NAKIVO®

eBook

The Complete Guide to VMware Clustering

Contents

Overview

Modern information technology evolves rapidly, and the resulting innovations are used in the growing number of industries. While these IT solutions provide automation, as well as ensuring rational usage of natural and human resources, their hardware requirements are gradually increasing. Even a powerful server can be overloaded with multiple computing tasks. For better performance and reliability, servers can now be connected with each other over networks. For this purpose, clustering technologies are widely used. This eBook explains what clusters are, what issues you can resolve with clustering, and how to deploy clusters in your VMware environment.

Cluster: Definition and Types

A **cluster** is a group of independent servers that communicate with each other over the network and can act as a single system. The servers forming a cluster are called “nodes” or “members” and are fine-tuned to perform the same tasks under the control of special software. Any cluster consists of at least two nodes.

There are three commonly known types of clusters:

- High-Performance Computing clusters
- High Availability clusters
- Load Balancing clusters

High-Performance Computing (HPC) clusters are also called “parallel clusters”. They provide a single system image. This means that an application can be executed on any of the servers within the cluster. HPC clusters are used to execute computation-intensive and data-intensive tasks by running a job on multiple nodes simultaneously, thus enhancing application performance.

High Availability (HA) clusters are also referred to as “failover clusters” and deliver robust operation with the minimal amount of downtime. Redundant storage, software instances, and networking provide continued service when system components fail. HA clusters usually use a heartbeat private network connection to monitor the health and status of each node in the cluster.

Load Balancing (LB) clusters ensure better performance. In LB clusters, tasks are distributed between nodes to load hardware more rationally and avoid overloading each server if there are enough computing resources available.

In VMware vSphere, you can deploy two of the above types of clusters working on the virtual machine layer: HA clusters and LB clusters (the latter of which are called Distributed Resource Scheduler (DRS) clusters in the context of VMware vSphere).

High Availability (HA) Cluster

A High Availability (HA) cluster supports the migration of virtual machines from one ESXi host to another in case of failure. Two or more ESXi servers on the same network with shared storage unite into a logical group called the “pool”. When one ESXi servers fails, the virtual machines that were running on this host are started on another ESXi server within the cluster. Powering on and loading these virtual machines may take some time (resulting in short periods of idle time). After an ESXi server is added to a cluster, a special agent called the **Fault Domain Manager** (FDM) is automatically installed. This utility monitors signals called **heartbeats** from other ESXi hosts in the cluster and communicates with the vCenter Server (once per second by default). If only one virtual machine fails, this VM is restarted on the same ESXi server. The type of action taken depends on the type of failure detected, and you can set rules in **Preferences**. The first five hosts added to a cluster are considered **primary**, and all subsequent hosts are **secondary**. If one of the primary hosts is removed from the cluster, a secondary takes up the primary role.

The main features of HA clusters are:

- **Host monitoring** – a feature that helps monitor each ESXi host in the cluster and make sure that this server is running. ESXi hosts exchange network heartbeats in the cluster. If an ESXi host fails, that host’s virtual machines can be restarted on another host.
- **Admission control** – a feature that controls the policy used by an HA cluster for reserving resources to ensure failover capacity within the cluster.
- **VM monitoring** – a feature that helps monitor each virtual machine in the cluster with VMware Tools heartbeats to ensure this VM is running. Any virtual machines that fail are restarted.
- **Datastore heartbeating** – a feature that uses datastores to monitor hosts and virtual machines when the management network fails. Moreover, this feature reduces the probability of false restarts and false migration.
- **Fault tolerance** – a feature that allows you to avoid downtime of virtual machines by running a VM replica on another ESXi host within the cluster.

Distributed Resource Scheduler (DRS) Cluster

A Distributed Resource Scheduler (DRS) cluster supports distributing computing resources between hosts based on the performance required by virtual machines and the availability of free ESXi host resources. The DRS checks the performance of your virtual machines and makes placement decisions – that is, the scheduler determines to which host within the cluster a particular VM should be migrated automatically or manually after receiving a notification. Some virtual machines can be idle and “wake up” when they are required to execute some important tasks, using CPU, memory, along with network bandwidth.

This might prompt the DRS to move these VMs to another host with more free resources available. The feature helps save management time that would otherwise be spent on monitoring and maintaining the infrastructure.

The main features of DRS clusters are:

- **Load balancing** – a feature that allows performing or recommending migrations of virtual machines between ESXi hosts to balance the load according to the settings you select.
- **Power management** – a feature that supports migration of virtual machines from one ESXi host to another, if there are enough free resources, and sets the standby power mode for the source ESXi server.
- **Affinity rules** – a feature that allows you to control the placement of virtual machines among hosts by establishing rules.

How to Create a VMware Cluster

The hardware and software requirements for a VMware cluster are as follows:

- Availability of at least two ESXi servers with unique host names and static IP addresses. For full compatibility, they should have processors of the same family, produced by the same vendor.
- All hosts within the cluster should be attached to some form of shared storage, such as network-attached storage (NAS) device or storage area network (SAN), via Fibre Channel, Internet Small Computer System Interface (iSCSI), or Network File System (NFS) protocols. Virtual Machine File System (VMFS) volumes must be used. There must be sufficient free space on the storage medium.

NOTE: When choosing NAS or SAN solutions, use an authorized vendor that meet your requirements for your production environment. Set up the storage according to the manufacturer documentation. Multiple NAS or SAN devices can be used to create a VMware cluster.

- All volumes on the ESXi hosts must use the same volume names.
- At least one VM must have the Active Directory Domain Controller has to be installed.
- At least one VM must have vCenter installed.

To create a VMware cluster, the following steps must be performed (each is explored with an in-depth walkthrough in this section):

1. Install a VMware ESXi Server.
2. Install Active Directory Domain Controller.
3. Install and set up vCenter Server.
4. Set up a shared datastore.
5. Connect hosts in clusters.
6. Configure the network for the cluster.
7. Configure HA and/or DRS clusters.

Installing VMware ESXi Server

VMware ESXi Server is an enterprise-class type-1 hypervisor with a proprietary kernel **(VMkernel)** that runs directly on server hardware and does not require the installation of an additional underlying operating system (OS). ESXi is highly reliable and includes an ultra-thin architecture that is not dependent on a general-purpose OS. The smaller code-base contributes to a low-vulnerability environment and makes for quick installation as well as booting. As a virtualization server, ESXi is the most important component of the vSphere environment. While the VMs themselves run on ESXi Server, the virtual disks of the VMs can be stored either on internal data storage located directly on ESXi Server (such as hardware SAS RAID) or a on a shared external datastore. You can access ESXi Server remotely via the Secure Shell (SSH) client, the VMware Command Line Interface (CLI), or vSphere Client. SSH access is disabled by default.

The minimum hardware requirements for ESXi are as follows:

- 64-bit processor with at least two cores.
- At least 8 GB of RAM to take full advantage of ESXi 5.1+ features and run virtual machines in typical production environments.
- Support for hardware virtualization (Intel VT-x or AMD RVI).
- Two or more Ethernet controllers (1Gb or 10Gb) to provide network redundancy for the cluster.
- Small Computer System Interface (SCSI) disk, Serial Attached SCSI (SAS) disk, or a local, non-network, Redundant Array of Independent Disks (RAID) Logical Unit Number (LUN) with unpartitioned space.
- Serial ATA (SATA) disks connected through supported SAS controllers, or supported on-board SATA controllers that are considered remote, not local; these disks are not used as a scratch partition by default, because they are seen as remote.

To install ESXi Server, do the following:

1. Insert the installation disc into the optical drive, select this disc as the first boot device in BIOS, and boot from this disc. Alternatively, you can write the installation image to a USB flash drive.

Select the Installer from the boot menu (*see Figure 1.1*).

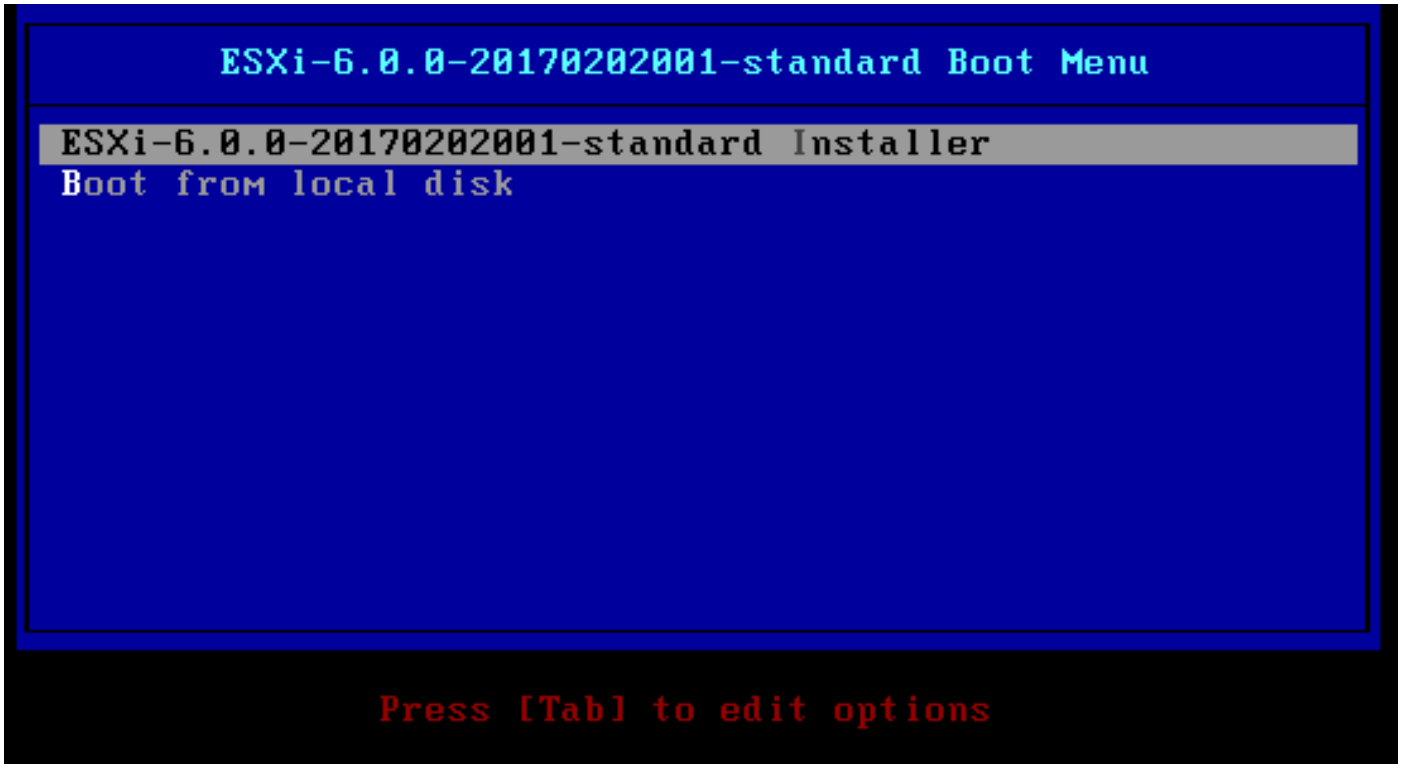


Figure 1.1

NOTE: If your system hangs at the “user loaded successfully” stage (see Figure 1.2), this may be due to insufficient RAM. Check the amount of memory available. Press Alt+F12 to view details.

Figure 1.2

If everything is okay, the “welcome” installation screen appears (see *Figure 1.3*).

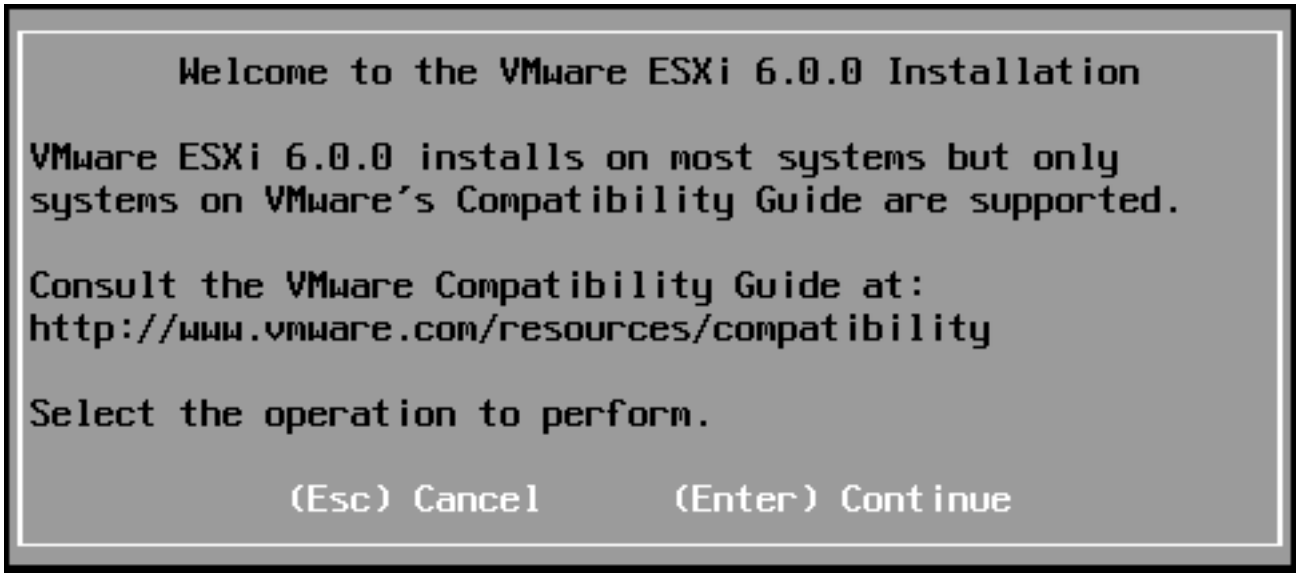


Figure 1.3

2. Select a disk on which to install ESXi (see *Figure 1.4*).

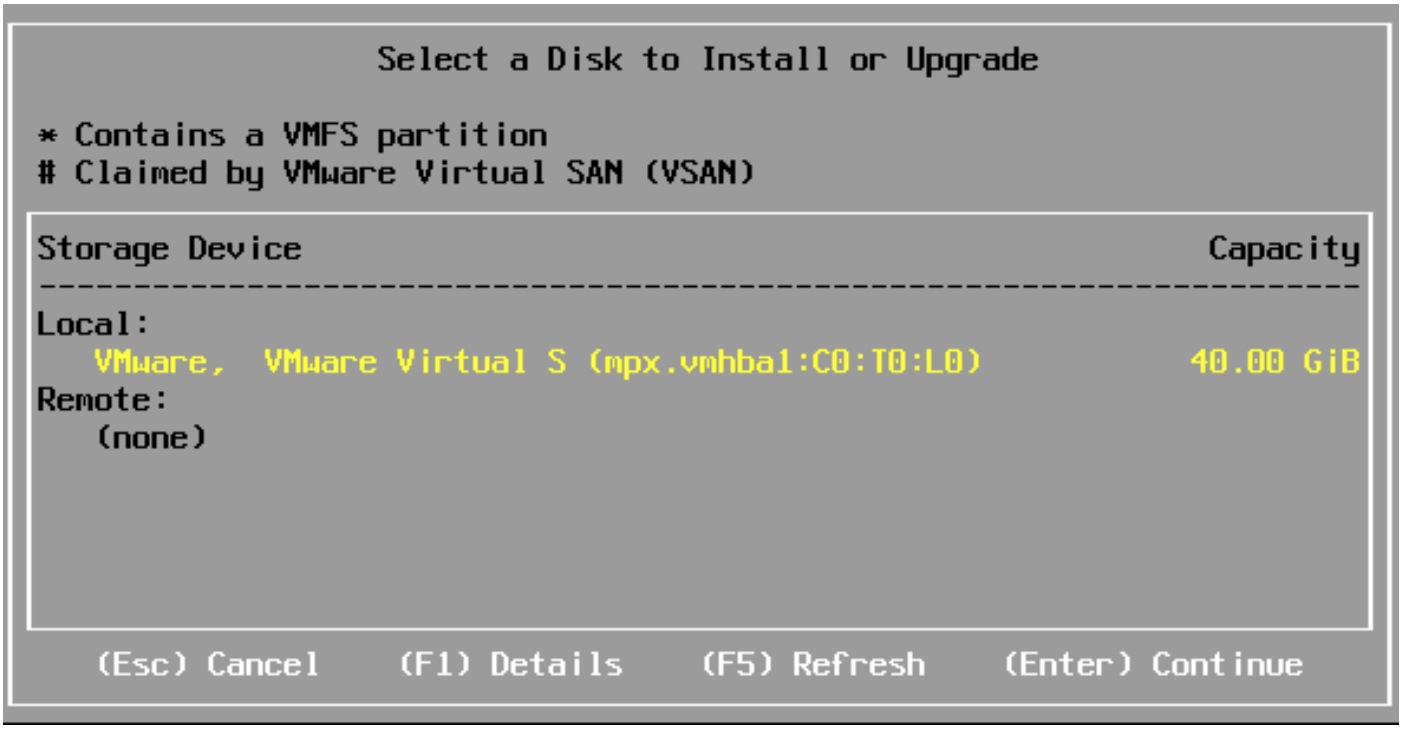


Figure 1.4

3. Select your keyboard layout.
4. Enter a root password (see *Figure 1.5*).

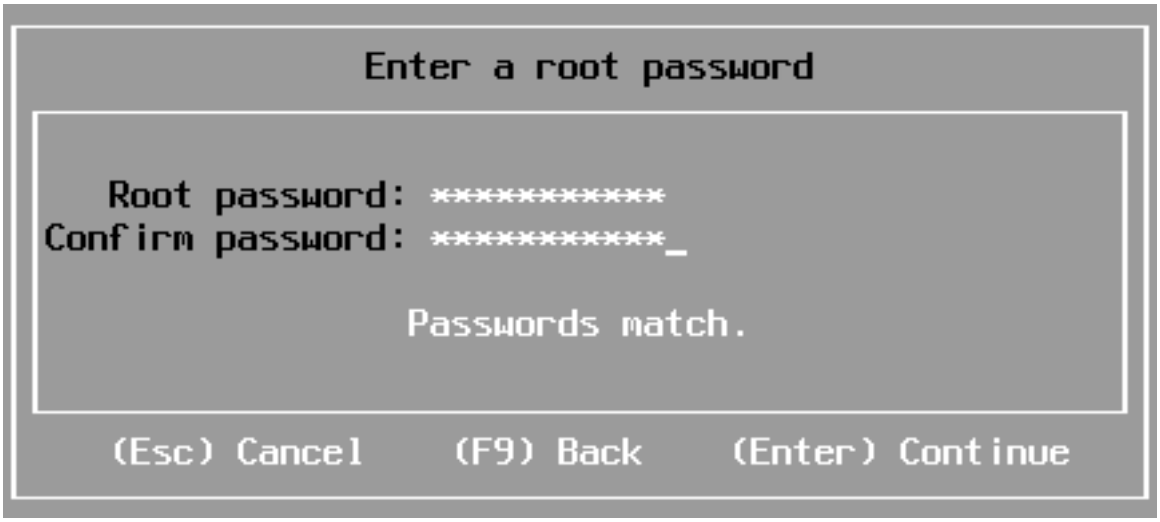


Figure 1.5

Then wait for system scanning to complete (see *Figure 1.6*).

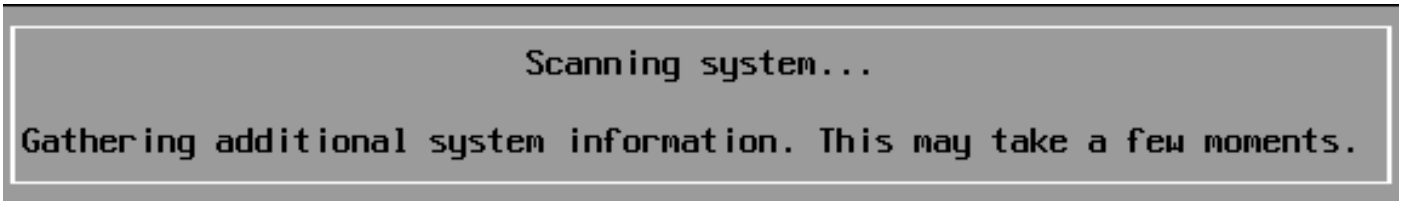


Figure 1.6

NOTE: If there are less than 2 CPU cores, an error message appears (see *Figure 1.7*).

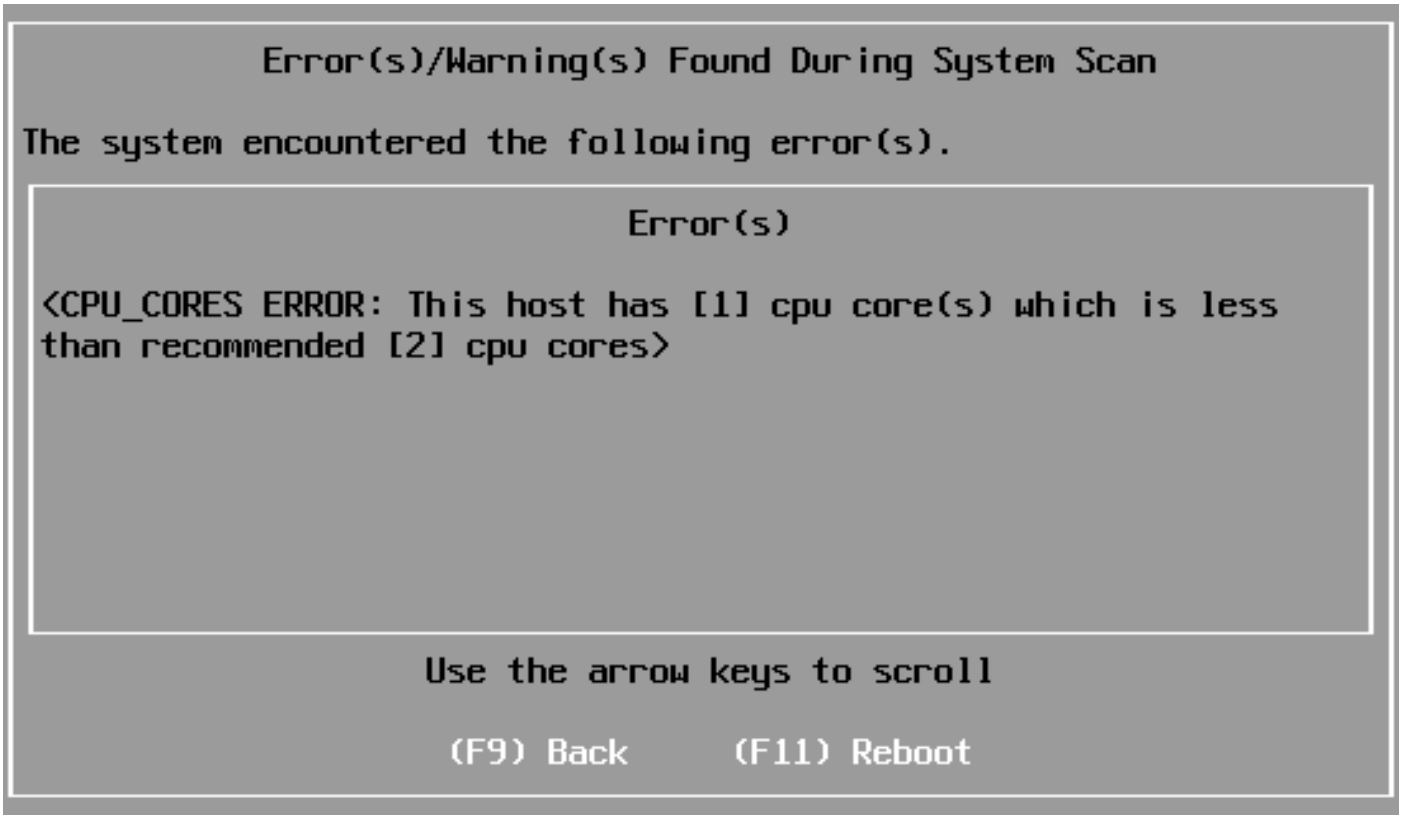


Figure 1.7

If everything is okay, the confirmation message is displayed (see *Figure 1.8*).

