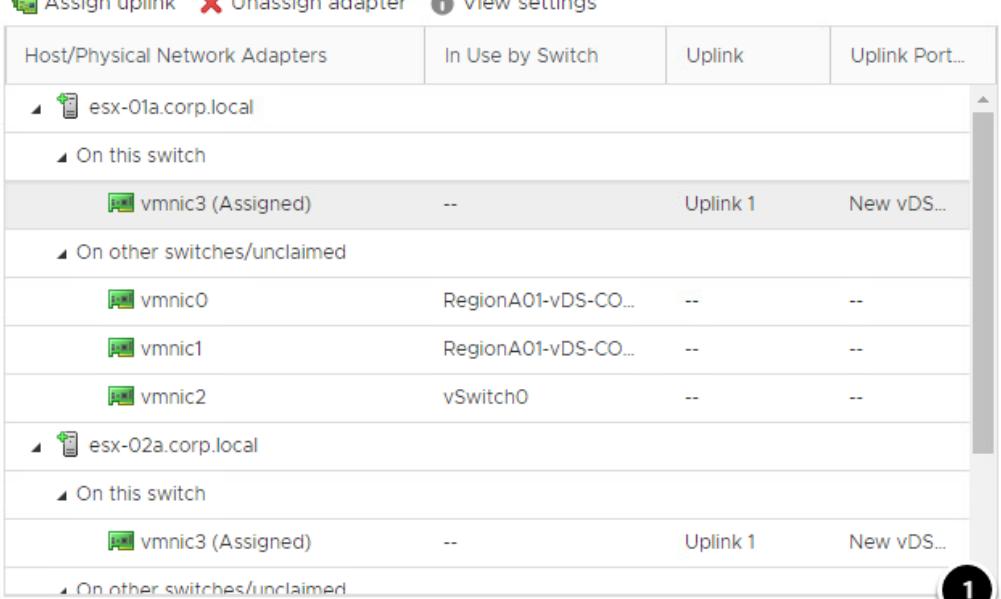
3. Click **OK**.

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.



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

NEXT

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

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, just click **Next** here.

Migrate VM networking

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

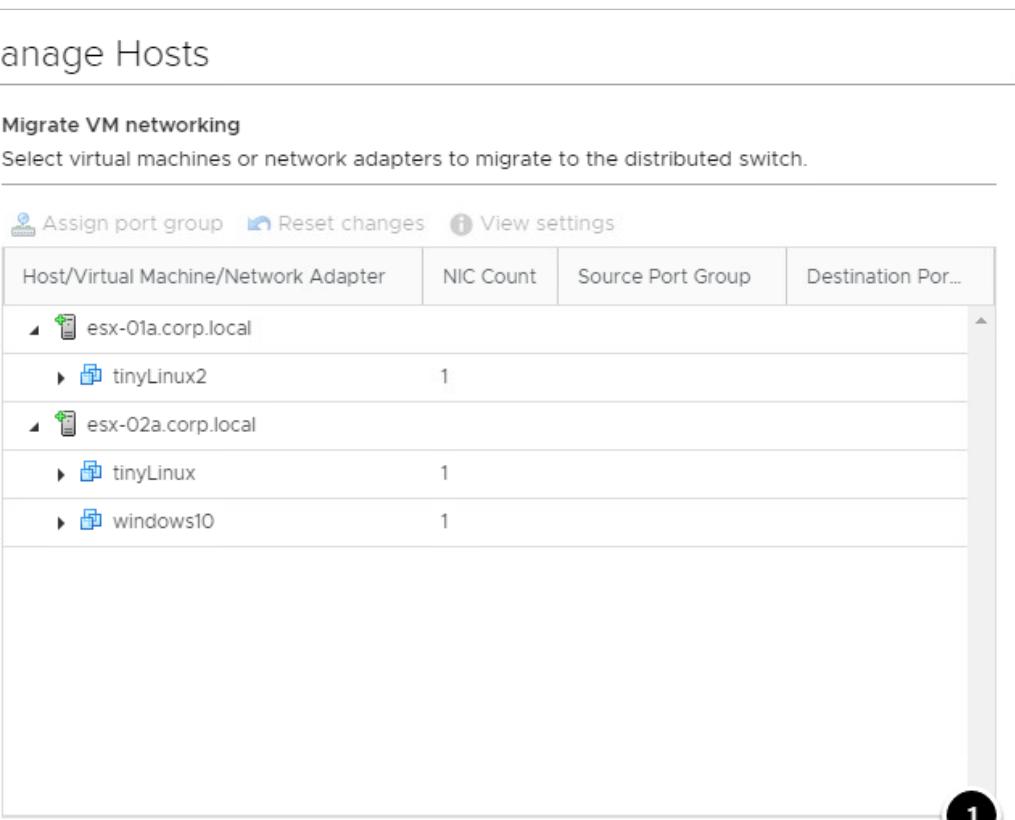
Migrate VM networking
Select virtual machines or network adapters to migrate to the distributed switch.

Assign port group Reset changes View settings

Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group	Destination Por...
esx-01a.corp.local			
tinyLinux2	1		
esx-02a.corp.local			
tinyLinux	1		
windows10	1		

1

CANCEL BACK **NEXT**



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

New vDS - Add and Manage Hosts

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

Review your settings selections before finishing the wizard.

Number of managed hosts
Hosts to add 2

Number of network adapters for update
Physical adapters 2

1 FINISH

1. On the Ready to Complete page, click **Finish**.

Explore your new vDS

New vDS | ACTIONS ▾

Summary Monitor Configure Permissions Ports **Hosts** VMs Networks

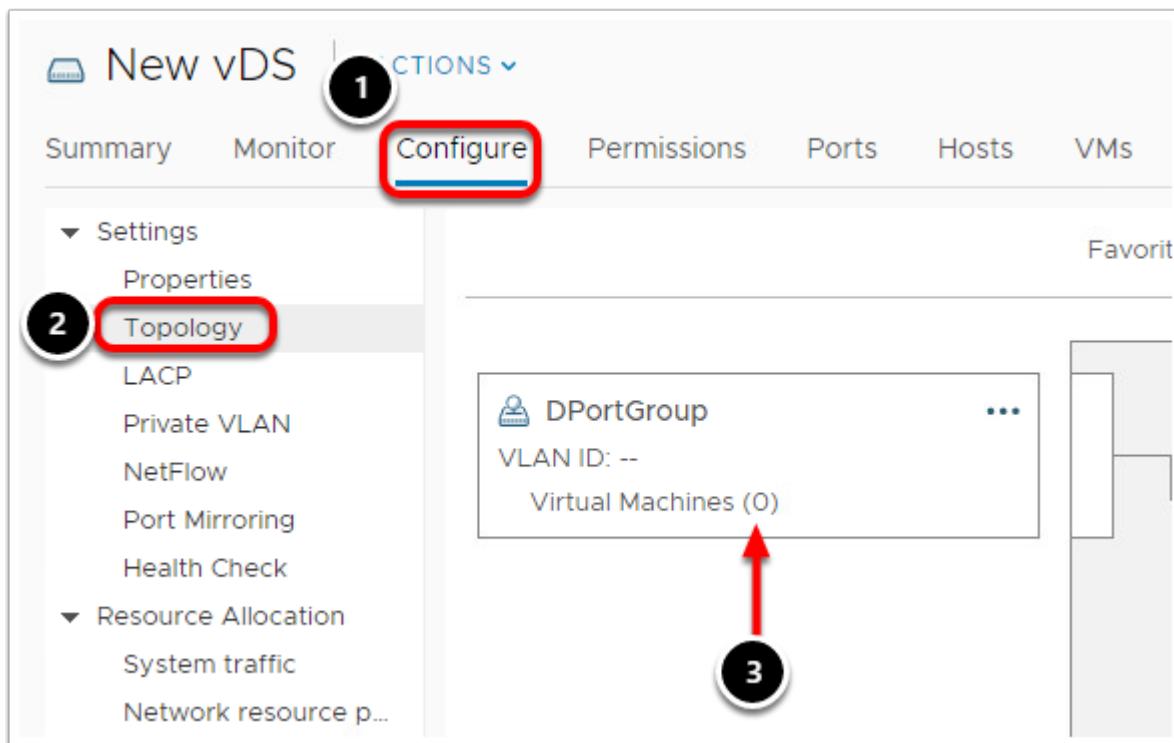
1

Name ↑	State	Status	Cluster
esx-01a.corp.local	Connected	✓ Normal	Site A Cluster 1
esx-02a.corp.local	Connected	✓ Normal	Site A Cluster 1

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

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

Topology



1. Click **Configure**
2. Click **Topology**
3. Note that your distributed port group DPortGroup does not have any VMs connected to it.

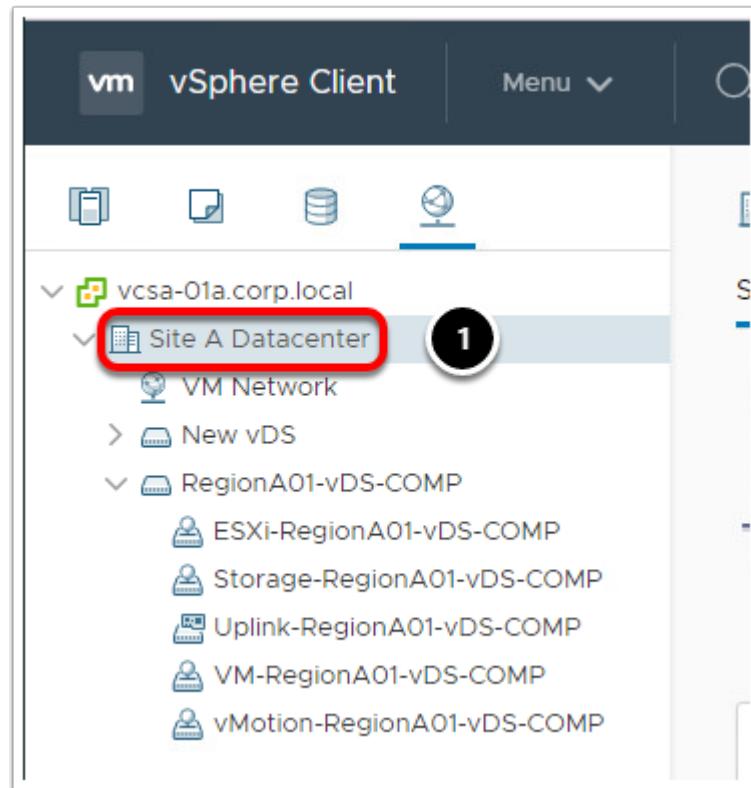
The next lesson will walk through the process of migrating VMs to the new vDS.

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.

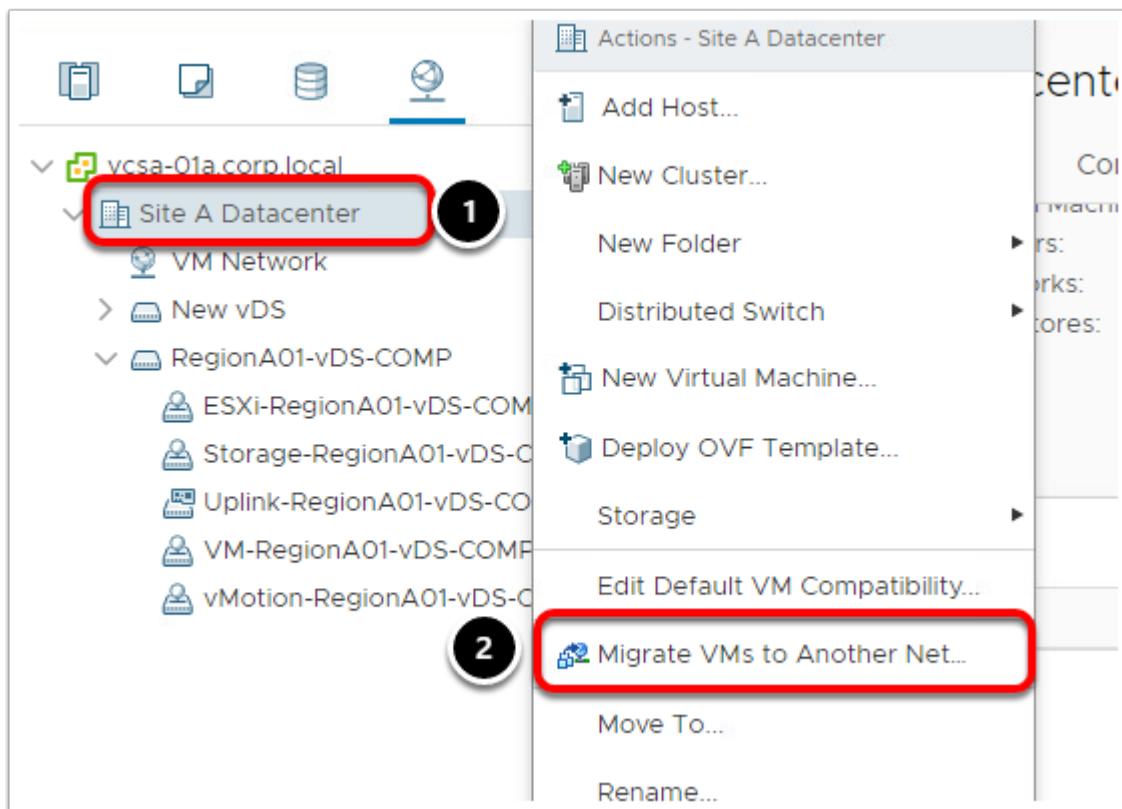
In the vSphere Client, there are numerous ways to accomplish the task of VM network migration. However, we will be walking through the procedures specifically outlined in the vSphere product documentation.

Navigate to your datacenter



To get started, click on **Site A Datacenter**.

Migrate VMs



1. Right click on **Site A Datacenter**
2. Select **Migrate VMs to Another Network**

Select source network

Migrate VMs to Another Network

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

Select source and destination networks for the migration of virtual machine network adapters

Source network

Specific network **BROWSE ...**

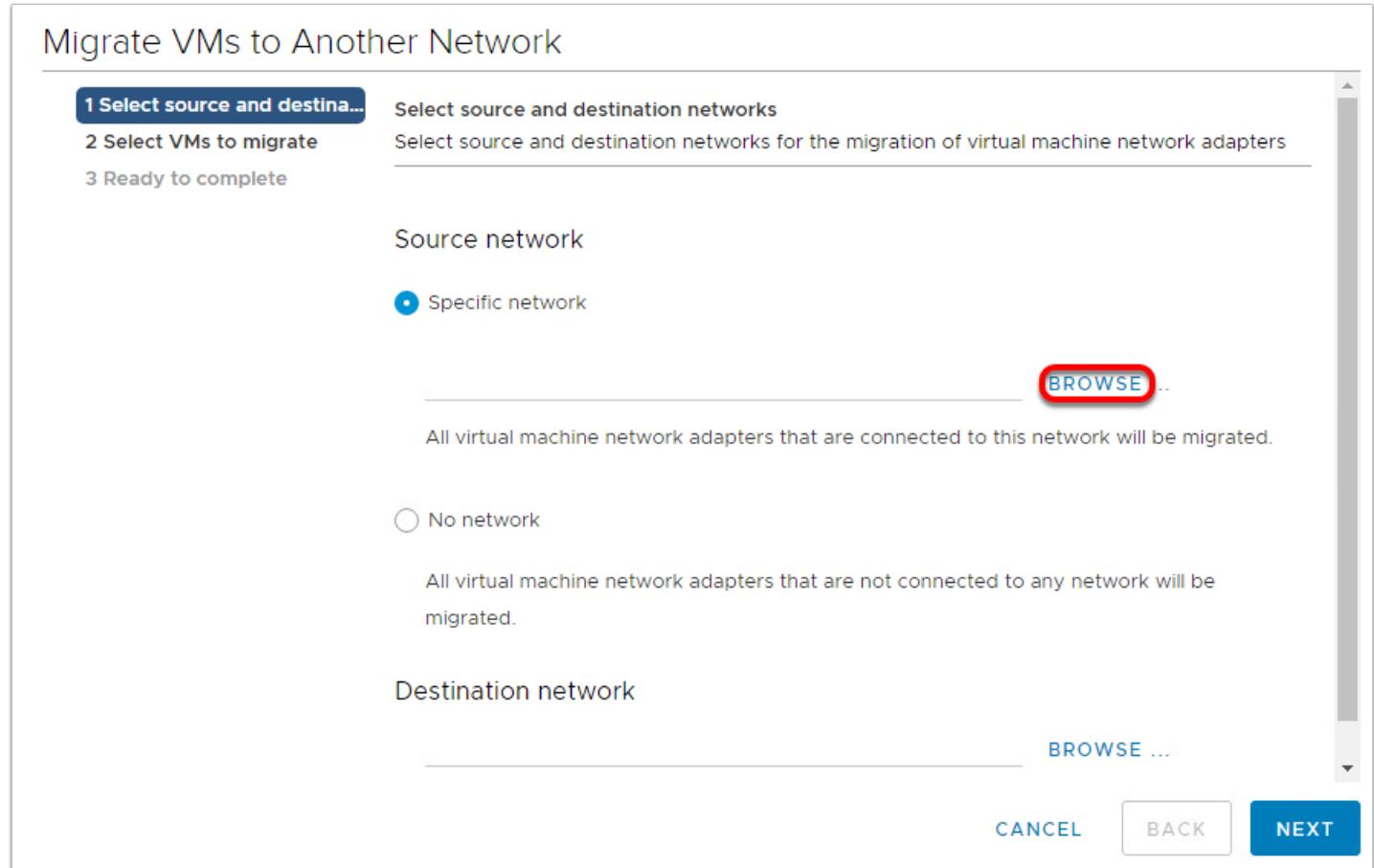
All virtual machine network adapters that are connected to this network will be migrated.

No network

All virtual machine network adapters that are not connected to any network will be migrated.

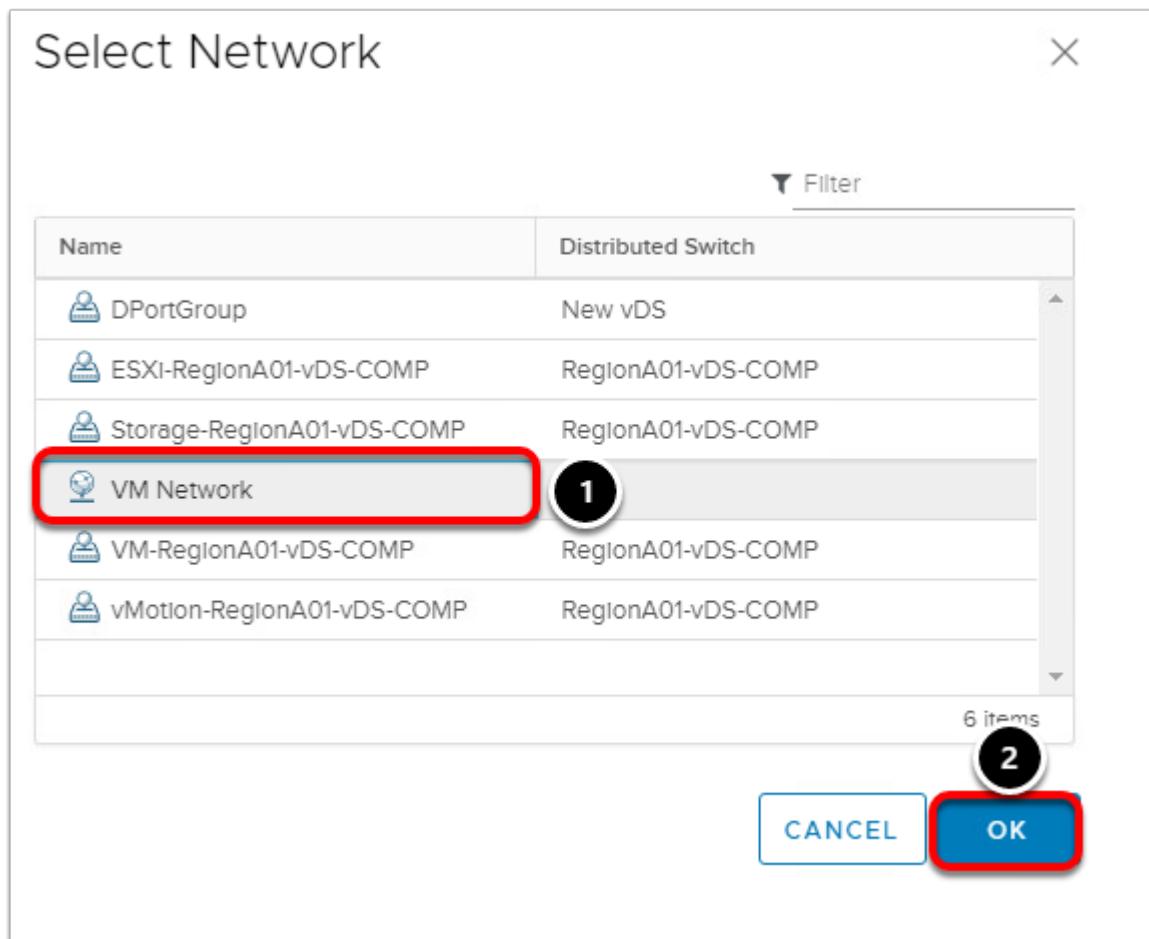
Destination network **BROWSE ...**

CANCEL **BACK** **NEXT**



1. In the Select source and destination networks section, click on **Browse** under **Source network**.

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

Migrate VMs to Another Network

1 Select source and destina... Select source and destination networks for the migration of virtual machine network adapters

2 Select VMs to migrate

3 Ready to complete

Source network

Specific network

VM Network BROWSE ...

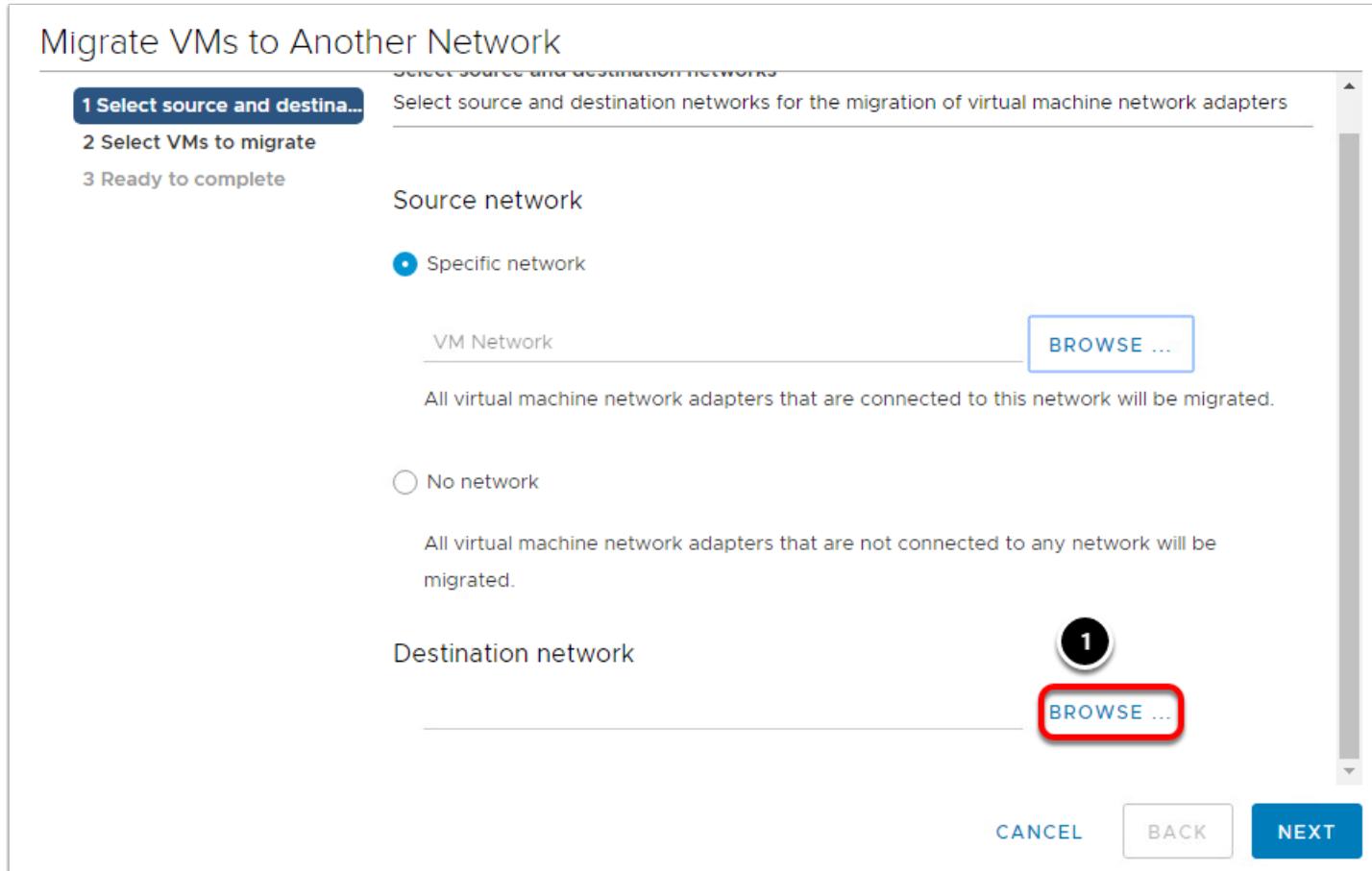
All virtual machine network adapters that are connected to this network will be migrated.

No network

All virtual machine network adapters that are not connected to any network will be migrated.

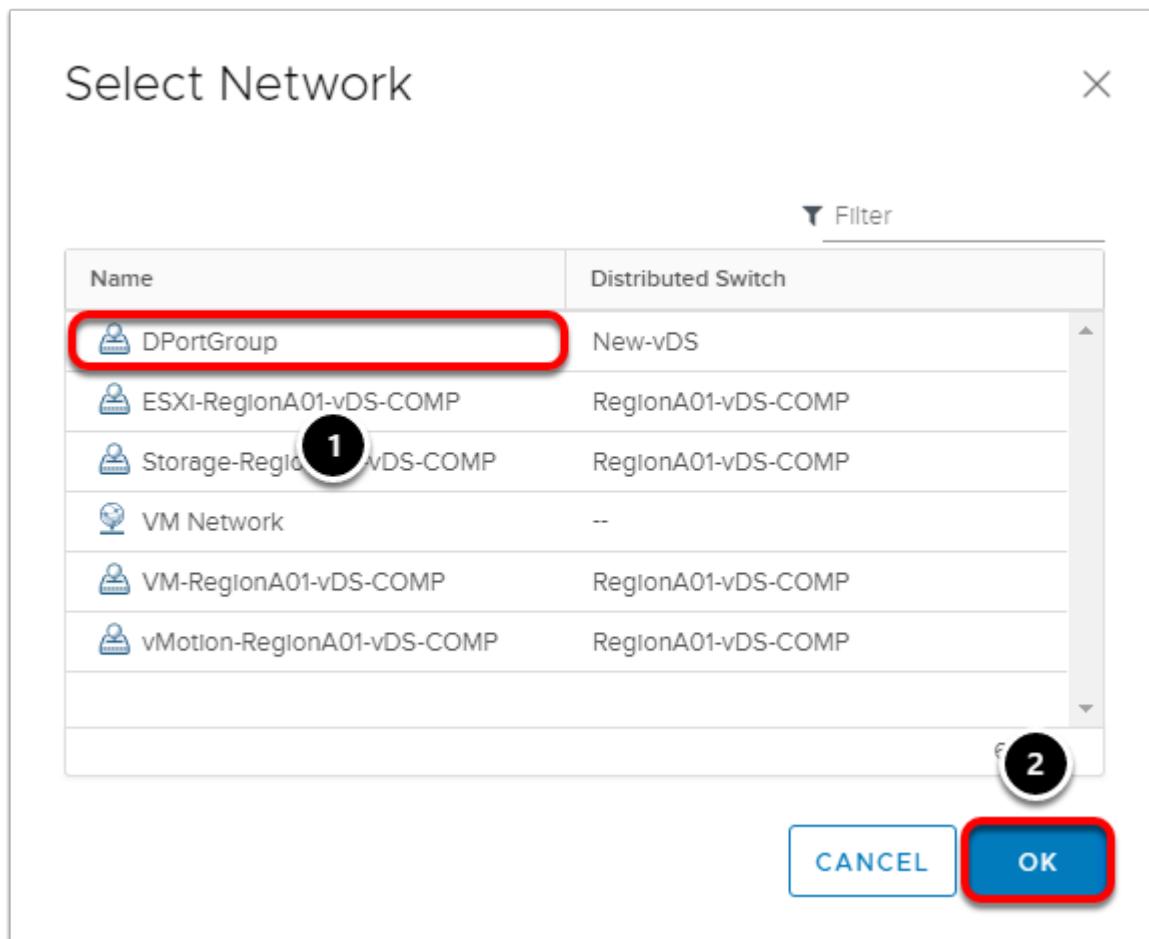
Destination network 1 BROWSE ...

CANCEL BACK NEXT



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

Migrate VMs to Another Network

1 Select source and destina... Select source and destination networks

2 Select VMs to migrate

3 Ready to complete

Source network

Specific network

VM Network BROWSE ...

All virtual machine network adapters that are connected to this network will be migrated.

No network

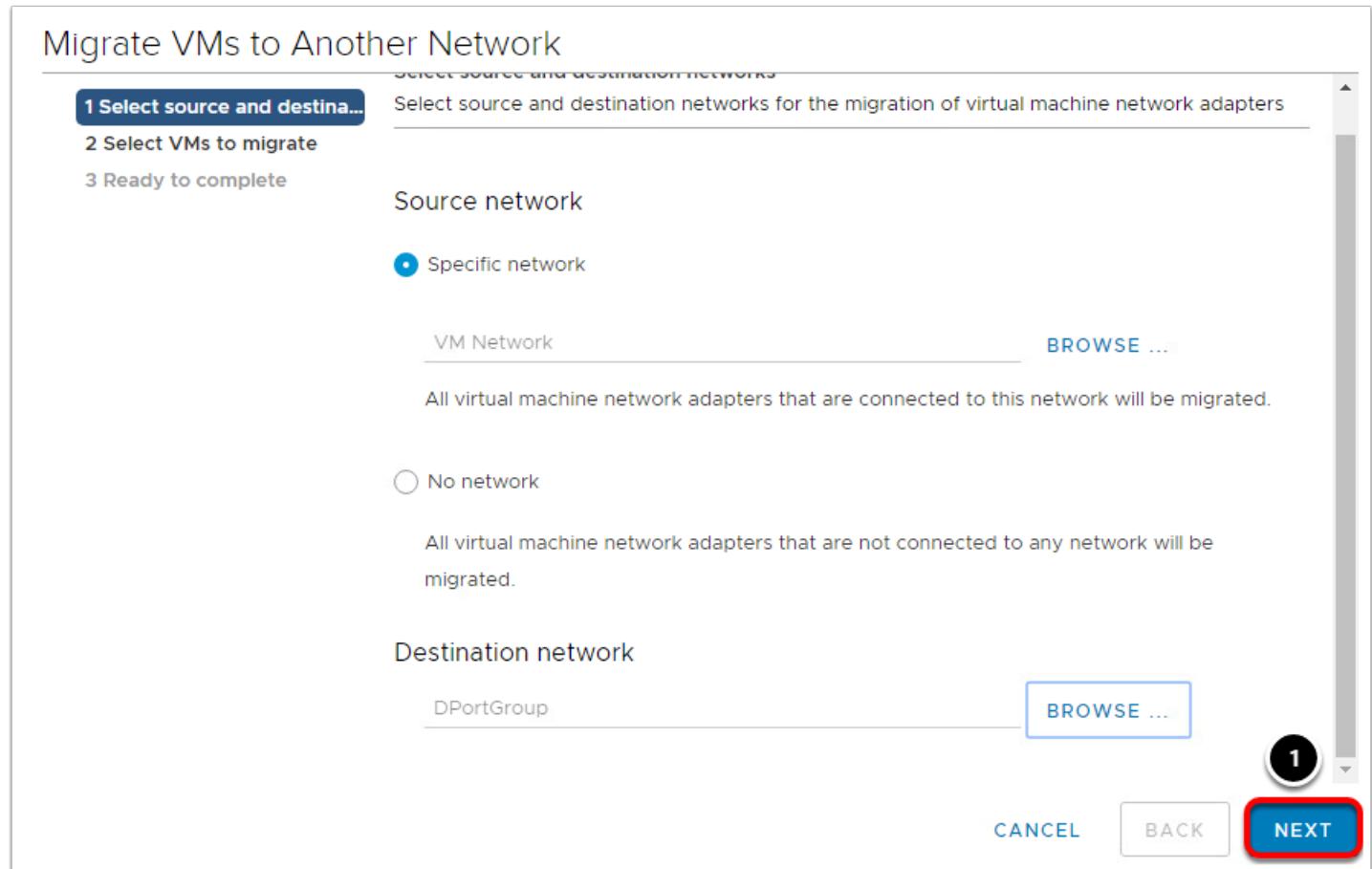
All virtual machine network adapters that are not connected to any network will be migrated.

Destination network

DPortGroup BROWSE ...

1

CANCEL BACK **NEXT**



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

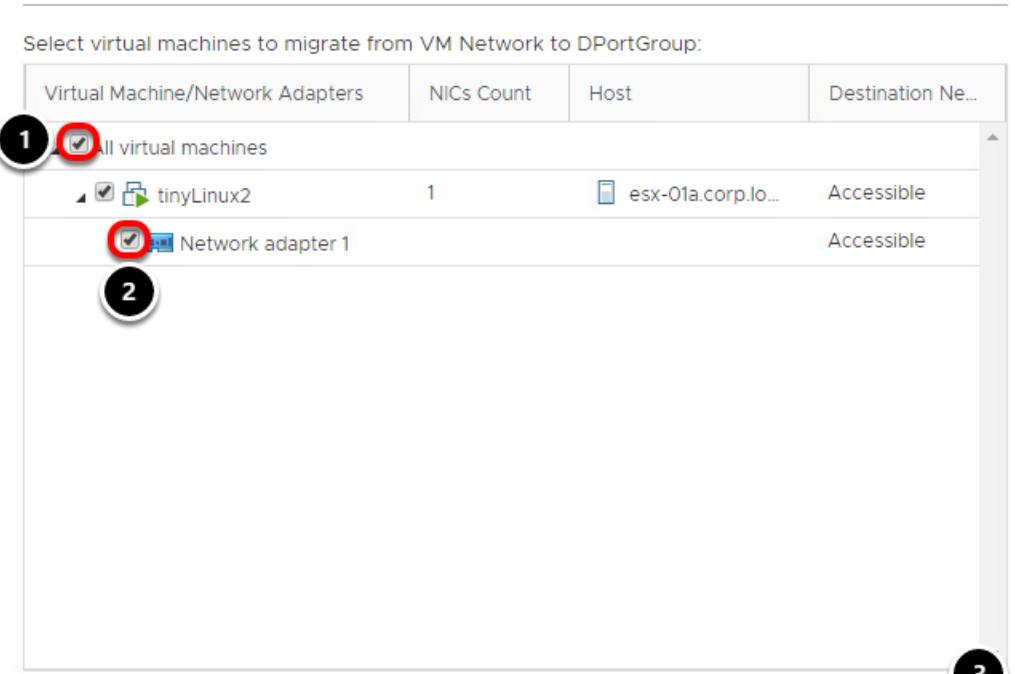
Select virtual machines to migrate from VM Network to DPortGroup:

Virtual Machine/Network Adapters	NICs Count	Host	Destination Ne...
1 <input checked="" type="checkbox"/> All virtual machines			
2 <input checked="" type="checkbox"/> tinyLinux2	1	esx-01a.corp.io...	Accessible
3 <input checked="" type="checkbox"/> Network adapter 1			Accessible

1 All virtual machines
2 tinyLinux2
3 Network adapter 1

3

CANCEL BACK **NEXT**



1. On the Select VMs to migrate page, click on the expand arrow of the **tinyLinux2** VM to show the network adapters associate with this virtual machine.

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. Select the check box for **Network adapter 1**.
3. Click **Next**.

Ready to Complete

Migrate VMs to Another Network

✓ 1 Select source and destina...

✓ 2 Select VMs to migrate

3 Ready to complete

Ready to complete

Review your settings selections before finishing the wizard.

Source network	VM Network
Destination network	DPortGroup
Virtual machines to migrate	1
Network adapters to migrate	1

1

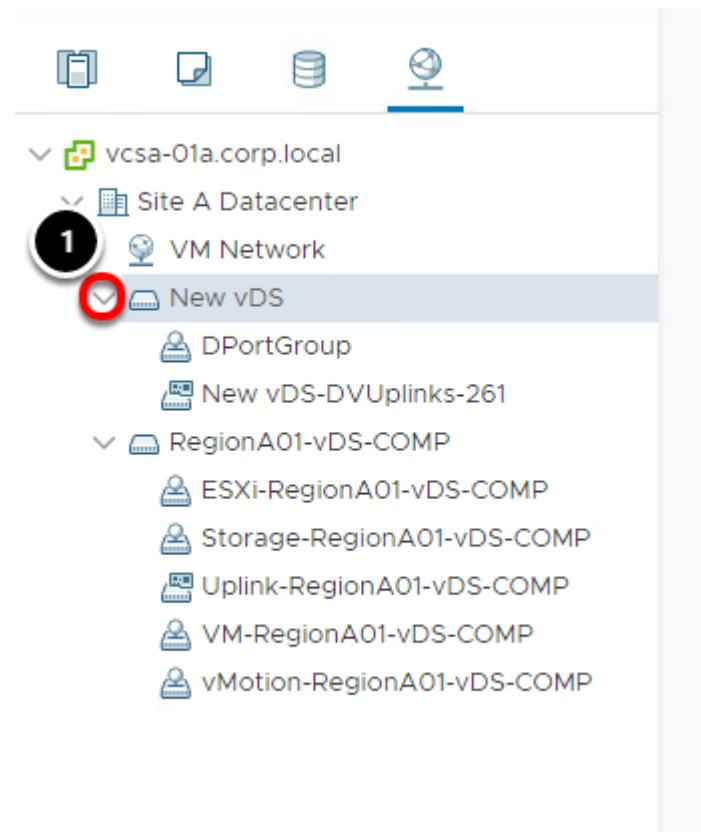
CANCEL

BACK

FINISH

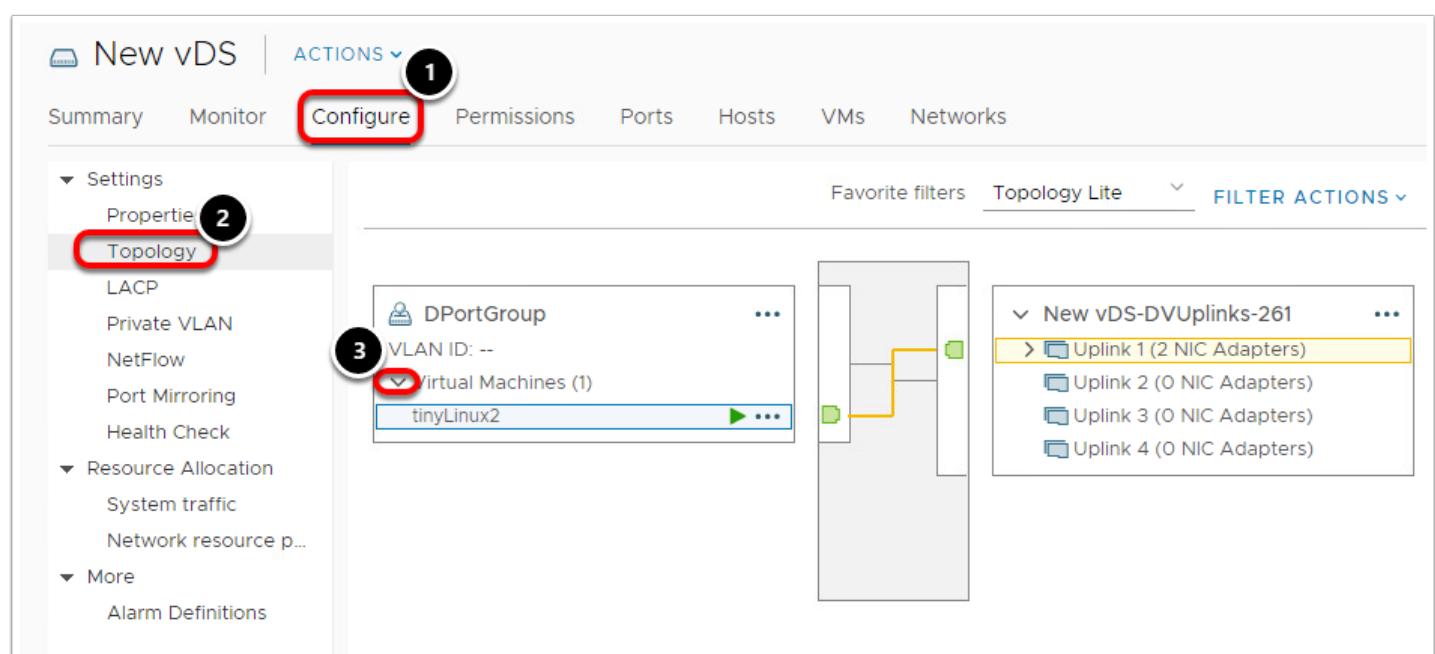
1. Click **Finish** to migrate the VM from a Standard Switch to the new Distributed Switch.

Explore your changes



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

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.

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).

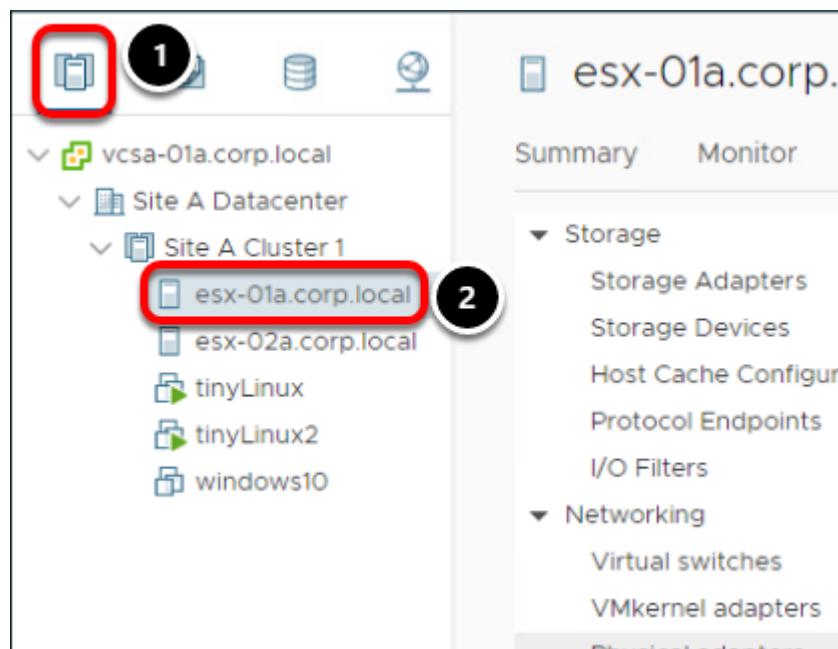
NOTES:

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.

