HANDS-ON LABS MANUAL - 2023

HOL-2210-01-SDC

Virtualization 101: Introduction to vSphere

vmware®

Table of contents

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

Virtualization

[2]

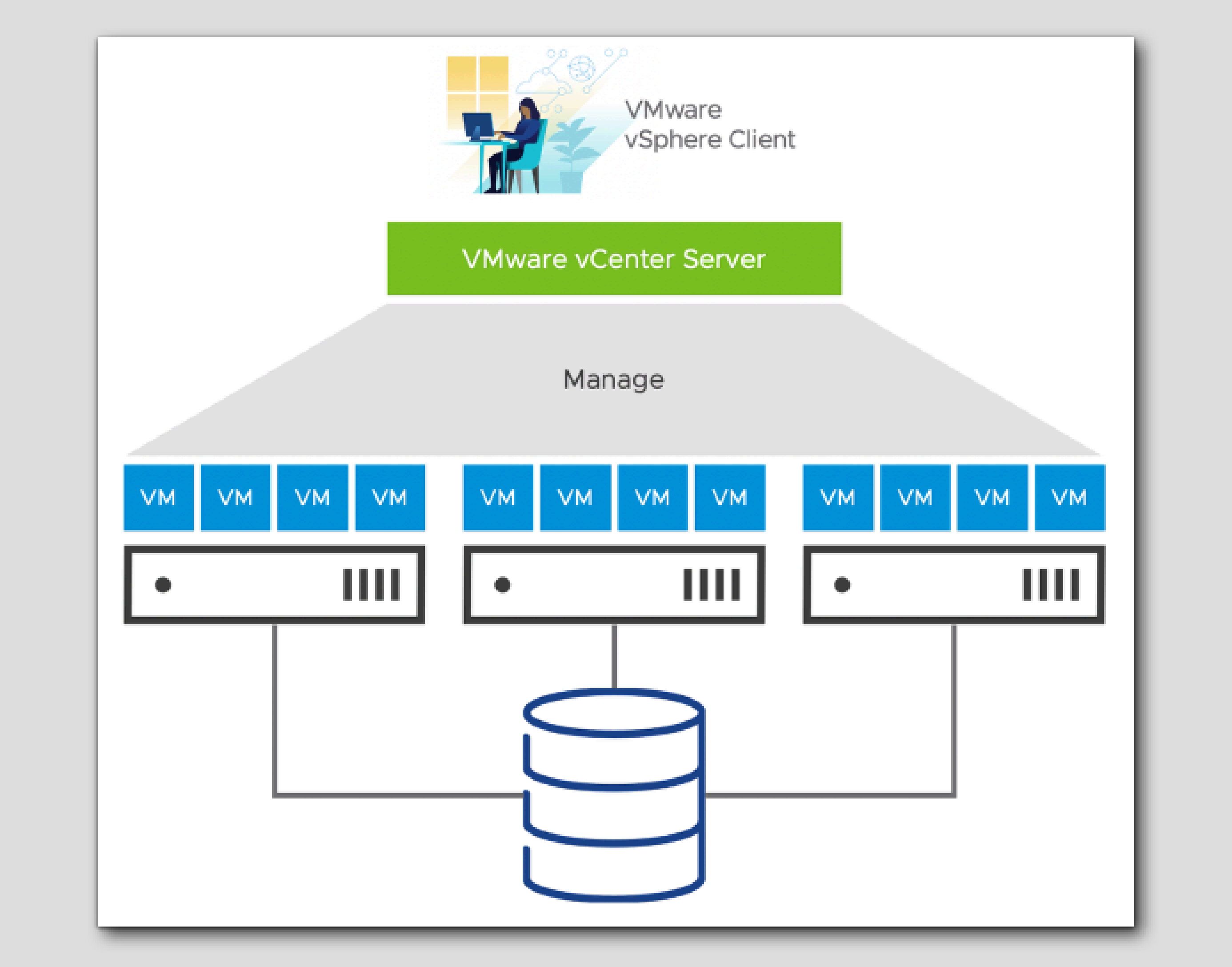
If you are not familiar with Virtualization, this lesson will give you an introduction to it.

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

What is Virtualization:

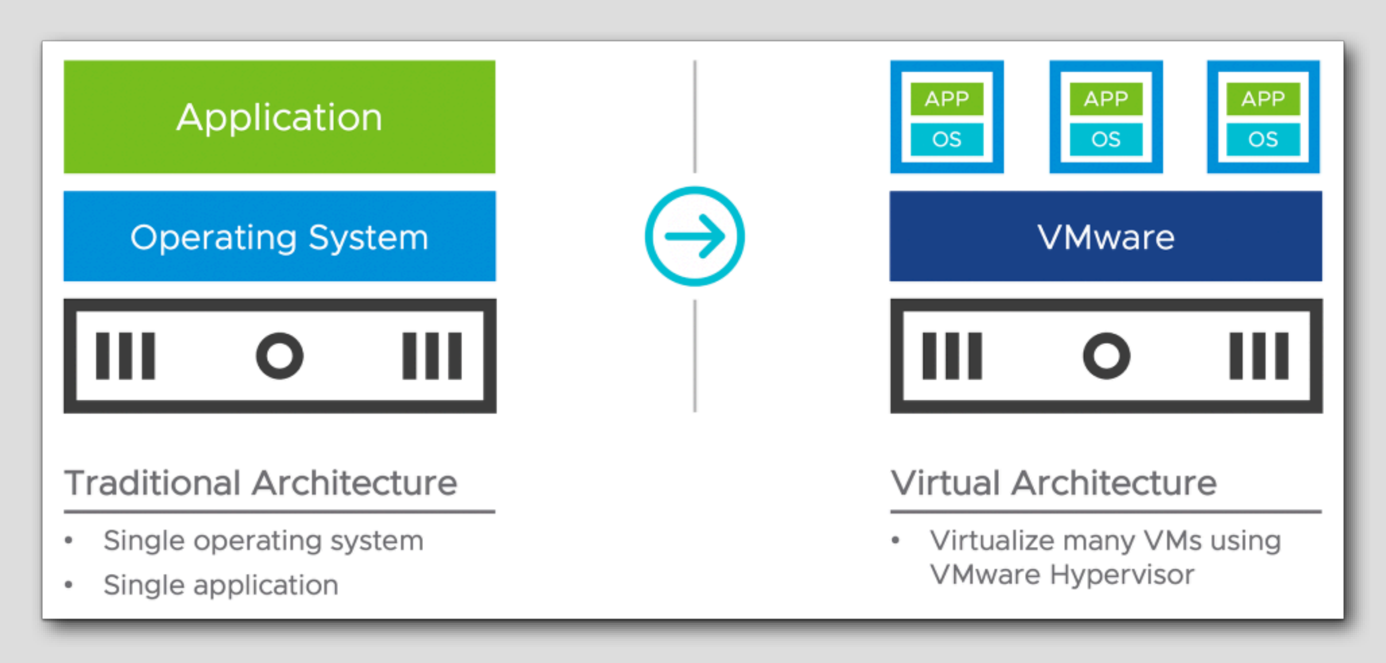
[3]

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


VMware
vSphere Client
VMware vCenter Server
Manage
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM

Virtualization Defined

[4]



Traditional Architecture

- Single operating system
- Single application

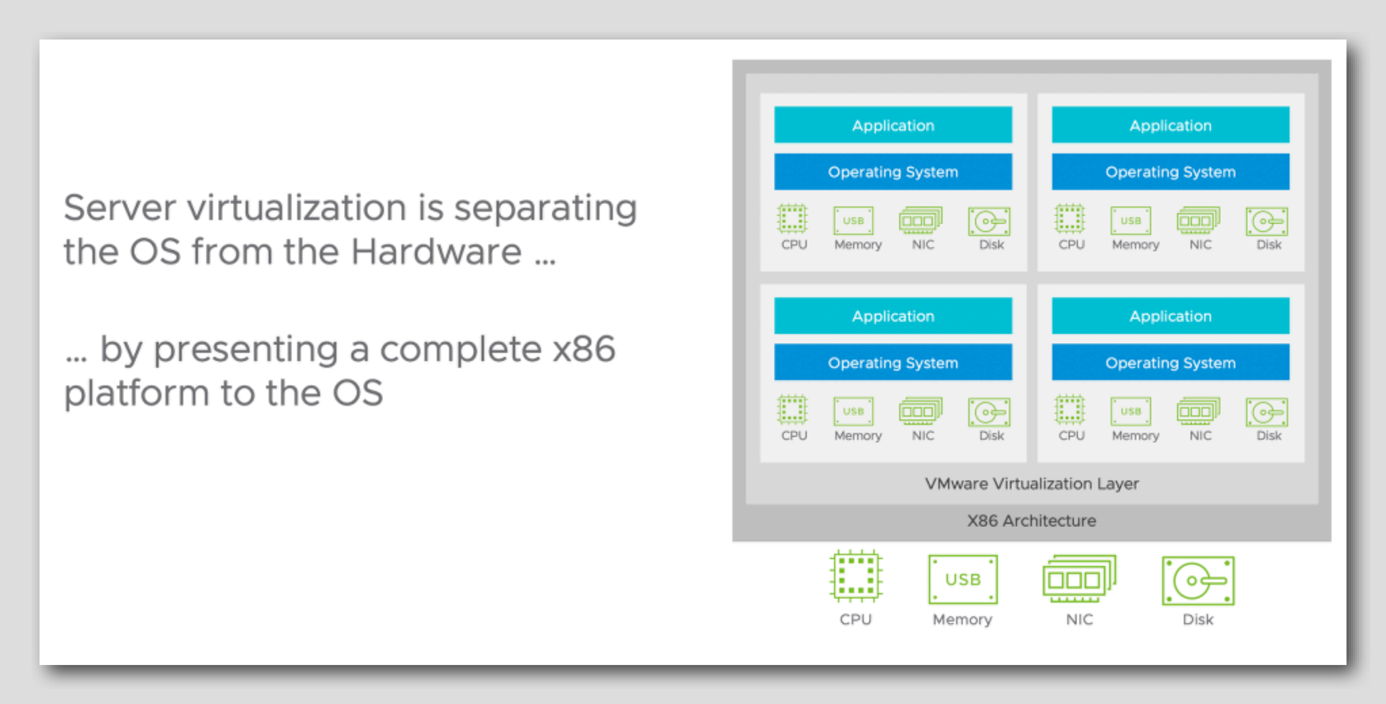
Virtual Architecture

- Virtualize many VMs using VMware Hypervisor

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

[5]



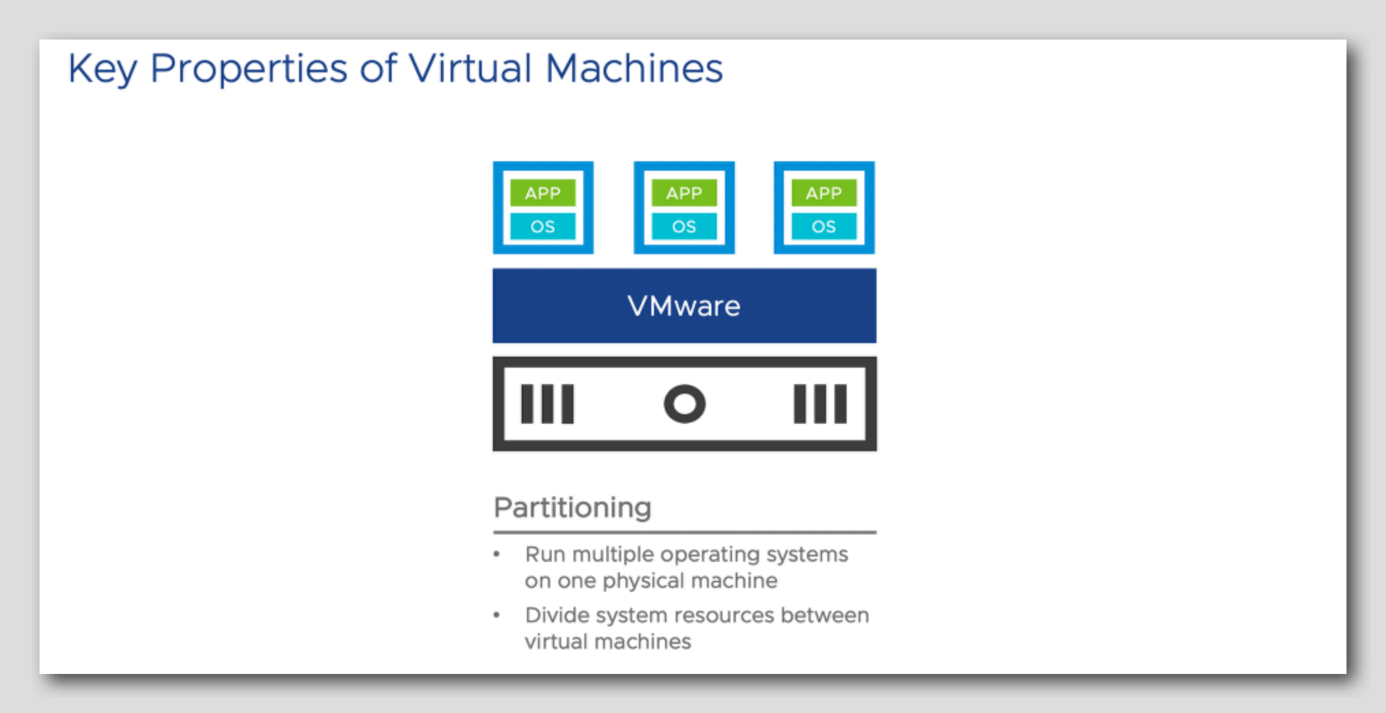
Server virtualization is separating the OS from the Hardware ...

... 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

[6]



Key Properties of Virtual Machines

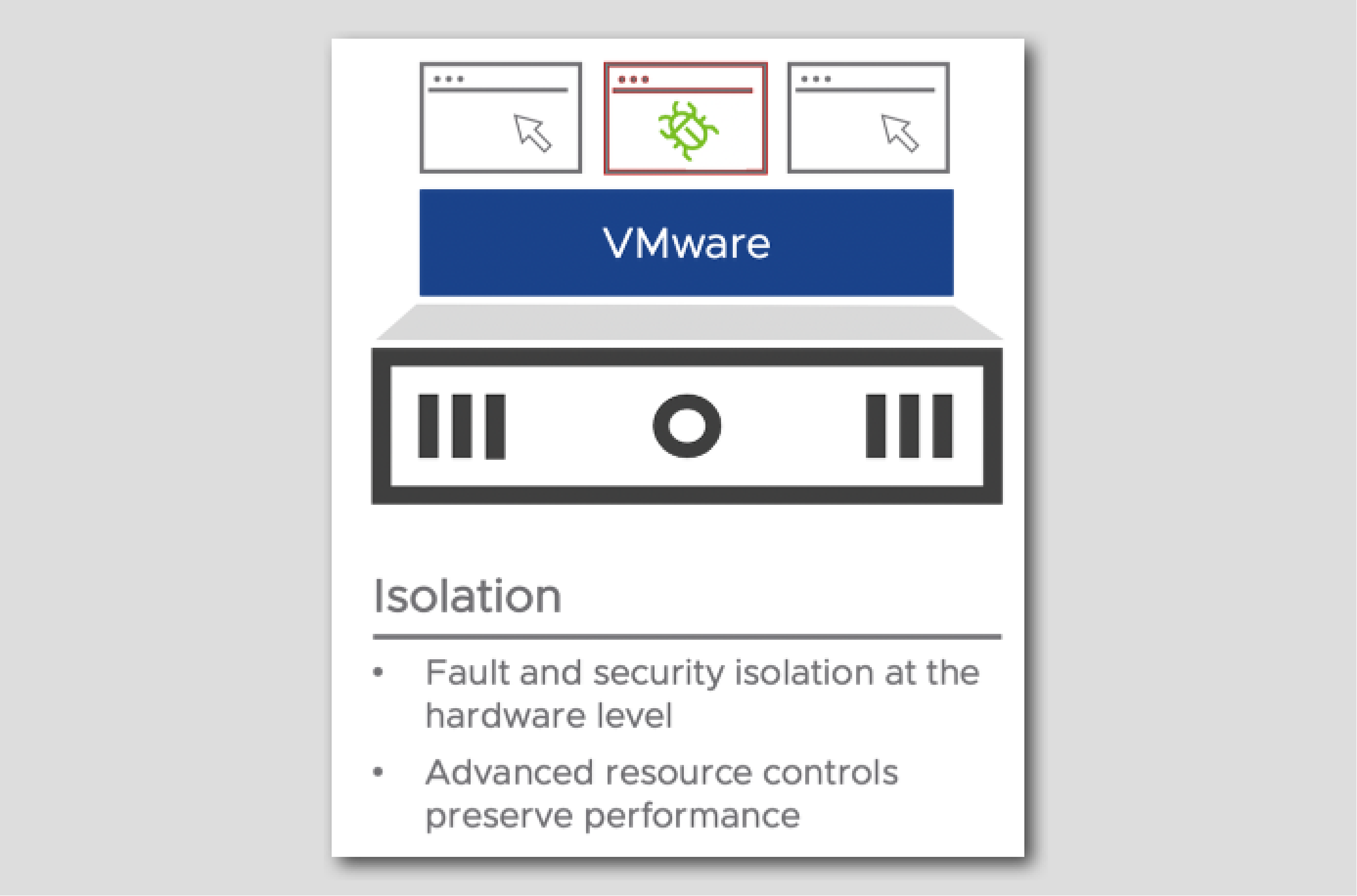
Partitioning

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

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

Isolation

[7]



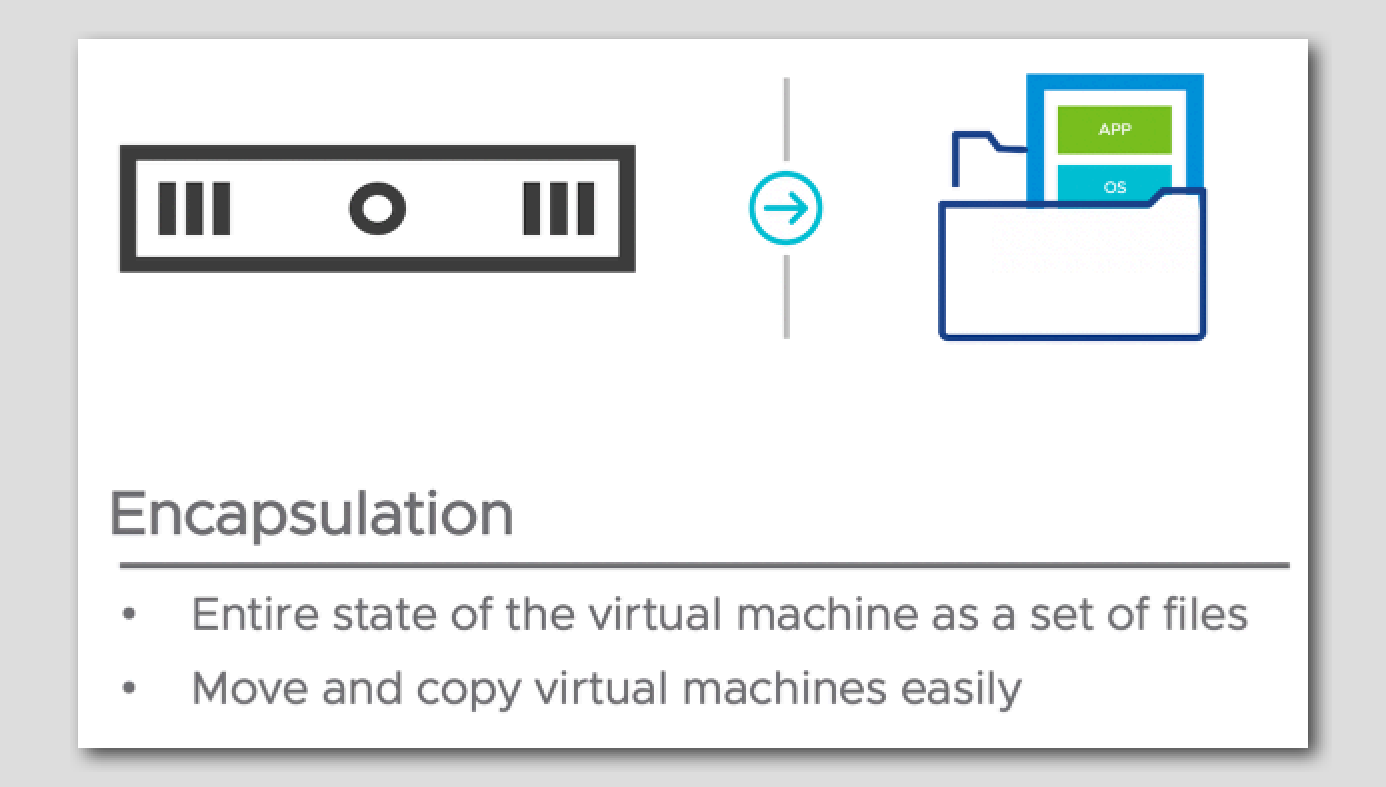
Isolation

- 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

[8]



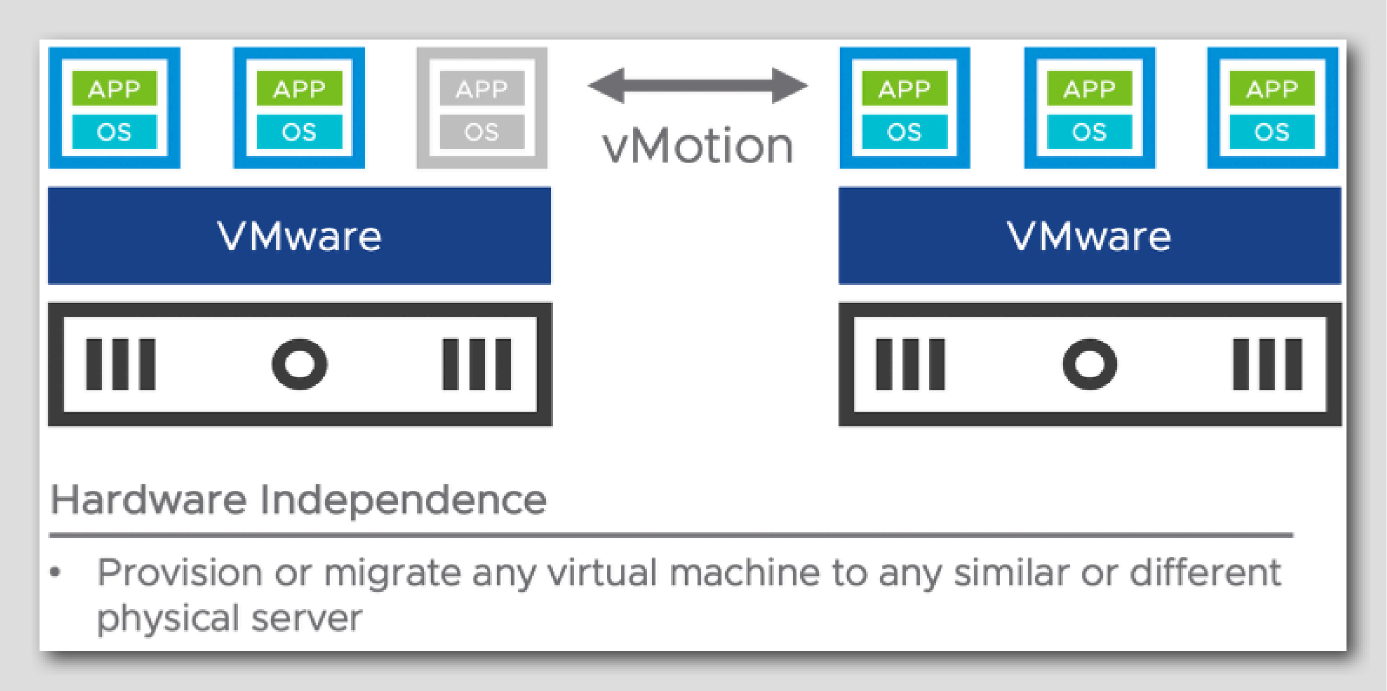
Encapsulation

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

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

Hardware Independence

[9]



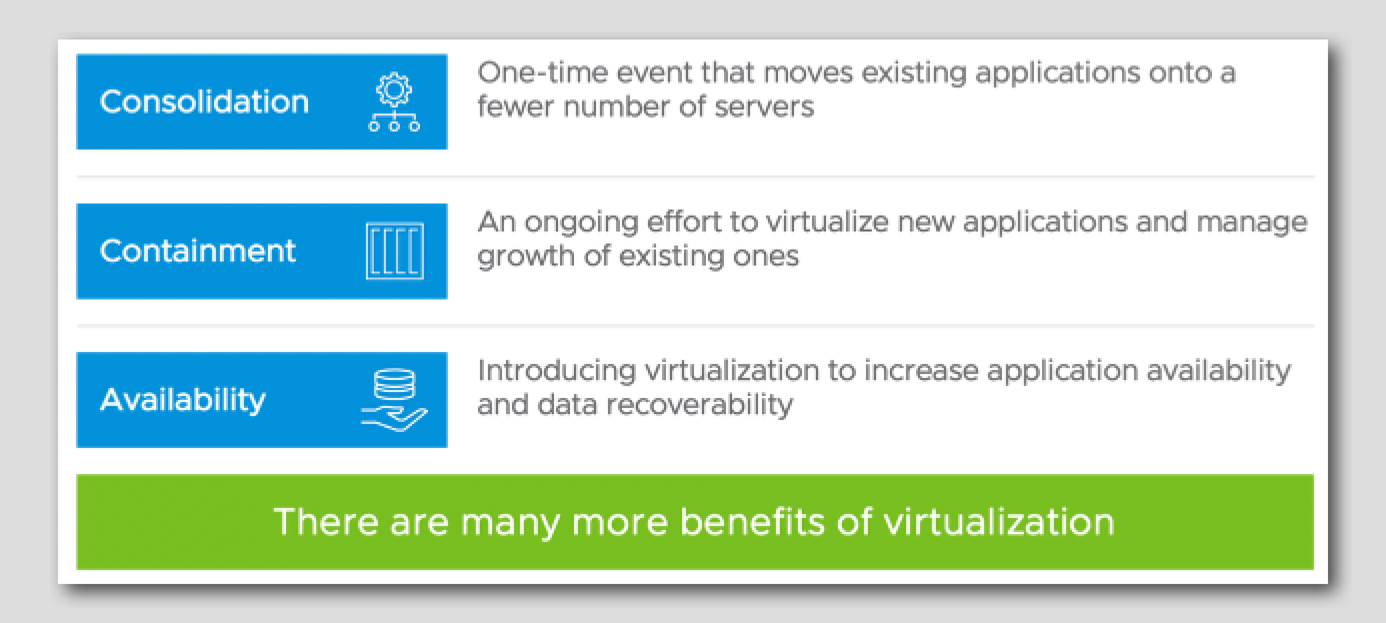
Hardware Independence

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

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

Benefits

[10]



Consolidation One-time event that moves existing applications onto a fewer number of servers

Containment An ongoing effort to virtualize new applications and manage growth of existing ones

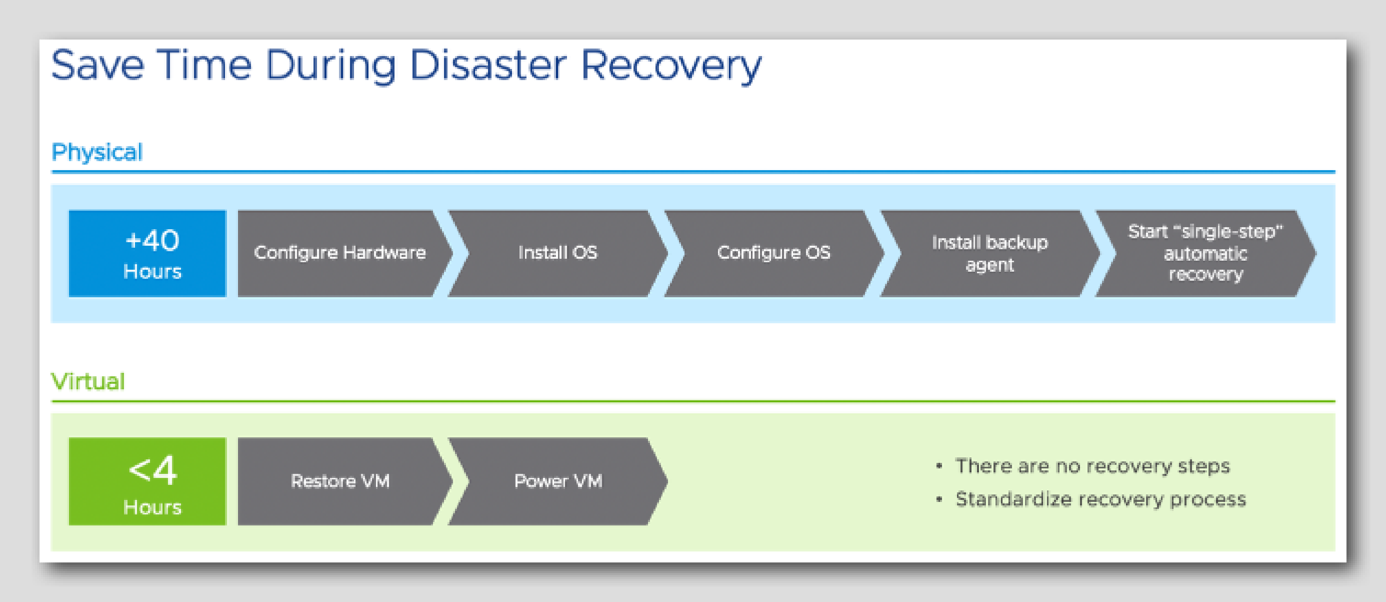
Availability Introducing virtualization to increase application availability and data recoverability

There are many more benefits of virtualization

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

Simplify Recovery

[11]



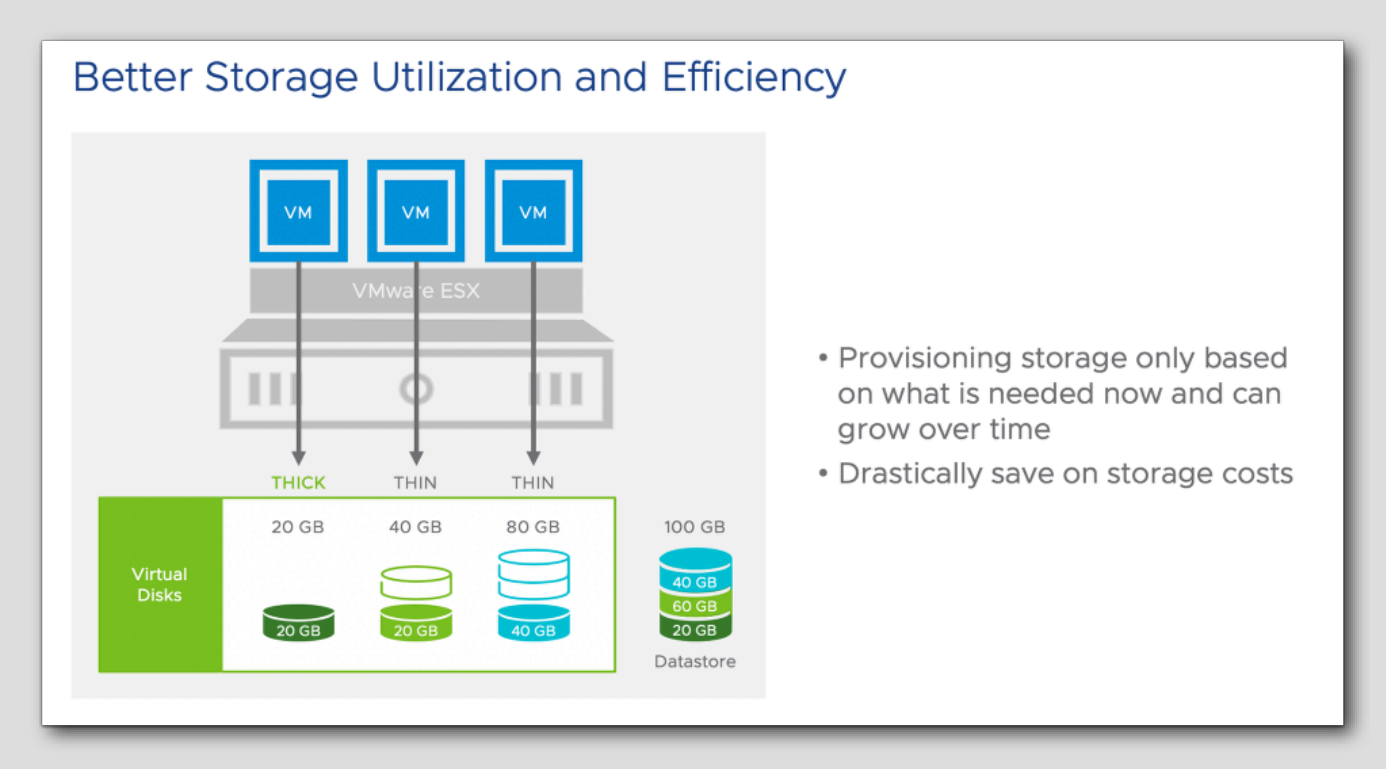
Save Time During Disaster Recovery

- There are no recovery steps
- Standardize recovery process

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

[12]



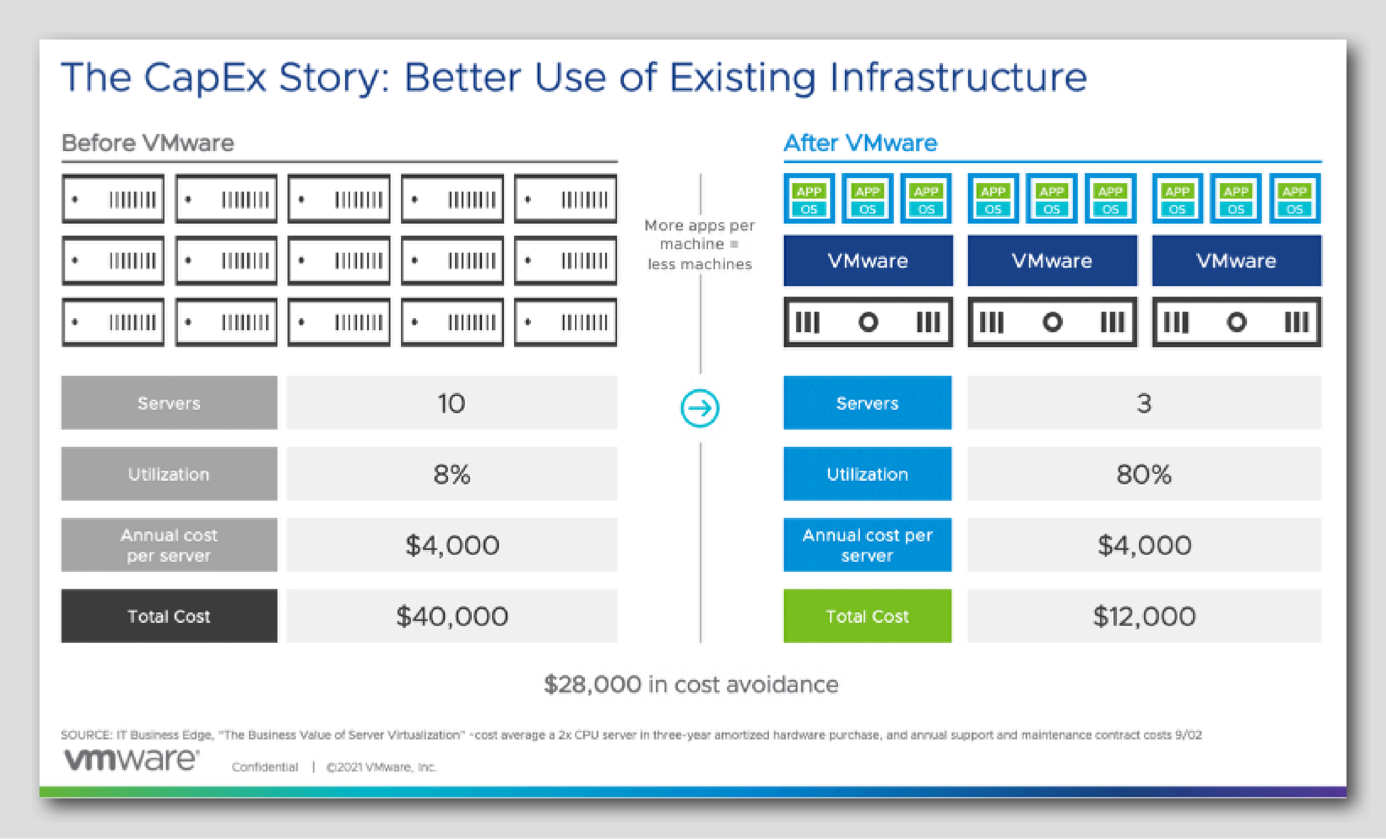
Better Storage Utilization and Efficiency

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

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

Cost Avoidance

[13]



The CapEx Story: Better Use of Existing Infrastructure

Before VMware

After VMware

More apps per machine = less machines

Before VMware		After VMware	
Servers	10	Servers	3
Utilization	8%	Utilization	80%
Annual cost per server	$4,000	Annual cost per server	$4,000
Total Cost	$40,000	Total Cost	$12,000

$28,000 in cost avoidance

SOURCE: IT Business Edge, "The Business Value of Server Virtualization" -cost average a 2x CPU server in three-year amortized hardware purchase, and annual support and maintenance contract costs 9/02

vmware Confidential | ©2021 VMware, Inc.

Lab Guidance

[14]

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

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

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

Lab Module List:

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

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

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

Lab Captains:

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

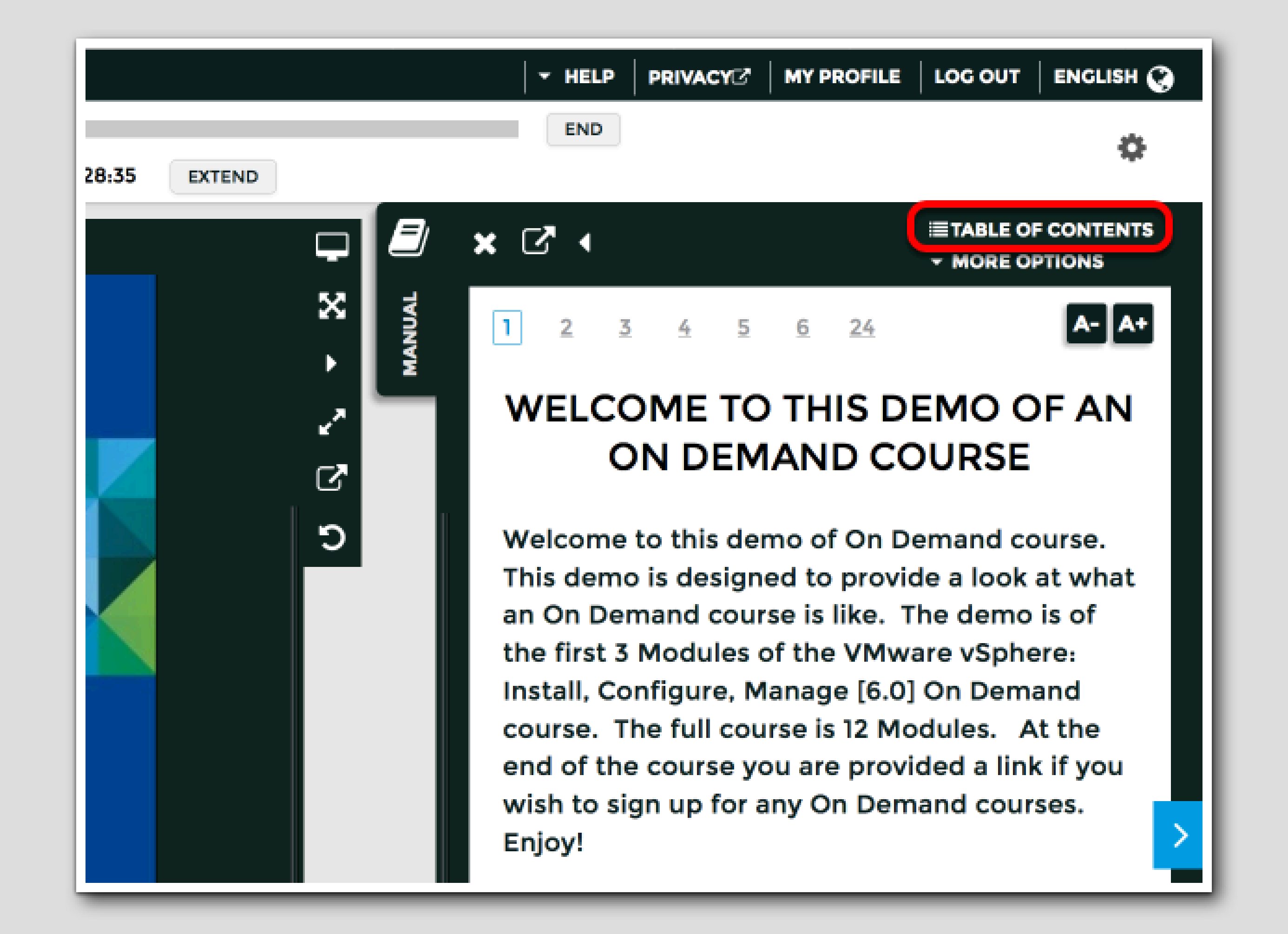
This lab manual can be downloaded from the Hands-on Labs document site found here:

http://docs.hol.vmware.com

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

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

First time using Hands-on Labs?



WELCOME TO THIS DEMO OF AN ON DEMAND COURSE

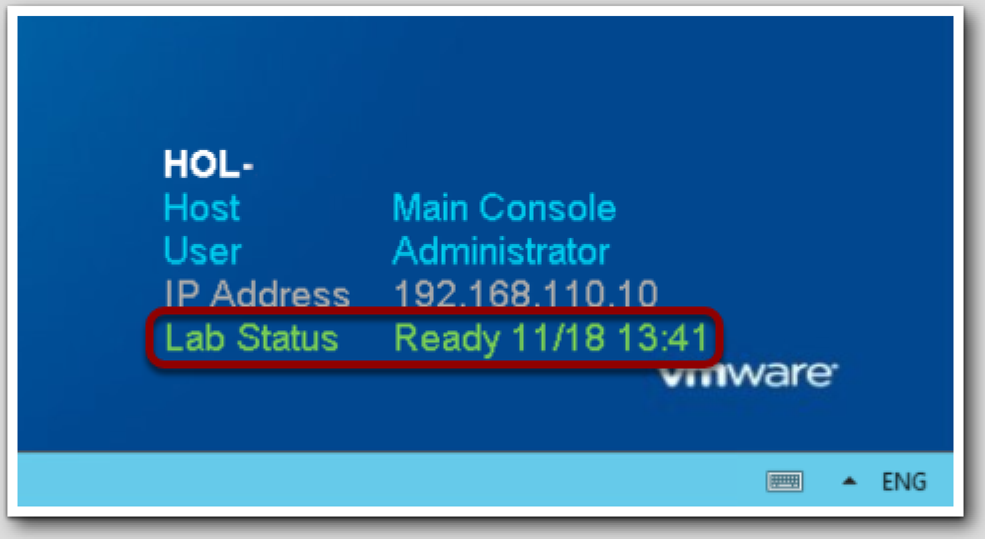
Welcome to this demo of On Demand course. This demo is designed to provide a look at what an On Demand course is like. The demo is of the first 3 Modules of the VMware vSphere: Install, Configure, Manage [6.0] On Demand course. The full course is 12 Modules. At the end of the course you are provided a link if you wish to sign up for any On Demand courses. Enjoy!

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

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

You are ready....is your lab?

[16]



HOL-
Host Main Console
User Administrator
IP Address 192.168.110.10
Lab Status Ready 11/18 13:41

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

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

Introduction

[18]

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

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

Hands-on Labs Interactive Simulation: ESXi Installation and Configuration

[19]

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

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

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

ESXi Host Client

[20]

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

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

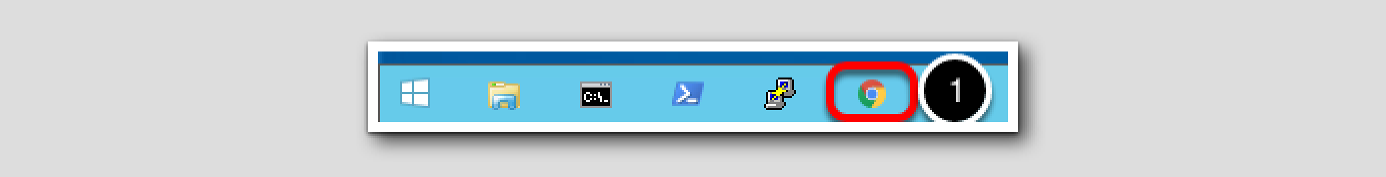
It is important to know that the VMware Host Client is different from the vSphere Web Client, regardless of their similar user interfaces. You use the vSphere Web Client to connect to vCenter Server and manage multiple ESXi hosts, whereas you use the VMware Host Client to manage a single ESXi host.

For additional details on the VMware Host Client, please see this PDF (*https://docs.vmware.com/en/VMware-vSphere/7.0/vsphere-esxi-host-client-1370-guide.pdf*)

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

Launch Chrome

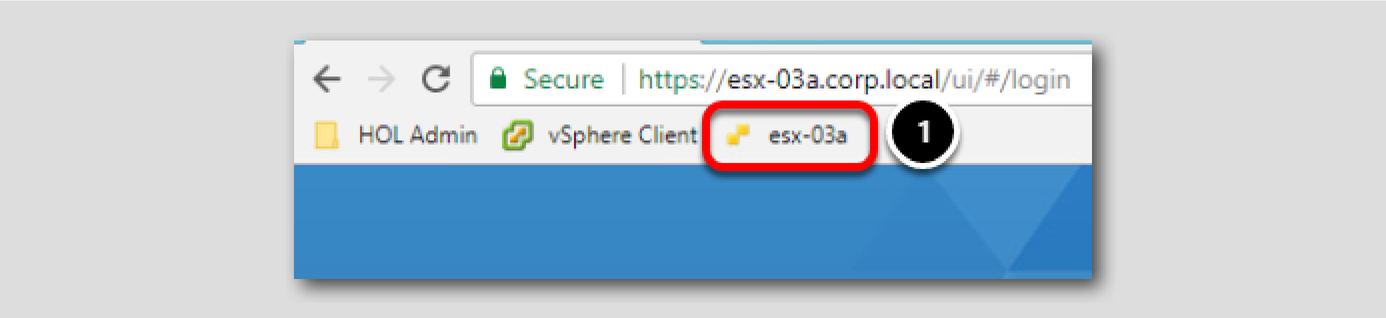
[21]



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

Select esx-03a

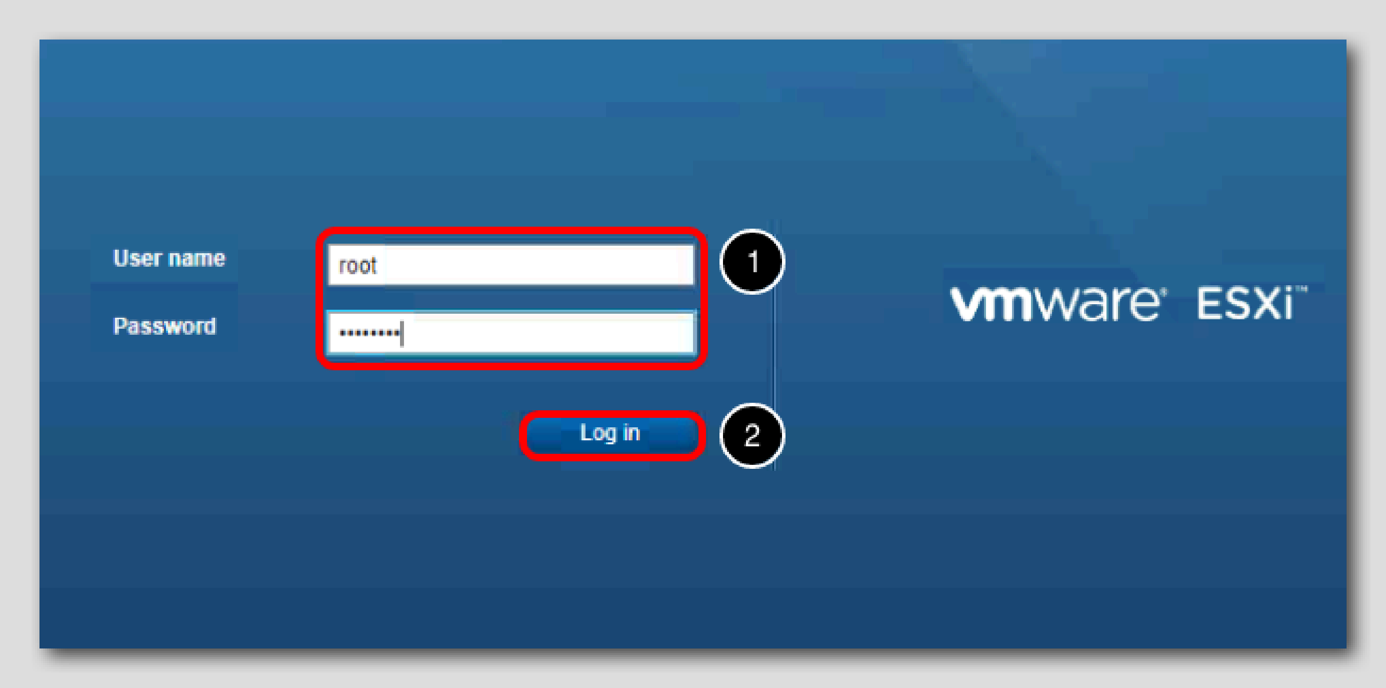
[22]



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

Login

[23]

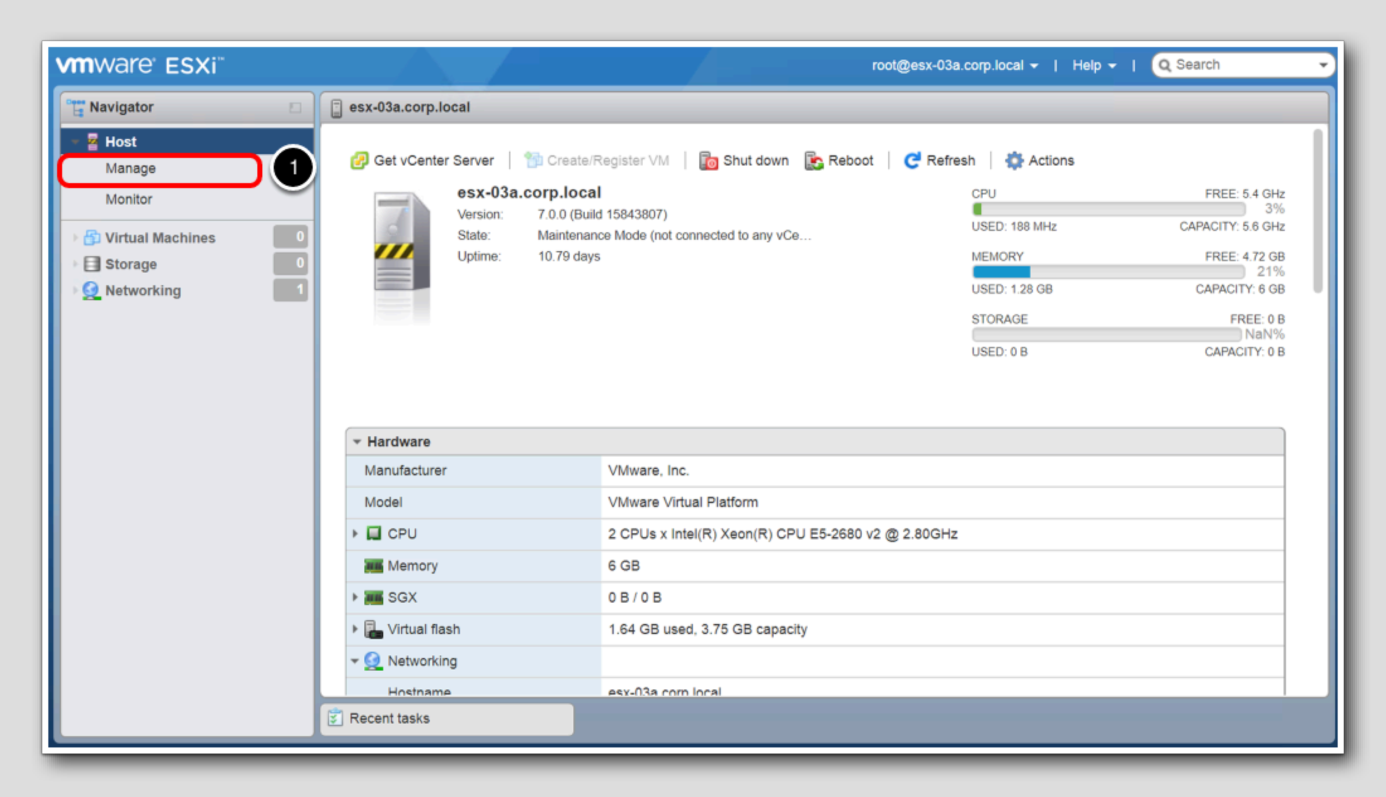


1. Login with the following credentials:

- User name: root
- Password: VMware1!

2. Click the **Log in** button

ESXi Host Client


vmware ESXi
root@esx-03a.corp.local ▾ | Help ▾ | Search
Navigator
Host
Manage
Monitor
1
Virtual Machines 0
Storage 0
Networking 1
esx-03a.corp.local
Get vCenter Server | Create/Register VM | Shut down | Reboot | Refresh | Actions
Recent tasks

esx-03a.corp.local

Version: 7.0.0 (Build 15843807)
State: Maintenance Mode (not connected to any vCe…
Uptime: 10.79 days

CPU FREE: 5.4 GHz 3% USED: 188 MHz CAPACITY: 5.6 GHz
MEMORY FREE: 4.72 GB 21% USED: 1.28 GB CAPACITY: 6 GB
STORAGE FREE: 0 B NaN% USED: 0 B CAPACITY: 0 B

Hardware

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
CPU	2 CPUs x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Memory	6 GB
SGX	0 B / 0 B
Virtual flash	1.64 GB used, 3.75 GB capacity
Networking	
Hostname	esx-03a.corp.local

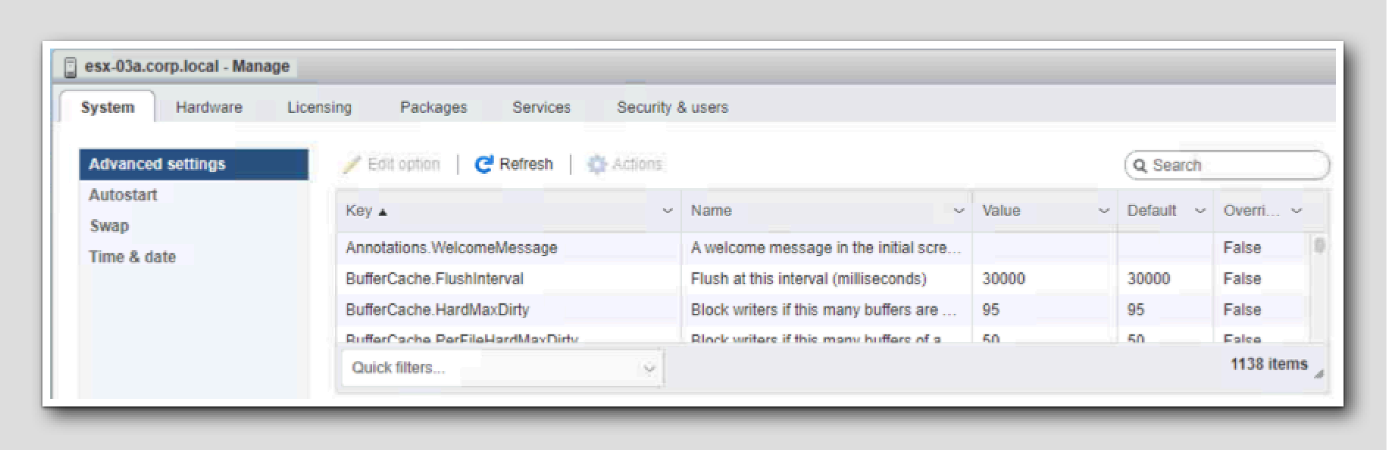
The ESXi Host, in this case, esx-03a, can now be directly managed. This can be useful in test/dev environments where a vCenter Server is not present or in a production environment where the vCenter Server is not reachable.

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

1. Click on Manage

System

[25]

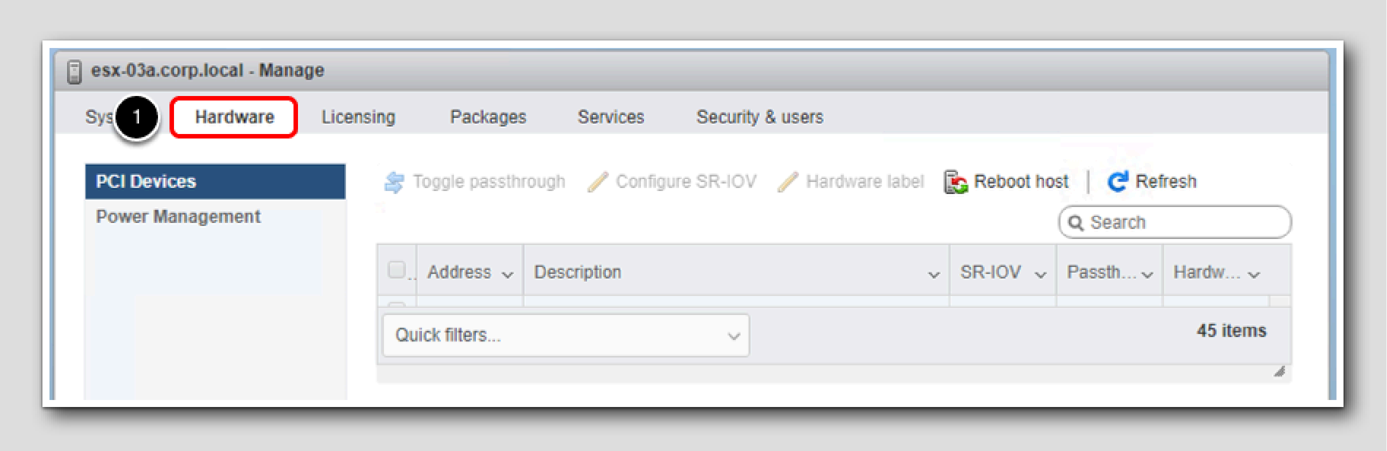


Key ▲	Name	Value	Default	Overri...
Annotations.WelcomeMessage	A welcome message in the initial scre...			False
BufferCache.FlushInterval	Flush at this interval (milliseconds)	30000	30000	False
BufferCache.HardMaxDirty	Block writers if this many buffers are ...	95	95	False
BufferCache.PerFileHardMaxDirty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

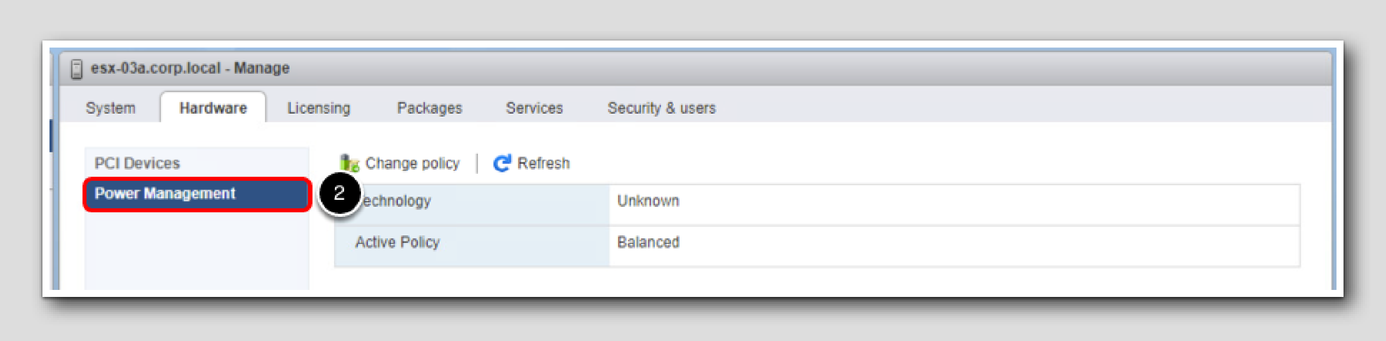
On the **System** tab, the most common options set here are the date and time for the host. It can be set and synchronized with an NTP server or set manually. In addition, Autostart settings for the host can be configured here as well.

Hardware

[26]



1. Click on the **Hardware** tab



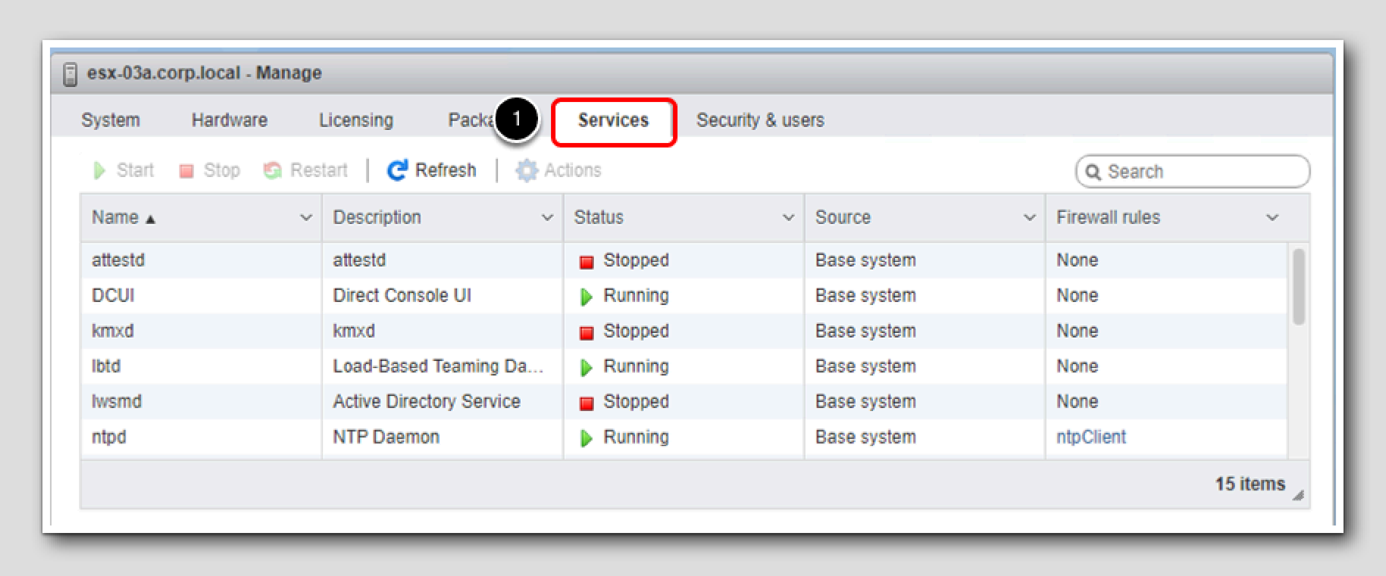
Technology	Unknown
Active Policy	Balanced

2. Click Power Management

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

Services

[27]



Name ▲	Description	Status	Source	Firewall rules
attestd	attestd	🟥 Stopped	Base system	None
DCUI	Direct Console UI	▶ Running	Base system	None
kmxd	kmxd	🟥 Stopped	Base system	None
lbtd	Load-Based Teaming Da...	▶ Running	Base system	None
lwsmd	Active Directory Service	🟥 Stopped	Base system	None
ntpd	NTP Daemon	▶ Running	Base system	ntpClient

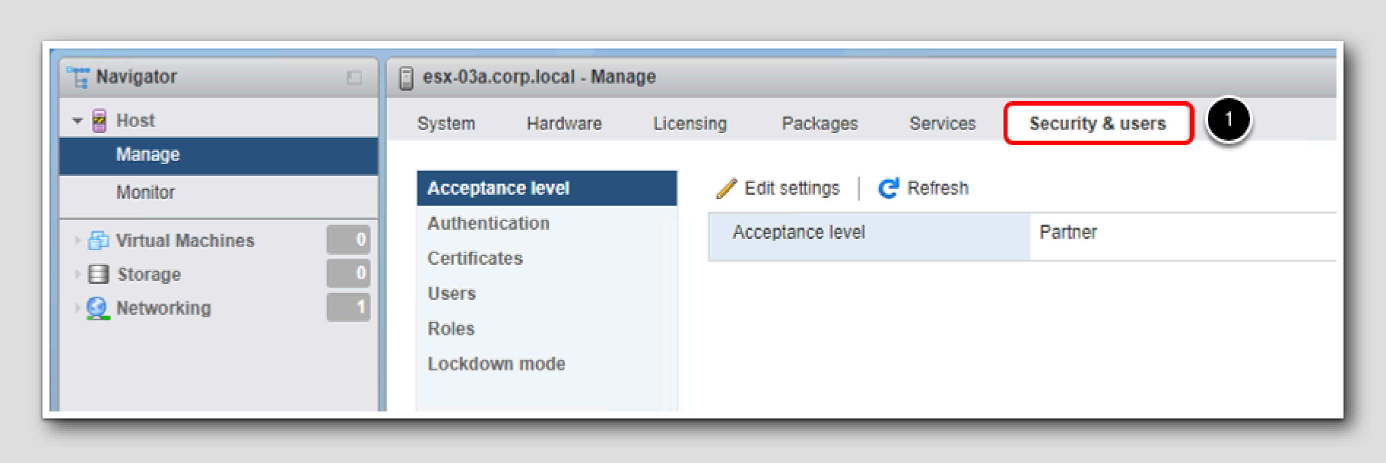
15 items

1. Click the Services tab

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

Security and Users

[28]



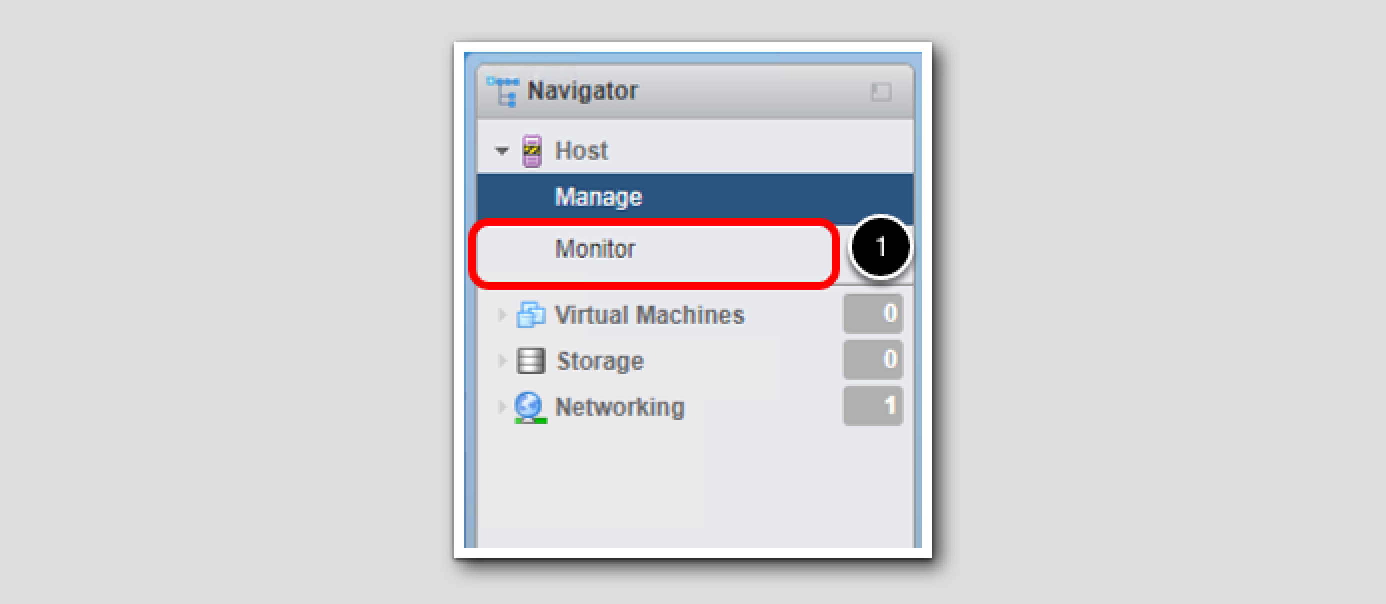
Acceptance level	Partner

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

1. Click on Security & users

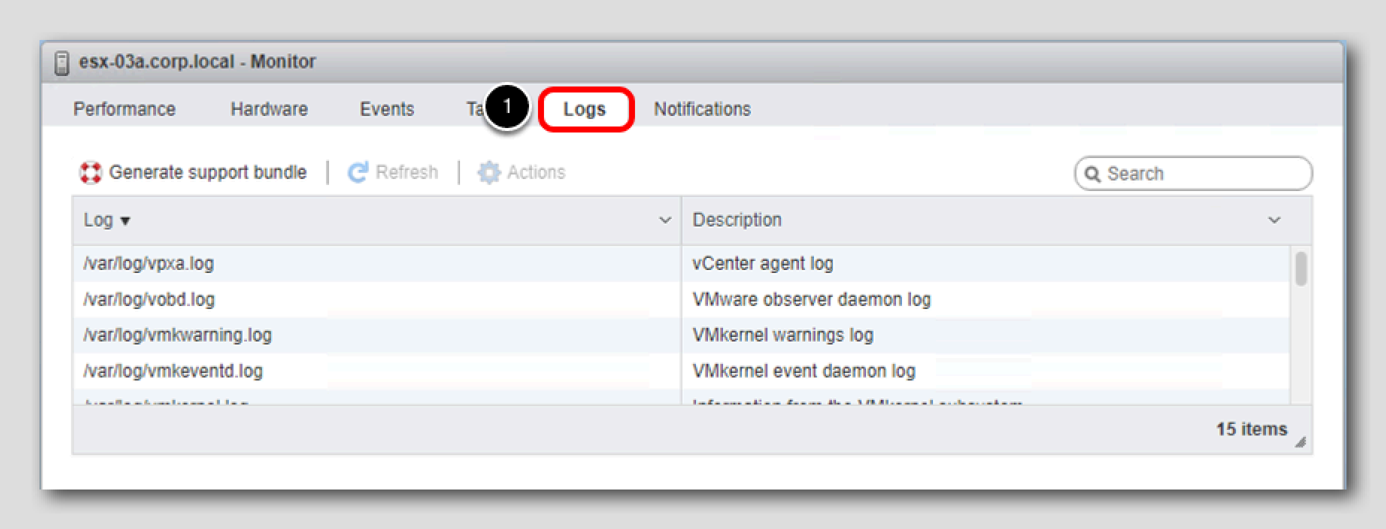
Monitor

[29]



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

1. Click on **Monitor**



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

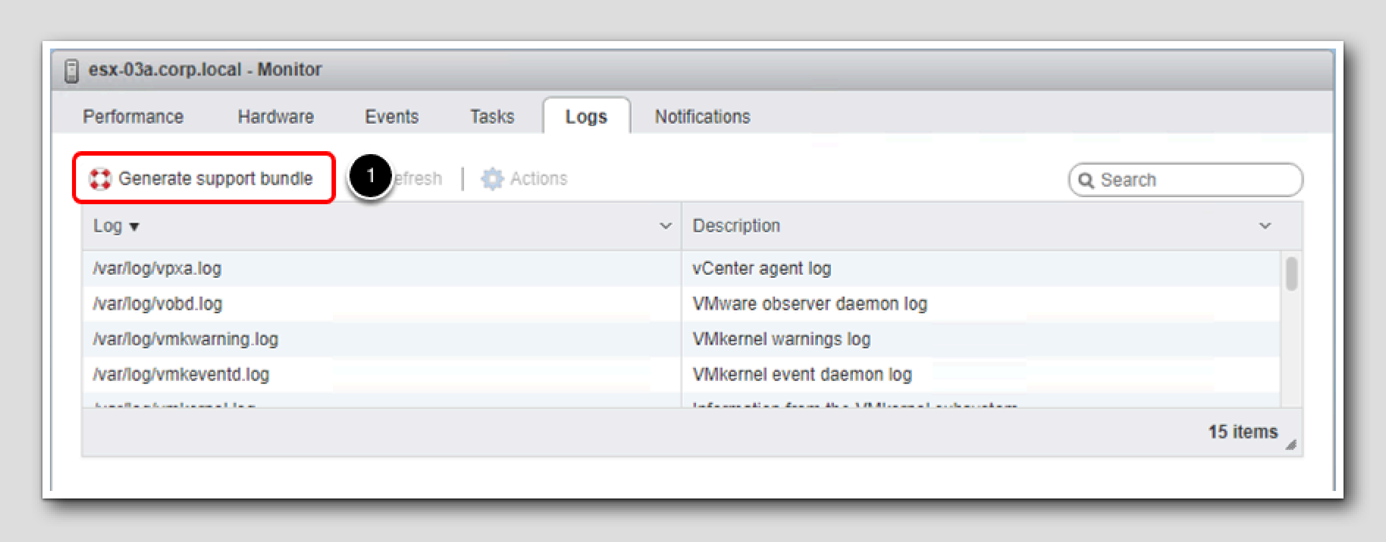
15 items

1. Click the **Logs** tab

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

Generate Support Bundle

[30]



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

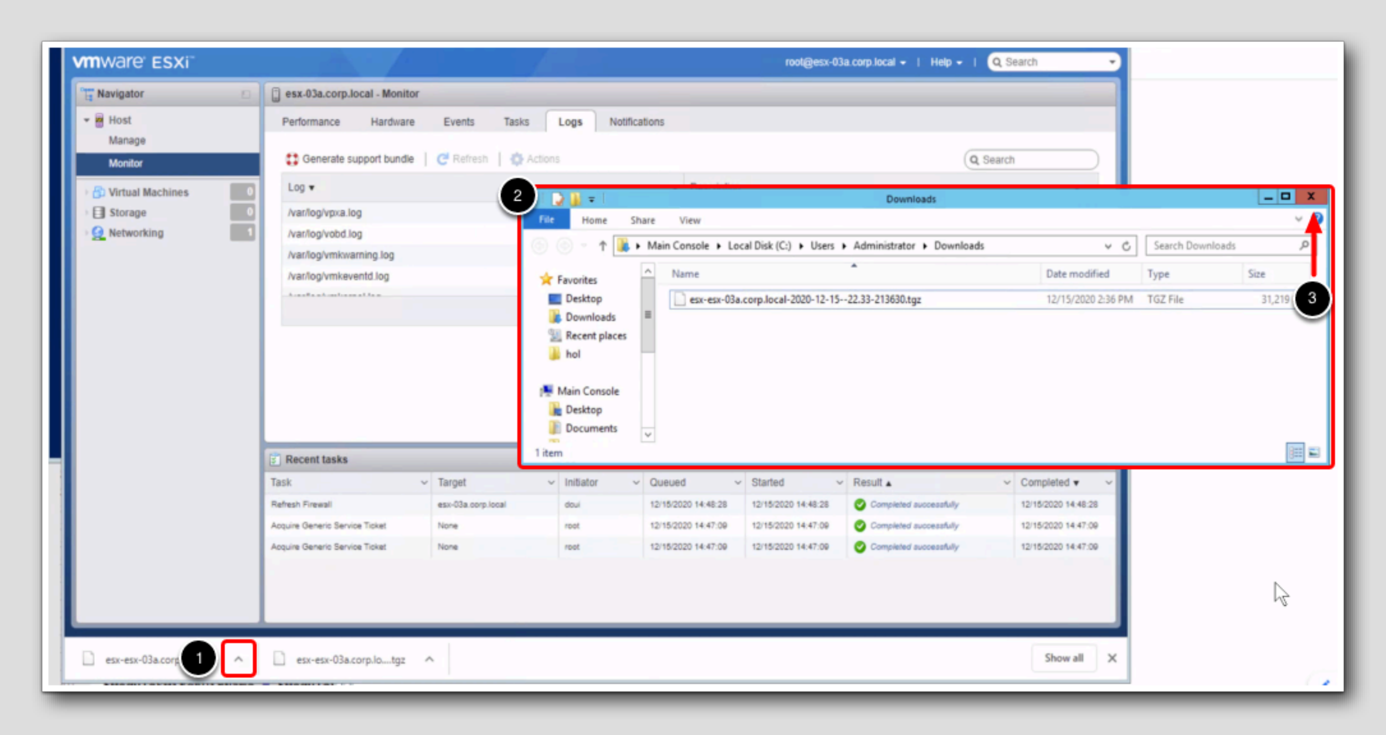
15 items

1. Click the **Generate Support Bundle** button

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

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

- **Username**: root
- **Password**: VMware1!



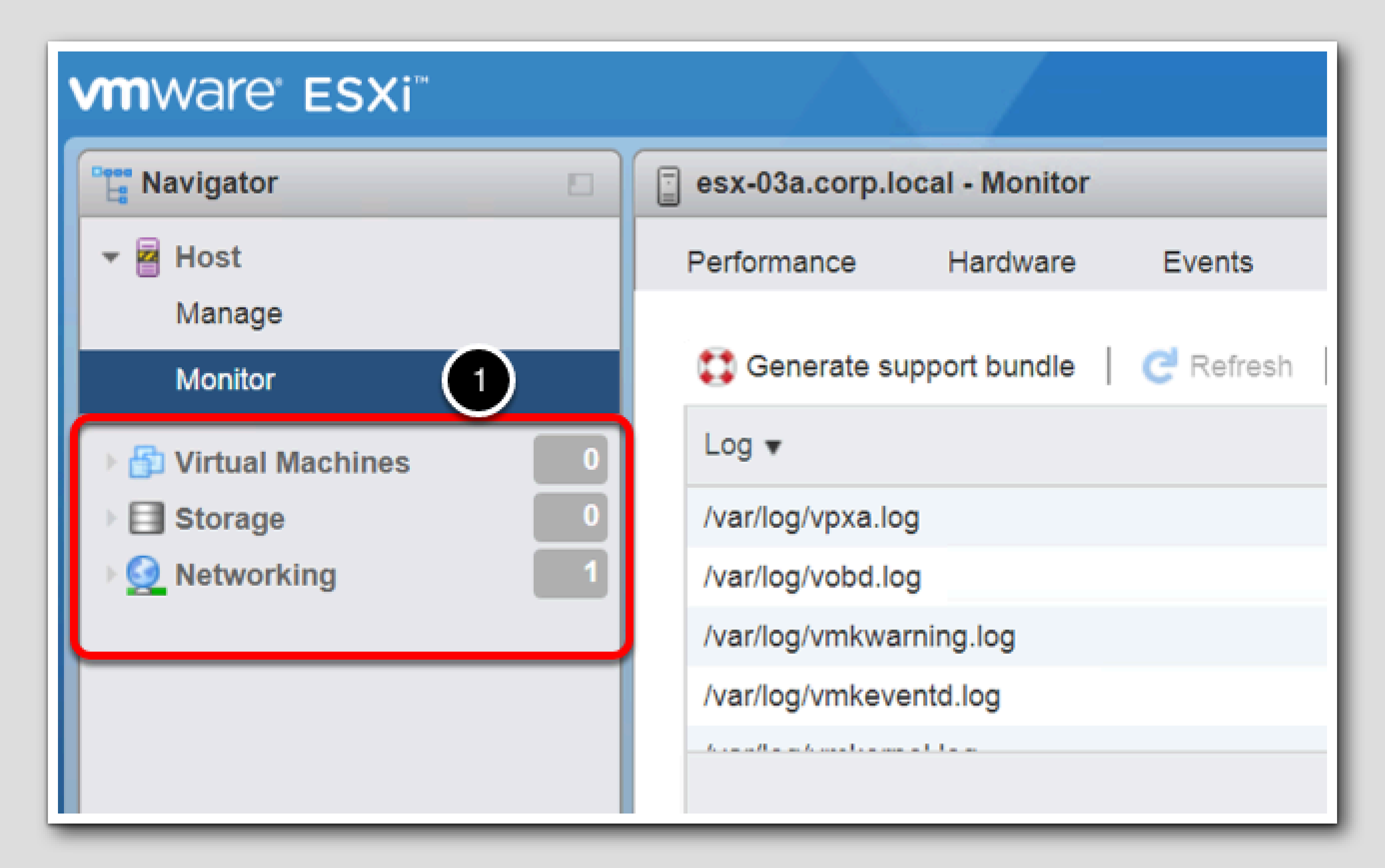
Name	Date modified	Type	Size
esx-esx-03a.corp.local-2020-12-15--22.33-213630.tgz	12/15/2020 2:36 PM	TGZ File	31,219

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Refresh Firewall	esx-03a.corp.local	doui	12/15/2020 14:48:28	12/15/2020 14:48:28	✓ Completed successfully	12/15/2020 14:48:28
Acquire Generic Service Ticket	None	root	12/15/2020 14:47:09	12/15/2020 14:47:09	✓ Completed successfully	12/15/2020 14:47:09
Acquire Generic Service Ticket	None	root	12/15/2020 14:47:09	12/15/2020 14:47:09	✓ Completed successfully	12/15/2020 14:47:09

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

VMs, Storage and Networking

[31]



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

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

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

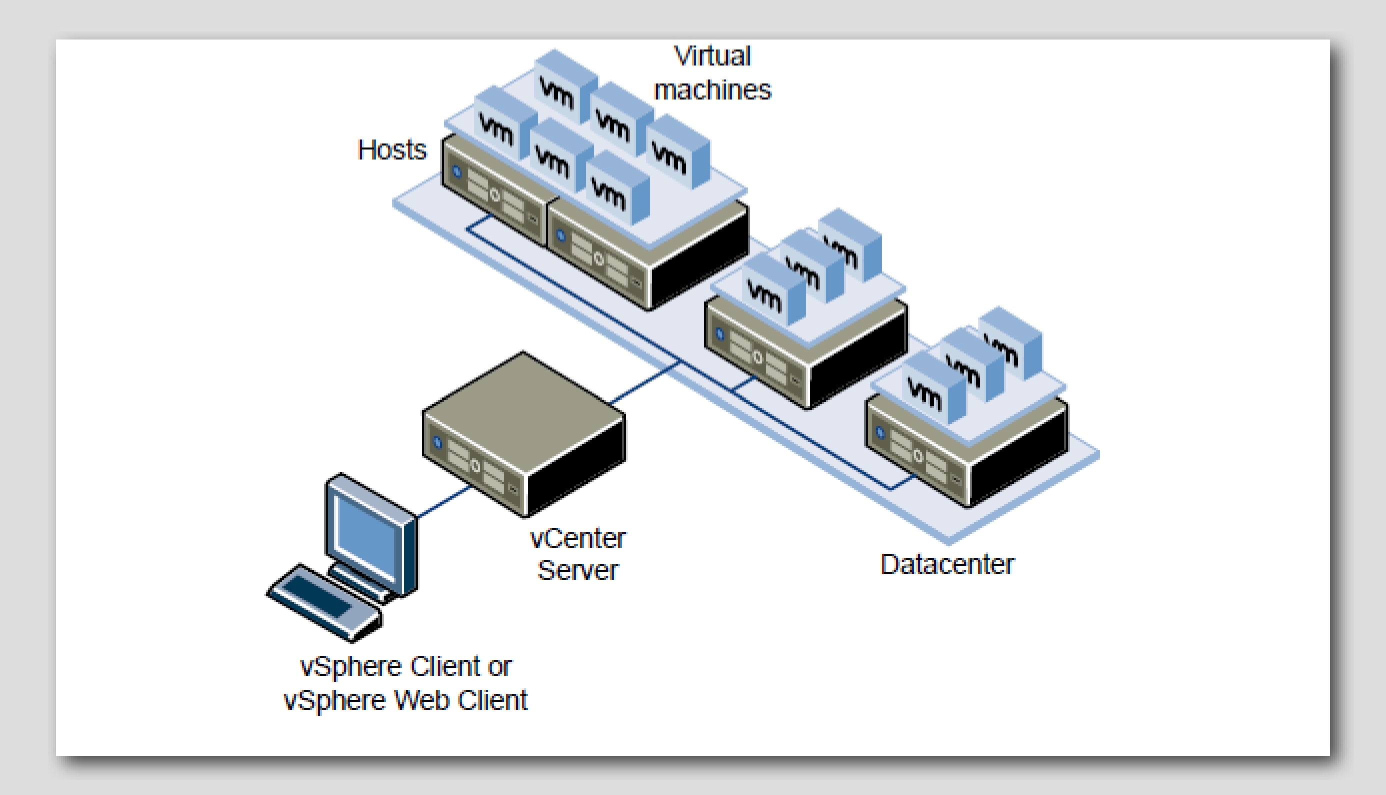
vCenter 7 Overview

[32]

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

vSphere Components

[33]

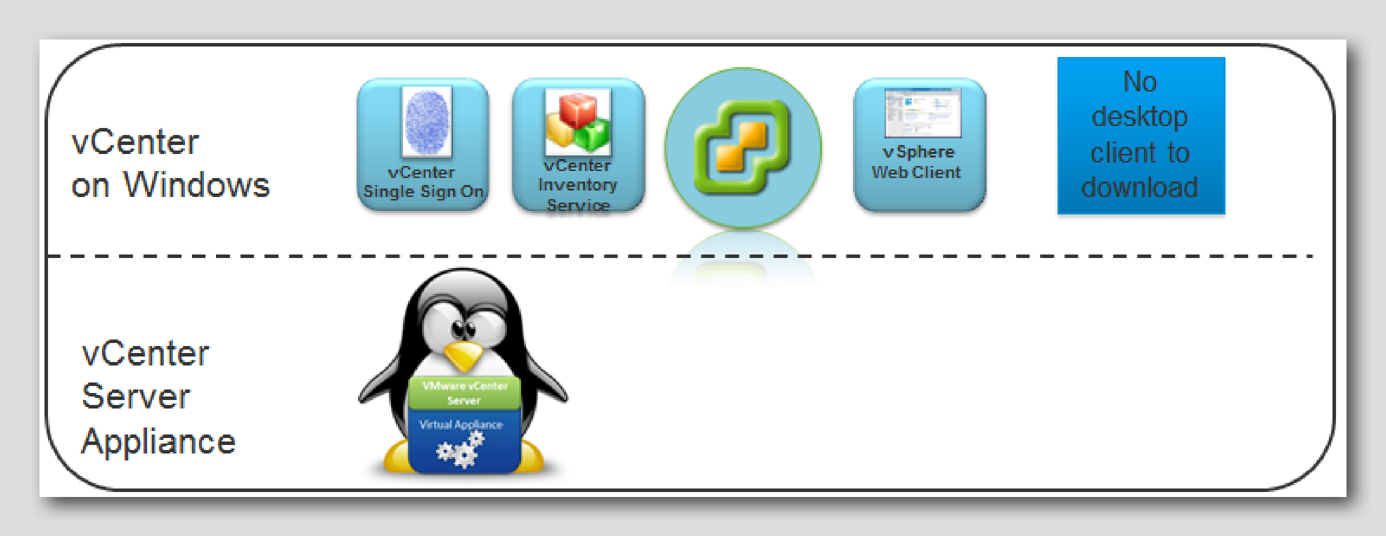


The above diagram shows how vCenter fits in the vSphere stack. With vCenter installed, you have a central point of management. vCenter Server allows the use of advanced vSphere features such as vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), vSphere vMotion, and vSphere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

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

vCenter 7 Components

[34]

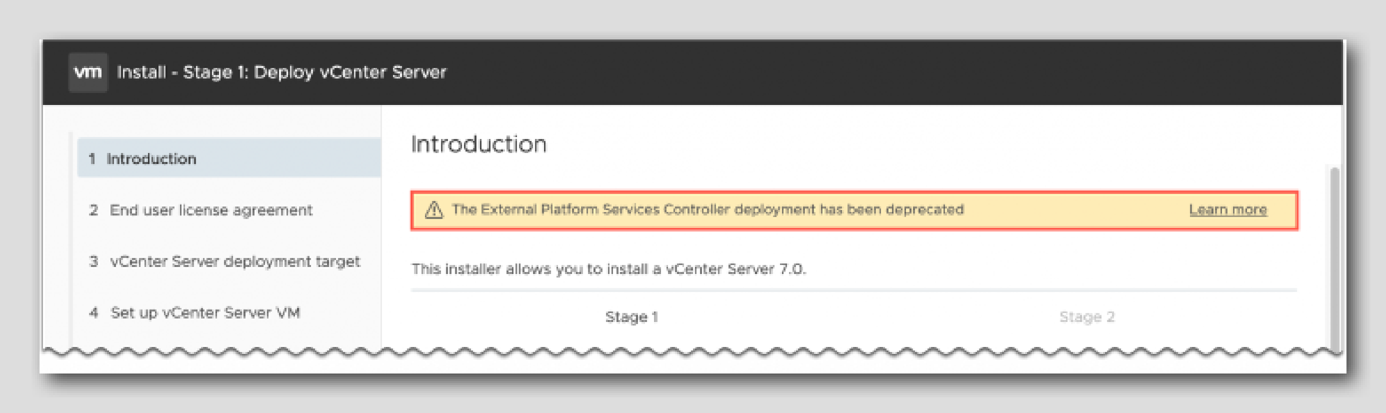


First, there is no longer an option to deploy the external Platform Services Controller (PSC). The only option is the vCenter Server Appliance which contains an embedded PSC. Embedded PSCs have all of the services required to manage a vSphere SSO Domain.

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)

[35]


vm
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
Introduction
Learn more
Stage 1
Stage 2

⚠ The External Platform Services Controller deployment has been deprecated

This installer allows you to install a vCenter Server 7.0.

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.

In vCenter Server 7, PSC convergence now happens automatically during a vCenter Server upgrade!There is no longer a need to perform an upgrade and a convergence as two separate tasks. When upgrading your vCenter Server from version 6.5 or 6.7 to 7.0, the installer can detect external PSCs which allows these two processes to be merged for a simplistic method of upgrading and consolidating *deprecated SSO topologies*.

Once the Platform Services Controller is converged, it remains in inventory to be decommissioned by the vSphere Administrator. The upgrade and convergence process in vCenter Server 7 does not decommission the PSC automatically.

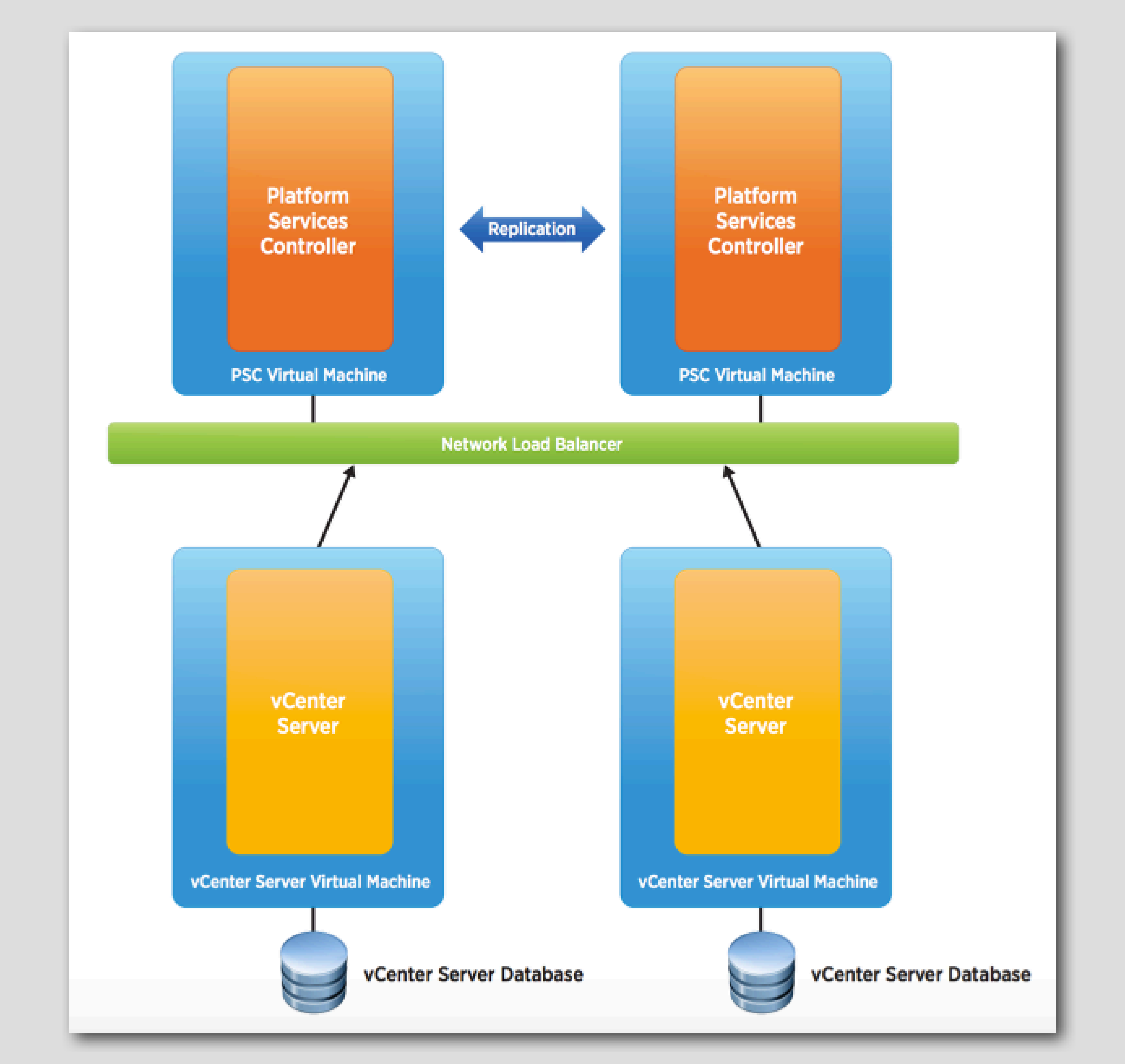
vCenter Single Sign On

[36]

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

vCenter Single Sign On - Typical Deployment

[37]



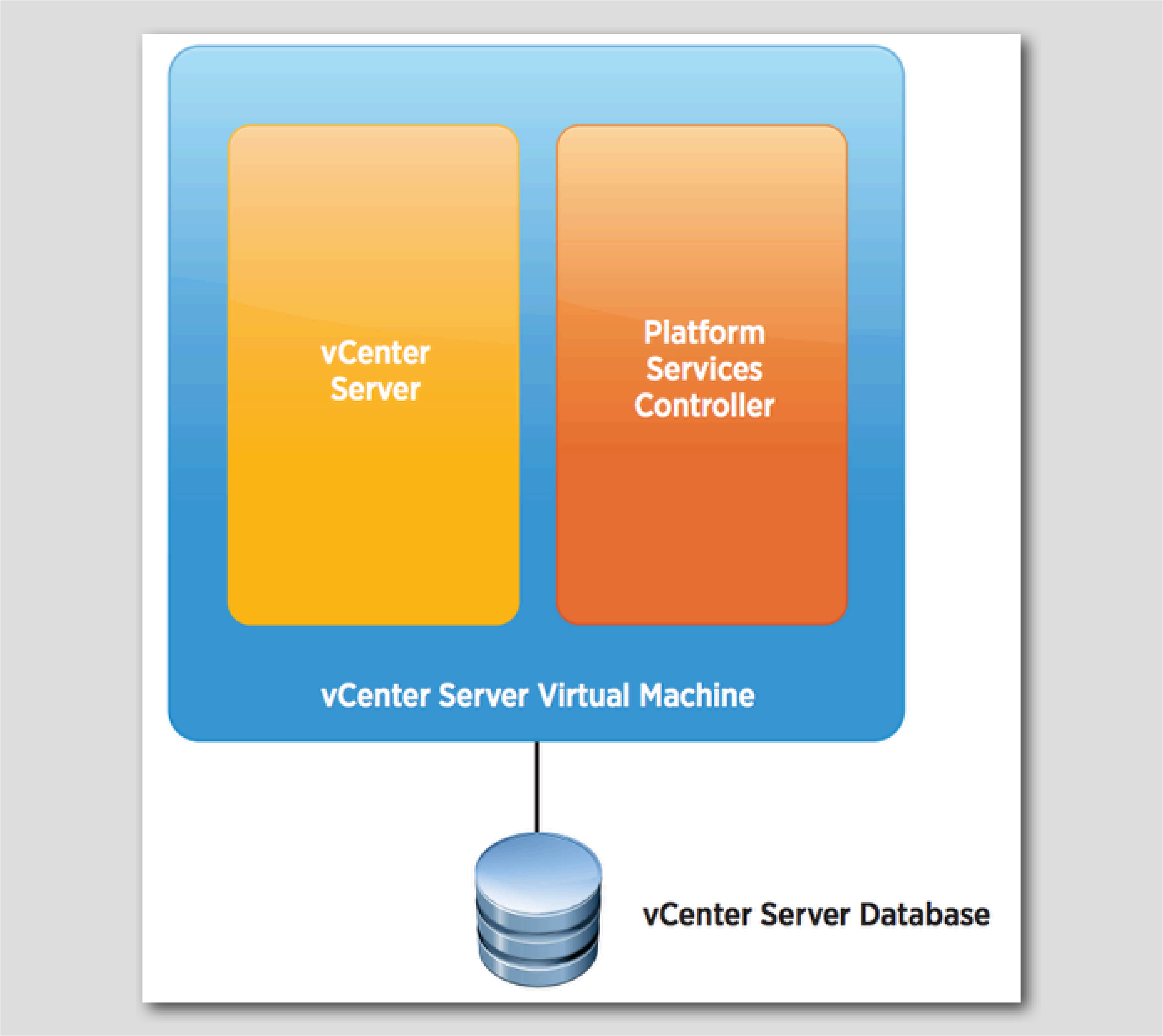
Starting with version 5.1, vSphere includes a vCenter Single Sign-On service as part of the vCenter Server management infrastructure.

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

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

vCenter Single Sign On - Single vCenter

[38]



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

[39]

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

However, you can also refer to the *vCenter 7 Deployment Guide* for more in-depth requirements and considerations for SSO architecture in vCenter 7.

vCenter Server and Creating a Virtual Machine

[40]

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.

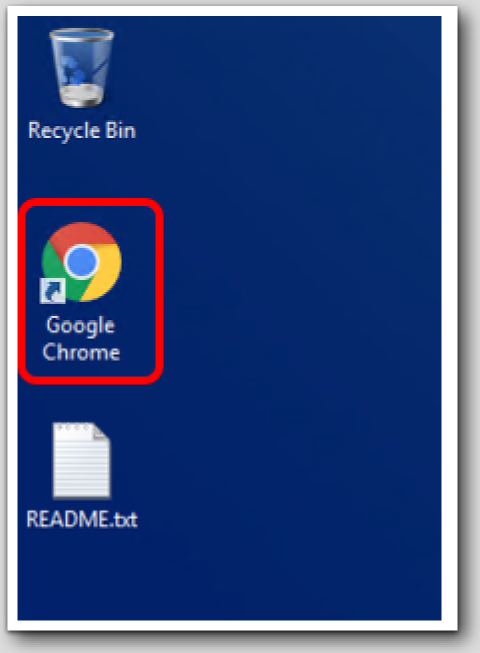
The vSphere Client is a Web browser-based application that you can use to manage, monitor, and administer the objects that make up your virtualized data center. You can use the vSphere Client to observe and modify the vSphere environment in the following ways.

- 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

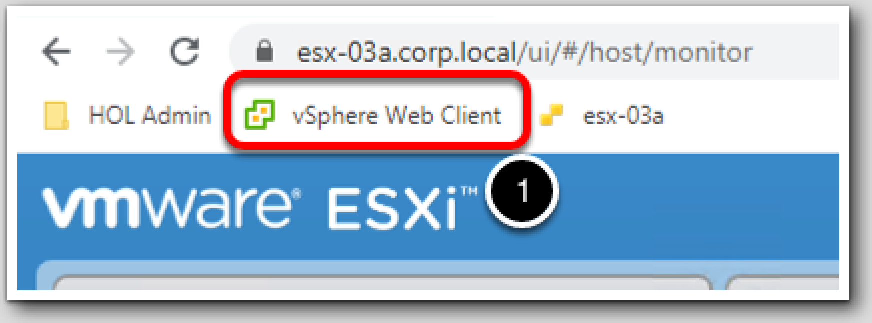
[41]



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

Select vSphere Client

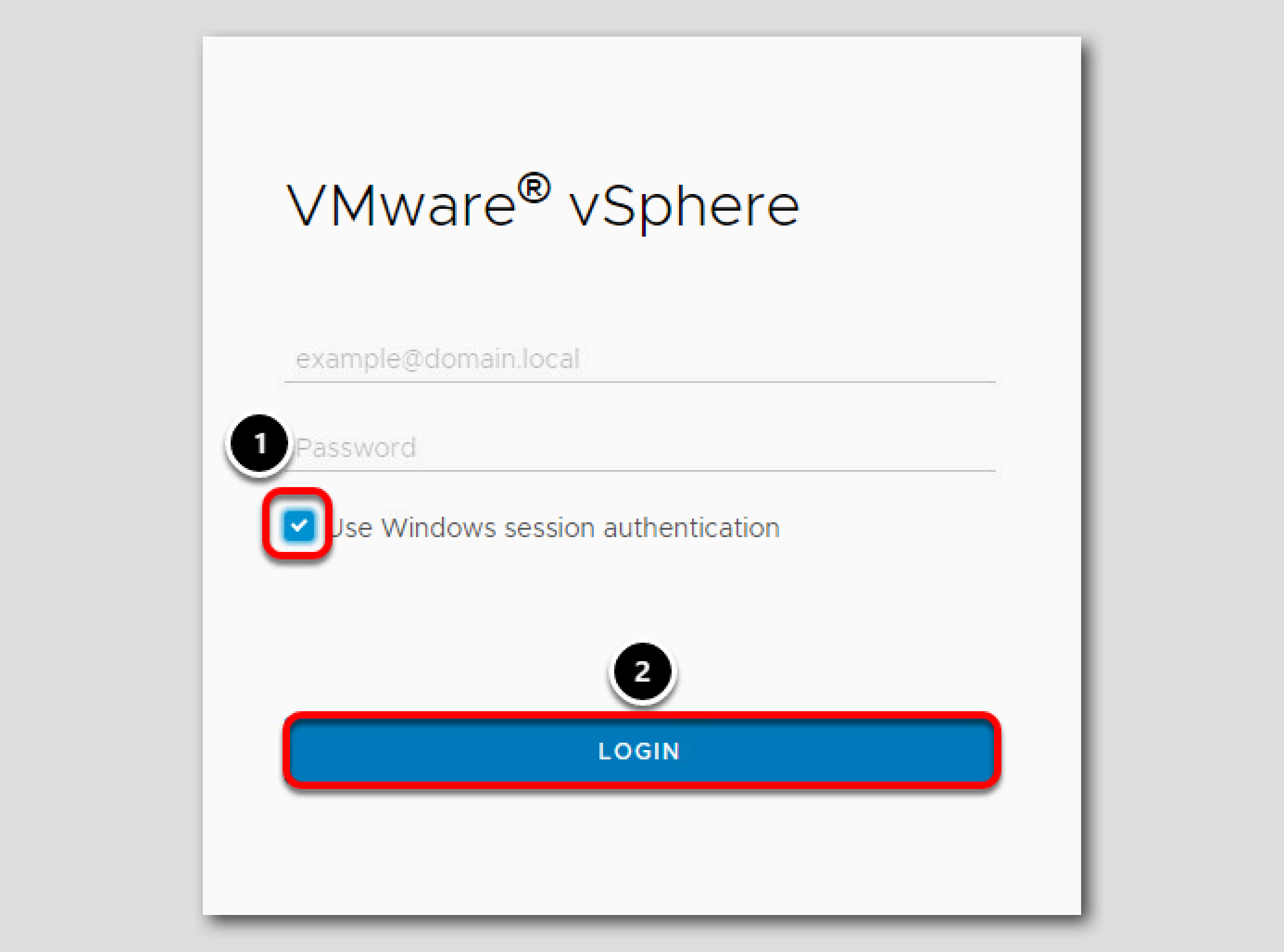
[42]



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

Login to vCenter

[43]


VMware® vSphere

example@domain.local

Password

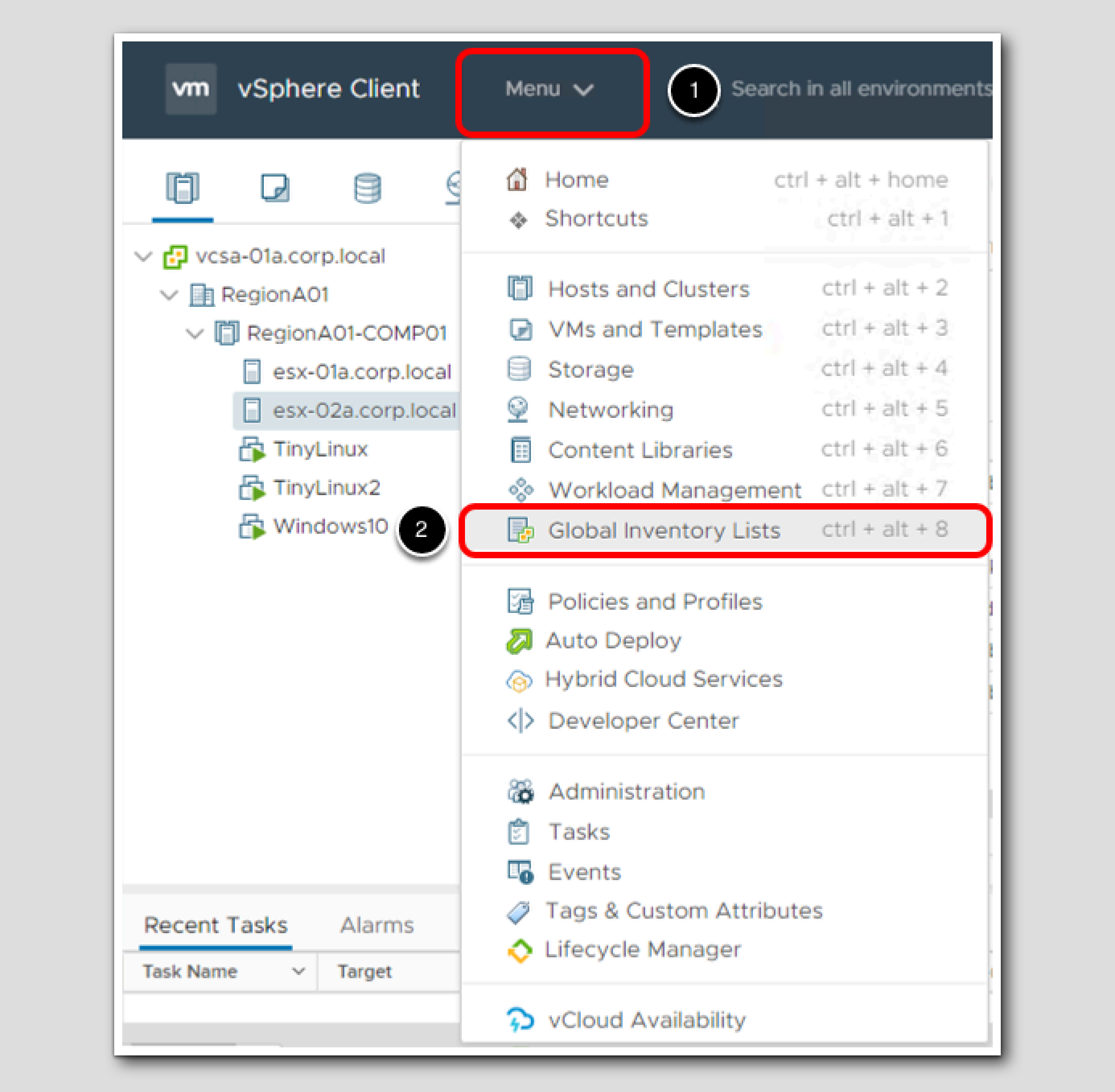
☑ Use Windows session authentication

Log in using the following method:

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

vCenter Inventory

[44]



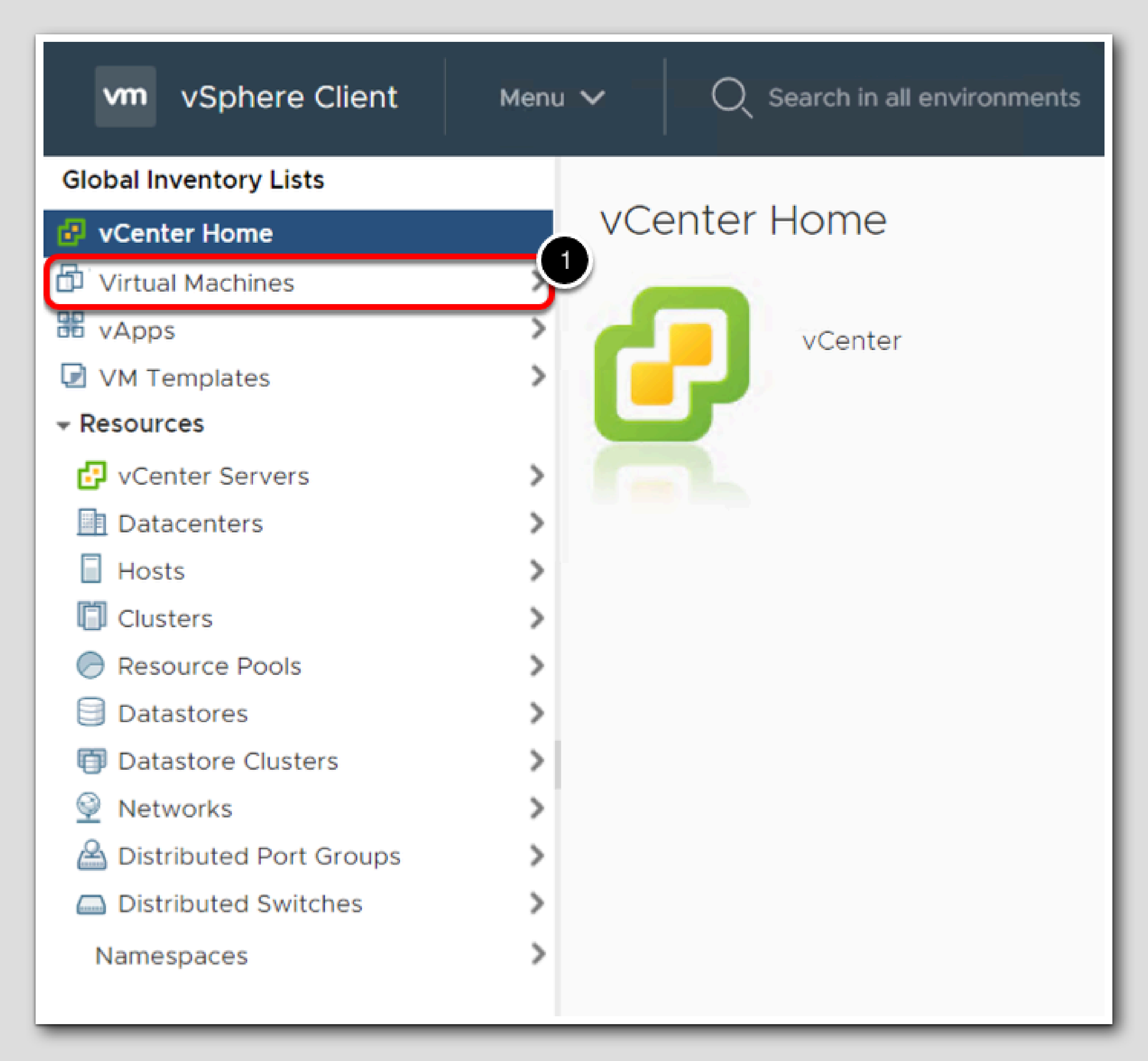
By default, you are brought to a view that shows the Hosts and Clusters attached to vCenter. Get a more complete look by viewing the Global Inventory Lists.

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

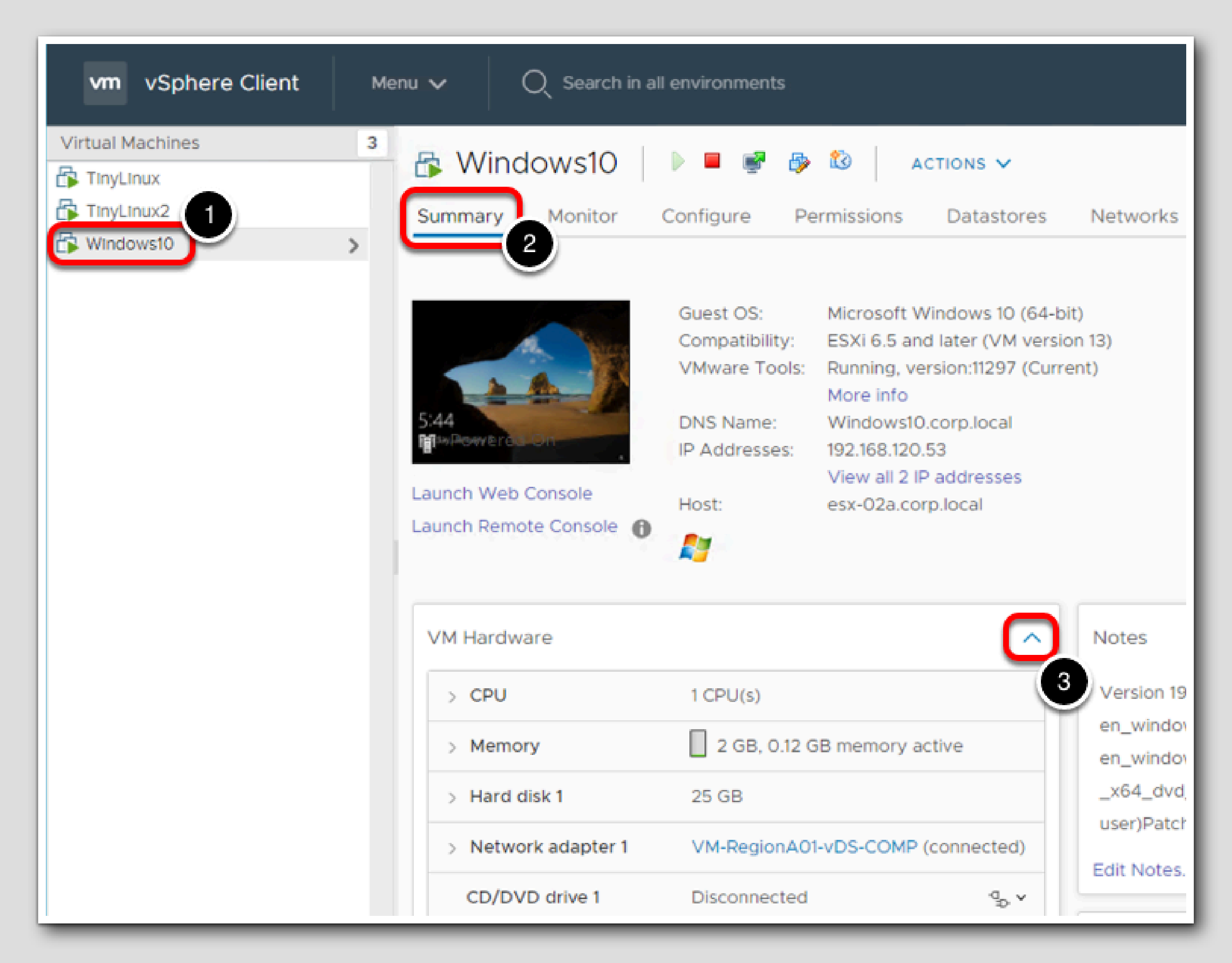
[45]



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

[46]



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

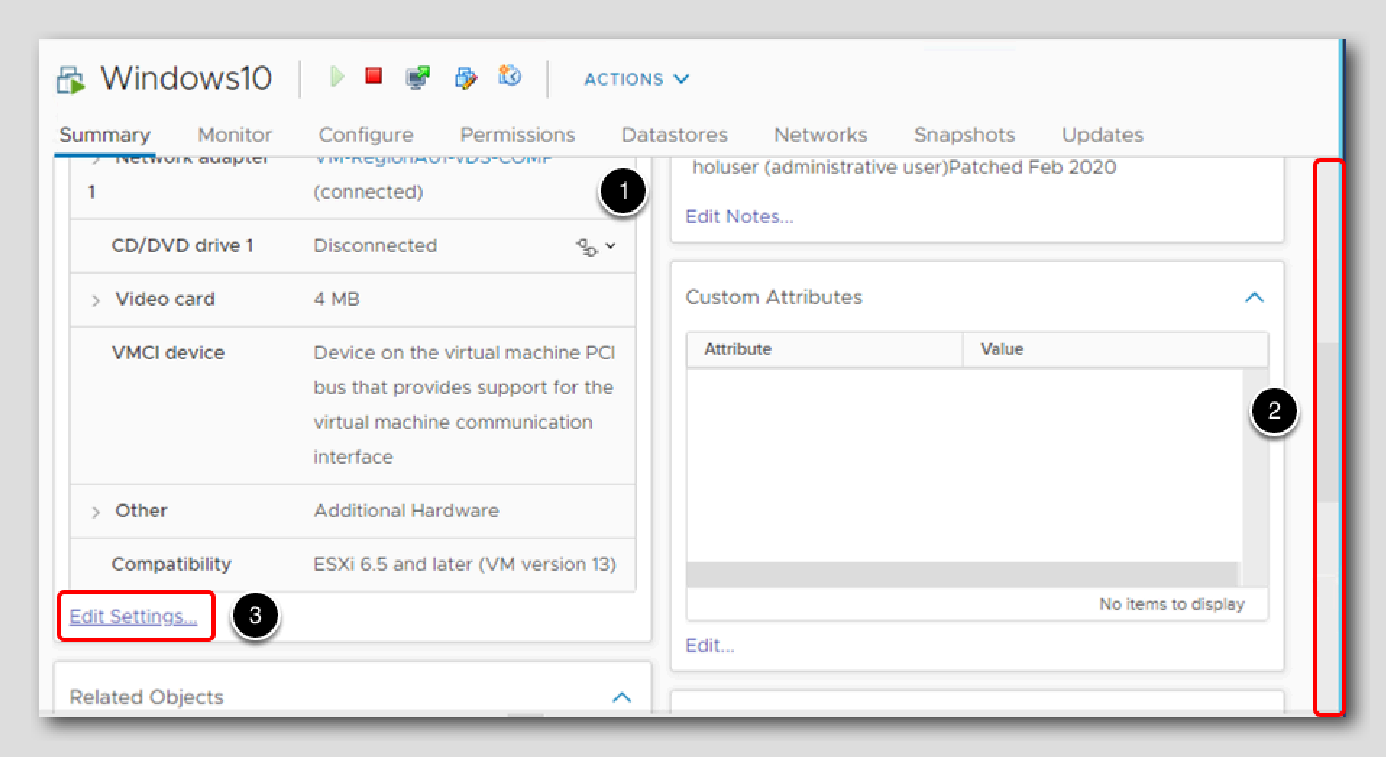
CPU	1 CPU(s)
Memory	2 GB, 0.12 GB memory active
Hard disk 1	25 GB
Network adapter 1	VM-RegionA01-vDS-COMP (connected)
CD/DVD drive 1	Disconnected

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

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

Edit the settings of a virtual machine.

[47]



Network adapter 1	VM-RegionA01-vDS-COMP (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 6.5 and later (VM version 13)

holuser (administrative user)Patched Feb 2020

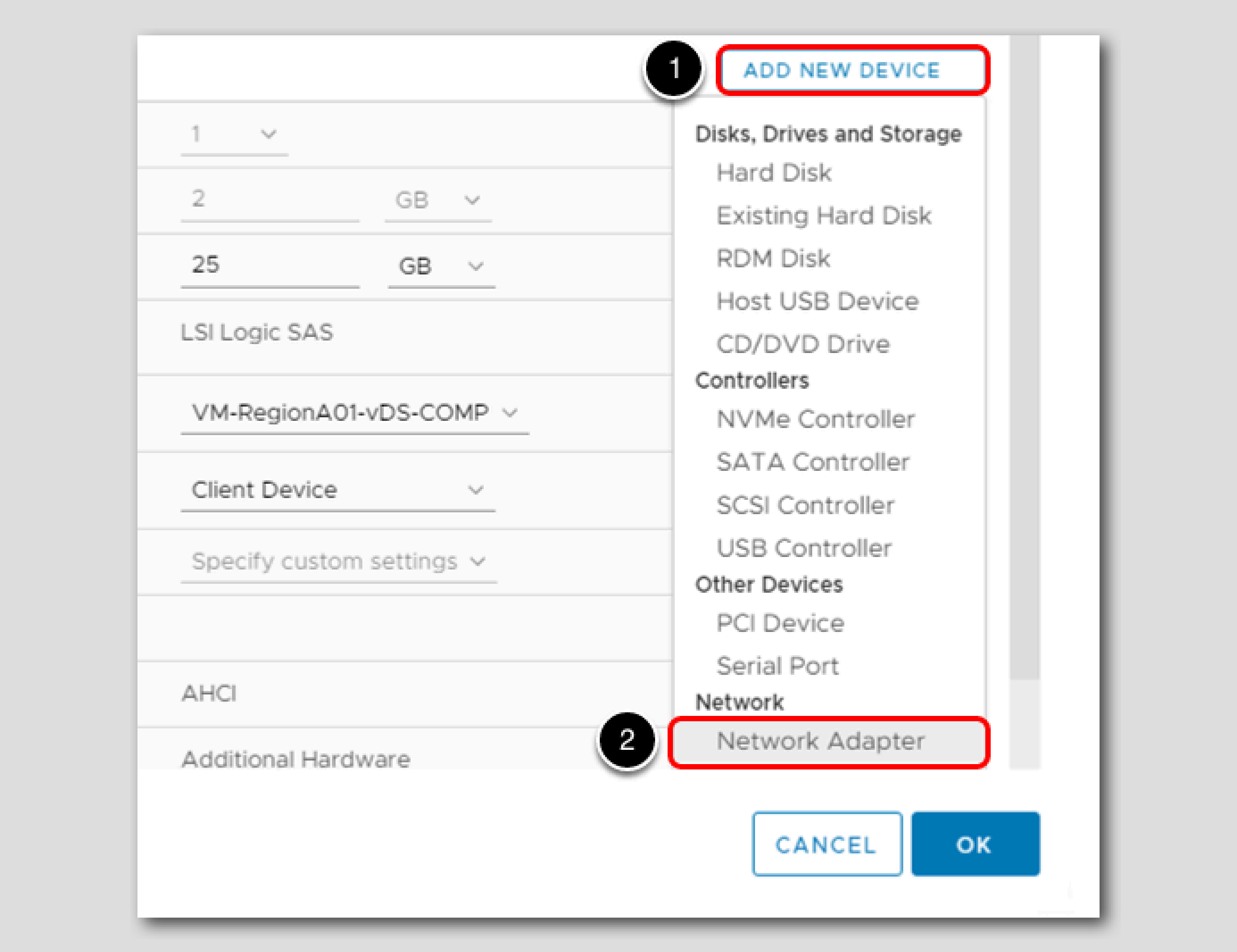
Attribute	Value

No items to display

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

[48]

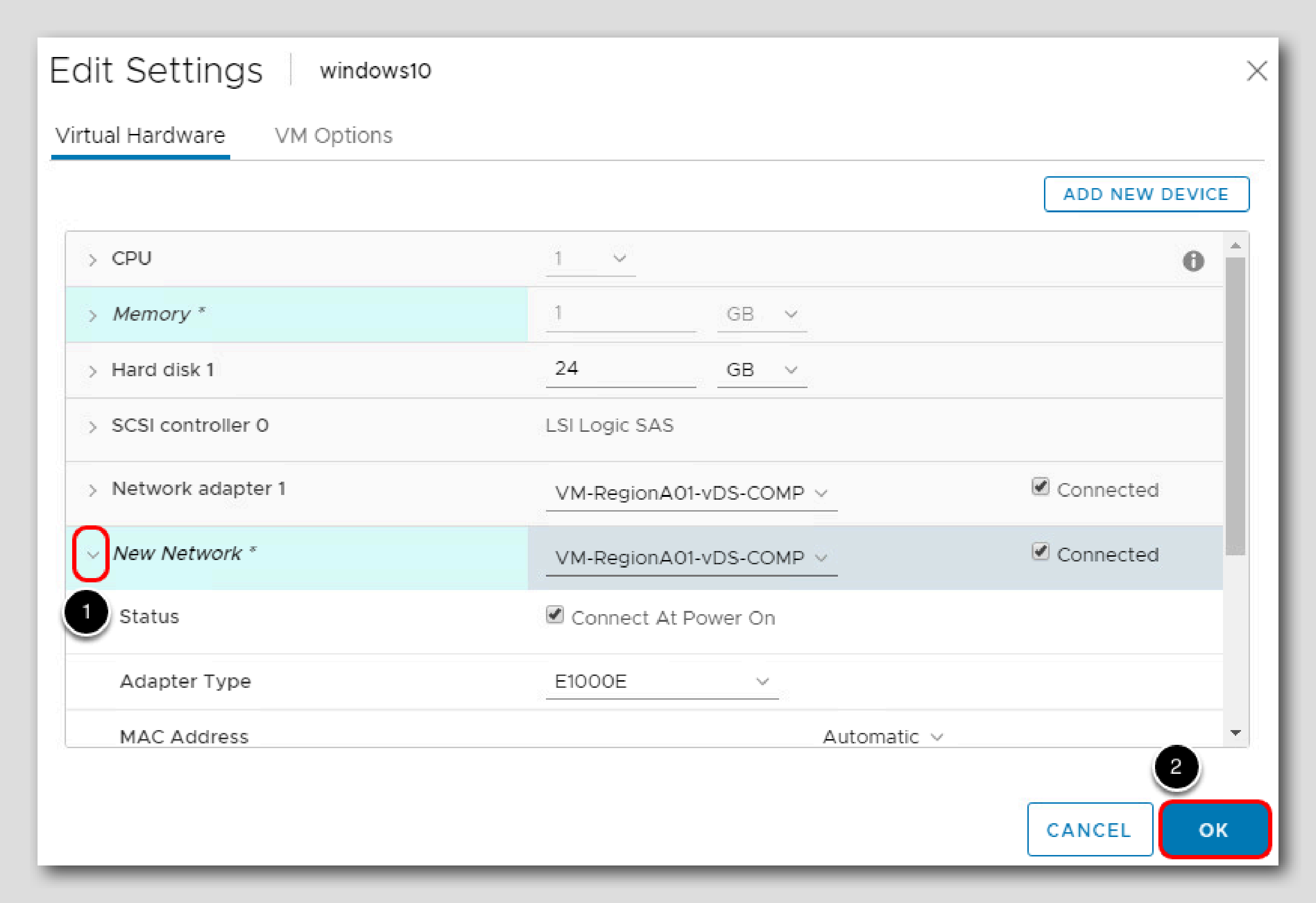


Add another network adapter to the windows10 machine.

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.

[49]



Edit Settings | windows10

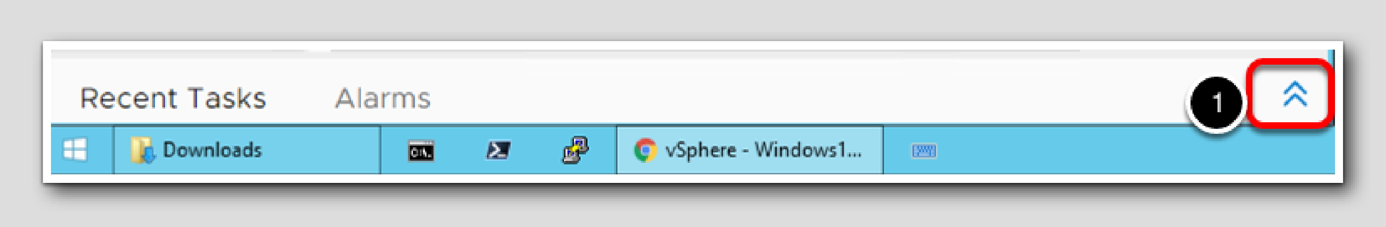
Virtual Hardware | VM Options

CPU	1	
*Memory **	1 GB	
Hard disk 1	24 GB	
SCSI controller 0	LSI Logic SAS	
Network adapter 1	VM-RegionA01-vDS-COMP	☑ Connected
*New Network **	VM-RegionA01-vDS-COMP	☑ Connected
Status	☑ Connect At Power On	
Adapter Type	E1000E	
MAC Address		Automatic

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

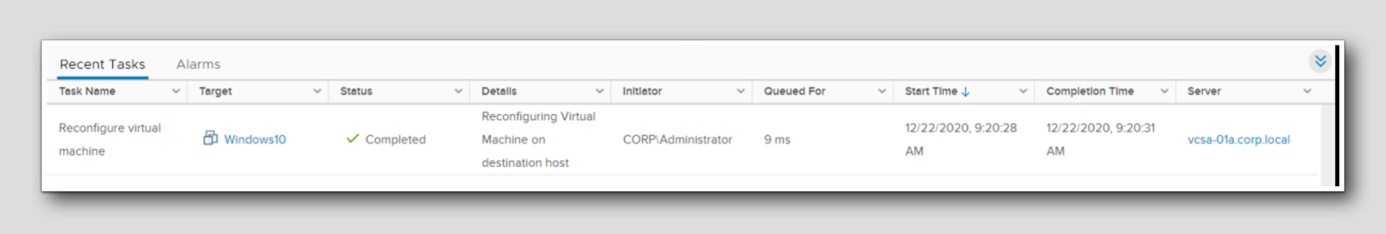
[50]



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

Recent Tasks List

[51]



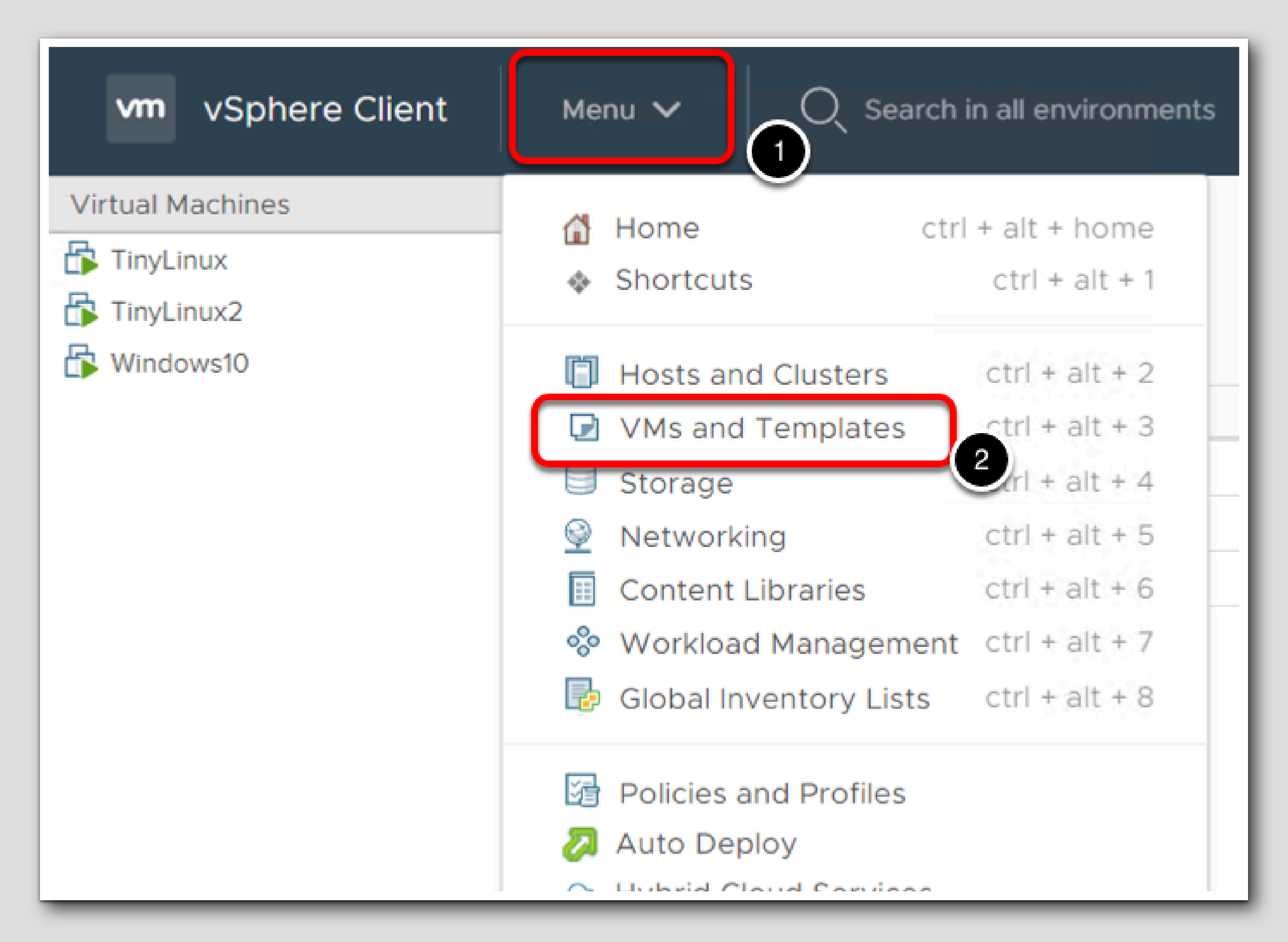
Task Name	Target	Status	Details	Initiator	Queued For	Start Time ↓	Completion Time	Server
Reconfigure virtual machine	Windows10	✓ Completed	Reconfiguring Virtual Machine on destination host	CORP\Administrator	9 ms	12/22/2020, 9:20:28 AM	12/22/2020, 9:20:31 AM	vcsa-01a.corp.local

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

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

Create a Virtual Machine

[52]

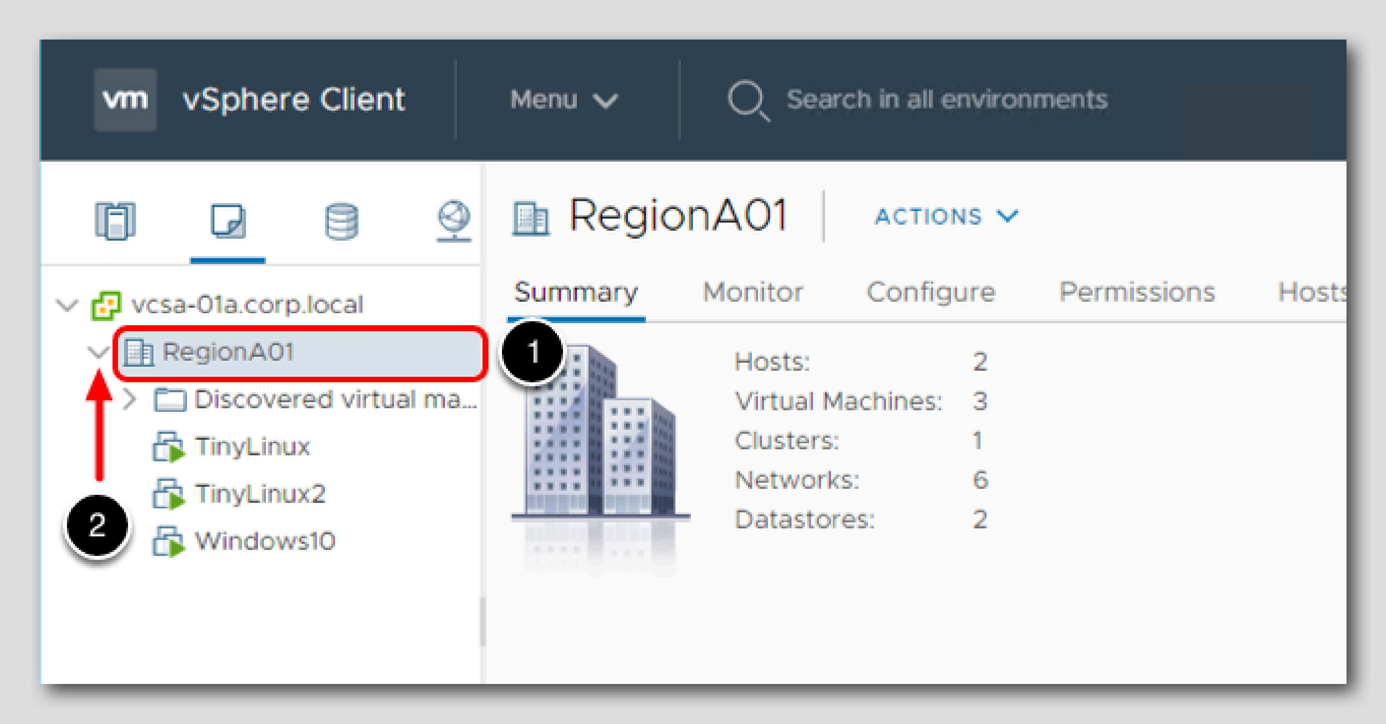

vm vSphere Client
Menu
Search in all environments
1
Virtual Machines
TinyLinux
TinyLinux2
Windows10
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
2
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Workload Management ctrl + alt + 7
Global Inventory Lists ctrl + alt + 8
Policies and Profiles
Auto Deploy
Hybrid Cloud Services

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

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

Select and Expand Datacenter

[53]

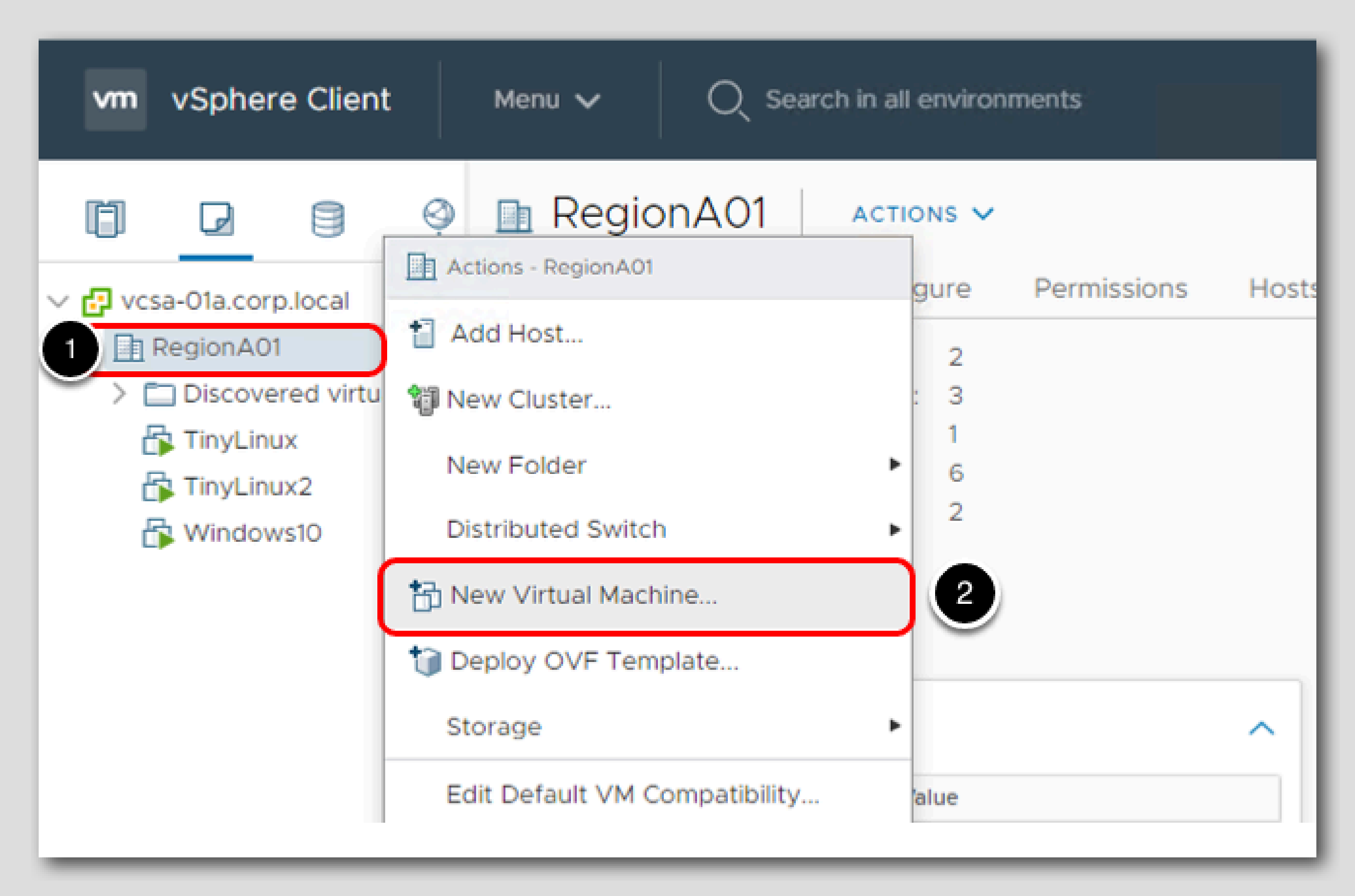


Hosts: 2
Virtual Machines: 3
Clusters: 1
Networks: 6
Datastores: 2

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

Start the New Virtual Machine Wizard

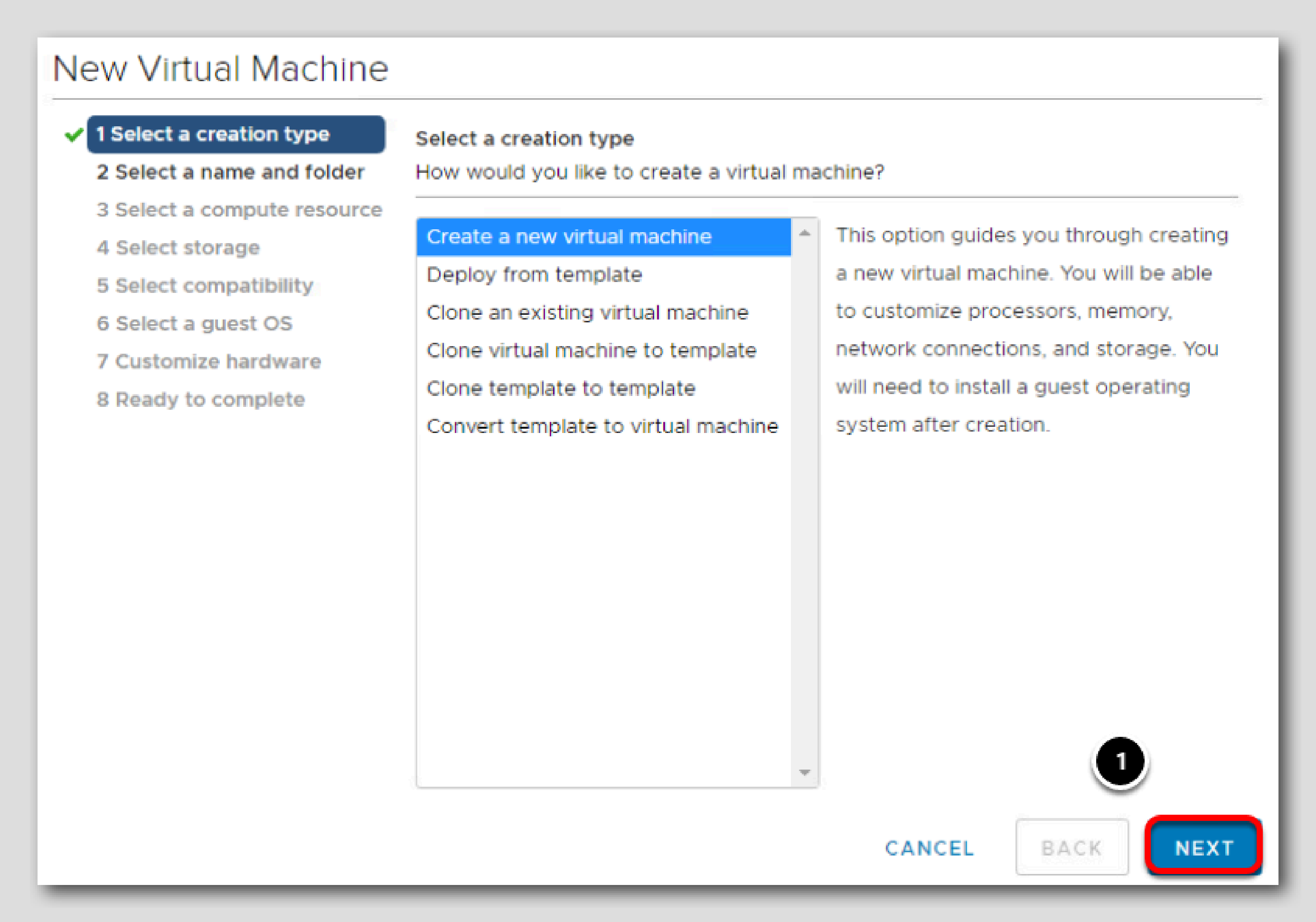
[54]



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

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

Virtual Machine wizard



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 creation type
How would you like to create a virtual machine?

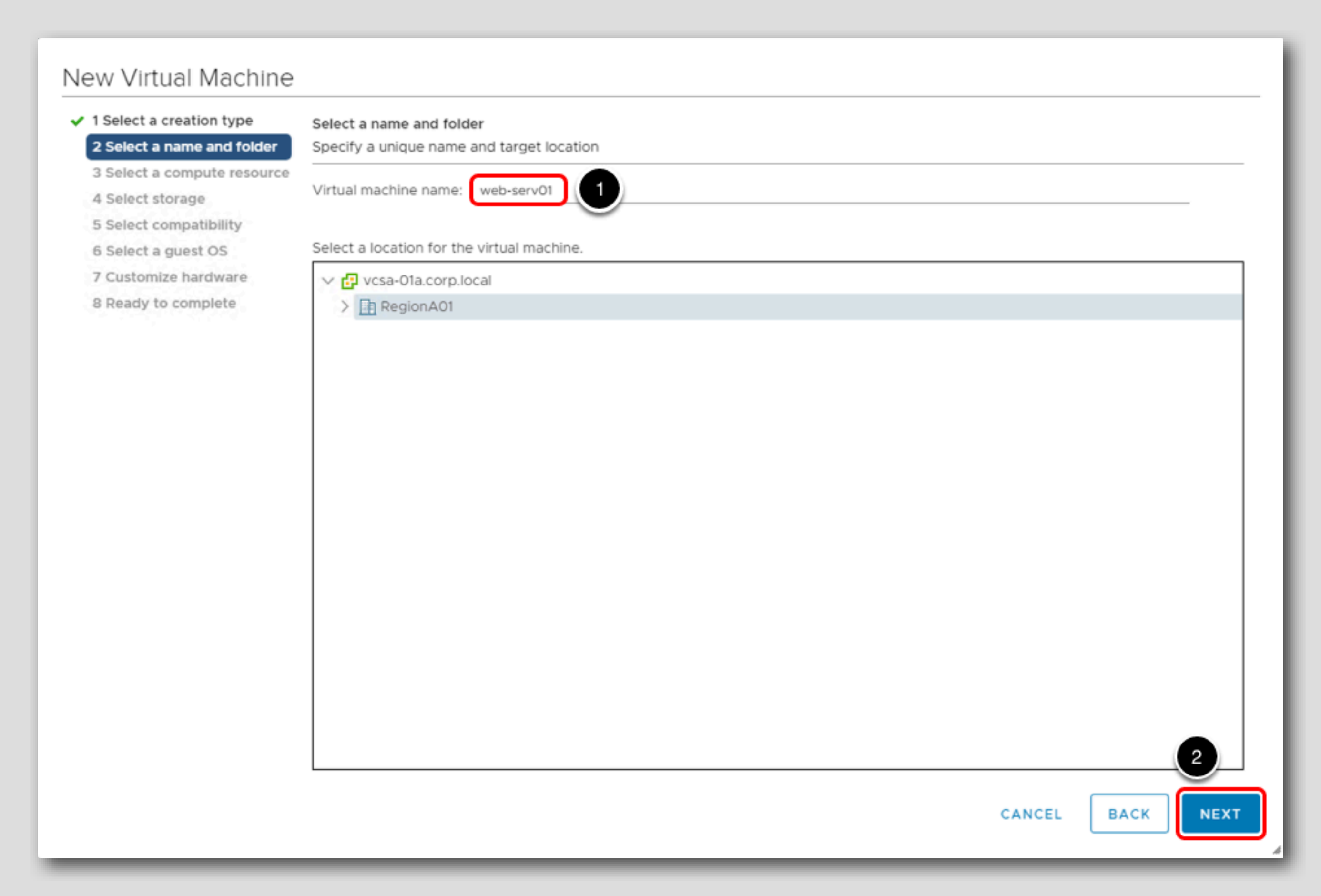
- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

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.

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

Name the Virtual Machine

[56]



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

Virtual machine name: web-serv01

Select a location for the virtual machine.

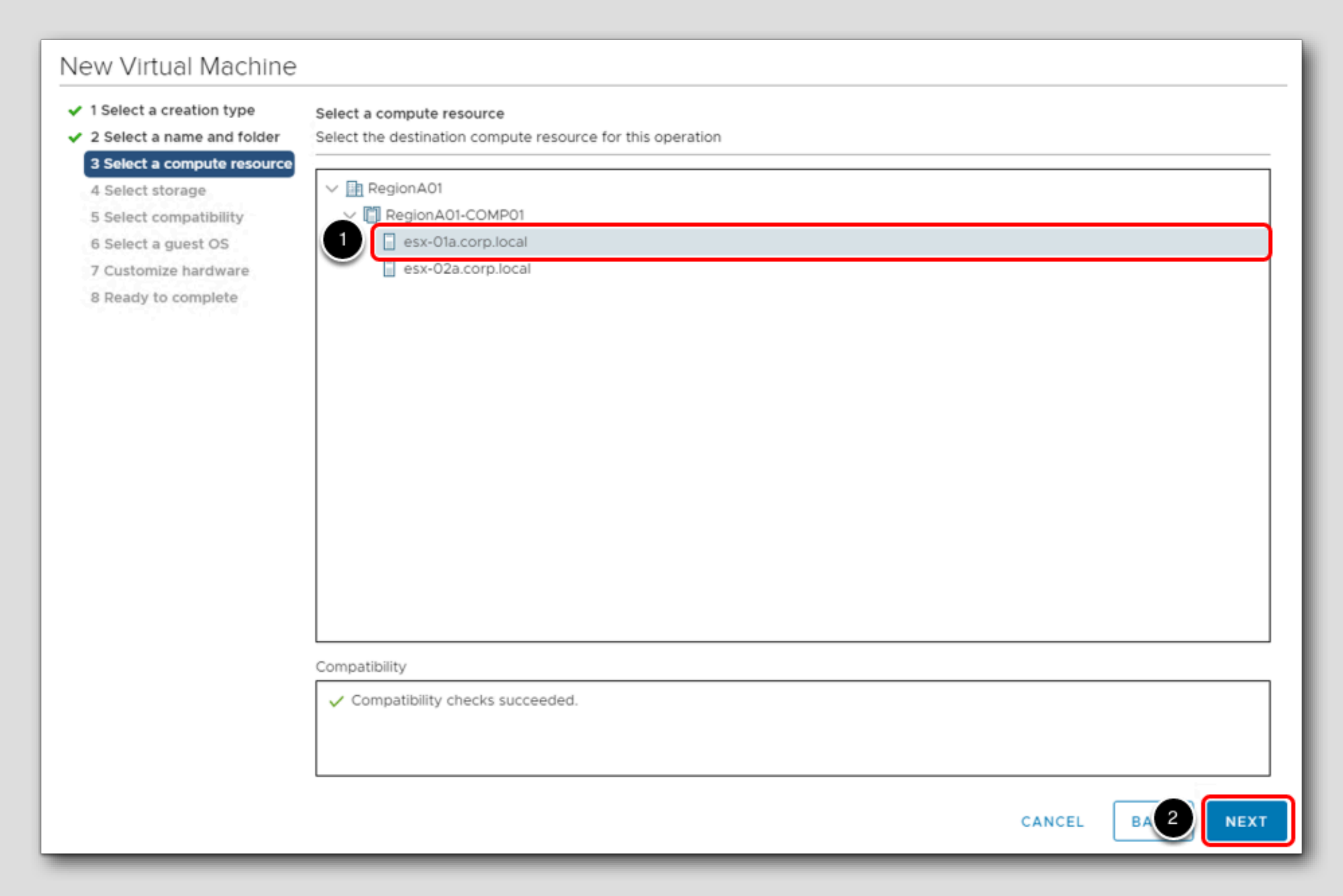
vcsa-01a.corp.local

RegionA01

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

Virtual Machine Placement

[57]



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

- RegionA01
  - RegionA01-COMP01
    - esx-01a.corp.local
    - esx-02a.corp.local

Compatibility

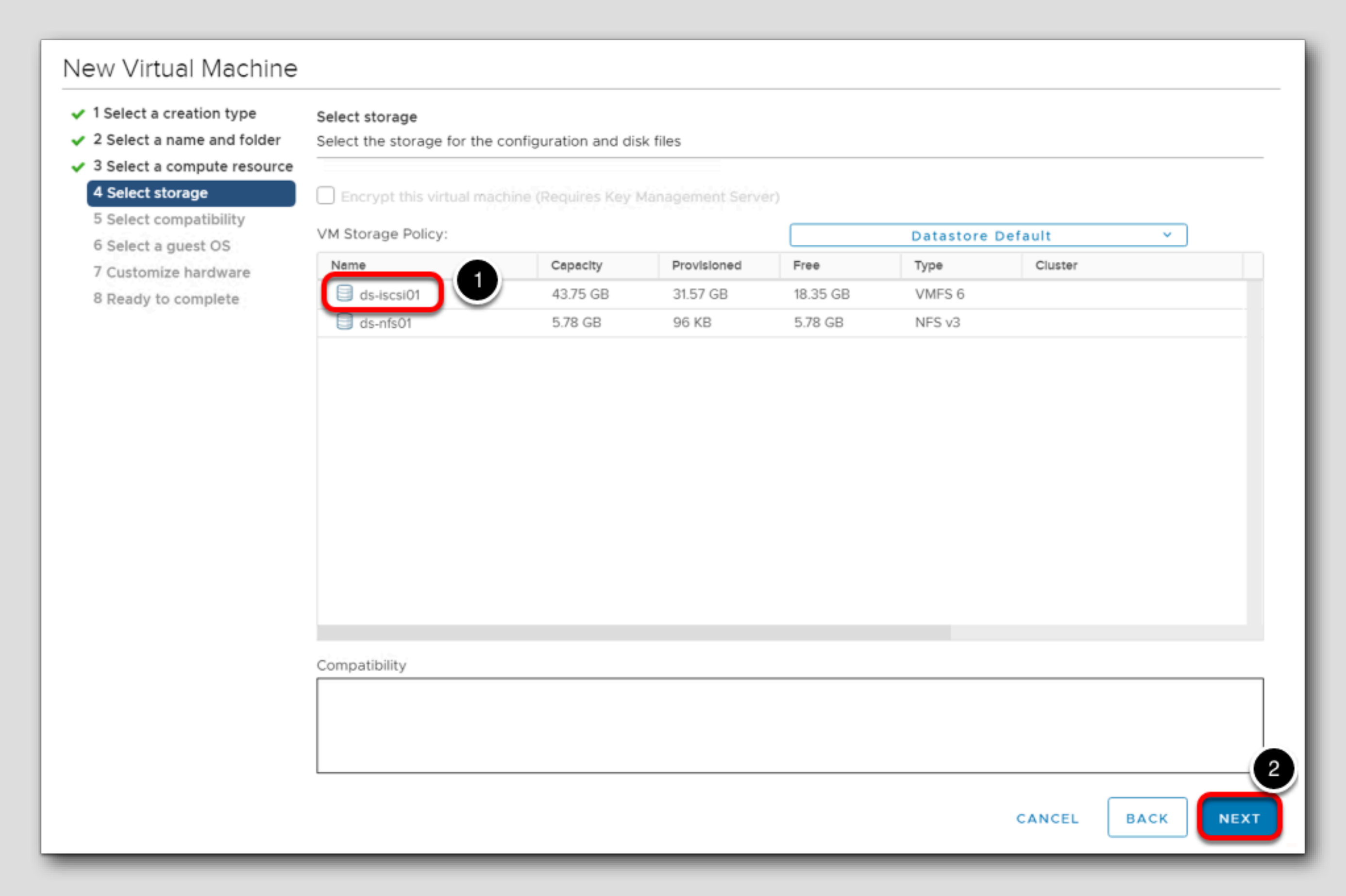
✓ Compatibility checks succeeded.

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

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

Select Storage

[58]



Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy: Datastore Default

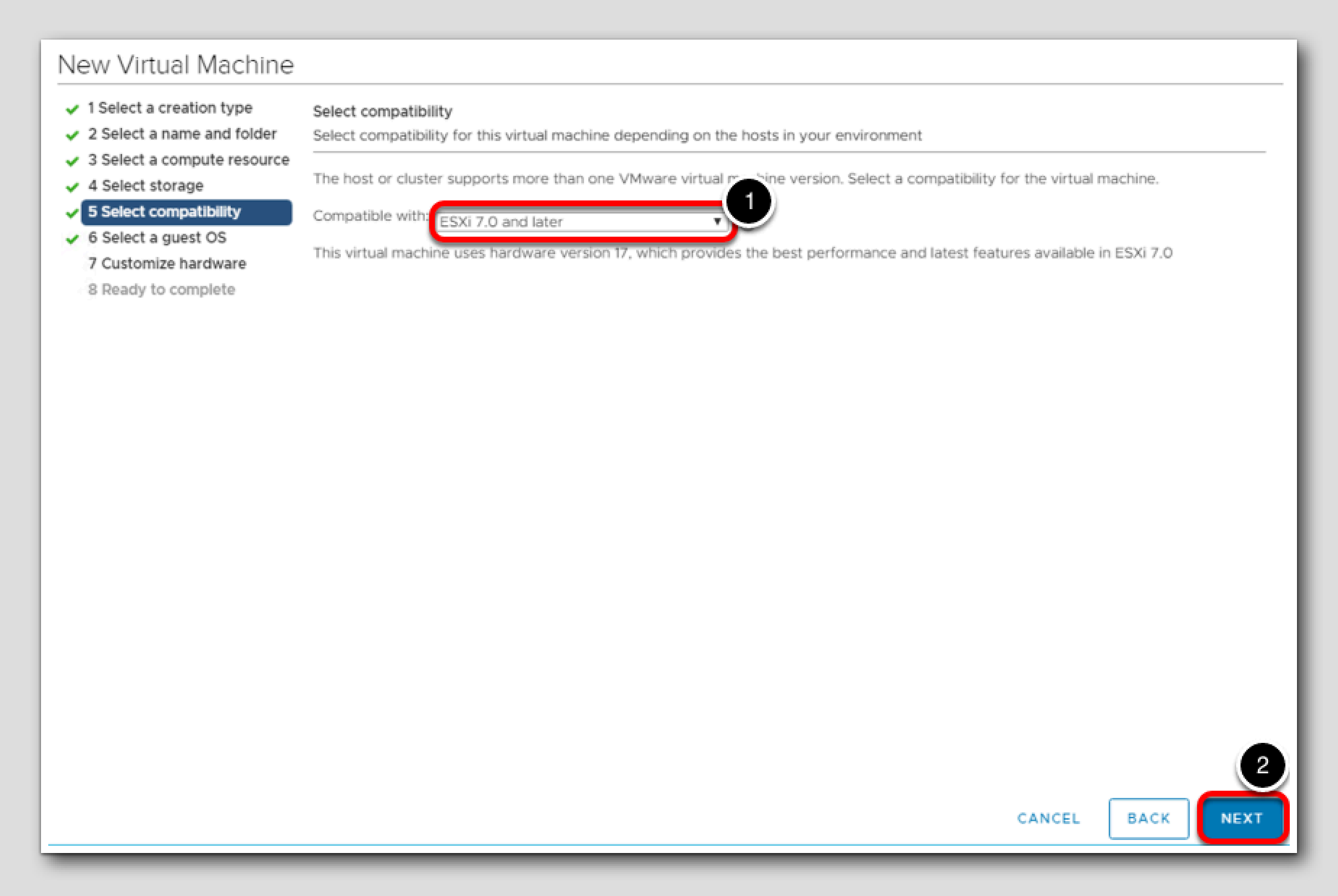
Name	Capacity	Provisioned	Free	Type	Cluster
ds-iscsi01	43.75 GB	31.57 GB	18.35 GB	VMFS 6	
ds-nfs01	5.78 GB	96 KB	5.78 GB	NFS v3	

Compatibility

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

Compatibility

[59]



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

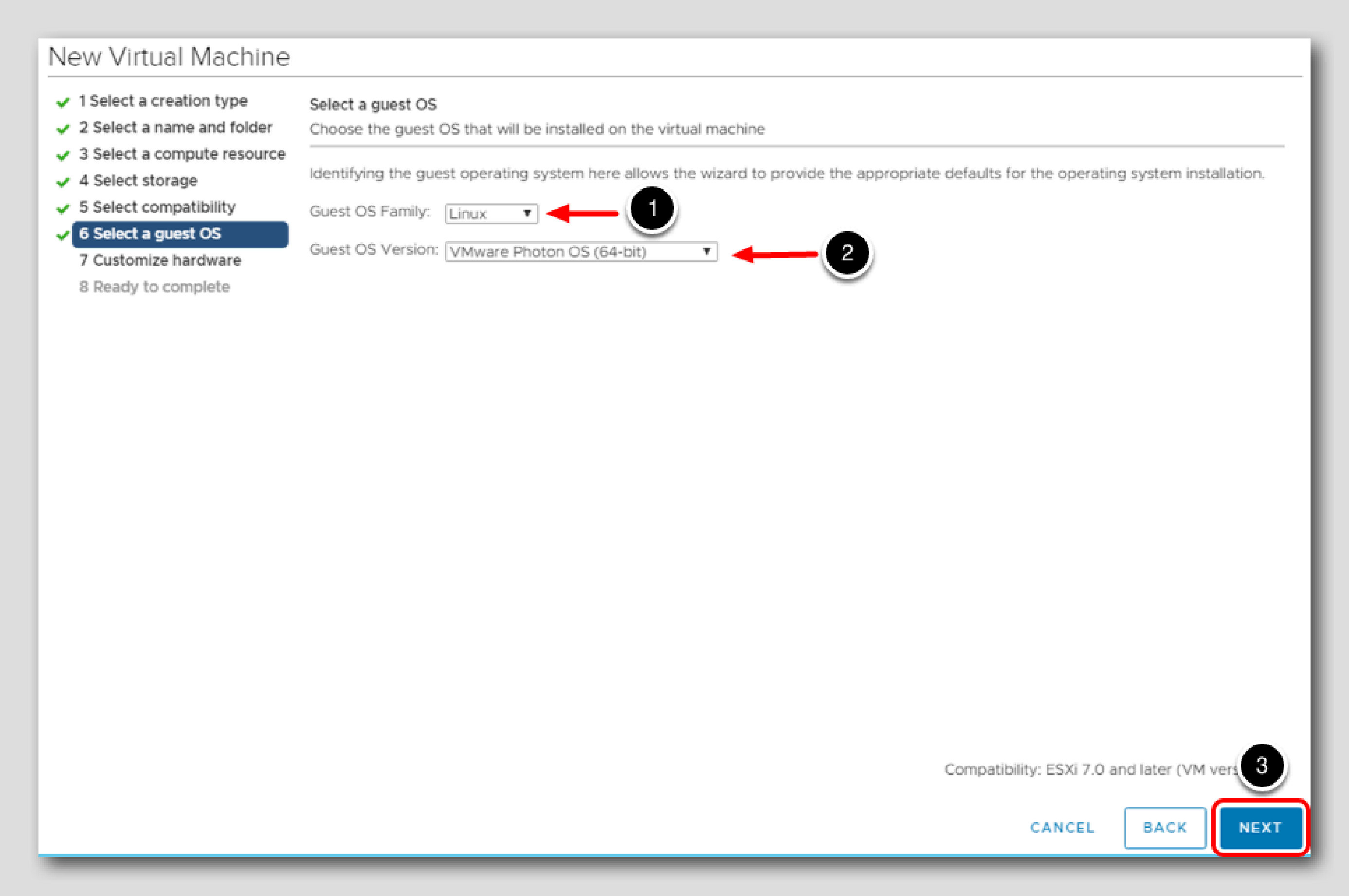
The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 7.0 and later

This virtual machine uses hardware version 17, which provides the best performance and latest features available in ESXi 7.0

1. Select **ESXi 7.0 and later**.
2. Click **Next** to accept.

Guest OS



New Virtual Machine

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

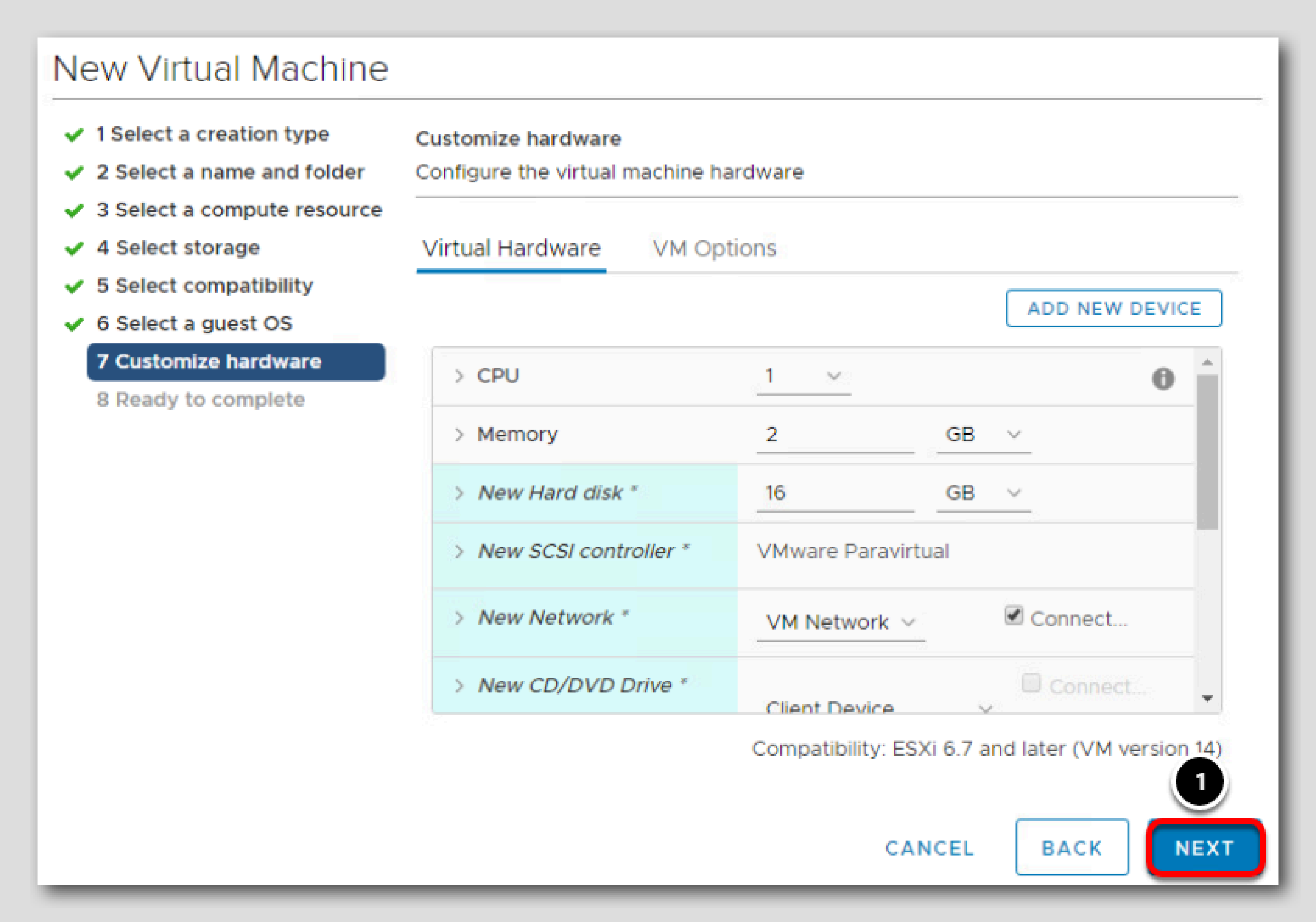
Guest OS Version: VMware Photon OS (64-bit)

Compatibility: ESXi 7.0 and later (VM vers

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

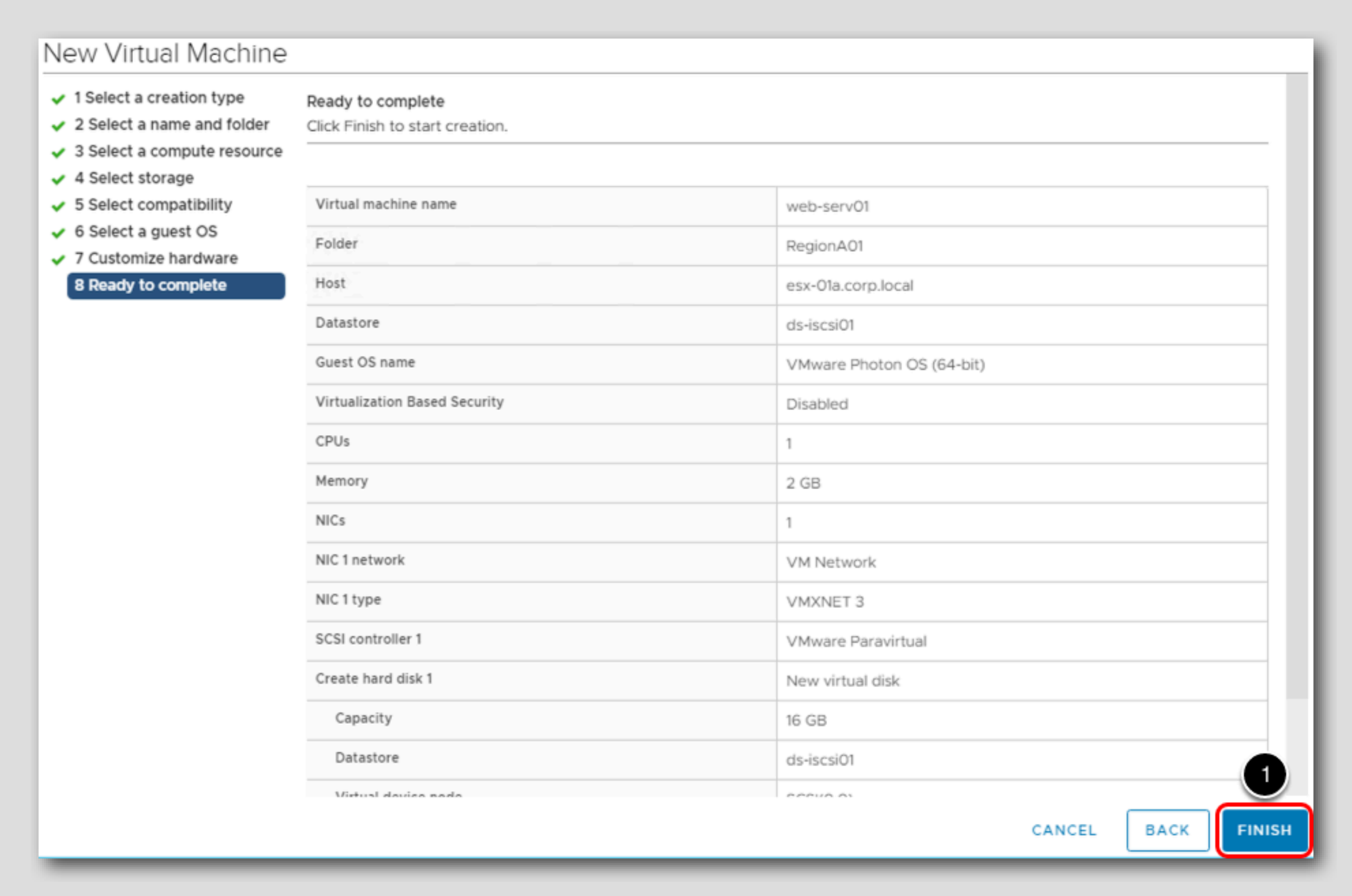
CPU	1	
Memory	2	GB
New Hard disk *	16	GB
New SCSI controller *	VMware Paravirtual	
New Network *	VM Network	☑ Connect...
New CD/DVD Drive *	Client Device	□ Connect...

Compatibility: ESXi 6.7 and later (VM version 14)

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

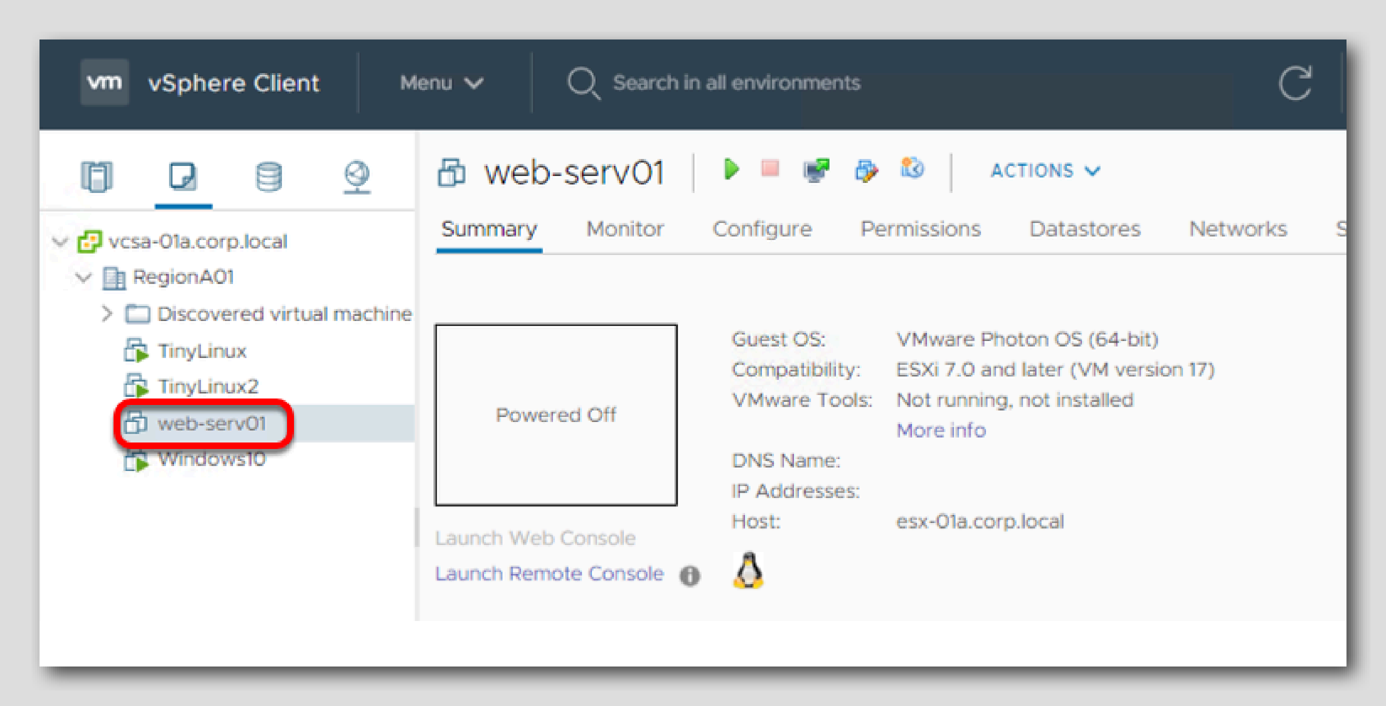
Click Finish to start creation.

Virtual machine name	web-serv01
Folder	RegionA01
Host	esx-01a.corp.local
Datastore	ds-iscsi01
Guest OS name	VMware Photon OS (64-bit)
Virtualization Based Security	Disabled
CPUs	1
Memory	2 GB
NICs	1
NIC 1 network	VM Network
NIC 1 type	VMXNET 3
SCSI controller 1	VMware Paravirtual
Create hard disk 1	New virtual disk
Capacity	16 GB
Datastore	ds-iscsi01
Virtual device node	SCSI(0:0)

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



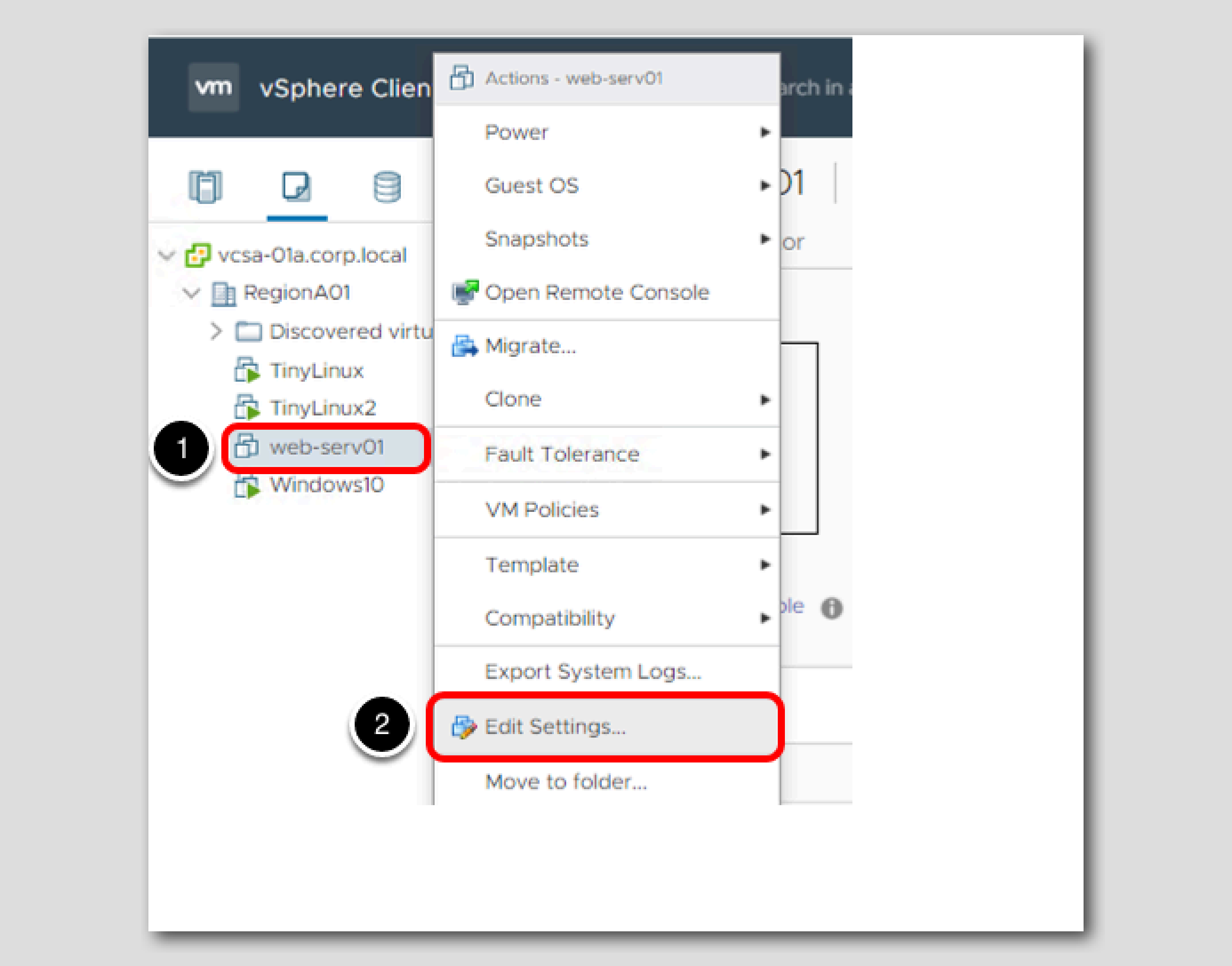
Guest OS: VMware Photon OS (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Not running, not installed
More info
DNS Name:
IP Addresses:
Host: esx-01a.corp.local

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

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

Attaching an ISO to a Virtual Machine

[64]

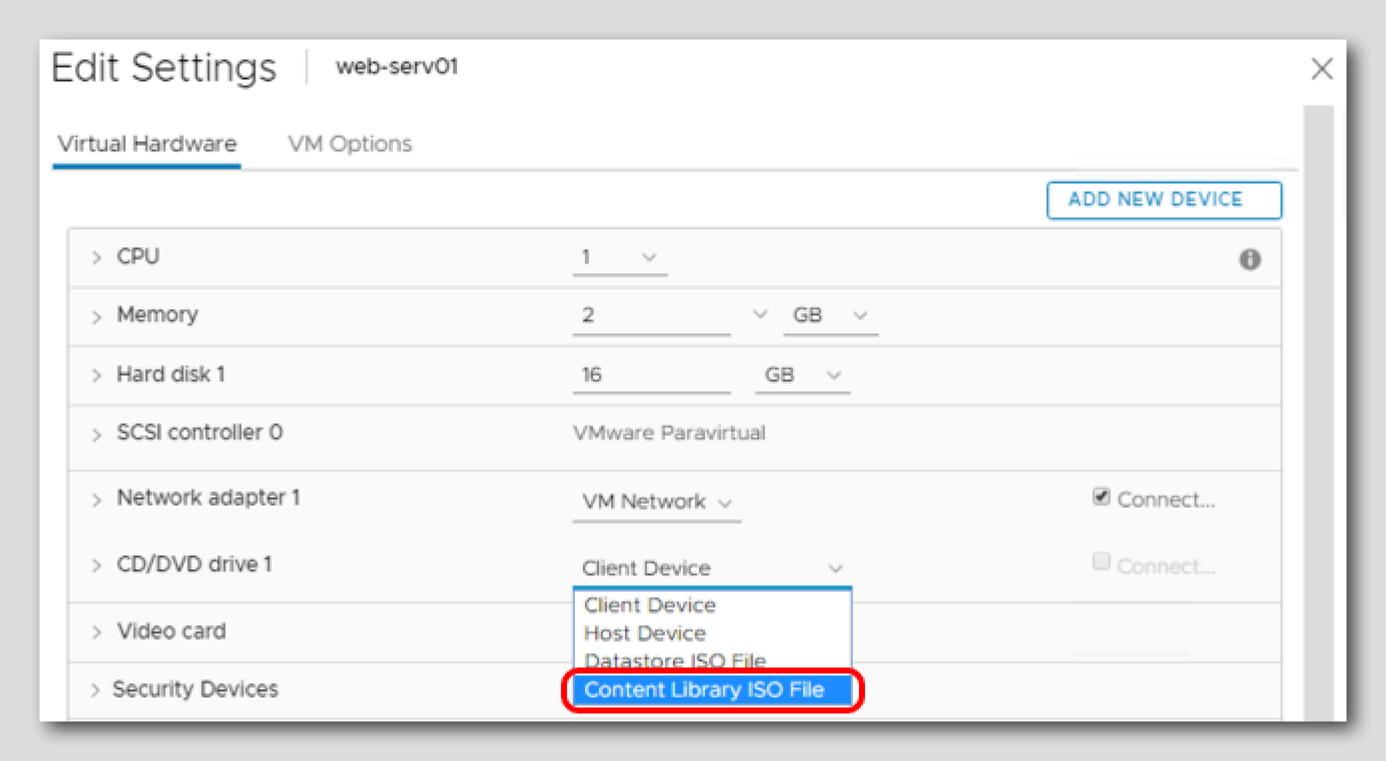


To make it easier to install operating systems on virtual machines, ISO images can be used. These can be kept in the same storage used for virtual machines. In addition, vCenter offers a Content Library as a repository. Content Libraries can then be synchronized to ensure every location is using the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

[65]



Edit Settings | web-serv01

Virtual Hardware | VM Options

ADD NEW DEVICE

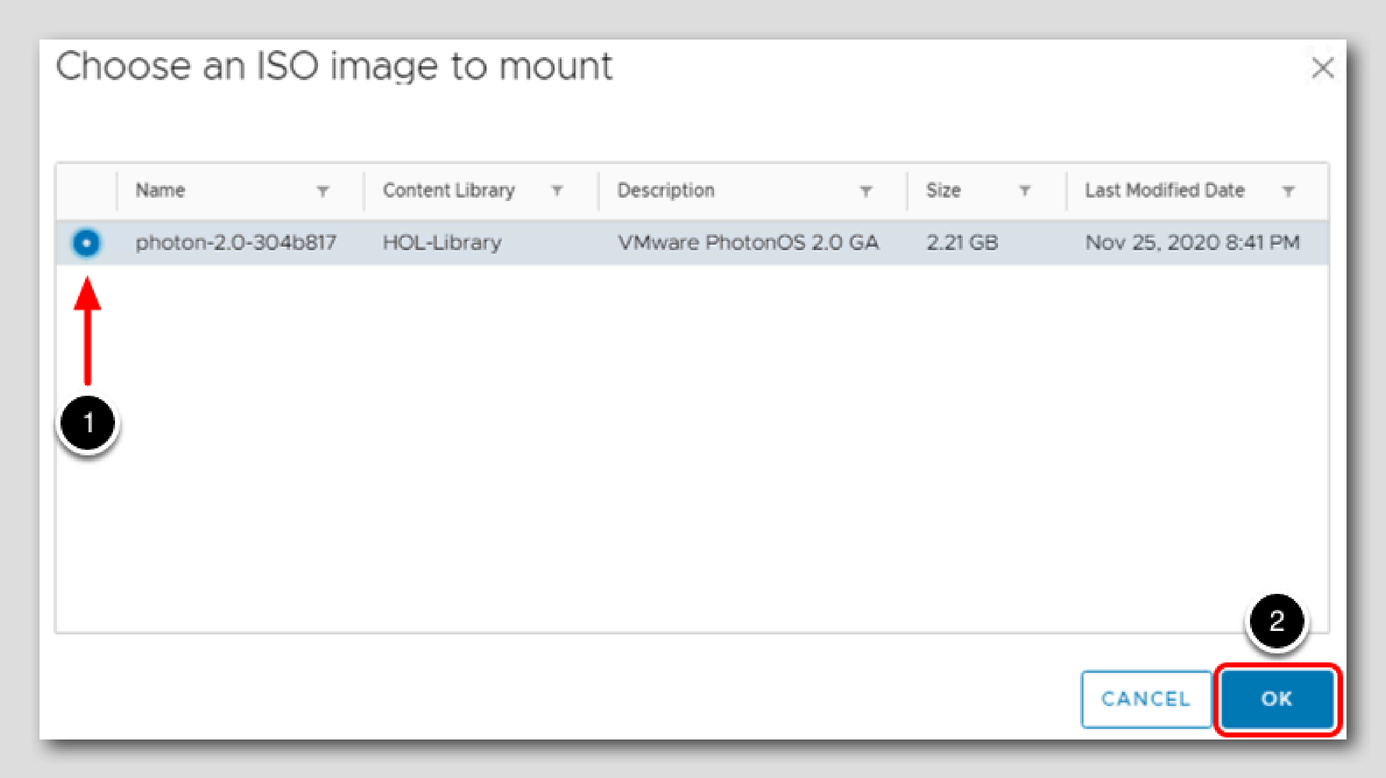
CPU	1	
Memory	2 GB	
Hard disk 1	16 GB	
SCSI controller 0	VMware Paravirtual	
Network adapter 1	VM Network	☑ Connect...
CD/DVD drive 1	Client Device	□ Connect...
Video card		
Security Devices		

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

[66]



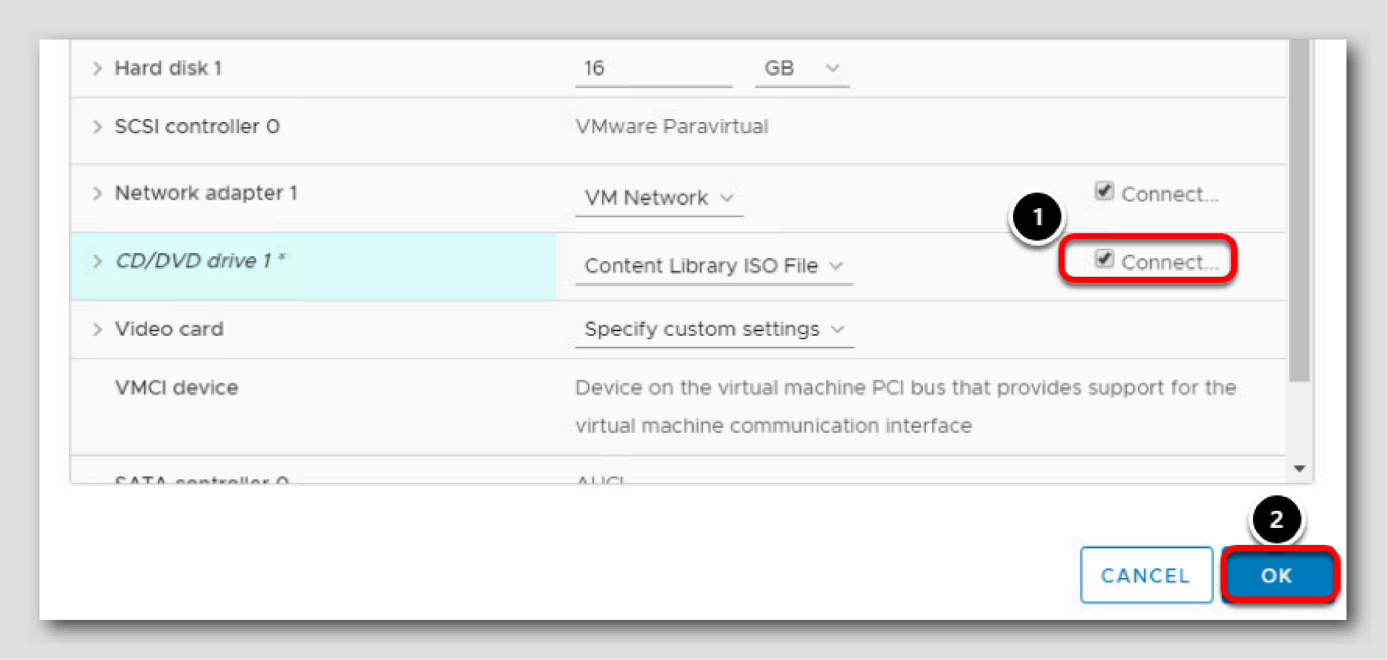
Choose an ISO image to mount

	Name	Content Library	Description	Size	Last Modified Date
●	photon-2.0-304b817	HOL-Library	VMware PhotonOS 2.0 GA	2.21 GB	Nov 25, 2020 8:41 PM

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

Connect the drive

[67]



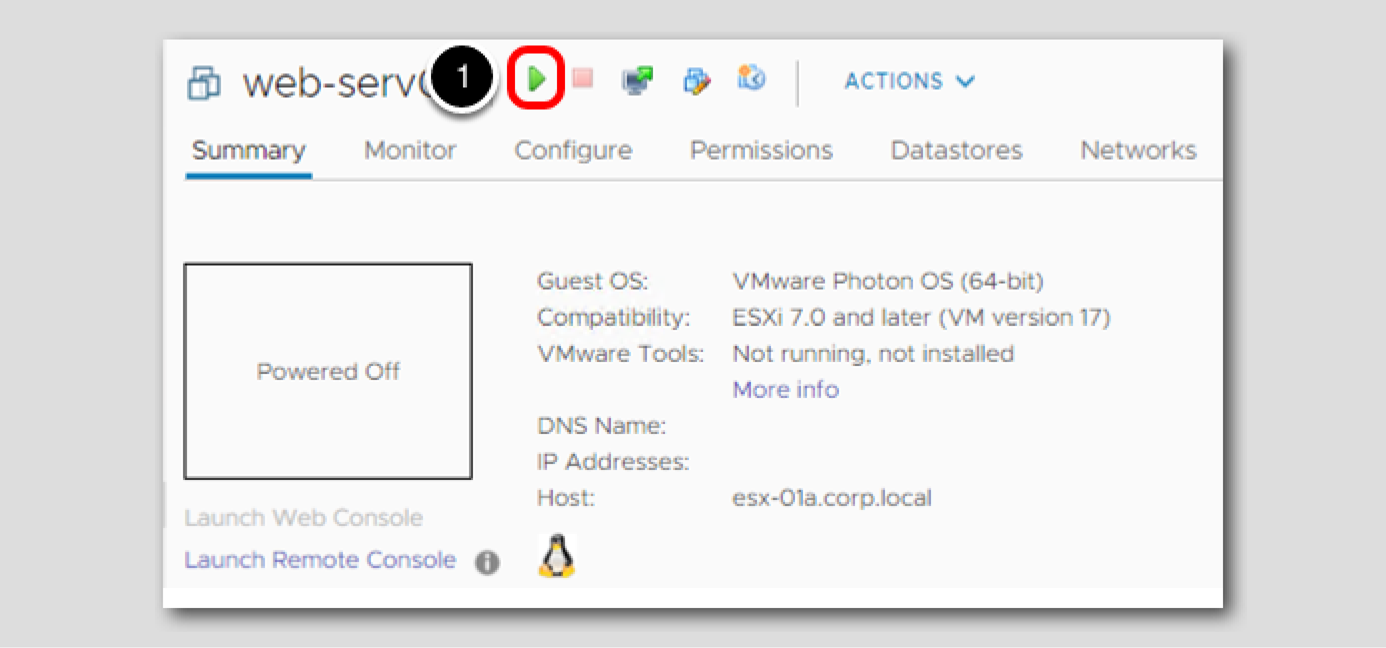
> Hard disk 1	16 GB ⌄	
> SCSI controller 0	VMware Paravirtual	
> Network adapter 1	VM Network ⌄	☑ Connect...
> *CD/DVD drive 1 **	Content Library ISO File ⌄	☑ Connect...
> Video card	Specify custom settings ⌄	
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface	
SATA controller 0	AHCI	

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

[68]

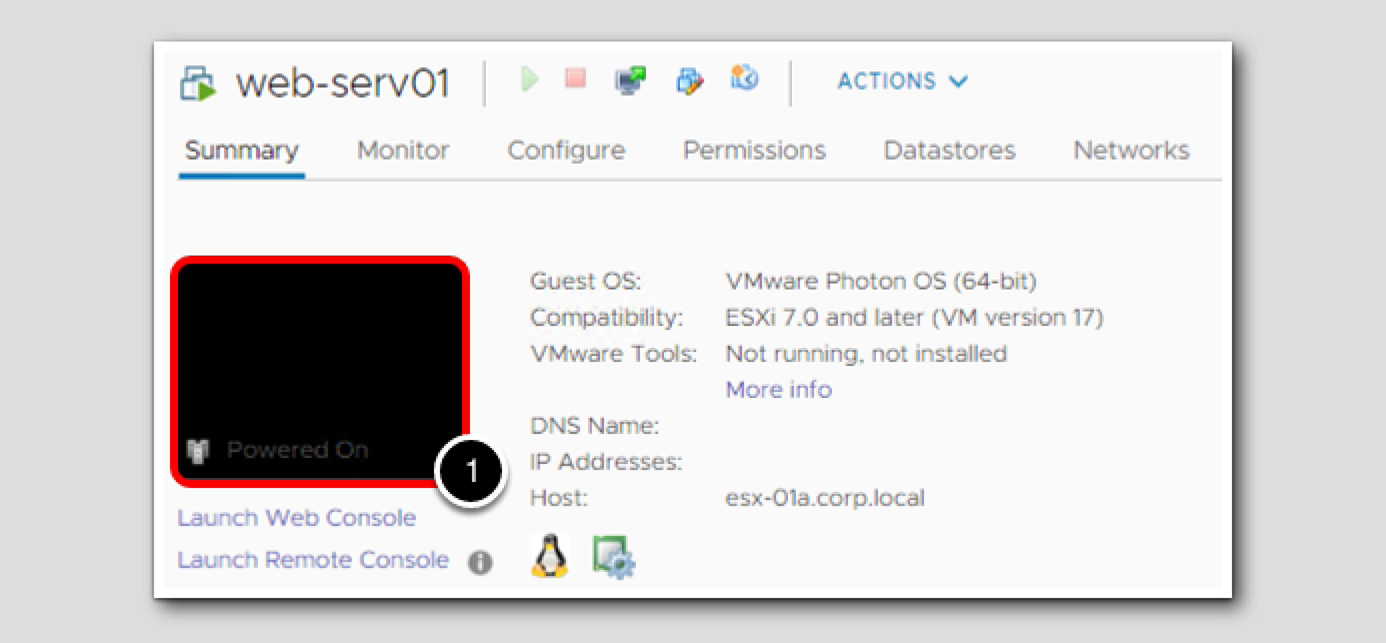


Guest OS: VMware Photon OS (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Not running, not installed
More info
DNS Name:
IP Addresses:
Host: esx-01a.corp.local

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

Launch Console

[69]

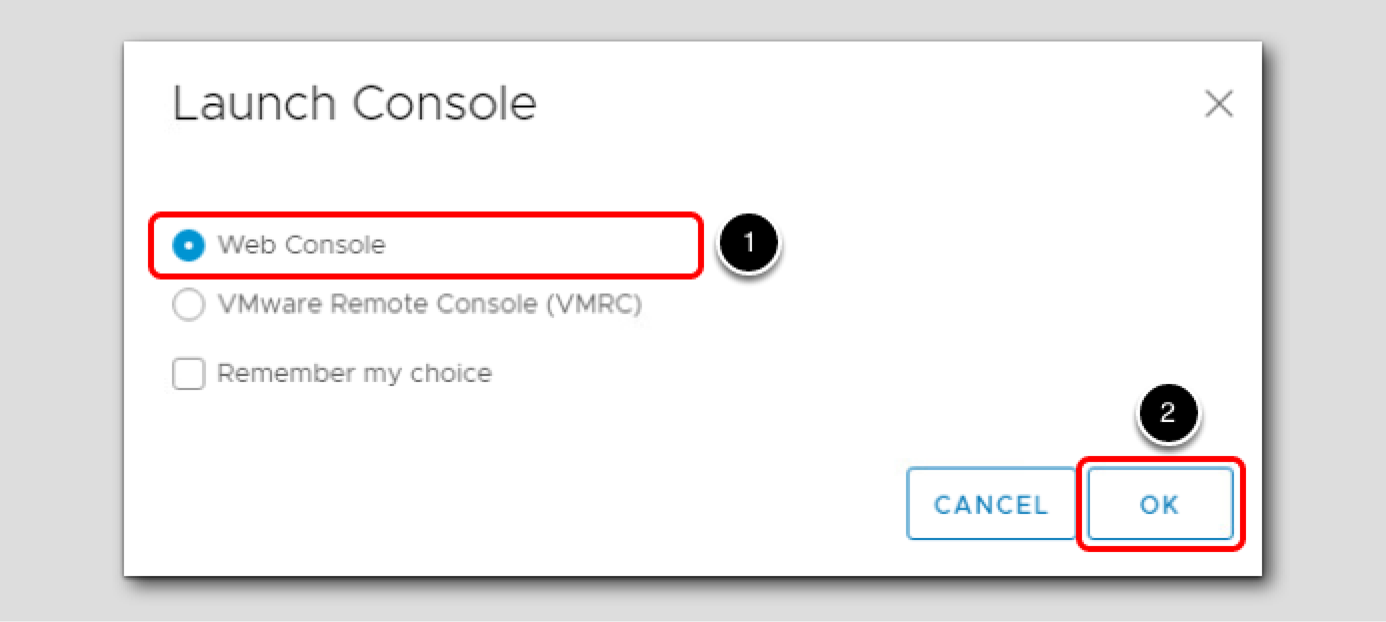


Guest OS: VMware Photon OS (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Not running, not installed
More info
DNS Name:
IP Addresses:
Host: esx-01a.corp.local

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

Web Console

[70]

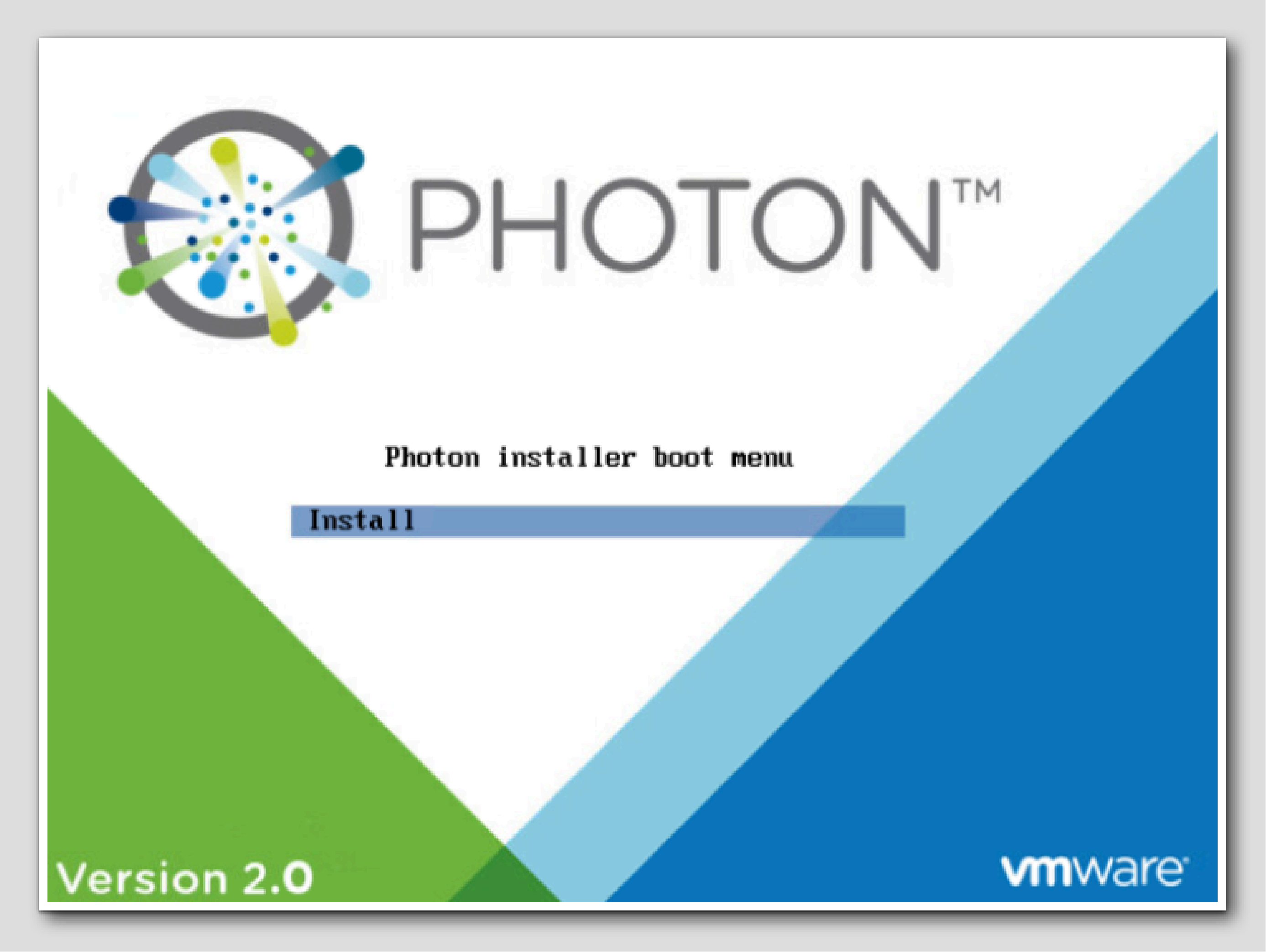


1. Select the **Web Console**.
2. Click **OK**.

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

Photon Boot Screen

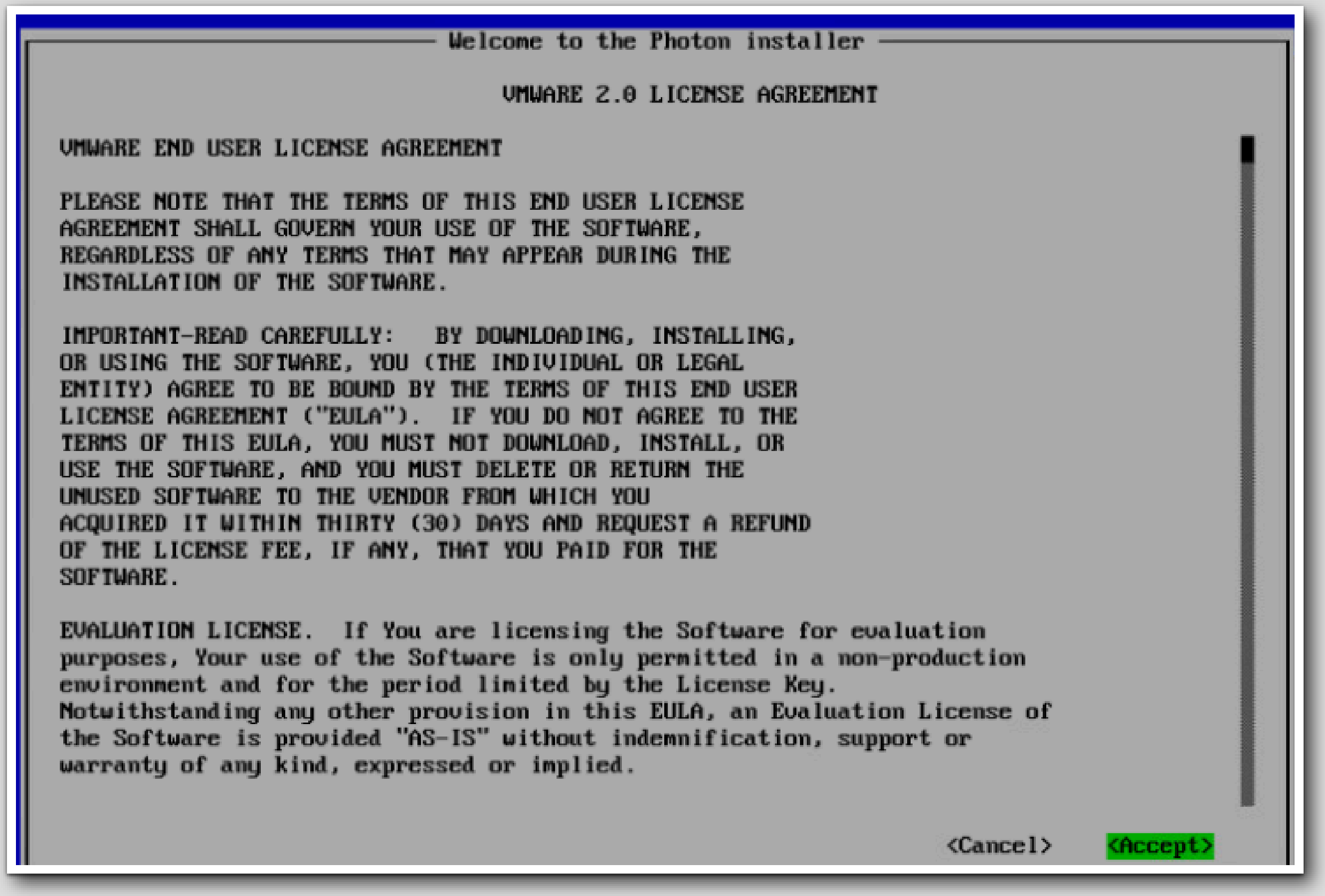
[71]



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

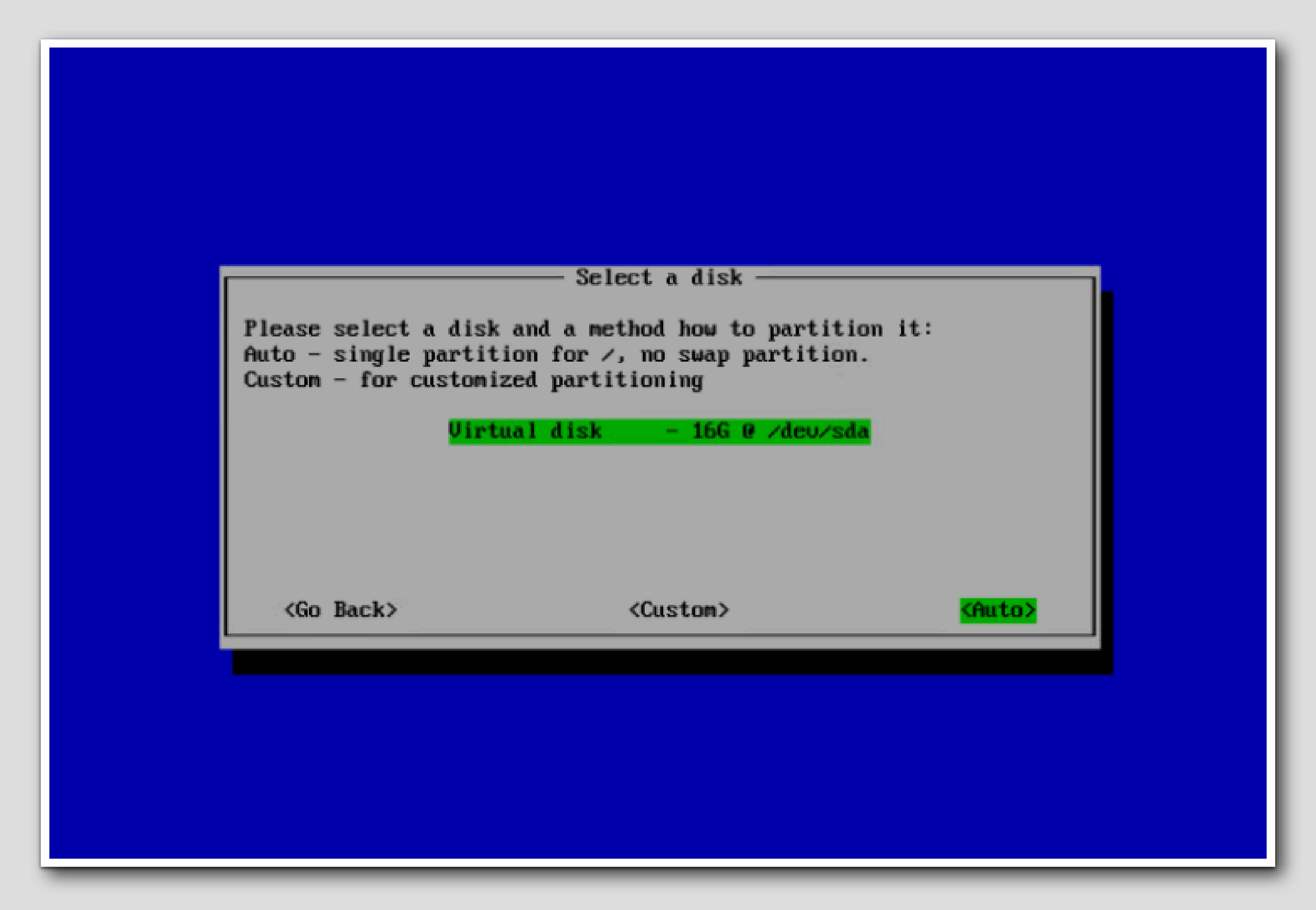


```
Welcome to the Photon installer

VMWARE 2.0 LICENSE AGREEMENT

VMWARE END USER LICENSE AGREEMENT

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

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

EVALUATION LICENSE.  If You are licensing the Software for evaluation
purposes, Your use of the Software is only permitted in a non-production
environment and for the period limited by the License Key.
Notwithstanding any other provision in this EULA, an Evaluation License of
the Software is provided "AS-IS" without indemnification, support or
warranty of any kind, expressed or implied.
```

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

1. Press Enter to accept.

Select Disk

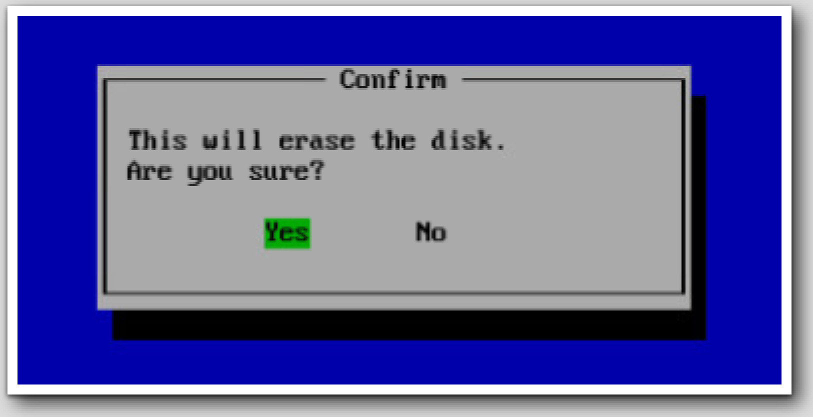


```
Select a disk

Please select a disk and a method how to partition it:
Auto - single partition for /, no swap partition.
Custom - for customized partitioning

        Virtual disk      - 16G @ /dev/sda
```

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

Confirm

[74]



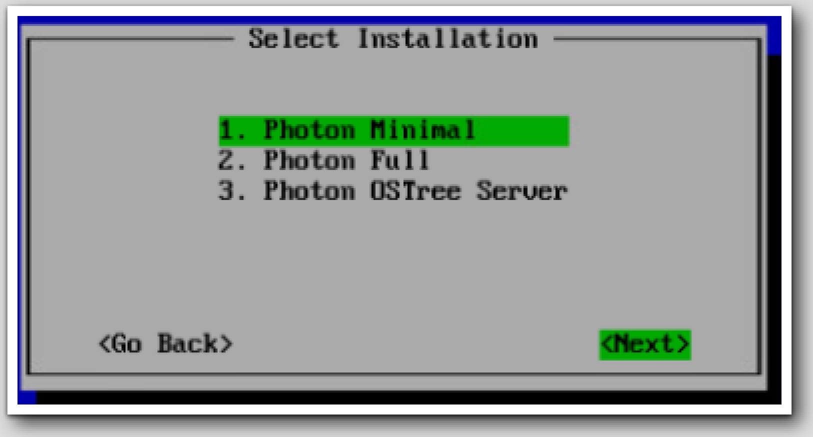
Confirm

This will erase the disk.
Are you sure?

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

Select Installation

[75]

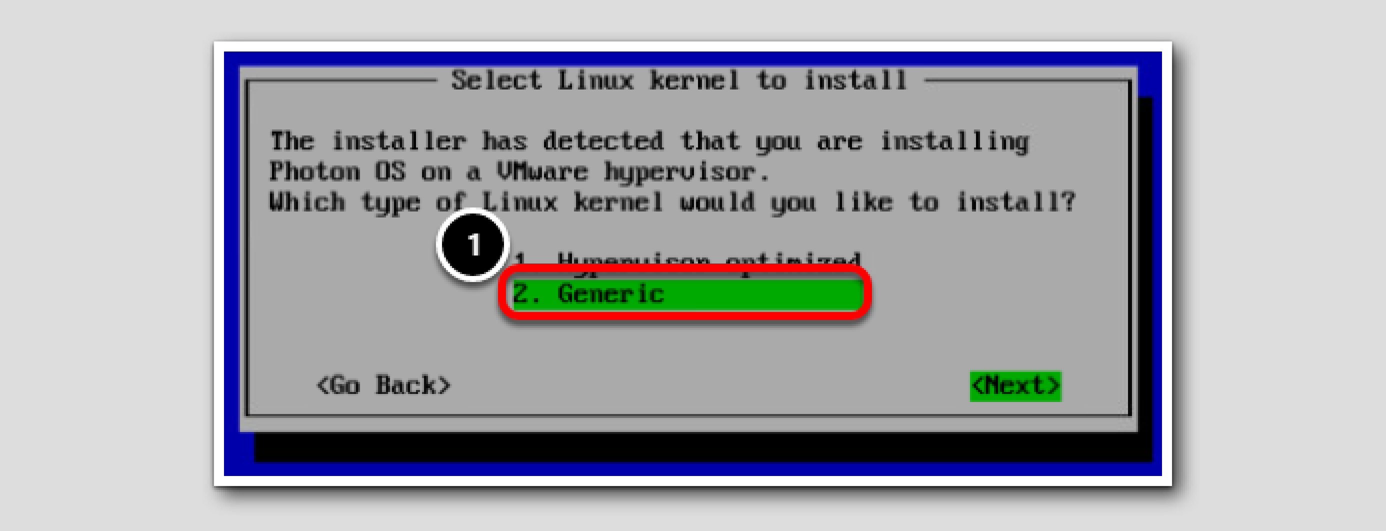


Select Installation

1. Photon Minimal
2. Photon Full
3. Photon OSTree Server

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

Linux Kernel [76]

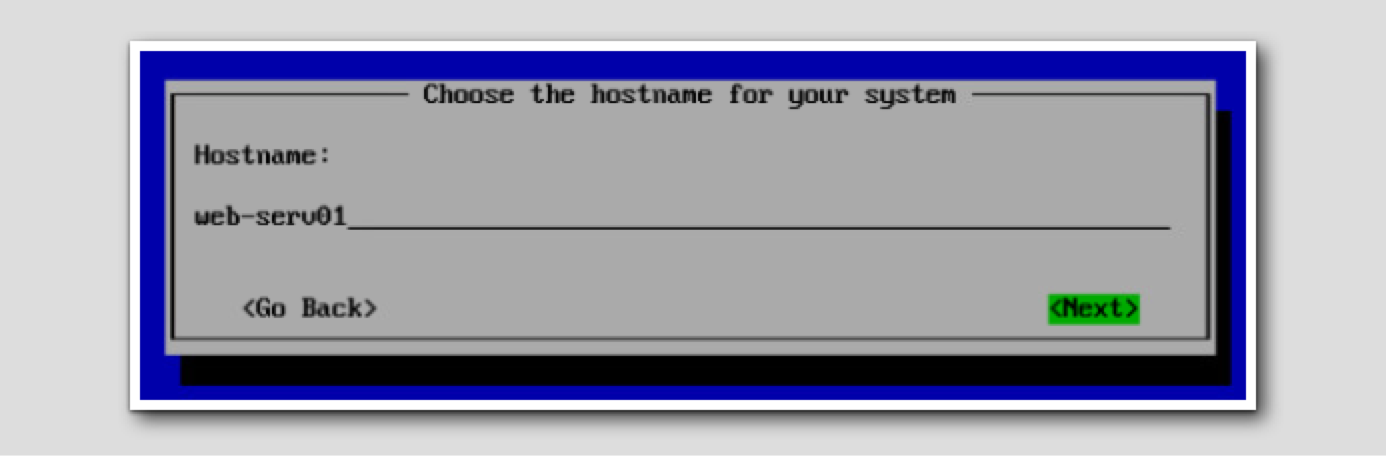


```
Select Linux kernel to install

The installer has detected that you are installing
Photon OS on a VMware hypervisor.
Which type of Linux kernel would you like to install?

        1. Hypervisor optimized
        2. Generic

  <Go Back>                                    <Next>
```

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 [77]

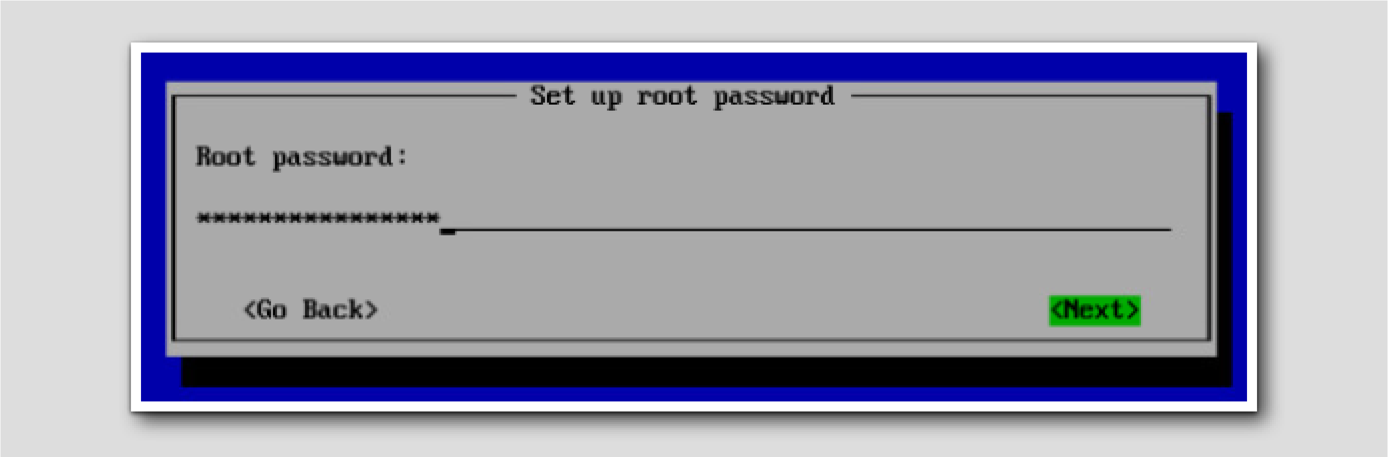


```
Choose the hostname for your system

Hostname:

web-serv01_______________________________________________

  <Go Back>                                    <Next>
```

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

Password

[78]



Set up root password

Root password:

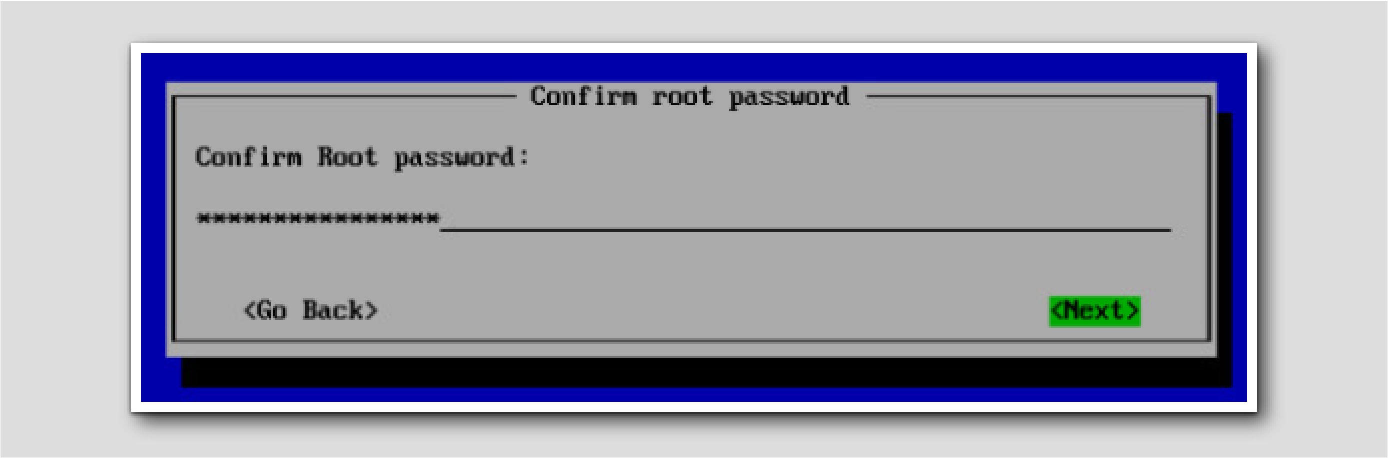
```
****************
```

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

[79]



Confirm root password

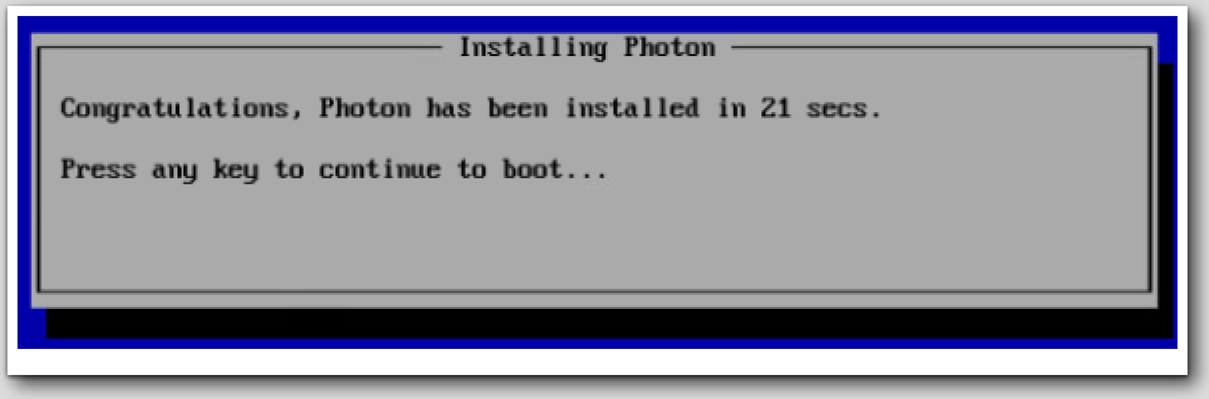
Confirm Root password:

```
****************
```

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

Installation Complete

[80]



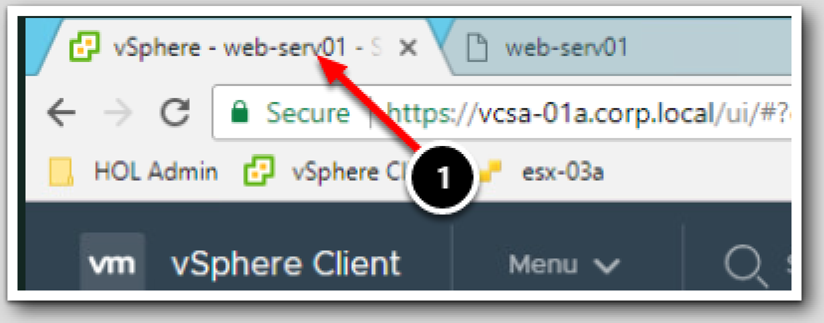
```
Installing Photon

Congratulations, Photon has been installed in 21 secs.

Press any key to continue to boot...
```

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

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

vSphere Tab

[81]

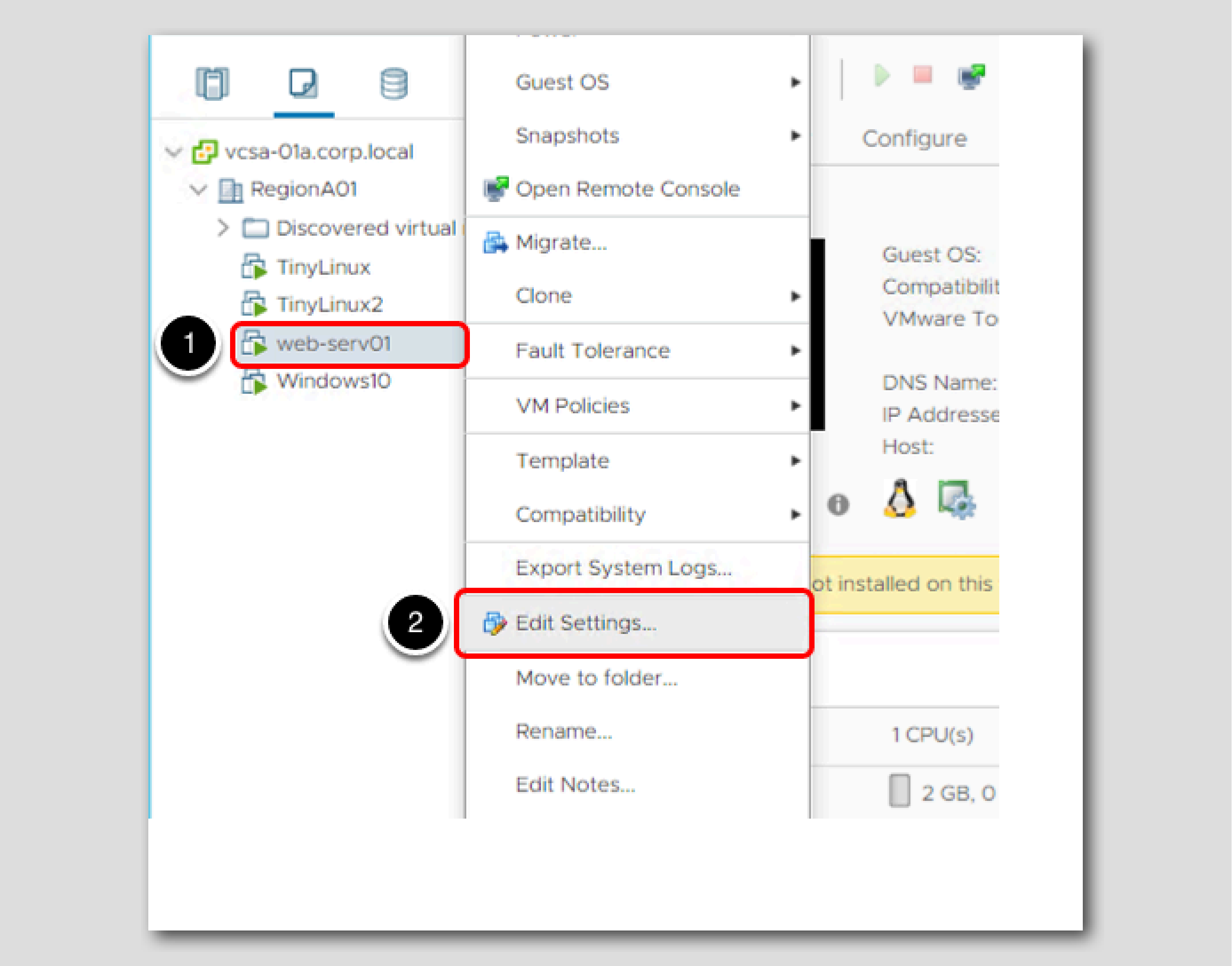


Now that the operating system has been installed and is up and running, the ISO image needs to be disconnected from the virtual machine.