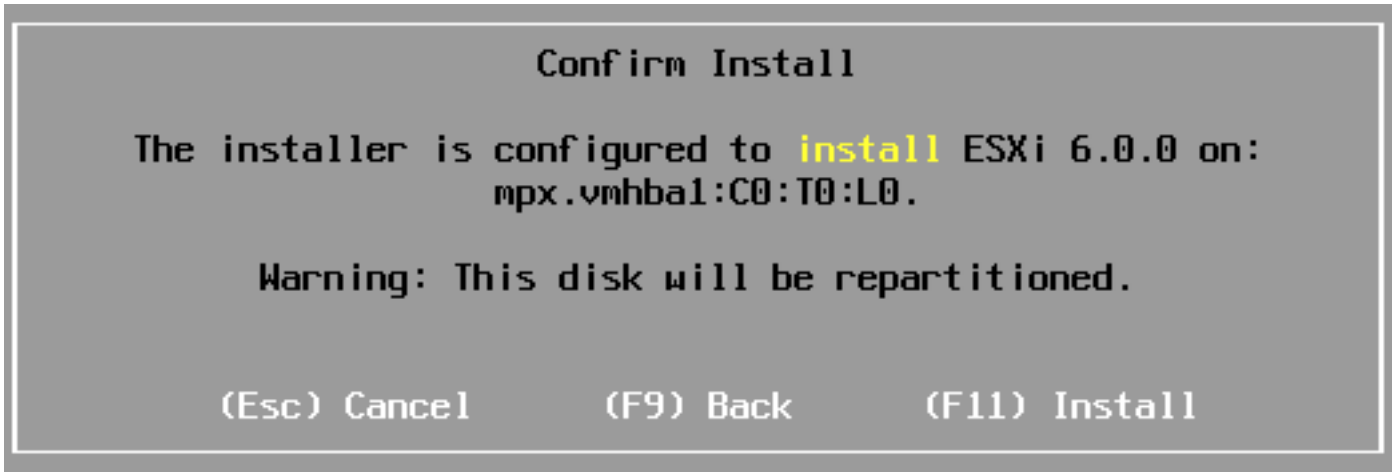


Figure 1.8

8. Press **Install** and wait for the installation progress to complete (see *Figure 1.9*).

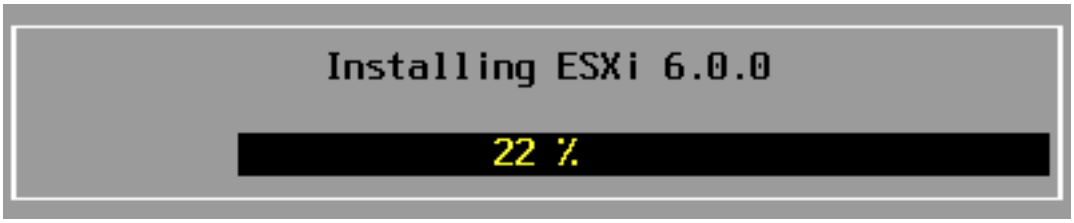


Figure 1.9

7. You can see the “Installation Complete” message. Press **Enter** (see *Figure 1.10*).

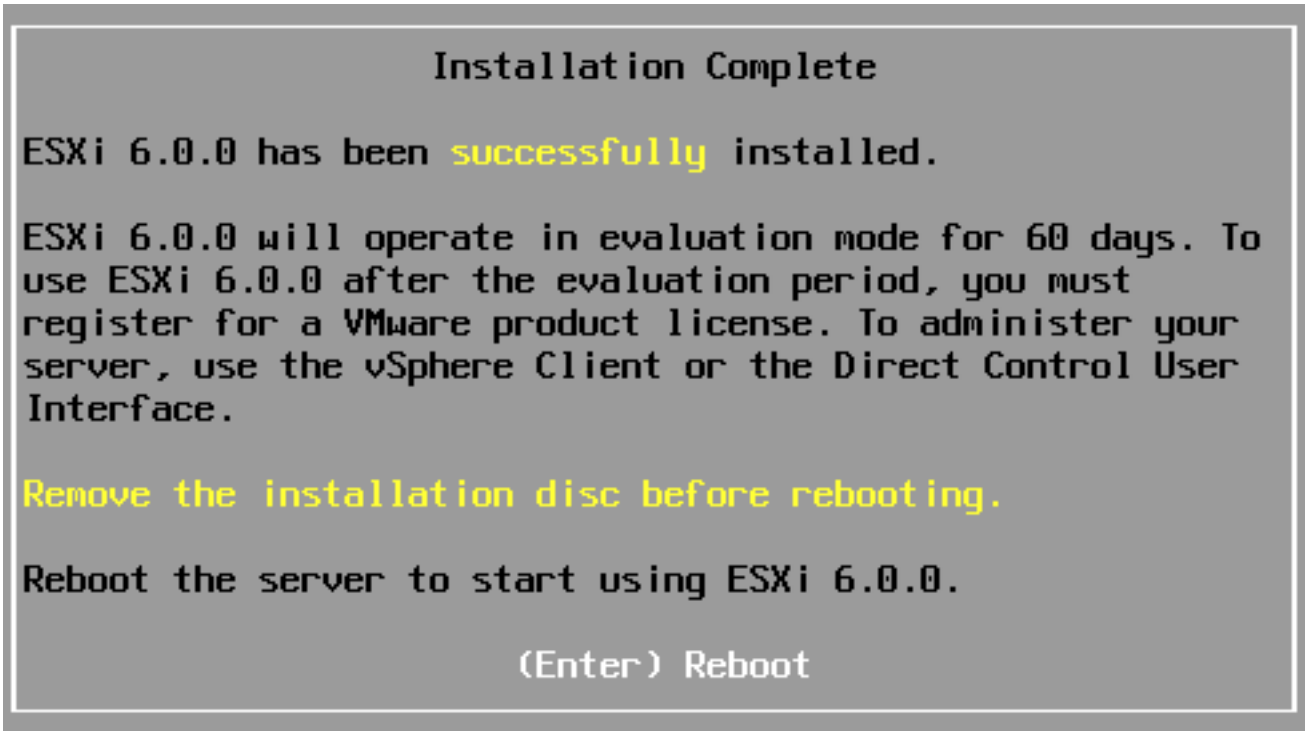


Figure 1.10

Wait for the server to reboot (see *Figure 1.11*).

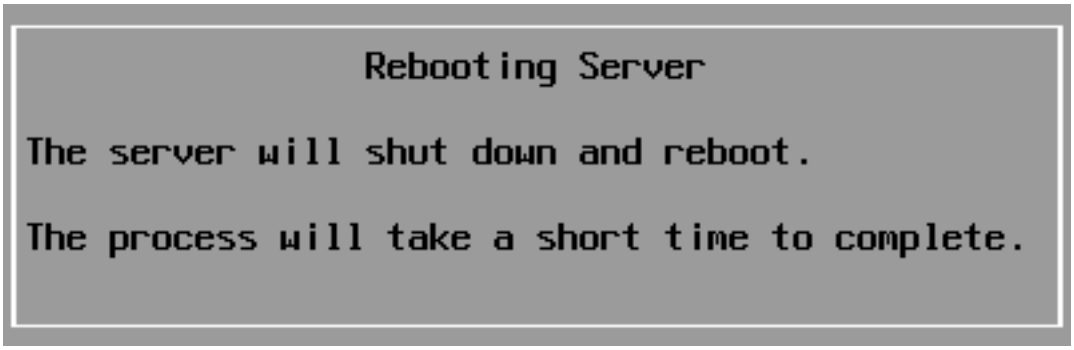


Figure 1.11

8. After rebooting the server, log in ESXi (see *Figure 1.12*).
9. Press F2.

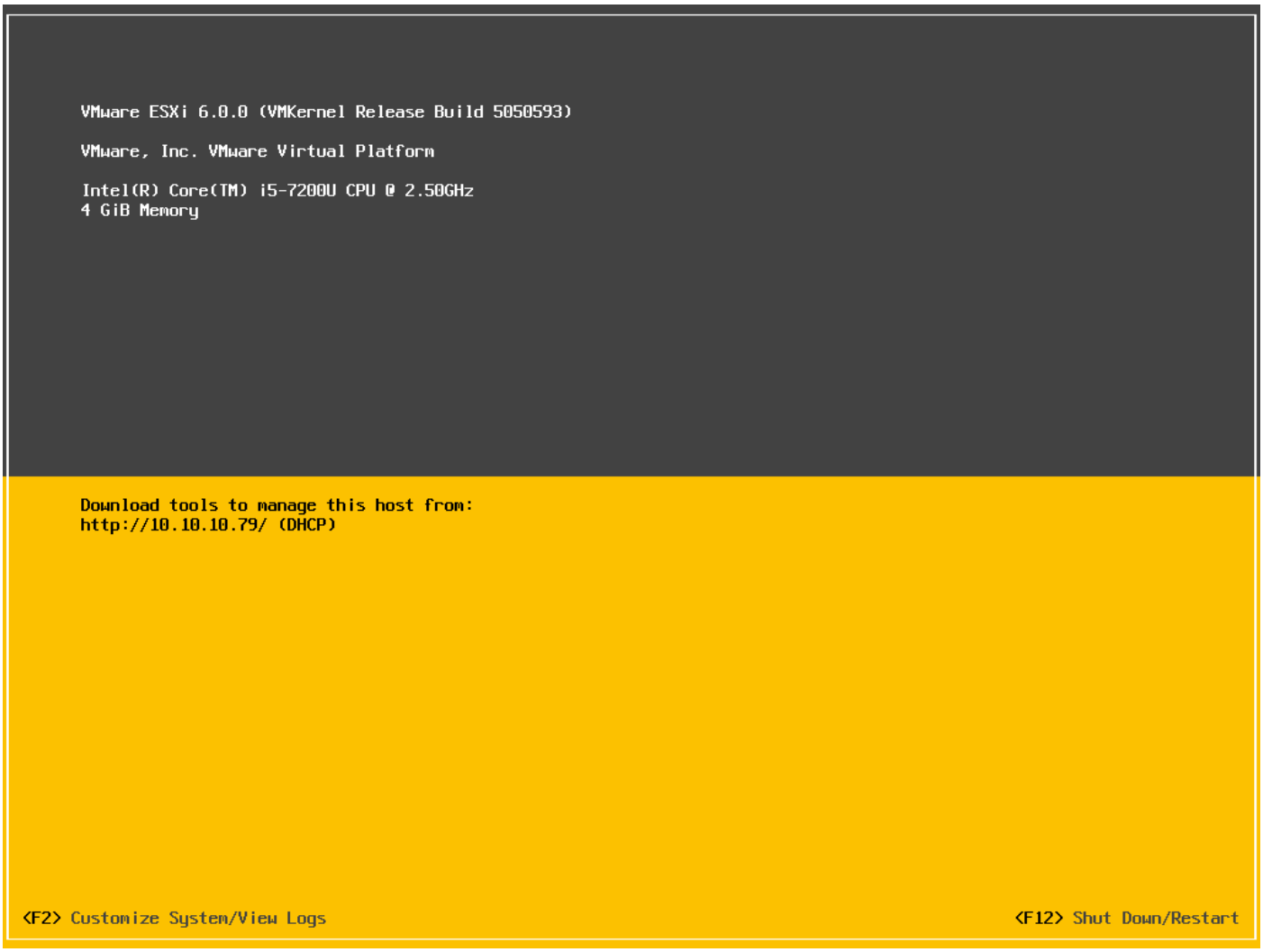


Figure 1.12

10. Select **Configure Management Network** from the menu, and set up the host name along with the IP address manually – for example, 10.10.10.46 (see *Figure 1.13*).

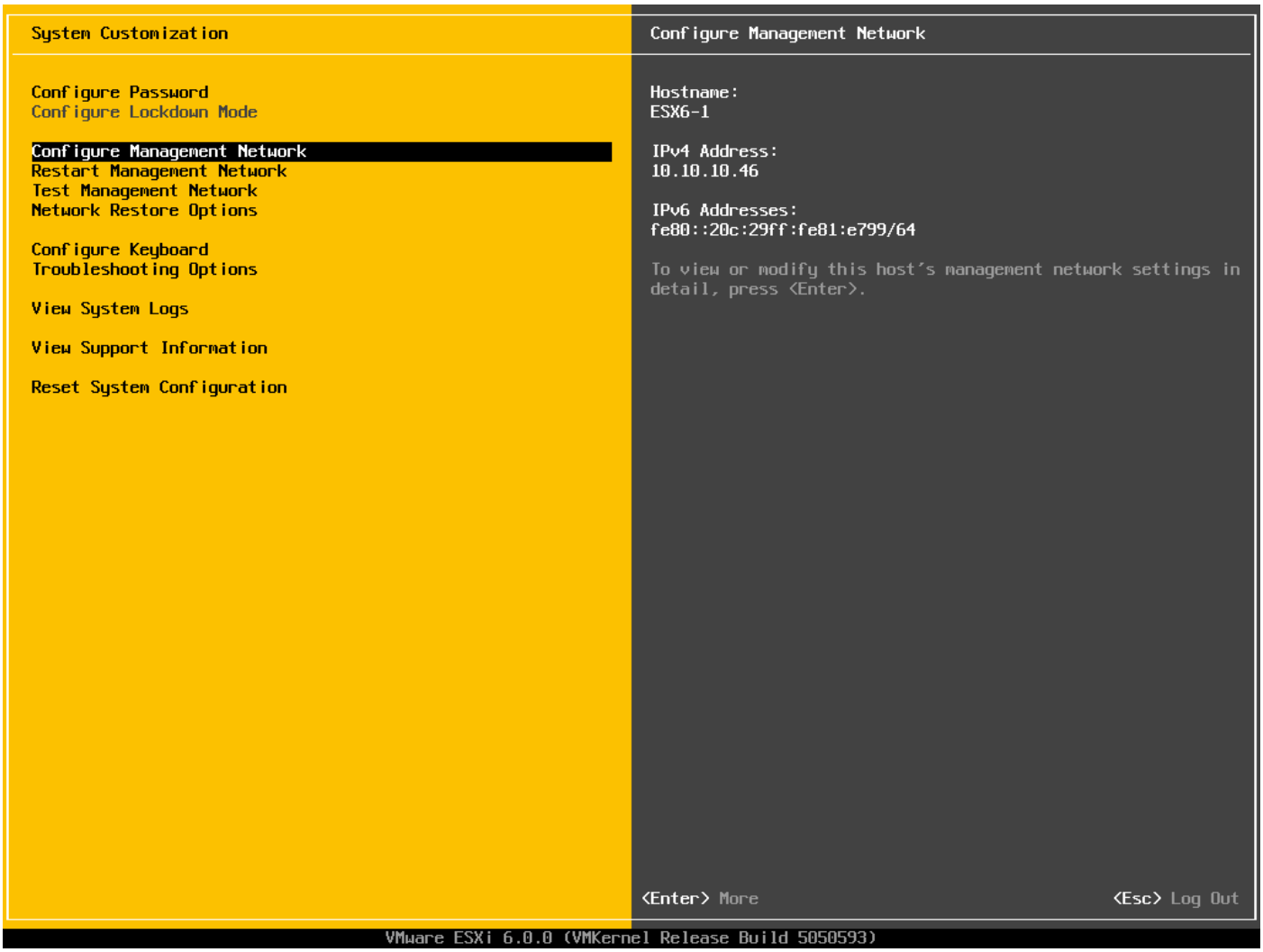


Figure 1.13

11. Press **Yes** to confirm the network changes (see *Figure 1.14*).

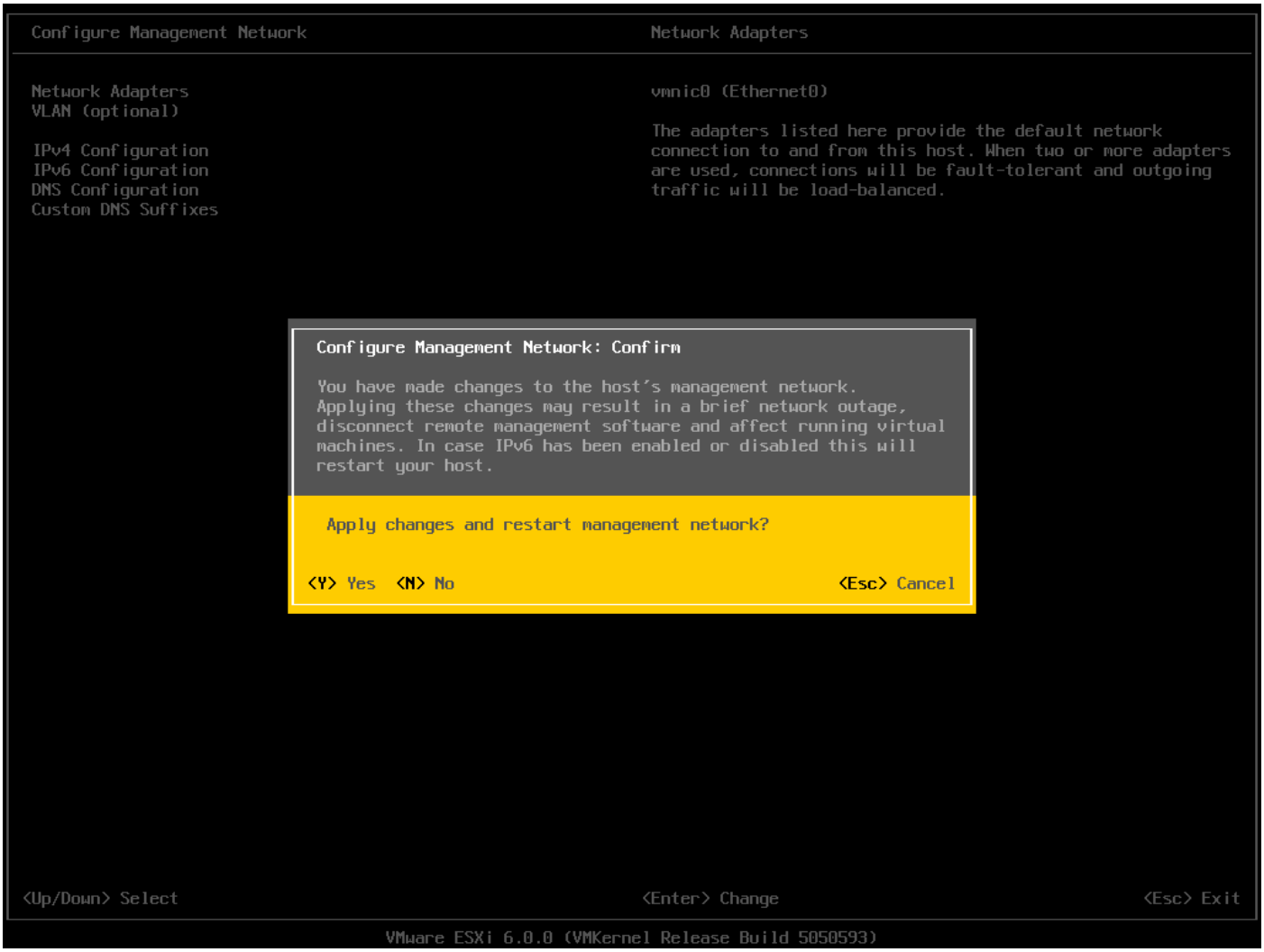


Figure 1.14

12. Now, you can download VMware vSphere Client. Open your web browser and enter the URL of your ESXi server (see *Figure 1.15*).

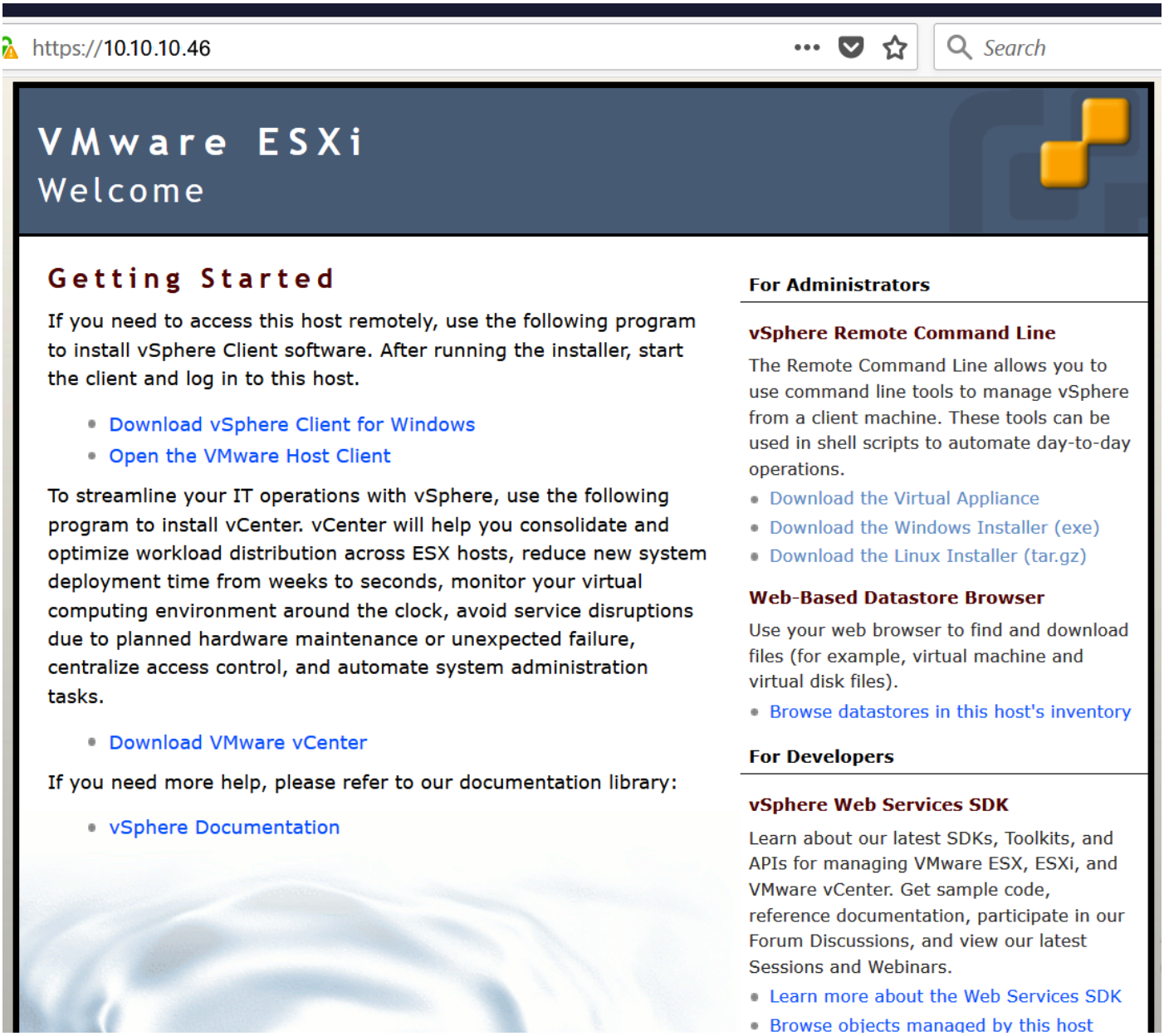


Figure 1.15

Follow the **Download vSphere Client for Windows** link and download the installer from the official VMware website.

13. Install VMware vSphere Client by following the steps the installation wizard guides you through (see *Figure 1.16*).

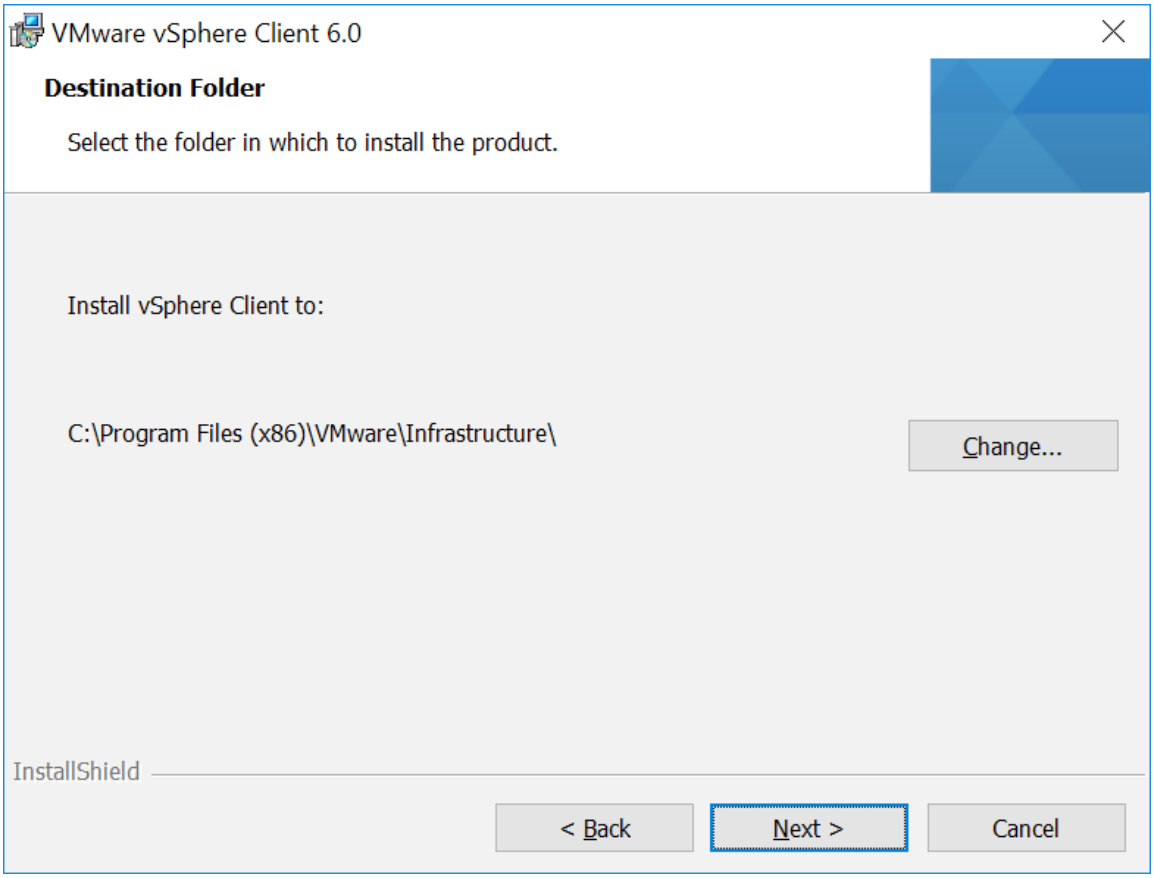


Figure 1.16

14. Log in to ESXi Server via vSphere Client by entering the user name and password you specified during the ESXi installation (see *Figure 1.17*).

NOTE: Ignore the certificate warning.

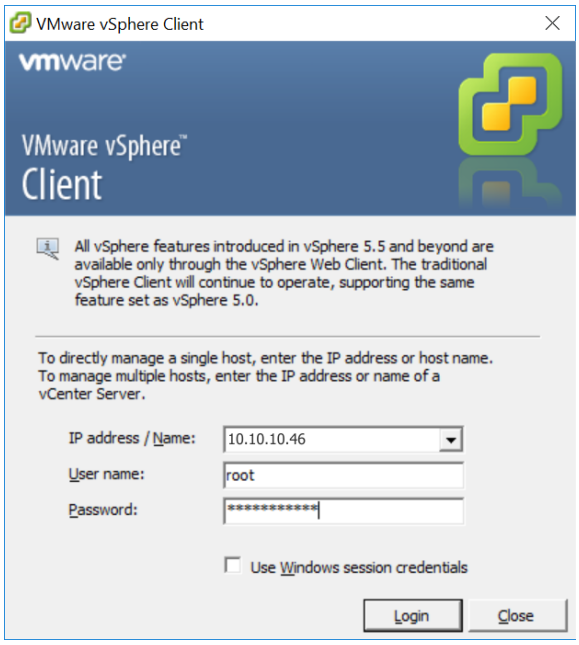


Figure 1.17

You now have one ESXi server installed. The second one can be installed in the same way. This is how the vSphere Client interface looks (see *Figure 1.18*):

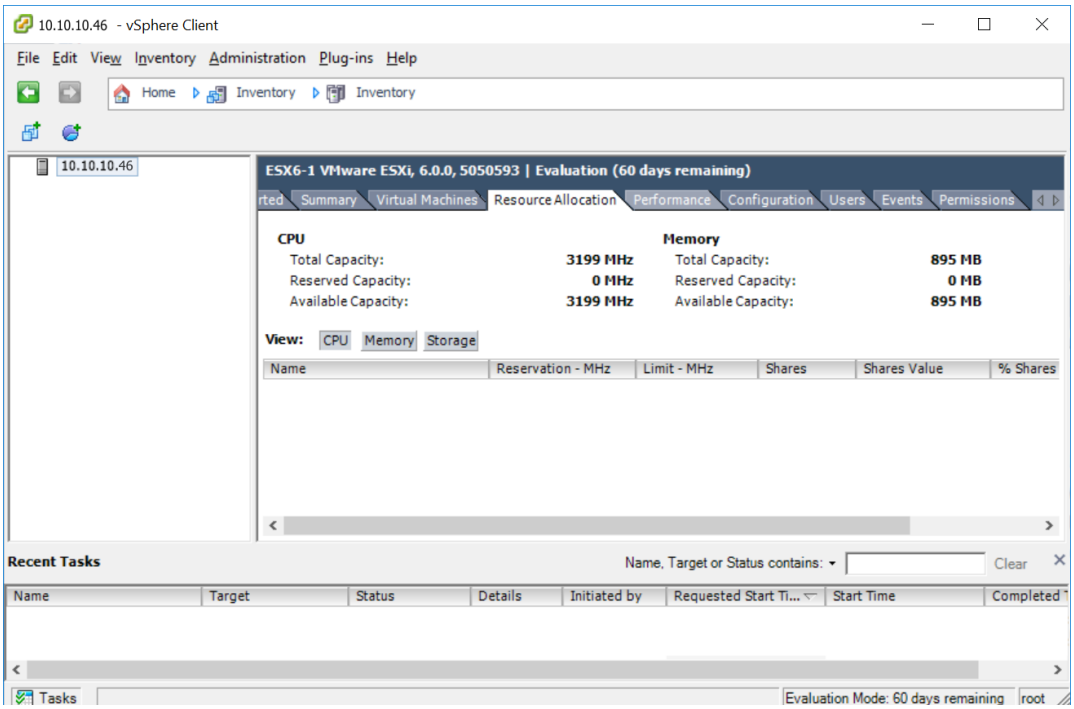


Figure 1.18

Installing Active Directory Domain Controller

vCenter needs a domain controller with a Domain Name System (DNS) server installed for centralized management and resolving DNS names to IP addresses. The Domain Controller is the main component of the Active Directory Domain Services server role, which needs to be installed in this case.