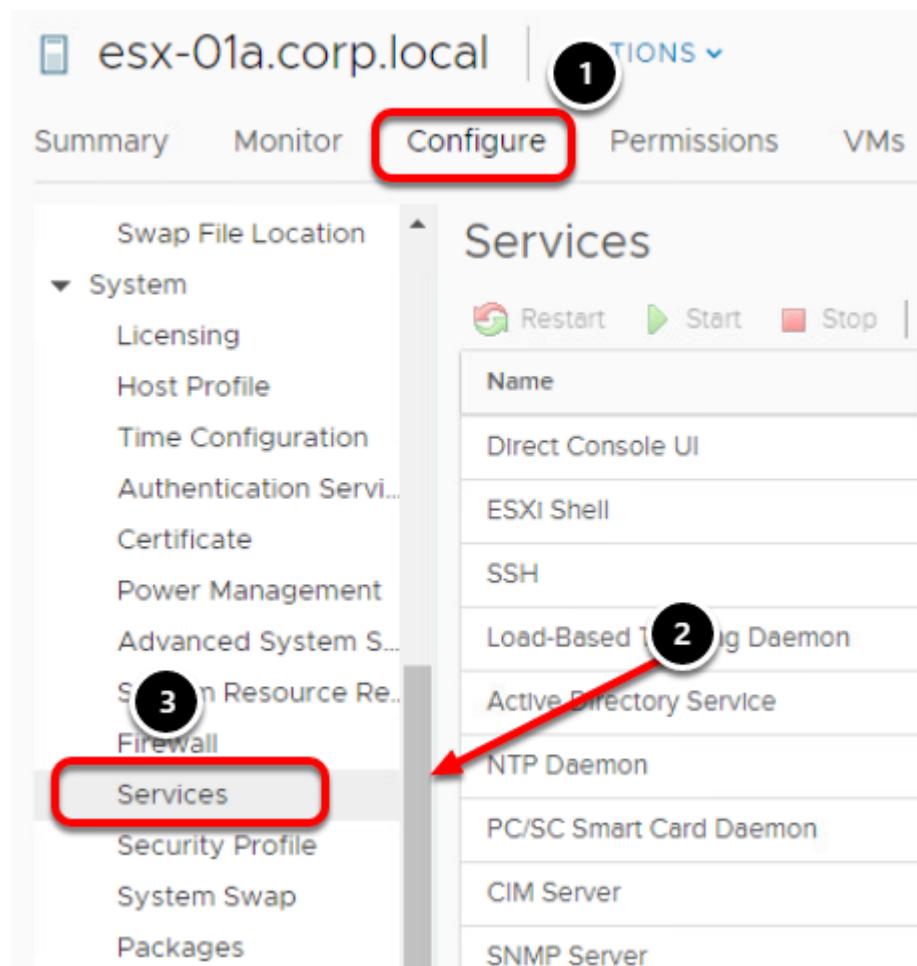
Select Hosts and Clusters



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



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

Services

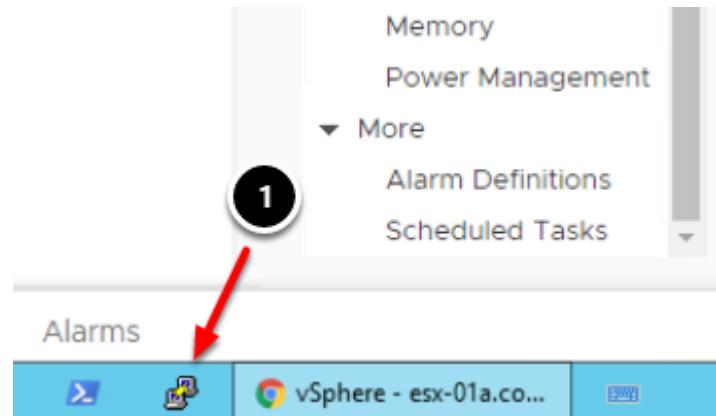
REFRESH

Restart Start Stop | Edit Startup Policy...

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.

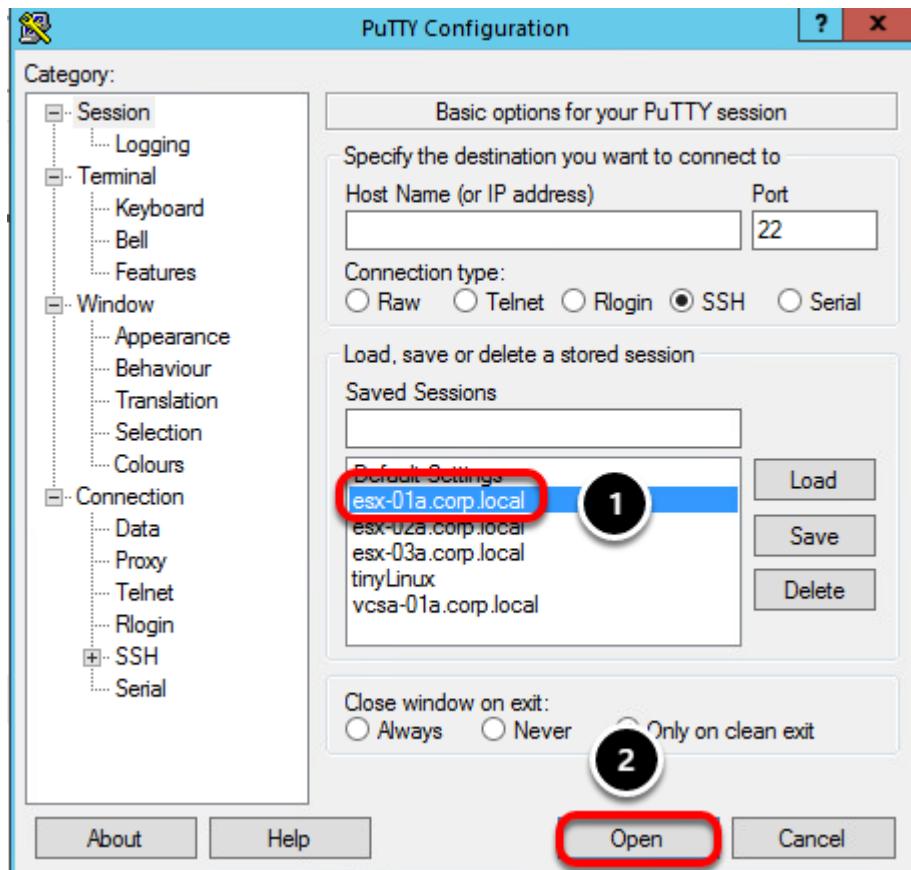
Open an SSH session to esx-01a



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

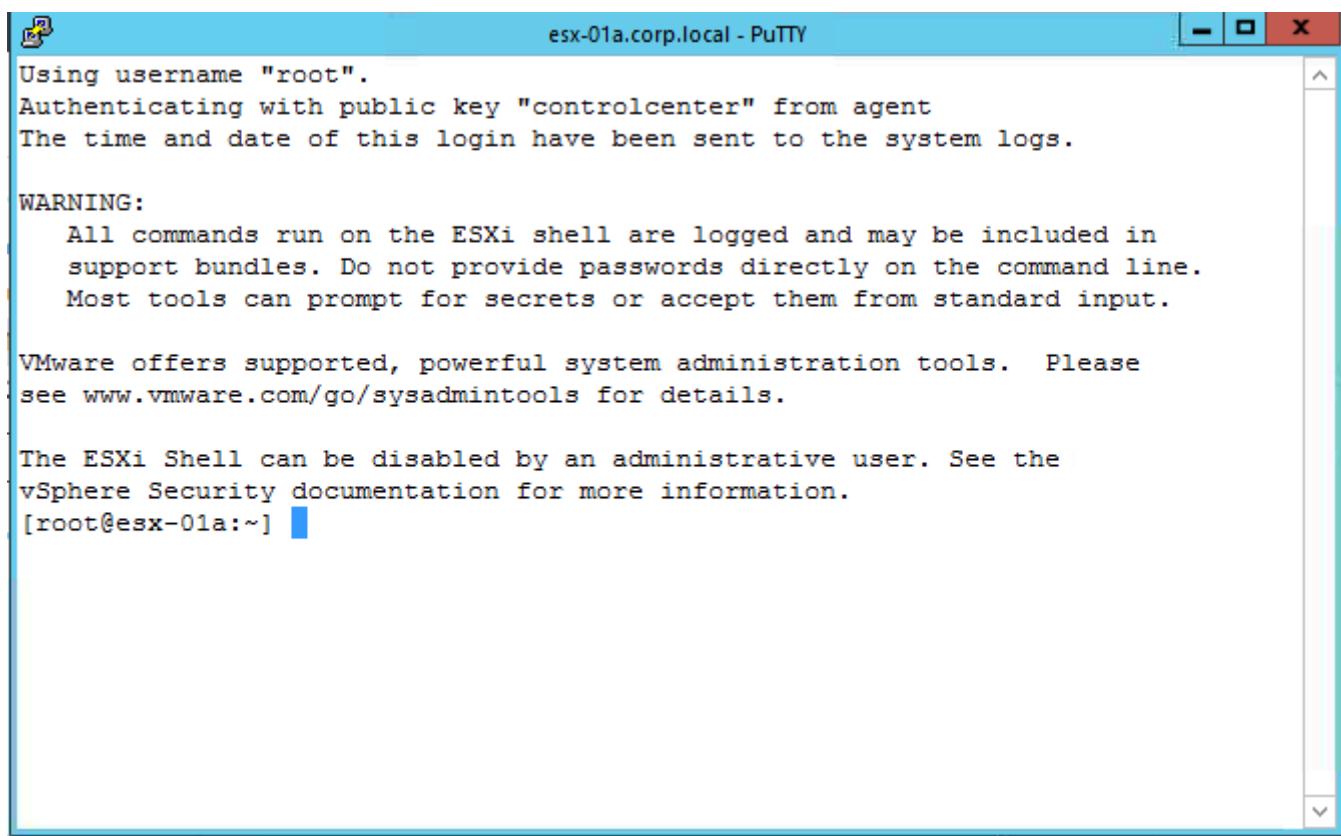
1. From the Windows Taskbar, click on the **PuTTY** icon.

Connect to esx-01a



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

Logged into esx-01a



esx-01a.corp.local - PuTTY

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

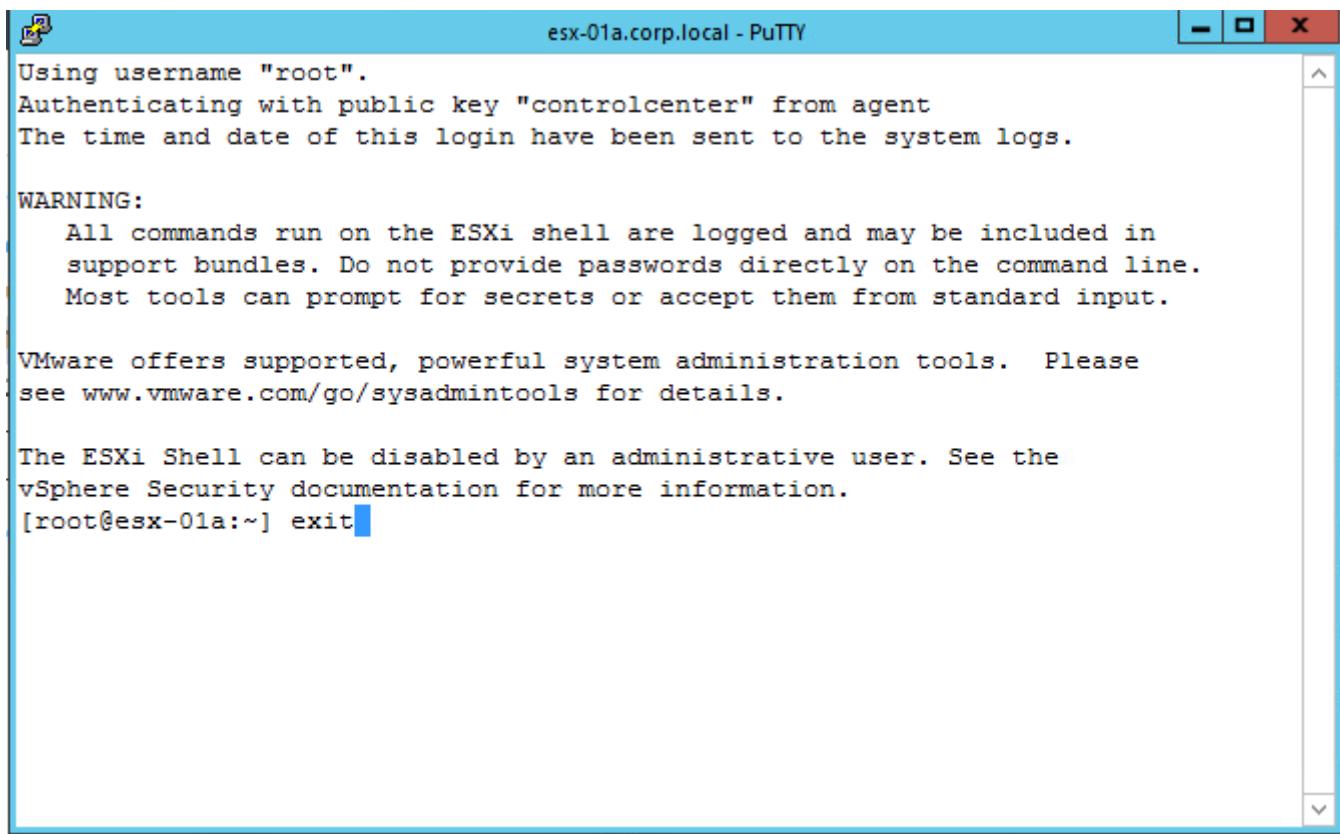
WARNING:
  All commands run on the ESXi shell are logged and may be included in
  support bundles. Do not provide passwords directly on the command line.
  Most tools can prompt for secrets or accept them from standard input.

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



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

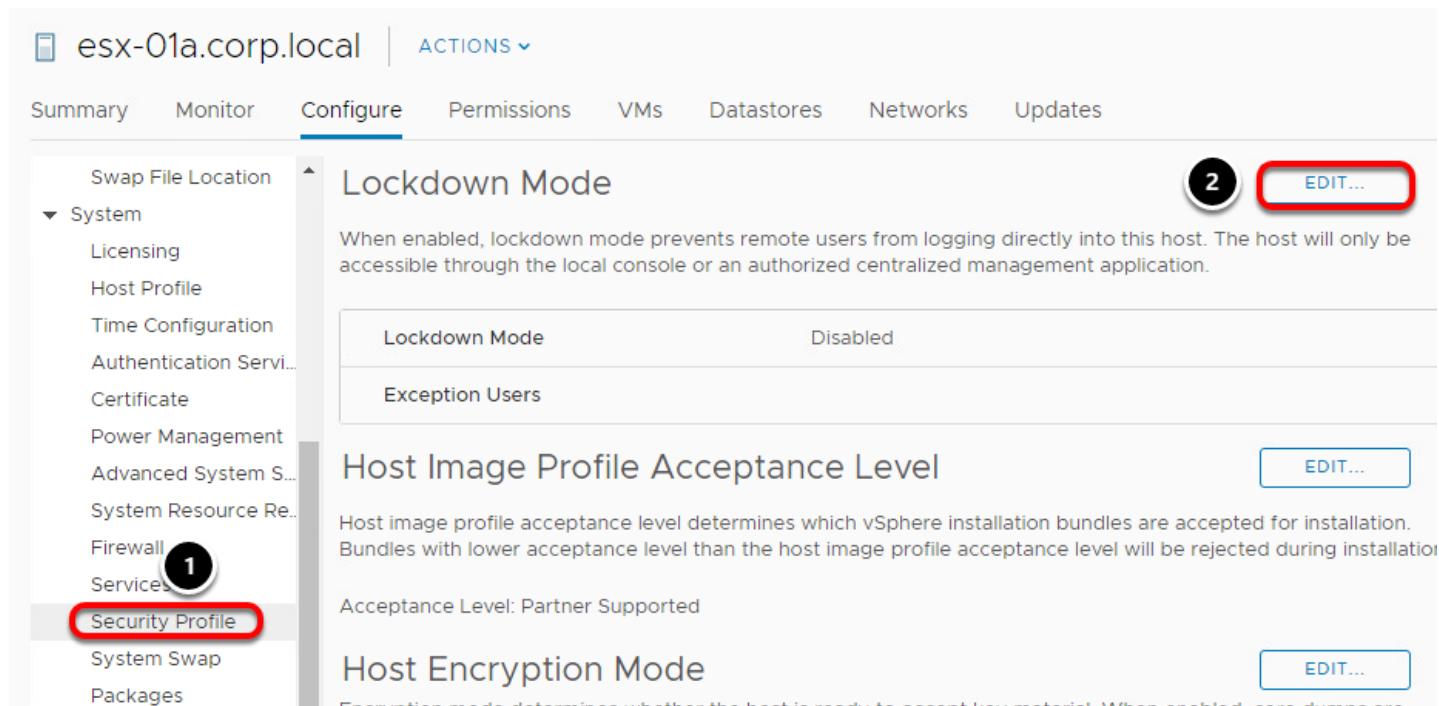
WARNING:
  All commands run on the ESXi shell are logged and may be included in
  support bundles. Do not provide passwords directly on the command line.
  Most tools can prompt for secrets or accept them from standard input.