1. Select the **vSphere- web-serv01** tab.

Edit Settings

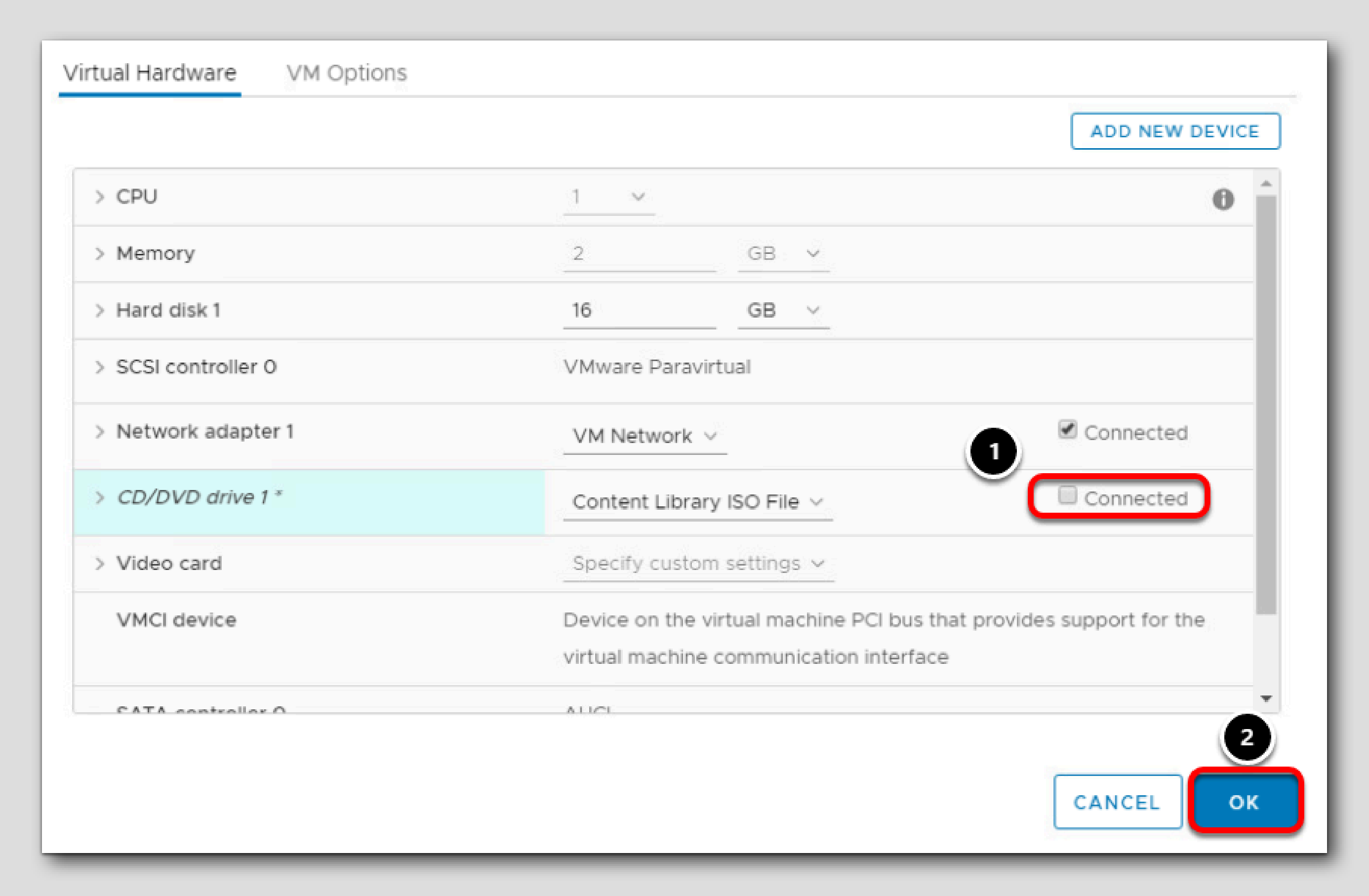
[82]



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

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

Disconnect CD/DVD

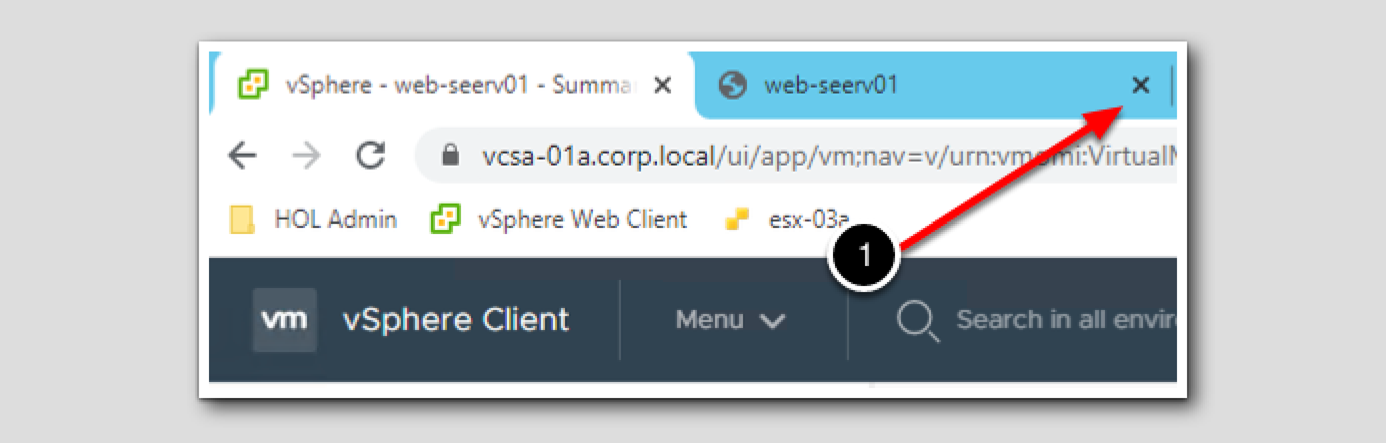


CPU	1		
Memory	2	GB	
Hard disk 1	16	GB	
SCSI controller 0	VMware Paravirtual		
Network adapter 1	VM Network		☑ Connected
CD/DVD drive 1 *	Content Library ISO File		□ Connected
Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
SATA controller 0	AHCI		

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

web-serv01 Console

[84]



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

Cloning Virtual Machines and Using Templates

[85]

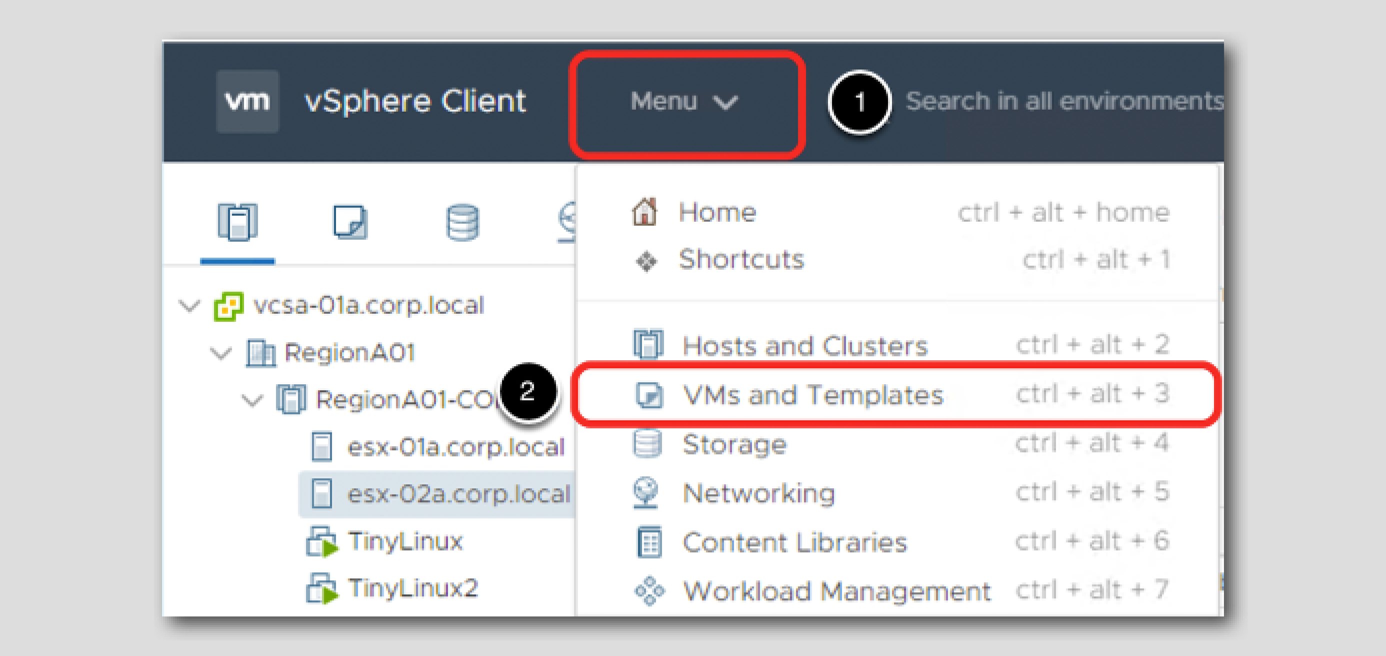
VMware provides several ways to provision vSphere virtual machines. In the last lesson, you saw how to create a virtual machine and manually install the operating system.

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

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

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

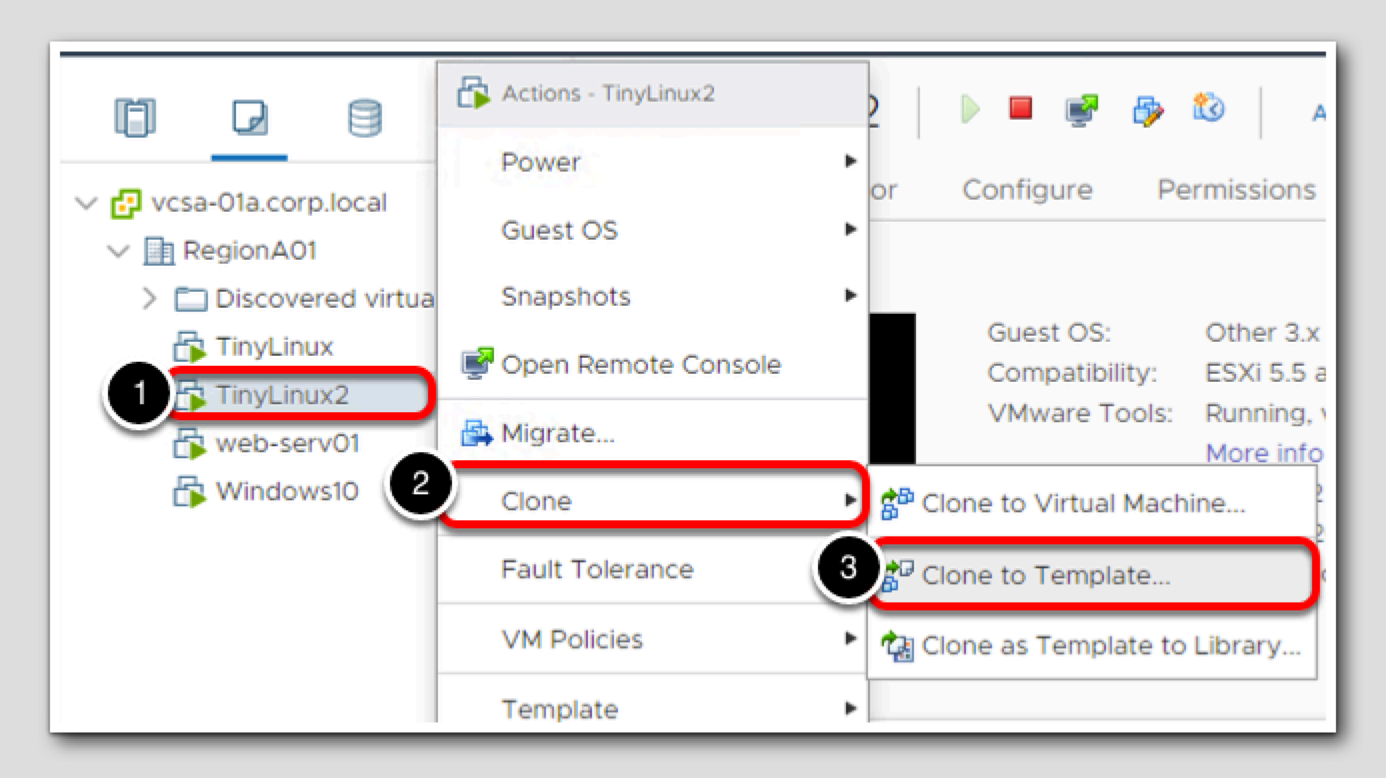
Navigate to the VMs and Templates management pane



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

Launch the Clone Virtual Machine to Template wizard

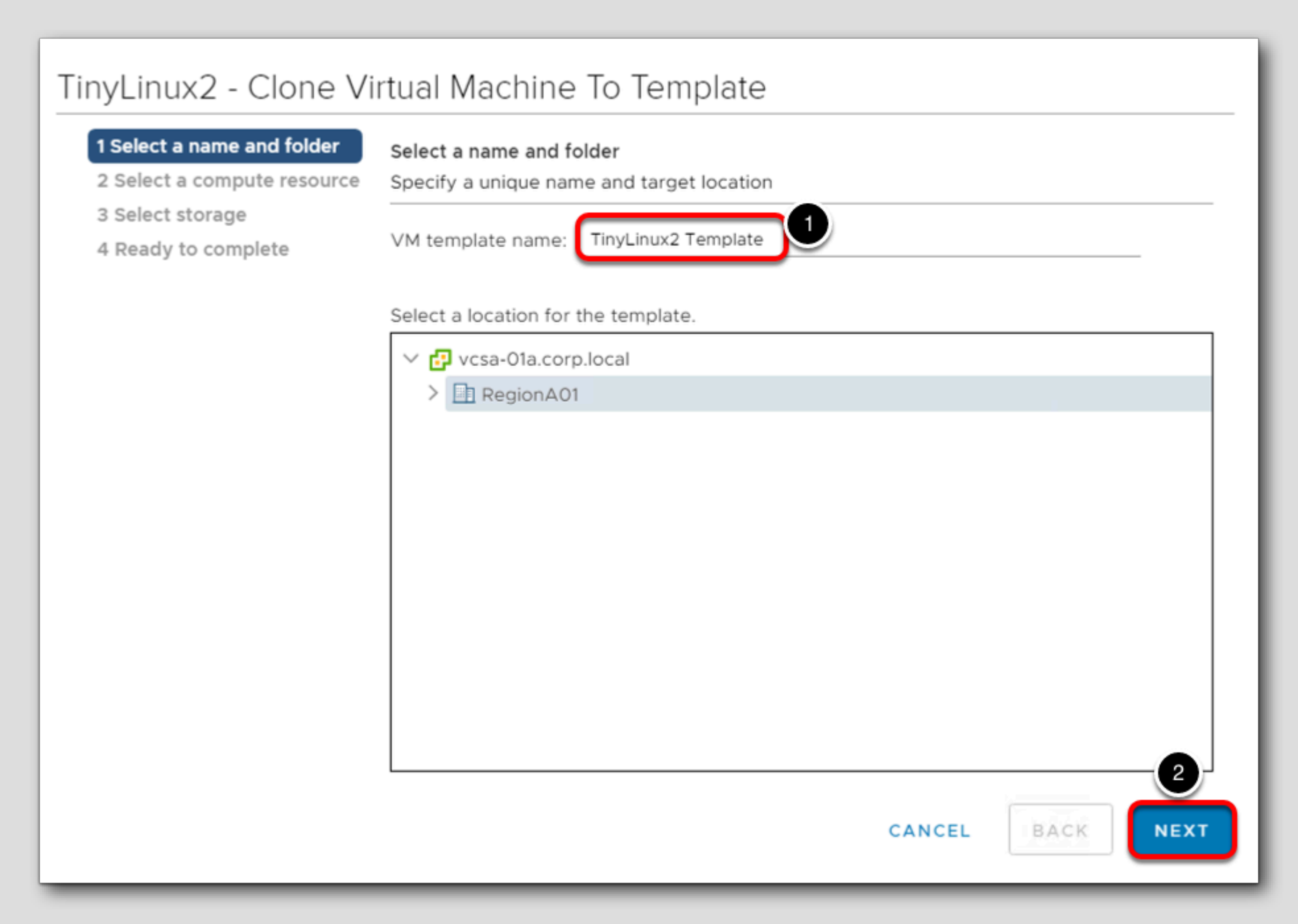
[87]



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

Select a name and folder

[88]



TinyLinux2 - Clone Virtual Machine To Template

Select a name and folder

Specify a unique name and target location

VM template name: TinyLinux2 Template

Select a location for the template.

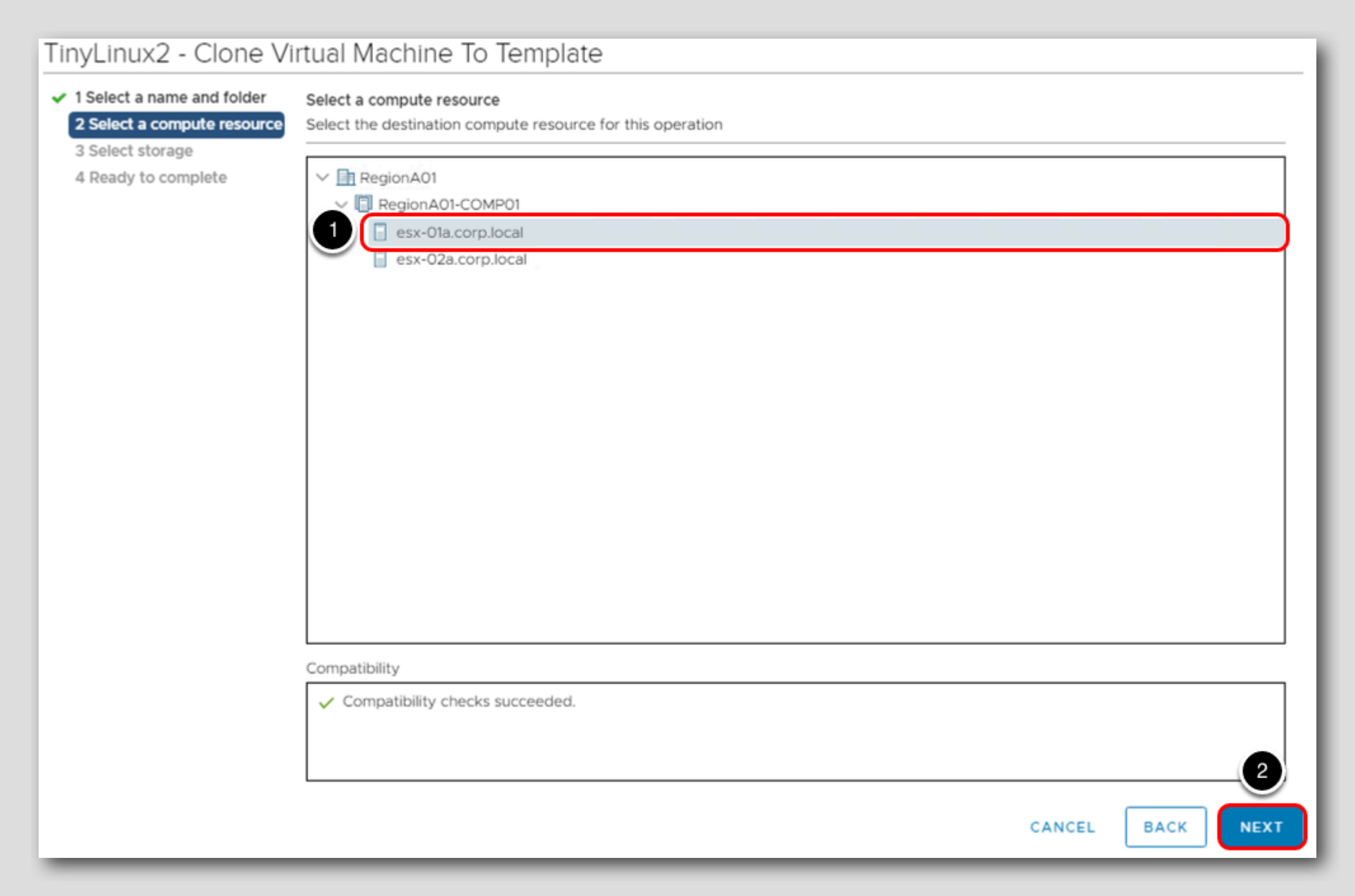
1. In the Clone Virtual Machine to Template wizard, provide a name for the Template - TinyLinux2 Template

Please leave the location as RegionA01 for this lab.

2. Click Next

Select Compute Resource

[89]



TinyLinux2 - Clone Virtual Machine To Template

Select a compute resource

Select the destination compute resource for this operation

Compatibility

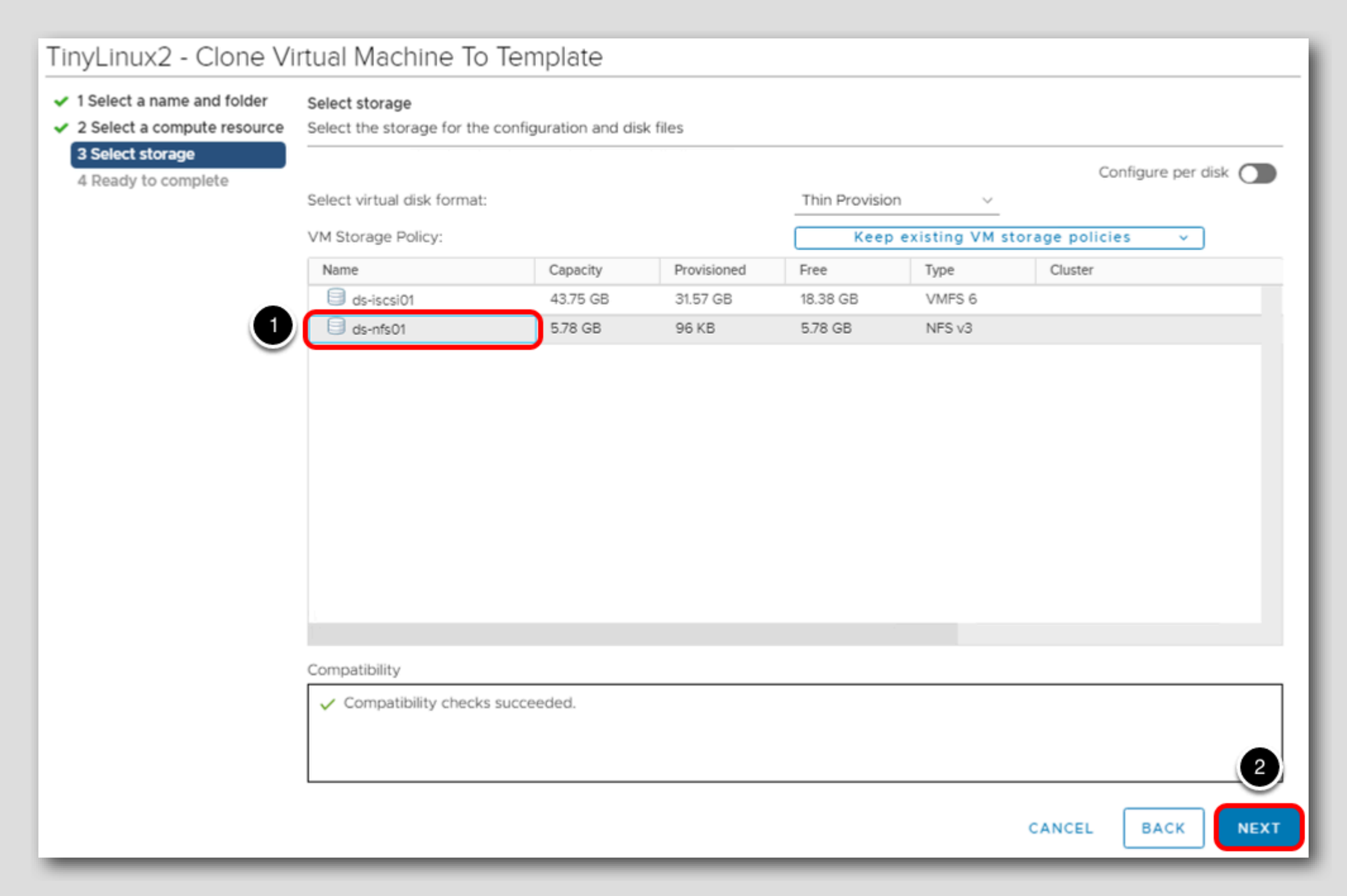
✓ Compatibility checks succeeded.

Select a compute resource:

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

Select Storage

[90]



TinyLinux2 - Clone Virtual Machine To Template

Select storage
Select the storage for the configuration and disk files

Configure per disk: off

Select virtual disk format: Thin Provision

VM Storage Policy: Keep existing VM storage policies

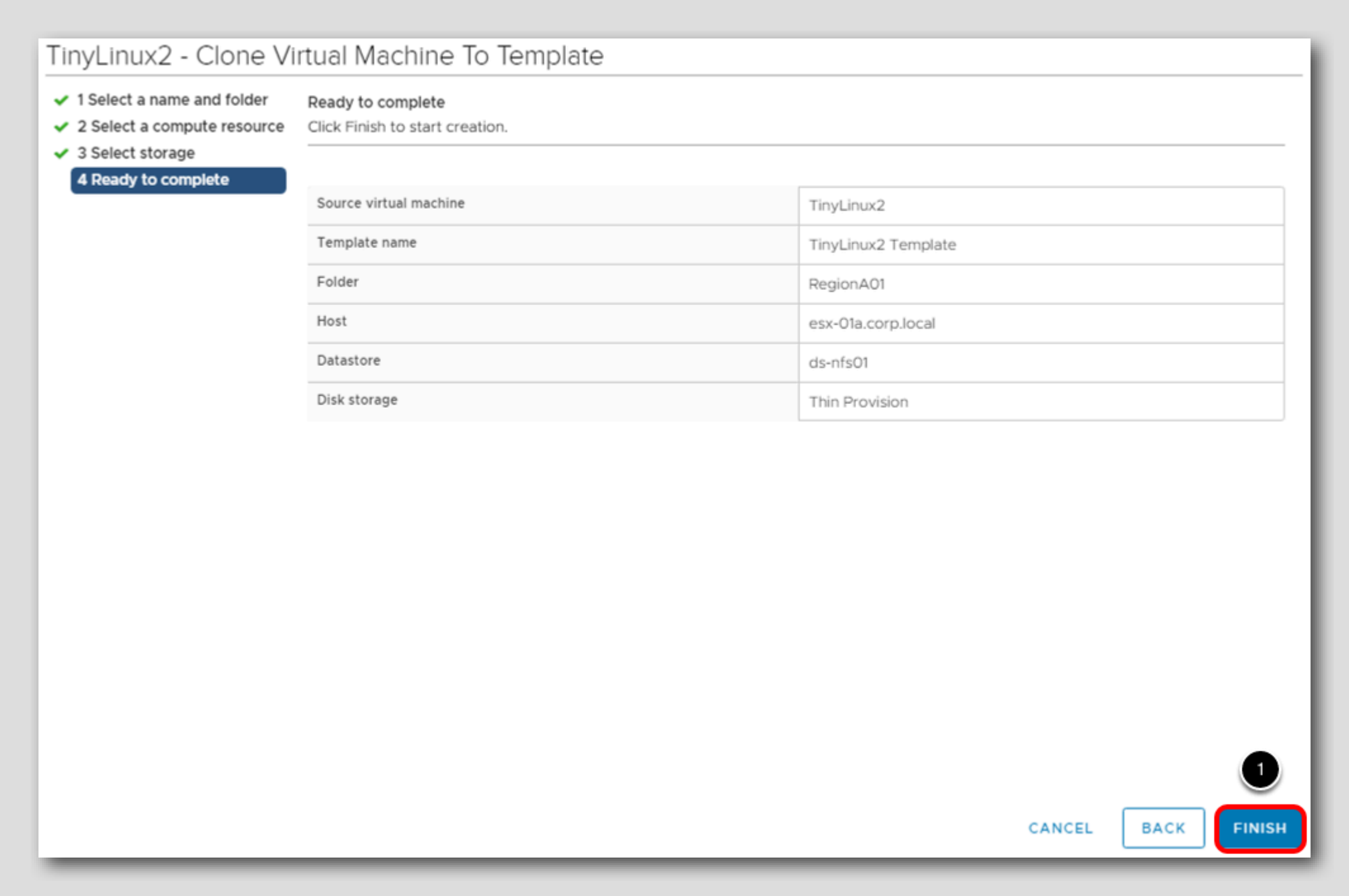
Name	Capacity	Provisioned	Free	Type	Cluster
ds-iscsi01	43.75 GB	31.57 GB	18.38 GB	VMFS 6	
ds-nfs01	5.78 GB	96 KB	5.78 GB	NFS v3	

Compatibility
✓ Compatibility checks succeeded.

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

Review the VM Template Settings

[91]



TinyLinux2 - Clone Virtual Machine To Template

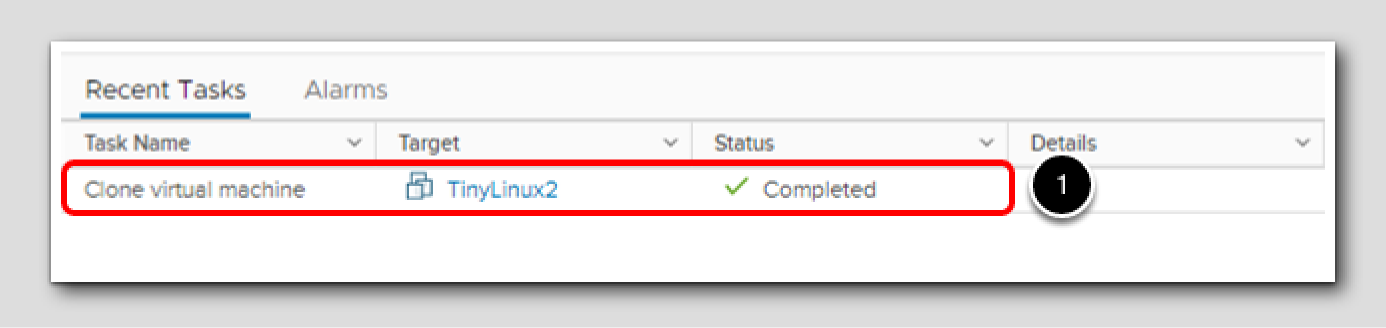
Ready to complete

Click Finish to start creation.

Source virtual machine	TinyLinux2
Template name	TinyLinux2 Template
Folder	RegionA01
Host	esx-01a.corp.local
Datastore	ds-nfs01
Disk storage	Thin Provision

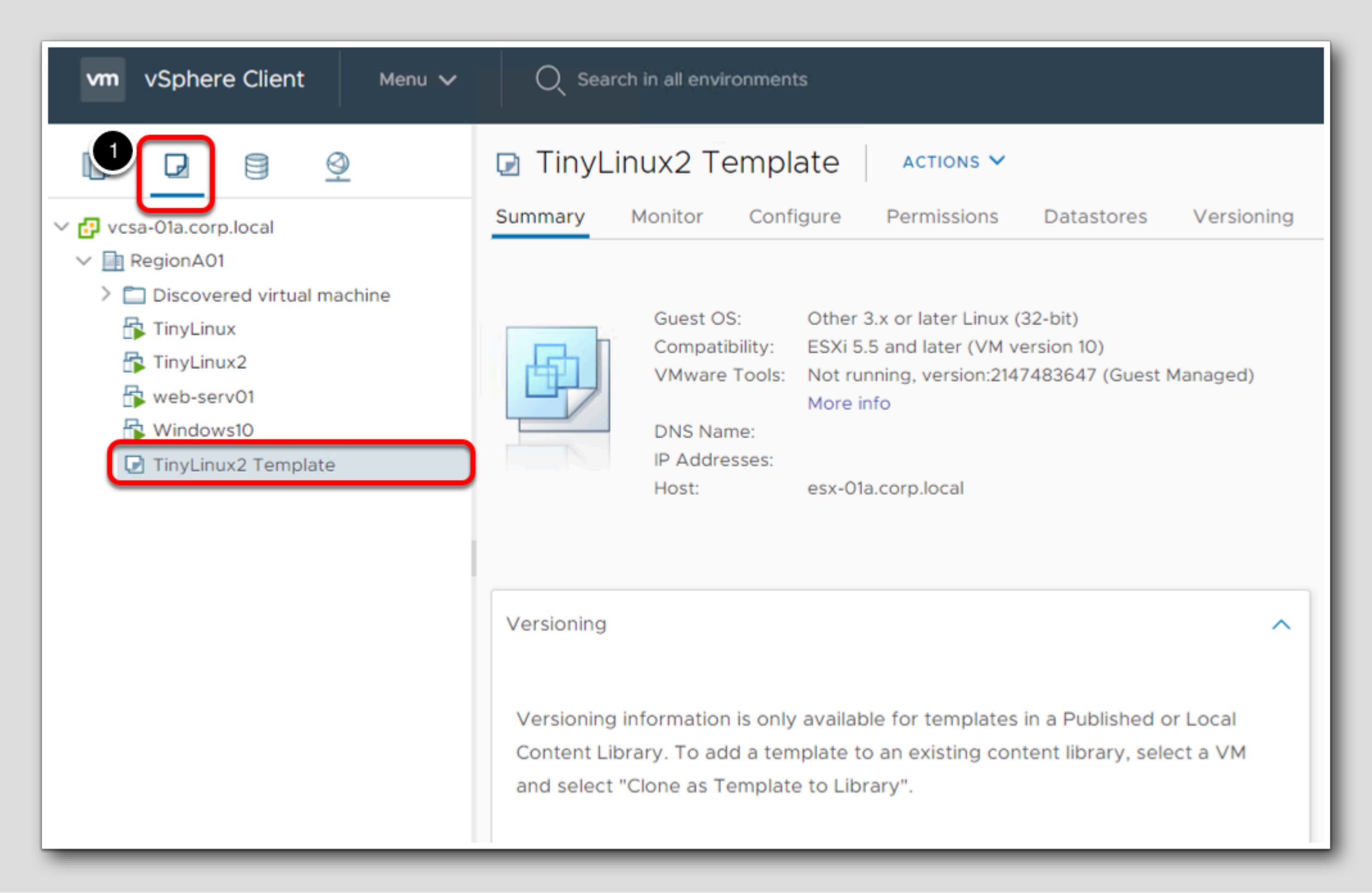
1. Review the VM Template settings and press the Finish button.

Monitor task progress



Task Name	Target	Status	Details
Clone virtual machine	TinyLinux2	✓ Completed	

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



TinyLinux2 Template

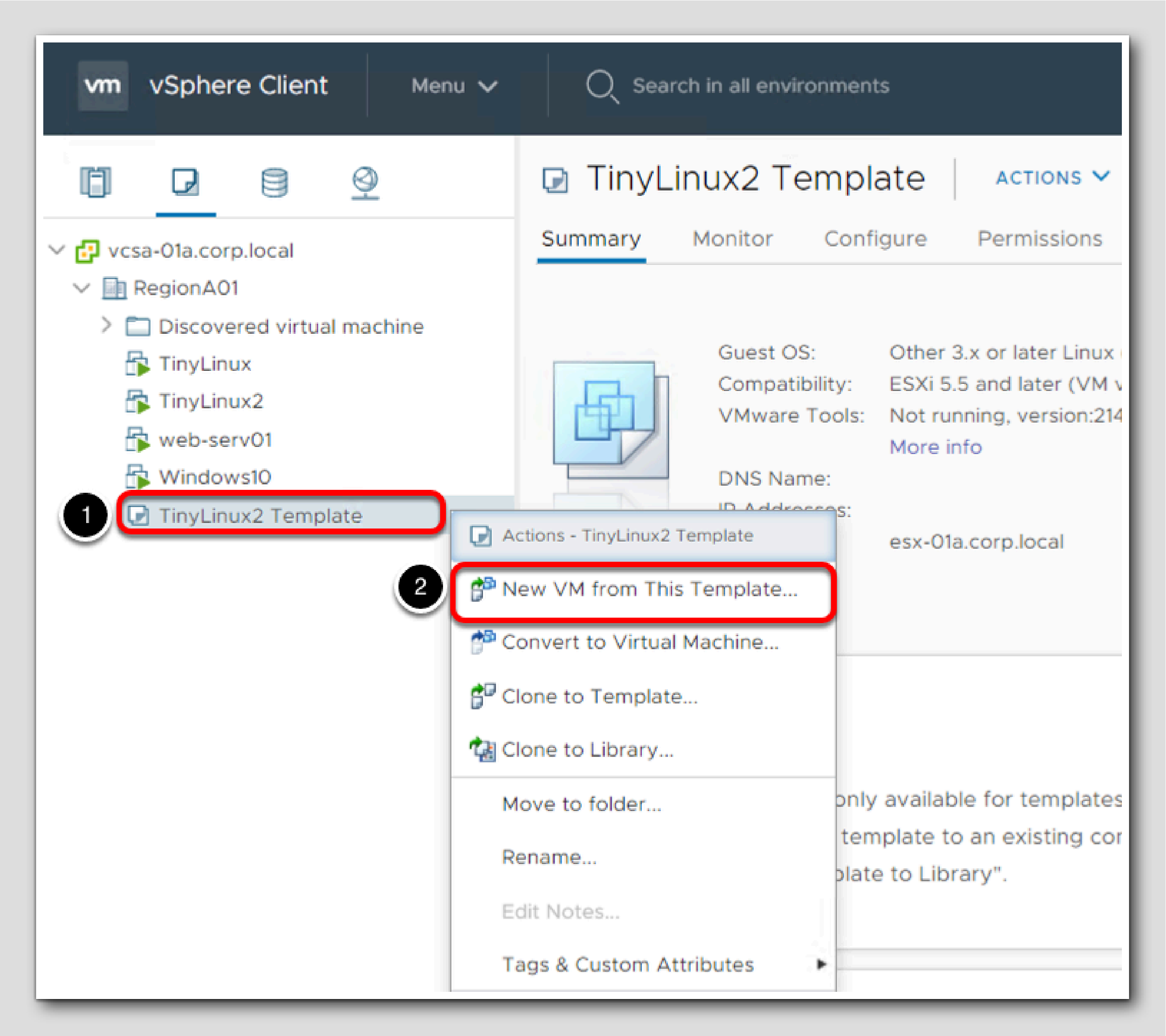
Guest OS: Other 3.x or later Linux (32-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Not running, version:2147483647 (Guest Managed)
More info
DNS Name:
IP Addresses:
Host: esx-01a.corp.local

Versioning information is only available for templates in a Published or Local Content Library. To add a template to an existing content library, select a VM and select "Clone as Template to Library".

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

Launch the Deploy From Template wizard

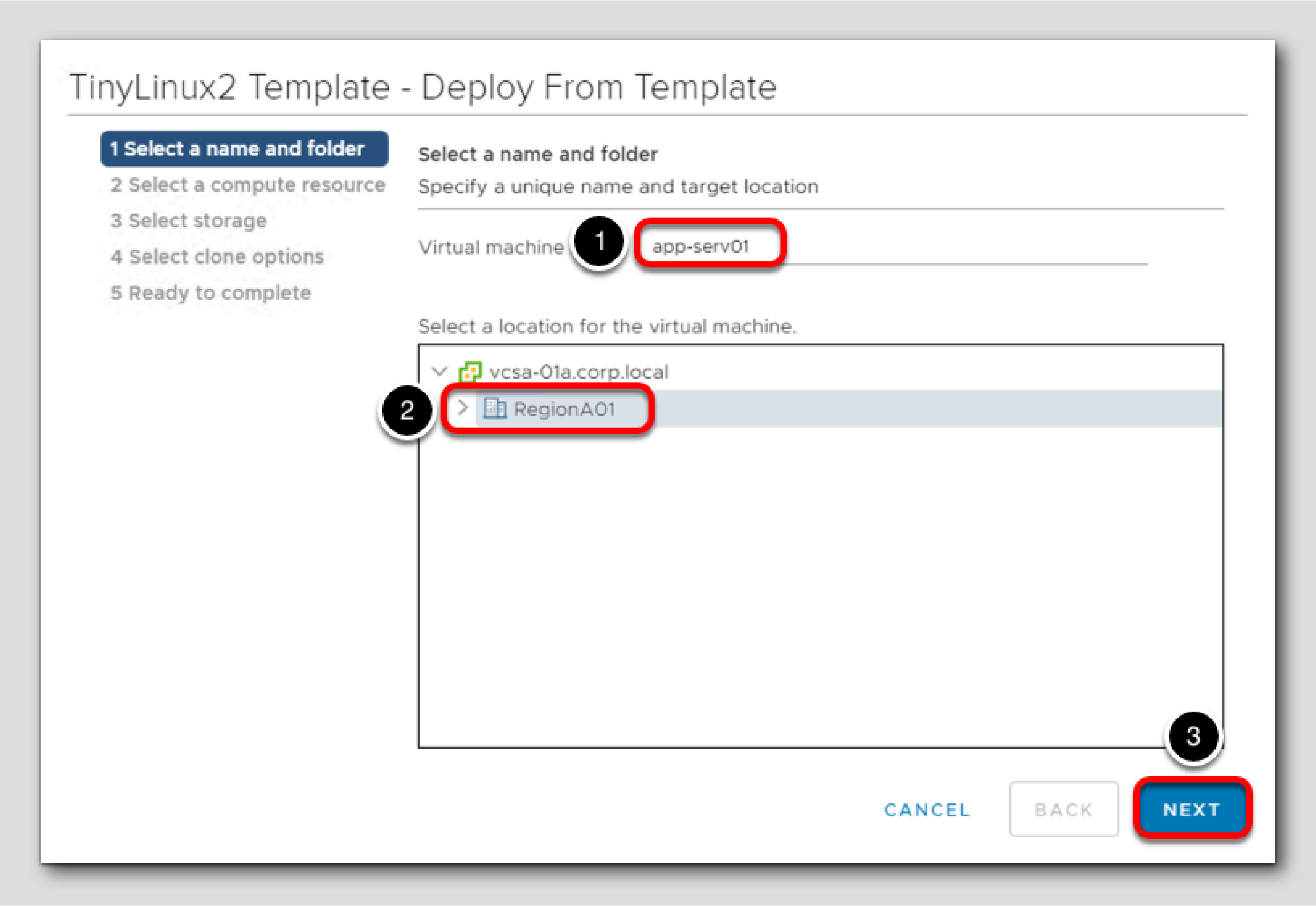
[93]



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

Select a name and folder

[94]



TinyLinux2 Template - Deploy From Template

Select a name and folder

Specify a unique name and target location

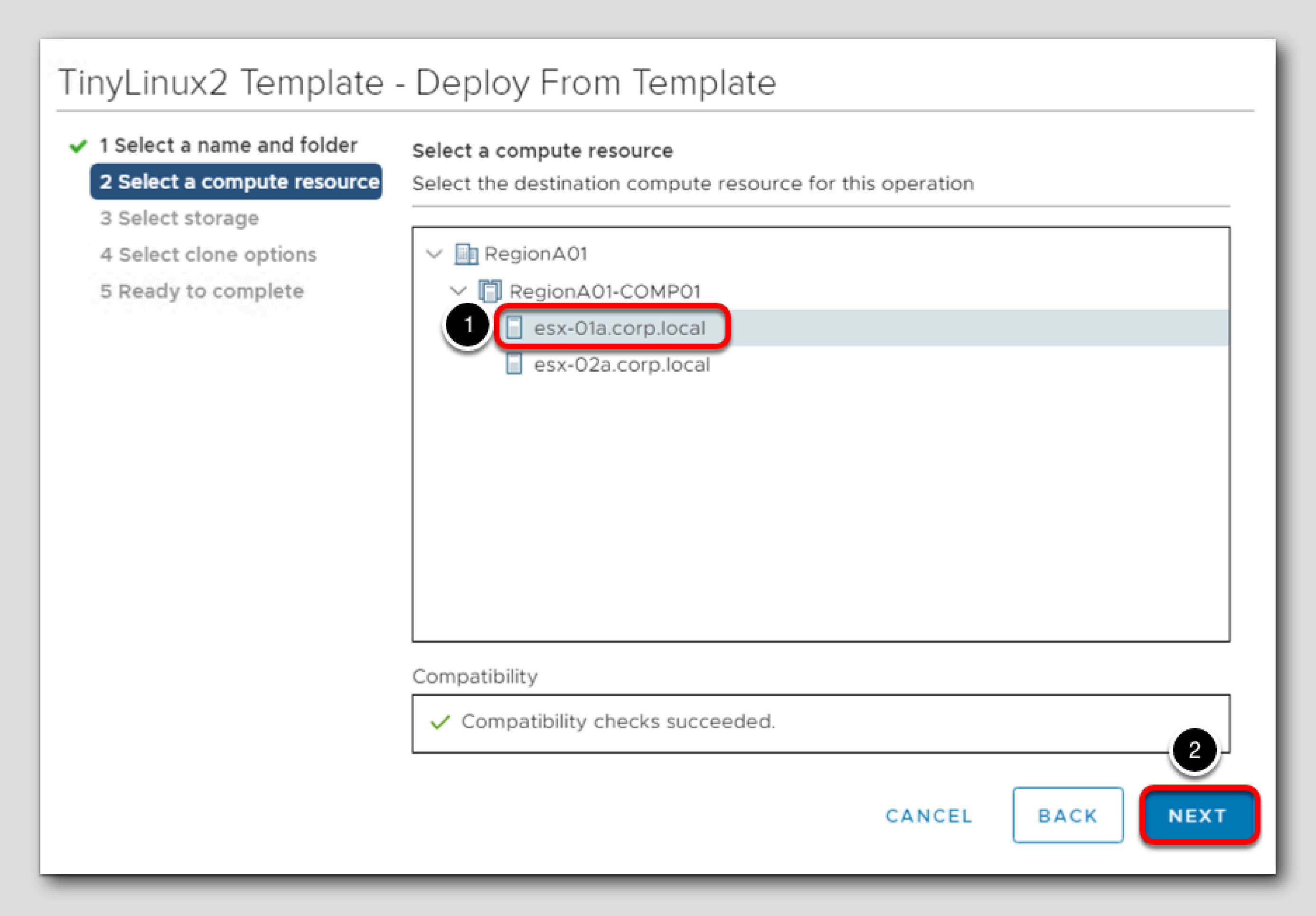
Virtual machine: app-serv01

Select a location for the virtual machine.

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

Select compute resource

[95]



TinyLinux2 Template - Deploy From Template

Select a compute resource

Select the destination compute resource for this operation

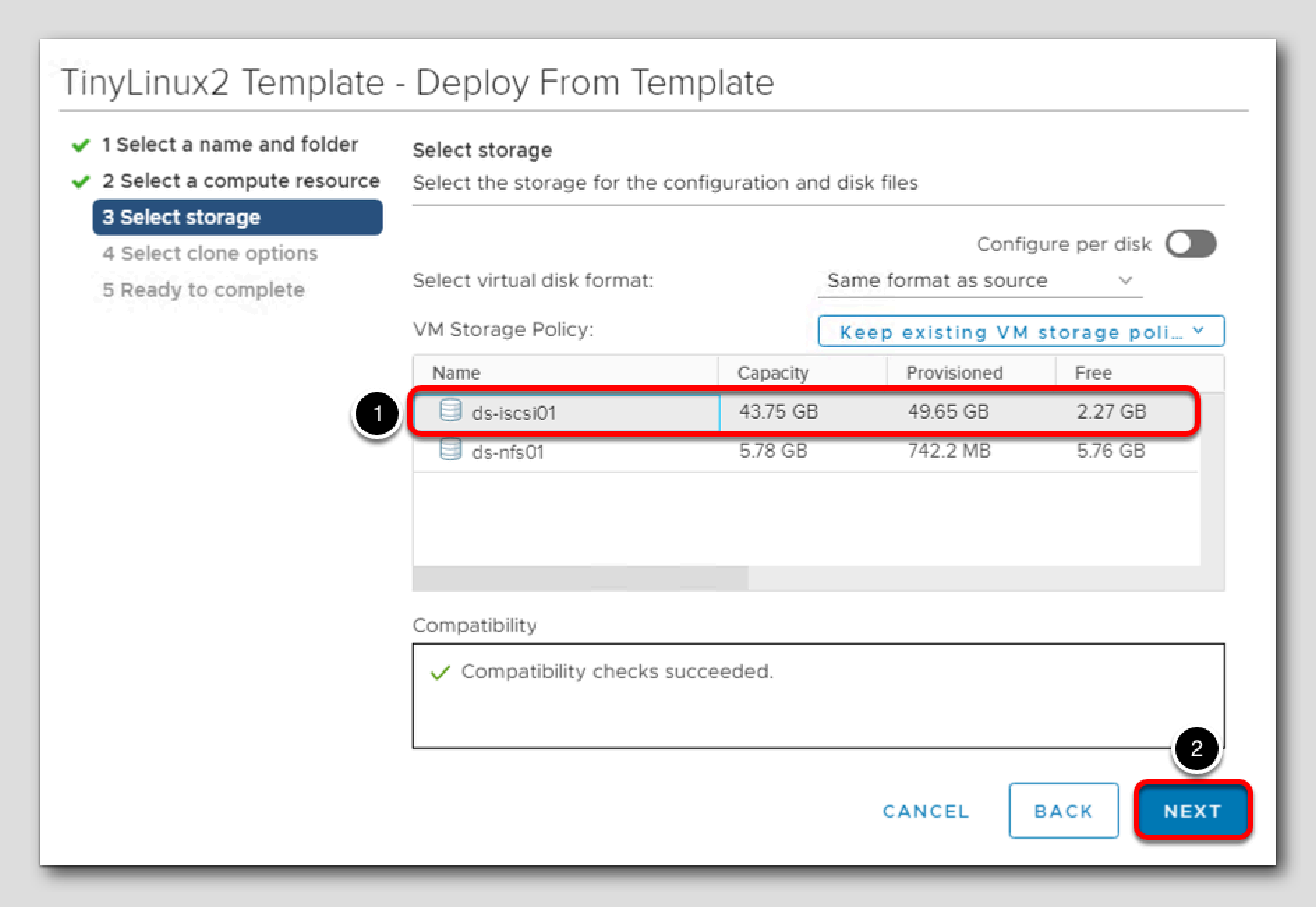
Compatibility

✓ Compatibility checks succeeded.

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

Select storage

[96]



TinyLinux2 Template - Deploy From Template

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

Select storage

Select the storage for the configuration and disk files

Configure per disk ○

Select virtual disk format: Same format as source

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

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

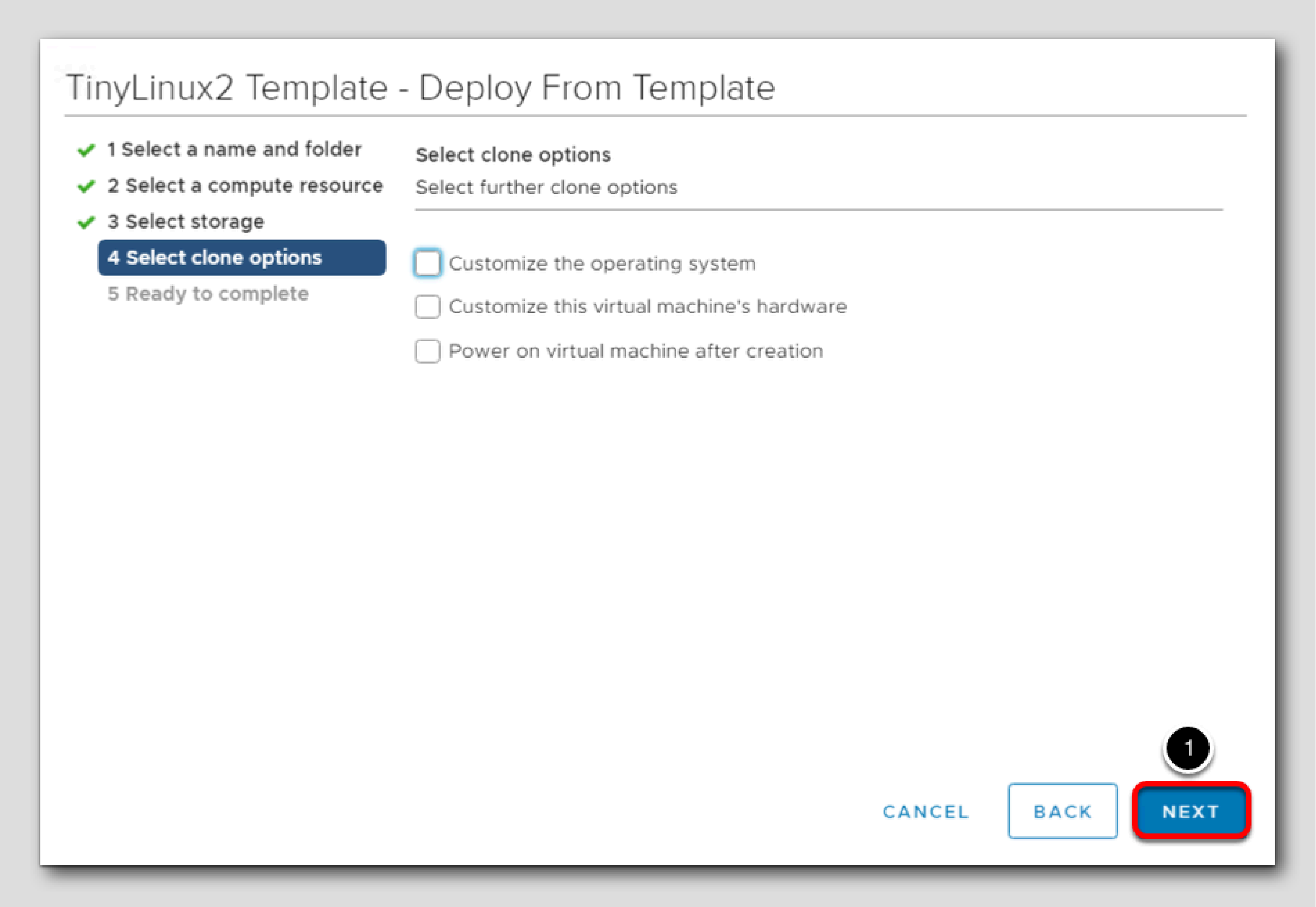
Compatibility

✓ Compatibility checks succeeded.

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

Select clone options

[97]



TinyLinux2 Template - Deploy From Template

Select clone options

Select further clone options

□ Customize the operating system

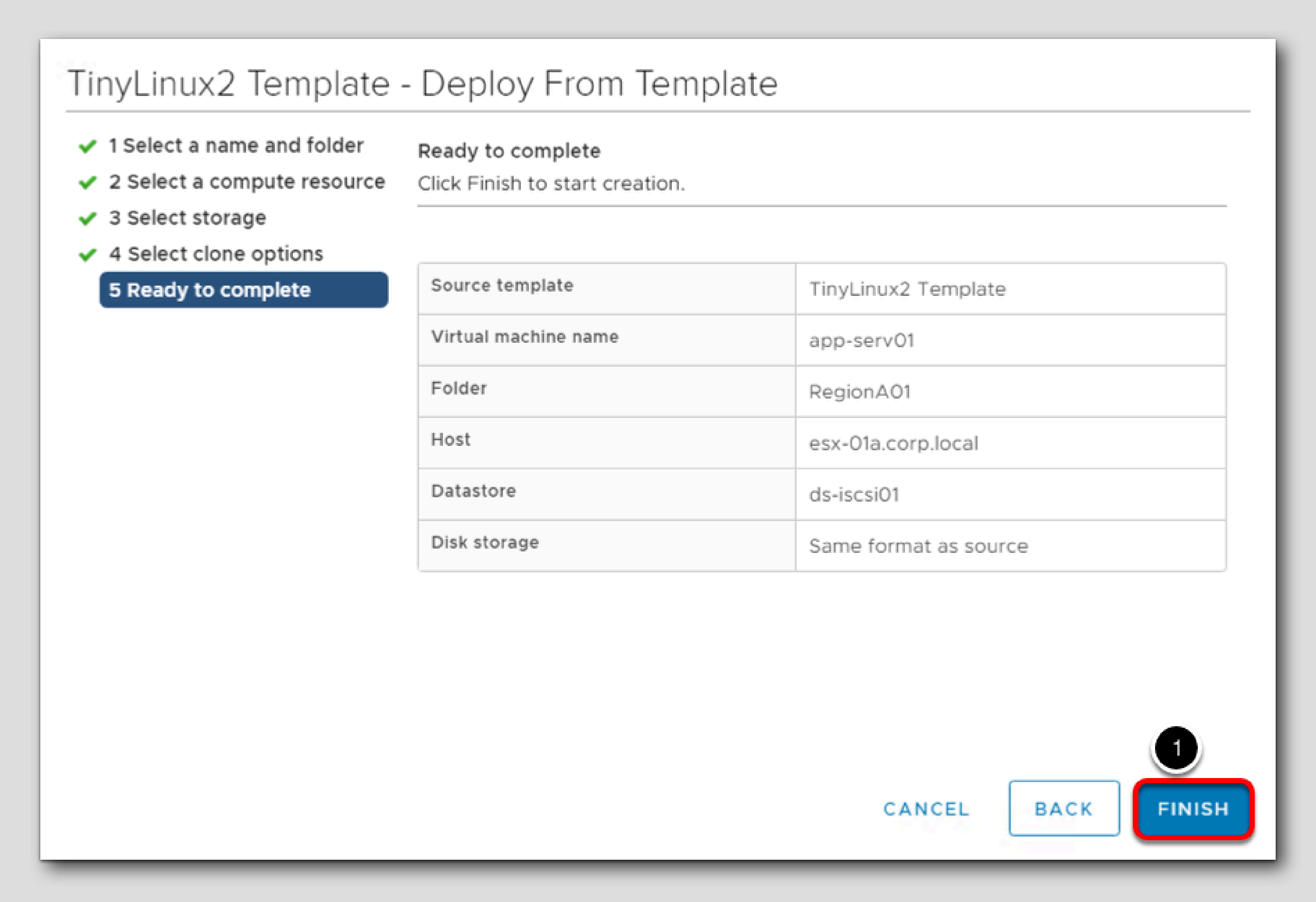
□ Customize this virtual machine's hardware

□ 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

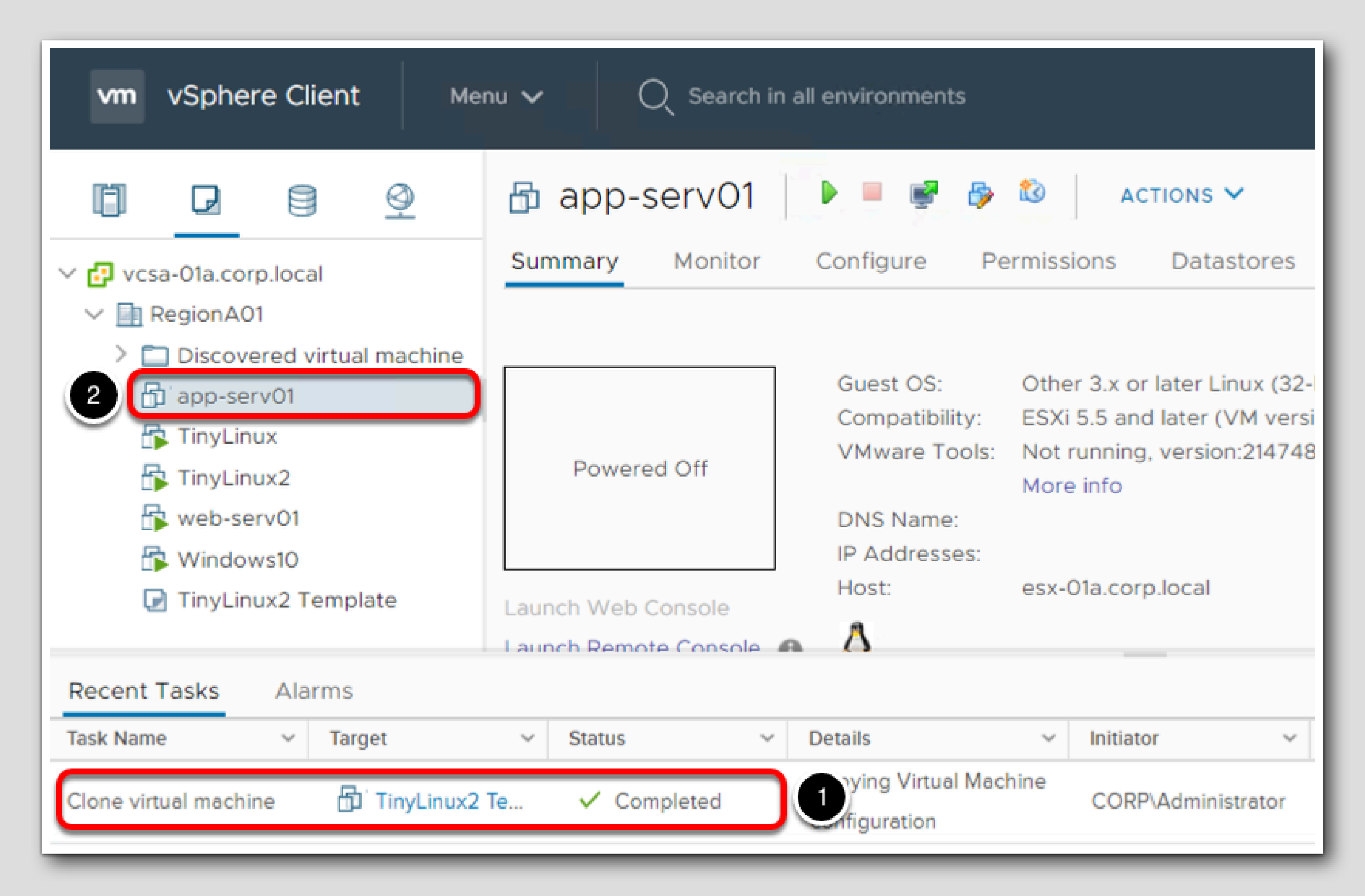
Ready to complete

Click Finish to start creation.

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

1. Review the deployment options and then click Finish.

Monitor task progress



Guest OS: Other 3.x or later Linux (32-

Compatibility: ESXi 5.5 and later (VM versi

VMware Tools: Not running, version:214748

More info

DNS Name:

IP Addresses:

Host: esx-01a.corp.local

Task Name	Target	Status	Details	Initiator
Clone virtual machine	TinyLinux2 Te...	✓ Completed	ying Virtual Machine figuration	CORP\Administrator

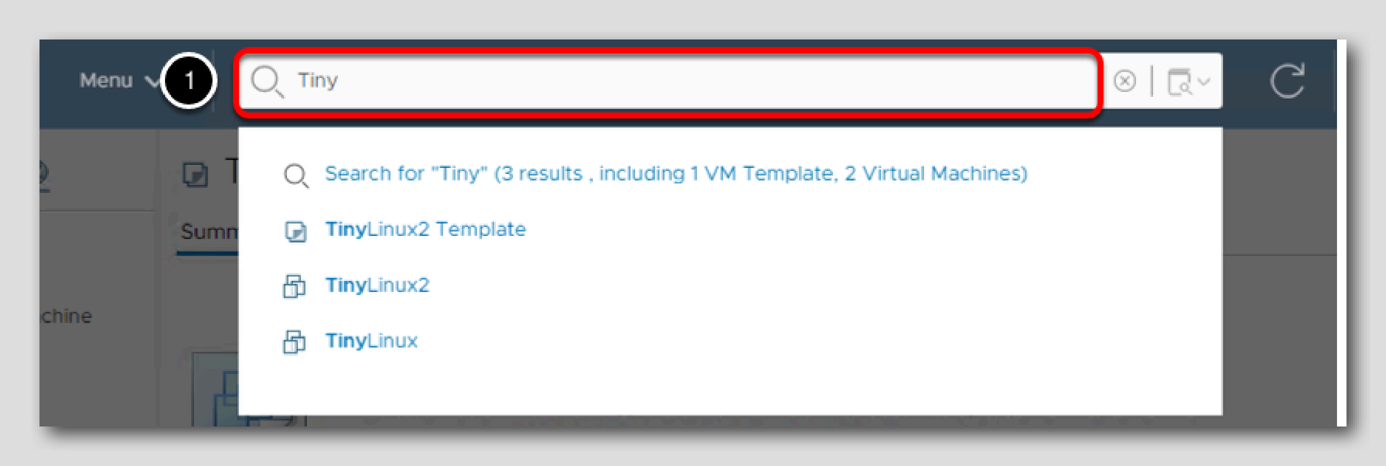
1. You can view the Recent Tasks window to monitor the virtual machine being created from the template.
2. When the task is complete, you will see the **app-serv01** virtual machine in the inventory pane.

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

[101]



Search for "Tiny" (3 results , including 1 VM Template, 2 Virtual Machines)
TinyLinux2 Template
TinyLinux2
TinyLinux

At the top of the vSphere Client is a search bar that can be used to find objects quickly. This can 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.

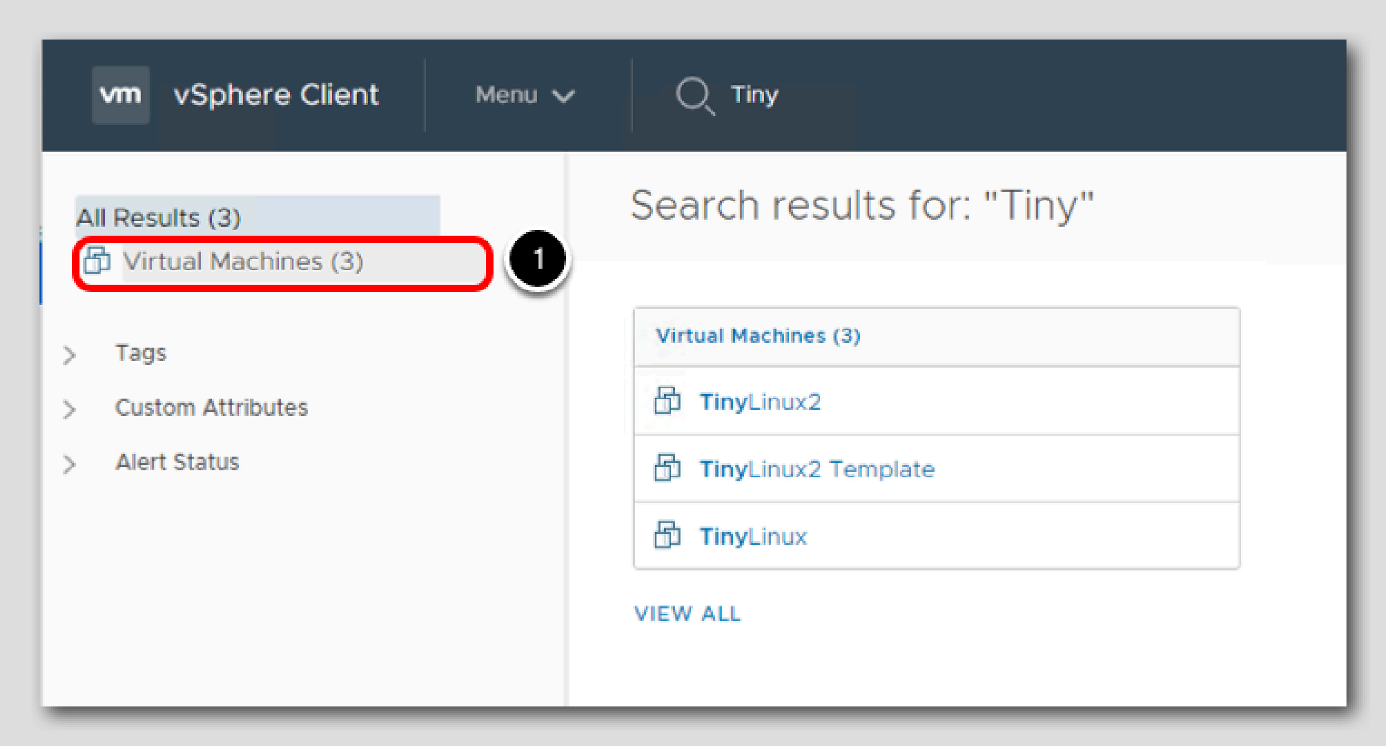
1. Click on the search bar at the top of the screen and type Tiny.

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

2. Press the Enter key.

Search Results

[102]



Search results for: "Tiny"

Virtual Machines (3)

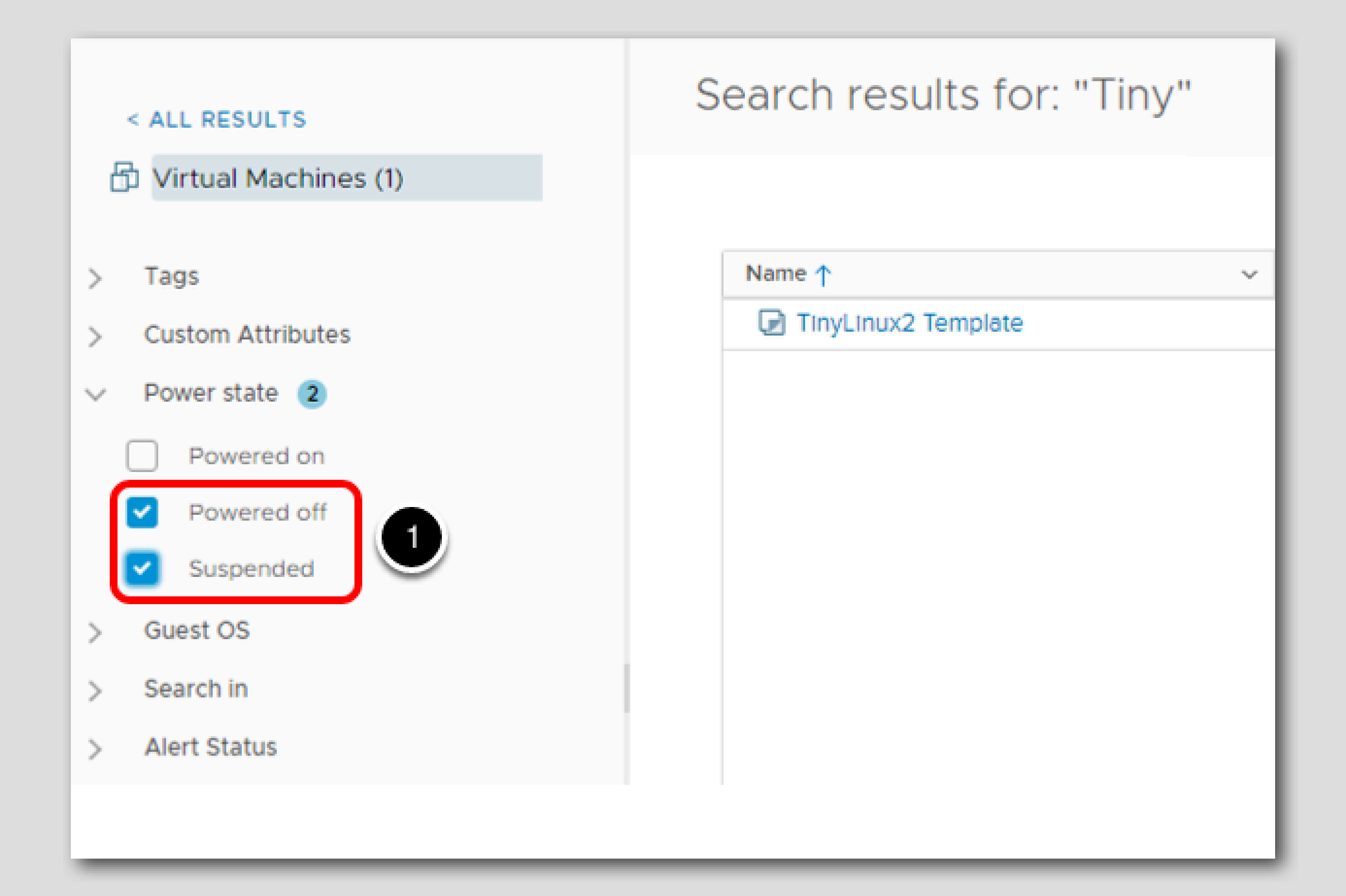
- TinyLinux2
- TinyLinux2 Template
- TinyLinux

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

[103]



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

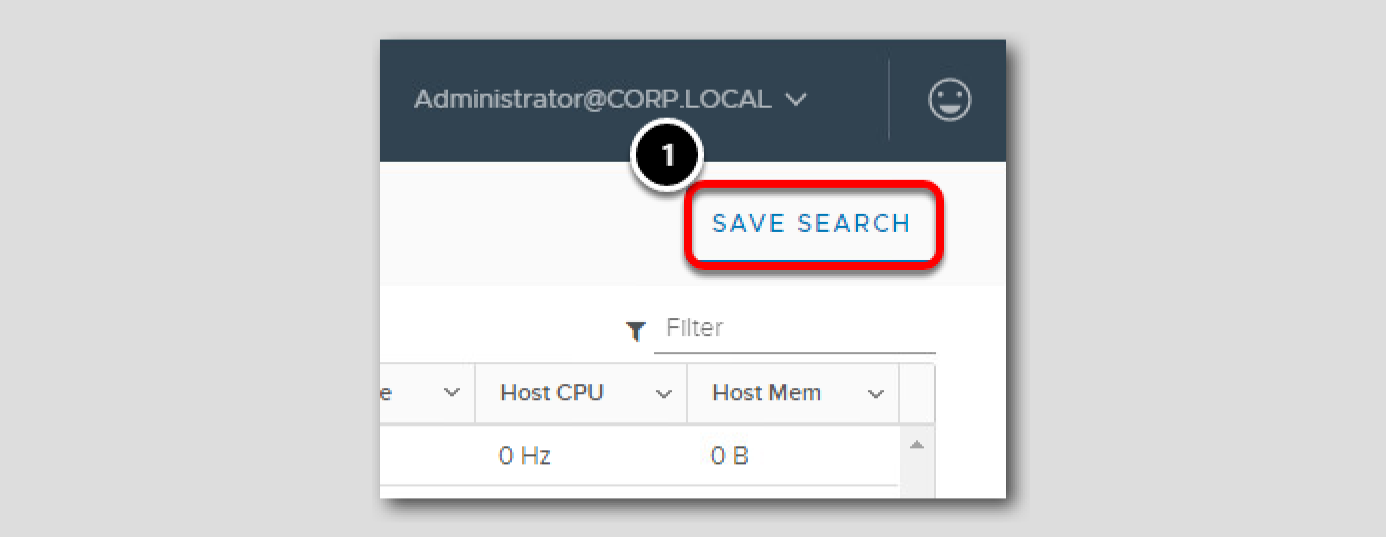
- The Power state of the virtual machine
- What operating system is running in the virtual machine
- What Host, Cluster or Datacenter to search in

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

The search field is updated with the results.

Save the Search

[104]

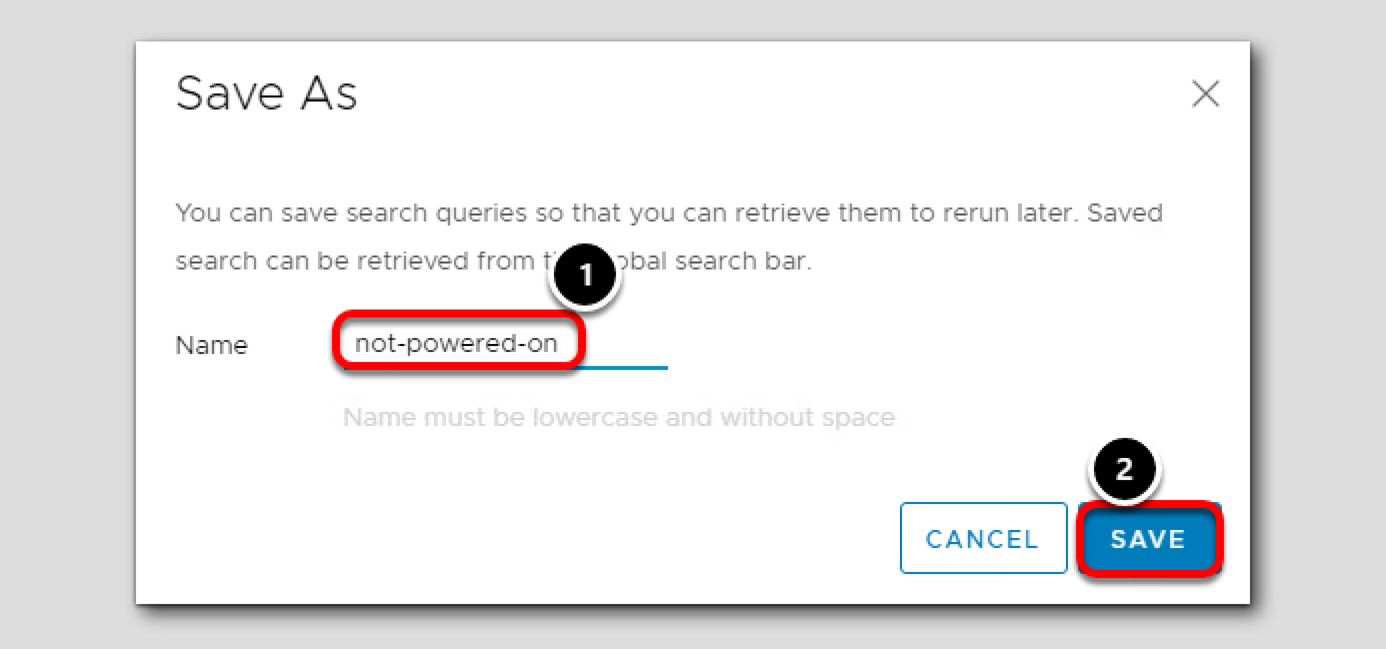


If this is a frequently used search, it can be saved for use in the future.

1. Click the Save Search button.

Name Search

[105]



Save As

You can save search queries so that you can retrieve them to rerun later. Saved search can be retrieved from the global search bar.

Name: not-powered-on

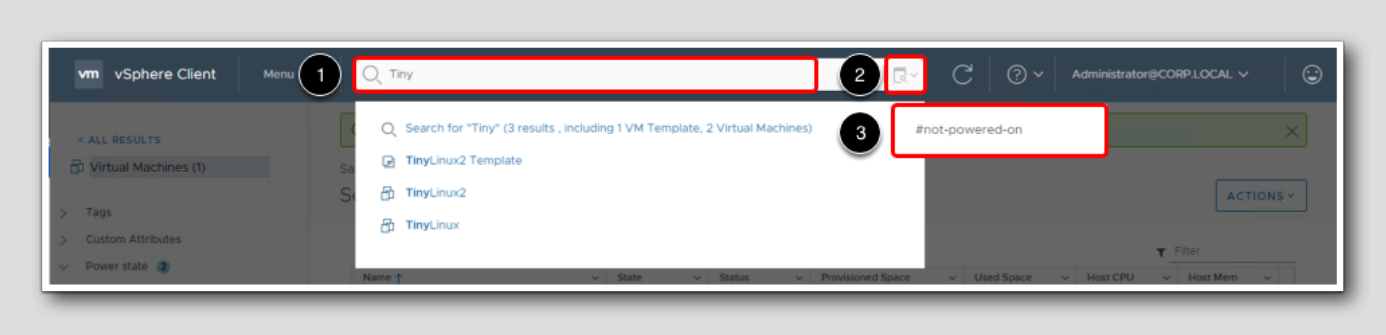
Name must be lowercase and without space

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

[106]



Tiny

Search for "Tiny" (3 results , including 1 VM Template, 2 Virtual Machines)

TinyLinux2 Template

TinyLinux2

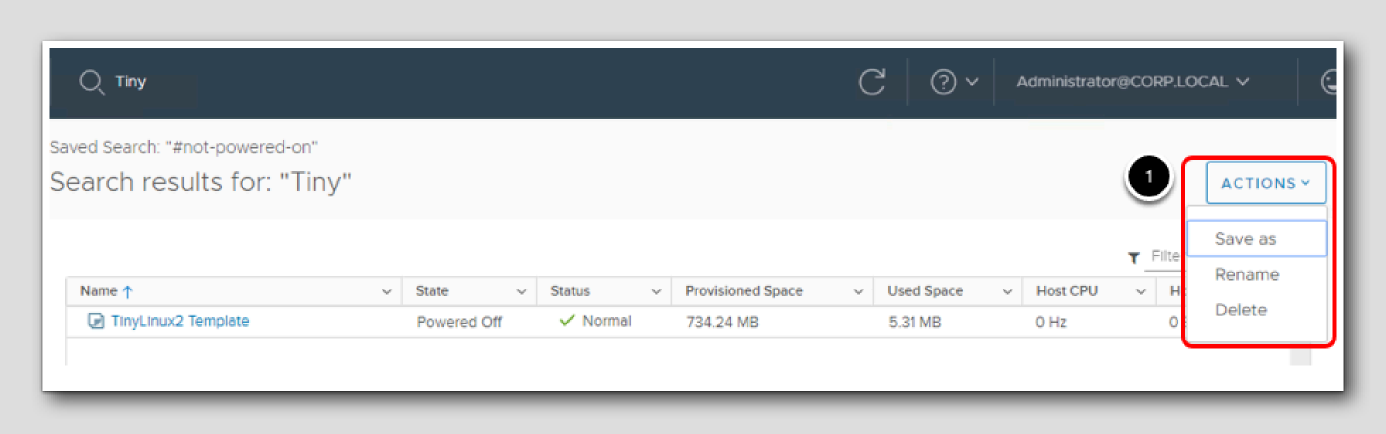
TinyLinux

#not-powered-on

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

Not-Powered-On-VMs

[107]



Saved Search: "#not-powered-on"

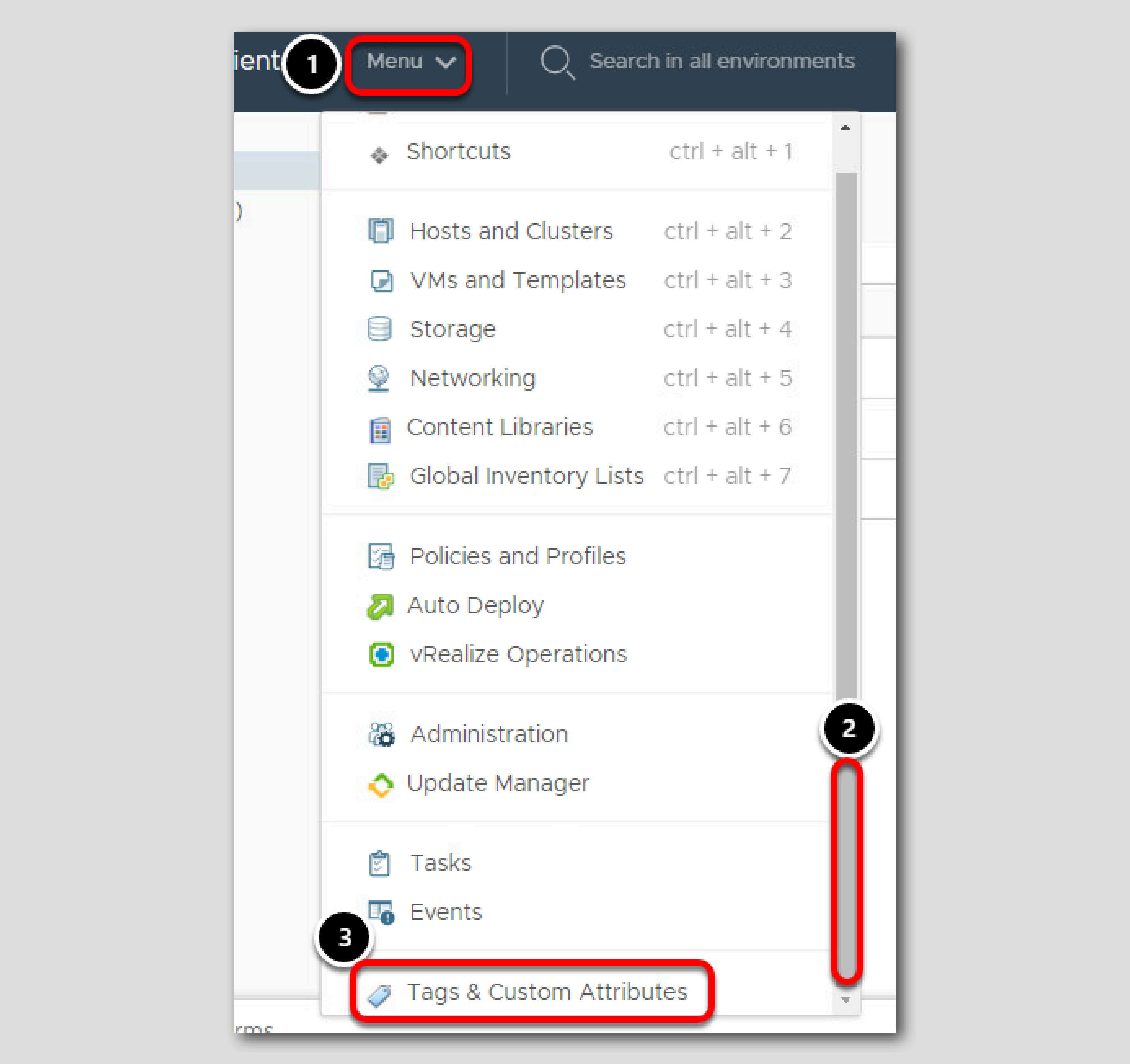
Search results for: "Tiny"

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

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

[108]

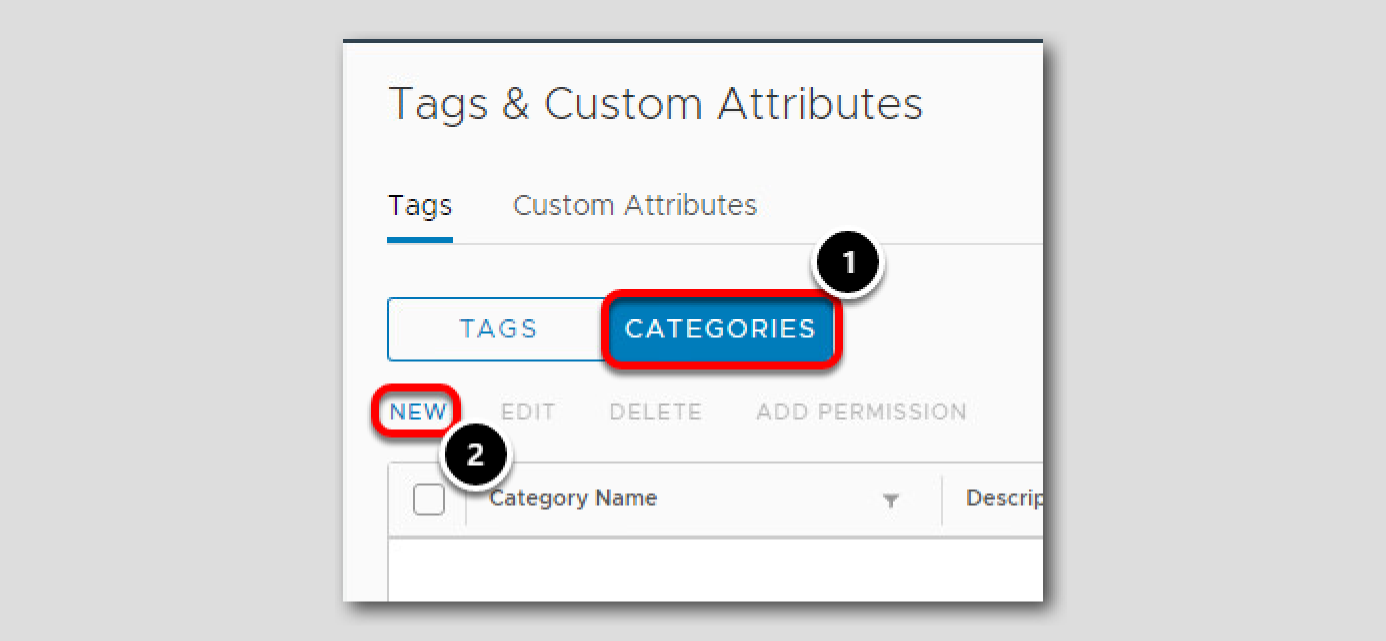

ient
1
Menu
Search in all environments
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Global Inventory Lists ctrl + alt + 7
Policies and Profiles
Auto Deploy
vRealize Operations
2
Administration
Update Manager
Tasks
Events
3
Tags & Custom Attributes

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

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

Creating Tag Categories

[109]



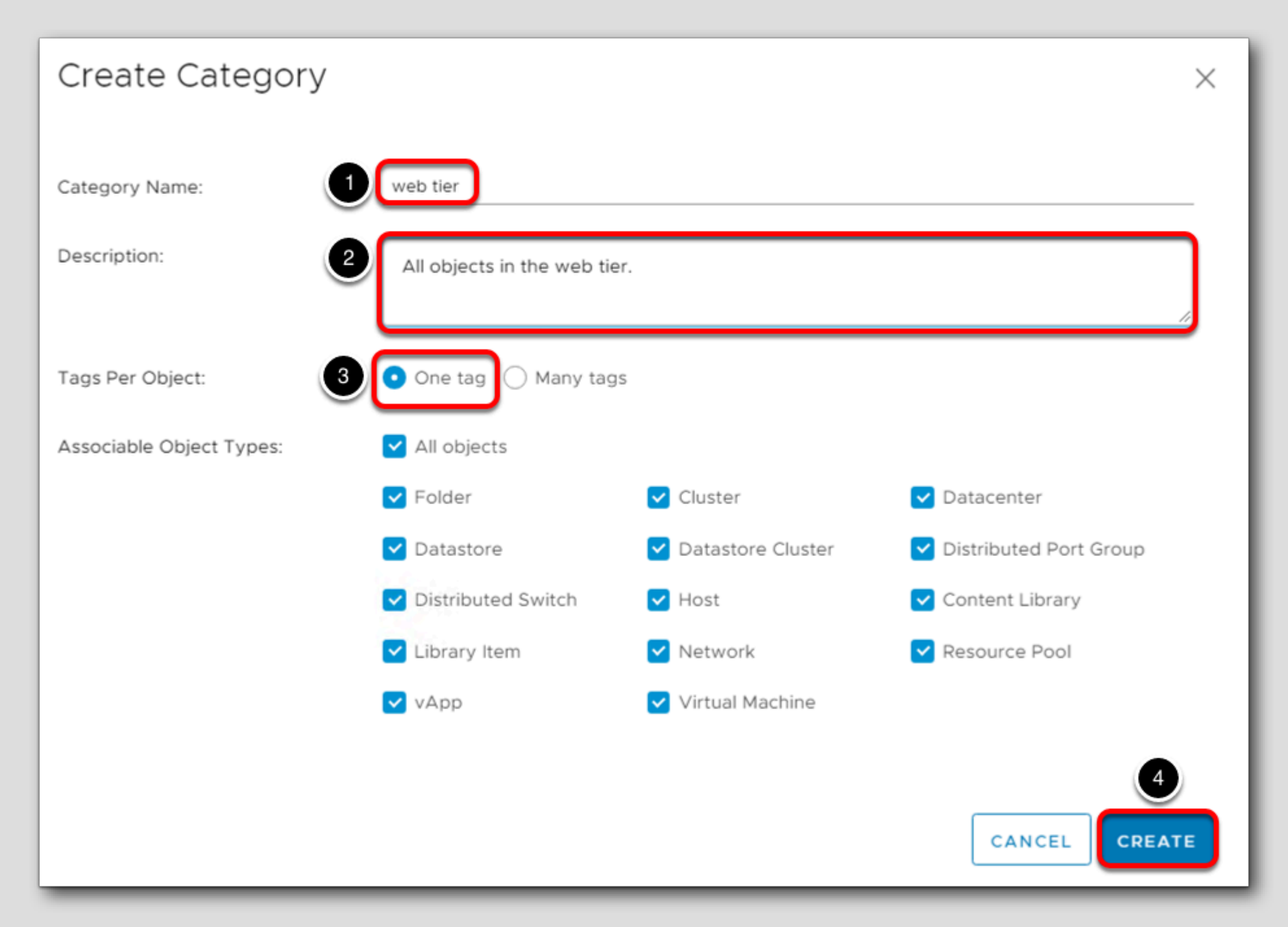
You use categories to group tags together and define how tags can be applied to objects.

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

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

New Category

[110]



Create Category

Category Name: web tier

Description: All objects in the web tier.

Tags Per Object: ● One tag ○ Many tags

Associable Object Types:

☑ All objects

☑ Folder ☑ Cluster ☑ Datacenter

☑ Datastore ☑ Datastore Cluster ☑ Distributed Port Group

☑ Distributed Switch ☑ Host ☑ Content Library

☑ Library Item ☑ Network ☑ Resource Pool

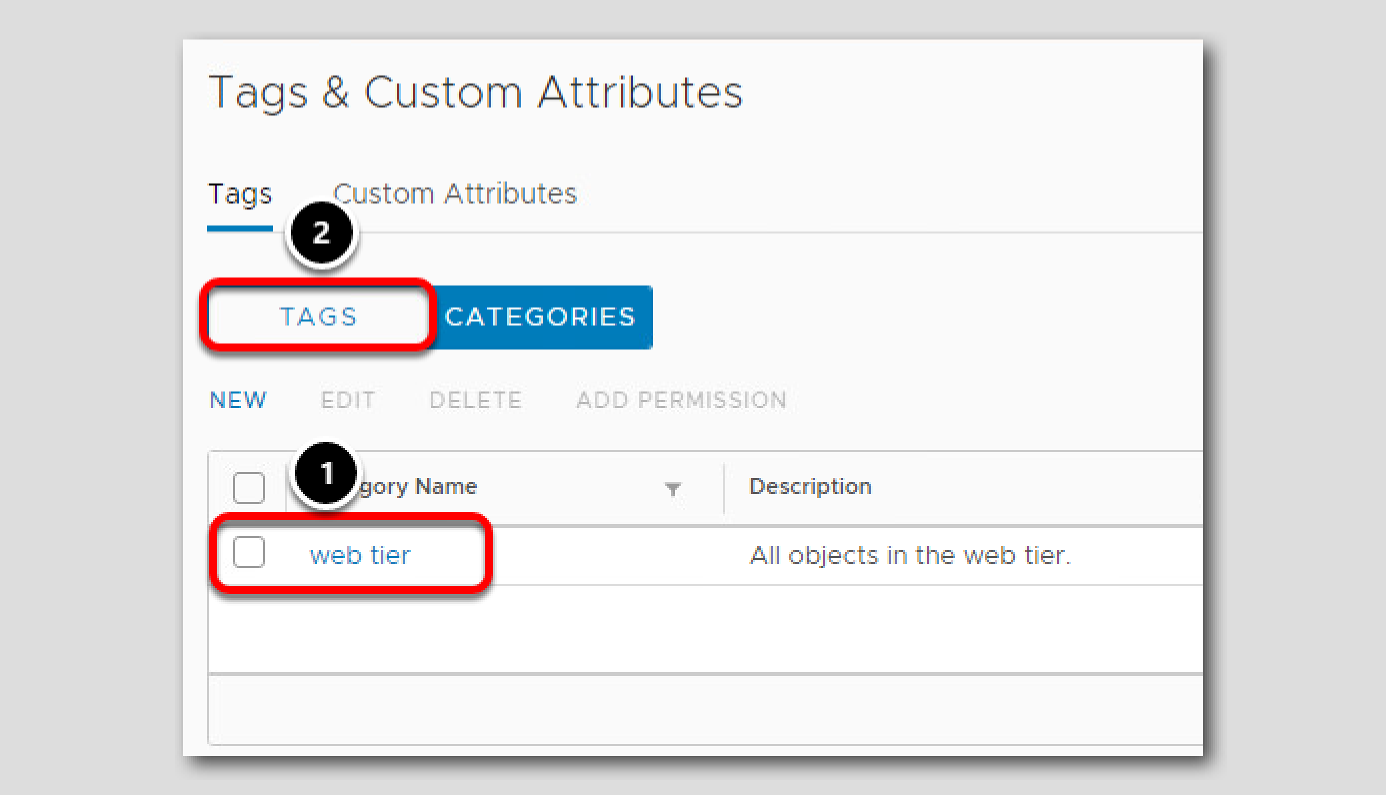
☑ vApp ☑ Virtual Machine

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

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

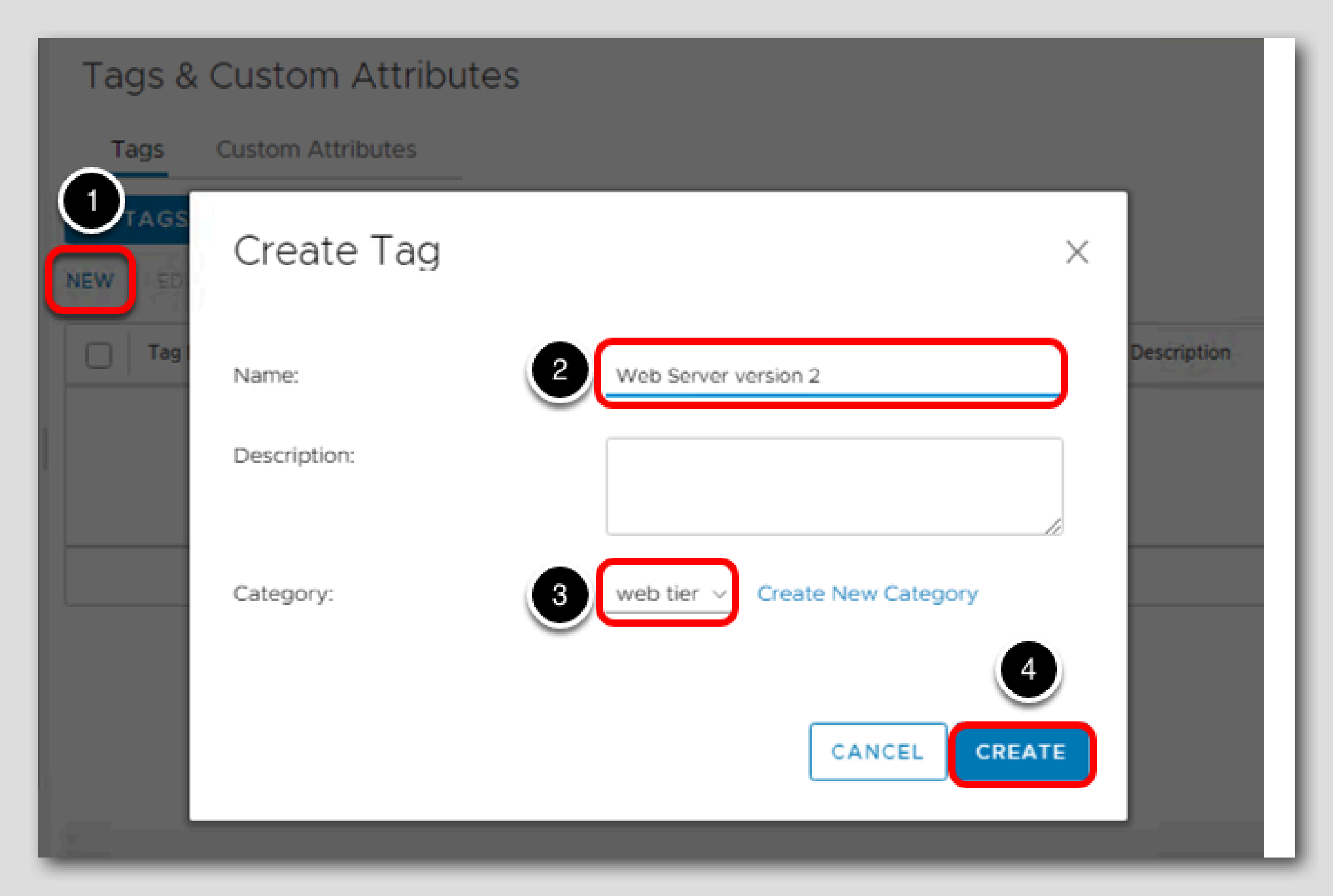
Create a New Tag

[111]



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

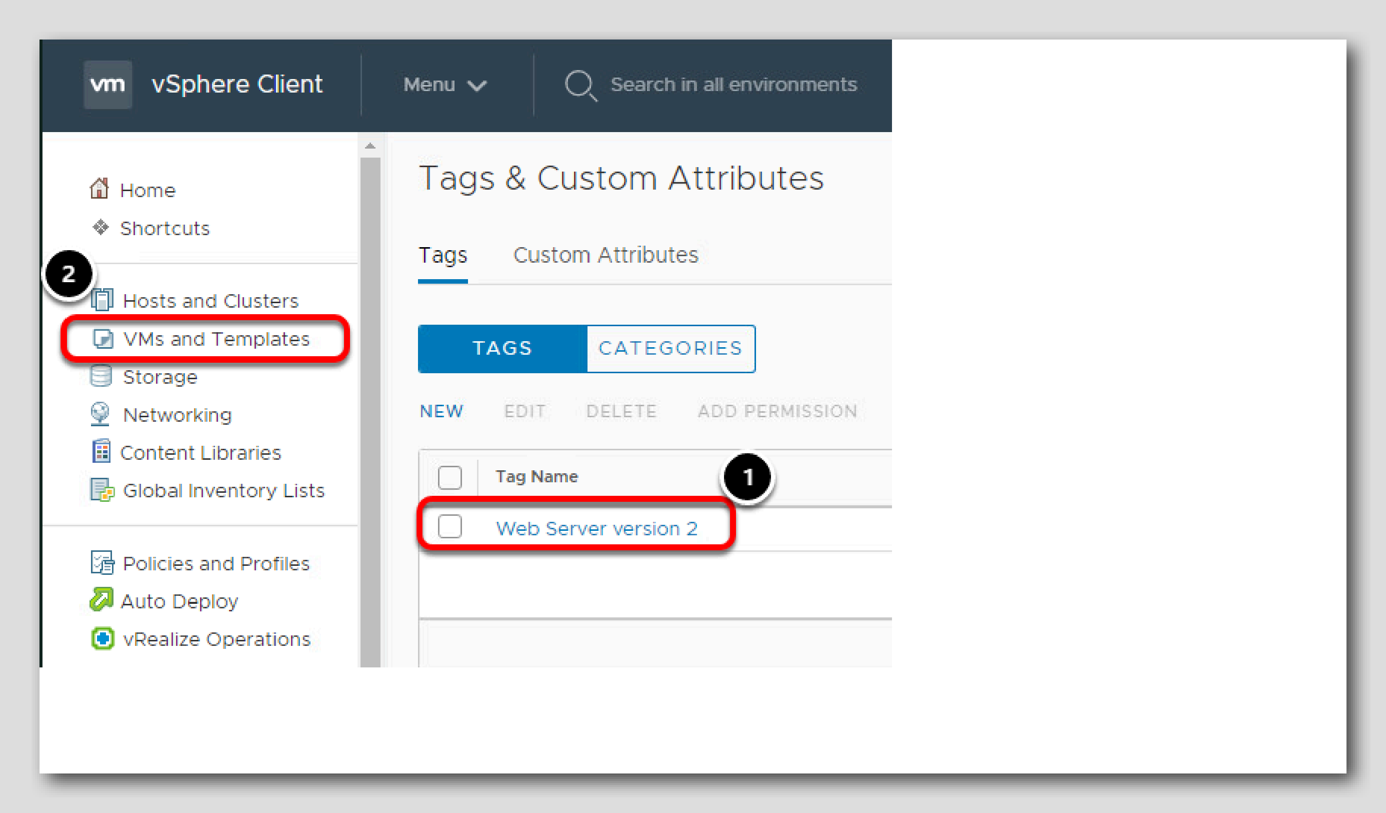
Add Tag



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

New Tag

[113]



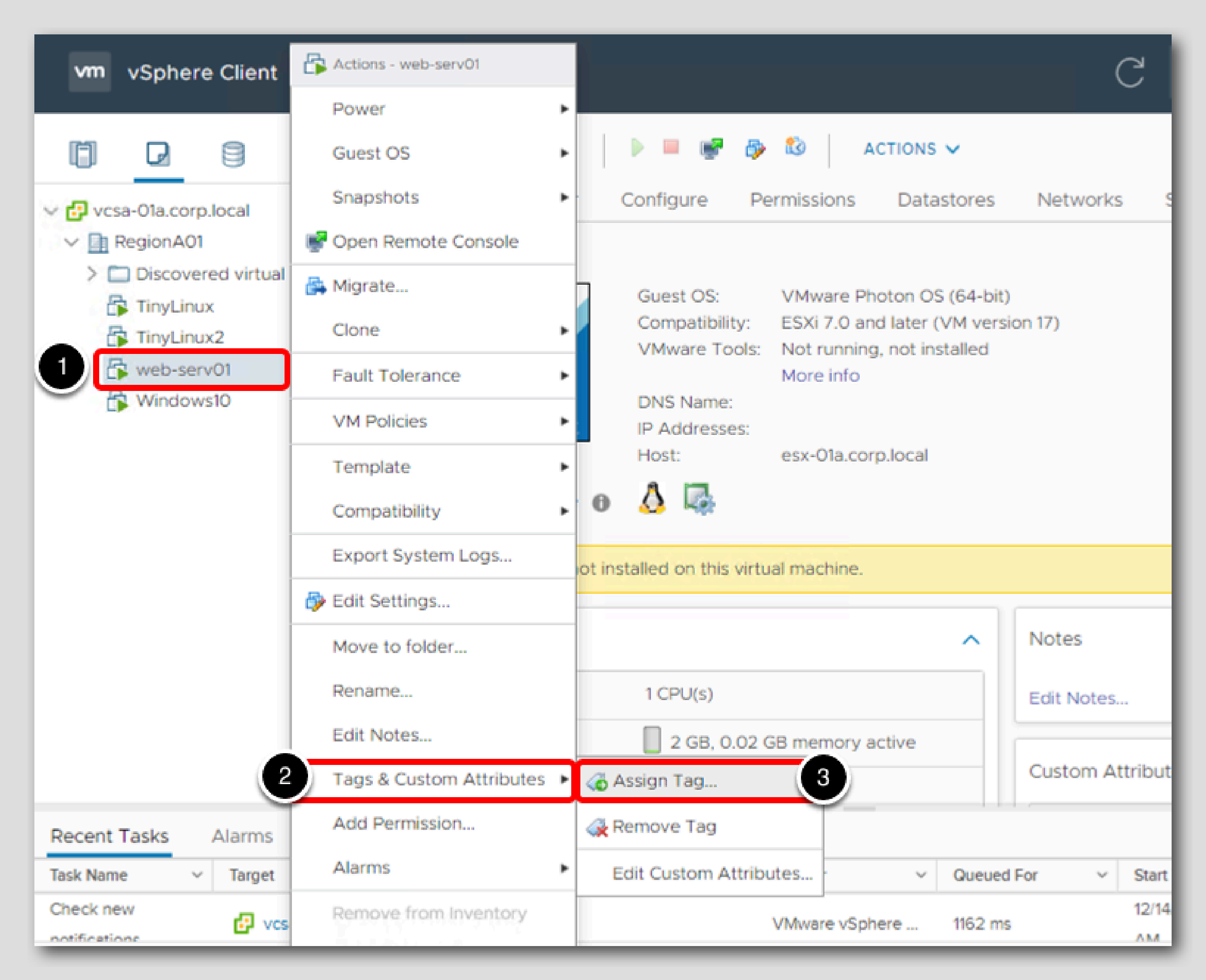
1. The newly created tag has now been added.

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

[114]



Guest OS: VMware Photon OS (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Host: esx-01a.corp.local

ot installed on this virtual machine.

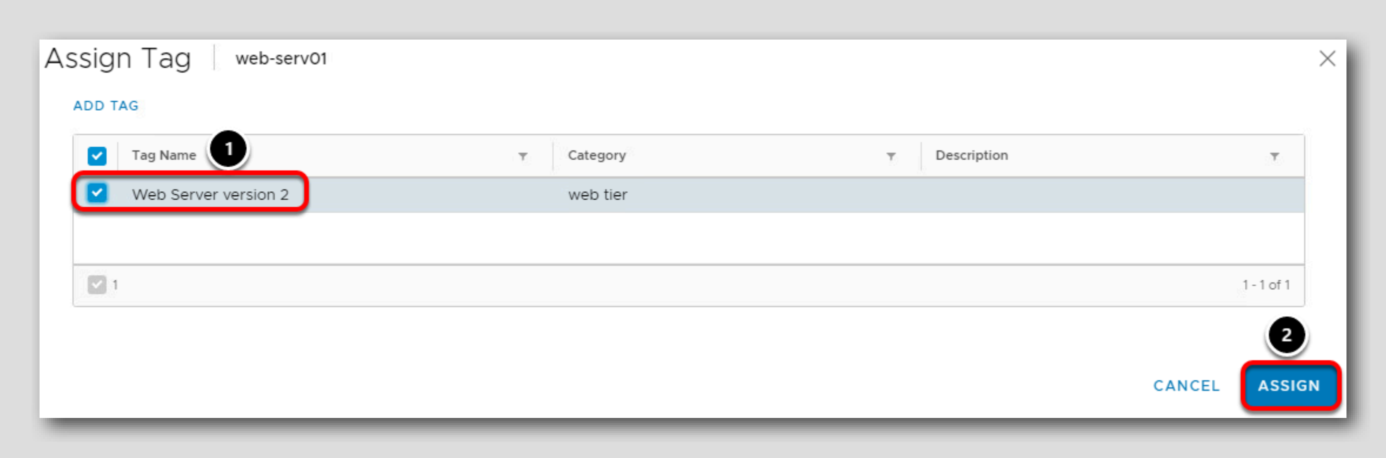
1 CPU(s)
2 GB, 0.02 GB memory active

Check new notifications | vcs | VMware vSphere ... | 1162 ms | 12/14 AM

1. Right-click the virtual machine **web-serv01**.
2. Find **Tags & Custom Attributes**
3. Click **Assign Tag...**

Assign Tag

[115]



Assign Tag | web-serv01

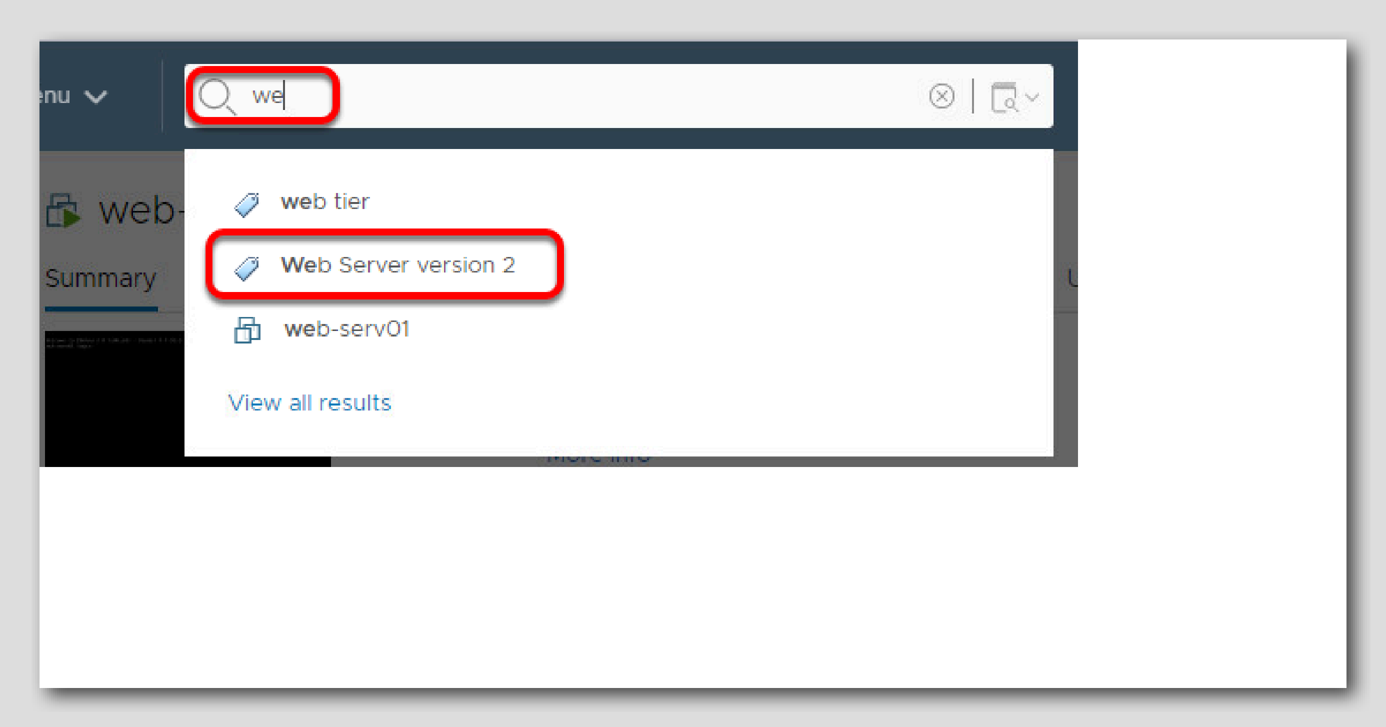
☑	Tag Name	Category	Description
☑	Web Server version 2	web tier	

☑ 1 1 - 1 of 1

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

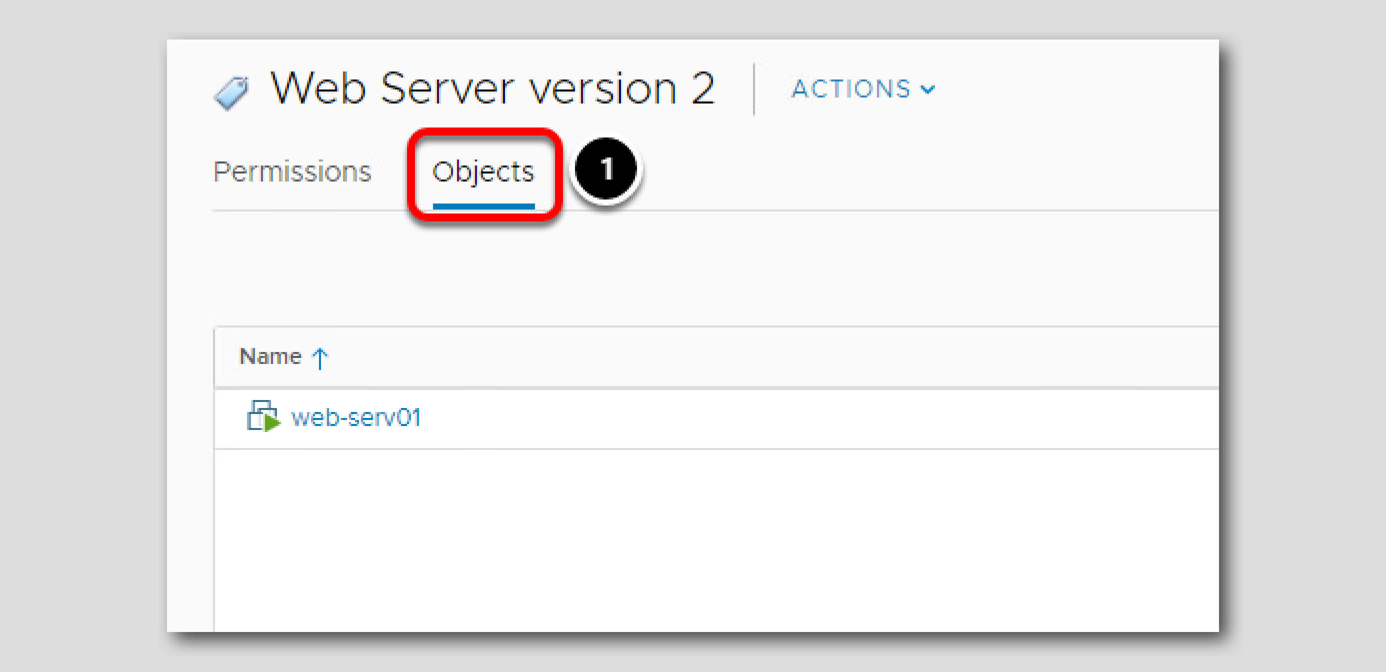
Search Using Tags

[116]



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

Search Results



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

Understanding vSphere Availability and Distributed Resource Scheduler (DRS)

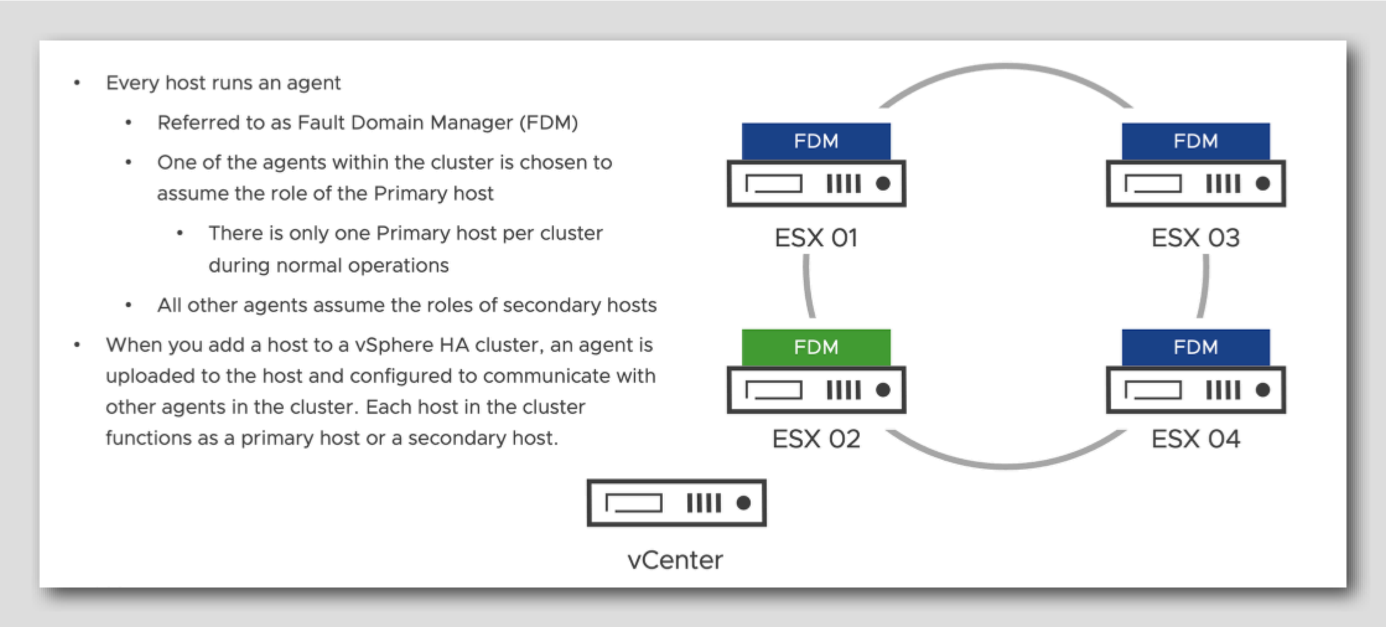
This lab shows how to use the VMware vSphere web client to enable and configure vSphere Availability and Dynamic Resource Scheduling (DRS). HA protects from down time by automating recovery in the event of a host failure. DRS ensures performance by balancing virtual machine workloads across hosts a cluster.

What is vSphere Availability? [119]

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 primary host. The primary host communicates with vCenter Server and monitors the state of all protected virtual machines and of the secondary hosts. Different types of host failures are possible, and the primary host must detect and appropriately deal with the failure. The primary 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.

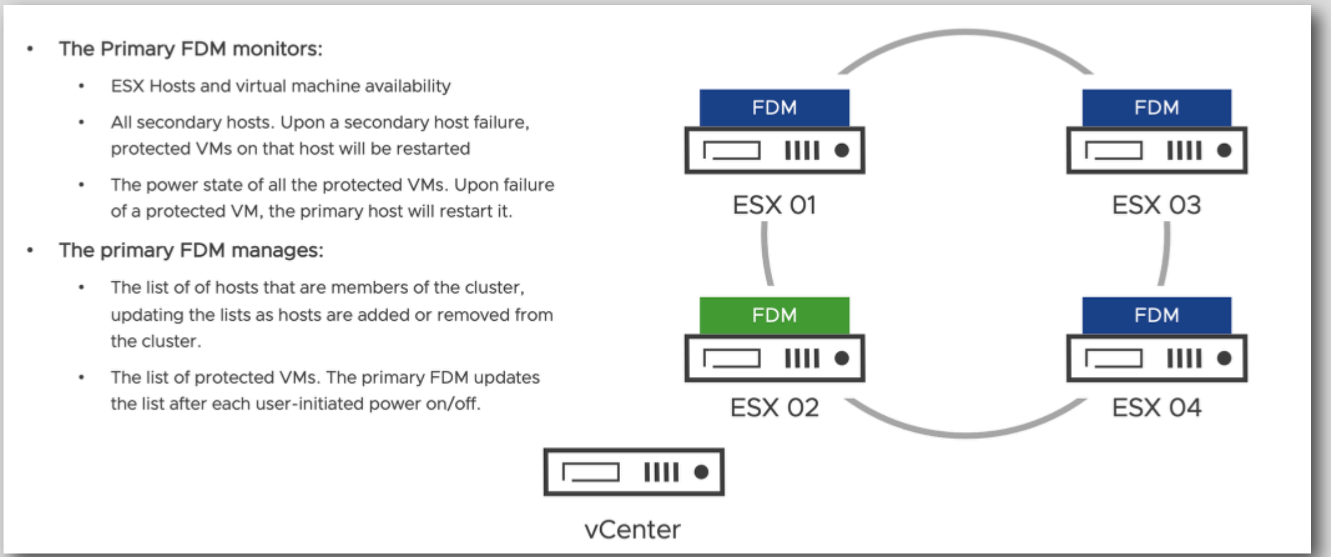
vSphere Availability Primary Components [120]



- Every host runs an agent
  - Referred to as Fault Domain Manager (FDM)
  - One of the agents within the cluster is chosen to assume the role of the Primary host
    - There is only one Primary host per cluster during normal operations
  - All other agents assume the roles of secondary hosts
- When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster. Each host in the cluster functions as a primary host or a secondary host.

The Primary Host Role

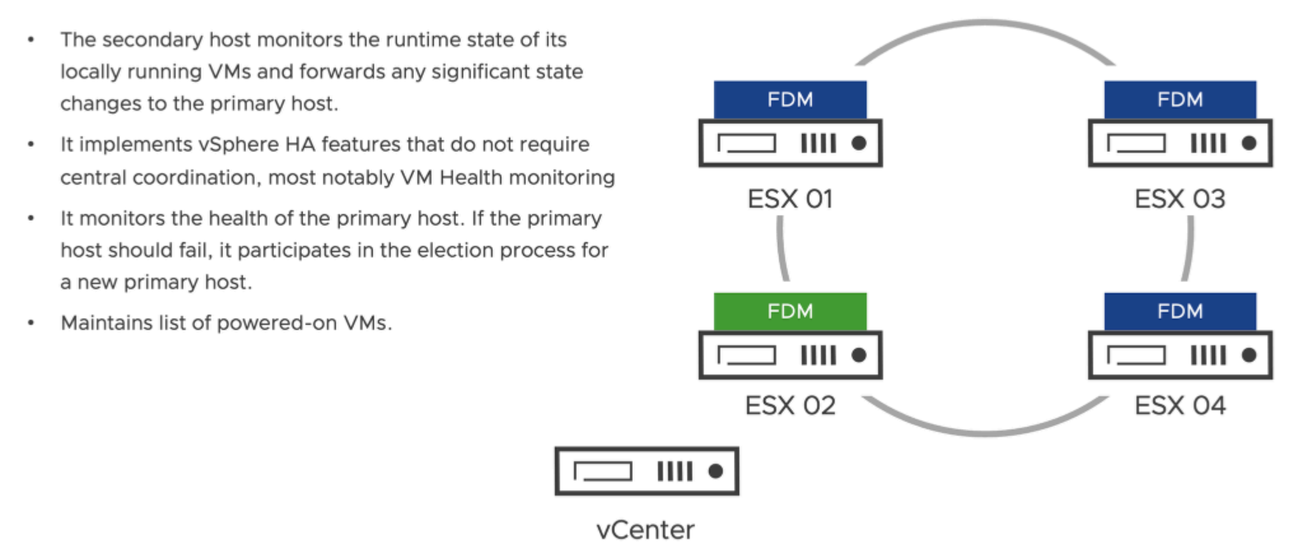
[121]



- **The Primary FDM monitors:**
  - ESX Hosts and virtual machine availability
  - All secondary hosts. Upon a secondary 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 primary host will restart it.
- **The primary FDM manages:**
  - The list of of hosts that are members of the cluster, updating the lists as hosts are added or removed from the cluster.
  - The list of protected VMs. The primary FDM updates the list after each user-initiated power on/off.

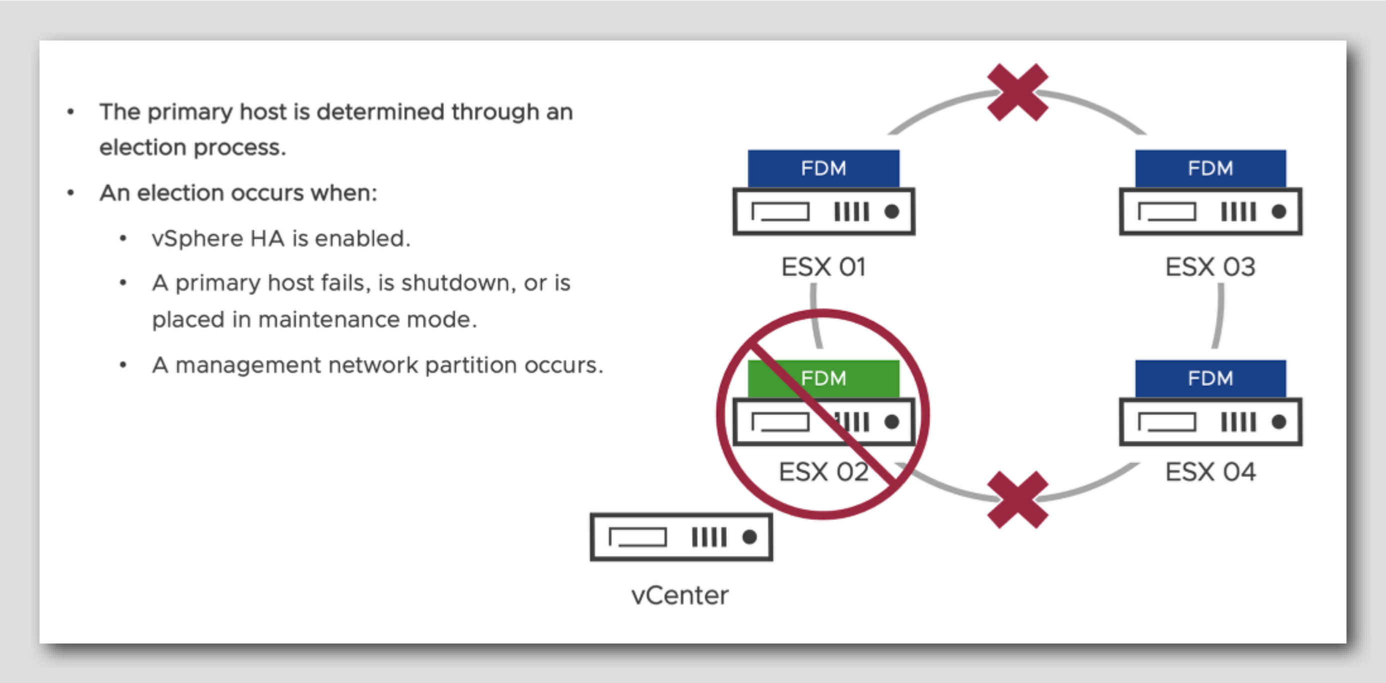
The Secondary Host Role

[122]



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

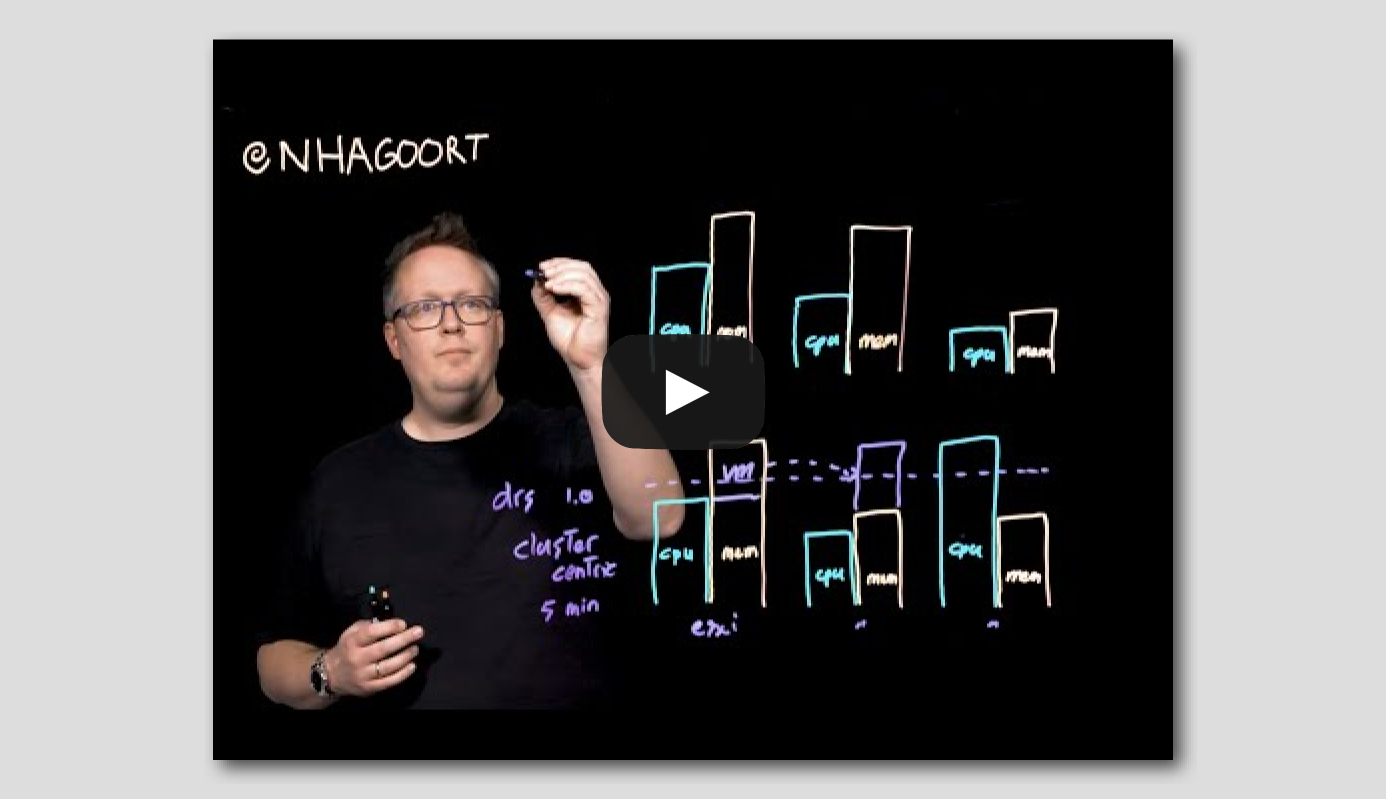
The Primary Host Election Process [123]



- The primary host is determined through an election process.
- An election occurs when:
  - vSphere HA is enabled.
  - A primary host fails, is shutdown, or is placed in maintenance mode.
  - A management network partition occurs.

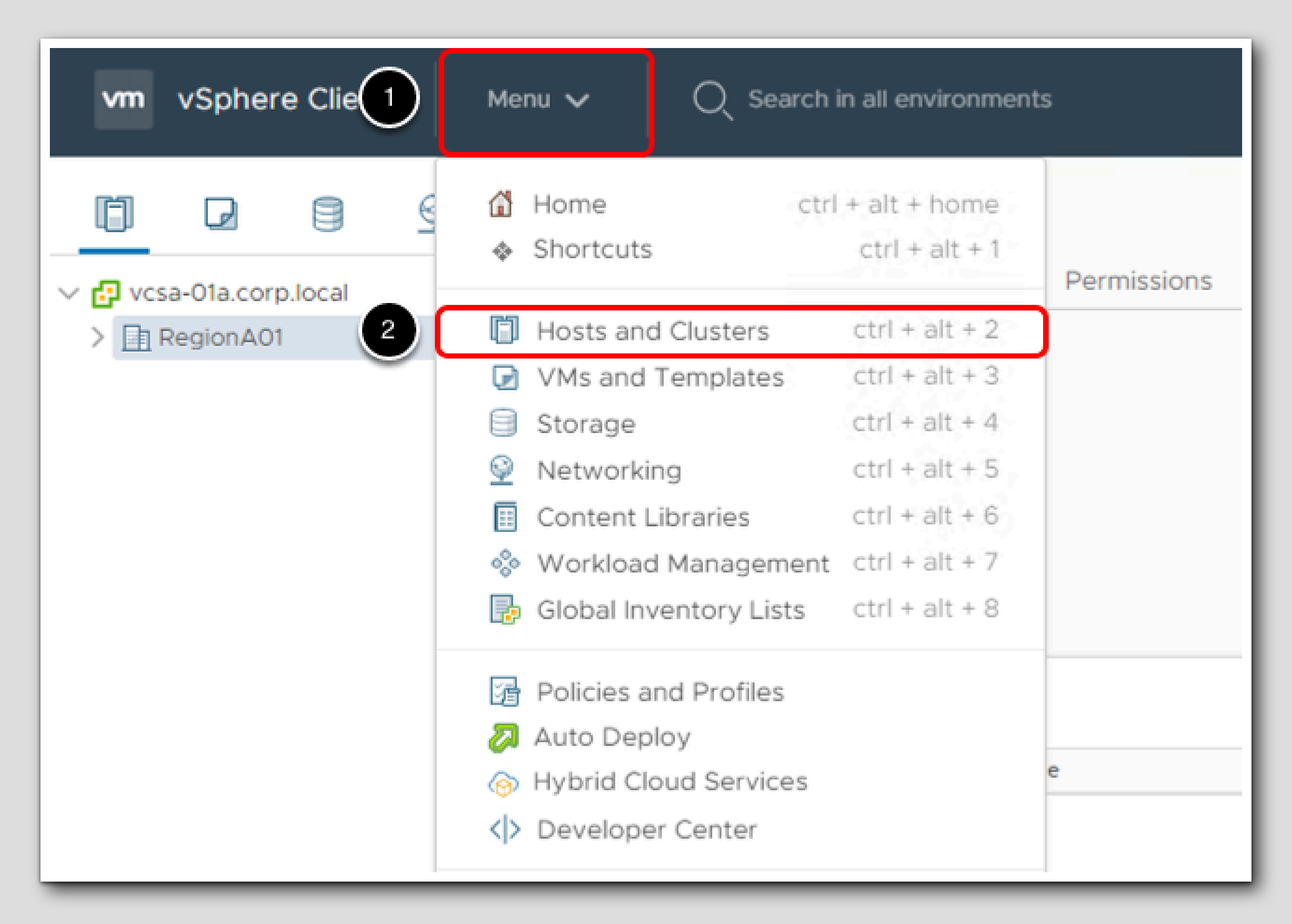
What&#39;s New with DRS in vSphere 7 (5:47) [124]

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



Enable and Configure vSphere Availability

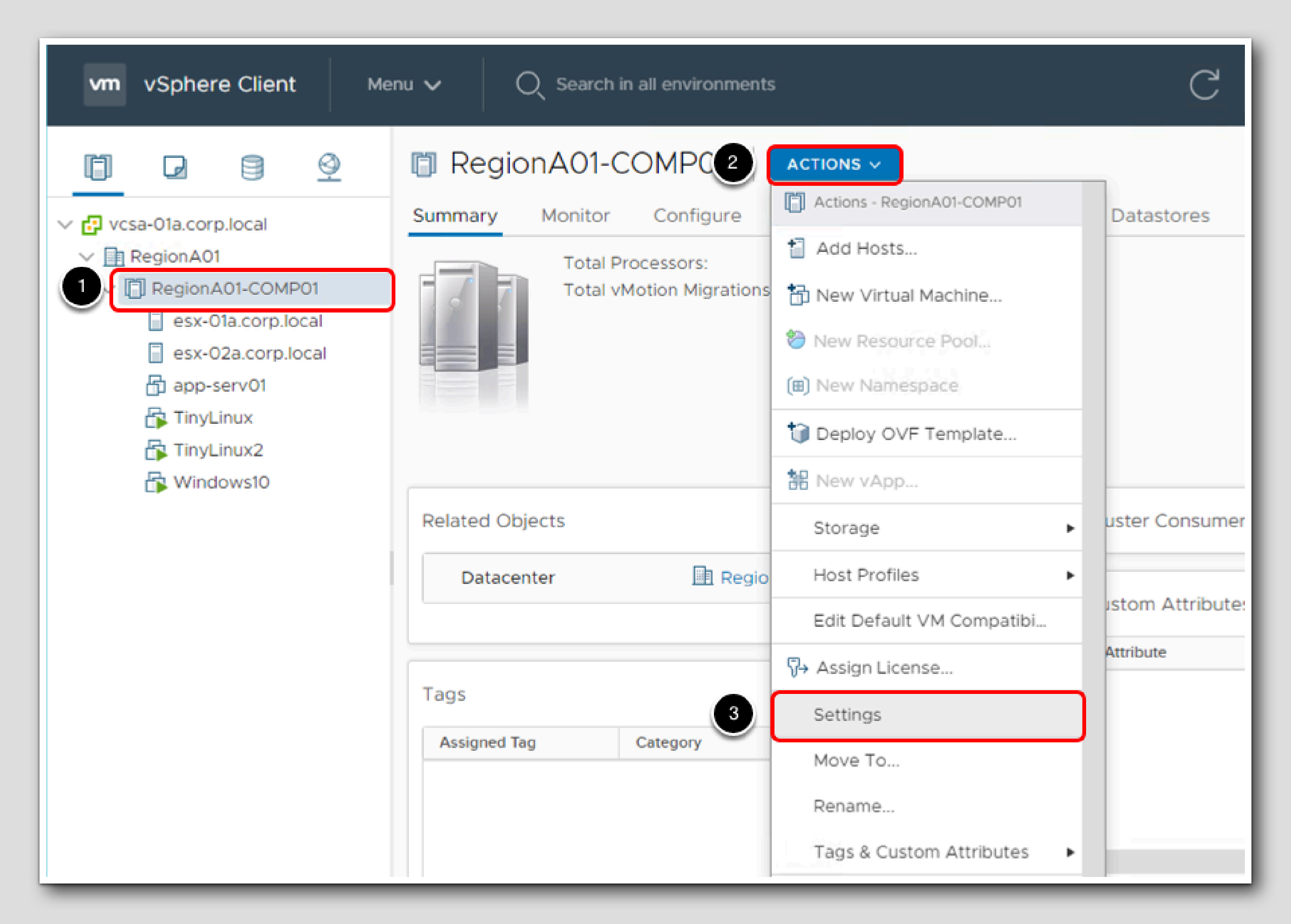
[125]


vm
vSphere Clie
1
Menu
Search in all environments
vcsa-01a.corp.local
RegionA01
2
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Workload Management ctrl + alt + 7
Global Inventory Lists ctrl + alt + 8
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Permissions

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

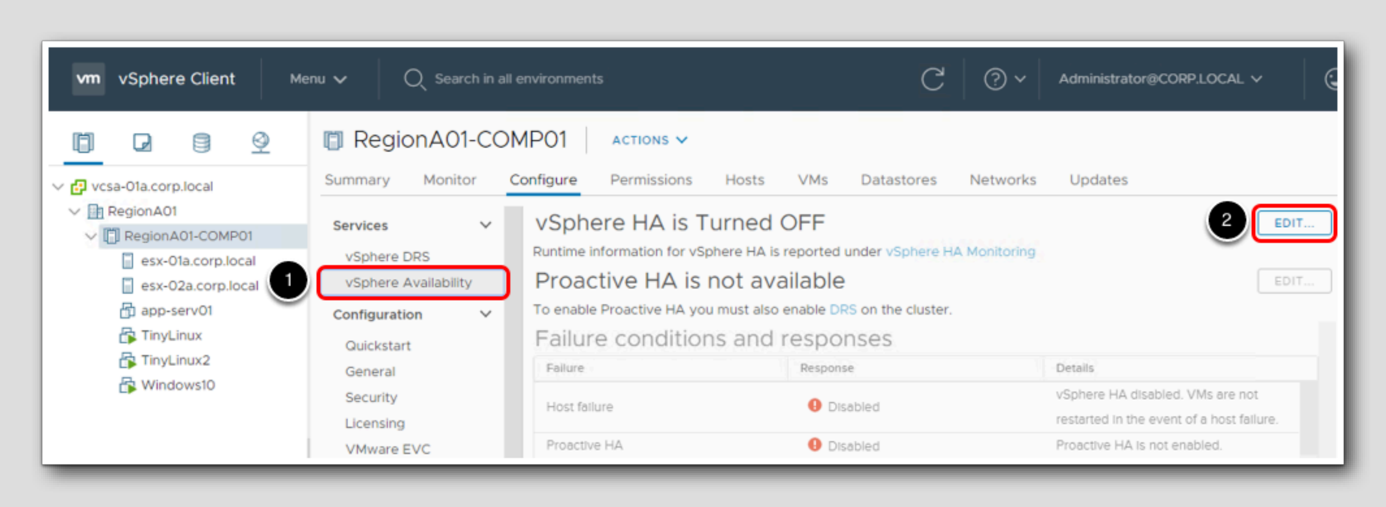
Settings for vSphere Availability

[126]



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

Cluster Settings



vSphere HA is Turned OFF

Runtime information for vSphere HA is reported under vSphere HA Monitoring

Proactive HA is not available

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

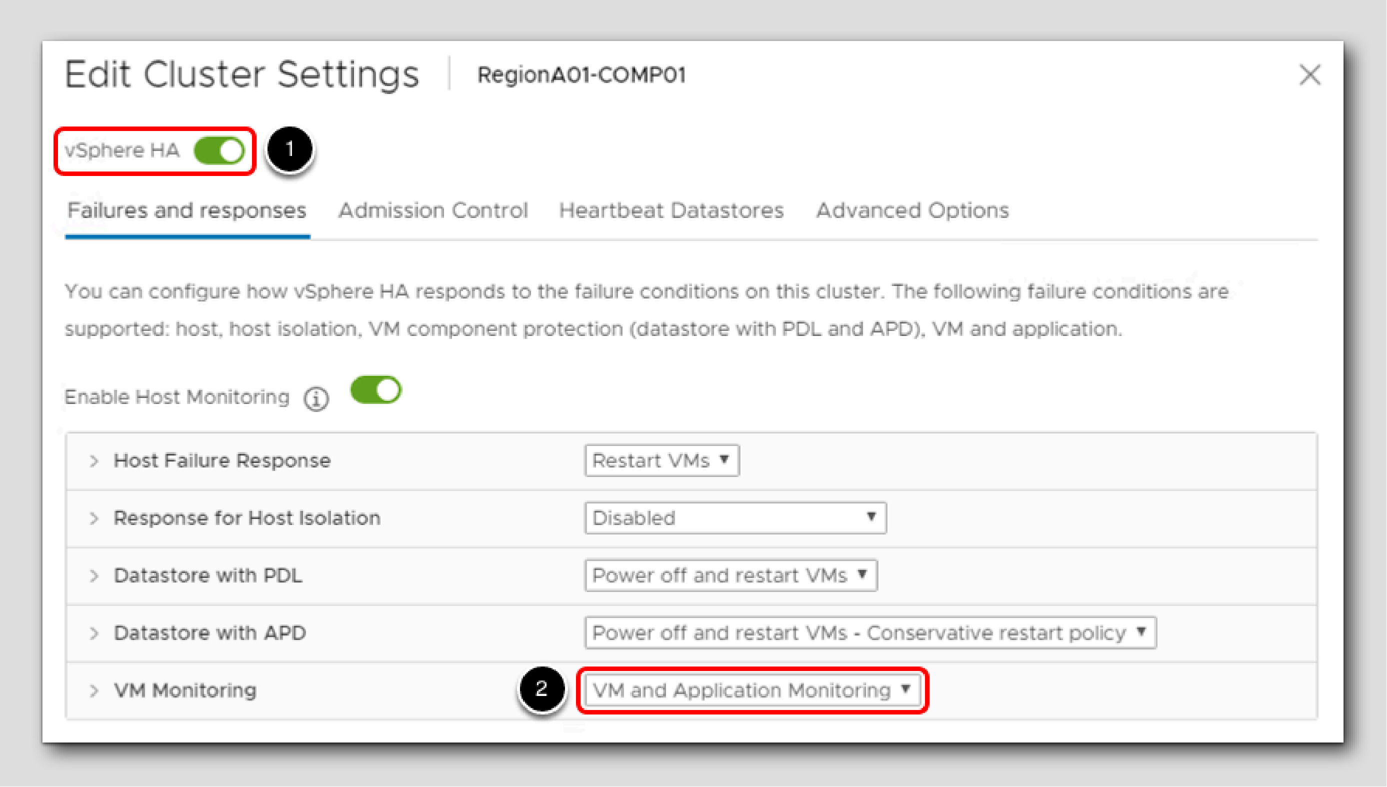
Failure conditions and responses

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

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

[128]



Edit Cluster Settings | RegionA01-COMP01

vSphere HA

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

Enable Host Monitoring

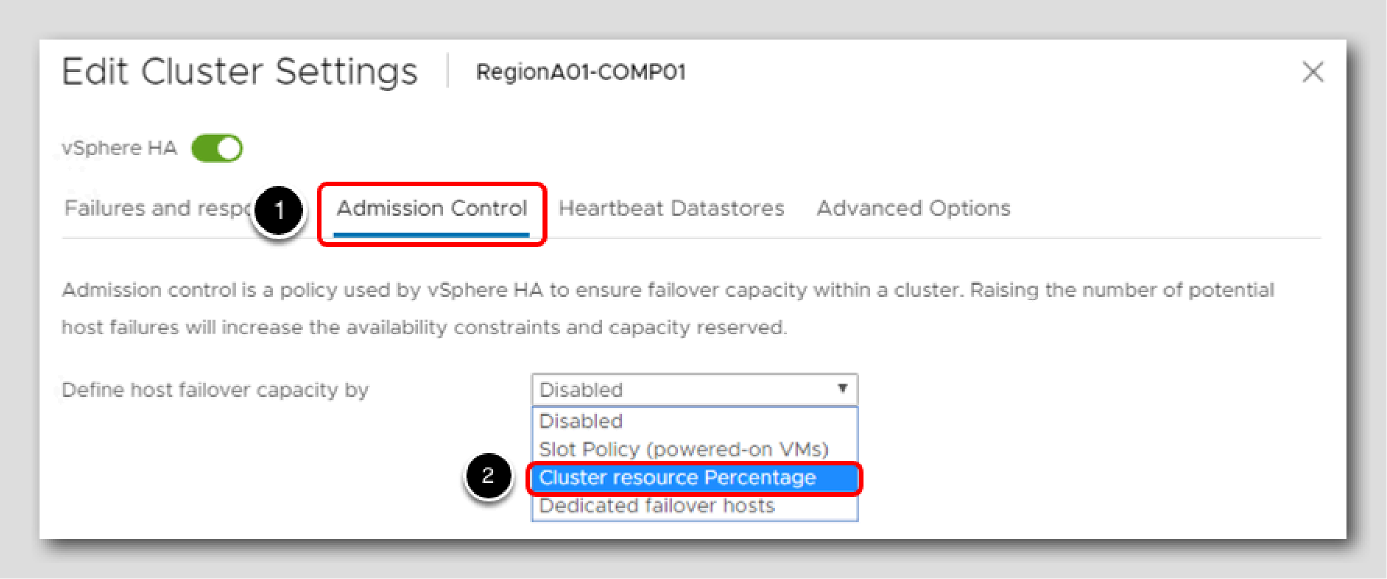
Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	VM and Application Monitoring

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.

Admission Control

[129]



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.

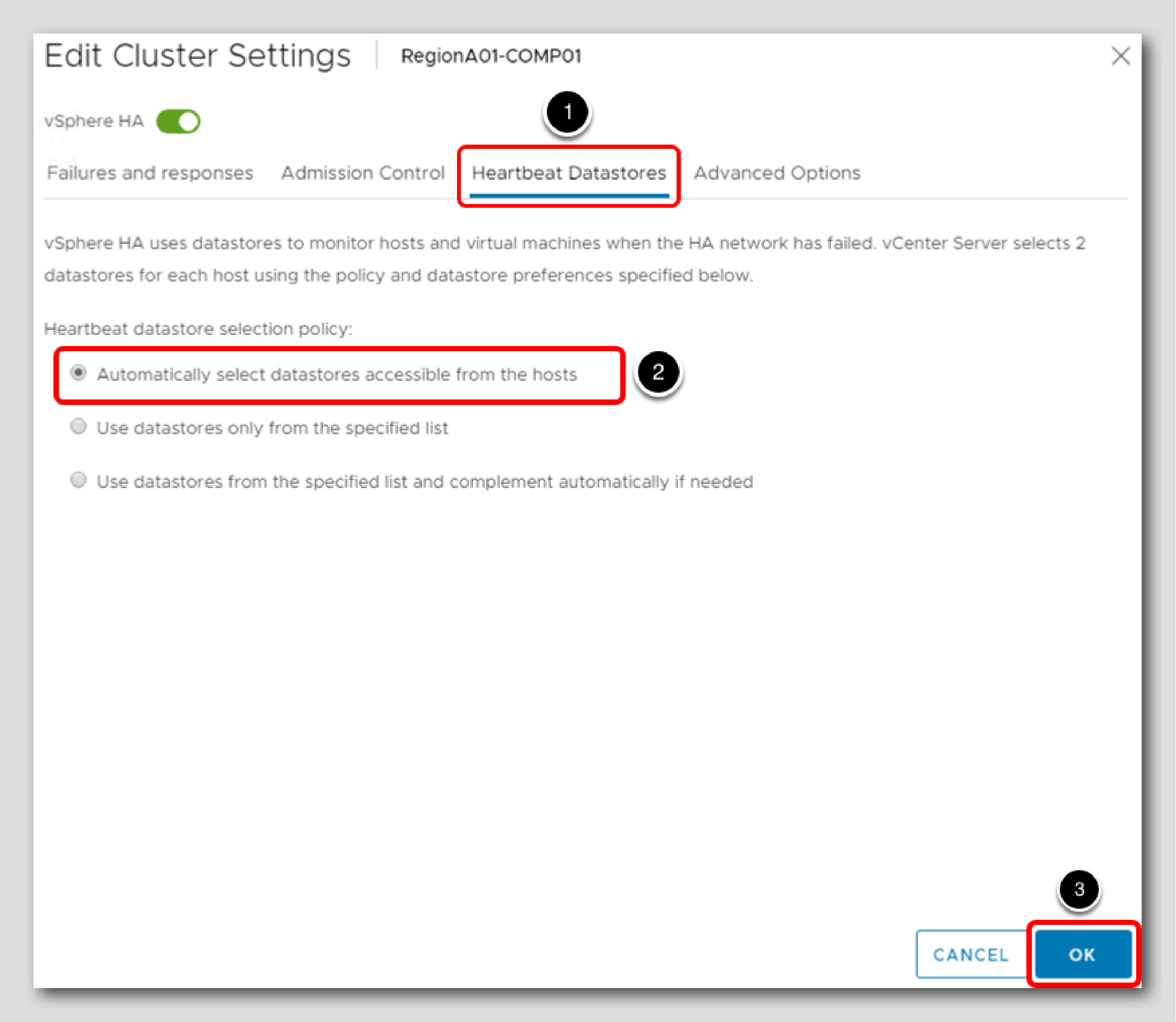
Define host failover capacity by: Disabled

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

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

Heartbeat Datastores

[130]



Edit Cluster Settings | RegionA01-COMP01

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

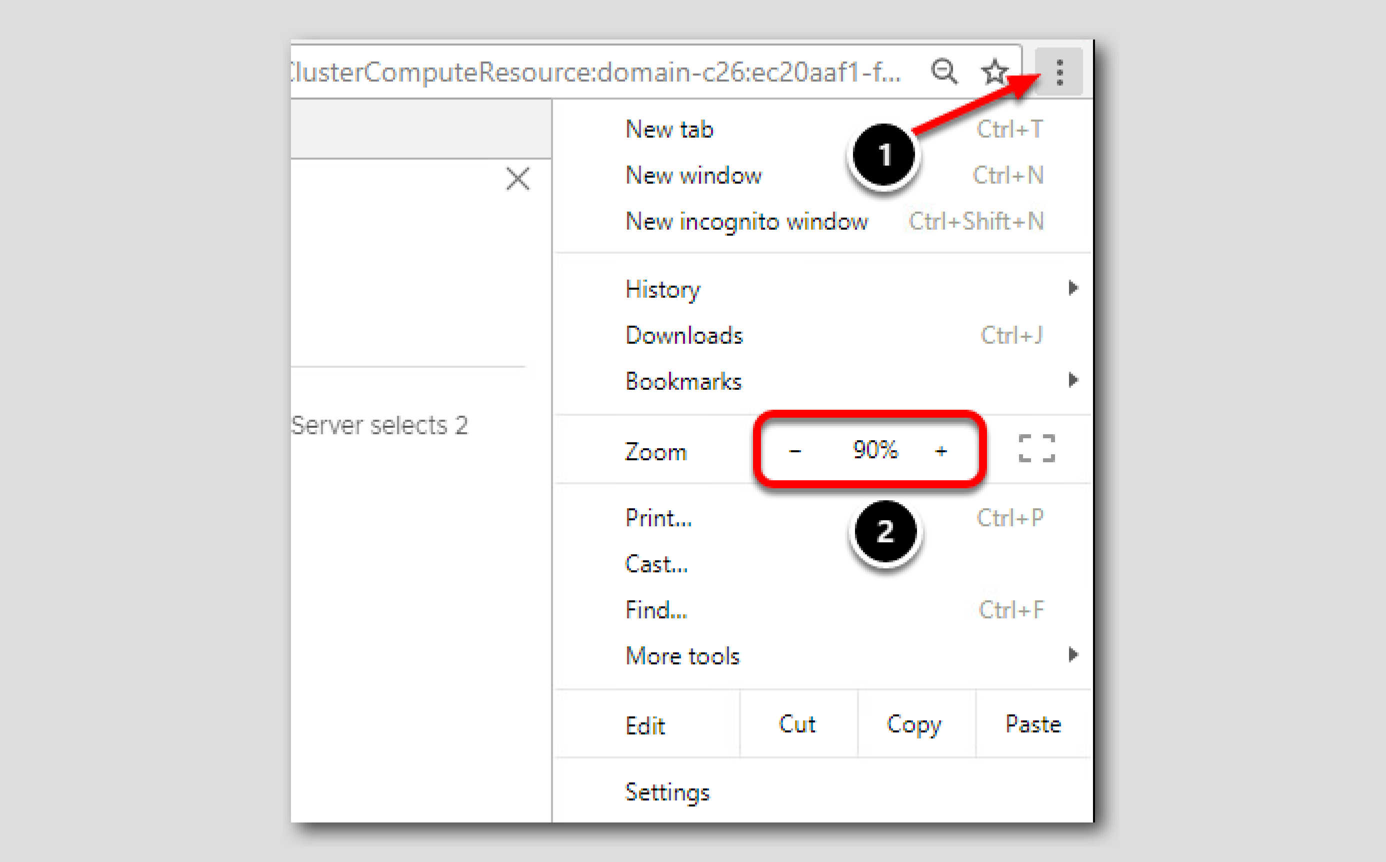
○ Use datastores only from the specified list

○ Use datastores from the specified list and complement automatically if needed

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

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

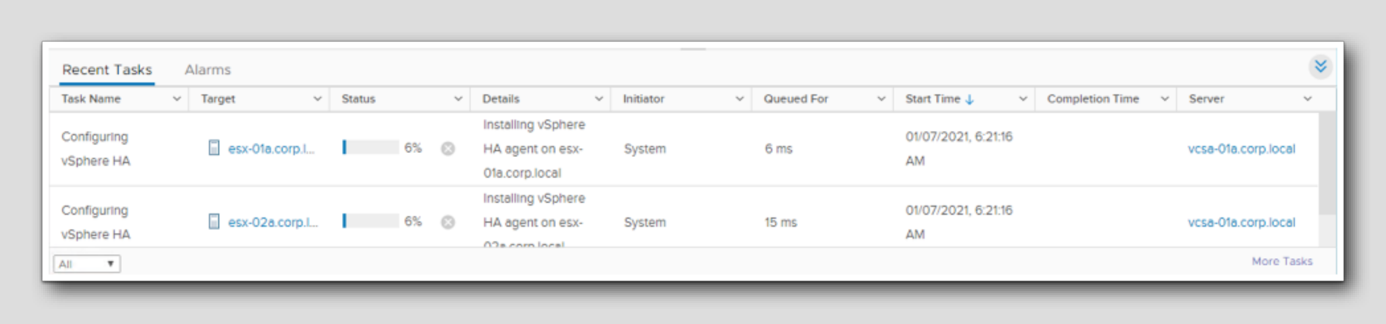
2. Click OK to enable vSphere HA.



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

Monitor the task

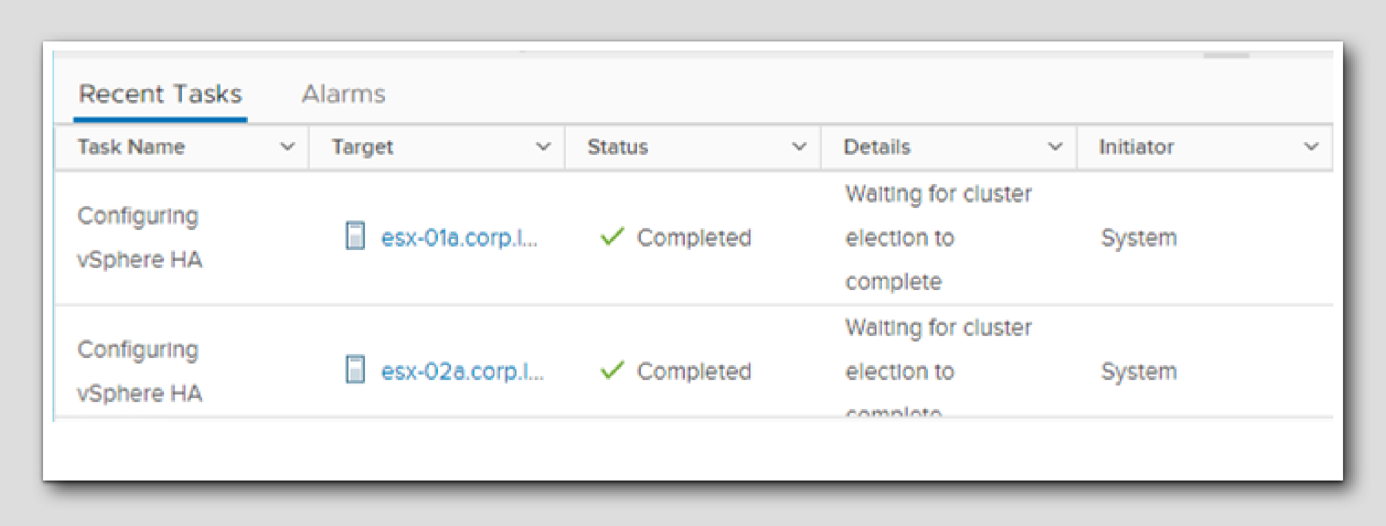
[131]



Recent Tasks | Alarms

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

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

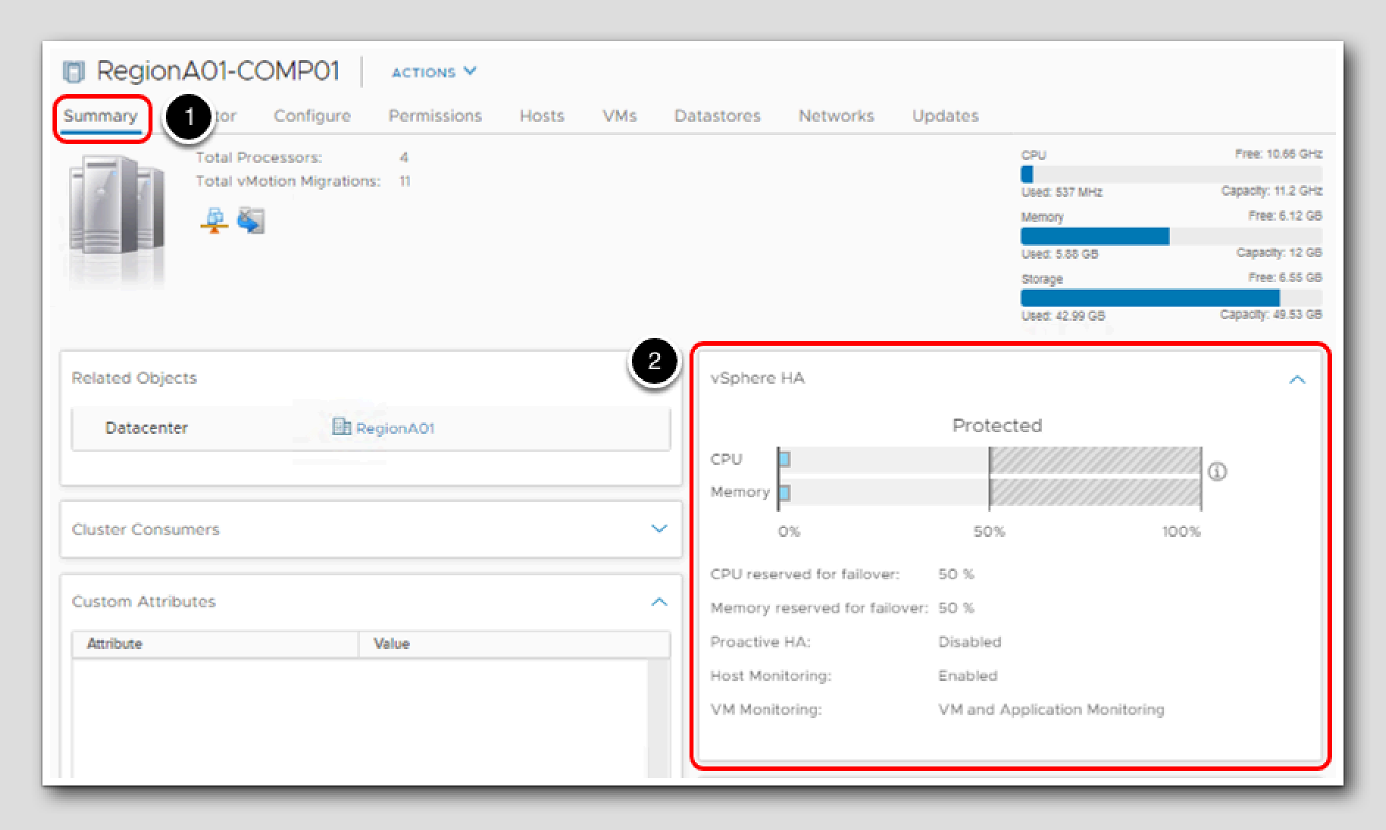


Task Name	Target	Status	Details	Initiator
Configuring vSphere HA	esx-01a.corp.l...	✓ Completed	Waiting for cluster election to complete	System
Configuring vSphere HA	esx-02a.corp.l...	✓ Completed	Waiting for cluster election to complete	System

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

Use the Summary Tab to Verify that HA Is Enabled

[132]



Total Processors: 4

Total vMotion Migrations: 11

CPU Free: 10.66 GHz

Used: 537 MHz Capacity: 11.2 GHz

Memory Free: 6.12 GB

Used: 5.88 GB Capacity: 12 GB

Storage Free: 6.55 GB

Used: 42.99 GB Capacity: 49.53 GB

Related Objects

Datacenter	RegionA01

Cluster Consumers

Custom Attributes

Attribute	Value

vSphere HA

Protected

CPU

Memory

CPU reserved for failover: 50 %

Memory reserved for failover: 50 %

Proactive HA: Disabled

Host Monitoring: Enabled

VM Monitoring: VM and Application Monitoring

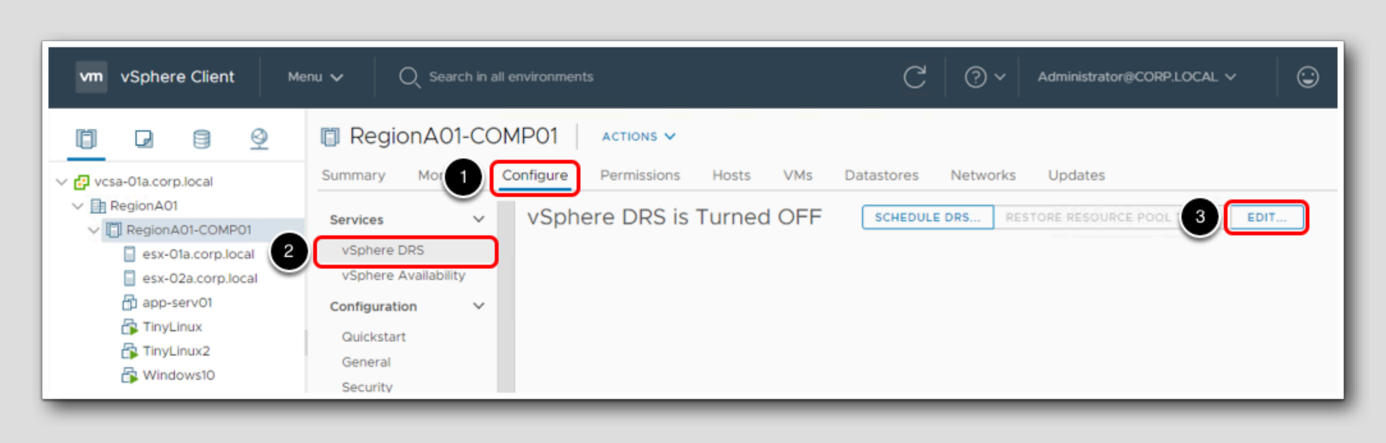
1. Click the **Summary** tab
2. Locate and expand the **vSphere HA** panel in the data area: click on the ">" to the right of the panel's name to expand it.

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

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

Enable Distributed Resource Scheduler (DRS)

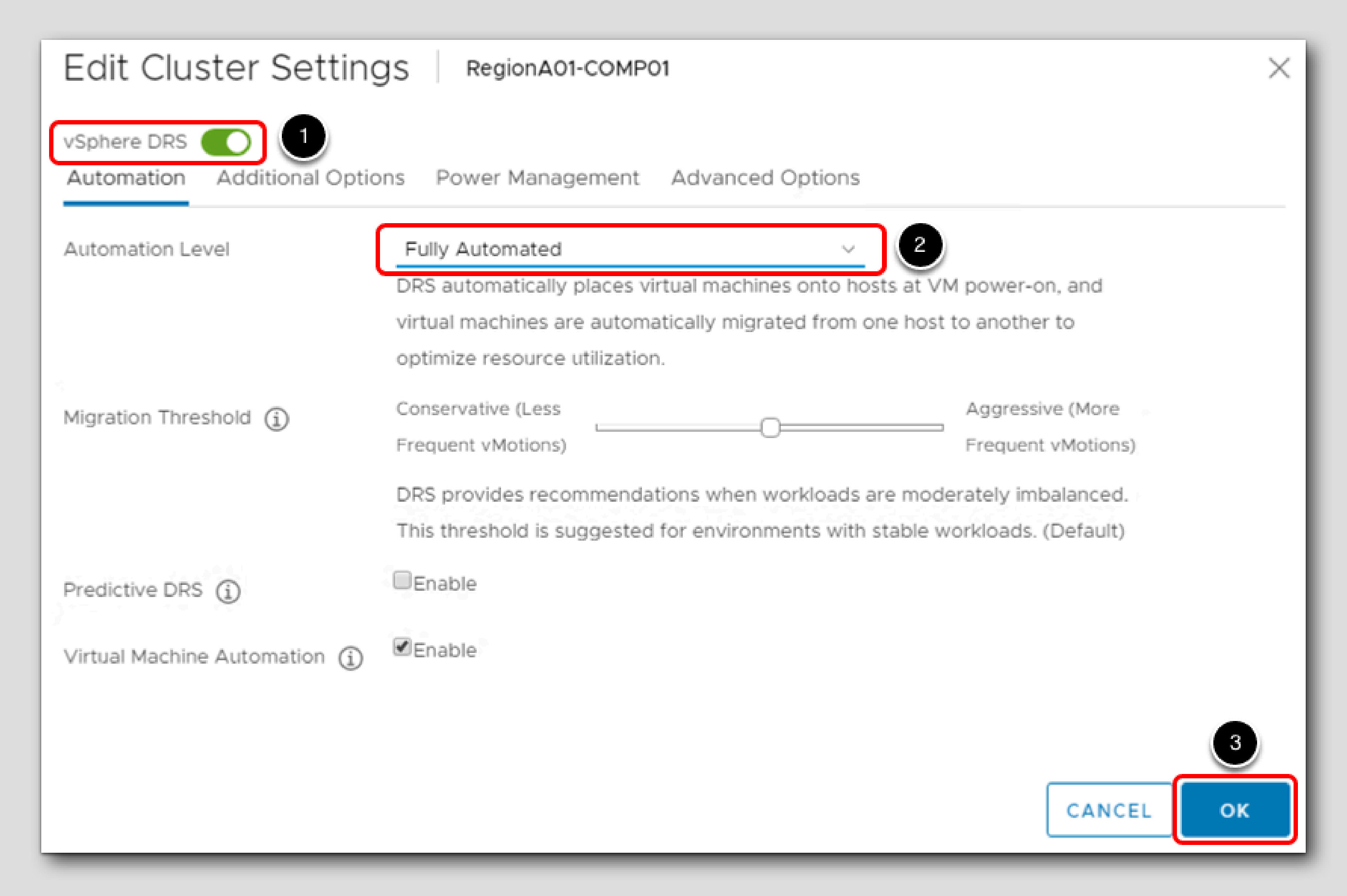
[133]



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)

[134]



Edit Cluster Settings | RegionA01-COMP01

vSphere DRS (on)

Automation Level: Fully Automated

DRS automatically places virtual machines onto hosts at VM power-on, and virtual machines are automatically migrated from one host to another to optimize resource utilization.

Migration Threshold: Conservative (Less Frequent vMotions) — Aggressive (More Frequent vMotions)

DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

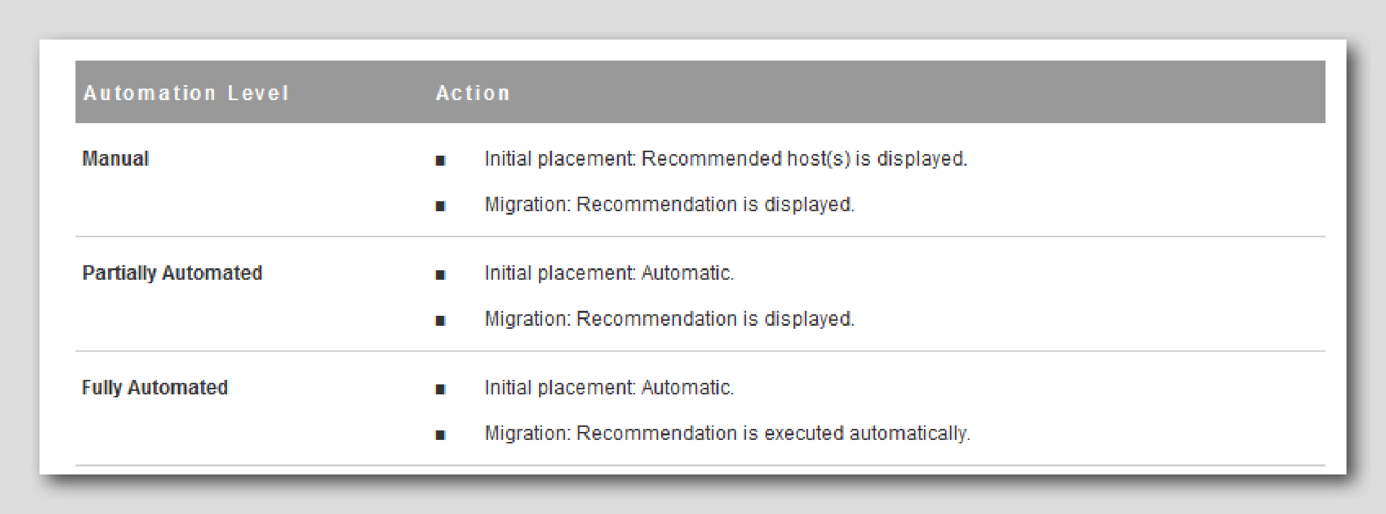
Predictive DRS: □ Enable

Virtual Machine Automation: ☑ Enable

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

Automation Levels

[135]

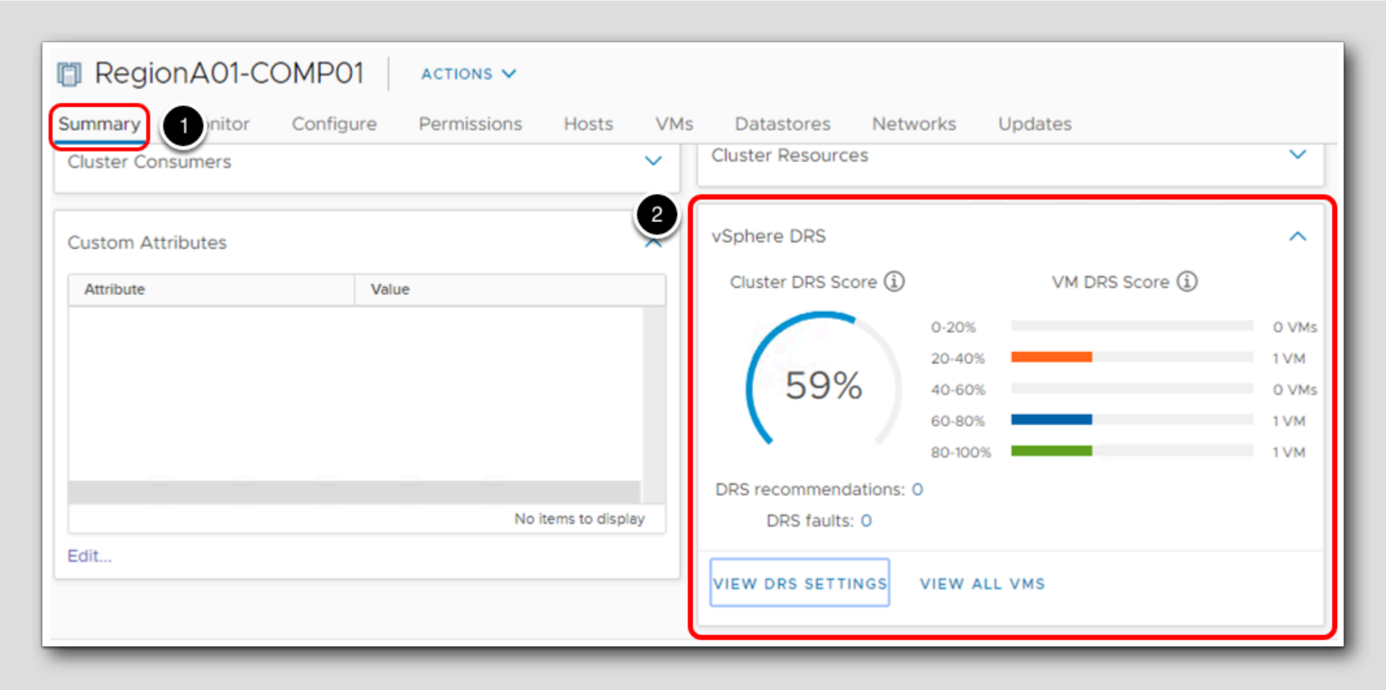


Automation Level	Action
Manual	■ Initial placement: Recommended host(s) is displayed. ■ Migration: Recommendation is displayed.
Partially Automated	■ Initial placement: Automatic. ■ Migration: Recommendation is displayed.
Fully Automated	■ Initial placement: Automatic. ■ Migration: Recommendation is 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&#39;s Summary Tab to Check Cluster Balance

[136]



Attribute	Value

No items to display

Cluster DRS Score: 59%

VM DRS Score

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

DRS recommendations: 0

DRS faults: 0

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

vSphere 7 Fault Tolerance Provides Continuous Availability

[137]

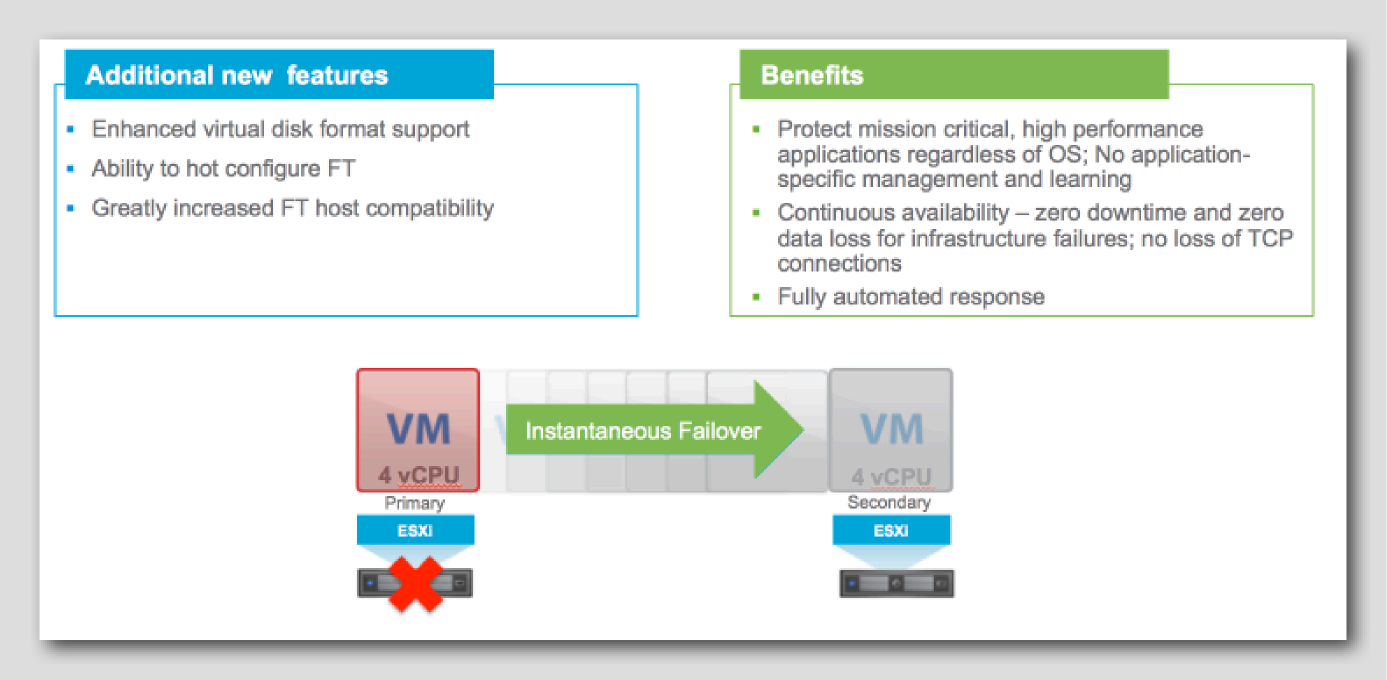
You can use vSphere Fault Tolerance for your virtual machines to ensure continuity with higher levels of availability and data protection. Fault Tolerance is built on the ESXi host platform, and it provides availability by having identical Virtual Machines (VM) run on separate hosts.

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

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

VMware vSphere Fault Tolerance

[138]



Additional new features

- Enhanced virtual disk format support
- Ability to hot configure FT
- Greatly increased FT host compatibility

Benefits

- 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

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

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

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

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

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

[139]

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

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

Cluster Prerequisites for Fault Tolerance

- Enable host certificate checking
- Configure networking for each host
- Create the vSphere HA cluster, add hosts, and check compliance

Monitoring Events and Creating Alarms [140]

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

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

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

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

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

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

Alarms have the following severity levels:

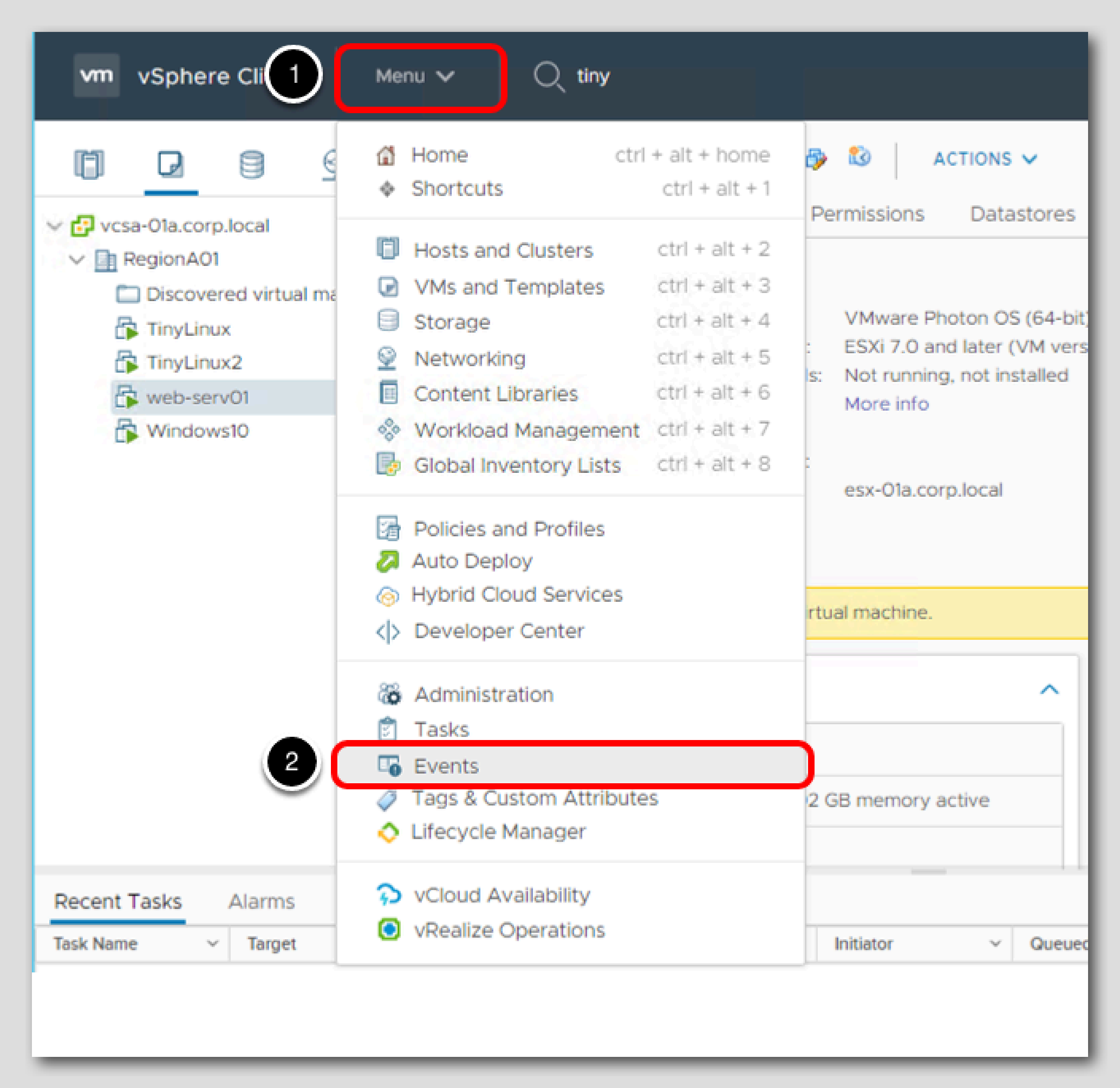
- Normal – green
- Warning – yellow
- Alert – red

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

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

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

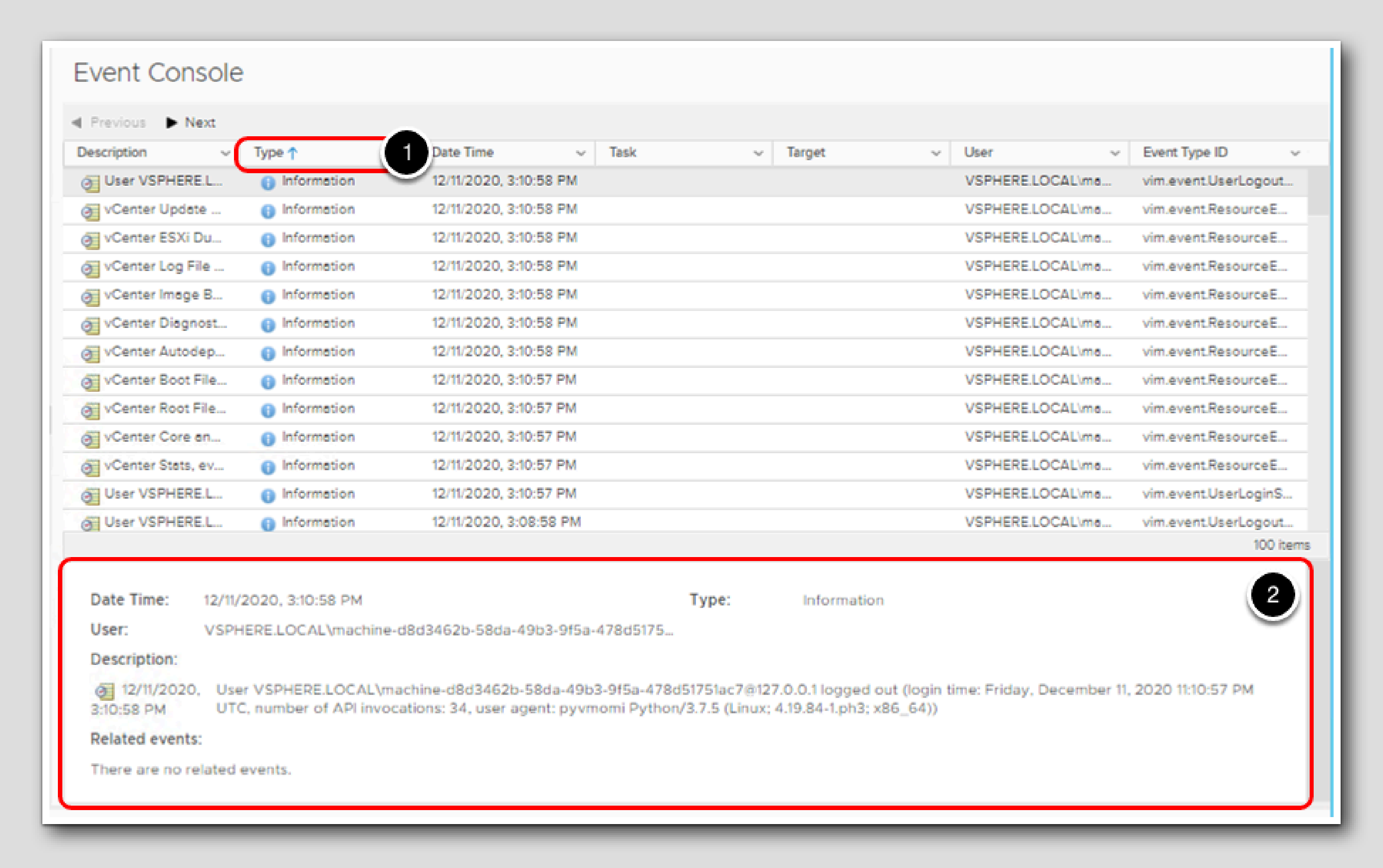
Review default alerts



1. Click **Menu**
2. Click on **Events** menu item

Event Console

[142]



Event Console

◀ Previous ▶ Next

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

100 items

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

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

Description:

12/11/2020, 3:10:58 PM User VSPHERE.LOCAL\machine-d8d3462b-58da-49b3-9f5a-478d51751ac7@127.0.0.1 logged out (login time: Friday, December 11, 2020 11:10:57 PM UTC, number of API invocations: 34, user agent: pyvmomi Python/3.7.5 (Linux; 4.19.84-1.ph3; x86_64))

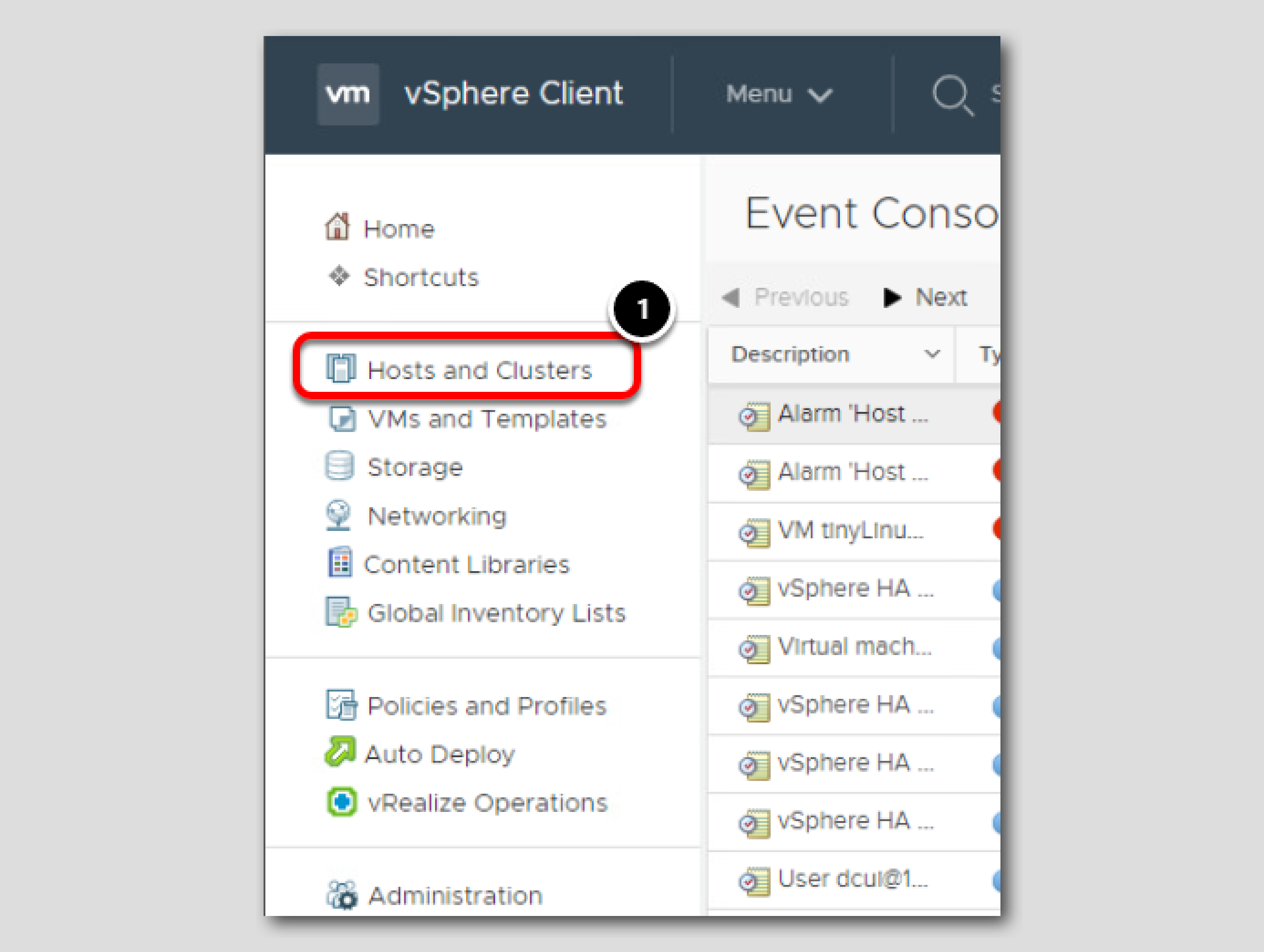
Related events:

There are no related events.

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

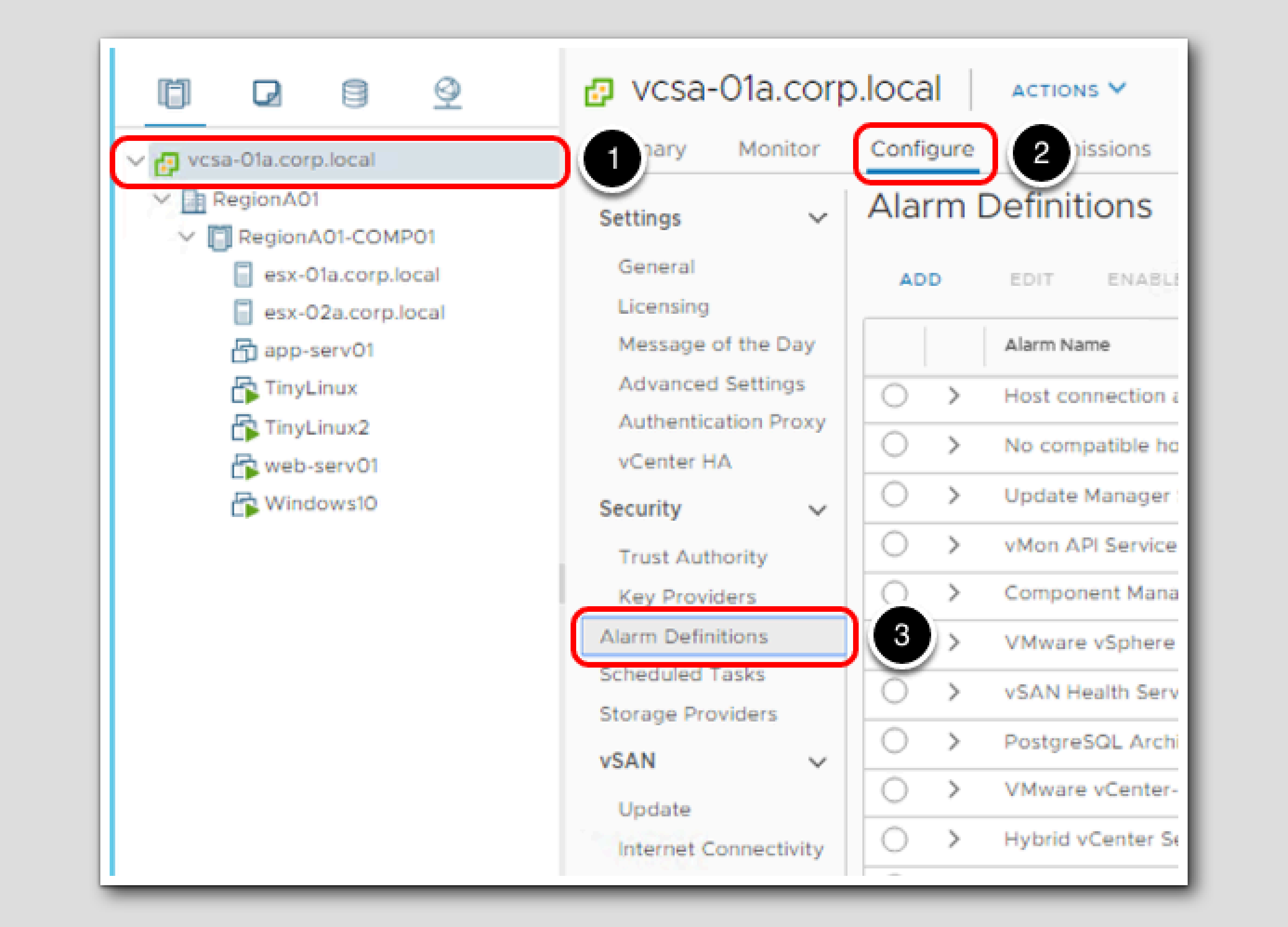
Setup notifications

[143]



1. Click Hosts and Clusters.

Setup Notifications

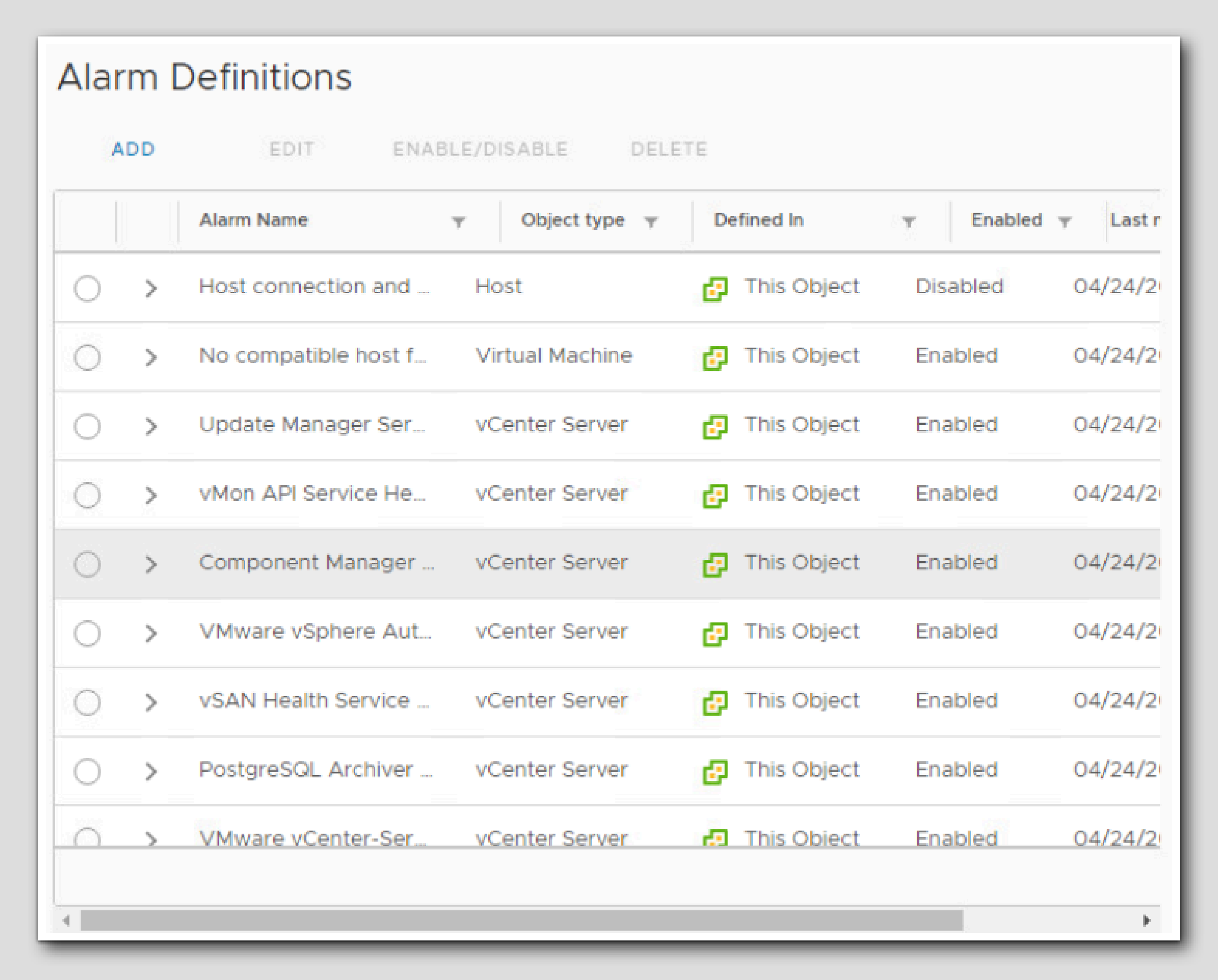


1. Select the vCenter - vcsa-01a.corp.local
2. Click the Configure tab
3. Click on Alarm Definitions. The default alarm definitions are shown.

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

[145]

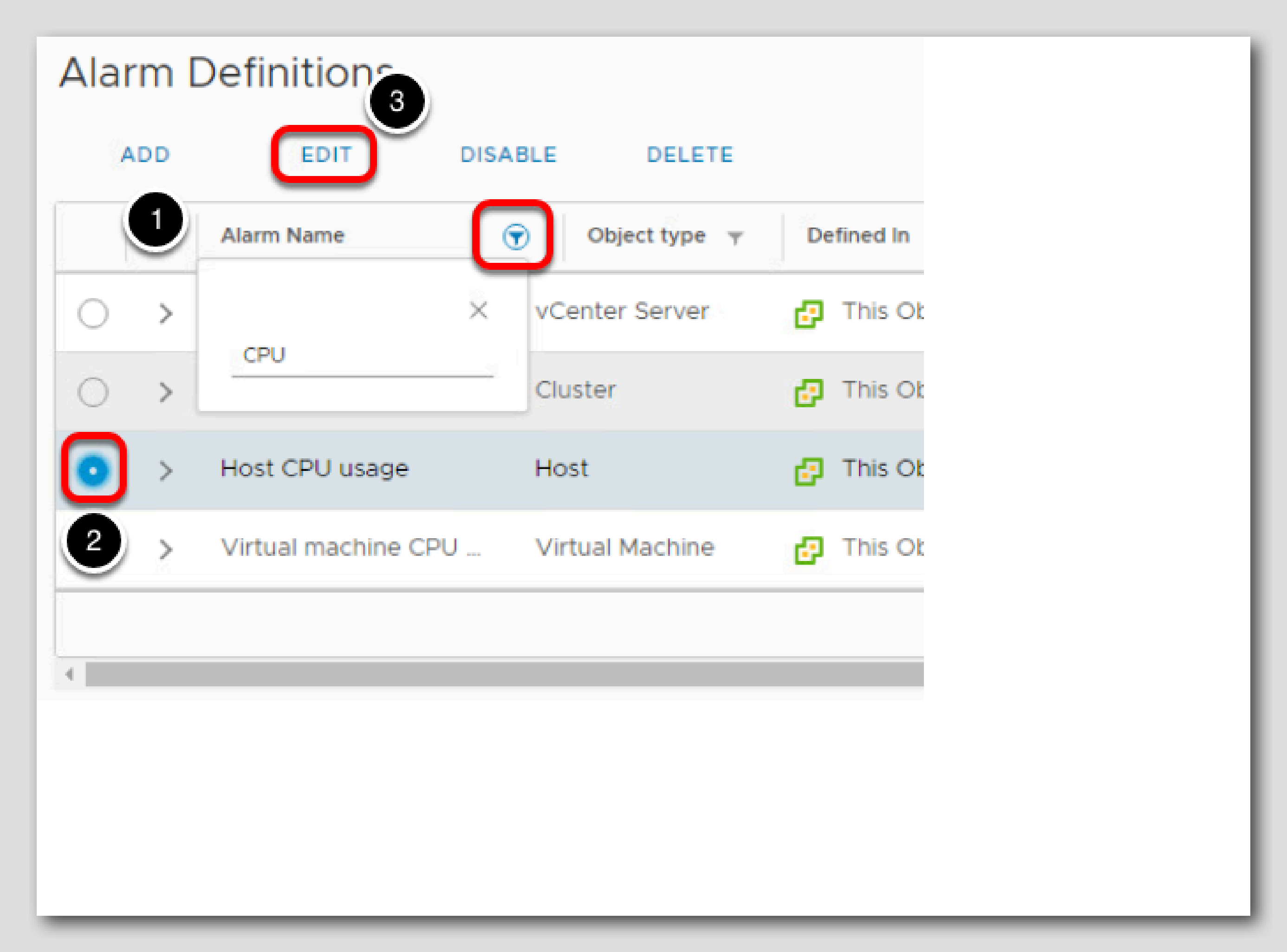


Alarm Definitions

		Alarm Name	Object type	Defined In	Enabled	Last r
○	>	Host connection and ...	Host	This Object	Disabled	04/24/2
○	>	No compatible host f...	Virtual Machine	This Object	Enabled	04/24/2
○	>	Update Manager Ser...	vCenter Server	This Object	Enabled	04/24/2
○	>	vMon API Service He...	vCenter Server	This Object	Enabled	04/24/2
○	>	Component Manager ...	vCenter Server	This Object	Enabled	04/24/2
○	>	VMware vSphere Aut...	vCenter Server	This Object	Enabled	04/24/2
○	>	vSAN Health Service ...	vCenter Server	This Object	Enabled	04/24/2
○	>	PostgreSQL Archiver ...	vCenter Server	This Object	Enabled	04/24/2
○	>	VMware vCenter-Ser...	vCenter Server	This Object	Enabled	04/24/2

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



Alarm Definitions

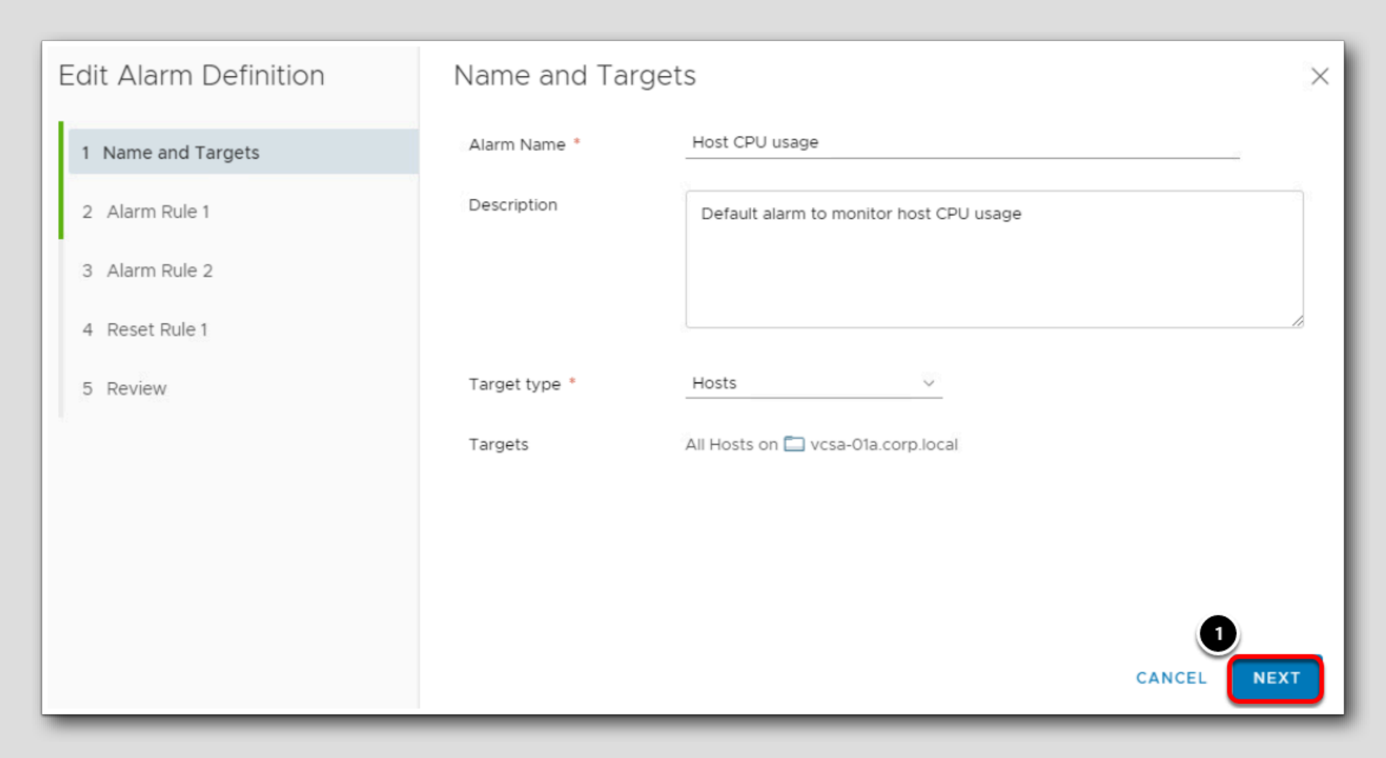
ADD EDIT DISABLE DELETE

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

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

Name and Targets

[147]



Alarm Name * Host CPU usage

Description Default alarm to monitor host CPU usage

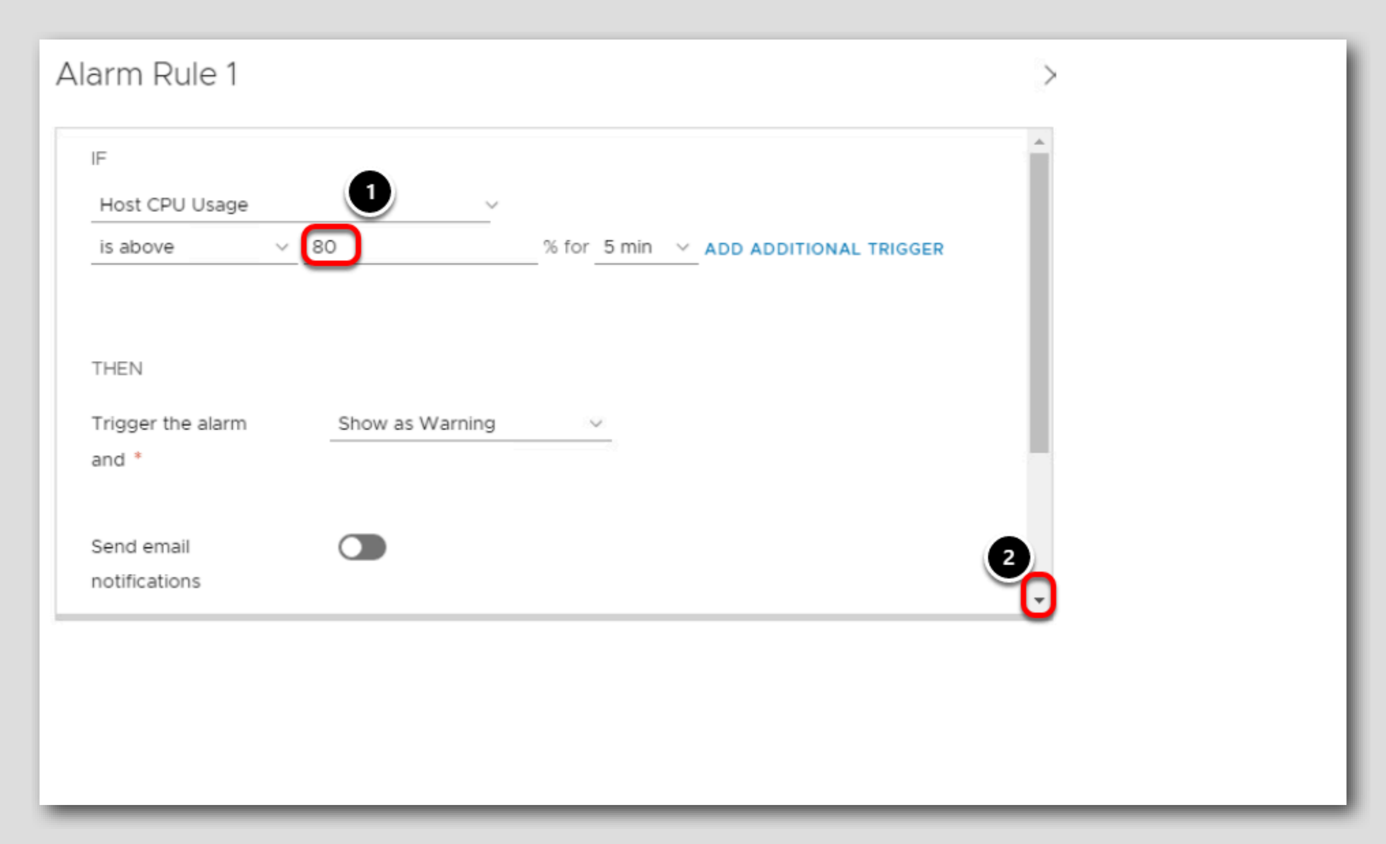
Target type * Hosts

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

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

THEN

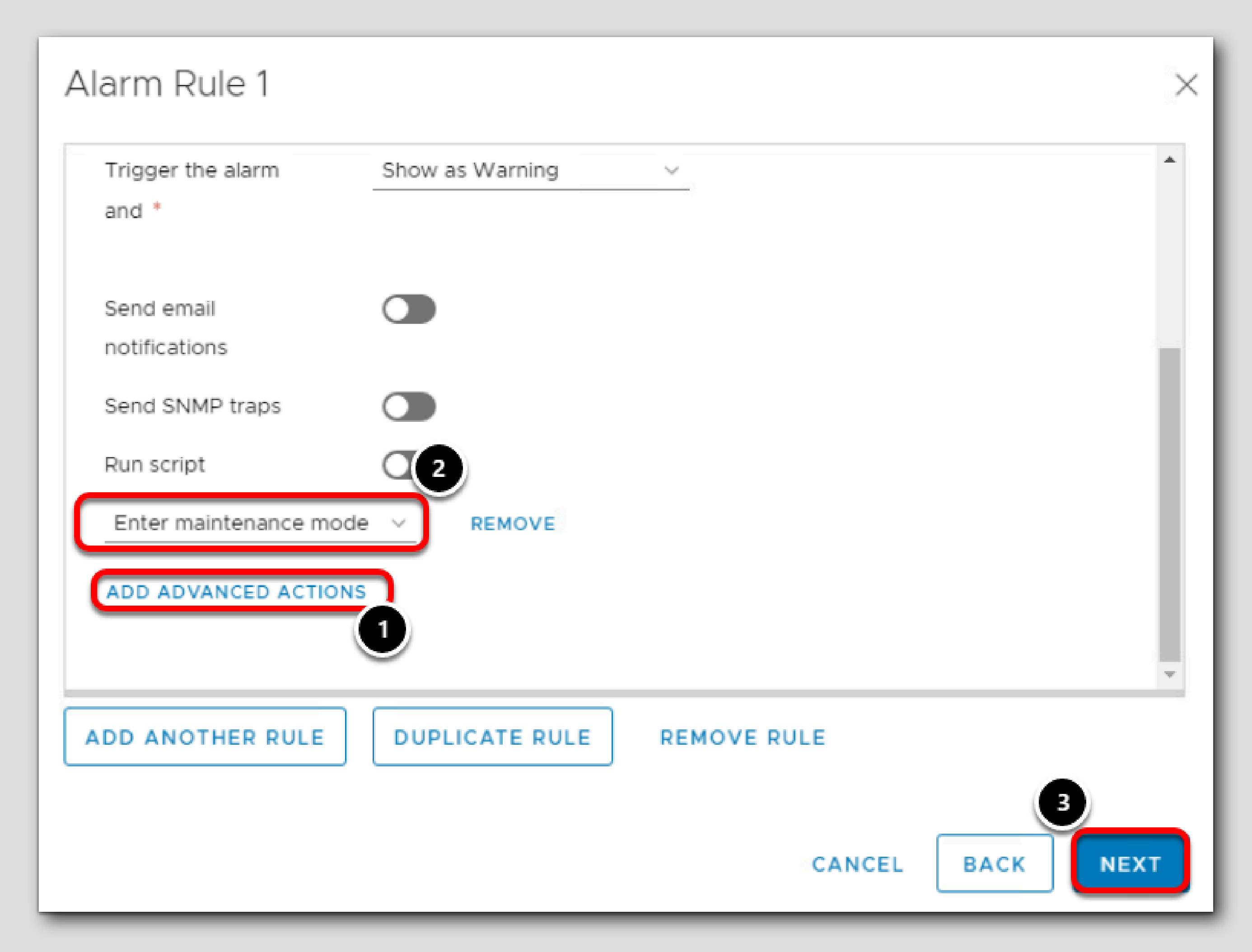
Trigger the alarm and * Show as Warning

Send email notifications

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



Alarm Rule 1

Trigger the alarm and * Show as Warning

Send email notifications ○

Send SNMP traps ○

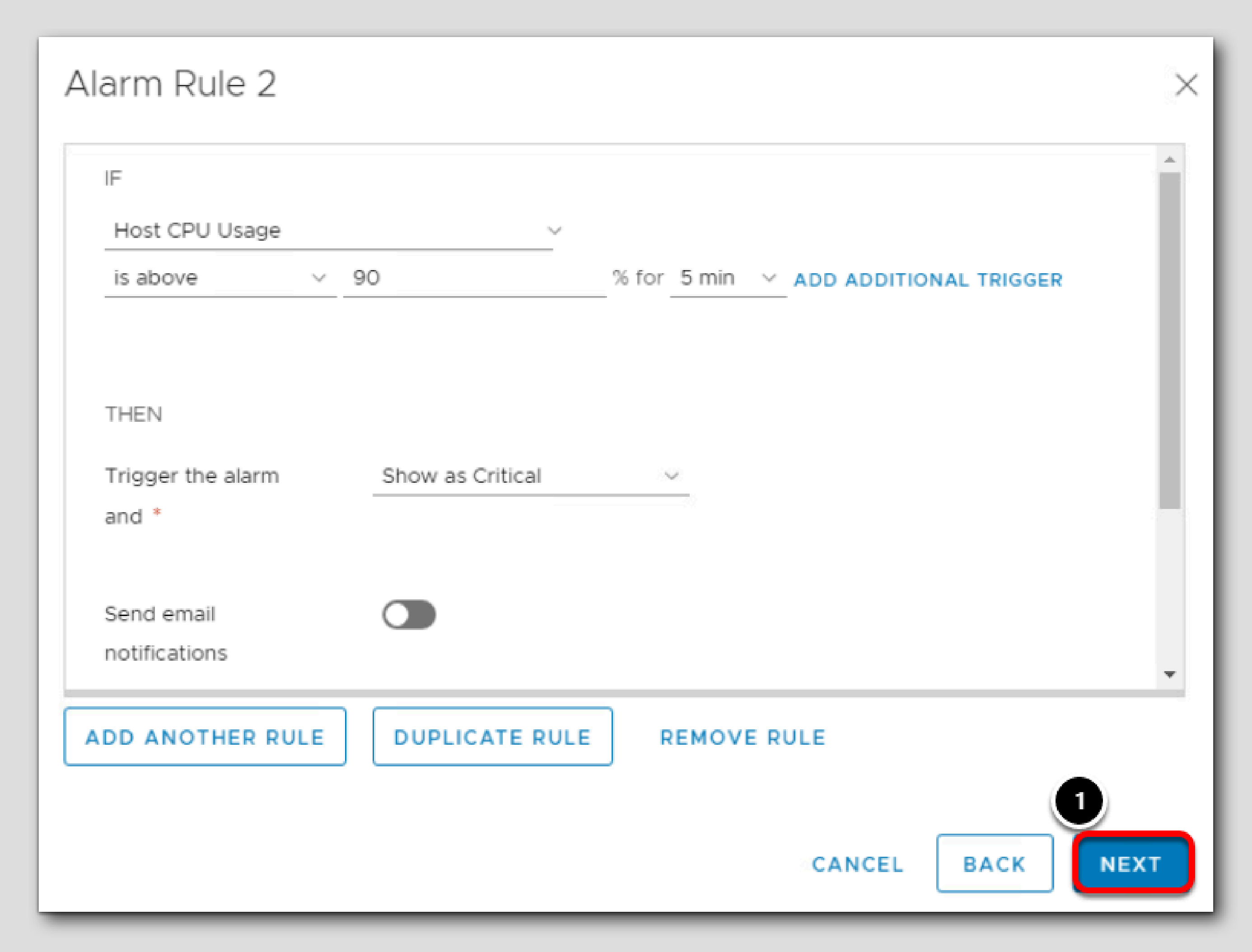
Run script ○

Enter maintenance mode

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

IF

Host CPU Usage

is above 90 % for 5 min

THEN

Trigger the alarm Show as Critical

and *

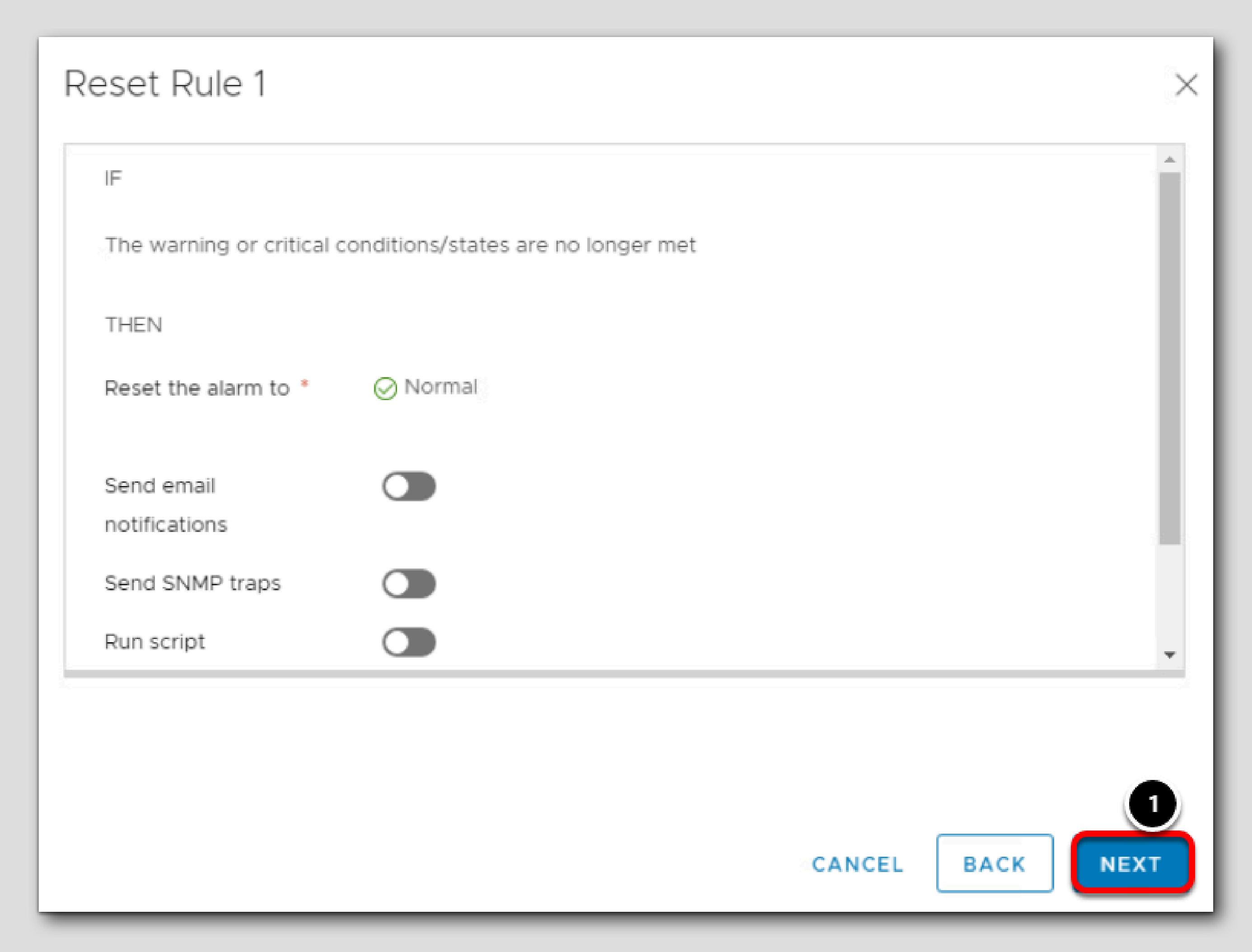
Send email notifications

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

[151]



Reset Rule 1

IF

The warning or critical conditions/states are no longer met

THEN

Reset the alarm to * ✓ Normal

Send email notifications

Send SNMP traps

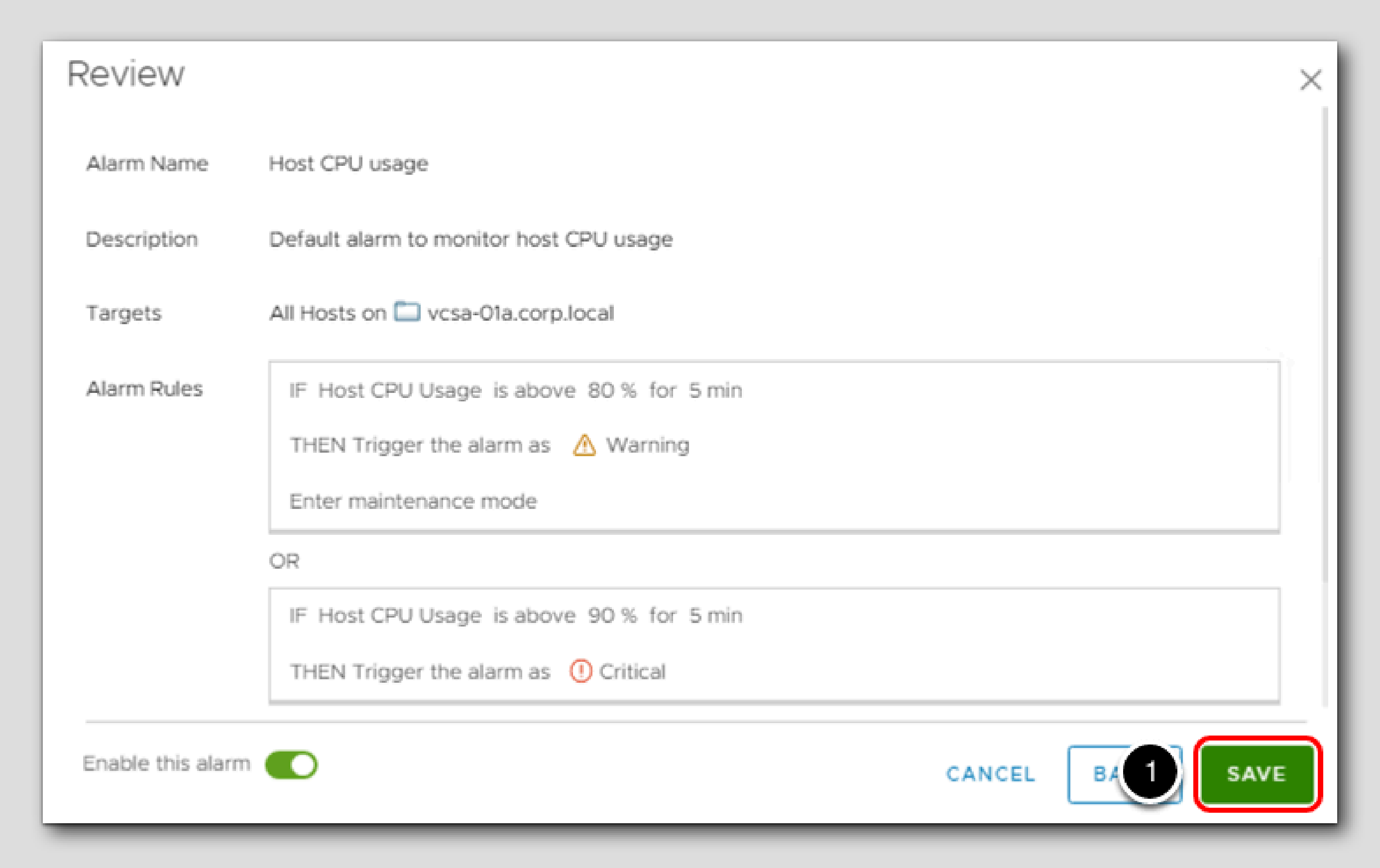
Run script

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

[152]



Review

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

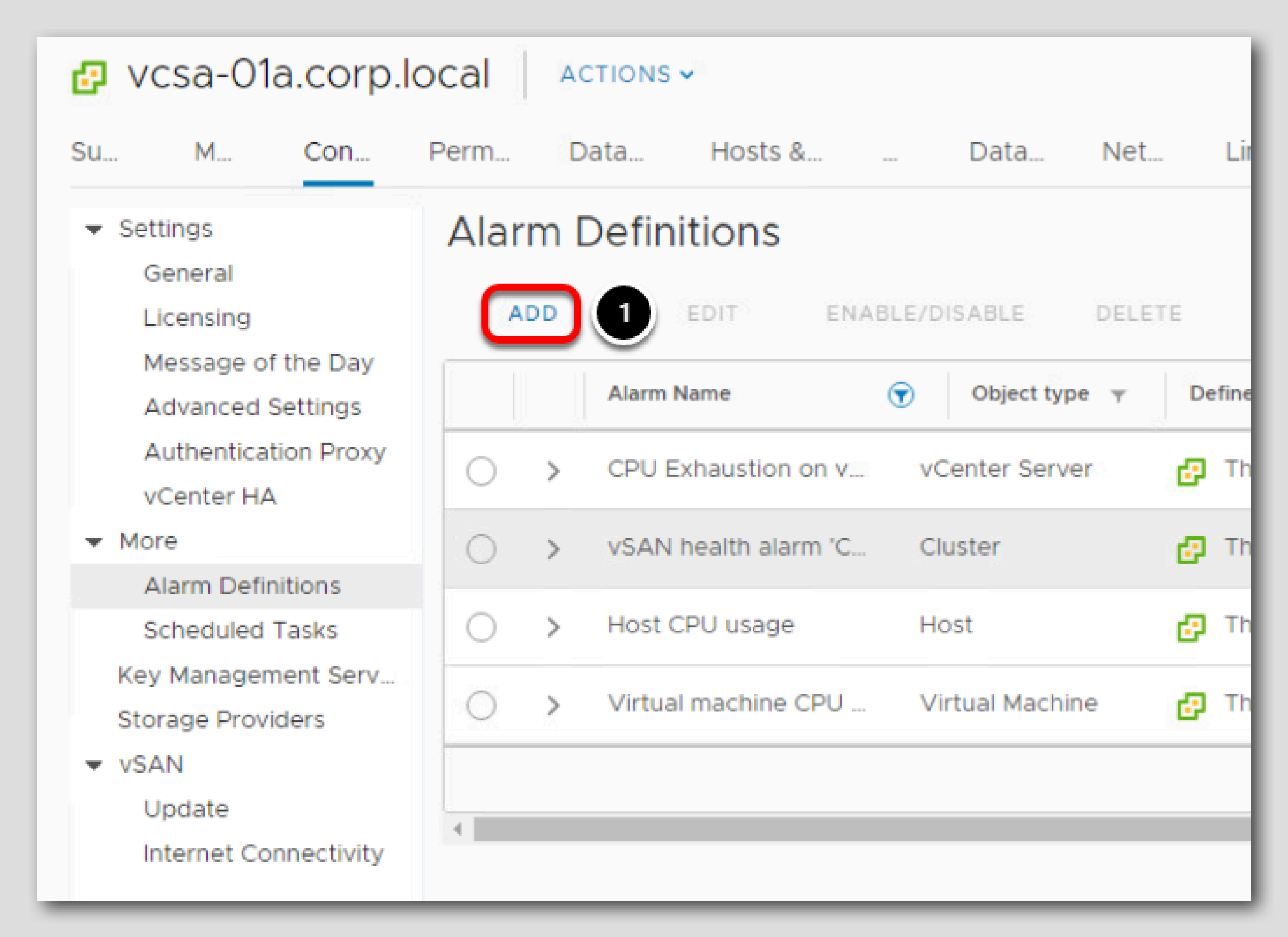
Enable this alarm

The Review screen shows what was configured.

