VMware vSphere Install, Configure, Manage | Lab Guide

Version 24.07

Ahmed Abdelwahed
ahmed@abdelwahed.me
LinkedIn

VMware vSphere Install, Configure, Manage | Lab Guide

Contents

Importance of Virtualization:

- **Efficiency**:
  - Maximizes hardware usage.
  - Reduces the need for multiple physical machines.
- **Cost Savings:**
  - Reduces power consumption.
  - Lowers cooling and hardware costs.
- **Flexibility:**
  - Enables rapid VM deployment.
  - Supports scaling and migration.
- **Business Continuity:**
  - Simplifies backup processes.
  - Bolsters disaster recovery.
  - Ensures high availability.
- **Isolation:**
  - Provides distinct environments for applications.
  - Enhances both security and performance.

VMware vSphere Introduction:

- **vSphere:** VMware's leading virtualization platform.
  - **ESXi Hypervisor**: Bare-metal hypervisor for creating VMs.
  - **vCenter Server:** Centralized management for ESXi hosts. Features include:
    - Centralized control and automation of resources.
    - Simplified deployment and management of virtual environments.
  - **vSAN:** Software-defined storage for hyper-converged infrastructure.
    - **Performance**: Flash-optimized storage.
    - **Resilient**: Fault-tolerant and offers data protection.
    - **Scalable**: Effortlessly add capacity as needs grow.
  - **Cloud Integration:** Seamless connection to public cloud platforms.
    - **Hybrid Deployment**: Combine on-premises and cloud resources.
    - **Scale on Demand**: Extend infrastructure to the cloud when needed.
    - **Disaster Recovery**: Backup and restore with cloud solutions.

ESXi Installation and Configuration:

ESXi is the bare-metal hypervisor from VMware that provides the foundation for running virtual machines on a physical server. In this section, we will cover the basic steps for installing and configuring ESXi.

1. Check hardware compatibility:

- Before installing ESXi, you need to ensure that the hardware is compatible. You can check the hardware compatibility by visiting the VMware Compatibility Guide - System Search.

2. Download ESXi ISO image and burn to CD/DVD or USB drive:

- Once you have downloaded the ESXi ISO image, you can burn it to a CD/DVD or USB drive using a tool like Rufus or the built-in Windows USB/DVD Download Tool.

3. Boot the server from the CD/DVD or USB drive:

- Insert the CD/DVD or USB drive into the server and boot from it. The ESXi installer will start.

4. Install ESXi:

- Follow the on-screen instructions to install ESXi. You will need to select the disk on which to install ESXi and provide basic networking information like IP address, subnet mask, default gateway, and DNS server.

5. Configure ESXi:

- After installing ESXi, you can configure it by logging in to the vSphere Web Client or vSphere Client. You can configure settings like hostname, network configuration, time zone, and NTP server.

6. Create a virtual machine:

- Once ESXi is installed and configured, you can create virtual machines using the vSphere Web Client or vSphere Client. You will need to provide settings like virtual machine name, guest operating system, number of CPUs, amount of RAM, and storage.

7. Power on and access the virtual machine:

- After creating the virtual machine, you can power it on and access it using a remote desktop or a console connection. You can also install an operating system and other software on the virtual machine.

Note: All instructions are explained in detail below with screenshots to guide you through each step of the process.

DNS Configuration for all ESXi Hosts and vCenter Servers

Configuring Domain Name System (DNS) for all ESXi hosts and vCenter Servers is important as it allows these hosts to communicate with other hosts and services on the network using domain names instead of IP addresses.

Forward Lookup Zone Configuration

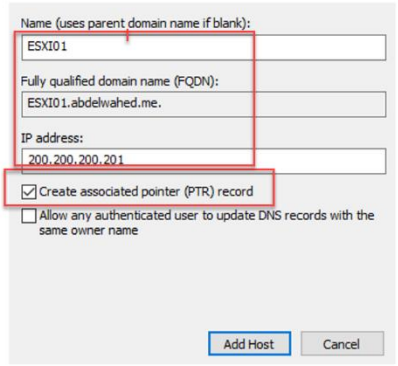
1. **Add A (Address) Records**:
   - Open your DNS manager.
   - Navigate to the forward lookup zone for abdelwahed.me.
   - Add the following A records for each ESXi host, vCenter server:

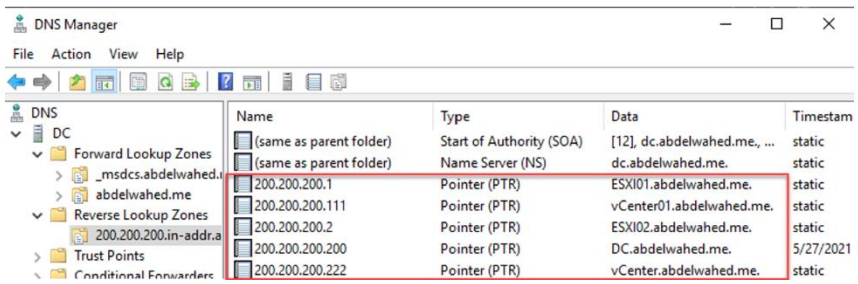
Hostname	IP Address
ESXI01	200.200.200.201
ESXI02	200.200.200.202
vCenter01	200.200.200.111
DC	200.200.200.200

Reverse Lookup Zone Configuration

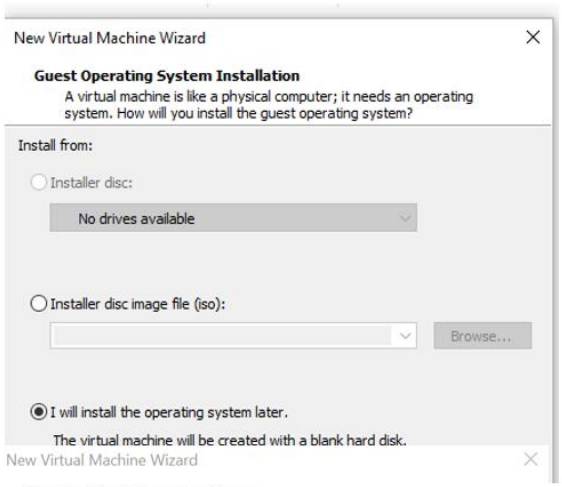
1. **Add Reverse Lookup Zone**:
   - Open your DNS manager.
   - Create a new reverse lookup zone for the network 200.200.200.x.
2. **Add PTR (Pointer) Records**:
   - Within the reverse lookup zone, add the following PTR records:

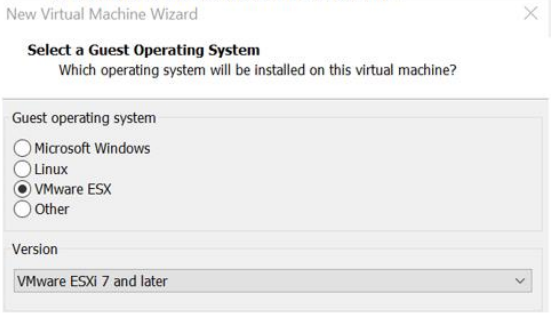
IP Address	Hostname
200.200.200.201	ESXI01.abdelwahed.me
200.200.200.202	ESXI02.abdelwahed.me
200.200.200.111	vCenter01.abdelwahed.me
200.200.200.200	dc.abdelwahed.me

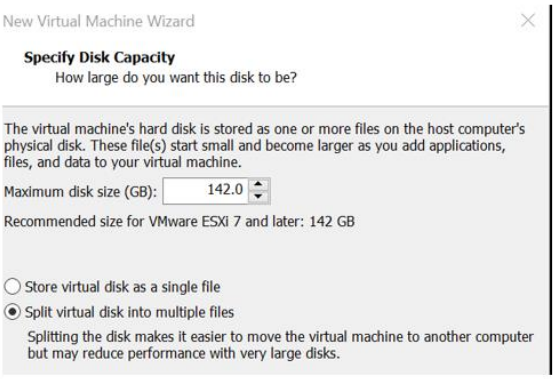


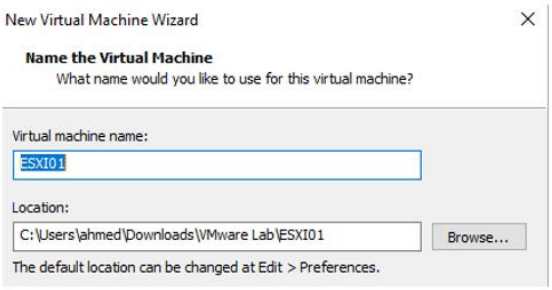


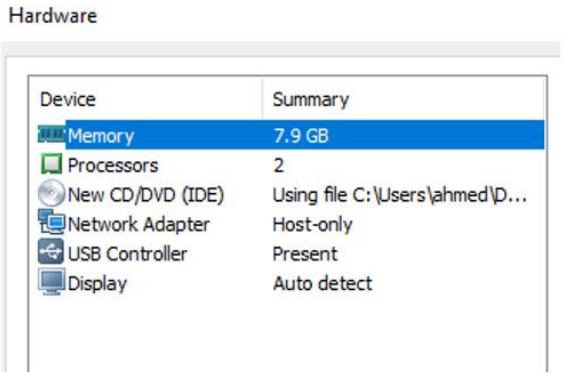
Basic Configuration for a Virtual Machine to Host ESXi Server inside VMware Workstation

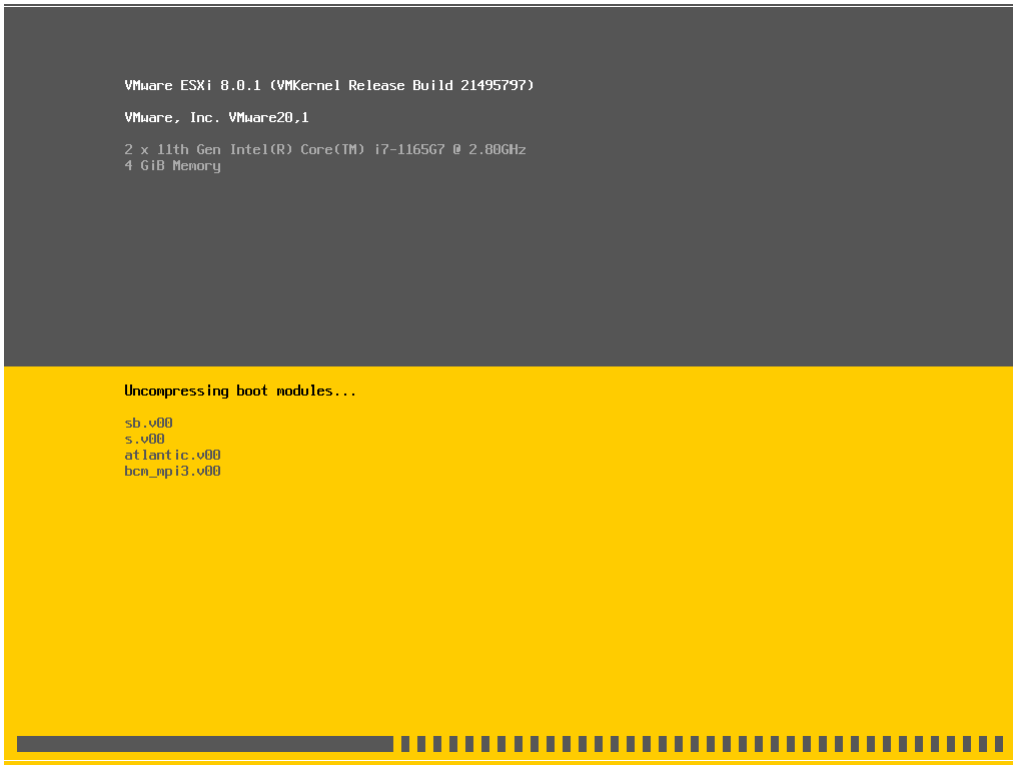




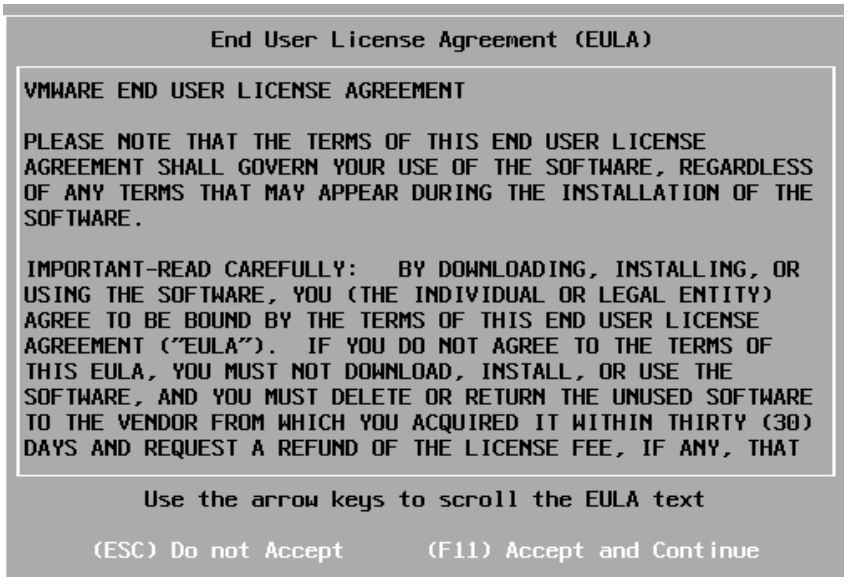




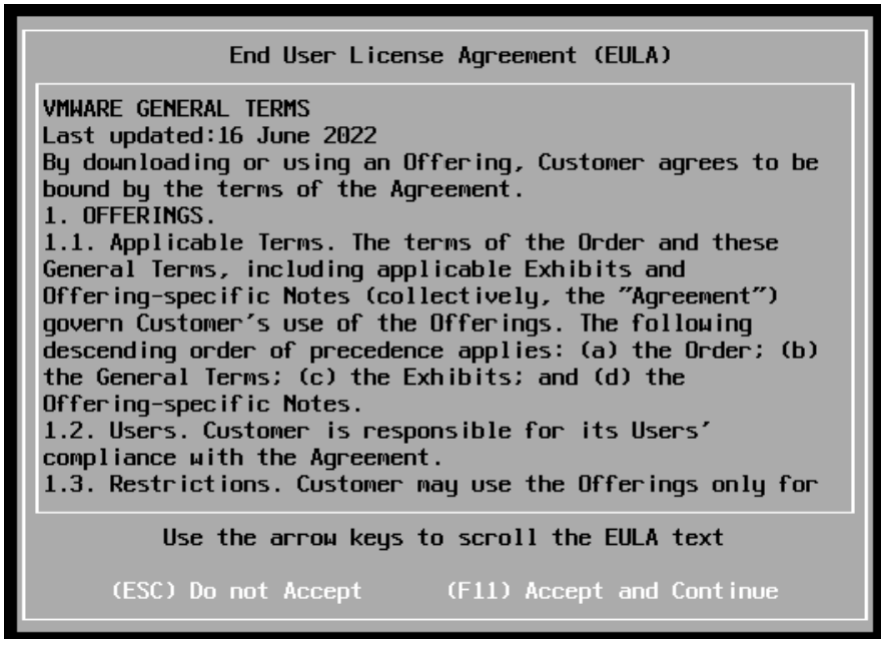


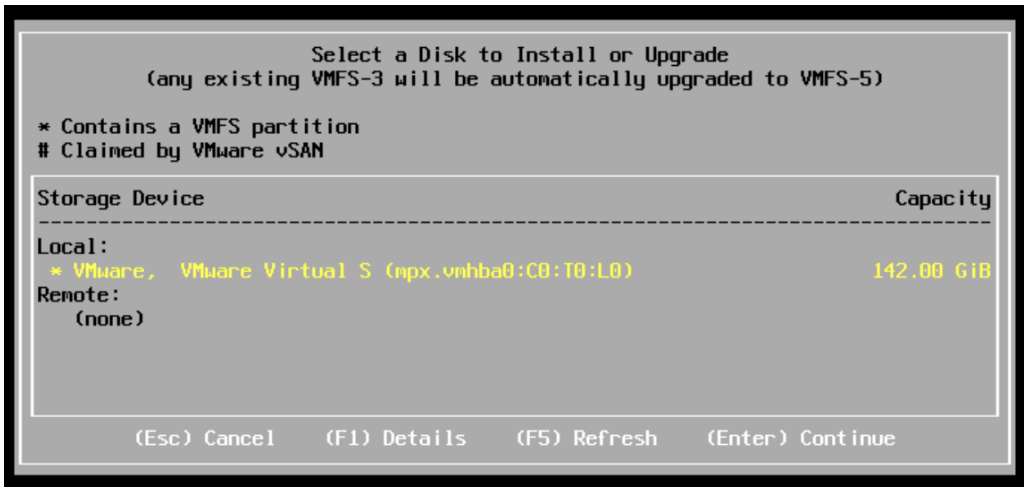


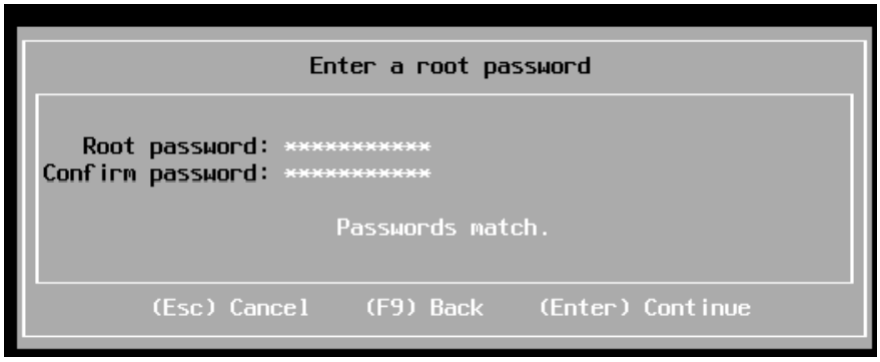
Press F11 to agree to the license.

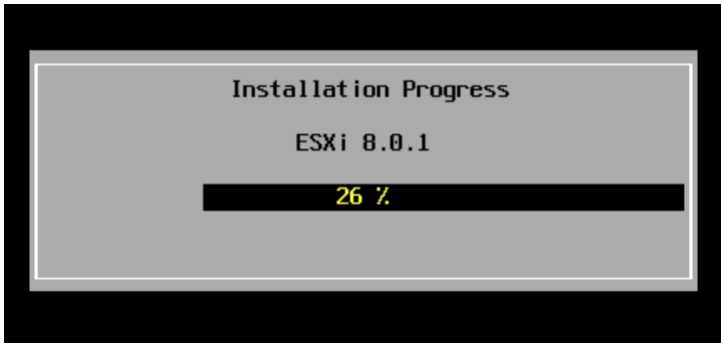



VMware ESXi 8.0.1 Installer
Welcome to the VMware ESXi 8.0.1 Installation
VMware ESXi 8.0.1 installs on most systems but only systems on VMware's Compatibility Guide are supported.
Consult the VMware Compatibility Guide at: http://www.vmware.com/resources/compatibility
Select the operation to perform.
(Esc) Cancel
(Enter) Continue

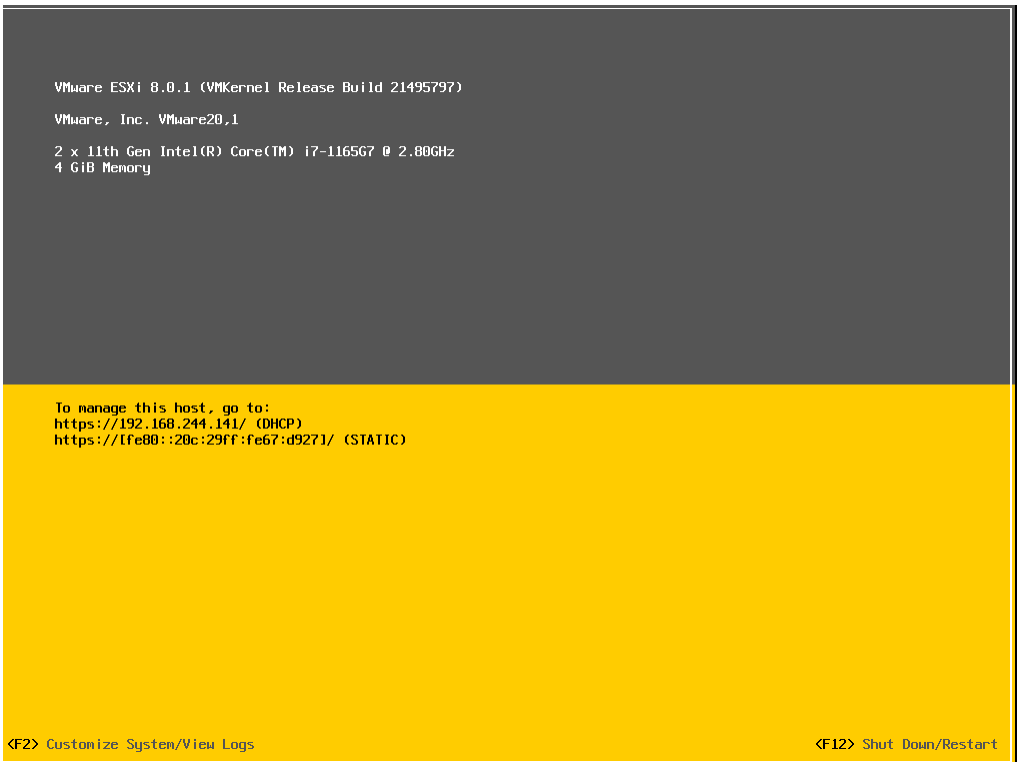

End User License Agreement (EULA)
VMWARE GENERAL TERMS
Last updated:16 June 2022
By downloading or using an Offering, Customer agrees to be bound by the terms of the Agreement.
1. OFFERINGS.
1.1. Applicable Terms. The terms of the Order and these General Terms, including applicable Exhibits and Offering-specific Notes (collectively, the "Agreement") govern Customer's use of the Offerings. The following descending order of precedence applies: (a) the Order; (b) the General Terms; (c) the Exhibits; and (d) the Offering-specific Notes.
1.2. Users. Customer is responsible for its Users' compliance with the Agreement.
1.3. Restrictions. Customer may use the Offerings only for
Use the arrow keys to scroll the EULA text
(ESC) Do not Accept
(F11) Accept and Continue


Select a Disk to Install or Upgrade
(any existing VMFS-3 will be automatically upgraded to VMFS-5)
* Contains a VMFS partition
# Claimed by VMware vSAN
Storage Device
Capacity
Local:
* VMware, VMware Virtual S (mpx.vmhba0:C0:T0:L0)
142.00 GiB
Remote:
(none)
(Esc) Cancel
(F1) Details
(F5) Refresh
(Enter) Continue


Enter a root password
Root password: **********
Confirm password: **********
Passwords match.
(Esc) Cancel
(F9) Back
(Enter) Continue

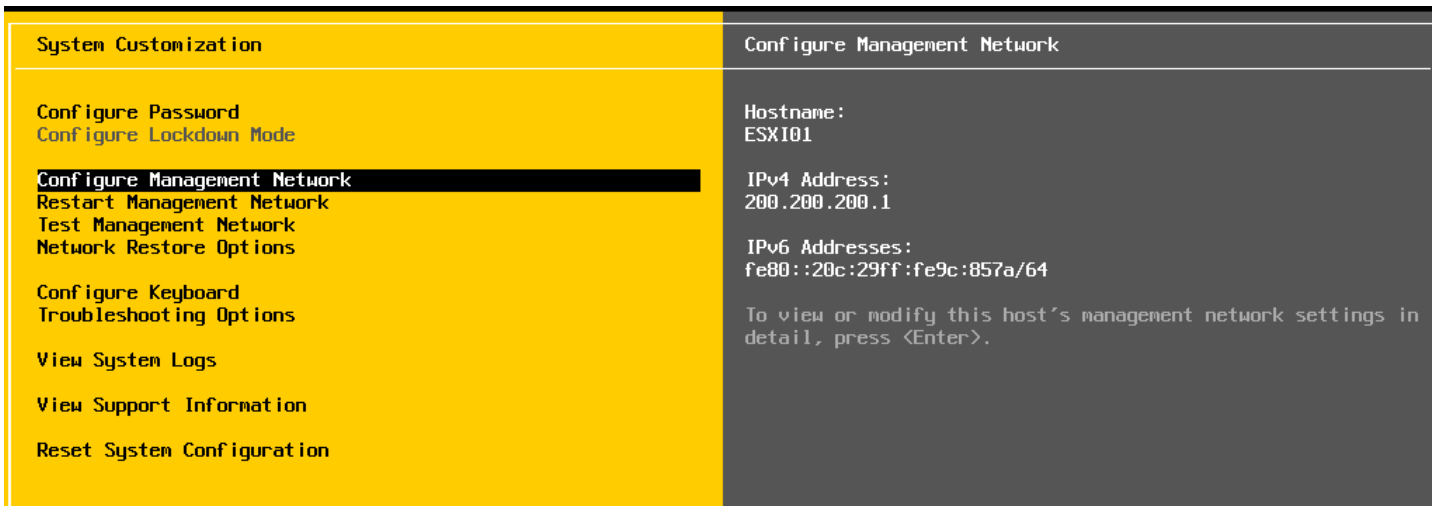

Installation Progress
ESXi 8.0.1
26 %

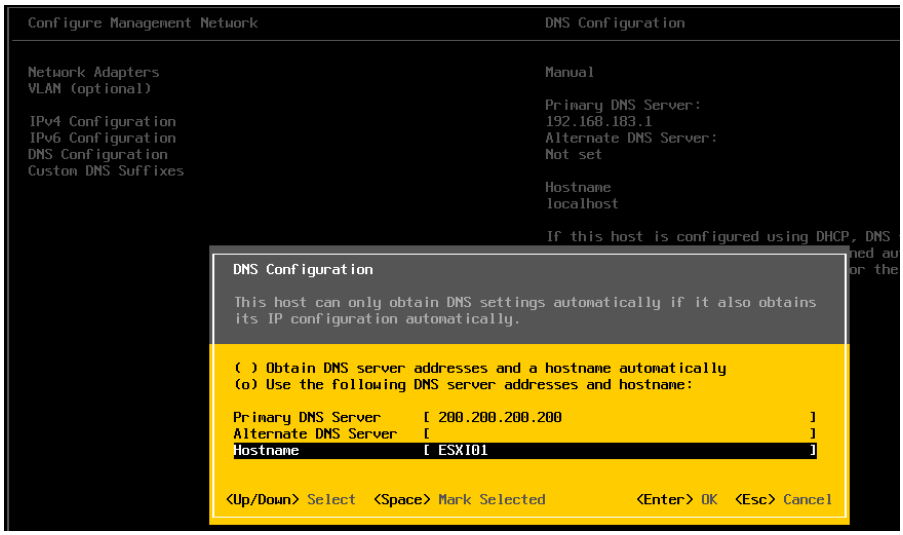
Press F2 to sign in as the root user.

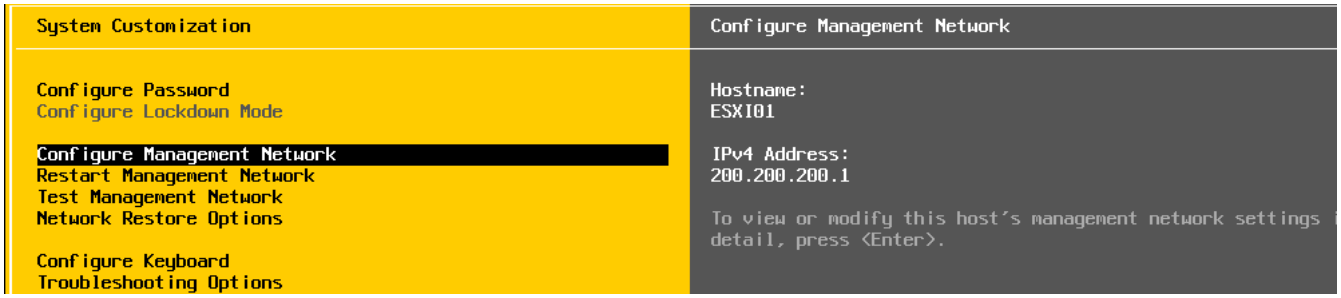


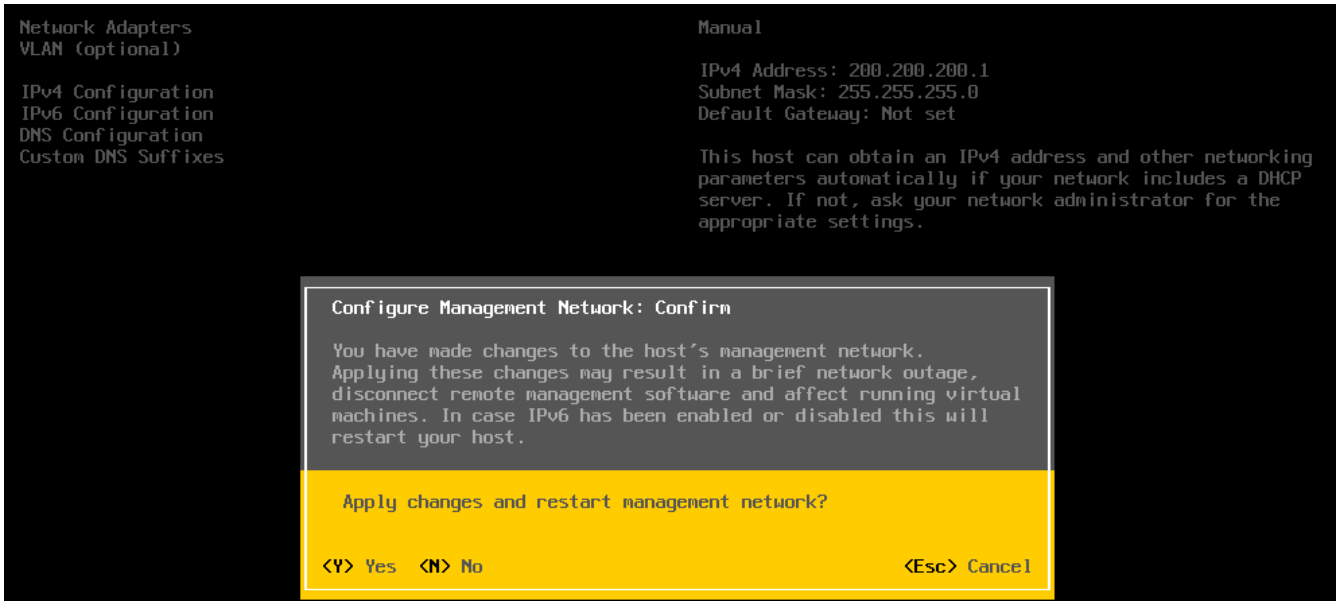
Set up the hostname and network configurations.

You can now set up the hostname and network to enable remote management of the server via http.

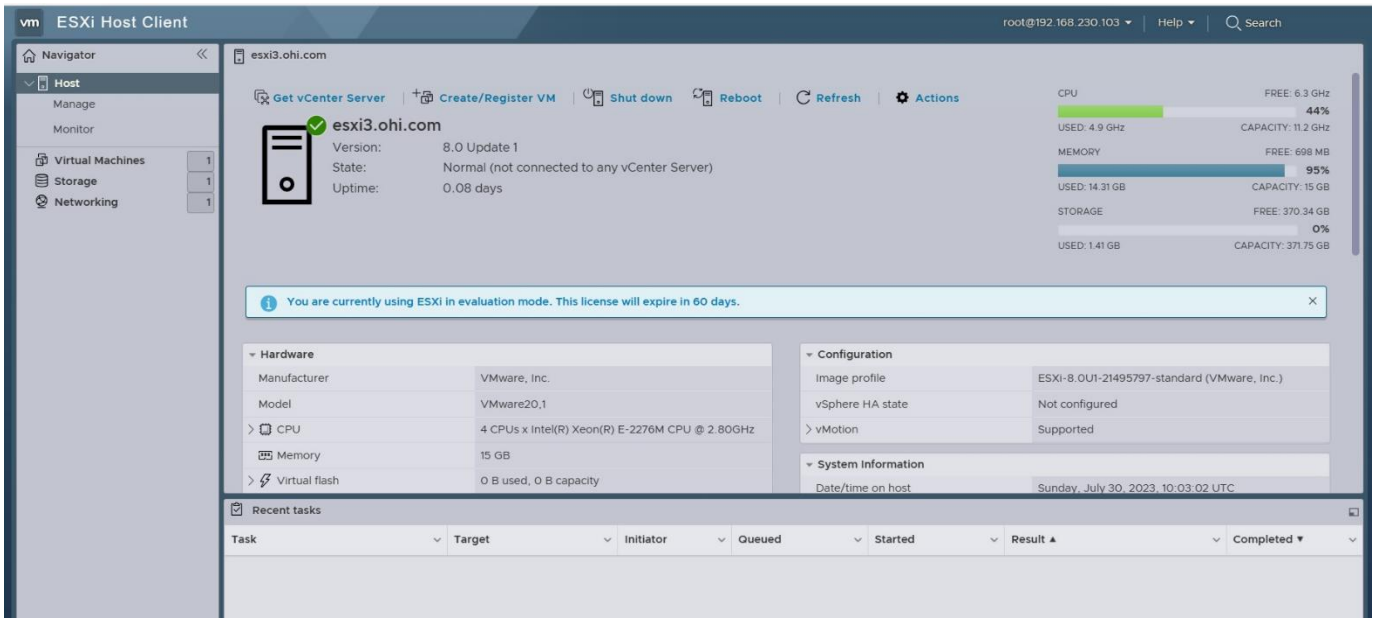



Configure Management Network
DNS Configuration
Network Adapters
VLAN (optional)
IPv4 Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes
Manual
Primary DNS Server:
192.168.183.1
Alternate DNS Server:
Not set
Hostname
localhost
DNS Configuration
This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.
( ) Obtain DNS server addresses and a hostname automatically
(o) Use the following DNS server addresses and hostname:
Primary DNS Server [200.200.200.200]
Alternate DNS Server [ ]
Hostname [ESXI01]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel


System Customization
Configure Password
Configure Lockdown Mode
Configure Management Network
Restart Management Network
Test Management Network
Network Restore Options
Configure Keyboard
Troubleshooting Options
Configure Management Network
Hostname:
ESXI01
IPv4 Address:
200.200.200.1
To view or modify this host's management network settings
detail, press <Enter>.


Network Adapters
VLAN (optional)
IPv4 Configuration
IPv6 Configuration
DNS Configuration
Custom DNS Suffixes
Manual
IPv4 Address: 200.200.200.1
Subnet Mask: 255.255.255.0
Default Gateway: Not set
This host can obtain an IPv4 address and other networking parameters automatically if your network includes a DHCP server. If not, ask your network administrator for the appropriate settings.
Configure Management Network: Confirm
You have made changes to the host's management network. Applying these changes may result in a brief network outage, disconnect remote management software and affect running virtual machines. In case IPv6 has been enabled or disabled this will restart your host.
Apply changes and restart management network?
<Y> Yes <N> No <Esc> Cancel

Now, all ESXi servers are manageable directly through a web browser.



Repeat these steps for every ESXi server you intend to set up.

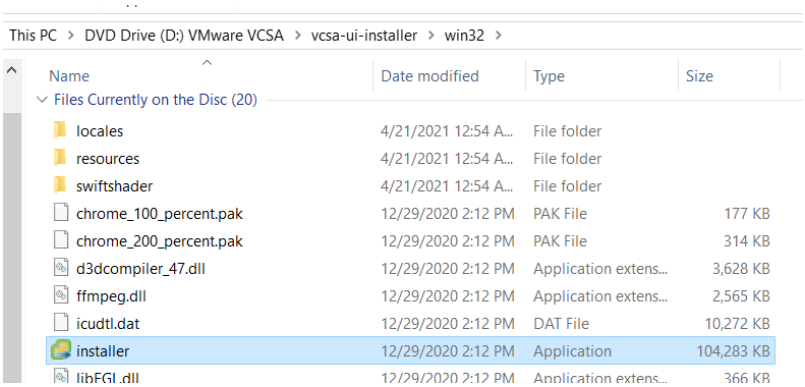
vCenter

vCenter is a management software platform for VMware vSphere, a virtualization platform used by many organizations to host and manage virtual machines. vCenter allows administrators to manage multiple ESXi hosts and their virtual machines from a single centralized location, providing a more streamlined and efficient way to manage a virtual infrastructure. Here are some of the key features and benefits of vCenter:

1. **Centralized Management**:
    - With vCenter, administrators can manage multiple ESXi hosts and their virtual machines from a single, unified console.
    - This provides a more streamlined and efficient way to manage virtual infrastructure, as well as more control over the virtual environment.
2. **High Availability**:
    - vCenter supports high availability features, such as vCenter High Availability (vCHA), that ensure that vCenter remains available in the event of hardware or software failures.
3. **Automation**:
    - vCenter includes automation features, such as vSphere Auto Deploy and vSphere PowerCLI, that allow administrators to automate tasks and workflows in the virtual environment, reducing the workload and potential for human error.
4. **Security**:
    - vCenter includes security features, such as vCenter Single Sign-On (SSO), that help ensure that the virtual environment is secure and protected from unauthorized access.
5. **Performance Monitoring**:
    - vCenter includes performance monitoring features, such as vSphere Distributed Resource Scheduler (DRS) and vSphere High Availability (HA), that help administrators optimize the performance and availability of the virtual environment.

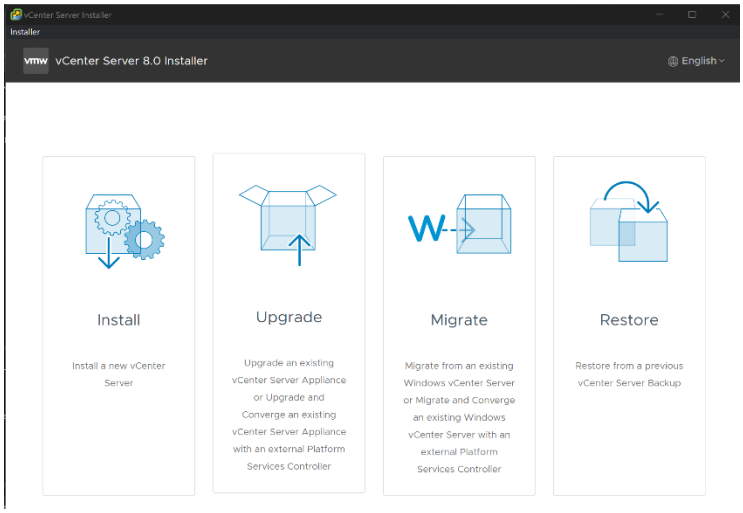
Deploy vCenter

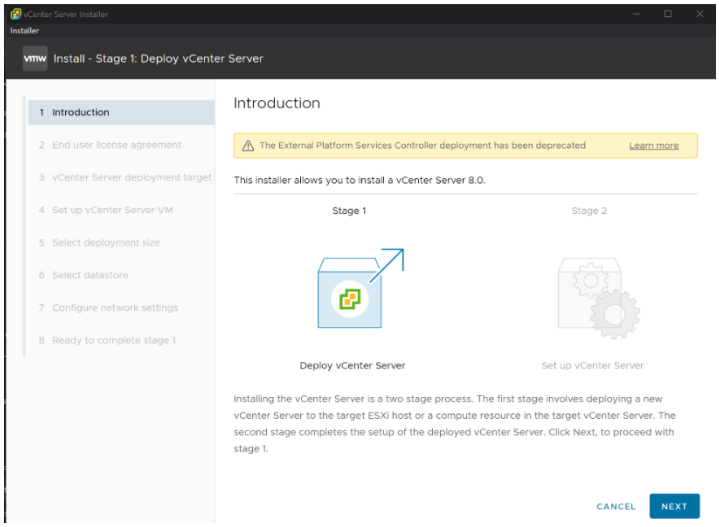
Install vCenter by mounting the VCA ISO onto a Domain Controller or any virtual machine that is part of the abdelwahed.me domain. Begin the installation process with ESXI1 designated as the host for deploying vCenter.

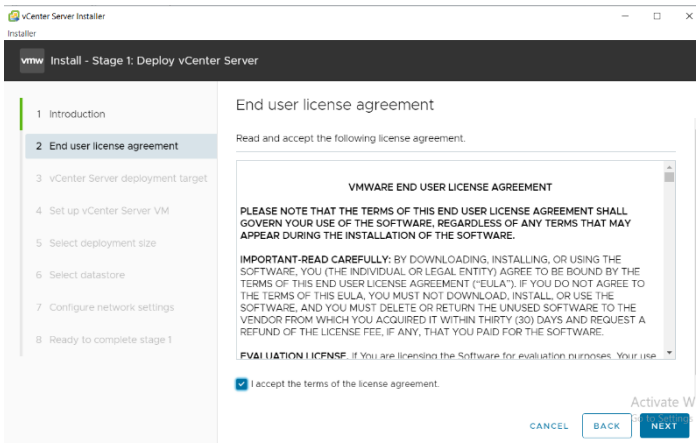


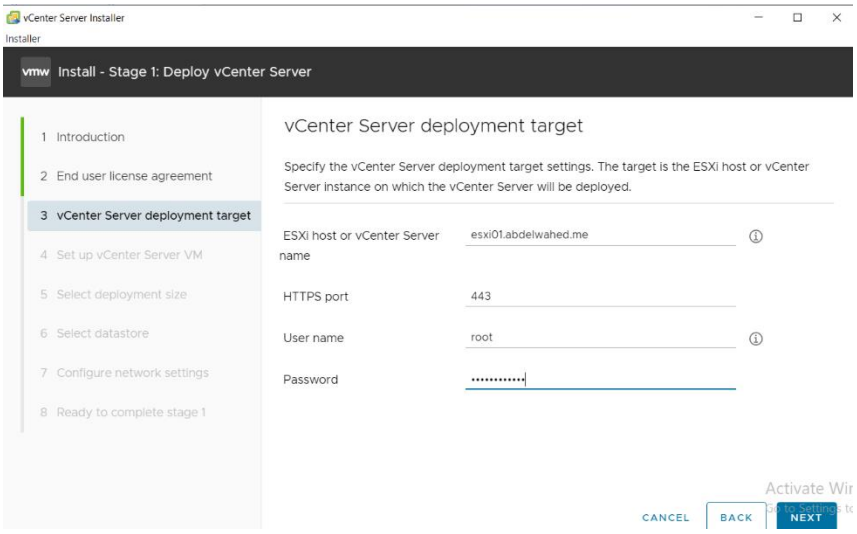
vCenter Server 8.0 Installer interface, which provides four main options:

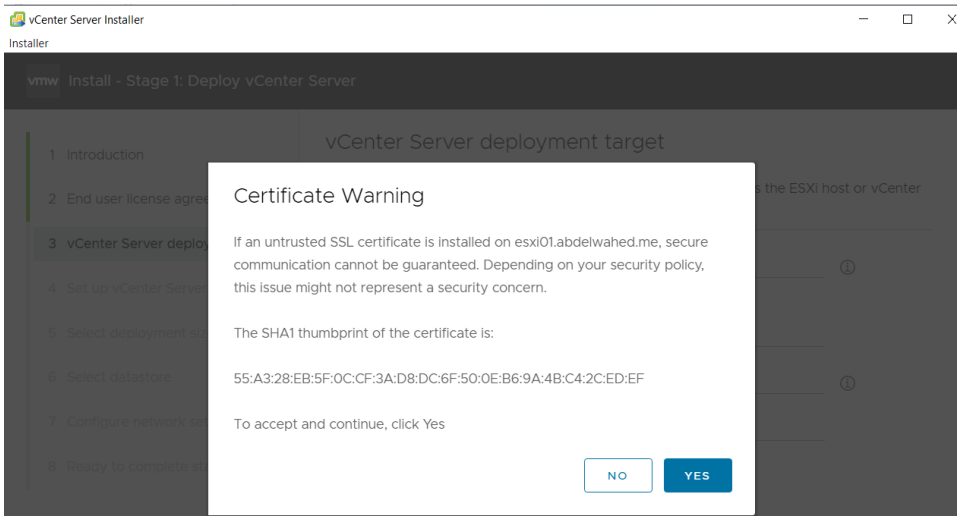
1. **Install**:
    - Install a new vCenter Server.
2. **Upgrade**:
    - Upgrade an existing vCenter Server Appliance or upgrade and converge an existing vCenter Server Appliance with an external Platform Services Controller.
3. **Migrate**:
    - Migrate from an existing Windows vCenter Server or migrate and converge an existing Windows vCenter Server with an external Platform Services Controller.
4. **Restore**:
    - Restore from a previous vCenter Server Backup.

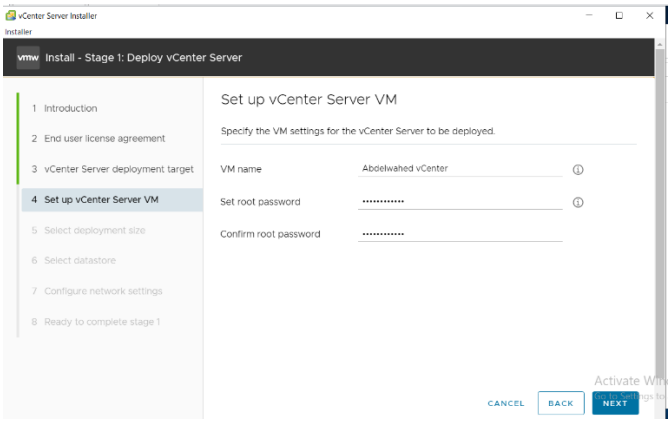


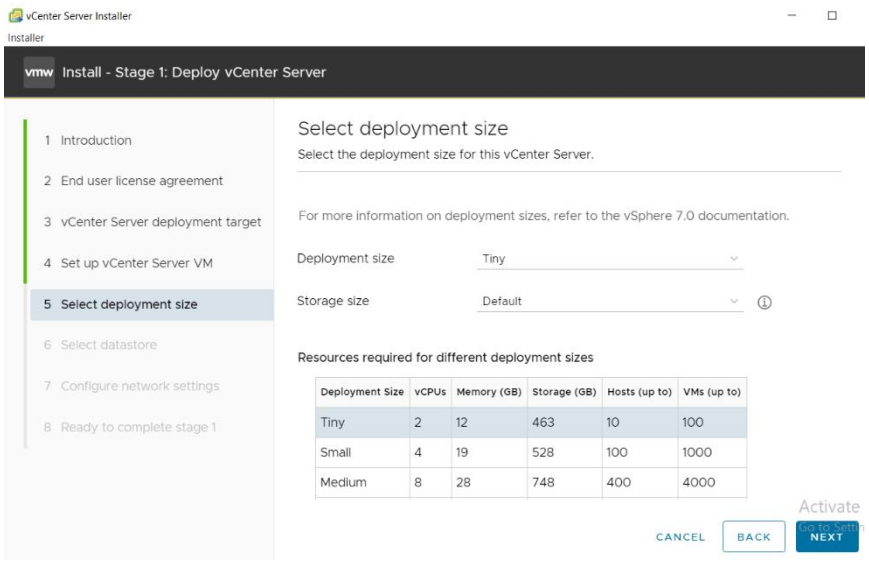


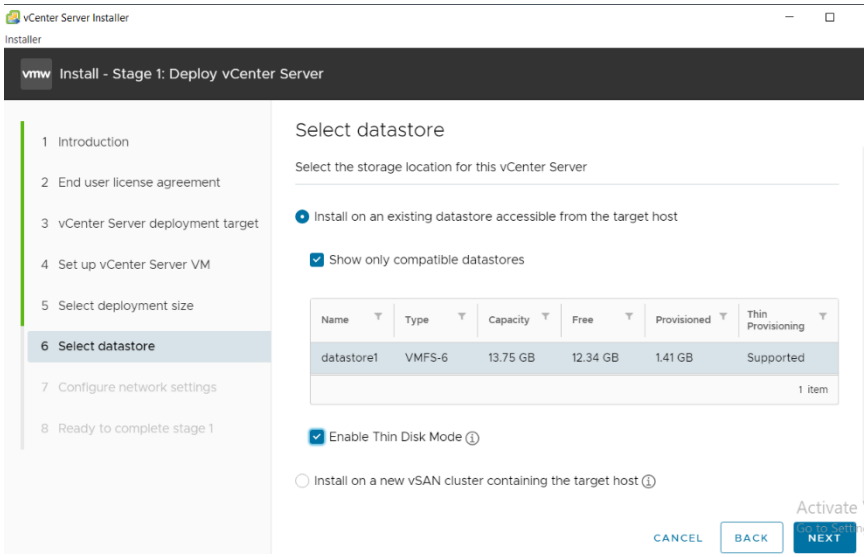

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
End user license agreement
Read and accept the following 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
I accept the terms of the license agreement.
CANCEL
BACK
NEXT

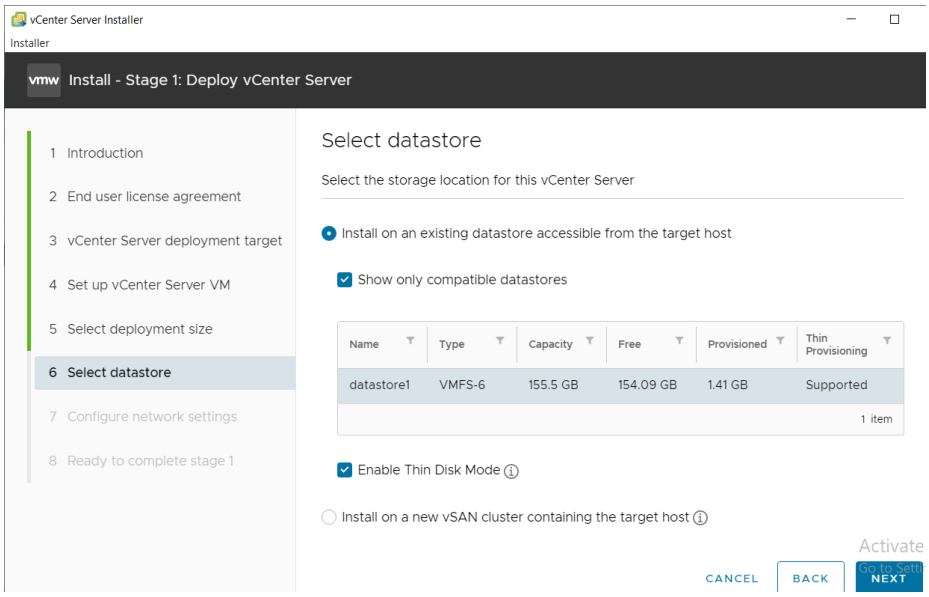

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
vCenter Server deployment target
Specify the vCenter Server deployment target settings. The target is the ESXi host or vCenter Server instance on which the vCenter Server will be deployed.
ESXi host or vCenter Server name
esxi01.abdelwahed.me
HTTPS port
443
User name
root
Password
CANCEL
BACK
NEXT

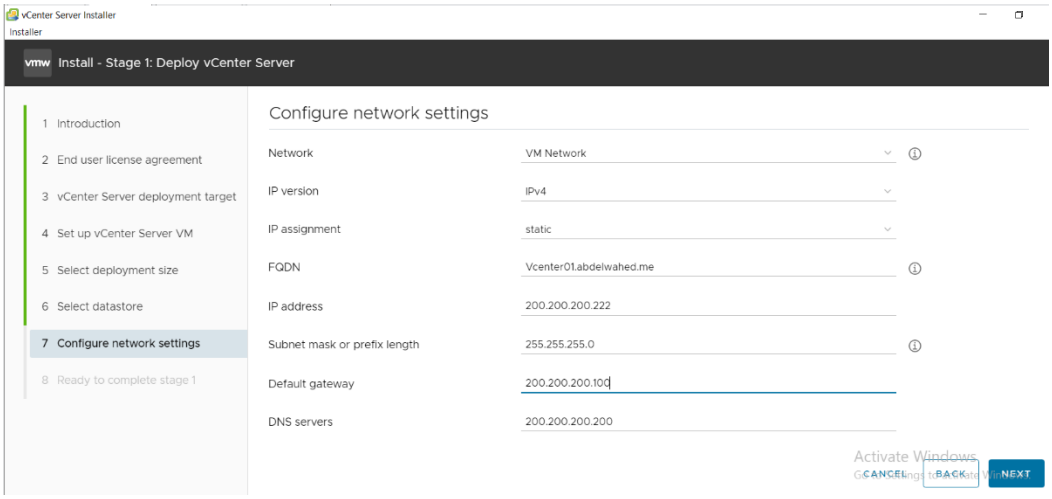

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
vCenter Server deployment target
Certificate Warning
If an untrusted SSL certificate is installed on esxi01.abdelwahed.me, secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern.
The SHA1 thumbprint of the certificate is:
55:A3:28:EB:5F:0C:CF:3A:D8:DC:6F:50:0E:B6:9A:4B:C4:2C:ED:EF
To accept and continue, click Yes
NO
YES

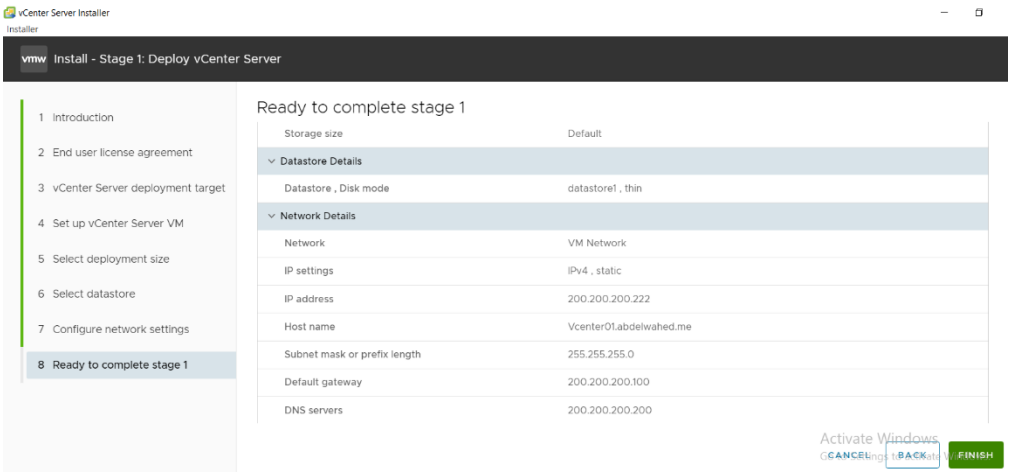

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Set up vCenter Server VM
Specify the VM settings for the vCenter Server to be deployed.
VM name
Abdelwahed vCenter
Set root password
Confirm root password
CANCEL
BACK
NEXT

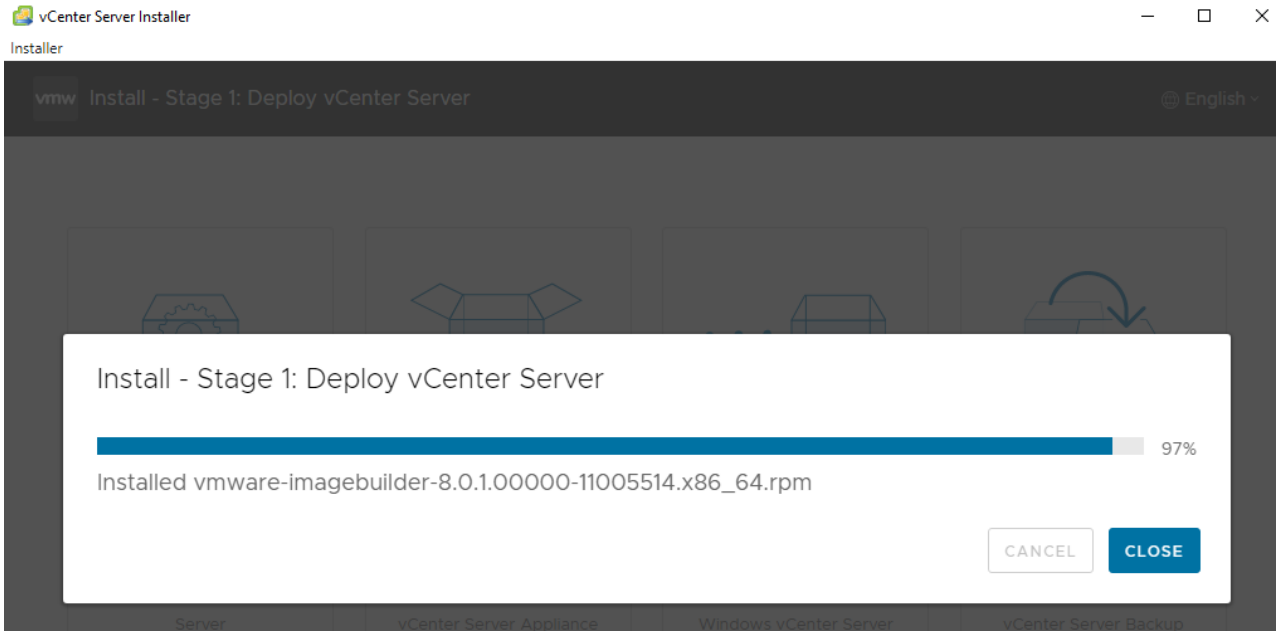

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Select deployment size
Select the deployment size for this vCenter Server.
For more information on deployment sizes, refer to the vSphere 7.0 documentation.
Deployment size
Tiny
Storage size
Default
Resources required for different deployment sizes
Deployment Size | vCPUs | Memory (GB) | Storage (GB) | Hosts (up to) | VMs (up to)
Tiny | 2 | 12 | 463 | 10 | 100
Small | 4 | 19 | 528 | 100 | 1000
Medium | 8 | 28 | 748 | 400 | 4000
CANCEL
BACK
NEXT

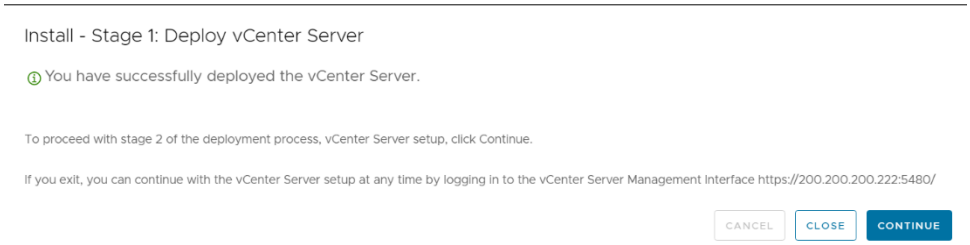

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Select datastore
Select the storage location for this vCenter Server
Install on an existing datastore accessible from the target host
Show only compatible datastores
Name | Type | Capacity | Free | Provisioned | Thin Provisioning
datastore1 | VMFS-6 | 13.75 GB | 12.34 GB | 1.41 GB | Supported
1 item
Enable Thin Disk Mode
Install on a new vSAN cluster containing the target host
CANCEL
BACK
NEXT

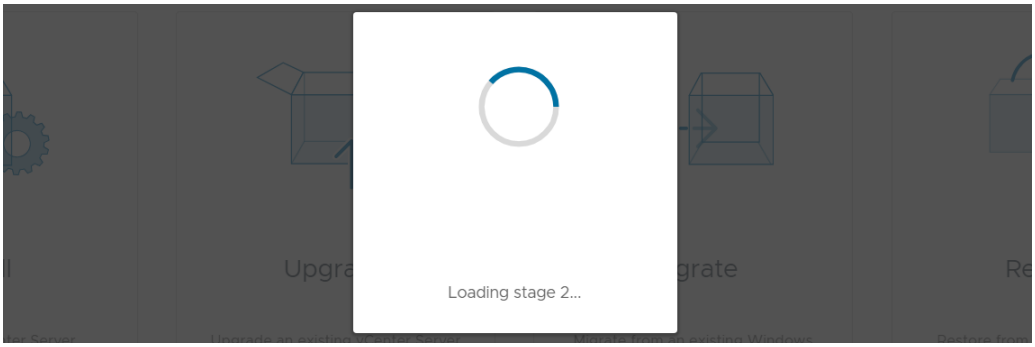

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Select datastore
Select the storage location for this vCenter Server
Install on an existing datastore accessible from the target host
Show only compatible datastores
Name
Type
Capacity
Free
Provisioned
Thin Provisioning
datastore1
VMFS-6
155.5 GB
154.09 GB
1.41 GB
Supported
1 item
Enable Thin Disk Mode
Install on a new vSAN cluster containing the target host
CANCEL
BACK
NEXT

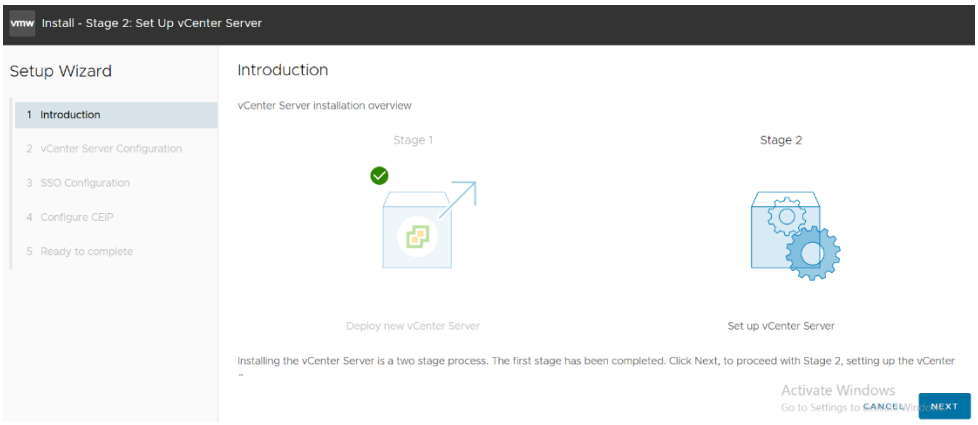

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Configure network settings
Network
VM Network
IP version
IPv4
IP assignment
static
FQDN
Vcenter01.abdelwahed.me
IP address
200.200.200.222
Subnet mask or prefix length
255.255.255.0
Default gateway
200.200.200.100
DNS servers
200.200.200.200
CANCEL
BACK
NEXT

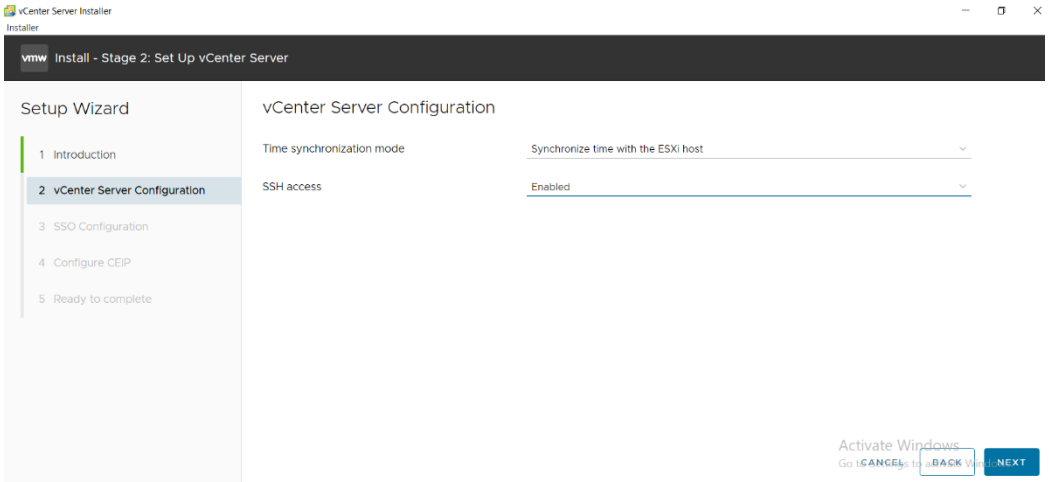

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 vCenter Server deployment target
4 Set up vCenter Server VM
5 Select deployment size
6 Select datastore
7 Configure network settings
8 Ready to complete stage 1
Ready to complete stage 1
Storage size
Default
Datastore Details
Datastore , Disk mode
datastore1 , thin
Network Details
Network
VM Network
IP settings
IPv4 , static
IP address
200.200.200.222
Host name
Vcenter01.abdelwahed.me
Subnet mask or prefix length
255.255.255.0
Default gateway
200.200.200.100
DNS servers
200.200.200.200
CANCEL
BACK
FINISH

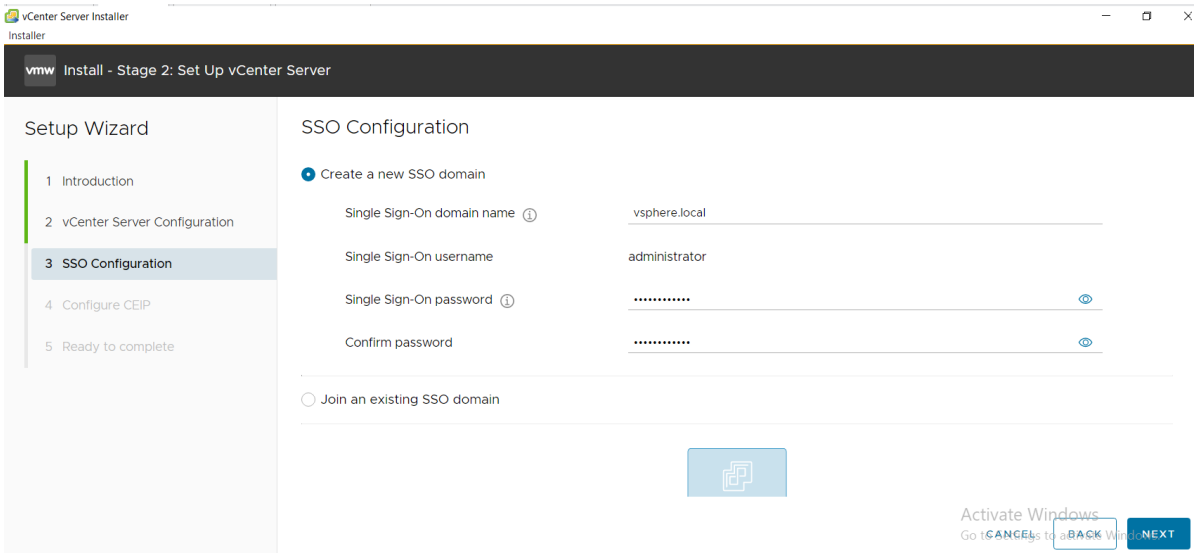

vCenter Server Installer
Installer
Install - Stage 1: Deploy vCenter Server
English
Install - Stage 1: Deploy vCenter Server
97%
Installed vmware-imagebuilder-8.0.1.00000-11005514.x86_64.rpm
CANCEL
CLOSE
Server
vCenter Server Appliance
Windows vCenter Server
vCenter Server Backup

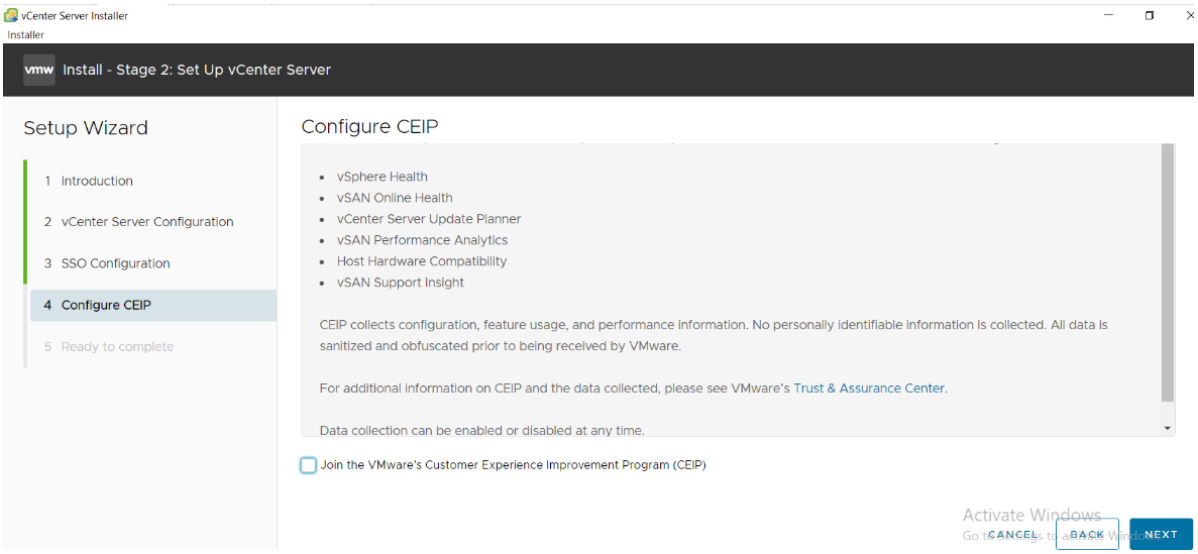

Install - Stage 1: Deploy vCenter Server
You have successfully deployed the vCenter Server.
To proceed with stage 2 of the deployment process, vCenter Server setup, click Continue.
If you exit, you can continue with the vCenter Server setup at any time by logging in to the vCenter Server Management Interface https://200.200.200.222:5480/
CANCEL
CLOSE
CONTINUE

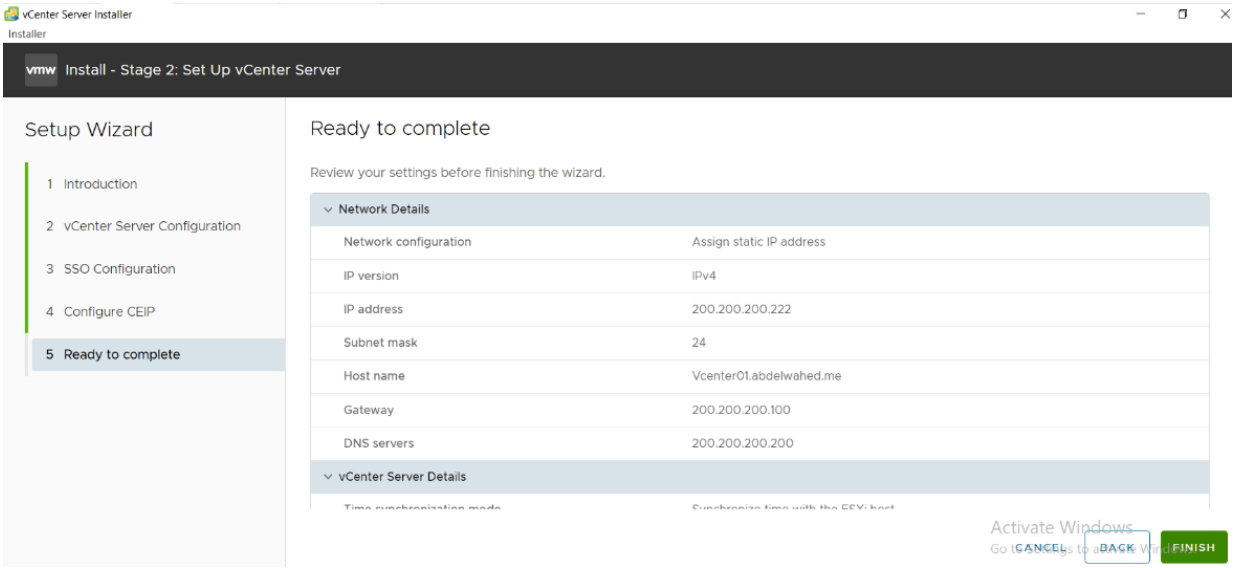

Loading stage 2...

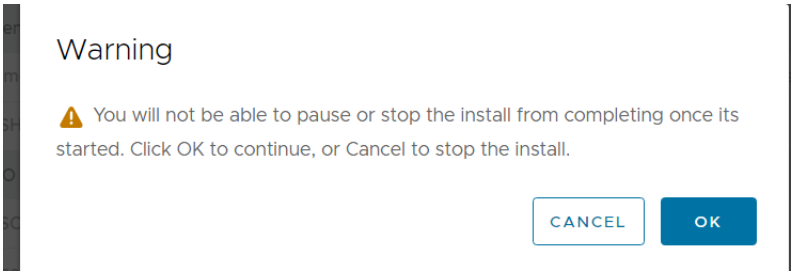

Install - Stage 2: Set Up vCenter Server
Setup Wizard
1 Introduction
2 vCenter Server Configuration
3 SSO Configuration
4 Configure CEIP
5 Ready to complete
Introduction
vCenter Server installation overview
Stage 1
Stage 2
Deploy new vCenter Server
Set up vCenter Server
Installing the vCenter Server is a two stage process. The first stage has been completed. Click Next, to proceed with Stage 2, setting up the vCenter
Activate Windows
CANCEL
NEXT


vCenter Server Installer
Installer
Install - Stage 2: Set Up vCenter Server
Setup Wizard
1 Introduction
2 vCenter Server Configuration
3 SSO Configuration
4 Configure CEIP
5 Ready to complete
vCenter Server Configuration
Time synchronization mode
Synchronize time with the ESXi host
SSH access
Enabled
Activate Windows
CANCEL
BACK
NEXT

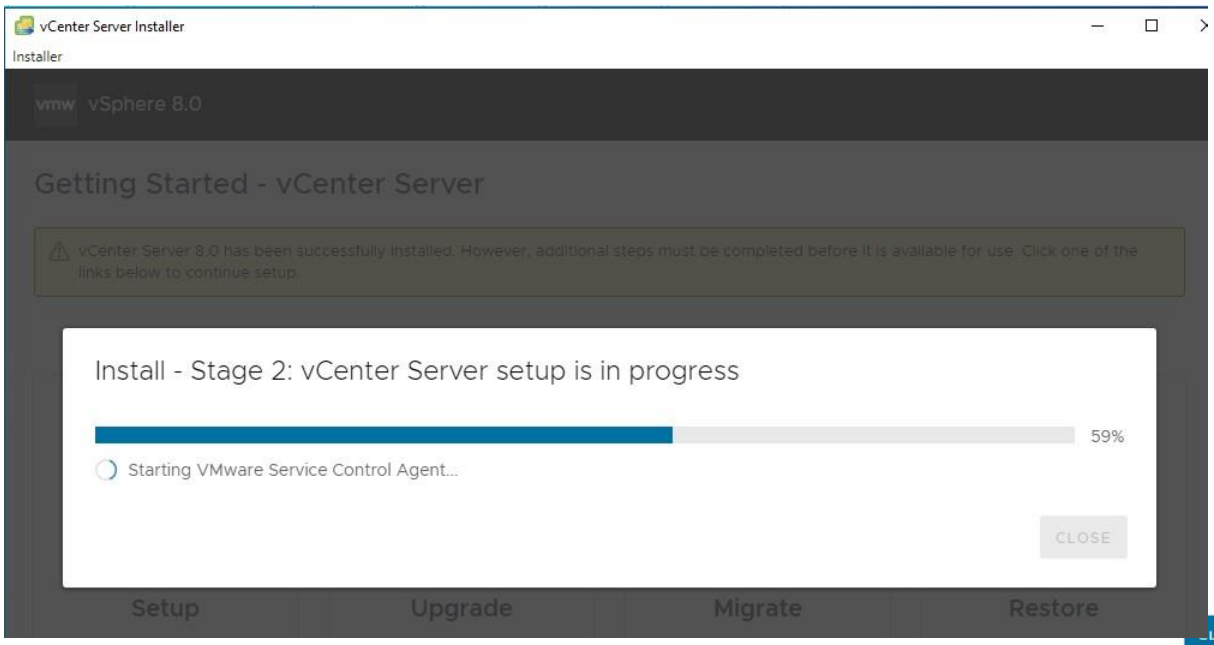

vCenter Server Installer
Installer
Install - Stage 2: Set Up vCenter Server
Setup Wizard
1 Introduction
2 vCenter Server Configuration
3 SSO Configuration
4 Configure CEIP
5 Ready to complete
SSO Configuration
Create a new SSO domain
Single Sign-On domain name
vsphere.local
Single Sign-On username
administrator
Single Sign-On password
Confirm password
Join an existing SSO domain
Activate Windows
CANCEL
BACK
NEXT

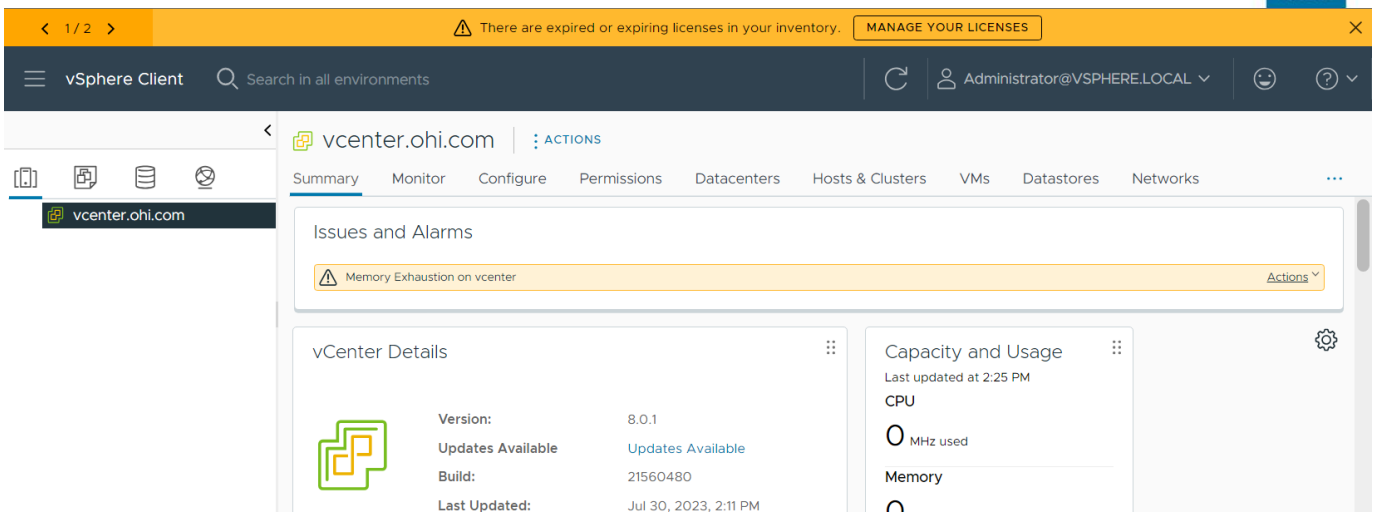

vCenter Server Installer
Installer
Install - Stage 2: Set Up vCenter Server
Setup Wizard
1 Introduction
2 vCenter Server Configuration
3 SSO Configuration
4 Configure CEIP
5 Ready to complete
Configure CEIP
vSphere Health
vSAN Online Health
vCenter Server Update Planner
vSAN Performance Analytics
Host Hardware Compatibility
vSAN Support Insight
CEIP collects configuration, feature usage, and performance information. No personally identifiable information is collected. All data is sanitized and obfuscated prior to being received by VMware.
For additional information on CEIP and the data collected, please see VMware's Trust & Assurance Center.
Data collection can be enabled or disabled at any time.
Join the VMware's Customer Experience Improvement Program (CEIP)
Activate Windows
CANCEL
BACK
NEXT

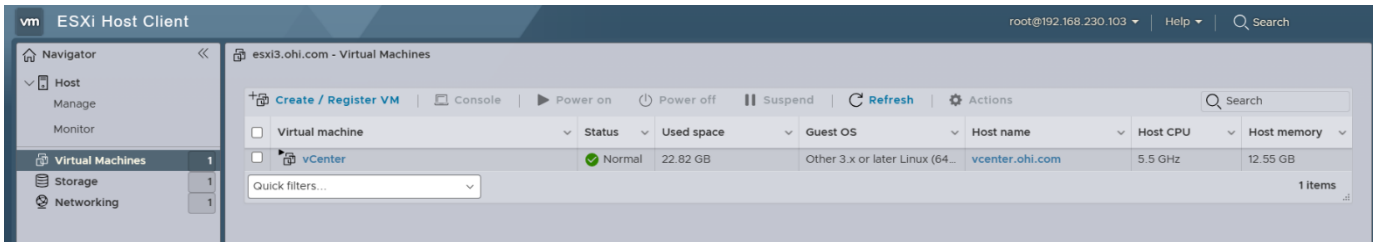

vCenter Server Installer
Installer
Install - Stage 2: Set Up vCenter Server
Setup Wizard
1 Introduction
2 vCenter Server Configuration
3 SSO Configuration
4 Configure CEIP
5 Ready to complete
Ready to complete
Review your settings before finishing the wizard.
Network Details
Network configuration
Assign static IP address
IP version
IPv4
IP address
200.200.200.222
Subnet mask
24
Host name
Vcenter01.abdelwahed.me
Gateway
200.200.200.100
DNS servers
200.200.200.200
vCenter Server Details
Activate Windows
CANCEL
BACK
FINISH


Warning
You will not be able to pause or stop the install from completing once its started. Click OK to continue, or Cancel to stop the install.
CANCEL
OK

VMware vSphere Install, Configure, Manage | Lab Guide



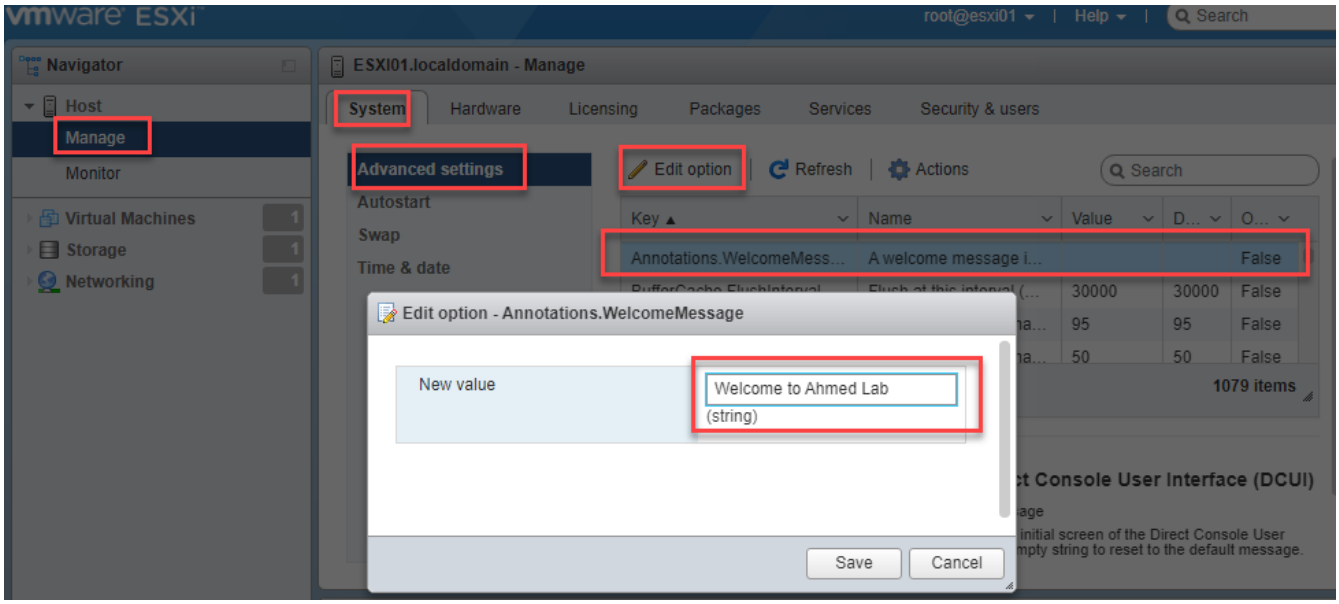




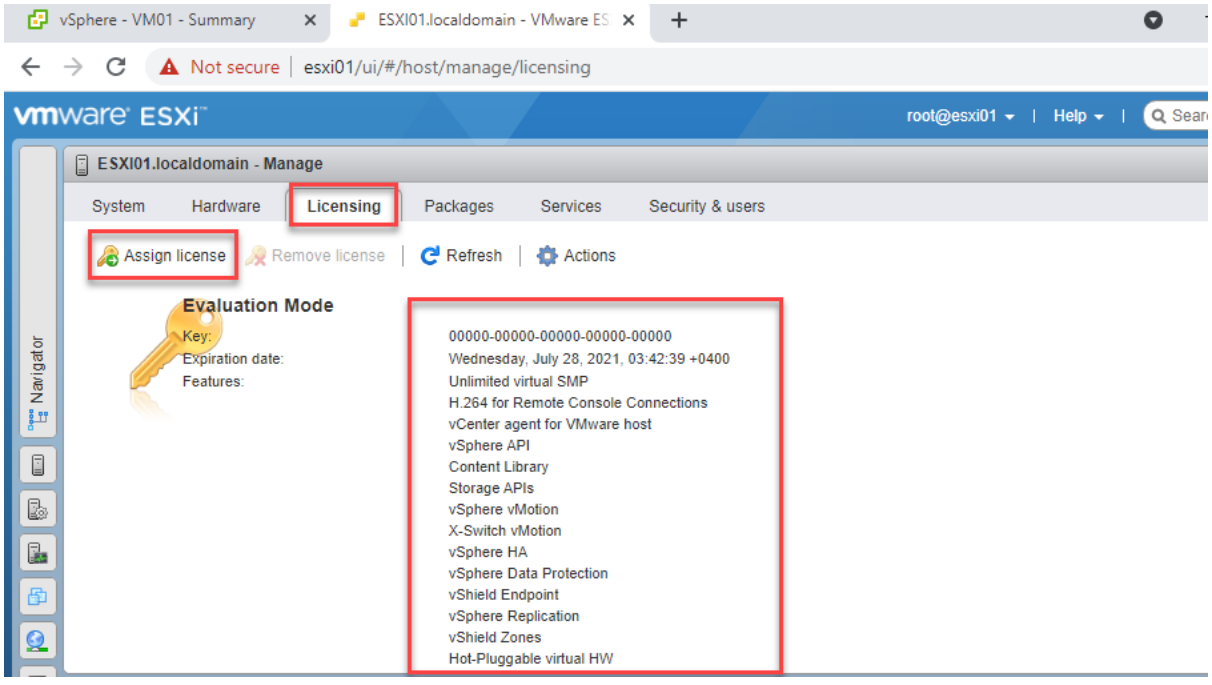
Prior to installing vCenter, it's crucial to create DNS A and PTR records for the server to ensure that other systems can identify the vCenter's hostname and IP, which is essential for seamless interaction within the vSphere infrastructure.

Configuring and managing using ESXi host.

Add a welcome message and assign license

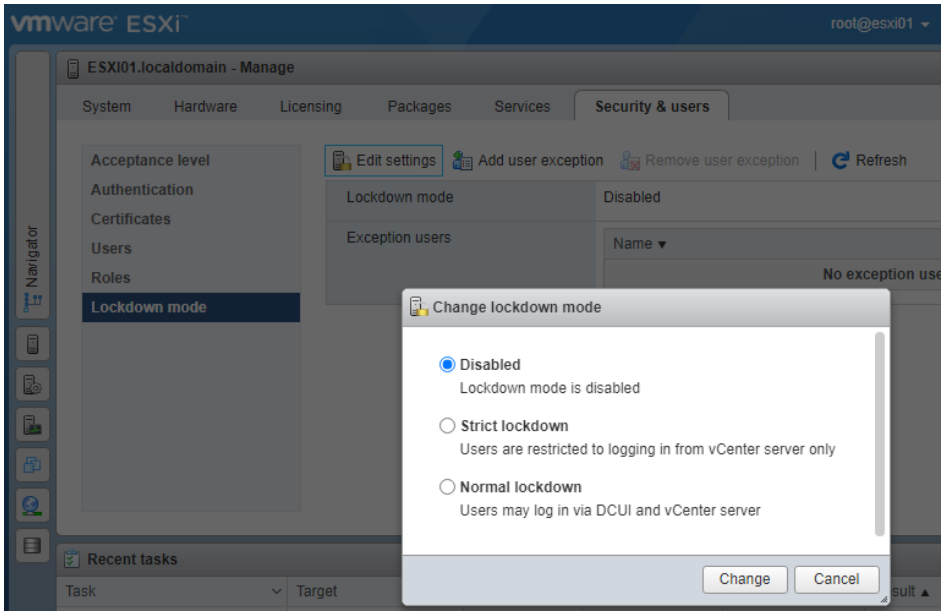


- Based on the license you assign, additional features will be added.
- A trial license is available and works for 60 days, during the trial period, all features are fully functional.



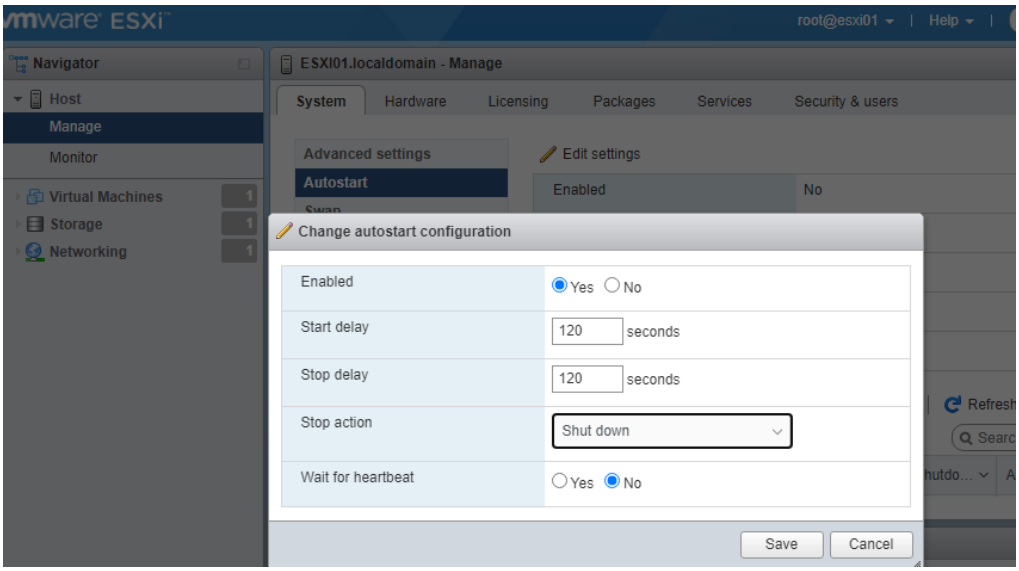
Lockdown Mode and Auto Restart Option

- **Purpose**: Lockdown mode is a security feature in ESXi that restricts access to the host to prevent unauthorized changes to its configuration.
- **Functionality**:
  - When Lockdown mode is enabled, only the vCenter Server system and the local DCUI (Direct Console User Interface) can perform operations on the host.
  - All other access to the host, including SSH, console, and vSphere Web Client, is blocked.



Auto Restart Option:

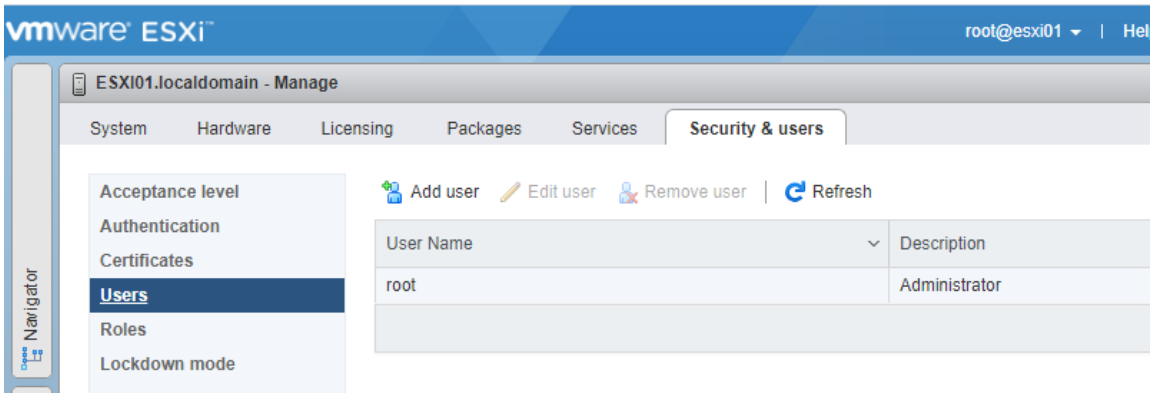
- The Auto Restart option allows virtual machines (VMs) to automatically restart if the ESXi host they are running on is restarted or fails. This ensures that critical VMs are brought back online without manual intervention, enhancing the availability and resilience of the virtual environment.

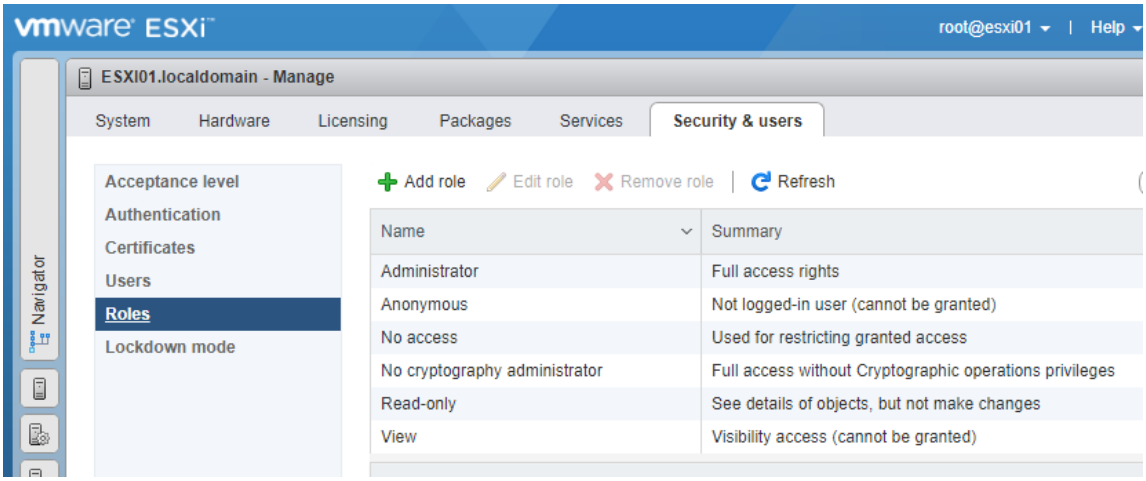


Adding Local Users to ESXi Host

ESXi hosts have the ability to create and manage local user accounts. Local user accounts can be used to allow users to log in to the ESXi host using the vSphere Web Client, vSphere Client, or SSH. Once you have added local user accounts to the ESXi host, users can log in to the host using their username and password. Local user accounts have a limited set of privileges, which can be modified using the vSphere Web Client or vSphere Client.

Steps to Add Local Users to ESXi Host





Add and Manage Datastore

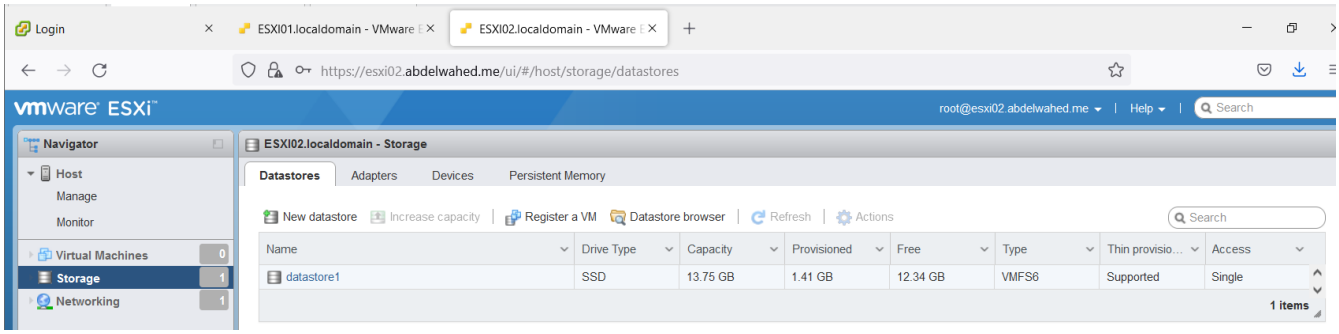
A datastore is a storage location in vSphere where you can store virtual machine files, ISO images, templates, and other files. Adding and managing datastores in vSphere is an important part of managing your virtual infrastructure.

Steps to Add and Manage a Datastore in vSphere

1. **Add a Datastore**:
    - To add a datastore, go to the host or cluster that you want to add the datastore to in the vSphere Web Client or vSphere Client, and click the Storage tab.
    - Click the "Add Datastore" button and select the type of datastore that you want to add, such as NFS, iSCSI, or VMFS.
    - Follow the prompts to configure the settings for the datastore, such as the datastore name, capacity, and storage location.
2. **Manage a Datastore**:
    - After adding a datastore, you can manage it by performing various tasks, such as formatting, extending, and deleting the datastore.
        - **Format a Datastore**: Go to the host or cluster that the datastore is attached to, select the datastore in the Storage tab, and click the "Format Datastore" button.
        - **Extend a Datastore:** Select the datastore and click the "Extend Datastore" button, and follow the prompts to add more storage capacity.
        - **Delete a Datastore**: Select the datastore and click the "Delete Datastore" button, and follow the prompts to confirm the deletion.
3. **Monitor a Datastore**:
    - You can also monitor the performance and usage of a datastore in vSphere.
    - To do this, go to the host or cluster that the datastore is attached to, select the datastore in the Storage tab, and click the "Monitor" tab.
    - Here, you can view charts and statistics for the datastore, such as the amount of free space, the number of virtual machines using the datastore, and the amount of read and write activity.

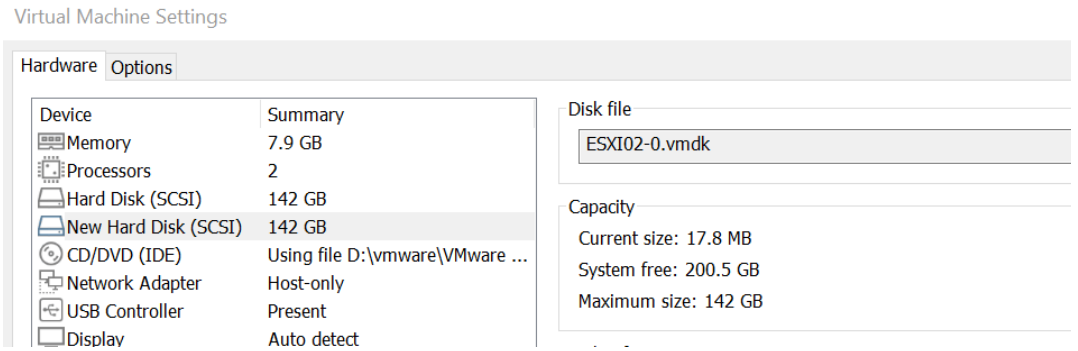
Storage Allocation for ESXi Hosts

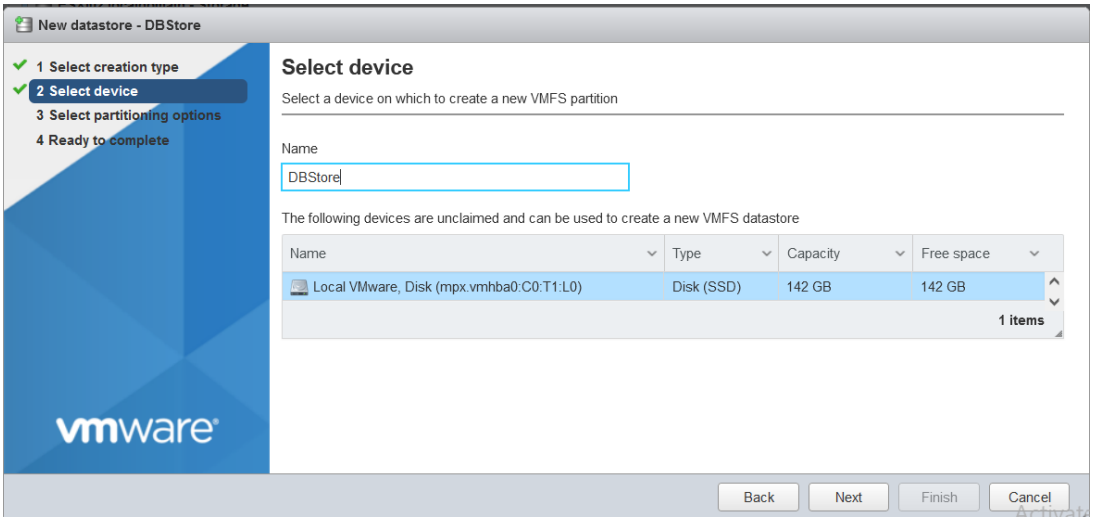
Both servers book around 8GB for the OS, and the rest of the hard disk space is allocated for datastores to save any kind of data, including VM data and OS ISO files.

