VMware ESXi Cookbook

Over 50 recipes to master VMware vSphere administration

Mohammed Raffic Kajamoideen
Aravind Sivaraman

[PACKT] enterprise 88
PUBLISHING   professional expertise distilled

VMware ESXi Cookbook

Over 50 recipes to master VMware vSphere administration

Mohammed Raffic Kajamoideen

Aravind Sivaraman

VMware ESXi Cookbook

Credits

Authors
Mohammed Raffic Kajamoideen
Aravind Sivaraman

Reviewers
Jason Langer
Alexzander Nepomnjashiy
Fernando F. Rodrigues
Timothy Smith

Acquisition Editor
Owen Roberts

Content Development Editor
Balaji Naidu

Technical Editors
Venu Manthena
Mrunmayee Patil
Shruti Rawool
Aman Preet Singh
Nachiket Vartak

Copy Editors
Roshni Banerjee
Janbal Dharmaraj
Sayanee Mukherjee
Karuna Narayanan
Alfida Paiva
Laxmi Subramanian

Project Coordinator
Sanchita Mandal

Proofreaders
Ameesha Green
Samantha Lyon
Lindsey Thomas

Indexers
Rekha Nair
Priya Subramani

Graphics
Sheetal Aute

Production Coordinator
Pooja Chiplunkar

Cover Work
Pooja Chiplunkar

About the Authors

Mohammed Raffic Kajamoideen (@VMwareArena) is a subject matter expert for VMware virtualization technology and works as a system administrator in VMware Inc. where he provides high-level technical guidance to support and implement VMware's virtualization products. He is an author, a technology enthusiast, and a blogger focusing on virtualization and cloud computing.

He has over six years of high-level knowledge in remote infrastructure services, consulting, designing, implementing, and troubleshooting VMware virtualization technology. He is well known for his contribution towards the virtualization community through his virtualization blog (http://www.vmwarearena.com).

He holds many specialized certifications from VMware, Microsoft, and Citrix®, which includes VCP4, VCP5, VCAP4-DCA, VCAP5-DCA, VCP-Cloud, MCTS-virtualization, CCA, and MCSA. Prior to joining VMware, he has served other large organizations such as CGI, Infosys, and Microsoft as a virtualization support engineer and a subject matter expert.

Aravind Sivaraman is a virtualization engineer with over eight years of experience in the IT industry and for the past five years he has been focused on virtualization solutions, especially on VMware products. He holds different certifications from VMware, Microsoft, and Cisco and has been awarded the vExpert for the year 2013. He is a VMware Technology Network (VMTN) and Experts Exchange contributor and maintains his personal blog at `http://aravindsivaraman.com/`. He can be followed on Twitter at `@ss_aravind`.

He is also the technical reviewer for the book *Troubleshooting vSphere Storage*, *Mike Preston*, *Packt Publishing*.

About the Reviewers

Jason Langer works as a solutions architect for VMware Partner in the Pacific Northwest helping customers achieve their datacenter virtualization and end user computing goals. Jason has obtained multiple levels of certification both from Microsoft (MCSE/MCSA) and VMware (VCP/VCAP) and brings 15 years of IT experience that spans large enterprise and SMB. When not working during the day, he is active in the VMware community as a member of the Seattle VMUG Steering Committee, on Twitter (`@jaslanger`), and generating content for his blog (`www.virtuallanger.com`).

He is also the technical reviewer of the following books:

> ▸ *VMware Horizon View 5.3 Design Patterns and Best Practices, Jason Ventresco, Packt Publishing*
>
> ▸ *Troubleshooting vSphere Storage*, Mike Preston, *Packt Publishing*

Alexzander Nepomnjashiy is an independent consultant and freelancer. He is particularly interested in the following IT technologies: Windows Server OSes administration, Microsoft SQL Servers internals, virtualization (VMware ESXi), OLAP, and business intelligence.

Fernando F. Rodrigues is an IT professional with more than 10 years experience in systems administration, especially with Linux and VMware. He is a system administrator who also focuses on programming (Perl, PowerCLI, Bash, and so on) and is currently learning Ruby and Python. He has experience in projects for the government sector and financial institutions. He is a technology enthusiast and his areas of interest include cloud computing, virtualization, infrastructure automation, Linux administration, and Raspberry Pi.

Timothy Smith has over 15 years experience in system administration and has been working with VMware products almost since the beginning. He is a VMware vExpert, and a VMware certified professional, and holds various Microsoft certifications. As an active blogger (`http://tsmith.co`), Tim has been actively testing and working with VMware vSphere and giving back helpful articles and posts to the community regarding various problems he has come across.

www.PacktPub.com

Support files, eBooks, discount offers and more

You might want to visit `www.PacktPub.com` for support files and downloads related to your book.

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at `www.PacktPub.com` and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at `service@packtpub.com` for more details.

At `www.PacktPub.com`, you can also read a collection of free technical articles, sign up for a range of free newsletters and receive exclusive discounts and offers on Packt books and eBooks.

PACKTLiB

`http://PacktLib.PacktPub.com`

Do you need instant solutions to your IT questions? PacktLib is Packt's online digital book library. Here, you can access, read, and search across Packt's entire library of books.

Why Subscribe?
- ▶ Fully searchable across every book published by Packt
- ▶ Copy and paste, print, and bookmark content
- ▶ On demand and accessible via web browser

Free Access for Packt account holders

If you have an account with Packt at `www.PacktPub.com`, you can use this to access PacktLib today and view nine entirely free books. Simply use your login credentials for immediate access.

Instant Updates on New Packt Books

Get notified! Find out when new books are published by following `@PacktEnterprise` on Twitter, or the *Packt Enterprise* Facebook page.

Table of Contents

Preface

VMware vSphere is a key virtualization technology which acts as the base platform for cloud computing. ESXi 5.1 has been released with a lot of new cool features to strengthen the virtualization platform. Nowadays, all the enterprises and IT environments are switching towards virtualization and cloud computing technologies. ESXi is the base component of cloud computing and it is also called as Cloud OS. VMware ESXi has a smaller code base and a reliable and secure hypervisor, which is part of the vSphere suite. Its smaller footprint allows it to be embedded in mainstream physical servers for simpler and faster deployments. So many users are excited to learn about the VMware virtualization technology.

VMware ESXi Cookbook focuses on helping you perform your virtual environment administration using vSphere Web Client. It offers a comprehensive understanding of new features released with vSphere 5.1 and how it enhances your VMware virtual environment.

VMware ESXi Cookbook covers a wide variety of day-to-day tasks that need to be performed by the VMware administrators and also teaches advance level tasks with a lot of tips and tricks to ease the job of an admin. This book will enable the reader to configure and administer various features of vSphere including High Availability (HA), Distributed Resource Scheduler (DRS), Fault Tolerance (FT), vMotion, svMotion, virtual machine provisioning, Update Manager, and distributed virtual switches. It also focuses on how vSphere environment can be secured and enabled by the reader and explains how to monitor the virtual environment using default alarms available with the vCenter Server.

What this book covers

Chapter 1, *Installing and Configuring ESXi*, begins by introducing ESXi, different vSphere licensing options available, and then explains how to select the right hardware for deployment. This chapter also covers different deployment methods of the ESXi host and then moves on to some of the configuration to be done after the host deployment.

Chapter 2, *Installing and Using vCenter*, chalks out the importance of the vCenter Server in the vSphere Infrastructure and demonstrates how to plan, install, and configure the vCenter Server.

Chapter 3, *Networking*, helps you to the understand the vSphere networking concepts—both vSphere standard and the distributed switch—then moves on to discuss some of the more advanced networking configurations available in the distributed switch, and then ends with the security policies available in vSphere.

Chapter 4, *Storage*, talks about implementing and configuring various storage options and optimizing storage using storage I/O control and storage profiles.

Chapter 5, *Resource Management and High Availability*, helps you understand how to create and configure various clusters including High Availability (HA), Distributed Resource Scheduler (DRS), Dynamic Power Management (DPM), and Storage DRS.

Chapter 6, *Managing Virtual Machines*, teaches you to provision and manage virtual machines, configure Fault Tolerance for VMs, and understand the methods to use snapshot, template, and clone.

Chapter 7, *Securing the ESXi Server and Virtual Machines*, dwells on the subject of securing ESXi hosts using firewall, configuring AD authentication, and strengthening the security for virtual machines.

Chapter 8, *Performance Monitoring and Alerts*, helps you understand how to view performance graphs and export the graph for future reference. It also teaches you to configure vCenter alarms and export logs for troubleshooting.

Chapter 9, *vSphere Update Manager*, educates you on the installation steps for Update Manager and also explains how to upgrade the ESXi host and virtual machine using Update Manager.

What you need for this book

You will need to set up the following software for this book:

- ▶ VMware ESXi 5.1
- ▶ VMware vCenter Server 5.1
- ▶ VMware vCenter Server Appliance 5.1
- ▶ Compliance Checker for vSphere
- ▶ VMware Update Manager 5.1
- ▶ Update Manager Download Service

Who this book is for

The book is primarily written for technical professionals with system administration skills and basic knowledge of virtualization who wish to learn installation, configuration, and administration of vSphere 5.1. Essential virtualization and ESX or ESXi knowledge is advantageous.

Conventions

In this book, you will find a number of styles of text that distinguish between different kinds of information. Here are some examples of these styles, and an explanation of their meaning.

Code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles are shown as follows: " Alternatively, the NTP setting can be configured using the PowerCLI cmdlet, `Add-VmHostNtpServer`, which will help us configure the NTP setting."

Any command-line input or output is written as follows:

```
Add-EsxSoftwareDepot C:\VMware-Esxi-5.1.0-799733-depot.zip
```

New terms and **important words** are shown in bold. Words that you see on the screen, in menus or dialog boxes for example, appear in the text like this: "Click on **Enter Key...** and this will pop up an **Add license key** window, where you need to enter the license key."

> Warnings or important notes appear in a box like this.

> Tips and tricks appear like this.

Reader Feedback

Feedback from our readers is always welcome. Let us know what you think about this book— what you liked or may have disliked. Reader feedback is important for us to develop titles that you really get the most out of.

To send us general feedback, simply send an e-mail to `feedback@packtpub.com`, and mention the book title via the subject of your message.

If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, see our author guide on `www.packtpub.com/authors`.

Customer support

Now that you are the proud owner of a Packt book, we have a number of things to help you to get the most from your purchase.

Errata

Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you find a mistake in one of our books—maybe a mistake in the text or the code—we would be grateful if you would report this to us. By doing so, you can save other readers from frustration and help us improve subsequent versions of this book. If you find any errata, please report them by visiting `http://www.packtpub.com/submit-errata`, selecting your book, clicking on the **errata submission form** link, and entering the details of your errata. Once your errata are verified, your submission will be accepted and the errata will be uploaded on our website, or added to any list of existing errata, under the Errata section of that title. Any existing errata can be viewed by selecting your title from `http://www.packtpub.com/support`.

Piracy

Piracy of copyright material on the Internet is an ongoing problem across all media. At Packt, we take the protection of our copyright and licenses very seriously. If you come across any illegal copies of our works, in any form, on the Internet, please provide us with the location address or website name immediately so that we can pursue a remedy.

Please contact us at `copyright@packtpub.com` with a link to the suspected pirated material.

We appreciate your help in protecting our authors, and our ability to bring you valuable content.

Questions

You can contact us at `questions@packtpub.com` if you are having a problem with any aspect of the book, and we will do our best to address it.

1

Installing and Configuring ESXi

In this chapter, we will cover the following topics:

- ▸ Installing ESXi using Interactive Mode
- ▸ Deploying ESXi hosts using scripted installation
- ▸ Deploying ESXi hosts using Auto Deploy
- ▸ Installing vSphere Client
- ▸ Configuring NTP settings on ESXi hosts
- ▸ Configuring DNS and Routing
- ▸ Licensing an ESXi host

Introduction

VMware ESXi is a hypervisor that is built directly on top of an x86 hardware. It abstracts the underlying hardware and allows multiple virtual machines to use the same hardware resources. It includes an ultra-thin architecture, and the footprint in the memory is 32 MB, which makes it more reliable and it only takes a few minutes to install. ESXi is offered in two different types: *ESXi Embedded* and *ESXi Installable*, and there is no functional difference between them. Both use the same code and provide us with the same functionality and features depending on the license used. The two different types of ESXi are explained as follows:

- ▸ **ESXi Embedded**: This is available in the **Original Equipment Manufacturer** (**OEM**) format, and it is installed on a USB or an SD card when the hardware is being purchased. It saves the cost of purchasing additional hard drives and saves valuable time for vSphere administrators, as there is no need to install hypervisors.

▶ **ESXi Installable**: This is a traditional form of installing the hypervisor on a local disk or SAN using an ISO image.

A **VMware vSphere License** is based on per physical CPU and the vCenter Server is licensed separately. There are three editions of vCenter and five editions of VMware vSphere license available.

vCenter is available in the following three editions:

▶ **vCenter Server Essentials**: This is bundled with the vSphere Essentials kit, and it allows centralized management of three ESXi hosts.

▶ **vCenter Foundation**: This vCenter edition limits vSphere host management and is limited to only three ESXi hosts. It also doesn't support the vCenter linked mode or include vCenter Orchestrator.

▶ **vCenter Standard**: This is used in large-scale deployments for rapid provisioning, management, automation, and monitoring, and supports up to 1000 ESXi hosts.

The vSphere licenses are categorized for SMB and large enterprise customers. If you are an SMB customer, two kits are available, which are bundled with the hypervisor and the vCenter:

▶ The Essentials kit allows you to use up to three ESXi hosts, each with two physical processors, but this license only includes the hypervisor and does not include any other features

▶ The Essentials Plus kit allows you to use up to three ESXi hosts, each with two physical processors, and this kit includes features such as vMotion, **High Availability** (**HA**), data protection, vShield end point, and vSphere replication, along with the vSphere hypervisor

If you are running more than three ESXi hosts in the environment and looking for more vSphere features, then you might consider using one of the following licenses:

▶ Standard

▶ Enterprise

▶ Enterprise Plus

A full comparison of the features included in each edition can be found at `http://www.vmware.com/in/products/vsphere/compare.html`.

Choosing hardware for vSphere deployments

You need to make sure that the right hardware is procured to perform the right job, and selecting the hardware plays a major role in the vSphere deployment. VMware has put together a list of supported servers and hardware after the vendors have done extensive testing. VMware Compatibility Guide (`http://www.vmware.com/resources/compatibility/search.php`) gives us the list of supported vendors and their hardware for the vSphere deployment.

As an example, the following screenshot is filtered to list the supported HP servers for ESXi:

Partner Name	Model	CPU Series	Supported Releases				
HP	ProLiant DL580 G7	Intel Xeon E7-4800 Series	ESX	4.1 U3	4.1 U2	4.1 U1	
			ESXi Installable	4.1 U3	4.1 U2	4.1 U1	
			ESXi Embedded	4.1 U3	4.1 U2	4.1 U1	
			ESXi	5.5	5.1 U1	5.1	5.0 U3 ...
HP	ProLiant DL580 G7	Intel Xeon E7-8800 Series	ESX	4.1 U3	4.1 U2	4.1 U1	
			ESXi Installable	4.1 U3	4.1 U2	4.1 U1	
			ESXi Embedded	4.1 U3	4.1 U2	4.1 U1	
			ESXi	5.5	5.1 U1	5.1	5.0 U3 ...
HP	ProLiant BL280c G6	Intel Xeon 55xx Series	ESX	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Installable	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Embedded	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi	5.1 U1	5.1	5.0 U3	5.0 U2 ...
HP	ProLiant BL280c G6	Intel Xeon 56xx Series	ESX	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Installable	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Embedded	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi	5.1 U1	5.1	5.0 U3	5.0 U2 ...
HP	ProLiant BL2x220c G6	Intel Xeon 55xx Series	ESX	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Installable	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi Embedded	4.1 U3	4.1 U2	4.1 U1	4.1 ...
			ESXi	5.1 U1	5.1	5.0 U3	5.0 U2 ...

VMware Compatibility Guide is not only for listing the supported servers but you can also drill down to list out the supported storage arrays, I/O devices, guest OS, and many other features.

Requirements for installing ESXi

Every traditional operating system needs to fulfill a certain hardware requirement for its successful installation; similarly, we have a set of hardware requirements that are required for ESXi installation:

▶ A supported 64-bit processor with a minimum of two cores

▶ CPU with support for LAHF and SAHF instructions

▶ NX/XD bit enabled for the CPU in the BIOS

▶ 2 GB RAM is required for the successful installation of ESXi, but VMware recommends at least 8 GB RAM in the production environment

▶ Hardware virtualization (Intel VT-x or AMD RVI) has to be enabled to run 64-bit virtual machines

▶ A minimum of one Gigabit or 10 Gb network adapters

Deploying VMware ESXi

Once you have selected the hardware and fulfilled the requirements for the ESXi installation, you have to decide the deployment option for ESXi. Four deployment options are available and they are as follows:

- ▸ Interactive ESXi installation
- ▸ Scripted ESXi installation
- ▸ Auto Deploy ESXi installation
- ▸ Customizing installation with ESXi Image Builder

The first three deployment methods will be covered in this chapter.

Installing ESXi using Interactive Mode

Performing ESXi installation using Interactive Mode is fairly straightforward and it's the easiest method of performing the installation.

Getting ready

Make sure that the installer files are downloaded from `http://www.vmware.com/download`, and if the installation is performed remotely, make sure you have access to the hardware remote console (ILO, DRAC, RSA, and so on).

How to do it...

Now, let's look at the steps for installing ESXi:

1. Insert the CD/DVD image into the CD ROM or mount it using a Virtual CD/DVD ROM.
2. Boot the server from the ISO.
3. Select **ESXi-5.1.0-799733-standard Installer** from the boot menu, as shown in the following screenshot:

```
        ESXi-5.1.0-799733-standard Boot Menu

ESXi-5.1.0-799733-standard Installer
Boot from local disk




                Press [Tab] to edit options

          Automatic boot in 5 seconds...
```
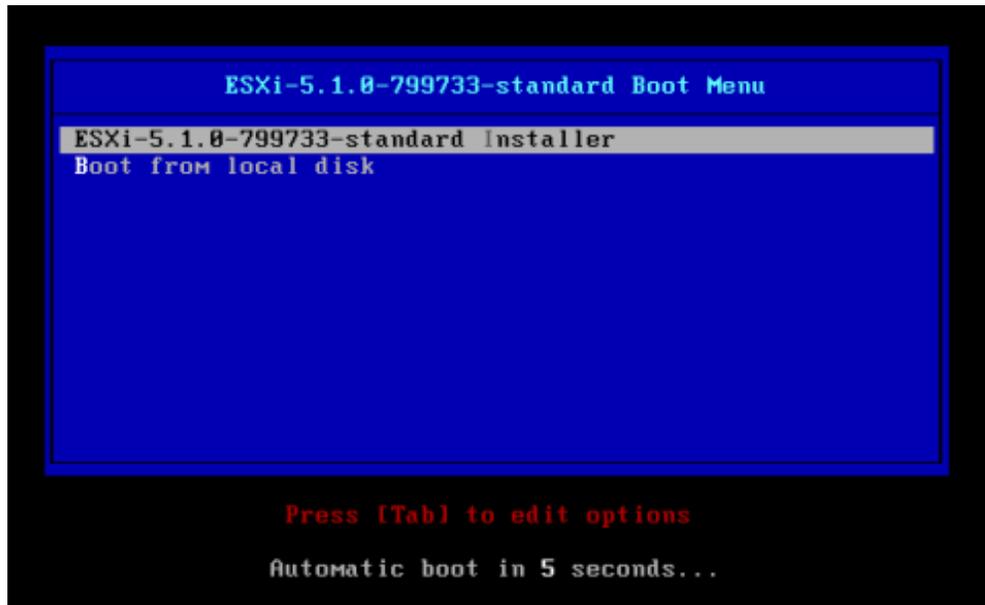
The build number (799733) will change whenever a new security patch or an update is released by VMware.

4. The ESXi installer image will load, and it will present the following screenshot. Press *Enter* to continue.

```
        Welcome to the VMware ESXi 5.1.0 Installation

VMware ESXi 5.1.0 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
```
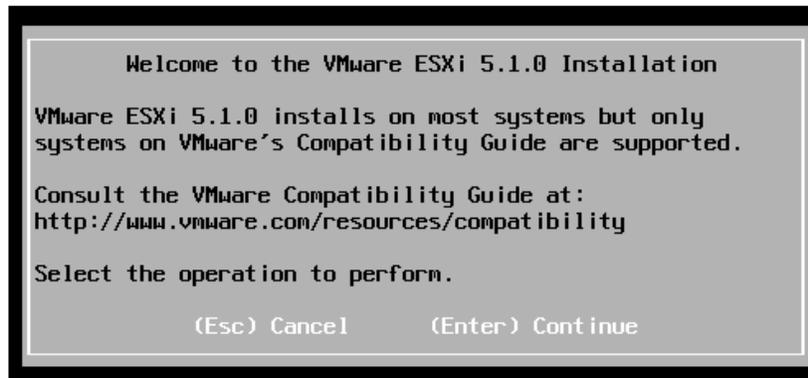
5. In the next screen, accept the license agreement by pressing *F11* to proceed.

6. Next, the installer will look for the list of available devices to install the ESXi and will display a list of both the local and the remote disks available for the host, as shown in the following screenshot:

```
                 Select a Disk to Install or Upgrade

 * Contains a VMFS partition

 Storage Device                                              Capacity
 --------------------------------------------------------------------
 Local:
    VMware,  VMware Virtual S (mpx.vmhba1:C0:T0:L0)          20.00 GiB
 Remote:
    (none)




     (Esc) Cancel     (F1) Details     (F5) Refresh     (Enter) Continue
```
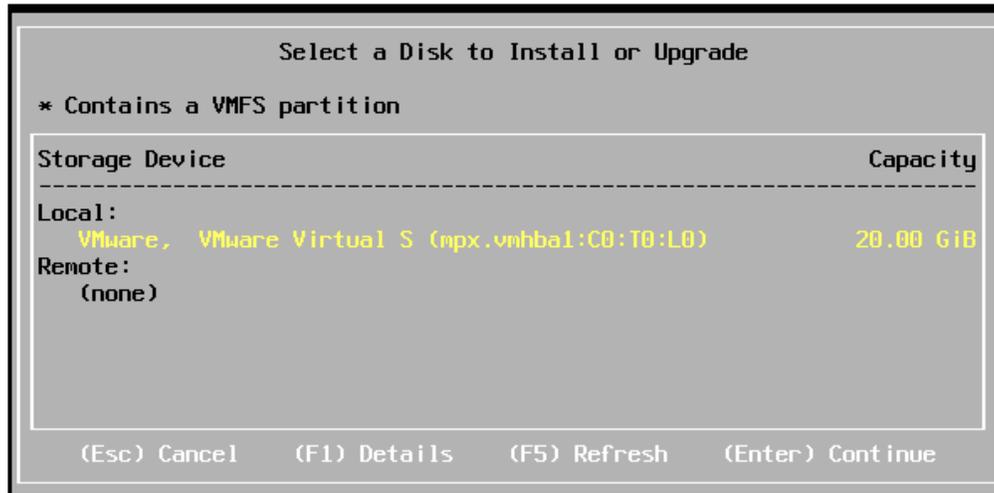
> In case you are using FC SAN and installing the ESXi on a local disk, make sure that you disconnect the FC cables as a precaution, and if you are installing the ESXi as boot from SAN, make sure the correct boot LUN is being selected.

7. Once you have confirmed the disk on to which the ESXi has to be installed, select the disk and press *Enter* to continue.

8. Select the desired keyboard layout and press *Enter* to continue.

9. Now, enter the password as per your security standards and press *Enter* to continue.

10. If there any errors or warnings, it will be listed in the next screen; if everything looks good, you will be asked for a confirmation to install ESXi, as shown in the following screenshot. Press *F11* to allow the installation to complete.

```
                        Confirm Install

        The installer is configured to install ESXi 5.1.0 on:
                     mpx.vmhba1:C0:T0:L0.

            Warning: This disk will be repartitioned.


        (Esc) Cancel        (F9) Back        (F11) Install
```
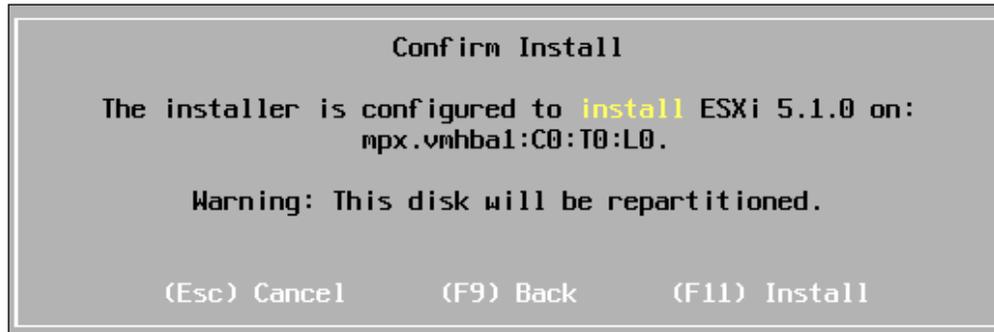
11. When the installation is complete, as shown in the following screenshot, remove the installation media and press *Enter* to reboot the server:

```
                    Installation Complete

ESXi 5.1.0 has been successfully installed.

ESXi 5.1.0 will operate in evaluation mode for 60 days. To
use ESXi 5.1.0 after the evaluation period, you must
register for a VMware product license. To administer your
server, use the vSphere Client or the Direct Control User
Interface.

Remove the installation disc before rebooting.

Reboot the server to start using ESXi 5.1.0.

                    (Enter) Reboot
```

12. After the reboot, the following screenshot will be available on the console and, if DHCP is available in the environment, the host will obtain an IP from the DHCP server:

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

VMware, Inc. VMware Virtual Platform

2 x Intel(R) Core(TM)2 Quad CPU Q8400 @ 2.66GHz
4 GiB Memory




Download tools to manage this host from:
http://192.168.19.130/ (DHCP)
http://[fe80::20c:29ff:fe8b:c2b6]/ (STATIC)
```

There's more...

Once the installation of ESXi is complete, you will be able to perform the following tasks using **Direct Console User Interface** (**DCUI**):

▶ Change the root password

▶ Configure the networking settings

▶ Enable the ESXi shell and remote SSH to troubleshoot from the console

▶ Restart management network and management agents

▶ Perform network restore

▶ Shutdown or restart/reboot ESXi hosts

▶ View system logs

▶ Remove custom extensions

▶ Reset the system configuration

▶ Configure the lockdown mode

Deploying ESXi hosts using scripted installation

Performing a scripted installation is an efficient way of deploying multiple ESXi hosts. The installation script (`ks.cfg`) contains the installation and configuration parameters of ESXi. Using a scripted installation, you can make sure you have a similar configuration for your entire infrastructure. This makes it easy for deploying multiple ESXi hosts in a short amount of time.

Getting ready

Make sure that the hardware used is listed in VMware Compatibility Guide (`http://www.vmware.com/resources/compatibility/search.php`) for ESXi installation, also make sure that the ESXi installer ISO is available, and that the installation script is placed in any one of the following locations:

- CD/DVD device
- USB flash drive or USB storage device
- NFS
- FTP
- HTTP/HTTPS

How to do it...

A scripted installation can be performed using two different methods:

- When the ESXi installer is booting, press *Shift + O* to provide the location of the script file:

  ```
  Ks=https://10.0.1.65/esxi/ks.cfg ip=10.0.1.150
  netmask=255.255.255.0 gateway=10.0.1.1
  ```

  Syntax: `ks=<location of installation script> <boot command line options>`

- The deployment of ESXi hosts can be fully automated using the PXE infrastructure where the options are passed through the `kernelopt` line of the `boot.cfg` file. The `boot.cfg` file is located in the installation media and the content would look similar to the following. Edit the `kernelopt` section by changing the script location for automating the deployment:

  ```
  bootstate=0
  title=Loading ESXi installer
  kernel=/tboot.b00
  kernelopt=runweasel
  modules=/b.b00 --- /useropts.gz --- /k.b00 --- /
  ```

The location of the script file is entered when the installer is booted as shown in the following screenshot:

How it works...

Boot options are specified to access the kickstart file; the following table summarizes the `ks` parameters available during boot for accessing the installation script:

Boot option	Description
`BOOTIF<MAC>`	This uses the specified network address location when looking for a script
`Gateway = <IP Address>`	This uses the network gateway as the default gateway
`ip = <IP Address>`	This uses a static IP address
`Nameserver = <IP Address>`	This looks for the specified domain name server
`netmask=subnet mask`	Subnet mask is specified for the network adapter
`vlanid=vlanid`	A specific vLAN ID is used for the network adapter
`ks=protocol://<serverpath>`	This uses the given URL to locate the installation script
`ks=file://<path>`	This uses the scripts that are specified in the path
`ks=cdrom:/<path\>`	This uses the script that is located in the specified CDROM path
`ks=usb`	This looks for the `ks.cfg` file on the attached USB disk and performs the installation
`ks=usb:/path`	This uses the specified path on the USB disk for the installation script

There's more...

VMware has made available a standard installation script that can be used, or you can create a customized script based on your environment with the required parameter. The standard installation script is located on ESXi under the `/etc/vmware/weasel` path and the content of the `ks.cfg` file would be as follows:

```
#
# Sample scripted installation file
#
# Accept the VMware End User License Agreement
vmaccepteula
# Set the root password for the DCUI and Tech Support Mode
rootpw mypassword
# The install media is in the CD-ROM drive
install --firstdisk --overwritevmfs
# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0
# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

In the previously mentioned script, the end user agreement will be accepted. The password for the host will be `mypassword`, and this will obtain the IP address via DHCP on VMNIC0. The installation will happen on the first disk, and it will overwrite the existing VMFS partition. In case you are interested in using a customized script, you have the following list of commands:

▸ `install`: This command specifies that it's a fresh installation of the ESXi host.

▸ `upgrade`: This command specifies that it's an upgrade of the ESXi host.

▸ `--overwritevmfs`: This command is used in case you want to overwrite the existing datastore.

▸ `--preservervmfs`: This command will preserve any existing VMFS partition on the disk.

▸ `--firstdisk`: This command is used to specify the disk on which the installation/upgrade should happen; by default, the local disk will be chosen followed by the remote disk and USB. If you want to change the order, you need to specify the order as:`--firstdisk=USB,remote,local`.

▸ `keyboard`: This is used to set the keyboard layout type.

▸ `accepteula` or `vmaccepteula`: These commands are *required* and used to accept the VMware license agreement.

▸ `rootpw`: This command is *required*, and it's used to set the root password for ESXi.

▸ `hostreboot`: When specified, this command reboots the ESXi host after the script execution.

It is also possible to specify pre, post, and first boot sections with the help of Python or the `busybox` interpreter command. If you want to enable SSH and create an additional vSwitch, you have to mention that in the first boot section with the help of ESXCLI and `vim-cmd`. We will now see an example of enabling SSH in the first boot section:

```
%firstboot --interpreter=busybox
#commands enable and start both Local and remote tech support mode
vim-cmd hostsvc/enable_ssh
vim-cmd hostsvc/start_ssh
vim-cmd hostsvc/enable_esx_shell
vim-cmd hostsvc/start_esx_shell
```

The preceding syntax enables and starts the Local and Tech Support Modes during the first boot after the installation has been completed.

One caveat with the `%firstboot` script is that any errors in the script will not be known until the installation is complete. If you just want to parse and check the kickstart file, you can use the `dryrun` command.

The next deployment method is using Auto Deploy, which is a little complex compared to the other two methods.

Deploying ESXi hosts using Auto Deploy

Auto Deploy is another method of deploying ESXi. With the help of Auto Deploy, you can specify the image to be deployed on the host. Auto Deploy is used in two different modes, **Stateless caching** and **Stateful installs**, which are explained next.

- ▶ **Stateless caching**: In this method, the ESXi host configuration is not stored in the disk, but it's linked to an image profile. While rebooting the host, it uses the Auto Deploy server to boot, and when the server is not reachable, the host will boot from the local cache.

- ▶ **Stateful installs**: In this method, the host is provisioned with Auto Deploy, but the host configuration and state are stored in the local disk. On every reboot, the host boots from the disk just as if it were installed using the ESXi Installer.

Auto Deploy components

The following figure depicts the Auto Deploy components:
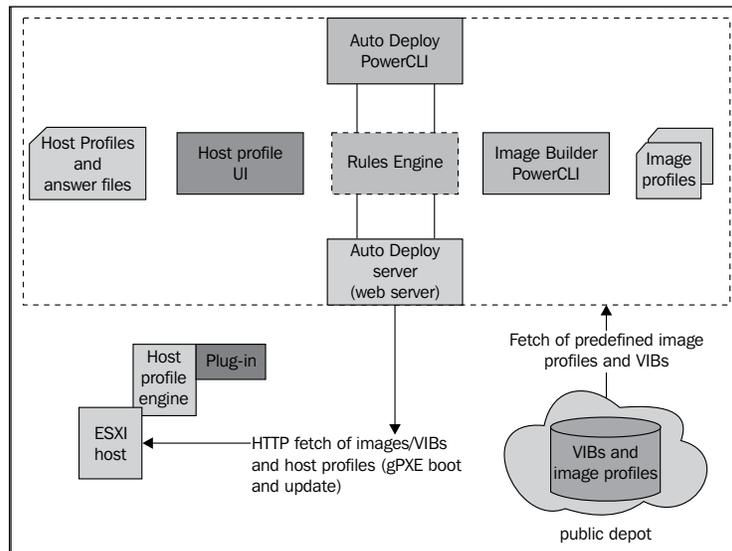
Source: VMware

Each component is explained as follows:

▸ **Auto Deploy server**: This has the information of the ESXi image and host profile, which are associated with the hosts.