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

Create New Alarm

[153]

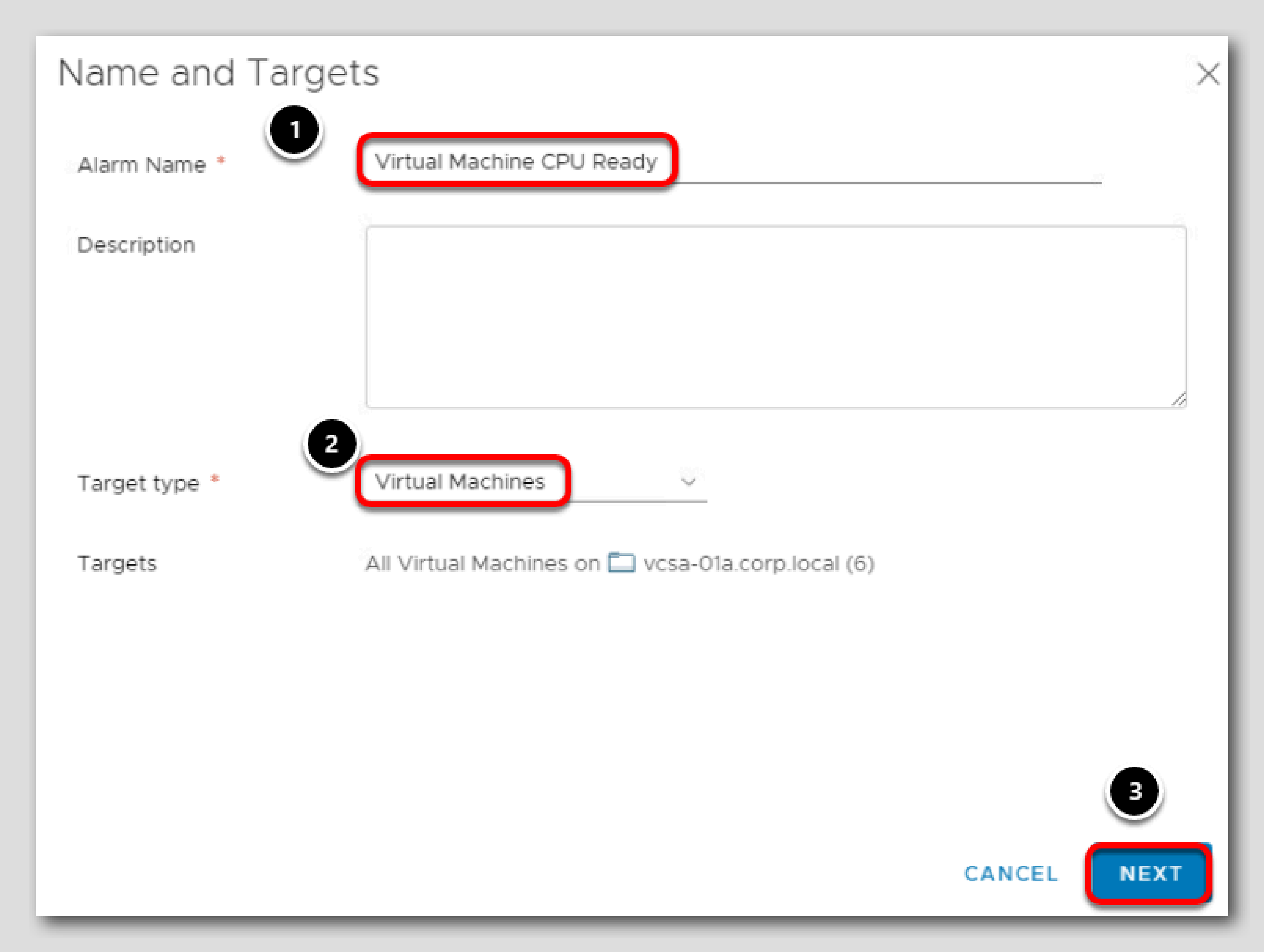


		Alarm Name	Object type	Define
○	›	CPU Exhaustion on v...	vCenter Server	Th
○	›	vSAN health alarm 'C...	Cluster	Th
○	›	Host CPU usage	Host	Th
○	›	Virtual machine CPU ...	Virtual Machine	Th

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

New Alarm Definition

[154]



Name and Targets

1

Alarm Name * Virtual Machine CPU Ready

Description

2

Target type * Virtual Machines

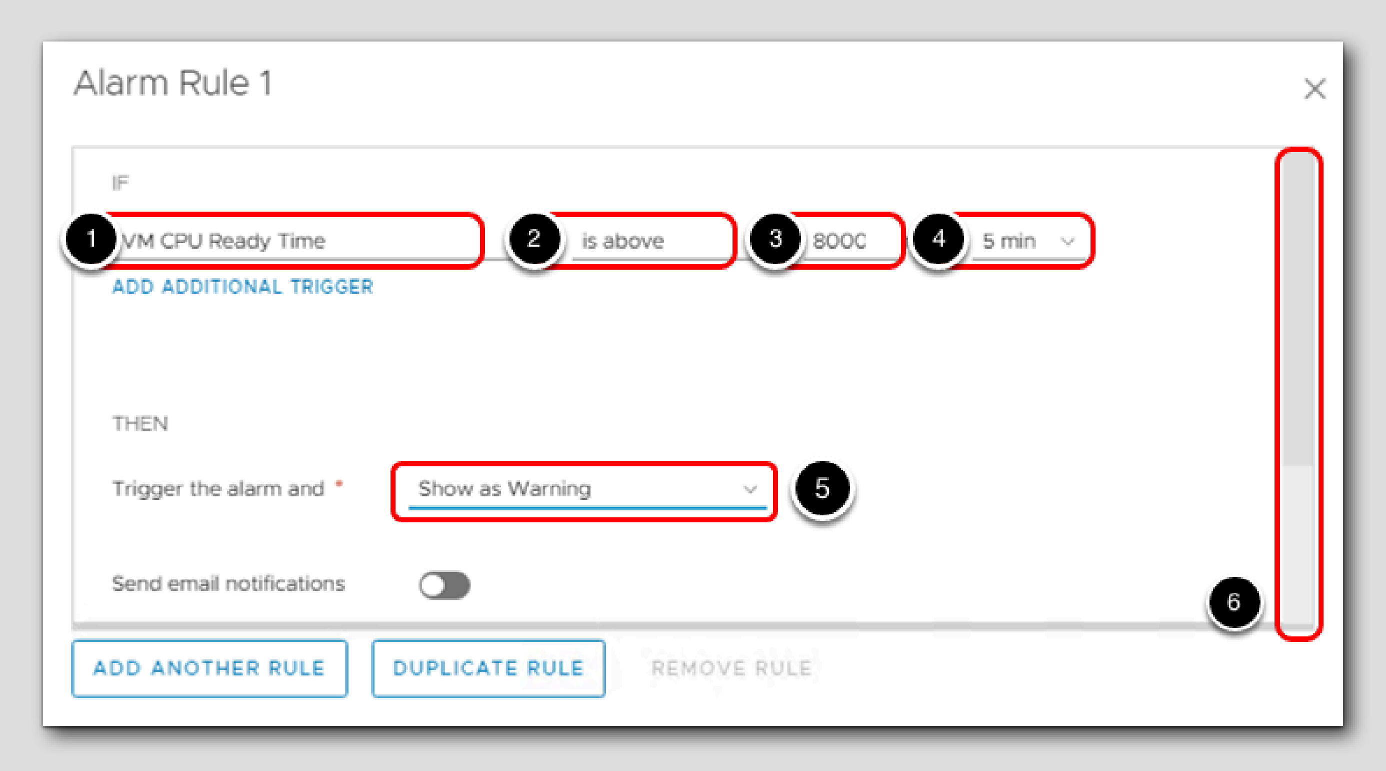
Targets All Virtual Machines on vcsa-01a.corp.local (6)

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

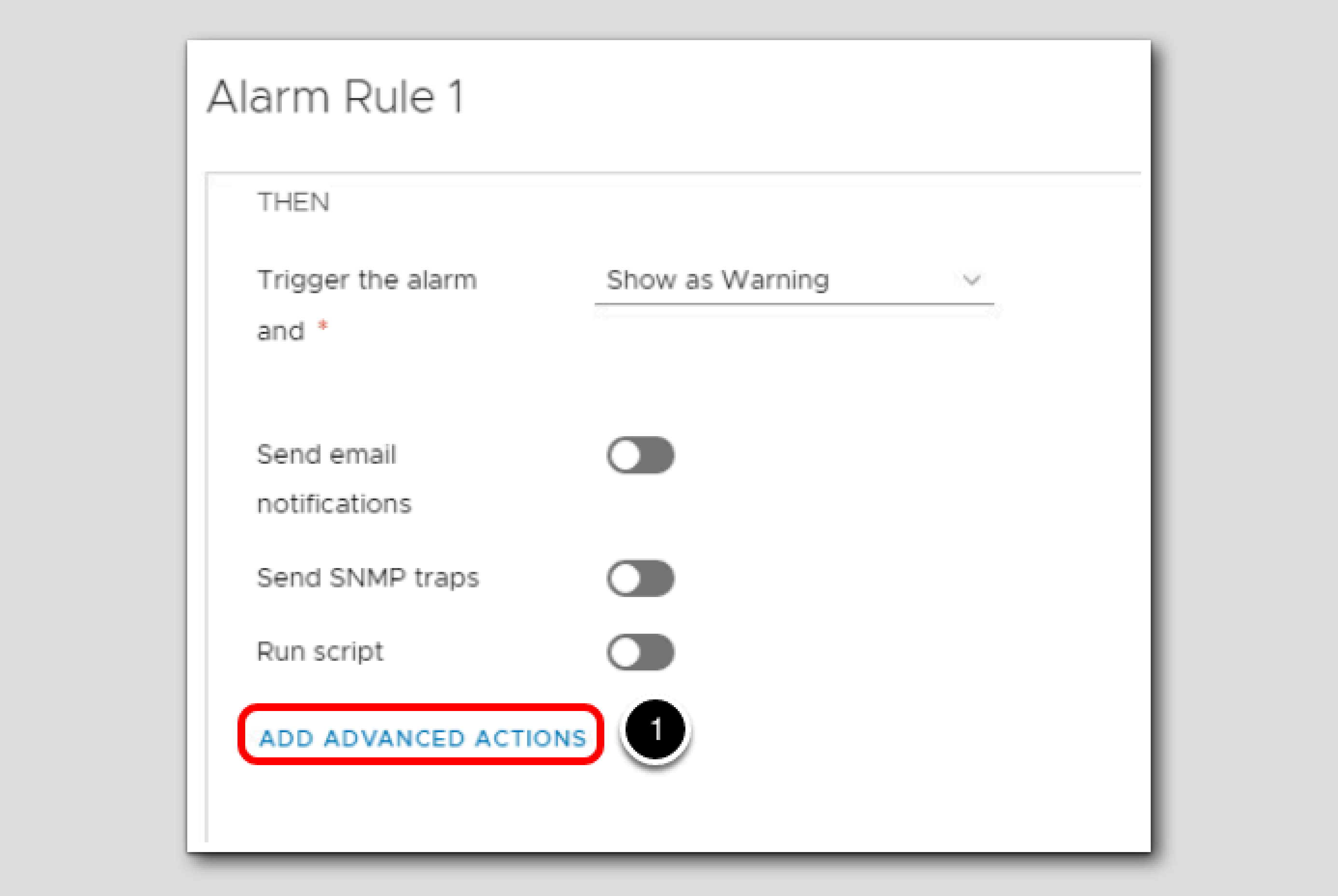
[155]



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

Add Advanced Action

[156]



Alarm Rule 1

THEN

Trigger the alarm and * Show as Warning

Send email notifications

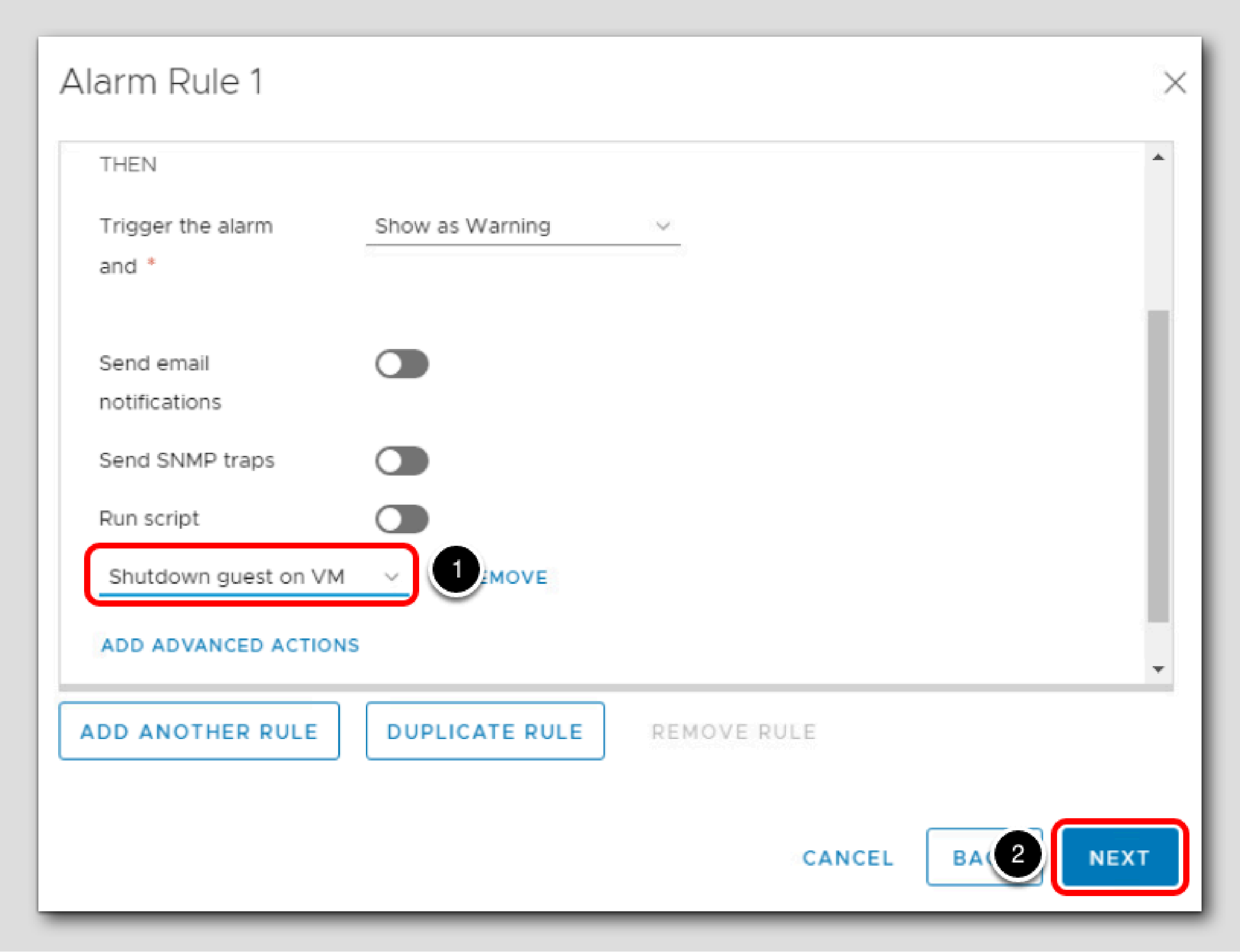
Send SNMP traps

Run script

1. Click Add Advanced Actions

Migrate VM

[157]



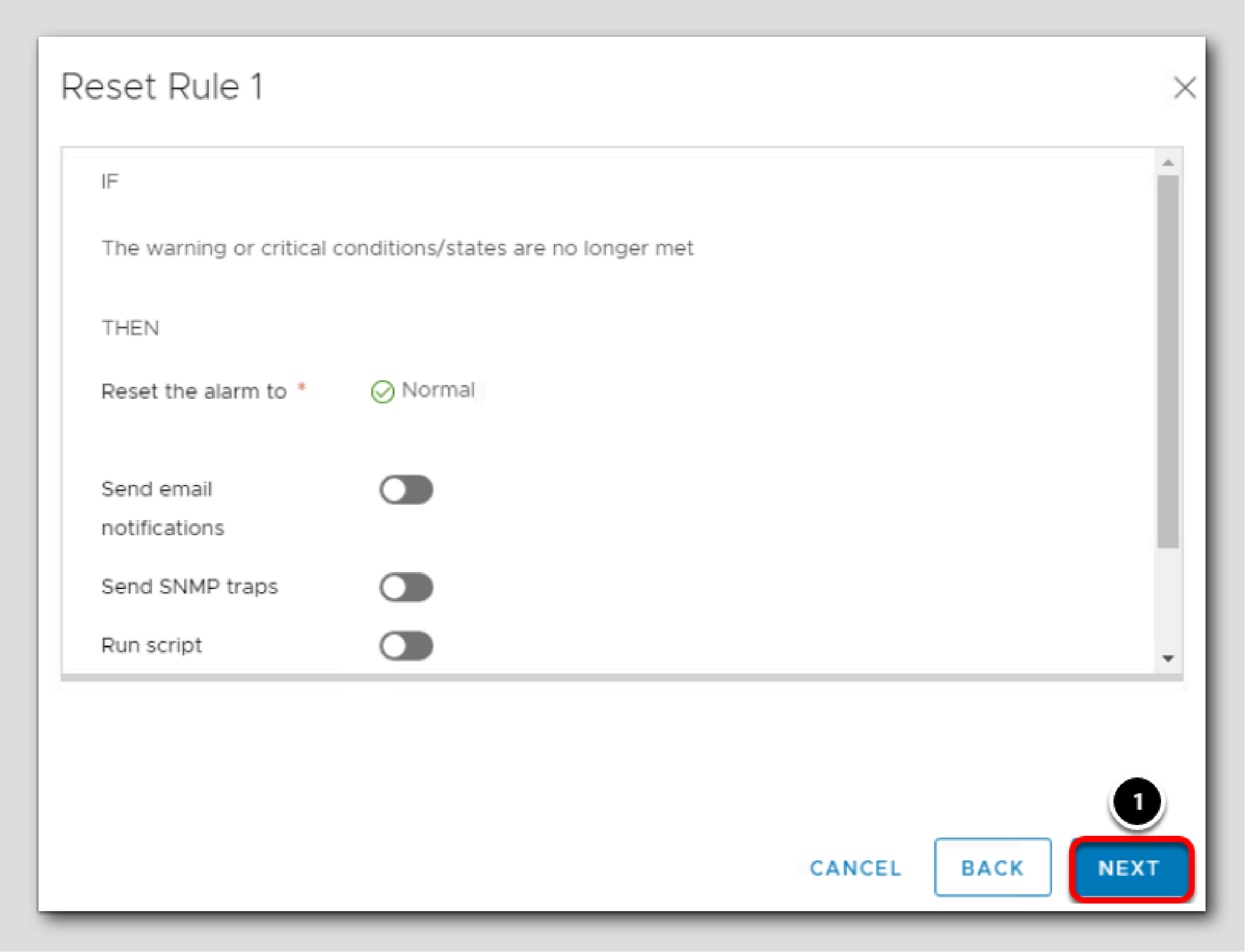
1. From the drop-down menu, select Shutdown guest on VM.

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

2. Click Next.

Reset Rule 1

[158]



Reset Rule 1

IF

The warning or critical conditions/states are no longer met

THEN

Reset the alarm to * ✓ Normal

Send email notifications ○

Send SNMP traps ○

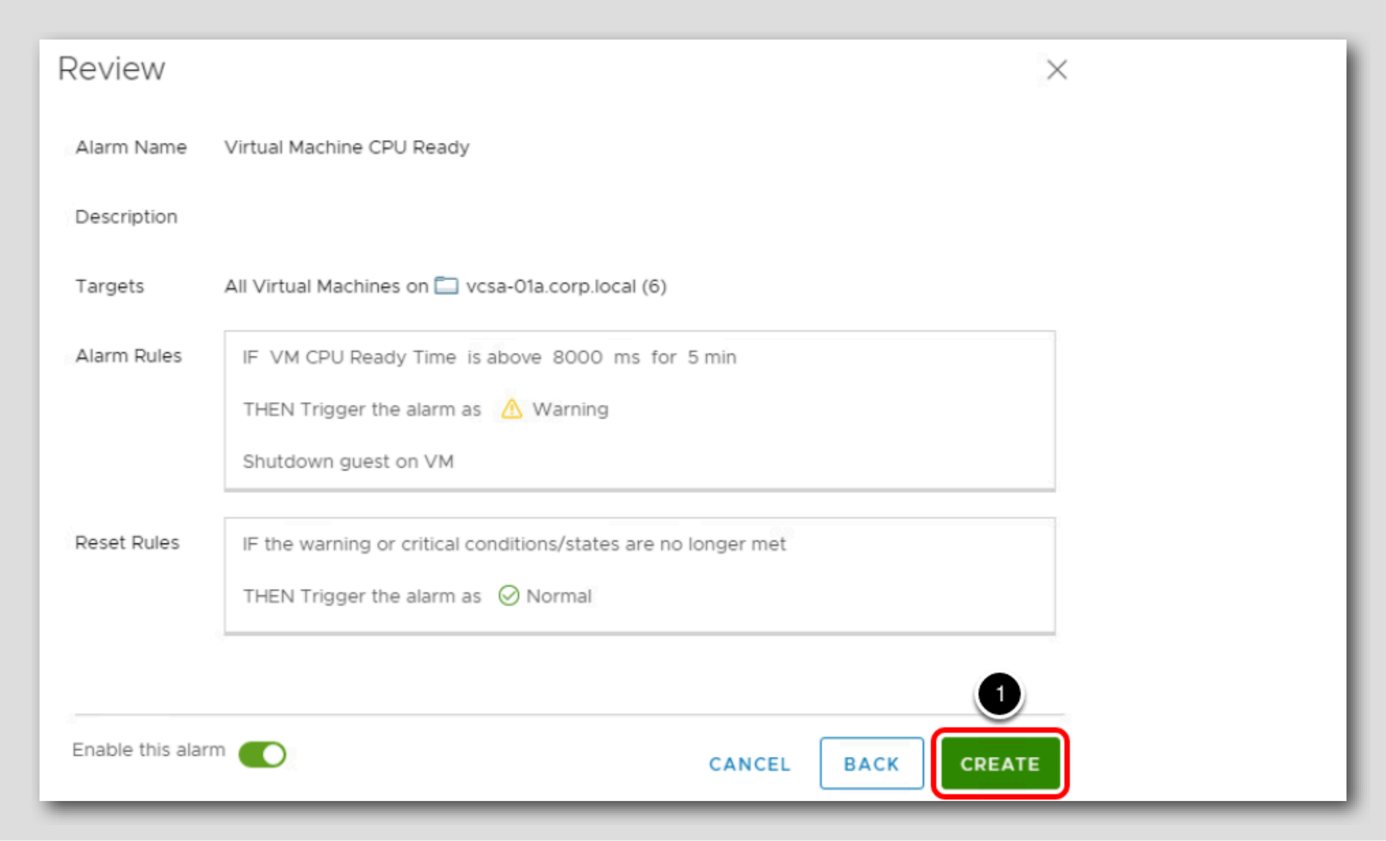
Run script ○

Additional options could be specified once the conditions are clear.

1. Click Next

Review

[159]



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

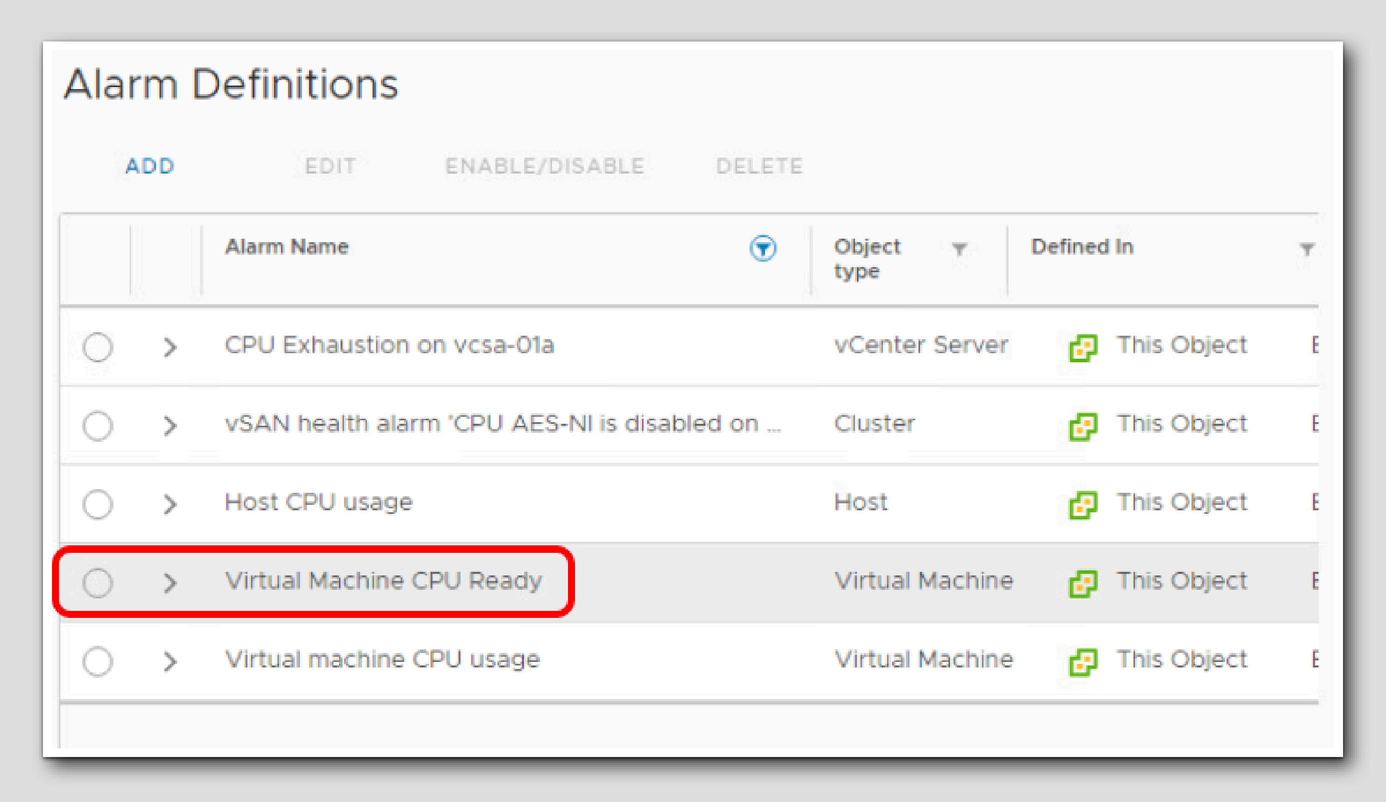
Enable this alarm ●

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

1. Click Create.

New Alarm Created

[160]



Alarm Definitions

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

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

Configure Shares and Resources

[161]

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

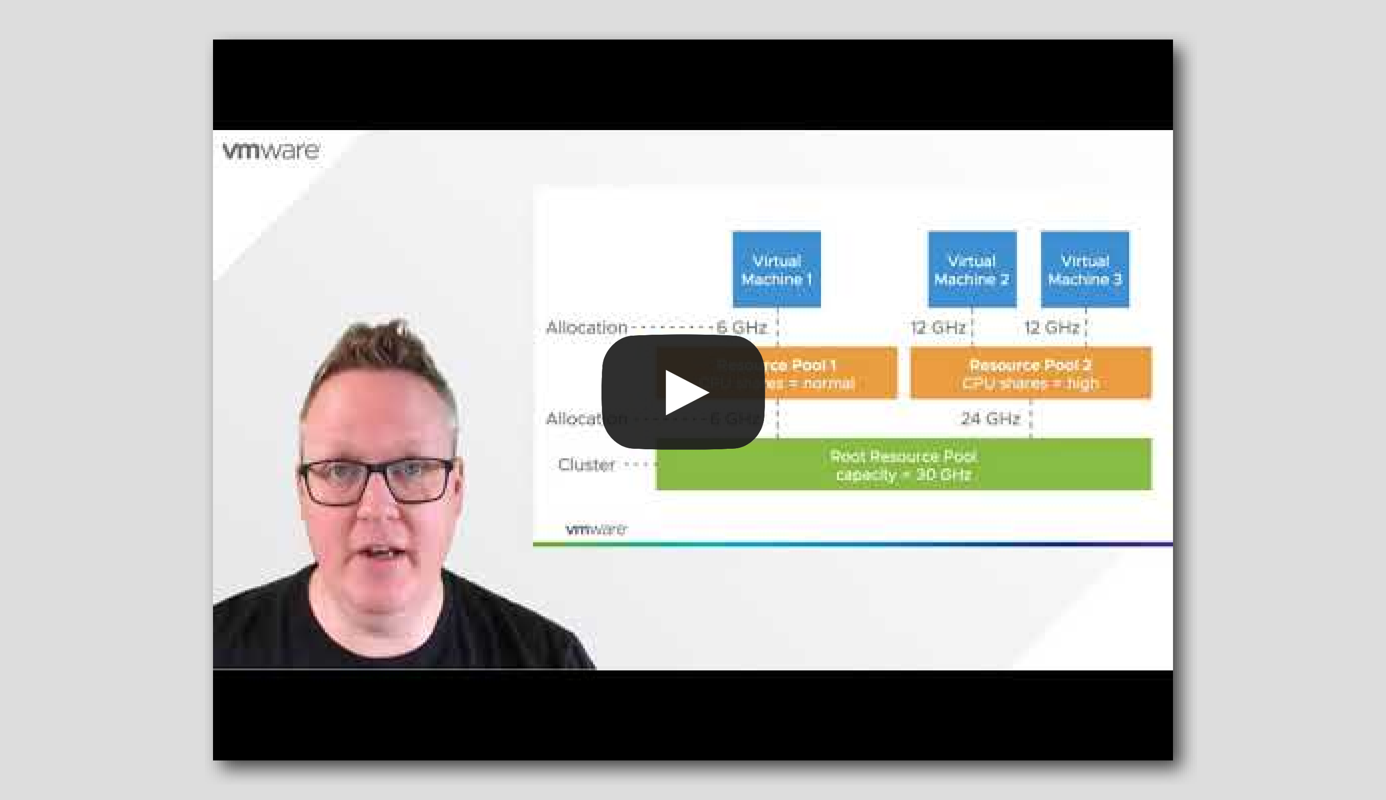
Shares are typically specified as High, Normal, or Low

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

[162]

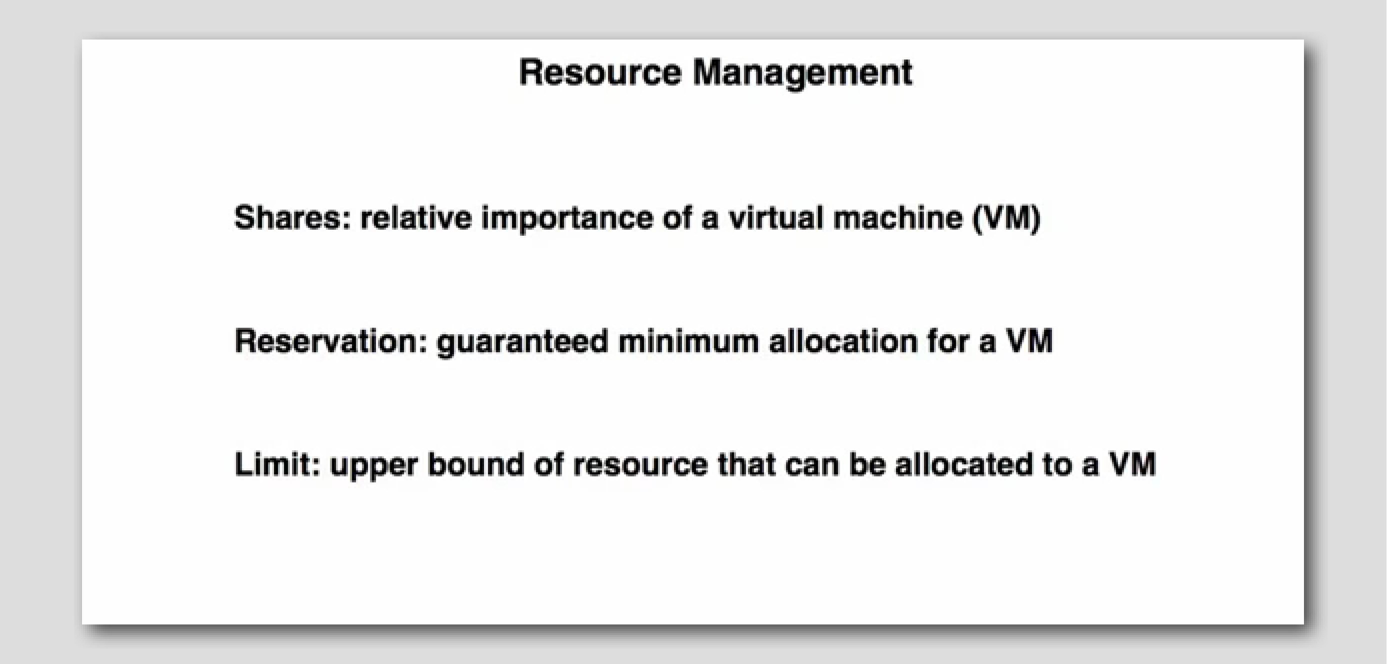
This video explains how scalable shares are and how are they used in order to effectively distribute compute and memory resources among virtual machines.

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



Shares, Limits and Reservations

[163]



Resource Management

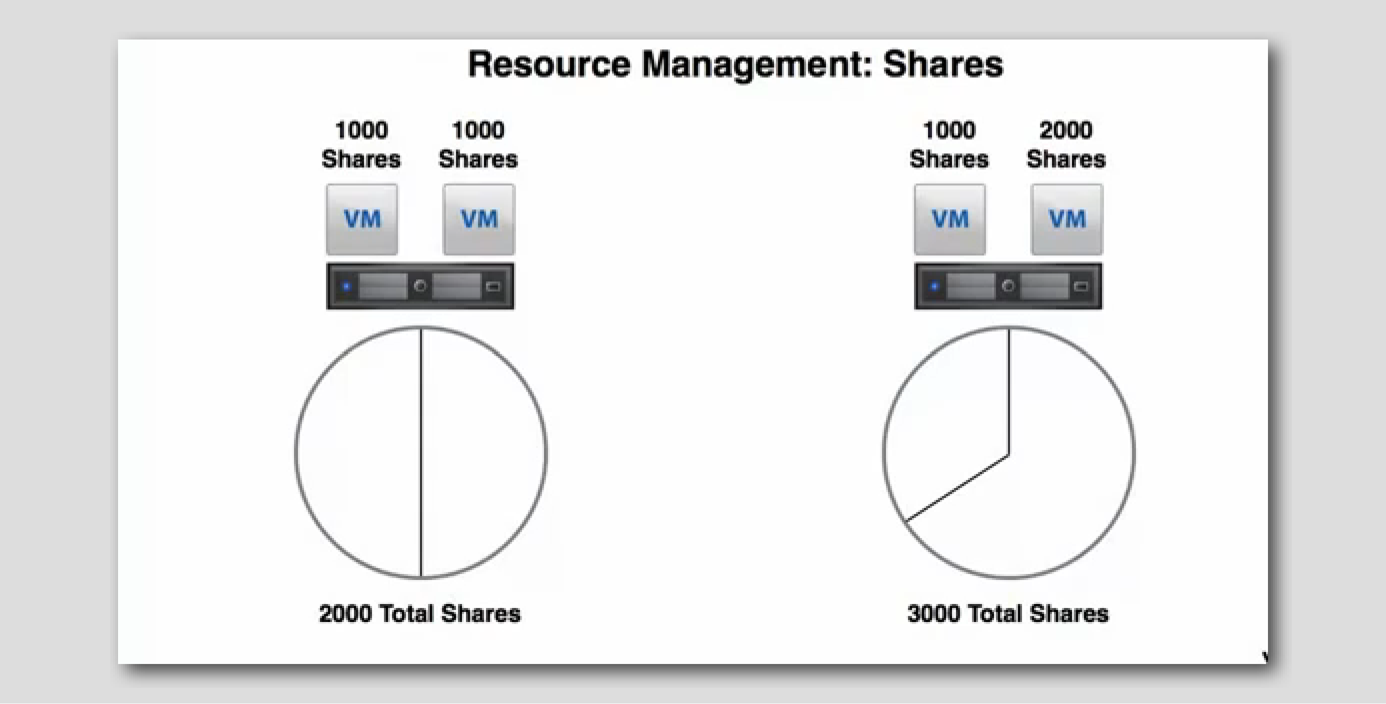
Shares: relative importance of a virtual machine (VM)

Reservation: guaranteed minimum allocation for a VM

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

Understanding Shares

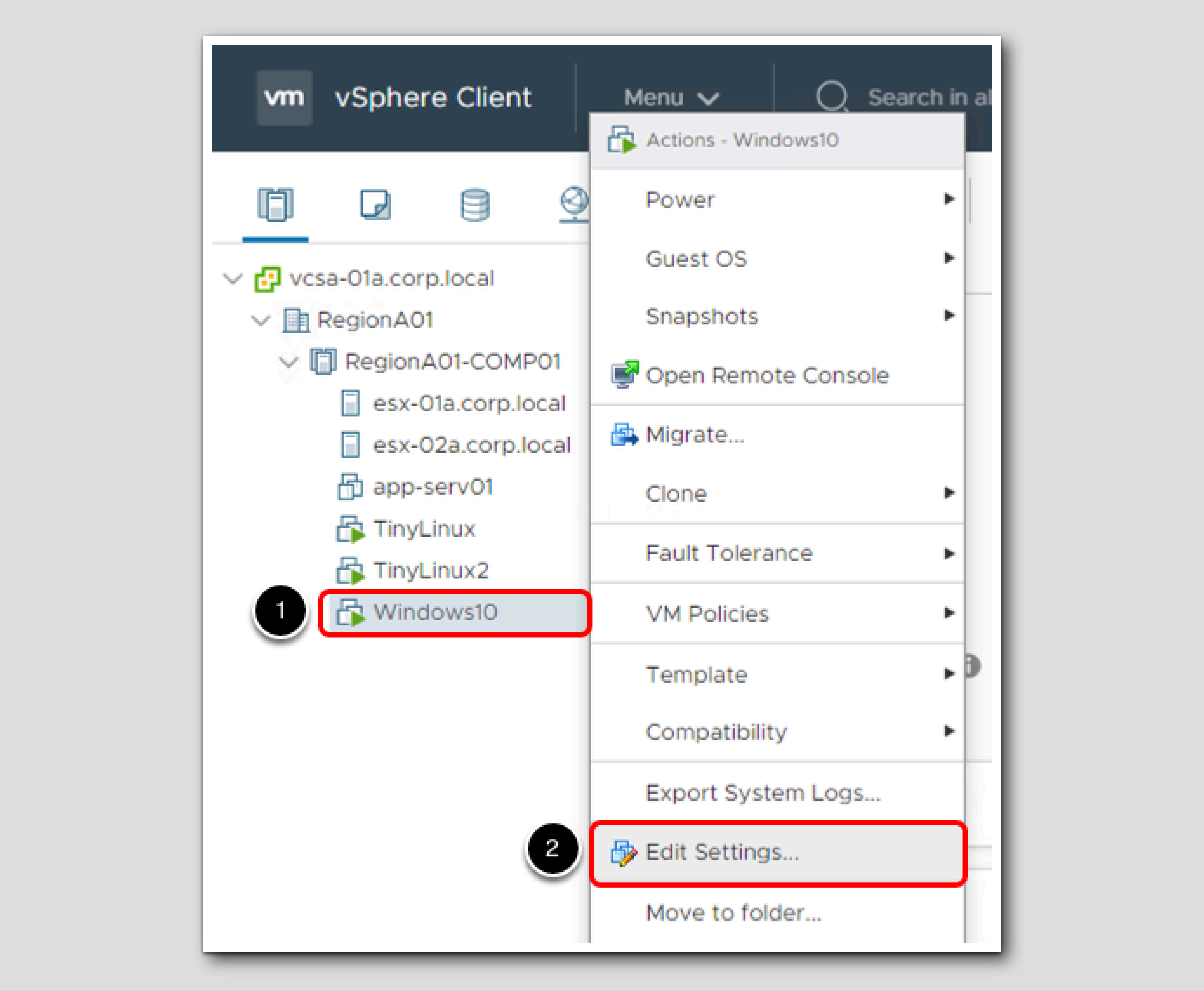
[164]



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

Review CPU settings

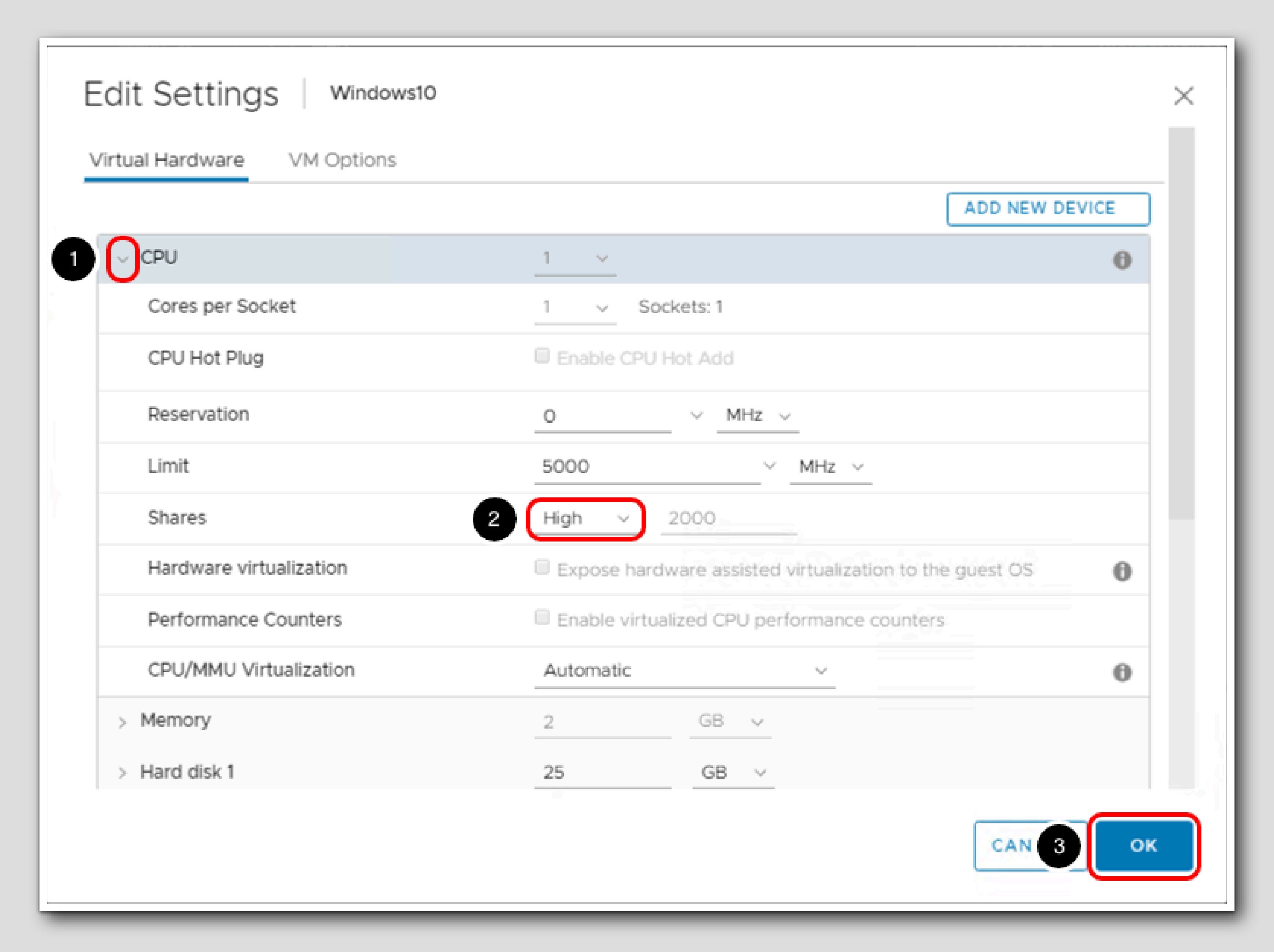
[165]



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

Changing Resource Allocation of CPU shares.

[166]



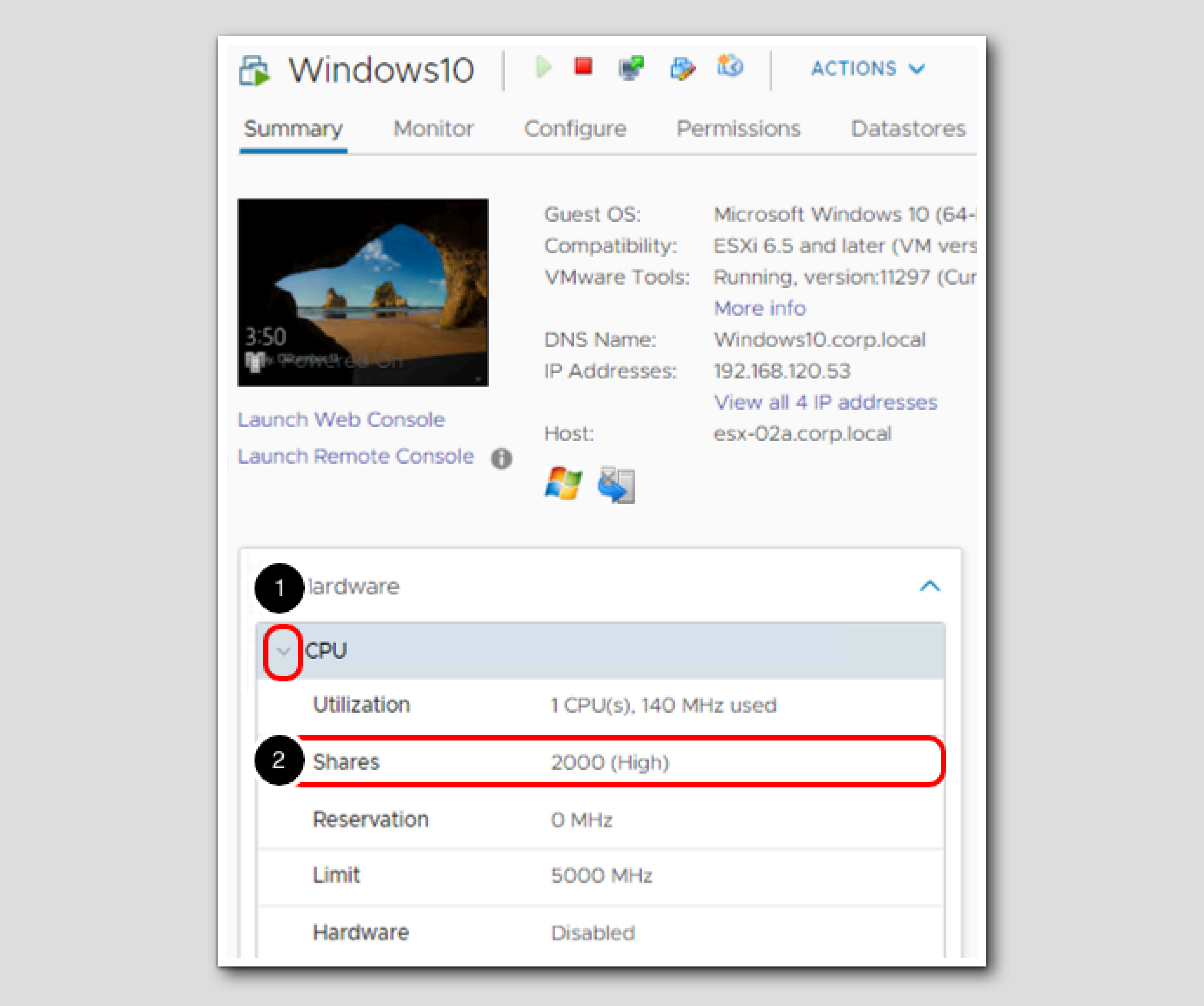
Edit Settings | Windows10

CPU	1	
Cores per Socket	1	Sockets: 1
CPU Hot Plug	□ Enable CPU Hot Add	
Reservation	0	MHz
Limit	5000	MHz
Shares	High	2000
Hardware virtualization	□ Expose hardware assisted virtualization to the guest OS	
Performance Counters	□ Enable virtualized CPU performance counters	
CPU/MMU Virtualization	Automatic	
Memory	2	GB
Hard disk 1	25	GB

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



Guest OS:	Microsoft Windows 10 (64-
Compatibility:	ESXi 6.5 and later (VM vers
VMware Tools:	Running, version:11297 (Cur More info
DNS Name:	Windows10.corp.local
IP Addresses:	192.168.120.53 View all 4 IP addresses
Host:	esx-02a.corp.local

lardware

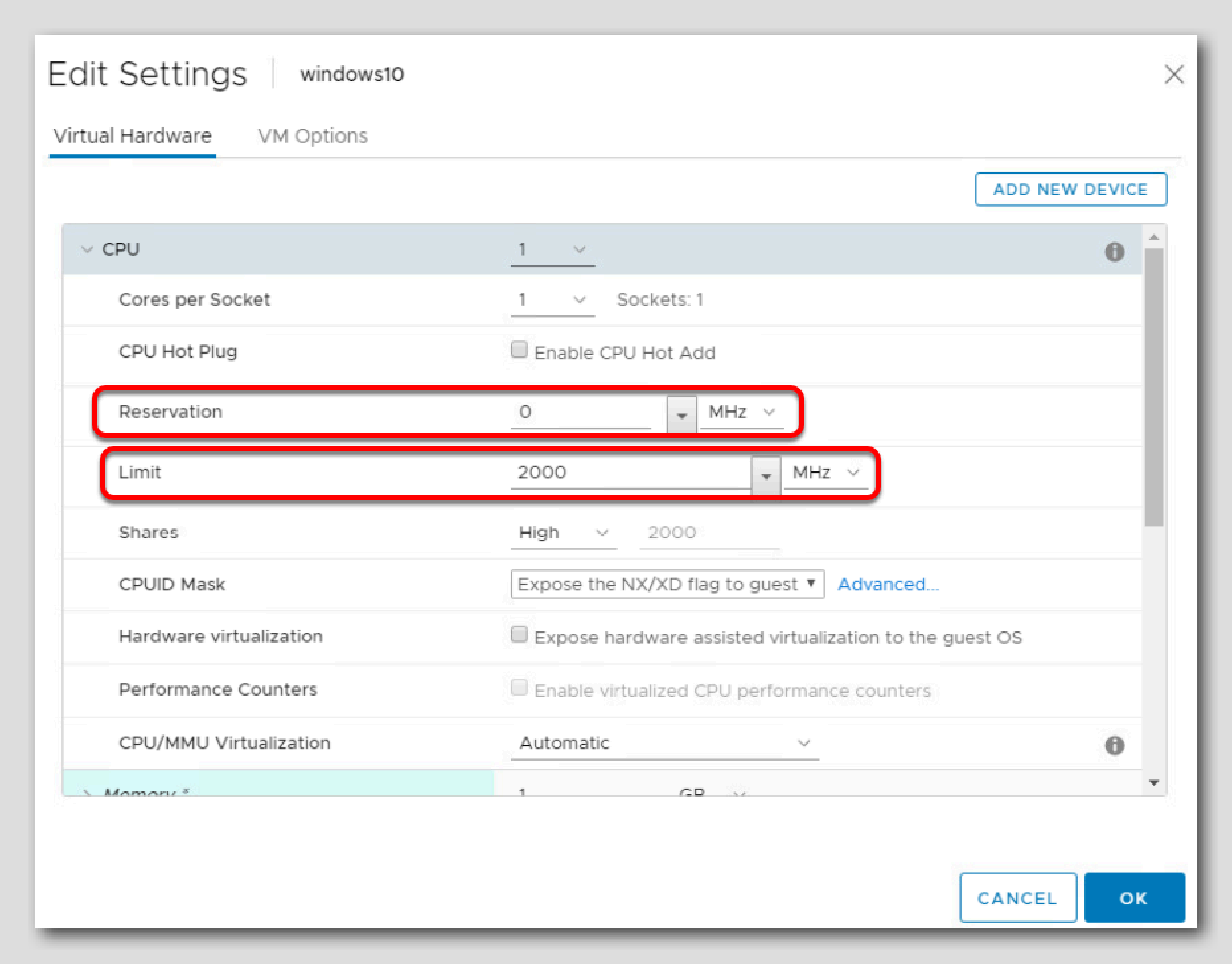
CPU

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

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

Settings for Limits and Reservations.

[168]



Edit Settings | windows10

CPU 1
Cores per Socket 1 Sockets: 1
CPU Hot Plug □ 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 □ Expose hardware assisted virtualization to the guest OS
Performance Counters □ Enable virtualized CPU performance counters
CPU/MMU Virtualization Automatic
Memory * 1 GB

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

[169]

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

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

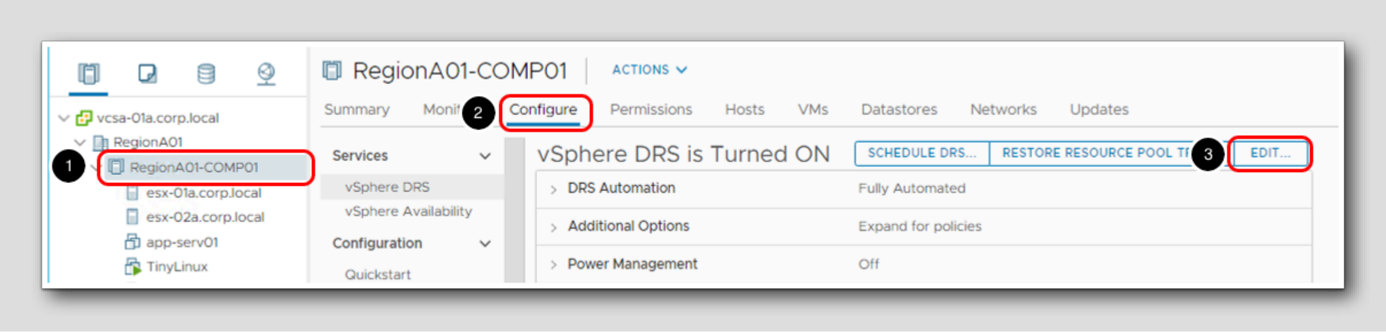
- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

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

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

Edit Cluster Settings

[170]



vSphere DRS is Turned ON

DRS Automation Fully Automated

Additional Options Expand for policies

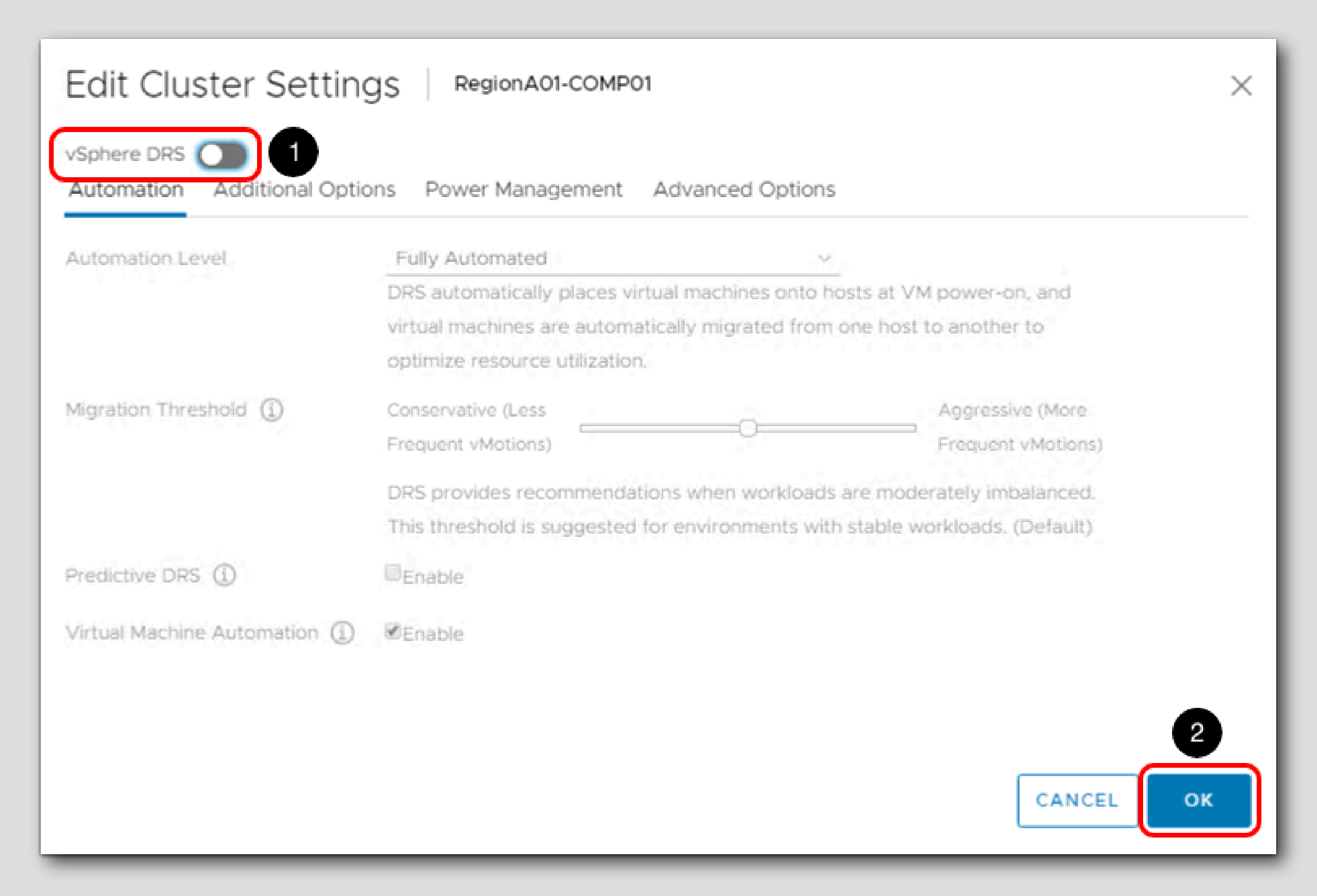
Power Management Off

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

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

Disable DRS

[171]



Edit Cluster Settings | RegionA01-COMP01

vSphere DRS

Automation Level: Fully Automated

DRS automatically places virtual machines onto hosts at VM power-on, and virtual machines are automatically migrated from one host to another to optimize resource utilization.

Migration Threshold: Conservative (Less Frequent vMotions) — Aggressive (More Frequent vMotions)

DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

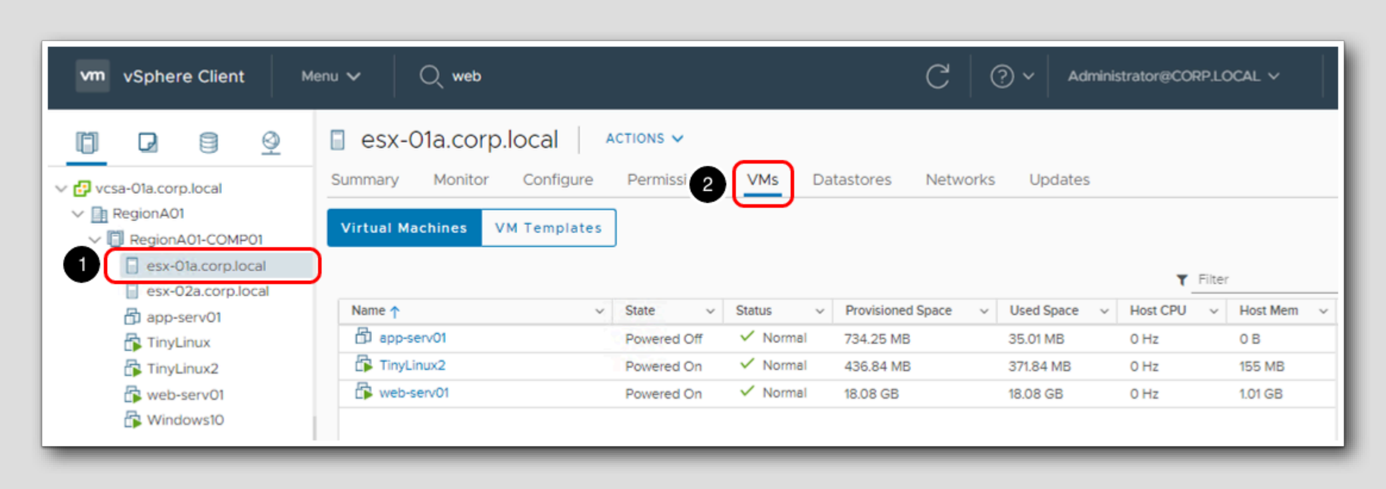
Predictive DRS: □ Enable

Virtual Machine Automation: ☑ Enable

1. Flip the switch to disable vSphere DRS.
2. Click OK

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

Migrating to esx-02a.corp.local



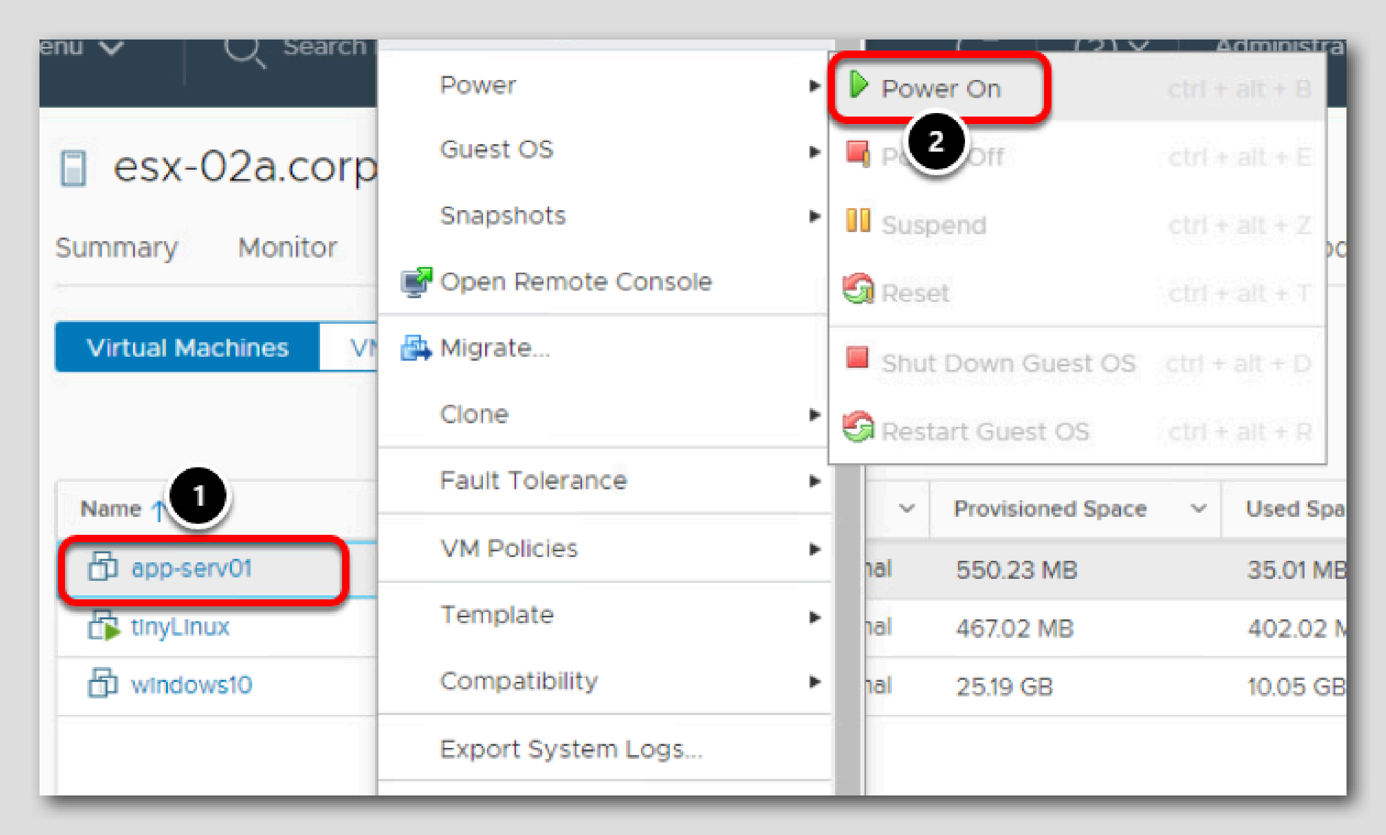
Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
app-serv01	Powered Off	✓ Normal	734.25 MB	35.01 MB	0 Hz	0 B
TinyLinux2	Powered On	✓ Normal	436.84 MB	371.84 MB	0 Hz	155 MB
web-serv01	Powered On	✓ Normal	18.08 GB	18.08 GB	0 Hz	1.01 GB

1. Select **esx-01a.corp.local**
2. Click the **VMs** tab

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

Power on VMs

[173]

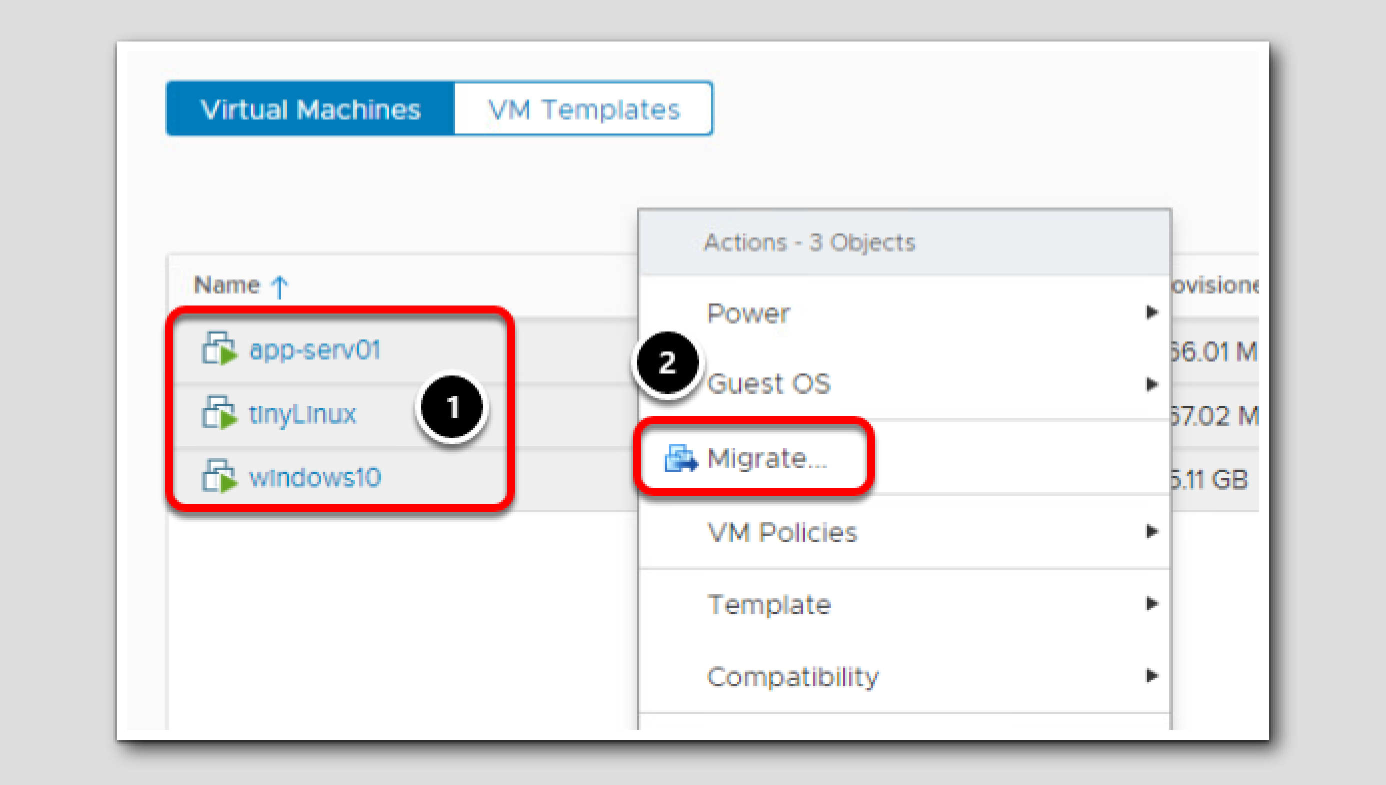


1. Look for any virtual machines that are Powered Off and select them. Multiple virtual machines can be selected by holding the Ctrl key and clicking on them.
2. Right click and select Power/Power On

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

Migrate VMs

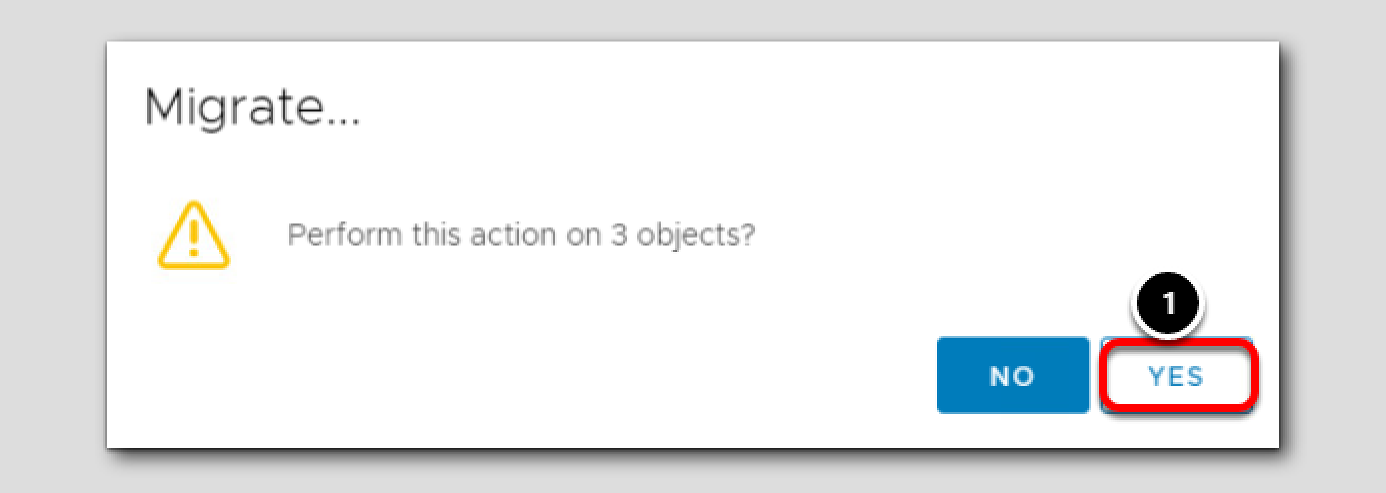
[174]



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

[175]



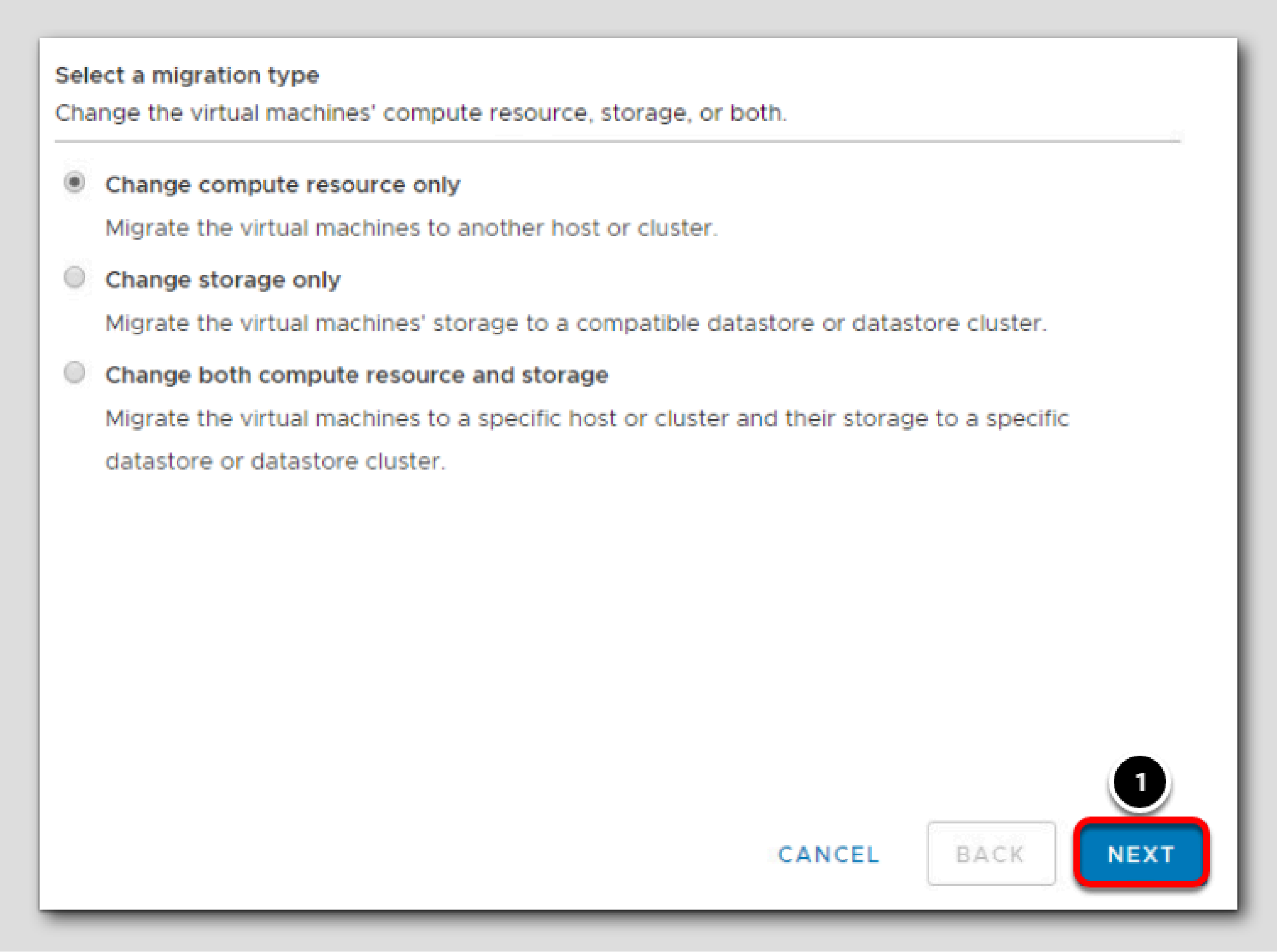
Migrate...

Perform this action on 3 objects?

Click Yes to start the migration process.

Migration Type

[176]



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.

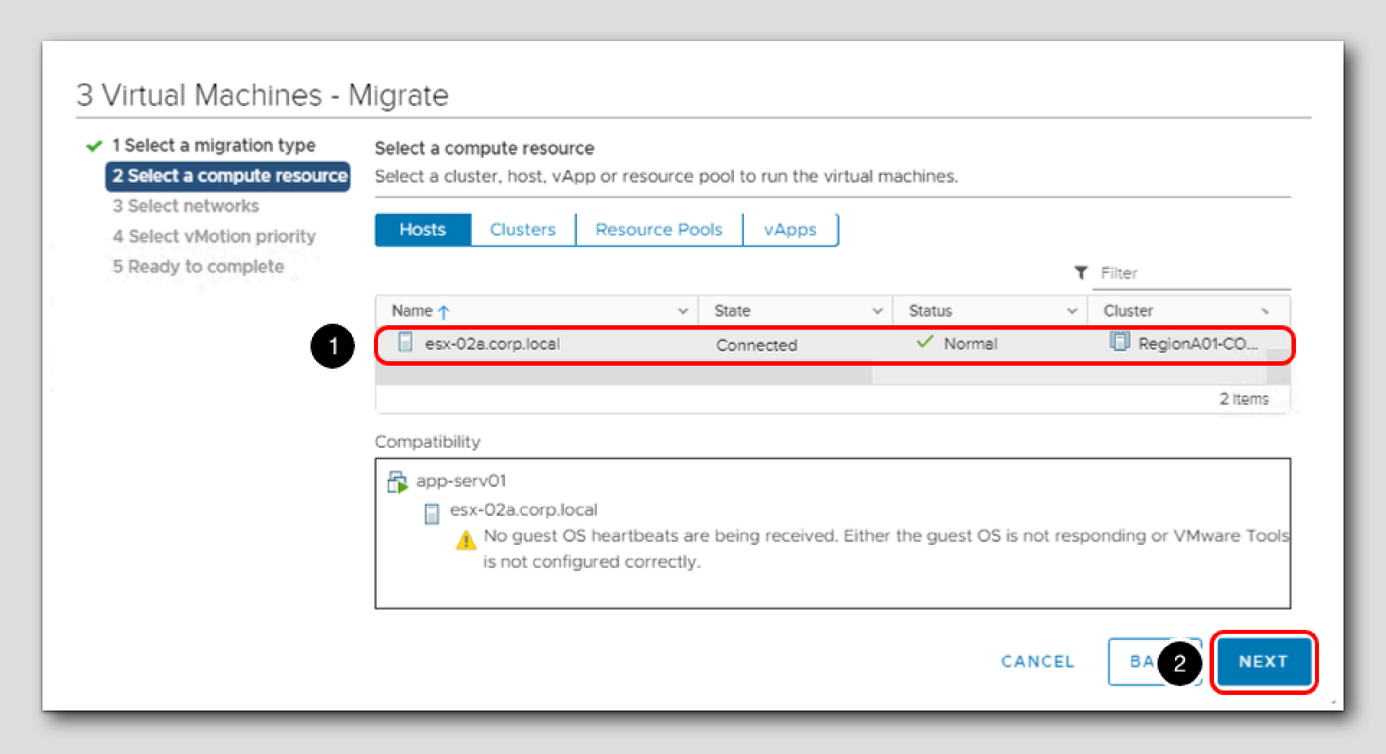
○ **Change both compute resource and storage**

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

1. Leave the default setting and click Next

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

Compute Resource



3 Virtual Machines - Migrate

Select a compute resource

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

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

2 items

Compatibility

app-serv01

esx-02a.corp.local

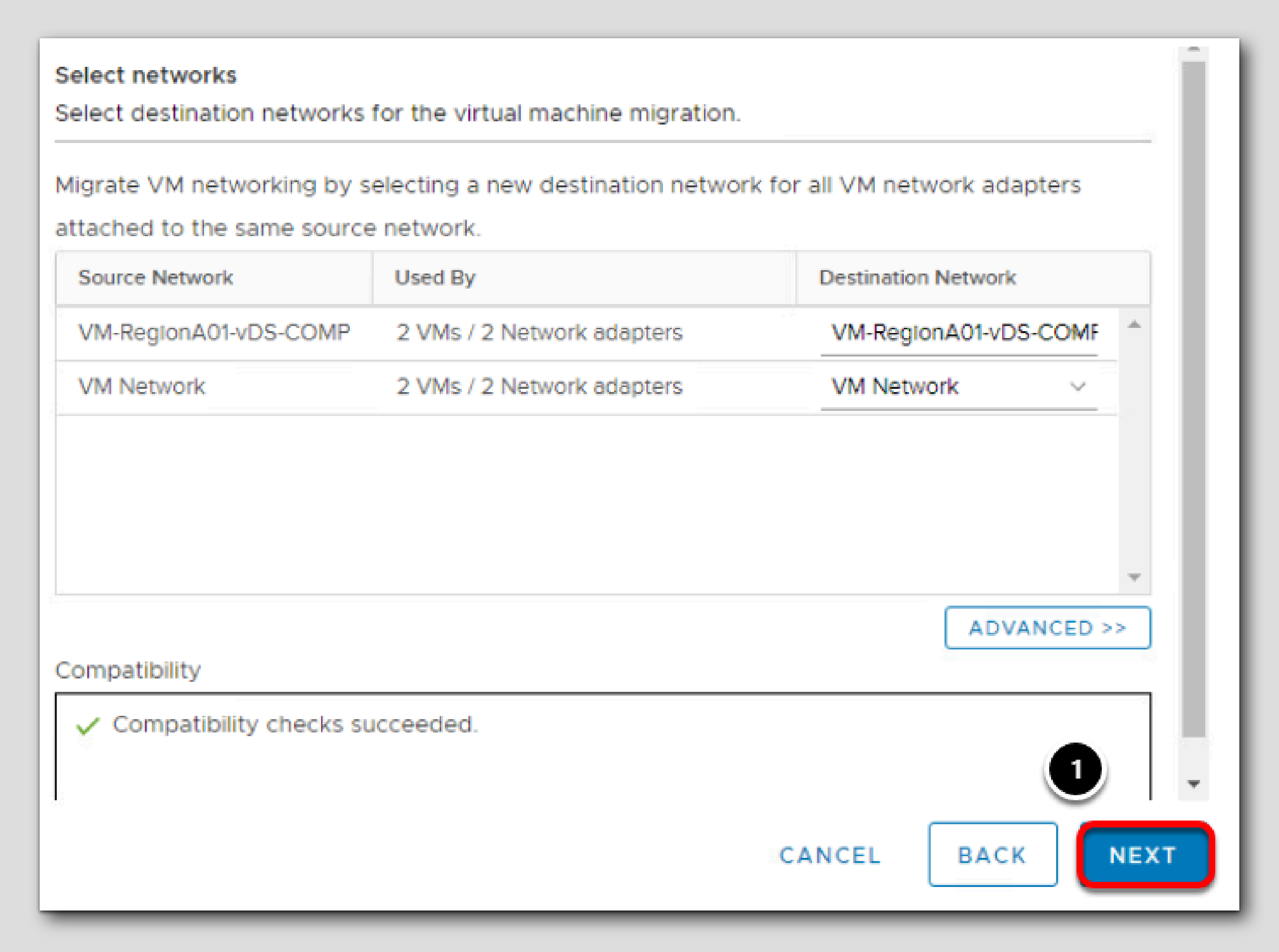
No guest OS heartbeats are being received. Either the guest OS is not responding or VMware Tools is not configured correctly.

1. Select esx-02a.corp.local
2. Click Next

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

Networks

[178]



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-COMF
VM Network	2 VMs / 2 Network adapters	VM Network

Compatibility

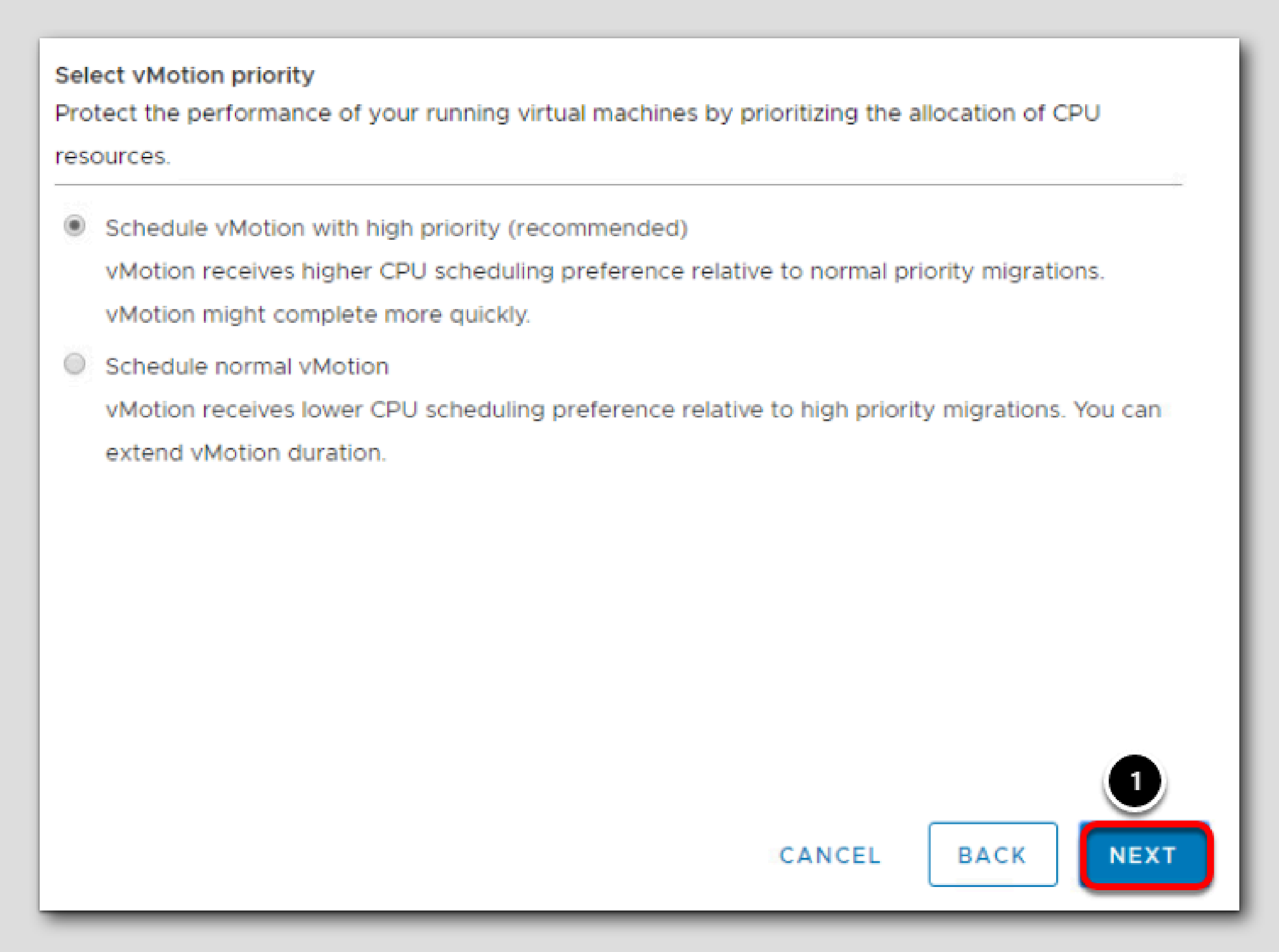
✓ Compatibility checks succeeded.

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

1. Click Next

vMotion Priority

[179]



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.

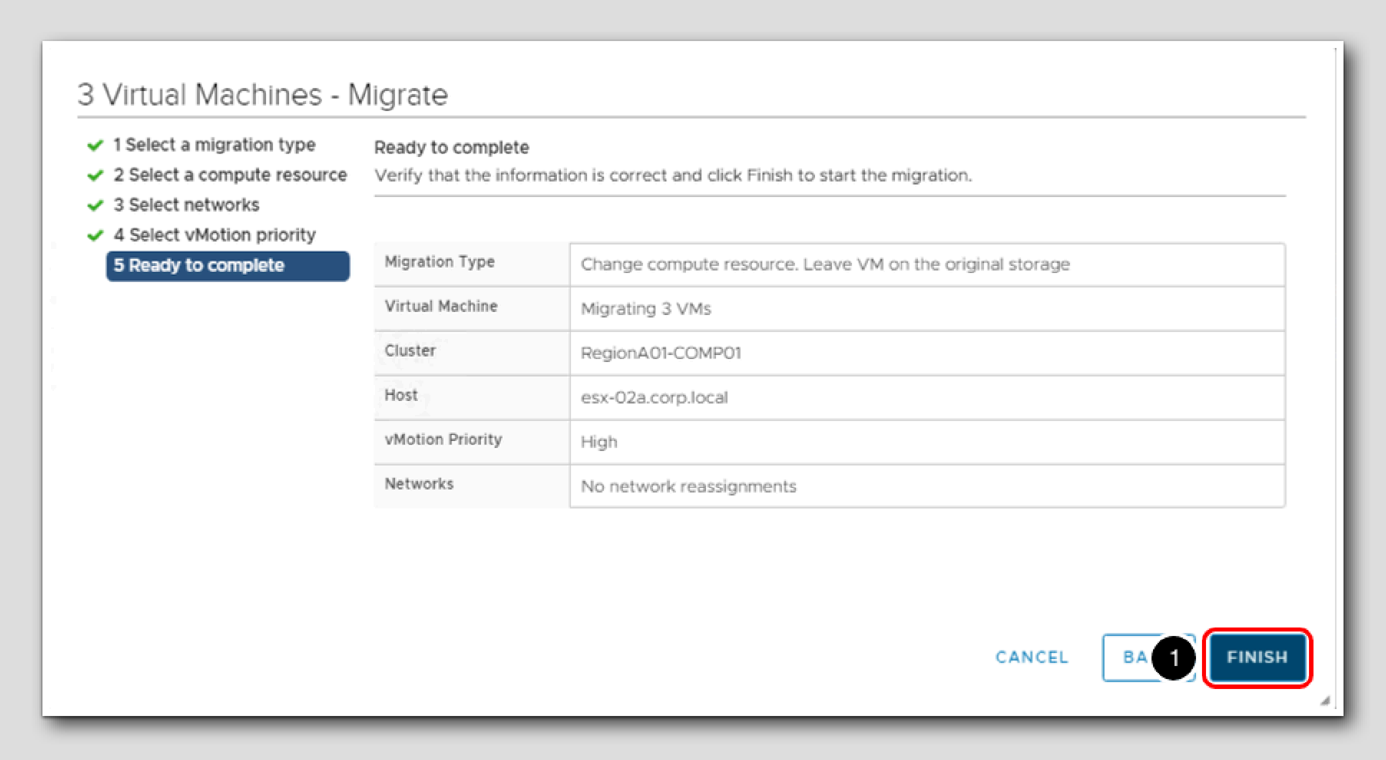
○ Schedule normal vMotion
vMotion receives lower CPU scheduling preference relative to high priority migrations. You can extend vMotion duration.

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

[180]



3 Virtual Machines - Migrate

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

Ready to complete

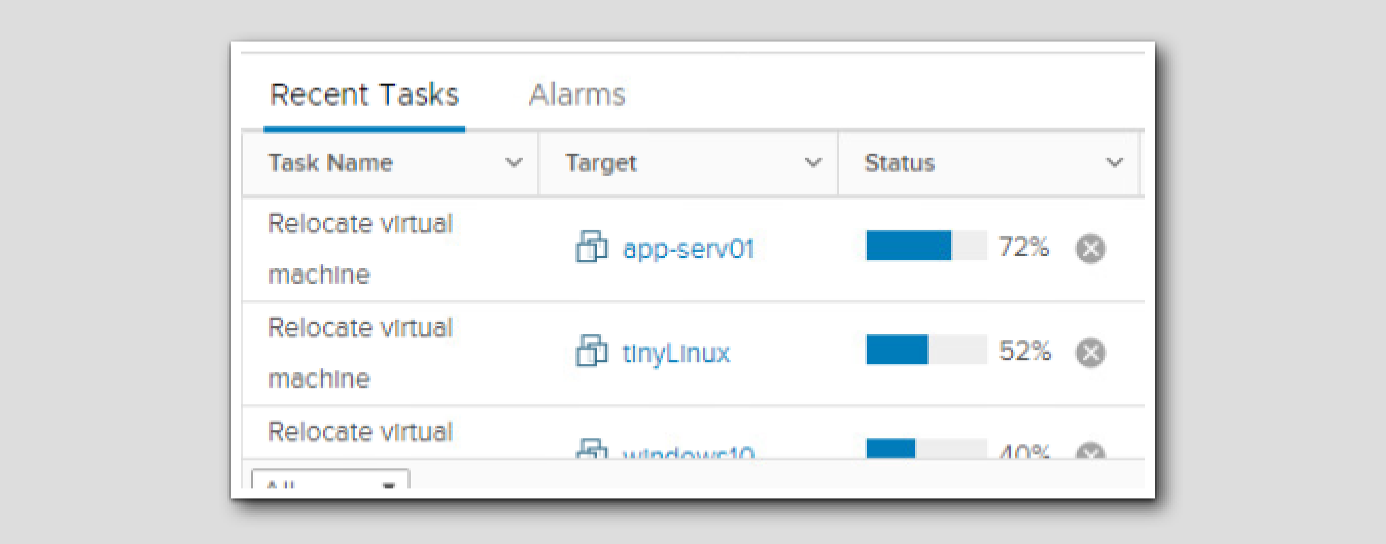
Verify that the information is correct and click Finish to start the migration.

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

Review the settings and click Finish to migrate the virtual machines to esx-02a.corp.local.

Monitor Progress

[181]

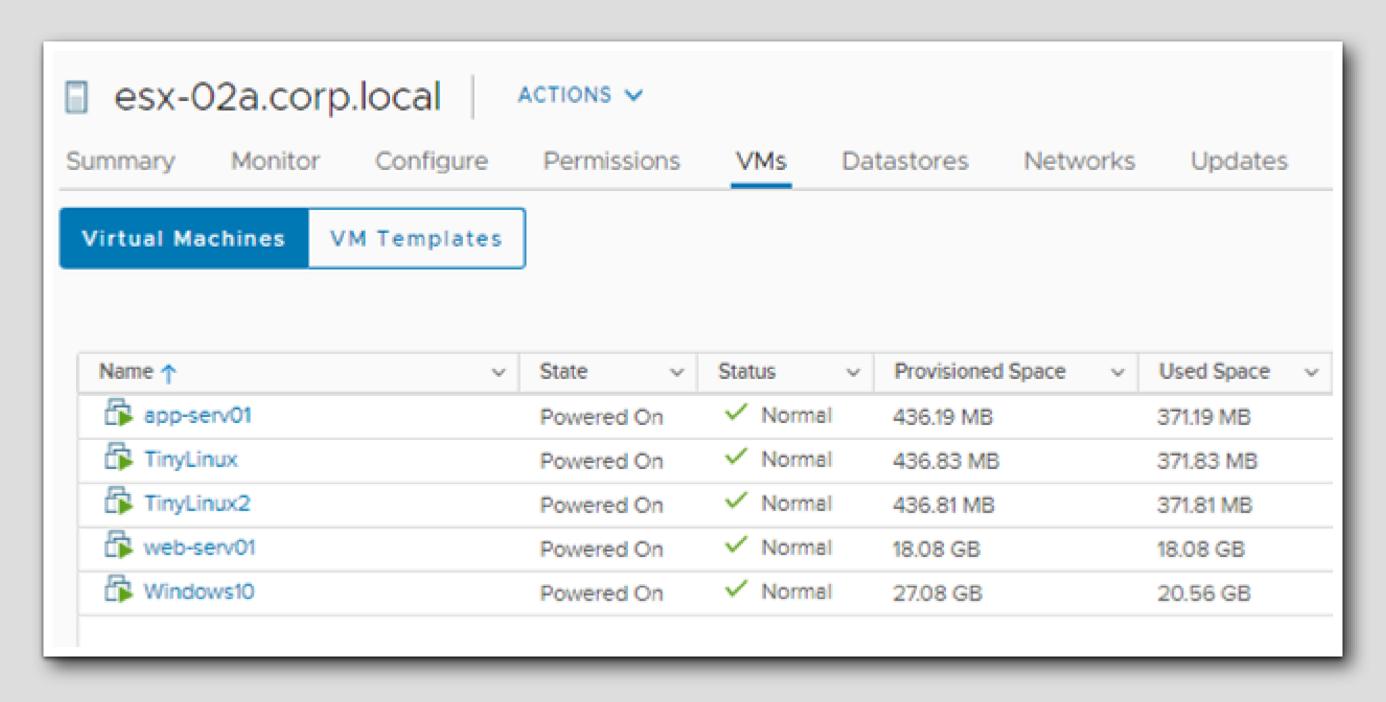


Task Name	Target	Status
Relocate virtual machine	app-serv01	72%
Relocate virtual machine	tinyLinux	52%
Relocate virtual	windows10	40%

You can monitor progress using Recent Tasks.

Migration Complete

[182]



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

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

vSphere Monitoring and Performance

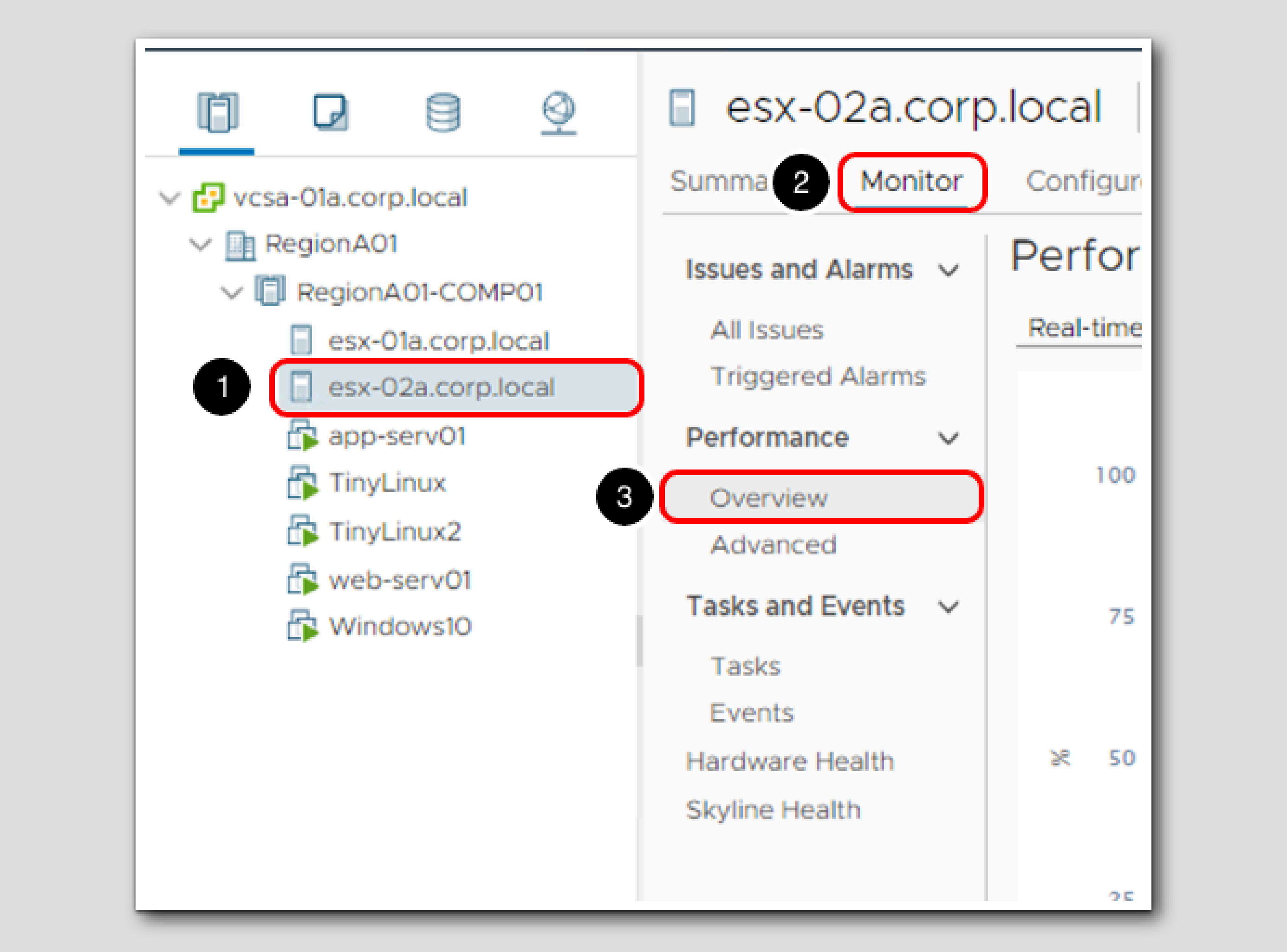
[183]

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

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

Select esx-02a

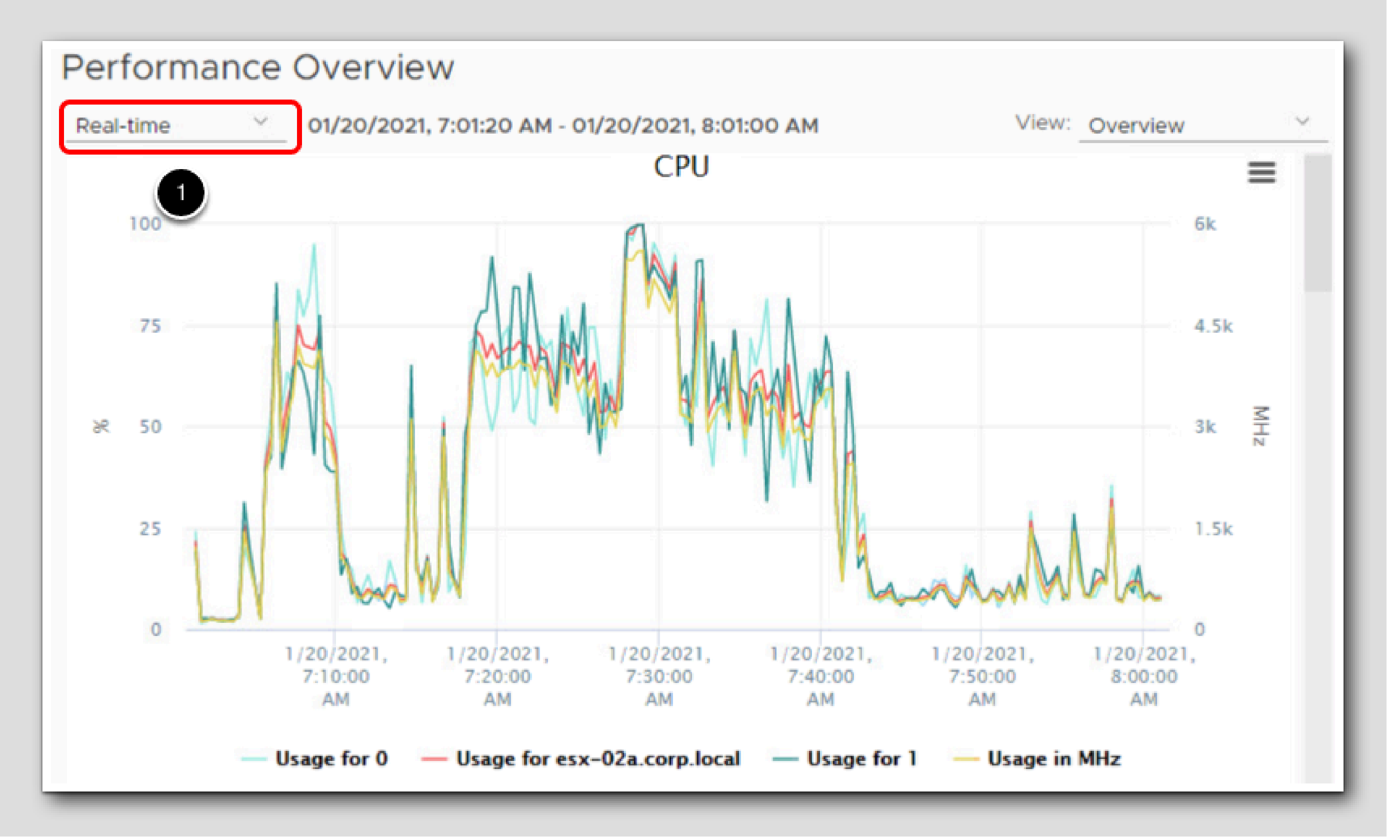
[184]



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

Host CPU Usage

[185]



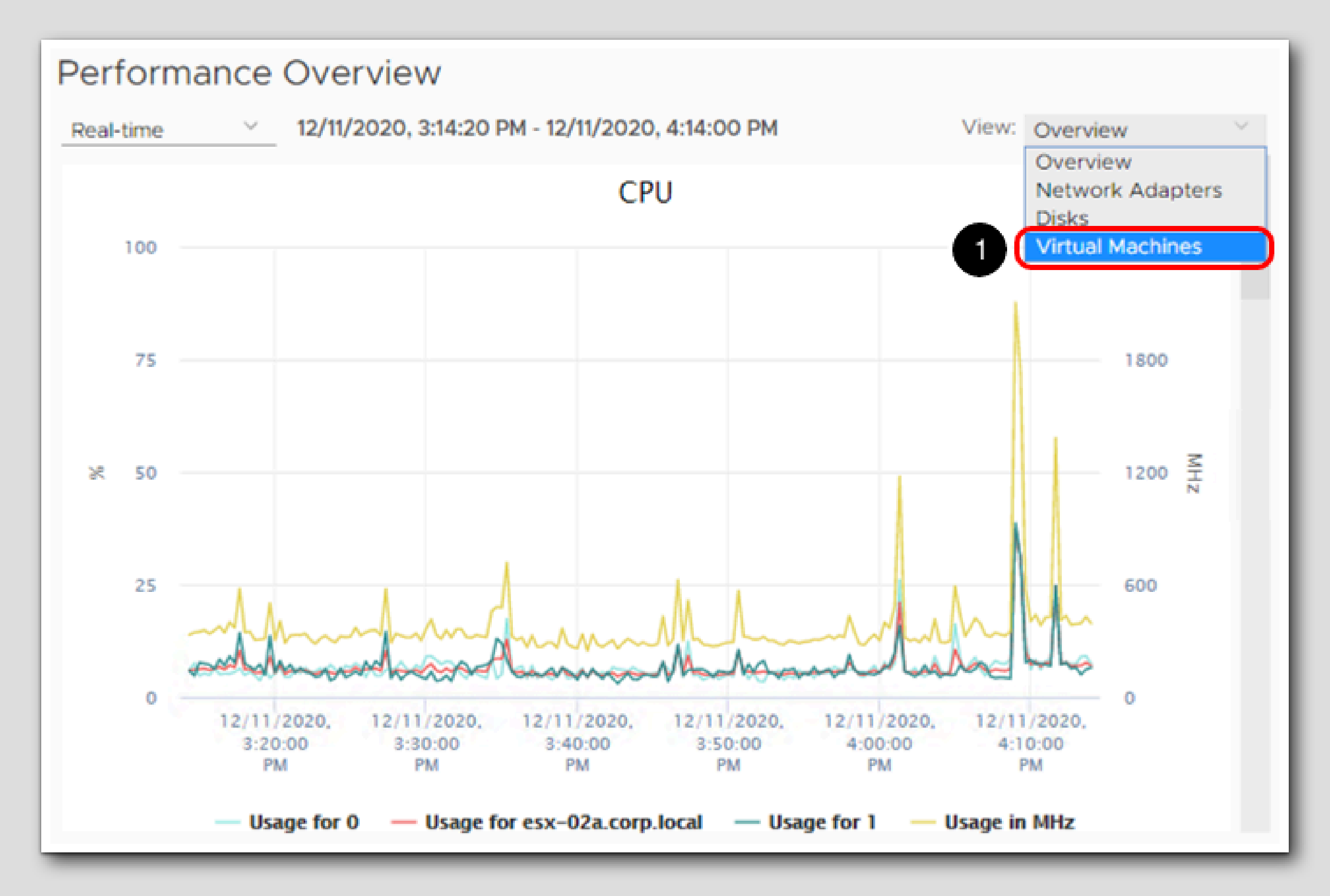
Performance Overview

Real-time 01/20/2021, 7:01:20 AM - 01/20/2021, 8:01:00 AM View: Overview

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

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

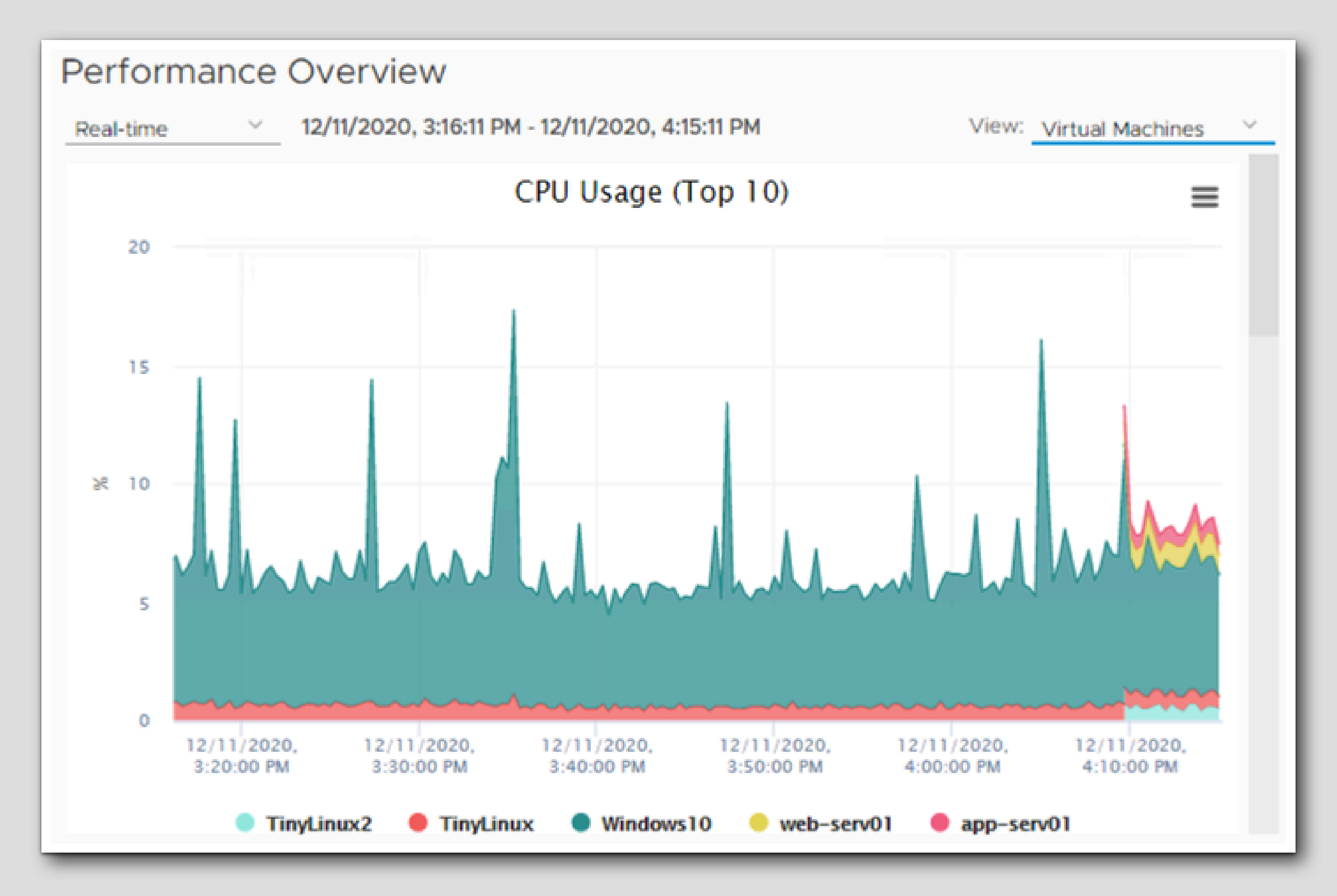
Virtual Machine CPU Usage



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

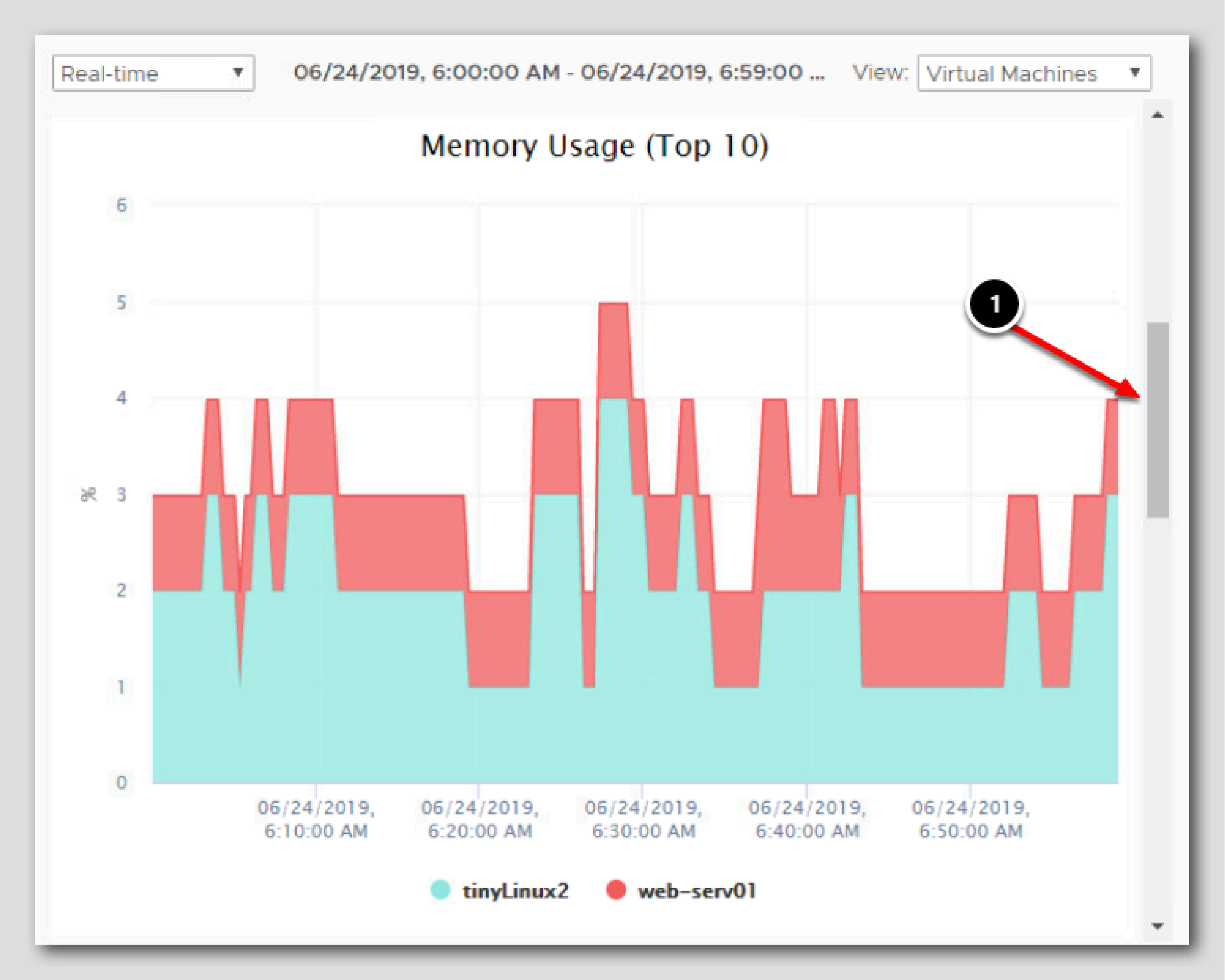
Combined CPU Usage

[187]



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).

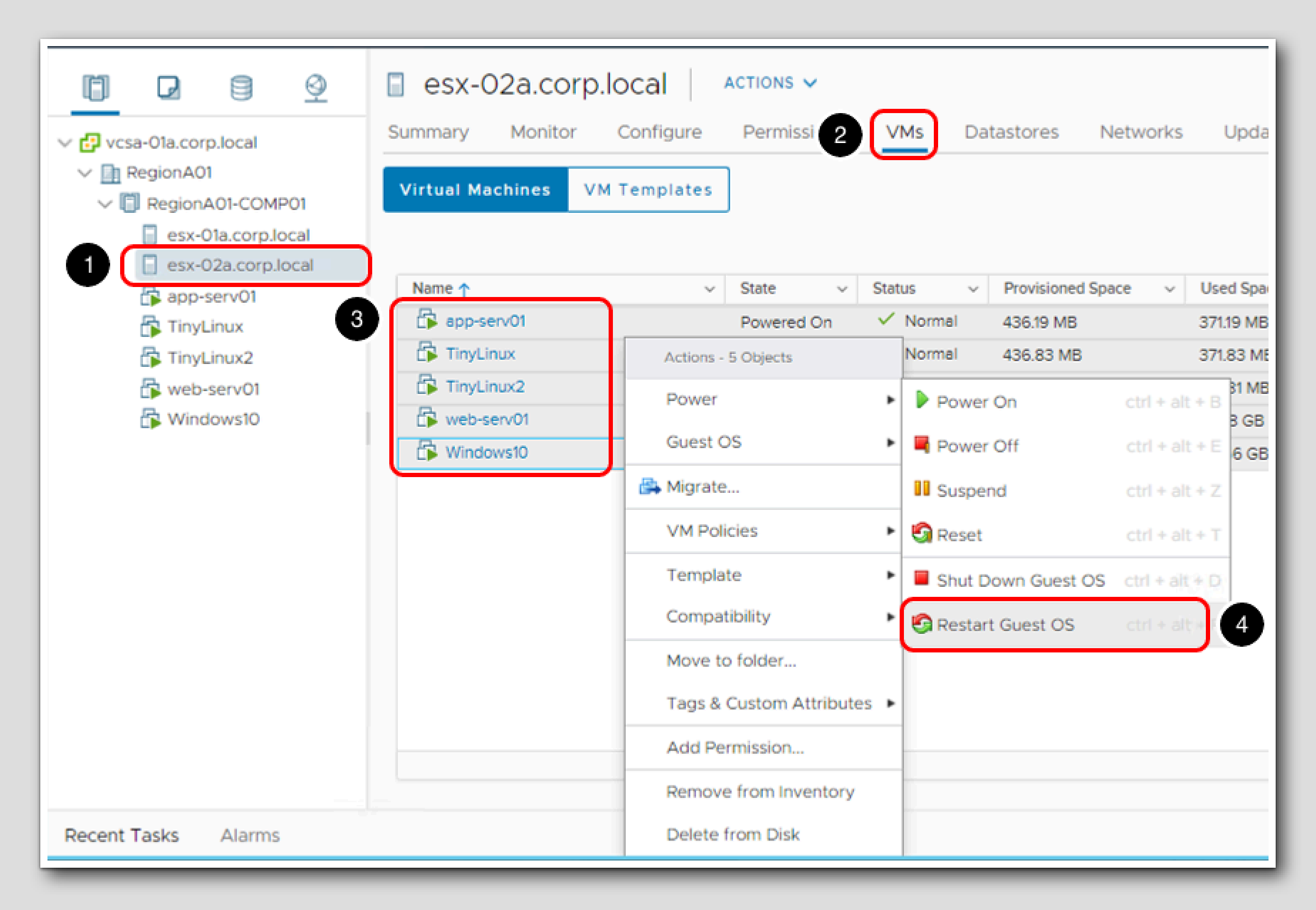
1. Use the scroll bars to access the additional charts.

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

[189]

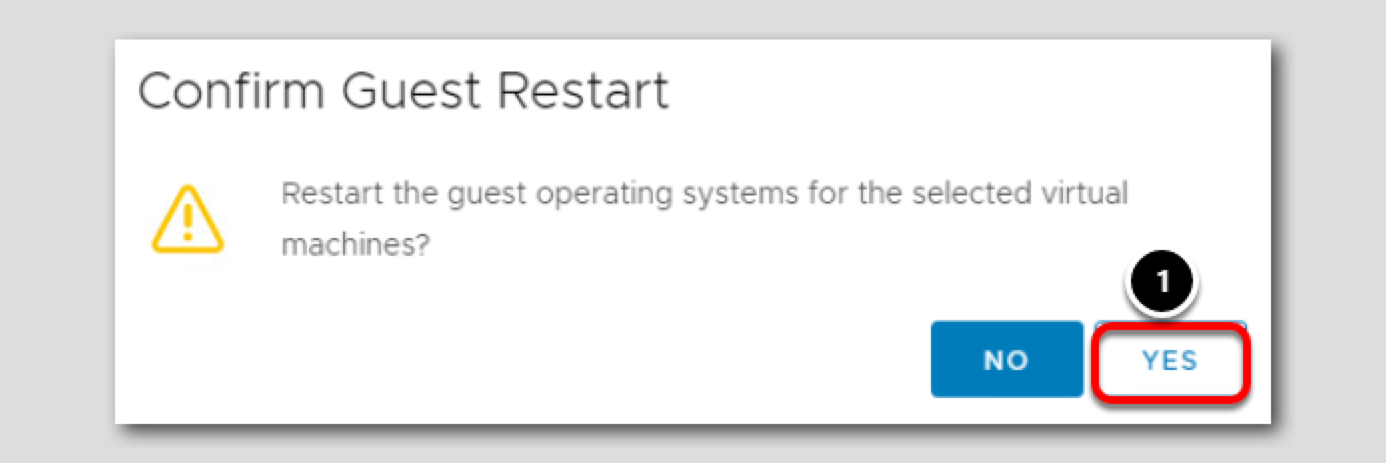


To generate some activity on esx-02a.corp.local, the virtual machines will be rebooted.

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

Confirm Restart

[190]



Confirm Guest Restart

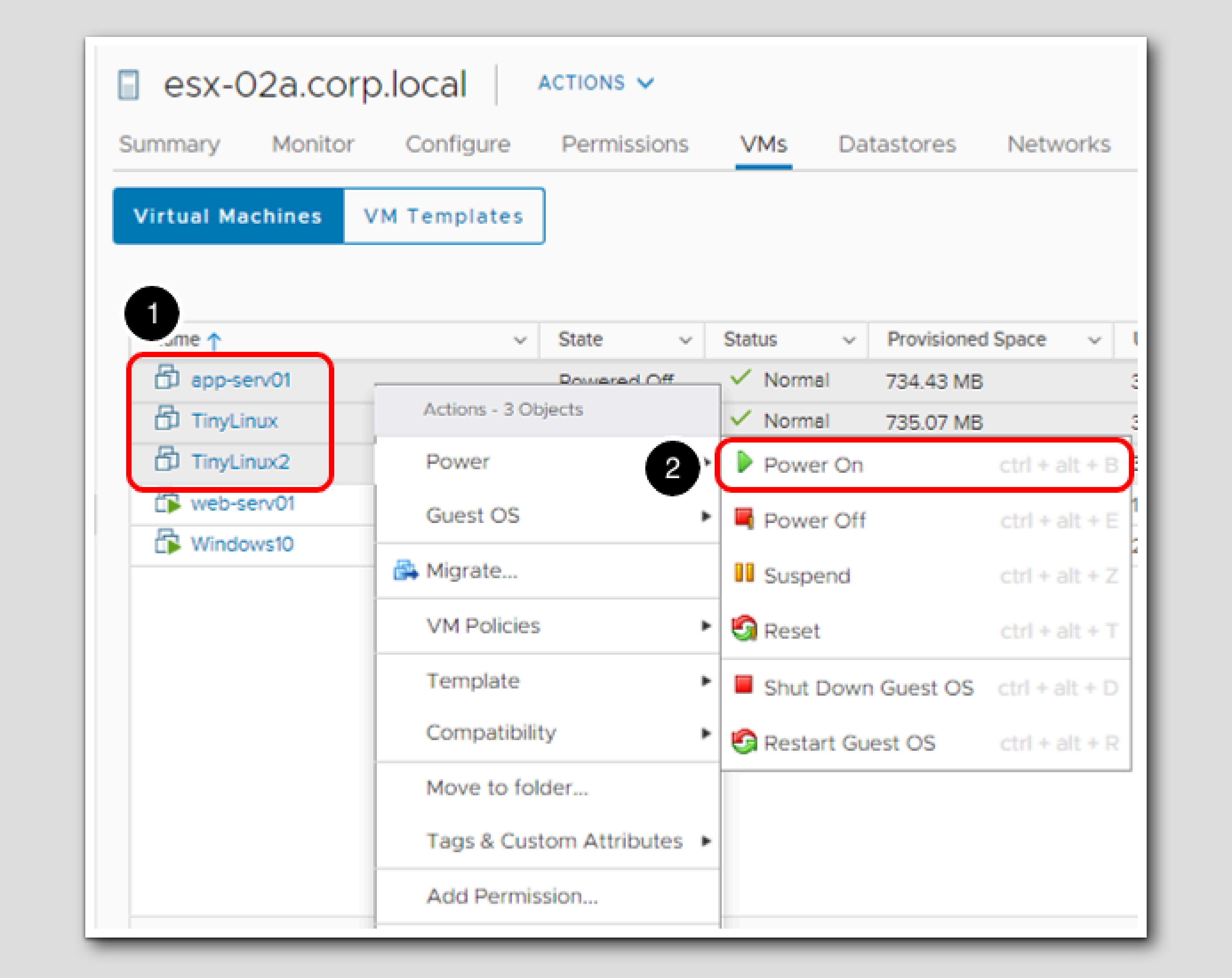
Restart the guest operating systems for the selected virtual machines?

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

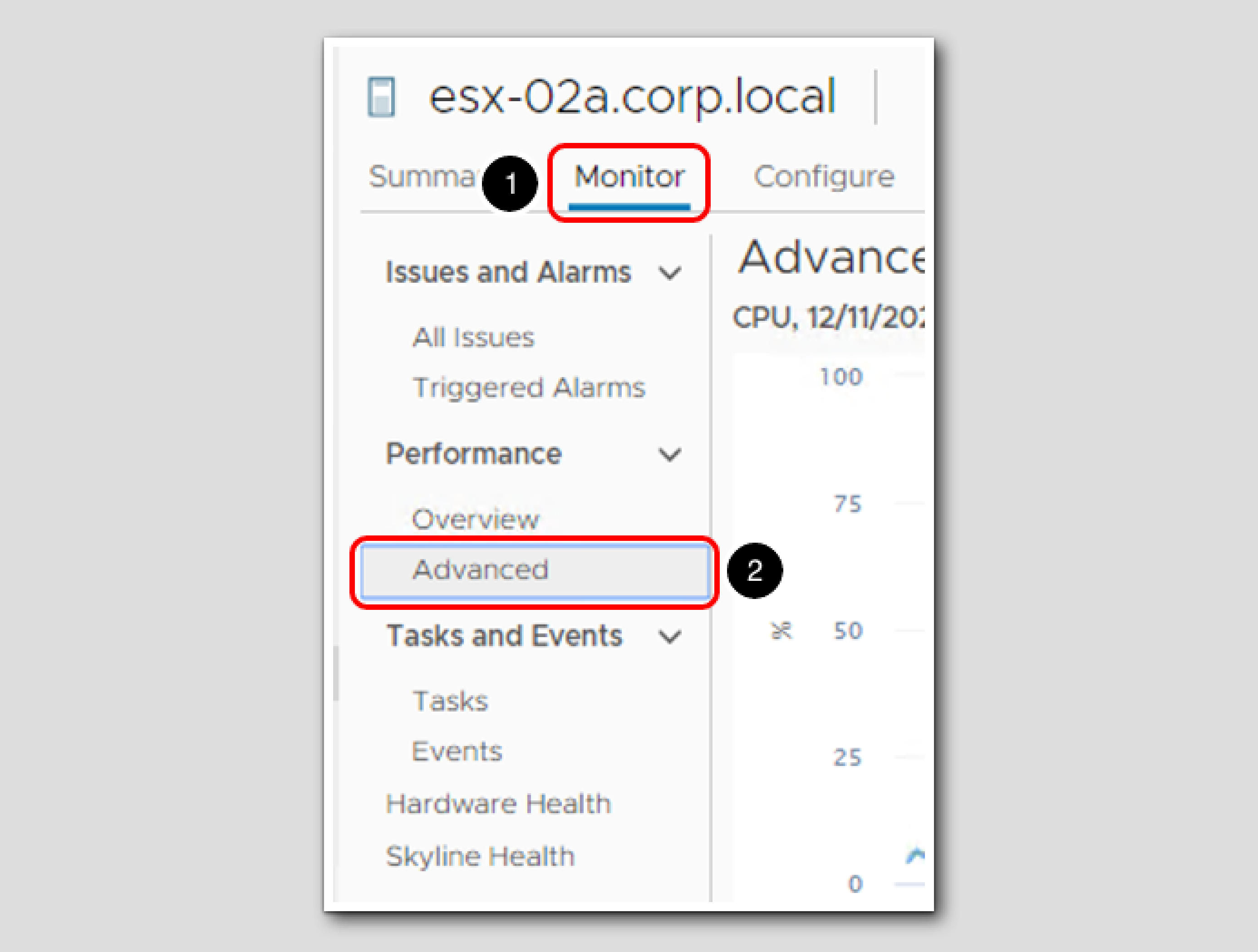
[191]



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

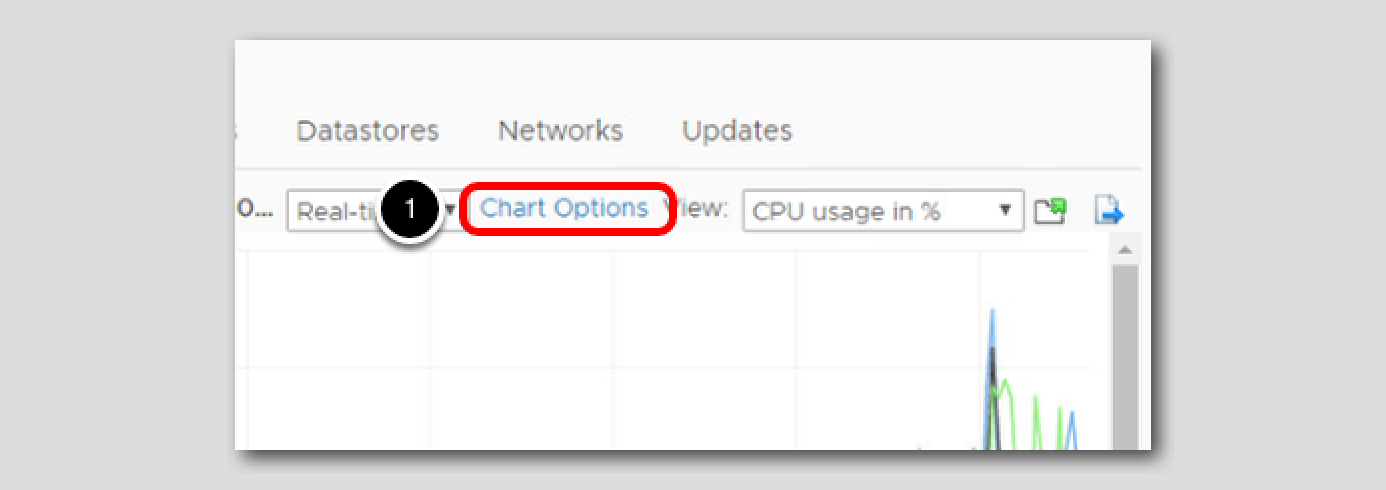
Monitor Performance

[192]



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

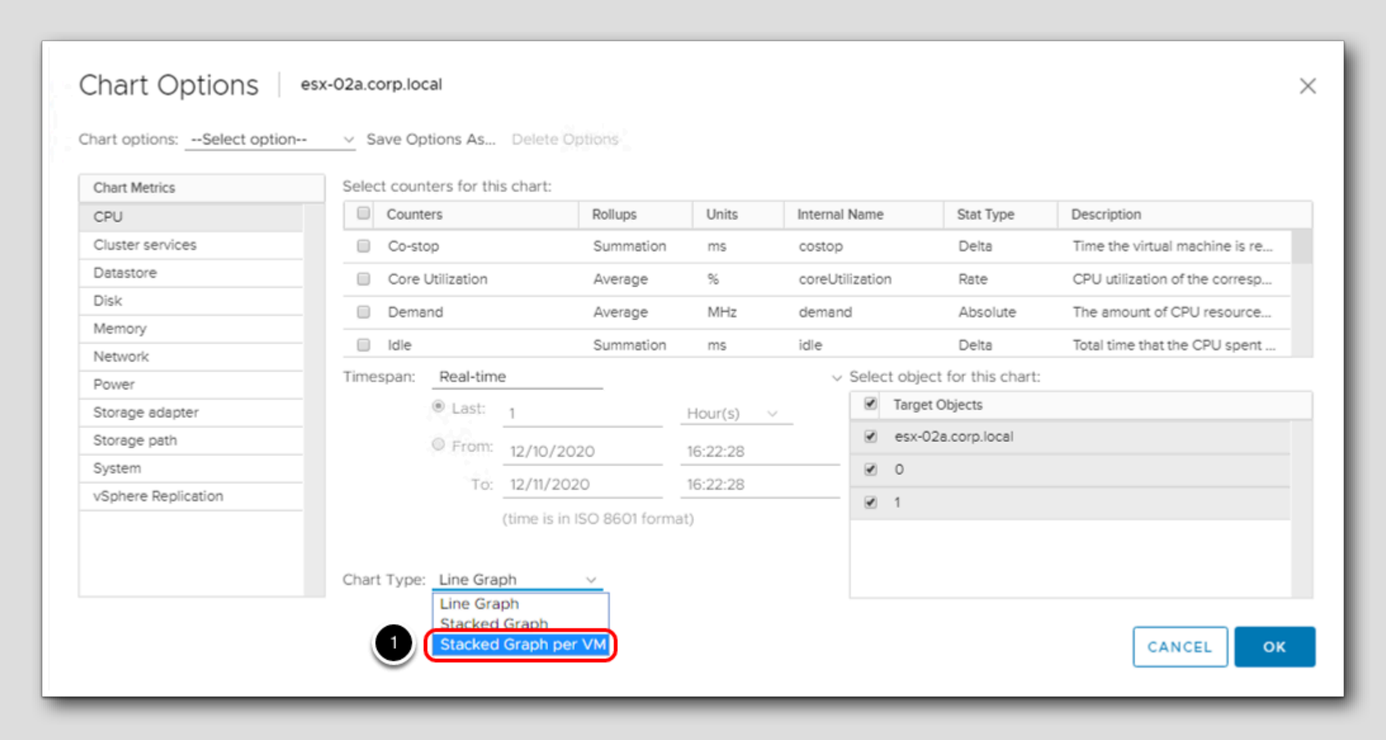


Chart Options | esx-02a.corp.local

Chart options: --Select option-- 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 machine is re...
□	Core Utilization	Average	%	coreUtilization	Rate	CPU utilization of the corresp...
□	Demand	Average	MHz	demand	Absolute	The amount of CPU resource...
□	Idle	Summation	ms	idle	Delta	Total time that the CPU spent ...

Timespan: Real-time

● Last: 1 Hour(s)

○ From: 12/10/2020 16:22:28

To: 12/11/2020 16:22:28

(time is in ISO 8601 format)

Select object for this chart:

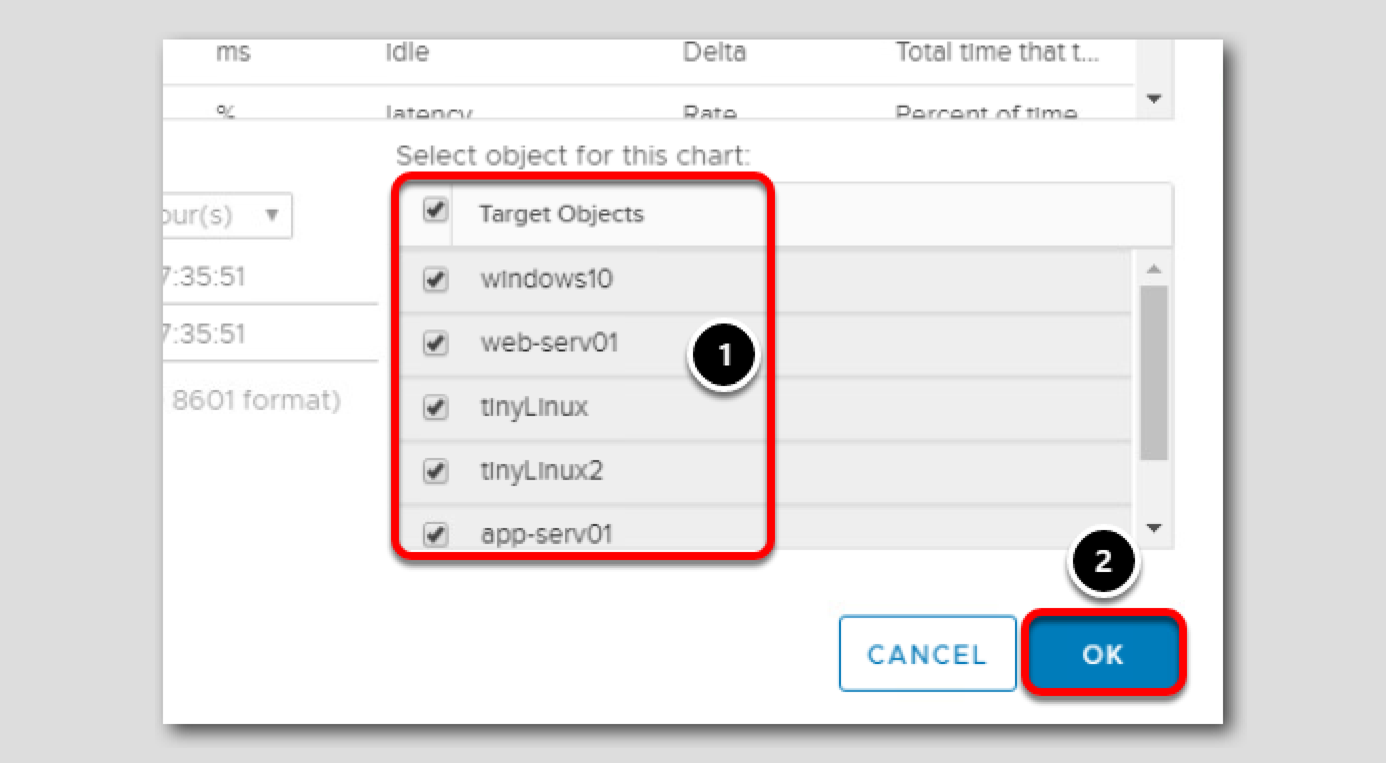
☑	Target Objects
☑	esx-02a.corp.local
☑	0
☑	1

Chart Type: Line Graph

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

Select Objects

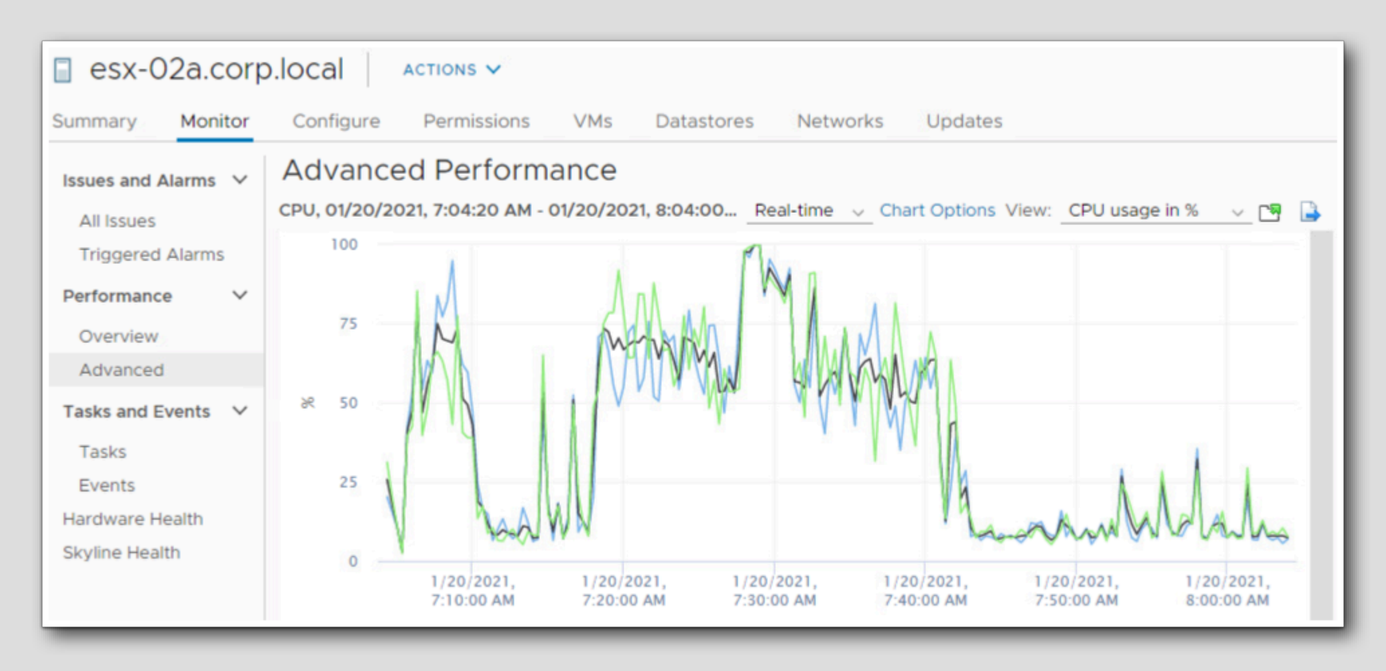
[195]



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

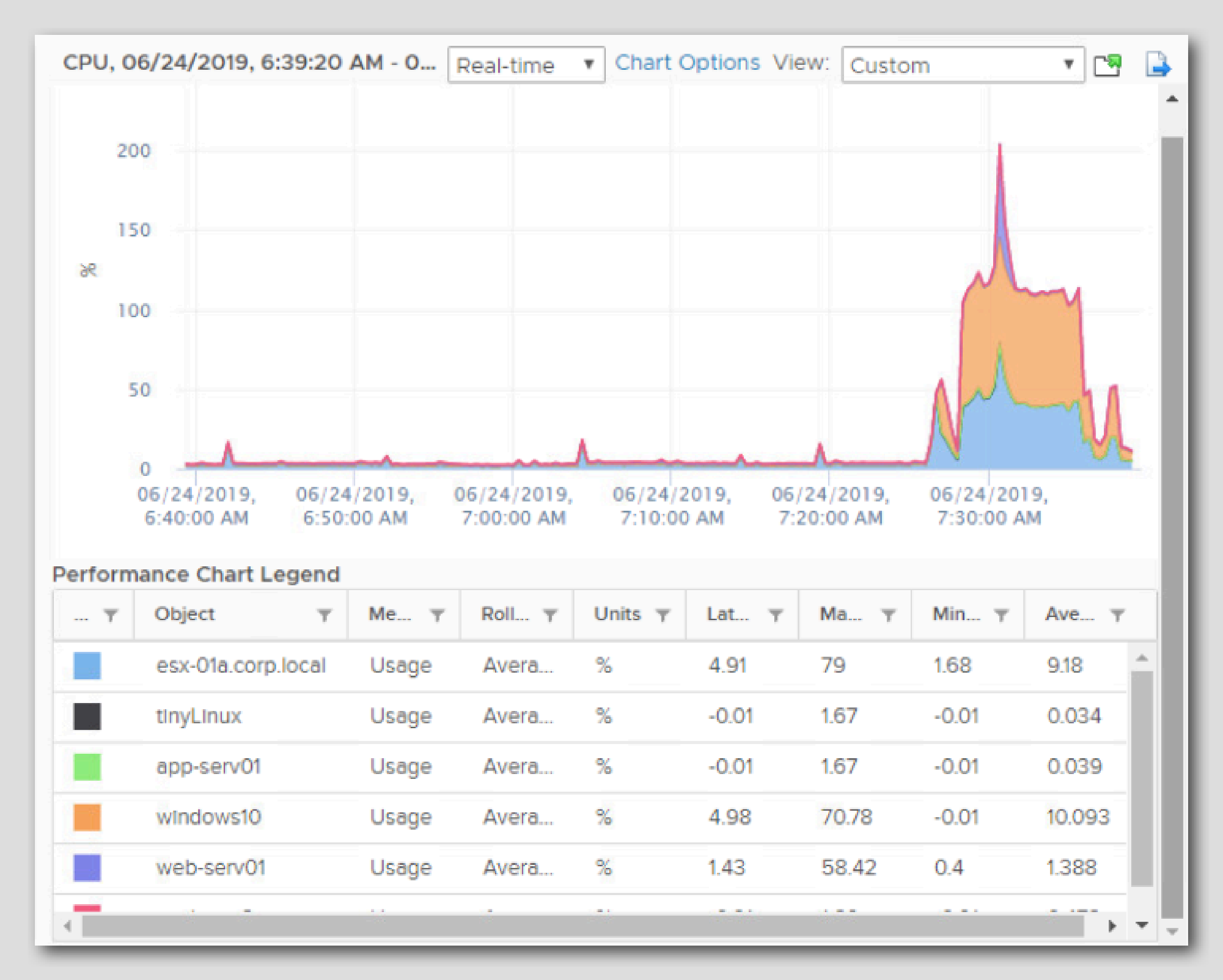
[196]



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

Performance Chart Legend

[197]

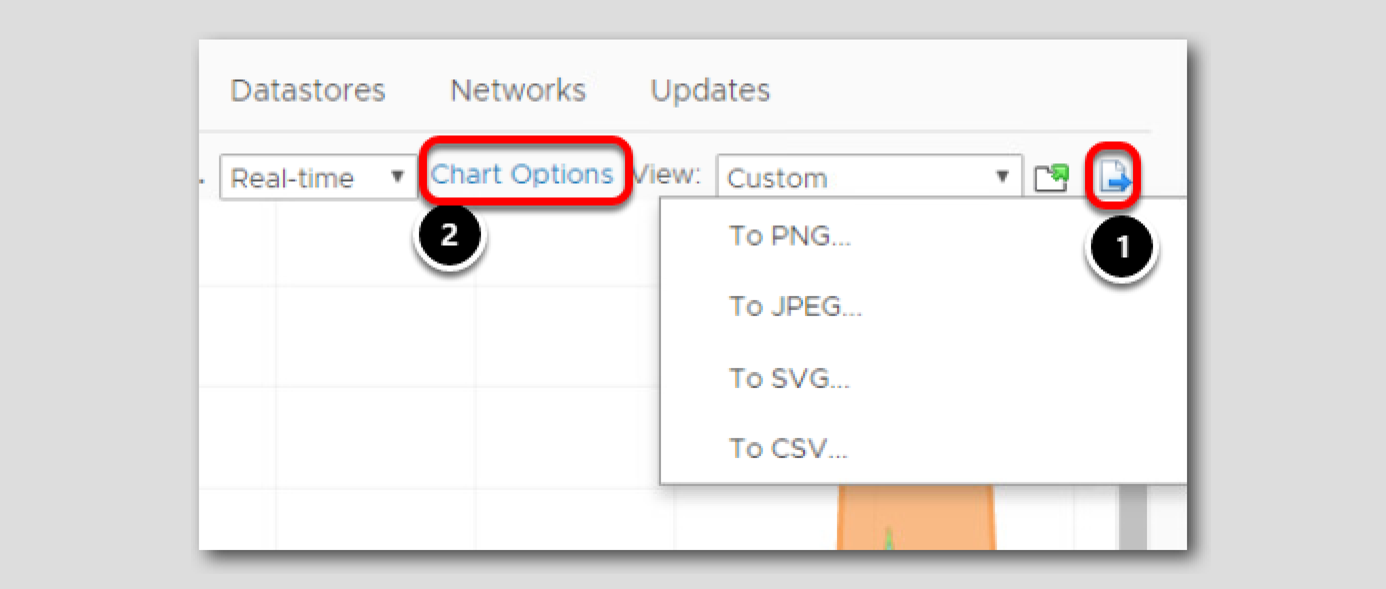


Performance Chart Legend

...	Object	Me...	Roll...	Units	Lat...	Ma...	Min...	Ave...
🟦	esx-01a.corp.local	Usage	Avera...	%	4.91	79	1.68	9.18
⬛	tinyLinux	Usage	Avera...	%	-0.01	1.67	-0.01	0.034
🟩	app-serv01	Usage	Avera...	%	-0.01	1.67	-0.01	0.039
🟧	windows10	Usage	Avera...	%	4.98	70.78	-0.01	10.093
🟪	web-serv01	Usage	Avera...	%	1.43	58.42	0.4	1.388

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

[199]

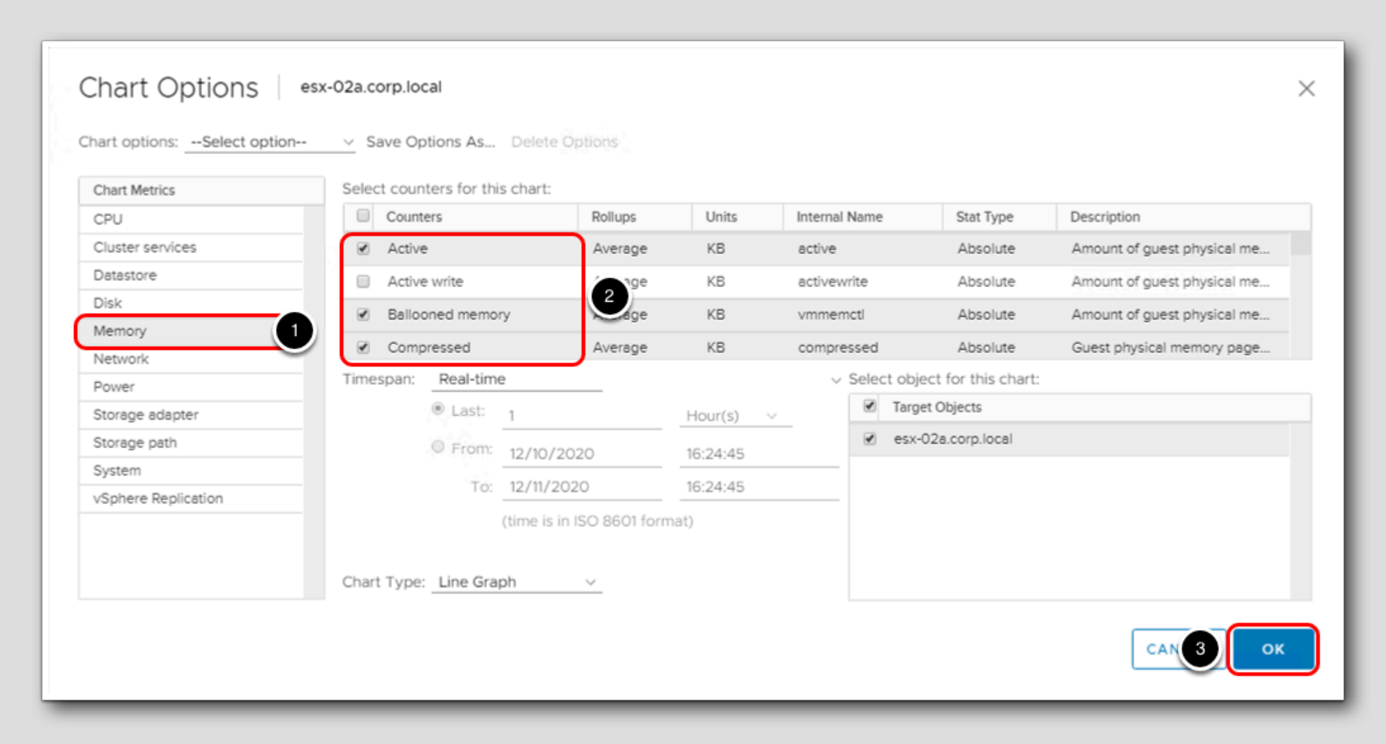


Chart Options | esx-02a.corp.local

Chart options: --Select option-- Save Options As... Delete Options

Chart Metrics
CPU
Cluster services
Datastore
Disk
Memory
Network
Power
Storage adapter
Storage path
System
vSphere Replication

Select counters for this chart:

☐	Counters	Rollups	Units	Internal Name	Stat Type	Description
☑	Active	Average	KB	active	Absolute	Amount of guest physical me...
☐	Active write	Average	KB	activewrite	Absolute	Amount of guest physical me...
☑	Ballooned memory	Average	KB	vmmemctl	Absolute	Amount of guest physical me...
☑	Compressed	Average	KB	compressed	Absolute	Guest physical memory page...

Timespan: Real-time

● Last: 1 Hour(s)

○ From: 12/10/2020 16:24:45

To: 12/11/2020 16:24:45

(time is in ISO 8601 format)

Chart Type: Line Graph

Select object for this chart:

☑	Target Objects
☑	esx-02a.corp.local

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**.

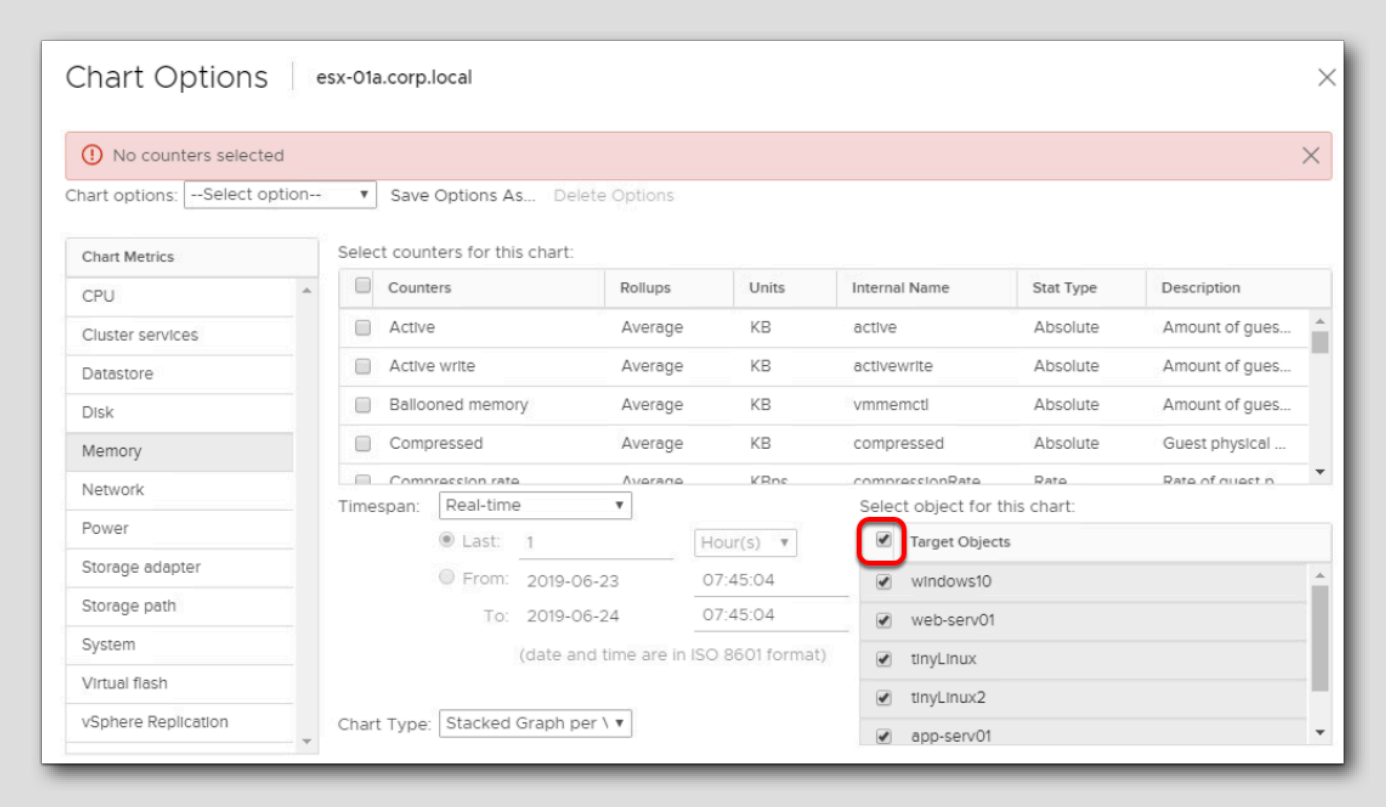


Chart Options | esx-01a.corp.local

No counters selected

Chart options: --Select option-- ▾ Save Options As... Delete Options

Chart Metrics
- CPU
- Cluster services
- Datastore
- Disk
- Memory
- Network
- Power
- Storage adapter
- Storage path
- System
- Virtual flash
- vSphere Replication

Select counters for this chart:

□ Counters	Rollups	Units	Internal Name	Stat Type	Description
□ Active	Average	KB	active	Absolute	Amount of gues...
□ Active write	Average	KB	activewrite	Absolute	Amount of gues...
□ Ballooned memory	Average	KB	vmmemctl	Absolute	Amount of gues...
□ Compressed	Average	KB	compressed	Absolute	Guest physical ...
□ Compression rate	Average	KBps	compressionRate	Rate	Rate of guest p...

Timespan: Real-time ▾

● 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: Stacked Graph per \ ▾

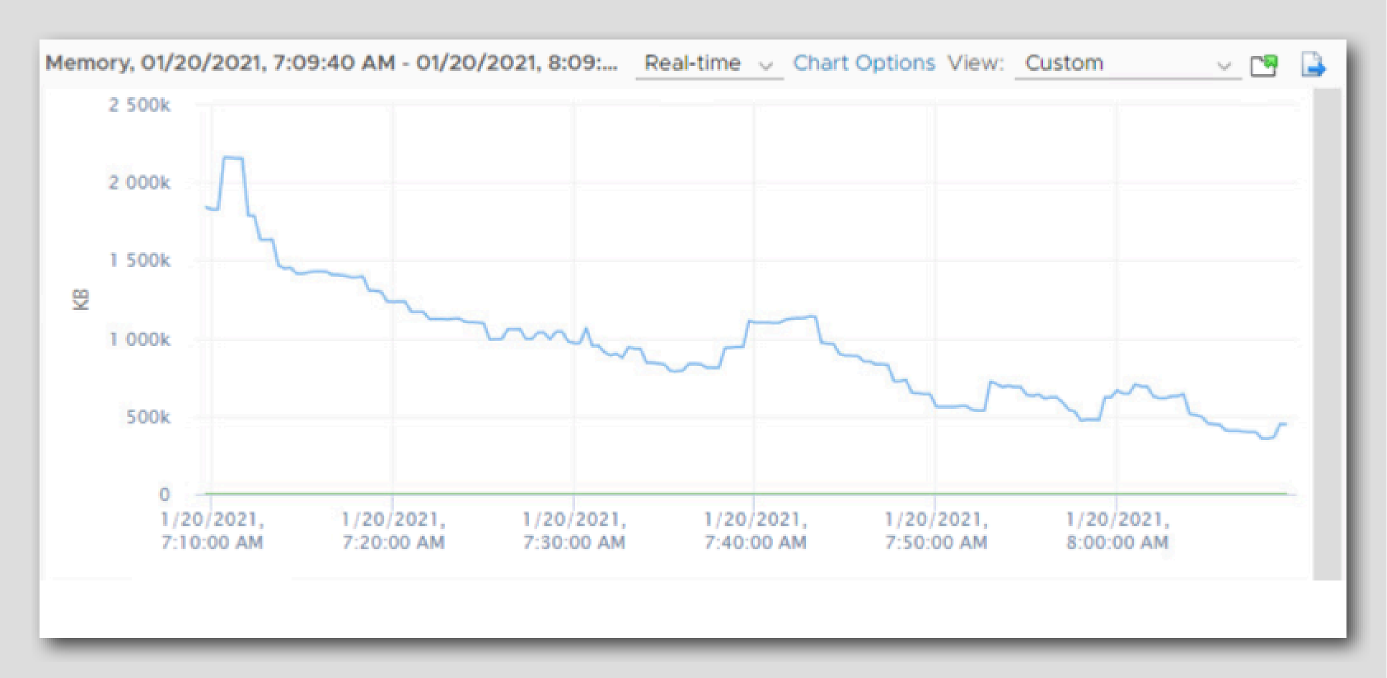
Select object for this chart:

- ☑ Target Objects
- ☑ windows10
- ☑ web-serv01
- ☑ tinyLinux
- ☑ tinyLinux2
- ☑ app-serv01

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

Memory Real-time

[200]

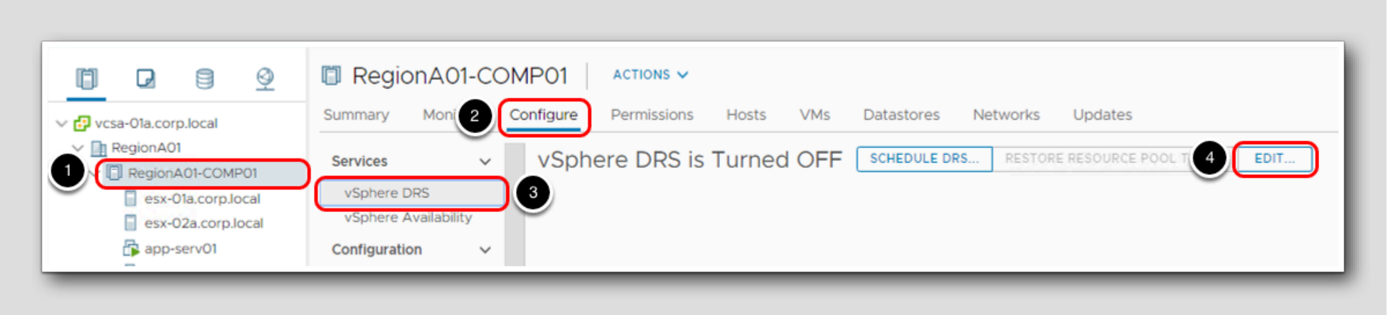


This chart shows the memory counters relative to memory for esx-02a.corp.local. Scroll down the Performance Chart Legend to see the counter each line represents.

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

Enable DRS

[201]

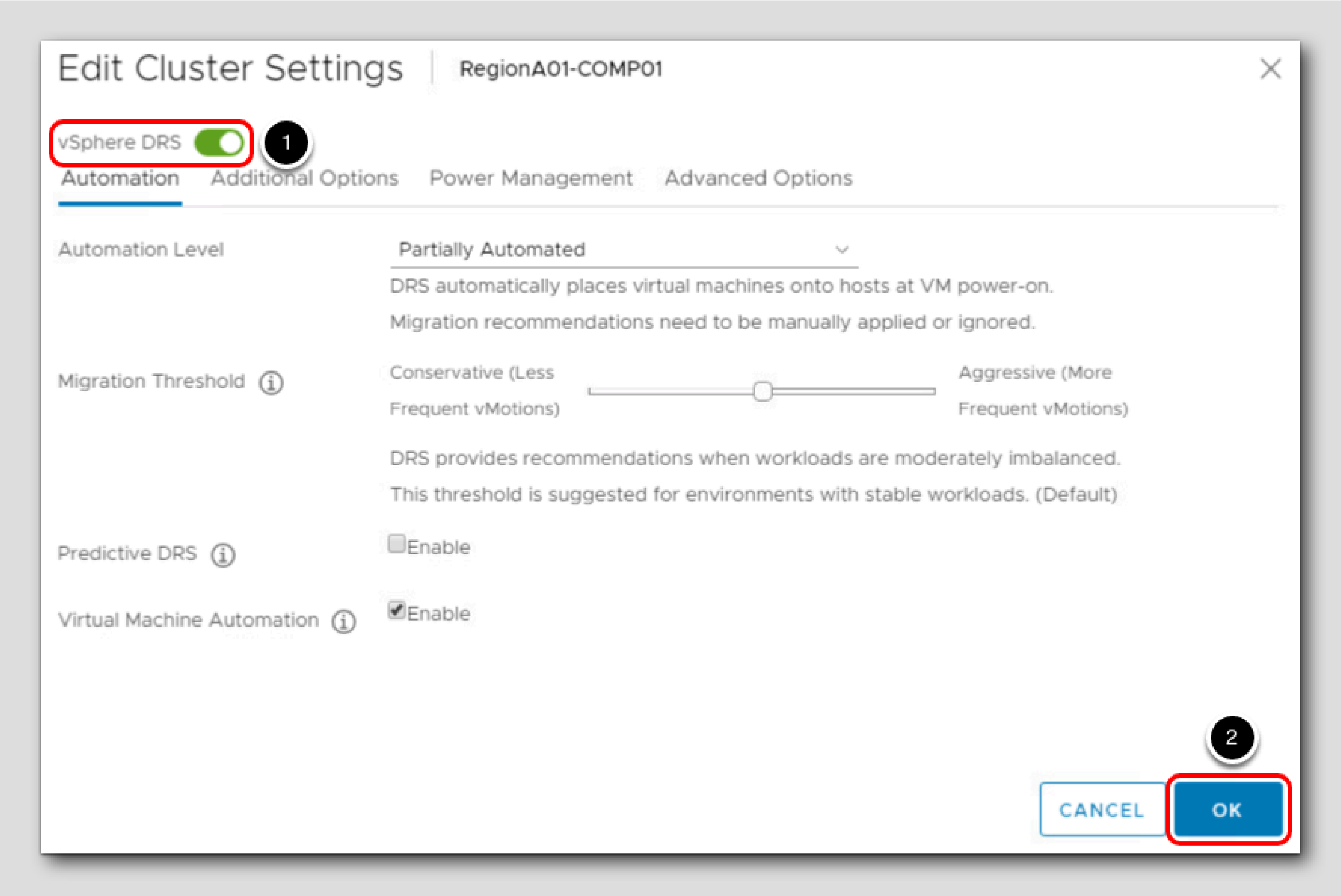


Once you have finished viewing the charts, DRS needs to be enabled again.

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

Turn ON vSphere DRS

[202]



Edit Cluster Settings | RegionA01-COMP01

vSphere DRS (on)

Automation Level: Partially Automated

DRS automatically places virtual machines onto hosts at VM power-on.
Migration recommendations need to be manually applied or ignored.

Migration Threshold: Conservative (Less Frequent vMotions) — Aggressive (More Frequent vMotions)

DRS provides recommendations when workloads are moderately imbalanced.
This threshold is suggested for environments with stable workloads. (Default)

Predictive DRS: □ Enable

Virtual Machine Automation: ☑ Enable

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

Further Information

[203]

For more information on performance charts, you can view the *vSphere Monitoring and Performance* guide.

Introduction to vSphere with Tanzu

[204]

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

Common Platform for Running both Kubernetes/Containerized Workloads and VMs

[205]

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

Agile Operations for Kubernetes Applications

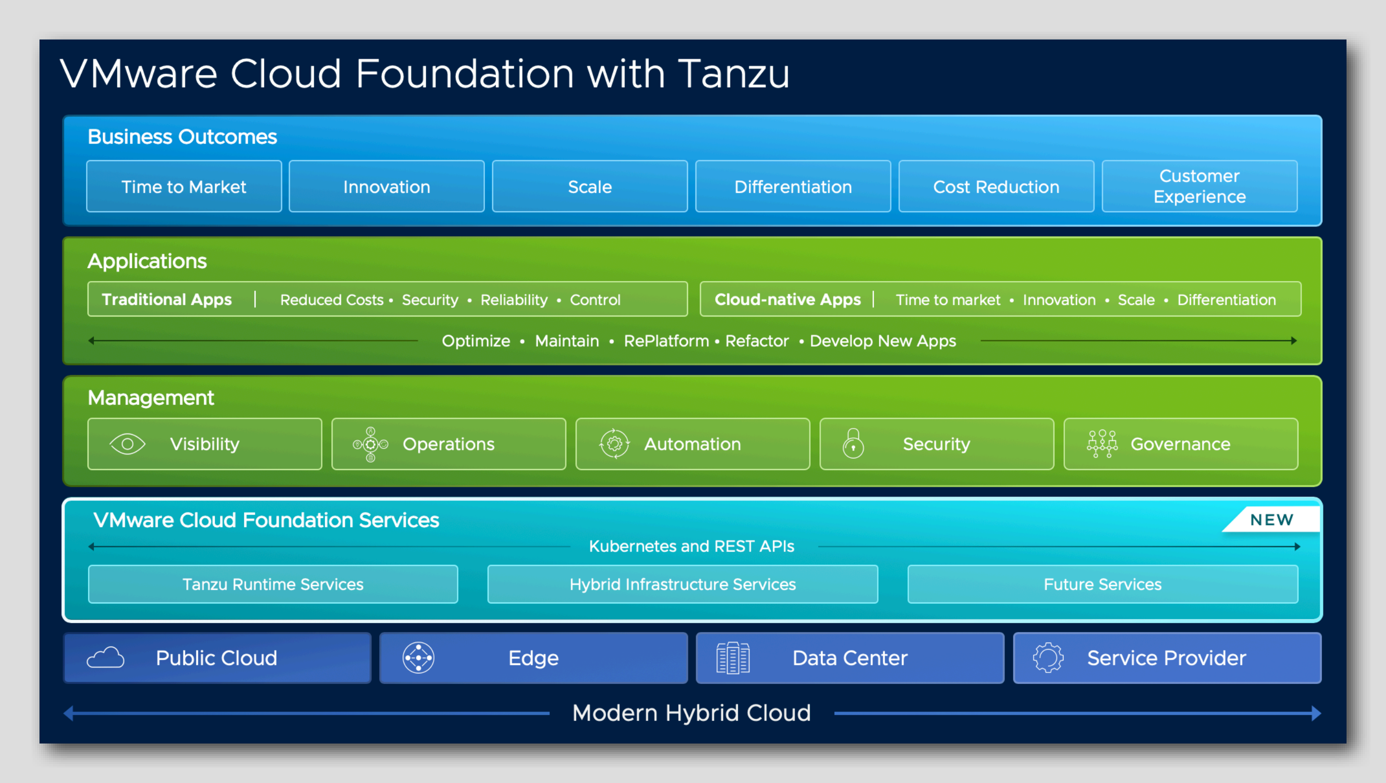
[206]

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

VMware Cloud Foundation Services

[207]

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



VMware Cloud Foundation with Tanzu

Business Outcomes

Time to Market | Innovation | Scale | Differentiation | Cost Reduction | Customer Experience

Applications

Traditional Apps | Reduced Costs • Security • Reliability • Control

Cloud-native Apps | Time to market • Innovation • Scale • Differentiation

Optimize • Maintain • RePlatform • Refactor • Develop New Apps

Management

Visibility | Operations | Automation | Security | Governance

VMware Cloud Foundation Services

NEW

Kubernetes and REST APIs

Tanzu Runtime Services | Hybrid Infrastructure Services | Future Services

Public Cloud | Edge | Data Center | Service Provider

Modern Hybrid Cloud

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

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

Conclusion

[208]

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

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

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

ESXi Install and Configure

[209]

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

Video: Installing and Configuring vSphere (4:36)

[210]

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

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

```
VMware ESXi 5.1.0 (VMkernel Release Build 799733)

Cisco Systems Inc N20-B6620-1

2 x Intel(R) Xeon(R) CPU E5540 @ 2.53GHz
48 GiB Memory

Download tools to manage this host from:
http://[illegible] (waiting for DHCP...)
http://[illegible]

  Warning: DHCP lookup failed. You may be unable to access this system until you customize its
  network configuration.
```

Video: Overview of the DCUI (4:58)

[211]

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

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

Certification Path

[212]

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

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

Learn More Here: *https://www.vmware.com/learning/certification/vcap-dcv-deploy.html*

vmware®
CERTIFIED
ADVANCED PROFESSIONAL
Data Center Virtualization Deploy 2021

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

Introduction

[214]

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

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

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

Types of virtual switches

[215]

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

vNetwork Standard Switch (vSwitch, vSS)

[216]

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

vSwitches are configured on each ESXi/ESX host.

vNetwork Distributed Switch (dvSwitch, vDS)

[217]

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

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

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

Comparing vNetwork Standard Switch with vNetwork Distributed Switch

[218]

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

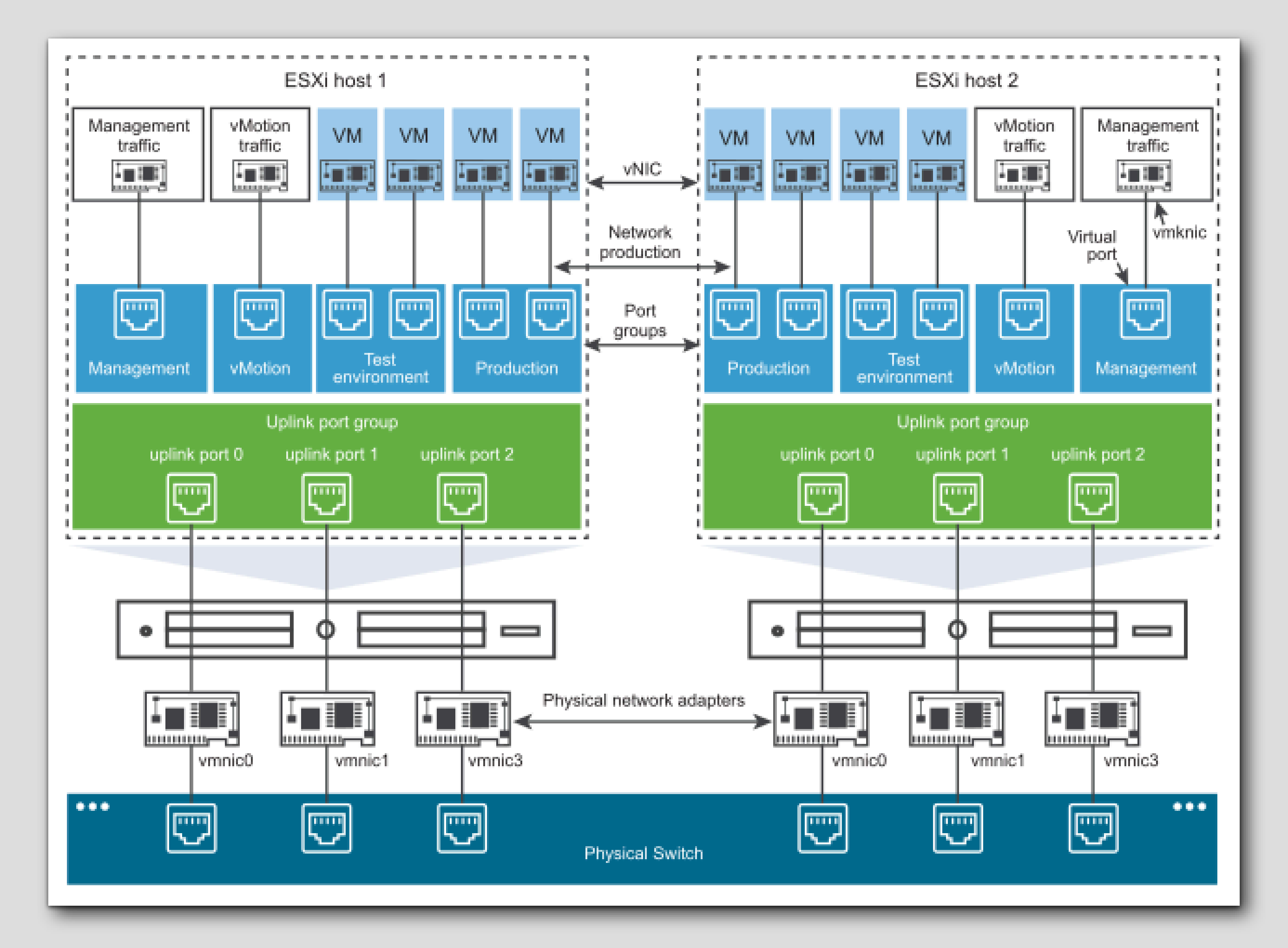
[219]

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.

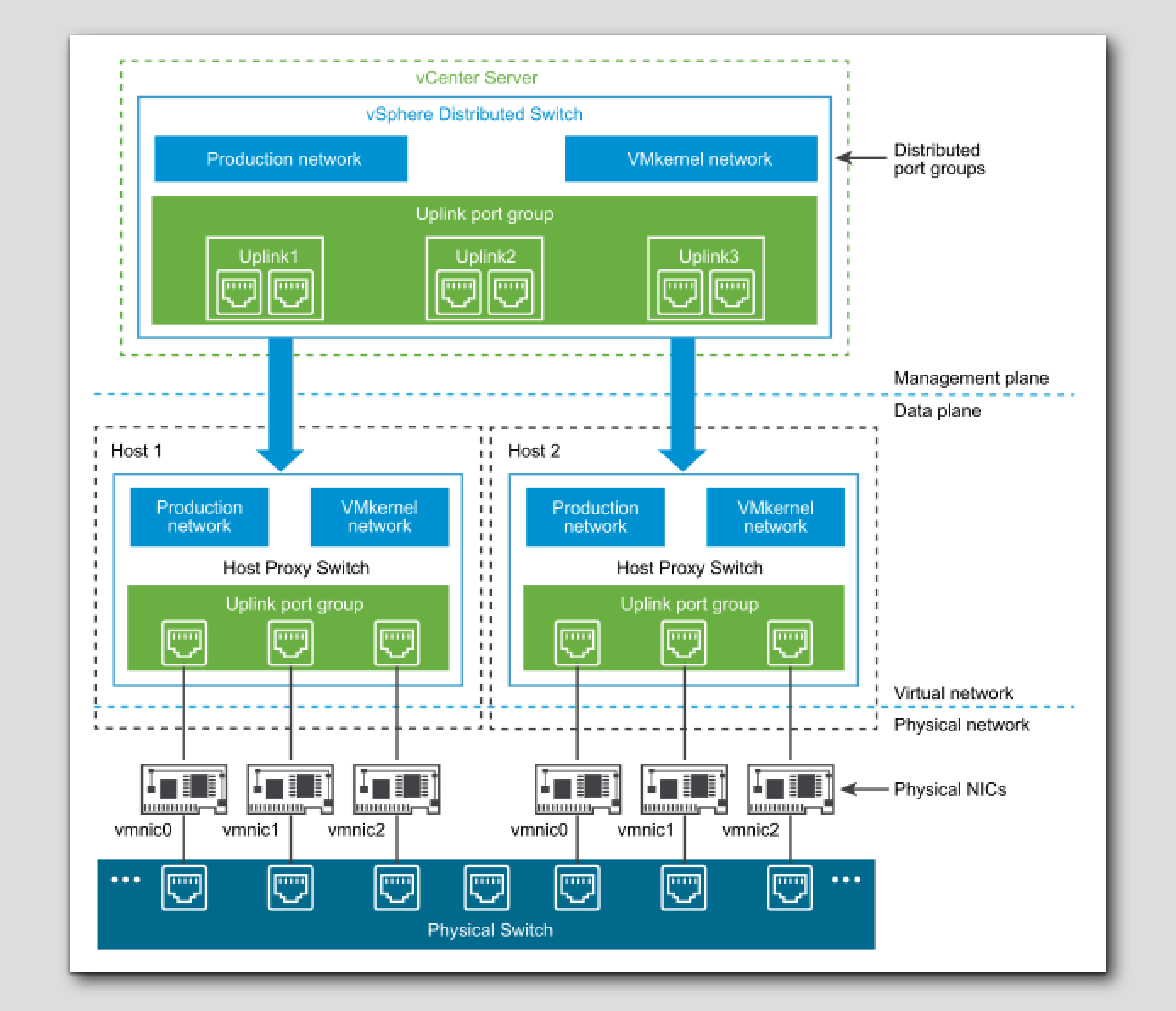
vSphere Standard Switch Architecture

[220]



vSphere Distributed Switch Architecture

[221]



Let&#39;s get started!

[222]

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

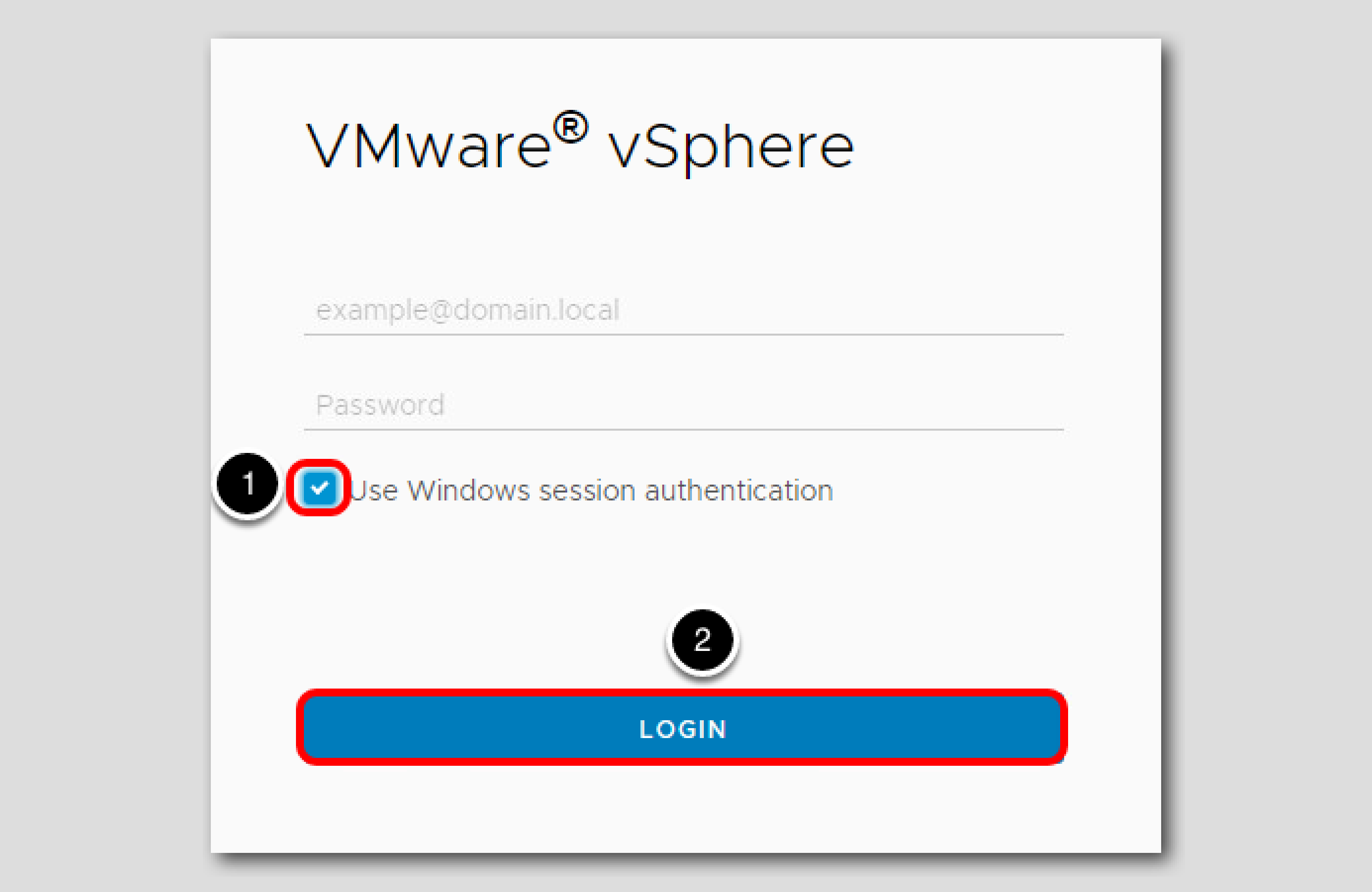
Adding and Configuring vSphere Standard Switch

[223]

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

Adding a Virtual Machine Port Group with the vSphere Client

[224]



VMware® vSphere

example@domain.local

Password

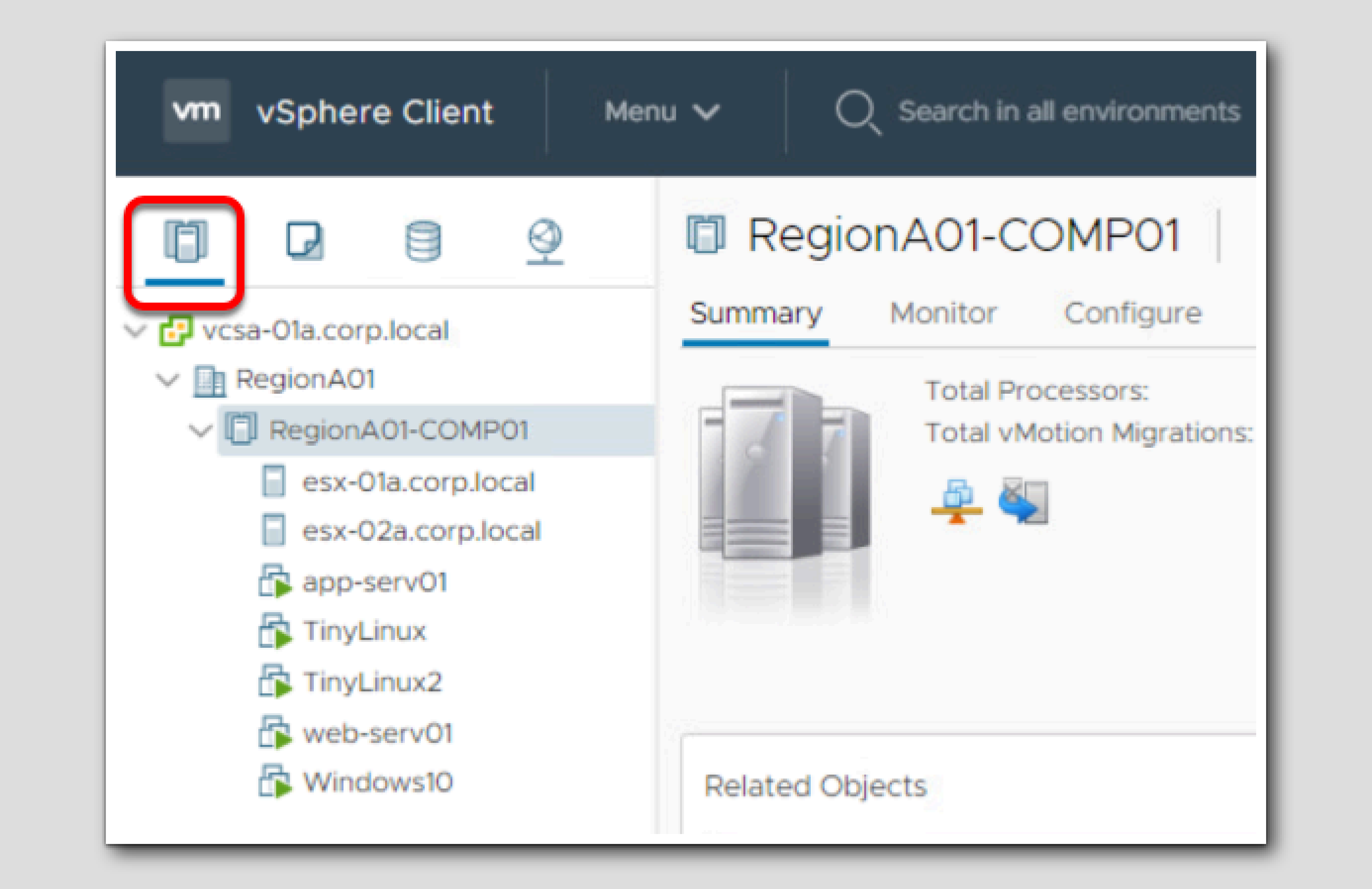
☑ Use Windows session authentication

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**"

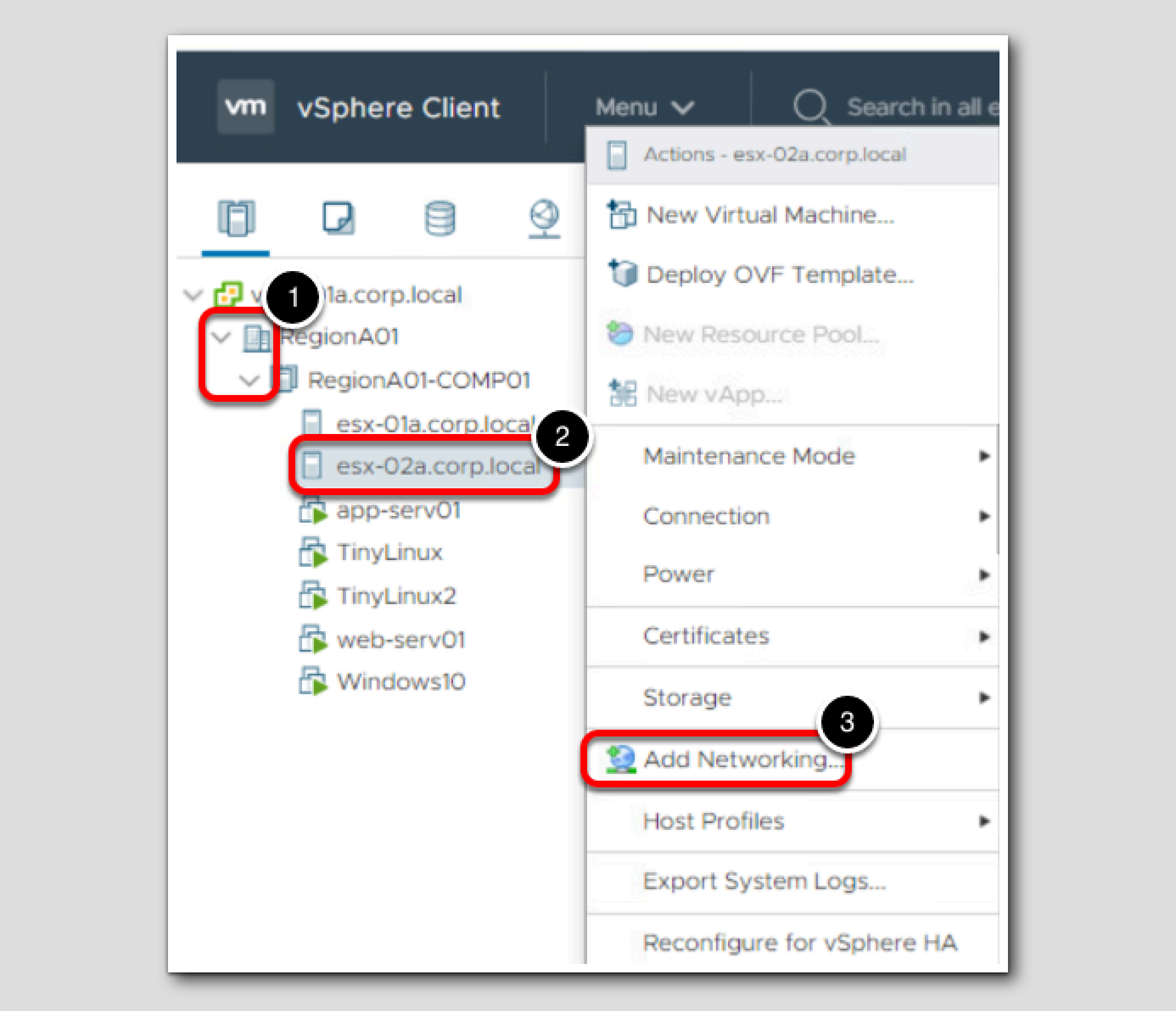
Select Hosts and Clusters

[225]



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

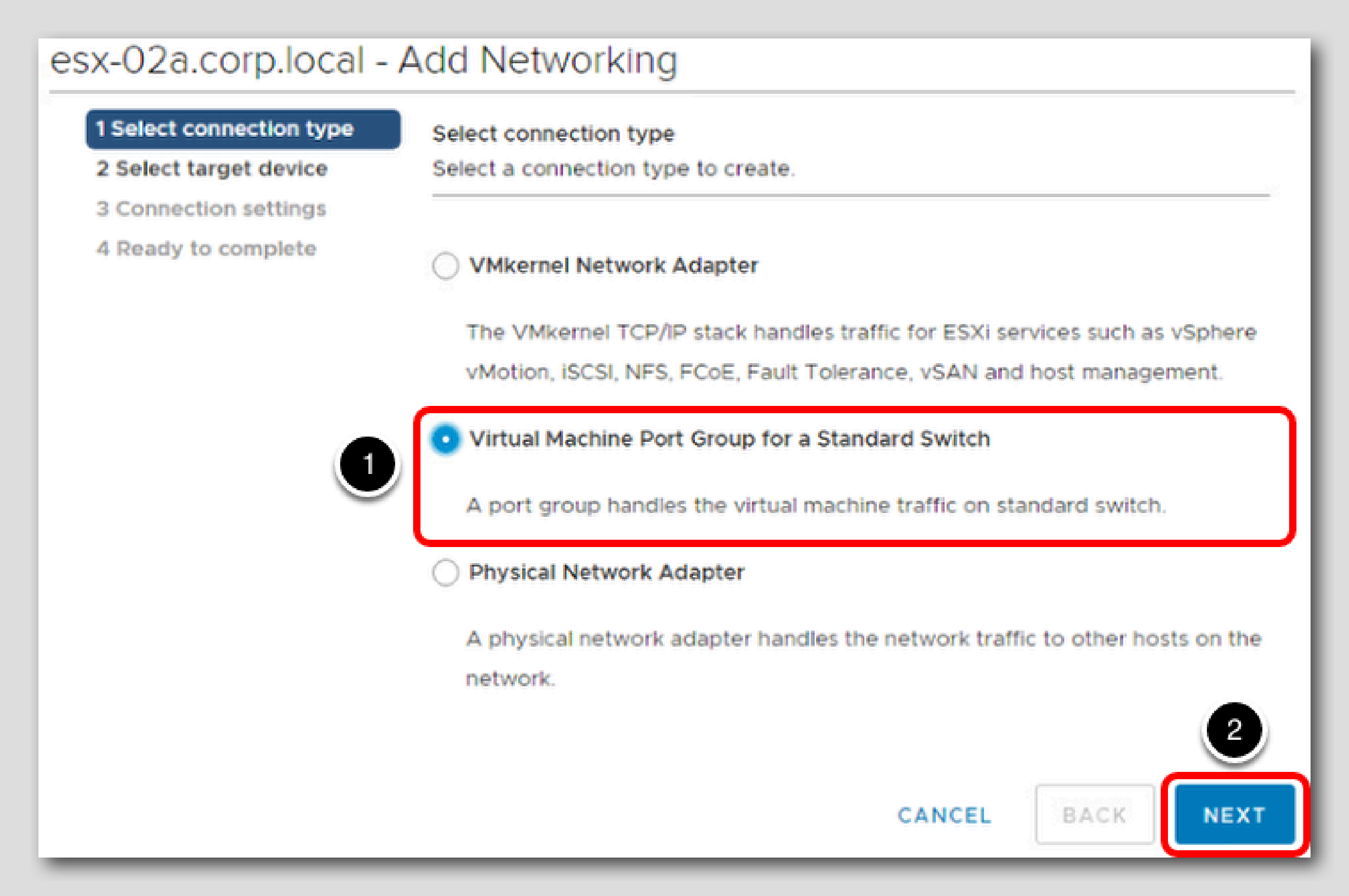
Add Networking



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

Connection Type

[227]



esx-02a.corp.local - Add Networking

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 port group handles the virtual machine traffic on standard switch.

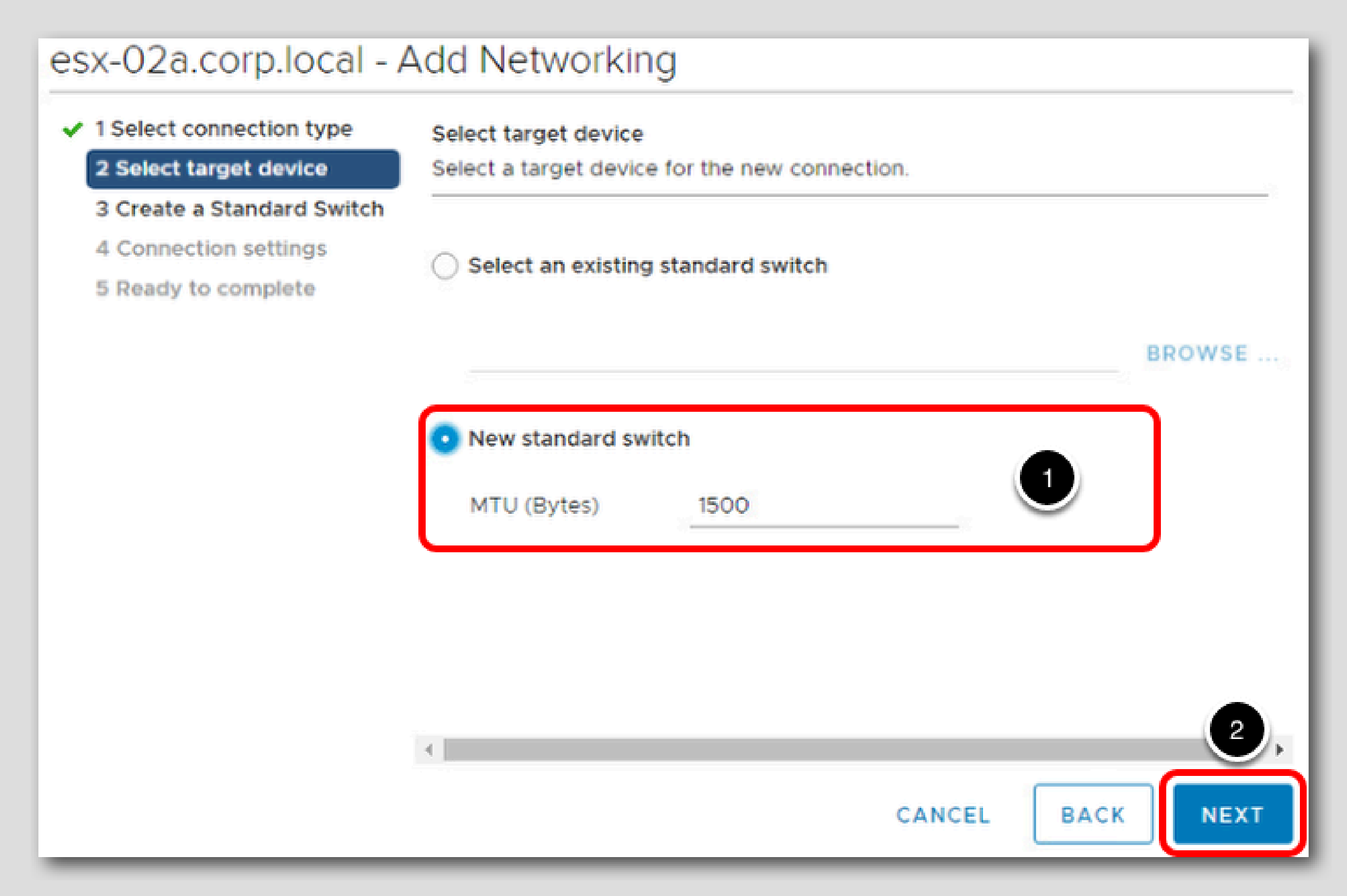
○ Physical Network Adapter

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

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

Target Device

[228]



esx-02a.corp.local - Add Networking

Select target device

Select a target device for the new connection.

○ Select an existing standard switch

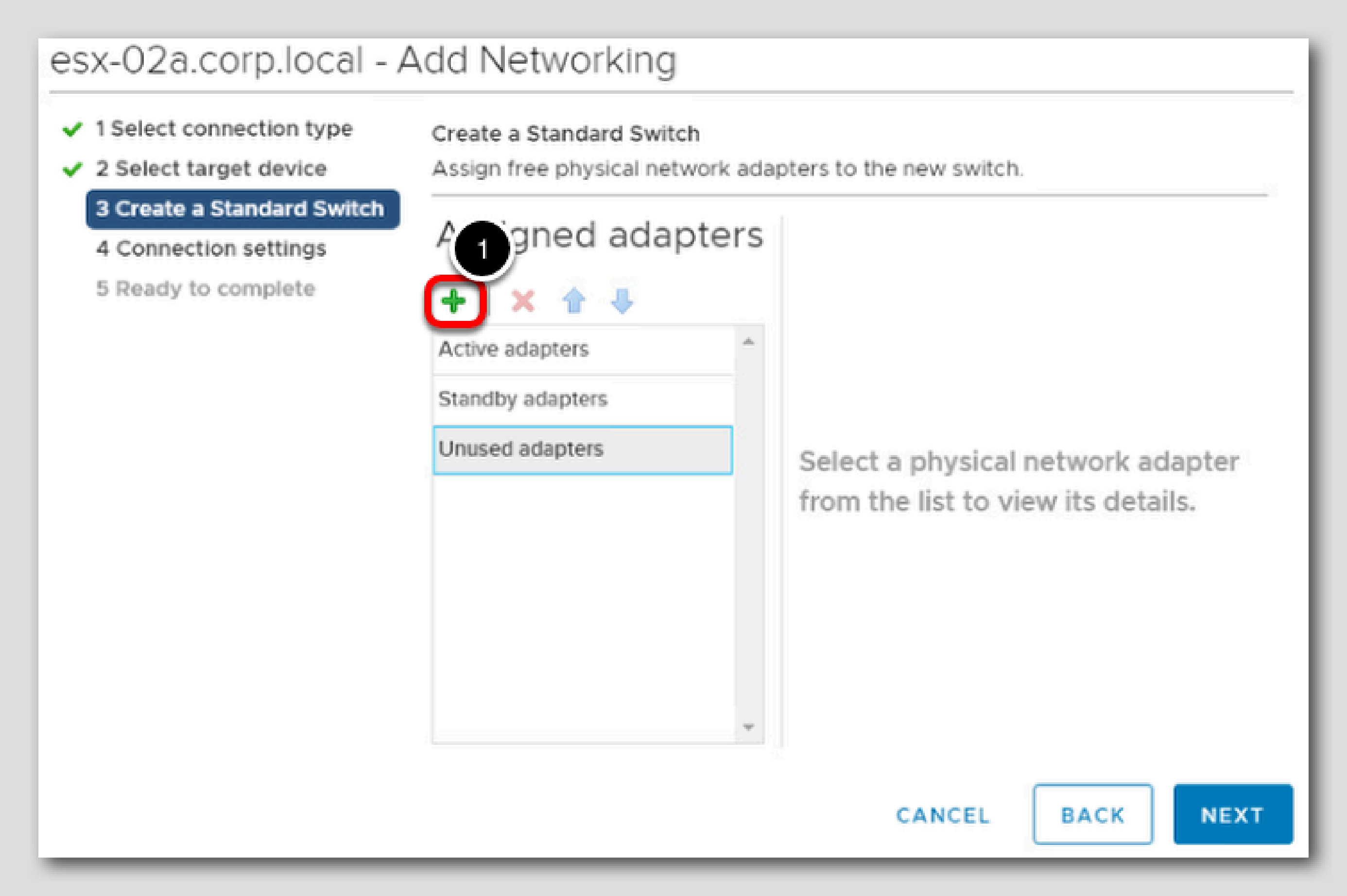
● New standard switch

MTU (Bytes) 1500

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

[229]



esx-02a.corp.local - Add Networking

Create a Standard Switch

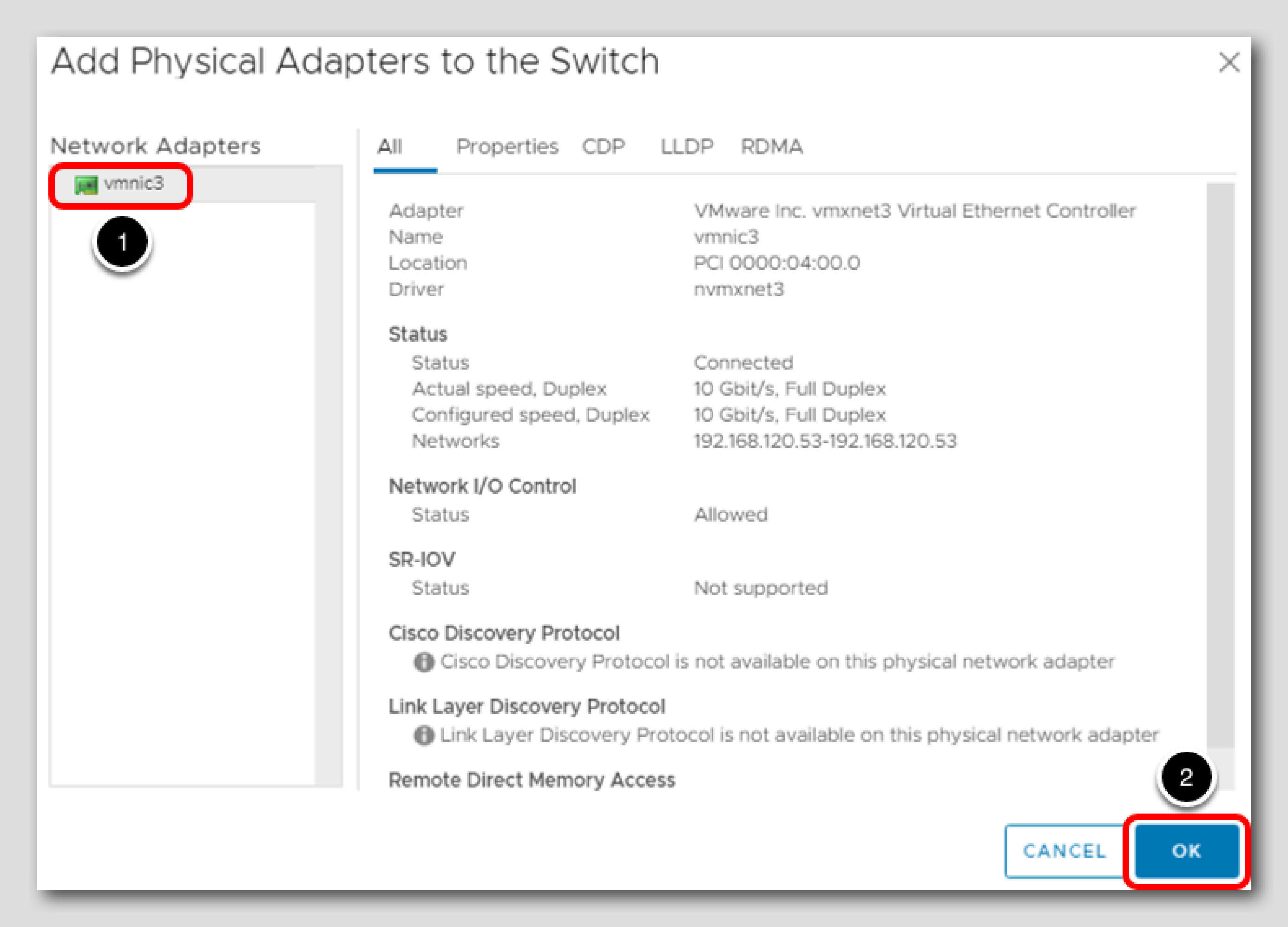
Assign free physical network adapters to the new switch.

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

1. Click the '+' button.

Add Physical Adapter

[230]



Adapter	VMware Inc. vmxnet3 Virtual Ethernet Controller
Name	vmnic3
Location	PCI 0000:04:00.0
Driver	nvmxnet3
Status	
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full Duplex
Configured speed, Duplex	10 Gbit/s, Full Duplex
Networks	192.168.120.53-192.168.120.53
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

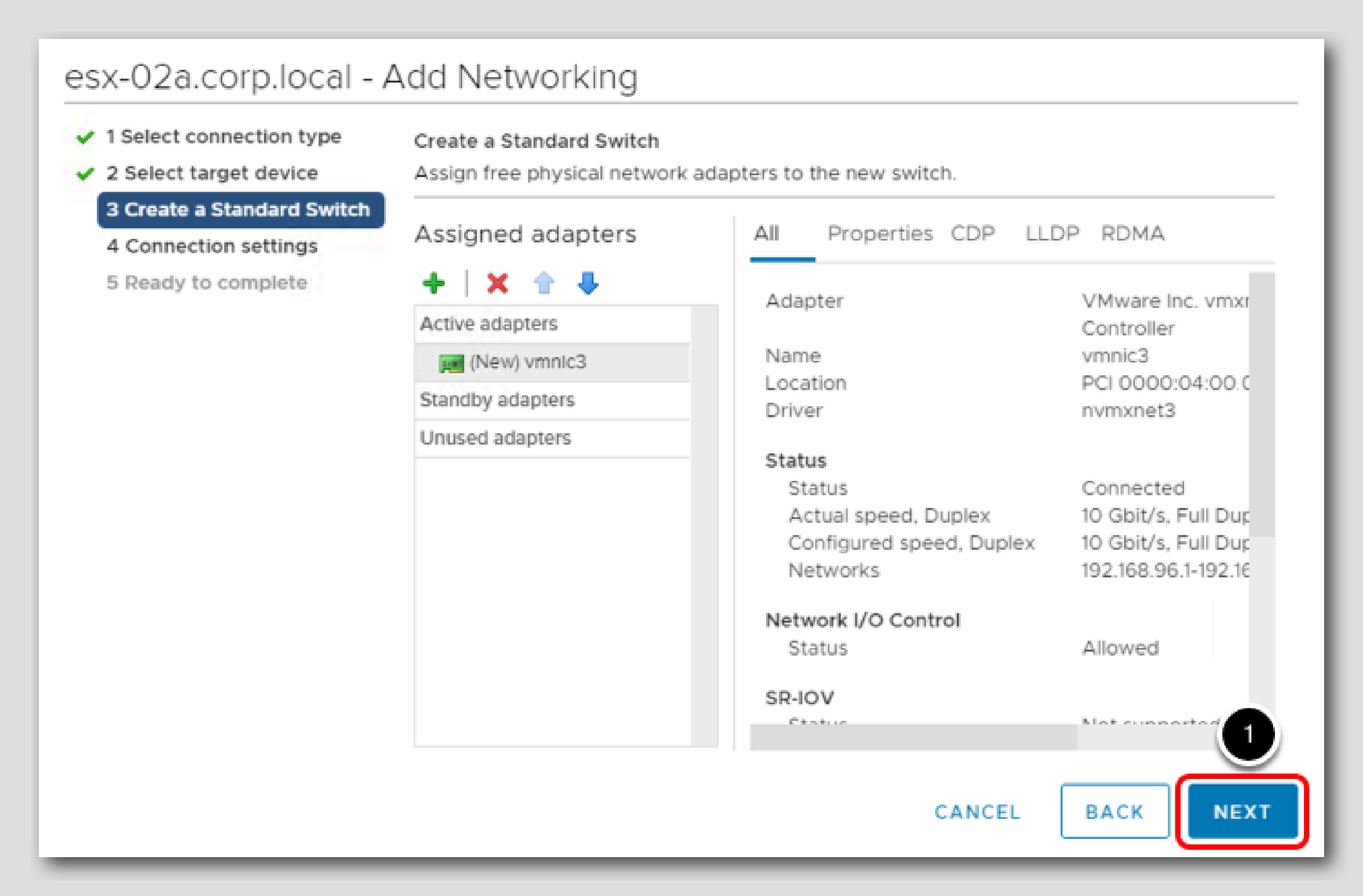
Link Layer Discovery Protocol

Link Layer Discovery Protocol is not available on this physical network adapter

Remote Direct Memory Access

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

Active adapters

(New) vmnic3

Standby adapters

Unused adapters

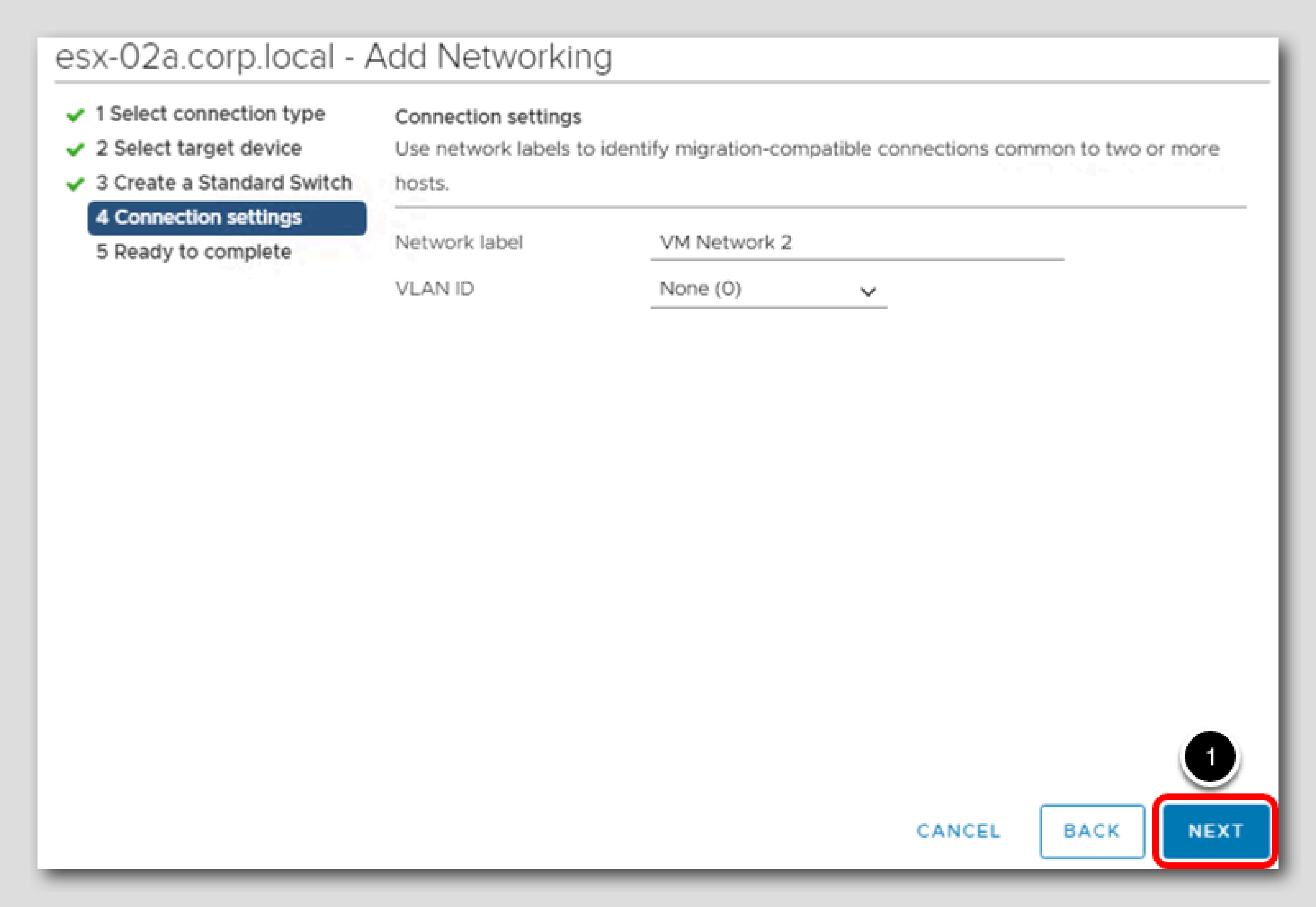
All | Properties | CDP | LLDP | RDMA

Adapter	VMware Inc. vmx Controller
Name	vmnic3
Location	PCI 0000:04:00.0
Driver	nvmxnet3
Status	
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full Dup
Configured speed, Duplex	10 Gbit/s, Full Dup
Networks	192.168.96.1-192.16
Network I/O Control	
Status	Allowed
SR-IOV	
Status	Not supported

1. Click Next to continue.

Connection Settings

[232]



esx-02a.corp.local - Add Networking

Connection settings

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

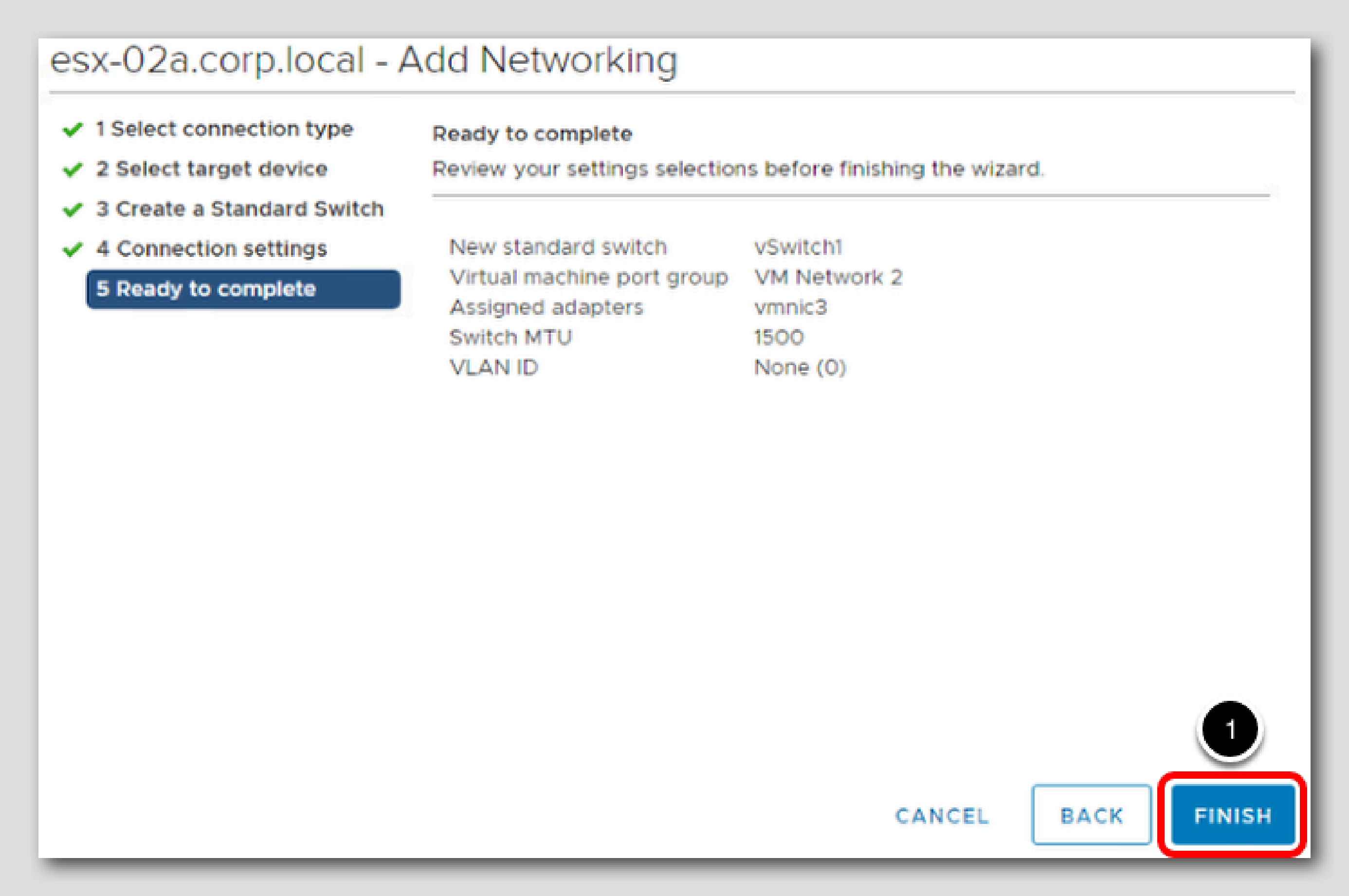
Network label: VM Network 2

VLAN ID: None (0)

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

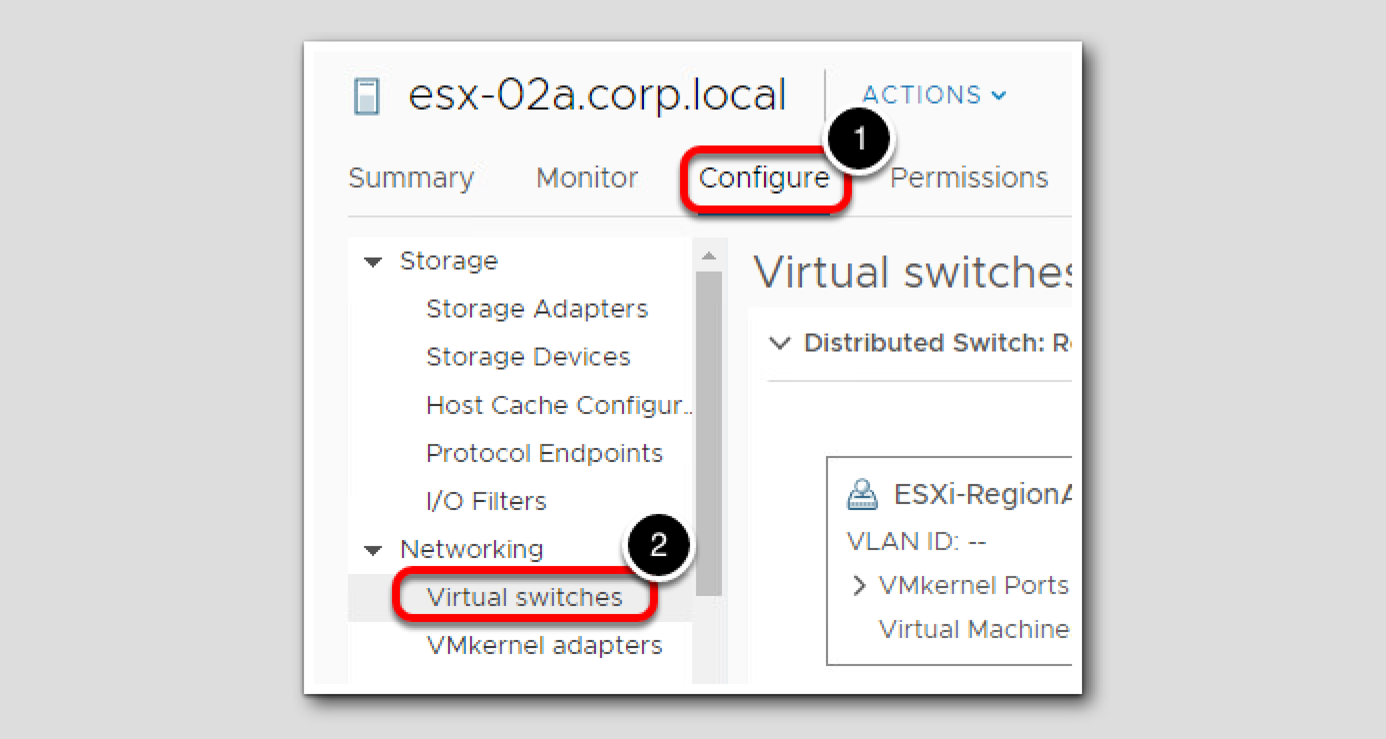
Ready to complete

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

Virtual Switches

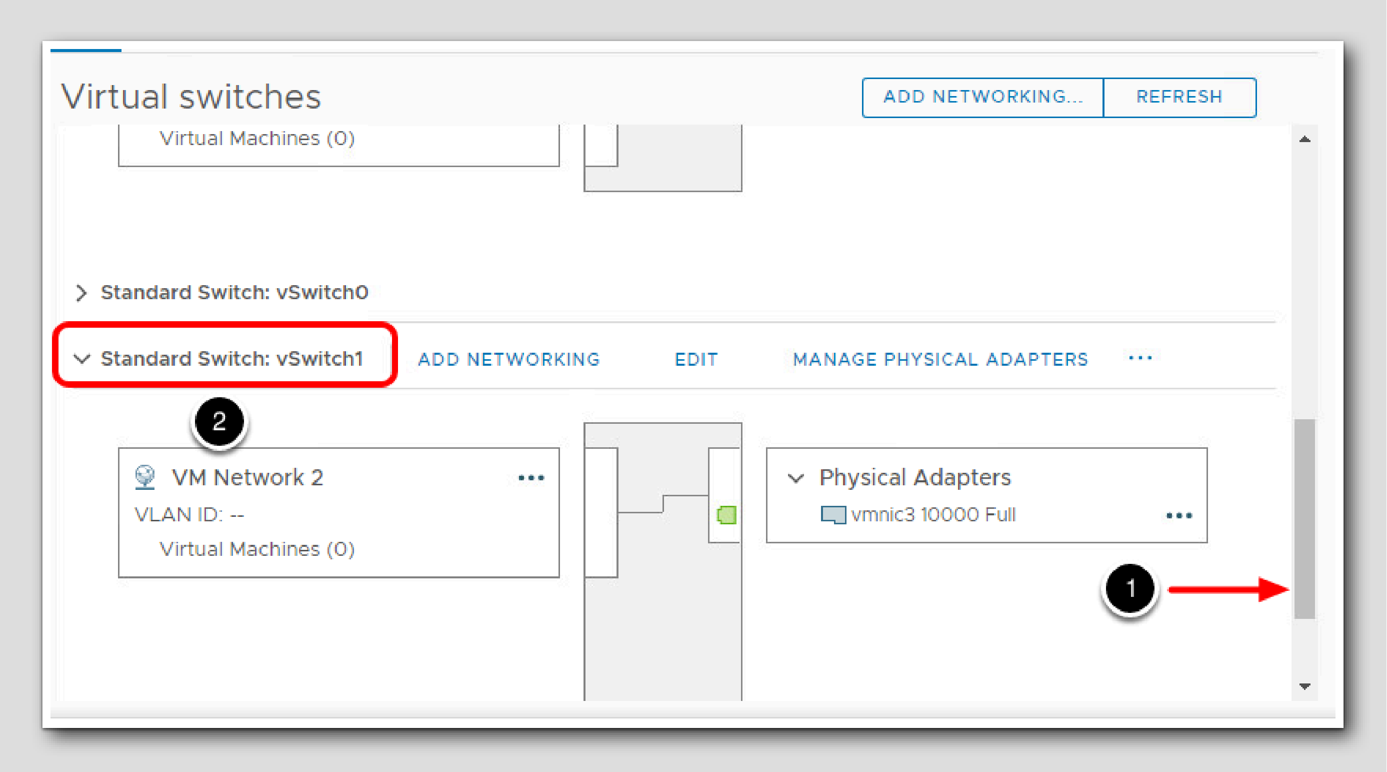


Next, we will verify the switch has been created.

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

Standard Switch: vSwitch1

[235]



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.

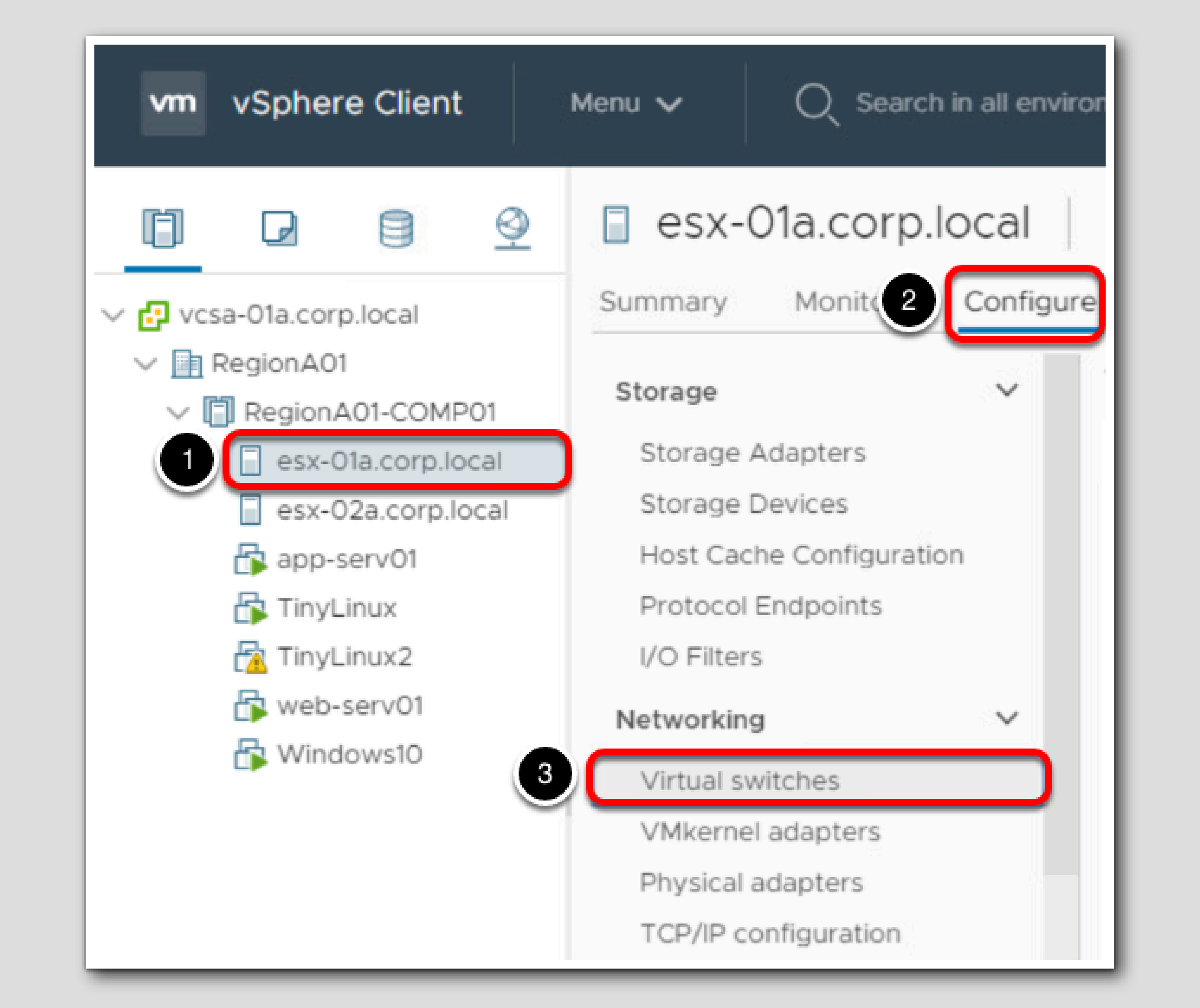
Editing a Standard Switch in the vSphere Web Client

[236]

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.