NOTE: Consult the table on the VMware website displaying the compatibility of the various versions of Microsoft Windows Server with the version of vCenter you are using to make sure that the installation can work properly. In the walkthrough that follows, Windows Server 2008 R2 x64 is used, as this version of Windows Server is compatible with most versions of vCenter.

NOTE: The instance of Windows Server you use as the domain controller can be installed on a physical server or a virtual machine.

To install Active Directory Domain Services, take the following steps:

1. Press **Win+R** (or go to **Start -> Run**) and type **"dcpromo"** in the **Run** window (see *Figure 2.1*).

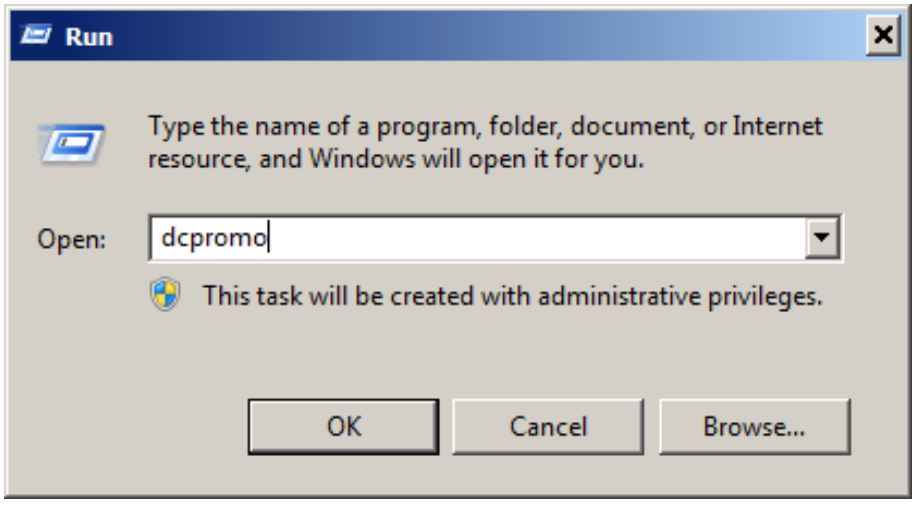


Figure 2.1

Wait for the installation wizard to launch (see *Figure 2.2*).

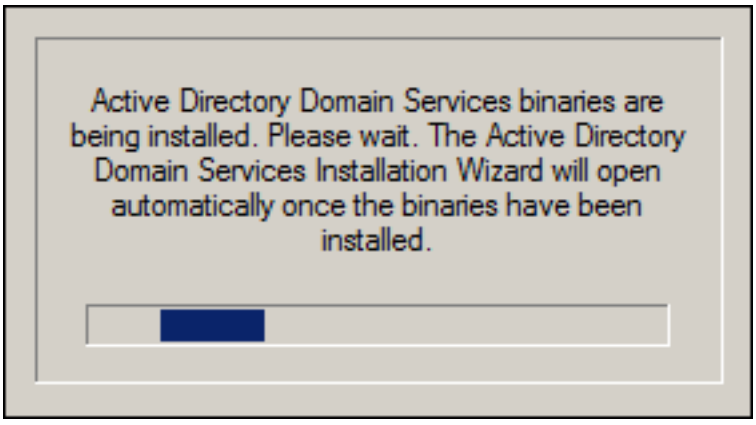


Figure 2.2

2. Tick the checkbox near **Use advanced mode installation** and click **Next** (see *Figure 2.3*).

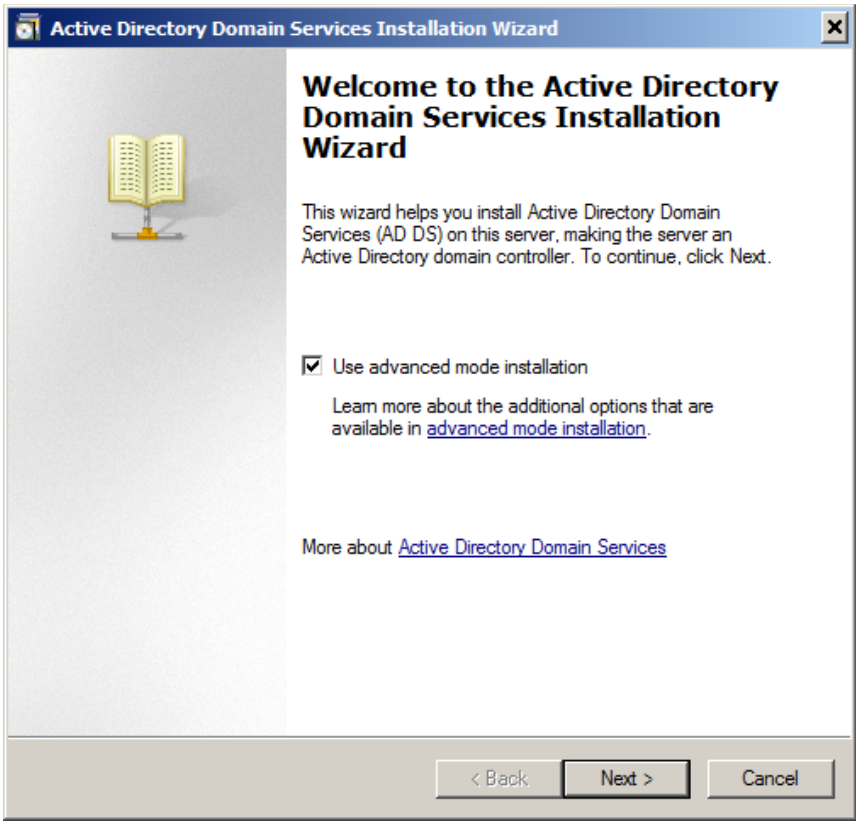


Figure 2.3

3. Read the information on OS compatibility and click **Next** (see *Figure 2.4*).

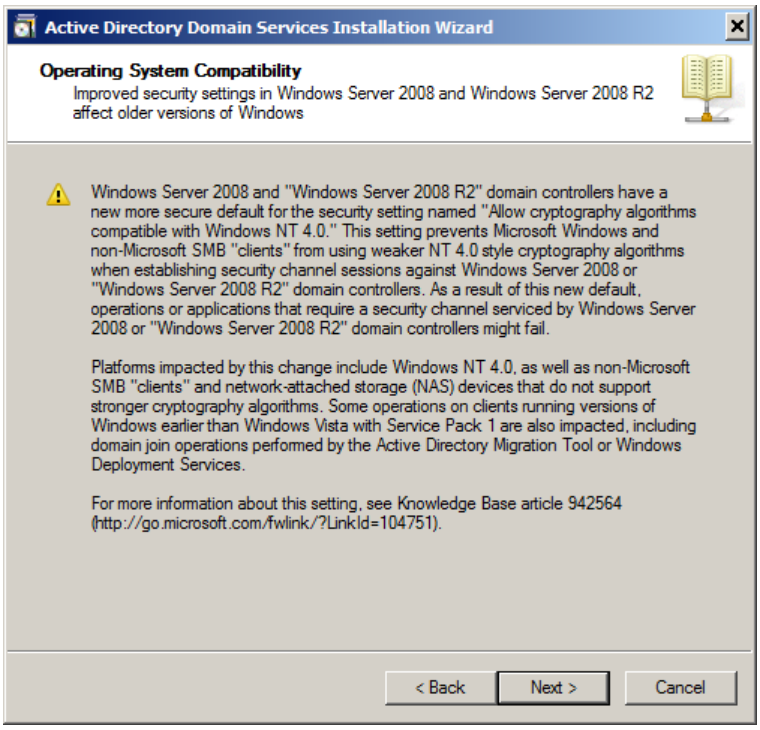


Figure 2.4

4. For the first Domain Controller setup in your infrastructure, select **Create a new domain in a new forest** (see *Figure 2.5*).

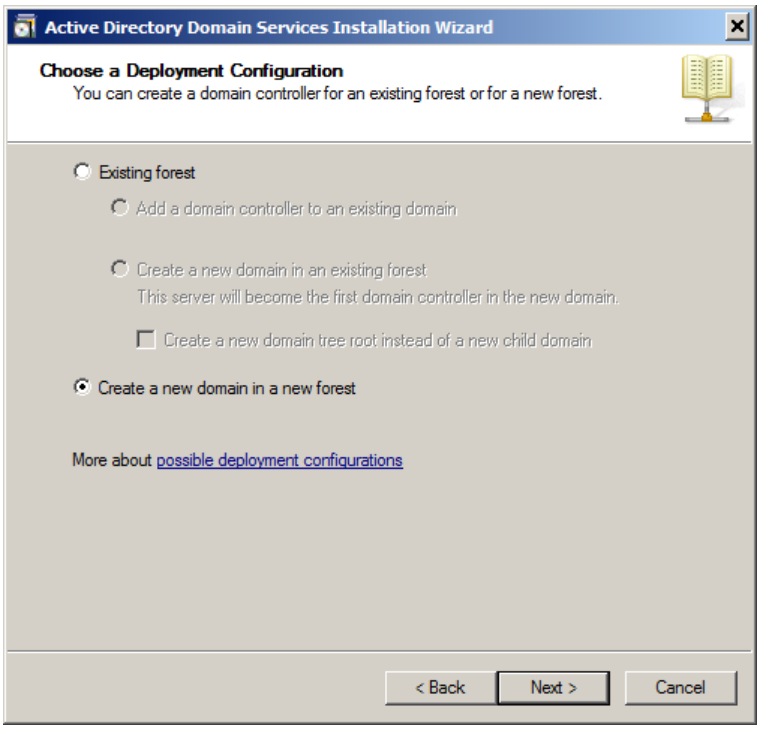


Figure 2.5

5. Enter your domain name (see *Figure 2.6*).

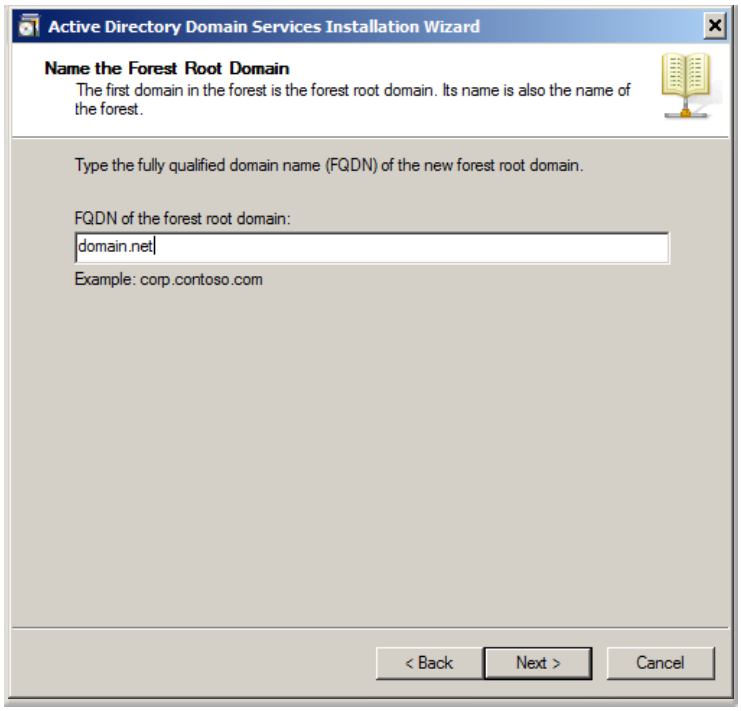


Figure 2.6

6. Enter Accept the Domain NetBIOS name, or alter the one provided, if necessary. (see *Figure 2.7*).

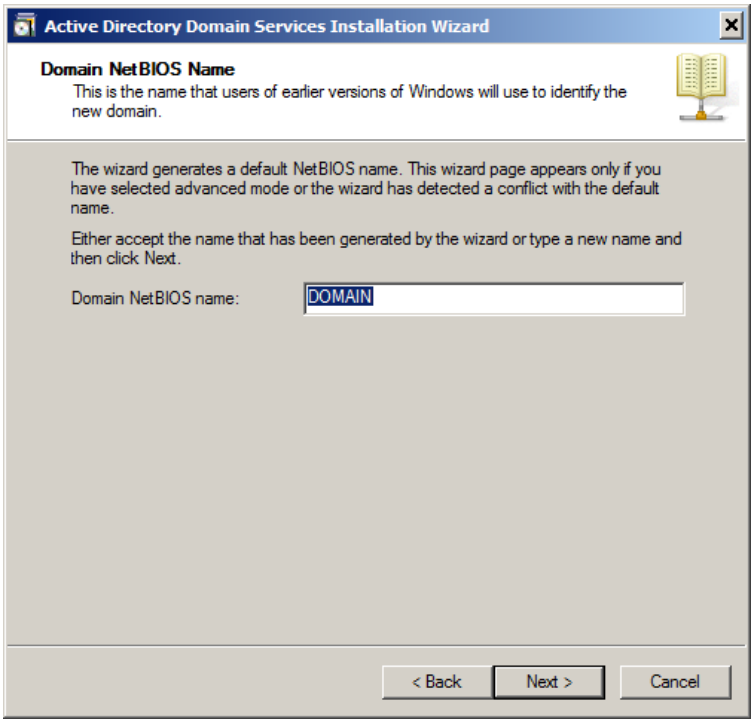


Figure 2.7

7. Set the forest **functional level** (see *Figure 2.8*).

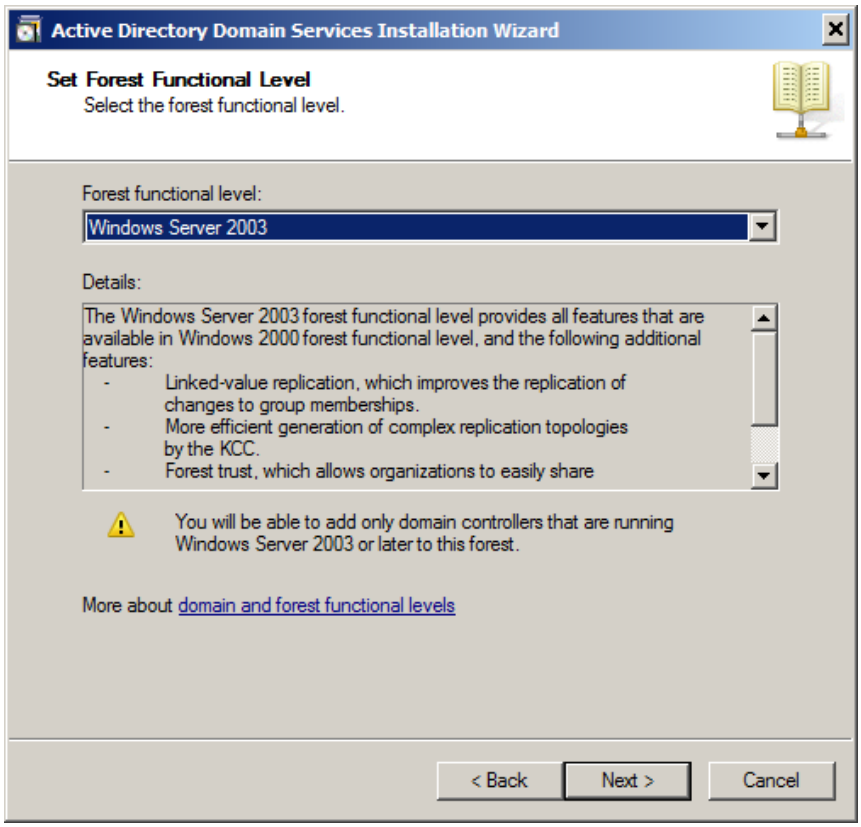


Figure 2.8

NOTE: If there are no Windows Server operating systems older than Windows Server 2008 that you want added to the domain as domain controllers, set the forest functional level to **Windows Server 2008**.

8. Similarly, set the **domain functional level** (see *Figure 2.9*).

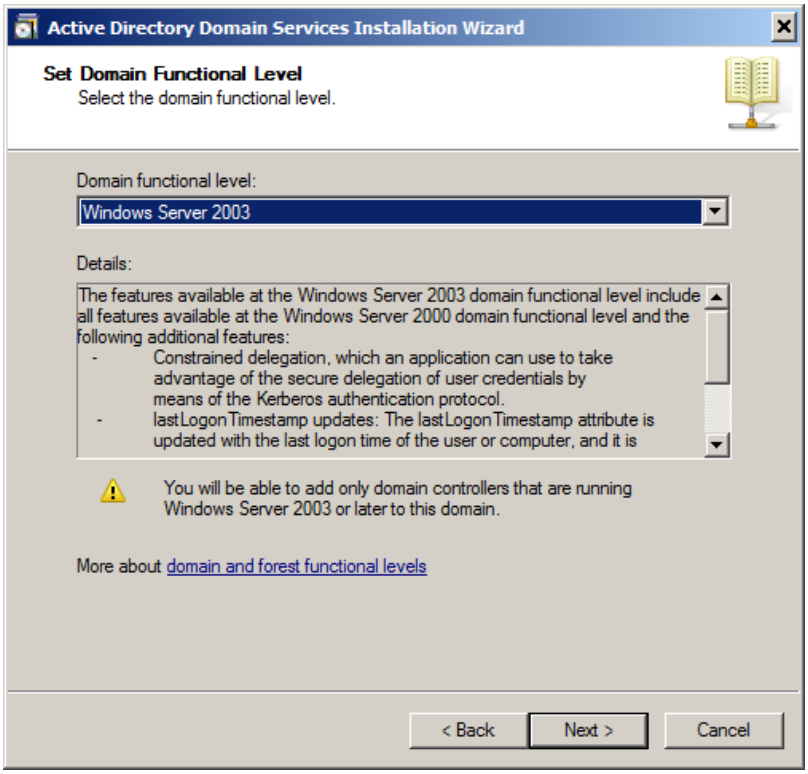


Figure 2.9

9. Under Additional Domain Controller Options, tick the checkbox near **DNS server** (see *Figure 2.10*).

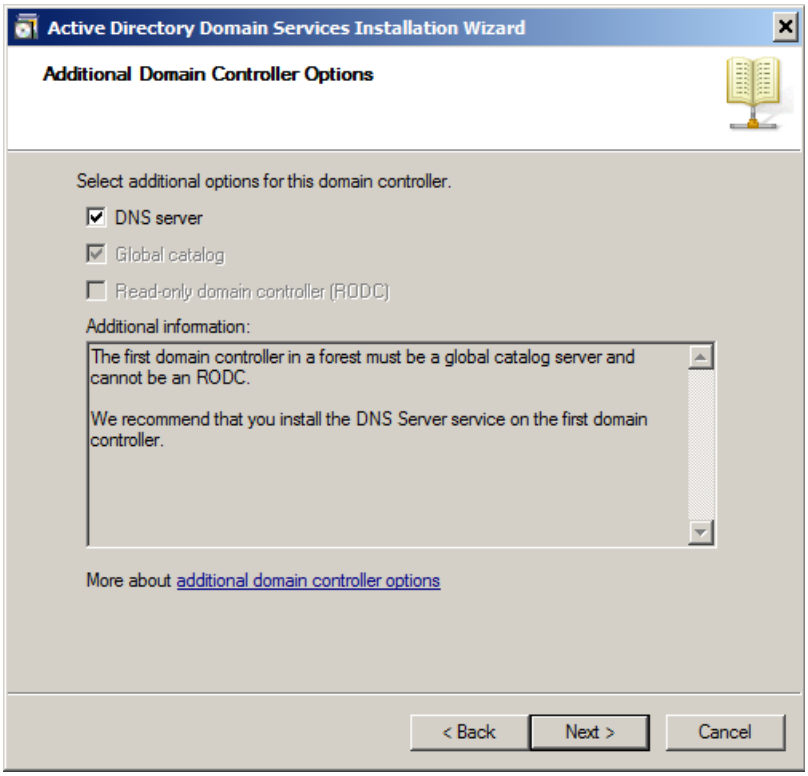


Figure 2.10

10. As this is an internal domain, click **Yes** to continue (see *Figure 2.11*).

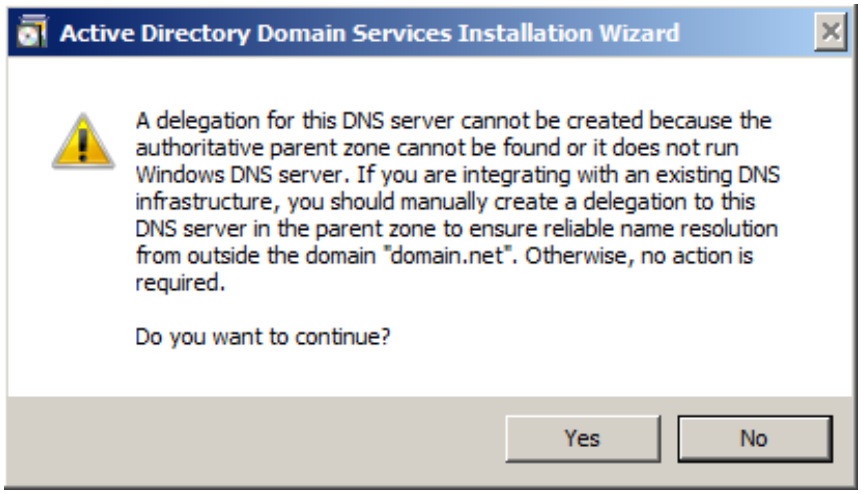


Figure 2.11

11. Set the location for the Domain Controller files. You can leave the default location (see *Figure 2.12*).

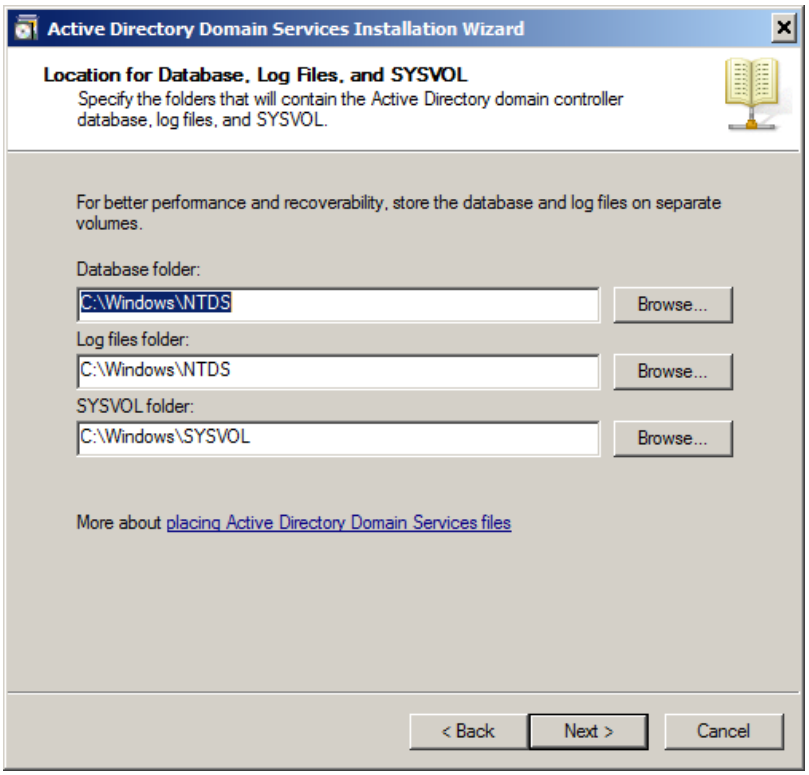


Figure 2.12

12. Set the password for the Domain Controller Administrator account. The password must meet the complexity requirements set in the default Domain Controller security policy (see *Figure 2.13*).

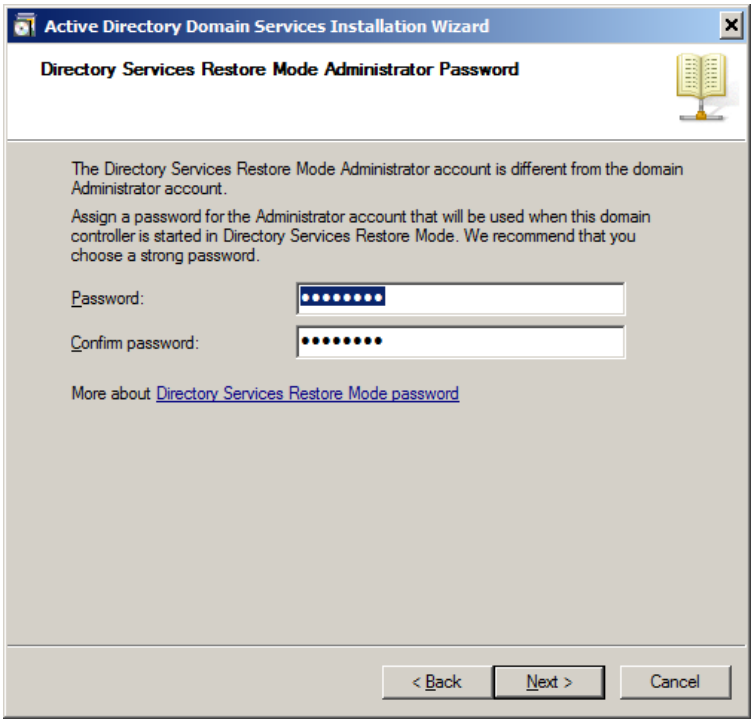


Figure 2.13

13. View the summary and click **Next** to start the installation (see *Figure 2.14*).

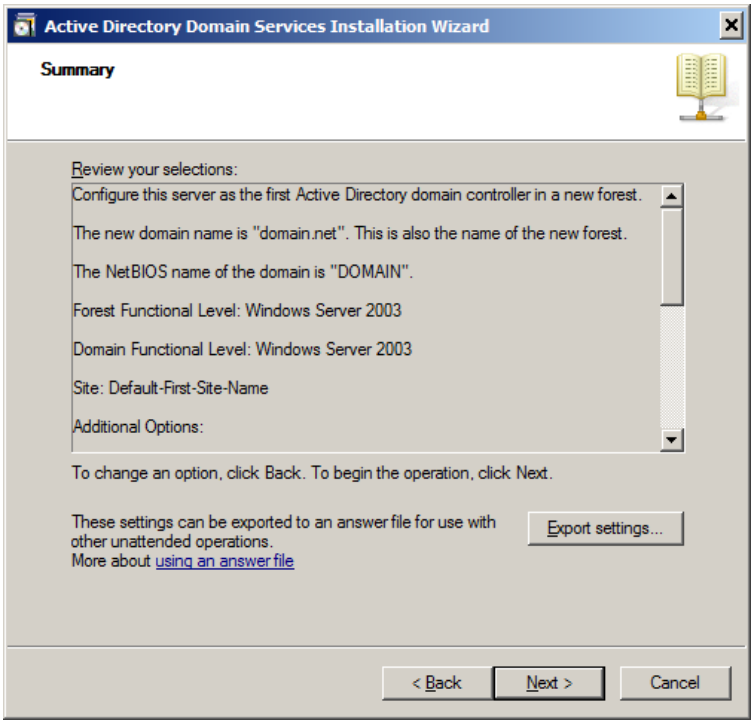


Figure 2.14

Wait for the installation to complete (see *Figure 2.15*).