▸ **Auto Deploy rules engine**: This specifies which image and host profiles have to be used by the ESXi host. The rule definition is being done by Auto Deploy PowerCLI.

▸ **Image profile**: This component specifies VIBs, which are available for download from VMware.

▸ **Host profiles**: This has been created with a reference host that will have the correct set of configuration, such as network, storage, and so on. This profile can be applied to another host to maintain a consistent configuration across the environment.

▸ **Host customization**: This stores the information that will be given by admins when the host profile is applied to the host.

Getting ready

Make sure you have following components with you:

- ▸ Auto Deploy binaries
- ▸ PowerShell and PowerCLI binaries
- ▸ TFTP software
- ▸ DHCP server
- ▸ ESXi 5.1 offline bundle file

How to do it...

In this recipe, we will learn how to deploy ESXi host using Auto Deploy.

> The steps for installing Auto Deploy Server have been covered in *Chapter 2, Installing and Using vCenter*.

Now, let's see the steps involved in deploying ESXi:

1. Install the Auto Deploy Server and it can be installed on the vCenter Server or on a new server.
2. Install PowerShell and PowerCLI along with Auto Deploy and Image Builder cmdlets.
3. Install the TFTP server on vCenter and configure the TFTP root directory (for example, `D:\TFTP_Root\`).

4. Download the TFTP Boot Zip file from the Auto Deploy Server. It can be downloaded from the vCenter Server using vSphere Web Client. Navigate to **vCenter Server** | **Manage** | **Auto Deploy** | **Download TFTP Boot Zip** and extract the content under the TFTP root directory:

5. Log in to the DHCP server and open the DHCP console, right-click on **Scope Options**, click on **Configure Options...**, and configure the following parameters:

   ❑ Select the checkbox for **066 Boot Server Host Name** and provide the TFTP server IP address:
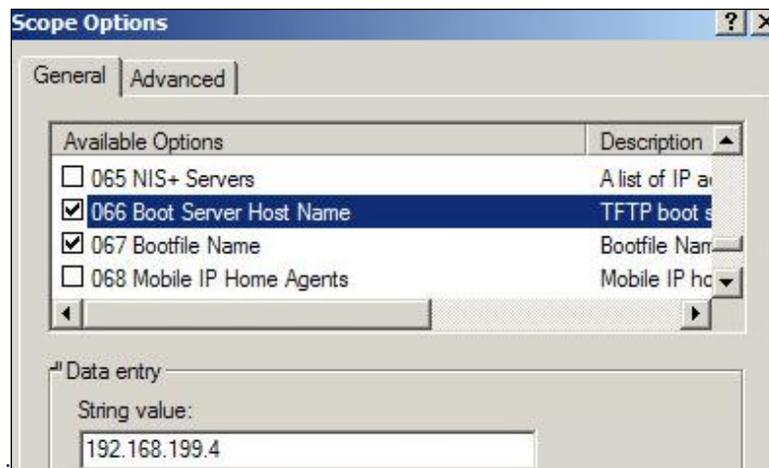
❑ Select **067 Bootfile Name** and configure **undionly.kpxe.vmw-hardwired**:

6. Make sure the host is set to PXE boot.

7. Connect to the vCenter Server using PowerCLI and import the metadata from the software depot or ZIP file using the following cmdlet:

```
Add-EsxSoftwareDepot C:\VMware-Esxi-5.1.0-799733-depot.zip
```

You can see the cmdlet in the following screenshot:

The **deployment** rule is a must, and it is created to assign an image profile to the servers, which are specified within the `Pattern` parameter. In the following example, we have created a rule name called **Adrule**, and this rule is applicable for the hosts that are within the specified IP range (10.1.1.200-10.1.1.225):

```
New-DeployRule –Name "Adrule"–Item "ESXi-5.1.0-799733-
standard" –Pattern "ipv4=10.1.1.200-10.1.1.225
```

You can see the cmdlet in the following screenshot:

```
PowerCLI C:\Windows\system32> New-DeployRule -Name "Adrule" -Item "ESXi-5.1.0-799733-standard" -Pattern "ipv4=10.1.1.200-10.1.1.225"
Downloading scsi-bnx2i 1.9.1d.v50.1-5vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading sata-sata-promise 2.12-3vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading scsi-mptsas 4.23.01.00-6vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading net-forcedeth 0.61-2vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading esx-xserver 5.1.0-0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading misc-cnic-register 1.1-1vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
Downloading net-tg3 3.110h.v50.4-4vmw.510.0.0.799733
Download finished, uploading to AutoDeploy...
Upload finished.
```

The rules that are created are not part of the rule sets until we add them manually, and there are two types of rule sets available: **active rule set** and **working rule set**. They are explained as follows:

❑ **Active rule set**: When a deployment starts, the Auto Deploy server checks the active rule set for matching rules

❑ **Working rule set**: This allows the rules to be tested before making the changes active

The deployment rule that was created previously has to be added to the active rule sets, and this can be done with the help of the `Add-DeployRule` cmdlet. By default, the rules will be added to both of the rules. If you wish to make the rule inactive, use the `NoActivate` parameter.

The following syntax will add the rule to both active and working rule sets:

Add-DeployRule -DeployRule Adrule

```
PowerCLI C:\Windows\system32> Add-DeployRule -DeployRule Adrule

Name        : Adrule
PatternList : {ipv4=10.1.1.200-10.1.1.225}
ItemList    : {ESXi-5.1.0-799733-standard}
```

8. Now, when you boot the physical host, it will start deploying the ESXi image.

There's more...

Now, let's see some of the PowerCLI cmdlets, which can be used while creating software depots and rules while using Auto Deploy:

- ▸ `Add-EsxSoftwareDepot`: This is used to import the metadata from the software depot or ZIP file
- ▸ `Get-EsxImageProfile`: This is used to list down the images that are added to the depots
- ▸ `New-EsxImageProfile`: This is used to create a new image profile by cloning the existing one or by creating an image profile from scratch
- ▸ `Export-EsxImageProfile`: This is used to export the image profile as an ISO or ZIP file once the packaging is done
- ▸ `New-DeployRule`: This is used to create a deployment rule, which matches the physical host configuration such as the host hardware or the servers, that is within a specific IP range
- ▸ `Add-DeployRule`: This is used to add rules to the working rule sets
- ▸ `Get-DeployRuleSet`: This lists the current working or active rule set

Installing vSphere Client

Now that we have seen the deployment of ESXi, the next step will be to configure the ESXi host, which is done using the vSphere Client. As an alternative to the vSphere Client, the vSphere Web Client provides a web interface for interaction with the vCenter Server system and manages the ESXi hosts through a browser. We will learn more about the vCenter Server and vSphere Web Client in *Chapter 2*, *Installing and Using vCenter*.

> With the release of vSphere 5.1, VMware has made an entire new feature available only via the Web Client if the host is managed by the vCenter Server.

Getting ready

The installer of the vSphere Client can be found in vCenter Server Installation Media. Alternatively, you can download the installer by accessing the ESXi host via a web browser where you will find a link to download the vSphere Client, which will be redirected to `vsphereclient.vmware.com`.

How to do it...

The steps involved in installing the vSphere Client are quite simple, and are as follows:

1. Run the VMware vSphere Client installer.

2. Select **Language** and click on **OK**.

3. Click on **Next** in the **Welcome to the installation** screen.

4. Click on **Next** in the **End User Patent Agreement** window.

5. Accept the End User Agreement and click on **Next**.

6. Change the **Destination** folder if required and click on **Next**.

7. Select **Install** in the **Ready to install program** screen.

8. Allow the installation to complete and click on **Finish** when done.

Configuring NTP settings on the ESXi host

ESXi uses the UTC time by default, and it's not possible to change the time zone on the ESXi host. To ensure that we maintain the correct time system across the environment, it is recommended to synchronize the ESXi host with NTP servers.

Getting ready

Before you start with the NTP configuration, make sure that you have the NTP server details and access to the ESXi host.

How to do it...

In order to configure the NTP settings, perform the following steps:

1. Log in to the ESXi host using the vSphere Client.

2. Under the **Configuration** tab, click on **Time Configuration** under **Software**.

3. Click on **Properties...** on the top-right corner:

4. Select **NTP Client Enabled** and click on **Options...**, as shown in the following screenshot:
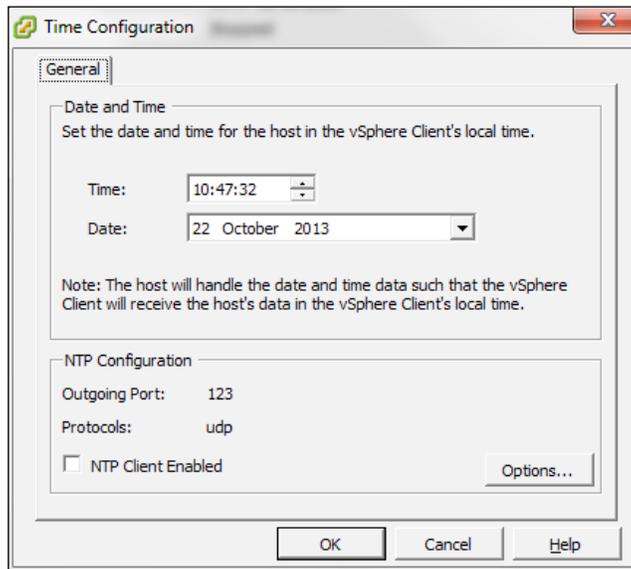
5. Under the **General** section in the left pane, select the appropriate **Startup Policy** as per your environment. VMware recommends that you choose **Start automatically if any ports are open, and stop when all ports are closed**:
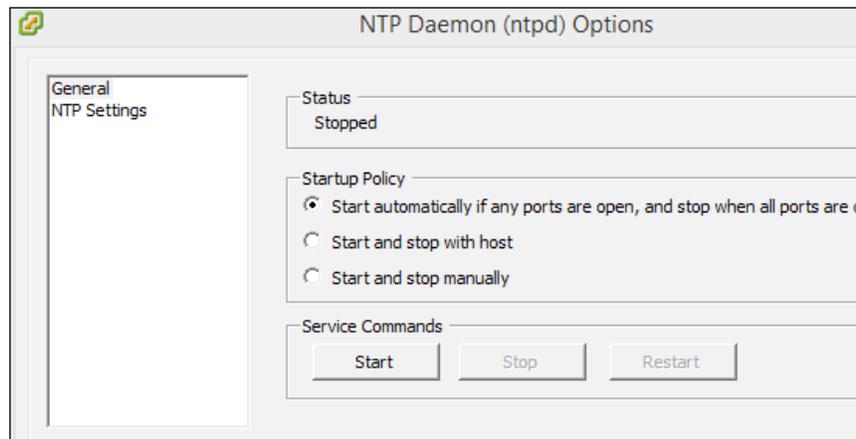
6. Select **NTP Settings** on the left pane, click on **Add**, enter the IP Address of your NTP source, and click on **OK**.

7. Select **Restart NTP service to apply changes** checkbox and click on **OK**.

There's more...

Alternatively, the NTP setting can be configured using the PowerCLI cmdlet, `Add-VmHostNtpServer`, which will help us configure the NTP setting. Make sure you connect to the vCenter Server from PowerCLI and use the following command:

```
Add-VmHostNtpServer -NtpServer "IP Address" -VMHost (Get-VMHost)
```

As an alternative, you can connect to the ESXi host using PowerCLI and execute the following command:

```
Add-VmHostNtpServer -NtpServer "IP Address"
```

Configuring DNS and Routing

Similar to the other servers in the network, you need to make sure that the ESXi host is configured with the correct DNS server and Routing details so that you do not encounter any issues.

Getting ready

Make sure that you have the DNS and default gateway details before starting the configuration.

How to do it...

In this recipe, we will learn to configure DNS and its default setting using the vSphere Client.

> You need to manually create the DNS records for the ESXi host.

Now, let's see the steps involved in creating the DNS records:

1. Login to the ESXi host using the vSphere Client.
2. Select the **Configuration** tab on the right pane and click on **DNS and Routing** under **Software**.
3. Click on **Properties** on the top-right corner of the screen.

4. In the DNS configuration, review the current configuration and make the necessary changes, such as the **hostname**, **Domain**, **DNS server**, and **search domain** fields:
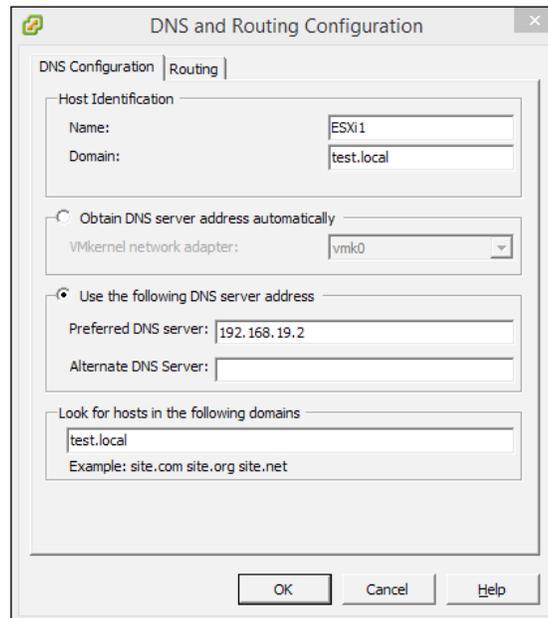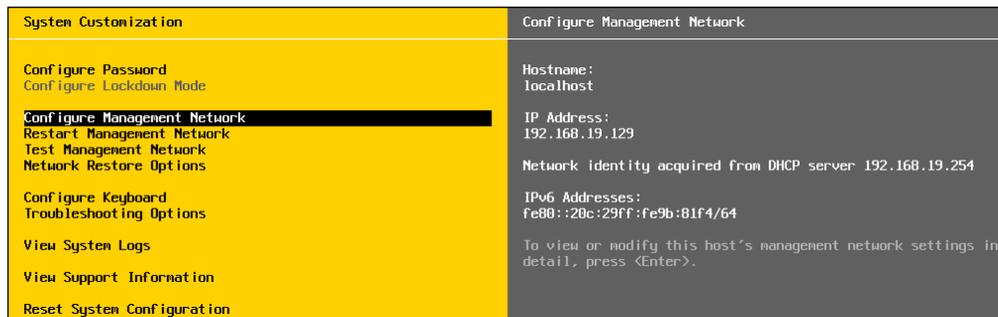

5. Click on the **Routing** tab and make sure that the correct default gateway is listed. If required, make any relevant changes and click on **OK**:
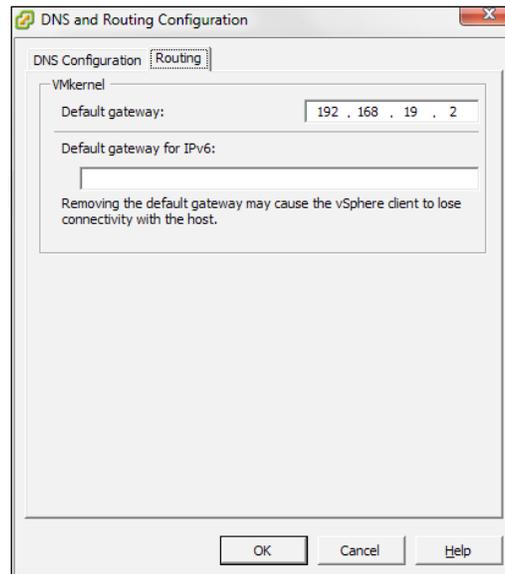
There's more...

Alternatively, you can also configure DNS and Routing using DCUI by performing the following steps:

1. Connect to the ESXi console and Press *F2* to log in to DCUI.

2. In the **System Customization** screen, move the cursor down and select **Configure Management Network**:

```
System Customization                        Configure Management Network

Configure Password                          Hostname:
Configure Lockdown Mode                      localhost

Configure Management Network                 IP Address:
Restart Management Network                   192.168.19.129
Test Management Network
Network Restore Options                      Network identity acquired from DHCP server 192.168.19.254

Configure Keyboard                           IPv6 Addresses:
Troubleshooting Options                      fe80::20c:29ff:fe9b:81f4/64

View System Logs                             To view or modify this host's management network settings in
                                             detail, press <Enter>.
View Support Information

Reset System Configuration
```

3. Select **IP Configuration** and press *Enter* to assign an IP address for the ESXi host:

```
IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must
specified:

( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:

IP Address                          [ 192.168.19.129
Subnet Mask                         [ 255.255.255.0
Default Gateway                     [ 192.168.19.2
```

4. If required, make the changes on the screen and press *Enter* and exit the screen.

5. Now, you will be back on the **Configure Management** screen; scroll down to the DNS Configuration and press *Enter* to modify the DNS IP settings.

6. You will be presented with the DNS configuration where you need to enter the DNS Server IP address and hostname of the ESXi host. When you have finished entering the details, press *Enter* to exit the screen.

```
 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      [ 192.168.19.2                              ]
 Alternate DNS Server    [                                           ]
 Hostname                [ ESXi1.test.local_                         ]


 <Up/Down> Select   <Space> Mark Selected        <Enter> OK  <Esc> Cancel
```

7. Now, you will be back on the **Configure Management** screen. Scroll down to **Custom DNS Suffixes** and press *Enter* to change DNS suffixes.

8. In **Custom DNS Suffixes**, modify the **suffixes** as required, press *Enter* for **OK**, and exit the screen:

```
 Custom DNS Suffixes

 DNS queries will attempt to locate hosts by appending the
 suffixes specified here to short, unqualified names.

 Use spaces or commas to separate multiple entries.


 Suffixes:           [ test.local_                          ]

                               <Enter> OK  <Esc> Cancel
```

9. Now, you need to save the configuration that has been changed, so from the **Configure Management Network**, press *Esc* to exit and you will be asked for confirmation on the **Configure Management Network** scene:

```
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
```
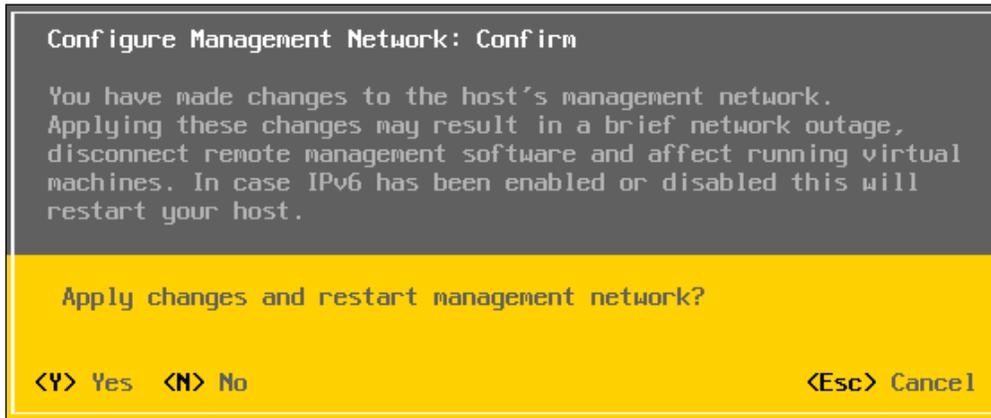
10. Press *Y* to confirm the settings; this will save the settings and restart the management network to apply the configuration.

11. You will then be back on the **System Customization** screen; if you want to make sure that the configuration is correct, you can perform the test management network operation. To proceed with the test, select **Test Management Network** and press *Enter*.

12. The ESXi host will try to ping the DNS servers and the default gateway and resolve the configured hostname:

```
Test Management Network

By default, this test will attempt to ping your default gateway
and DNS servers, and resolve your hostname.

Ping Address #0:          [ 192.168.19.2          ]
Ping Address #1:          [ 192.168.19.5_         ]
Ping Address #2:          [                       ]
Resolve Hostname          [ ESXi1.test.local      ]

<Up/Down> Select                      <Enter> OK   <Esc> Cancel
```
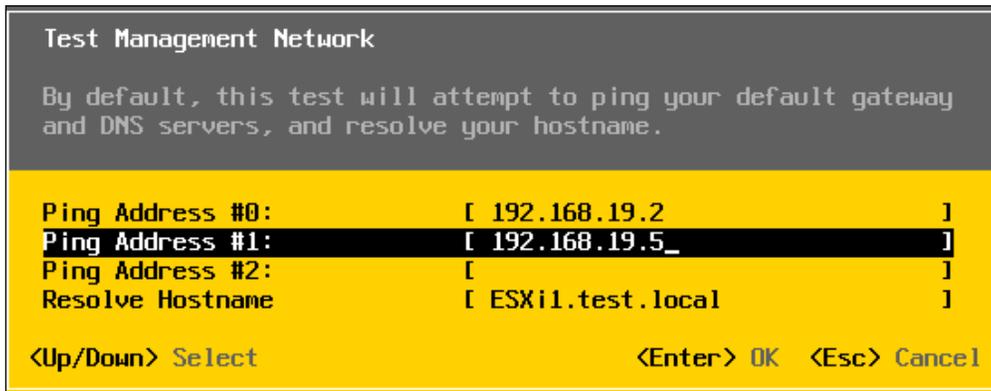
13. Press *Enter* to proceed with the testing, and the test will show the status as **OK** or **Failed**. If you notice any failure, make sure that you have configured the correct settings.

Licensing an ESXi host

By default, when you install an ESXi host, it will run in the evaluation mode for 60 days. After this period, you need to assign a license key to the host. If you are using vCenter, the license management will be done at the vCenter level by adding the license keys on vCenter and assigning them to the appropriate ESXi host. If you have only a standalone ESXi host, then you have to assign the license directly on the ESXi host.

How to do it...

The following steps have to be performed in order to license an ESXi host:

1. Connect to the ESXi host using the vSphere Client.
2. Select the **Configuration** tab in the right pane and select **Licensed Features** under **Software**.
3. Click on **Edit** on the top-right corner of the screen.
4. Select the **Assign a new license key to this host** radio button:
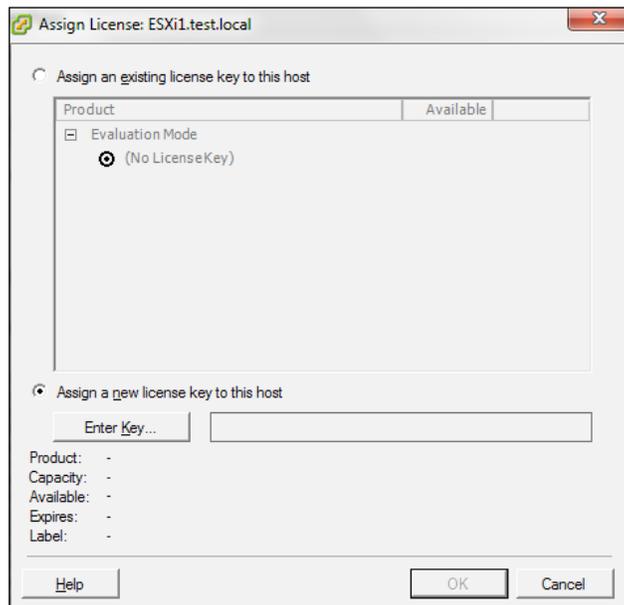
5. Click on **Enter Key...** and this will pop up an **Add license key** window, where you need to enter the license key.
6. Click on **OK** in the **Assign License Key** window.

2
Installing and Using vCenter

In this chapter, we will cover the following topics:

- ▶ Installing vCenter Single Sign-On
- ▶ Installing VMware vCenter
- ▶ Installing vSphere Web Client
- ▶ Installing vSphere Auto Deploy
- ▶ Working with the vCenter inventory objects
- ▶ Configuring the vCenter Server settings
- ▶ Working with tags
- ▶ Using schedule tasks
- ▶ Managing the plug-ins in vCenter
- ▶ Deploying VMware vCenter Server Appliance

Introduction

vCenter is one of the major components of the vSphere suite as it is required for the configuration and proper functioning of most of the vSphere features. As the virtual infrastructure keeps growing, it becomes very difficult for the vSphere administrator to manage the ESXi host individually. vCenter allows us to centralize the management of the entire virtual infrastructure by adding the ESXi host to the vCenter. Prior to vSphere 5.1, all vCenter components had to be installed on the same server. However, from vSphere 5.1, we have the option to install the vCenter 5.1 components in the same or a different server. This is because there is a change in the vCenter architecture with the inclusion of vCenter **Single Sign-On** (**SSO**). The components that are a part of the vCenter 5.1 are as follows:

- ▶ vCenter SSO
- ▶ vCenter Inventory Service
- ▶ vCenter Server
- ▶ vSphere Web Client

vCenter is available as an appliance (vCSA) and as an installer version, which can be installed on the Windows operating system. However, there are a few drawbacks of the appliance version of vCenter. The following table gives a comparison of both the versions of vCenter:

Feature	vCenter Windows	vCenter Appliance
Operating system	vCenter Windows can work on any 64-bit Windows.	vCenter Appliance is preconfigured on SUSE Linux.
Database	vCenter Windows can support database such as SQL, Oracle, and IBM DB2.	vCenter Appliance supports in-built vPostgress and external Oracle.
Host and VM support	vCenter Windows can support 1000 hosts and 10,000 VMs.	vCenter Appliance can support 100 hosts and 3000 VMs with the vPostgress database and 1000 hosts and 10,000 VMs with the Oracle database.
IP support	vCenter Windows supports both IPv4 and IPv6.	Only IPv4 is supported in vCenter Appliance.
Linked mode	This feature is supported in vCenter Windows.	This feature is not supported in vCenter Appliance.
vCenter Heartbeat	This feature is compatible with vCenter Windows.	This feature is not compatible with vCenter Appliance.
vCenter Update Manager	This feature can be installed on the same server as vCenter.	This feature should be installed on a separate Windows' server.

Feature	vCenter Windows	vCenter Appliance
Single Sign-On	This feature can be installed on vCenter's server or a different server.	This feature is preinstalled in vCenter Appliance.
Inventory Service	This feature can be installed on vCenter's server or a different server.	This feature is preinstalled in vCenter Appliance.
Web client	This feature can be installed on vCenter's server or a different server.	This feature is preinstalled in vCenter Appliance.
Auto Deploy	This feature can be installed on vCenter's server or a different server.	This feature is preinstalled here.
Syslog Collector	This feature is preinstalled on vCenter's server or a different one.	This feature is preinstalled in vCenter Appliance.
ESXi Dump Collector	This feature can be installed on vCenter's server or a different server.	This feature is preinstalled in vCenter Appliance.

The Windows' version of vCenter can be installed in two different methods: **simple install** or **custom install** method.

In the simple installation method, vCenter and the additional components are installed on the same server, whereas in the custom installation method you have an option to choose the installation of vCenter and its components in the same or separate server. vCenter has to be installed in the following order:

- ▶ vCenter SSO
- ▶ vCenter Inventory Service
- ▶ vCenter Server

The following is a small checklist to plan the installation:

- ▶ Which installation method are you using (Simple/Custom)?
- ▶ Which database are you going to use?
- ▶ Do you have the required database instance and its credential details?
- ▶ Have you verified whether the operating system is supported?
- ▶ Does the server that you are going to install for vCenter and its components meet the prerequisites?
- ▶ Are you going to install SSO in basic, **high-availability** (**HA**) cluster, or multisite mode?
- ▶ Are you going to install vCenter as standalone or in the vCenter Linked mode?
- ▶ Are you going to protect vCenter services using vCenter Heartbeat or any third-party, high-availability products?
- ▶ Are you going to change any of the default ports during the installation?
- ▶ Do you have the required SSL certificates?

It is very important that you check the database compatibility, and it can be checked from the VMware's Product Interoperability Matrixes at:

```
http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php
```

Installing vCenter SSO

vCenter SSO is a new component that has been added to vCenter's architecture in vSphere 5.1. With the inclusion of SSO, the way users get authenticated to vCenter has changed. Prior to vSphere 5.1, the users of the **Active Directory** (**AD**) domain, to which vCenter server is joined, are authenticated to vCenter Server. vSphere 5.1 supports the following types of user repositories as an identity source:

- ▸ OpenLDAP's Version 2.4 and later
- ▸ AD's Version 2003 and later
- ▸ Local operating system users where SSO is installed

Getting ready

The following prerequisites have to be met for successful installation of an SSO service:

- ▸ A valid DNS resolution.
- ▸ Microsoft .NET 3.5 SP1 Framework.
- ▸ Time is synchronized and pointing to the correct source.
- ▸ Server that is used for the installation is not a Domain Controller.
- ▸ The Server is the part of a domain (vCenter can be installed on a workgroup, but it is recommended that it is installed on domain server).
- ▸ The user account that is used for the installation has the required privileges on the server and has the following read permissions on AD:
    - ❑ It is a member of the administrators' group
    - ❑ It acts as a part of the operating system
    - ❑ It can log on as a service

One of the important steps is the database configuration for the SSO. It is necessary to have the SSO database user, admin, and table space created, as suggested by VMware. To ease this, VMware has given a preconfigured script for all the supported databases, and it can be used to create the required account and table. This script can be found in the vCenter Installation media at `Media\Single Sign On\DBScripts\SSOServer\schema`.

How to do it...