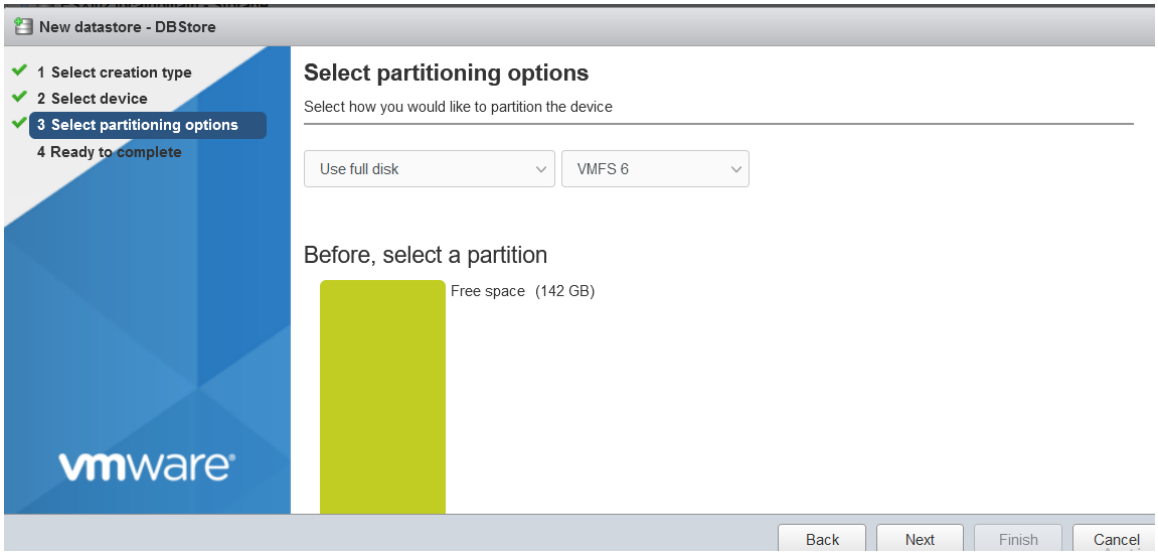


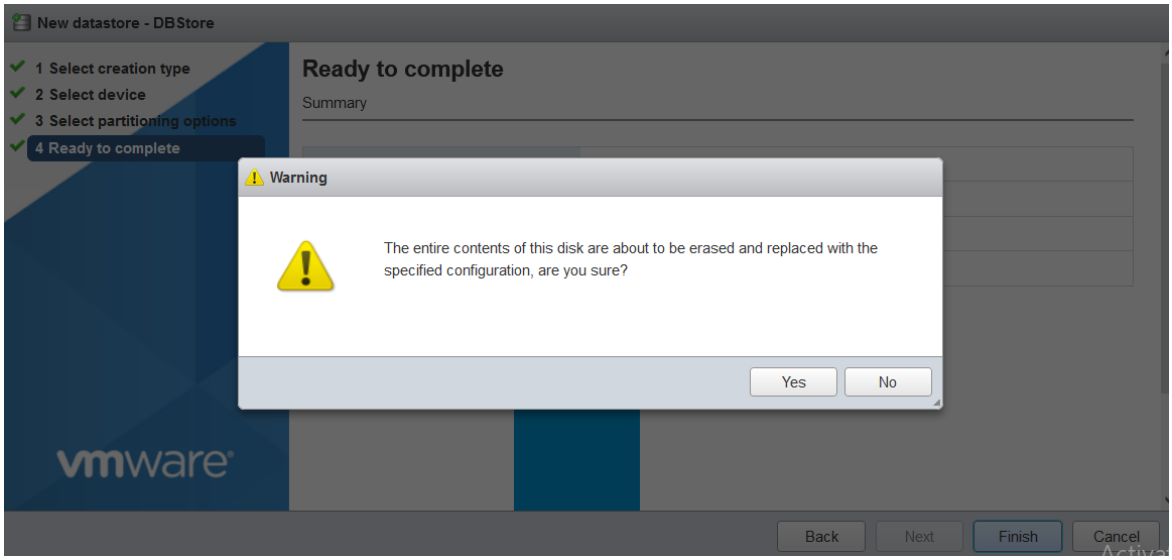
Create new local datastore (VMFS) using ESXi

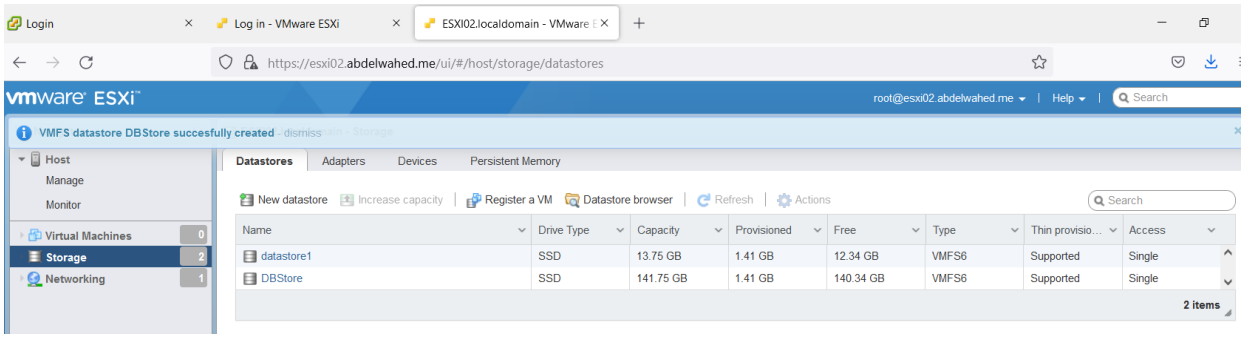
To establish a new local datastore (VMFS) using ESXi, first, you need to install a new hard drive on the server. Afterward, either reboot the ESXi server or perform a storage rescan without restarting by utilizing vCenter. Simply right-click on the ESXi server, select 'storage', and choose 'rescan'. Then proceed as follows:





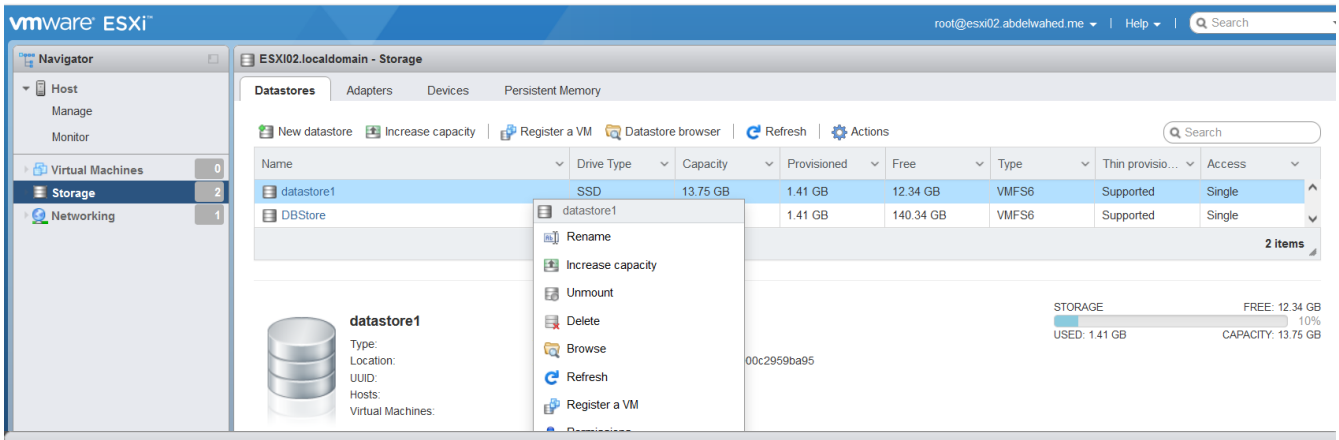


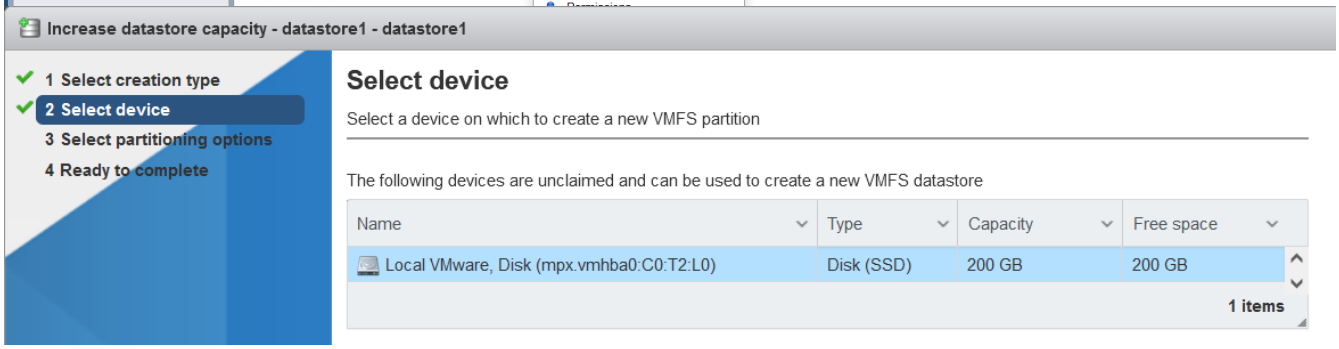

New datastore - DBStore
1 Select creation type
2 Select device
3 Select partitioning options
4 Ready to complete
Ready to complete
Summary
Warning
The entire contents of this disk are about to be erased and replaced with the specified configuration, are you sure?
Yes
No
vmware
Back
Next
Finish
Cancel

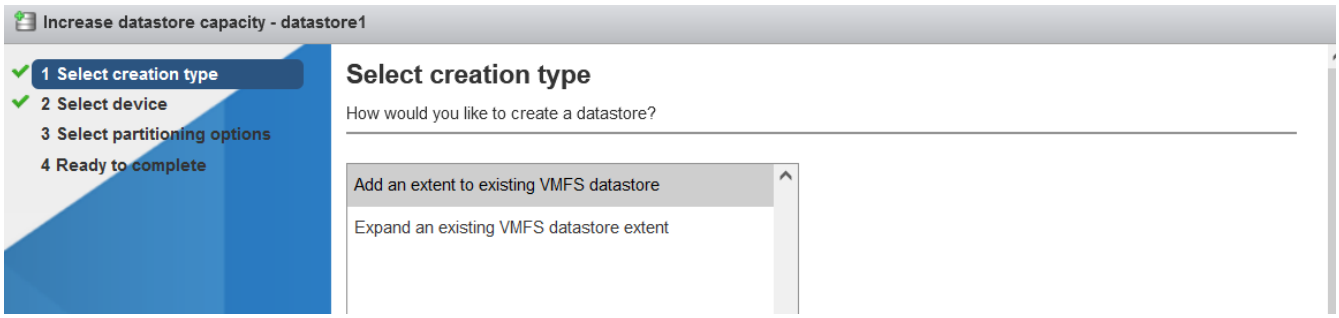

Login
Log in - VMware ESXi
ESXI02.localdomain - VMware
https://esxi02.abdelwahed.me/ui/#/host/storage/datastores
vmware ESXi
root@esxi02.abdelwahed.me
Help
Search
VMFS datastore DBStore succesfully created
dismiss
Host
Manage
Monitor
Virtual Machines
Storage
Networking
Datastores
Adapters
Devices
Persistent Memory
New datastore
Increase capacity
Register a VM
Datastore browser
Refresh
Actions
Name
Drive Type
Capacity
Provisioned
Free
Type
Thin provisio...
Access
datastore1
SSD
13.75 GB
1.41 GB
12.34 GB
VMFS6
Supported
Single
DBStore
SSD
141.75 GB
1.41 GB
140.34 GB
VMFS6
Supported
Single
2 items

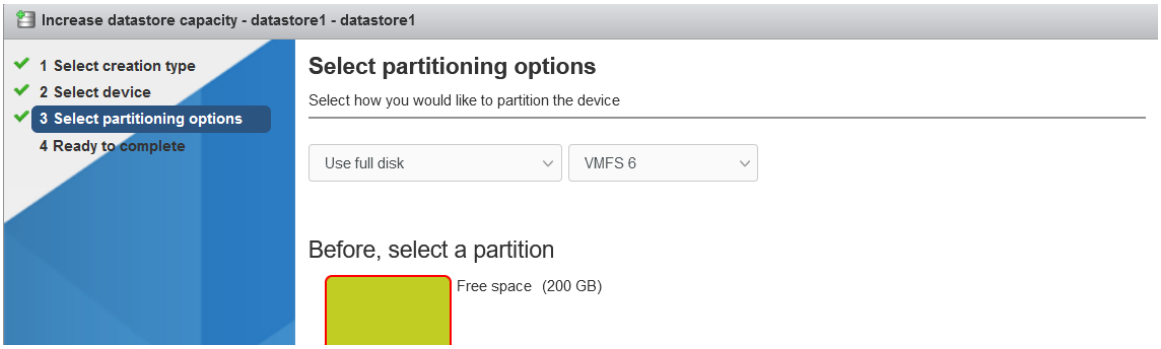
Extend Existing Datastore

To extend an existing datastore, follow these steps. In this example, we will add a 200GB hard disk to extend datastore1. Note that you may need to restart the server for the new hard disk to be recognized, or you can rescan the storage without restarting.

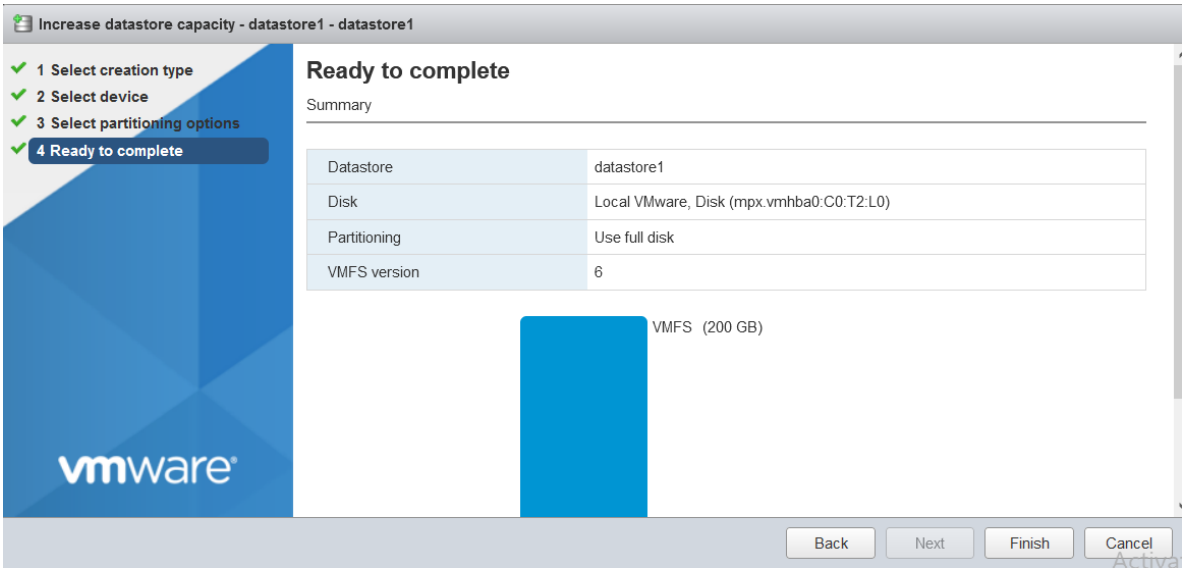


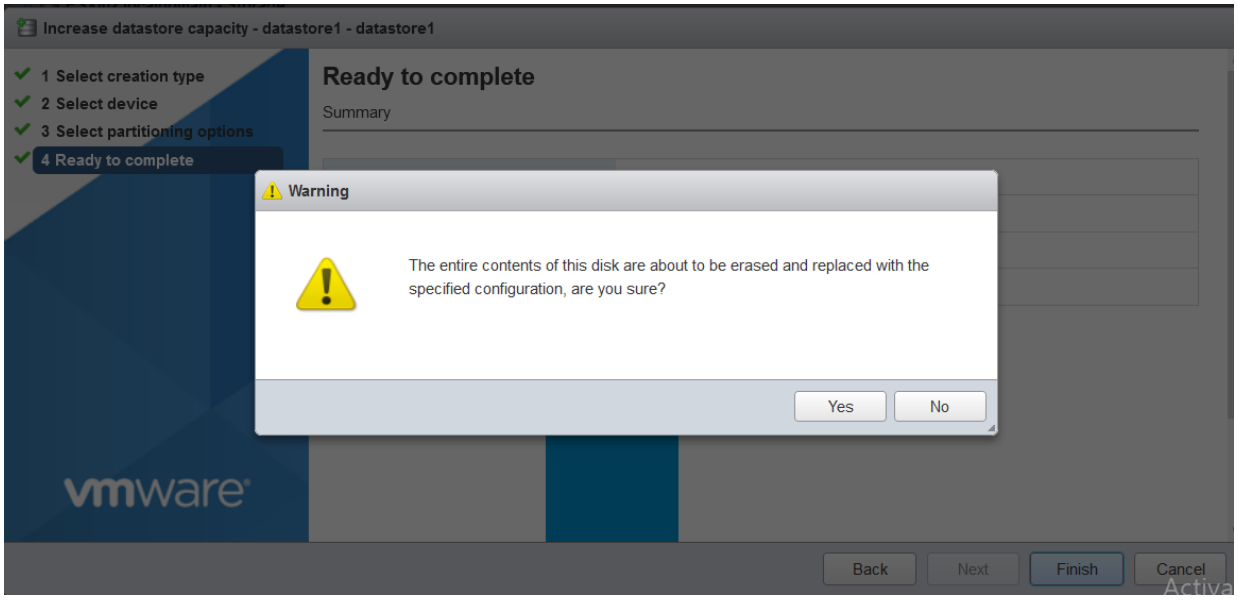


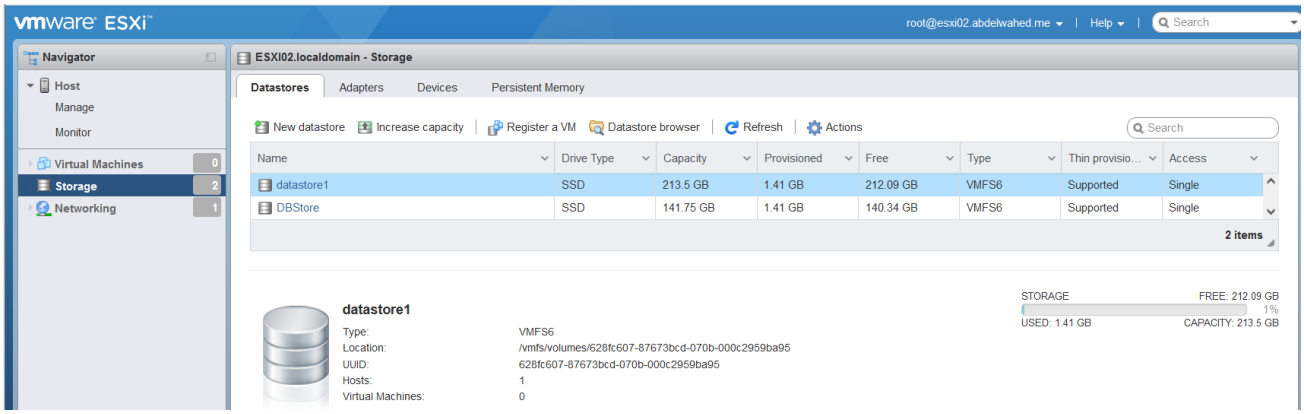




VMware vSphere Install, Configure, Manage | Lab Guide

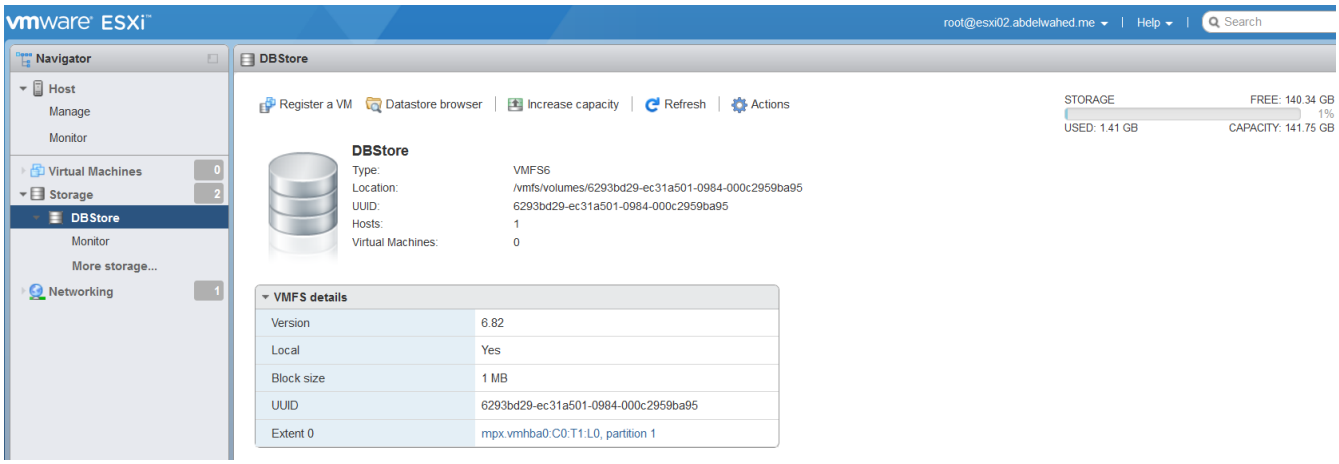


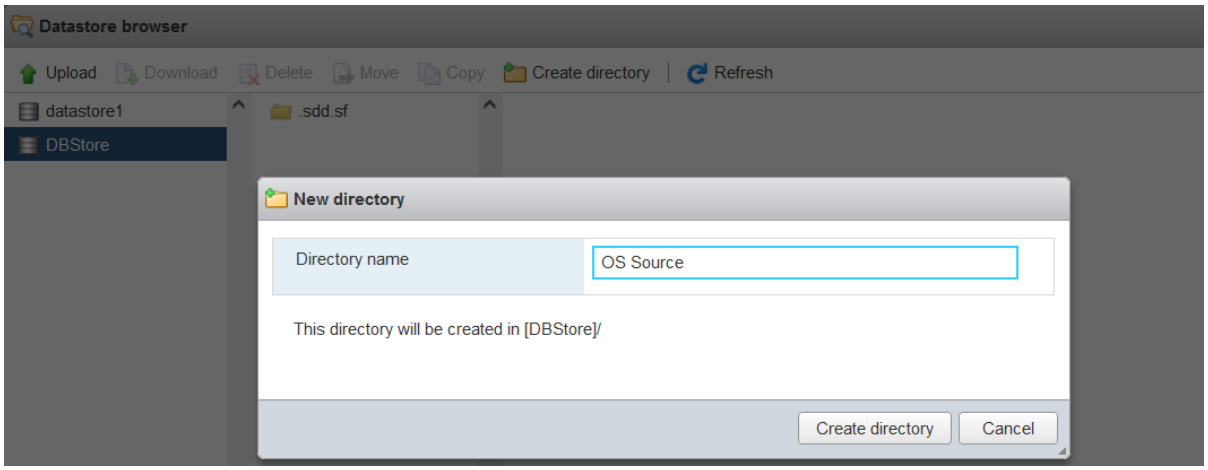




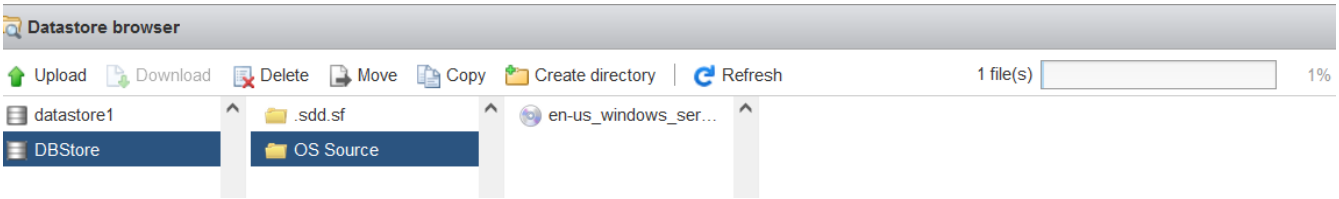
Upload the ISO file to the datastore.

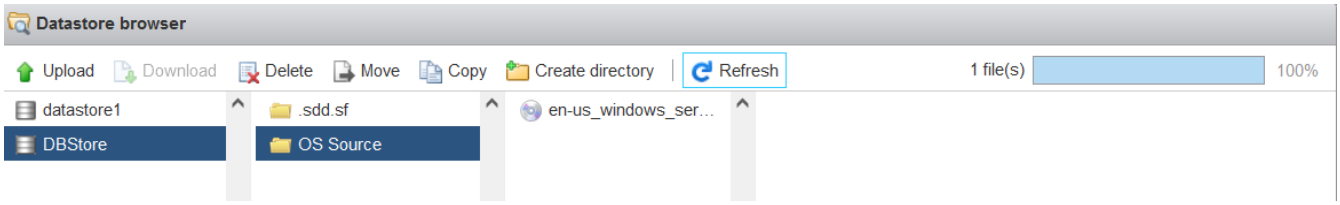
Begin by navigating to that store.





Next, transfer the ISO file to the **OS Source** directory.



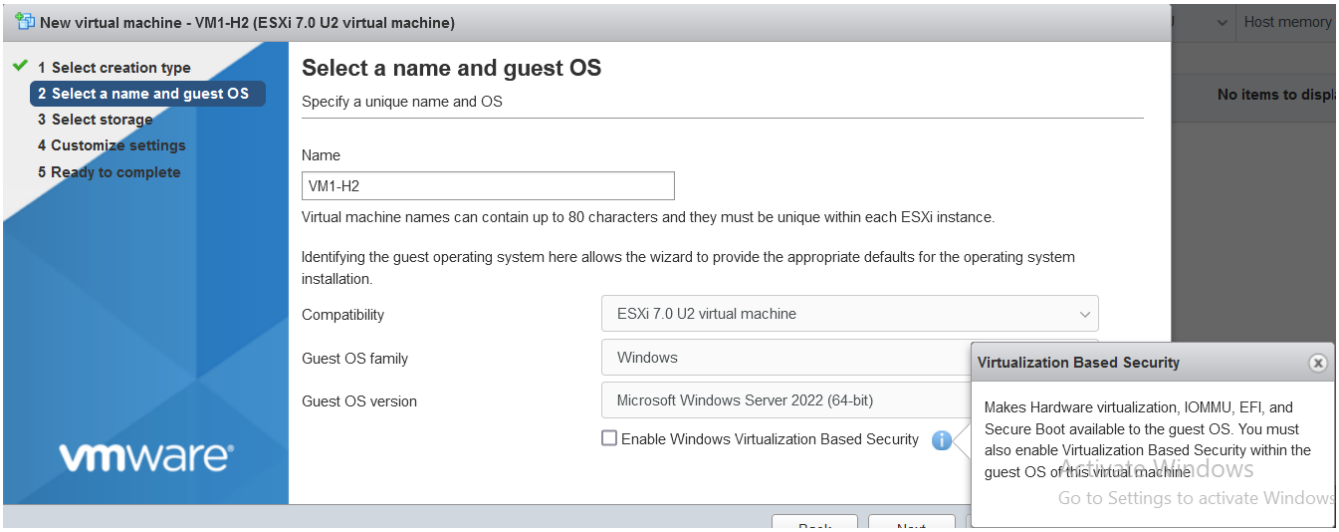


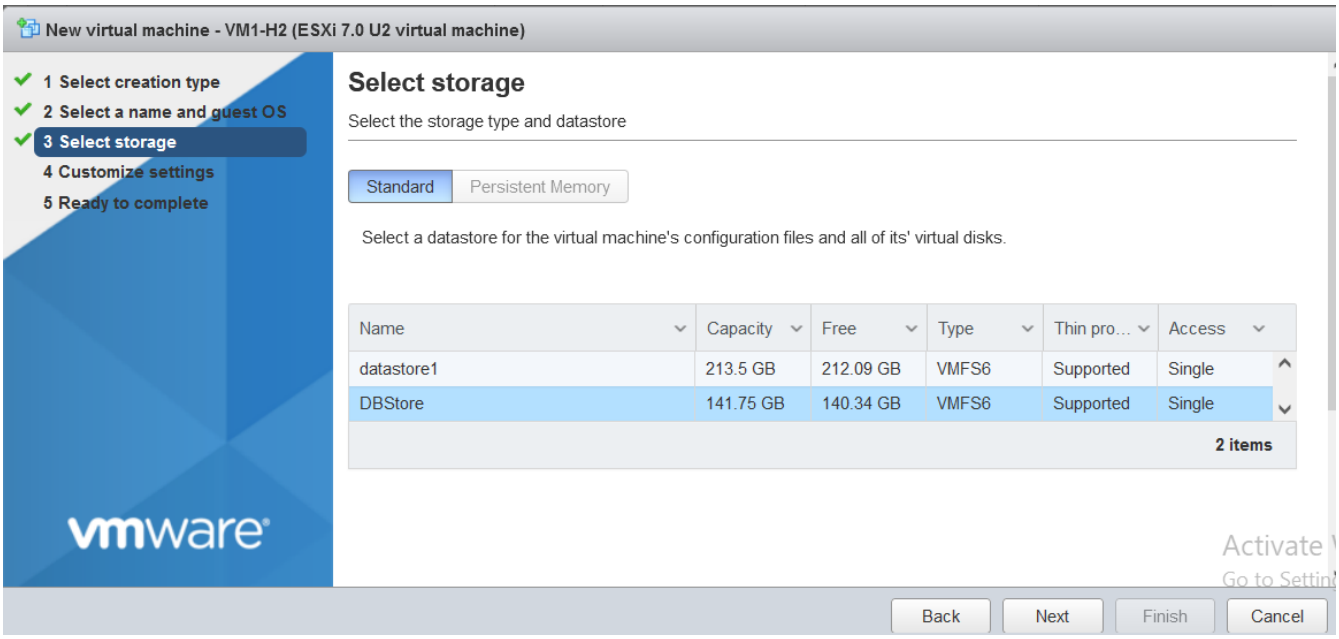
Create and configure VM through ESXi02 host

To create and configure a virtual machine (VM) through ESXi02 host, follow these steps:

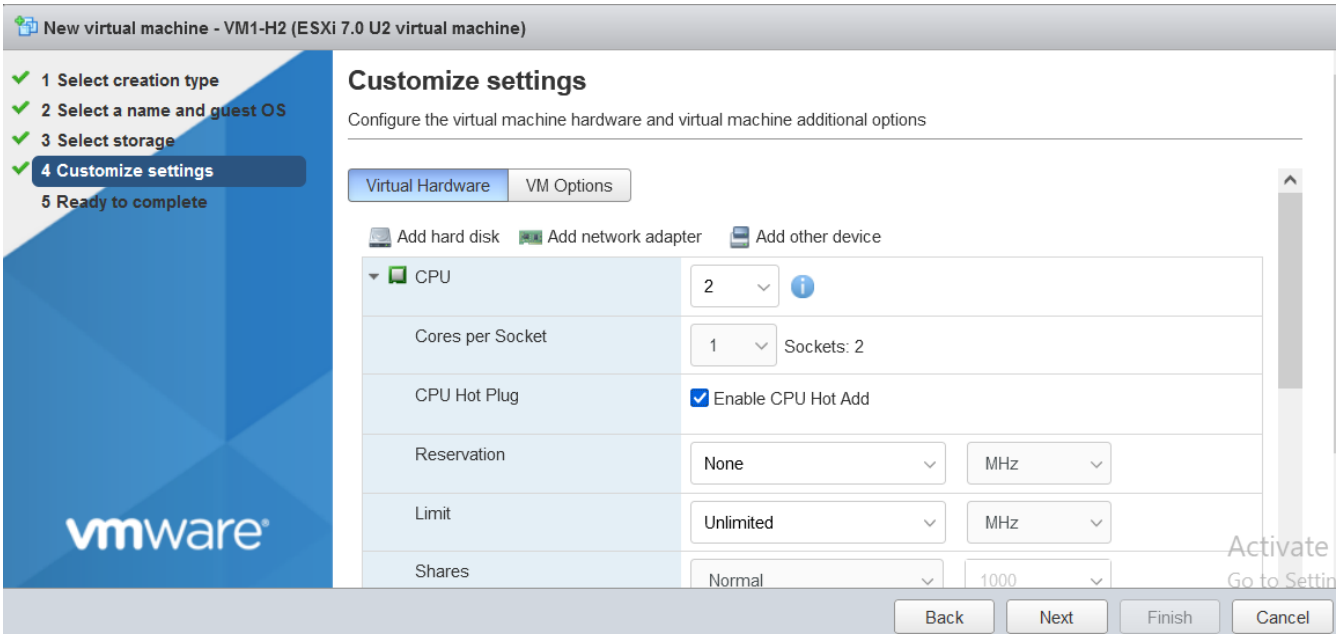
1. Log in to the vSphere Web Client or vSphere Client using the credentials for the ESXi02 host.
2. Select the ESXi02 host from the inventory and go to the Virtual Machines tab.
3. Click the Create/Register VM button to create a new virtual machine.
4. In the New Virtual Machine wizard, select the type of VM that you want to create, such as a typical VM or a custom VM.
5. Follow the prompts to configure the settings for the VM, such as the VM name, guest operating system, virtual hardware, and storage.
6. After the VM is created, select it in the inventory and go to the Configure tab to configure additional settings.
7. Configure the VM settings as appropriate for your environment, such as the network adapter, storage adapter, CPU and memory allocation, and advanced settings.
8. Power on the VM to begin using it.
9. To access the console of the VM, select the VM in the inventory and go to the Console tab.
10. Use the console to install the guest operating system, install applications, and configure the VM as needed.

Creating a Virtual Machine in ESXi

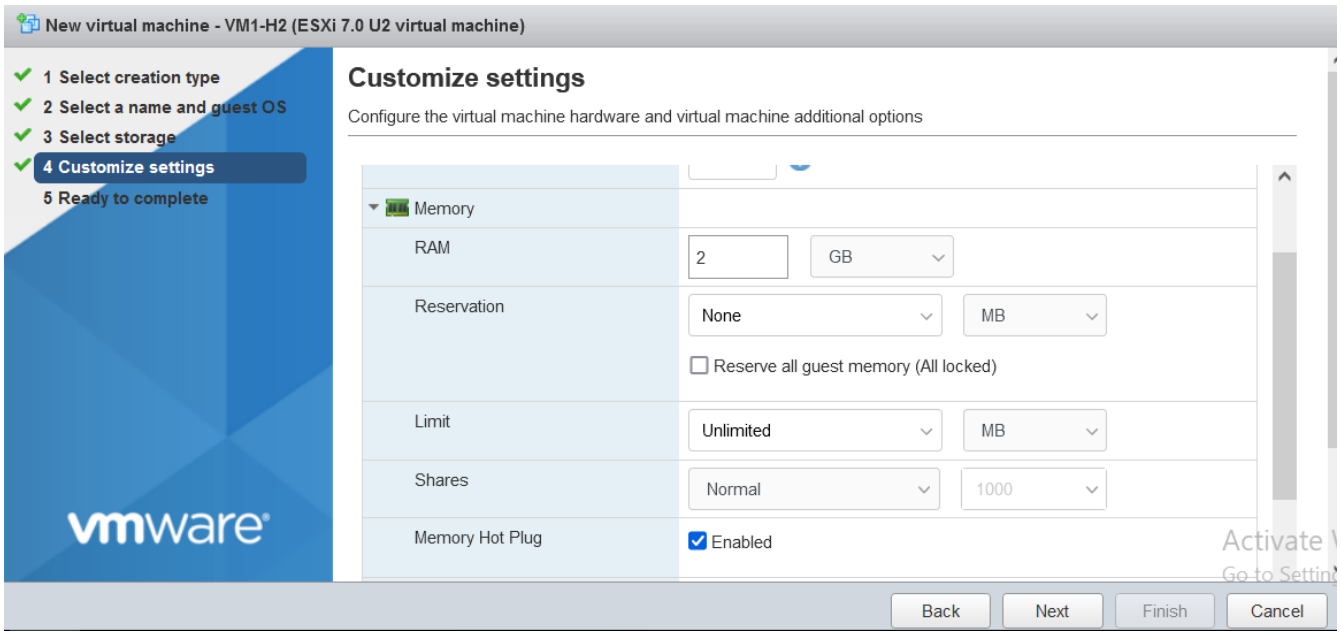




Choose CPU Settings



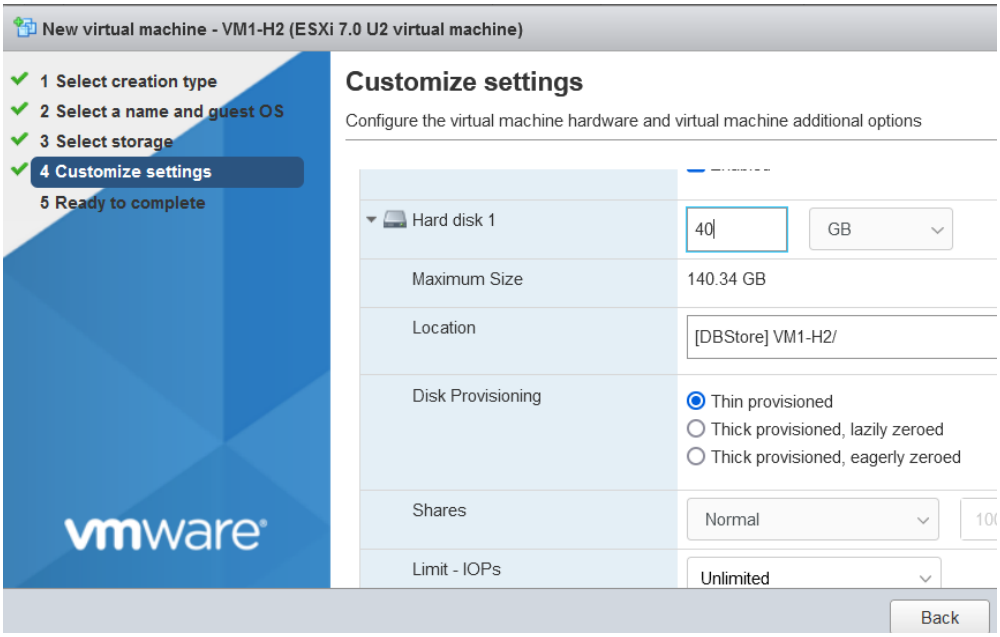
Choose memory configurations.



Options for Hard Disk Storage

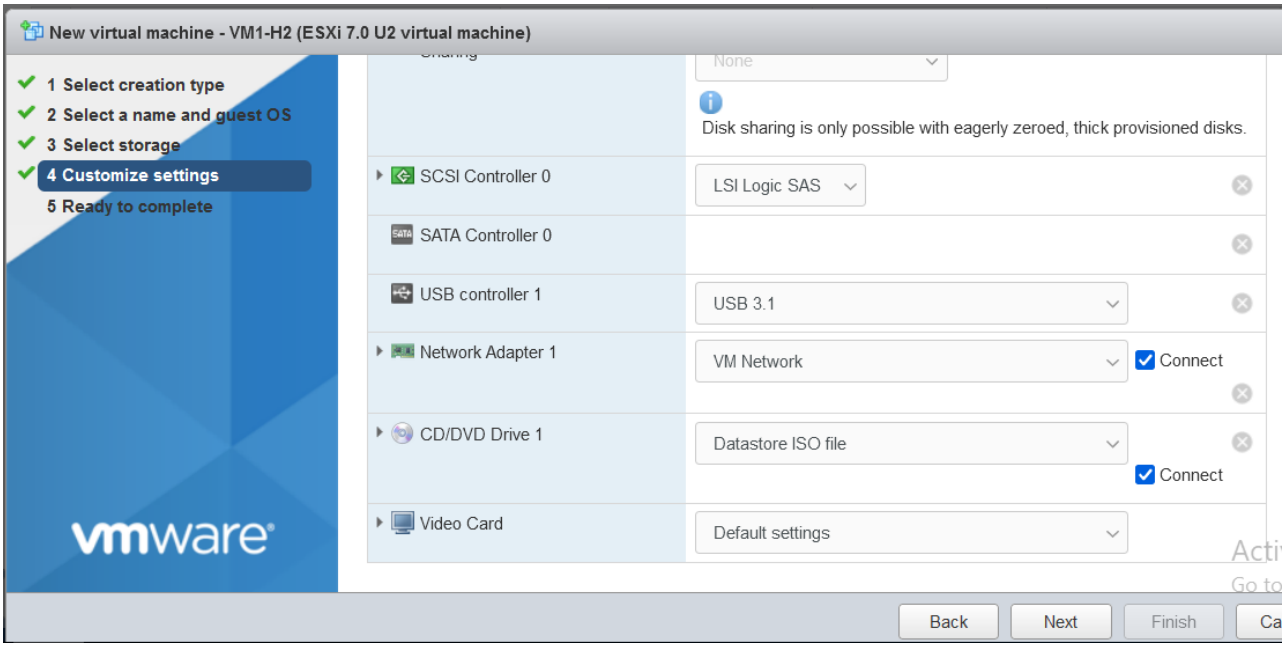
Disk Provisioning: Options include:

- **Thin Provisioned**: Selected option, which allocates storage space as needed.
- **Thick Provisioned, Lazily Zeroed:** Allocates storage space immediately but zeros out blocks as they are written.

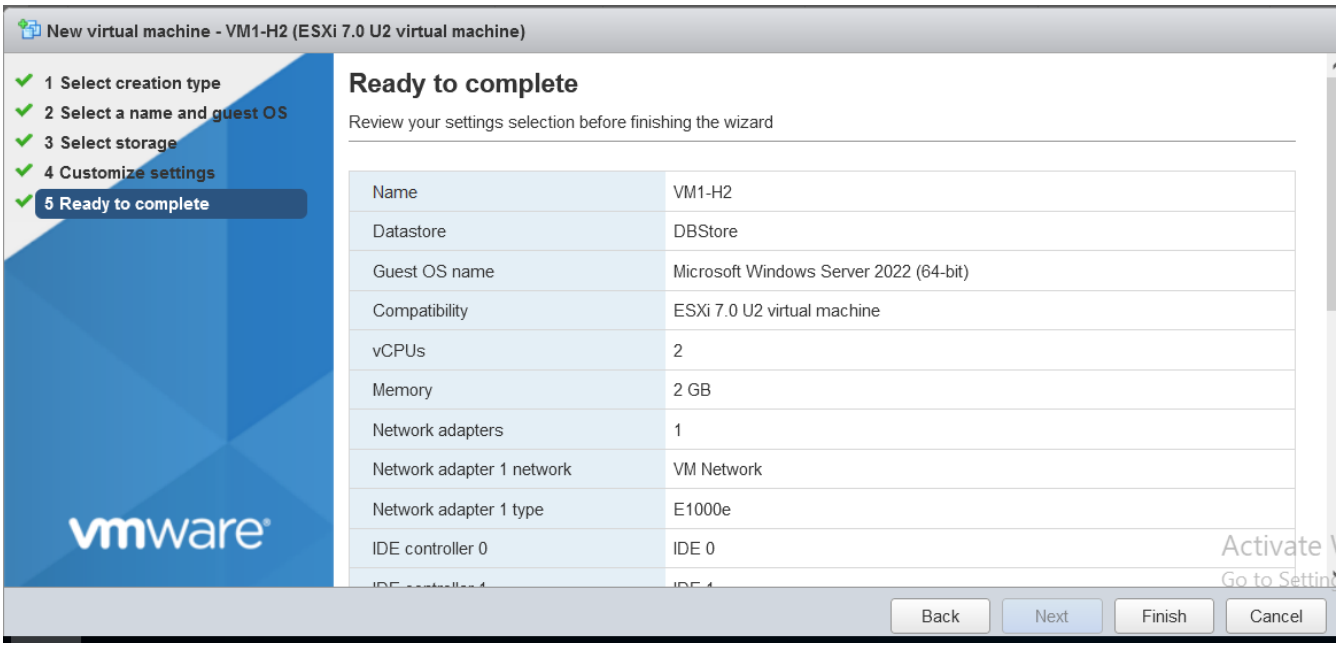


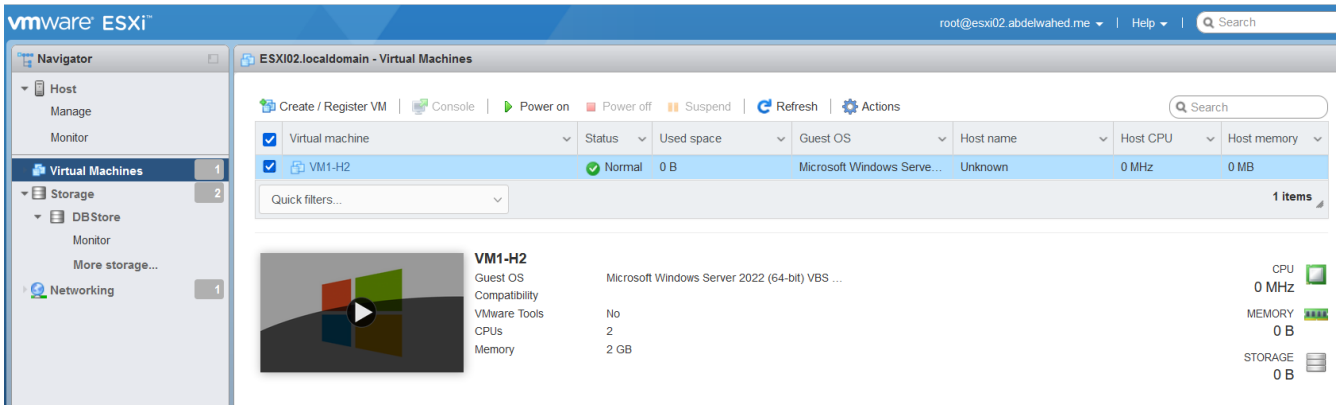
- **Thick Provisioned, Eagerly Zeroed:** Allocates and zeroes out storage space immediately.

Options for NIC and DVD (choose an ISO file from the datastore)

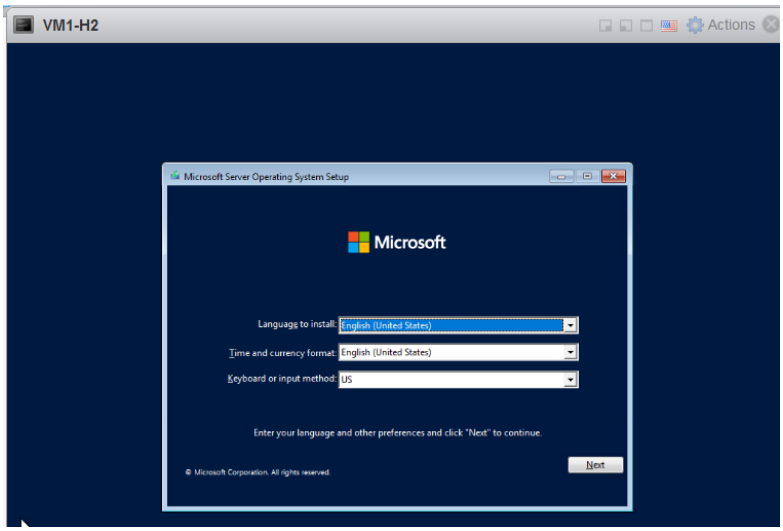


VMware vSphere Install, Configure, Manage | Lab Guide

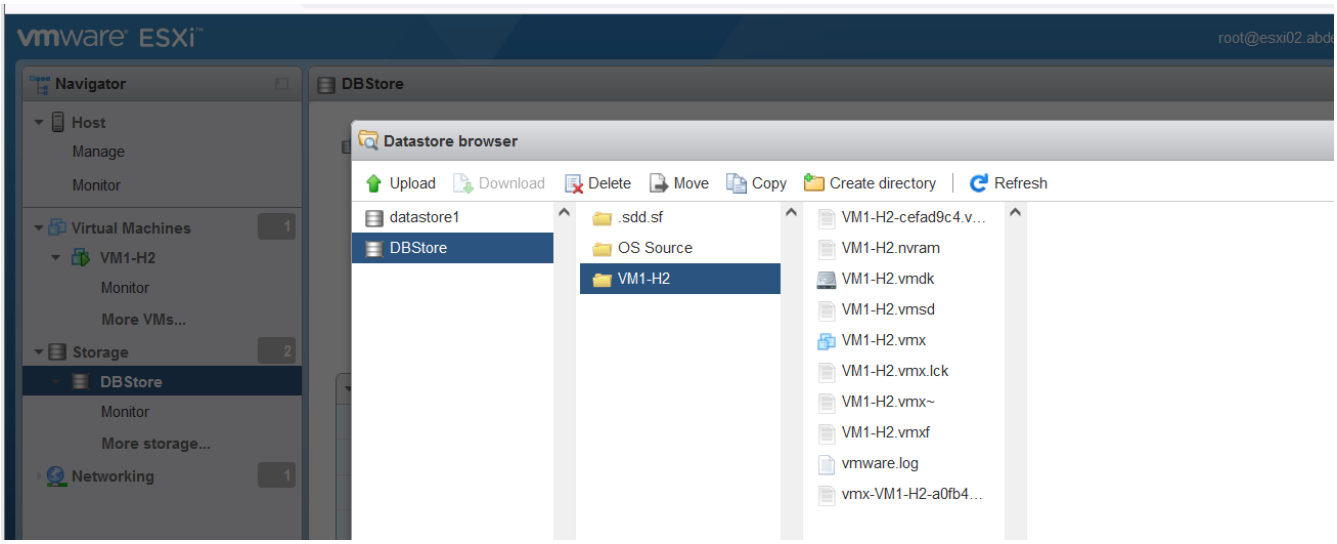




beginning installation



VM files saved inside selected datastore.



Download and Install VMRC

VMRC (VMware Remote Console) is a standalone application that allows you to connect to virtual machines on an ESXi host or vCenter Server using a remote console. Here are the steps to download and install VMRC:

Go to the VMware VMRC Download Page:

Visit the following URL: [VMware VMRC Download Page](#).

Download VMRC Installer:

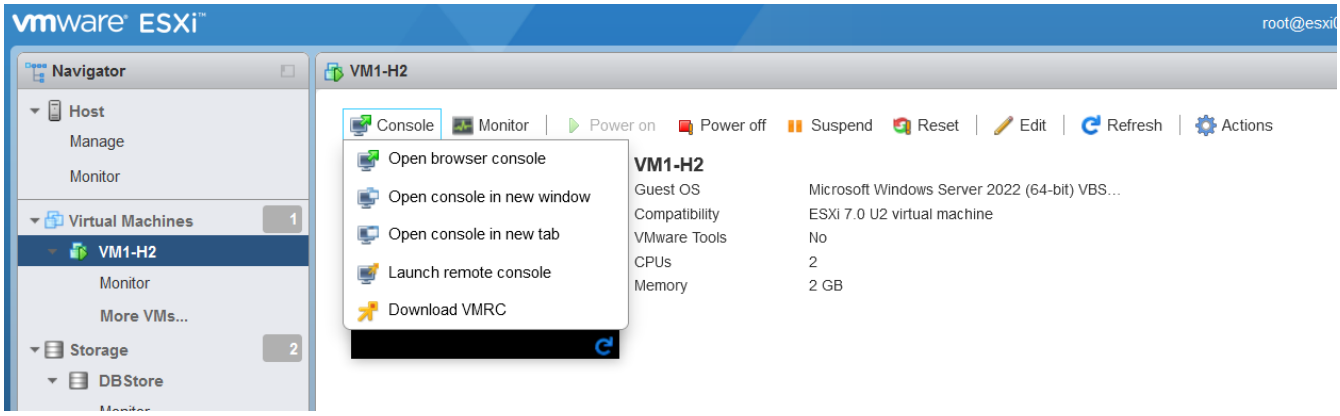
Click the "Download" button to download the VMRC installer for your operating system.

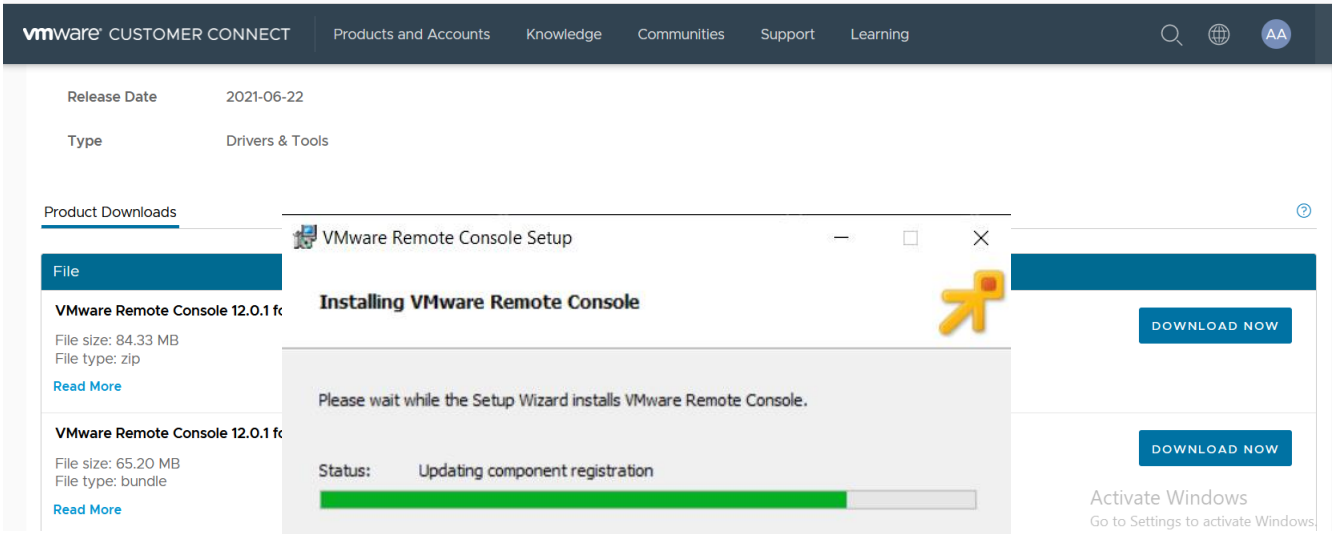
You will need to log in with your VMware account or create a new one if you don't have one already.

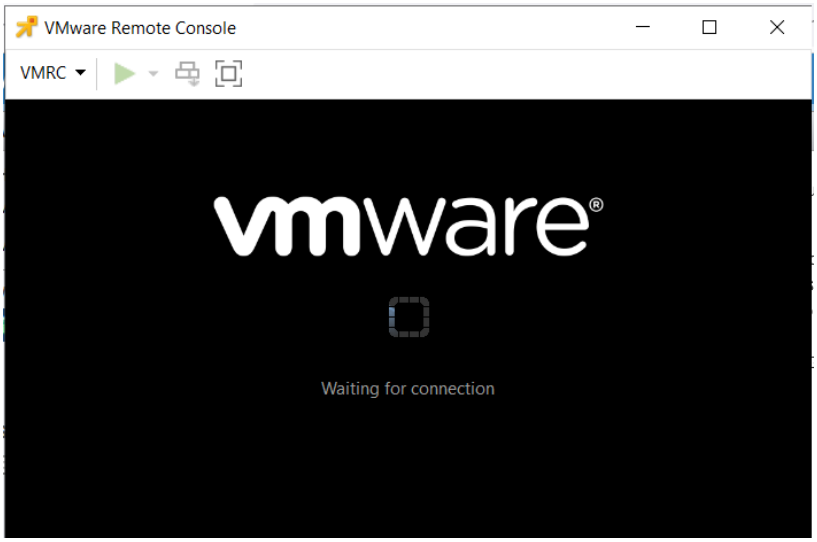
Install VMRC:

Once the download is complete, run the installer.

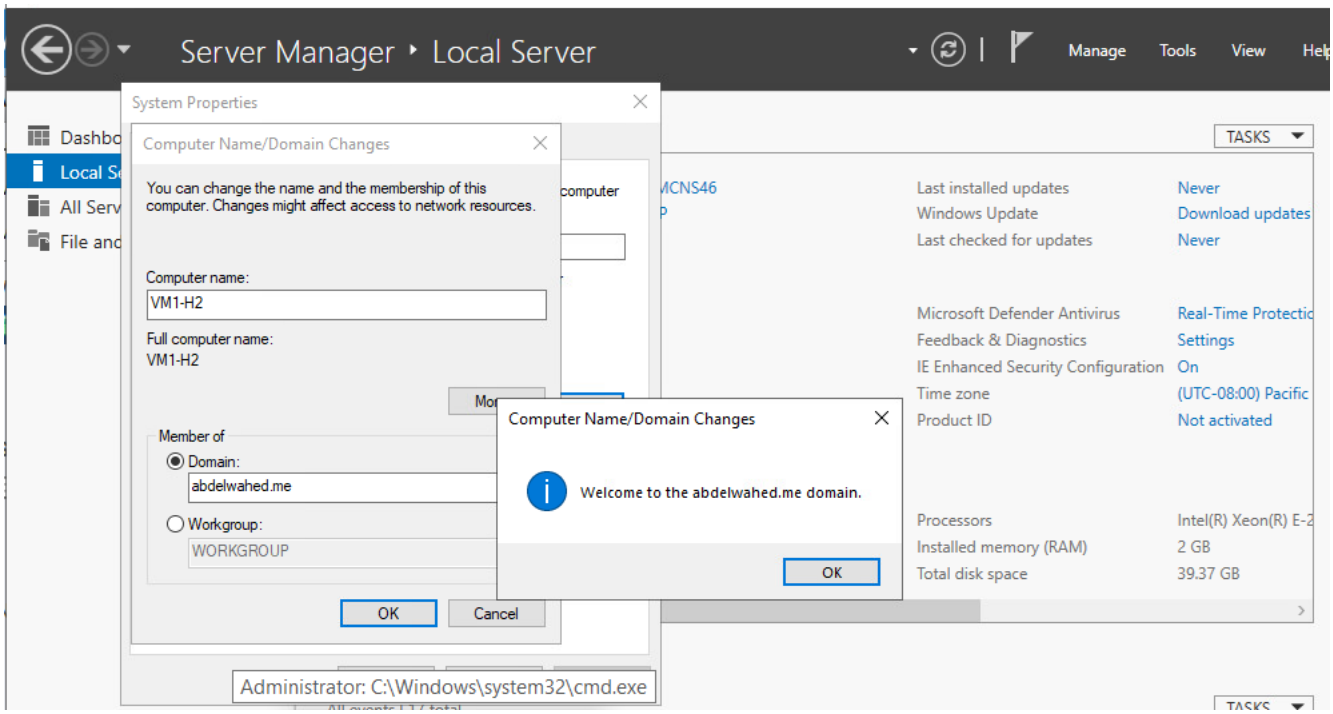
Follow the installation wizard to install VMRC on your system.





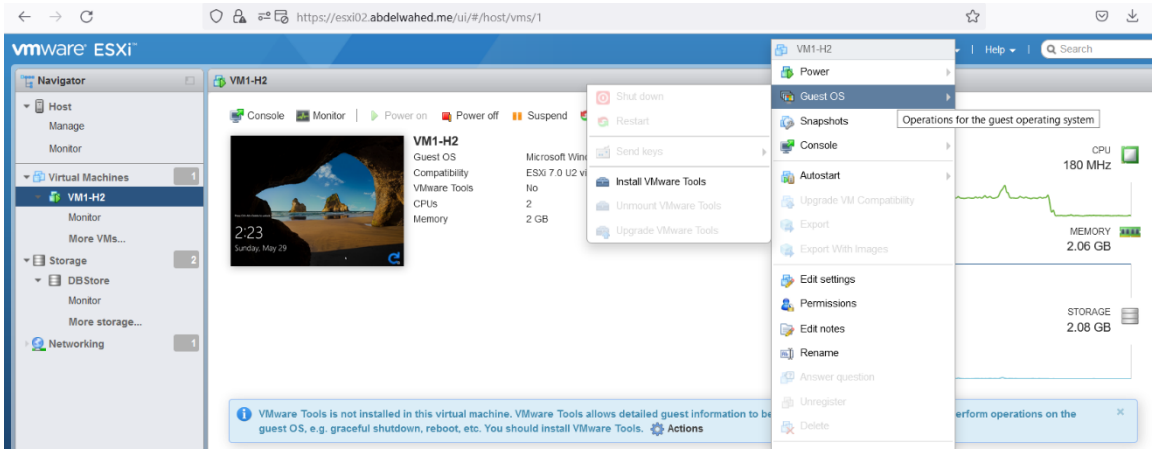


You can add that VM to the abdelwahed.me domain.

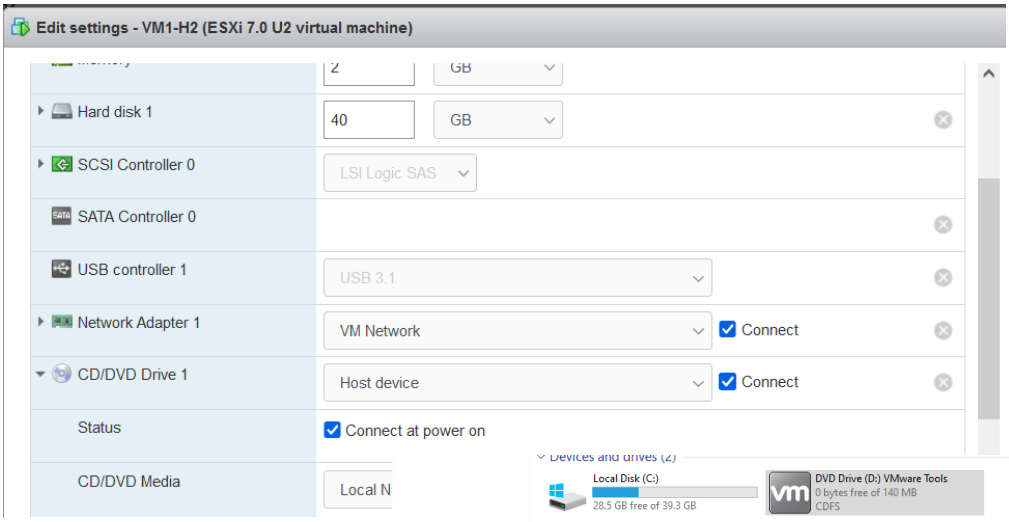


Set up VMware Tools.

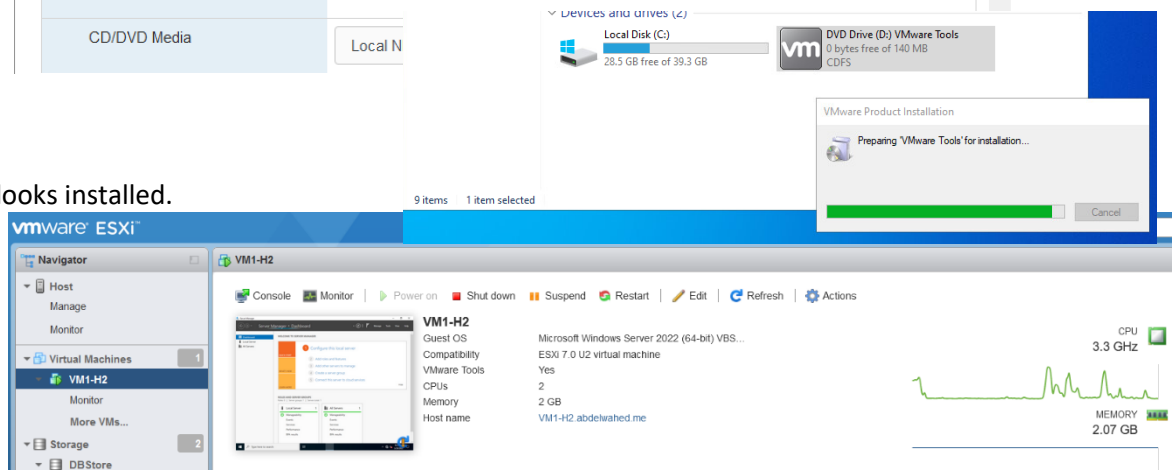
VMware Tools comprises various utilities and drivers that improve the performance and capabilities of virtual machines within vSphere.



If VMware Tools do not appear in this VM area, edit the CD/DVD VM settings (connect at power) as shown below.



Now VM tools looks installed.

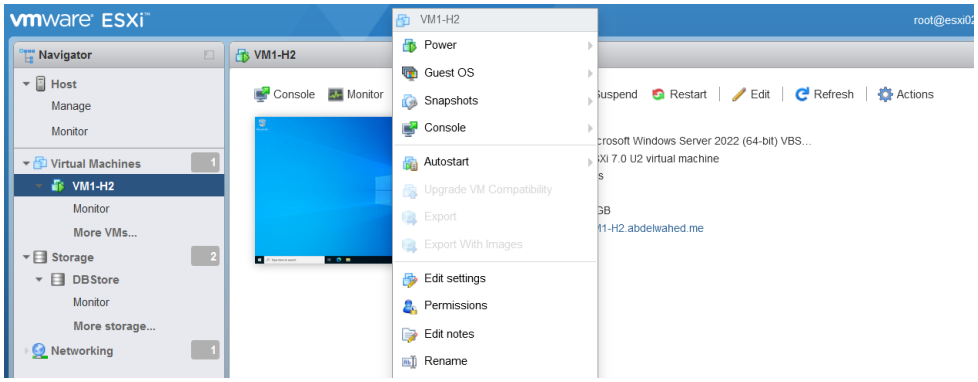


Edit VM settings.

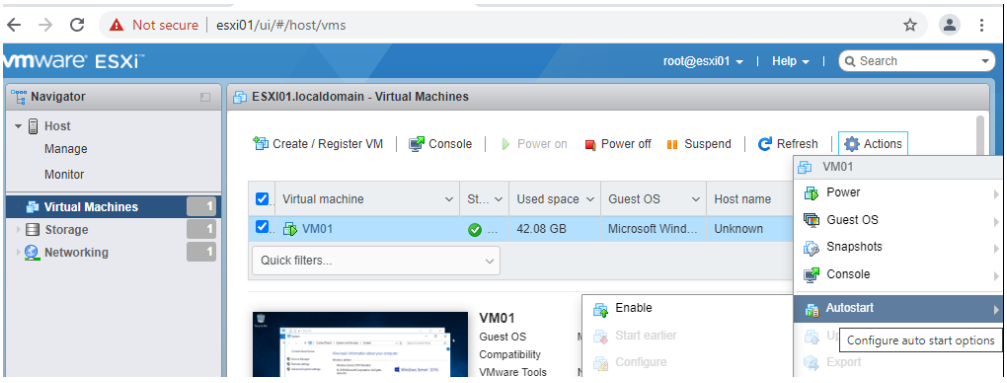
By editing the settings of a VM using ESXi, you can modify its configuration to meet the needs of your environment.

Key Configuration Changes

1. **Adjust CPU and Memory Allocation**:
   - **CPU Allocation**: Modify the number of virtual CPUs assigned to the VM.
   - **Memory Allocation**: Adjust the amount of memory allocated to the VM.
2. **Add or Remove Virtual Disks**:
   - **Add Disks**: Increase storage capacity by adding new virtual disks.
   - **Remove Disks**: Free up resources by removing unnecessary virtual disks.
3. **Configure Network Adapters**:
   - **Add Adapters**: Connect the VM to different networks or increase bandwidth.
   - **Remove Adapters**: Simplify network configuration by removing unused adapters.



With the ESXI01 server, you are able to adjust few settings such as AutoStart directly.



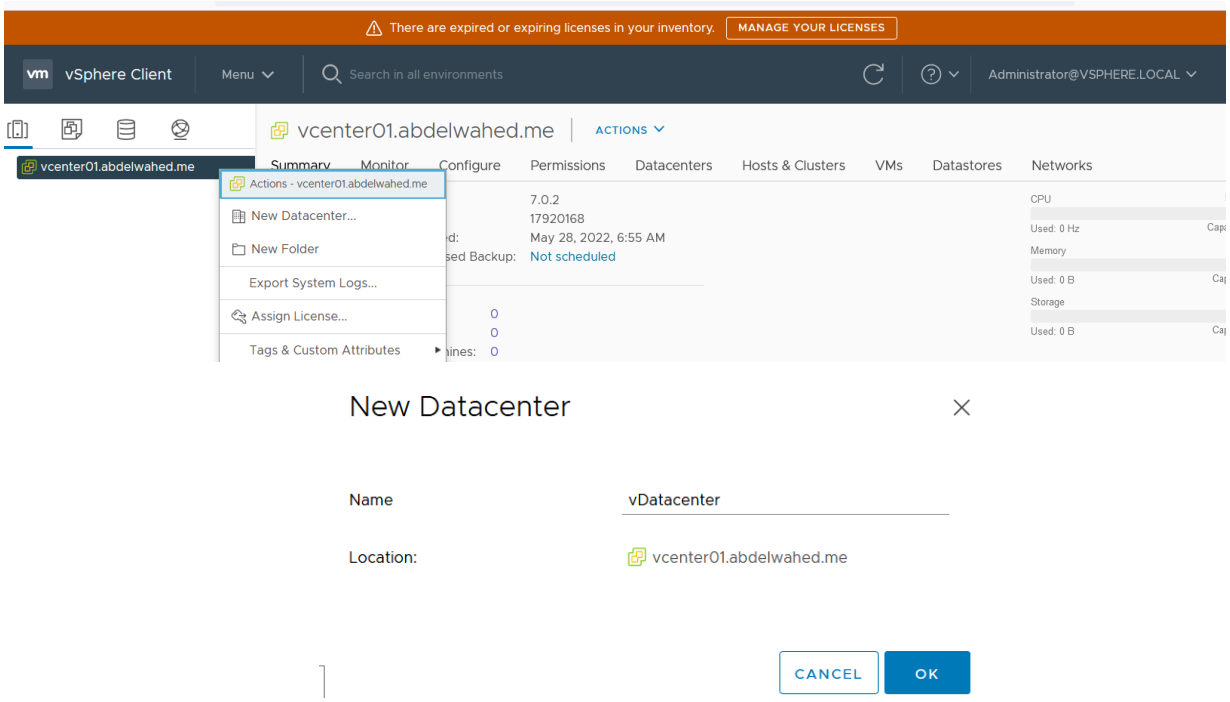
As indicated, the management of VMs via ESXi comes with a set of limited features; therefore, we transition to using Vcenter which offers an expanded suite of management tools including migration, cloning, and high availability options.

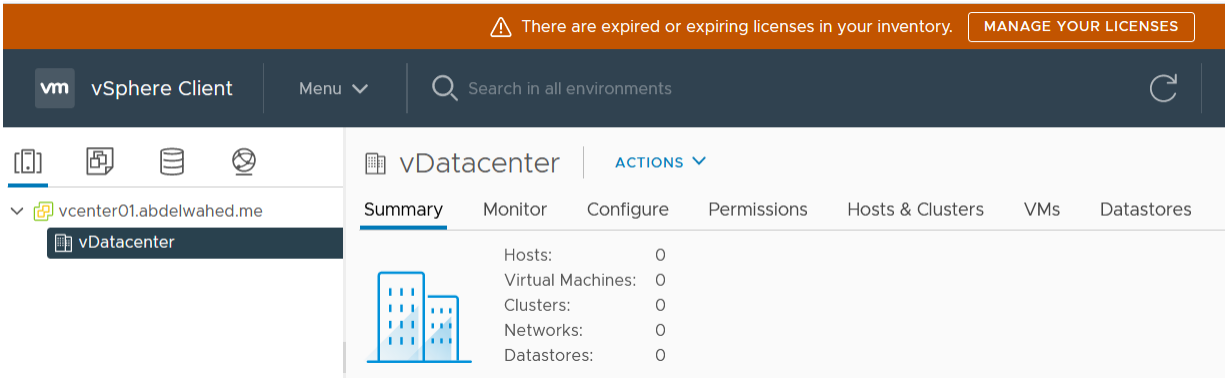
Configuring and Managing ESXi Servers Using vCenter

vCenter Server: **vCenter01**
|
|-- **Datacenters**
| |
| |-- **Datacenter1**
| | |
| | |-- **Clusters**
| | | |
| | | |-- **ClusterA**
| | | | |
| | | | |-- **Hosts (ESXi Servers)**
| | | | | |
| | | | | |-- **ESXi1.ohi.com**
| | | | | | |
| | | | | | |-- **VM01**
| | | | | | |
| | | | | | |-- **VM02**
| | | | | |
| | | | | |-- **ESXi02.ohi.com**
| | | | | |
| | | | | |-- **VM03**
| | | | |
| | | | |-- **Resource Pools**
| | | | |
| | | | |-- **HighPriorityPool**
| | | | |
| | | | |-- **LowPriorityPool**
| | |
| | |-- **Folders**
| | | |
| | | |-- **ProdVMs**
| | | | |
| | | | |-- **VM04**
| | | |
| | | |-- **TestVMs**
| | |
| | |-- **VM05**

VMware vSphere Install, Configure, Manage | Lab Guide

By adding **ESXi** servers to **vCenter**, you can centralize the management of your virtual environment and perform tasks such as creating virtual machines, configuring storage and networking, and monitoring performance. It's important to follow best practices for managing ESXi servers, such as keeping them up-to-date with the latest patches and updates, monitoring their performance and usage, and securing them with appropriate permissions and firewall rules.

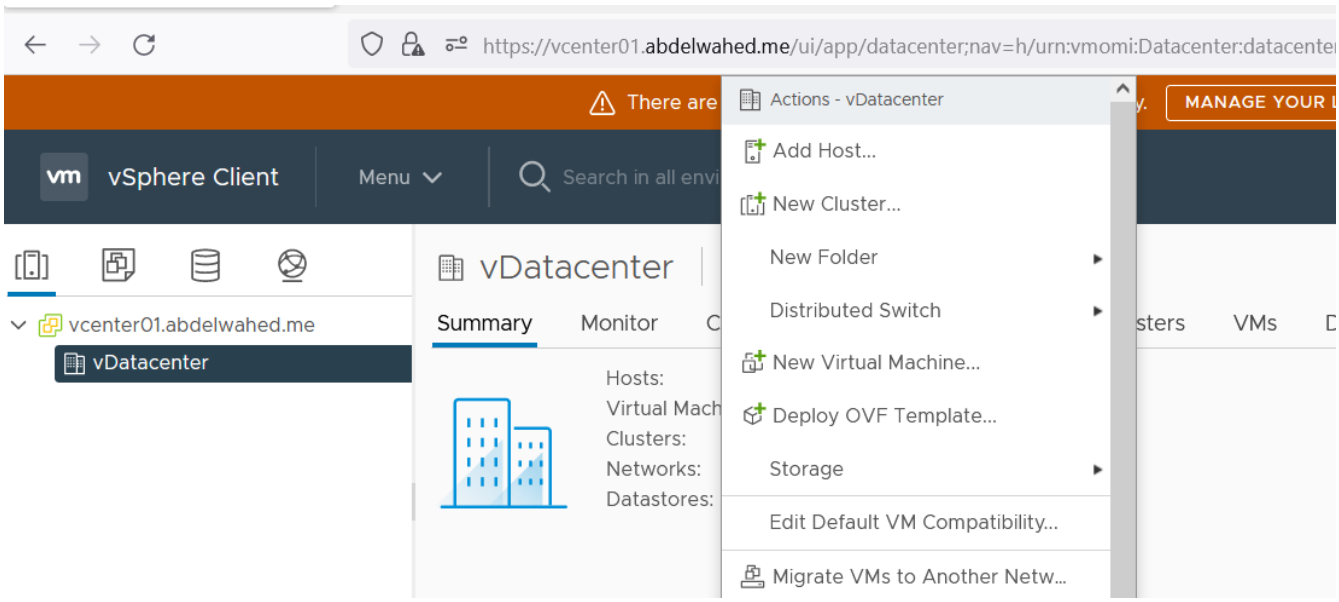




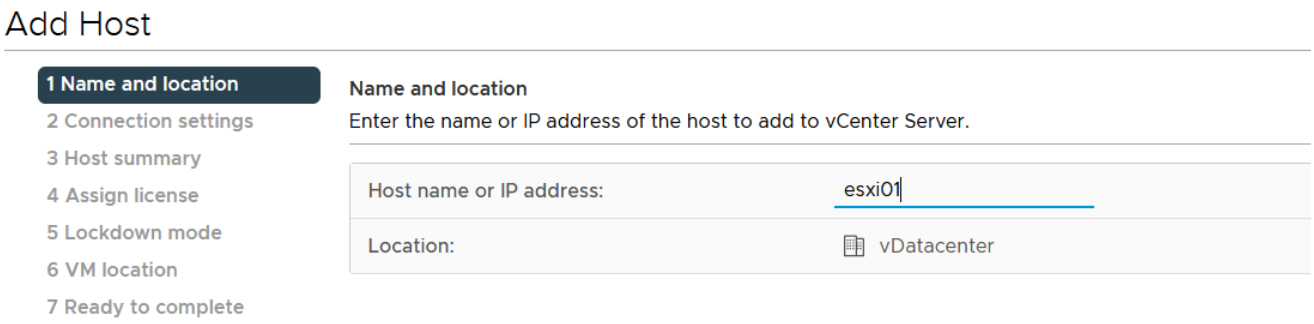
Adding ESXi hosts is now possible.

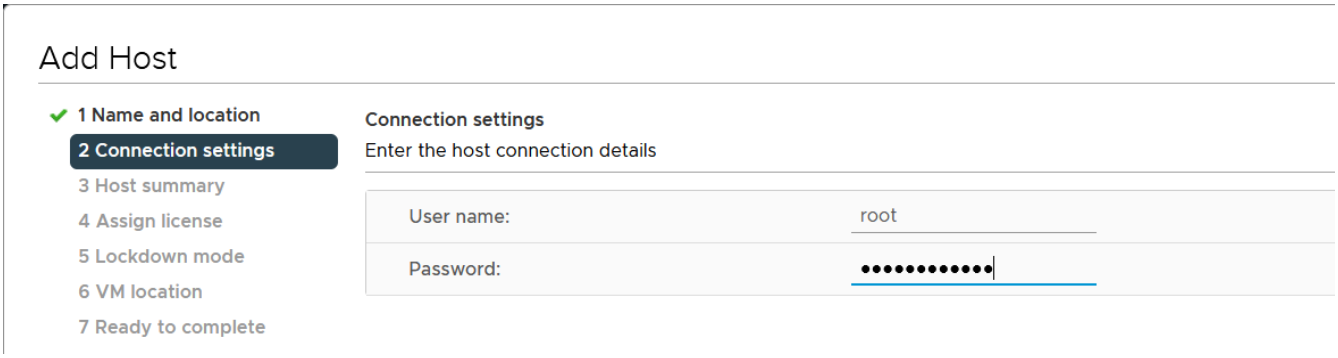
---

www.abdelwahed.me



Remember to review the new folder option.





Add Host

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

Host summary

Review the summary for the host

Name	esxi01.abdelwahed.me
Vendor	VMware, Inc.
Model	VMware7,1
Version	VMware ESXi 7.0.2 build-17867351
Virtual Machines	vCenter Server

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	Ca
Evaluation License	--	--	--	--

Add Host

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

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.

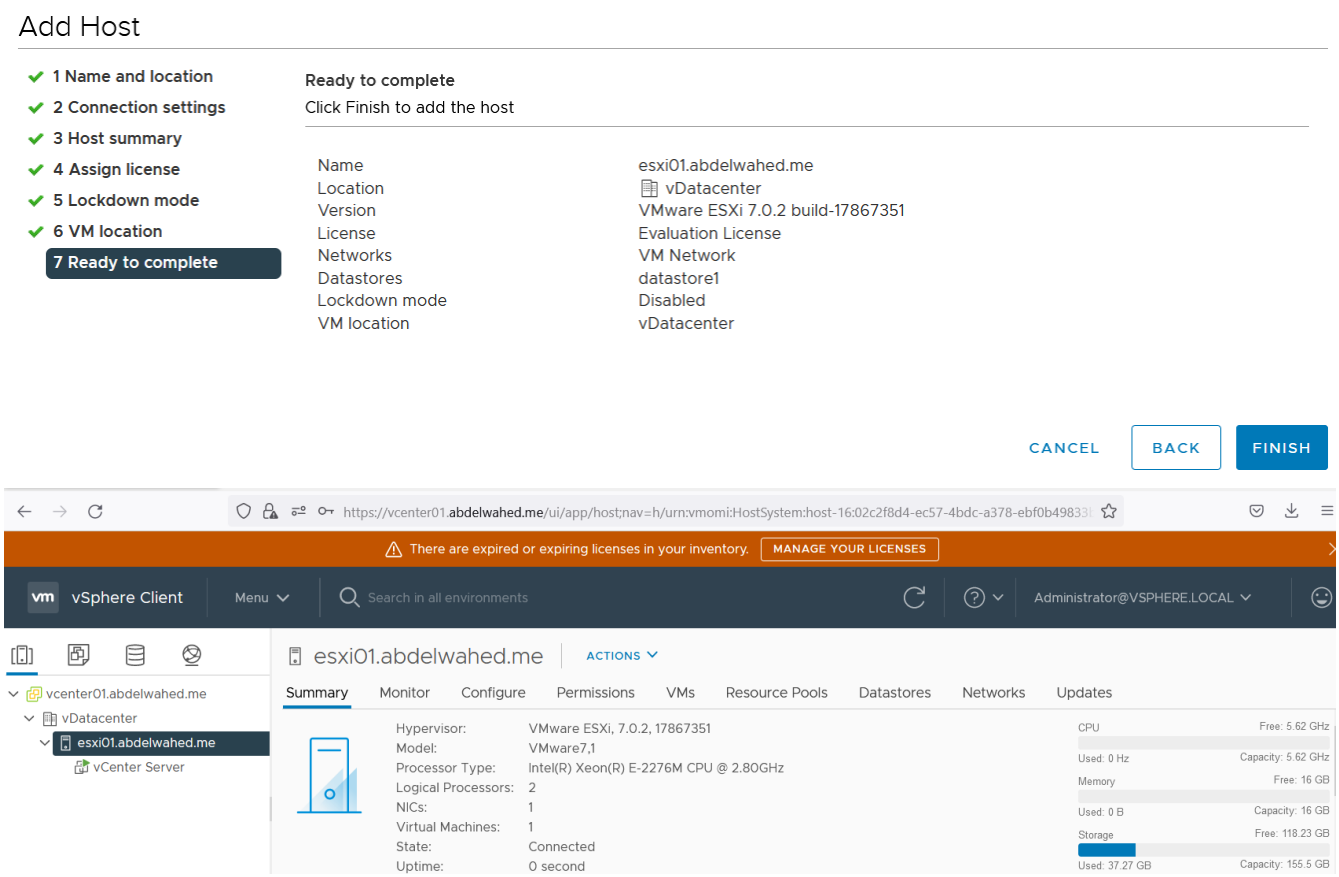
- (•) Disabled
- ( ) **Normal**
  The host is accessible only through the local console or vCenter Server.
- ( ) **Strict**
  The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

Add Host

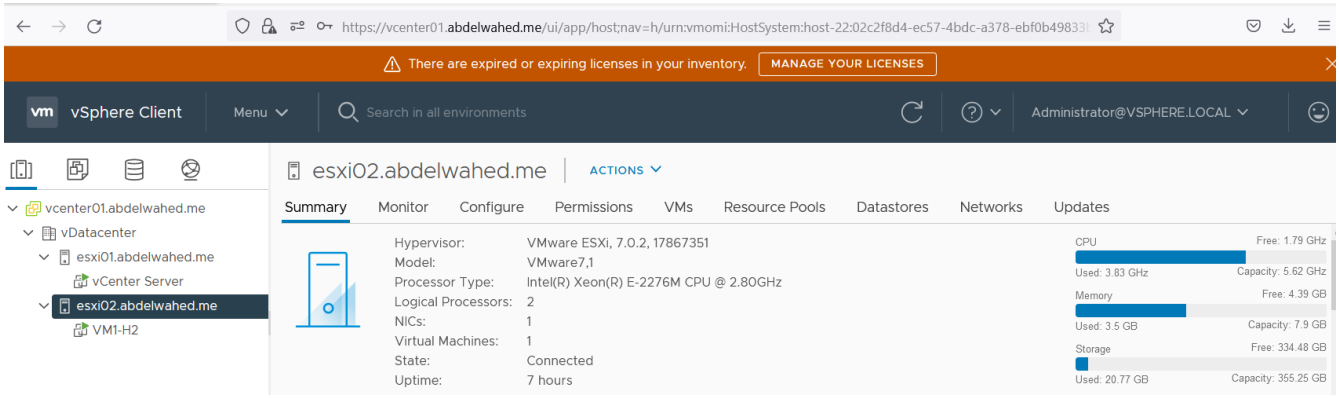
- ✔ 1 Name and location
- ✔ 2 Connection settings
- ✔ 3 Host summary
- ✔ 4 Assign license
- ✔ 5 Lockdown mode
- 6 VM location
- 7 Ready to complete

VM location

vDatacenter



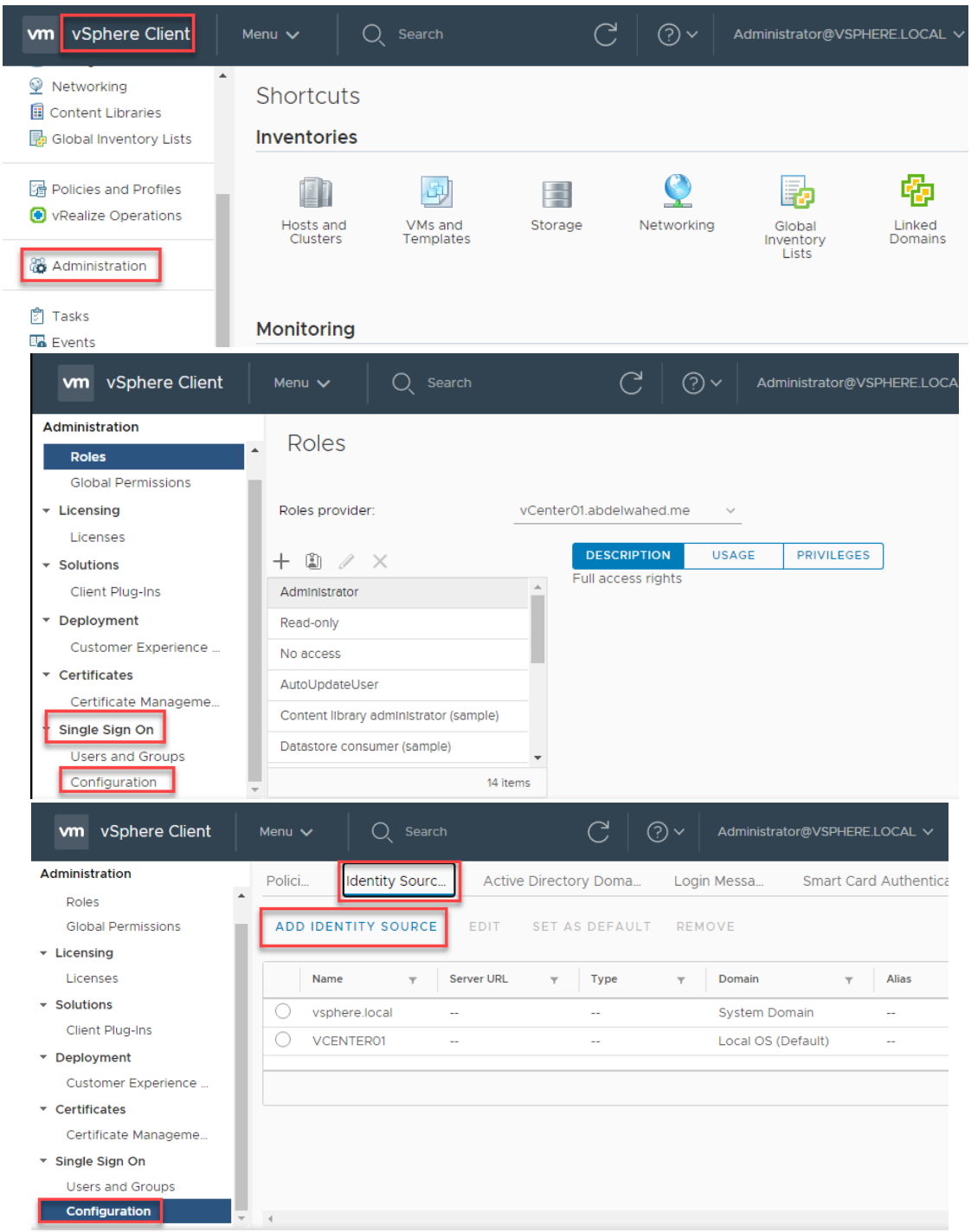
Apply the same process to ESXi02 for integration into our data center.

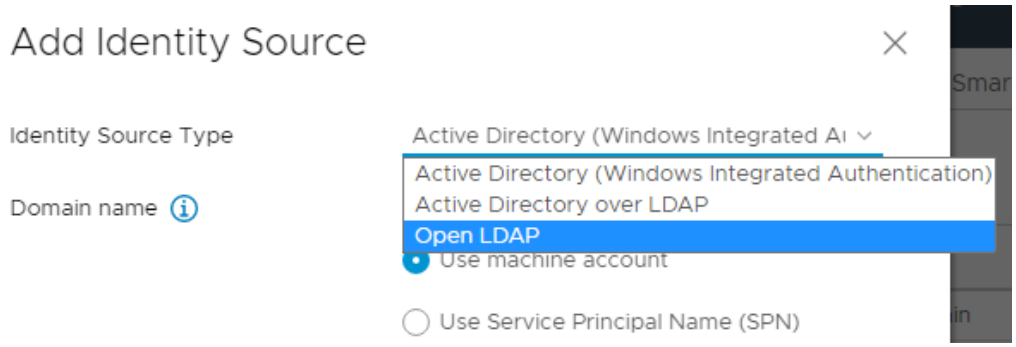


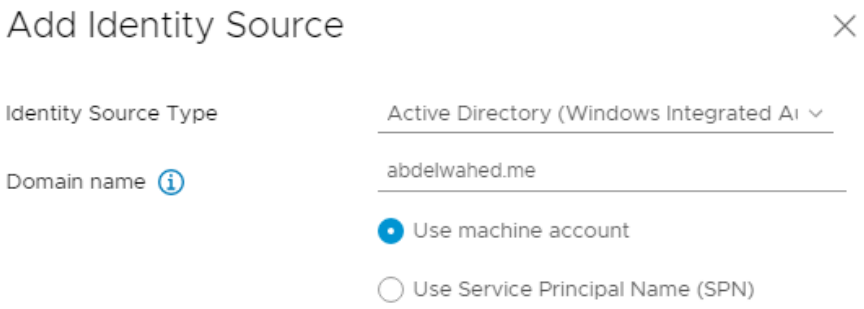
Both hosts have now been added.

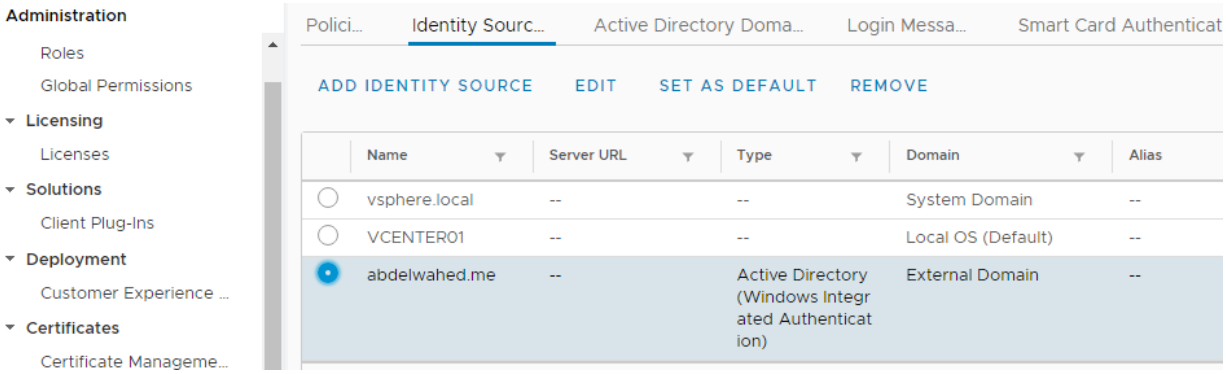
Integrate vSphere with Active Directory

Integrating vSphere with Active Directory (AD) allows you to use AD user accounts and groups to authenticate and authorize access to vSphere resources. This simplifies user management, improves security, and provides a centralized view of user permissions across the organization. Here are the steps to integrate vSphere with AD:



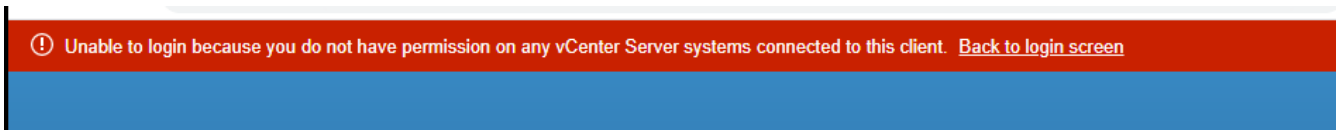




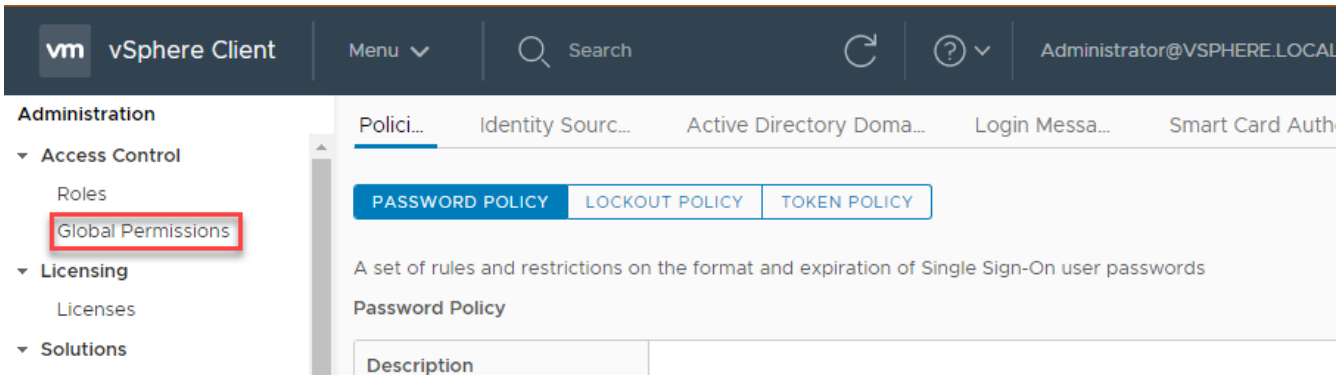


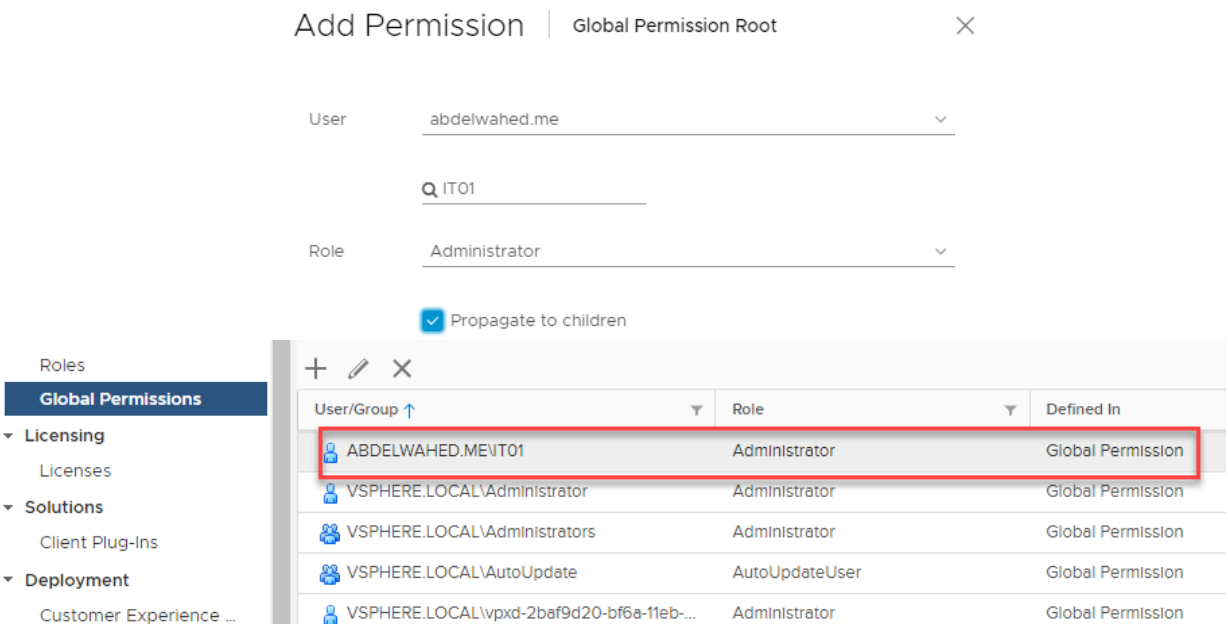
sign in using domain accounts and privileges

You are now able to log in, however, you lack the necessary permissions to access vCenter resources.

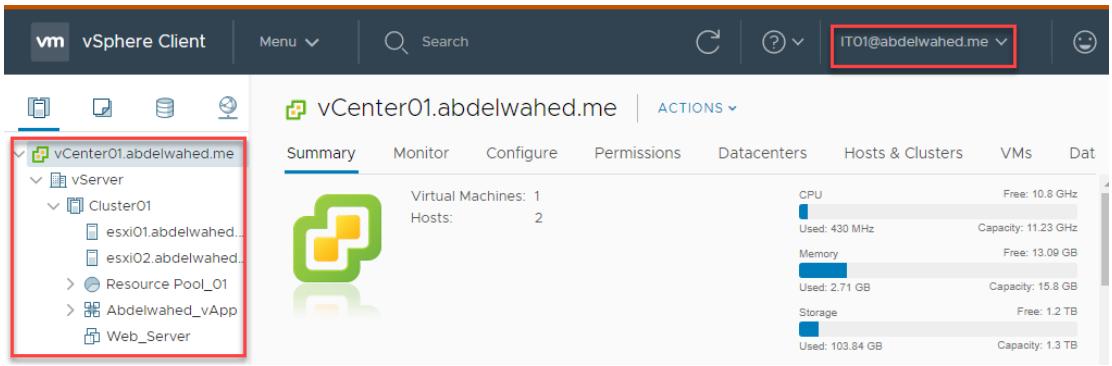


Now grant it01@abdelwahed.me permissions using Role-Based Access Control (RBAC).

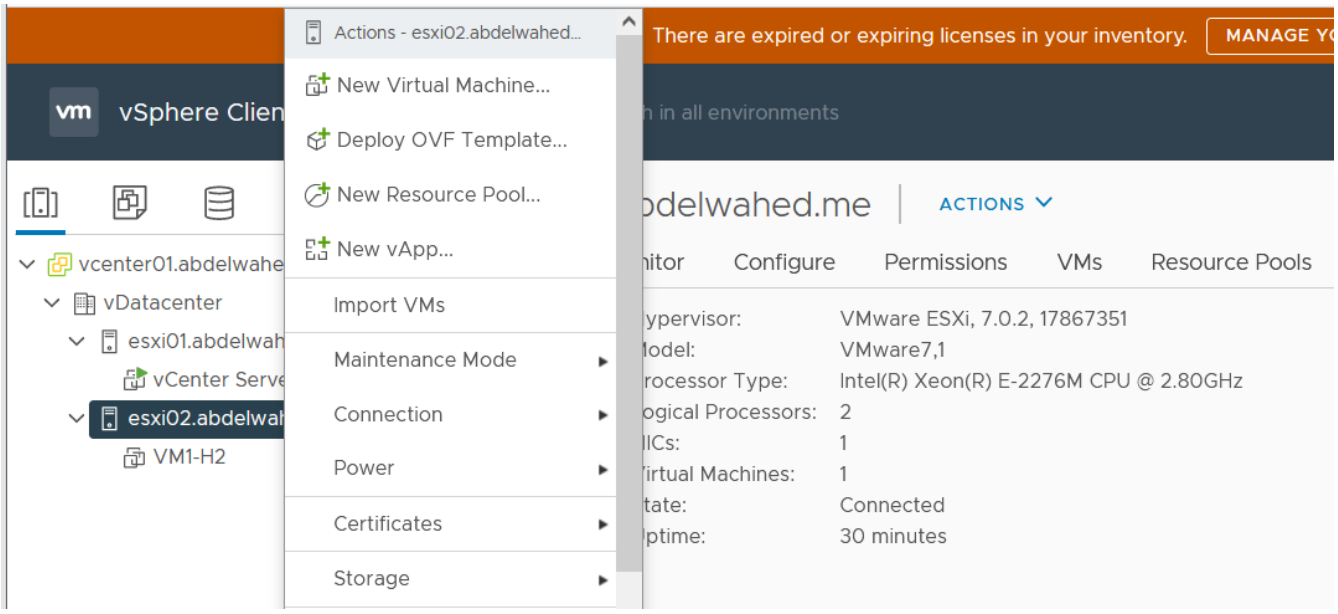


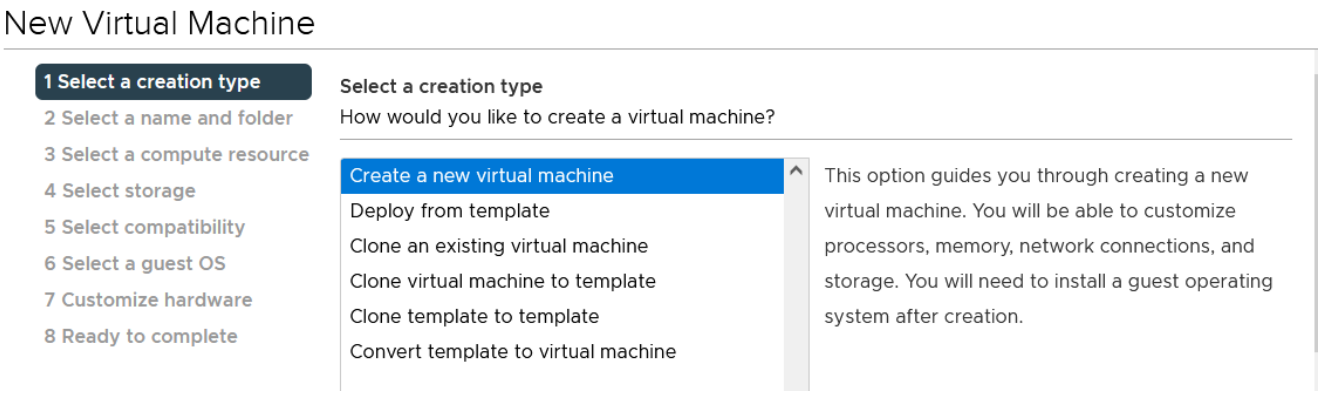


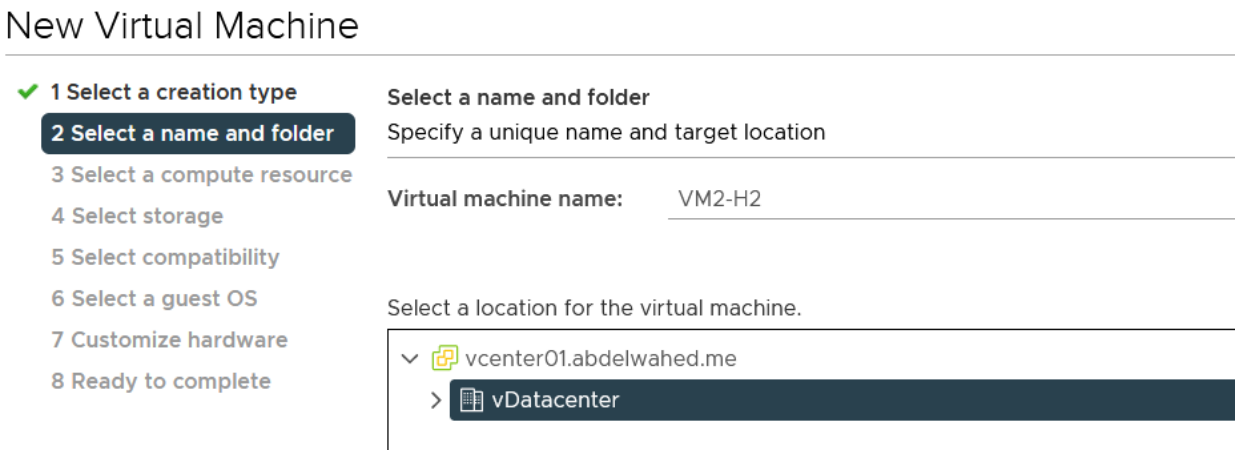
IT01 now has a full access.