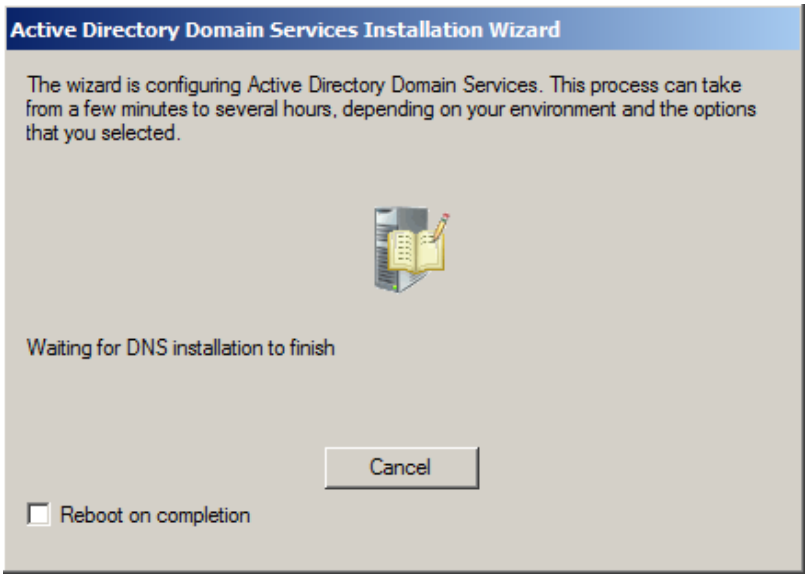


Figure 2.15

14. Click **Finish** and reboot the server (see *Figure 2.16*).

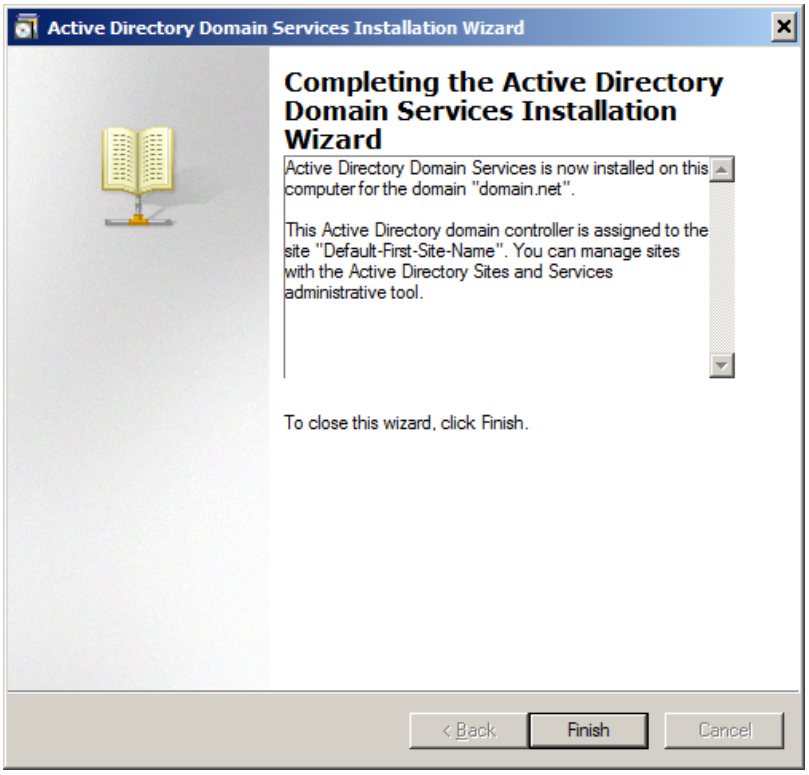


Figure 2.16

Installing and Setting Up vCenter Server

vCenter is a VMware centralized management server application that controls all virtual infrastructure, providing resource provisioning and performance evaluation of virtual machines in the vSphere virtual environment. vCenter Server can be installed manually on Windows or deployed as a virtual appliance. The vCenter Virtual Appliance is a preconfigured Linux-based virtual machine image with all the necessary software already installed.

NOTE: Do not install vCenter Server on the machine with Active Directory Domain Controller installed.

vCenter can be installed either on a physical machine or a virtual machine. Installing vCenter on a virtual machine offers a number of advantages, including the following:

- no need to dedicate a separate server.
- snapshots usage and ease of backup.
- easy migration of VMs from one host to another.
- provision of high availability for the vCenter Server system by using vSphere HA.

The following are the minimum requirements for vCenter Server installation:

- 64-bit operating system, such as Windows Server 2008R2 x64 (this is required for some versions of vSphere, but not all)
- CPU: 2 GHz or faster Dual Core 64-bit processor
- RAM: 8 GB minimum (requirements can increase with higher numbers of virtual machines in vSphere)
- Disk storage: 40 GB minimum (this varies depending on the database type and the number of VMs)

To install and set up vCenter Server, take the following steps:

1. Insert the installation media for the machine on which you want to install vCenter Server and run **autorun.exe** (see *Figure 3.1*).

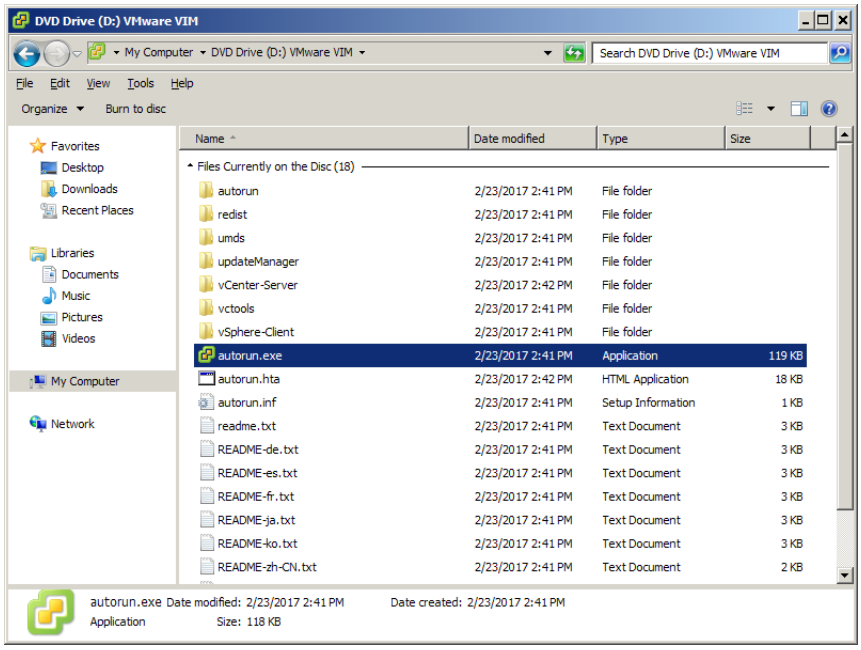


Figure 3.1

2. In the VMware vCenter Installer window, select **vCenter Server for Windows** and click **Install** (see *Figure 3.2*).

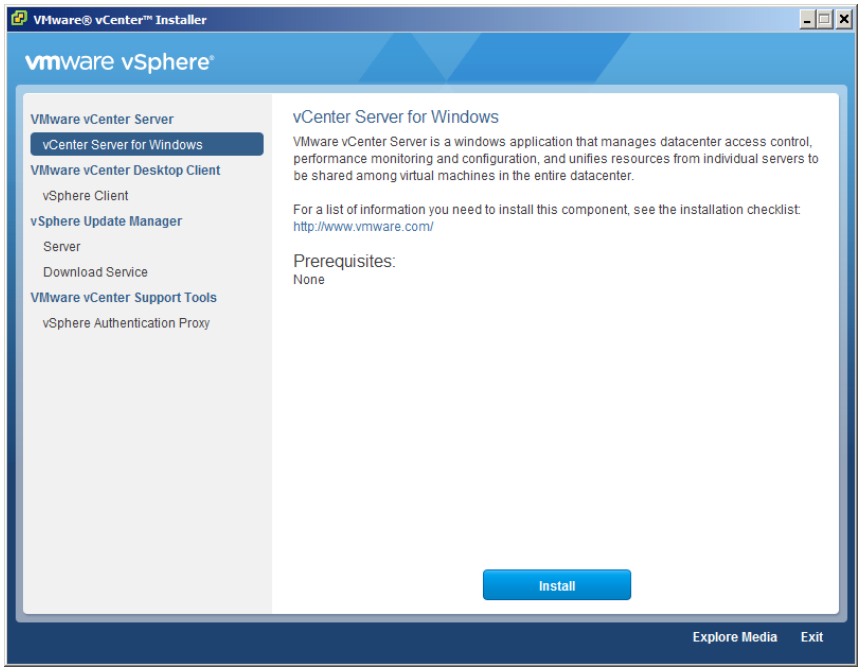


Figure 3.2

3. Read and accept the terms of the End User License Agreement displayed. Click **Next** (see *Figure 3.3*).

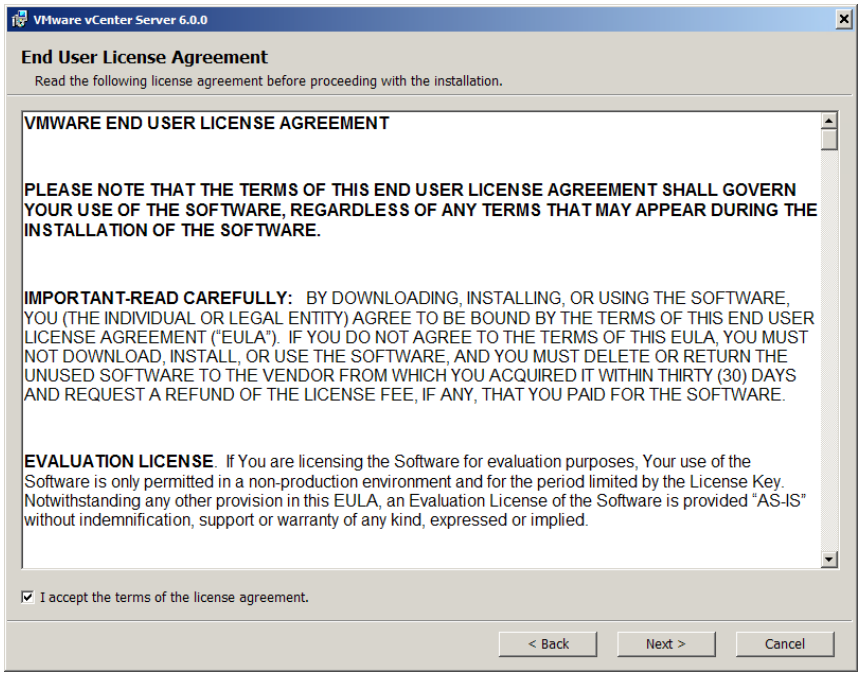


Figure 3.3

4. Select the deployment type. In this installation walkthrough, the **Embedded Deployment** was used. Click **Next** (see *Figure 3.4*).

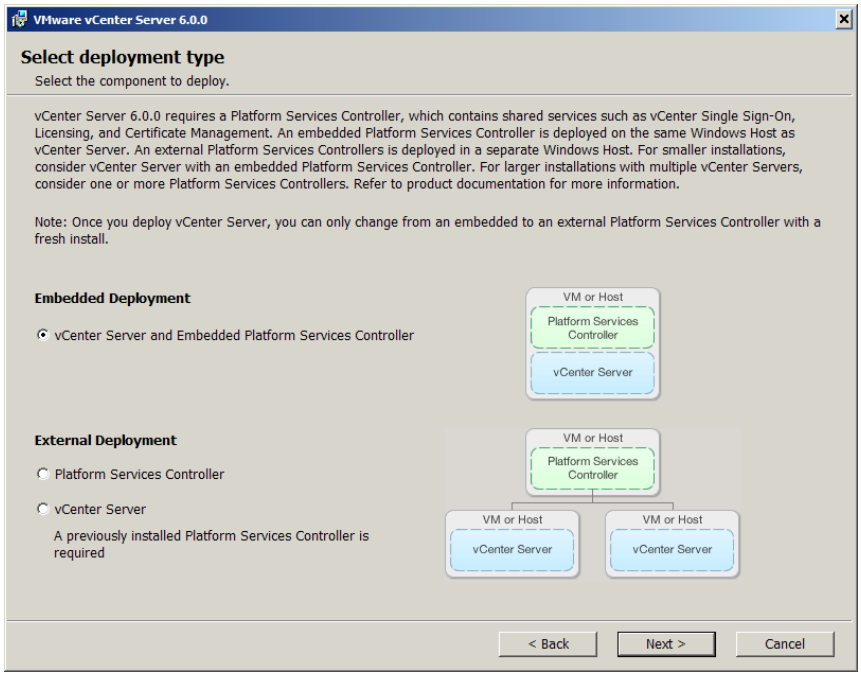


Figure 3.4

5. Enter the System Network Name (see *Figure 3.5*).

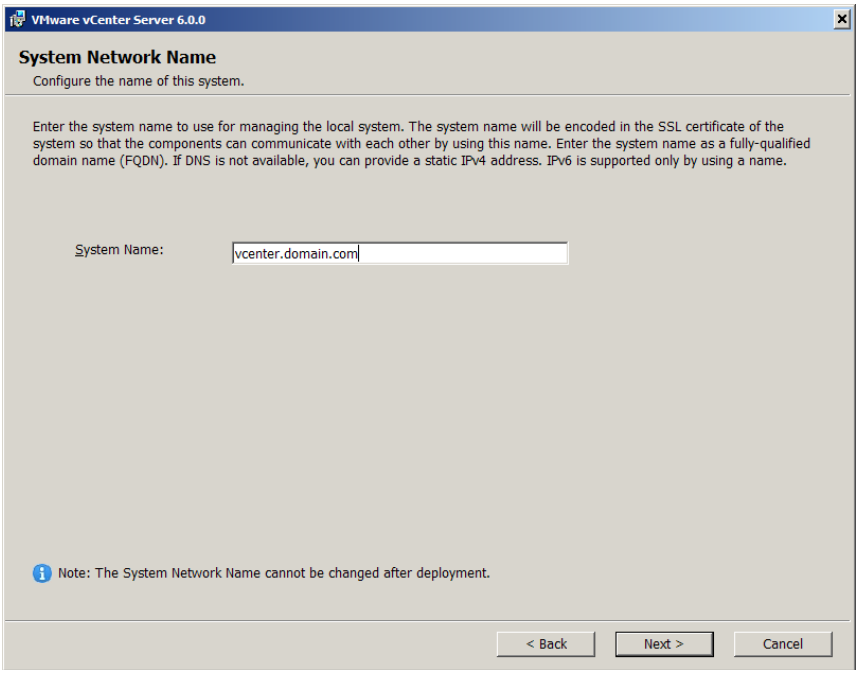


Figure 3.5

5. Set vCenter Single Sign-On domain and click **Next** (see *Figure 3.6*).

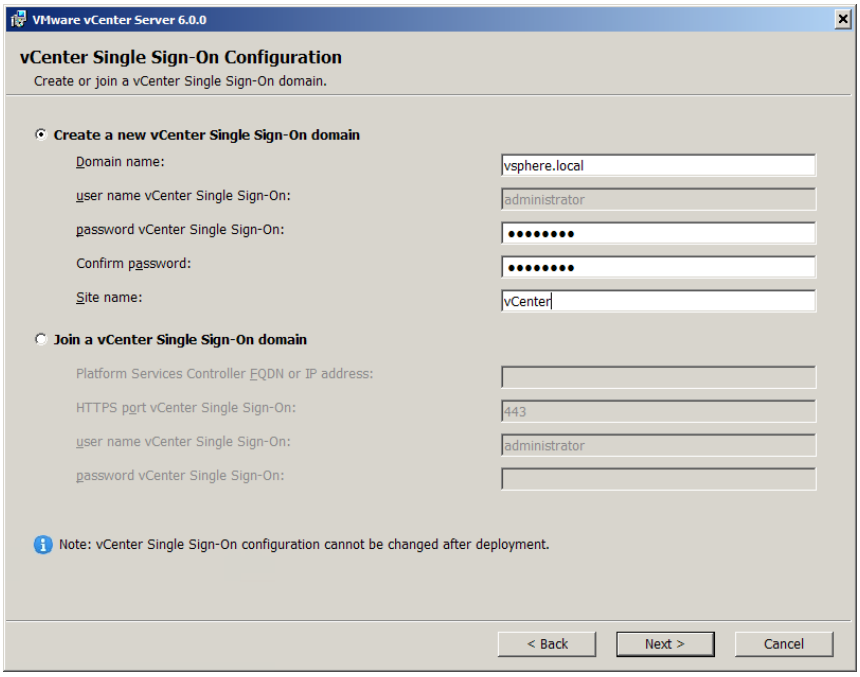


Figure 3.6

7. Specify a vCenter Server Service Account for logging into vCenter with the vSphere Client. Click **Next** (see *Figure 3.7*).

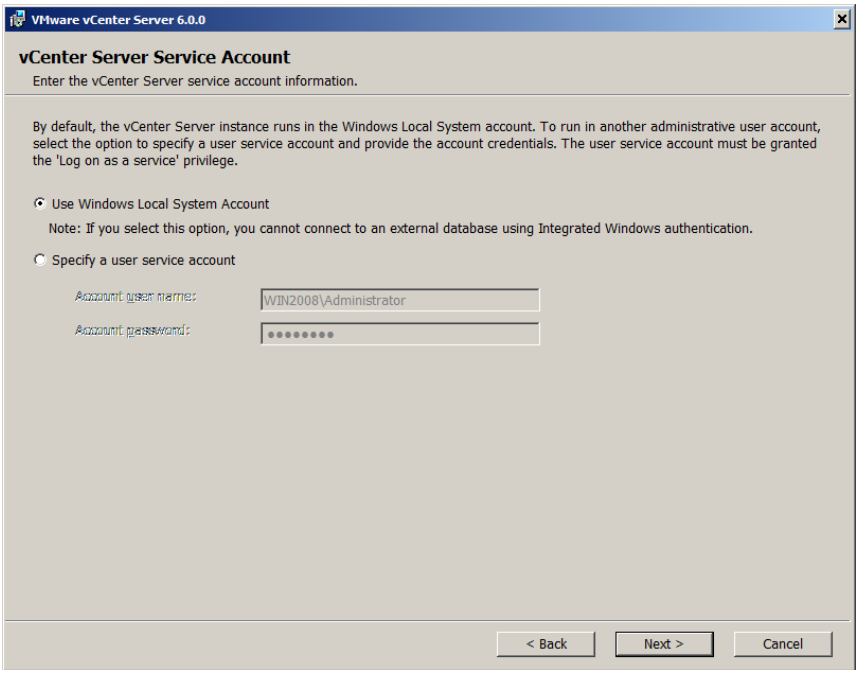


Figure 3.7

8. Select a database for deployment (see *Figure 3.8*).

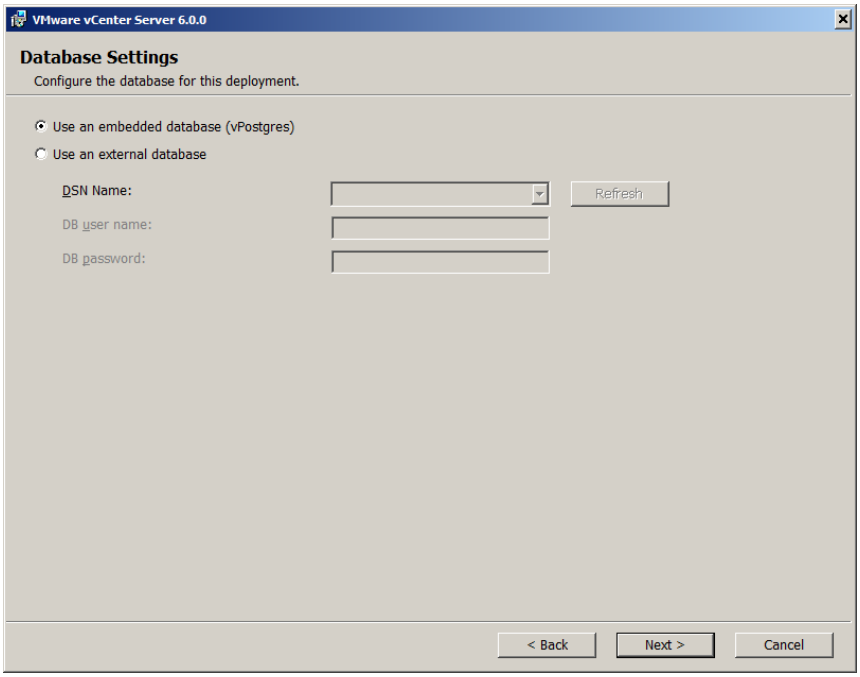


Figure 3.8

NOTE: The embedded PostgreSQL database can be used in environments of up to 20 ESXi hosts and 200 virtual machines. Larger infrastructures require a supported external database, such as Oracle or MS SQL.

9. Configure ports. You may leave the default settings (see *Figure 3.9*).

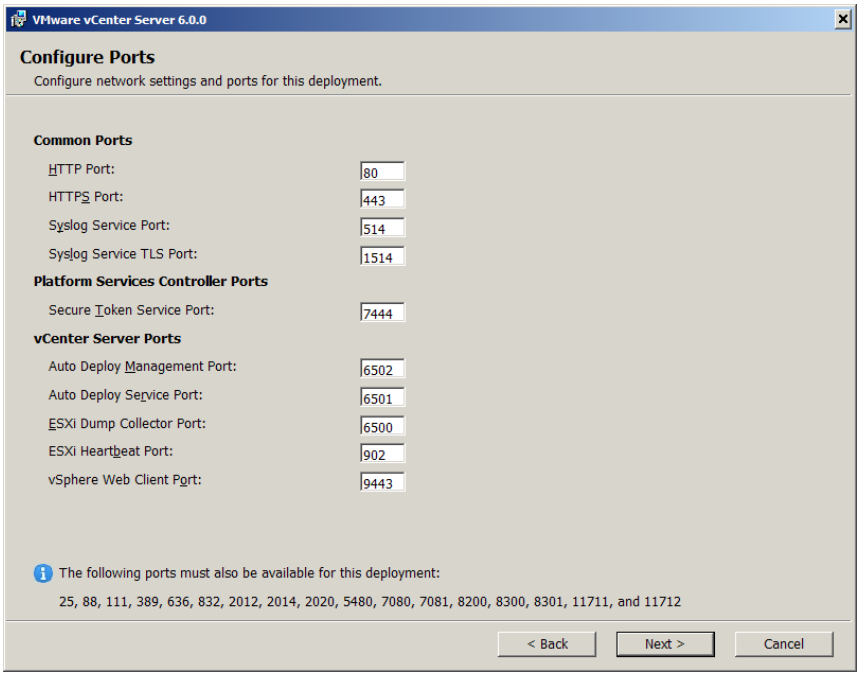


Figure 3.9

10. Select the destination directory (see *Figure 3.10*).

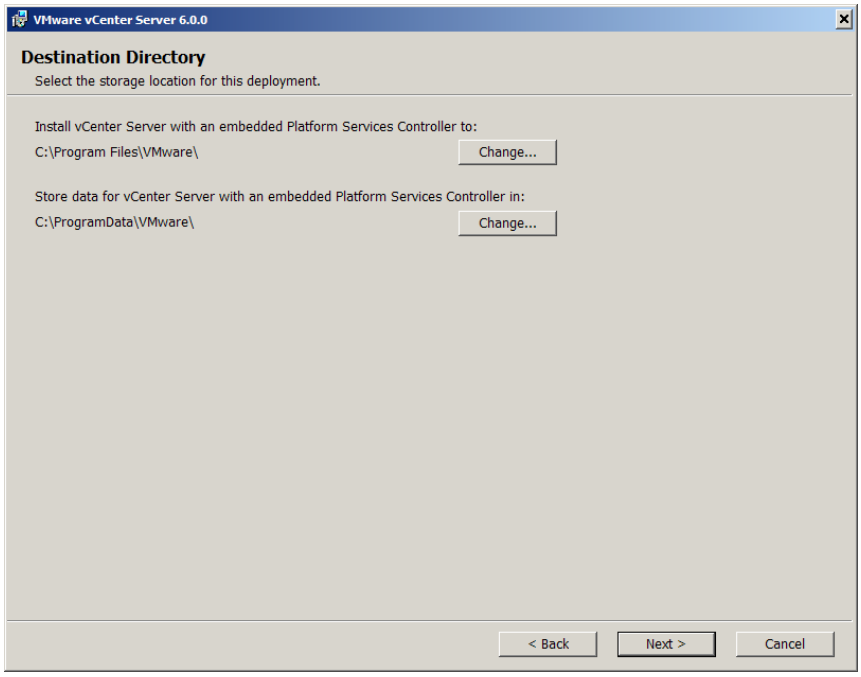


Figure 3.10

11. Tick the checkbox near **Join the VMware Customer Experience Improvement Program**, if you want to participate (see *Figure 3.11*).