Now, let's see the steps to install SSO:

1. Run the installation media, select **vCenter Single Sign On**, and click on **Install**.

2. Select the appropriate language in the vCenter Single Sign On's **InstallShield** wizard and click on **OK**.

3. Click on **Next** on the welcome screen.

4. Click on **Next** in **End User Patent Agreement**, accept **End User License agreement**, and click on **Next**.

5. If this is the first installation of the SSO service, select the default **Create the primary node for the new vCenter Single Sign On installation**. If you are installing a secondary SSO instance for the HA or multisite mode, select **Join an existing vCenter Single Sign On installation**. If you want to recover a corrupted SSO instance from backup, select **Recover installed instance of vCenter Single Sign On from a backup** and click on **Next**:
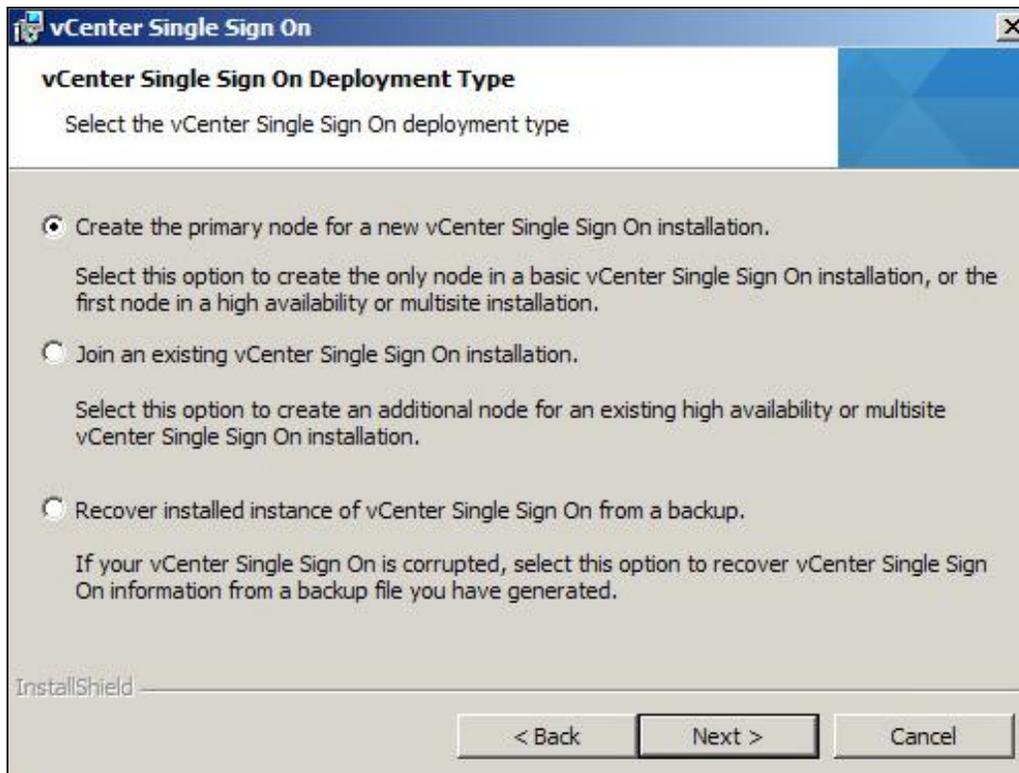
6.   Specify the vCenter SSO type and click on **Next**:
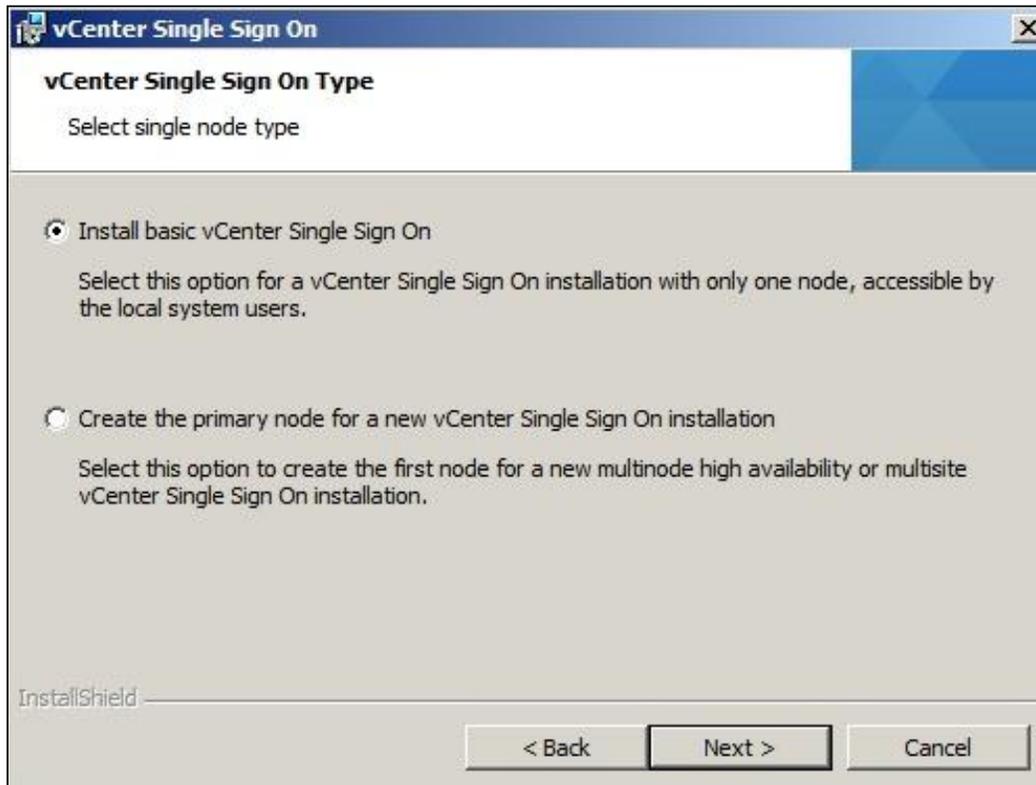
7. The **admin@System-Domain** username is the default account to manage the SSO. Enter a password and click on **Next**:

8. Now select a database and click on **Next**.

9. Here, we have chosen the SQL 2008 R2 express edition, which is bundled with the installation package. Enter the password for the DB credentials and click on **Next**:

```
vCenter Single Sign On                                                    [X]

Set Database User Information

Set the required information for vCenter Single Sign On.

Provide the database SQL user names and passwords. These user names and passwords will
be created in the database. These credentials must comply with the local or Active Directory
password policy and Microsoft SQL naming conventions. If the credentials do not comply, the
installation will fail.

DBA user name:              RSA_DBA

DBA user password :         ●●●●●●●●●●

Confirm password:           ●●●●●●●●●●

User name:                  RSA_USER

User password :             ●●●●●●●●●●

Confirm password:           ●●●●●●●●●●

InstallShield

                            < Back      Next >       Cancel
```

10. Check the **fully qualified domain name** (**FQDN**) or the IP address for the SSO server and click on **Next**.

11. Enter the user credentials to run the service and click on **Next**.

12. Select the destination folder for the SSO installation and click on **Next**.

13. By default, SSO uses the HTTPS port 7444. Accept or change the default port, and then click on **Next**.

14. On the ready to install screen, click on **Install**.

> The installation will take a few minutes to complete. Once it is done, click on **Finish**. If the installation is failing for some reason, you can check the installer logs which can be found at:
>
> `C:\Program Files\VMware\Infrastructure\`
> `SSOServer\utils\logs\imsTrace.log`
>
> `C:\Program Files\VMware\Infrastructure\`
> `SSOServer\utils\logs\install.log`
>
> `%TEMP%\vminst.log`

There's more...

In vSphere 5.1, you have an option to install vCenter Inventory Service on a separate server or in the same server. So, what does the Inventory Service do exactly? Well it's used to cache the queries from the web client and reduce the load on vCenter Server. It's also used to store all the custom tags within the web client.

The installation of the Inventory Service is fairly straightforward:

1. Run the installation media, select **VMware vCenter Inventory Service**, and click on **Install**.
2. Select the appropriate language in the VMware vCenter Inventory Service's **InstallShield** wizard and click on **OK**.
3. Click on **Next** on the welcome screen.
4. Click on **Next** in **End User Patent Agreement**, accept **End User License agreement** and click on **Next**.
5. Select the appropriate destination folder and click on **Next**.
6. Check **FQDN of the Inventory Service Server** and click on **Next**.
7. In the **Configure Ports** section, accept or change the default ports and click on **Next**.
8. It is very important to select the inventory size correctly as it determines the JVM heap settings for Tomcat and the Inventory Service. It is also possible to change the size after the installation.
9. Check **vCenter Single Sign-On information**, **Lookup Service URL** and click on **Next**.
10. Click on **Install Certificates**.
11. Click on **Install** in the ready to install the screen.

It is possible to have more than one identity source configured on the SSO server. So, that brings up the question: what if the SSO server is down? Well, you won't be able to access the vCenter Server management. So, it is necessary to have SSO configured with some redundancy so that we don't lose access to vCenter if one of our SSO servers' is down. So, you have got three different deployment modes for SSO:
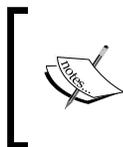
> **Identity source**: An identity source is a repository where the users and groups are stored. The repository can be AD, LDAP, or accounts that are local to an operating system.

- ▸ **Basic**: It's the default installation mode when a simple installation of vCenter is performed, and it is a standalone instance of SSO. So, if an SSO server is down, you will lose access to the vCenter management.

- ▸ **High availability**: In this mode, you can have two or more SSO servers and place them behind the network load balancer. The database and identity source used by the SSO server should be the same. Please note that this method doesn't provide any load balancing on SSO request, it just sends the request to the secondary SSO servers when primary SSO server is down. It is also worth noting that the local operating systems cannot be used as an identity source.

- ▸ **Multisite**: This mode is used when there are multiple physical locations, and each site's SSO instance is connected to the local instance of the AD and has its own database. The mode doesn't provide any site level failover. So when SSO fails in one site, the authentication is not redirected to the other site. SSO has to be deployed in the HA mode for redundancy.

Installing VMware vCenter

vCenter is one of the main components of the vSphere suite as it is required for the functioning of almost all the features in the vSphere suite.

Getting ready

Make sure the following prerequisites are met:

- ▸ vCenter Single Sign On and vCenter Inventory Service is installed.
- ▸ An operating system that is supported by 64-bit Windows is available.
- ▸ An ODBC entry with a 64-bit DSN has been created.
- ▸ Microsoft .NET 3.5 SP1 Framework has been installed.
- ▸ DNS resolution is working.
- ▸ Time is synchronized and is pointing to the correct source.
- ▸ Server that is used for the installation is not a domain controller.
- ▸ Server is a part of the domain (vCenter can be installed on workgroup, but it is recommended that you install it on the domain server).
- ▸ The user account that is used for the installation has the required privileges on the server and has the following read permission on the AD:

    - ❑ It is a member of the administrator's group
    - ❑ It acts as part of the operating system
    - ❑ It logs on as an service

How to do it...

Let's see the steps involved in this installation:

1. Run the installation media, select **VMware vCenter Server**, and click on **Install**.

2. Select the appropriate language in the VMware vCenter Server's **InstallShield** wizard and click on **OK**.

3. Click on **Next** on the welcome screen.

4. Click on **Next** in **End User Patent Agreement**, accept **End User License agreement**, and click on **Next**.

5. Enter the license key and click on **Next**. (If this is not entered, vCenter will get installed for a 60 days evaluation period.)

6. Select the database option if you are pointing to the external database. Make sure the required DSN's have already been created.

7. If you have selected the external database, you will be prompted with the credentials for the DB authentication.

8. Now, enter the user credentials under which the vCenter Server service will be running.

9. If this is the second vCenter installation in your environment and if you want to be part of Linked mode, and then select **Join a VMware vCenter server group using Linked mode**. Otherwise, if it's a first installation or you do not want to have Linked mode, select **Create a standalone VMware vCenter Instance** and click on **Next**.

> Multiple vCenter Server's can be joined using vCenter's **Linked mode**, which will allows the viewing and managing of the inventories of the linked vCenter Server systems.
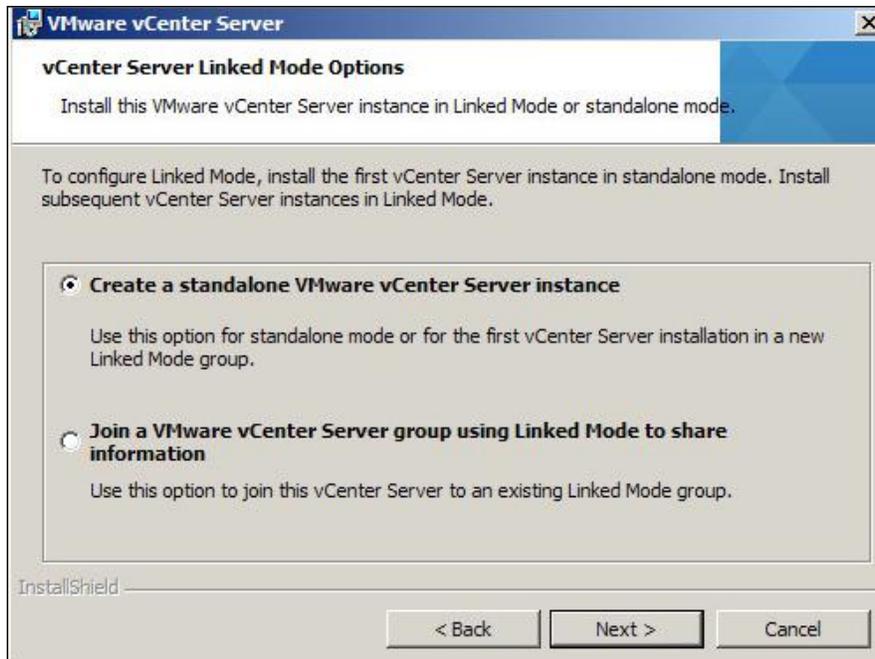
10. Accept or change the default ports and click on **Next**:
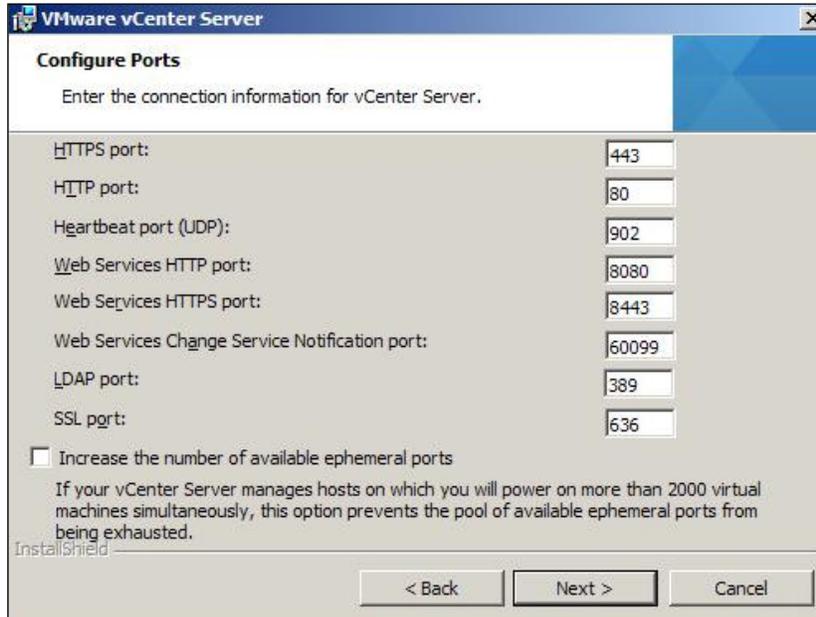
11. On the **vCenter Server JVM Memory** screen, select the option that best describes the size of your environment, and click on **Next**:
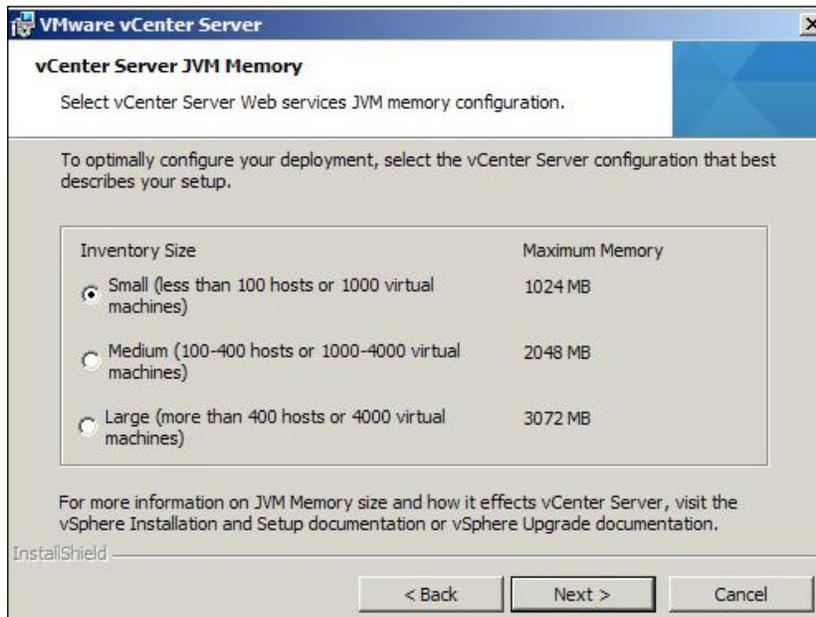
12. Provide the vCenter SSO information and **Lookup Service URL** credentials to register vCenter Server with vCenter SSO, and then click on **Next**:

13. In the next screen, provide the names of the users or groups that have to be granted administrator privileges on vCenter Server. Then, click on **Next**.

14. Enter the vCenter Inventory Service information and click on **Next**:
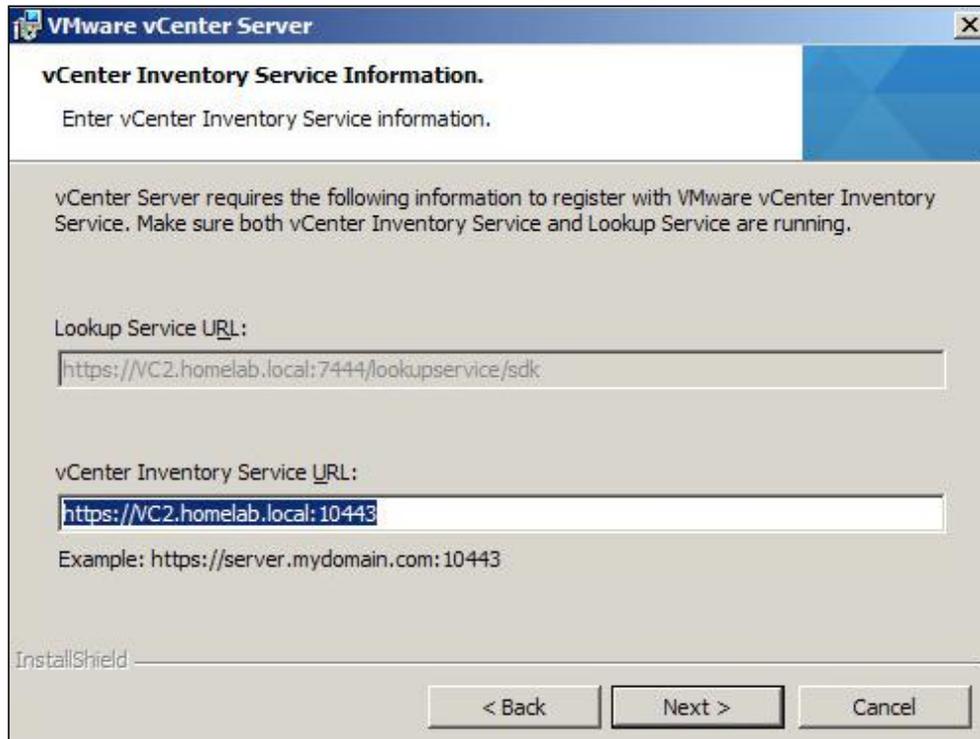
15. Select the destination folder and click on **Next**.

16. On the **Ready to install the program** screen, click on **Install**.

17. Now, the installation will begin and it will take a few minutes. Once the installation is complete, click on **Finish**.

Installing vSphere Web Client

The vSphere Web Client is the default client to manage the vSphere infrastructure, and all the new features are available only via a Web Client. However, there are still some features that are available only via the traditional vSphere client. The following table summarizes these features:

vSphere Web Client	vSphere Client
▶ vCenter SSO	▶ VMware plug-ins (VUM and SRM)
▶ Navigation with inventory lists	▶ VXLAN networking
▶ Inventory tagging	▶ Ability to change the guest OS on an existing virtual machine
▶ Work In Progress (Pause)	
▶ vSphere Replication	▶ vCenter Server Maps
▶ vSphere Data Protection	▶ Create and edit custom attributes
▶ Enhanced vMotion	▶ Connect to a vSphere host directly
▶ Distributed Switch (vDS)	▶ Inflate the thin disk option found in the datastore browser
▶ Health Check	
▶ Export/Restore Configuration	
▶ Diagram Filtering	
▶ Log Browser Plugin	

Getting ready

Make sure the prerequisites are met before starting the installation of vSphere Web Client. The prerequisites are as follows:

- ▶ vCenter SSO and Inventory Service should be running on 5.1 Version or higher.
- ▶ The account that is used for installation should be a member of the local administrator's group.
- ▶ To access the Web Client, one of the following browsers should be supported:
    - ❑ Microsoft Internet Explorer 7, 8, 9, and 10 (64-bit only)
    - ❑ Mozilla Firefox 17
    - ❑ Google Chrome 23
- ▶ Adobe Flash Player 11.1.0 should be present or should later be installed with the required plugin for the browser.

How to do it...

Let's see the steps involved in vSphere Web Client's installation:

1. Run the installation media, select **VMware vSphere Web Client**, and click on **Install**.
2. Select the appropriate language in the VMware vSphere Web Client's **InstallShield** wizard and click on **OK**.
3. Click on **Next** on the welcome screen.
4. Click on **Next** in the **End User Patent Agreement**, accept the **End User License agreement**, and click on **Next**.
5. Select the destination folder and click on **Next**.
6. The next screen provides the default ports used by the Web Client; change this if required, or accept the default and click on **Next**:
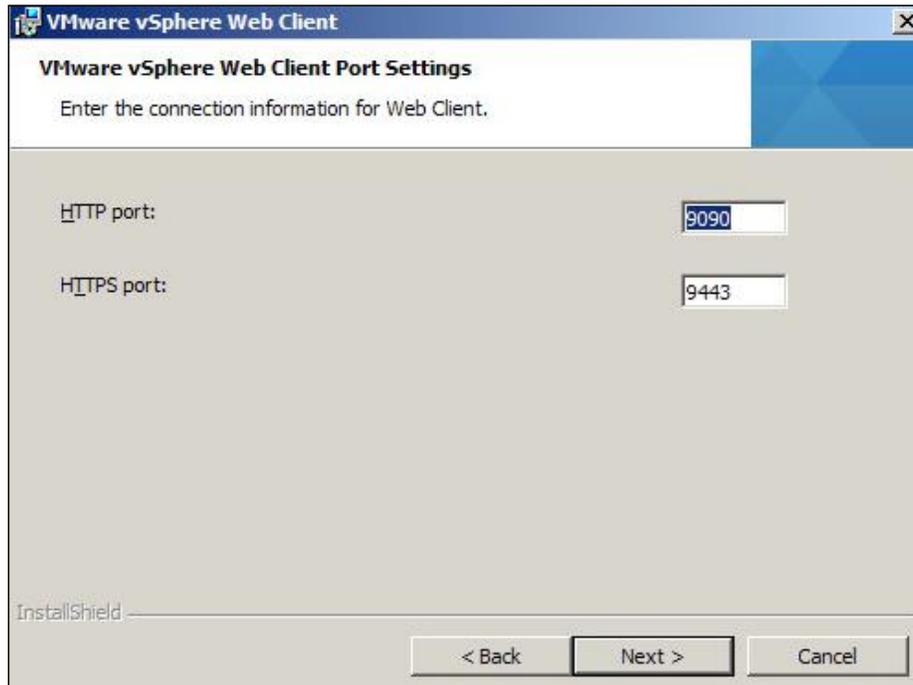
7. Provide the vCenter SSO information, **Lookup Service URL**, and click on **Next**:

8. Click on **Install** in the **Ready to install** screen, and then allow the installation to complete.

> Once the installation is complete, log in to vSphere Web Client by pointing the web browser to `https://vSphere_Web_Client_host_name_or_IP:9443/vsphere-client`.

Installing vSphere Auto Deploy

In the previous chapter, we have seen how to deploy the ESXi host using Auto Deploy. Now, you will learn the steps involved in the installation of Auto Deploy.

How to do it...

The installation of Auto Deploy can be performed using the following steps:

1. Run the vCenter Server installation media, select **VMware vSphere Auto Deploy**, and click on **Install**.

2. Select the appropriate language in the VMware vSphere Auto Deploy's **InstallShield** wizard and click on **OK**.

3. Click on **Next** on the welcome screen.

4. Click on Next on **End User Patent Agreement**, accept **End User License agreement**, and click on **Next**.

5. Change the destination folder if required. You also have an option to provide a maximum size for the Auto Deploy repository:
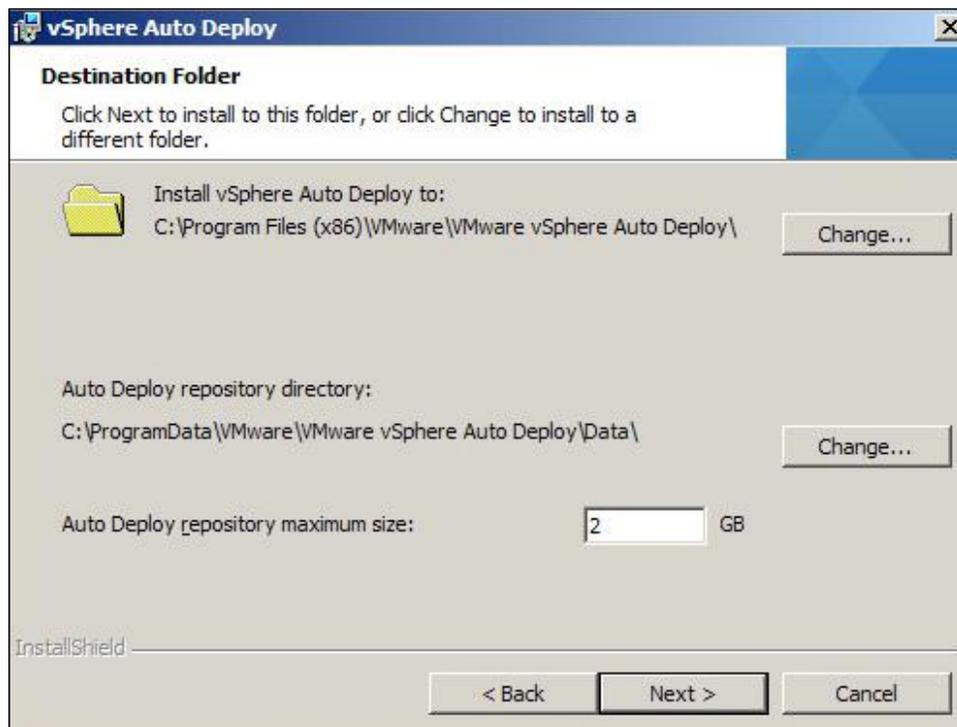
6. Provide the authentication information in the **VMware vCenter Server Information** screen and click on **Next**:

7. You will be presented with an SSL certificate warning, click on **Yes** to continue.

8. On the next screen, you will need to give the default Auto Deploy port details, review, and click on **Next**:
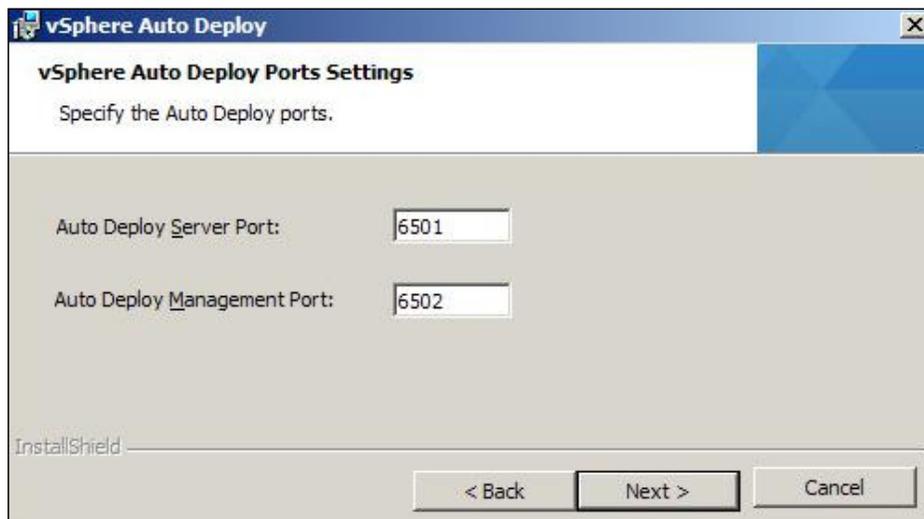
9. Specify how the Auto Deploy server has to be visible on the network; you can provide either the hostname or the IP address. Then, click on **Next**:
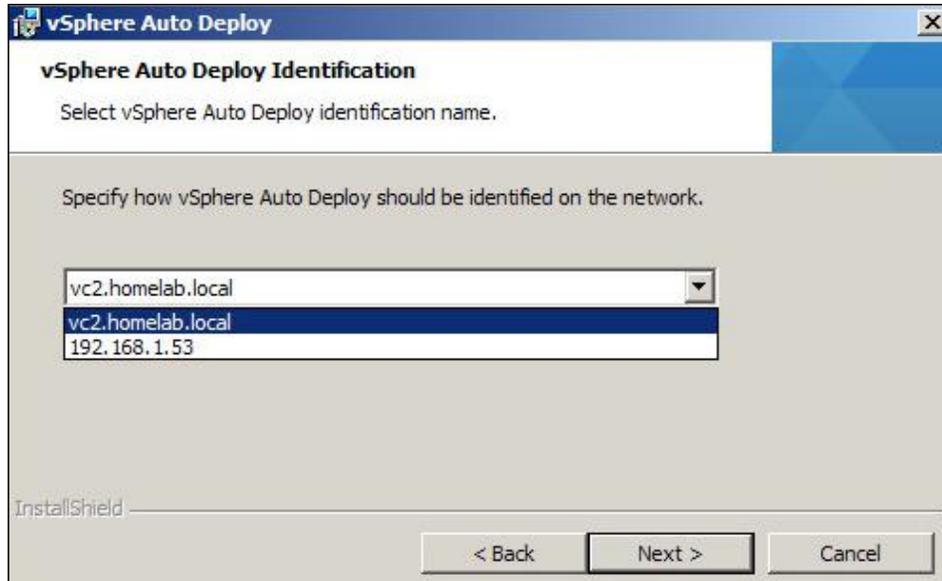
10. Click on **Install** and allow the installation to complete.

11. After the installation is complete, you can connect to vCenter Server via the vSphere Web Client and navigate to **vCenter** | **Manage** | **Settings** | **Auto Deploy**. Here, you will find the boot file that needs to be downloaded and placed on the **Trivial File Transfer Protocol** (**TFTP**) server for the Auto Deploy deployments.

Working with the vCenter inventory objects

The first step after the vCenter is built is to create a vCenter inventory as per the organization's needs. The vCenter inventory is just the logical representation of how you are going to manage the virtual environment. So, for example, if you are managing a different set of ESXi hosts' across a different geographical area, department, project, and so on, you can create a separate view for each of these and assign permissions to individual objects.

Getting ready

Connect to vCenter Server using vSphere Web Client.

How to do it...

In this section, you will learn about the various inventory objects in vCenter Server by using the vSphere Web Client that will be explained next.

Creating a Datacenter object

You can add an ESXi host directly to a Datacenter object or create a Cluster object under a Datacenter object and add ESXi to it, as explained in the following steps:

1. Log in to vSphere Web Client.

2. On the home screen, click on **vCenter** and on **Host and Clusters** under **Inventory Trees**.

3. Select the **vCenter** instance, click on the **Action** menu, and select **New Datacenter**.

4. Enter the name of the Datacenter in the pop-up screen and click on **OK**.

> Once the Datacenter object is created, the next step is to create a Cluster object or add an ESXi host to the vCenter Datacenter object.

Creating a cluster object

A cluster object has to be created to use vSphere's feature such as **High Availability** (**HA**), **Distributed Resource Scheduler** (**DRS**), and **Enhanced vMotion Compatibility** (**EVC**) as explained in the following steps:

1. Select the Datacenter on which the cluster will be created.

2. Select **Actions | New Cluster**.

3. Provide the cluster name and enable the features DRS, HA, and EVC as required.

4. Click on **OK** when the required settings are configured.

Adding ESXi hosts

So, now that you have learned to create the Datacenter and Cluster objects, the next step would be to add the ESXi host. This can be done using the following steps:

1. Log in to vCenter Server using vSphere Web Client.

2. Right-click on **Datacenter** or **Cluster** and click on **Add Host**.

3. Enter the hostname or IP address of the ESXi host and click on **Next**.

> Make sure the DNS resolution is working correctly if the hostname is used to add the ESXi.

4. Provide the credentials to connect to the ESXi host: the username will be `root` and the password will be the one that you have assigned. Then, click on **Next**.

5. Review the **Host Summary** screen and click on **Next**.

6. Assign the license keys for the ESXi host and click on **Next**.
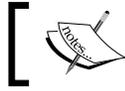
> The license key can be assigned to the host even after adding the host.

7. If required, enable the Lockdown mode and click on **Next**.

> When a Lockdown mode is enabled, no operations can be performed directly on the ESXi host, and it forces all tasks to be performed through vCenter. This applies to any script or any external management software that is schedule to run across the ESXi host. Users granted with **Direct Console User Interface** (**DCUI**) access can access the host console DCUI.

8. Click on **Finish** to add the ESXi host to vCenter Server.

Configuring the vCenter Server settings

vCenter Server is the centralized management interface for the whole virtual infrastructure. There are some advanced settings, such as logging, SMTP, and SNMP, that can be configured to help the vSphere administration. There are around 13 settings that are available for configuration.

How to do it...

In this section, you will learn to configure some of the vCenter Server settings by using the vSphere Web Client.

Configuring the licensing

vCenter Server runs on a 60-day evaluation mode if the license keys are not provided during the installation. So, once the evaluation mode has expired, you need to license vCenter Server. To assign the license key, perform the following steps:

1. Select vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **Licensing** under **Settings**.

3. Click on **Assign license key** and select **Assign a new license key** from the dropdown.

4. Enter the license key and click on **OK**.

Configuring the statistics settings

vCenter Server collects the performance statistics of the managed object and stores the information in the database. This information can be accessed through a command line or performance charts when required.

There are four levels of data collection available. The steps to perform the changes in the statistics settings are as follows:

1. Select vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Click on **Edit** and select **Interval Duration** and **Statistics level required** in **Statistics intervals**, and then click on **OK**.

> By default, the collection intervals are as follows:
>
> - Samples that are collected every 5 minutes are stored for a day
> - Samples that are collected every 30 minutes are stored for a week
> - Samples that are collected every 2 hours are stored for a month
> - Samples that are collected for a day are stored for a year

Configuring the runtime settings

The runtime settings are used when there are multiple vCenter Servers in the environment. The wizard will help you to change vCenter Server's unique ID, vCenter's managed address, and the vCenter Server name. To configure the settings, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Click on **Edit** and select **Runtime Settings**. Enter the unique settings for vCenter Server and click on **OK** after finishing.

> If the runtime setting has been changed, then vCenter Server has to be restarted for the changes to take effect.

Configuring the user directory settings

The user directory settings help us to set the way vCenter Server interacts with the active directory for authentication. This can be done by setting the timeout value (in seconds), limiting the users and groups that are queried against the active directory database, and enabling the validation and the validation period (in minutes) of vCenter Server to check users and groups in the directory's server. To perform the changes, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Click on **Edit** and select **User Directory**. Provide the unique settings for vCenter Server and click on **OK** after finishing.

Configuring the mail settings

The mail settings would be one of most commonly used settings, as this allows vCenter Server to send e-mail notifications when there is an alarm triggered. The SMTP server and the sender account details have to be configured. To configure the settings, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Select **Mail** in **Edit vCenter server settings**. In **Mail Server**, provide the SMTP server's IP address, provide the sender's e-mail account information in **Mail Sender**, and then click on **OK**.