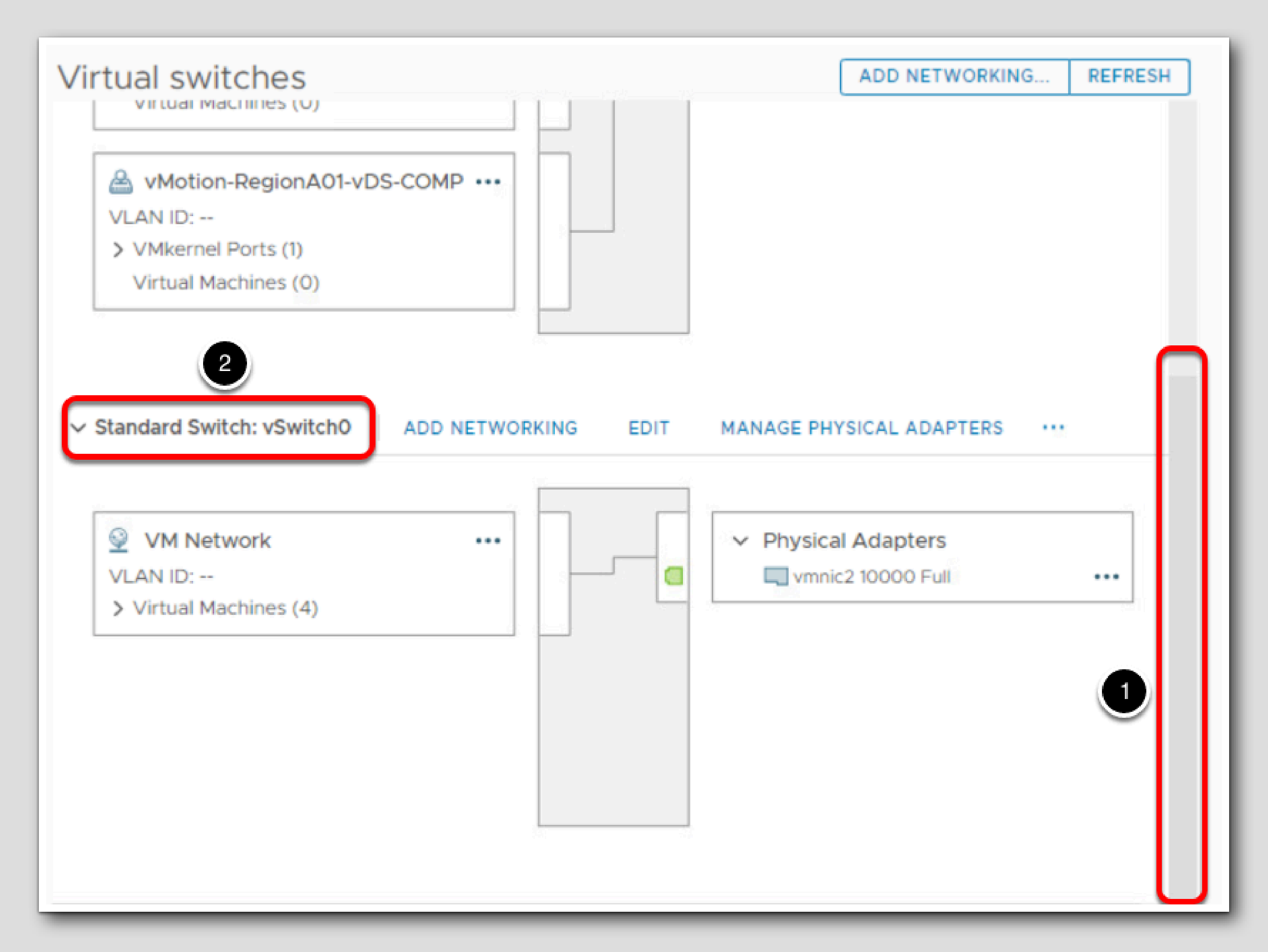
Select esxi-01a.corp.local



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

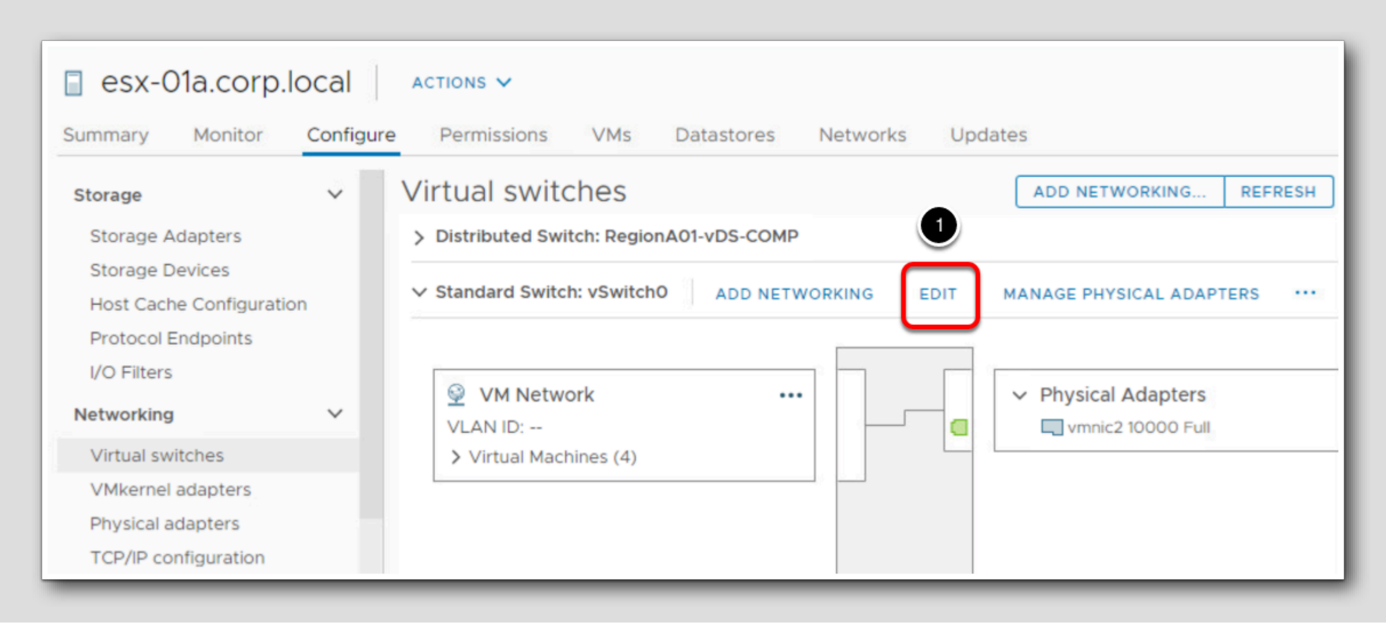
Select vSwitch0

[238]



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.

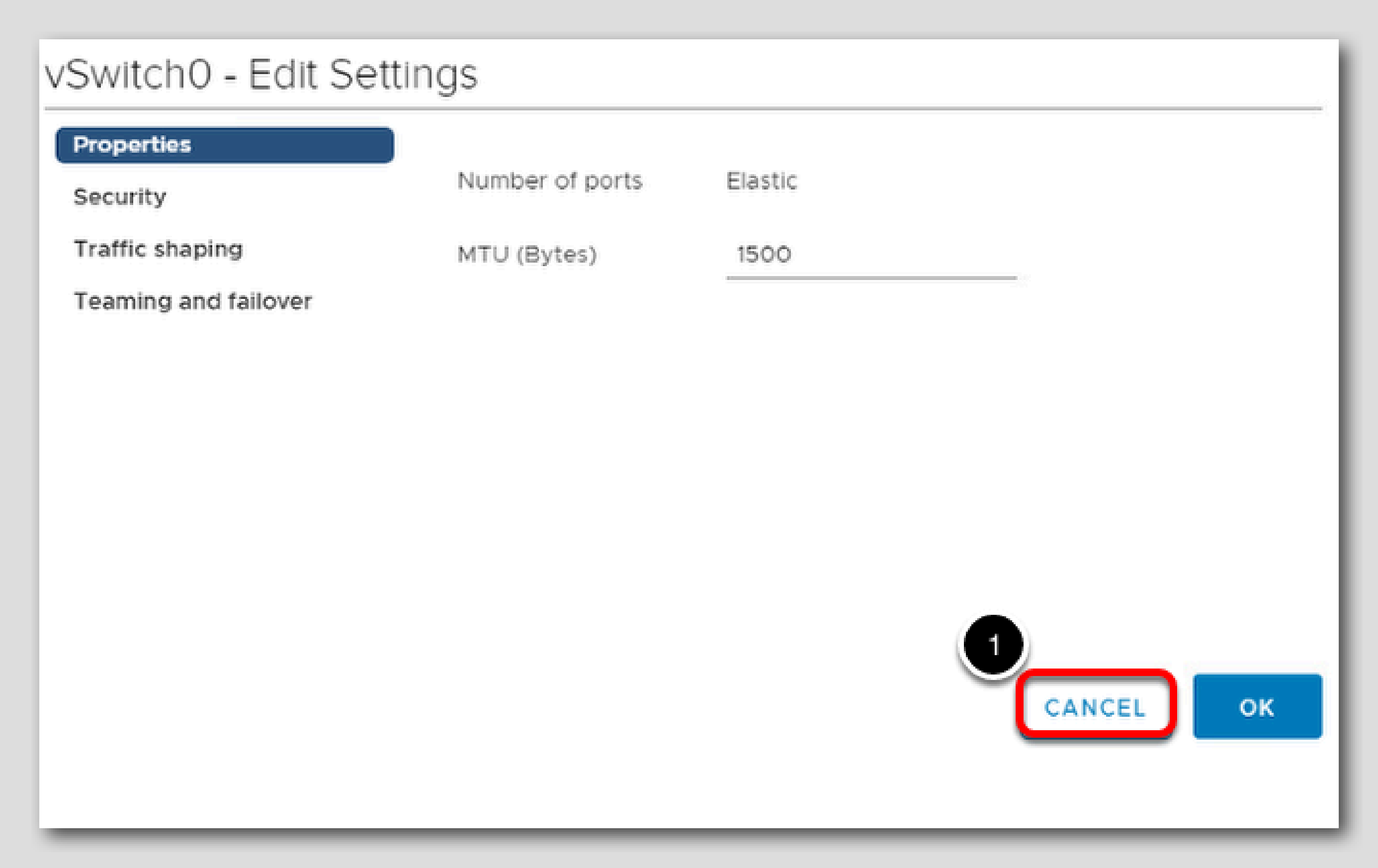
Edit vSwitch1



1. Click Edit.

Properties (MTU Setting)

[240]



vSwitch0 - Edit Settings

Number of ports: Elastic

MTU (Bytes): 1500

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.

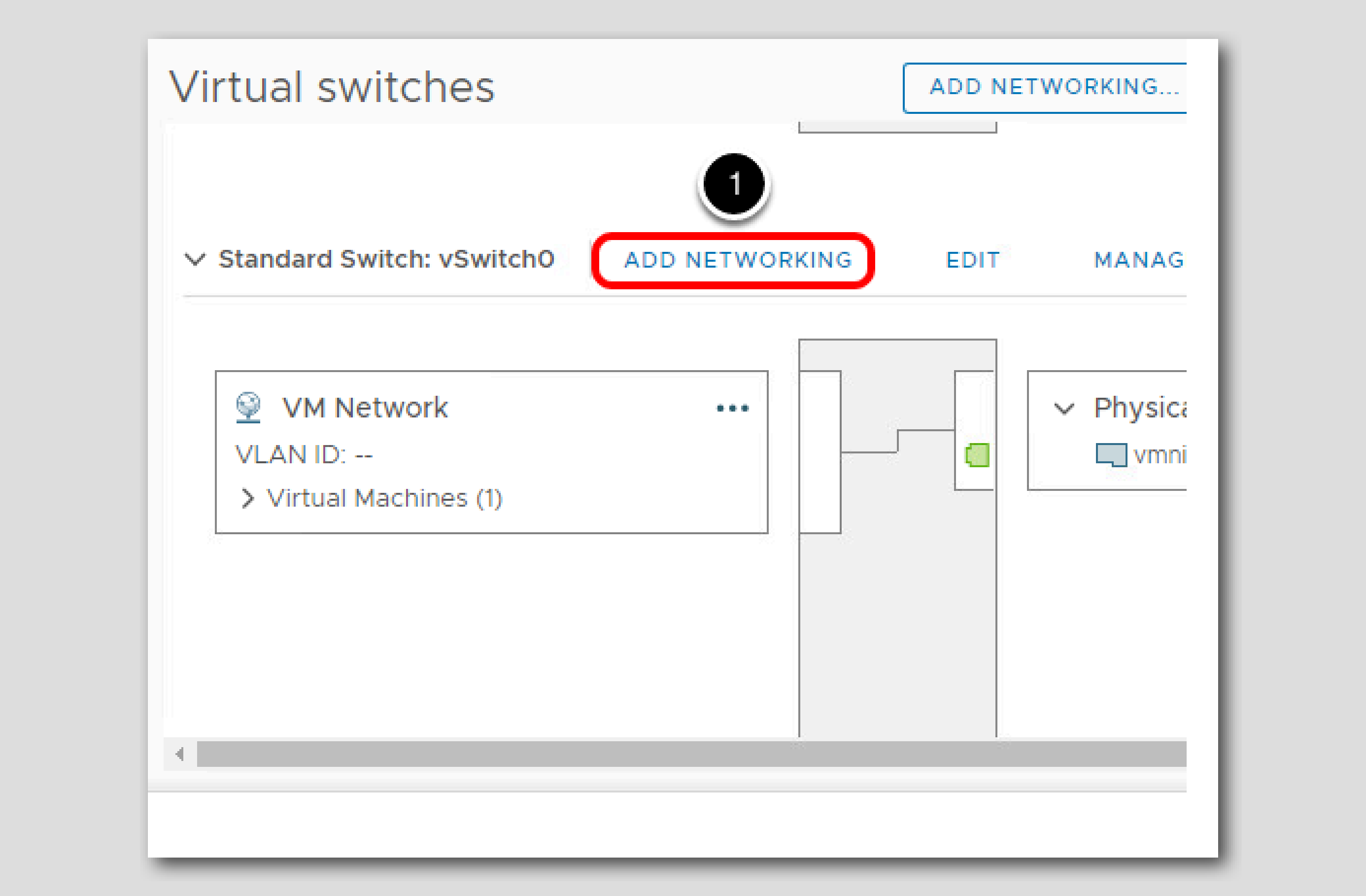
Add Uplink Adapters in the vSphere Web Client

[241]

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

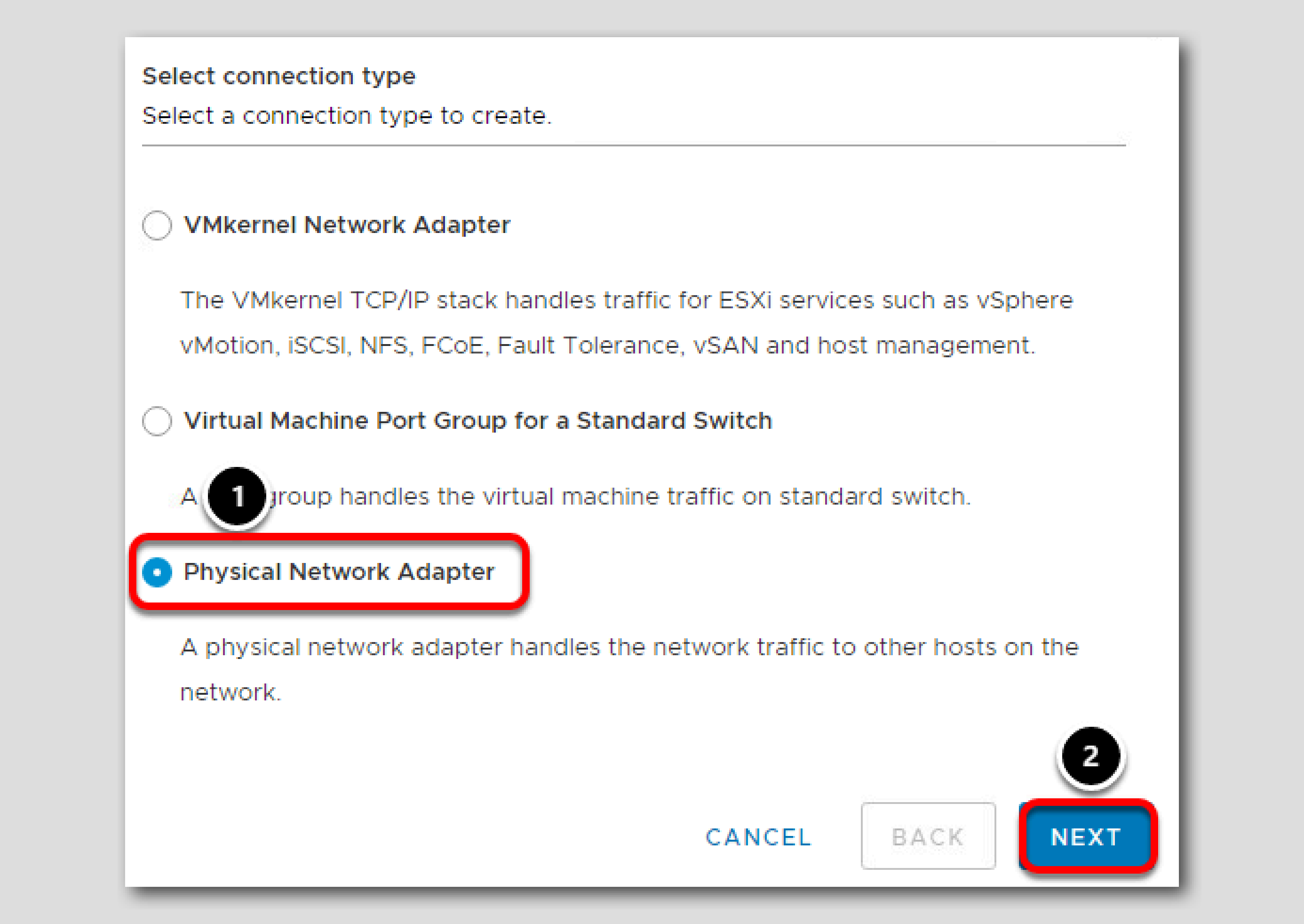
[242]



1. Click Add Networking

Select Connection Type

[243]



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 group handles the virtual machine traffic on standard switch.

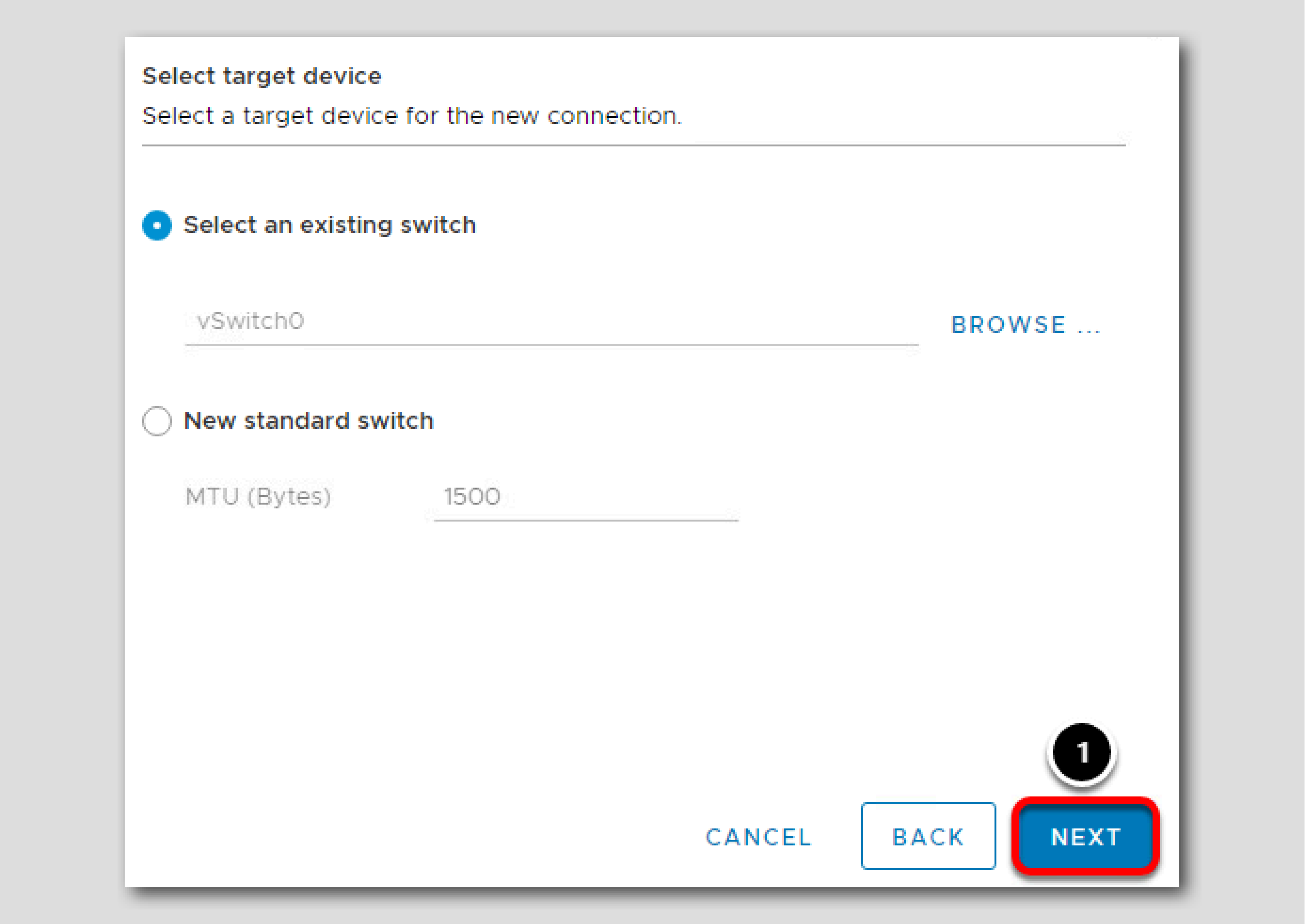
● Physical Network Adapter

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

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

Select Target Device

[244]



Select target device

Select a target device for the new connection.

● Select an existing switch

vSwitch0

○ New standard switch

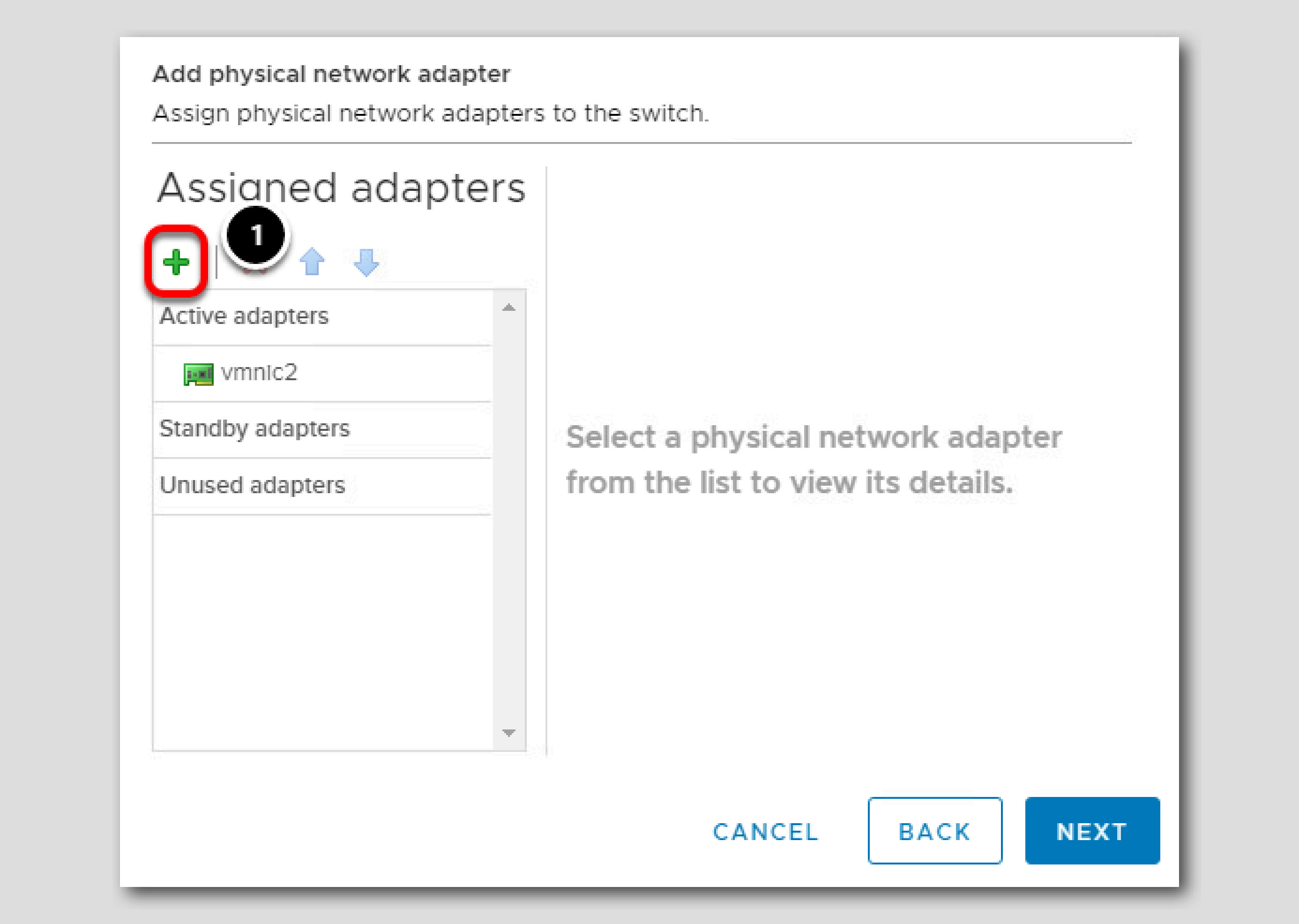
MTU (Bytes) 1500

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

1. Click **Next**.

Add Networking

[245]

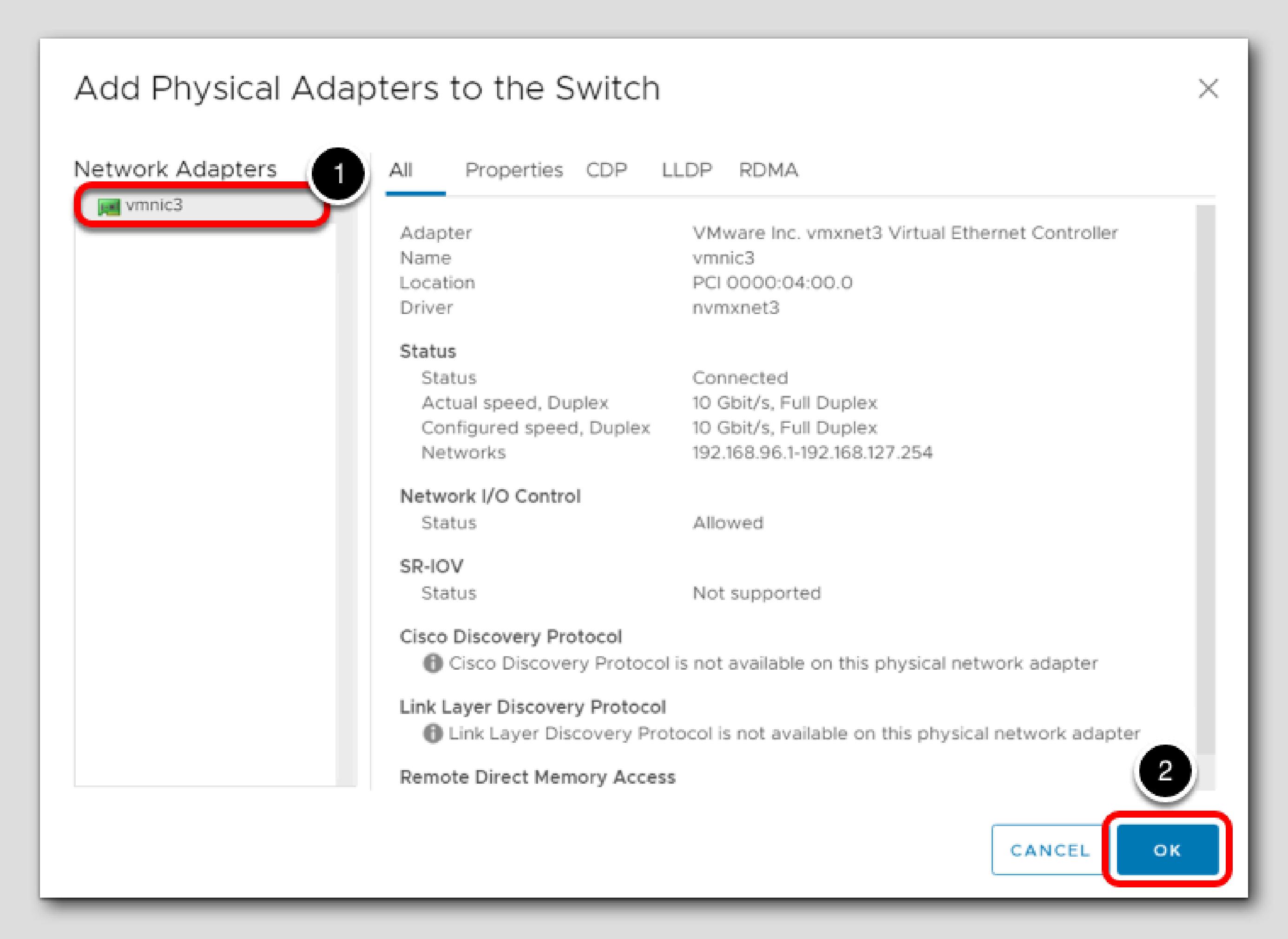


Add physical network adapter

Assign physical network adapters to the switch.

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

Add vmnic3



Add Physical Adapters to the Switch

Adapter	VMware Inc. vmxnet3 Virtual Ethernet Controller
Name	vmnic3
Location	PCI 0000:04:00.0
Driver	nvmxnet3
Status	
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full Duplex
Configured speed, Duplex	10 Gbit/s, Full Duplex
Networks	192.168.96.1-192.168.127.254
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

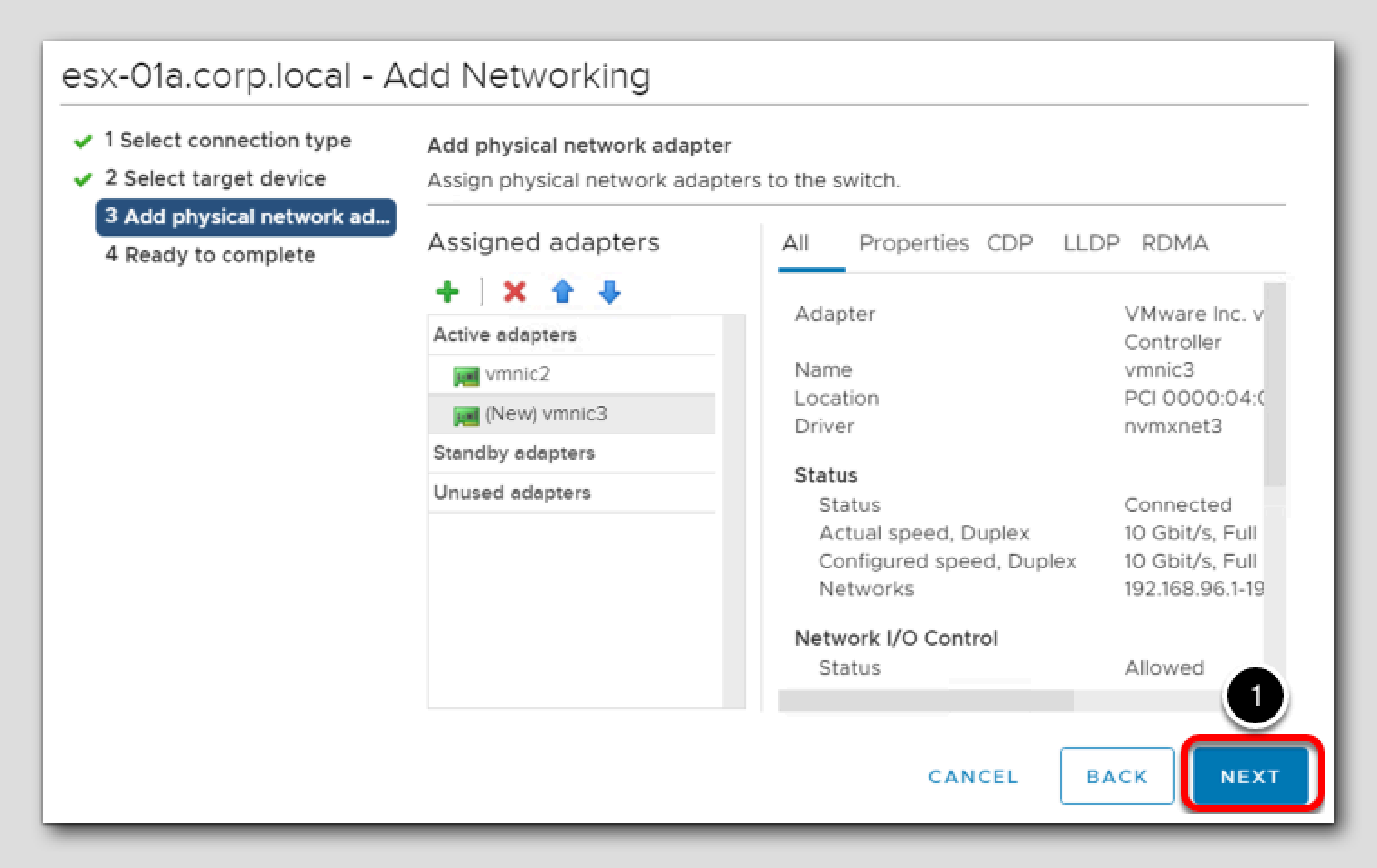
Link Layer Discovery Protocol is not available on this physical network adapter

Remote Direct Memory Access

1. Click on vmnic3
2. Click OK

Assigned Adapters

[247]



esx-01a.corp.local - Add Networking

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

Add physical network adapter

Assign physical network adapters to the switch.

Assigned adapters

Active adapters
- vmnic2
- (New) vmnic3

Standby adapters

Unused adapters

All | Properties | CDP | LLDP | RDMA

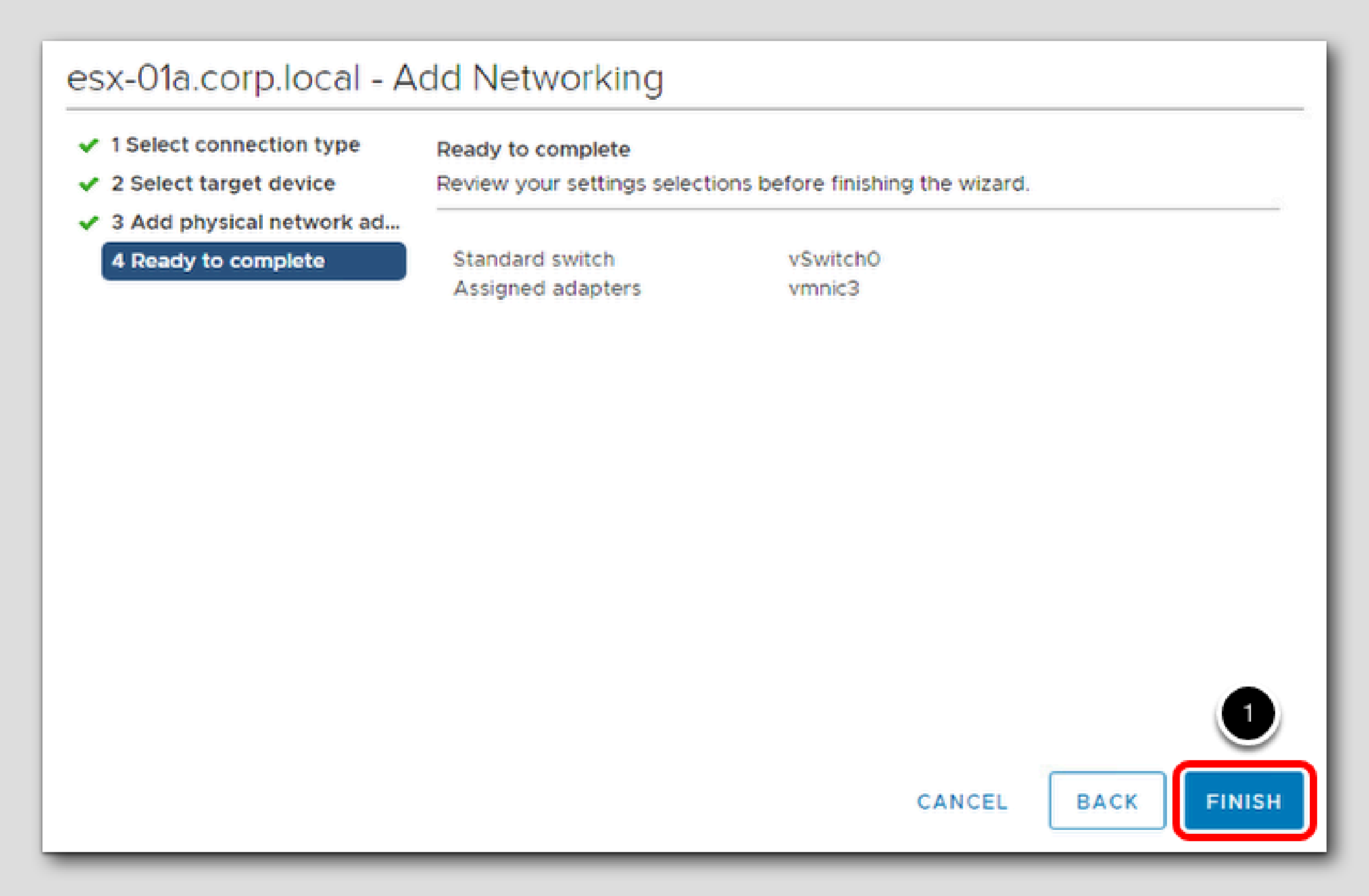
Adapter	VMware Inc. v Controller
Name	vmnic3
Location	PCI 0000:04:(
Driver	nvmxnet3
Status	
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full
Configured speed, Duplex	10 Gbit/s, Full
Networks	192.168.96.1-19
Network I/O Control	
Status	Allowed

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

[248]



esx-01a.corp.local - Add Networking

Ready to complete

Review your settings selections before finishing the wizard.

Standard switch vSwitch0
Assigned adapters vmnic3

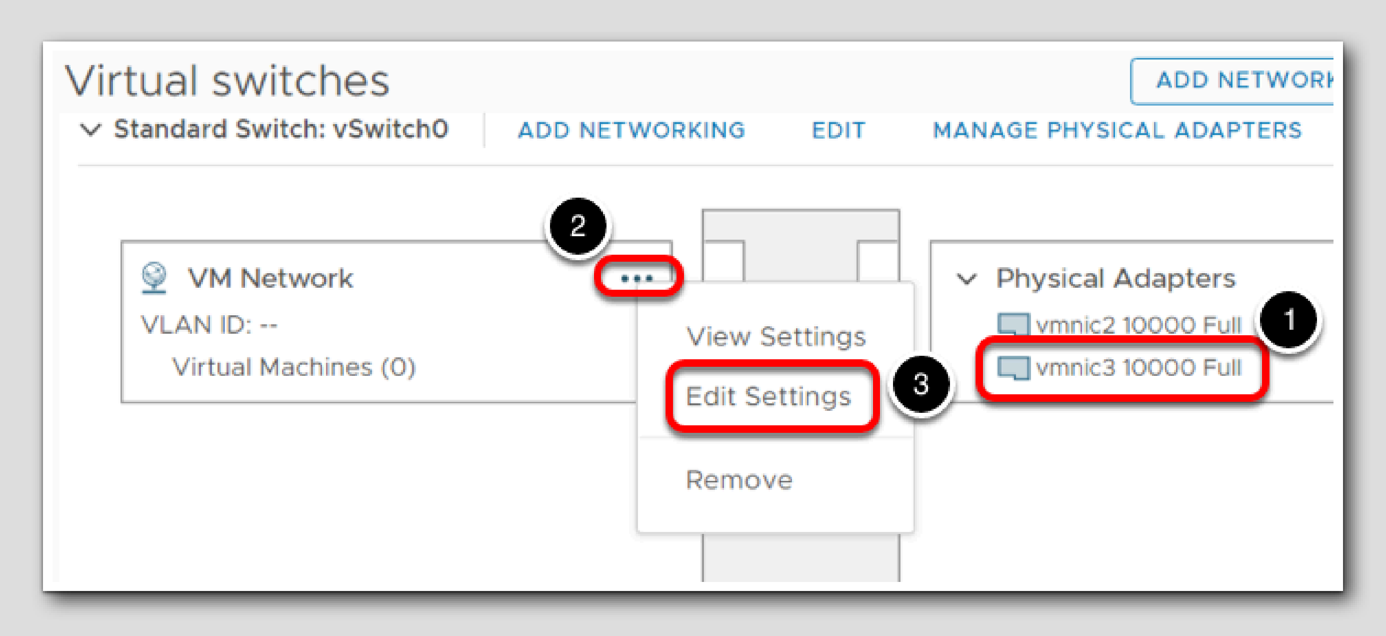
Click **Finish** to add vmnic3 to vSwitch0.

Editing a Standard Switch Port Group

[249]

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

New vmnic Added



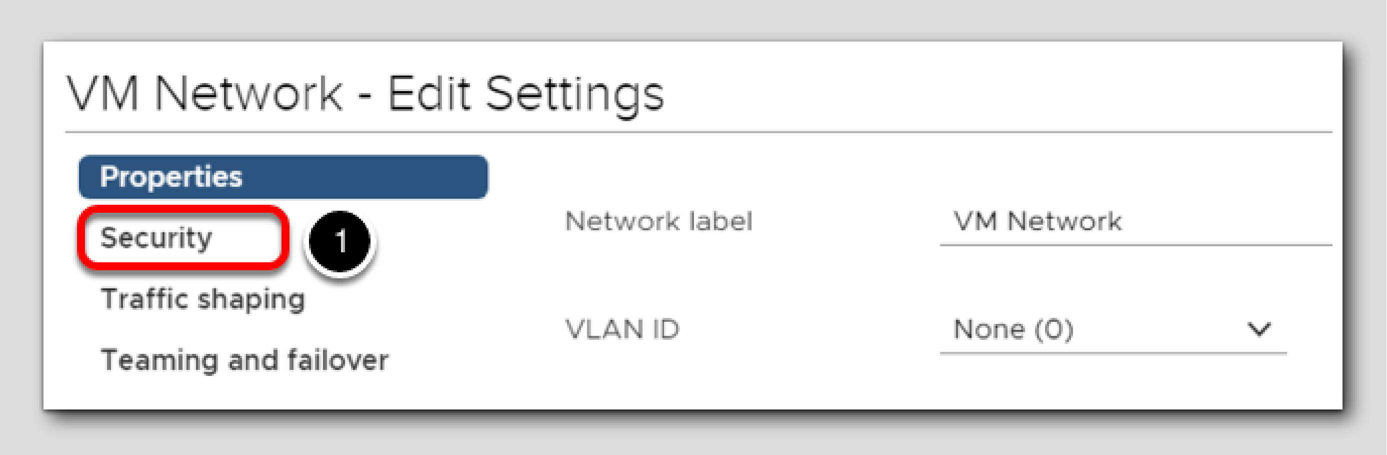
1. In the Physical Adapters section, vmnic3 has been added to the switch.

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

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

Port Group Properties

[251]



Network label VM Network

VLAN ID None (0)

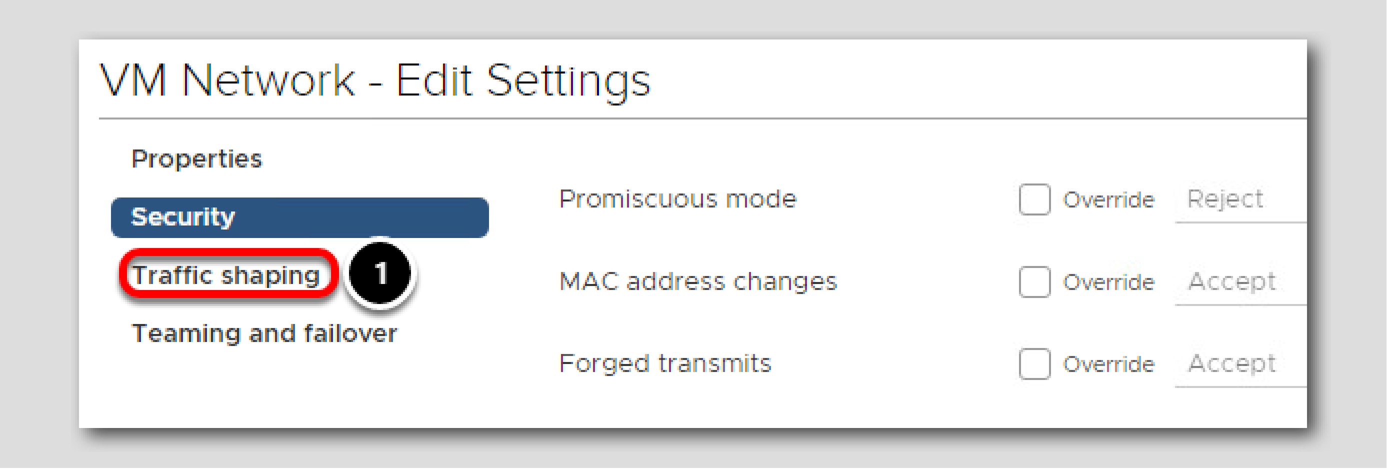
The Properties setting section is where the name or VLAN ID of the port group can be modified.

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

1. Click Security.

Port Group Security

[252]



Promiscuous mode □ Override Reject

MAC address changes □ Override Accept

Forged transmits □ 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

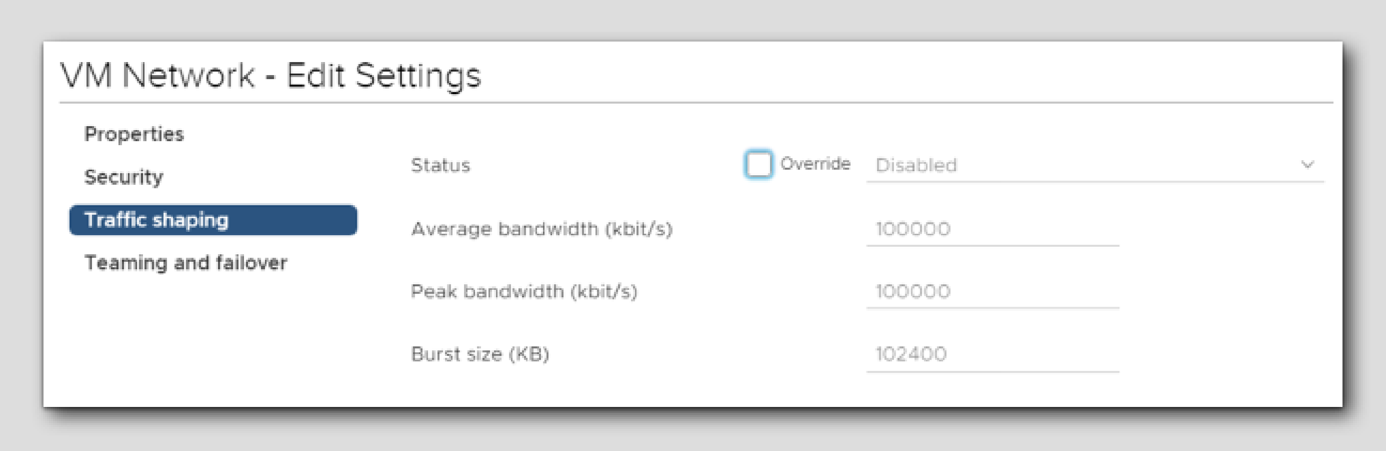
- Reject — Any outbound frame with a source MAC address that is different from the one currently set on the adapter are dropped.
- Accept — No filtering is performed and all outbound frames are passed.

No changes are needed here.

1. Click Traffic shaping.

Traffic Shaping

[253]



VM Network - Edit Settings

Status □ Override Disabled

Average bandwidth (kbit/s) 100000

Peak bandwidth (kbit/s) 100000

Burst size (KB) 102400

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

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

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

Average Bandwidth

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

Peak Bandwidth

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

Burst Size

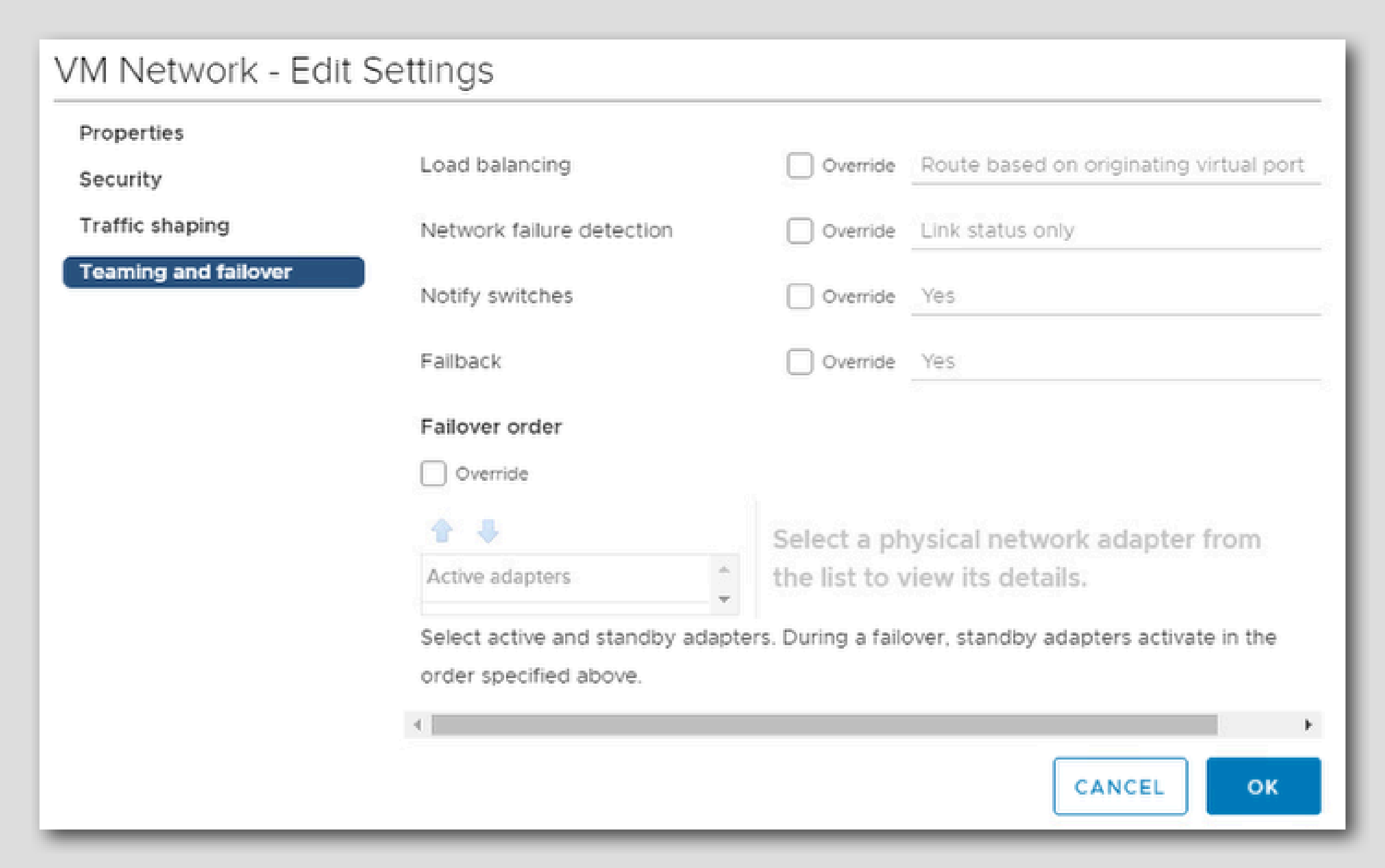
- Maximum number of bytes to allow in a burst. If this parameter is set, a port might gain a burst bonus if it does not use all its allocated bandwidth. When the port needs more bandwidth than specified by the average bandwidth, it might be allowed to temporarily transmit data at a higher speed if a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

No changes are needed here.

1. Clicking Teaming and failover.

Teaming and Failover

[254]



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
Failback	□ 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.

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.

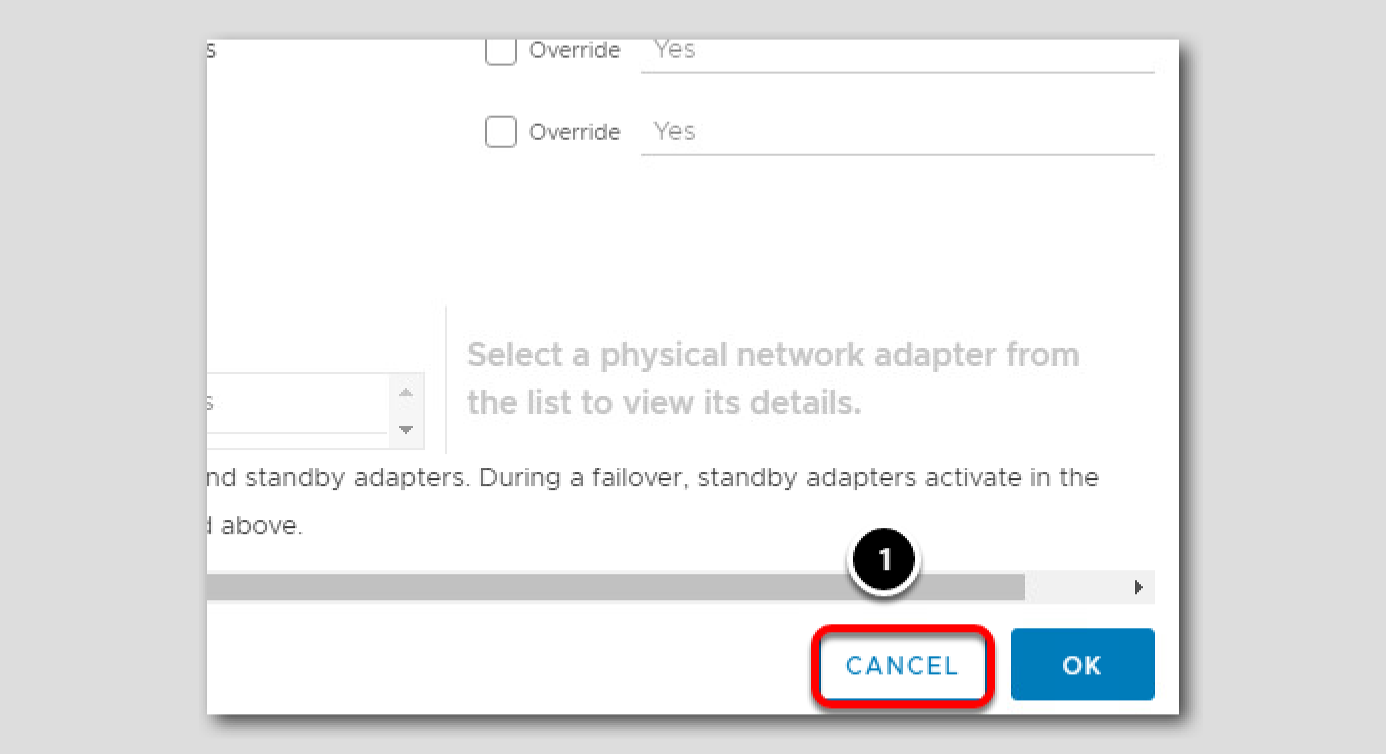
- If failback is set to Yes, the default selection, the adapter is returned to active duty immediately upon recovery, displacing the standby adapter that took over its slot, if any.
- If failback is set to No for a standard port, a failed adapter is left inactive after recovery until another currently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

[255]

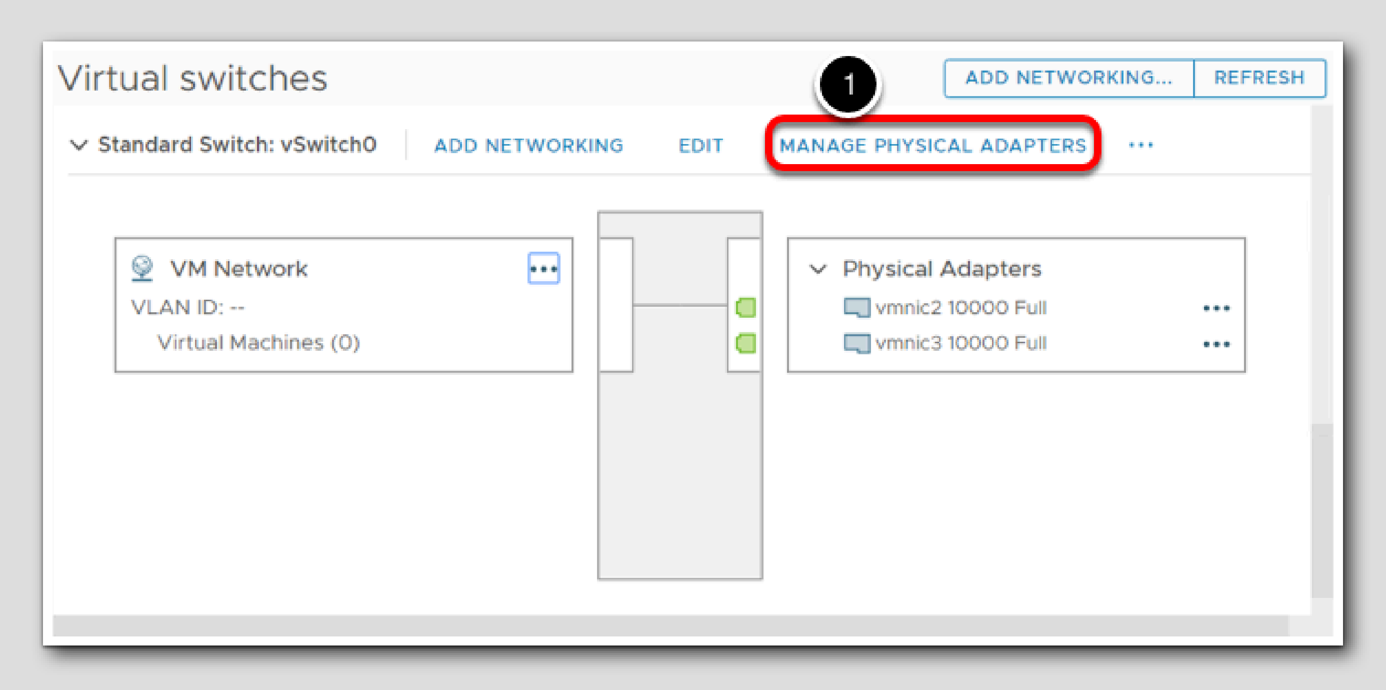


□ Override Yes
□ Override Yes
Select a physical network adapter from the list to view its details.
nd standby adapters. During a failover, standby adapters activate in the
d above.
1
CANCEL
OK

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

Removing a Physical Adapter

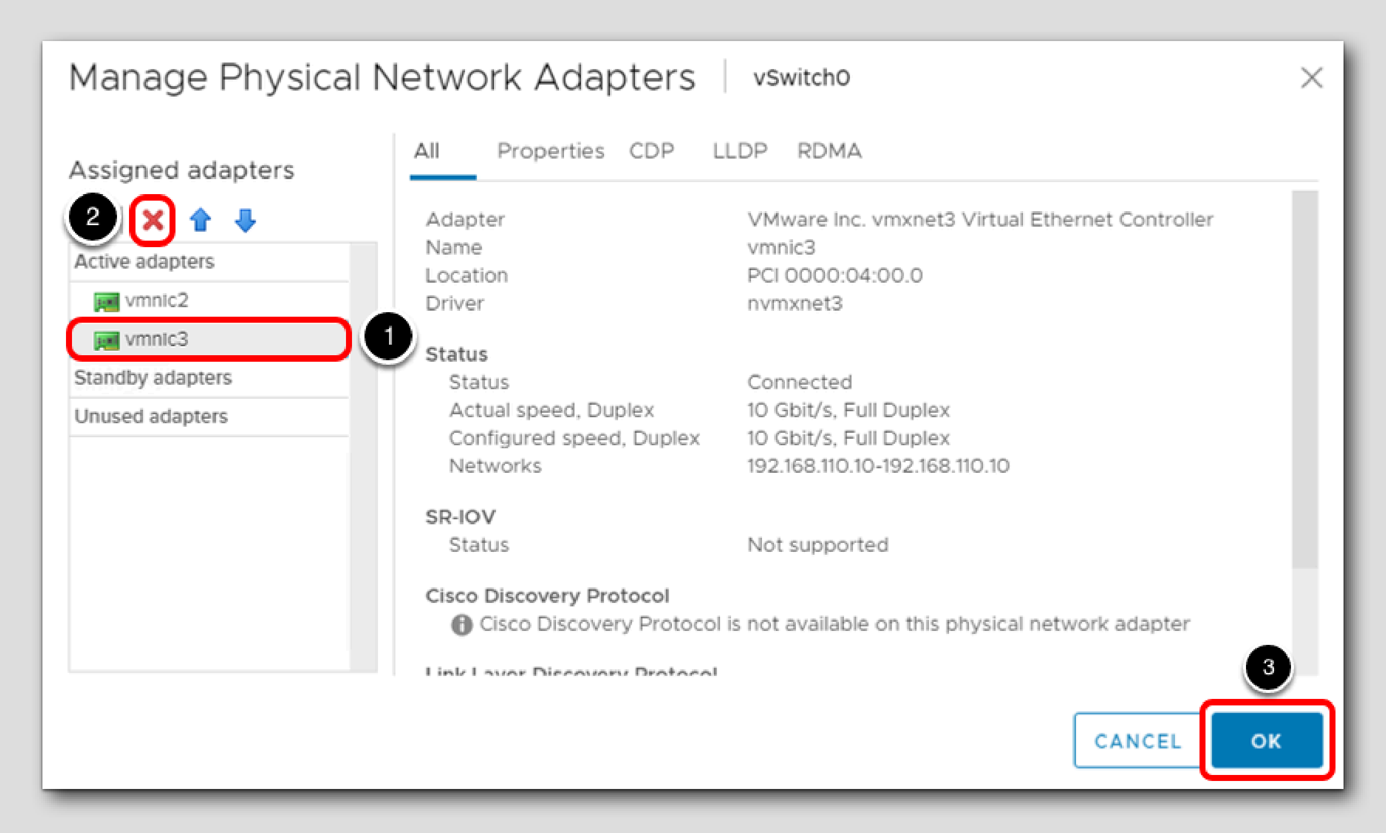
[256]



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

Remove vmnic3

[257]


Manage Physical Network Adapters | vSwitch0

Assigned adapters

Active adapters
vmnic2
vmnic3
Standby adapters
Unused adapters

All | Properties | CDP | LLDP | RDMA

Adapter VMware Inc. vmxnet3 Virtual Ethernet Controller
Name vmnic3
Location PCI 0000:04:00.0
Driver nvmxnet3

Status
Status Connected
Actual speed, Duplex 10 Gbit/s, Full Duplex
Configured speed, Duplex 10 Gbit/s, Full Duplex
Networks 192.168.110.10-192.168.110.10

SR-IOV
Status Not supported

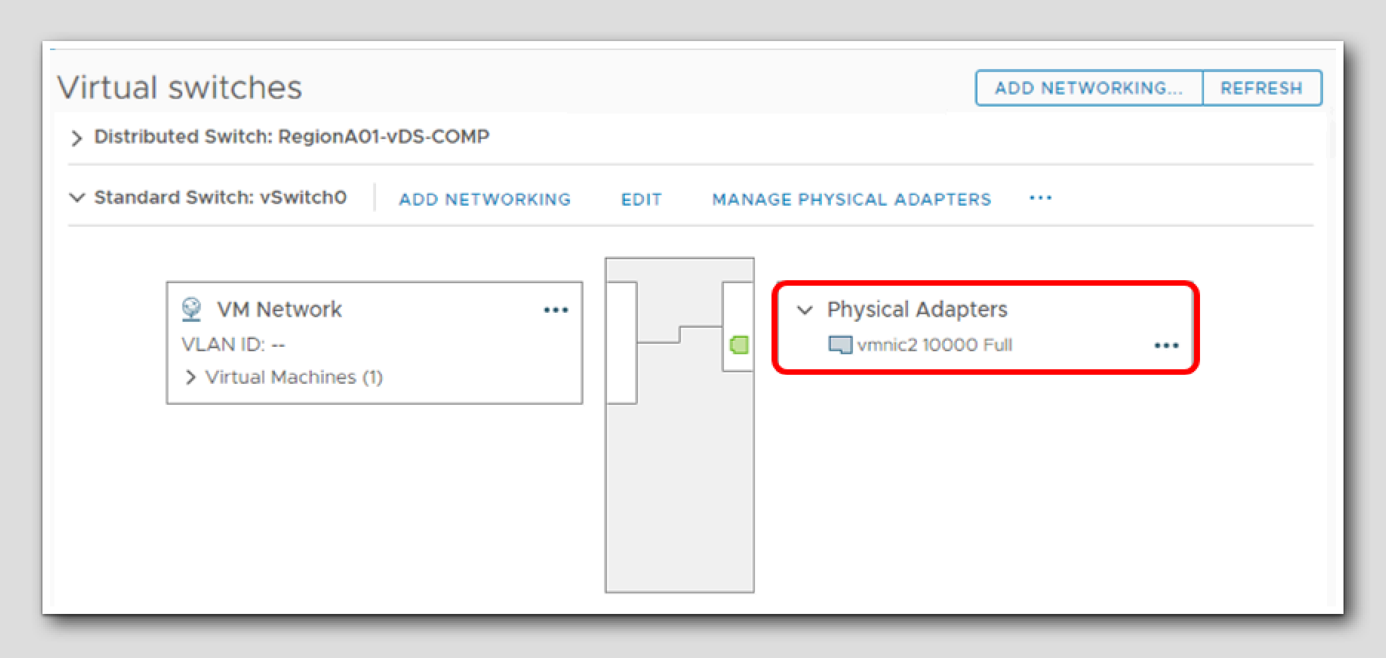
Cisco Discovery Protocol
Cisco Discovery Protocol is not available on this physical network adapter

Link Layer Discovery Protocol

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

Adapter Removed

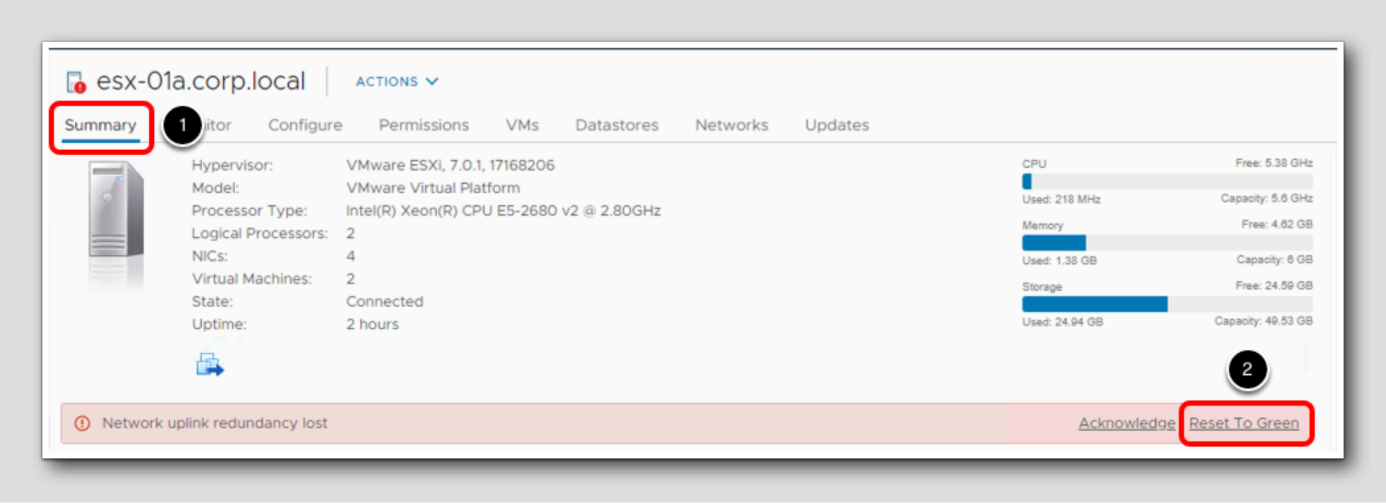
[258]



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

Clear Alerts

[259]

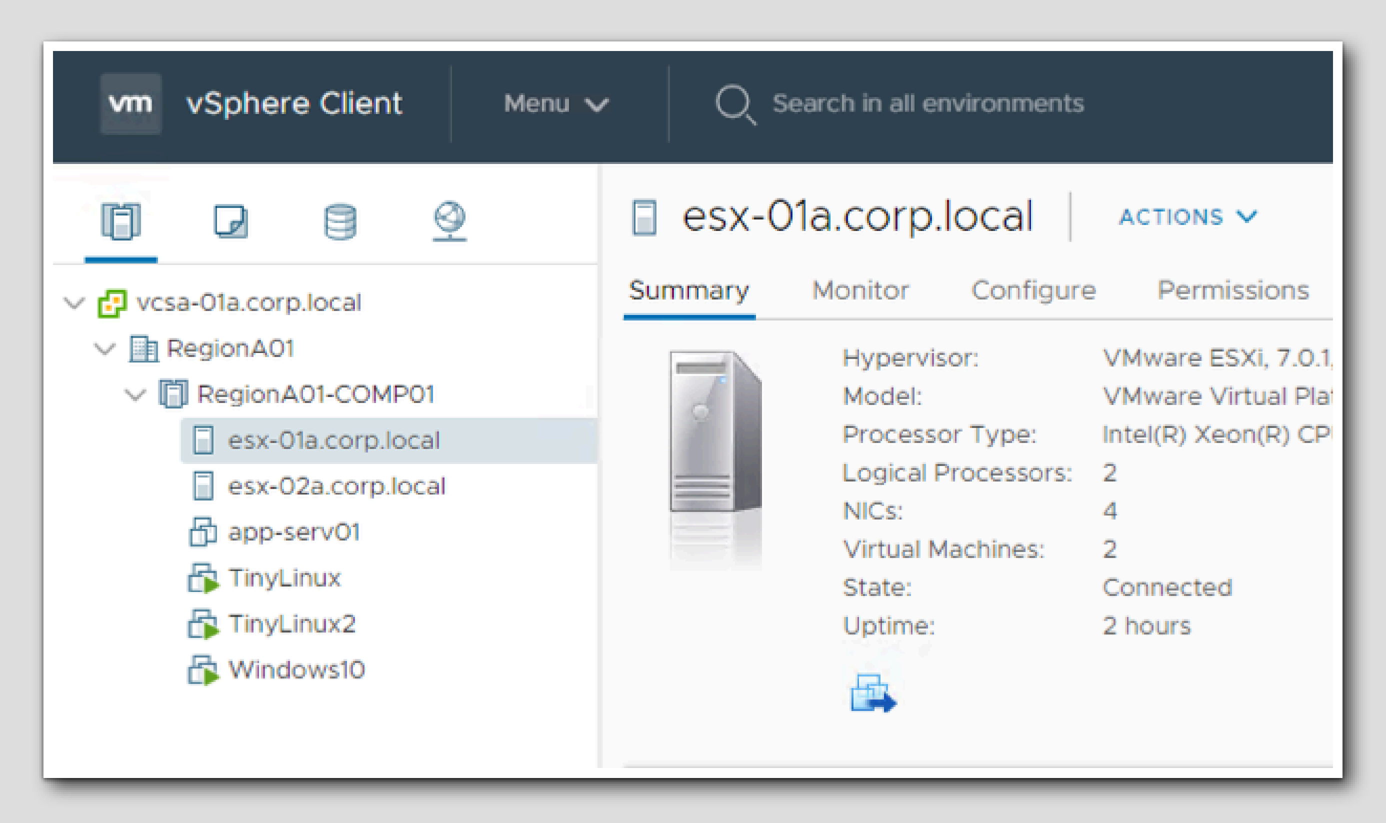


Hypervisor: VMware ESXi, 7.0.1, 17168206
Model: VMware Virtual Platform
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 2
NICs: 4
Virtual Machines: 2
State: Connected
Uptime: 2 hours

Network uplink redundancy lost

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

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

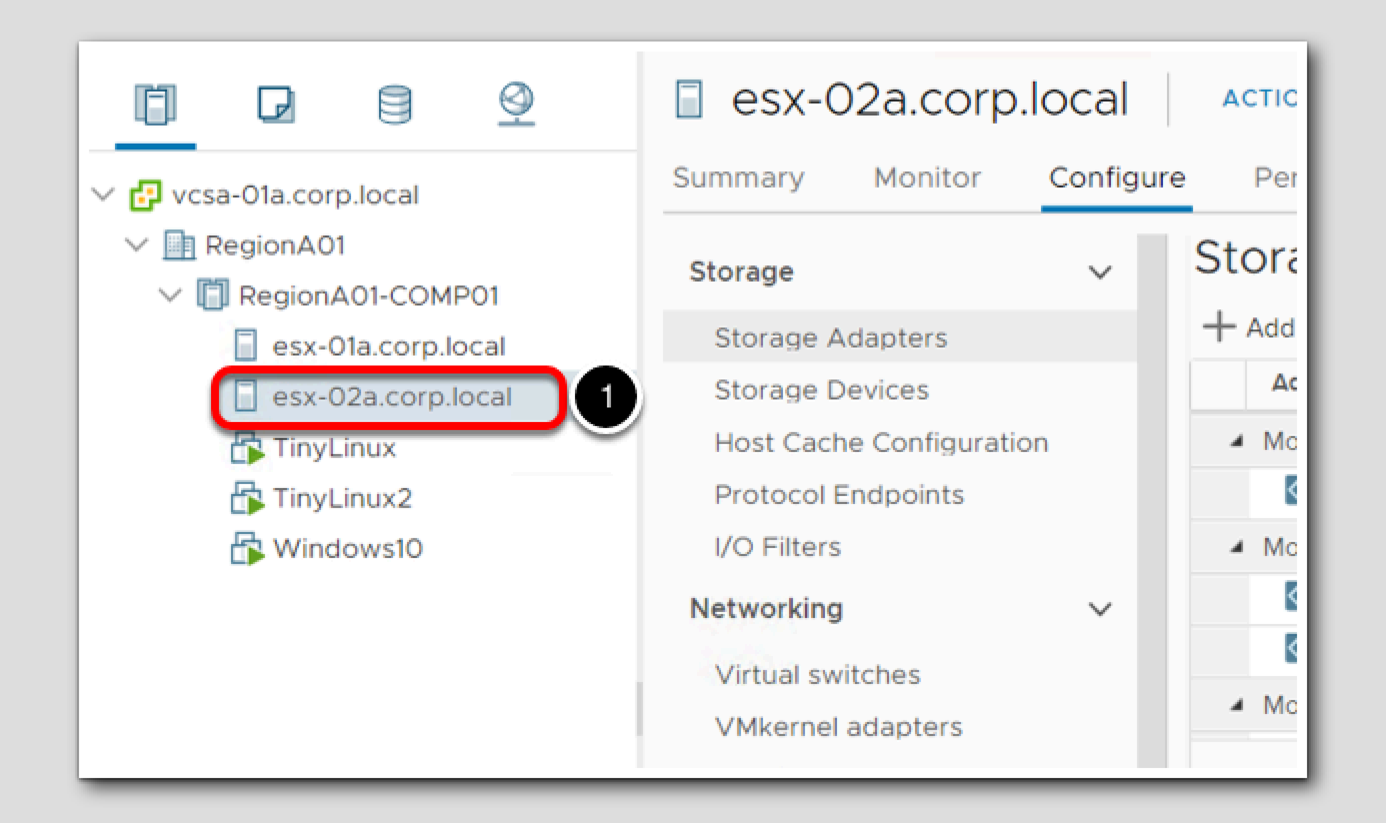


Hypervisor: VMware ESXi, 7.0.1,
Model: VMware Virtual Pla
Processor Type: Intel(R) Xeon(R) CP
Logical Processors: 2
NICs: 4
Virtual Machines: 2
State: Connected
Uptime: 2 hours

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

Deleting a Standard Switch

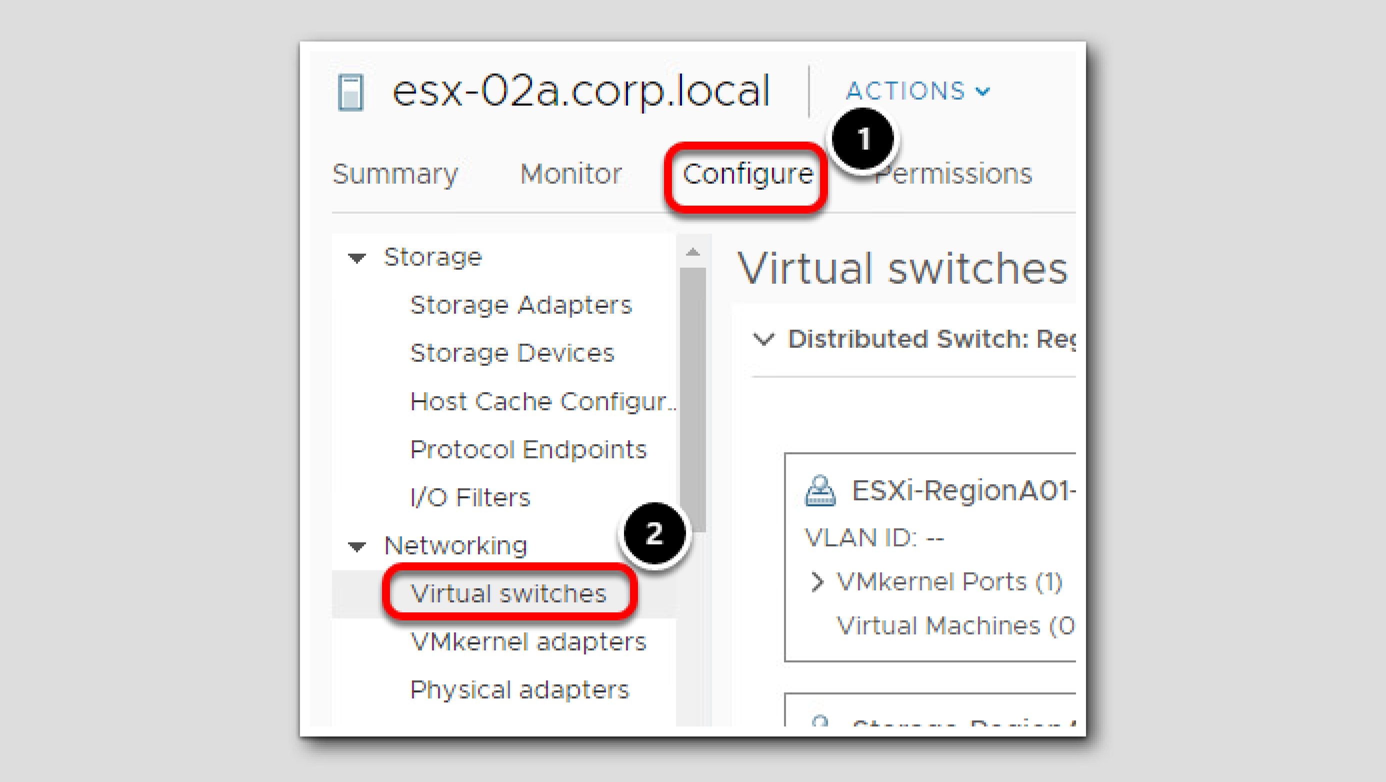
[260]



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

Virtual Switches

[261]

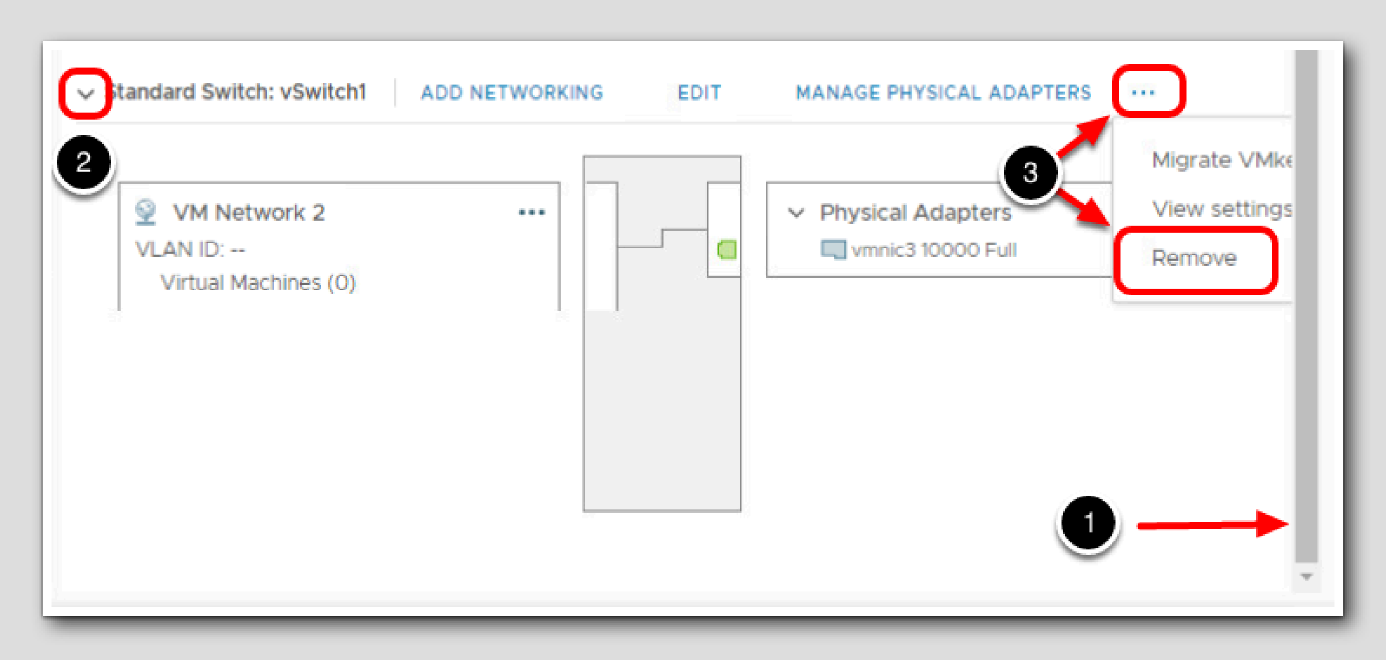


In preparation for the next lesson, we will delete the Standard Switch we created on esx-02a.corp.local.

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

Standard Switch: vSwitch1

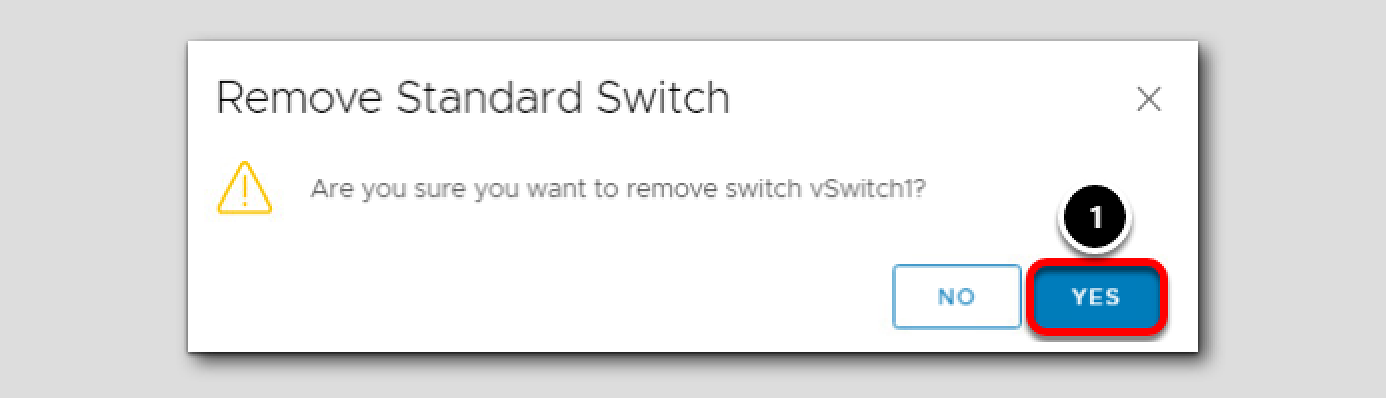
[262]



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

[263]



1. Click Yes to remove vSwitch1.

Conclusion

[264]

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

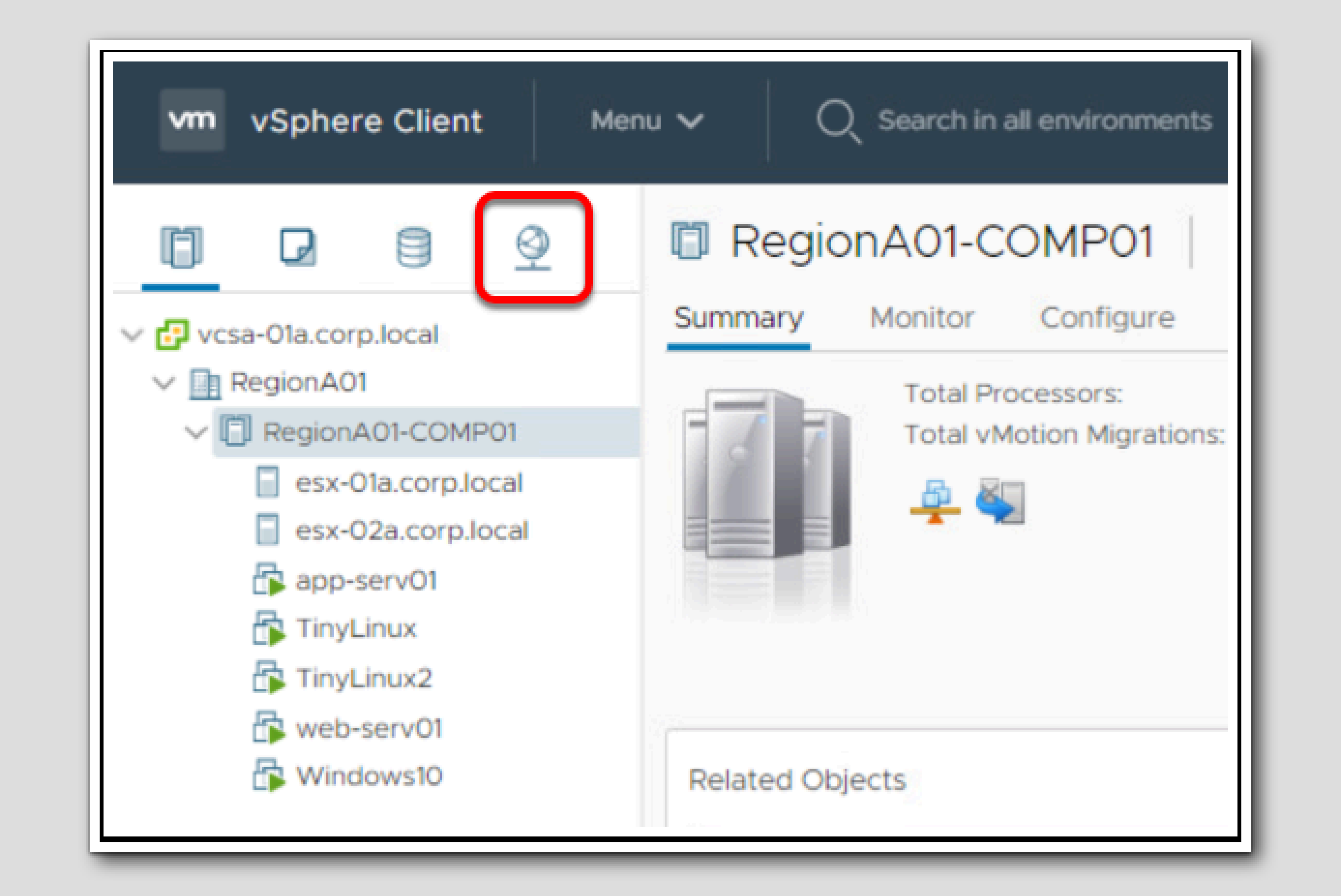
[265]

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

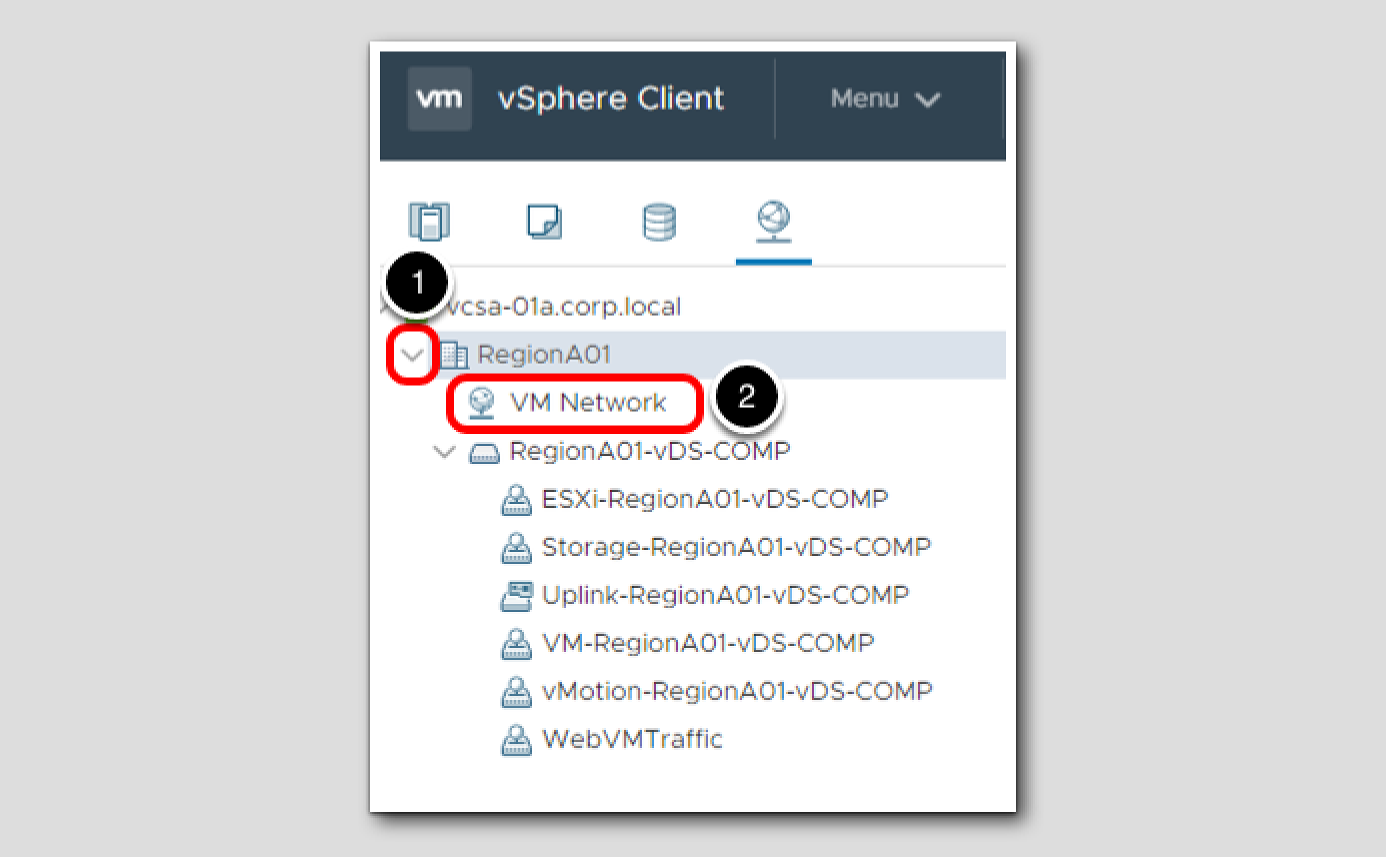
[266]



1. Click on the **Networking** icon

View Standard vSwitch

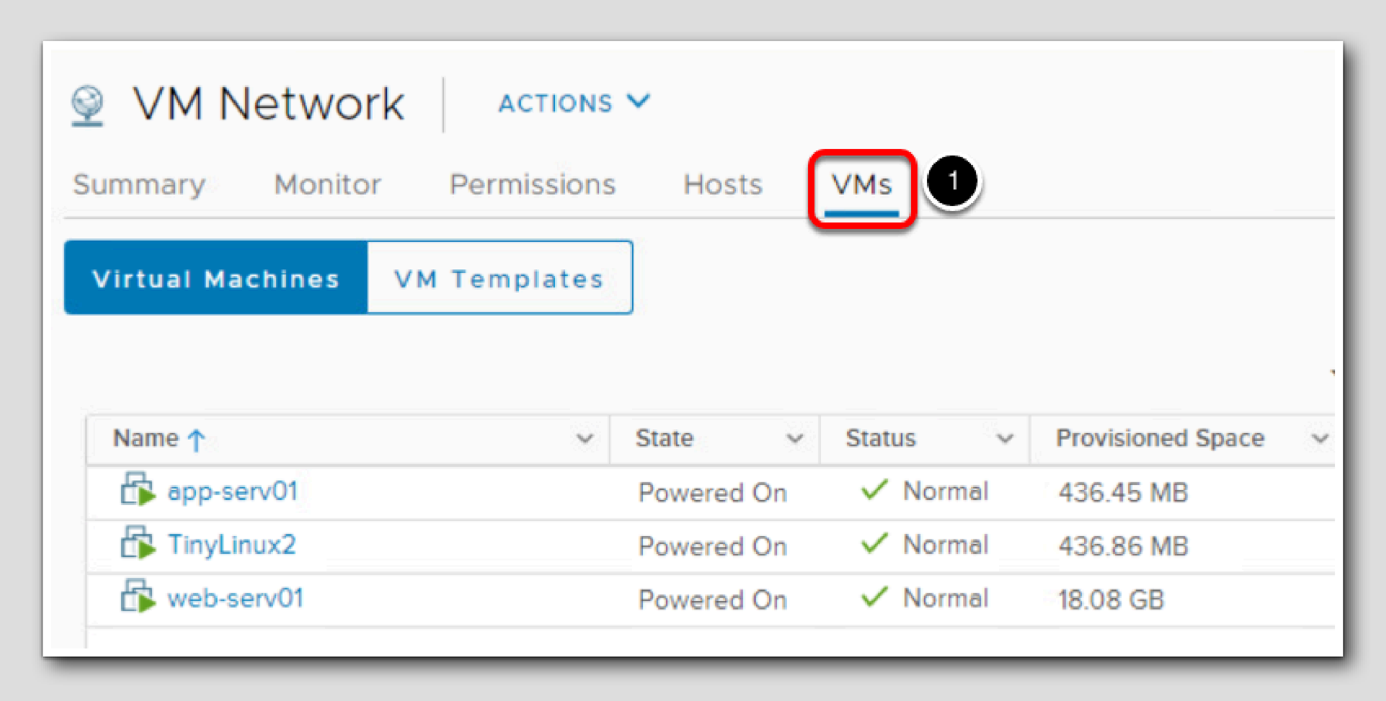
[267]



1. Expand RegionA01
2. Select VM Network

VM Network

[268]



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

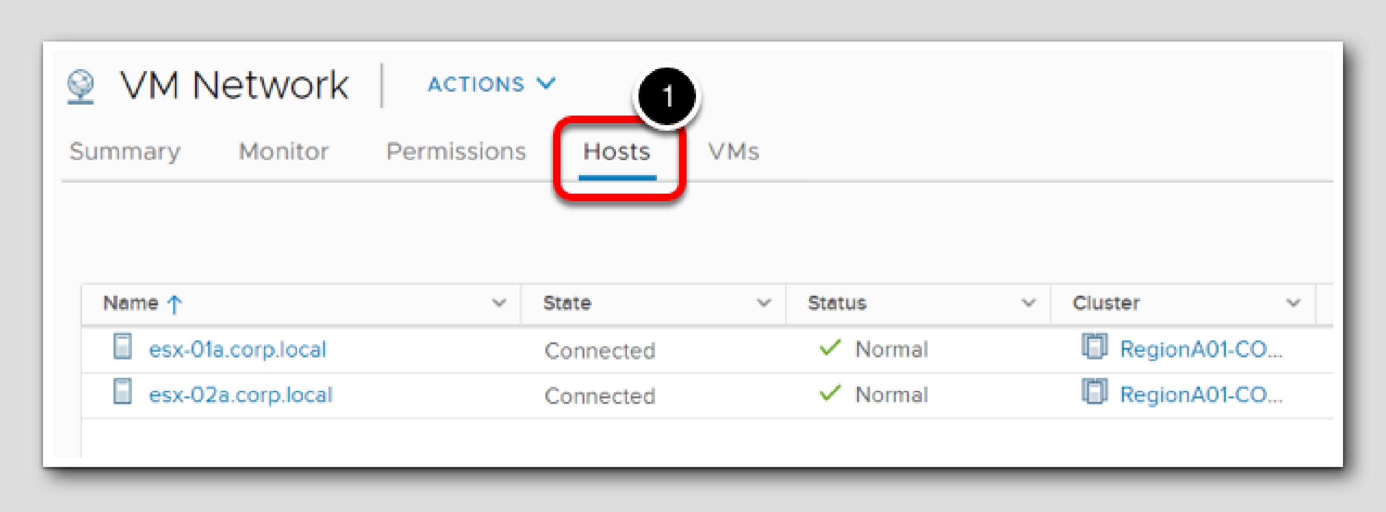
1. Click on VMs tab

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

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

Hosts

[269]



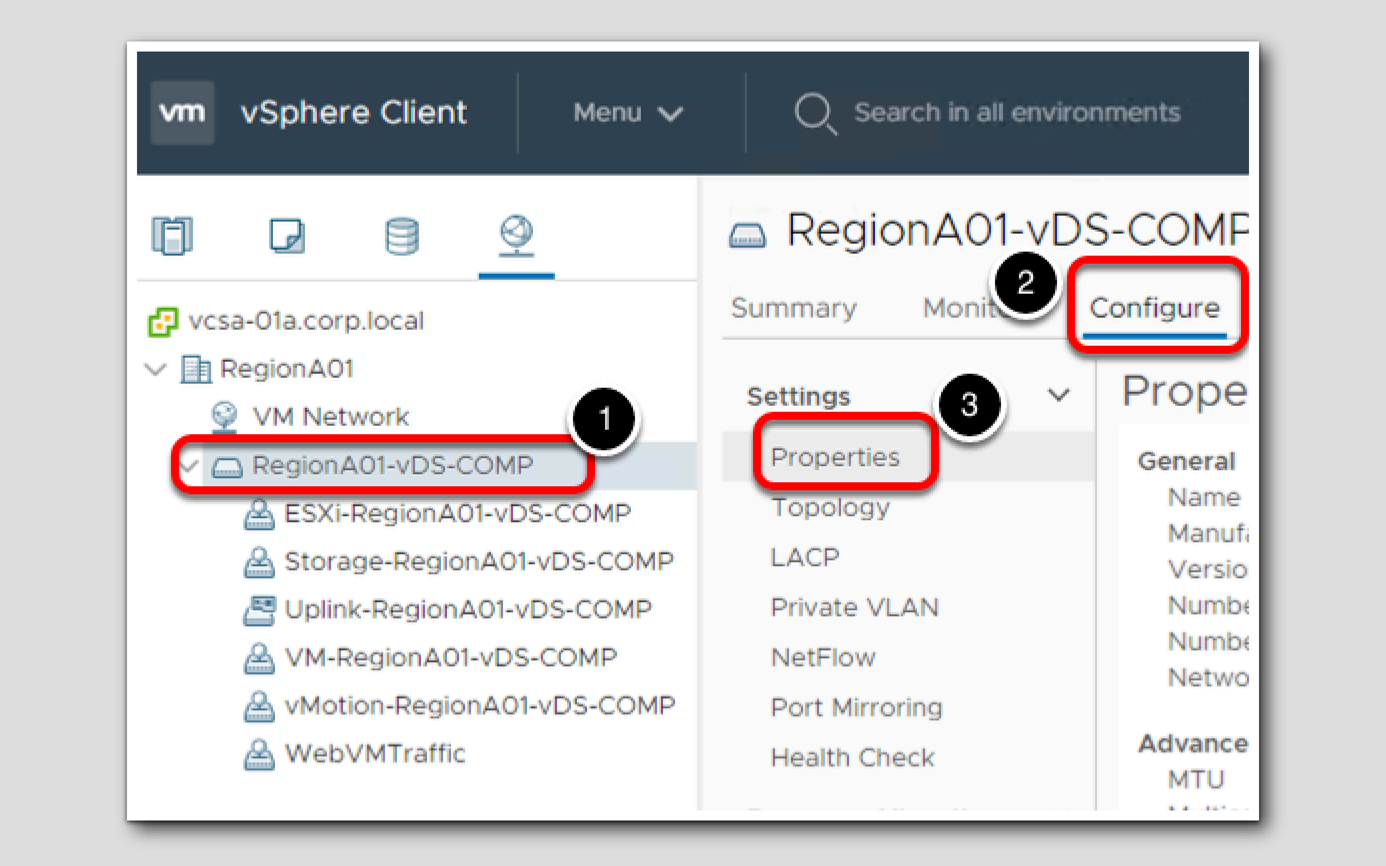
Name ↑	State	Status	Cluster
esx-01a.corp.local	Connected	✓ Normal	RegionA01-CO...
esx-02a.corp.local	Connected	✓ Normal	RegionA01-CO...

1. Click on Hosts tab

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

View Distributed Switch

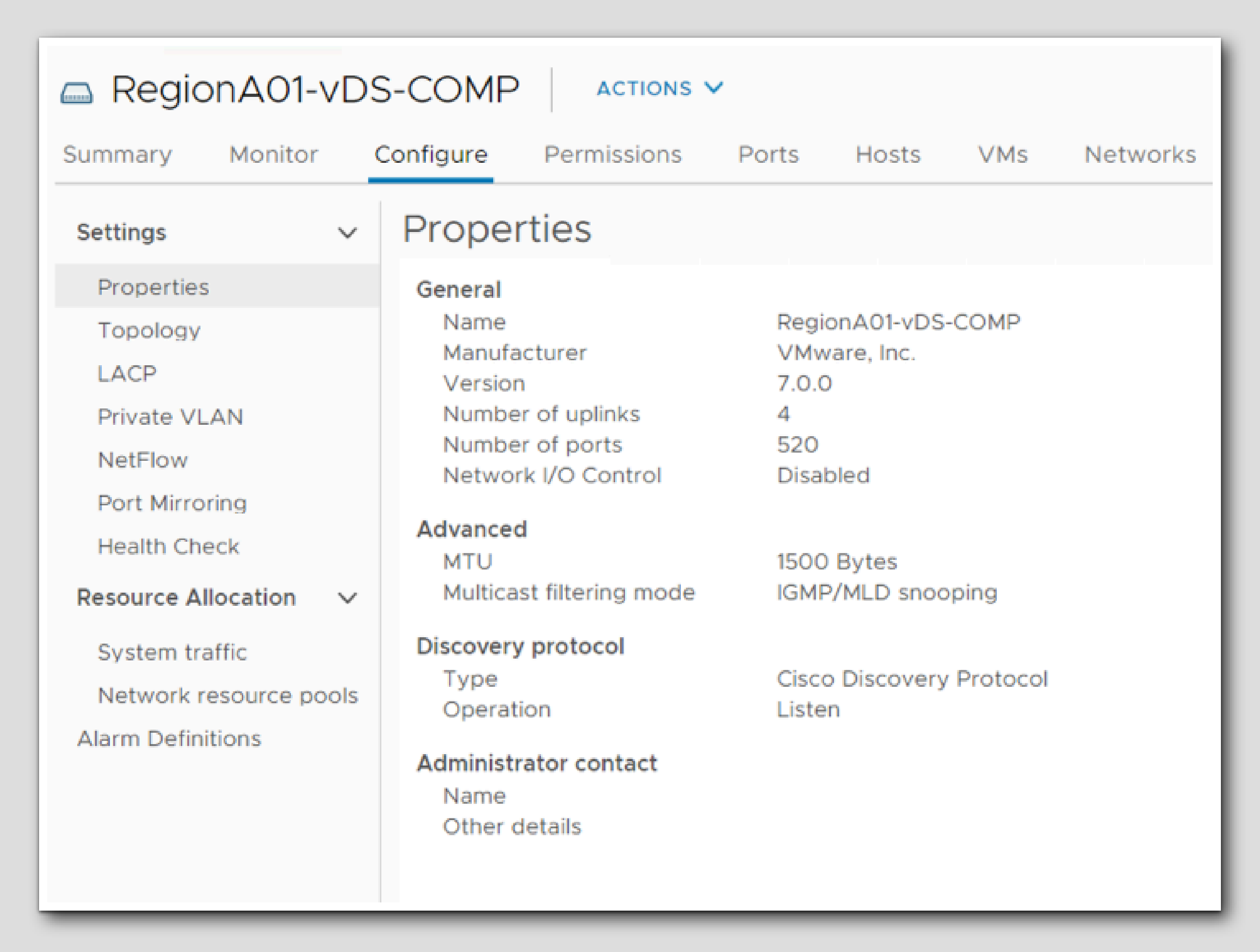
[270]



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

Review vDS configuration

[271]



RegionA01-vDS-COMP

Properties

General

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

Advanced

MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

Discovery protocol

Type	Cisco Discovery Protocol
Operation	Listen

Administrator contact

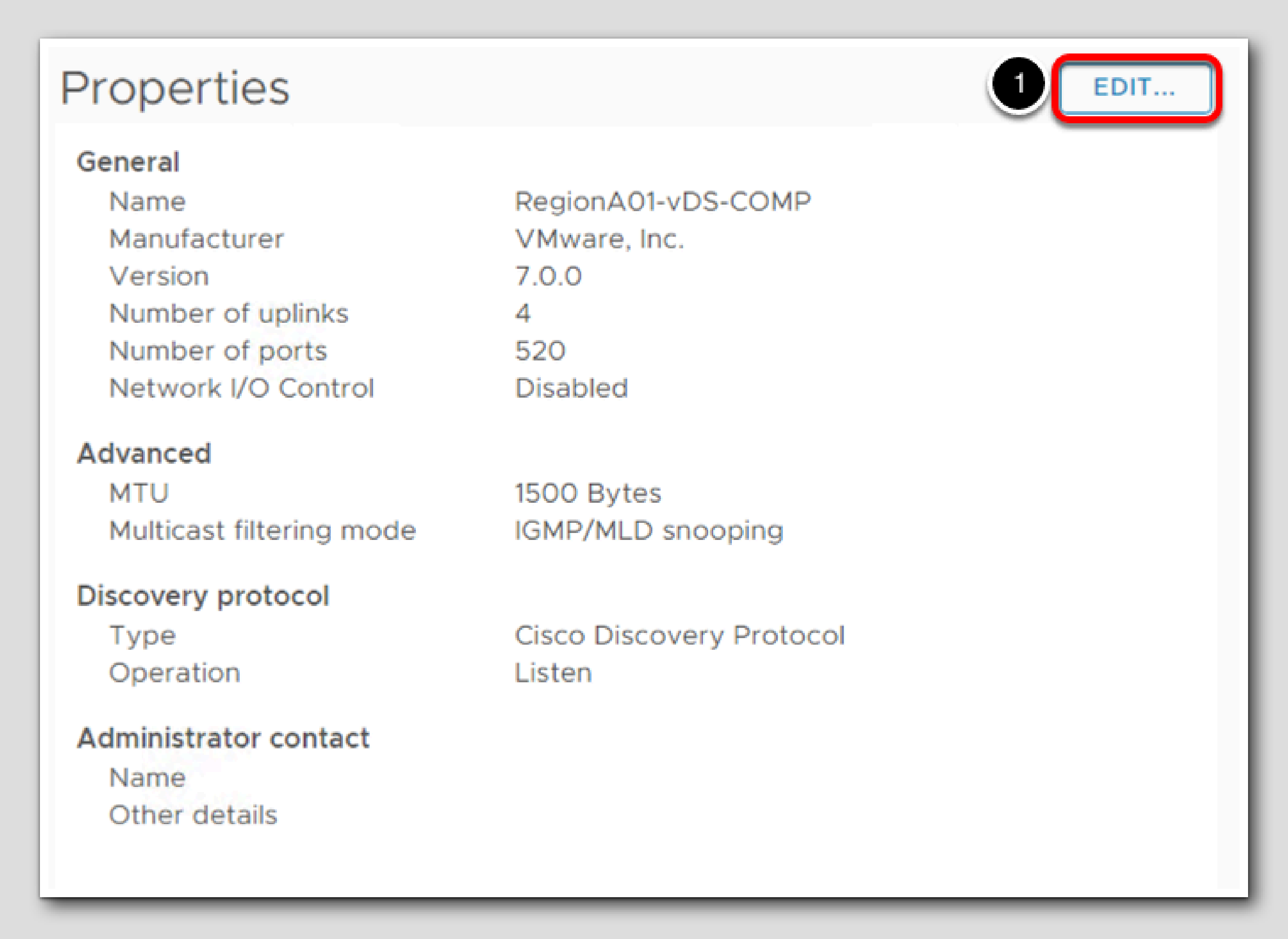
Name

Other details

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

Edit the switch properties

[272]



Properties

General

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

Advanced

MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

Discovery protocol

Type	Cisco Discovery Protocol
Operation	Listen

Administrator contact

Name

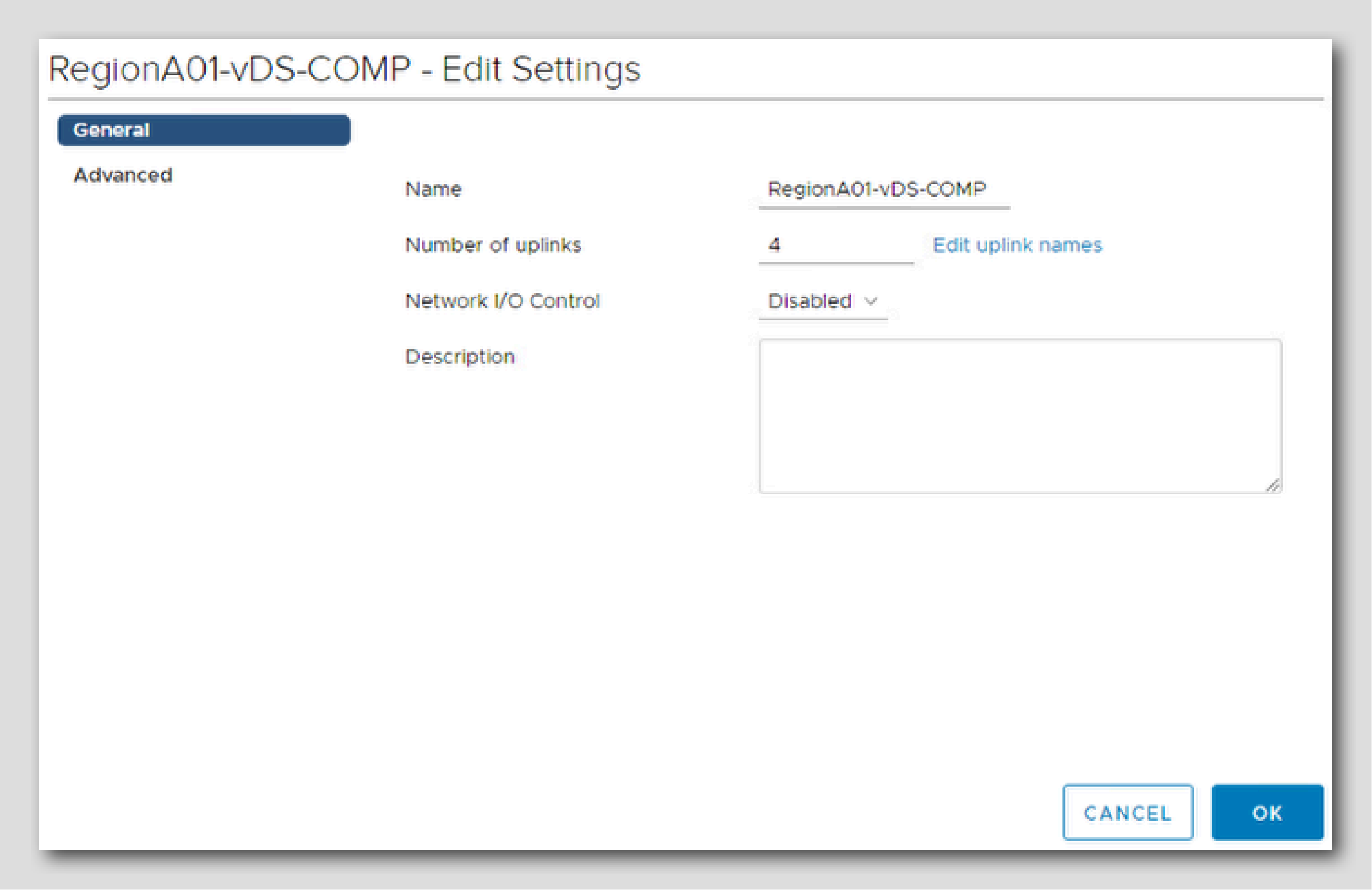
Other details

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

1. Click Edit

General Settings

[273]



RegionA01-vDS-COMP - Edit Settings

Name: RegionA01-vDS-COMP

Number of uplinks: 4

Network I/O Control: Disabled

Description:

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.

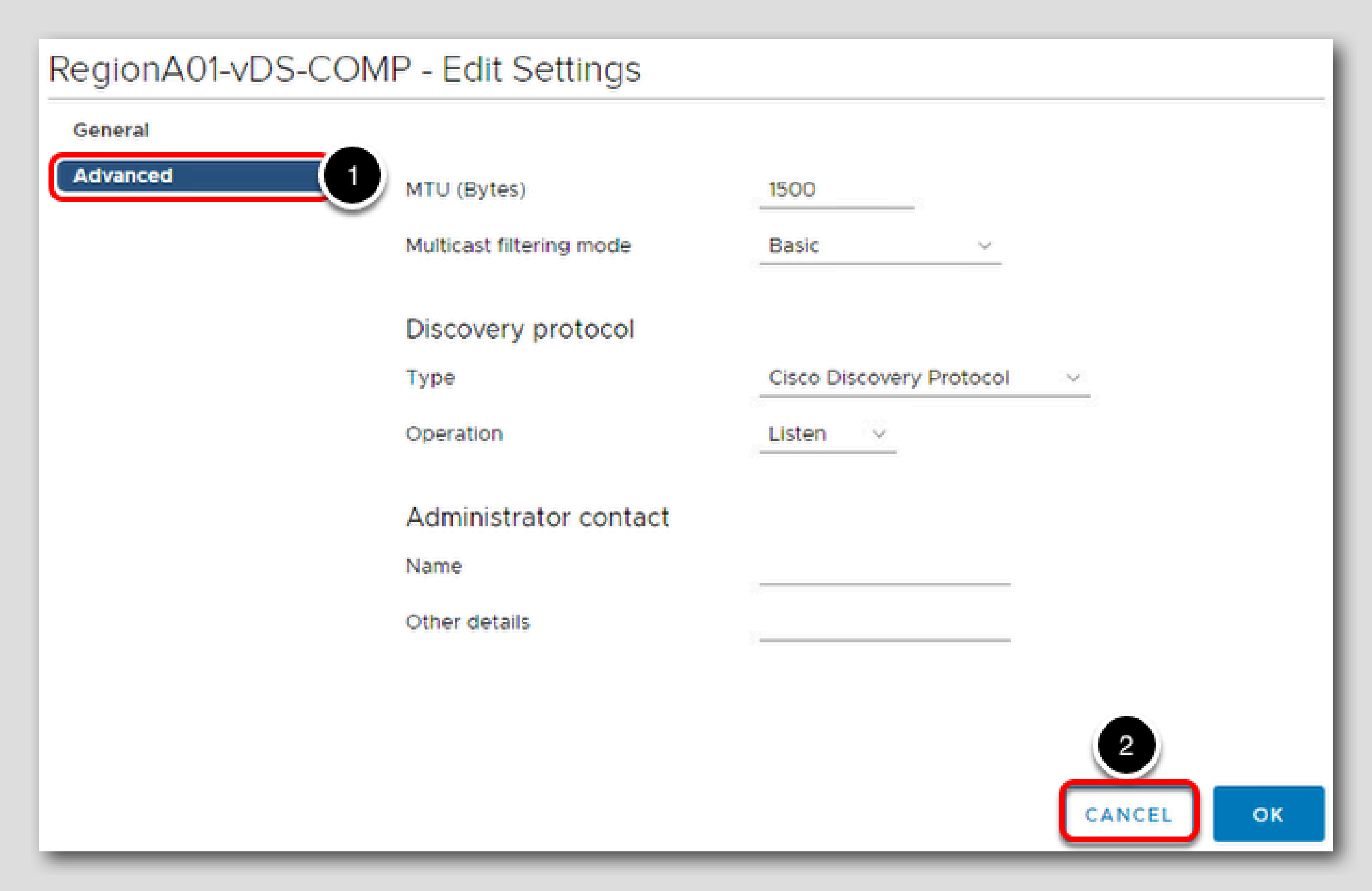
Number of Ports: This setting cannot be modified. The port count will dynamically be scaled up or down by default.

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

[274]



RegionA01-vDS-COMP - Edit Settings

MTU (Bytes) 1500

Multicast filtering mode Basic

Discovery protocol

Type Cisco Discovery Protocol

Operation Listen

Administrator contact

Name

Other details

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.

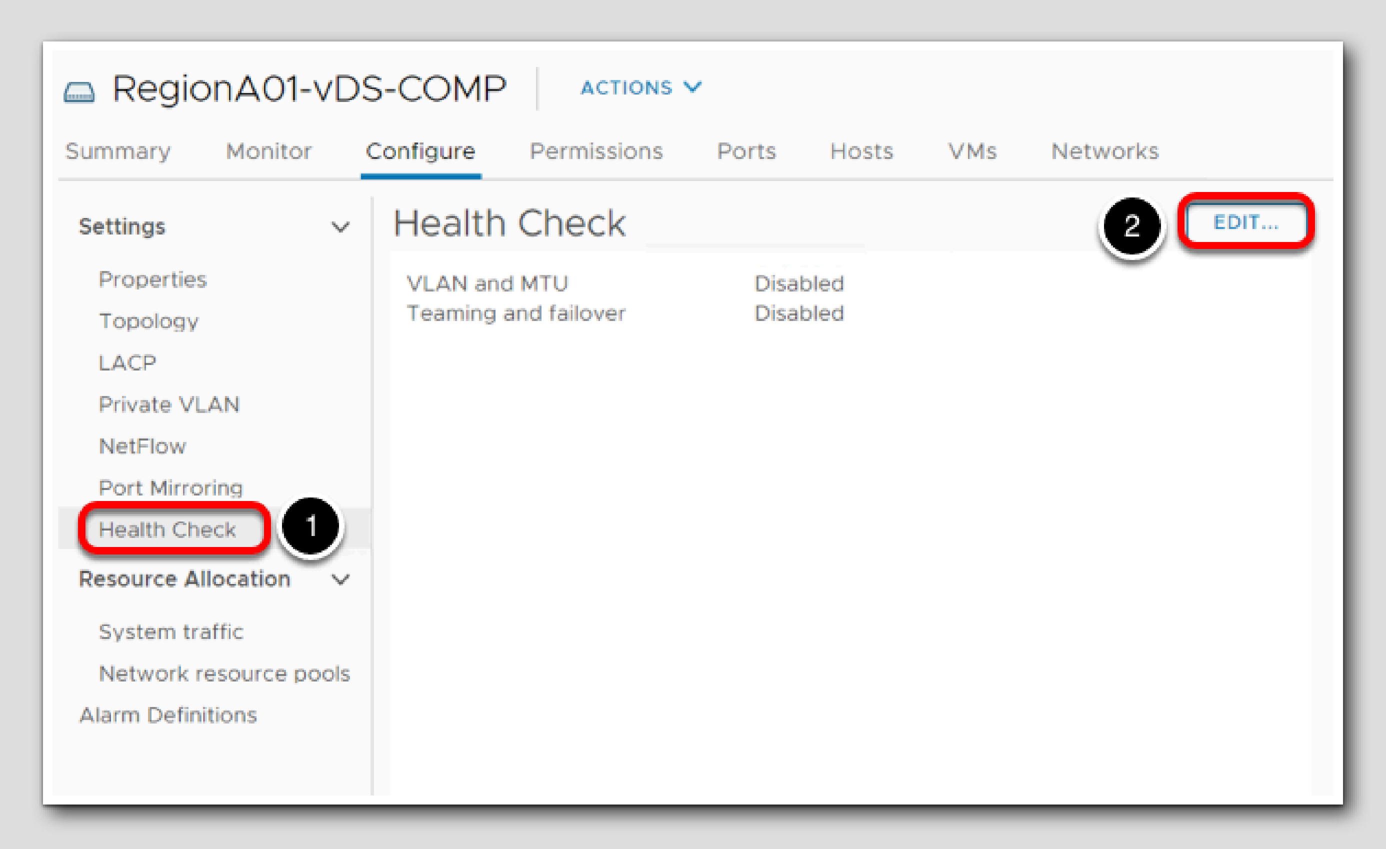
Discovery Protocol

- 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



VLAN and MTU	Disabled
Teaming and failover	Disabled

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.

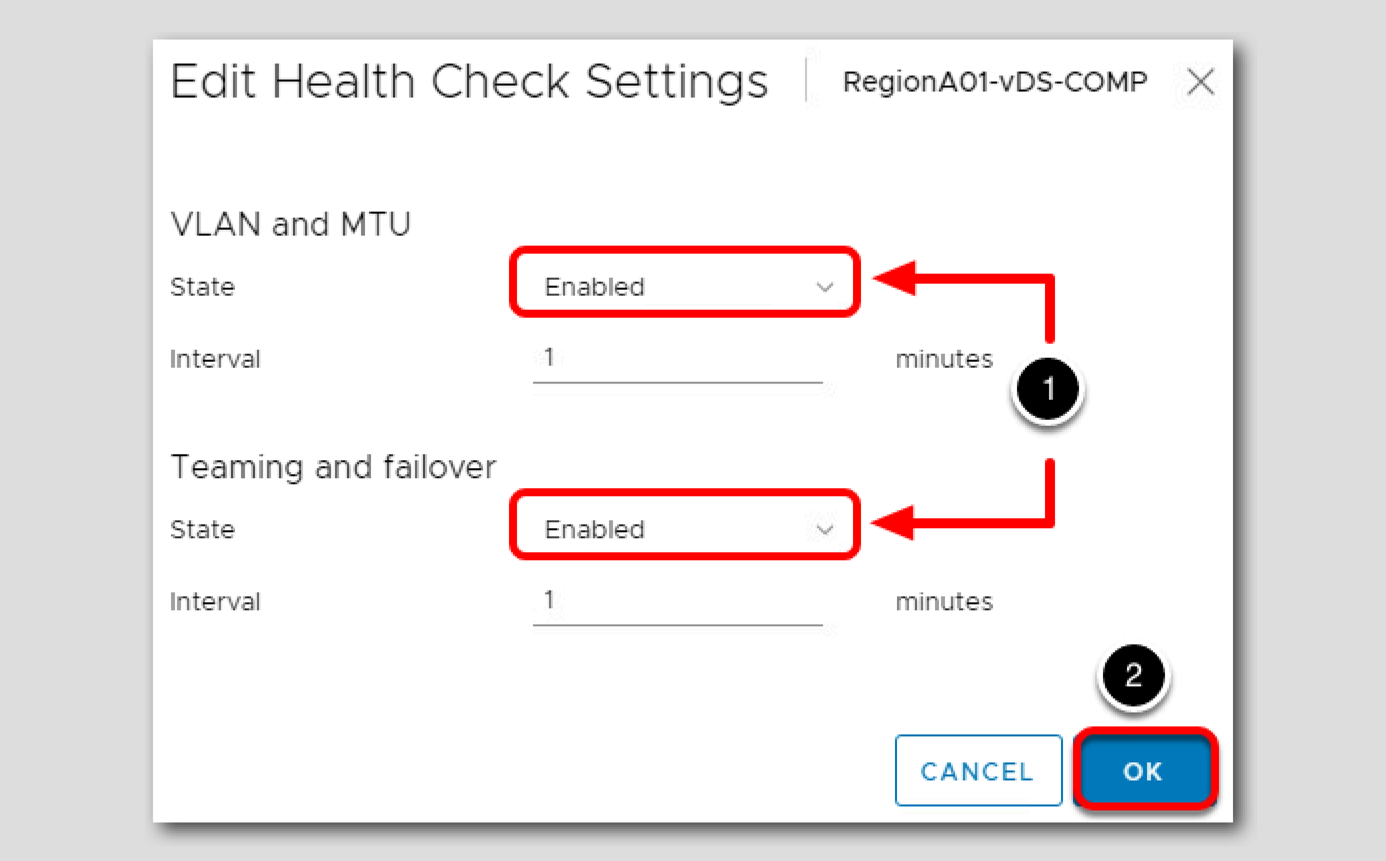
Health Check is available on ESXi 5.1 Distributed Switches and higher.

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

VLAN and MTU

State: Enabled

Interval: 1 minutes

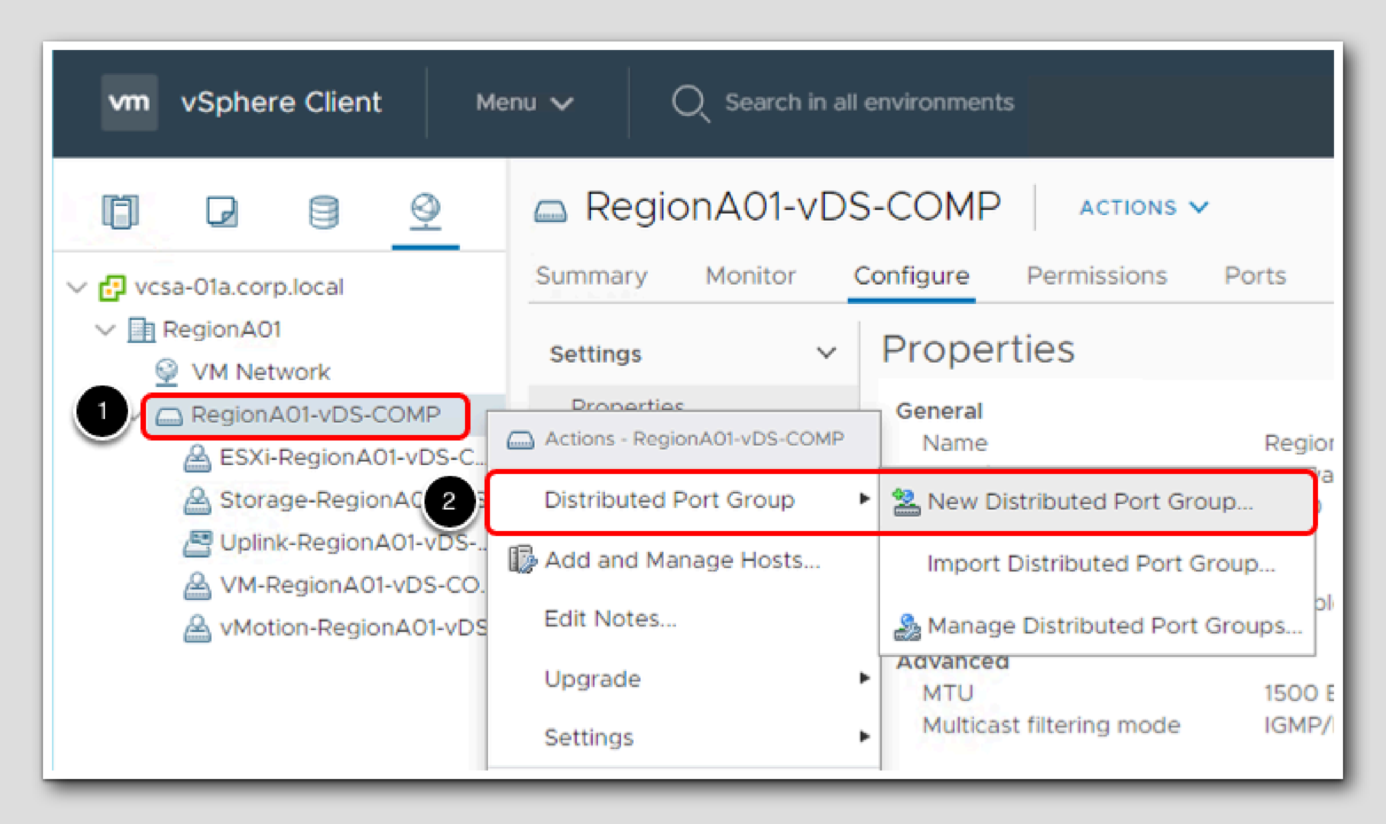
Teaming and failover

State: Enabled

Interval: 1 minutes

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

Distributed Port Groups

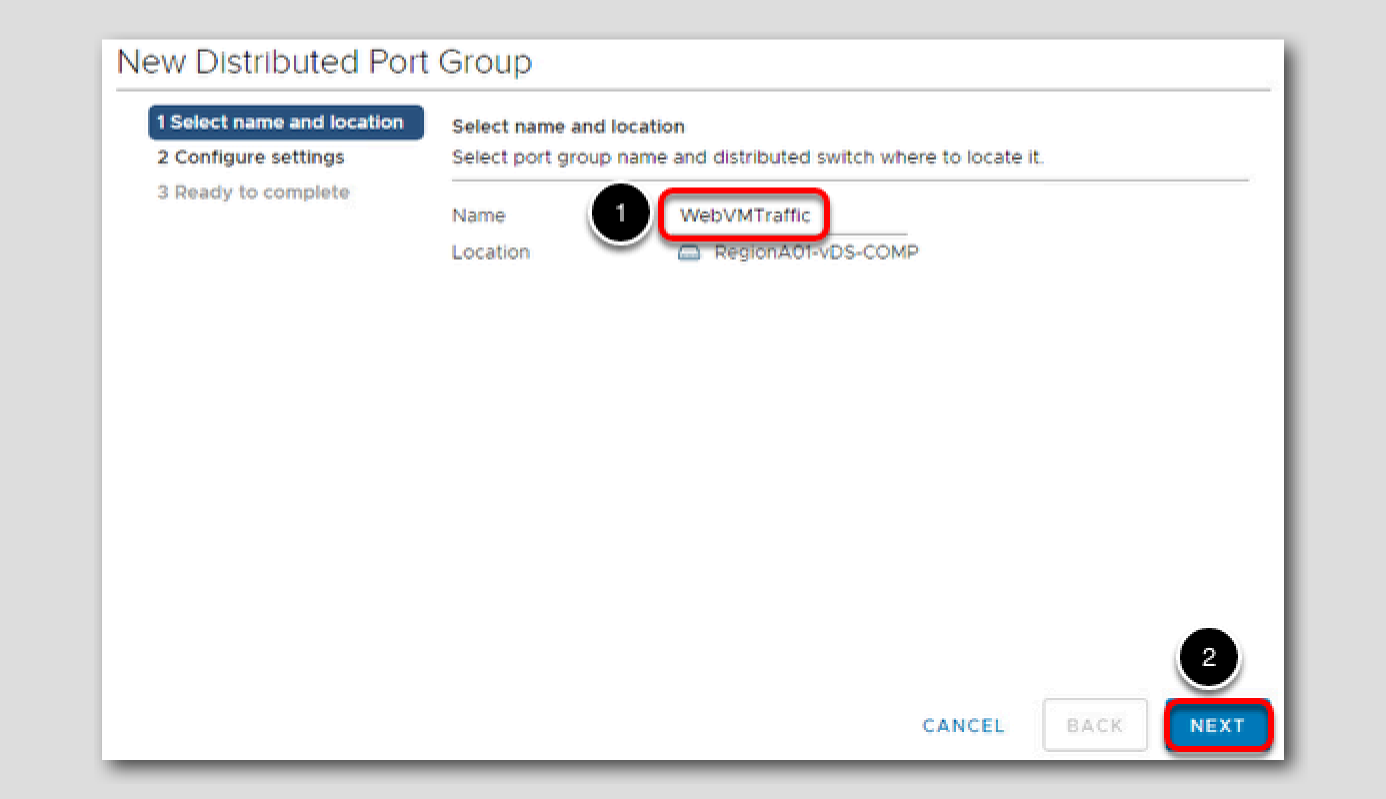


A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

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

Select name and location section

[278]



New Distributed Port Group

Select name and location

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

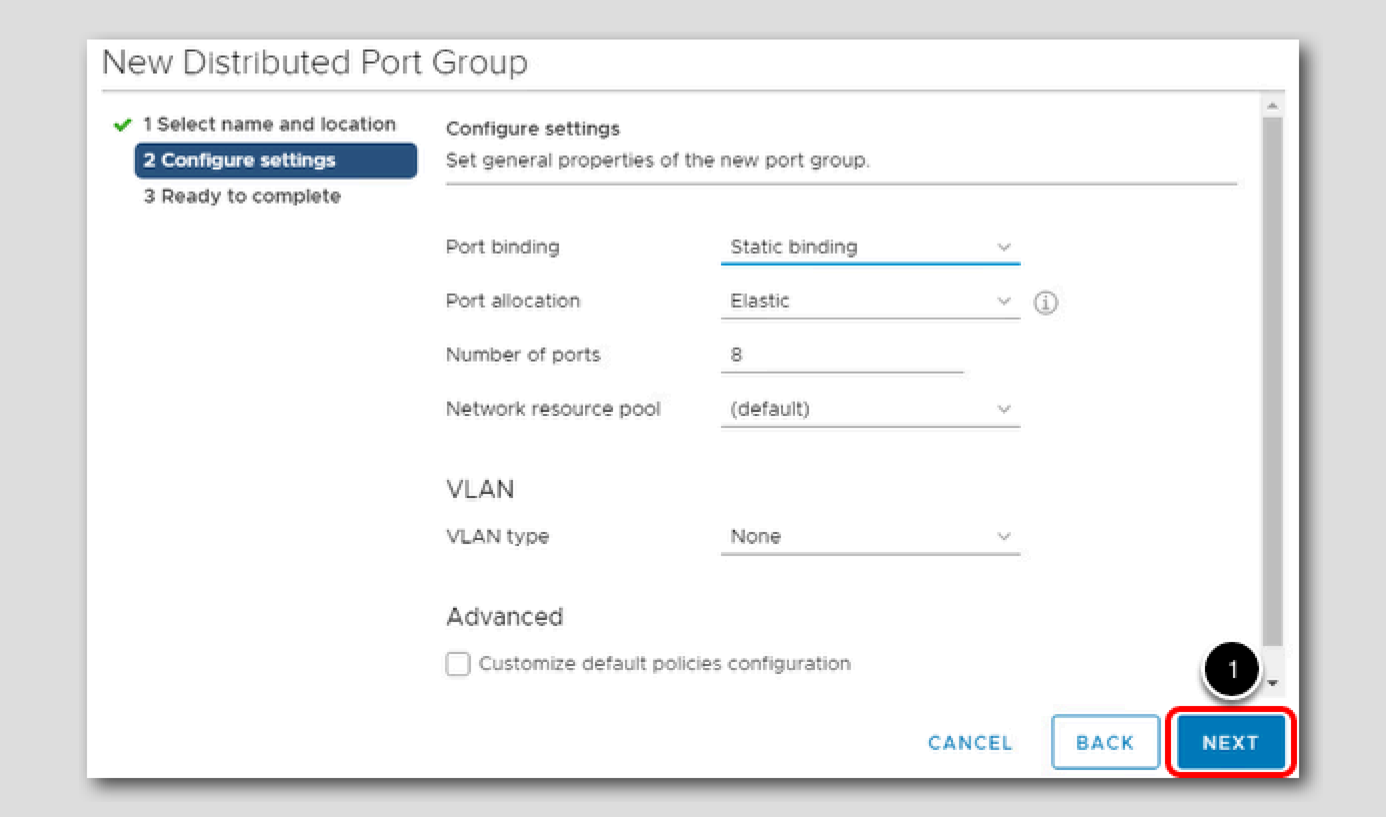
Name 1 WebVMTraffic

Location RegionA01-vDS-COMP

1. Name the new port group WebVMTraffic
2. Click Next

Configure settings

[279]



New Distributed Port Group

✓ 1 Select name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

VLAN

VLAN type: None

Advanced

□ Customize default policies configuration

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:

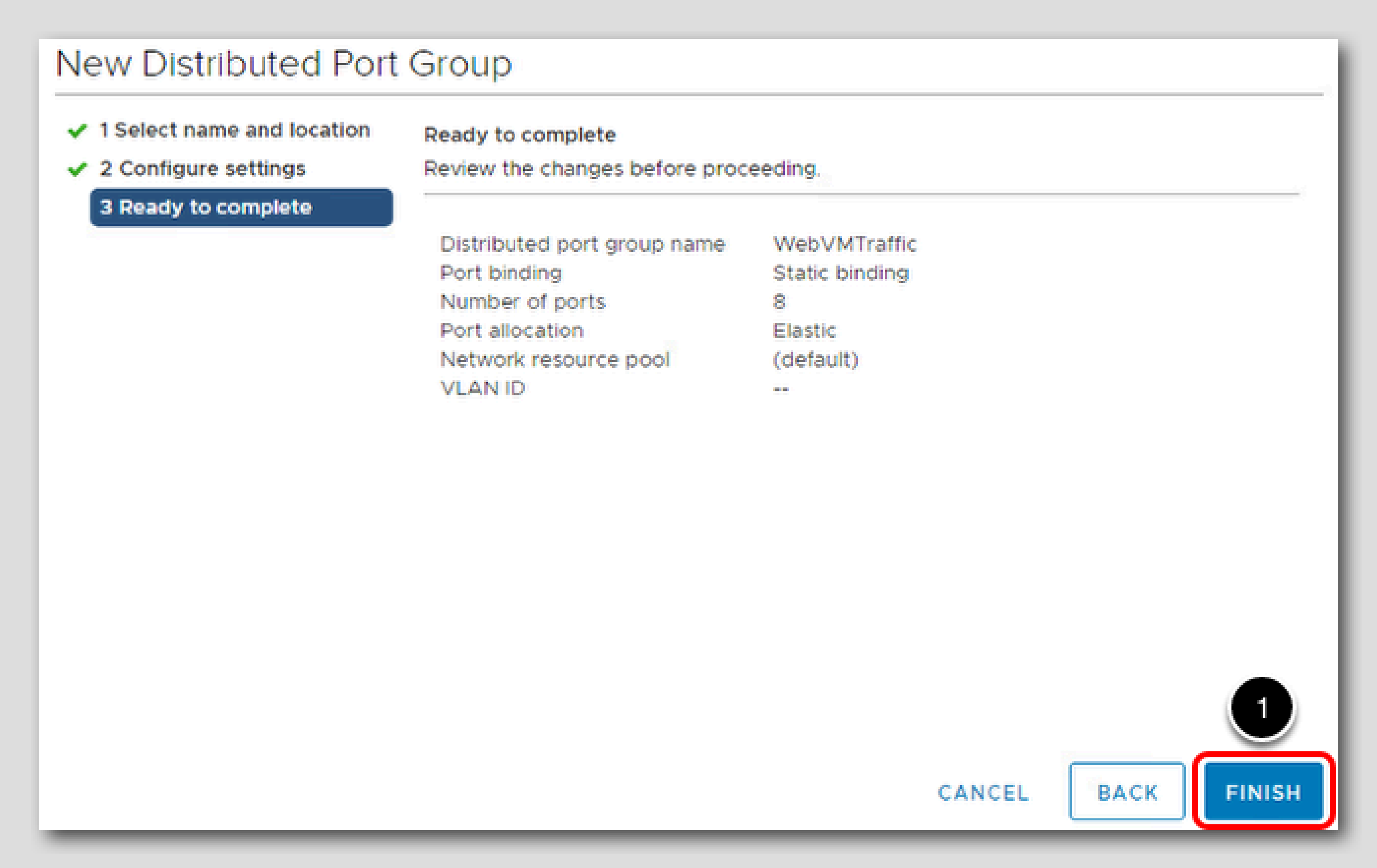
- None - Do not use VLAN.
- VLAN - In the VLAN ID field, enter a number between 1 and 4094.
- VLAN Trunking - Enter a VLAN trunk range.
- Private VLAN - Select a private VLAN entry. If you did not create any private VLANs, this menu is empty.

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

[280]



New Distributed Port Group

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

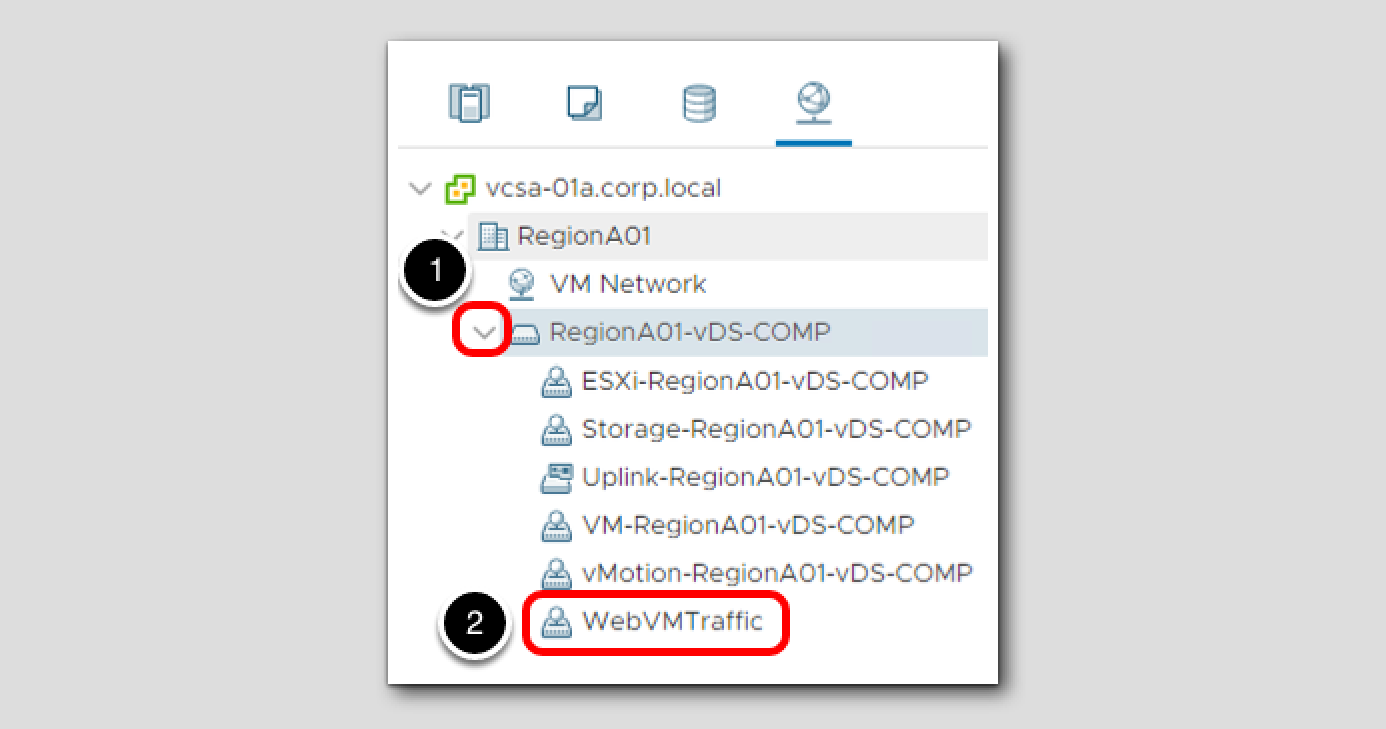
Ready to complete

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	--

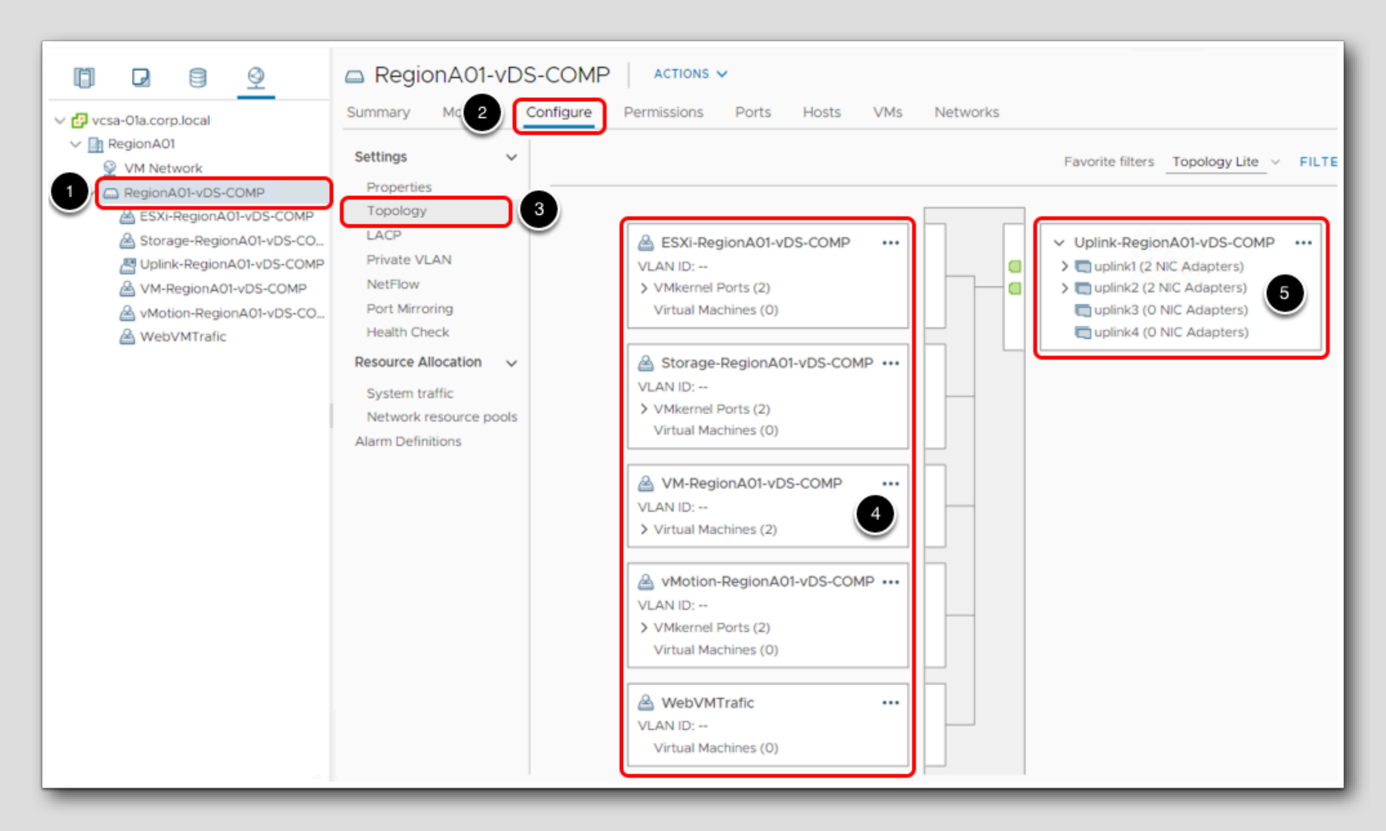
1. Review your settings and click Finish

View the new Distributed Port Group



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

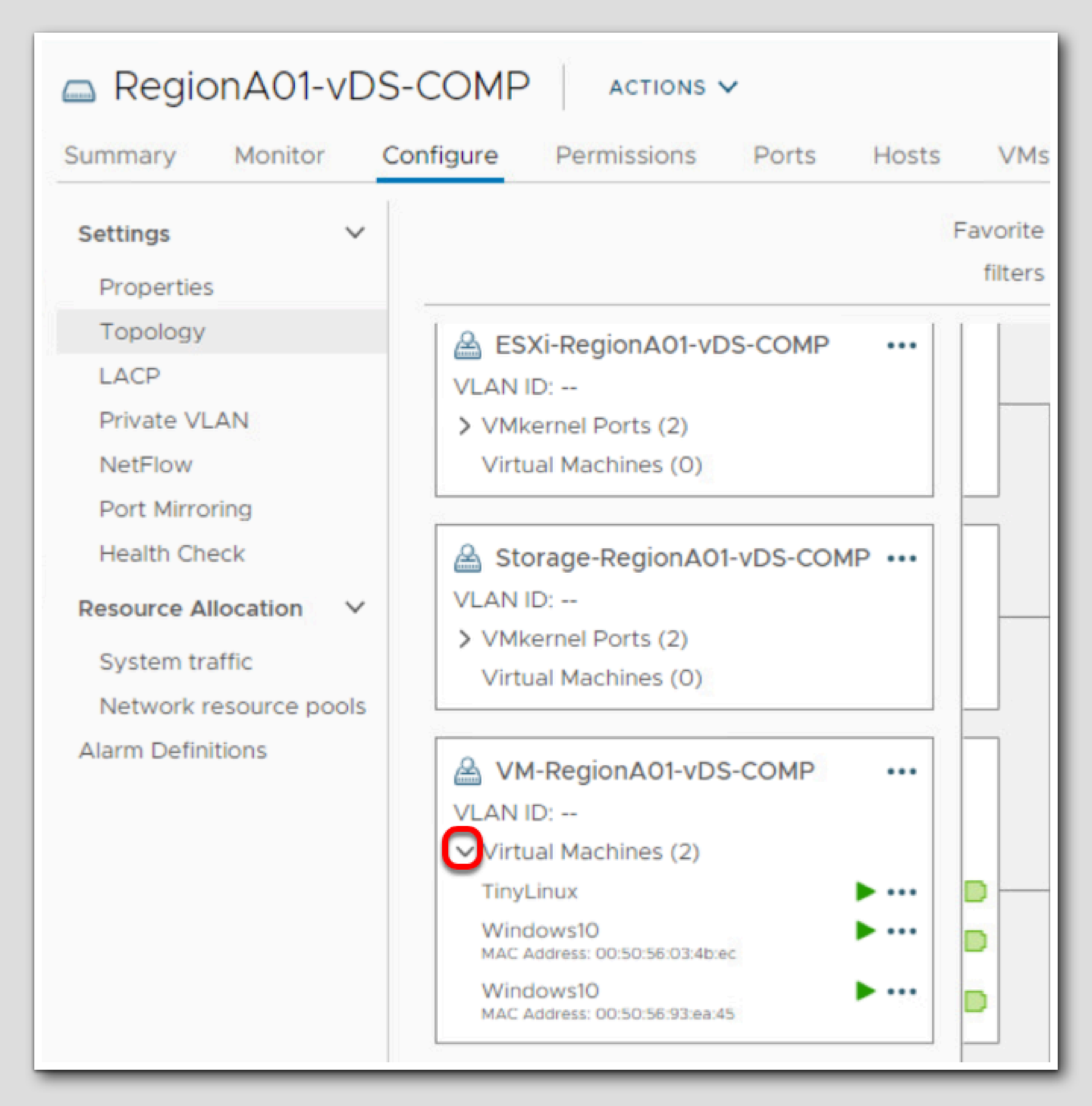
Topology



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

VM Port Group

[283]



RegionA01-vDS-COMP ACTIONS

Summary Monitor Configure Permissions Ports Hosts VMs

Settings
- Properties
- Topology
- LACP
- Private VLAN
- NetFlow
- Port Mirroring
- Health Check

Resource Allocation
- System traffic
- Network resource pools

Alarm Definitions

Favorite filters

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

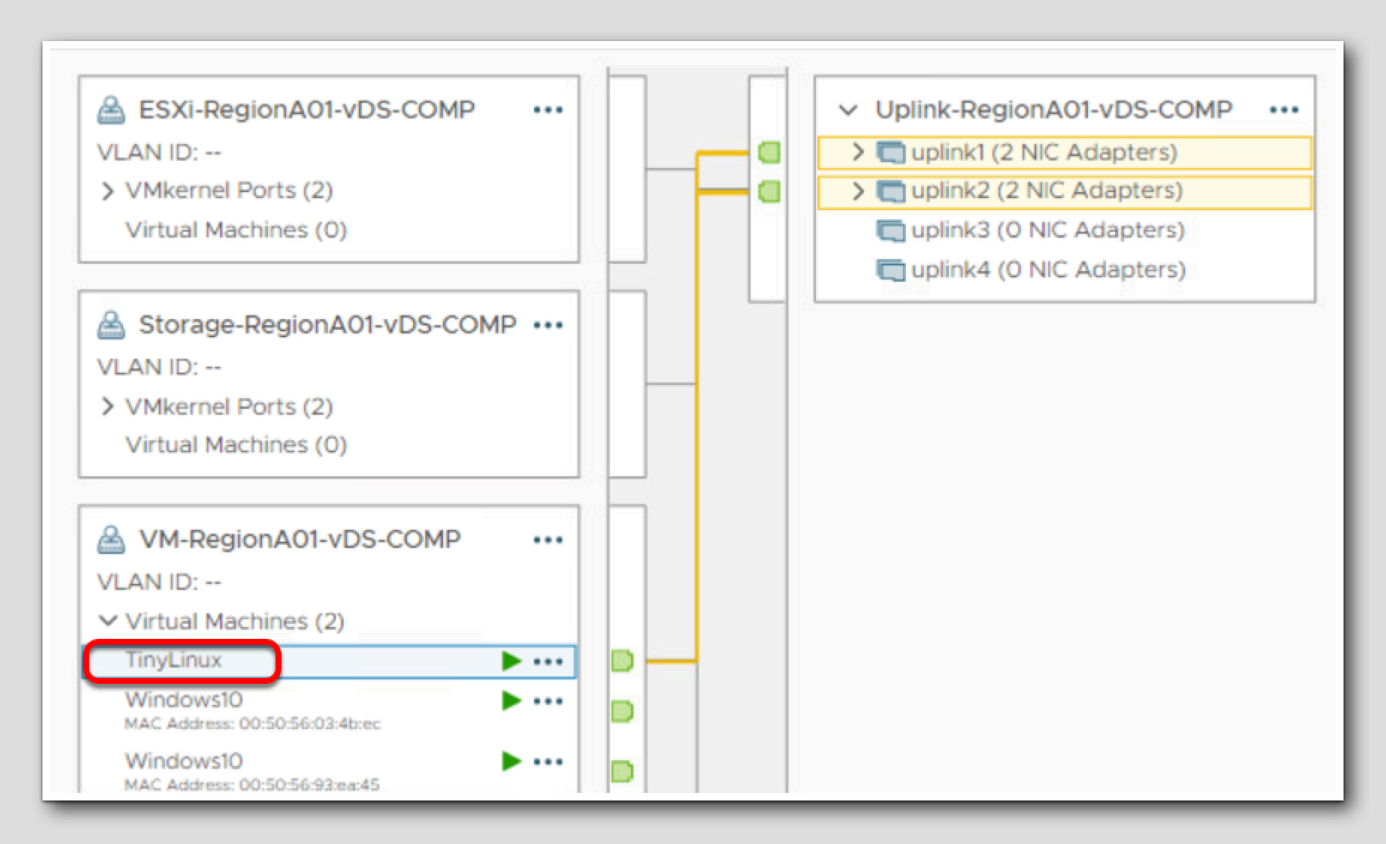
Storage-RegionA01-vDS-COMP
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (0)

VM-RegionA01-vDS-COMP
VLAN ID: --
Virtual Machines (2)
TinyLinux
Windows10
MAC Address: 00:50:56:03:4b:ec
Windows10
MAC Address: 00:50:56:93:ea:45

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

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

Path to Uplinks [284]



1. Click on **TinyLinux**

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

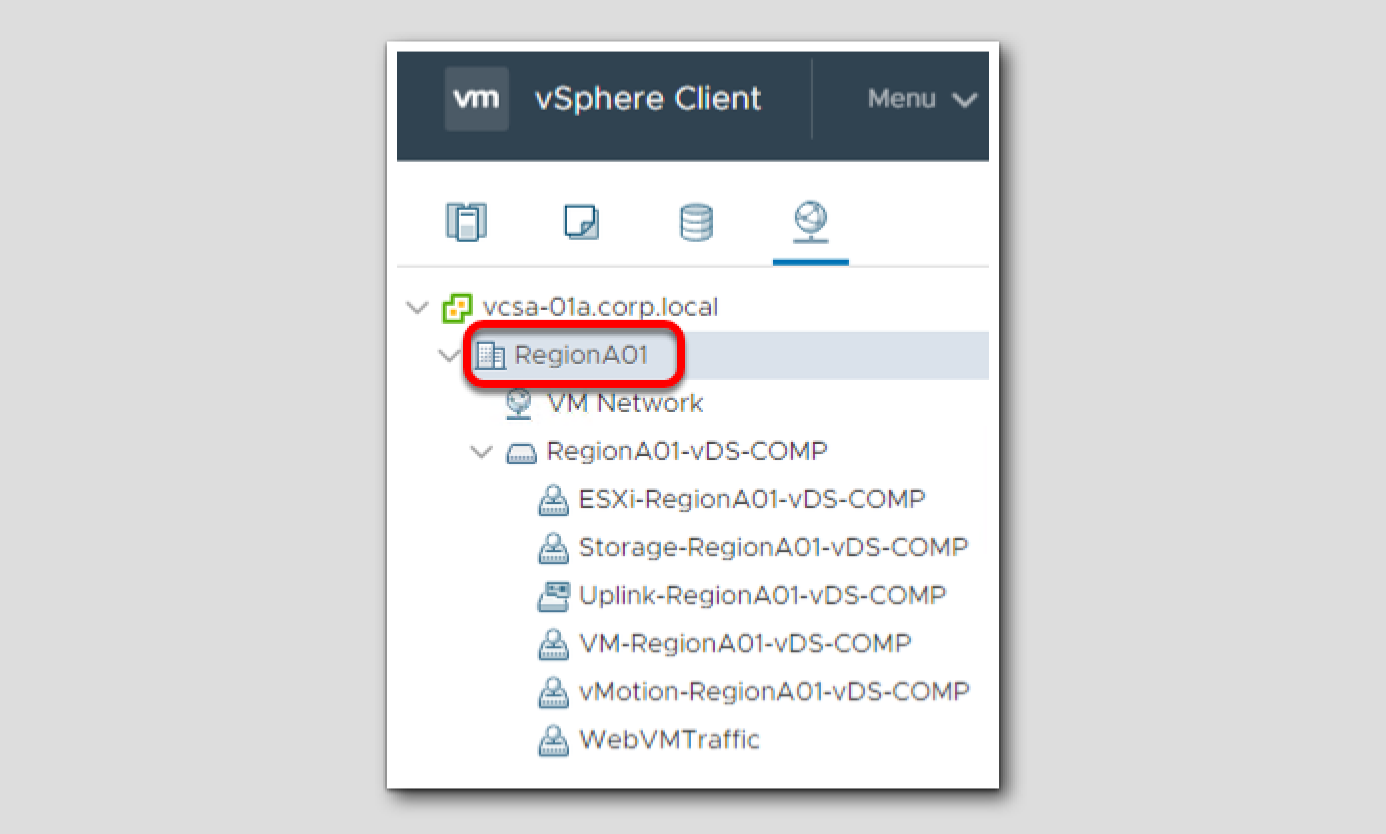
Creating a new Distributed Switch [285]

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

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

Navigate to RegionA01 Datacenter

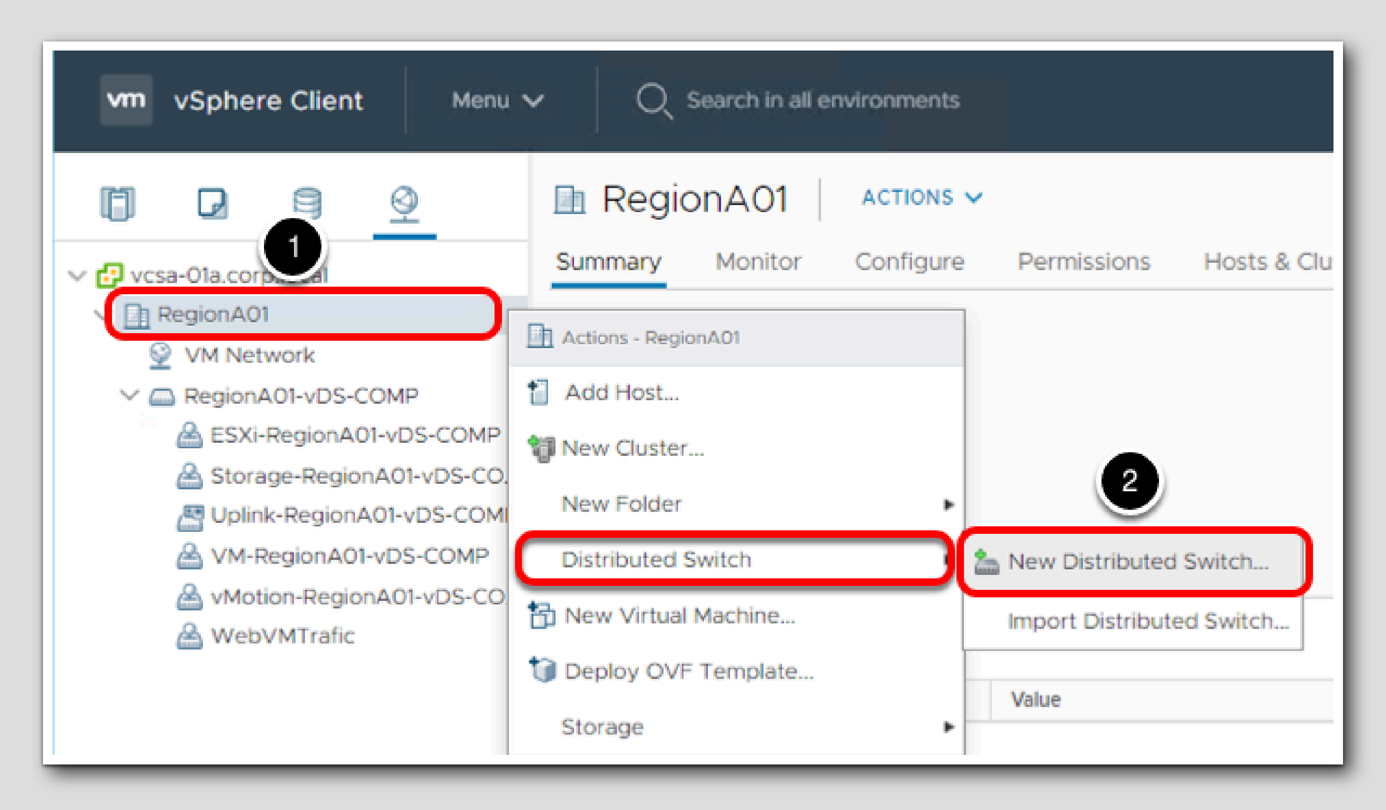
[286]



1. In the vSphere Web Client, click on RegionA01

Create a new Distributed Switch

[287]

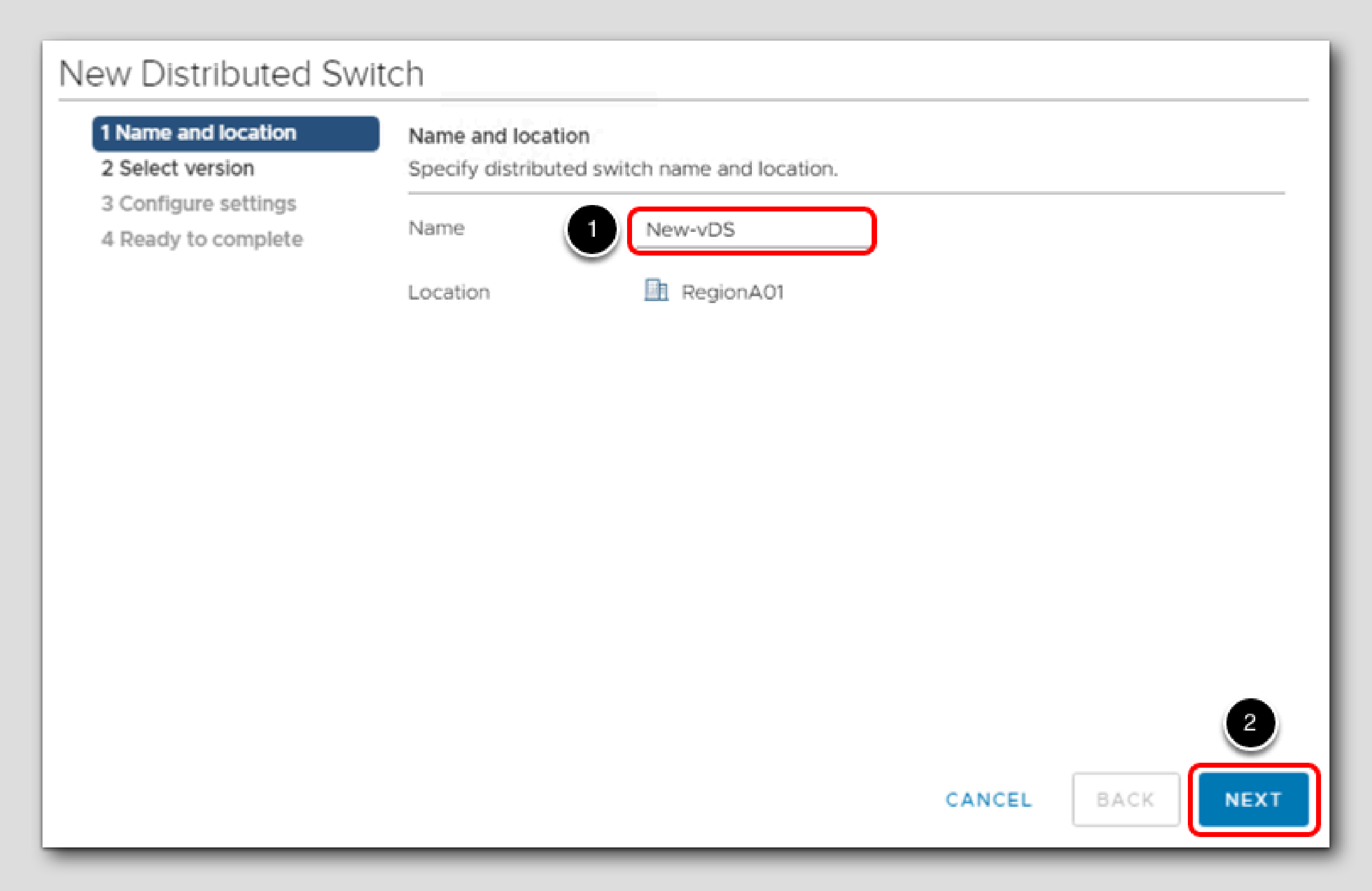


1. In the navigator, right-click the RegionA01
2. Select Distributed Switch and then New Distributed Switch

This will open the New Distributed Switch wizard.

Name the Distributed Switch

[288]



New Distributed Switch

Name and location

Specify distributed switch name and location.

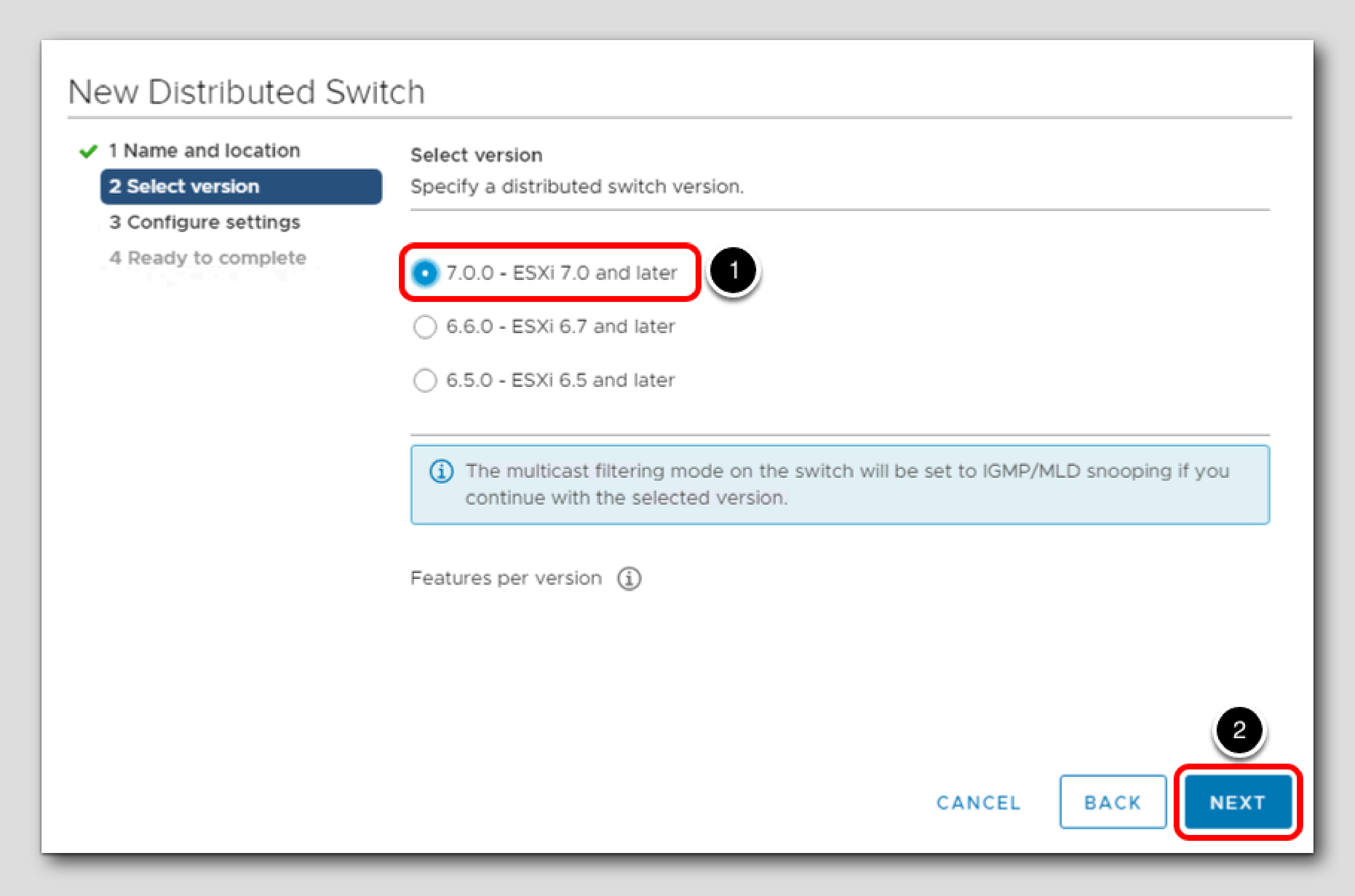
Name: New-vDS

Location: RegionA01

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

Select the version

[289]



New Distributed Switch

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

Select version
Specify a distributed switch version.

● 7.0.0 - ESXi 7.0 and later
○ 6.6.0 - ESXi 6.7 and later
○ 6.5.0 - ESXi 6.5 and later

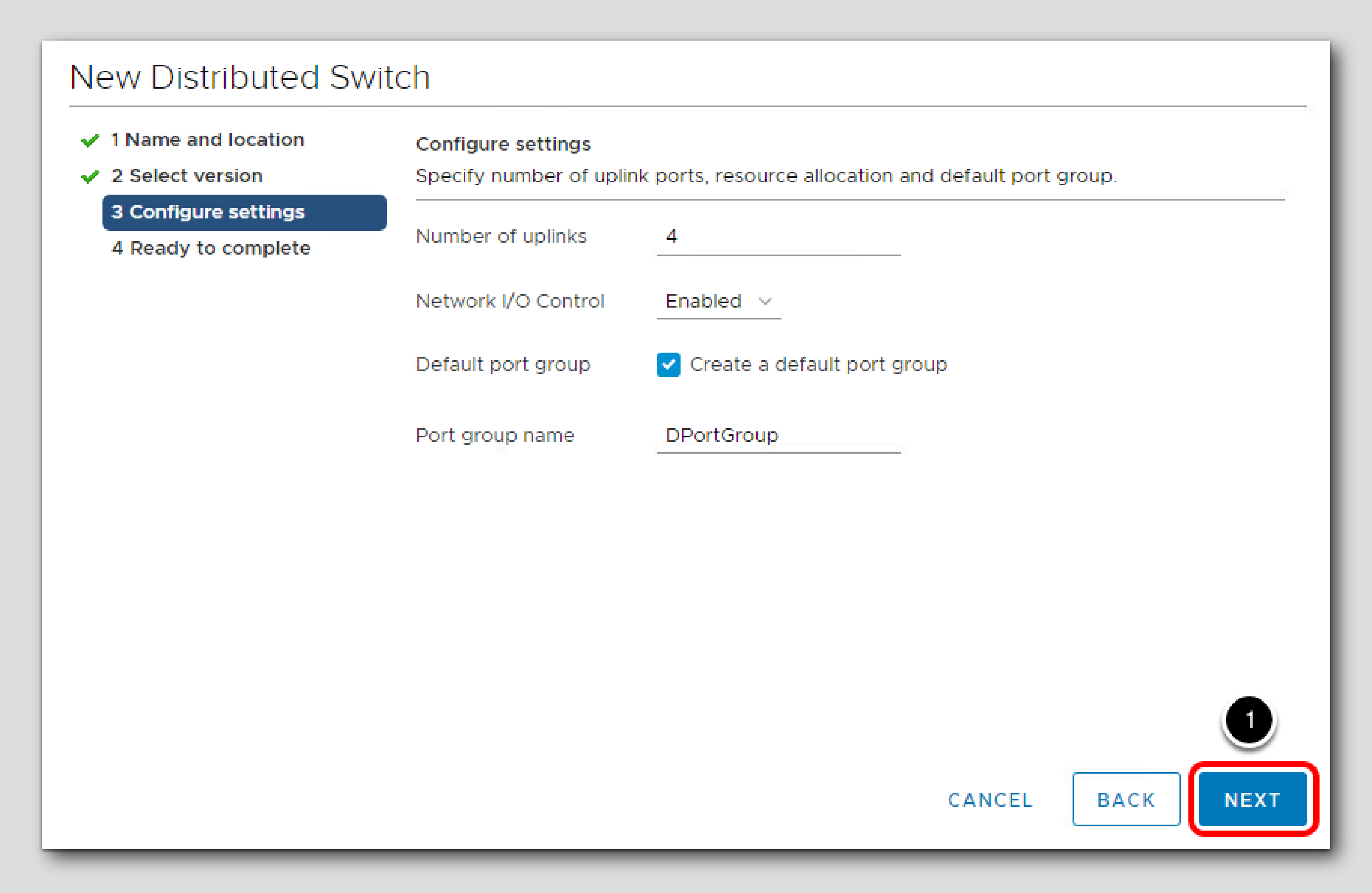
The multicast filtering mode on the switch will be set to IGMP/MLD snooping if you continue with the selected version.

Features per version

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

Configure settings

[290]



New Distributed Switch

Configure settings

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

Number of uplinks: 4

Network I/O Control: Enabled

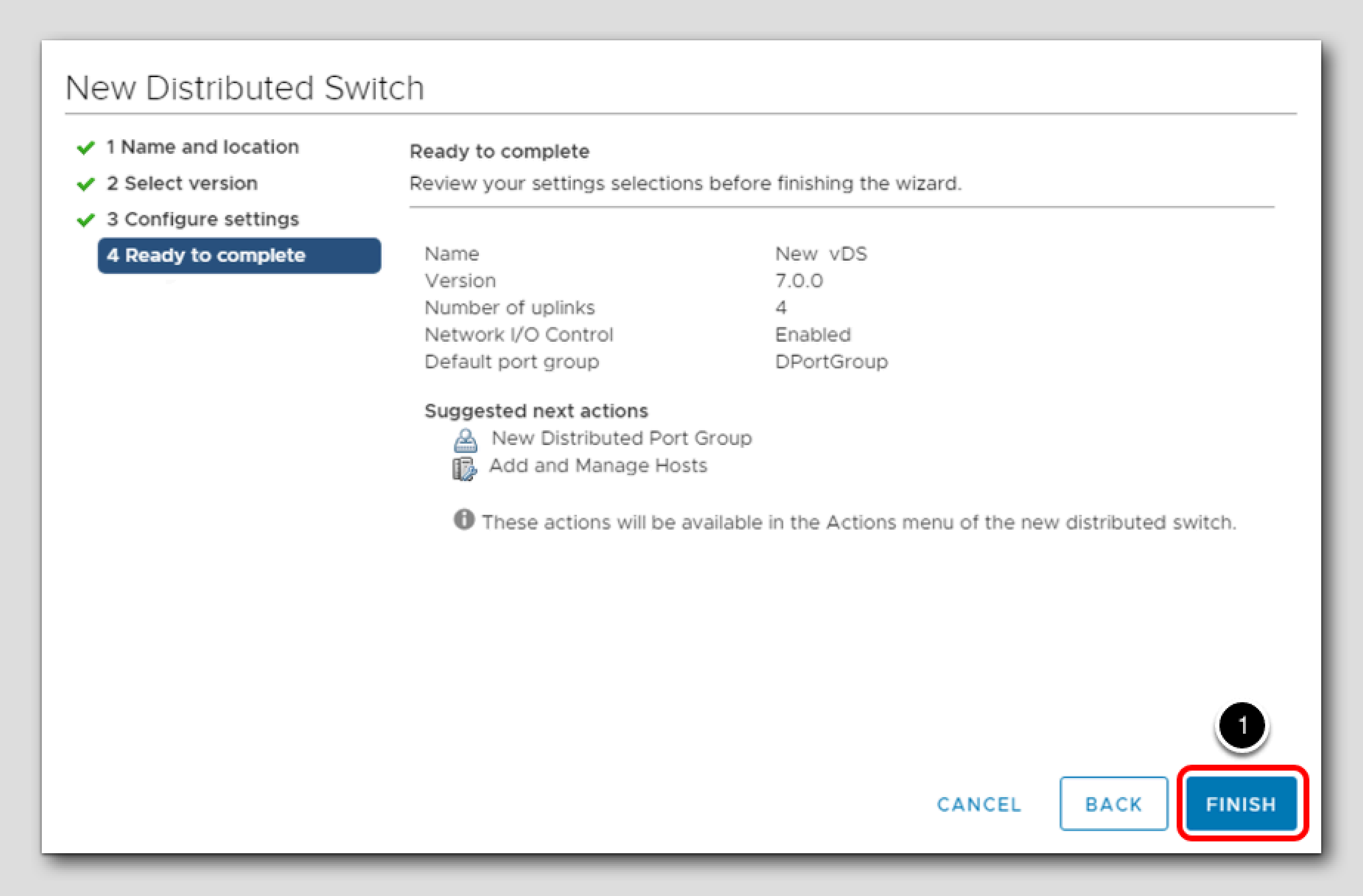
Default port group: ☑ Create a default port group

Port group name: DPortGroup

1. Leave the default options and click Next

Complete the build

[291]



New Distributed Switch

Ready to complete

Review your settings selections before finishing the wizard.

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

Suggested next actions

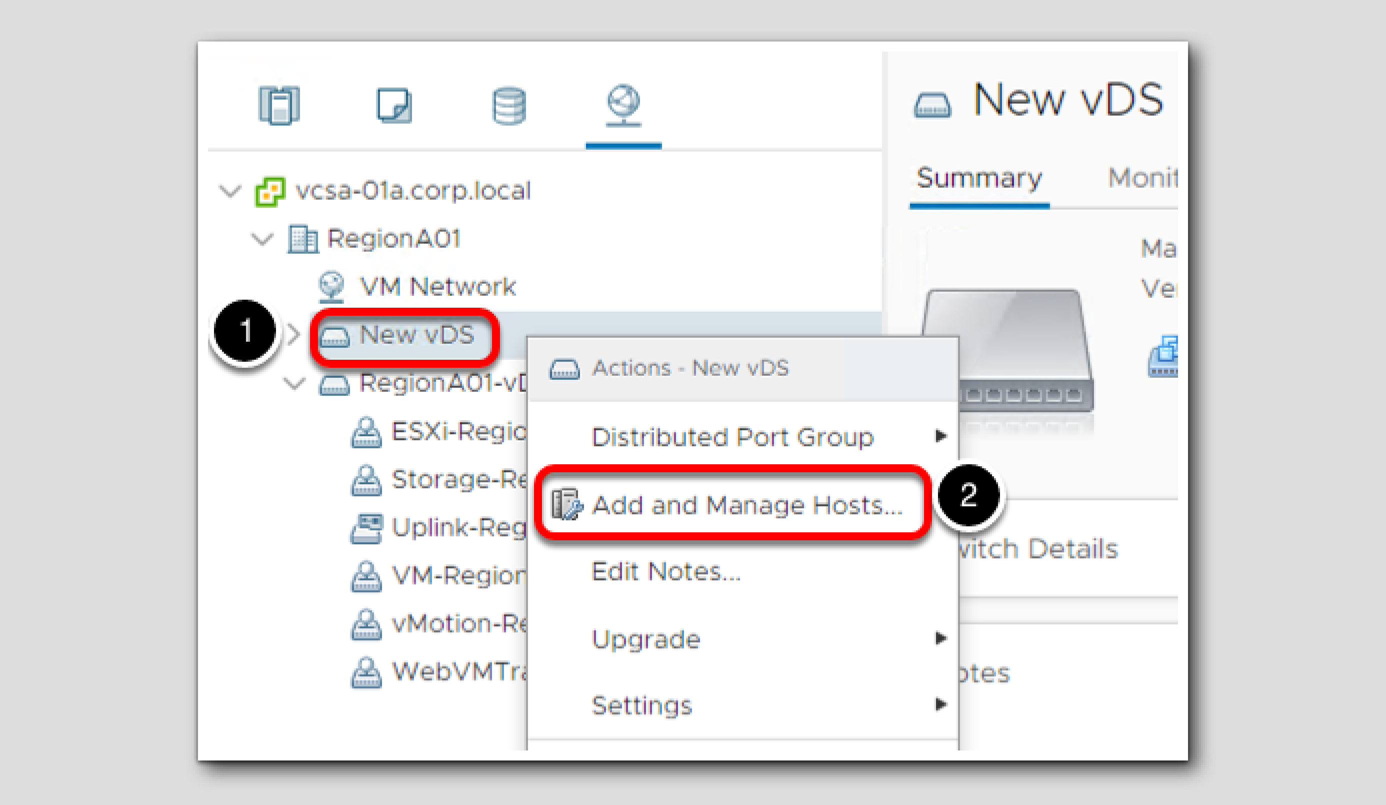
New Distributed Port Group

Add and Manage Hosts

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

1. Review your settings and click Finish

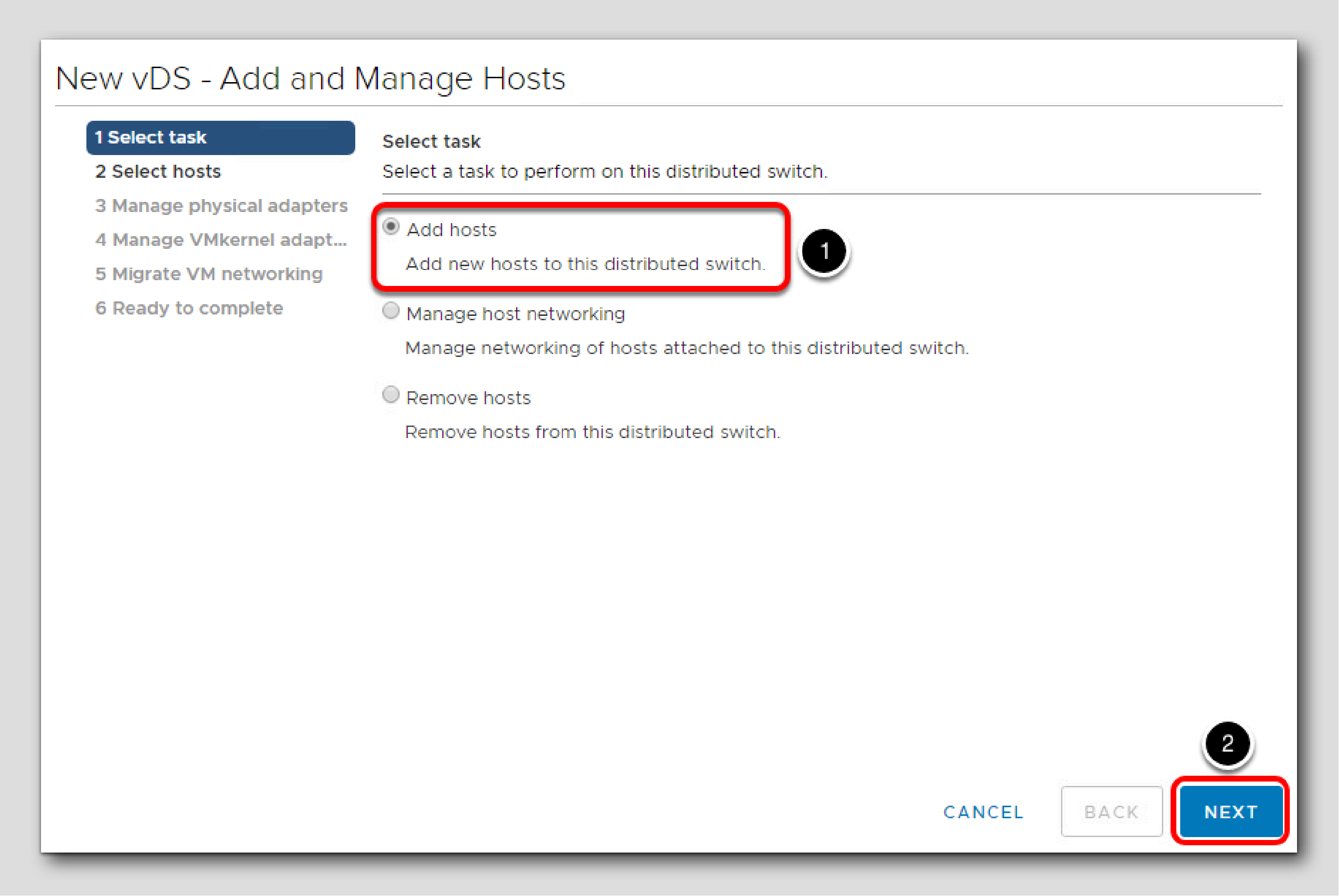
Add hosts to new Distributed Switch



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

Select task

[293]



New vDS - Add and Manage Hosts

Select task

Select a task to perform on this distributed switch.

● Add hosts

Add new hosts to this distributed switch.

○ Manage host networking

Manage networking of hosts attached to this distributed switch.

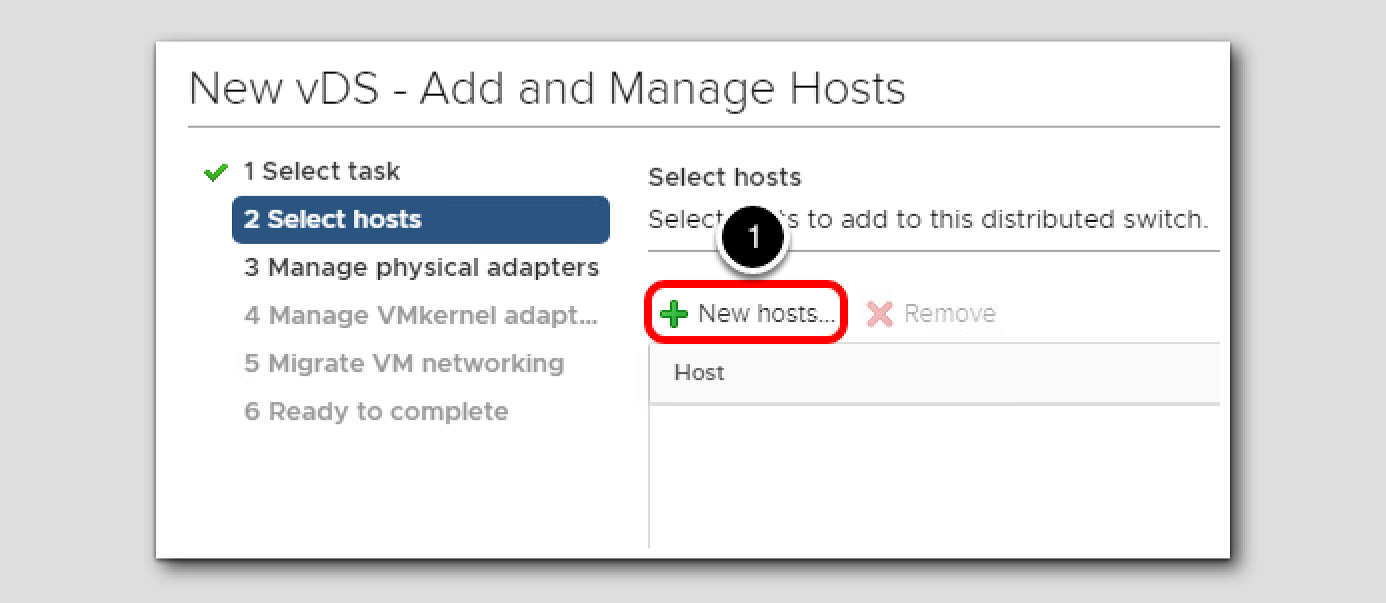
○ Remove hosts

Remove hosts from this distributed switch.

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

Select hosts

[294]



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

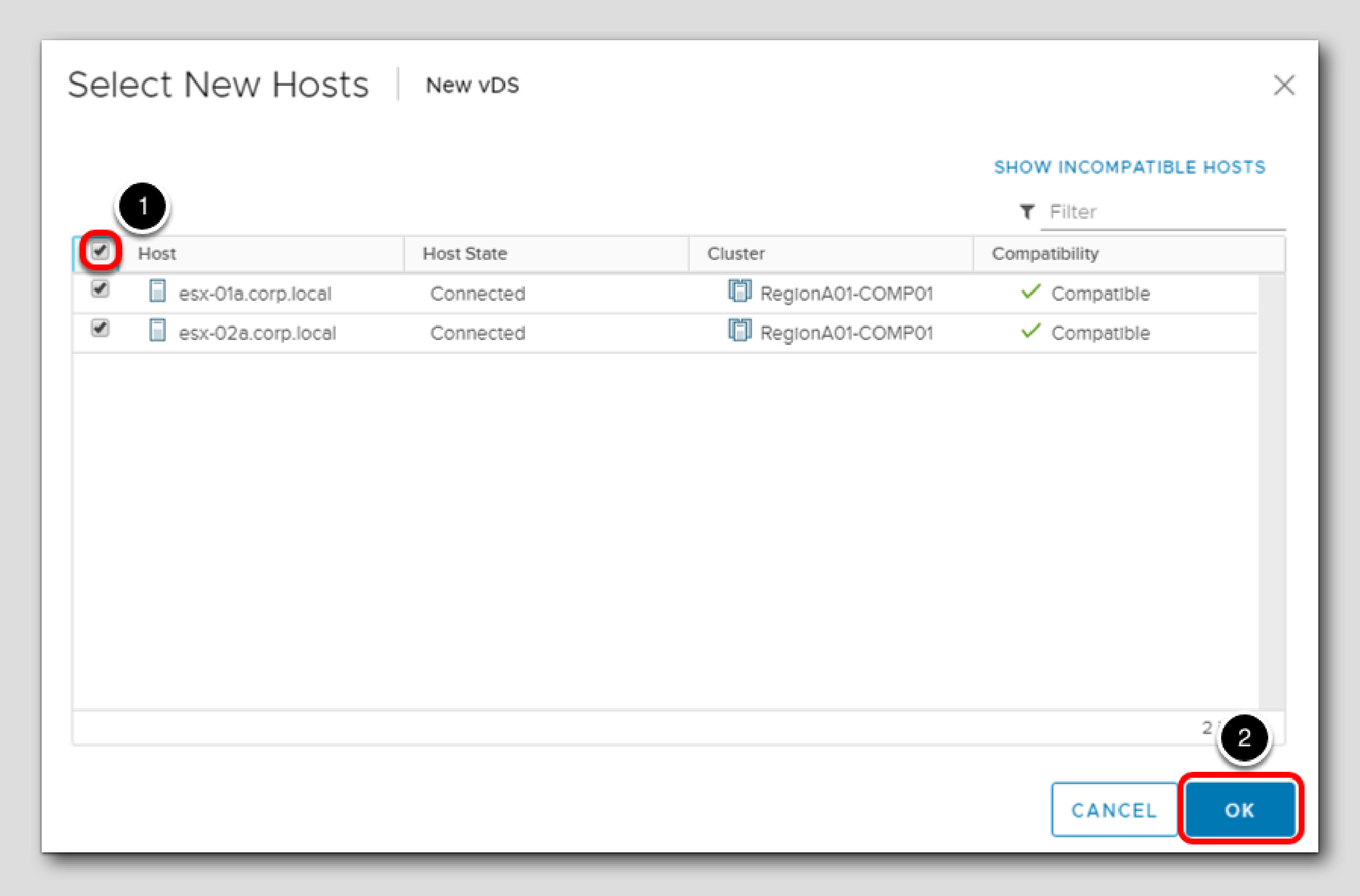
Select hosts

Select hosts to add to this distributed switch.

1. On the Select hosts page, click New hosts

Select New Hosts

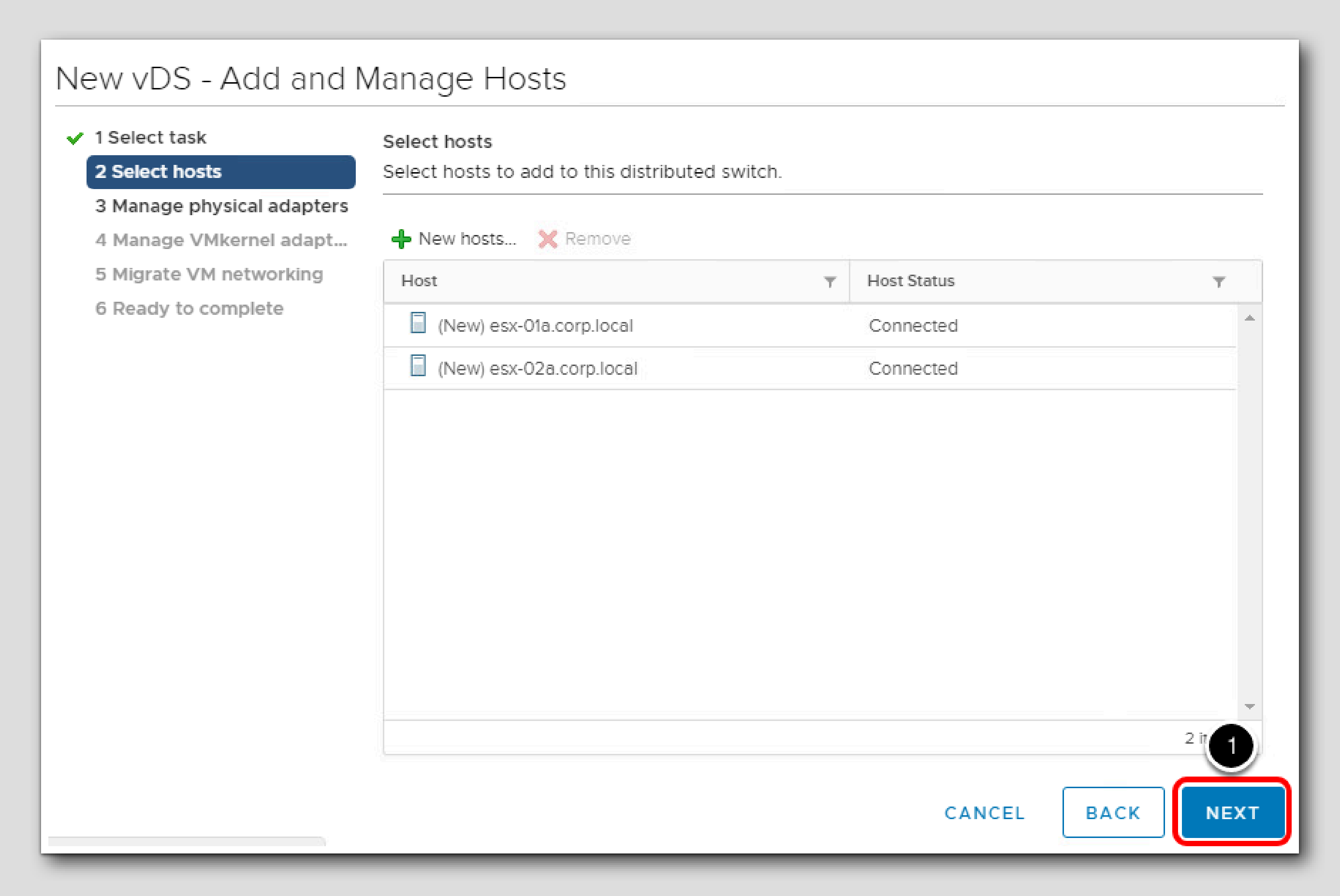
[295]



☑	Host	Host State	Cluster	Compatibility
☑	esx-01a.corp.local	Connected	RegionA01-COMP01	✓ Compatible
☑	esx-02a.corp.local	Connected	RegionA01-COMP01	✓ 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

Select hosts

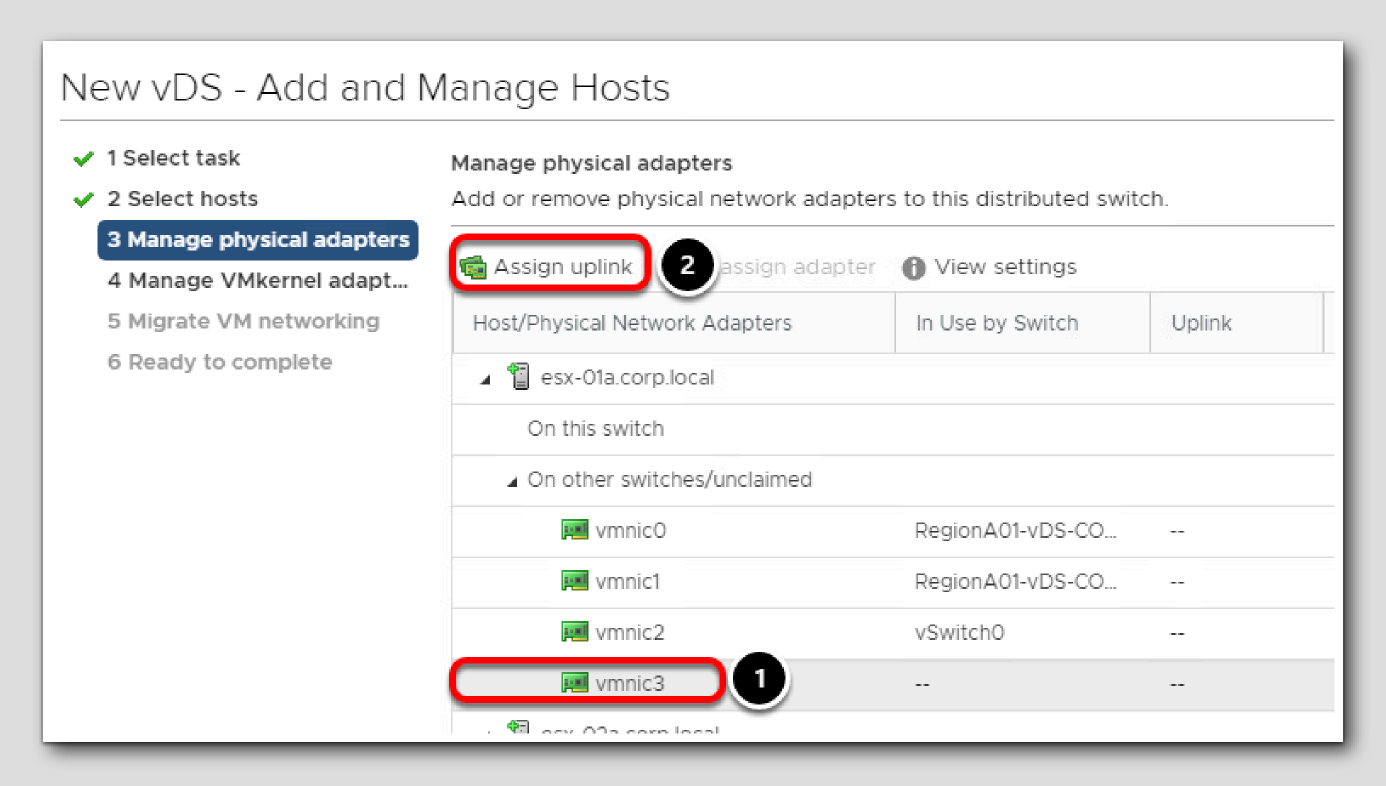
Select hosts to add to this distributed switch.

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

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

Assign physical adapters

[297]



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.

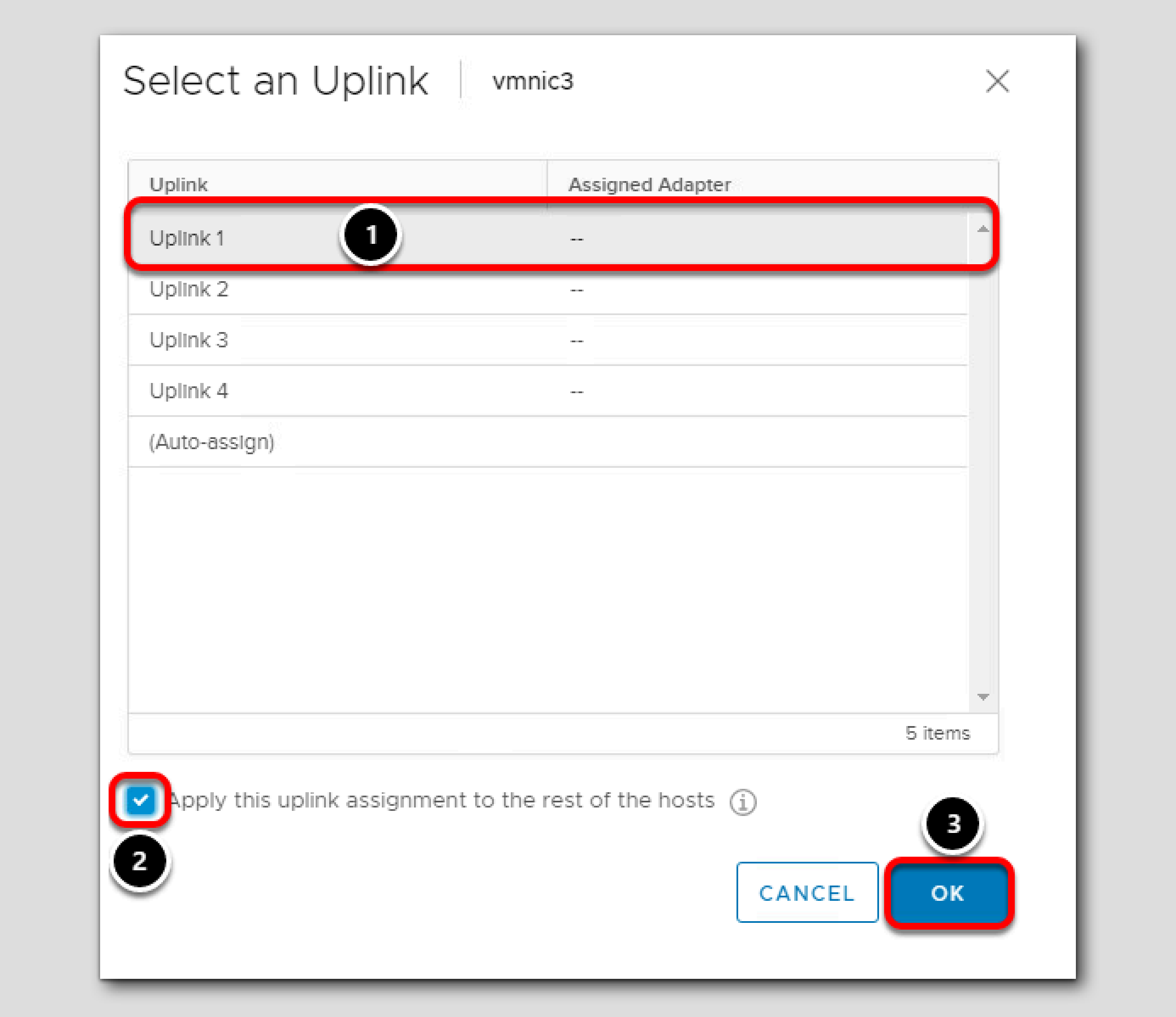
Host/Physical Network Adapters	In Use by Switch	Uplink
esx-01a.corp.local		
On this switch		
On other switches/unclaimed		
vmnic0	RegionA01-vDS-CO...	--
vmnic1	RegionA01-vDS-CO...	--
vmnic2	vSwitch0	--
vmnic3	--	--
esx-02a.corp.local		

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

[298]



Select an Uplink | vmnic3

Uplink	Assigned Adapter
Uplink 1	--
Uplink 2	--
Uplink 3	--
Uplink 4	--
(Auto-assign)	

5 items

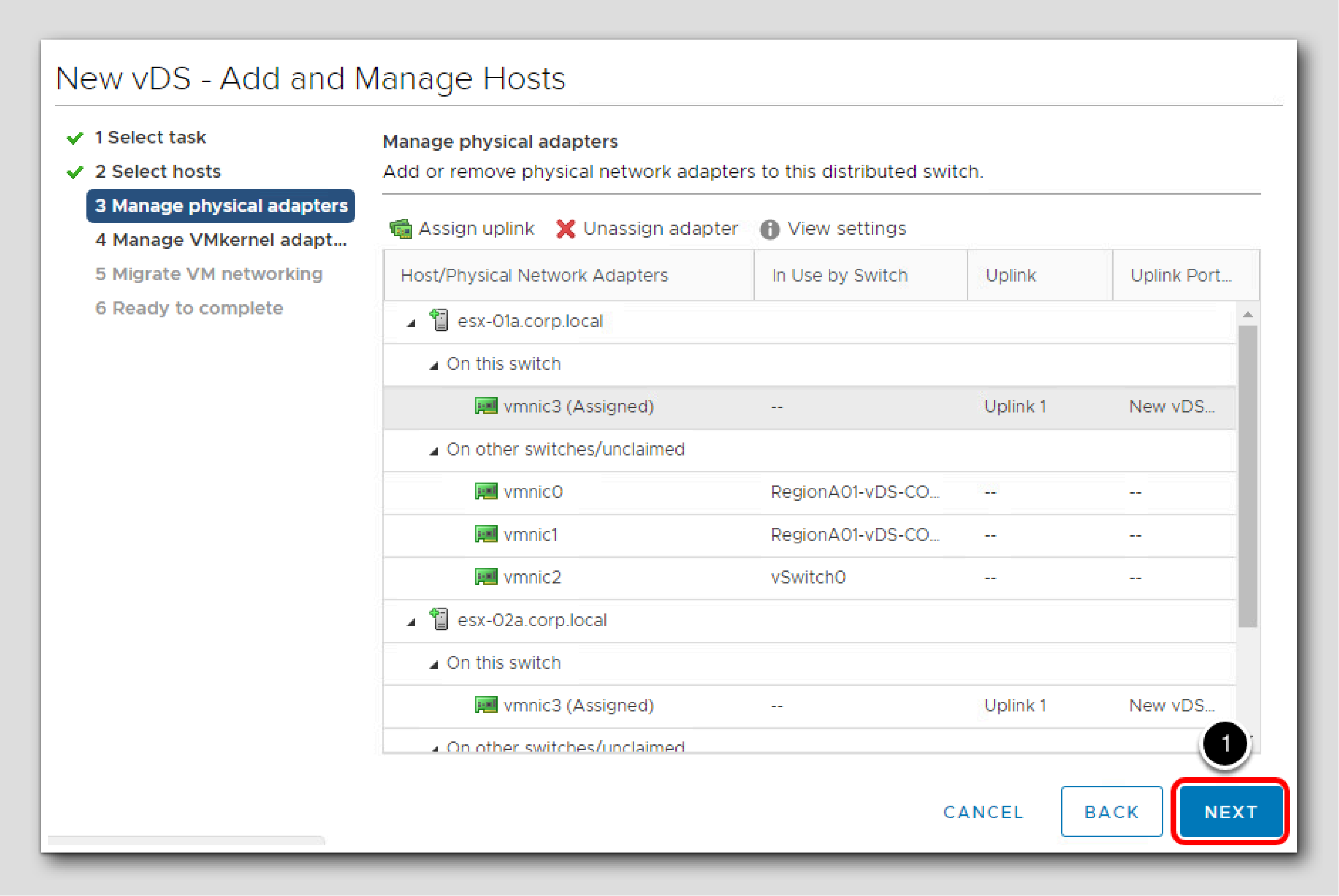
☑ Apply this uplink assignment to the rest of the hosts

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

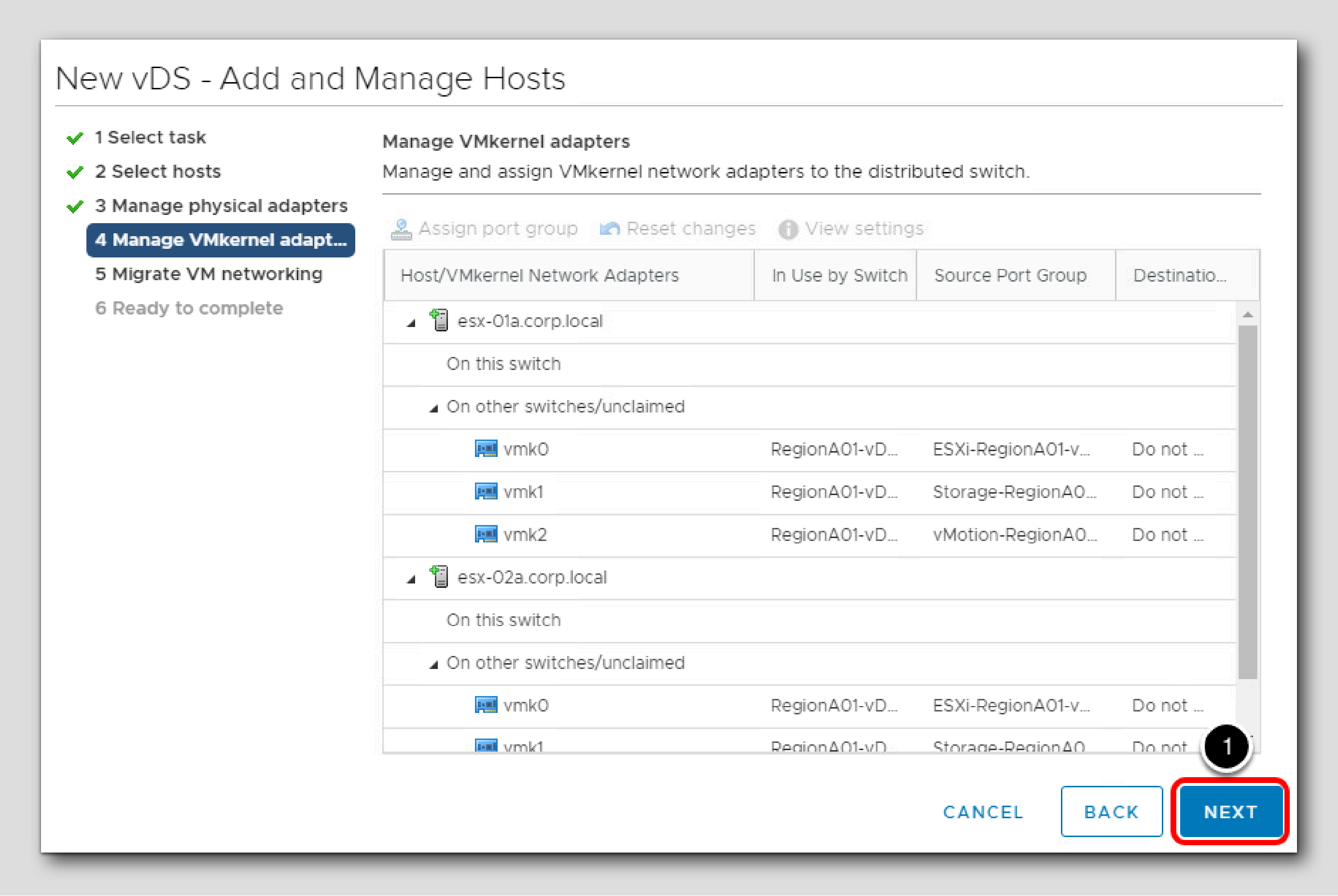
Manage physical adapters

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

Manage VMkernel adapters



New vDS - Add and Manage Hosts

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

Manage VMkernel adapters

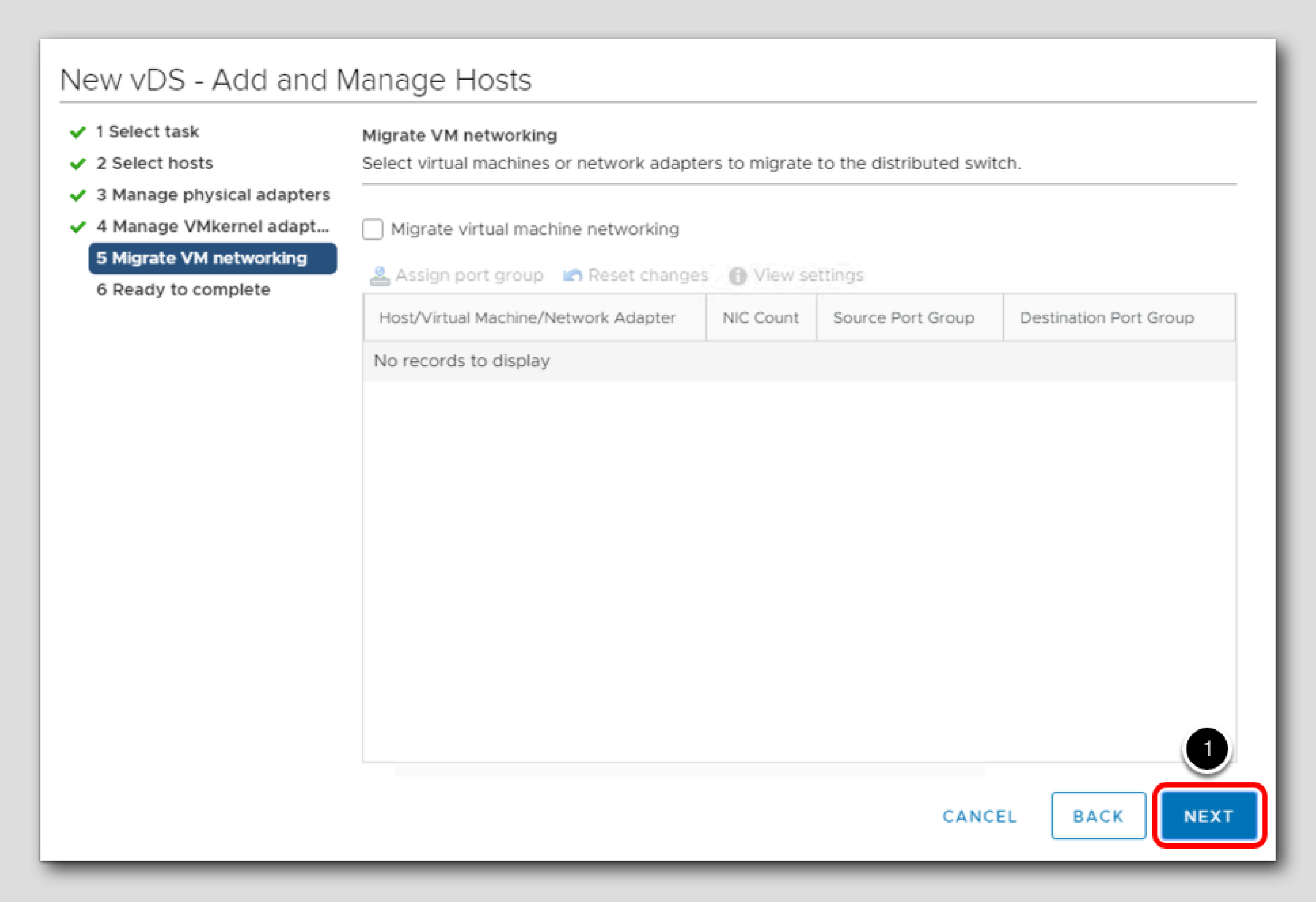
Manage and assign VMkernel network adapters to the distributed switch.

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

Migrate VM networking

[301]



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.

□ Migrate virtual machine networking

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

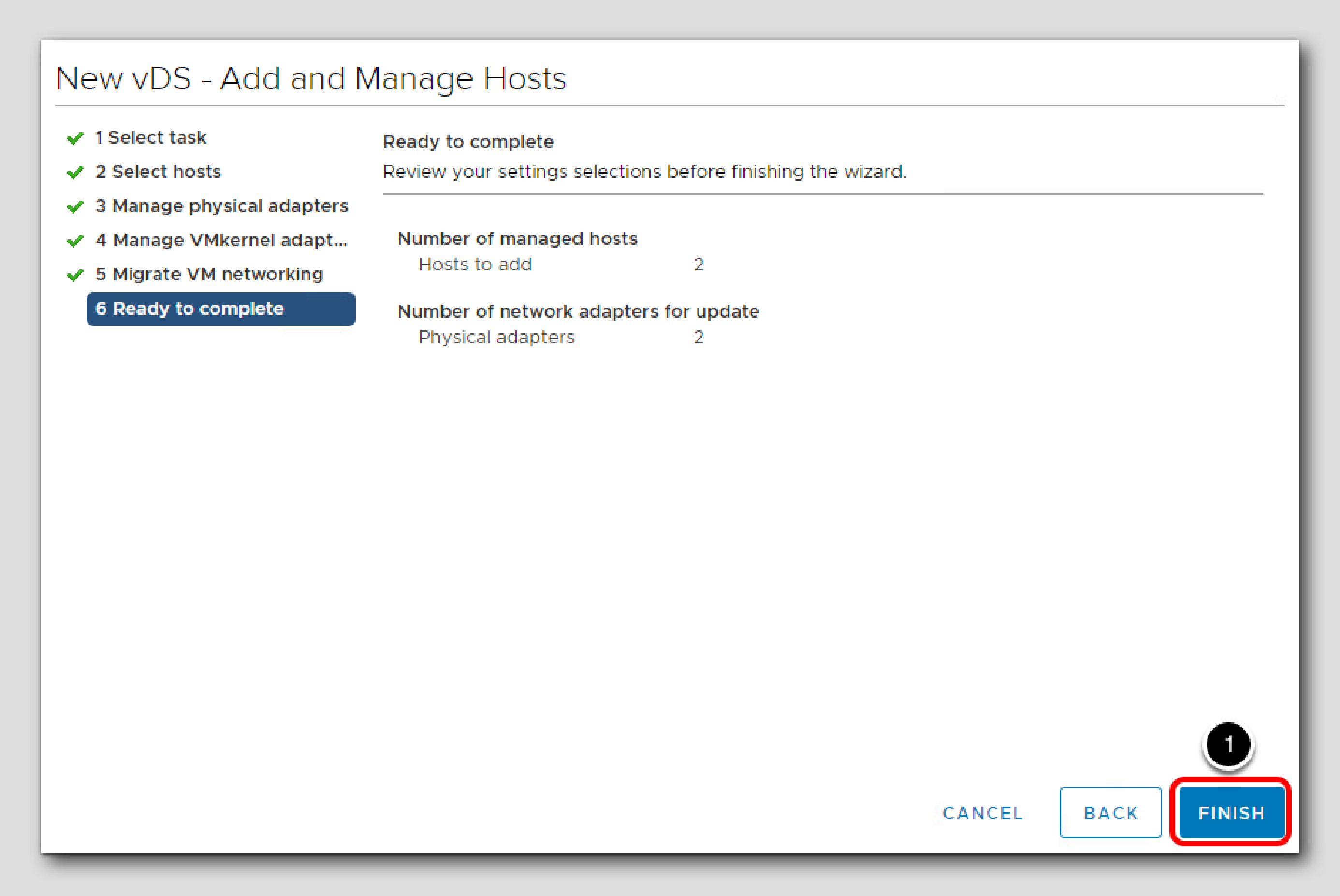
The add hosts wizard also gives us the ability to migrate VMs from one distributed switch to another on this page. While this action can be done here, we will be doing this in the next lesson.

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

[302]



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

Ready to complete

Review your settings selections before finishing the wizard.

Number of managed hosts

Hosts to add	2

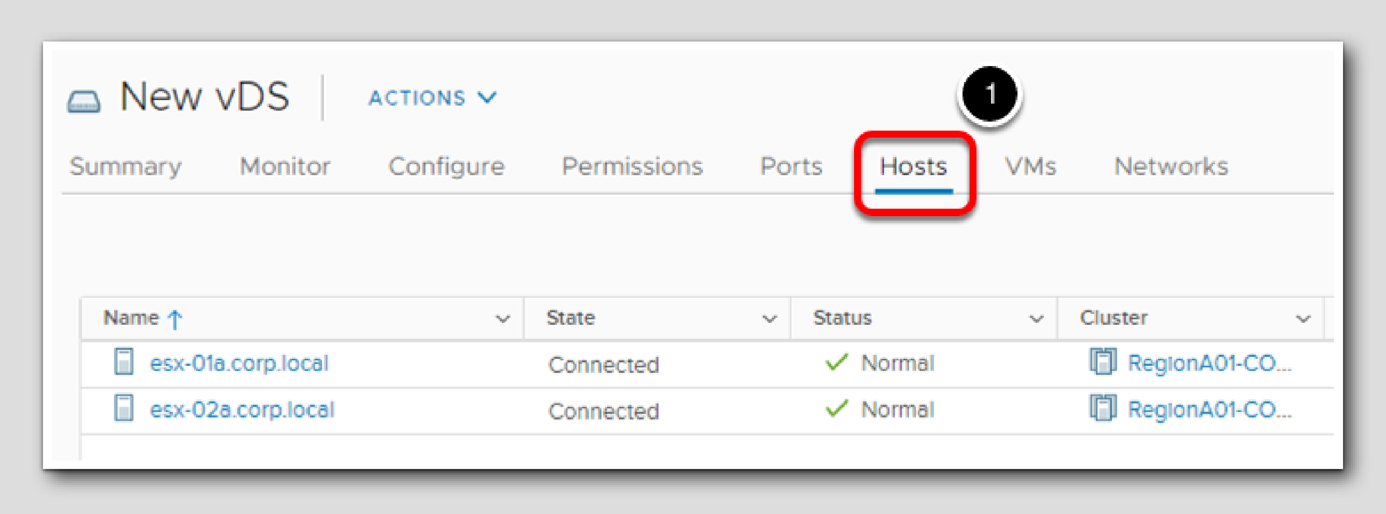
Number of network adapters for update

Physical adapters	2

1. On the Ready to Complete page, click Finish

Explore your new vDS

[303]



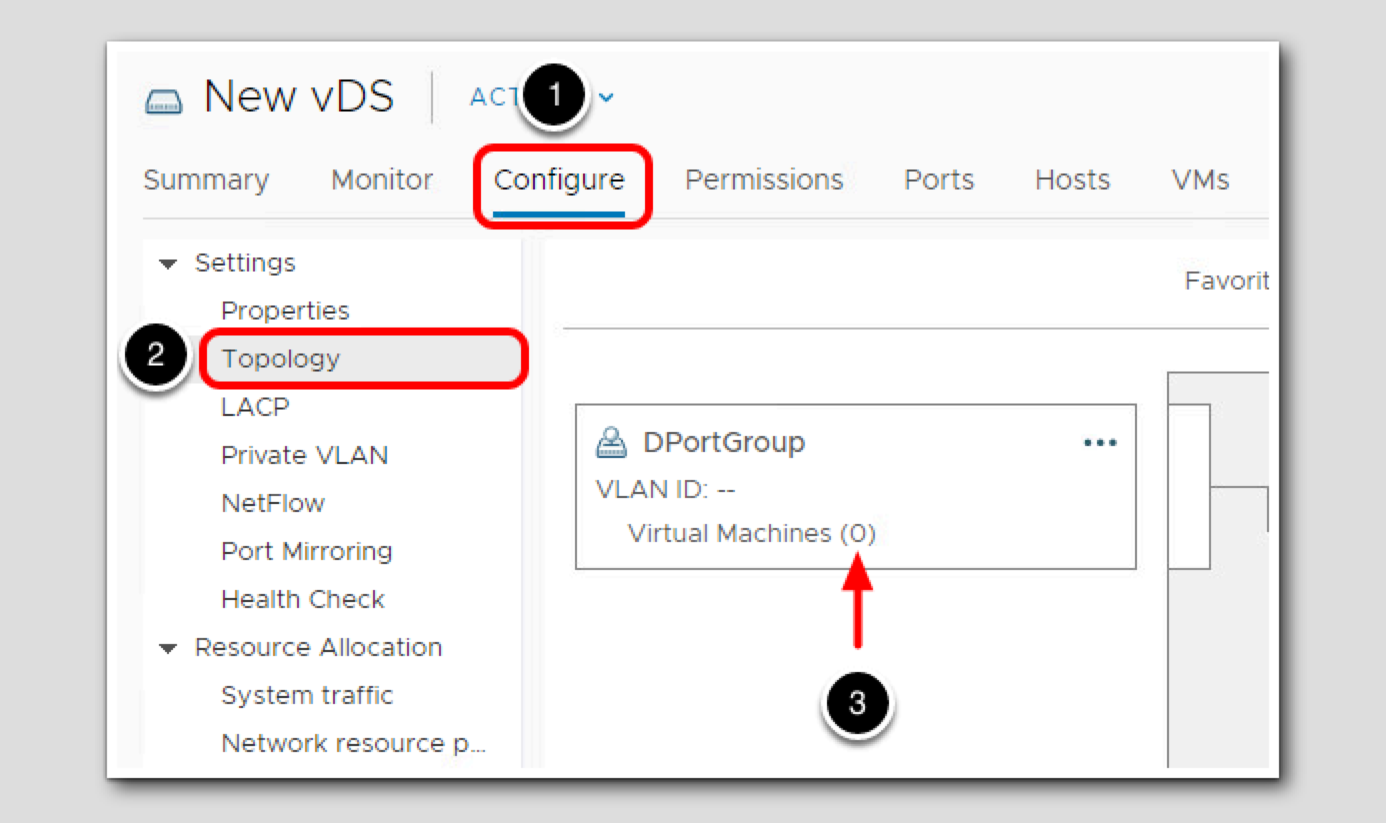
Name ↑	State	Status	Cluster
esx-01a.corp.local	Connected	✓ Normal	RegionA01-CO...
esx-02a.corp.local	Connected	✓ Normal	RegionA01-CO...