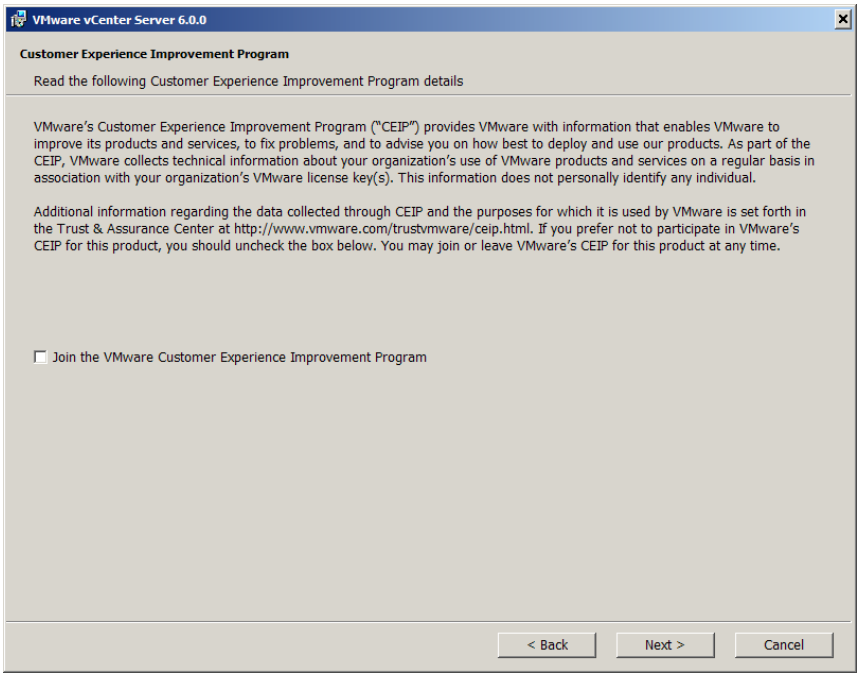


Figure 3.11

12. View the installation summary and click **Install** (see *Figure 3.12*).

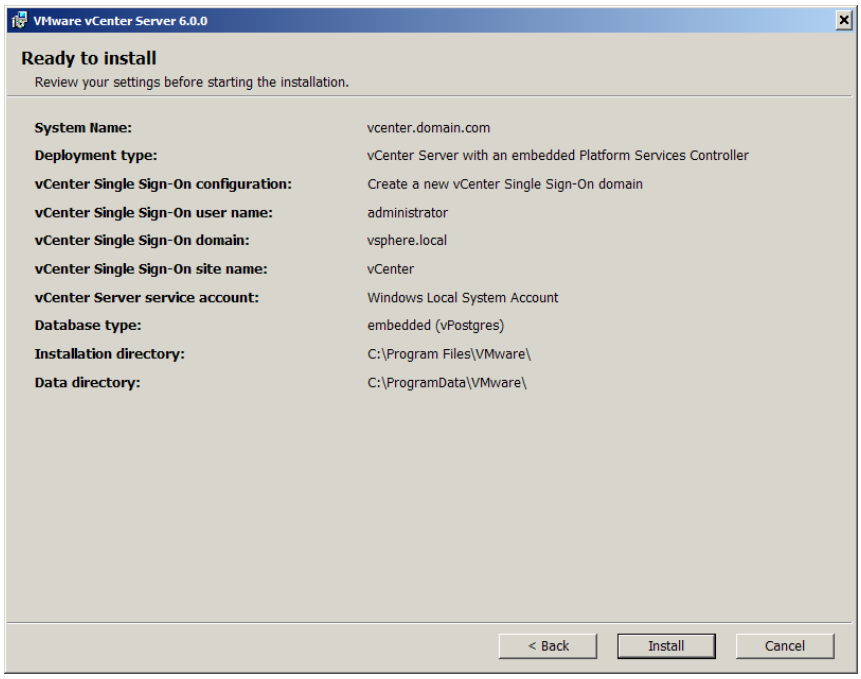


Figure 3.12

Wait for the installation process to complete (see *Figure 3.13*).

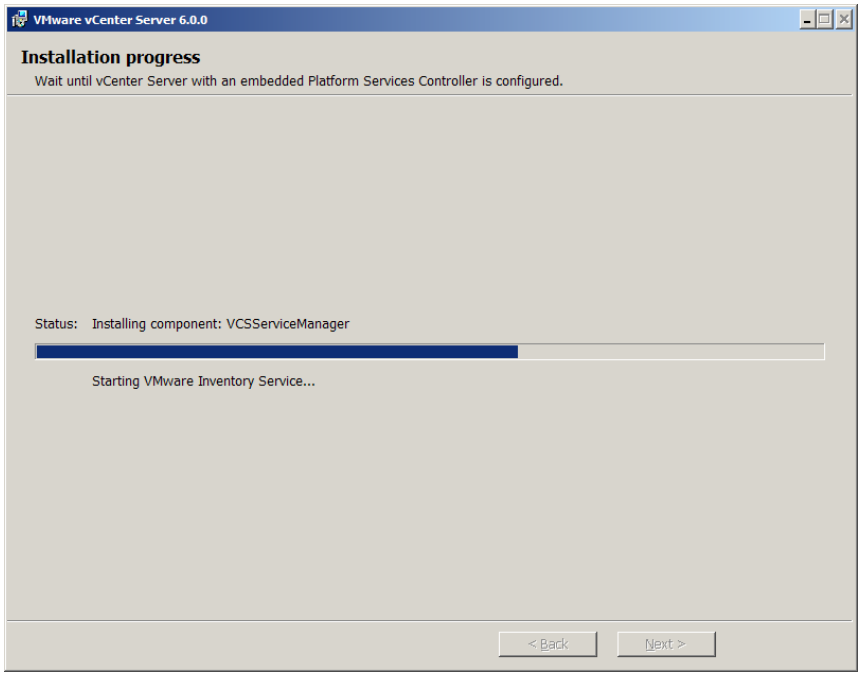


Figure 3.13

You can now launch **vSphere Web Client** (see *Figure 3.14*).

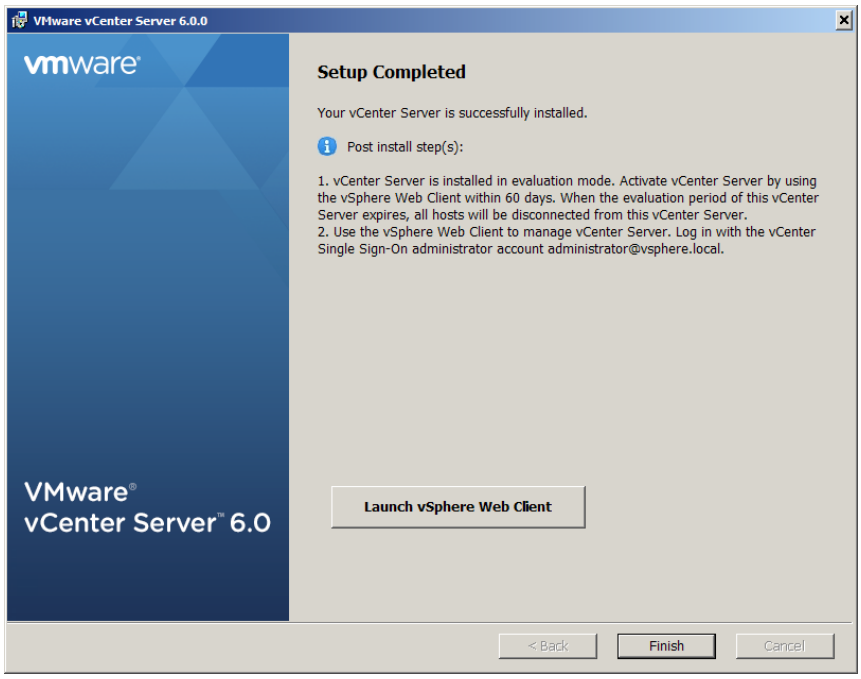


Figure 3.14

Setting up a Shared Datastore

For high availability, ESXi hosts need access to shared data storage resources.

To set up a shared datastore, take the following steps:

1. Browse hosts and clusters in the vSphere Web Client, select a host, then click the **Manage** tab. Select the **Storage** subtab.
2. Click **Storage Adapters** to view the list of available adapters (see *Figure 4.1*).

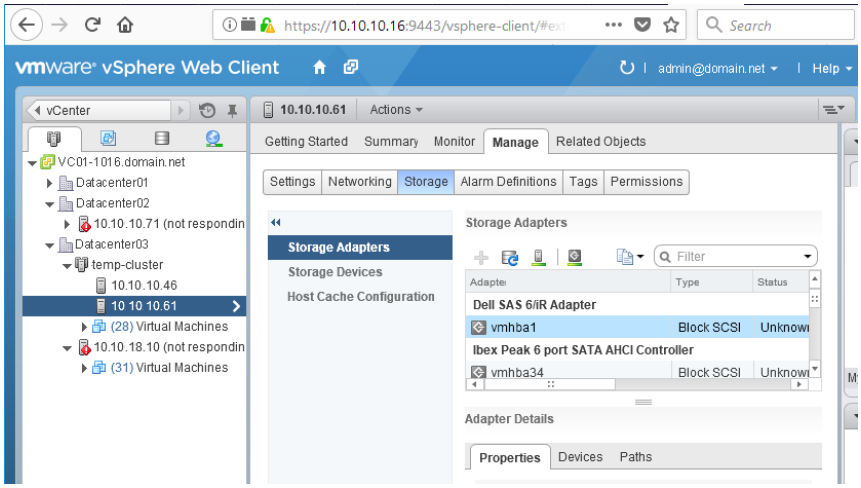


Figure 4.1

3. Click **Storage Devices** to view the list of available devices (see *Figure 4.2*).

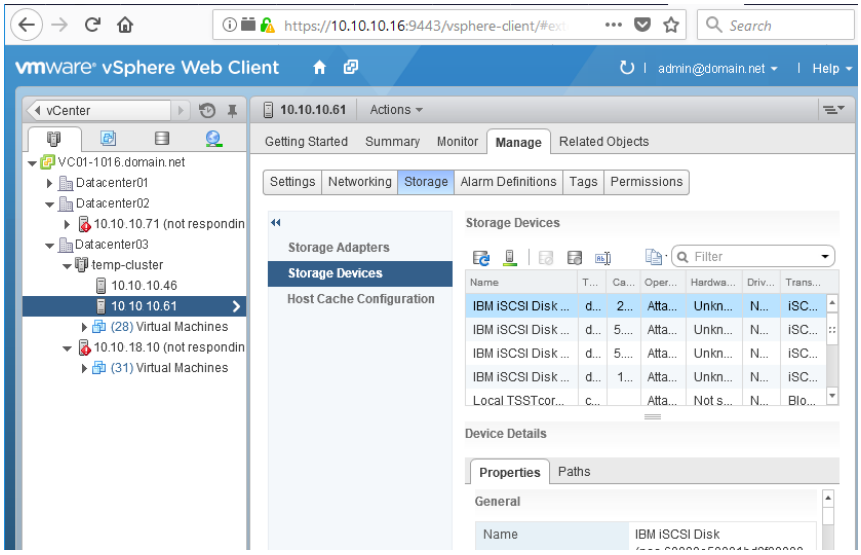


Figure 4.2

4. Go to **Home -> vCenter -> Datastores**. Click the **Create a new datastore** icon to add the shared datastore you want (see *Figure 4.3*).

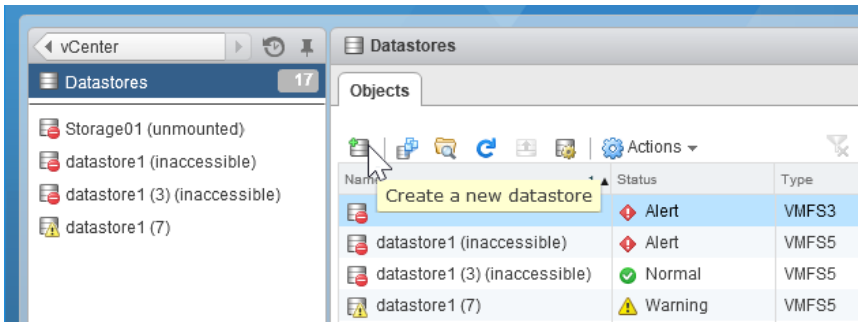


Figure 4.3

5. Select the IP address of the datastore you want to connect via network using the NFS, iSCSI, or Fibre Channel protocols (see *Figure 4.4*).

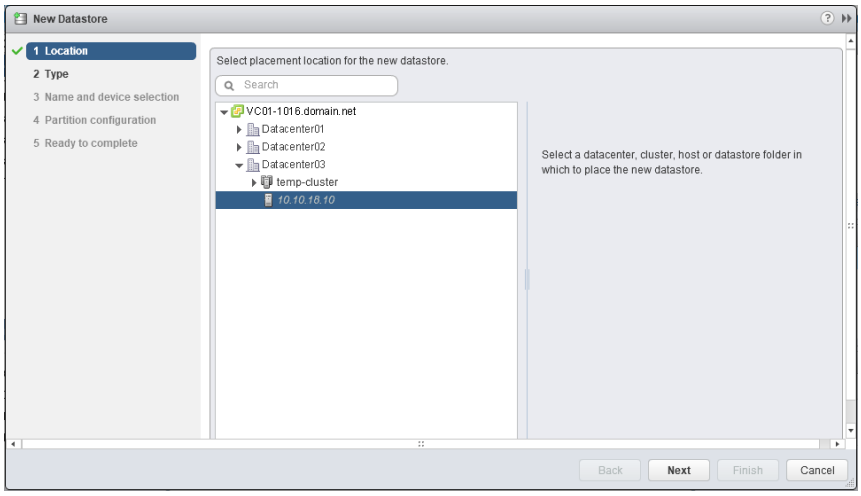


Figure 4.4

NOTE: The recommended redundant storage network scheme is as follows: two ESXi hosts connected via redundant network to a SAN with two storage processors. However, you can use a NAS server for this purpose (see *Figure 4.5*).

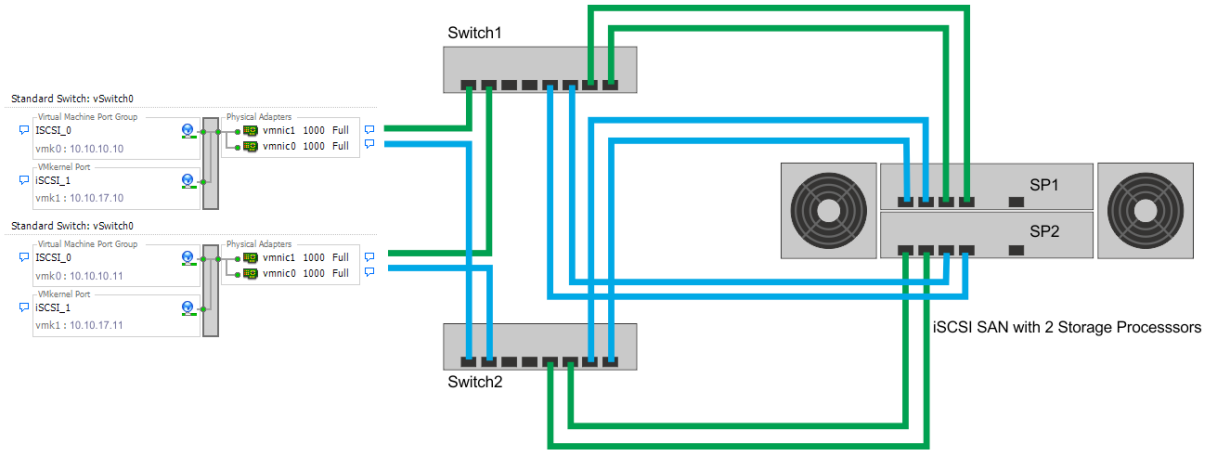


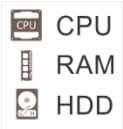
Figure 4.5

Connecting Hosts in Clusters

Now that the ESXi server, Domain Controller, and vCenter Server are installed, with a Shared Datastore (NAS or SAN) set up, you can create a cluster.

There are several ways to connect hosts in clusters:

NOTE: The icons in the diagrams below signify the following:



1. In this scenario, the Domain Controller and vCenter Server are installed on physical machines (see Figure 5.1). Bear in mind that if you use this setup initially, you can always use VMware vCenter Converter to convert a physical machine into a virtual machine at any time. You could thus migrate vCenter Server or Domain Controller to the vSphere environment later.

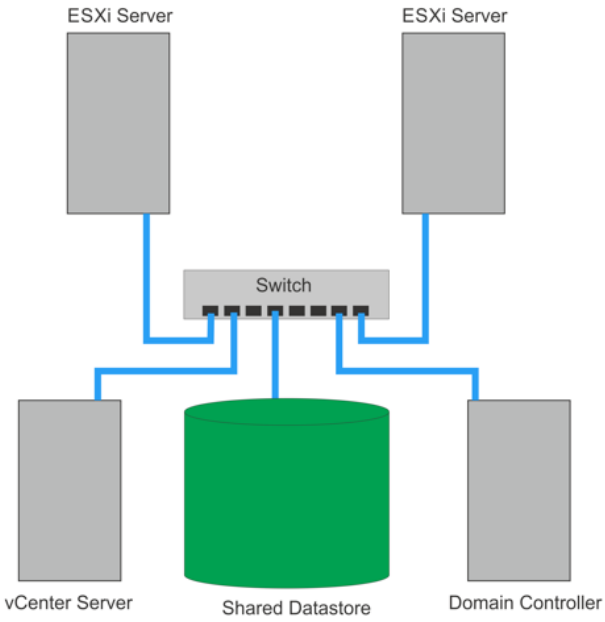


Figure 5.1

2. In this scenario, vCenter Server is a virtual machine that is installed on an ESXi server, using the CPU, RAM, and storage of the ESXi server (see *Figure 5.2*).

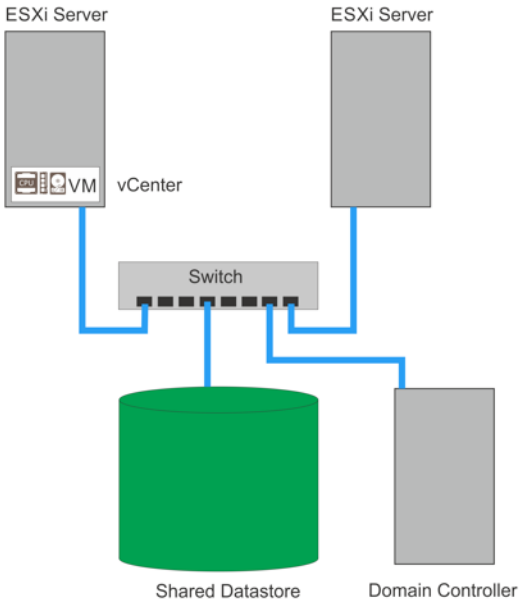


Figure 5.2

3. vCenter Server is a virtual machine running on an ESXi Server that uses CPU and RAM of the ESXi server, but the virtual disk is stored on a shared datastore (see Figure 5.3). This method of connecting hosts in a cluster allows you to use clustering features, such as High Availability, the Distributed Resource Scheduler, and Fault Tolerance.

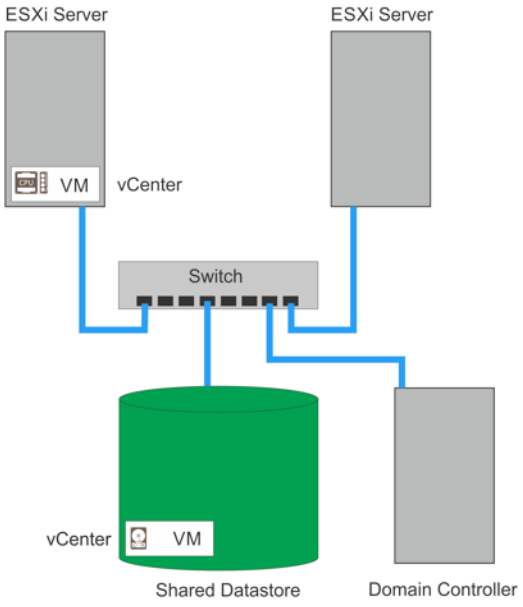


Figure 5.3

4. Domain Controller as well as vCenter Server are both installed and running on an ESXi server. They are using CPU, RAM, and storage resources of the ESXi server (*Figure 5.4*).

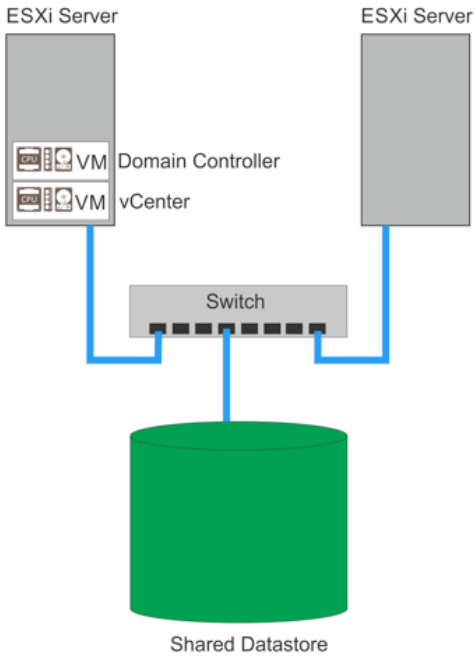


Figure 5.4

5. Domain Controller and vCenter Server are running on ESXi Server. They are using CPU, RAM, and storage of the ESXi server, but virtual disks of these VMs are stored on the shared datastore (Figure 5.5). This connection method offers similar advantages to Scenario 3.

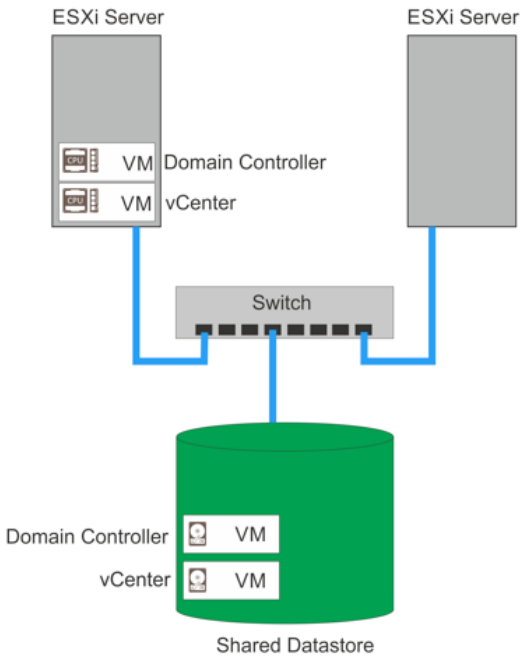


Figure 5.5

To create a cluster, take the following steps:

1. Log in to vCenter with vSphere Client or vSphere Web Client. In order to log in, enter vCenter IP and port 9443 in the address bar.

NOTE: vSphere Client is a C#-based locally installed application for Windows only. vSphere Web Client is a cross-platform web application. Both vSphere Client and vSphere Web Client can connect to vCenter, or directly with ESXi hosts with the full range of administrative functionality. Since vCenter Server 5.1, VMware recommends using the vSphere Web Client to administer virtual environments. For older versions of vSphere Web Client, you may need to install a Flash player plugin. The newest versions of vSphere Web Client use HTML5 rather than Flash.

This is how the main screen of vSphere Web Client interface looks (see *Figure 5.6*):

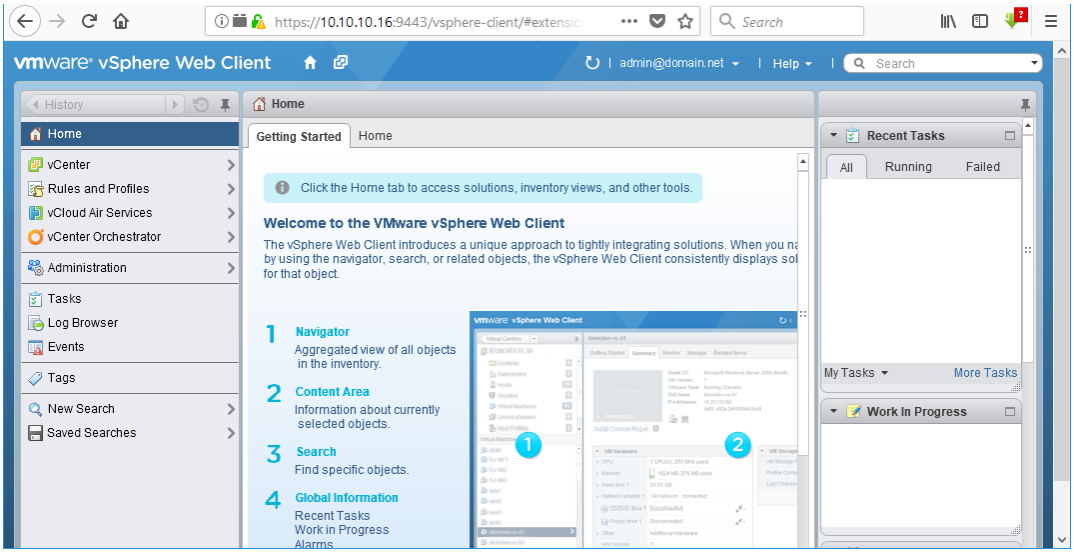


Figure 5.6

2. In the left pane of the vSphere Web Client interface, select **vCenter -> Datacenters –> New Datacenter** to create a new datacenter.

NOTE: A datacenter is a container for all the inventory objects required for a fully functional environment for virtual machine operation. You can create multiple datacenters for each department in your enterprise, or for different purposes, such as low- and high-performance tasks. Your virtual machines can hot-migrate from one ESXi host to another ESXi host within the same datacenter. However, they cannot migrate from a host in one datacenter to a host in a different datacenter.

3. Type the name for your new datacenter (in our case – “Datacenter03”; (see *Figure 5.7*).

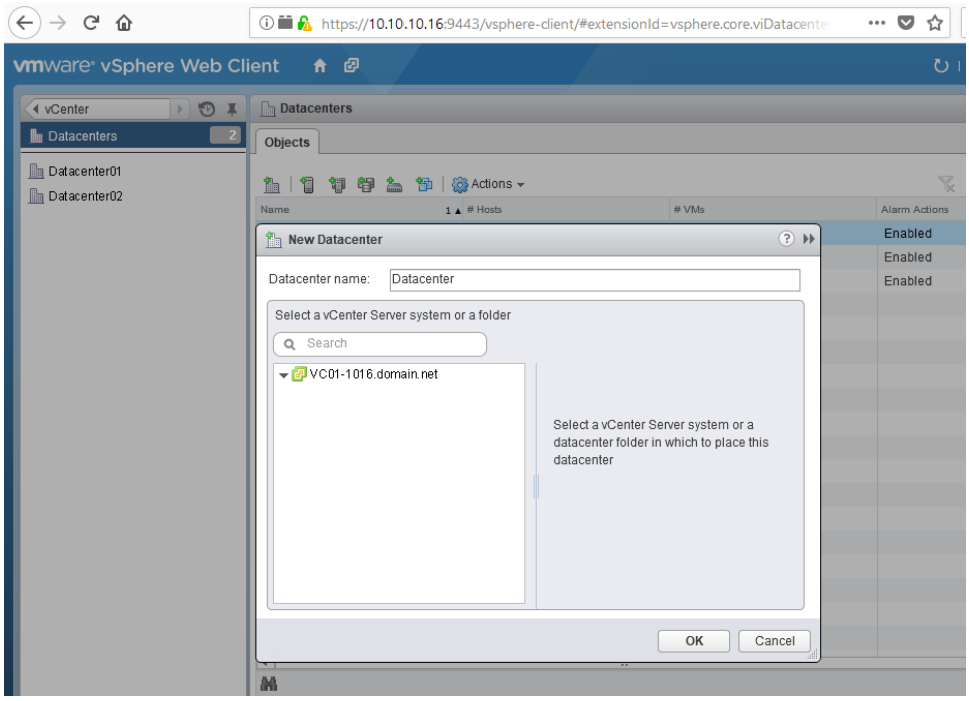


Figure 5.7

4. Add your ESXi host(s) to the Datacenter. Right-click on the newly created datacenter and select **Add Host**. Enter the IP address and root credentials of your ESXi host on the Connection Settings page of the Add Host Wizard. Do the same for each ESXi host you want added to the datacenter.

Now, right-click on the newly created datacenter and select the **Create New Cluster** option (see *Figure 5.8*).