Configuring the SNMP settings

vCenter server has the ability to send SNMP trap notifications to the monitoring server when an event is triggered. Up to four SNMP receivers can be configured. For each receiver's hostname, a port and a community string has to be provided. To configure the settings, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Select **SNMP receivers** in **Edit vCenter server settings**. In **Receiver URL**, provide the hostname or IP address of the SNMP receiver. In **Receiver port**, provide the port number used by the SNMP receiver and type the **Community identifier** in **Community string**.

4. Click on **OK**.

Configuring the timeout settings

The timeout option specifies the period of time after which the Web Client has to timeout for a particular operation. You will configure a timeout for normal and long operations. By default, for a normal operation the timeout is 30 seconds and for a long operation it's 120 seconds. To perform the changes, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.

2. In the **Manage** tab, select **General** under **Settings**.

3. Select **Timeout Settings** in **Edit vCenter Server settings**, and specify the timeout value in both **Normal operation** and **Long operation**.

4. Click on **OK** when finished.

5. Then, restart vCenter Server.

Configuring the logging options

When it comes to the troubleshooting, the log files play an important role. The logging option allows you to configure the level of logging that will be captured by vCenter Server. There are six levels of logging available:

- ▸ **None (Disable Logging)**: In this option, logging will be turned off and no logs will be captured. It's not the recommended setting in a production environment.
- ▸ **Error (Errors only)**: This option only displays error messages.
- ▸ **Warning (Errors and Warnings)**: This option only displays warning and error messages.
- ▸ **Info (Normal Logging)**: This option only displays information, warning, and error messages.
- ▸ **Verbose (Verbose)**: This option displays information, error, warning, and verbose messages in the vCenter log entries. It is used for troubleshooting purposes.
- ▸ **Trivia (Extended Verbose)**: This option displays information, error, warning, verbose, and trivia logs in the vCenter log entries.

> The log files are located in the following locations:
>
> - ▸ **vCenter Server 5.x and earlier versions on Windows XP, 2000, 2003**: `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter\Logs\`
> - ▸ **vCenter Server 5.x and earlier versions on Windows Vista, 7, 2008**: `C:\ProgramData\VMware\VMware VirtualCenter\Logs\`
> - ▸ **vCSA log file**: `/var/log/vmware/vpx/`

To configure the logging, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.
2. In the **Manage** tab, select **General** under **Settings**.
3. Select **Logging Settings** in **Edit vCenter server settings**, and then select the appropriate logging options.
4. Click on **OK** when finished.

Configuring the database settings

The database settings allow to you to configure the maximum number of simultaneous connections to the backend database, and you can also configure the database retention for the events and tasks retained in the database server. To configure the database settings, follow the given steps:

1. Select the vCenter Server instance in vSphere Web Client.
2. In the **Manage** tab, select **General** under **Settings**.

3. Select **Database settings** in **Edit vCenter server settings** and enter the maximum connection. Then enable the retention for the tasks and events required.

4. Click on **OK** when finished.

> If you want to maintain the logs all the time doesn't enable the database retention.

Configuring SSL settings

The SSL settings have the ability to validate that both vCenter and the Web Client have a valid SSL certificate before making a connection to the ESXi for adding or while making remote console connection to the virtual machines.

Configuring advanced settings

The advanced settings wizard is used to perform any addition to the vCenter configuration file (`vpxd.cfg`) with the advanced parameters.

> The advanced parameters have to be added and modified only when instructed by VMware GSS team.

Working with tags

Tagging is a new feature which is available in vSphere 5.1 and it's enhancement to the custom attribute enabled users to categorize inventory objects. Tags are classified in categories and there are two types of categories where only one tag can be assigned to the object, or multiple tags can be assigned to the object.

An example of tagging is if you want to group the VMs based on an operating system such as Windows, Linux, and so on; first you create a category called "OS" and specify that only one tag can be applied to VMs. Then create a tag in the category (OS) called Windows, Linux, and so on.

How to do it...

Creating a tag and applying it to an object is a three step process. You will learn how to perform it in the next sections.

Creating a tag category

The first step in the tagging process is to create a category; the steps are as follows:

1. In the vSphere Web Client home page, click on **Tags** in the left pane.

2. Select the **Items** tab and click on **Categories**.

3. Click on the New Category Icon.

4. In the **Category** options provide **Category Name**, **Cardinality**, and **Associated object types**.

> **Cardinality**: Here you will select either one tag per object or many tags per object. Note that once cardinality has been set, it is possible to change from one tag per object to many tags per object but not vice-versa.
>
> **Associate object types**: Here you will select whether the tag is restricted to a certain object or if it can be assigned to all types of object

5. When finished click **OK**.

Creating a tag

Once a tag category has been created, the next step is to create tags:

1. On the vSphere Web Client home page, click on **Tags** in the left pane.

2. Select the **Items** tab and click on **Tags**.

3. Click on the New Tag icon.

4. If the vCenter is in Linked mode, select the appropriate vCenter name for which the tag has to be created.

5. Provide a name for the tag.

6. Select a category which has already been created or if required create a new category.

7. When finished click on **OK**.

Assigning a tag to an object

After the categories and tags have been created, the next step is to apply them to the object:

1. Select the object in vSphere Web Client.

2. Select the **Manage** tab and click on **Tags**.

3. Select the Assign Tag icon and select the tags from the list.

4. When finished click on **OK**.

Using schedule tasks

vCenter provides an option to schedule certain repetitive tasks with the help of vSphere Web Client. For instance, if you want to keep rebooting a VM every day at a certain point in time, you can create a scheduled task and automate the process. The scheduled task can be used for a limited number of operations by using the Web Client. For any tasks that are not available, vSphere API can be used. The list of tasks that can be automated with the help of scheduled tasks is as follows:

- ▶ Changing the power state of a VM
- ▶ Creating a VM
- ▶ Deploying a VM
- ▶ Cloning a VM
- ▶ Migrating a VM
- ▶ Taking a snapshot of a VM
- ▶ Adding a host
- ▶ Changing the cluster power settings
- ▶ Scanning for updates
- ▶ Remediation
- ▶ Checking the compliance of a profile

How to do it...

Now, let's see the steps to create and remove a scheduled task from vSphere Web Client.

Creating a schedule task

The steps to create a scheduled task are as follows:

1. Connect to vCenter Server using Web Client.
2. Navigate to an object (Datacenter, Cluster, Host, or VM) for which you want to schedule a task.
3. Click on **Manage** tab and select **Scheduled Tasks**.
4. From the **Schedule New Task** drop-down list, select the task that you want to schedule.
5. The wizard will open to schedule the task that you have selected in the previous step.
6. On the **Scheduling Options** screen, enter the name and description of the task.

7. To configure the scheduling settings, click on **Change next to Configured Scheduler**, which will then provide you with the following options:

   ❑ **Run this action now**: It will run the task immediately.

   ❑ **Run this action after startup**: It will run the task after a certain amount of minutes.

   ❑ **Schedule this action to run later**: It will run the task at the date and time which you specify.

   ❑ **Setup a recurring schedule for this action**: It will run the task based on the recurring schedule which you have defined. Available recurring schedules are **Hourly**, **Daily**, **Weekly**, and **Monthly**.

8. Setup an e-mail notification about the task status that will be sent, and then click on **OK**.

Removing a schedule task

The steps for removing a scheduled task are as follows:

1. Connect to vCenter Server using vSphere Client.
2. Navigate to the object (Datacenter, Cluster, Host, or VM) for which you want to edit a scheduled task.
3. Click on **Manage** and select **Scheduled Tasks**.
4. Right-click the scheduled task and select **Remove**.
5. Click on **OK**.

There's more...

As a vSphere administrator, you will spend a considerable amount of time with the vCenter Management Interface to perform the day-to-day administrative tasks. In the following subsections, you will learn about the vCenter maps, log browser, and roles and permissions.

vCenter maps

vCenter maps helps to identify the relationship between the different objects within the **Virtual Infrastructure**. This feature comes very handy when you want to identify to which network and datastore a particular VM is connected. Also, it helps when you are documenting the Virtual Infrastructure. vCenter provides a map relation for these resources:

▶ Virtual Machine resource

▶ Host resource

▶ Datastore resource

In addition to the preceding three resources, you can also customize the maps based on your needs and you will find out the hosts that are compatible for the vMotion. vCenter provides you with an option to view the maps within the vSphere Client, or you can print or export the maps to an image file for any further analysis.

The log browser

When troubleshooting a problem, the first place that you will look is the logs. In vSphere Web Client, with the help of the log browser, you can view and search the logs for a specific host or vCenter or you can browse the log file for individual objects. When you are viewing the log browser for the first time, there is a chance that no logs will be displayed. So, you need to retrieve the logs by selecting the object. There are different options available through the log browser:

- **Search Log Files**: This option allows the searching of log files by text or time
- **Filter Log Files**: This option allows the filtering of log files based on a particular word
- **Adjust Log Times**: This option allows the adjustment of the times in log files to a different time zone
- **Export Logs**: This option allows the exporting of the logs to a local system

Roles and permission

Roles are a predefined set of privileges. When you assign permission to a user or group, you are mapping a user or group with a role from the available list of roles. Either you can map a user or group with the existing default roles, or you create a role and select the privileges as per your organizational needs, and then assign a user or group to the newly created custom roles. All default roles are assigned with predefined permission. You cannot edit defined permissions for the default roles. You can either create a role, or you can clone an existing role and change the permissions. The following is a list of default roles that are available in vCenter Server:

- No access
- Anonymous
- View
- Read-only
- Administrator
- Virtual Machine Power User (sample)
- Virtual Machine user (sample)
- Resource pool administrator (sample)
- VMware Consolidated Backup user (sample)
- Datastore Consumer (sample)
- Network administrator (sample)

Managing the plug-ins in vCenter

The VMware vCenter plugin allows the addition of new functionality to vCenter Server. vCenter Server is developed with a highly extensible architecture. Many third-party plug-ins, such as hardware management, storage management, and monitoring software, can be integrated with the vCenter. By default, there are a few plug-ins available with the vCenter Server installation and a few more plug-ins will be added to vCenter Server. If you have added additional components, such as Update Manager, Converter, vCOPS, Auto Deploy, the plugin would allow you to manage the add-on components from vCenter Server.

How to do it...

Now let's see the steps to install and manage the vCenter plugin:

Installing plug-ins

The plug-ins can be installed using **Plugin manager**:

1. Log in to vCenter Server using vSphere Client.
2. Click on **Plug-ins | Manage Plug-ins**.
3. In the **Available Plug-ins** section, you will find a list of the plug-ins available for the vCenter instance. Click on **Download and Install** to complete the installation.
4. Once the plugin is installed, it will be listed in the **Installed** section and status will show as **enabled**.

Enabling and disabling the plug-ins

Here's how we can enable and disable a plugin:

1. Log in to vCenter Server using vSphere Client.
2. Click on **Plug-ins | Manage Plug-ins**.
3. In the **Installed Plug-ins** section, right-click on the plugin and select **enable** or **disable**.

There's more...

The following default plug-ins are installed and enabled as a part of the vCenter installation:

- ▸ **vCenter service Status**: This plugin helps to display the health status of the vCenter Server services
- ▸ **vCenter server storage monitoring**: This plugin helps to review and monitor the storage usage
- ▸ **vCenter hardware status**: This plugin helps to display the hardware status of the ESXi hosts by using the CIM monitoring

Deploying the VMware vCenter Server Appliance

The **vCenter Appliance** (**vCSA**) is based on the SUSE OS that is preinstalled with vCenter Server and the other vCenter components. vCSA is configured with two vCPUs, 8 GB RAM, and two virtual disks of the size 25 GB and 60 GB.

Getting ready

Download vCSA from the VMware website.

How to do it...

Now, let's see the steps involved in deploying and configuring vCSA:

1. Connect to the ESXi host using vSphere Client.

2. Click on **File** | **Deploy OVF Template**.

3. In the **Source** screen, provide the URL to download the OVF package or the location of OVA file where it has been downloaded to. Then, click on **Next**.

4. Review and click on **Next** in the **OVF Template** details screen.

5. Provide a name for the appliance and click on **Next**.

6. Select the storage (**Datastore Location**) and click on **Next**.

7. Select the **Disk Format** as required and click on **Next**.

8. Map the **Port group** for the VM and click on **Next**.

9. Click on **Finish** in the **Ready to complete** screen.

Deployment will begin and you can verify the status in the **Recent Tasks** pane.

3. Press *6* to assign a static IP address. Similarly, configure the hostname and DNS settings from the console.

4. Once the configuration is completed, access vCSA from a web browser to log in to vCSA. For example, `https://vCSA_IP Address:5480`.

5. When you have logged in, you will be prompted to accept the license agreement:
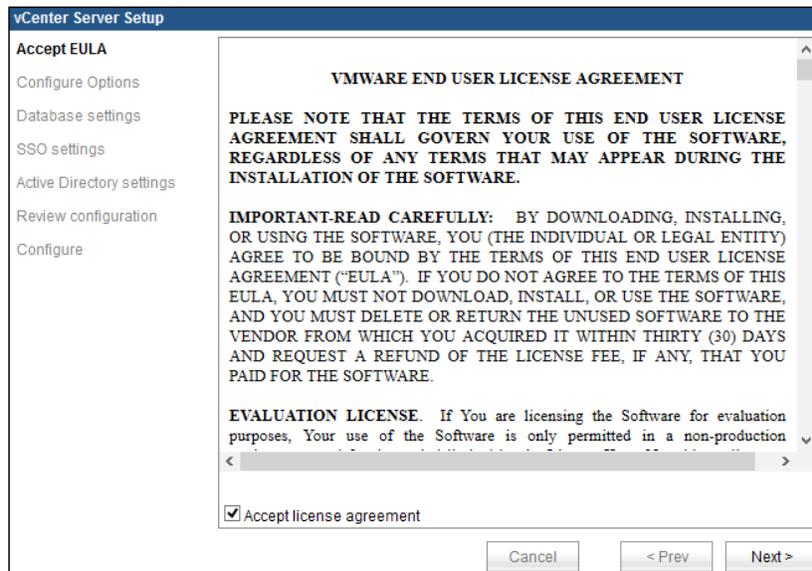
6. In the **Configure Options** screen, select the appropriate option and click on **Next**:
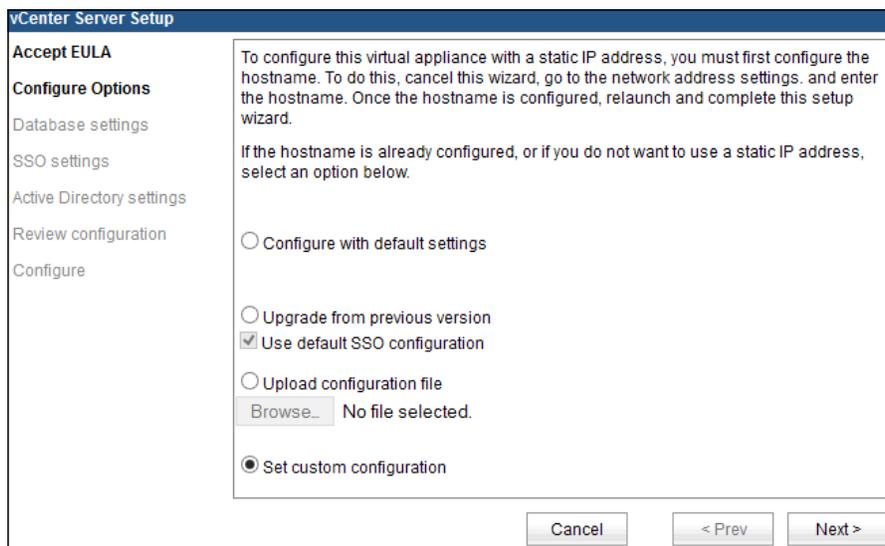
7. In the **Database settings**, you will choose the **embedded** DB or an external **oracle** DB. Select as appropriate and click on **Next**:

8. Select the SSO database and the deployment type, and then click on **Next**:

9. In the **Active Directory settings** screen, you will have an option to join vCSA to the AD domain. Provide the domain details and the required credentials, and then click on **Next**:

10. Review the configuration and click on **Start** to proceed with the configuration:

3
Networking

In this chapter, we will cover the following topics

- ▶ Creating and deleting VM network port groups
- ▶ Creating VMkernel port groups
- ▶ Modifying vSwitch properties
- ▶ Working with vSphere Distributed Switches
- ▶ Configuring Private VLANs (PVLAN)
- ▶ Working with advanced networking
- ▶ Enabling jumbo frames
- ▶ Configuring network policies

Introduction

Networking plays an important role in the Infrastructure as it provides communication to different components in the environment. VMware provides a software-based switch that resides on VMkernel, which provides communication between the VMs on the same host and to other devices on the physical network. The virtual switches are operated in the same way as traditional physical switches and provide functions such as layer 2 switching, VLAN segmentation, and maintaining MAC addresses. There are two types of virtual switches provided by VMware, and they are as follows:

- ▶ **vSphere Standard Switches** (**vSS**): This is created by default when an ESXi host is installed with a VMkernel port group for the Management traffic. vSS is used for the ESXi host communication and is available on all editions of the vSphere license. If vSS is used in the environment, it is necessary to configure vSS on all the ESXi hosts individually and maintain a consistent configuration.

- ▶ **vSphere Distributed Switches** (**vDS**): These configured and managed at the vCenter level, and there is no need to create the virtual switches at the individual host level. vDS provides additional features compared to vSS. To use vDS, you need to have enterprise plus license.

Now, let's look at some of the terminologies used in vSphere networking:

- ▸ **vSS**: This is a vSphere Standard Switch.
- ▸ **vDS** : This is a vSphere Distributed Switch
- ▸ **Port Group**: It is a logical object on a virtual switch that provides network traffic for VMkernel and VMs.
- ▸ **Uplink**: This is a physical NIC, which connects to an external physical network.
- ▸ **Vmnic**: This is a physical Ethernet adapter present on the server.
- ▸ **vNIC**: This is a virtual network adapter that is connected to the VM.

Creating and deleting VM network port groups

For the Virtual Machine communication, you will need to create a separate port group, and you will learn how to create and delete the vSwitch.

Getting ready

To create the VM Port group, you need to have the following details: VLAN ID (optional), uplink to be used, and network label.

How to do it...

In this section, you will see the steps to create and delete a VM network port group in vSwitch.

The following steps will create a Virtual Machine port group:

1. Log in to the vSphere Web Client and browse to an ESXi host.
2. Click on the **Manage** tab.
3. Click on the **Networking** tab, then click on **Virtual switches** and select the add host networking icon, as shown in the following screenshot, or navigate to **Actions | All vCenter Action | Add Networking**:
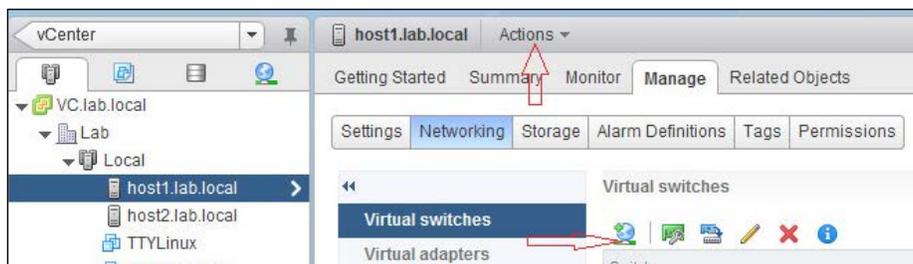
4. Select the connection type as **Virtual Machine Port Group for a Standard Switch**, as shown in the following screenshot, and click on **Next**:

5. In the target device section, select **New standard switch** and set the **Number of ports** from the drop-down menu, as shown in the following screenshot, click on **Next**:
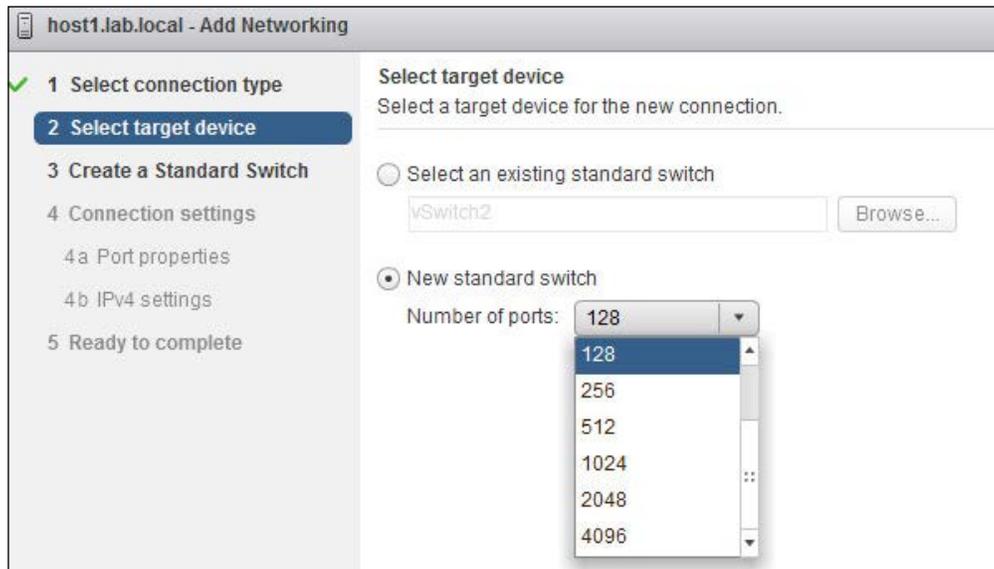
6. Click on the **+** icon to assign one or more physical adapter(s) to the vSwitch:

    1. In the **Failover order group** drop-down menu, select **Active Adapters**.

    2. In the **Network Adapter** dropdown, select the uplink for the vSwitch and click on **OK**.

> It is also possible to create a vSwitch without any network adapters. This switch would be called as an internal-only switch.

7. Click on **Next** to continue.

8. Provide a **Network Label** for the VM port group, **VLAN ID** (optional) if required, and click on **Next**.

9. In the **Ready to complete** screen, review the settings and click on **Finish**.

The following steps will delete a Virtual Machine port group:

1. Log in to the vSphere Web Client and browse to an ESXi host.

2. Click on the **Manage** tab.

3. Select the **Networking** tab, click on **Virtual switches**, and select the vSwitch on which the port group exists.

4. Select the port group and click on the **Remove selected port group** icon.
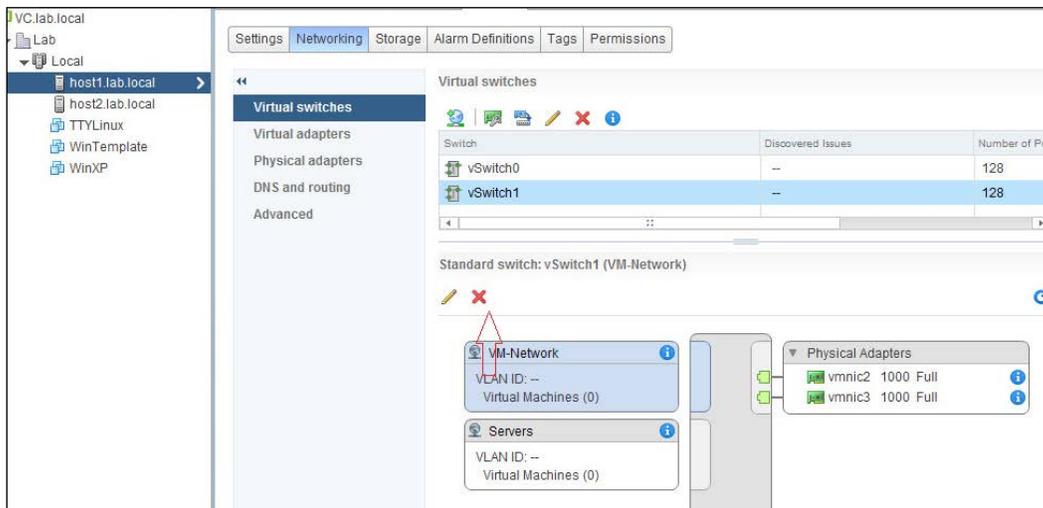
How it works...

A vSwitch with a VM port group acts similar to that of an unmanaged physical switch. Multiple uplinks can be added to the vSwitch and they are connected to the physical switch. The physical switch ports are configured with the required VLAN and they are placed in the trunk. The default ports on the vSwitch are 128, but only 120 ports will be available and shown via the GUI interface and the remaining 8 ports are reserved by VMkernel for its own use. The VLAN ID would be in the range of 1-4094, but VLAN ID 4095 is also used by the vSphere environment, which is called as virtual guest tagging. The use of VLAN ID 4095 can be used in the guest OS that supports and understand the VLAN tags.

There's more...

There are multiple ways to create and configure vSS; it can be done either using ESXCLI commands or VMware PowerCLI. Now, let's see some of the tasks which can be performed using ESXCLI. Run the following SSH commands on the host using Putty:

- ▸ To create a new vSphere standard switch called vSwitch1:

  ```
  esxcli network vswitch standard add -v vSwitch1
  ```

- ▸ To list all standard virtual switches and its associated port groups:

  ```
  esxcli network vswitch standard list
  ```

- ▸ To list a port group currently associated with the standard virtual switch:

  ```
  esxcli network vswitch standard portgroup list
  ```

- ▸ To list the information about all the VMkernel network interfaces:

  ```
  esxcli network ip interface list
  ```

- ▸ To list the uplink adapters associated with the virtual switch:

  ```
  esxcli network vswitch standard list
  ```

Creating VMkernel port groups

A VMkernel port group is created when an IP-based storage is being used, and it is also required when you configure vMotion and FT in the environment. By default, a VMkernel port group is created when an ESXi host is deployed for Management traffic.

Getting ready

A separate IP address is required while creating the VMkernel port group, so have the IP address, subnet mask, and default gateway ready.

How to do it...

Now, let's look at the steps involved in creating a VMkernel portgroup:

1. Log in to the vSphere Web Client and browse to an ESXi host.

2. Click on the **Manage** tab.

3. Select the **Networking** tab, click on **Virtual Switches**, and click on the add |host networking icon, as shown in the following screenshot, or navigate to **Actions** | **All vCenter Action** | **Add Networking**:
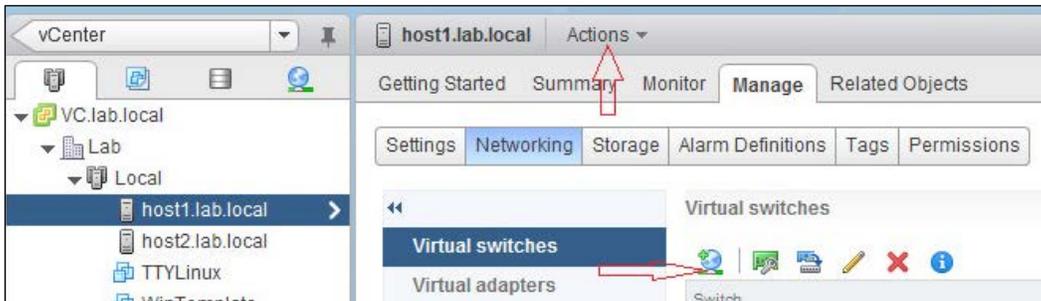
4. Select the connection type as **VMkernel Network Adapter**, as shown in the following screenshot, and click on **Next**.

5. In the **Select target device** screen, you will have the option to either use the **Select an existing standard switch**, as shown in the following screenshot, or create a **New standard switch** and click on **Next**:

6. If the **New standard switch** option is selected, you will be asked to select the physical adapter for the vSwitch, as explained in the previous recipe. In the **Port properties** screen, provide a network label, VLAN ID, and IP settings. Optionally, you can also enable the following services, which are shown in the following screenshot:

   - **vMotion traffic**
   - **Fault Tolerance logging**
   - **Management traffic**
   - **vSphere Replication traffic**
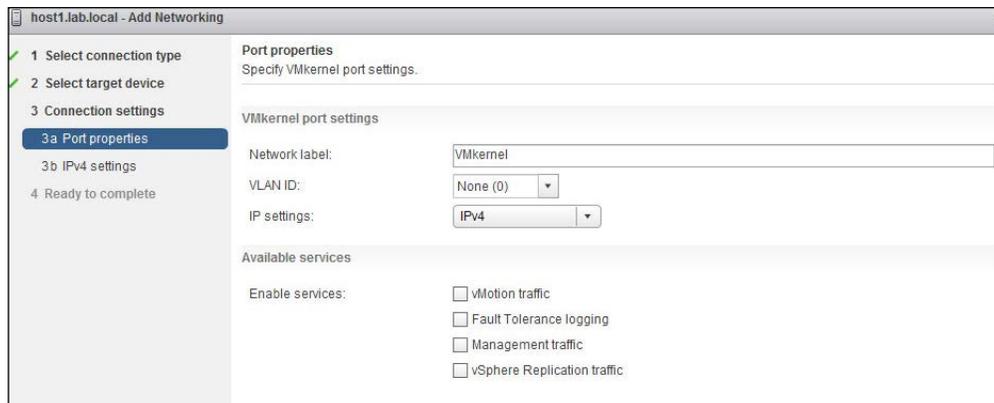
7. The next step is to configure the **IPv4 settings** for the VMkernel port group; you have the option to choose IPv4 or IPv6 or both.

8. If IPv4 is being selected, you can either set it to **Obtain IPv4 settings automatically** or **Use static IPv4 settings** (recommended), which shown in the following screenshot:

9. If IPv6 is being used, select either **Obtain IPv6 address automatically through DHCP**, **Obtain IPv6 address automatically through Router Advertisement**, or **Static IPv6 addresses**, which are shown in the following screenshot:

10. Click on **Next** when the IP address has been set.

11. In the **Ready to complete** screen, review the configuration and click on **Finish**.

How it works...

A VMkernel port group is used for the communication of the ESXi host, which we call as management traffic. In addition to this, a VMkernel port group is required for the functioning of vMotion, IP-based storage traffic, Fault Tolerance (FT), and vSphere replication. VMkernel port groups can be created in the same vSS where the VM port group exists, or you can create a dedicated vSS for the VMkernel traffic. A VMkernel port group has two different components: a port in a vSS and in vmknic, where you need to assign an IP address.

> It is recommended that you create a separate vSS with dedicated uplinks for the VMkernel port group traffic.

There's more...

Similar to creating a standard port group using ESXCLI, it is also possible to create a VMkernel interface; the following are some of the commands that can be used:

- To create a port group called `MGMTNET` in a standard virtual switch `vSwitch1`:

  ```
  esxcli network vswitch standard portgroup add -p MGMTNET -v
    vSwitch1
  ```

- To create a new VMkernel interface called `VMK1` in the `MGMTNET` port group:

  ```
  esxcli network ip interface add -i vmk1 -p MGMTNET
  ```

- To configure the `192.168.0.76` IP (IPv4) address with the `255.255.255.0` subnet mask for a newly added VMkernel interface, `vmk1`:

  ```
  esxcli network ip interface ipv4 set -i vmk1 -I 192.168.0.76 -
    N 255.255.255.0 -t static
  ```

- To set up a port group with the VLAN ID, `25`, for the `MGMTNET` port group:

  ```
  esxcli network vswitch standard portgroup set -p MGMTNET
    -v 25
  ```

Modifying vSwitch properties

Sometimes you may need to modify the existing vSwitch properties, such as NIC speed and the number of ports, or add an additional uplink to the vSwitch.

Getting ready

Log in to the vCenter Server using the vSphere Web Client.

How to do it...

Now you will learn the steps involved in modifying the vSwitch properties.

The following steps will add an uplink to the vSwitch:

1. Select an ESXi host and click on the **Manage** tab.
2. Navigate to **Networking | Virtual Switches** and select the vSwitch to which the uplink has to be added.
3. Click on the **Manage the physical adapter connected to the selected switch** icon.

4. Click on the **+** icon to add the adapter and select the adapter to be added and **failover order group** from the drop-down menu. Then click on **OK**, as shown in the following screenshot:
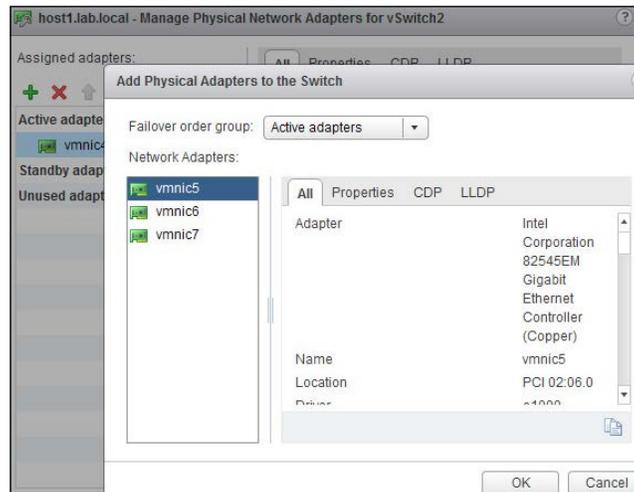
5. Click on **OK** to reconfigure the vSwitch.