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

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

Topology

[304]



1. Click Configure
2. Click Topology

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

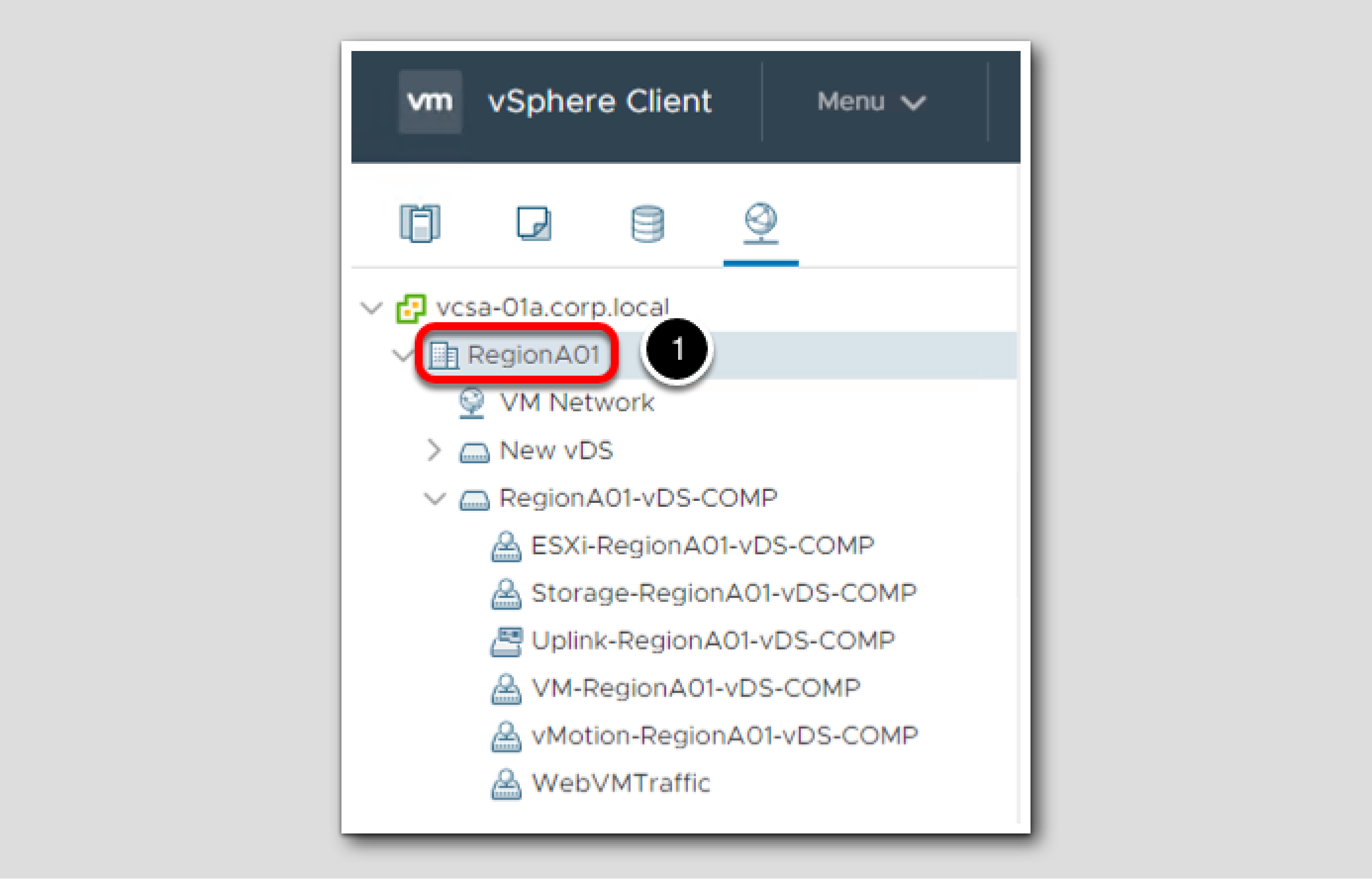
Migrating VMs from vDS to vDS

[305]

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



vSphere Client

vcsa-01a.corp.local

RegionA01

VM Network

New vDS

RegionA01-vDS-COMP

ESXi-RegionA01-vDS-COMP

Storage-RegionA01-vDS-COMP

Uplink-RegionA01-vDS-COMP

VM-RegionA01-vDS-COMP

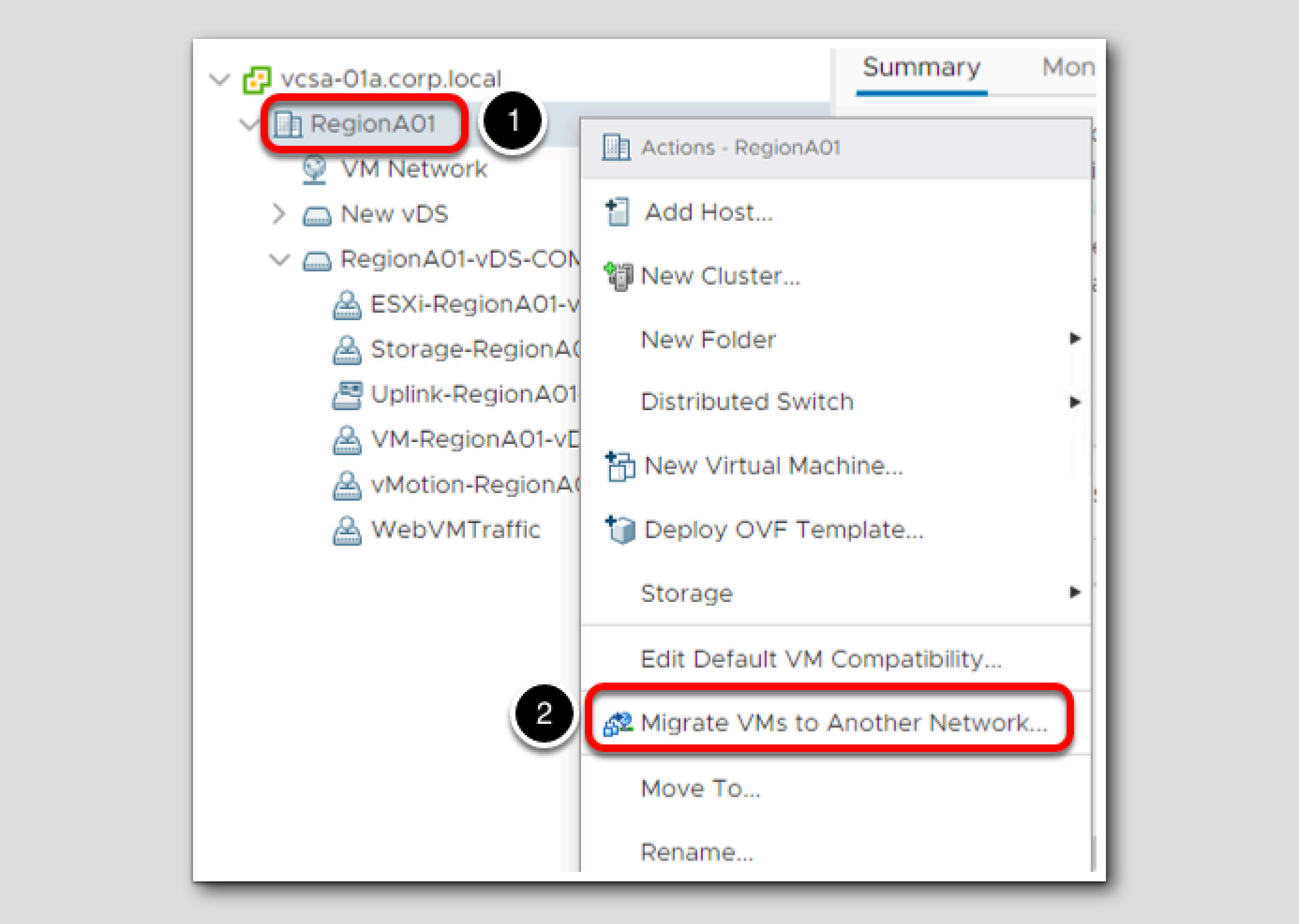
vMotion-RegionA01-vDS-COMP

WebVMTraffic

1. To get started, click on RegionA01

Migrate VMs

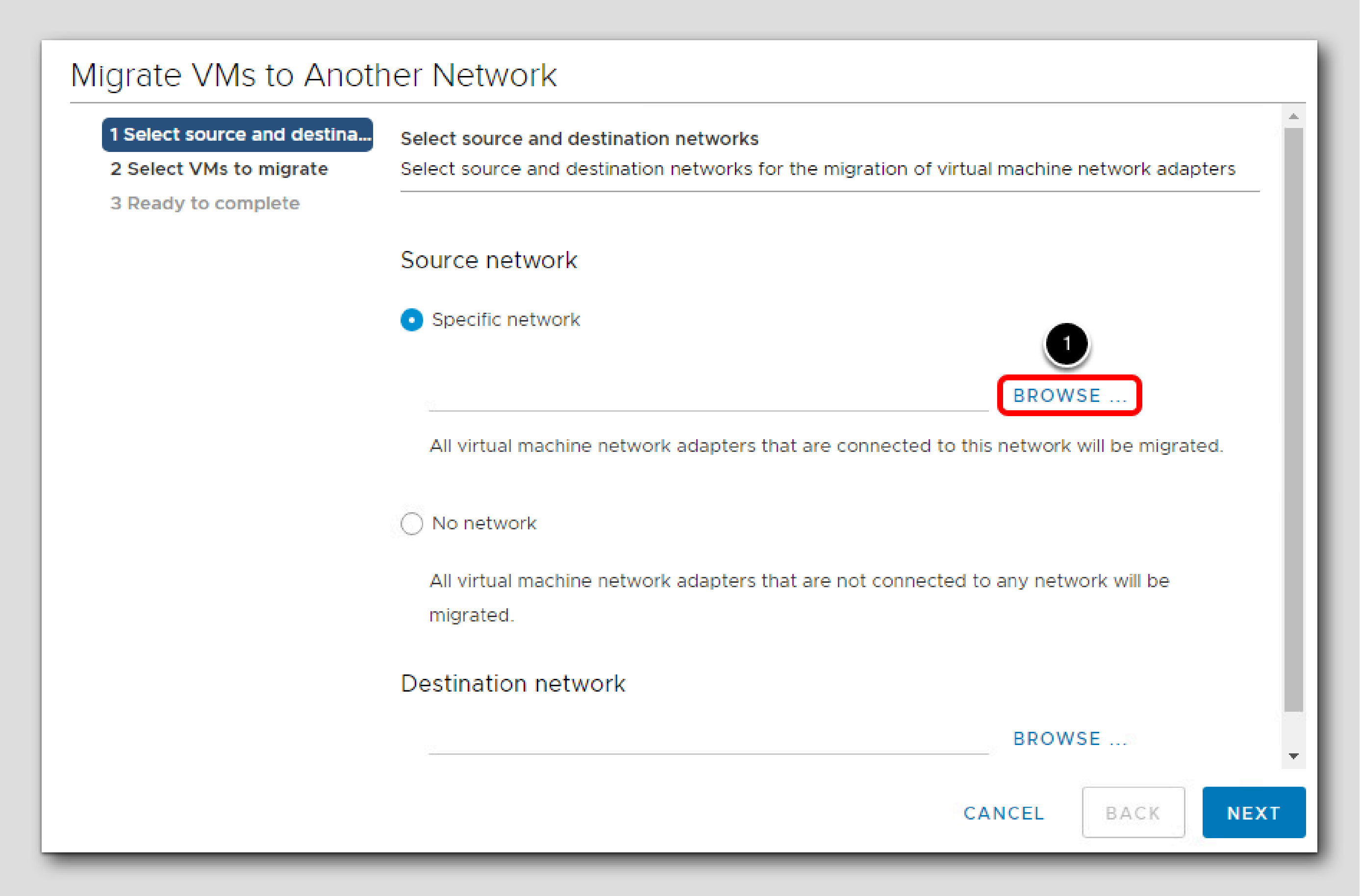
[307]



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

Select source network

[308]



Migrate VMs to Another Network

Select source and destination networks

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

Source network

● Specific network

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

○ No network

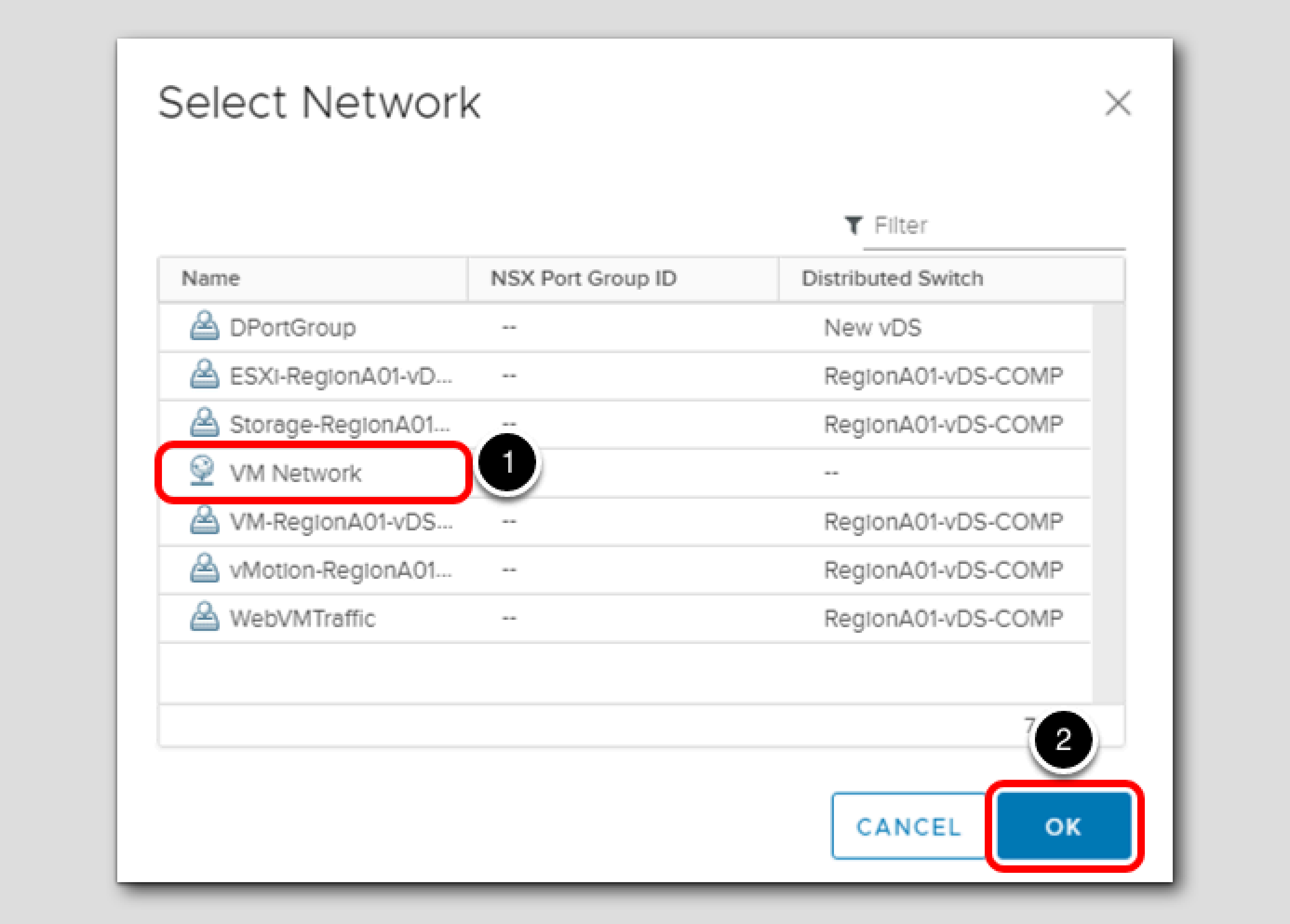
All virtual machine network adapters that are not connected to any network will be migrated.

Destination network

1. Under **Source network** click on **Browse**

VM Network

[309]



Select Network

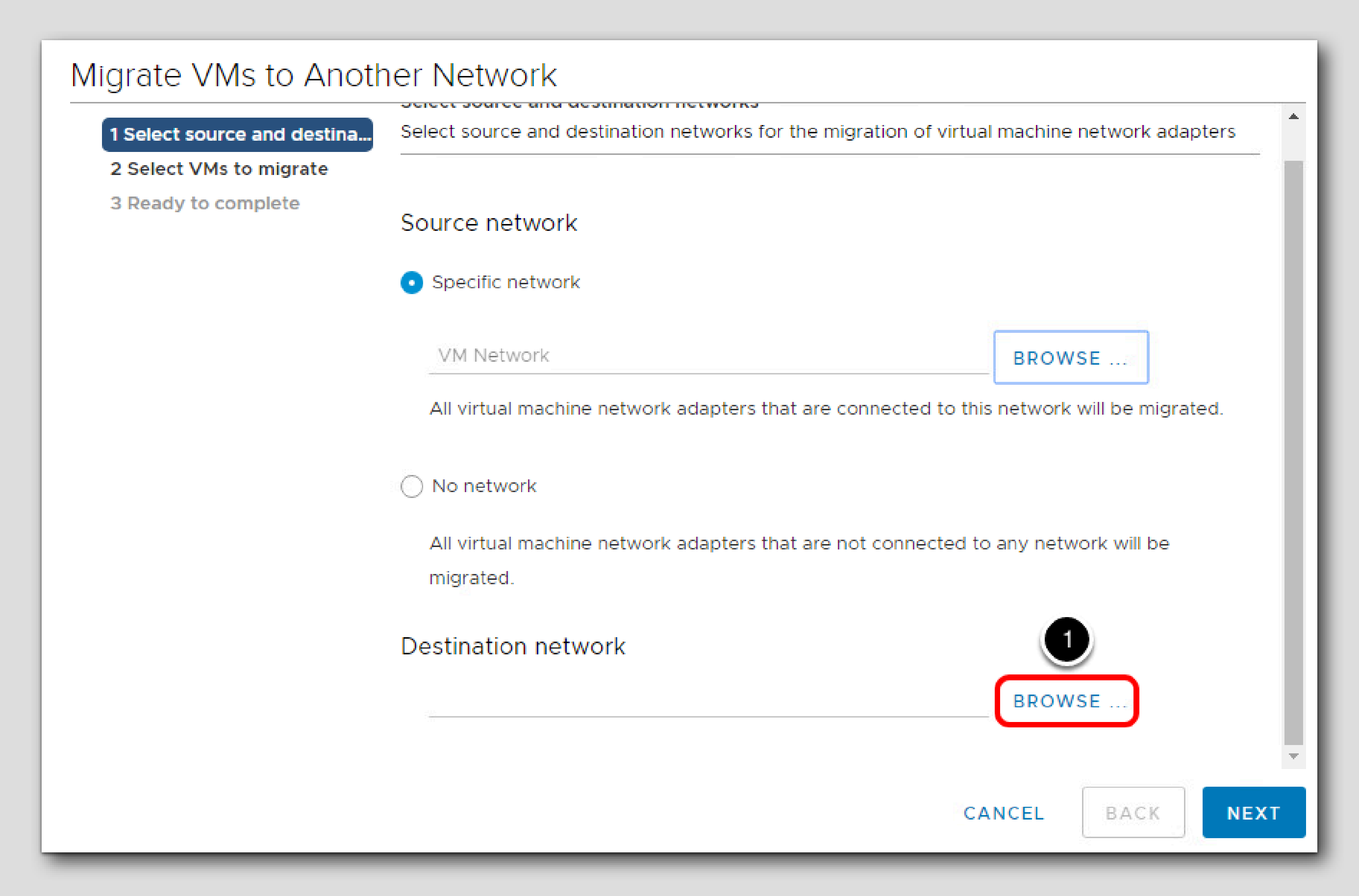
Name	NSX Port Group ID	Distributed Switch
DPortGroup	--	New vDS
ESXi-RegionA01-vD...	--	RegionA01-vDS-COMP
Storage-RegionA01...	--	RegionA01-vDS-COMP
VM Network		--
VM-RegionA01-vDS...	--	RegionA01-vDS-COMP
vMotion-RegionA01...	--	RegionA01-vDS-COMP
WebVMTraffic	--	RegionA01-vDS-COMP

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

[310]



Migrate VMs to Another Network

Select source and destination networks

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

Source network

● Specific network

VM Network

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

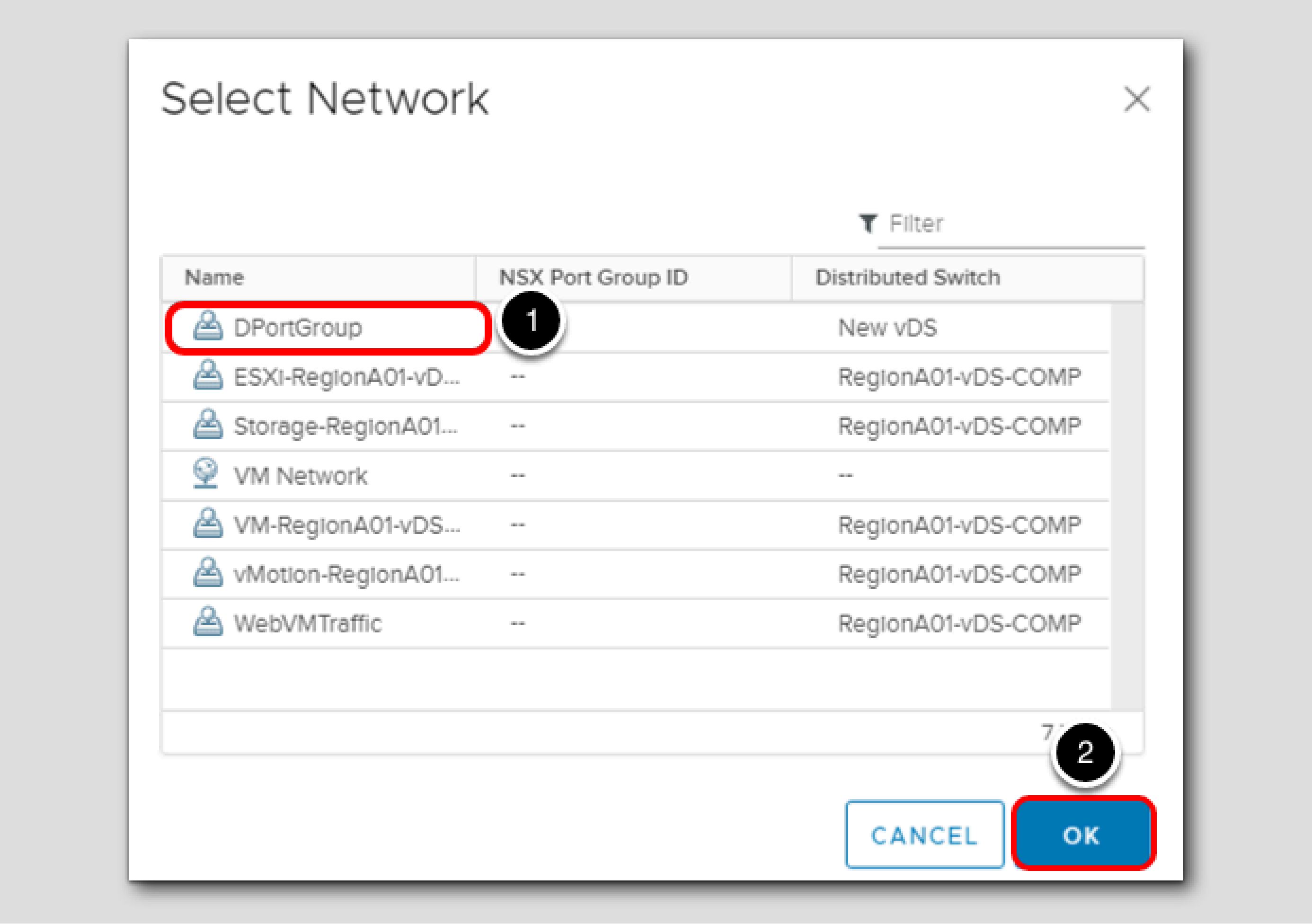
○ No network

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

Destination network

1. Under Destination network select Browse

DPortGroup



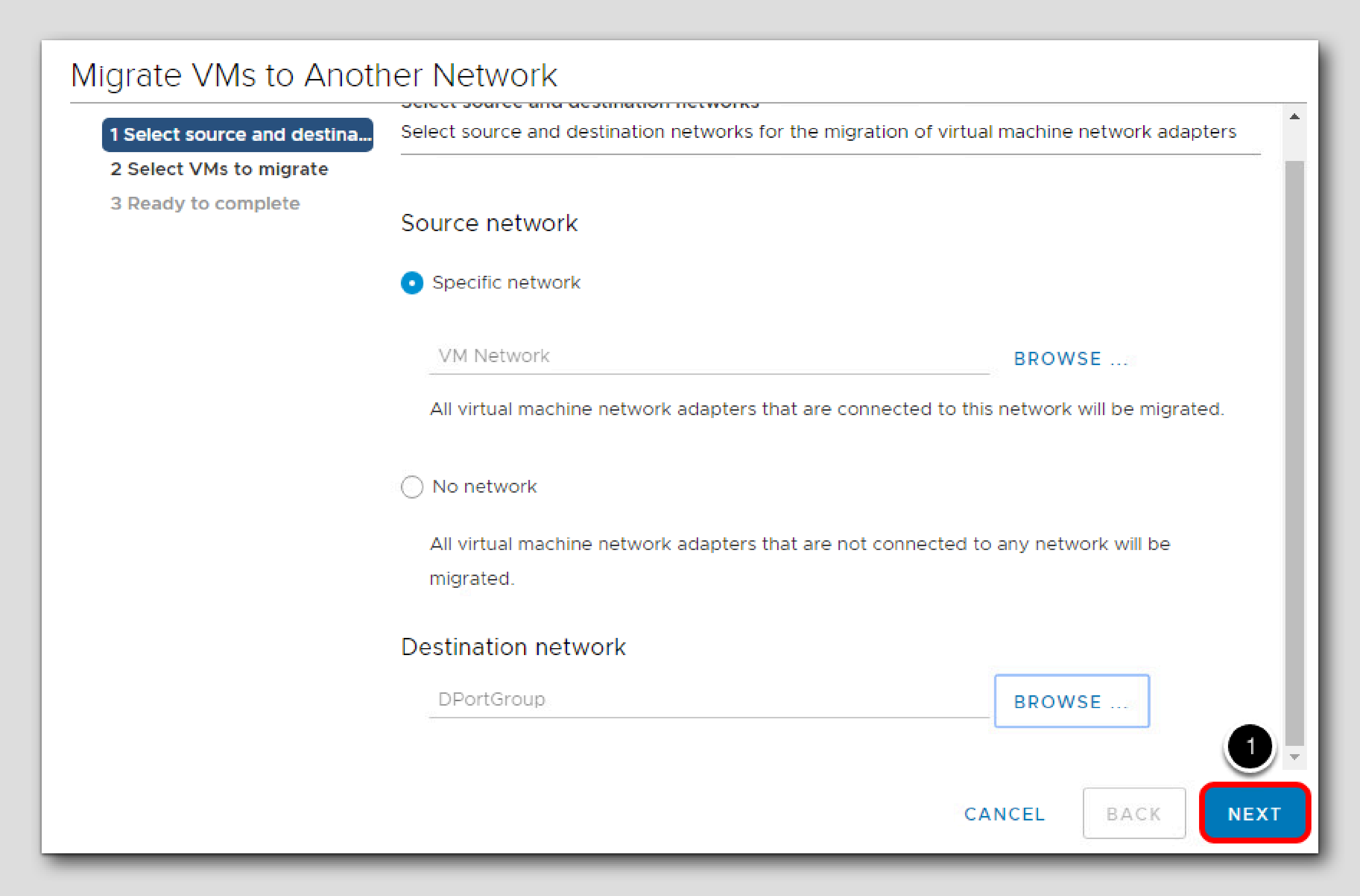
Name	NSX Port Group ID	Distributed Switch
DPortGroup		New vDS
ESXi-RegionA01-vD...	--	RegionA01-vDS-COMP
Storage-RegionA01...	--	RegionA01-vDS-COMP
VM Network	--	--
VM-RegionA01-vDS...	--	RegionA01-vDS-COMP
vMotion-RegionA01...	--	RegionA01-vDS-COMP
WebVMTraffic	--	RegionA01-vDS-COMP

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

[312]



Migrate VMs to Another Network

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

Source network

● Specific network

VM Network

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.

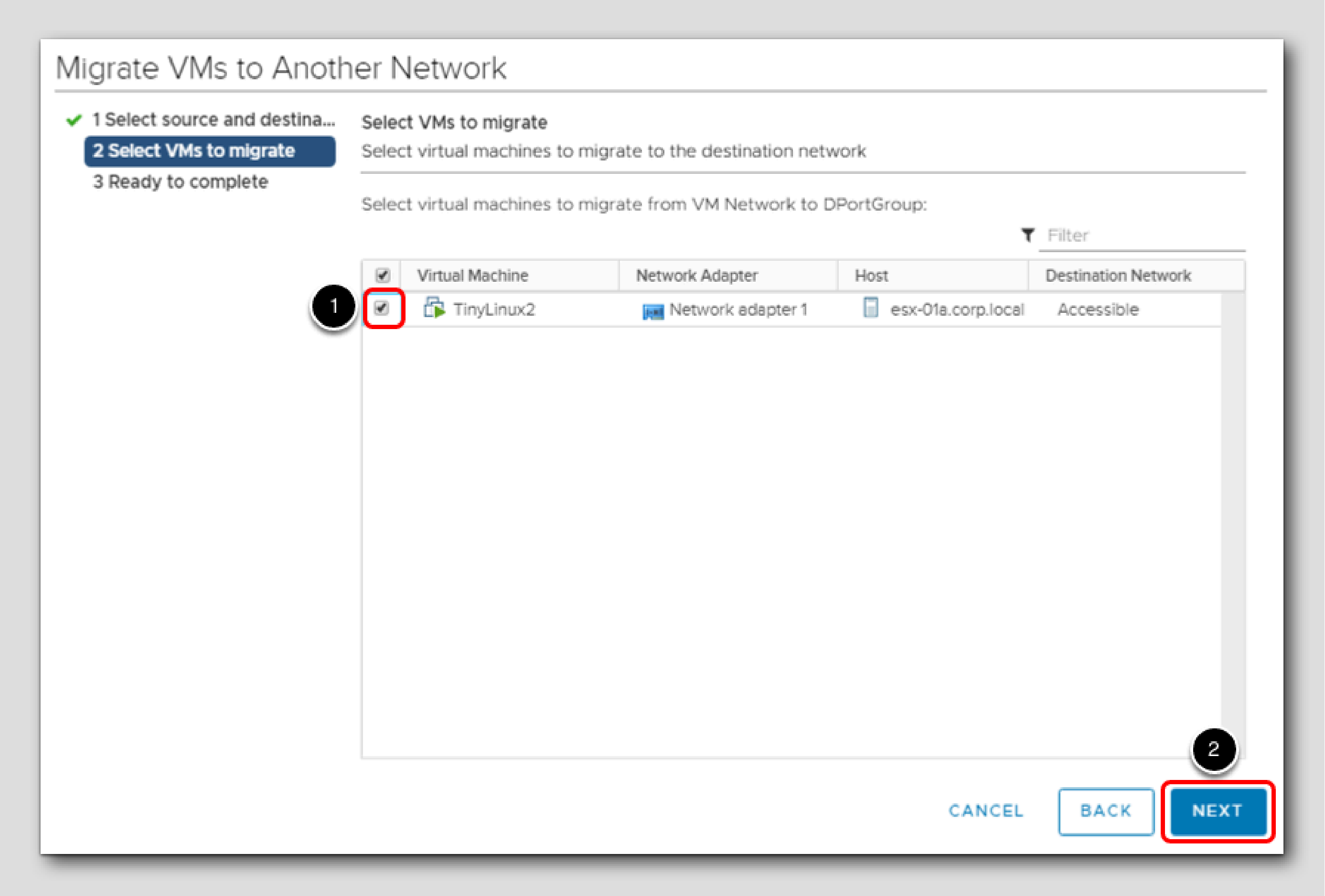
Destination network

DPortGroup

1. Click Next

Select VM to migrate

[313]



Migrate VMs to Another Network

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

Select VMs to migrate

Select virtual machines to migrate to the destination network

Select virtual machines to migrate from VM Network to DPortGroup:

☑	Virtual Machine	Network Adapter	Host	Destination Network
☑	TinyLinux2	Network adapter 1	esx-01a.corp.local	Accessible

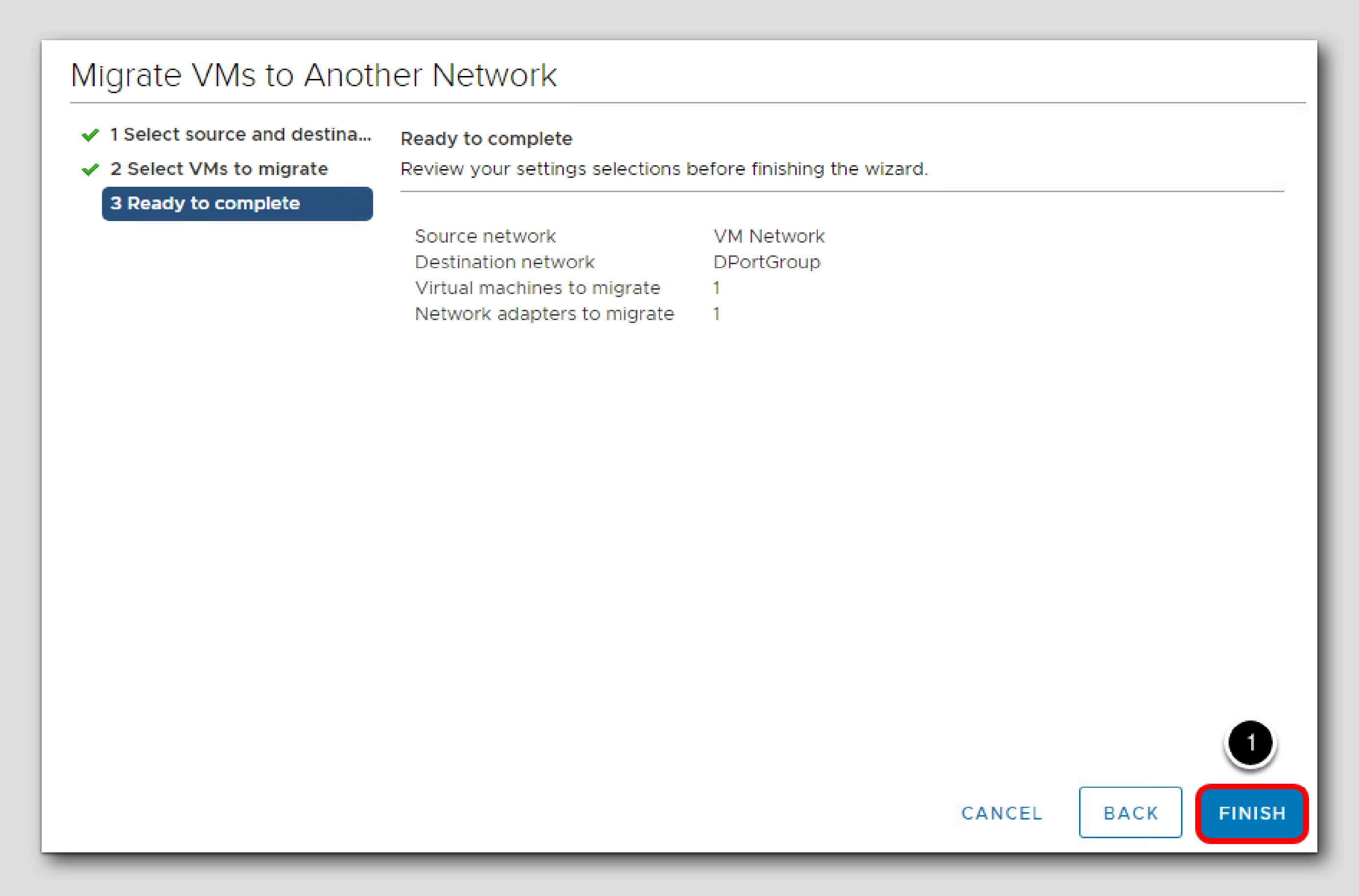
1. Click on TinyLinux2

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

2. Click Next.

Ready to Complete

[314]



Migrate VMs to Another Network

Ready to complete

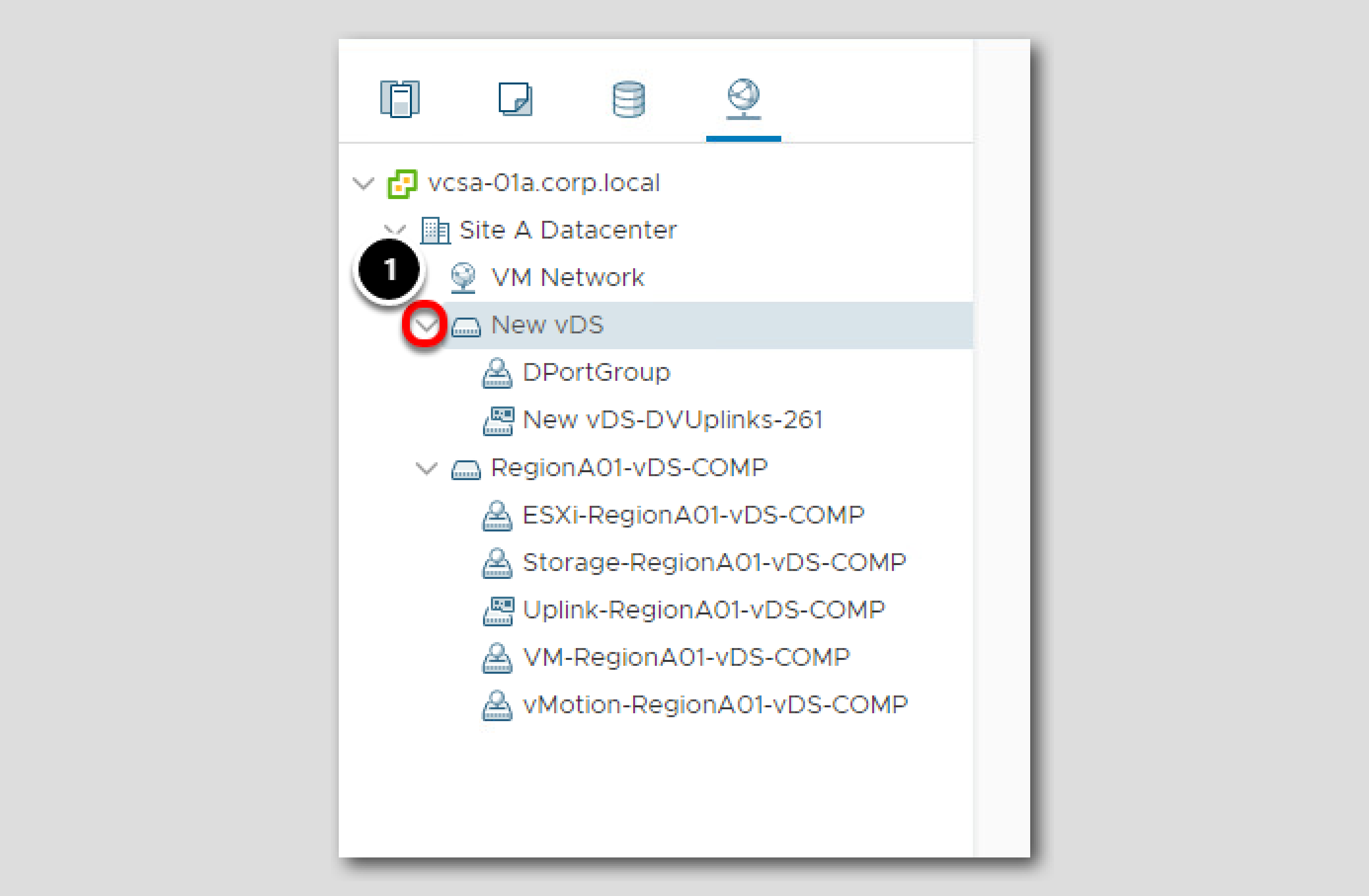
Review your settings selections before finishing the wizard.

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

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

Explore your changes

[315]

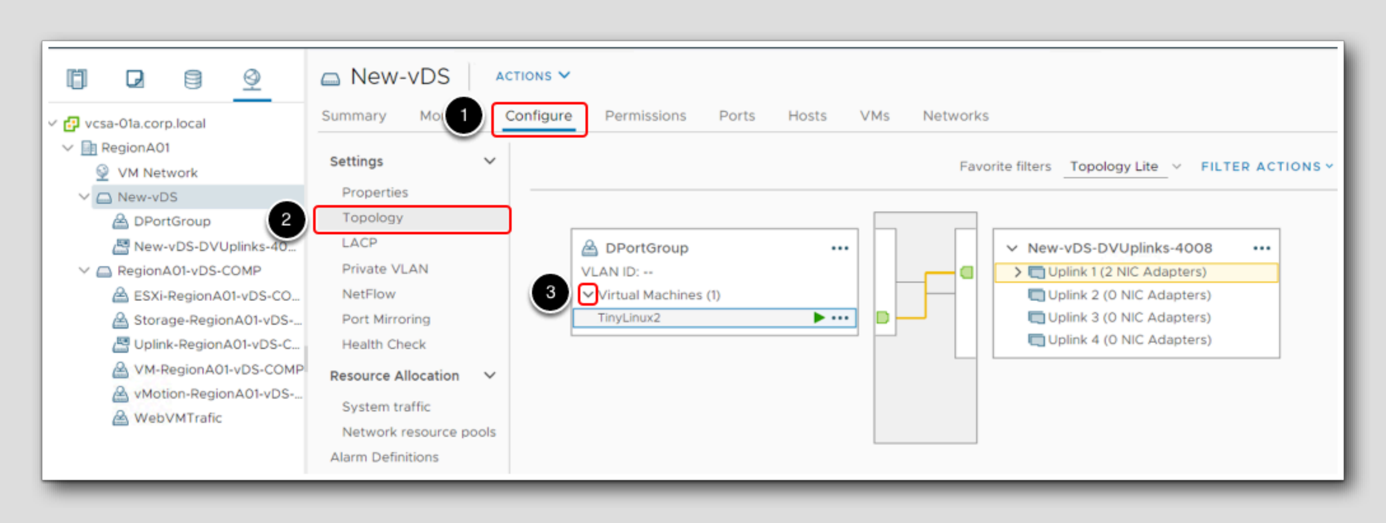


- vcsa-01a.corp.local
  - Site A Datacenter
    - VM Network
    - New vDS
      - DPortGroup
      - New vDS-DVUplinks-261
    - RegionA01-vDS-COMP
      - ESXi-RegionA01-vDS-COMP
      - Storage-RegionA01-vDS-COMP
      - Uplink-RegionA01-vDS-COMP
      - VM-RegionA01-vDS-COMP
      - vMotion-RegionA01-vDS-COMP

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

New-vDS Topology Map

[316]



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

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

Adding and Configuring a vSphere Distributed Switch

[317]

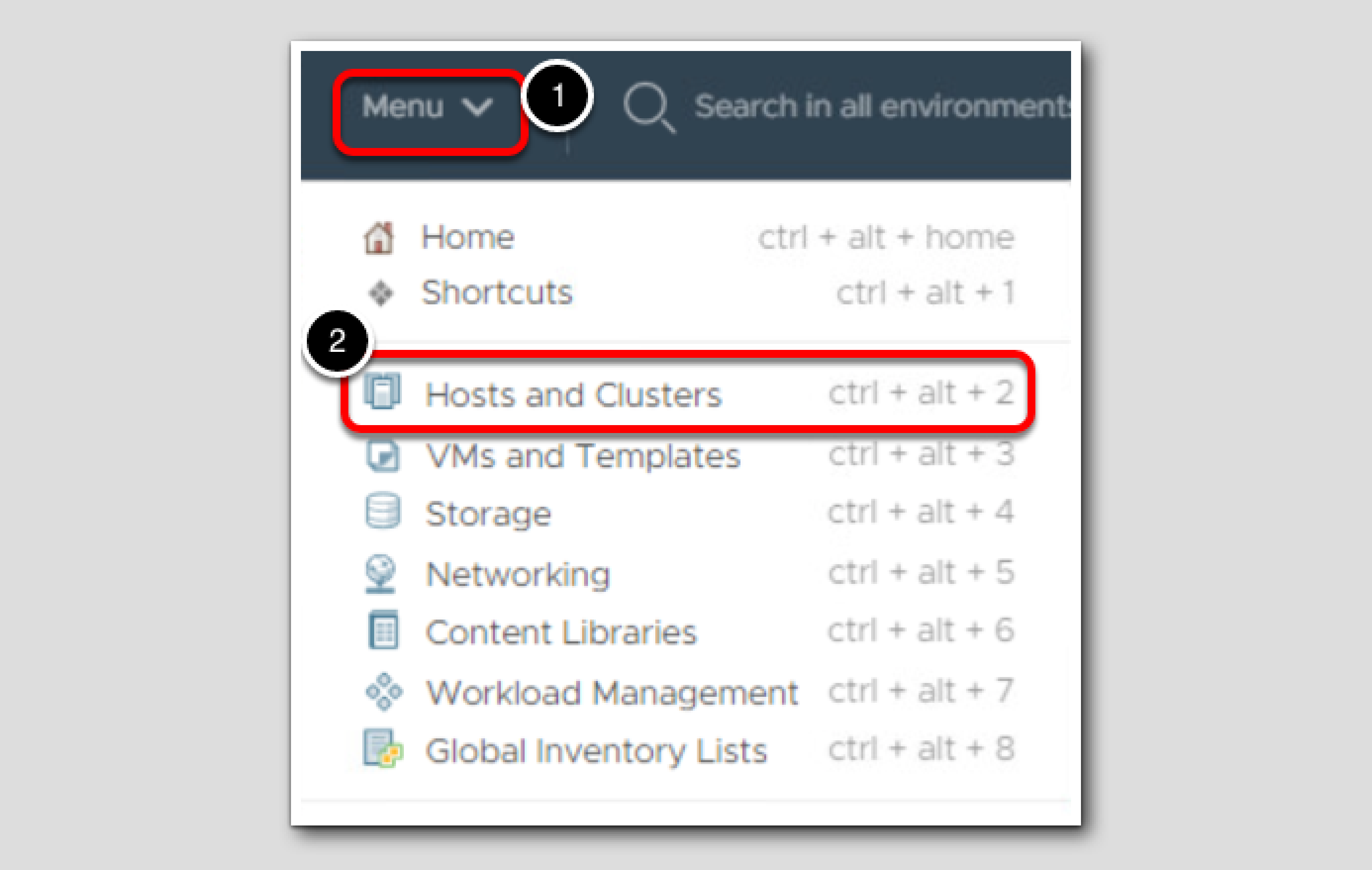
This lesson will walk you through adding and configuring a Distributed Switch.

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

1. Keep the default values and click **Next**

Select Host and Clusters

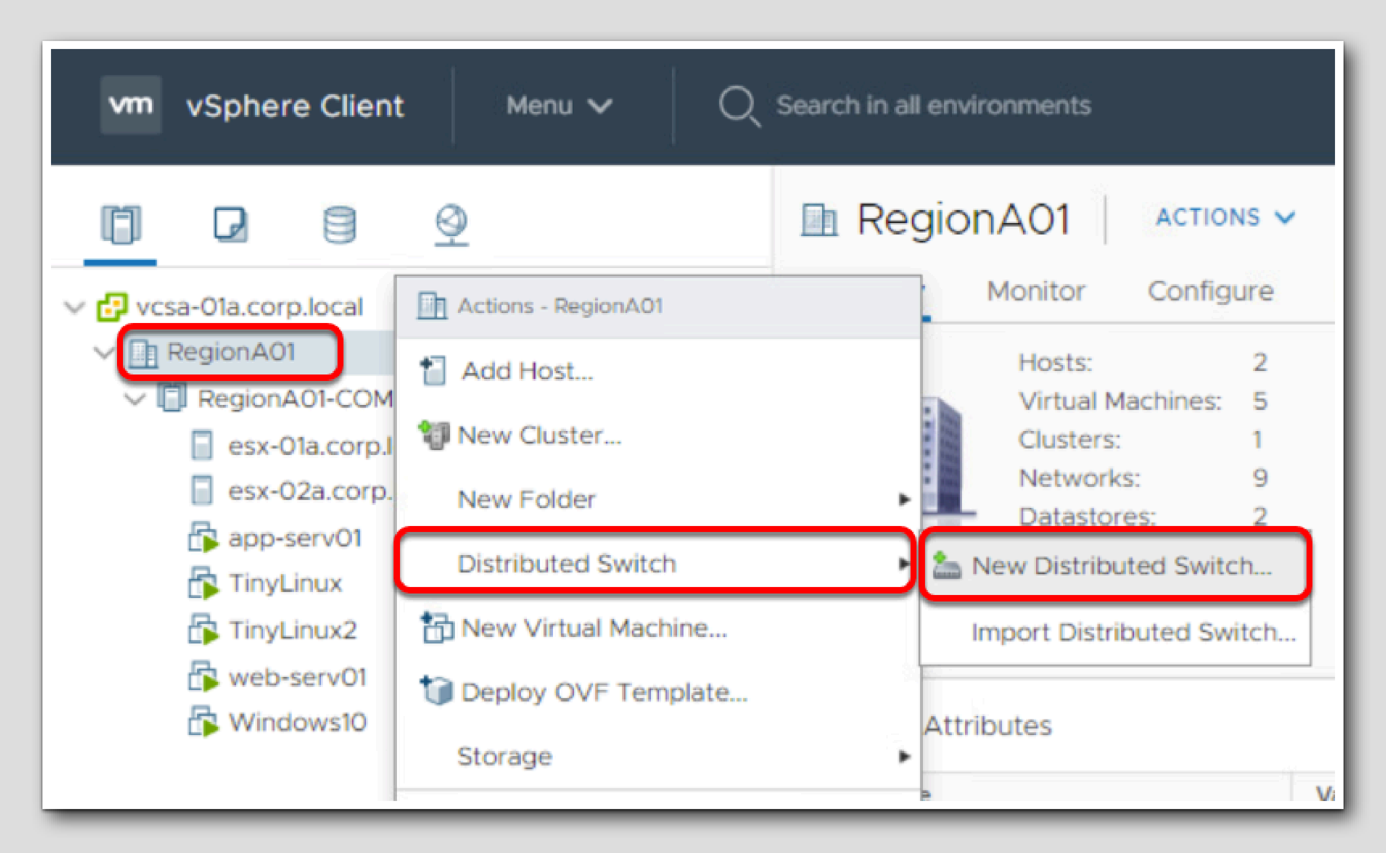
[318]


Menu
1
Search in all environments
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
2
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Workload Management ctrl + alt + 7
Global Inventory Lists ctrl + alt + 8

1. Click Menu
2. Click Host and Clusters

Add a vSphere Distributed Switch using the vSphere Web Client

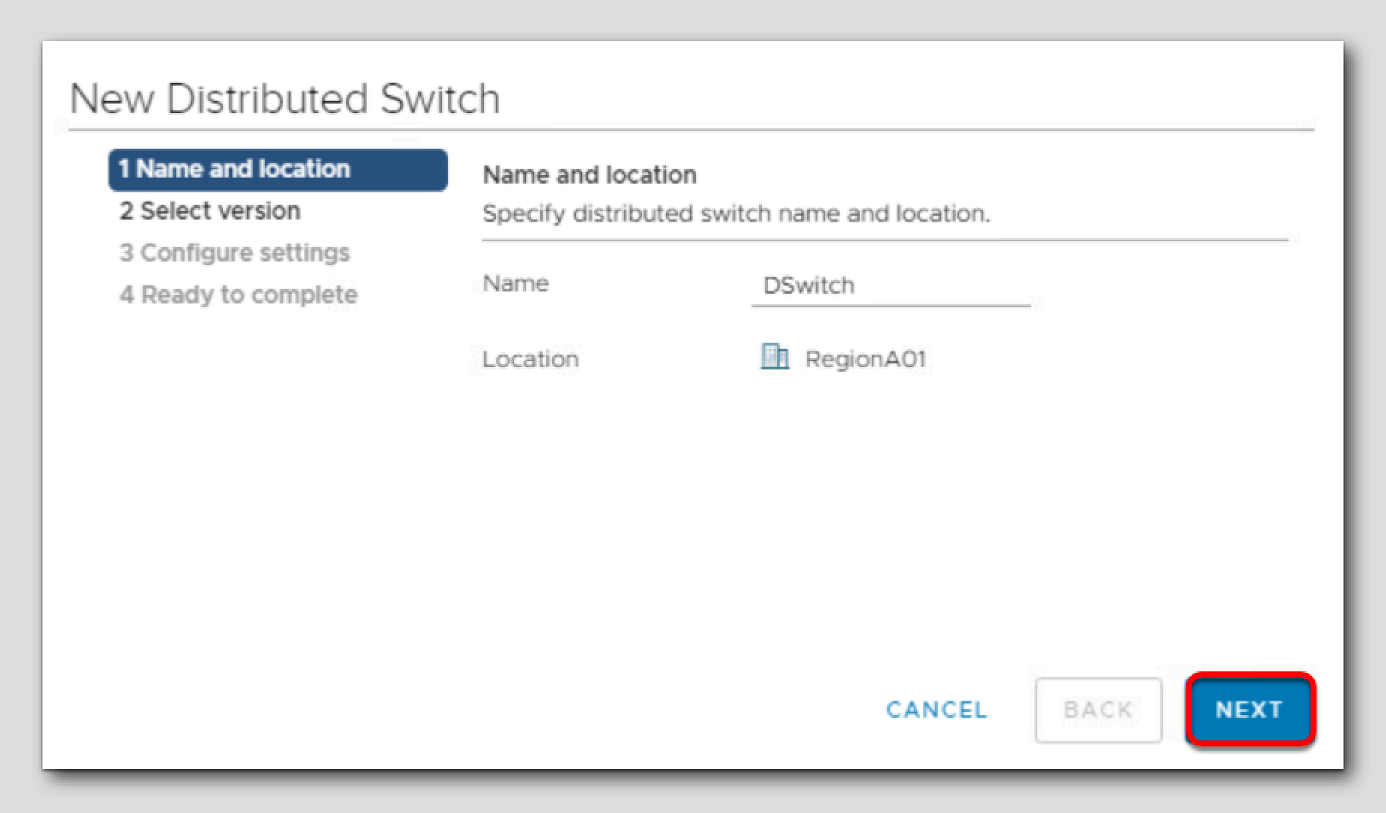
[319]



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

Name and Location

[320]



New Distributed Switch

Name and location

Specify distributed switch name and location.

Name DSwitch

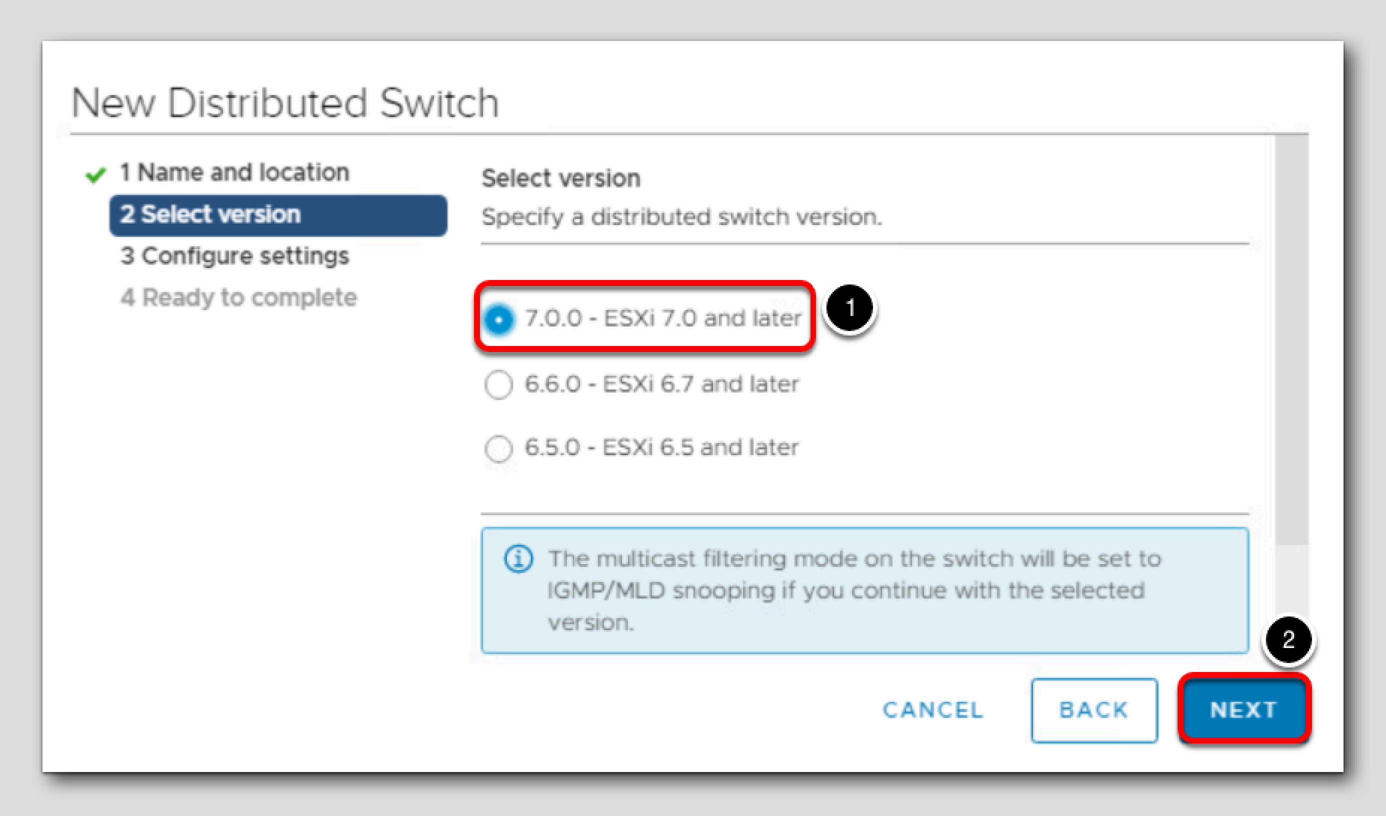
Location RegionA01

Keep the default name for the new distributed switch.

1. Click Next

Select version

[321]



New Distributed Switch

Select version

Specify a distributed switch version.

● 7.0.0 - ESXi 7.0 and later

○ 6.6.0 - ESXi 6.7 and later

○ 6.5.0 - ESXi 6.5 and later

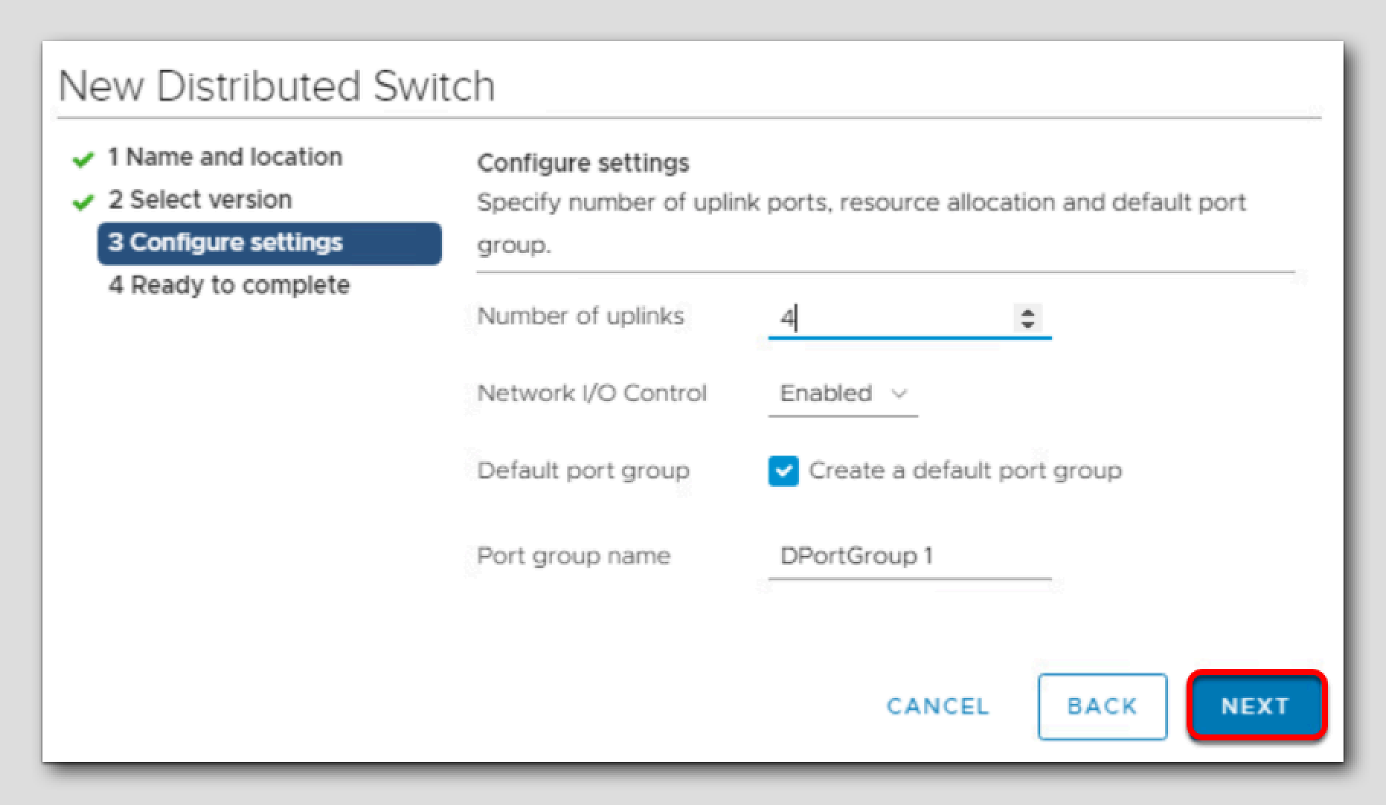
The multicast filtering mode on the switch will be set to IGMP/MLD snooping if you continue with the selected version.

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

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

Edit Settings

[322]



New Distributed Switch

Configure settings

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

Number of uplinks: 4

Network I/O Control: Enabled

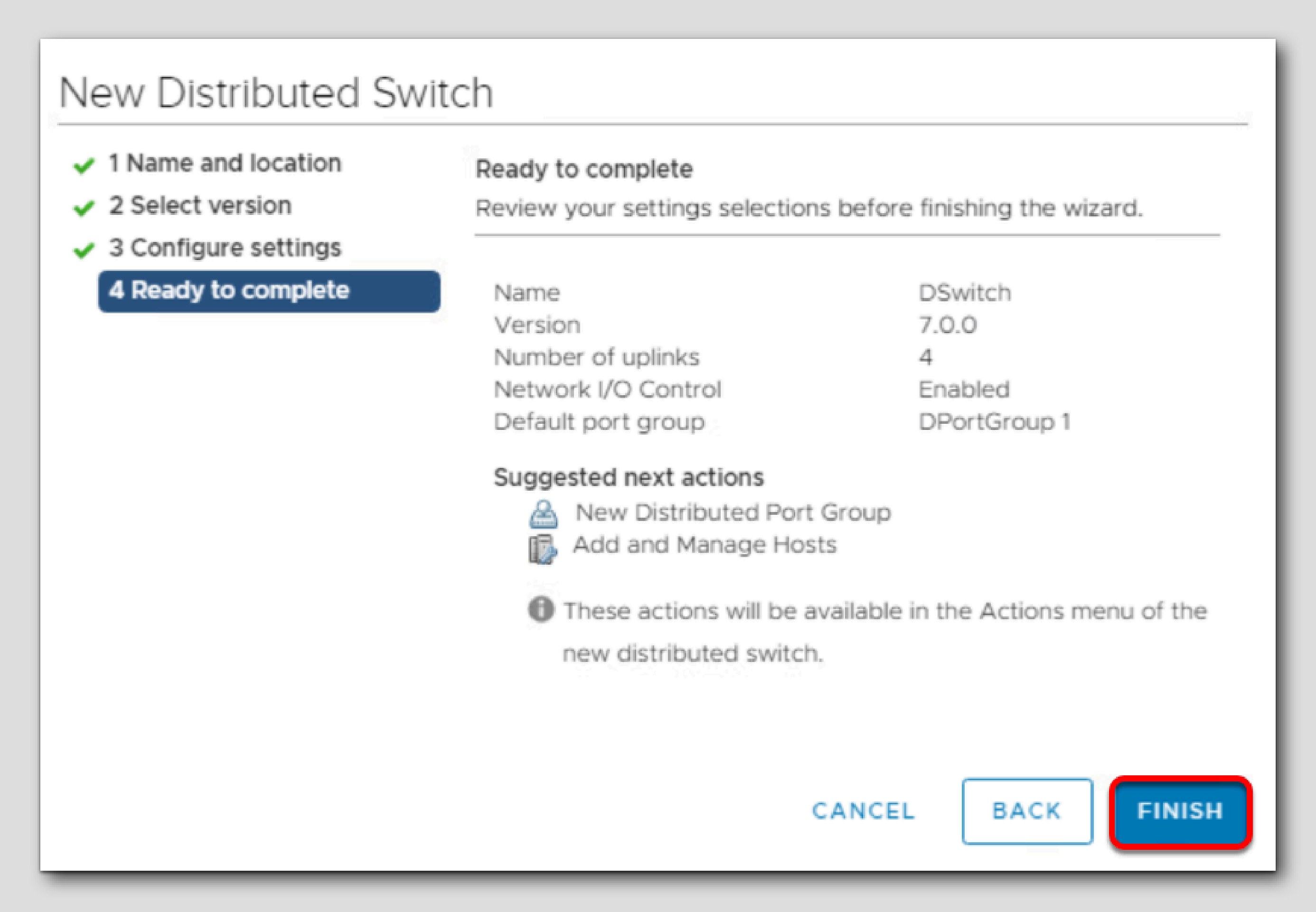
Default port group: ☑ Create a default port group

Port group name: DPortGroup 1

1. Leave the default options and click Next

Ready to complete

[323]



New Distributed Switch

Ready to complete

Review your settings selections before finishing the wizard.

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

Suggested next actions

New Distributed Port Group
Add and Manage Hosts

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

1. Review the settings and click Finish

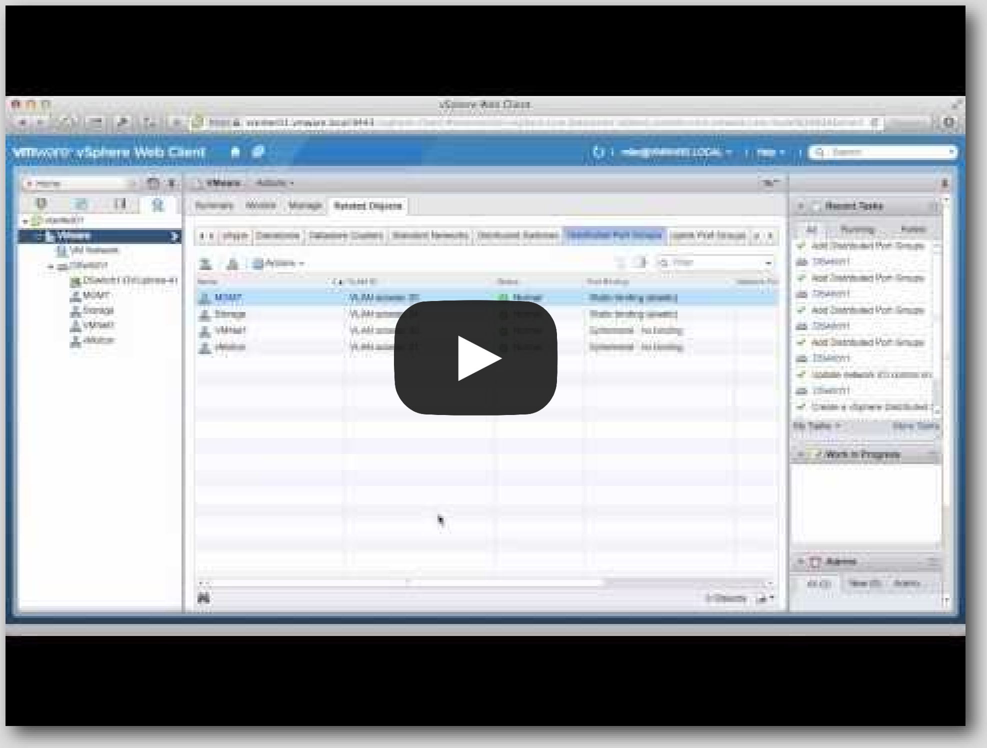
Notice the next suggested steps are to create Distributed Port Groups and adding Hosts.

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

[324]

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

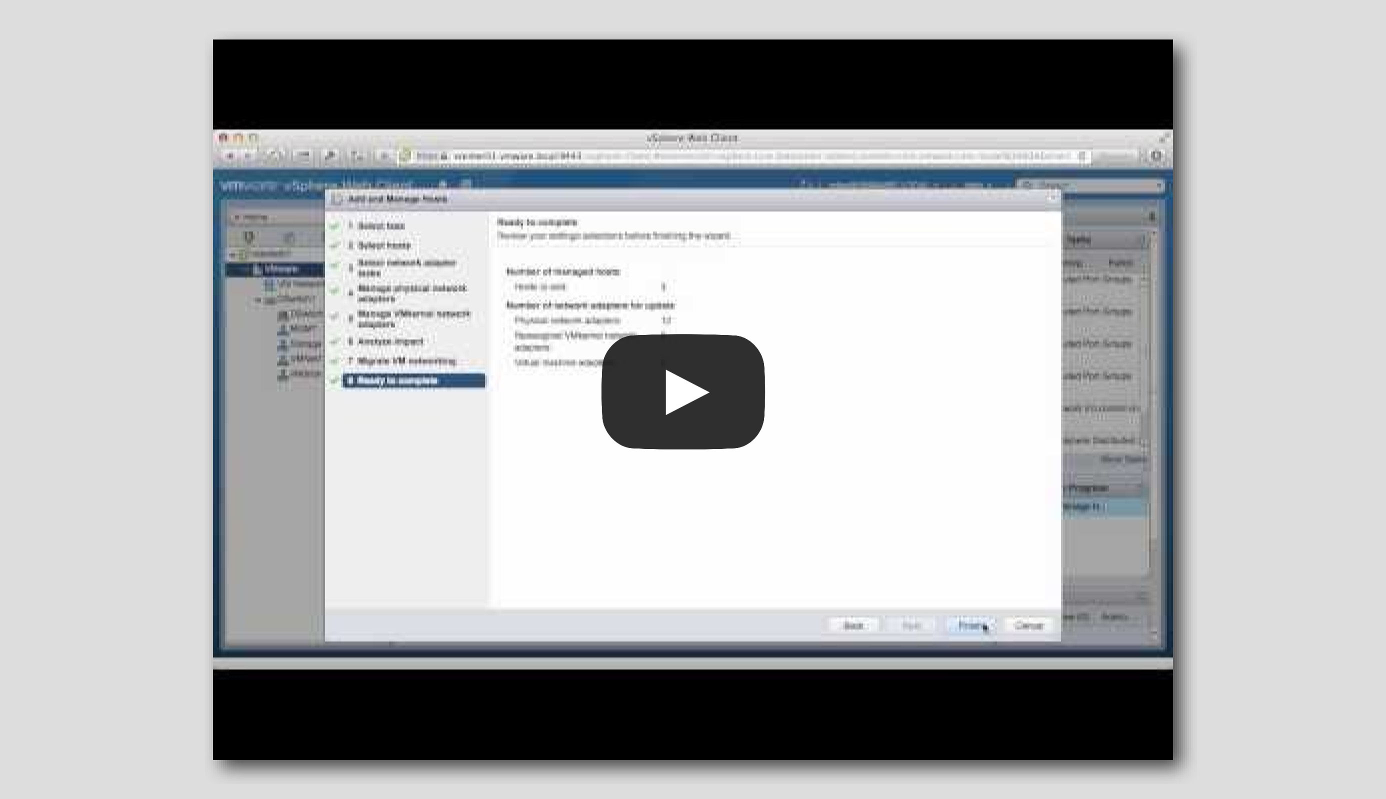
https://www.youtube.com/watch?v=NGQ5ejGfuDY



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

[325]

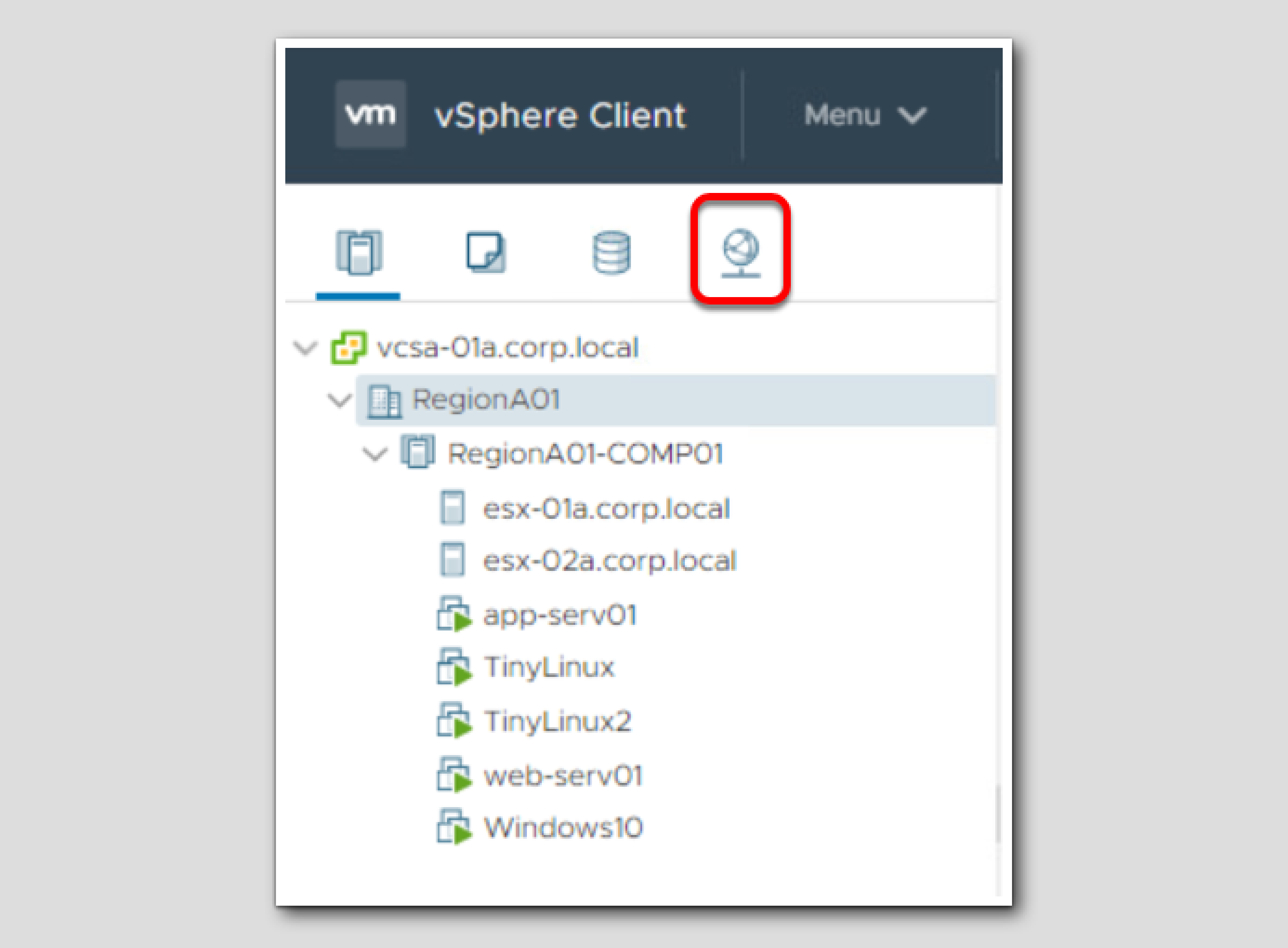
https://www.youtube.com/watch?v=hiu8DLSIoA0



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

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

[326]

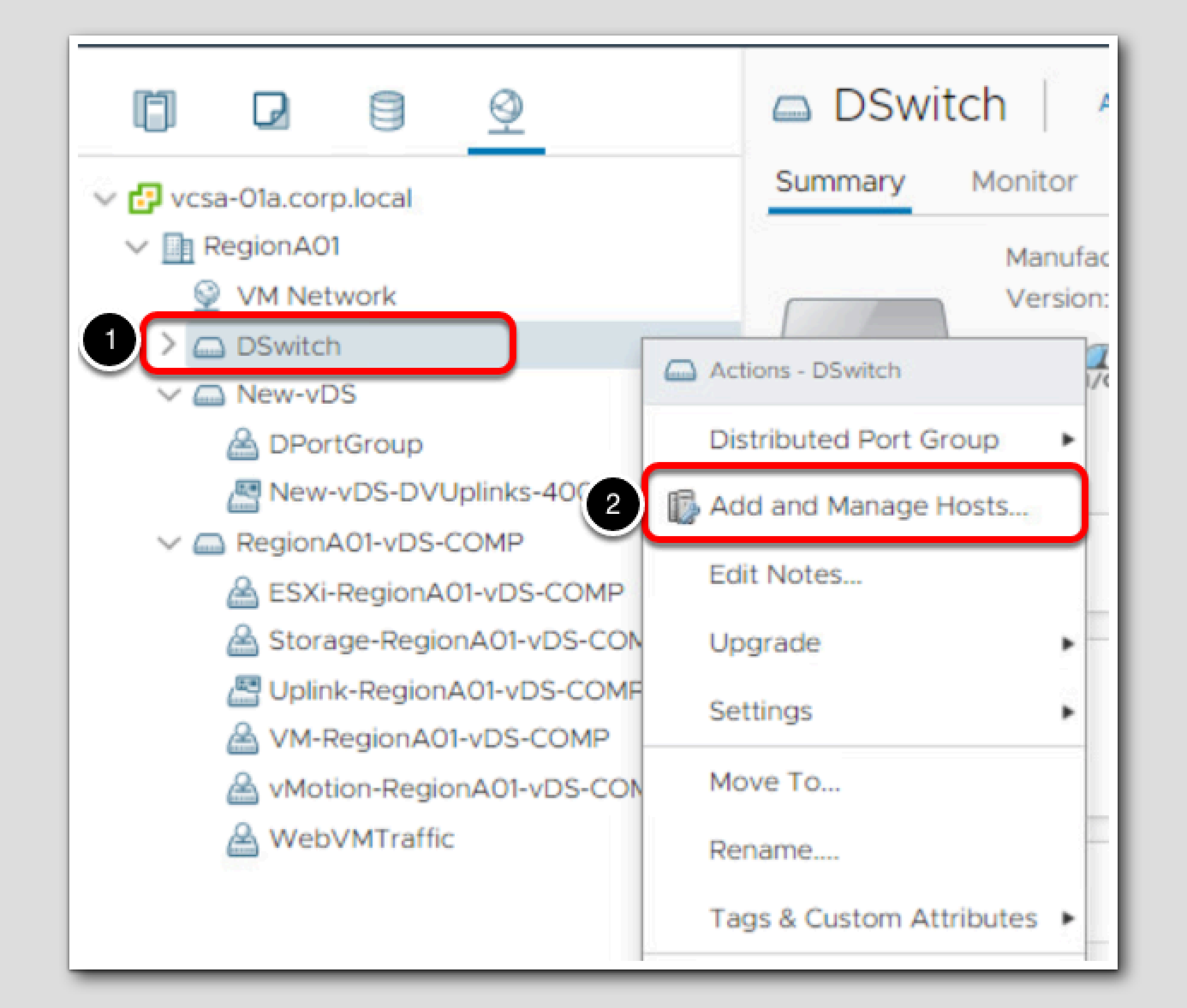


Now that we have created a vSphere distributed switch, let's add hosts and physical adapters to create a virtual network.

1. Click on the **Networking** icon

Add Hosts

[327]

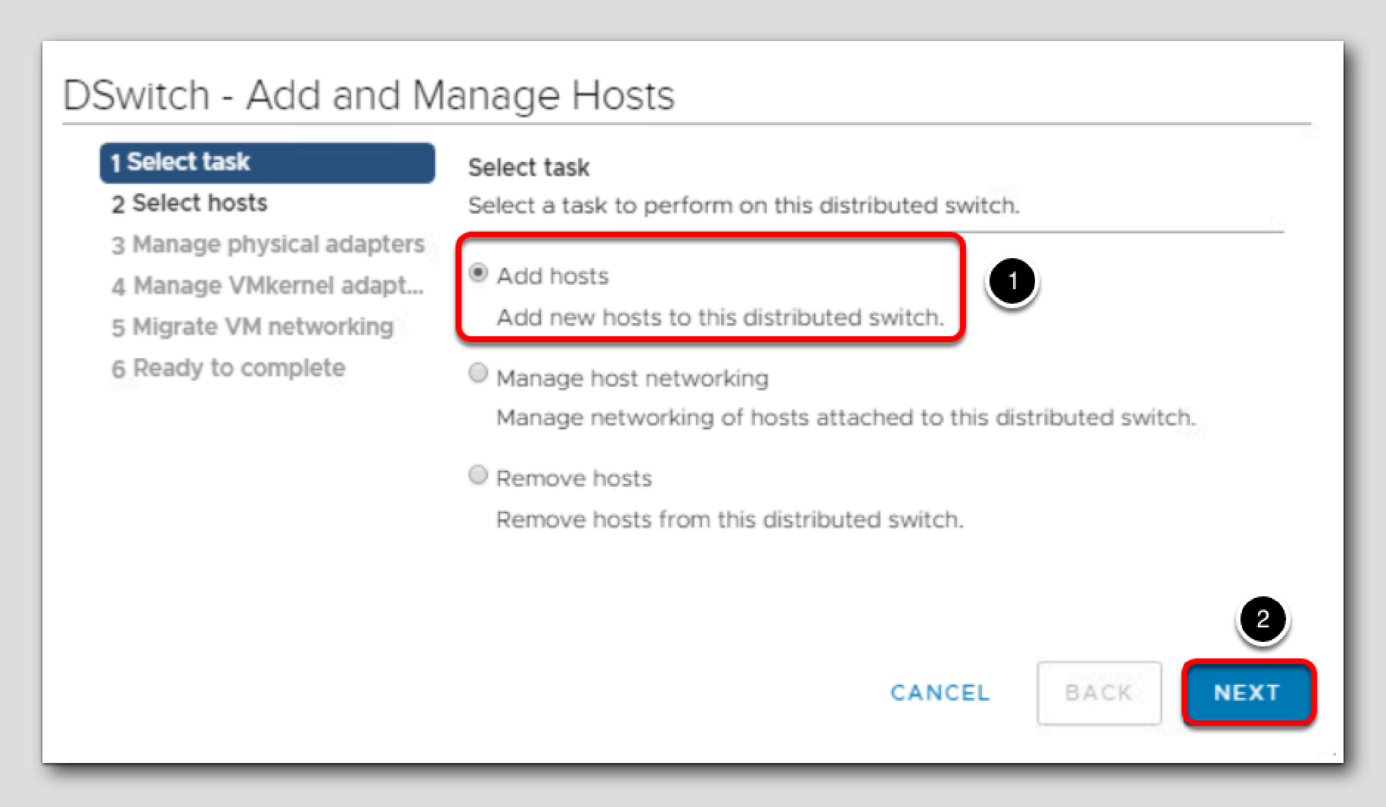


Expand **RegionA01** until you see the Distributed Switch we just created, **DSwitch**.

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

Select task

[328]



DSwitch - Add and Manage Hosts

Select task

Select a task to perform on this distributed switch.

● Add hosts

Add new hosts to this distributed switch.

○ Manage host networking

Manage networking of hosts attached to this distributed switch.

○ Remove hosts

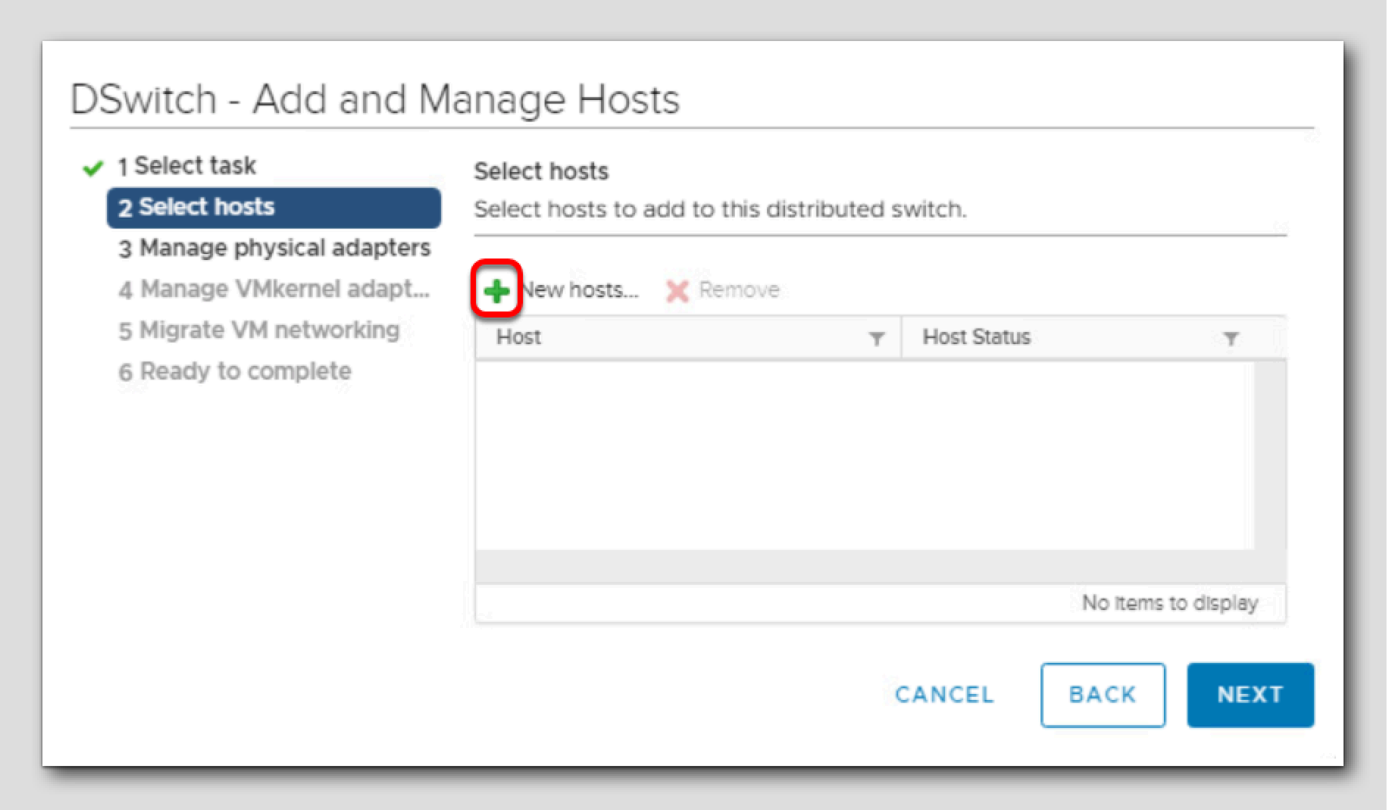
Remove hosts from this distributed switch.

1. Select Add hosts
2. Click Next

Select hosts

[329]

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



DSwitch - Add and Manage Hosts

Select hosts

Select hosts to add to this distributed switch.

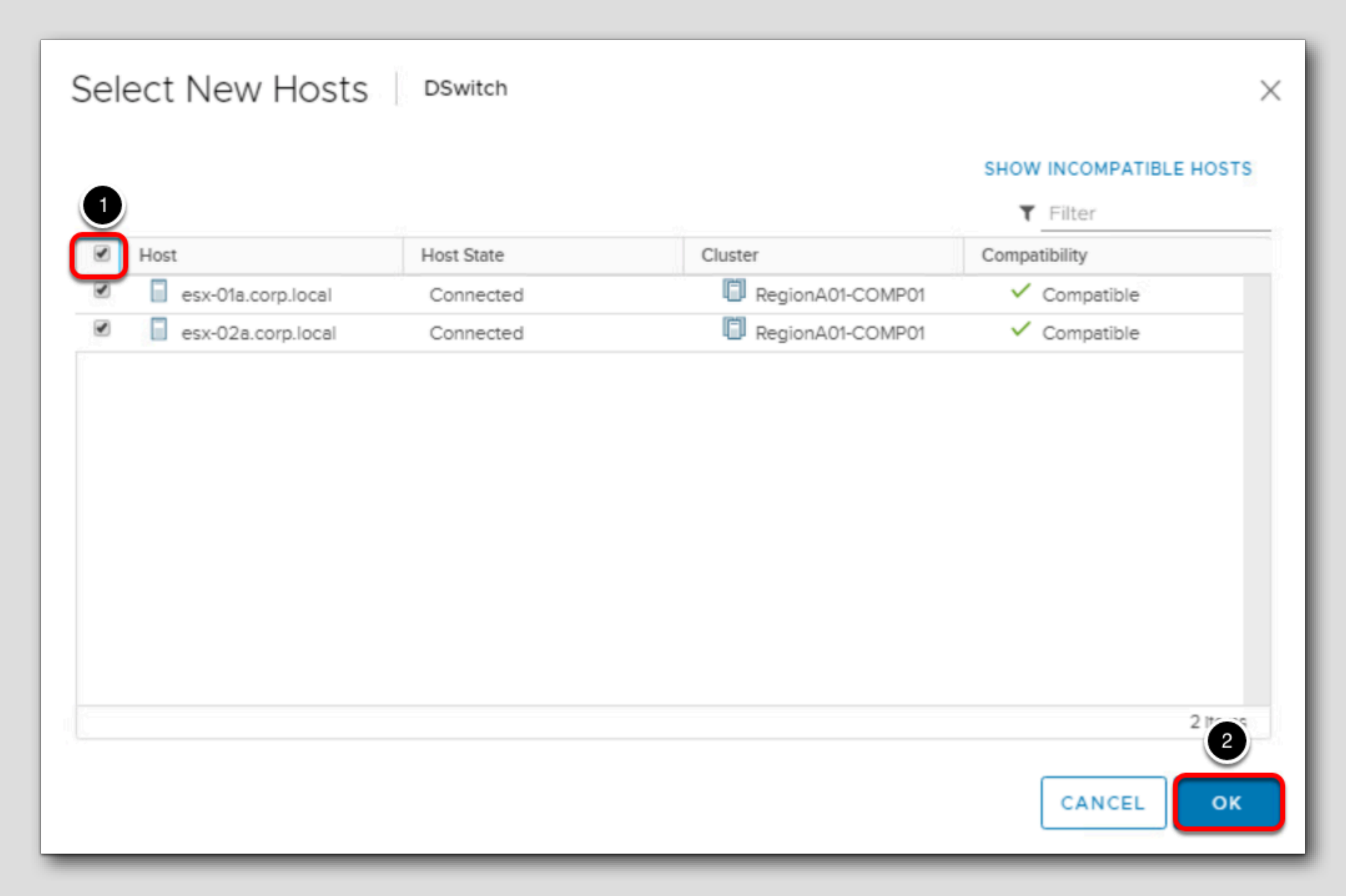
Host	Host Status

No items to display

1. Click New hosts

Select your Hosts

[330]



Select New Hosts | DSwitch

SHOW INCOMPATIBLE HOSTS

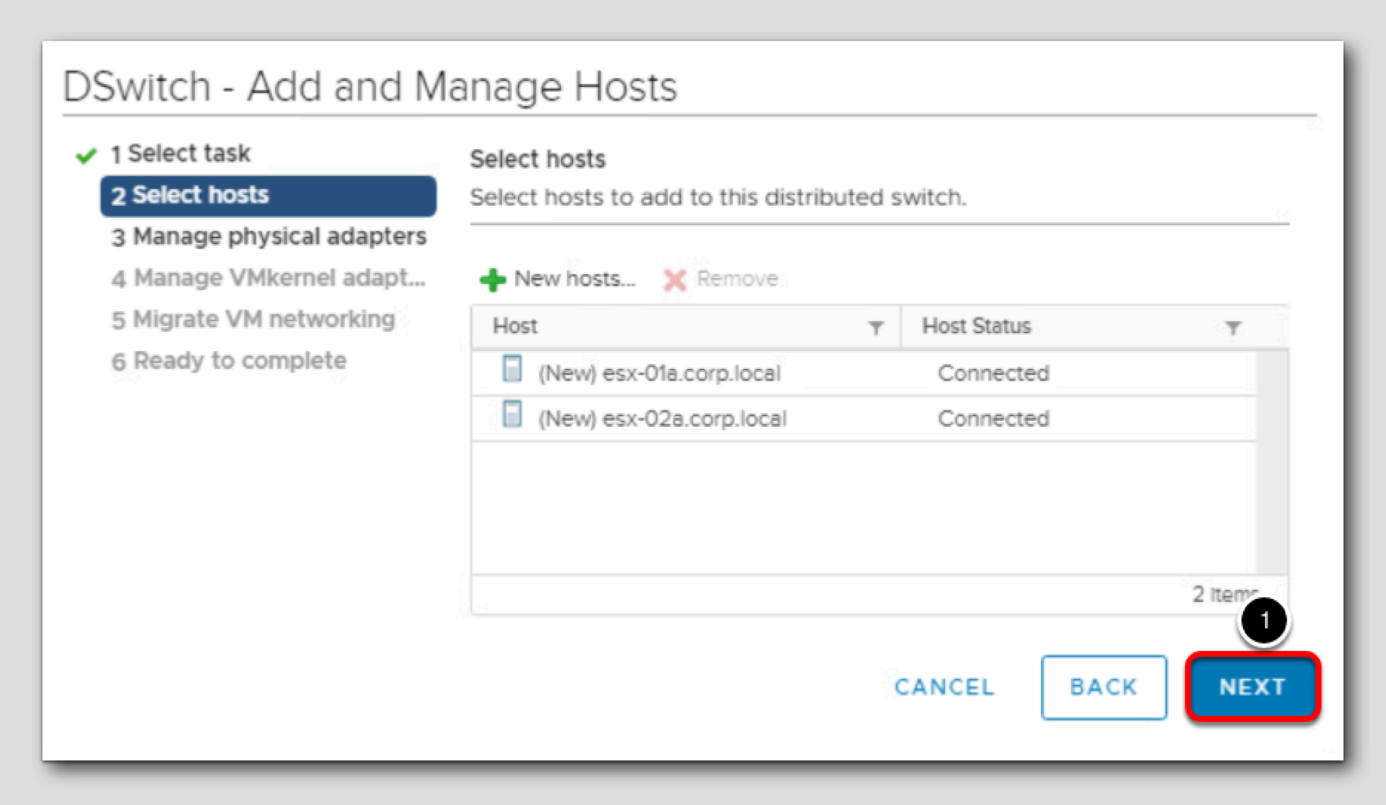
Filter

☑	Host	Host State	Cluster	Compatibility
☑	esx-01a.corp.local	Connected	RegionA01-COMP01	✓ Compatible
☑	esx-02a.corp.local	Connected	RegionA01-COMP01	✓ Compatible

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

Select hosts (cont.)

[331]



DSwitch - Add and Manage Hosts

Select hosts

Select hosts to add to this distributed switch.

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

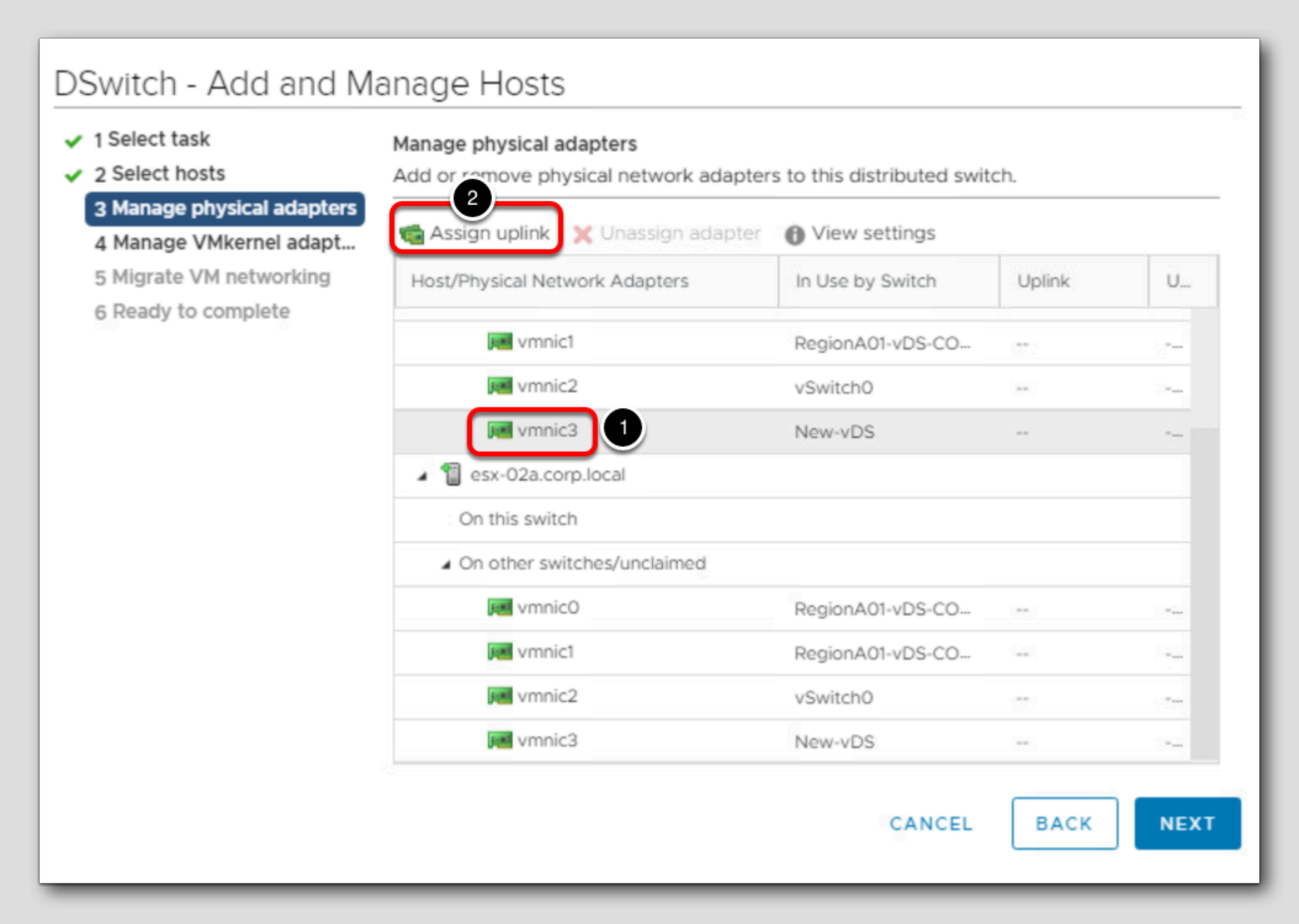
2 items

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

1. Click Next

Manage physical network adapters

[332]



DSwitch - Add and Manage Hosts

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

Manage physical adapters

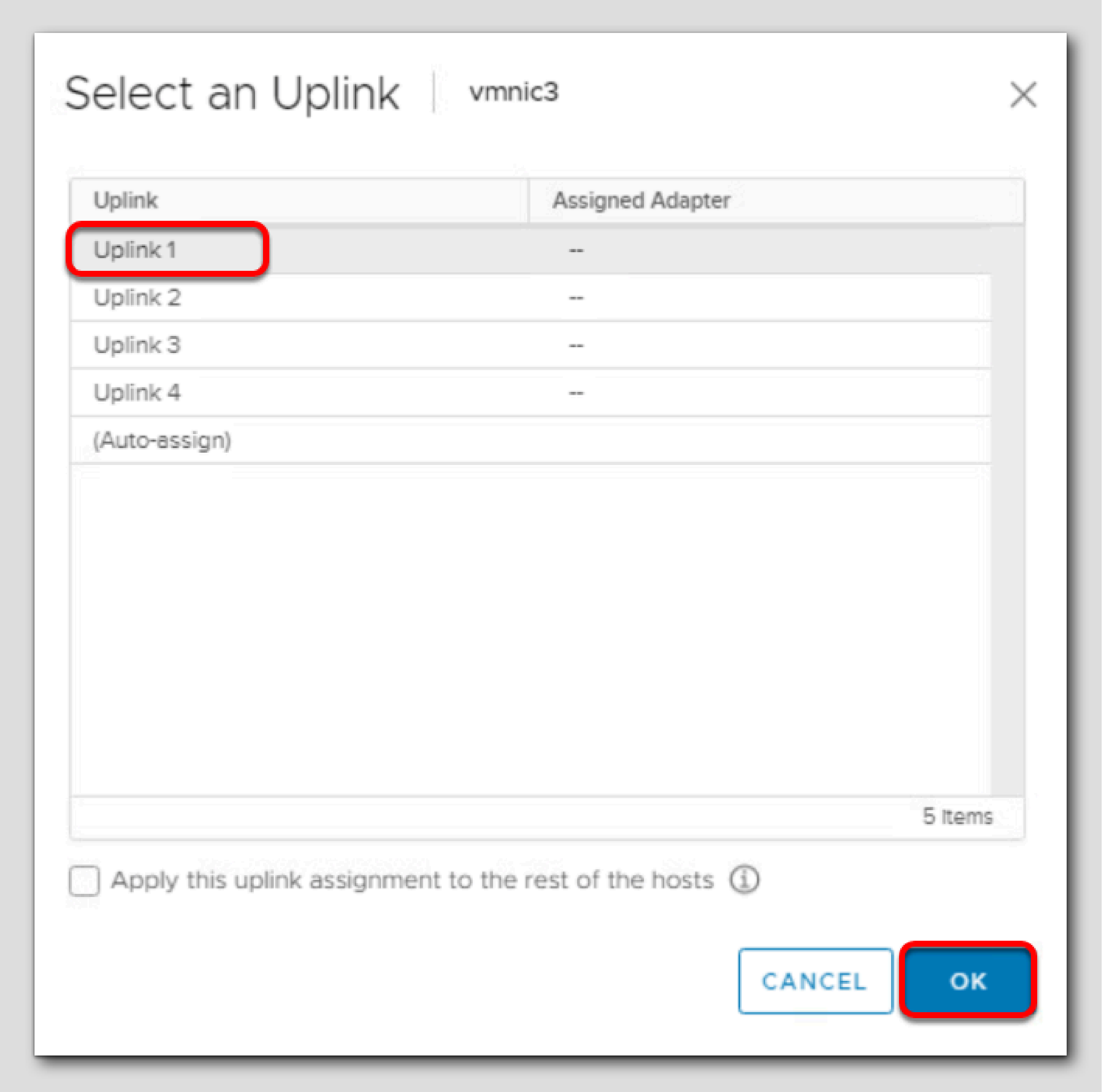
Add or remove physical network adapters to this distributed switch.

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

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

1. Select vmnic3
2. Click Assign uplink

Select an Uplink for vmnic3



Select an Uplink | vmnic3

Uplink	Assigned Adapter
Uplink 1	--
Uplink 2	--
Uplink 3	--
Uplink 4	--
(Auto-assign)	

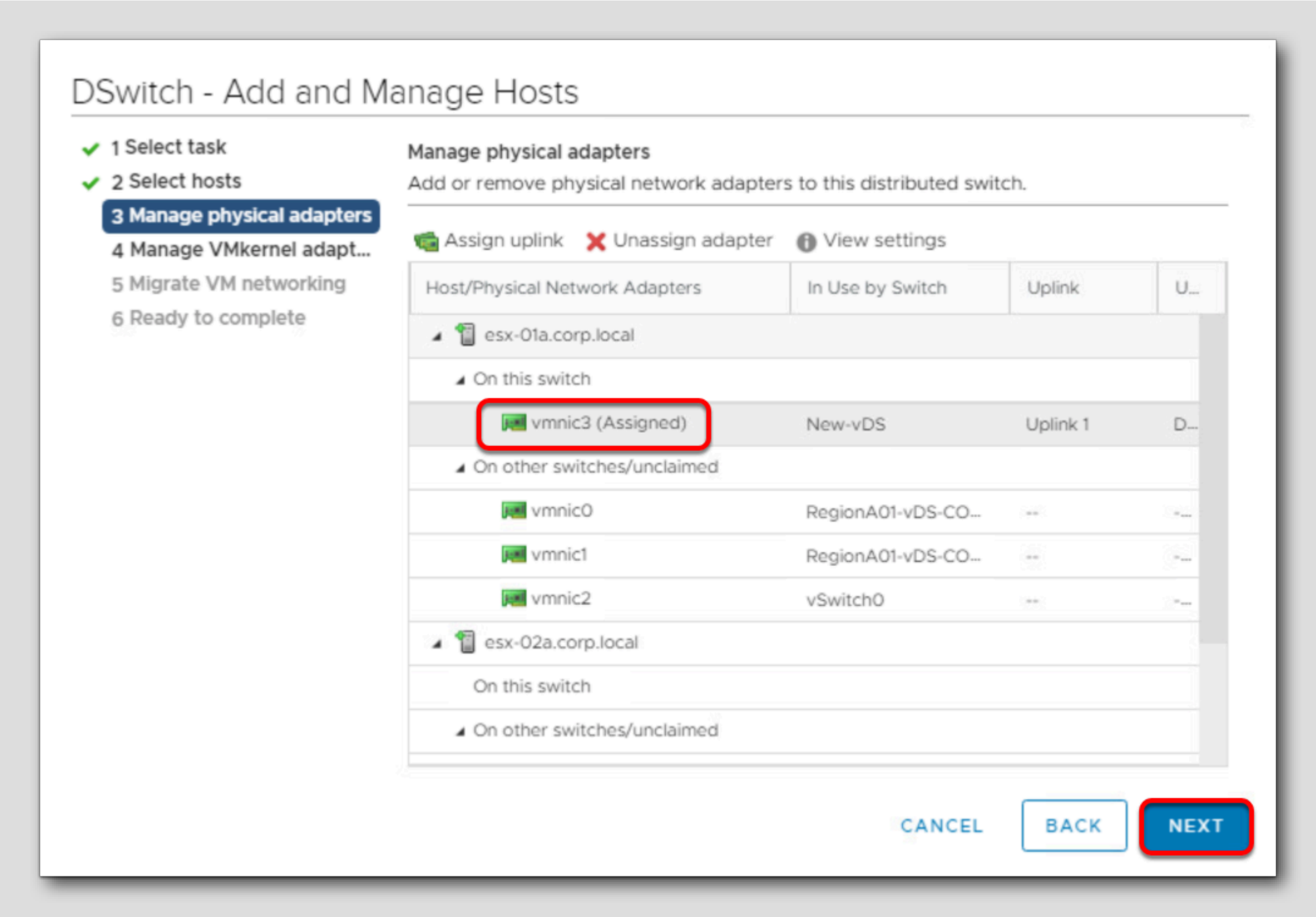
5 Items

□ Apply this uplink assignment to the rest of the hosts

1. Select Uplink 1
2. Click OK

Confirm Addition

[334]



DSwitch - Add and Manage Hosts

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

Manage physical adapters

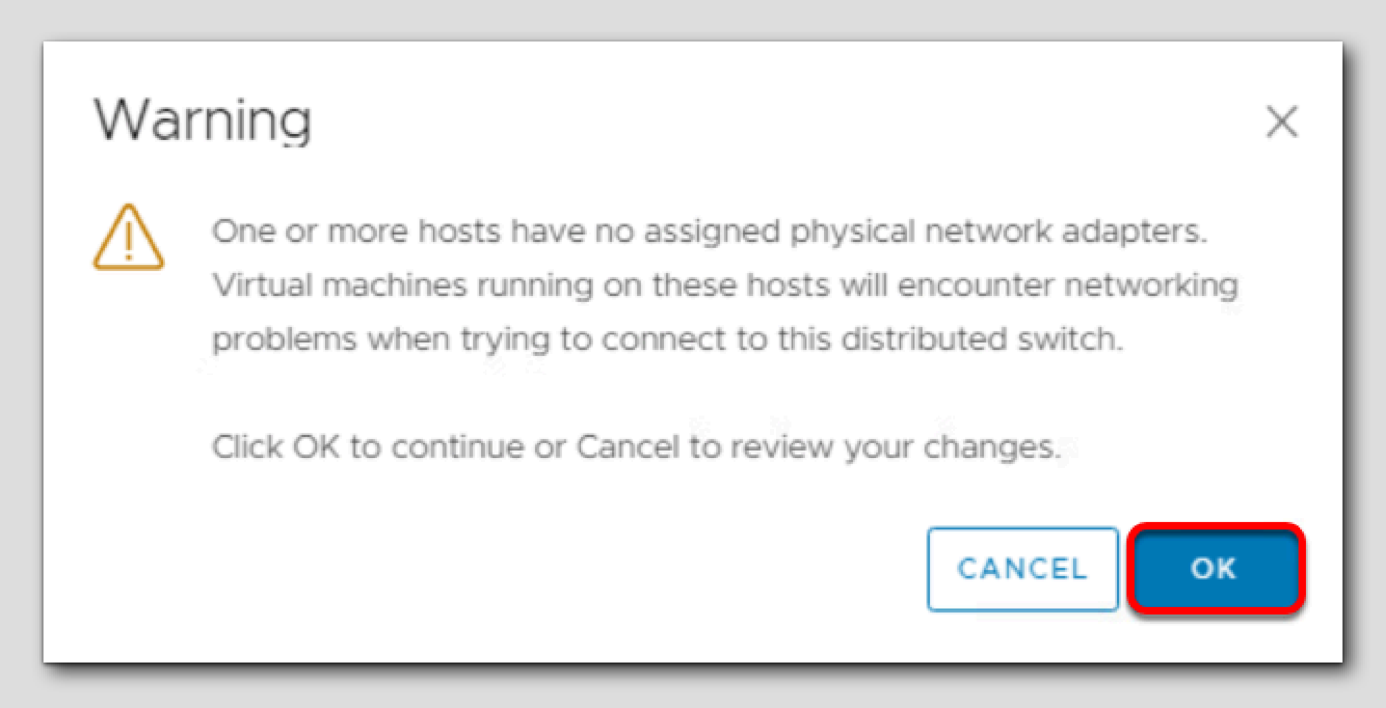
Add or remove physical network adapters to this distributed switch.

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

1. vmnic3 is assigned and click Next to continue

Warning message

[335]



Warning

One or more hosts have no assigned physical network adapters. Virtual machines running on these hosts will encounter networking problems when trying to connect to this distributed switch.

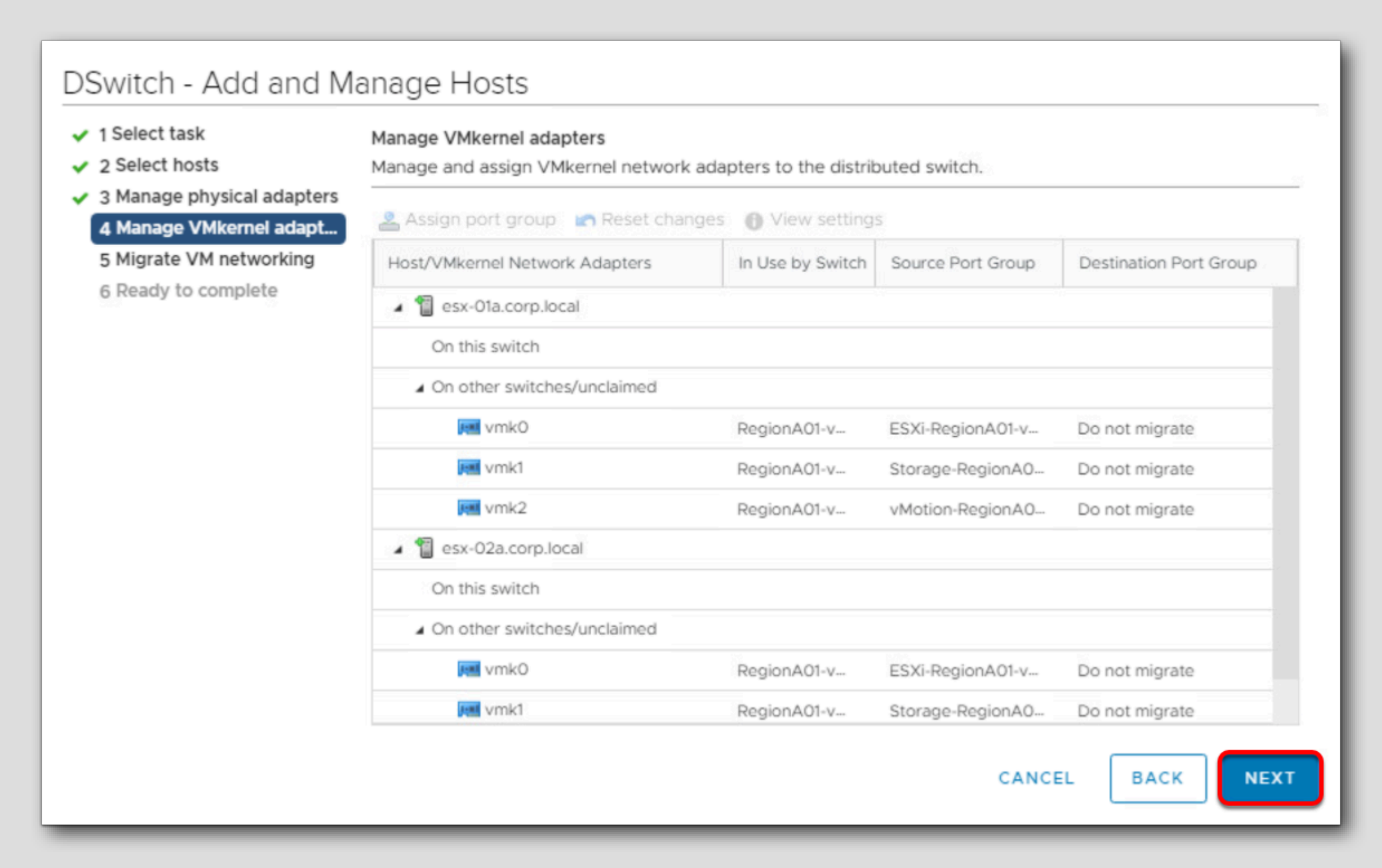
Click OK to continue or Cancel to review your changes.

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

1. Click OK to continue

Manage virtual network adapters

[336]



DSwitch - Add and Manage Hosts

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

Manage VMkernel adapters

Manage and assign VMkernel network adapters to the distributed switch.

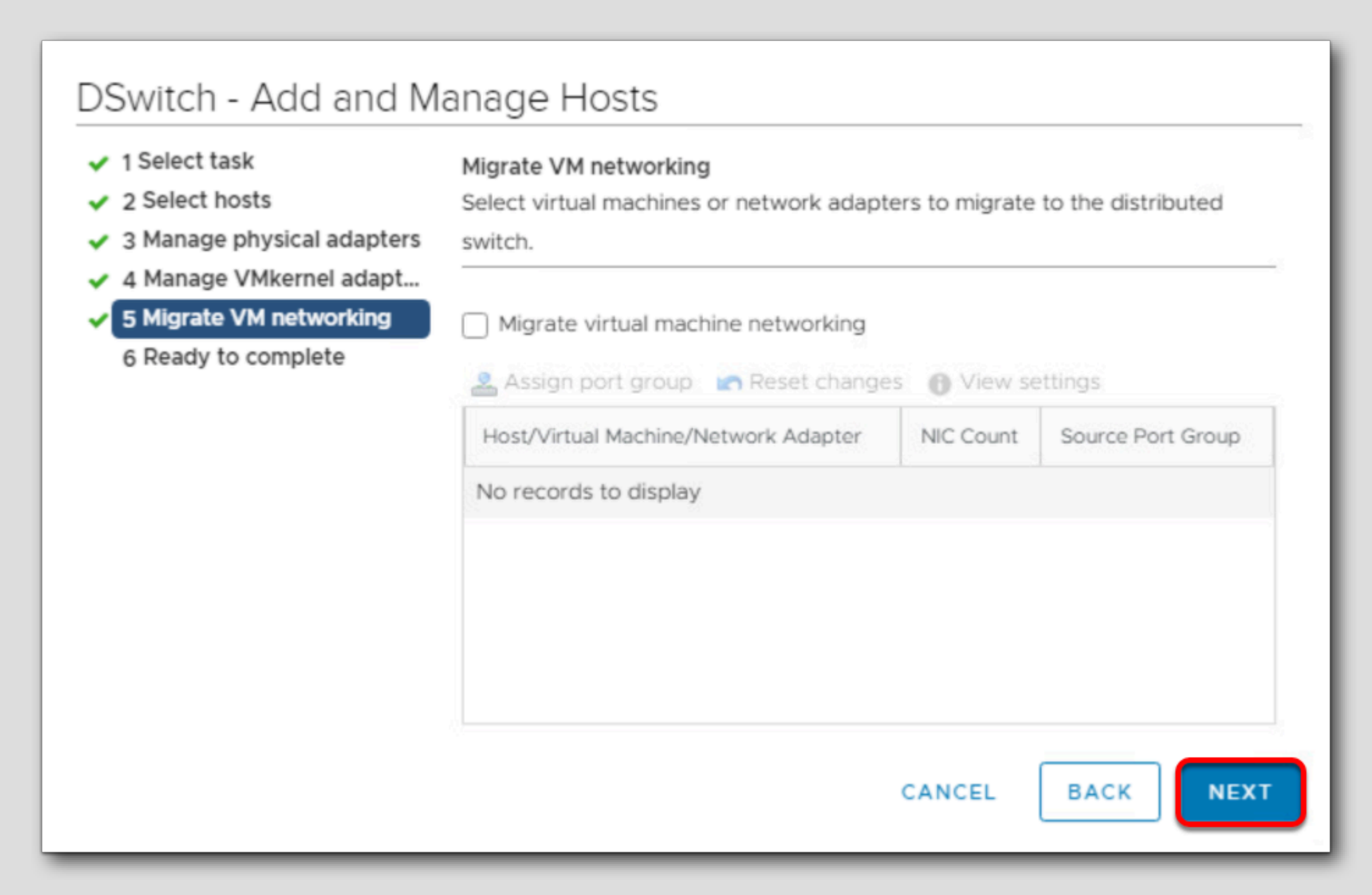
Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
esx-01a.corp.local			
On this switch			
On other switches/unclaimed			
vmk0	RegionA01-v...	ESXi-RegionA01-v...	Do not migrate
vmk1	RegionA01-v...	Storage-RegionA0...	Do not migrate
vmk2	RegionA01-v...	vMotion-RegionA0...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

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

1. Click Next to continue

Migrate VM Networking

[337]



DSwitch - Add and Manage Hosts

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

Migrate VM networking

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

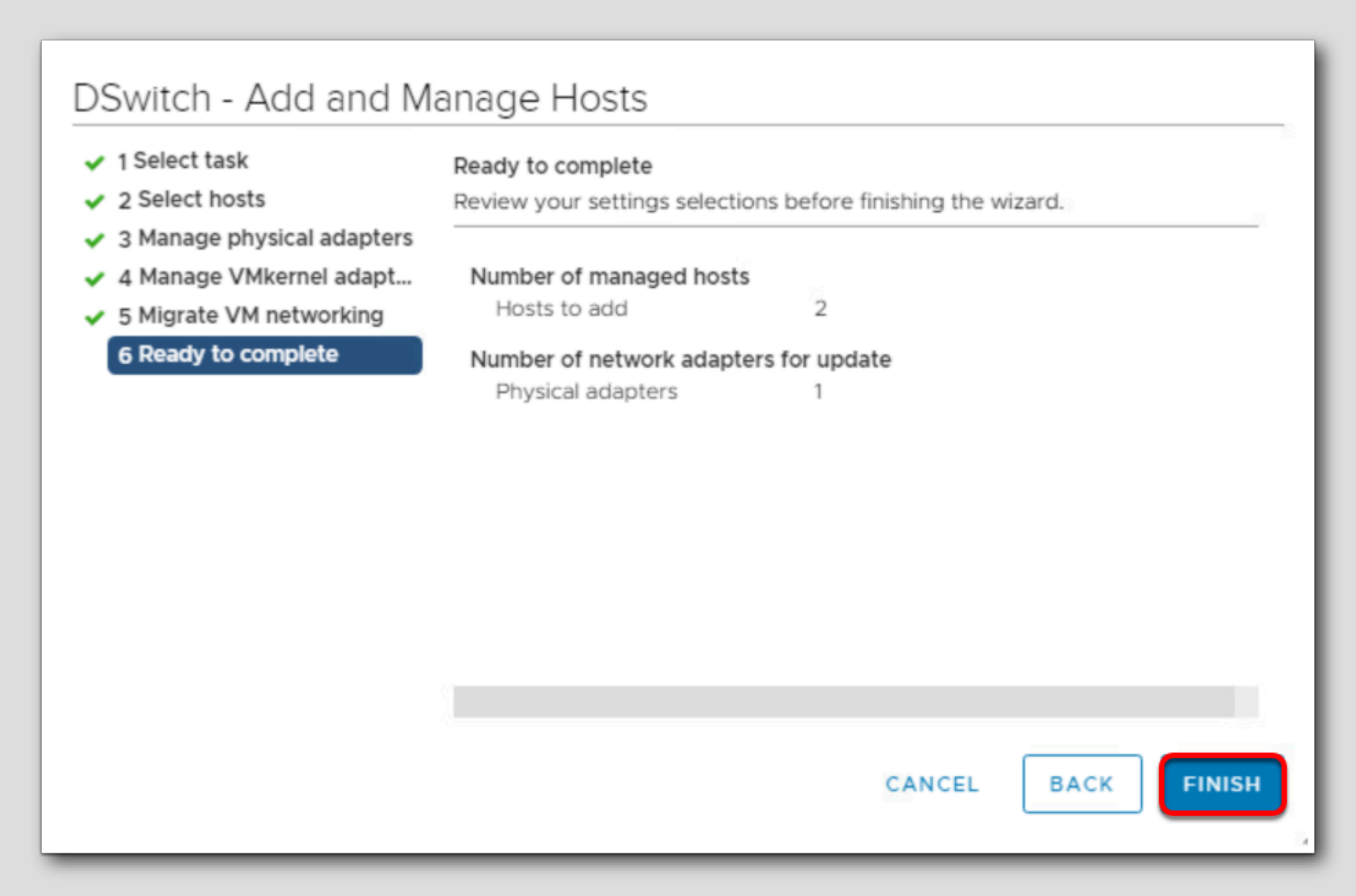
☐ Migrate virtual machine networking

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

1. Click **Next** to continue

Ready to complete

[338]



DSwitch - Add and Manage Hosts

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

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

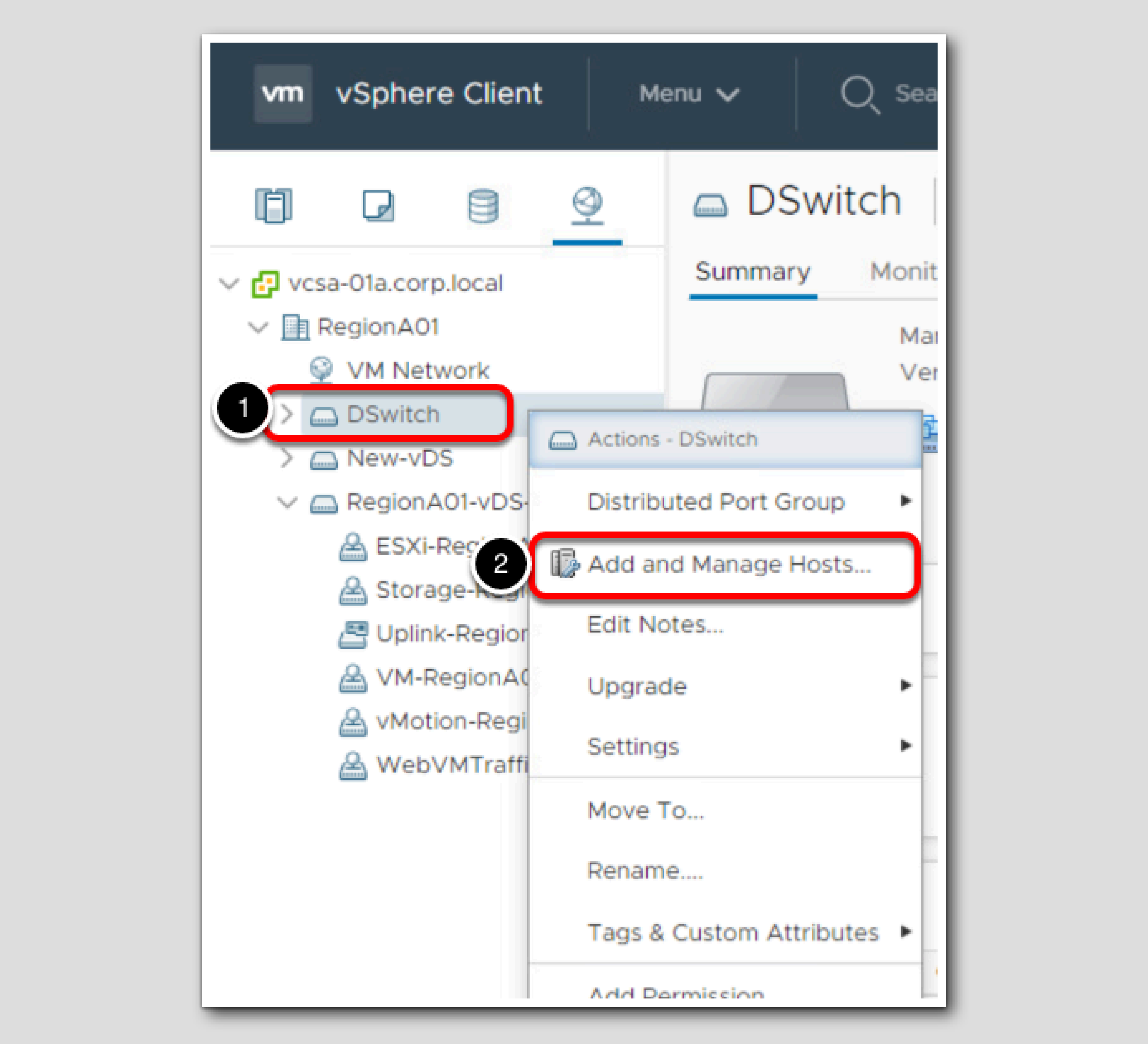
Physical adapters	1

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

1. Click Finish to commit the changes

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

[339]

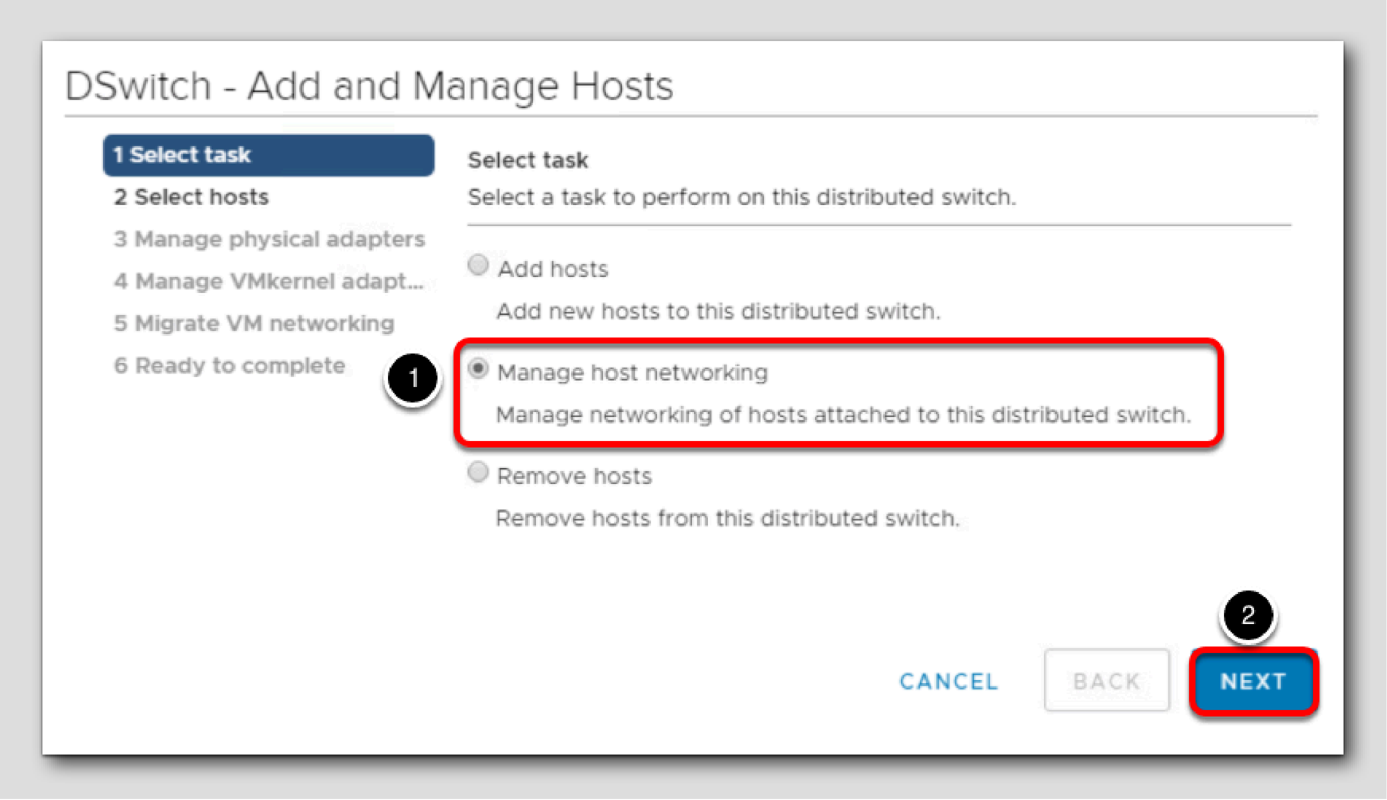


You can change the configuration for hosts and physical adapters on a vSphere Distributed Switch after they are added to the distributed switch.

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

Select Task

[340]



DSwitch - Add and Manage Hosts

Select task

Select a task to perform on this distributed switch.

○ Add hosts

Add new hosts to this distributed switch.

● Manage host networking

Manage networking of hosts attached to this distributed switch.

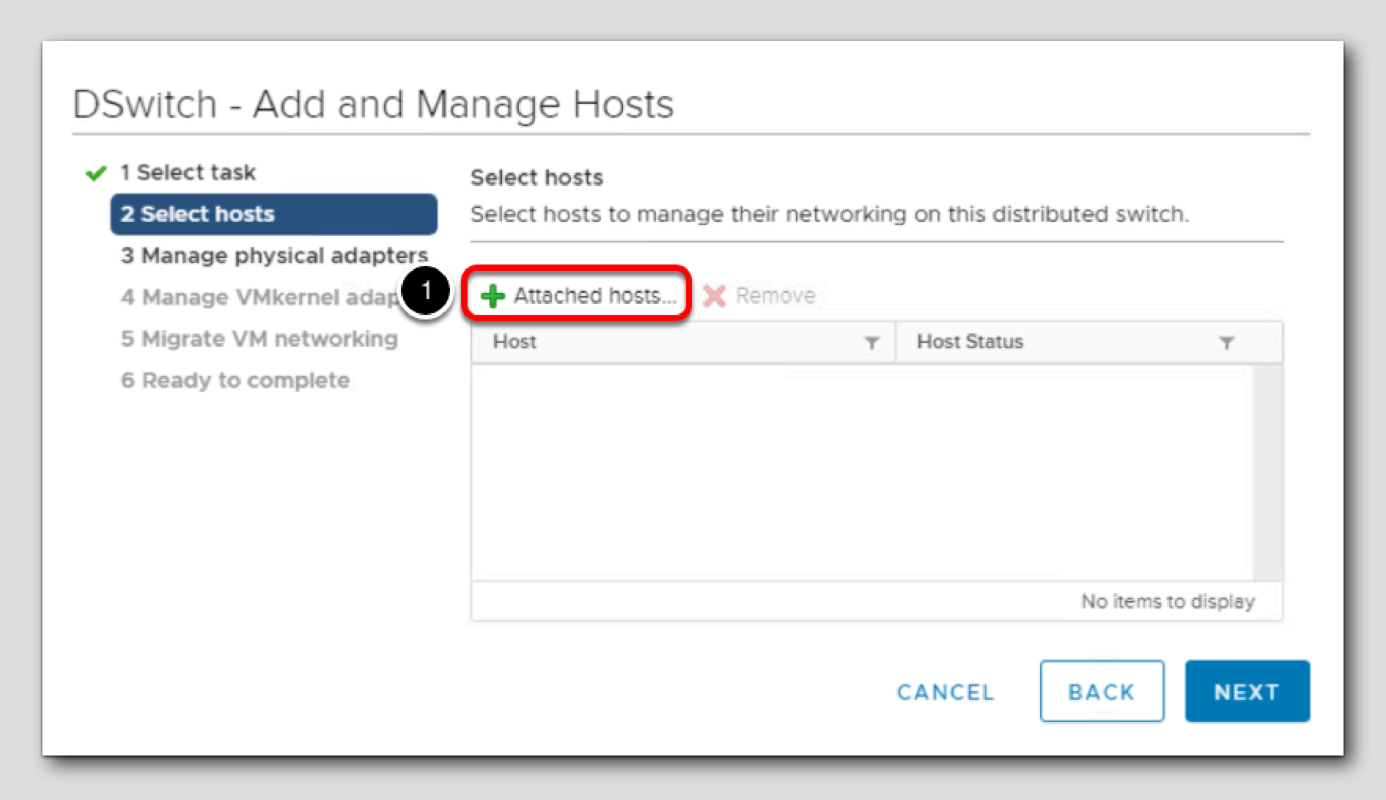
○ Remove hosts

Remove hosts from this distributed switch.

1. On the 'Select tasks' page, select Manage host networking
2. Click Next

Select hosts

[341]



DSwitch - Add and Manage Hosts

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

Select hosts

Select hosts to manage their networking on this distributed switch.

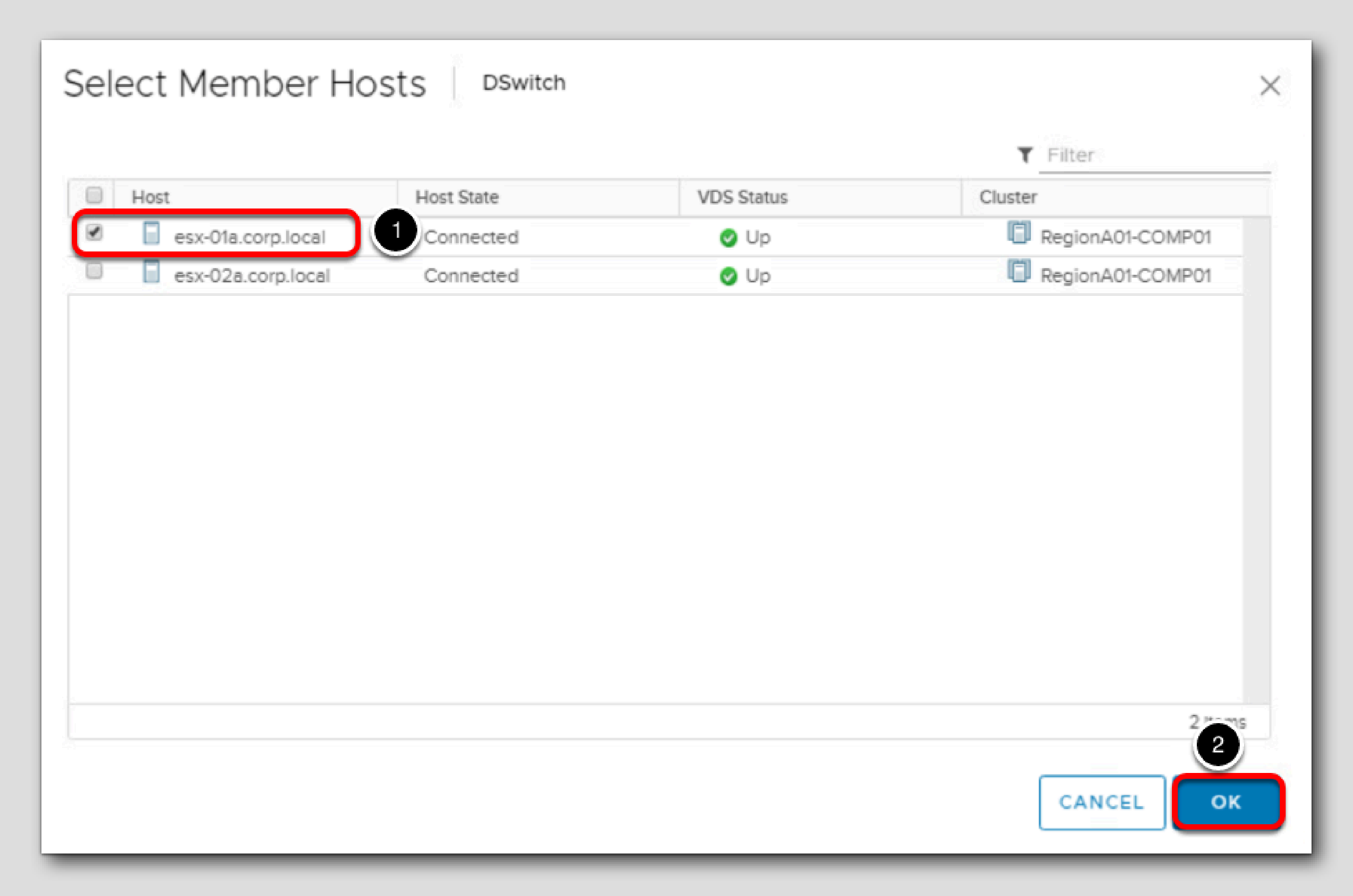
Host	Host Status

No items to display

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

Select member hosts

[342]



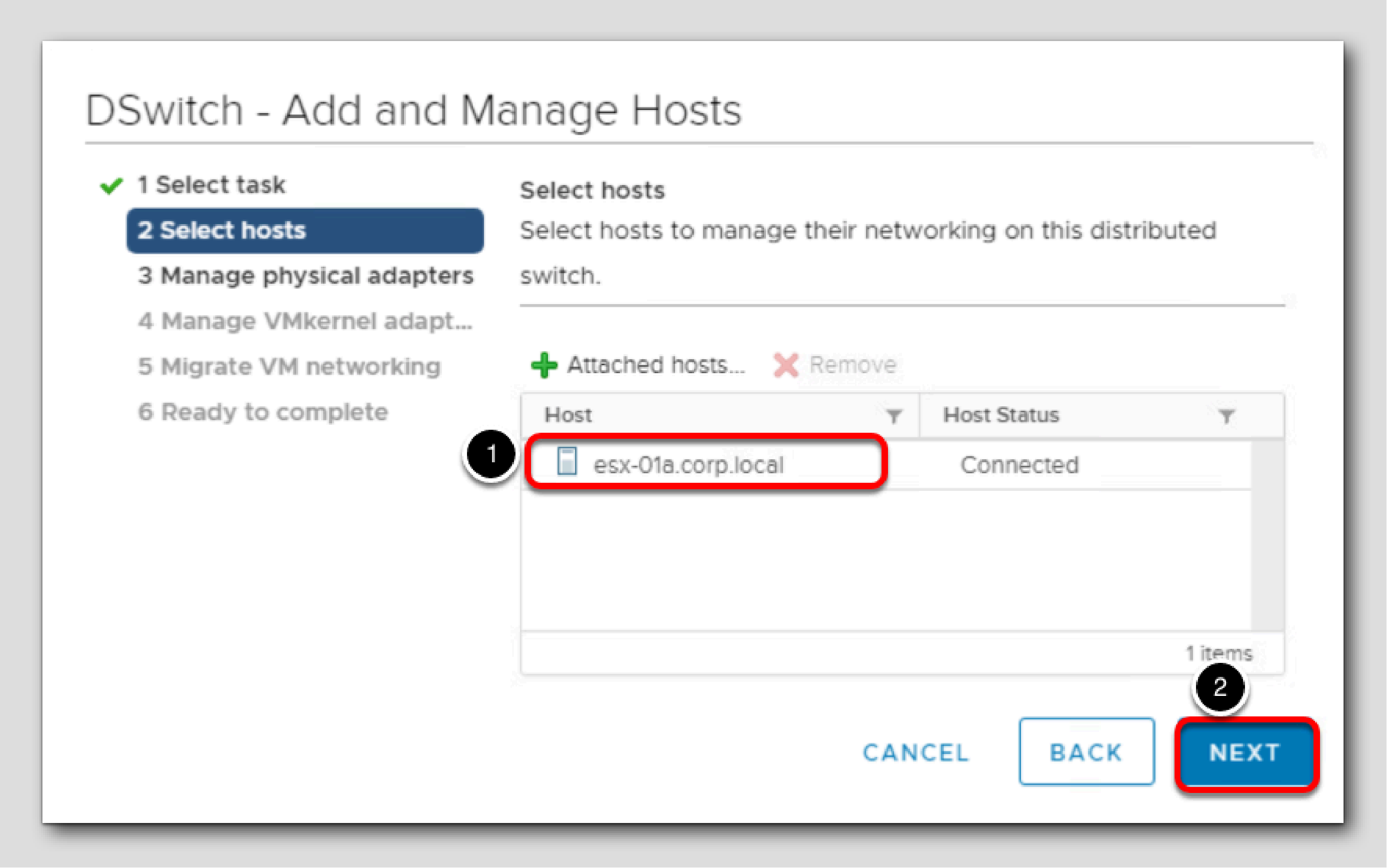
Select Member Hosts | DSwitch

☐	Host	Host State	VDS Status	Cluster
☑	esx-01a.corp.local	Connected	✓ Up	RegionA01-COMP01
☐	esx-02a.corp.local	Connected	✓ Up	RegionA01-COMP01

2 items

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

Select hosts (cont.)



DSwitch - Add and Manage Hosts

Select hosts

Select hosts to manage their networking on this distributed switch.

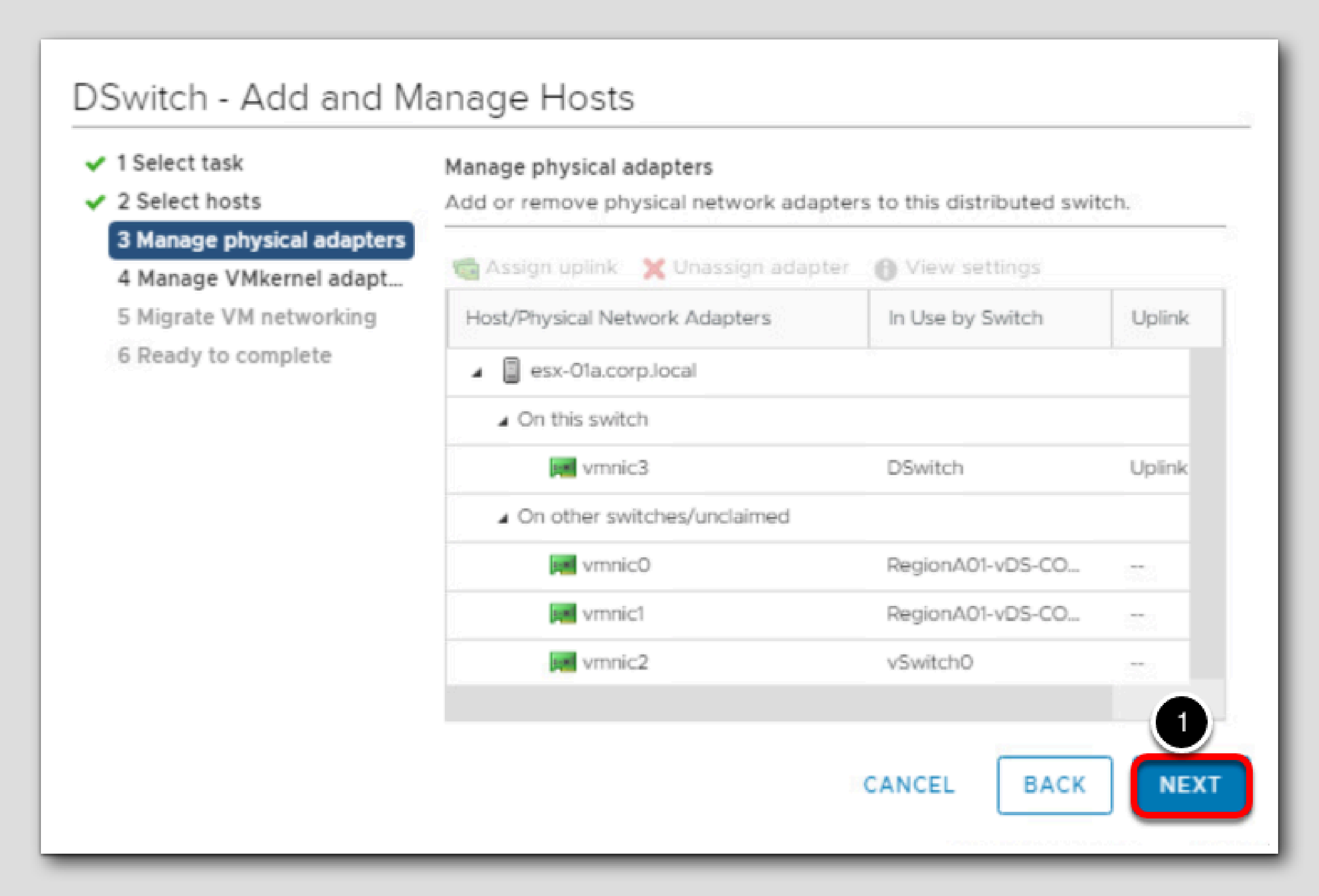
Host	Host Status
esx-01a.corp.local	Connected

1 items

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

Manage physical network adapters

[344]



DSwitch - Add and Manage Hosts

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

Manage physical adapters

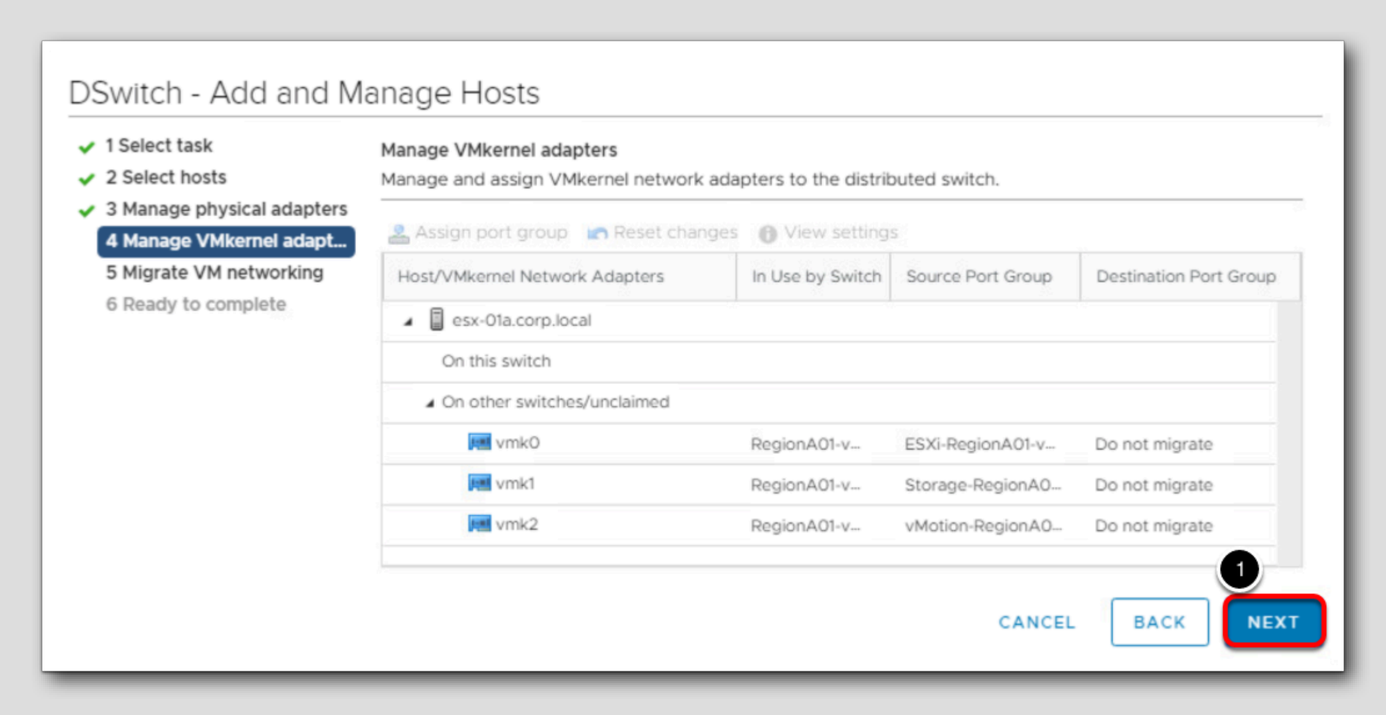
Add or remove physical network adapters to this distributed switch.

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

1. Click Next to continue

Manage VMKernal Adapters

[345]



DSwitch - Add and Manage Hosts

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

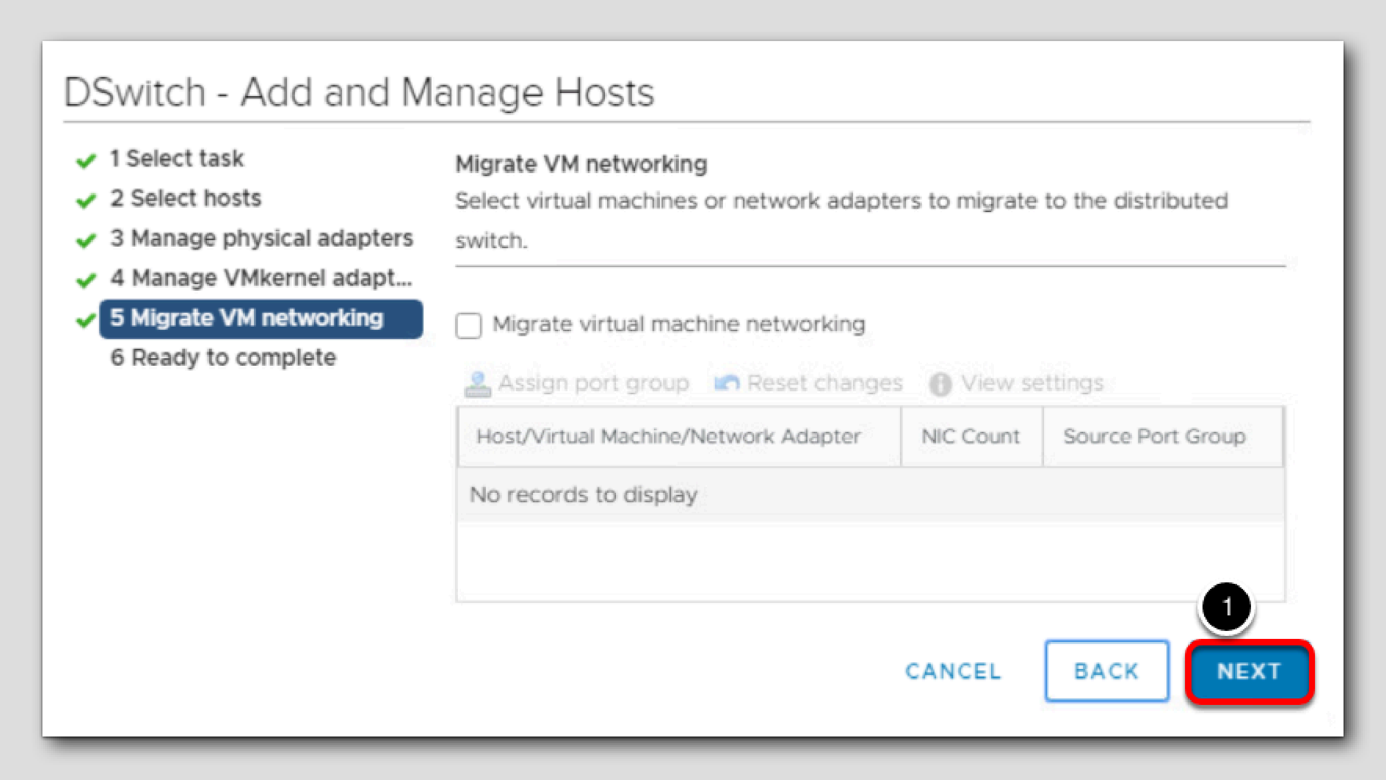
Manage VMkernel adapters

Manage and assign VMkernel network adapters to the distributed switch.

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

Migrate VM Networking

[346]



DSwitch - Add and Manage Hosts

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

Migrate VM networking

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

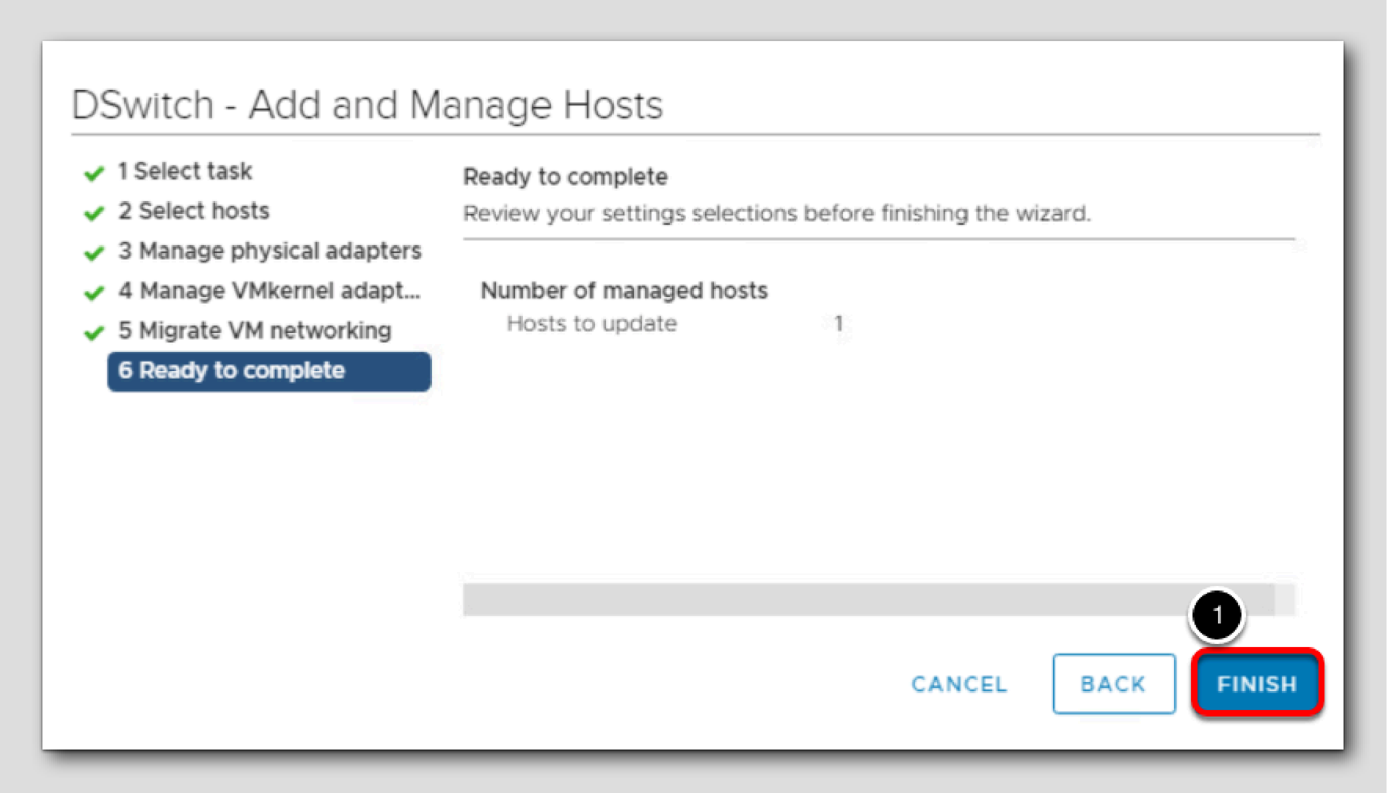
□ Migrate virtual machine networking

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

1. Click Next to continue

Ready to complete

[347]



DSwitch - Add and Manage Hosts

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

Ready to complete

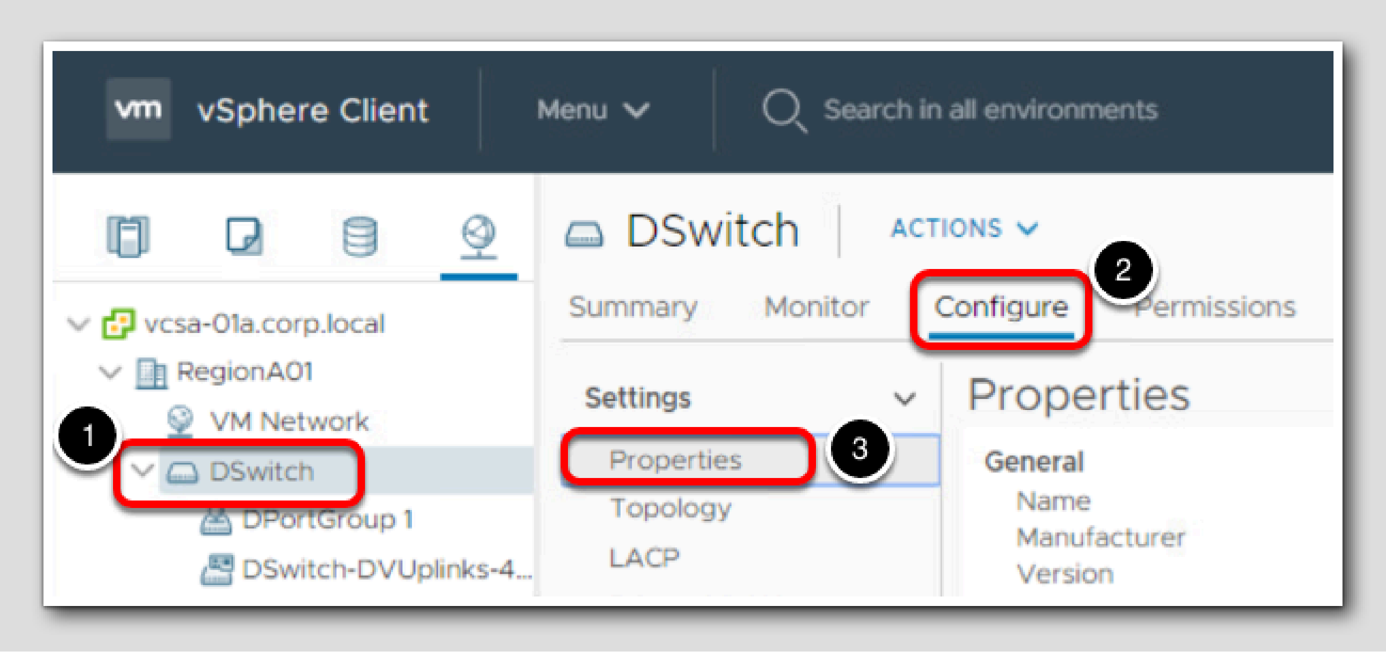
Review your settings selections before finishing the wizard.

Number of managed hosts

Hosts to update 1

1. Click **Finish**

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

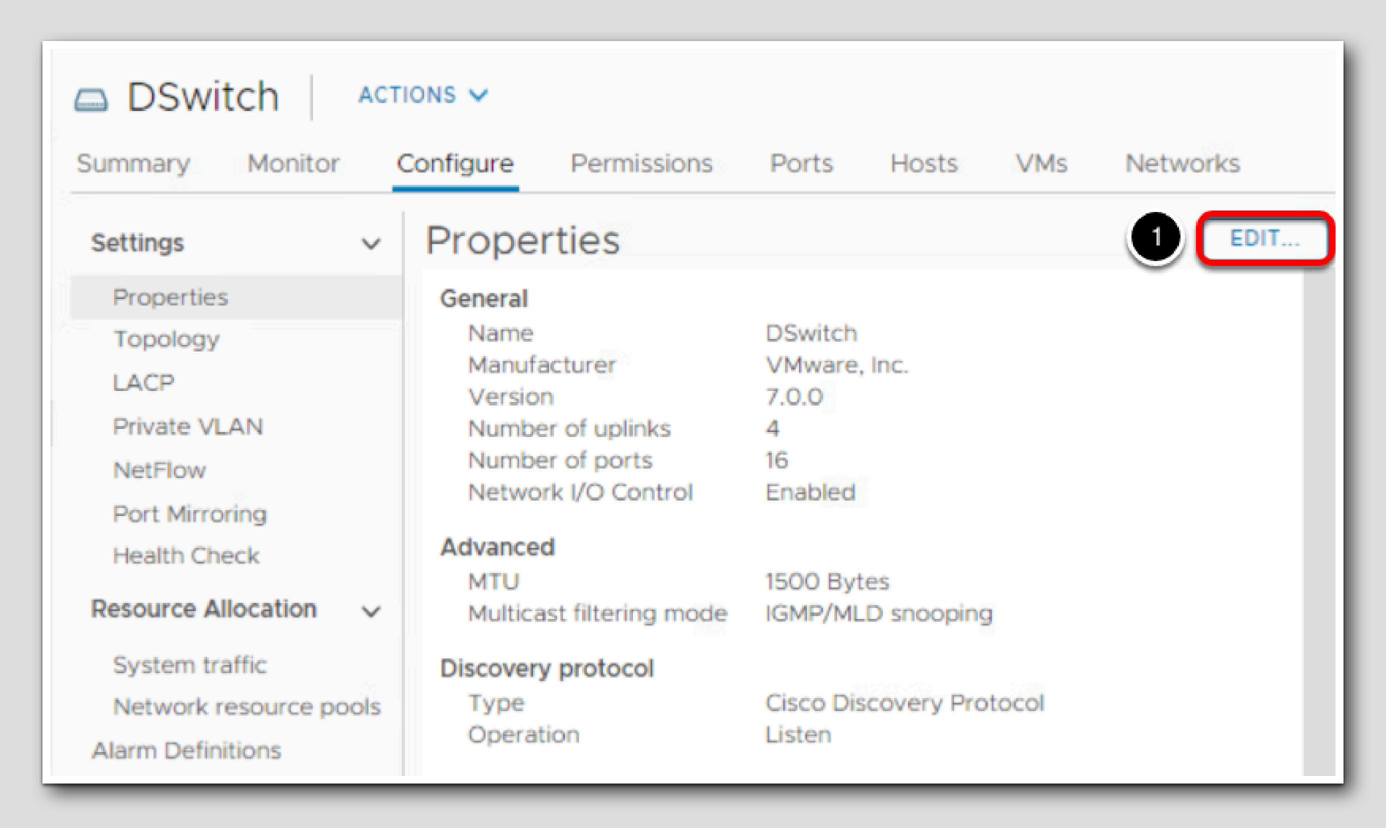


General settings for a vSphere Distributed Switch include the distributed switch name and the number of uplink ports on the distributed switch. Advanced settings for a vSphere Distributed Switch include the Discovery Protocol configuration and the maximum MTU for the switch. Both general and advanced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

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

Edit the switch properties

[349]



Properties

General

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

Advanced

MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

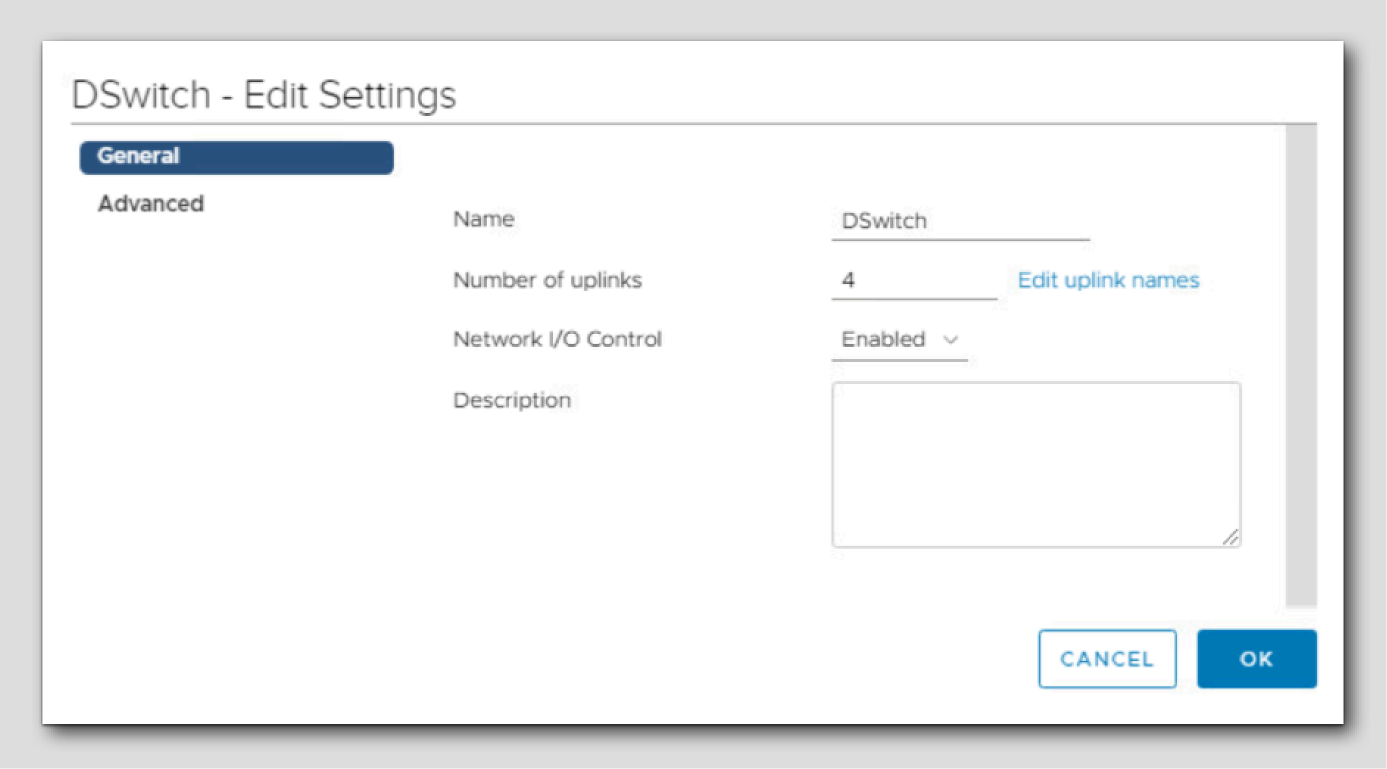
Discovery protocol

Type	Cisco Discovery Protocol
Operation	Listen

1. Click Edit

General Settings

[350]



DSwitch - Edit Settings

Name: DSwitch

Number of uplinks: 4

Network I/O Control: Enabled

Description:

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.

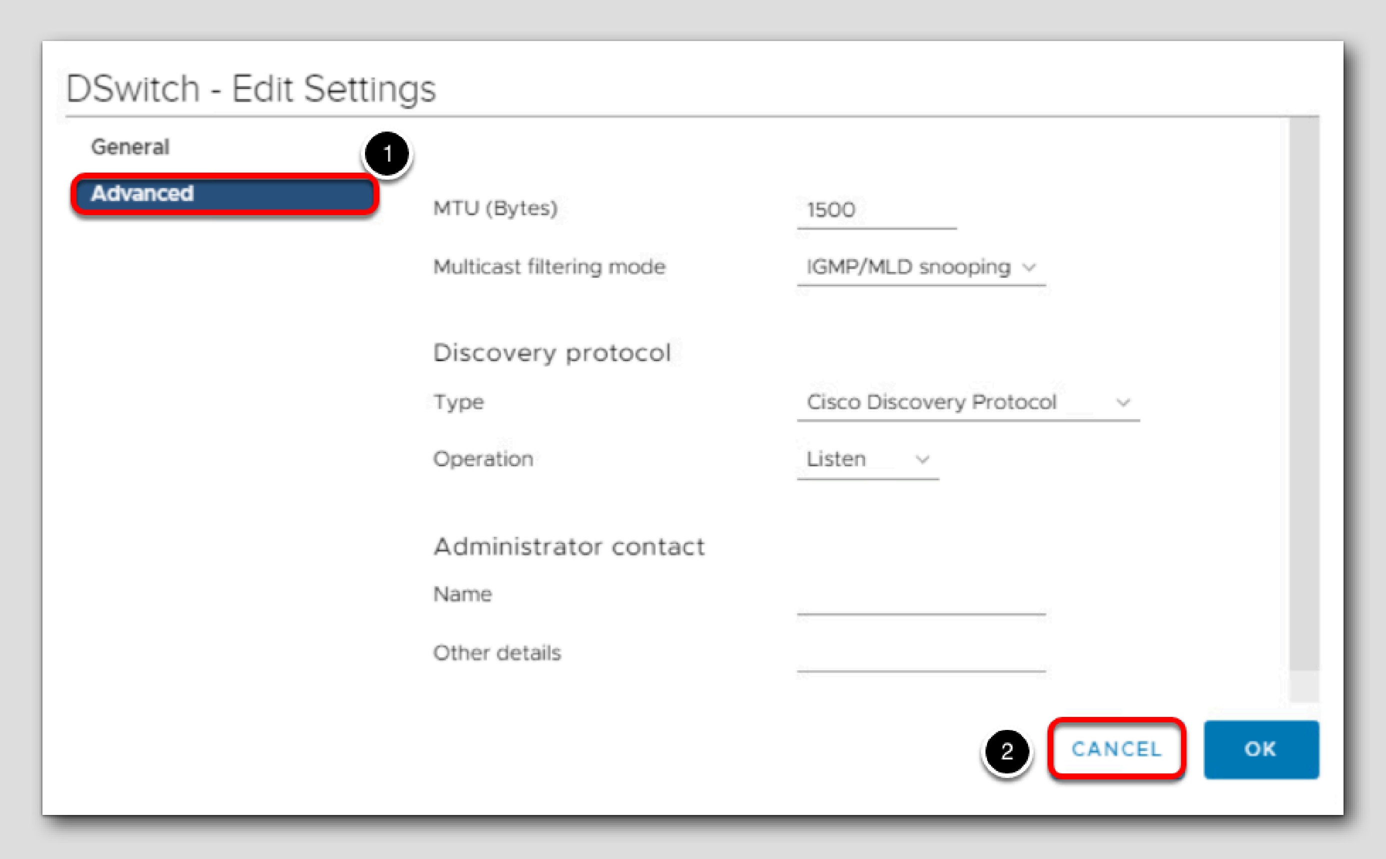
Number of Ports: This setting cannot be modified. The port count will dynamically be scaled up or down by default.

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

[351]



DSwitch - Edit Settings

MTU (Bytes): 1500

Multicast filtering mode: IGMP/MLD snooping

Discovery protocol

Type: Cisco Discovery Protocol

Operation: Listen

Administrator contact

Name

Other details

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

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

Multicast filtering mode

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

Discovery Protocol

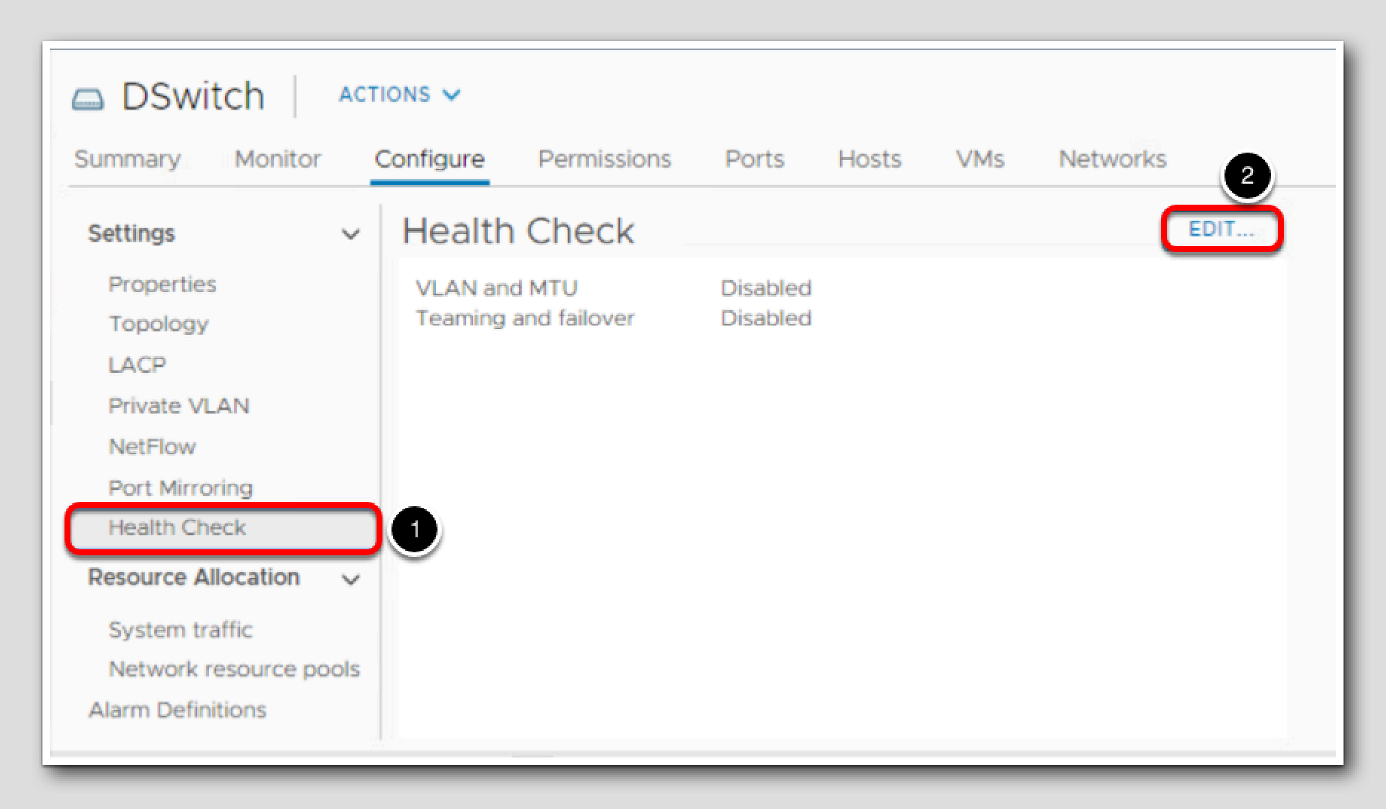
- Type - Cisco Discovery Protocol, Link Layer Discovery Protocol, or disabled..
- Operation - to Listen, Advertise, or Both.

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

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

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

[352]



VLAN and MTU	Disabled
Teaming and failover	Disabled

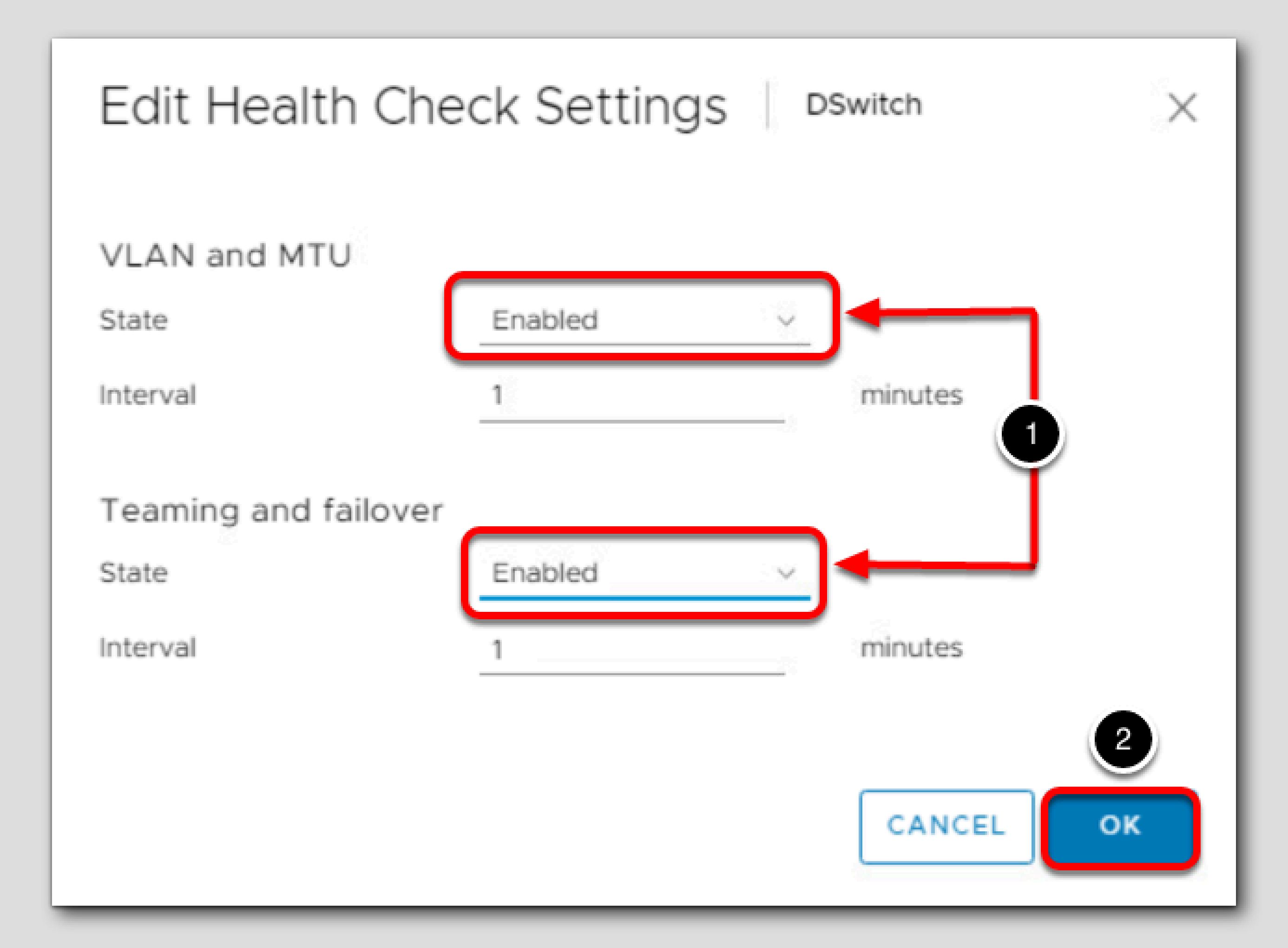
The Distributed Switch Health Check monitors for changes in vSphere Distributed Switch configurations. You must enable vSphere Distributed Switch Health Check to perform checks on Distributed Switch configurations.

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

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

Edit Health Check Settings

[353]



Edit Health Check Settings | DSwitch

VLAN and MTU

State: Enabled

Interval: 1 minutes

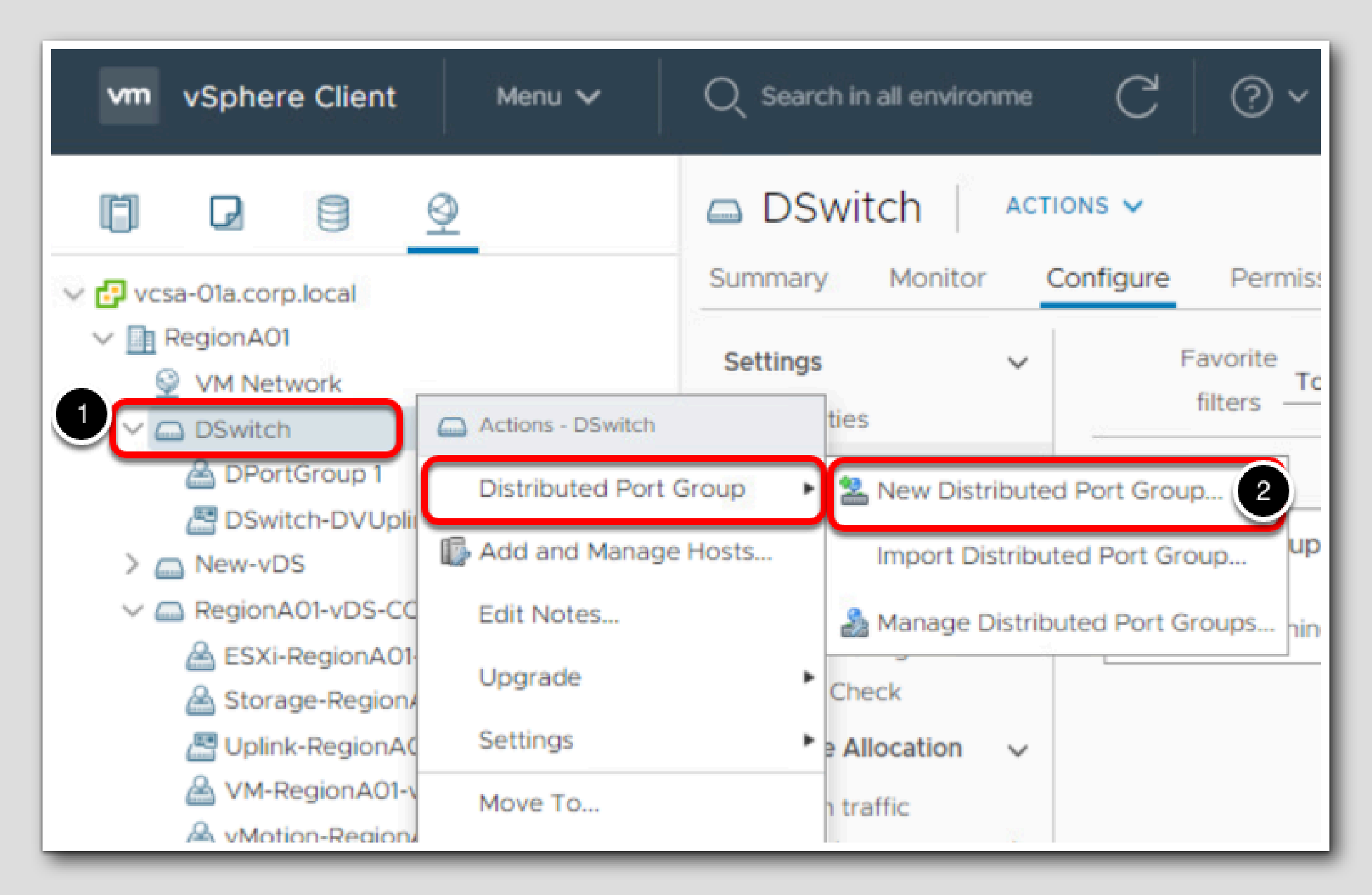
Teaming and failover

State: Enabled

Interval: 1 minutes

1. Select Enabled for both
2. Click OK

Distributed Port Groups

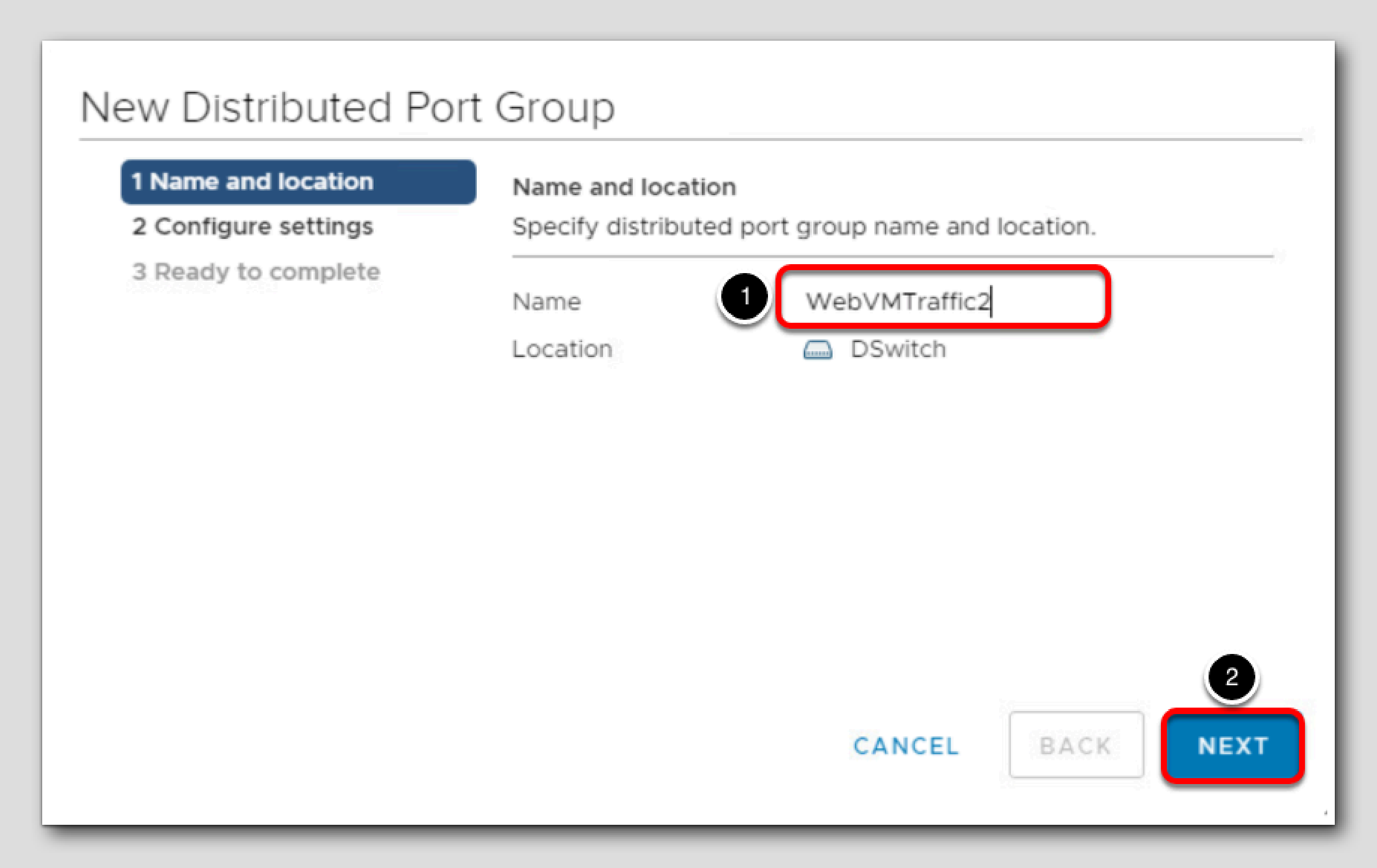


A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

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

Select name and location section

[355]



New Distributed Port Group

Name and location

Specify distributed port group name and location.

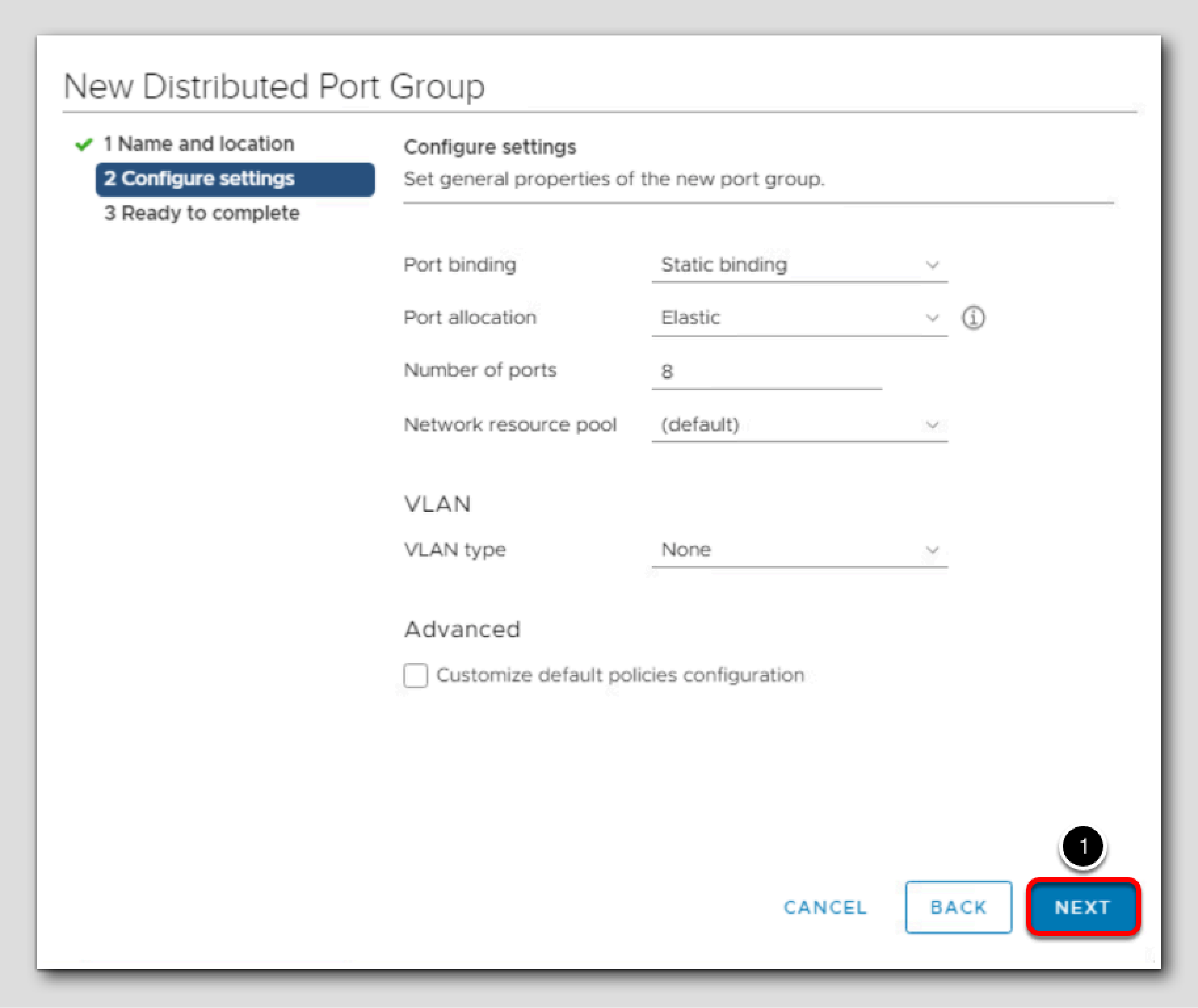
Name: WebVMTraffic2

Location: DSwitch

1. Name the new port group WebVMTraffic2
2. Click Next

Configure settings

[356]



New Distributed Port Group

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

Configure settings

Set general properties of the new port group.

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

VLAN

VLAN type: None

Advanced

□ Customize default policies configuration

1. Keep default settings and click Next

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

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

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

Port allocation

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

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

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

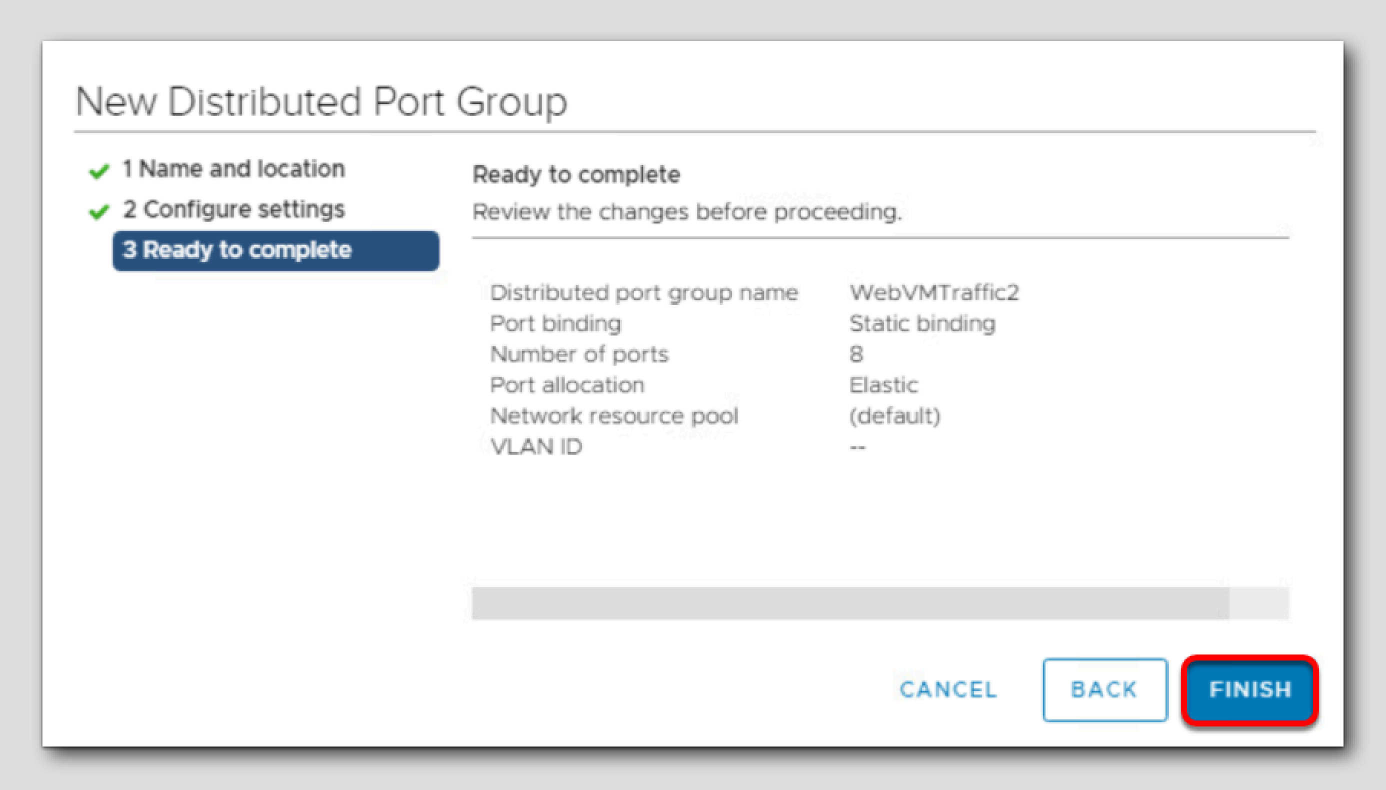
VLAN: Use the Type drop-down menu to select VLAN options:

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

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

Ready to complete

[357]



Ready to complete

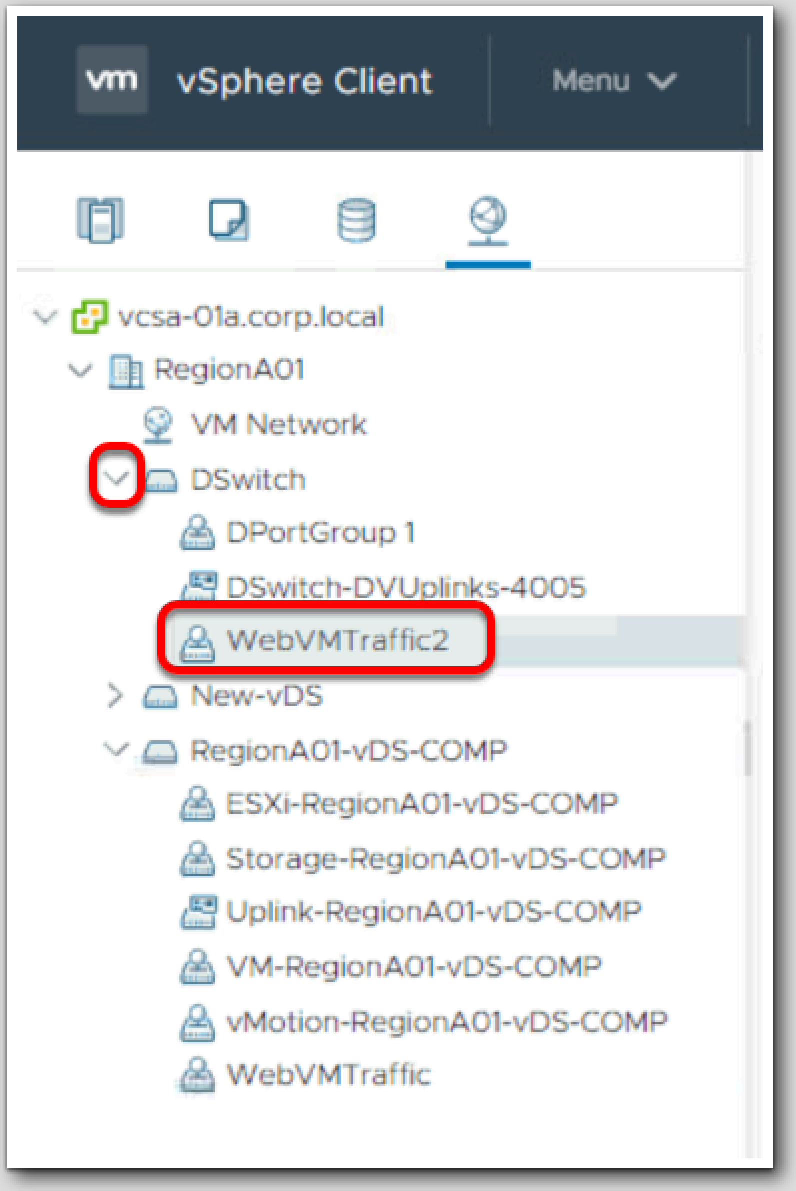
Review the changes before proceeding.

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

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

View the new Distributed Port Group

[358]



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

Using Host Lockdown Mode

[359]

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

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

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

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

NOTES:

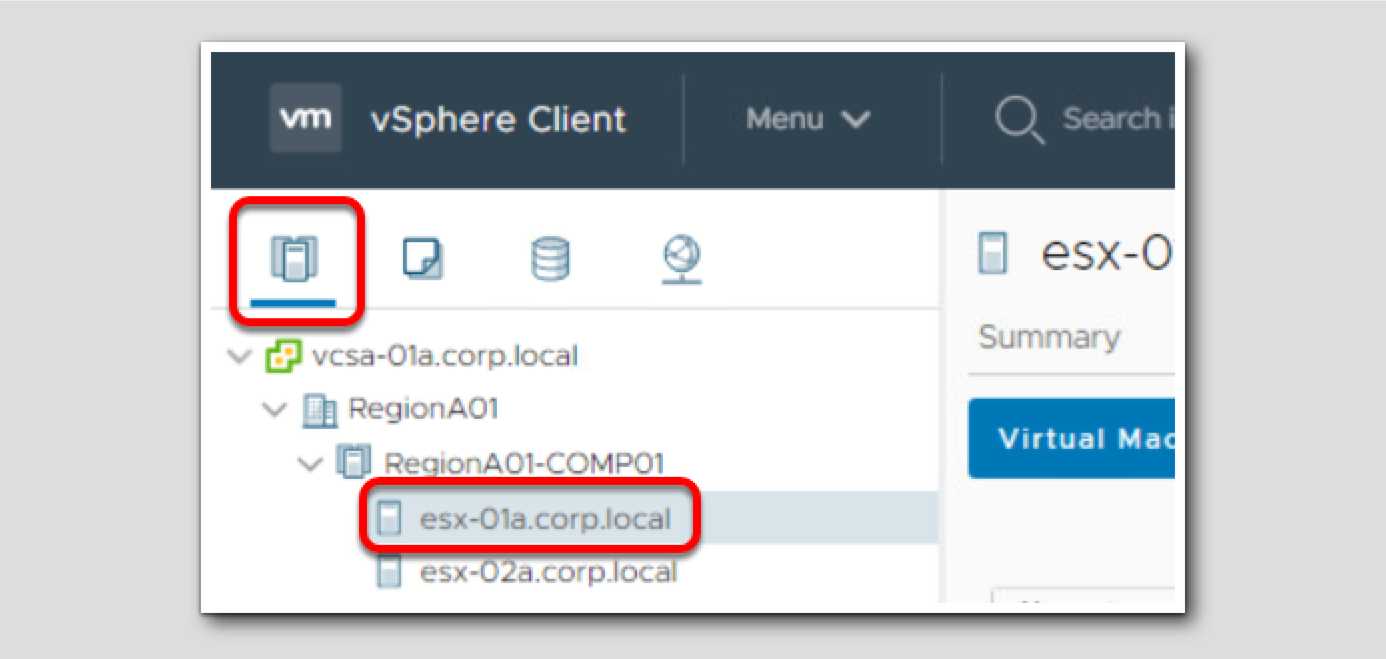
Users with the DCUI Access privilege are authorized to log in to the Direct Console User Interface (DCUI) when lockdown mode is enabled. When you disable lockdown mode using the DCUI, all users with the DCUI Access privilege are granted the Administrator role on the host. The DCUI Access privilege is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

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

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

Select Hosts and Clusters

[360]

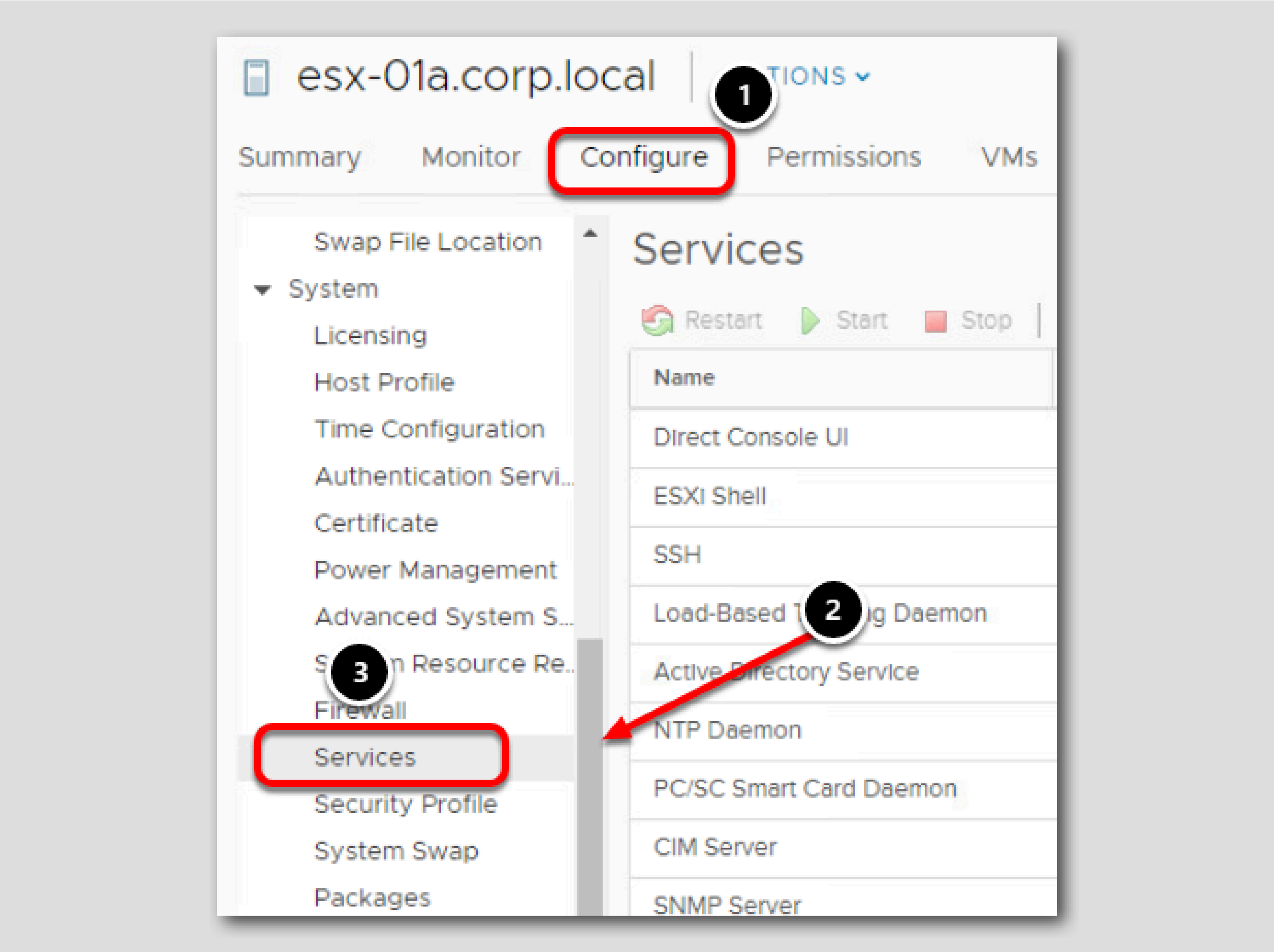


First, you will enable Host Lockdown Mode with the Normal setting on esx-01a.corp.local. This will mean the host will be accessible from vCenter and through the DCUI, but not remotely over SSH.

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

Security Profile

[361]



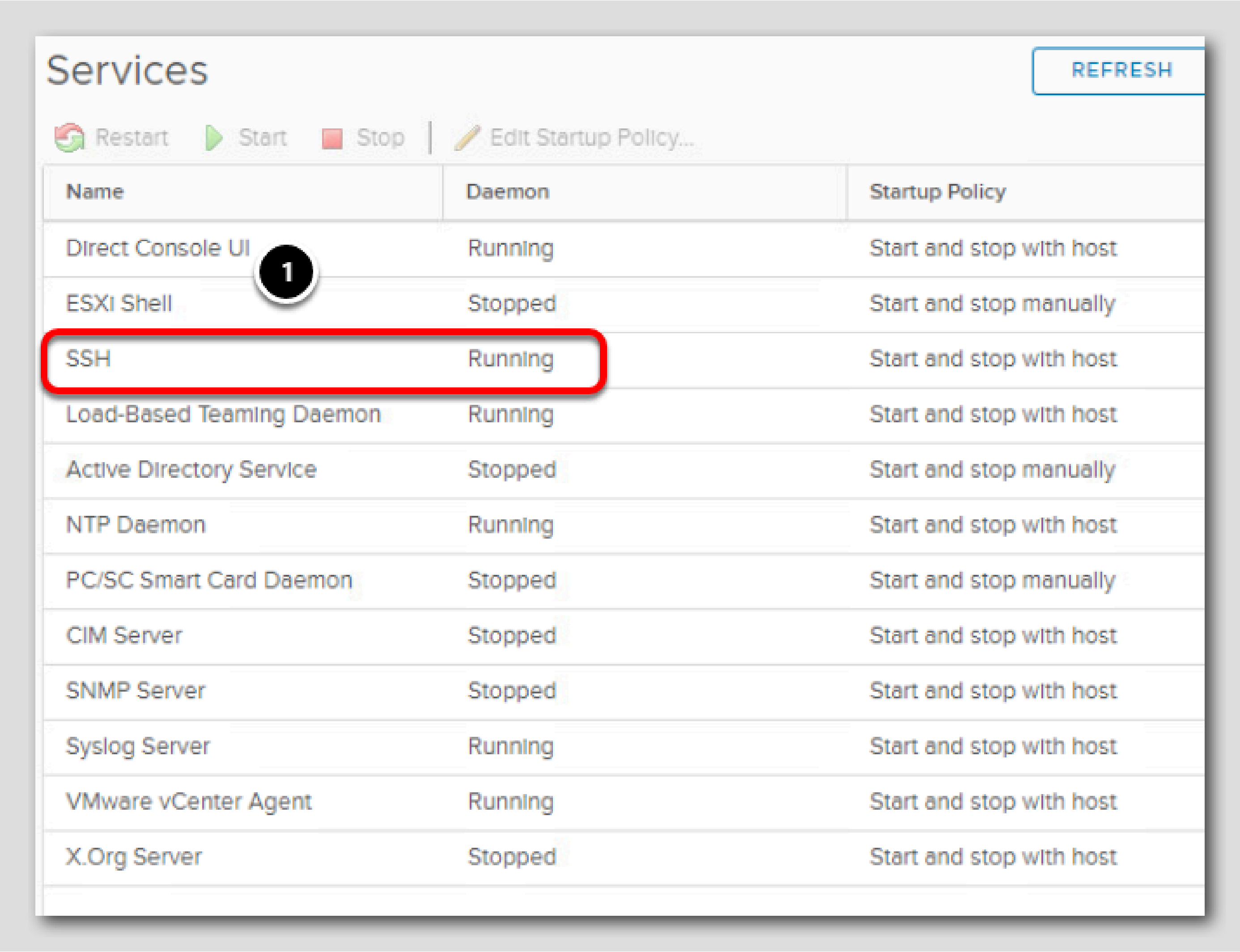
Name
Direct Console UI
ESXi Shell
SSH
Load-Based T g Daemon
Active Directory Service
NTP Daemon
PC/SC Smart Card Daemon
CIM Server
SNMP Server

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

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

Verify SSH is Enabled

[362]



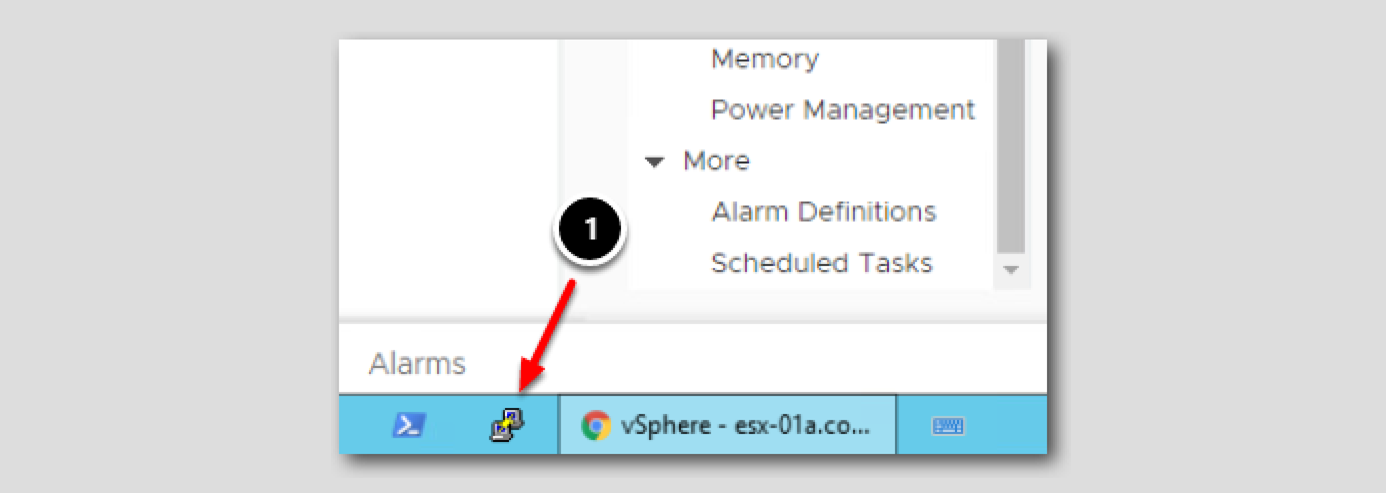
Services

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

[363]

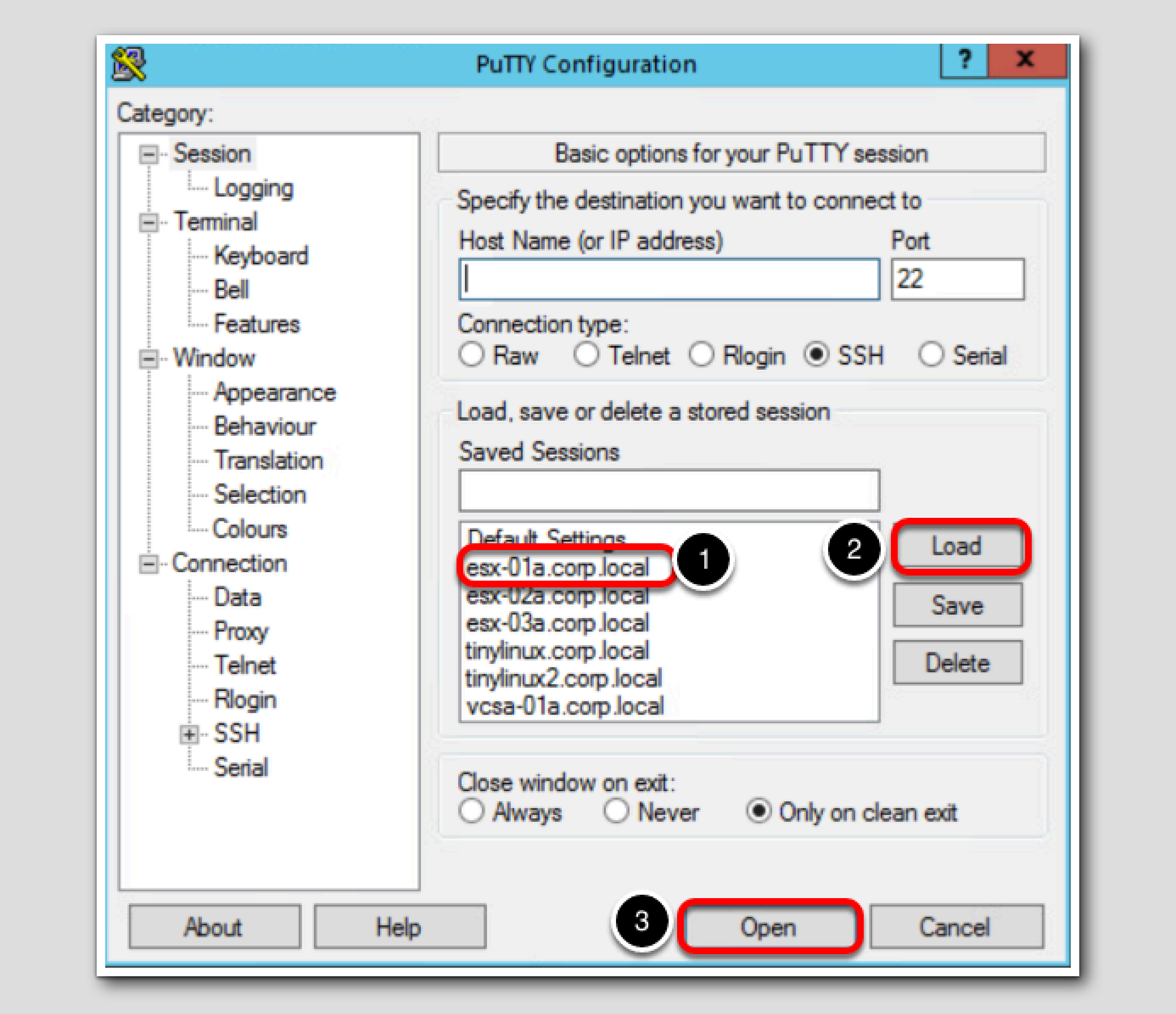


First, verify you can login to esx-01a using an SSH connection.

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

Connect to esx-01a

[364]



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

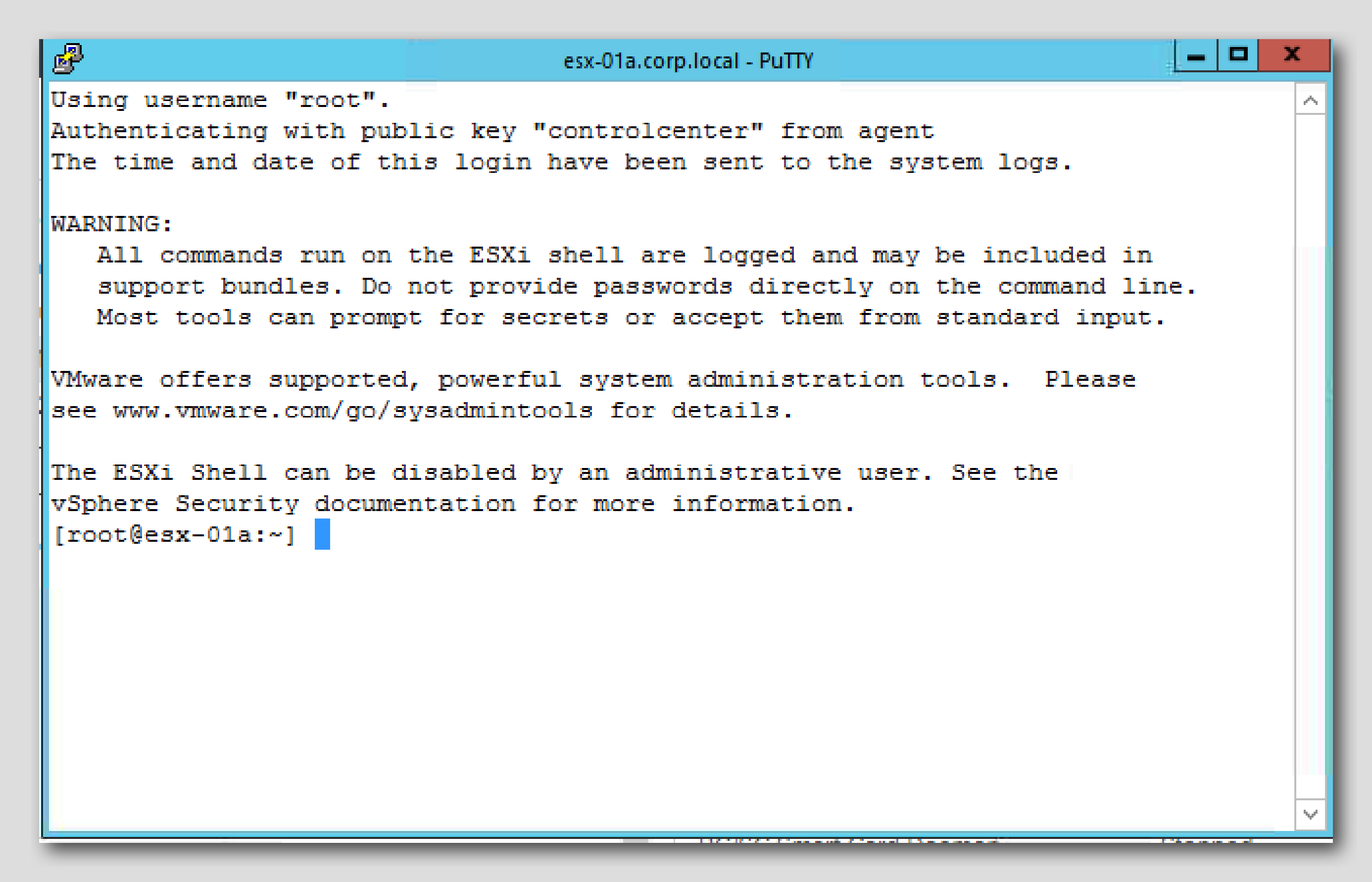
- Default Settings
- esx-01a.corp.local
- esx-02a.corp.local
- esx-03a.corp.local
- tinylinux.corp.local
- tinylinux2.corp.local
- vcsa-01a.corp.local

Close window on exit: ○ Always ○ Never ● Only on clean exit

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

Logged into esx-01a

[365]

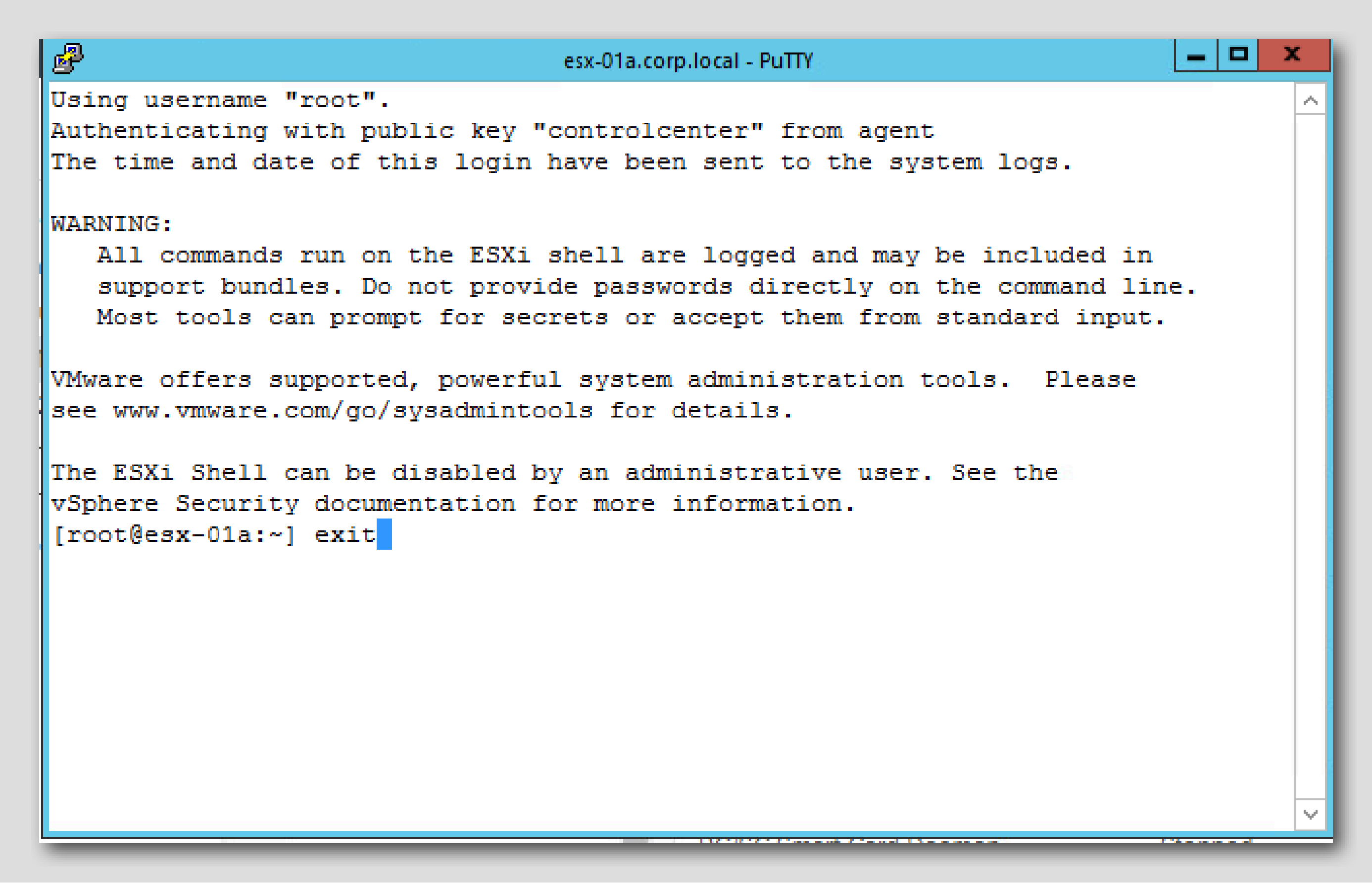


```
Using username "root".
Authenticating with public key "controlcenter" from agent
The time and date of this login have been sent to the system logs.

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

[366]



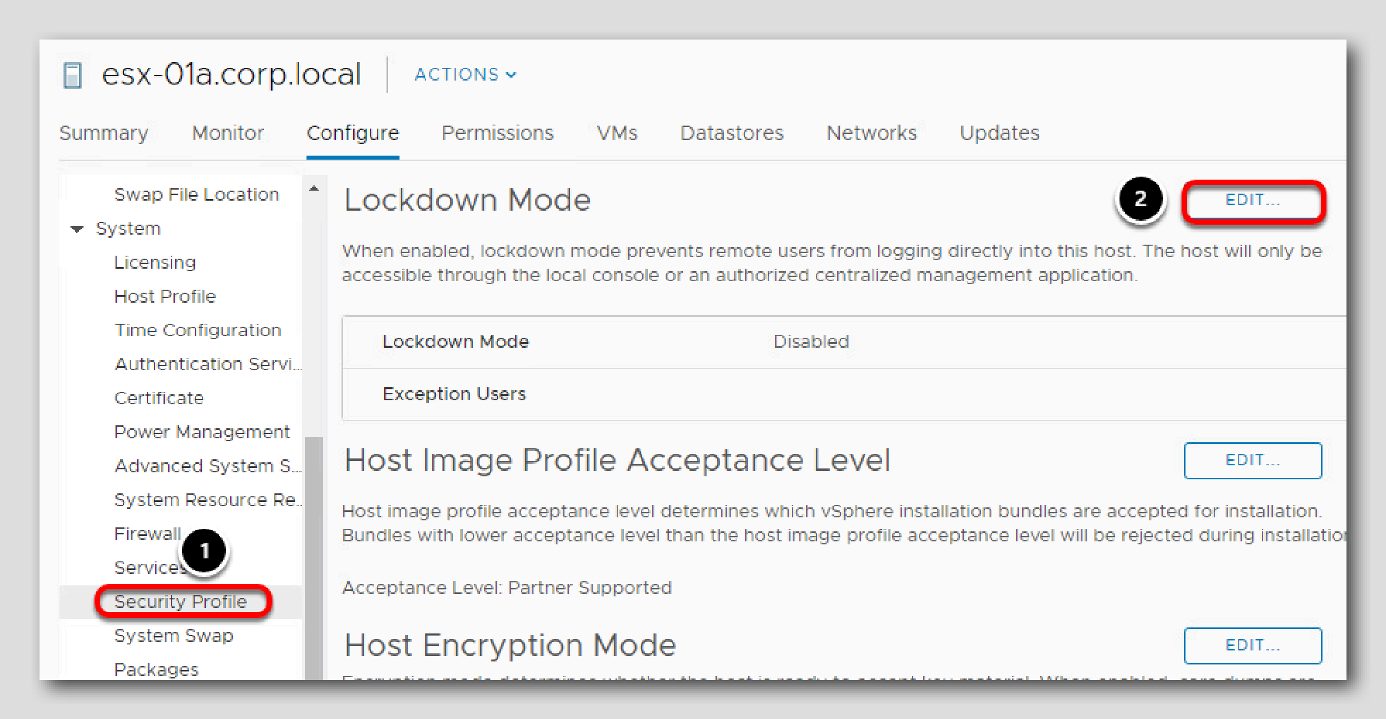
```
Using username "root".
Authenticating with public key "controlcenter" from agent
The time and date of this login have been sent to the system logs.