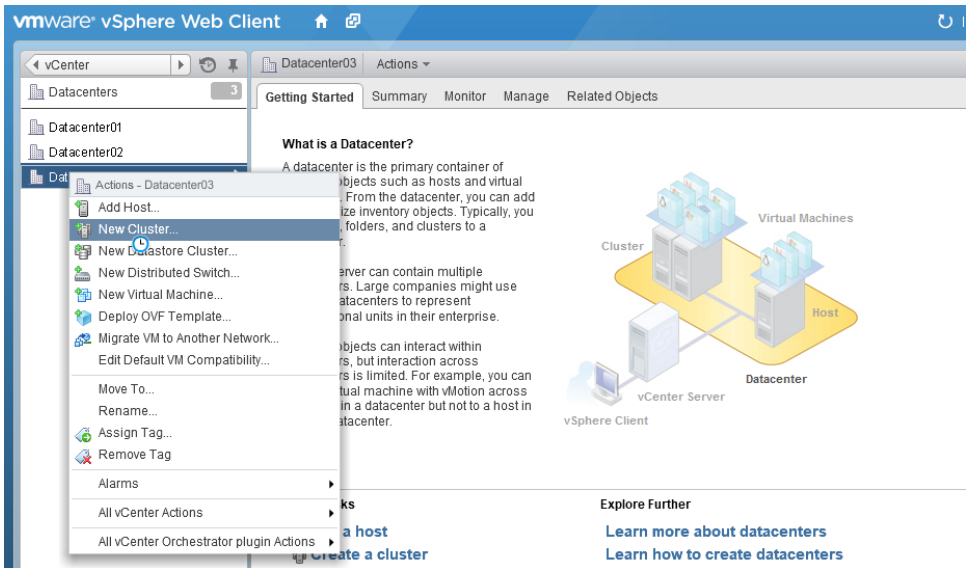


Figure 5.8

5. Set a name for your cluster. Leave the checkboxes for the DRS and vSphere HA options unticked (you can add these functionalities later; see *Figure 5.9*).

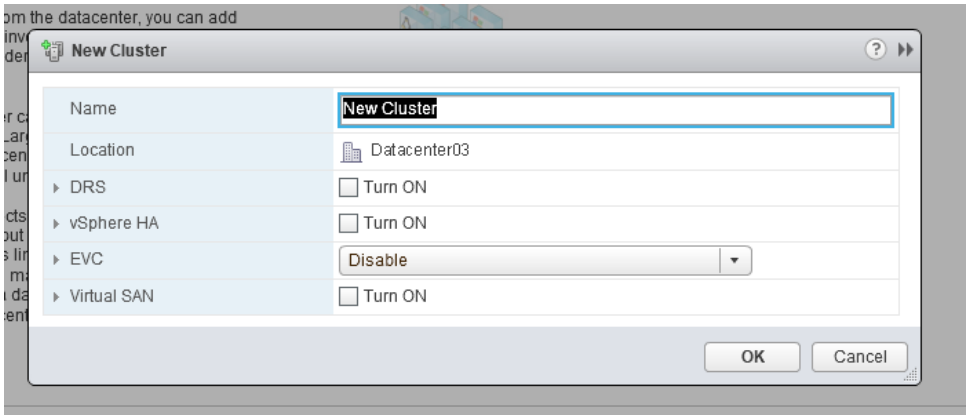


Figure 5.9

6. Add ESXi hosts to the cluster. Note that your ESXi hosts must belong to the same datacenter. Click "**Add Host...**" (see *Figure 5.10*).

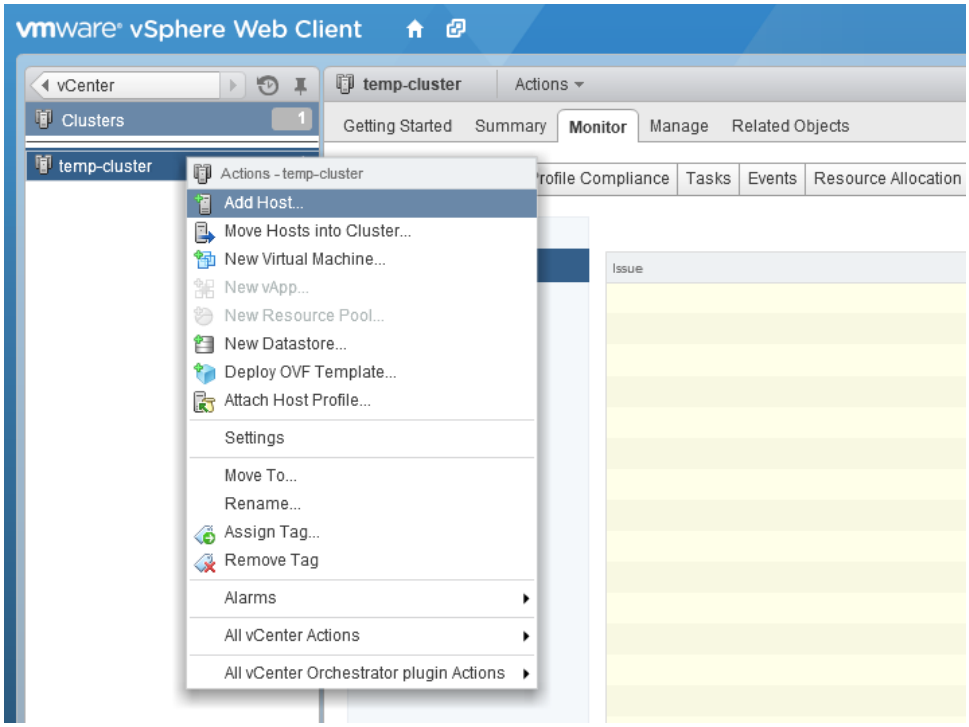


Figure 5.10

7. Enter the name or IP address of the ESXi host you want added to your cluster (see *Figure 5.11*).

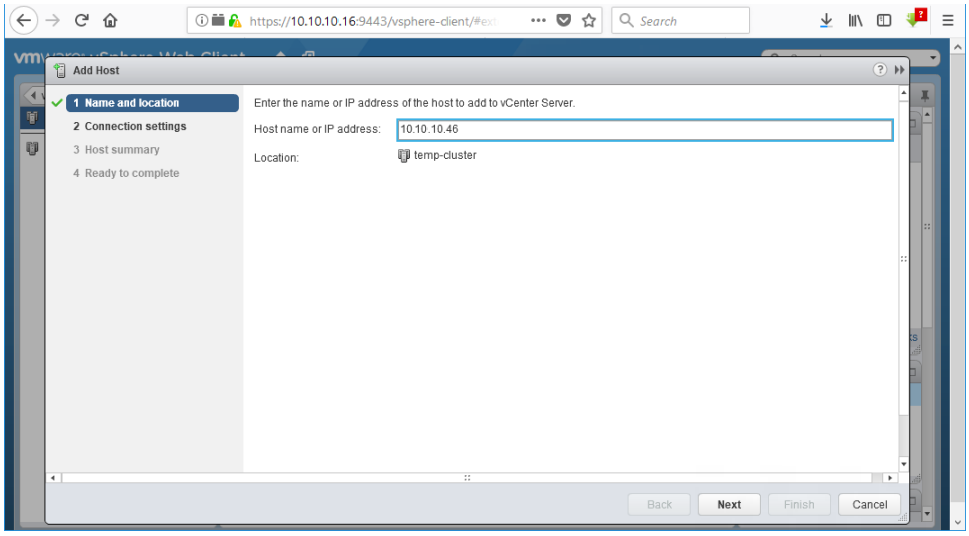


Figure 5.11

8. Enter the username and password for the administrative account of the ESXi host (*see Figure 5.12*). The root user is the administrator by default.

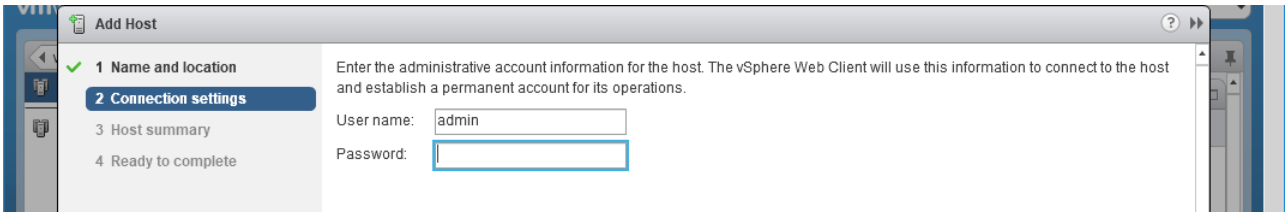


Figure 5.12

9. Assign a license, if needed. You may try a 60-day Evaluation license.

10. Leave the lockdown mode disabled and click **Next** (see Figure 5.13).

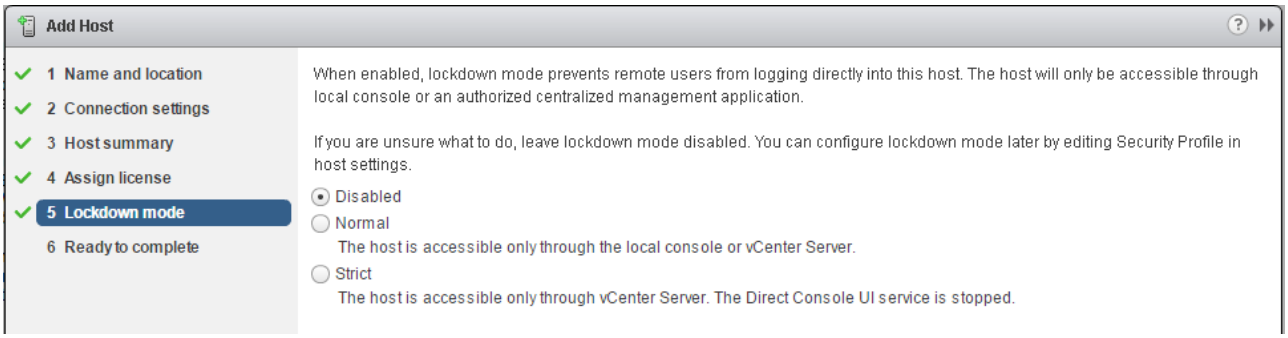


Figure 5.13

11. Set the resource pool. This option defines what to do with existing virtual machines and resource pools on the ESXi host. If there are no virtual machines on the ESXi host, accept the default option. Click **Next** (see *Figure 5.14*).

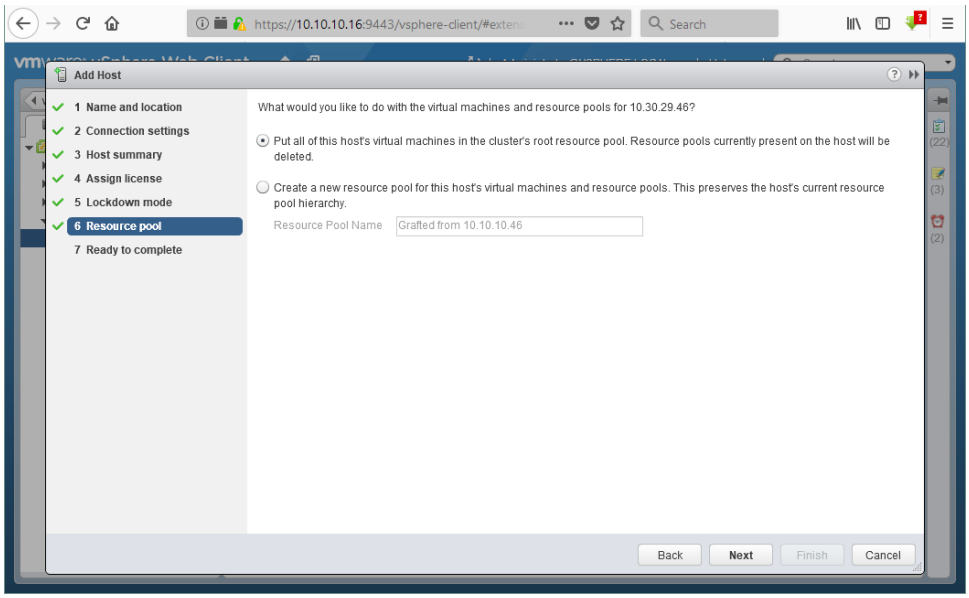


Figure 5.14

12. At the final screen, click **Finish**.

NOTE: Repeat steps 6 through 12 for each ESXi host that you want added in the cluster.

Configuring Network for the Cluster

To configure the network for your cluster, take the following steps:

1. Go to **ESXi host -> Manage -> Networking**.

NOTE: You can view or change the settings of physical network controllers, virtual network controllers, and virtual switches from your vSphere Web Client (see *Figure 6.1*).

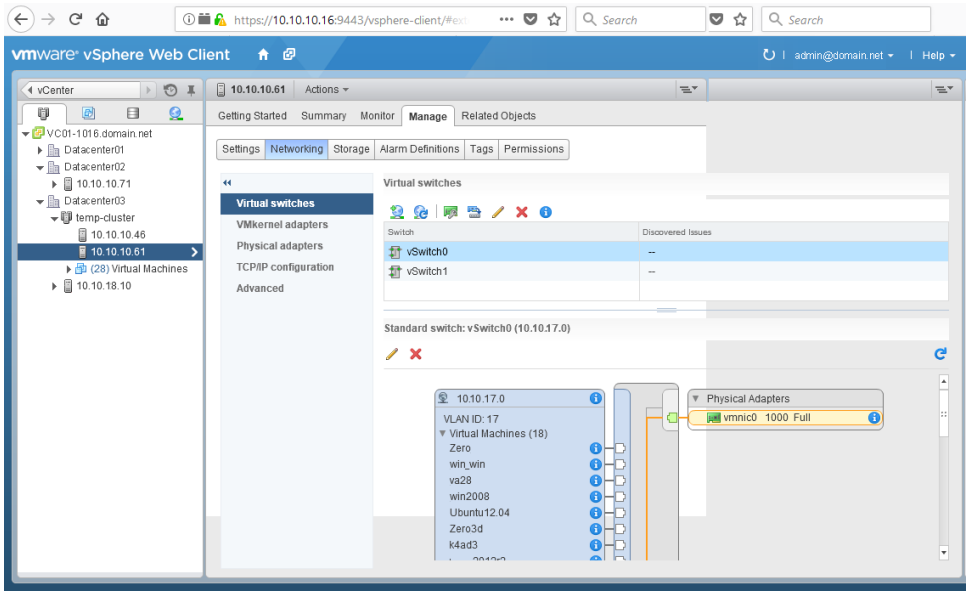


Figure 6.1

Physical adapters are hardware network adapters of ESXi servers (see *Figure 6.2*).

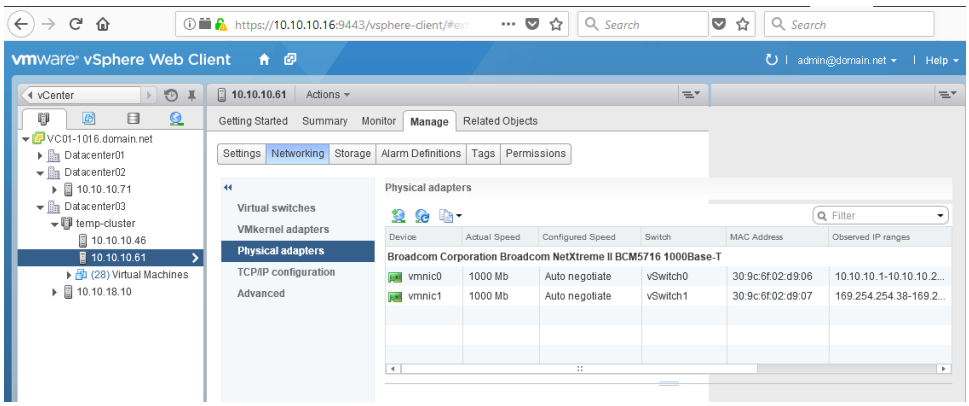


Figure 6.2

The standard Maximum Transmission Unit (MTU) of a Frame is 1500 Bytes. In the Properties tab, you can set the MTU value as high as 9000 Bytes to enable using Jumbo Frames, if needed (see *Figure 6.3*).

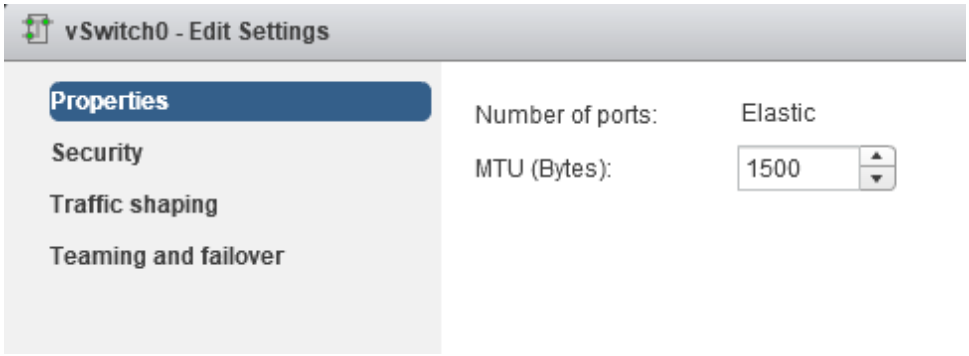


Figure 6.3

The VMkernel network adapter is used to provide network connectivity for hosts as well as handling system traffic for vSphere vMotion, IP storage, Fault Tolerance logging, and vSAN (see *Figure 6.4*).

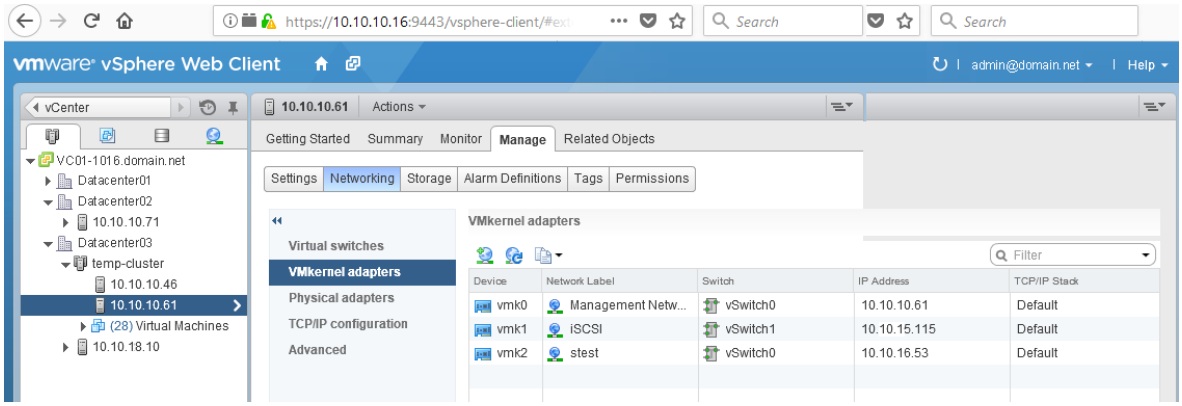


Figure 6.4

2. Add a Virtual Switch

If there are more than two Network Interface Controllers (NICs) available in the ESXi server, create two virtual switches. One of them should host the Service Console and VMkernel (including iSCSI as well as vMotion traffic). The other should be dedicated to virtual machine traffic. The NICs carrying the iSCSI traffic should be connected to redundant Ethernet switches (see *Figure 4.5* above).

There are two types of virtual switches (vSwitches) in vSphere: standard and distributed. The standard virtual switch is configured manually on each host and is used for small environments. The Distributed vSwitch allows you to manage networks for multiple hosts from a single vCenter interface. Use the standard switch for the purposes of this walkthrough.

To edit virtual switches, go to **Manage –> Networking –> Virtual switches** (Figure 4.6 above).

Select a virtual switch and click the **Edit Settings** icon. In the **Teaming and Failover** tab, you can set active adapters, standby adapters, and unused adapters.

Active adapters use the uplink if the network adapter connectivity is up and active.

Standby adapters use this uplink if one of the active physical adapters is down.

3. Click the **Add host networking** icon (see *Figure 6.5*).

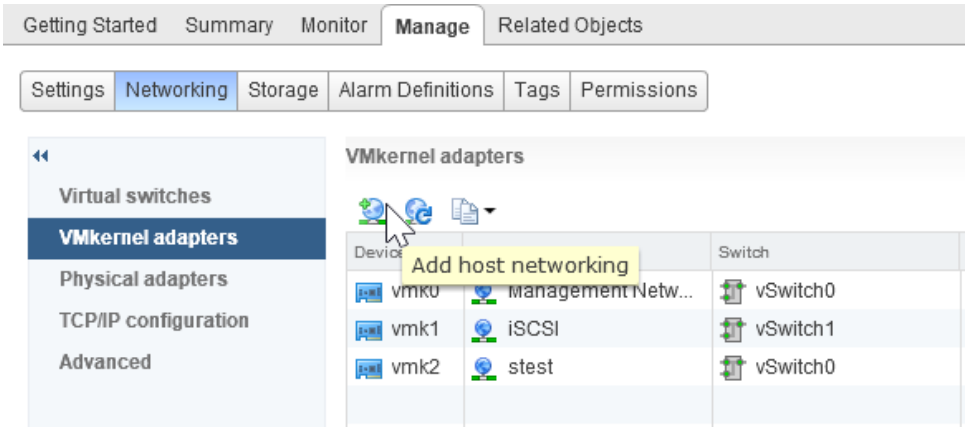


Figure 6.5

Here you can select VMkernel Network Adapter (see *Figure 6.6*).

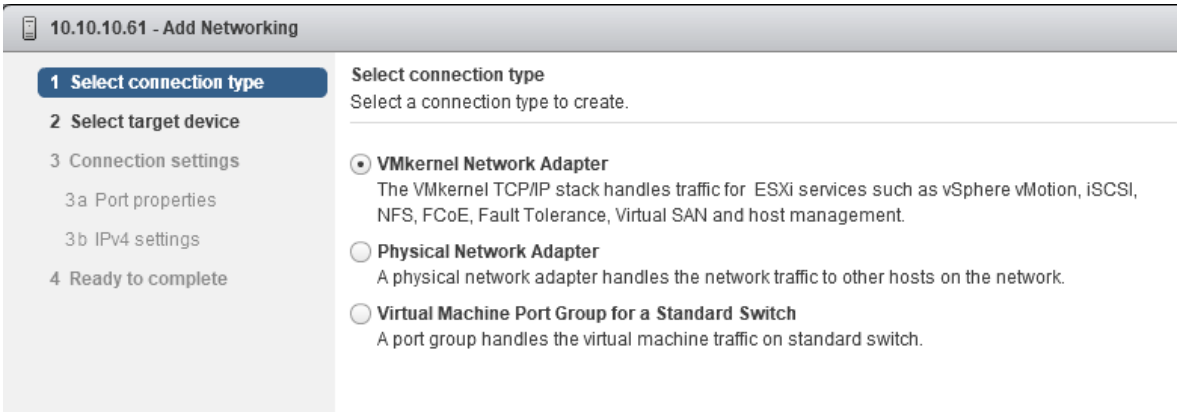


Figure 6.6

4. Select **New standard switch** as a target device (see *Figure 6.7*).

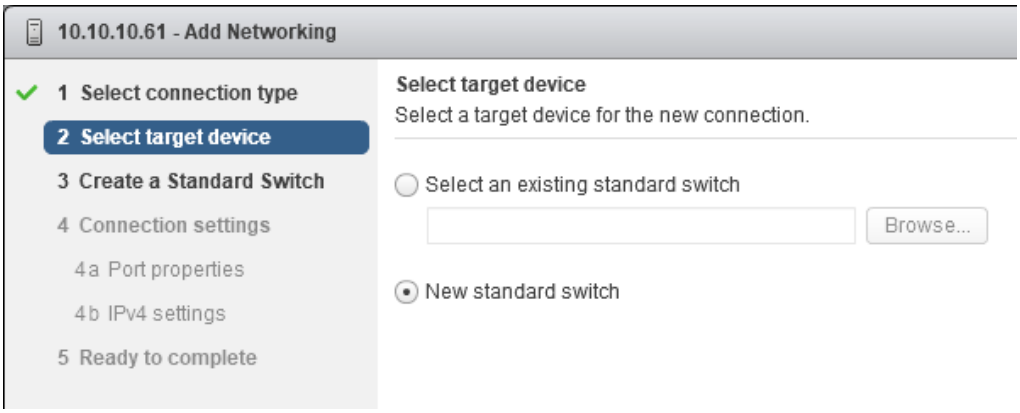


Figure 6.7

5. Configure an IP address for the new VMkernel port and select the appropriate services to be used for the cluster. These could include vMotion traffic, provisioning traffic, Fault Tolerance logging, management traffic, vSphere replication traffic, vSphere replication NFC traffic, and/or Virtual SAN traffic.

NOTE: If you already have a virtual adapter created, you can select this adapter and edit settings by clicking the **Edit Settings** icon (see *Figure 6.8*).

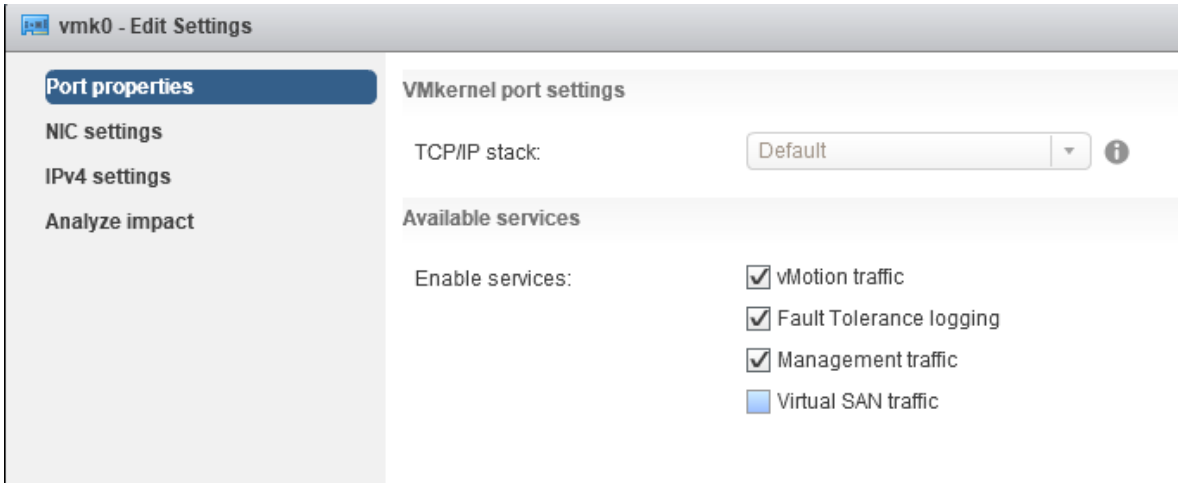


Figure 6.8

Below, you can see an example of a vMotion virtual network scheme (see *Figure 6.9*):

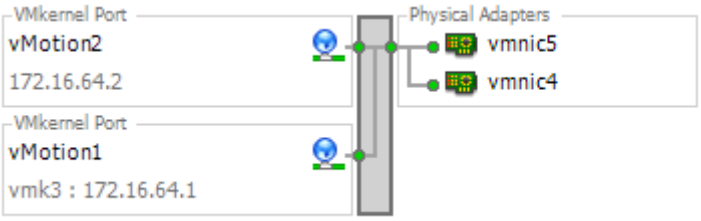


Figure 6.9

vMotion is a feature that lets you hot-migrate powered-on virtual machines from one ESXi host to another. Enable vMotion if you want to create a DRS or HA cluster. Separate the vMotion network, the storage network, and the production network. This can help you prevent overloading and reduce network bandwidth usage (see *Figure 6.10*).