You can also edit the number of ports. By default, the vSwitch is configured with 128 ports. If you want to change this number, perform the following steps:

1. Select the host and click on the **Manage** tab.

2. Navigate to **Networking** | **Virtual Switches** and select the vSwitch to which the port has to be modified.

3. Click on the **Edit Settings** icon.

4. From the drop-down menu, change the **Number of Ports**, as shown in the following screenshot, and click on **OK**:
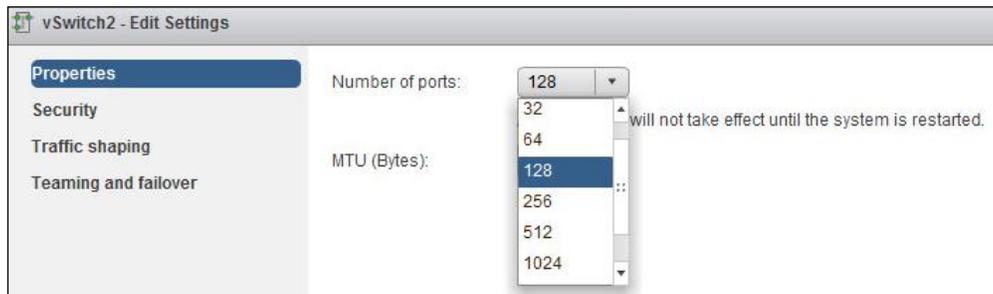
A host reboot is required for the changes to take effect.

By default, the physical NIC would be set to the **Auto negotiate** option, but sometimes you willl need to set a fixed speed and duplex to avoid any network traffic issue. Perform the following steps:

1. Select the host and click on the **Manage** tab.

2. Navigate to **Networking** | **Physical Adapters** and select the vmnic that has to be modified.

3. Click on the **Edit Adapter Speed** icon.

4. From the **Configured speed, Duplex** drop-down menu, select the appropriate speed and duplex for the vmnic, as shown in the following screenshot:
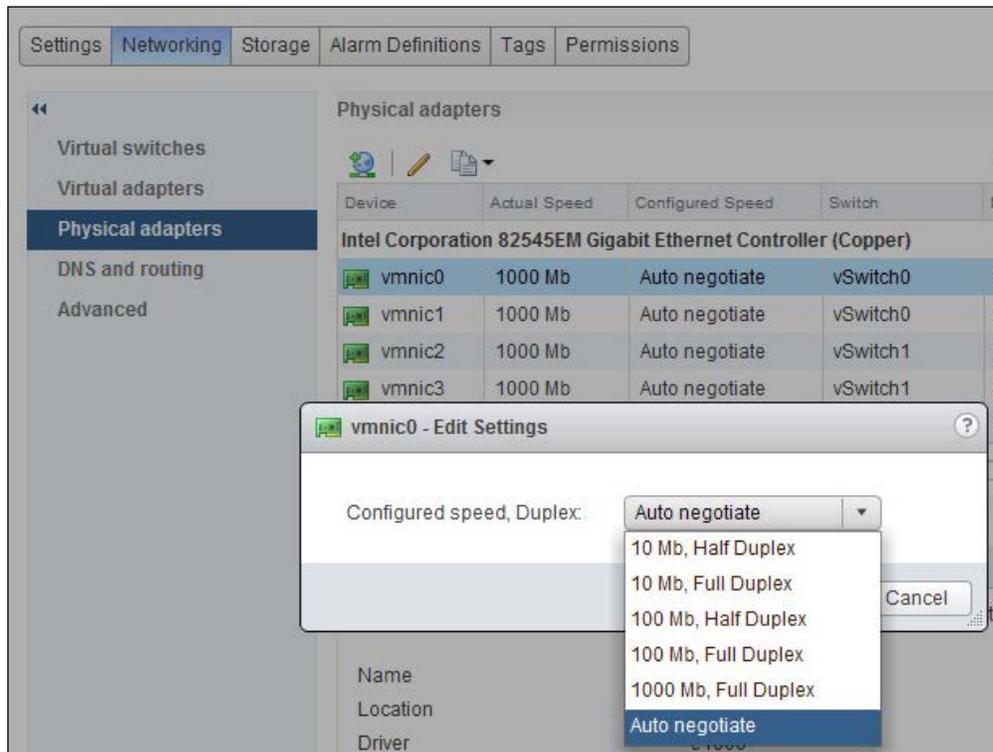
How it works...

When you add an additional uplink to the vSS, it provides a redundancy in the network in the case of a physical NIC failure. However, if you want to have redundancy in the instance of switch failure, it is recommended that you connect the uplinks to different physical switches so that you have redundancy at both the host level and the switch level.

Working with vSphere Distributed Switches

A vSphere Distributed Switch (vDS) is similar to a standard switch, but vDS spans across multiple hosts instead of creating an individual switch on each host. The vDS is created at the vCenter level, and the configuration is stored in the vCenter database. A cached copy of the vDS configuration is also stored on each host in case of a vCenter outage.

Getting ready

Log in to the vCenter Server using the vSphere Web Client.

How to do it...

In this section, you will learn how to create a vDS, dvportgroup, and manage the ESXi host using the vDS.

First, we will create a vSphere Distributed Switch. The steps involved in creating a vDS are as follows:

1. Select the datacenter on which the vDS has to be created.

2. Navigate to **Actions** | **New Distributed Switch...**., as shown in the following screenshot:
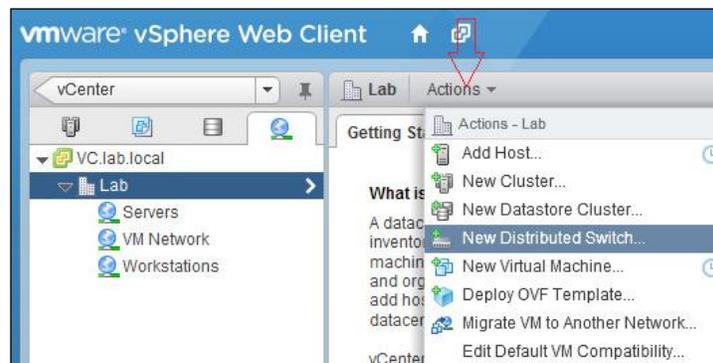
3. Enter the **Name and location** for the vDS and click on **Next**.

4. Select the version for the vDS, as shown in the following screenshot, and click on **Next**:

> If you have an older version of the ESXi host managed by vCenter, make sure you select the appropriate vDS version.

5. In the **Edit settings** page, provide the following details:

   ❑ **Number of uplinks**: This specifies the number of physical NIC of the host which would be part of the vDS.

   ❑ **Network I/O Control**: This option controls the input/output to the network and can be set to either **Enabled** or **Disabled**.

   ❑ **Default port group**: This option lets you create a default port group. To create one, enable the checkbox and provide the **Port group name**.

   ❑ Click on **Next** when finished.

6. In the **Ready to complete** screen, review the settings and click on **Finish**.

The following steps will create a new distributed port group:

1. The next step after creating a vDS is to create a new port group if it is not been created as part of the vDS. Select the vDS and click on **Actions** | **New Distributed Port Group**.

2. Provide the **name** and select the **location** for the port group and click on **Next**.

3. In the **Configure settings** screen, set the following general properties for the port group:

   ❑ **Port binding**: This provides us with three options, namely, **Static**, **Dynamic**, and **Ephemeral** (no binding).

      Static binding: This is selected when a VM is connected to the port group where a port is assigned and reserved for the VM. Only when the VM is deleted, the port is freed up.

      Ephemeral binding: This port is created and assigned to the VM by the host when a VM is powered on and the port is deleted when the VM is powered off.

      Dynamic binding: This is depreciated in ESXi 5.x version and is no longer in use, but the option is still available in the vSphere Client.

   ❑ **Port allocation**: This can be set to either **Elastic** or **Fixed**.

      Elastic: The default port is 8, and when all ports are used, a new set of ports is created automatically

      Fixed: The ports are fixed to 8, and no additional ports are created when all ports are used up

   ❑ **Number of ports**: This option is set to 8 by default.

   ❑ **Network resource pool**: This option is enabled only if a user-defined network pool is created; it can be set even after creating the port group.

   ❑ **VLAN type**: The available options are **None**, **VLAN**, **VLAN trunking**, and **Private VLAN**.

      None: This means that no VLAN is used

      VLAN: This implies that VLAN is used and the ID has to be specified

      VLAN trunking: This implies that a group of VLANs is being trunked and their respective ID have to be used

Private VLAN: This menu is empty if a private VLAN does not exist; you will learn more about Private VLAN later in this chapter


Select the **Customize default policies configuration** checkbox if you wish to configure the security, load balancing policy, and so on as part of the port group creation.

4. In the **Ready to complete** screen, review the settings and click on **Finish**.

The next step after creating a distributed port group is to add the ESXi host to the vDS. While the host is being added, it is possible to migrate the VMkernel and VM port group from the vSS to vDS, or it can be done later. Now, let's see the steps involved:

1. Select the Distributed Switch in the vSphere Web Client.

2. Navigate to **Actions** | **Add and Manage Hosts**.

3. In the **Select task** screen, select **Add hosts**, as shown in the following screenshot, and click on **Next**:
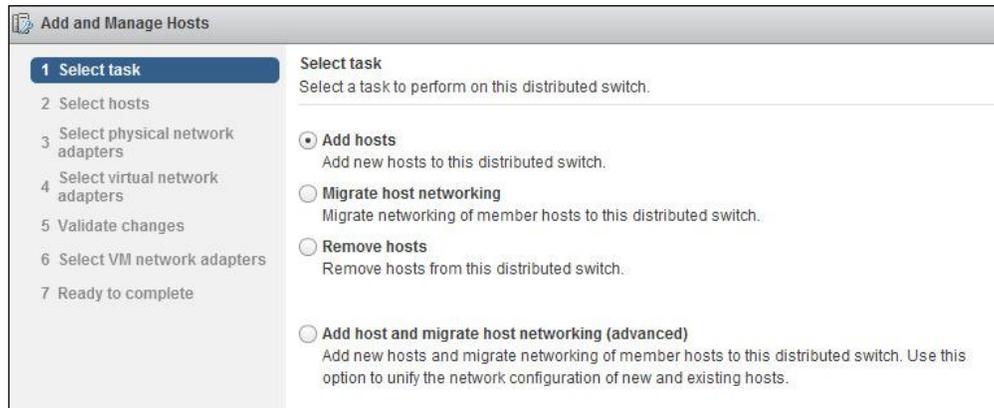
4. Click on the **+** icon to select hosts to be added and click on **OK**.

5. Click on **Next** in the **Select new hosts** screen.

6. Select the physical network adapters, which will be used as an uplink for the vDS, and click on **Next**.

7. In the **Select virtual network adapters** screen, you will have the option to migrate the VMkernel interface to the vDS group; select the appropriate option and click on **Next**.

8. Review any dependencies on the validation page and click on **Next**.

9. Optionally, you can migrate the VM Network to the vDS port group in the **Select VM network adapters** screen by selecting the appropriate option and clicking on **Next**.

10. In the **Ready to complete** screen, review the settings and click on **Finish**.

An ESXi host can be removed from the vDS only if there is no VM still connected to the vDS. Make sure the VMs are either migrated to the standard switch or to another vDS. The following steps will remove an ESXi host from the Distributed Switch:

1. Browse to the Distributed Switch in the vSphere Web Client.

2. Navigate to **Actions** | **Add and Manage Hosts**.

3. In the **Select task** screen, select **Remove hosts**, as shown in the following screenshot, and click on **Next**:
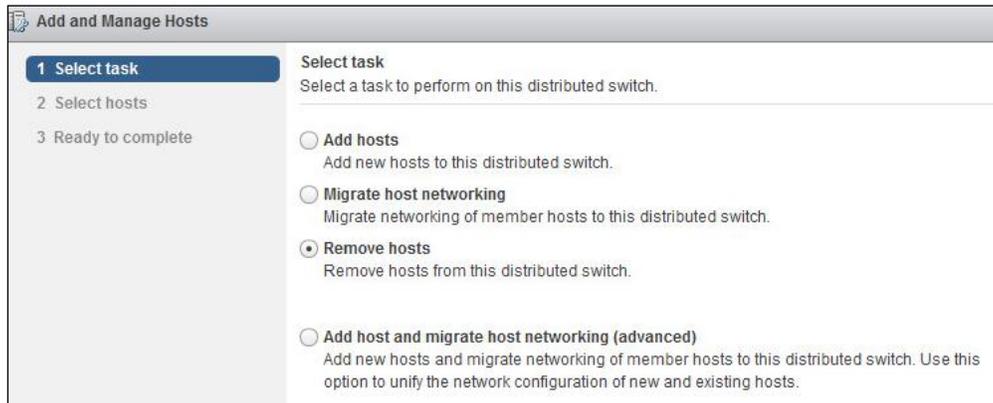
4. Click on the **+** icon to select new hosts to be removed and click on **OK**.

5. Click on **Next** in the **Select hosts** screen.

6. In the **Ready to complete** screen, review the settings and click on **Finish**.

When the entire host is being added to the vDS, you can start to migrate the resources from vSS to vDS. The following steps will help you migrate from a Standard to a Distributed Switch:

1. Select the Distributed Switch in the vSphere Web Client.

2. Navigate to **Actions | Migrate VM to Another Network**.

3. In the **Select source and destination networks** screen, you have the option to browse to a specific network or no network for source network migration. These options are described as follows:

   ❑ **Specific network**: This option allows you to select the VMs residing on a particular port group

   ❑ **No network**: This option implies that VMs that are not connected to any network will be selected for migration

4. In the **Destination network** option, browse and select the distributed port group for the VM network and click on **Next**.

5. Select the VM to migrate and click on **Next**.

6. In the **Ready to complete** screen, review the settings and click on **Finish**.

How it works...

vSphere Distributed Switches extend the capabilities of virtual networking. vDS can be broken into the following two logical sections; one is the data plane and the other is management plane:

- ▸ Data plane: This is also called the I/O plane and it takes cares of the actual packet switching, filtering, tagging, and all networking-related activities.
- ▸ Management plane: This is also known as the control plane. It is a centralized control to manage and configure the data plane functionality.

There's more...

It is possible to preserve the vSphere Distributed Switch configuration information to a file. You can use these configurations for other deployments and also as a backup. You can restore the port group configuration in case of any misconfiguration.

The following steps will export the vSphere Distributed Switch configuration:

1. Select the vSphere Distributed Switch from the vSphere Web Client.
2. Navigate to **Actions** | **All vCenter Actions** | **Export Configurations**.
3. In **Configuration to export**, you will have the following two options. Select the appropriate one.
   - ❑ **Distributed Switch and all port groups**
   - ❑ **Distributed Switch only**
4. Click on **OK**.
5. Exporting would begin, and once done, it would ask for saving the configuration. Click on **Yes** and provide the path to store the file.

The import configuration function can be used to create a copy of the exported vDS from the existing configuration file. The following steps will import the vSphere Distributed Switch configuration file:

1. Select the Distributed Switch from the vSphere Web Client.
2. Navigate to **Actions** | **All vCenter Actions** | **Import distributed port group**.
3. In the **Import Port Group Configuration** option, browse to the backup file and click on **Next**.
4. Review the import settings and click on **Finish**.

The following steps will restore the vSphere distributed port group configuration:

1. Select the distributed port group from the vSphere Web Client.

2. Navigate to **Actions** | **All vCenter Actions** | **Restore Configuration**.

3. Select one of the following options and click on **OK**:

   ❏ **Restore to a previous configuration**: This allows you to restore the configuration of the port group to your previous snapshot

   ❏ **Restore configuration from a file**: This allows you to restore to the configuration from the file saved on your local system

4. In the **Ready to complete** screen, review the settings and click on **Finish**.

> The export and import options can be automated using PowerCLI, and a scheduled task can be created to backup data on a daily or weekly basis.

Configuring Private VLANs (PVLAN)

A Private VLAN (PVLAN) is an extension of the standard VLAN and it provides further segmentation of the broadcast domain by creating private groups. The private VLAN concept is available in all the latest physical switches and also in vDS.

Getting ready

Log in to the vCenter Server using the vSphere Web Client.

How to do it...

In this section, you will learn how to create a PVLAN using the following steps:

1. Browse to the vDS in the vSphere Web Client.

2. Select the **Manage** tab and click on **Private VLAN** under **Settings**.

3. Click on **Edit** and click on **Add** in the **Edit Private VLAN settings** pop-up screen.

4. Enter the primary VLAN ID.

5. In the **Secondary VLAN ID** section, click on **Add**, enter the VLAN ID, and select the VLAN type as **Community** or **Isolated** from the drop-down menu.

6. Click on **OK**.

Once created, the **Private LAN** section should look similar to the following screenshot:

How it works...

The PVLAN is further divided into two different types:

- **Primary PVLAN**: This is the native VLAN, which is further segmented into a different VLAN.

- **Secondary PVLAN**: This exists only under PVLAN, and there are three VLAN types available under the Secondary PVLAN. They are as follows:

  - **Promiscuous**: A device attached to the promiscuous PVLAN can send and receive packets to any other device attached to the same Primary VLAN.

  - **Community**: A device attached to the community PVLAN can send and receive packets which are in the same Secondary PVLAN and to the device in the promiscuous PVLAN.

  - **Isolated**: A device attached to the community PVLAN can send and receive packets only to the device in Promiscuous PVLAN.

Working with advanced networking

The vSphere advanced networking provides a good control over the vSphere environment. Now let's see some of the things that can be done in vSphere.

Getting ready

Connect to the vCenter Server using the vSphere Web Client.

How do to it...

In this section, you will learn some of the advanced configurations, which are applicable only for the vDS.

Network rollback

In vSphere 5.1, you get an option to rollback networking to a previous state if there is any misconfiguration done on the host or vDS level, which could cause the host to get disconnected from the vCenter. Roll back is available for both Standard and Distributed Switches:

1. Click on **Actions** | **All vCenter Actions** | **Restore Configuration**.

2. If the distributed port group or the uplink is to be restored from the vSphere Web Client, select one of the following options and click on **Next**.

   - ❑ **Restore to a previous configuration**
   - ❑ **Restore configuration from a file**

3. If the distributed switch configuration is restored, select one of the following options and click on **Next**.

   - ❑ **Restore distributed switch and all port groups**
   - ❑ **Restore distributed switch only**

4. In the **Ready to complete** screen, review the settings and click on **Finish**.

Network recovery

Recovery is performed directly on the host using DCUI when the host is disconnected from vCenter. When a recovery is performed, a local port is created by the DCUI and the connectivity to vCenter is restored. The following steps will perform a network recovery:

1. Log in to the DCUI of the ESXi host.

2. Select **Network Restore Options** under **System Customization**.

3. Select either **Restore Network Settings**, **Restore Standard Switch**, or **Restore vDS**.

4. Provide the VLAN ID and uplink to be used as required.

Working with NetFlow

NetFlow is a mechanism to identify the way the traffic flows. It is used to export the network flow of the application, such as source, destination, protocol, and volume of network traffic, to the collector device for analysis. It helps to ensure that we have the correct I/O resource for the application. NetFlow can be enabled at the individual port, port group, or at the uplink level as follows:

1. Select the vDS in the vSphere Web Client.

2. Click on the **Manage** tab and select **NetFlow** under **Settings**.

3. Click on **Edit** and configure the following parameters, which are then shown in the following screenshot:

- ❑ **IP address**: Specify the IP address of the collector appliance.
- ❑ **Port**: Specify the port number used by the collector.
- ❑ **Switch IP address**: If you want to use a single source for all the vDS traffic, then specify the vDS IP address, otherwise each individual ESXi host management address would be shown as a source in NetFlow.
- ❑ **Active flow export timeout**: By default, the VDS would send the active network flow to the collector device after 60 seconds.
- ❑ **Idle flow export timeout**: By default, after 15 seconds of initial packets have passed, the VDS will export the data.
- ❑ **Sampling rate**: Specifies the frequency at which the data has to be captured. If the rate is set to 5, every fifth packet would be captured.
- ❑ **Process internal flows only**: By default this option is disabled. If it is enabled, only the network activity of the VMs on the same host is collected.

4. Click on **OK** when finished.

Switch discovery protocol

With the help of switch discovery protocol, you can identify to which physical ports the uplink is connected, and it also identifies some of the physical switch properties such as device ID, software version, and so on. Two types of protocols are supported by vSphere. They are as follows:

▸ **Cisco Discovery Protocol** (**CDP**): This is available on both vSS and vDS

▸ **Link Layer Discovery Protocol** (**LLDP**): This is available only on vDS

The following steps will enable the switch discovery protocol:

1. Browse the vDS in the vSphere Web Client.

2. Select the **Manage** tab, click on **Properties** under **Settings**, and then click on **Edit**.

3. Click on the **Advanced** section under **Discovery protocol** and perform the following steps:

    1. Select either **Cisco Discovery Protocol** or **Link Layer Discovery Protocol** from the **Type** drop down, as shown in the following screenshot:

    2. Select **Listen**, **Advertise**, or **Both** from the **Operation** drop down. Let's look at each of these options:

        Listen: This implies that the host will display information about the switch port, but the vDS information is not available to the network administrator

        Advertise: This implies that the vDS information is available to the network administrator, but the Cisco switch port details are not available to the host

        Both: The host will detect and display information about the Cisco switch port and vDS information will be available to the network administrator

4. Click on **OK** when done.

How it works...

The switch discovery comes very handy when you need to get details about the physical switch to which the host is connected for any troubleshooting purpose without engaging your network team.

Enabling jumbo frames

If you are using an IP-based storage and if you want to increase the performance of the storage network, then jumbo frames have to be enabled for the iSCSI or the NFS port group.

Getting ready

The physical switch ports carrying the traffic are set to the MTU size of 9000.

How to do it...

In this section, you will learn how to change the MTU size in both vSS and vDS.

The following steps will enable jumbo frames on vSS:

1. Navigate to **Host** | **Manage tab** | **Networking** | **Virtual Switches**.
2. Select the vSwitch and click on the **Edit** icon.
3. In the pop-up screen, change the MTU (bytes) value to 9000 and click on **OK**.

The following steps will enable jumbo frames on vDS:

1. Browse vDS in the vSphere Web Client.
2. Click on the **Manage** tab and select **Properties** under **Settings**.
3. Click on **Edit**.
4. Go to the **Advanced** section, change the MTU (bytes) value to 9000, and click on **OK**.

How it works...

The Ethernet frame carried in the network is 1500 MTU, but in some cases, you may need to increase the maximum frame size, especially when iSCSI- or NFS-based storage is used. By enabling jumbo frame, the frame size can be increased up to 9000 MTU. Jumbo frames have to be enabled end to end in the network, so make sure the physical devices support jumbo frames traffic.

There's more...

Alternatively, an ESXCLI command can be used to set the MTU size on the switch. The following command can be used to set the MTU size to 9000 on vSwitch1:

```
esxcli network vswitch standard set -m 9000 -v vSwitch1
```

Configuring network policies

VMware provides a set of networking policies, which can be applied at the distributed port group or at the vDS level.

Getting ready

Connect to the vCenter using the vSphere Web Client.

How to do it...

Let's see some of the policies that are applicable only for the vDS.

Port blocking policy

This policy allows blocking the ports from receiving and sending data. The policy can be applied to an individual port, port group, or to a particular uplink using the following steps:

1. Select a vDS in the vSphere Web Client.

2. Click on the **Manage** tab and then on **Ports**.

3. Select the port that has to be blocked and click on **Edit distributed port settings**.

4. Select **Miscellaneous** and mark the **Override** check box in the **Block port** option, which are shown in the following screenshot. Select **Yes** from the drop-down menu as shown in the following screenshot:
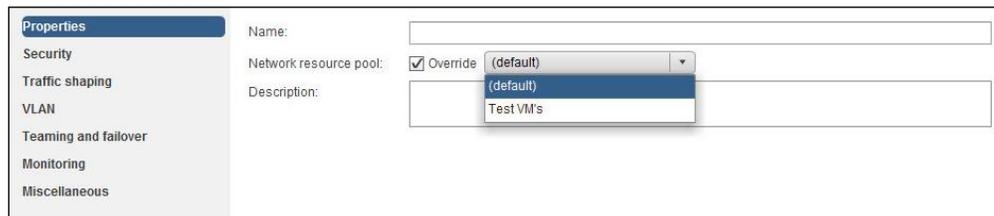

5. Click on **OK** when done.

Alternatively, if you want to block the entire port group, perform the following steps:

1. Select the vDS in the vSphere Web Client.

2. Right-click on the vDS and select **Manage Distributed Port Groups**.

3. Select the **Miscellaneous** checkbox and click on **Next**.

4. Select the vDS port groups and click on **Next**.

5. In the **Miscellaneous** section, select **Yes** from the **Block all ports** drop-down menu and click on **Next**.

6. In the **Ready to complete** screen, click on **Finish**.
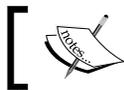
> This will shut down the ports that are part of this port group, so please be cautious.

Monitoring policy

NetFlow can be enabled or disabled on the port with the help of monitoring policy as follows:

1. Select the vDS in the vSphereWeb Client.

2. Navigate to **Manage | Ports**.

3. Select the port that has to be monitored and click on **Edit distributed port settings**.

4. Select **Monitoring** and then select the **Override** check box. Select **Enabled** from the drop-down menu.

5. Click on **OK** when done.

Alternatively, if you want to enable NetFlow for the entire port group, perform the following steps:

1. Select the vDS in the vSphere Web Client.

2. Right-click on the vDS and select **Manage Distributed Port Groups**.

3. Select the **Monitoring** checkbox and click on **Next**.

4. Select the DV port groups and click on **Next**.

5. In the **Monitoring** section, select **Enabled** from the drop-down menu and click on **Next**.

6. In the **Ready to complete** screen, click on **Finish**.

Resource allocation policy

The resource allocation policy allows you to associate a distributed port or port group with a user-created network resource pool. This policy provides you with greater control over the bandwidth given to the port or port group. This can be applied to a distributed port group level or port level. Network I/O control should be enabled on the host, and user-defined network resource pools should be created on the distributed switch to apply the resource allocation policy at the distributed port group level or port level. This can be done as follows:

1. Select the vDS in the vSphere Web Client.

2. Navigate to **Manage | Ports**.

3. Select the port from the list and click on **Edit distributed port settings**.

4. Select **Properties** and enable the **Override** check box. Select the user-defined network pool as shown in the following screenshot:

5. Click on **OK** when done.

Alternatively, if you want to enable resource allocation for the entire port group, perform the following steps:

1. Select the VDS in the vSphere Web Client.

2. Right-click on VDS and select **Manage Distributed Port Groups**.

3. Select the **Resource Allocation** checkbox and click on **Next**.

4. Select the DV port groups and click on **Next**.

5. In the **Resource Allocation** section, select the user-defined network resource pool from the drop-down menu and click on **Next**.

6. In the **Ready to complete** screen, click on **Finish**.

How it works...

The vSphere networking policies are almost similar to the policies available in the physical switches. Enabling the policy on the vSphere level provides an additional layer of security to the virtual environment. The policies can be enabled at the virtual switch level or the individual port group level. It is possible to override the policy at the port group level if virtual switch level policies are applied.

There's more...

In the previous section, you learned about the policy that was applicable only for the Distributed Switch. Now, let's see the policies that are common for both the Standard and Distributed Switches.

Security policy

It's a layer 2 security policy, and it determines how the inbound and outbound frames have to be filtered. The policy can be set at the virtual switch level or the port group level, and in case of vDS, it can be set only at the distributed port group level. So, we have three types of security policies in vSphere:

▶ **Promiscuous mode**: It is set to reject by default, so the virtual adapter receives the frames that are applicable only for them. If it's set to accept, the virtual adapter will detect all the frames passed through the switch.

▶ **MAC address changes**: When a VM is created, it has been assigned with a MAC address, which is written to the configuration (VMX) file. For any reason, if the guest OS MAC address changes, all the inbound traffic to the VM would be dropped if the option is set to **Reject**, by default it is set to **Accept**.

▶ **Forged transmits**:The only difference to this policy and the MAC address changes policy is that the outbound traffic from the VM to the vSwitch would be dropped if it is set to **Reject**. By default, this option is also set to **Accept**.

Load balancing and failover policy

Using this policy, you can set how the load has to be distributed across the uplinks, and you can set to re-route the network traffic in case of an uplink failure. You can perform the following configurations in this policy:

▶ Load balancing
▶ Network failure detection
▶ Notify switches
▶ Failback
▶ Failover order

Load balancing

This policy determines how the load is balanced between the NIC teams. We have four of the following policies available, and only one of them can be configured at a time:

▸ **Route based on the originating virtual port**: This is the default policy. It pins each virtual port to a specific uplink and ensures that the VM traffic is flowing through the same physical adapter. This policy doesn't provide any load balancing, and in the event of an uplink failure, the traffic is routed through the other uplink associated with the vSwitch.

▸ **Route based on IP hash**: This policy assigns an uplink for communication based on the source and destination IP addresses. A VM can use a different uplink when communicating with a different destination IP address. It is necessary to have EtherChannel configured on the physical switch if this policy is used.

▸ **Route based on source MAC hash**: This policy assigns an uplink based on the source MAC address. The policy can be best used when a VM has multiple virtual adapters so that for multiple source MAC addresses, different uplinks are used.

▸ **Use explicit failover order**: This policy doesn't provide any load balancing rather it just specifies the order in which NIC has to be failed over incase an active NIC has failed. The policy works in conjunction with **Failover order**.

▸ **Route based on physical NIC load**: This policy is available only on vDS and the ESXi chooses the uplink based on the current utilization of the physical adapter. If there is more than 75 percent utilization for around 30 seconds, ESXi will re-assign a different uplink for the VM traffic.

Network failure detection

This policy determines how the network failure has to be determined, and there are two methods available for the same. They are as follows:

- ▸ **Link status only**: This policy identifies if there is a failure in the link status, such as a cable pull, physical switch failure, and so on. However, it does not detect any configuration error beyond the directly connected switch.

- ▸ **Beacon probing**: This policy sends out Beacon probes to all the uplinks in the team to identify an NIC failure or switch misconfiguration and a minimum of three NIC's should be in team if beacon probing is enabled.

> Do not use Beacon probing if IP-hash load balancing is used as you may notice a network flapping error, and the ESXi hosts will lose their connection to the vCenter.

Notify switches

You have an option to set this configuration to **Yes** or **No** from the drop-down menu. This policy would send a notification to the physical switch to update the MAC address table on the physical switch in case of a failure in the NIC team.

> Notify switches has to be set to **No** if you are using Microsoft **Network Load Balancing** (**NLB**) in a unicast mode.

Failback

You have an option to set this configuration to **Yes** or **No** from the drop-down menu. This policy specifies if the adapter has to be returned to the active state after its recovery from failure.

Failover order

Here, you specify how to balance the load across different adapters. You can place the adapters in standby, so they can be used if the active adapter has failed.

4
Storage

In this chapter, we will cover the following topics:

- ▸ Implementing the iSCSI storage
- ▸ Implementing FC and FCoE storages
- ▸ Configuring Raw Device Mapping
- ▸ Managing VMFS and NFS datastores
- ▸ Configuring the storage profiles of a virtual machine

Introduction

Storage is one of the key components of a virtual environment. ESXi supports two types of storage, including local storage and network storage, such as **Fibre Channel** (**FC**), **Fibre Channel over Ethernet** (**FCoE**), **Internet SCSI** (**iSCSI**), and **Network File System** (**NFS**). The external shared storage is used to store virtual machine files remotely. These datastores are concurrently shared across multiple hosts. The ESXi host formats its attached storage with the **Virtual Machine File System** (**VMFS**) format. Virtual machines are made up of a set of files and virtual disks, which are stored in the VMFS datastores. The ESXi hypervisor logically abstracts the physical storage layer and provides storage to Virtual Machines. A virtual machine uses virtual SCSI controllers to access the attached virtual disks. The two types of storage that ESXi supports are as follows:

- ▸ **Local storage**: This can store the virtual machine files, templates and ISO files on directly connected storage disks. These disks are directly connected to the ESXi host using protocols such as SAS or SATA. This local storage cannot be shared among multiple hosts. The ESXi host that owns the hard disk holds the single connection to the storage disk.

▶ **Network storage**: This provides shared storage, which is one of the important requirements for the vSphere environment. A lot of vSphere features, such as **High Availability** (**HA**), **Distributed Resource Schedule** (**DRS**), **vMotion**, and **Fault Tolerance** depend on the shared storage. vSphere supports different types of shared storages such as Fibre Channel, iSCSI, and the Network file system.

VMware vSphere 5.1 was released with a lot of new storage capabilities to enhance the features released with vSphere 5.0. The new storage features of vSphere allow integration with the VMware products such as **VMware vCloud Director** and **VMware View**. The vSphere 5.1 storage enhancement brings improved scalability and performance capabilities to the virtual environment, some of them are as follows:

▶ **VMware vSphere VMFS-5 File Sharing Enhancements**: This feature, which was introduced with the release of vSphere 5.1, increases the maximum number of hosts that can share a read-only file on a VMFS datastore from 8 to 32. This allows more flexibility for VMware View and VMware vCloud Director by allowing the the linked clone deployed from the base image to be hosted on any one of the 32 hosts sharing the same datastore. Linked clones can be used for the fast provisioning of vCloud Director vApps.

▶ **Space-Efficient Sparse Virtual Disks**: This is a new type of virtual disk introduced in vSphere 5.1. The main feature of this disk is to reclaim the previously used and unused spaces within the guest operating systems. It also has the ability to set up a virtual machine disk block allocation size based on the application's requirement. As of vSphere 5.1, SE sparse disk type can only be used with VMware View.