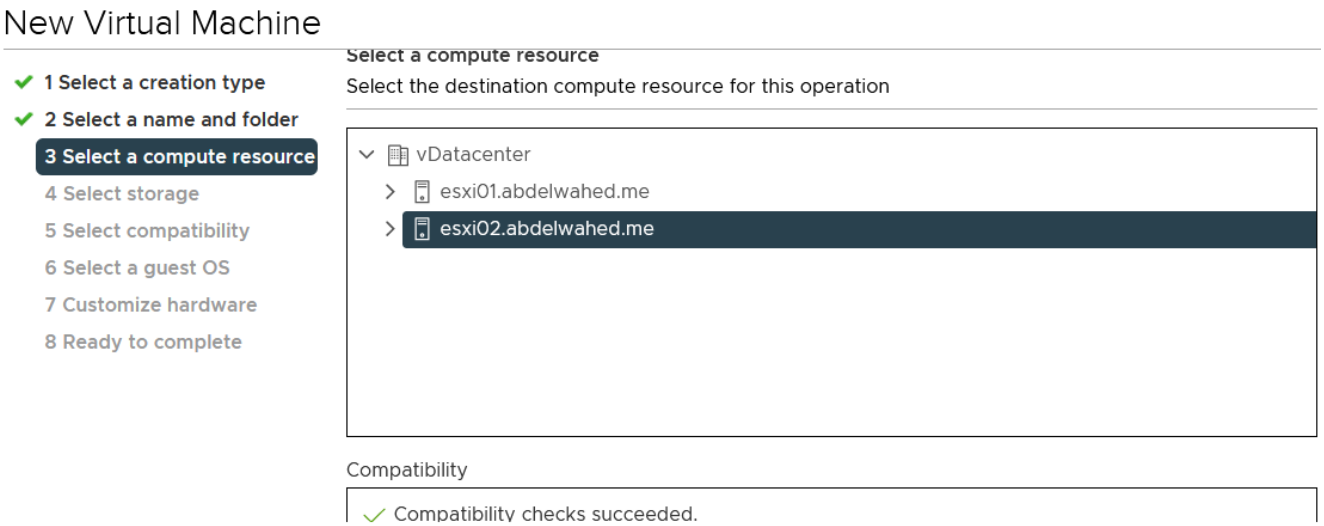


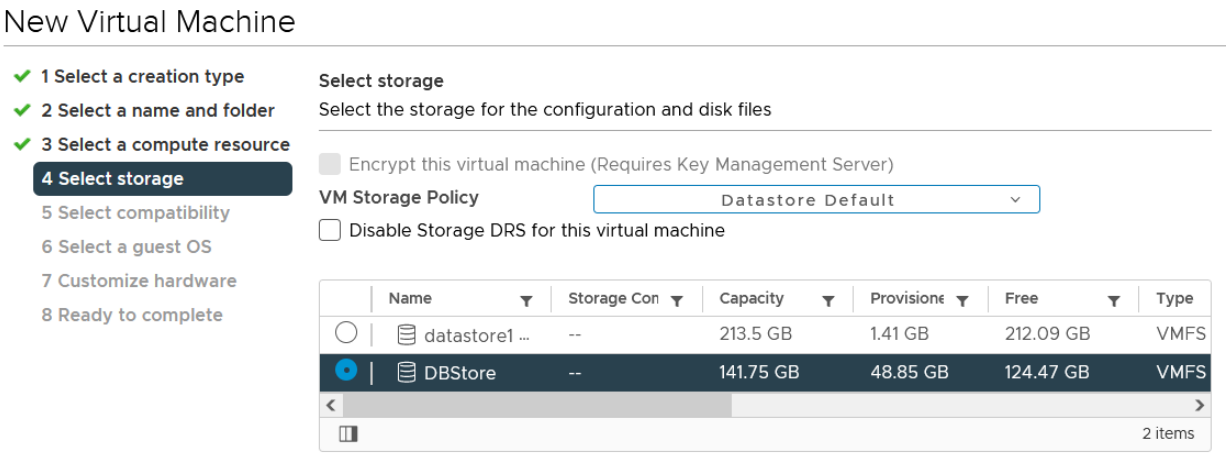
Create VM using vCenter

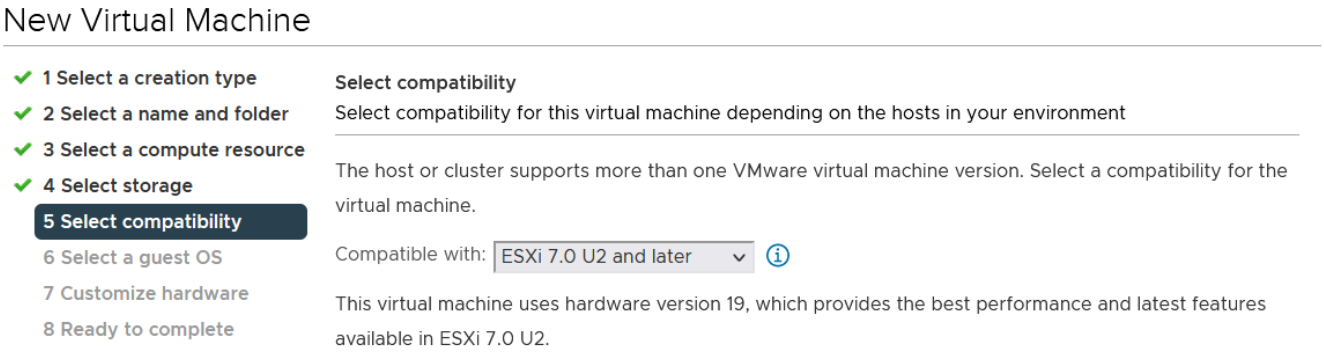


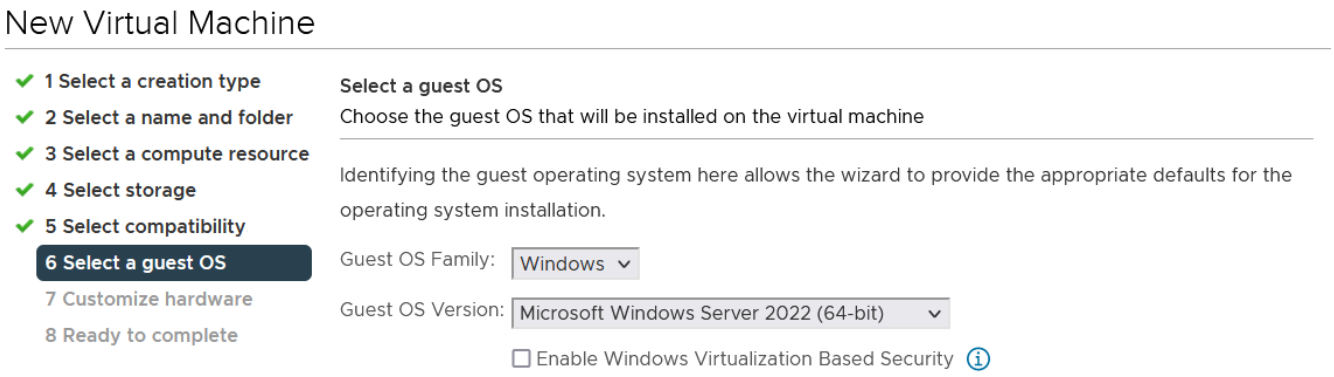




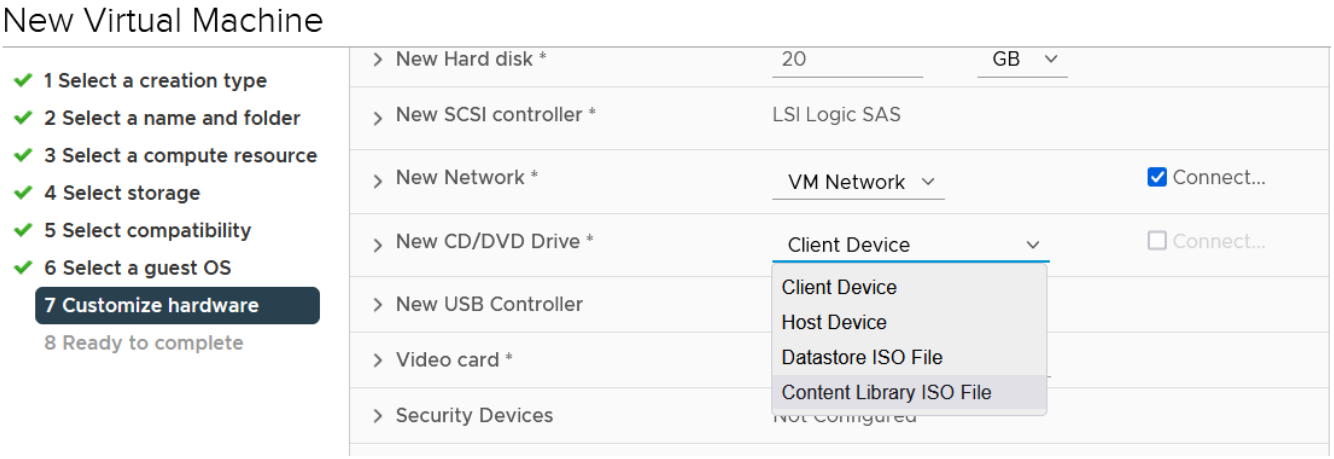

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select a compute resource
Select the destination compute resource for this operation
vDatacenter
esxi01.abdelwahed.me
esxi02.abdelwahed.me
Compatibility
Compatibility checks succeeded.

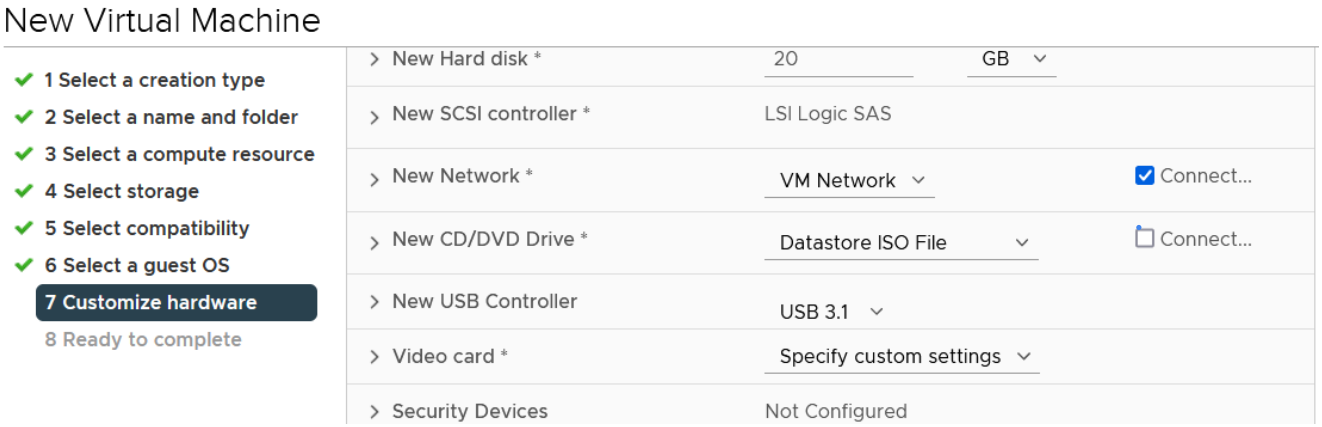

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select storage
Select the storage for the configuration and disk files
Encrypt this virtual machine (Requires Key Management Server)
VM Storage Policy
Datastore Default
Disable Storage DRS for this virtual machine
Name
Storage Con
Capacity
Provisione
Free
Type
datastore1 ...
--
213.5 GB
1.41 GB
212.09 GB
VMFS
DBStore
--
141.75 GB
48.85 GB
124.47 GB
VMFS
2 items

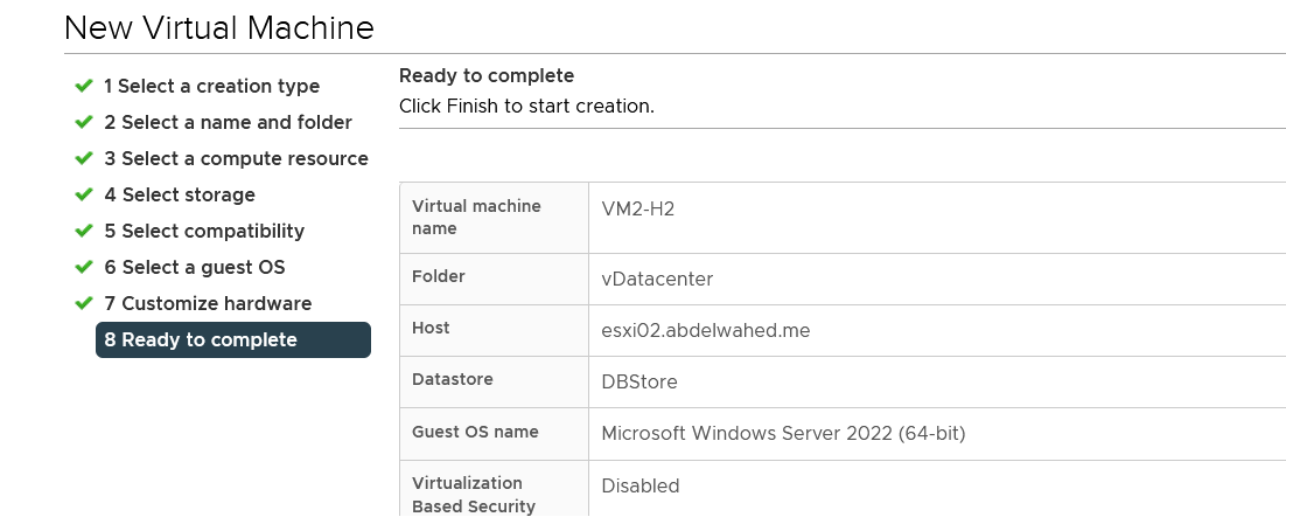

New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Select compatibility
Select compatibility for this virtual machine depending on the hosts in your environment
The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.
Compatible with:
ESXi 7.0 U2 and later
This virtual machine uses hardware version 19, which provides the best performance and latest features available in ESXi 7.0 U2.



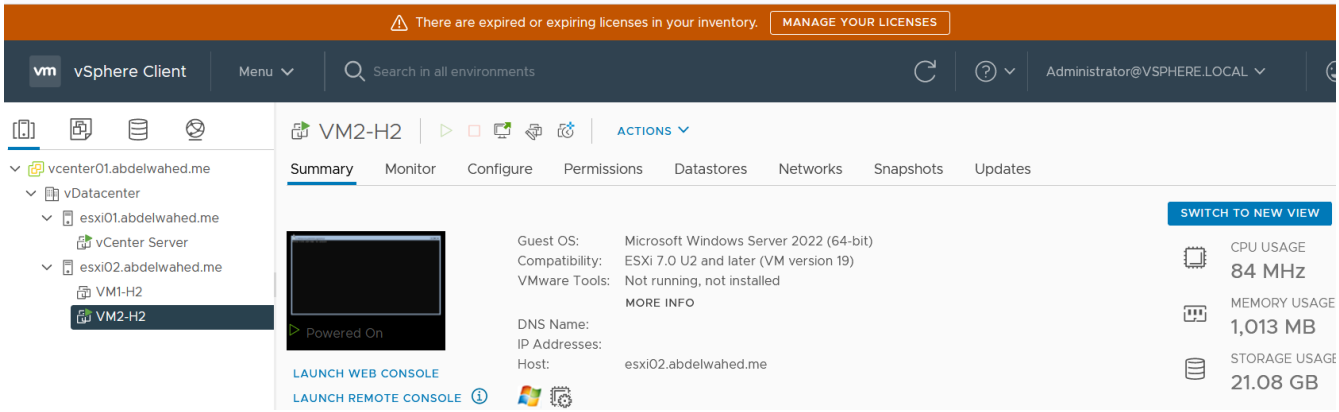
Compatibility: ESXi 7.0 U2 and later (VM version 19)

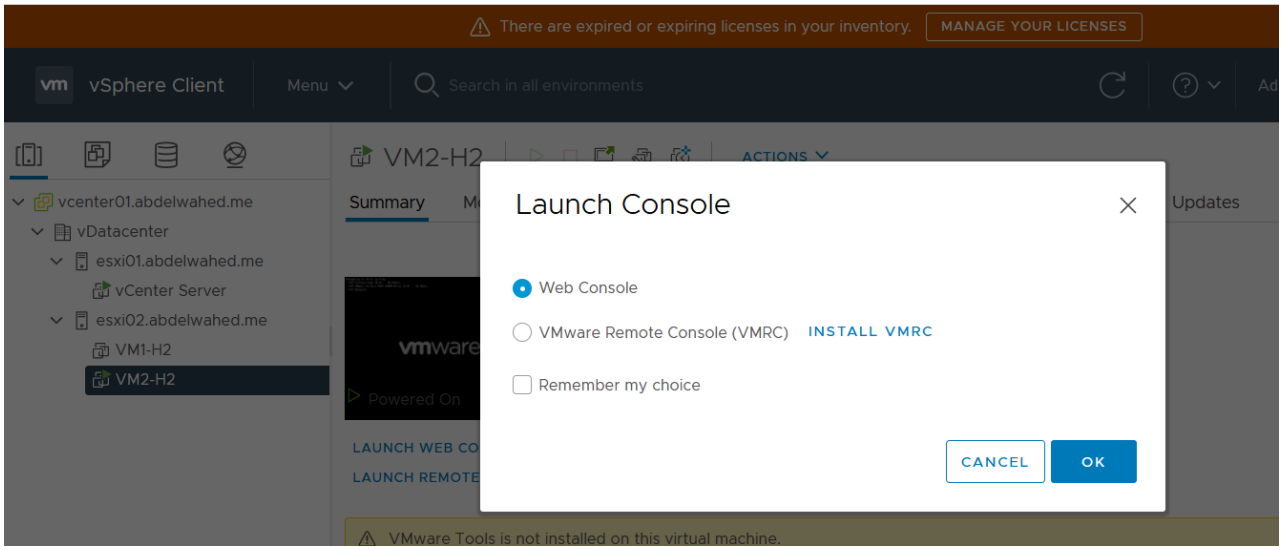






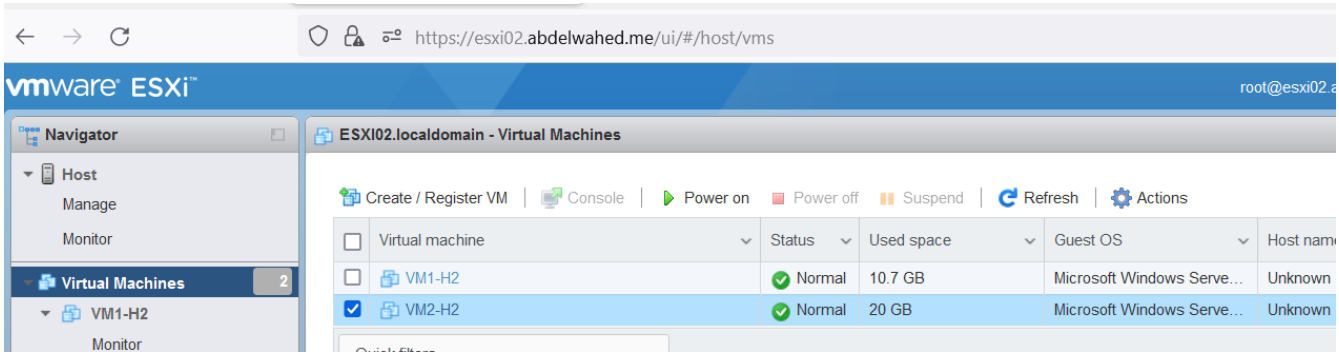
Server Core 2022 is now installed.



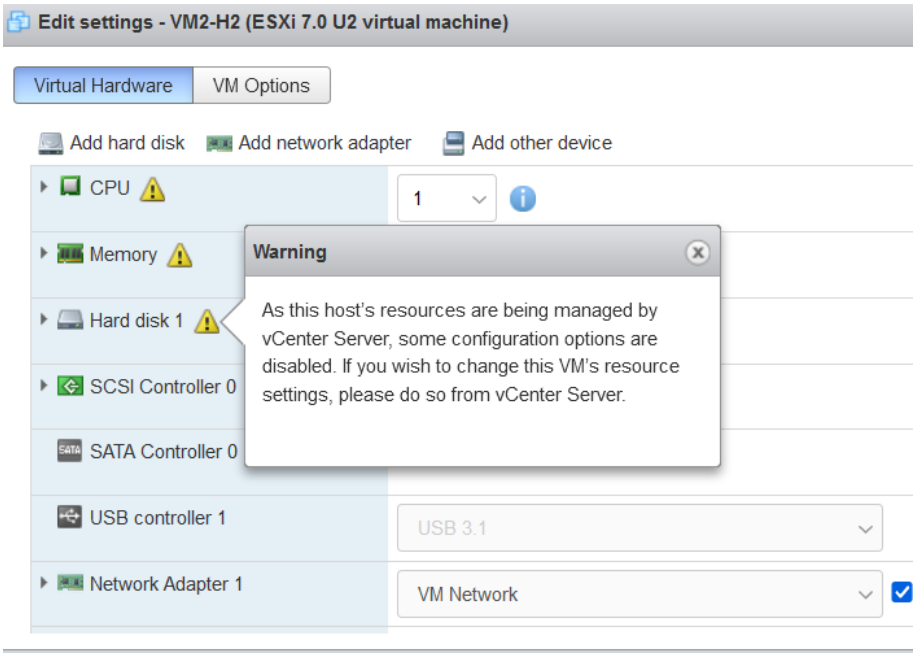


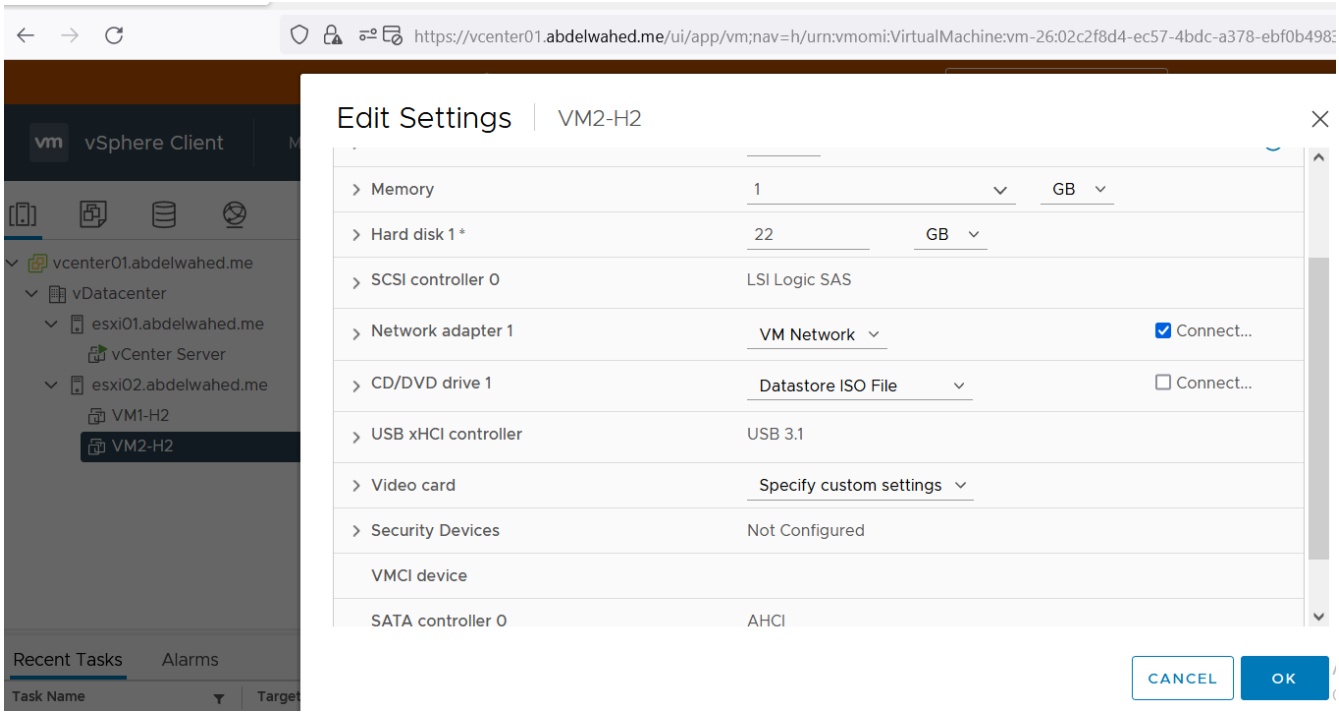
Edit VM Settings from vCenter.

With VM configurations, you are able to modify various virtual machine settings. In this instance, we will be demonstrating how to increase the size of the hard drive (note that some settings may necessitate turning the power off).

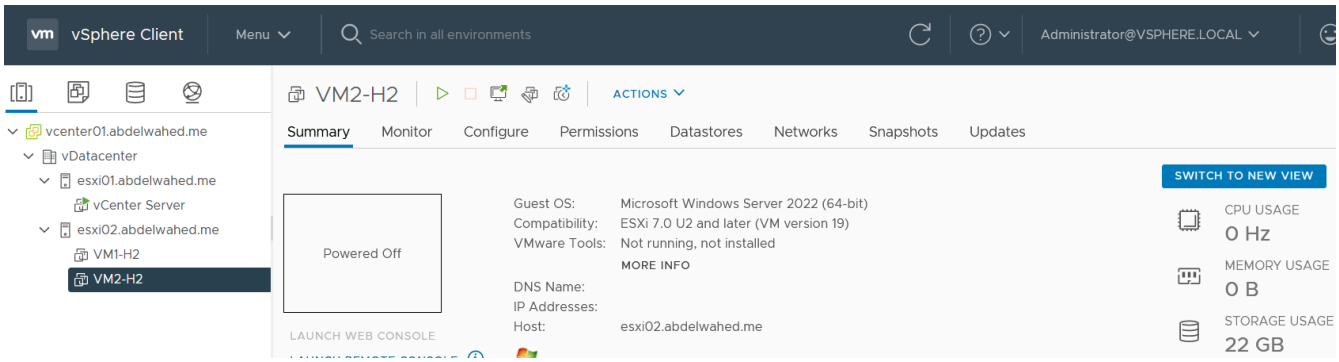


Using vCenter, we will increase the VM's hard drive size from 20 GB to 22 GB.



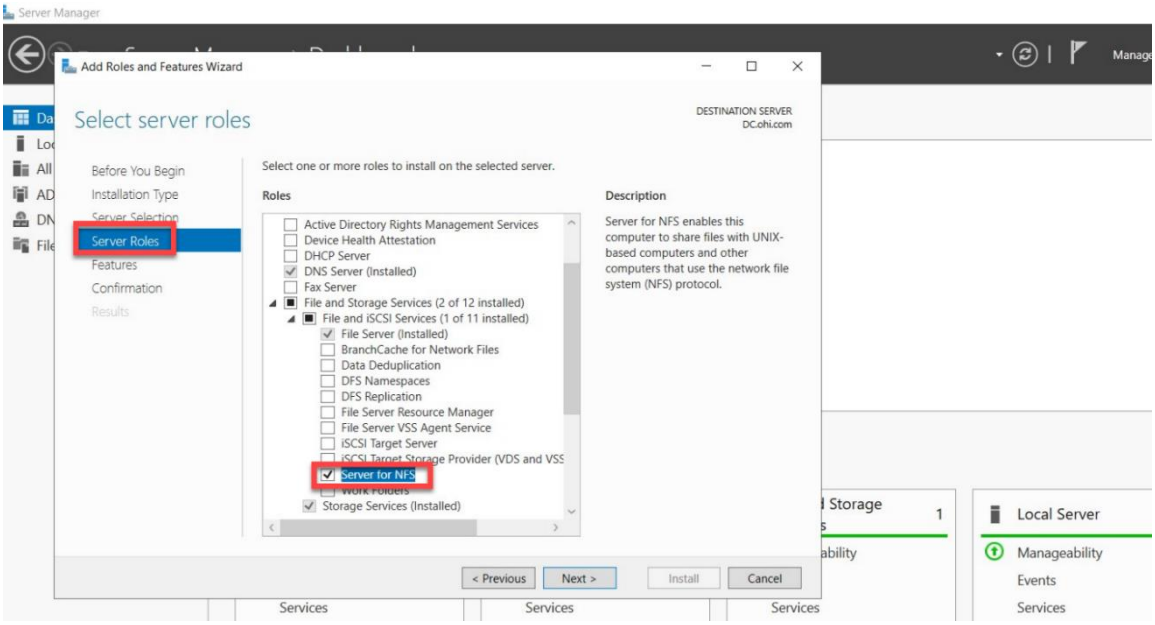


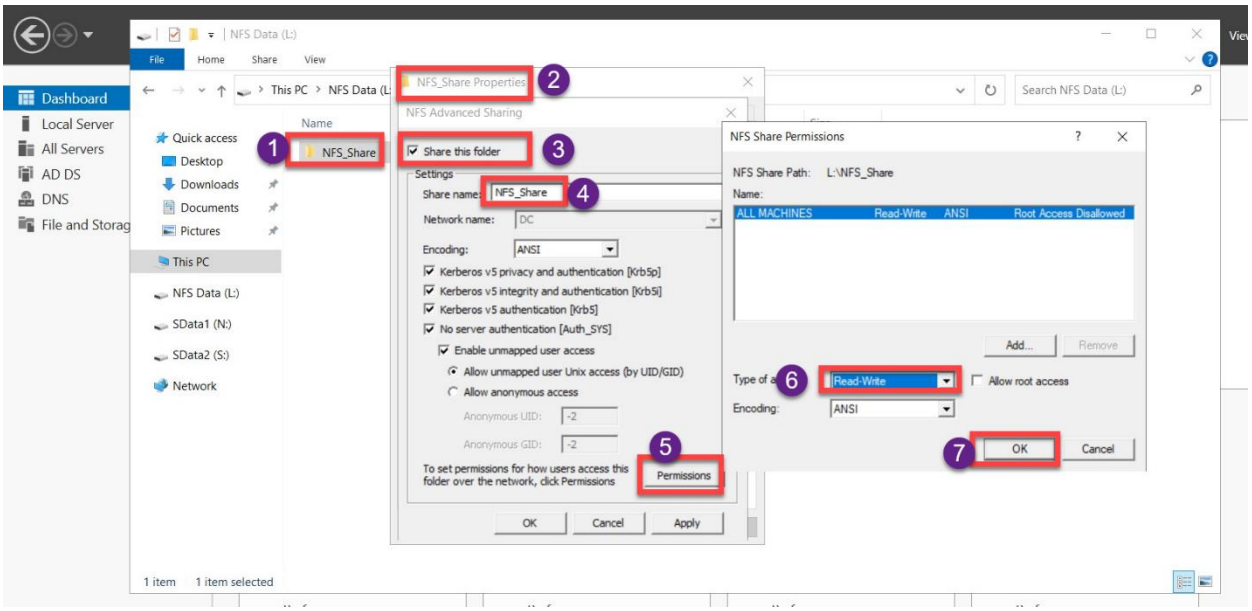
Hard drive now expanded to 22GB



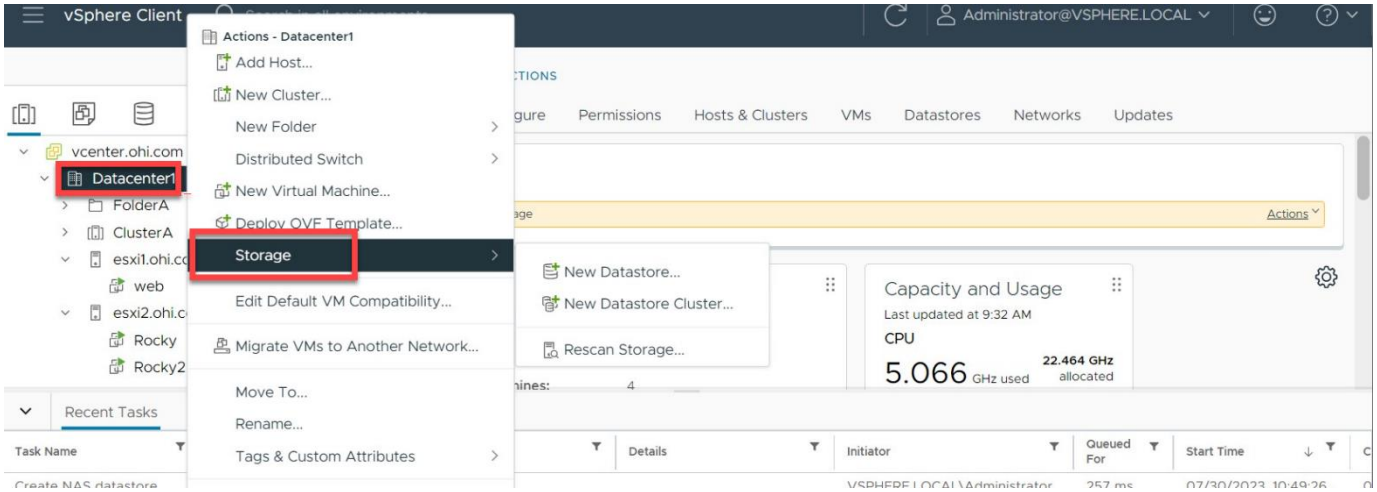
Configuring NFS Server on Windows Server - NFS Datastore

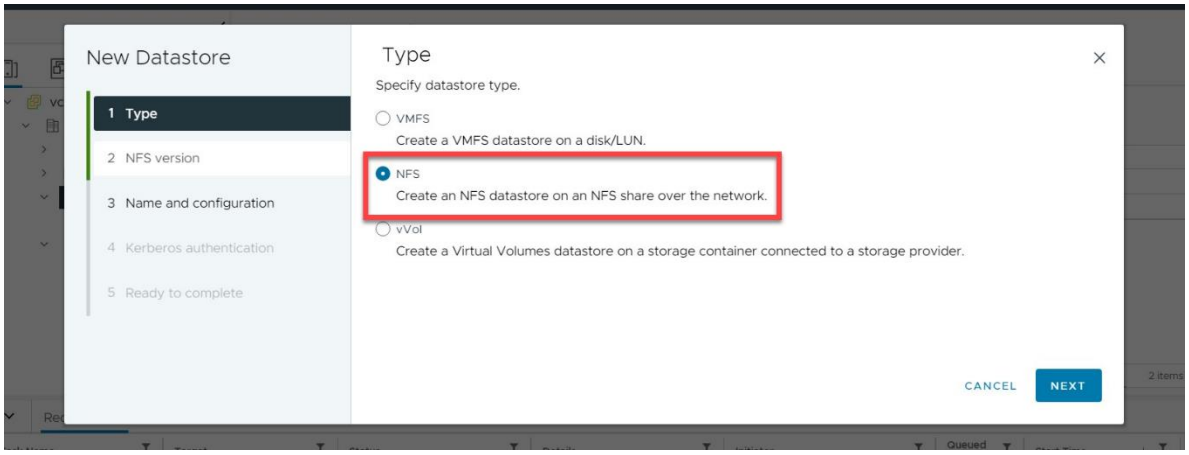
Creating an NFS datastore in vSphere using a Windows Server involves setting up the NFS Server role on the Windows machine and then configuring vSphere to mount the NFS share as a datastore. Here's a step-by-step guide on how to achieve this:

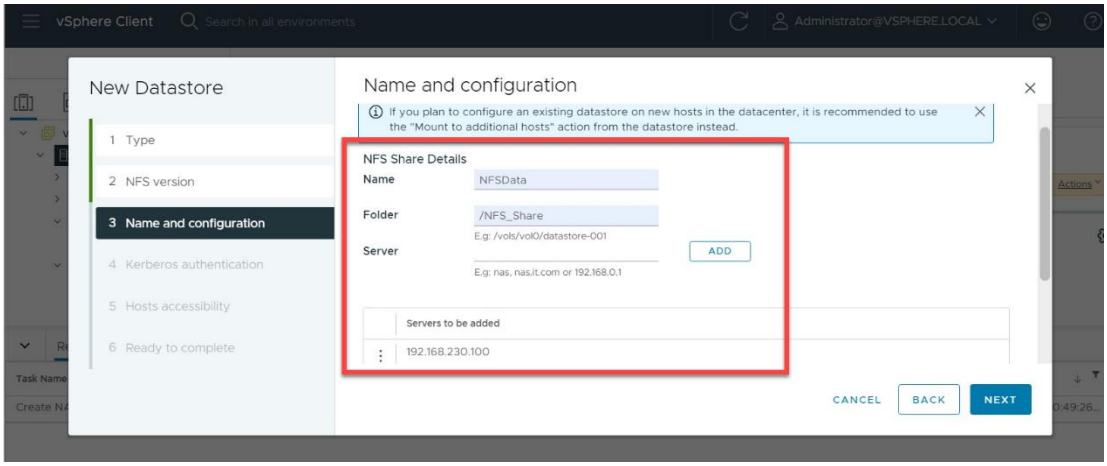


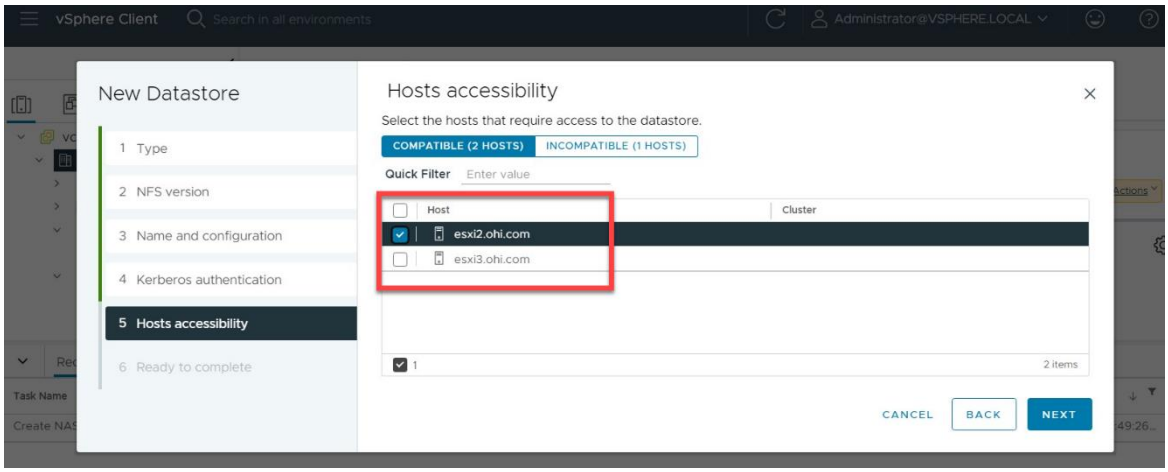


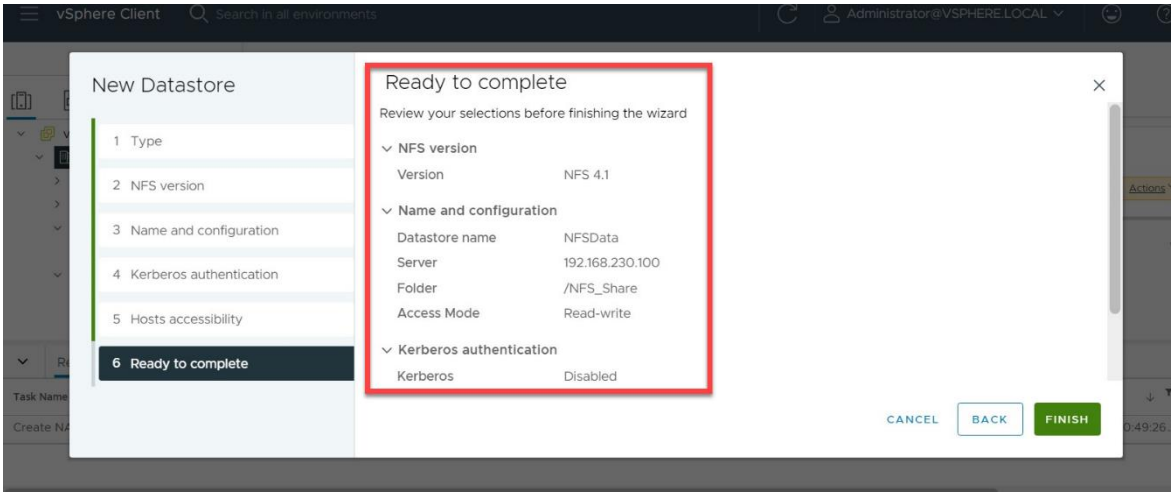
The upcoming configuration will enable NFS on all ESXi servers in the datacenter, and these steps can be replicated at the ESXi level.





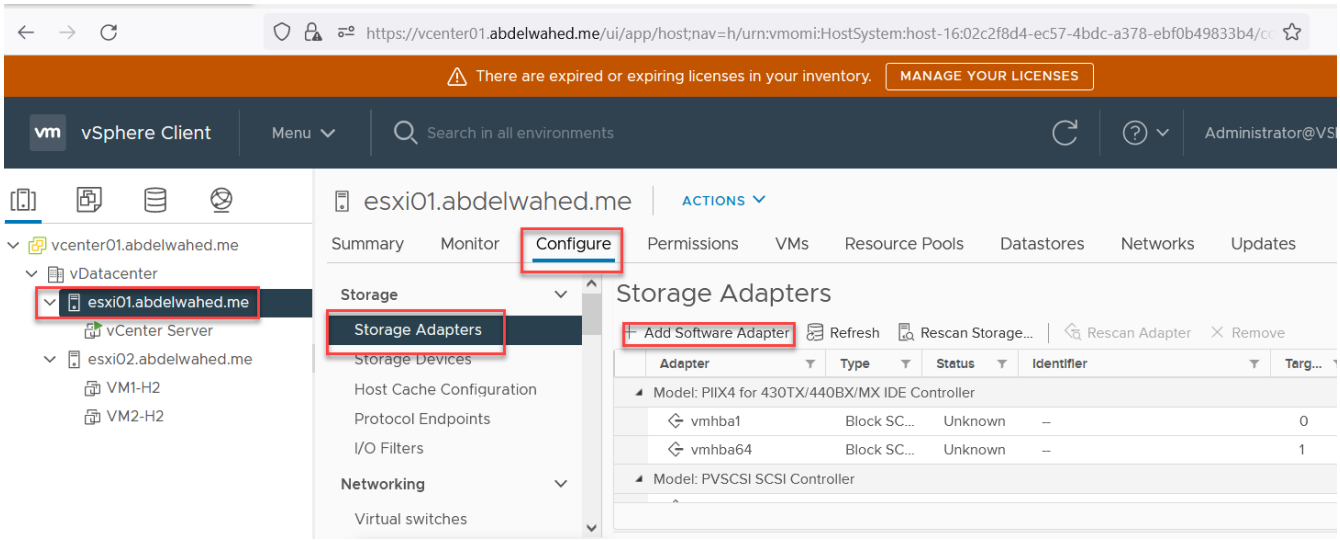



vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
New Datastore
1 Type
2 NFS version
3 Name and configuration
4 Kerberos authentication
5 Hosts accessibility
6 Ready to complete
Hosts accessibility
Select the hosts that require access to the datastore.
COMPATIBLE (2 HOSTS)
INCOMPATIBLE (1 HOSTS)
Quick Filter
Enter value
Host
Cluster
esxi2.ohi.com
esxi3.ohi.com
1
2 items
CANCEL
BACK
NEXT

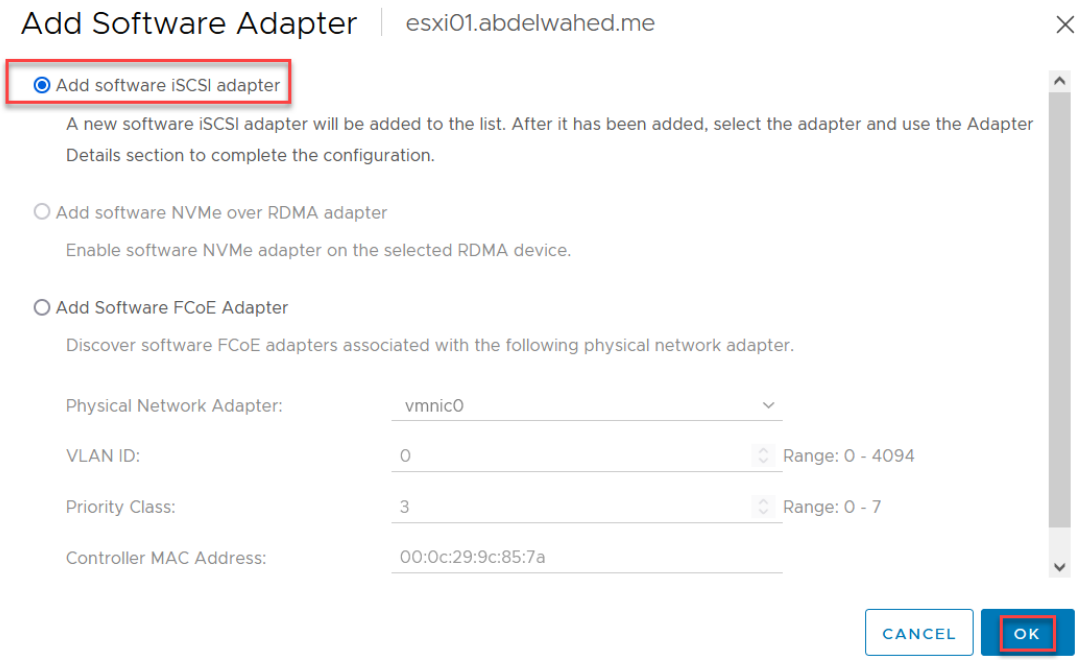

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
New Datastore
1 Type
2 NFS version
3 Name and configuration
4 Kerberos authentication
5 Hosts accessibility
6 Ready to complete
Ready to complete
Review your selections before finishing the wizard
NFS version
Version
NFS 4.1
Name and configuration
Datastore name
NFSData
Server
192.168.230.100
Folder
/NFS_Share
Access Mode
Read-write
Kerberos authentication
Kerberos
Disabled
CANCEL
BACK
FINISH

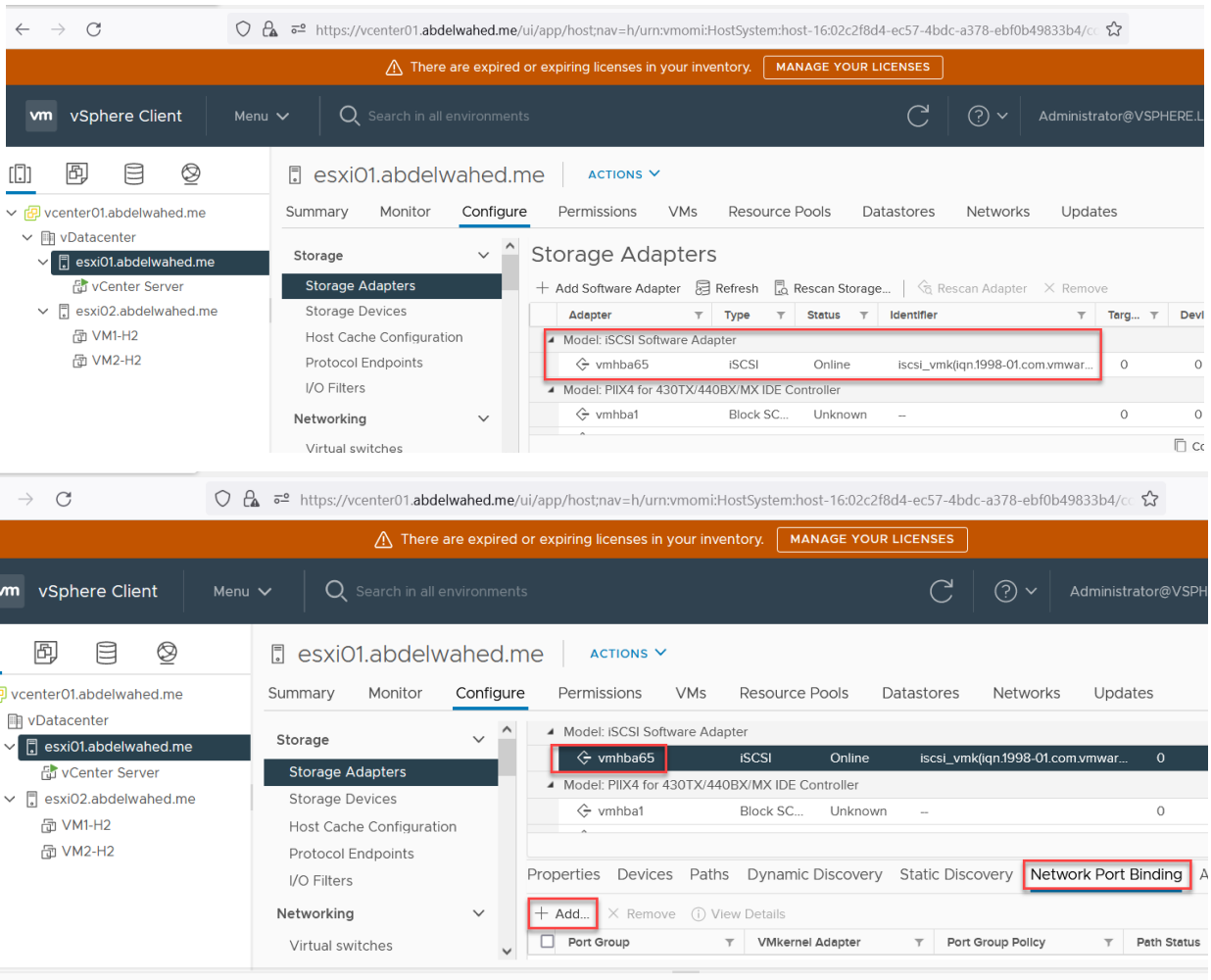
Add ISCSI disk to both ESXi servers using vCenter.

Initially, I set up dc.abdelwahed.me for ISCSI storage and permitted the two ESXI servers access to this storage via the network. In this setup, I utilized two ISCSI disks, with capacities of 800 GB and 700 GB respectively. At this point, the ISCSI software (ISCSI initiator) is used..

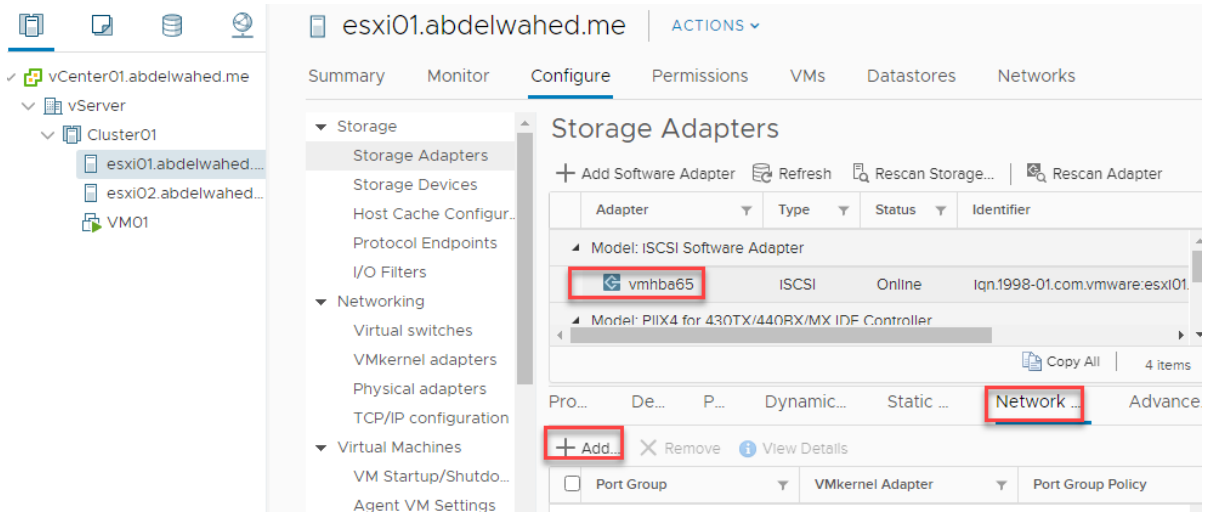


- **NVMe over RDMA Adapter**: Enable this option if using NVMe storage devices that are shared over an RDMA network for high performance.
- **Software FCoE Adapter**: Discover and use software Fibre Channel over Ethernet (FCoE) adapters.

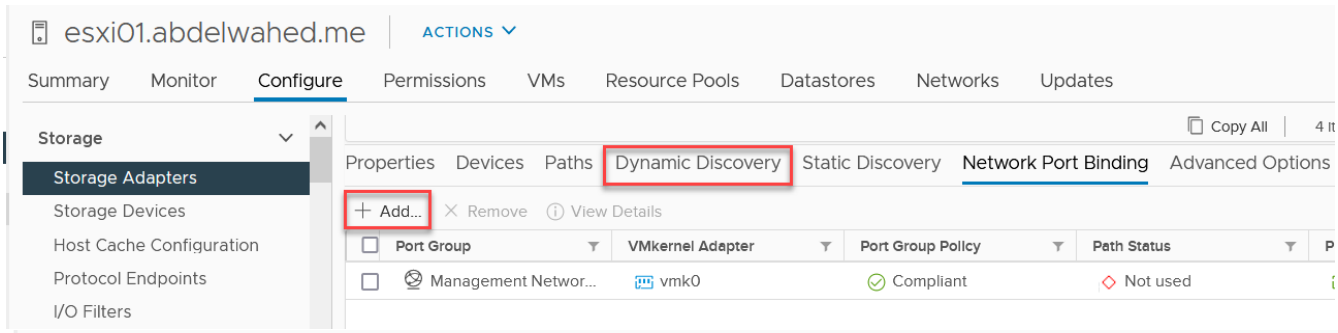


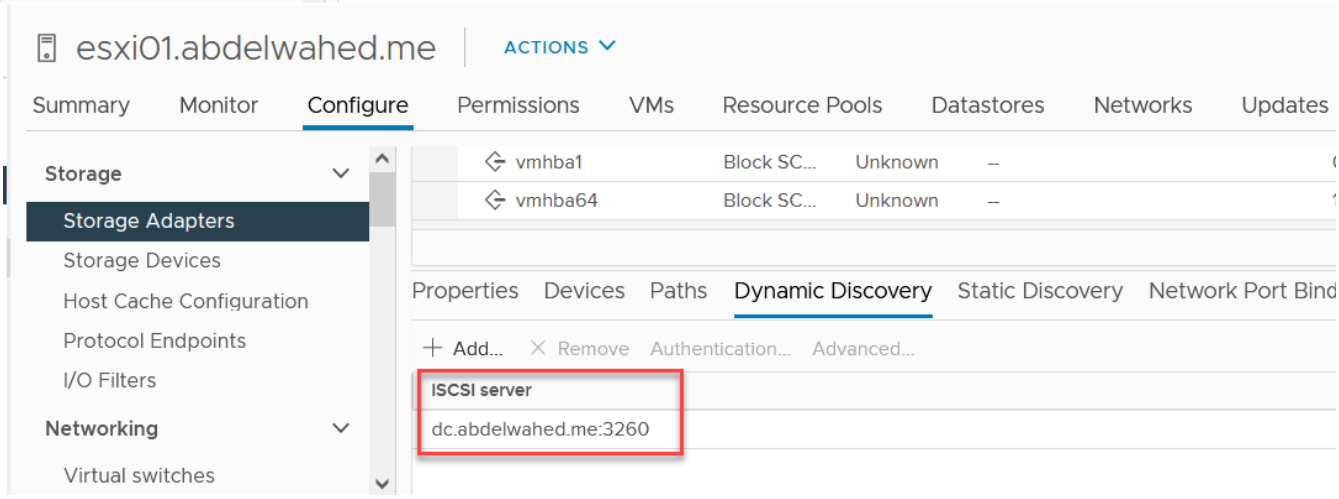


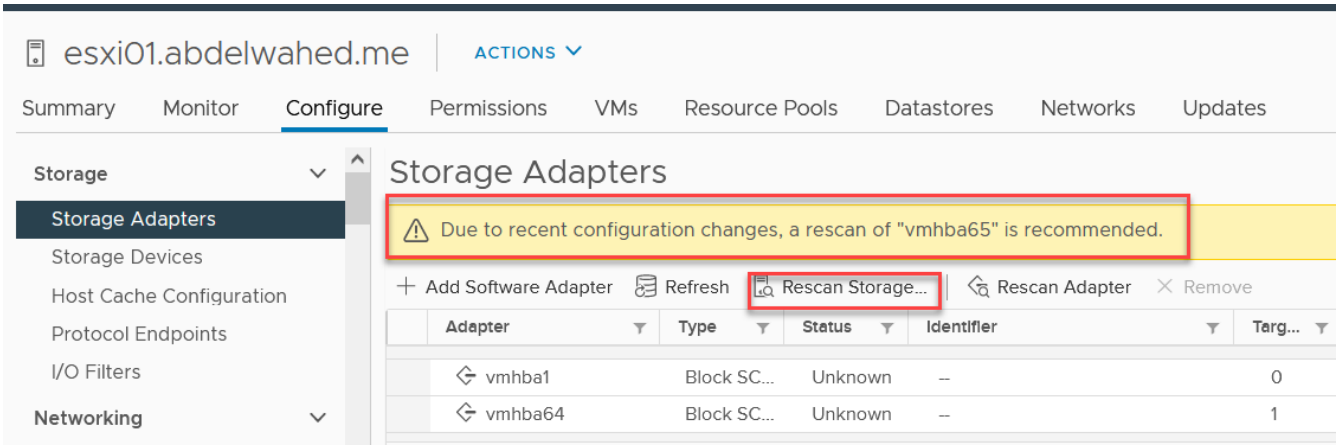
Link the ISCSI software you installed to the network adapter.

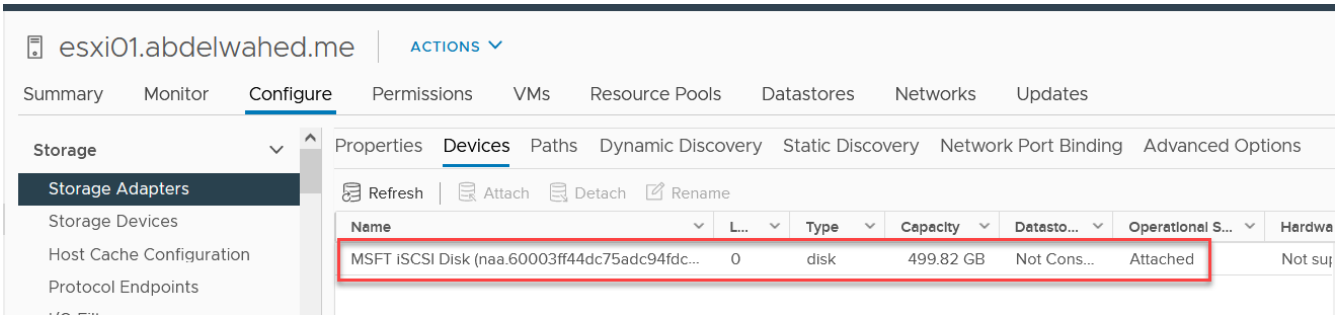


VMware vSphere Install, Configure, Manage | Lab Guide

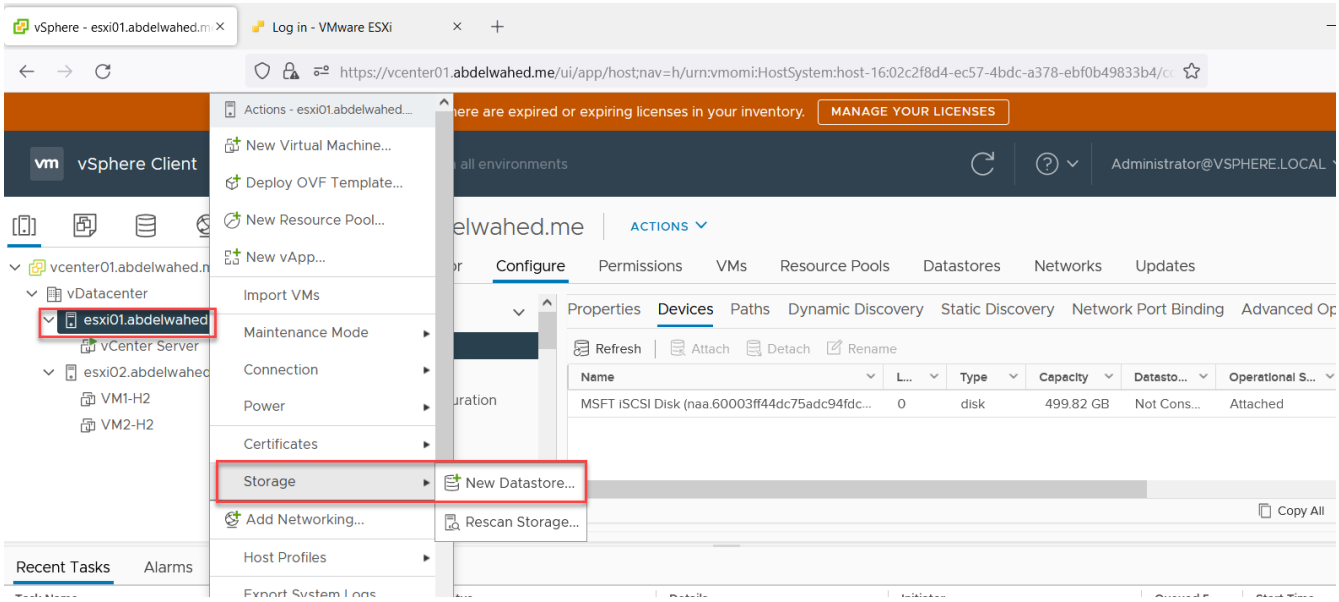


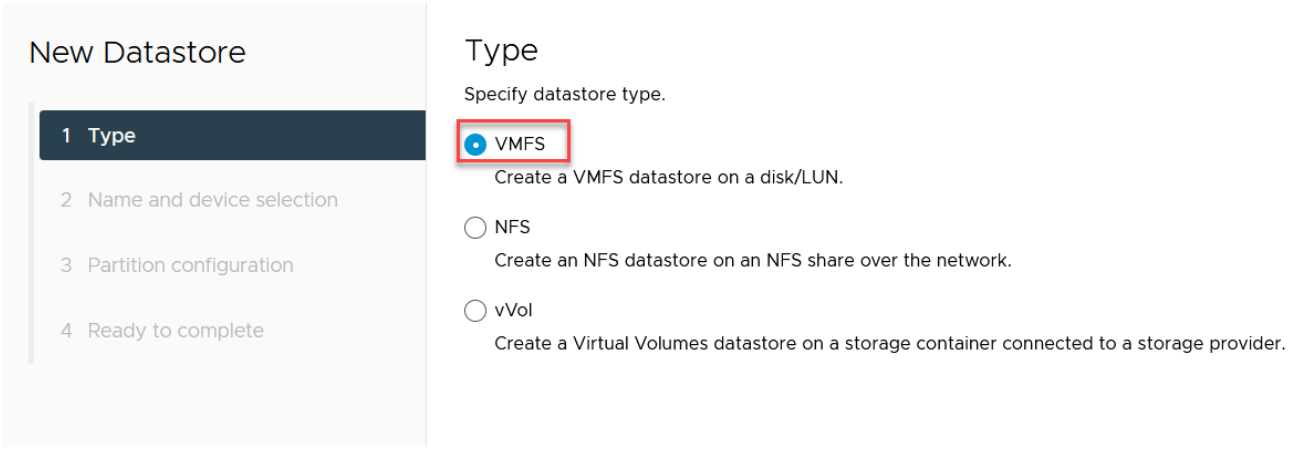


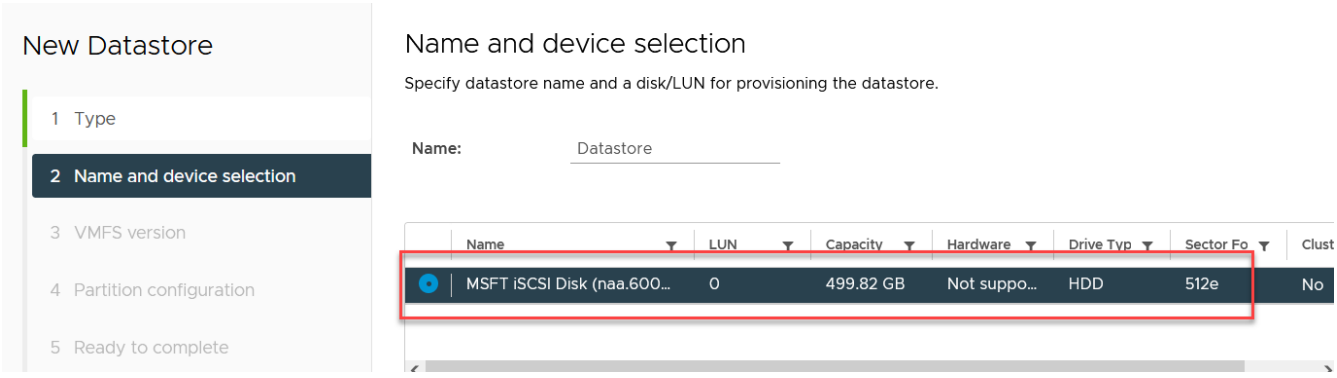


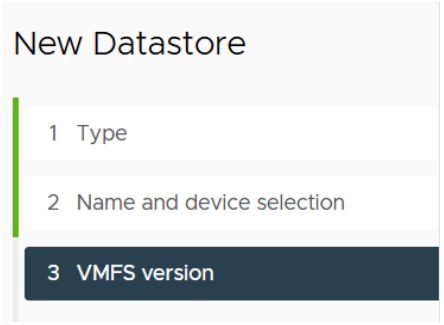


The ISCSI Disk becomes visible and is available for addition as a datastore.





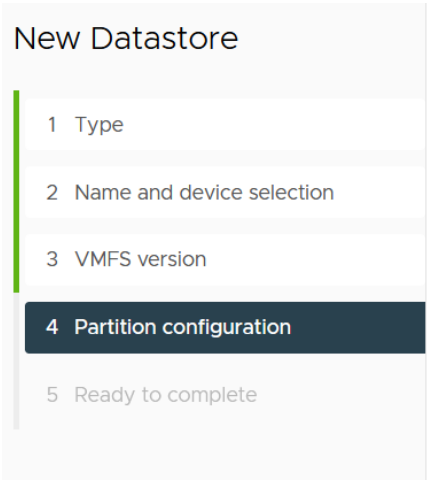




VMFS version

Specify the VMFS version for the datastore.

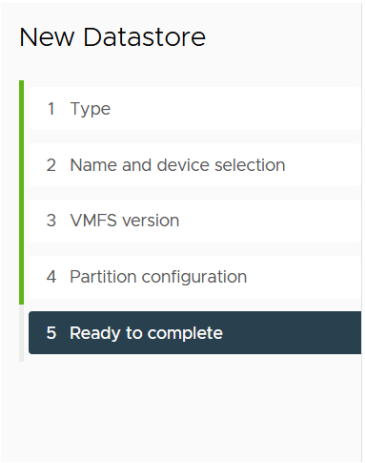
- (•) VMFS 6
  VMFS 6 enables advanced format (512e) and automatic space reclamation support.
- ( ) VMFS 5
  VMFS 5 enables 2+TB LUN support.



Partition configuration

Review the disk layout and specify partition configuration details.

Partition Configuration	Use all available partitions
Datastore Size	499.8 GB
Block size	1 MB
Space Reclamation Granularity	1 MB
Space Reclamation Priority	Low



Ready to complete

Review your settings selections before finishing the wizard.

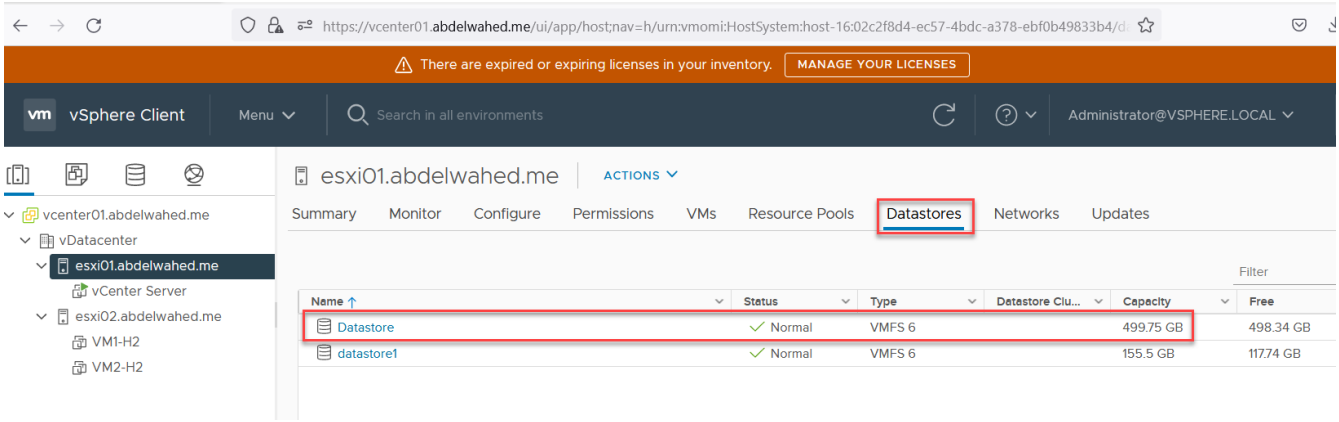
General

Name:	Datastore
Type:	VMFS
Datastore size:	499.82 GB

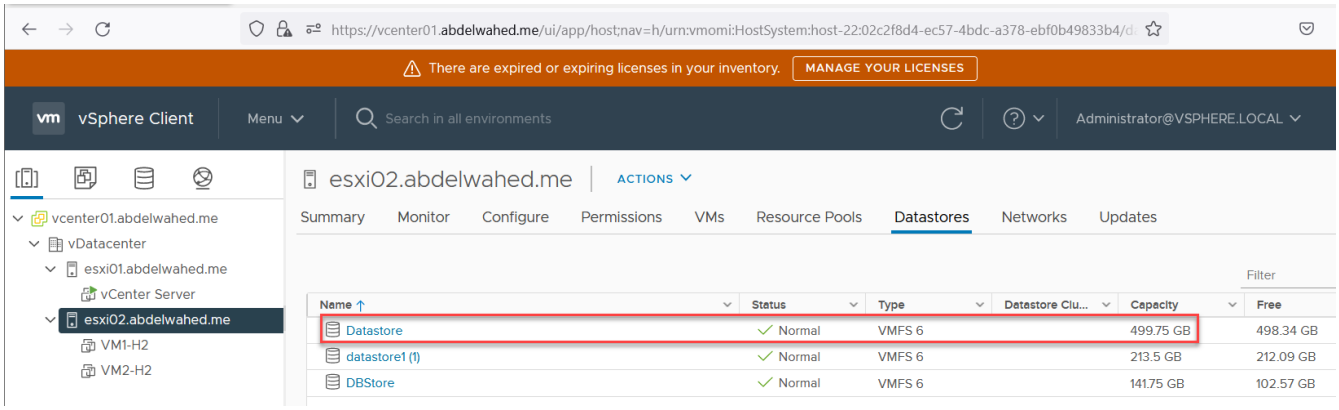
Device and Formatting

Disk/LUN:	MSFT iSCSI Disk (naa.60003ff44dc75adc94fdc2b8b8c3c3e6)
Partition Format:	GPT
VMFS Version:	VMFS 6

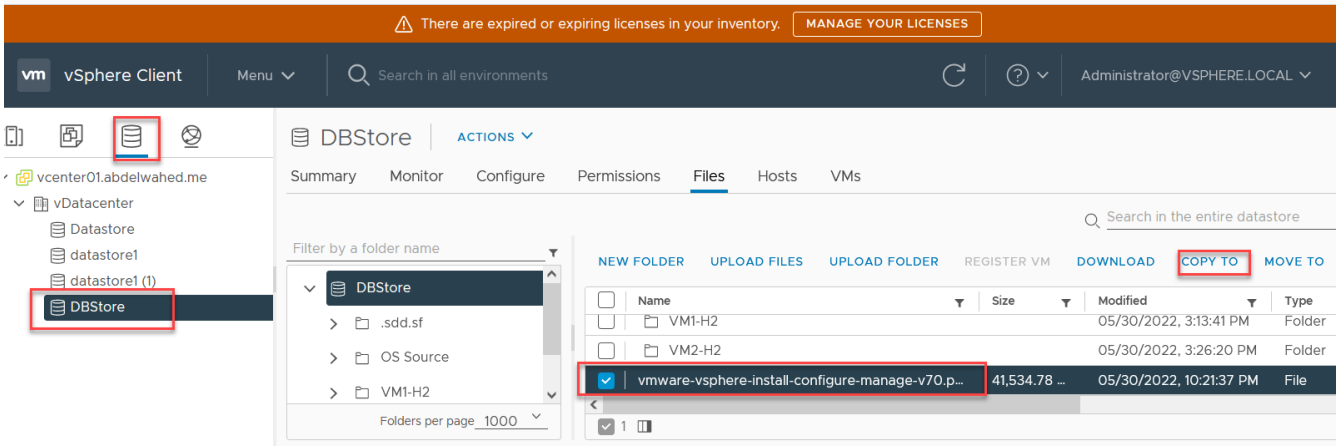
CANCEL BACK FINISH

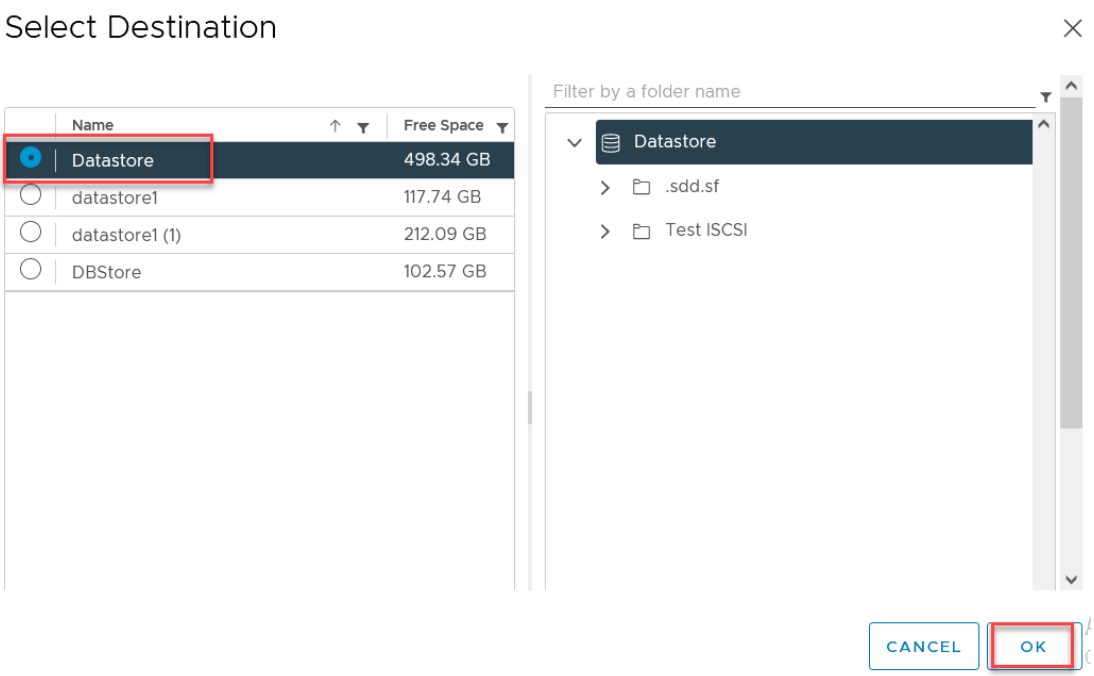


Now, do the same for ESXi02. We won't add a new datastore; we just want to connect it.



Please proceed to upload files to the ISCSI storage.




Select Destination
Name
Free Space
Datastore
498.34 GB
datastore1
117.74 GB
datastore1 (1)
212.09 GB
DBStore
102.57 GB
Filter by a folder name
Datastore
.sdd.sf
Test ISCSI
CANCEL
OK

Migrate VM to Another iSCSI Datastore

Cold Migration (Without vMotion)

Without vMotion enabled, it is not possible to move a virtual machine (VM) during its powered-on state. The only way to move a VM in this state is through a process called "cold migration," which involves powering off the VM, moving its files to another location, and then powering it back on.

Hot Migration (With vMotion)

On the other hand, with vSphere vMotion, it is possible to move a VM while it is in a powered-on state, without any disruption to its services. This type of migration is often referred to as "hot migration" or "live migration," and it is a key feature of vSphere that allows for more flexibility and agility in managing virtual environments.

Key Points About vSphere vMotion

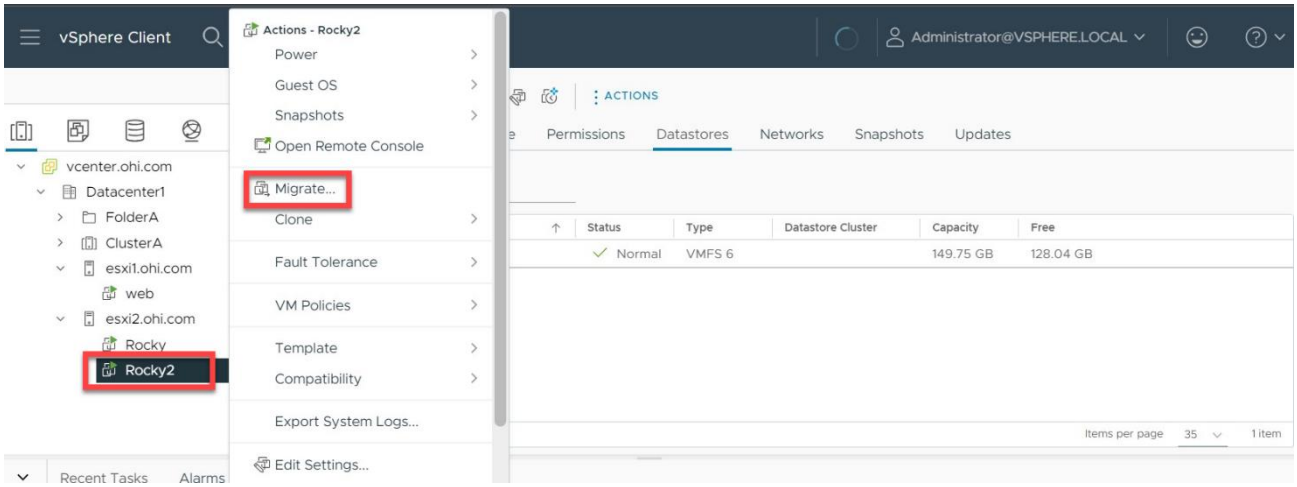
- **Live Migration**: vSphere vMotion enables the live migration of a running virtual machine from one host to another with zero downtime.
- **Use Cases**: You can move virtual machines between hosts for load balancing, maintenance, or other reasons, without any disruption to their services.
- **Requirements**:
    - **Shared Storage**: vMotion relies on shared storage accessible by both the source and target hosts.
    - **High-Speed Network Connection**: A high-speed network connection between the hosts is essential.
    - **License**: vSphere Enterprise Plus license is required to use vMotion.

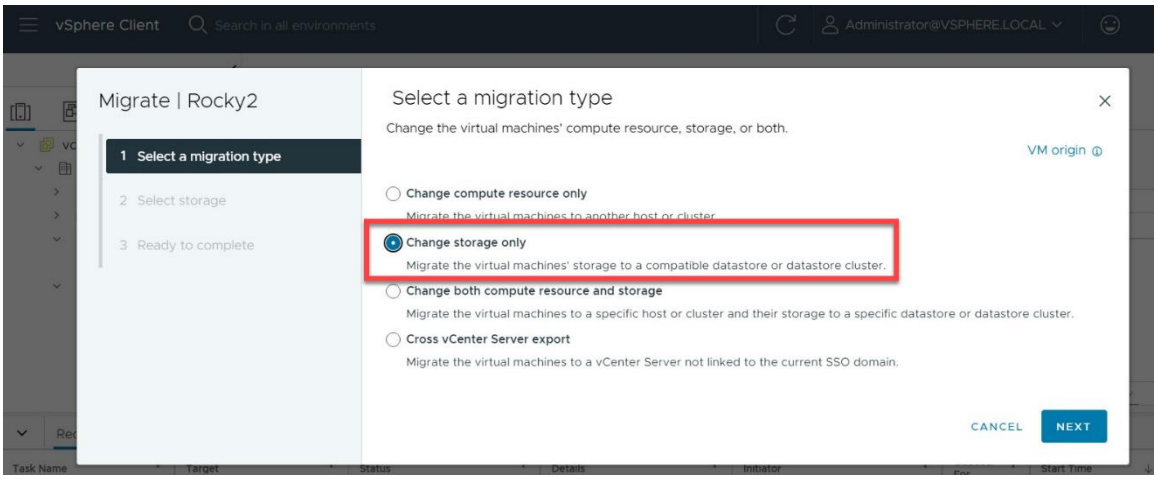
Best Practices for Using vMotion

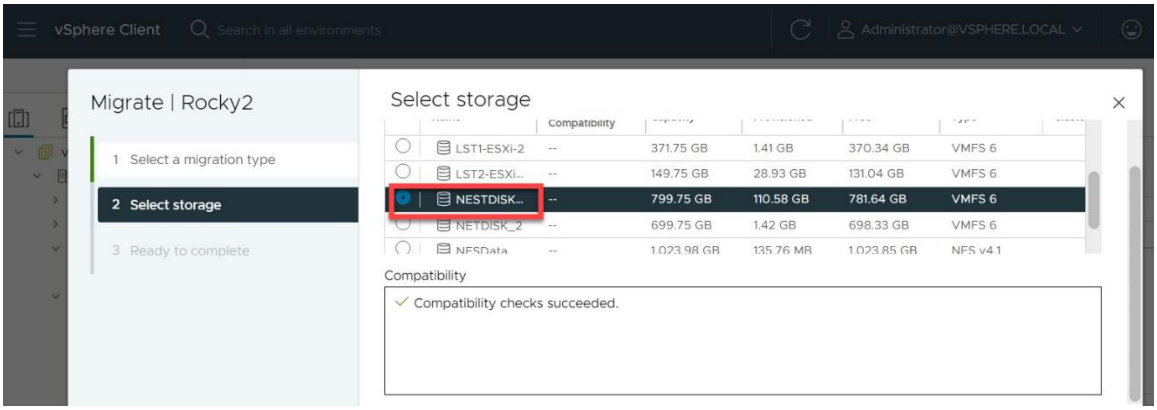
- **Monitor Network and Storage Performance**: Ensure that network and storage resources are sufficient to handle the migration process.
- **Check VM Compatibility**: Verify that the virtual machines are compatible with the target hosts.
- **Secure vMotion**: Implement appropriate permissions and firewall rules to secure the vMotion process.

Cold Migration Without the Need for vMotion

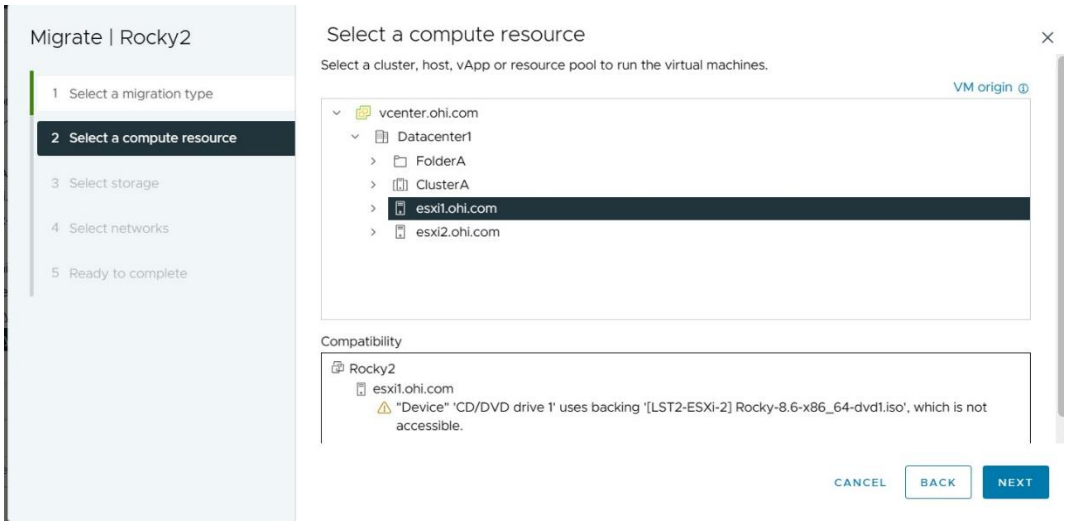
Disk Migration

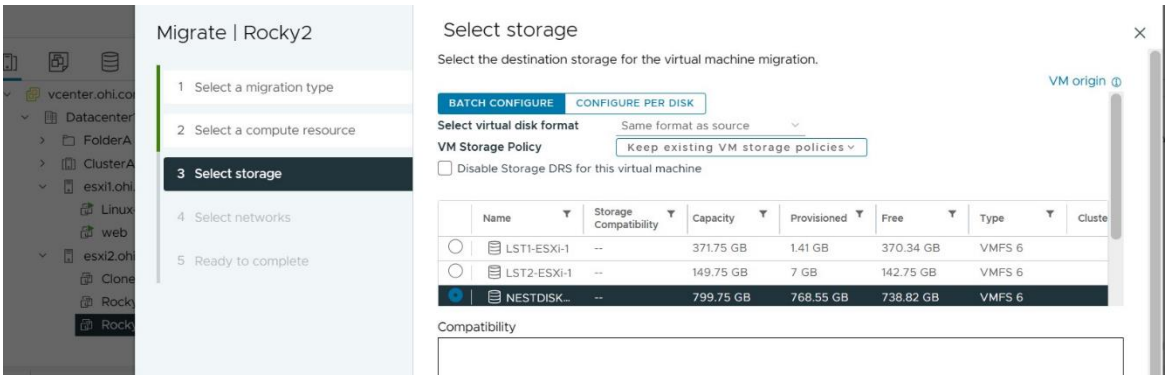


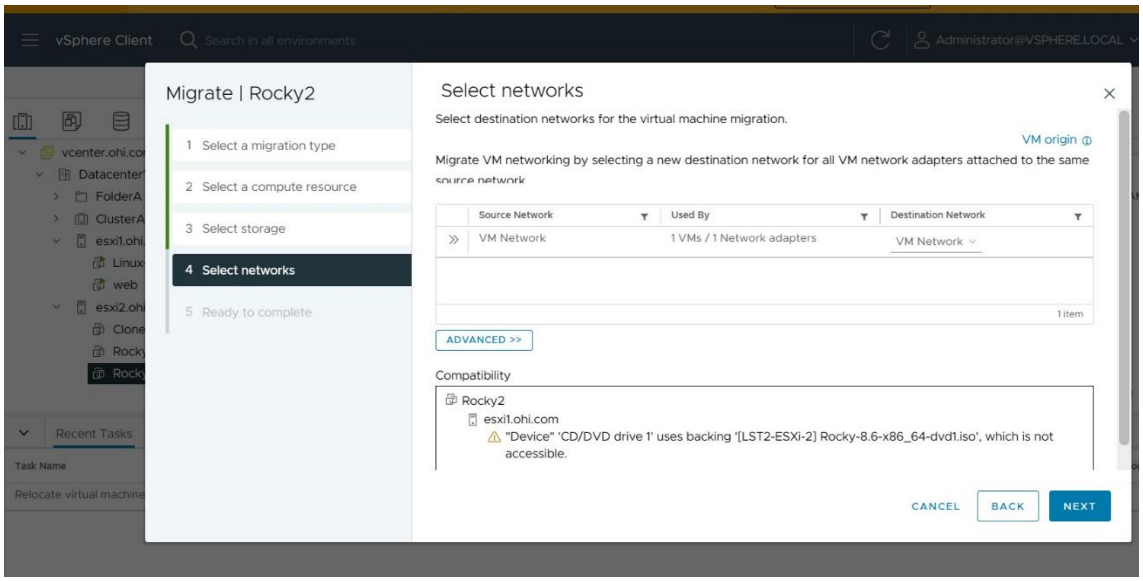




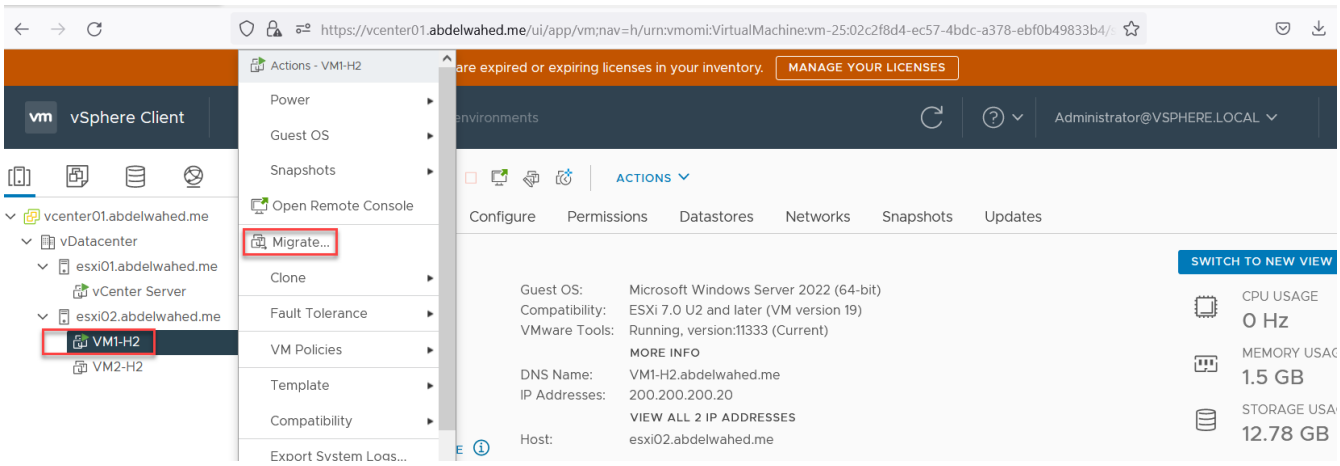
VM Migration (Power off required)

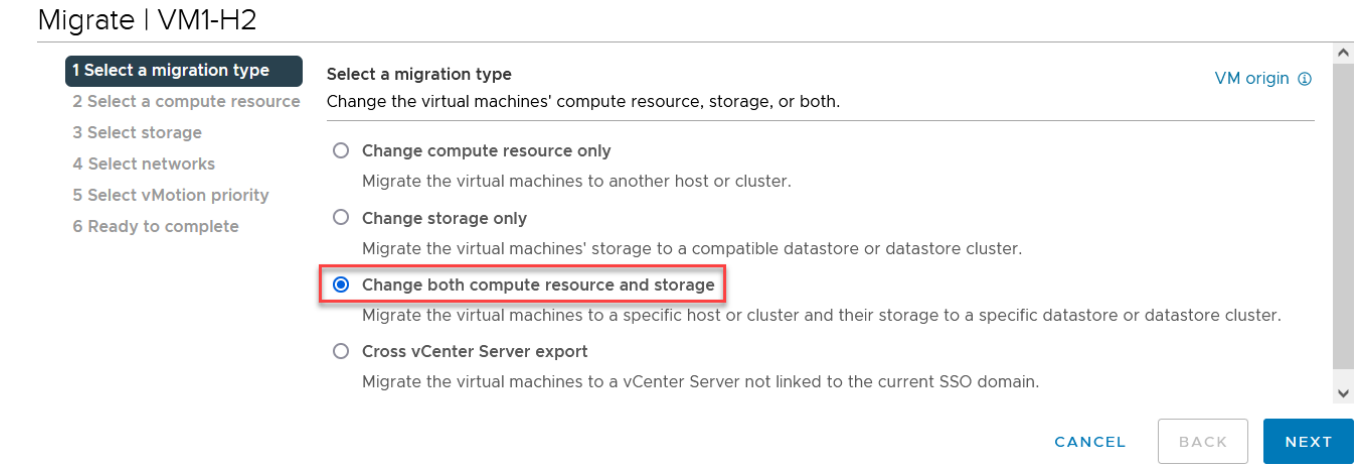


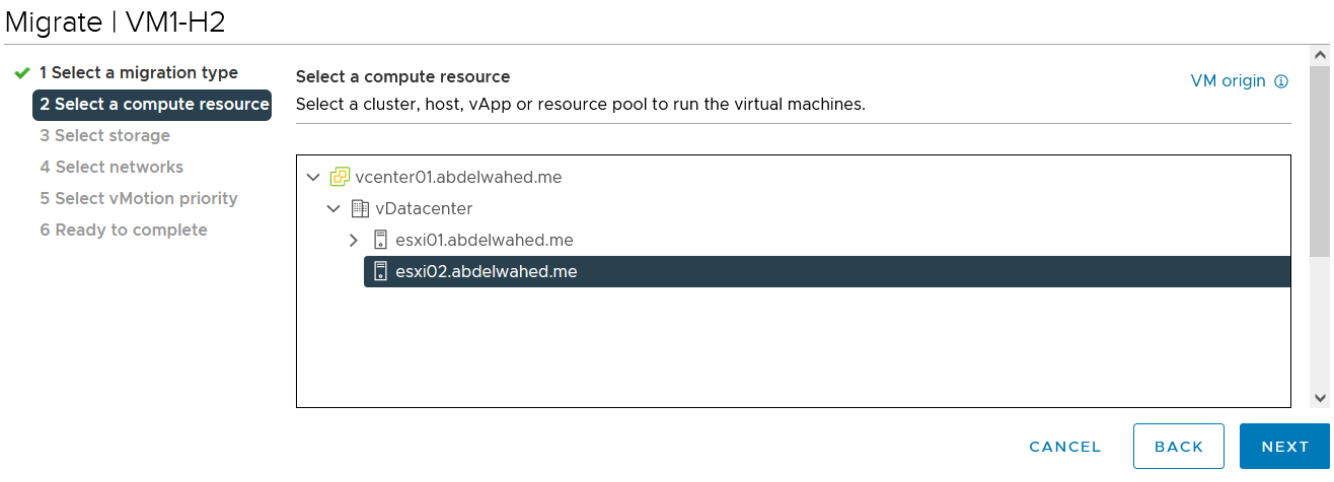




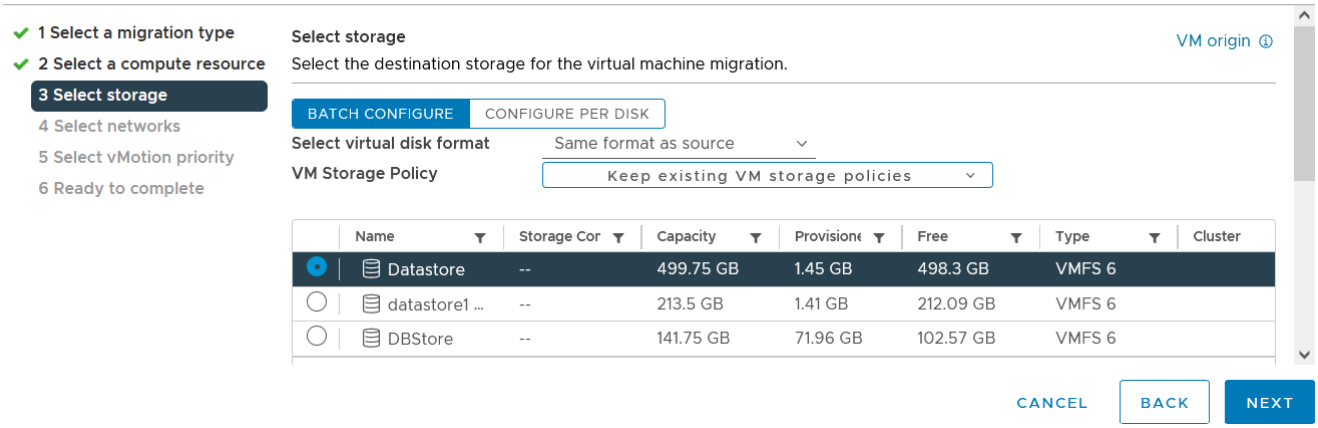
Live Migrate (vMotion needed)



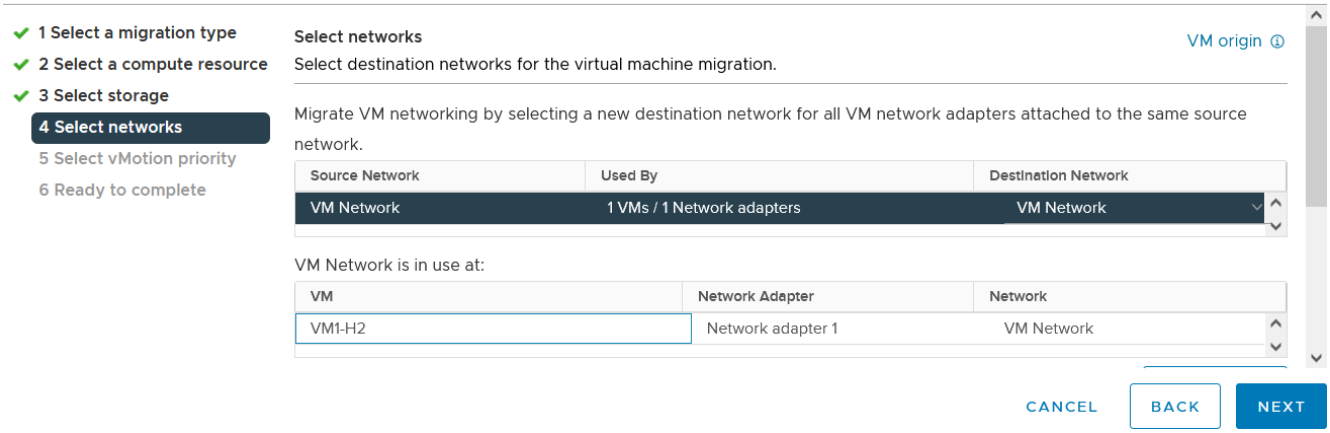




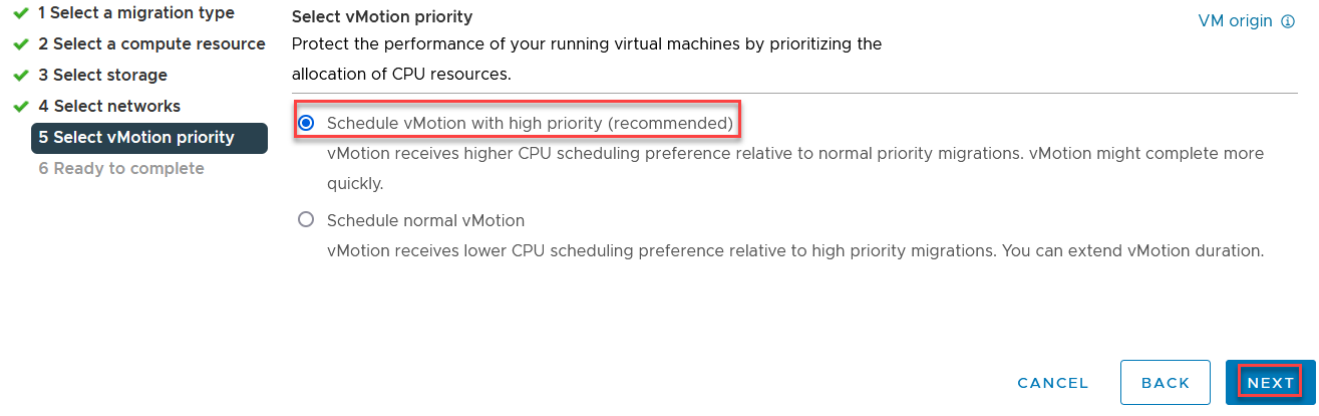
Migrate | VM1-H2

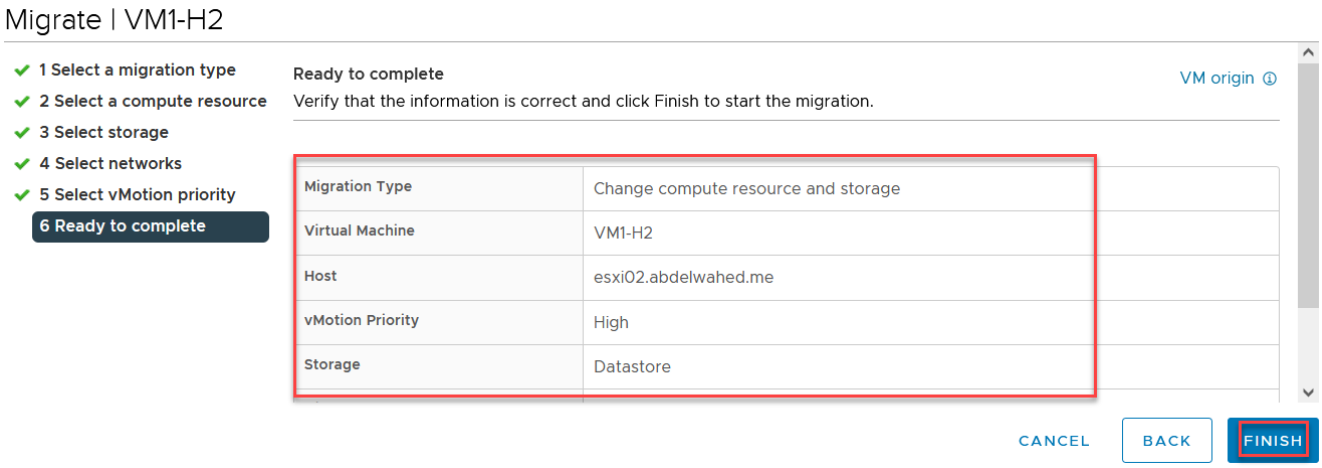


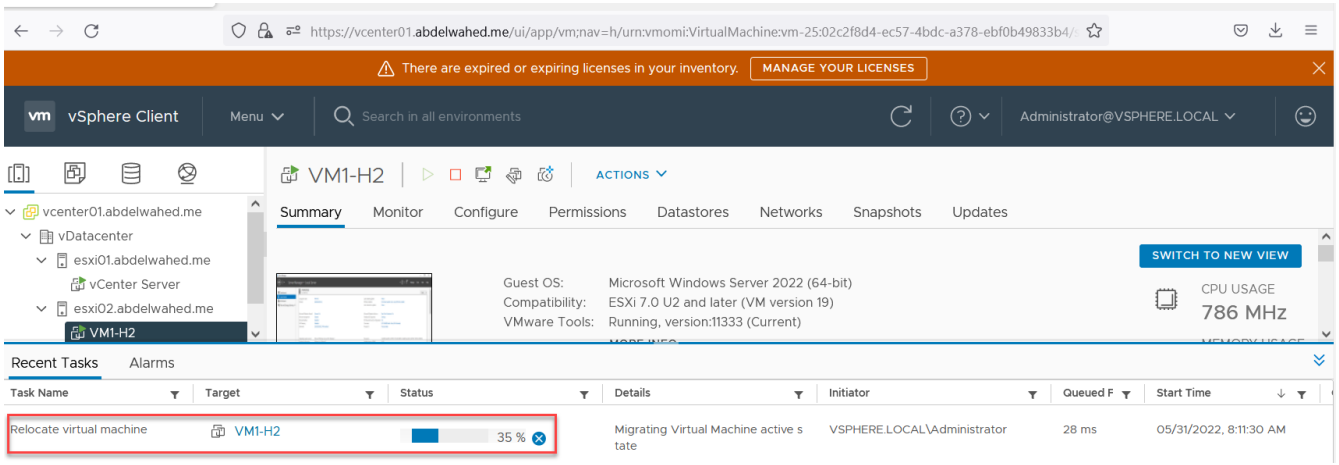
Migrate | VM1-H2

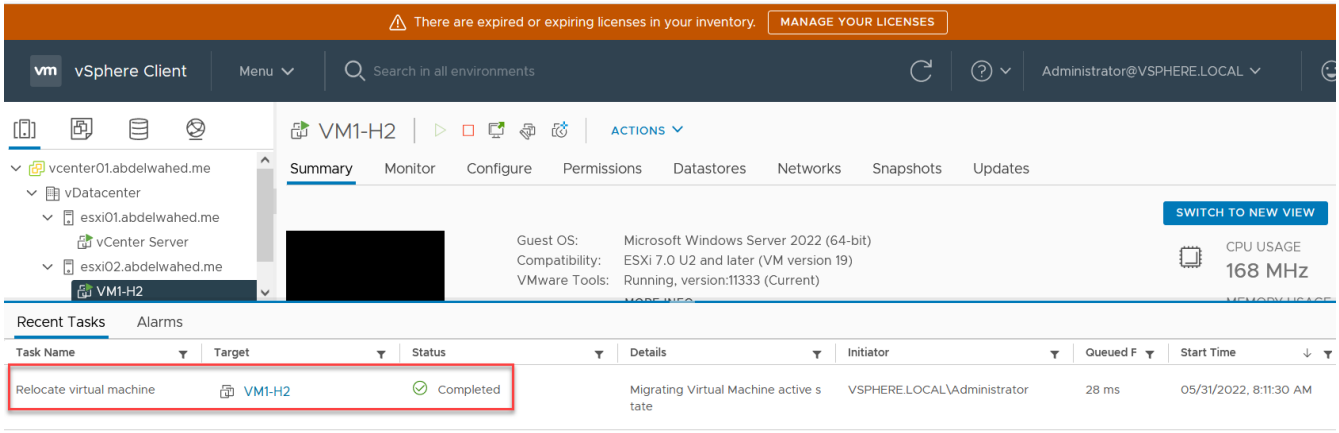


Migrate | VM1-H2




Migrate | VM1-H2
1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Select vMotion priority
6 Ready to complete
Ready to complete
Verify that the information is correct and click Finish to start the migration.
VM origin
Migration Type
Change compute resource and storage
Virtual Machine
VM1-H2
Host
esxi02.abdelwahed.me
vMotion Priority
High
Storage
Datastore
CANCEL
BACK
FINISH


There are expired or expiring licenses in your inventory.
MANAGE YOUR LICENSES
vSphere Client
Menu
Search in all environments
Administrator@VSPHERE.LOCAL
VM1-H2
ACTIONS
Summary
Monitor
Configure
Permissions
Datastores
Networks
Snapshots
Updates
vcenter01.abdelwahed.me
vDatacenter
esxi01.abdelwahed.me
vCenter Server
esxi02.abdelwahed.me
VM1-H2
SWITCH TO NEW VIEW
Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11333 (Current)
CPU USAGE
786 MHz
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued F
Start Time
Relocate virtual machine
VM1-H2
35 %
Migrating Virtual Machine active s tate
VSPHERE.LOCAL\Administrator
28 ms
05/31/2022, 8:11:30 AM


There are expired or expiring licenses in your inventory.
MANAGE YOUR LICENSES
vSphere Client
Menu
Search in all environments
Administrator@VSPHERE.LOCAL
VM1-H2
ACTIONS
Summary
Monitor
Configure
Permissions
Datastores
Networks
Snapshots
Updates
vcenter01.abdelwahed.me
vDatacenter
esxi01.abdelwahed.me
vCenter Server
esxi02.abdelwahed.me
VM1-H2
SWITCH TO NEW VIEW
Guest OS: Microsoft Windows Server 2022 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11333 (Current)
CPU USAGE
168 MHz
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued F
Start Time
Relocate virtual machine
VM1-H2
Completed
Migrating Virtual Machine active s tate
VSPHERE.LOCAL\Administrator
28 ms
05/31/2022, 8:11:30 AM

VM Cloning, Templating, and Snapshot in vSphere

VM Cloning

Cloning involves making an exact copy of a VM. Key points about cloning:

1. **Exact Copy:**
   - A cloned VM is an exact replica of the original VM, including virtual hardware, configuration settings, and data.
2. **Use Cases:**
   - Useful for testing, backup, or disaster recovery.
3. **Any Power State:**
   - Cloning can be done at any time, regardless of the VM's power state.
4. **MAC Address:**
   - Option to keep the same MAC address or generate a new one.
5. **Source VM**:
   - The source VM remains unchanged and functional after cloning.