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:~] exit
```

Close the PuTTY session by typing '**exit**' and pressing Enter. Once you hit Enter, the PuTTY window will disappear.

Enabling Lockdown Mode



esx-01a.corp.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Swap File Location

System

- Licensing
- Host Profile
- Time Configuration
- Authentication Servi...
- Certificate
- Power Management
- Advanced System S...
- System Resource Re...
- Firewall
- Services 1
- Security Profile** 2
- System Swap
- Packages

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	Disabled
Exception Users	

Host Image Profile Acceptance Level

Host image profile acceptance level determines which vSphere installation bundles are accepted for installation. Bundles with lower acceptance level than the host image profile acceptance level will be rejected during installation.

Acceptance Level: Partner Supported

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

esx-01a.corp.local - Lockdown Mode

Lockdown Mode

Exception Users

2

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

Disabled

Lockdown mode is disabled.

Normal

1

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

Strict

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

CANCEL

OK

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

esx-01a.corp.local - Lockdown Mode

Lockdown Mode

Exception Users

Exception Users

A list of user accounts that keep their permissions when the host enters lockdown mode. The accounts are used by third-party solutions and external applications that must continue their function in lockdown mode. To keep lockdown mode uncompromised, you should add only user accounts that are associated with applications.

 Add User  Remove User

User

No items displayed

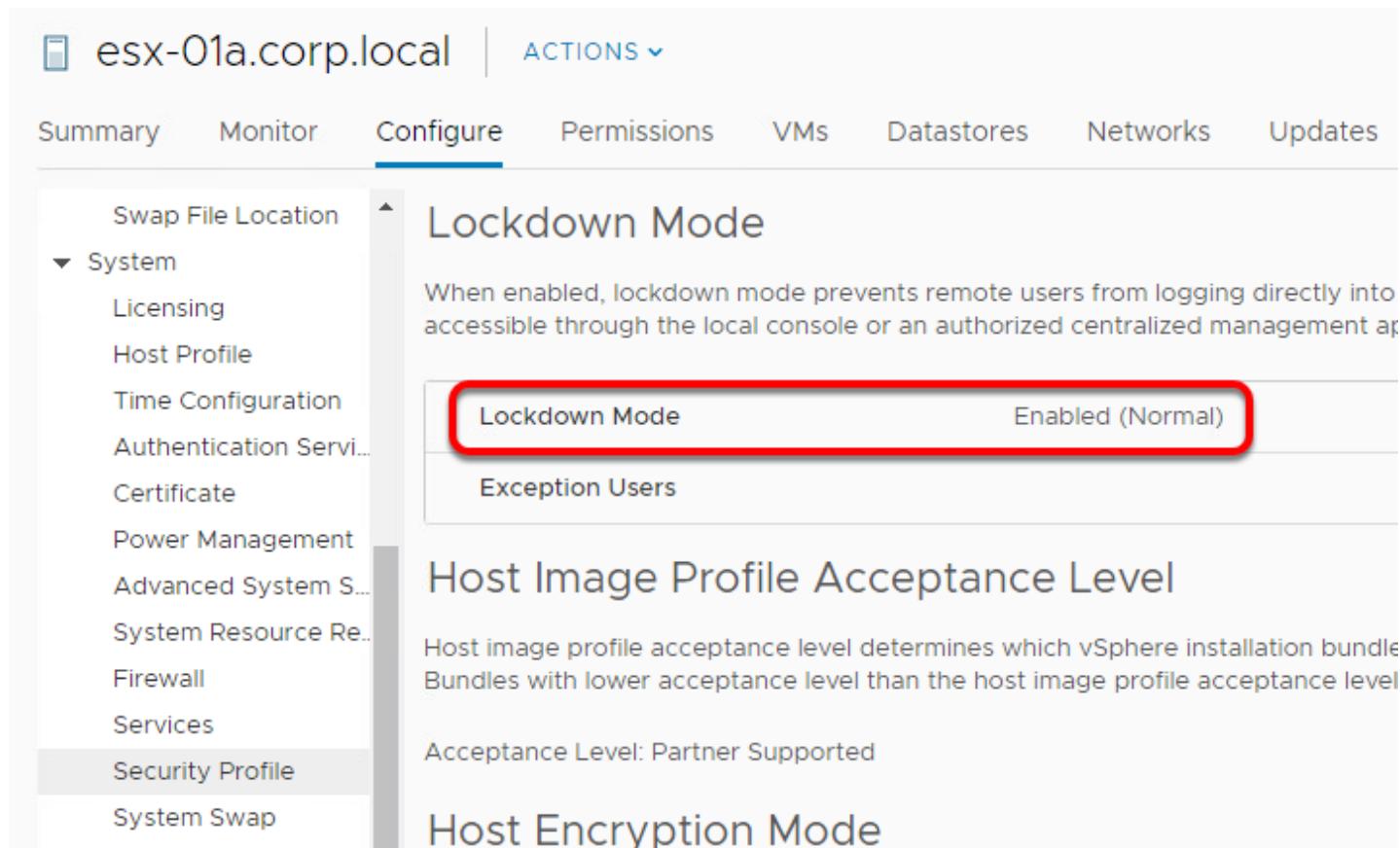
1

CANCEL **OK**

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



esx-01a.corp.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Swap File Location

System

- Licensing
- Host Profile
- Time Configuration
- Authentication Servi...
- Certificate
- Power Management
- Advanced System S...
- System Resource Re...
- Firewall
- Services
- Security Profile
- System Swap

Lockdown Mode

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

Lockdown Mode	Enabled (Normal)
Exception Users	

Host Image Profile Acceptance Level

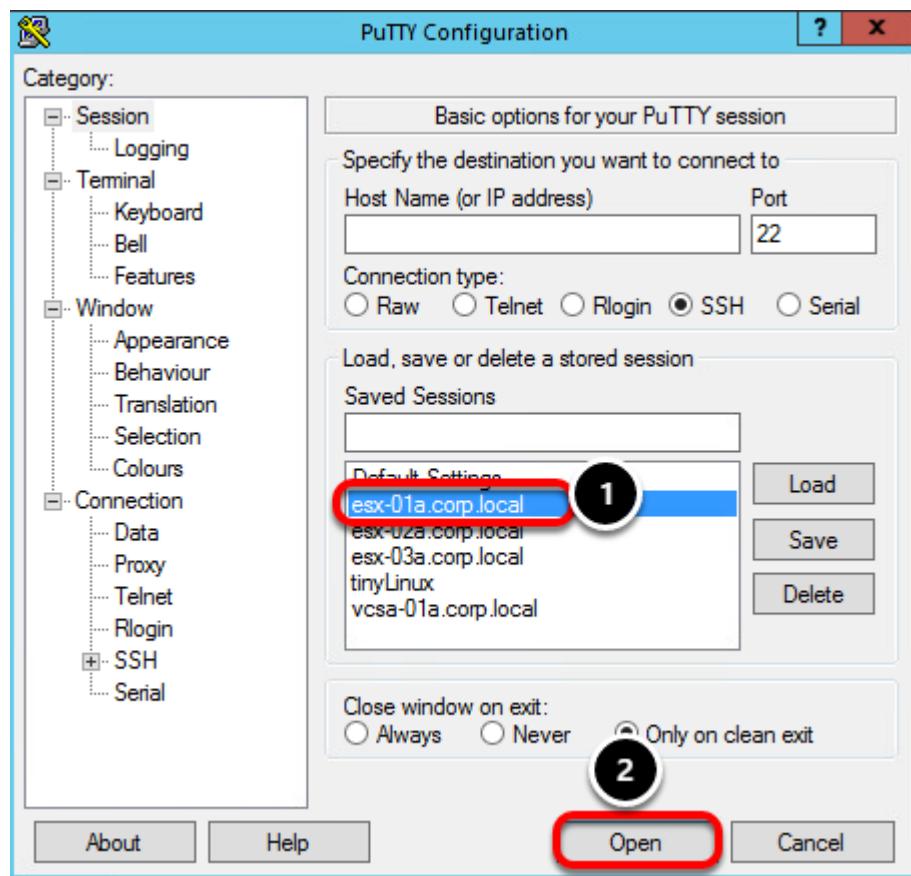
Host image profile acceptance level determines which vSphere installation bundle Bundles with lower acceptance level than the host image profile acceptance level

Acceptance Level: Partner Supported

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 **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

cal | ACTIONS ▾

configure Permissions VMs Datastores Networks Updates

1 **Lockdown Mode** EDIT...

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 (Normal)
Exception Users	

Go back to the vSphere Client.

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

Lockdown Mode

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host.

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

Specify host lockdown mode:

Disabled 1

Lockdown mode is disabled.

Normal

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

Strict

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



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.

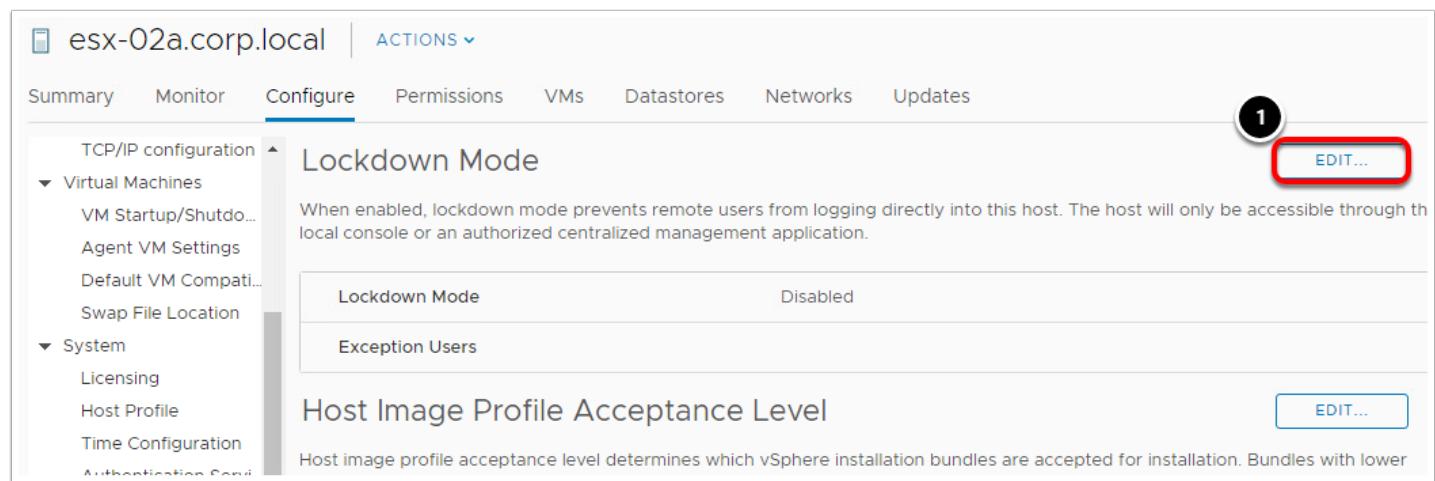
Strict Mode

The screenshot shows the vSphere Client interface. The left sidebar displays a tree structure of vCenter servers, datacenters, and hosts. A host named 'esx-02a.corp.local' is selected and highlighted with a red box and a circled '1'. The right pane shows the host configuration interface. The 'Configure' tab is selected and highlighted with a red box and a circled '2'. The 'Security Profile' option in the configuration menu is also highlighted with a red box and a circled '3'. The configuration menu includes options like Host Profile, Time Configuration, Authentication Service, Certificate, Power Management, Advanced System Settings, System Resource Reservation, Firewall, Services, and Security Profile.

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



The screenshot shows the vSphere Web Client interface for host esx-02a.corp.local. The 'Configure' tab is selected. On the left, a sidebar shows sections like TCP/IP configuration, Virtual Machines, System, and Host Image Profile Acceptance Level. The 'Lockdown Mode' section is expanded, showing a table with 'Lockdown Mode' set to 'Disabled' and an 'Exception Users' section. A red box highlights the 'Edit...' button next to the 'Lockdown Mode' table, with a circled '1' above it, indicating the first step in the process.

1. Click on the **Edit...** button.

Lockdown Mode - Strict

esx-02a.corp.local - Lockdown Mode

Lockdown Mode

Exception Users

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

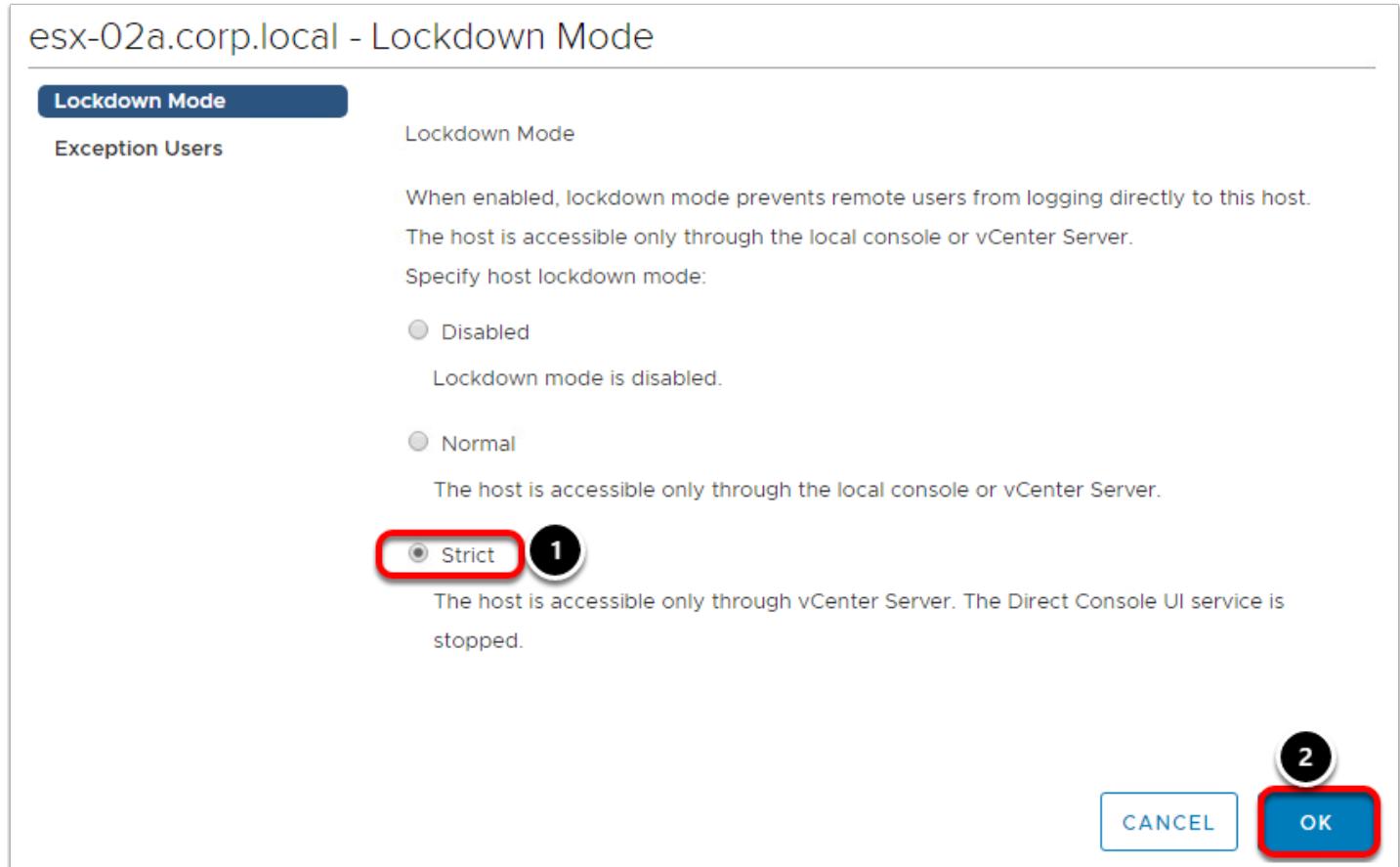
Disabled
Lockdown mode is disabled.

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

Strict 1

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

2 OK CANCEL



1. Click button next to **Strict**.
2. Click **OK**.

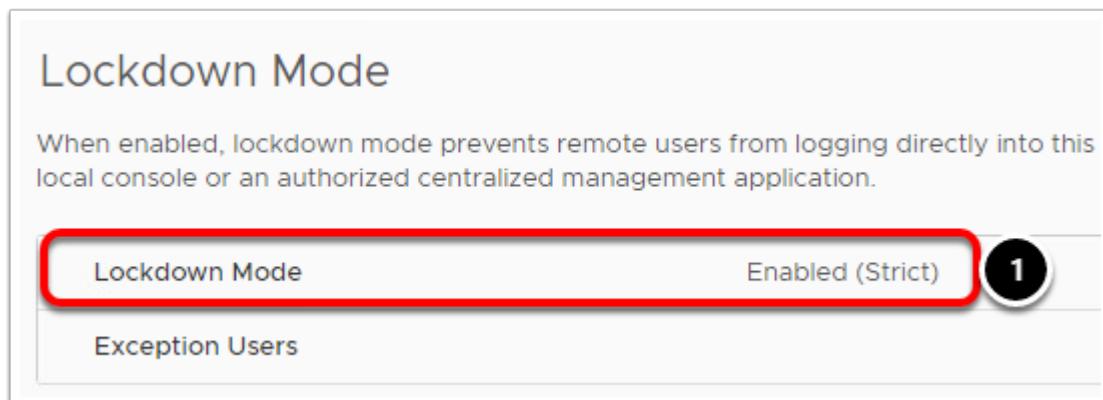
Again, note that users can be added to the exception list. This will only apply to SSH and not the DCUI.

Strict Mode - Enabled

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this local console or an authorized centralized management application.

Lockdown Mode	Enabled (Strict) 1
Exception Users	



1. Notice Lockdown Mode is now Enabled.

Services

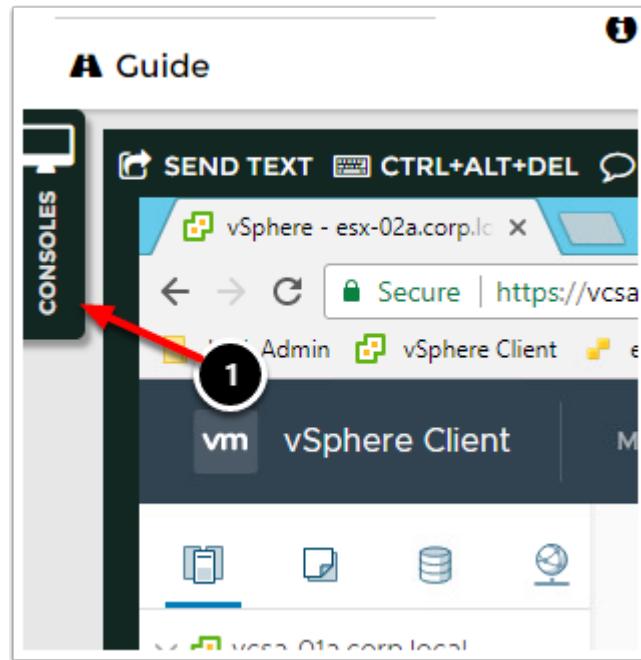
The screenshot shows the vSphere Web Client interface for host `esx-02a.corp.local`. The `Configure` tab is selected. On the left, a sidebar lists `TCP/IP configuration`, `Virtual Machines` (with `VM Startup/Shutdo...`, `Agent VM Settings`, `Default VM Compati...`, and `Swap File Location`), and `System` (with `Licensing`, `Host Profile`, `Time Configuration`, `Authentication Servi...`, `Certificate`, `Power Management`, `Advanced System S...`, `System Resource Re...`, `Firewall`, `Services` (circled with 1), and `Security Profile`). The main content area is titled `Services` and contains a table with the following data:

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.

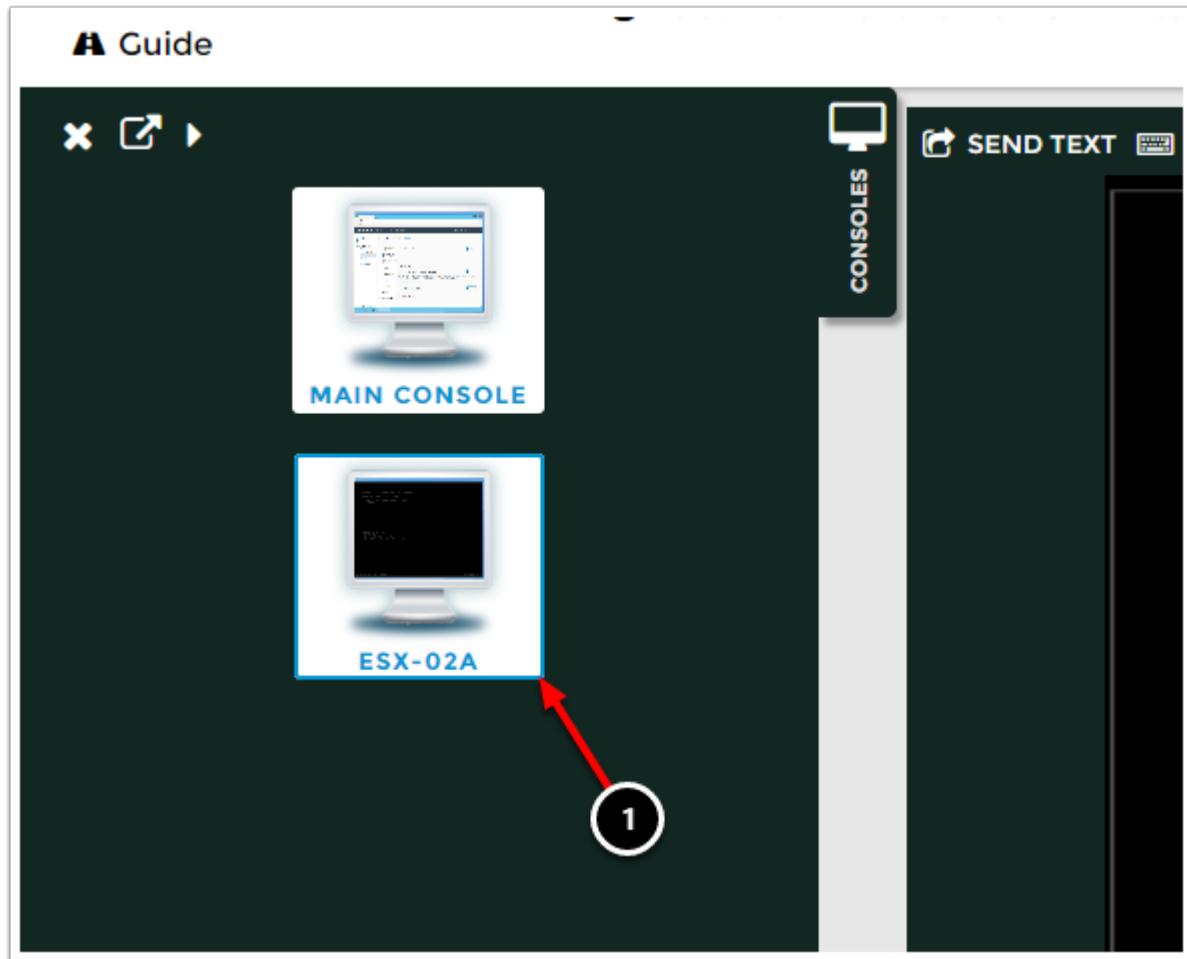
DCUI Disabled



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



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

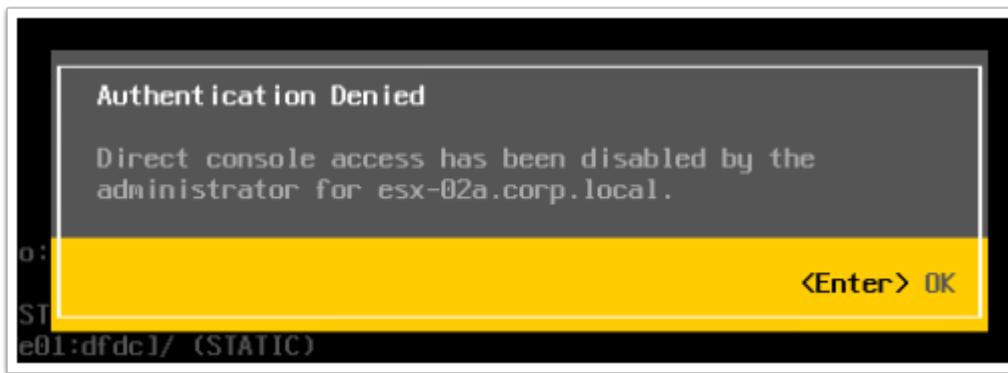
The console window will load the DCUI for esx-02a.corp.local.

Click in the Console



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

Press F2

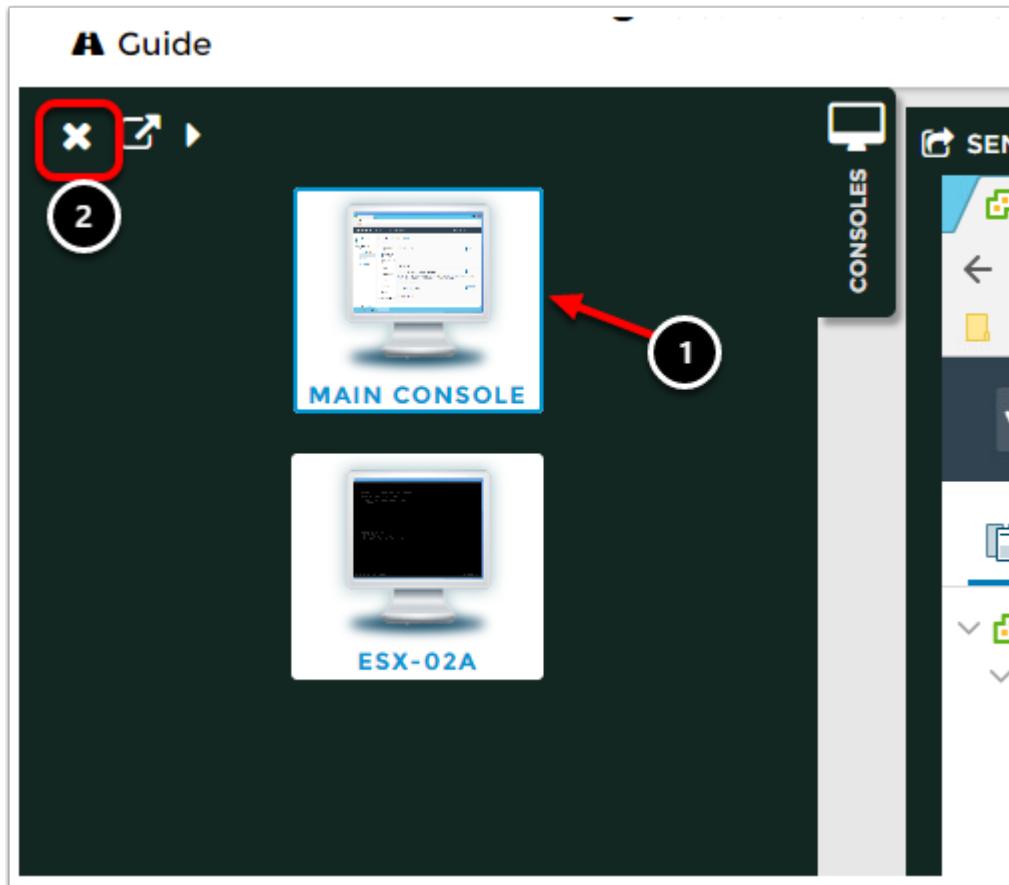


1. Now press the **F2** key to log in to the DCUI.

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 Serv... Certificate Power Management Advanced System S... System Resource Re... Firewall Services Security Profile **1**

Lockdown Mode **2** EDIT...

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 **EDIT...**

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

Go back to the vSphere Client.

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

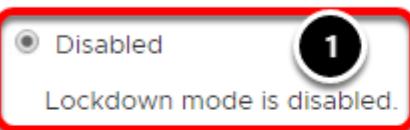
Lockdown Mode

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host.

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

Specify host lockdown mode:



Disabled

1

Lockdown mode is disabled.

Normal

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

Strict

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



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.

User Access and Authentication Roles

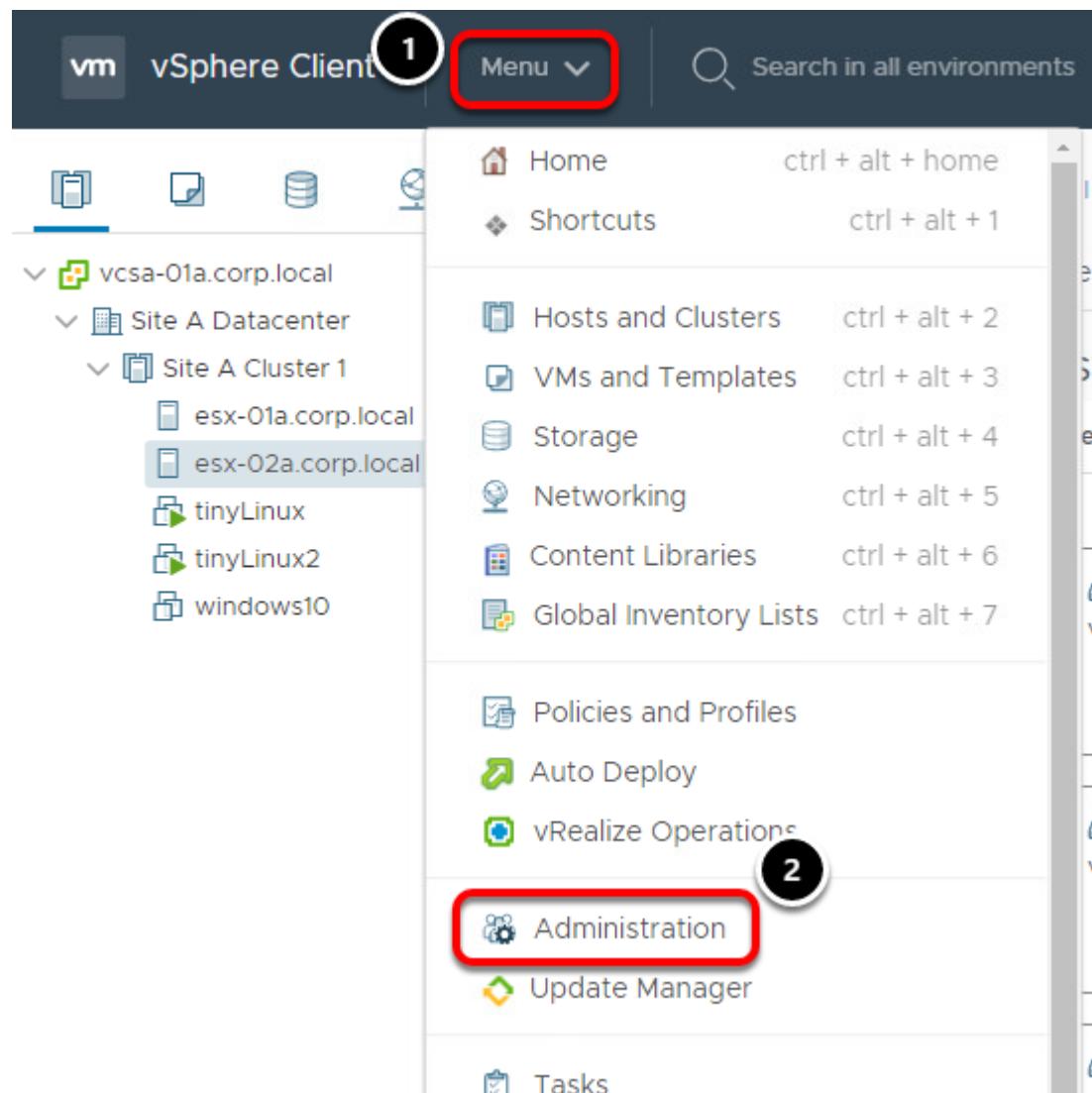
VMware recommends that you create roles to suit the access control needs of your environment. If you create or edit a role on a vCenter Server system that is part of a connected group in Linked Mode, the changes that you make are propagated to all other vCenter Server systems in the group.

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

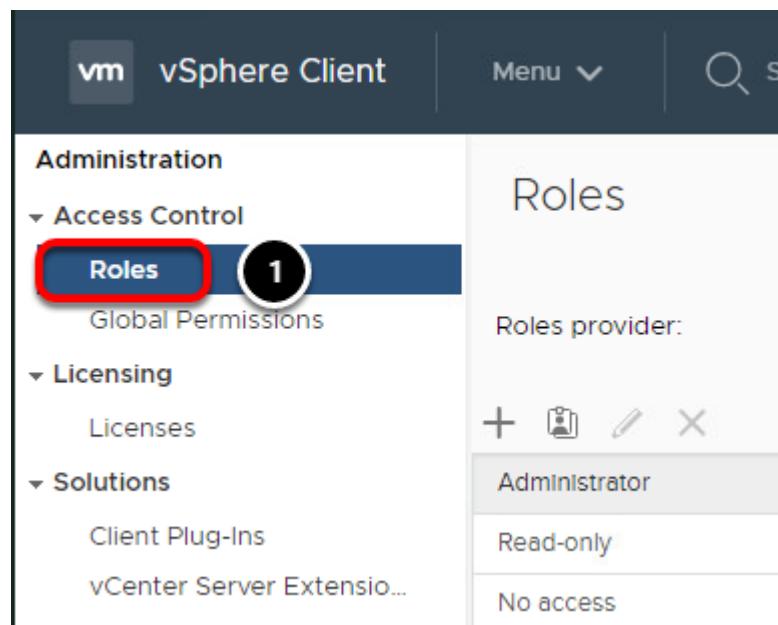
In the following steps, we will create a role in the vSphere Client that we can assign rights for the role.

Administration



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

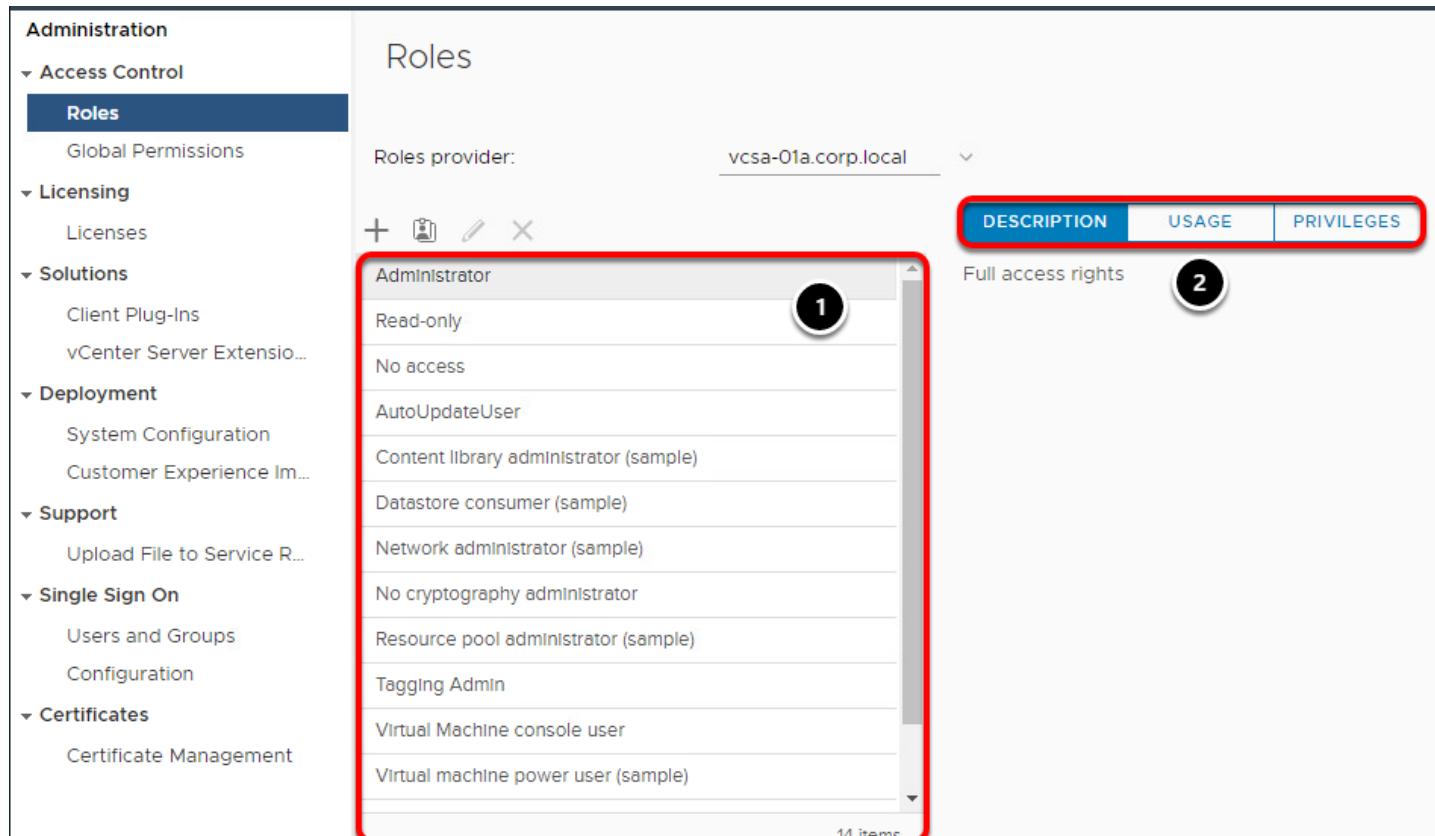
Roles



The screenshot shows the vSphere Client interface. The left sidebar has a 'Administration' section with 'Access Control' expanded, showing 'Roles' (which is highlighted with a red box and a circled '1') and 'Global Permissions'. Below that are 'Licensing' and 'Solutions' sections. The main pane is titled 'Roles' and shows a list of roles: 'Administrator', 'Read-only', and 'No access'. Below the list are buttons for '+', 'Edit', and 'X'. The status bar at the bottom says '14 items'.

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

Roles Overview

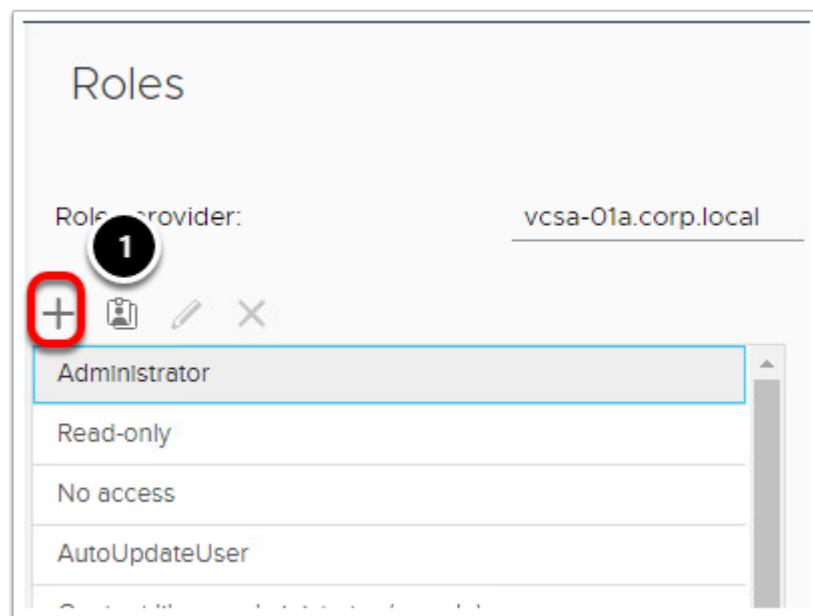


The screenshot shows the 'Roles' list in the vSphere Client. The left sidebar has expanded sections for 'Access Control' (with 'Roles' selected, circled '1'), 'Licensing', 'Solutions' (with 'Client Plug-Ins' and 'vCenter Server Extensio...'), 'Deployment' (with 'System Configuration' and 'Customer Experience Im...'), 'Support' (with 'Upload File to Service R...'), 'Single Sign On' (with 'Users and Groups' and 'Configuration'), and 'Certificates' (with 'Certificate Management'). The main pane is titled 'Roles' and shows a list of roles. The header has tabs for 'DESCRIPTION' (which is highlighted with a red box and circled '2'), 'USAGE', and 'PRIVILEGES'. The list includes: 'Administrator', 'Read-only', 'No access', 'AutoUpdateUser', 'Content library administrator (sample)', 'Datastore consumer (sample)', 'Network administrator (sample)', 'No cryptography administrator', 'Resource pool administrator (sample)', 'Tagging Admin', 'Virtual Machine console user', and 'Virtual machine power user (sample)'. The status bar at the bottom says '14 items'.

1. The Roles panel shows various roles that already exist or are provided as sample to use or create your own roles from.
2. When a role clicked , the Description of the role, where the role is used and what privileges the role has is will be displayed by clicking the appropriate button.

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 one the role will need.

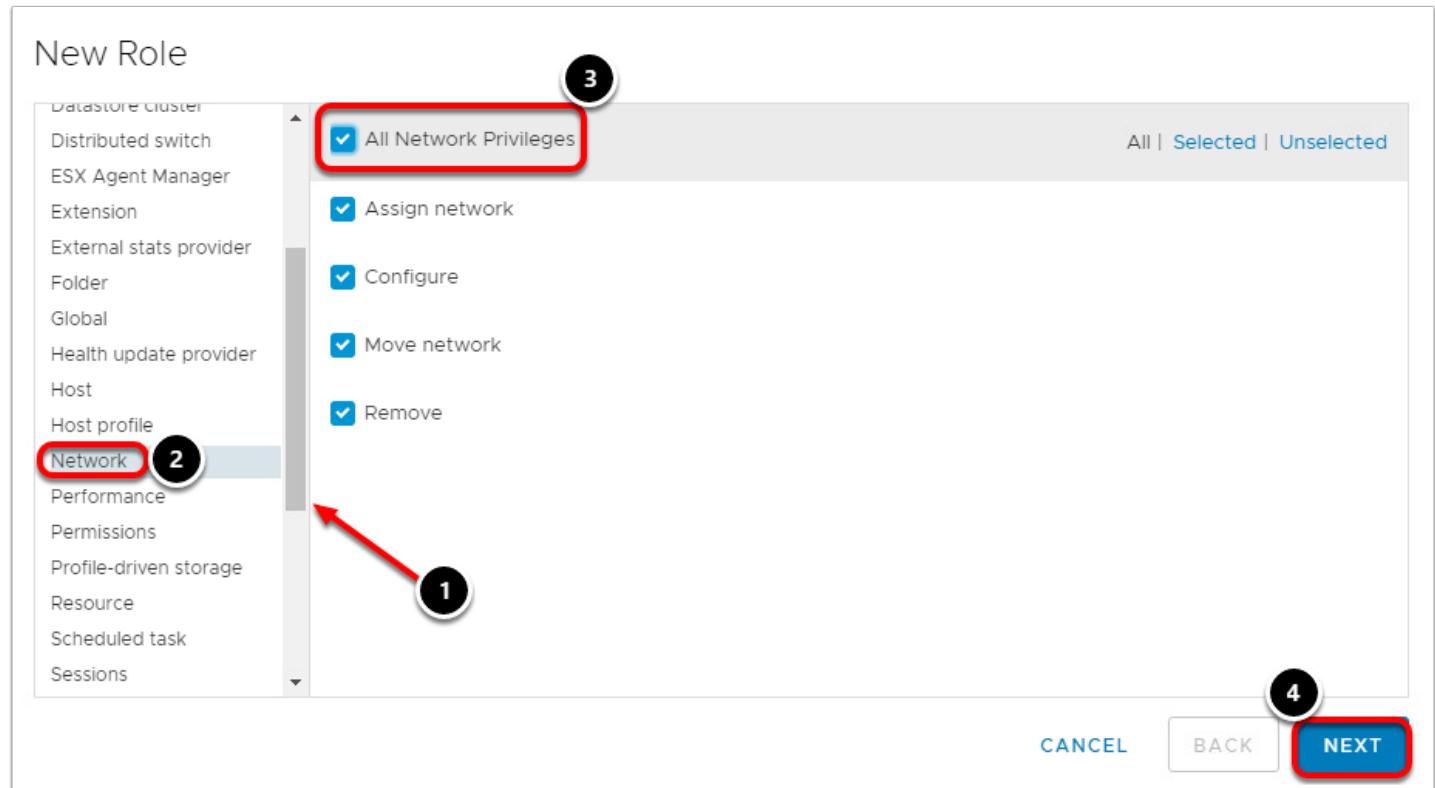
Add A Role



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

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

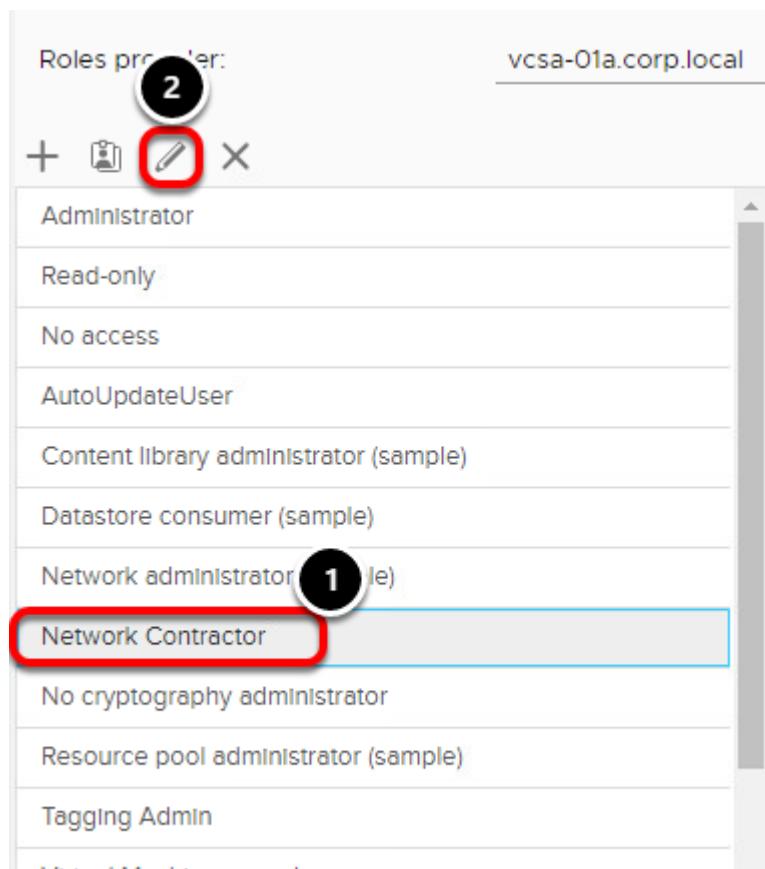
CANCEL BACK FINISH

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



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. Click on the role **Network Contractor** to select it
2. Click the **pencil** button to edit to role.

Add Permissions

Edit Role