▶ **All Paths Down** (**APD**) **condition–handling enhancements**: This is another feature that was added in vSphere 5.1, where a lot of enhancements were made to handle APD and **Permanent Device Loss** (**PDL**). APD can occur when a storage device is removed in an uncontrolled manner or when a device fails. This enhancement will not allow hostd to hang when the storage devices are removed in an uncontrolled manner. This is also enhanced with HA, to detect the PDL situation, and to restart the Virtual Machines on other hosts which might not have this PDL situation on the datastore. In addition to this, the ESXi host can determine the difference between Permanent Device Loss and temporary device unavailability for iSCSI arrays.

▶ **Storage protocol supportability improvements**: With vSphere 5.1, the ESXi host can be installed and booted from a FCoE LUN using a software FCoE initiator. In vSphere 5.0, it requires a dedicated FCoE hardware adapter to install and boot the ESXi server from a FCoE LUN. Jumbo frames are now supported for all types of iSCSI adapters, including software iSCSI adapters and dependent and independent hardware iSCSI adapters.

▶ **VMware vSphere Storage APIs – Array Integration** (**VAAI**): vSPhere 5.1 introduces enhancements to VAAI NAS to enable array-based snapshots to be used for vCloud Director Fast-Provisioned vApps.VAAI is the vSphere storage API for array integration. It enables us to off-load certain storage operations from the ESXi host to the storage array.

▶ **Solid State Disk (SSD) monitoring**: It is very important to monitor the Solid State Drive (SSD) from the ESXi host. The ESXi 5.1 host has a smartd daemon which is a SSD **Self-Monitoring Analysis and Reporting Technology** (**SMART**). It runs every 30 minutes and makes API calls to gather disk information. These events and statistics are only available via the ESXCLI command line and not from the vSphere Windows or Web Client.

▶ **VMware vSphere Storage I/O Control and DRS enhancements**: vSphere 5.1 enables interoperability between **Storage DRS** and vCloud Director. vCloud Director can detect datastore cluster objects from Storage DRS and also SDRS can detect linked clones. Storage DRS can be used with vCloud Director for initial placement, space utilization, and I/O load balancing of fast provisioned vApps.

▶ **VMware vSphere Storage vMotion enhancements**: vSphere 5.1 allows up to four parallel disk copies per Storage vMotion, while the previous versions of vSphere used to copy disks serially.

Please refer to *What's New in VMware vSphere 5.1 - Storage* at `http://www.vmware.com/ files/pdf/techpaper/Whats-New-VMware-vSphere-51-Storage-Technical- Whitepaper.pdf` to find out more about it.

Implementing the iSCSI storage

iSCSI is an IP-based storage network. iSCSI storage uses TCP/IP connections and components such as iSCSI HBA adapters or network interface cards, network switches, and routers for the storage traffic.

Getting ready

Make sure your iSCSI Storage is configured and can be accessed from the ESXi host. Connect to your VMware vCenter server using the vSphere Web Client and browse to your ESXi host; then select the ESXi host and click on the **Manage** tab.

How to do it...

We'll see the step-by-step procedure on how to configure the prerequisites for iSCSI Storage, create the iSCSI datastore, and configure advanced properties of iSCSI Storage.

The following steps will show you how to add a software iSCSI adapter:

1. Select the **Storage** tab and click on **Storage Adapters**.
2. Click on the **+** sign to add new storage adapters.
3. Select **Software iSCSI adapter** from the dropdown to select the adapter type.

4. Confirm the selection and click on **OK**.
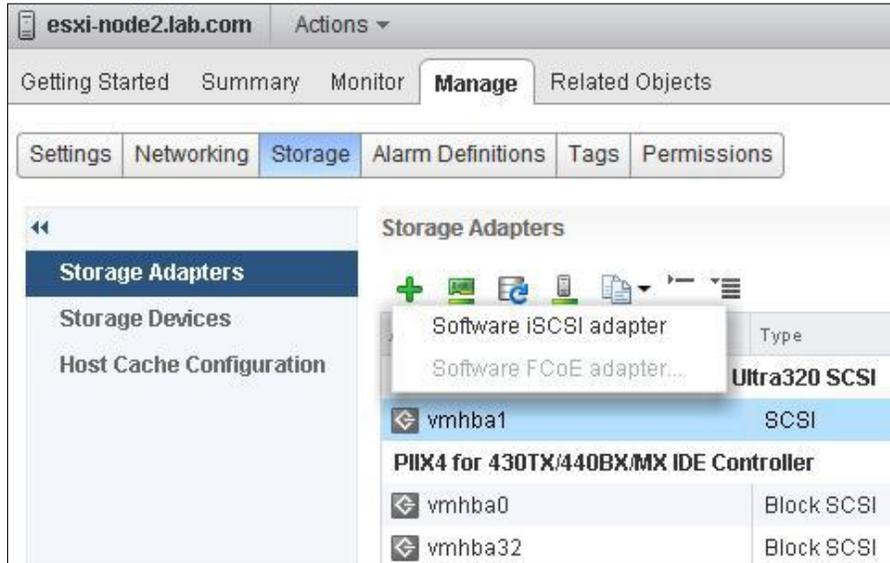
Let us now see how to add a VMkernel adapter for the iSCSI network binding by performing the following steps:

1. Select **Networking** and click on the **Add host networking** option.

2. Select **VMKernel Network Adapter** to create a connection type and then click on **Next**.

3. Select an existing standard switch in the select target device page if you want to add the port group into an existing virtual switch, as follows:

    1. Click on **Browse**.

    2. Select a standard switch from the list.

    3. Click on **OK**.

4. Select a new standard switch in the select target device page if you want to add the port group into a new virtual switch, as follows:

    1. Select **New standard switch** and click on **Next**.

    2. Select **Number of ports** from the dropdown if you want to change the default number of ports and click on **Next**.

    3. Click on the **+** symbol to add the network uplink adapter for this virtual switch.

4. Under the **Failover Order Group**, select **Active adapter** to add the first uplink adapter for this virtual switch.

5. Select the **Network Adapter** from the list and click on **OK**.

6. Repeat the same steps if you want to add multiple network adapters for this virtual switch and then click on **Next**.

5. Provide the network label for this VMKernel port group.

6. Select or enter the **VLAN ID** if you have configured any.

7. In the IPv4 settings page, select the method of IP assignment for this VMkernel interface either via **DHCP** or **Static IP** settings. Specify the following information if you chose the Static IP option:

1. Enter the IP address for the VMkernel interface.

2. Enter the subnet mask for the VMkernel interface.

3. The gateway address will be taken based on the information provided during the installation. Edit the values if you want to change the default gateway address.

4. The DNS server information is taken from the information provided during the ESXi installation. Then click on **Next**.

8. Review your settings and click on **Finish** to create the VMkernel interface.

You can configure the **Teaming and Failover** order for iSCSI Storage binding by performing the following steps:

1. Select **Networking**.

2. Click on the virtual switch where your VMkernel adapter exists and click on the virtual switch diagram.

3. Select the **VMKernel adapter** and click on **Edit settings**.

4. Click on **Teaming and failover** and select the **Override** checkbox under **Failover order**.

5. Select only one adapter under **Active adapters** and move all the other physical adapters under **Unused adapters**. The VMkernel adapter should have only one active adapter and no standby uplink to be eligible for iSCSI HBA binding.
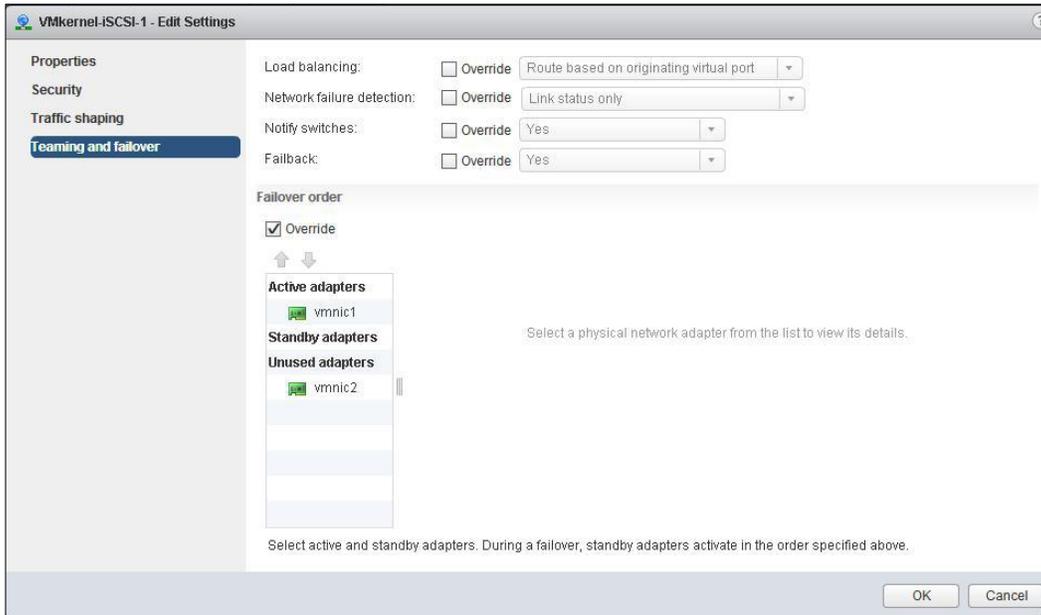
6. Repeat the steps 3 to 7 for each VMkernel adapter to be bound with iSCSI HBA.
7. Click on **OK**.

You can bind the iSCSI storage adapter with the VMKernel adapter by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.
2. Select the **Storage** tab and click on **Storage adapters**.
3. Select the software iSCSI adapter and click on the **Network port binding** tab under the **Adapter details** section.

4. Click on the **+** sign and select a VMkernel adapter to bind with this iSCSI adapter. You can bind one or more VMkernel adapters with the software iSCSI adapter.
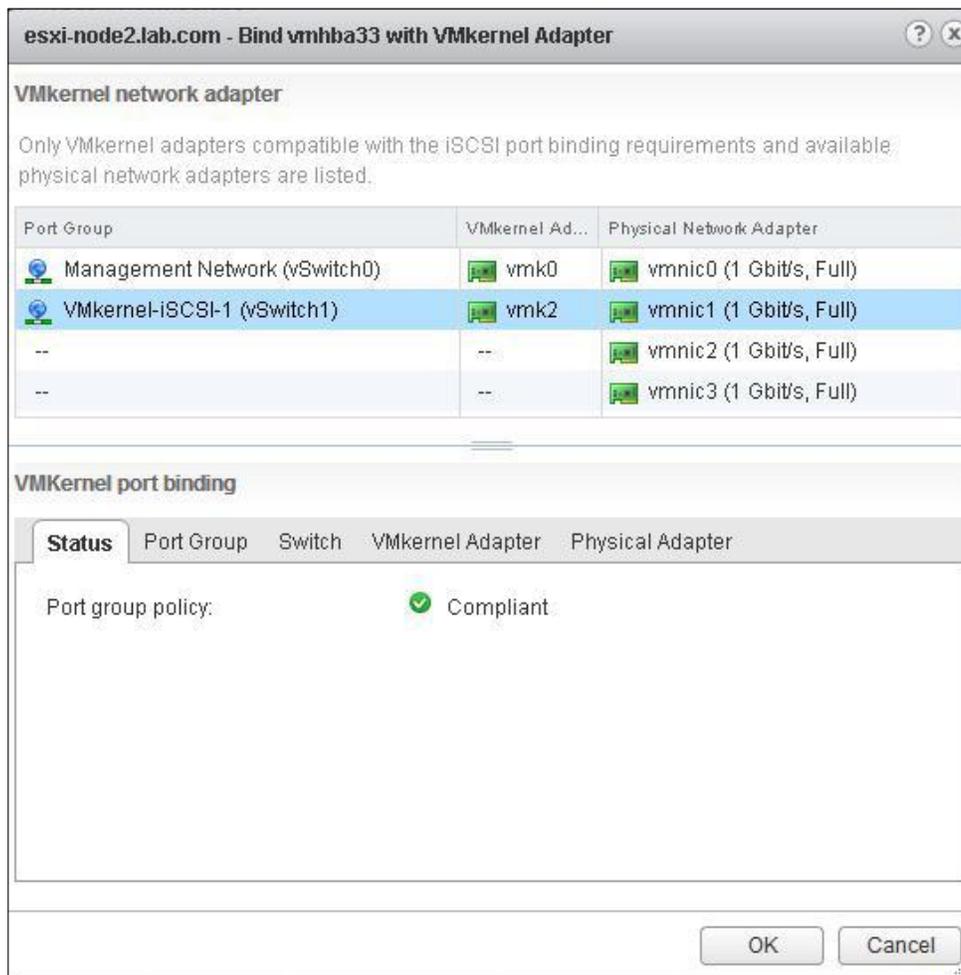
5. Click on **OK**. It will recommend that you perform a **Rescan of the iSCSI storage adapter** for the configuration changes to apply.

You can view the port binding details by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.

2. Select the **Storage** tab and click on **Storage adapters**.

3. Select the **Software iSCSI adapter** and click on the **Network port binding** tab under the **Adapter details** section.

4. Click on **View details**.

You can configure the dynamic iSCSI discovery by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.
2. Select the **Storage** tab and click on **Storage adapters**.
3. Select the **Targets** tab and click on **Dynamic discovery**.
4. Click on **Add**.
5. Enter the IP address or DNS name of the iSCSI target server and click on **OK**.
6. Rescan the storage adapter to list all the newly discovered targets.

You can configure the static iSCSI discovery by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.
2. Select the **Storage** tab and click on **Storage adapters**.
3. Select the **Targets** tab and click on **Static discovery**.
4. Click on **Add**.
5. Enter the **Target's information** and click on **OK**.
6. Rescan the iSCSI storage adapter. It will list all the devices discovered under the static target added in the **Devices** tab.

You can create a datastore from the iSCSI Storage by performing the following steps:

1. Select the ESXi host and click on **Actions**.
2. Select **All vCenter Actions** and click on **New Datastore**.
3. Enter the **Name** for the datastore.
4. Select the type as **VMFS datastore** to provision a VMFS datastore.
5. Select the device from the list of storage devices available.
6. Select the VMFS version as **VMFS 5**.
7. Choose the partition configuration as **Use all available partitions** and click on **Next**. The entire disk will be dedicated to a single VMFS datastore. All data currently stored on this device will be destroyed.
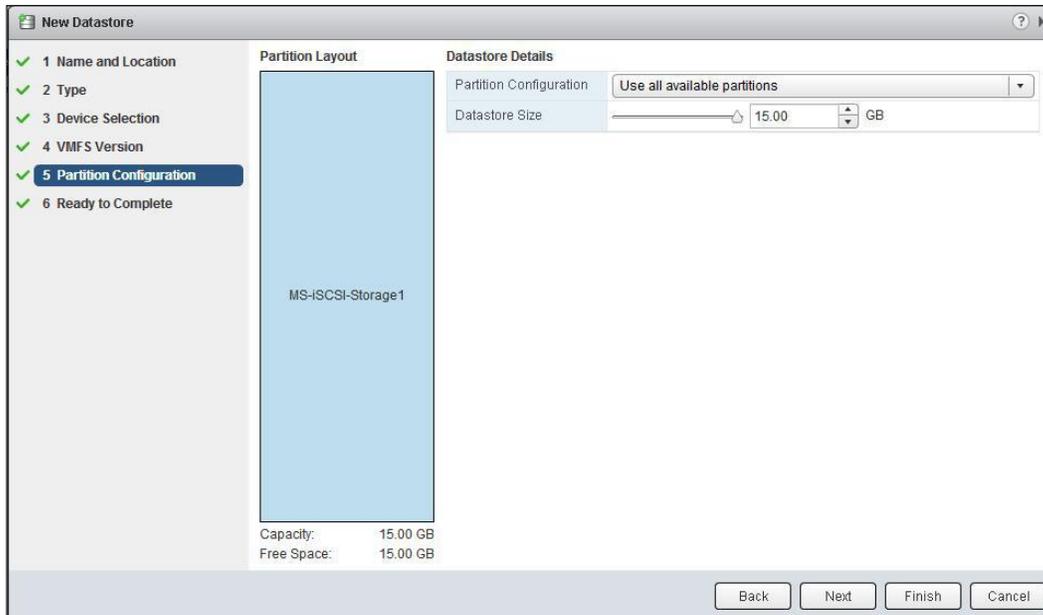
8. Review the configuration information and click on **Finish**.

How it works...

iSCSI SAN works in a client-server architecture. The iSCSI initiator works as a client, and it is attached to the ESXi host. The iSCSI initiator issues SCSI commands to the iSCSI target, which acts as a server. The iSCSI target server is a physical storage system on the network. We can utilize the multipathing technique for an iSCSI storage redundancy. Even software iSCSI adapters can be bound with one or more network adapters to utilize the multipathing technique. iSCSI uses a unique naming convention in the following format: `iqn.yyyy-mm.naming-authority:unique name`. The following is an example of the naming convention: `iqn.2000-03.com.lab.iscsi:cookbooktarget1`.

There's more...

Apart from discovering, adding, and binding network adapters to iSCSI storage, additional tasks are to secure the iSCSI storage discovery using **CHAP authentication** methods. The CHAP authentication will be only used for authentication purposes, and it will not encrypt any data. Let's take a look at how to set up the CHAP authentication and configure the advanced parameters of the iSCSI adapter and iSCSI target level.

You can set up the CHAP authentication for the iSCSI adapter by performing the following steps:

1. Connect to your vCenter server using the vSphere Web Client.
2. Browse towards your ESXi host.
3. Select the ESXi host and click on the **Manage** tab.
4. Select the **Storage** tab and click on **Storage adapter**.
5. Click on **Properties** and select **Edit** under **Authentication**.
6. Select the **Authentication Method** from the drop-down menu, which contains the following options:

   ❑ **None**: When this option is selected, the ESXi host does not use the CHAP authentication.

   ❑ **Use unidirectional CHAP if required by target**: This option implies that the ESXi host prefers a non-CHAP connection, but if it is required by target, the host can use a CHAP connection.

   ❑ **Use unidirectional CHAP unless prohibited by target**: The ESXi host prefers the CHAP connection, but if the iSCSI target does not support CHAP, the host can use non-CHAP connections.

   ❑ **Use unidirectional CHAP**: The ESXi host requires a successful CHAP authentication. If the CHAP authentication fails, it will cause connection failure.

   ❑ **Use bidirectional CHAP**: This makes both the ESXi host and the target support bidirectional CHAP.
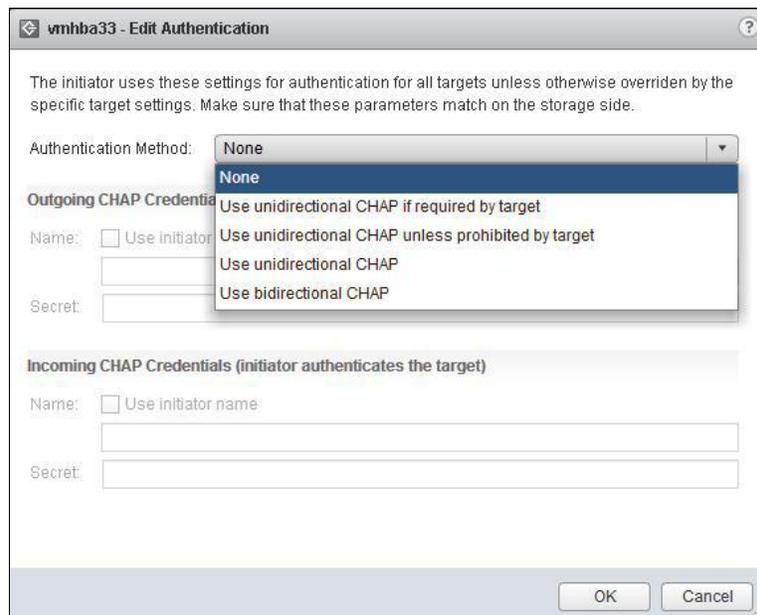
7. Configure the **Outgoing CHAP Credentials**. Select the **Use initiator name** checkbox to use the CHAP name as the iSCSI initiator name.

8. Enter the outgoing CHAP **Secret**. If you selected the **Use bidirectional CHAP** option, you have to configure both outgoing and incoming CHAP credentials.

9. Click on **OK** and rescan the iSCSI adapter.

You can configure the advanced parameters at the iSCSI adapter level by performing the following steps:

1. Connect to your vCenter server using the vSphere Web Client.

2. Browse towards your ESXi host.

3. Select the ESXi host and click on the **Manage** tab.

4. Select the **Storage** tab and click on the **Storage** adapter.

5. Select the **Advanced Options** tab and click on **Edit**.

6. Edit the advanced parameters you want to modify.

Please refer to the following link to find out more about the advanced parameters of iSCSI at `http://pubs.vmware.com/vsphere-55/index.jsp#com.vmware.vsphere.storage.doc/GUID-7FCA31F2-FA13-4BFD-8057-5A36DC3FBC14.html`.

> Do not make any changes to the advanced settings until it is recommended by VMware support.

Implementing FC and FCoE storages

Fibre Channel is a high-performance storage protocol that connects storage devices using a high-speed network to the host servers. SAN includes **Host Bus Adapters** (**HBA**) attached to the host servers, Fibre Channel switches, fabric cables and storage processors, and storage disk arrays. Fibre Channel SAN uses the FC protocol to access the shared storage.

The FCoE protocol allows access to Fibre Channel LUNs over Ethernet frames. The FCoE adapters can be used to access the Fibre Channel storage via Ethernet frames. There are two types of FCoE adapters: hardware and software FCoE adapters. ESXi allows you to access LUNs using software FCoE adapters without the need for dedicated FCoE adapters or HBAs if you have a network adapter which supports partial FCoE offload.

Getting ready

Connect to your VMware vCenter server using the vSphere Web Client and make sure your Fibre Channel storage is configured from the storage end and can be accessed from your ESXi servers. Browse towards your ESXi host in the vSphere Web Client to perform the following actions.

How to do it...

We'll see how to add Fibre Channel storage and configure FCoE adapters and network adapters to use with the FCoE adapter.

You can create the Fibre Channel datastore by performing the following steps:

1. Rescan your HBA adapters to detect all the configured Fibre Channel storage to your ESXi host.

2. Select the ESXi host and click on **Actions**.

3. Select **All vCenter Actions** and click on **New Datastore**.

4. Enter the **Name** for the datastore.

5. Select the type as **VMFS datastore** to provision a VMFS datastore.

6. Select the **Device** from the list of Fibre Channel storage devices available.

7. Select the VMFS version as **VMFS 5**.

8. Choose the partition configuration as **Use all available partitions** and click on **Next**. The entire disk will be dedicated to a single VMFS datastore. All the data currently stored on this device will be destroyed.

9. Review the configuration information and click on **Finish**.

You can configure the VMkernel adapter for the FCoE adapter by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.

2. Select **Networking** and click on the **Add networking** option.

3. Selecting **VMKernel Network Adapter** to create a connection type and click on **Next**.

4. You can create a new standard switch in the select target device page by performing the following steps:

    1. Select the **New standard switch** option and click on **Next**.

    2. Select the **Number of ports** from the dropdown if you want to change the default number of ports and click on **Next**.

    3. Click on the **+** symbol to add the network uplink adapter that supports FCoE.

    4. Under the **Failover Order Group**, select **Active adapter** to add the first uplink adapter for this virtual switch.

5. Select the network adapter that supports FCoE from the list and click on **OK**.

6. Provide the network label for this VMKernel port group

7. Select or enter the **VLAN ID**. It is always recommended to configure the FCoE traffic in an isolated network.

8. In the IPv4 settings page, select the method of IP assignment for this VMkernel interface either via DHCP or static IP settings. Enter the following details if you chose the static IP settings:

    1. Enter the IP address for the VMkernel interface.

    2. Enter the subnet mask for the VMkernel interface.

    3. The gateway address will be set automatically based on the information provided during the installation. Edit the values if you want to change the gateway address.

    4. The DNS server information is taken from the information provided during the ESXi installation.

9. Review your settings and click on **Finish** to create the VMkernel interface.

You can add the software FCoE adapter by performing the following steps:

1. Select the ESXi host and click on the **Manage** tab.

2. Select the **Storage** tab and click on **Storage adapters**.

3. Click on the **+** sign to add a new storage adapter.

4. Select the **Software FCoE** adapter in the option to select the adapter type.

5. Confirm the selection and click on **OK**.

6. Rescan the adapter to detect the storage devices in the FCoE adapter and create a datastore, which is similar to creating a datastore from the Fibre Channel storage device.

There's more...

NPIV (**N_PortID Virtualization**) is a Fibre Channel feature. NPIV enables you to have multiple unique N_port IDs per physical HBA. With the use of NPIV, each VM can have a unique Fibre Channel **WWN** (**World Wide Number**) to share a single physical HBA among Virtual Machines. It allows a SAN administrator to perform zoning for individual VMs so that a VM can access the Fibre Channel storage with direct access to the LUNs. There are a few requirements to implement NPIV; they are as follows:

▸ To implement NPIV, the Fibre Switch connected to HBA should support NPIV

▸ HBA connected to an ESXI host should also support the NPIV feature

▸ Only RDM disks can use NPIV; virtual disks cannot be used with NPIV

▸ To implement NPIV, the physical HBA WWN on the ESXi server must have access to all LUNs that are accessed by the Virtual Machines

You can configure Fibre Channel NPIV for a virtual machine by performing the following steps:

1. Connect to your vCenter server using the vSphere Web Client.

2. Browse to your virtual machine.

3. Right-click on the powered off virtual machine and click on **Edit Virtual Machine Settings**.

4. Click on **VM Options** and expand the **Fibre Channel NPIV** options.

5. Deselect the **Temporarily disable NPIV for this Virtual Machine** checkbox.

6. Select **Generate new WWNs** and specify the number of WWNs and WWPNs.

7. Click on **OK**. Note down the number of WWNs generated to provide storage access to the virtual machine.

8. Configure your storage to provide access to the virtual WWNs so that the virtual machine can access the Storage LUNs directly with the use of virtual WWNs.
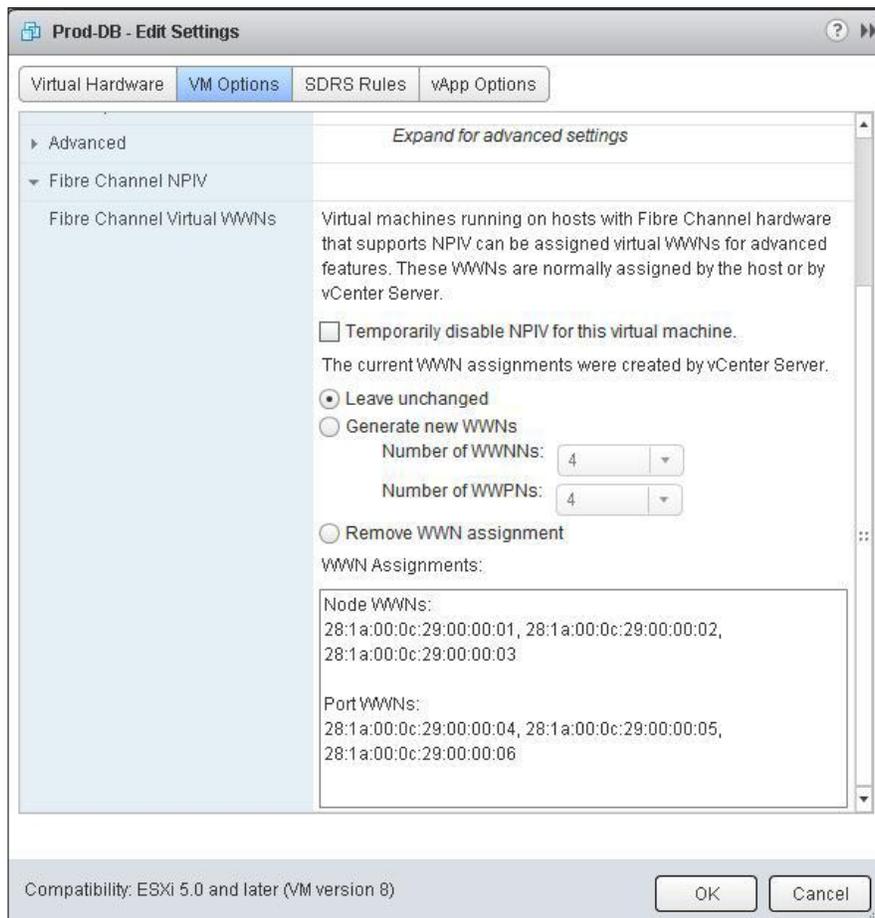
Configuring Raw Device Mapping

Raw Device Mapping (RDM) is a method to provide direct access of iSCSI or Fibre Channel storage LUN to a virtual machine. RDM is basically a mapping file placed in a VMFS volume, which acts as a proxy for a raw physical storage device. A virtual machine can access the storage device directly using RDM, and RDM contains metadata, which controls the disk access to the physical device. The following are some of the use case scenarios for using Raw Device Mapping:

▸ For Microsoft cluster configuration in a virtual machine (virtual-to-virtual or physical-to-virtual configuration)

▸ For configuring a virtual machine to use N_Port ID Virtualization (NPIV)

▸ For running the SAN management software (storage resource management software, storage array snapshot software, replication software, and so on) inside a virtual machine

▸ For any application running on a virtual machine that needs to access a device using hardware-specific SCSI commands

▸ For any physical-to-virtual conversion operations by avoiding the migration of a large data LUN to a VMDK

Getting ready

Connect to your vCenter server via the vSphere Web Client login.

How to do it...

We will take a look at the step-by-step procedure to attach a RDM disk to a virtual machine and to configure a path policy for an RDM mapped LUN.

You can attach a Raw Device Mapping disk to a virtual machine by performing the following steps:

1. Browse to the virtual machine in the vSphere Web Client.
2. Right-click on the virtual machine and select **All vCenter Actions**.
3. Choose **Edit settings** and then select **Virtual Hardware**.

4. Choose an RDM Disk from the **New device** drop-down menu and click on **Add**.

5. From the list of available LUNs, choose a Raw LUN for your virtual machine.

6. Click on the newly added RDM disk to expand its properties.

7. Select the location from the drop-down menu to save the RDM disk:

    ❑ **Store with the virtual machine**

    ❑ Click on **Browse** to save it in a different location and select the datastore to store this RDM disk

8. Choose one of the following compatibility modes for your RDM disk from the **Compatibility Mode** dropdown:

    ❑ **Virtual** compatibility mode

    ❑ **Physical** compatibility mode

9. Verify the Physical LUN path and LUN ID.

10. Select the SCSI controller from the **Virtual Device Node** drop-down list.

11. Select any one **Disk Mode** from the following three options if you chose the virtual compatibility mode. The **Disk Mode** option will be grayed out if you chose the physical compatibility mode for your RDM disk.

    ❑ **Dependent**: This allows dependent disks to be included in snapshots.

    ❑ **Independent - Persistent**: This causes the changes to be immediately and permanently written to the disk, which is similar to your physical hard disk. Persistent disks are not affected by snapshots.

    ❑ **Independent - Nonpersistent**: This causes the changes made to the disks to be discarded when powered off, reset, or reverted to the snapshot. Changes to the disk are deleted when you power off or reset.