VM Templating

Templating involves creating a new VM based on a master template. Key points about templating:

1. **Master Copy:**
   - A template is a master copy of a VM used to create new VMs with the same configuration and software settings.
2. **Use Cases:**
   - Useful for creating multiple identical VMs for specific purposes, like web server farms or development environments.
3. **Create Template:**
   - First, create a VM with desired settings, then convert it to a template.
4. **Customization:**
   - When creating a new VM from a template, customize settings and assign a unique name and MAC address.
5. **Source VM**:
   - The source VM is converted into a template and becomes unavailable as a regular VM.

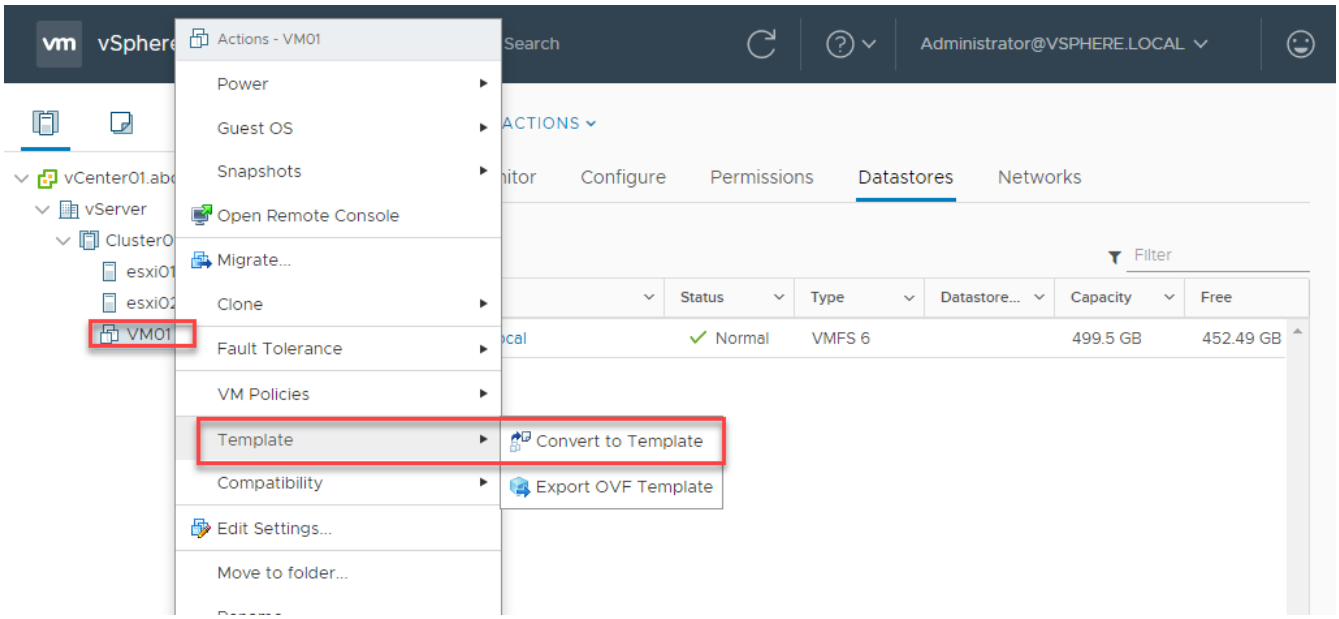
VM Snapshots

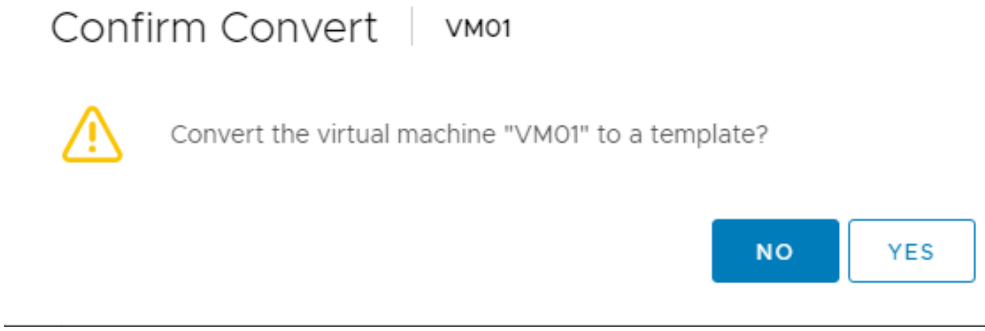
Snapshots capture the state of a VM at a specific point in time. Key points about snapshots:

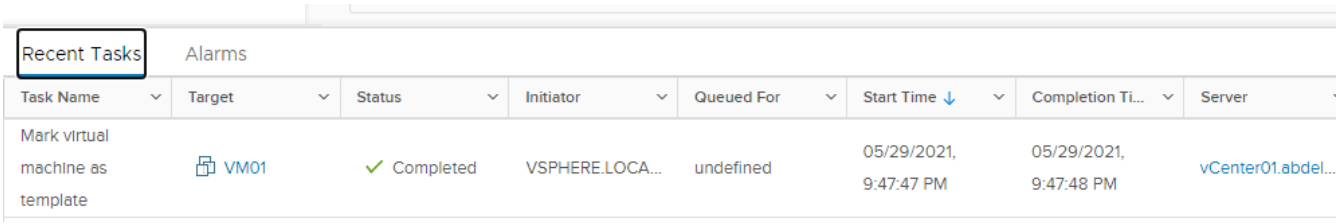
1. **State Capture:**
   - A snapshot captures the state, configuration, and data of a VM at a particular moment.
2. **Revert Changes:**
   - Useful for reverting the VM to a previous state in case of errors or issues during updates or changes.
3. **Multiple Snapshots:**
   - Multiple snapshots can be taken, but it's best to manage and limit the number to avoid performance issues.
4. **Source VM**:
   - The source VM continues to operate normally after taking a snapshot.

Steps to Create a Template:

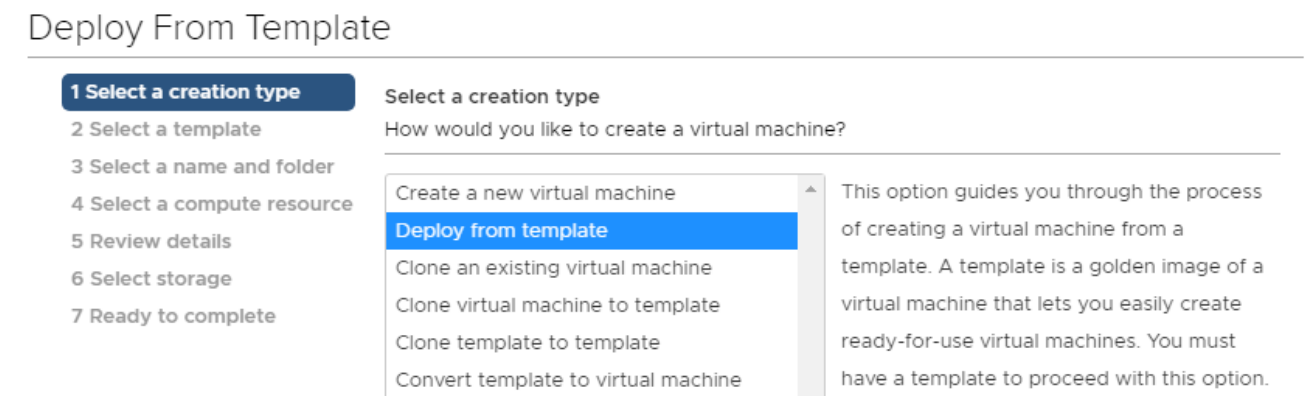
It is essential to turn off the virtual machine (VM) before converting it into a template to secure a consistent and stable condition.

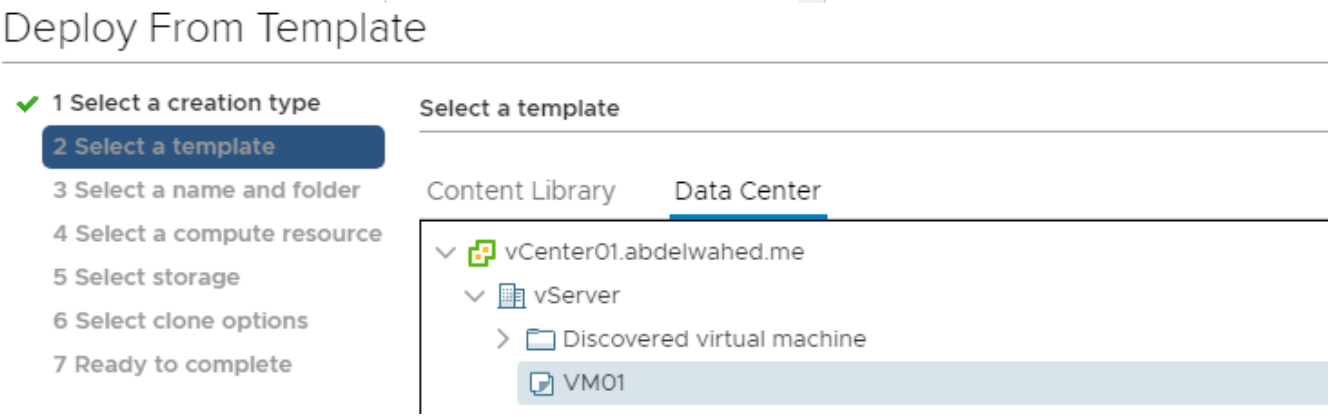


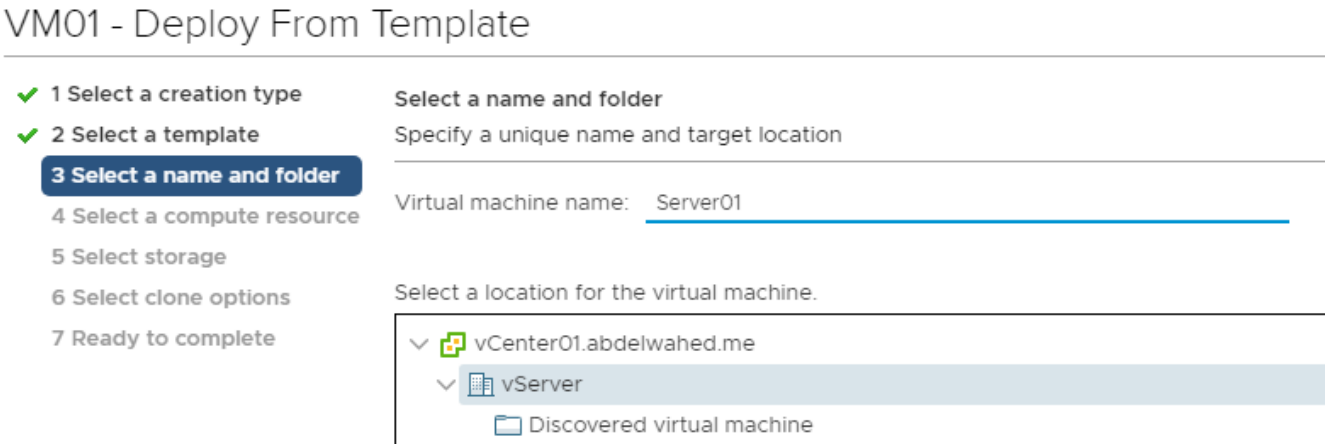


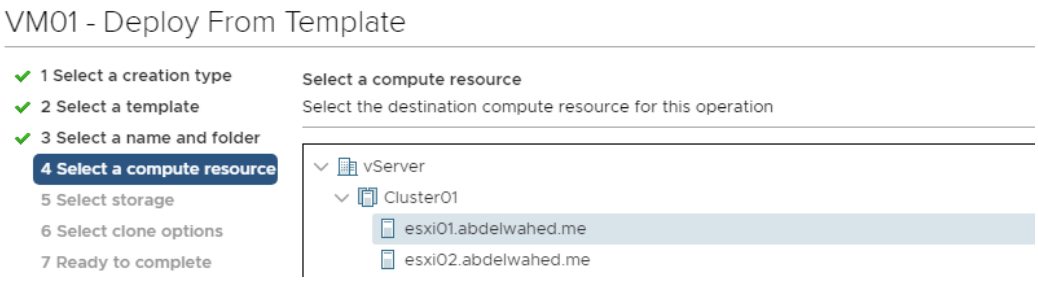


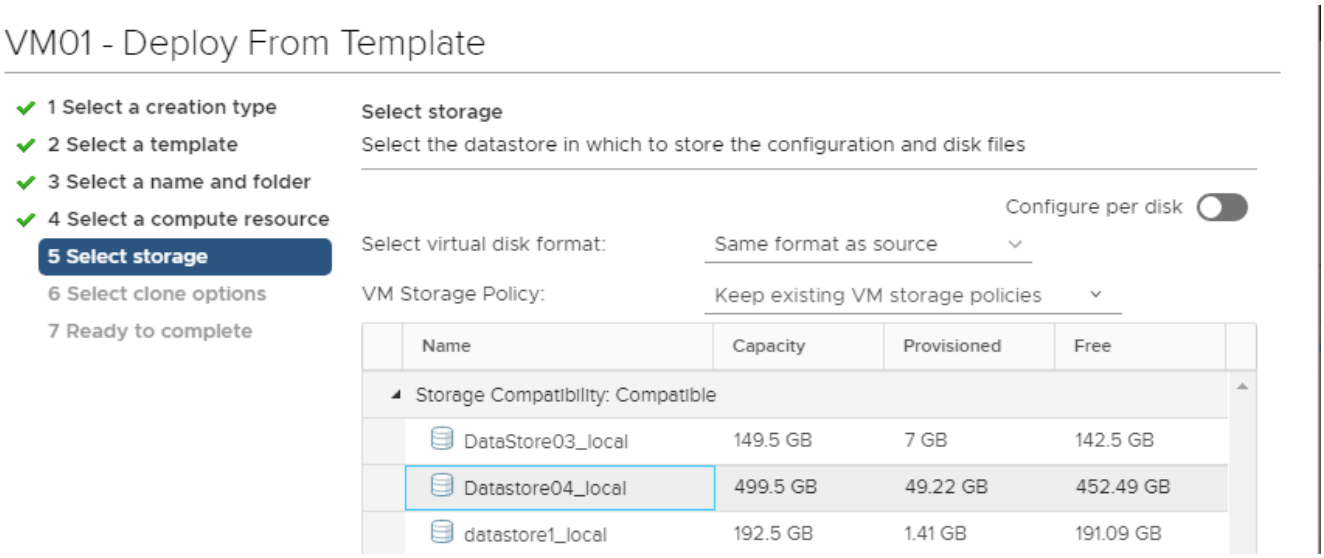
Create a virtual machine using a template.

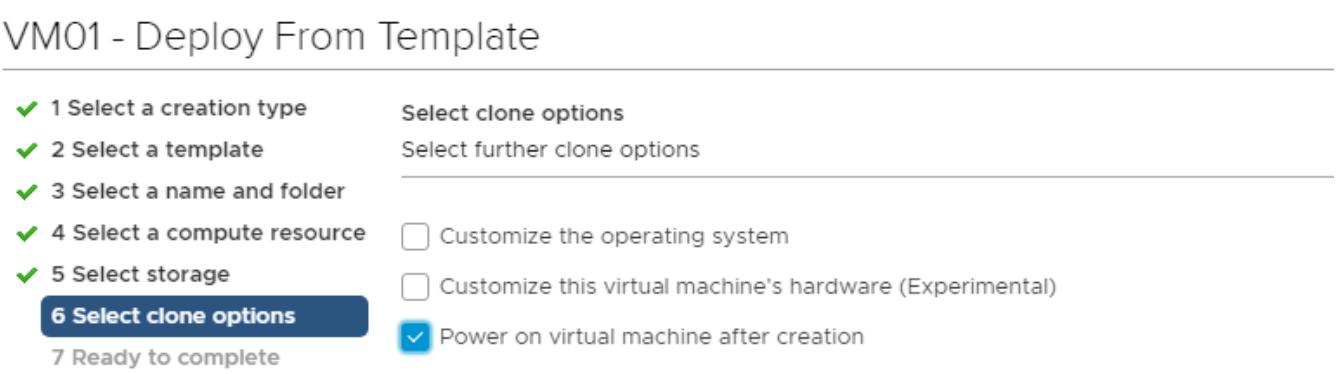




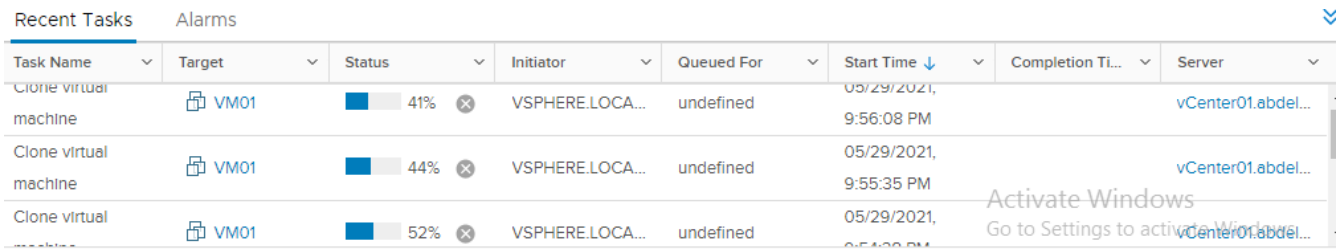






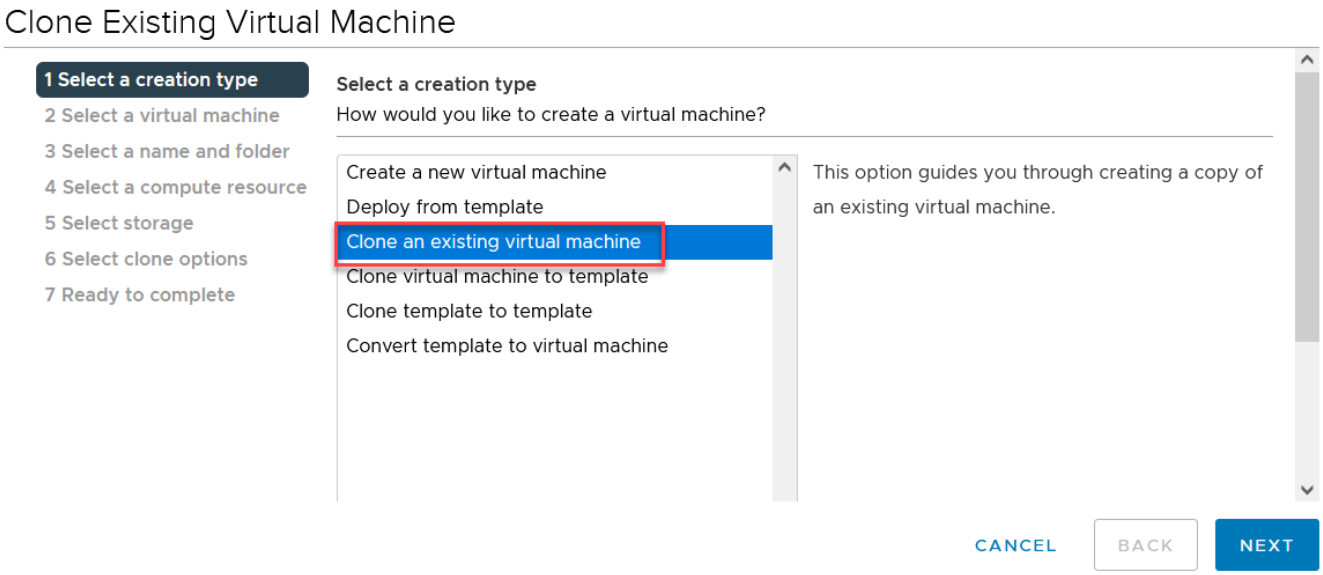


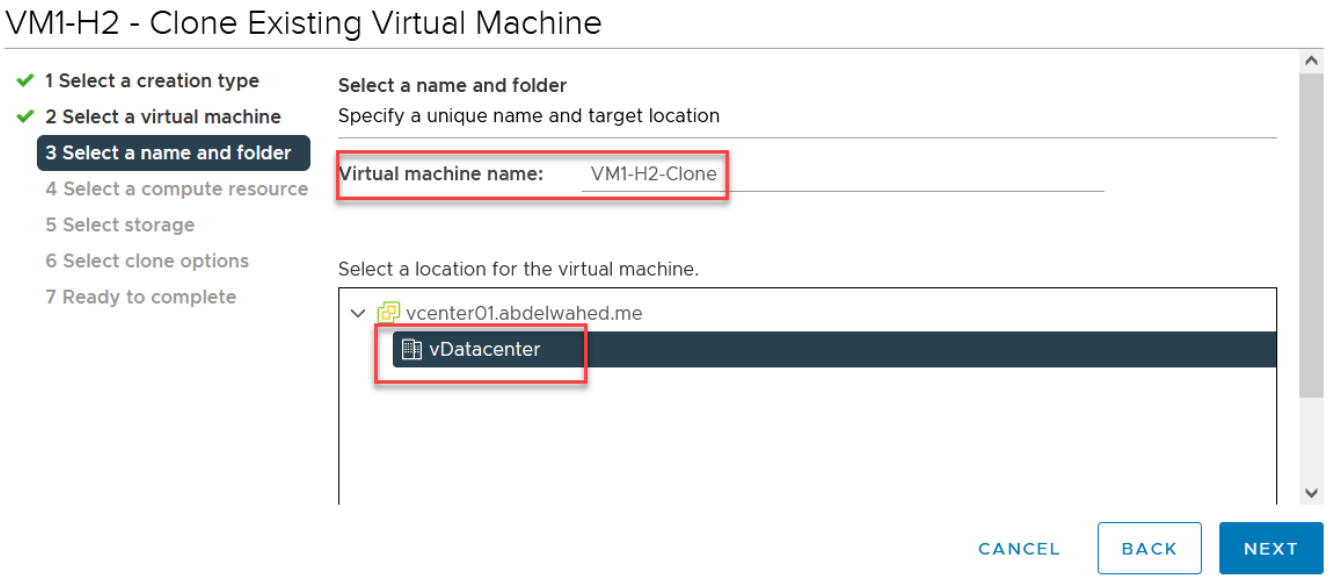
I set up four servers with two VMs on each host.



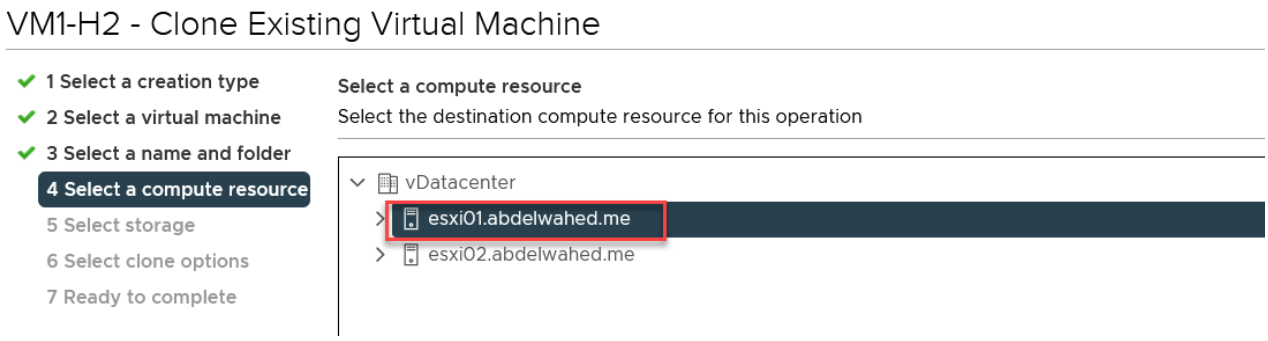
Steps to Clone a VM:

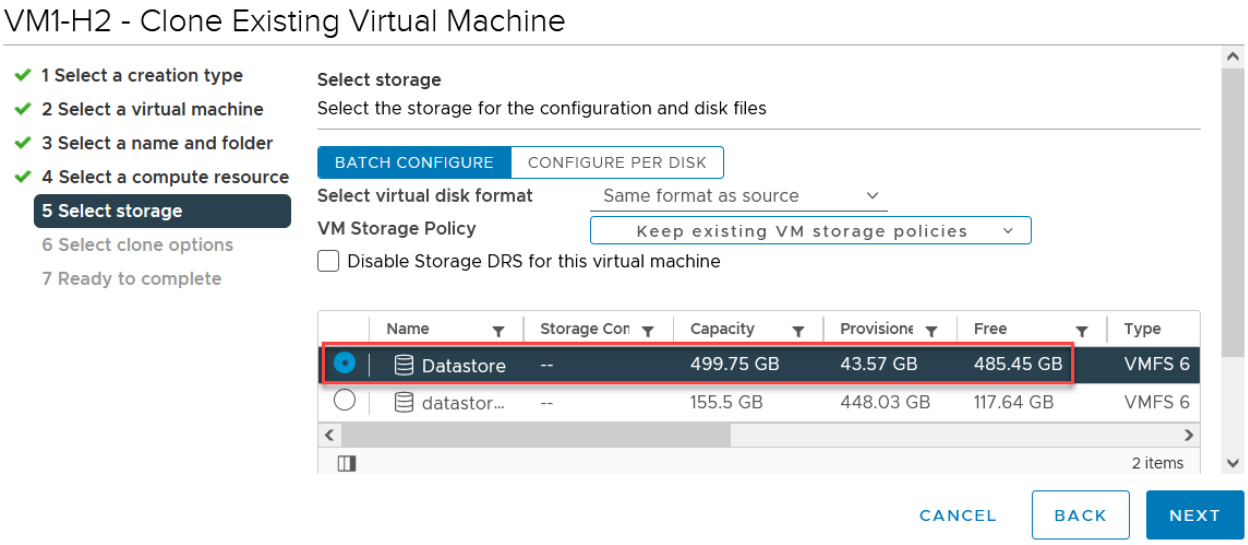
Cloning a running VM will create a new VM that is an exact copy of the source VM, while converting a VM to a template will convert the source VM into a template and make it unavailable as a regular VM. Both cloning and creating a template will generate a new UUID for the new VM or template. You can check the VM's UUID by running the following command on the guest operating system: `wmic path win32_computersystemproduct get uuid`



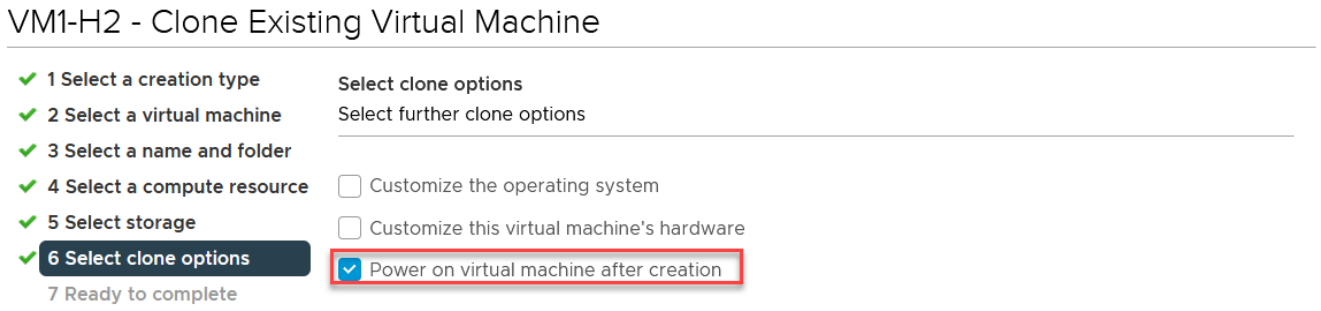


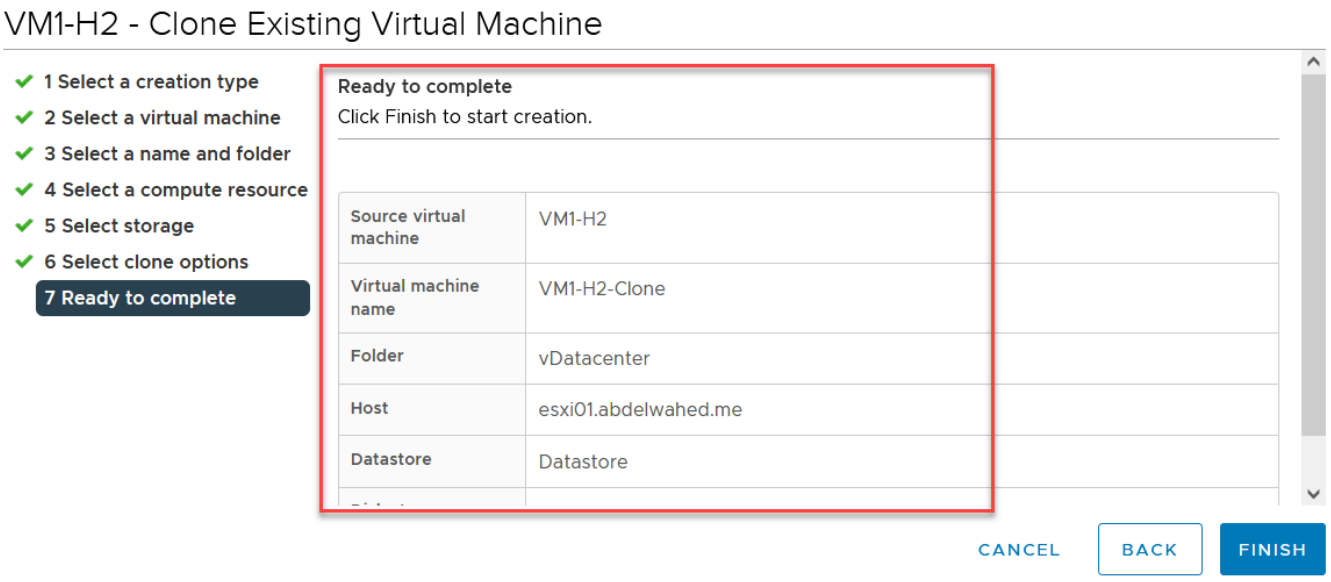
I will be transferring to a different ESXI host.

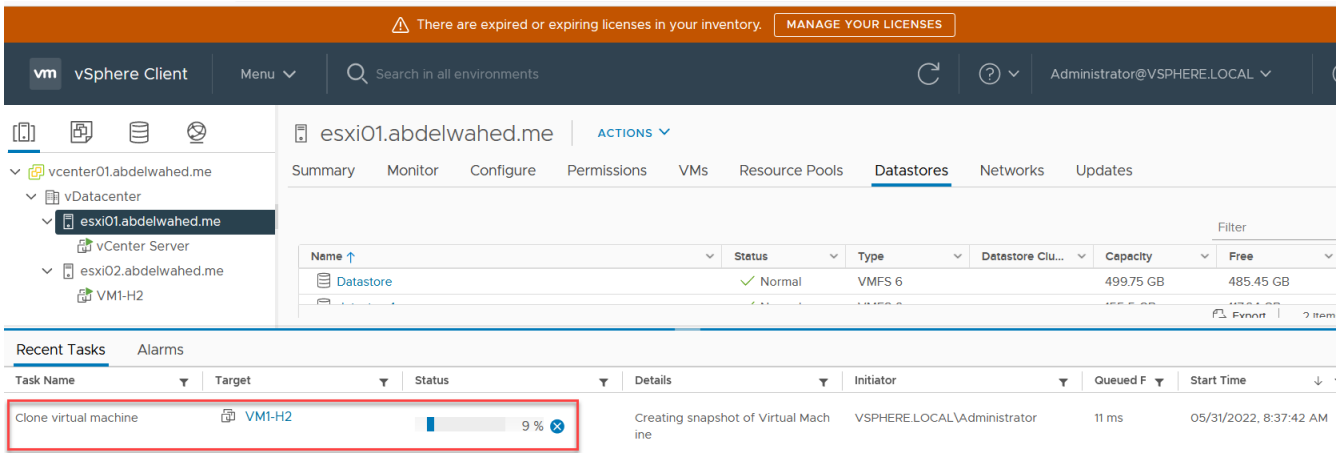


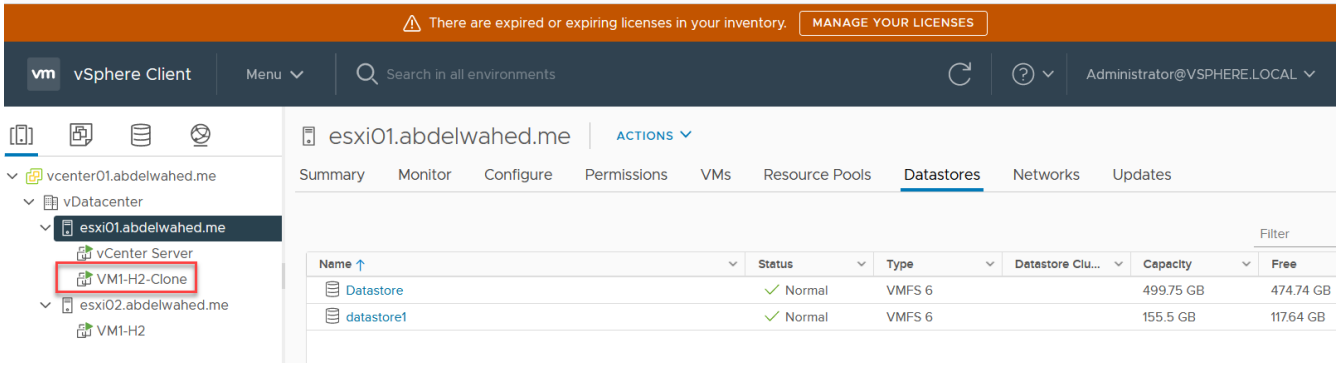


To adjust the hardware settings of a virtual machine, opt for the second choice.

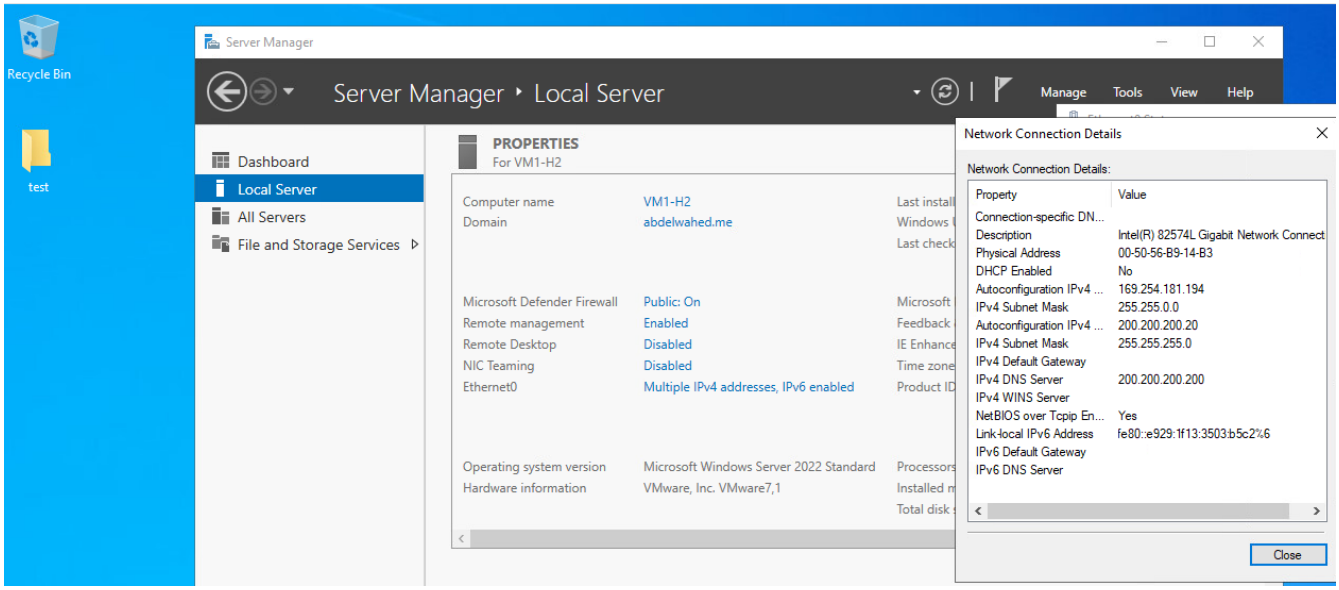




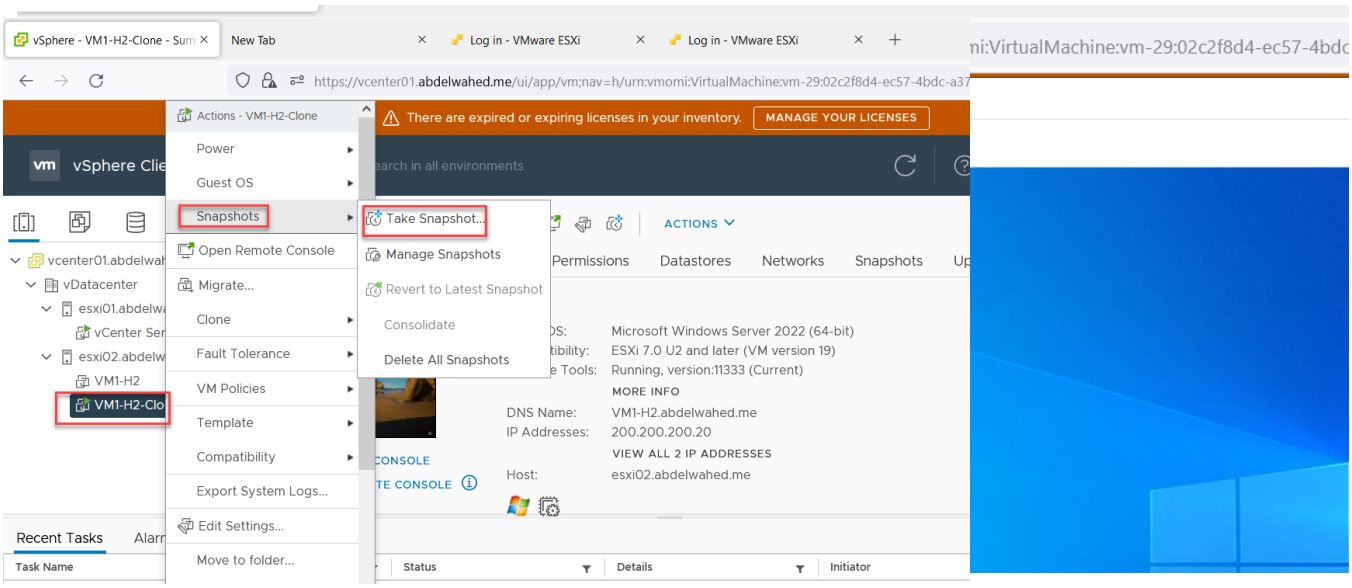


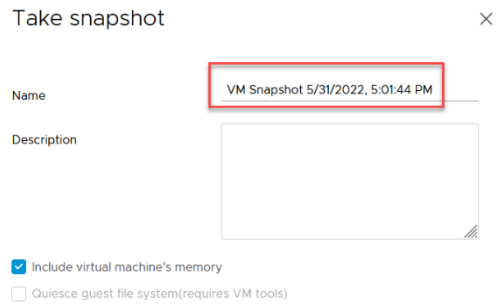


Post-cloning, all attributes remain unchanged except for the IP address and UUID.

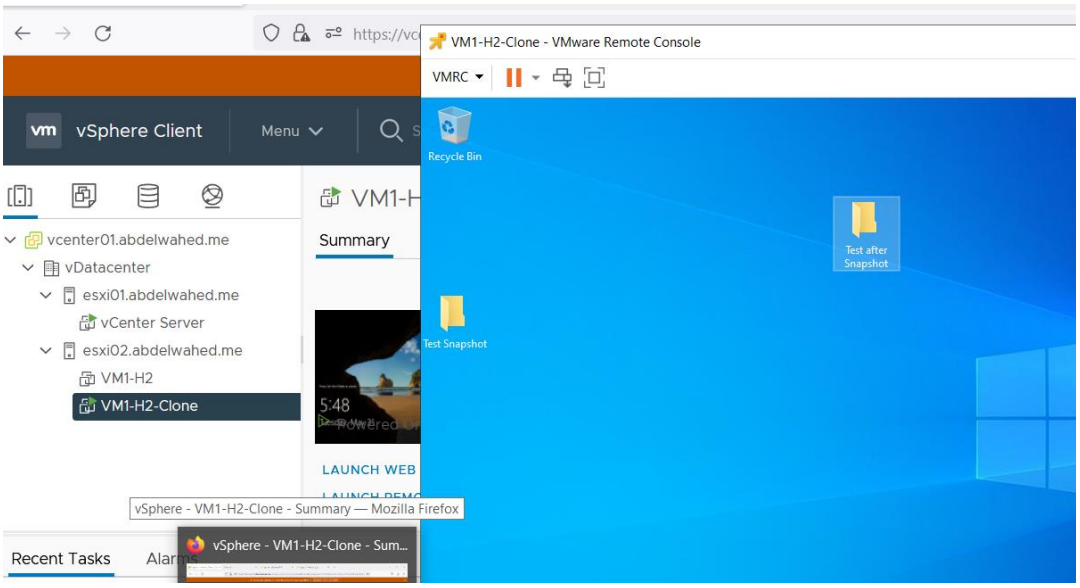


Steps to take a Snapshot

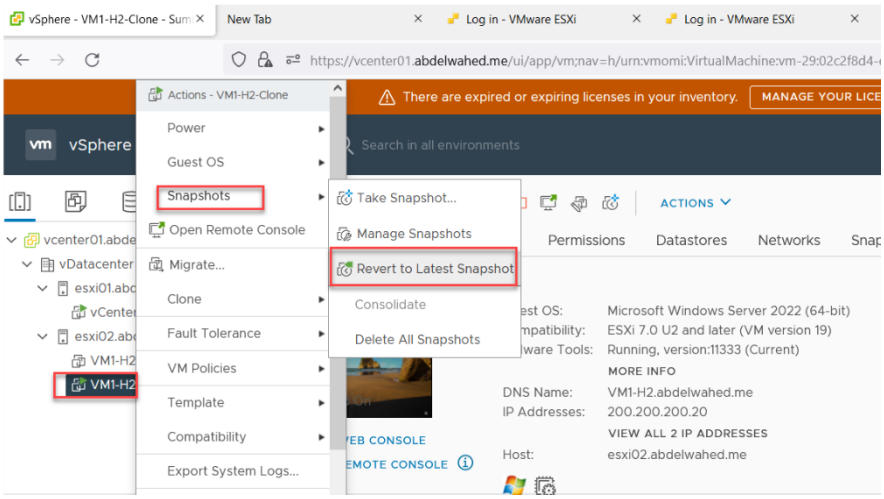


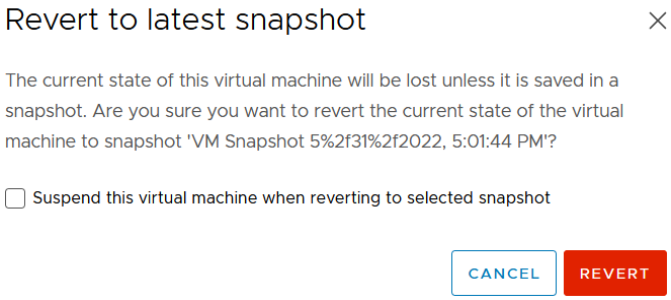


Once I captured a snapshot, I included an additional folder as demonstrated below.

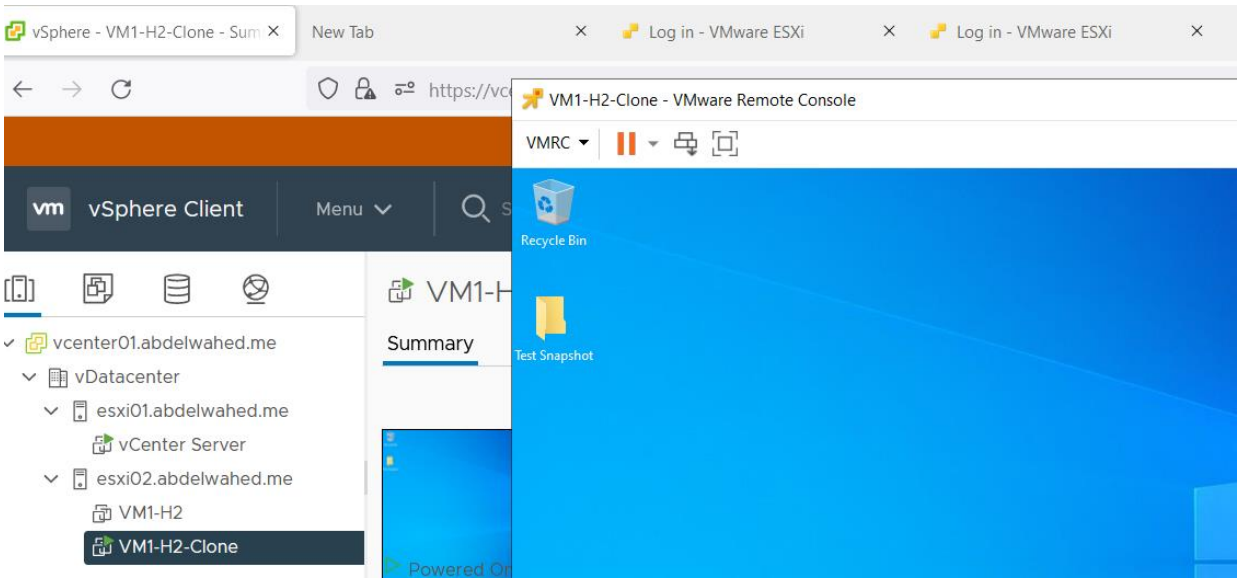


Now I'm going to restore the virtual machine to its previous state to observe the modifications.





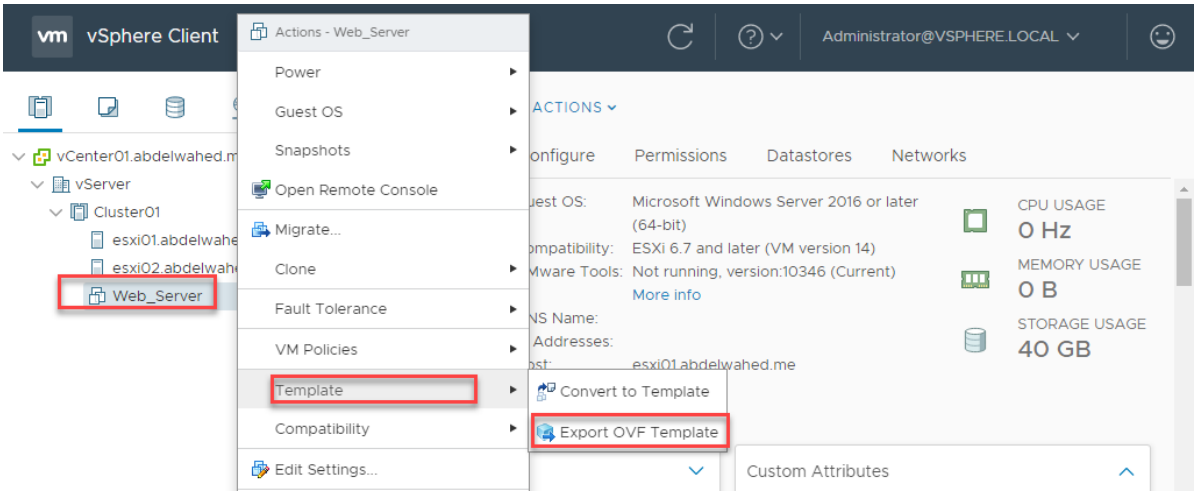
The recently added folder has been removed.

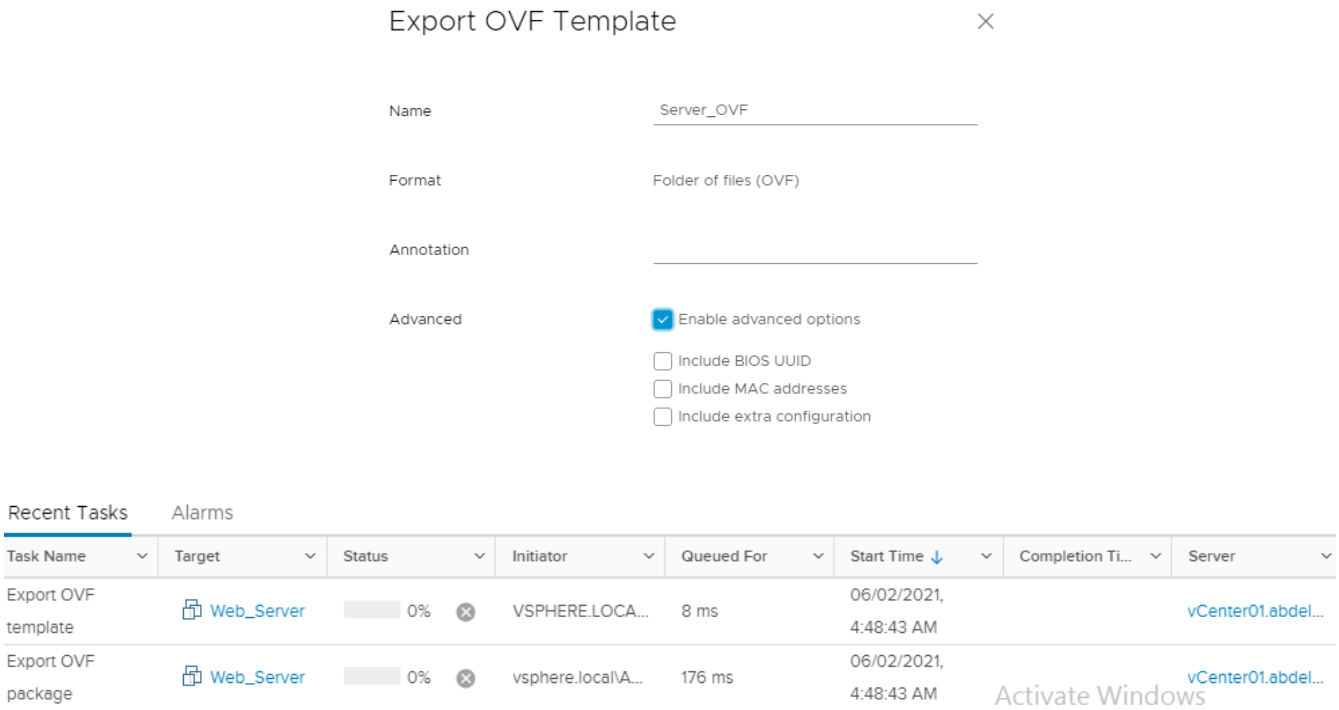


OVF and OVA Template (Open Visualization Format and Appliance)

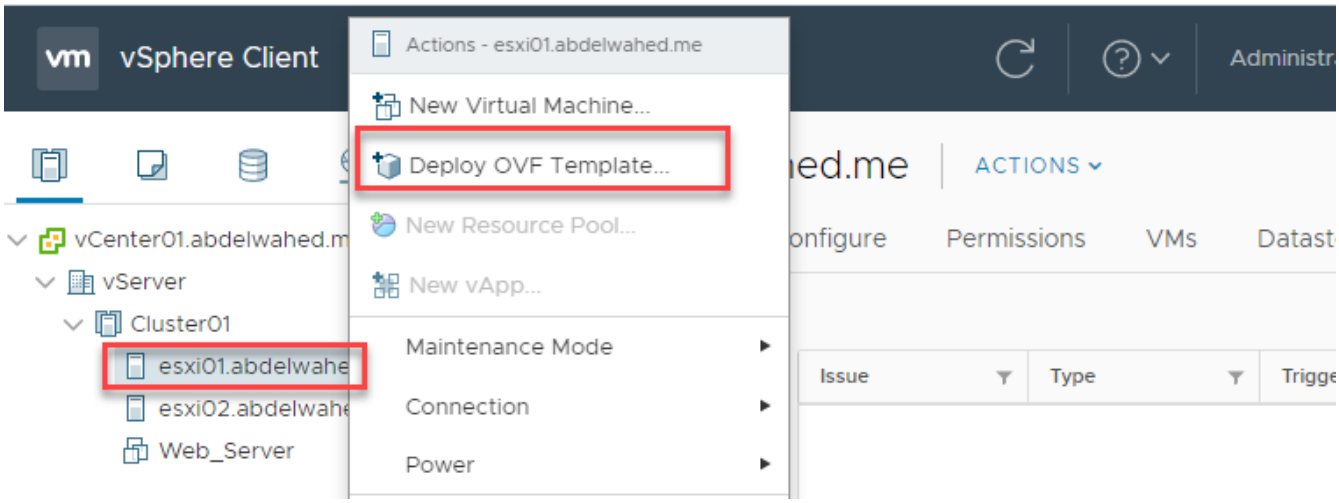
Using OVF (Open Virtualization Format) or OVA (Open Virtualization Appliance) templates, users can create preconfigured VMs that can be easily deployed in different virtualization environments. These templates include all necessary configuration settings, such as the number of virtual CPUs, the amount of memory, and the disk configuration, making it easy to import and deploy the VM without having to manually configure these settings.

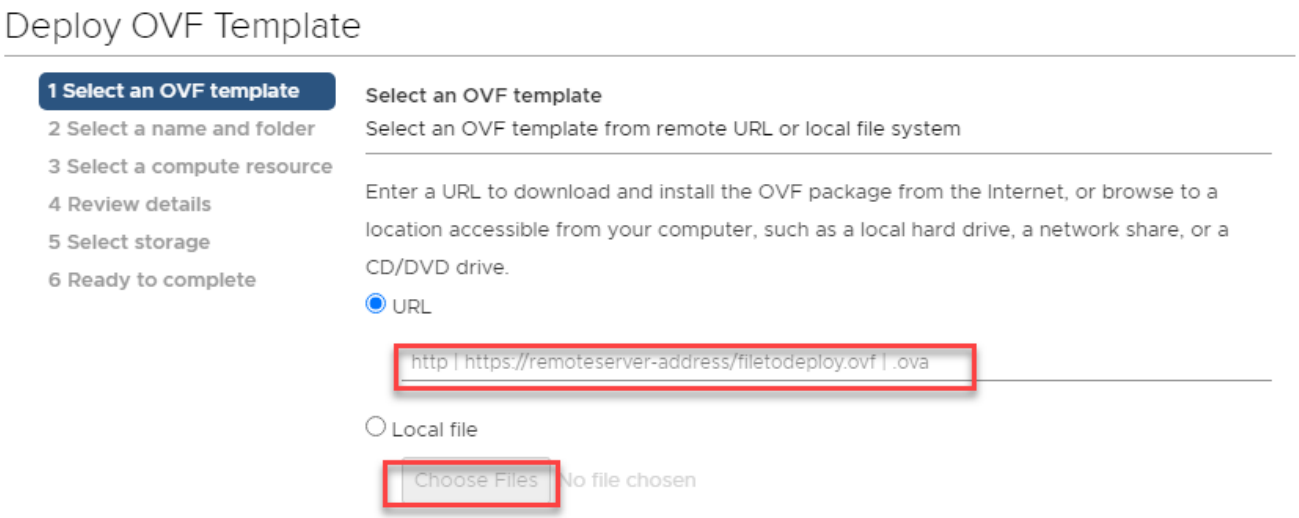
Before exporting the VM, ensure it is powered off.





You can now import the OVF into either the same environment or a different one by following these steps:





VM Files

Virtual machines (VMs) in VMware vSphere are encapsulated by a set of files stored on a VMFS (Virtual Machine File System) datastore. These files collectively define the VM's behavior, configuration, and content.

Overview of VM Files

File	Description	Example	VM State Where File Appears
.vmx	Main configuration file for the VM.	Stores settings like the VM's CPU and memory configuration.	Always Present
.vmdk	Represents the VM's hard drive.	The VM's 80GB hard drive data is stored here.	Always Present
.nvram	Contains the VM's BIOS or EFI configuration.	Changes to the boot order in the VM's BIOS are saved here.	Always Present
.log	Log files for operational activities of the VM.	Provides logging while the VM is managed by vSphere.	Always Present
.vswp	vSwap file used for virtual memory.	If a VM with 8GB RAM and 2GB reservation uses its physical RAM, ESXi might swap memory pages to this file.	Powered On
.vmsd	Maintains snapshot metadata.	Stores snapshot information.	When VM has Snapshots
.vmsn	Represents the state of a snapshot. One for each snapshot	Captures the running state of a VM at the time a snapshot was taken.	When VM has Snapshots
.vmss	Suspended state file.	Captures the exact running state of a VM at the time of suspension.	Suspended

Content Library in VMware vSphere

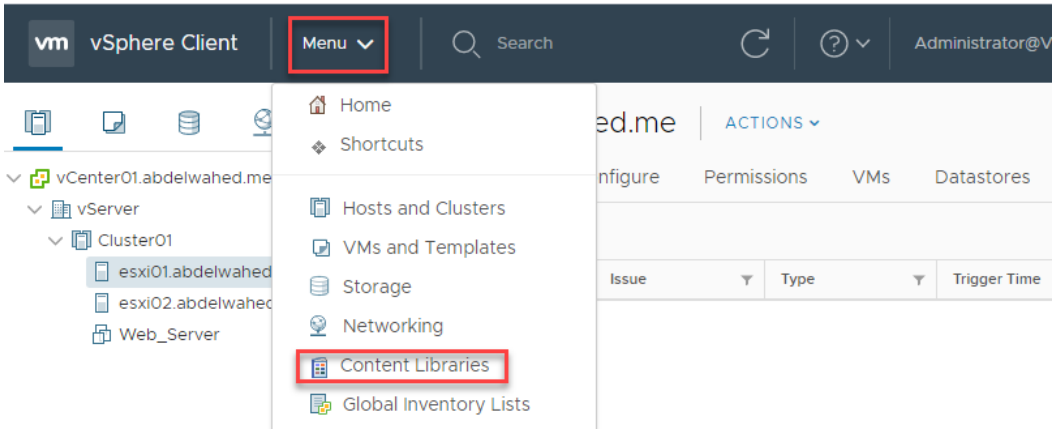
A Content Library is a centralized repository for storing and managing virtual machine templates, ISO images, scripts, and other files that can be used to create and deploy virtual machines in a VMware vSphere environment. This feature allows users to create, share, and manage a library of virtual machine content across multiple vCenter Server instances.

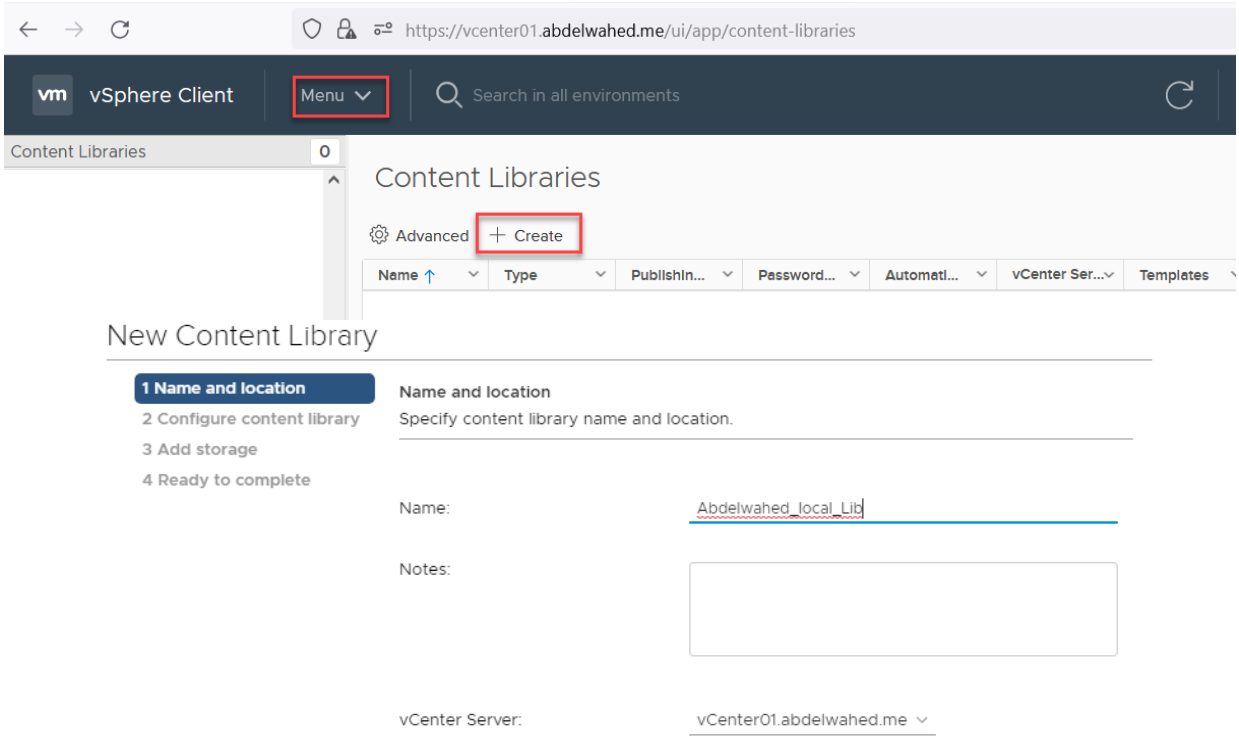
Key Features and Benefits

1. **Centralized Storage**:
   - The Content Library is stored on a datastore, which can be shared across multiple hosts and vCenter Server instances. This centralization makes it easier to manage and distribute content across the entire virtual infrastructure.
2. **Organization:**
   - Content can be organized into folders and subfolders, making it easy to manage and find specific items. It also supports versioning to keep track of changes and updates.
3. **Variety of Content Types:**
   - **Virtual Machine Templates**: Preconfigured VMs used as starting points for creating new VMs.
   - **ISO Images**: Bootable images for installing operating systems or applications on VMs.
   - **Scripts**: Scripts or configuration files for automating VM configurations.
   - **Other Files**: Documentation, images, and multimedia files.
4. **Consistency and Efficiency:**
   - Eliminates the need to duplicate content across multiple hosts and vCenter Server instances, saving time and storage space while ensuring consistency across the virtual infrastructure.
5. **Automation:**
   - Facilitates the automated deployment of VMs, allowing for quick provisioning of new resources as needed.

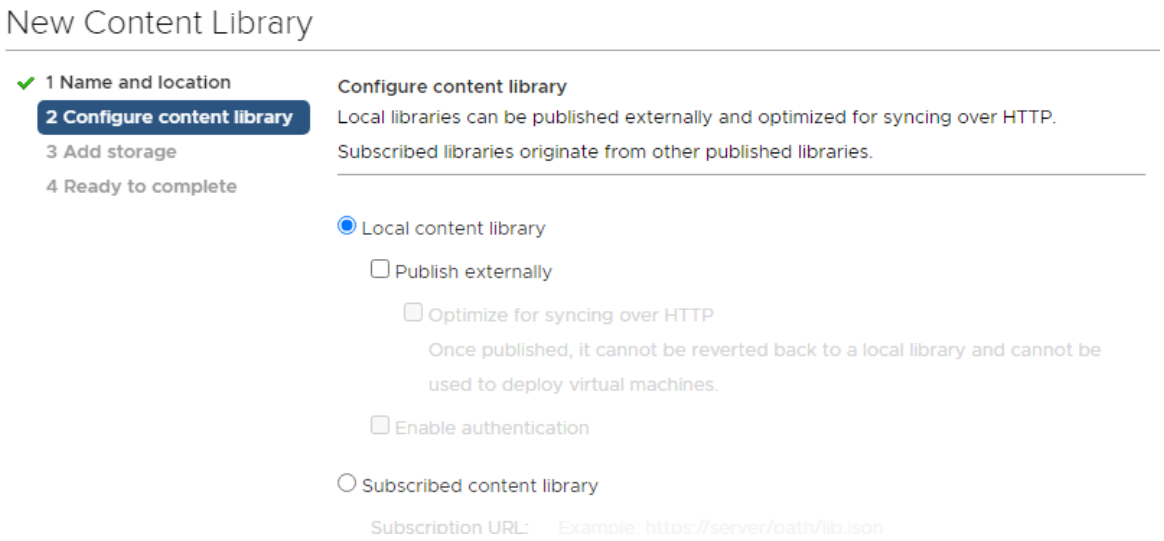
Benefits of Using a Content Library

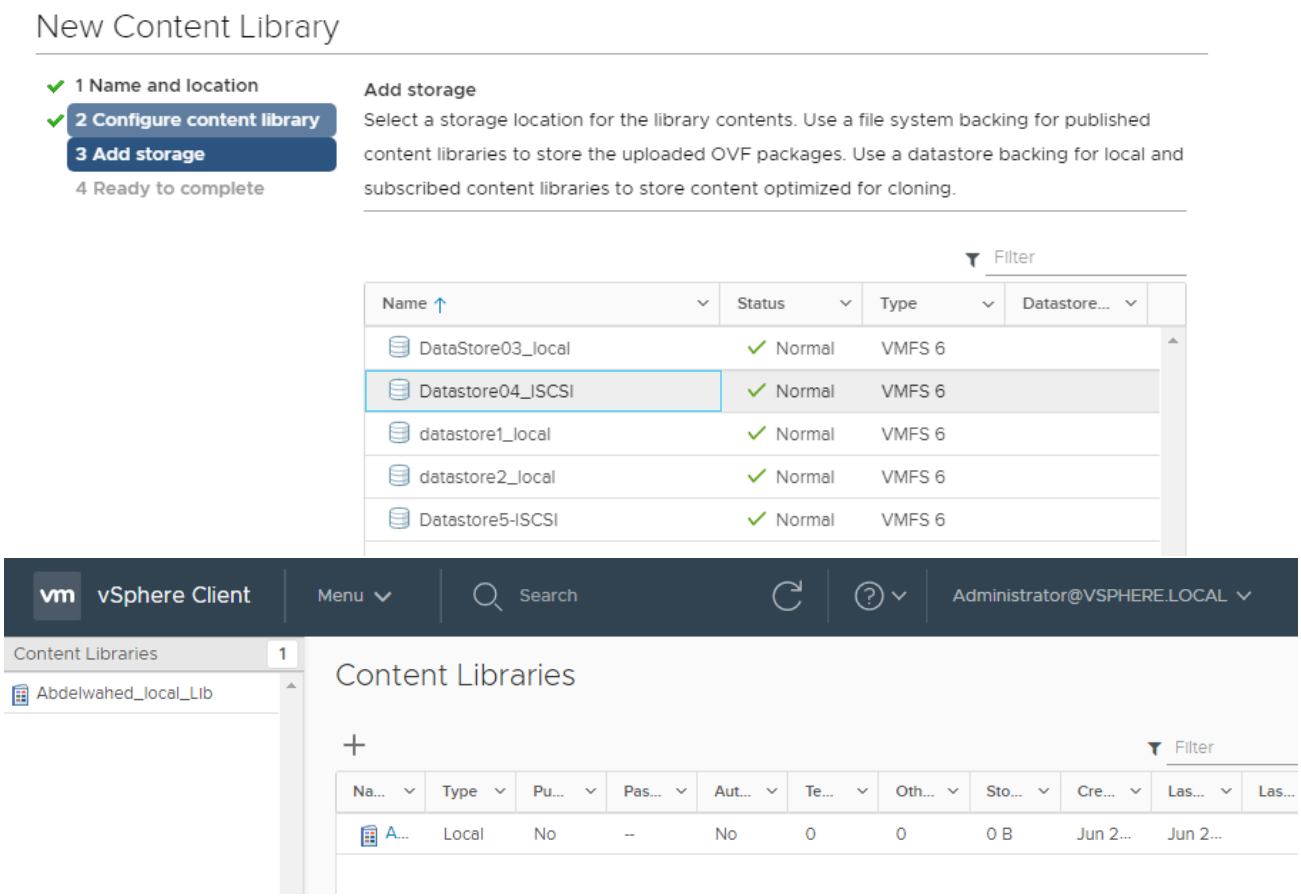
- **Centralized Management**: Simplifies the management of VM templates, ISO images, and other resources.
- **Resource Sharing**: Enables sharing of content across multiple vCenter Server instances and hosts.
- **Consistency**: Ensures consistent deployment and configuration of VMs across the environment.
- **Storage Efficiency**: Reduces the need for duplicate copies of templates and other content, saving storage space.
- **Automation**: Streamlines the process of deploying VMs, making it easier to quickly provision new resources.



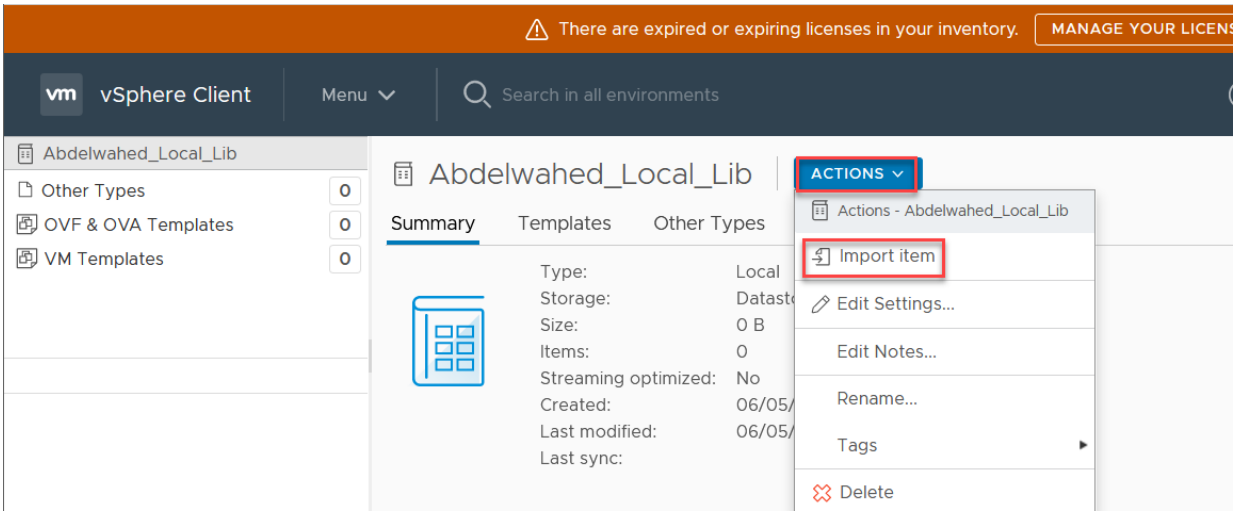


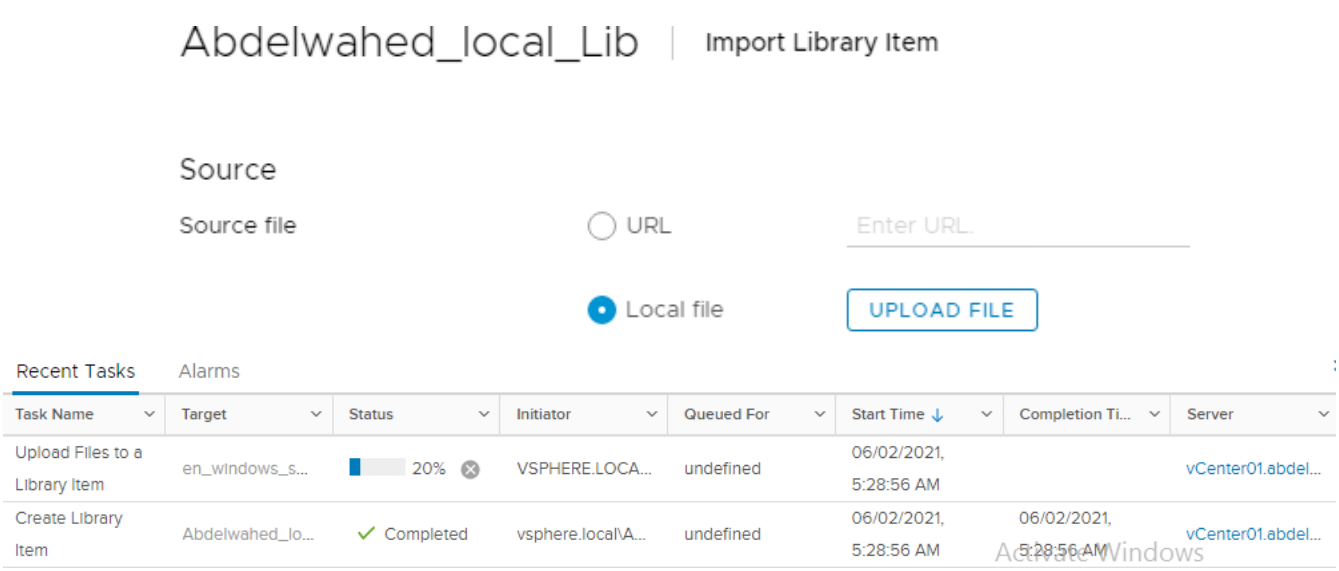
This library can be made public, allowing another vCenter to link to it and utilize its resources.



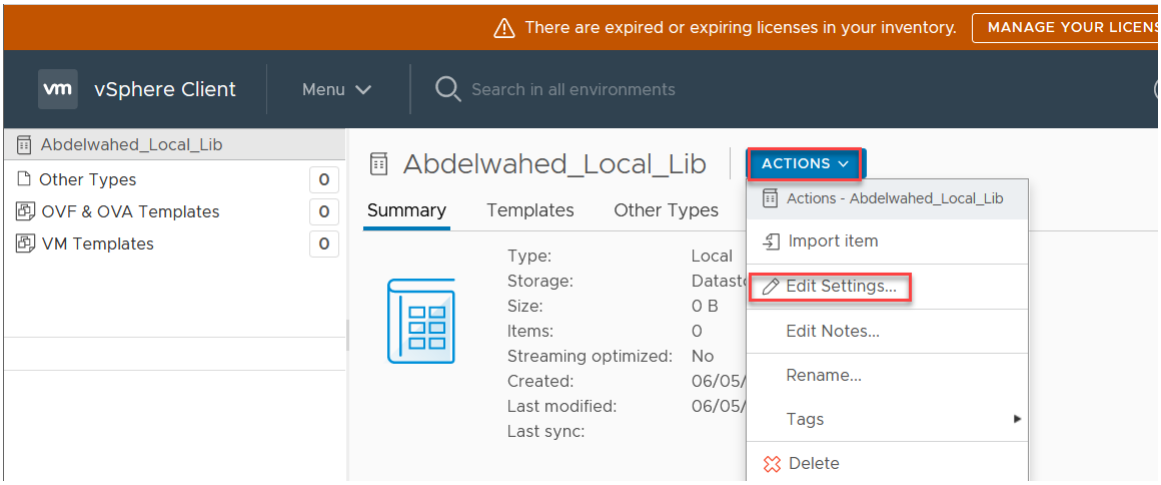


You now have the ability to upload various kinds of data to it.

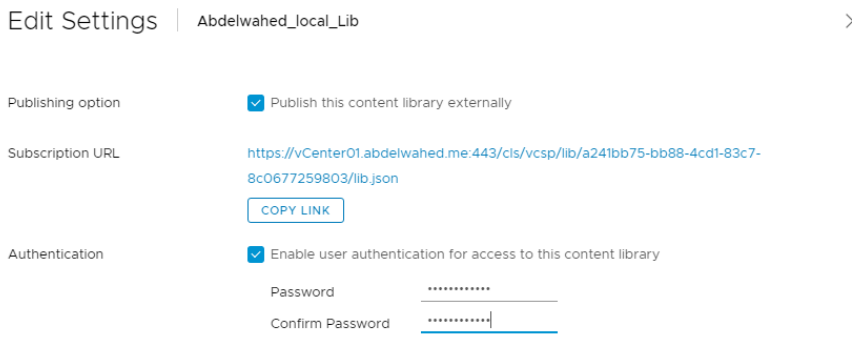




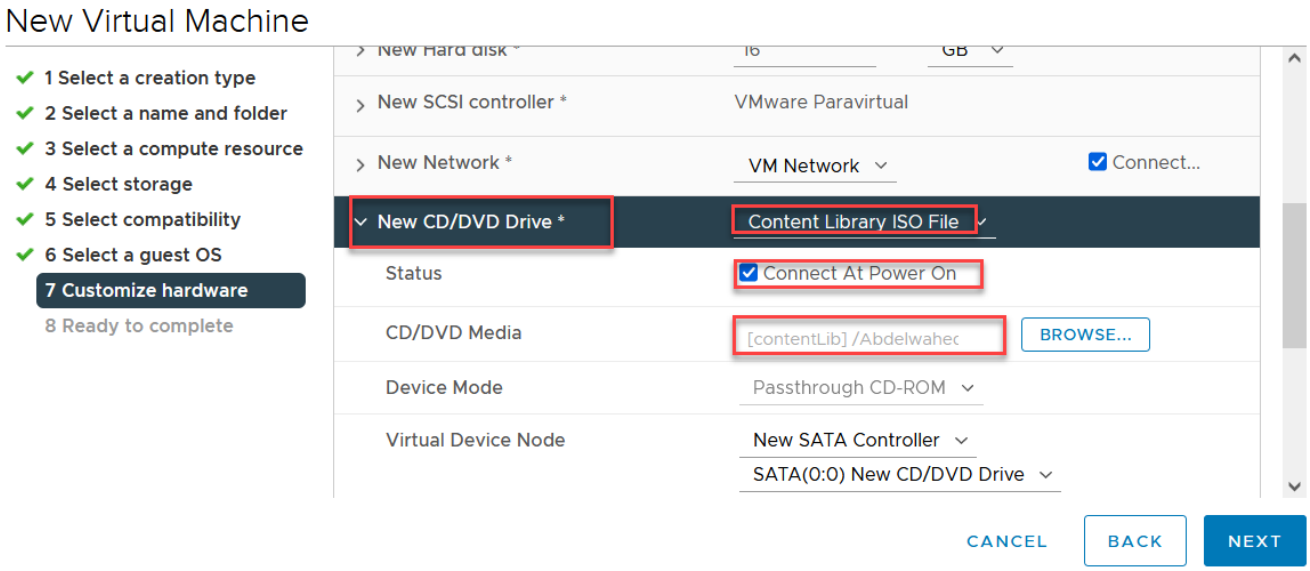
You have the option to change this local library into a subscription-based web library.



You can also utilize this link as a local library for another vCenter.

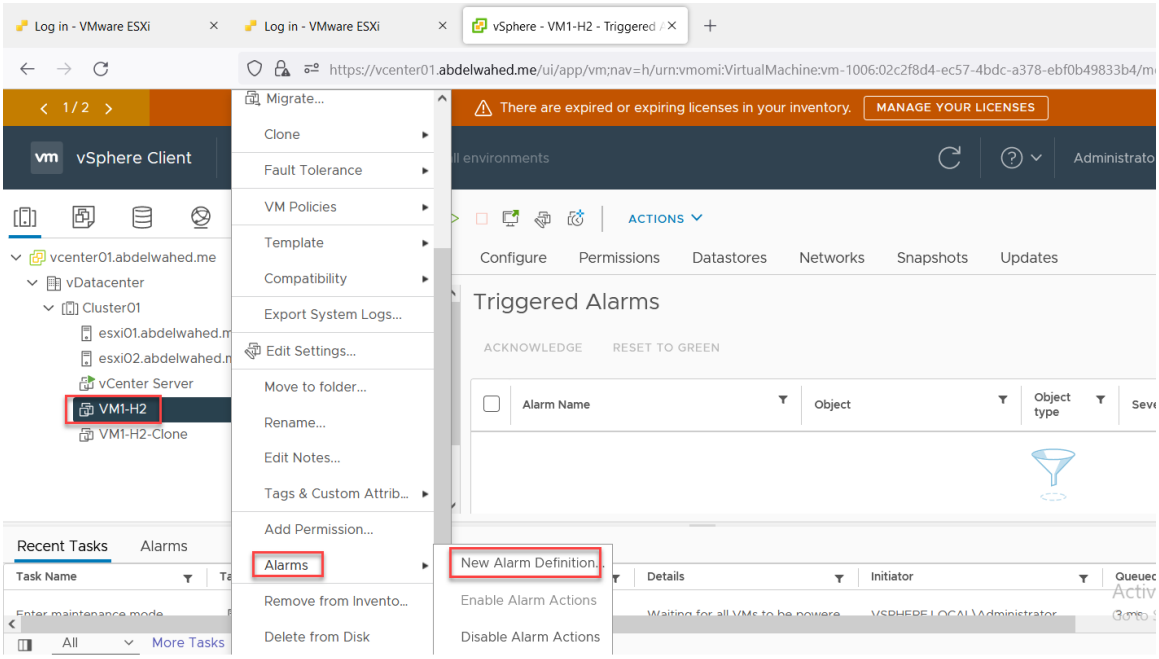


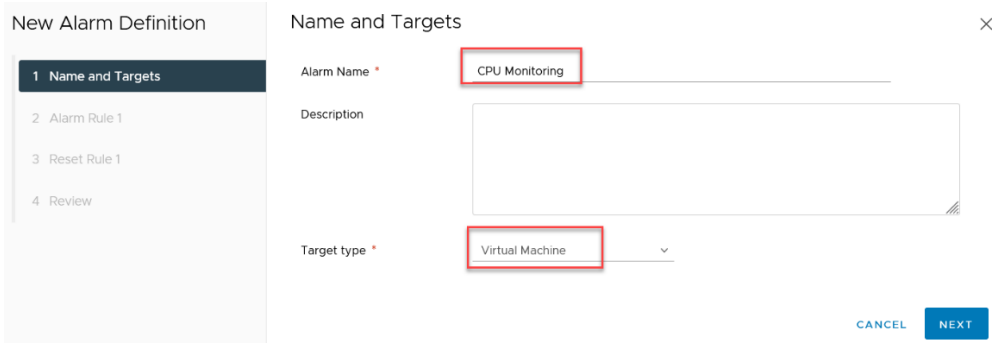
You can now use the ISO that's been uploaded to the library to set up a new virtual machine.

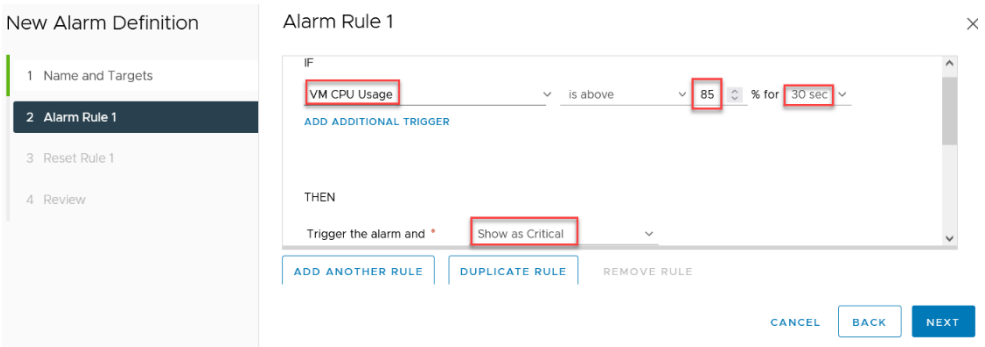


Using Alarms

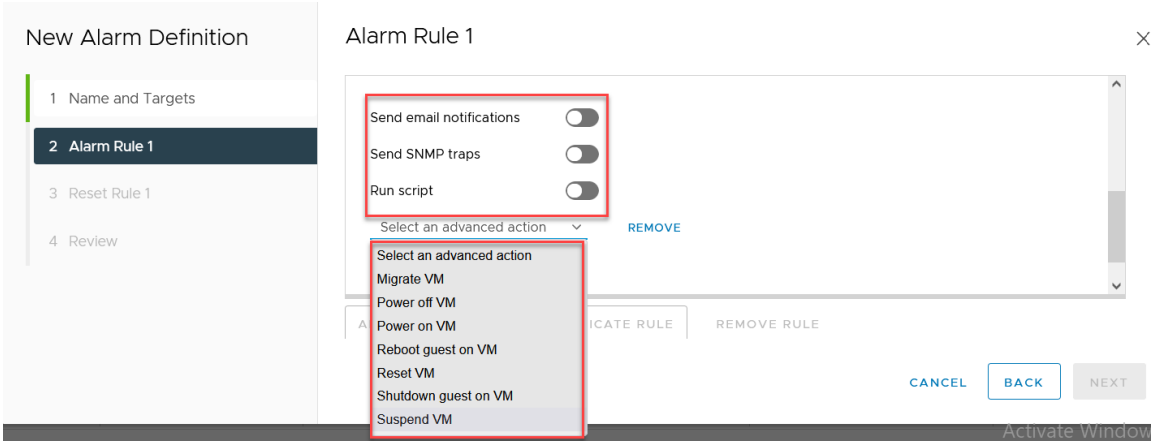
In a VMware vSphere environment, alarms can be created to monitor events and conditions related to virtual machines (VMs). Alarms can be configured to alert administrators when specific events or conditions occur, allowing them to quickly take action to resolve issues and maintain the health of the virtual infrastructure.

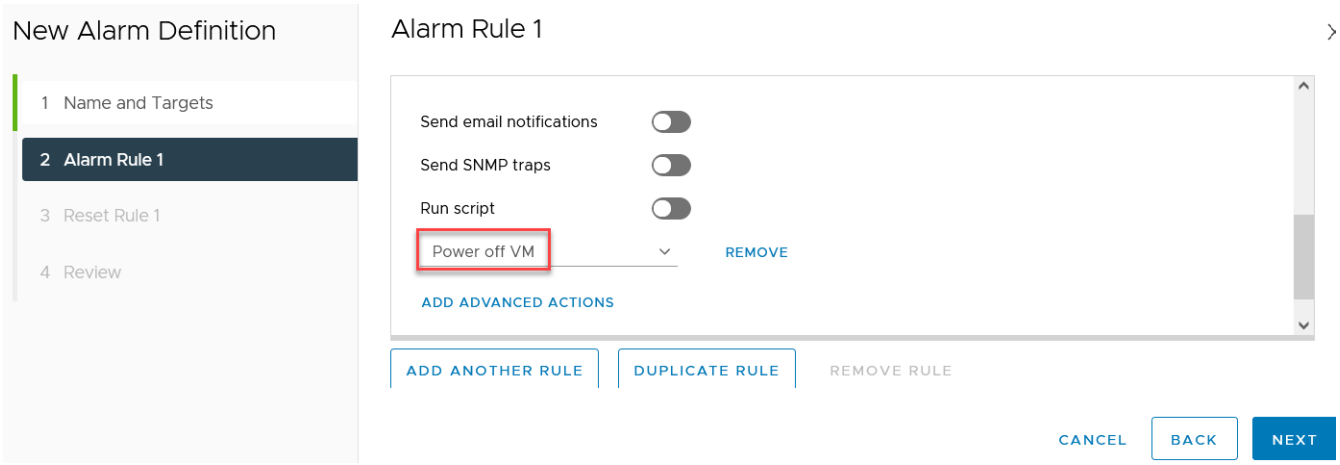


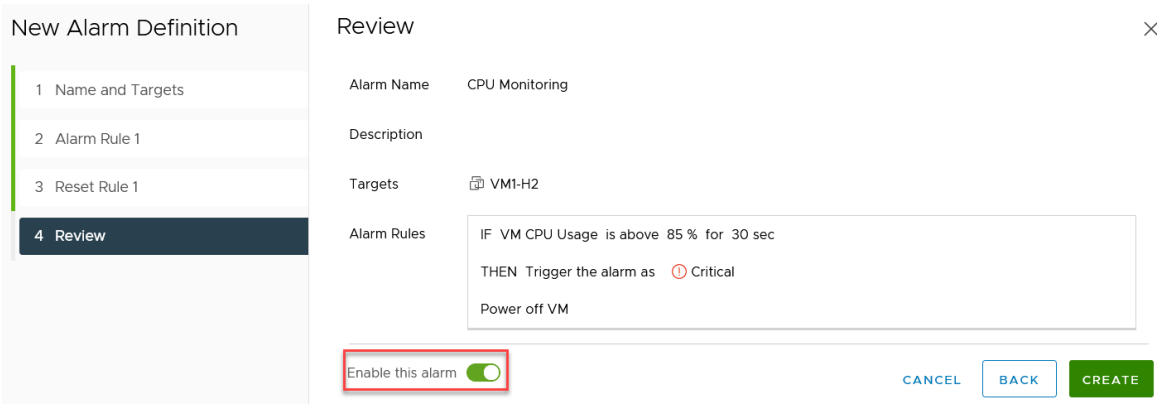




You can initiate actions once your criteria are fulfilled.







Host Profile in VMware vSphere

Host Profile is a feature in vSphere that allows you to create a template for configuring and managing ESXi hosts in your environment. With Host Profile, you can define a standard set of configuration settings, policies, and security settings, and apply them to one or more hosts at once. This ensures consistency and compliance across your host infrastructure and simplifies host management.

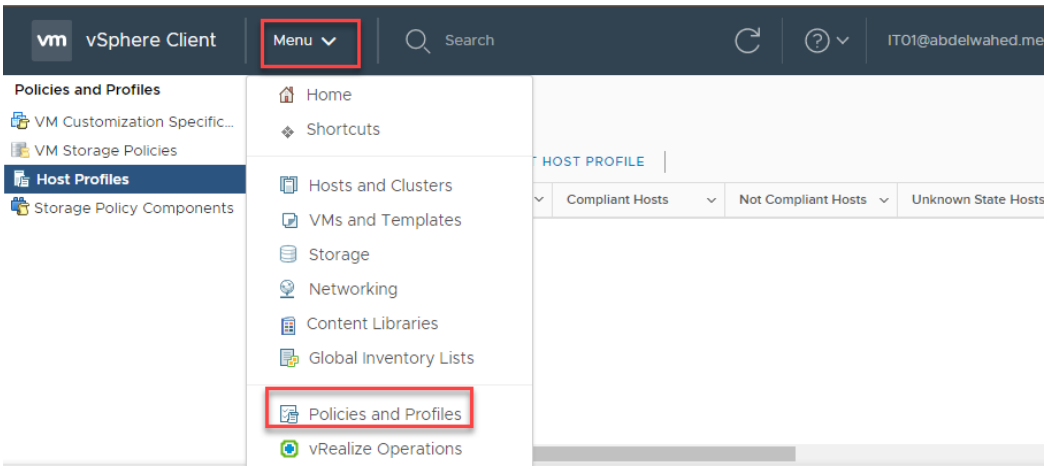
Steps to Create and Apply a Host Profile in vSphere

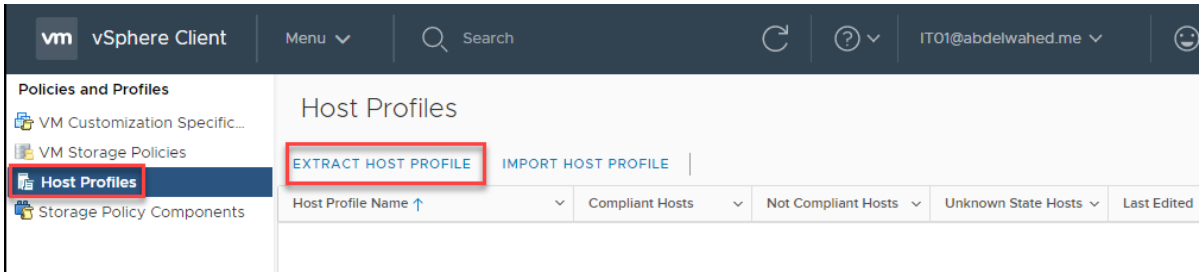
1. **Create a Host Profile**:
   - **Access Host Profiles**: Go to the Host Profiles section in the vSphere Web Client or vSphere Client.
   - **Create Profile**: Click Create Profile, provide a name and description for the profile, and select the host to use as the reference.
   - **Configure Settings**: Define the settings for the profile, including networking, storage, security, and advanced settings. You can also add custom scripts and commands.
2. **Edit the Host Profile**:
   - **Access Host Profiles**: Go to the Host Profiles section and select the profile to edit.
   - **Edit Profile**: Click Edit Profile and make the necessary changes to the settings.
3. **Attach the Host Profile**:
   - **Select Hosts**: Go to the Hosts and Clusters view and select the hosts to apply the profile to.
   - **Attach Profile**: Click the Attach/Detach Host Profile button, select the Host Profile to apply, and click Attach.
4. **Remediate the Host Profile**:
   - **Select Host Profile**: Go to the Host Profiles section and select the Host Profile to remediate.
   - **Remediate Hosts**: Click Remediate, select the hosts to remediate, and the vSphere system will check the host's current settings against the profile settings and apply the changes if necessary.

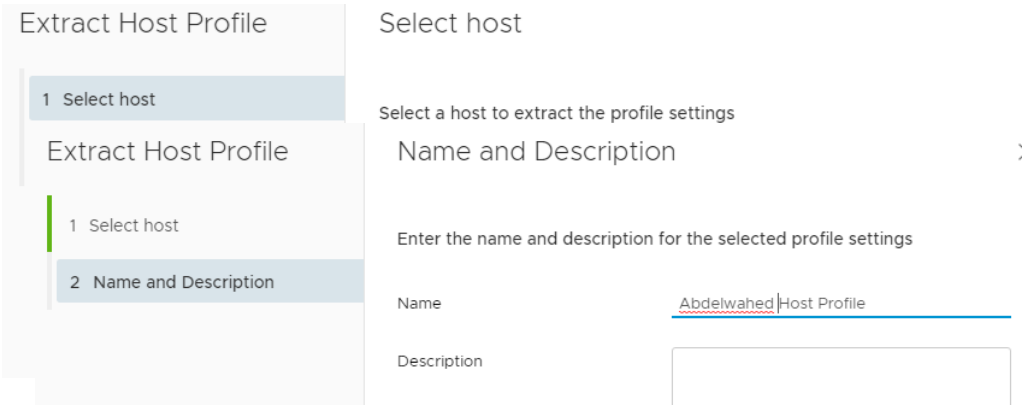
Benefits of Using Host Profiles

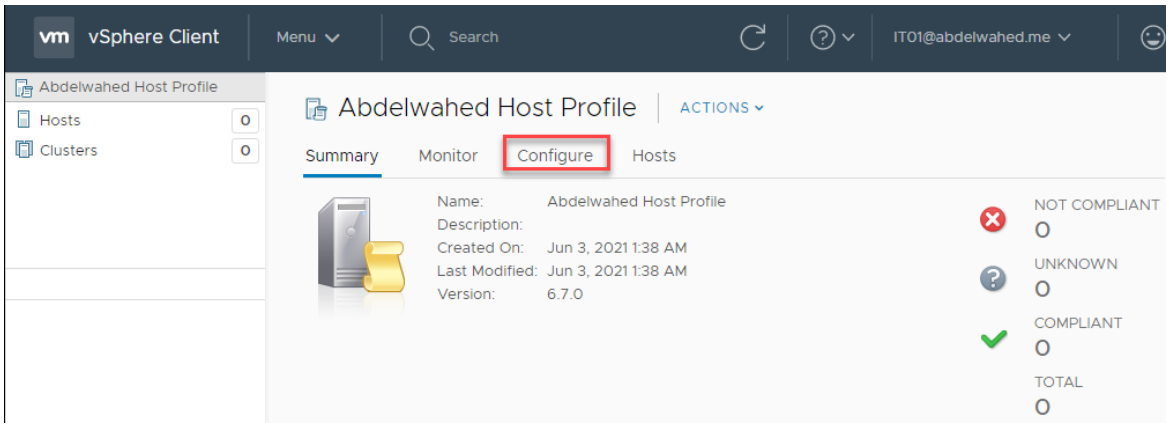
- **Consistency**: Ensures that all ESXi hosts adhere to a standardized configuration, reducing configuration drift.
- **Compliance**: Helps maintain compliance with internal and external policies by enforcing consistent settings across hosts.
- **Simplified Management**: Streamlines the management of multiple hosts by allowing administrators to apply configuration changes to all hosts from a central location.
- **Automated Remediation**: Automatically identifies and corrects configuration deviations from the defined Host Profile.

Resetting the Password for ESXi Root Accounts

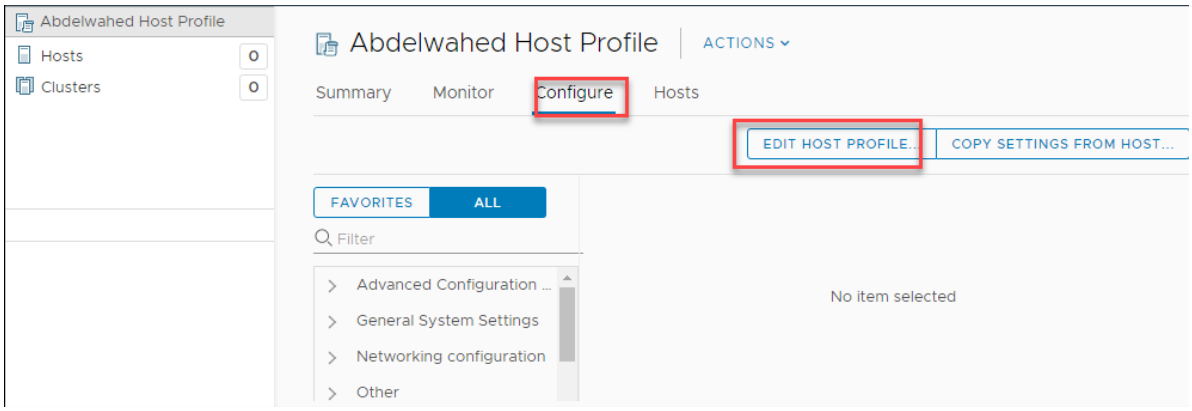


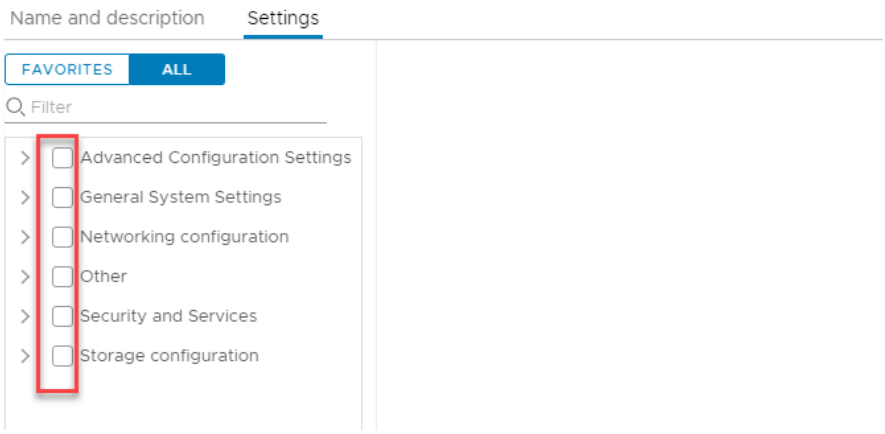


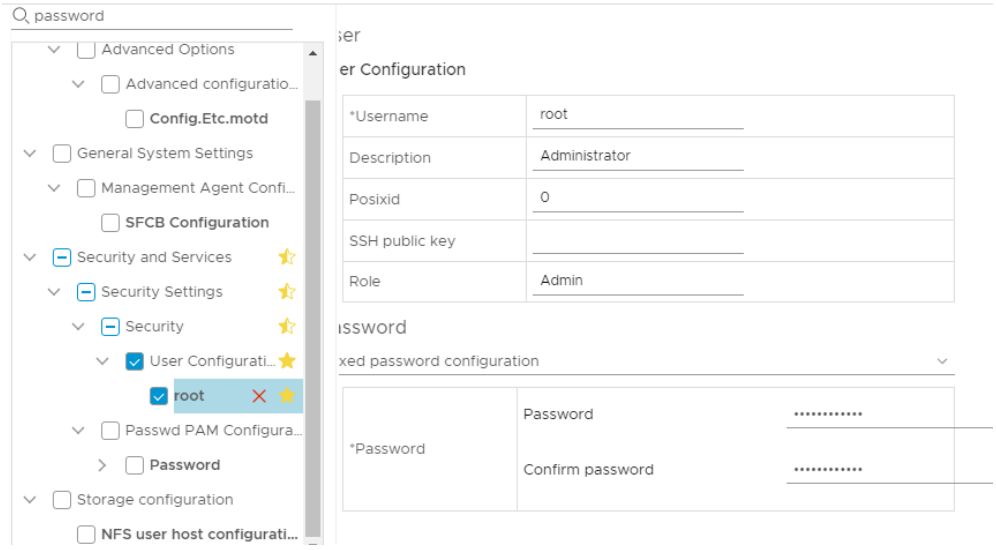




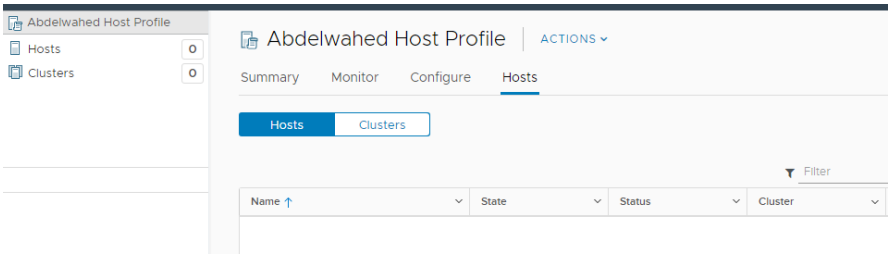
To set this profile as default, clear all current configurations to prevent conflicts before adding your custom settings.

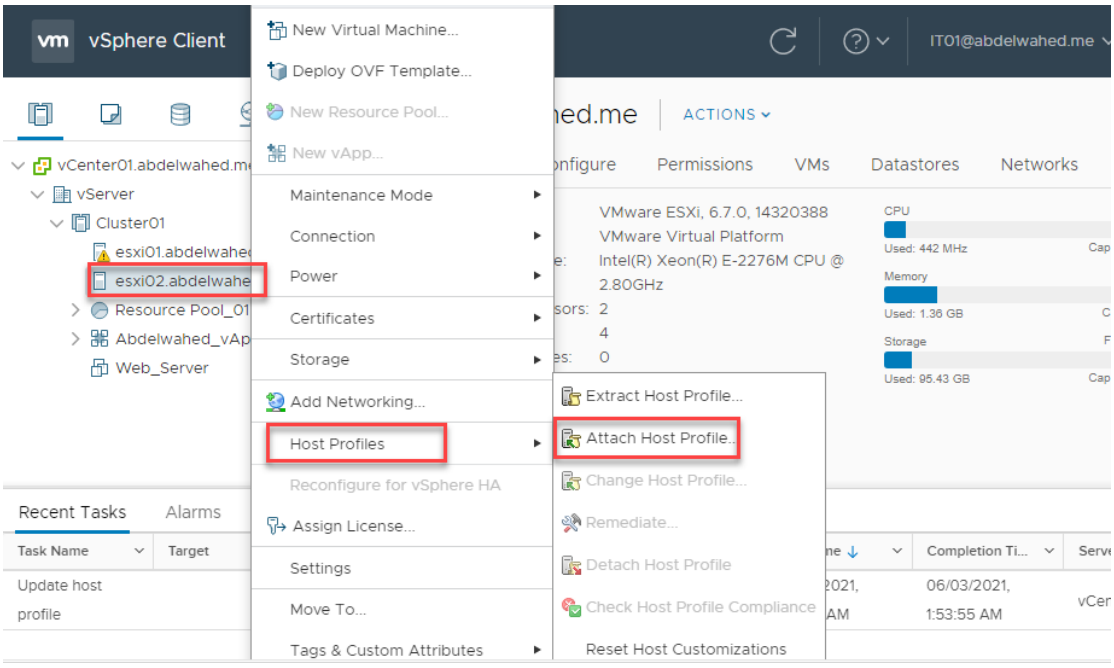


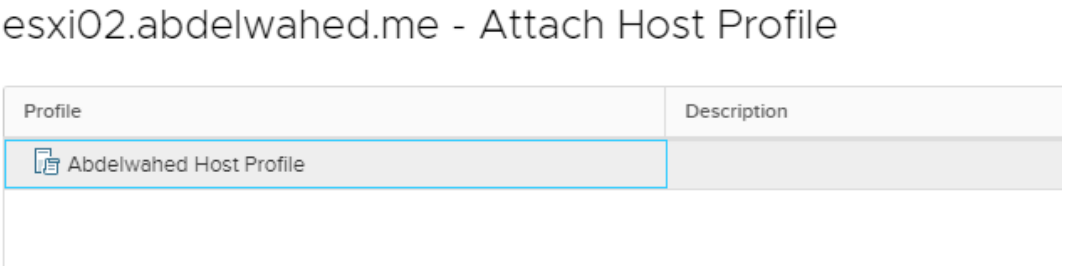




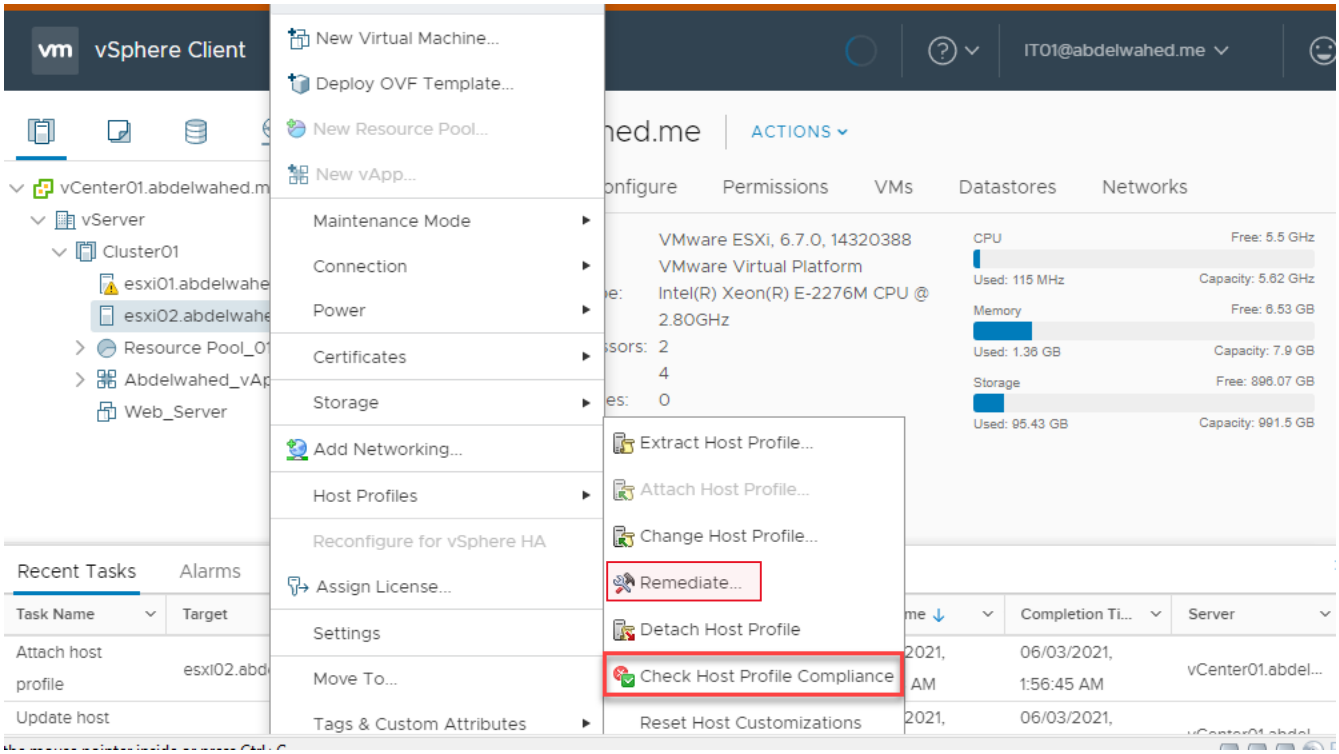
No host is linked to the profile yet.