NOTE: The production network is the network to which your physical computers (workstations), routers, printers, etc. are connected.

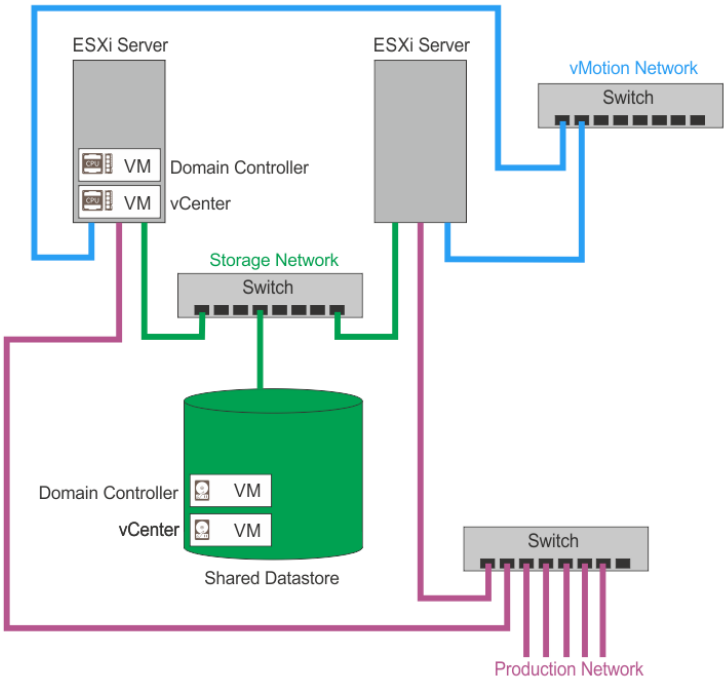


Figure 6.10

Now that you have created a cluster, you can set up the DRS and/or HA features.

How to Create a DRS Cluster

In order to create a Distributed Resource Scheduler cluster, take the following steps:

1. Go to **vCenter -> Cluster** and select your cluster (in the example, our cluster is named “temp-cluster”)
2. Click **Settings**, select **vSphere DRS** and click **Edit** (see *Figure 7.1*).

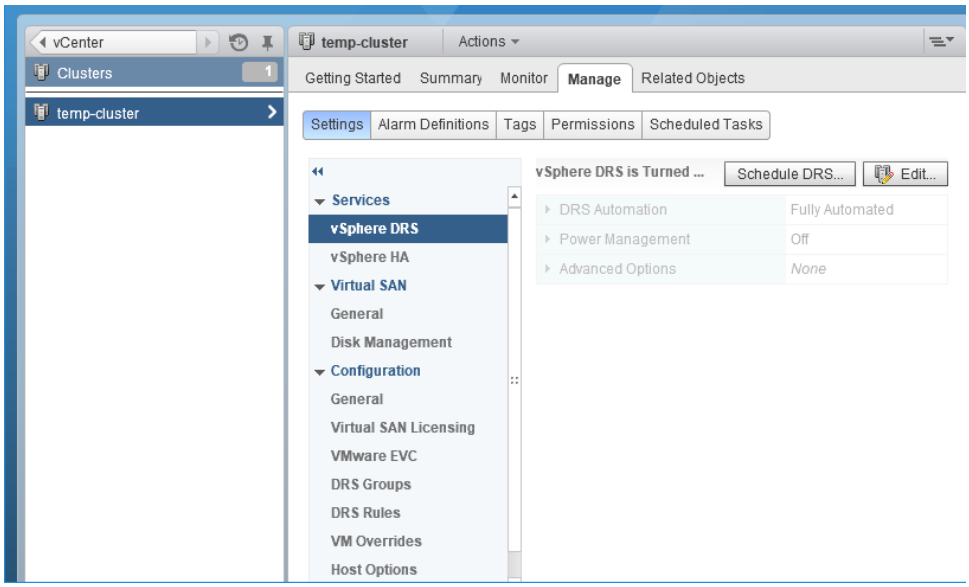


Figure 7.1

3. Mark the **Turn on vSphere DRS** checkbox.

4. Configure the Automation Level, Migration Threshold, and Virtual Machine Automation settings. There are useful tips displayed in the vSphere client interface that can help you understand what settings could best meet your needs (see *Figure 7.2*).

- Under **Automation Level**, you can select Manual, Partially Automated, or Fully Automated for the level of Load Balancing automation.
- **Migration Threshold** is the option that controls how conservatively or aggressively the DRS runs. You can set the threshold at a value from 1 to 5. Migration Threshold 1 means that only migration recommendations of the highest priority are executed. The only such instances are affinity rules that you set yourself, or a host entering Maintenance Mode. Cluster imbalance or VM demand do not result in migrations. Aside from Migration Threshold 1, Migration Threshold 2 is the most conservative and Migration Threshold 5 is the most aggressive. The higher the Migration Threshold, the more migrations are allowed. Thus, at Migration Threshold 5, the DRS executes recommended migrations even if they can only yield very slight benefits to performance or cluster balance, whereas at Migration Threshold 2, the potential benefits must be very significant.
- **Virtual Machine Automation** is the option that allows setting custom automation levels for VMs.

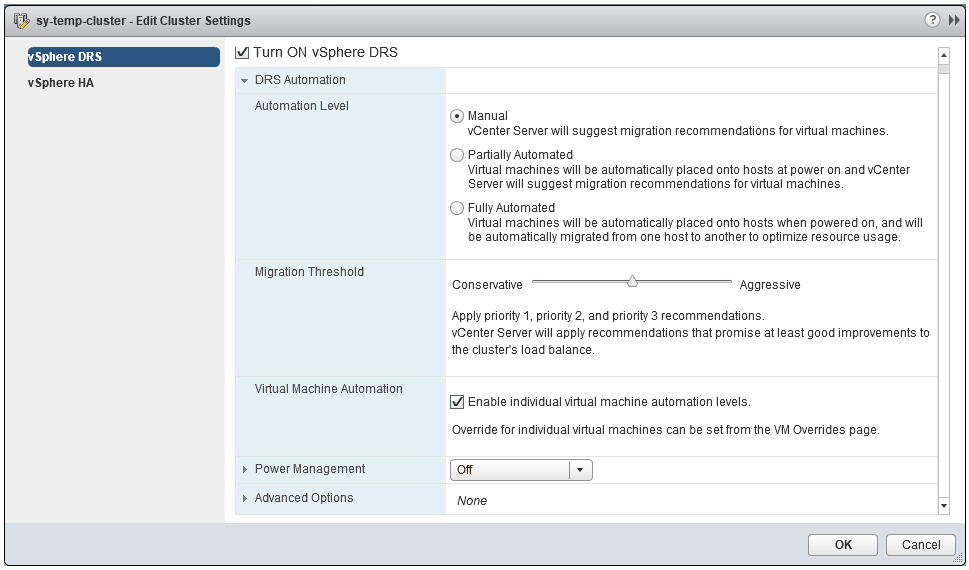


Figure 7.2

5. Set the Power Management settings (see *Figure 7.3*).

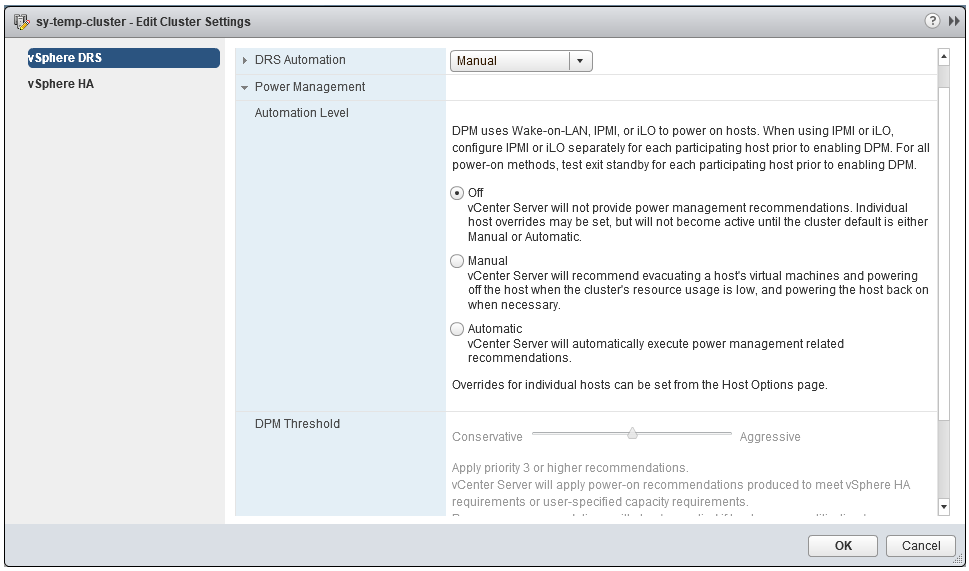


Figure 7.3

VMware Distributed Power Management (DPM) supports three power management protocols to bring a host out of standby mode:

- Intelligent Platform Management Interface (IPMI);
- Hewlett Packard Enterprise Integrated Lights-Out (iLO);
- Wake-on-LAN (WOL).

Each of these protocols requires separate hardware support and configuration. If a host does not support any of these protocols, this host cannot be put into a standby mode by the DPM. If a host supports multiple protocols, they are used in the following order: IPMI, iLO, WOL.

6. Add Affinity Rules, if necessary.

NOTE: Affinity Rules allow you to control the placement of virtual machines that interact in particular ways with each other. For example, if you run a database server, a web server, and an application server on different virtual machines, and they interact closely, you can create an affinity rule to place ensure they reside on the same ESXi host. This would reduce network load and can increase performance.

Go to **vCenter -> Hosts and clusters**. Select your cluster. Then click the **Manage tab -> Settings -> DRS Rules** (see *Figure 7.4*).

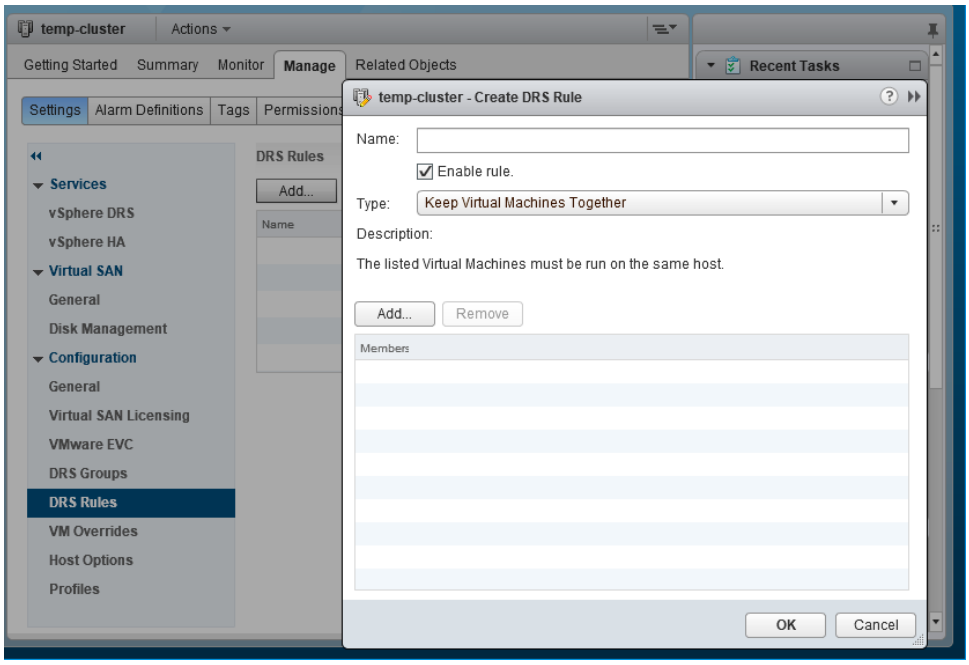


Figure 7.4

Choose from three types of affinity rules: Keep Virtual Machines Together (affinity), Separate Virtual Machines (anti-affinity), and Virtual Machines to Hosts (affinity or anti-affinity)

How to Create a HA Cluster

In order to create a High Availability cluster, take the following steps:

1. Go to **vCenter -> Cluster** and select your cluster (temp-cluster in this walkthrough's case).
2. Click **Settings**.
3. Select **vSphere HA** and click **Edit** (see *Figure 7.5*).

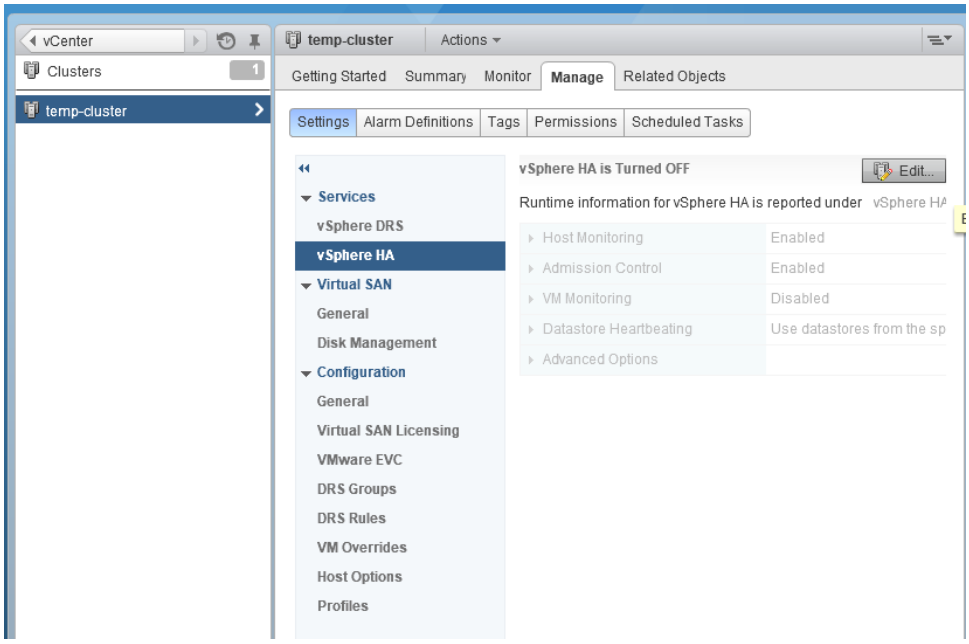


Figure 7.5

4. Tick the **Turn on vSphere HA** checkbox and set the following options (see *Figure 7.6*).

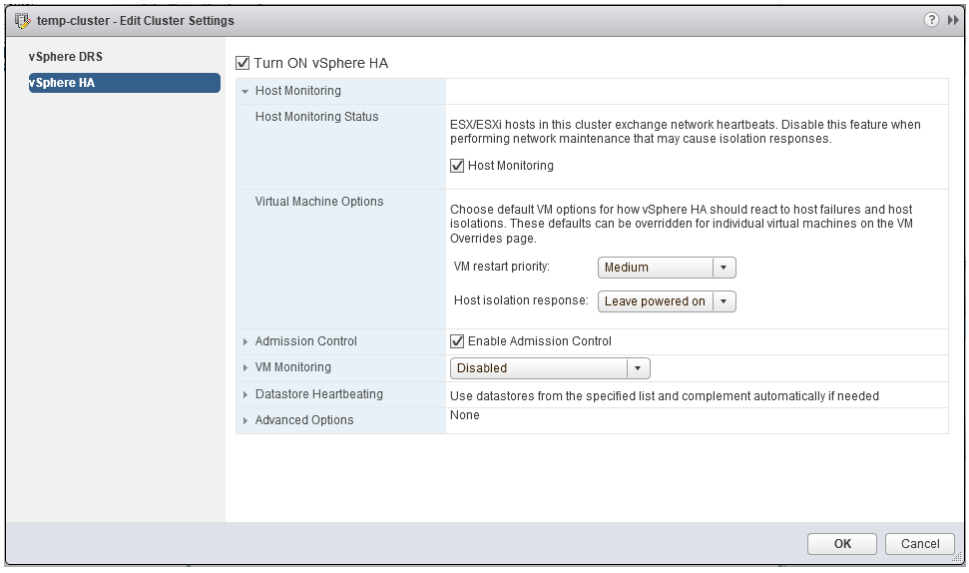


Figure 7.6

- **Host Monitoring:** If this option is enabled, frequent checks are performed to ensure each ESXi host in the cluster is running. If a host failure occurs, the relevant virtual machines are restarted on another host. Host Monitoring is also required for the VMware Fault Tolerance recovery process to function properly. Remember to disable Host Monitoring when performing network maintenance.

- **Virtual machine options**. These options define how High Availability should react to host failures and isolations:
  - ***VM Restart Priority*** – determines the relative order in which virtual machines are restarted after a host failure. You can specify the priority level for each VM: Disabled, Low, Medium, or High. You can set your main VMs, such as those that run the Domain Controller, the database server, and/or the email server, to restart with high priority.
  - ***Host Isolation Response*** – three options are available here:
    - **Leave powered on** – when a network isolation occurs for the ESXi host, the state of the virtual machines on the host remains unchanged. The virtual machines on the isolated host continue to run, even if the host can no longer communicate with other hosts in the cluster. This setting reduces the chances of a false positive.
    - **Power off, then failover** – when a network isolation occurs, all virtual machines are powered off and restarted on another ESXi host. This is a hard stop. A power-off response is initiated on the fourteenth second, and a restart is initiated on the fifteenth second.
    - **Shutdown, then failover** – when a network isolation occurs, all virtual machines running on that host are shut down via VMware Tools and restarted on another ESXi host. This approach allows the services and programs that are running on the virtual machines to be stopped correctly. If shutdown is not successful within 5 minutes, a power-off response type is executed.
- **Admission control** (see *Figure 7.7*). Admission control is used by vCenter to ensure that sufficient resources are available in a cluster for failover protection. The cluster reserves resources to allow failover for all running virtual machines on the specified number of hosts.

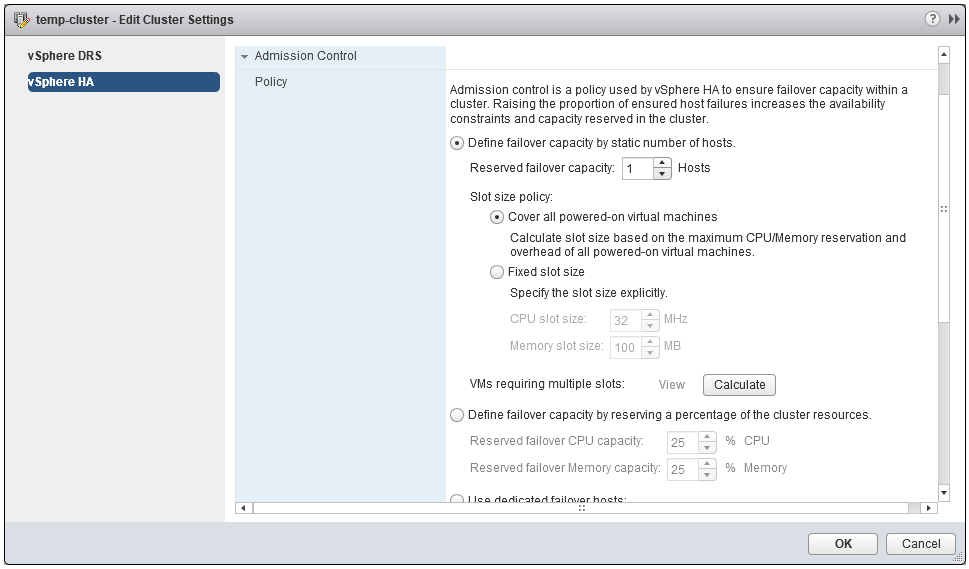


Figure 7.7

Each Admission Control Policy has a separate Admission Control mechanism. Slots dictate how many virtual machines can be powered on before vCenter triggers the “Out of resources” notification. The Admission Control process is a function of vCenter, and not of the ESXi host.

The percentage of Cluster Resources Reserved is the least restrictive and most flexible Admission Control policy. 25% is the default reserved percentage, meaning that 25% of the total CPU and total memory resource across the entire cluster is reserved for the cluster.

Failover hosts are the ESXi hosts that are reserved for a failover situation. Failover hosts don’t factor into DRS recommendations or migrations, and virtual machines can’t run on these hosts in the regular mode.

NOTE: Remember to enable Admission Control, because this option guarantees the ability of virtual machines restart after a failure.

- **VM Monitoring.** This service evaluates whether each virtual machine in the cluster is running by checking for regular heartbeats and input/output activity from the VMware Tools process running inside the guest. VM Monitoring is different from the host monitoring in that the item being watched is an individual virtual machine, rather than an ESXi host. If vSphere can’t detect VM heartbeats, the VM reboot happens. You can select the level of sensitivity using a preset, or set the failure interval, the minimum uptime, and the maximum per-VM resets manually (see *Figure 7.8*).

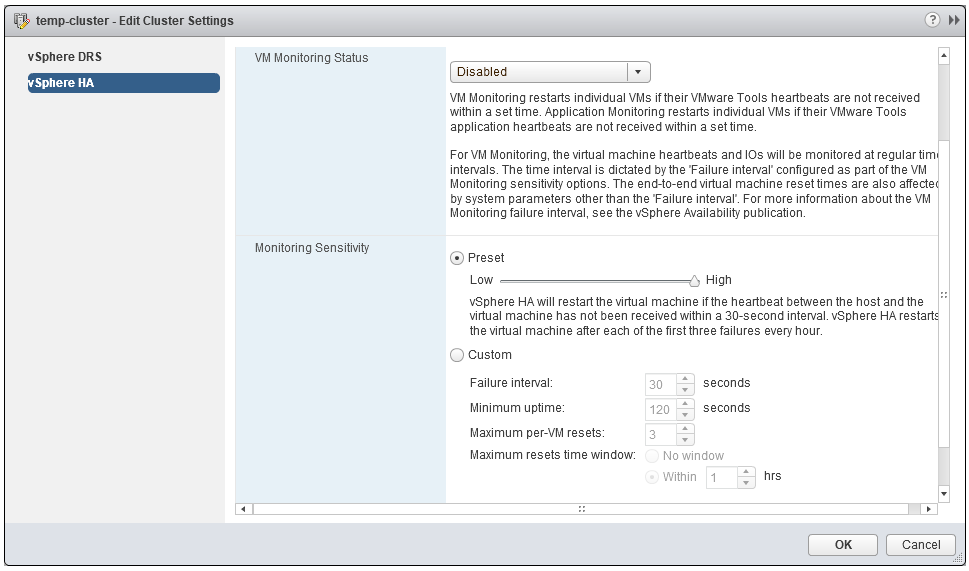


Figure 7.8

- **Datastore Heartbeating** (see *Figure 7.9*). If the management network of an ESXi host becomes isolated but the virtual machines are running, a restart signal is sent. Datastore Heartbeating is used to determine more accurately the state of the ESXi host, even if the management network fails. Thus, the feature reduces the probability of falsely triggering the virtual machine reboot mechanism. There are locking mechanisms to prevent

concurrent usage of open files located on shared storage and avoid file corruption. HA manages the existing Virtual Machine File System (VMFS) locking mechanism, which is also called a “Heartbeat Region”; this is updated as long as the lock file exists. HA determines that at least one file is opened on the VMFS volume by checking files specially created for Datastore Heartbeating. These files are named in the VMname-hb format: WindowsVM-hb, LinuxTest-hb, host1tst-hb, etc. You can find them in the .vSphere-HA directory which is located on the shared datastore with vSphere Client. Go to **Home -> Datastores -> DatastoreName -> Manage -> Files**. Don’t delete or modify these files.

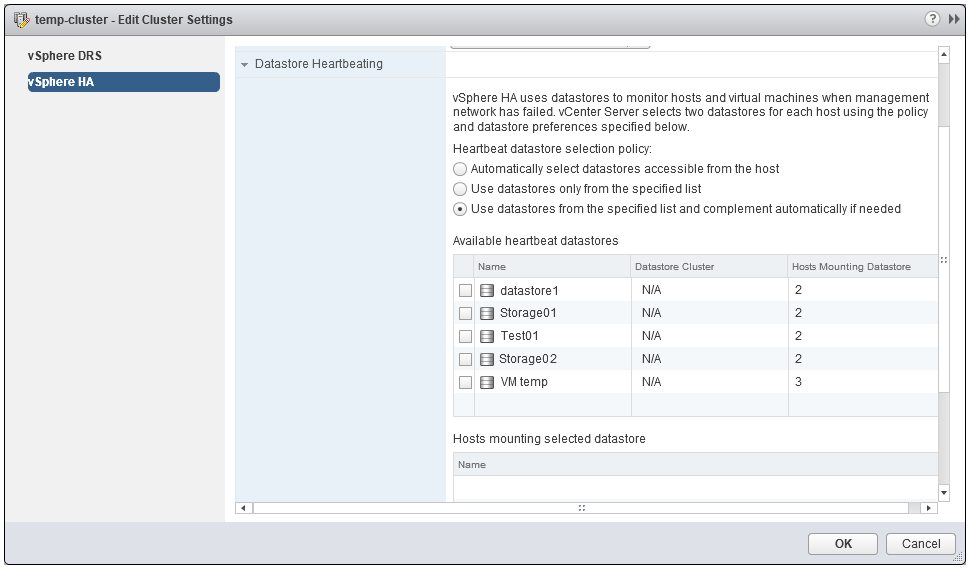


Figure 7.9

5. Click **OK** to finish the High Availability setup and wait while vSphere HA is configured (see *Figure 7.10*).

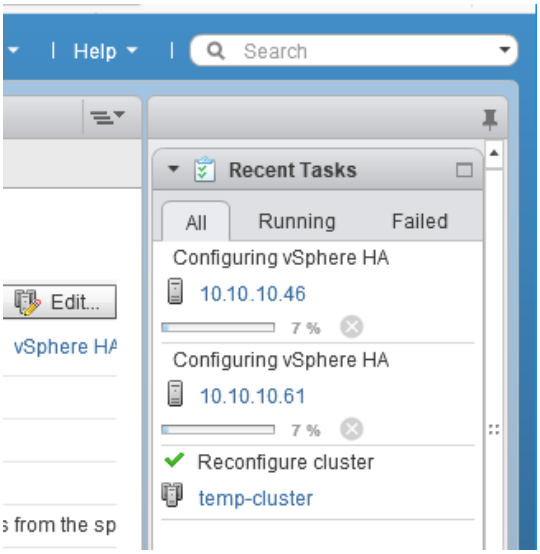


Figure 7.10

Fault Tolerance: Purpose and Setup

Fault Tolerance (FT) provides continuous availability for virtual machines and enables them to survive a physical server failure. With this great feature, you can have an exact and continuously available replica VM on another ESXi host that can take over from the virtual machine affected at the time of failure.

In High Availability mode, virtual machines need some time to load on another ESXi host after the ESXi host on which they were running fails. With Fault Tolerance, a virtual machine has a copy running on another ESXi host with disabled VM network connection. If the ESXi host with the primary copy of a VM fails, the secondary copy on another ESXi host just needs to have networking enabled; this is why the migration process looks seamless. If there are more than two ESXi servers included in the cluster, vSphere HA runs the replica of the VM on the second ESXi server at the moment of failure, then creates a new VM replica on a third ESXi server.