The screenshot shows the 'Edit Role' dialog box. On the left, a sidebar lists various categories: Alarms, AutoDeploy, Certificates, Content Library, Cryptographic operations, Datacenter, Datastore, Datastore cluster, Distributed switch, ESX Agent Manager, Extension, External stats provider, Folder, Global, Health update provider, Host, and Host profile. The 'Host' category is highlighted with a red box and a circled '1'. The main pane displays 'All Host Privileges' with several checkboxes: CIM, CIM interaction, Configuration, Advanced settings, Change PciPassthru settings, Change date and time settings, Connection, Authentication Store, Change SNMP settings, Change settings, and Firmware. The 'All Host Privileges' checkbox is checked and highlighted with a red box and a circled '2'. At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons, with 'NEXT' being highlighted with a red box and a circled '3'.

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

Edit Role

Edit Role

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

1

[CANCEL](#) [BACK](#) [FINISH](#)

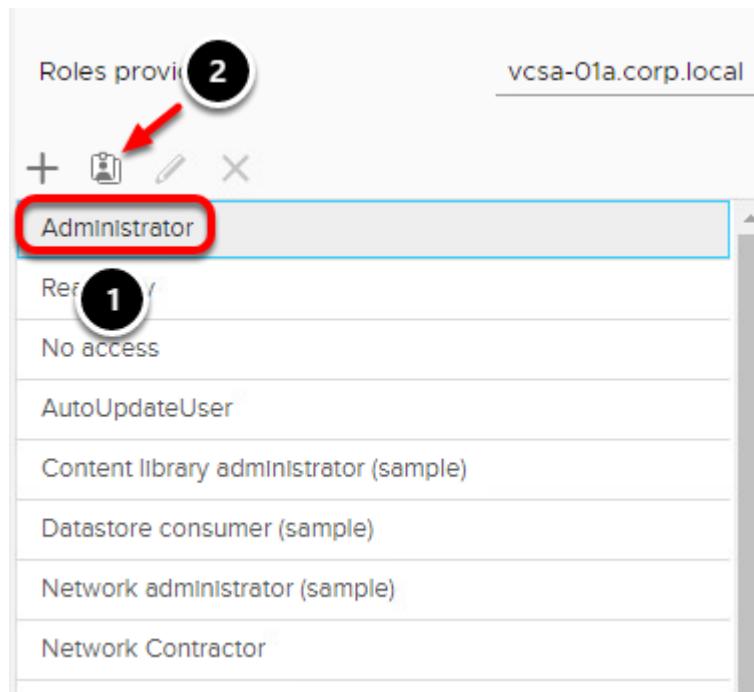
We will keep the same Role name.

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 to select it.
2. Click the **Clone** button.

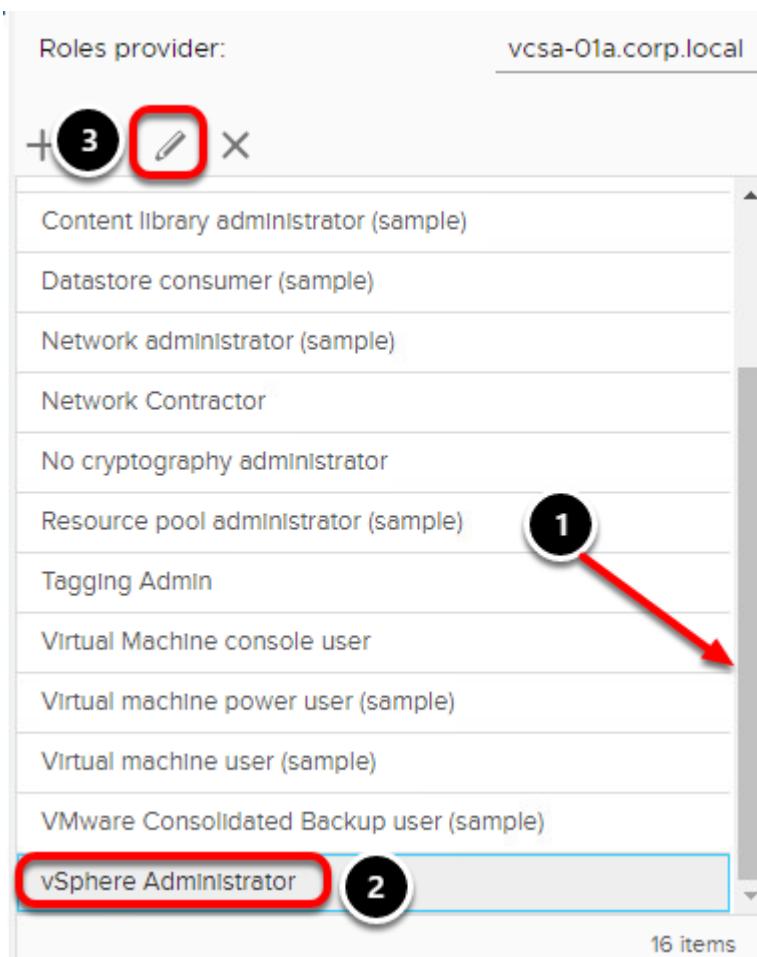
Clone Role



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.

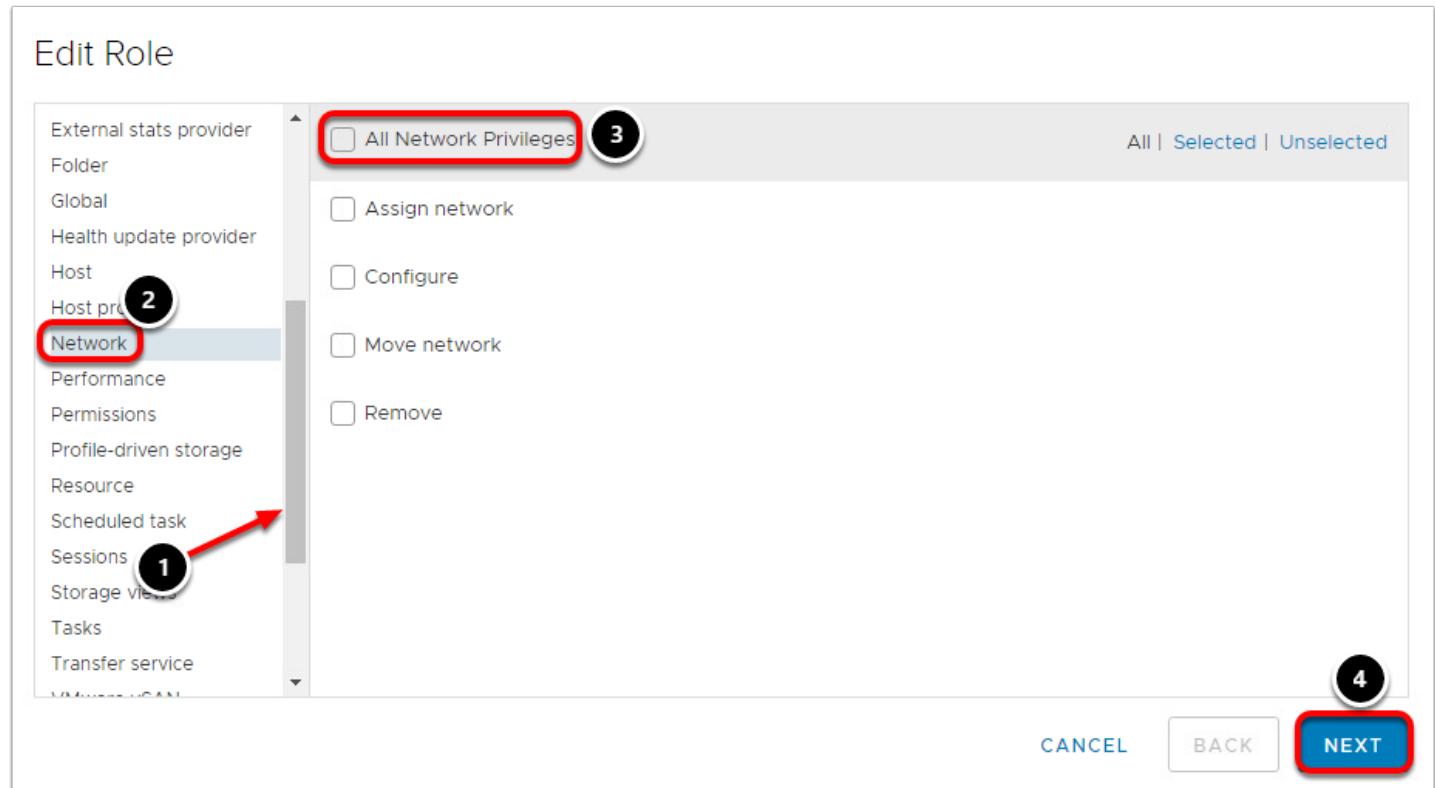
1. For the Role name, type **vSphere Administrator**.
2. In the Description field, type **Full rights to all but Networking**.
3. Click **OK**.

New Role Cloned



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

Edit Role

Role name

Description

1 1

CANCEL BACK **FINISH**

1. Keep the same role name and click the **Finish** button.

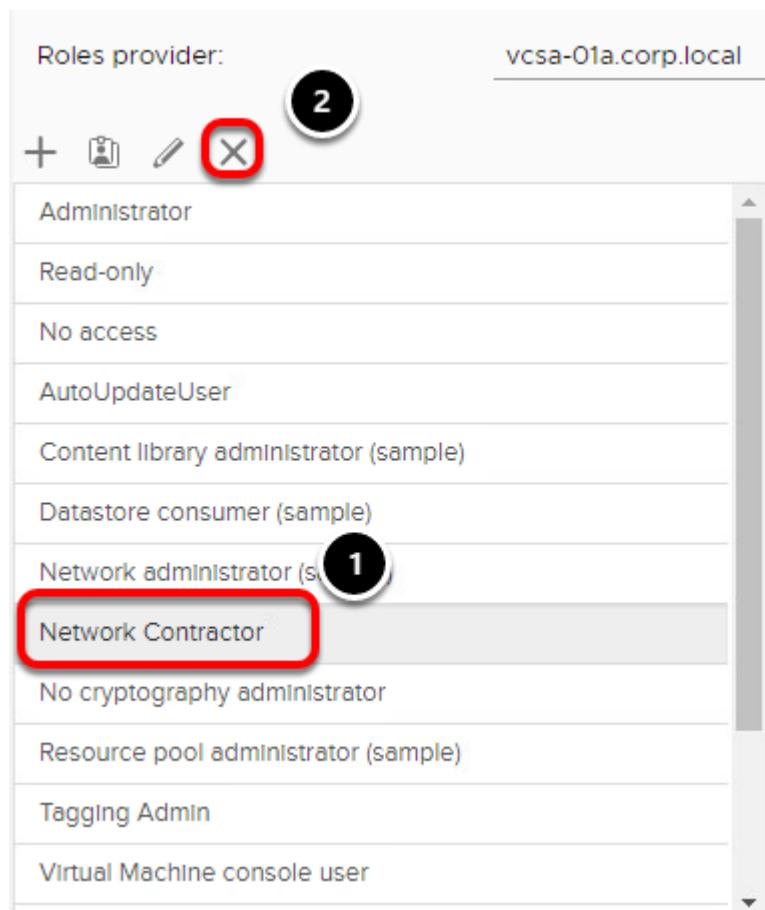
Remove a Role in the vSphere Client

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



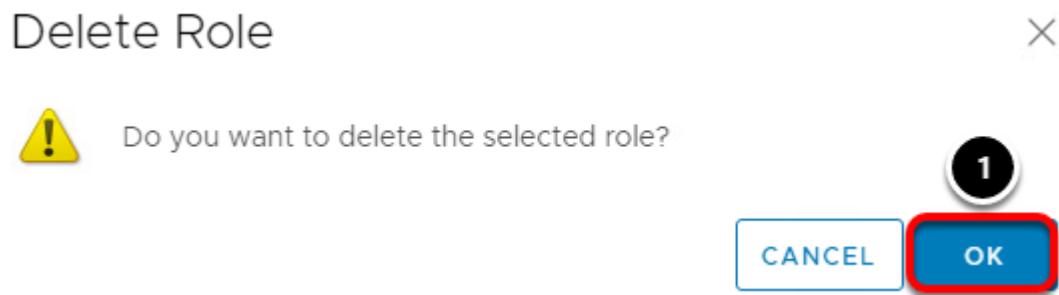
Roles provider: vcsa-01a.corp.local

+ 2

Administrator
Read-only
No access
AutoUpdateUser
Content library administrator (sample)
Datastore consumer (sample)
Network administrator (s)
Network Contractor
No cryptography administrator
Resource pool administrator (sample)
Tagging Admin
Virtual Machine console user

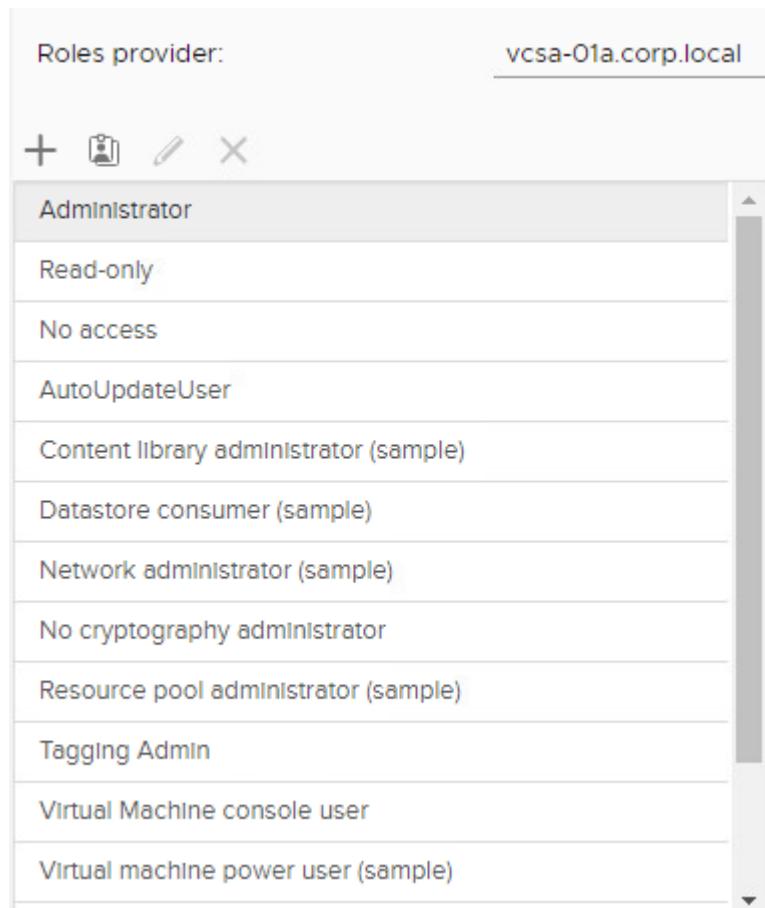
1. Click on the **Network Contractor** role to select it.
2. Click the **Delete** button.

Confirm Deletion



1. Click **OK** to confirm you want to delete this role.

Role Deleted



The screenshot shows a list of roles in a vSphere interface. The top bar indicates the 'Roles provider' is 'vcsa-01a.corp.local'. Below the provider name are four icons: a plus sign, a clipboard, a pencil, and a close button. The list of roles is as follows:

- Administrator
- Read-only
- No access
- AutoUpdateUser
- Content library administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- No cryptography administrator
- Resource pool administrator (sample)
- Tagging Admin
- Virtual Machine console user
- Virtual machine power user (sample)

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.

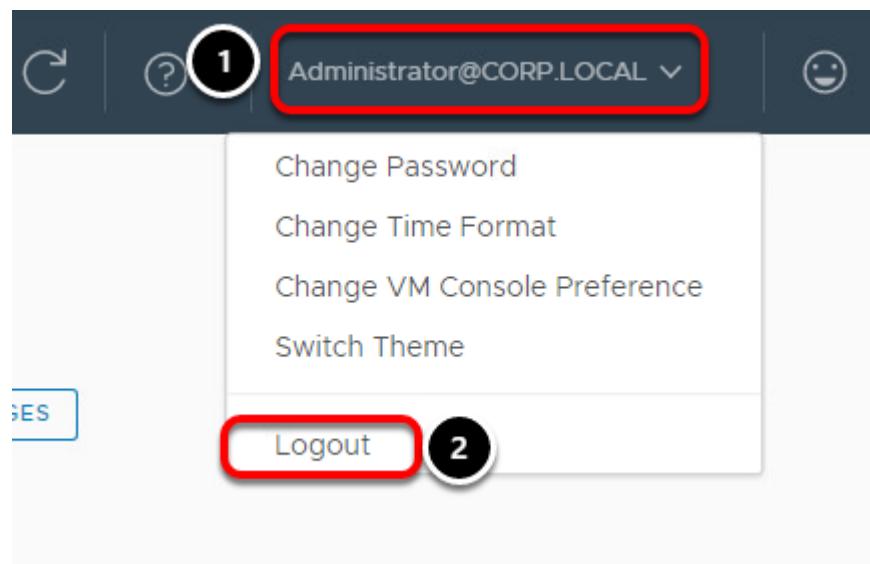
NOTE: Logging in to the vSphere Web Client with Windows session credentials is supported only for Active Directory users of the domain to which the Single Sign On system belongs.

Single Sign-On Identity Sources

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.

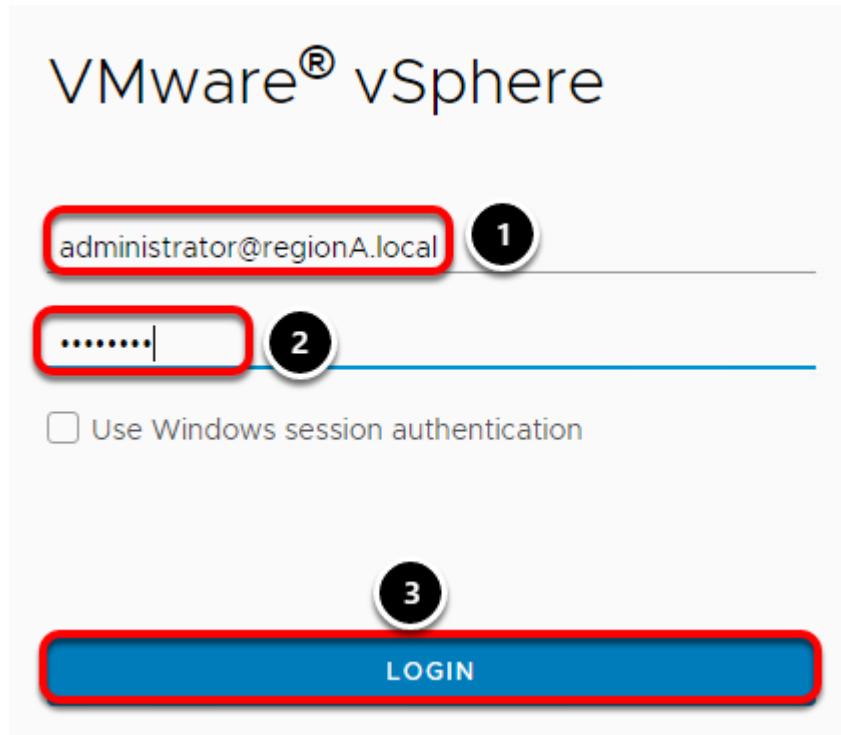
In this section, we will look at the configured Identity Sources within Single Sign-on.

Log out as Administrator@CORP.LOCAL



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

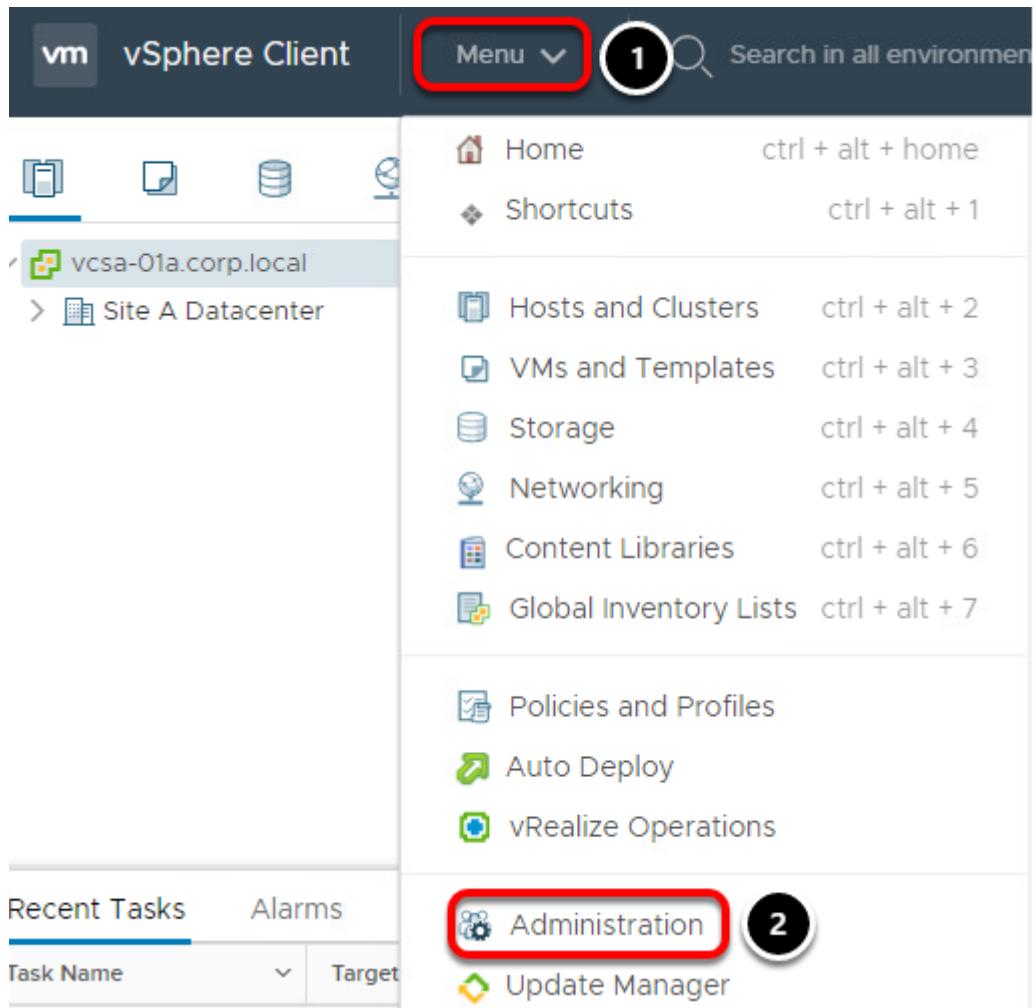


Login to the vSphere Web Client with an account which has the SSO Admin privilege:

1. Username - **administrator@regionA.local**

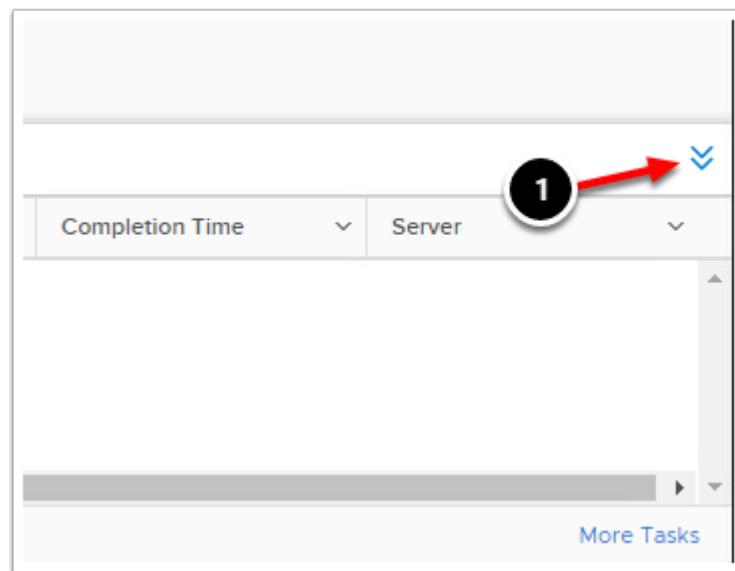
2. Password - **VMware1!**
3. Click **Login**

Navigate to Administration



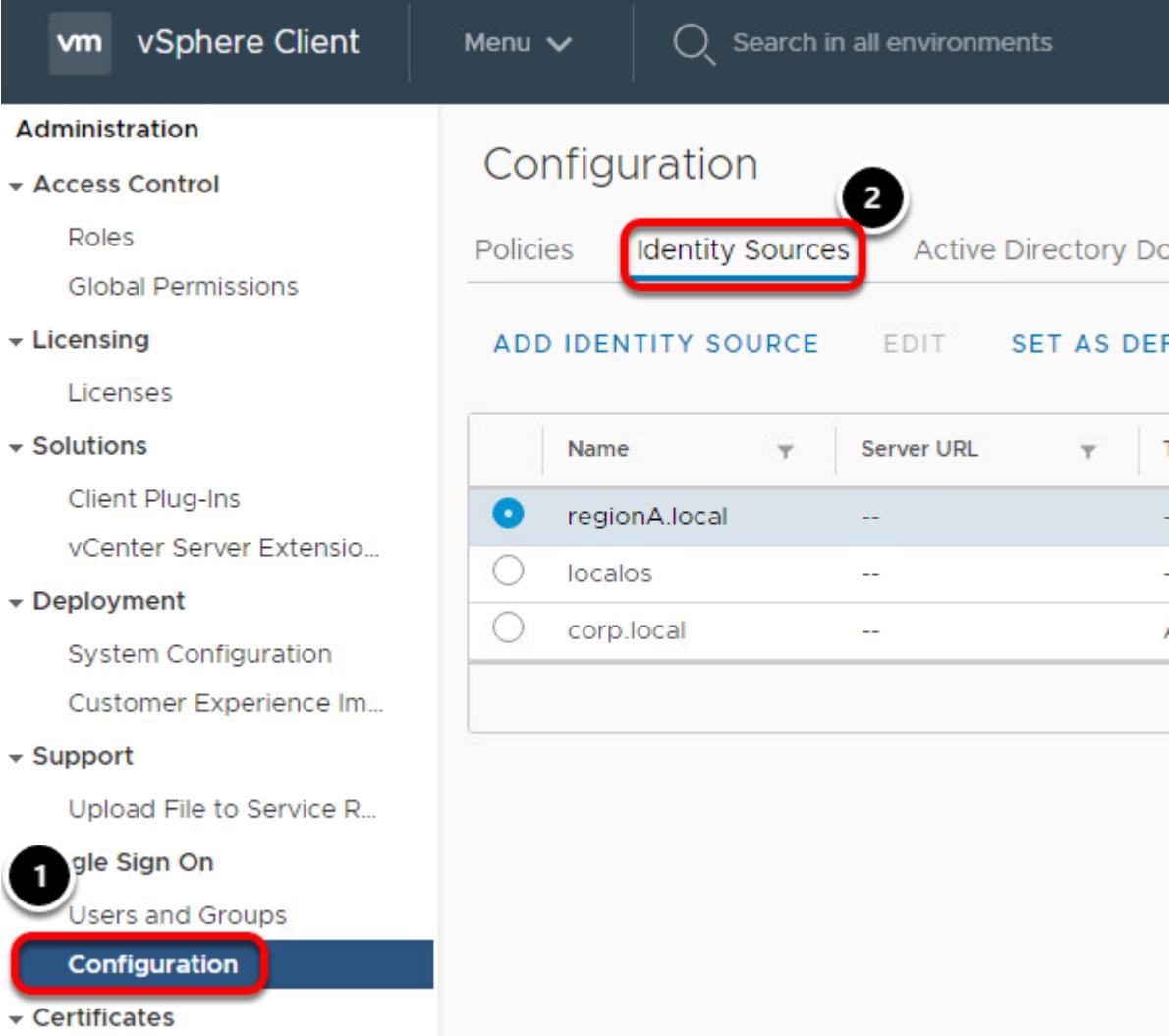
1. Click **Menu**.
2. Select **Administration**.

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 following navigation path:

- VM (selected)
- vSphere Client
- Menu
- Search in all environments

The left sidebar (Administration) includes the following sections:

- Access Control (Roles, Global Permissions)
- Licensing (Licenses)
- Solutions (Client Plug-Ins, vCenter Server Extensions)
- Deployment (System Configuration, Customer Experience Im...)
- Support (Upload File to Service R...)
- Single Sign On (1)
 - Users and Groups
 - Configuration** (highlighted with a red box)
 - Certificates

The main content area is titled "Configuration" and shows the "Identity Sources" tab (2) highlighted with a red box. The "Policies" tab is also visible. Below the tabs is a table with the following data:

Name	Server URL
regionA.local	--
localos	--
corp.local	--

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

Configuration

Policies **Identity Sources** Active Directory Domain Login Message Smart Card Authentication

ADD IDENTITY SOURCE EDIT SET AS DEFAULT REMOVE

Name	Server URL	Type	Domain	Alias
regionA.local	--		System Domain	--
localos	--		Local OS (Default)	--
corp.local	--	Active Directory (Windows Integrated Authentication)	External Domain	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, "regionA.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

Administration

- Access Control
 - Roles
 - Global Permissions
- Licensing
 - Licenses
- Solutions
 - Client Plug-Ins
 - vCenter Server Extension...
- Deployment
 - System Configuration
 - Customer Experience Im...
- Support
 - Upload File to Service R...
 - Single Sign On
 - 1 **Users and Groups**
 - Configuration
- Certificates

Users and Groups

Users **Groups**

Domain: **regionA.local** **2**

ADD USER **3**

Username	First Name	Last Name
⋮ K/M		
⋮ krbtgt/REGIONA.LOCAL		
⋮ waiter-64fc23f8-1550-4a50-91e1-784e816464cf	waiter	64fc23f8-1550-4a50-91e1-784e816464cf
⋮ Administrator	Administrator	regionA.local

1. Click on **Users and Groups** under Single Sign-On.
2. From the drop-down list, select **regionA.local** for the Domain.
3. On the Users tab, click the **Add User** icon.

Enter Properties for New User

Add User X

1

Username *	holadmin	i
Password *	*****	
Confirm Password *	*****	
First Name	HOL	
Last Name	Admin	
Email	holadmin@regionA.local	

Description

2

CANCEL ADD

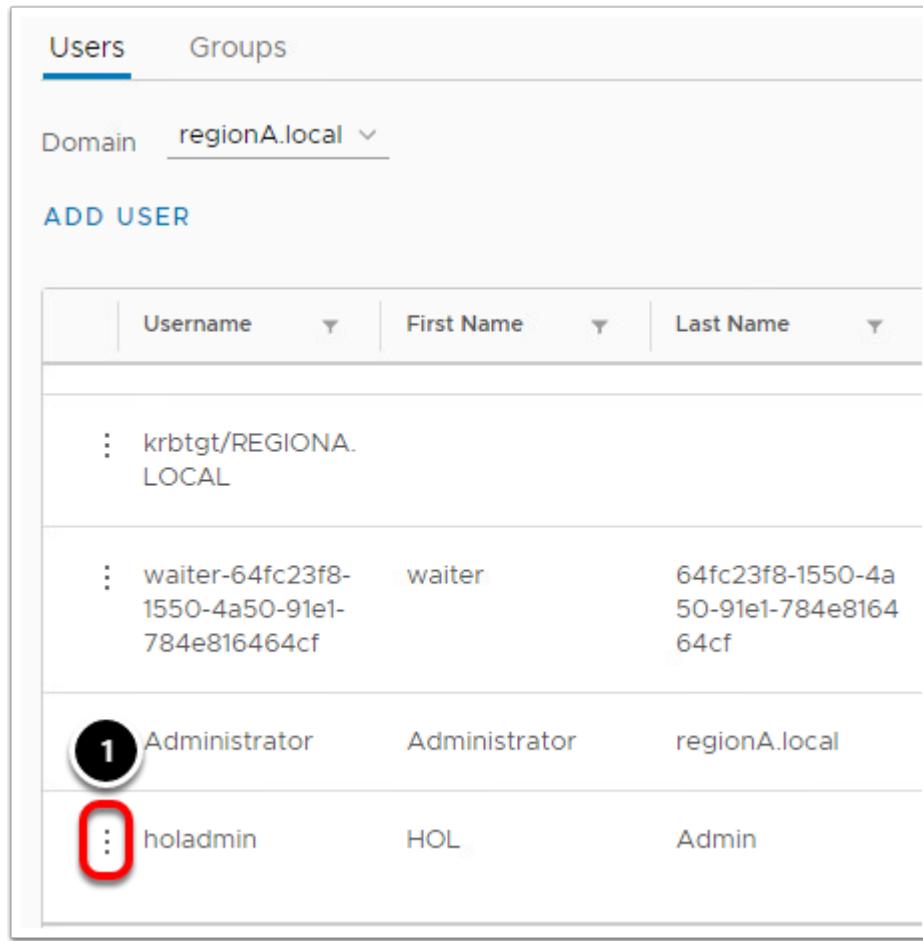
1. Fill out the New User form as follows:

- **Username:** holadmin
- **Password:** VMware1!
- **Confirm password:** VMware1!
- **First name:** HOL
- **Last name:** Admin
- **Email address:** holadmin@regionA.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



The screenshot shows the 'Users' tab in the vSphere Client. The domain is set to 'regionA.local'. The 'ADD USER' button is visible. The user list table has columns for Username, First Name, and Last Name. The data is as follows:

	Username	First Name	Last Name
1	krbtgt/REGIONA.LOCAL		
	waiter-64fc23f8-1550-4a50-91e1-784e816464cf	waiter	64fc23f8-1550-4a50-91e1-784e816464cf
	holadmin	HOL	Admin

Here we can see the new user has been added.

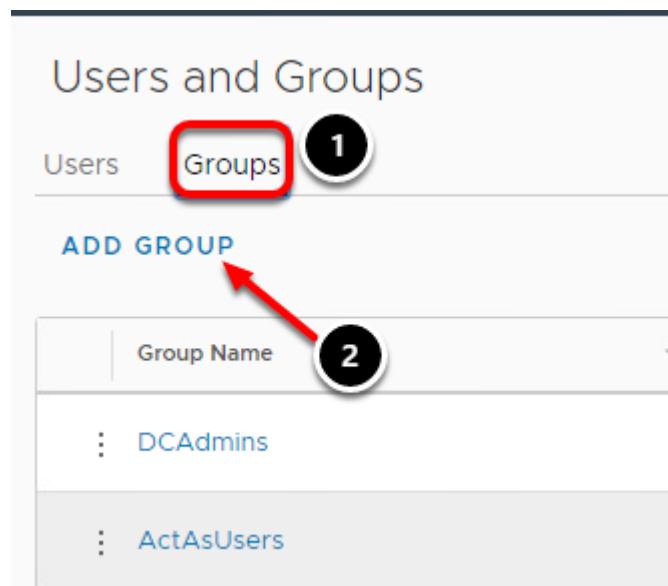
1. Clicking on the three dots next to the username, allows for editing, deleting or disabling the user.

Add a vCenter Single Sign On Group with the vSphere Client

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

Add Group

The screenshot shows a 'Add Group' form with the following steps:

- 1** Group Name (The input field is highlighted with a red box.)
- 2** Add Members (The input field is highlighted with a red box.)
- 3** A dropdown menu is open, showing a list of users. The user 'holadmin' is selected and highlighted with a red box. A red arrow points from step 3 to the 'holadmin' entry in the list.
- 4** At the bottom right, there are two buttons: 'CANCEL' (white background) and 'ADD' (blue background, highlighted with a red box).

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

ADD GROUP		
Group Name	Description	
⋮ SolutionUsers	Well-known solution users' group, which contains all solution users as members.	
⋮ SystemConfiguration.BashShellAdministrators	Access bash shell and manage local users on nodes	
⋮ SyncUsers	Sync Users	
⋮ ComponentManager.Administrators	Component Manager Administrators	
⋮ HOL Group		

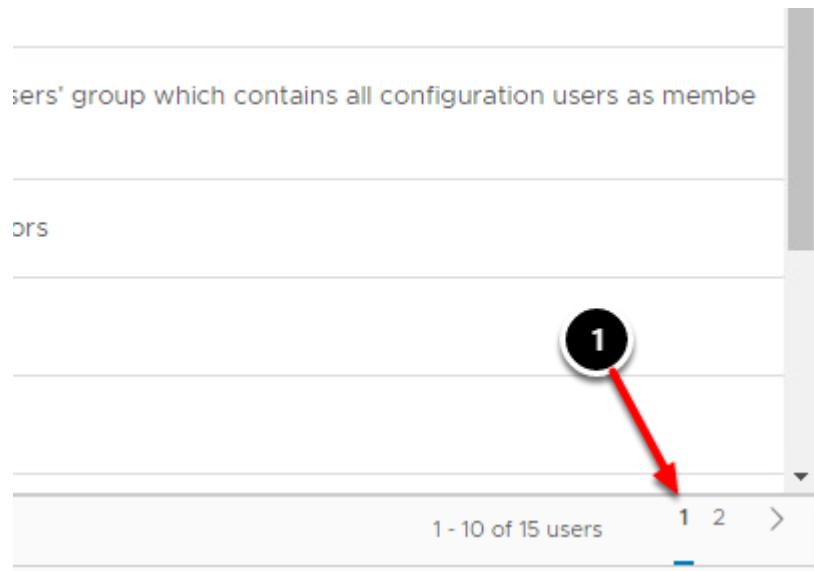
11 - 15 of 15 users < 1 2

1. Click on the **2** to move to the second 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 1



1. Click on 1 to return to the first page of Groups.

Add Members to Users and Groups

A screenshot of the 'Add Members to Users and Groups' page. The 'Groups' tab is selected. The page shows a list of groups with the following details:

Group Name	Description
LicenseService Administrators	License Service Administrators
CAAdmins	
DCClients	
Administrators	1
Users	
ExternalIDPUsers	Well-known external IDP users' group
AutoUpdate	Users allowed to perform update rel

A red box highlights the 'Administrators' group, and a red arrow points from the text 'Click on Administrators to return to the first page of Groups.' to the 'Administrators' entry in the list, which is also enclosed in a black circle.

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 'Users and Groups' interface. The 'Groups' tab is selected. A link to 'ALL GROUPS' is visible. The 'Administrators' group is selected, indicated by a circled '1'. The 'ADD MEMBERS' button is highlighted with a red box and circled '1'. The table below lists members of the Administrators group, showing two entries: 'Administrator' from 'corp.local' and 'Administrator' from 'regionA.local'.

Member Name	Domain
Administrator	corp.local
Administrator	regionA.local

The Administrator account for the regionA.local and corp.local domains are members.

1. Click **Add Members**.

Edit Group

Edit Group

Group Name *

Administrators

Description

Add Members *

regionA.local

HOL Gr

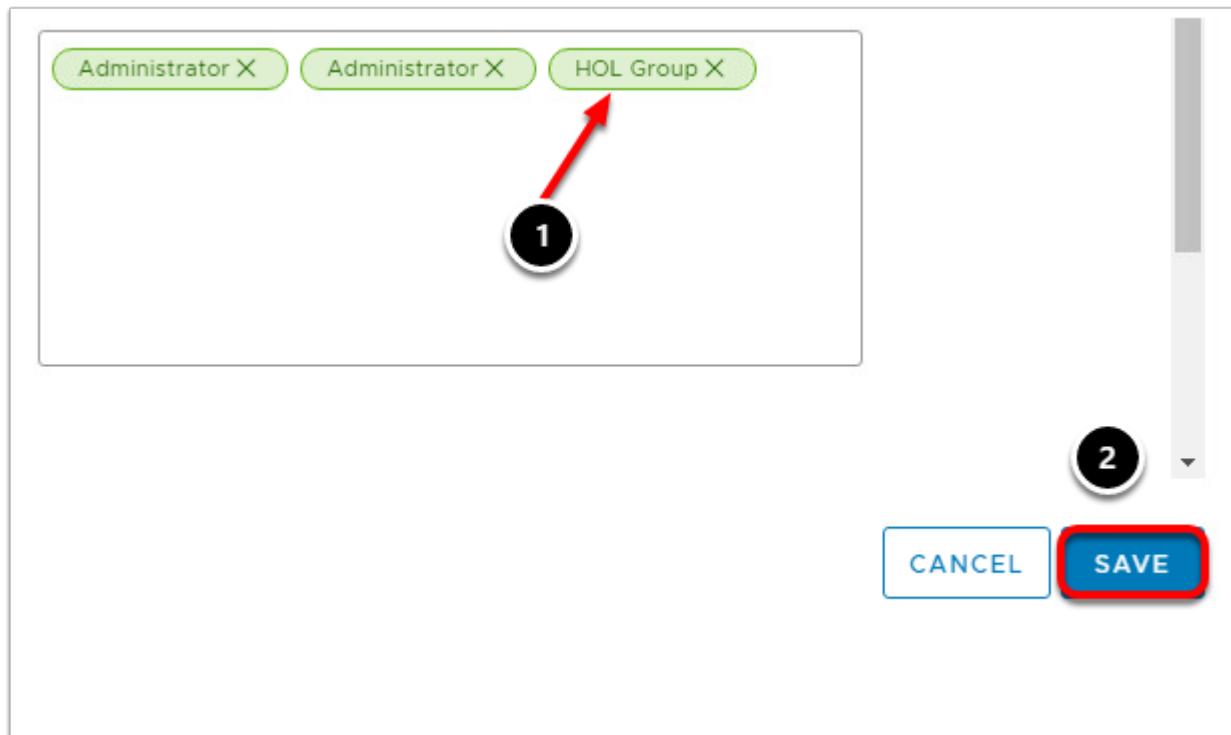
HOL Group

1

2

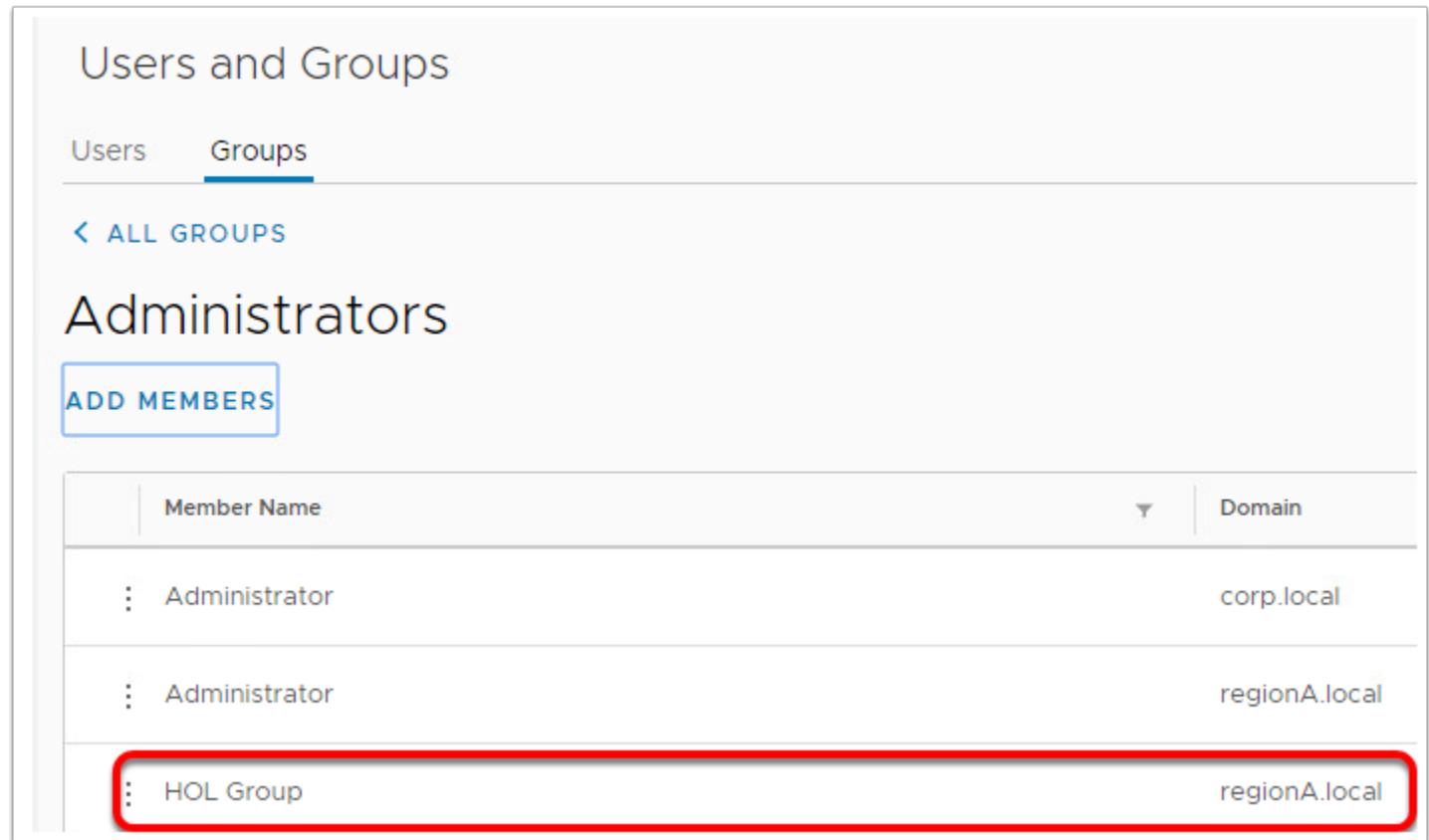
3

1. Make sure the domain selected is **regionA.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

Users Groups

ALL GROUPS

Administrators

ADD MEMBERS

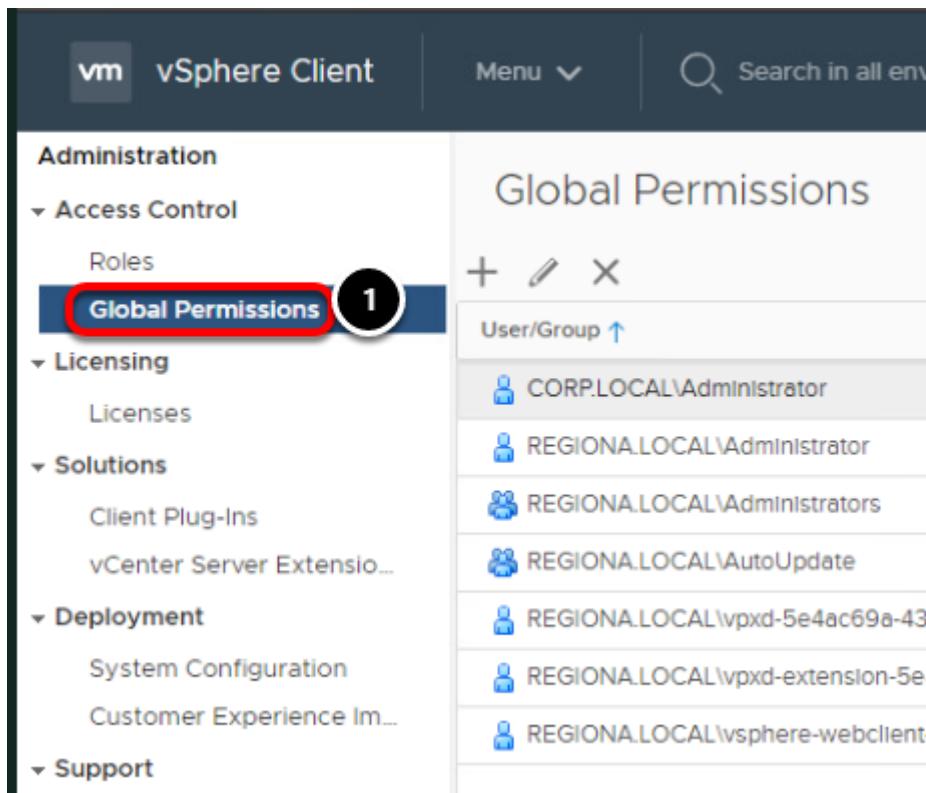
Member Name	Domain
Administrator	corp.local
Administrator	regionA.local
HOL Group	regionA.local

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

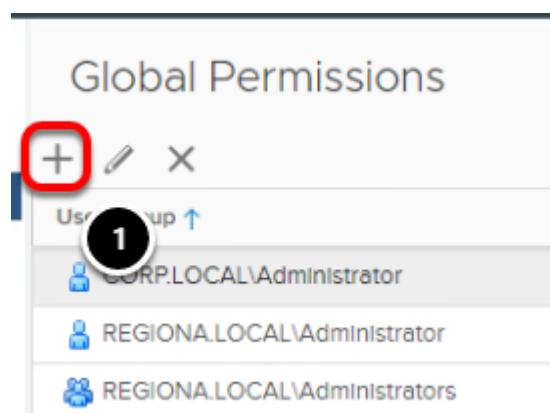


The screenshot shows the vSphere Client interface. The left sidebar has a tree structure with categories like Administration, Access Control, Licensing, Solutions, Deployment, and Support. Under Access Control, the 'Global Permissions' item is highlighted with a red box and a circled '1'. The main pane is titled 'Global Permissions' and lists several entries under 'User/Group ↑': CORP.LOCAL\Administrator, REGIONA.LOCAL\Administrator, REGIONA.LOCAL\Administrators, REGIONA.LOCAL\AutoUpdate, REGIONA.LOCAL\vpdx-5e4ac69a-431, REGIONA.LOCAL\vpdx-extension-5e4, and REGIONA.LOCAL\vsphere-webclient-. The 'User/Group ↑' label has an upward arrow icon.

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

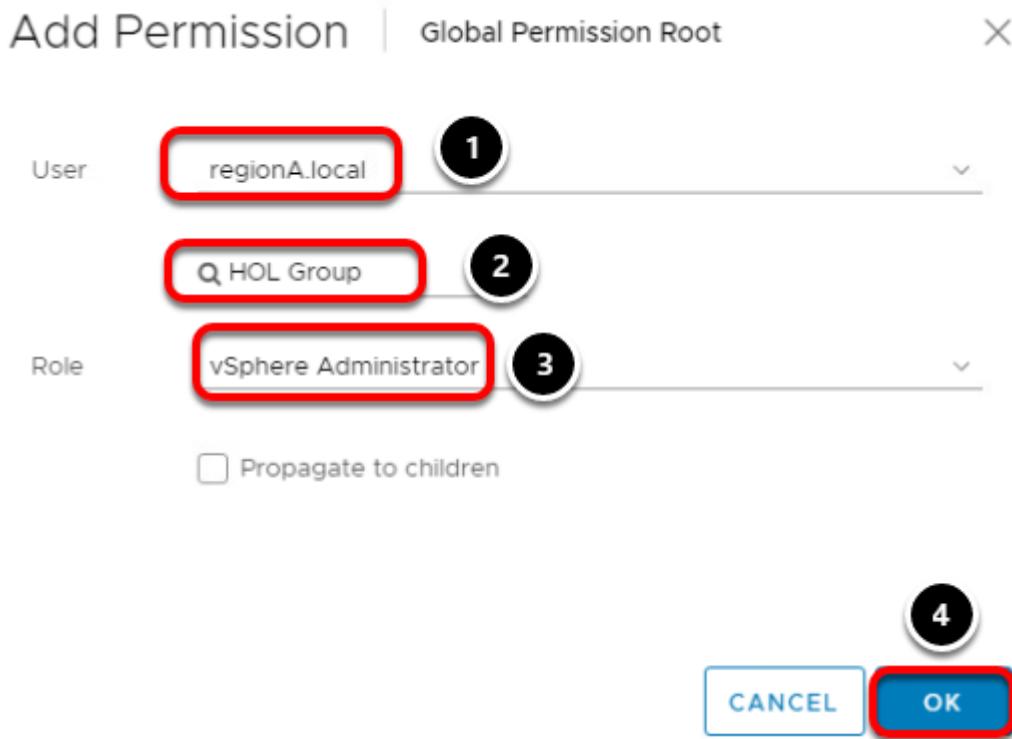