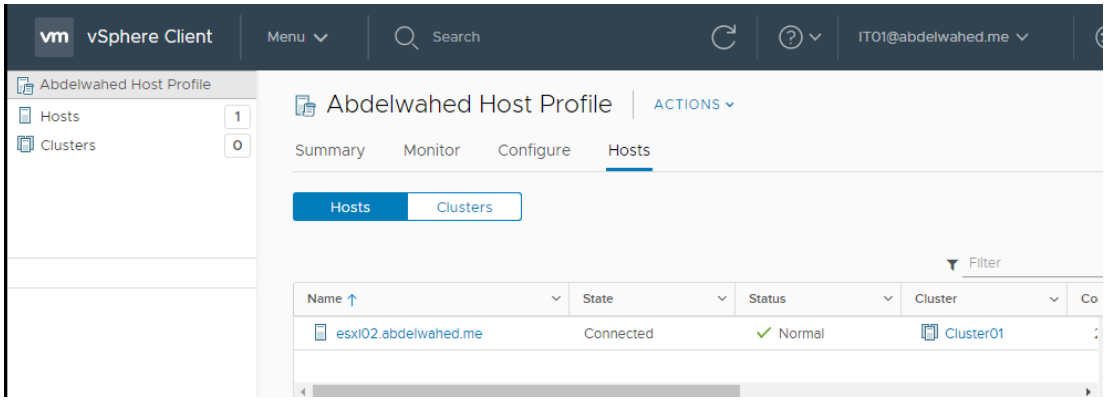






A host is now connected to that profile, and you can also link it to a cluster.

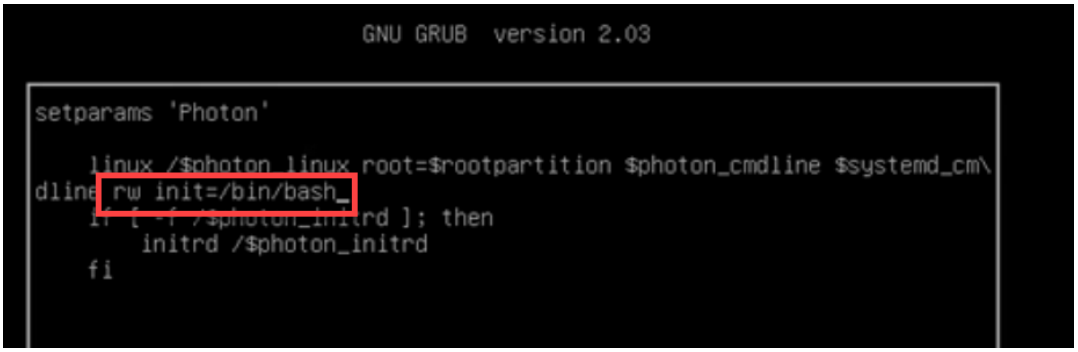


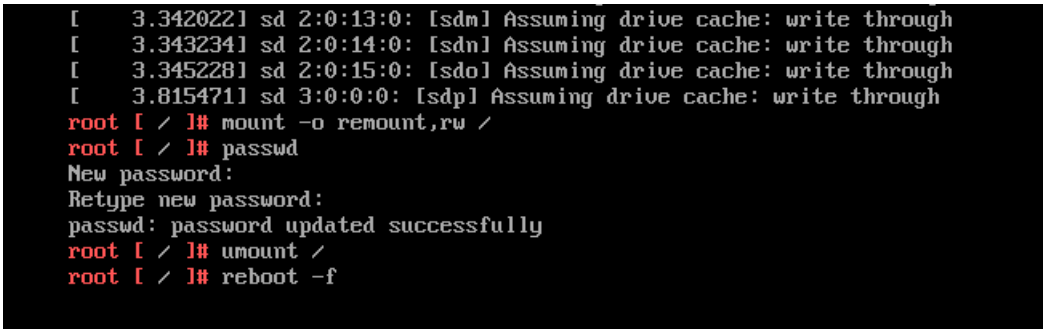


vCenter password reset

Password reset for vCenter root

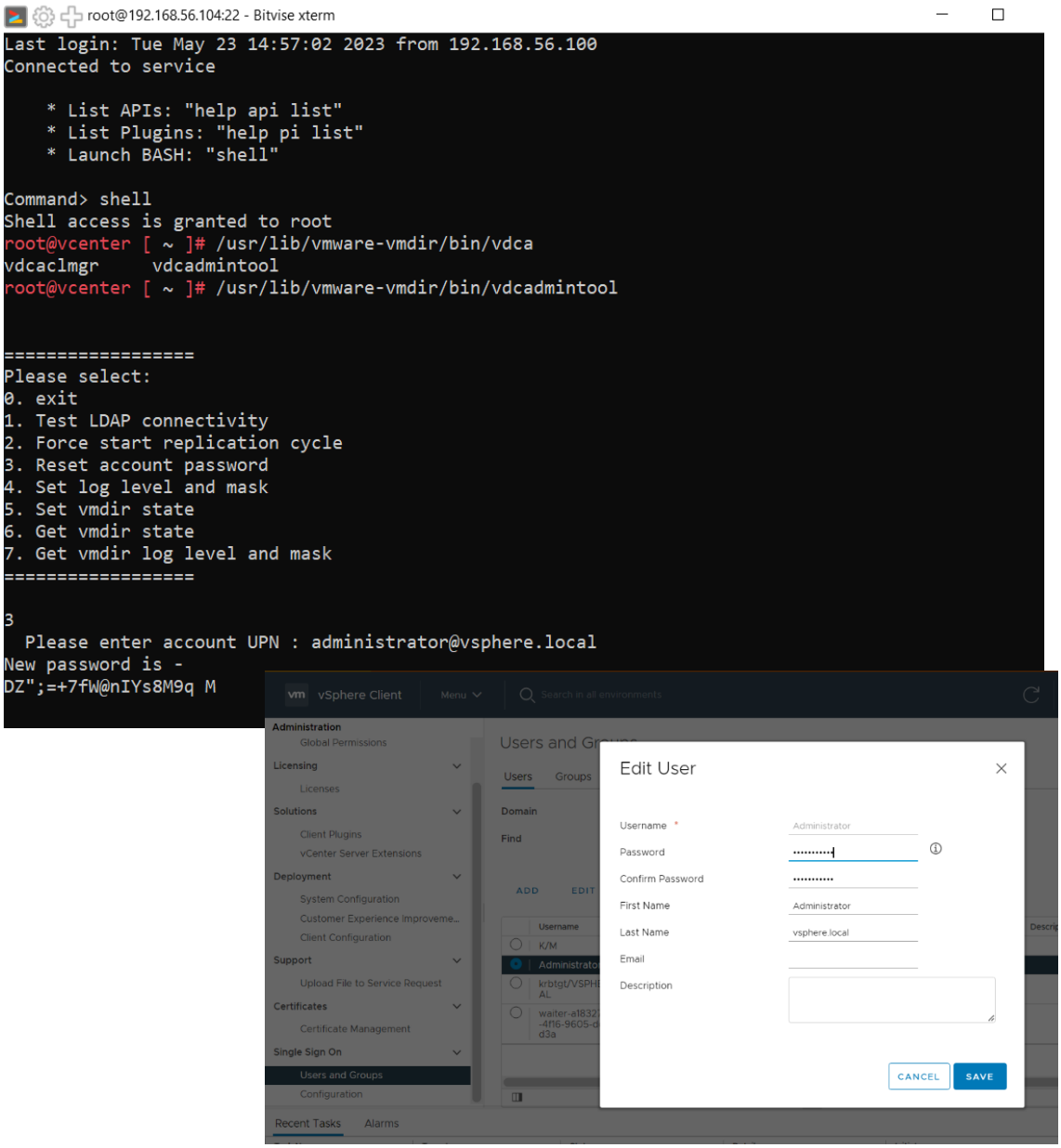
1. Restart the vCenter server.
2. During the boot process, access the GRUB menu by pressing "e."
3. Edit the selected entry and append **"rw init=/bin/bash"** to the end of the line starting with **"linux /$photon"**
4. Boot into single-user mode with a root shell prompt.
5. Remount the root filesystem in read-write mode: **mount -o remount,rw /**
6. Reset the root password: **passwd root**
7. Reboot the server: **reboot -f**
8. After the server restarts, log in to vCenter using the new root password.





Reinitialize the vCenter administrator credentials.

1. Log in to the VCSA management portal using root credentials through port 5480
2. Navigate to the "Administration" section.
3. Look for the "Access" tab or similar option that provides SSH and Bash access settings. Enable SSH and Bash access if they are not already enabled.
4. Open an SSH client (such as PuTTY) and connect to the vCenter server using the SSH protocol on port 22. Use the IP address or hostname of the vCenter server. using root user.



VMware vSphere Network

Use Two Networks

It's advised to have two distinct network types in a VMware vSphere environment:

1. **ESXi Management Network**:
    - Specifically for managing ESXi hosts.
2. **VM Network:**
    - Exclusively for virtual machine (VM) traffic.

Benefits

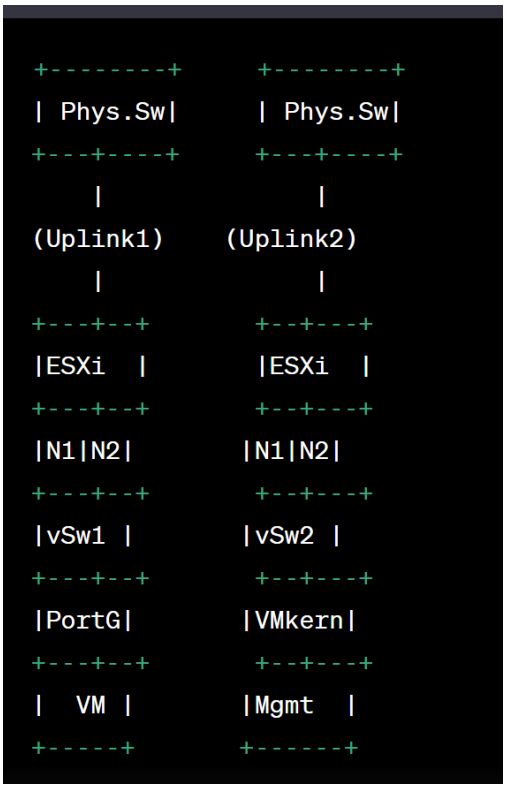
1. **Improved Security**:
    - By segregating traffic, potential security vulnerabilities are minimized.
2. **Enhanced Performance**:
    - Isolates VM traffic from ESXi management traffic, ensuring smooth operations.

Network Configuration

1. **Two Virtual Switches**:
    - Create two standard virtual switches in vSphere.
2. **Connectivity with Failover and Load Balancing:**
    - **Two Uplinks per Virtual Switch**:
        - Each virtual switch should be linked to two uplinks (NICs) connected to two physical switches.
    - **Failover:**
        - Configuring failover ensures that if one NIC fails, the other can take over, ensuring continuous connectivity.
    - **Load Balancing:**
        - Distributing the network traffic across both NICs optimizes bandwidth utilization and potentially increases throughput.
3. **Port Group on vSwitch1:**
    - Used for VM connections.
4. **VMkernel Port on vSwitch2:**
    - Used for ESXi management connections.
5. **IP Assignments:**
    - VMkernel port gets its IP from the uplink (NIC), while the VM gets its IP from the port group.

Default Configuration

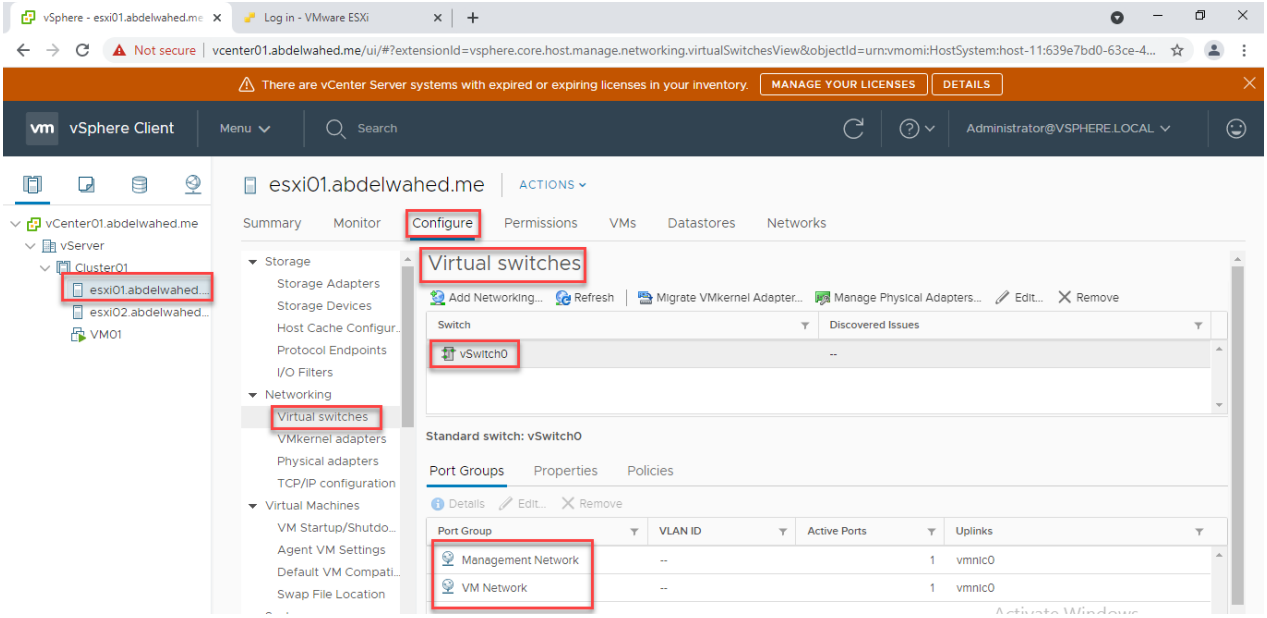
1. **vSwitch0**:
    - Post ESXi installation, a standard virtual switch named vSwitch0 is created.
2. **Port Groups:**
    - Includes a port group named VM Network.
3. **VMkernel Port:**
    - Named Management Network for ESXi management.

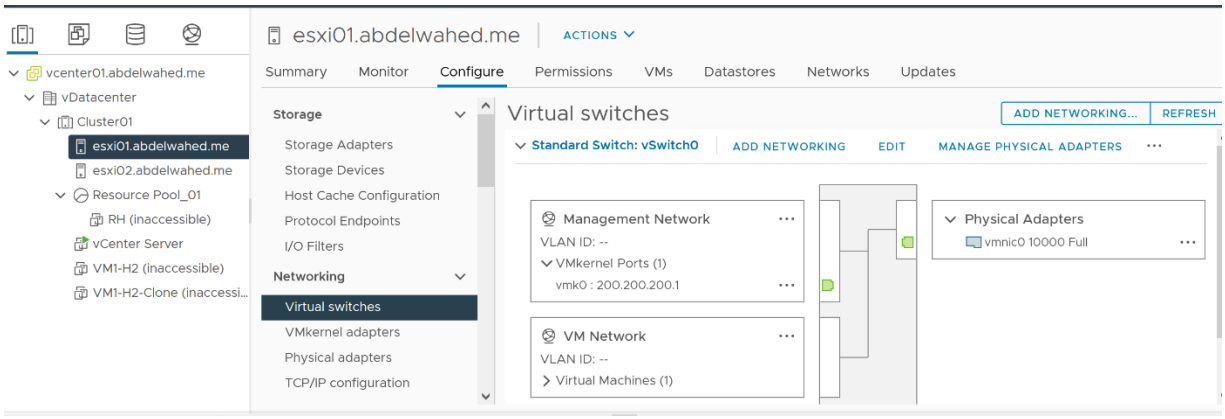


Explanation:

- **Phys.Sw**: Physical Switch
- **Uplink1/Uplink2**: Uplinks connecting ESXi hosts to physical switches.
- **ESXi**: ESXi hosts
- **N1 | N2**: Network interfaces (NICs) on the ESXi hosts.
- **vSw1**: Virtual Switch 1 for VM connections.
- **vSw2**: Virtual Switch 2 for ESXi management connections.
- **PortG**: Port Group on Virtual Switch 1 for VMs.
- **VMKern**: VMkernel Port on Virtual Switch 2 for ESXi management.
- **VM**: Virtual Machine network traffic.
- **Mgmt**: Management network traffic.

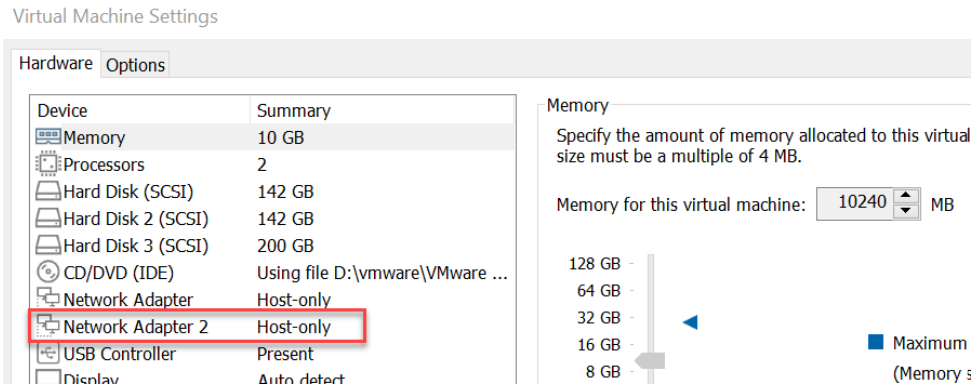
VMware vSphere Install, Configure, Manage | Lab Guide



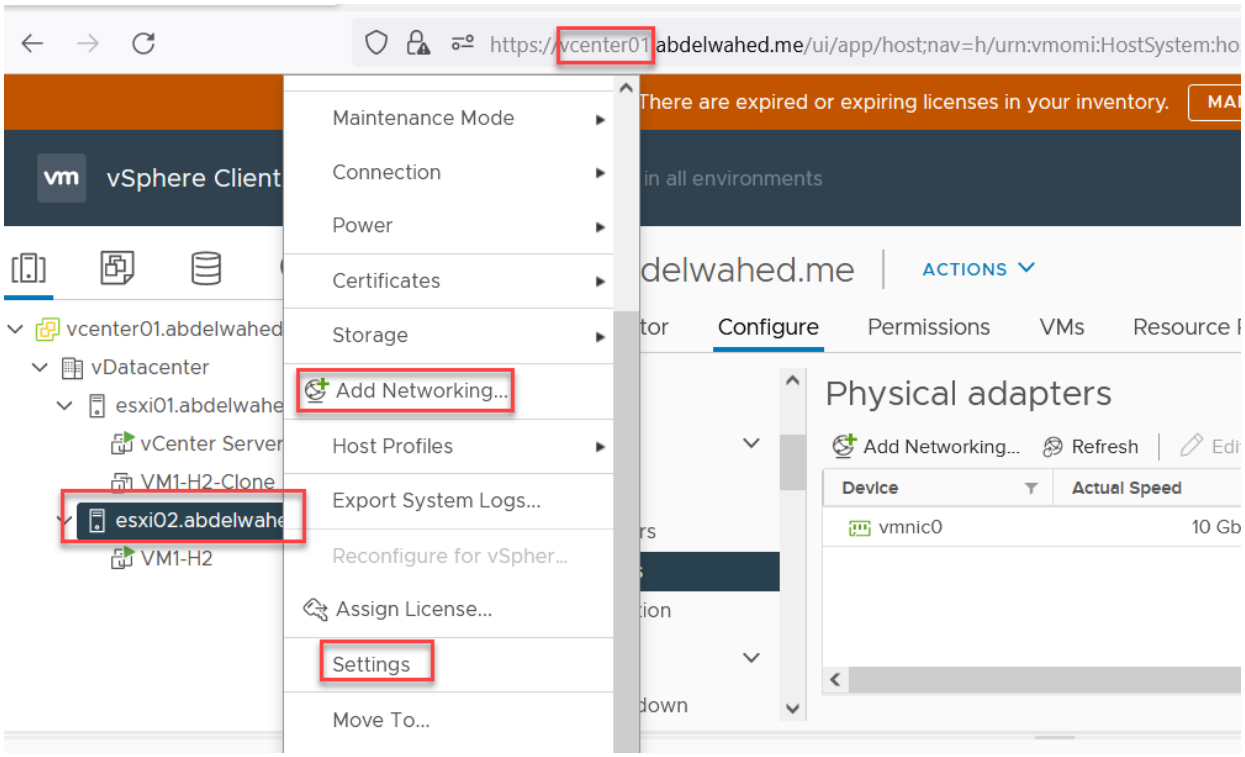


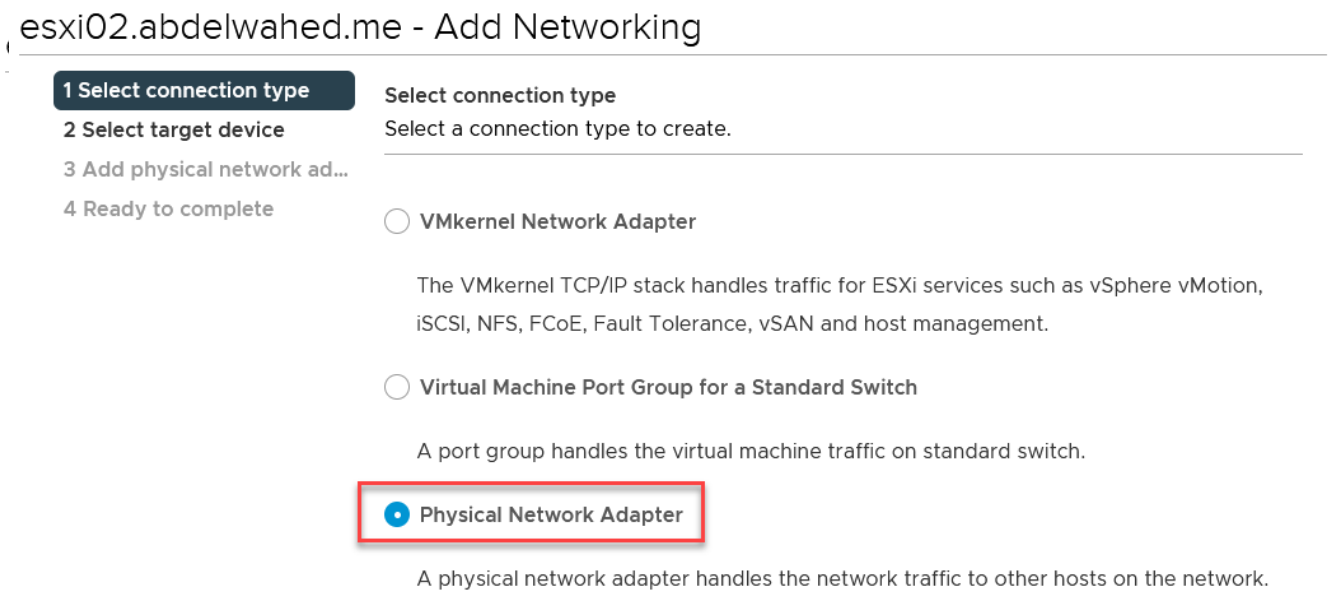
Install an additional NIC on ESXi02 for load balancing through vCenter.

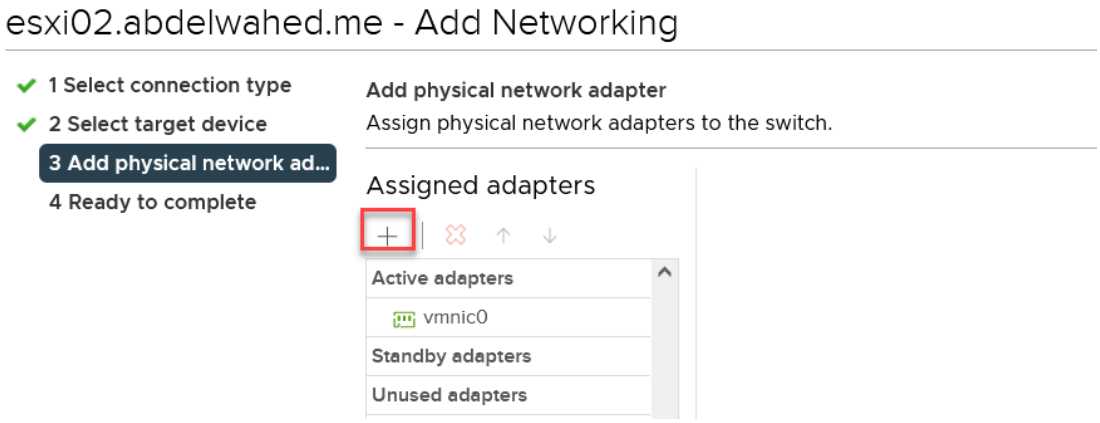
Insert an additional network interface card via the ESXi VM settings and reboot the server.

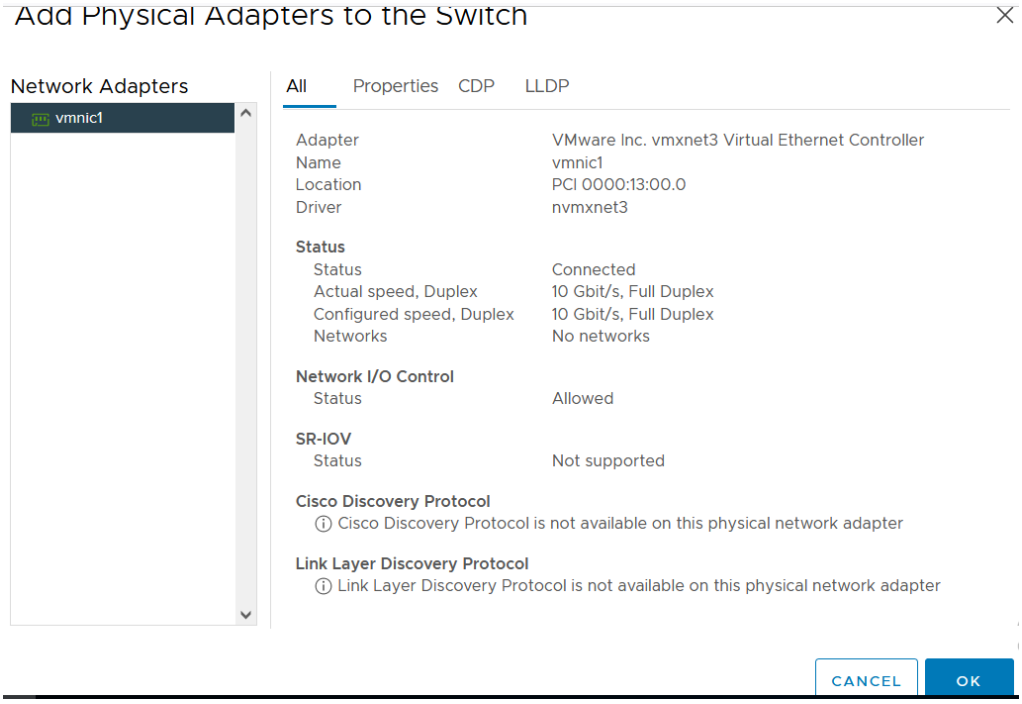


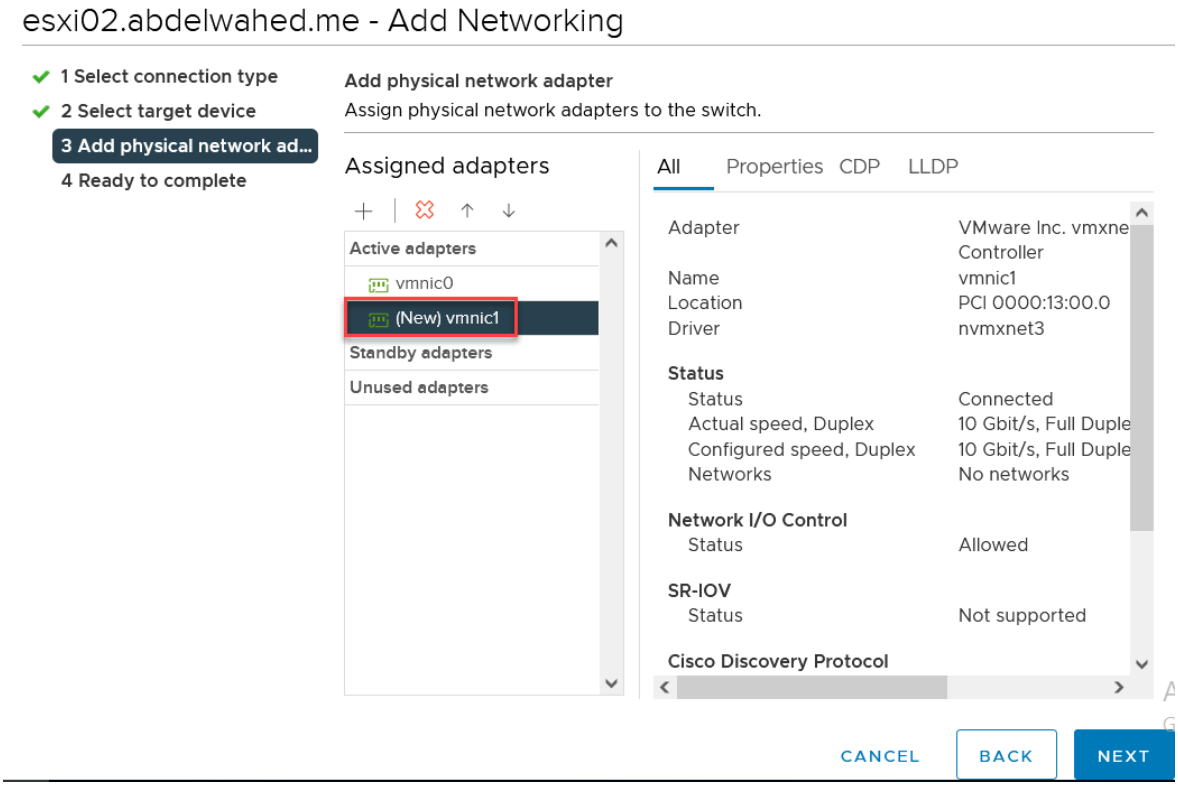
Below are two methods to add a network adapter: directly using 'Add Networking' or via the settings menu.

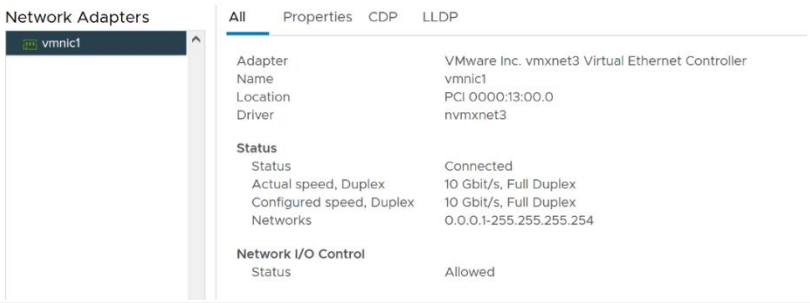


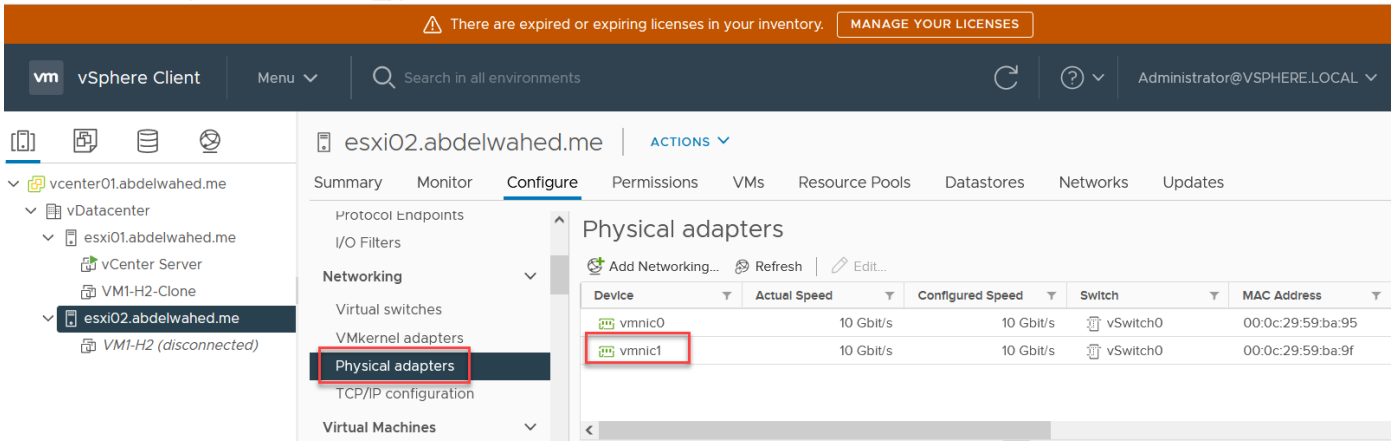

esxi02.abdelwahed.me - Add Networking
1 Select connection type
2 Select target device
3 Add physical network ad...
4 Ready to complete
Select connection type
Select a connection type to create.
VMkernel Network Adapter
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.
Virtual Machine Port Group for a Standard Switch
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.


esxi02.abdelwahed.me - 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
vmnic0
Standby adapters
Unused adapters

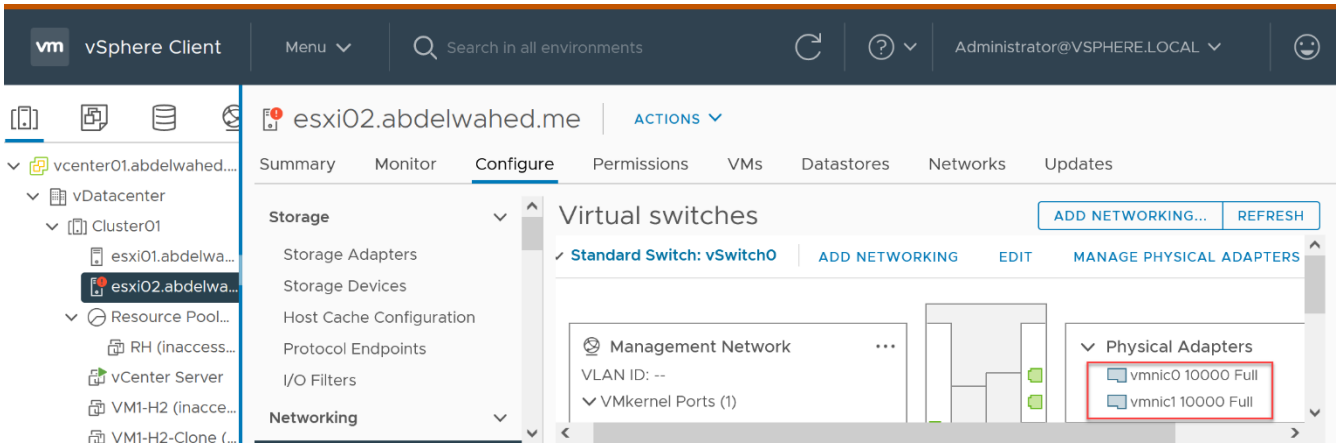

Add Physical Adapters to the Switch
Network Adapters
vmnic1
All
Properties
CDP
LLDP
Adapter
VMware Inc. vmxnet3 Virtual Ethernet Controller
Name
vmnic1
Location
PCI 0000:13:00.0
Driver
nvmxnet3
Status
Status
Connected
Actual speed, Duplex
10 Gbit/s, Full Duplex
Configured speed, Duplex
10 Gbit/s, Full Duplex
Networks
No networks
Network I/O Control
Status
Allowed
SR-IOV
Status
Not supported
Cisco Discovery Protocol
Cisco Discovery Protocol is not available on this physical network adapter
Link Layer Discovery Protocol
Link Layer Discovery Protocol is not available on this physical network adapter
CANCEL
OK


esxi02.abdelwahed.me - 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
vmnic0
(New) vmnic1
Standby adapters
Unused adapters
All
Properties
CDP
LLDP
Adapter
VMware Inc. vmxne
Controller
Name
vmnic1
Location
PCI 0000:13:00.0
Driver
nvmxnet3
Status
Status
Connected
Actual speed, Duplex
10 Gbit/s, Full Duple
Configured speed, Duplex
10 Gbit/s, Full Duple
Networks
No networks
Network I/O Control
Status
Allowed
SR-IOV
Status
Not supported
Cisco Discovery Protocol
CANCEL
BACK
NEXT



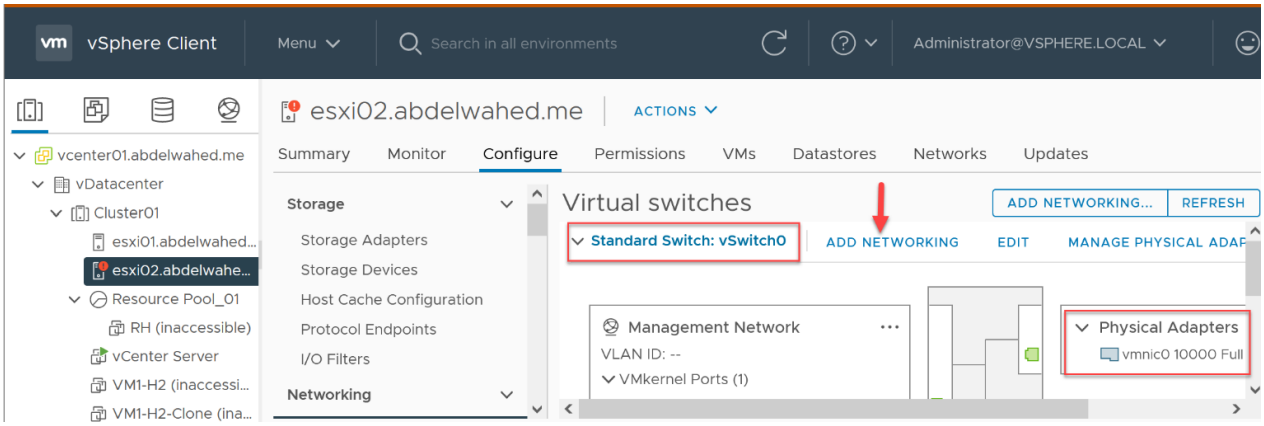


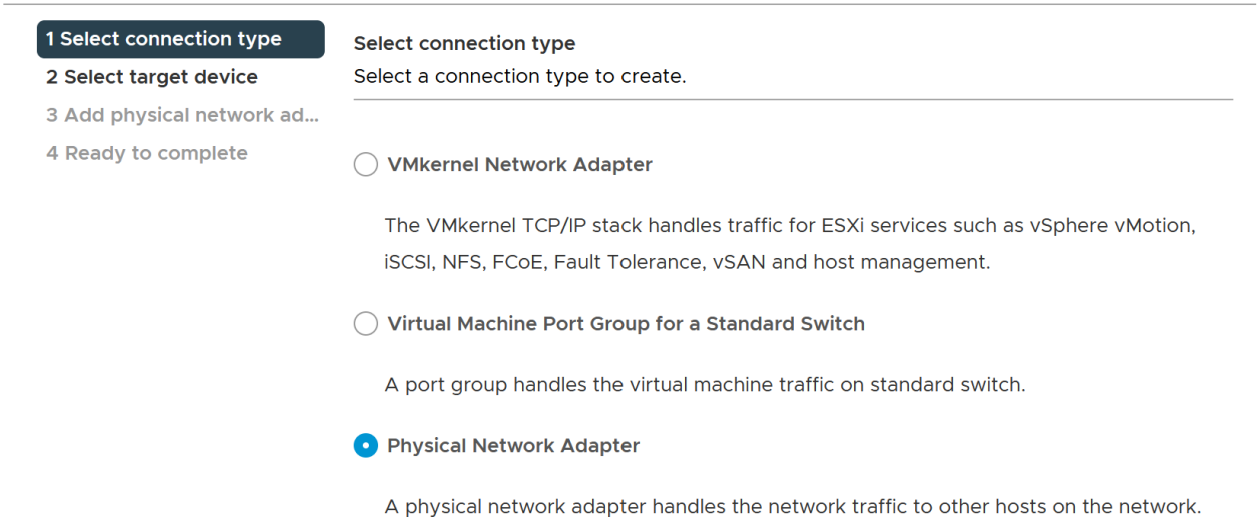
- Setting both NICs to "Active" on a vSphere vSwitch activates load balancing, which distributes network traffic between the NICs for better bandwidth utilization and improved network efficiency.

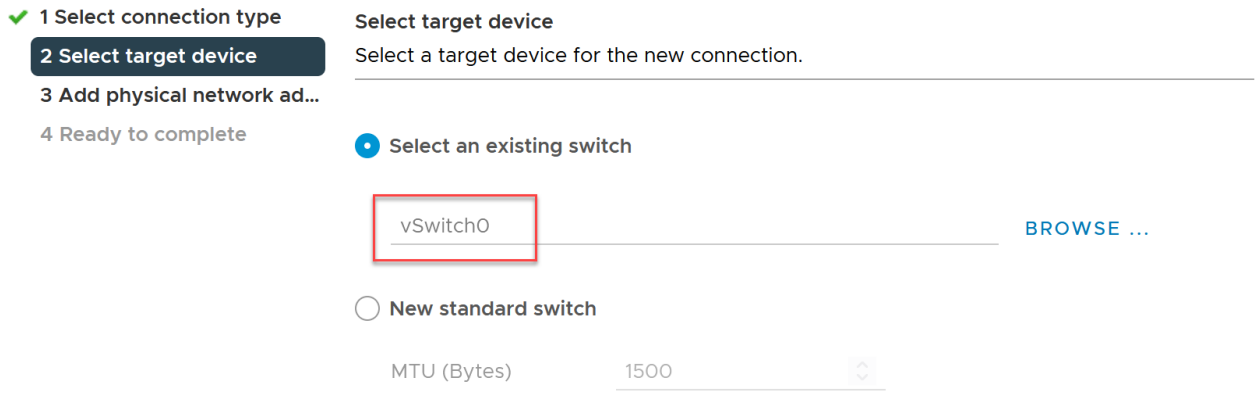


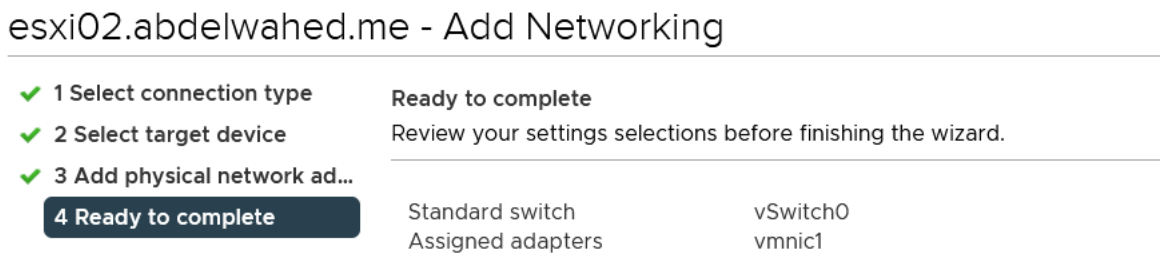
Attach a backup physical adapter to vSwitch0 (standard switch).

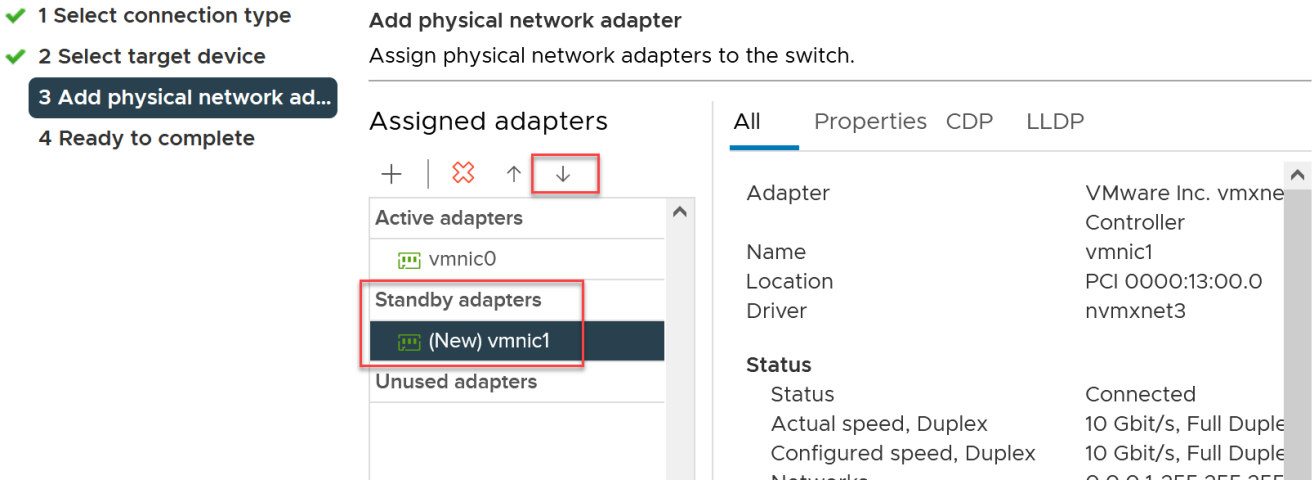
Begin by installing a new NIC adapter to the virtual machine and then proceed with the subsequent steps.



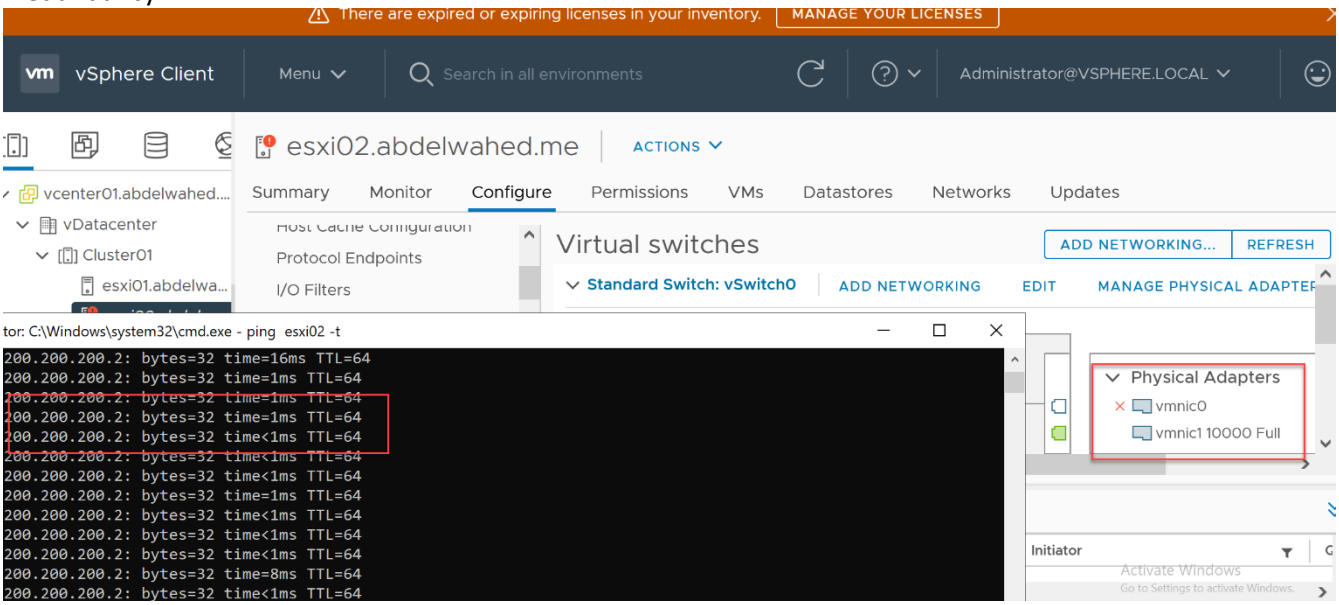



1 Select connection type
2 Select target device
3 Add physical network ad...
4 Ready to complete
Select target device
Select a target device for the new connection.
Select an existing switch
vSwitch0
BROWSE ...
New standard switch
MTU (Bytes)
1500

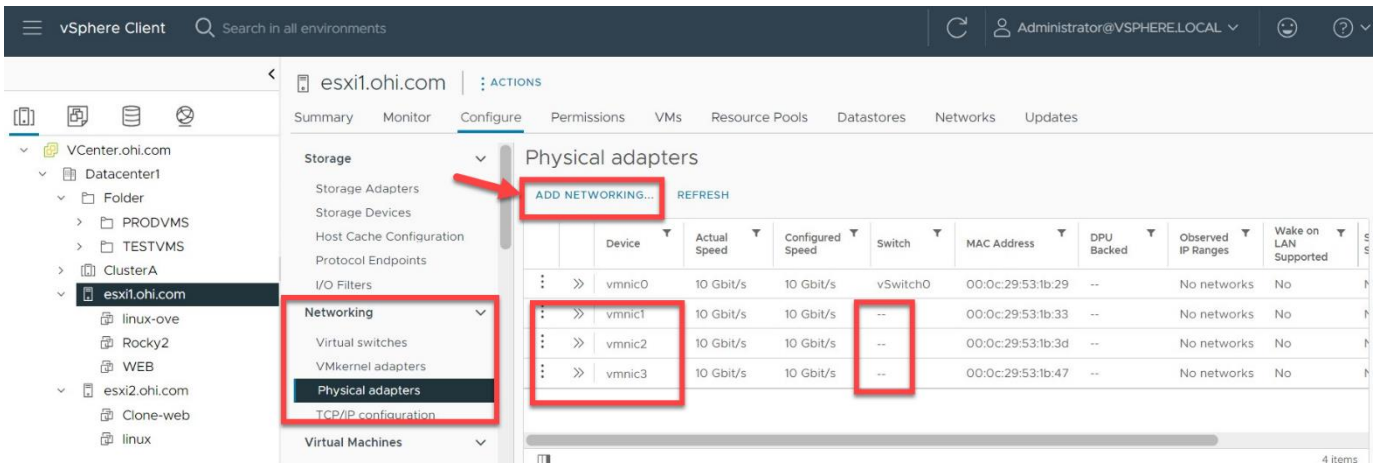

esxi02.abdelwahed.me - Add Networking
1 Select connection type
2 Select target device
3 Add physical network ad...
4 Ready to complete
Ready to complete
Review your settings selections before finishing the wizard.
Standard switch
vSwitch0
Assigned adapters
vmnic1

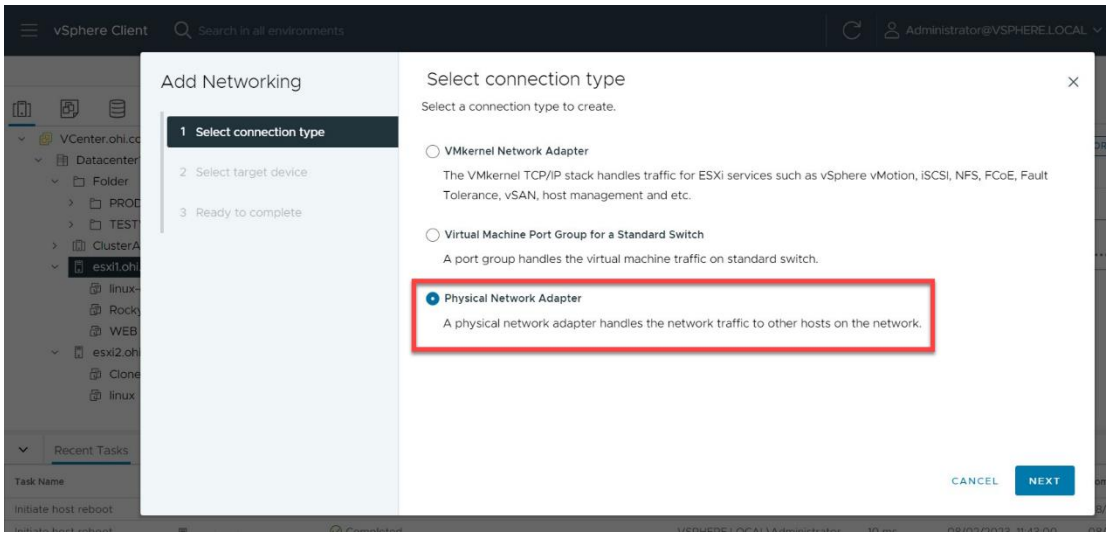

1 Select connection type
2 Select target device
3 Add physical network ad...
4 Ready to complete
Add physical network adapter
Assign physical network adapters to the switch.
Assigned adapters
Active adapters
vmnic0
Standby adapters
(New) vmnic1
Unused adapters
All
Properties
CDP
LLDP
Adapter
VMware Inc. vmxne
Controller
Name
vmnic1
Location
PCI 0000:13:00.0
Driver
nvmxnet3
Status
Status
Connected
Actual speed, Duplex
10 Gbit/s, Full Duple
Configured speed, Duplex
10 Gbit/s, Full Duple

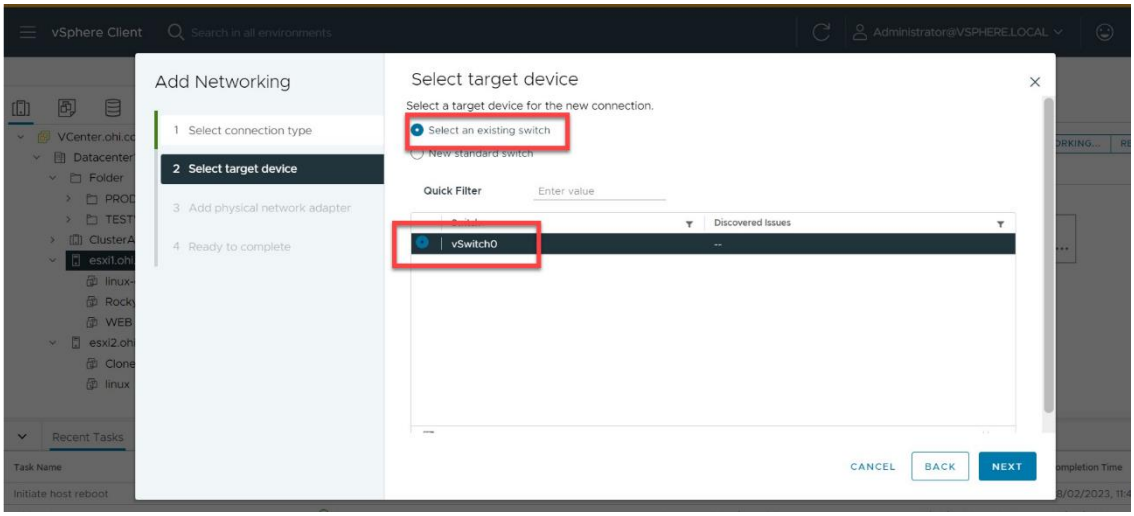
Upon disconnection of the primary network interface card, ESXi02 maintains continuous operation due to the failover capabilities in place on the secondary NIC. This guarantees consistent performance and provides network redundancy.

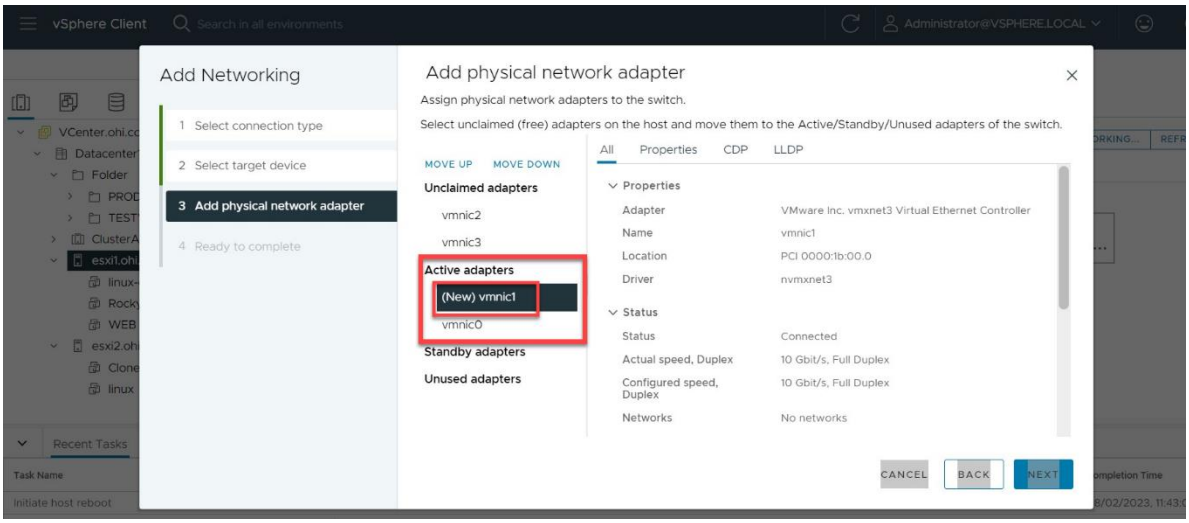


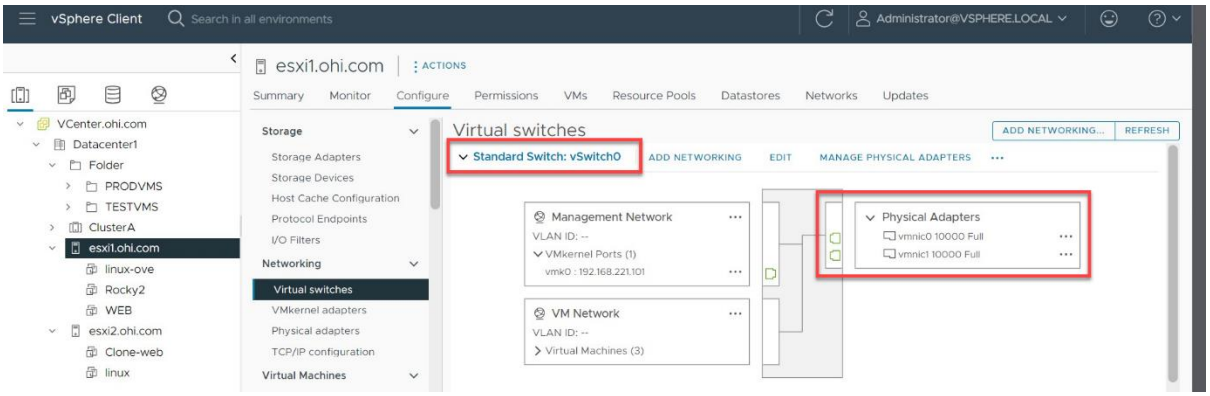
Load Balancing and Standby NIC Features in vSphere 8



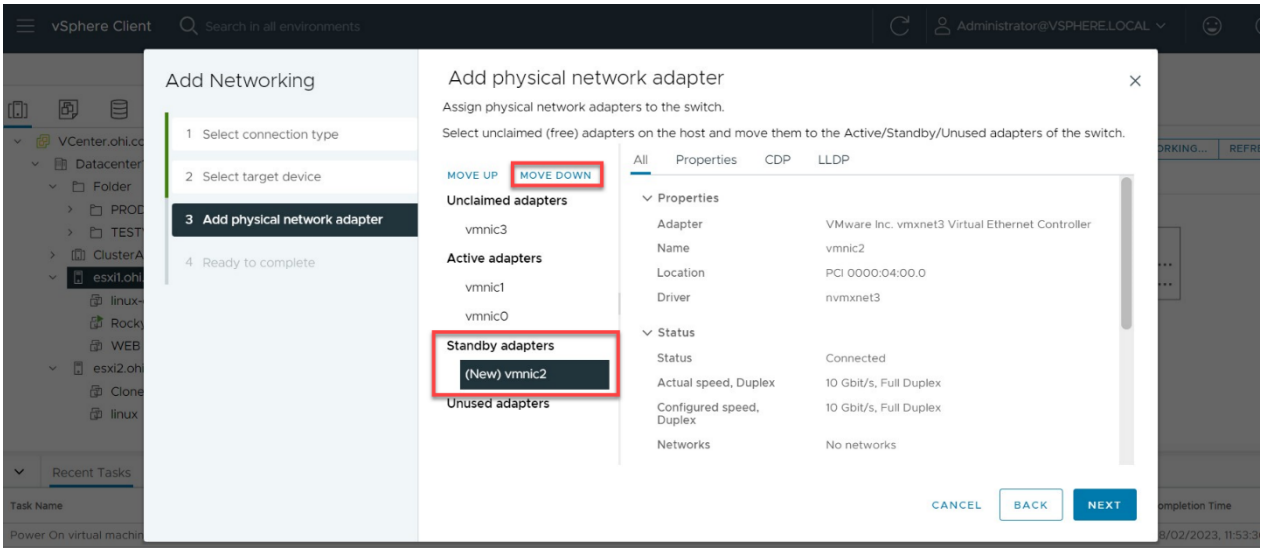


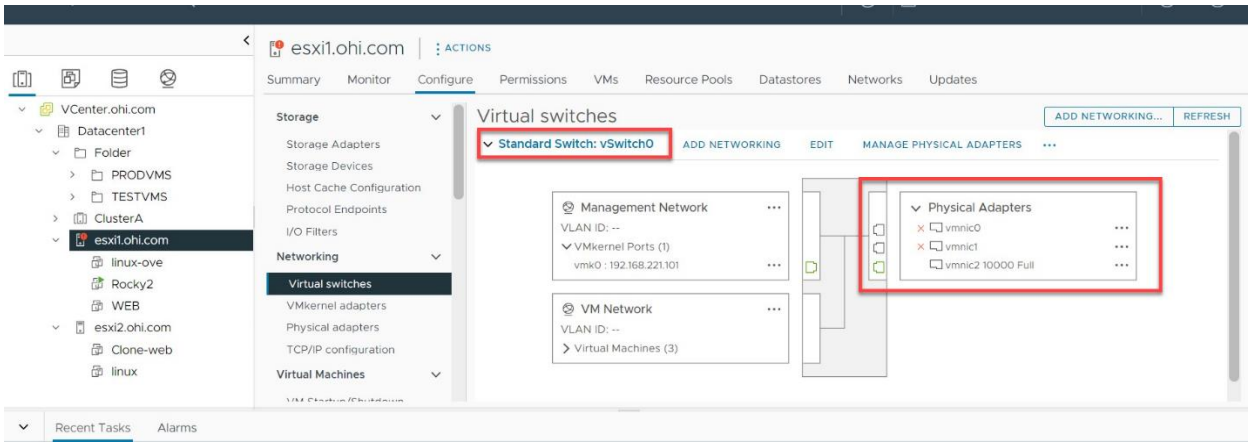






Up next on standby.

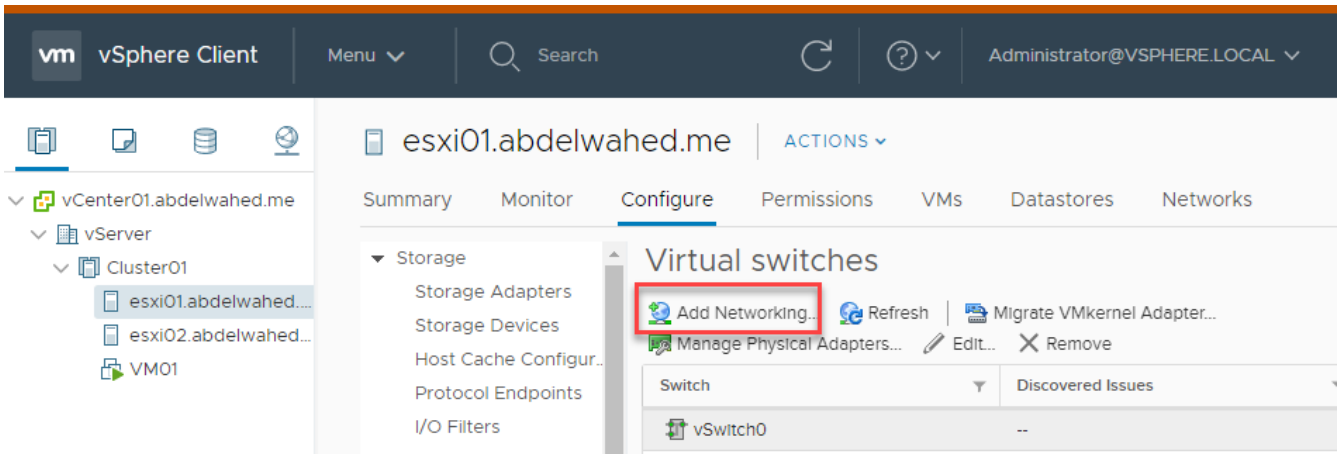


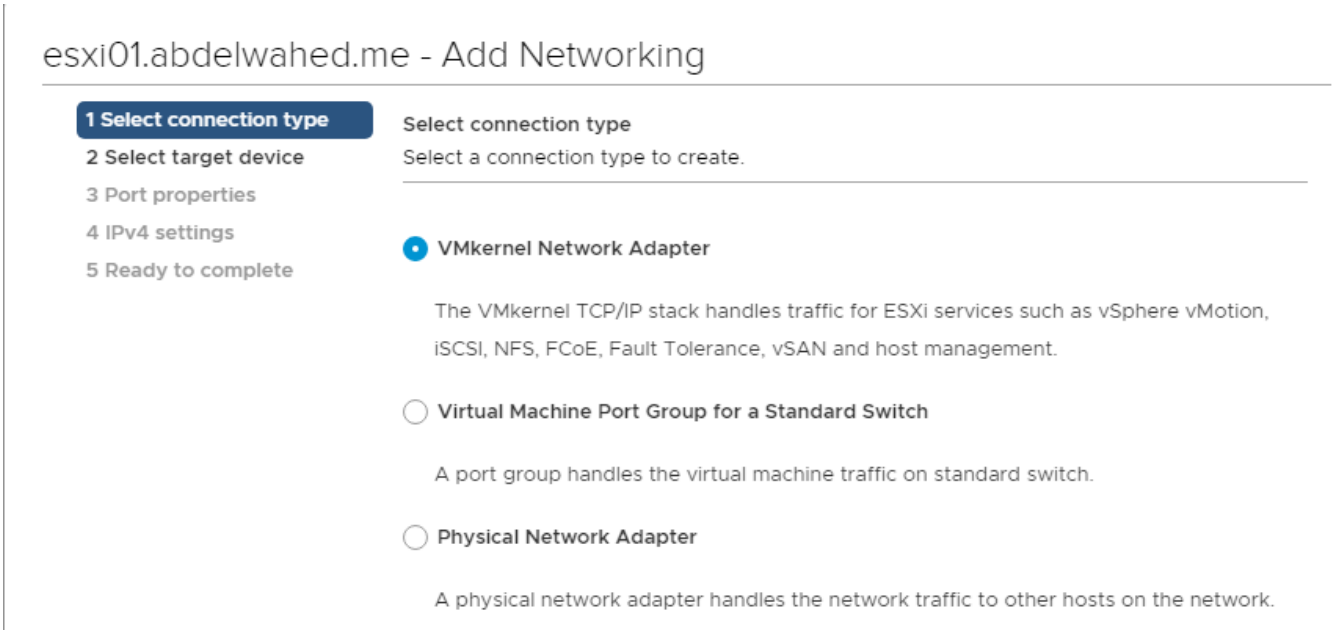

esxi1.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
VCenter.ohi.com
Datacenter1
Folder
PRODVMS
TESTVMS
ClusterA
esxi1.ohi.com
linux-ove
Rocky2
WEB
esxi2.ohi.com
Clone-web
linux
Storage
Storage Adapters
Storage Devices
Host Cache Configuration
Protocol Endpoints
I/O Filters
Networking
Virtual switches
VMkernel adapters
Physical adapters
TCP/IP configuration
Virtual Machines
Virtual switches
ADD NETWORKING...
REFRESH
Standard Switch: vSwitch0
ADD NETWORKING
EDIT
MANAGE PHYSICAL ADAPTERS
Management Network
VLAN ID: --
VMkernel Ports (1)
vmk0 : 192.168.221.101
VM Network
VLAN ID: --
Virtual Machines (3)
Physical Adapters
vmnic0
vmnic1
vmnic2 10000 Full
Recent Tasks
Alarms

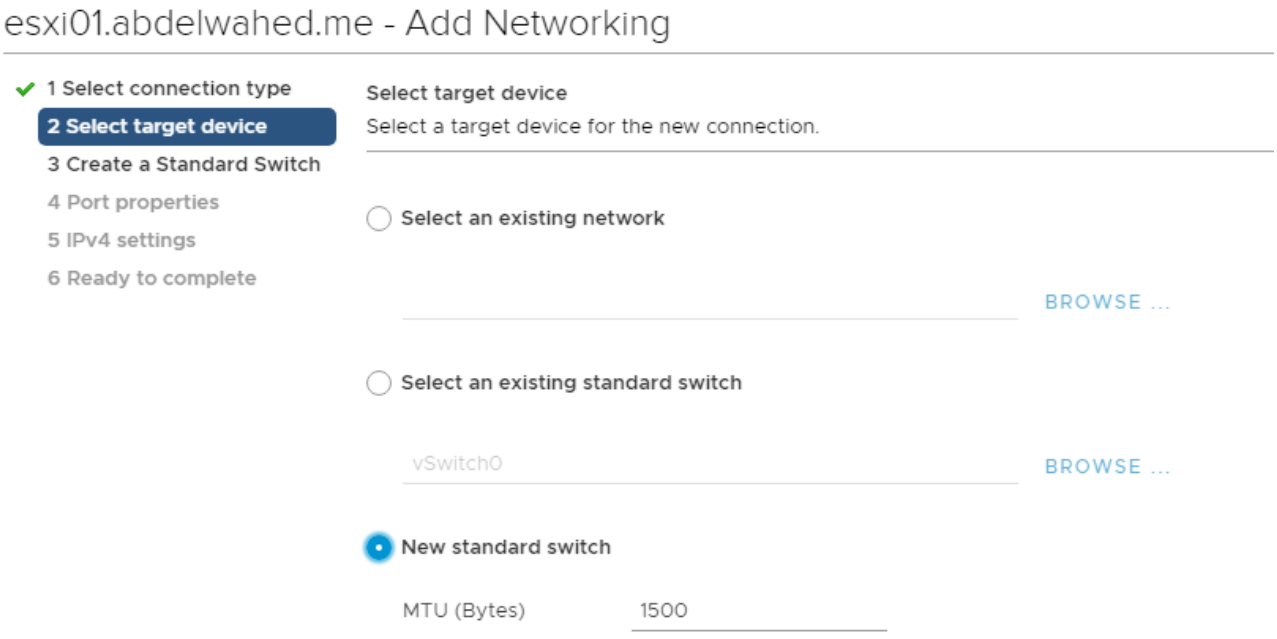
Adding VMkernel Port for Management in vSphere

1- For both ESXi servers, install a new NIC with a Host-only profile (restart the network management for the NIC to show up) and do not assign an IP address.
2- Add a new switch to both ESXi servers for VMKernel port assignment.

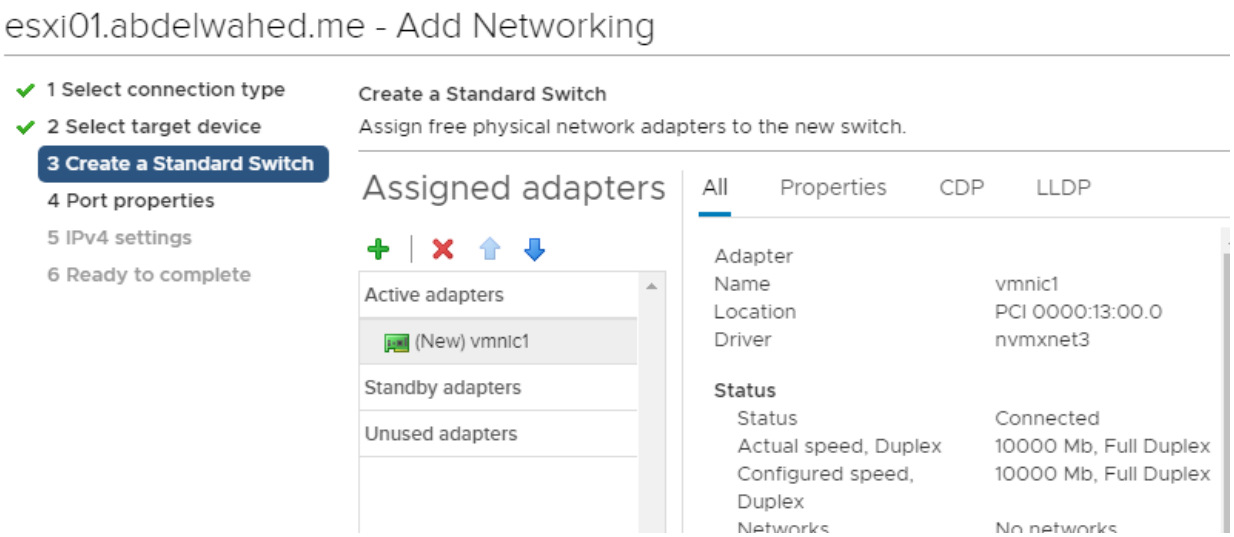
Please be aware that it's advisable for each VMkernel to serve a single purpose, possess a distinct IP address, and be set up on a separate VLAN.

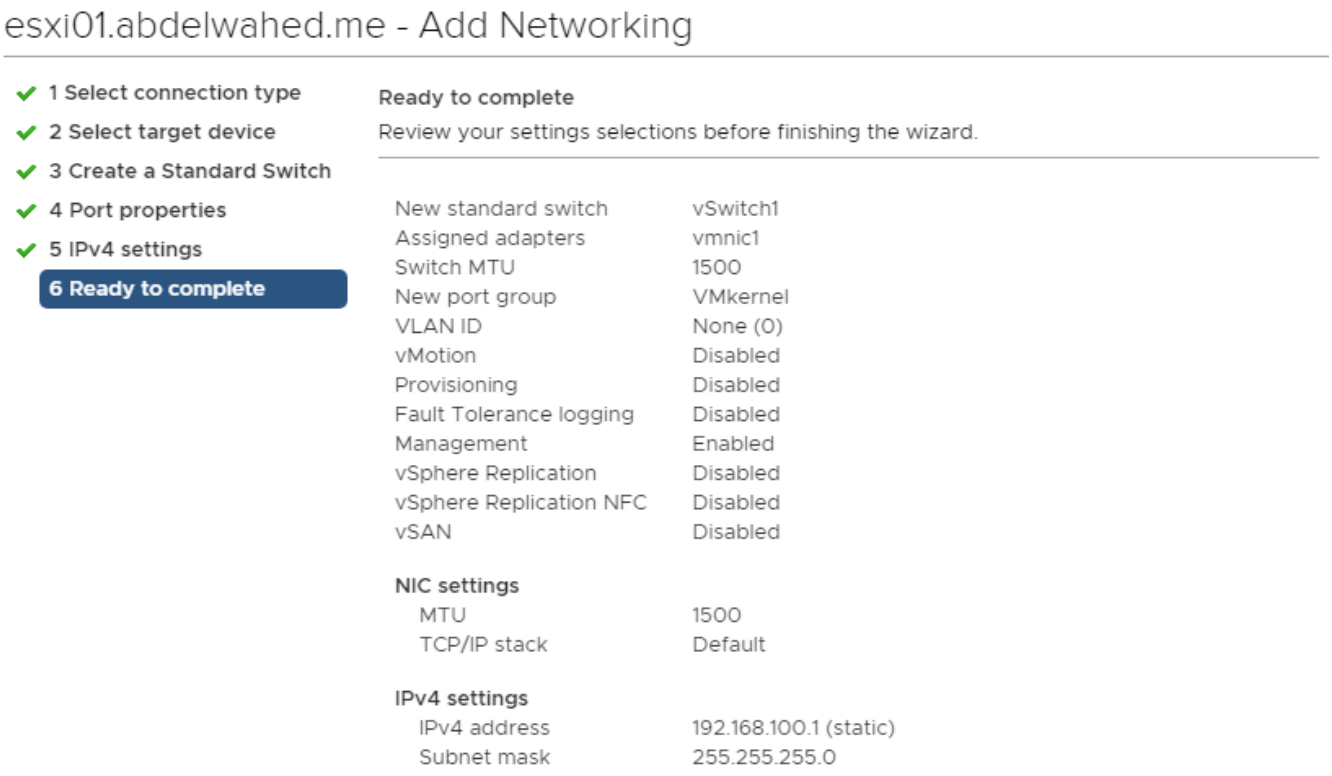


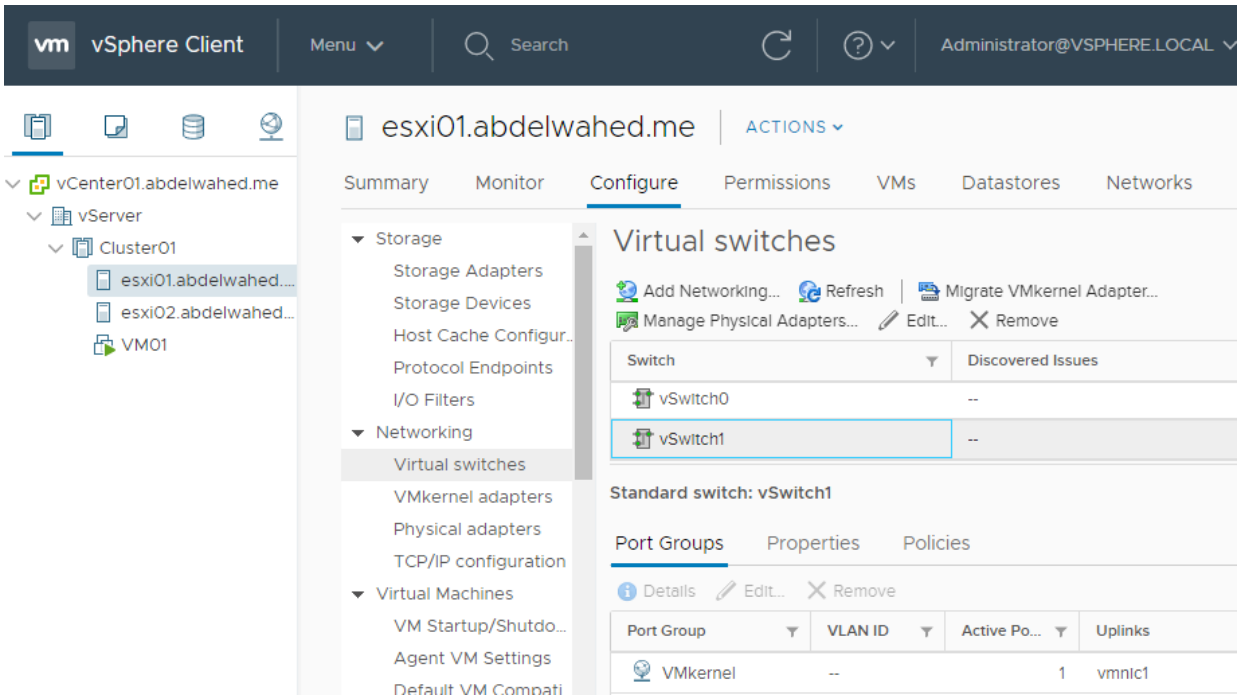


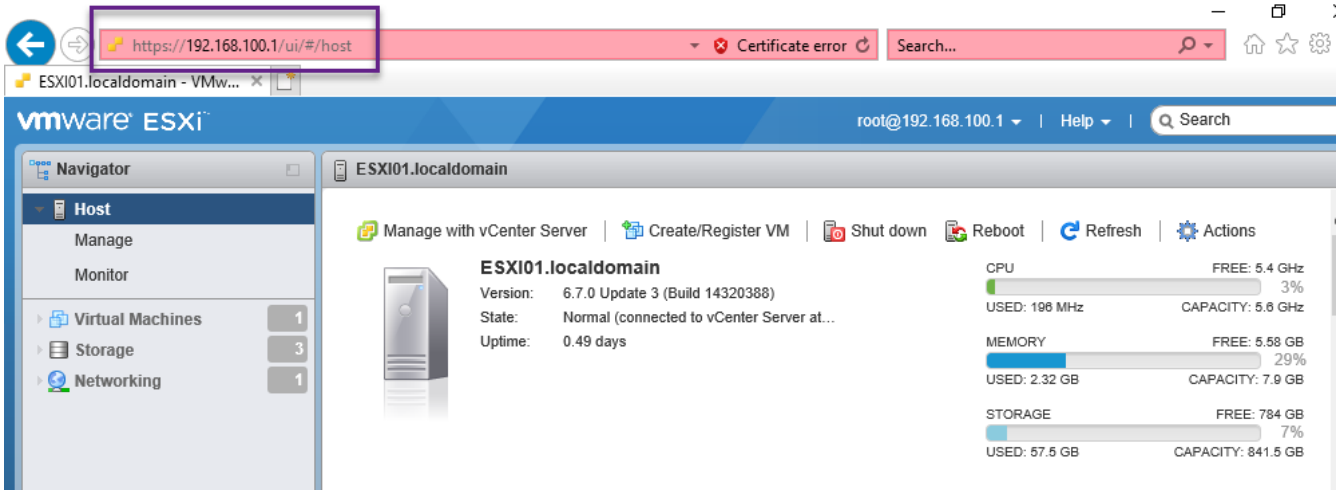


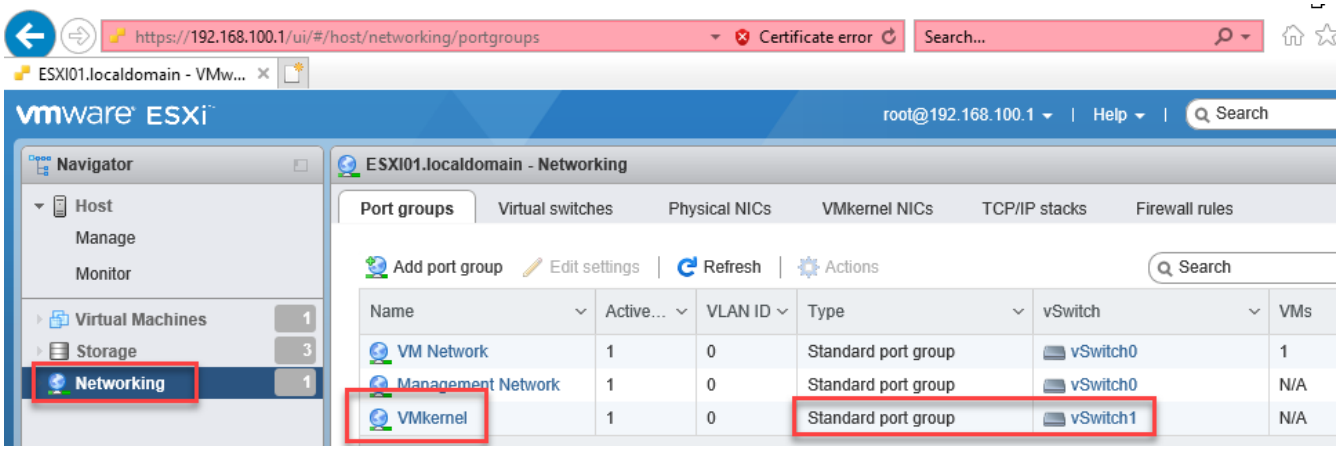
- **MTU (Maximum Transmission Unit)** represents the largest packet or frame size, specified in bytes, that can be sent over a network interface without fragmentation.
- **Ethernet Default**: For Ethernet, the default MTU size is typically **1500 bytes**.
- **Jumbo Frames**: In modern Ethernet networks, especially in data centers and for specific use-cases, the MTU can be increased to up to **9000 bytes**. This is often referred to as using "jumbo frames".
- **Example**: Jumbo frames might be used within a storage area network (SAN) because larger frames can improve efficiency by reducing the overhead of the header information for each packet.



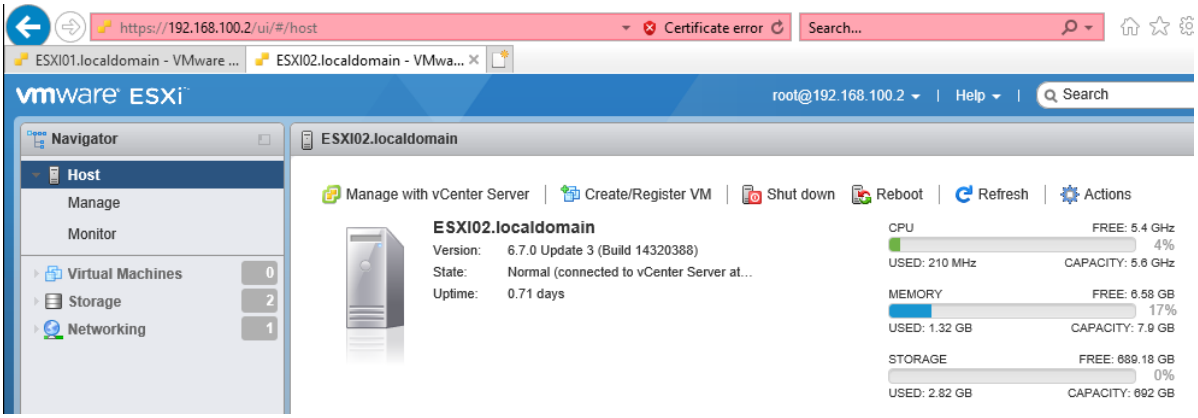

esxi01.abdelwahed.me - Add Networking
1 Select connection type
2 Select target device
3 Create a Standard Switch
4 Port properties
5 IPv4 settings
6 Ready to complete
Ready to complete
Review your settings selections before finishing the wizard.
New standard switch vSwitch1
Assigned adapters vmnic1
Switch MTU 1500
New port group VMkernel
VLAN ID None (0)
vMotion Disabled
Provisioning Disabled
Fault Tolerance logging Disabled
Management Enabled
vSphere Replication Disabled
vSphere Replication NFC Disabled
vSAN Disabled
NIC settings
MTU 1500
TCP/IP stack Default
IPv4 settings
IPv4 address 192.168.100.1 (static)
Subnet mask 255.255.255.0


vSphere Client
Menu
Search
Administrator@VSPHERE.LOCAL
vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed....
esxi02.abdelwahed...
VM01
esxi01.abdelwahed.me
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Datastores
Networks
Storage
Storage Adapters
Storage Devices
Host Cache Configur...
Protocol Endpoints
I/O Filters
Networking
Virtual switches
VMkernel adapters
Physical adapters
TCP/IP configuration
Virtual Machines
VM Startup/Shutdo...
Agent VM Settings
Default VM Compati...
Virtual switches
Add Networking...
Refresh
Migrate VMkernel Adapter...
Manage Physical Adapters...
Edit...
Remove
Switch
Discovered Issues
vSwitch0
vSwitch1
Standard switch: vSwitch1
Port Groups
Properties
Policies
Details
Edit...
Remove
Port Group
VLAN ID
Active Po...
Uplinks
VMkernel
1
vmnic1

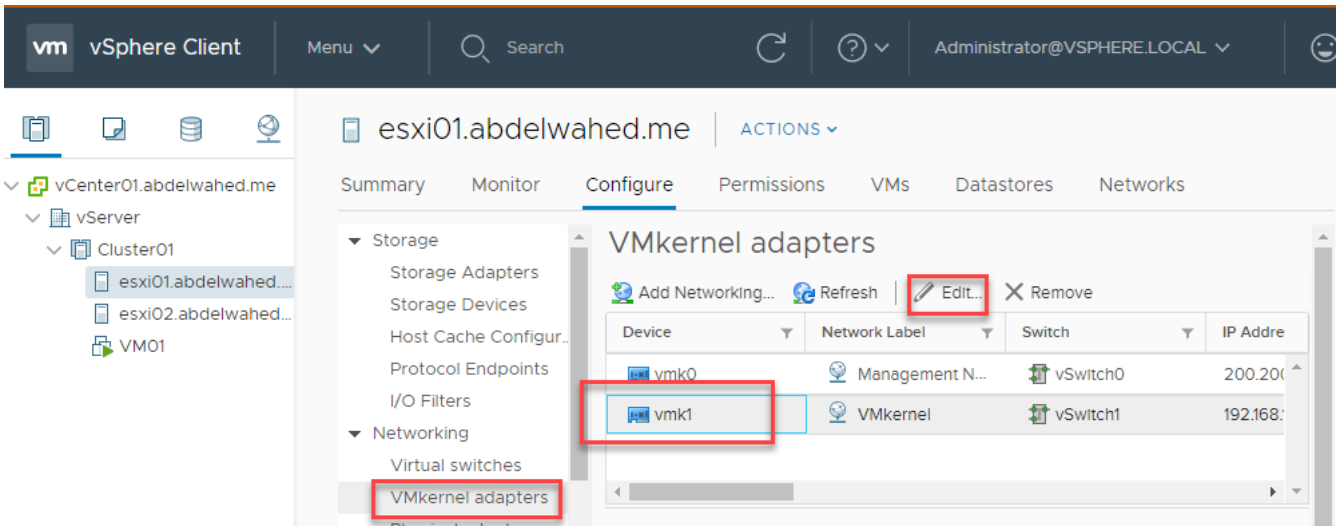


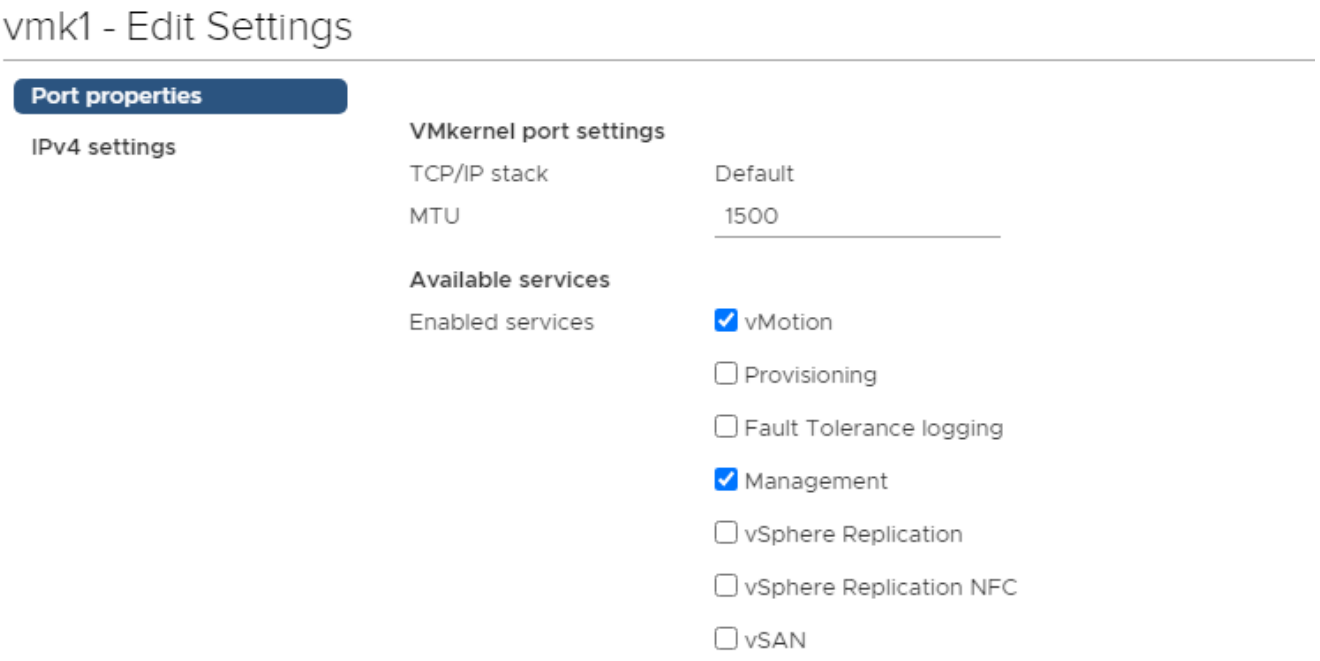


On a different computer, assign an additional IP address to the Network Interface Card and attempt to connect to the VMKernel port of ESXi01, then apply the same configuration to ESXi02.



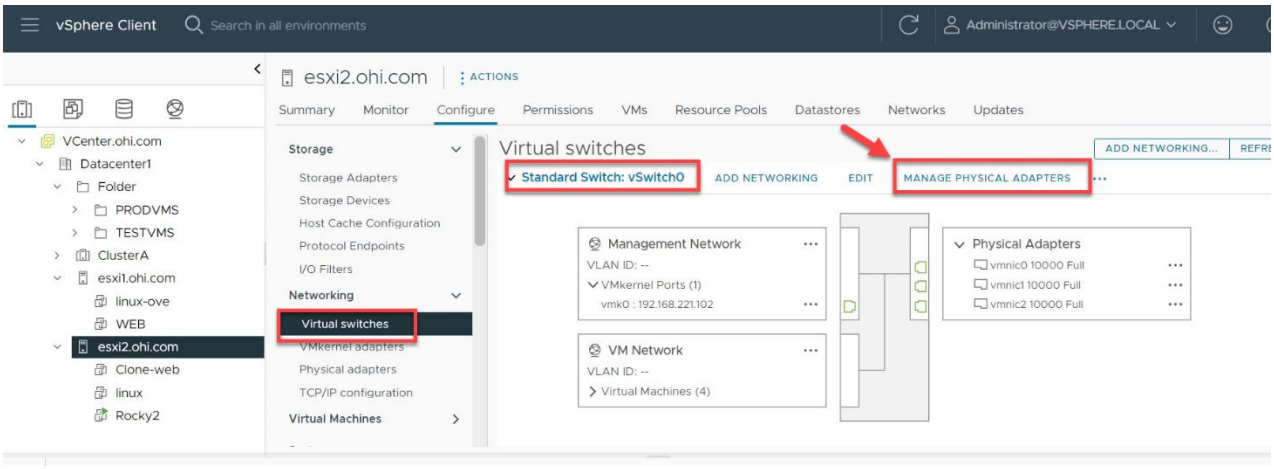
Modify VMkernel port settings to enable vMotion capability (for storage and VM migration).



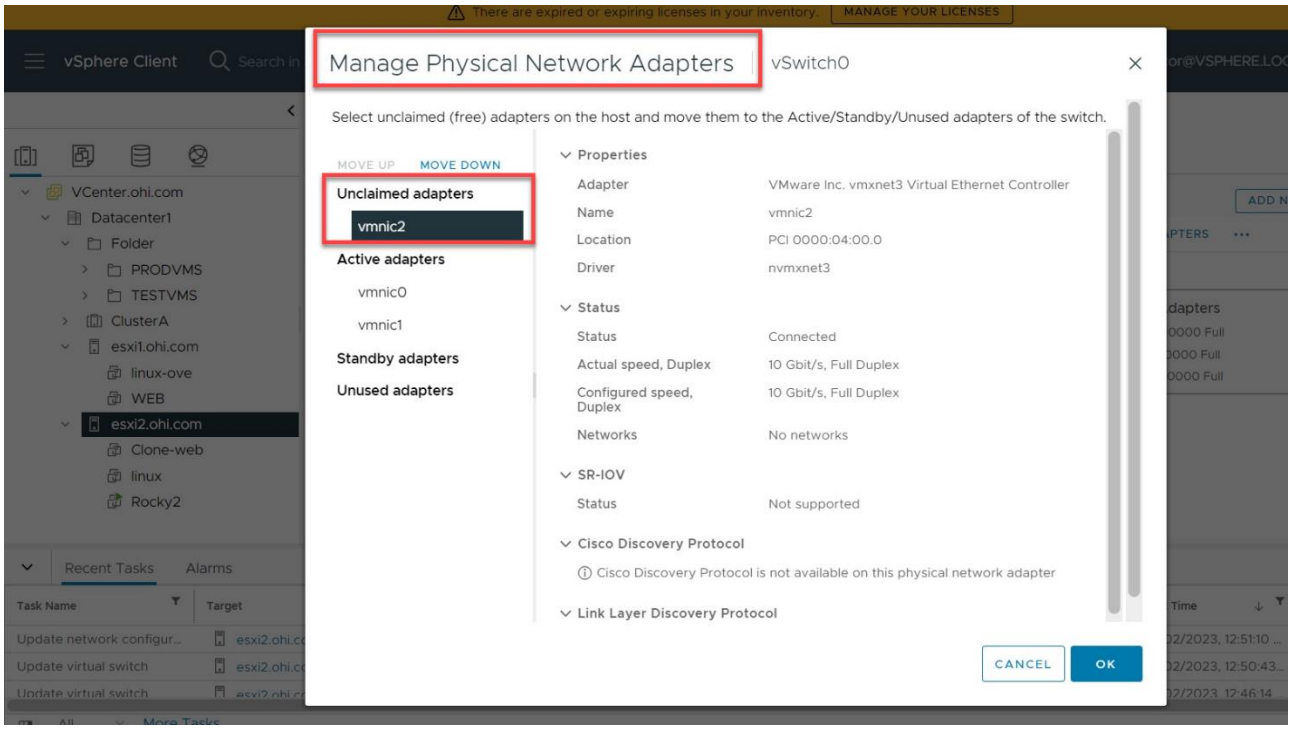


Please be aware that for executing storage or VM migration across ESXi hosts, it's crucial to set up a dedicated VMKernel adapter to handle vMotion traffic. This task can be accomplished by creating a new adapter or enabling the vMotion capability on an existing one, allowing the live relocation of virtual machines between hosts seamlessly and without any interruptions.

Remove Physical NIC from vSwitch



Transfer that network interface card to the unassigned adapter.

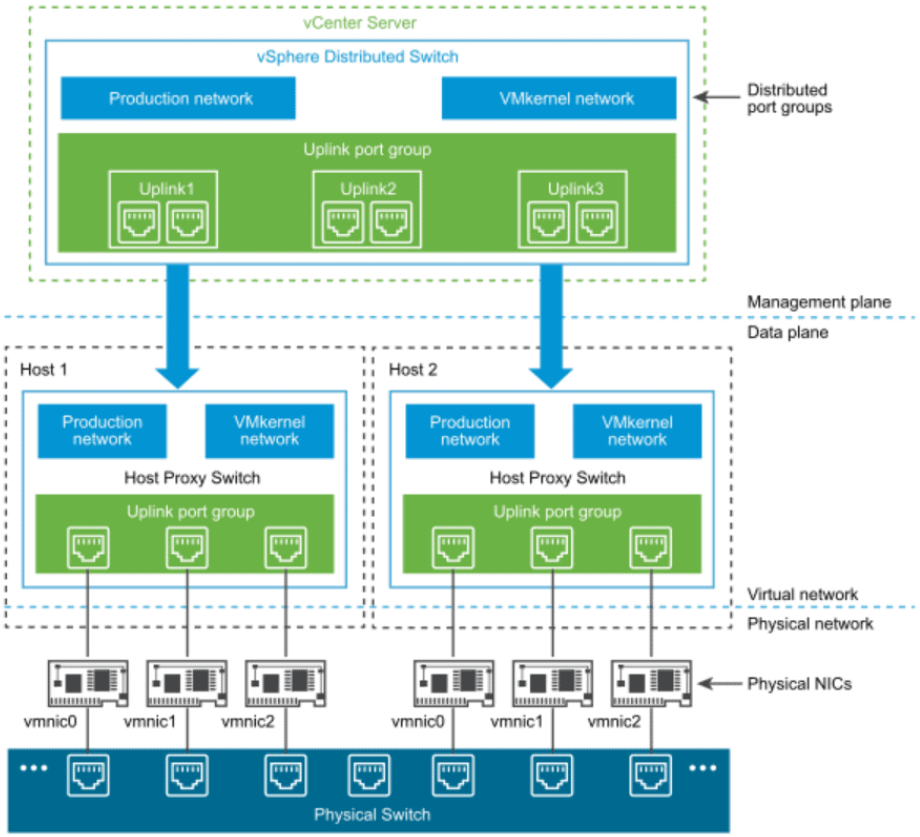


VMware vSphere Distributed Virtual Switch (VDS)

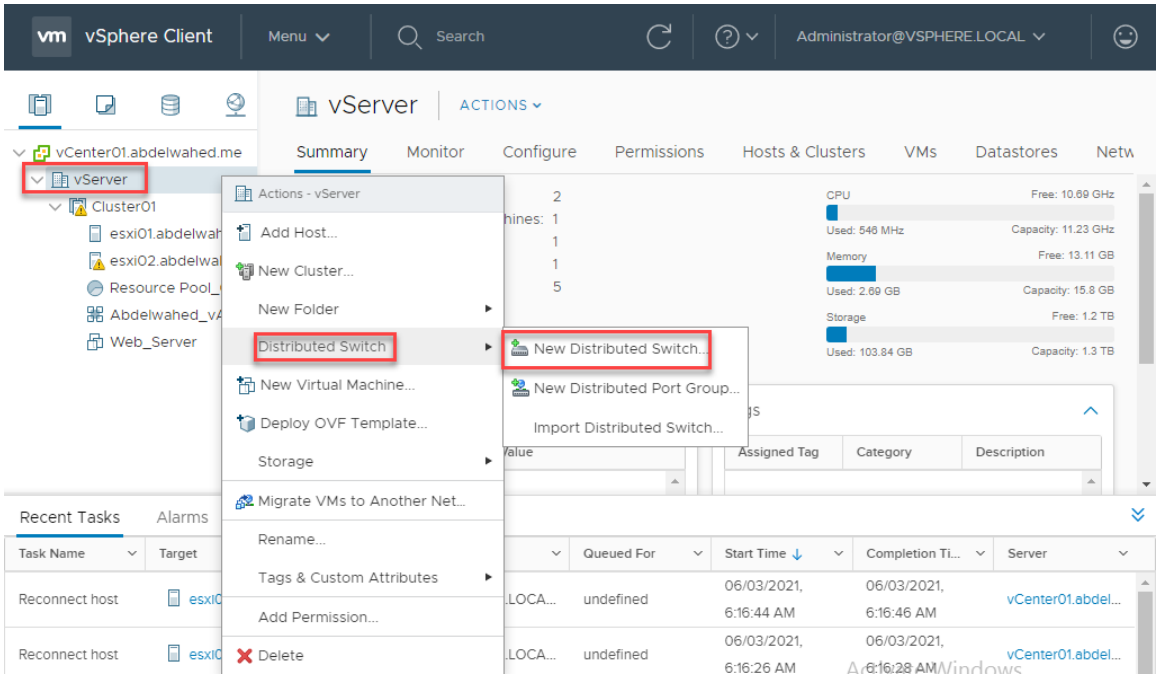
A VMware Virtual Distributed Switch (VDS) allows you to manage network switches centrally at the data center level, which can help to simplify management and improve efficiency. Instead of creating separate switches for each ESXi server, you can create a single VDS that spans multiple hosts within a data center.