Requirements for Virtual Machines with FT (v.6.0)

- 10-Gigabit network adapters on ESXi hosts;
- Maximum 4 vCPU;
- Maximum 64 GB RAM;
- Maximum 4 VMs to run simultaneously on one ESXi host;
- Disabled CPU Hot-Add and RAM Hot-Add;

NOTE: The following restrictions apply:

- If more than one vCPU is used, Storage vMotion is not supported.
- Snapshots and thin disks are supported.
- HA cluster needs to be configured.

How to Enable Fault Tolerance

To enable FT for virtual machines, do the following:

1. Select your cluster and go to the list of virtual machines.
2. Right click on the virtual machine you want to make fault-tolerant: **All vCenter Actions –> Fault Tolerance –> Turn On Fault Tolerance** (see *Figure 8.1*).

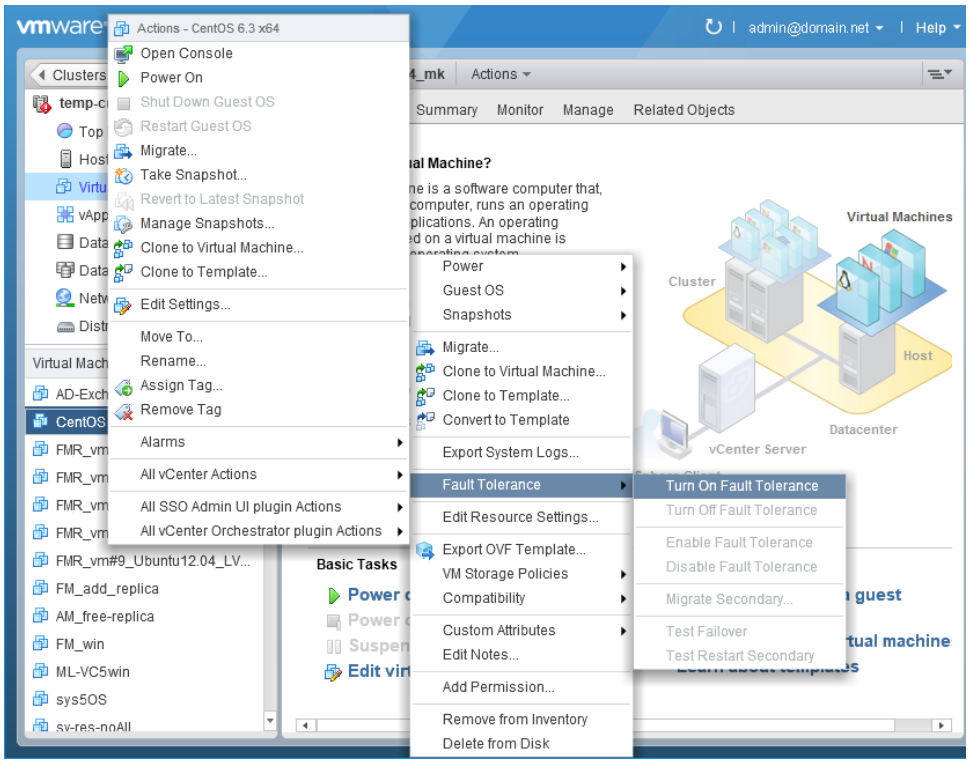


Figure 8.1

A confirmation message appears for vSphere version 5.5, informing you of disk conversion (see *Figure 8.2*). If you turn on Fault Tolerance, thin-provisioned disks, as well as disks that zero out blocks as they were written to (lazy-zeroed thick-provisioned disks), become disks with all blocks zeroed out (eager-zeroed, thick-provisioned disks). This conversion means that the virtual machine uses more disk space and needs some processing time. This warning does not appear in vSphere 6, as thin-provisioned disks are supported.

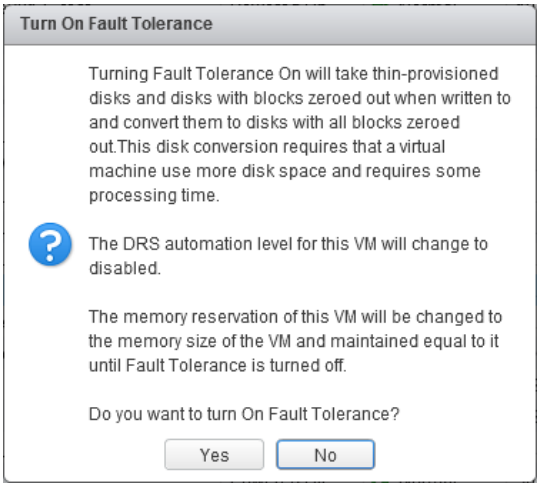


Figure 8.2

3. Click **Yes** to continue.
The virtual machine Fault Tolerance status is displayed in VM -> Summary tab.
4. Now you can set up **Latency Sensitivity** (a high performance mode for the virtual machine). Go to **VM –> Manage –> Settings –> Advanced settings** (see *Figure 8.3*).

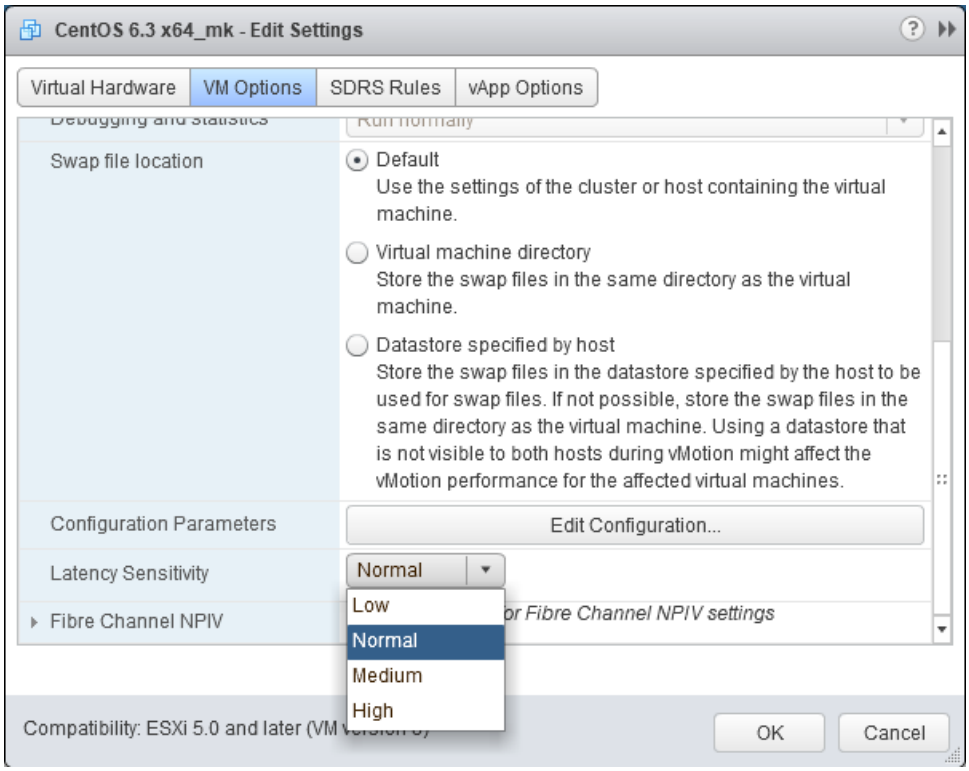


Figure 8.3

With “High” Latency Sensitivity, the ESXi host provides vCPU access to physical CPU while calculating the actual CPU load. With this option enabled, a virtual machine processor can interact directly with the physical processor, without using the VMkernel scheduler. Thus, the Latency Sensitivity mode is useful for virtual machines demanding high performance.

Here is an example of how High Availability and Fault Tolerance features work.

Both of ESXi servers are running in a High Availability cluster. The virtual machine VM2 is running on ESXi Server 1 with the Fault Tolerance option enabled, and has an exact replica with disabled networking running on ESXi Server2. VM1 is also running on ESXi Server 1, but the Fault Tolerance option is disabled for this virtual machine (see *Figure 8.4*):

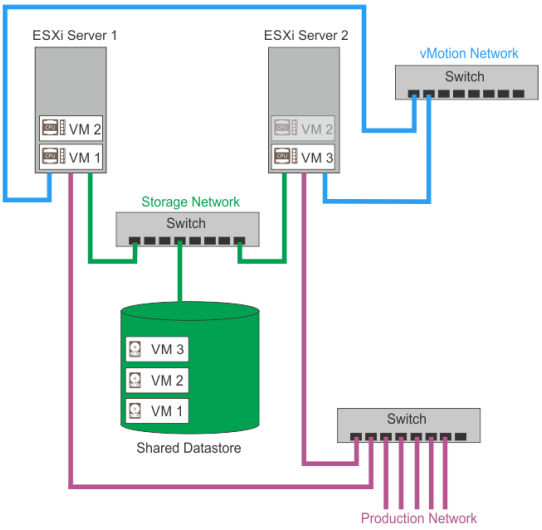


Figure 8.4

Now, a failure occurs for ESXi Server 1. VM2, which was running on ESXi Server 1, also fails, but the replica of VM2 that is still running on ESXi Server 2 becomes reachable in an instant; networking is enabled for the replica by the automatic failover protection of the VMware Fault Tolerance feature. VM2's failover is seamless and instant. VM1 becomes unreachable because of the same Server 1 failure, but since there is no replica of VM1, this virtual machine must be migrated to ESXi Server 2. Loading VM1's operating system and other services may take some time (see *Figure 8.5*):

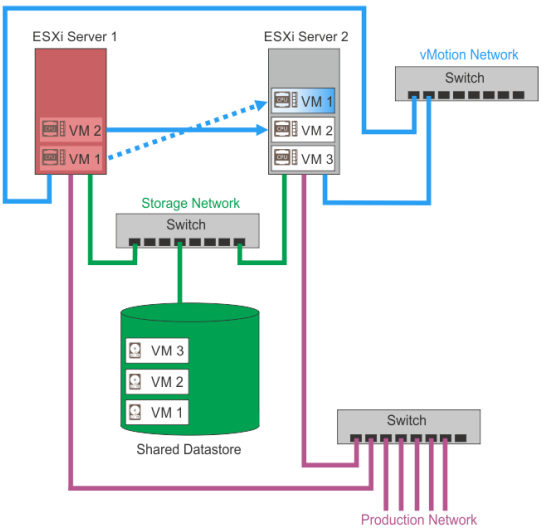


Figure 8.5

If you decide to turn off Fault Tolerance, click on the respective virtual machine and select: **All vCenter Actions –> Fault Tolerance –> Turn Off Fault Tolerance.**

NOTE: There is a difference between disabling Fault Tolerance and turning off Fault Tolerance. If you disable FT, the secondary virtual machines are preserved with their configuration and history. Using this option allows you to re-enable FT in the future. Turning off VMware FT deletes all secondary virtual machines, their configurations, and their history. Use this option if you do not plan on re-enabling VMware FT (see *Figure 8.6*).

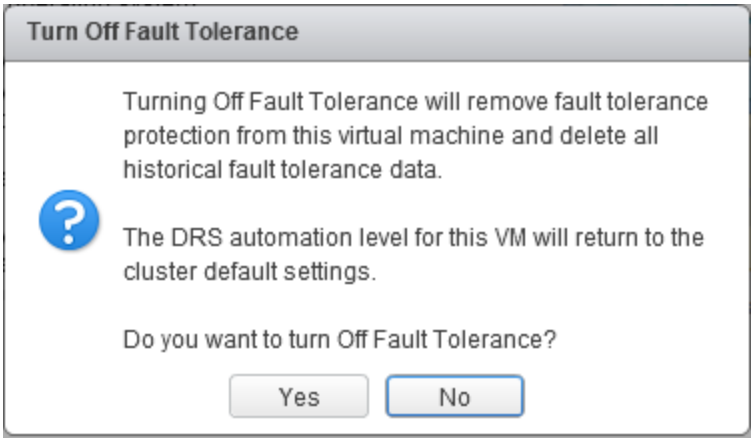


Figure 8.6

Removing Hosts from the Cluster

If, for any reason, you decide to remove an ESXi host from the cluster, take the following steps:

1. Power off all virtual machines that are running on the host.
2. Right-click the ESXi host and select **Enter Maintenance Mode** (see *Figure 9.1*).

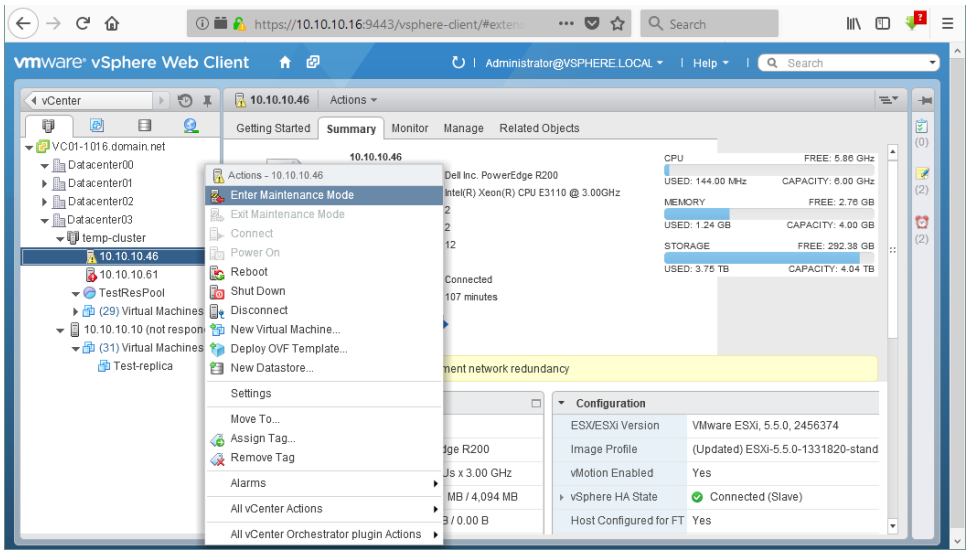


Figure 9.1

A confirmation prompt appears (see *Figure 9.2*).

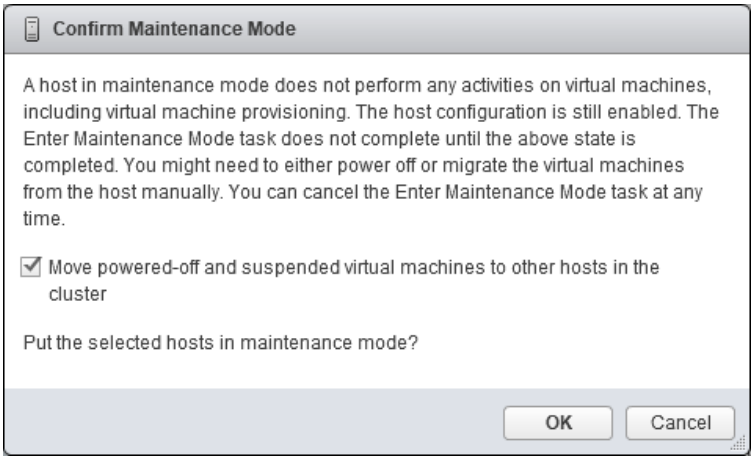


Figure 9.2

3. Right-click the ESXi host you want to remove from the cluster and select **Move To...** (see *Figure 9.3*).

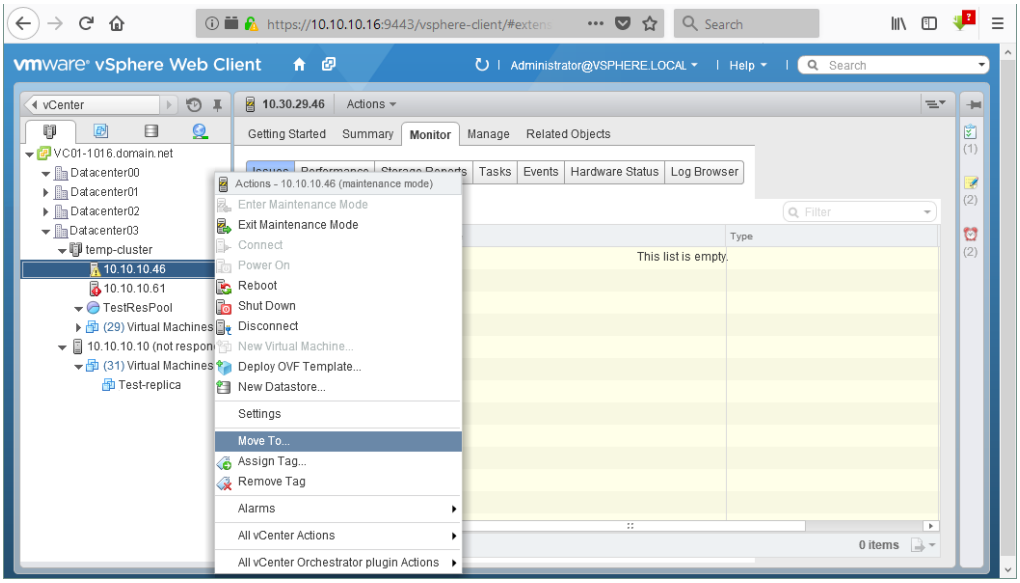


Figure 9.3

4. Select a new location for the host (see *Figure 9.4*).

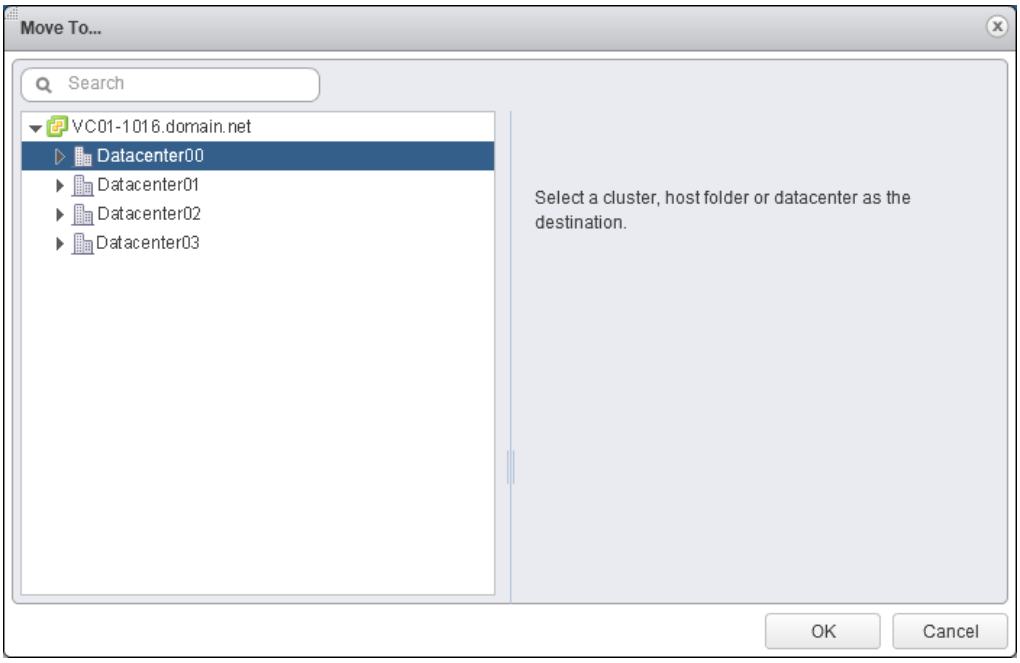


Figure 9.4

5. Right-click the ESXi host and select **Exit Maintenance Mode** (see *Figure 9.5*).

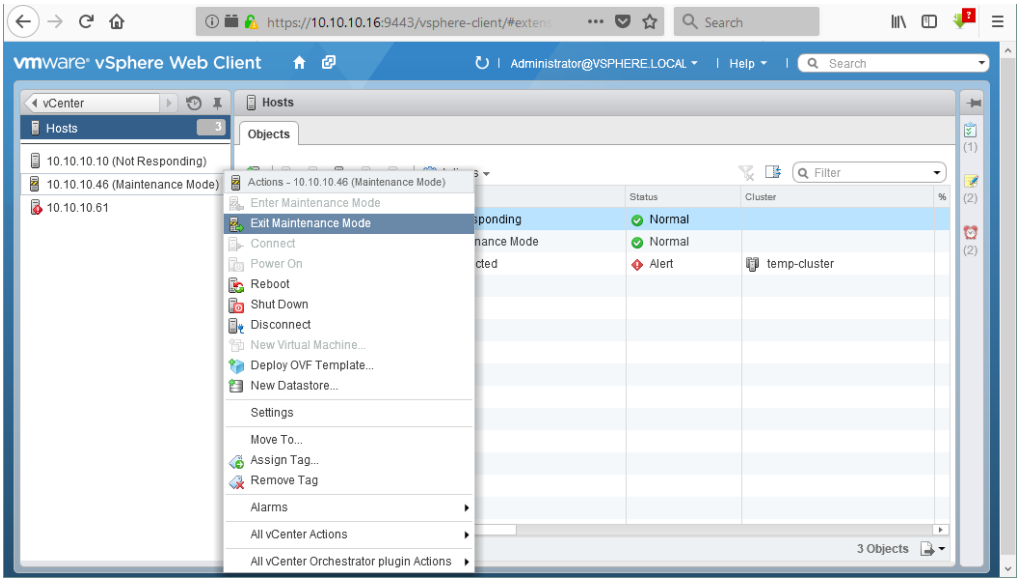


Figure 9.5

More protection of your cluster with NAKIVO Backup & Replication

NAKIVO Backup & Replication is a fast, reliable, and affordable solution for protecting VMware environments. The product offers image-based, application-aware backup and replication, as well as a wide variety of recovery options for DR scenarios, all from an intuitive web UI.
The solution ensures that backups are small by using VMware's Changed Block Tracking (CBT) technology to identify and copy only the data that has changed since the last increment. Repository-wide deduplication and several compression options mean that your backups will occupy minimal storage space and can be transferred quickly.
LAN-free data transfer and Network Acceleration features can boost your VM backup speed, making the process even shorter.
The product also offers backup-to-cloud functionality and automated failover to prevent data loss or downtime in the event of a site-wide disaster. Screenshot verification for completed jobs allows you to check that your VMs are recoverable. When disaster strikes, you can use Flash VM Boot to instantly recover an entire VM or restore files or application objects to their source location granularly.
Easy scheduling and management of all types of jobs (backup, replication, backup copy, or failover) from the Calendar Dashboard, as well as the option to chain them, makes the solution suitable for businesses of all sizes.
NAKIVO Backup & Replication provides the following cluster-friendly features for the protection of VMs residing on ESXi hosts:

Adding VMware containers to inventory

Entire VMware containers, such as standalone ESXi hosts or vCenter servers, can be added to the inventory of NAKIVO Backup & Replication. When an ESXi host or vCenter server is added, the VMs, VM folders, datacenters, clusters, and resource pools that belong to it are added automatically. Thus, you can add all the needed objects to your inventory quickly and easily.

Backup of VMware containers, including clusters

Clustering can provide high availability for your VMs, but you can increase your protection level by creating backups and replicas of your VMs. This approach drastically increases your chances of successful failover and disaster recovery. By using NAKIVO Backup & Replication, you can select VMware containers with all the objects inside them for backup. When you select an ESXi host to be backed up, all VMs residing on the host are selected as well. When you select a cluster, all VMs that belong to the cluster are selected; thus, you can back up the entire cluster in a few clicks. All new VMs added to a container that is protected with NAKIVO Backup & Replication are automatically included in subsequent backup jobs. (You are free to manually select additional VMs or deselect automatically included VMs and other objects in the job options.)

Automatic tracking of VMs migrating within a cluster

VMs can migrate from one ESXi host to another within a cluster during failover or load balancing events. NAKIVO Backup & Replication tracks the migrating VMs within a cluster automatically. As a result, such VMs are always protected by the product and can be backed up or replicated without any added effort.

Replication of VMs from one cluster to another

NAKIVO Backup & Replication can replicate VMs to a cluster. Thus, you can replicate the business-critical VMs from a local cluster to a remote cluster and use the resulting VM replicas for failover during disaster recovery. NAKIVO Backup & Replication includes a feature that called Automated VM Failover, with which you can perform failover using a VM replica. With Network Mapping and Re-IP features, your replicas are automatically adapted to the new virtual environment; the network settings of the VMs are changed automatically during failover. All you need to do is create a rule when configuring the replication or failover job.

Conclusion

VMware vSphere is a virtual environment with a long list of features that help manage virtual machines, provide great capability, reliability, and scalability. Clustering technologies are widely used in vSphere to connect servers over the network and achieve better performance in executing resource-intensive tasks. VMware supports creating Distributed Resource Scheduler (DRS) clusters and High Availability (HA) clusters. Creating a DRS cluster helps improve performance by rational usage of computing resources. A HA cluster reduces the downtime of virtual machines in the event of failure by restarting VMs on another host via redundant network. Fault Tolerance feature of HA clusters ensures avoiding the downtime and provides for the seamless migration of virtual machines from the failed host to the running host. That is vital for business critical processes. Using vSphere HA and DRS together combines automatic failover with load balancing. This helps provide a more balanced cluster after vSphere HA moves virtual machines to different hosts.

High Availability and Fault Tolerance do not replace the need for data backup. In the event of cluster usage, virtual machines are stored on a shared datastore and should be backed up to another storage. A combination of VMware cluster features with backup ensures the efficient resource management, increased reliability, and protection.

NAKIVO Backup & Replication at a Glance

NAKIVO Backup & Replication is a fast, reliable, and affordable VM backup solution. The product protects VMware, Hyper-V, and AWS EC2 environments. NAKIVO Backup & Replication offers advanced features that increase backup performance, improve reliability, and speed up recovery. As a result, you can save time and money.

Deploy in under 1 minute
Pre-configured VMware VA and AWS AMI; 1-click deployment on ASUSTOR, QNAP, Synology, or WD NAS; 1-click Windows installer, 1-command Linux installer

Reduce backup size
Forever-incremental backups with CBT/RCT, LAN-free data transfer, network acceleration; up to 2X performance when installed on NAS

Protect VMs
Native, agentless, image-based, application-aware backup and replication for VMware, Hyper-V VMs, as well as AWS EC2 instances

Ensure recoverability
Instant backup verification with screenshots of test-recovered VMs; backup copy offsite/to the cloud

Increase backup speed
Exclusion of SWAP files and partitions, global backup deduplication, adjustable backup compression

Decrease recovery time
Instant recovery of VMs, files, Exchange objects, SQL objects, Active Directory objects; DR with VM replicas

About NAKIVO

The winner of a “Best of VMworld 2018” and the Gold Award for Data Protection, NAKIVO is a US corporation dedicated to developing the ultimate VM backup and site recovery solution. With 20 consecutive quarters of double-digit growth, 5-star online community reviews, 97.3% customer satisfaction with support, and more than 10,000 deployments worldwide, NAKIVO delivers an unprecedented level of protection for VMware, Hyper-V, and Amazon EC2 environments.

As a unique feature, NAKIVO Backup & Replication runs natively on leading storage systems including QNAP, Synology, ASUSTOR, Western Digital, and NETGEAR to deliver up to 2X performance advantage. The product also offers support for high-end deduplication appliances including Dell/EMC Data Domain and NEC HYDRAstor. Being one of the fastest-growing data protection software vendors in the industry, NAKIVO provides a data protection solution for major companies such as Coca-Cola, Honda, and China Airlines, as well as works with over 3,000 channel partners in 137 countries worldwide. Learn more at www.nakivo.com