The screenshot shows the 'Global Permissions' list with the '+' button highlighted with a red box and a circled '1'. The list includes the same entries as the previous screenshot: CORP.LOCAL\Administrator, REGIONA.LOCAL\Administrator, REGIONA.LOCAL\Administrators, REGIONA.LOCAL\AutoUpdate, REGIONA.LOCAL\vpdx-5e4ac69a-431, REGIONA.LOCAL\vpdx-extension-5e4, and REGIONA.LOCAL\vsphere-webclient-.

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 (+) to open the Add New Permission window
2. Click the **Add...** button

Locate the HOL Group



1. Ensure that the **regionA.local** domain is selected.
2. Type **HOL Group** in the search field.
3. For the Role, select the **vSphere Administrator** group.
4. Click the **OK** button.

New Global Permission

Global Permissions			
User/Group	Role	Defined In	
CORP.LOCAL\Administrator	Administrator	Global Permission	
REGIONA.LOCAL\Administrator	Administrator	Global Permission	
REGIONA.LOCAL\Administrators	Administrator	Global Permission	
REGIONA.LOCAL\AutoUpdate	AutoUpdateUser	Global Permission	
REGIONA.LOCAL\HOL Group	vSphere Administrator	Global Permission	
REGIONA.LOCAL\vpxd-5e4ac69a-43f8-4166-ab80-75e36d9d93bd	Administrator	Global Permission	
REGIONA.LOCAL\vpxd-extension-5e4ac69a-43f8-4166-ab80-75e3...	Administrator	Global Permission	
REGIONA.LOCAL\vsphere-webclient-5e4ac69a-43f8-4166-ab80-7...	Read-only	Global Permission	

1. The newly created 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.

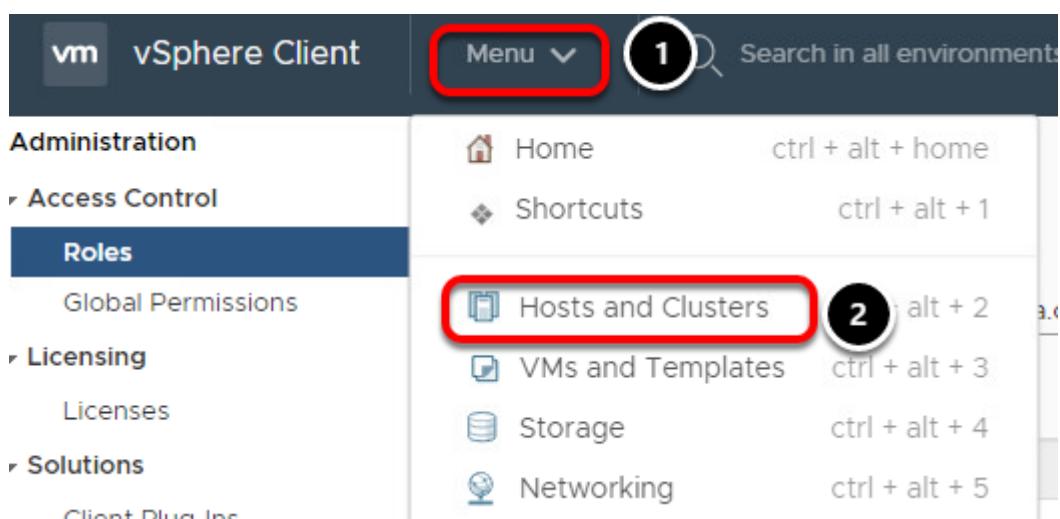
Adding an ESXi Host to Active Directory

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

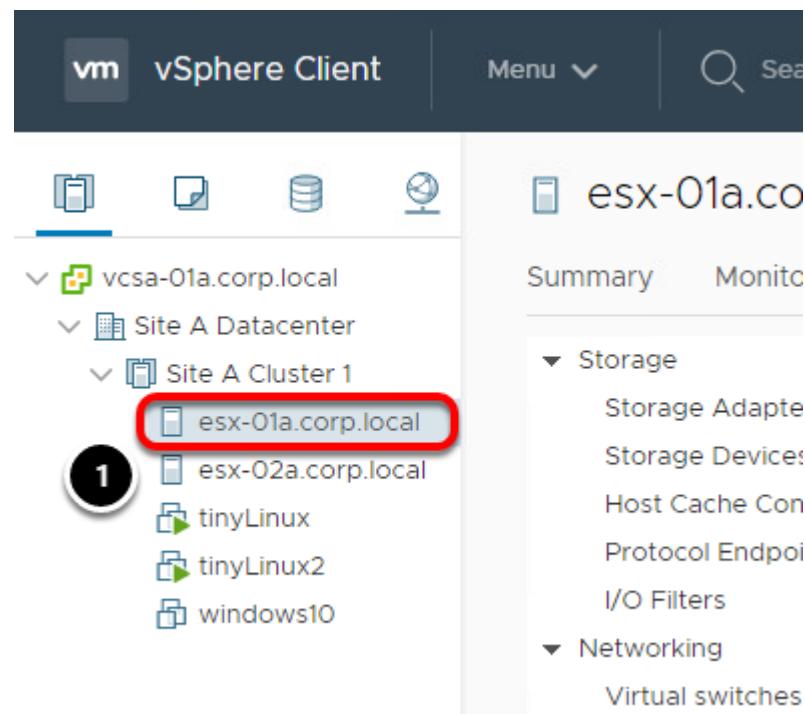
In this lesson, we walk through the process of adding a vSphere Host to authenticate against Active Directory.

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

The screenshot shows the vSphere Web Client interface for managing a host named 'esx-01a.corp.local'. The 'Configure' tab is highlighted with a red box and a black circle containing the number 1. In the 'Networking' section of the left sidebar, the 'TCP/IP configuration' item is highlighted with a red box and a black circle containing the number 2. The main content area is titled 'TCP/IP Configuration' and contains a table with three rows: 'Default' (System stack), 'Provisioning' (System stack), and 'vMotion' (System stack).

TCP/IP Stack	Type	VMkernel...
Default	System stack	2
Provisioning	System stack	0
vMotion	System stack	1

1. Click on the **Configure** tab.
2. Select the **TCP/IP configuration** in the Networking section.

Edit Default System Stack

The screenshot shows the 'Edit Default System Stack' dialog. The 'Edit...' button is highlighted with a red box and a black circle containing the number 2. The 'Default' stack is selected in the list, highlighted with a red box and a black circle containing the number 1. The table shows three stacks: 'Default' (System stack, ID 2), 'Provisioning' (System stack, ID 0), and 'vMotion' (System stack, ID 1).

TCP/IP Stack	Type	VMkernel...
Default	System stack	2
Provisioning	System stack	0
vMotion	System stack	1

TCP/IP Stack: Default

1. Click on **Default** under System stacks
2. Click the **Pencil Icon** to edit the stack.

DNS configuration

- Obtain settings automatically from a VMkernel network adapter

VMkernel network adapter

- Enter settings manually

Host name

esx-01a

Domain

corp.local

1

Preferred DNS server

192.168.110.10

Alternate DNS server

Search domains

corp.local

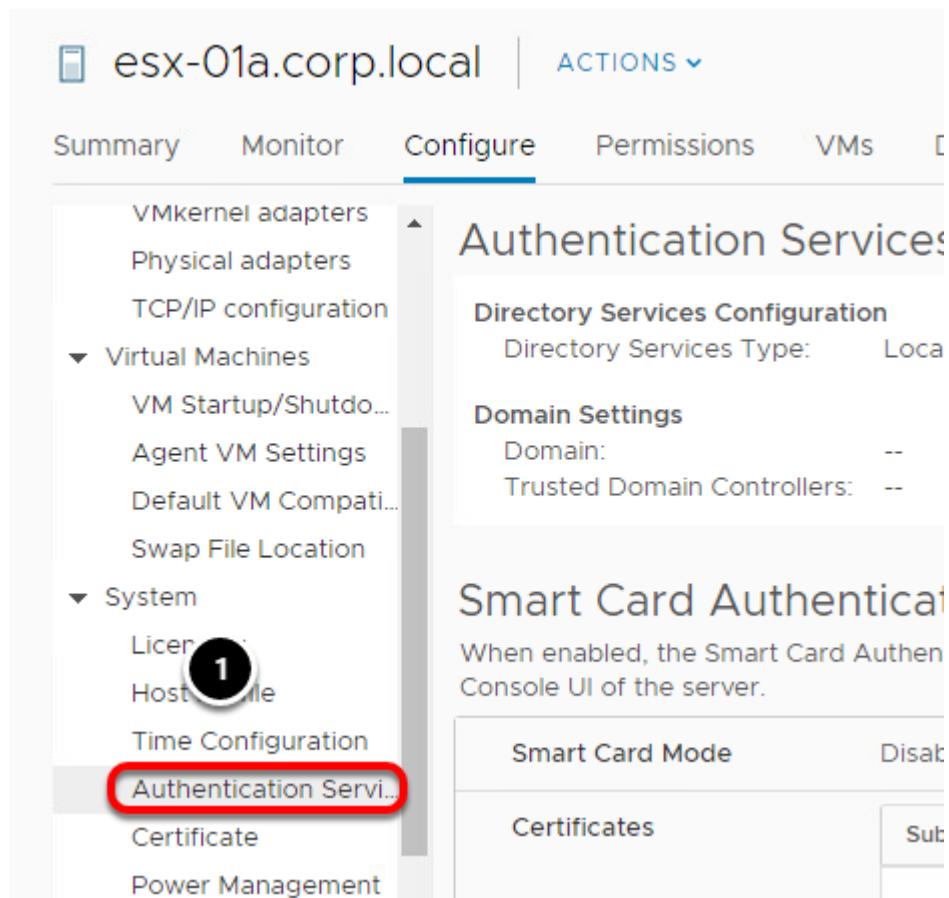
2

CANCEL

OK

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

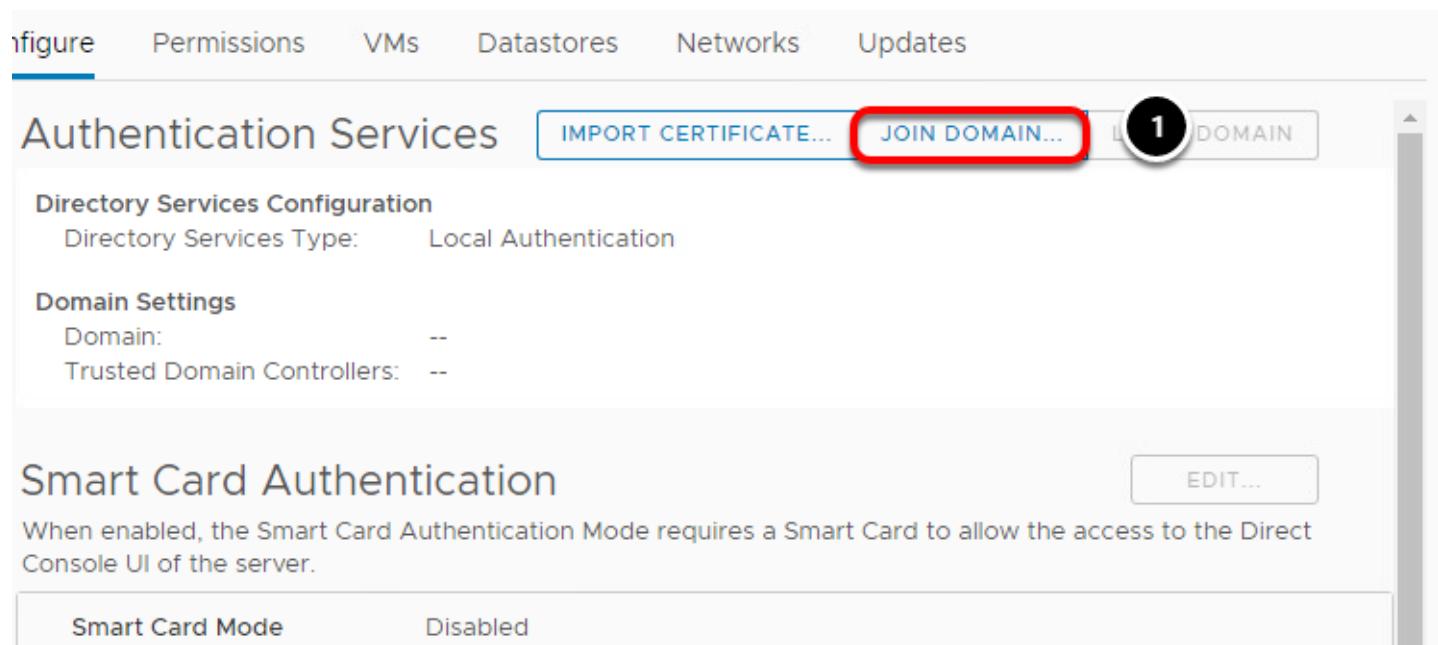


The screenshot shows the vSphere Client interface for a host named 'esx-01a.corp.local'. The 'Configure' tab is selected. On the left, a navigation tree shows 'Virtual Machines' and 'System' sections. In the 'System' section, the 'Authentication Service...' option is highlighted with a red box and a circled '1'. The main content area displays the 'Authentication Services' configuration, including 'Directory Services Configuration' (set to 'Local') and 'Domain Settings' (Domain and Trusted Domain Controllers both set to '--'). Below this is a section for 'Smart Card Authentication'.

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



The screenshot shows the 'Join Domain' button highlighted with a red box and the number '1' in a circle. The 'JOIN DOMAIN...' button is located in the top right corner of the 'Authentication Services' section.

Authentication Services

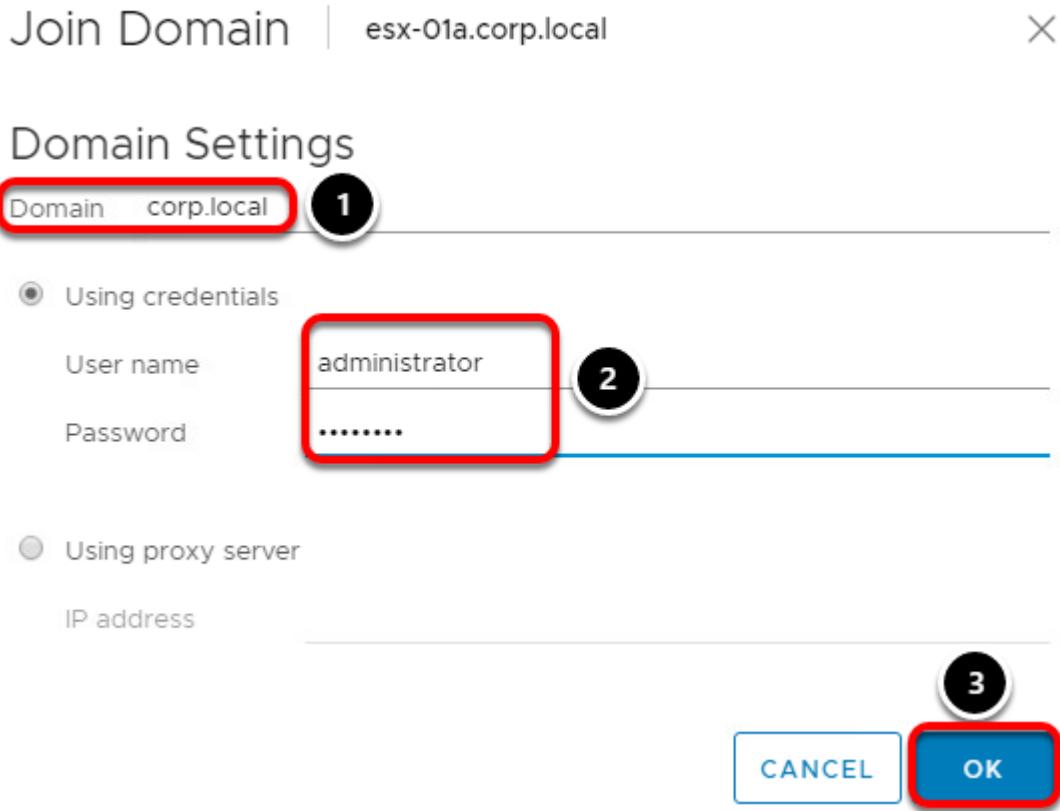
Directory Services Configuration
Directory Services Type: Local Authentication

Domain Settings
Domain: --
Trusted Domain Controllers: --

Smart Card Authentication
When enabled, the Smart Card Authentication Mode requires a Smart Card to allow the access to the Direct Console UI of the server.
Smart Card Mode: Disabled

1. Click the **Join Domain** button.

Join Domain Settings



The screenshot shows the 'Join Domain Settings' dialog box. Step 1 highlights the 'Domain' field with 'corp.local'. Step 2 highlights the 'User name' field with 'administrator'. Step 3 highlights the 'OK' button.

Join Domain | esx-01a.corp.local

Domain Settings

Domain: corp.local (1)

Using credentials (radio button selected):

- User name: administrator (2)
- Password: (2)

Using proxy server (radio button):

IP address: _____

CANCEL OK (3)

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	Initiator
List Smart Card Trust Anchors	esx-01a.corp.lo...	0%	CORP\Ad
Join Windows Domain	esx-01a.corp.lo...	0%	CORP\Ad
List Smart Card Trust	esx-01a.corp.lo...	Completed	CORP\Ad

Progress can be monitored using the Recent Tasks window. It should take a minute or two to complete.

Added to Active Directory

esx-01a.corp.local | ACTIONS ▾

Summary Monitor **Configure** Permissions VMs Datastores Networks

VMkernel adapters
Physical adapters
TCP/IP configuration
Virtual Machines
VM Startup/Shutdo...
Agent VM Settings
Default VM Compati...
Swap File Location
System
Licensing
Host Profile

Authentication Services IMPORT CERTIFICATE...

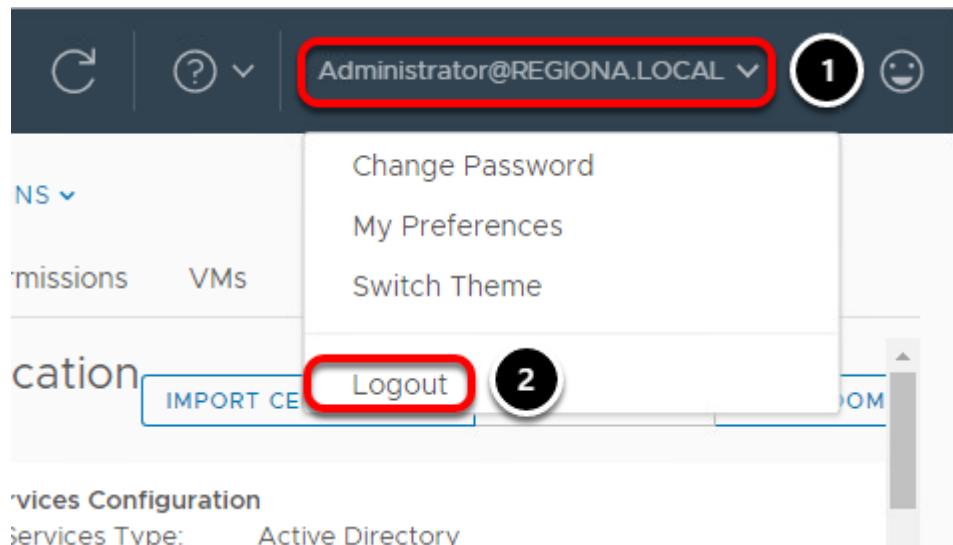
Directory Services Configuration
Directory Services Type: Active Directory

Domain Settings
Domain: CORP.LOCAL
Trusted Domain Controllers:

Smart Card Authentication
When enabled, the Smart Card Authentication Mode requires a Smart Console UI of the server.

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@regionA.local.

1. Click **Administrator@REGIONA.LOCAL**.
2. Click **Logout**.

Conclusion

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 \(60 Minutes\)](#)

Module 3 - Introduction to vSphere Storage (60 Min)

vSphere Storage Overview

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.

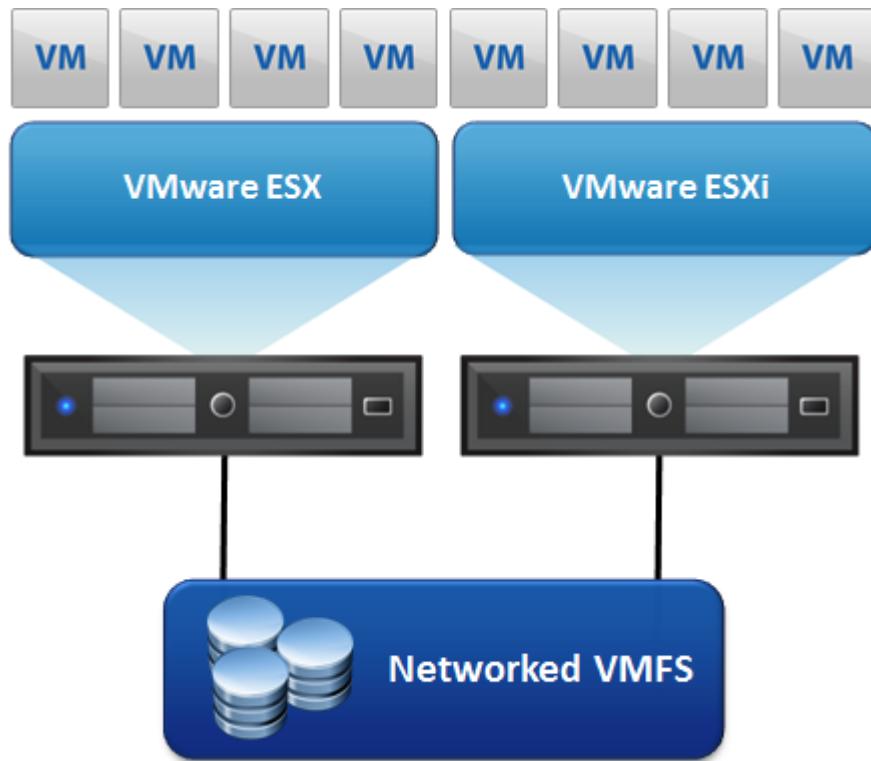
Local Storage



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.

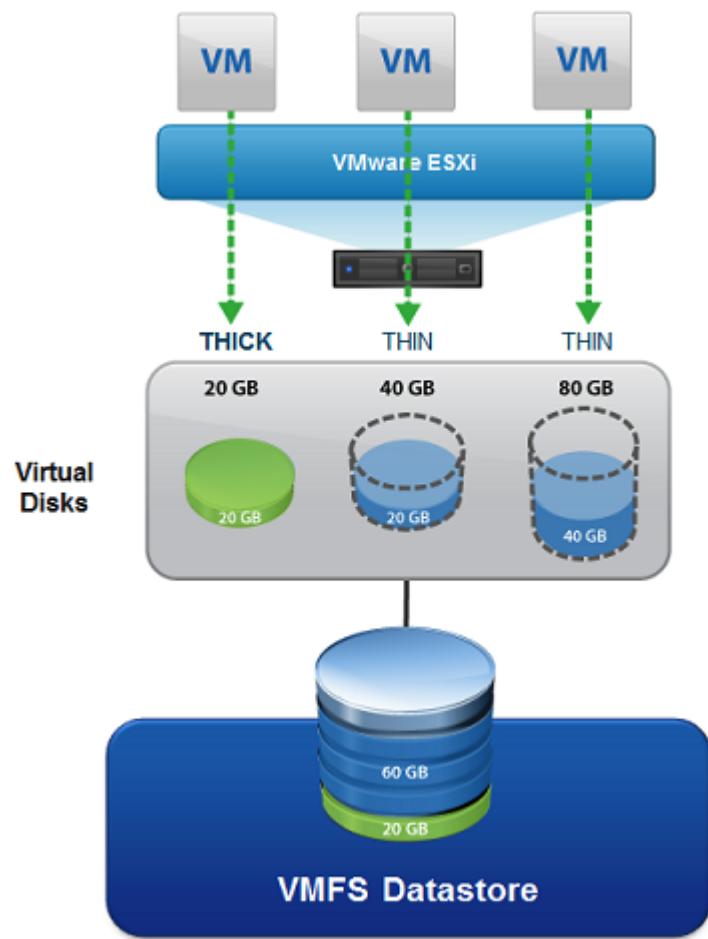
Networked Storage



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

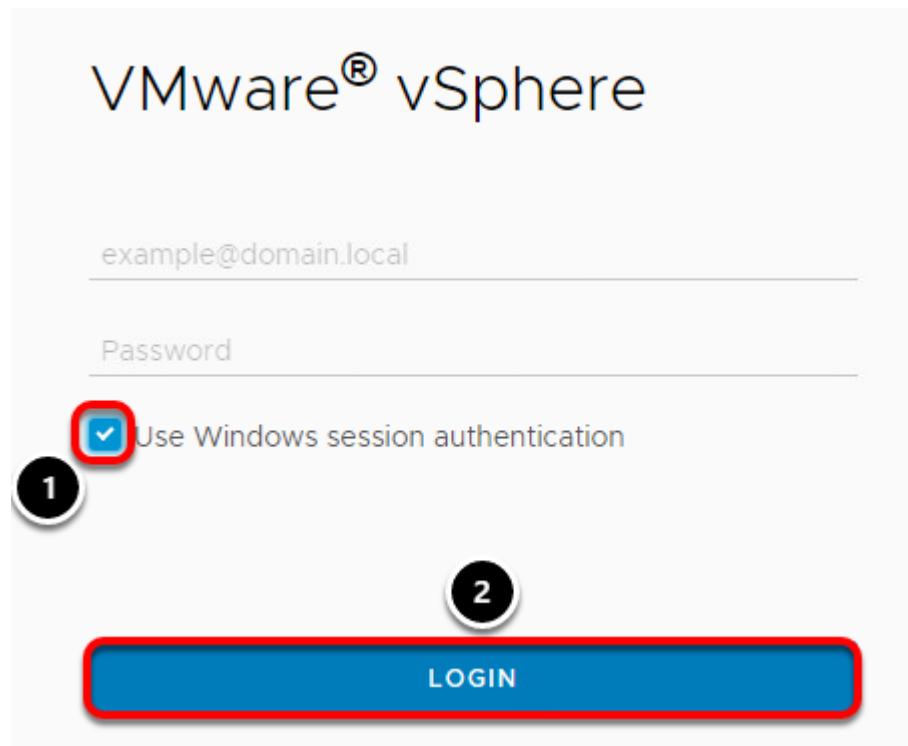
This lesson will walk you through creating and configuring an NFS, and an iSCSI vSphere Datastore. Also adding and configuring an iSCSI software adapter.

Launch Google Chrome web browser

1. Select **Google Chrome** from the Main Console desktop



Enter credentials and log in

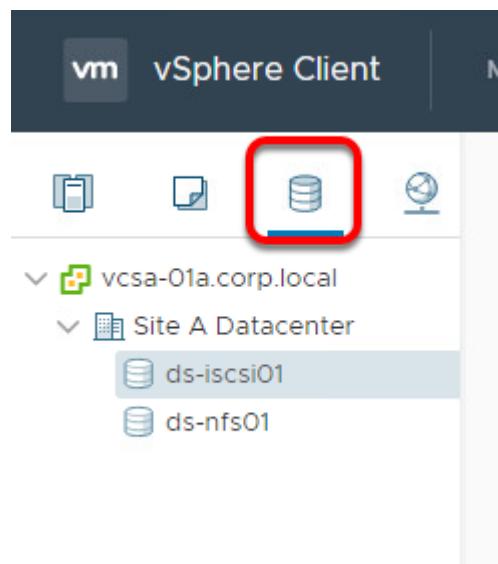


Note: Selecting "Use Windows session authentication" will pass the same credentials as entering them as username "CORP\Administrator" and password "VMware1!"

1. Select **Use Windows session authentication**

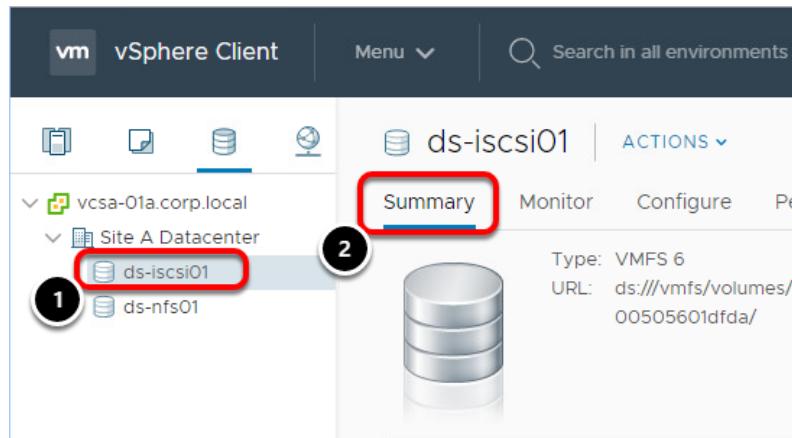
2. Select **Login**

Navigate to Storage Management



1. Select the **Storage** tab.

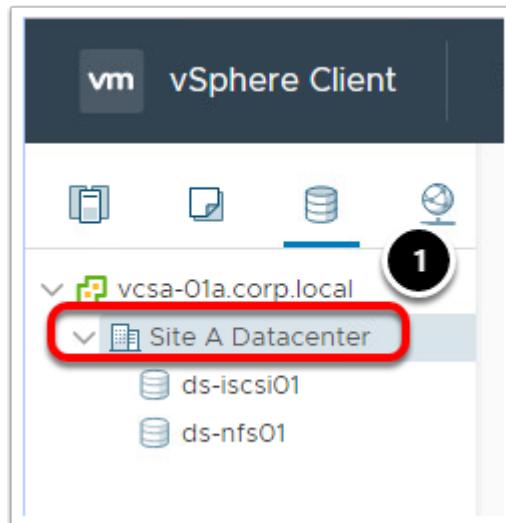
Expand Site A Datacenter



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.

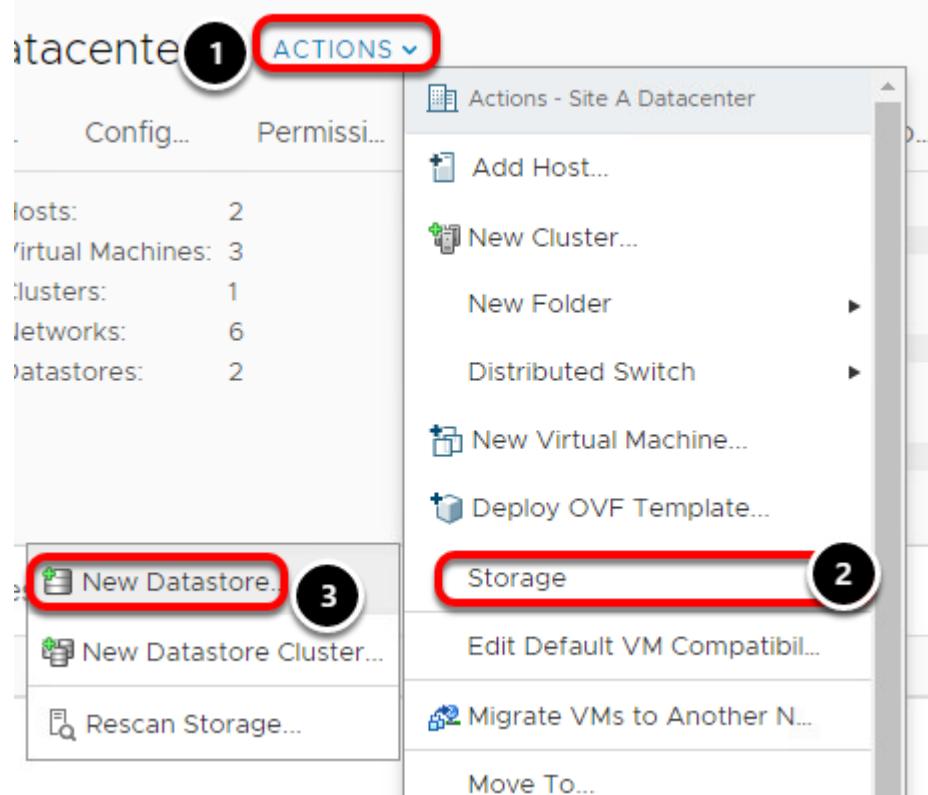
Create a vSphere NFS Datastore



In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select **Site A 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

New Datastore

1 Type

2 Select NFS version
3 Name and configuration
4 Host accessibility
5 Ready to complete

Type
Specify datastore type.

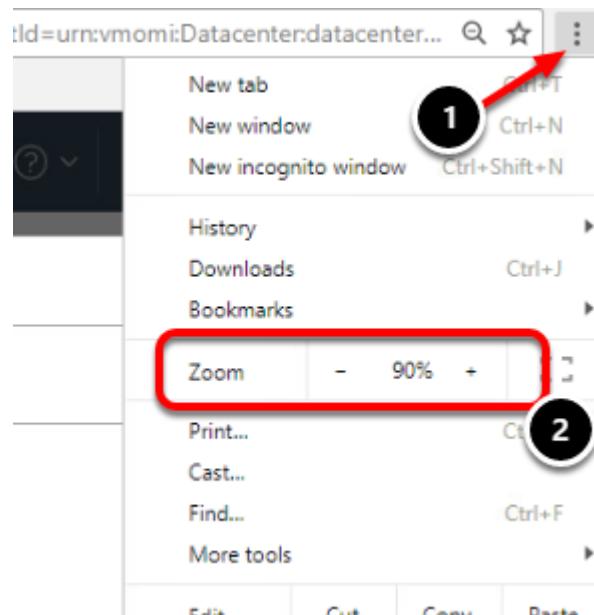
VMFS
Create a VMFS datastore on a disk/LUN. 1

NFS
Create an NFS datastore on an NFS share over the network. 2

VVol
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

CANCEL BACK **NEXT**

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

✓ 1 Type
2 Select NFS version

3 Name and configuration
 4 Host accessibility
 5 Ready to complete

1

Select NFS version

NFS Version

NFS 3
 NFS 3 allows the datastore to be accessed by ESX/ESXi hosts of version earlier than 6.0

NFS 4.1
 NFS 4.1 provides multipathing for servers and supports the Kerberos authentication protocol

2

CANCEL BACK **NEXT**

New Datastore - Name and configuration

New Datastore

- ✓ 1 Type
- ✓ 2 Select NFS version
- 3 Name and configuration**
- 4 Host accessibility
- 5 Ready to complete

Name and configuration
Specify name and configuration.

① If you plan to configure an existing datastore on new hosts in the datacenter, it is recommended to use the "Mount to additional hosts" action from the datastore instead. X

NFS Share Details

Datastore name: **ds-nfs02** 1
Folder: **/mnt/NFS02** 2
Server: **10.10.20.60** 3
E.g: /vols/vol0/ds-nfs01

Access Mode

Mount NFS as read-only

CANCEL

BACK

NEXT

4

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

New Datastore

- ✓ 1 Type
- ✓ 2 Select NFS version
- ✓ 3 Name and configuration
- 4 Host accessibility**

5 Ready to complete

1

Host accessibility

Select the hosts that require access to the datastore.

	Host	Cluster
<input checked="" type="checkbox"/>	esx-01a.corp.local	Site A Cluster 1
<input checked="" type="checkbox"/>	esx-02a.corp.local	Site A Cluster 1

2

2 items

[CANCEL](#)[BACK](#)[NEXT](#)

1. Select the **check box** to include all hosts.
2. Click **Next**.

New Datastore - Ready to complete

New Datastore

- ✓ 1 Type
- ✓ 2 Select NFS version
- ✓ 3 Name and configuration
- ✓ 4 Host accessibility

5 Ready to complete

Ready to complete

Review your settings selections before finishing the wizard.

General

Name: ds-nfs02
Type: NFS 3

NFS settings

Server: 10.10.20.60
Folder: /mnt/NFS02
Access Mode: Read-write

Hosts that will have access to this datastore

Hosts: esx-01a.corp.local
 esx-02a.corp.local

1

CANCEL

BACK

FINISH

1. Review New Datastore configuration and click **Finish**.

Monitor task progress

1. Recent Tasks

2. Site A Datacenter

Site A Datacenter

Summary

ACTIONS ▾

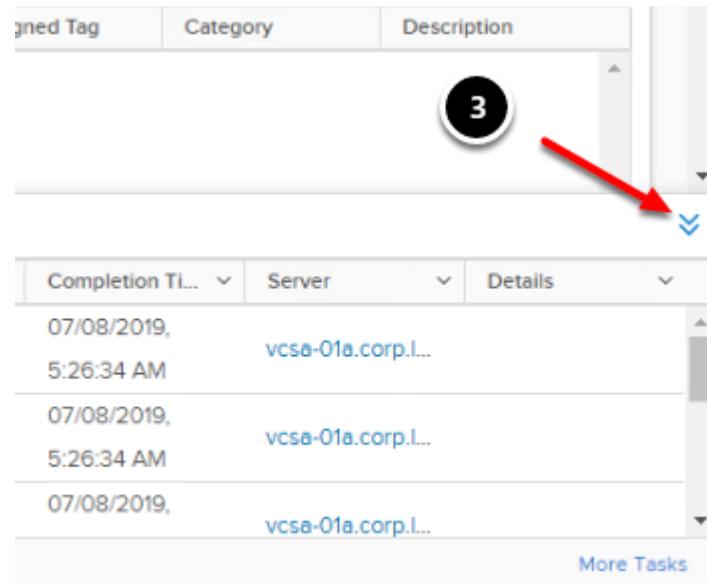
Hosts: 2
Virtual Machines: 3
Clusters: 1
Networks: 6
Datastores: 2

Custom Attributes

Attribute	Value
No items to display	

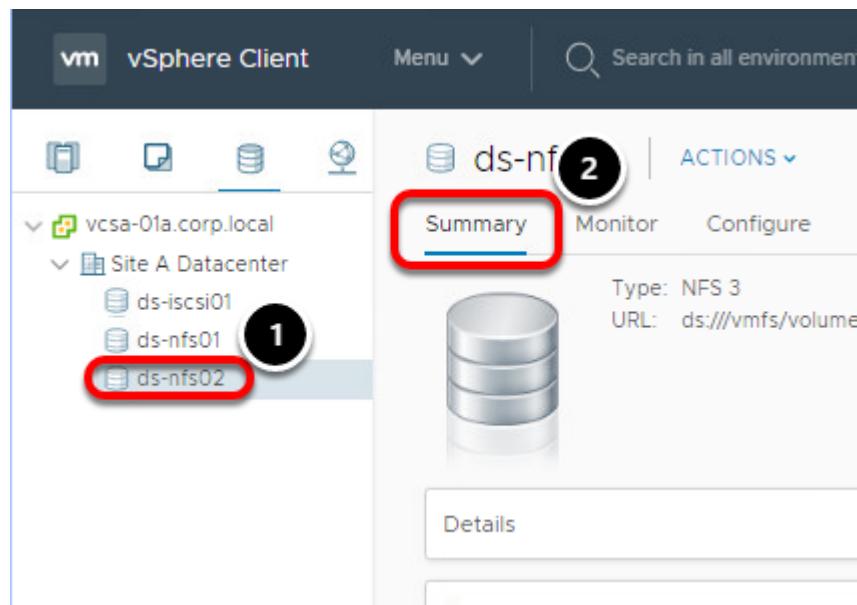
Task Name	Target	Status	Initiator	Queued For
Create NAS datastore	esx-02a.corp.local	✓ Completed	CORP\Administrator	6 ms
Create NAS datastore	esx-01a.corp.local	✓ Completed	CORP\Administrator	9 ms

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.



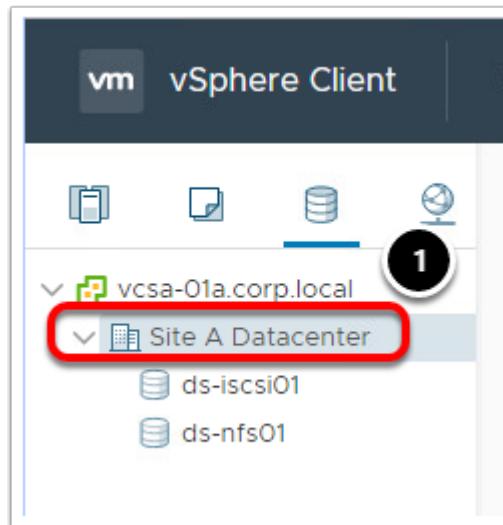
3. Minimize the **Recent Tasks** pane before continuing to the next step.

Review new Datastore Settings



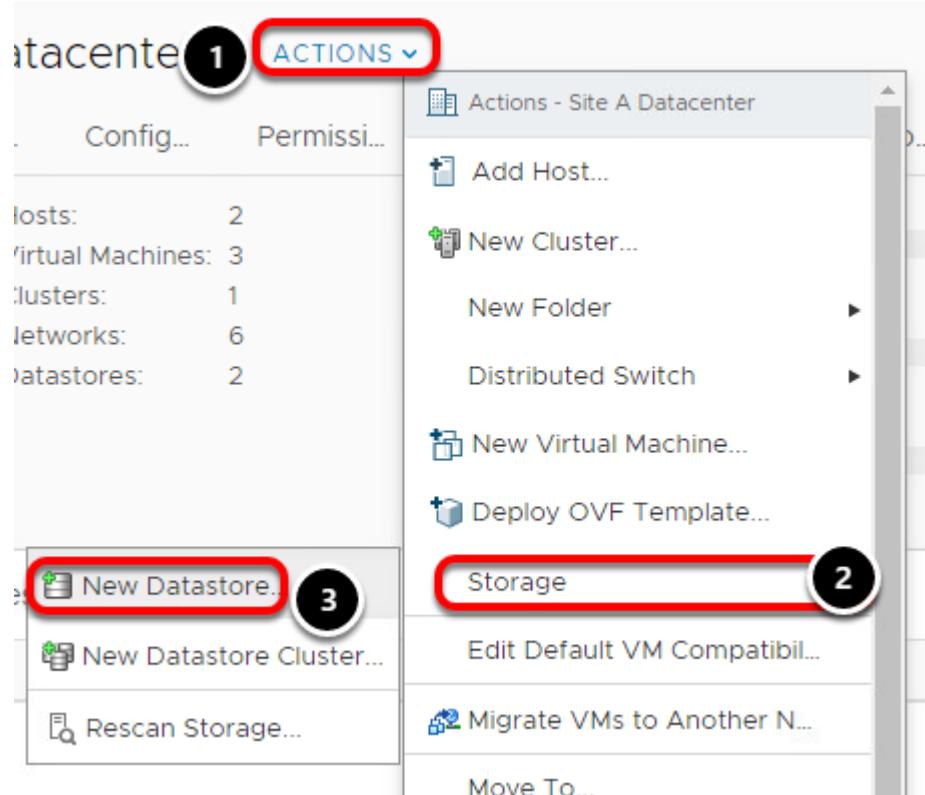
1. Select the datastore **ds-nfs02** from the inventory list