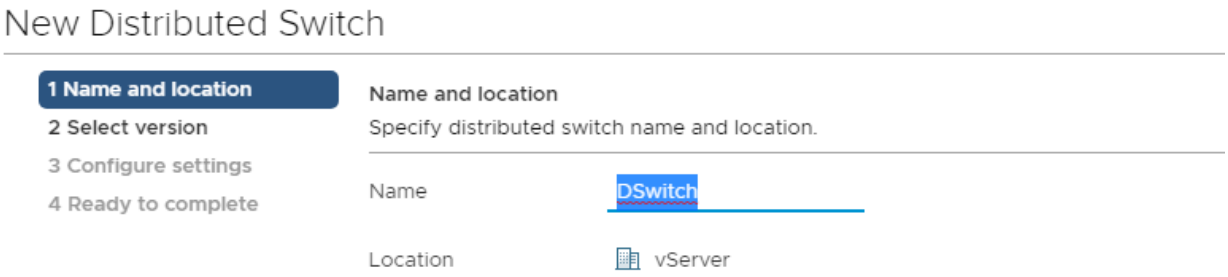
Key Benefits of VDS

1. **Centralized Management**:
   - Configure network settings such as VLANs, port groups, and traffic shaping from a central location.
   - Apply settings to all hosts that are part of the VDS to ensure consistency and avoid errors.
2. **Consistency**:
   - Ensures that network configurations are consistent across all ESXi hosts in the data center.
   - Reduces the risk of misconfiguration by managing switches at the individual host level.
3. **Policy Application**:
   - Apply policies and settings across multiple hosts to meet security and compliance requirements consistently.
   - Monitor network traffic and performance from a central location and optimize as needed.

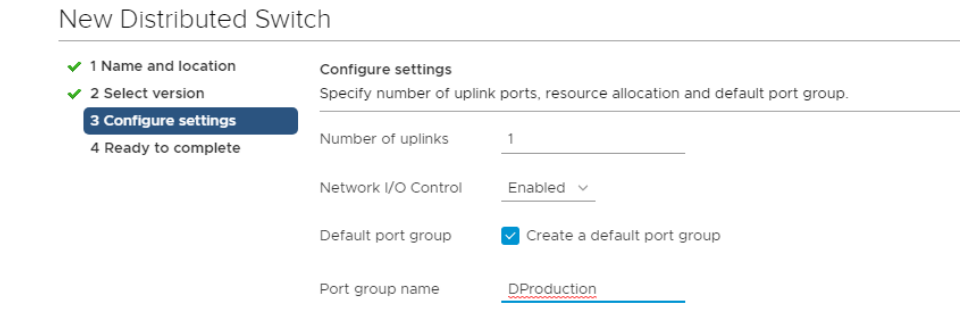


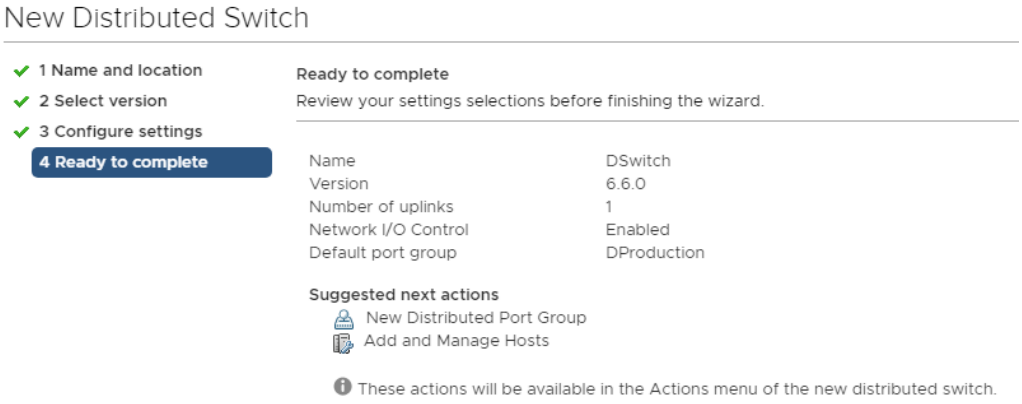
Initially, install NICs on the ESXi servers.

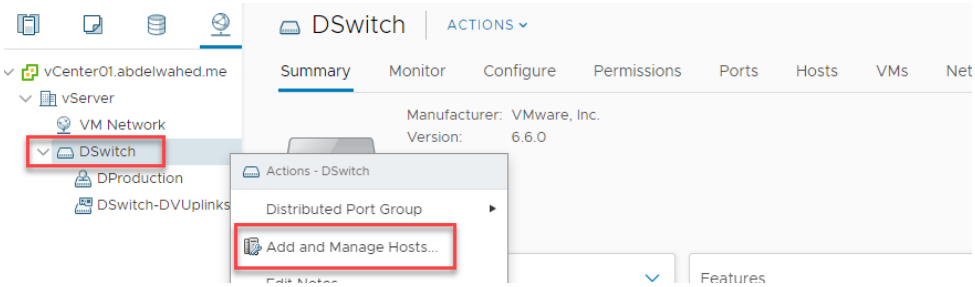


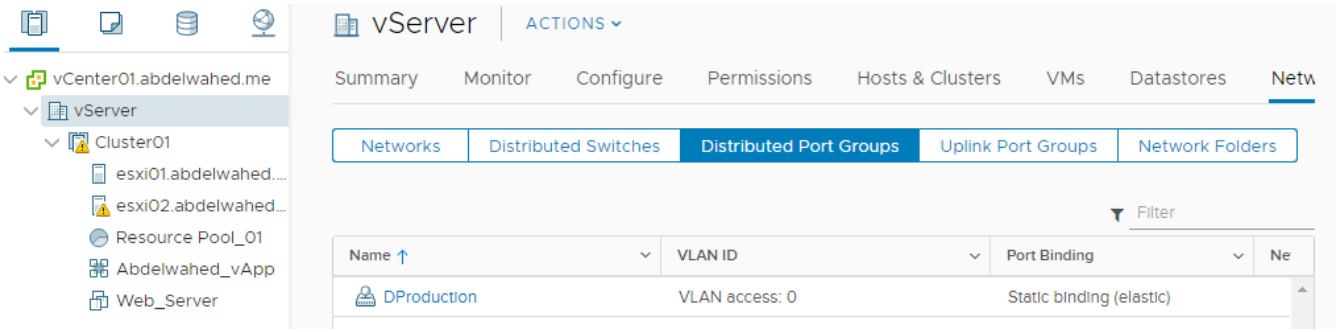


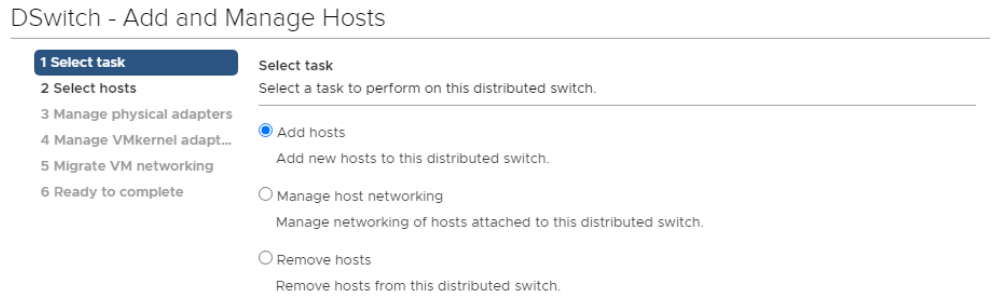
Choose the earliest version of ESXi available if you're working with various versions, and remember that this choice cannot be downgraded later.

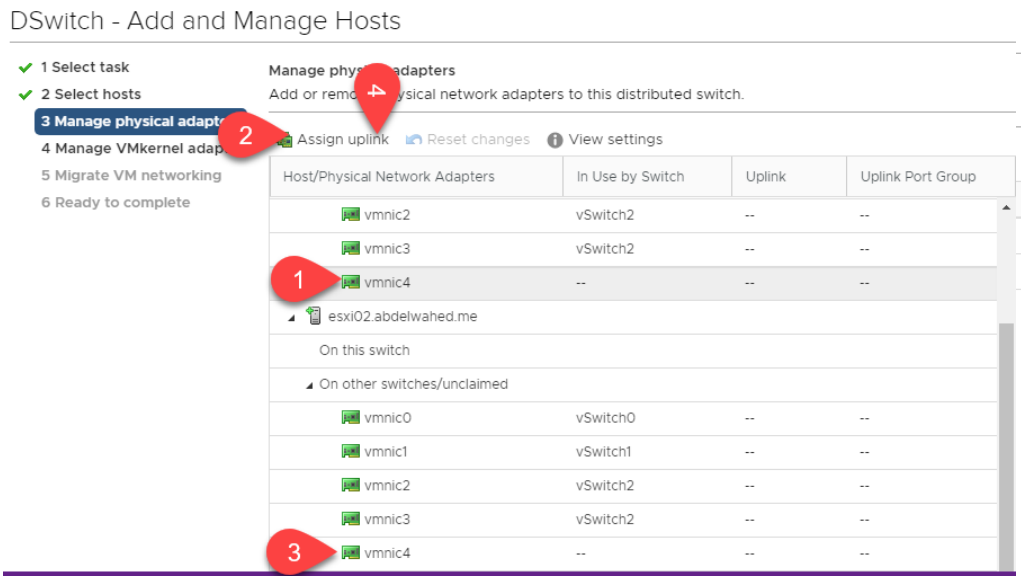

New Distributed Switch
1 Name and location
2 Select version
3 Configure settings
4 Ready to complete
Configure settings
Specify number of uplink ports, resource allocation and default port group.
Number of uplinks
1
Network I/O Control
Enabled
Default port group
Create a default port group
Port group name
DProduction


New Distributed Switch
1 Name and location
2 Select version
3 Configure settings
4 Ready to complete
Ready to complete
Review your settings selections before finishing the wizard.
Name
DSwitch
Version
6.6.0
Number of uplinks
1
Network I/O Control
Enabled
Default port group
DProduction
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.

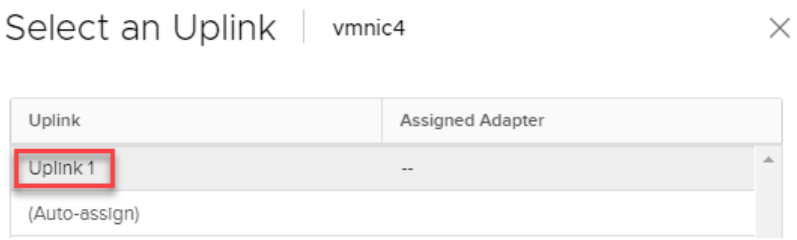

DSwitch
ACTIONS
vCenter01.abdelwahed.me
vServer
VM Network
DSwitch
DProduction
DSwitch-DVUplinks
Summary
Monitor
Configure
Permissions
Ports
Hosts
VMs
Manufacturer: VMware, Inc.
Version: 6.6.0
Actions - DSwitch
Distributed Port Group
Add and Manage Hosts...
Features


vServer
ACTIONS
vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed....
esxi02.abdelwahed...
Resource Pool_01
Abdelwahed_vApp
Web_Server
Summary
Monitor
Configure
Permissions
Hosts & Clusters
VMs
Datastores
Netw
Networks
Distributed Switches
Distributed Port Groups
Uplink Port Groups
Network Folders
Filter
Name
VLAN ID
Port Binding
Ne
DProduction
VLAN access: 0
Static binding (elastic)

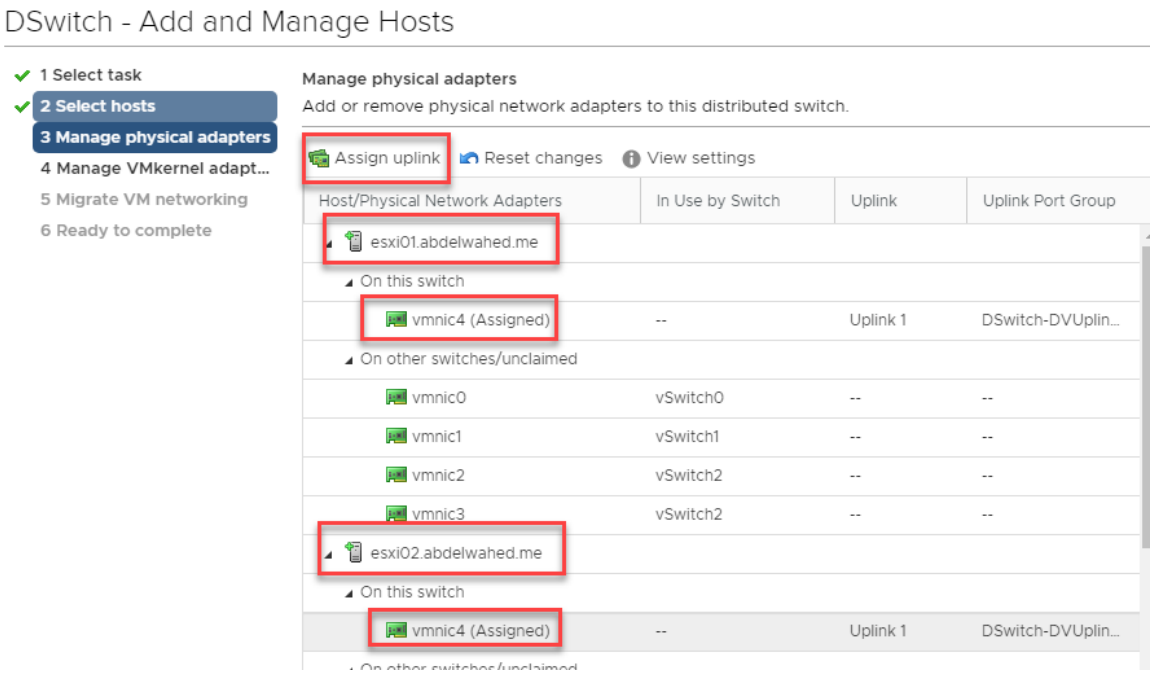


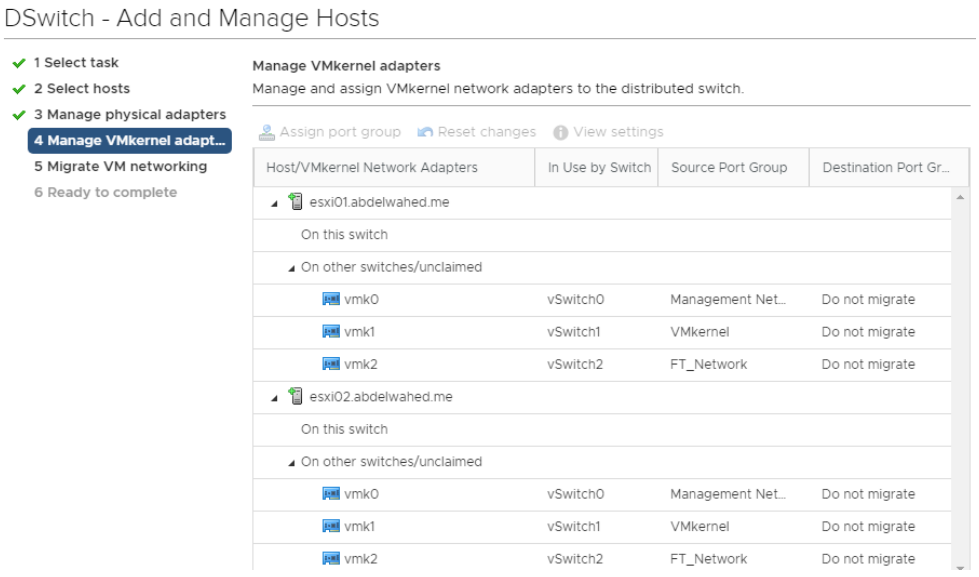


Uplinks correspond to the count of Network Interface Cards (NICs), which you can later adjust by adding or reducing the number. For instance, if there are initially 2 uplinks per server, you can increase the total to 4.

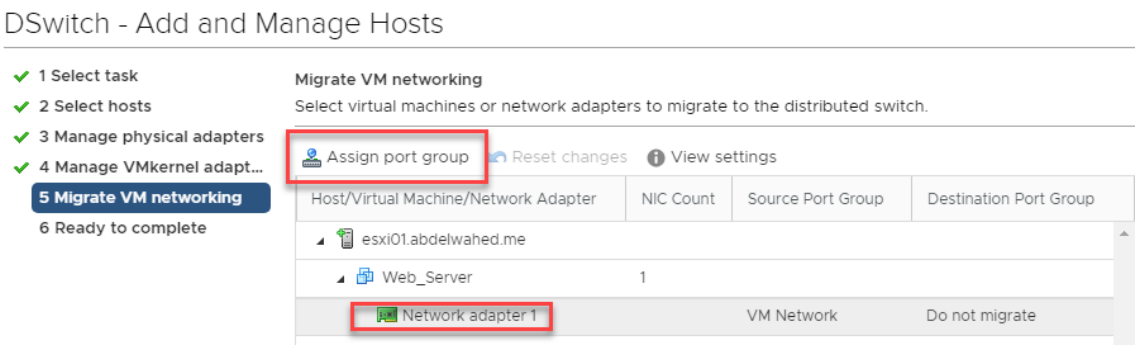


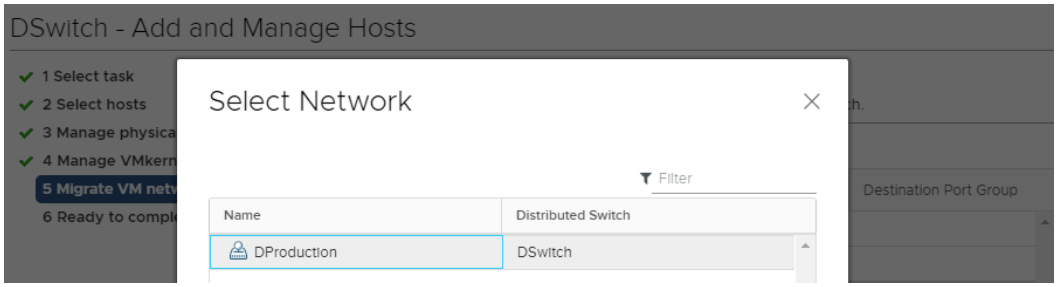
NIC now connected to DSwitch.

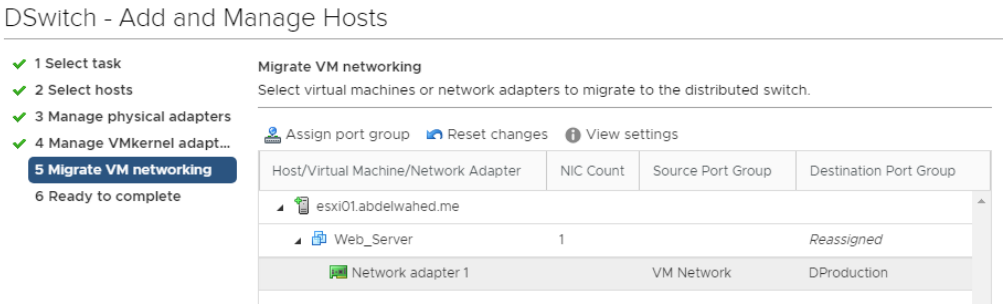


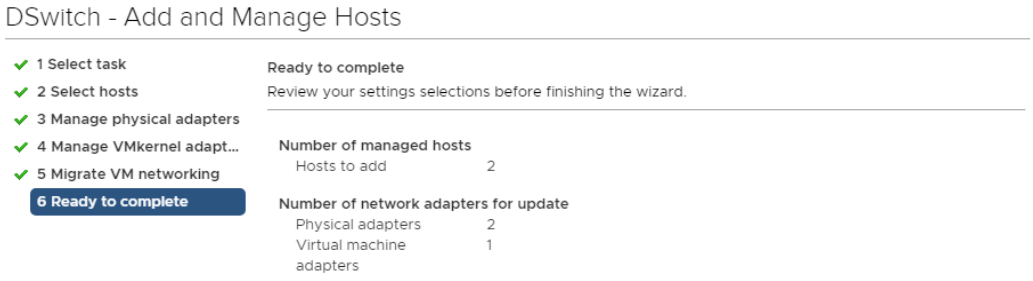


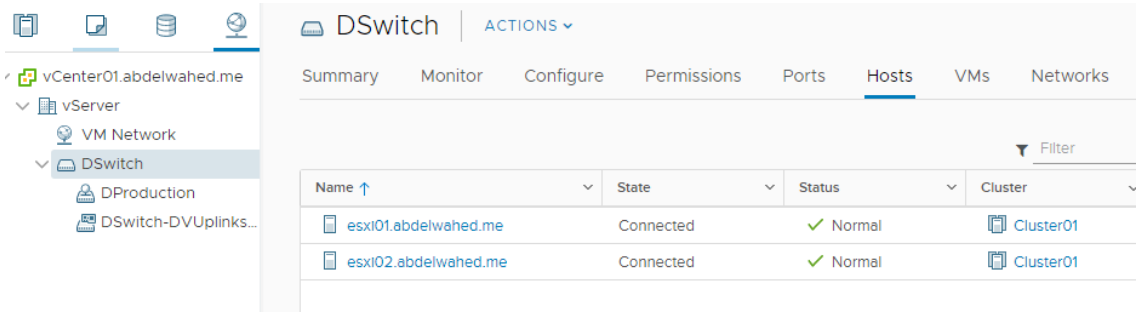
Now transfer the VM network to the new production DSwitch (currently, we have only the Web-Server on ESXi01).


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.
Assign port group
Reset changes
View settings
Host/Virtual Machine/Network Adapter
NIC Count
Source Port Group
Destination Port Group
esxi01.abdelwahed.me
Web_Server
1
Network adapter 1
VM Network
Do not migrate

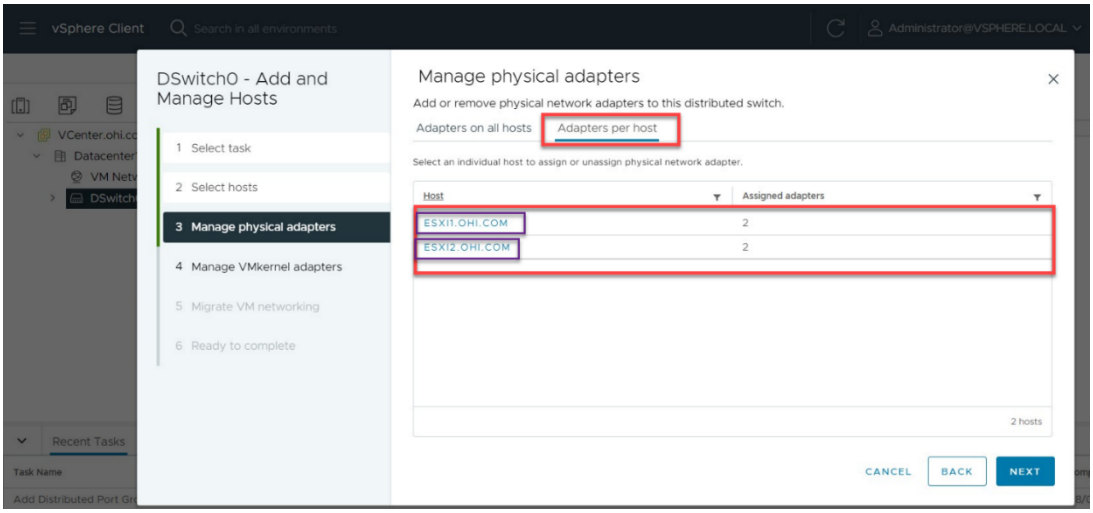

DSwitch - Add and Manage Hosts
Select Network
Filter
Name
Distributed Switch
DProduction
DSwitch
Destination Port Group

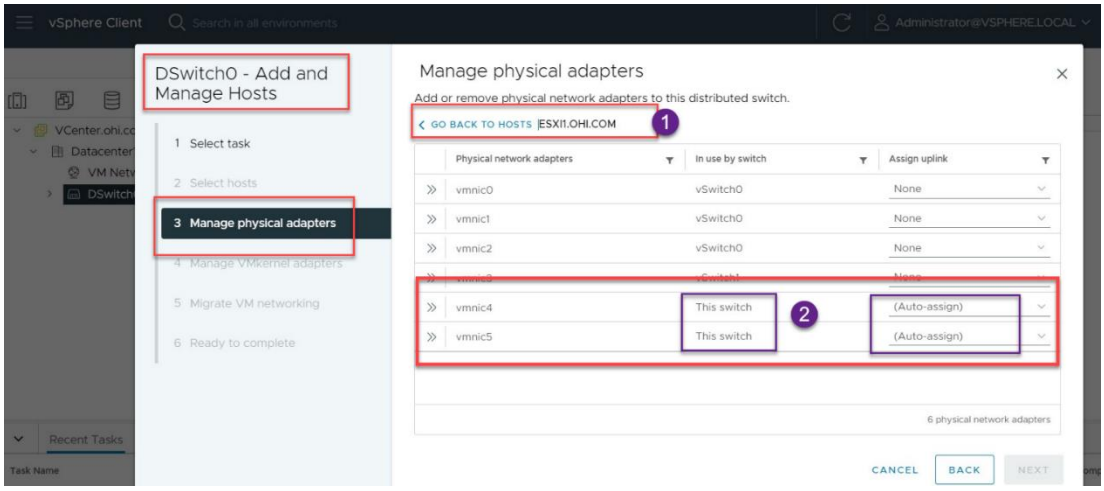

DSwitch - Add and Manage Hosts
1 Select task
2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete
Migrate VM networking
Select virtual machines or network adapters to migrate to the distributed switch.
Assign port group
Reset changes
View settings
Host/Virtual Machine/Network Adapter
NIC Count
Source Port Group
Destination Port Group
esxi01.abdelwahed.me
Web_Server
1
Reassigned
Network adapter 1
VM Network
DProduction


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 2
Virtual machine adapters 1

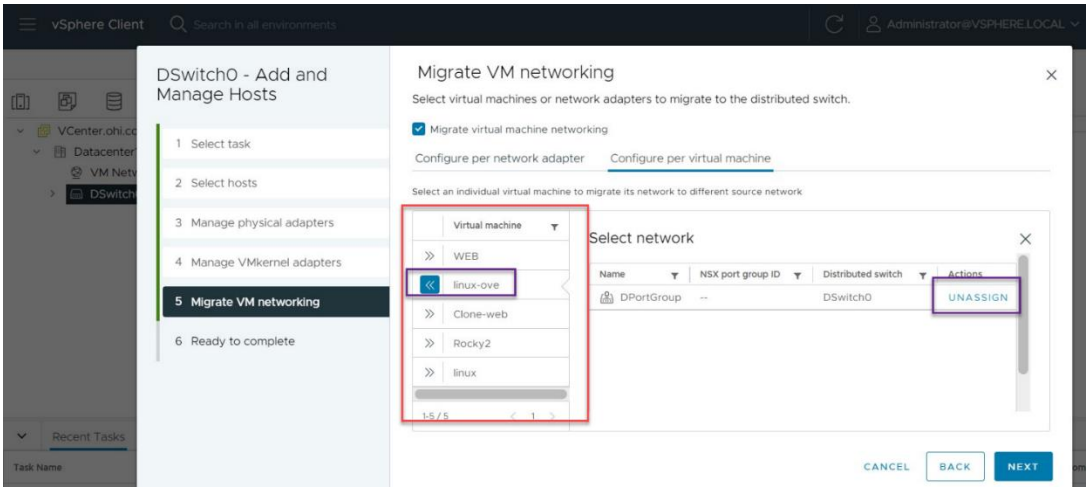

vCenter01.abdelwahed.me
vServer
VM Network
DSwitch
DProduction
DSwitch-DVUplinks...
DSwitch
ACTIONS
Summary
Monitor
Configure
Permissions
Ports
Hosts
VMs
Networks
Filter
Name
State
Status
Cluster
esxi01.abdelwahed.me
Connected
Normal
Cluster01
esxi02.abdelwahed.me
Connected
Normal
Cluster01

Be aware of the changes to NIC assignments in vSphere 8.





Allocate virtual machines to the newly created distributed switch.



VMware Cluster and Distributed Resource Scheduler (DRS)

Adding VMware Cluster

For the following labs, you must add a VMware cluster using vCenter and move the ESXi servers to it.

VMware vSphere Distributed Resource Scheduler (DRS) – Power of Cluster

Overview

VMware DRS (Distributed Resource Scheduler) is a feature available with a vCenter cluster. Once DRS is enabled, it monitors CPU and memory utilization on each ESXi host in the cluster and will automatically migrate included virtual machines to another ESXi host if the utilization of a particular host exceeds a certain threshold.

- **Workload Balancing**: Ensures that each host is used efficiently and that VMs have access to the resources they need.
- **Improves Performance:** Reduces the risk of downtime or other issues.

DRS Automation Levels

1. **Manual**:
    - DRS makes recommendations for VM placement, requiring manual approval for migrations.
2. **Partially Automated:**
    - DRS automatically migrates VMs in response to resource imbalances but prompts for approval if disruptions may occur.
3. **Fully Automated:**
    - DRS automatically migrates VMs without requiring manual approval.

Choosing the Appropriate Automation Level

- **Fully Automated Mode**: Effective at balancing workloads but may cause frequent migrations that could impact performance.
- **Manual Mode:** Provides more control but requires more intervention.

DRS Rules

Even if DRS is set to fully automated mode, you can still add DRS rules to guide its behavior:

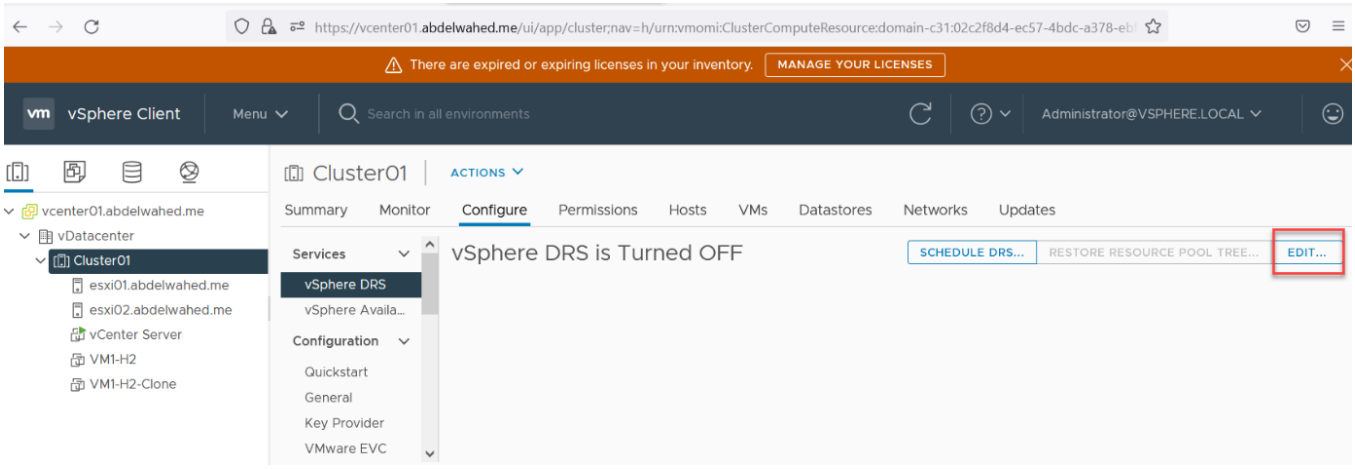
1. **Separating Critical VMs**:
    - Ensure that critical VMs, such as domain controllers and Active Directory servers, are always separated across different ESXi hosts in case of hardware failure.

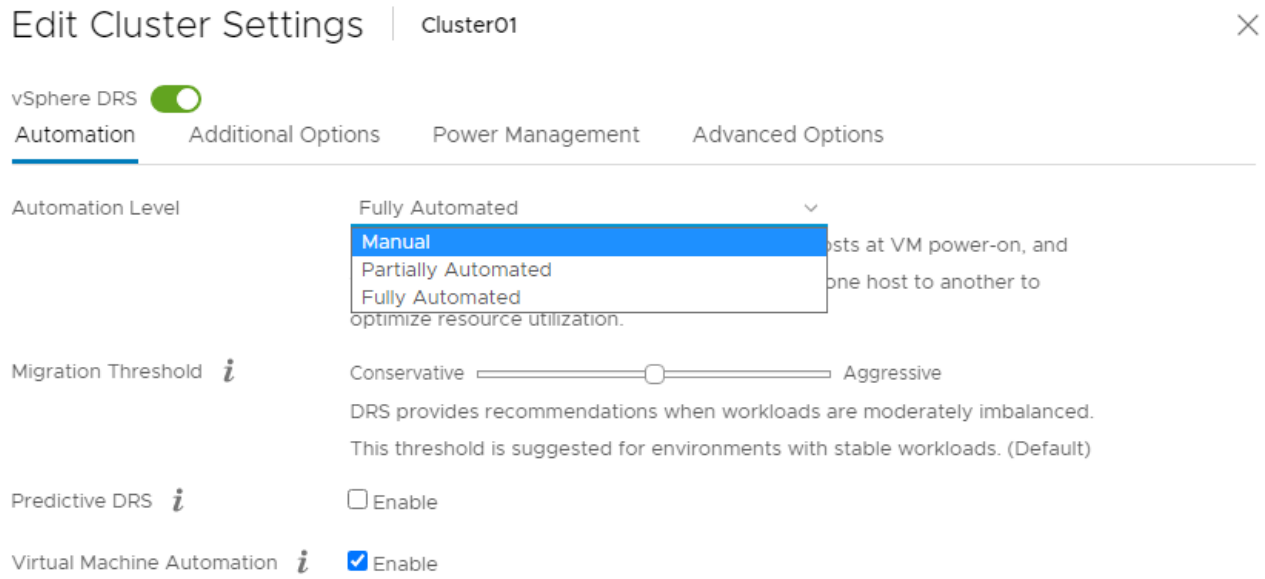
2. **Keeping Application Servers Together:**
    - Ensure that application servers and database servers are always kept together on the same ESXi host to reduce latency and improve performance.
3. **Preventing Power Disconnects:**
    - Prevent VMs from being migrated to ESXi hosts in different compute racks in case of power disconnects to ensure high availability.
4. **Predictive DRS:**
    - Use historical performance data to predict and initiate VM migrations before resource utilization reaches critical levels.

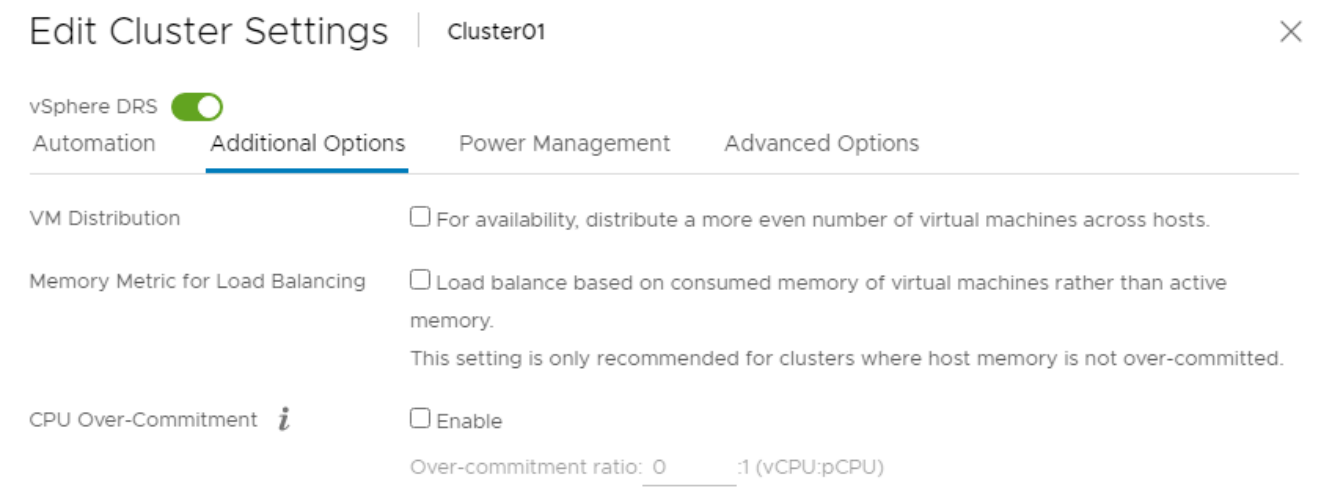
Additional Options in DRS

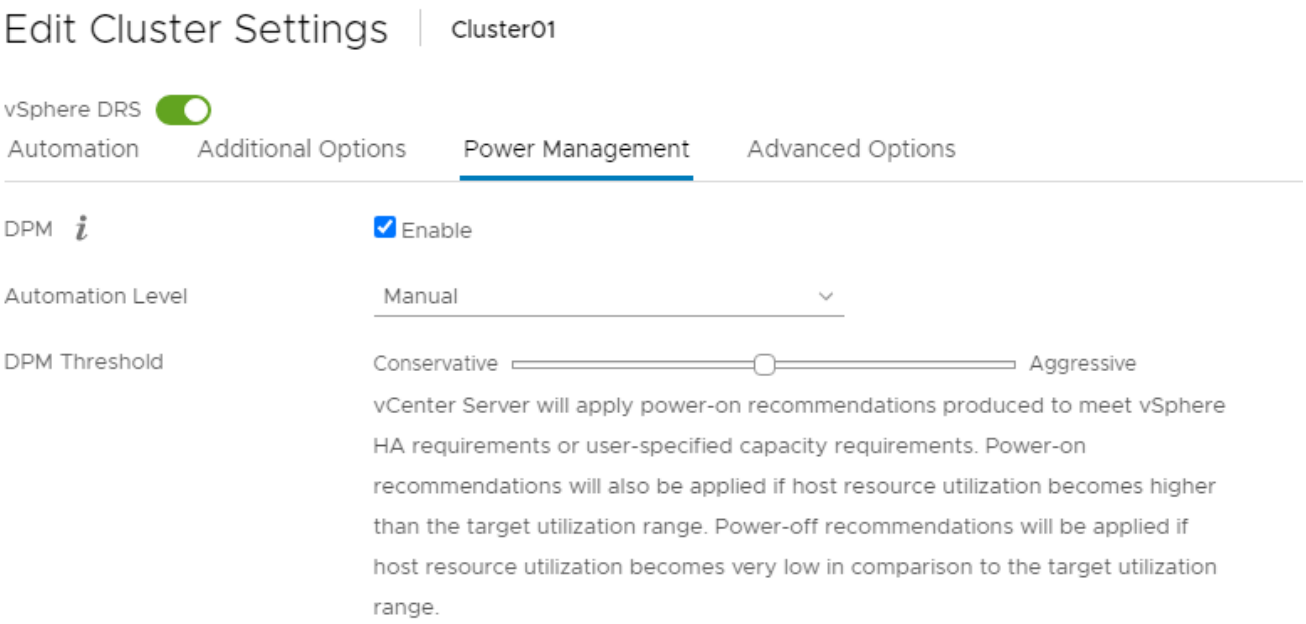
1. **Automation Level**:
    - Determines how much automation DRS uses to manage resource allocation and workload placement (Manual, Partially Automated, Fully Automated).
2. **Migration Threshold:**
    - Determines the threshold at which DRS will initiate a migration of VMs to balance resource utilization (Conservative, Moderate, Aggressive).
3. **Power Management:**
    - Allows you to enable or disable vSphere Distributed Power Management (DPM) to dynamically power on and power off hosts to balance resource utilization and save energy.
4. **CPU Overcommitment:**
    - Allows you to enable or disable CPU overcommitment, allowing multiple VMs to share a physical CPU core.
5. **Memory Overcommitment:**
    - Allows you to enable or disable memory overcommitment, allowing VMs to share memory resources.
6. **CPU Affinity Rules:**
    - Allows you to configure CPU affinity rules to control the placement of VMs on physical hosts.
7. **VM Distribution:**
    - Allows you to configure how DRS distributes VMs across physical hosts (Spread, Pack, Evenly Balanced).

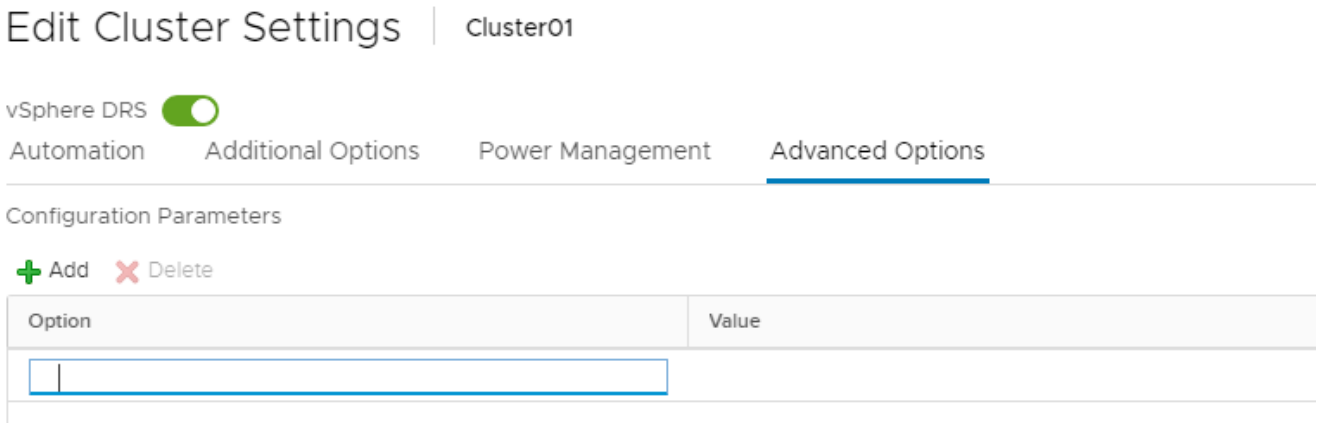
Steps to create DRS

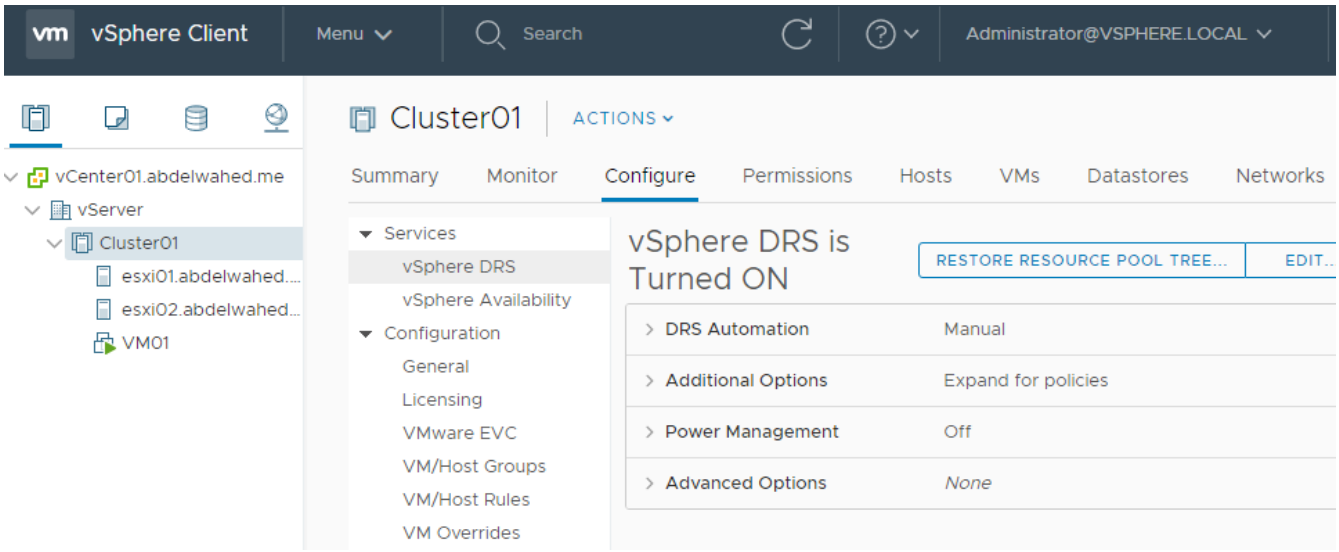




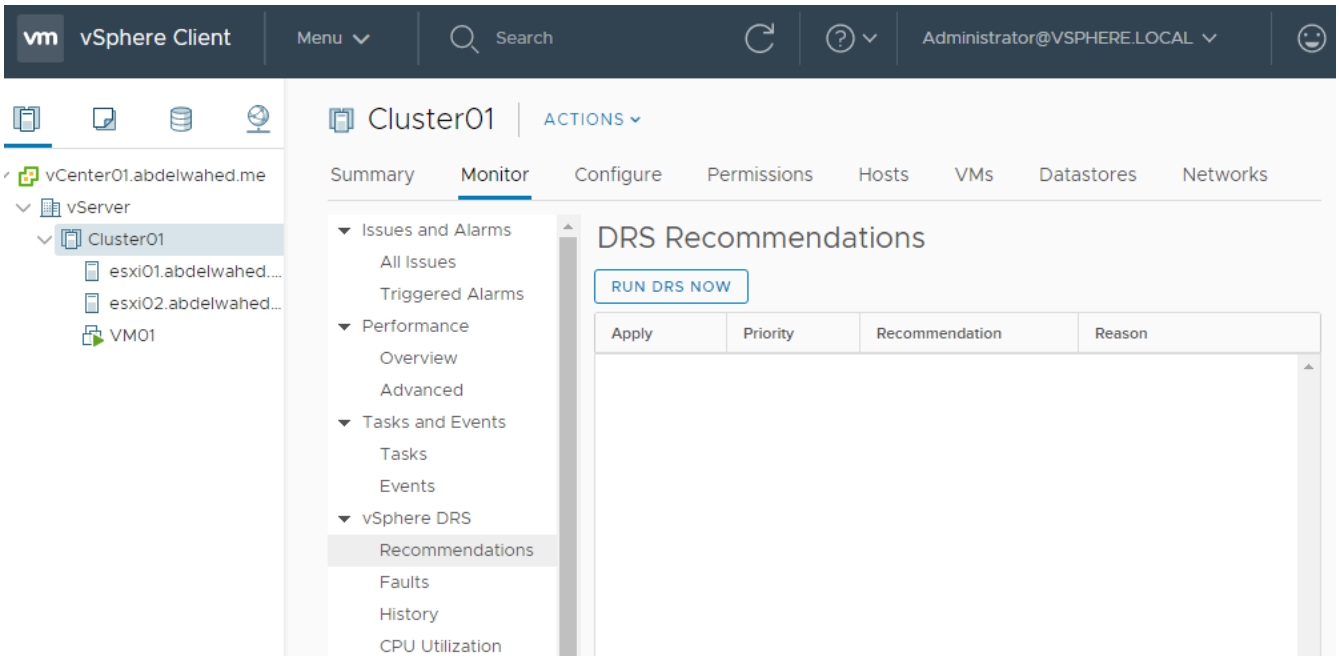

Edit Cluster Settings
Cluster01
vSphere DRS
Automation
Additional Options
Power Management
Advanced Options
VM Distribution
For availability, distribute a more even number of virtual machines across hosts.
Memory Metric for Load Balancing
Load balance based on consumed memory of virtual machines rather than active memory.
This setting is only recommended for clusters where host memory is not over-committed.
CPU Over-Commitment
Enable
Over-commitment ratio: 0
:1 (vCPU:pCPU)


Edit Cluster Settings
Cluster01
vSphere DRS
Automation
Additional Options
Power Management
Advanced Options
DPM
Enable
Automation Level
Manual
DPM Threshold
Conservative
Aggressive
vCenter Server will apply power-on recommendations produced to meet vSphere HA requirements or user-specified capacity requirements. Power-on recommendations will also be applied if host resource utilization becomes higher than the target utilization range. Power-off recommendations will be applied if host resource utilization becomes very low in comparison to the target utilization range.


Edit Cluster Settings
Cluster01
vSphere DRS
Automation
Additional Options
Power Management
Advanced Options
Configuration Parameters
Add
Delete
Option
Value



Any suggestions provided here can be considered and implemented as needed.



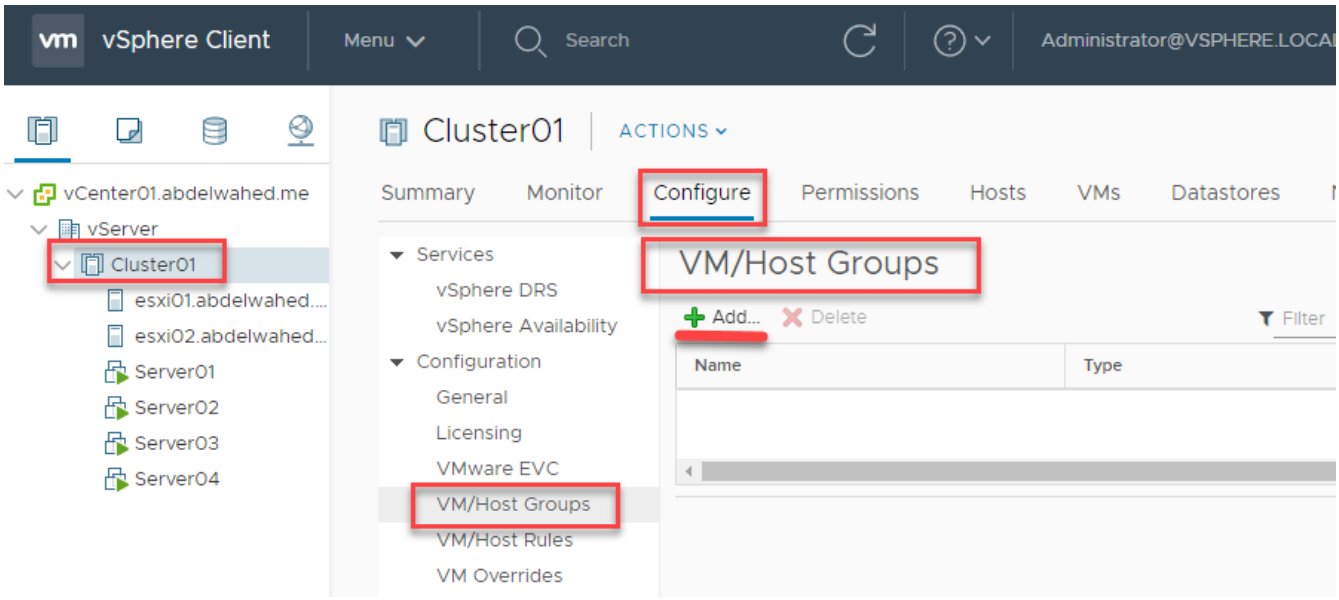
Creating VM and Host Groups in VMware vSphere

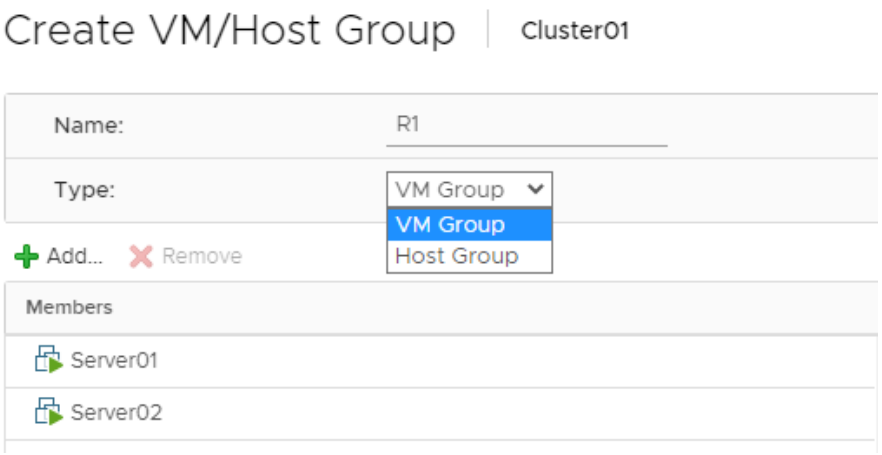
In a VMware vSphere environment, creating VM and host groups helps organize and manage virtual machines and ESXi hosts based on specific criteria. These groups can simplify management tasks, improve performance and availability, and ensure optimal resource utilization.

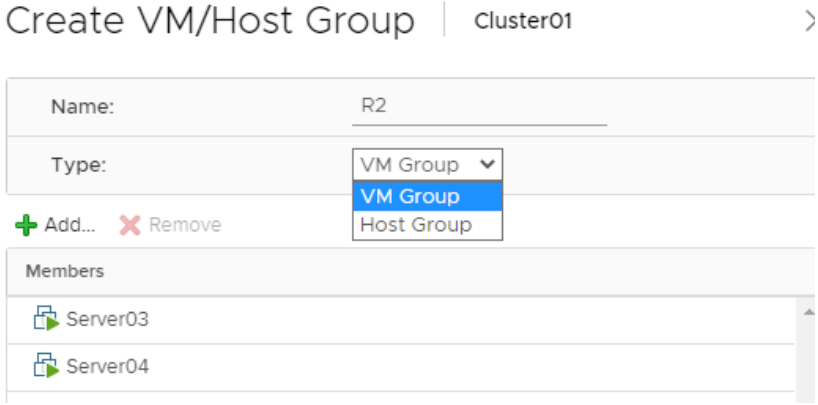
Uses of VM and Host Groups

1. **Resource Allocation**:
    - **Purpose**: Ensure that VMs are distributed across ESXi hosts to maximize resource utilization.
    - **Example**: Group VMs based on CPU or memory requirements and distribute them across capable ESXi hosts.
2. **High Availability:**
    - **Purpose**: Ensure that VMs are distributed to maximize high availability.
    - **Example**: Group critical VMs and ensure they are distributed across ESXi hosts in different compute racks or datacenters to ensure high availability in case of hardware failure.
3. **Simplified Management:**
    - **Purpose**: Simplify management tasks such as patching, updates, or migration.
    - **Example**: Group VMs based on their application and ensure they are patched and updated together to minimize disruptions.

Steps to Create VM and Host Groups

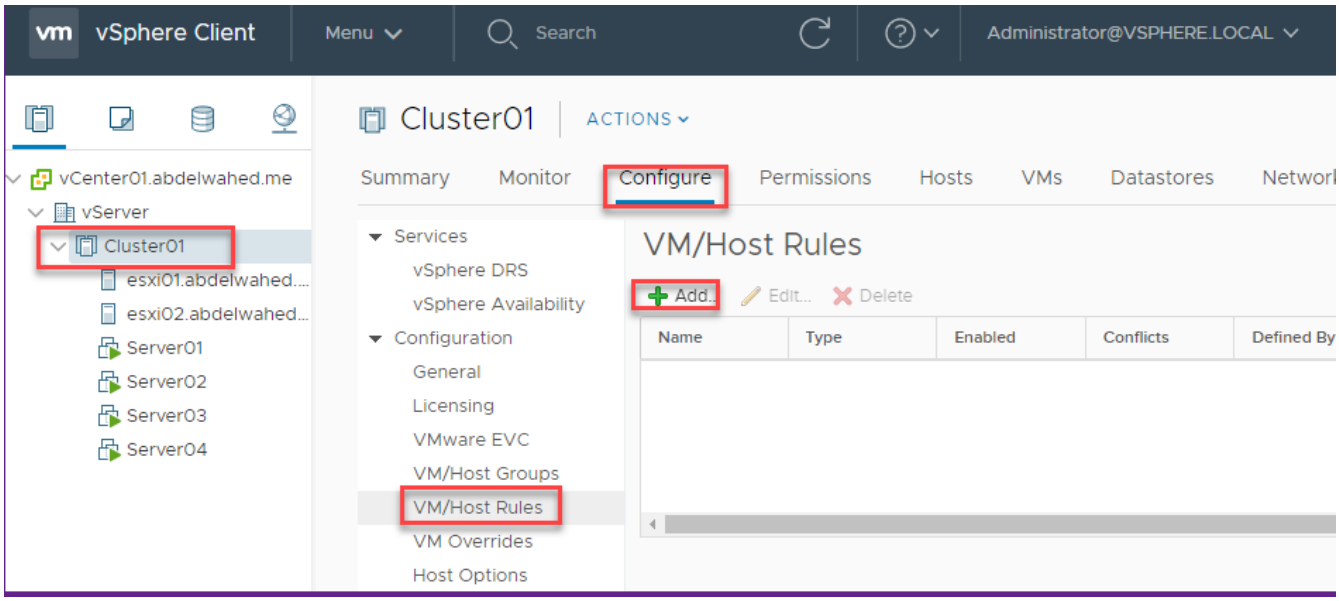


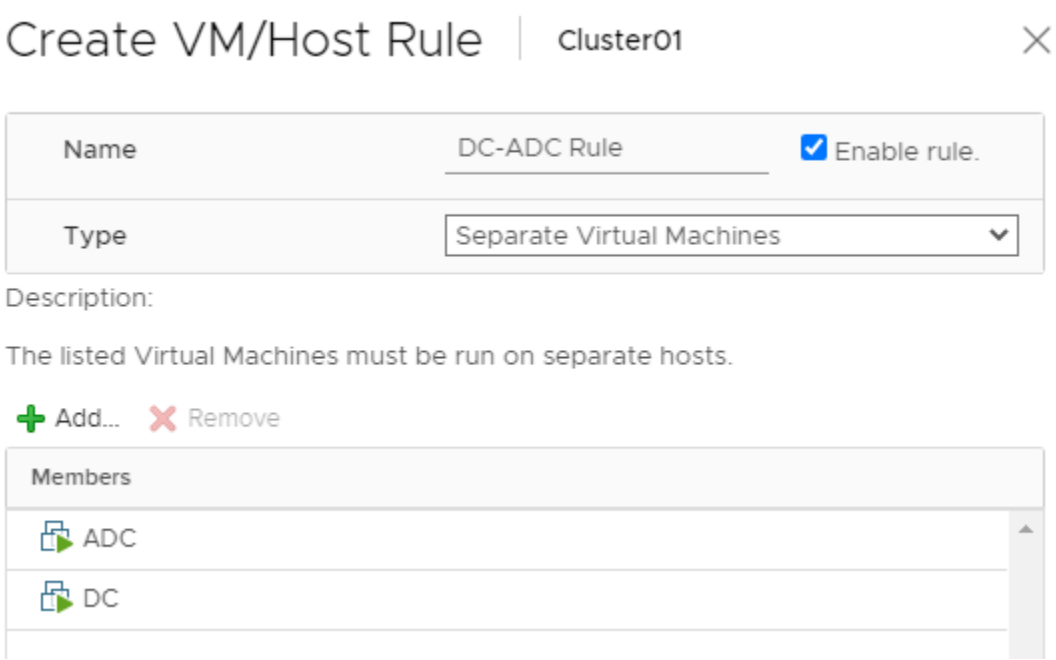


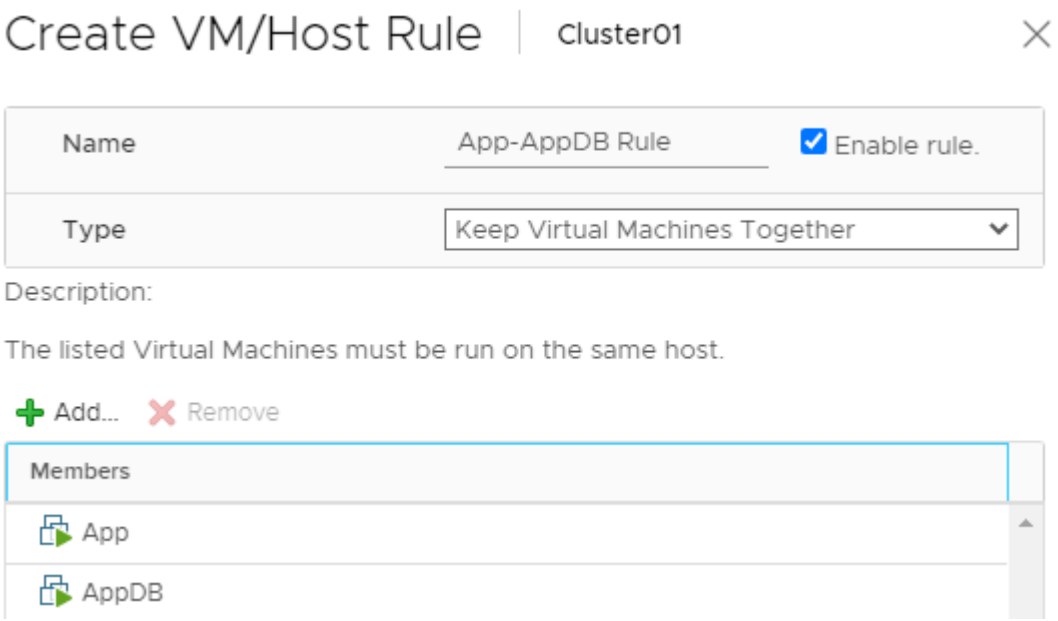


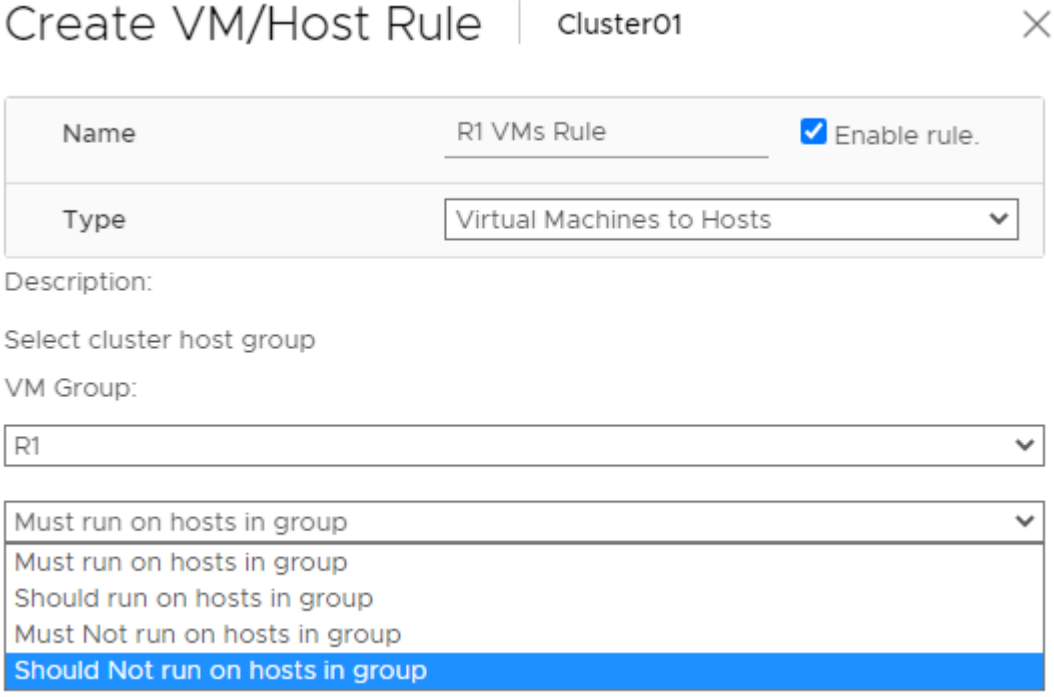
Set Up VM/Host Rules

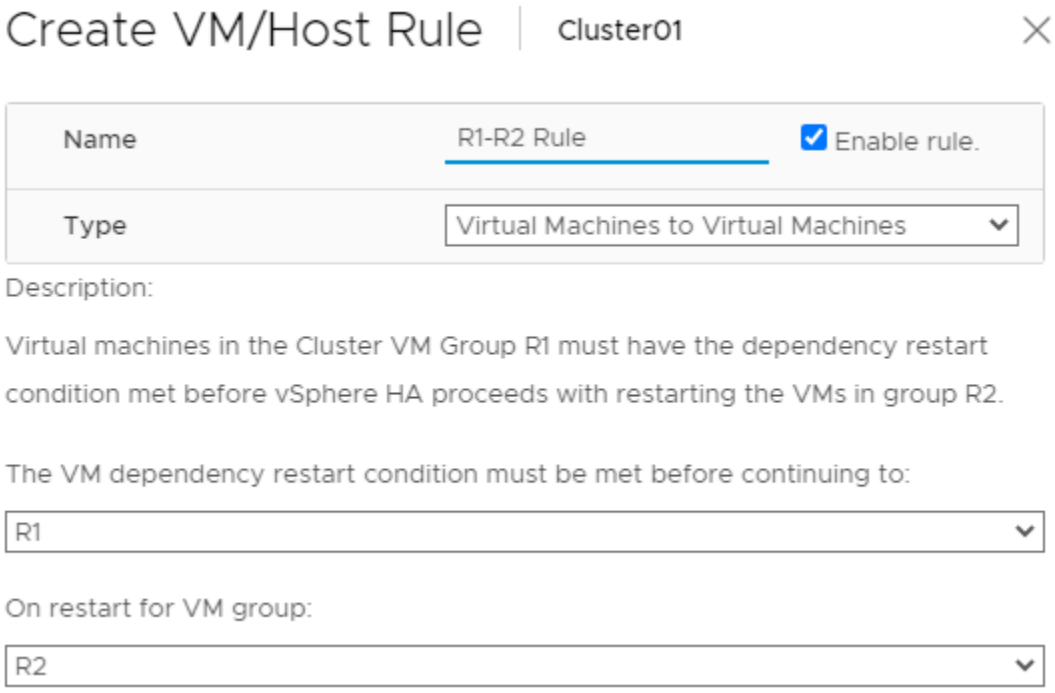
To manage DRS actions.





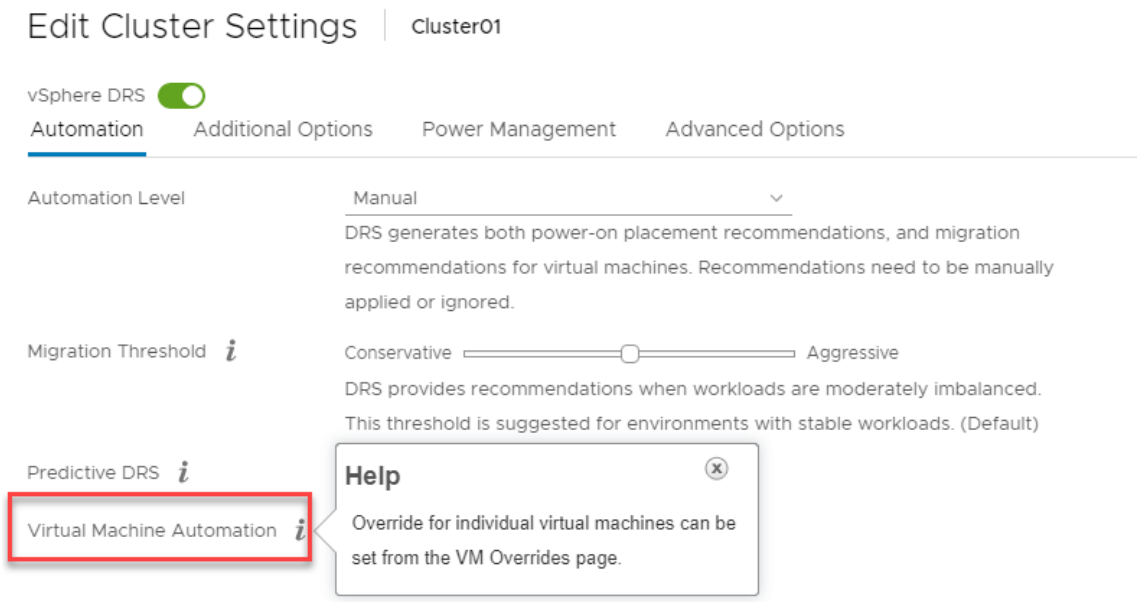

Create VM/Host Rule
Cluster01
Name
App-AppDB Rule
Enable rule.
Type
Keep Virtual Machines Together
Description:
The listed Virtual Machines must be run on the same host.
Add...
Remove
Members
App
AppDB


Create VM/Host Rule
Cluster01
Name
R1 VMs Rule
Enable rule.
Type
Virtual Machines to Hosts
Description:
Select cluster host group
VM Group:
R1
Must run on hosts in group
Must run on hosts in group
Should run on hosts in group
Must Not run on hosts in group
Should Not run on hosts in group

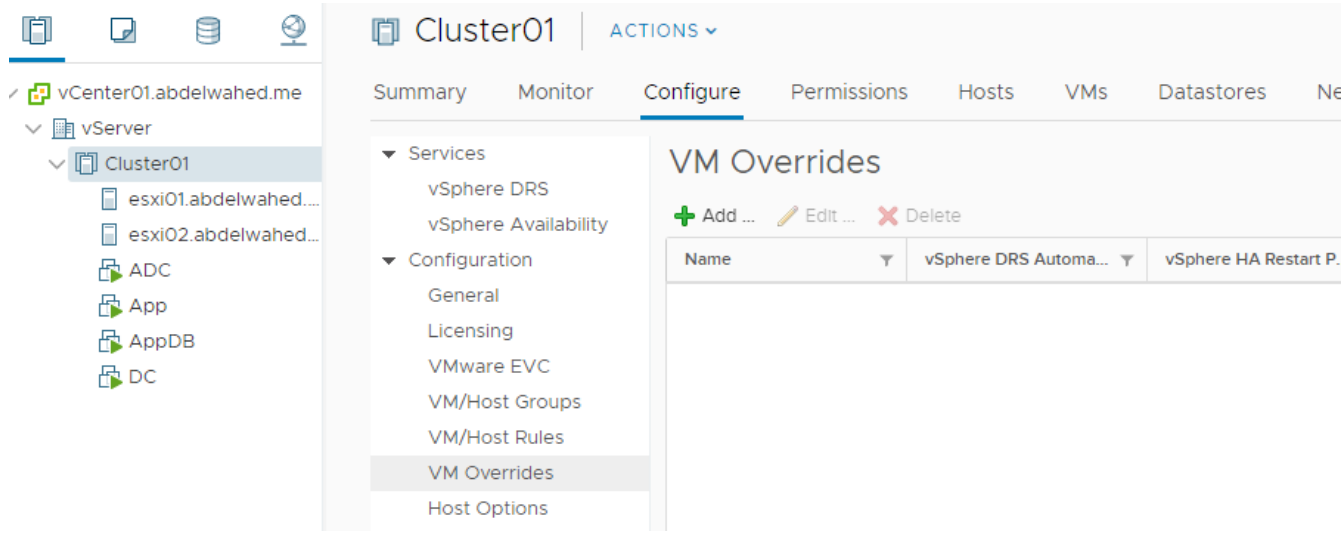


Virtual Machine Overrides

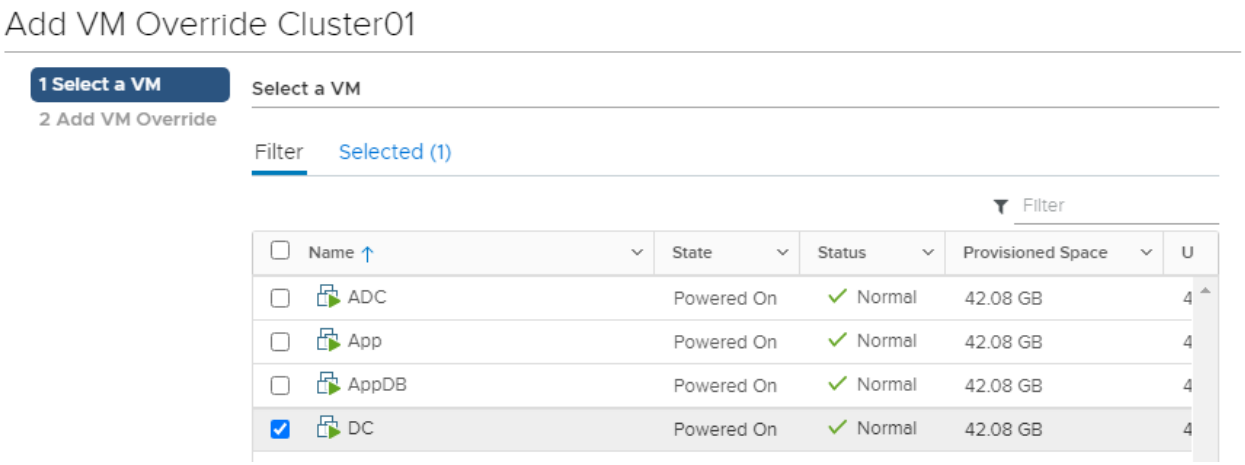
Enable this option during DRS setup to customize settings and other details for a particular VM.

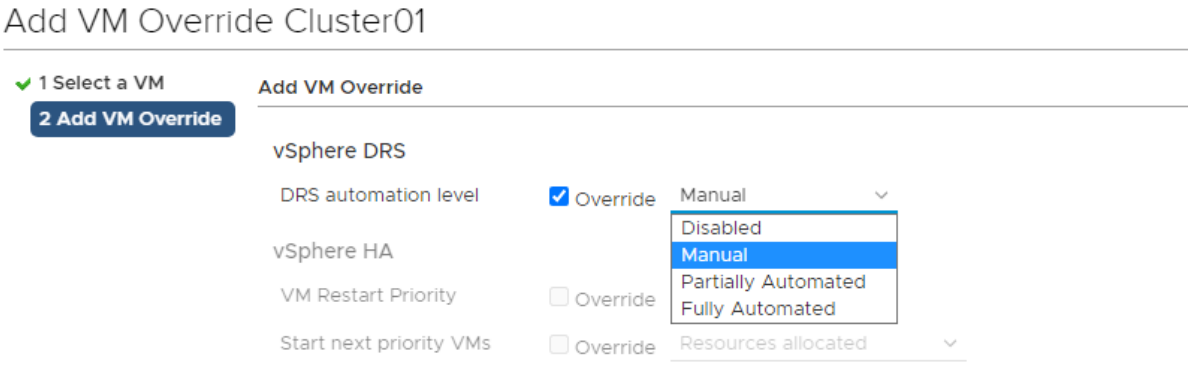


After activating, you can set up configurations from



Begin by choosing the virtual machine (VM) on which to apply various DRS settings.





VMware High Availability (HA)

VMware HA (High Availability) is designed to reduce downtime by automatically restarting virtual machines on another ESXi host in the event of a host failure. Here are the key points and features of VMware HA:

Key Points of VMware HA

1. **Network Storage Requirement**:
   - VMware HA requires network storage (such as iSCSI or NFS) to store the virtual machine data, allowing multiple ESXi hosts to access it.
2. **Downtime and Fault Tolerance:**
   - While HA reduces downtime by restarting VMs on another host, there may still be some downtime during the reboot process.
   - For true zero-downtime operation, use VMware Fault Tolerance (FT), which creates a real-time duplicate of a VM on a secondary host.
3. **Heartbeat Monitoring:**
   - VMware HA uses heartbeat monitoring to detect host failures. Heartbeat traffic is sent over multiple channels (network, storage, and management interfaces) to ensure robustness.
4. **vCenter Server Independence:**
   - If the vCenter Server goes down, VMware HA will continue to operate because the master host in the cluster manages the HA configuration. If the master host fails, another host is elected to take its place.
5. **Admission Control:**
   - Ensures sufficient resources are available in the cluster to accommodate VM failover. This can involve reserving a percentage of resources on each host or an entire host as a standby.
   - Admission control can also trigger VM resource reduction to ensure a VM can be restarted on a different host even with limited resources.
6. **Shared Datastores and Network Settings:**
   - VMware HA requires at least two shared datastores and properly configured network settings (including a default gateway) to ensure proper operation and fault detection.

vSphere Cluster Services (vCLS)

vCLS ensures essential vSphere cluster services (like DRS) operate even if vCenter Server is unavailable.

Key Points of vCLS

1. **vCLS VMs**:
   - Lightweight VMs, typically three per cluster, identifiable with the "vCLS" prefix.
2. **Functionality:**
   - Allows DRS to function without vCenter.
   - Monitors ESXi host health.
3. **Operational Notes:**
   - Do not manually power off or delete vCLS VMs. If deleted, they are automatically recreated.
   - vCLS VMs dynamically adjust resources as per cluster needs.

Best Practices for vCLS

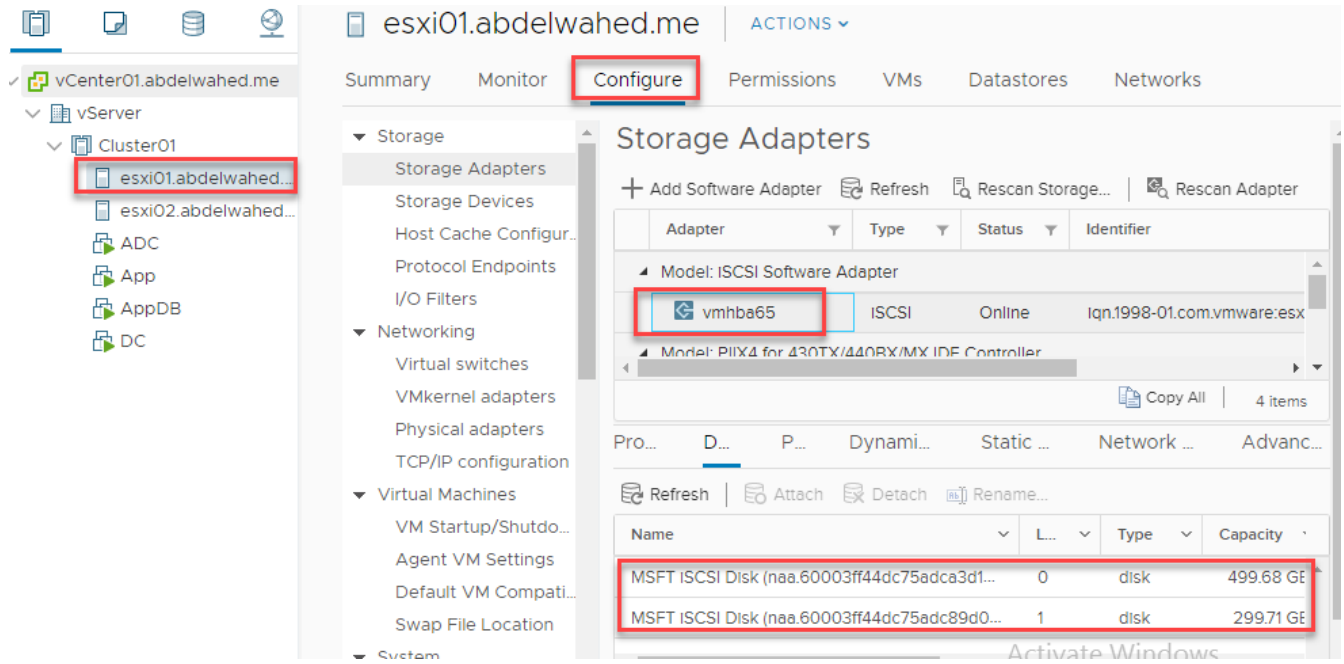
- **Monitor Rather Than Modify**: It's optimal to monitor vCLS VMs rather than modify them manually.
- **Understanding vCLS Role**: Understanding their role can lead to better cluster management decisions. For instance, if vCLS VMs are deleted, vCenter will redeploy them to ensure uninterrupted DRS functionality.

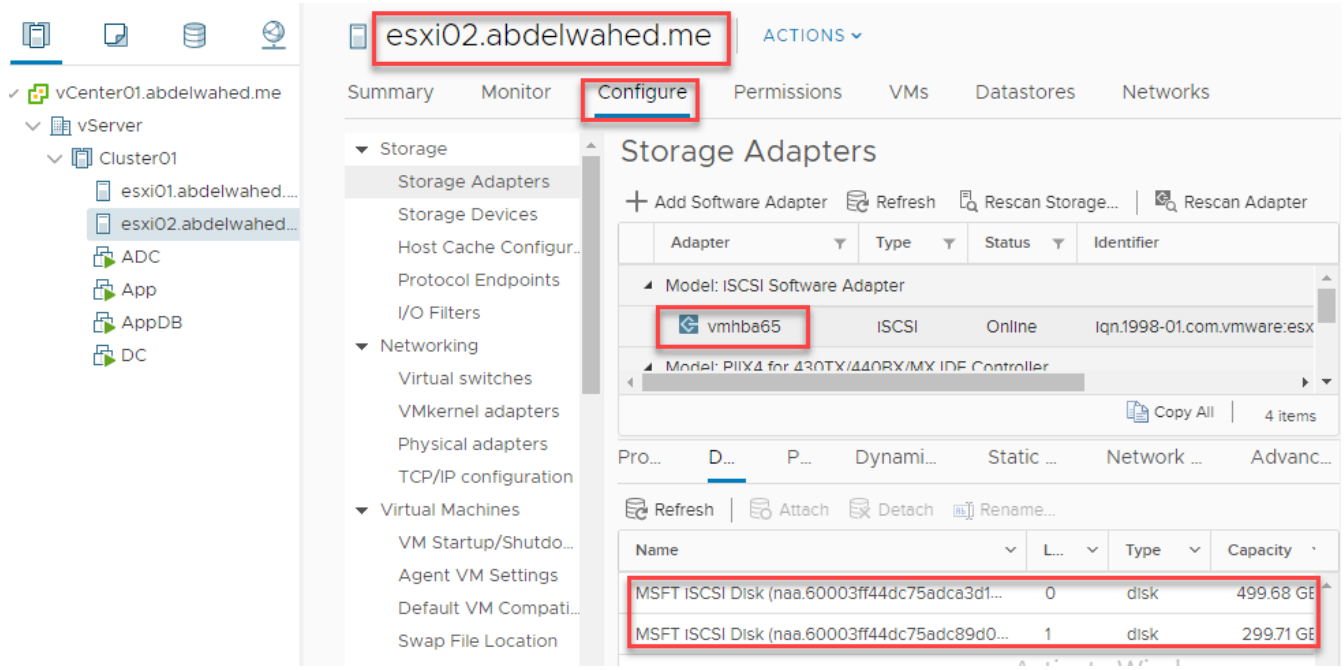
Example

- **DRS Functionality Without vCenter**:
   - DRS can rebalance VM workloads across hosts in a cluster even if vCenter Server is down, ensuring continuous operation and resource optimization.

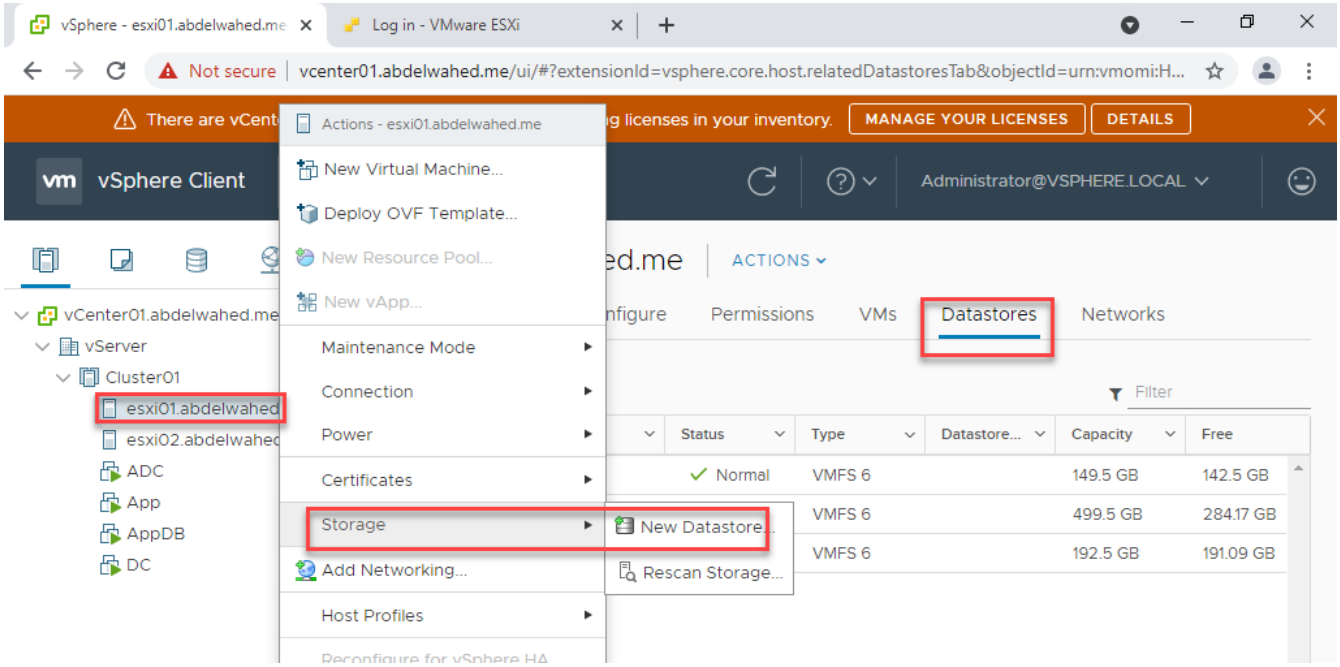
Set up High Availability

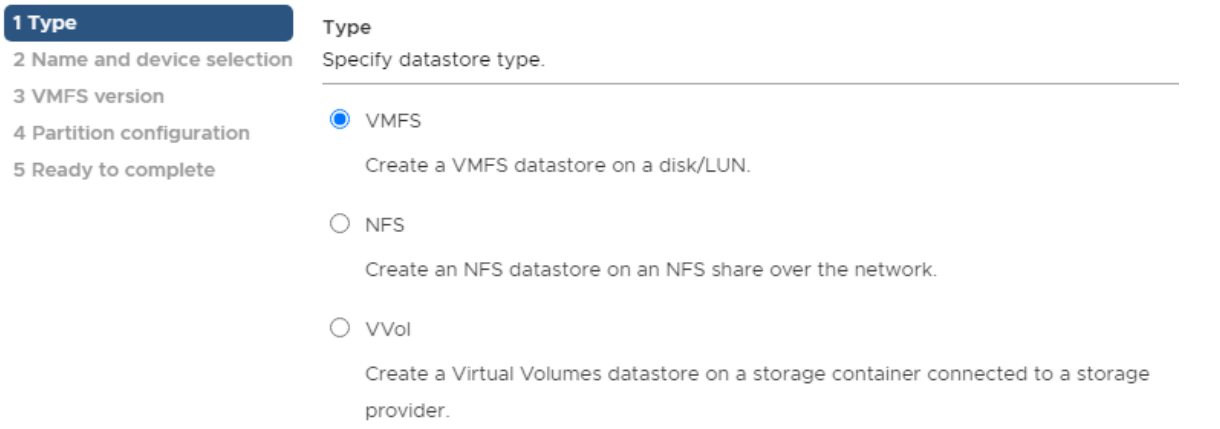
Attach two ISCSI disks to each server and then create a new datastore.

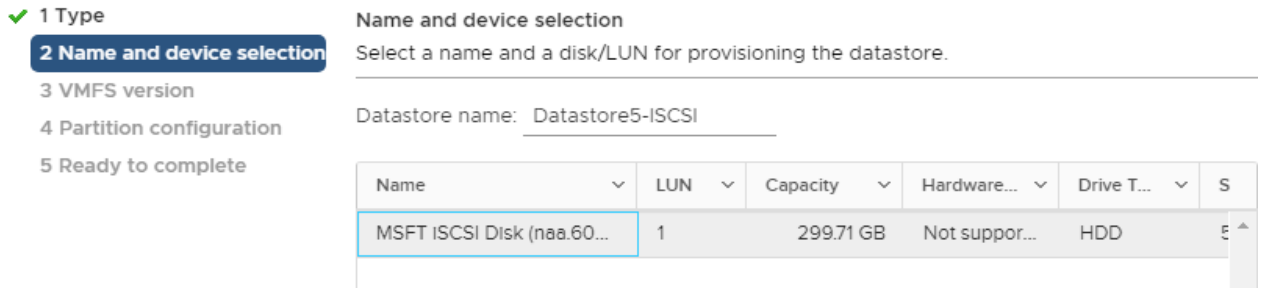


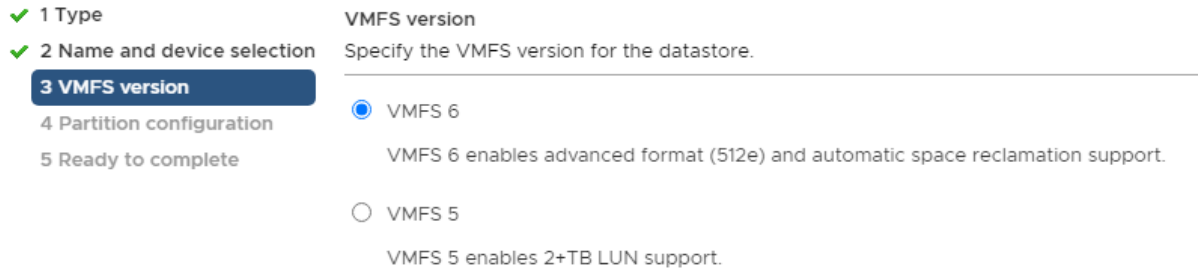


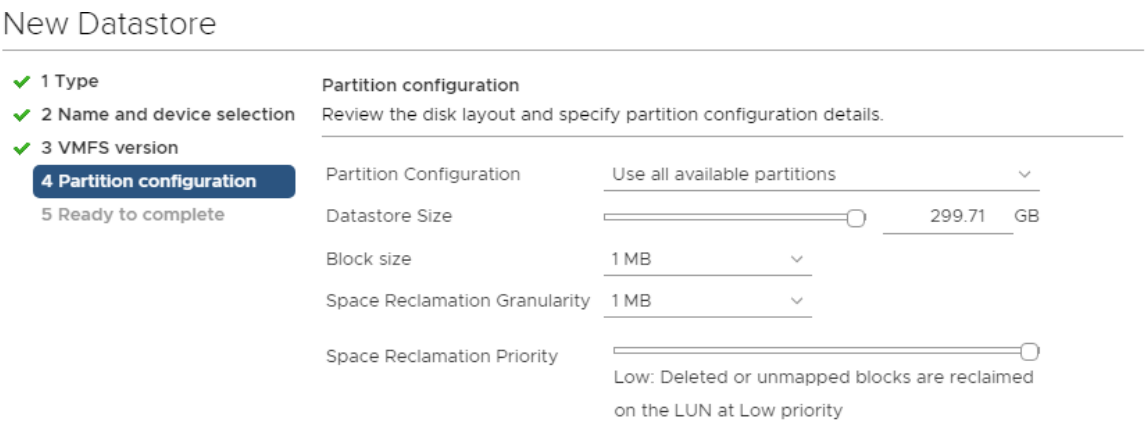
We have previously configured an ISCSI datastore of 500GB size; now we are proceeding to add an additional ISCSI datastore with a capacity of 300GB.

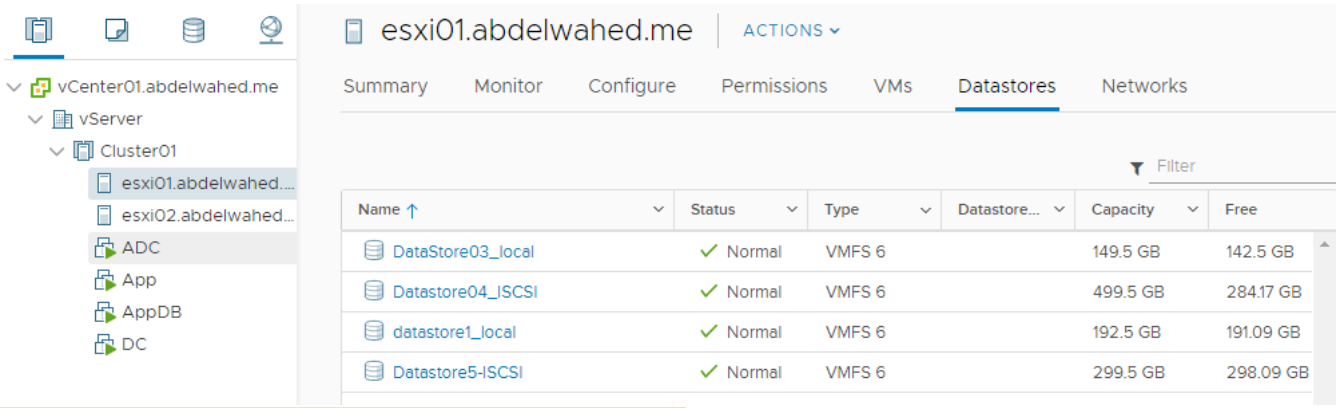




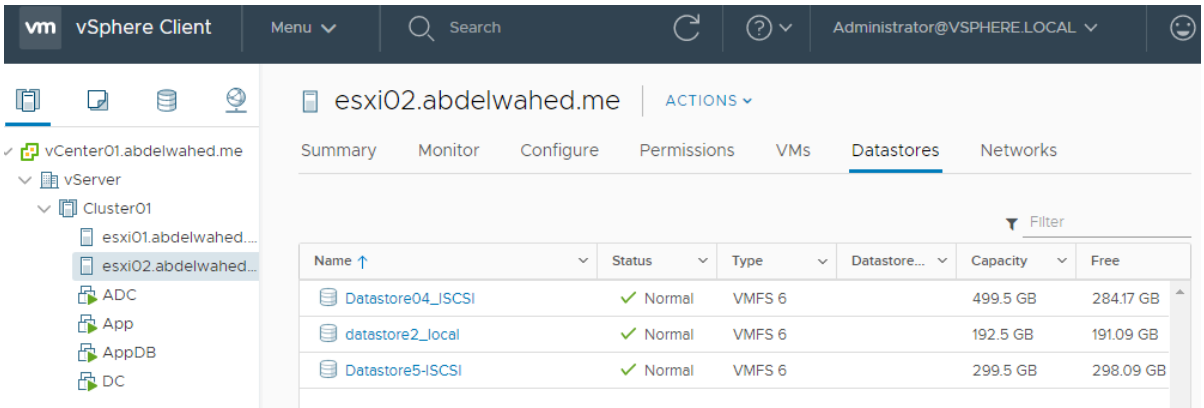




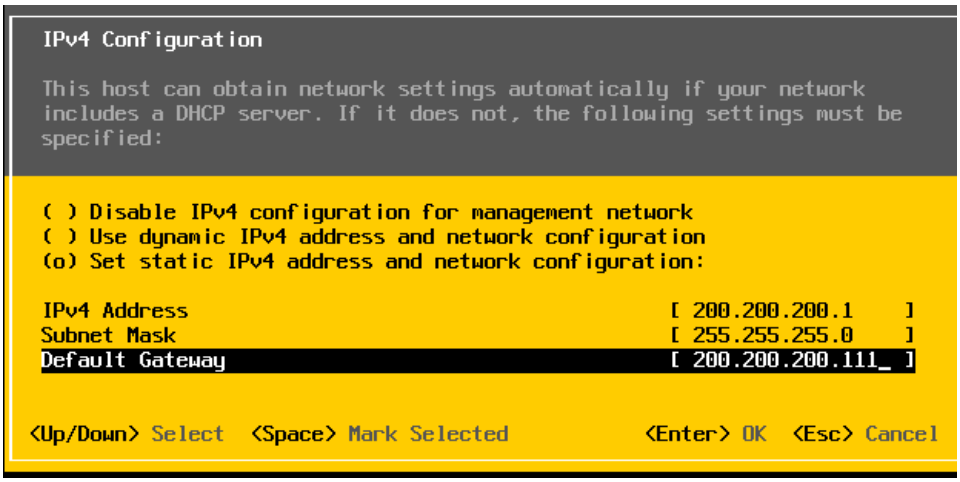




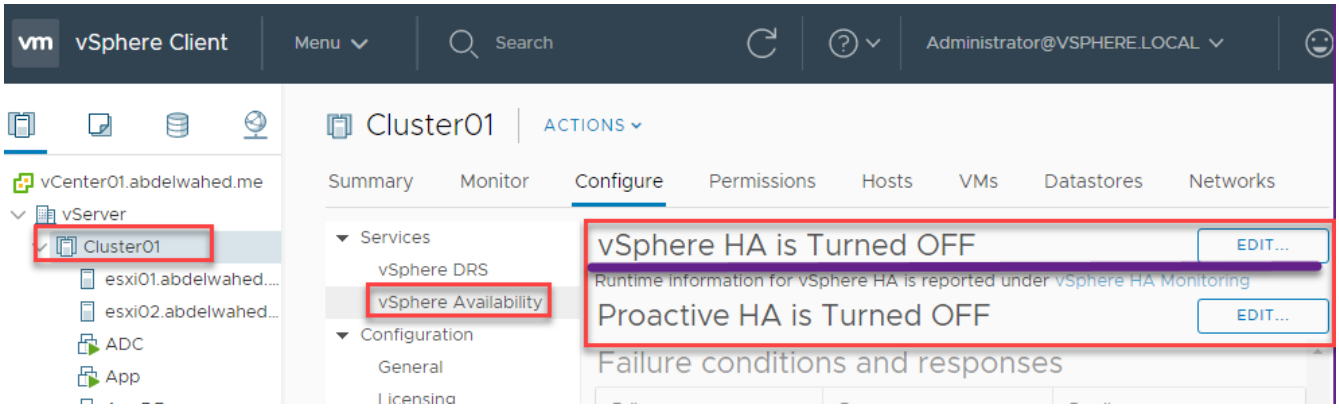
Currently, both hosts are connected to two iSCSI datastores.

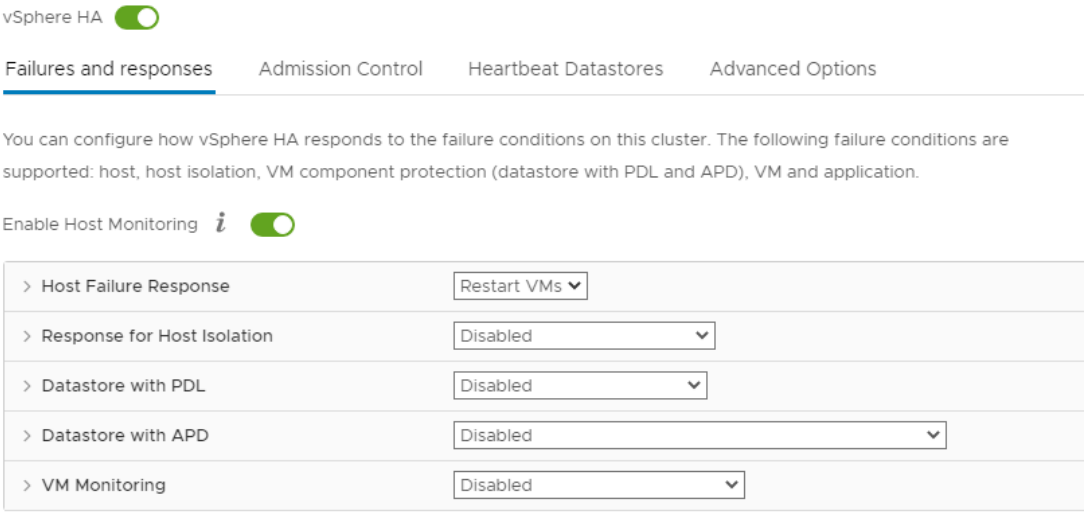


Set a pingable default gateway for both hosts (using the vCenter IP as an example).



Now you can enable HA





Summary of HA Response Options in VMware vSphere

Response for Host Isolation

- **Disabled**: No action taken when a host is isolated.
- **Power off and restart VMs:** VMs on the isolated host are powered off and restarted on another host.
- **Shut down and restart VMs:** VMs on the isolated host are gracefully shut down and then restarted on another host.

Datastore with PDL (Permanent Device Loss) Failure Response

- **Disabled:** No action taken on the affected VMs.
- **Issue events:** No action taken on the affected VMs, but events are generated.
- **Power off and restart VMs:** All affected VMs are terminated, and vSphere HA attempts to restart them on hosts with datastore connectivity.

Datastore with APD (All Paths Down) Failure Response

- **Disabled:** No action taken on the affected VMs.
- **Issue events:** No action taken on the affected VMs, but events are generated.
- **Power off and restart VMs - Conservative restart policy:** A VM is powered off if HA determines it can be restarted on a different host.
- **Power off and restart VMs - Aggressive restart policy:** A VM is powered off if HA determines it can be restarted on a different host or if it cannot detect resources on other hosts due to network partition.


Response for Host Isolation
Disabled
Disabled
Power off and restart VMs
Shut down and restart VMs
Datastore with PDL
Datastore with APD
Disabled
Datastore with PDL
Datastore with PDL Failure Response
Allows you to configure the cluster to respond to PDL Datastore failures.
Disabled
No action will be taken to the affected VMs.
Issue events
No action will be taken to the affected VMs; events will be generated.
Power off and restart VMs
All affected VMs will be terminated and vSphere HA will attempt to restart the VMs on hosts that still have connectivity to the datastore.
All Paths Down (APD) Failure Response
Allows you to configure the cluster to respond to APD Datastore failures
Disabled
No action will be taken on the affected VMs.
Issue events
No action will be taken on the affected VMs. Events will be generated.
Power off and restart VMs - Conservative restart policy
A VM will be powered off, if HA determines the VM can be restarted on a different host.
Power off and restart VMs - Aggressive restart policy
A VM will be powered off, If HA determines the VM can be restarted on a different host, or if HA cannot detect the resources on other hosts because of network connectivity loss (network partition).
VM Monitoring
Enable heartbeat monitoring
VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.
Disabled
VM Monitoring Only
Turns on VMware tools heartbeats. When heartbeats are not received within a set time, the VM is reset.
VM and Application Monitoring
Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

Summary of VMware HA Settings

Host Failure Response

- **Disabled**: Host Monitoring is turned off. vCenter will not respond to host failures.
- **Restart VMs:** When a host failure is detected, VMs are restarted in the order determined by their restart priority.

Default VM Restart Priority

- Options to set the default restart priority for VMs (e.g., Medium).

VM Dependency Restart Condition

- **Resources Allocated:** vSphere HA proceeds with the next VM restart priority after the condition is met.
- **Additional Delay:** Specify a delay before restarting VMs.
- **VM Dependency Restart Condition Timeout:** Set a timeout period for VM dependency restart conditions (e.g., 600 seconds).

Datastore Usage for Heartbeat

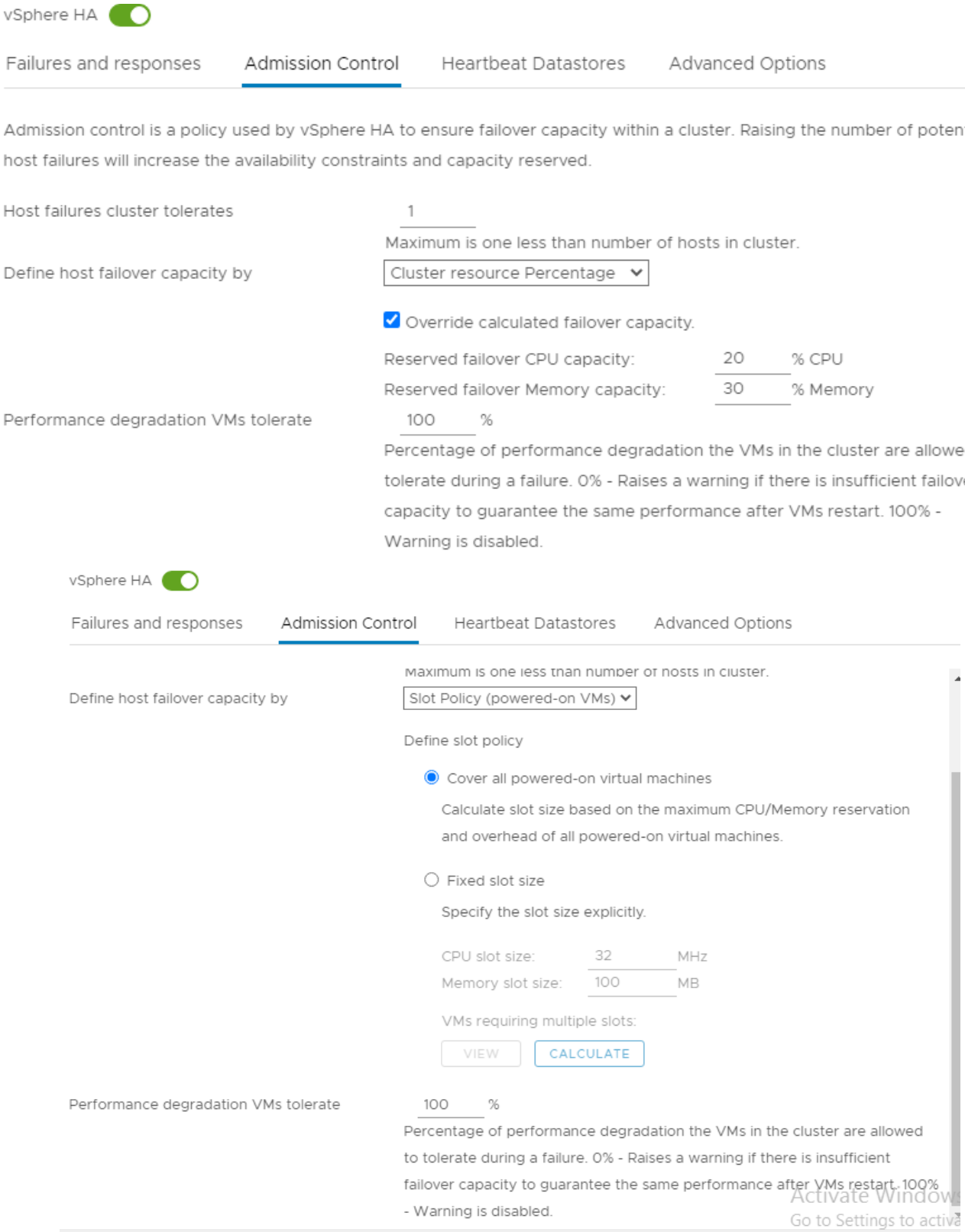
- **Use Datastores Only from the Specified List:** Restrict to specified datastores.
- **Use Datastores from the Specified List and Complement Automatically if Needed:** Allows automatic selection of additional datastores if necessary.