12. Click on **OK** to create and attach the RDM disk to the virtual machine, as shown in the following screenshot:
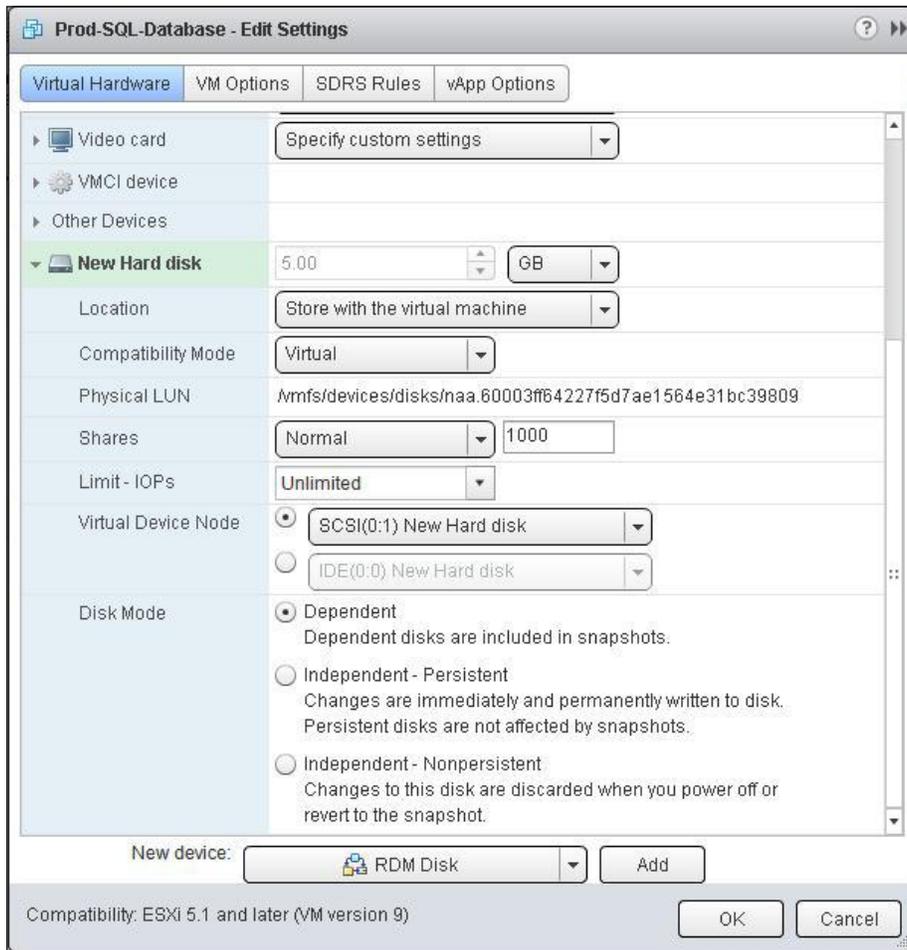
You can configure the path policy for an RDM-mapped LUN by performing the following steps:

1. Browse to the virtual machine in the vSphere Web Client.

2. Right-click on the virtual machine and select **All vCenter Actions**.

3. Choose **Edit settings** and select **Virtual Hardware**.

4. Click on the RDM disk to expand the disk properties.

5. Click on the **Manage paths** option in the multipathing setting:
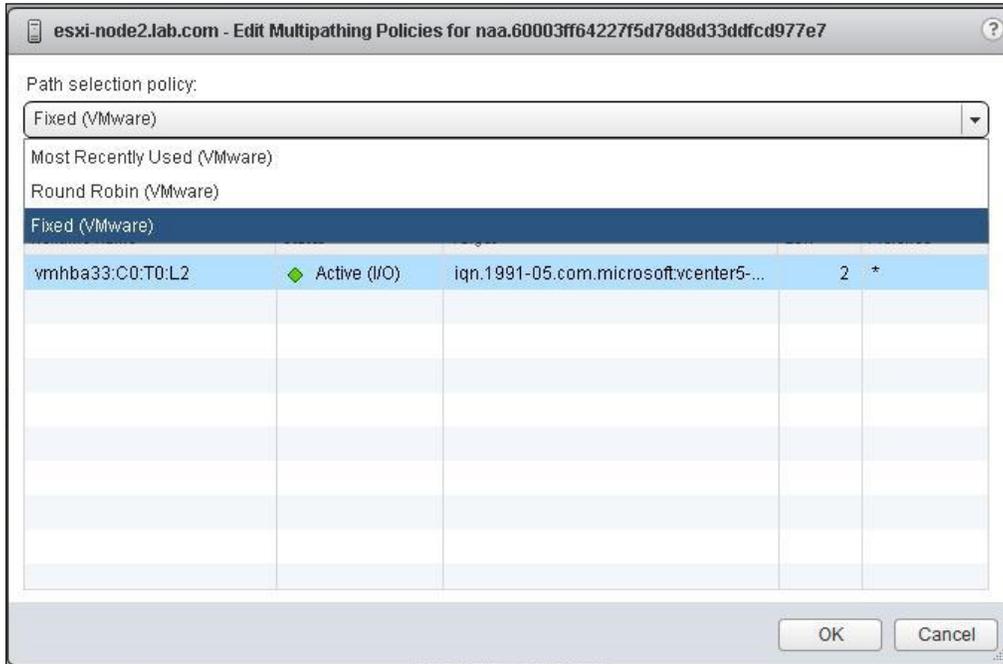
6. Choose one **Path selection policy** among the following from the dropdown:

   ❑ **Most Recently Used (VMware)**

   ❑ **Round Robin (VMware)**

   ❑ **Fixed (VMware)**

7. Click on **OK** for the path policy selected in the virtual machine properties window to apply the multipathing policy.

How it works...

RDM is basically a mapping file that acts as a proxy for a raw physical storage device placed in a VMFS volume. Raw Device Mapping works with two different compatibility levels. They are as follows:

▸ **Virtual Compatibility Level**: In this mode, the mapped raw LUN looks similar to a virtual disk stored in a VMFS volume to a guest operating system. VMkernel hides the real characteristics of physical storage and only sends read and write operations to the mapped device. The virtual compatibility mode is of a very flexible type. It allows us to use features such as advanced file locking for data protection and snapshot support for Virtual Machines.

▶ **Physical Compatibility Level**: In this mode, the RDM works in exactly the opposite way to the virtual mode. All the physical characteristics of the storage devices are exposed to the guest operating system. In this mode, VMkernel simply passes all the SCSI commands to the device. This physical mode RDM is useful in scenarios such as running the SAN management software in the virtual machine and also in the Microsoft cluster between virtual and physical servers. If you want to use a disk capacity of more than 2 TB, you can use the physical compatibility mode. Along with benefits, physical RDM has limitations while performing a storage vMotion of disks larger than 2 TB. Also, disks larger than 2 TB cannot be converted to virtual disks using clone, and snapshots of a virtual machine with physical compatibility mode RDM are not allowed.

There's more...

Apart from the GUI, we will take a look at how to create RDM Mapping LUN using vmkfstools.

Let us see how to create a Raw Device Mapping using the vmkfstools command. First, identify the pathname of the LUN to be used for the RDM. Use the following command to list all the physical devices attached to the ESXi host:

```
ls -l /vmfs/devices/disks
```

Identify the LUN path for the RDM starting with `naa.xxxxxxxxxxxxxxxxx` and note down the device ID to create the RDM disk. Verify and confirm the device ID and LUN size to create the RDM and copy the device ID so that it can be used later. To create the RDM from the available LUN, execute the following command:

```
vmkfstools -z /vmfs/devices/diks/<deviceid> /vmfs/volumes/<datastore-
name>/<VM-folder-name>/<rdmname>.vmdk
```

For example, take a look at the following command:

```
vmkfstools -z /vmfs/devices/disks/naa.xxxxxxxxxxxxxxxxxxxxxxxx
  /vmfs/volumes/FC-datastore1/sqlprod/sqlprod-rdm0.vmdk
```

Once an RDM disk is created, attach the RDM disk to a virtual machine using the **Add Hardware Wizard**. Use the existing disk option to browse to the location of the RDM disk and attach it to the virtual machine to use the RDM disk.

Managing VMFS and NFS datastores

VMFS stands for **Virtual Machine File System**. VMFS and NFS datastores are used to store virtual machines running on ESXi hosts. Datastores are like logical containers that hide the physical world of storage from Virtual Machines. The VMFS filesystem is also a clustered filesystem. It can be shared across multiple ESXi hosts concurrently. Up to 128 ESXi hosts can concurrently connect to a single VMFS datastore. vSphere5 uses the VMFS version 5. VMFS5 was released with a lot of improvement in performance and scalability as compared to VMFS3 available with the older version of vSphere.

Getting ready

Connect to your vCenter server via your vSphere Web Client login. Browse towards your datastore from the vSphere Web Client and select the datastore to expand its size. Select **Actions** and choose **Increase Datastore Capacity**.

How to do it...

We will take a look at the step-by-step procedure to perform various operations to manage the VMFS and NFS datastores via the vSphere Web Client.

You can expand the VMFS datastore (to use the storage capacity available within the same storage LUN) by performing the following steps:

1. Choose the storage LUN which is marked as **Yes** in the **Expandable** section, as shown in the following screenshot:
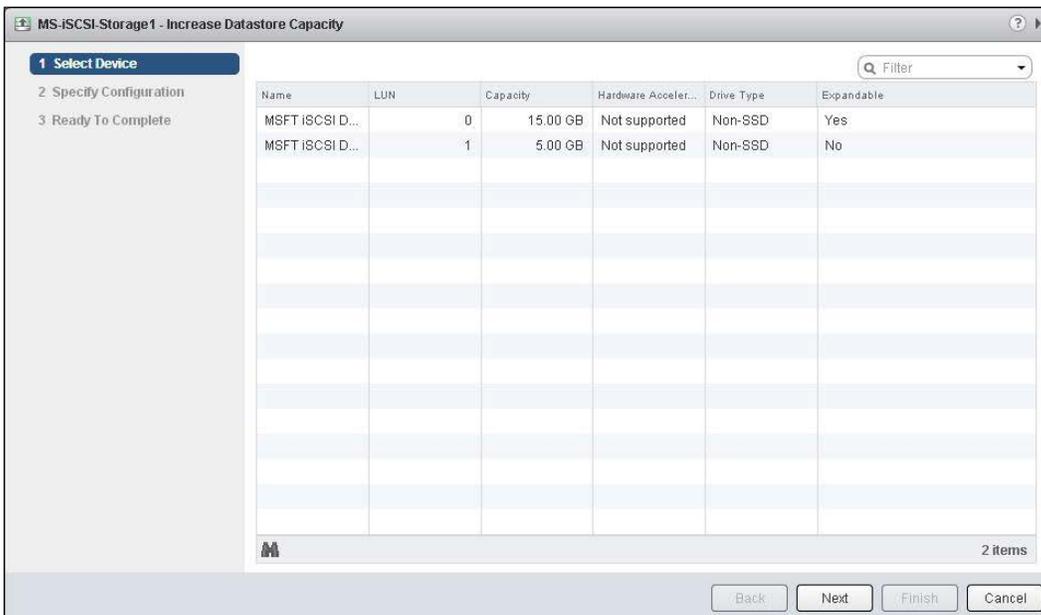
2. From the **Partition Configuration** drop-down menu, choose **Use 'Free Space xx.xx GB' to expand the datastore**, as shown in the following screenshot:
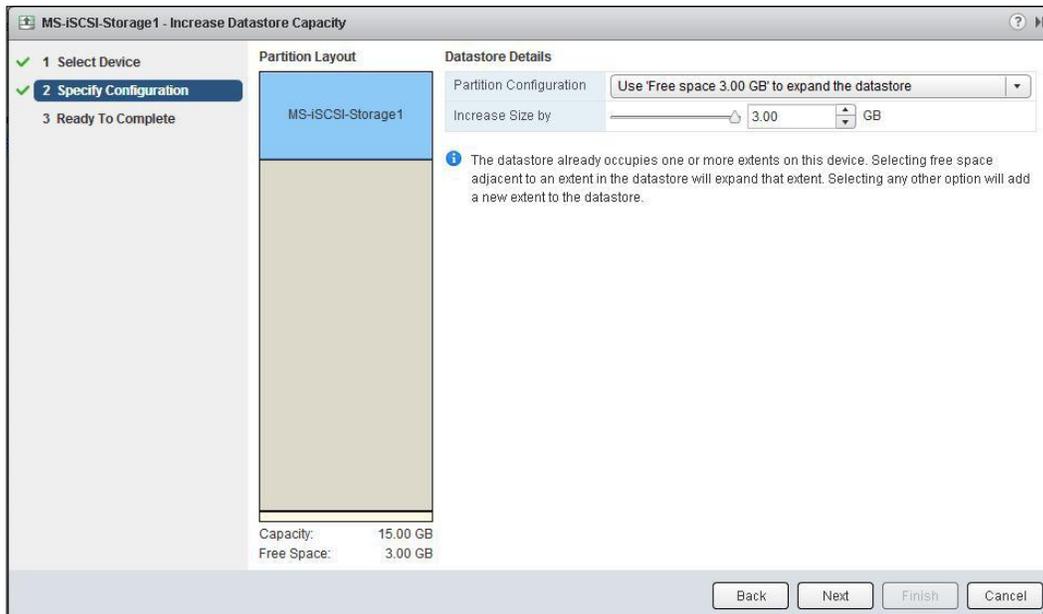
3. Adjust the **Increase size by** option as per your requirement.

4. Click on **Next** and review the information.

5. Click on **OK** to increase the capacity of the datastore.

You can extend the VMFS datastore (to use the storage capacity available within the different storage LUN) by performing the following steps:

6. Choose the storage LUN that is marked as **No** in the **Expandable** section.

7. From the **Partition Configuration** dropdown, choose **Use all available partitions**, as shown in the following screenshot:
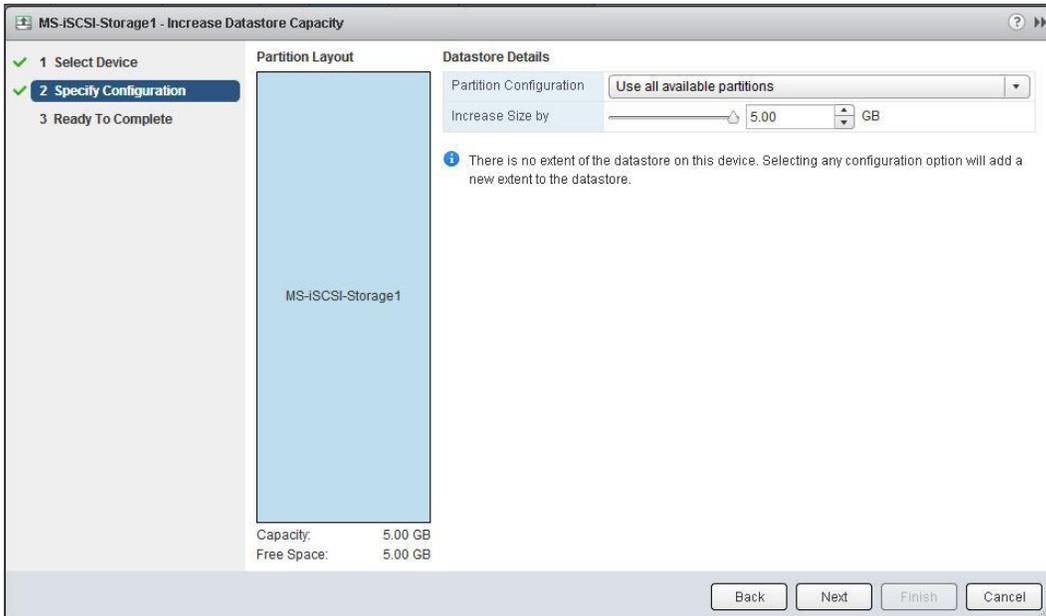
8. Adjust the **Increase size by** option as per your requirement.

9. Click on **Next** and review the information.

10. Click on **OK** to increase the capacity of the datastore using the extend option.

If you unmount a datastore from the ESXi host, it is no longer seen only from the hosts that you specify the datastore to unmount from. It will remain connected to the other hosts that remain mounted. Be cautious when performing this step in production environments. You can use the following steps to unmount a VMFS datastore:

1. Browse towards your datastore from the vSphere Web Client.

2. Select the **Datastore** to unmount.

3. Select **Actions** and choose **All vCenter Actions**.

4. Click on **Unmount Datastore**.

5. Select the ESXi hosts that you want to unmount the datastore from.

6. Click on **OK**.

You can mount a VMFS datastore by performing the following steps:

1. Browse towards your datastore from the vSphere Web Client.
2. Select the **Datastore** to unmount.
3. Select **Actions** and choose **All vCenter Actions**.
4. Click on **Mount Datastore**.
5. Select the ESXi hosts that you want to mount the datastore on.
6. Click on **OK**.

The VMFS file browser can be used for various purposes, including for viewing or searching the datastore content. It can also be used to upload and download files from your datastore to your local desktop or vice versaand to delete the files from the datastore. Register your Virtual Machines stored on the datastore to the vCenter inventory and also to use the inflate option to convert the disk format from thick to thin and thin to thick. To use a file browser in vSphere Web Client, the client integration must be installed by performing the following steps:

1. Browse towards your datastore from the vSphere Web Client.
2. Select the **Datastore** to browse.
3. Select **Actions** and choose **File browser**.
4. Click on **Install the client integration plug-in to enable the file transfers** and follow the installation instructions.
5. Once it is installed, you can upload, download, and delete the files using the VMFS file browser.

You can create an NFS datastore by performing the following steps:

1. Browse towards your ESXi host.
2. Select the ESXi host and click on **Actions**.
3. Select **All vCenter Actions** and click on **New Datastore**.
4. Enter a **Name** for the datastore.
5. Select the type as **NFS datastore** to create an NFS datastore.
6. In the configuration information option page, enter your NFS server's IP address or host name in the server option.

7. Enter the complete folder path of your NFS mount. If you want to mount the NFS as read-only, select the **Mount NFS as read-only** checkbox, as shown in the following screenshot:
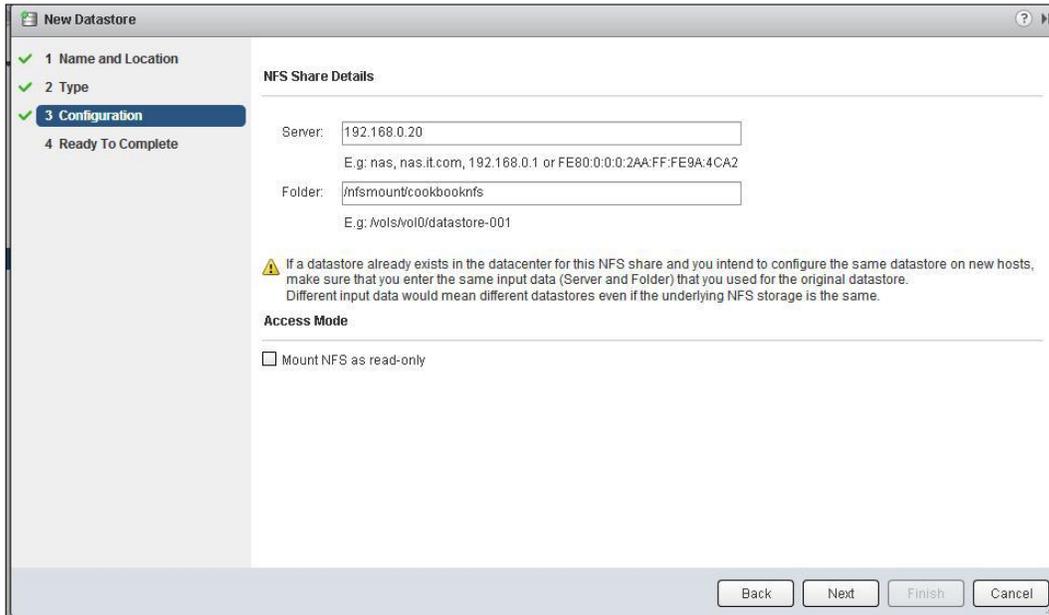
8. Review the options and click on **Finish** to create the NFS datastore.

If you unmount an NFS datastore from the ESXi host, it is no longer seen only from the hosts that you specify the datastore to unmount from. It will remain connected to the other hosts that remain mounted. You can unmount an NFS datastore by performing the following steps:

1. Browse towards your datastore from the vSphere Web Client.

2. Select the **NFS Datastore** to unmount.

3. Select **Actions** and choose **All vCenter Actions**.

4. Click on **Unmount datastore**.

5. Select the ESXi hosts that you want to unmount the datastore from.

6. Click on **OK**.

How it works...

The datastore which is created from the locally attached disk or directly attached storage. The Fibre Channel LUNs and iSCSI storage LUNs are formatted with the VMFS filesystem, but the datastore created from the NFS storage will not be formatted with the VMFS filesystem. ESXi supports two file systems to store the virtual machine: VMFS and NFS. Basically, shared storage of either VMFS or NFS datastore is required to support the advanced features of vSphere, including vMotion, svMotion, High Availability (HA), and Distributed Resources Scheduler (DRS). They are also required to store media files, such as ISO images, templates, and clones, in a centralized location to simplify the virtual machine provisioning.

There's more...

With the release of vSphere 5, VMFS5 brings lots of performance and scalability improvements as compared to the older version of VMFS filesystems. You are required to upgrade your VMFS version 5 to utilize the new features of VMFS5. There are few requirements that need to be taken care of before upgrading VMFS to version 5. These requirements are as follows:

- ▸ VMFS3 can be directly upgraded to VMFS5, but if you have VMFS2, then it needs to be upgraded to VMFS3 first
- ▸ All ESXi hosts accessing that datastore should support the VMFS5 version
- ▸ The datastore to be upgraded should have at least 2 MB of free blocks available and one free file descriptor

Please refer to the following article to find out the difference between native VMFS5 and VMFS5 upgraded from VMFS3:

```
http://www.vmwarearena.com/2013/07/difference-between-upgraded-vmfs-
5-and.html
```

You can upgrade from VMFS3 to VMFS5 by performing the following steps:

1. Browse to your datastore from the vSphere Web Client.
2. Select the VMFS datastore to upgrade.
3. Select **Actions** and choose **All vCenter Actions**.

4. Choose **Upgrade to VMFS5**, as shown in the following screenshot:
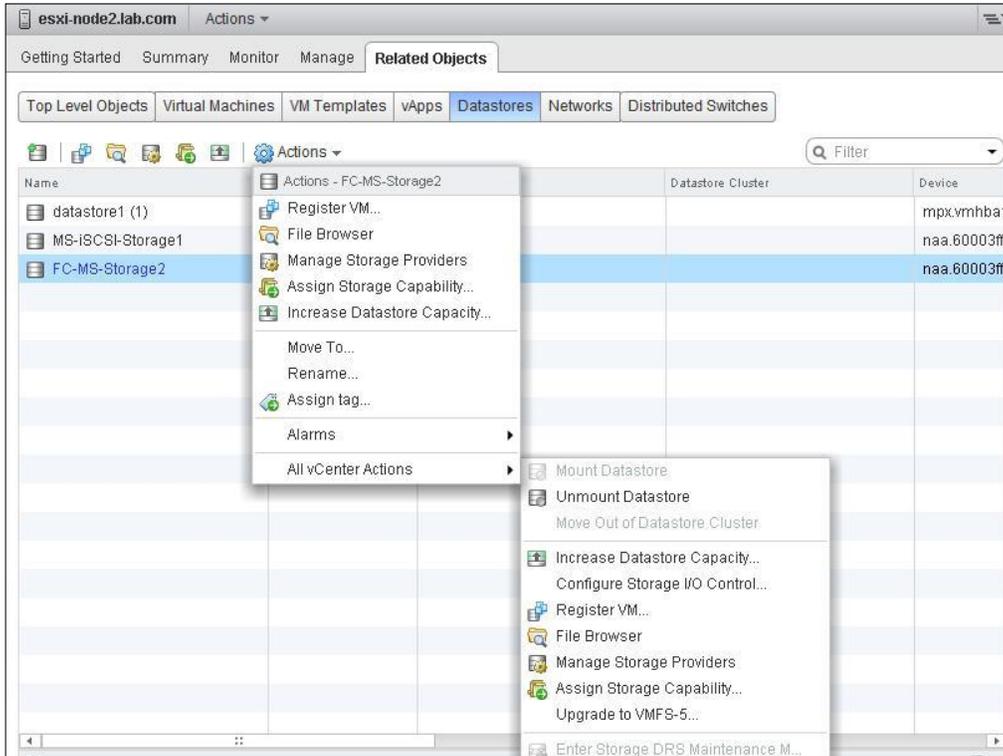
5. Review the validation and make sure that validation status is **Validation succeeded**.
6. Click on **OK** to upgrade to VMFS5.

Configuring the storage profiles of a virtual machine

Profile-driven storage is a feature of vSphere5, which allows you to deploy the Virtual Machines in the right datastore based on the capabilities of the datastore. Let's assume that you have a production database that always needs to be placed in the high-performance storage devices. You can assign the storage profiles while provisioning the virtual machine, or you can manually assign the storage profiles to the virtual machine to ensure that the virtual machine are always placed on the assigned storage devices which match the capabilities. Even during storage migration, you can ensure that it moves to the right storage. At anytime, you can verify the compliance of storage profiles for your virtual machine and take the respective actions to move the VM back to its assigned storage profile.

Getting ready

Connect to your vCenter server via the vSphere Web Client login.

How to do it...

We will take a look at the step-by-step procedure to configure virtual machine storage profiles.

You can add user-defined storage capabilities by performing the following steps:

1. At the home page, click on **Rules and Profiles** and select **VM storage profiles**.
2. Click on the **Create, Remove or Edit** storage capabilities icon.
3. Click on the **+** symbol to add new storage capabilities, as shown in the following screenshot:
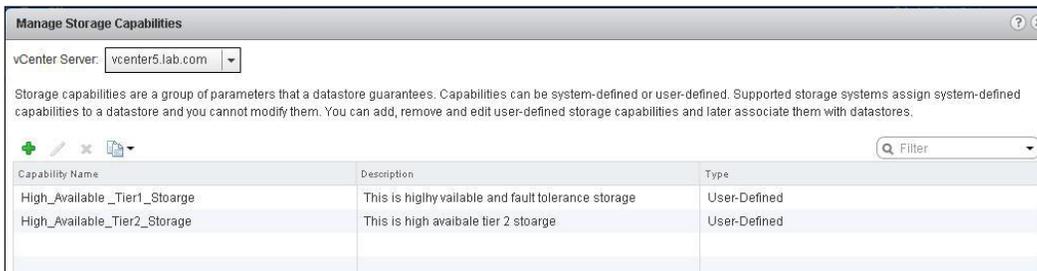
4. Enter the name and description for the new user-defined capabilities.
5. Click on **OK**.

You can assign the user-defined storage capabilities to a datastore by performing the following steps:

1. Browse towards your storage and choose the datastores from the list.
2. Right-click on the datastore and choose the **Assign Storage Capability** option.

3. Choose one of the storage capabilities from the dropdown or create one new capability to assign to your datastore, as shown in the following screenshot:
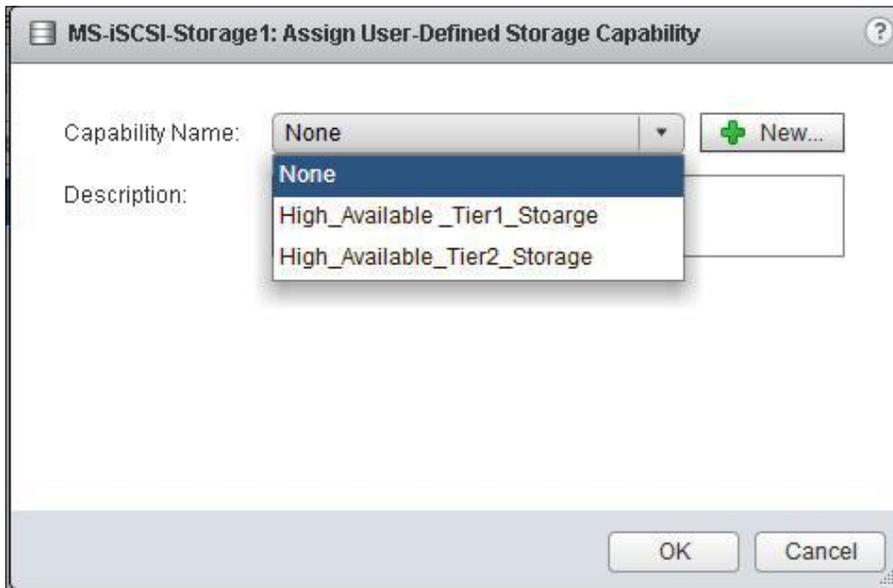
4. Click on **OK**.

You can remove the user-defined storage capabilities by performing the following steps:

1. On the home page, click on **Rules and Profiles** and select **VM storage profiles**.

2. Click on the **Create, Remove or Edit** storage capabilities icon.

3. Select the storage capability from the drop-down list.

4. Click on the remove icon and then on **OK**.

You can enable the virtual machine storage profiles by performing the following steps:

1. On the home page, click on **Rules and Profiles**.

2. Select **VM storage profiles** and click on **Enable VM storage profile**.

3. Choose your **vCenter** server from the dropdown, and it will display all the hosts that are licensed to use storage profiles.

4. Choose the hosts or clusters from the list and click on **Enable**.

5. Make sure that the status of the hosts and clusters is changed to **Enabled for Virtual Machine storage profiles**.

You can create the virtual machine storage profiles by performing the following steps:

1. On the home page, click on **Rules and Profiles** and select **VM storage profiles**.
2. Click on the **Create VM storage Profiles** icon and select the vCenter server.
3. Enter the **Name** and **Description** for the virtual machine storage profile, as shown in the following screenshot:

4. Select the storage capabilities to include in the storage profiles.
5. Click on **OK** to create the virtual machine storage profile.

You can apply the virtual machine storage profiles by performing the following steps:

1. Browse to the virtual machine from vSphere Web Client.
2. Select the virtual machine to apply the VM storage profiles to.
3. Click on the **Manage** tab and select **Profiles**.
4. Click on **Manage storage profiles**.
5. Select the storage profile from the **Home VM Storage Profile** dropdown.

6. Click on **Propagate to disks** to apply the same storage profile to VMDK, or you can apply different profiles to different VMDK disks.
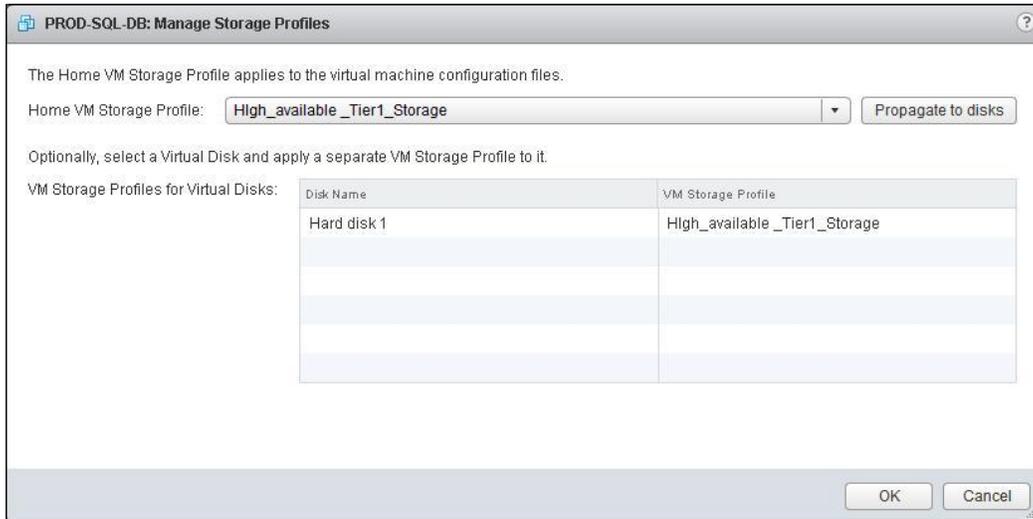
7. Click on **OK**.

How it works...

Virtual machine storage profiles ensure that the assigned Virtual Machines are always placed in the right datastore based on the storage capability of the datastore. Follow the ensuing steps to create and assign user-defined storage capabilities and virtual machine storage profiles:

1. If you don't have system-defined storage capabilities that are a part of storage devices, create user-defined storage capacities.

2. Associate the user-defined capabilities with the datastores available on your vCenter server.

3. Enable the virtual machine storage profiles for the host or clusters in your vCenter server.

4. Create a virtual machine storage profile by defining the storage capabilities created in the previous steps.

5. Associate a virtual machine storage profile to virtual machine and virtual disks.

6. Verify whether your virtual machine and virtual disks are compliant as per the associated virtual machine storage profile.

There's more...

You can check the status of the virtual machine storage profile compliance:

1. Connect to the vCenter server using the vSphere Client.

2. On the home page, click on **Rules and Profiles** and select **VM storage profiles**.

3. Click on any storage profile and then on the **Monitor** tab.

4. Click on **Check Compliance Now**.

5. Check the compliance status of the virtual machine, as shown in the following screenshot:
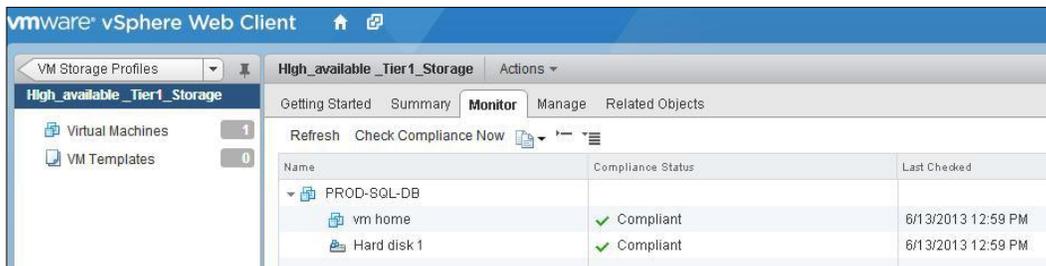
6. Make sure that the virtual machine and virtual disks are compliant for the applied storage profiles.

5

Resource Management and High Availability

In this chapter, we will cover the following topics:

- ▶ Preparing hosts for vMotion
- ▶ Implementing resource pools
- ▶ Implementing **Distributed Resource Scheduling** (**DRS**)
- ▶ Implementing **Distributed Power Management** (**DPM**)
- ▶ Implementing **High Availability** (**HA**)
- ▶ Implementing **Storage Dynamic Resource Scheduling** (**SDRS**)

Introduction

The main goal of virtualization is to utilize the underlying hardware efficiently. The need for resource management arises from overcommitment of resources such as CPU and memory. Over commitment of resources is allocating more resources than the actual capacity. vSphere resource management allows you to dynamically allocate resources so that you can use the available capacity more efficiently. We will take a look at resource management features, such as resource pools and **Dynamic Resource Scheduling (DRS)**, of vSphere.

Business availability is one of the needs of the modern datacenter. vSphere provides high availability to virtual machines running on ESXi hosts and applications running on a virtual machine's guest operating system. vSphere provides intelligent high availability solutions such as vSphere **High Availability (HA)** to keep the business continuity of your datacenter more efficient.