2. Select **Summary** to review capacity and configuration details

Create a vSphere iSCSI Datastore



1. Select **Site A Datacenter**

New Datastore



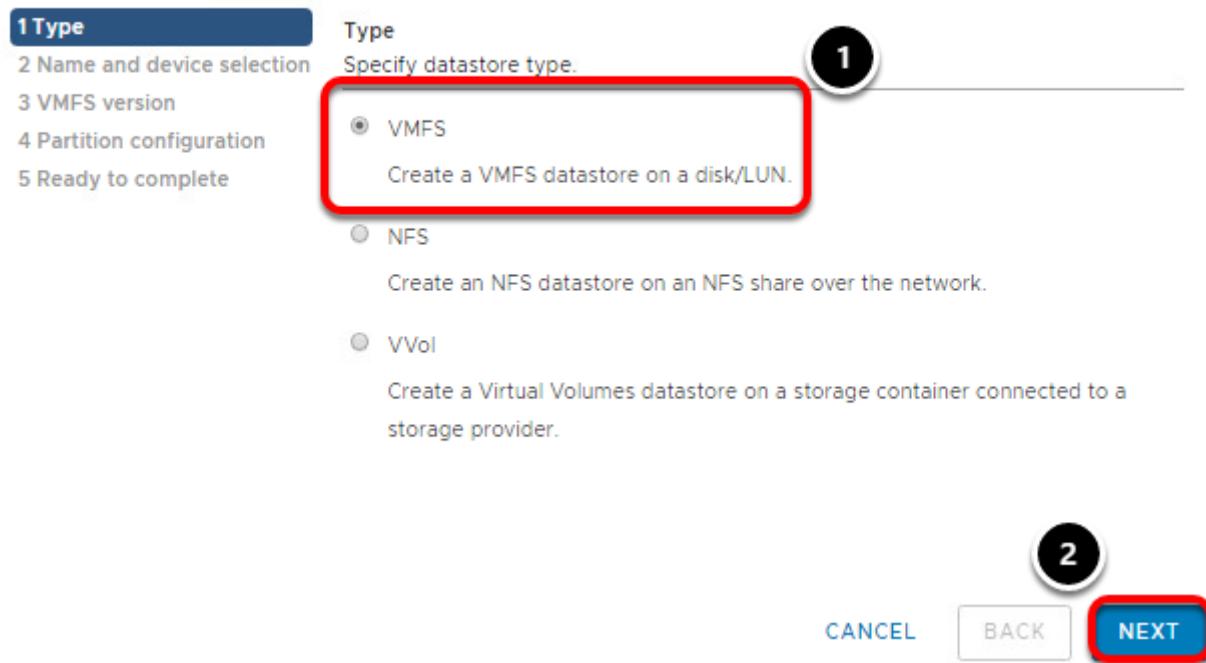
In this section, you will create a new vSphere iSCSI Datastore with a pre-provisioned iSCSI LUN.

1. Select **Actions**

2. Select **Storage**
3. Select **New Datastore**

New Datastore - Type

New Datastore



1. Verify type - **VMFS** - is selected.
2. Click **Next**

New Datastore - Name and Device configuration

New Datastore

✓ 1 Type
2 Name and device selection
3 VMFS version
4 Partition configuration
5 Ready to complete

Name and device selection
Select a name and a disk/LUN for provisioning the datastore.

Datastore name: **ds-iscsi02**

1

2

Note: The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host to view its accessible disks/LUNs: <select a host>

Name	LUN	Capacity	Drive T...	Sector
<select a host>				
esx-01a.corp.local				
esx-02a.corp.local				

CANCEL BACK NEXT

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.)

New Datastore

✓ 1 Type
2 Name and device selection
 3 VMFS version
 4 Partition configuration
 5 Ready to complete

Name and device selection
 Select a name and a disk/LUN for provisioning the datastore.

Datastore name: ds-iscsi02

1 ⓘ The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN. X

Select host to view its accessible disks/LUNs: esx-01a.corp.local

Name	LUN	Capacity	Hardware...	Drive T...	Sector
FreeNAS iSCSI Disk (nqe....)	2	45.00 GB	Supported	HDD	--
Local VMware Disk (mpx.v...)	0	2.00 GB	Not support...	Flash	512n

2 CANCEL BACK **NEXT**

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

New Datastore

- ✓ 1 Type
- ✓ 2 Name and device selection
- 3 VMFS version**
- 4 Partition configuration
- 5 Ready to complete

VMFS version

Specify the VMFS version for the datastore.

VMFS 6

VMFS 6 enables advanced format (512e) and automatic space reclamation support.

VMFS 5

VMFS 5 enables 2+TB LUN support.

1

CANCEL

BACK

2

NEXT

1. Leave the default of **VMFS 6** selected
2. Click **Next**

New Datastore - Partition Configuration

New Datastore

- ✓ 1 Type
- ✓ 2 Name and device selection
- ✓ 3 VMFS version
- 4 Partition configuration**
- 5 Ready to complete

Partition configuration
Review the disk layout and specify partition configuration details.

Partition Configuration	Use all available partitions
Datastore Size	<input type="range" value="45"/> 45 GB
Block size	1 MB
Space Reclamation Granularity	1 MB
Space Reclamation Priority	<input type="range"/> Low: Deleted or unmapped blocks are reclaimed on the LUN at Low priority

Empty: 45.0 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
- ✓ 2 Name and device selection
- ✓ 3 VMFS version
- ✓ 4 Partition configuration

5 Ready to complete

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

General

Name: ds-iscsi02
Type: VMFS
Datastore size: 45.00 GB

Device and Formatting

Disk/LUN: FreeNAS iSCSI Disk
(naa.6589cf000000a40b49d9abb957bf02b)
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, the navigation tree shows a vCenter server named 'vcsa-01a.corp.local' with a 'Site A Datacenter' folder expanded. Inside 'Site A Datacenter', there are five datastores: 'ds-iscsi01', 'ds-iscsi02' (which is highlighted with a red oval and a circled '2'), 'ds-nfs01', 'ds-nfs02', and 'ds-nfs03'. The 'Summary' tab is selected in the main content area, displaying statistics for hosts, virtual machines, clusters, networks, and datastores. On the right, a 'Recent Tasks' pane is open, showing a table of completed tasks. The table has columns for Task Name, Target, Status, and Initiator. The tasks listed are: 'Process VMFS datastore updates' (target: esx-02a.corp.local, status: Completed, initiator: System), 'Create VMFS datastore' (target: esx-01a.corp.local, status: Completed, initiator: CORP\Administrator), and 'Compute disk partition' (target: esx-01a.corp.local, status: Completed, initiator: CORP\Administrator). The 'Recent Tasks' pane is highlighted with a red box and a circled '1'.

Task Name	Target	Status	Initiator
Process VMFS datastore updates	esx-02a.corp.local	Completed	System
Create VMFS datastore	esx-01a.corp.local	Completed	CORP\Administrator
Compute disk partition	esx-01a.corp.local	Completed	CORP\Administrator

1. Note the progress in the **Recent Tasks** pane
2. When complete, you should see the **ds-iscsi02** Datastore available for use

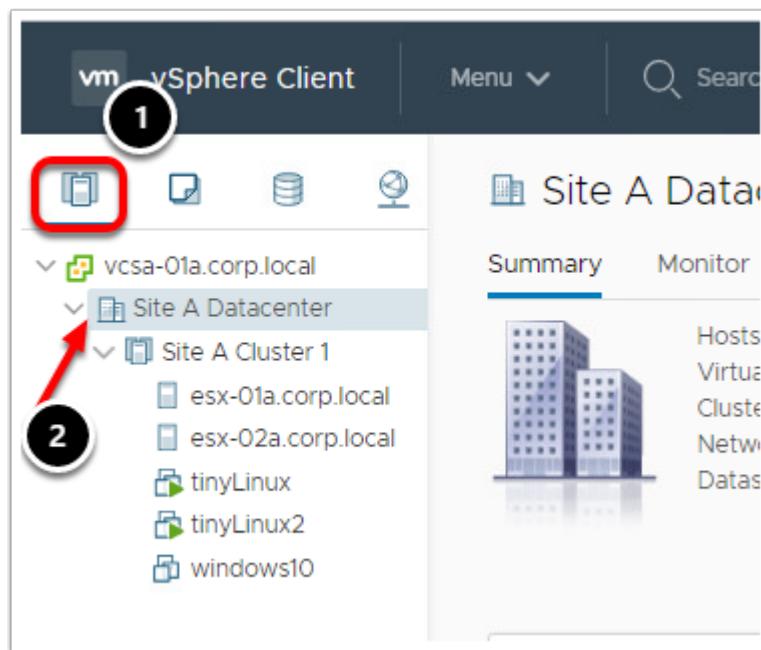
New Datastore - Review Settings

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 Site A and ensure that it has the appropriate storage configured so that it can become a productive member of the cluster.

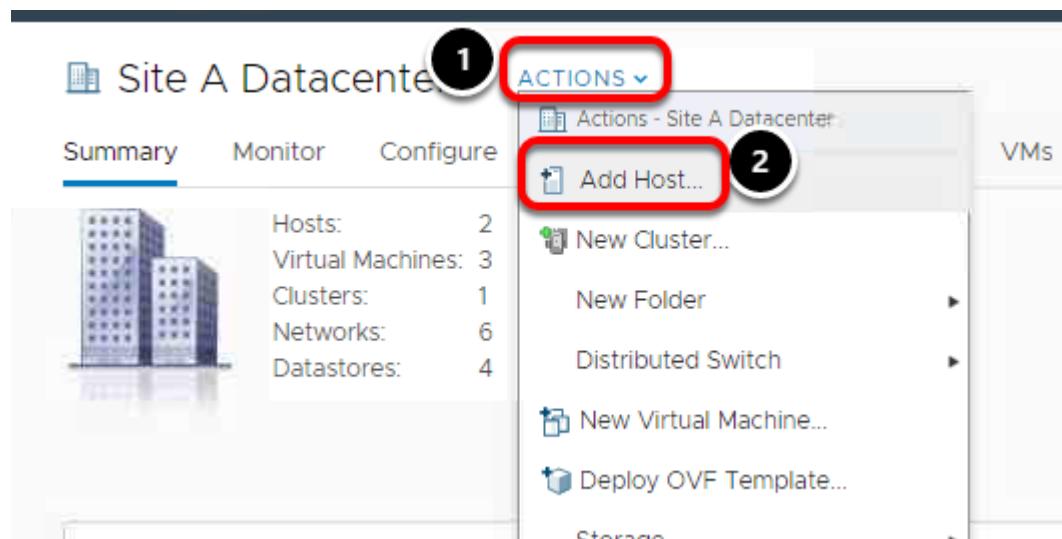
Hosts and Clusters View



1. Click on the **Hosts and Clusters** icon to return to that Inventory view
2. Select **Site A 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

Add Host

1 Name and location

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

Name and location

Enter the name or IP address of the host to add to vCenter Server

Host name or IP address: **esx-03a.corp.local**

Location:  Site A Datacenter

1[CANCEL](#)[BACK](#)[NEXT](#)**2**

1. In the **Host name or IP address**, enter: **esx-03a.corp.local**
2. Click **Next**

Connection Settings

Add Host

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

Connection settings
Enter the host connection details

User name: 1

Password: 1

CANCEL BACK **NEXT** 2

1. Enter the following login details:

- **User name:** root
- **Password:** VMware1!

2. Click **Next**

Host Summary

Add Host

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

Host summary

Review the summary for the host

Name	esx-03a.corp.local
Vendor	VMware, Inc.
Model	VMware Virtual Platform
Version	VMware ESXi 6.7.0 build-13006603
Virtual Machines	

1

CANCEL

BACK

NEXT

This screen shows the details of the host.

Click **Next**

Assign License

Add Host

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

Assign license

Assign an existing or a new license to this host

License	License Key	Product
<input checked="" type="radio"/> FOR VMWARE HA...	--	VMware vSphere
<input type="radio"/> Evaluation License	--	--

Assignment Validation for FOR VMWARE HANDS-ON LABS USE ONLY

- The license assignment is valid.

[CANCEL](#)

[BACK](#)

[NEXT](#)

Leave the default license choice and click **Next**.

Lockdown Mode

Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- ✓ 4 Assign license

5 Lockdown mode

6 VM location

7 Ready to complete

Lockdown mode

Specify whether to enable lockdown mode on the host

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

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

Disabled

Normal

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

Strict

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

1

CANCEL

BACK

NEXT

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

Add Host

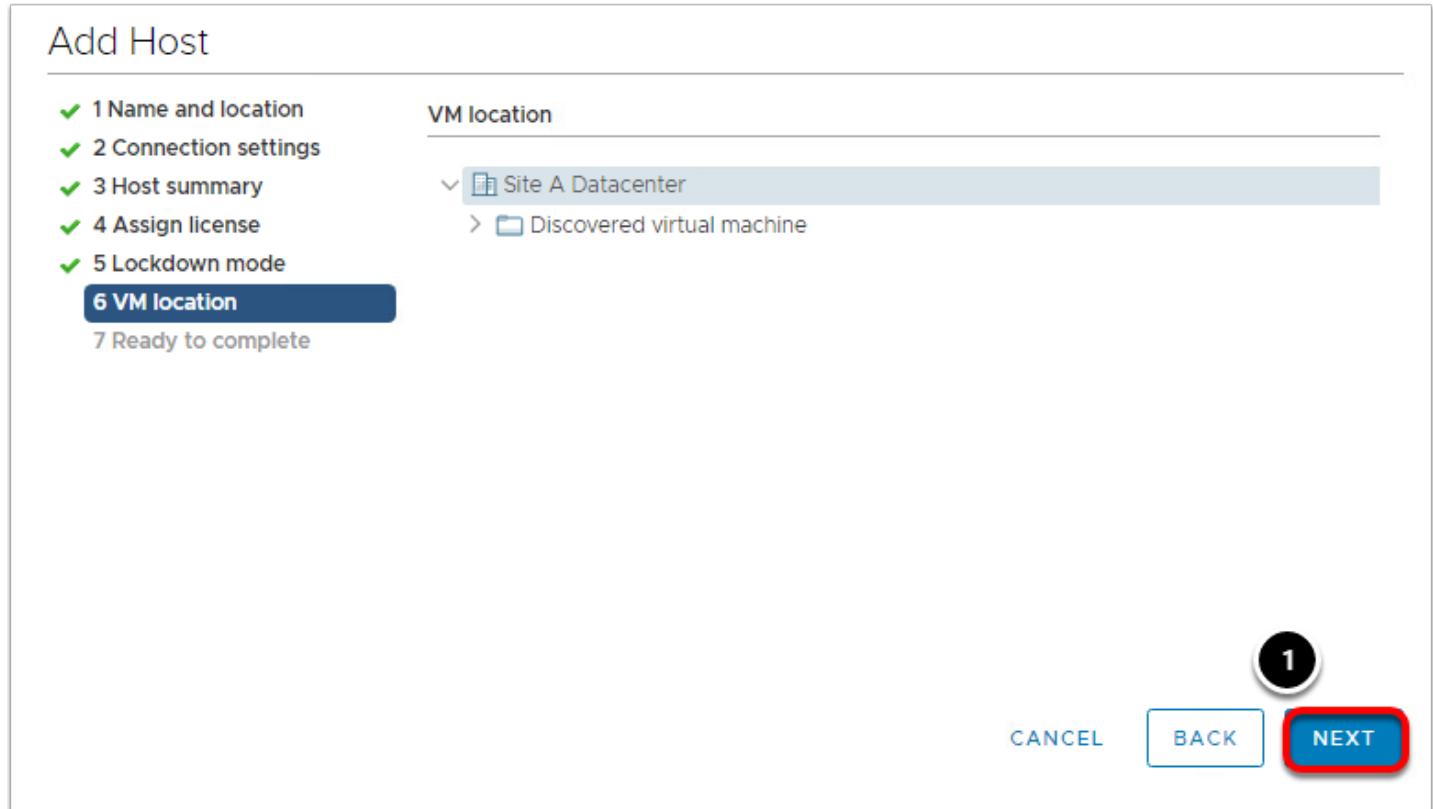
✓ 1 Name and location
✓ 2 Connection settings
✓ 3 Host summary
✓ 4 Assign license
✓ 5 Lockdown mode
6 VM location
7 Ready to complete

VM location

Site A Datacenter
Discovered virtual machine

1

CANCEL BACK **NEXT**



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

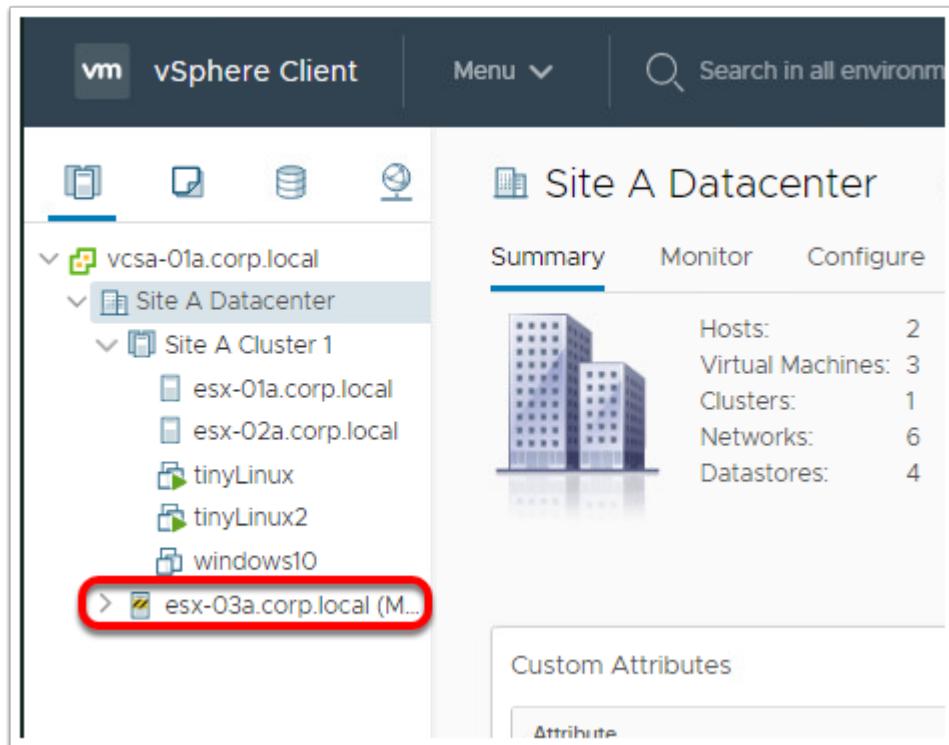
Click Finish to add the host

✓ 1 Name and location	Name	esx-03a.corp.local
✓ 2 Connection settings	Location	Site A Datacenter
✓ 3 Host summary	Version	VMware ESXi 6.7.0 build-10302608
✓ 4 Assign license	License	FOR VMWARE HANDS-ON LABS USE ONLY
✓ 5 Lockdown mode	Networks	
✓ 6 VM location	Datstores	
7 Ready to complete	Lockdown mode	Disabled
	VM location	Site A Datacenter

CANCEL **BACK** **FINISH**

Review the settings and click **Finish** to add the esx-03a.corp.local to the datacenter.

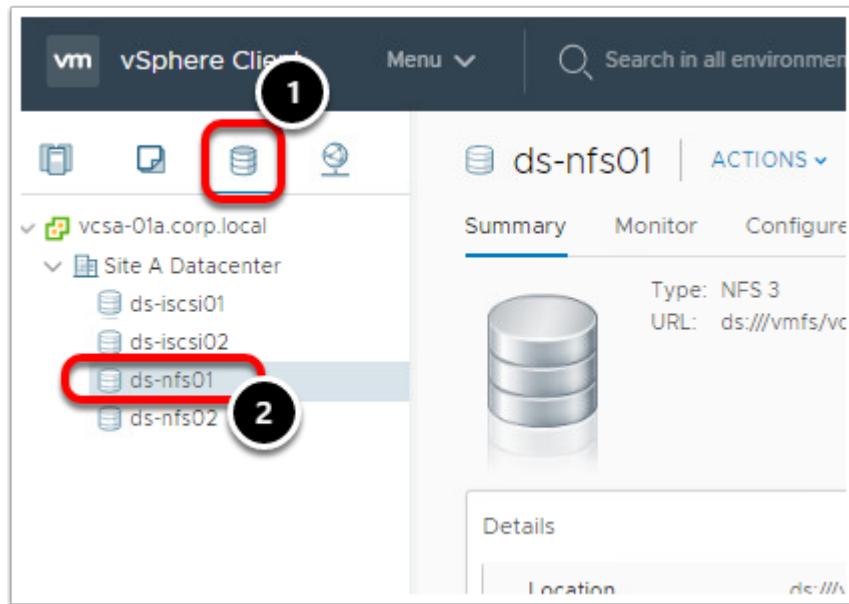
Host Added to Datacenter



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.

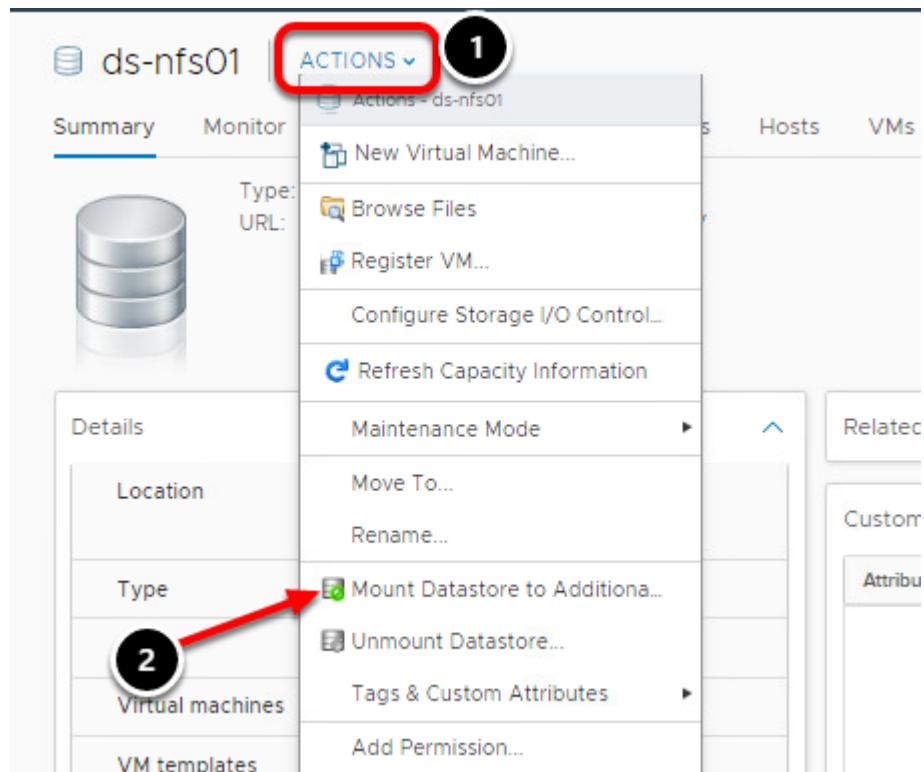
Datastore view



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

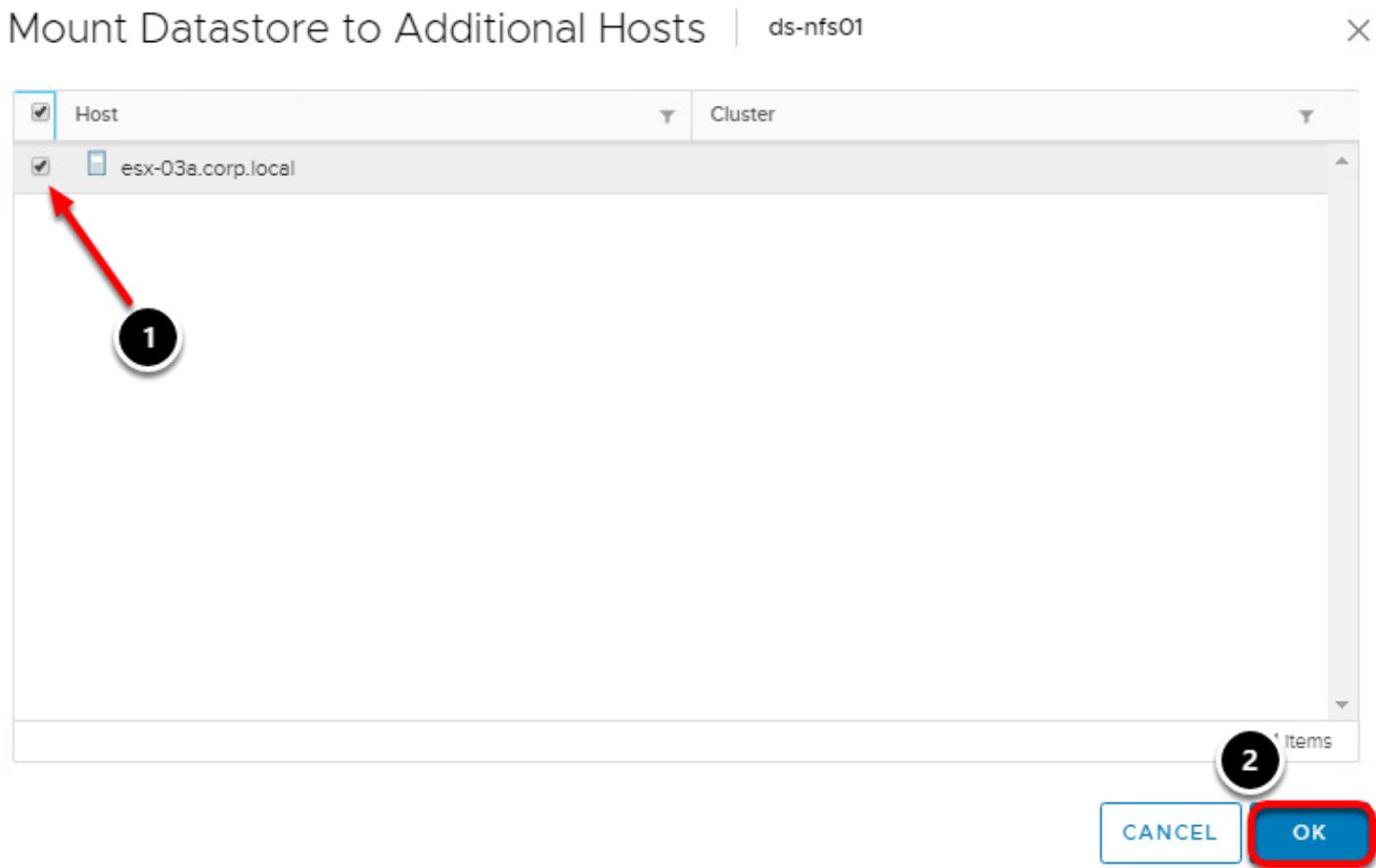
Mount NFS Datastore to New Host Wizard



In this case, there are two NFS datastores used by the Cluster Site A cluster. Adding an existing NFS datastore to a new host is a simple process.

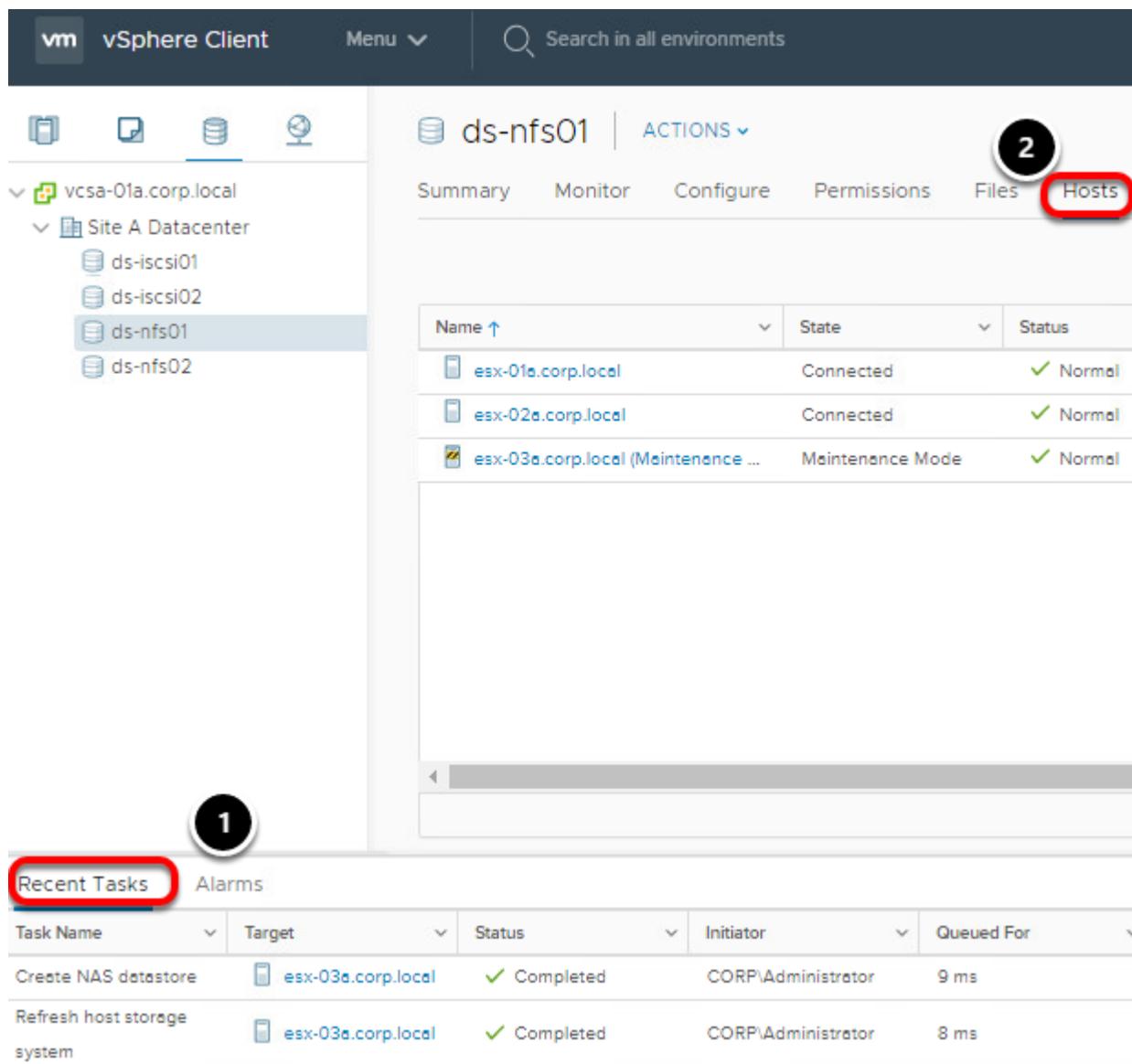
1. Click on the **Actions** menu
2. Select **Mount Datastore to Additional Hosts...**

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. On the left, the inventory tree shows a folder named 'vcsa-01a.corp.local' containing 'Site A Datacenter', 'ds-iscsi01', 'ds-iscsi02', 'ds-nfs01' (which is selected), and 'ds-nfs02'. On the right, the 'ds-nfs01' details page is displayed. The 'Hosts' tab is highlighted with a red box and a circled '2'. The 'Recent Tasks' tab is also highlighted with a red box and a circled '1'. The 'Hosts' table lists three hosts: 'esx-01a.corp.local' (Connected, Normal), 'esx-02a.corp.local' (Connected, Normal), and 'esx-03a.corp.local (Maintenance ...)' (Maintenance Mode, Normal).

Name	State	Status
esx-01a.corp.local	Connected	Normal
esx-02a.corp.local	Connected	Normal
esx-03a.corp.local (Maintenance ...)	Maintenance Mode	Normal

1. The mount task can be monitored using 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.

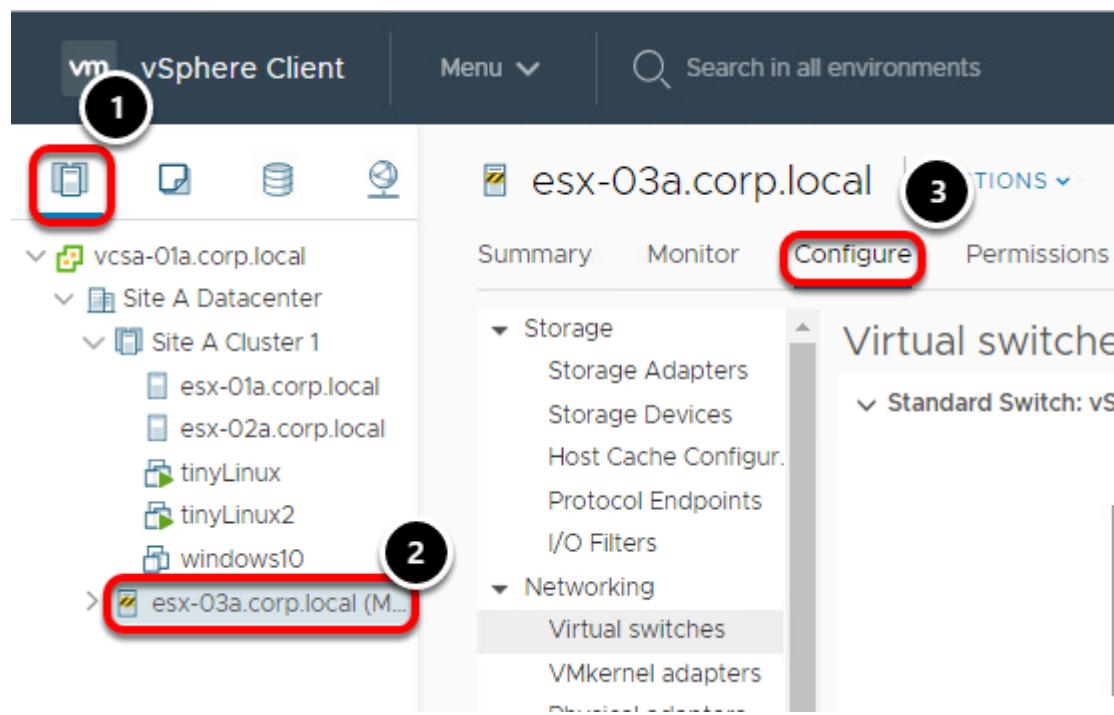
For additional practice, perform the same steps to mount the other NFS datastore, **ds-nfs02** to the **esx-03a.corp.local** host.

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



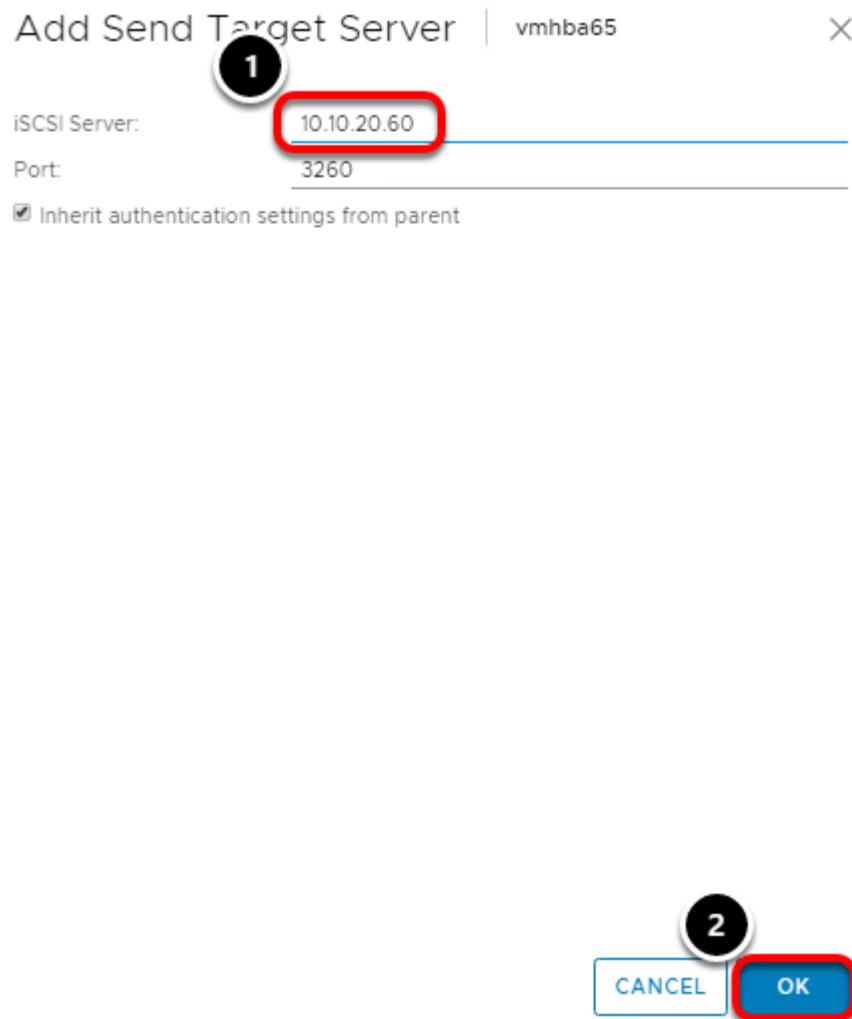
1. Select the **Hosts and Clusters** icon and
2. Click on **esx-03a.corp.local**.
3. Finally, click the **Configure** tab.

Perform Dynamic Discovery

The screenshot shows the vSphere Web Client interface for host `esx-03a.corp.local`. The navigation bar includes `S`, `1` (highlighted), `Monitor`, `Configure` (highlighted), `Permissions`, `VMs`, `Datastores`, `Networks`, and `Updates`. The left sidebar shows `Storage` (highlighted), `Storage Adapters` (highlighted), `Storage Devices`, `Host Cache Configuration`, `Protocol Endpoints`, and `I/O Filters`. Under `Networking`, it lists `Virtual switches`, `VMkernel adapters`, `Physical adapters`, and `TCP/IP configuration`. Under `Virtual Machines`, it lists `VM Startup/Shutdown`, `Agent VM Settings`, `Default VM Compatibility`, and `Swap File Location`. The main content area is titled `Storage Adapters` and displays a table of adapters. The table has columns: `Adapter`, `Type`, `Status`, `Identifier`, and `Targ...`. It shows three entries: `vmhba65` (iSCSI, Online, `iqn.1998-01.com.vmware:esx-0...`, 0), `vmhba1` (Block S..., Unknown, --, 1), and `vmhba64` (Block S..., Unknown, --, 0). The toolbar below the table includes buttons for `Property`, `4` (highlighted), `Device...`, `Pat...`, `Dynamic Disc...` (highlighted), `Static Discov...`, and `Network Port`. The `Dynamic Disc...` button is circled with a red box. The `Add...` button is also circled with a red box.

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