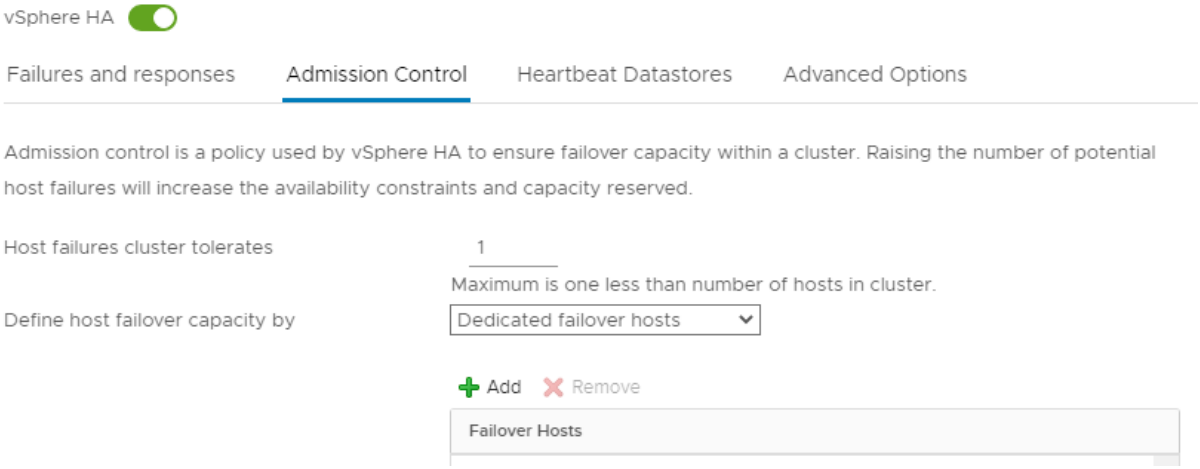
Available Heartbeat Datastores

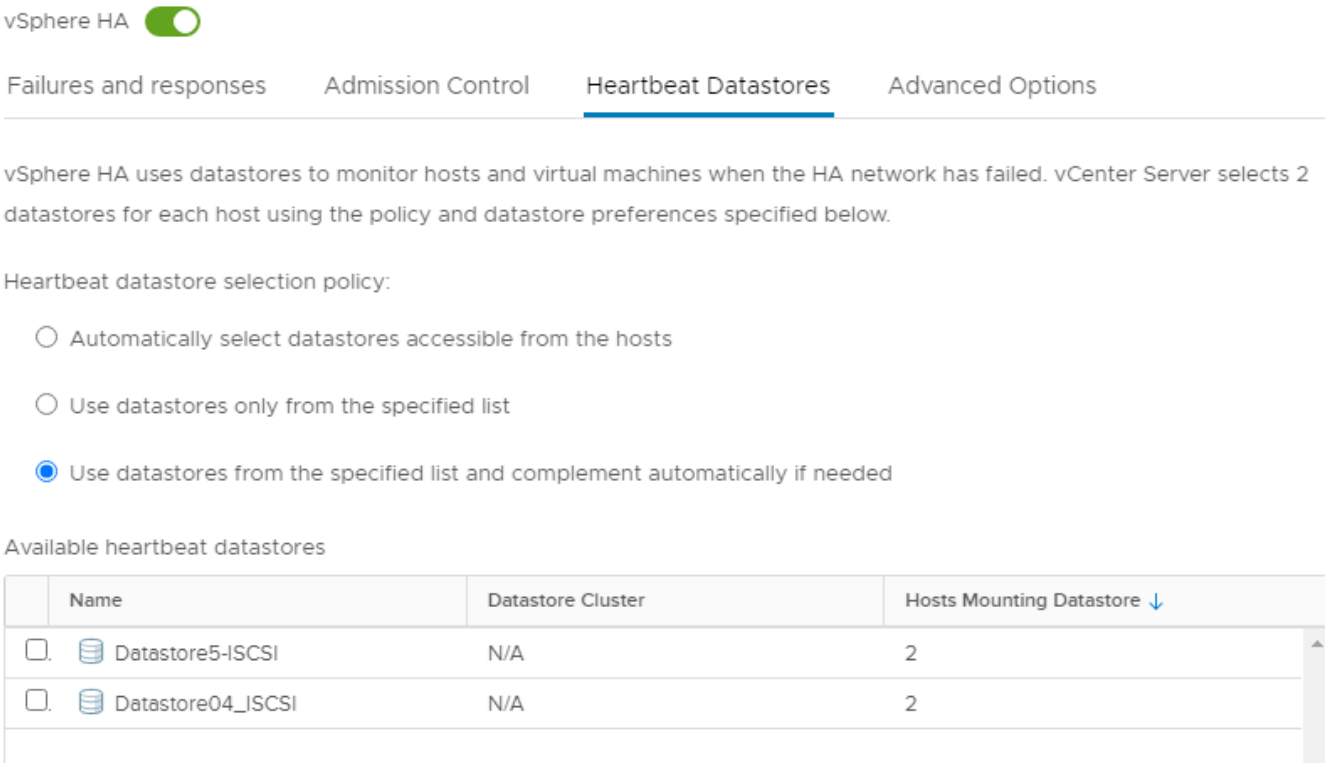
- List of datastores selected for heartbeat:
    - **Datastore5-ISCSI**
    - **Datastore04-ISCSI**
    - Hosts mounting each datastore (e.g., 2 hosts).

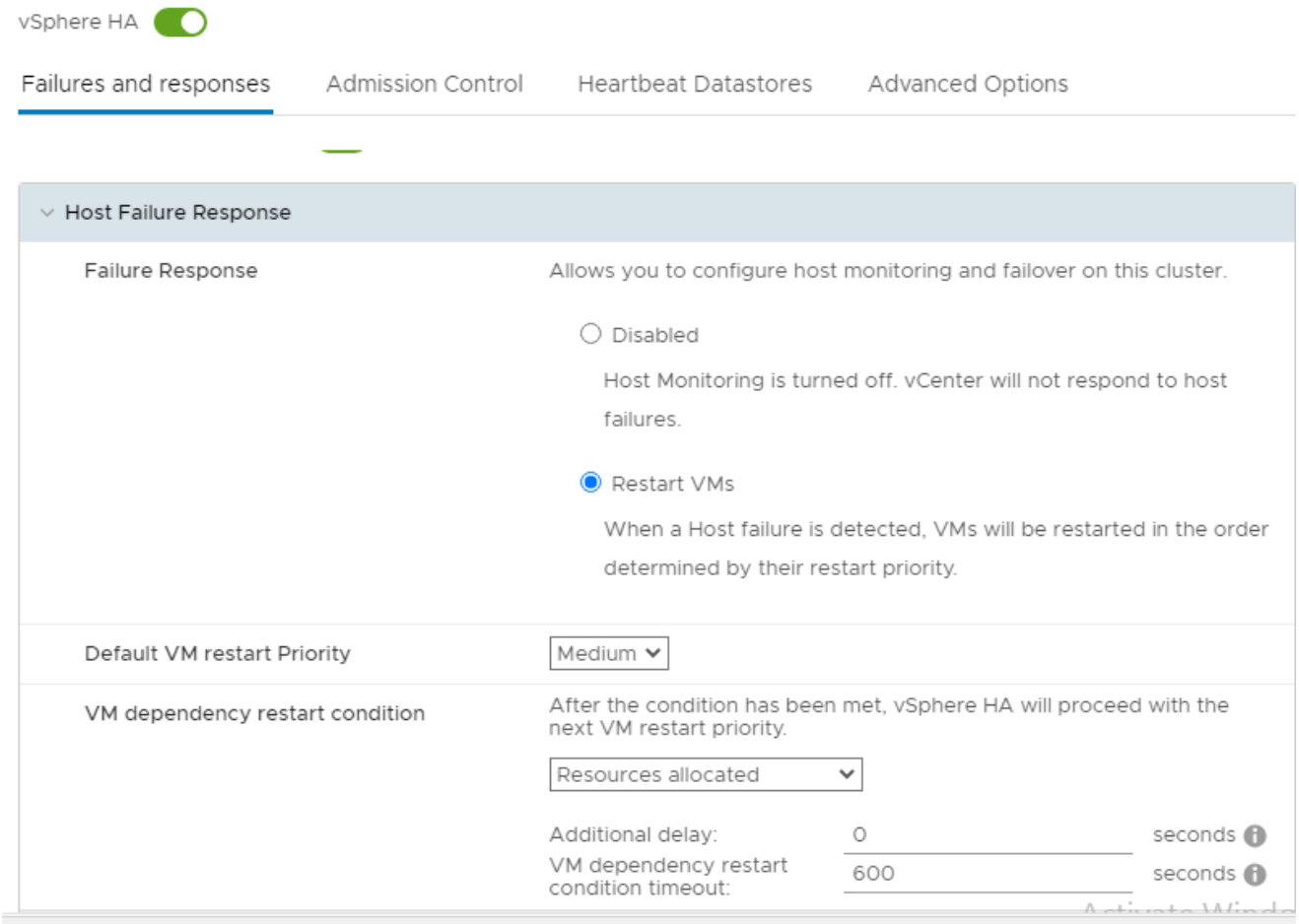
Performance Degradation VMs Tolerate

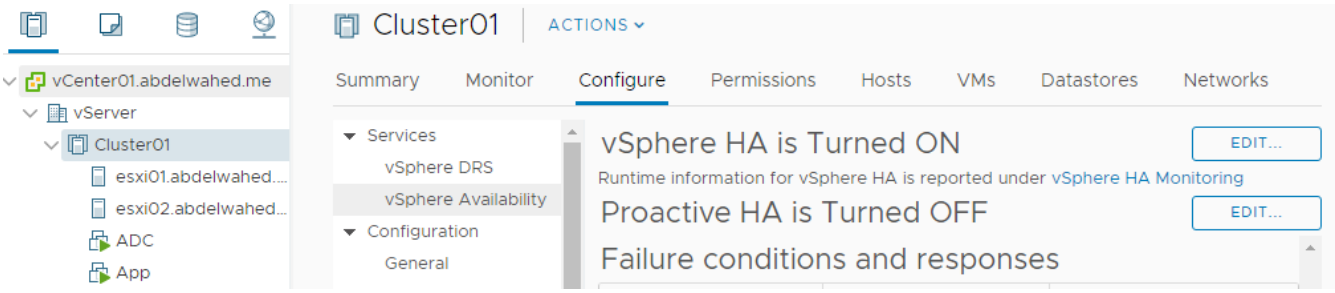
- **Percentage (%):** Indicates the percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure (e.g., 100%).
    - 0% raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart.
    - 100% disables the warning.


vSphere HA
Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options
Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.
Host failures cluster tolerates
1
Maximum is one less than number of hosts in cluster.
Define host failover capacity by
Cluster resource Percentage
Override calculated failover capacity.
Reserved failover CPU capacity:
20
% CPU
Reserved failover Memory capacity:
30
% Memory
Performance degradation VMs tolerate
100
%
Percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure. 0% - Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart. 100% - Warning is disabled.
vSphere HA
Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options
Maximum is one less than number of hosts in cluster.
Define host failover capacity by
Slot Policy (powered-on VMs)
Define slot policy
Cover all powered-on virtual machines
Calculate slot size based on the maximum CPU/Memory reservation and overhead of all powered-on virtual machines.
Fixed slot size
Specify the slot size explicitly.
CPU slot size:
32
MHz
Memory slot size:
100
MB
VMs requiring multiple slots:
VIEW
CALCULATE
Performance degradation VMs tolerate
100
%
Percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure. 0% - Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart. 100% - Warning is disabled.
Activate Windows
Go to Settings to activa


vSphere HA
Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options
Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.
Host failures cluster tolerates
1
Maximum is one less than number of hosts in cluster.
Define host failover capacity by
Dedicated failover hosts
Add
Remove
Failover Hosts


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
Available heartbeat datastores
Name
Datastore Cluster
Hosts Mounting Datastore
Datastore5-ISCSI
N/A
2
Datastore04_ISCSI
N/A
2


vSphere HA
Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options
Host Failure Response
Failure Response
Allows you to configure host monitoring and failover on this cluster.
Disabled
Host Monitoring is turned off. vCenter will not respond to host failures.
Restart VMs
When a Host failure is detected, VMs will be restarted in the order determined by their restart priority.
Default VM restart Priority
Medium
VM dependency restart condition
After the condition has been met, vSphere HA will proceed with the next VM restart priority.
Resources allocated
Additional delay:
0
seconds
VM dependency restart condition timeout:
600
seconds


vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed....
esxi02.abdelwahed...
ADC
App
Cluster01
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Services
vSphere DRS
vSphere Availability
Configuration
General
vSphere HA is Turned ON
EDIT...
Runtime information for vSphere HA is reported under vSphere HA Monitoring
Proactive HA is Turned OFF
EDIT...
Failure conditions and responses

Testing VMware HA Failover

Scenario: Testing Failover by Disconnecting ESXi02

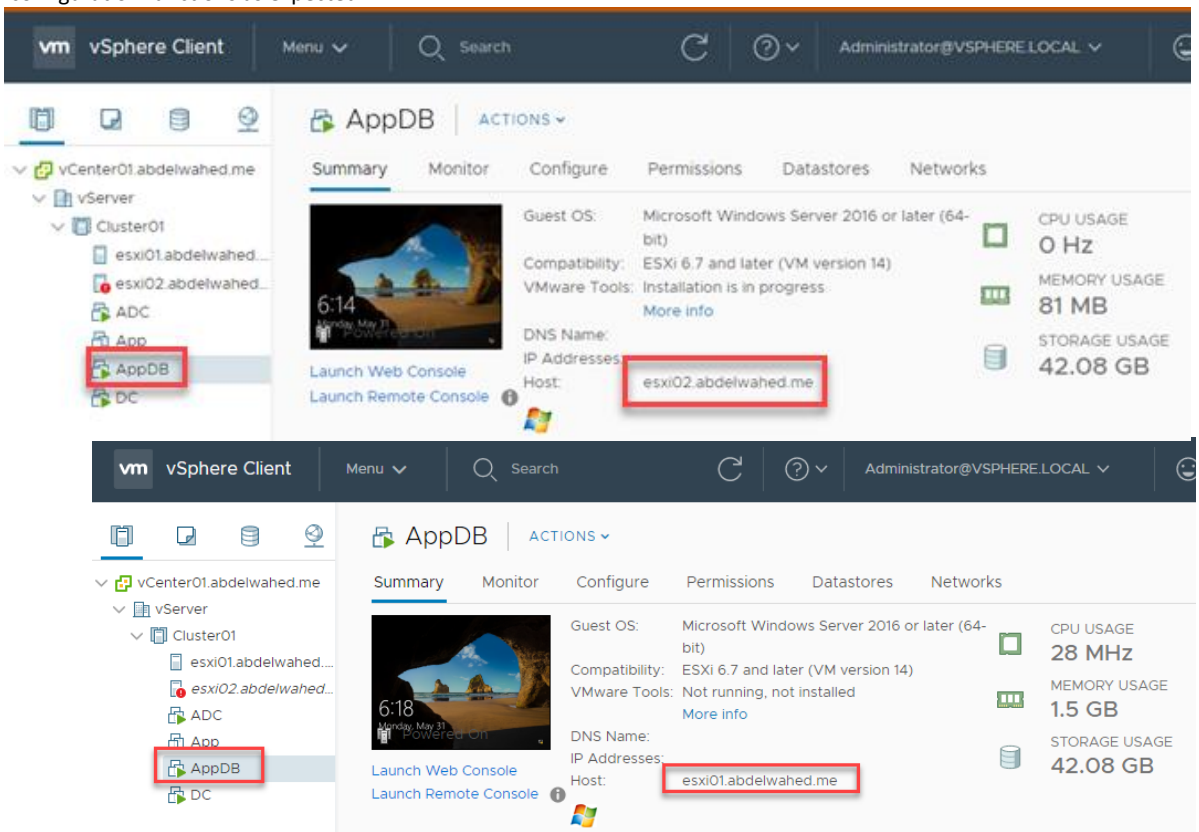
Objective: Verify that VMware HA properly triggers a failover event when ESXi02 is disconnected from the network, and the AppDB virtual machine is restarted on ESXi01.

Steps and Expected Outcomes

1. **Network Disconnection**:
   - **Action**: Disconnect ESXi02 from the network.
   - **Expected Outcome**: VMware HA detects the loss of network connection to ESXi02.
2. **Failover Event:**
   - **Response**: If configured correctly, VMware HA will initiate the process to restart the virtual machines from ESXi02 on another host in the cluster, such as ESXi01.
3. **Resource Allocation:**
   - **Assumption**: ESXi01 has sufficient resources to accommodate the virtual machines from ESXi02.
   - **Outcome**: The AppDB virtual machine should be automatically restarted on ESXi01.
4. **Time to Completion:**
   - **Consideration**: The time required to restart the virtual machine depends on its size and complexity.
   - **Expected Outcome**: The virtual machine is restarted and operational on ESXi01.
5. **Post-Failover Connectivity:**
   - **Verification**: Connect to the AppDB virtual machine on ESXi01.
   - **Expected Outcome**: You should be able to connect and use the virtual machine as usual.

Important Considerations

- **Potential Downtime**: VMware HA aims to minimize downtime but does not guarantee zero downtime. There may be a delay during the failover process.
- **Application Configuration:** Some applications may require additional configuration to operate correctly after a failover.
- **Testing in Controlled Environment:** Always test failover scenarios in a controlled environment to ensure that your HA configuration functions as expected.



VMware vCenter Proactive HA

VMware vCenter Server can utilize Proactive HA to monitor the health of physical server hardware components and proactively migrate virtual machines to healthy hosts before a hardware failure occurs. This feature requires specific hardware monitoring plugins such as Dell OpenManage or HP Insight Manager installed on the ESXi hosts.

Key Features of Proactive HA

1. **Health Monitoring**:
   - Monitors hardware components like CPUs, memory, and storage for potential failures or performance degradation.
2. **Proactive Migration:**
   - Uses vCenter and Distributed Resource Scheduler (DRS) to migrate VMs to healthy hosts if an issue is detected before it leads to hardware failure.
3. **Minimize Downtime:**
   - Helps to minimize downtime and prevent data loss by taking preventive measures.

Requirements

- **Hardware Monitoring Plugins**: Plugins provided by hardware vendors (e.g., Dell OpenManage, HP Insight Manager) need to be installed on ESXi hosts.
- **Appropriate Hardware Sensors:** Ensure the hardware supports the necessary sensors for health monitoring.
- **Configuration:** Additional configuration beyond basic vCenter HA.

Configuration and Testing

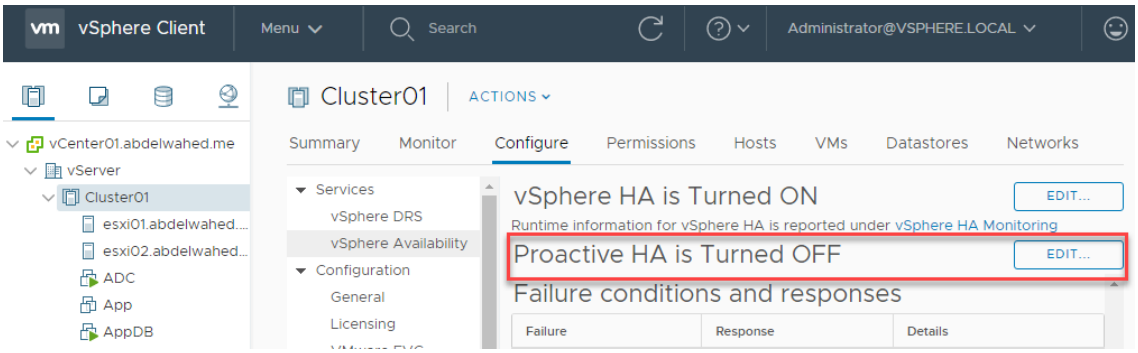
1. **Install Plugins:**
   - Install the necessary hardware monitoring plugins on the ESXi hosts.
2. **Enable Proactive HA:**
   - In vCenter, navigate to the cluster settings and enable Proactive HA.
   - Configure the hardware health monitoring settings and thresholds.
3. **Define Remediation Policies:**
   - Set policies for how VMs should be migrated in case of hardware degradation.
   - Determine whether remediation should be automatic or manual.
4. **Test Configuration:**
   - Carefully test and validate the Proactive HA configuration to ensure it works properly.
   - Simulate hardware failures or degradations to verify that VMs are migrated as expected.

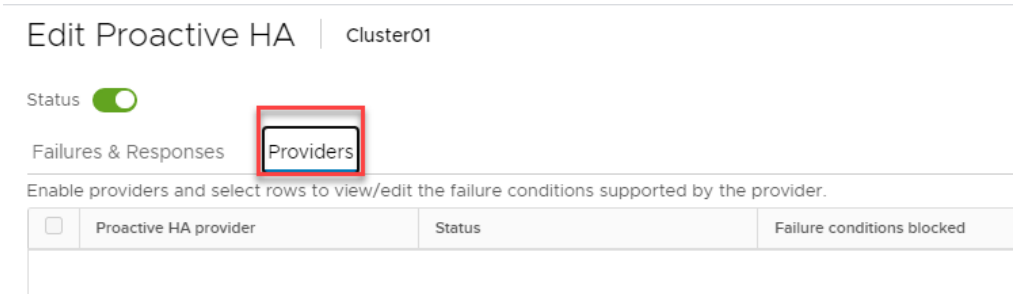
Remediation Actions

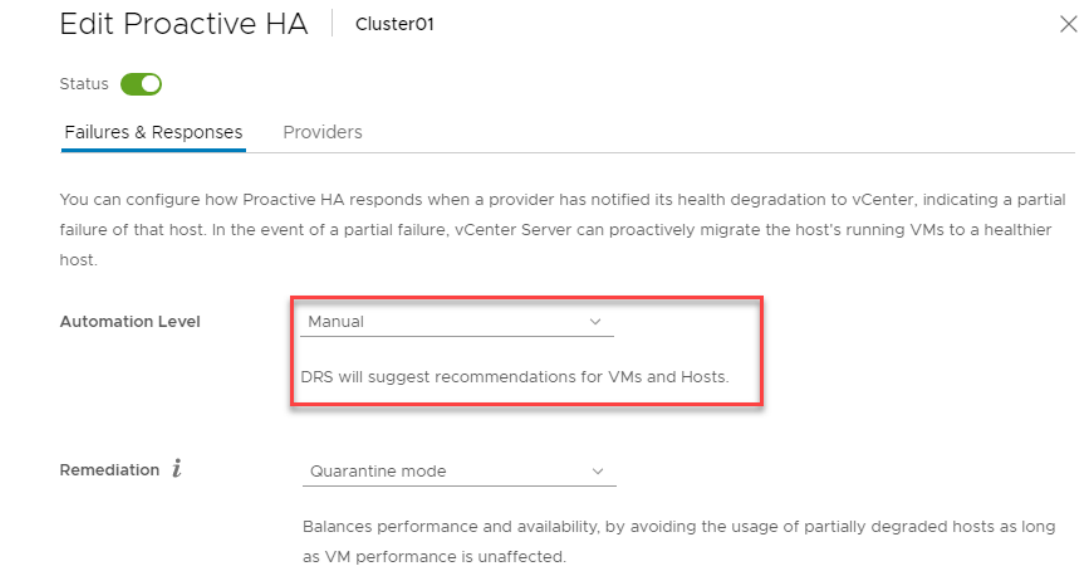
- **Proactive HA Remediation**:
  - Migrates VMs to healthy hosts before hardware failure occurs based on detected issues.
- **vSphere DRS:**
  - Balances resource utilization across hosts, automatically migrating VMs as needed to ensure optimal resource allocation and minimize downtime.

Policies and Planning

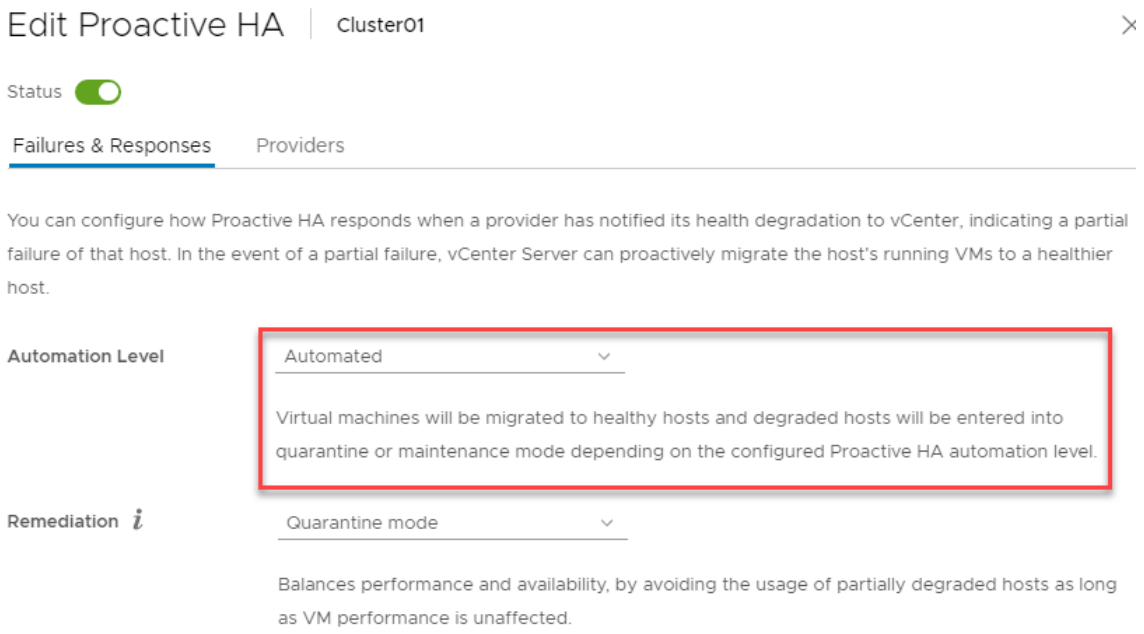
1. **Define Policies**:
   - Set policies for migration to standby hosts or hosts with specific performance characteristics.
   - Decide on automatic vs. manual remediation based on the severity of issues and impact on VM operations.
2. **Regular Testing:**
   - Regularly test remediation policies to ensure timely and efficient VM migration.
   - Ensure minimal disruption to critical workloads and avoid unnecessary risk.


vSphere Client
Menu
Search
Administrator@VSPHERE.LOCAL
Cluster01
ACTIONS
vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed....
esxi02.abdelwahed...
ADC
App
AppDB
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Services
vSphere DRS
vSphere Availability
Configuration
General
Licensing
vSphere HA is Turned ON
EDIT...
Runtime information for vSphere HA is reported under vSphere HA Monitoring
Proactive HA is Turned OFF
EDIT...
Failure conditions and responses
Failure
Response
Details

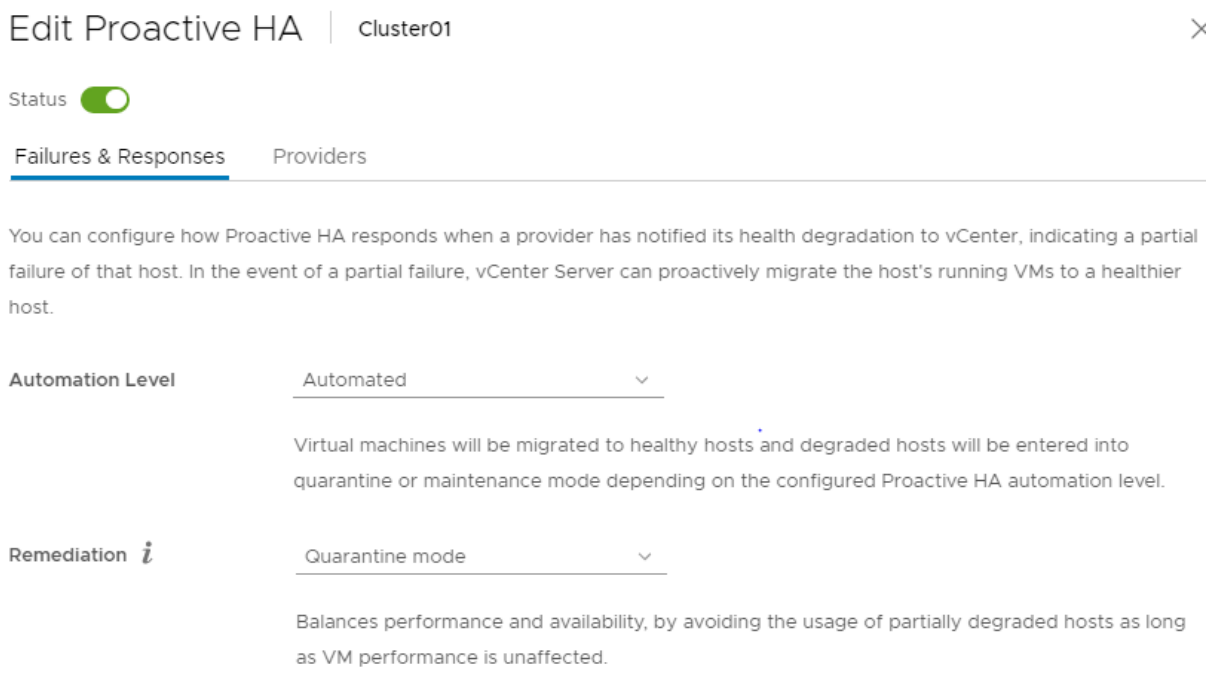

Edit Proactive HA
Cluster01
Status
Failures & Responses
Providers
Enable providers and select rows to view/edit the failure conditions supported by the provider.
Proactive HA provider
Status
Failure conditions blocked


Edit Proactive HA
Cluster01
Status
Failures & Responses
Providers
You can configure how Proactive HA responds when a provider has notified its health degradation to vCenter, indicating a partial failure of that host. In the event of a partial failure, vCenter Server can proactively migrate the host's running VMs to a healthier host.
Automation Level
Manual
DRS will suggest recommendations for VMs and Hosts.
Remediation
Quarantine mode
Balances performance and availability, by avoiding the usage of partially degraded hosts as long as VM performance is unaffected.

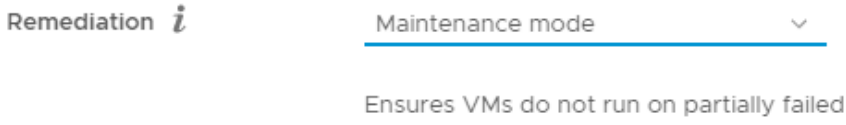
Remediation dictates the response (for HA) when a server is flagged for hardware degradation.



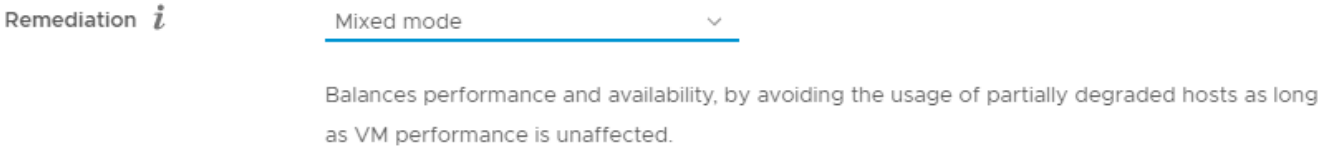
- When a server is in **quarantine mode**, it's excluded from high-availability tasks such as being selected for server transfers or chosen as the master.



- Maintenance mode, move all included VMs to another host.

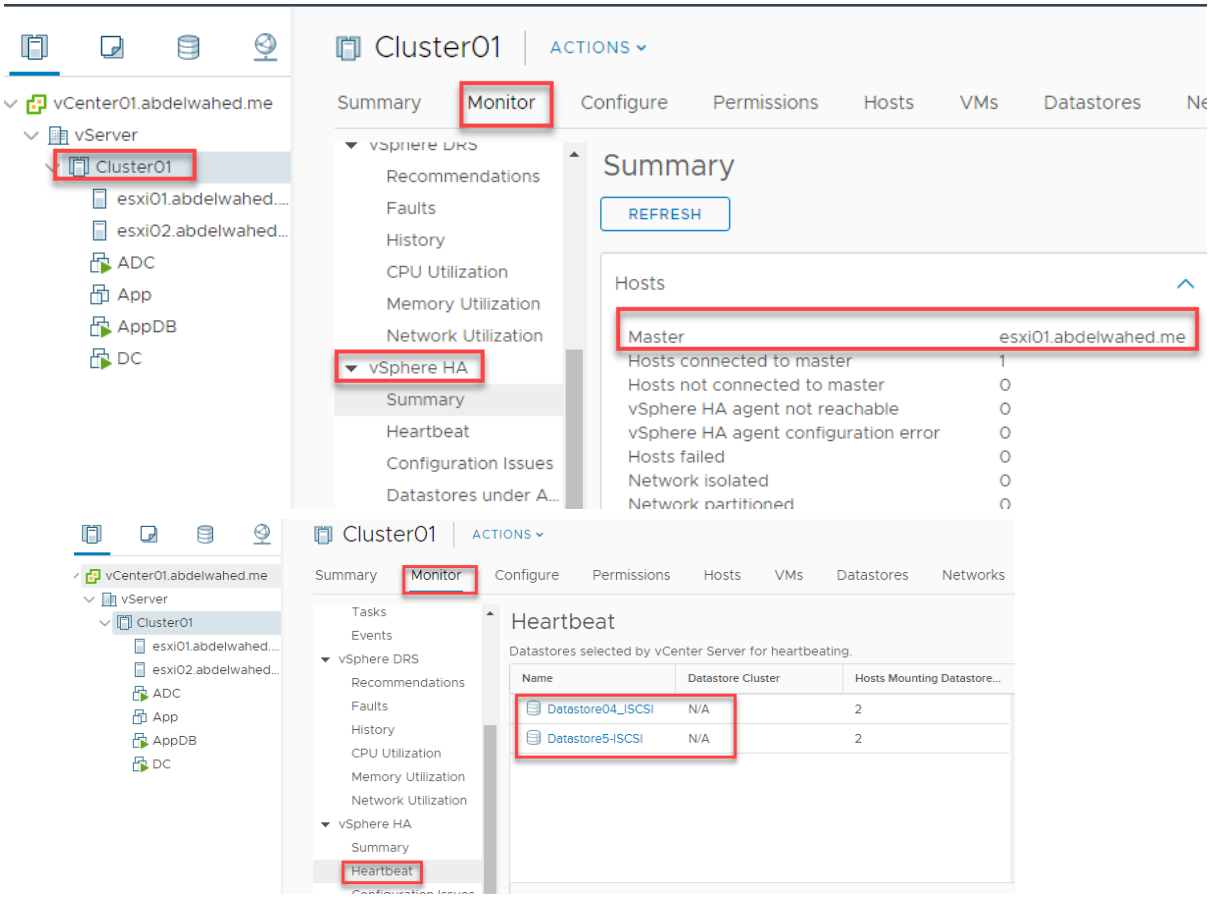


- Mixed mode, move VMs to another host and mark as quarantine



HA Summary and Heartbeat

voted master server



VMware Fault Tolerance (FT) for Zero Downtime

VMware Fault Tolerance (FT) provides a way to achieve zero downtime by duplicating a virtual machine (VM) on another host in the cluster and maintaining real-time synchronization of storage and memory between the primary and secondary VMs. If the primary VM fails or becomes unavailable, the secondary VM takes over seamlessly without any interruption.

Requirements and Considerations

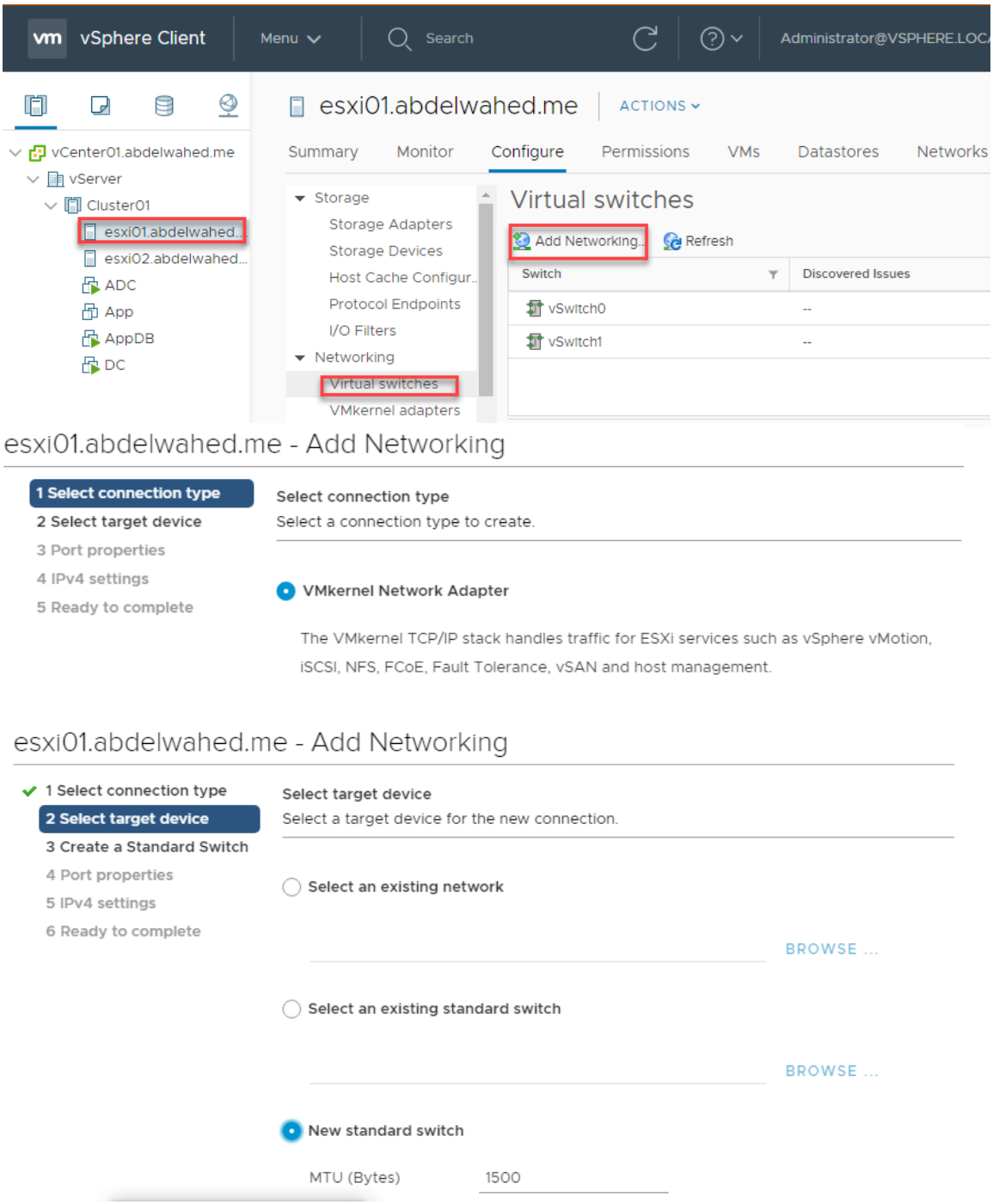
1. **Network Interface Cards (NICs)**:
   - Each host in the cluster must have at least two dedicated NICs with 1 Gbps speed or higher.
2. **Storage:**
   - The VM must be running on a datastore hosted on SSD storage to ensure optimal performance.
3. **Licensing:**
   - A valid VMware Fault Tolerance license must be available for each host in the cluster.
4. **VMware High Availability (HA):**
   - VMware HA must be enabled on the cluster.

Configuration Steps

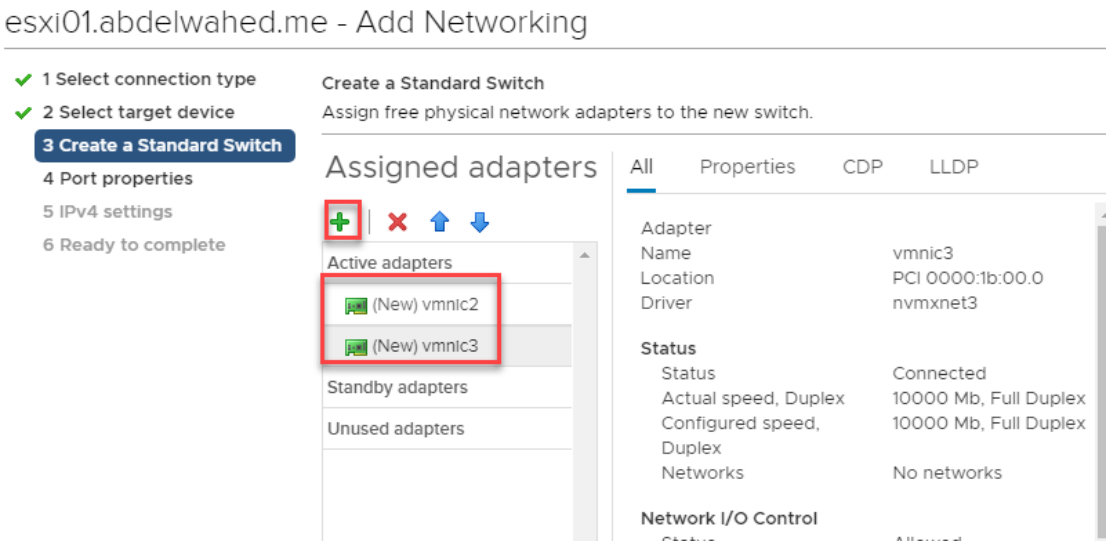
1. **Add and Configure NICs**:
   - Add the additional NICs to each ESXi host.
   - Ensure that the network settings are properly configured.
2. **Enable Fault Tolerance:**
   - Use the vSphere Client or vSphere Web Client to enable Fault Tolerance for the VM.
   - This process creates a duplicate VM on another host in the cluster and synchronizes the storage and memory between the primary and secondary VMs.

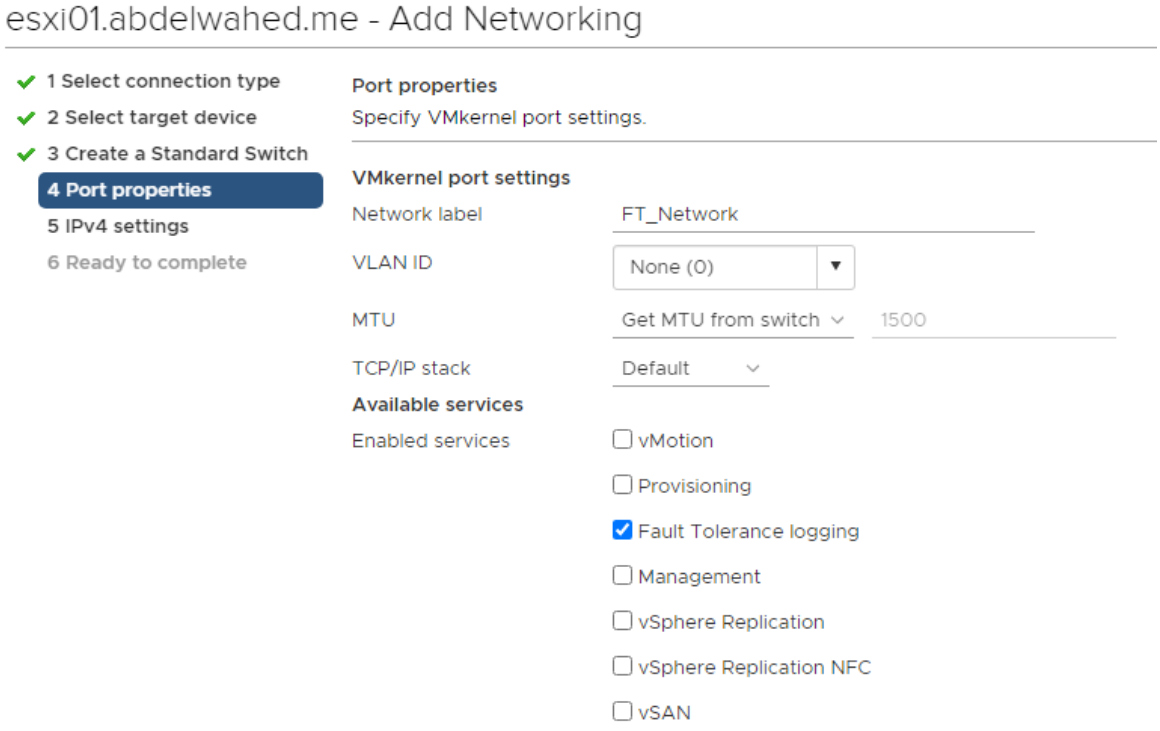
Important Notes

- **Not a Replacement for Backups**:
  - Fault Tolerance helps maintain zero downtime but does not protect against data loss or other types of disruptions.
  - Maintain a comprehensive disaster recovery plan, including regular backups, replication, and other measures to ensure data availability and integrity.

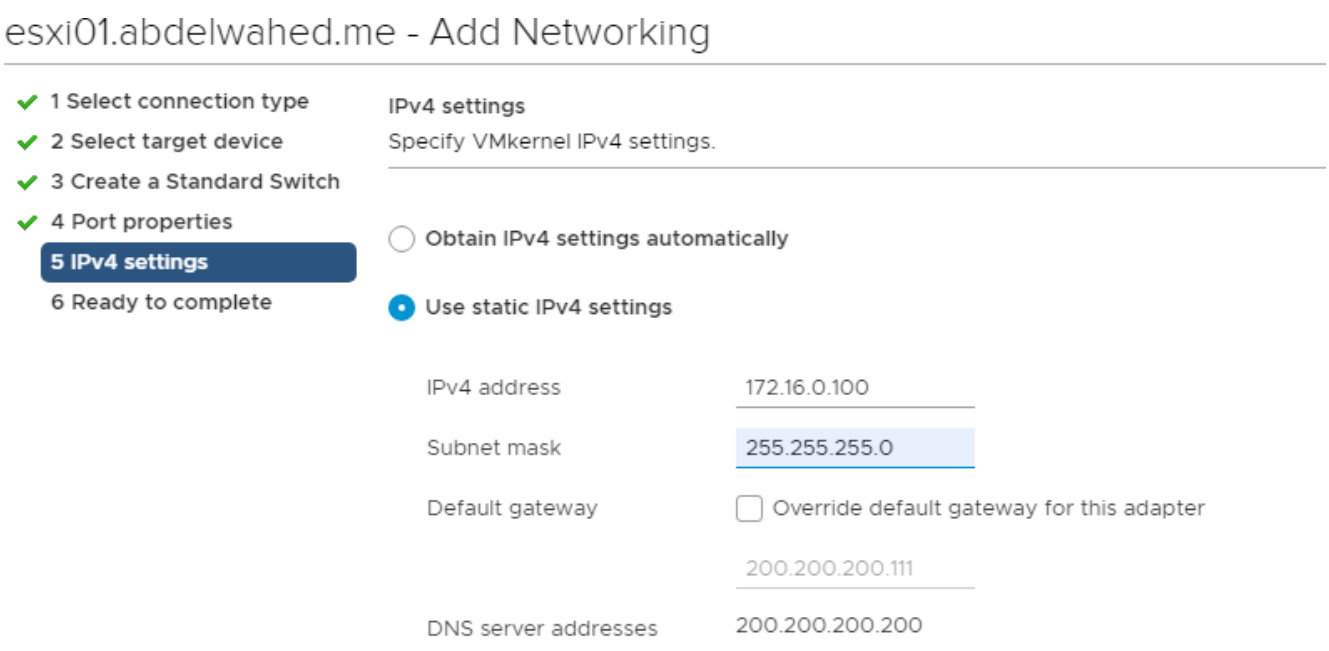


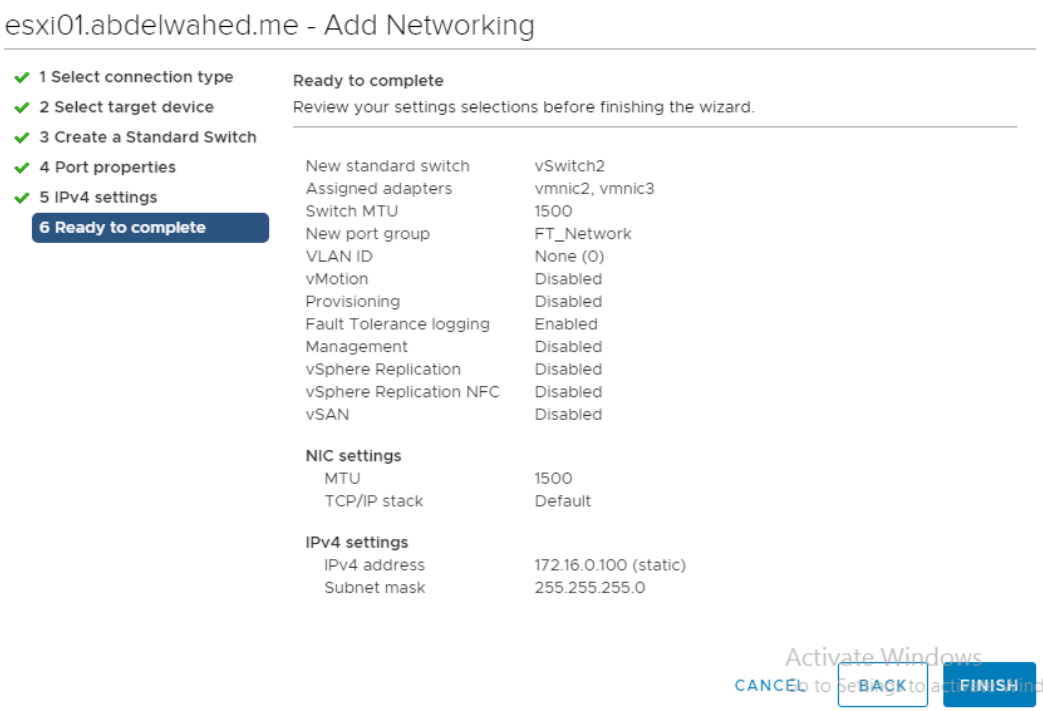
Include both adapters that were attached to the ESXi in the virtual switch.





Set up a distinct IP addressing scheme.

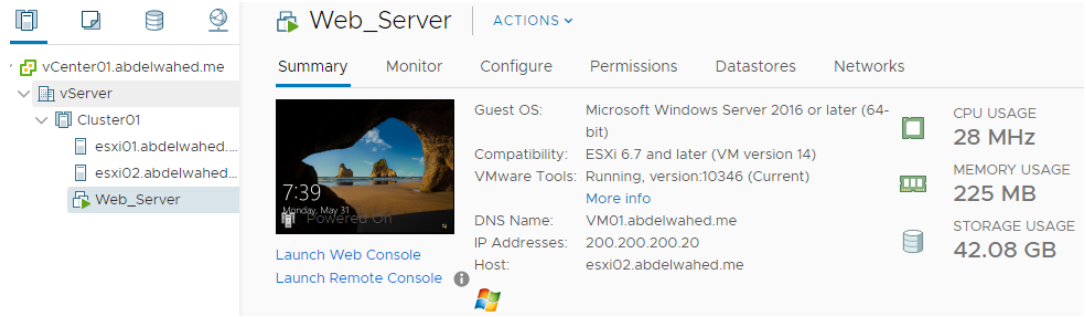


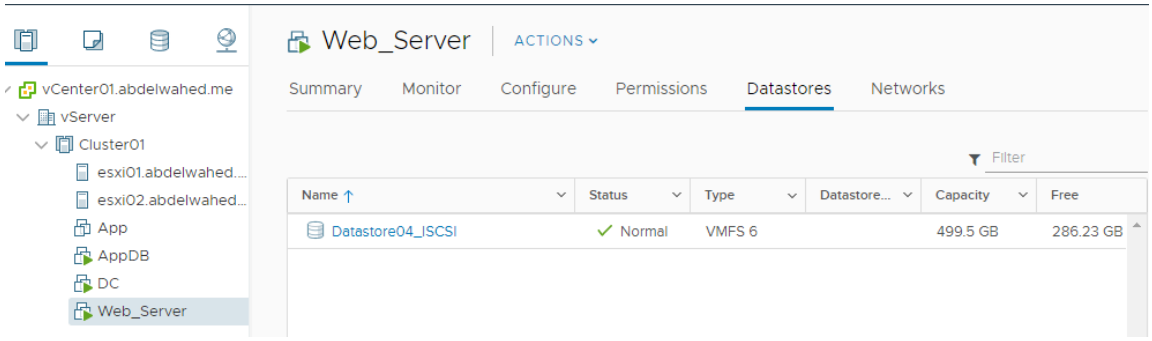


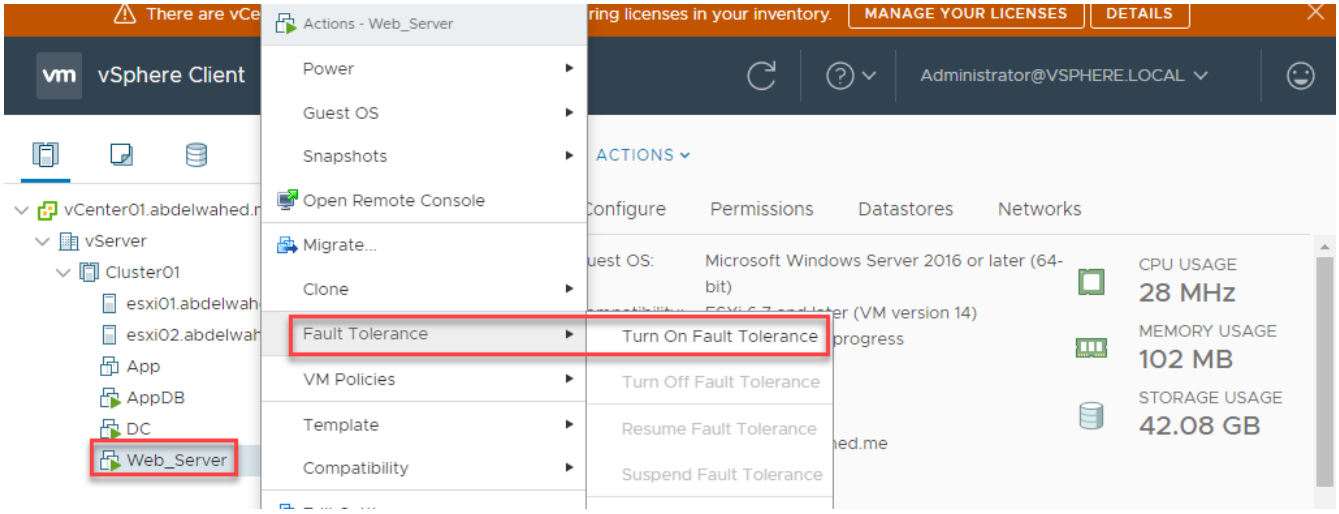
Do the same for EXSi02, which has the IP address 172.16.0.101.

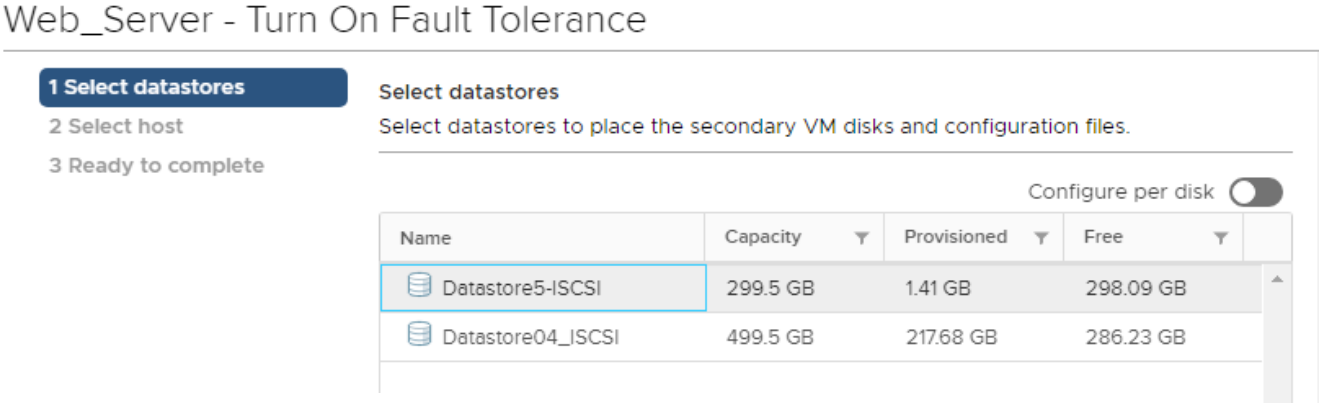
Enabling Fault Tolerance (FT) for App Server

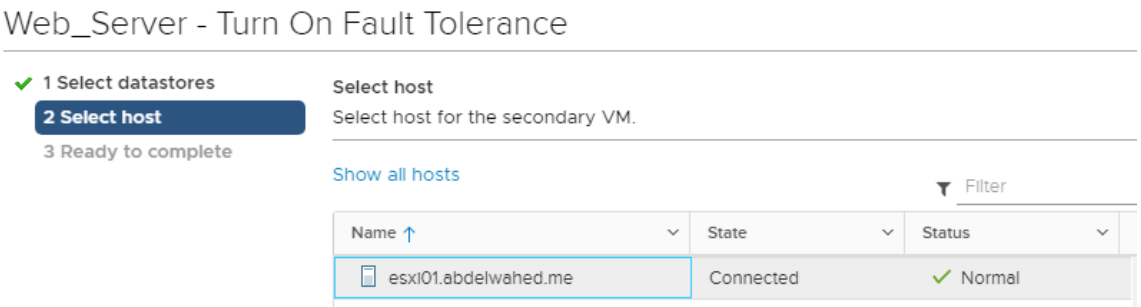
To enable FT for the Web_Server VM hosted on ESXi01 and ensure the secondary VM is stored in a different iSCSI datastore

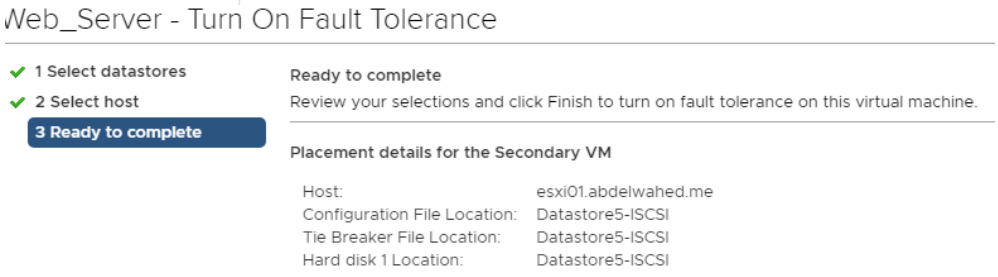


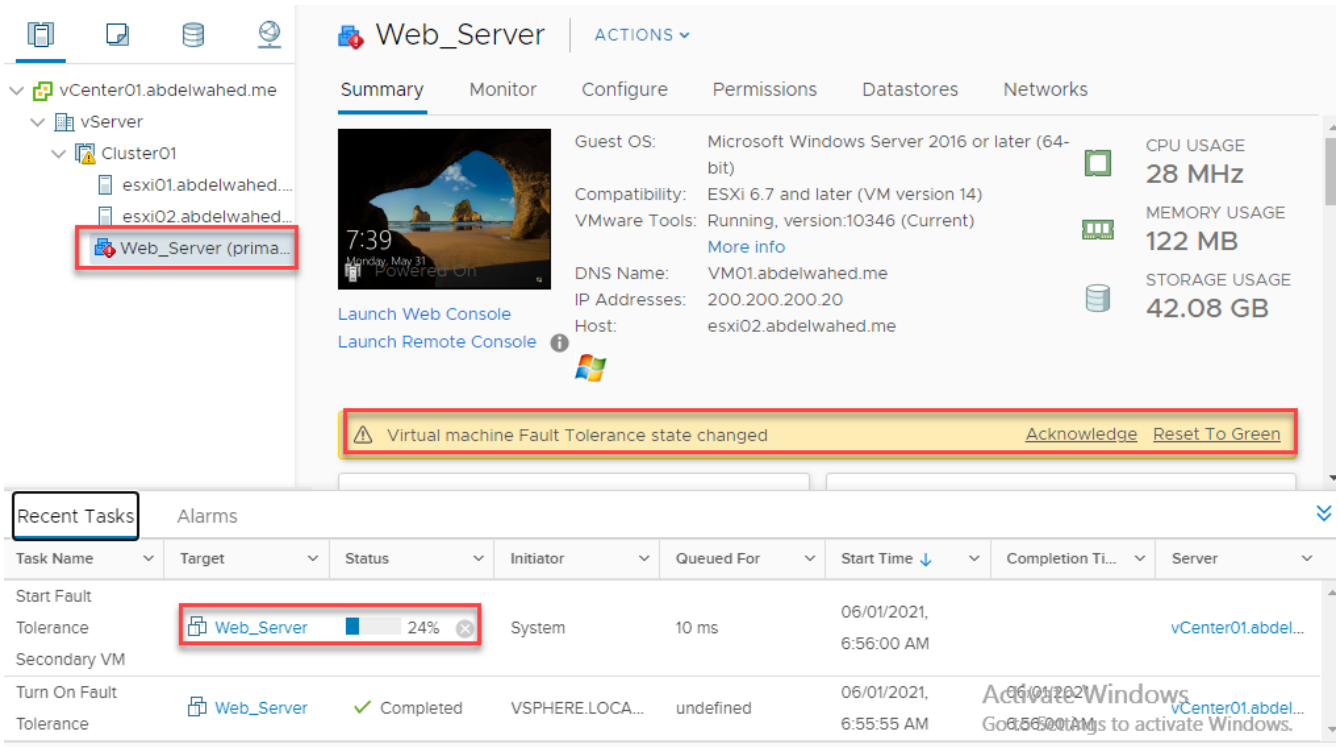


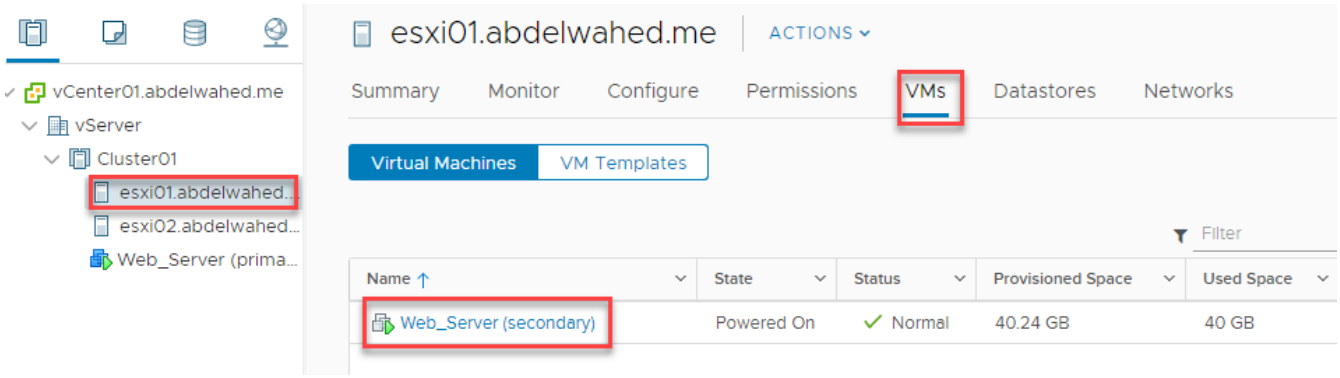

There are vCe
ring licenses in your inventory.
MANAGE YOUR LICENSES
DETAILS
vSphere Client
Administrator@VSPHERE.LOCAL
ACTIONS
vCenter01.abdelwahed.r
vServer
Cluster01
esxi01.abdelwah
esxi02.abdelwah
App
AppDB
DC
Web_Server
Actions - Web_Server
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Turn On Fault Tolerance
Turn Off Fault Tolerance
Resume Fault Tolerance
Suspend Fault Tolerance
Configure
Permissions
Datastores
Networks
uest OS:
Microsoft Windows Server 2016 or later (64-bit)
progress
CPU USAGE
28 MHz
MEMORY USAGE
102 MB
STORAGE USAGE
42.08 GB


Web_Server - Turn On Fault Tolerance
1 Select datastores
2 Select host
3 Ready to complete
Select datastores
Select datastores to place the secondary VM disks and configuration files.
Configure per disk
Name
Capacity
Provisioned
Free
Datastore5-ISCSI
299.5 GB
1.41 GB
298.09 GB
Datastore04_ISCSI
499.5 GB
217.68 GB
286.23 GB


Web_Server - Turn On Fault Tolerance
1 Select datastores
2 Select host
3 Ready to complete
Select host
Select host for the secondary VM.
Show all hosts
Filter
Name
State
Status
esxi01.abdelwahed.me
Connected
Normal

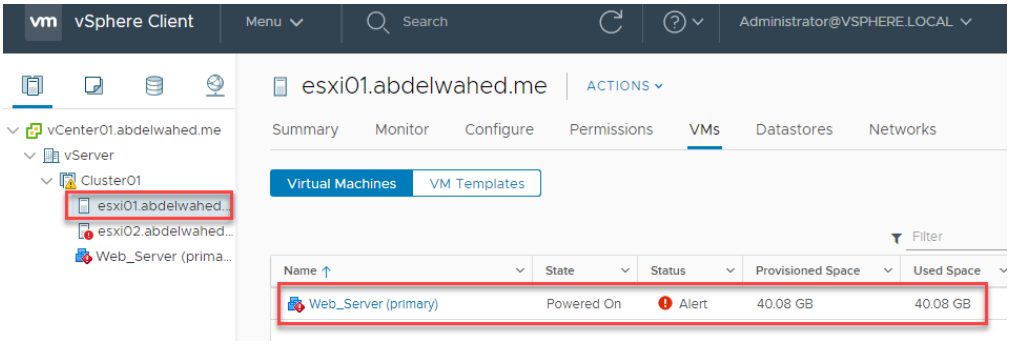

Web_Server - Turn On Fault Tolerance
1 Select datastores
2 Select host
3 Ready to complete
Ready to complete
Review your selections and click Finish to turn on fault tolerance on this virtual machine.
Placement details for the Secondary VM
Host:
esxi01.abdelwahed.me
Configuration File Location:
Datastore5-ISCSI
Tie Breaker File Location:
Datastore5-ISCSI
Hard disk 1 Location:
Datastore5-ISCSI





Testing Fault Tolerance (FT) by Disconnect ESXi02 (Primary Host)

Objective: Verify that VMware Fault Tolerance (FT) functions correctly when the primary host (ESXi02) is disconnected from the network, ensuring zero downtime for the Web_Server VM.



Migrating a Virtual Machine Without Failure in VMware

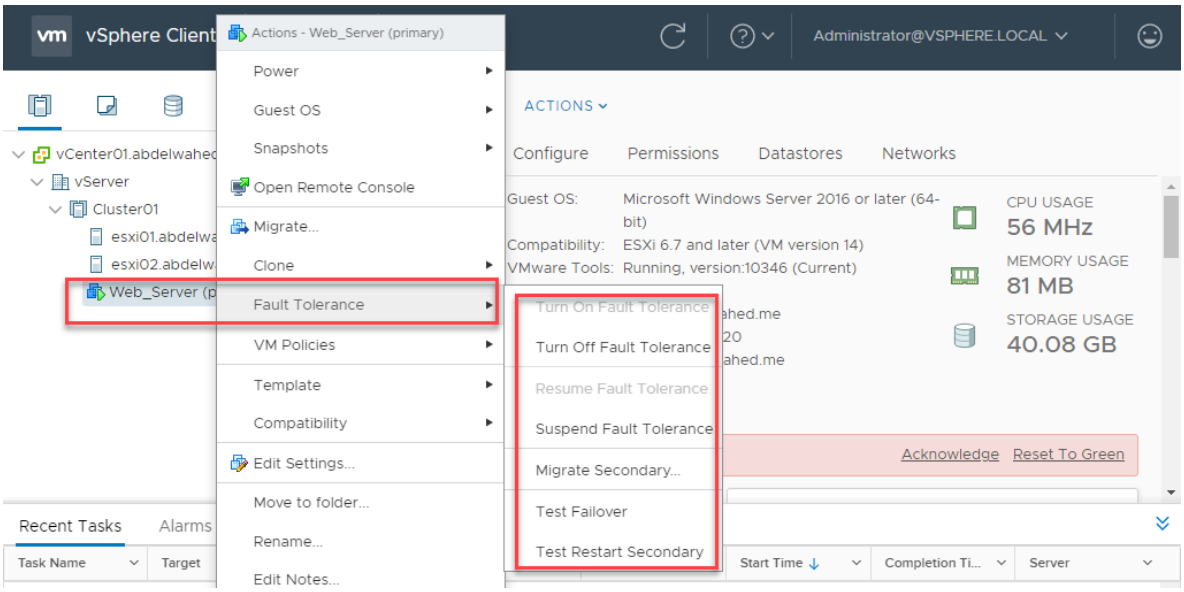
Migrating a virtual machine (VM) in VMware can be accomplished with minimal downtime and disruption by following best practices and ensuring proper planning. Here are the steps and considerations for a successful VM migration using vSphere vMotion, Storage vMotion, or Cross-Host vMotion.

Types of VM Migration

1. **vSphere vMotion**: Migrates a running VM from one physical host to another without downtime.
2. **Storage vMotion:** Migrates a VM's disk files from one datastore to another without downtime.
3. **Cross-Host vMotion:** Migrates VMs across different vCenter Server instances.

Best Practices for Migration

1. **Compatibility Check**:
   - Ensure that the source and destination hosts are compatible, including CPU, memory, and storage requirements.
   - Verify that both hosts are running compatible versions of ESXi.
2. **Resource Allocation:**
   - Check that the VM has the necessary resources allocated (CPU, memory, and storage).
   - Ensure that there is sufficient capacity on the destination host to accommodate the VM.
3. **Network Configuration:**
   - Verify that the network settings are properly configured on both the source and destination hosts.
   - Ensure that the VM can communicate with other network resources post-migration.
4. **Software and Applications:**
   - Ensure that any software or applications running on the VM are properly configured and will function correctly after migration.
   - Test applications in a similar environment before performing the actual migration.
5. **Backup:**
   - Take a snapshot or backup of the VM before initiating the migration process to ensure data safety.



Creating and Managing Resource Pools in VMware vSphere

Resource pools in VMware vSphere allow you to manage the allocation of resources (CPU and memory) for groups of virtual machines (VMs) within a cluster. They help in ensuring that resources are distributed based on priority, workload, and other factors. To create and manage resource pools, you need to enable the Distributed Resource Scheduler (DRS) on your cluster.

Prerequisites

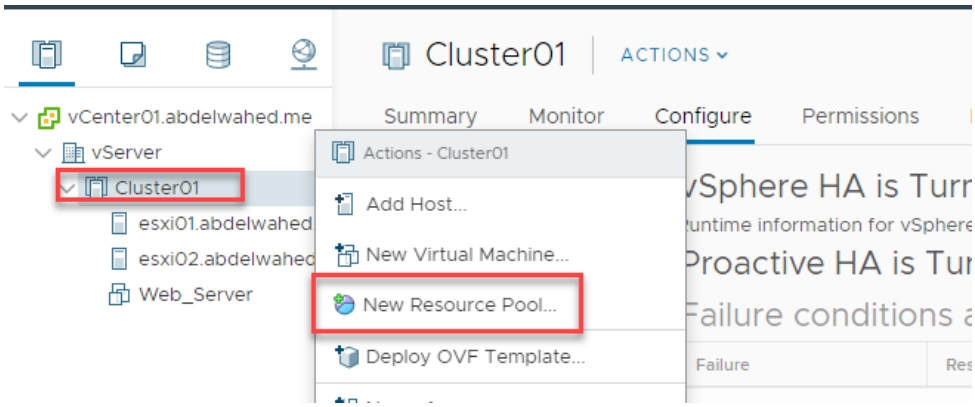
1. **Enable DRS**:
    - DRS must be enabled on the cluster to allow for automatic balancing of resource utilization across hosts.
    - Log in to vSphere Client, navigate to the cluster, and enable DRS under the "Configure" tab.

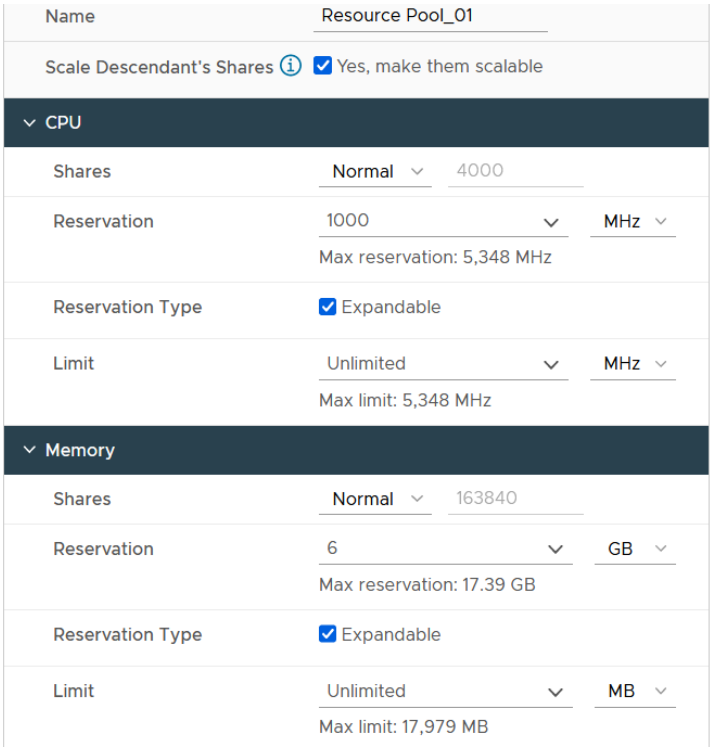
Steps to Create a Resource Pool

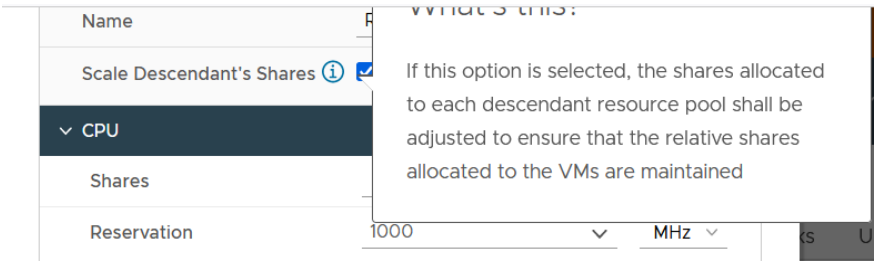
1. **Log in to vSphere Client**:
    - Open vSphere Client or vSphere Web Client and log in with appropriate credentials.
2. **Select the Cluster or Host:**
    - Navigate to the cluster or host where you want to create the resource pool.
3. **Navigate to Resource Pools:**
    - Go to the "Configure" tab.
    - Under "Resource Management," select "Resource Pools."
4. **Create a New Resource Pool:**
    - Click "Add" to create a new resource pool.
    - Provide a name and description for the resource pool.
5. **Configure Resource Pool Settings:**
    - **CPU Settings**:
        - **Reservation**: The guaranteed CPU resources for the resource pool.
        - **Limit**: The maximum CPU resources that the resource pool can use.
        - **Shares**: The relative priority of the resource pool in terms of CPU resources.
    - **Memory Settings**:
        - **Reservation**: The guaranteed memory resources for the resource pool.
        - **Limit**: The maximum memory resources that the resource pool can use.
        - **Shares**: The relative priority of the resource pool in terms of memory resources.
6. **Set Priorities:**
    - Assign high priority to critical workloads and low priority to less important workloads to ensure appropriate resource allocation.
7. **Create the Resource Pool:**
    - Review the settings and click "OK" to create the resource pool.

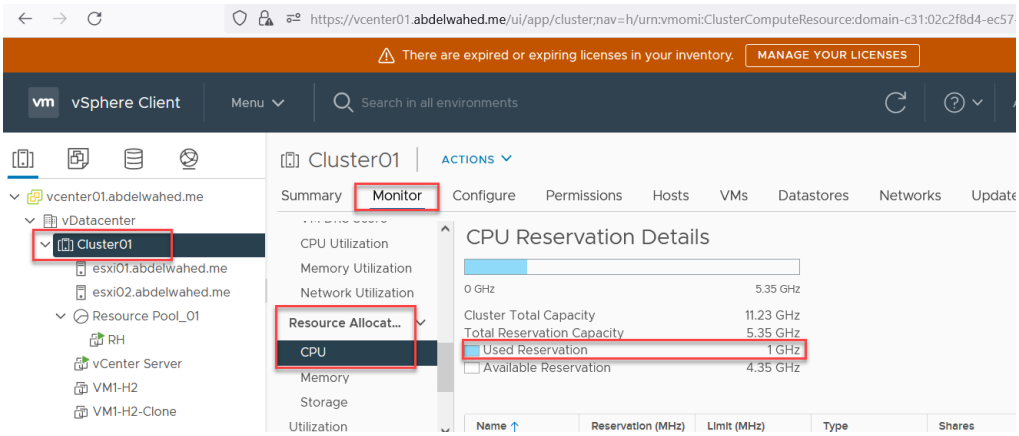
Managing Resource Pools

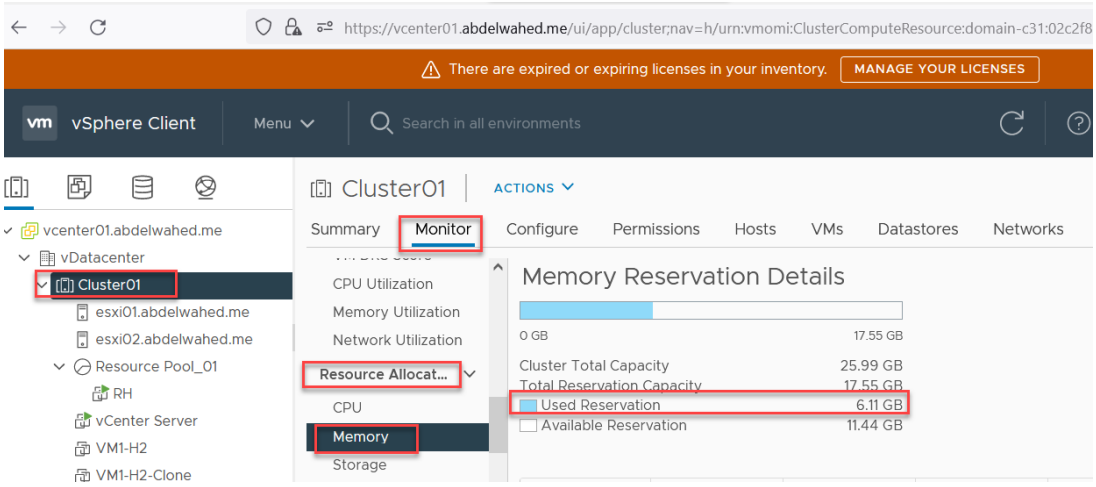
1. **Monitoring**:
    - Regularly monitor resource utilization to ensure that VMs are receiving appropriate resources.
    - Use performance charts and alerts to track resource usage and identify potential issues.
2. **Adjusting Settings**:
    - Adjust resource pool settings as needed to avoid resource contention and maintain optimal performance.
    - Modify reservations, limits, and shares based on current workload requirements.
3. **Allocating VMs to Resource Pools**:
    - Move VMs into the resource pool by dragging and dropping them into the desired pool.
    - Ensure that VMs are grouped appropriately based on their resource needs and priority.


Cluster01
ACTIONS
vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed
esxi02.abdelwahed
Web_Server
Summary
Monitor
Configure
Permissions
Actions - Cluster01
Add Host...
New Virtual Machine...
New Resource Pool...
Deploy OVF Template...
Failure

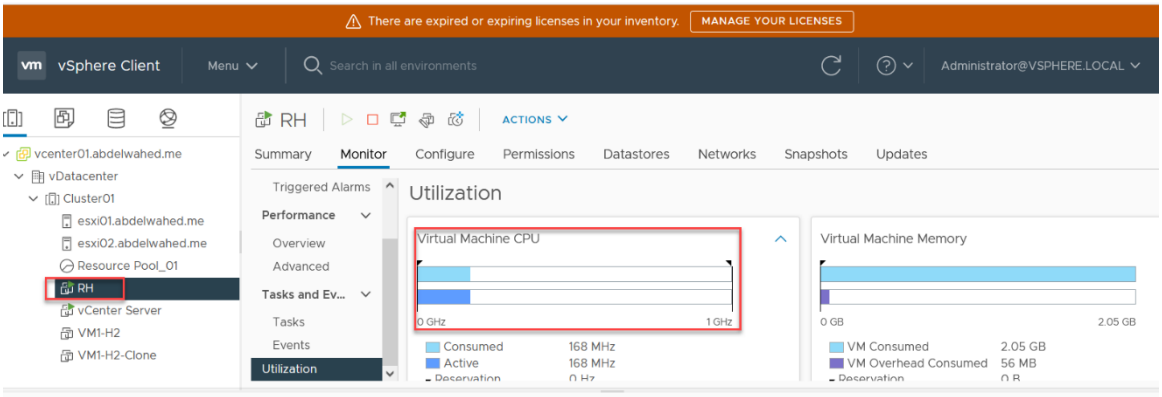

Name
Resource Pool_01
Scale Descendant's Shares
Yes, make them scalable
CPU
Shares
Normal
4000
Reservation
1000
MHz
Max reservation: 5,348 MHz
Reservation Type
Expandable
Limit
Unlimited
MHz
Max limit: 5,348 MHz
Memory
Shares
Normal
163840
Reservation
6
GB
Max reservation: 17.39 GB
Reservation Type
Expandable
Limit
Unlimited
MB
Max limit: 17,979 MB

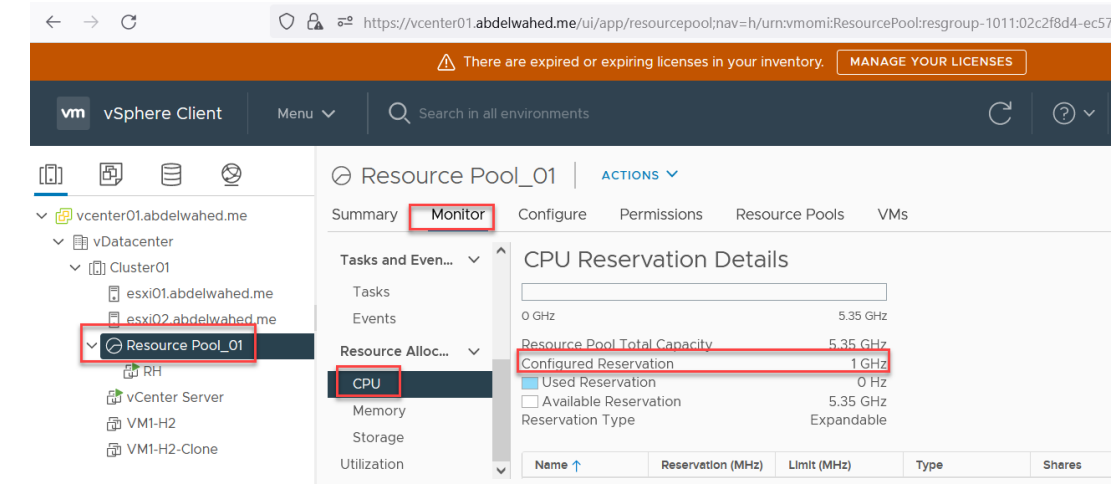

Name
Scale Descendant's Shares
CPU
Shares
Reservation
1000
MHz
If this option is selected, the shares allocated to each descendant resource pool shall be adjusted to ensure that the relative shares allocated to the VMs are maintained

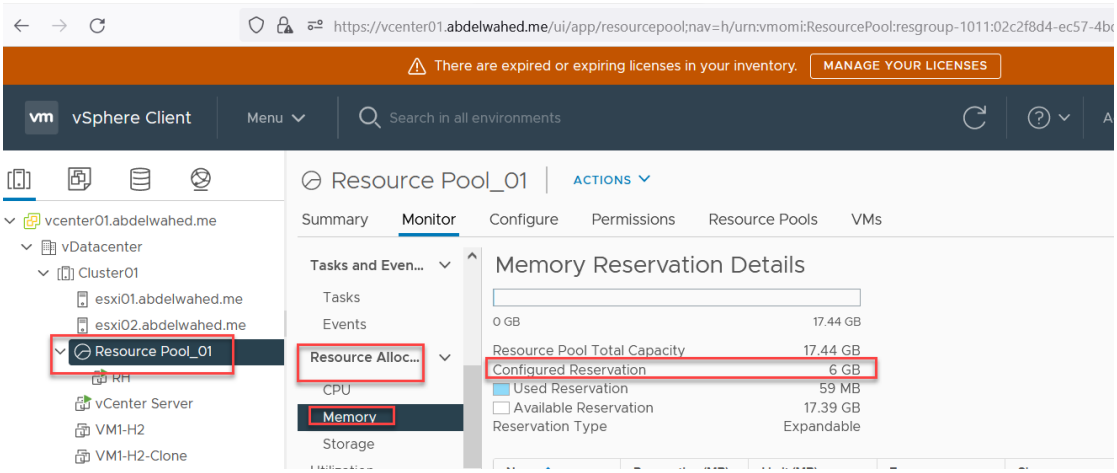




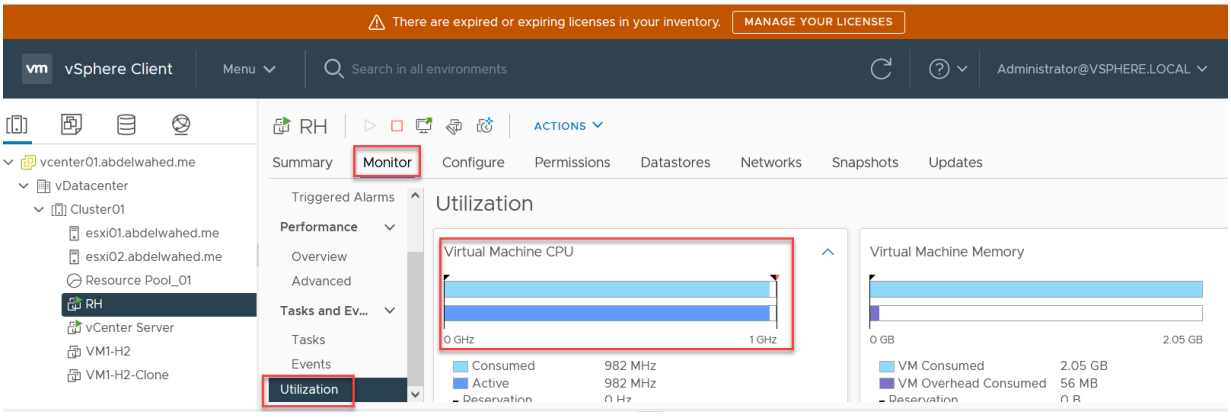
For testing purposes, I am utilizing a RedHat VM that operates at 1GHZ CPU speed.





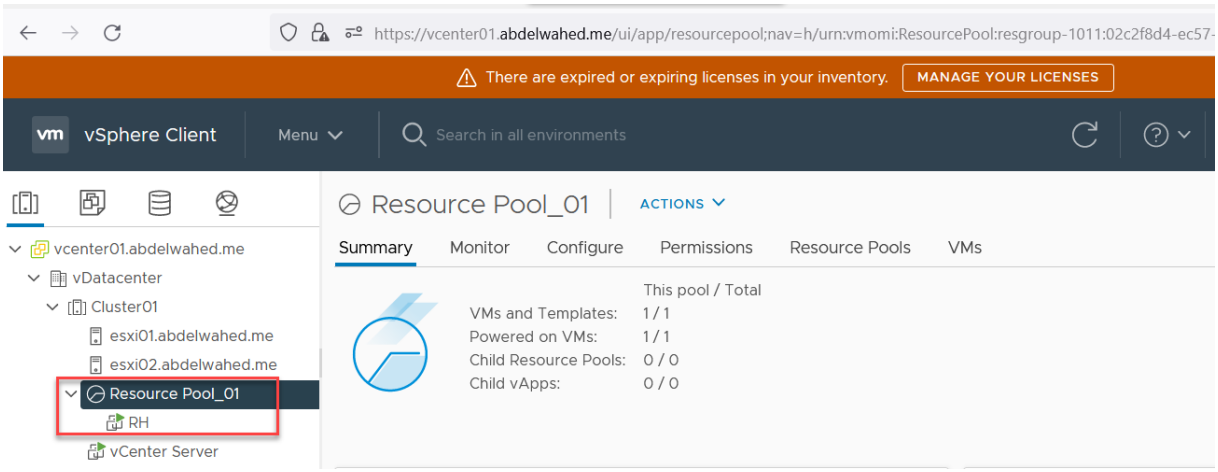


I plan to escalate CPU utilization by running the command dd if=/dev/zero of=/dev/null and will observe the changes in CPU performance.



Now, move

the RH VM into the new resource pool. Additionally, we can make a sub-pool, and deleting a resource pool won't affect the included VMs; it will just sever their connection to that pool.



vApp in VMware vSphere

A vApp in VMware is a container that allows you to group multiple virtual machines (VMs) together and manage them as a single entity. It extends the functionality of resource pools by providing additional management features and a higher level of abstraction.

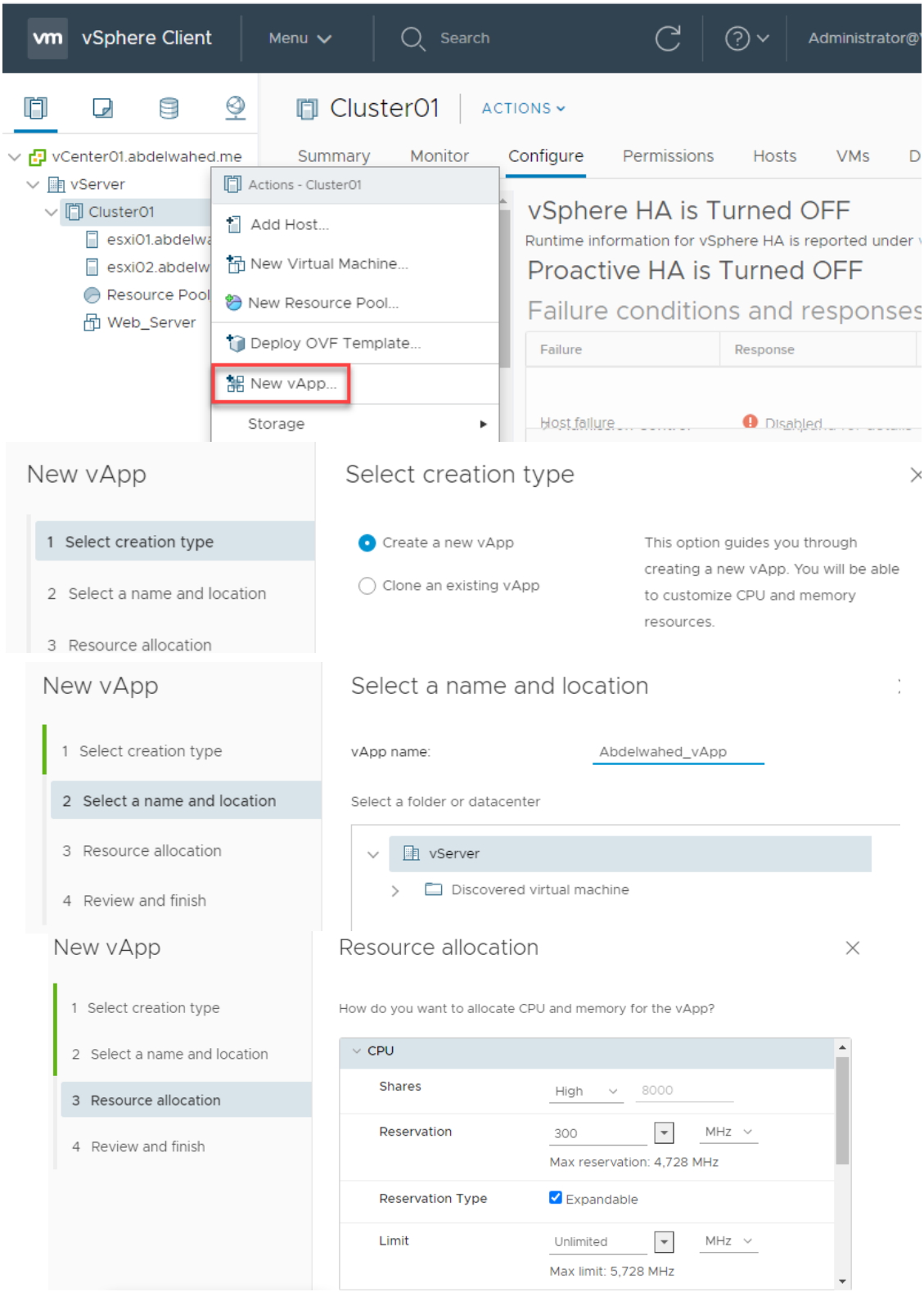
Key Features of vApp

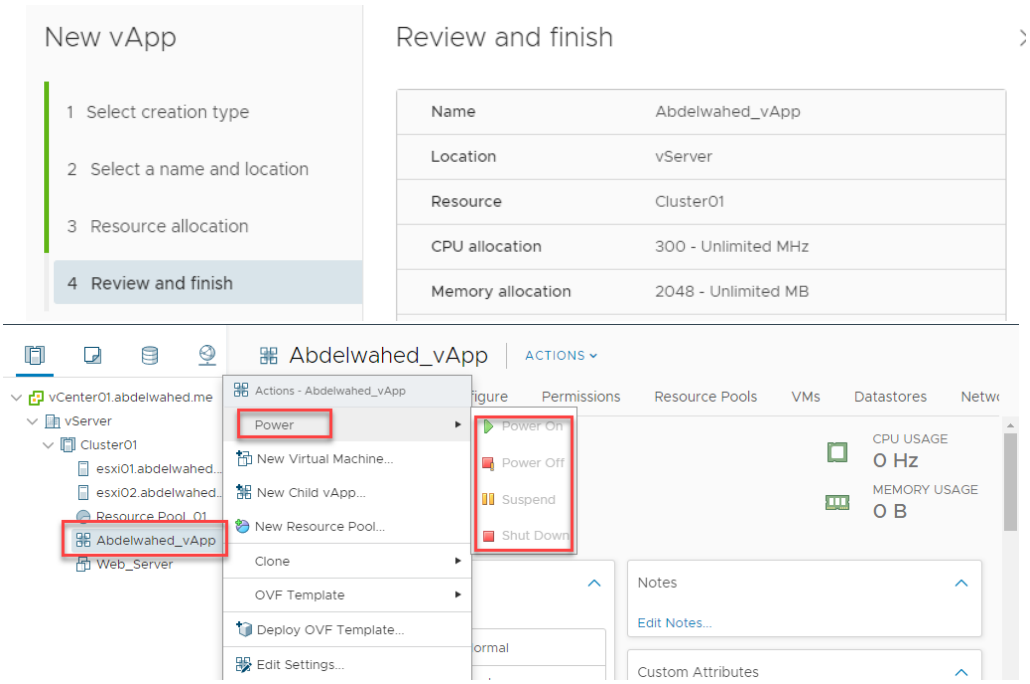
1. **Resource Allocation**:
   - Like resource pools, vApps allow you to allocate resources (CPU and memory) to a group of VMs based on their priority and workload.
2. **Start Order**:
   - You can define the start order for VMs within the vApp, ensuring that dependent applications or services are started in the correct sequence.
3. **Power State Control**:
   - You can control the power state of all VMs within the vApp simultaneously. This is useful for managing maintenance windows or other operational tasks.
4. **Simplified Management**:
   - Instead of managing individual VMs, you can manage the vApp as a single entity, simplifying management and improving efficiency.

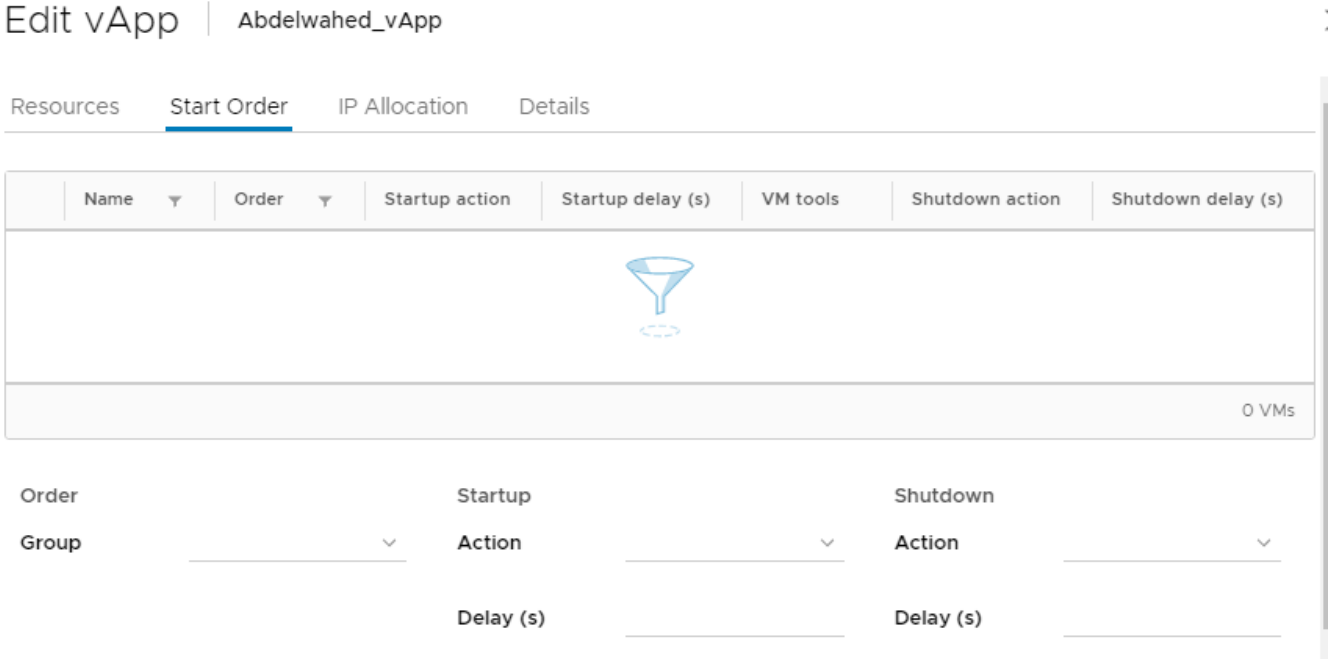
Use Cases for vApp

- **Multi-Tiered Applications**:
  - Group related VMs that form a multi-tiered application (e.g., web server, application server, database server) and manage them together.
- **Development Environments**:
  - Create development or test environments with multiple VMs and manage them as a single unit.
- **Maintenance**:
  - Power on or off all VMs in the vApp at the same time for maintenance purposes.

Creating and Managing a vApp




New vApp
1 Select creation type
2 Select a name and location
3 Resource allocation
4 Review and finish
Review and finish
Name
Abdelwahed_vApp
Location
vServer
Resource
Cluster01
CPU allocation
300 - Unlimited MHz
Memory allocation
2048 - Unlimited MB
Abdelwahed_vApp
ACTIONS
vCenter01.abdelwahed.me
vServer
Cluster01
esxi01.abdelwahed...
esxi02.abdelwahed...
Resource Pool_01
Abdelwahed_vApp
Web_Server
Actions - Abdelwahed_vApp
Power
New Virtual Machine...
New Child vApp...
New Resource Pool...
Clone
OVF Template
Deploy OVF Template...
Edit Settings...
Power On
Power Off
Suspend
Shut Down
Permissions
Resource Pools
VMs
Datastores
CPU USAGE
0 Hz
MEMORY USAGE
0 B
Notes
Edit Notes...
Custom Attributes


Edit vApp
Abdelwahed_vApp
Resources
Start Order
IP Allocation
Details
Name
Order
Startup action
Startup delay (s)
VM tools
Shutdown action
Shutdown delay (s)
0 VMs
Order
Group
Startup
Action
Delay (s)
Shutdown
Action
Delay (s)

VMware vSphere Lifecycle Manager

VMware vSphere Lifecycle Manager is a feature integrated into vCenter Server, providing centralized management for the lifecycle of ESXi hosts. It simplifies updating, patching, and configuring hardware and software components, ensuring compliance and optimal performance.

Key Features

1. **Centralized Management**:
   - Provides a single interface for managing the entire lifecycle of ESXi hosts.
   - Included with vCenter Server, no additional installation required.
2. **Lifecycle Stages**:
   - **Deployment**: Deploy new ESXi hosts.
   - **Maintenance**: Apply updates and patches.
   - **Retirement**: Decommission and retire hosts.
3. **Baselines and Compliance**:
   - Create and apply baselines for host configuration and software updates.
   - Ensure hosts meet compliance standards for security and regulations.
4. **Hardware and Software Management**:
   - Visibility into firmware, driver versions, and other hardware components.
   - Update and manage hardware and software components as needed.
5. **HTML5-Based Interface**:
   - Accessible through the vSphere Client, providing a modern, intuitive interface for managing host lifecycles.

Steps to Use vSphere Lifecycle Manager

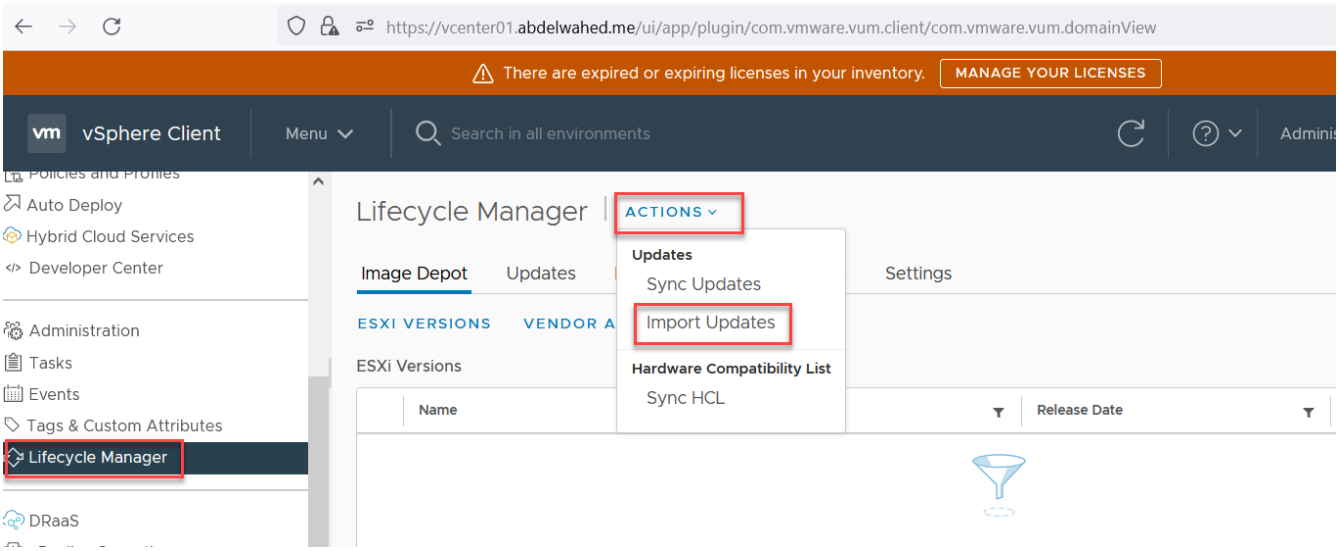
1. **Access vSphere Lifecycle Manager**:
   - Open the vSphere Client and navigate to the Lifecycle Manager interface.
2. **Create Baselines**:
   - Define baselines for host configurations and software updates.
   - Baselines can include patches, updates, and configurations needed for compliance.
3. **Attach Baselines to Hosts**:
   - Select individual hosts or groups of hosts to apply baselines.
   - Ensure that hosts are evaluated against the baselines to identify non-compliance.
4. **Update and Patch Hosts**:
   - Use the Lifecycle Manager to apply updates and patches to ESXi hosts.
   - Schedule updates to minimize disruption to operations.
5. **Monitor Compliance**:
   - Regularly check host compliance with defined baselines.
   - Address any compliance issues by applying necessary updates and configurations.
6. **Manage Hardware Components**:
   - View detailed information on host hardware components.
   - Update firmware and drivers to maintain compatibility and performance.