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
```

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

Once you hit Enter, the PuTTY window will disappear.

Enabling Lockdown Mode

[367]



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 installatio

Acceptance Level: Partner Supported

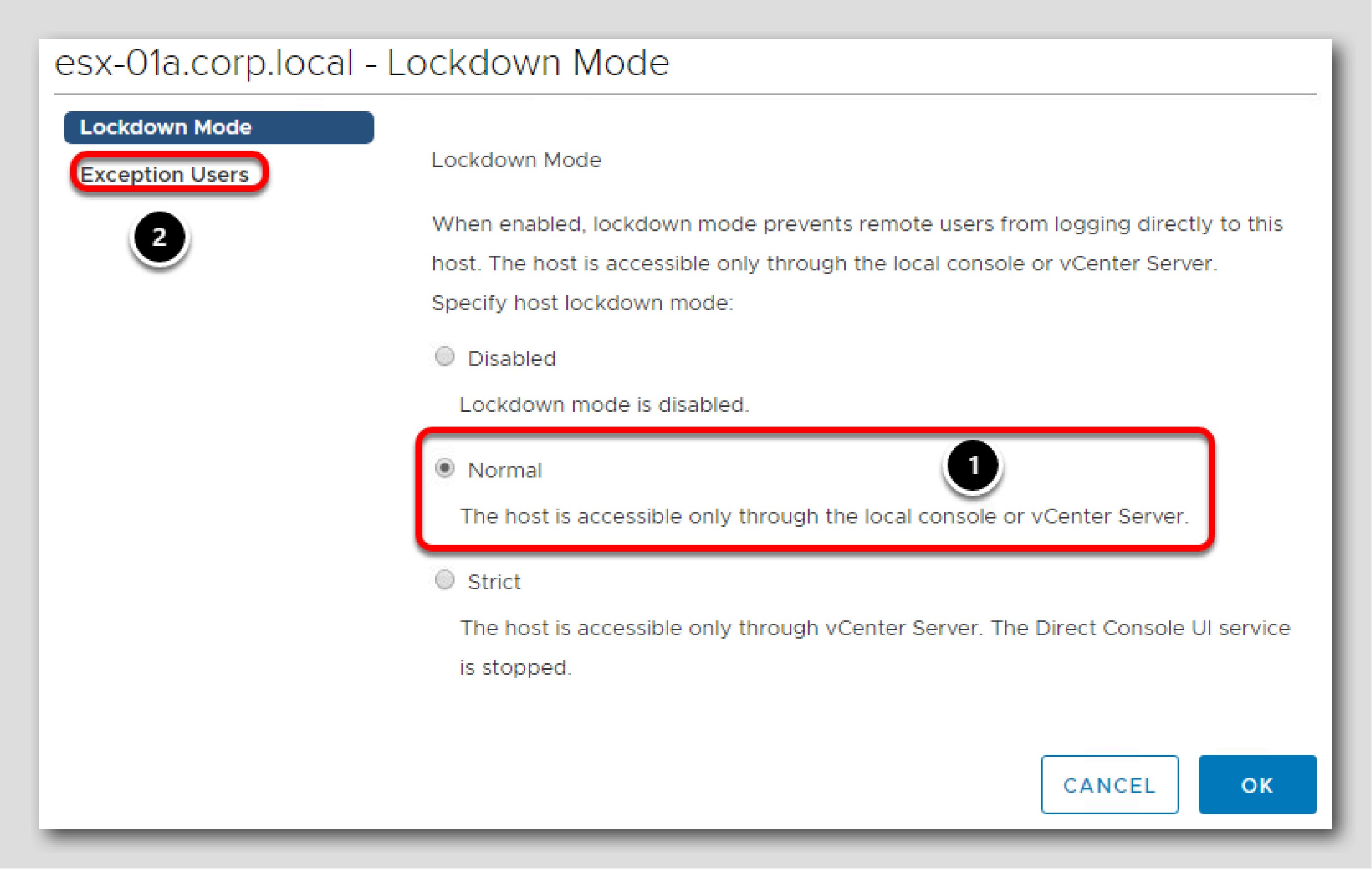
Host Encryption Mode

Go back to the vSphere Client

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

Lockdown Mode

[368]



esx-01a.corp.local - 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

Lockdown mode is disabled.

● Normal

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

○ Strict

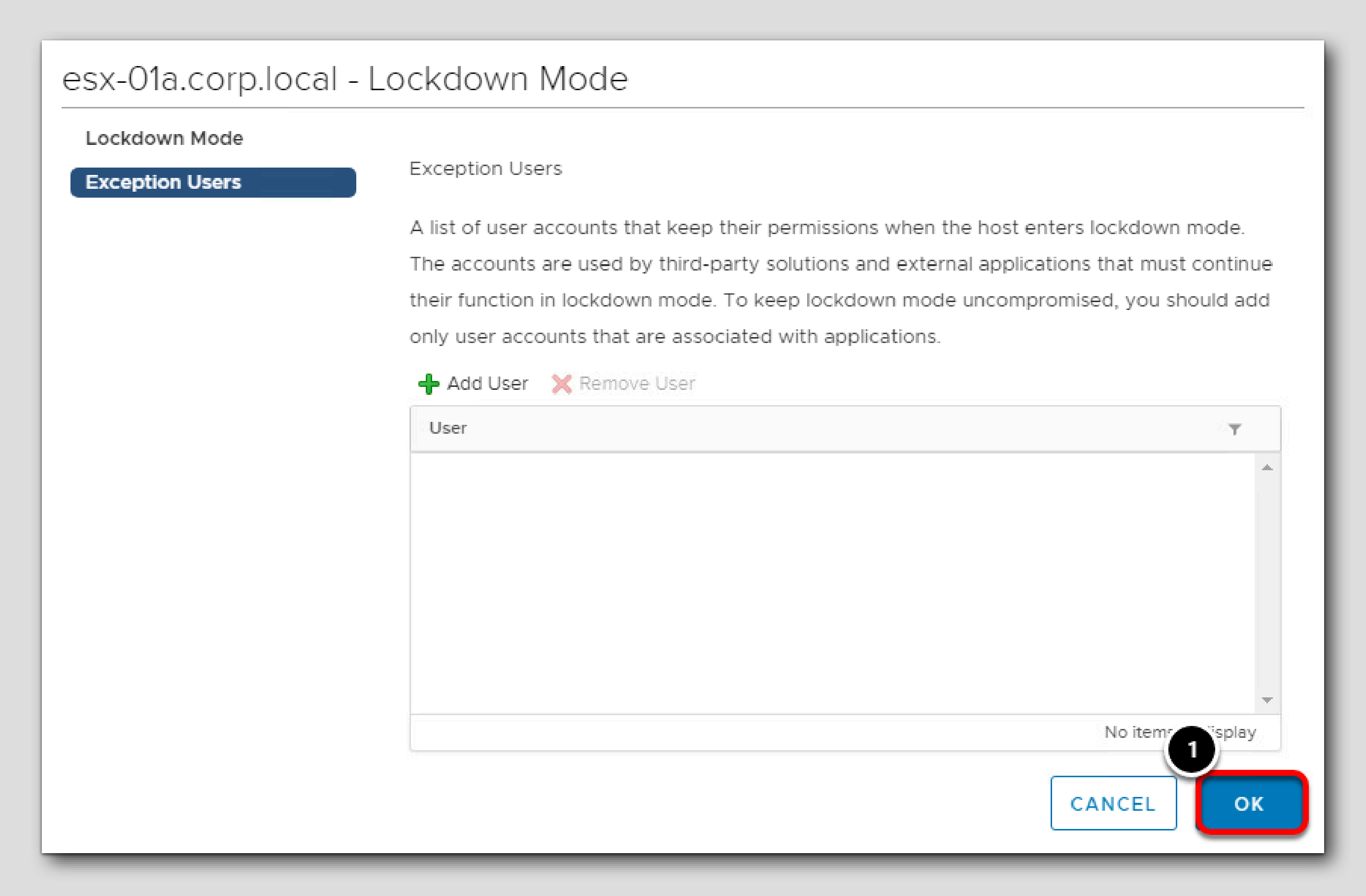
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

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

[369]



esx-01a.corp.local - Lockdown Mode

Exception Users

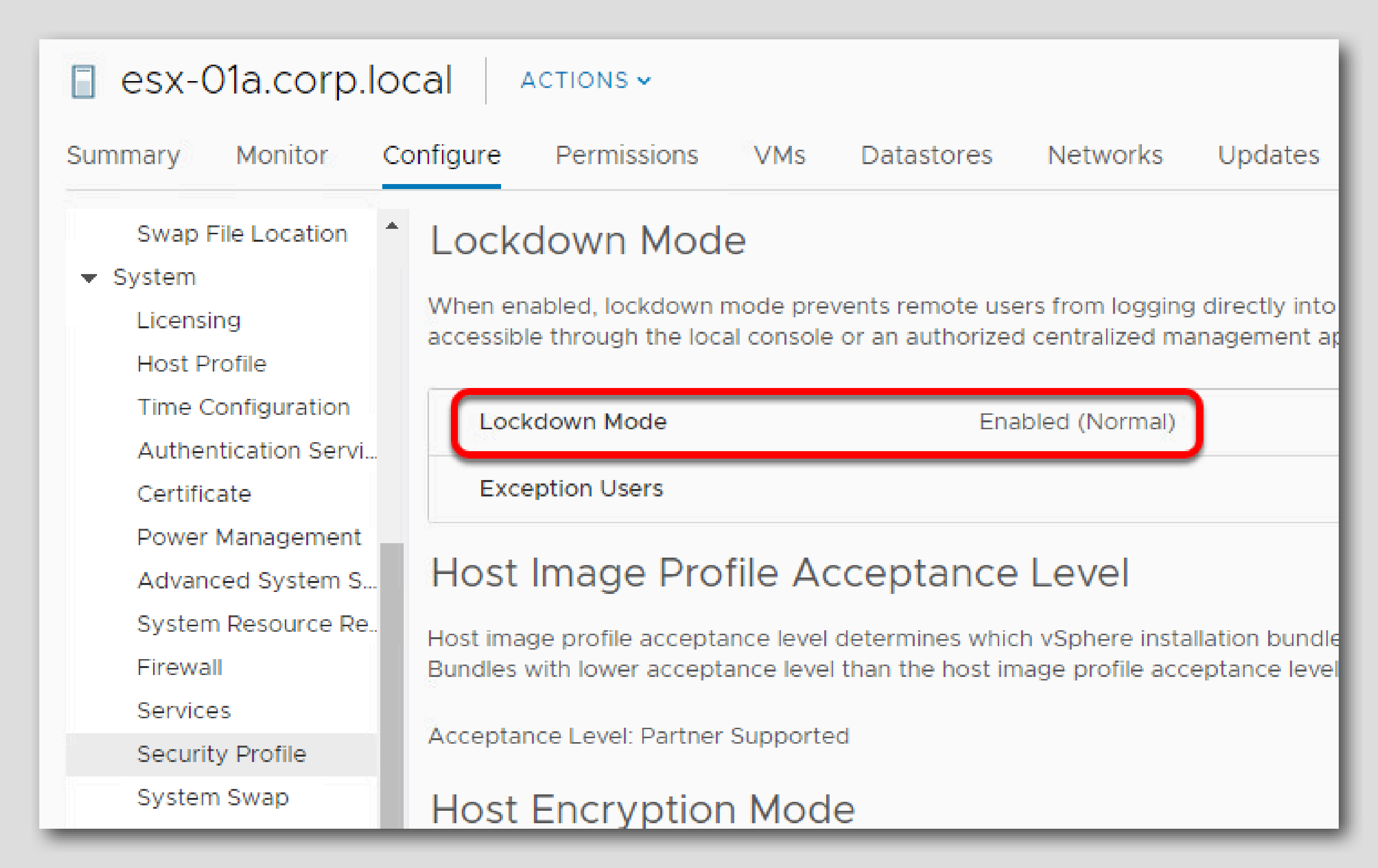
A list of user accounts that keep their permissions when the host enters lockdown mode. The accounts are used by third-party solutions and external applications that must continue their function in lockdown mode. To keep lockdown mode uncompromised, you should add only user accounts that are associated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

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

[370]



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

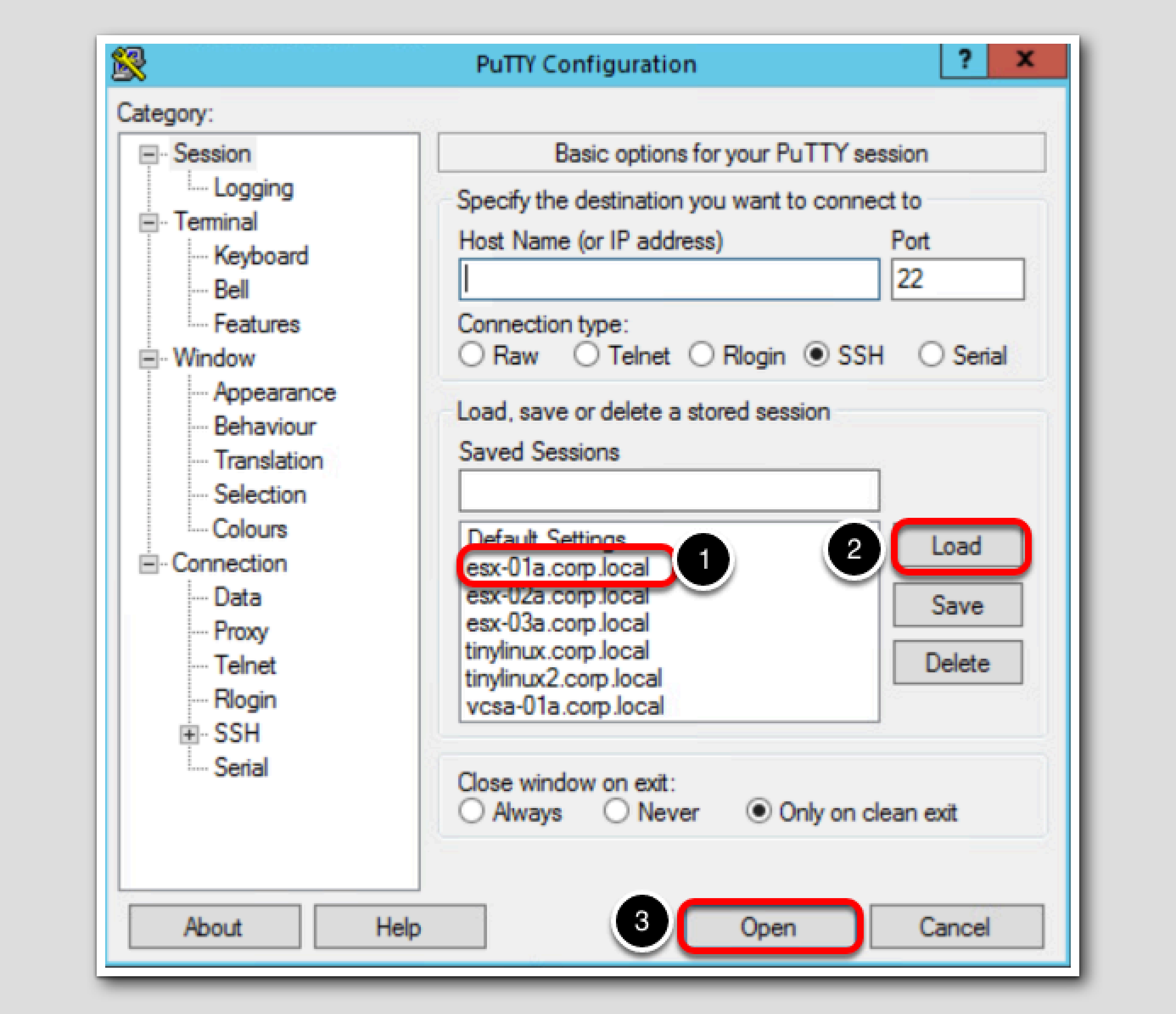
Acceptance Level: Partner Supported

Host Encryption Mode

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

PuTTY Session to esx-01a

[371]

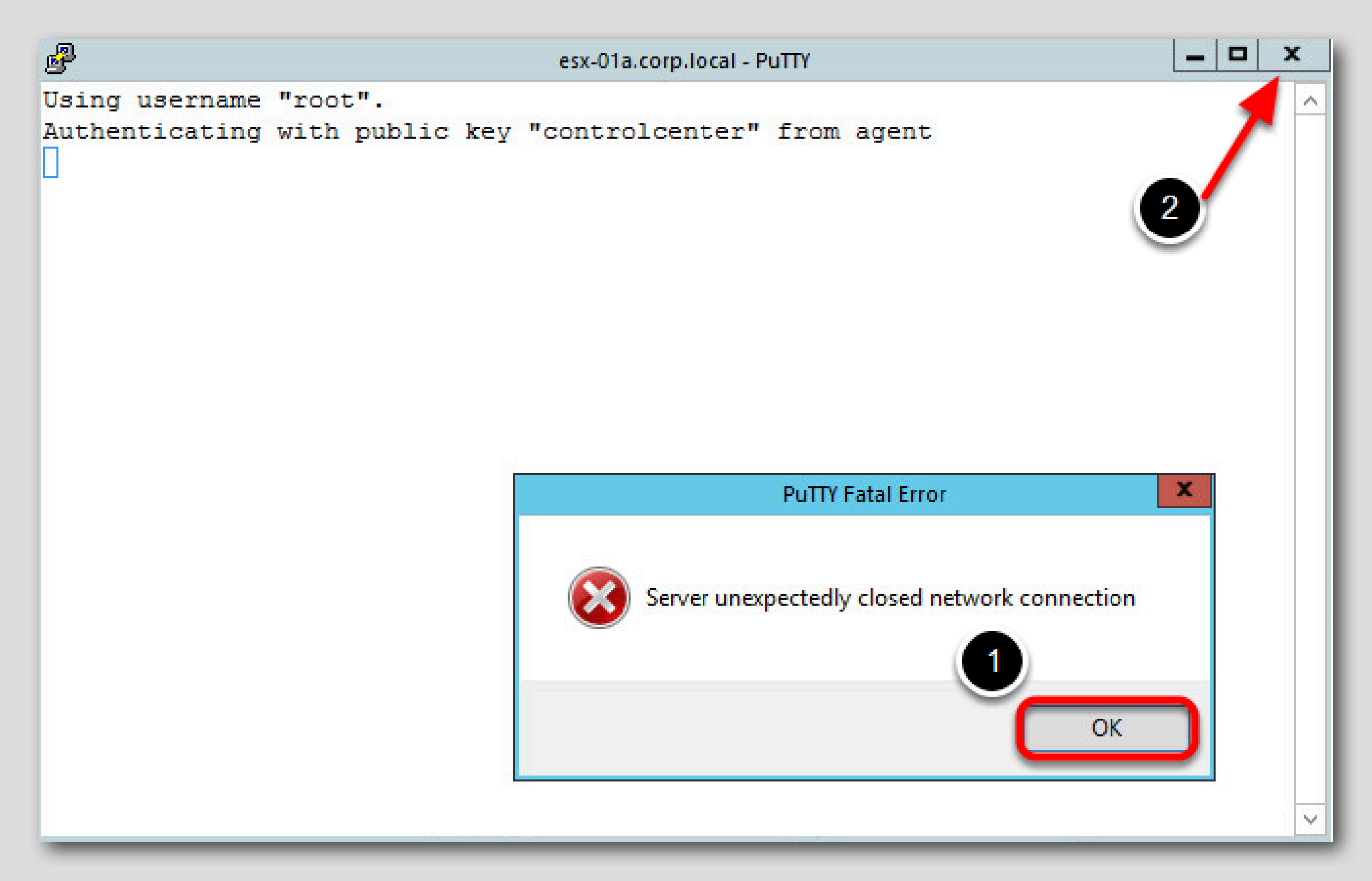


Using the same steps we used above, open the PuTTY application from the Windows Taskbar.

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

Denied!

[372]



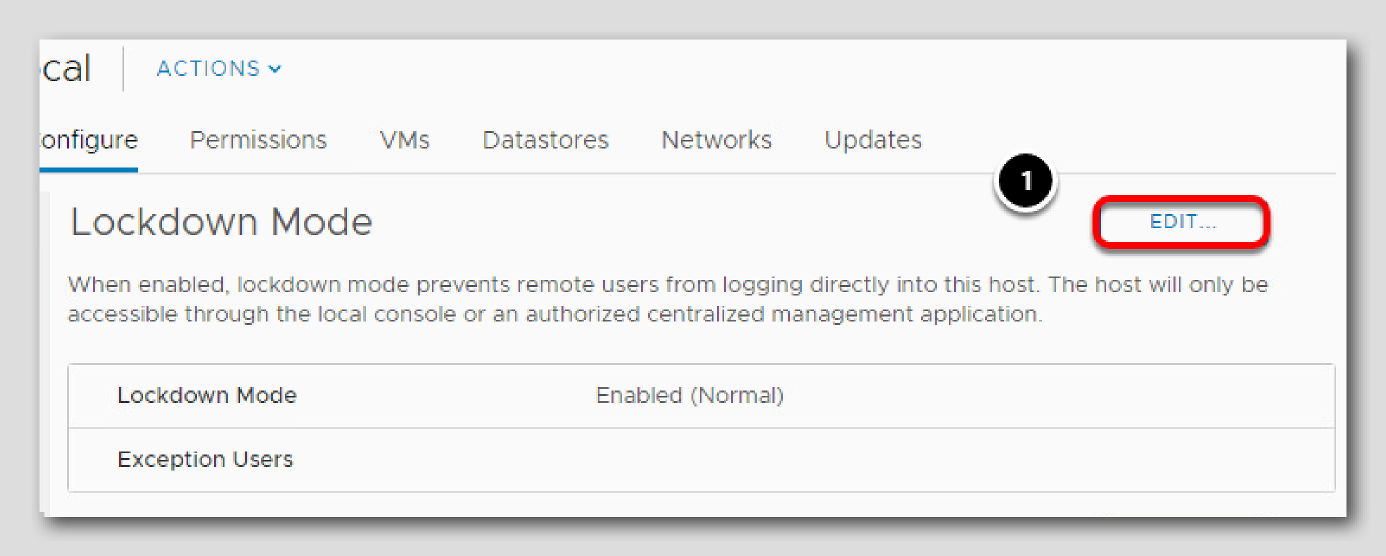
```
Using username "root".
Authenticating with public key "controlcenter" from agent
```

Server unexpectedly closed network connection

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



Lockdown Mode

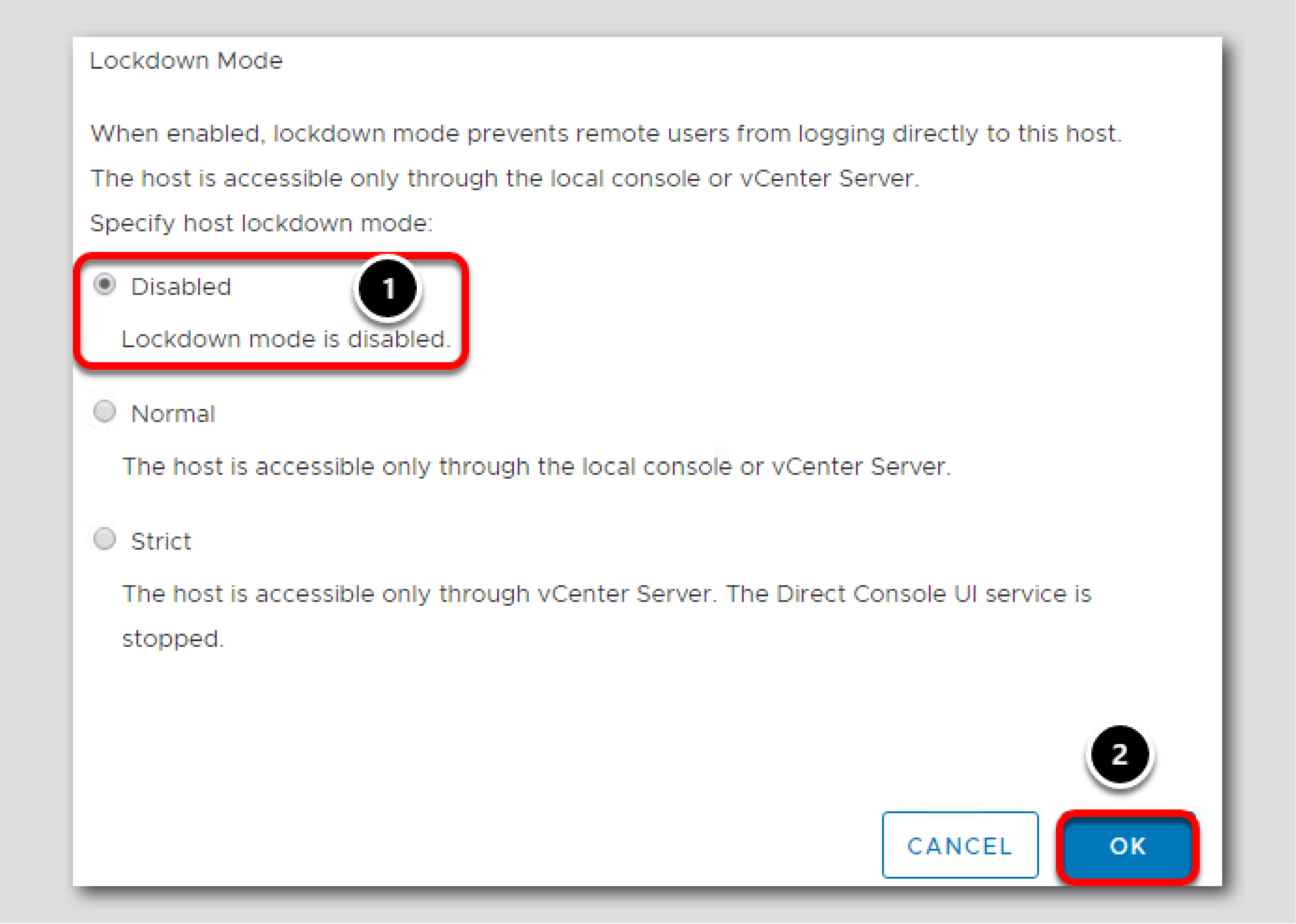
When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through the local console or an authorized centralized management application.

Lockdown Mode	Enabled (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

Lockdown mode is disabled.

○ Normal

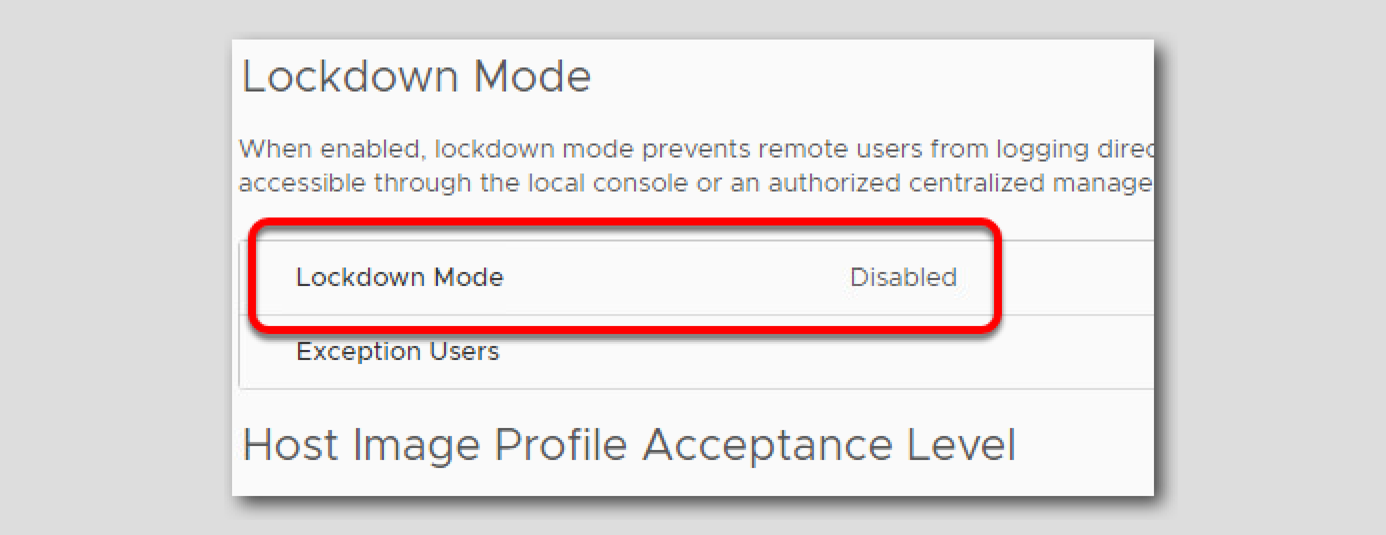
The host is accessible only through the local console or vCenter Server.

○ 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 direc
accessible through the local console or an authorized centralized manage

Lockdown Mode	Disabled
Exception Users	

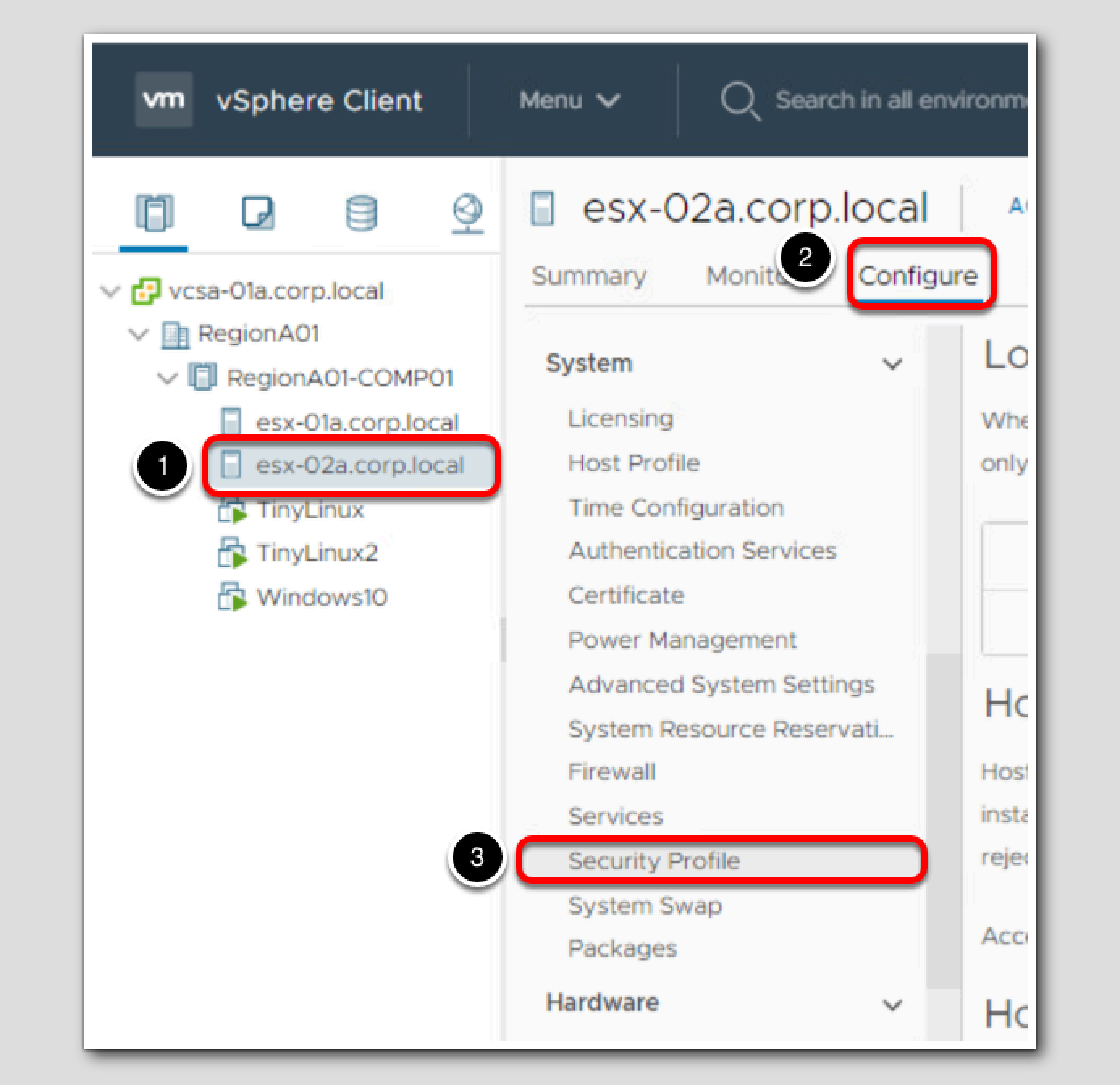
Host Image Profile Acceptance Level

Lockdown Mode for the host should now be disabled.

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

Strict Mode

[376]

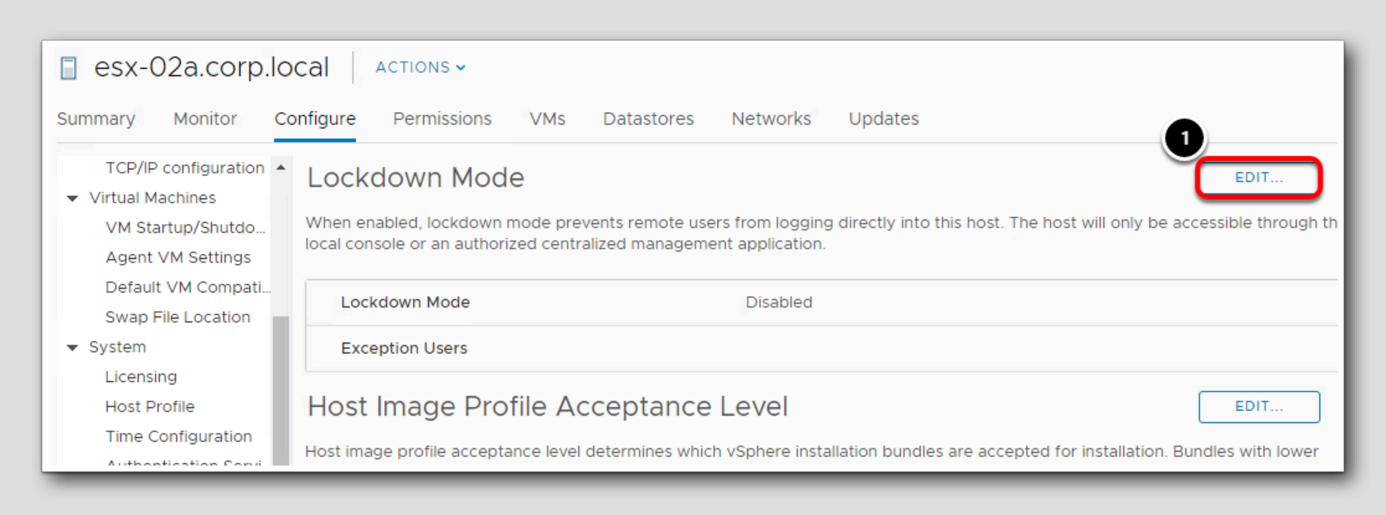


Now you will set esx-02a.corp.local to use the Strict Mode of Host Lockdown. This means the host is only available through vCenter Server and access to the DCUI and SSH are disabled.

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

Enable Lockdown Mode

[377]



Lockdown Mode

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

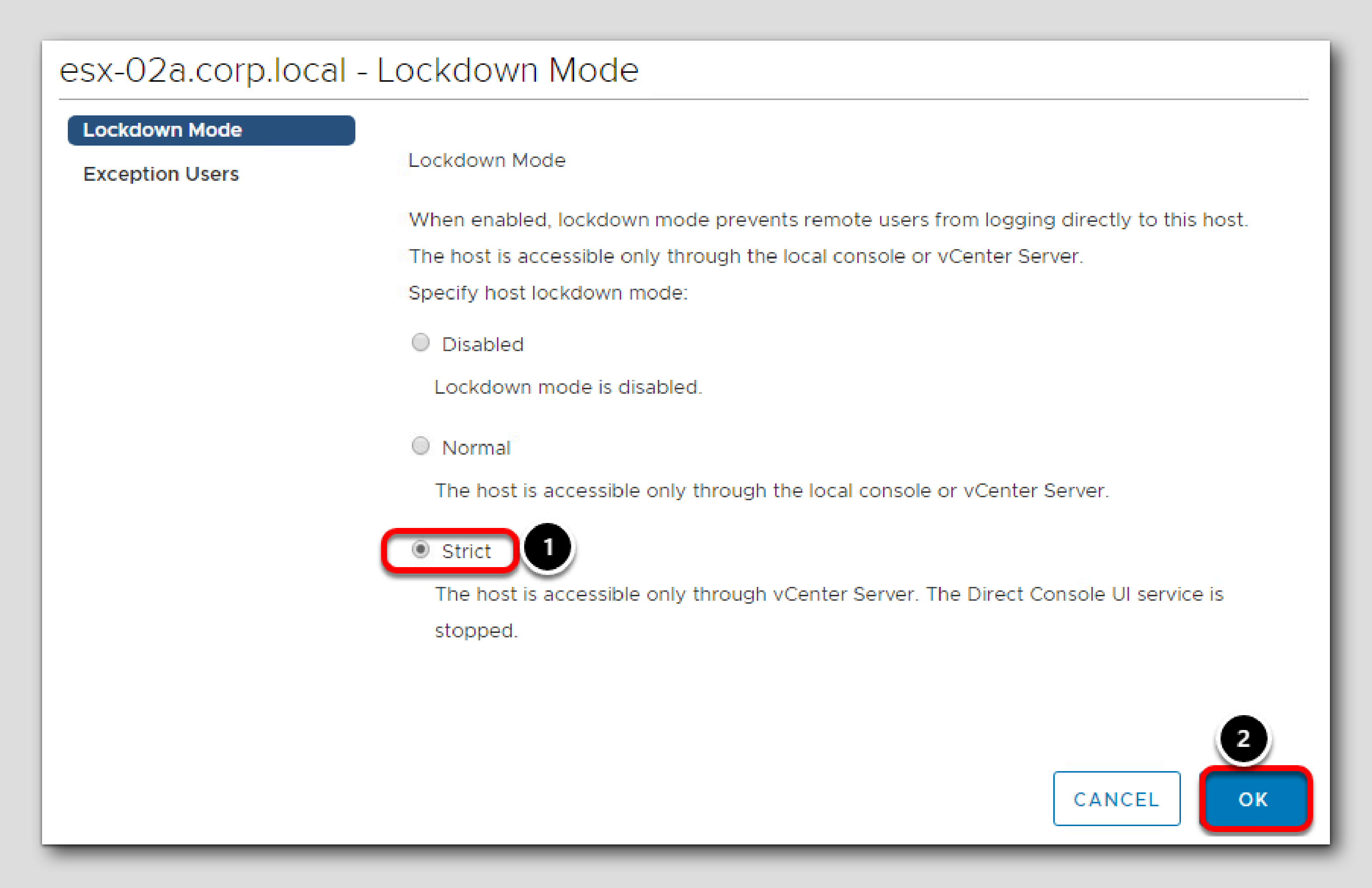
Lockdown Mode	Disabled
Exception Users	

Host Image Profile Acceptance Level

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

1. Click on the **Edit** button

Lockdown Mode - Strict



esx-02a.corp.local - 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

Lockdown mode is disabled.

○ Normal

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

● Strict

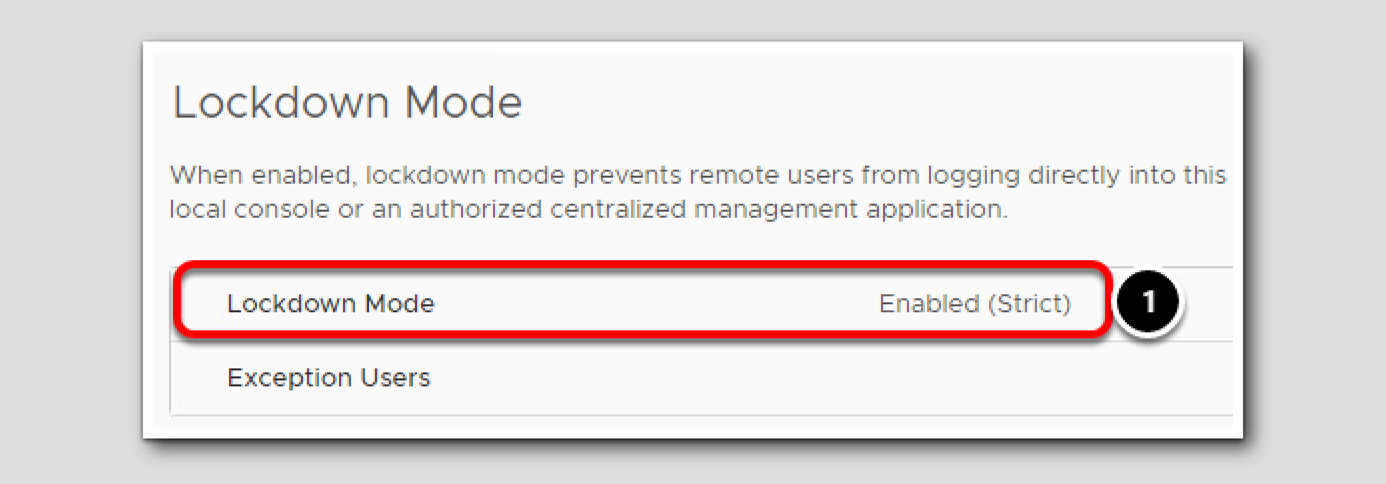
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

1. 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

[379]



Lockdown Mode

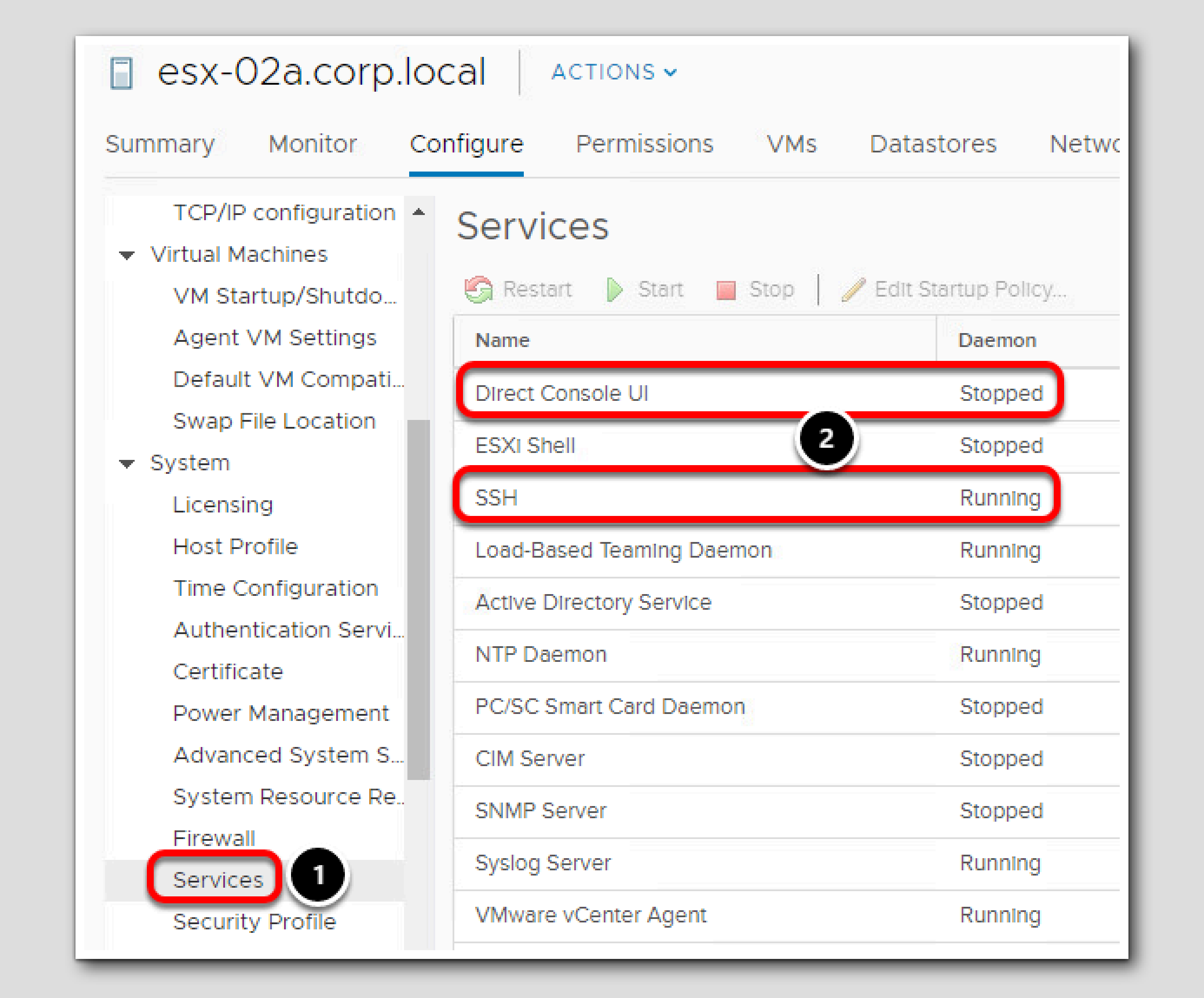
When enabled, lockdown mode prevents remote users from logging directly into this local console or an authorized centralized management application.

Lockdown Mode Enabled (Strict)

Exception Users

1. Notice Lockdown Mode is now Enabled

Services



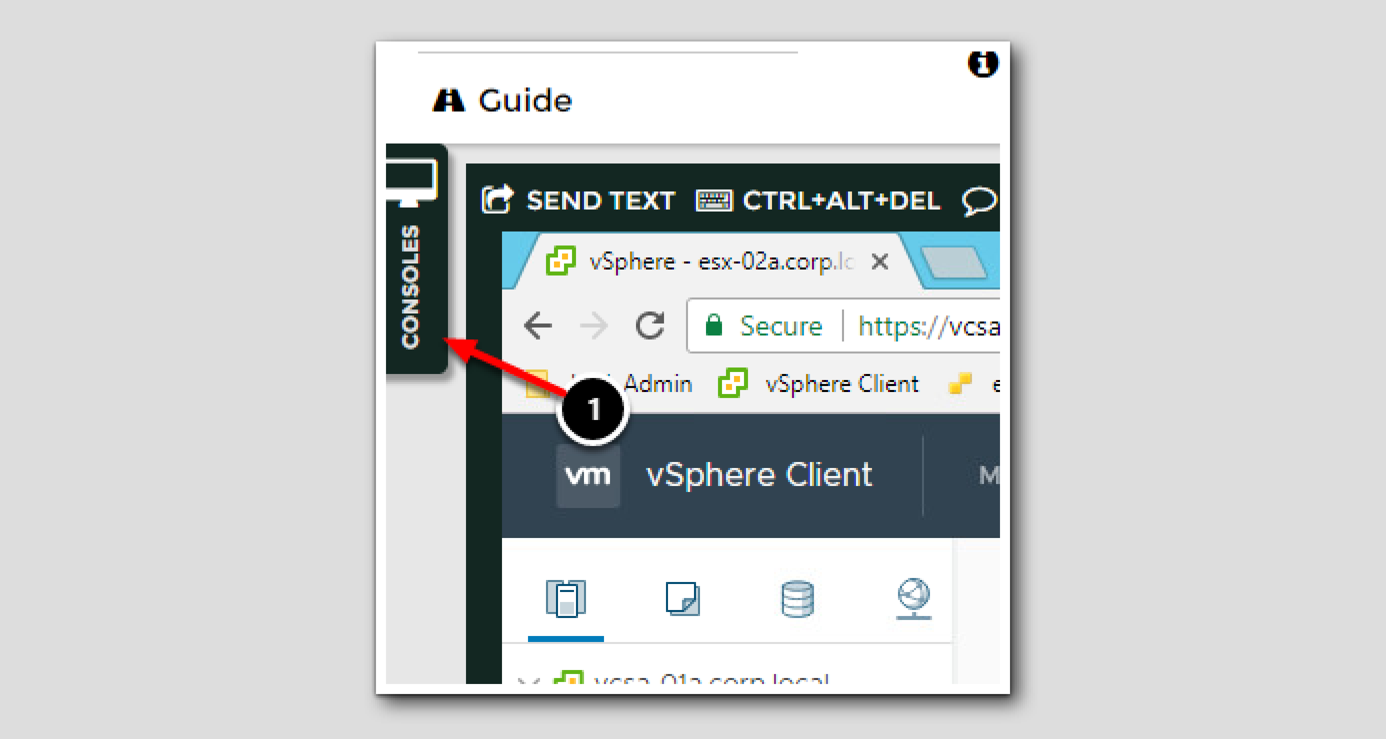
Name	Daemon
Direct Console UI	Stopped
ESXi Shell	Stopped
SSH	Running
Load-Based Teaming Daemon	Running
Active Directory Service	Stopped
NTP Daemon	Running
PC/SC Smart Card Daemon	Stopped
CIM Server	Stopped
SNMP Server	Stopped
Syslog Server	Running
VMware vCenter Agent	Running

1. Click on **Services**.

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

DCUI Disabled

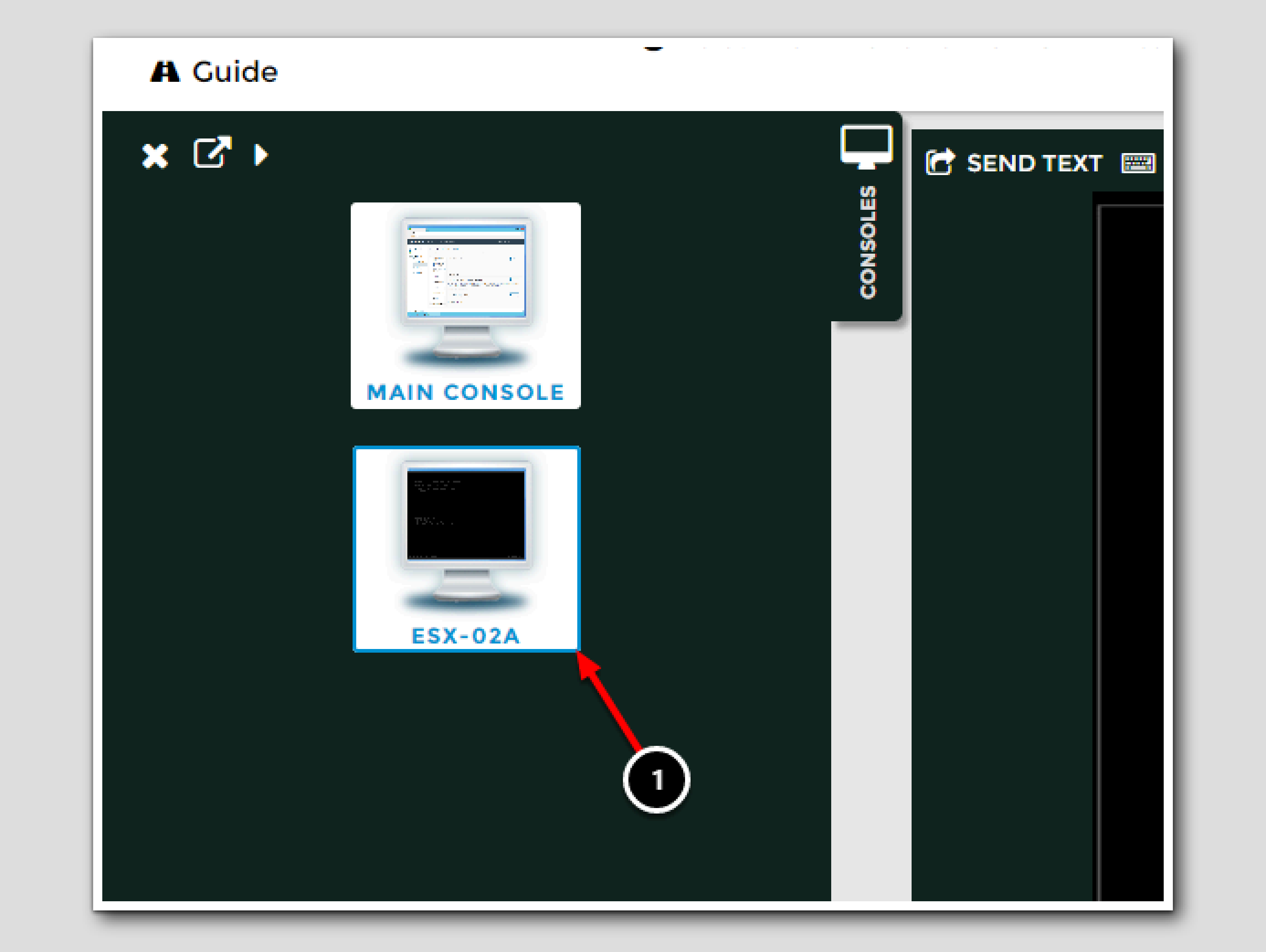
[381]



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

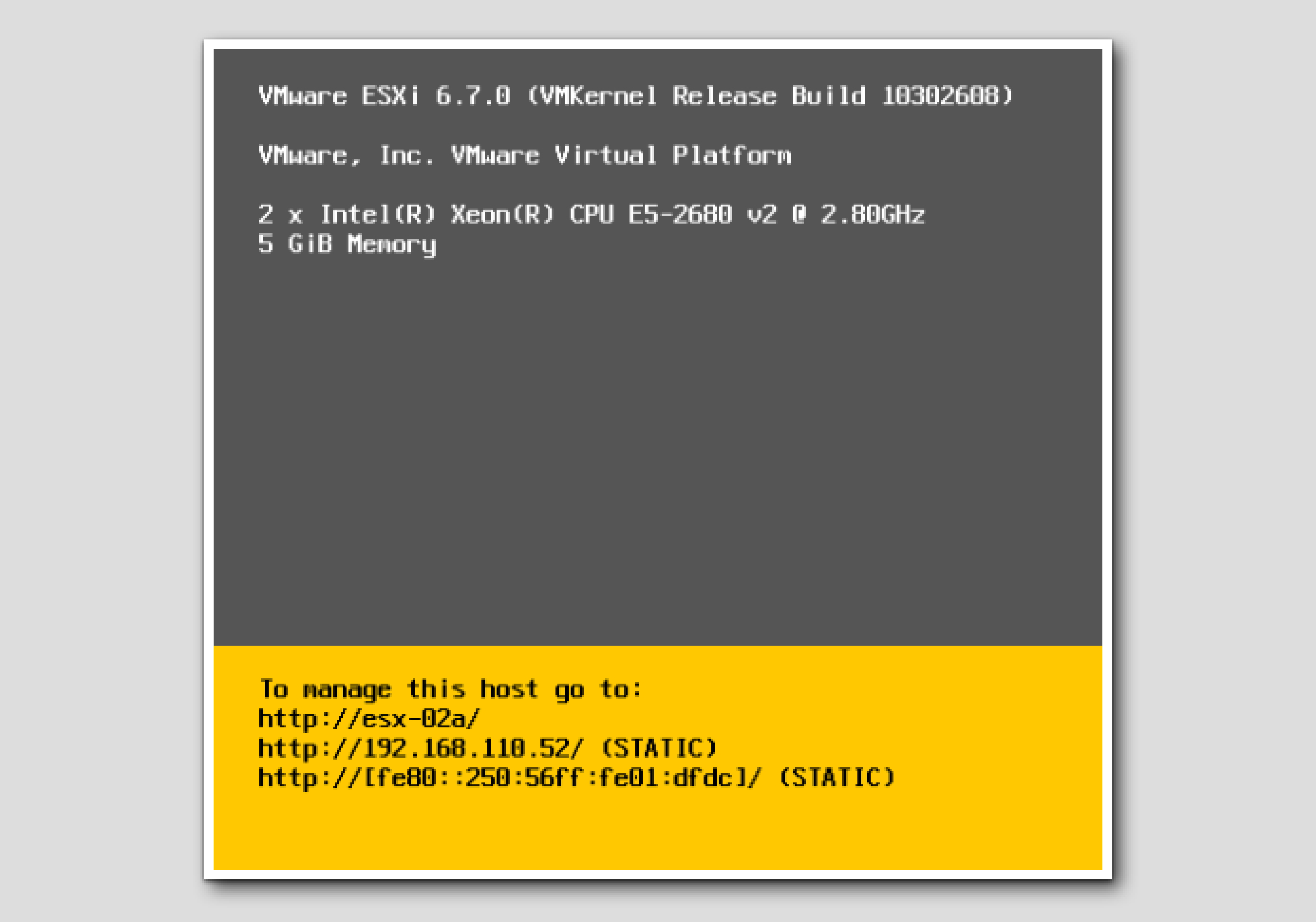


1. Click on the thumbnail for ESX-02A.

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

Click in the Console

[383]

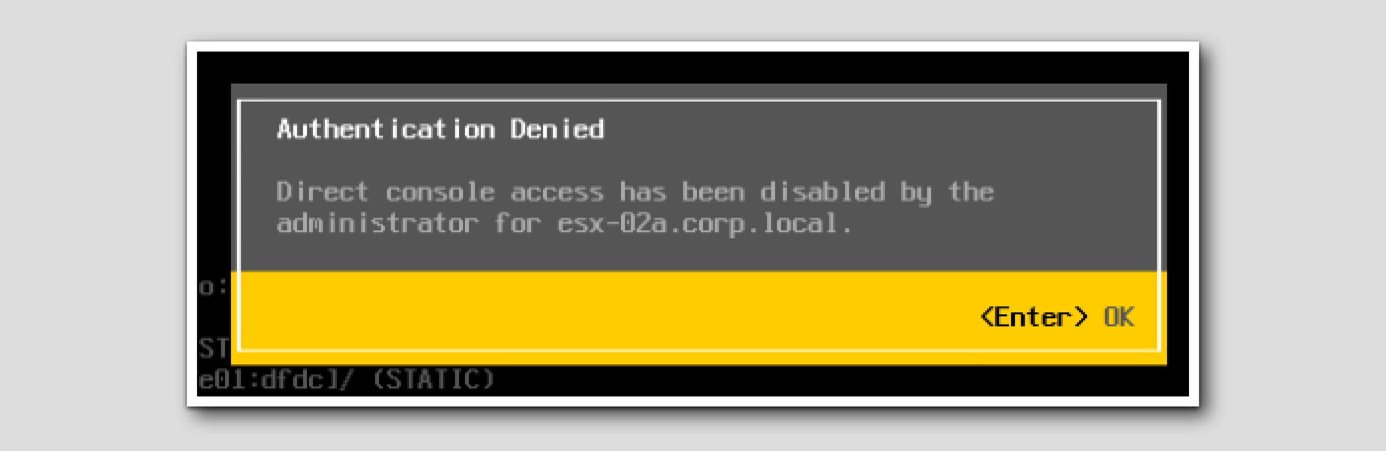


```
VMware ESXi 6.7.0 (VMKernel Release Build 10302608)