esx-03a.corp.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Storage Adapters

Storage Adapters Storage Devices Host Cache Configuration Protocol Endpoints I/O Filters

Networking Virtual switches VMkernel adapters Physical adapters TCP/IP configuration

Storage Adapters

Adapter Type Status Id

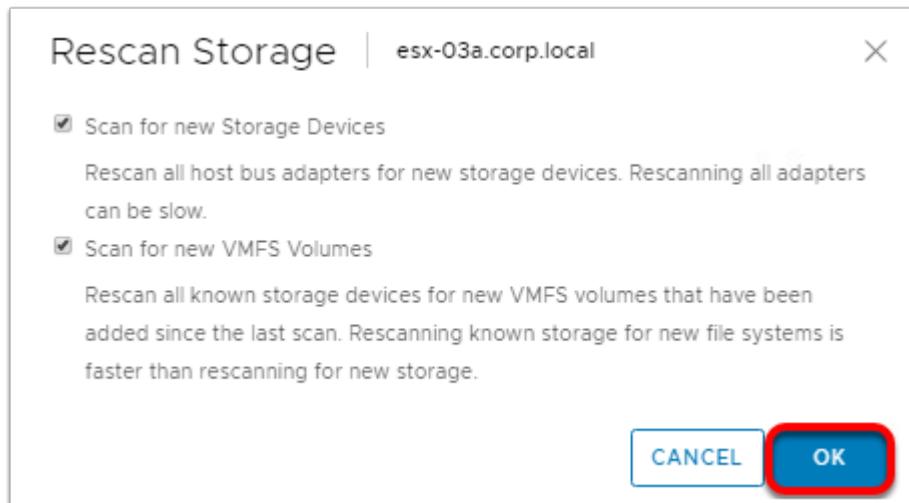
Model: iSCSI Adapter
vmhba65 iSCSI Online iqn.1998-01.com.vmware:esx-0... 1

Model: PII4 for 430TX/440BX/MX IDE Controller

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



Leave the default options selected and click **OK**.

Verify iSCSI Devices are Visible

esx-03a.corp.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Storage Devices

Name	L...	Type	Capacity
Local VMware Disk (mpx.vmhba0:C0:T0:L0)	0	disk	2.00 GB
FreeNAS iSCSI Disk (nqn.6589fc000000a40b...)	2	disk	45.00 GB
Local NECVMWar CD-ROM (mpx.vmhba1:C0:T0...)	0	cd	0.00 GB
FreeNAS iSCSI Disk (nqn.6589fc000000f4d...)	1	disk	45.00 GB

1. Once the rescan is complete, Click on **Storage Devices**.
2. You should now see two iSCSI disks connected, both with 45GB of capacity.

Verify iSCSI Datastore Availability

esx-03a.corp.local | ACTIONS ▾

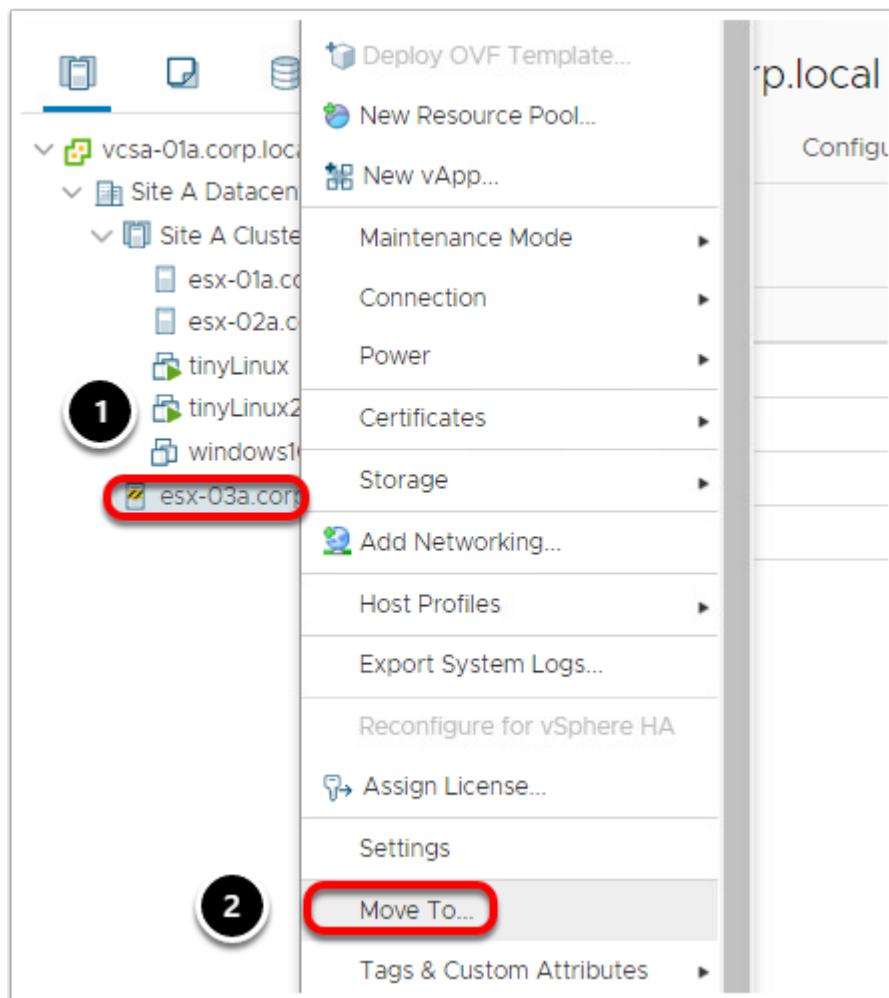
Summary Monitor Configure Permissions VMs Datastores Networks Updates

Name	Status	Type	Datastore Clus...	Capacity
ds-iscsi01	Normal	VMFS 6		44.75 GB
ds-iscsi02	Normal	VMFS 6		44.75 GB
ds-nfs01	Normal	NFS 3		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

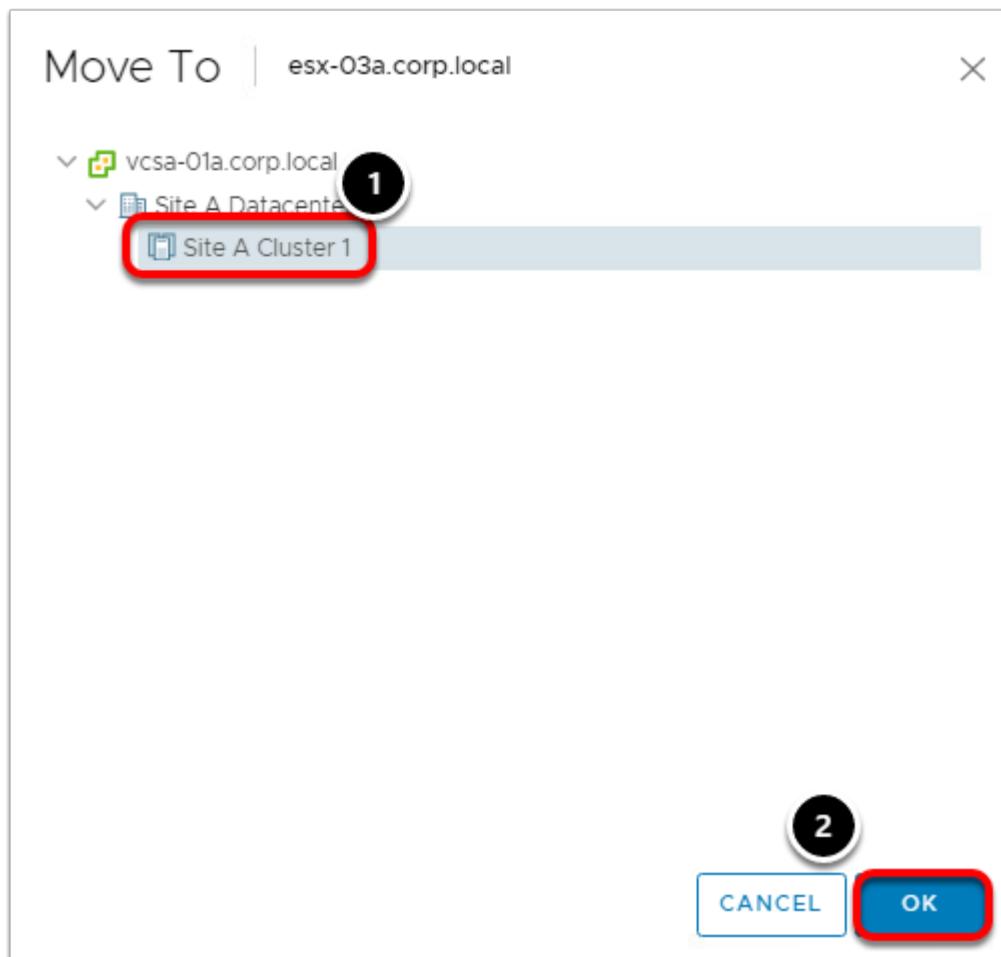
Move into the Cluster



Now that we have the storage configured, move the **esx-03a.corp.local** into **Site A Cluster 1**.

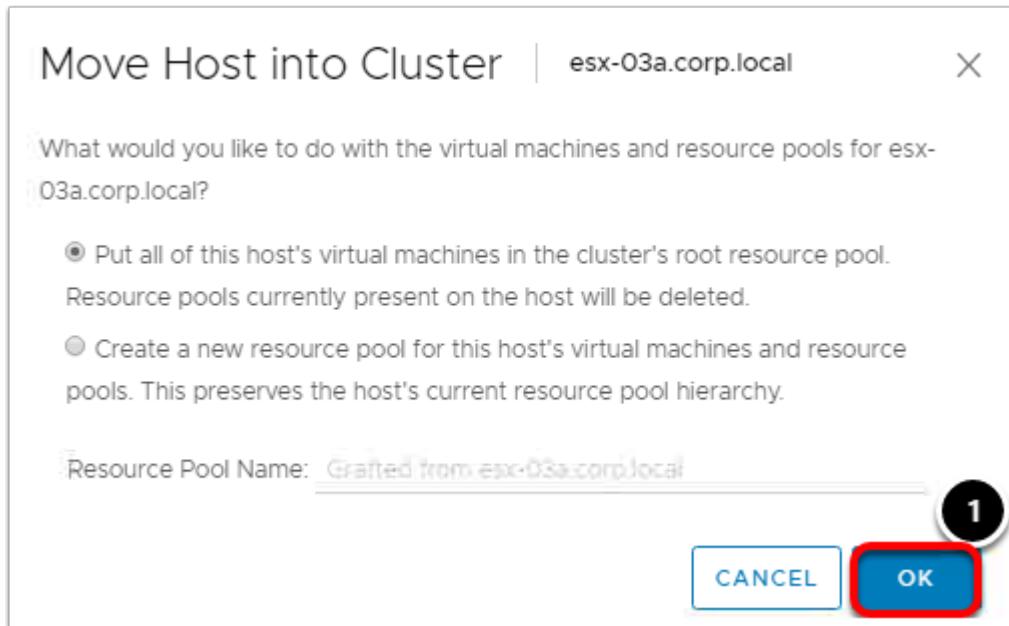
1. Right-click on **esx-03a.corp.local**
2. Select **Move To...**

Move To



1. Expand **Site A Datacenter** until you see **Site A Cluster 1** and select it.
2. Click **OK**.

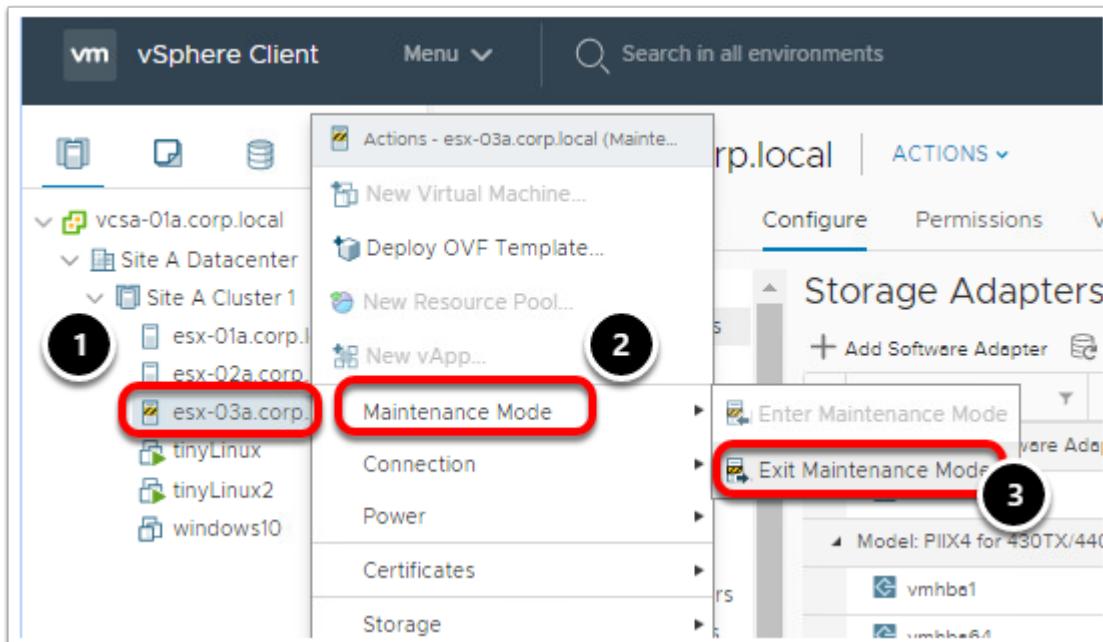
Resource Pools



We are given the option to either place all of the virtual machines hosted by esx-03a.corp.local into the Site A Cluster 1 Resource pool or create a new one.

1. Leave the default setting and click **OK**.

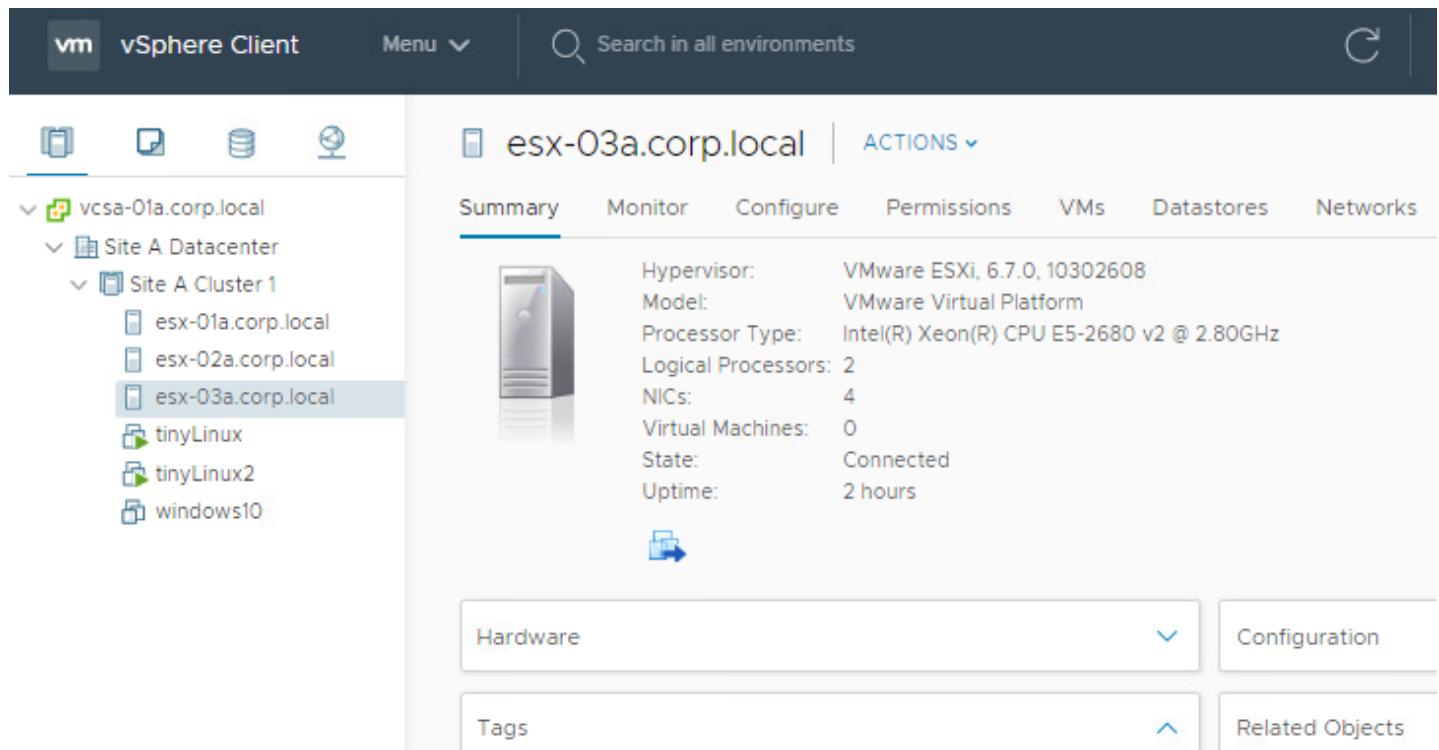
Exit Maintenance Mode



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



esx-03a.corp.local

ACTIONS

Summary Monitor Configure Permissions VMs Datastores Networks

	Hypervisor: VMware ESXi, 6.7.0, 10302608 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: 2 hours
---	---

Hardware **Configuration**

Tags **Related Objects**

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

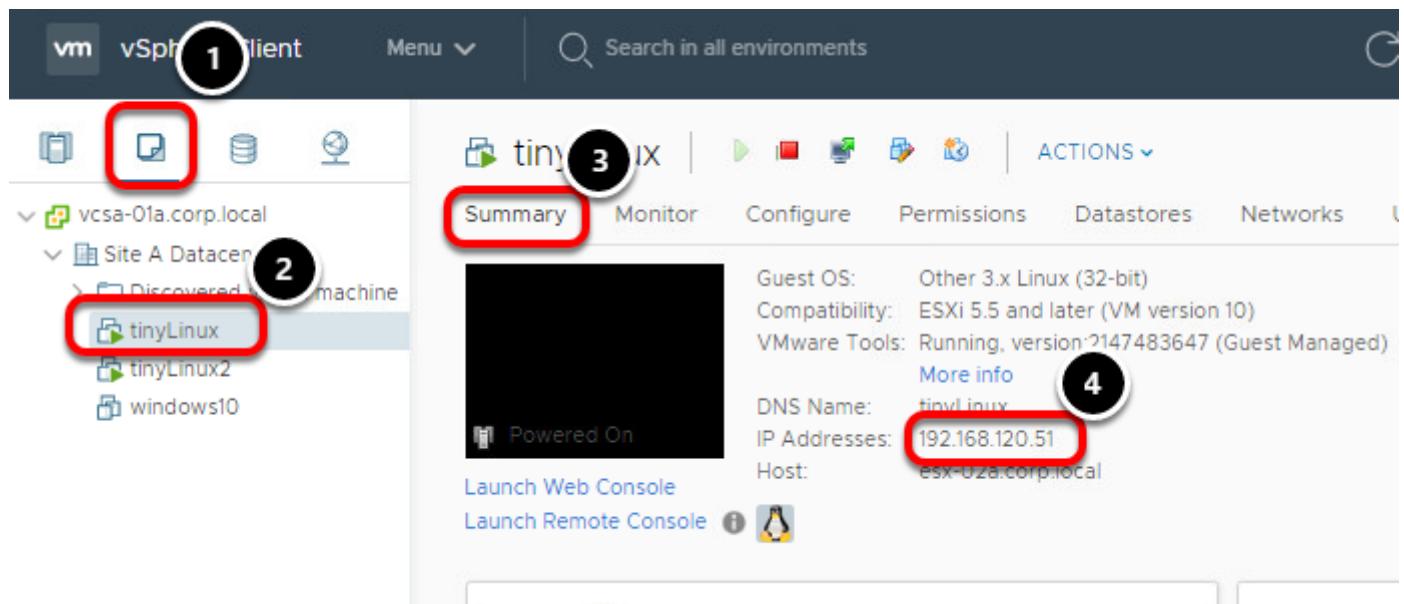
Planned downtime typically accounts for over 80% of datacenter downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule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

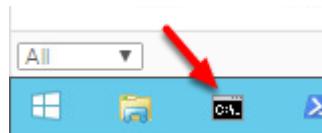
Navigate to Virtual Machines and Templates



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.

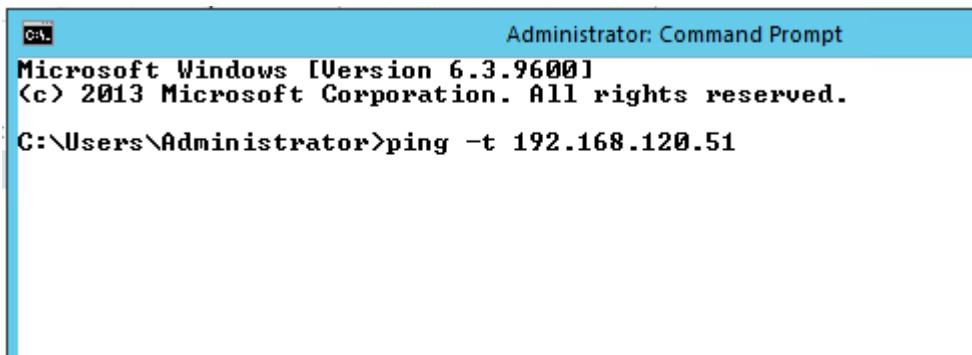
1. Click the **VMs and Templates** tab
2. Select **tinyLinux**
3. Ensure you are on the **Summary** tab
4. Note the IP Address of **tinyLinux, 192.168.120.51**

Open a Command Prompt



From the Windows Task Bar, click on the icon to open a command prompt.

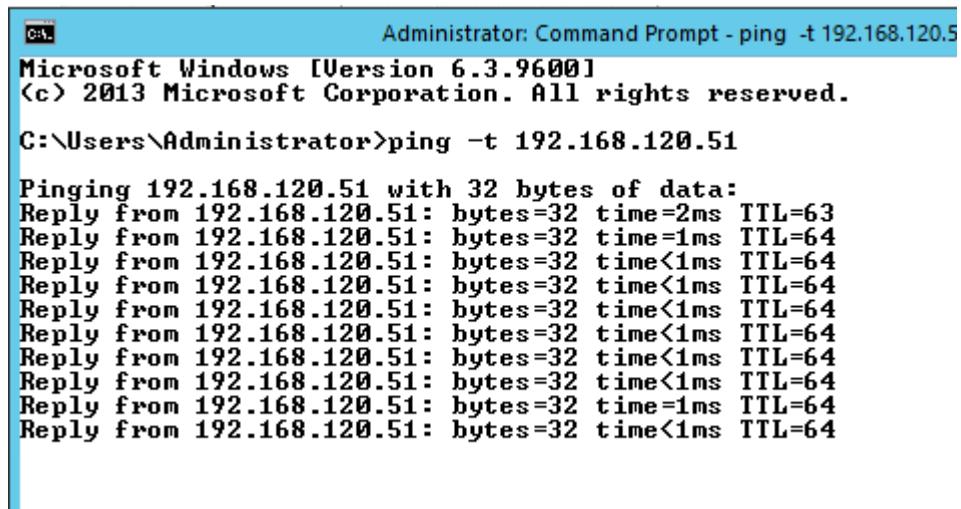
Ping TinyLinux-01



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

1. Click the **Storage** icon.

List Virtual Machines on a Specified Datastore

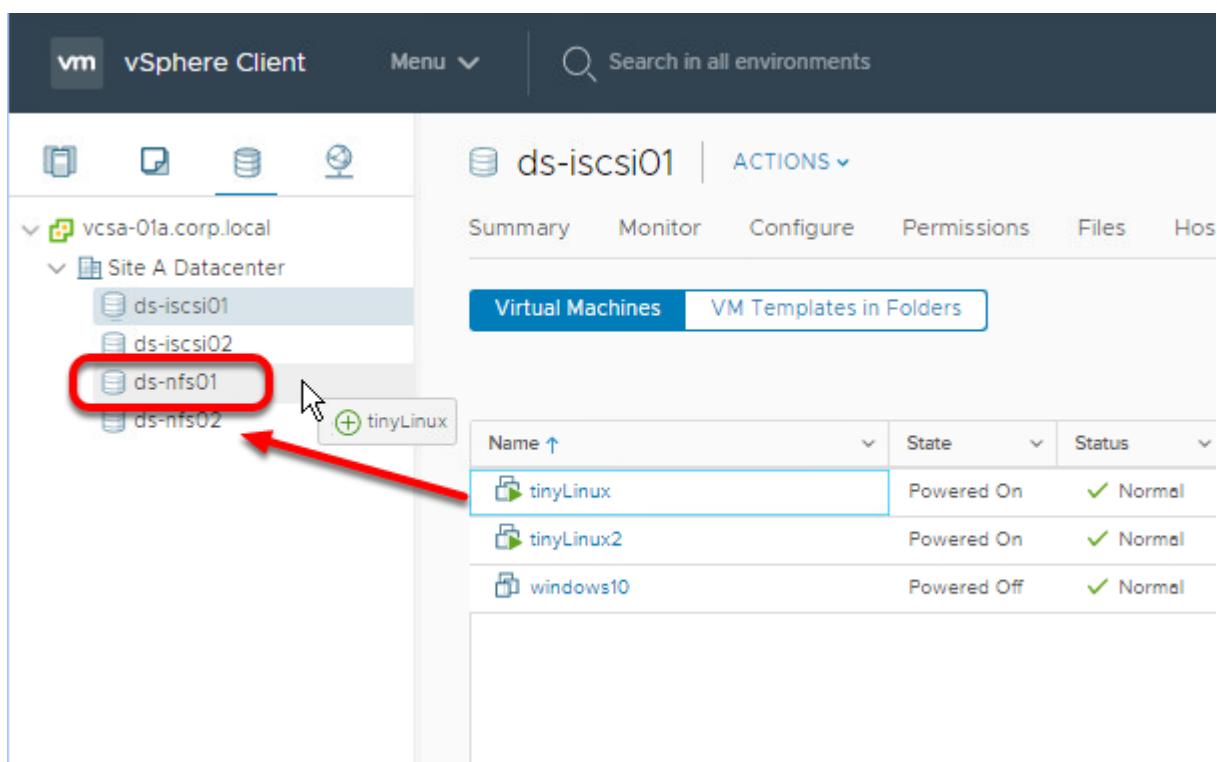
Name	State	Status	Provisioned Space
tinyLinux	Powered On	Normal	467.02 MB
tinyLinux2	Powered On	Normal	466.78 MB
windows10	Powered Off	Normal	25.19 GB

1. Navigate to and click on the **ds-iscsi01** datastore object in **Site A Datacenter** 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



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

tinyLinux - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

 Change compute resource only

Migrate the virtual machines to another host or cluster.

 Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

 Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

[CANCEL](#)[BACK](#)[NEXT](#)

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

tinyLinux - Migrate

✓ 1 Select a migration type
2 Select storage
 3 Ready to complete

Select storage
 Select the destination storage for the virtual machine migration.

Select virtual disk format: Thin Provision

VM Storage Policy: Keep existing VM storage policies

Configure per disk

	Name	Capacity	Provisioned	Free	Type	Clus
1	ds-iscsi01	44.75 GB	29.73 GB	30.3 GB	VMFS 6	
	ds-iscsi02	44.75 GB	1.41 GB	43.34 GB	VMFS 6	
	ds-nfs01	5.78 GB	88 KB	5.78 GB	NFS v3	
	ds-nfs02	5.78 GB	88 KB	5.78 GB	NFS v3	

Compatibility

✓ Compatibility checks succeeded.

2

CANCEL BACK **NEXT**

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

tinyLinux - Migrate

- ✓ 1 Select a migration type
- ✓ 2 Select storage
- 3 Ready to complete**

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

CANCEL

BACK

FINISH

Verify your selections on the Ready to complete screen and click **Finish** to start the migration.

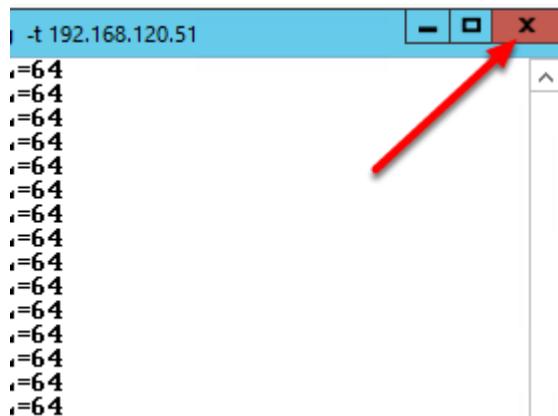
Feel free to monitor the operation within the Recent Tasks pane or move on to the next step.

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.

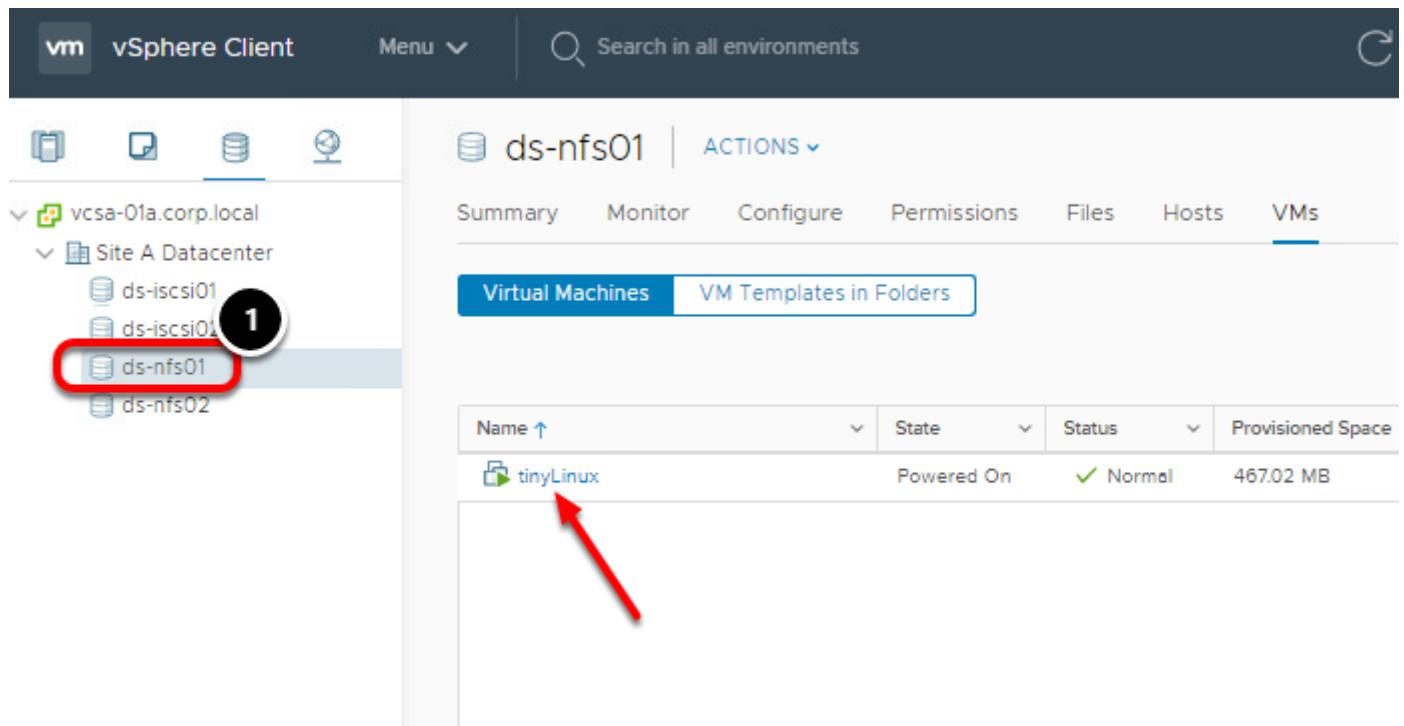
You may see instances where the time field increases to 2ms, but otherwise no packets should have dropped.

Stop the ping



Click the 'X' to stop the ping and close the command window.

Confirm Storage vMotion



The screenshot shows the vSphere Client interface. The left sidebar shows a tree structure with 'vcsa-01a.corp.local' expanded, containing 'Site A Datacenter', 'ds-iscsi01', 'ds-iscsi02', 'ds-nfs01' (which is circled with a black circle labeled '1'), and 'ds-nfs02'. The right panel shows the 'ds-nfs01' datastore details with the 'VMs' tab selected. The 'Virtual Machines' tab is active, showing a table with one row:

Name	State	Status	Provisioned Space
tinyLinux	Powered On	Normal	467.02 MB

The Storage vMotion progress can be monitored in the Recent Tasks panel

1. 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.

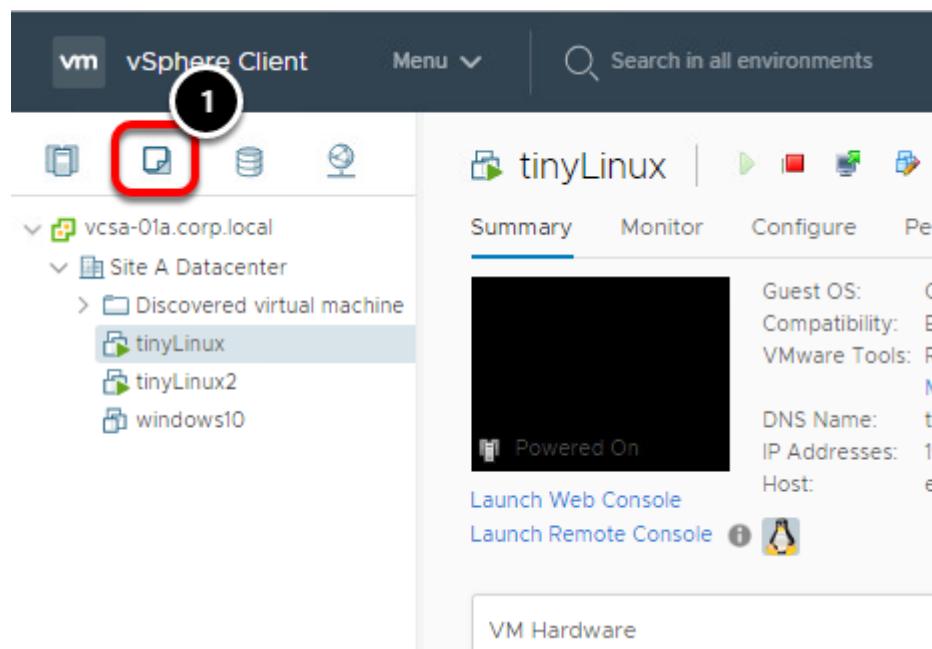
Managing Virtual Machine Disks

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.

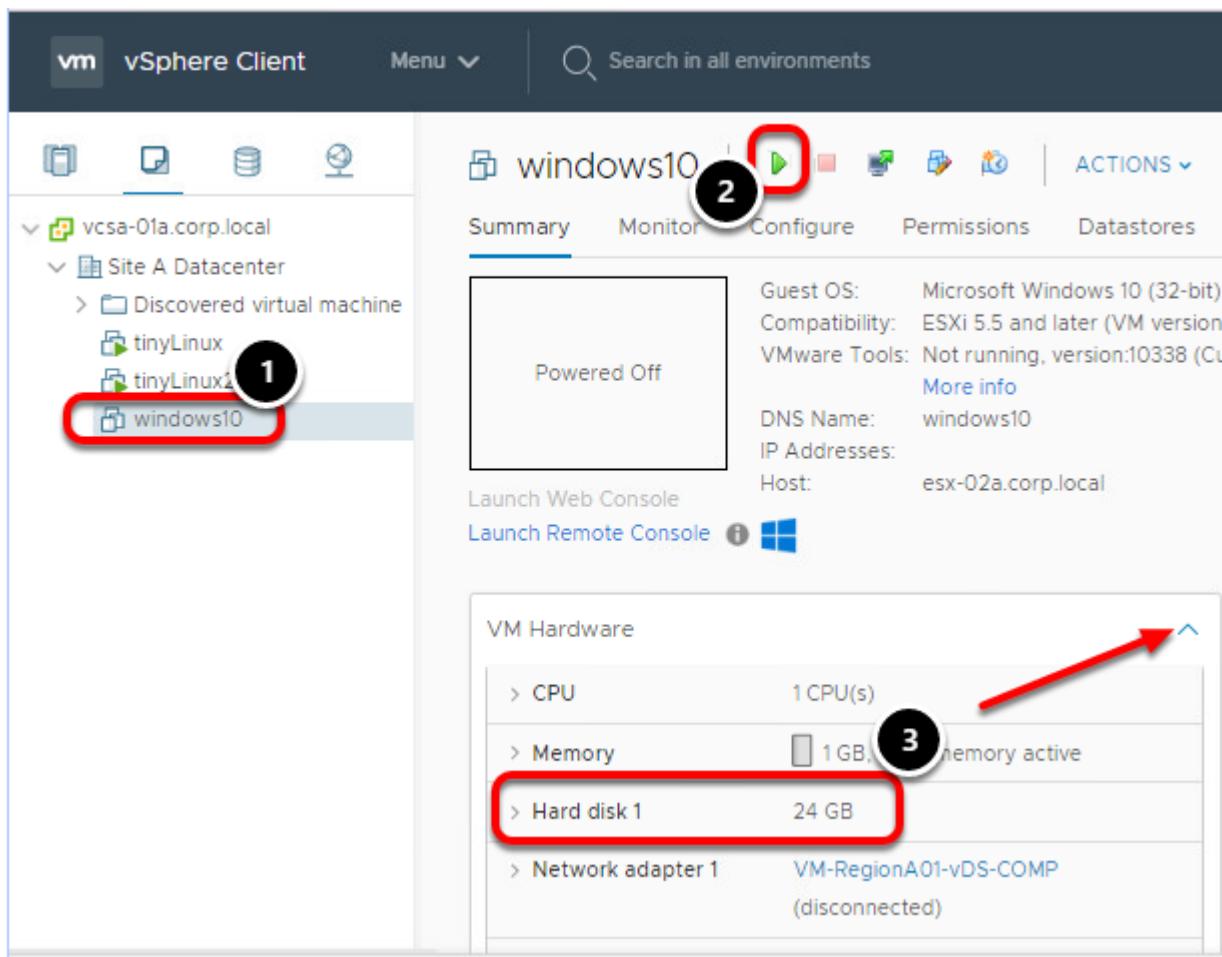
Navigate to the VMs and Templates management pane



1. Select VMs and Templates

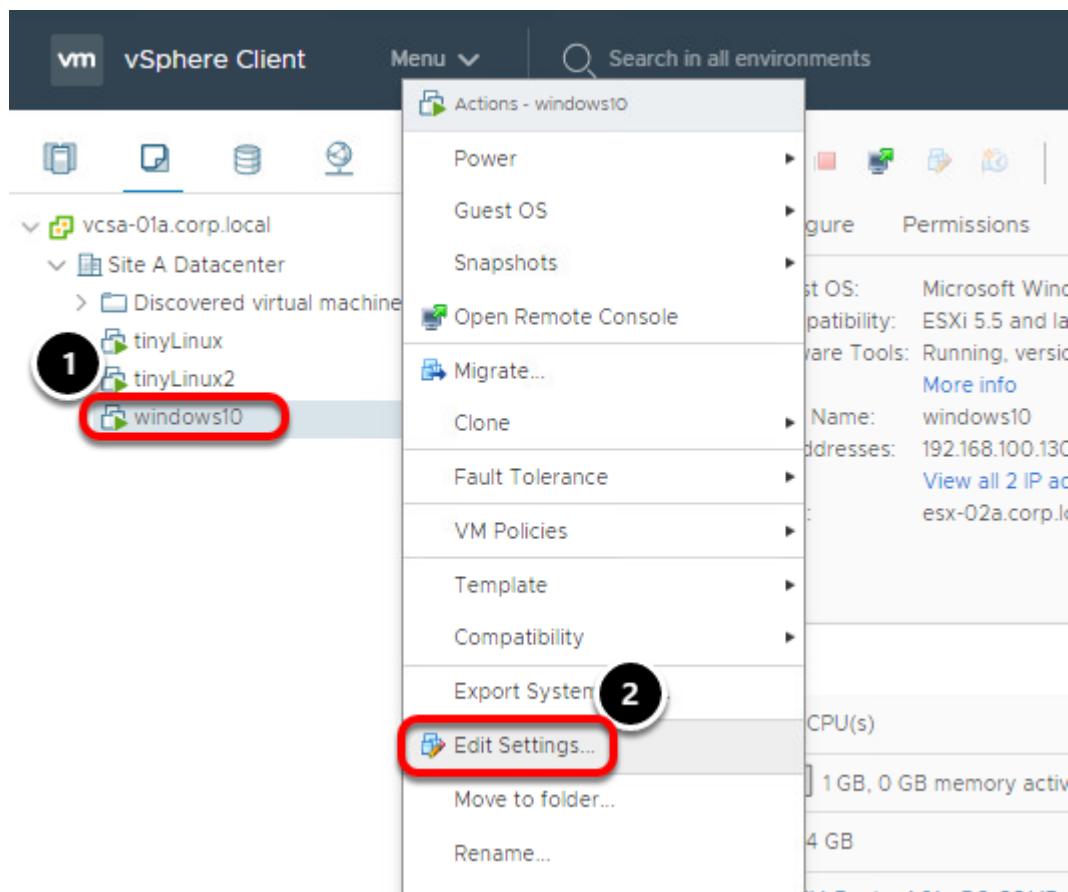
From this view, we can see that there are several existing Virtual Machines in our vSphere environment. In the next step, we will add a new virtual disk to the **windows10** Virtual Machine.

Verify windows10 Storage



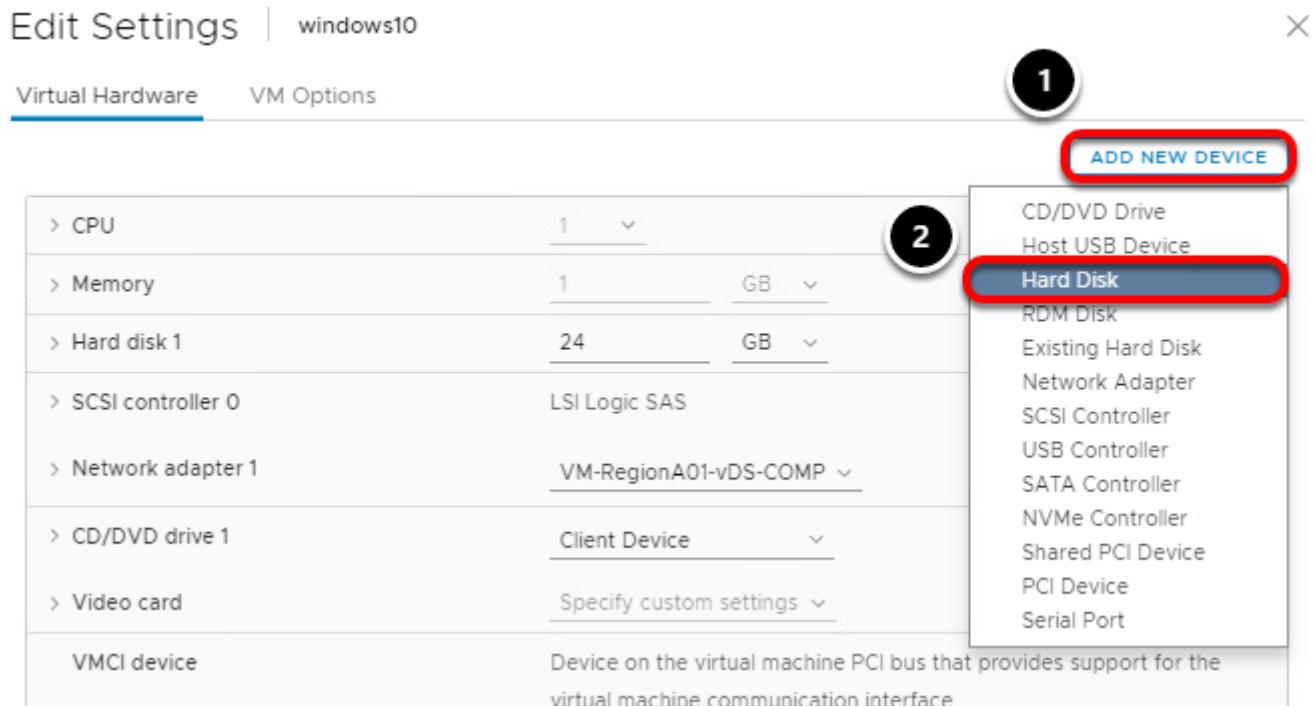
1. Select Virtual Machine **windows10** and click the **Summary** tab
2. If w12-core is not powered on, click the **power on** button.
3. In the VM Hardware pane, note the original disk configuration - single hard disk with a capacity of 24.00 GB. You may need to expand the VM Hardware section to see 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

Edit Settings | windows10

X

Virtual Hardware

VM Options

ADD NEW DEVICE

> CPU	1	▼	
> Memory	1	B	▼
> Hard disk 1	24	GB	▼
> New Hard disk *	5	GB	▼
> SCSI controller 0	LSI Logic SAS		
> Network adapter 1	VM-RegionA01-vDS-COMP	▼	<input checked="" type="checkbox"/> Connected
> CD/DVD drive 1	Client Device		
> Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

1

5

i

2

CANCEL

OK

1. Decrease the size to 5 GB
2. Click **OK** to create the new virtual disk

Monitor task progress

VM vSphere Client Menu Search in all environments

Summary Monitor Configure Permissions Datastores

Guest OS: Microsoft Windows 10 (32-bit)
Compatibility: ESXi 5.5 and later (VM version)
VMware Tools: Running, version:10338 (Current)
More info
DNS Name: windows10
IP Addresses: 192.168.100.130
View all 2 IP addresses
Host: esx-02a.corp.local

Launch Web Console Launch Remote Console

VM Hardware

> CPU	1 CPU(s)
> Memory	1 GB, 0.86 GB memory active
> Hard disk 1	24 GB
> Hard disk 2	5 GB

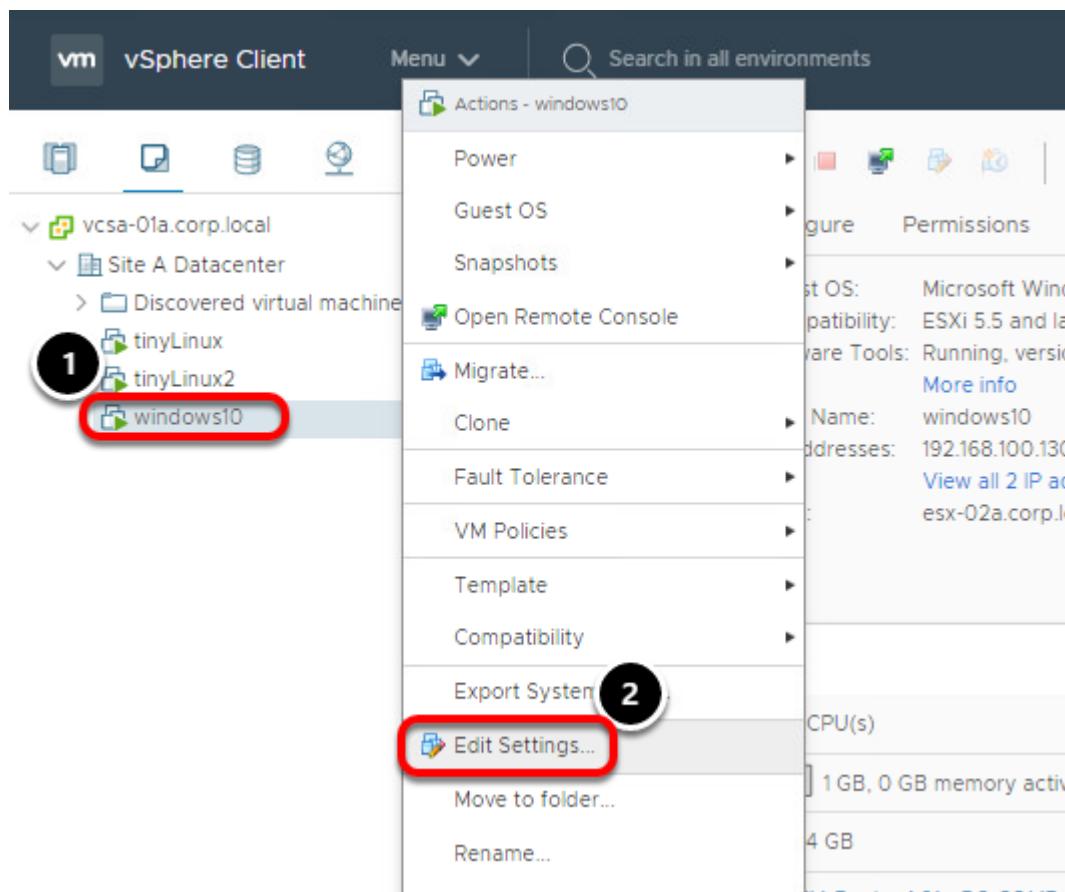
Recent Tasks Alarms

Task Name	Target	Status	Initiator	Queued For
Reconfigure virtual machine	windows10	Completed	CORP\Administrator	6 ms
Power On virtual	windows10	Completed	CORP\Administrator	51 ms

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

Edit Settings | windows10

Virtual Hardware VM Options

1	Memory	1	GB
1	Hard disk 1	24	GB
1	Hard disk 2	5	GB
1	SCSI controller 0	LSI Logic SAS	
1	Network adapter 1	VM-RegionA01-vDS-COMP	

1. In the Edit Settings wizard, note the capacity for Hard disk 1 is 24 GB.

Extend Hard disk 1

Edit Settings | windows10

X

Virtual Hardware

VM Options

ADD NEW DEVICE

> CPU	1	GB	1
> Memory	1	GB	1
> Hard disk 1 *	32	GB	32
> Hard disk 2	5	GB	5
> SCSI controller 0	LSI Logic SAS		
> Network adapter 1	VM-RegionA01-vDS-COMP	<input checked="" type="checkbox"/>	Connected
> CD/DVD drive 1	Client Device	<input type="checkbox"/>	Connected
> Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

1

32

1

2

CANCEL

OK

1. Type **32** Hard disk 1 capacity field.
2. Click **OK**

Monitor task progress

VM vSphere Client Menu Search in all environments

windows10 | ACTIONS

Summary Monitor Configure Permissions Datastores

Guest OS: Microsoft Windows 10 (32-bit)
Compatibility: ESXi 5.5 and later (VM version)
VMware Tools: Running, version:10338 (Current)
More info
DNS Name: windows10
IP Addresses: 192.168.100.130
View all 2 IP addresses
Host: esx-02a.corp.local

Launch Web Console Launch Remote Console

VM Hardware

> CPU	1 CPU(s)
> Memory	1 GB, 1 GB memory active
> Hard disk 1	32 GB
> Hard disk 2	5 GB

Recent Tasks Alarms

Task Name	Target	Status	Initiator	Queued For
Reconfigure virtual machine	windows10	Completed	CORP\Administrator	7 ms
Reconfigure virtual machine	windows10	Completed	CORP\Administrator	6 ms

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

Guest OS: Microsoft Windows 10 (32-bit)
 Compatibility: ESXi 5.5 and later (VM version 10)
 VMware Tools: Running, version:10341 (Current)
[More info](#)
 DNS Name: windows10
 IP Addresses: 192.168.100.130
[View all 2 IP addresses](#)
 Host: esx-02a.corp.local

CPU USAGE 1.85 GHz
 MEMORY USAGE 952 MB
STORAGE USAGE 16.12 GB

VM Hardware

> CPU	1 CPU(s)
> Memory	1 GB, 0.93 GB memory active
> Hard disk 1	32 GB
> Hard disk 2	5 GB

Notes

vCD shows Windows 8 (Windows 10 choice unavailable)
 MSDN 1511 build. Updates Dec 2016
 DHCP, NTP, holuser administrator account, remote access enabled

[Edit Notes...](#)

Custom Attributes

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

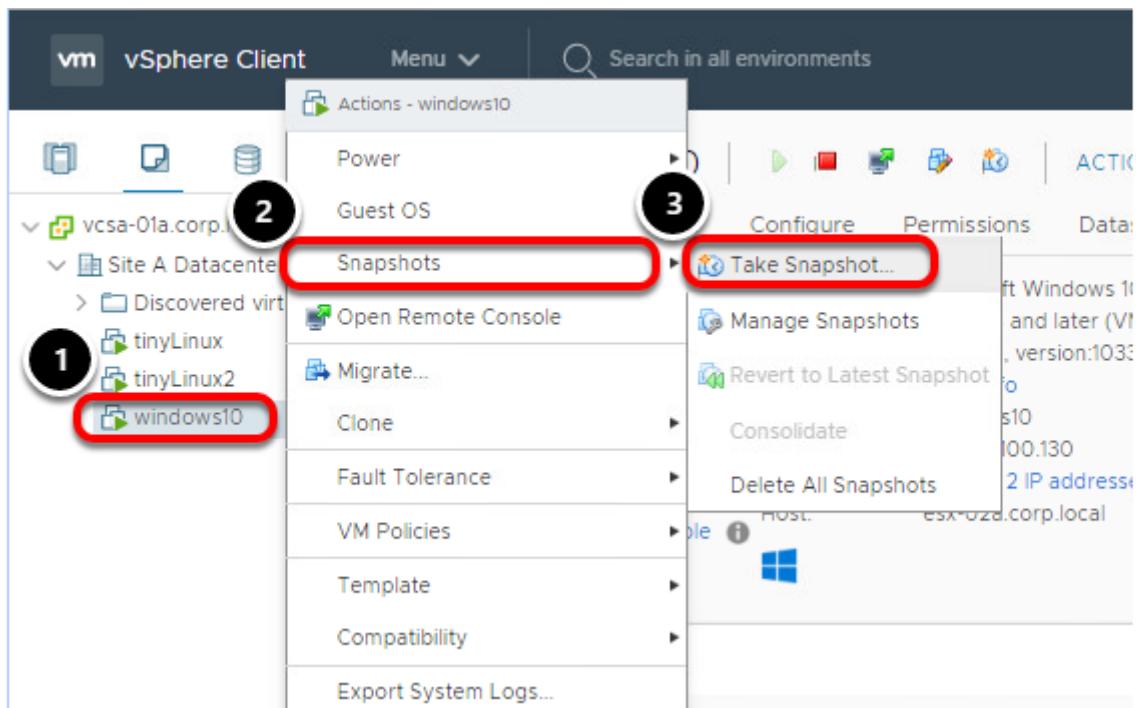
Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines. You can also take multiple snapshots of a virtual machine to create 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.

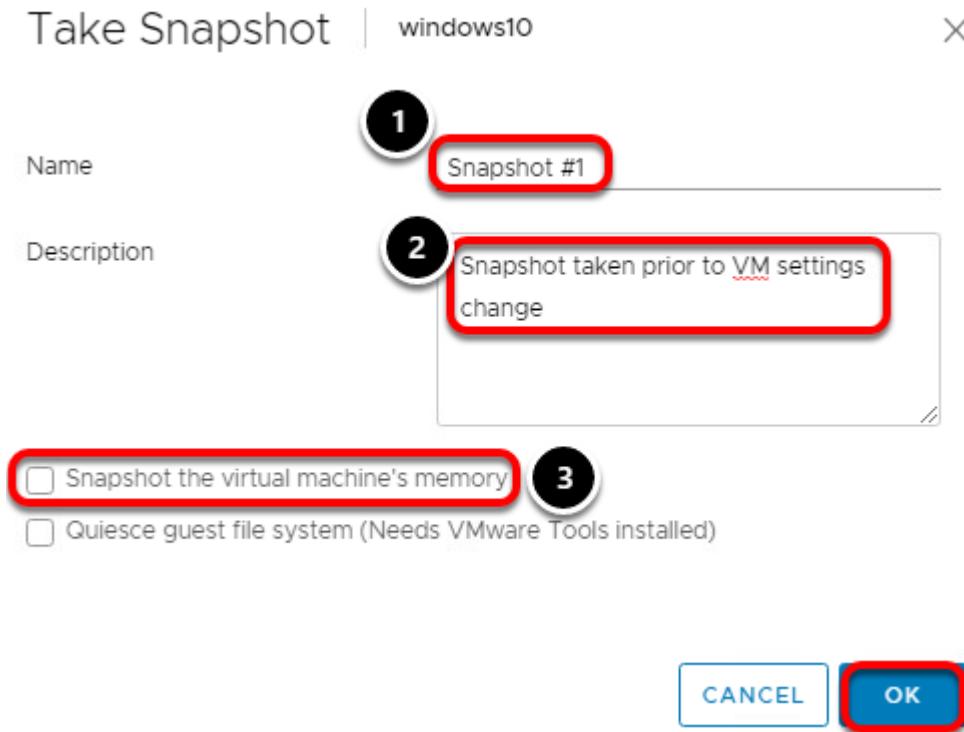
Take a Virtual Machine Snapshot



In this step, you'll take a Snapshot of a Virtual Machine.

1. Right-click **windows10**
2. Select **Snapshots**
3. Click **Take Snapshot...**

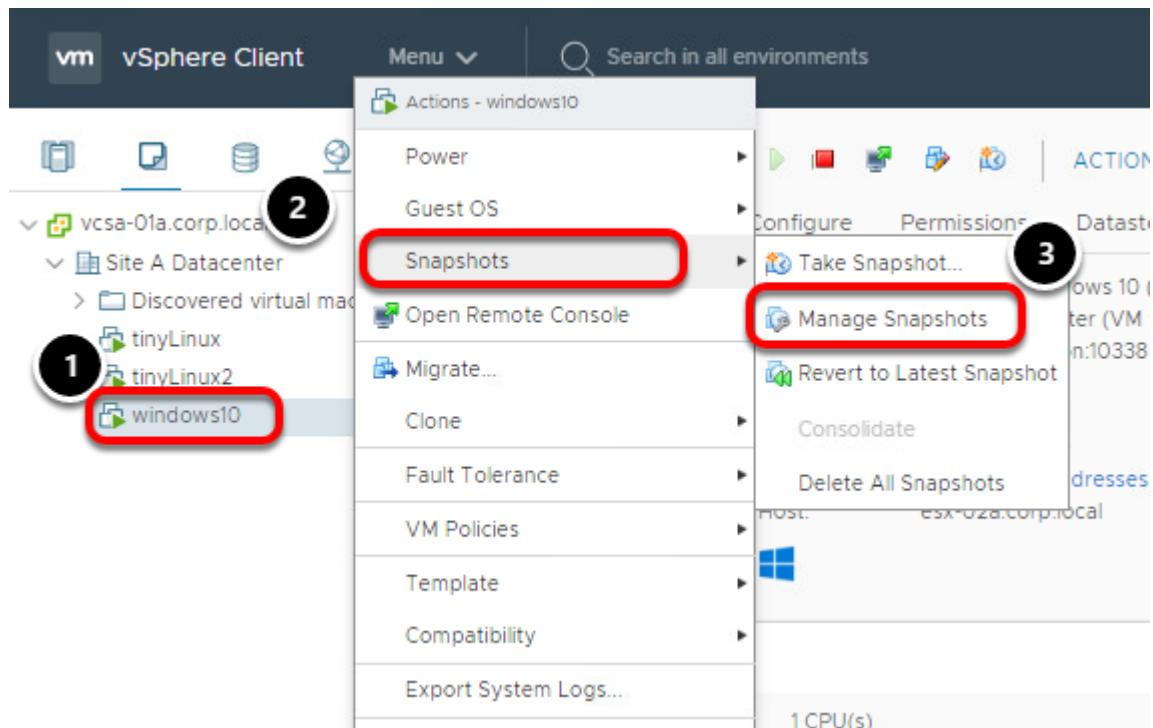