Benefits

- **Improved Efficiency**: Streamlines the process of managing ESXi host lifecycles from a central location.
- **Enhanced Compliance**: Helps ensure hosts meet security and regulatory standards.
- **Better Visibility**: Provides detailed insights into hardware and software components, aiding in proactive management.

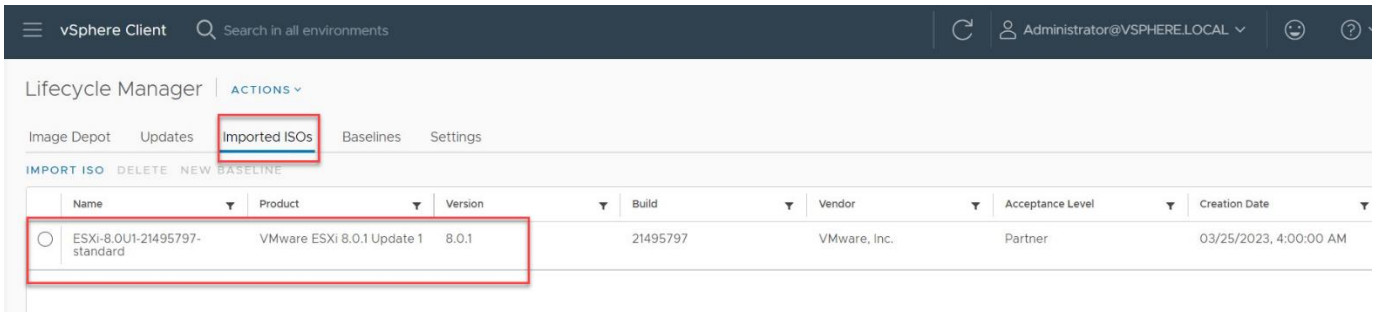
Best Practices

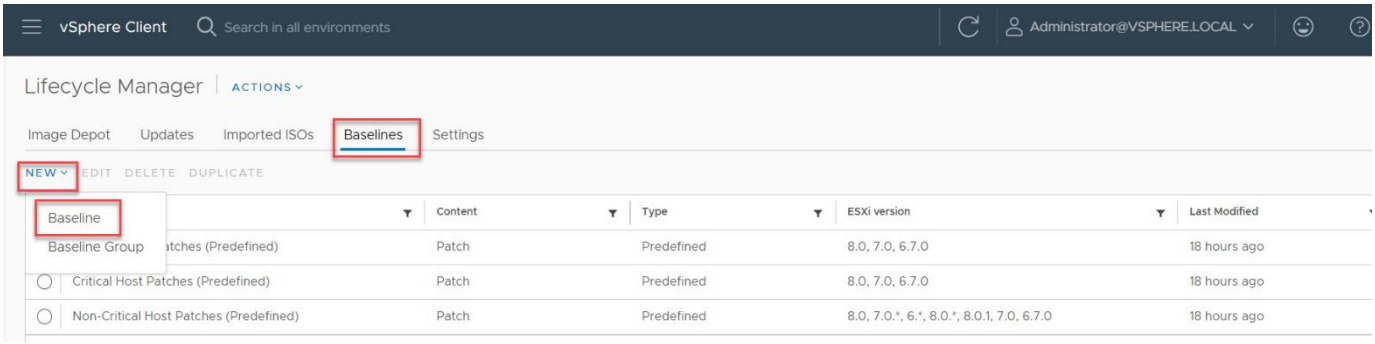
- **Regular Updates**: Frequently update baselines and apply patches to keep hosts secure and up-to-date.
- **Compliance Monitoring**: Continuously monitor host compliance to avoid potential security and regulatory issues.
- **Proactive Management**: Use the hardware and software management features to proactively address potential issues before they impact operations.

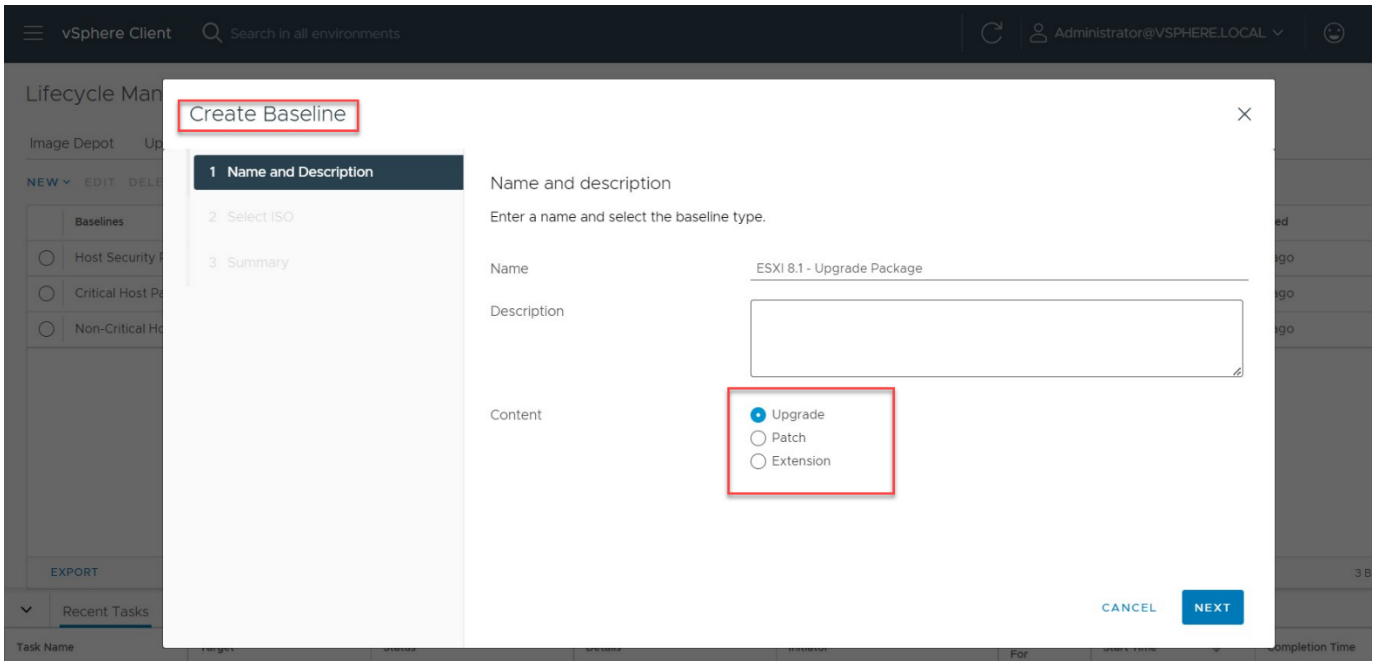


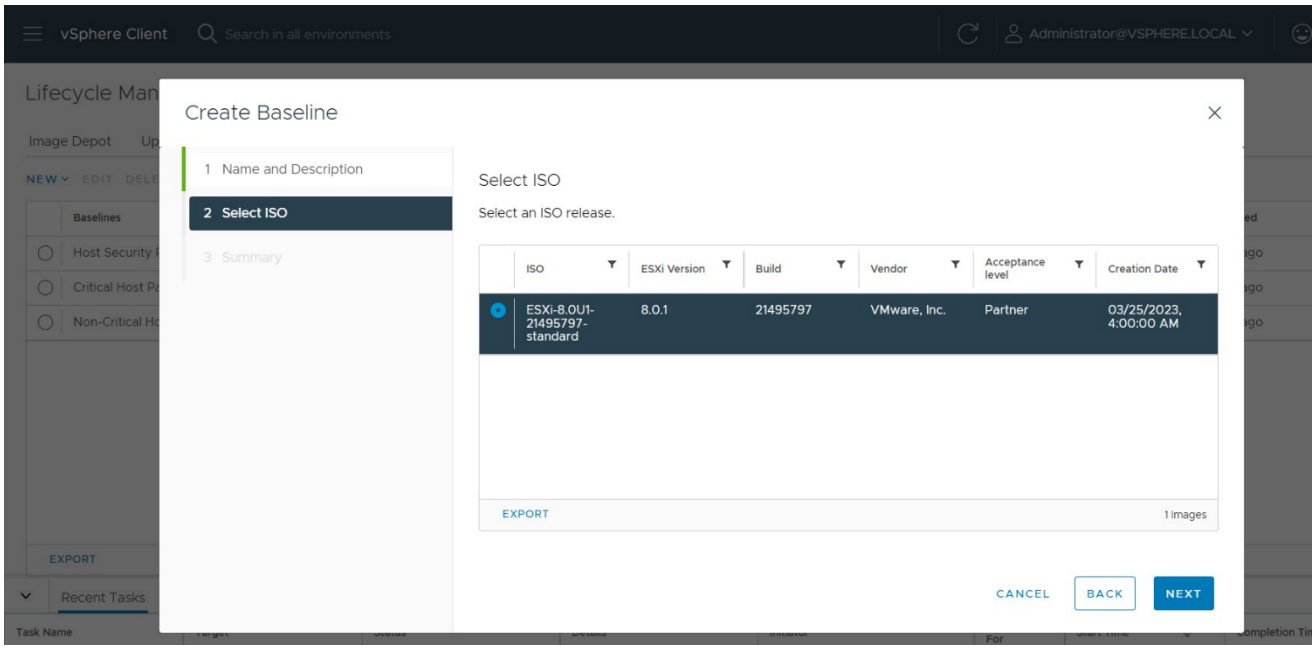
Upgrading ESXi Hosts Using VMware vSphere Lifecycle Manager

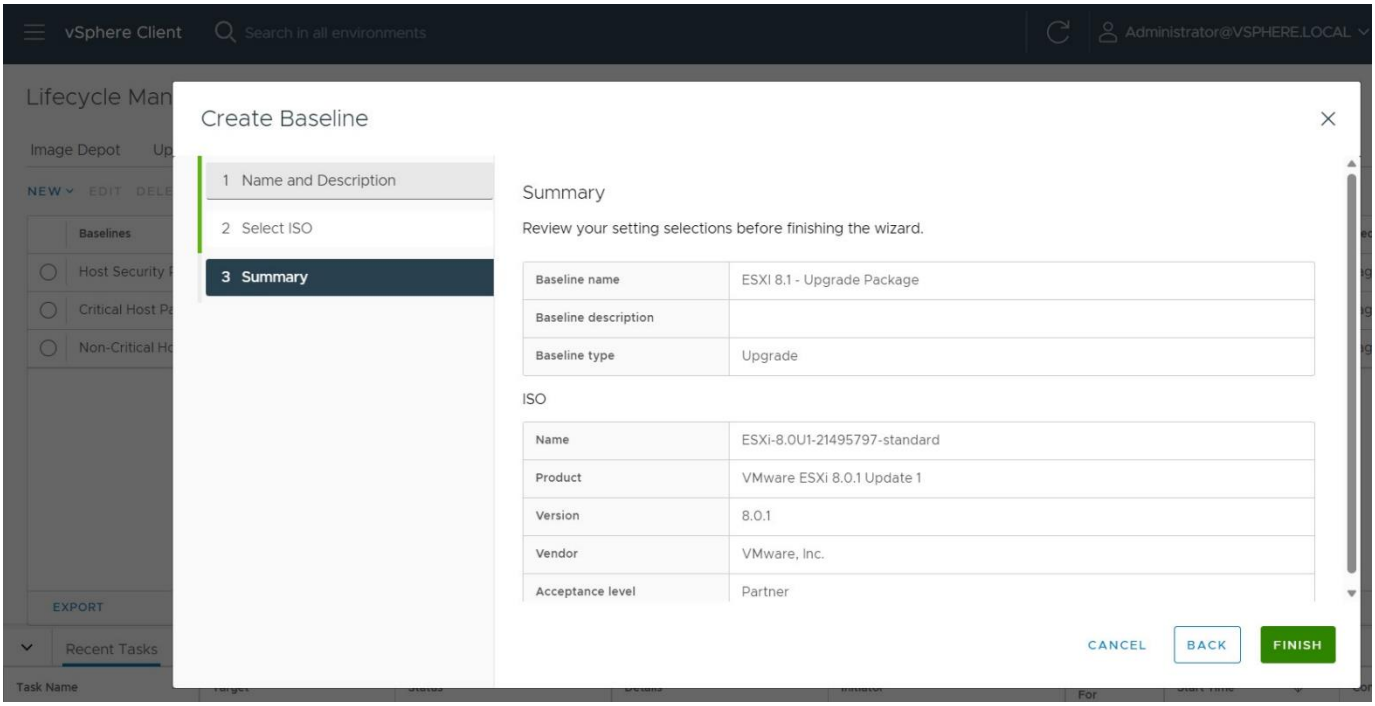
Steps to Upgrade ESXi Hosts



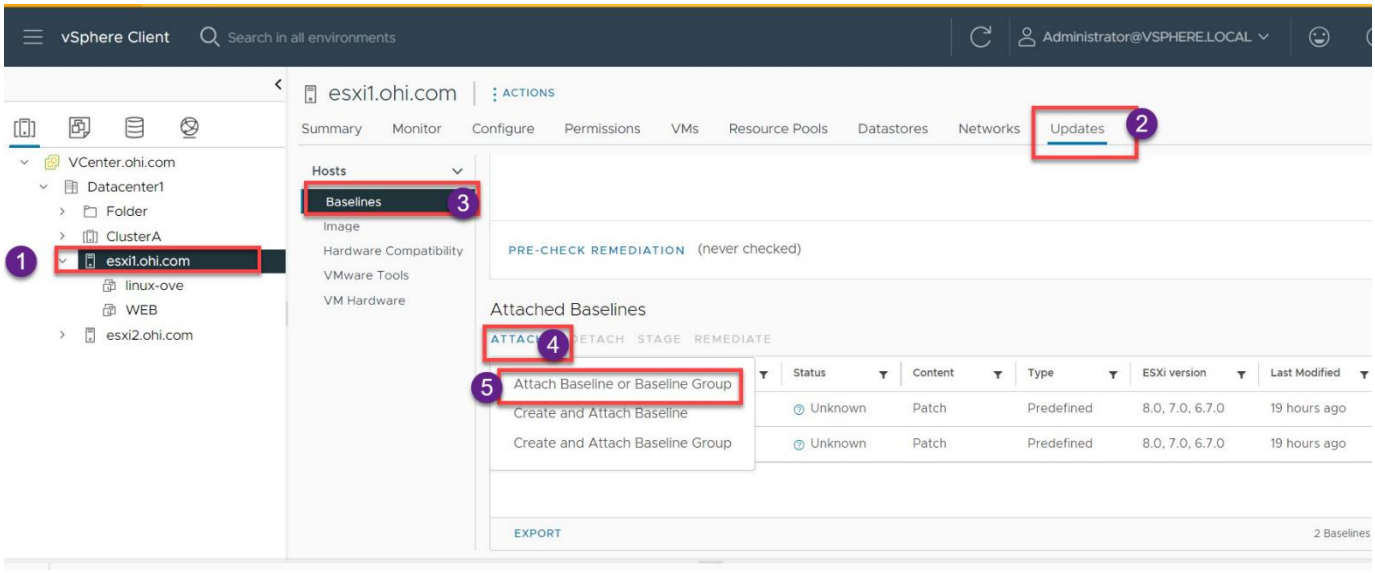


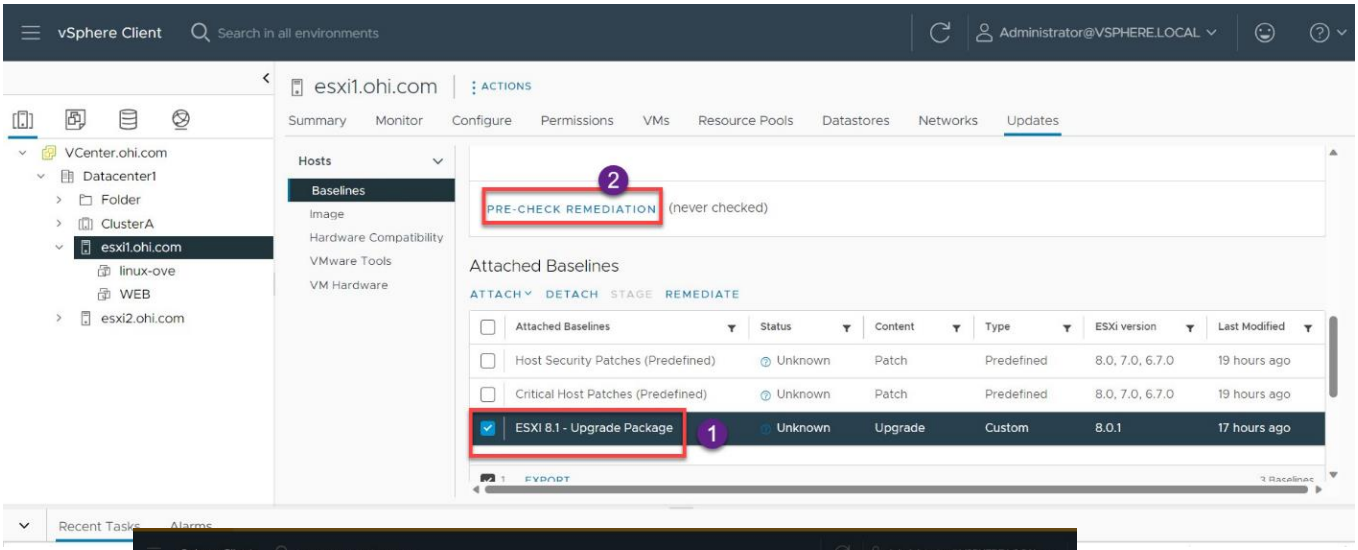


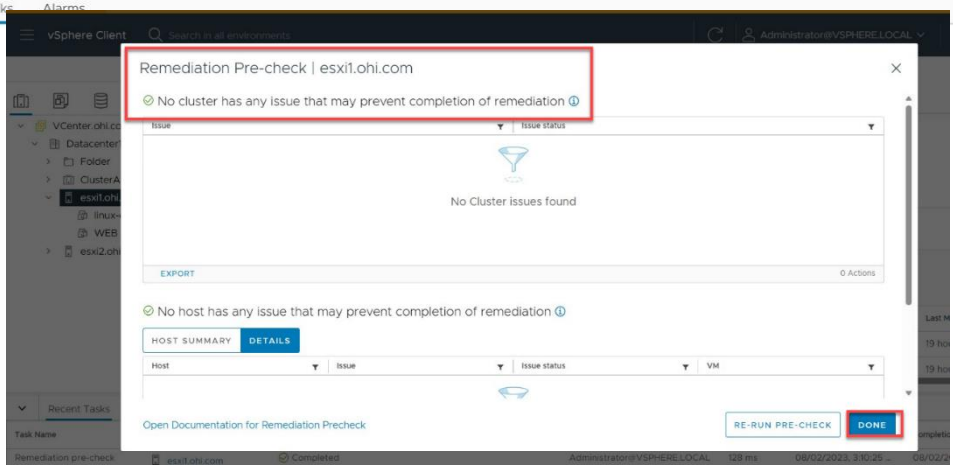

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
Create Baseline
1 Name and Description
2 Select ISO
3 Summary
Select ISO
Select an ISO release.
ISO
ESXi Version
Build
Vendor
Acceptance level
Creation Date
ESXi-8.0U1-21495797-standard
8.0.1
21495797
VMware, Inc.
Partner
03/25/2023, 4:00:00 AM
EXPORT
1 images
CANCEL
BACK
NEXT


vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
Create Baseline
1 Name and Description
2 Select ISO
3 Summary
Summary
Review your setting selections before finishing the wizard.
Baseline name
ESXI 8.1 - Upgrade Package
Baseline description
Baseline type
Upgrade
ISO
Name
ESXi-8.0U1-21495797-standard
Product
VMware ESXi 8.0.1 Update 1
Version
8.0.1
Vendor
VMware, Inc.
Acceptance level
Partner
CANCEL
BACK
FINISH

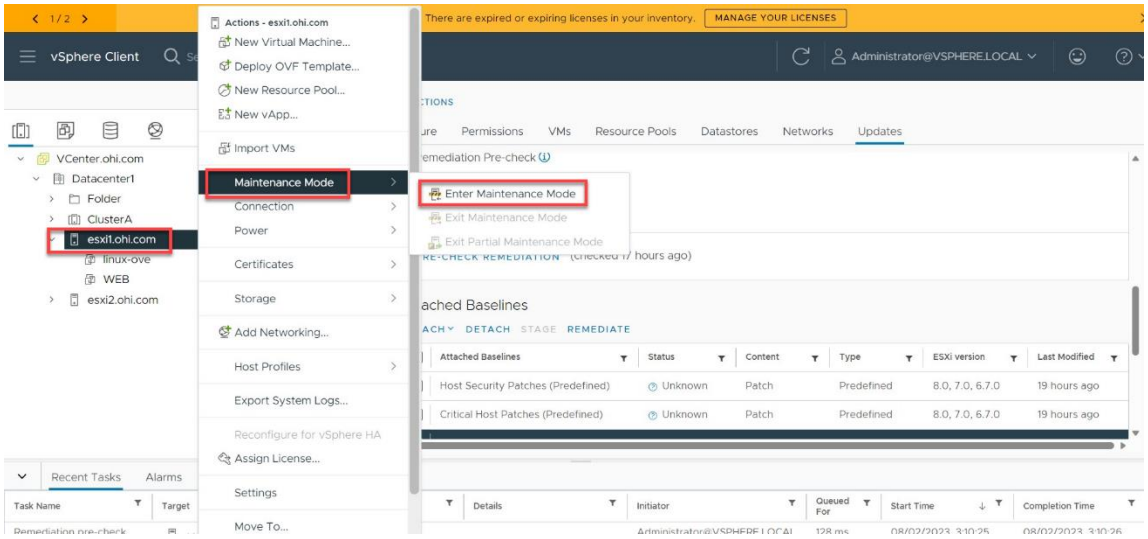
From the ESXi Perspective

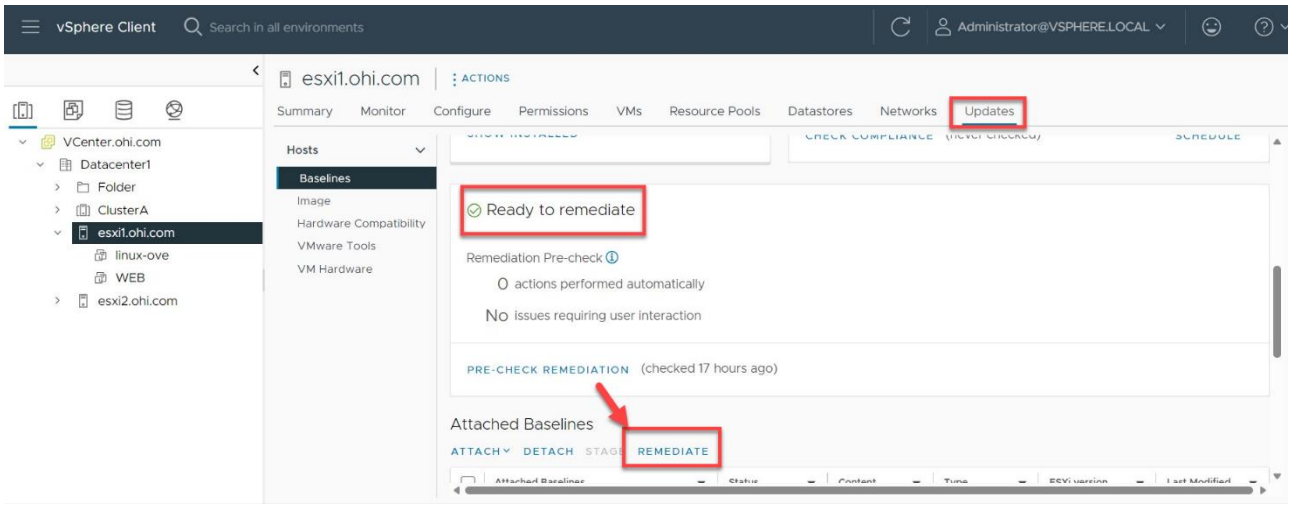


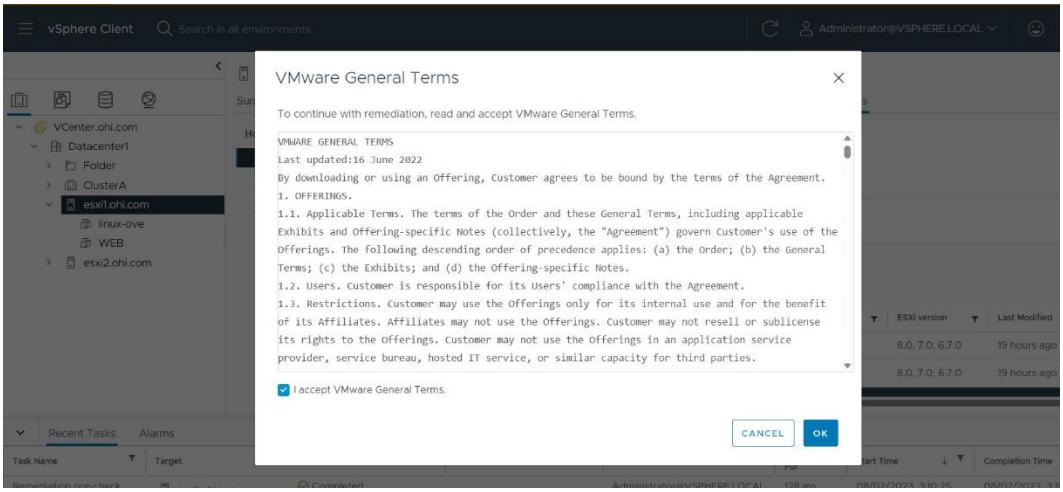




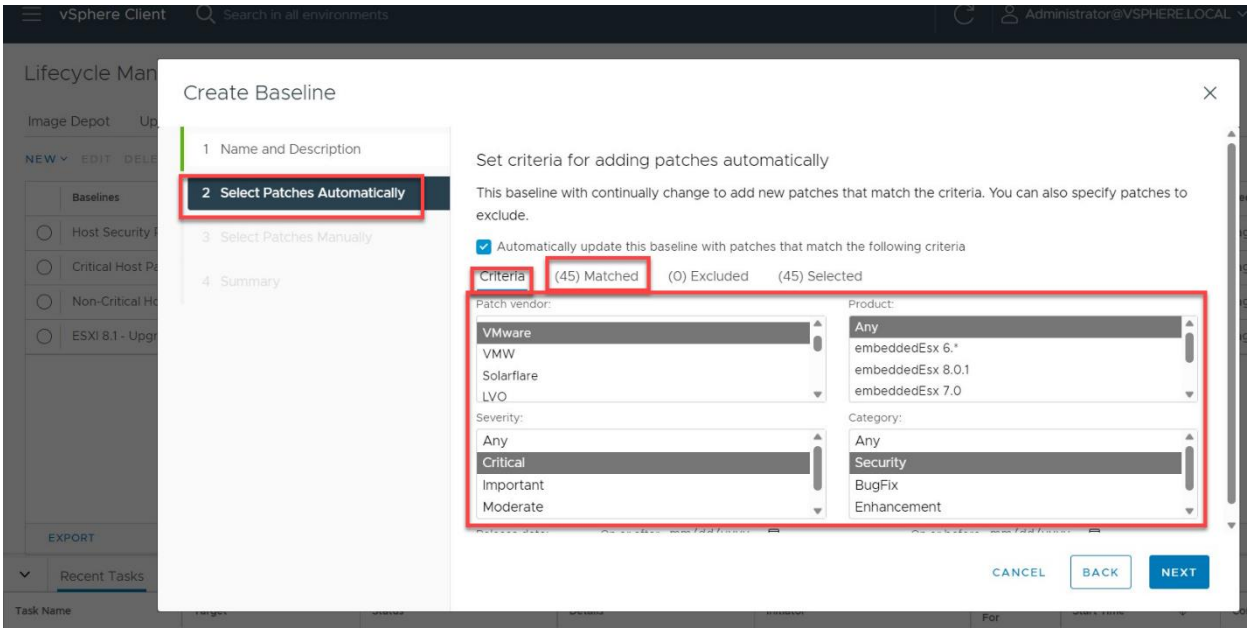
VMware vSphere Install, Configure, Manage | Lab Guide

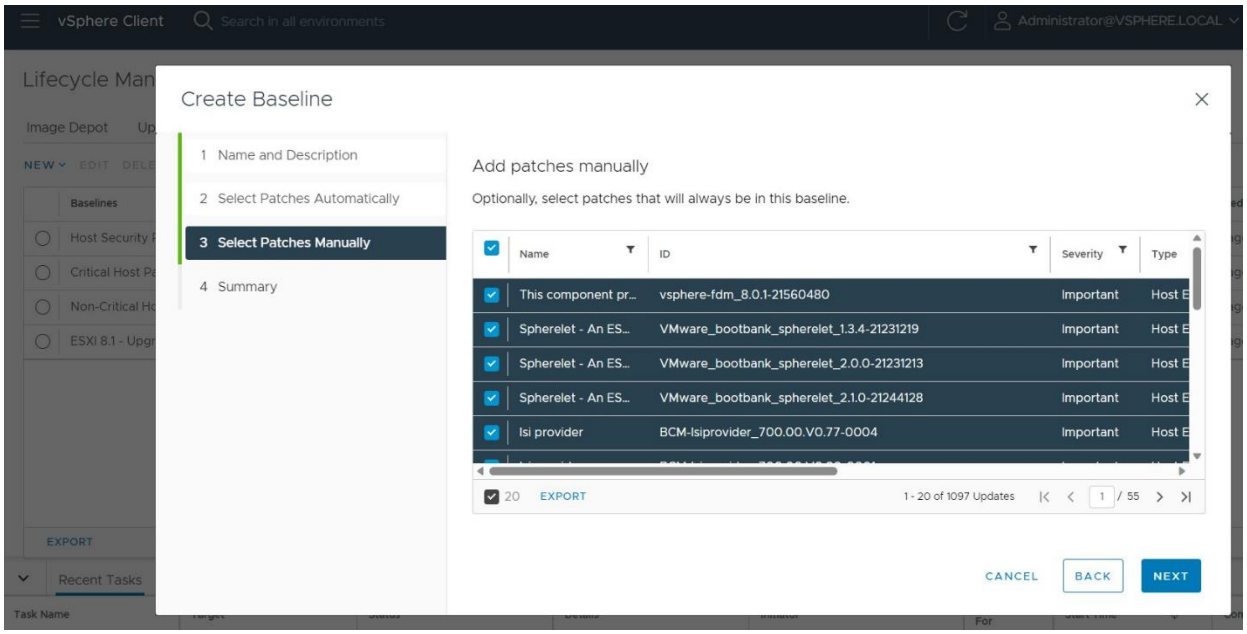


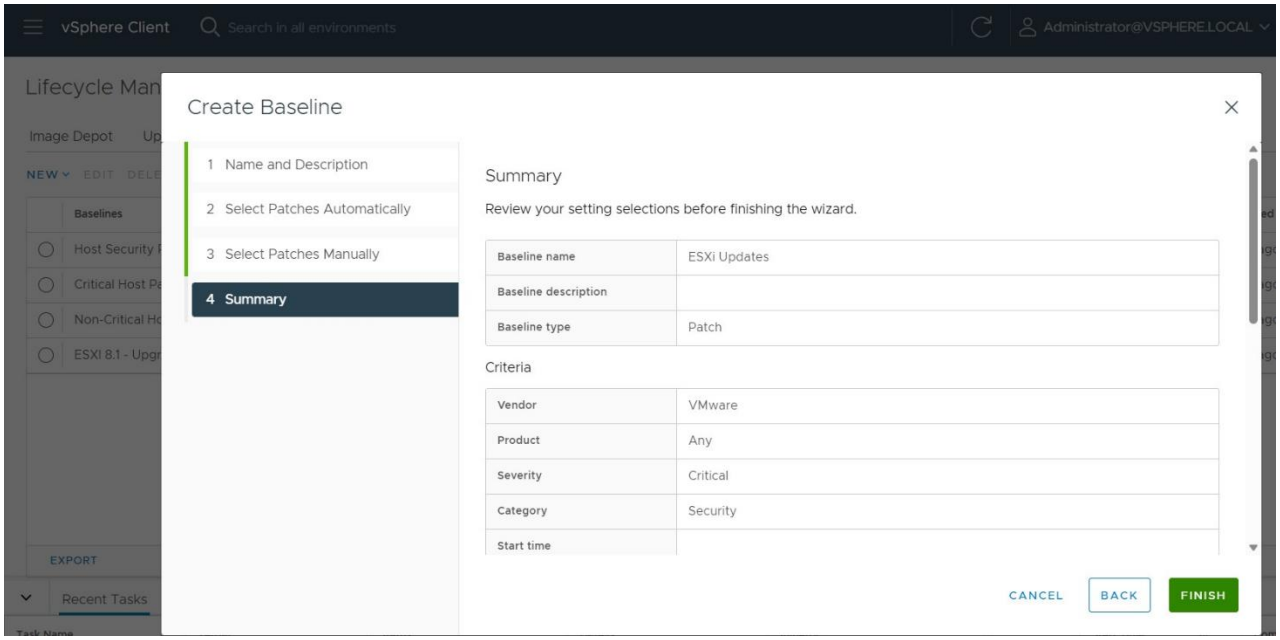


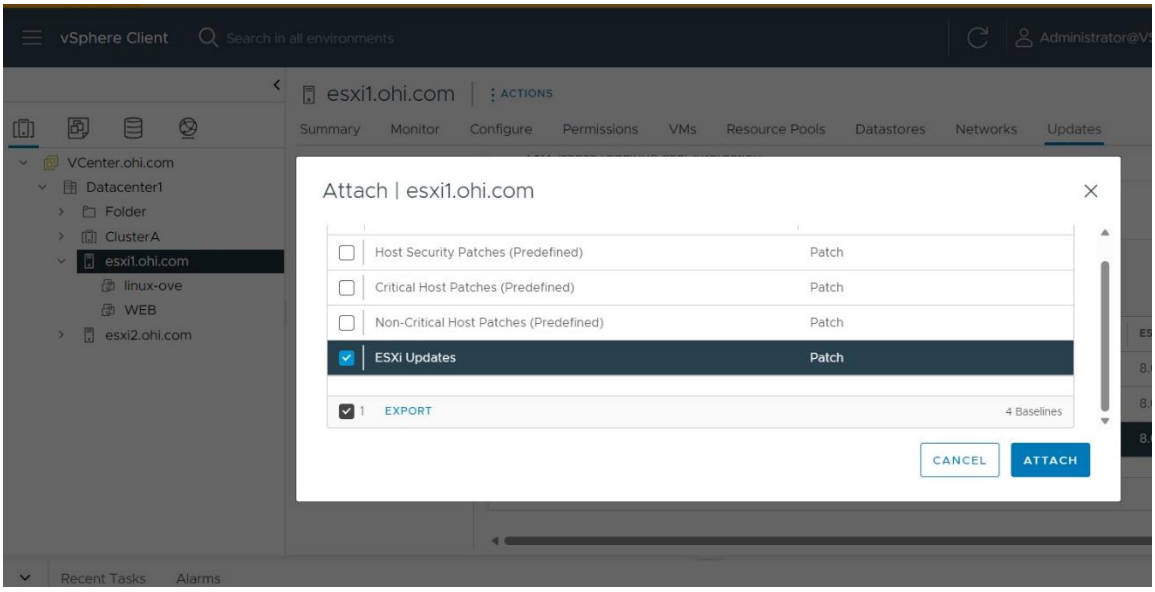


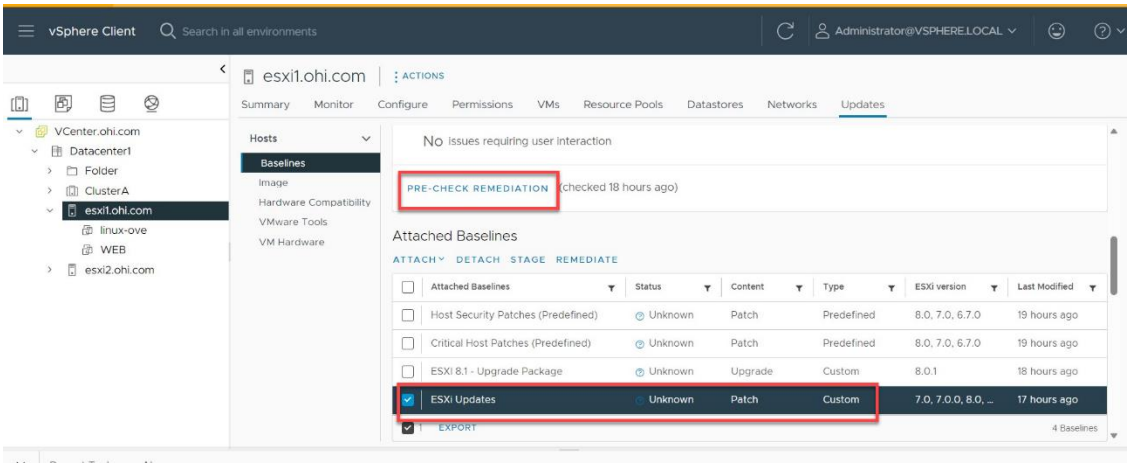
Establish and attach a new baseline for updates.

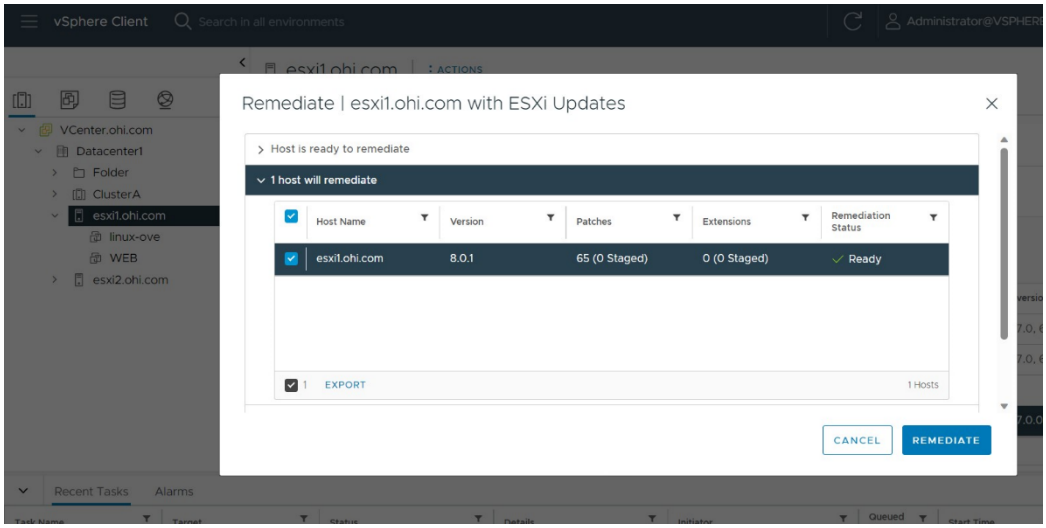




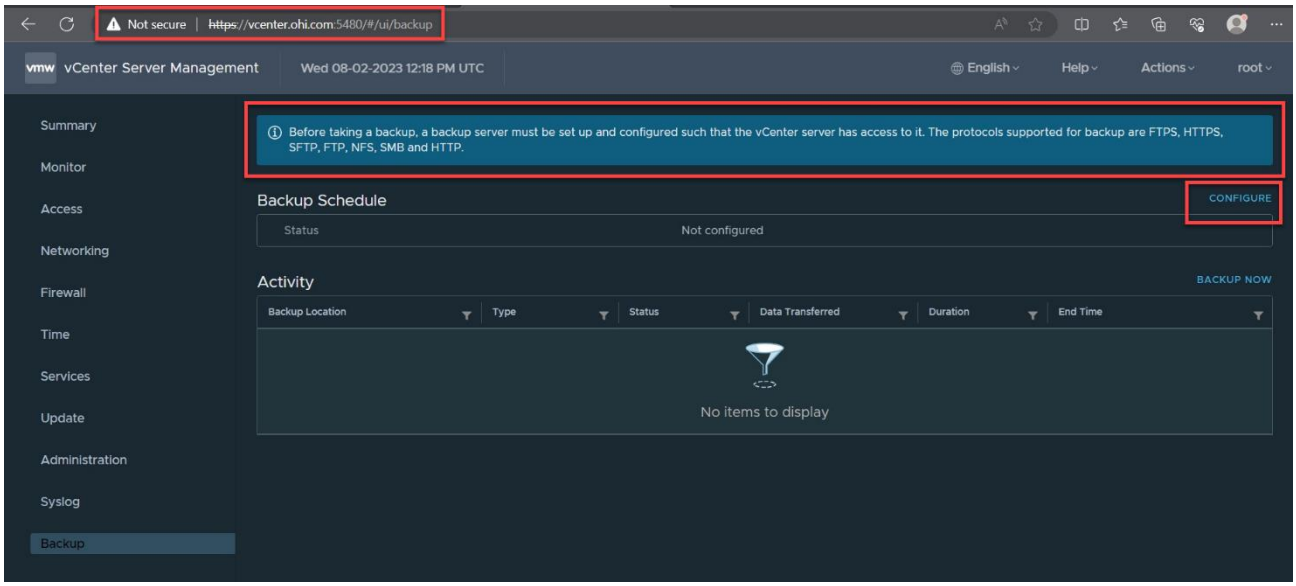

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
Create Baseline
1 Name and Description
2 Select Patches Automatically
3 Select Patches Manually
4 Summary
Summary
Review your setting selections before finishing the wizard.
Baseline name
ESXi Updates
Baseline description
Baseline type
Patch
Criteria
Vendor
VMware
Product
Any
Severity
Critical
Category
Security
Start time
CANCEL
BACK
FINISH

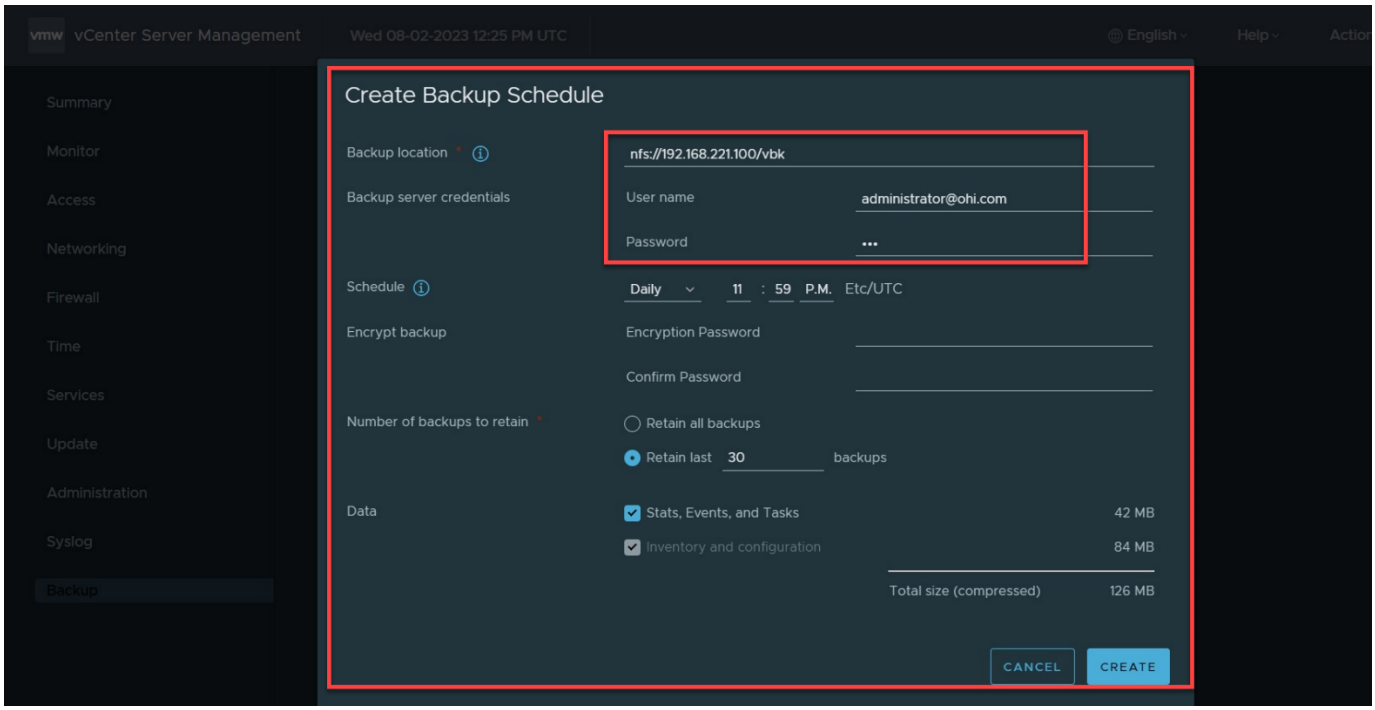

vSphere Client
Search in all environments
esxi1.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
VCenter.ohi.com
Datacenter1
Folder
ClusterA
esxi1.ohi.com
linux-ove
WEB
esxi2.ohi.com
Attach | esxi1.ohi.com
Host Security Patches (Predefined)
Patch
Critical Host Patches (Predefined)
Patch
Non-Critical Host Patches (Predefined)
Patch
ESXi Updates
Patch
EXPORT
4 Baselines
CANCEL
ATTACH
Recent Tasks
Alarms

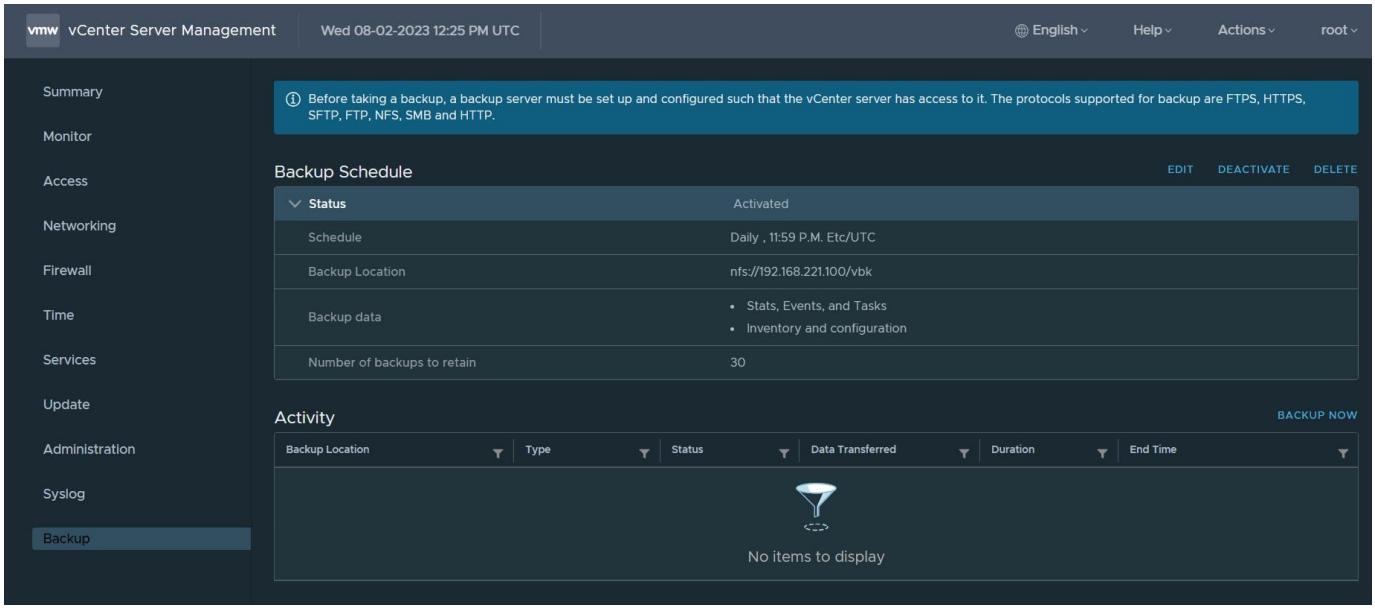

vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
esxi1.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
VCenter.ohi.com
Datacenter1
Folder
ClusterA
esxi1.ohi.com
linux-ove
WEB
esxi2.ohi.com
Hosts
Baselines
Image
Hardware Compatibility
VMware Tools
VM Hardware
No issues requiring user interaction
PRE-CHECK REMEDIATION
(checked 18 hours ago)
Attached Baselines
ATTACH
DETACH
STAGE
REMEDIATE
Attached Baselines
Status
Content
Type
ESXi version
Last Modified
Host Security Patches (Predefined)
Unknown
Patch
Predefined
8.0, 7.0, 6.7.0
19 hours ago
Critical Host Patches (Predefined)
Unknown
Patch
Predefined
8.0, 7.0, 6.7.0
19 hours ago
ESXi 8.1 - Upgrade Package
Unknown
Upgrade
Custom
8.0.1
18 hours ago
ESXi Updates
Unknown
Patch
Custom
7.0, 7.0.0, 8.0, ...
17 hours ago
EXPORT
4 Baselines

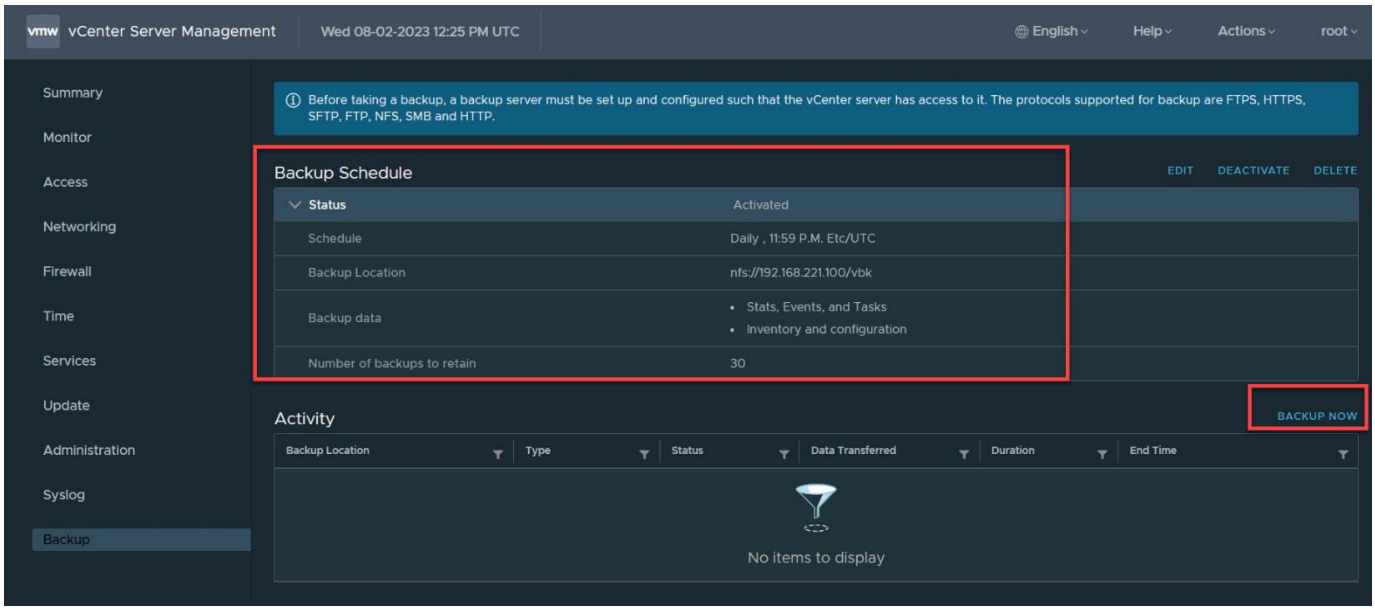

vSphere Client
Search in all environments
Remediate | esxi1.ohi.com with ESXi Updates
Host is ready to remediate
1 host will remediate
Host Name
Version
Patches
Extensions
Remediation Status
esxi1.ohi.com
8.0.1
65 (0 Staged)
0 (0 Staged)
Ready
EXPORT
1 Hosts
CANCEL
REMEDIATE
Recent Tasks
Alarms

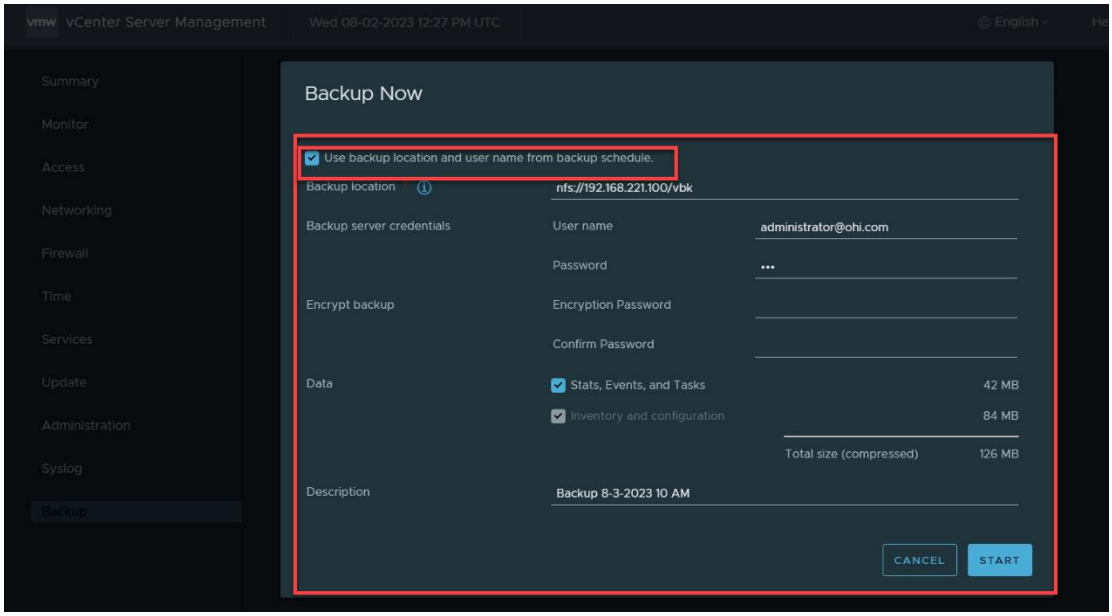
Backup and Restore vCenter Server

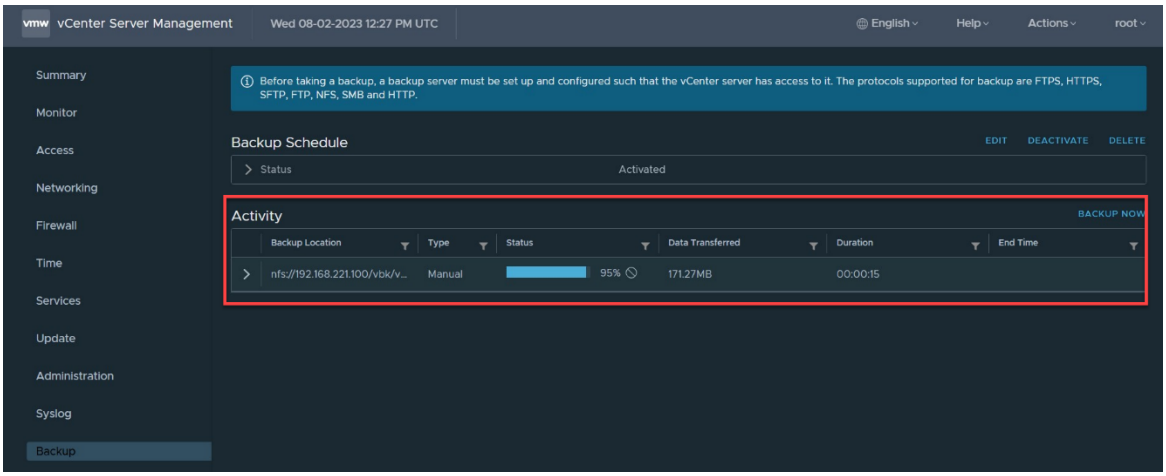


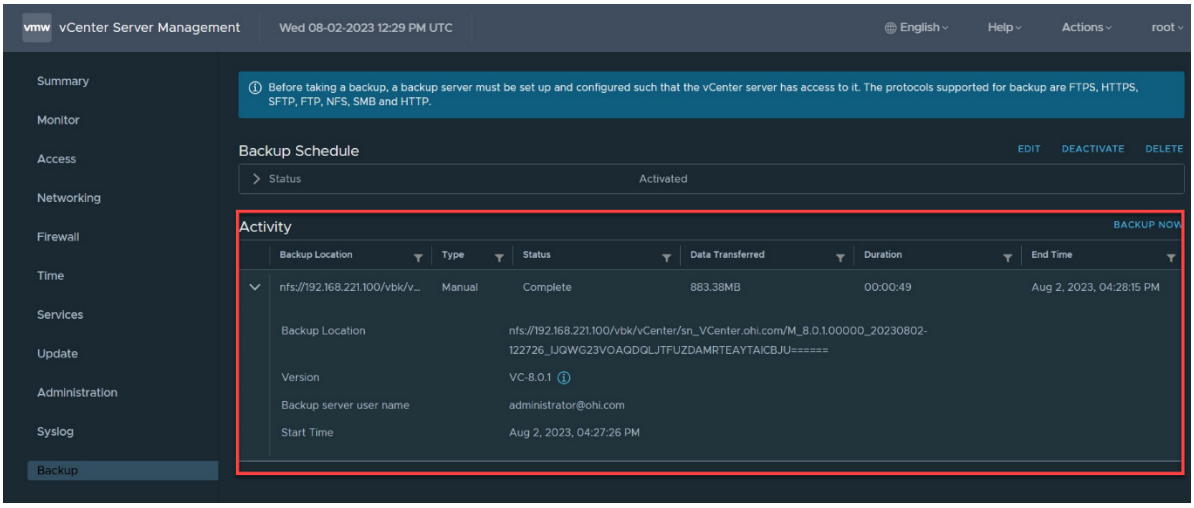



vCenter Server Management
Wed 08-02-2023 12:25 PM UTC
English
Help
Actions
root
Summary
Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup
Before taking a backup, a backup server must be set up and configured such that the vCenter server has access to it. The protocols supported for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB and HTTP.
Backup Schedule
EDIT
DEACTIVATE
DELETE
Status
Activated
Schedule
Daily , 11:59 P.M. Etc/UTC
Backup Location
nfs://192.168.221.100/vbk
Backup data
Stats, Events, and Tasks
Inventory and configuration
Number of backups to retain
30
Activity
BACKUP NOW
Backup Location
Type
Status
Data Transferred
Duration
End Time
No items to display

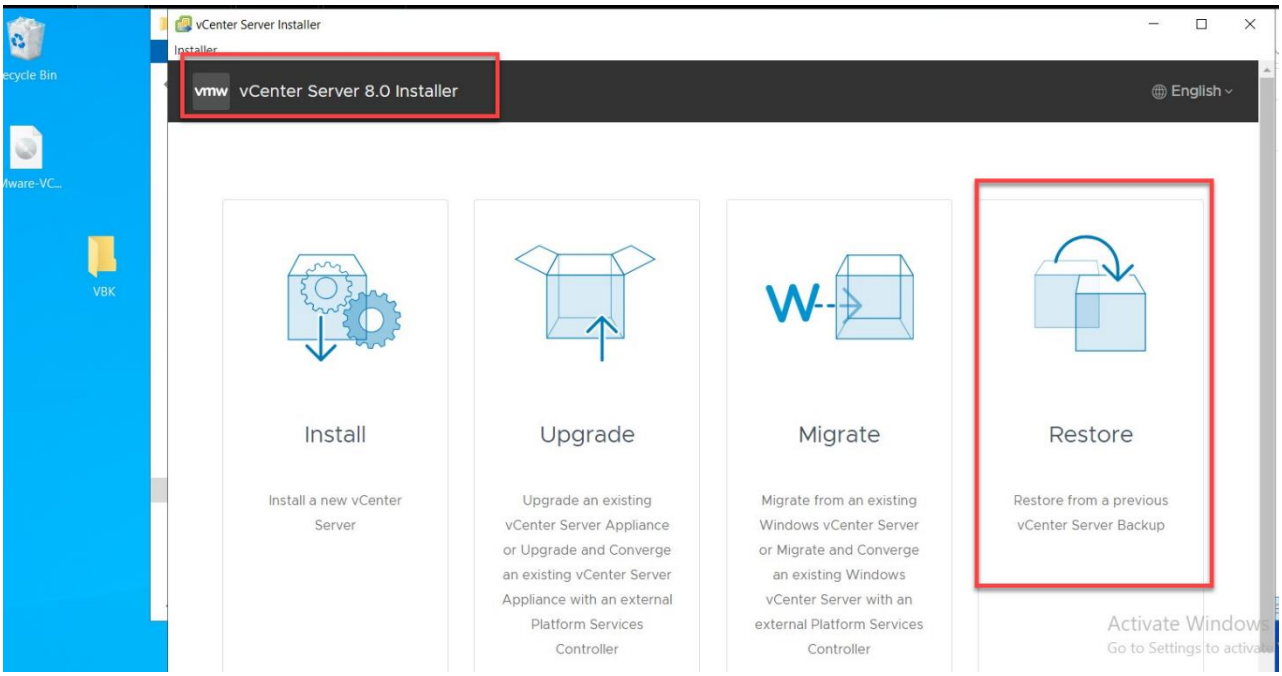

vCenter Server Management
Wed 08-02-2023 12:25 PM UTC
English
Help
Actions
root
Summary
Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup
Before taking a backup, a backup server must be set up and configured such that the vCenter server has access to it. The protocols supported for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB and HTTP.
Backup Schedule
EDIT
DEACTIVATE
DELETE
Status
Activated
Schedule
Daily , 11:59 P.M. Etc/UTC
Backup Location
nfs://192.168.221.100/vbk
Backup data
Stats, Events, and Tasks
Inventory and configuration
Number of backups to retain
30
Activity
BACKUP NOW
Backup Location
Type
Status
Data Transferred
Duration
End Time
No items to display

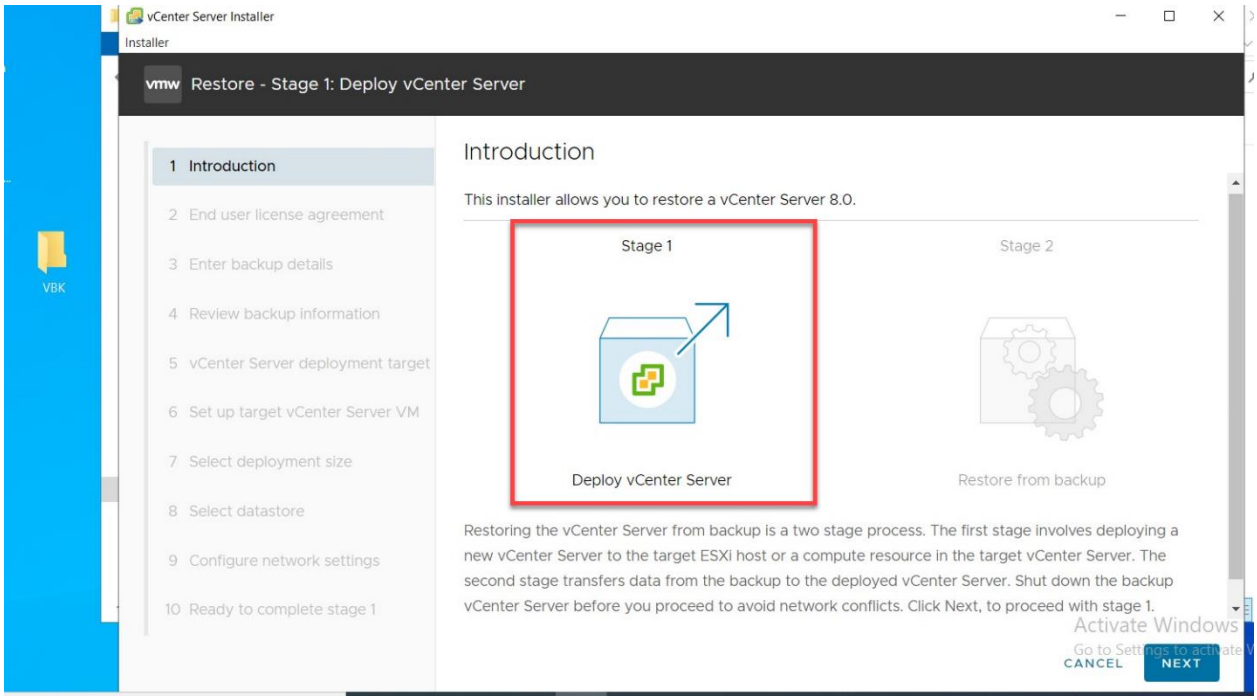

vCenter Server Management
Wed 08-02-2023 12:27 PM UTC
English
Summary
Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup
Backup Now
Use backup location and user name from backup schedule.
Backup location
nfs://192.168.221.100/vbk
Backup server credentials
User name
administrator@ohi.com
Password
Encrypt backup
Encryption Password
Confirm Password
Data
Stats, Events, and Tasks
42 MB
Inventory and configuration
84 MB
Total size (compressed)
126 MB
Description
Backup 8-3-2023 10 AM
CANCEL
START

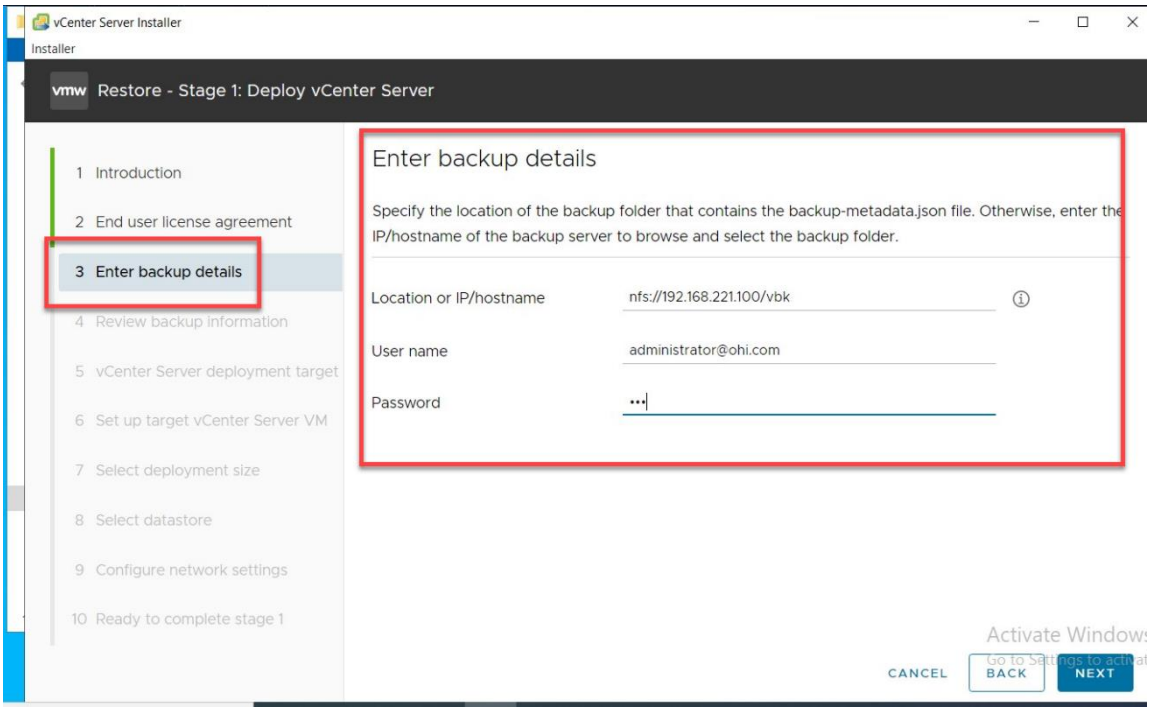

vCenter Server Management
Wed 08-02-2023 12:27 PM UTC
English
Help
Actions
root
Summary
Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup
Before taking a backup, a backup server must be set up and configured such that the vCenter server has access to it. The protocols supported for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB and HTTP.
Backup Schedule
EDIT
DEACTIVATE
DELETE
Status
Activated
Activity
BACKUP NOW
Backup Location
Type
Status
Data Transferred
Duration
End Time
nfs://192.168.221.100/vbk/v...
Manual
95%
171.27MB
00:00:15

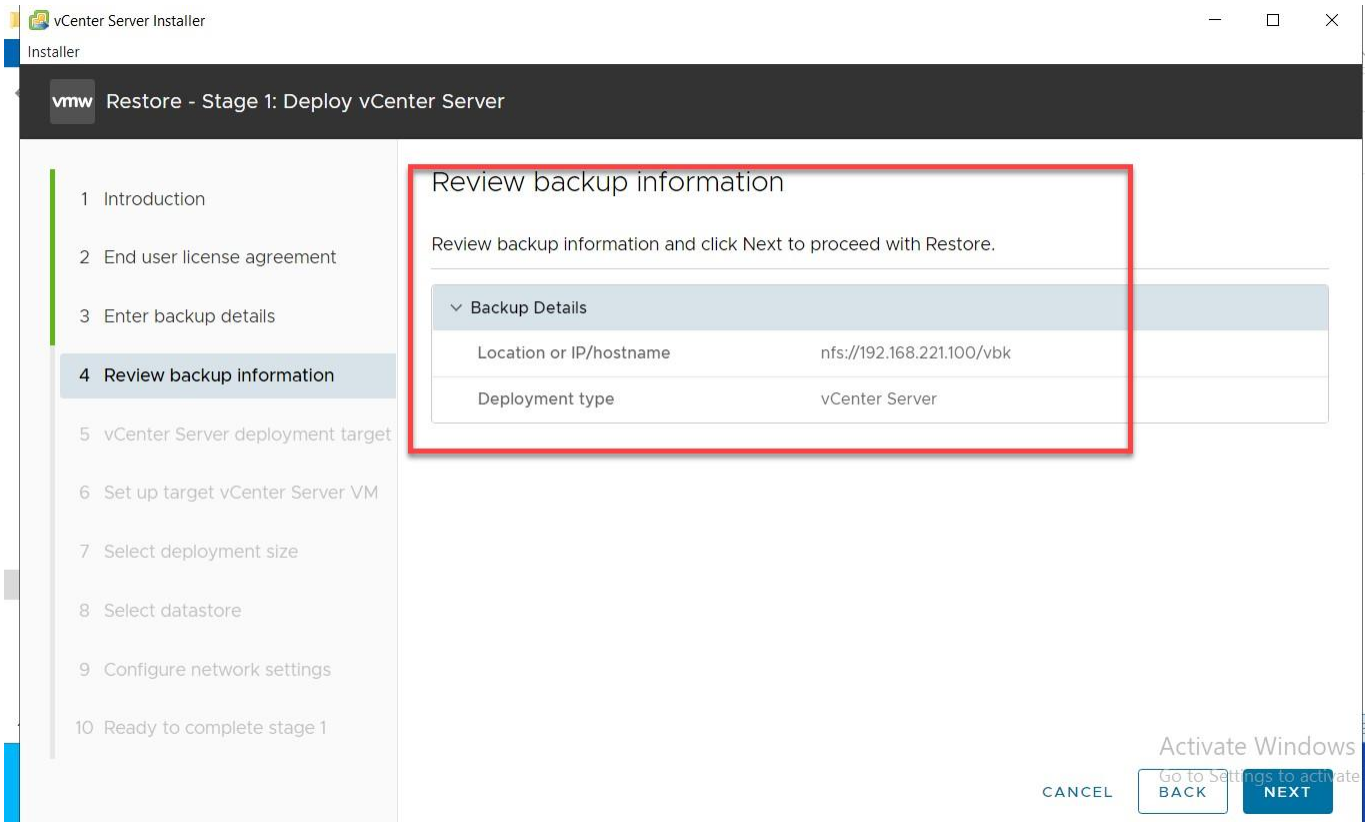


Restore using vCenter setup media.

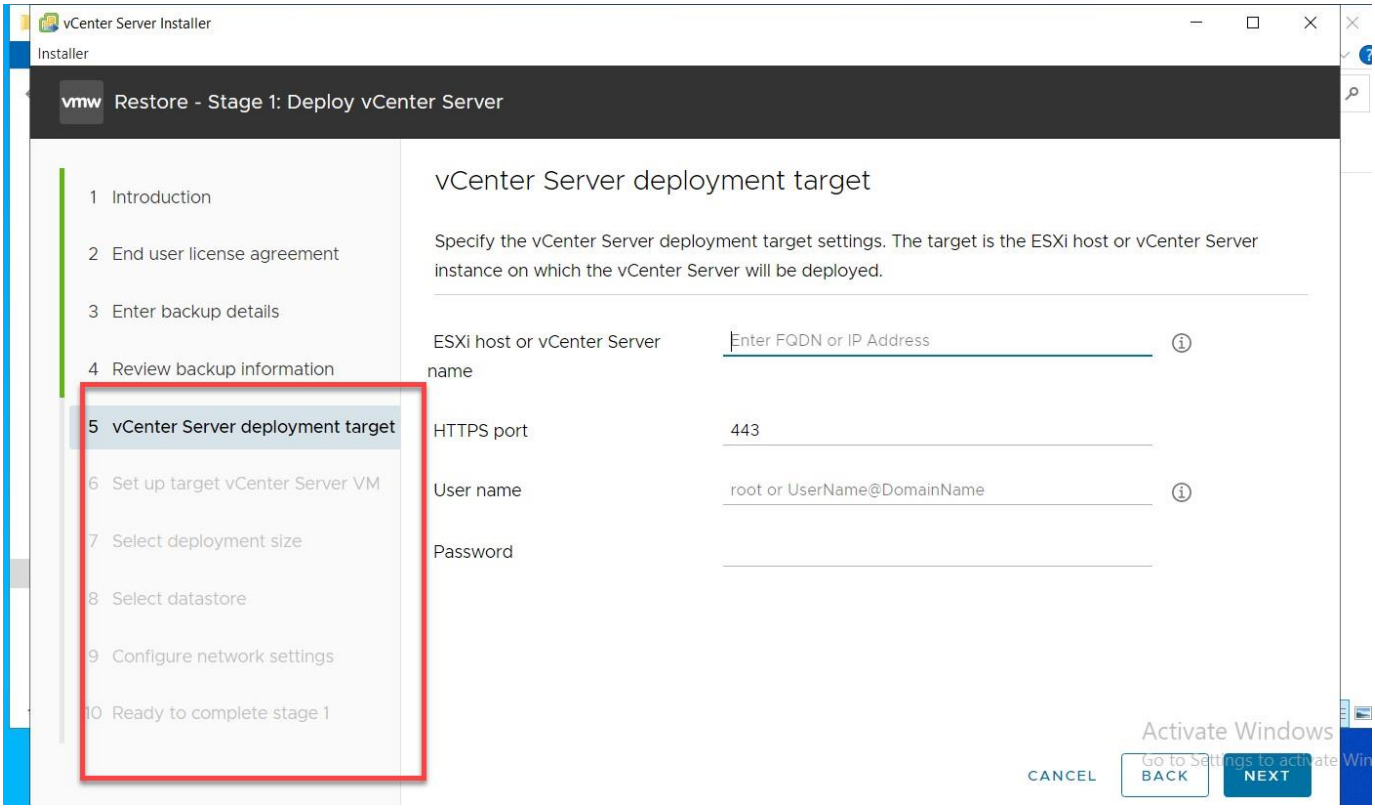



vCenter Server Installer
Installer
Restore - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 Enter backup details
4 Review backup information
5 vCenter Server deployment target
6 Set up target vCenter Server VM
7 Select deployment size
8 Select datastore
9 Configure network settings
10 Ready to complete stage 1
Introduction
This installer allows you to restore a vCenter Server 8.0.
Stage 1
Deploy vCenter Server
Stage 2
Restore from backup
Restoring the vCenter Server from backup is a two stage process. The first stage involves deploying a new vCenter Server to the target ESXi host or a compute resource in the target vCenter Server. The second stage transfers data from the backup to the deployed vCenter Server. Shut down the backup vCenter Server before you proceed to avoid network conflicts. Click Next, to proceed with stage 1.
CANCEL
NEXT

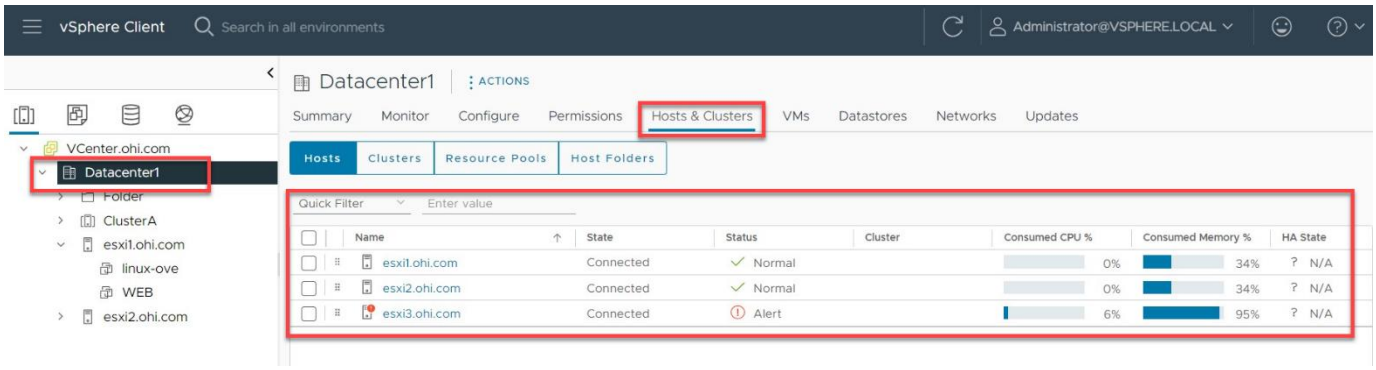

vCenter Server Installer
Installer
Restore - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 Enter backup details
4 Review backup information
5 vCenter Server deployment target
6 Set up target vCenter Server VM
7 Select deployment size
8 Select datastore
9 Configure network settings
10 Ready to complete stage 1
Enter backup details
Specify the location of the backup folder that contains the backup-metadata.json file. Otherwise, enter the IP/hostname of the backup server to browse and select the backup folder.
Location or IP/hostname
nfs://192.168.221.100/vbk
User name
administrator@ohi.com
Password
CANCEL
BACK
NEXT


vCenter Server Installer
Installer
vmw Restore - Stage 1: Deploy vCenter Server
1 Introduction
2 End user license agreement
3 Enter backup details
4 Review backup information
5 vCenter Server deployment target
6 Set up target vCenter Server VM
7 Select deployment size
8 Select datastore
9 Configure network settings
10 Ready to complete stage 1
Review backup information
Review backup information and click Next to proceed with Restore.
Backup Details
Location or IP/hostname
nfs://192.168.221.100/vbk
Deployment type
vCenter Server
Activate Windows
Go to Settings to activate.
CANCEL
BACK
NEXT

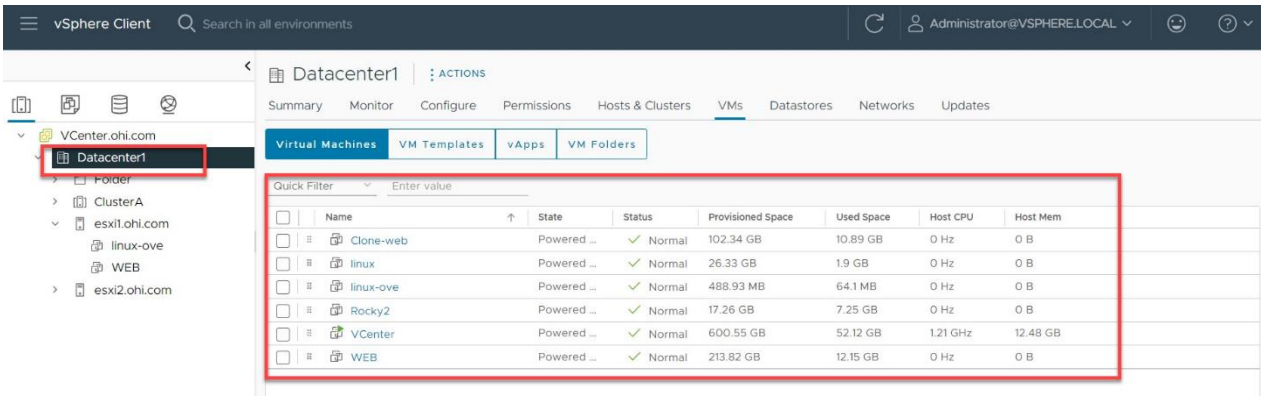
and complete the normal installation process.

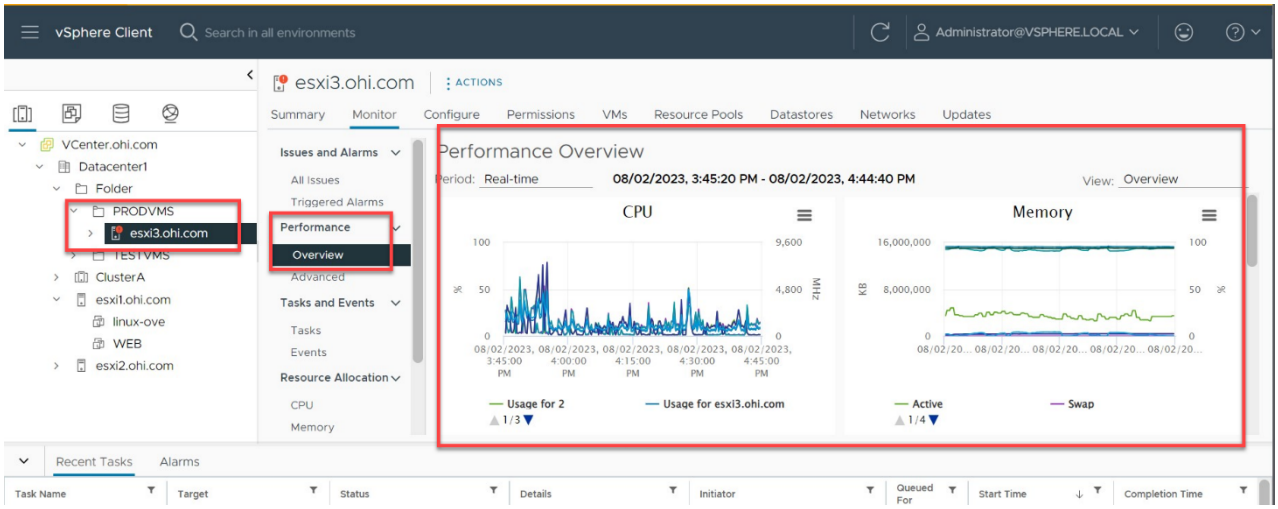


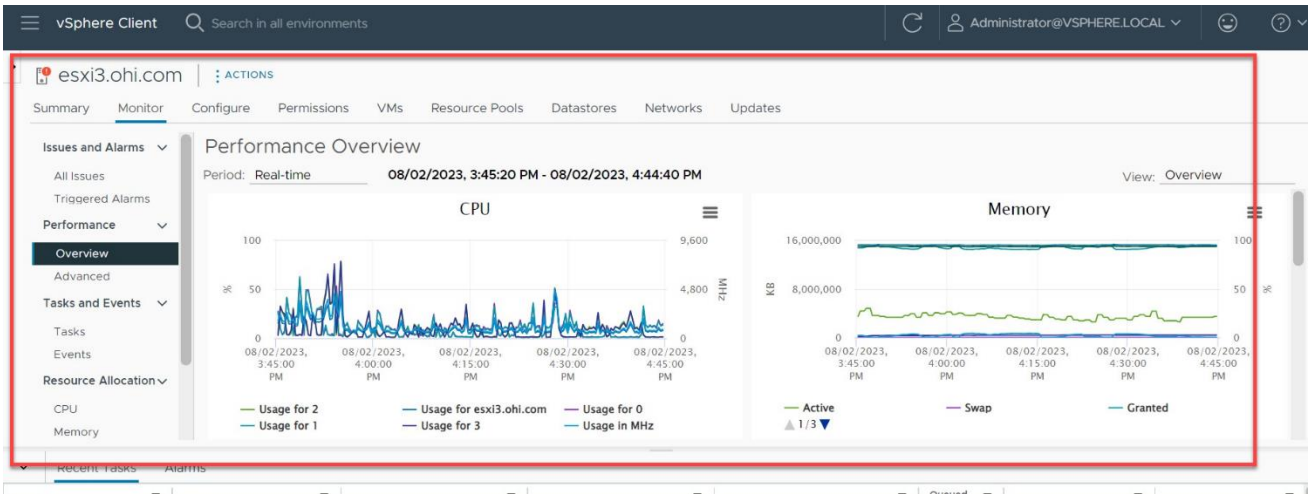
Performance Monitoring

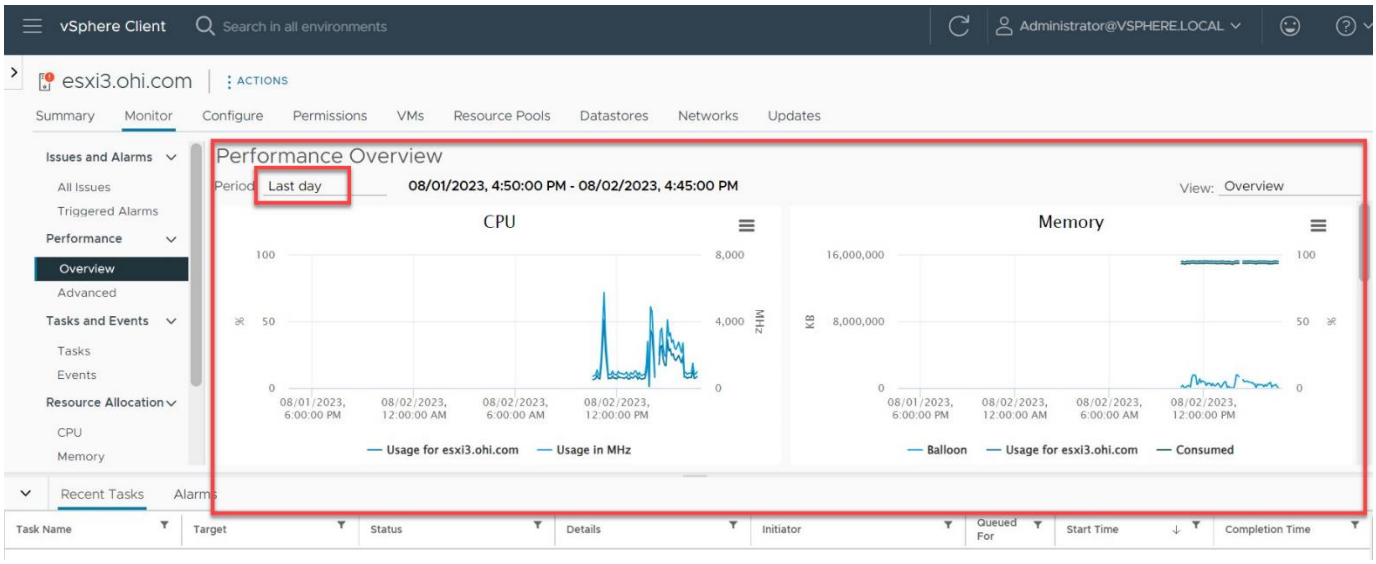


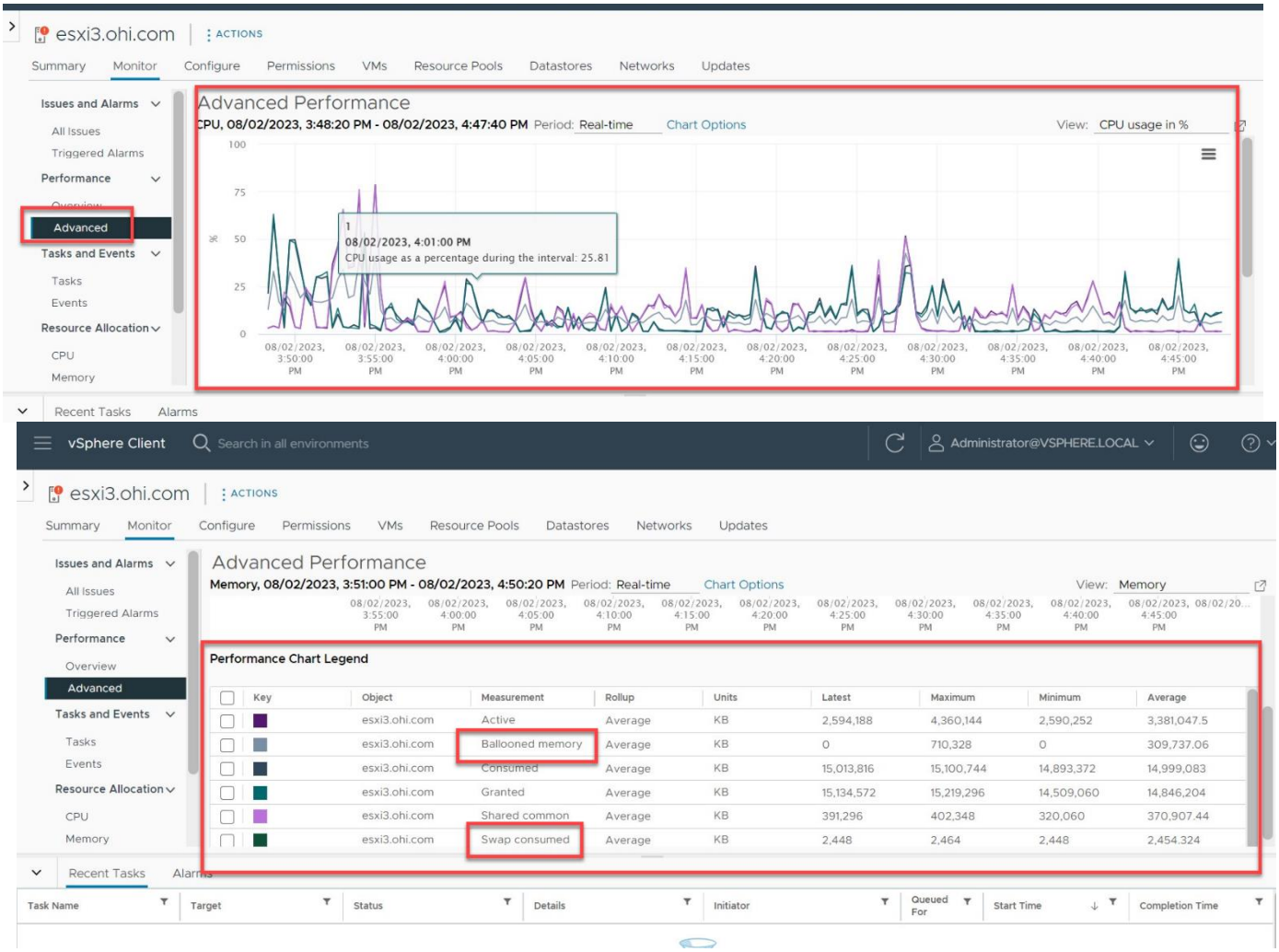
VMware vSphere Install, Configure, Manage | Lab Guide








vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
esxi3.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
Issues and Alarms
All Issues
Triggered Alarms
Performance
Overview
Advanced
Tasks and Events
Tasks
Events
Resource Allocation
CPU
Memory
Performance Overview
Period: Last day
08/01/2023, 4:50:00 PM - 08/02/2023, 4:45:00 PM
View: Overview
CPU
Memory
Usage for esxi3.ohi.com
Usage in MHz
Balloon
Usage for esxi3.ohi.com
Consumed
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
Completion Time


esxi3.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
Issues and Alarms
All Issues
Triggered Alarms
Performance
Advanced
Tasks and Events
Tasks
Events
Resource Allocation
CPU
Memory
Advanced Performance
CPU, 08/02/2023, 3:48:20 PM - 08/02/2023, 4:47:40 PM
Period: Real-time
Chart Options
View: CPU usage in %
08/02/2023, 4:01:00 PM
CPU usage as a percentage during the interval: 25.81
Recent Tasks
Alarms
vSphere Client
Search in all environments
Administrator@VSPHERE.LOCAL
esxi3.ohi.com
ACTIONS
Summary
Monitor
Configure
Permissions
VMs
Resource Pools
Datastores
Networks
Updates
Advanced Performance
Memory, 08/02/2023, 3:51:00 PM - 08/02/2023, 4:50:20 PM
Period: Real-time
Chart Options
View: Memory
Performance Chart Legend
Key
Object
Measurement
Rollup
Units
Latest
Maximum
Minimum
Average
esxi3.ohi.com Active Average KB 2,594,188 4,360,144 2,590,252 3,381,047.5
esxi3.ohi.com Ballooned memory Average KB 0 710,328 0 309,737.06
esxi3.ohi.com Consumed Average KB 15,013,816 15,100,744 14,893,372 14,999,083
esxi3.ohi.com Granted Average KB 15,134,572 15,219,296 14,509,060 14,846,204
esxi3.ohi.com Shared common Average KB 391,296 402,348 320,060 370,907.44
esxi3.ohi.com Swap consumed Average KB 2,448 2,464 2,448 2,454.324
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
Completion Time

Troubleshooting

Troubleshooting VMware vCenter can encompass a broad range of issues, as vCenter is a complex product with various components and dependencies. Here's a structured approach to troubleshooting vCenter:

1. Identify the Problem:

- **Symptoms**: Understand the specific issues being faced. Are there errors in the vCenter UI? Is vCenter unresponsive? Are there issues with specific functionalities like vMotion or provisioning VMs?

2. Check vCenter Server Status:

- **Services**: Ensure all necessary VMware services are running.
  - For Windows-based vCenter, check using the Services console.
  - For vCenter Server Appliance (VCSA), check using the VAMI interface or **service-control** command.
- **Logs**: Examine the vCenter logs for any errors or warnings. The logs can be found at:
  - Windows: **C:\ProgramData\VMware\vCenterServer\logs**
  - VCSA: **/var/log/vmware**

3. Database Issues:

- Check the health of the database. Ensure there's enough space and that the database service is running.
- Look for database connection errors in the logs.

4. Networking:

- **Connectivity**: Test the network connectivity to the vCenter server using tools like **ping** and **traceroute**.
- **Firewall**: Ensure required ports for vCenter are open and not blocked by a firewall.
- **DNS**: Confirm that DNS resolution is working for the vCenter server and ESXi hosts.

5. Authentication:

- **SSO (Single Sign-On)**: If there are authentication issues, check the status of the SSO service.
- **AD/LDAP**: If vCenter is integrated with Active Directory or another LDAP service, ensure it can connect and authenticate users.

6. Performance:

- If vCenter is slow or unresponsive, check CPU, memory, and disk utilization.
- Monitor database performance, especially if the database is external.

7. Licensing:

- Confirm that licenses haven't expired.
- Ensure there are no errors related to licensing in the logs.

8. Integration with Other Components:

- If you're using solutions integrated with vCenter (like NSX, vSAN, etc.), check their status and logs.

9. Backup and Recovery:

- If there's a critical failure, consider restoring from a backup.
- Always make backups before making significant changes or upgrades.

10. Reach Out to VMware Support:

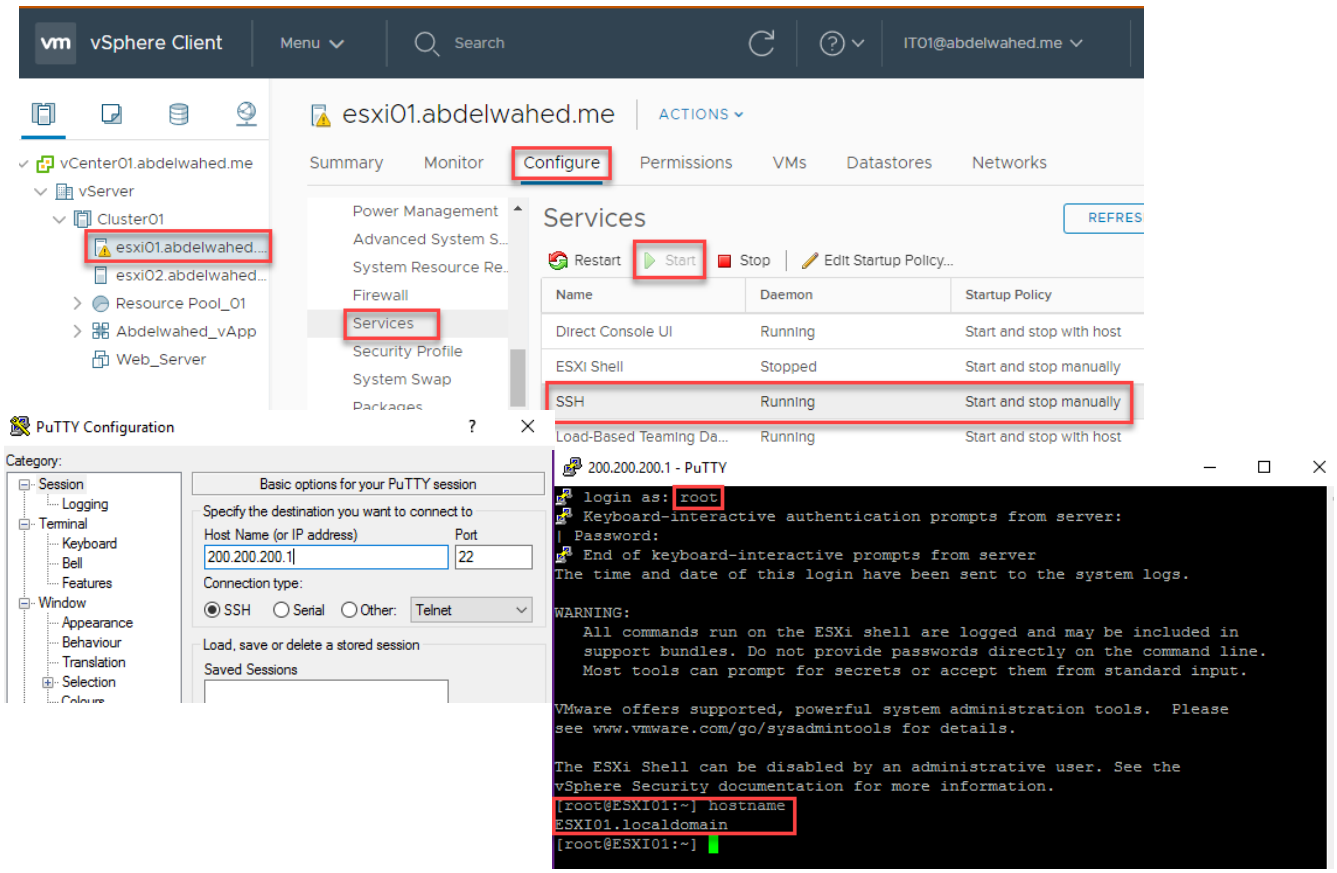
- If you can't identify the issue, consider creating a support bundle and contacting VMware support. The support bundle contains logs and configurations that can help VMware support diagnose the issue.

Services

Component	Service Name	Alias	Description	Default State
vCenter	vCenter Server	vpxd	Core service of vCenter, enabling VM provisioning, vMotion, DRS, etc.	Running
	VMware Directory Service	vmdir	Manages Single Sign-On (SSO) capabilities and security tokens.	Running
	VMware Content Library	content-library	Manages content libraries: containers for VM templates, vApp templates, etc.	Running
	vCenter Profile-Driven Storage Service	vpxd-profile	Manages VM storage profiles and associated policies (SPBM).	Running
	VMware vCenter Identity Services	vmware-stsd	Supports authentication services for VMware components.	Running
	VMware vSphere Update Manager	vmware-updatemgr	Automates tracking, patching, and updating VMs, appliances, and ESXi hosts.	Running
	VMware Certificate Authority	vmcad	Manages certificates for vCenter services ensuring secure communication.	Running
	vSphere Lifecycle Manager (v7 and later)	vLCM	Streamlines ESXi host lifecycle management.	Running
ESXi	Hostd	hostd	Manages most operations on the ESXi host, including HA.	Running
	Vpxa	vpxa	Acts as a communication bridge between the ESXi host and vCenter, assisting in DRS operations.	Running
	Fdm	fdm	VMware High Availability (HA) service. Manages VM restarts on other hosts in case of host failure.	Running (if HA is enabled)
	vLockstep	vLockstep	Part of VMware Fault Tolerance. Provides lockstep replication of VMs for zero downtime and data loss protection.	Running (if FT is enabled)
	ESXi Shell Service	esx.shell	Provides shell access to administer ESXi hosts.	Stopped (can be enabled)
	VMware vSAN service	vsanvpd (vSAN VASA Provider)	Offers VASA provider services for vSAN.	Running (if vSAN is enabled)
	NTP Daemon	ntpd	Maintains time synchronization on ESXi hosts.	Stopped (can be enabled)

Establish SSH connection to ESXi host and vCenter.

To use SSH for connecting to an ESXi host, first activate SSH on the host, then employ an SSH client for the connection. Follow these instructions to establish an SSH connection with an ESXi host:



After establishing an SSH connection to an ESXi host, you have the ability to deploy numerous commands for host management and observation. Below is a list of typical SSH commands that can aid in the administration of ESXi:

ESXi Command	Description	Example
esxcli system version get	This command allows you to see the version and build number of your ESXi host.	**Example:** You run the command and get output similar to "VMware ESXi 6.7.0 build-8169922".
esxcli network ip interface list	This command displays all network interfaces on your ESXi host, along with their respective IP addresses.	**Example:** Running this command shows an output including interfaces like "vmk0", "vmk1", with their associated IP addresses.

---

esxcli network ip dns server list	With this command, you can see the DNS servers that your ESXi host is configured to use.	**Example:** The command output shows "DNS servers: 192.0.2.53, 203.0.113.53", indicating these are the configured DNS servers.
esxcli storage core device list	This command reveals the storage devices that your ESXi host can access.	**Example:** Running this command might display devices like "naa.6006016045502500a7e03a8b8b7ed411" with additional information about the device.
esxcli storage vmfs extent list	Use this command to see the VMFS volumes and their extents on your ESXi host.	**Example:** The output might include volumes like "datastore1", along with the extent information.
esxcli hardware cpu list	This command provides detailed information about the CPUs on your ESXi host.	**Example:** You might see output like "CPU0, core 0, HT 0, Socket 0" which gives detailed info about each CPU.
esxcli hardware memory get	You can use this command to get the memory information from your ESXi host.	**Example:** The command might output something like "Physical Memory: 32 GB", showing the total physical memory.
esxcli software vib list	This command will show you the installed VIBs (vSphere Installation Bundles) on your ESXi host.	**Example:** Output may include VIBs like "esx-base", "vsan", each with version and installation dates.
esxcli vm process list	This command provides a list of the running virtual machines on your ESXi host.	**Example:** You might see an output including VM names like "vm1, vm2", with additional information such as World ID, UUID, and display name.

Keep in mind that the examples provided are for illustration purposes only and the real results will vary based on your ESXi host's particular setup and condition.

vCenter Server Appliance (VCSA):

Action	Command
List all services	**service-control --list**
Start a service	**service-control --start [servicename]**
Stop a service	**service-control --stop [servicename]**
Restart a service	**service-control --restart [servicename]**
List service dependencies	**service-control --list-dependencies [servicename]**
List required services	**service-control --required-by [servicename]**