VMware, Inc. VMware Virtual Platform

2 x Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
5 GiB Memory

To manage this host go to:
http://esx-02a/
http://192.168.110.52/ (STATIC)
http://[fe80::250:56ff:fe01:dfdc]/ (STATIC)
```

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

Press F2

[384]



Authentication Denied

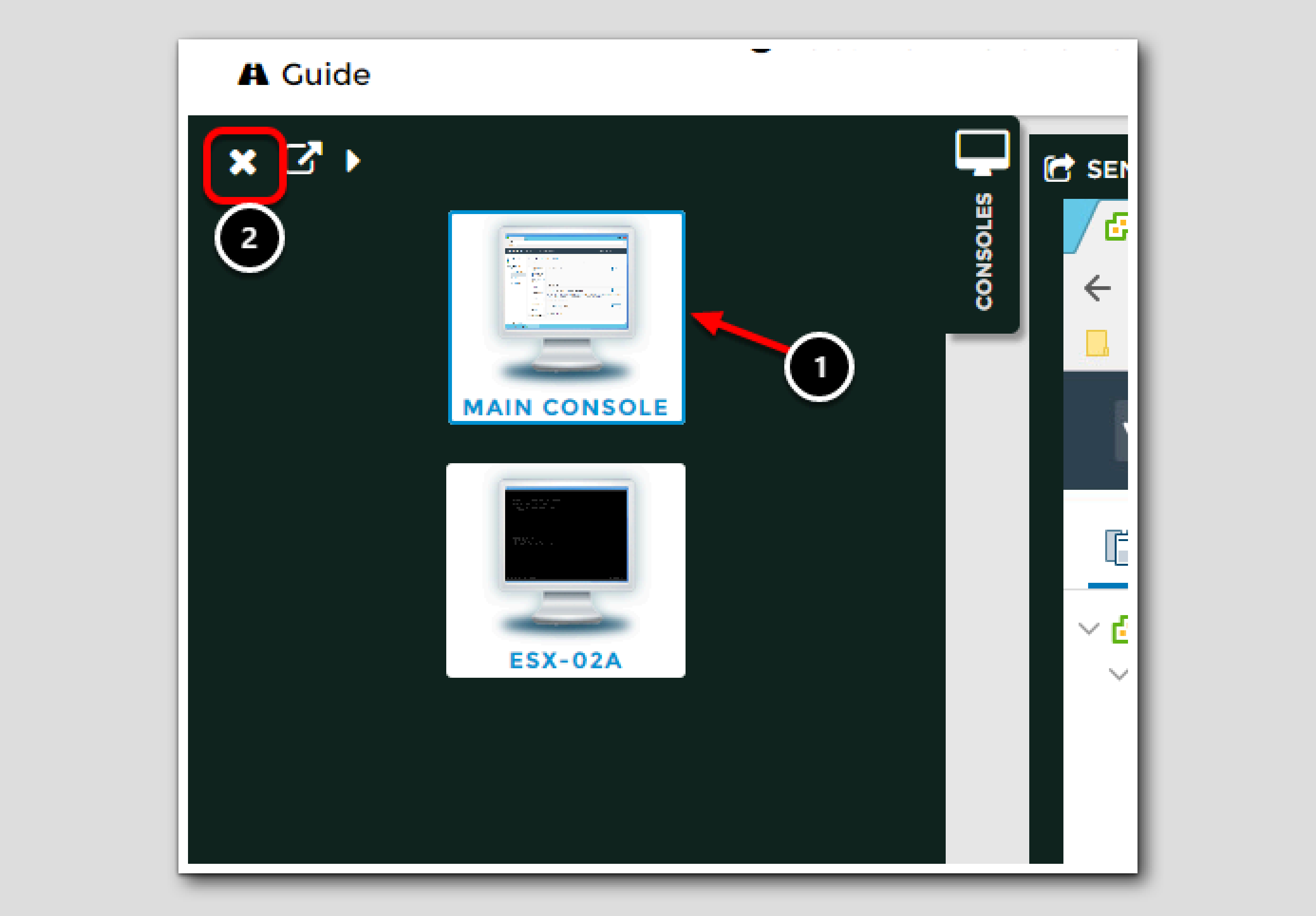
Direct console access has been disabled by the
administrator for esx-02a.corp.local.

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.

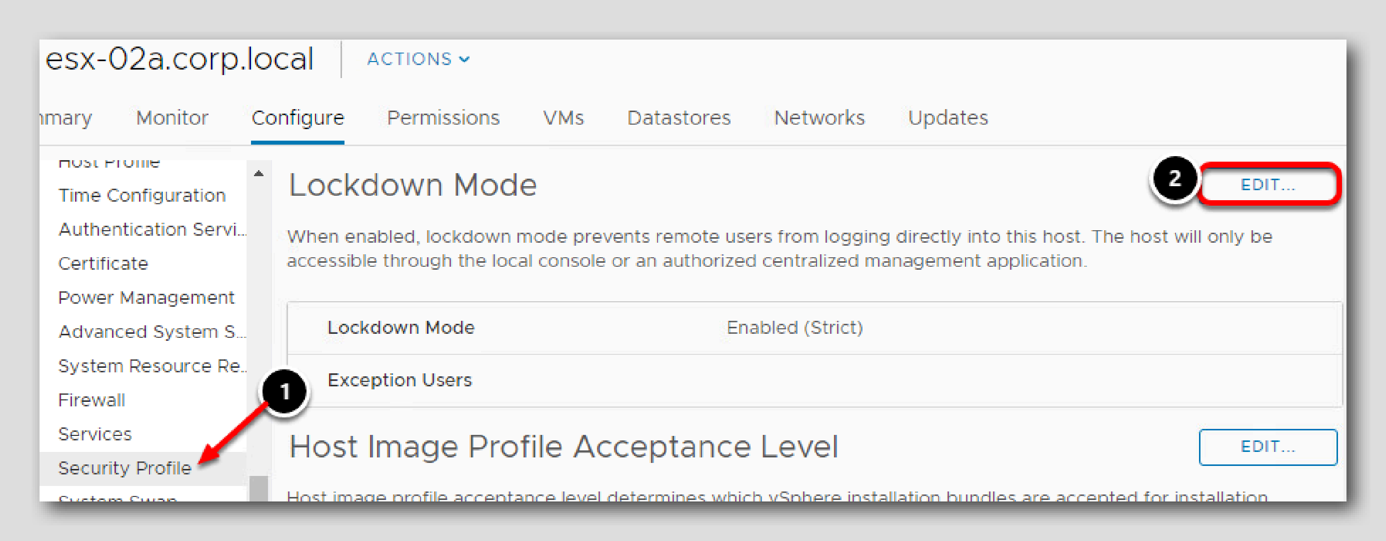
2. Press the Enter key to dismiss the message.

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



Lockdown Mode

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

Lockdown Mode	Enabled (Strict)
Exception Users	

Host Image Profile Acceptance Level

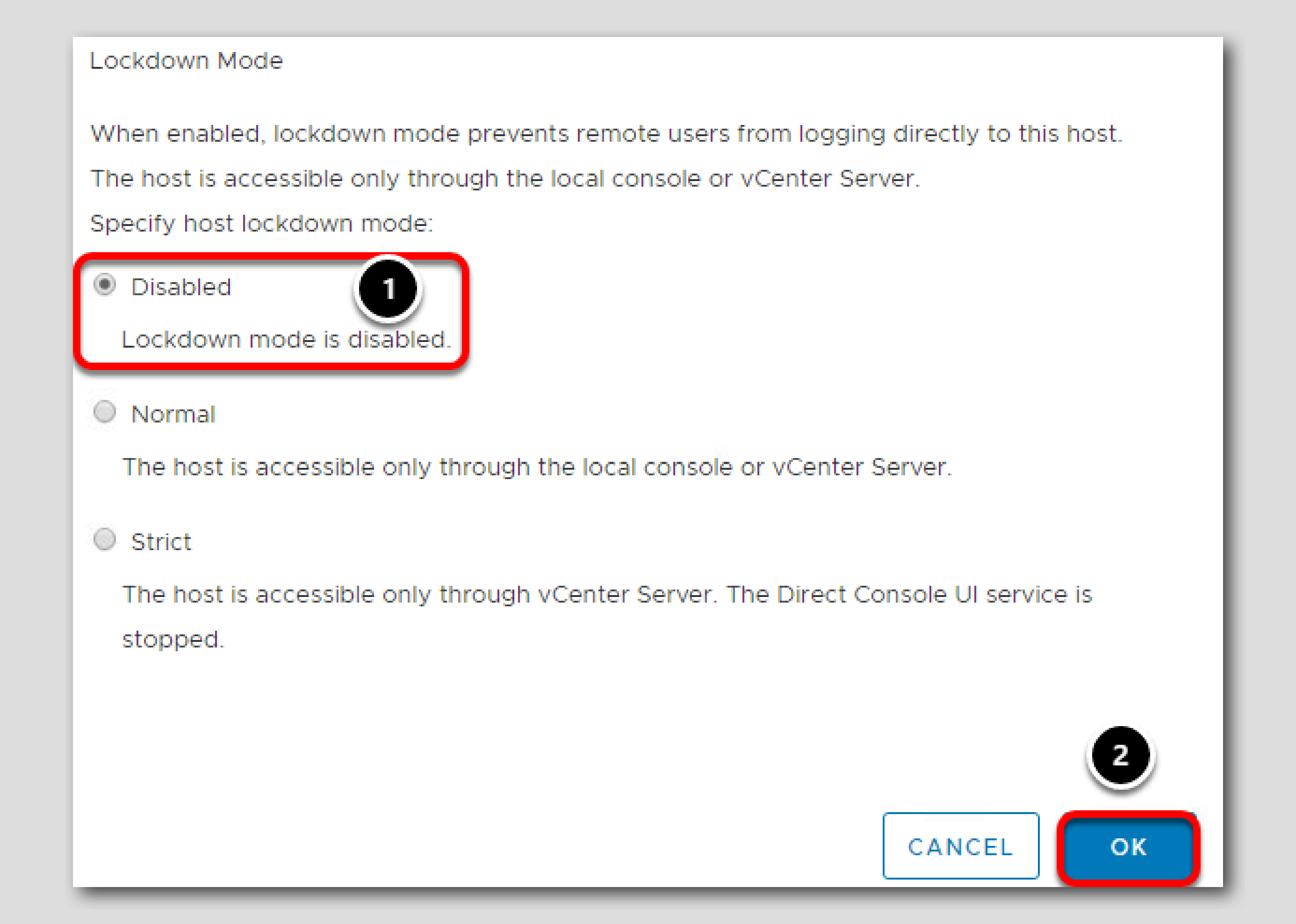
Host image profile acceptance level determines which vSphere installation bundles are accepted for installation

Go back to the vSphere Client.

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

Lockdown Mode

[387]



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.

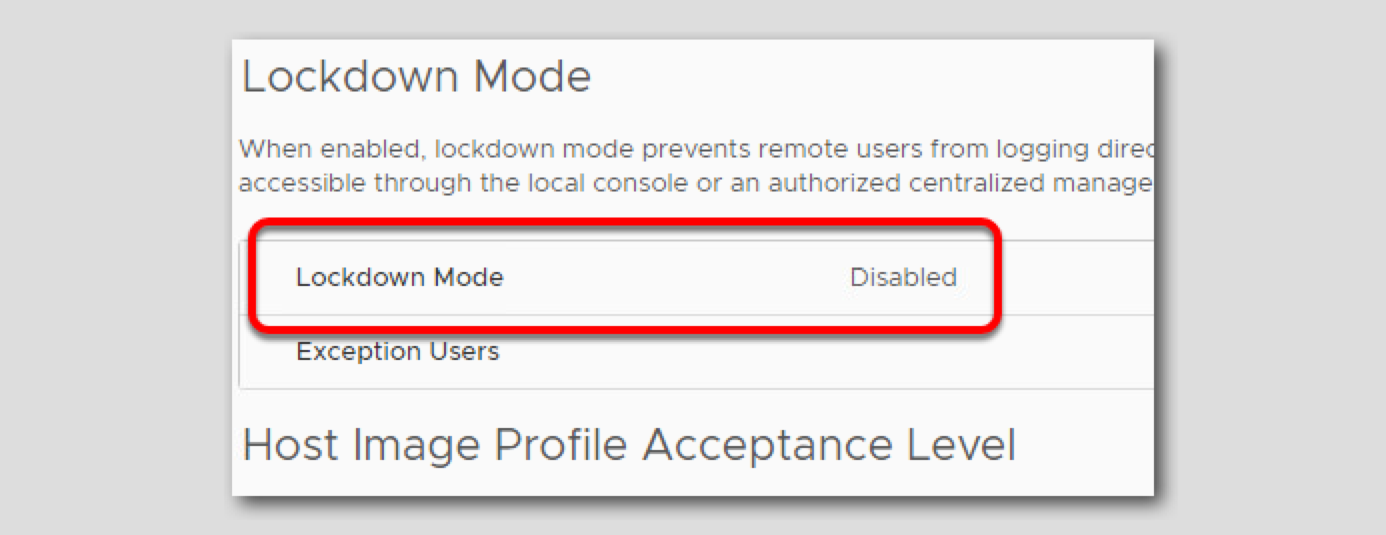
○ Strict

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

[388]



Lockdown Mode

When enabled, lockdown mode prevents remote users from logging direc
accessible through the local console or an authorized centralized manage

Lockdown Mode Disabled

Exception Users

Host Image Profile Acceptance Level

Lockdown Mode for the host should now be disabled.

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

Configuring the Host Services and Firewall

[389]

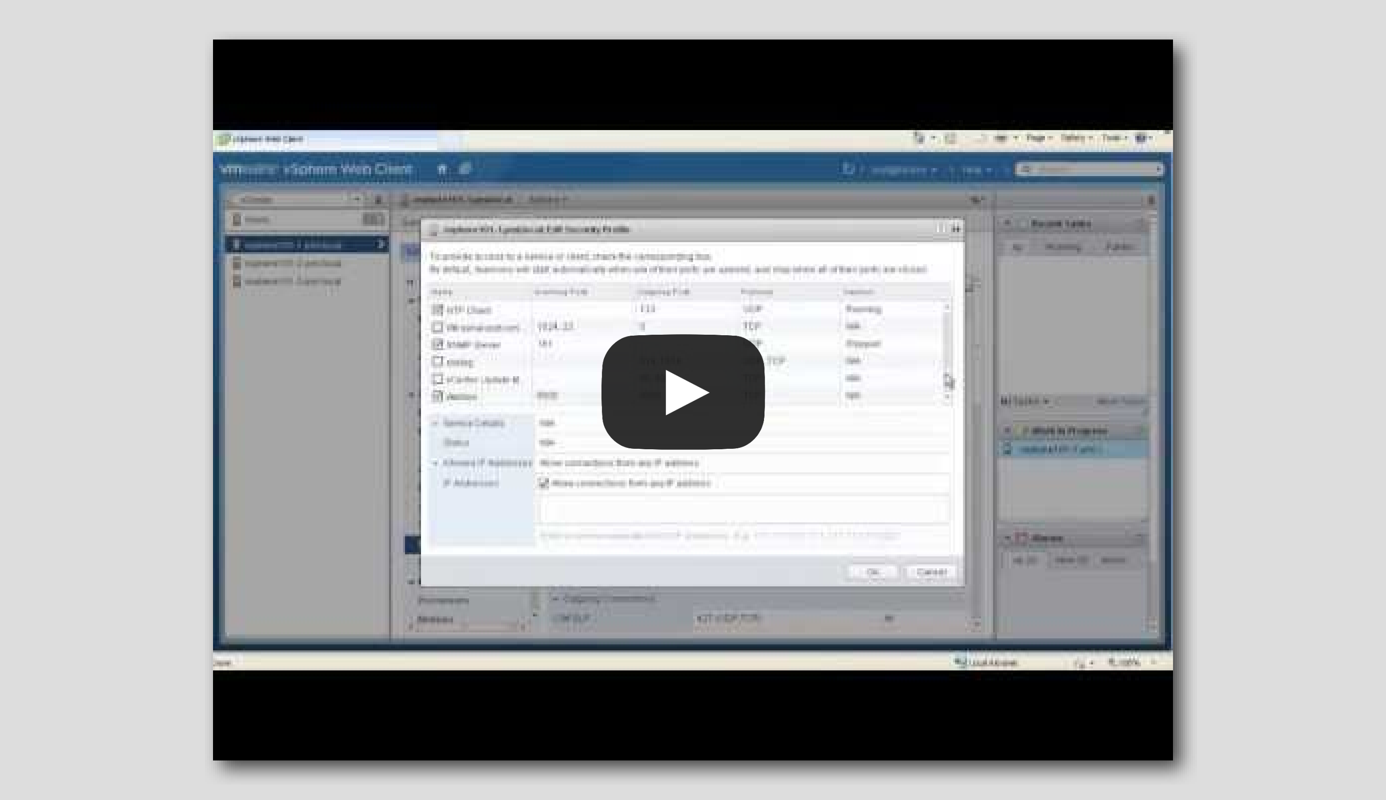
This lesson includes a short video on how to use the VMware ESXi firewall.

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

[390]

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

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



User Access and Authentication Roles [391]

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

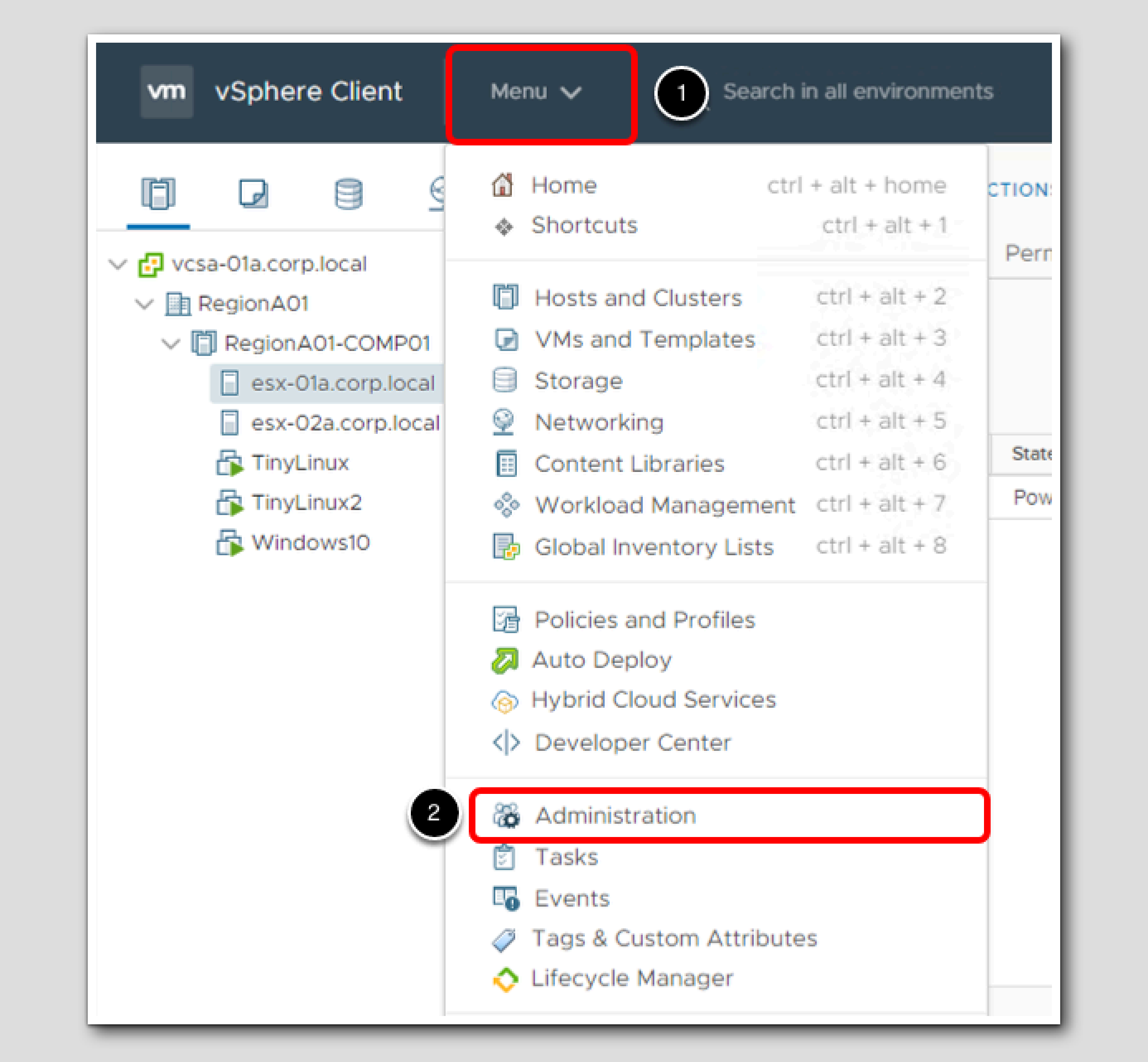
Linked Mode connects multiple vCenter Server systems together by using one or more Platform Services Controllers. It lets you view and search across all linked vCenter Servers and replicate roles, permissions, licenses, policies and tags.

Create a Role in the vSphere Client [392]

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

Administration

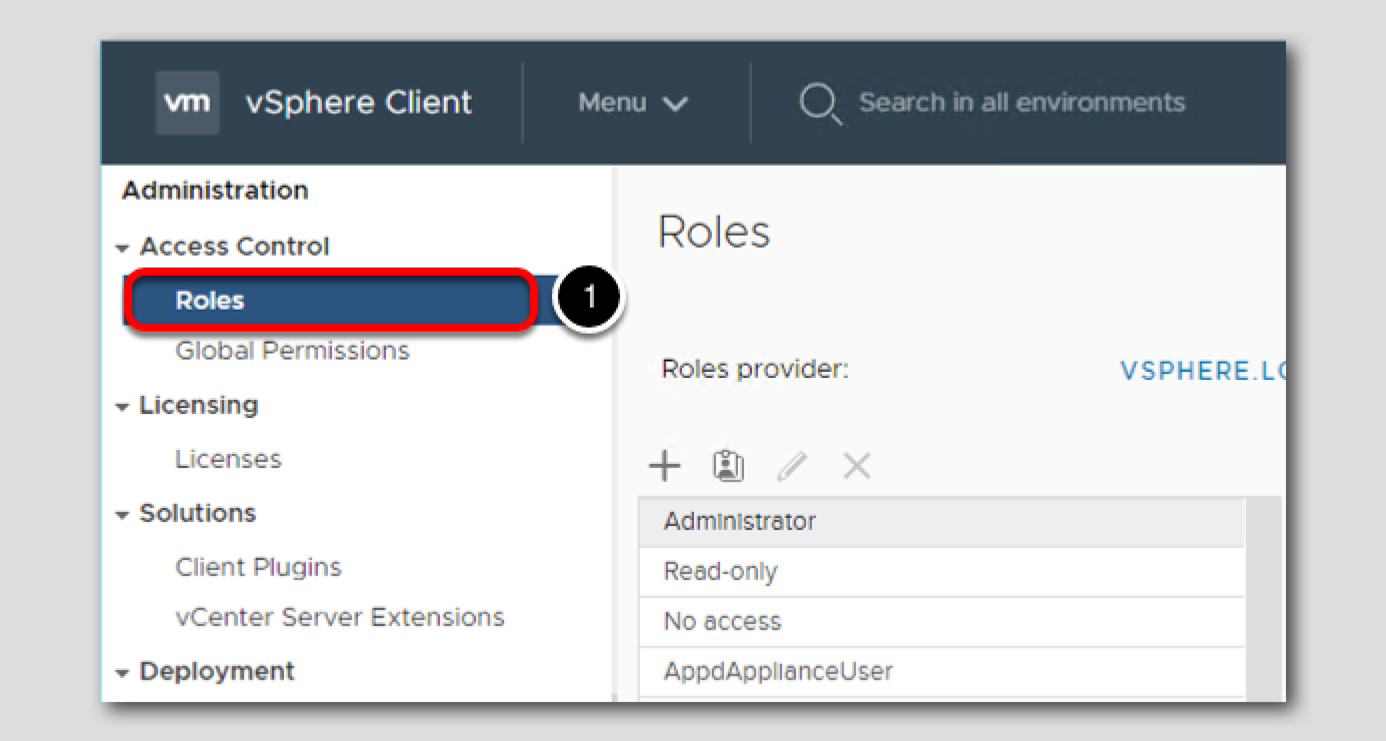
[393]



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

Roles

[394]



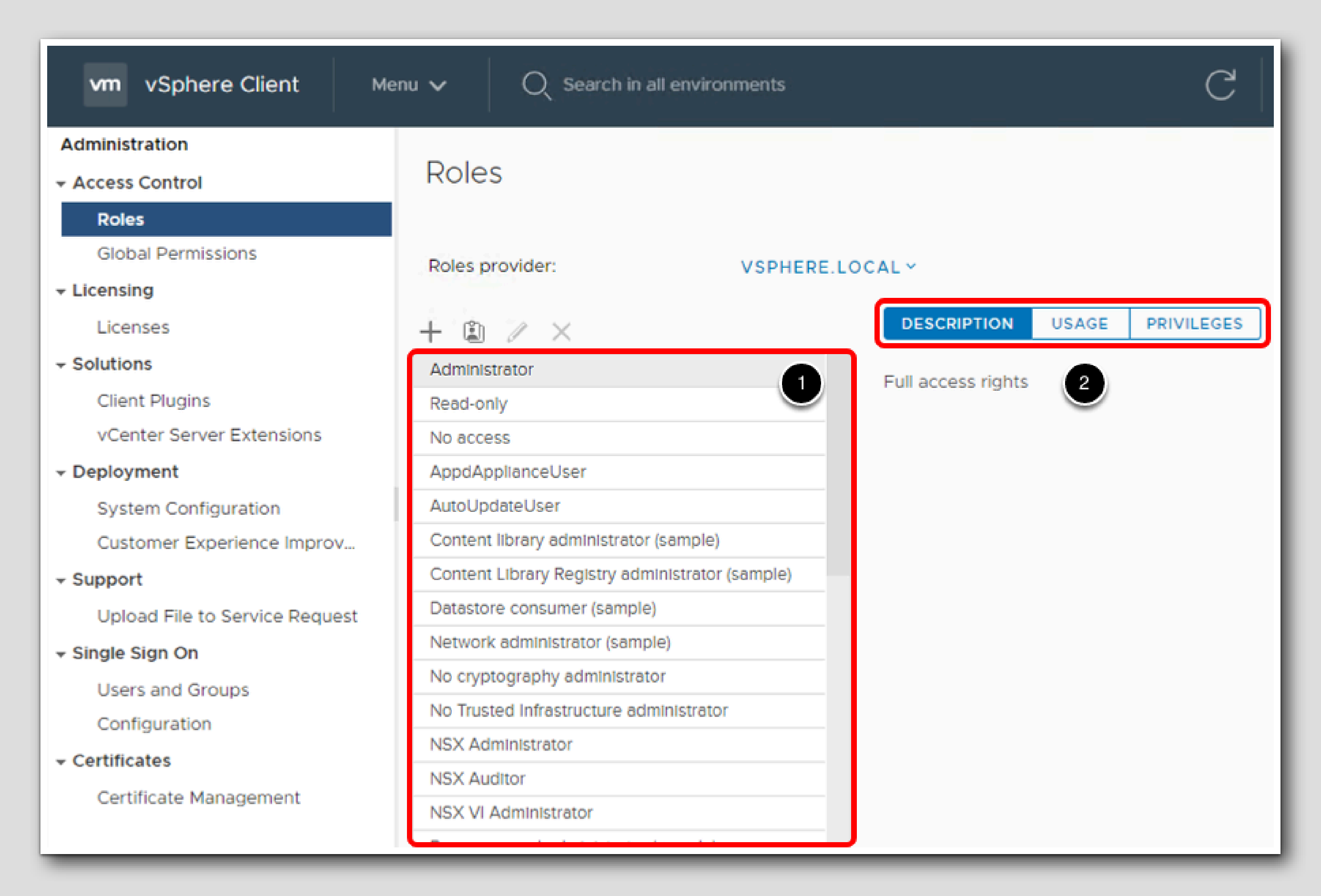
Roles

Roles provider: VSPHERE.LC

Administrator
Read-only
No access
AppdApplianceUser

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

Roles Overview



Roles provider: VSPHERE.LOCAL

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

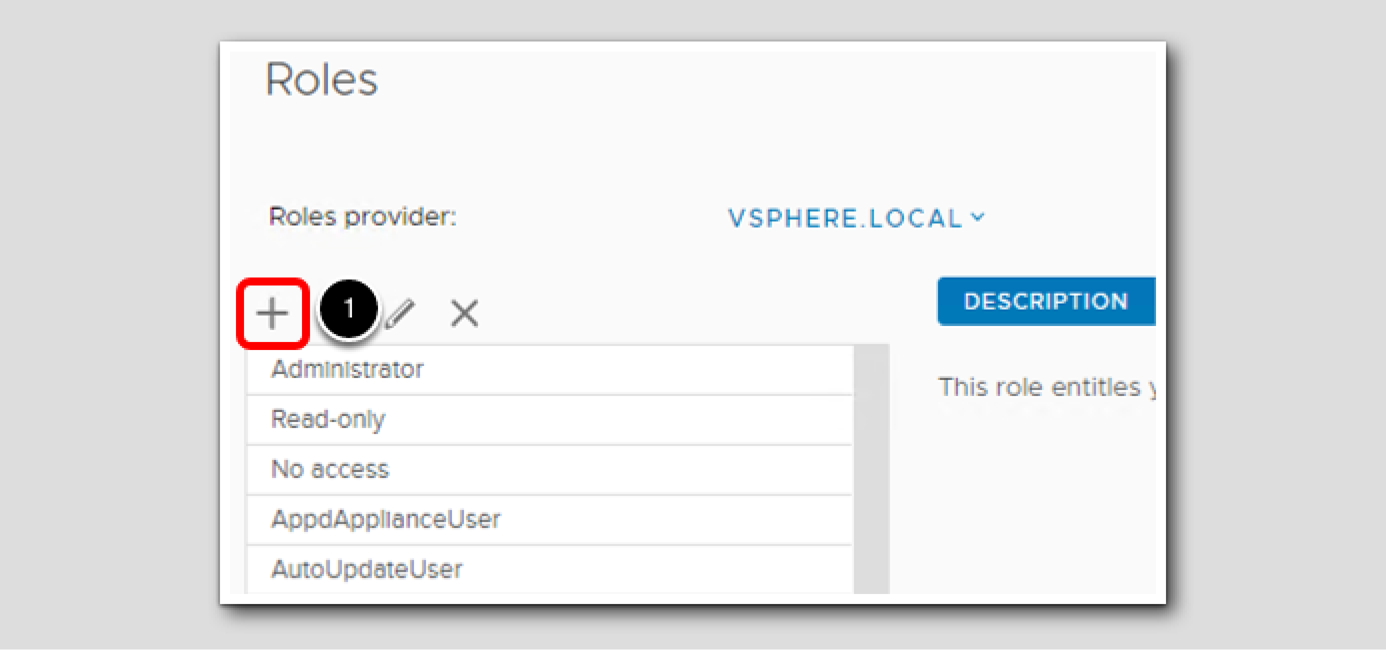
Full access rights

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

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

Add a Role

[396]


Roles

Roles provider:

VSPHERE.LOCAL

Administrator

Read-only

No access

AppdApplianceUser

AutoUpdateUser

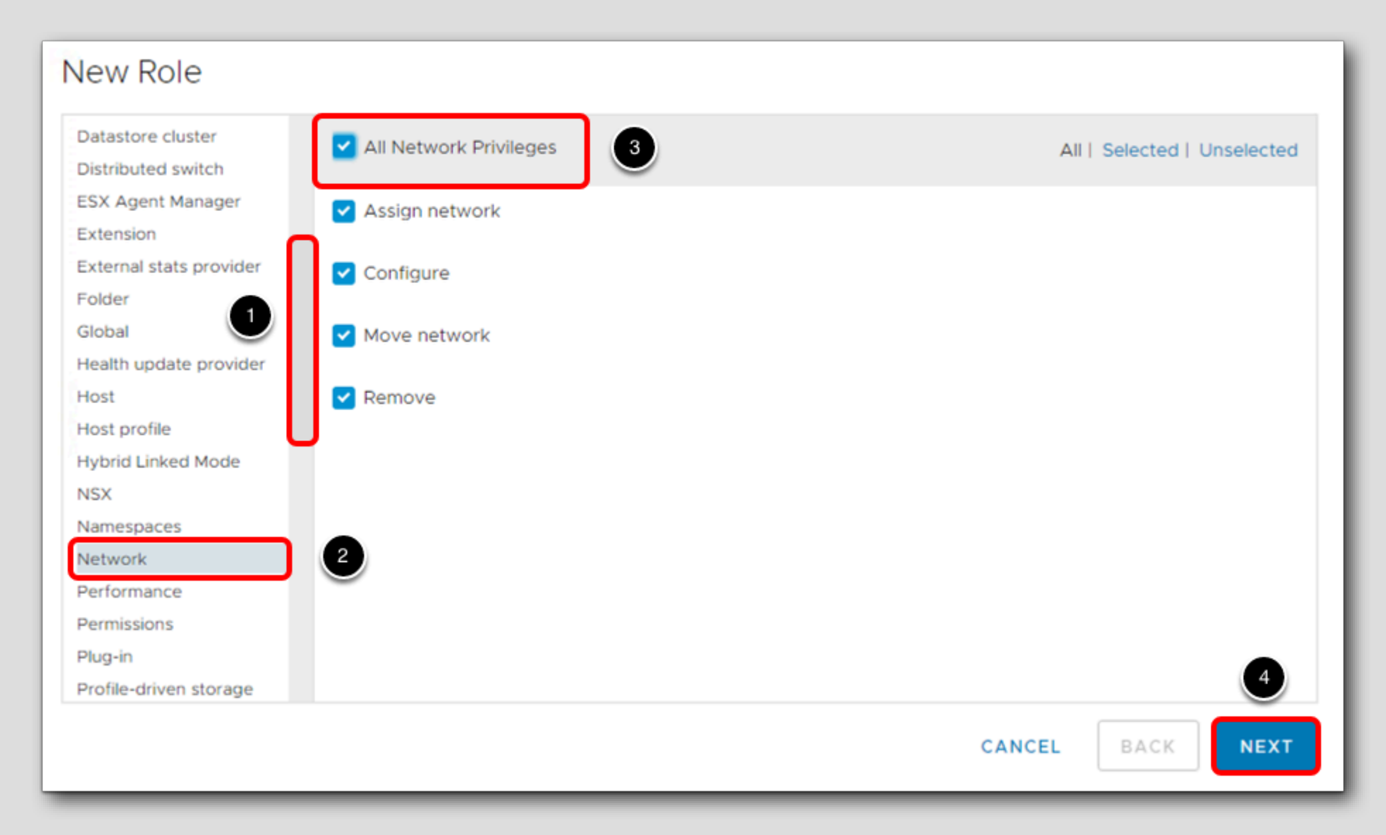
This role entitles y

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

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

New Role

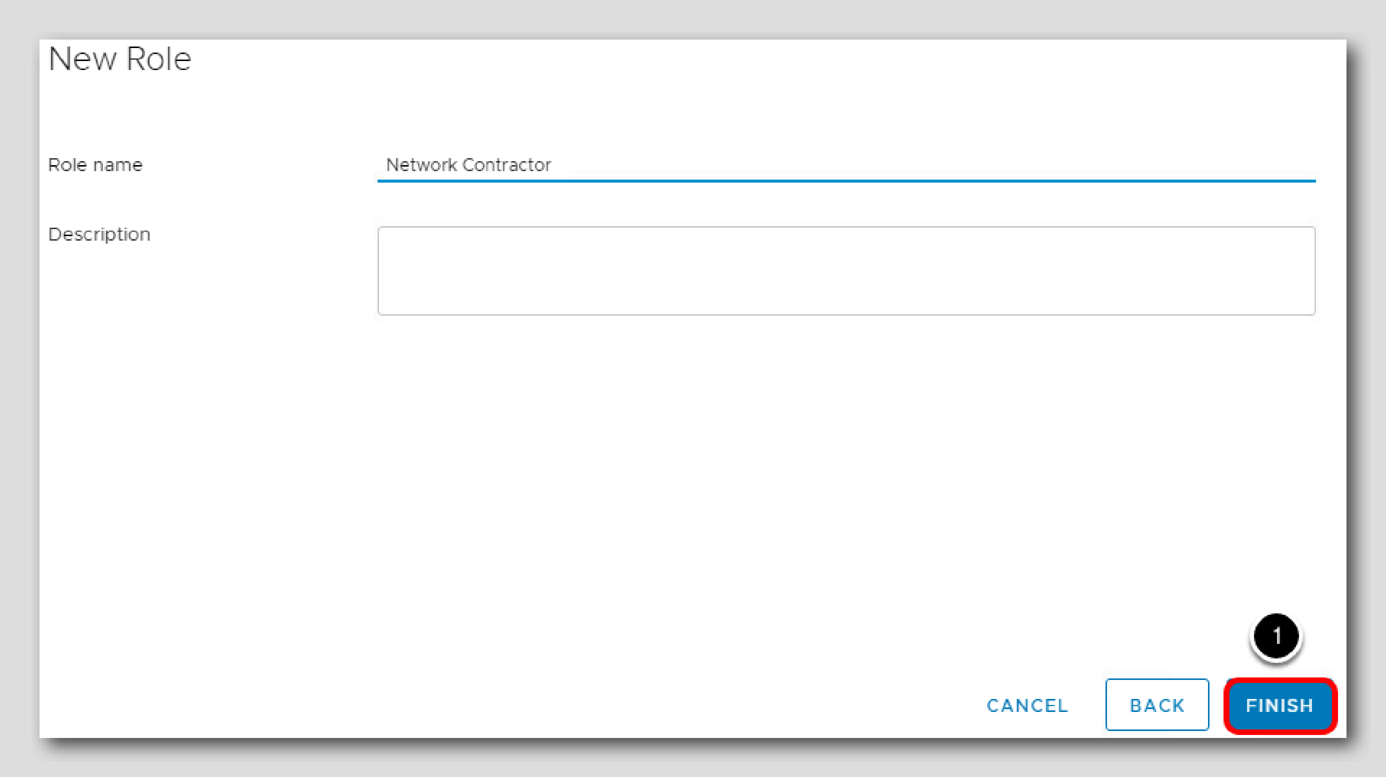
[397]



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

[398]



New Role

Role name: Network Contractor

Description:

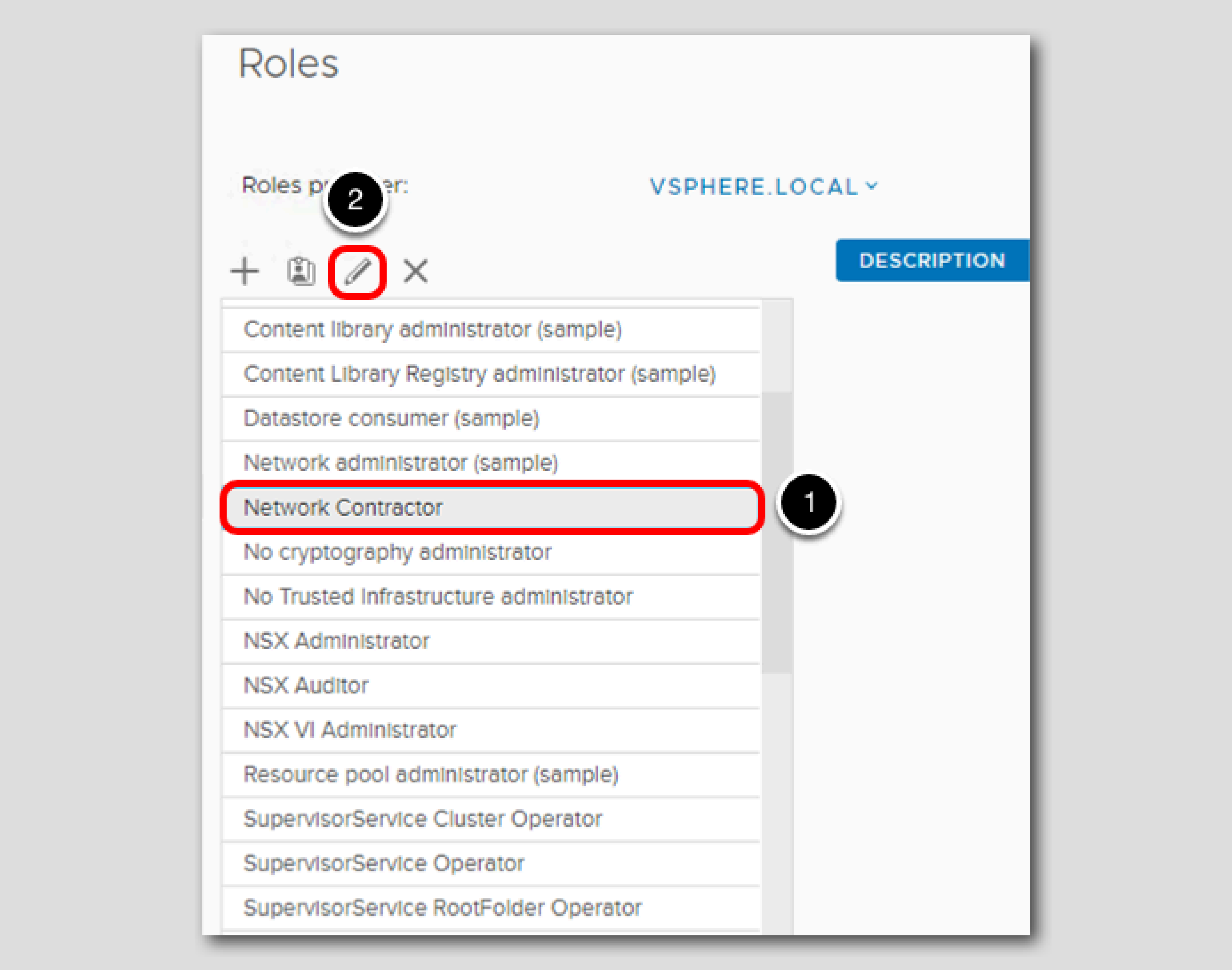
1. Name the role **Network Contractor**
2. Click the **Finish** button to create the new role

Edit a Role in the vSphere Client

[399]

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



Roles

Roles pr[2]er: VSPHERE.LOCAL

DESCRIPTION

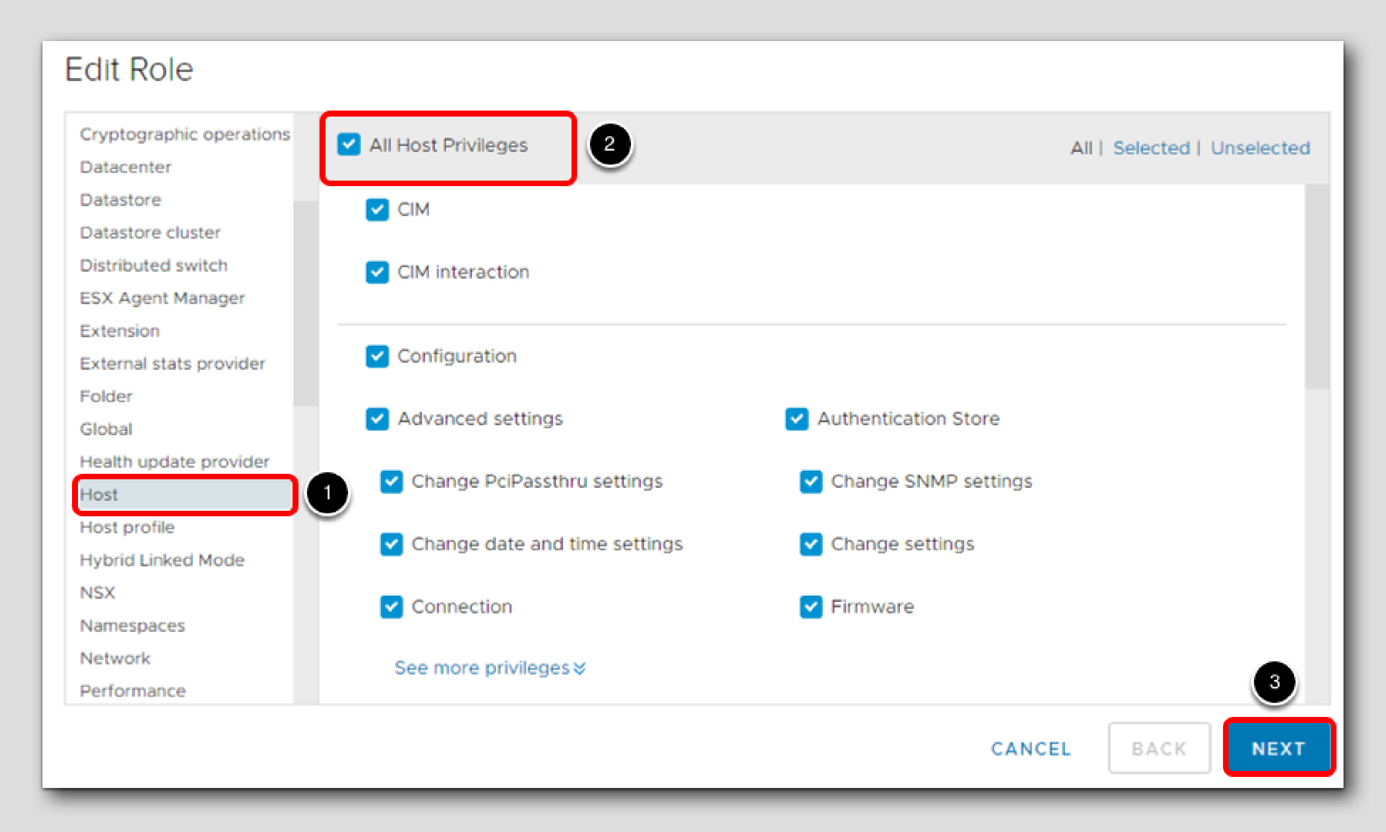
- Content library administrator (sample)
- Content Library Registry administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- Network Contractor
- No cryptography administrator
- No Trusted Infrastructure administrator
- NSX Administrator
- NSX Auditor
- NSX VI Administrator
- Resource pool administrator (sample)
- SupervisorService Cluster Operator
- SupervisorService Operator
- SupervisorService RootFolder Operator

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

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

Add Permissions

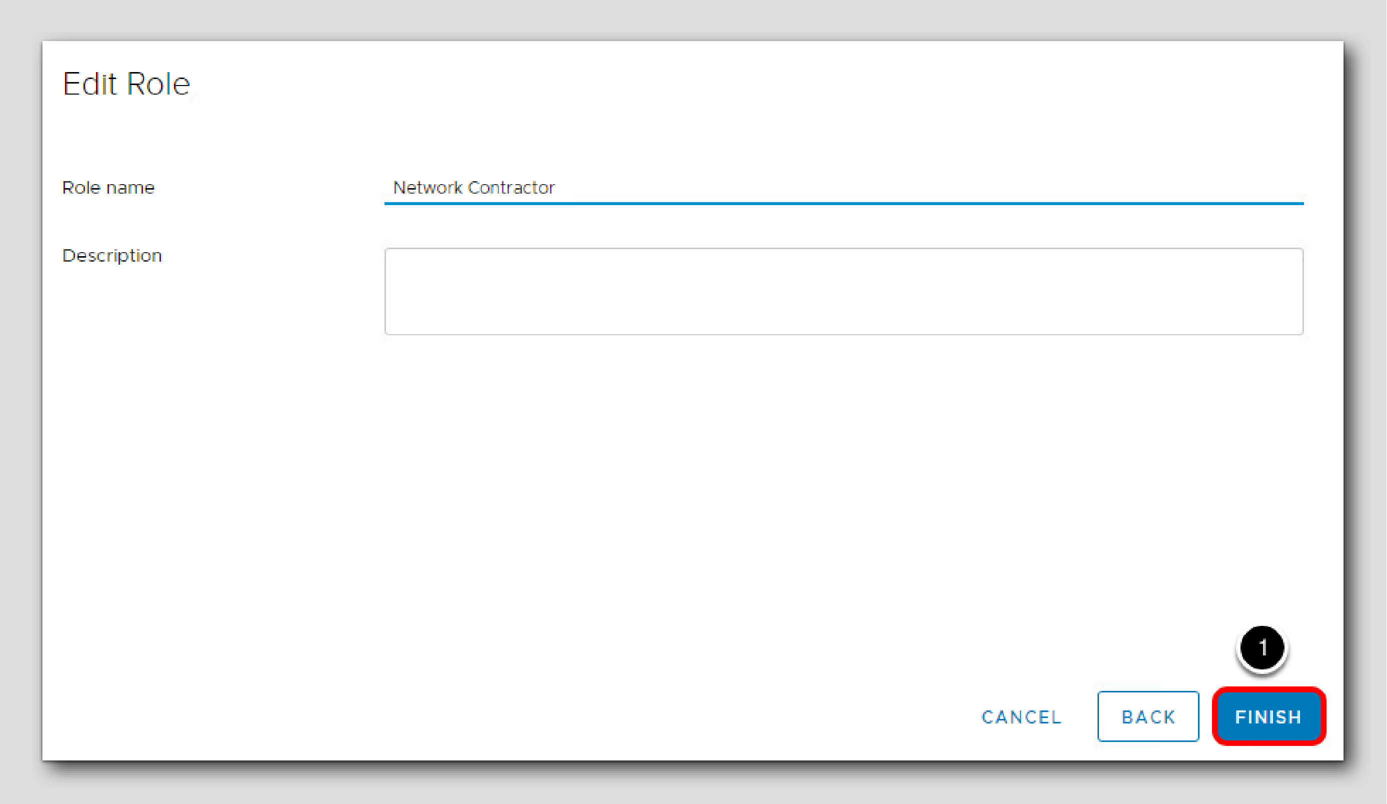
[401]



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

Edit Role

[402]



Edit Role

Role name: Network Contractor

Description:

We will keep the same Role name.

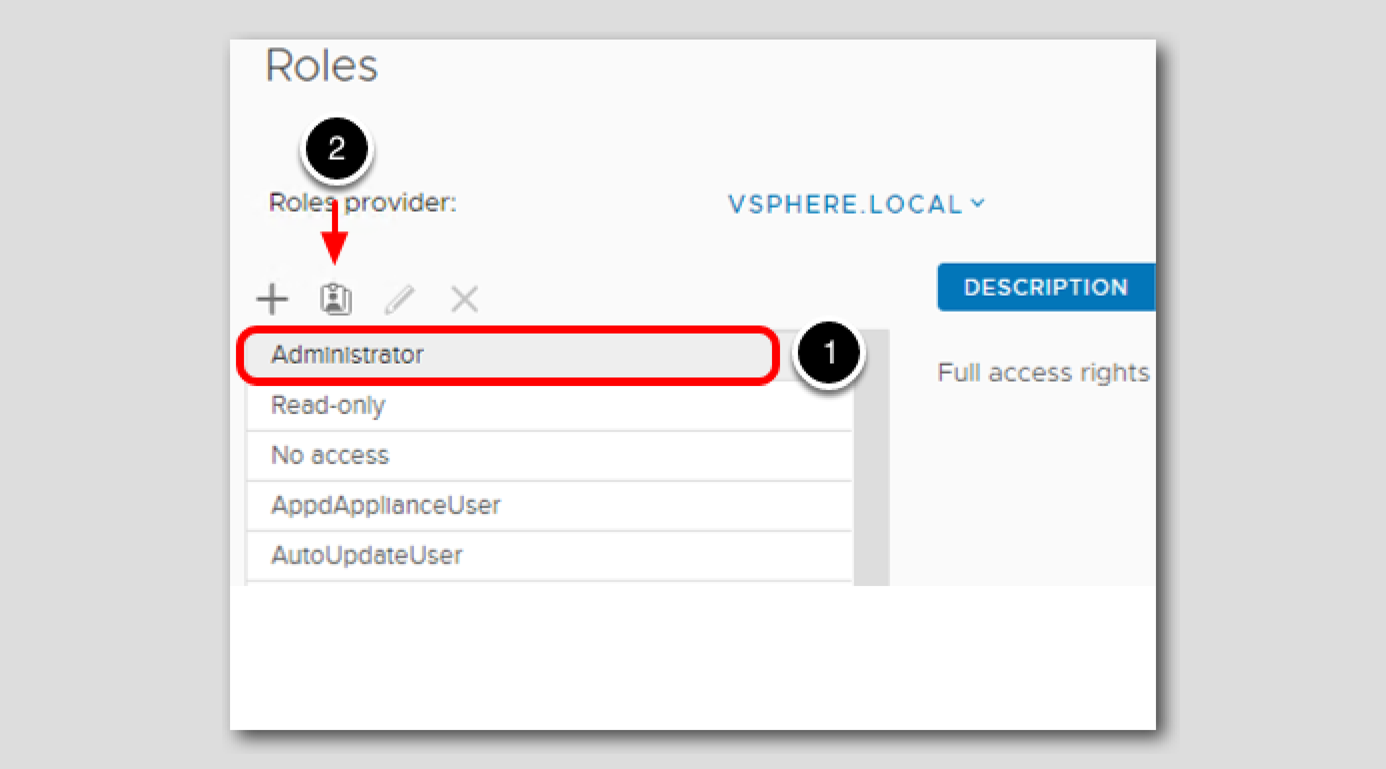
1. Click Finish.

Clone a Role in the vSphere Client

[403]

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



Roles

Roles provider: VSPHERE.LOCAL

DESCRIPTION

Administrator

Read-only

No access

AppdApplianceUser

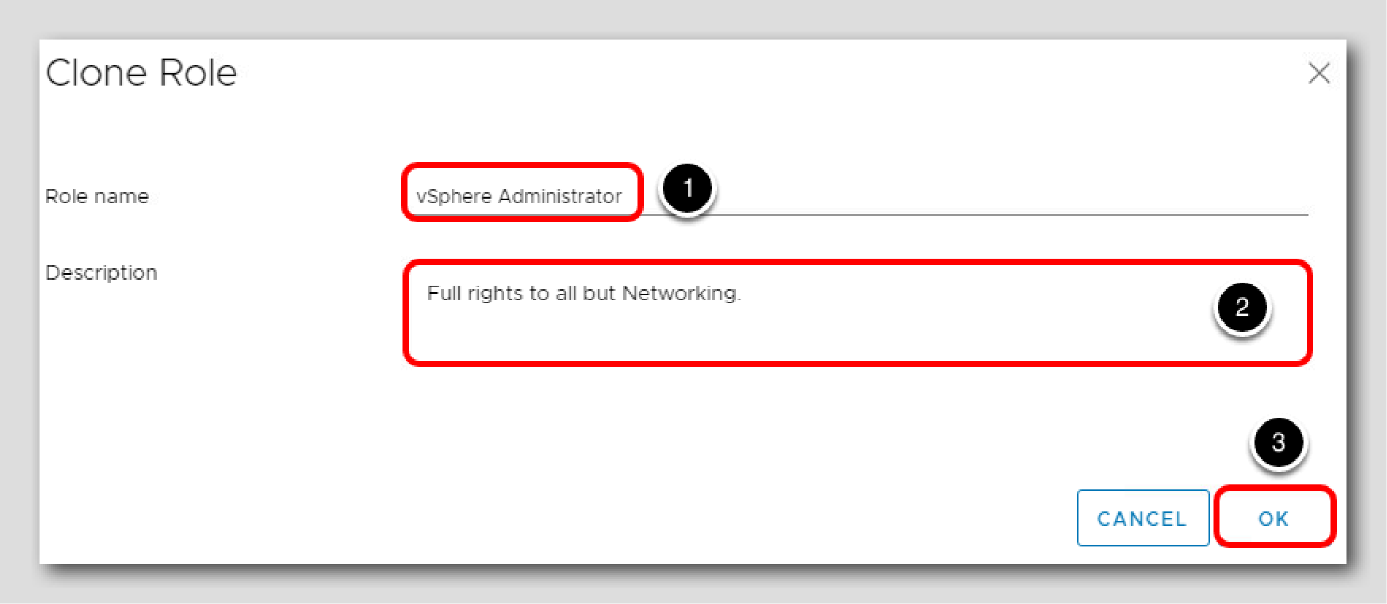
AutoUpdateUser

Full access rights

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

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

Clone Role



Clone Role

Role name vSphere Administrator

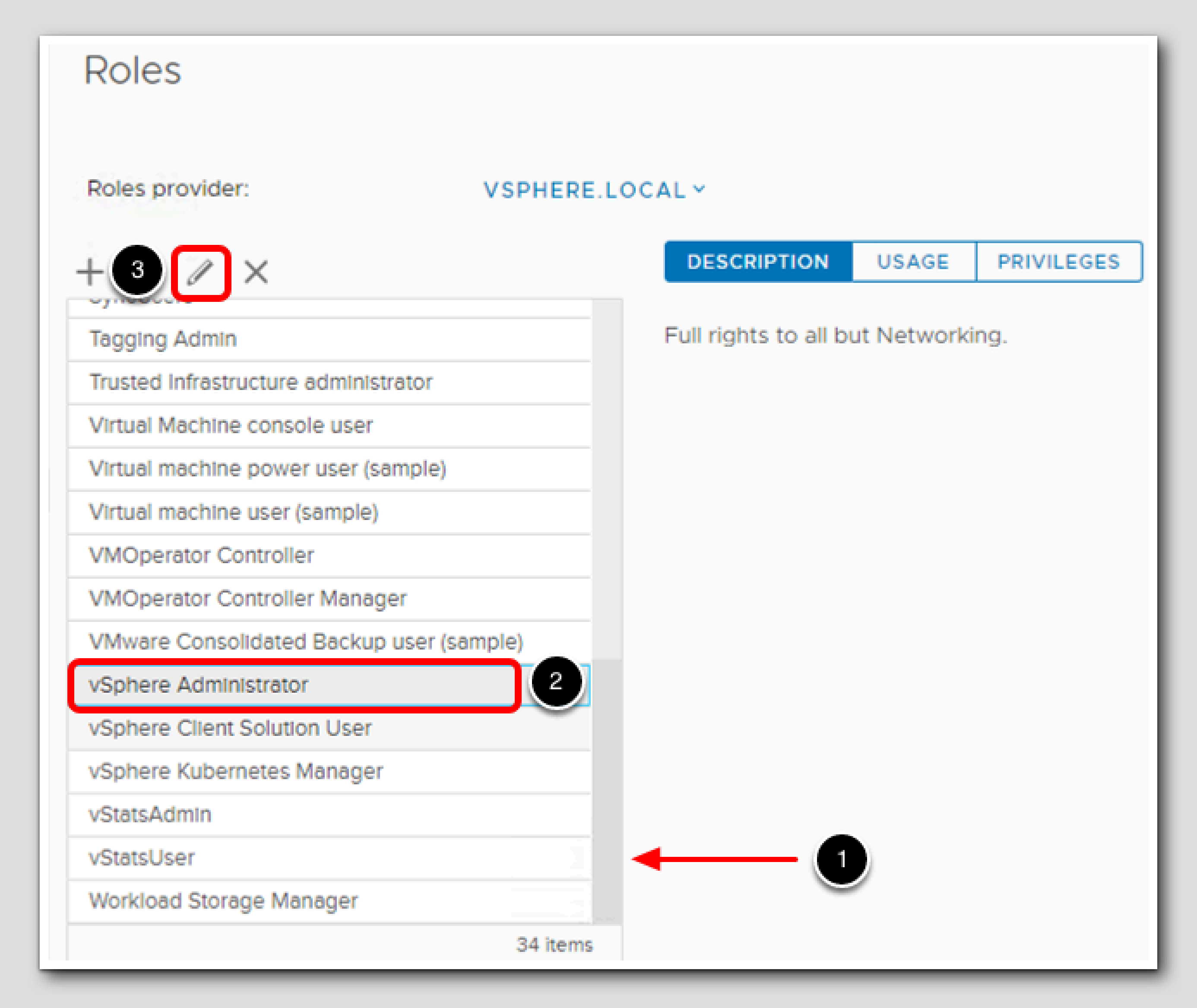
Description Full rights to all but Networking.

As an example, a new vSphere Amin 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

[406]



Roles

Roles provider: VSPHERE.LOCAL

Tagging Admin
Trusted Infrastructure administrator
Virtual Machine console user
Virtual machine power user (sample)
Virtual machine user (sample)
VMOperator Controller
VMOperator Controller Manager
VMware Consolidated Backup user (sample)
vSphere Administrator
vSphere Client Solution User
vSphere Kubernetes Manager
vStatsAdmin
vStatsUser
Workload Storage Manager

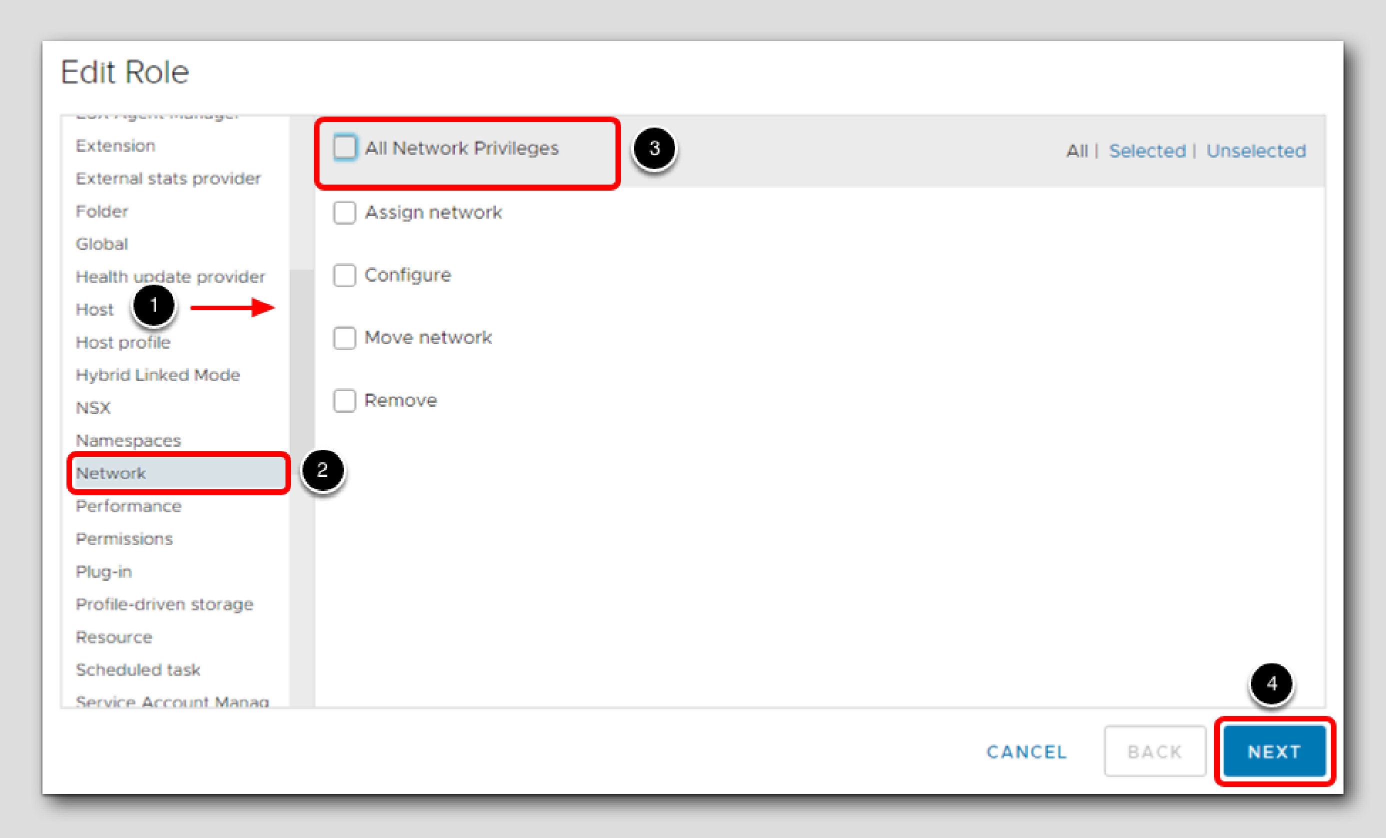
34 items

Full rights to all but Networking.

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

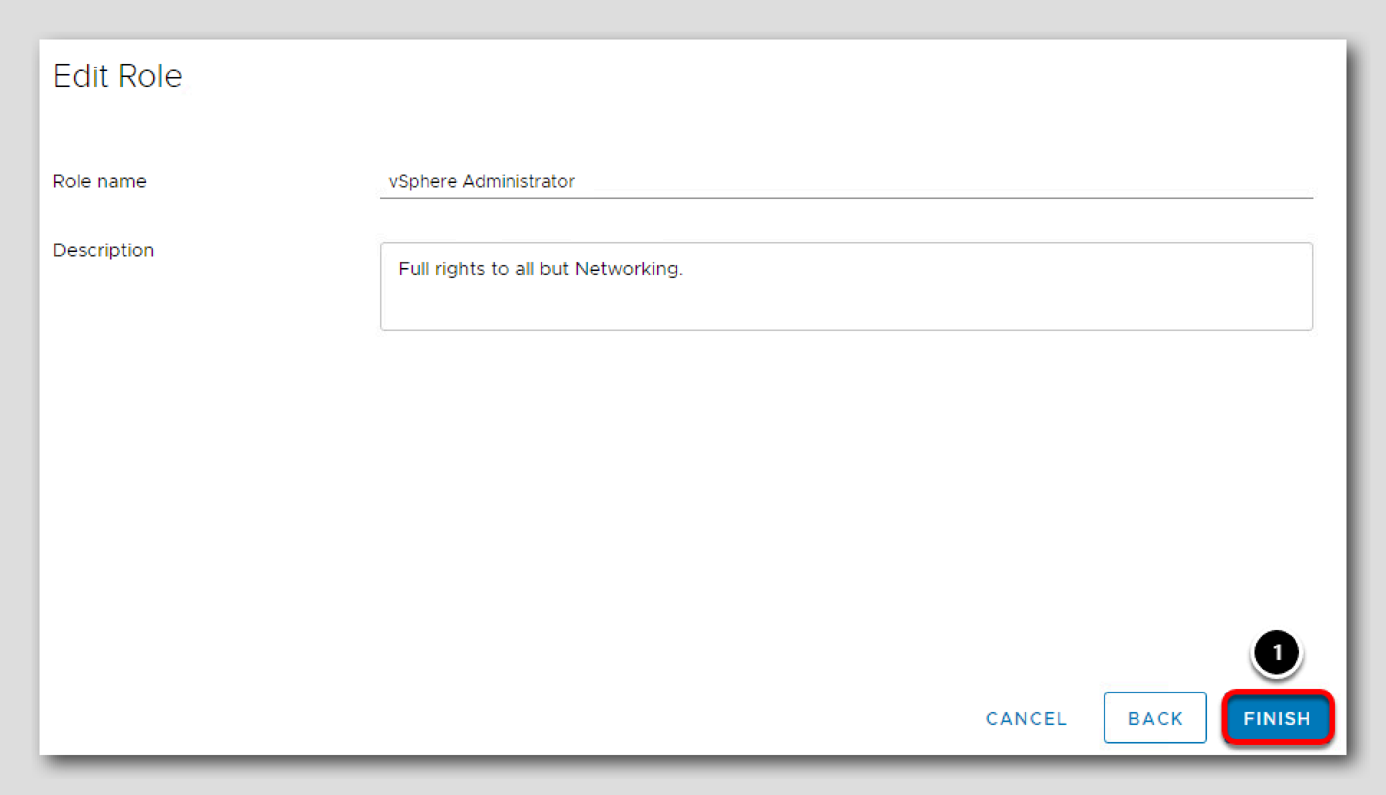
[407]



1. Scroll down until you see **Network**
2. Click on **Network**
3. Untick **All Network Privileges**
4. Click **Next**

Edit Role

[408]



Edit Role

Role name: vSphere Administrator

Description: Full rights to all but Networking.

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

Remove a Role in the vSphere Client

[409]

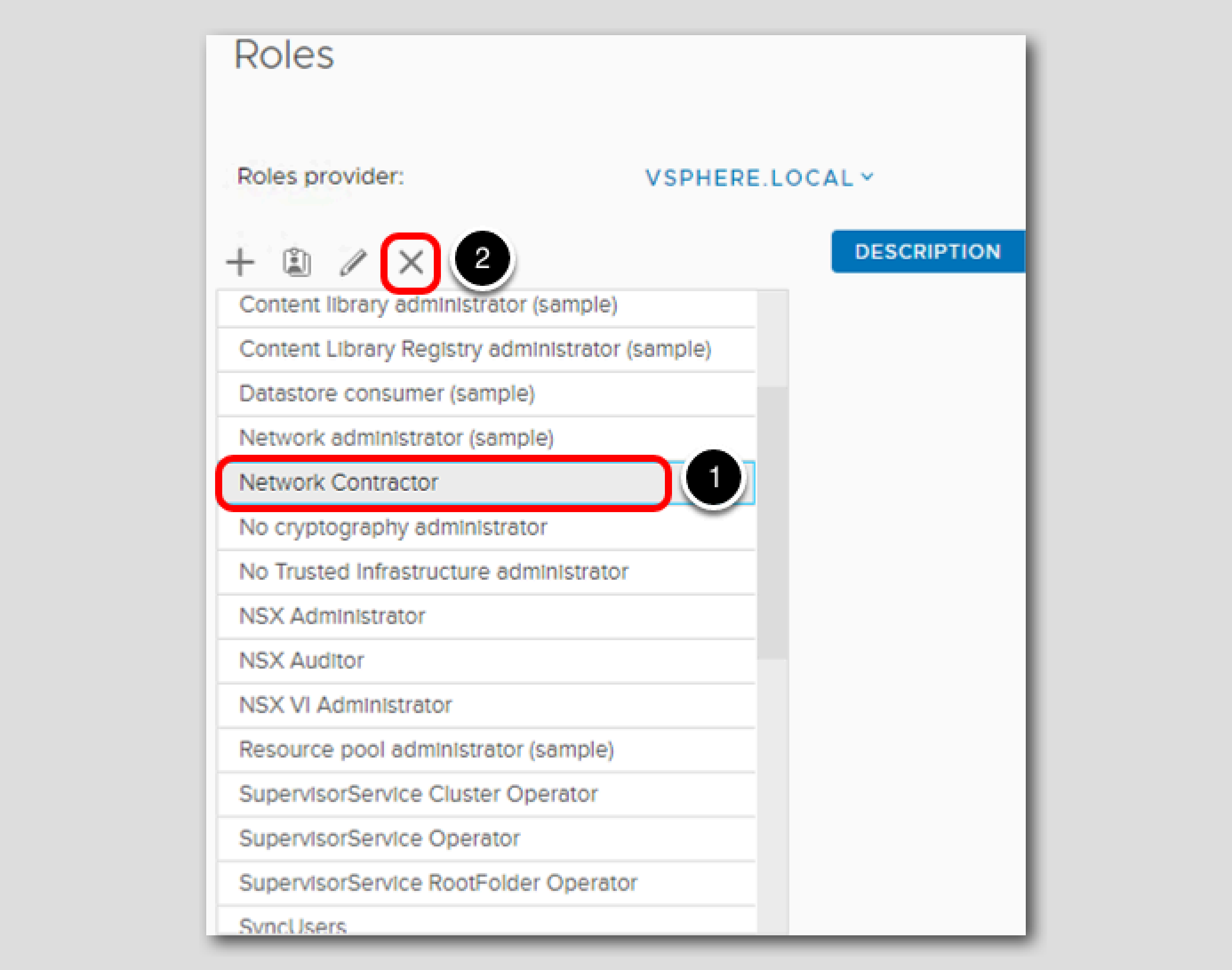
When you remove a role that is not assigned to any users or groups, the definition of the role is removed from the list of roles. When you remove a role that is assigned to a user or group, you can remove assignments or replace them with an assignment to another role.

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

[410]



Content library administrator (sample)

Content Library Registry administrator (sample)

Datastore consumer (sample)

Network administrator (sample)

Network Contractor

No cryptography administrator

No Trusted Infrastructure administrator

NSX Administrator

NSX Auditor

NSX VI Administrator

Resource pool administrator (sample)

SupervisorService Cluster Operator

SupervisorService Operator

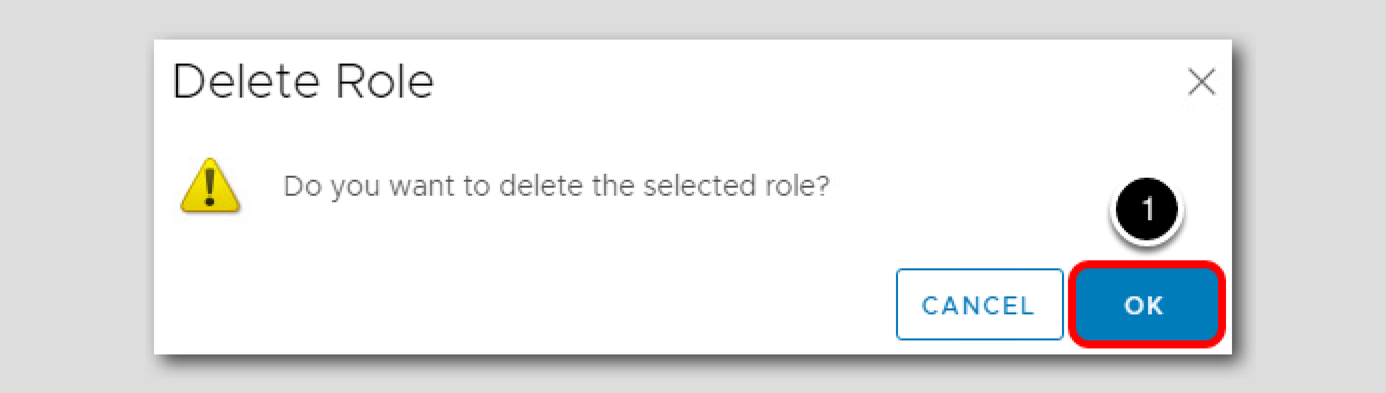
SupervisorService RootFolder Operator

SyncUsers

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

Confirm Deletion

[411]

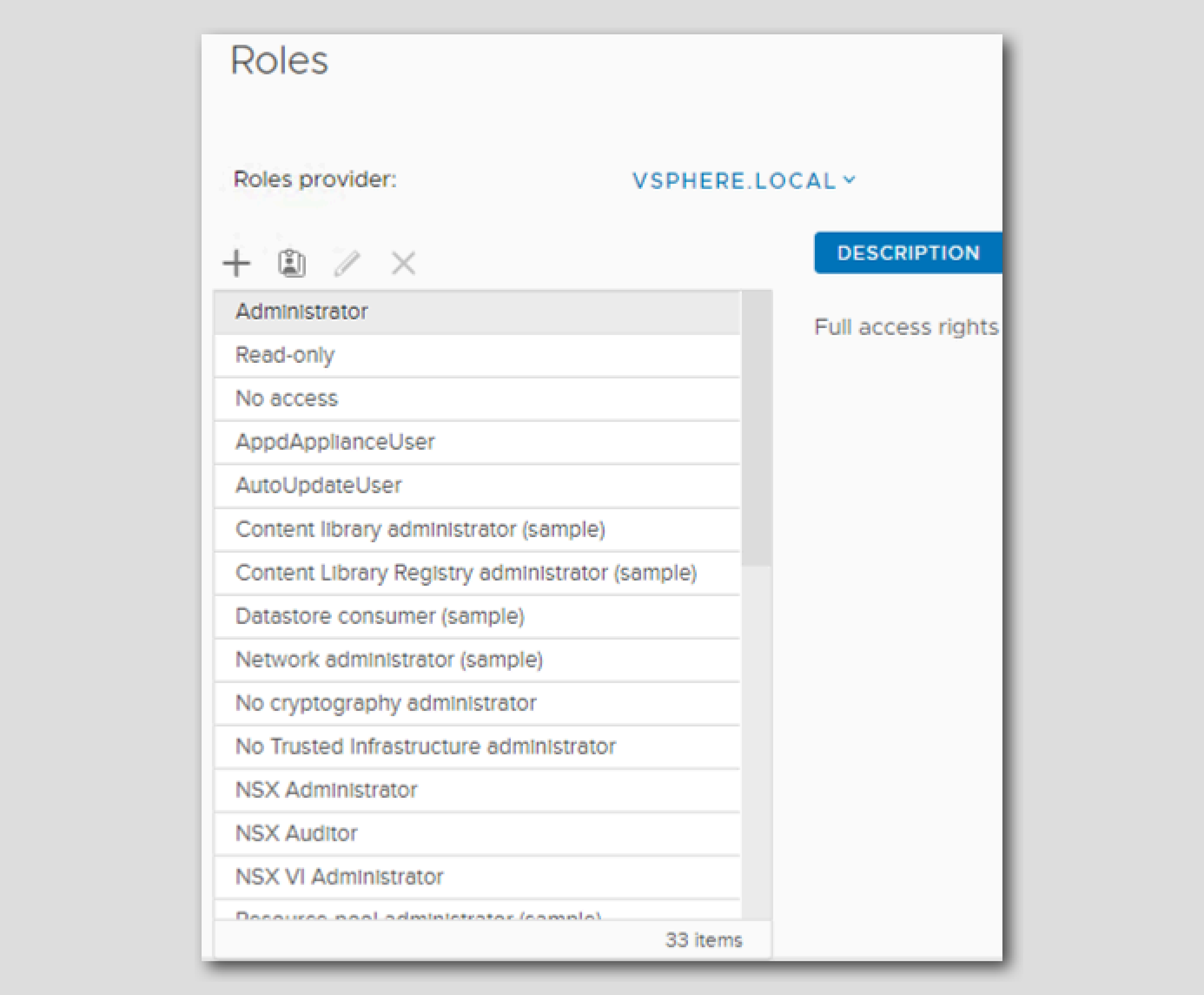


Delete Role

Do you want to delete the selected role?

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

Role Deleted



Roles provider: VSPHERE.LOCAL

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

33 items

Full access rights

We can see that the role named Network Contractor has been deleted.

Creating unique and granular roles for users in your organization enables better security for your vSphere infrastructure.

Understanding Single Sign On

You use vCenter Single Sign-On to authenticate and manage vCenter Server users.

The Single Sign-On administrative interface is part of the vSphere Web Client. To configure Single Sign-On and manage Single Sign-On users and groups, you log in to the vSphere Web Client as a user with Single Sign-On administrator privileges. This might not be the same user as the vCenter Server administrator. Enter the credentials on the vSphere Web Client login page and upon authentication, you can access the Single Sign-On administration tool to create users and assign administrative permissions to other users.

In vSphere versions prior to 5.1, users were authenticated when vCenter Server validated their credentials against an Active Directory domain or the list of local operating system users. As of vSphere 5.1, users authenticate through vCenter Single Sign On. The default Single Sign-On administrator for vSphere 5.1 is admin@System-Domain and administrator@vsphere.local for vSphere 5.5 and higher. The password for this account is the one you specified at installation. These credentials are used to log in to the vSphere Web Client to access the Single Sign-On administration tool. You can then assign Single Sign-On administrator privileges to specific users who are allowed to manage the Single Sign-On server. These users might be different from the users that administer vCenter Server.

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

Single Sign-On Identity Sources

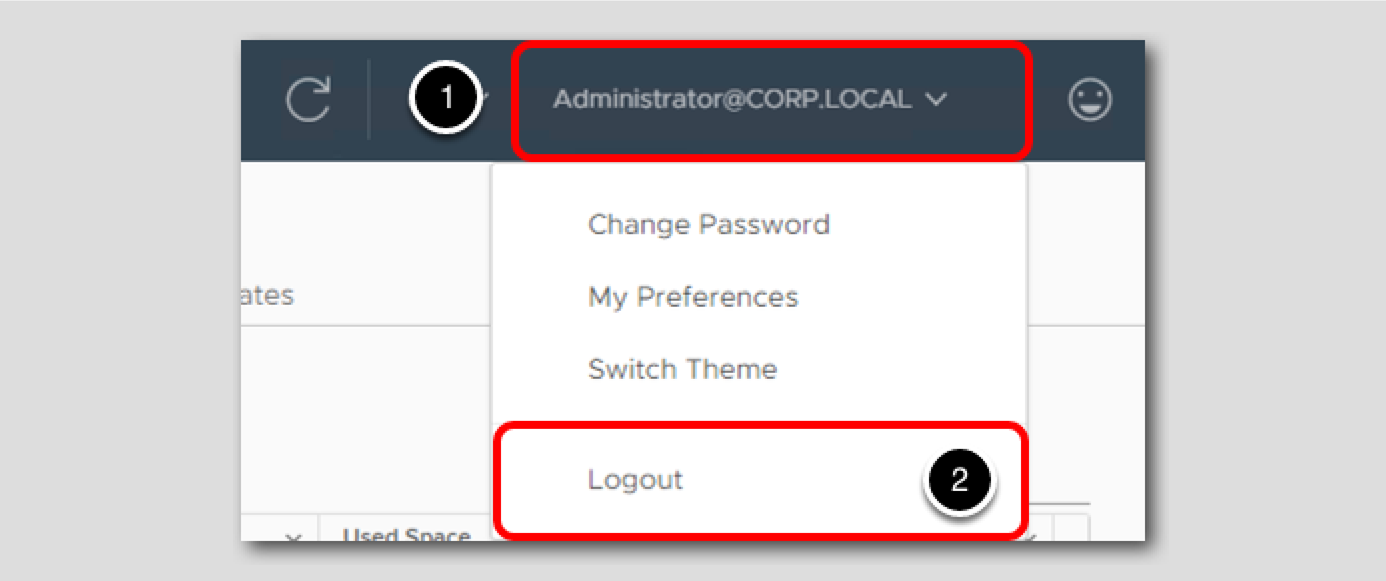
[414]

In most cases, vSphere SSO will be deployed to use an external Identity Source for primary authentication. In this lab environment, SSO has been integrated with Microsoft Active Directory so that users from the corp.local domain can log in to vSphere using their AD credentials.

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

Log out as Administrator@CORP.LOCAL

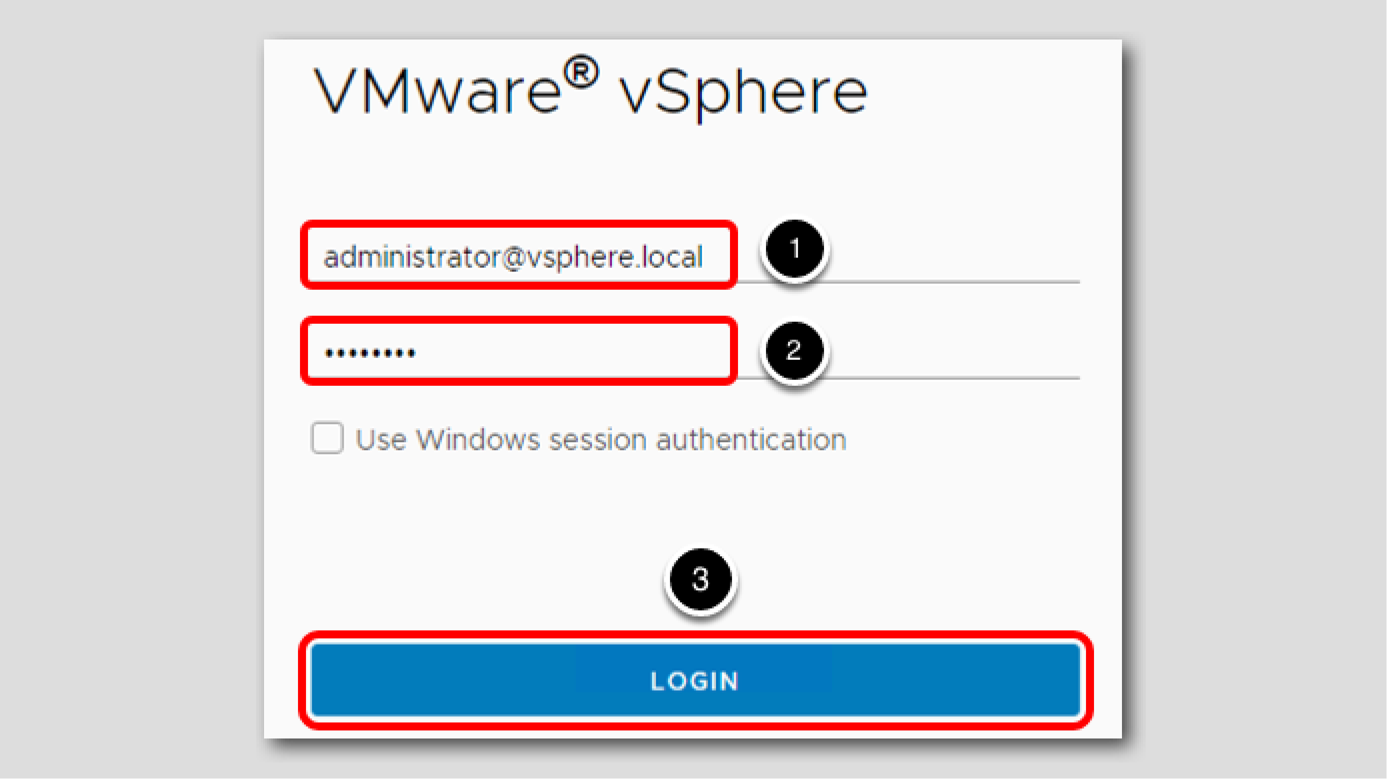
[415]



1. If you are currently logged in to the vSphere Web Client, click on Administrator@CORP.LOCAL
2. Select Logout

Log into vSphere Web Client as SSO Admin

[416]


VMware® vSphere

administrator@vsphere.local

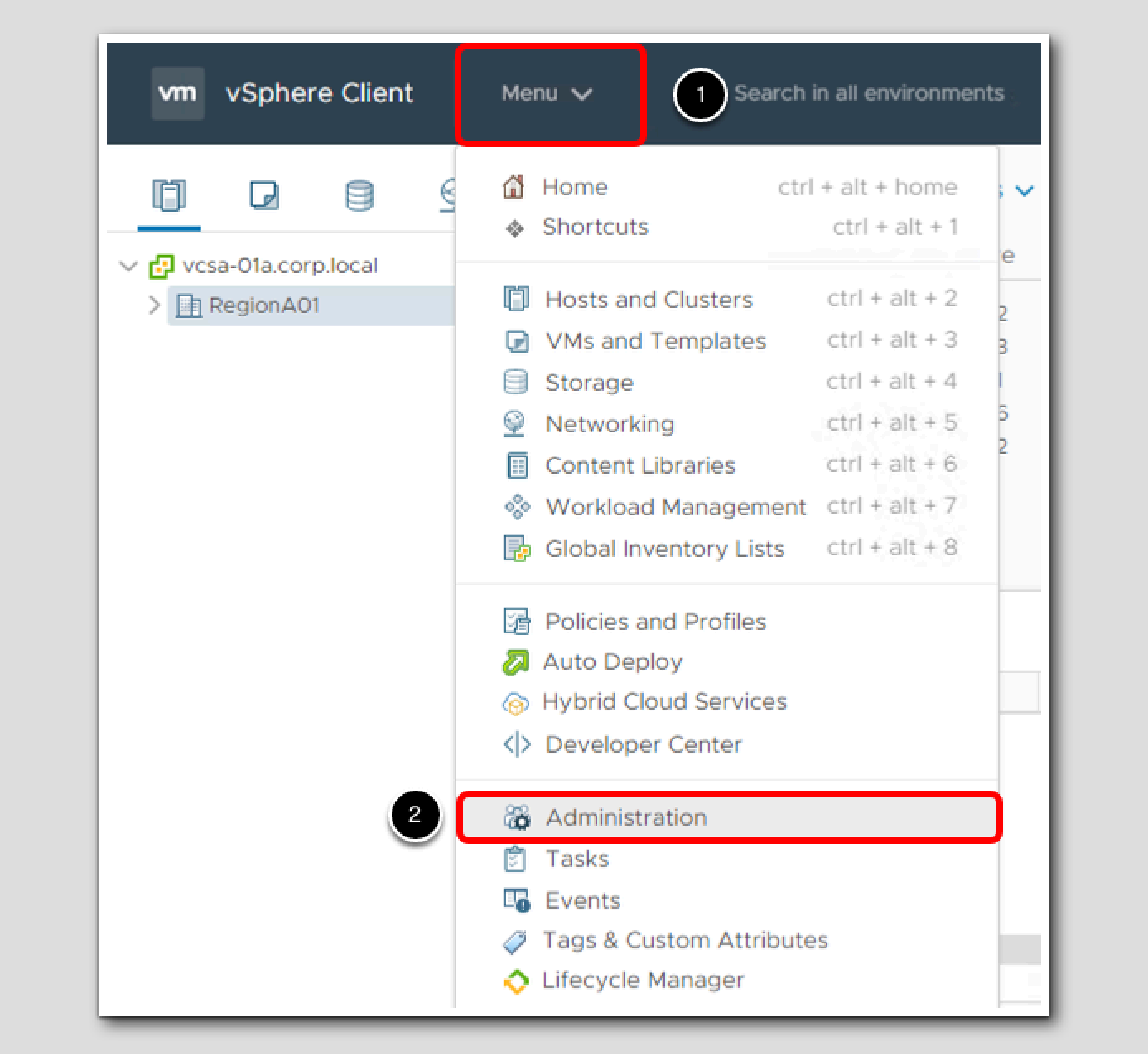
•••••••••

□ Use Windows session authentication

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

1. Username - administrator@vsphere.local
2. Password - VMware1!
3. Click Login

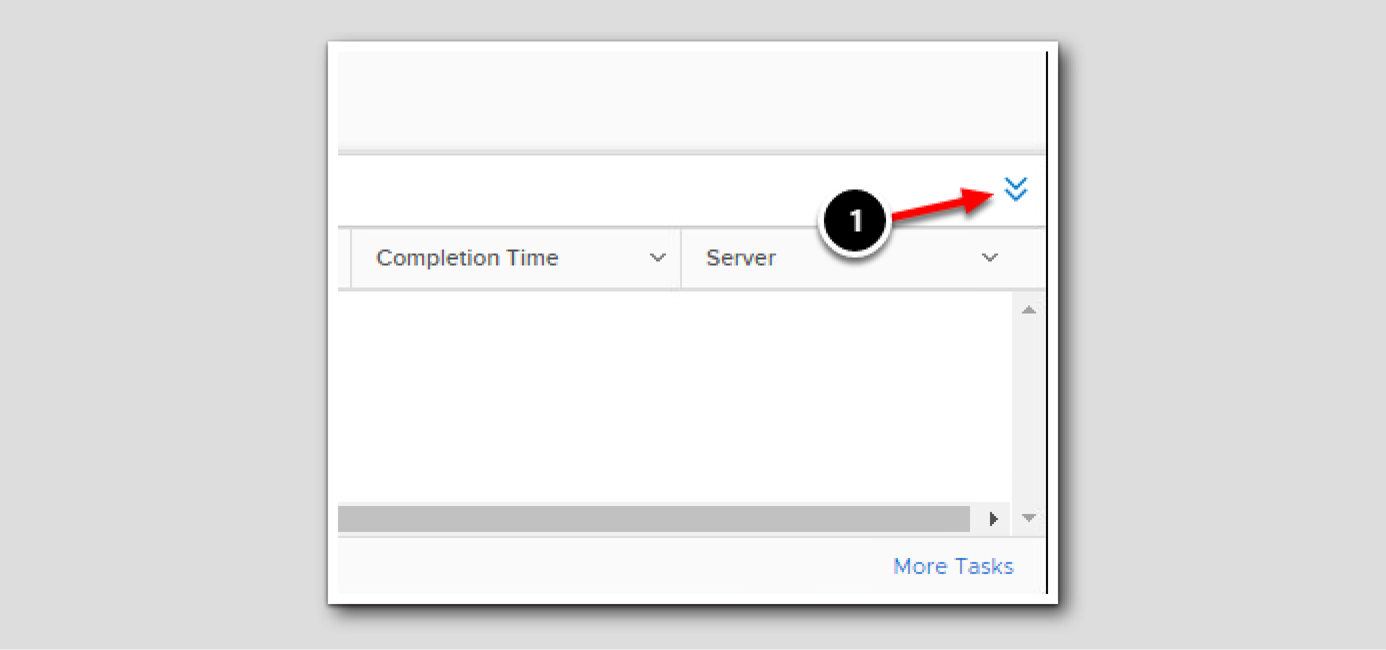
Navigate to Administration



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

Minimize Recent Tasks

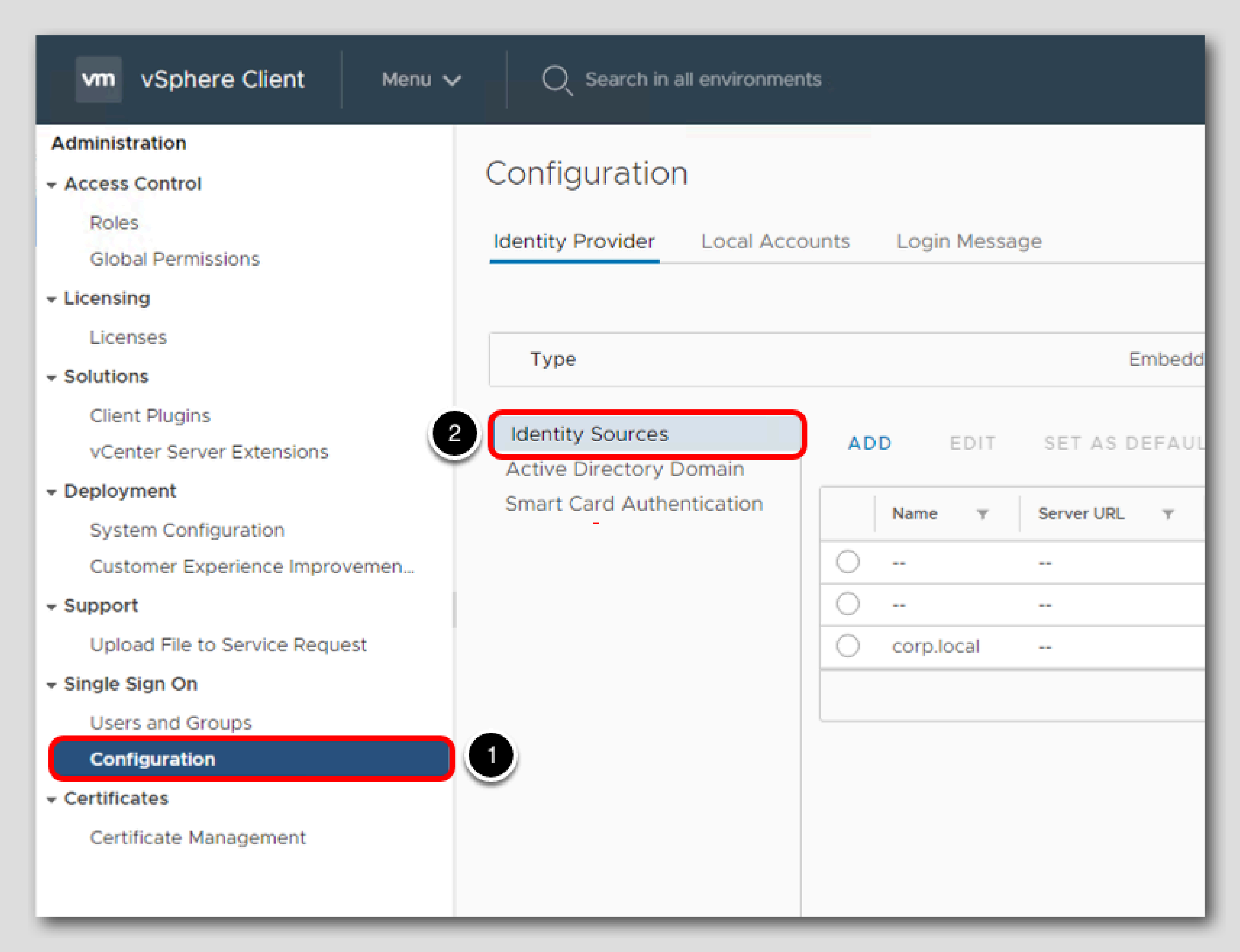
[418]



1. To see more of the vSphere Client, minimize the Recent Tasks window by clicking the two down arrows.

vSphere Single Sign-on

[419]

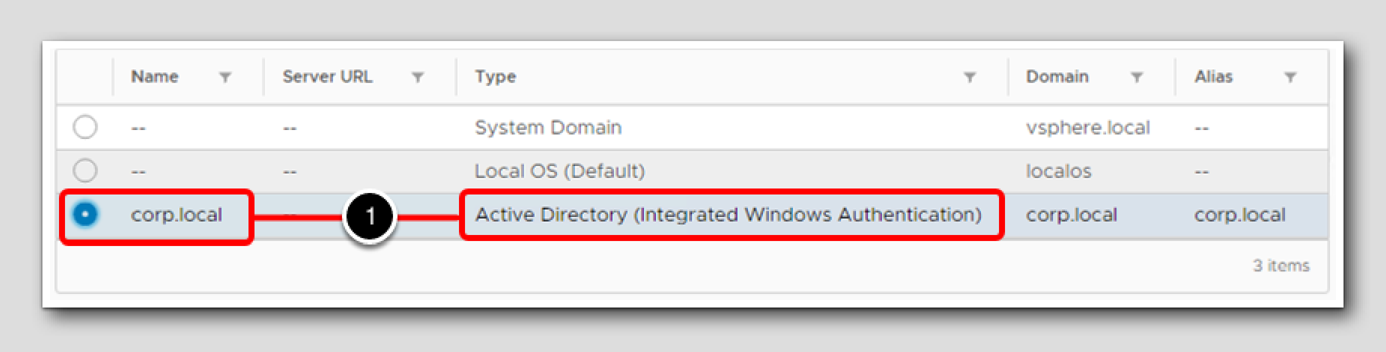


When the machine with the Platform Services Controller (PSC), which runs the Single Sign-On component, is added to an Active Directory domain, the Identity Source for that domain is automatically added to SSO.

1. Click on Configuration in the Single Sign-On section of the Navigator
2. Click on the Identity Sources tab

Identity Sources

[420]



	Name	Server URL	Type	Domain	Alias
○	--	--	System Domain	vsphere.local	--
○	--	--	Local OS (Default)	localos	--
●	corp.local	--	Active Directory (Integrated Windows Authentication)	corp.local	corp.local

3 items

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.

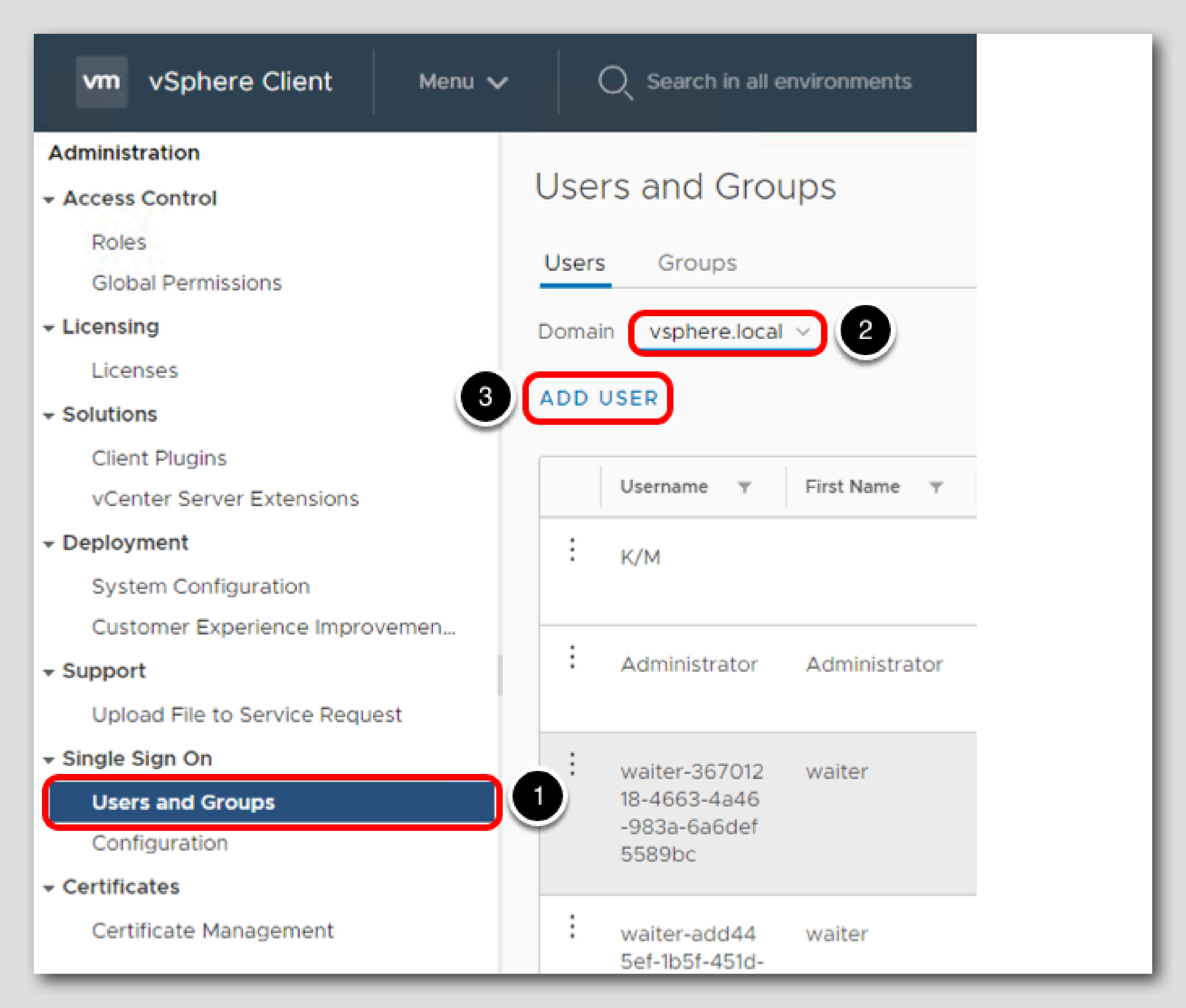
Add a vCenter Single Sign On User with the vSphere Client

[421]

In the vSphere Client, users listed on the Users tab are internal to vCenter Single Sign On. These users are not the same as local operating system users, which are local to the operating system of the machine where Single Sign On is installed (for example, Windows). When you add a Single Sign On user with the Single Sign On administration tool, that user is stored in the Single Sign On database, which runs on the system where Single Sign On is installed. These users are part of the SSO domain, by default, "vsphere.local" -- or "System-Domain" for vSphere 5.1. Exactly one system identity source is associated with an installation of Single Sign On.

List Current Users and Add New User

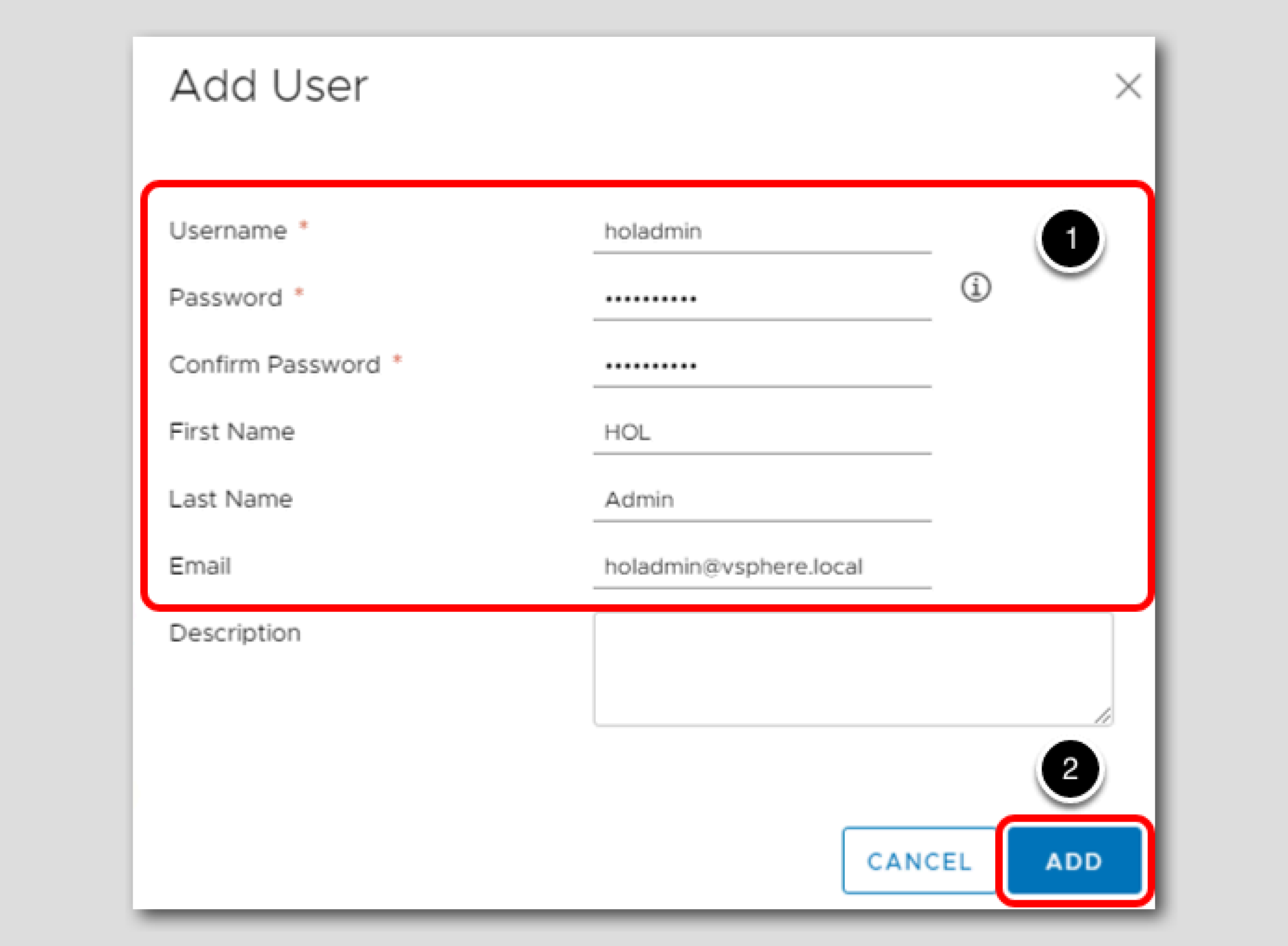
[422]



Username	First Name
K/M	
Administrator	Administrator
waiter-36701218-4663-4a46-983a-6a6def5589bc	waiter
waiter-add445ef-1b5f-451d-	waiter

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

Enter Properties for New User



Add User

Username * holadmin

Password * •••••••••••

Confirm Password * •••••••••••

First Name HOL

Last Name Admin

Email holadmin@vsphere.local

Description

1. Fill out the New User form as follows:

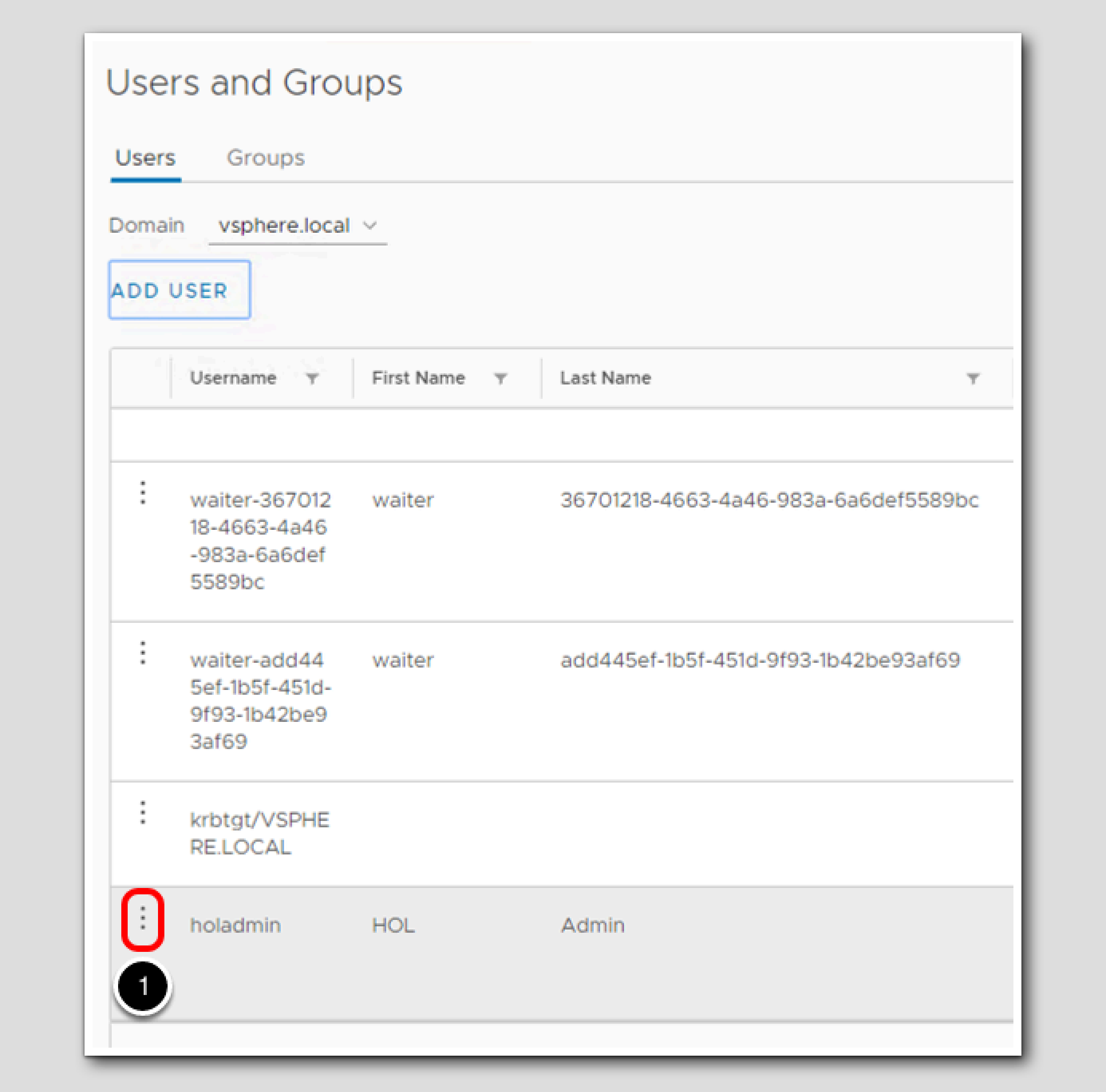
- Username: holadmin
- Password: VMware1!
- Confirm password: VMware1!
- First name: HOL
- Last name: Admin
- Email address: holadmin@vsphere.local

2. Click ADD to create the user

NOTE: You cannot change the user's name after you create the user. First and Last name are optional parameters.

New User Added

[424]



Users and Groups

Domain vsphere.local

Username	First Name	Last Name
waiter-36701218-4663-4a46-983a-6a6def5589bc	waiter	36701218-4663-4a46-983a-6a6def5589bc
waiter-add445ef-1b5f-451d-9f93-1b42be93af69	waiter	add445ef-1b5f-451d-9f93-1b42be93af69
krbtgt/VSPHERE.LOCAL		
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

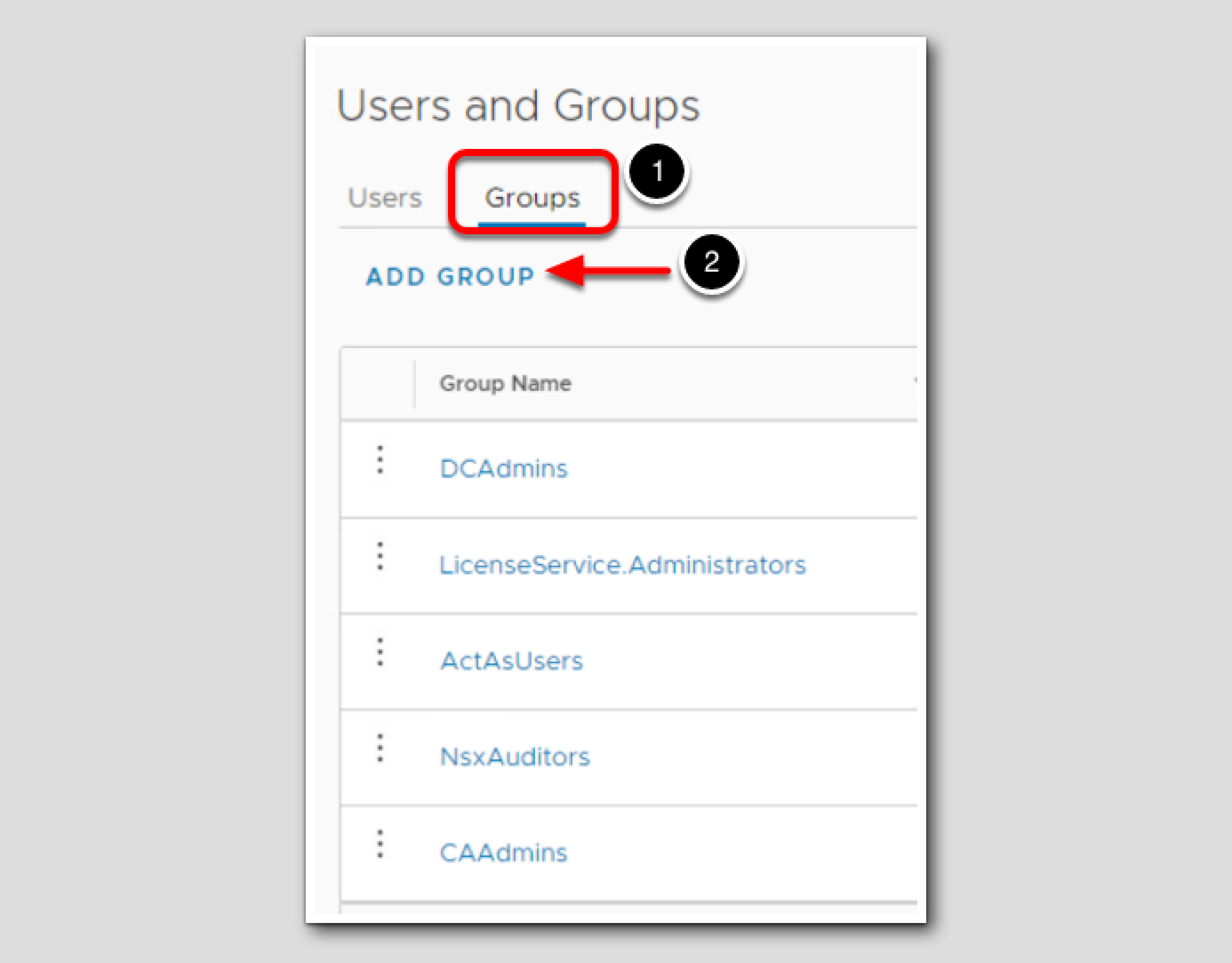
[425]

In the vSphere Client, groups listed on the Groups tab are internal to vCenter Single Sign On. A group lets you create a container for a collection of group members called principals. When you add a Single Sign On group with the Single Sign On administration tool, the group is stored in the Single Sign On database. The database runs on the system where Single Sign On is installed. These groups are part of the identity source domain vsphere.local (the default for vSphere 5.5 and higher), or System-Domain for vSphere 5.1.

Group members can be users or other groups, and a group can contain members from across multiple identity sources. After you create a group and add principals, you apply permissions to the group. Members of the group inherit the group permissions.

Click Groups

[426]

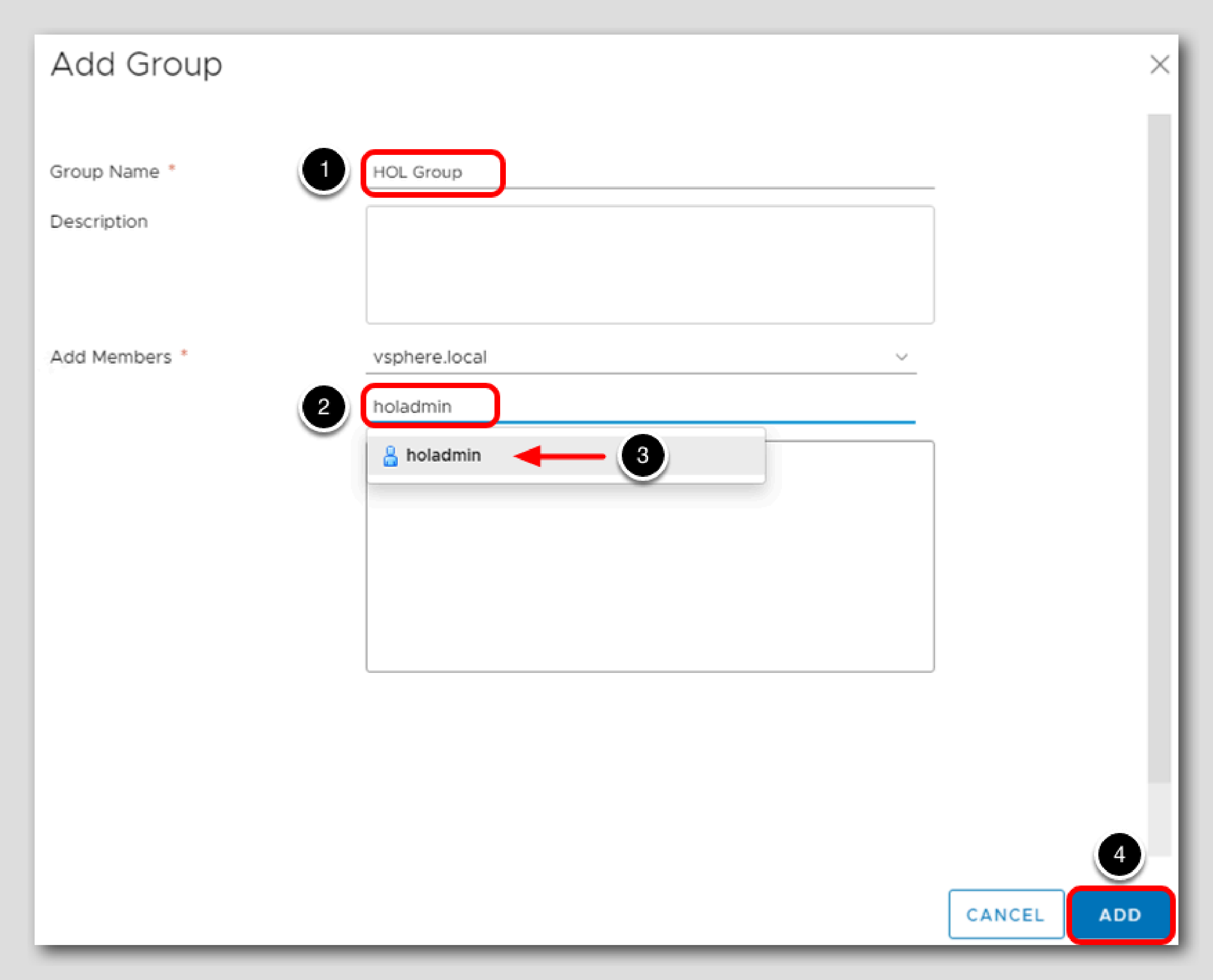


Users and Groups

	Group Name
⋮	DCAdmins
⋮	LicenseService.Administrators
⋮	ActAsUsers
⋮	NsxAuditors
⋮	CAAdmins

1. Click Groups
2. Click Add Group

Create the new group



Add Group

Group Name * HOL Group

Description

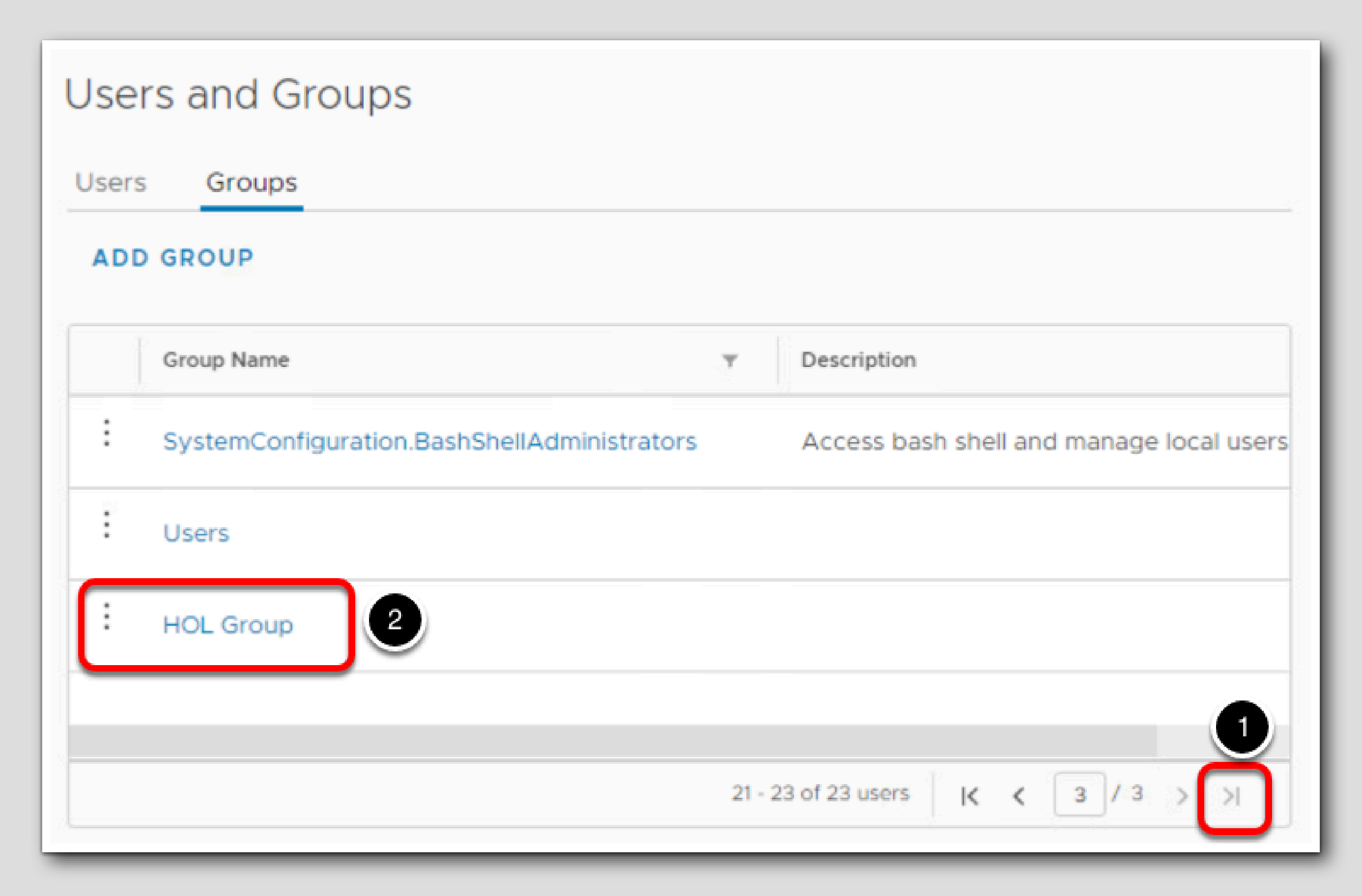
Add Members * vsphere.local

holadmin

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

[428]



Users and Groups

Group Name	Description
SystemConfiguration.BashShellAdministrators	Access bash shell and manage local users
Users	
HOL Group	

21 - 23 of 23 users   3 / 3

1. Click on the **arrow (⇥)** to move to the third page of Groups
2. Here is the group, **HOL Group** that was just created

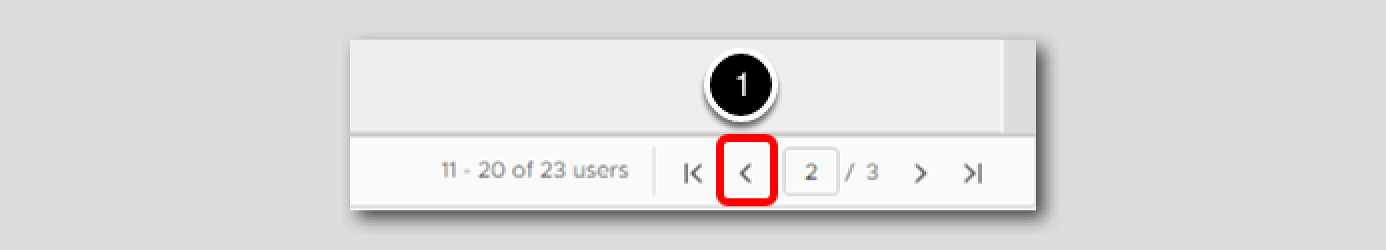
Add Members to a vCenter Single Sign On Group in the vSphere Client

[429]

Members of a vCenter Single Sign On group can be users or other groups from one or more identity sources. Members of a group are called principals. Groups listed on the Groups tab in the vSphere Client are internal to Single Sign On and are part of the identity source System-Domain. You can add group members from other domains to a local group. You can also nest groups.

Return to Page 2

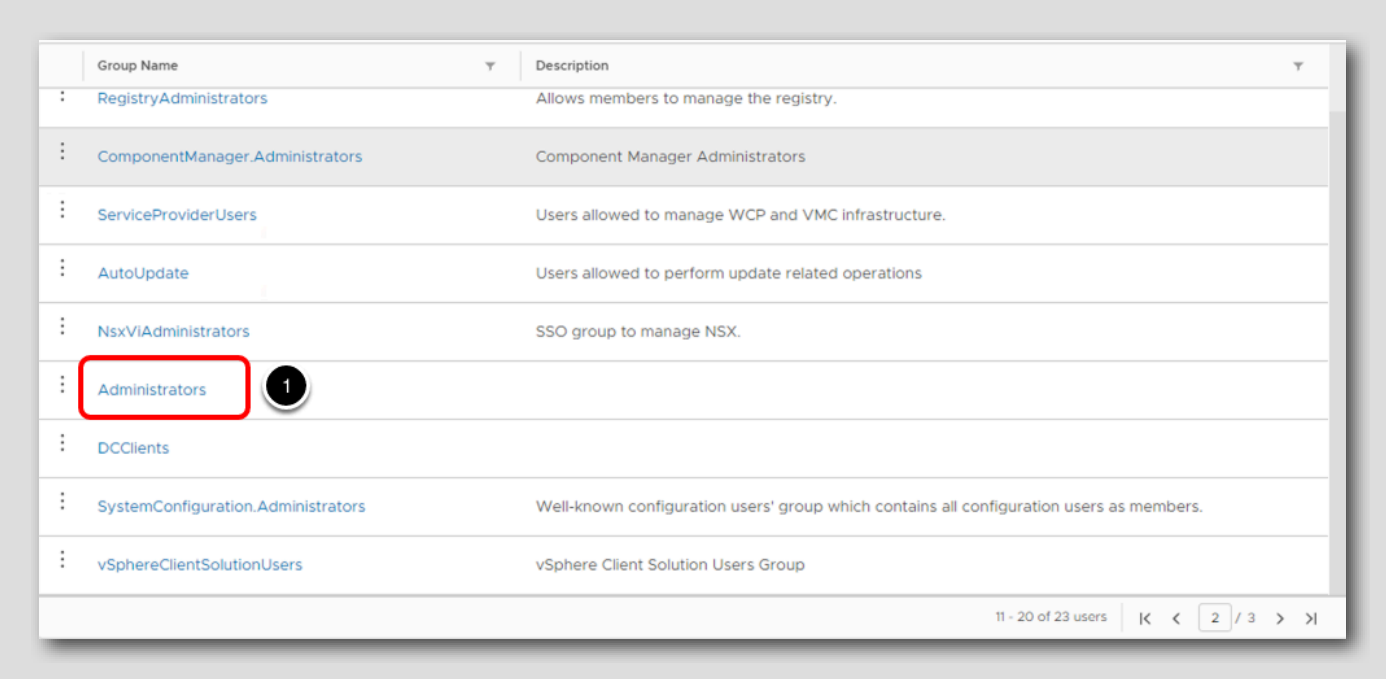
[430]



1. Click on the **left arrow** (<) to return to the second page of Groups.

Add Members to Users and Groups

[431]



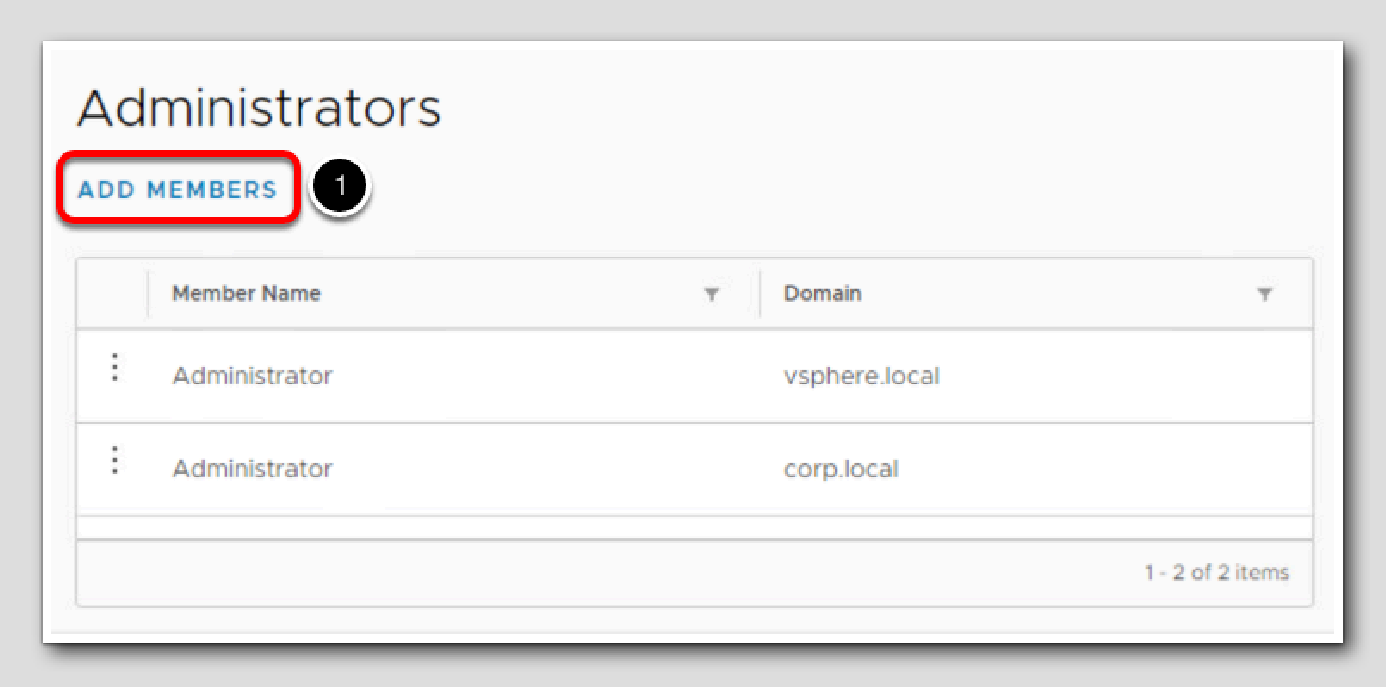
Group Name	Description
RegistryAdministrators	Allows members to manage the registry.
ComponentManager.Administrators	Component Manager Administrators
ServiceProviderUsers	Users allowed to manage WCP and VMC infrastructure.
AutoUpdate	Users allowed to perform update related operations
NsxViAdministrators	SSO group to manage NSX.
Administrators	
DCClients	
SystemConfiguration.Administrators	Well-known configuration users' group which contains all configuration users as members.
vSphereClientSolutionUsers	vSphere Client Solution Users Group

1. Click on the **Administrators** group under the Group Names table

Note: You may need to scroll down to see it.

Add Members

[432]



Administrators

Member Name	Domain
Administrator	vsphere.local
Administrator	corp.local

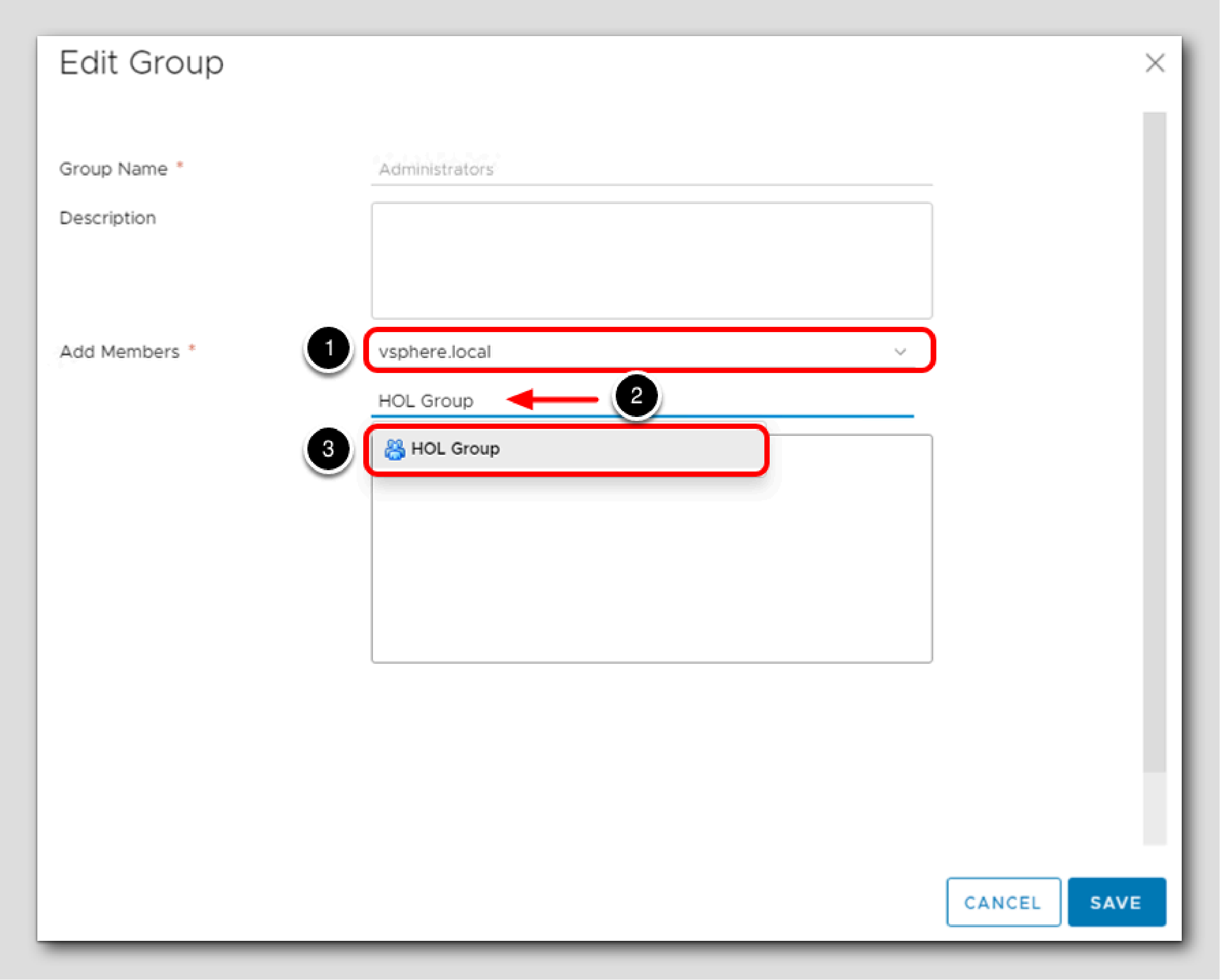
1 - 2 of 2 items

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

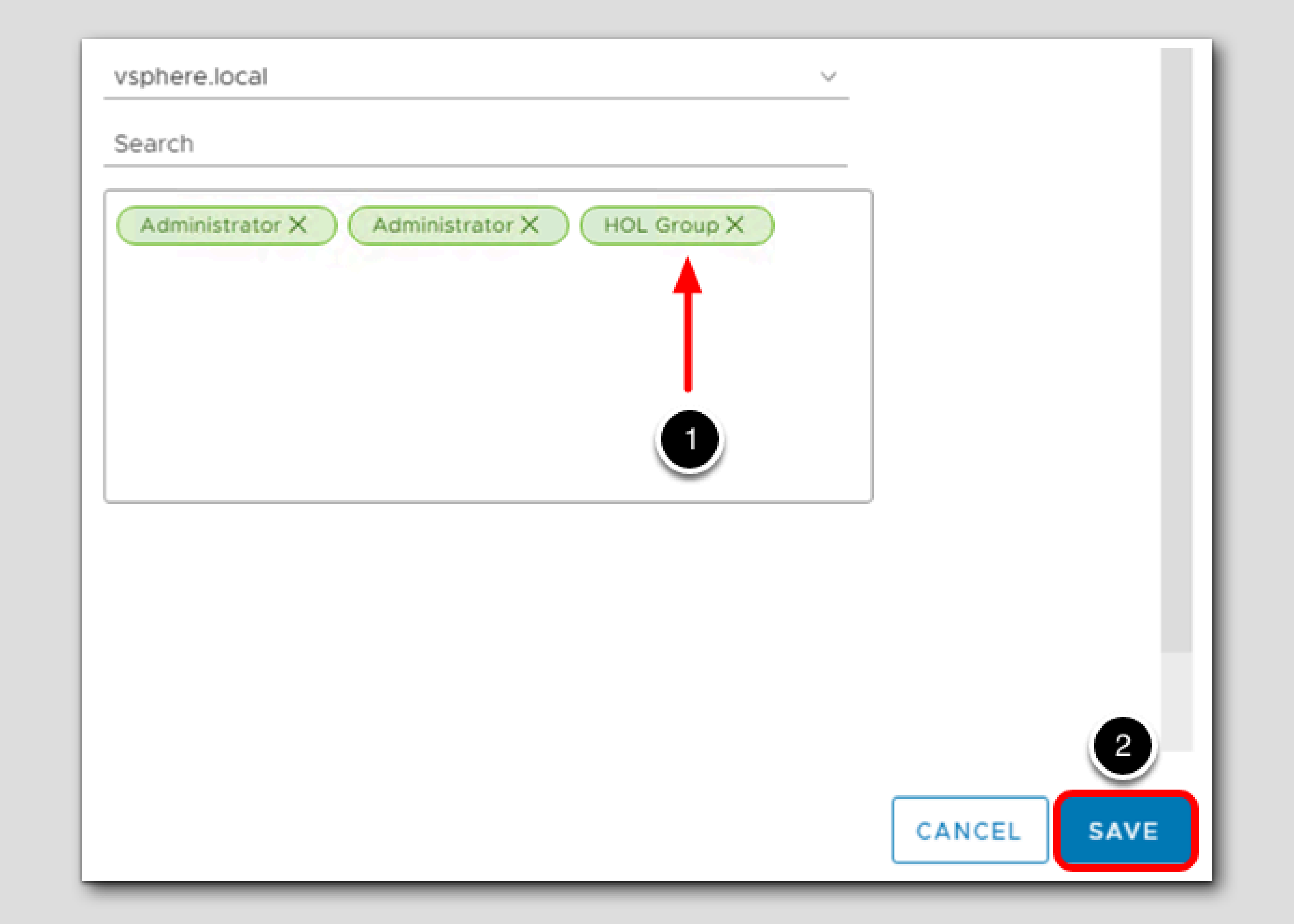
1. Click Add Members

Edit Group

[433]



1. Make sure the domain selected is vsphere.local
2. Type HOL Group in the search box
3. Click on HOL Group to add it to the member list



vsphere.local

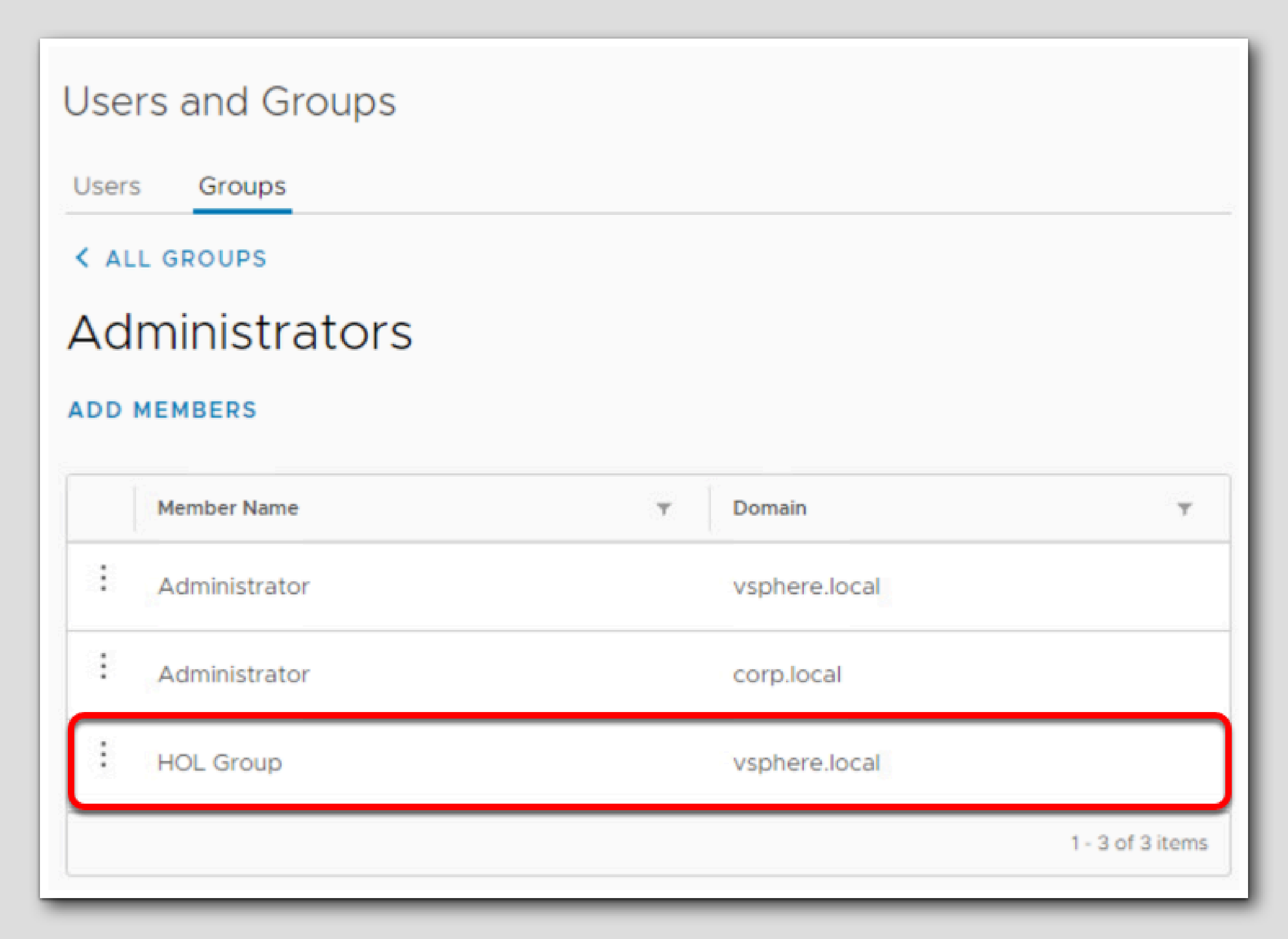
Search

Administrator ✕ Administrator ✕ HOL Group ✕

1. You should see HOL Group added to the list.
2. Click Save.

New Member Added

[434]



Users and Groups

Administrators

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

1 - 3 of 3 items

The **HOL Group** has now been added to the Administrator group.

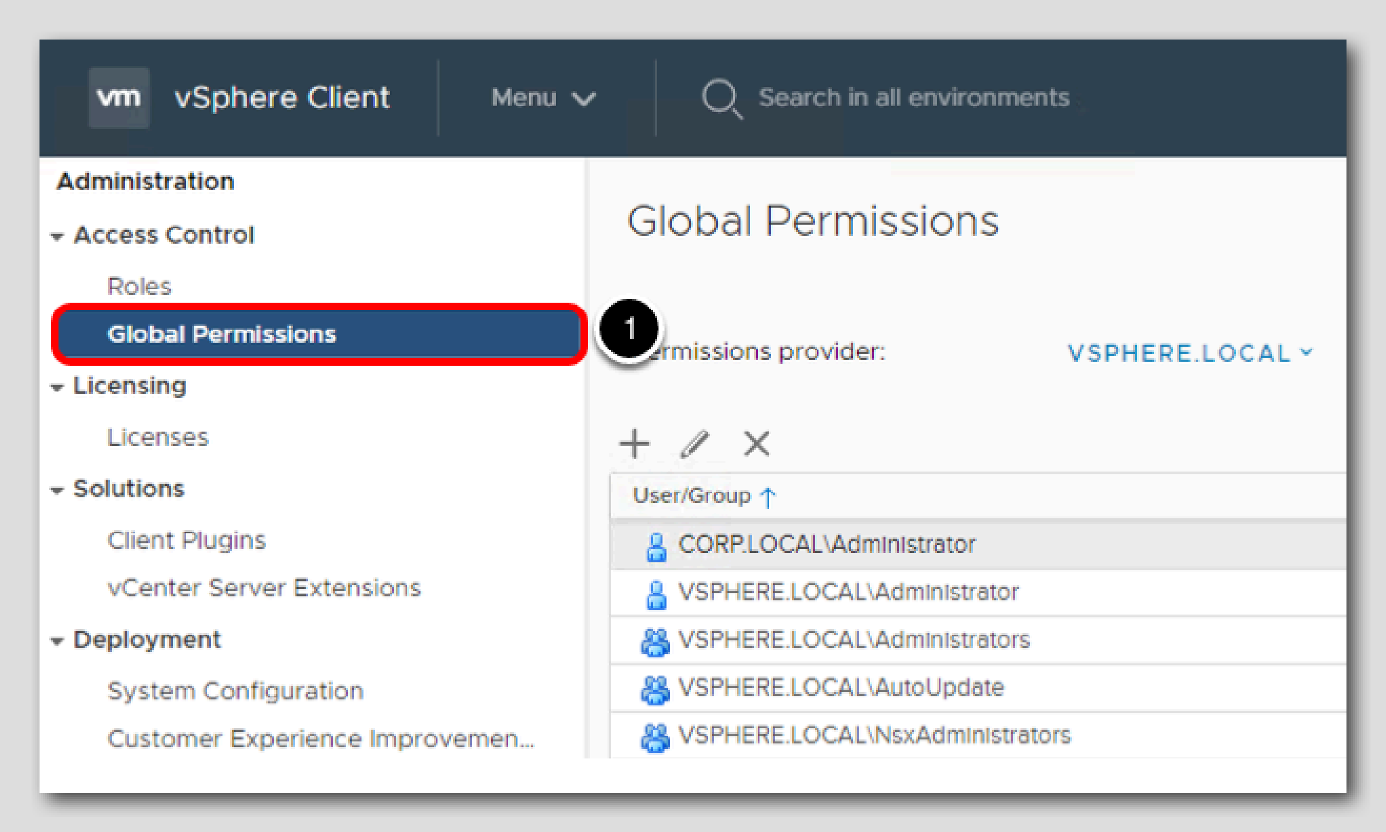
Assign Global Permissions

[435]

Once identity sources, users and groups have been configured, they must be assigned permissions in order to be useful in vSphere.

List Global Permissions

[436]

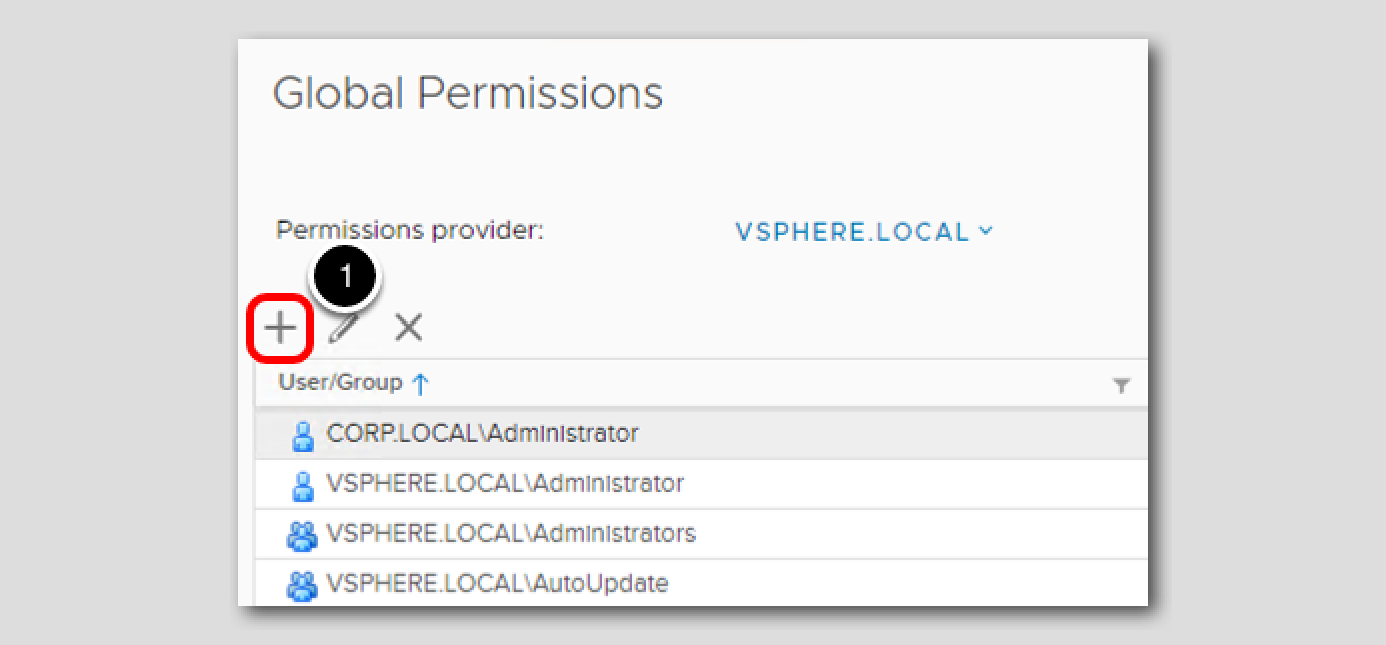


1. Click on the **Global Permissions** item under Access Control

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

[437]



Global Permissions

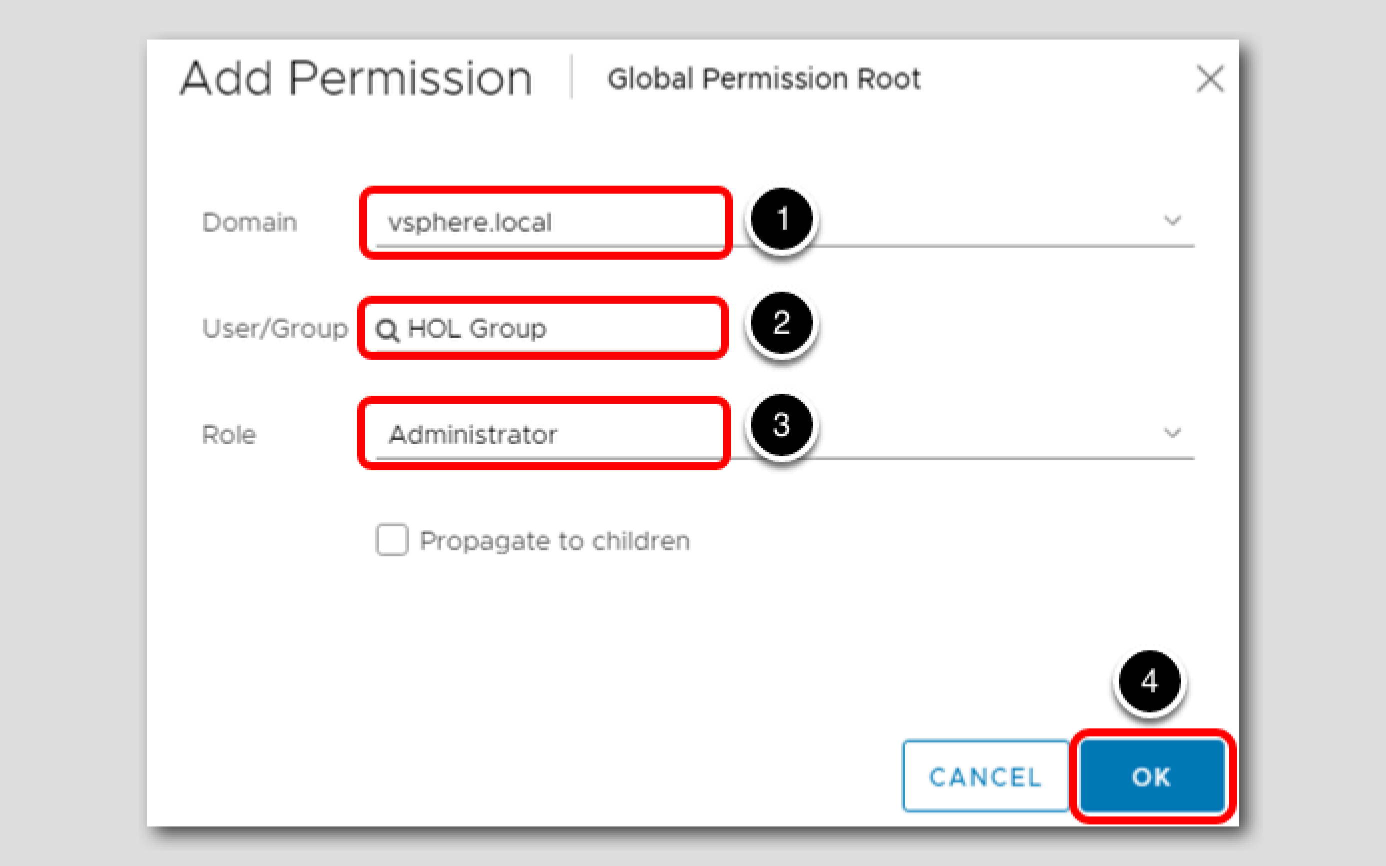
Permissions provider: VSPHERE.LOCAL

User/Group
CORP.LOCAL\Administrator
VSPHERE.LOCAL\Administrator
VSPHERE.LOCAL\Administrators
VSPHERE.LOCAL\AutoUpdate

The members of the HOL Group will need to manage all virtual machines in the environment, so we will configure permissions here.

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

Locate the HOL Group



Add Permission | Global Permission Root

Domain: vsphere.local

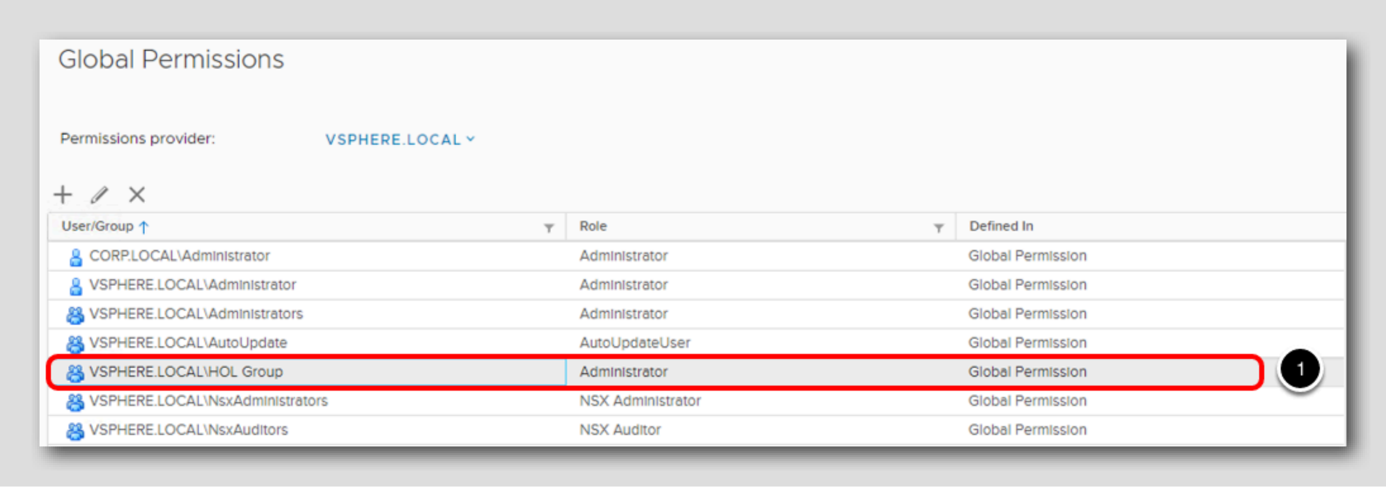
User/Group: HOL Group

Role: Administrator

☐ Propagate to children

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

New Global Permission [439]



Global Permissions

Permissions provider: VSPHERE.LOCAL

User/Group	Role	Defined In
CORP.LOCAL\Administrator	Administrator	Global Permission
VSPHERE.LOCAL\Administrator	Administrator	Global Permission
VSPHERE.LOCAL\Administrators	Administrator	Global Permission
VSPHERE.LOCAL\AutoUpdate	AutoUpdateUser	Global Permission
VSPHERE.LOCAL\HOL Group	Administrator	Global Permission
VSPHERE.LOCAL\NsxAdministrators	NSX Administrator	Global Permission
VSPHERE.LOCAL\NsxAuditors	NSX Auditor	Global Permission

The newly created **vsphere.local** Global Permission has been created.

Conclusion [440]

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 [441]

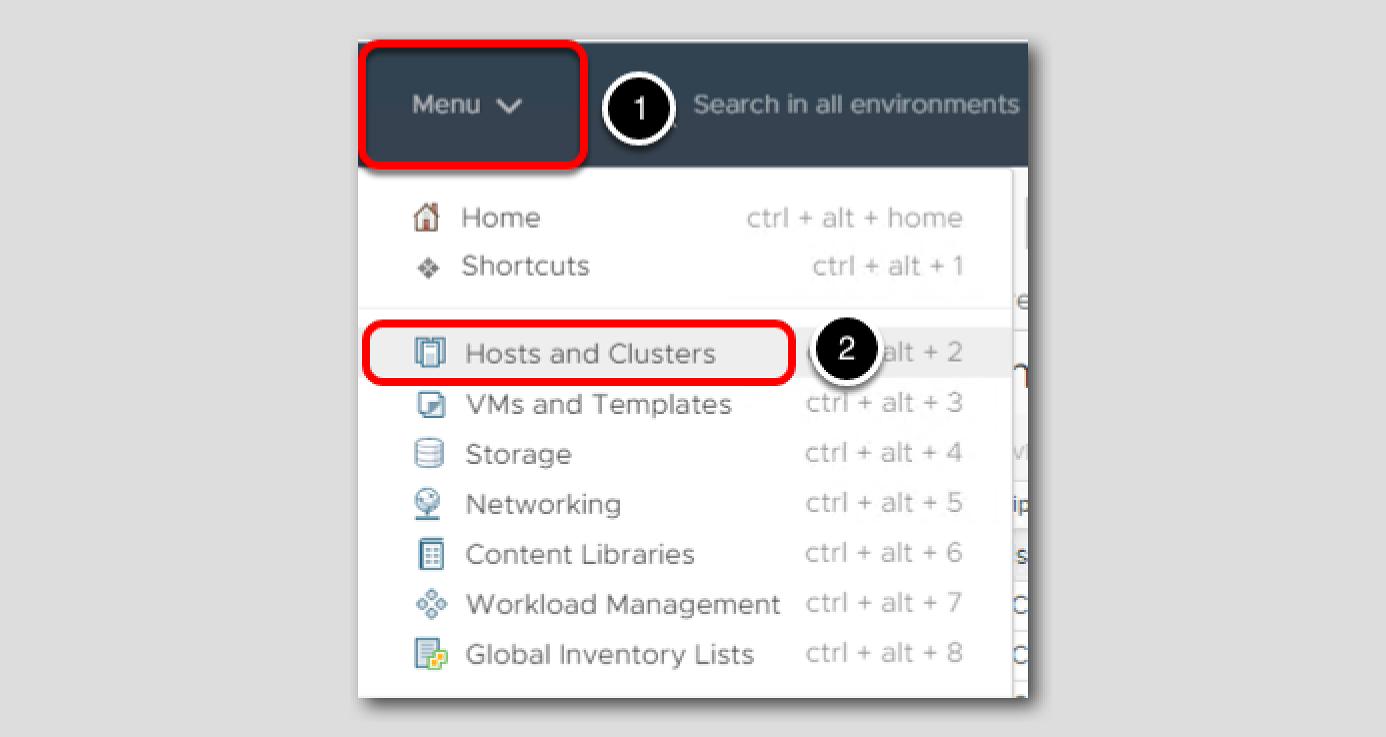
In this lesson, we will walk through the process of adding an ESXi host to Active Directory.

Configure a Host to Use Active Directory in the vSphere Web Client [442]

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

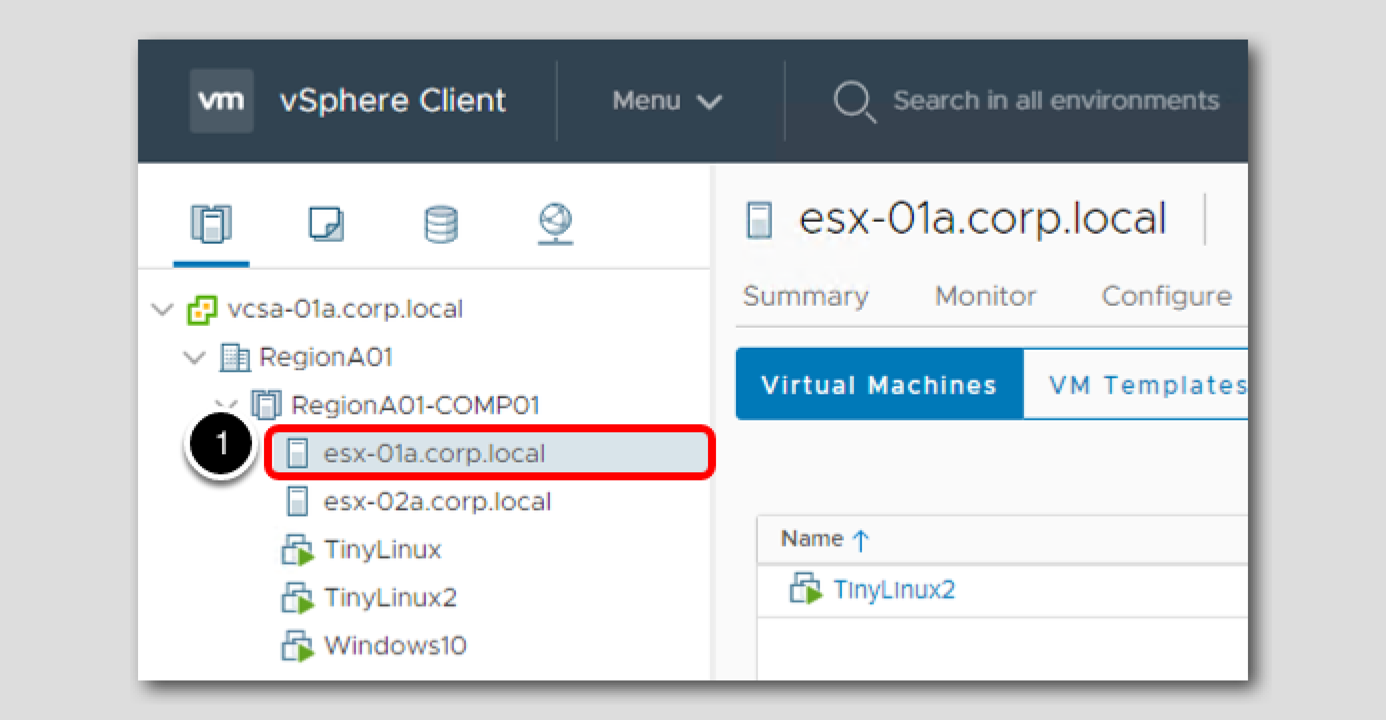
Hosts and Clusters

[443]


Menu
1
Search in all environments
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters
2
alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Workload Management ctrl + alt + 7
Global Inventory Lists ctrl + alt + 8

1. Click on **Menu**
2. Select **Hosts and Clusters**

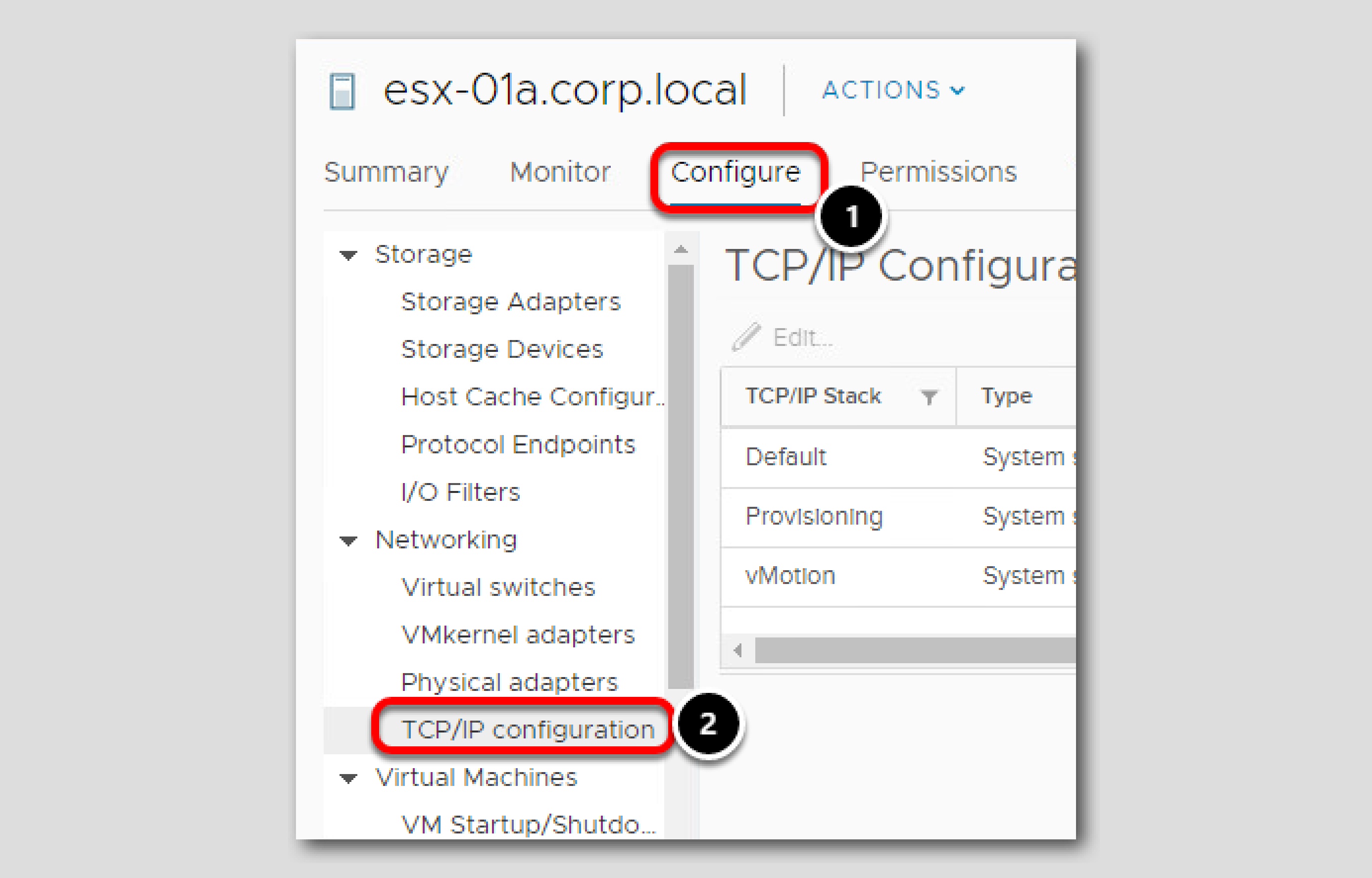
esx-01a.corp.local



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

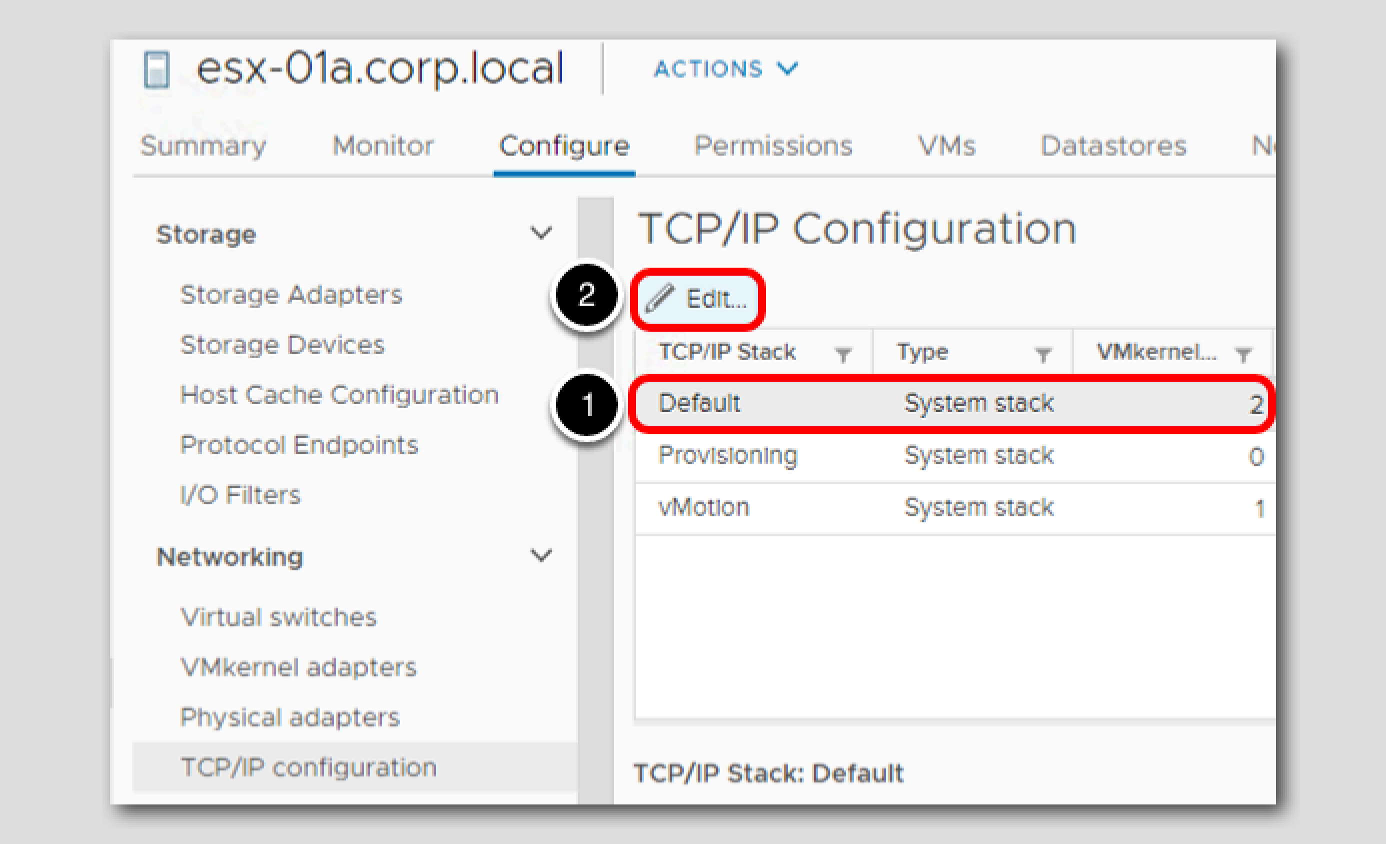


TCP/IP Stack	Type
Default	System
Provisioning	System
vMotion	System

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

Edit Default System Stack

[446]



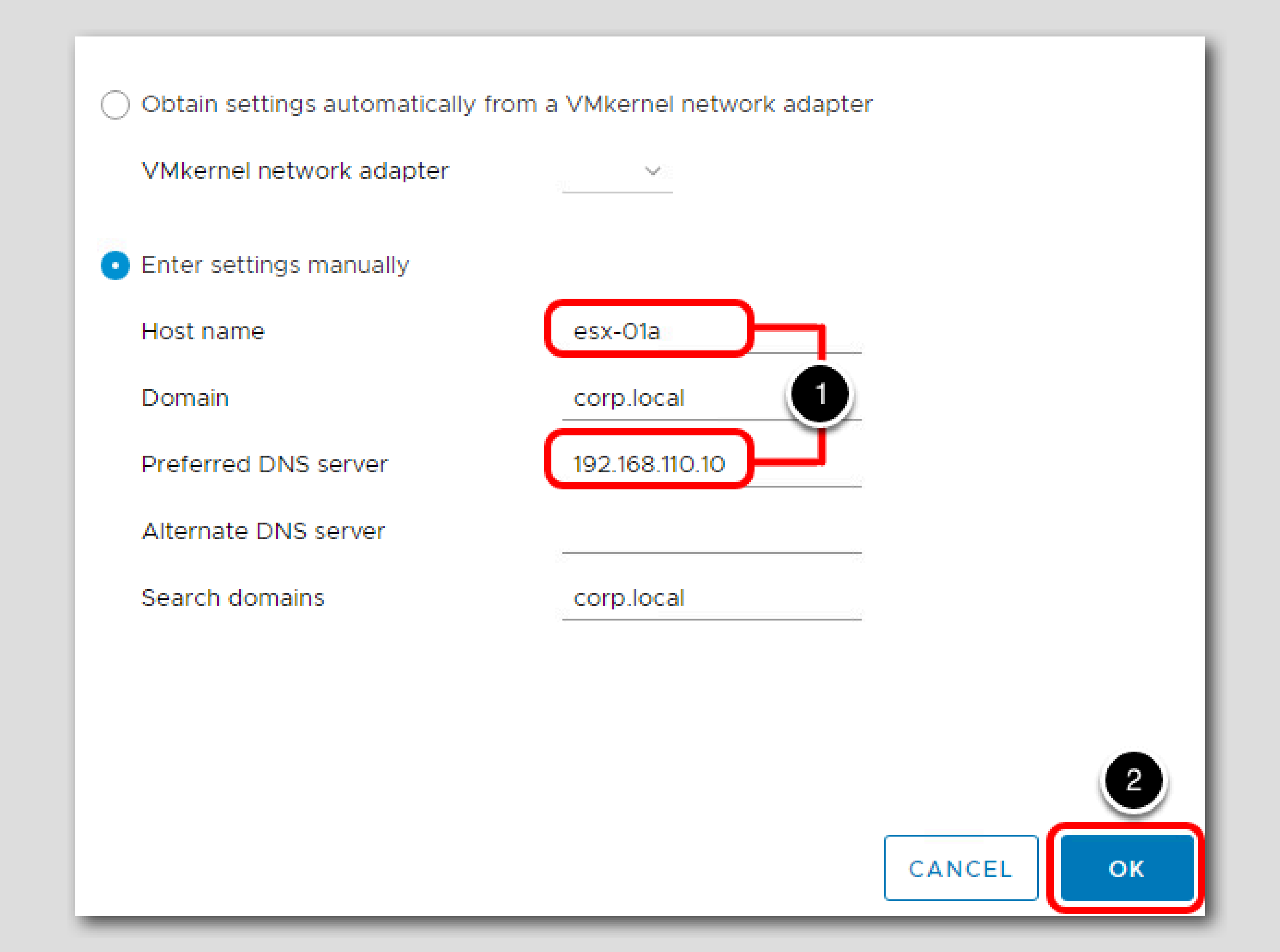
TCP/IP Stack	Type	VMkernel...
Default	System stack	2
Provisioning	System stack	0
vMotion	System stack	1

TCP/IP Stack: Default

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

DNS configuration

[447]



○ Obtain settings automatically from a VMkernel network adapter

VMkernel network adapter

● Enter settings manually

Host name: esx-01a

Domain: corp.local

Preferred DNS server: 192.168.110.10

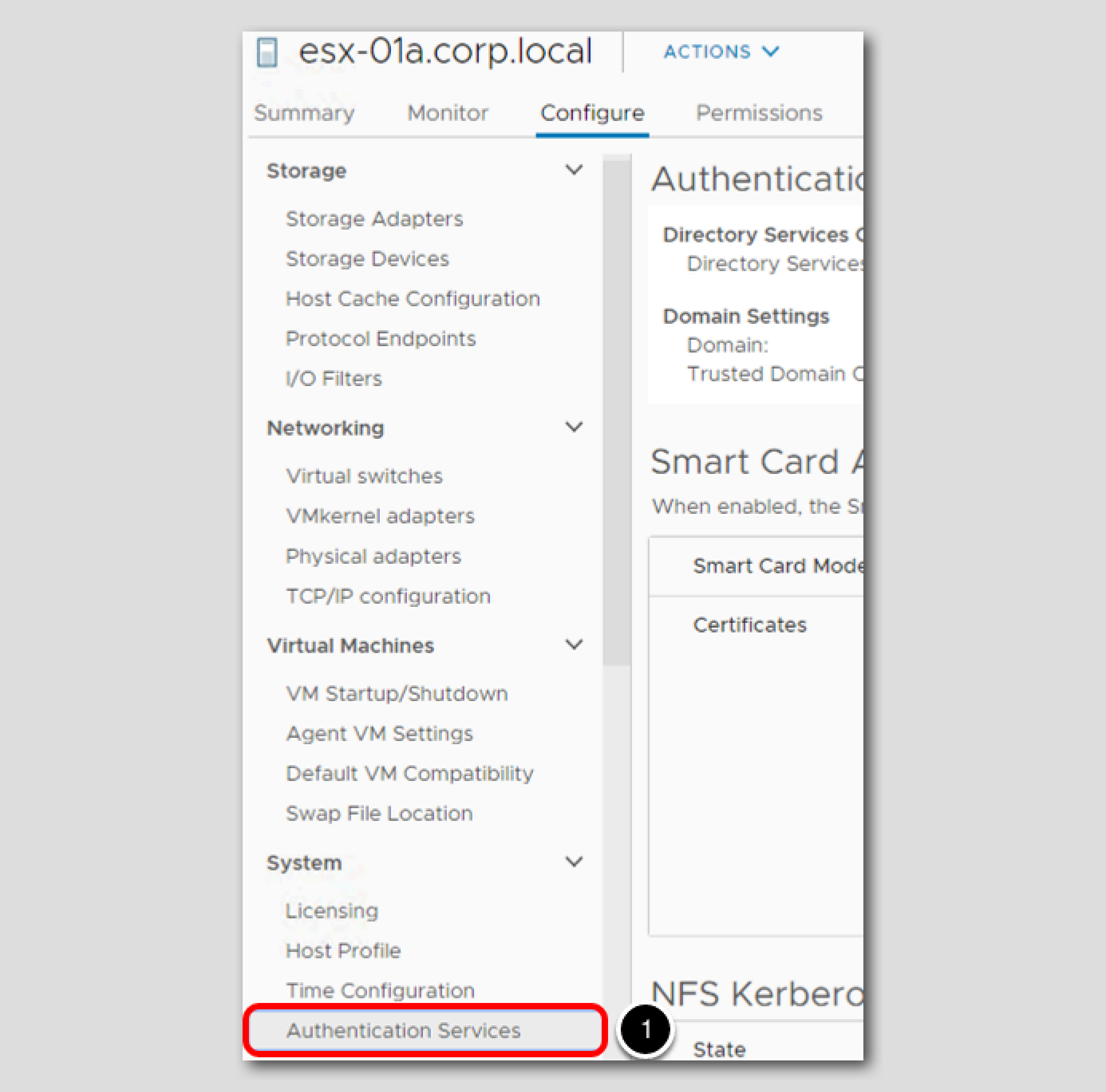
Alternate DNS server:

Search domains: corp.local

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

[448]



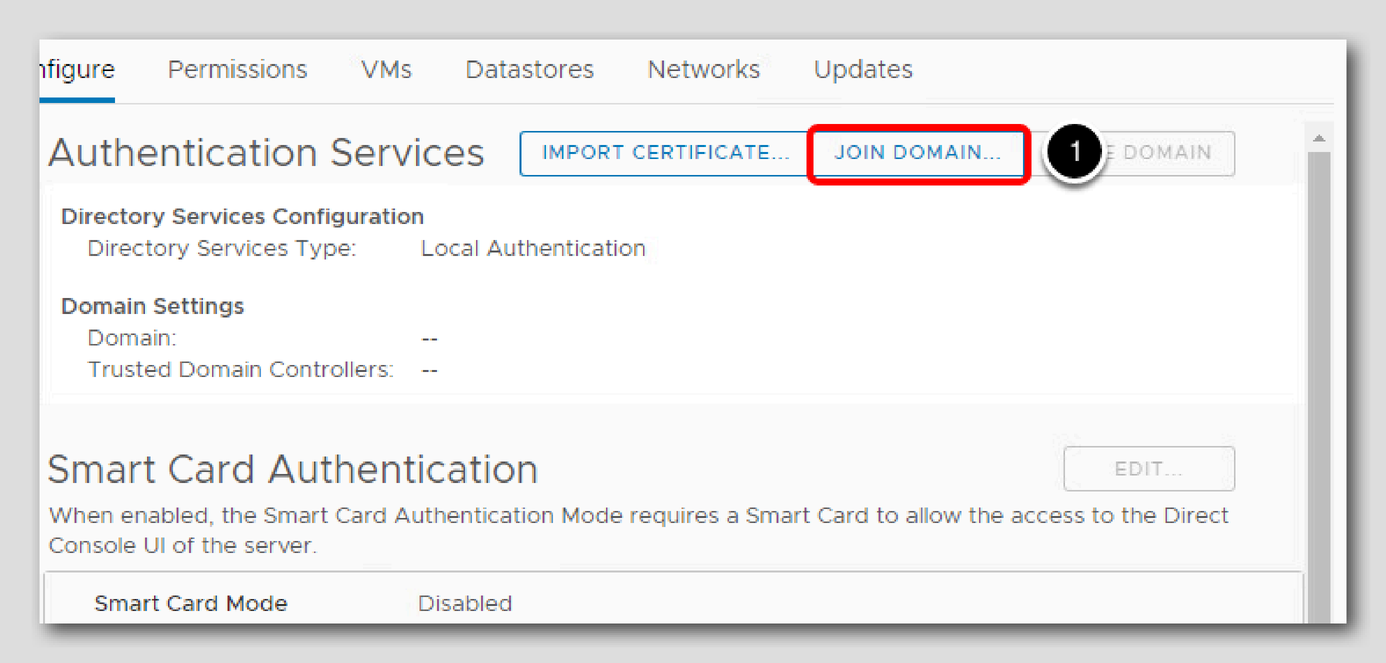
Now that the network settings have been verified, the host will be added to Active Directory.

1. Click on Authentication Services under the System section

You may need to scroll down to see it

Join Domain

[449]



Authentication Services

Directory Services Configuration
Directory Services Type: Local Authentication

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

Smart Card Authentication

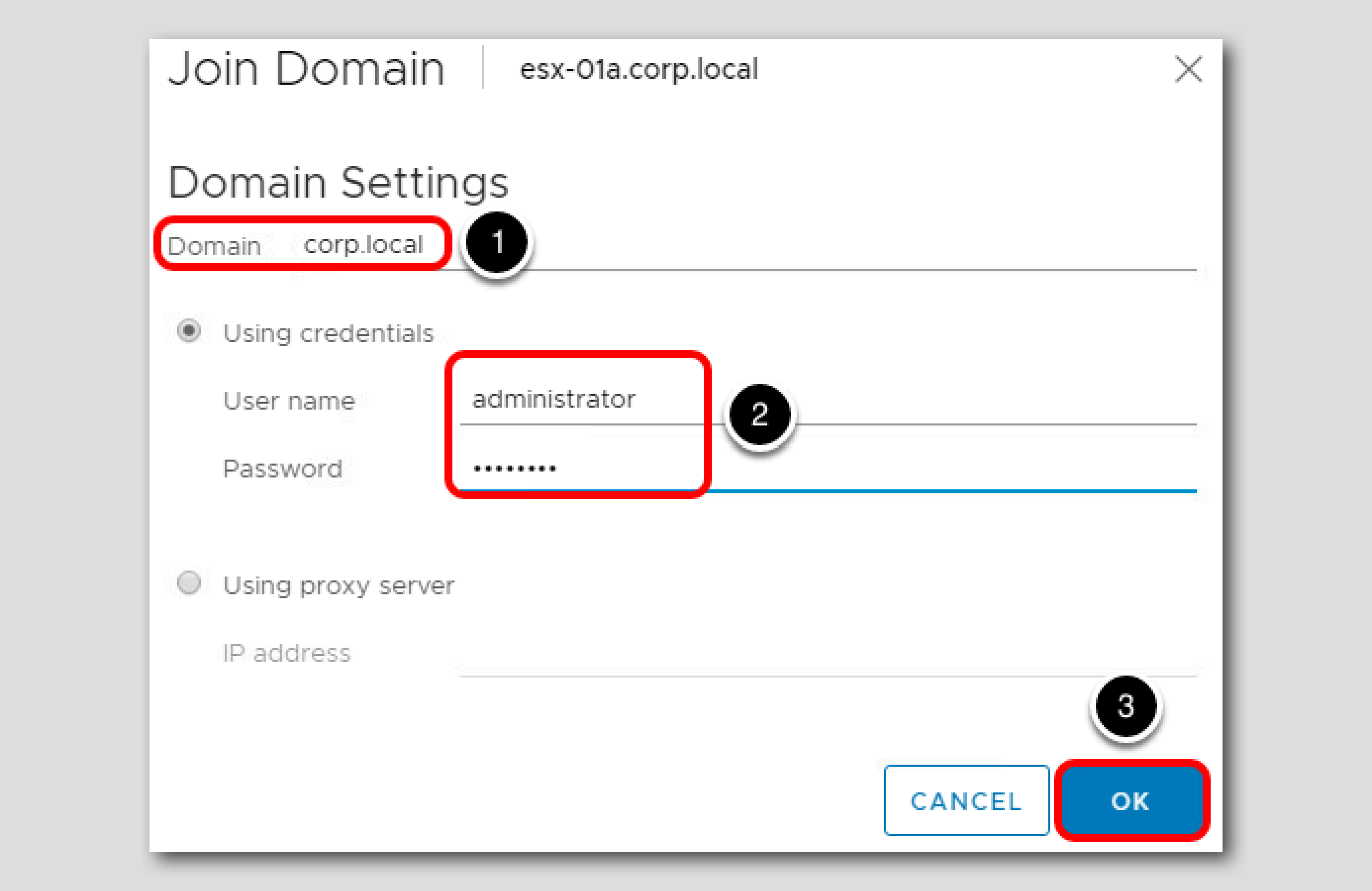
When enabled, the Smart Card Authentication Mode requires a Smart Card to allow the access to the Direct Console UI of the server.

Smart Card Mode Disabled

1. Click the Join Domain button.

Join Domain Settings

[450]



Join Domain | esx-01a.corp.local

Domain Settings

Domain corp.local

● Using credentials

User name administrator

Password •••••••••

○ Using proxy server

IP address

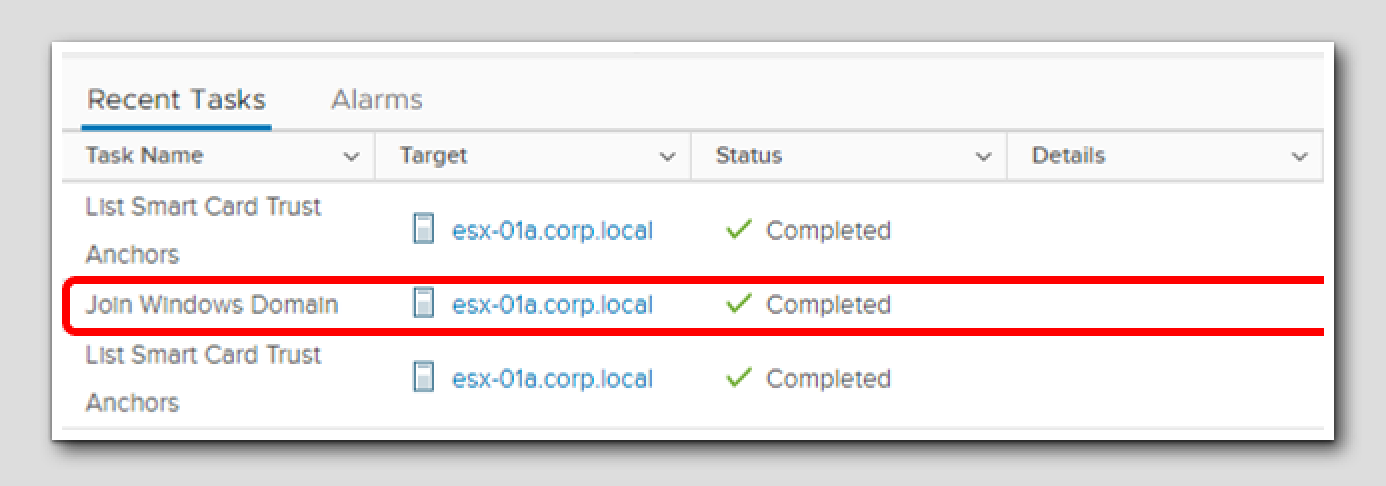
1. Enter corp.local for the Domain
2. In the Using Credentials section enter:

- Username: administrator
- Password: VMware1!

3. Click OK

Recent Tasks

[451]

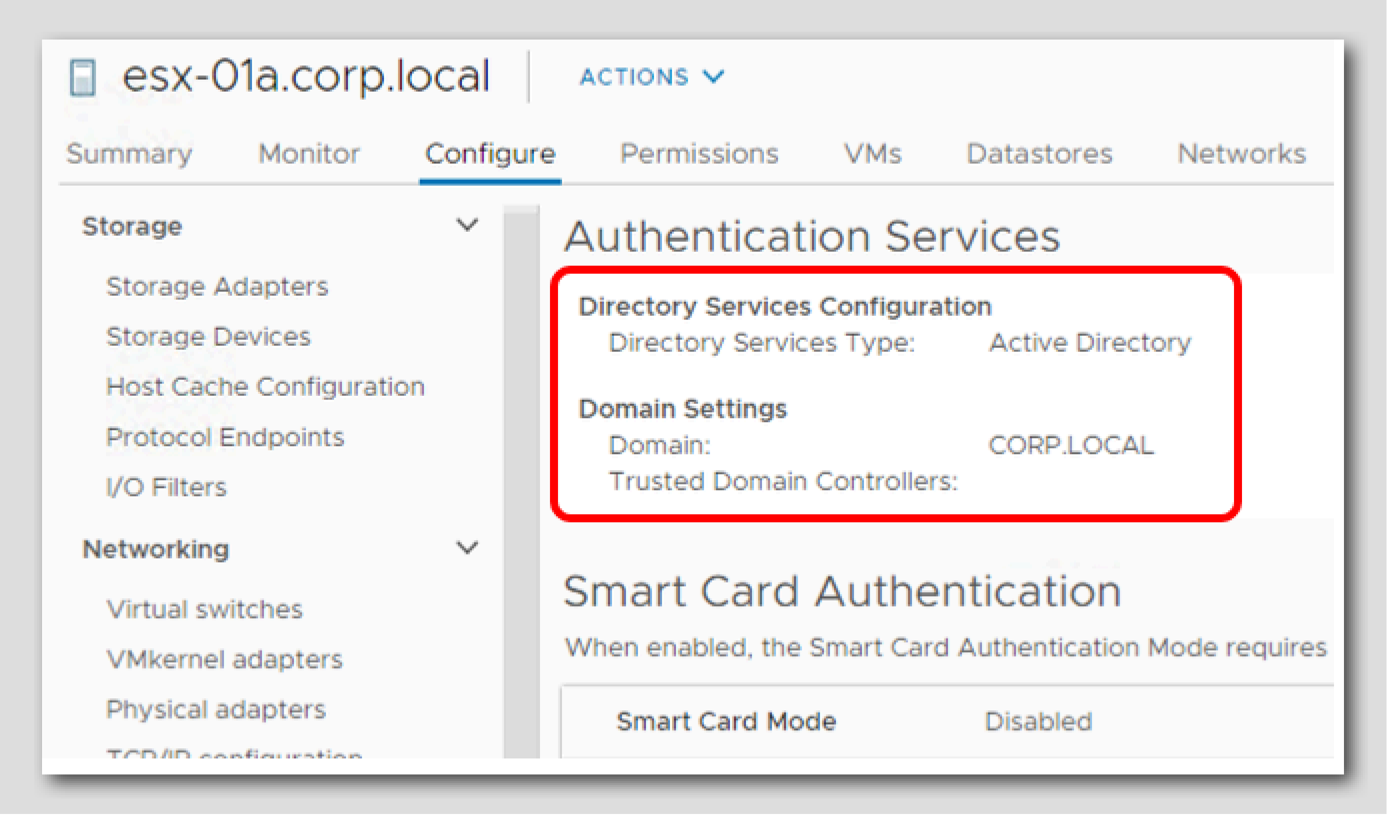


Task Name	Target	Status	Details
List Smart Card Trust Anchors	esx-01a.corp.local	✓ Completed	
Join Windows Domain	esx-01a.corp.local	✓ Completed	
List Smart Card Trust Anchors	esx-01a.corp.local	✓ Completed	

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

Added to Active Directory

[452]



Authentication Services

Directory Services Configuration

Directory Services Type: Active Directory

Domain Settings

Domain: CORP.LOCAL

Trusted Domain Controllers:

Smart Card Authentication

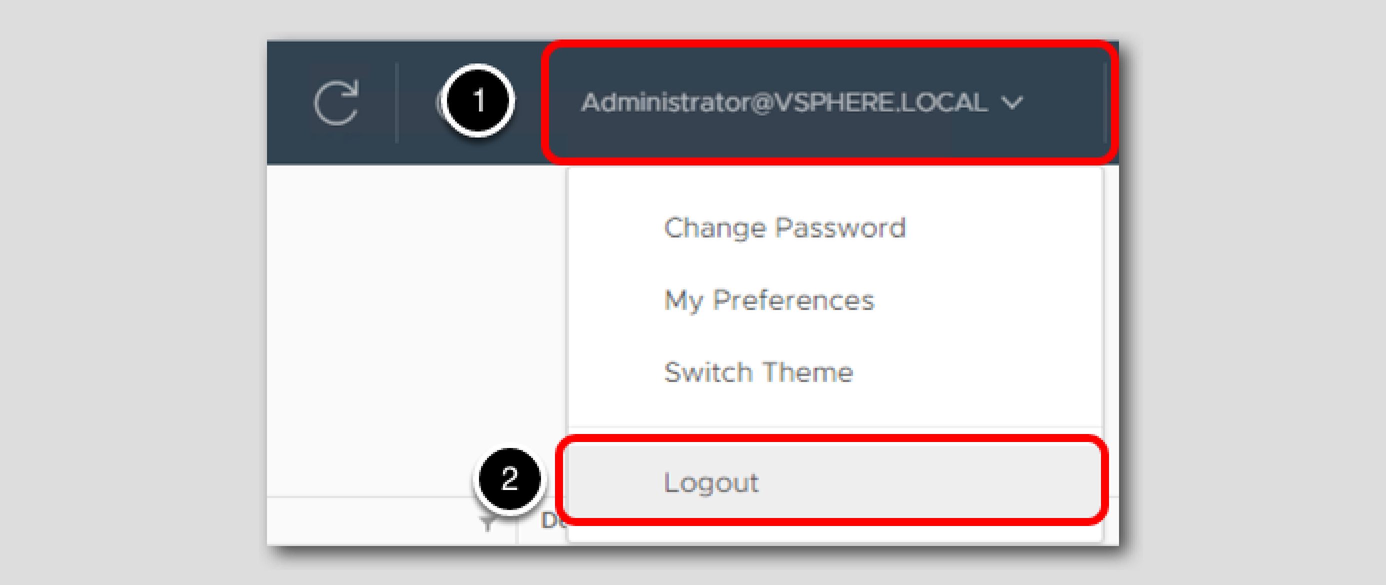
When enabled, the Smart Card Authentication Mode requires

Smart Card Mode Disabled

Once the task has been completed, the Authentication Services section will update to show the host is now connected to the Active Directory domain.

Log out

[453]



If you are continuing on to other modules in this lab, please log out as administrator@vsphere.local.

1. Click Administrator@VSPHERE.LOCAL
2. Click Logout

Conclusion

[454]

This concludes Module 2 - An Introduction to vSphere Networking and Security . We hope you have enjoyed taking this lab. Please remember to take the survey at the end.

If you have time remaining, here are the other Modules that are part of this lab, along with an estimated time to complete each one. Click on the Table of Contents button to quickly jump to that module in the manual.

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

Certification Path

[455]

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

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

Learn More Here: *https://www.vmware.com/learning/certification/vcap-dcv-deploy.html*

vmware®
CERTIFIED
ADVANCED PROFESSIONAL
Data Center Virtualization Deploy 2021

Module 3 - Introduction to vSphere Storage (60 Min)

vSphere Storage Overview

[457]

The following lesson provides an overview of the different types of storage available in vSphere.

The vSphere Hypervisor, ESXi, provides host-level storage virtualization, which logically abstracts the physical storage layer from virtual machines.

A vSphere virtual machine uses a virtual disk to store its operating system, program files, and other data associated with its activities. A virtual disk is a large physical file, or a set of files, that can be copied, moved, archived, and backed up as easily as any other file. You can configure virtual machines with multiple virtual disks.

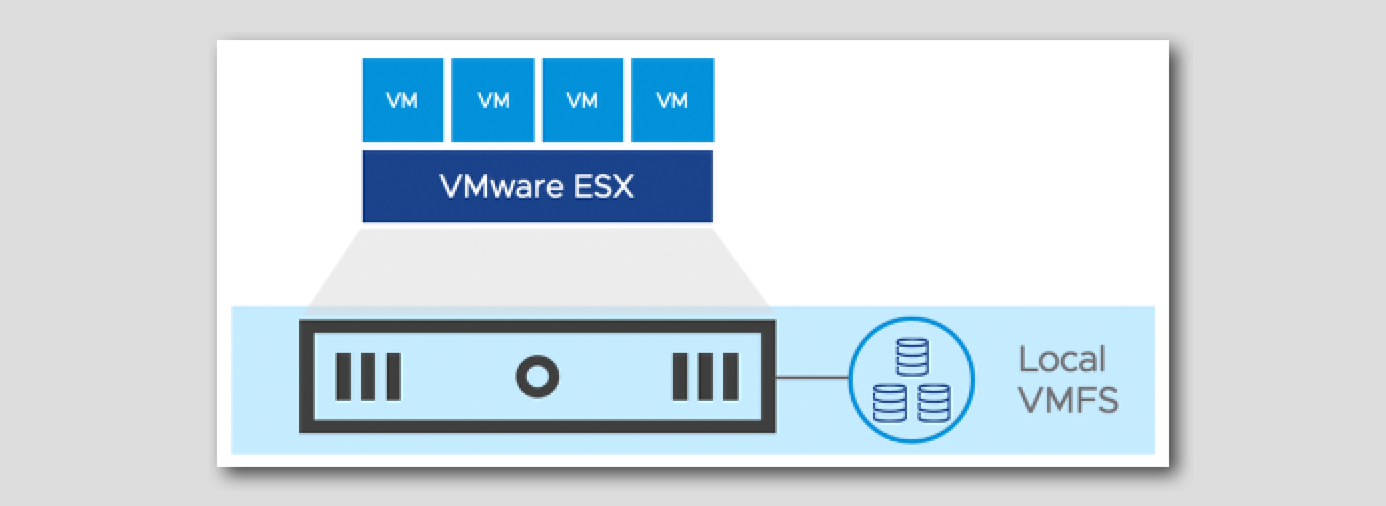
To access virtual disks, a virtual machine uses virtual SCSI controllers. These virtual controllers include BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. These controllers are the only types of SCSI controllers that a virtual machine can see and access.

Each virtual disk resides on a vSphere Virtual Machine File System (VMFS) datastore or an NFS-based datastore that are deployed on physical storage. From the standpoint of the virtual machine, each virtual disk appears as if it were a SCSI drive connected to a SCSI controller. Whether the actual physical storage device is being accessed through parallel SCSI, iSCSI, network, Fibre Channel, or FCoE adapters on the host is transparent to the guest operating system and to applications running on the virtual machine.

The vSphere storage management process starts with storage space that your storage administrator allocates on different storage systems prior to vSphere ESXi assignment. vSphere supports two types of storage - Local and Networked. Each type is detailed in the following lesson steps.

Local Storage

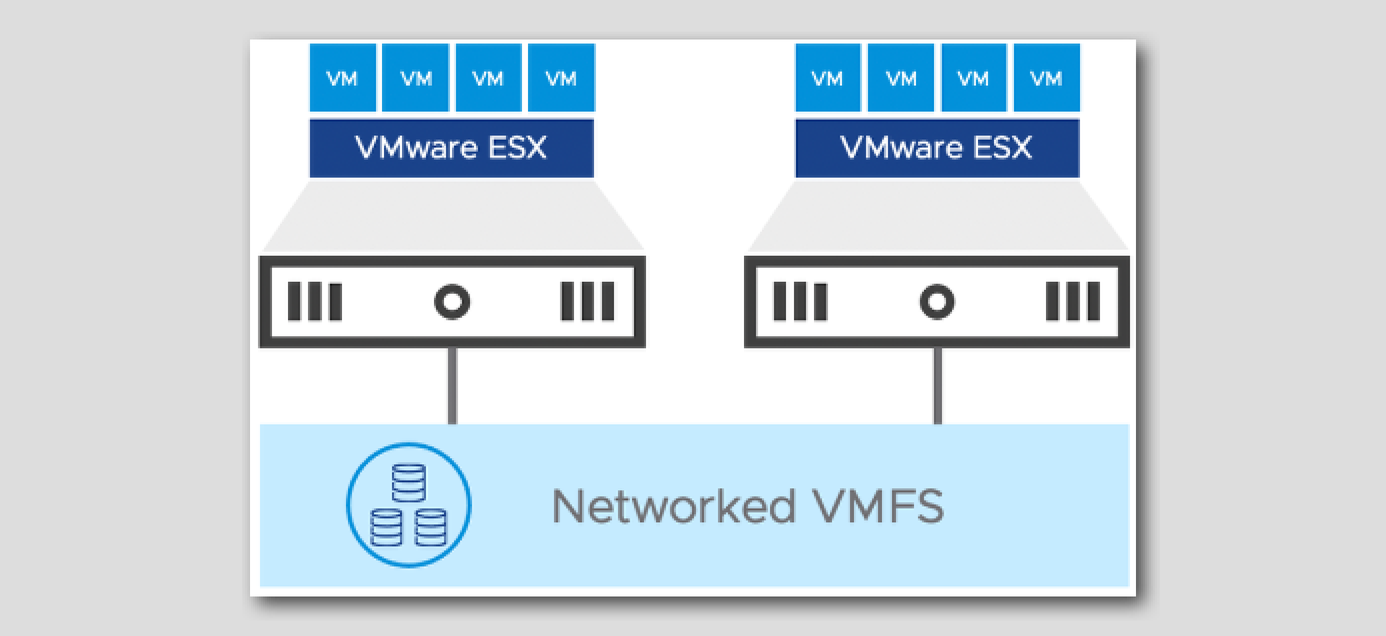
[458]



The illustration above depicts virtual machines using Local VMFS storage directly attached to a single ESXi host.

Local storage can be internal hard disks located inside your ESXi host, or it can be external storage systems located outside and connected to the host directly through protocols such as SAS or SATA.

Networked Storage

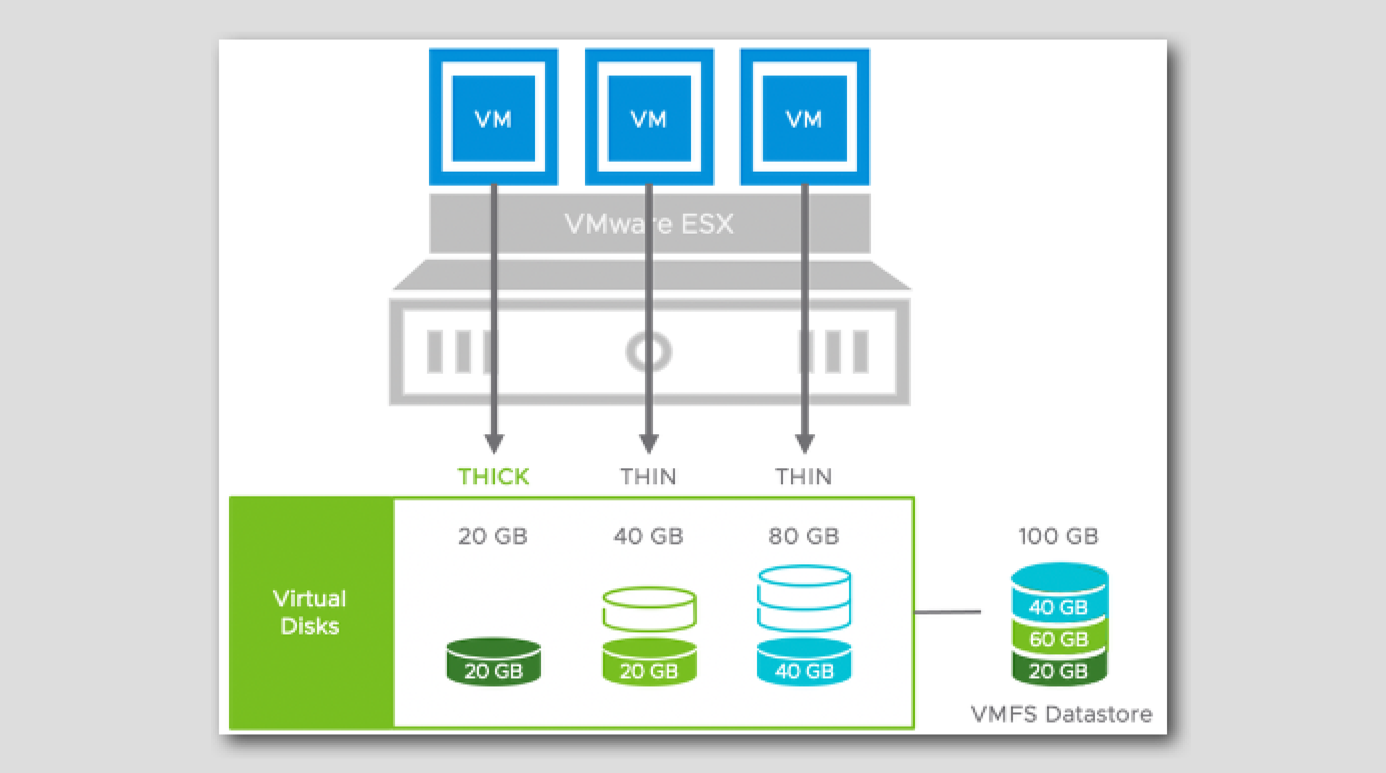


The illustration above depicts virtual machines using networked VMFS storage presented to multiple ESXi hosts.

Networked storage consists of external storage systems that your ESXi host uses to store virtual machine files remotely. Typically, the host accesses these systems over a high-speed storage network. Networked storage devices are typically shared. Datastores on networked storage devices can be accessed by multiple hosts concurrently, and as a result, enable additional vSphere technologies such as High Availability host clustering, Distributed Resource Scheduling, vMotion and Virtual Machines configured with Fault Tolerance. ESXi supports several networked storage technologies - Fiber Channel, iSCSI, NFS, and Shared SAS.

Virtual Machine Disks

[460]



The illustration above depicts virtual machines using different types of virtual disk formats against a shared VMFS Datastore.

When you perform certain virtual machine management operations, such as creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine, you can specify a provisioning policy for the virtual disk file format. There are three types of virtual disk formats:

Thin Provision

Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

Thick Provision Lazy Zeroed

Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.

Using the thick-provision, lazy-zeroed format does not zero out or eliminate the possibility of recovering deleted files or restoring old data that might be present on this allocated space. You cannot convert a thick-provisioned, lazy-zeroed disk to a thin disk.

Thick Provision Eager Zeroed

A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick-provision, lazy-zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. In general, it takes much longer to create disks in this format than to create other types of disks.

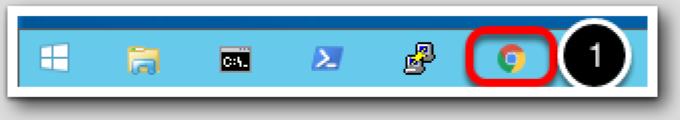
Creating and Configuring vSphere Datastores

[461]

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

Launch Google Chrome web browser

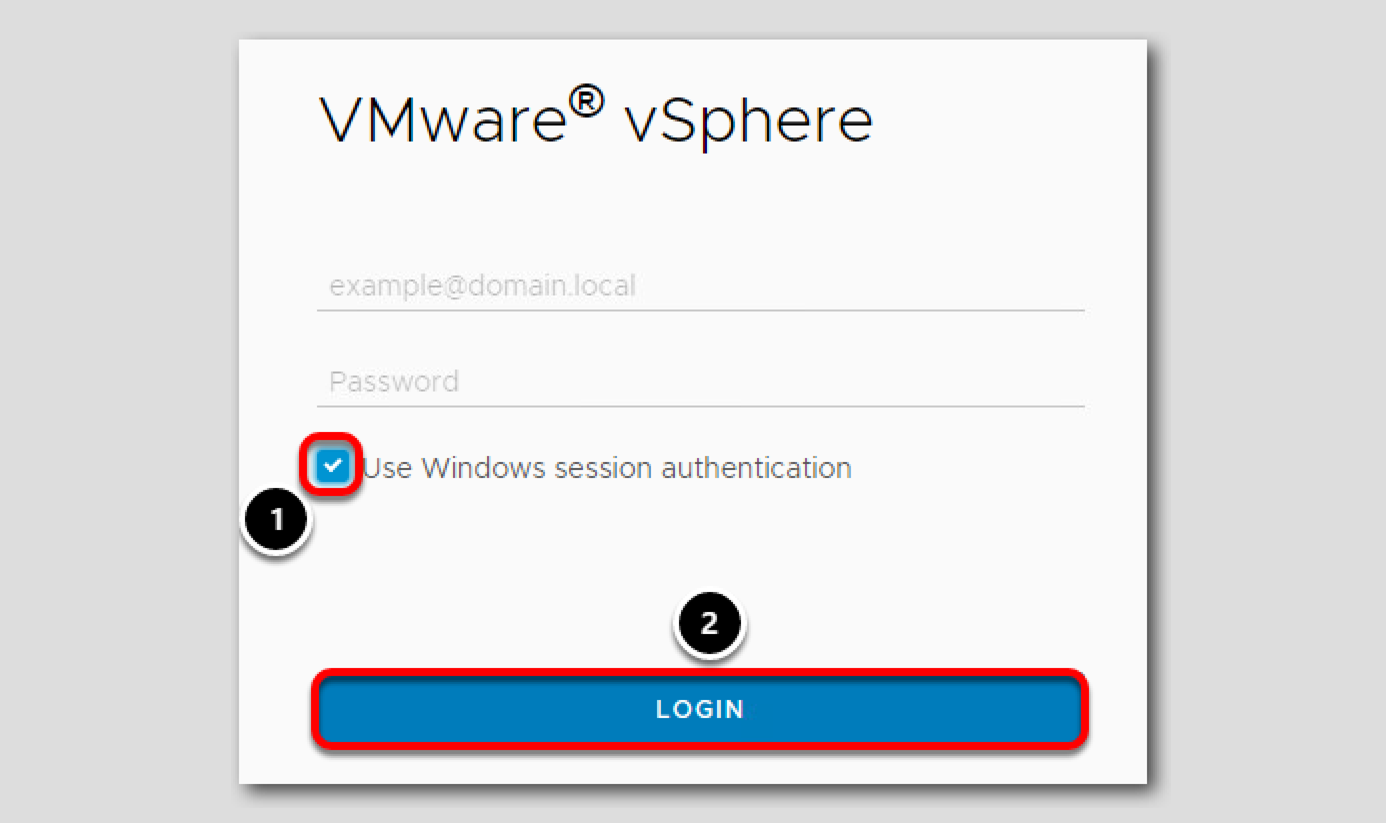
[462]



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

Enter credentials and log in

[463]



VMware® vSphere

example@domain.local

Password

☑ Use Windows session authentication

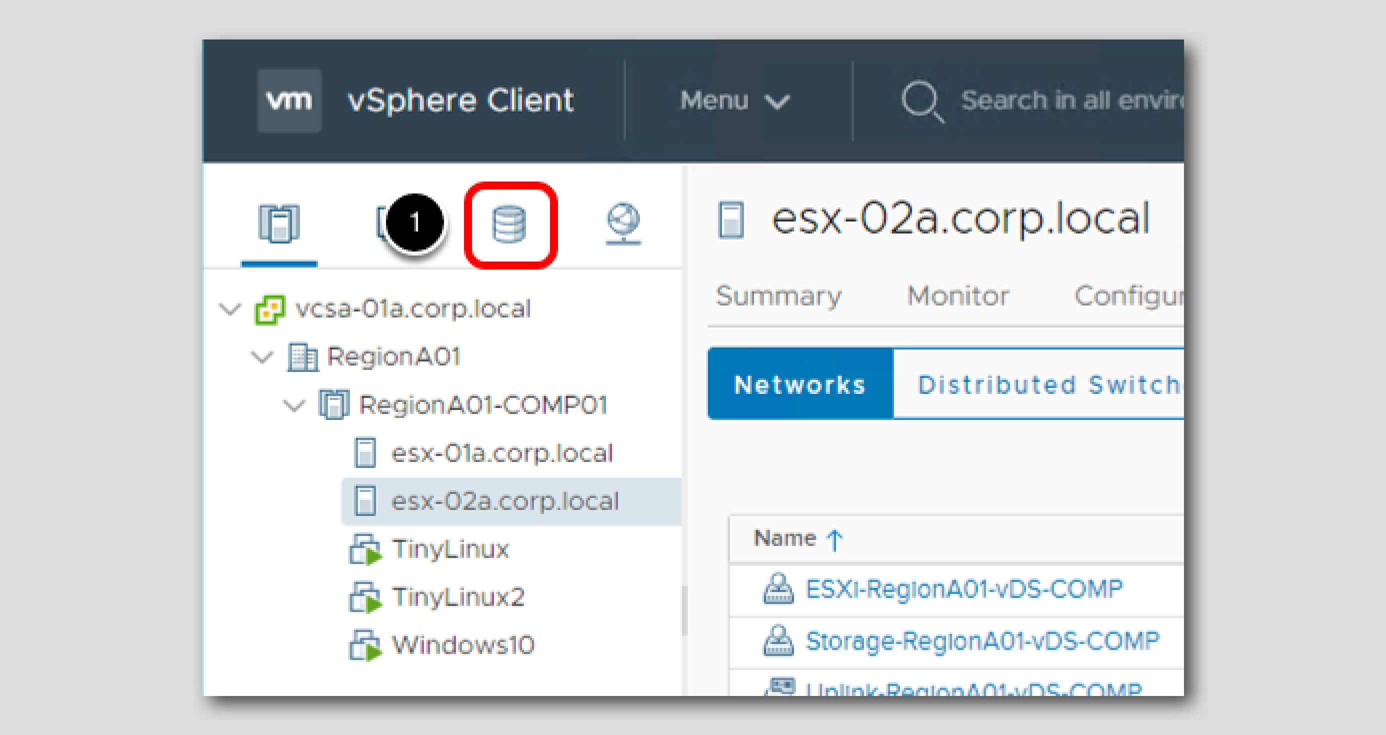
1. Select "Use Windows session authentication" check box
2. Select Login

If credentials aren't saved, use the following:

- username: administrator@corp.local
- password: VMware1!

Navigate to Storage Management

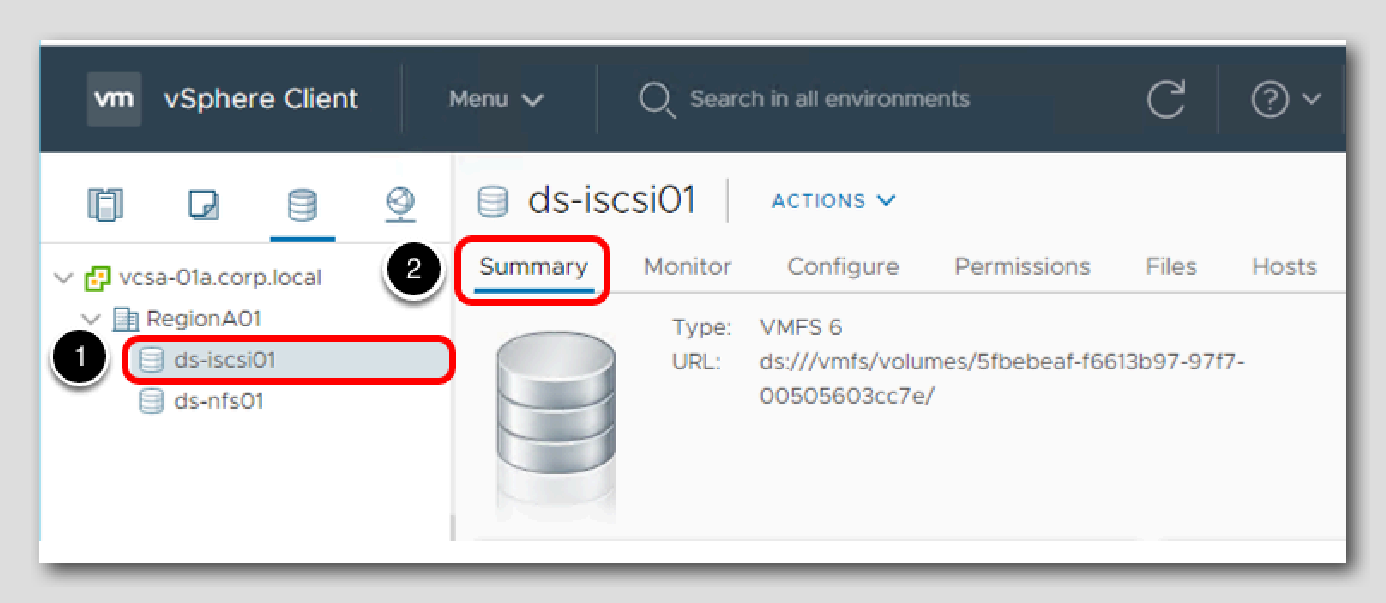
[464]



1. Select the **Storage** tab.

Expand RegionA01 Datacenter

[465]



Type: VMFS 6

URL: ds:///vmfs/volumes/5fbebeaf-f6613b97-97f7-00505603cc7e/

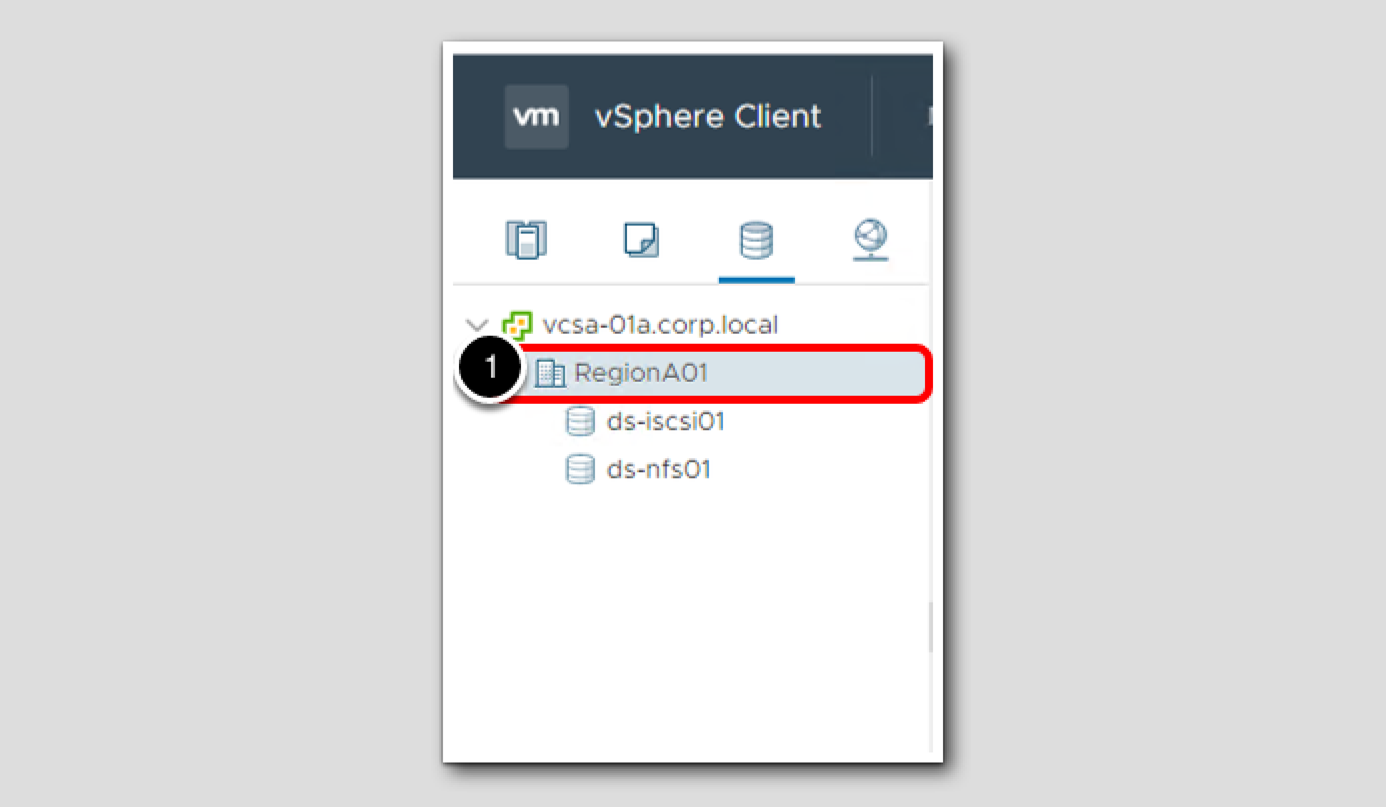
There are 2 storage datastores configured, an ISCSI datastore and an NFS datastore.

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

[466]

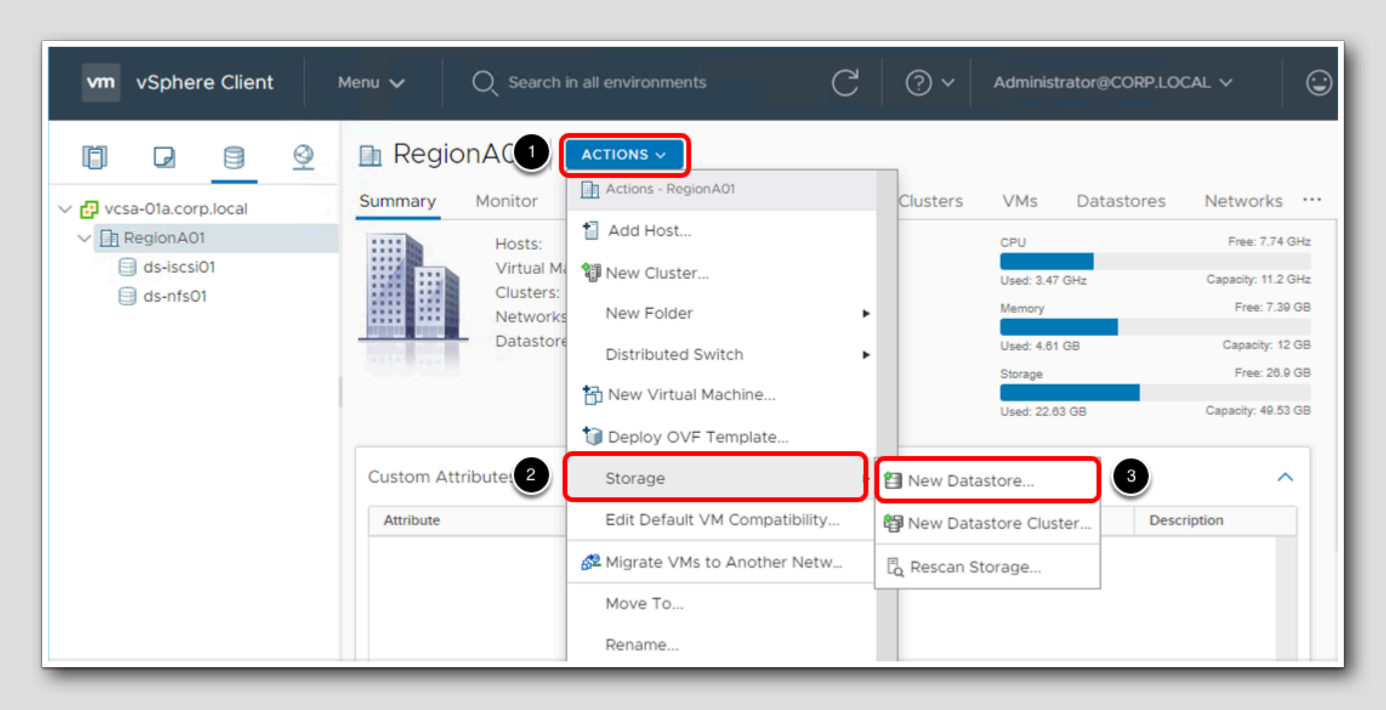


In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select **RegionA01** Datacenter.

New Datastore

[467]

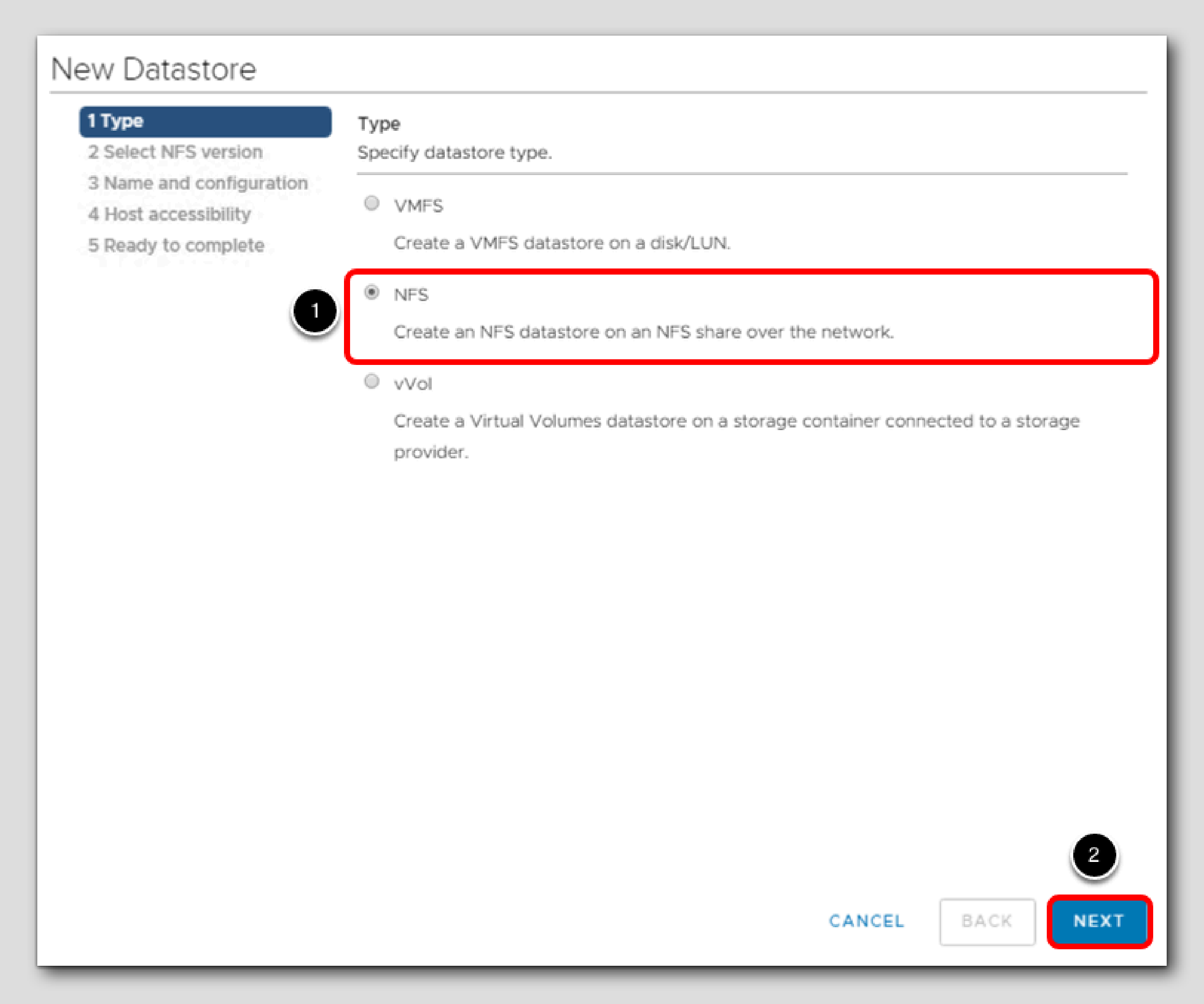


In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select Actions.
2. Select Storage.
3. Select New Datastore.

New Datastore - Type

[468]



New Datastore

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

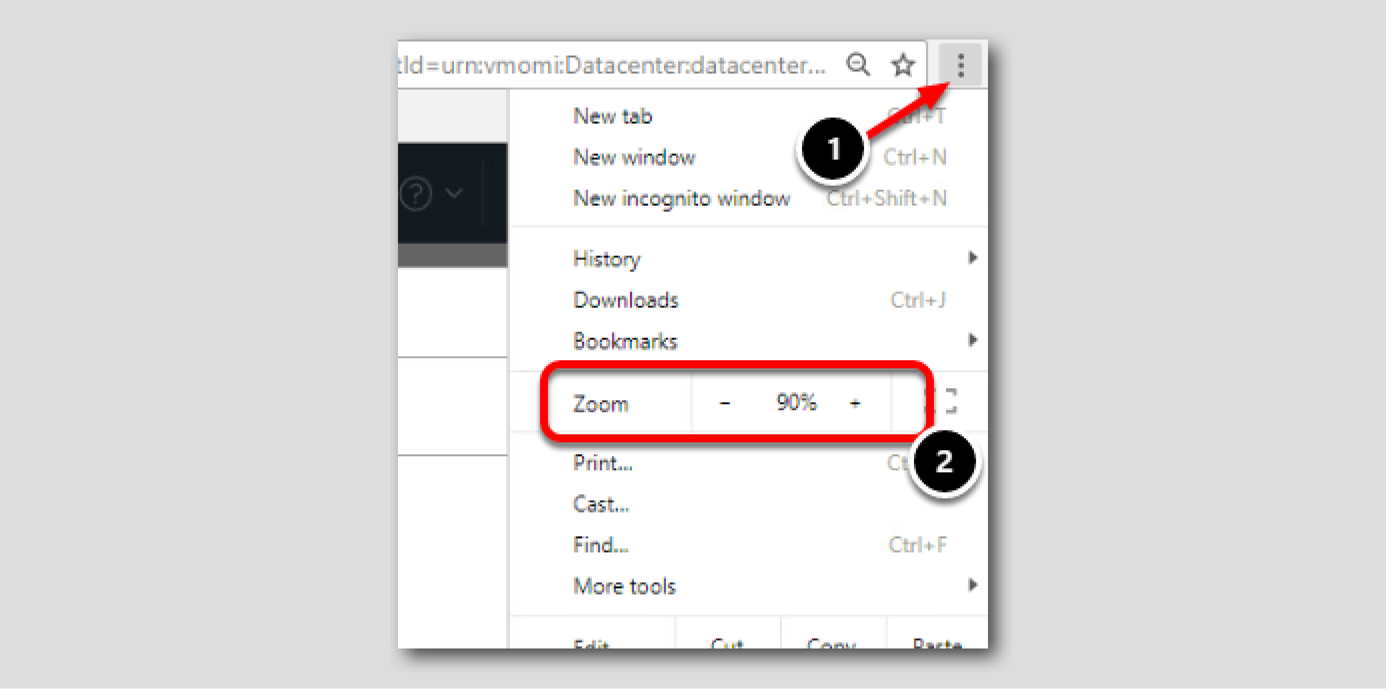
Type
Specify datastore type.

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

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

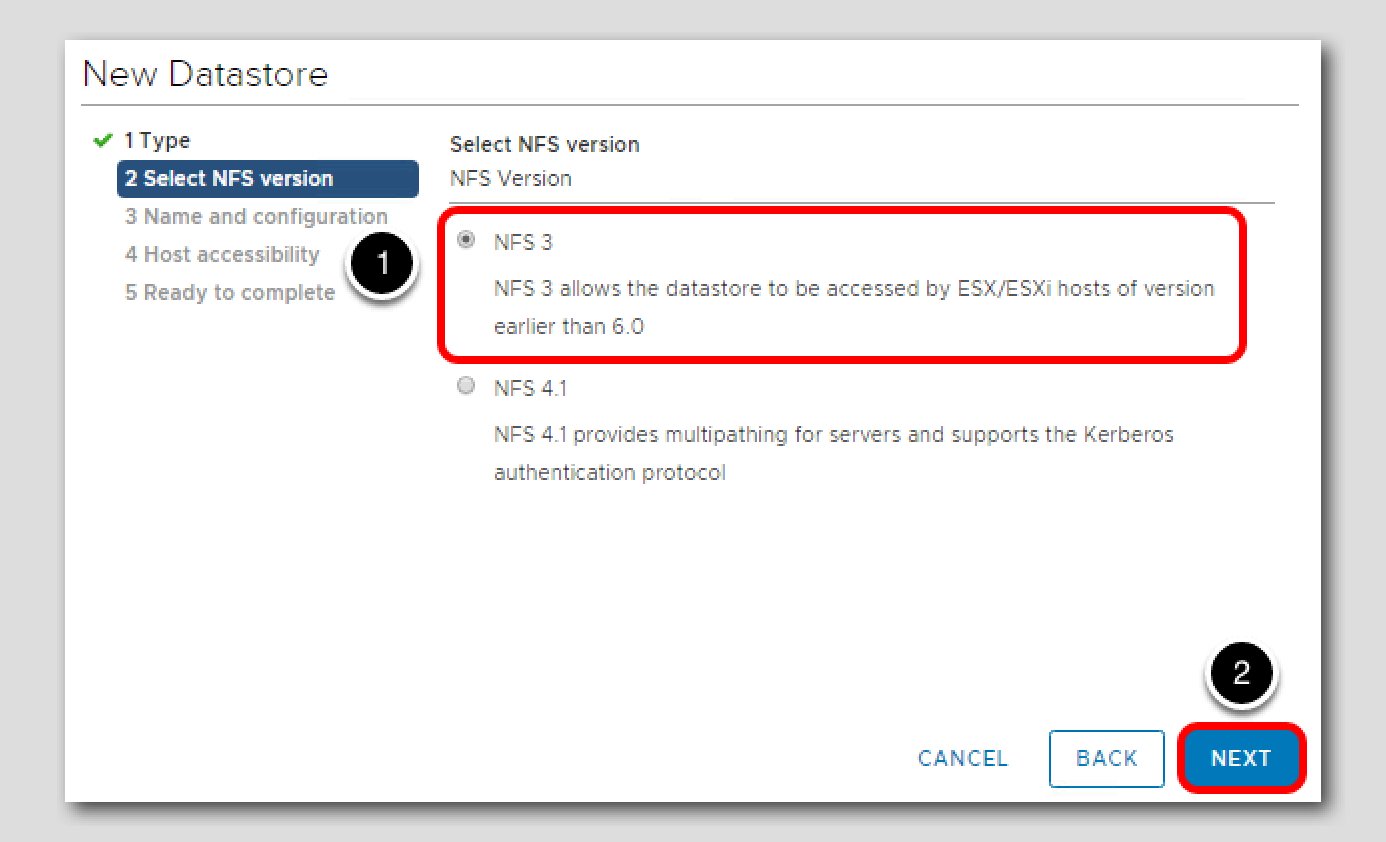
○ vVol
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

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



New Datastore

✓ 1 Type

2 Select NFS version

3 Name and configuration

4 Host accessibility

5 Ready to complete

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

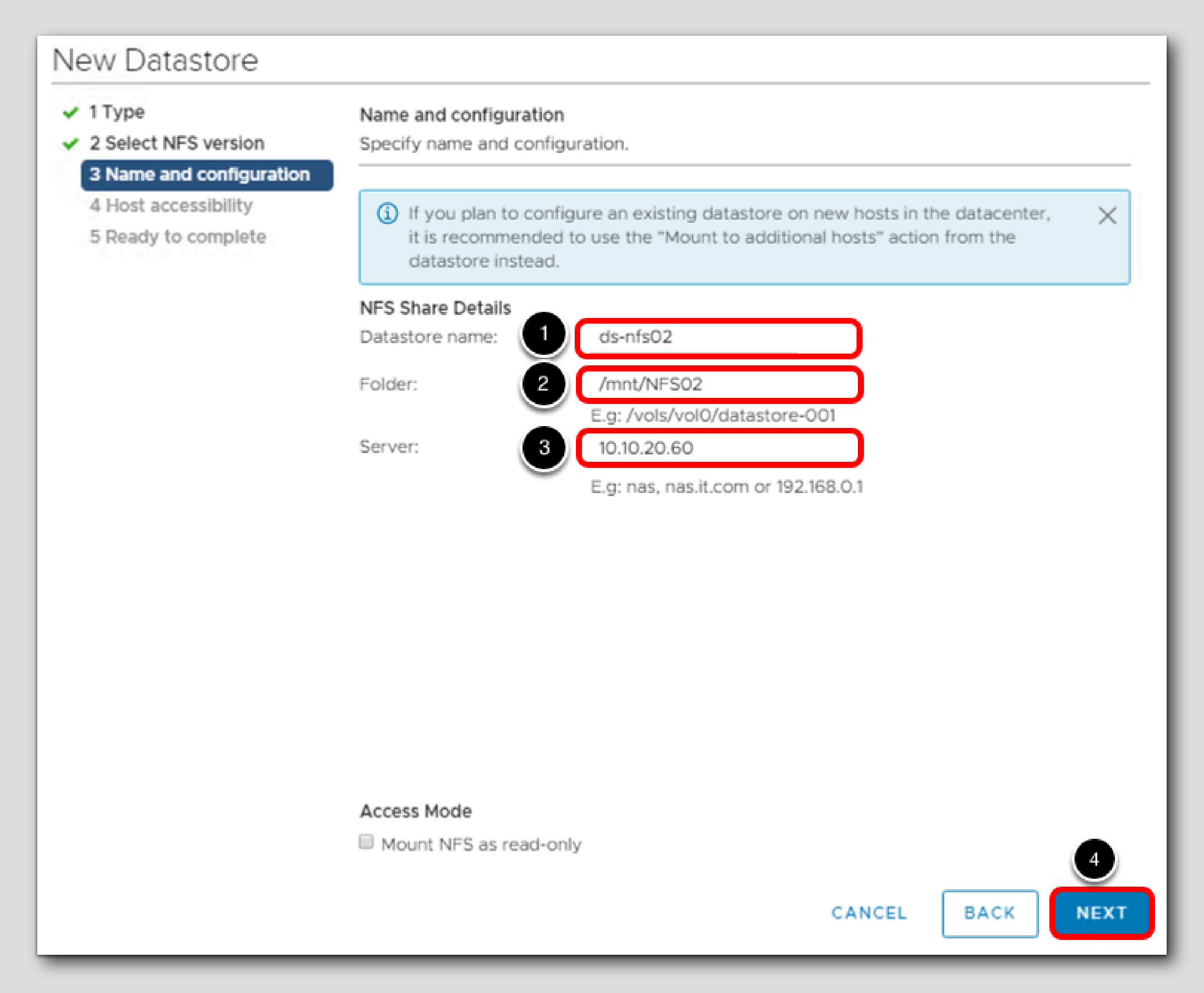
○ NFS 4.1

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

1. Verify NFS Version - NFS 3
2. Click Next

New Datastore - Name and configuration

[470]



New Datastore

Name and configuration

Specify name and configuration.

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.

NFS Share Details

1 Datastore name: ds-nfs02

2 Folder: /mnt/NFS02

E.g: /vols/vol0/datastore-001

3 Server: 10.10.20.60

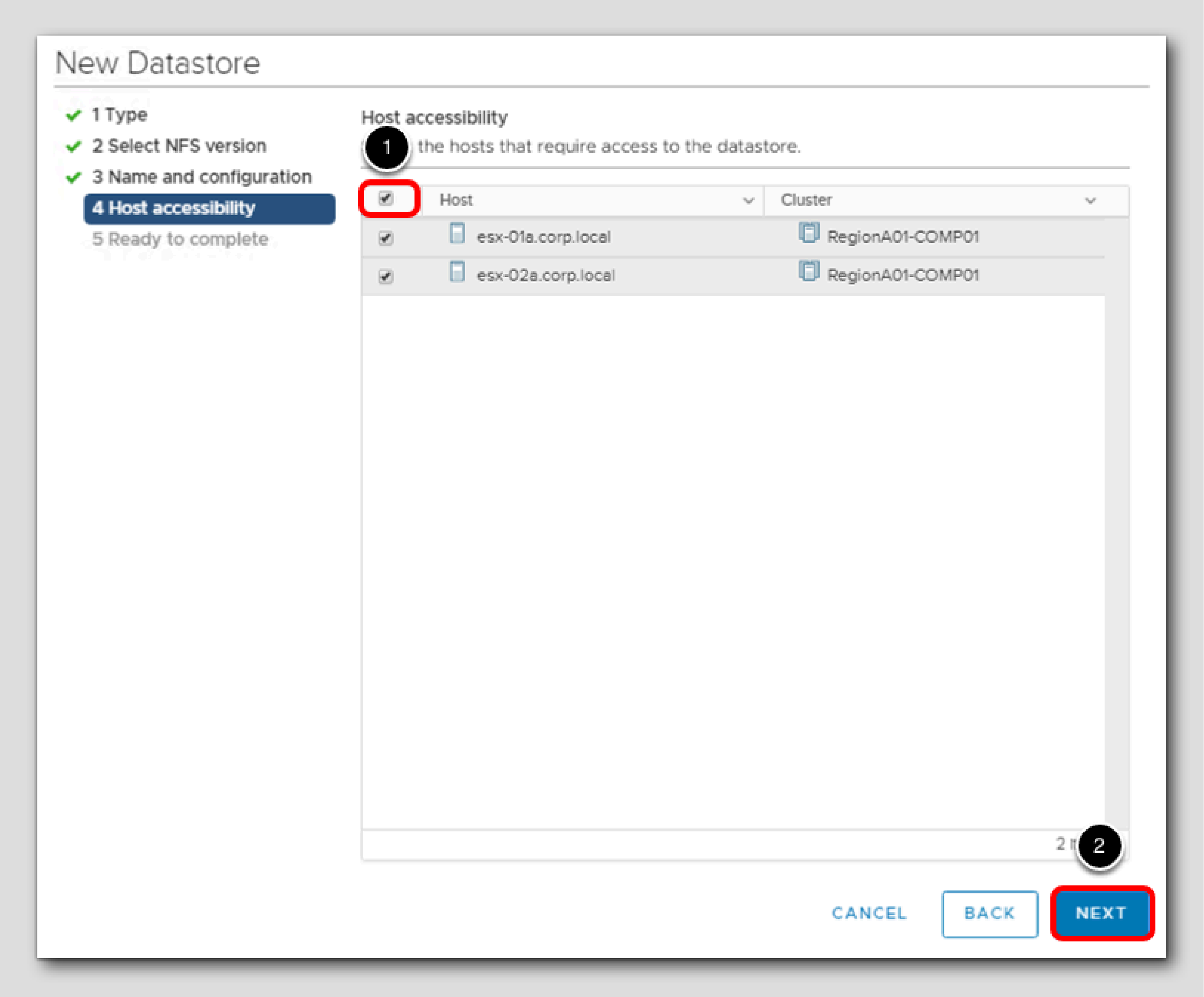
E.g: nas, nas.it.com or 192.168.0.1

Access Mode

□ Mount NFS as read-only

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

Host accessibility

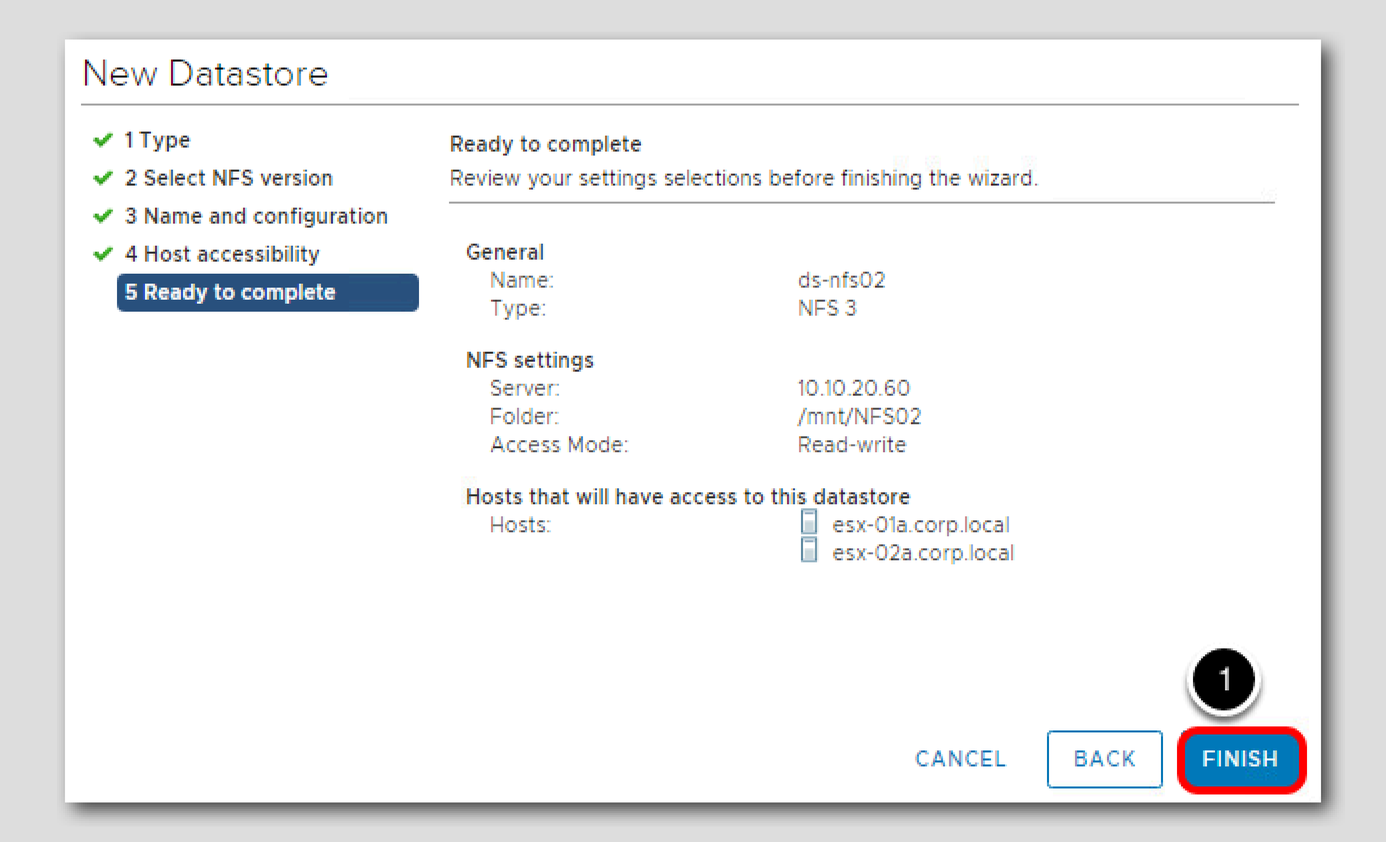
the hosts that require access to the datastore.

☑	Host	Cluster
☑	esx-01a.corp.local	RegionA01-COMP01
☑	esx-02a.corp.local	RegionA01-COMP01

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

New Datastore - Ready to complete

[472]



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

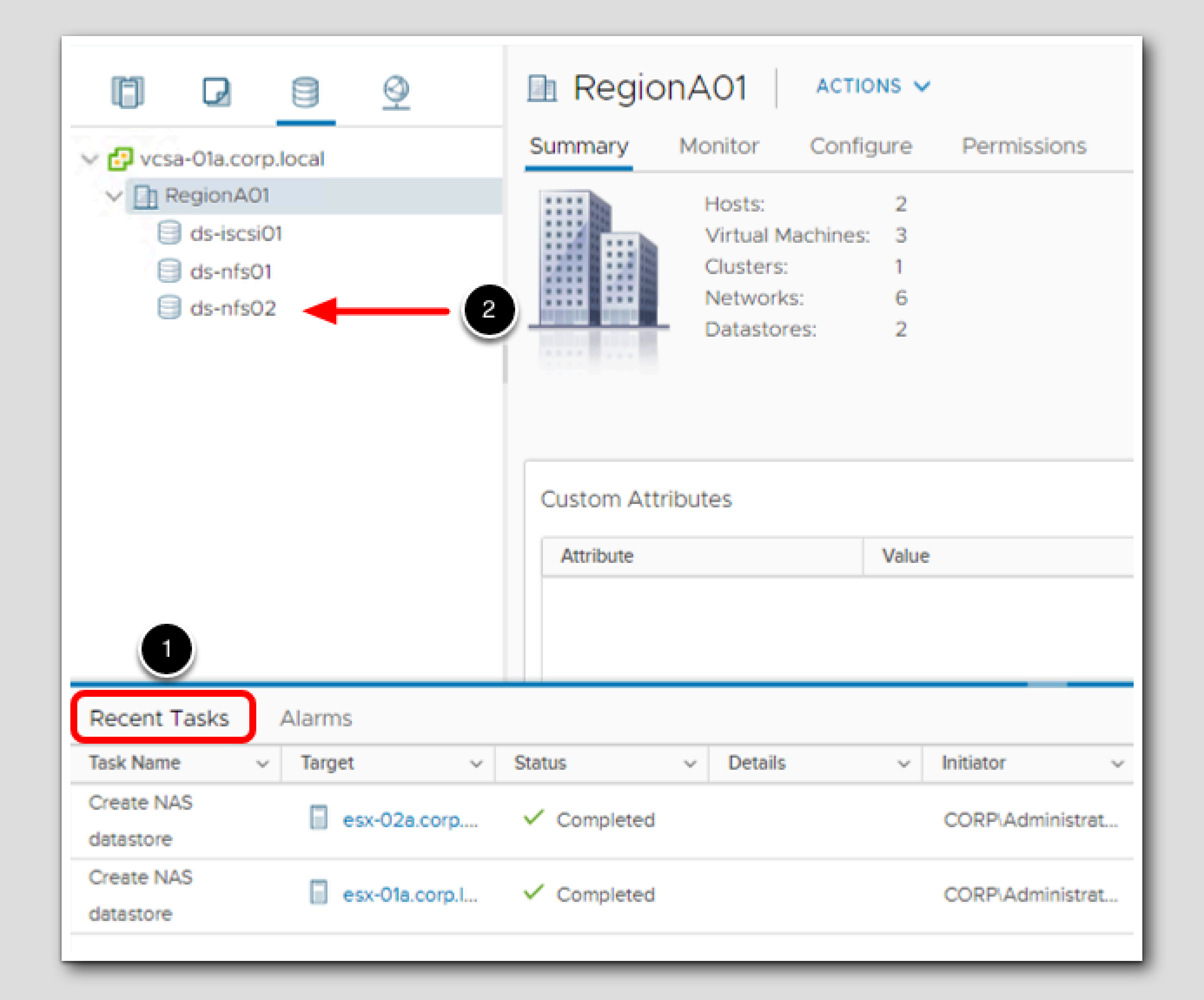
Server:	10.10.20.60
Folder:	/mnt/NFS02
Access Mode:	Read-write

Hosts that will have access to this datastore

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

1. Review New Datastore configuration and click Finish.

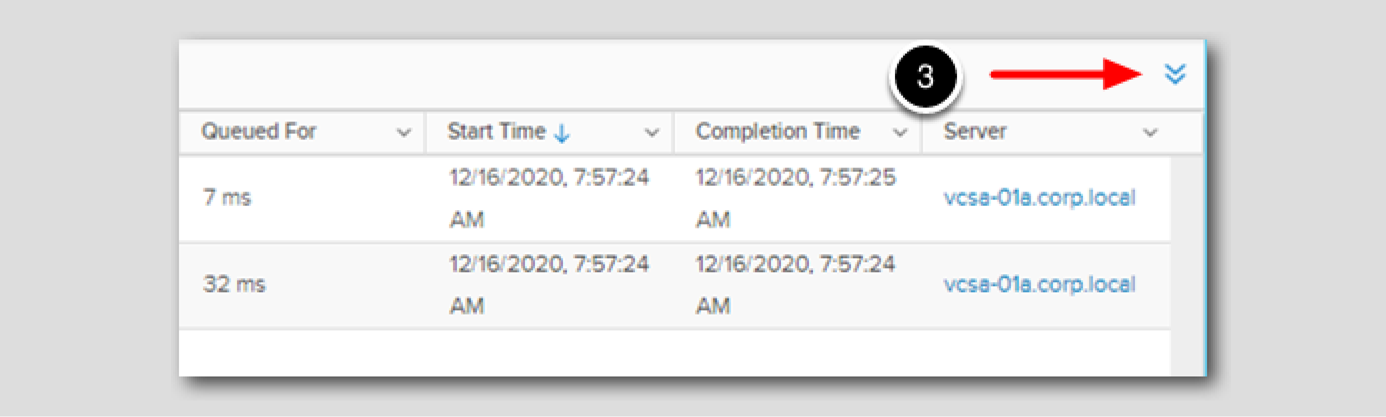
Monitor task progress



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

Task Name	Target	Status	Details	Initiator
Create NAS datastore	esx-02a.corp....	✓ Completed		CORP\Administrat...
Create NAS datastore	esx-01a.corp.l...	✓ Completed		CORP\Administrat...

1. You can follow the progress in the Recent Tasks pane (by clicking on Recent Tasks)
2. When complete, you should see the new ds-nfs02 Datastore available for use

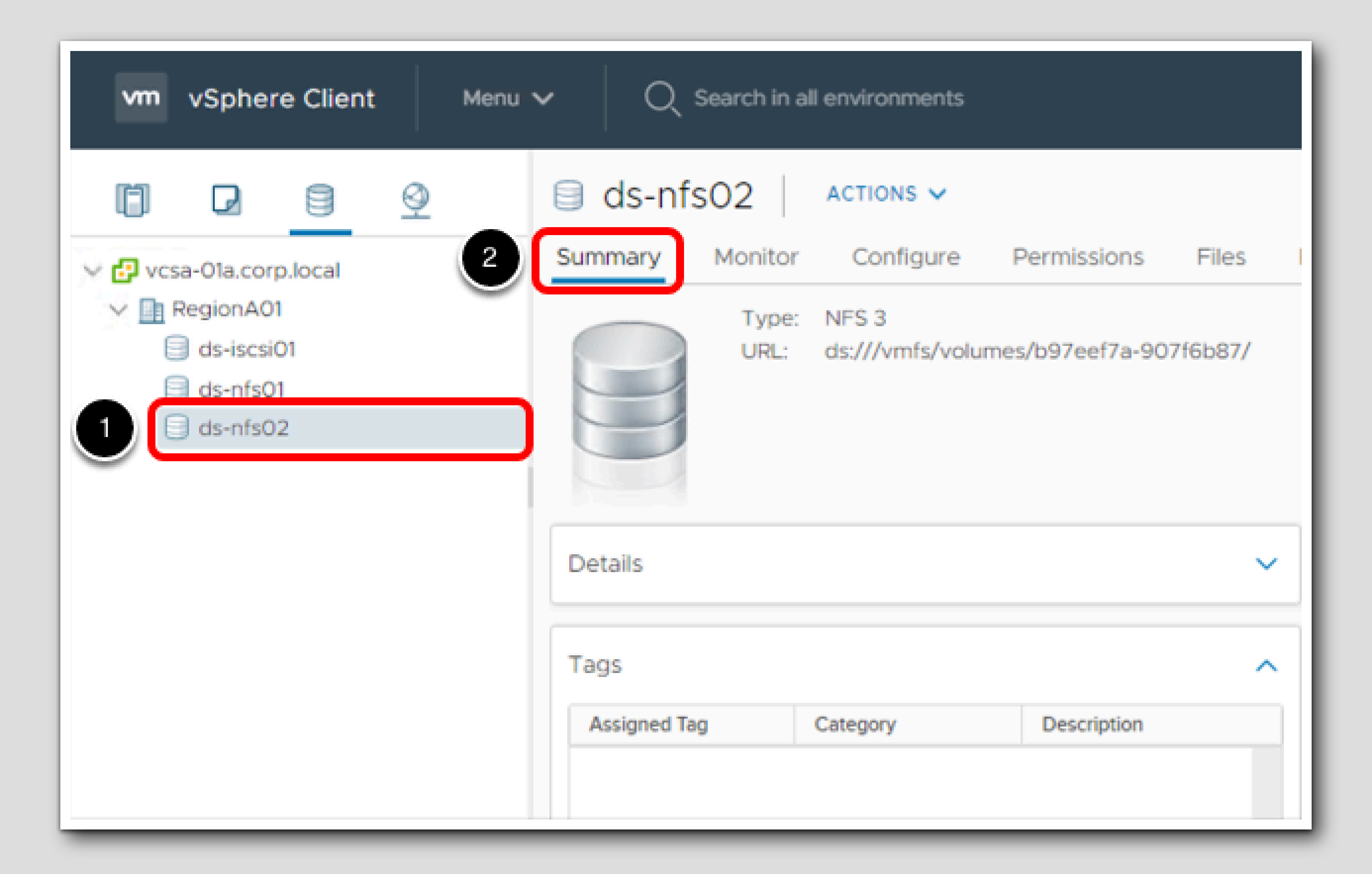


Queued For	Start Time ↓	Completion Time	Server
7 ms	12/16/2020, 7:57:24 AM	12/16/2020, 7:57:25 AM	vcsa-01a.corp.local
32 ms	12/16/2020, 7:57:24 AM	12/16/2020, 7:57:24 AM	vcsa-01a.corp.local

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

Review new Datastore Settings

[474]



Type: NFS 3

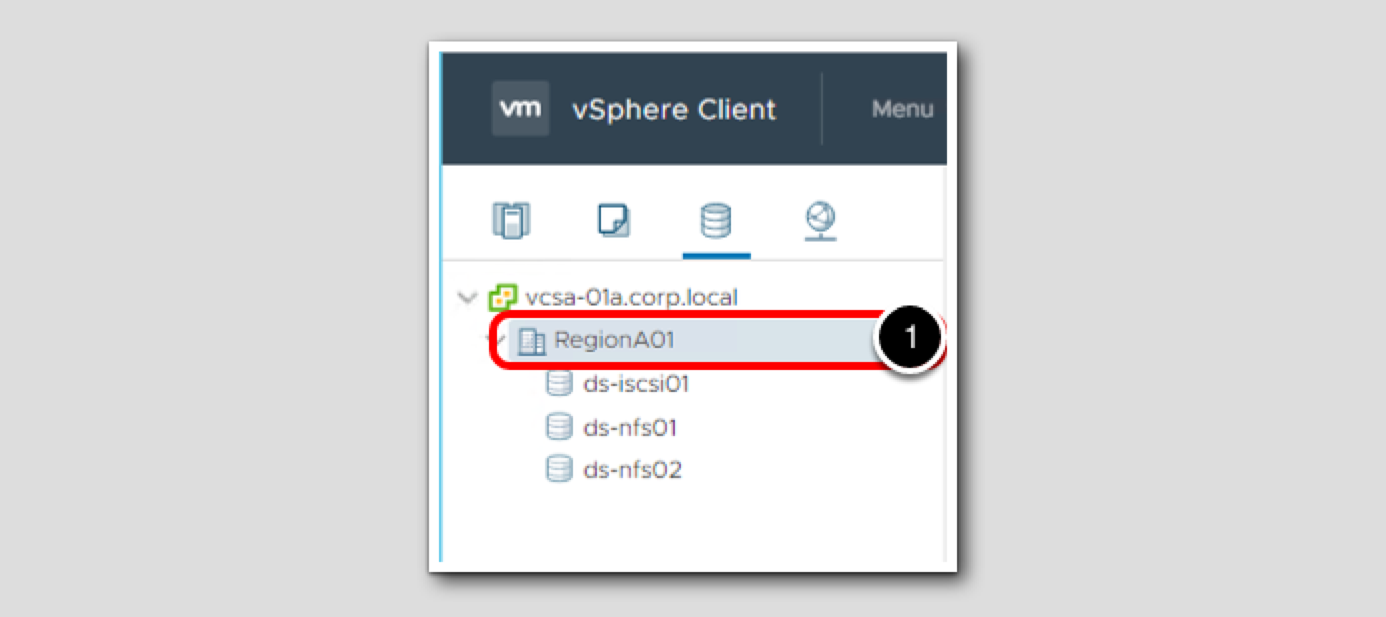
URL: ds:///vmfs/volumes/b97eef7a-907f6b87/

Assigned Tag	Category	Description

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

Create a vSphere iSCSI Datastore

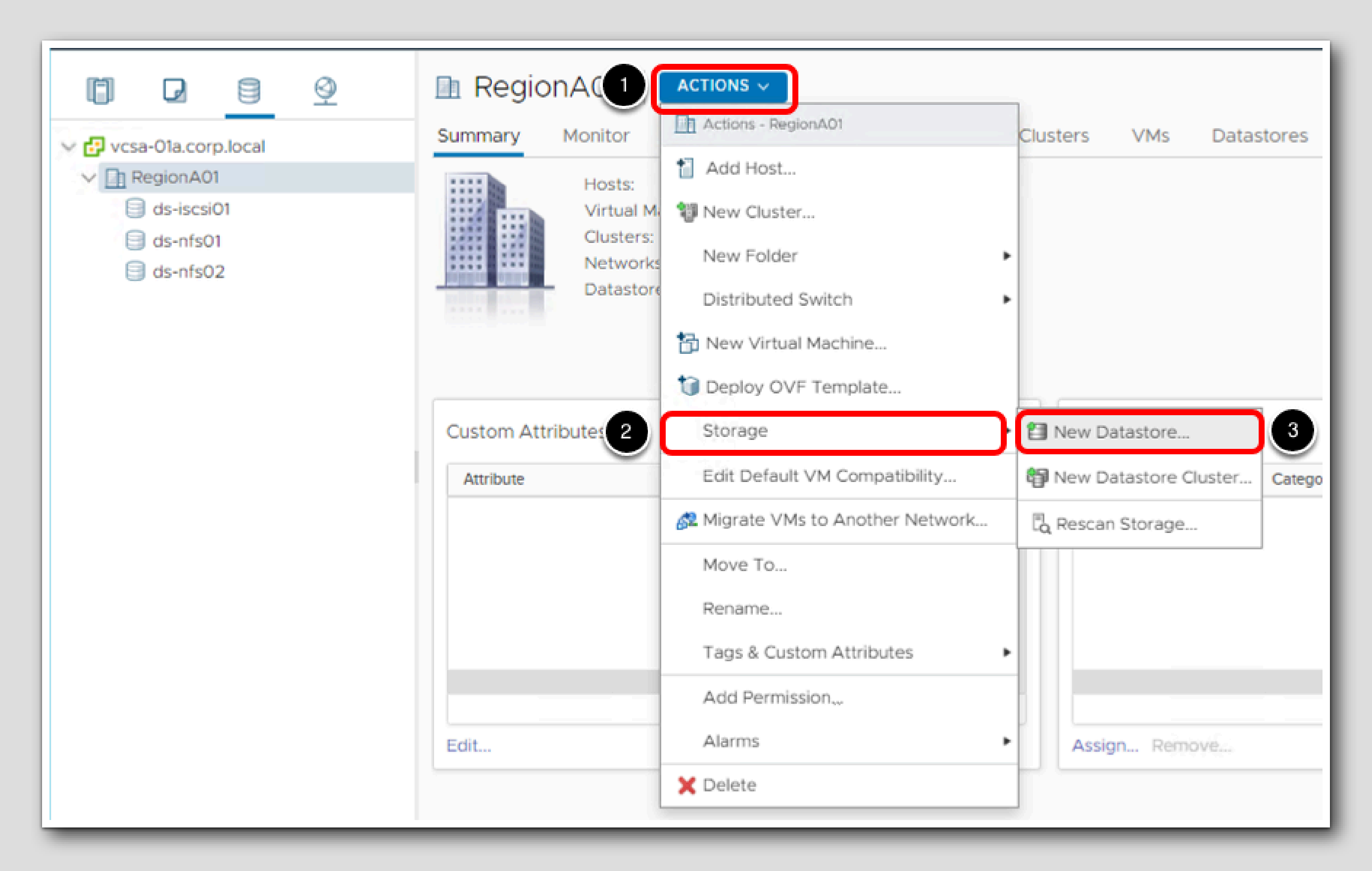
[475]



1. Select **RegionA01** Datacenter.

New Datastore

[476]

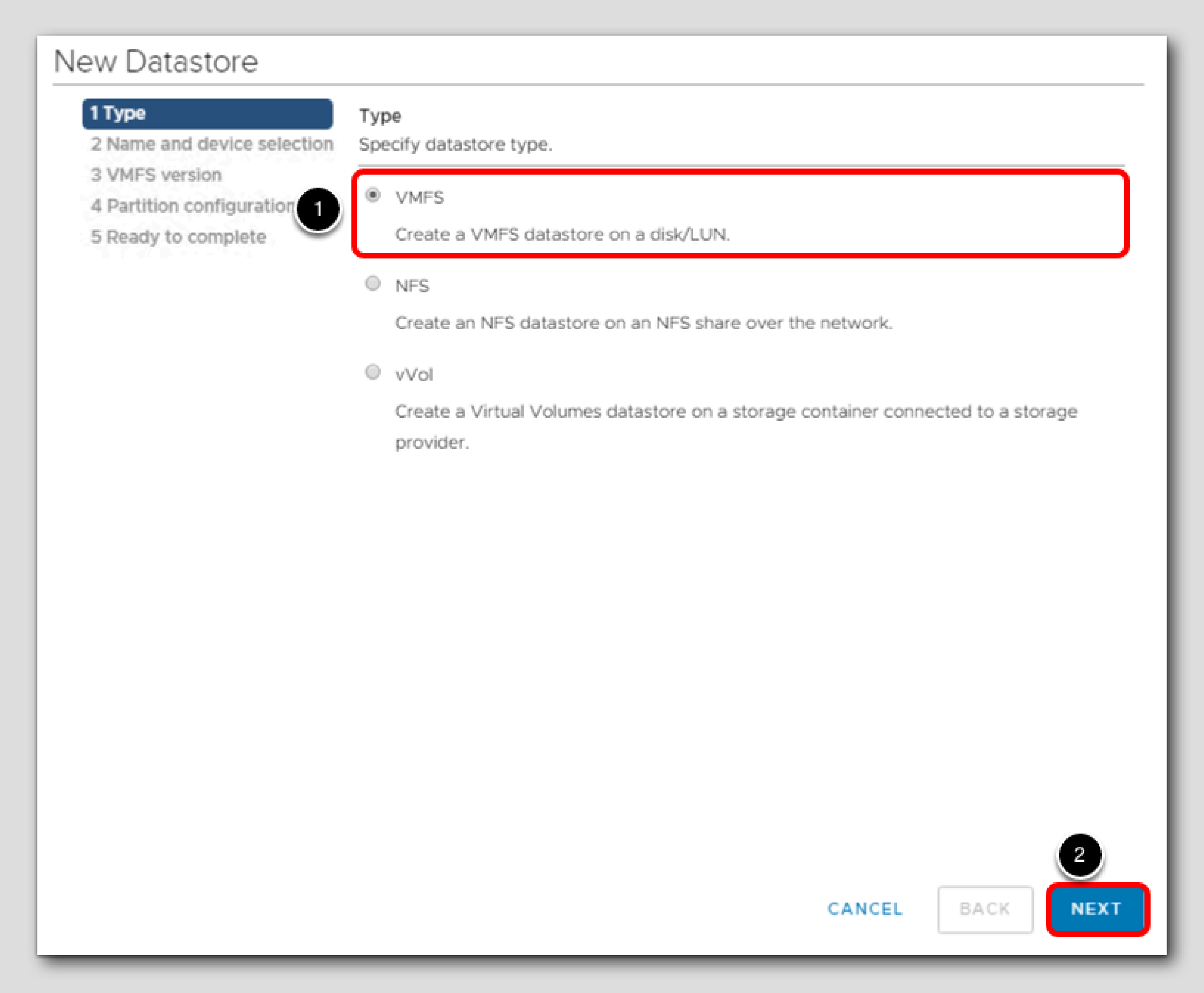


In this section, you will create a new vSphere iSCSI Datastore with a pre-provisioned iSCSI LUN.

1. Select Actions.
2. Select Storage.
3. Select New Datastore.

New Datastore - Type

[477]



New Datastore

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

Type

Specify datastore type.

● VMFS

Create a VMFS datastore on a disk/LUN.

○ NFS

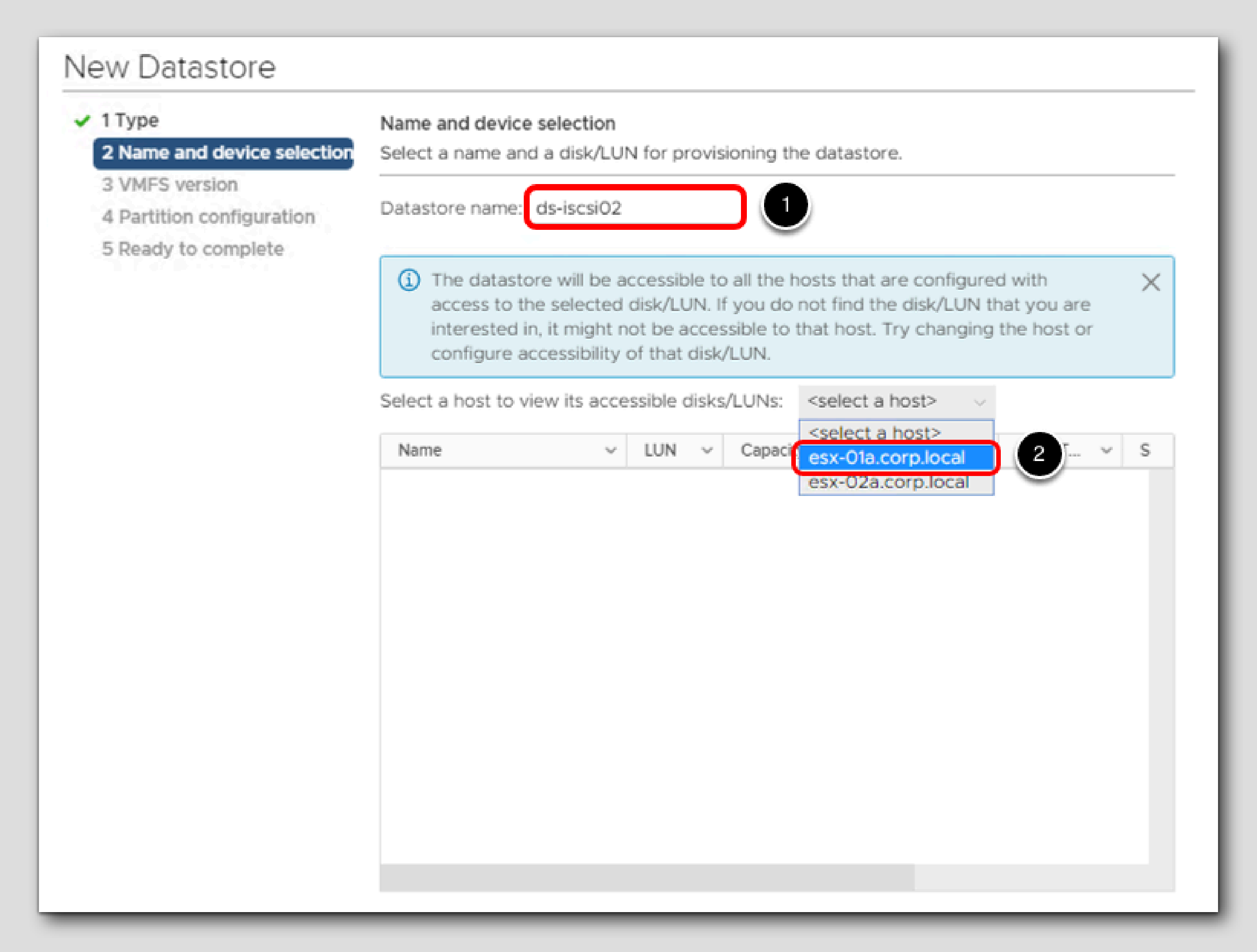
Create an NFS datastore on an NFS share over the network.

○ vVol

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

1. Verify **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

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.

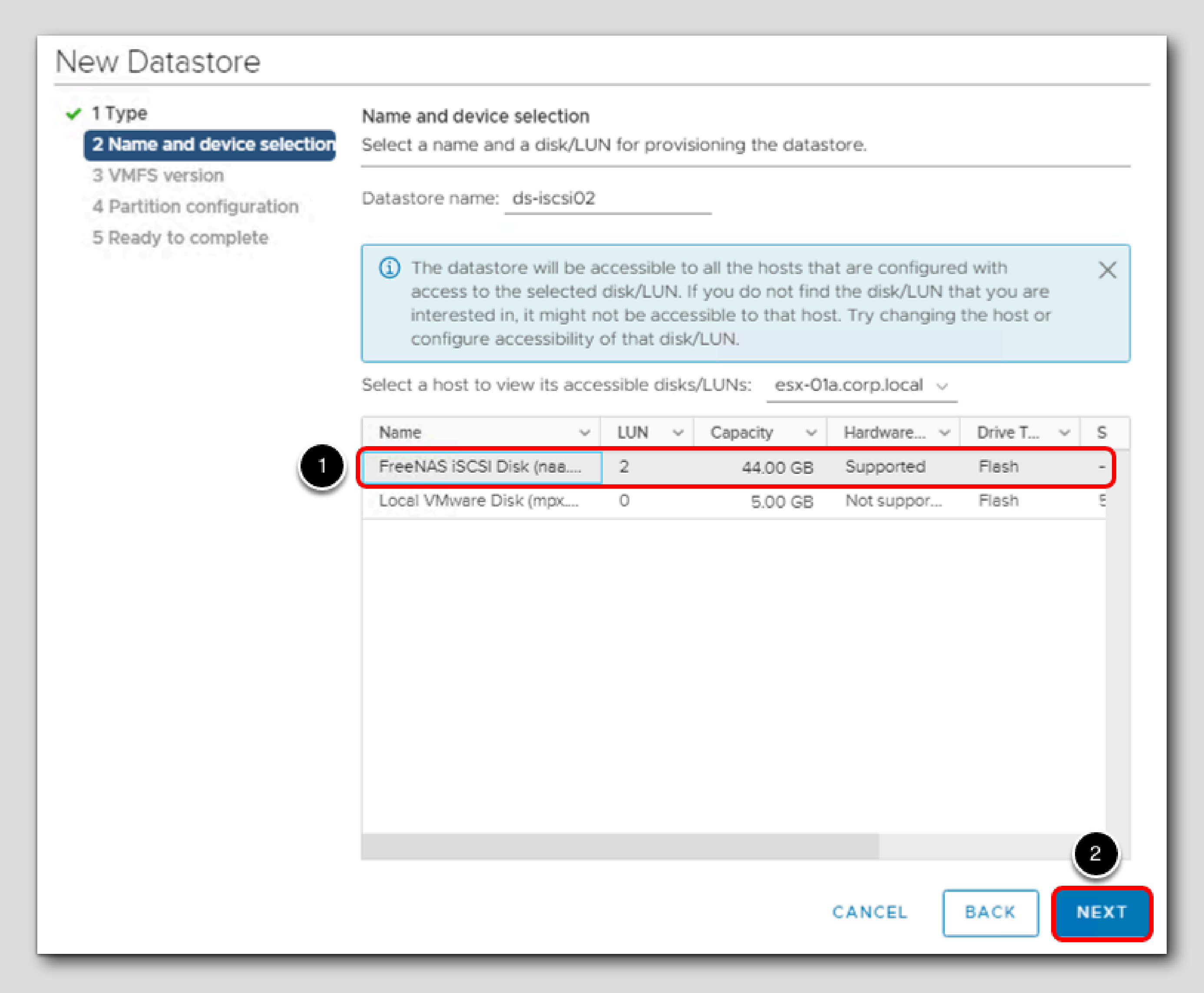
Select a host to view its accessible disks/LUNs: <select a host>

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.)

[479]



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

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: esx-01a.corp.local

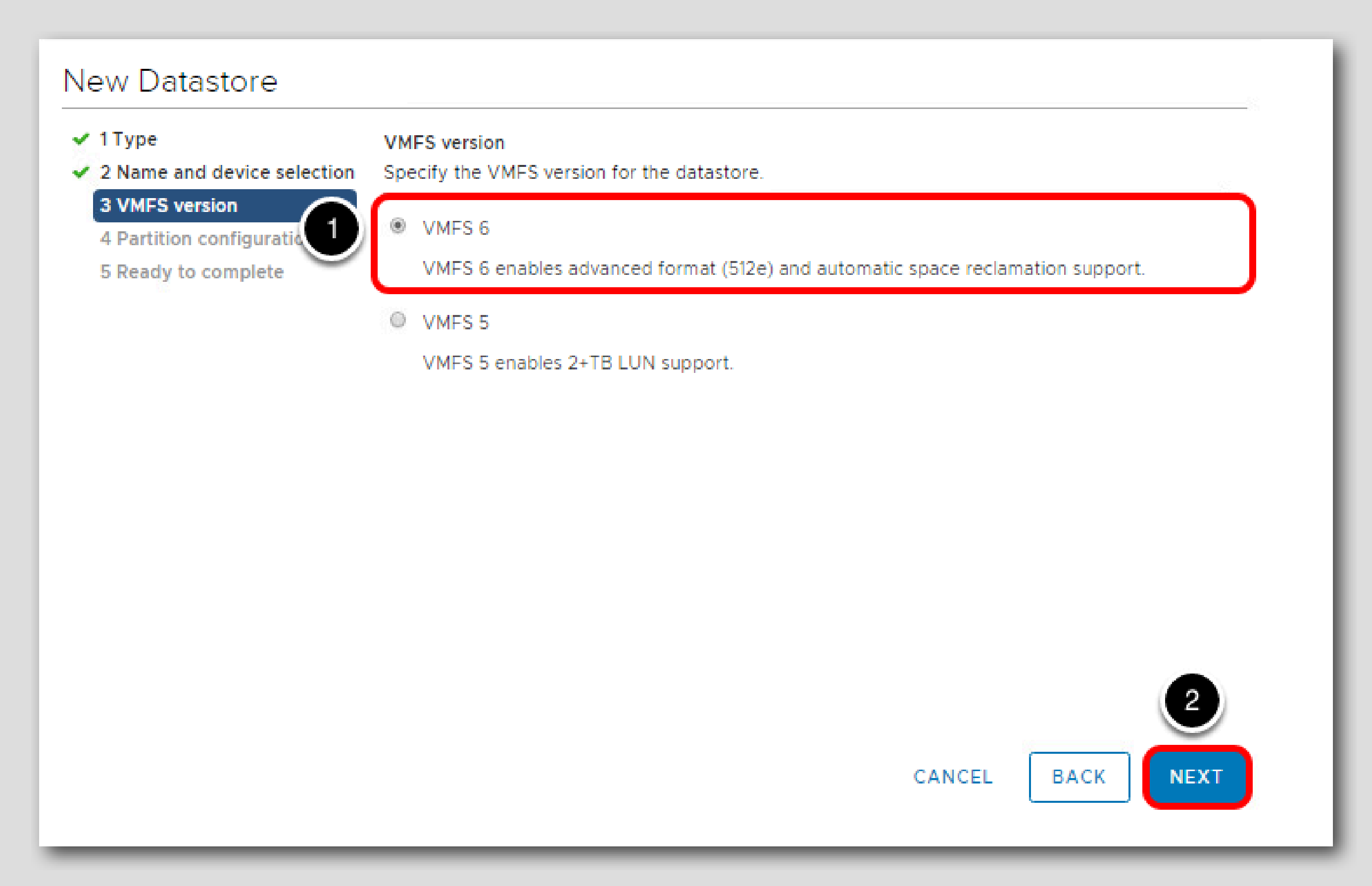
Name	LUN	Capacity	Hardware...	Drive T...	S
FreeNAS iSCSI Disk (naa....	2	44.00 GB	Supported	Flash	-
Local VMware Disk (mpx....	0	5.00 GB	Not suppor...	Flash	S

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

[480]



New Datastore

VMFS version

Specify the VMFS version for the datastore.

● VMFS 6

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

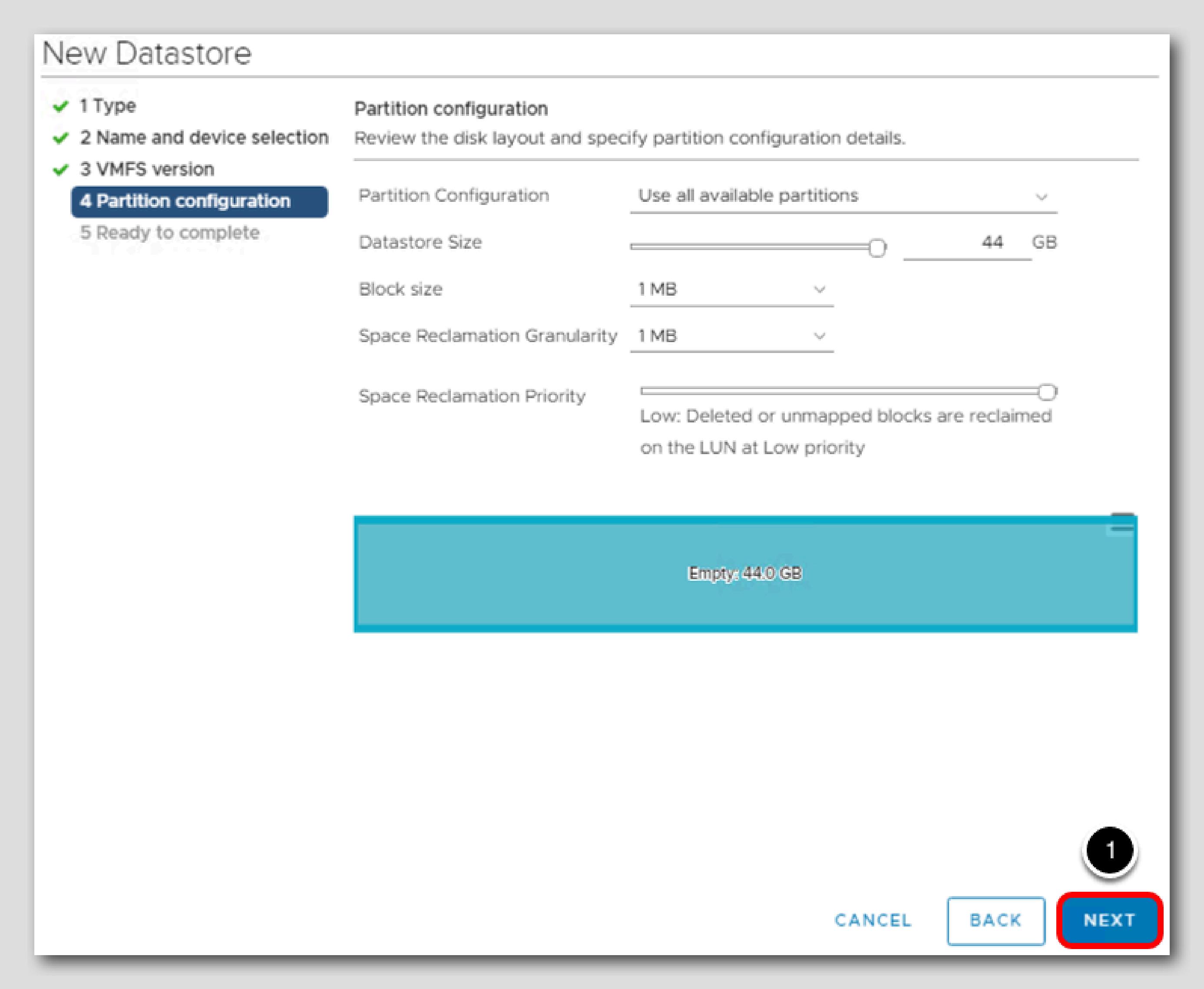
○ VMFS 5

VMFS 5 enables 2+TB LUN support.

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

New Datastore - Partition Configuration

[481]



New Datastore

Partition configuration

Review the disk layout and specify partition configuration details.

Partition Configuration: Use all available partitions

Datastore Size: 44 GB

Block size: 1 MB

Space Reclamation Granularity: 1 MB

Space Reclamation Priority: Low: Deleted or unmapped blocks are reclaimed on the LUN at Low priority

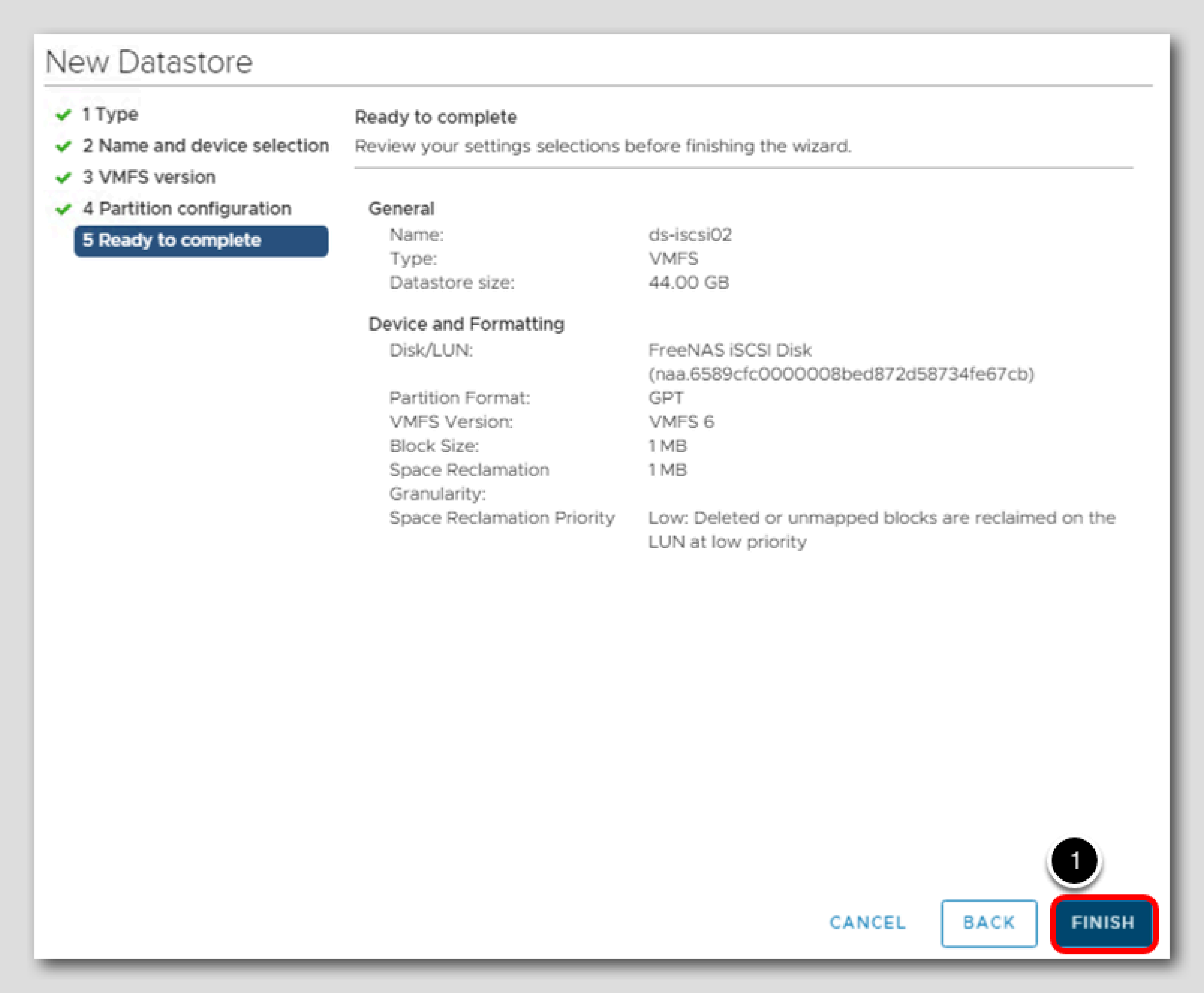
Empty: 44.0 GB

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

[482]



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

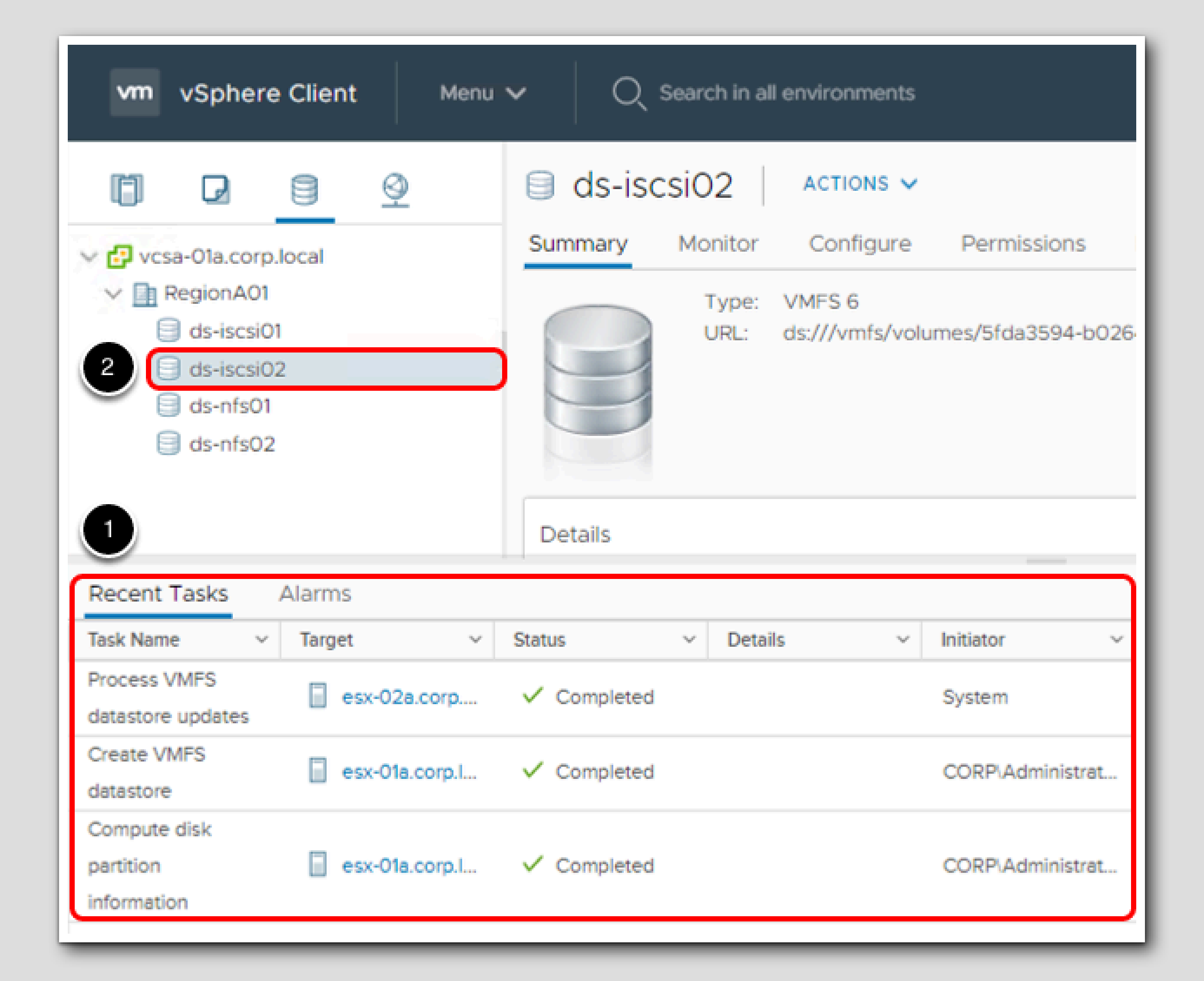
Name:	ds-iscsi02
Type:	VMFS
Datastore size:	44.00 GB

Device and Formatting

Disk/LUN:	FreeNAS iSCSI Disk (naa.6589cfc0000008bed872d58734fe67cb)
Partition Format:	GPT
VMFS Version:	VMFS 6
Block Size:	1 MB
Space Reclamation Granularity:	1 MB
Space Reclamation Priority	Low: Deleted or unmapped blocks are reclaimed on the LUN at low priority

1. Review New Datastore configuration and click Finish.

New Datastore - Monitor task progress



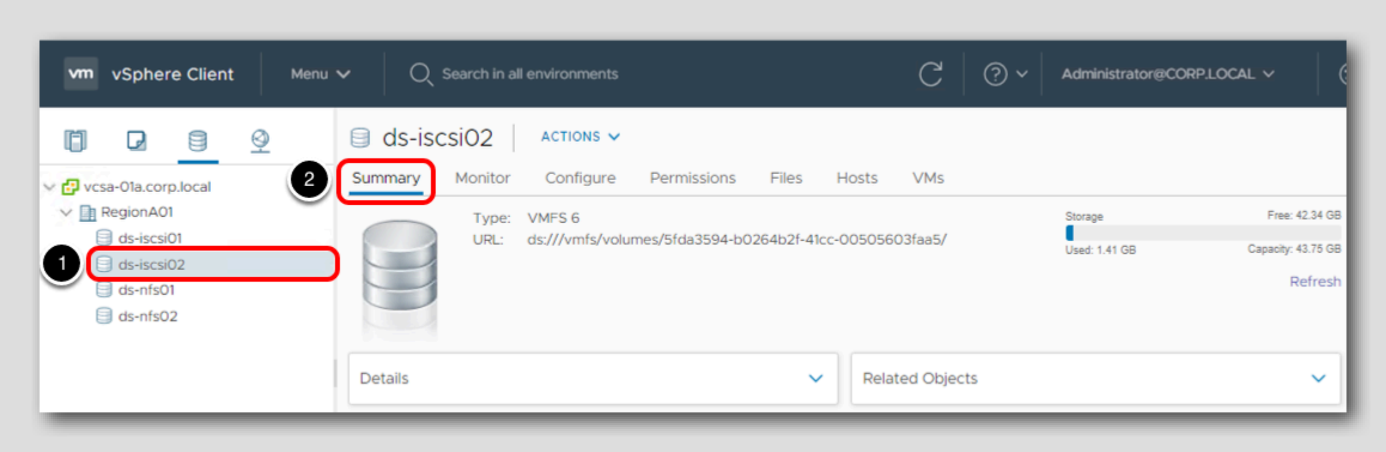
Type: VMFS 6
URL: ds:///vmfs/volumes/5fda3594-b026

Task Name	Target	Status	Details	Initiator
Process VMFS datastore updates	esx-02a.corp....	✓ Completed		System
Create VMFS datastore	esx-01a.corp.l...	✓ Completed		CORP\Administrat...
Compute disk partition information	esx-01a.corp.l...	✓ Completed		CORP\Administrat...

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

New Datastore - Review Settings

[484]



Type: VMFS 6
URL: ds:///vmfs/volumes/5fda3594-b0264b2f-41cc-00505603faa5/

1. Select the datastore ds-iscsi02 from the inventory list
2. Select Summary to review capacity and configuration details

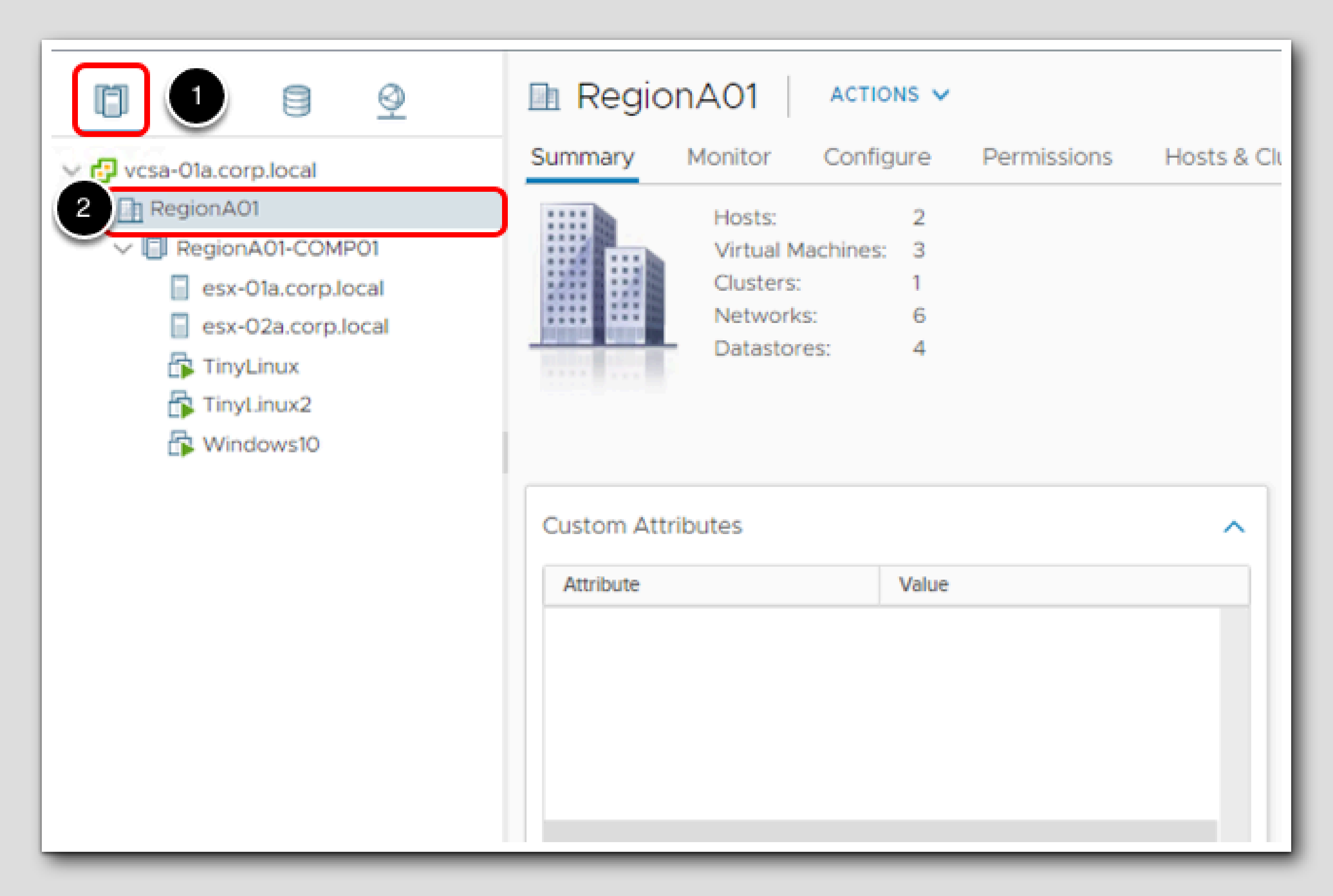
Add a new ESXi host

[485]

In this section, we will add a new ESXi host, esx-03a.corp.local, to the environment in RegionA01 and ensure that it has the appropriate storage configured so that it can become a productive member of the cluster.

Hosts and Clusters View

[486]



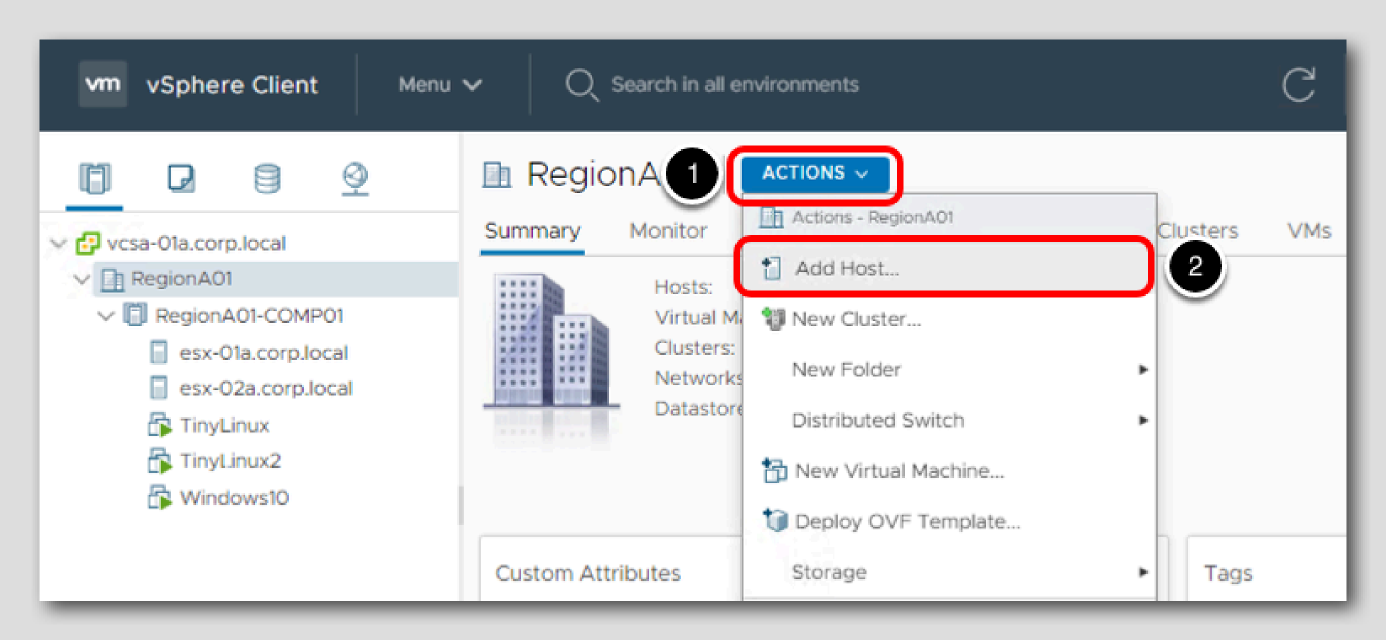
Hosts:	2
Virtual Machines:	3
Clusters:	1
Networks:	6
Datastores:	4

1. Click on the Hosts and Clusters icon to return to that Inventory view.
2. Select RegionA01 Datacenter.

It is a best practice to bring hosts into a datacenter first before adding them to a cluster. If a host is added to a cluster first, by not having access to the cluster's storage volumes, it could impact High Availability (see Module 1 for more details on High Availability).

Begin the Add Host workflow

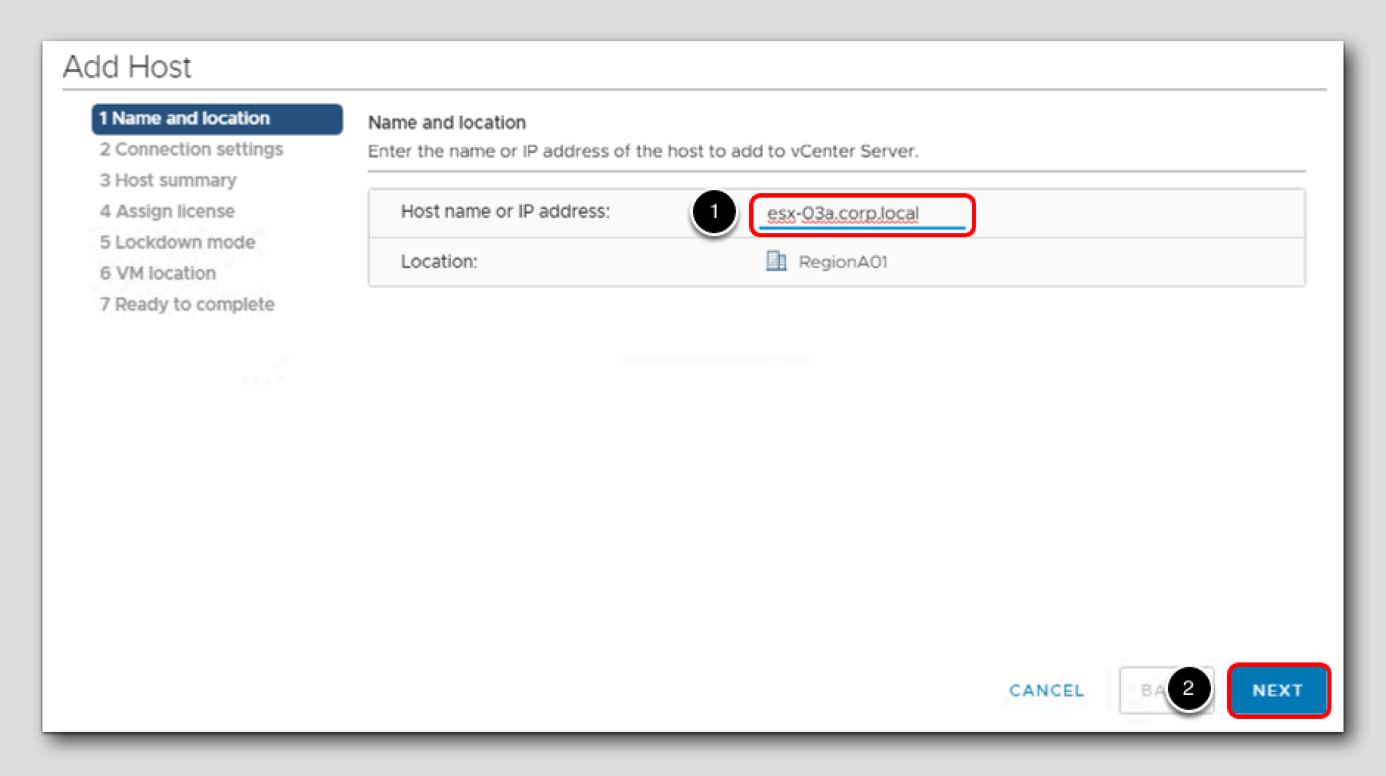
[487]



1. Go to the **Actions** menu.
2. Select **Add Hosts...**

Enter the hostname

[488]



Add Host

Name and location

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

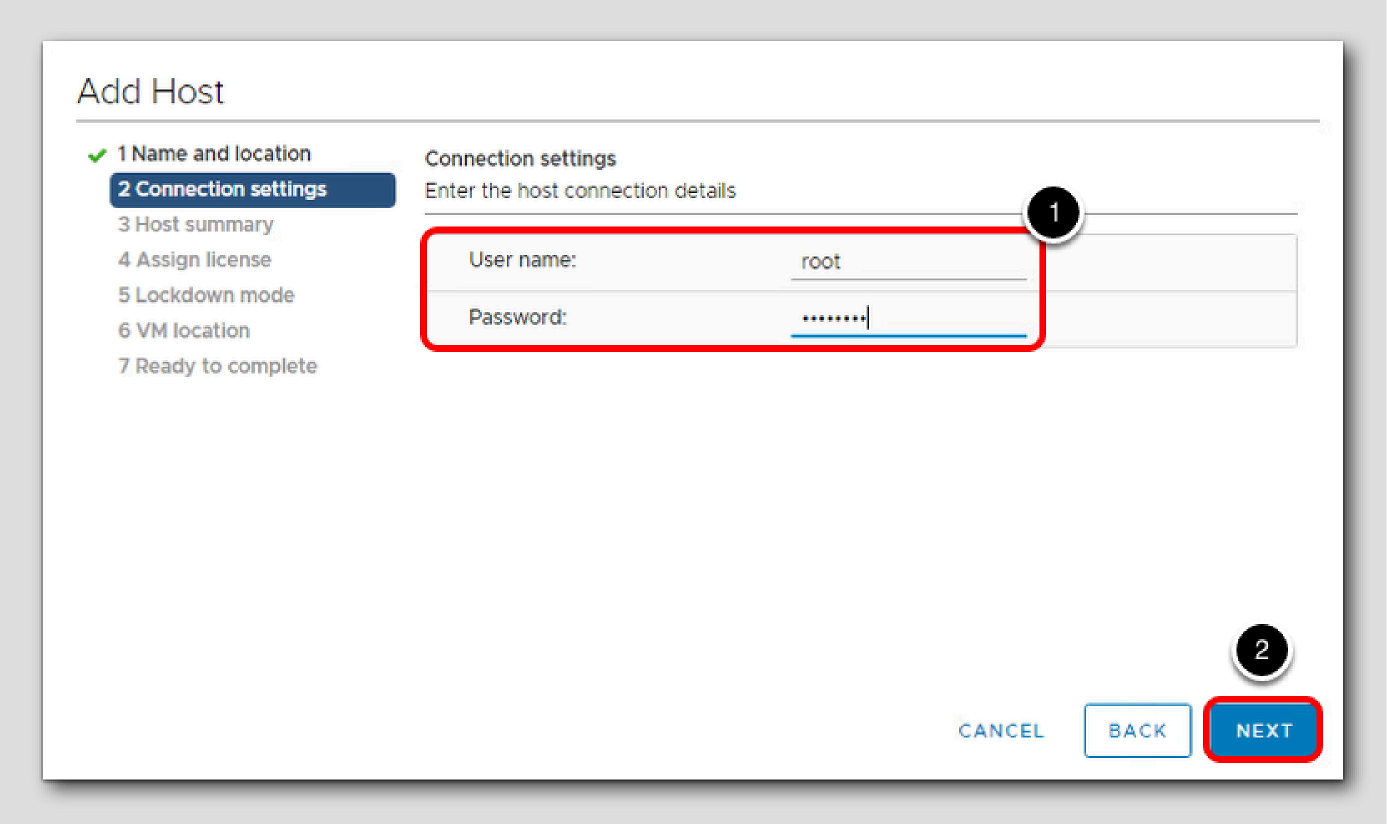
Host name or IP address: esx-03a.corp.local

Location: RegionA01

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

Connection Settings

[489]



Connection settings

Enter the host connection details

User name: root

Password: •••••••••

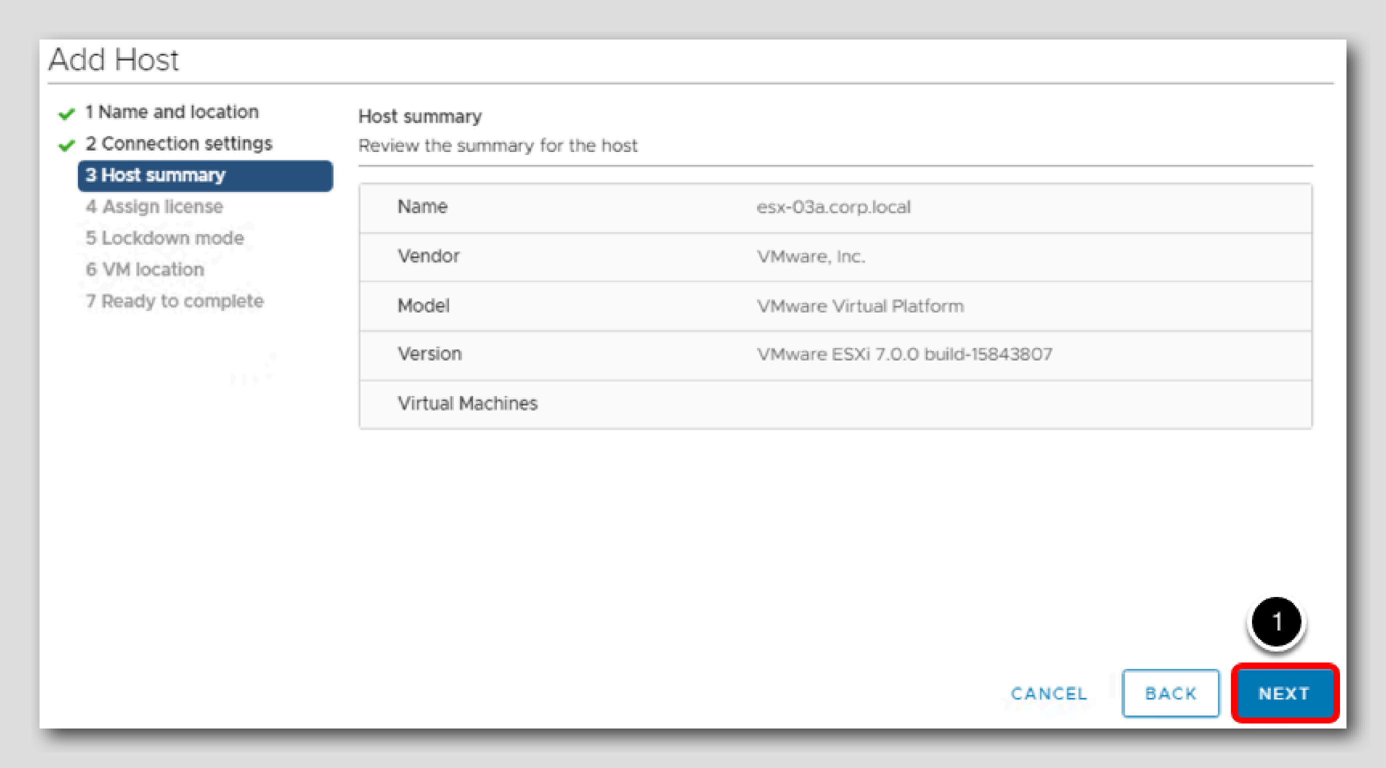
1. Enter the following login details:

- User name: root
- Password: VMware1!

2. Click Next.

Host Summary

[490]



Add Host

Host summary

Review the summary for the host

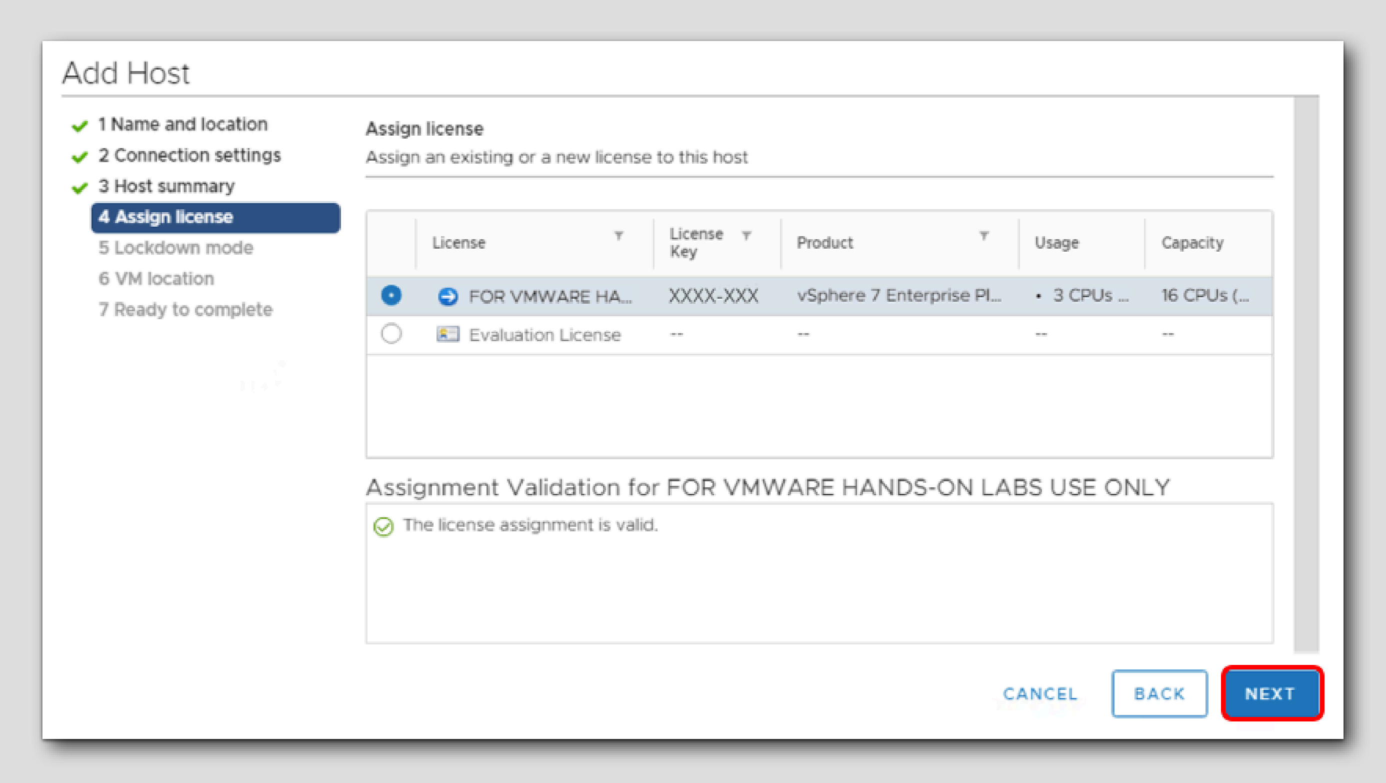
Name	esx-03a.corp.local
Vendor	VMware, Inc.
Model	VMware Virtual Platform
Version	VMware ESXi 7.0.0 build-15843807
Virtual Machines	

This screen shows the details of the host.

1. Click **Next**.

Assign License

[491]



Add Host

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

Assign license

Assign an existing or a new license to this host

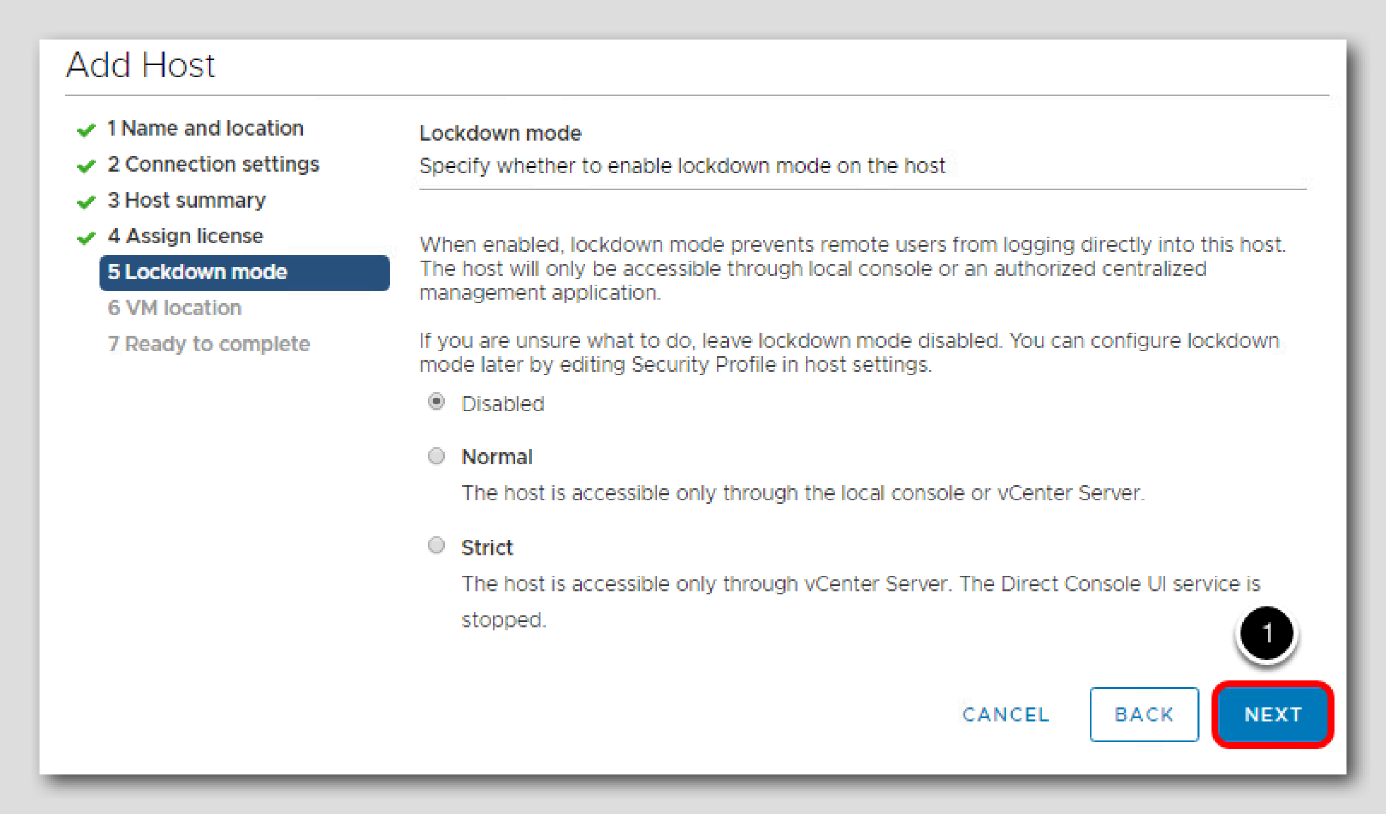
	License	License Key	Product	Usage	Capacity
●	FOR VMWARE HA...	XXXX-XXX	vSphere 7 Enterprise Pl...	• 3 CPUs ...	16 CPUs (...
○	Evaluation License	--	--	--	--

Assignment Validation for FOR VMWARE HANDS-ON LABS USE ONLY

✓ The license assignment is valid.

1. Leave the default license choice and click Next.

Lockdown Mode



Add Host

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

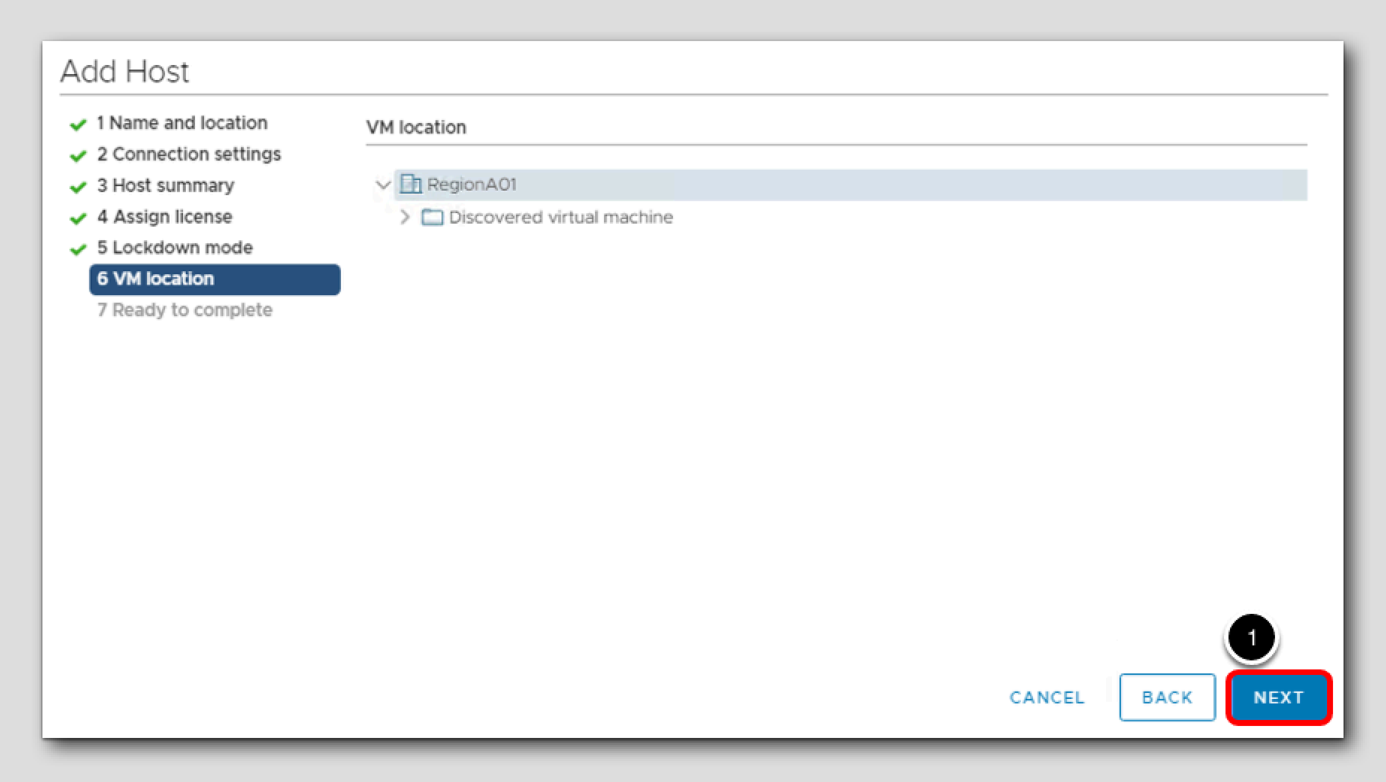
The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

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

[493]



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

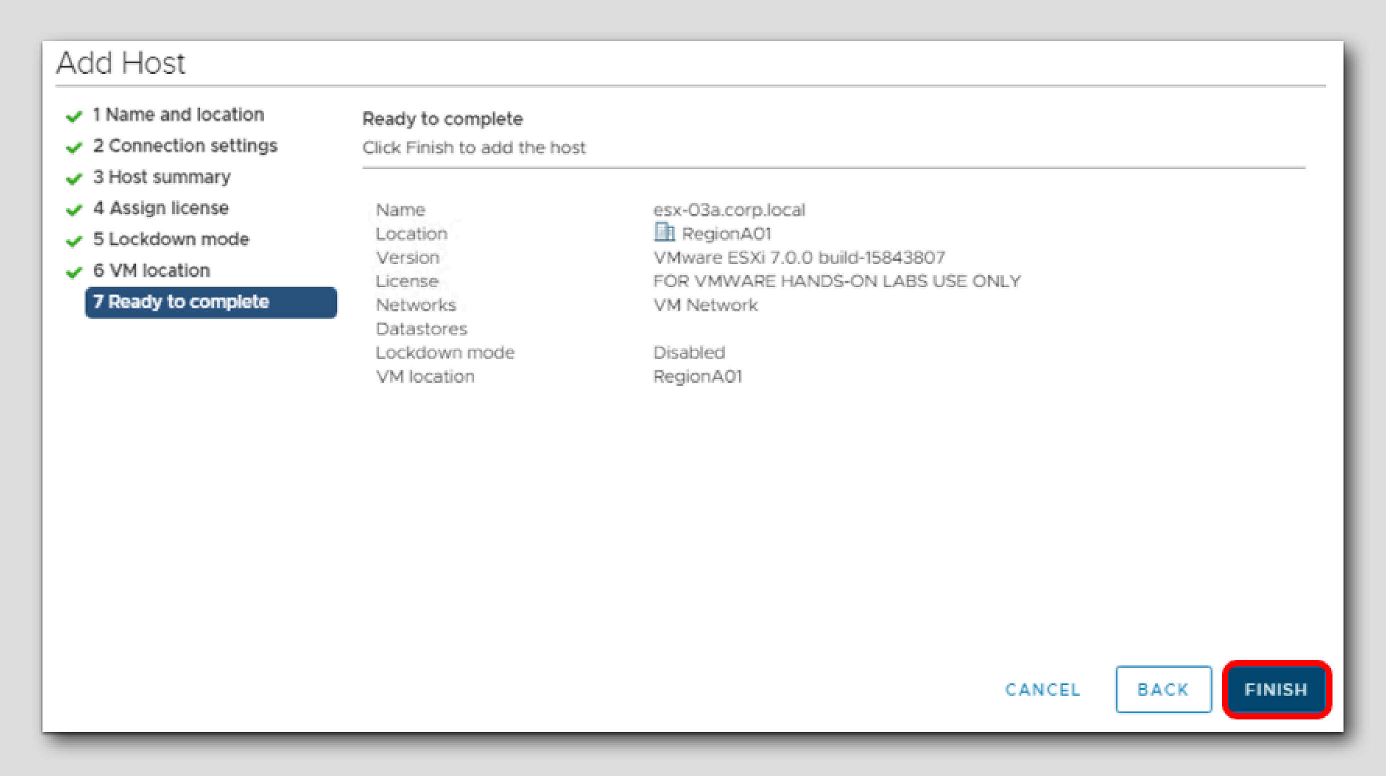
RegionA01
Discovered virtual machine

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

[494]



Add Host

Ready to complete

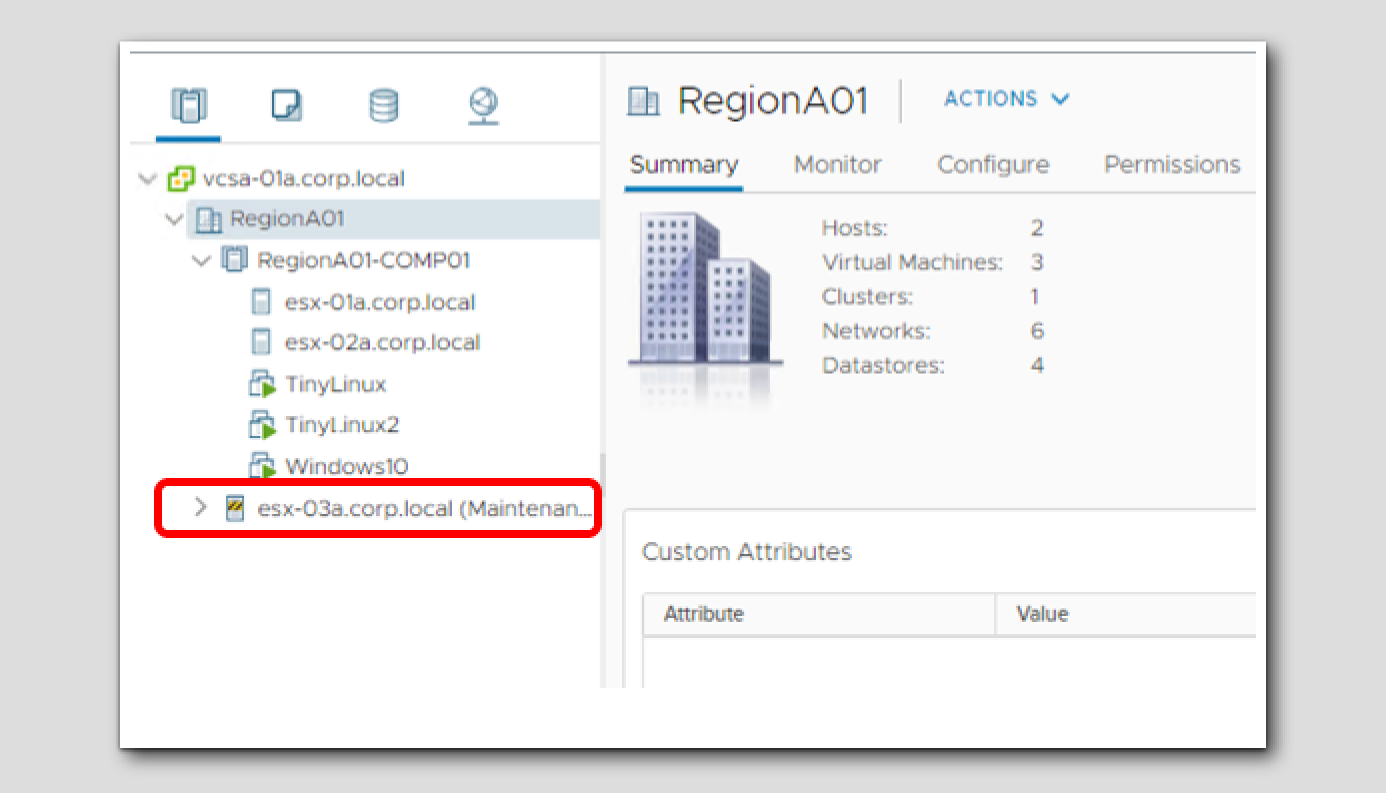
Click Finish to add the host

Name	esx-03a.corp.local
Location	RegionA01
Version	VMware ESXi 7.0.0 build-15843807
License	FOR VMWARE HANDS-ON LABS USE ONLY
Networks	VM Network
Datastores	
Lockdown mode	Disabled
VM location	RegionA01

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

Host Added to Datacenter

[495]



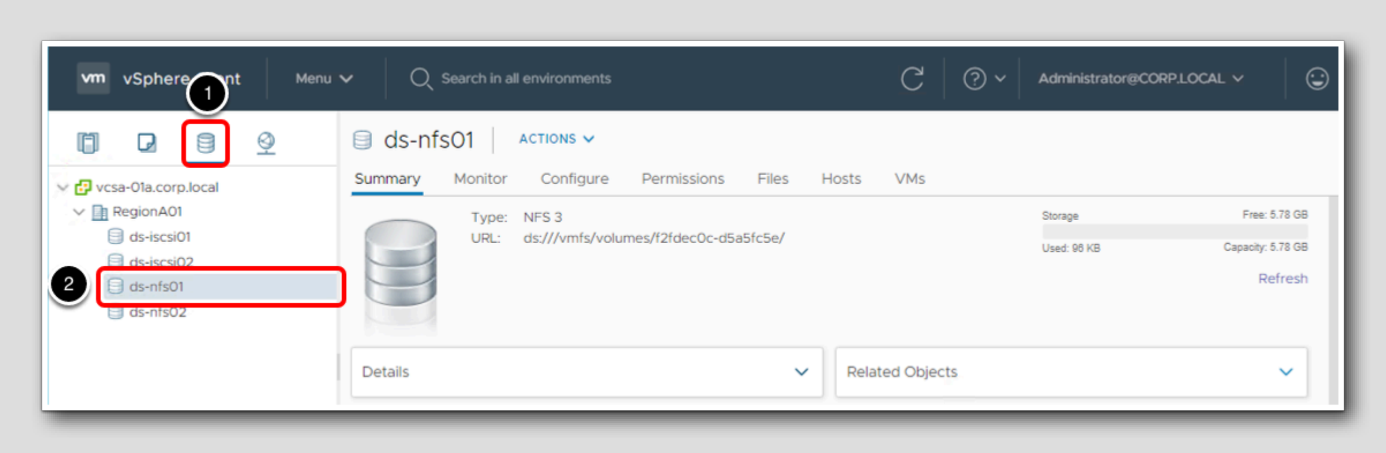
Hosts:	2
Virtual Machines:	3
Clusters:	1
Networks:	6
Datastores:	4

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

[496]

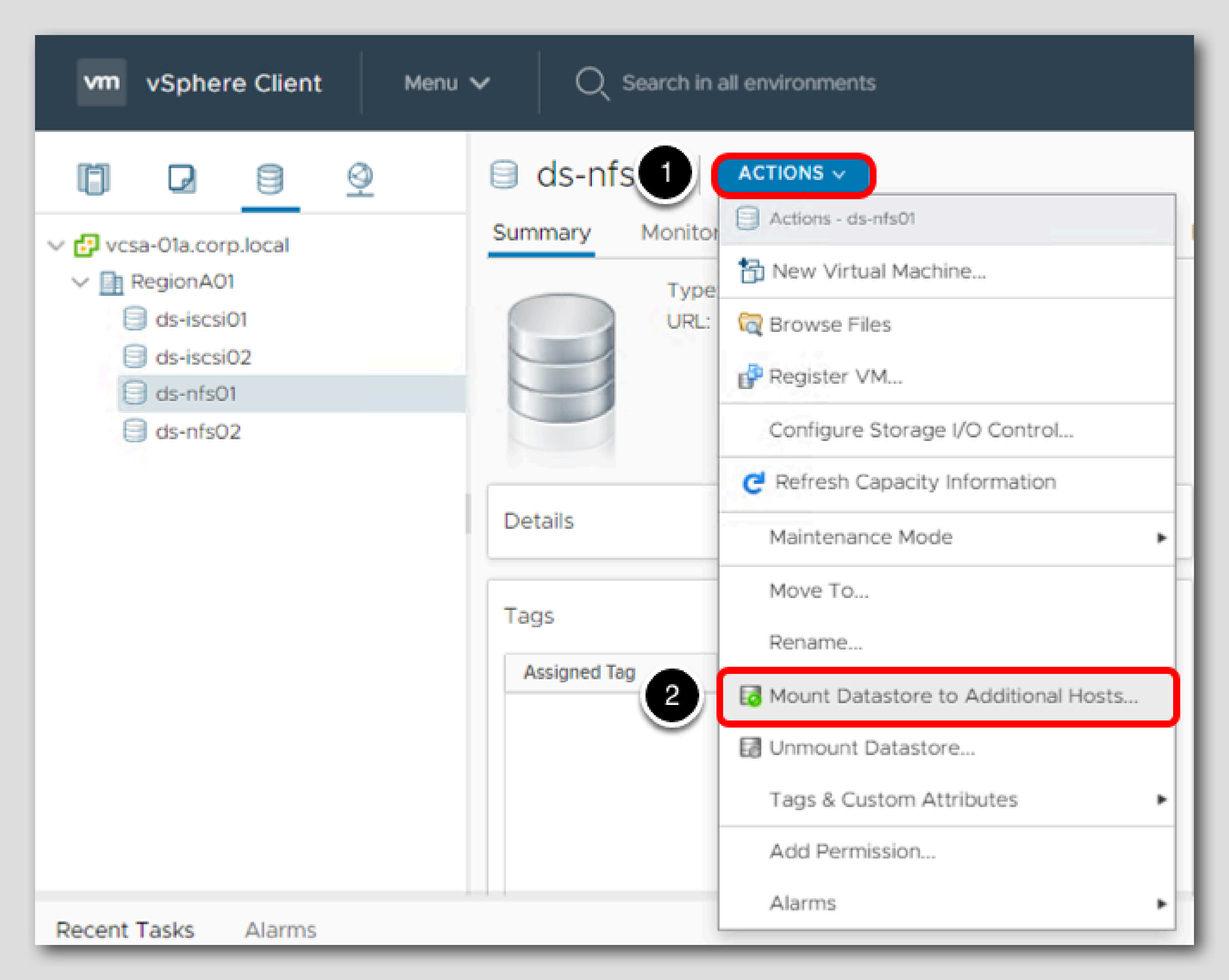


Prior to adding the new host to the cluster, an NFS datastore will be added to the host.

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

[497]

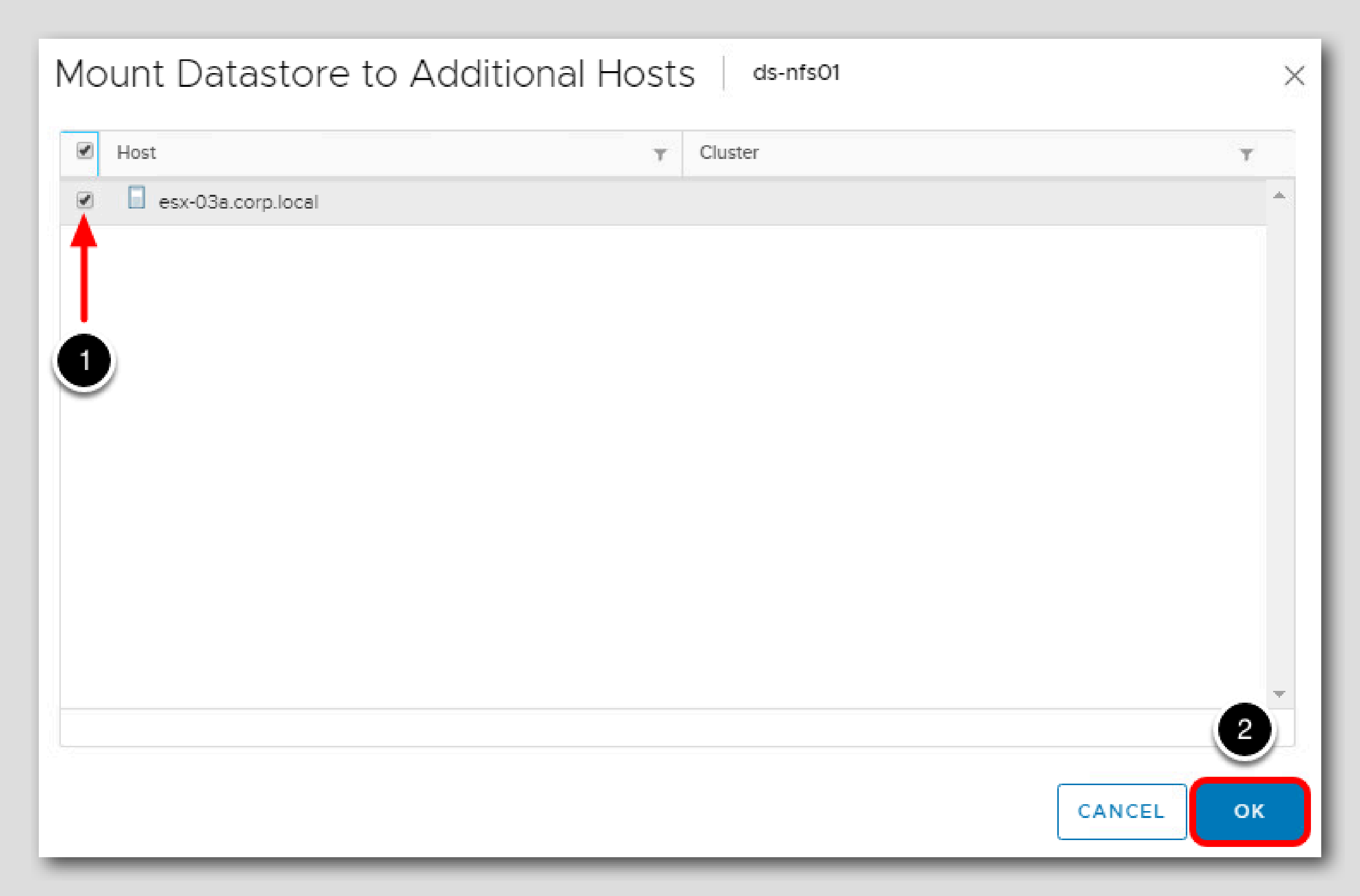


In this case, there are two NFS datastores used by RegionA01 cluster. Adding an existing NFS datastore to a new host is a simple process.

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

Mount NFS Datastore - Select Host

[498]



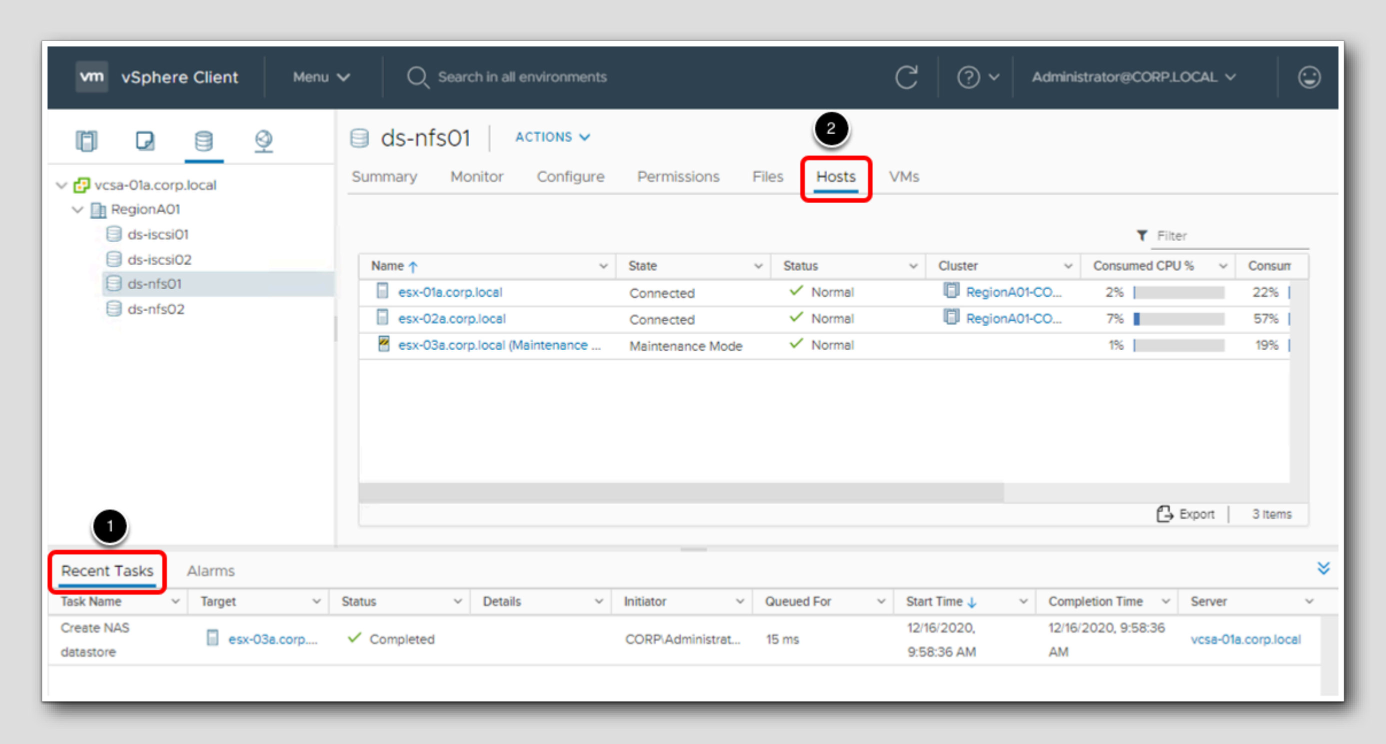
Mount Datastore to Additional Hosts | ds-nfs01

☑	Host	Cluster
☑	esx-03a.corp.local	

1. Click the checkbox next to esx-03a.corp.local
2. Click OK.

Mount NFS Datastore - Monitor Task

[499]



Name ↑	State	Status	Cluster	Consumed CPU %	Consum
esx-01a.corp.local	Connected	✓ Normal	RegionA01-CO...	2%	22%
esx-02a.corp.local	Connected	✓ Normal	RegionA01-CO...	7%	57%
esx-03a.corp.local (Maintenance ...	Maintenance Mode	✓ Normal		1%	19%

Task Name	Target	Status	Details	Initiator	Queued For	Start Time ↓	Completion Time	Server
Create NAS datastore	esx-03a.corp....	✓ Completed		CORP\Administrat...	15 ms	12/16/2020, 9:58:36 AM	12/16/2020, 9:58:36 AM	vcsa-01a.corp.local

1. The mount task can be monitored in Recent Tasks.
2. Once the mount completes, it can be verified by clicking on the Hosts tab.

This will show all hosts in the inventory that have mounted this datastore.

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

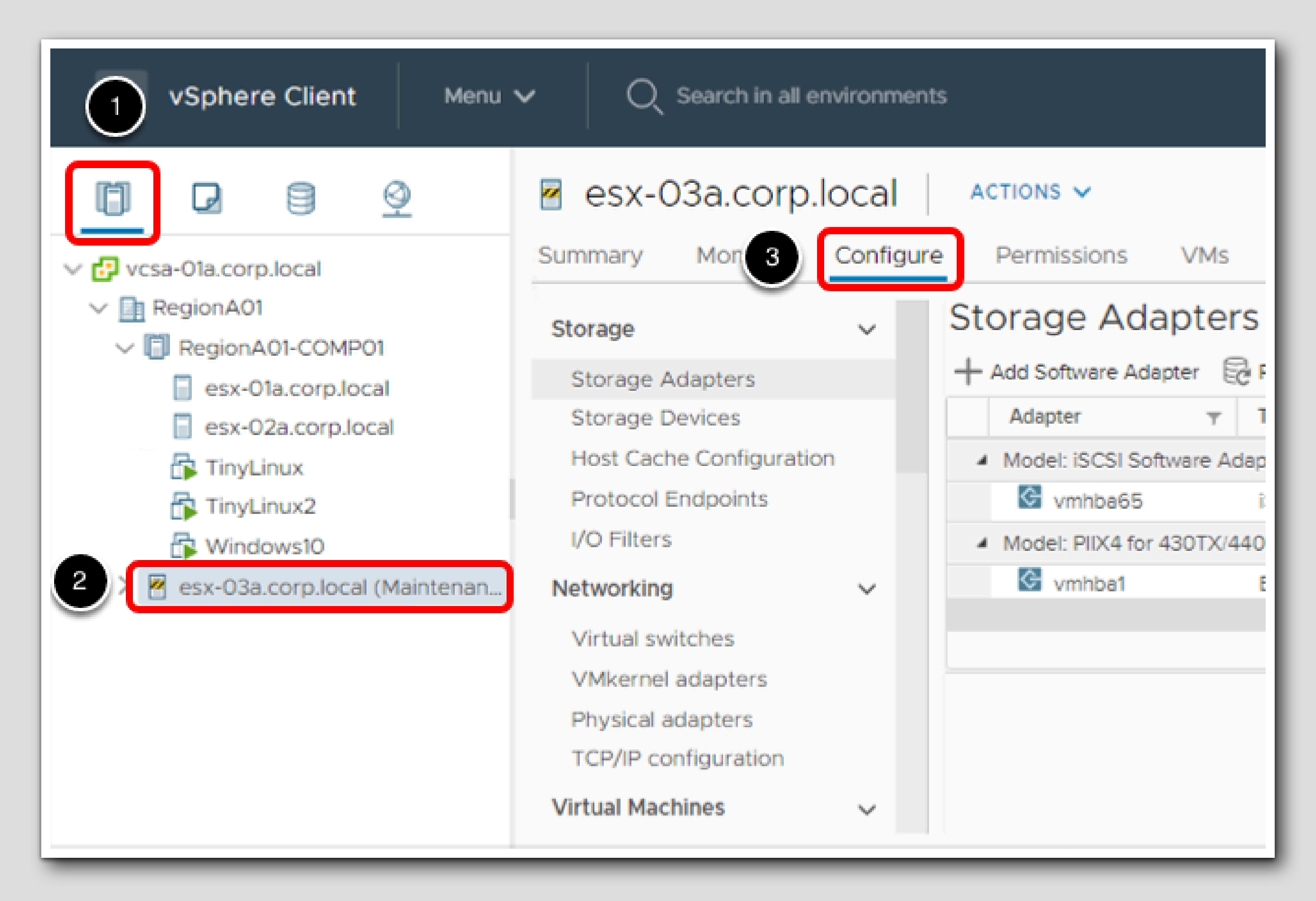
Add iSCSI Target to an ESXi host

[500]

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

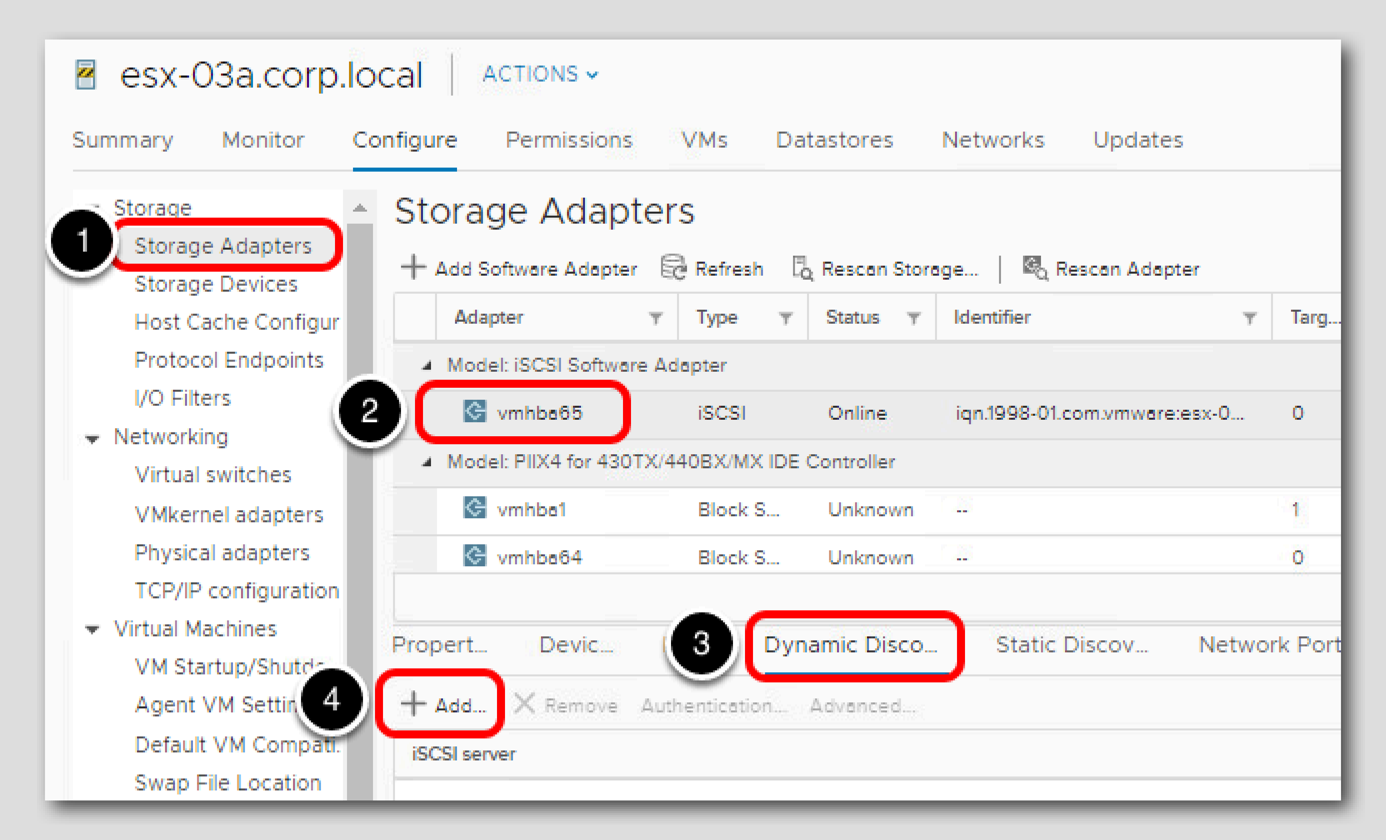
[501]



1. Select the Hosts and Clusters icon.
2. Click on esx-03a.corp.local (Maintenance Mode).
3. Click the Configure tab.

Perform Dynamic Discovery

[502]

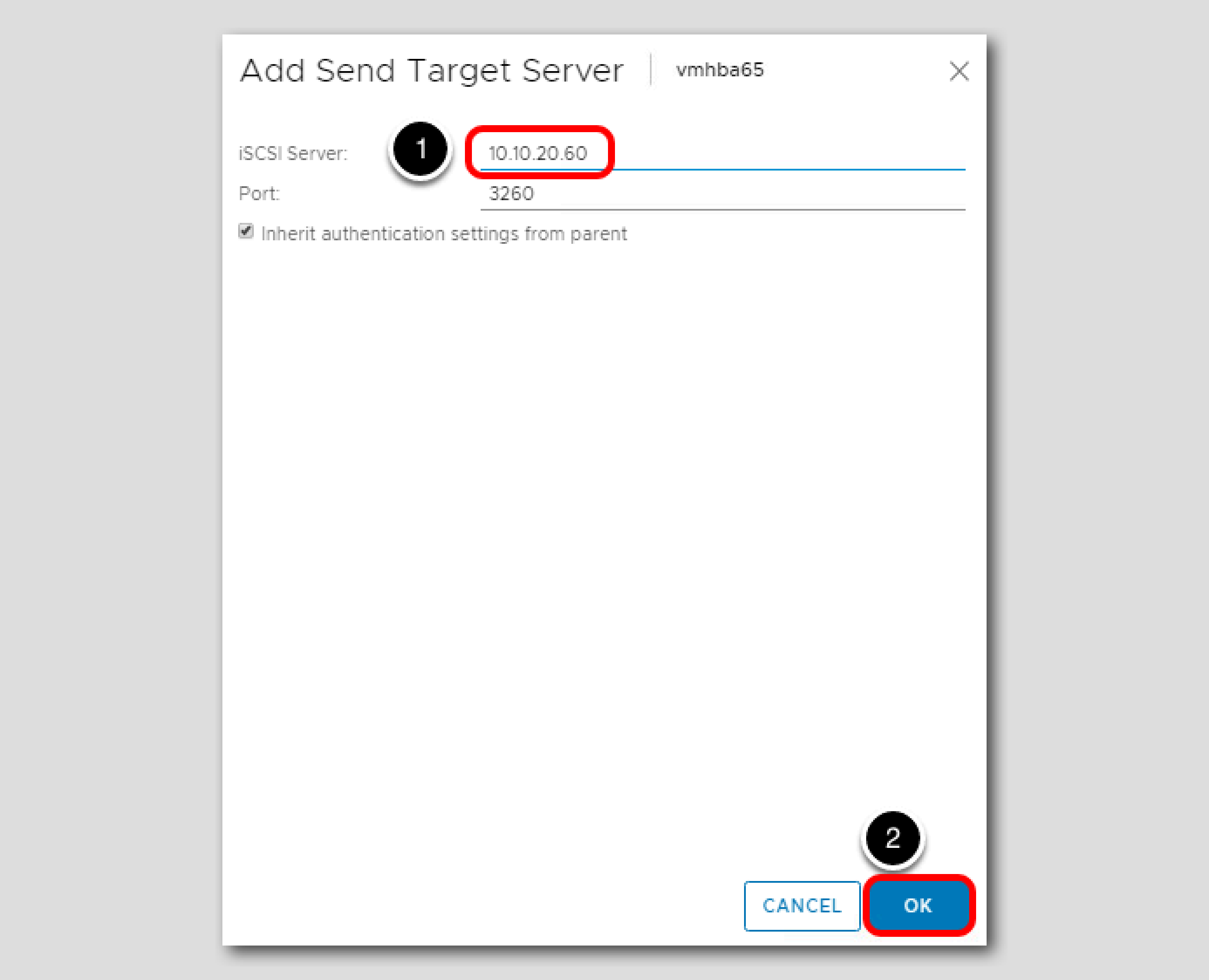


Adapter	Type	Status	Identifier	Targ...
Model: iSCSI Software Adapter				
vmhba65	iSCSI	Online	iqn.1998-01.com.vmware:esx-0...	0
Model: PIIX4 for 430TX/440BX/MX IDE Controller				
vmhba1	Block S...	Unknown	--	1
vmhba64	Block S...	Unknown	--	0

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

[503]



Add Send Target Server | vmhba65

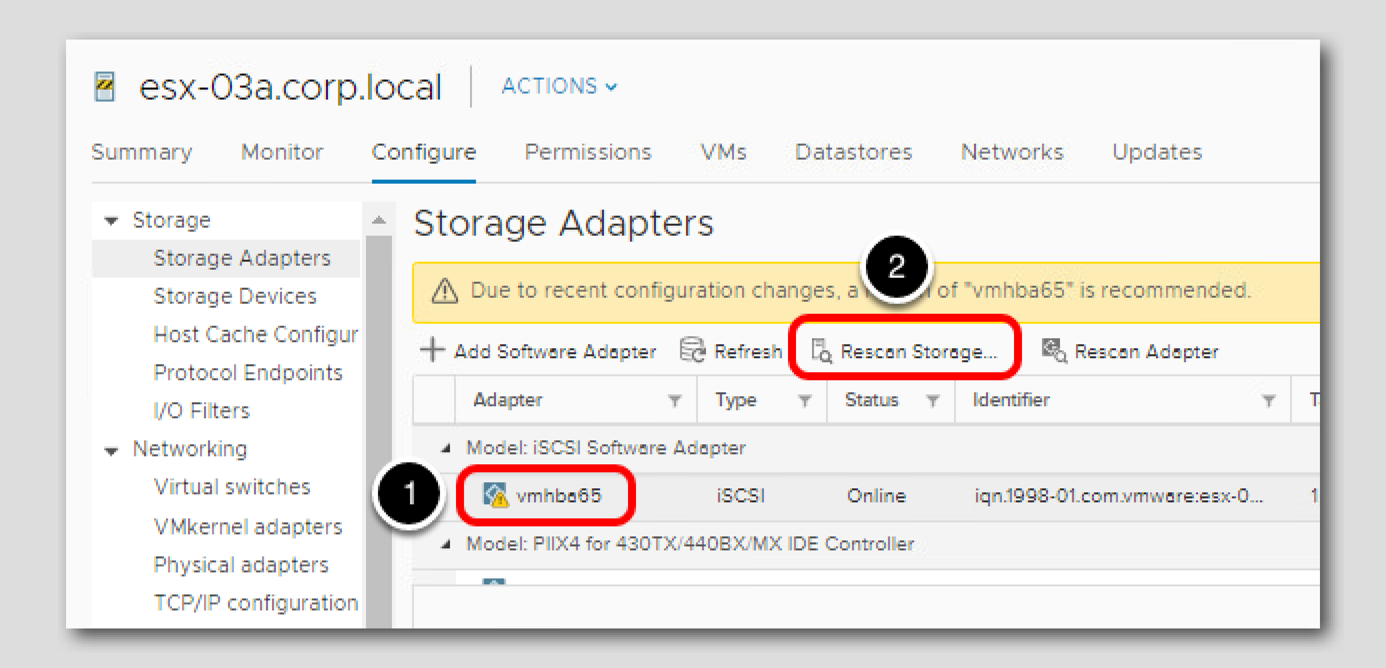
iSCSI Server: 10.10.20.60

Port: 3260

☑ Inherit authentication settings from parent

1. Enter the iSCSI Server Address: 10.10.20.60
2. Select OK.

Rescan the iSCSI storage adapter

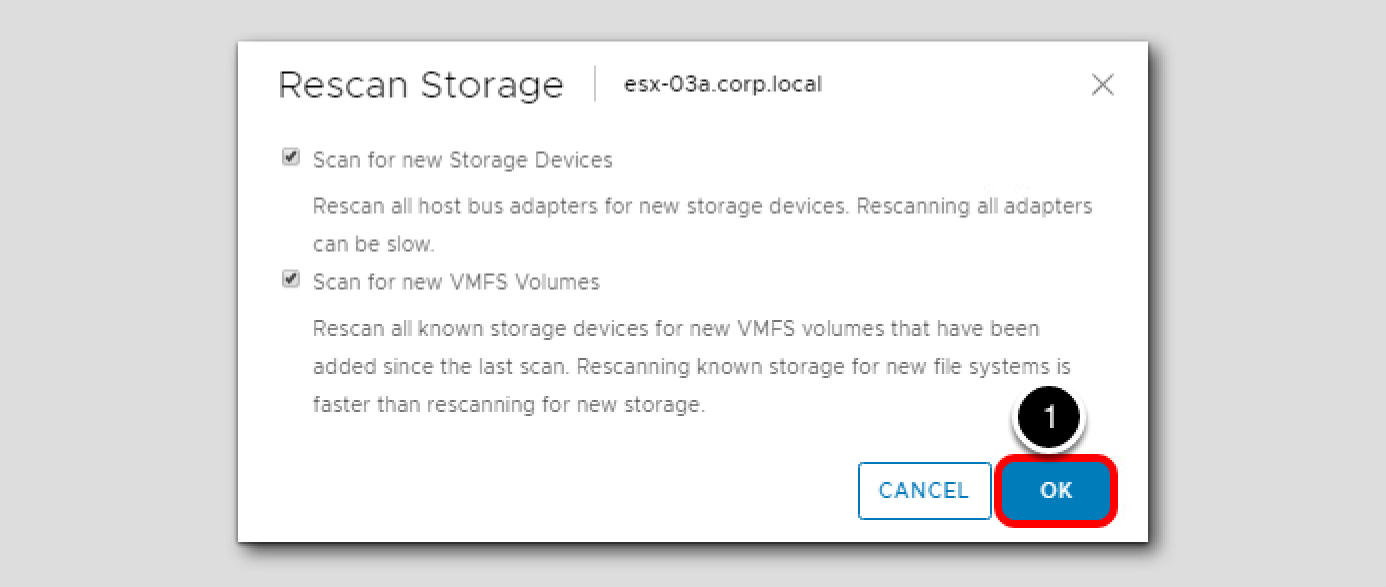


Once the new Target has been added, a message will appear in yellow to remind you of the need to tell the adapter to reach out and query the iSCSI Target.

1. Click on the **vmhba65** iSCSI adapter to select it.
2. Click the **Rescan Storage...** icon to rescan.

Rescan Storage

[505]



Rescan Storage | esx-03a.corp.local

☑ Scan for new Storage Devices

Rescan all host bus adapters for new storage devices. Rescanning all adapters can be slow.

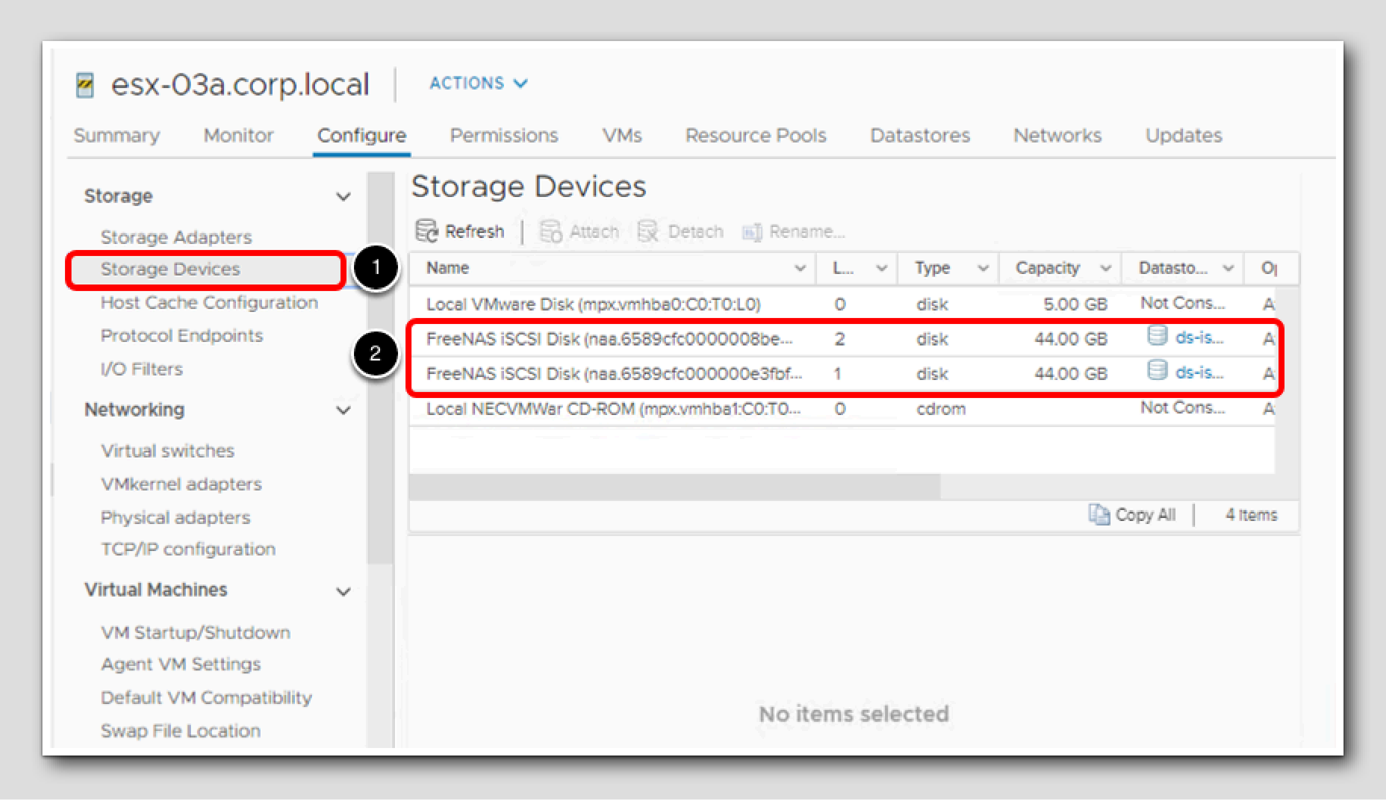
☑ Scan for new VMFS Volumes

Rescan all known storage devices for new VMFS volumes that have been added since the last scan. Rescanning known storage for new file systems is faster than rescanning for new storage.

1. Leave the default options selected and click OK.

Verify iSCSI Devices are Visible

[506]

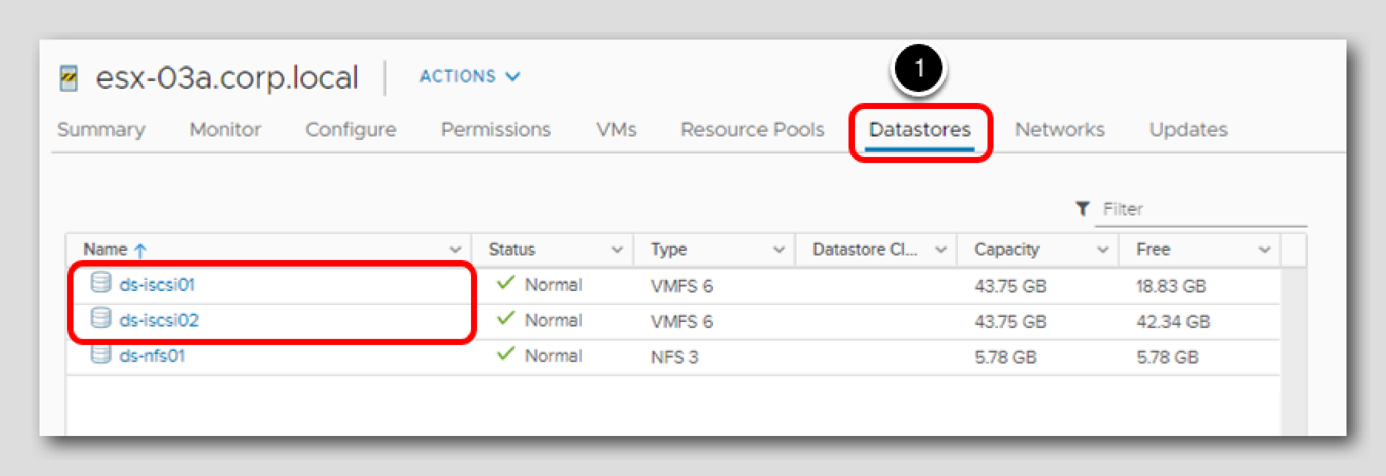


Name	L...	Type	Capacity	Datasto...	O|
Local VMware Disk (mpx.vmhba0:C0:T0:L0)	0	disk	5.00 GB	Not Cons...	A
FreeNAS iSCSI Disk (naa.6589cfc0000008be...	2	disk	44.00 GB	ds-is...	A
FreeNAS iSCSI Disk (naa.6589cfc000000e3fbf...	1	disk	44.00 GB	ds-is...	A
Local NECVMWar CD-ROM (mpx.vmhba1:C0:T0...	0	cdrom		Not Cons...	A

1. Once the rescan is complete, Click on Storage Devices.
2. You should now see two iSCSI disks connected, both with 44GB of capacity.

Verify iSCSI Datastore Availability

[507]



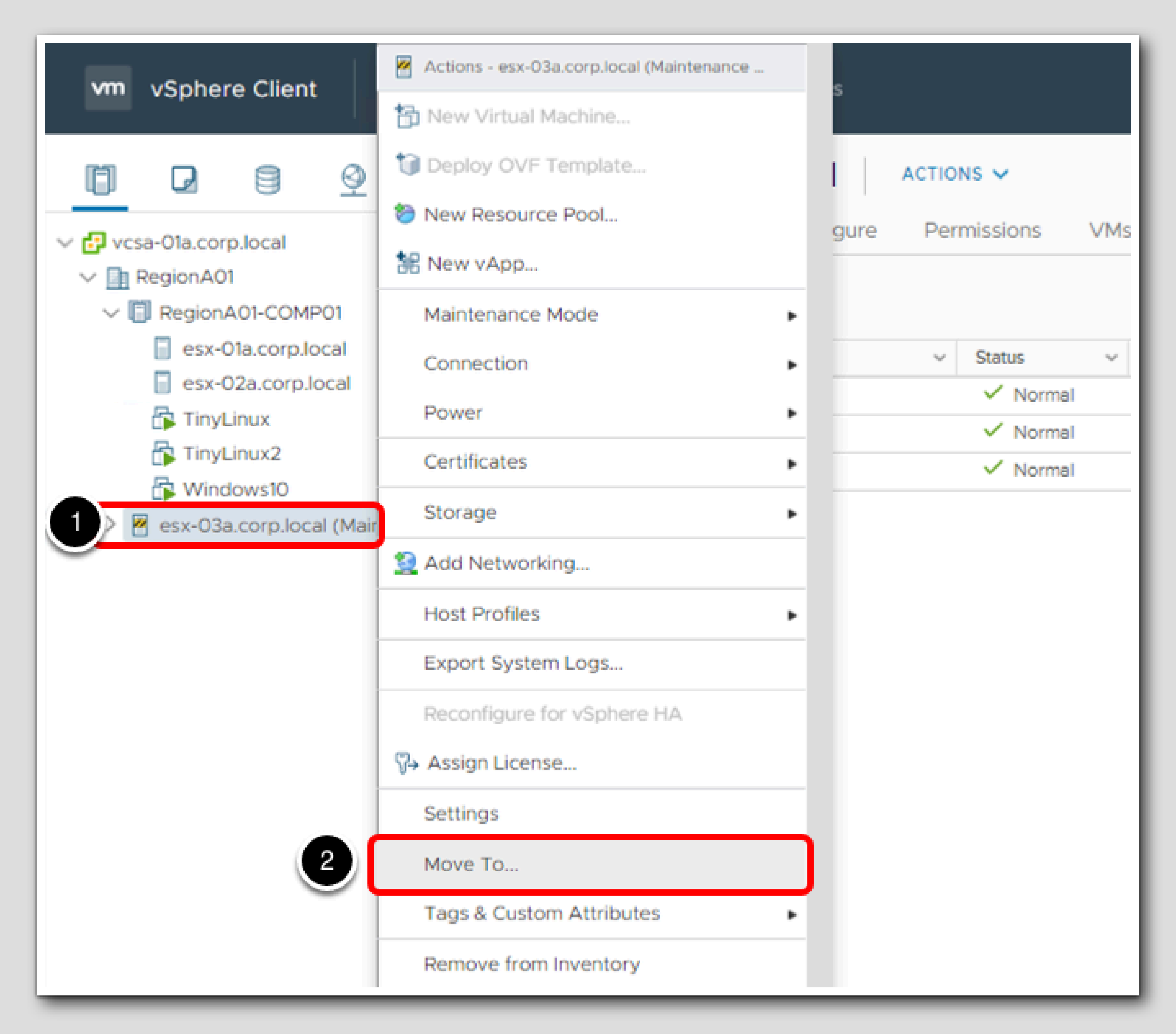
Name ↑	Status	Type	Datastore Cl...	Capacity	Free
ds-iscsi01	✓ Normal	VMFS 6		43.75 GB	18.83 GB
ds-iscsi02	✓ Normal	VMFS 6		43.75 GB	42.34 GB
ds-nfs01	✓ Normal	NFS 3		5.78 GB	5.78 GB

1. Click on the Datastores tab.

Notice that the two iSCSI datastores are now visible to the esx-03a.corp.local host.

Move into the Cluster

[508]

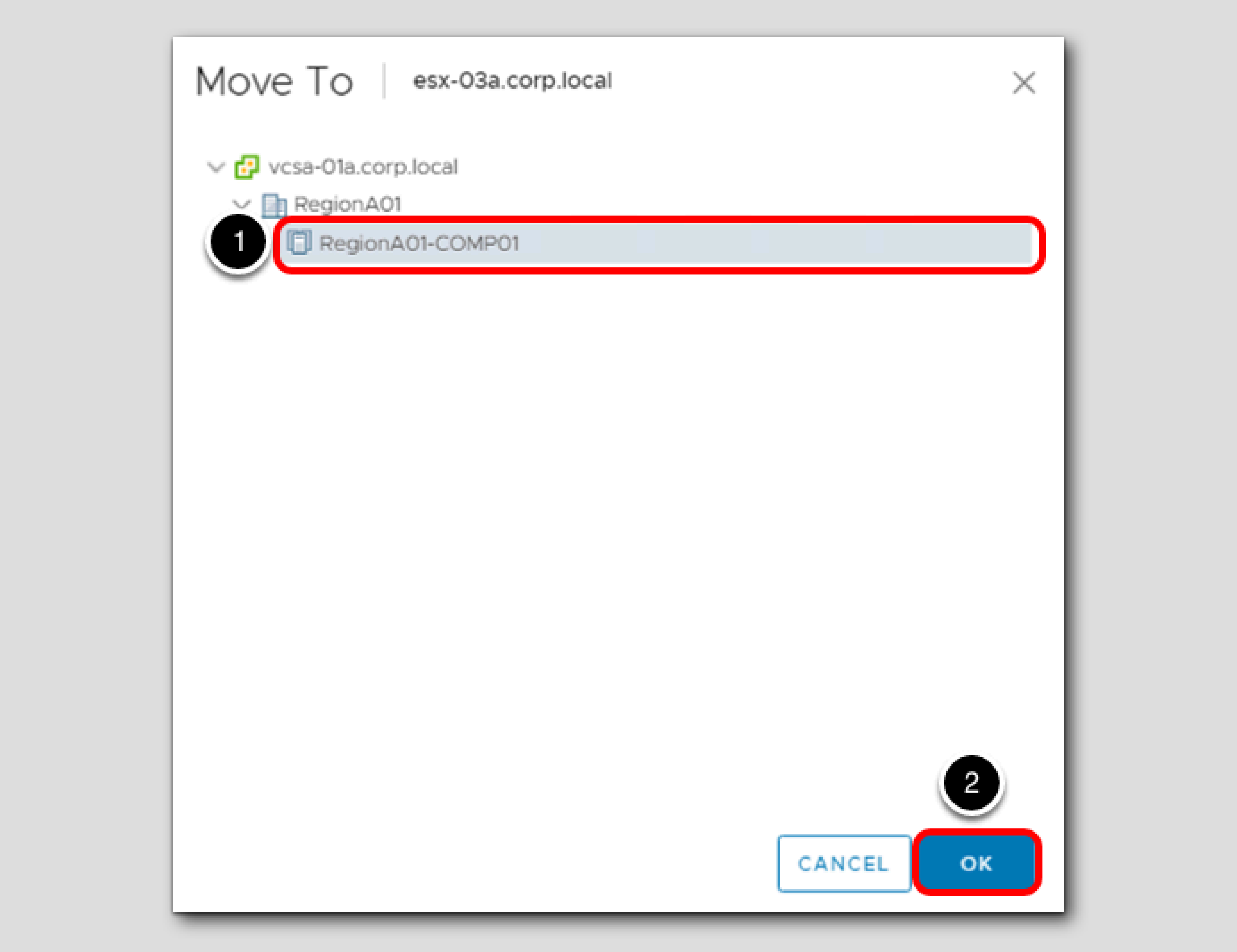


Now that we have the storage configured, move the esx-03a-corp.local into RegionA01-COMP01.

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

Move To

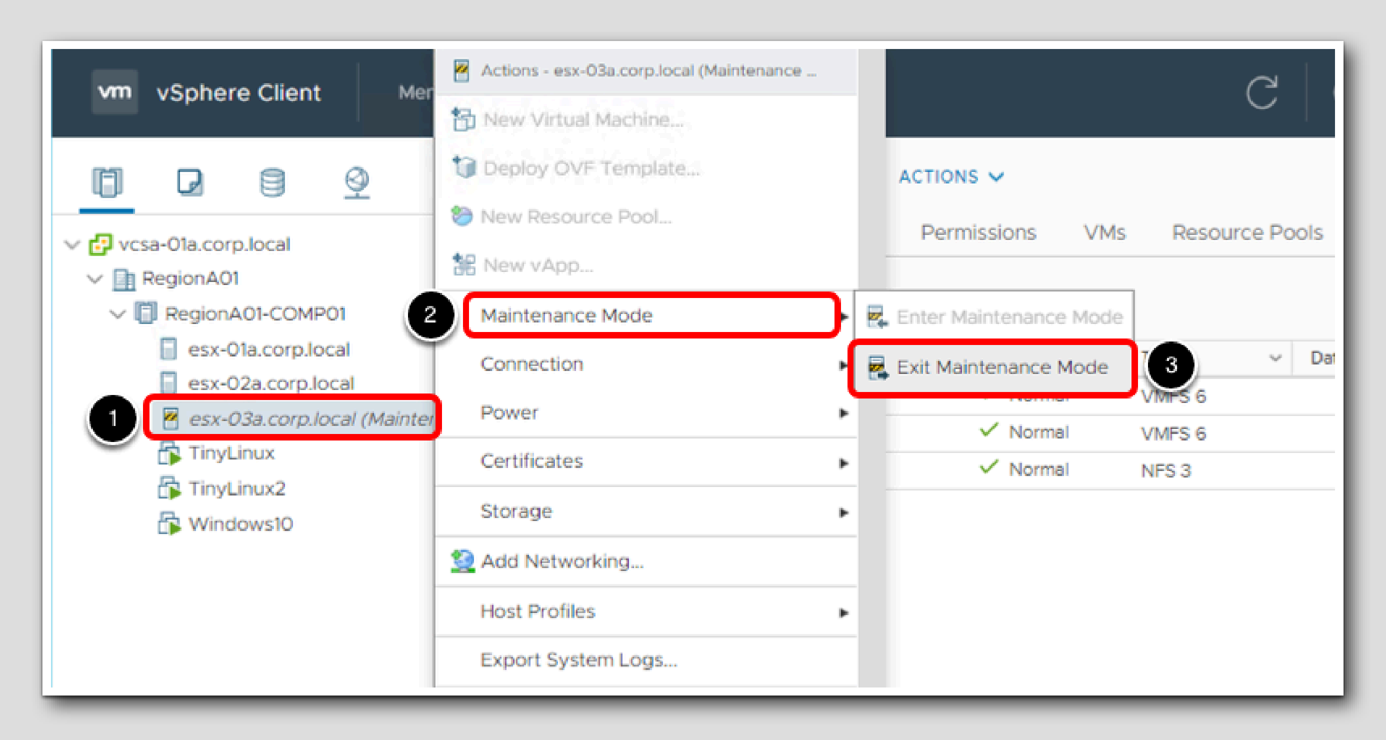
[509]



1. Expand **RegionA01** and select **RegionA01-COMP01**.
2. Click **OK**.

Exit Maintenance Mode

[510]

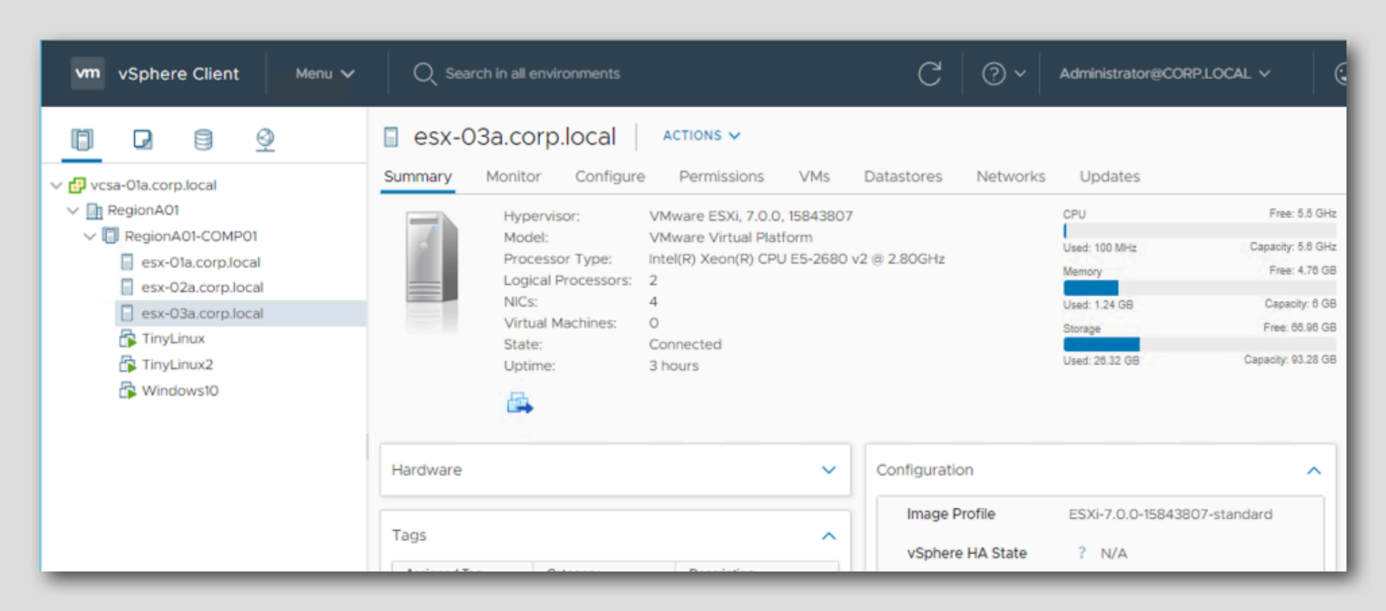


The host has been added to the cluster. Now it can exit Maintenance Mode and participate in the cluster.

1. Right-click on esx-03a.corp.local.
2. Select Maintenance Mode.
3. Click Exit Maintenance Mode.

Ready to Go

[511]



esx-03a.corp.local

Hypervisor: VMware ESXi, 7.0.0, 15843807
Model: VMware Virtual Platform
Processor Type: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz
Logical Processors: 2
NICs: 4
Virtual Machines: 0
State: Connected
Uptime: 3 hours

CPU Free: 5.5 GHz
Used: 100 MHz Capacity: 5.6 GHz
Memory Free: 4.76 GB
Used: 1.24 GB Capacity: 6 GB
Storage Free: 66.96 GB
Used: 26.32 GB Capacity: 93.28 GB

Image Profile ESXi-7.0.0-15843807-standard
vSphere HA State ? N/A

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

[512]

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.

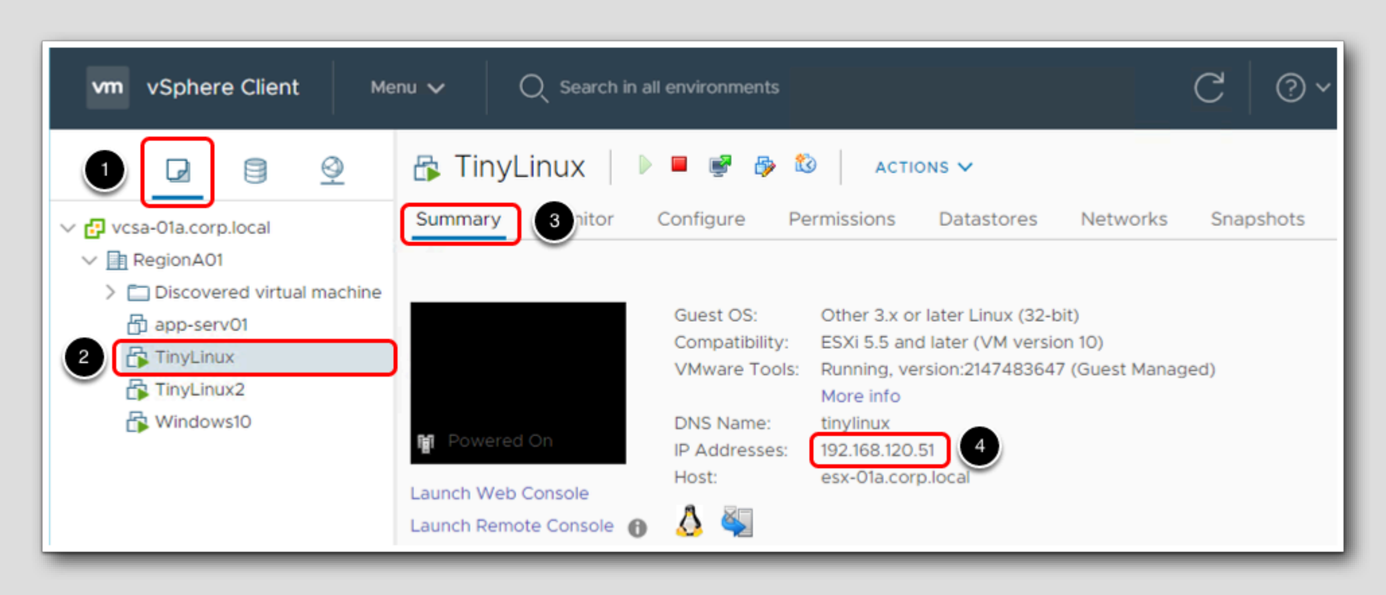
The vMotion and Storage vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers or to different underlying storage without service interruption. Administrators can 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

[513]



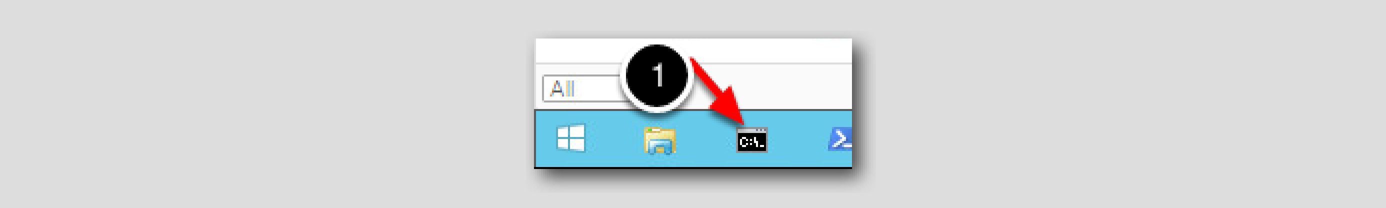
Guest OS: Other 3.x or later Linux (32-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Running, version:2147483647 (Guest Managed)
More info
DNS Name: tinylinux
IP Addresses: 192.168.120.51
Host: esx-01a.corp.local

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

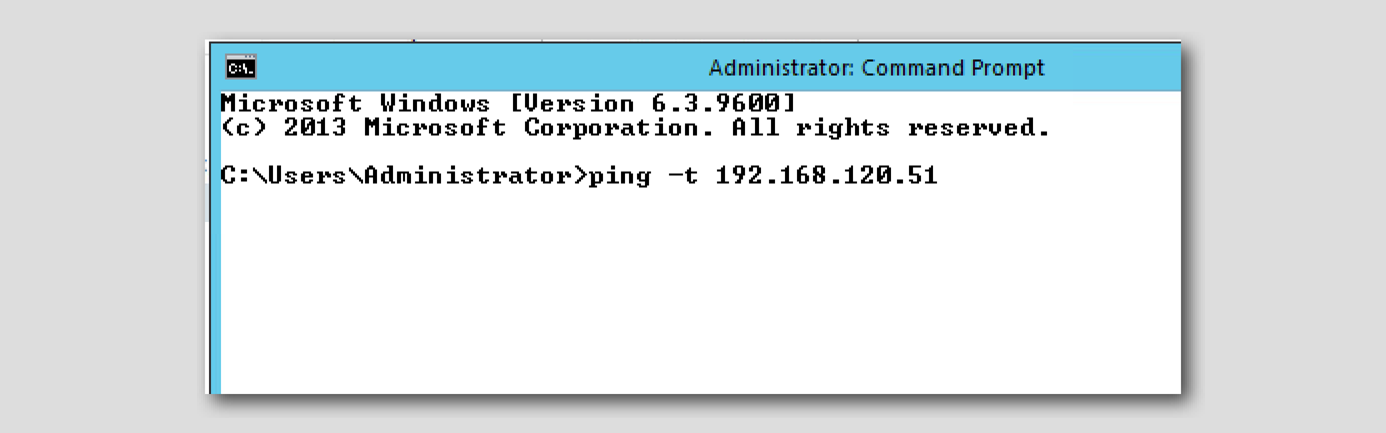
[514]



1. Click on the icon to open a command prompt from the Windows Task Bar.

Ping TinyLinux-01

[515]



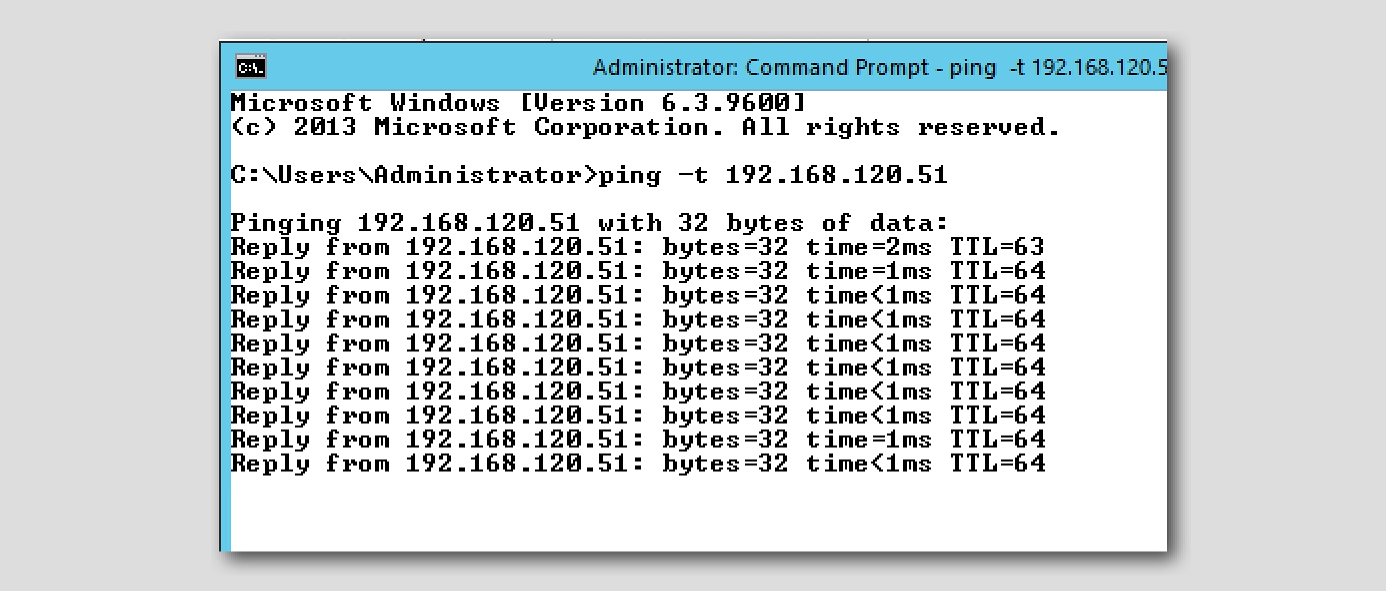
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping -t 192.168.120.51
```

Issue the following in the command prompt and press the Enter key:

```
ping -t 192.168.120.51
```

Ping Results

[516]