Enter a Name and Description for the VM Snapshot



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

Snapshot #1

You are here

Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	06/10/2019, 7:15:45 AM
Disk usage	10.04 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

EDIT

DELETE ALL **DELETE** **REVERT TO**

1 **DONE**

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

1 ACTIONS

2 Power

3 Power Off

Actions - windows10

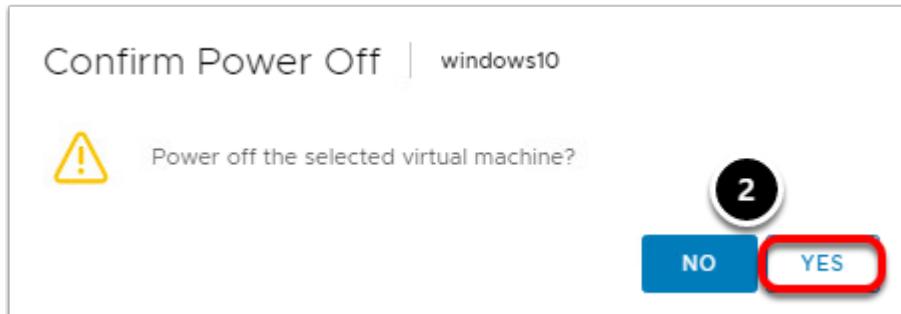
- Power On
- Power Off**
- Suspend
- Reset
- Shut Down Guest OS
- Restart Guest OS

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. From the **Actions** menu, Select **Power --> Power Off**. Select **Yes** to confirm 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.



2. Click the **Yes** button to power off the virtual machine.

Launch the Edit Settings wizard

The screenshot shows the vSphere Client interface with the following details:

- Left Panel:** Shows the inventory tree with 'vcsa-01a.corp.local' and 'Site A Datacenter' selected. Under 'Site A Datacenter', there are 'Discovered virtual machine' and 'windows10' (which is selected).
- Center Panel:** Summary tab for 'windows10' showing it is 'Powered Off'. It lists the following details:
 - Guest OS: Microsoft Windows 10 (32-bit)
 - Compatibility: ESXi 5.5 and later (VM version 1033)
 - VMware Tools: Not running, version:1033
 - DNS Name: windows10
 - IP Addresses: (empty)
 - Host: esx-02a.corp.local
- Right Panel:** Actions menu for 'windows10' with the following options:
 - Power
 - Guest OS
 - Snapshots
 - Open Remote Console
 - Migrate...
 - Clone
 - Fault Tolerance
 - VM Policies
 - Template
 - Compatibility
 - Export System L
 - Edit Settings...
 - Move to folder...

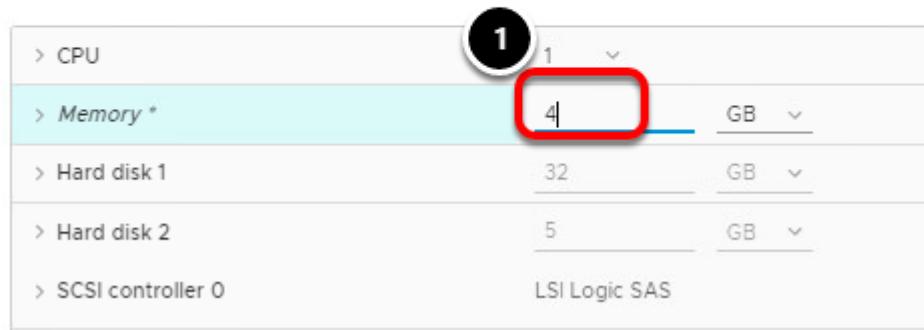
1. Click the "**Actions**" drop down menu
2. Select "**Edit Settings...**"

Change the Virtual Machine's settings

Edit Settings | windows10

Virtual Hardware

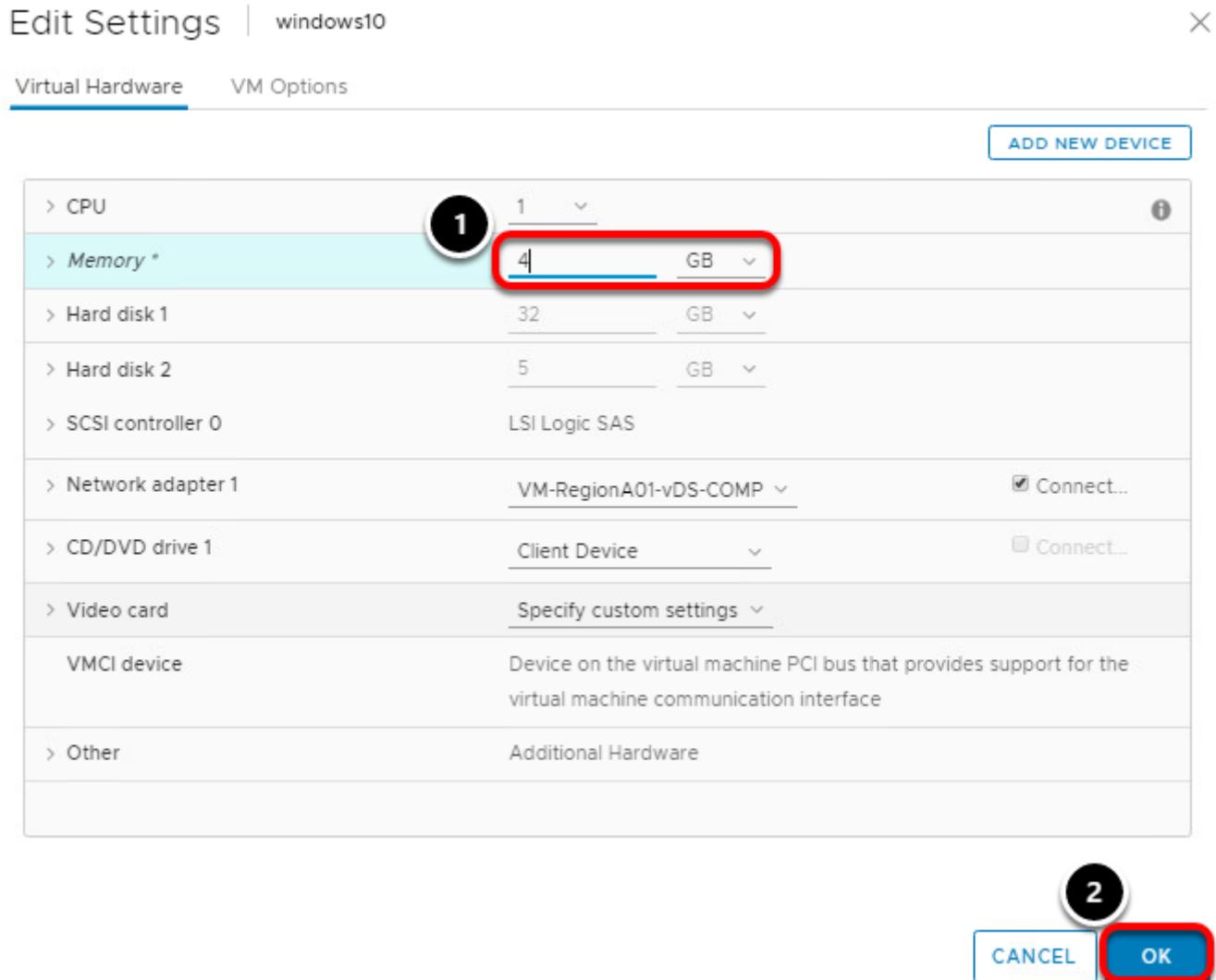
VM Options



> CPU	1	v
> Memory *	4	GB v
> Hard disk 1	32	GB v
> Hard disk 2	5	GB v
> SCSI controller 0	LSI Logic SAS	

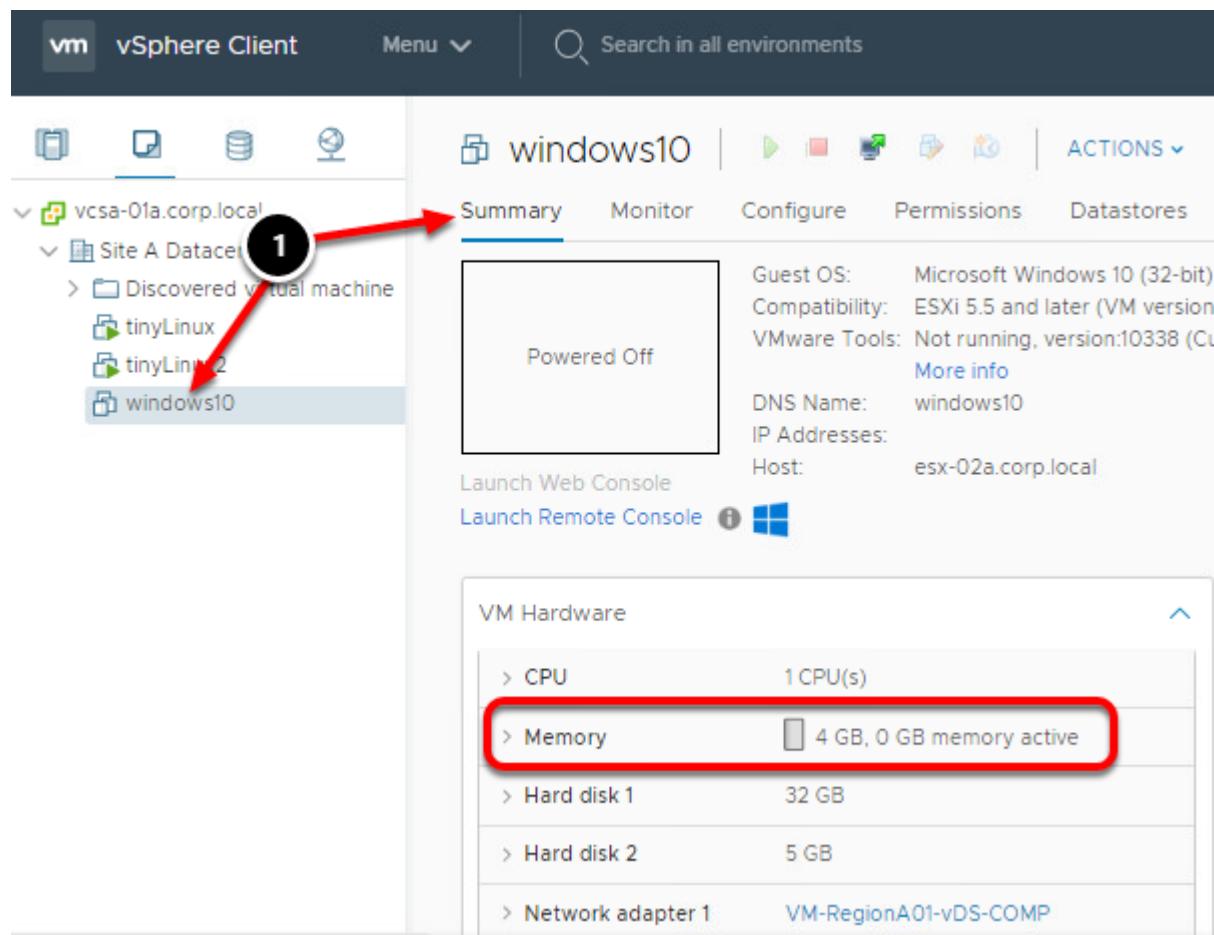
1. In the Memory field, change this setting to "4".

Review the Virtual Machine's new settings



1. Note the new Memory configuration
2. Click **OK** to continue.

Summary tab



1

windows10

Summary Monitor Configure Permissions Datastores

Powered Off

Guest OS: Microsoft Windows 10 (32-bit)
Compatibility: ESXi 5.5 and later (VM version)
VMware Tools: Not running, version:10338 (CU)
More info
DNS Name: windows10
IP Addresses:
Host: esx-02a.corp.local

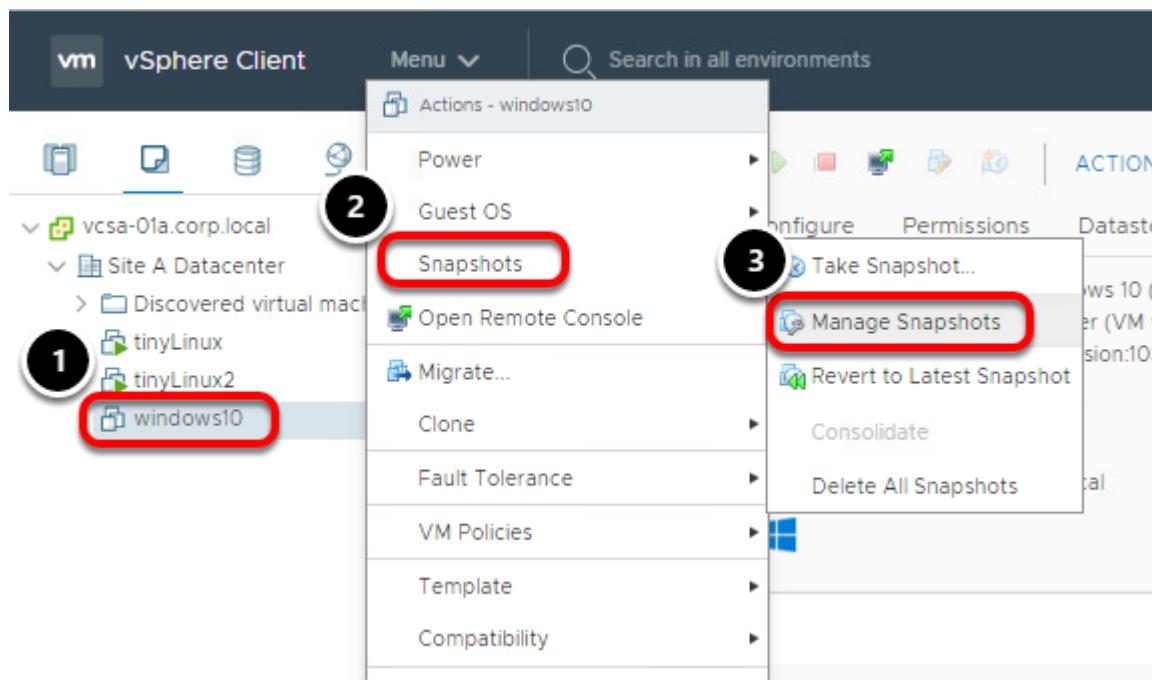
Launch Web Console
Launch Remote Console

VM Hardware

> CPU	1 CPU(s)
> Memory	4 GB, 0 GB memory active
> Hard disk 1	32 GB
> Hard disk 2	5 GB
> Network adapter 1	VM-RegionA01-vDS-COMP

1. Make sure you are on the **Summary** tab for **windows10** and verify the memory has been updated.

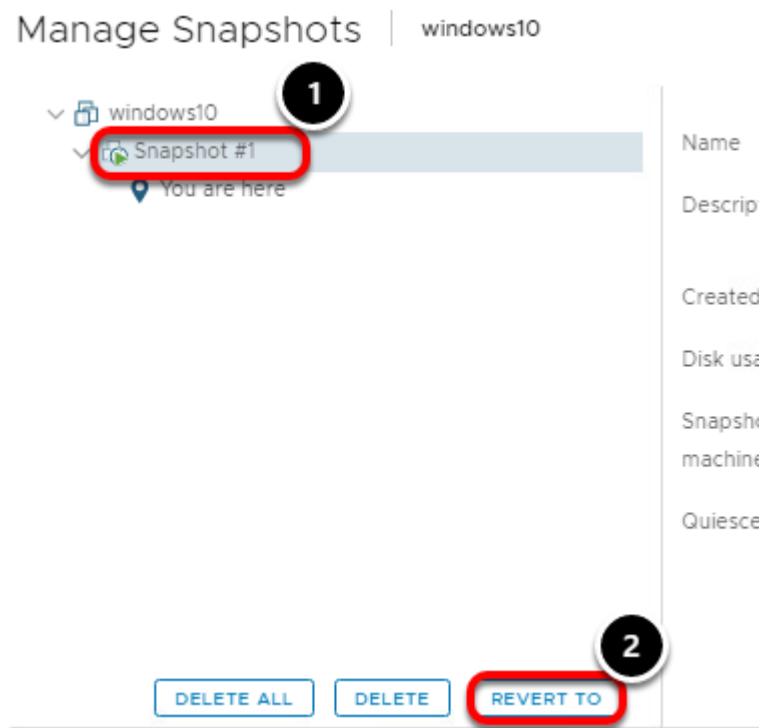
Revert Virtual Machine settings using the Snapshot Manager



In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

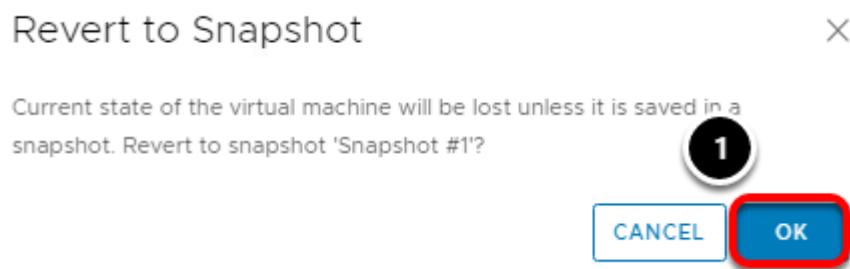
1. Right-click **windows10**
2. Select **Snapshots**
3. Click **Manage Snapshots**

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

Manage Snapshots windows10 X

windows10

Snapshot #1 You are here

Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	06/10/2019, 7:15:45 AM
Disk usage	10.04 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

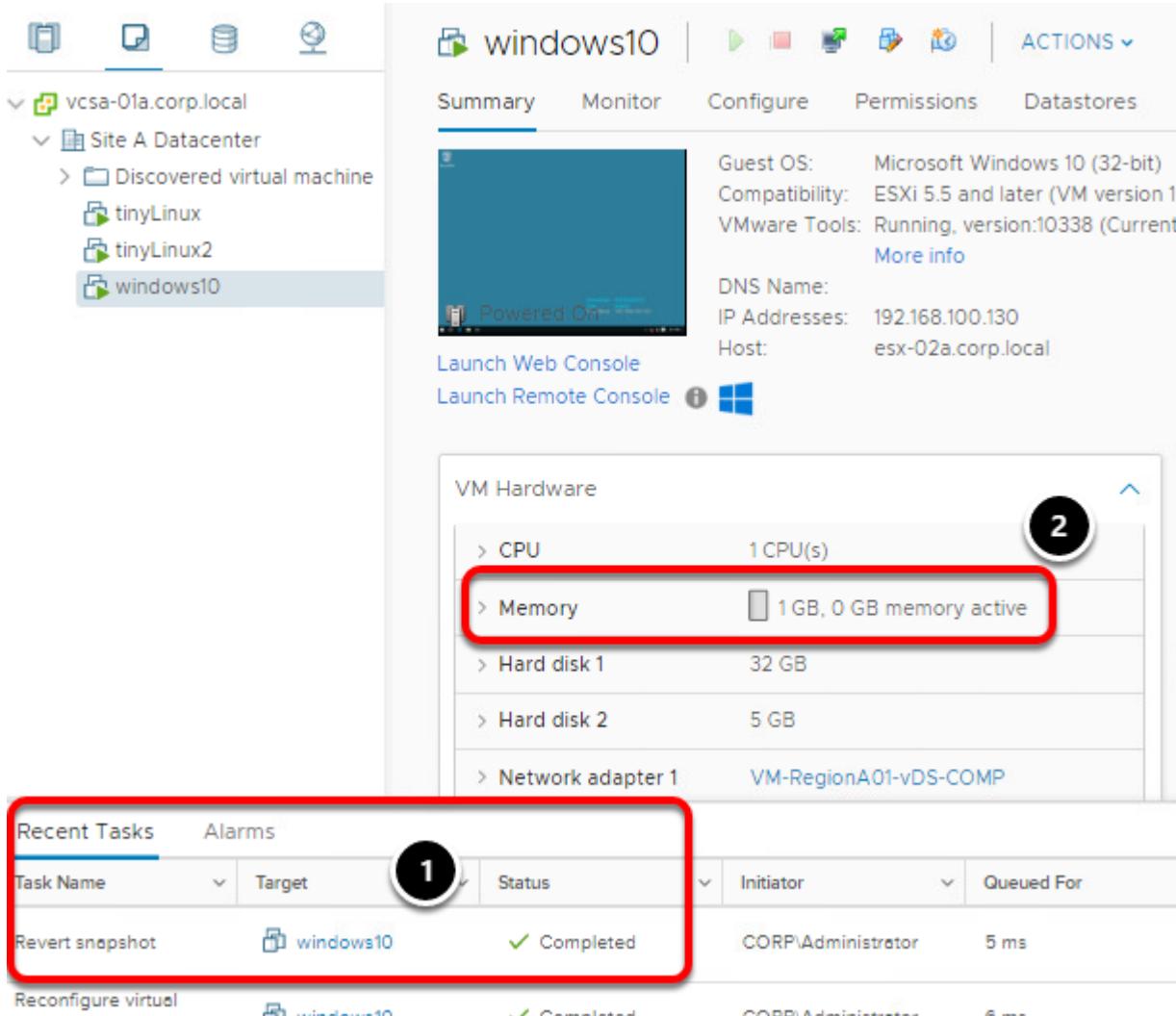
EDIT

DELETE ALL DELETE REVERT TO

1 DONE

1. Click **Done** to close the Snapshot window.

Monitor task progress



The screenshot shows the vSphere Web Client interface. On the left, the navigation tree shows a vCenter server named 'vcsa-01a.corp.local' with a datacenter named 'Site A Datacenter' containing several virtual machines: 'tinyLinux', 'tinyLinux2', and 'windows10'. The 'windows10' VM is selected and highlighted.

The main content area displays the 'Summary' tab for the 'windows10' VM. It shows the guest OS as 'Microsoft Windows 10 (32-bit)', compatibility as 'ESXi 5.5 and later (VM version 10338)', and VMware Tools status as 'Running, version:10338 (Current)'. Other details include DNS name, IP addresses (192.168.100.130), and host (esx-02a.corp.local).

Below the summary, the 'VM Hardware' section is shown. It lists the following components and their configurations:

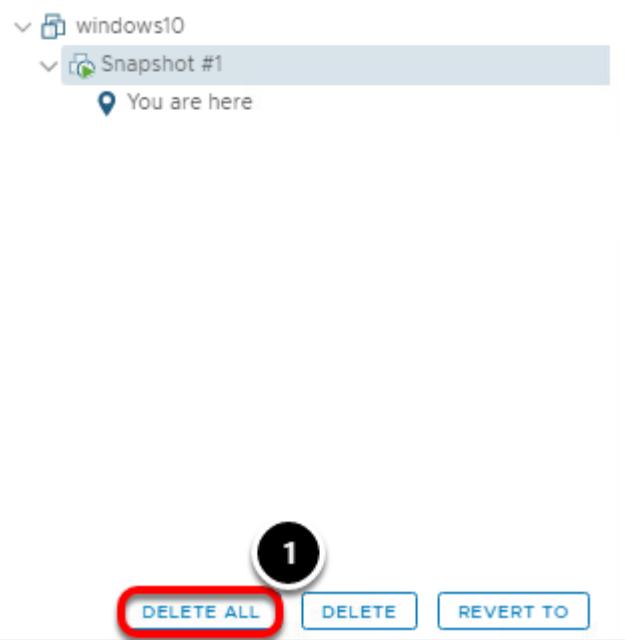
- CPU: 1 CPU(s)
- Memory: 1 GB, 0 GB memory active (highlighted with a red box and circled with a number 2)
- Hard disk 1: 32 GB
- Hard disk 2: 5 GB
- Network adapter 1: VM-RegionA01-vDS-COMP

The 'Recent Tasks' pane at the bottom shows a completed task: 'Revert snapshot' for the 'windows10' VM, initiated by 'CORP\Administrator' and completed in 5 ms. This task is also highlighted with a red box and circled with a number 1.

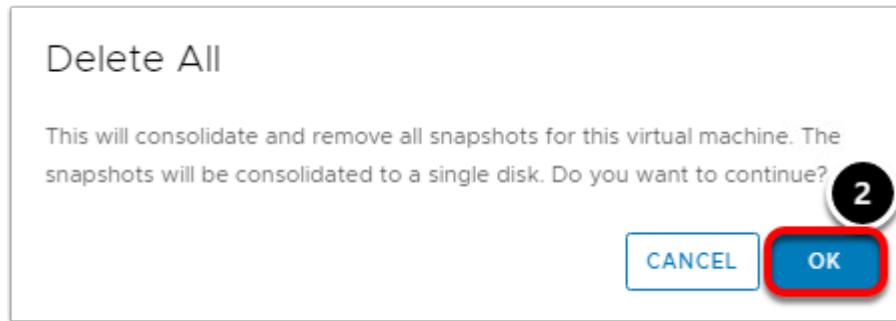
1. Note the progress in the **Recent Tasks** pane.
2. Note the Memory configuration has reverted back to **1 GB**.

Delete Snapshot #1

Manage Snapshots | windows10



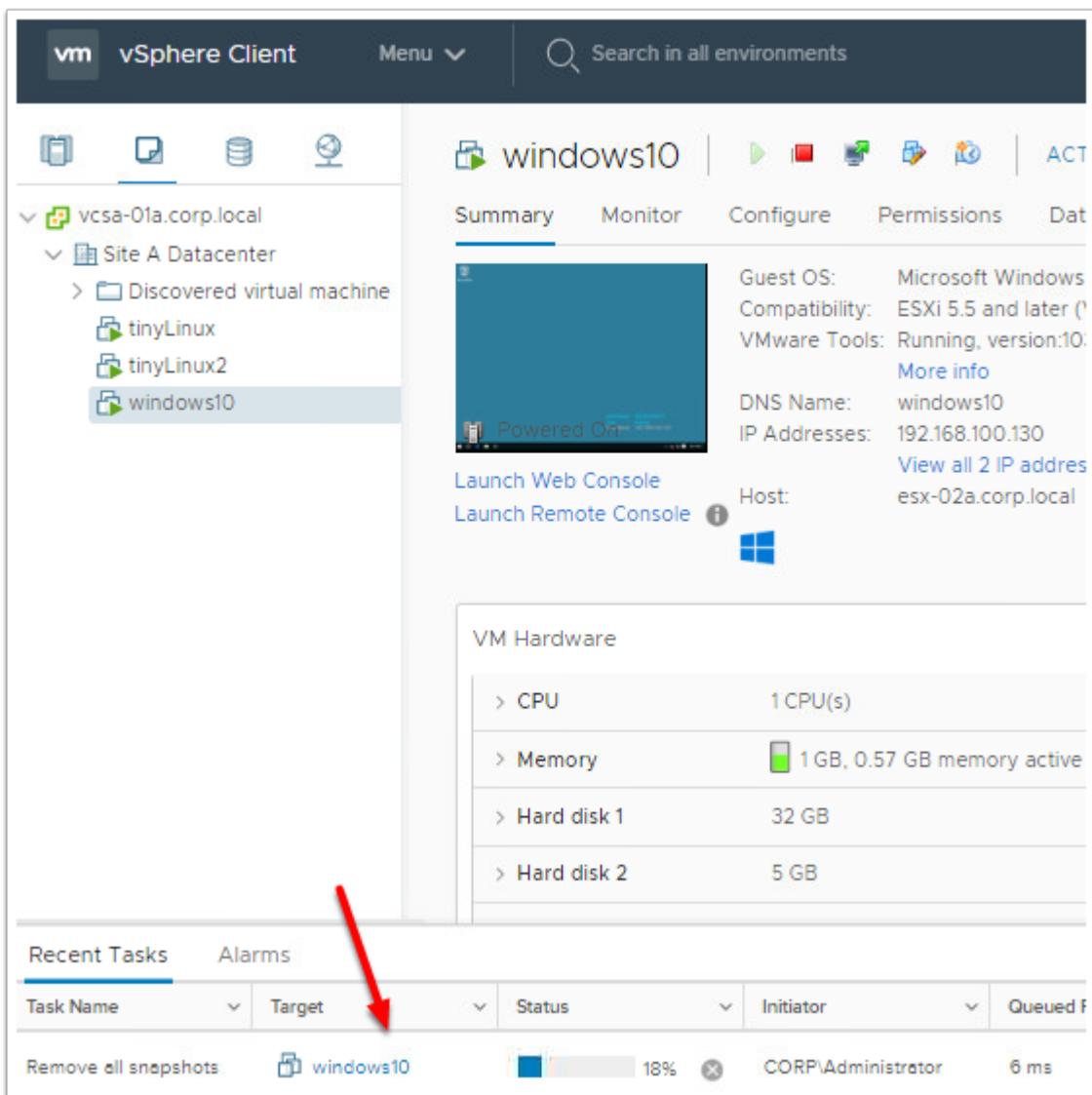
1. Click the **Delete All** button to remove the snapshot.



2. Click **OK** to confirm the deletion of all the snapshots.

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 navigation tree shows a datacenter with three virtual machines: tinyLinux, tinyLinux2, and windows10. The windows10 entry is selected. The main pane displays the 'Summary' tab for the windows10 VM. The VM is shown as 'Powered On'. The 'VM Hardware' section lists the CPU (1 CPU(s)), Memory (1GB, 0.57 GB memory active), Hard disk 1 (32 GB), and Hard disk 2 (5 GB). At the bottom of the screen, the 'Recent Tasks' table is visible, showing a task named 'Remove all snapshots' for the windows10 VM. A red arrow points to the progress bar of this task, which is currently at 18%. The task was initiated by 'CORP\Administrator' and has been running for 6 ms.

Task Name	Target	Status	Initiator	Queued For
Remove all snapshots	windows10	18%	CORP\Administrator	6 ms

You can watch the progress of the snapshot being deleted in the Recent Tasks window.

Video: More on Virtual Machine Snapshots (2:33)

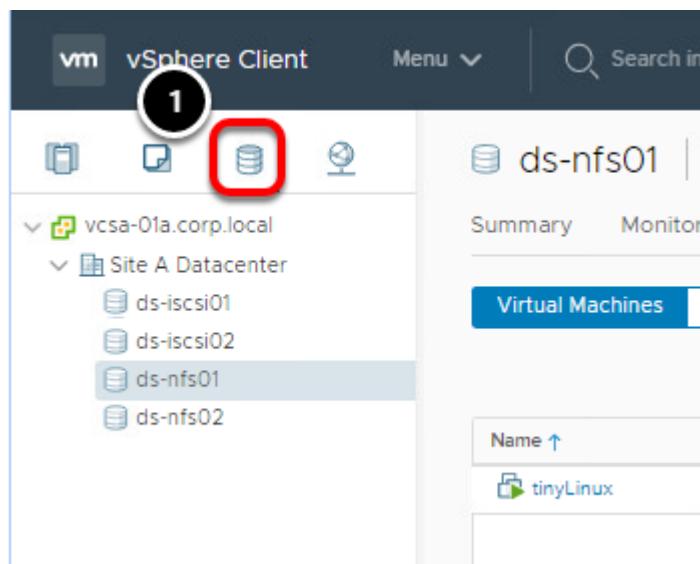
For more information on vSphere Virtual Machine Snapshots, be sure to check out this video.

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.

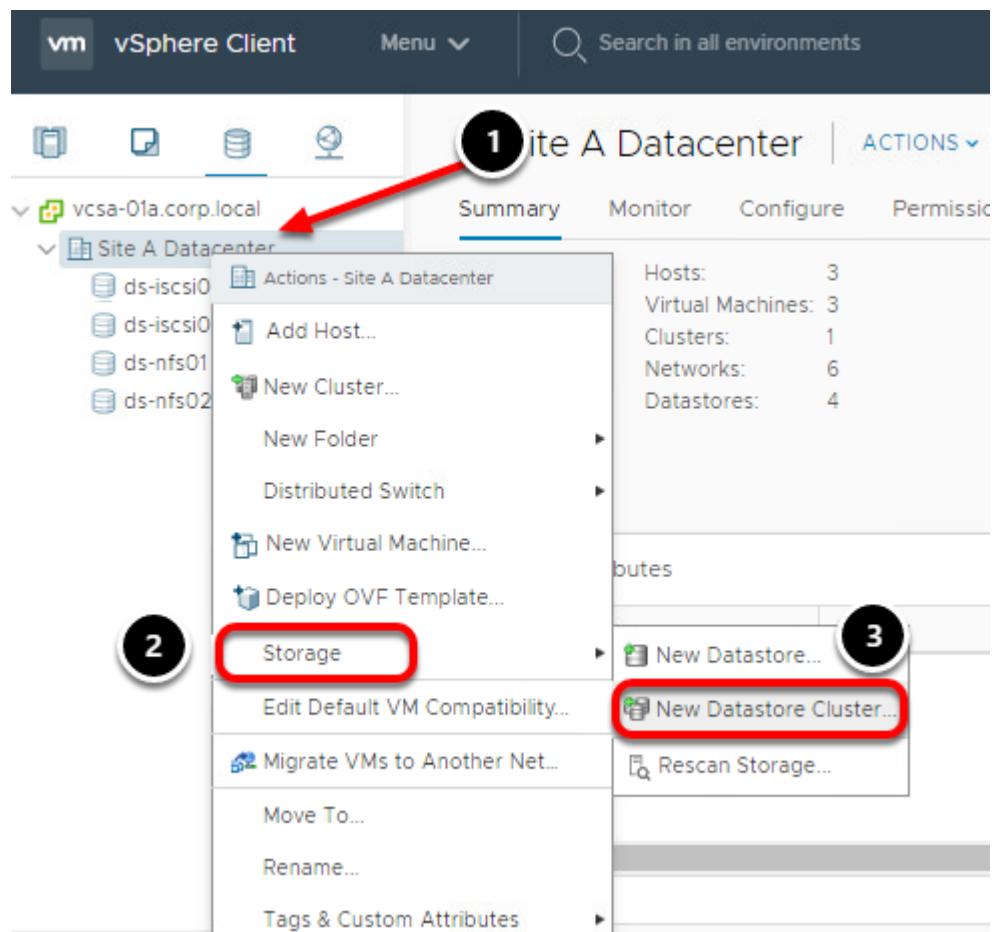
In this section, you will create a vSphere Datastore Cluster using two iSCSI datastores.

Navigate to Storage



1. Click on the **Storage** icon.

New Datastore Cluster



1. Right Click on **Site A Datacenter**
2. Select **Storage**
3. Click **New Datastore Cluster...**

New Datastore Cluster - Name and Location

New Datastore Cluster

1 Name and Location

2 Storage DRS Automation

3 Storage DRS Runtime Set...

4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Name and Location 1

Datastore cluster name: **DatastoreCluster-01**

Location: Site A Datacenter

Turn ON Storage DRS

vSphere Storage DRS enables vCenter Server to manage datastores as an aggregate pool of storage resources.

vSphere Storage DRS also enables vCenter Server to manage the assignment of virtual machines to datastores, suggesting placement when virtual machines are created, migrated or cloned, and migrating running virtual machines to balance load and enforce placement rules.

2

CANCEL BACK NEXT

1. Enter **DatastoreCluster-01** for the name.
2. Select **Next**.

New Datastore Cluster - Storage DRS Automation

New Datastore Cluster

✓ 1 Name and Location
✓ 2 Storage DRS Automation
3 Storage DRS Runtime Set...
4 Select Clusters and Hosts
5 Select Datastores
6 Ready to Complete

Storage DRS Automation

Cluster automation level

No Automation (Manual Mode)
vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.

Fully Automated
Files will be migrated automatically to optimize resource usage.

Space balance automation level

I/O balance automation level

Rule enforcement automation level

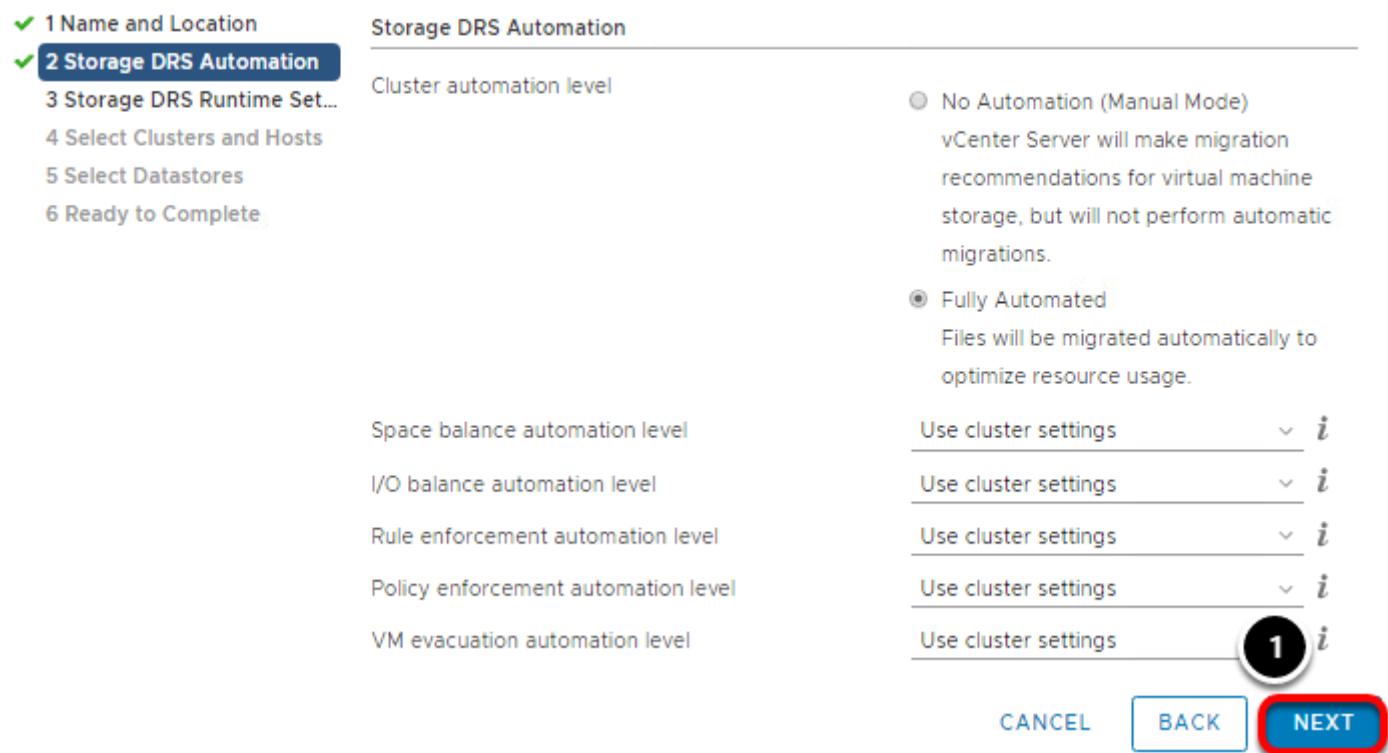
Policy enforcement automation level

VM evacuation automation level

Use cluster settings *i*

1 *i*

CANCEL **BACK** **NEXT**



1. Leave the defaults settings and select **Next**.

New Datastore Cluster - Storage DRS Runtime Settings

New Datastore Cluster

✓ 1 Name and Location
 ✓ 2 Storage DRS Automation
✓ 3 Storage DRS Runtime Set...
 4 Select Clusters and Hosts
 5 Select Datastores
 6 Ready to Complete

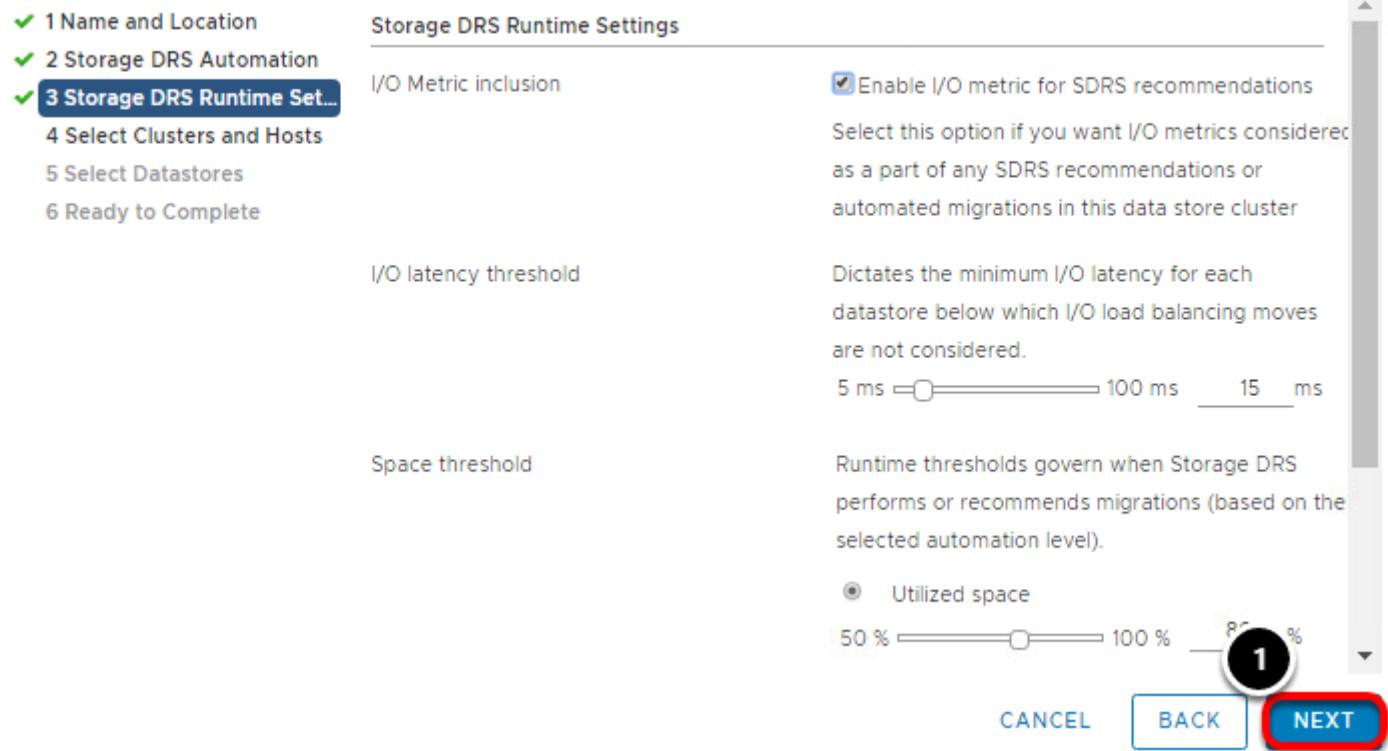
Storage DRS Runtime Settings

I/O Metric inclusion Enable I/O metric for SDRS recommendations
 Select this option if you want I/O metrics considered as a part of any SDRS recommendations or automated migrations in this data store cluster

I/O latency threshold
 Dictates the minimum I/O latency for each datastore below which I/O load balancing moves are not considered.
 5 ms 100 ms 15 ms

Space threshold
 Runtime thresholds govern when Storage DRS performs or recommends migrations (based on the selected automation level).
 Utilized space
 50 % 100 % 1 %

CANCEL **BACK** **NEXT**



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

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Set...
- ✓ 4 Select Clusters and Hosts**
- 5 Select Datastores
- 6 Ready to Complete

Select Clusters and Hosts

Filter Selected (1)

Clusters Standalone Hosts

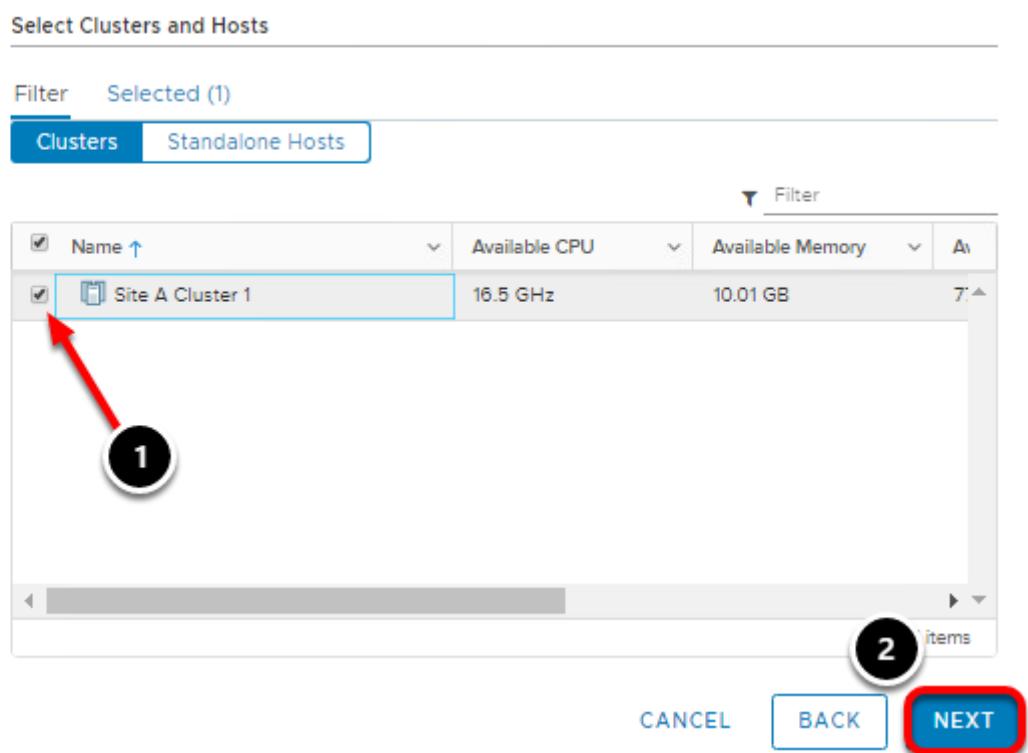
Filter

Name	Available CPU	Available Memory	Actions
Site A Cluster 1	16.5 GHz	10.01 GB	7 items

1

2

CANCEL BACK NEXT



1. Because there are no standalone hosts, please select **Site A Cluster**.
2. Click the **Next** button.

New Datastore Cluster - Select Datastores

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Set...
- ✓ 4 Select Clusters and Hosts
- ✓ 5 Select Datastores**

6 Ready to Complete

Select Datastores

Show datastores connected to all hosts ▾

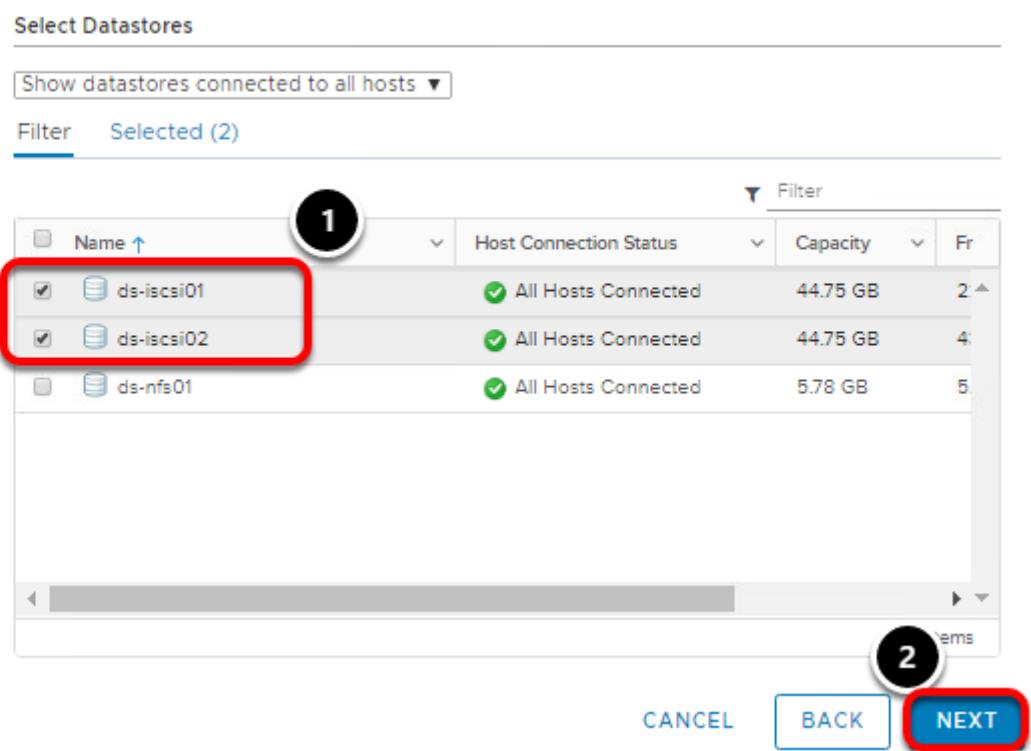
Filter Selected (2)

1

Name	Host Connection Status	Capacity	Fr
ds-iscsi01	All Hosts Connected	44.75 GB	2
ds-iscsi02	All Hosts Connected	44.75 GB	4
ds-nfs01	All Hosts Connected	5.78 GB	5

2

CANCEL BACK NEXT



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

✓ 1 Name and Location
 ✓ 2 Storage DRS Automation
 ✓ 3 Storage DRS Runtime Set...
 ✓ 4 Select Clusters and Hosts
 ✓ 5 Select Datastores
6 Ready to Complete

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-iscsi02	44.75 GB	43.34 GB	VMFS 6

FINISH (highlighted with a red circle)

1. Review the Storage DRS settings and click the **Finish** button.

New Datastore Cluster- Summary

Task Name	Target	Status
Move datastores into a datastore cluster	DatastoreCluster...	Completed
Configure Storage DRS	DatastoreCluster...	Completed
Create a datastore cluster	Site A Datacenter	Completed

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.

Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit <http://hol.vmware.com/> to continue your lab experience online.

Lab SKU: HOL-2010-01-SDC

Version: 20190914-211504