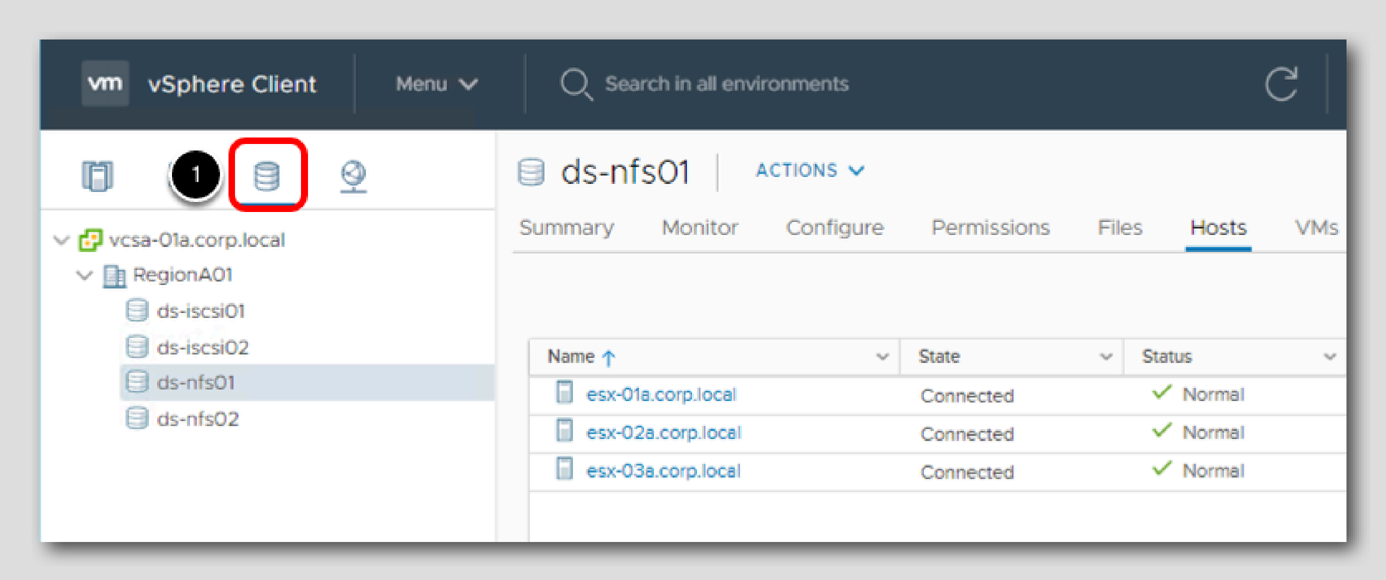


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping -t 192.168.120.51

Pinging 192.168.120.51 with 32 bytes of data:
Reply from 192.168.120.51: bytes=32 time=2ms TTL=63
Reply from 192.168.120.51: bytes=32 time=1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time=1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
```

You should now see a continuous ping to TinyLinux.

Storage View

[517]

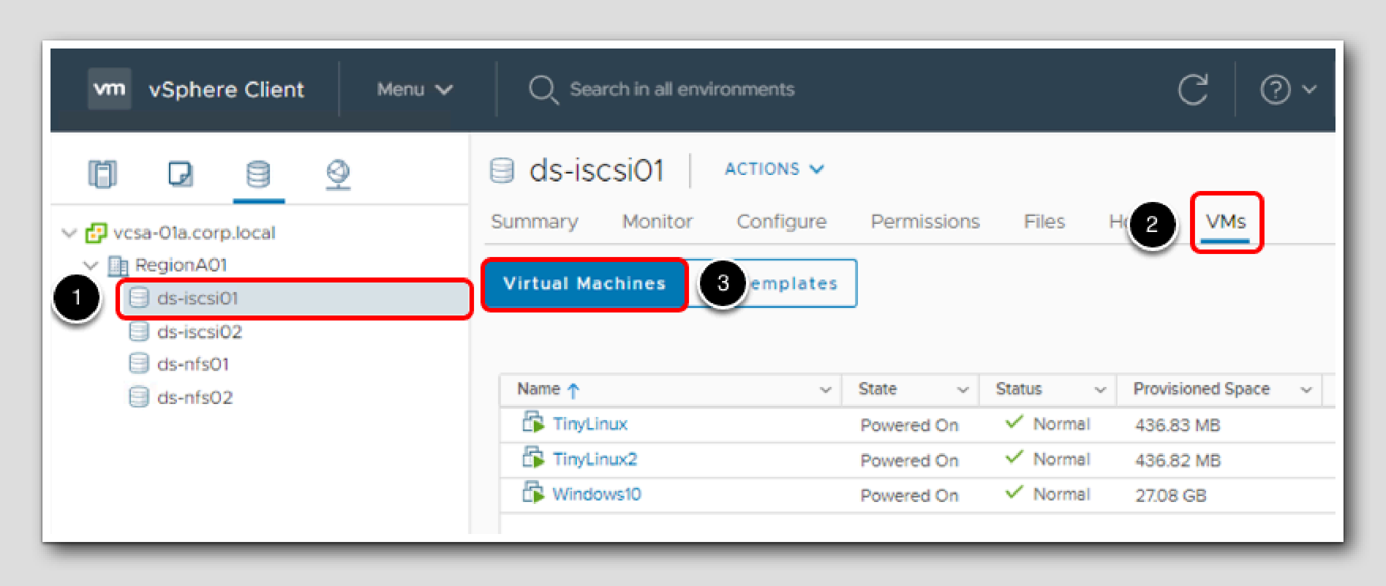


Name ↑	State	Status
esx-01a.corp.local	Connected	✓ Normal
esx-02a.corp.local	Connected	✓ Normal
esx-03a.corp.local	Connected	✓ Normal

1. Click the **Storage** icon.

List Virtual Machines on a Specified Datastore

[518]



Name ↑	State	Status	Provisioned Space
TinyLinux	Powered On	✓ Normal	436.83 MB
TinyLinux2	Powered On	✓ Normal	436.82 MB
Windows10	Powered On	✓ Normal	27.08 GB

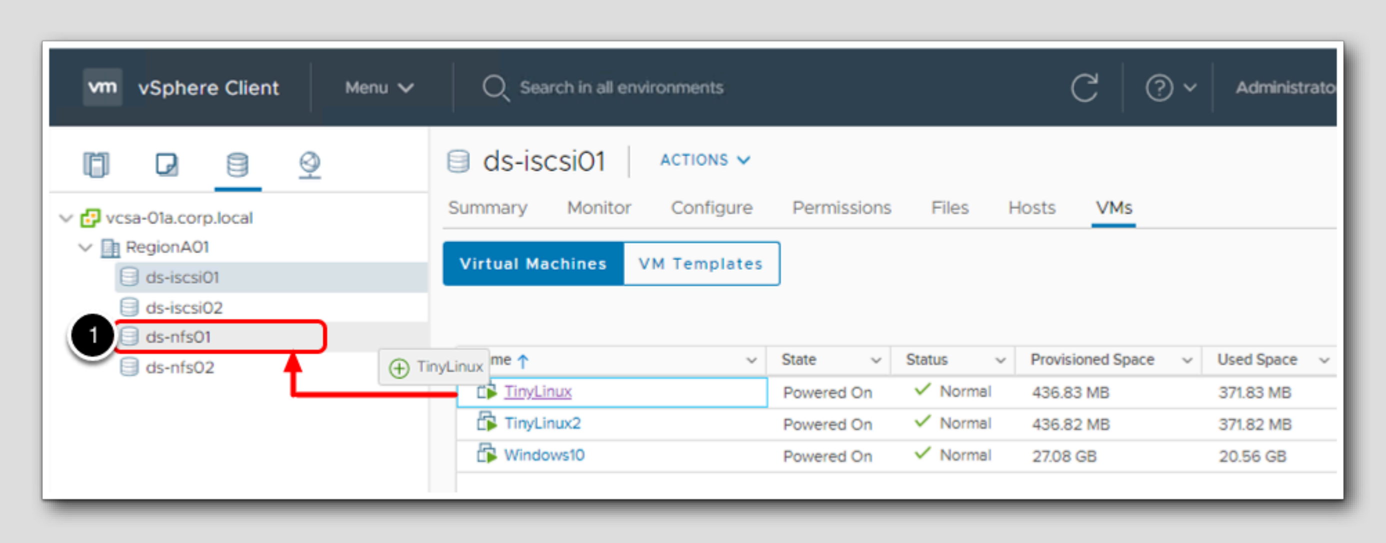
1. Click on the ds-iscsi01 datastore object in RegionA01 managed by the vcsa-01a.corp.local vCenter.
2. Click VMs.
3. Click the Virtual Machines tab.

You should now have a list of all virtual machines on the selected datastore.

Note: depending on which lessons you have completed, the available datastores and virtual machines may be different than the images.

Drag and Drop Storage vMotion

[519]



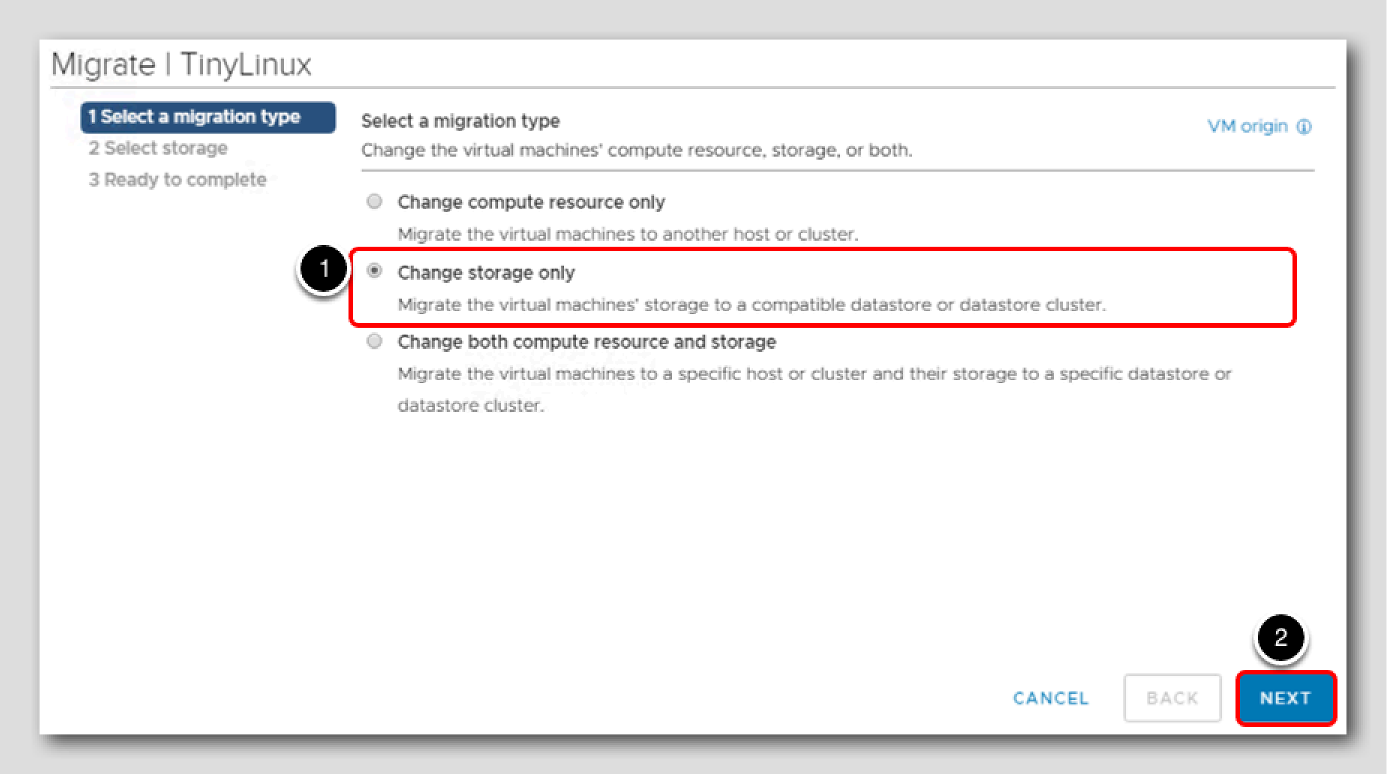
me ↑	State	Status	Provisioned Space	Used Space
TinyLinux	Powered On	✓ Normal	436.83 MB	371.83 MB
TinyLinux2	Powered On	✓ Normal	436.82 MB	371.82 MB
Windows10	Powered On	✓ Normal	27.08 GB	20.56 GB

The VM TinyLinux is initially on ds-iscsi01 and needs to be moved to ds-nfs01.

1. Click the TinyLinux VM and continue to hold the left mouse button while dragging the VM to the ds-nfs01 datastore object. A green + will appear near the mouse cursor (see picture) when it is pointing at objects which are suitable targets for the object being moved. Let go of the mouse button to drop the TinyLinux VM onto the ds-nfs01 object. The Migrate wizard will launch to complete the process.

Migrate Datastore

[520]



Migrate | TinyLinux

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.

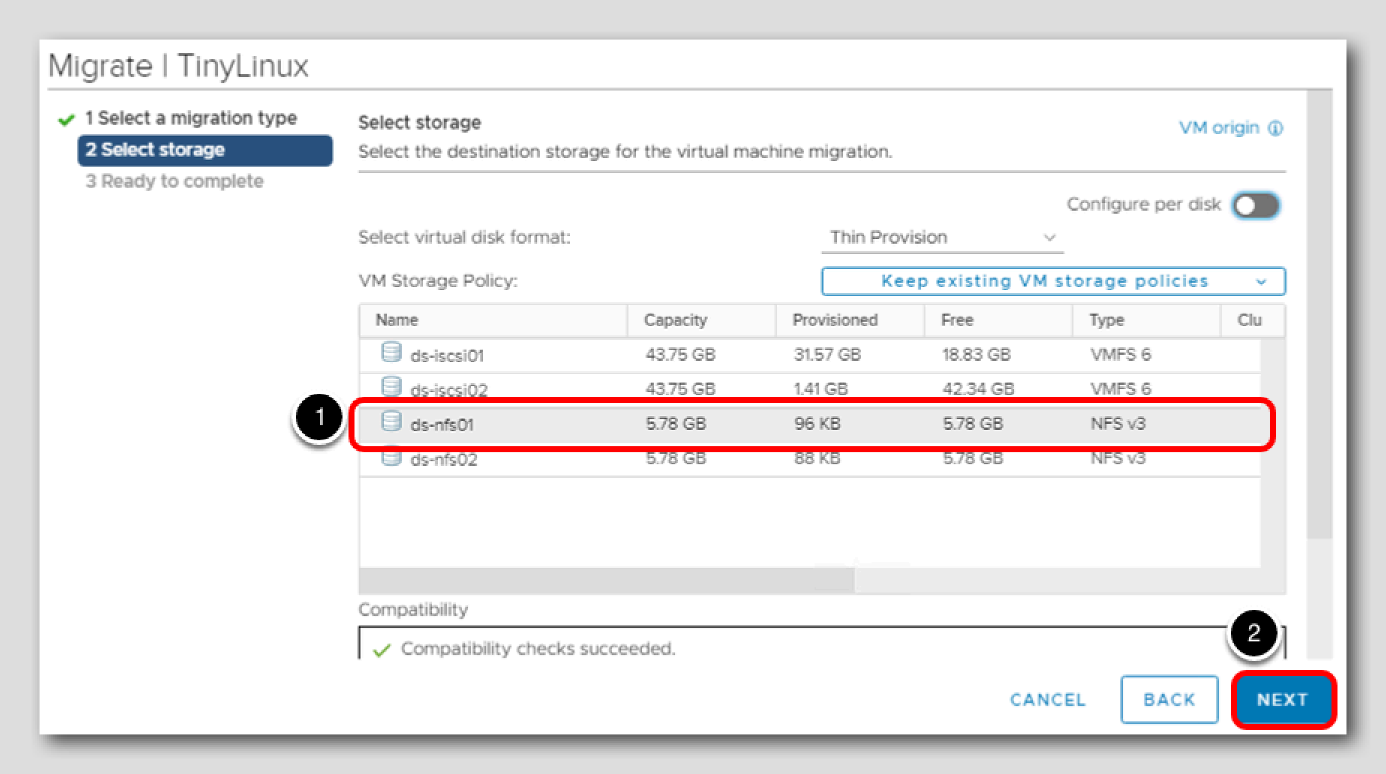
○ Change both compute resource and storage

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

1. 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

[521]



Migrate | TinyLinux

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

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

VM origin ⓘ

Configure per disk

Select virtual disk format: Thin Provision

VM Storage Policy: Keep existing VM storage policies

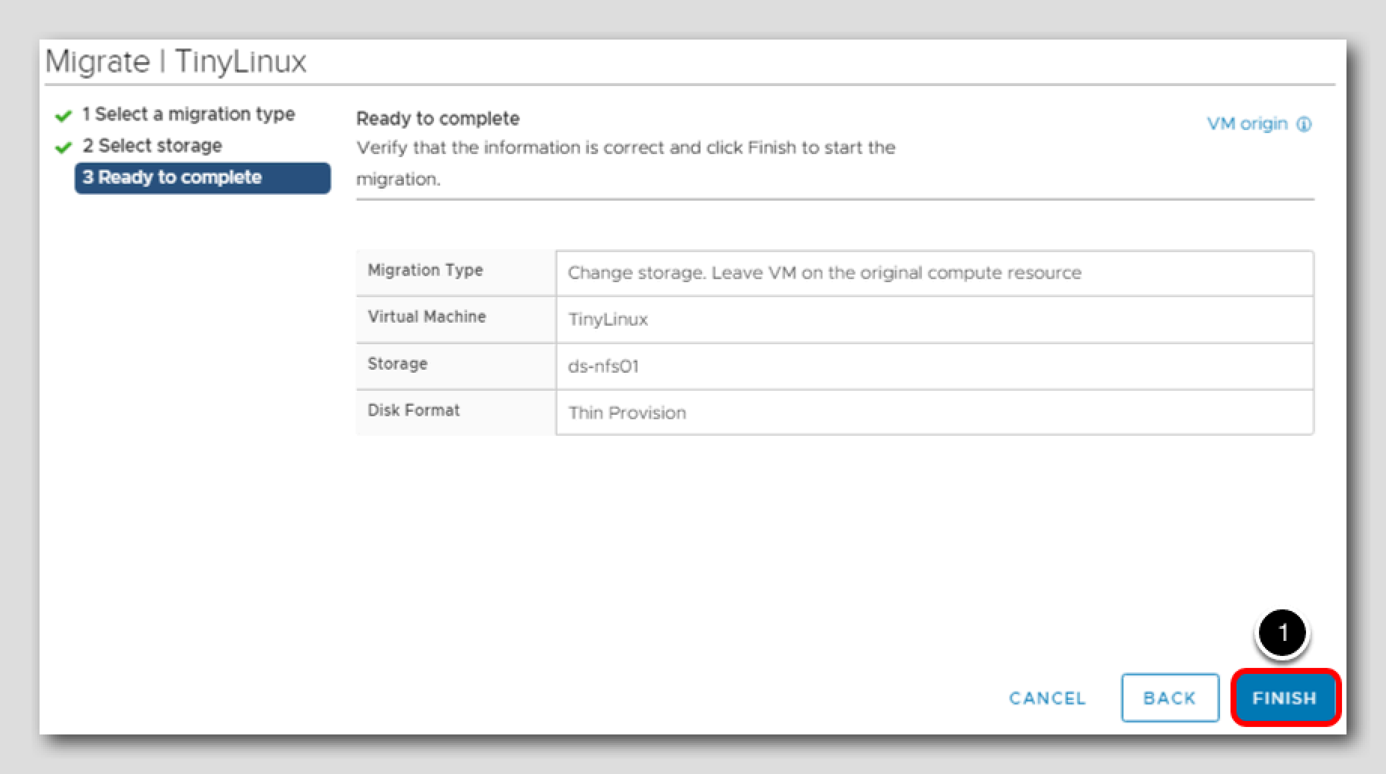
Name	Capacity	Provisioned	Free	Type	Clu
ds-iscsi01	43.75 GB	31.57 GB	18.83 GB	VMFS 6	
ds-iscsi02	43.75 GB	1.41 GB	42.34 GB	VMFS 6	
ds-nfs01	5.78 GB	96 KB	5.78 GB	NFS v3	
ds-nfs02	5.78 GB	88 KB	5.78 GB	NFS v3	

Compatibility
✓ Compatibility checks succeeded.

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

[522]



Migrate | TinyLinux

Ready to complete

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

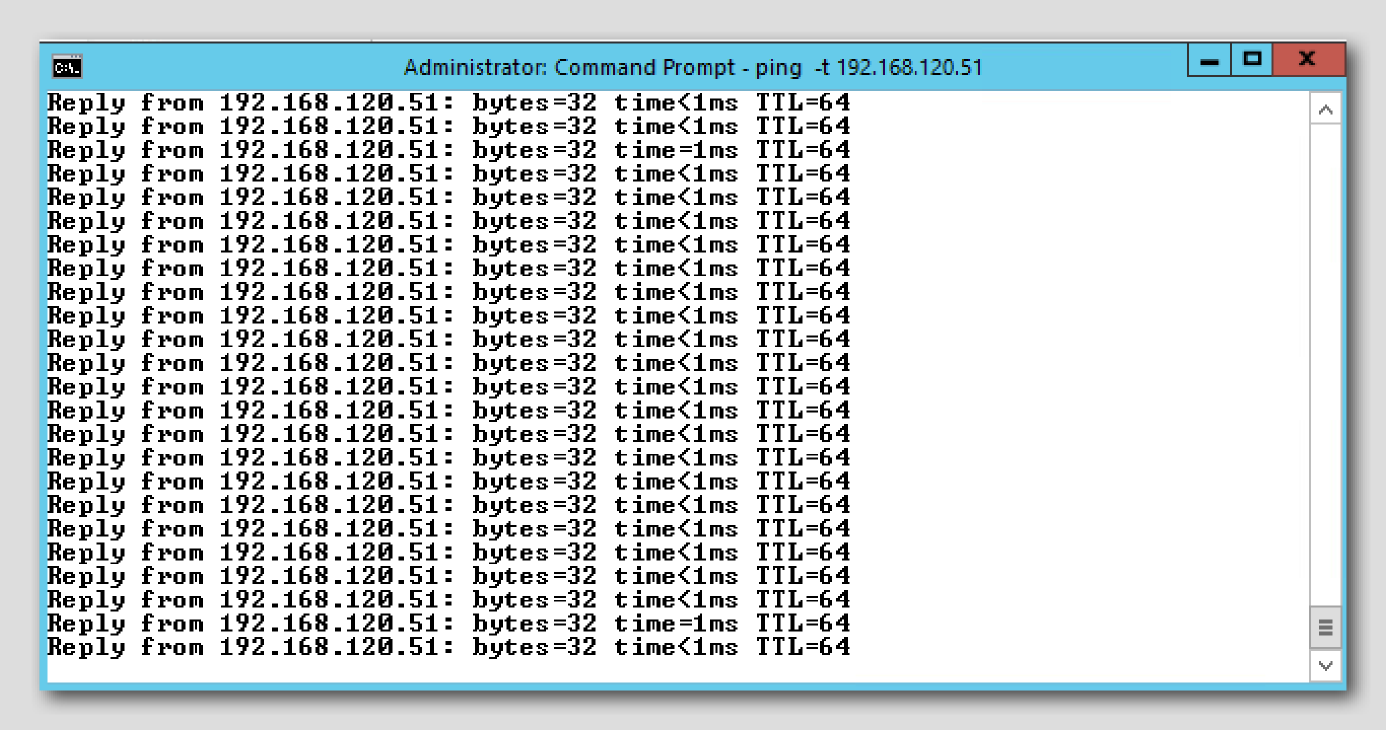
Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	TinyLinux
Storage	ds-nfs01
Disk Format	Thin Provision

1. 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

[523]



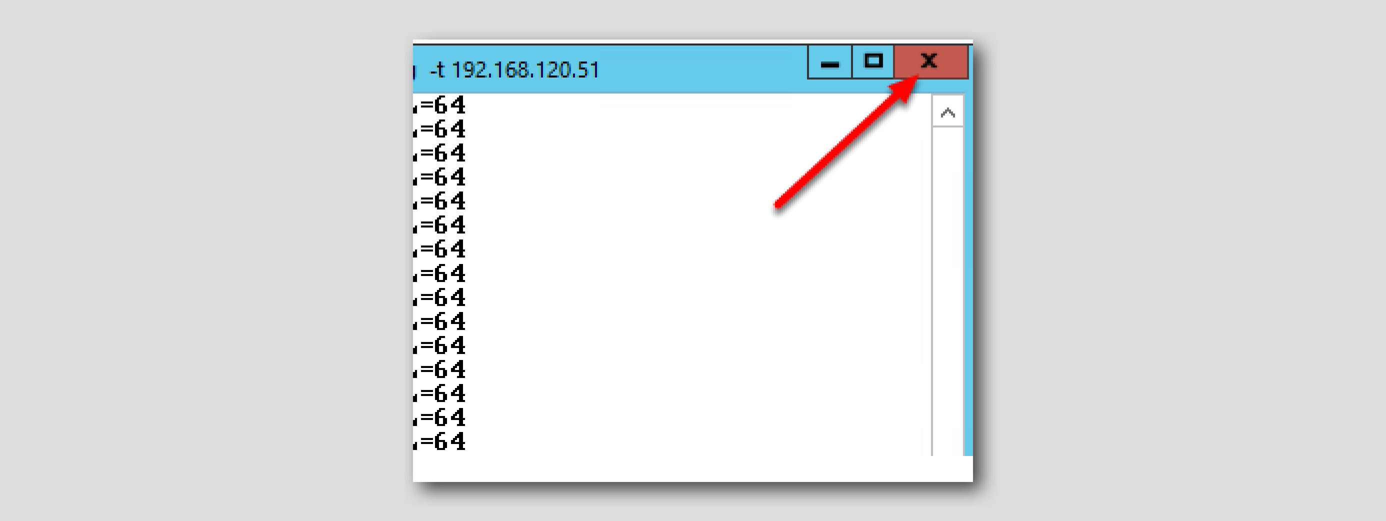
```
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time=1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time=1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
```

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

[524]

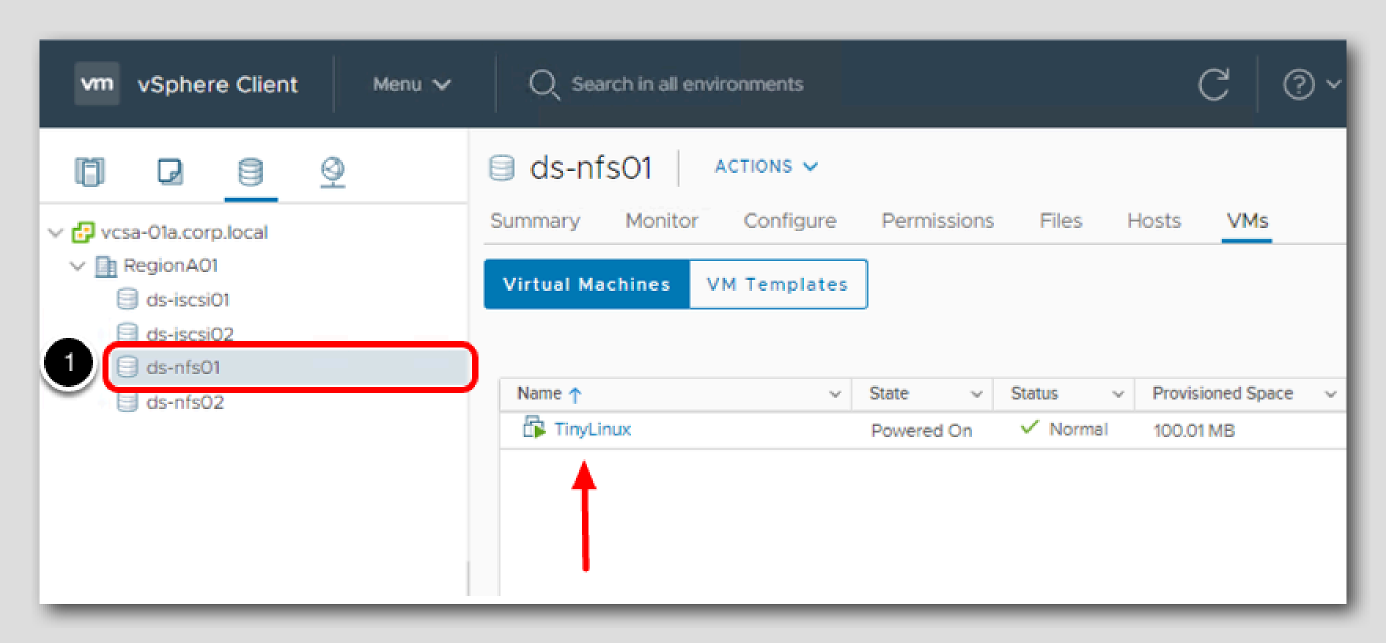


```
-t 192.168.120.51
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
=64
```

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

Confirm Storage vMotion

[525]



Name ↑	State	Status	Provisioned Space
TinyLinux	Powered On	✓ Normal	100.01 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

[526]

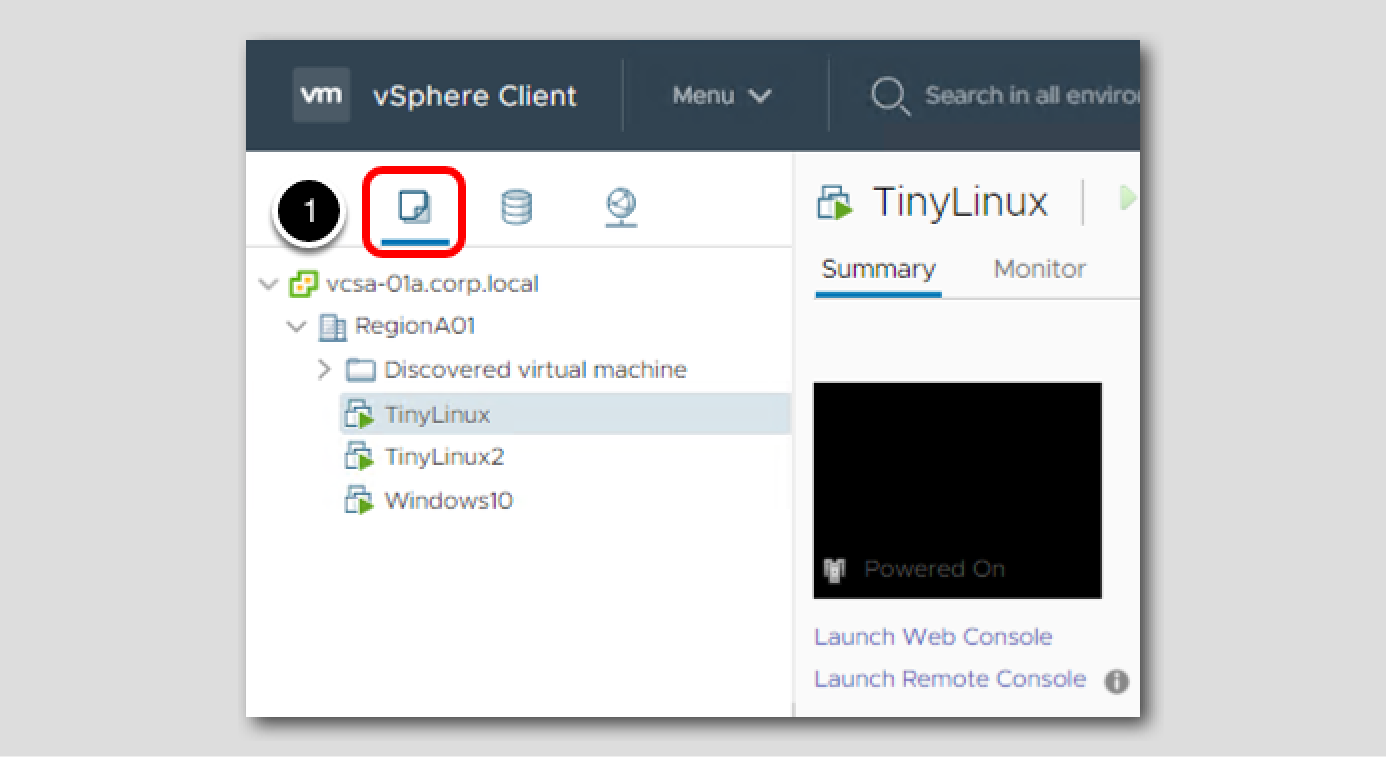
When working with Virtual Machines, you can create a virtual disk or use an existing virtual disk, A virtual disk comprises one or more files on the file system that appear as a single hard disk to the guest operating system. These disks are portable among hosts.

You use the "Create Virtual Machine" wizard to add virtual disks during virtual machine creation. However, in this lesson you will work with an existing Virtual Machine in the inventory.

This lesson will walk you through the process of adding a new virtual disk to an existing Virtual Machine. Additionally, you will extend the Virtual Machine's original disk to a larger capacity.

Navigate to the VMs and Templates management pane

[527]

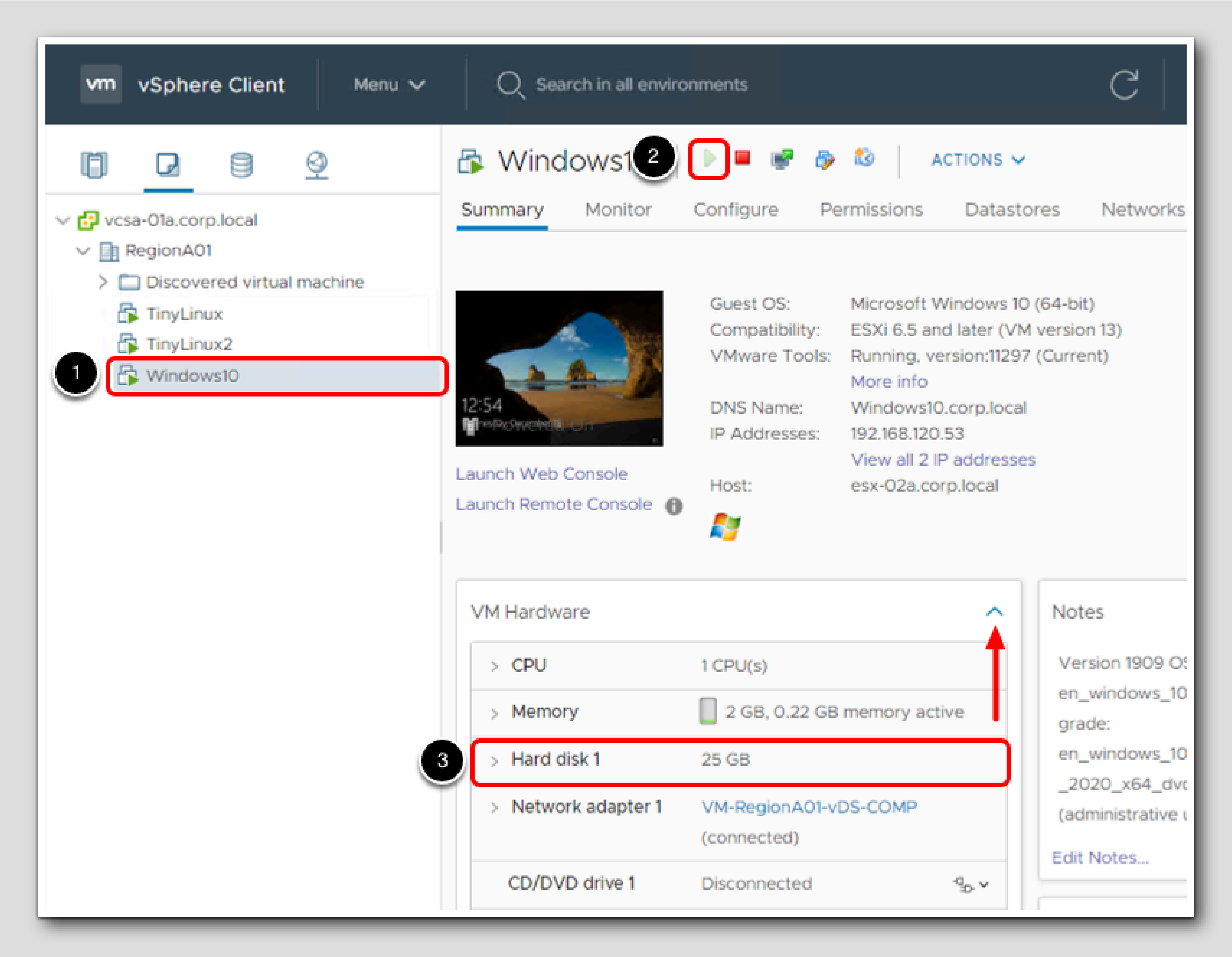


1. Select VMs and Templates.

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

[528]



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

VM Hardware

CPU	1 CPU(s)
Memory	2 GB, 0.22 GB memory active
Hard disk 1	25 GB
Network adapter 1	VM-RegionA01-vDS-COMP (connected)
CD/DVD drive 1	Disconnected

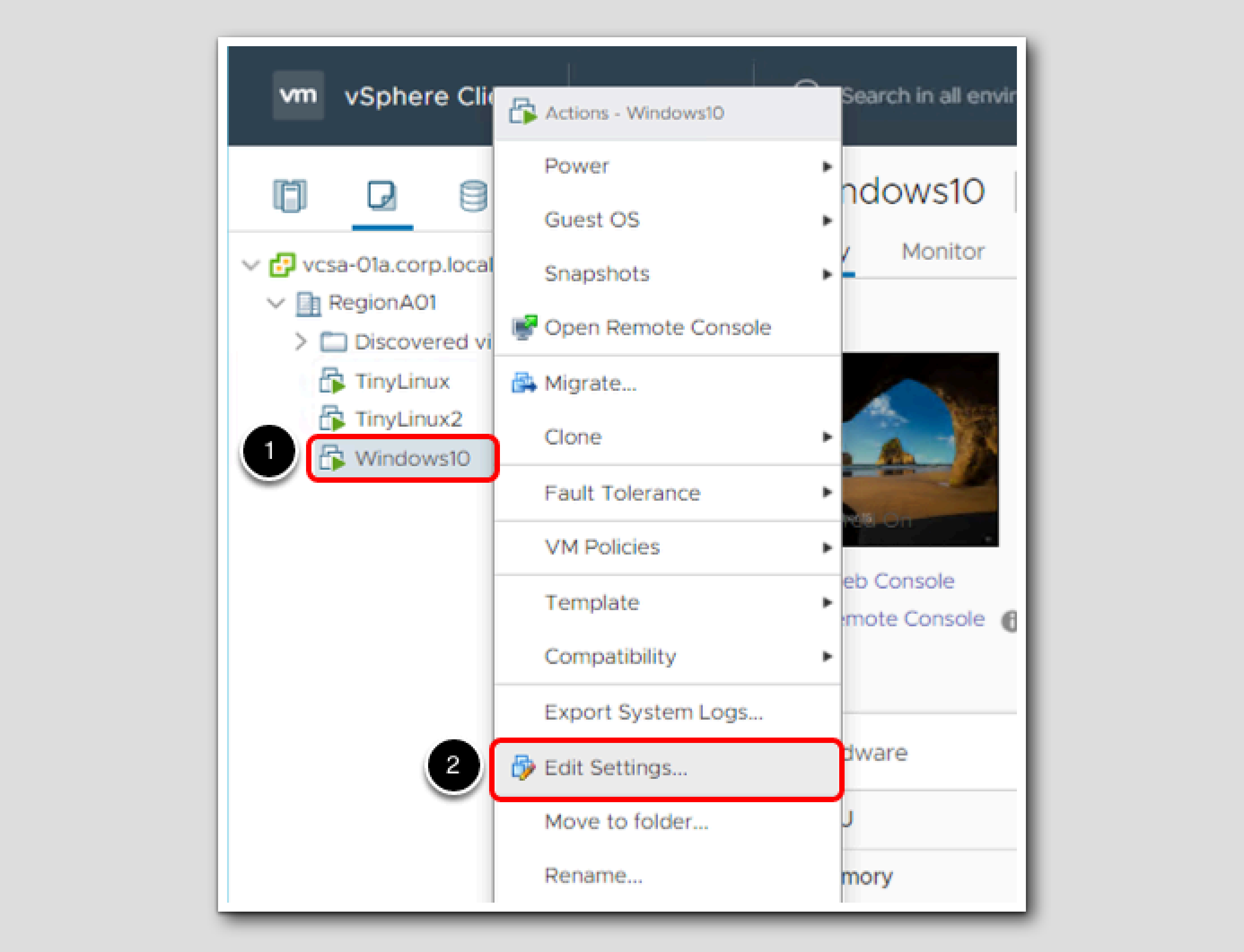
Notes

Version 1909 O
en_windows_10
grade:
en_windows_10
_2020_x64_dv
(administrative

1. Select Virtual Machine **Windows10** and click the **Summary** tab.
2. If w12-core is not powered on, click the **power on** button.
3. In the VM Hardware pane, note the original disk configuration - single hard disk with a capacity of 25.00 GB. You may need to expand the VM Hardware section to see it.

Edit VM Settings

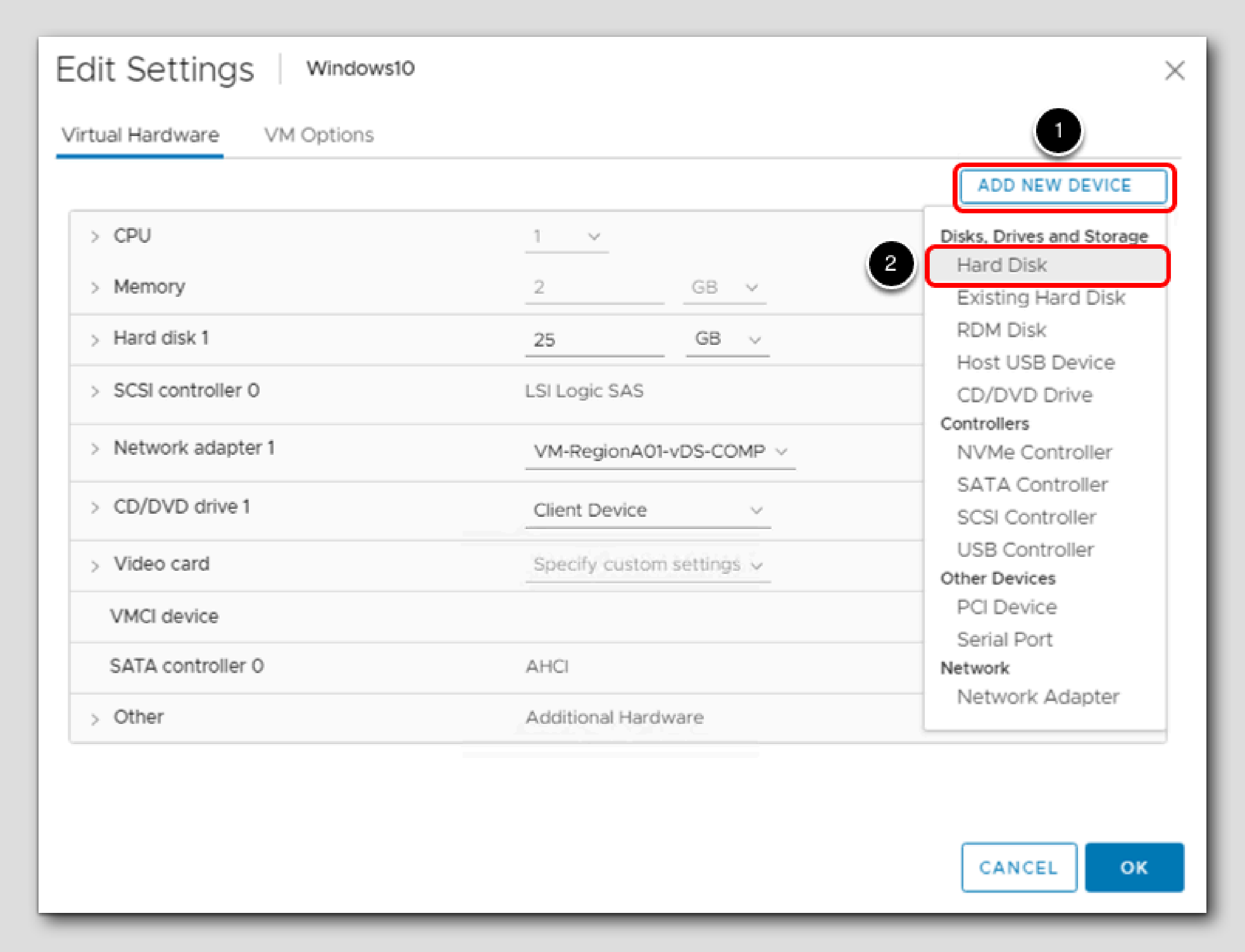
[529]



1. Right-click on Windows10
2. Select Edit Settings

Add New Device

[530]

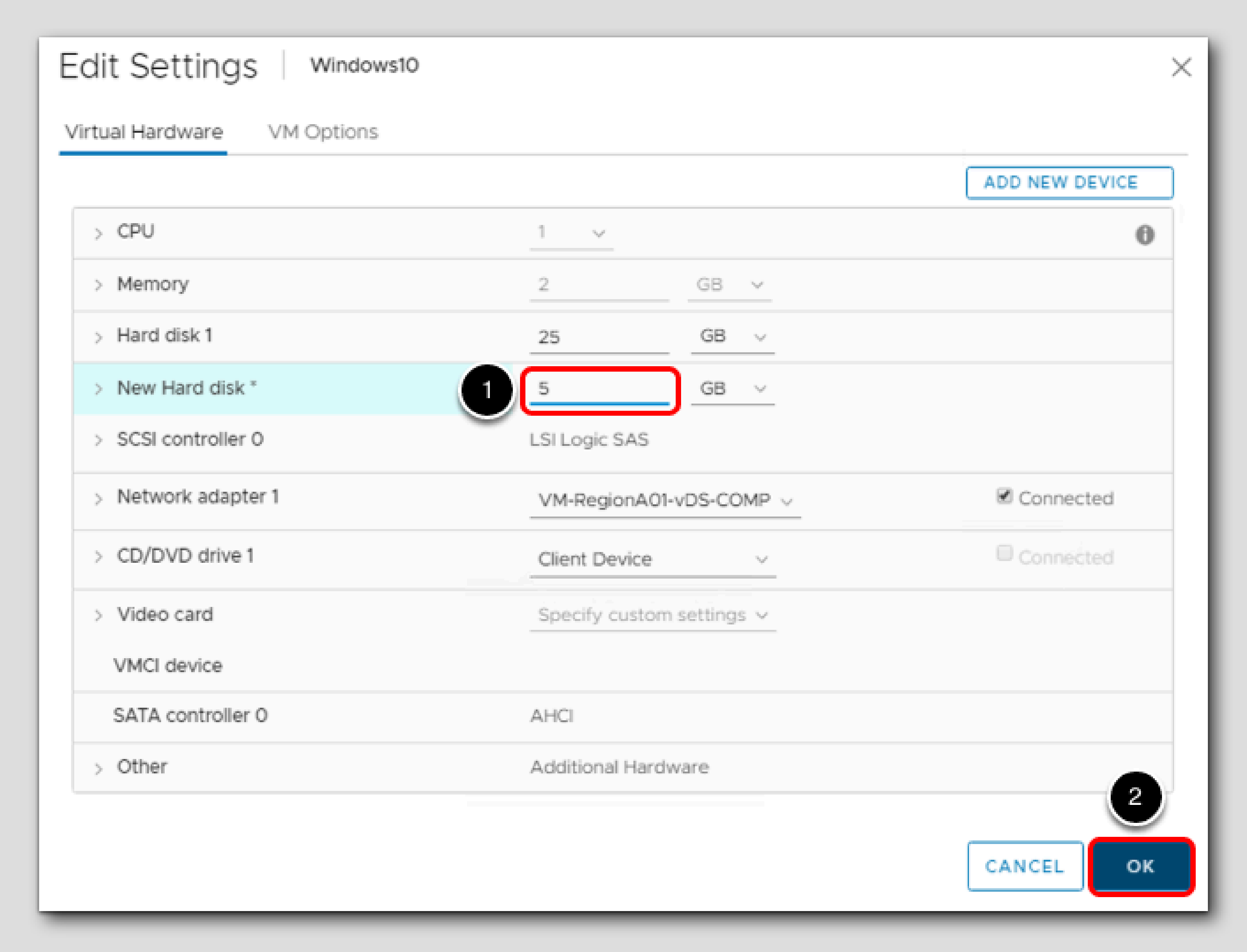


CPU 1
Memory 2 GB
Hard disk 1 25 GB
SCSI controller 0 LSI Logic SAS
Network adapter 1 VM-RegionA01-vDS-COMP
CD/DVD drive 1 Client Device
Video card Specify custom settings
VMCI device
SATA controller 0 AHCI
Other Additional Hardware

1. Click the Add New Device button.
2. Click Hard Disk.

Configure Size and Provisioning settings

[531]



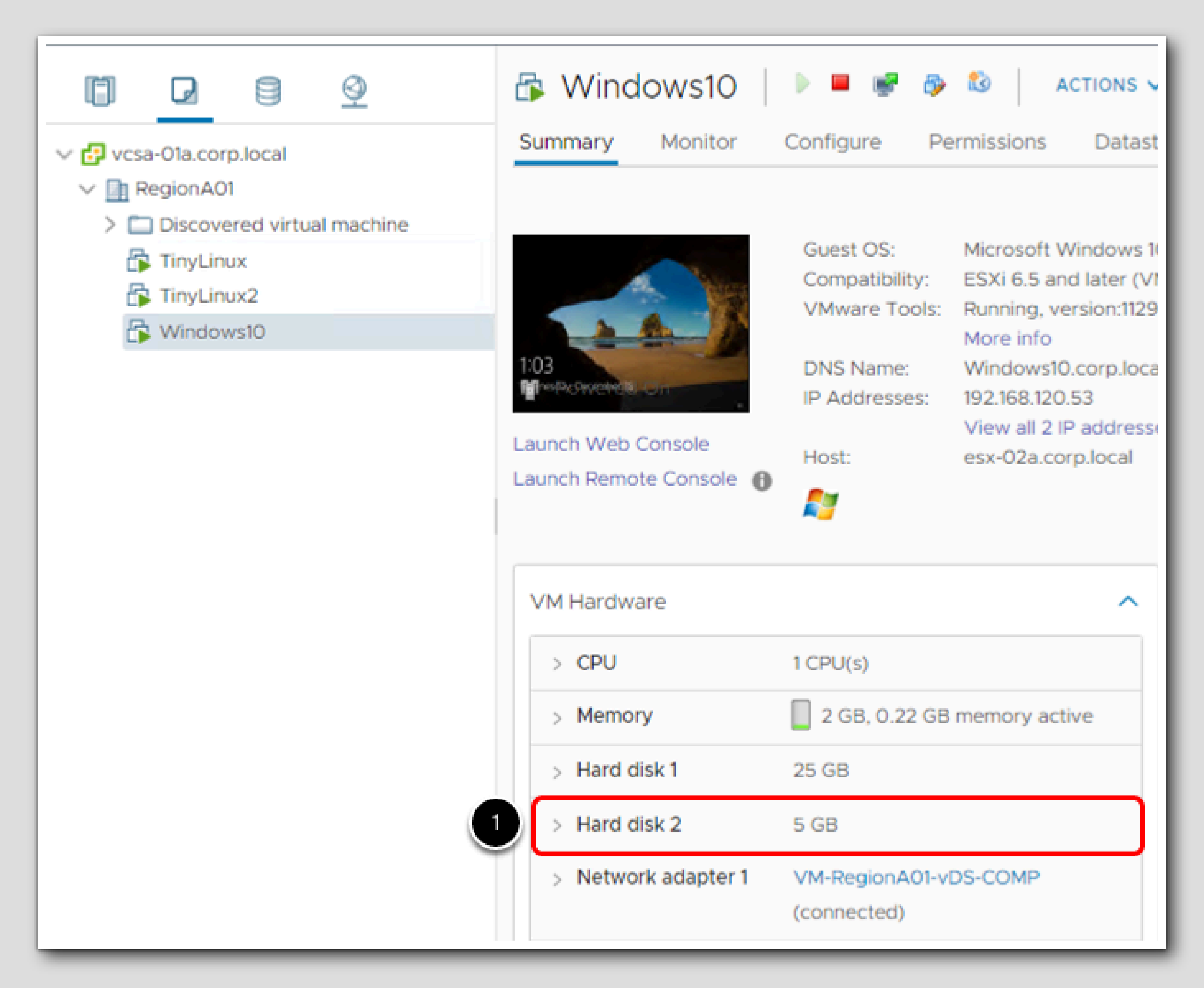
Edit Settings | Windows10

CPU	1		
Memory	2	GB	
Hard disk 1	25	GB	
New Hard disk *	5	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	VM-RegionA01-vDS-COMP		☑ Connected
CD/DVD drive 1	Client Device		□ Connected
Video card	Specify custom settings		
VMCI device			
SATA controller 0	AHCI		
Other	Additional Hardware		

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

Monitor task progress

[532]



Guest OS: Microsoft Windows 1
Compatibility: ESXi 6.5 and later (V
VMware Tools: Running, version:1129
More info
DNS Name: Windows10.corp.loca
IP Addresses: 192.168.120.53
View all 2 IP address
Host: esx-02a.corp.local

VM Hardware

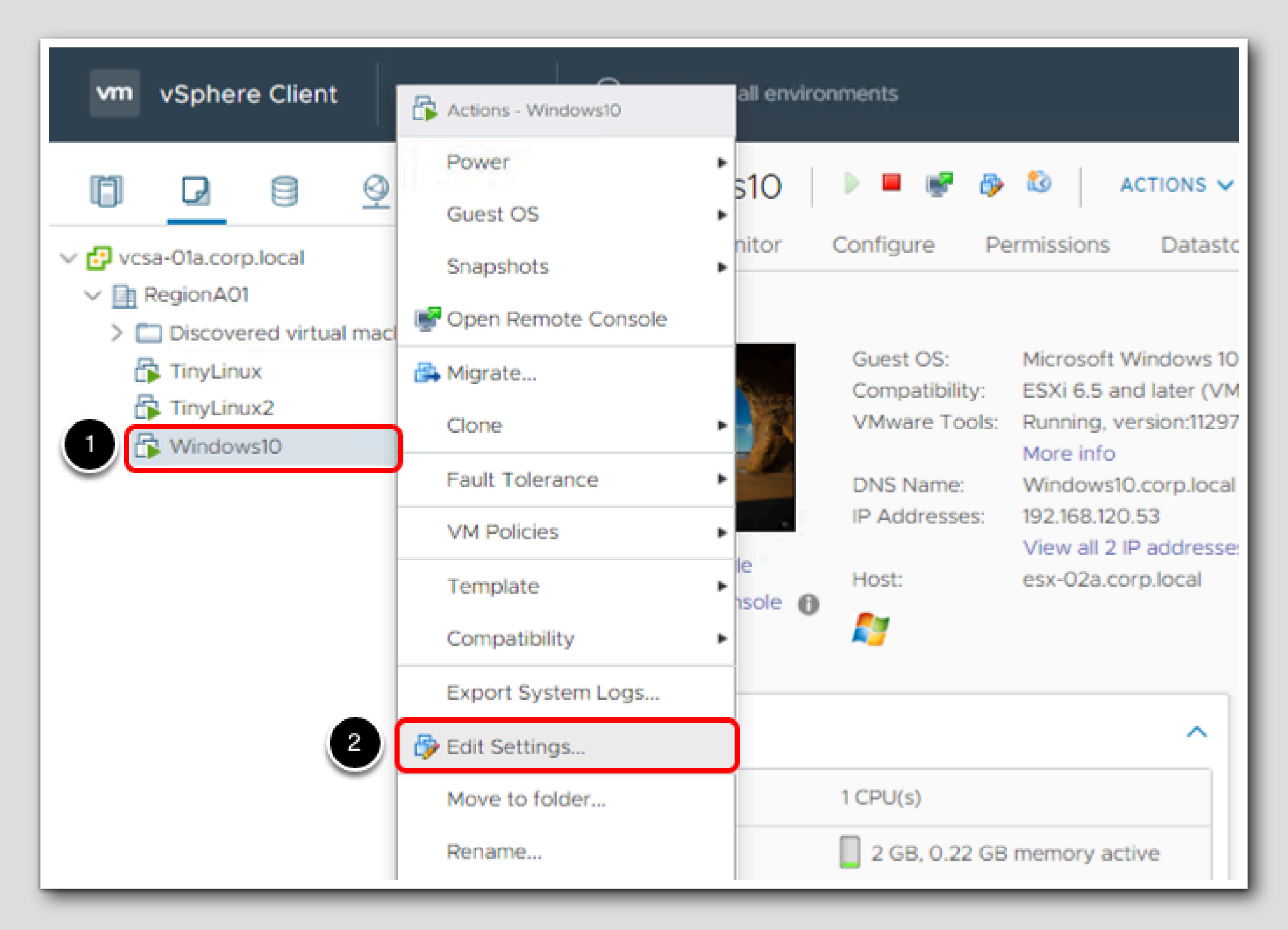
CPU	1 CPU(s)
Memory	2 GB, 0.22 GB memory active
Hard disk 1	25 GB
Hard disk 2	5 GB
Network adapter 1	VM-RegionA01-vDS-COMP (connected)

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

[533]

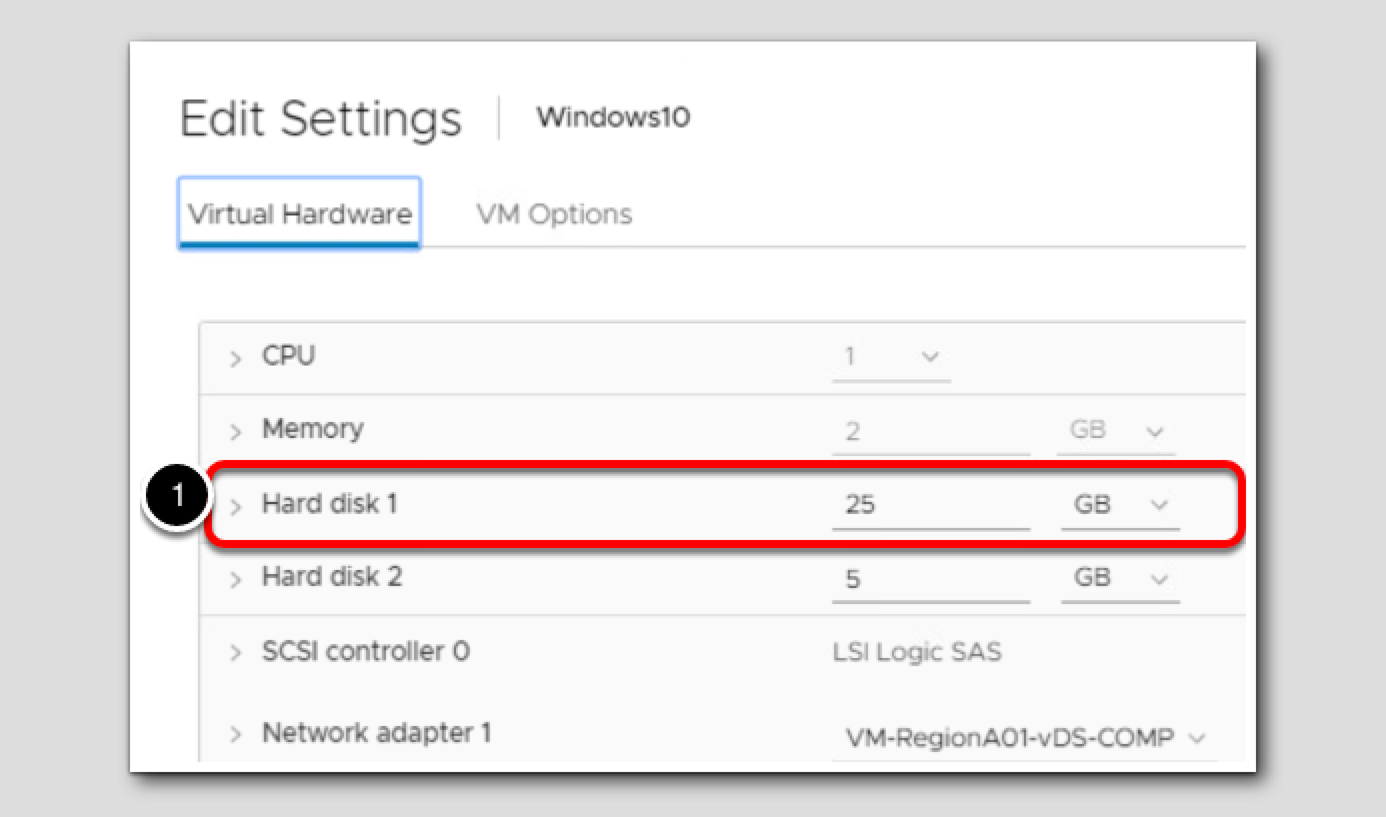


In this section, you will extend an existing Virtual Disk for a Virtual Machine.

1. Right-click the Virtual Machine **Windows10**.
2. Select **Edit Settings**.

Hard disk 1 settings

[534]



Edit Settings | Windows10

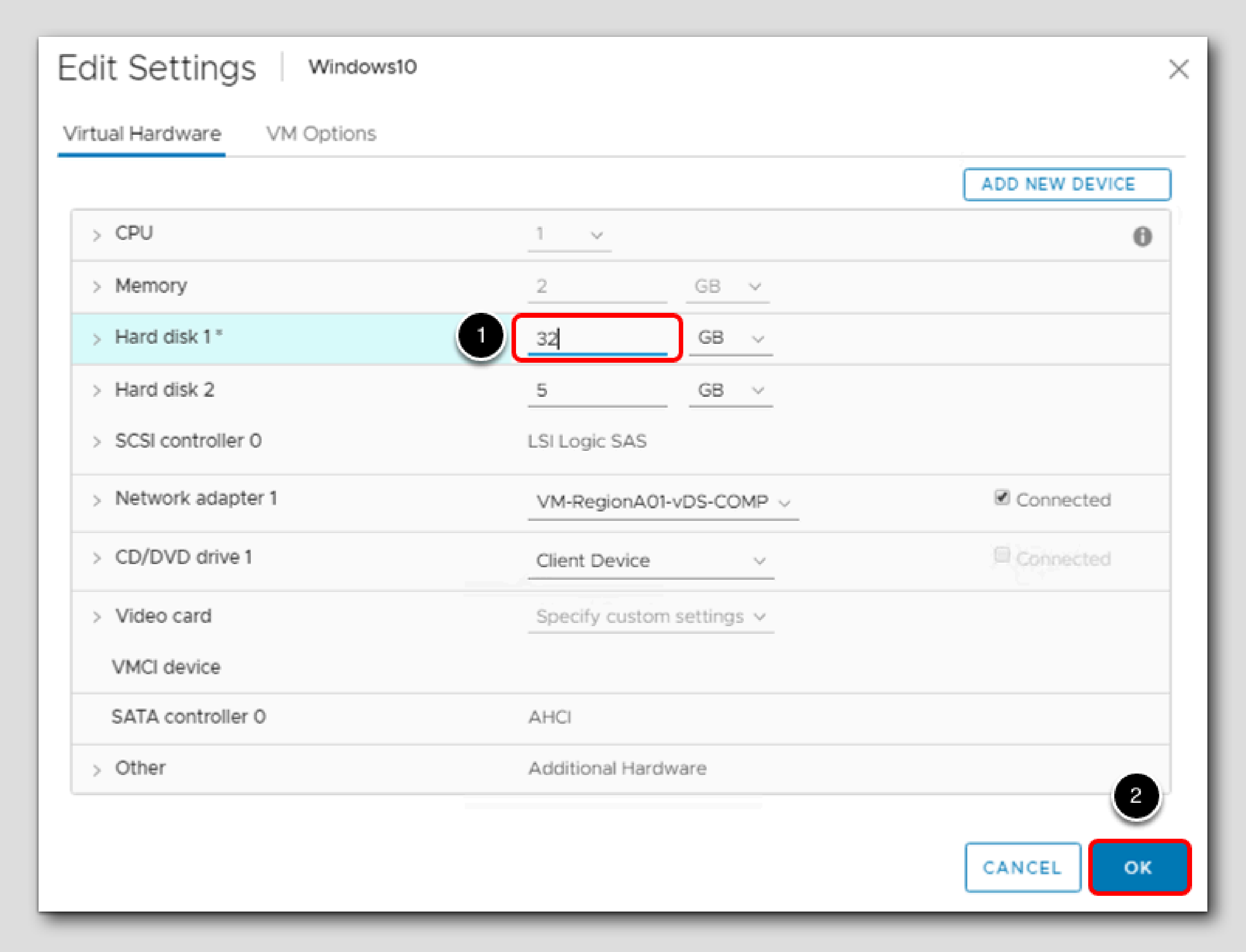
Virtual Hardware | VM Options

CPU	1	
Memory	2	GB
Hard disk 1	25	GB
Hard disk 2	5	GB
SCSI controller 0	LSI Logic SAS	
Network adapter 1	VM-RegionA01-vDS-COMP	

1. In the Edit Settings wizard, note the capacity for Hard disk 1 is **25** GB.

Extend Hard disk 1

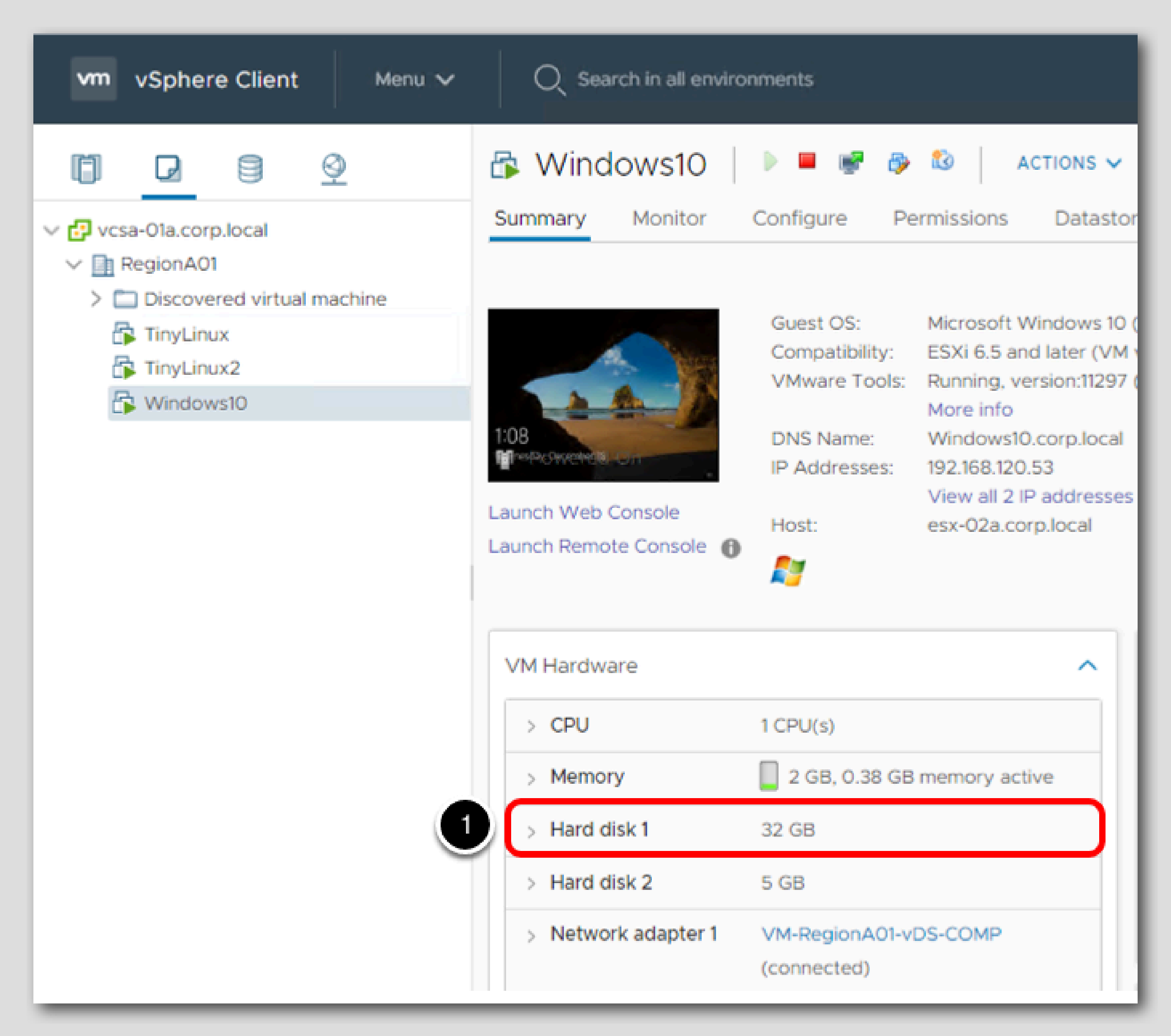
[535]



CPU	1		
Memory	2	GB	
Hard disk 1 *	32	GB	
Hard disk 2	5	GB	
SCSI controller 0	LSI Logic SAS		
Network adapter 1	VM-RegionA01-vDS-COMP		☑ Connected
CD/DVD drive 1	Client Device		□ Connected
Video card	Specify custom settings		
VMCI device			
SATA controller 0	AHCI		
Other	Additional Hardware		

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

Monitor task progress



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

VM Hardware

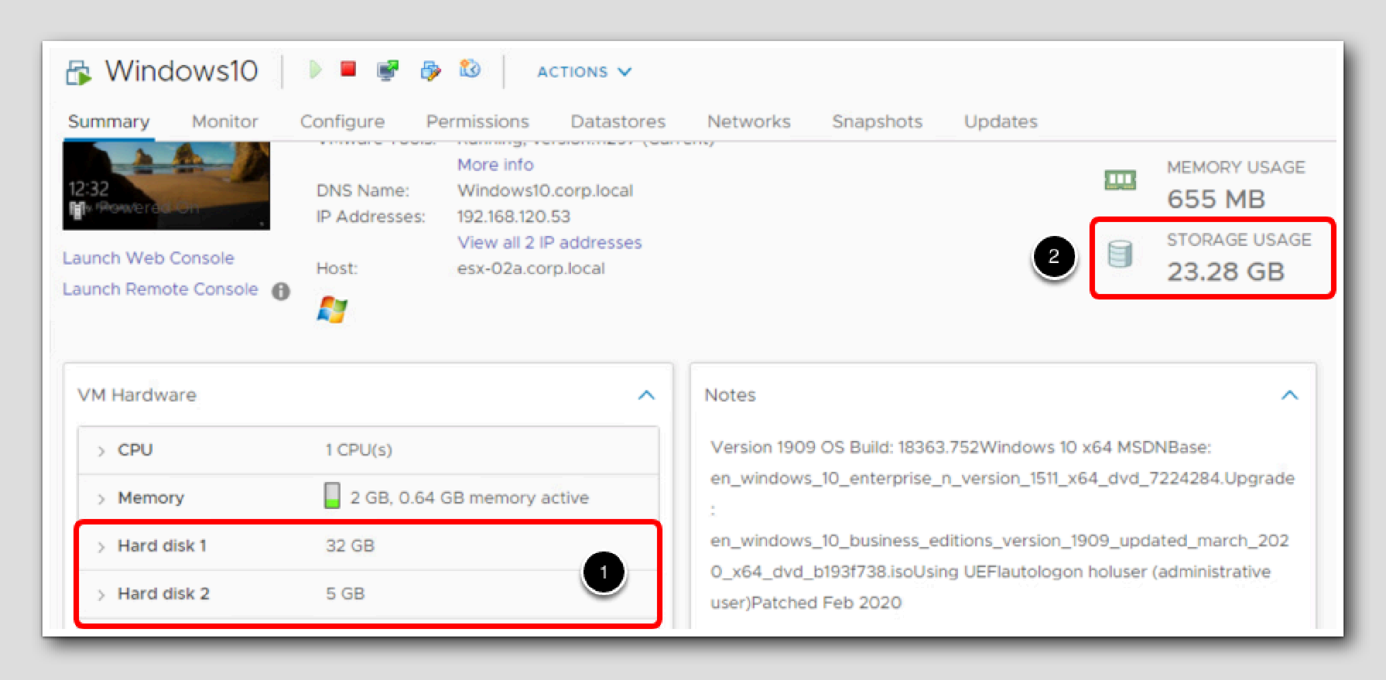
CPU	1 CPU(s)
Memory	2 GB, 0.38 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB
Network adapter 1	VM-RegionA01-vDS-COMP (connected)

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

[537]



More info

DNS Name: Windows10.corp.local

IP Addresses: 192.168.120.53

View all 2 IP addresses

Host: esx-02a.corp.local

MEMORY USAGE
655 MB

STORAGE USAGE
23.28 GB

VM Hardware

CPU	1 CPU(s)
Memory	2 GB, 0.64 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB

Notes

Version 1909 OS Build: 18363.752Windows 10 x64 MSDNBase: en_windows_10_enterprise_n_version_1511_x64_dvd_7224284.Upgrade : en_windows_10_business_editions_version_1909_updated_march_2020_x64_dvd_b193f738.isoUsing UEFIautologon holuser (administrative user)Patched Feb 2020

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

[538]

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.

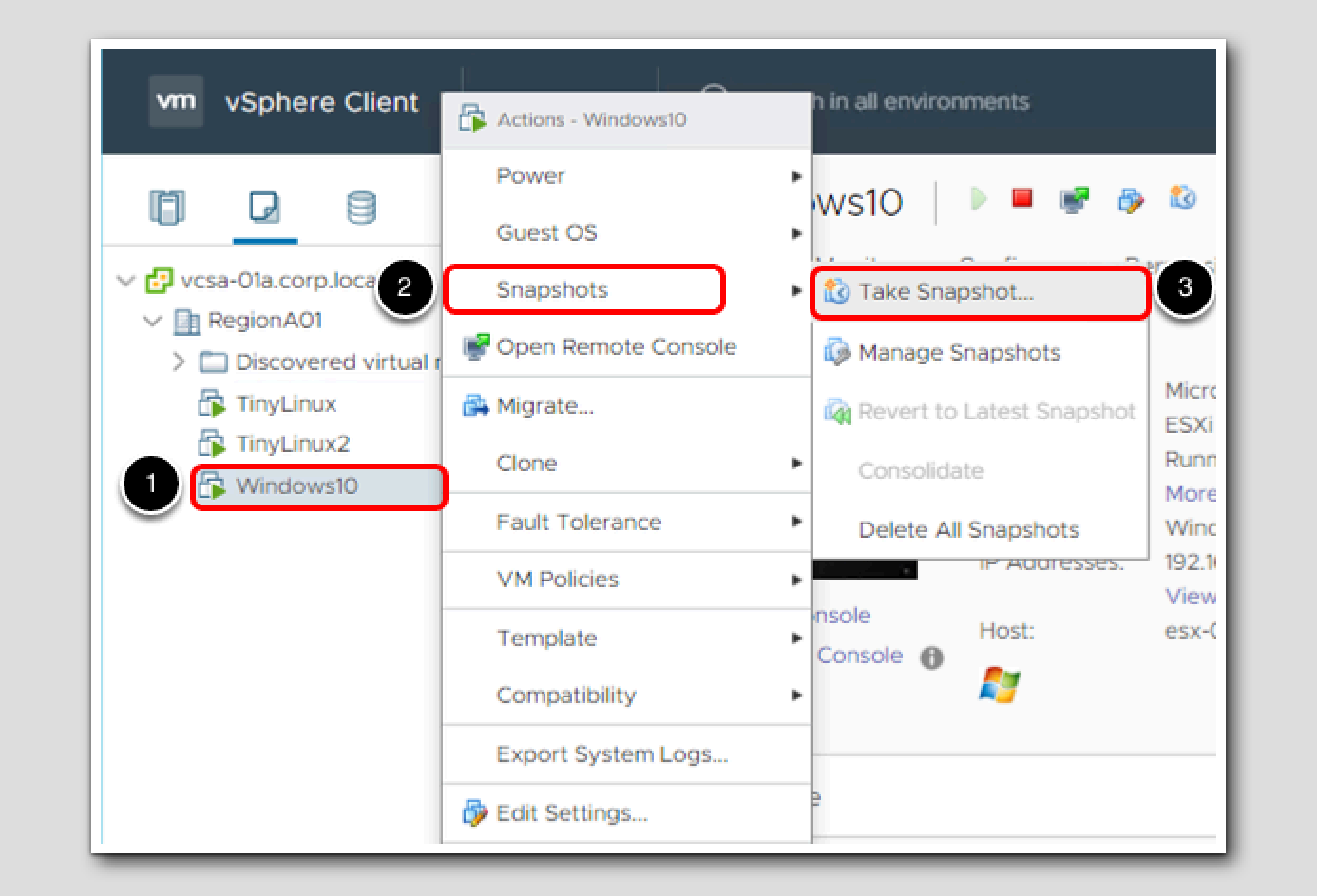
A Virtual Machine snapshot preserves the following information:

- 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

[539]

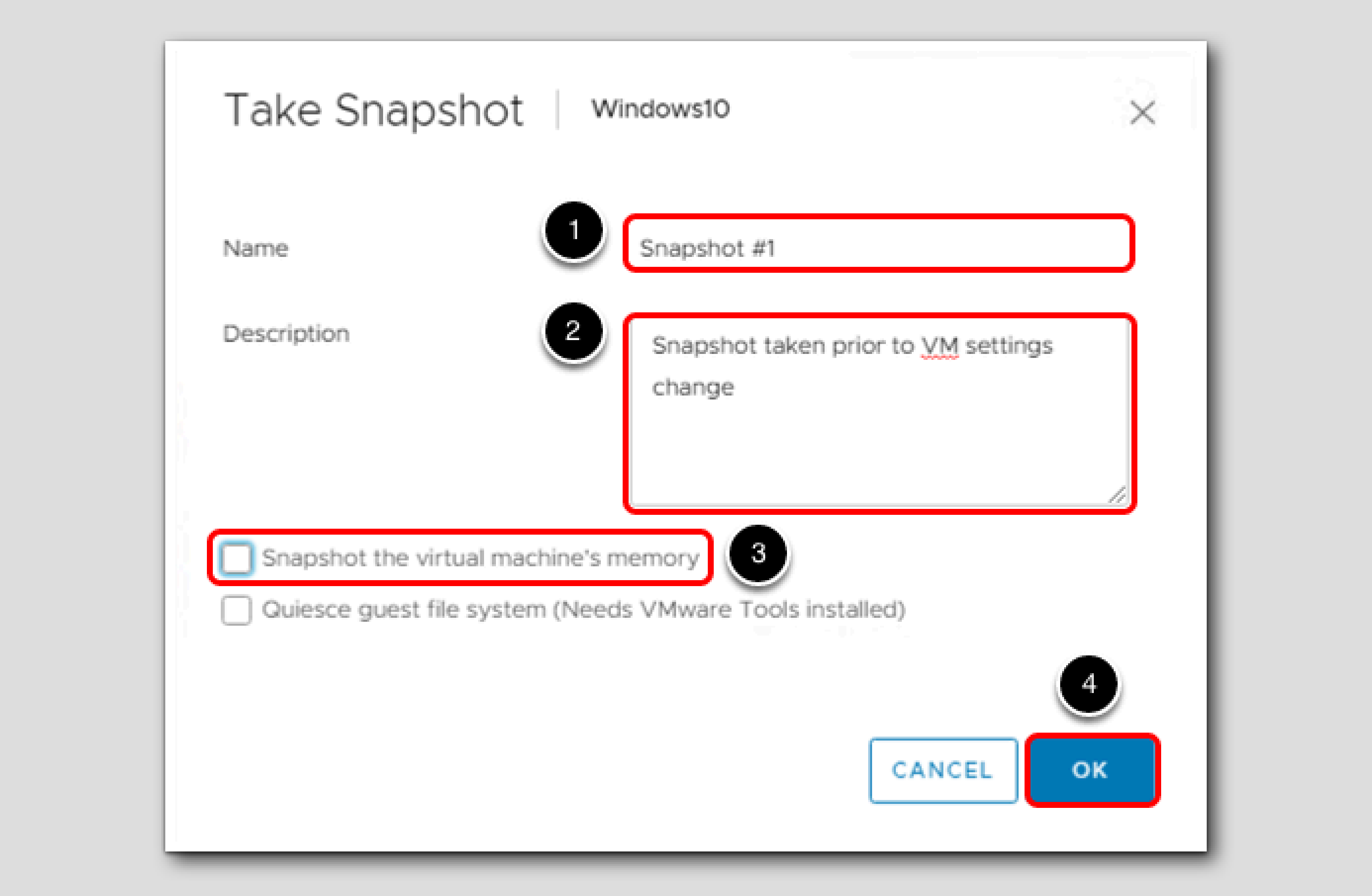


In this step, you'll take a Snapshot of a Virtual Machine.

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

Enter a Name and Description for the VM Snapshot

[540]



Take Snapshot | Windows10

Name: Snapshot #1

Description: Snapshot taken prior to VM settings change

□ Snapshot the virtual machine's memory

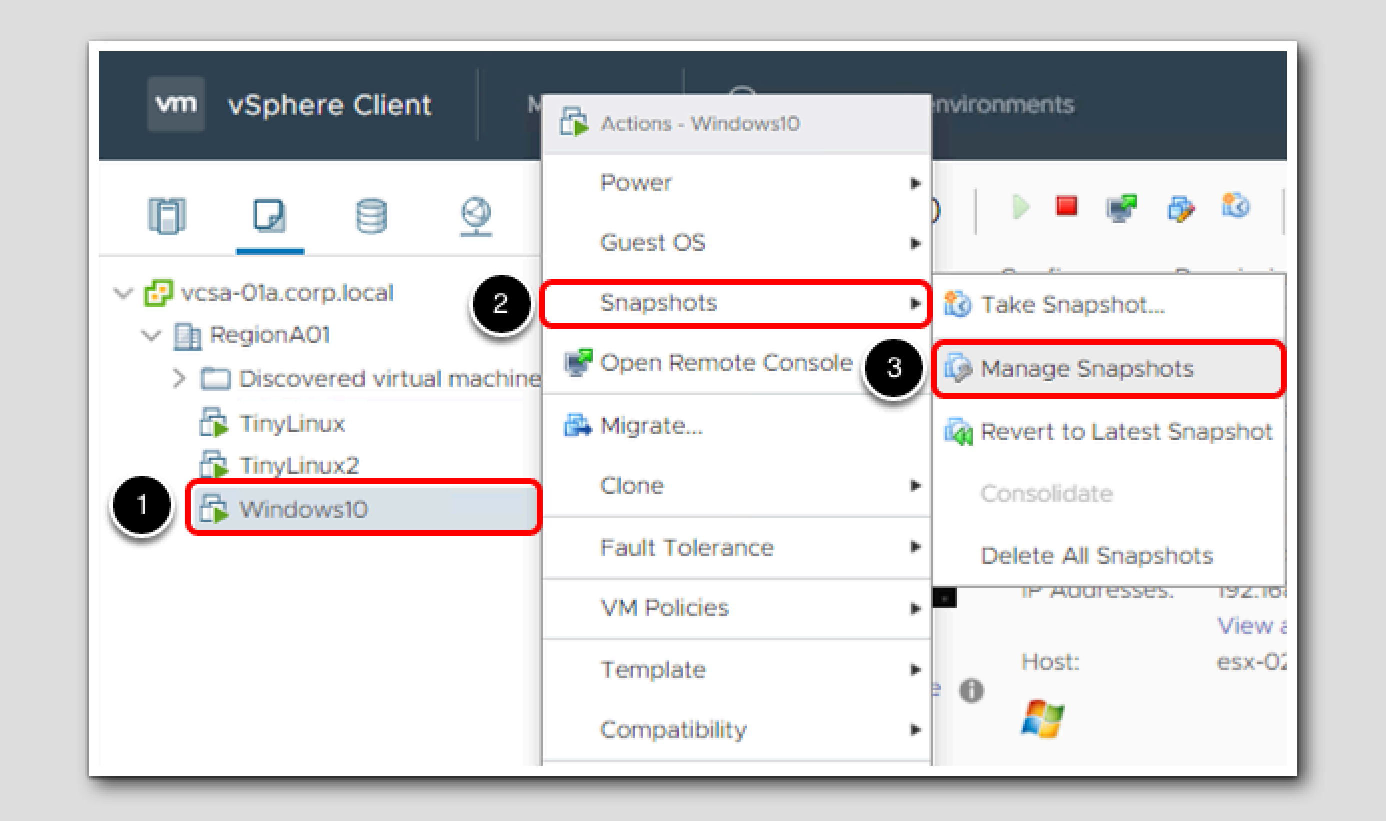
□ Quiesce guest file system (Needs VMware Tools installed)

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

[541]

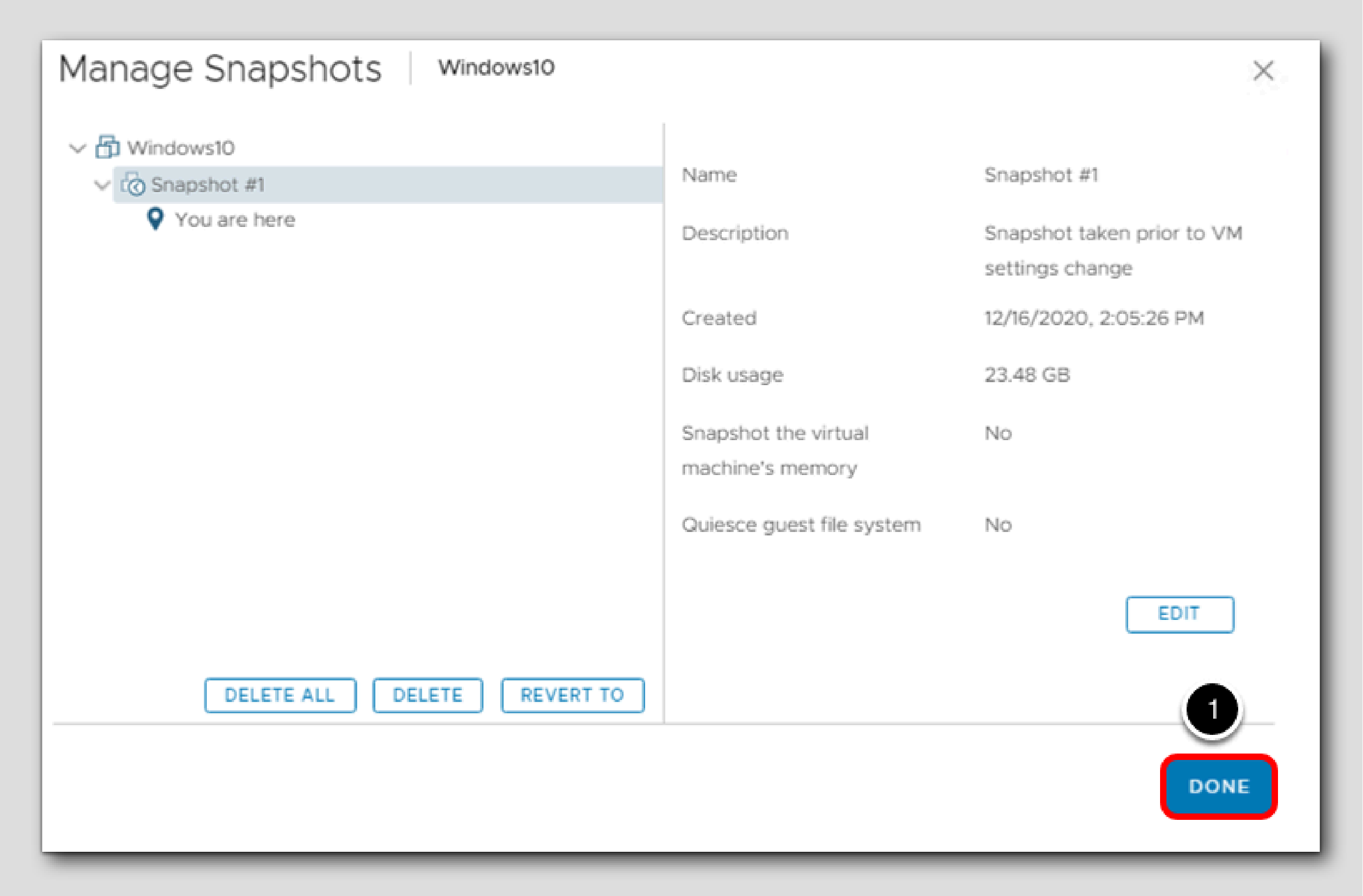


Note the progress in the Recent Tasks pane. Once the snapshot task is complete:

1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Snapshot Details

[542]



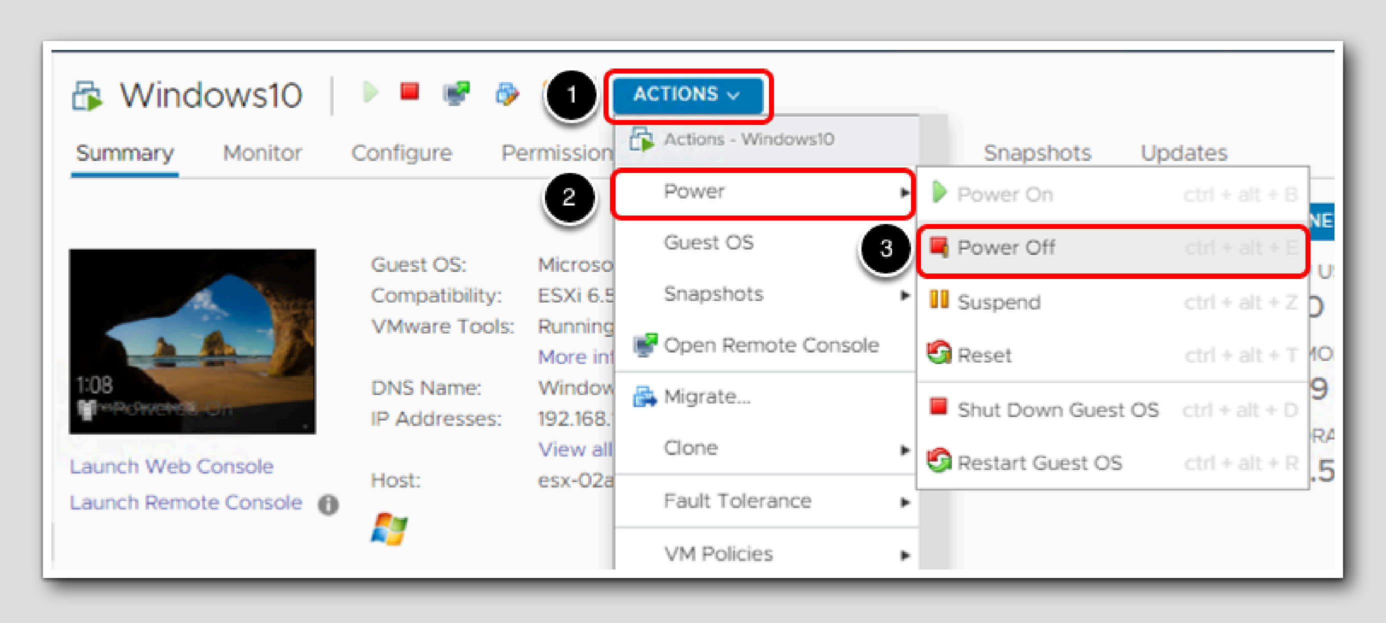
Manage Snapshots | Windows10

Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	12/16/2020, 2:05:26 PM
Disk usage	23.48 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

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



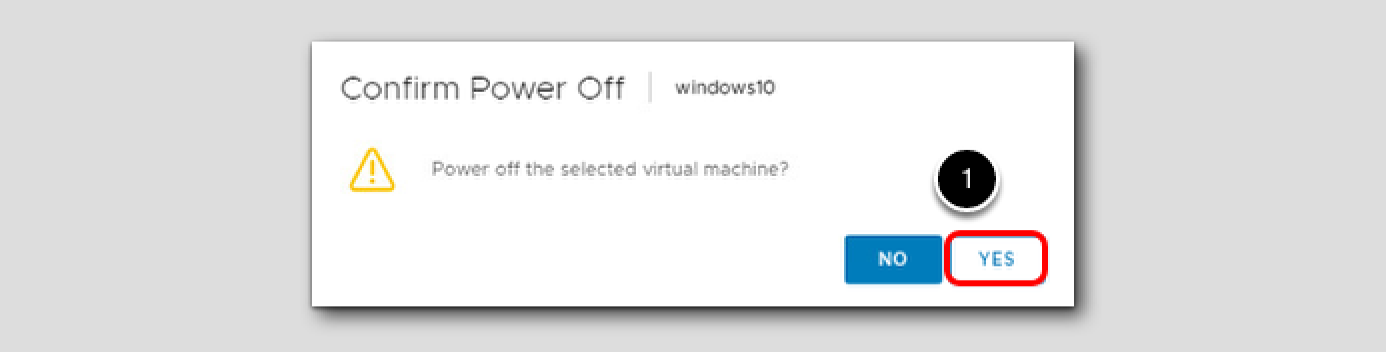
Guest OS: Microso
Compatibility: ESXi 6.5
VMware Tools: Running
More inf
DNS Name: Window
IP Addresses: 192.168.
View all
Host: esx-02a

In this section, you will change the memory configuration for the Virtual Machine.

To change the memory configuration for Windows10, we will need to shut it down.

1. Click the Actions menu.
2. Select Power.
3. Click on Power Off.

NOTE: This is not the proper way to shut the VM down gracefully, but for our lab environment, it provides a quick way to power off a machine.

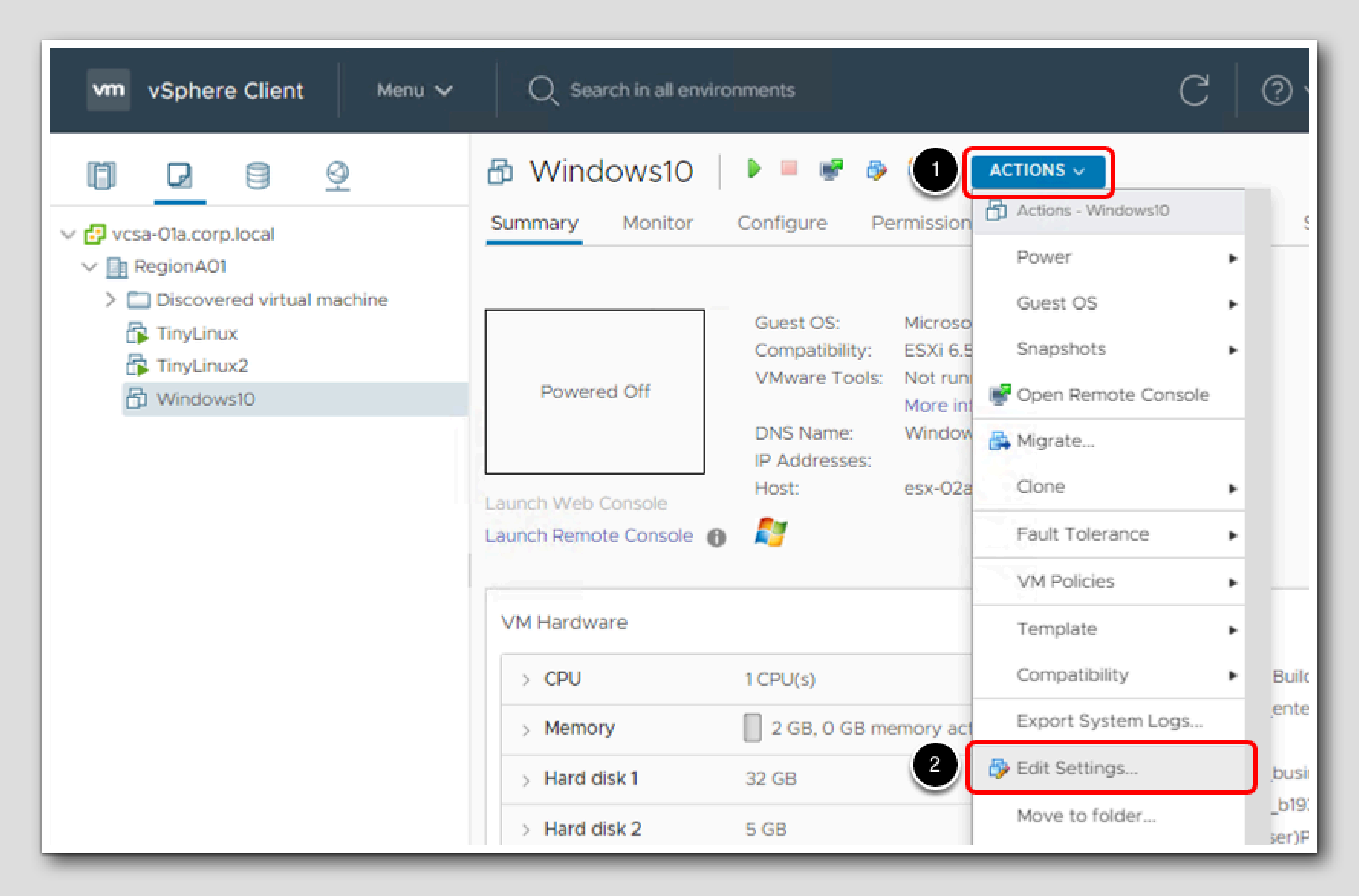


Power off the selected virtual machine?

1. Click the Yes button to power off the virtual machine.

Launch the Edit Settings wizard

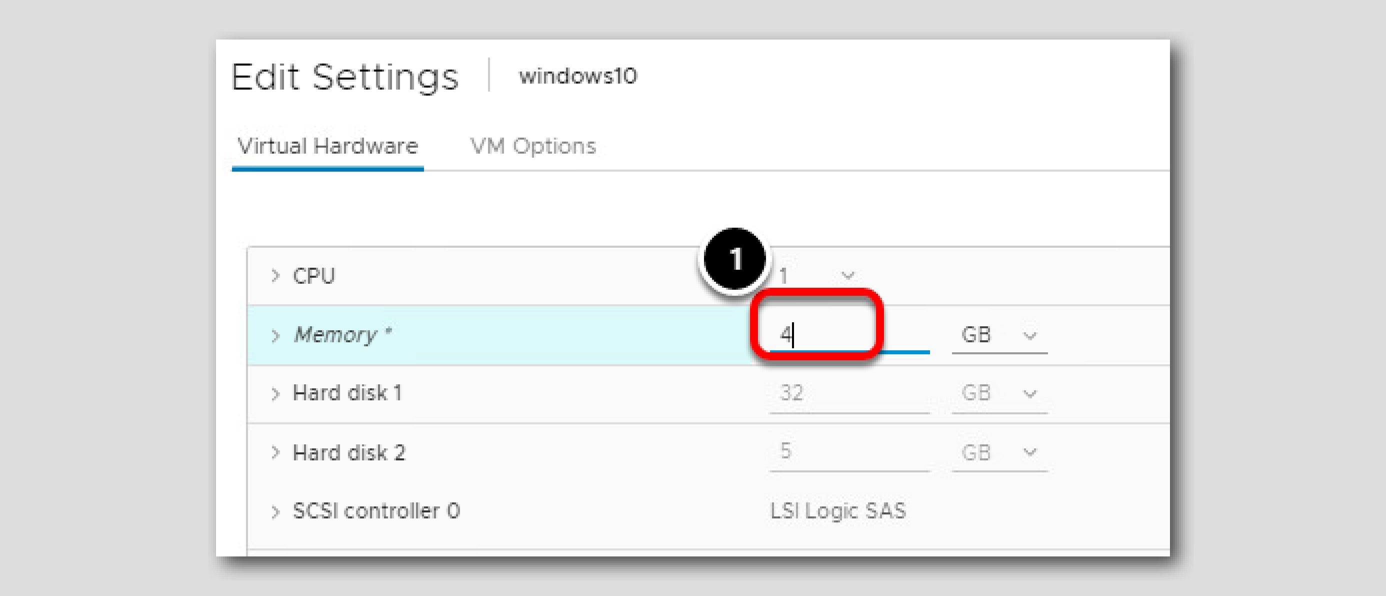
[544]



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

Change the Virtual Machine&#39;s settings

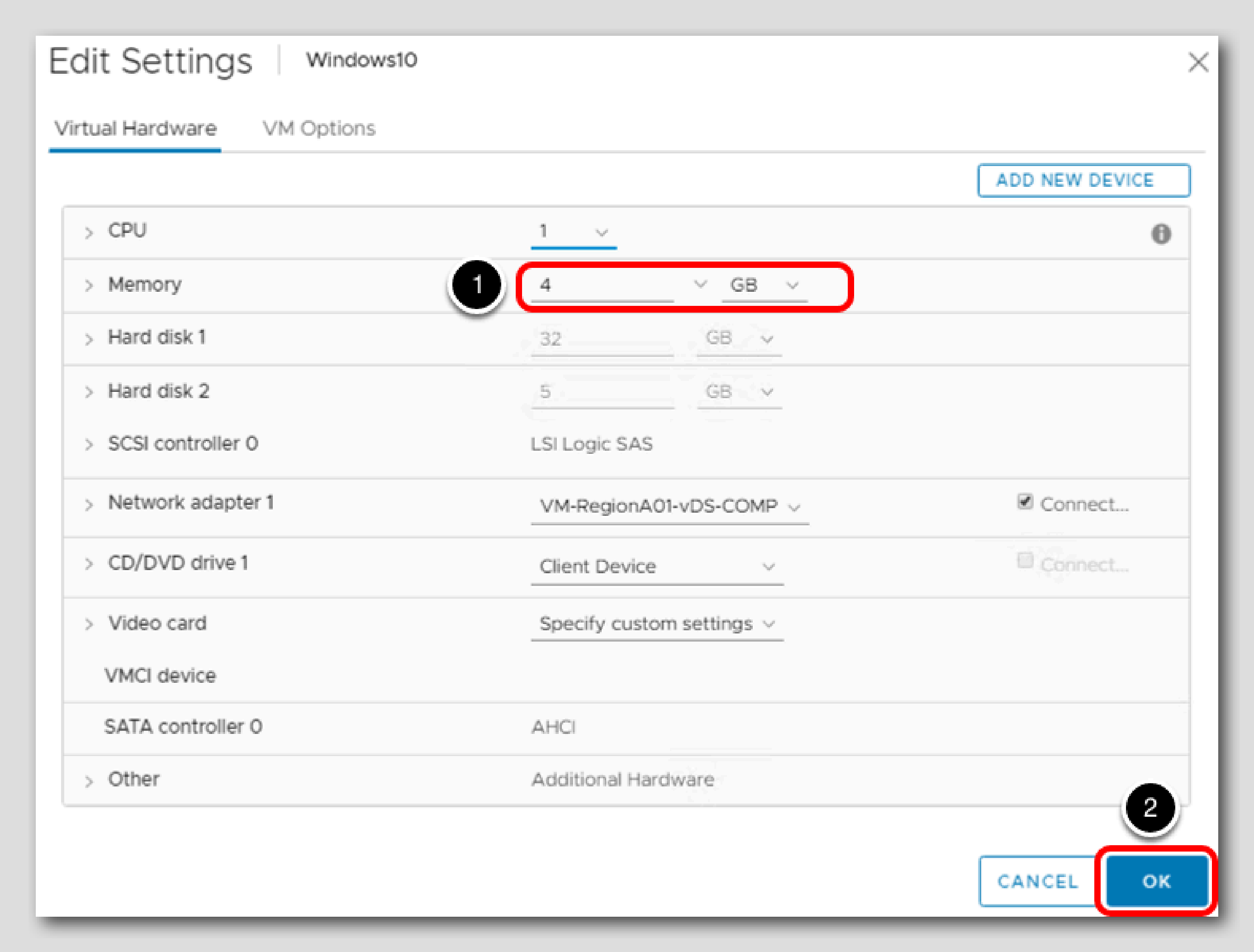
[545]



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

Review the Virtual Machine&#39;s new settings

[546]



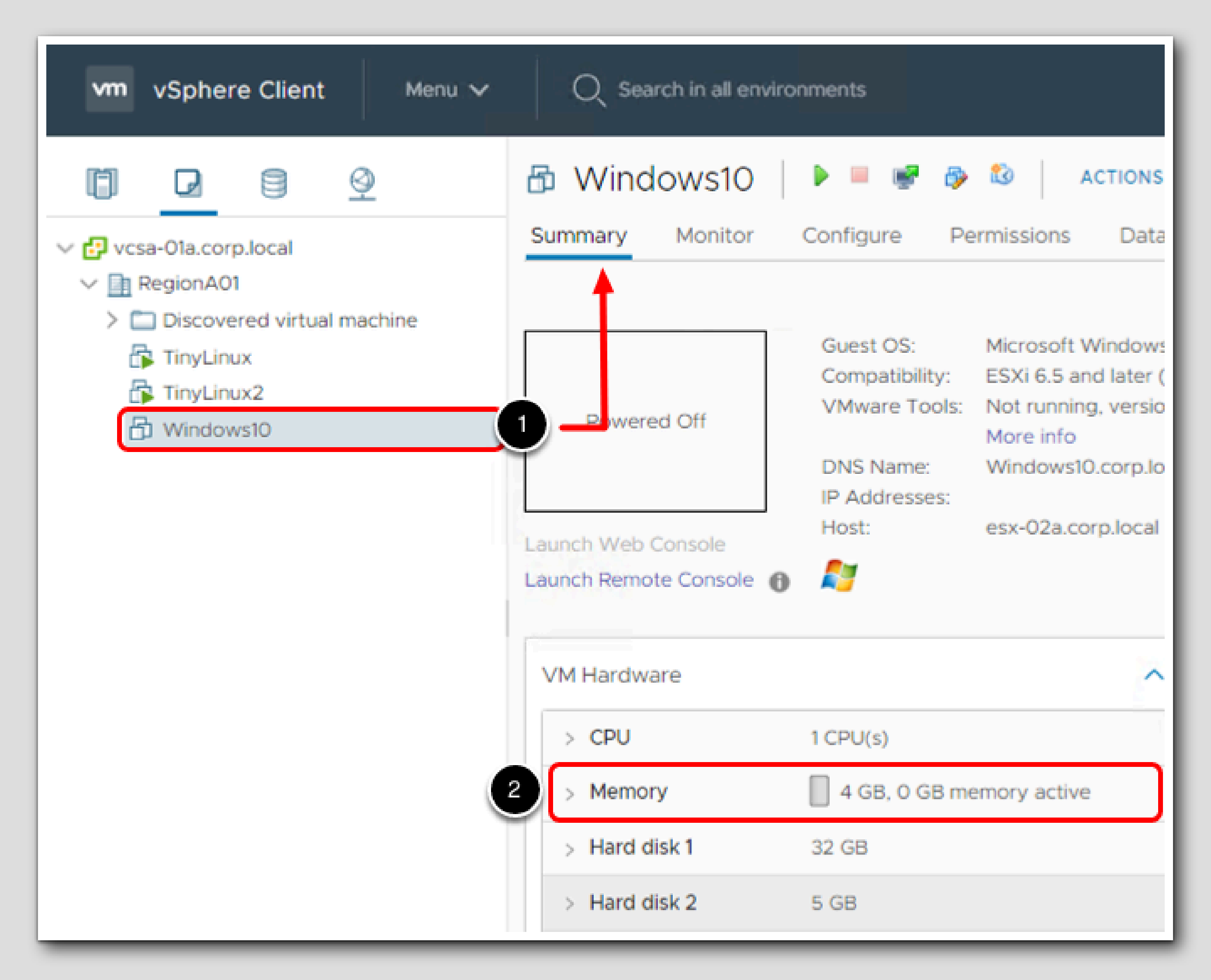
Edit Settings | Windows10

CPU	1	
Memory	4 GB	
Hard disk 1	32 GB	
Hard disk 2	5 GB	
SCSI controller 0	LSI Logic SAS	
Network adapter 1	VM-RegionA01-vDS-COMP	☑ Connect...
CD/DVD drive 1	Client Device	□ Connect...
Video card	Specify custom settings	
VMCI device		
SATA controller 0	AHCI	
Other	Additional Hardware	

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

Summary tab

[547]



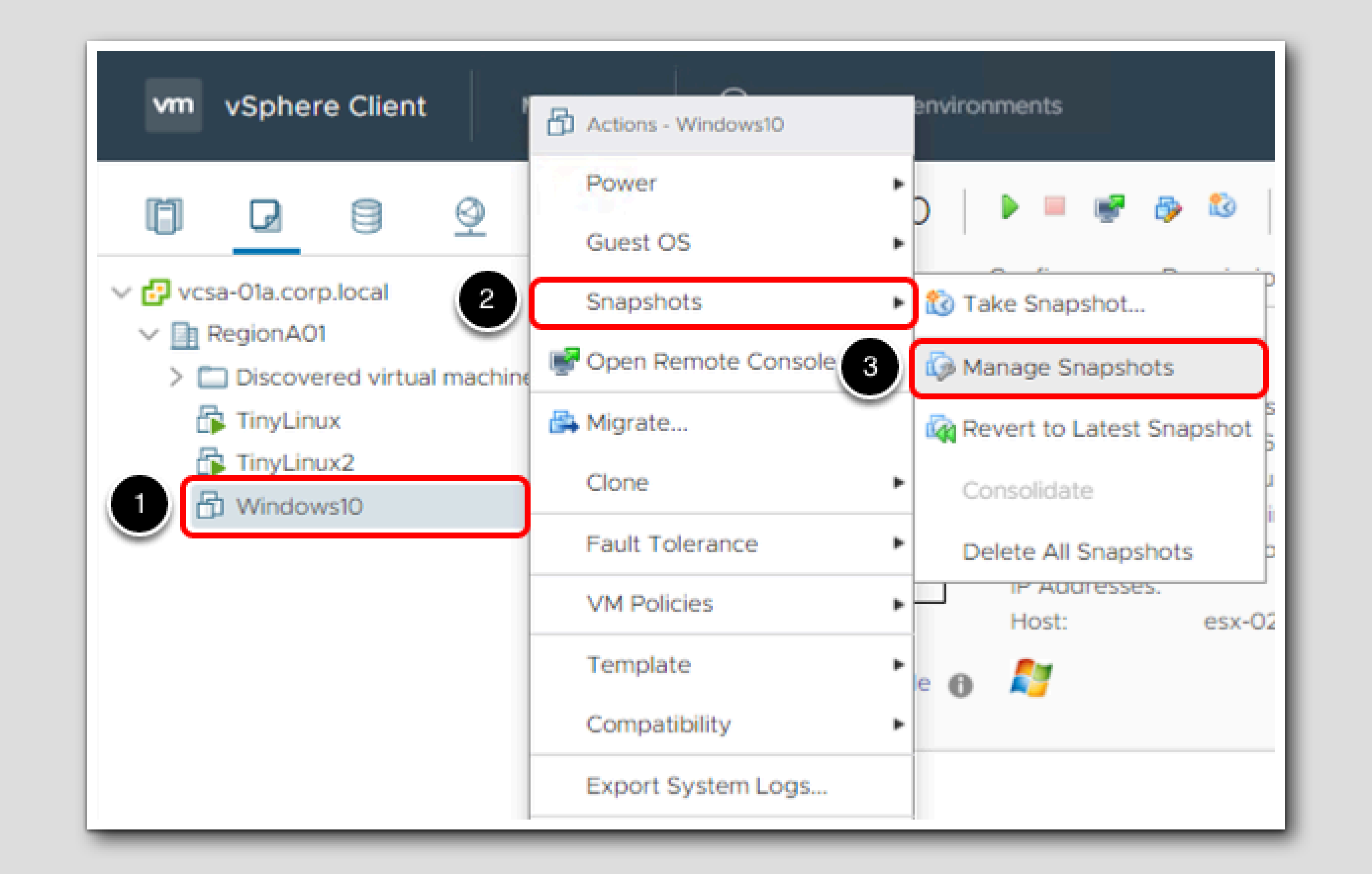
Guest OS: Microsoft Windows
Compatibility: ESXi 6.5 and later (
VMware Tools: Not running, versio
More info
DNS Name: Windows10.corp.lo
IP Addresses:
Host: esx-02a.corp.local

CPU	1 CPU(s)
Memory	4 GB, 0 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB

1. Make sure you are on the **Summary** tab for **Windows10**.
2. Verify the memory has been updated.

Revert Virtual Machine settings using the Snapshot Manager

[548]

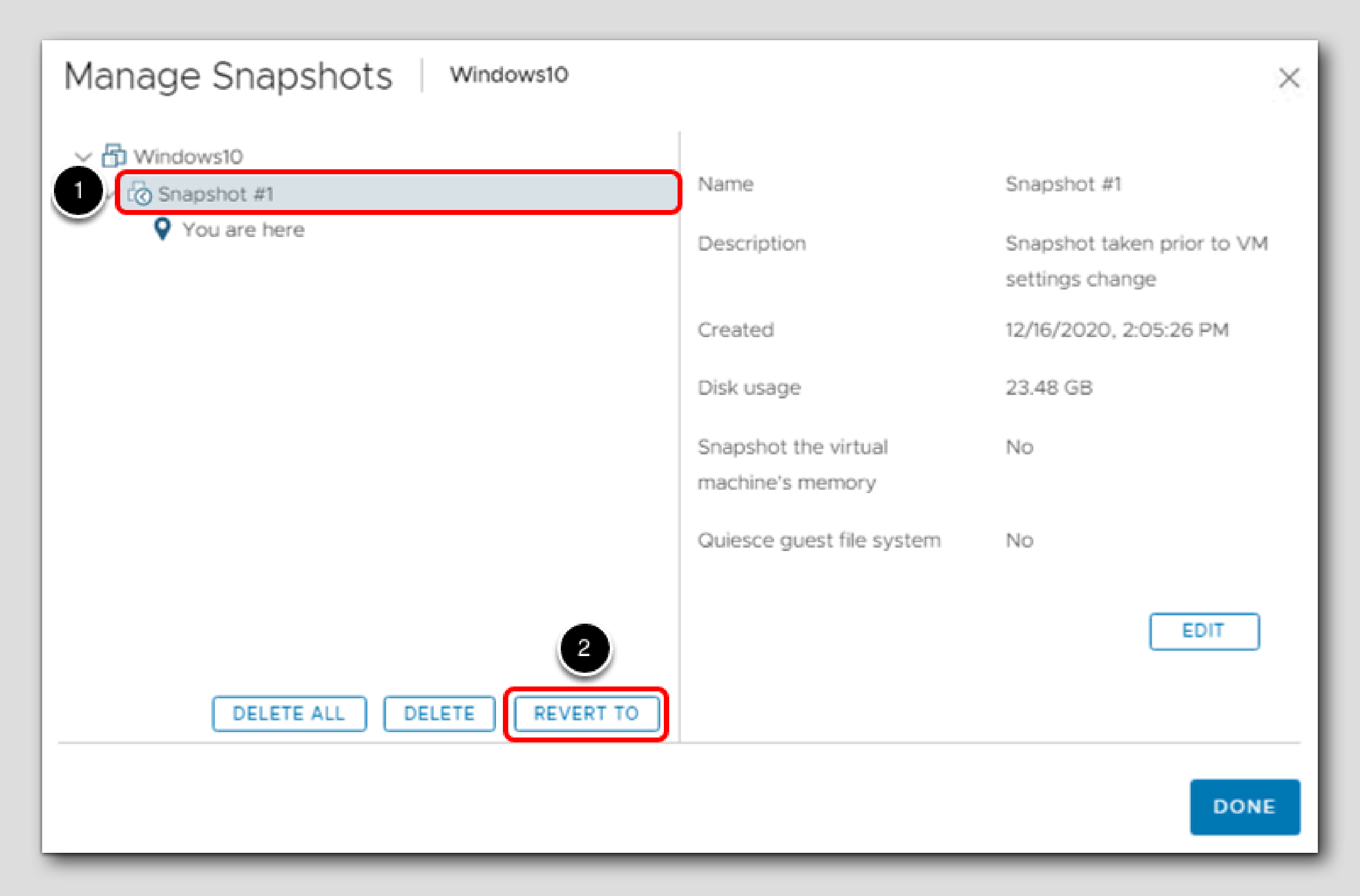


In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Select the VM Snapshot to Revert to

[549]

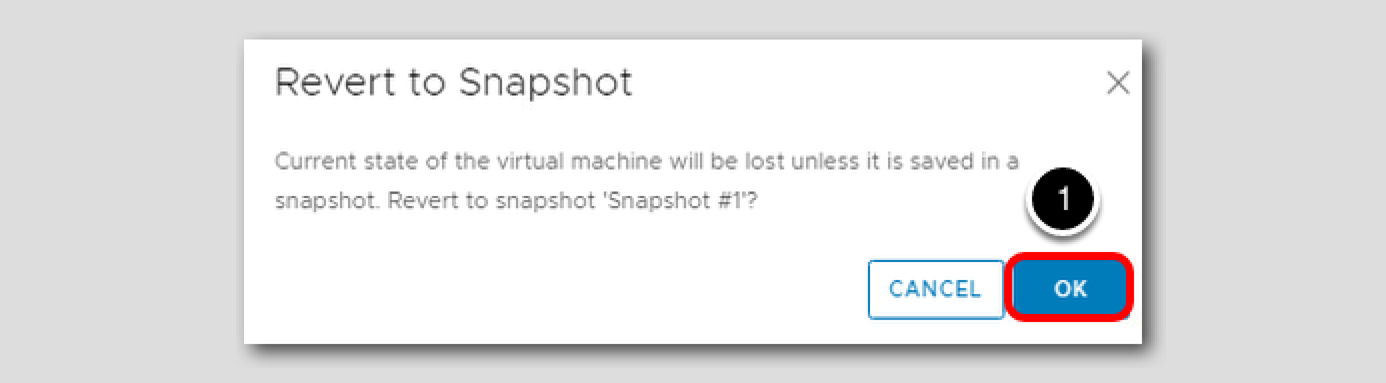


Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	12/16/2020, 2:05:26 PM
Disk usage	23.48 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

1. Make sure **Snapshot #1** is selected.
2. Click the **Revert To** button.

Confirm Revert to Snapshot

[550]



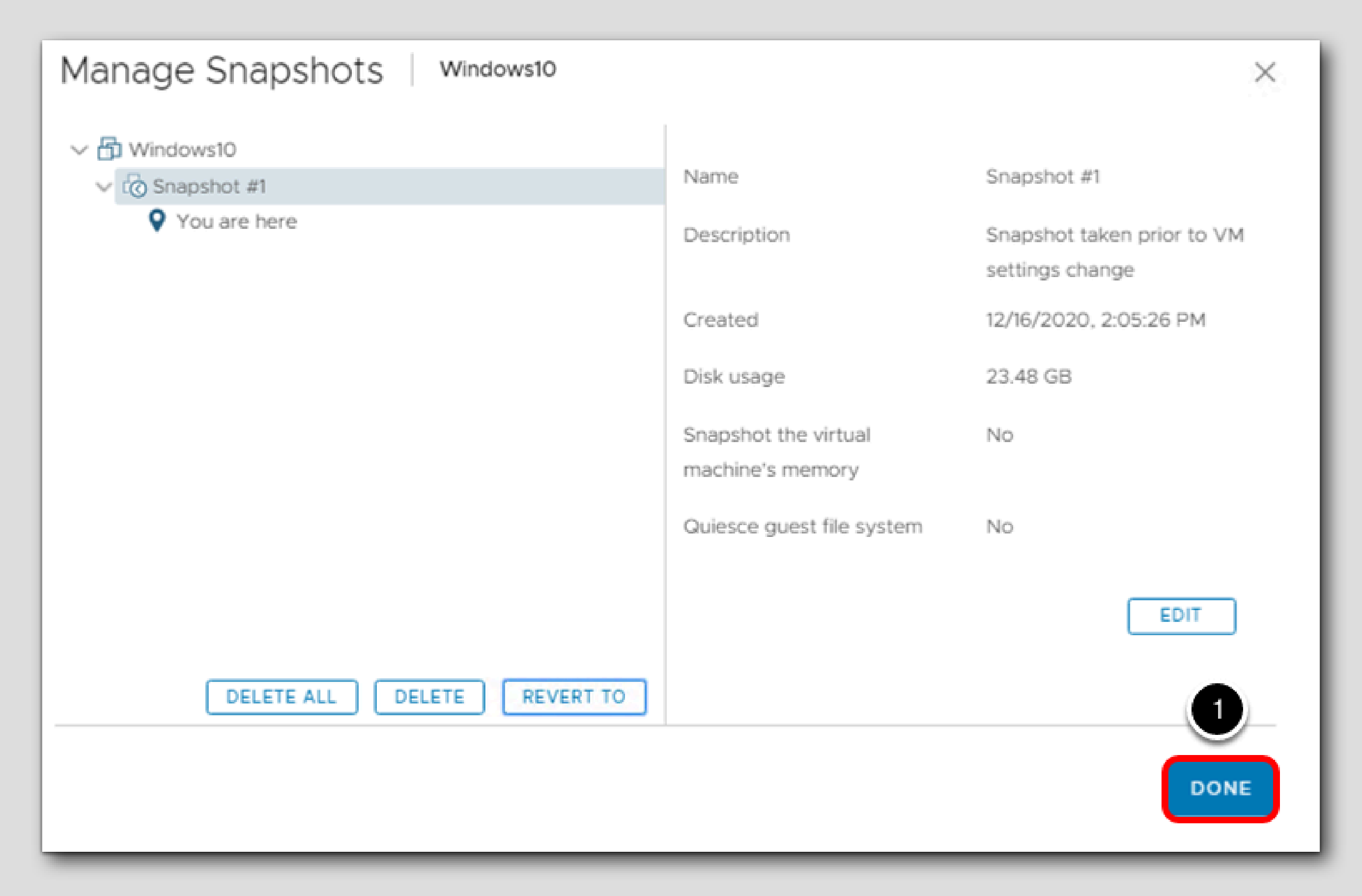
Revert to Snapshot

Current state of the virtual machine will be lost unless it is saved in a snapshot. Revert to snapshot 'Snapshot #1'?

1. Click OK to confirm action.

Close Snapshot Window

[551]

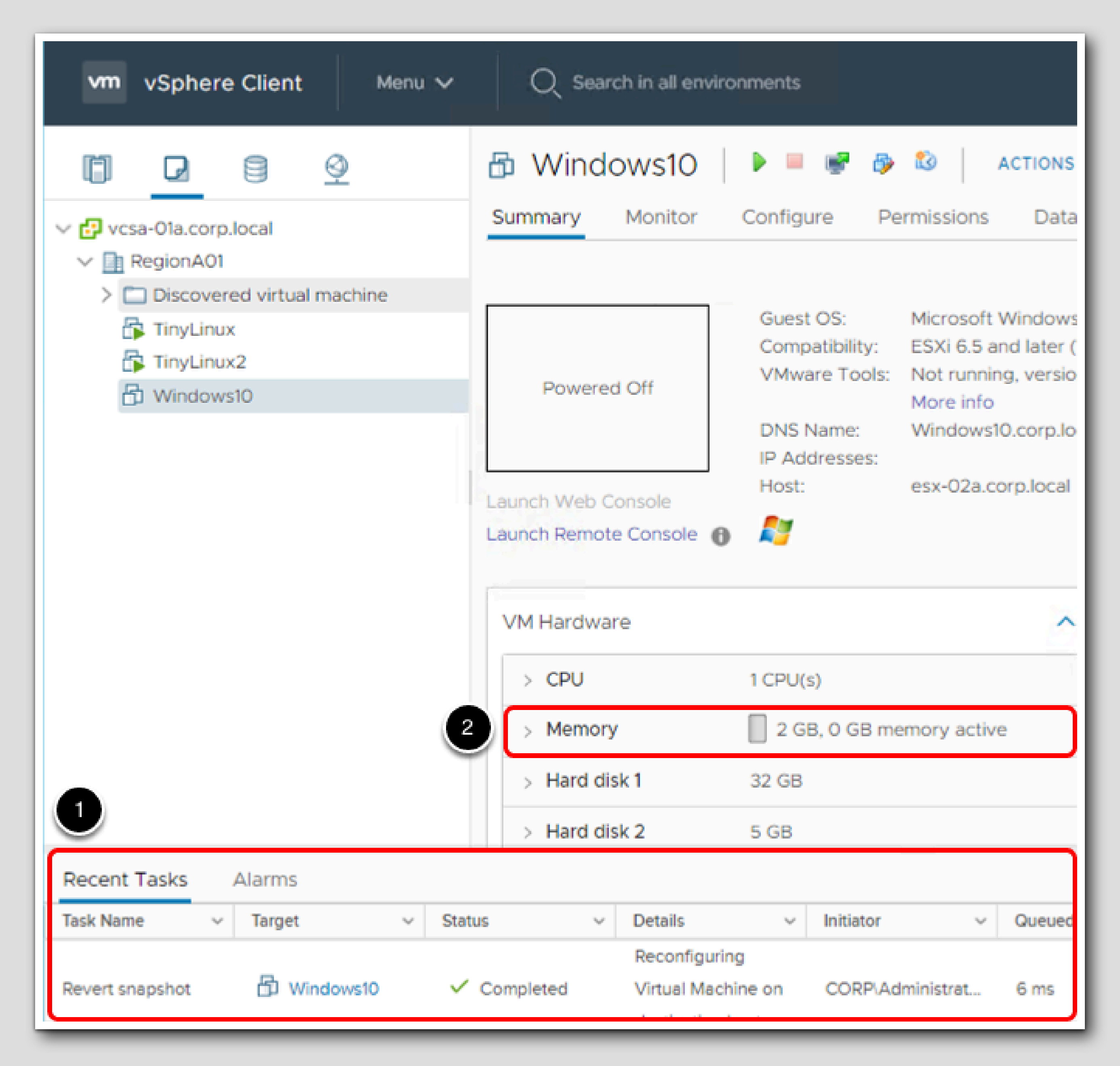


Manage Snapshots | Windows10

Name	Snapshot #1
Description	Snapshot taken prior to VM settings change
Created	12/16/2020, 2:05:26 PM
Disk usage	23.48 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

1. Click Done to close the Snapshot window.

Monitor task progress [552]



Guest OS: Microsoft Windows
Compatibility: ESXi 6.5 and later (
VMware Tools: Not running, versio
More info
DNS Name: Windows10.corp.lo
IP Addresses:
Host: esx-02a.corp.local

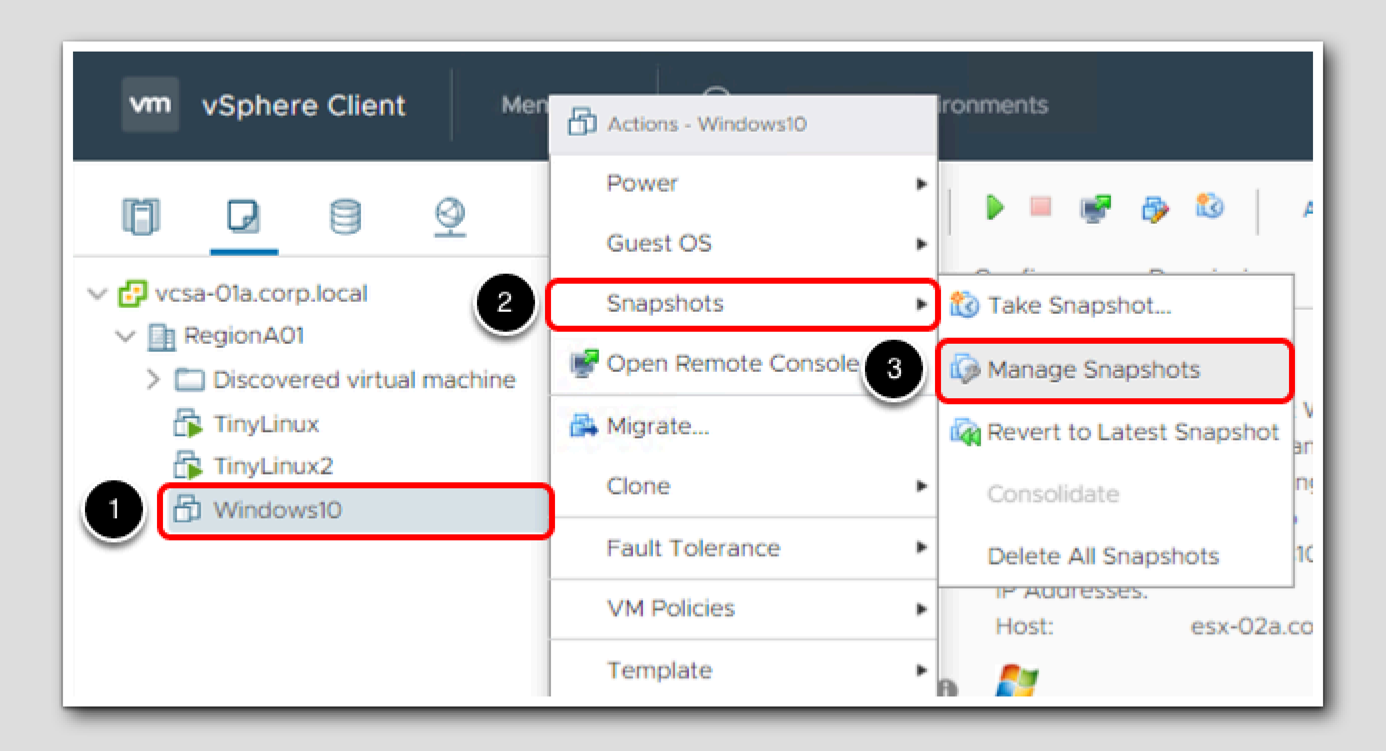
CPU	1 CPU(s)
Memory	2 GB, 0 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB

Task Name	Target	Status	Details	Initiator	Queued
Revert snapshot	Windows10	✓ Completed	Reconfiguring Virtual Machine on	CORP\Administrat...	6 ms

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

Delete Snapshot #1

[553]

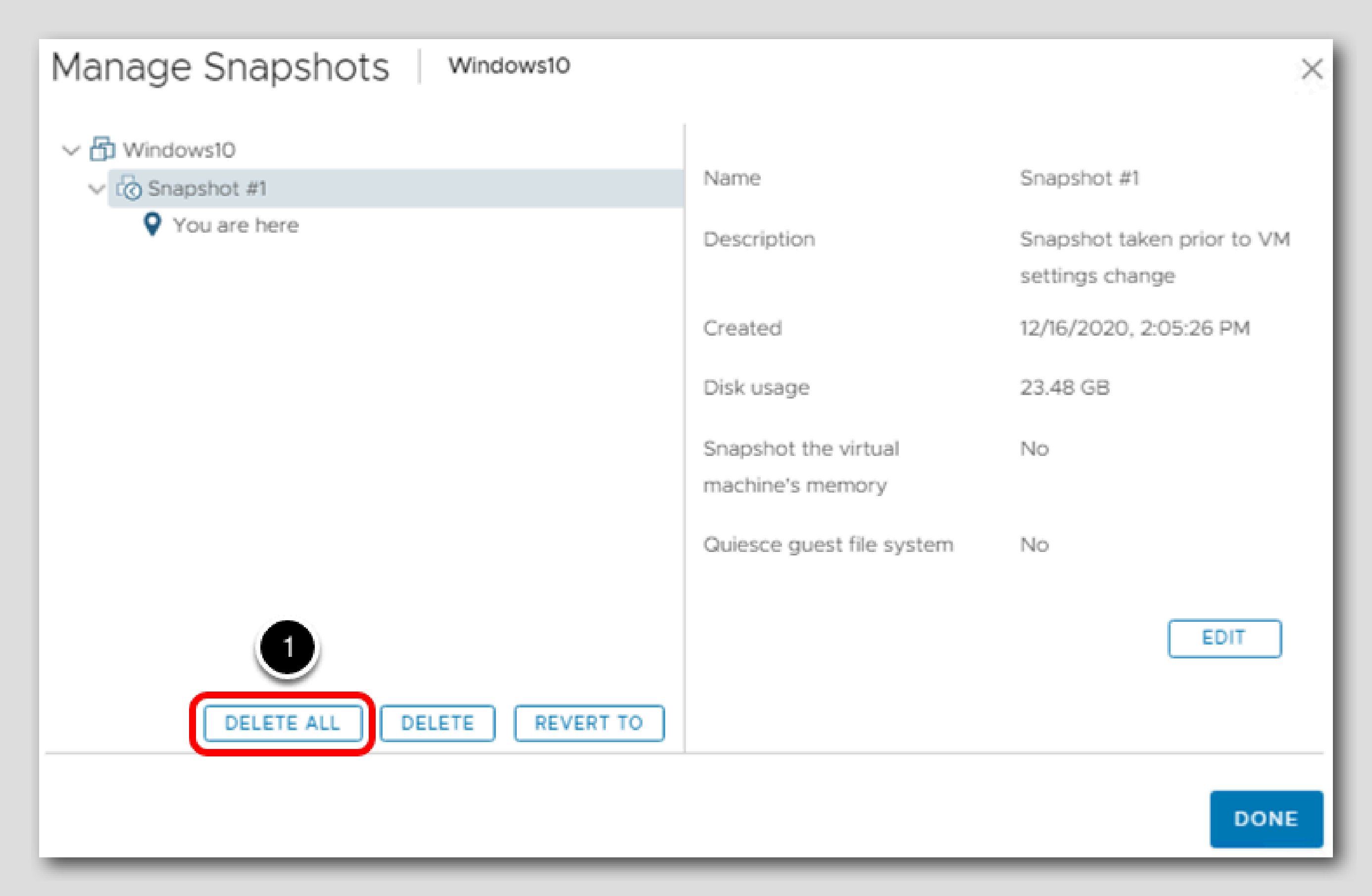


Here you can go and delete the taken snapshot.

1. Right-click Windows10.
2. Select Snapshots.
3. Click Manage Snapshots.

Select the VM Snapshot to Delete All

[554]



Manage Snapshots | Windows10

Name: Snapshot #1

Description: Snapshot taken prior to VM settings change

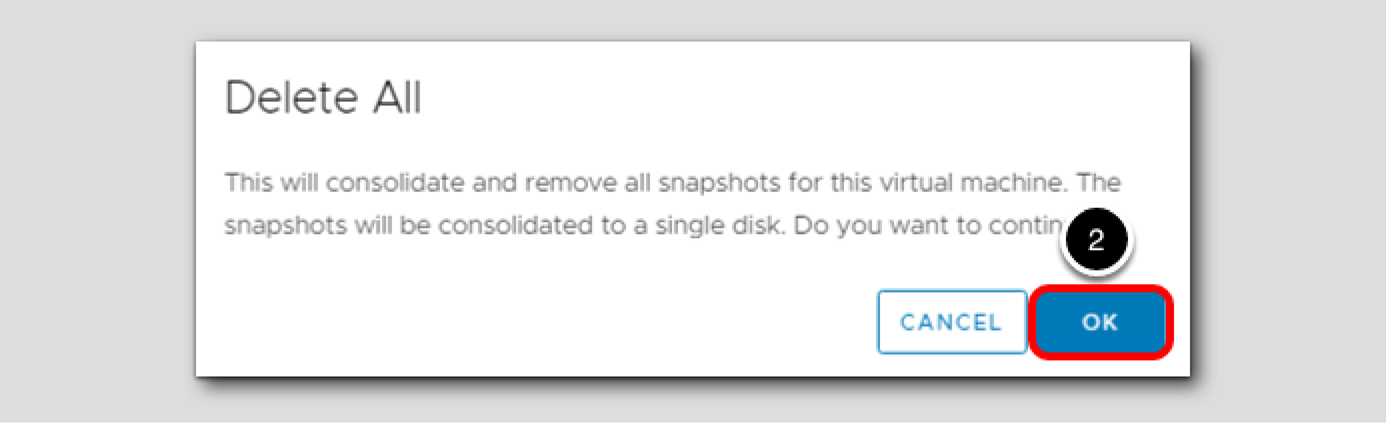
Created: 12/16/2020, 2:05:26 PM

Disk usage: 23.48 GB

Snapshot the virtual machine's memory: No

Quiesce guest file system: No

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



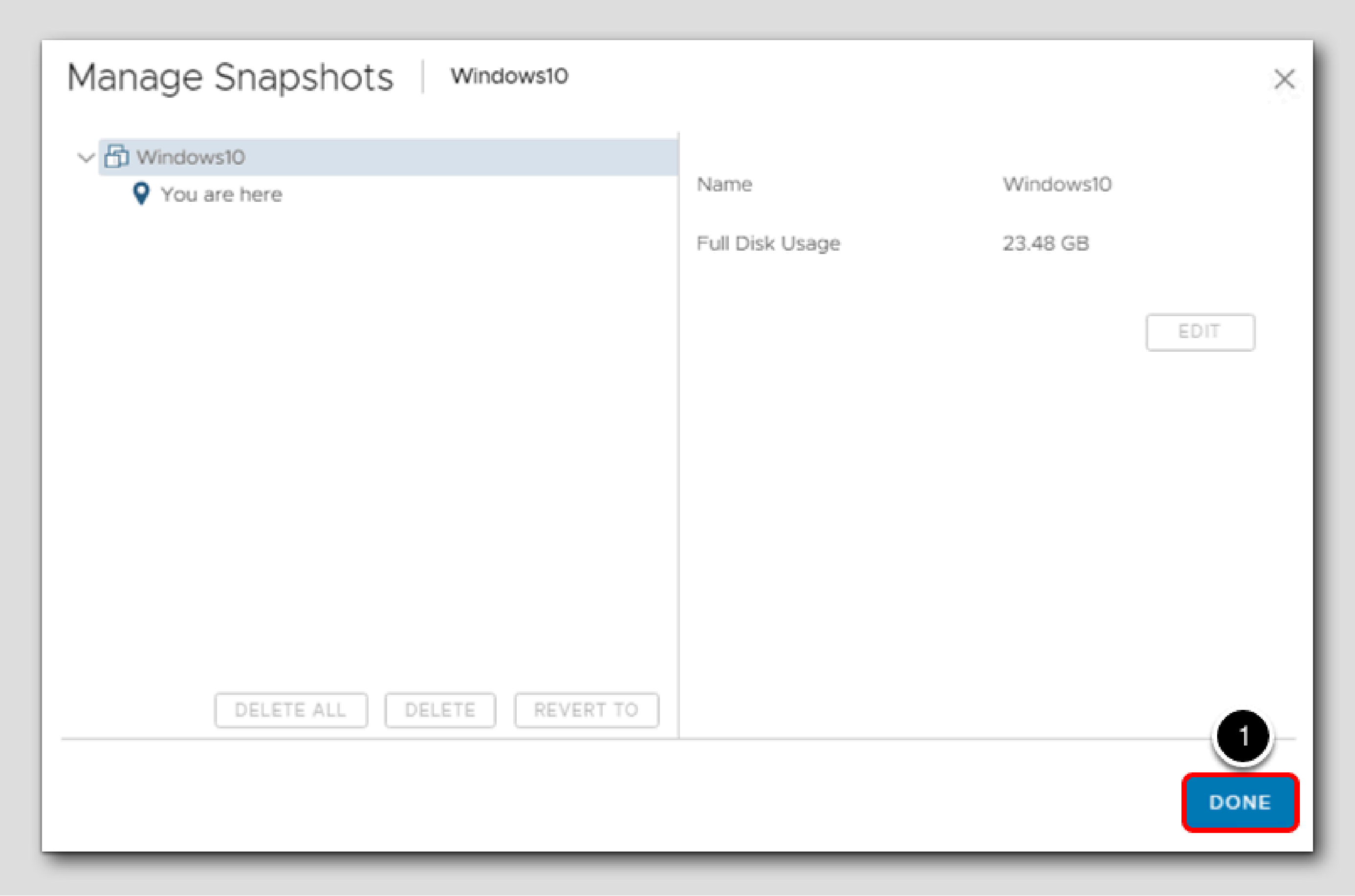
Delete All

This will consolidate and remove all snapshots for this virtual machine. The snapshots will be consolidated to a single disk. Do you want to contin

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

Close Snapshot Window

[555]



Manage Snapshots | Windows10

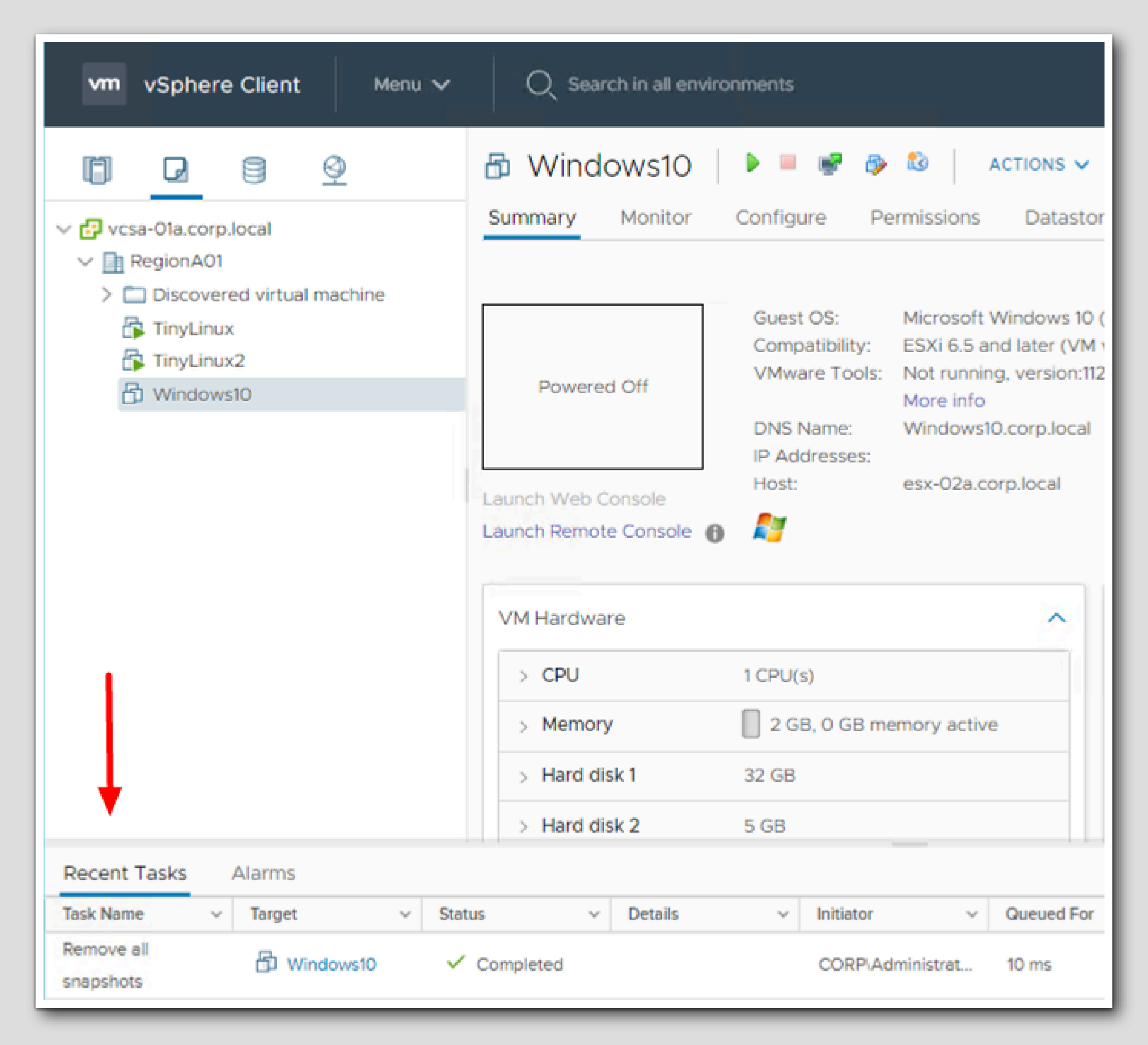
Name	Windows10
Full Disk Usage	23.48 GB

1. Click **Done** to exit the manage snapshots window.

It is a best practice to delete virtual machine snapshots when they are no longer needed. Over time the snapshot delta can grow to be quite large which could result in issues consolidating the virtual machine files and lead to performance issues.

Snapshot Removed

[556]



Guest OS: Microsoft Windows 10 (
Compatibility: ESXi 6.5 and later (VM
VMware Tools: Not running, version:112
More info
DNS Name: Windows10.corp.local
IP Addresses:
Host: esx-02a.corp.local

CPU	1 CPU(s)
Memory	2 GB, 0 GB memory active
Hard disk 1	32 GB
Hard disk 2	5 GB

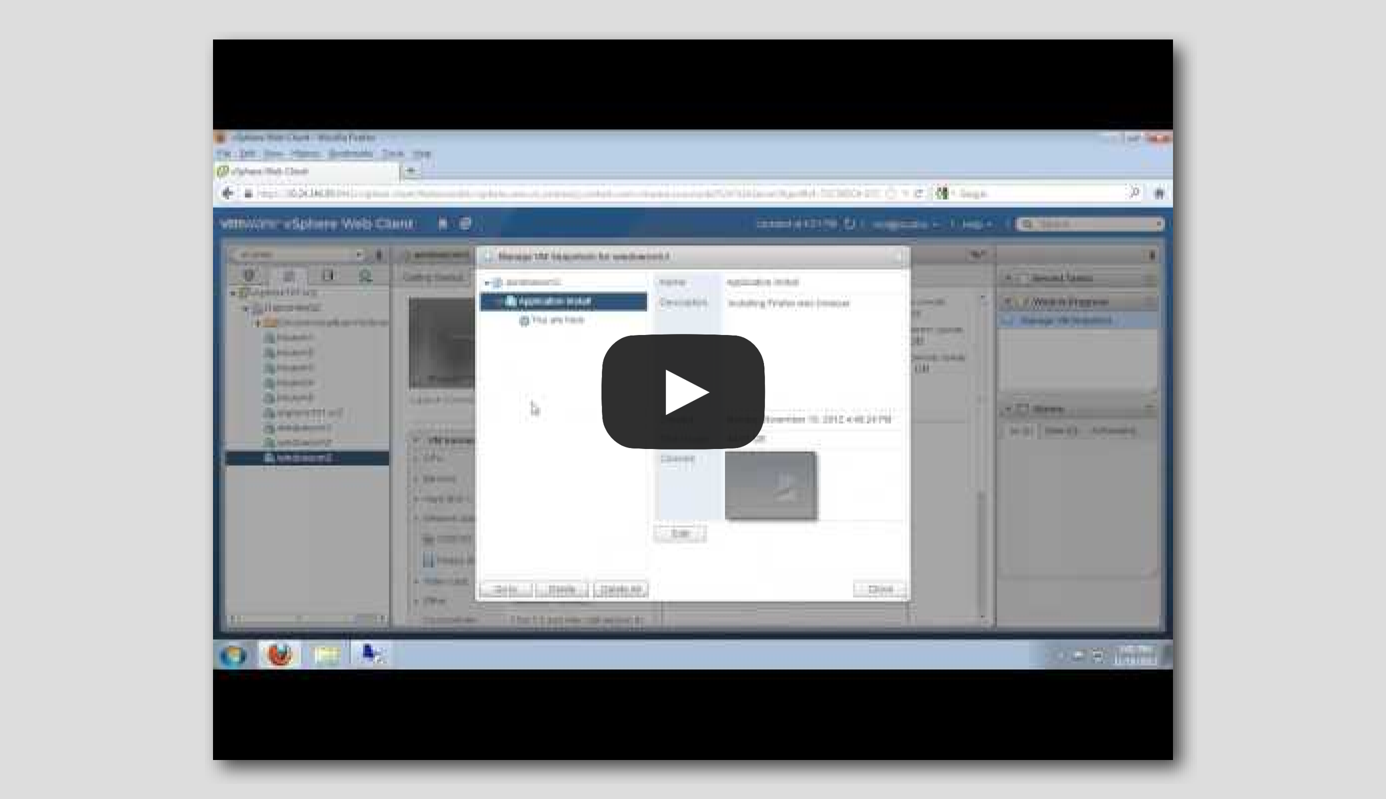
Task Name	Target	Status	Details	Initiator	Queued For
Remove all snapshots	Windows10	✓ Completed		CORP\Administrat...	10 ms

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

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

[557]

https://www.youtube.com/watch?v=7AVIWifTEMM



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

vSphere Datastore Cluster

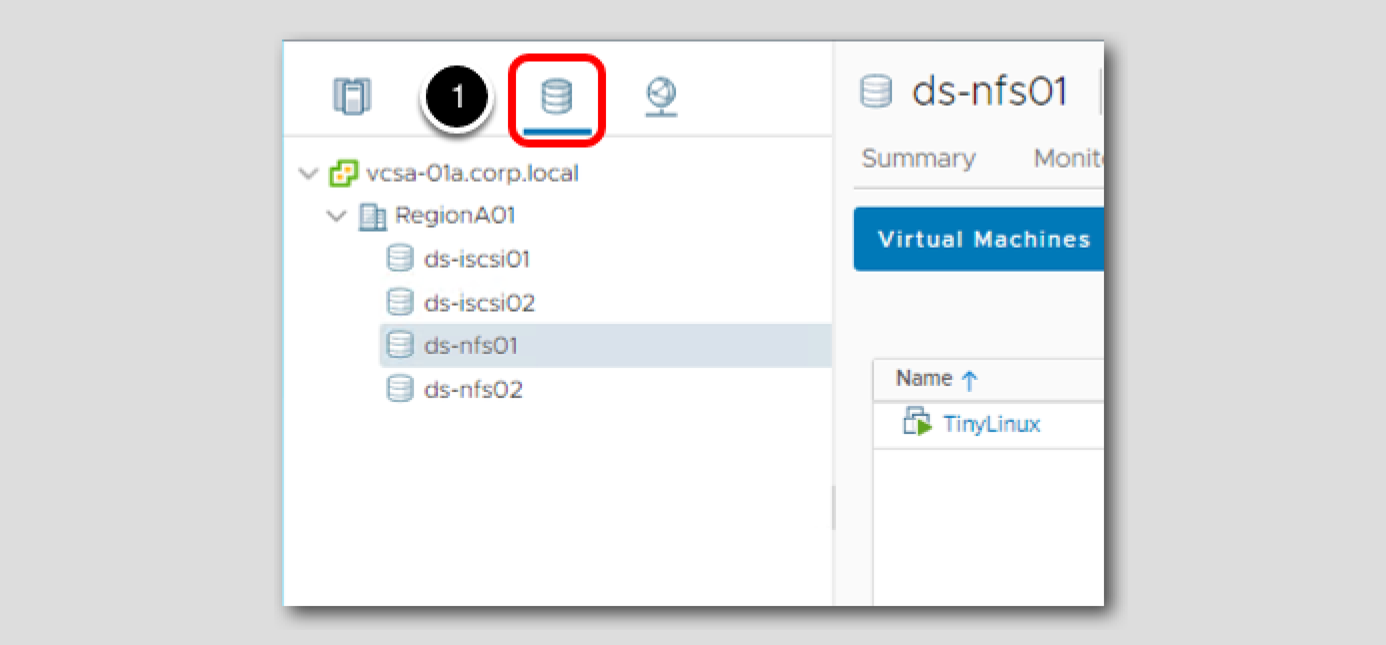
[558]

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

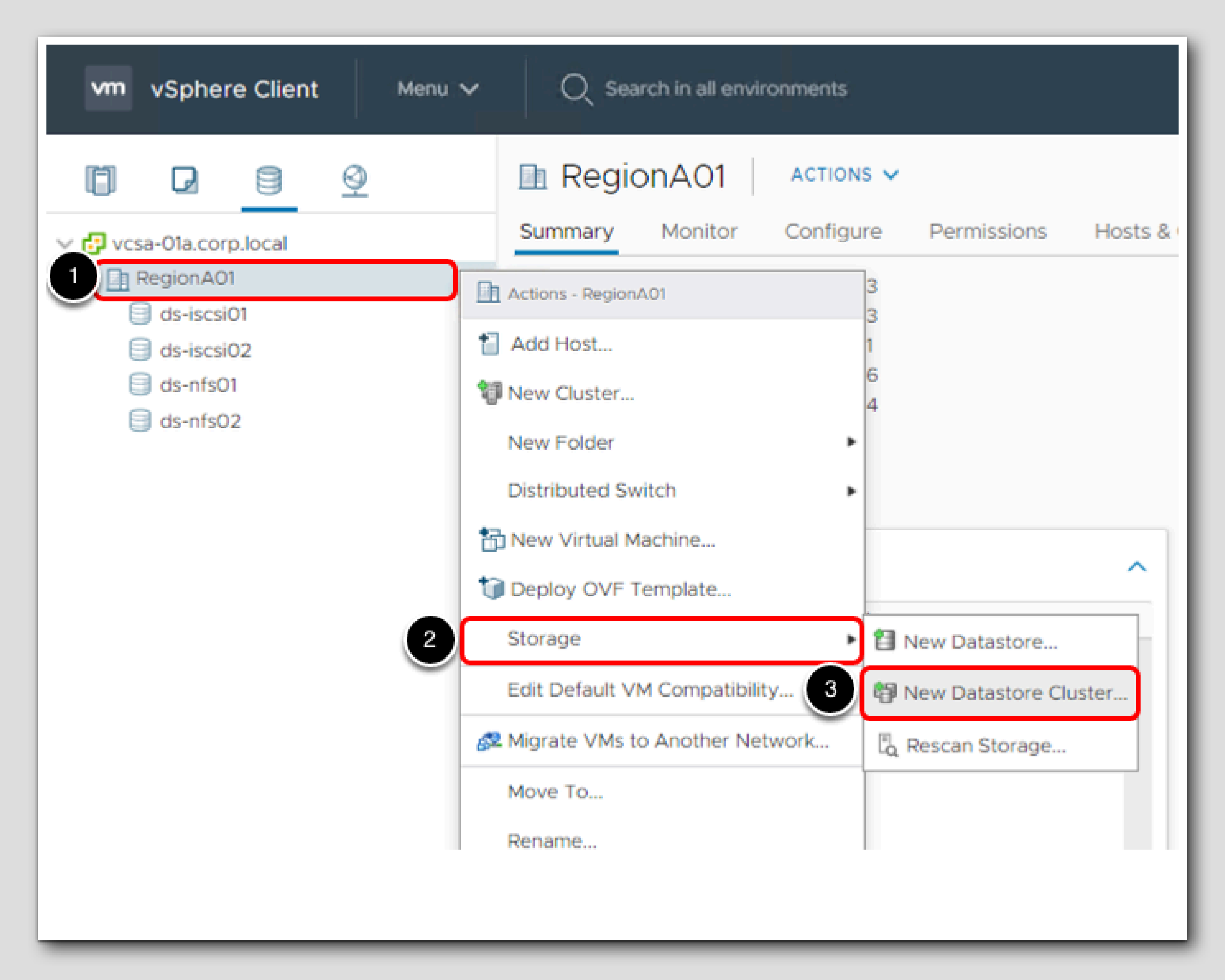
[559]



1. Click on the **Storage** icon

New Datastore Cluster

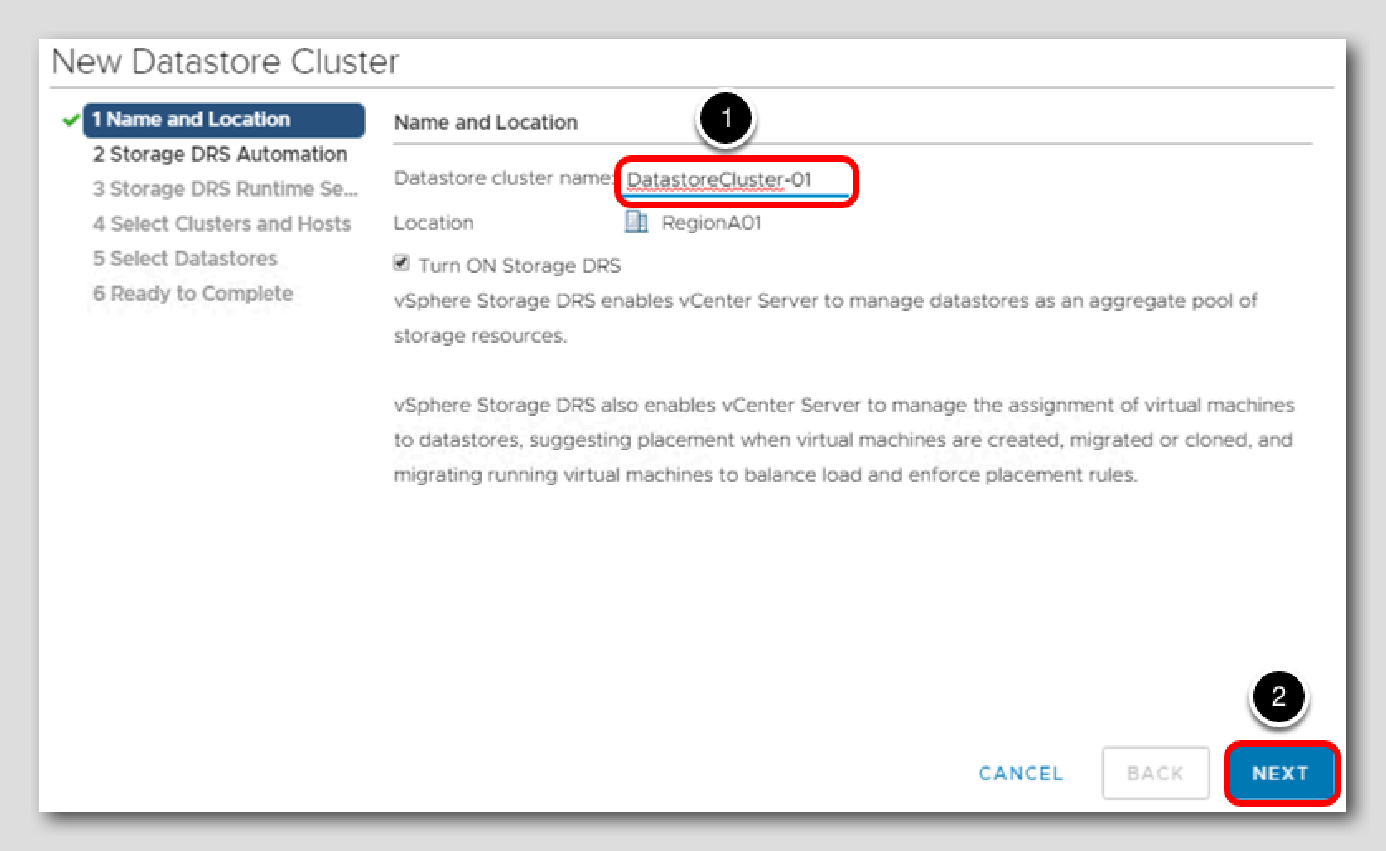
[560]



1. Right Click on RegionA01
2. Select Storage
3. Click New Datastore Cluster...

New Datastore Cluster - Name and Location

[561]



New Datastore Cluster

Name and Location

Datastore cluster name: DatastoreCluster-01

Location: RegionA01

☑ Turn ON Storage DRS

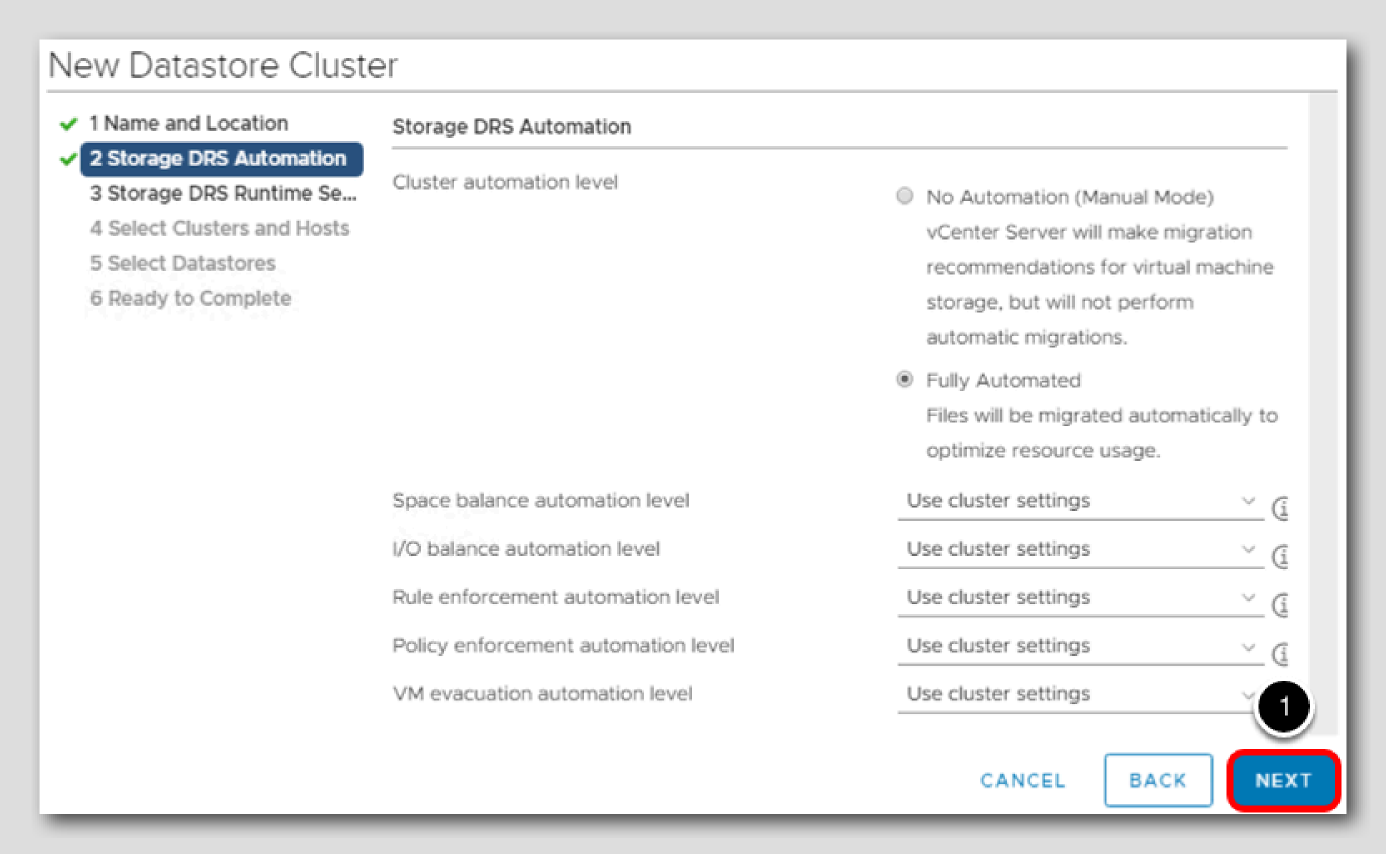
vSphere Storage DRS enables vCenter Server to manage datastores as an aggregate pool of storage resources.

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.

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

New Datastore Cluster - Storage DRS Automation

[562]



New Datastore Cluster

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

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.

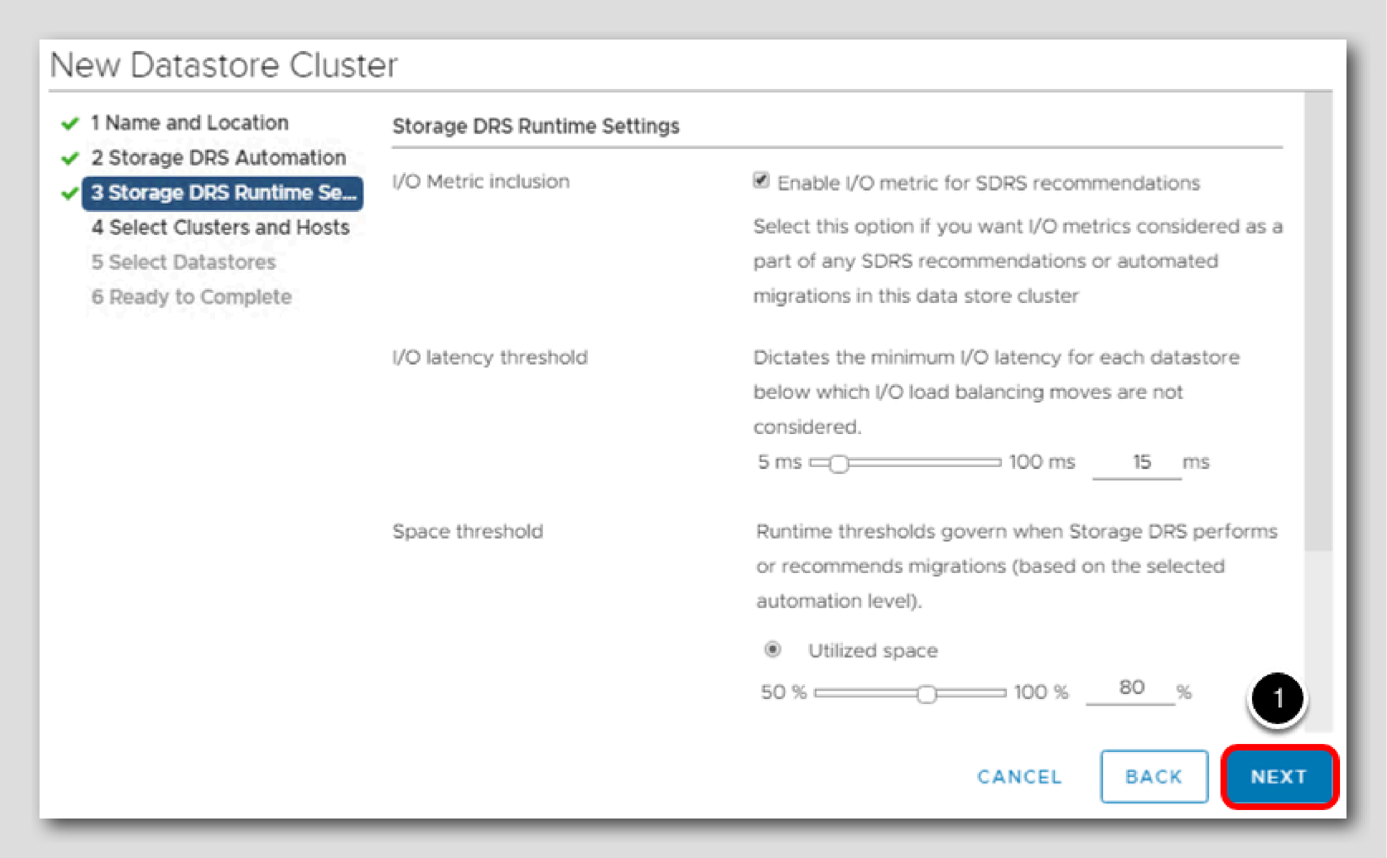
● Fully Automated
Files will be migrated automatically to optimize resource usage.

Space balance automation level	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

1. Leave the defaults settings and select Next

New Datastore Cluster - Storage DRS Runtime Settings

[563]



New Datastore Cluster

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

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).

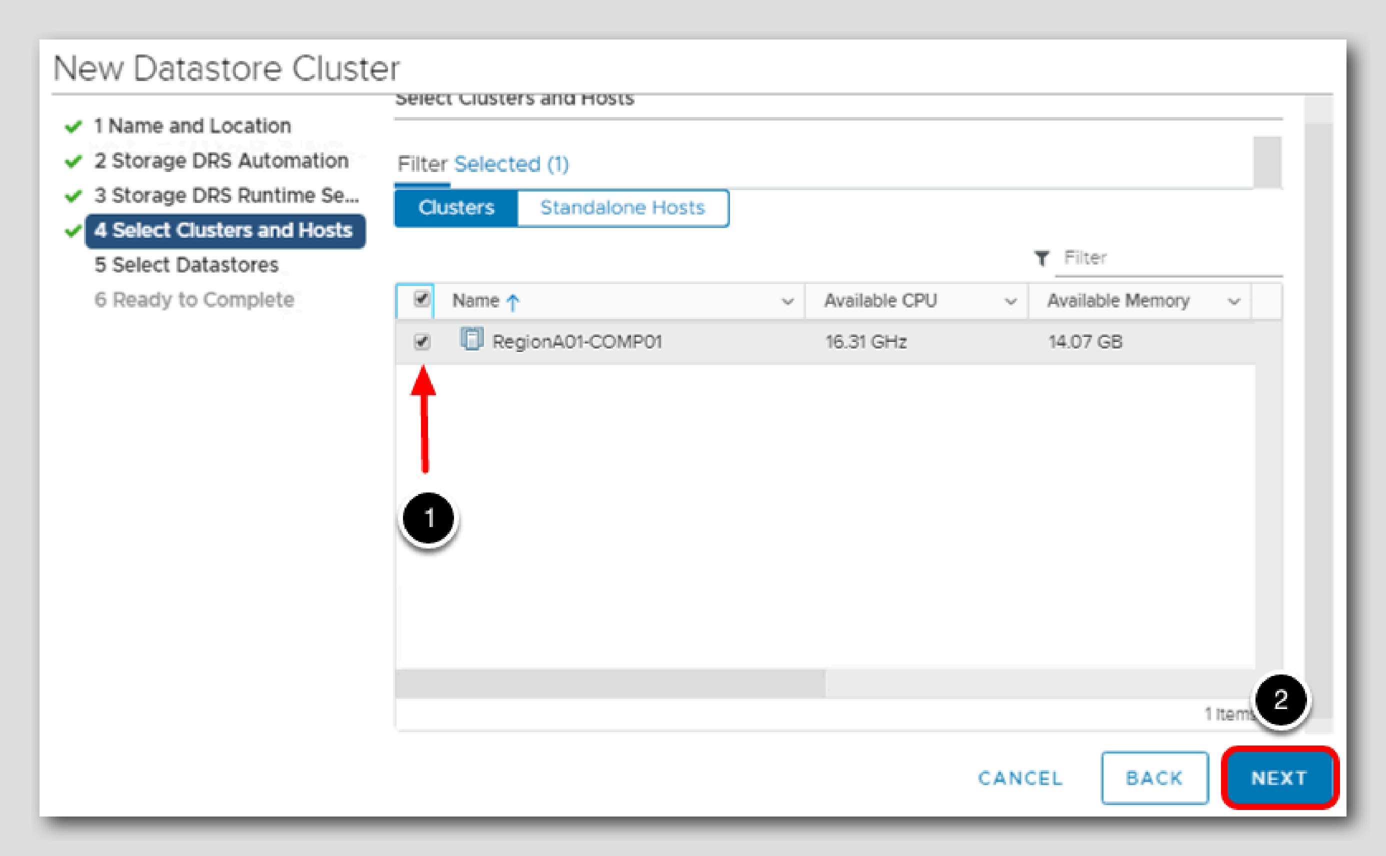
● Utilized space

50 % — 100 % 80 %

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

Select Clusters and Hosts

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

Filter Selected (1)

Clusters | Standalone Hosts

Filter

☑	Name ↑	Available CPU	Available Memory
☑	RegionA01-COMP01	16.31 GHz	14.07 GB

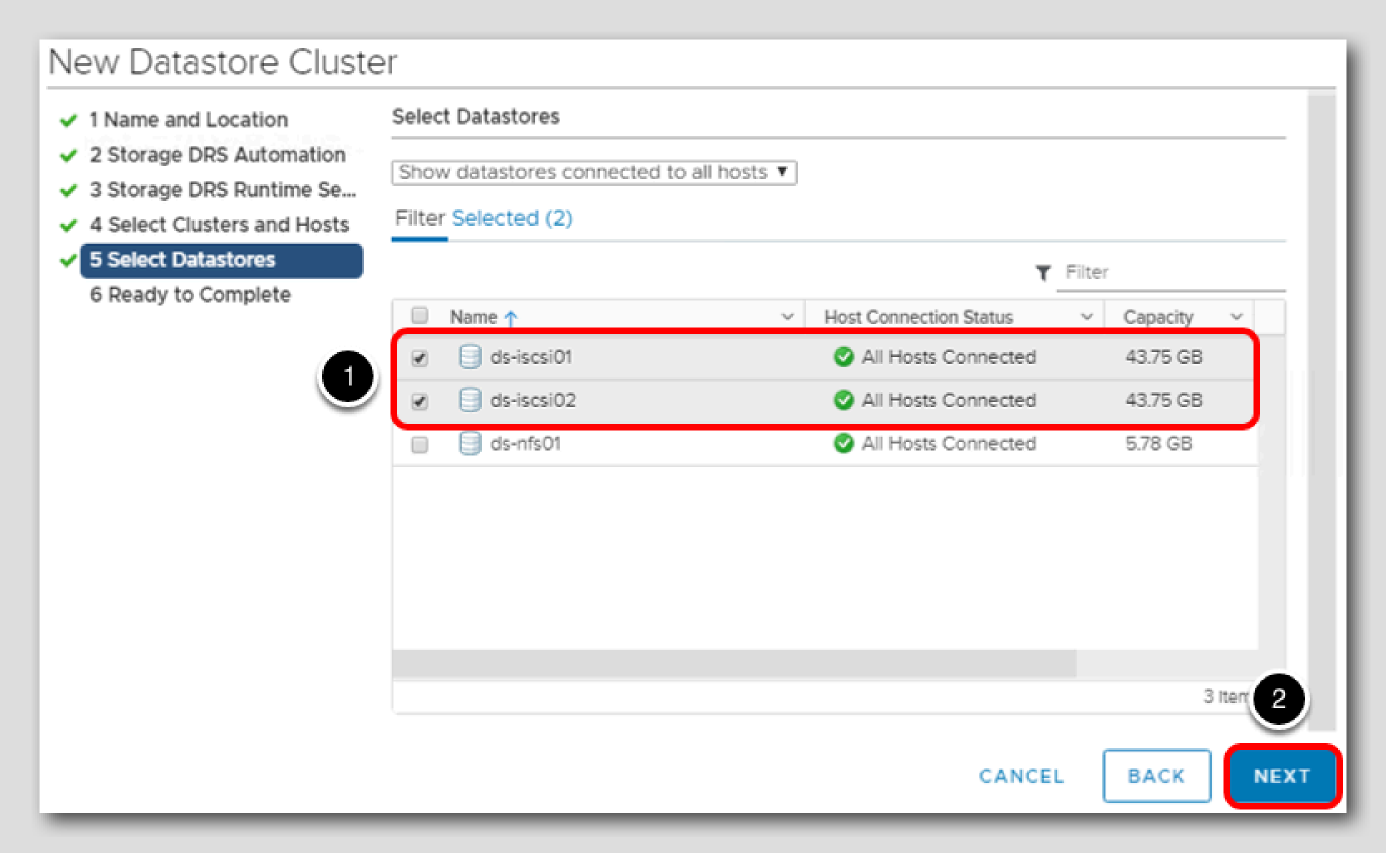
1 items

1. Because there are no standalone hosts, please select RegionA01-COMP01

2. Click the Next button

New Datastore Cluster - Select Datastores

[565]



New Datastore Cluster

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

Select Datastores

Show datastores connected to all hosts ▾

Filter Selected (2)

Filter

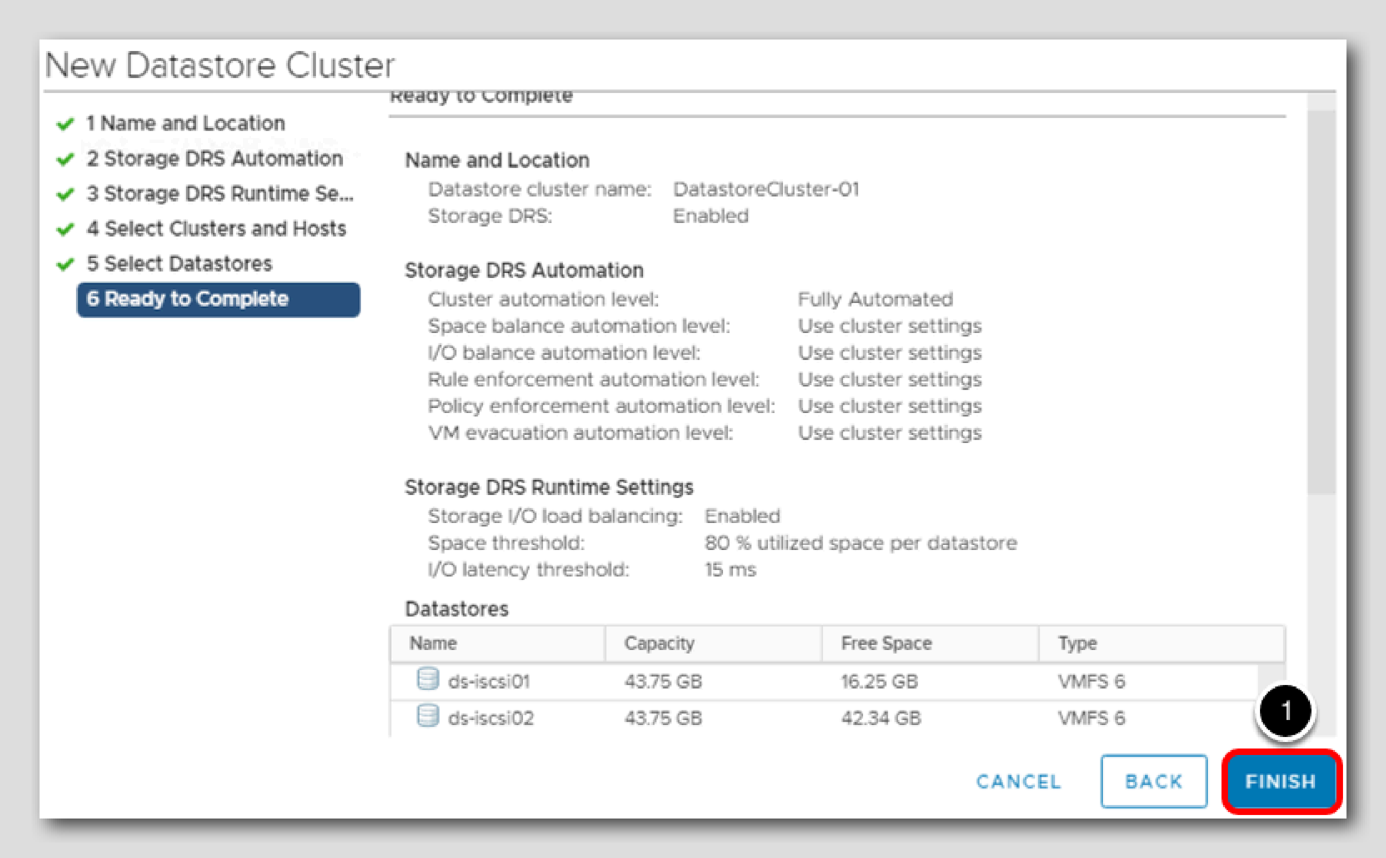
□	Name ↑	Host Connection Status	Capacity
☑	ds-iscsi01	✓ All Hosts Connected	43.75 GB
☑	ds-iscsi02	✓ All Hosts Connected	43.75 GB
□	ds-nfs01	✓ All Hosts Connected	5.78 GB

3 Item

1. Select the ds-iscsi01 and ds-iscsi02 datastores for the new Datastore Cluster
2. Click Next

New Datastore Cluster- Ready to Complete

[566]



Name and Location

Datastore cluster name: DatastoreCluster-01
Storage DRS: Enabled

Storage DRS Automation

Cluster automation level: Fully Automated
Space balance automation level: Use cluster settings
I/O balance automation level: Use cluster settings
Rule enforcement automation level: Use cluster settings
Policy enforcement automation level: Use cluster settings
VM evacuation automation level: Use cluster settings

Storage DRS Runtime Settings

Storage I/O load balancing: Enabled
Space threshold: 80 % utilized space per datastore
I/O latency threshold: 15 ms

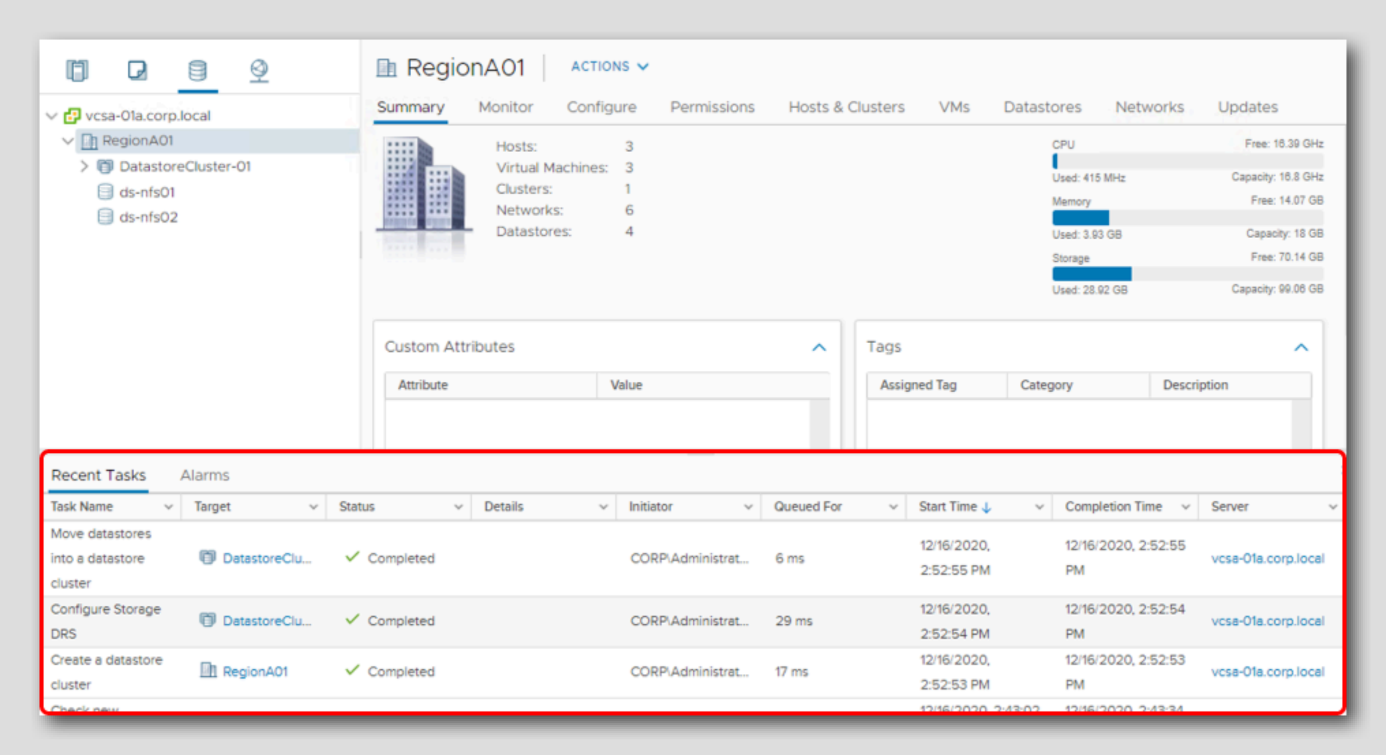
Datastores

Name	Capacity	Free Space	Type
ds-iscsi01	43.75 GB	16.25 GB	VMFS 6
ds-iscsi02	43.75 GB	42.34 GB	VMFS 6

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

New Datastore Cluster- Summary

[567]



Hosts: 3
Virtual Machines: 3
Clusters: 1
Networks: 6
Datastores: 4

CPU — Free: 16.39 GHz — Used: 415 MHz — Capacity: 16.8 GHz
Memory — Free: 14.07 GB — Used: 3.93 GB — Capacity: 18 GB
Storage — Free: 70.14 GB — Used: 28.92 GB — Capacity: 99.06 GB

Task Name	Target	Status	Details	Initiator	Queued For	Start Time ↓	Completion Time	Server
Move datastores into a datastore cluster	DatastoreClu...	✓ Completed		CORP\Administrat...	6 ms	12/16/2020, 2:52:55 PM	12/16/2020, 2:52:55 PM	vcsa-01a.corp.local
Configure Storage DRS	DatastoreClu...	✓ Completed		CORP\Administrat...	29 ms	12/16/2020, 2:52:54 PM	12/16/2020, 2:52:54 PM	vcsa-01a.corp.local
Create a datastore cluster	RegionA01	✓ Completed		CORP\Administrat...	17 ms	12/16/2020, 2:52:53 PM	12/16/2020, 2:52:53 PM	vcsa-01a.corp.local
Check new...						12/16/2020, 2:43:02	12/16/2020, 2:43:34	

View the **Recent Tasks** to check the progress of the operation.

Conclusion

[568]

Leveraging vSphere Datastore Clusters in your vSphere environment can help to ensure datastores are filled evenly and I/O is spread out across the group of datastores in the cluster. Storage DRS can automate the initial placement of new virtual machines and adjust virtual machine placement to maintain an even distribution of I/O across the datastore cluster.

Certification Path

[569]

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

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

Learn More Here: *https://www.vmware.com/learning/certification/vcap-dcv-deploy.html*

vmware®
CERTIFIED
ADVANCED PROFESSIONAL
Data Center Virtualization Deploy 2021

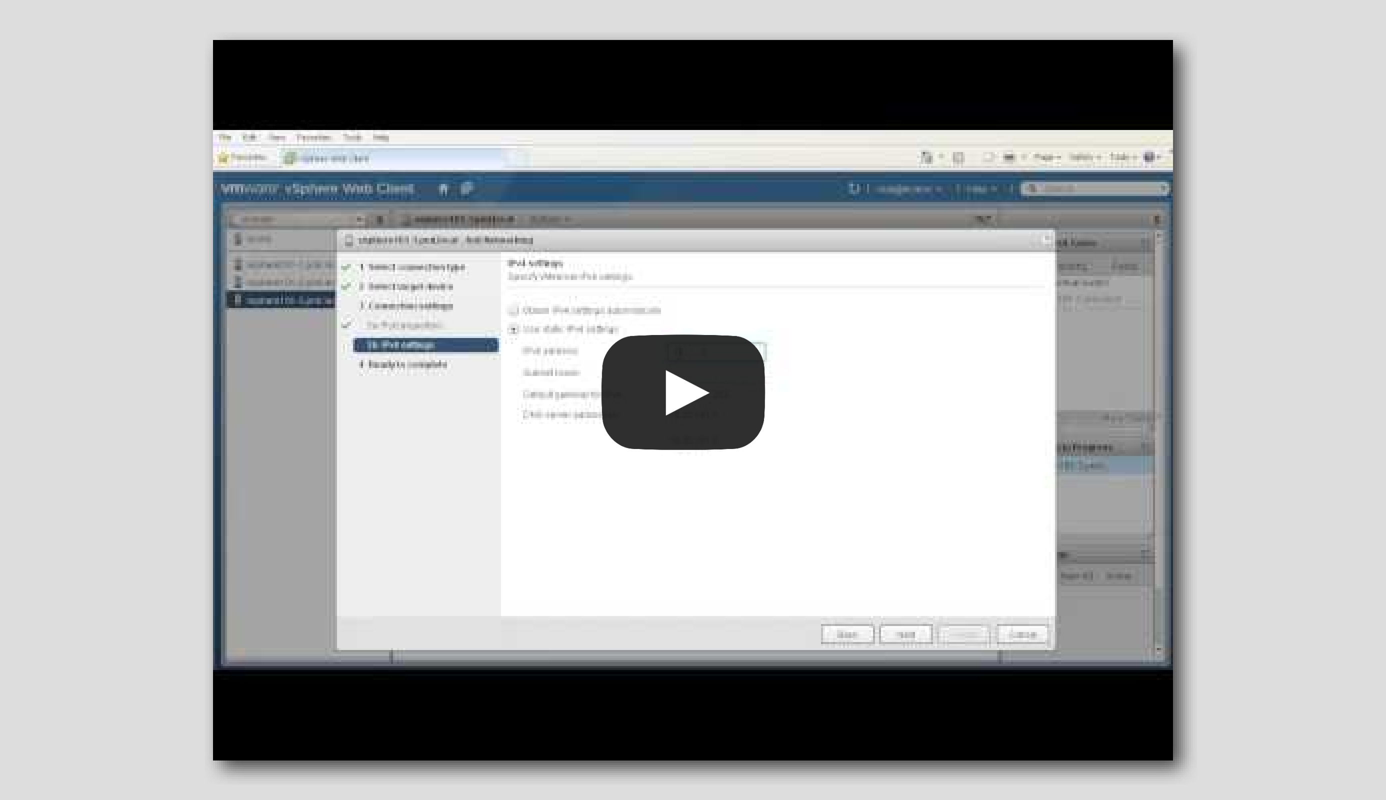
Conclusion

For More Information.... [571]

This section provides supplementary documentation and videos.

Video: How to Configure a vSphere Standard Switch (VSS) (4:22) [572]

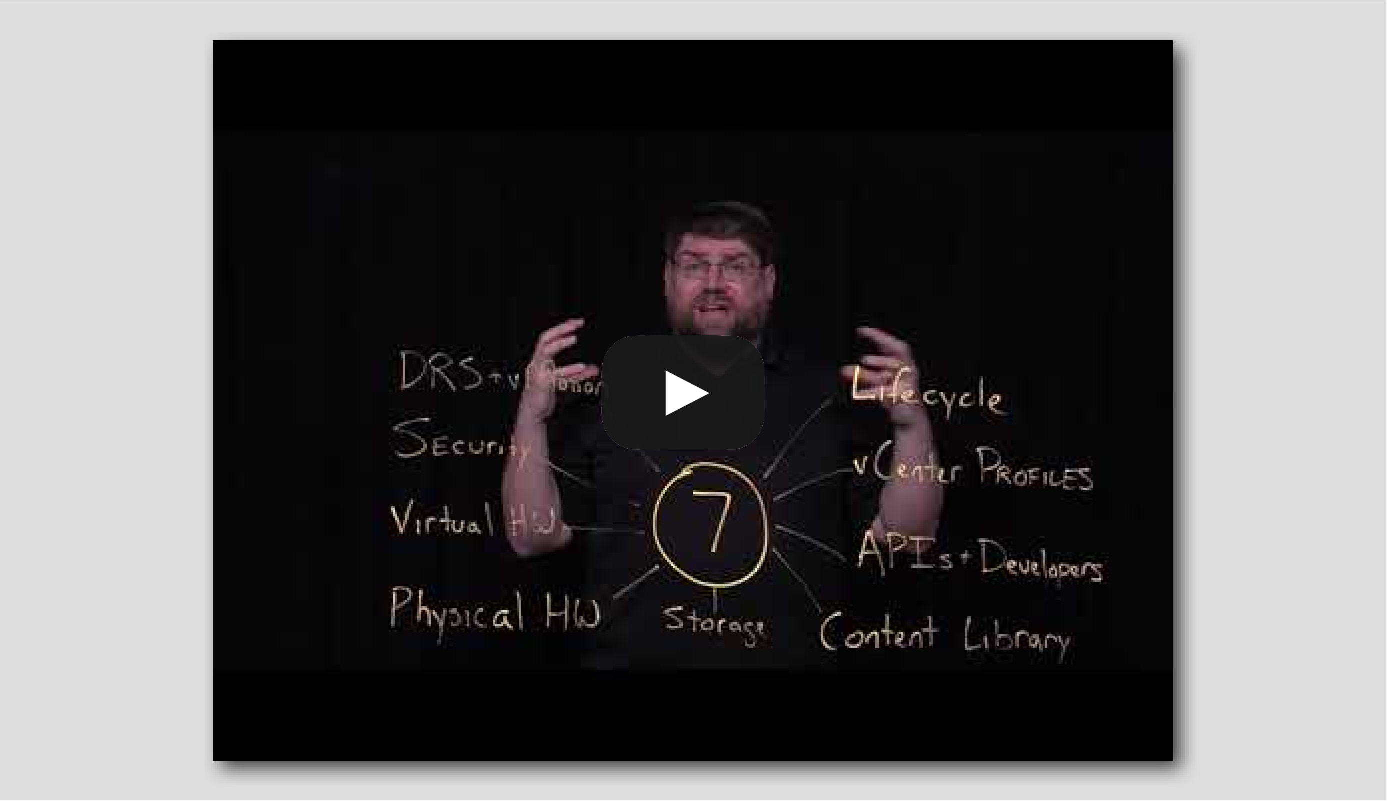
https://www.youtube.com/watch?v=XpXuhK0c-f4



This video shows how to use the VMware vSphere web client to configure basic networking for your vSphere hosts using the vSphere Standard Switch (VSS).

vSphere 7 - vCenter Server High Availability [573]

https://www.youtube.com/watch?v=XkP6QCutw9k

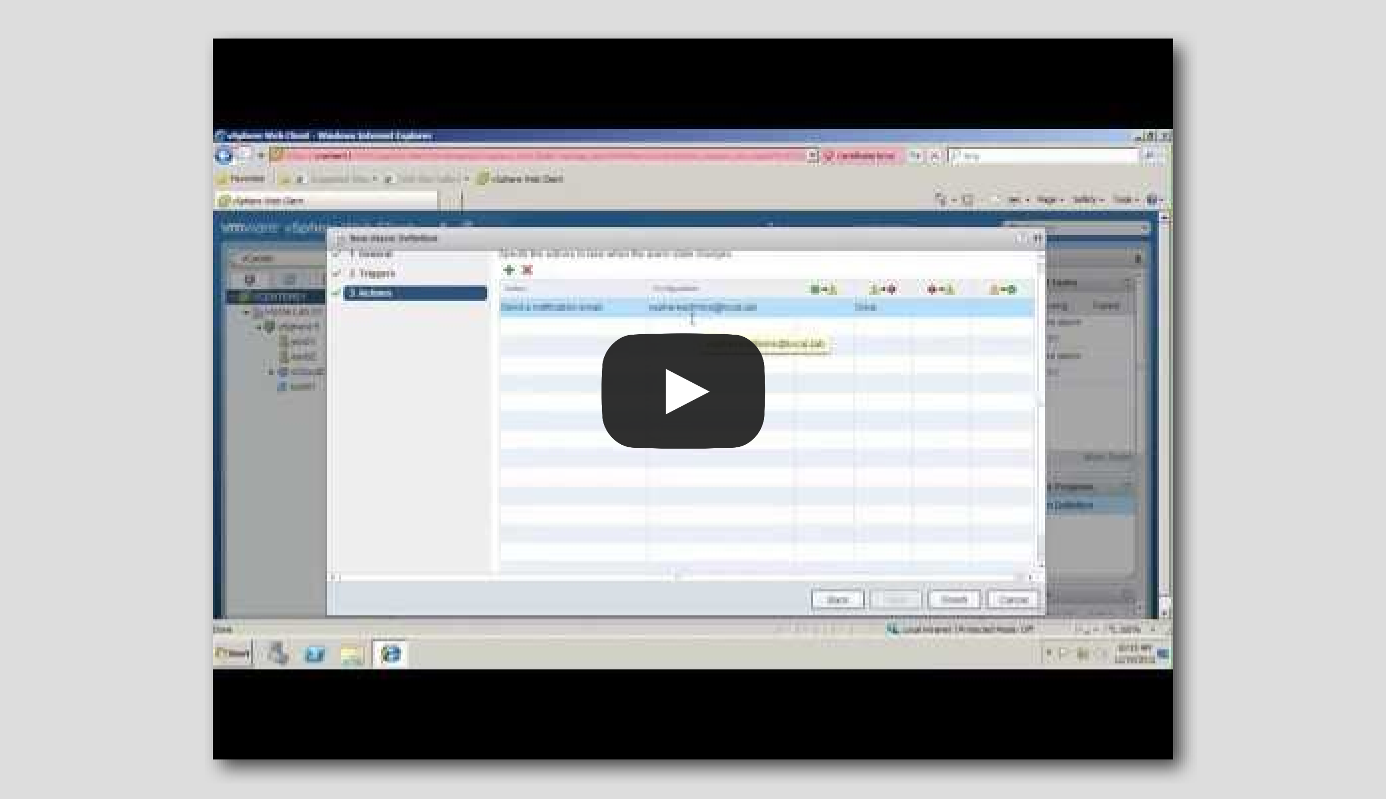


Lightboard illustration of the vCenter Server High Availability options for each deployment type.

Video: Configure Alarms and Notification for VMware vSphere (5:20) [574]

This video shows how to use the VMware vSphere web client to configure vCenter Server alarms and alerts and how to enable email notification.

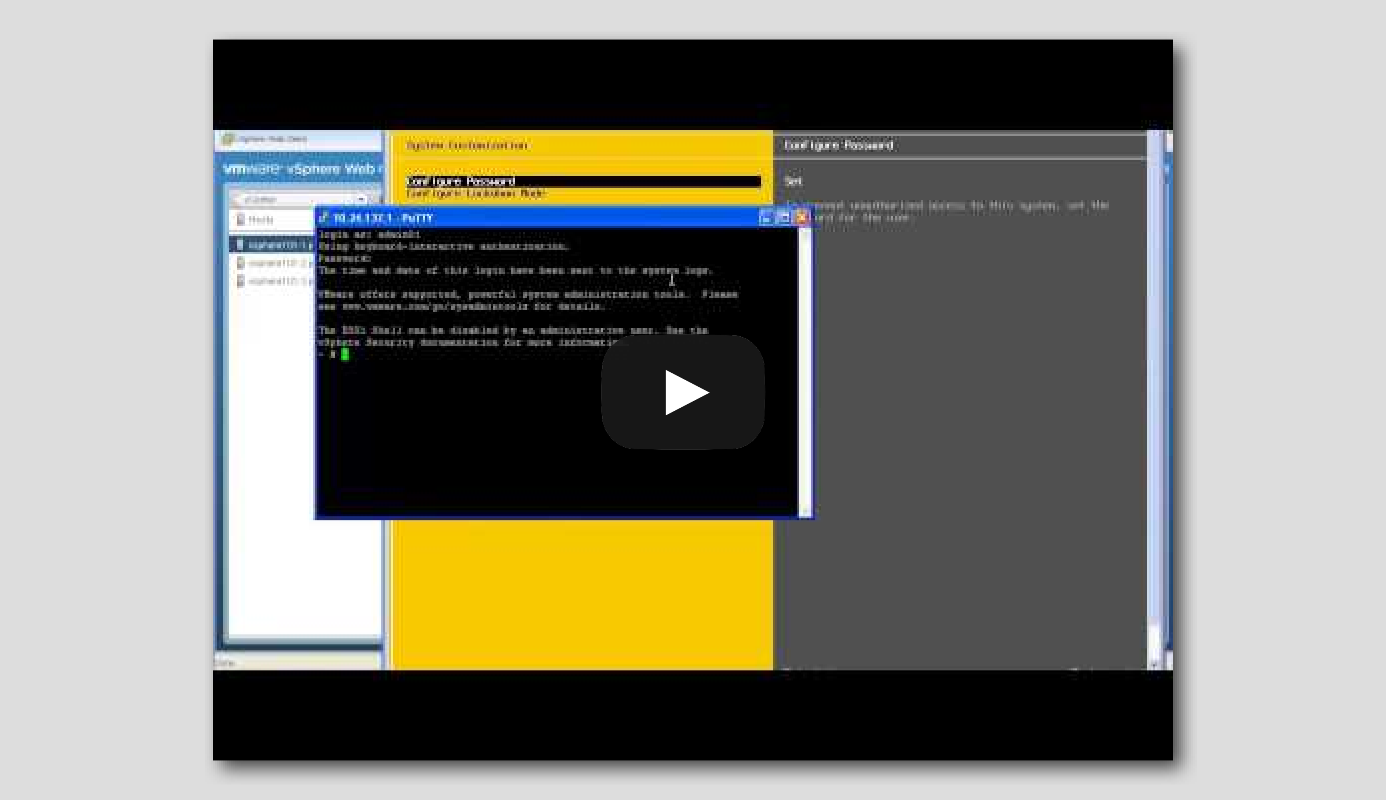
https://www.youtube.com/watch?v=8vWNVBDPcu4



Video: Enable vSphere Host Lockdown Mode for VMware vSphere (4:48) [575]

This video shows how to secure VMware vSphere hosts with Lockdown Mode in order to limit direct access to the host console and to require administrators manage hosts through vCenter Server.

https://www.youtube.com/watch?v=gWIb2HHu3bE



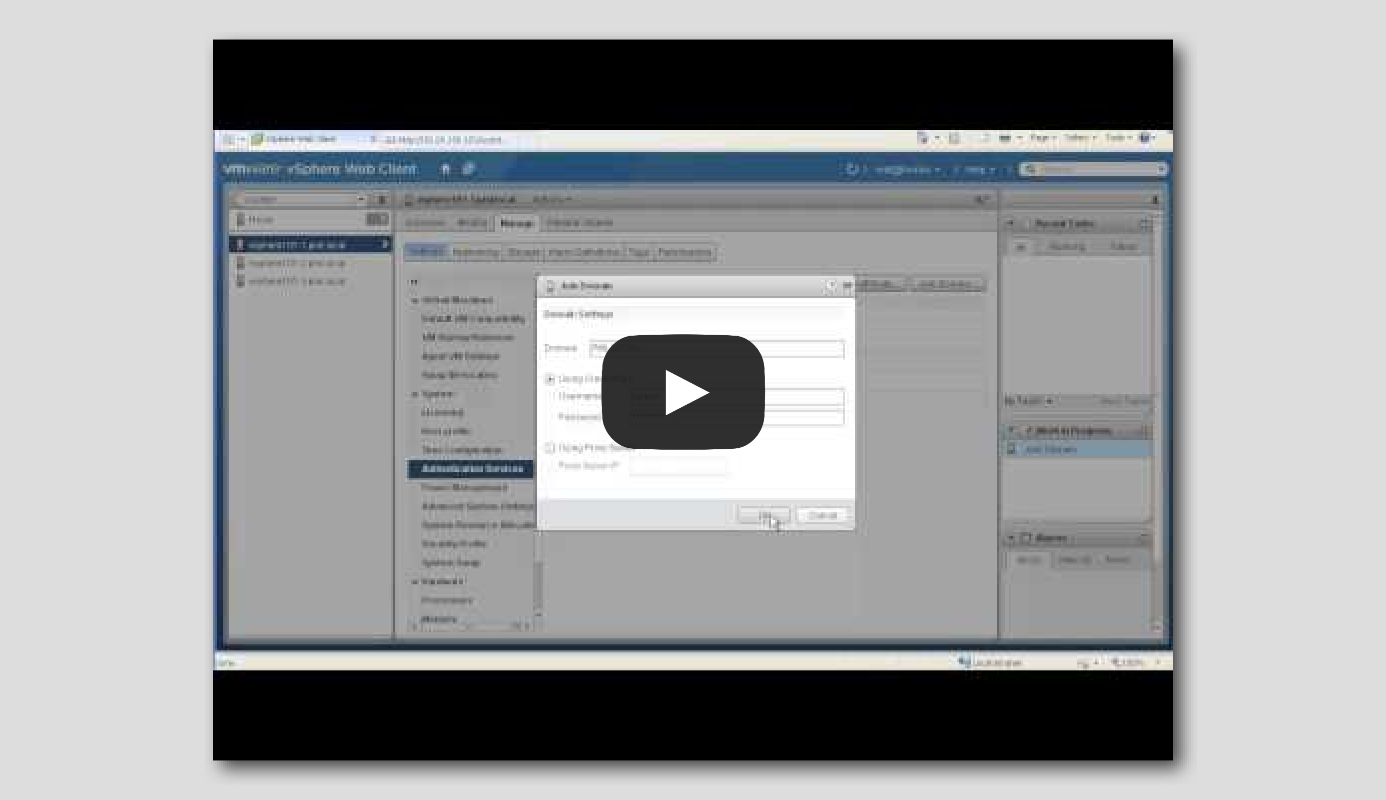
```
login as: [illegible]
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

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.
~ #
```

(Optional) Video: Add VMware vSphere Hosts to Active Directory (3:40)

[576]

This video shows how to join a VMware vSphere host to a Microsoft Active Directory (AD) domain in order to allow administrators to use their Active Directory credentials to access and manage hosts.

https://www.youtube.com/watch?v=H74M__Eshtw

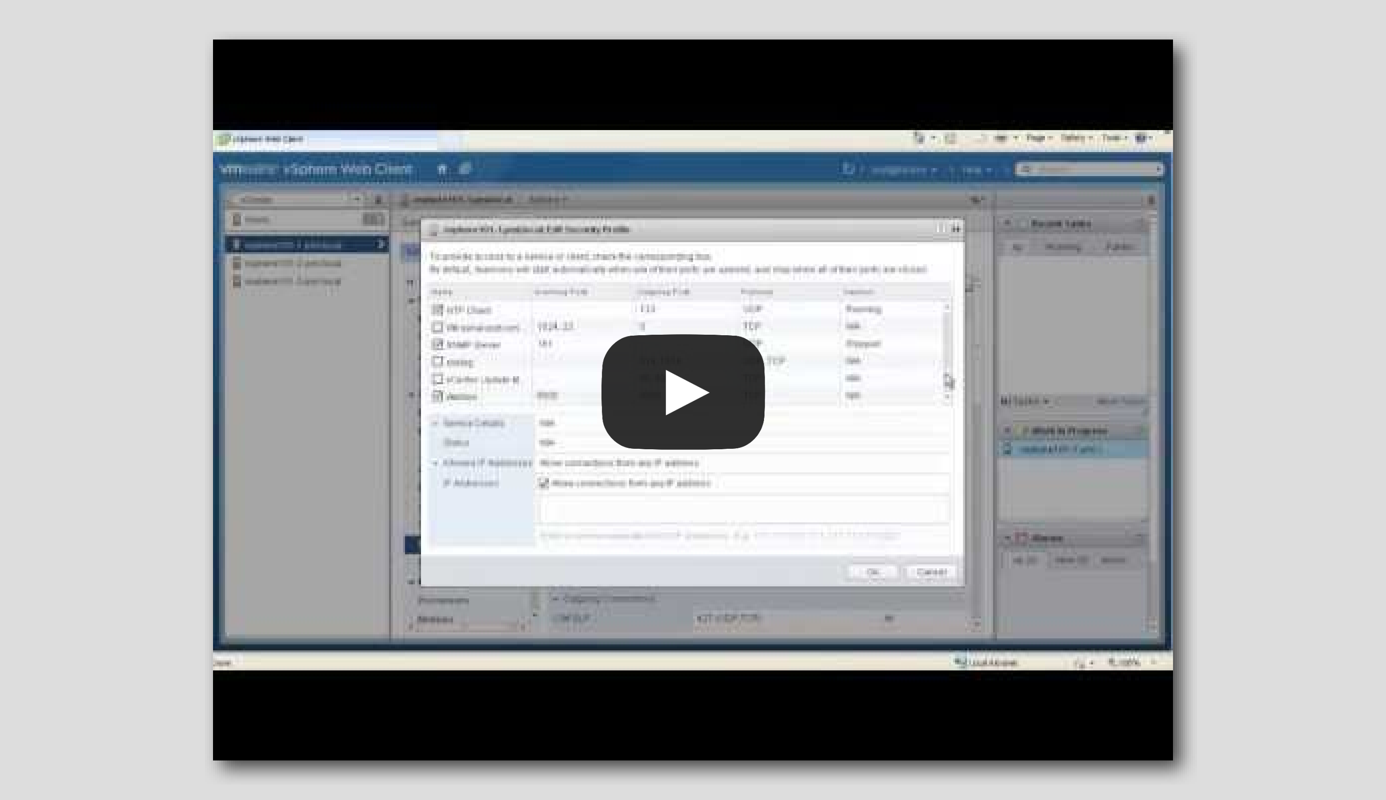


Video: Configure vSphere Host Firewall for VMware vSphere (4:34)

[577]

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

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



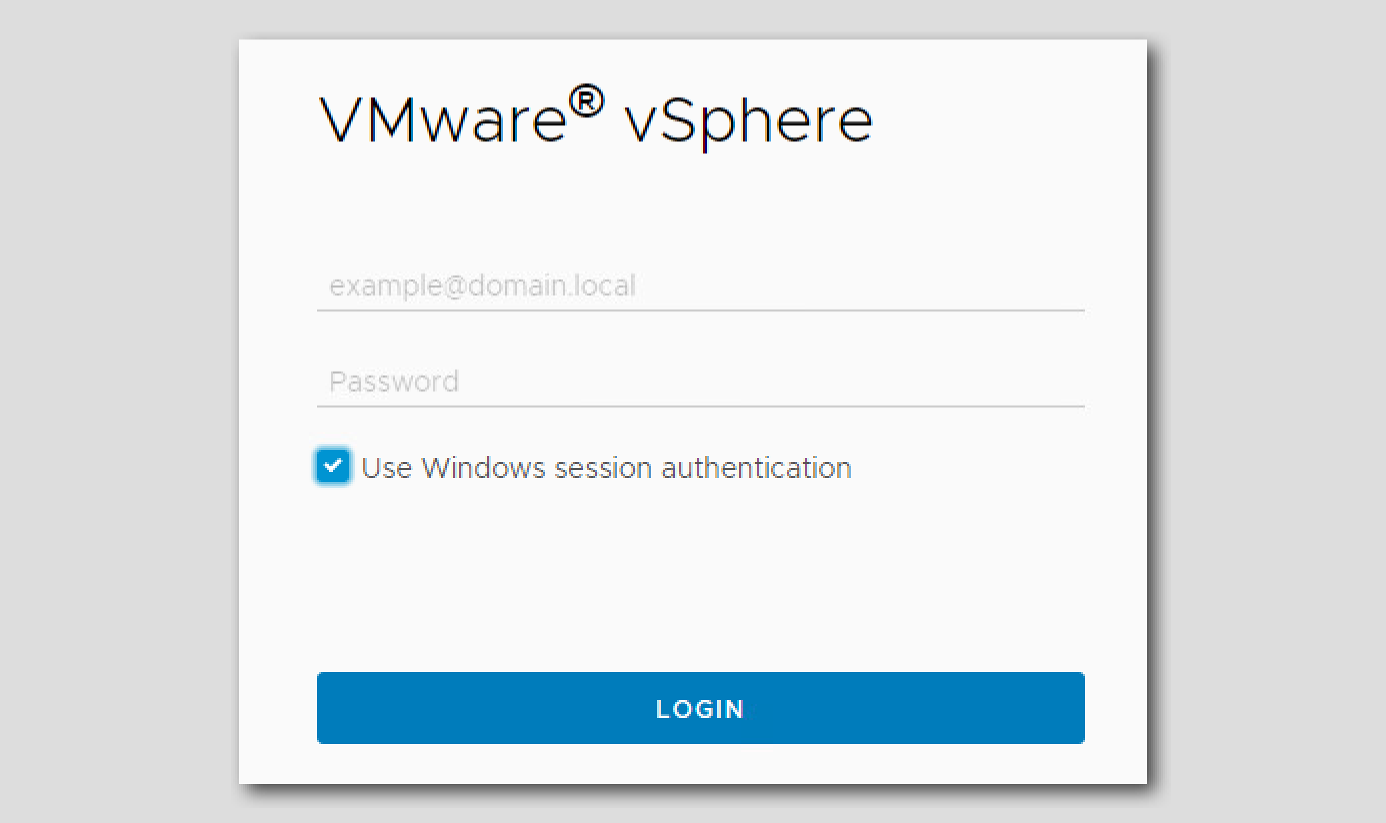
REFERENCE - Unlock vCenter Single Sign On Users in the vSphere Web Client [578]

A vCenter Single Sign On user account might be locked when a user exceeds the allowed number of failed login attempts. After a user account is locked, the user cannot log in to the Single Sign On system until the account is unlocked, either manually or after a certain amount of time has elapsed.

You specify the conditions under which a user account is locked in the Single Sign On Lockout Policy. Locked user accounts appear on the Users and Groups administration page. Users with appropriate privileges can manually unlock Single Sign On user accounts before the specified amount of time has elapsed. You must be a member of the Single Sign On Administrators group to unlock a Single Sign On user.

Locked Out User

[579]



VMware® vSphere

example@domain.local

Password

☑ Use Windows session authentication

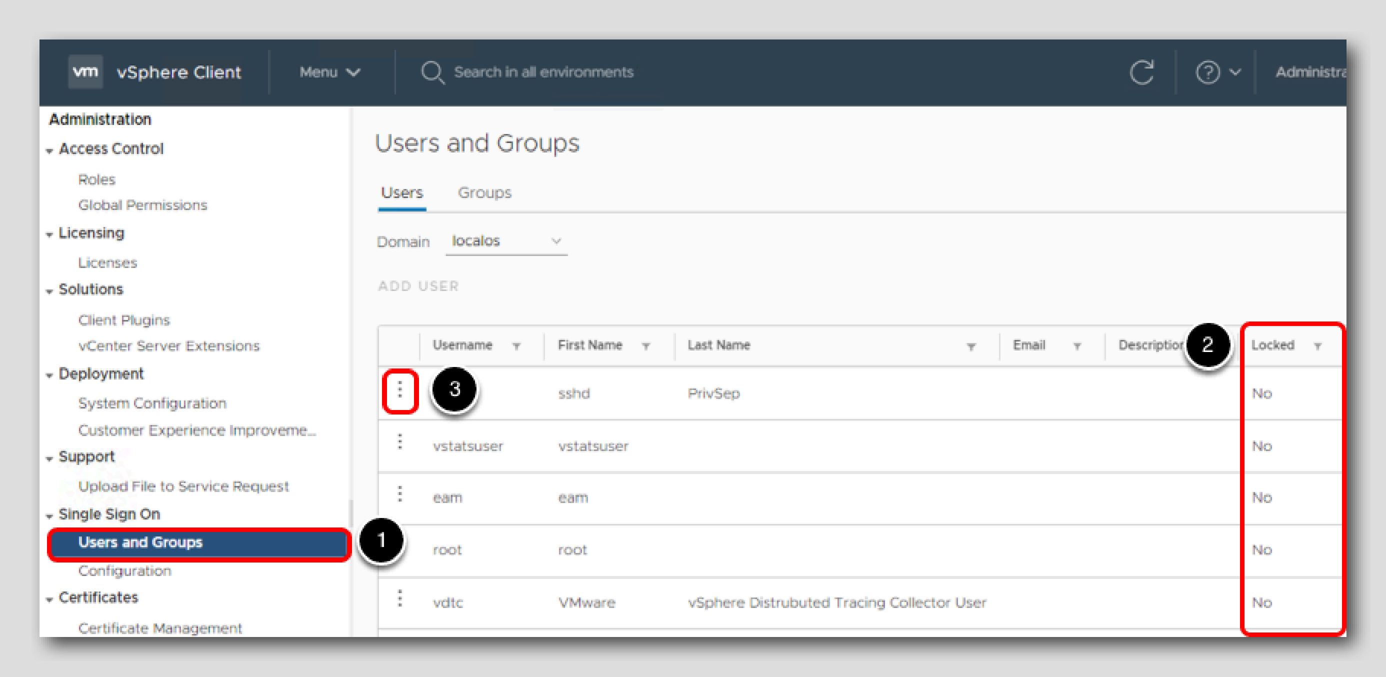
By default, after three failed login attempts, the Users' account is locked.

In the lab, this policy has been disabled in order to prevent login issues that frequently occur with non-US keyboards.

This section has been included for reference purposes only.

Unlocking a User

[580]



Domain localos

	Username	First Name	Last Name	Email	Descriptior	Locked
⋮		sshd	PrivSep			No
⋮	vstatsuser	vstatsuser				No
⋮	eam	eam				No
⋮	root	root				No
⋮	vdtc	VMware	vSphere Distrubuted Tracing Collector User			No

Login to the vSphere Web Client as a user with SSO Admin privileges and navigate Menu --> Administration.

1. Click on Users and Groups
2. Locate the locked user account -- it will show as "Yes" in the "Locked" column if the user is locked
3. Click the three dots on the left and select the unlock option

Log out of the Web Client.

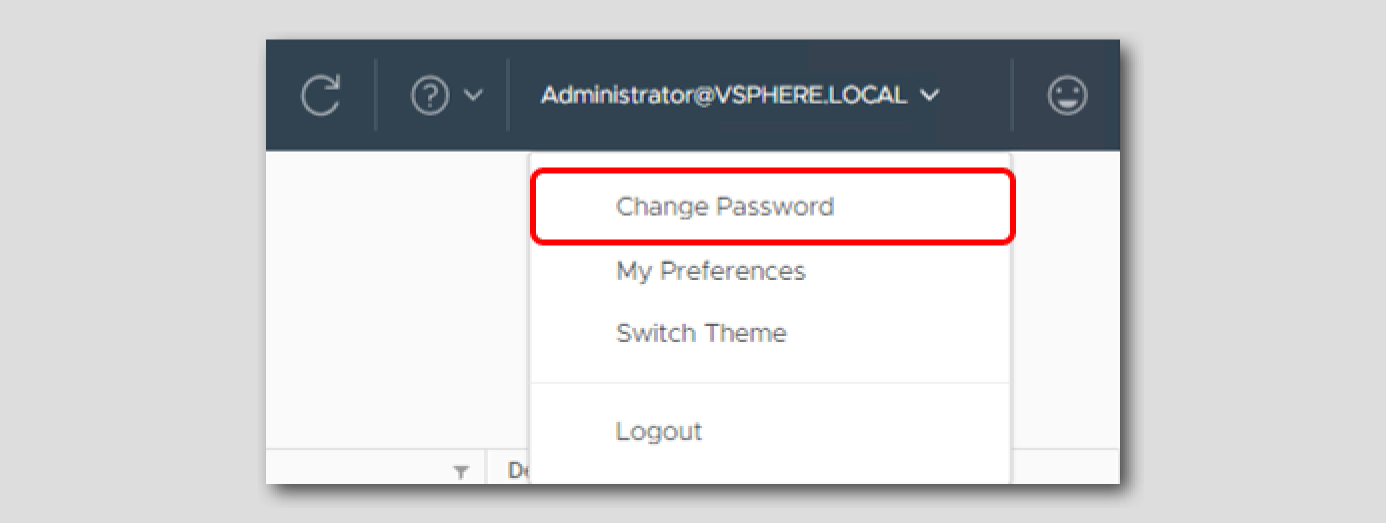
Change Your Password in the vSphere Web Client

[581]

Depending on your vCenter Single Sign On privileges, you might not be able to view or edit your Single Sign On user profile. However, all users can change their Single Sign On passwords in the vSphere Web Client. The password policy defined in the vCenter Single Sign-On configuration tool determines when your password expires. **By default, Single Sign-On passwords expire after 90 days in vSphere 6**, but your system administrator might change this depending on the policy of your organization. If you choose to keep the defaults, remember to change the password for the administrator@vsphere.local account password every 90 days or it will lock out on day 91.

Change Password

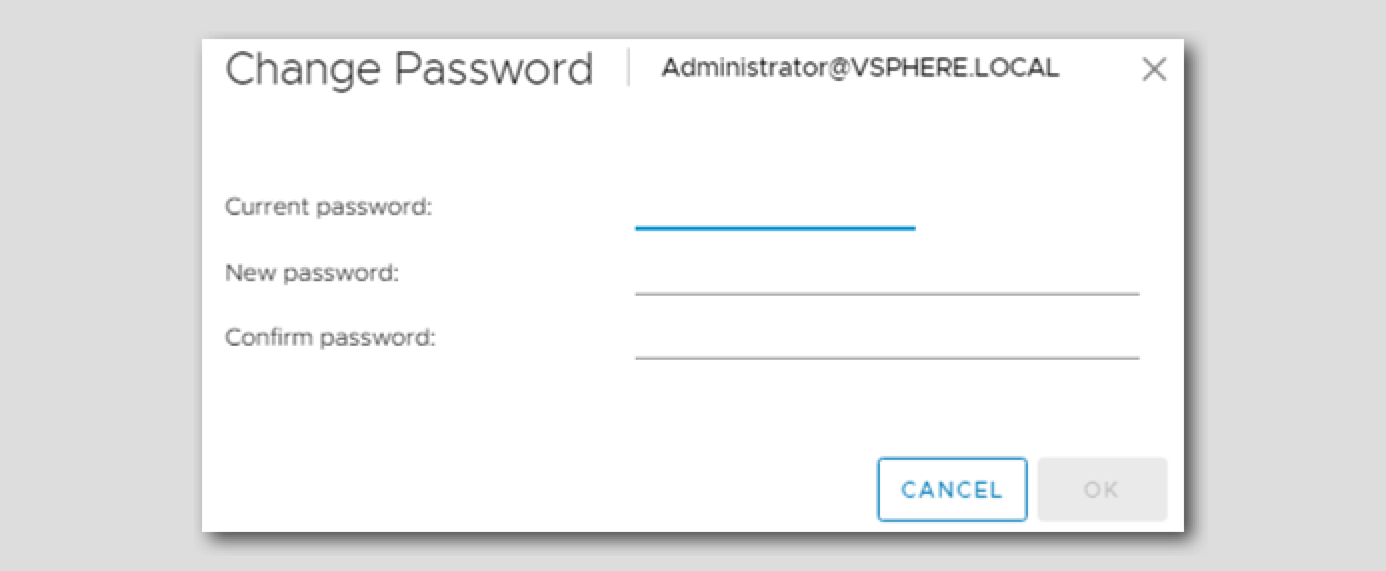
[582]



In the upper navigation pane, click your user name to pull down the menu.

Change Password Dialog

[583]


Change Password | Administrator@VSPHERE.LOCAL

Current password:

New password:

Confirm password:

Select Change Password and type your current password.

Enter a new password.

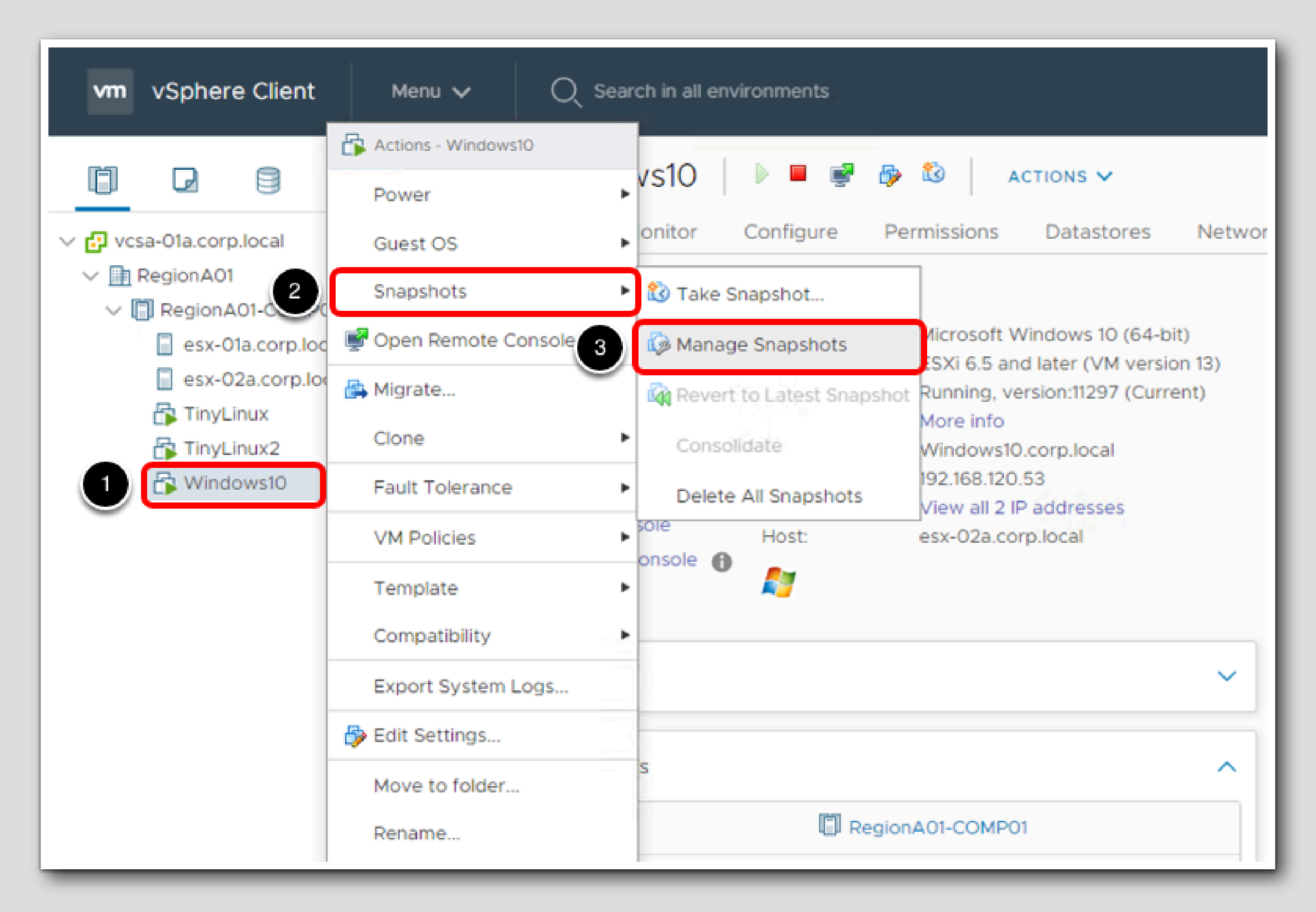
Type a new password and confirm it.

Click the OK button to make the change.

NOTE: If you do change the password, please make sure to remember it for other activities in the lab.

Snapshot Manager

[584]



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

1. Right-click **Windows10**
2. Select **Snapshots**
3. Click **Manage Snapshots**

What is vSphere Storage DRS? (5:08) [585]

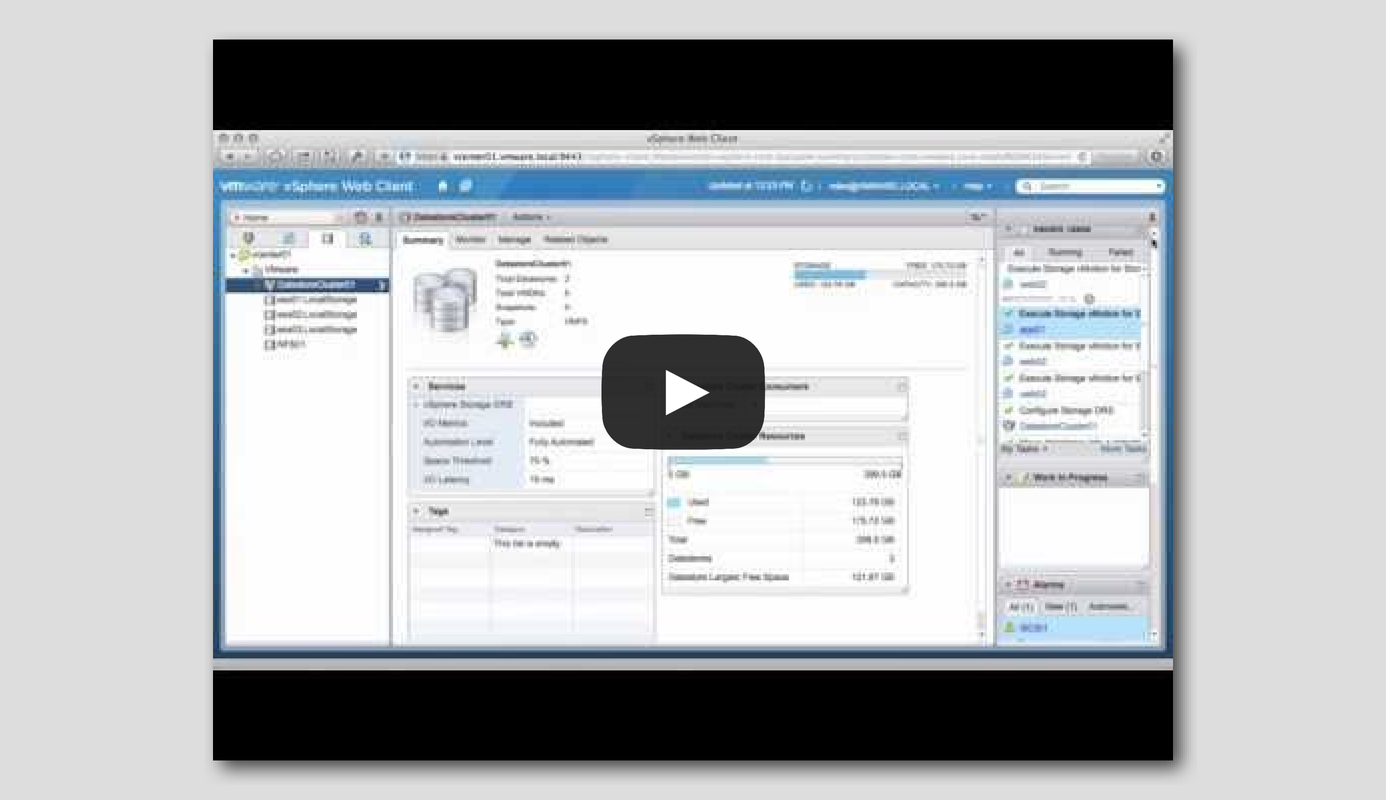
https://www.youtube.com/watch?v=z77xmaxoNec

This animated video shows how VMware Storage DRS reduces the time and complexity of provisioning virtual machines by aggregating data stores into a single pool, called a datastore cluster, enabling rapid placement of virtual machines and virtual machine disks.

Creating a Datastore Cluster with Storage DRS (3:23) [586]

This video reviews the process of creating and managing a datastore cluster in a vSphere environment.

https://www.youtube.com/watch?v=gATLj6pUxnk



Appendix

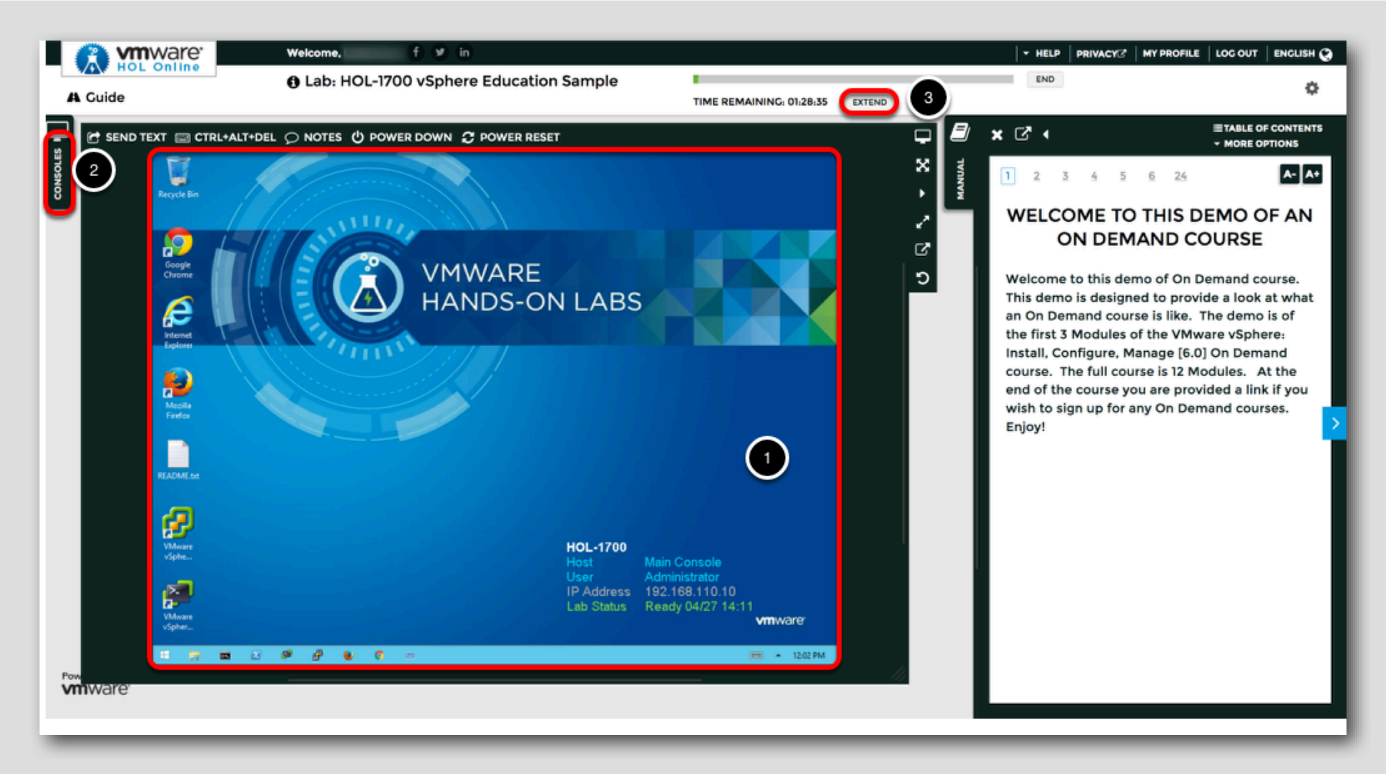
Hands-on Labs Interface

[588]

Welcome to Hands-on Labs! This overview of the interface and features will help you to get started quickly. Click next in the manual to explore the Main Console or use the Table of Contents to return to the Lab Overview page or another module.

Location of the Main Console

[589]



HOL-1700
Host Main Console
User Administrator
IP Address 192.168.110.10
Lab Status Ready 04/27 14:11

WELCOME TO THIS DEMO OF AN ON DEMAND COURSE

Welcome to this demo of On Demand course. This demo is designed to provide a look at what an On Demand course is like. The demo is of the first 3 Modules of the VMware vSphere: Install, Configure, Manage [6.0] On Demand course. The full course is 12 Modules. At the end of the course you are provided a link if you wish to sign up for any On Demand courses. Enjoy!

1. The area in the large RED box contains the Main Console. The Lab Manual is on the tab to the right of the Main Console.
2. Some labs have additional consoles found on separate tabs in the upper left. The lab manual will direct you to open another specific console if necessary.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. Your lab will end when the timer expires. Click the EXTEND button to increase the time allowed. If you are at a VMware event, you can extend your lab time twice up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

[590]

In this lab you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

[591]

https://www.youtube.com/watch?v=xS07n6GzGuo

(Note you can use [illegible] up arrow key)

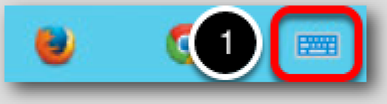
(Remember to use the SEND TEXT option.)

This should now fail.

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

[592]

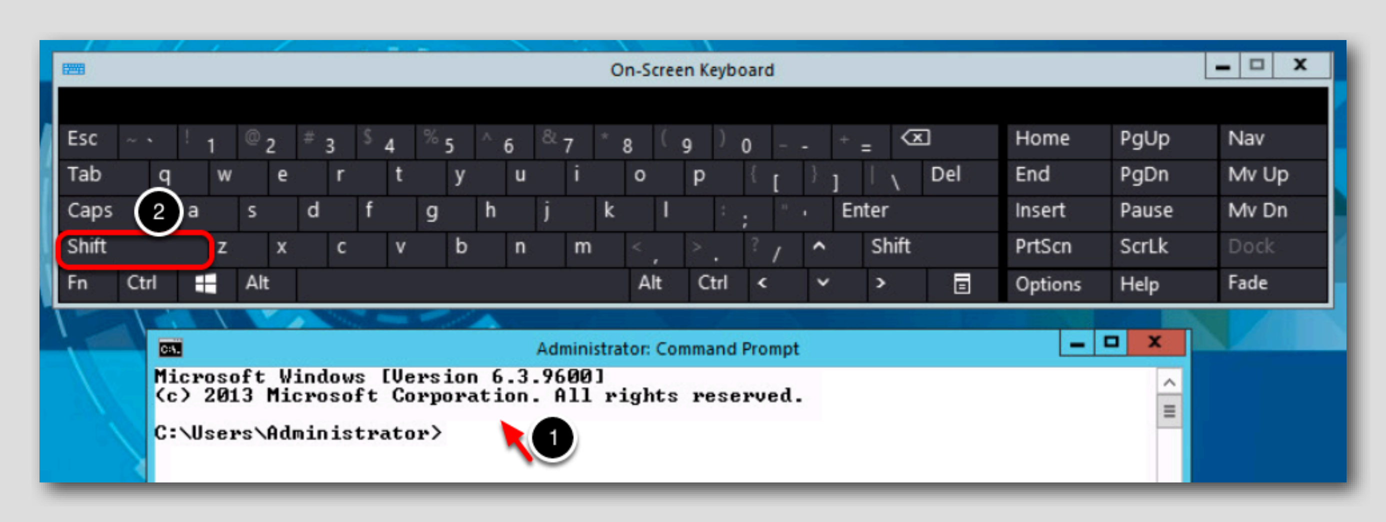


You can also use the Online International Keyboard found in the Main Console.

1. Click on the keyboard icon found on the Windows Quick Launch Task Bar.

Click once in active console window

[593]



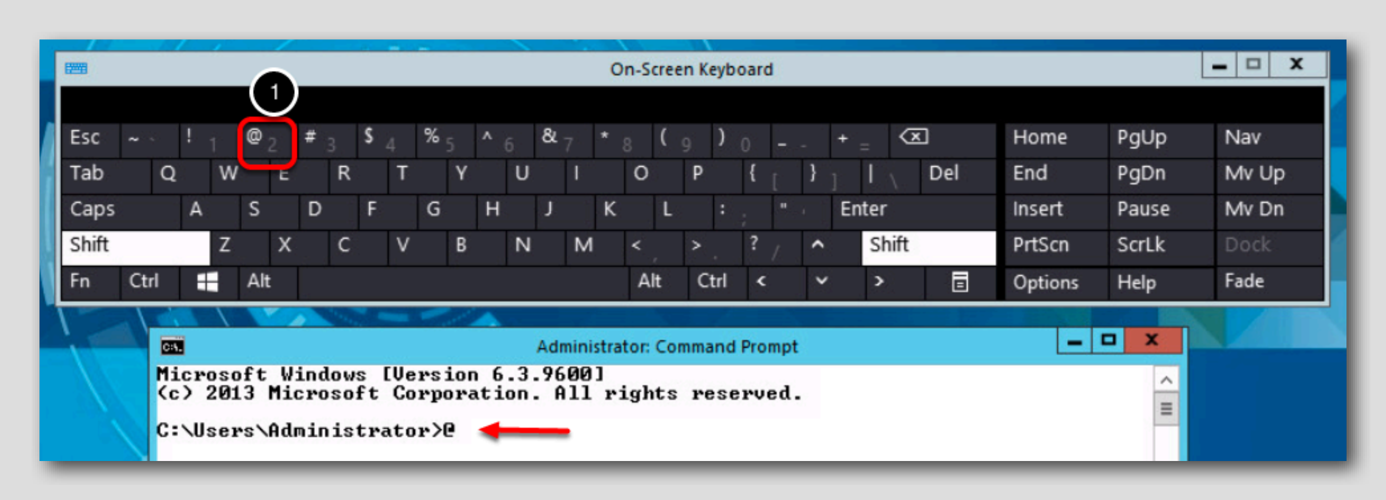
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
```

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

[594]


On-Screen Keyboard
1
Esc ~ ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 - + =
Tab Q W E R T Y U I O P { [}] | \ Del
Caps A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Fn Ctrl Alt Alt Ctrl
Home PgUp Nav
End PgDn Mv Up
Insert Pause Mv Dn
PrtScn ScrLk Dock
Options Help Fade
Administrator: Command Prompt

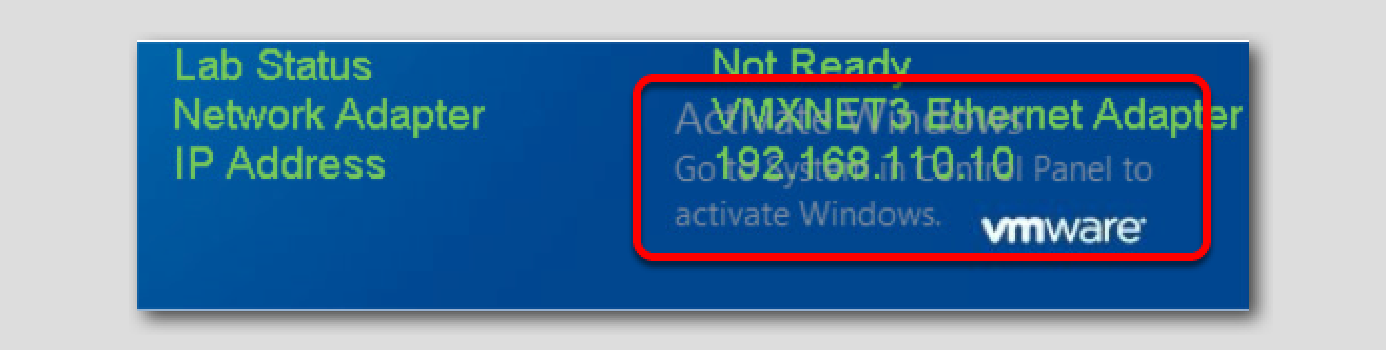
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>@
```

1. Click on the "@" key.

Notice the @ sign entered in the active console window.

Activation Prompt or Watermark

[595]



Lab Status Not Ready
Network Adapter VMXNET3 Ethernet Adapter
IP Address 192.168.110.10

Activate Windows
Go to System in Control Panel to
activate Windows.

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

A major benefit of virtualization allows virtual machines to be moved and run on any platform. Hands-on Labs utilizes this benefit and hosts labs from multiple datacenters. However, these datacenters may not have identical processors which triggers a Microsoft activation check through the Internet.

Rest assured VMware and Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet. Without this, the Microsoft activation process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Return to Lab Guidance [596]

Use the Table of Contents to return to the Lab Overview page or another module.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.

Lab SKU: HOL-2210-01-SDC Version: 20230526-200454