Preparing hosts for vMotion

vMotion allows you to migrate your running virtual machines between ESXi hosts without any downtime. Shared storage between ESXi hosts is one of the strong requirements for migrating the virtual machines with vMotion. With vSphere 5.1, vMotion allows you to migrate live virtual machines, including memory and storage between ESXi hosts, without any need of shared storage.

Getting ready

Connect to your VMware vCenter Server using the vSphere Web Client.

How to do it...

We'll demonstrate a step-by-step procedure to prepare hosts and virtual machines for vMotion, along with the detailed steps, by initiating vMotion of the virtual machine:

1. ESXi hosts must be licensed for vMotion. The host must be licensed with vSphere Essential Plus, Standard, Enterprise, or Enterprise Plus license.

2. DRS and DPM use the traditional vMotion for migration operations. So the ESXi hosts should be attached with shared storage such as **Fibre Channel (FC)**, **Internet Small Computer System Interface (iSCSI)**, or **Network filesystem (NFS)** between the ESXi hosts.

3. Source and destination hosts must be configured with the VMkernel port group for vMotion traffic:
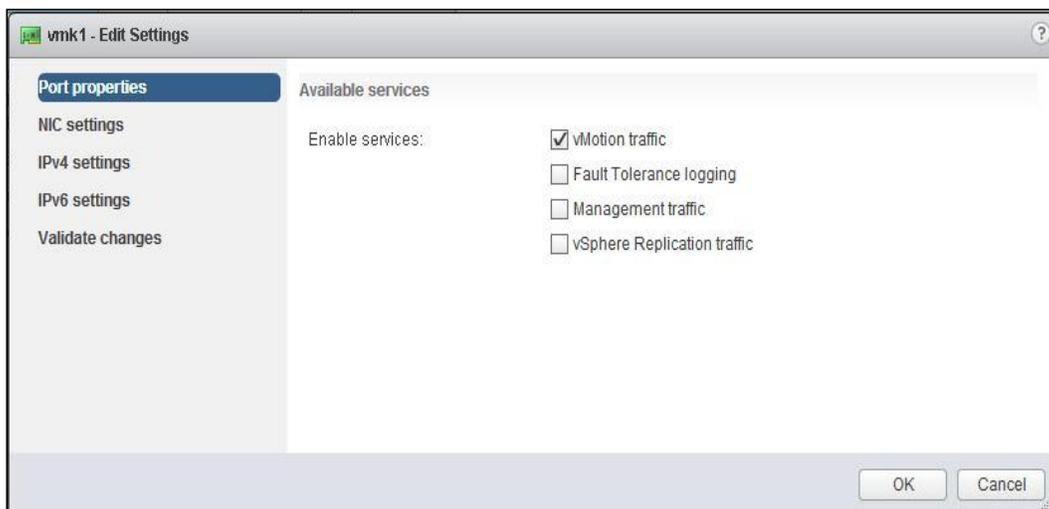
4. Network labels used for the virtual machine port group should be the same across ESXi hosts if you are using standard switches.

5. Virtual machines must have access to the same subnets on source and destination hosts.

6. The source and destination hosts must be members of all distributed switches that Virtual machines use for networking if you are using vSphere distributed switches.

7. The source and destination host should have a CPU from the same family and the same vendor because vMotion between multivendor CPUs (Intel and AMD) is not possible.

The following steps have to be performed to prepare a virtual machine for vMotion:

1. Virtual machines must have access to the same subnets on source and destination hosts.

2. Source and management network IP address families of the ESXi host must be the same, either IPv4 or IPv6.

3. A virtual machine configured with a raw disk for clustering cannot be migrated with vMotion.

4. Virtual machines connected with a CD drive, which is backed by the physical CD drive on the source ESXi host, cannot be migrated with vMotion. It must be disconnected before initiating vMotion. It is also applicable for other devices that are not accessible on the destination host.

5. Connection of Virtual machines should be migrated with the device, which is backed by a device on the client computer. You must disconnect the device before initiating vMotion.

6. Virtual machines, which are connected to the physical USB device on the host, can be migrated with USB devices. You must enable the devices for vMotion.

7. Virtual machines configured with a virtual CPU performance counter can be migrated only to the destination host, which has compatible CPU performance counters.

For performing vMotion of a virtual machine with shared storage, the following steps have to be performed:

1. Browse towards your virtual machine in the vSphere Web Client.

2. Right-click on the VM and select **Migrate**.

3. Select the **Change host** option from **Select Migration type**:
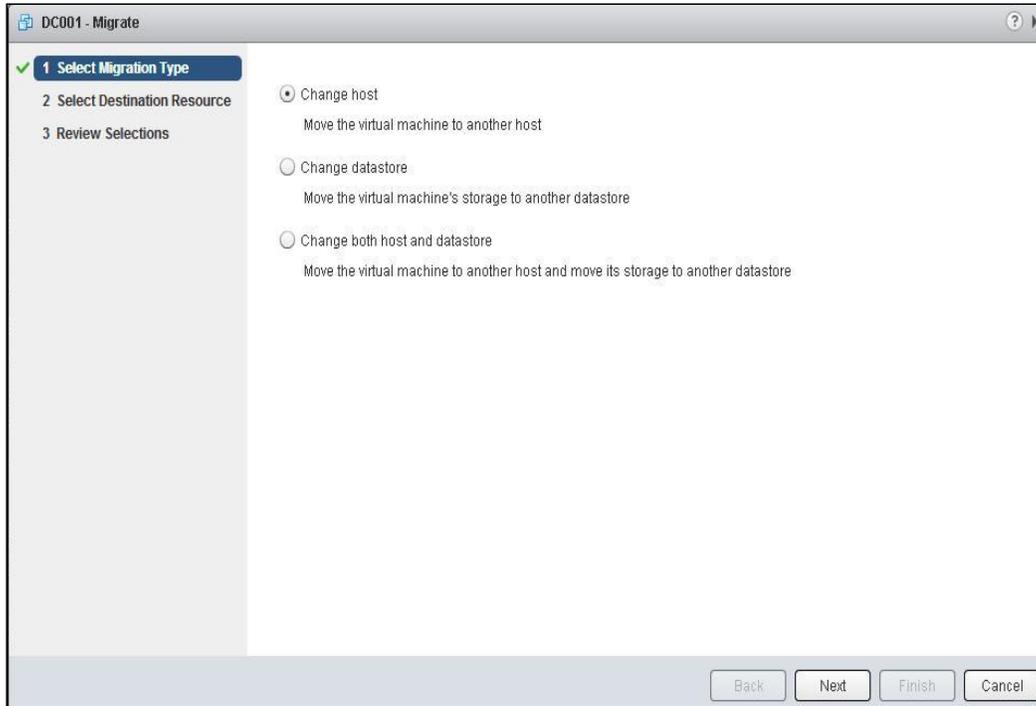
4. Select the **Cluster**, **host**, **resource pool**, or **vApp** options as the destination of this virtual machine migration.

5. Select the **Allow host selection within this cluster** checkbox to specifically choose the host from the cluster for this migration, and then click on **Next**:
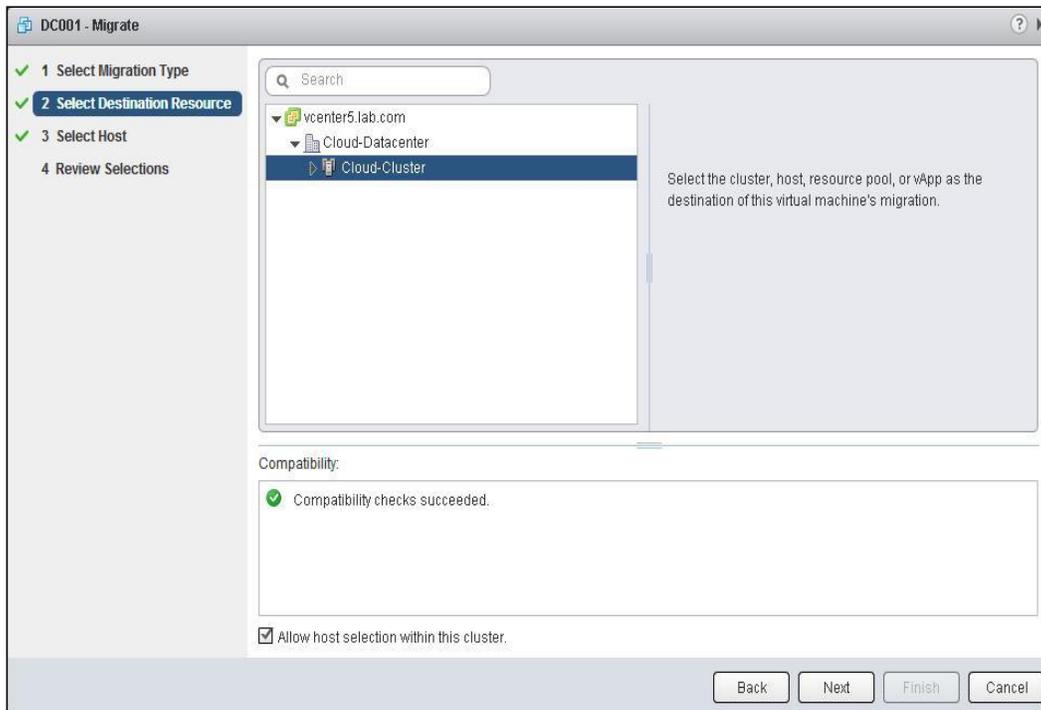
6. Select the specific host from the list and verify whether the compatibility checks have succeeded, and then click on **Next**.

7. Review the selection and click on **Finish** to initiate the vMotion migration of a virtual machine.

8. Verify that the recent task is showing the status of a recent migration (**Relocate virtual machine**) completed successfully with a green check:

How it works...

vMotion migrates the live virtual machine from one host to another without any downtime. vMotion uses the *pre-copy iterative* approach to transfer the memory contents of the virtual machine. There are phases in transferring the virtual machine's memory; they are explained as follows:

- ▸ **Guest trace phase**: During this phase, the virtual machine guest memory is staged for migration. Traces are placed on the guest memory pages to track the modifications performed by the guest during migration.

- ▸ **Pre-copy phase**: During this phase, a virtual machine continues to run on the source ESXi host and it actively modifies its memory state on the source ESXi host. Memory contents of the virtual machine are copied in an interactive process from the source ESXi host to the destination ESXi host. Each iteration copies only the modified memory pages that were modified during the previous iteration.

- ▸ **Switch-over phase**: During this phase, the virtual machine is temporarily quiesced on the source ESXi host, the last set of memory changes are copied to the destination ESXi host, the virtual machine is resumed on the target ESXi host, and it continues to run on the target ESXi host without any downtime to the applications running on the virtual machine.

There's more...

With vSphere 5.1, vMotion allows you to migrate the live virtual machines, including memory and storage between ESXi hosts without any need of shared storage. This feature is called **Shared Nothing vSphere vMotion**. Let's take a look at the detailed step-by-step procedure to initiate vMotion without shared storage between the source and destination ESXi hosts.

In order to perform vMotion without shared storage, the following steps have to be performed:

1. Browse towards your virtual machine in the vSphere Web Client.

2. Right-click on the VM and select **Migrate**.

3. Select the **Change both host and datastore** option from **Select Migration Type**:
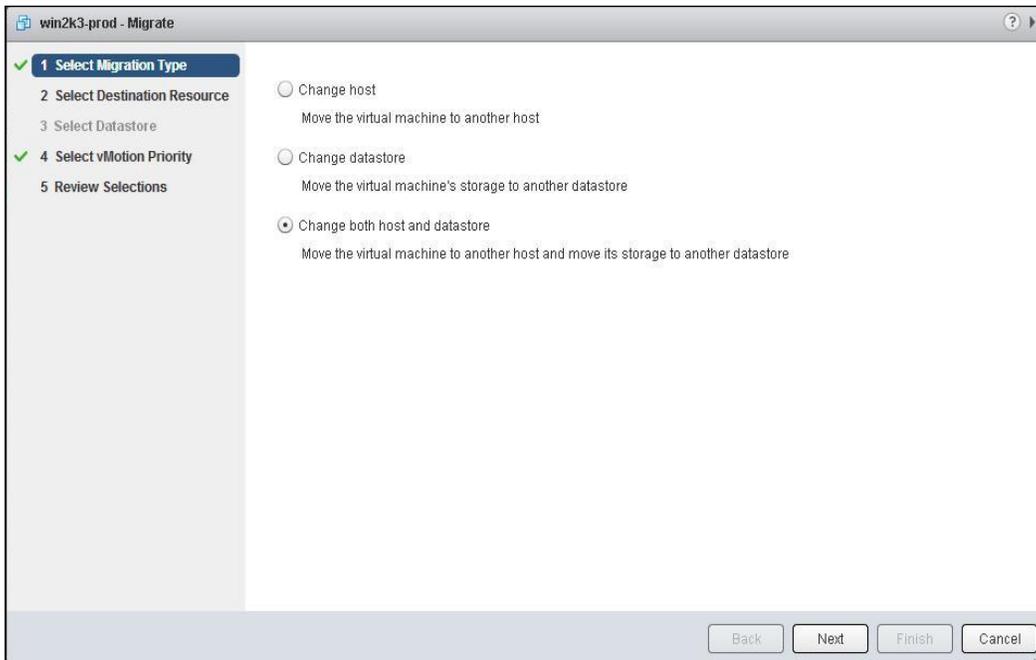
4. Select the **Cluster**, **host**, **resource pool**, or **vApp** options as the destination of this virtual machine migration.

5. Select the **Allow host selection within this cluster** checkbox to specifically choose the host from the cluster for this migration, and then click on **Next**.

6. Select the specific host from the list and verify that the compatibility checks succeeded; then click on **Next**.

7. Select the datastore from the list of available datastores. If you want to change the virtual disk format during this migration, select the **Disk Format** type from the **Select virtual disk format** dropdown and choose one of the following disk formats from the available options, as shown in the following screenshot:

❑ **Same format as source**

❑ **Thick Provision Lazy Zeroed**

❑ **Thick Provision Eager Zeroed**

❑ **Thin Provision**
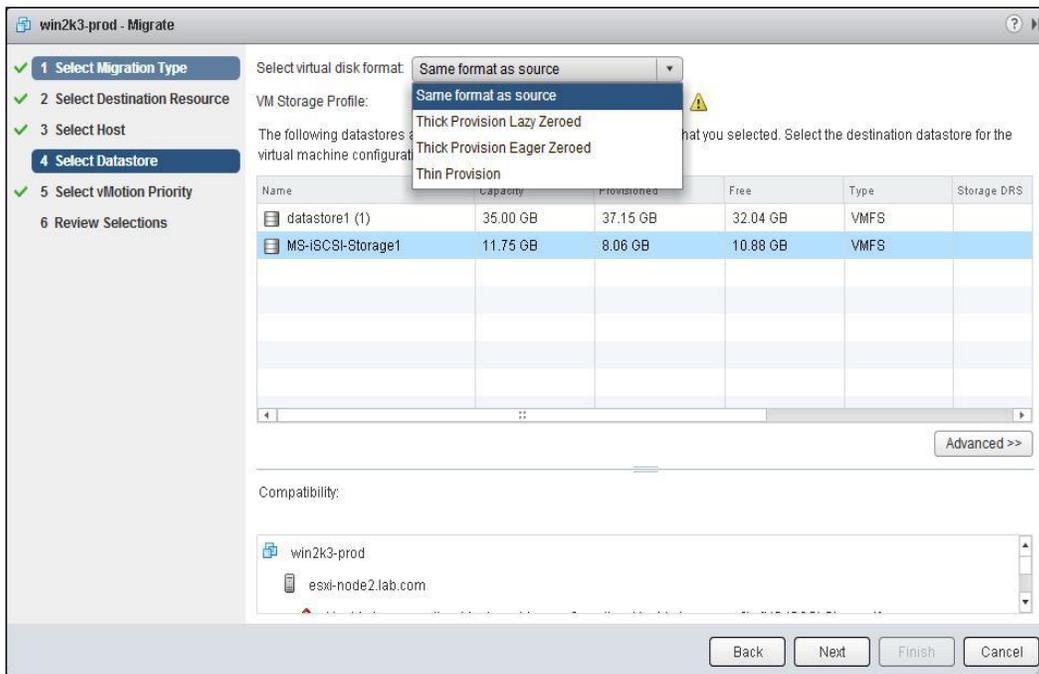
8. You can individually choose the virtual disk format and datastore location for each virtual disk of the virtual machine. Click on the **Advanced>>** button, choose the **Datastore** location and **Disk Format**, and click on **Next**:
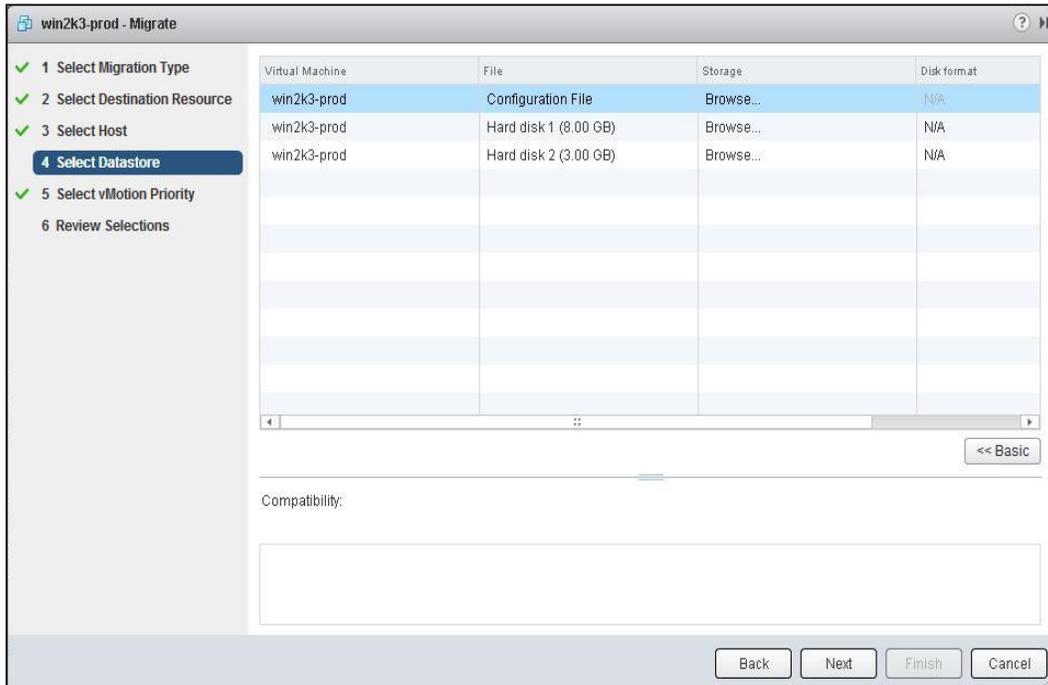
9. Click on **Select vMotion Priority** by selecting one of the following options for this migration and click on **Next**:

   ❑ **Reserve CPU for optimal vMotion performance (Recommended)**: This option is selected if sufficient CPU resources are not immediately available. In this case, vMotion will not be initiated.

❑ **Perform with available CPU resources**: This option is selected if there is a lack of CPU resources. In this case, the duration of vMotion might be extended.
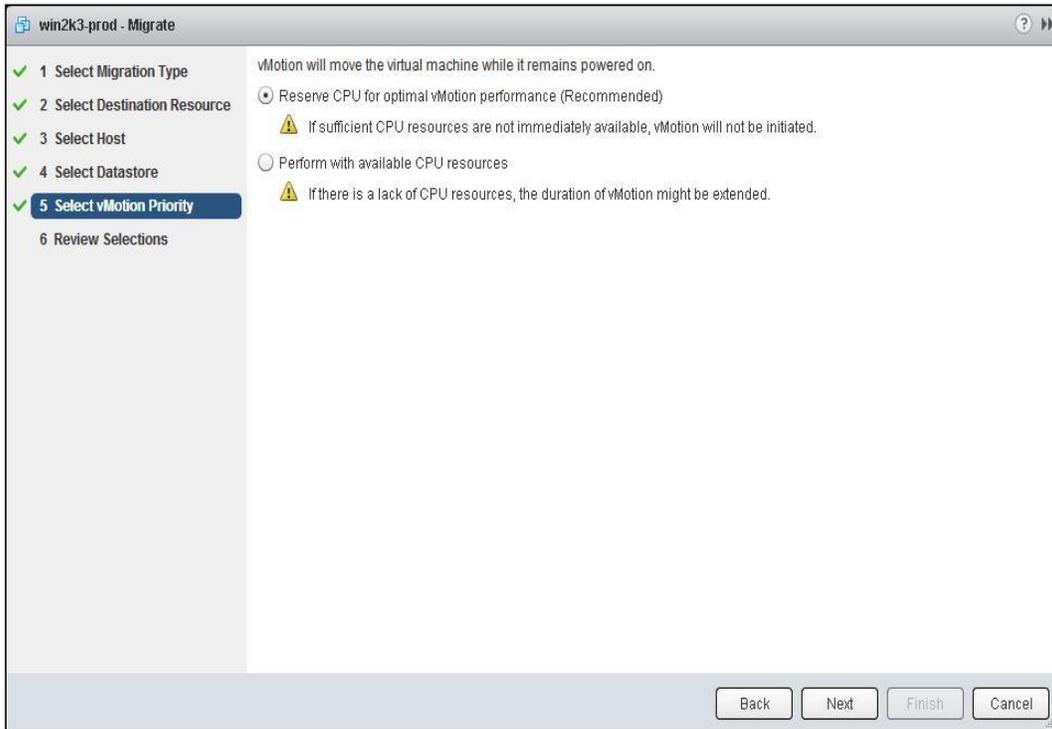
10. Review the options selected and click on **Finish** to initiate the migration.

Implementing resource pools

VMware vSphere clusters combine the computing resources from the ESXi under the clusters and handle resource management of virtual machines efficiently. This is called root resource pool. Resource pools can be created under ESXi hosts if an ESXi host is not a part of the cluster, or it can be created under cluster to create a resource partition of the available CPU and memory resources. It can also be created under another resource pool as a child resource pool. Resource pools can be used to efficiently manage the resource management for a group of virtual machines that belong to the same application or department. Resource pools can also be used to delegate administrative permissions to manage a specific group of virtual machines.

Getting ready

Connect to your VMware vCenter Server using the vSphere Web Client.

How to do it...

We'll take a look at the step-by-step procedure to create, edit, and remove resource pools using the vSphere Web Client.

The following steps have to be performed in order to create resource pools:

1. Browse towards the vSphere cluster from the vSphere Web Client.
2. Right-click on the cluster and select **New Resource Pool**.
3. Enter the name for the new resource pool.
4. Specify the **CPU and Memory Resource allocation** values for the new resource pool:

   ❑ **Shares**: The share value should be Low (Share Value = 2000), Normal (Share Value = 4000), or High (share value = 8000) for a CPU for this new resource pool with respect to the parent's total available resources. This share value differs for memory in values, but basically a share value of low, normal, or high works in both CPU and memory in the proportion of 1:2:4. Sibling resource pools at the same level of this resource pool share resources from the parent resource pool based on their relative values bounded by this share value. You can also choose Custom to manually specify the share value for this resource pool.

   ❑ **Reservation**: Set the reservation value for CPU in **MHz** or **GHz** and for memory in **MB** or **GB** for this resource pool. This ensures that the CPU or memory reserved for this resource pool will always be guaranteed for it.

   ❑ **Reservation type**: Expandable reservation is always enabled by default when you create the resource pool. If the resource required by the powered-on virtual machines in the resource pool is larger than the reservation configured at the resource pool, expandable reservation allows the virtual machines in the resource pool to use the resources available from its parent resource pool.

   ❑ **Limit**: Limits are always set to **Unlimited** by default. Enter the upper limit value for CPU in **MHz** or **GHz** and memory in **MB** or **GB** to configure the resource limit for this resource pool. If you have set the limit for the resource pool, it will not be able to use the resource beyond its configured limit value.

The following screenshot shows the **CPU and Memory Resource allocation** values for the new resource pool:
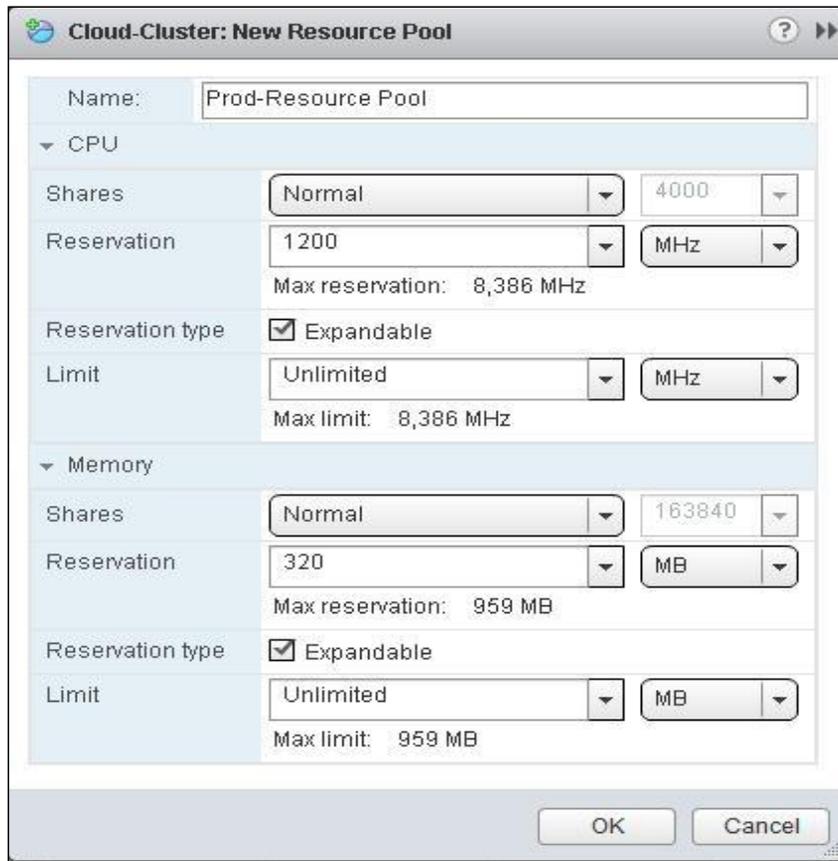
5. Click on **OK** to create the new resource pool under the cluster.

Virtual machines can be added to resource pools during its creation by defining the VM to be placed on the resource pool or during vMotion; another option to move the existing virtual machine into a resource pool is to use the **Move To** option. Let's take a look at how to add the existing virtual machine into resource pools using the **Move To** option. The following steps have to be performed to *add* a virtual machine into a resource pool:

1. Browse to your virtual machine in the vSphere Web Client.
2. Right-click on the virtual machine and select **Move...**.

3. Select the resource pool on the **Move To...** page:
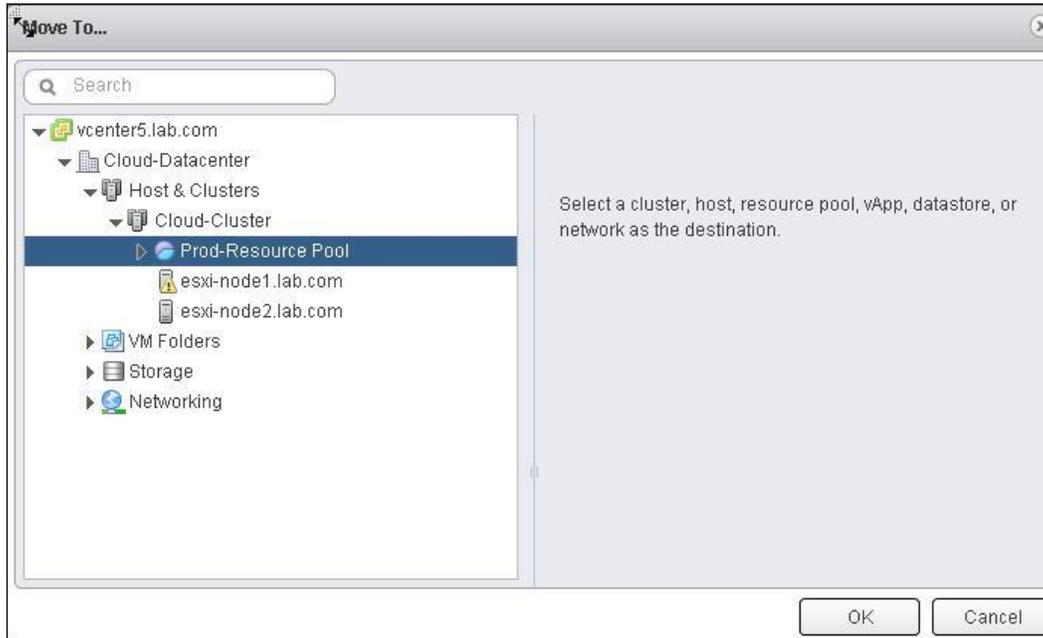
4. Click on **OK** to move the virtual machine under cluster or datacenter into the resource pool.

Virtual machines can be moved out of resources pools during vMotion or you can manually move the virtual machines using the **Move to** option. The following steps have to be performed to *remove* a virtual machine out of a resource pool.

1. Browse towards your virtual machine in the vSphere Web Client.

2. Right-click on the virtual machine under the resource pool and select **Move to**.

3. Select the **Cluster and Hosts** option in the **Move To...** page.

4. Click on **OK** to move the virtual machines out of the resource pool.

The following steps have to be performed to *edit* the resource pool settings:

1. Browse towards your resource pool in the vSphere Web Client.

2. Right-click on the resource pool and click on **Edit settings**.

3. Edit the **CPU and Memory resource** settings in the **Resource Pool-Edit Resource settings** page.

4. Click on **OK** to apply the modified resource settings to the resource pool.

The following steps have to be performed to *delete* the resource pools:

1. Browse towards your resource pool in the vSphere Web Client.
2. Right-click on the resource pool and select **All vCenter Actions**.
3. Choose **Remove from Inventory** to remove the resource pool from your vCenter Server.
4. Click on **OK** to remove the resource pool from the vCenter inventory.

How it works...

Resource pools can be used to create a resource partition of CPU and memory under vSphere clusters or ESXi hosts. Let's assume that you have three different categories of servers (production, development, and test) in your vSphere environment. You always want to ensure that a certain amount of CPU and memory resources is available to production virtual machines. This can be achieved by creating different resource pools for production, development, and test resource pools, and then placing the virtual machines belonging to each category into respective resource pools. In addition to that, if you have different categories of servers, such as database server, file server, or application server. Under production servers, you can even create a child resource pool under production resource pool and configure the CPU and memory shares. Configure CPU and memory shares, reservation, and limits to achieve the resource management of virtual machines under each resource pool.

There's more...

By default, users and groups who have been provided access to the vCenter level will have the permission to perform tasks on the child objects under the vCenter Server. However, there are situations when you want a set of users or groups only to manage the department or virtual machines belonging to that department. In that case, you can create a resource pool and add virtual machines under the department resource pool. Assign a set of users or groups with the permission to only manage the object under the resource pool or change the permission at resource pool to restrict someone from managing it. It minimizes the risk of giving unnecessary permissions to users or groups at vCenter, datacenter, or cluster level. Let's take a look at how to assign permission to the resource pool.

The following steps have to be performed in order to configure permission for resource pools:

1. Browse towards your resource pool in the vSphere Web Client.
2. Select the resource pool and click on the **Manage** tab.
3. Select the **Permission** tab and click on the **+** symbol to add permission to the resource pool.
4. Click on **Add** under the **Users and Groups** option.
5. Select your domain from the **Domain** dropdown.
6. Select the users or groups from the list to be added under the **Users and Groups** option and click on **Add**.
7. Click on **OK** to add the selected user or group to assign permission for this resource pool.

8. Select one of the roles from the **Assigned Role** dropdown to be assigned to the added user or group:

9. Select the **Propagate to children of the HR-Resource Pool resource pool** checkbox to ensure that permission applied at the resource pool level applies to the children under this resource pool; this option is selected by default.

10. Click on **OK** to apply the settings.

Implementing Distributed Resource Scheduler (DRS)

VMware **Distributed Resource Scheduler** (**DRS**) cluster aggregates the hardware resources available from the physical ESXi hosts in the cluster into logical resource pools. DRS continuously monitors the utilization of resource pools and allocates the available resources intelligently among the virtual machines based on the pre-defined DRS rules.

Getting ready

Connect to your vCenter Server via vSphere Web Client login.

How to do it...

We will take a look at the step-by-step procedure to create and configure the DRS cluster:

1. Browse towards the datacenter in the vSphere Web Client.
2. Right-click on the datacenter and select **New Cluster**.
3. Enter the **Name** for your cluster.
4. Select the **Turn ON** checkbox for the DRS.
5. Select one of the following **Automation Level** options for this DRS cluster:
   - **Manual**: This automation level displays the recommended hosts for the initial placement of virtual machines and also displays the recommendation for virtual machine migration. All the migrations need to be performed manually by the administrator based on the displayed DRS recommendation.
   - **Partially automated**: This automation level takes care of automatic initial placement of the virtual machine and displays the recommendation for migration. All the migrations need to be performed manually by the administrator based on the DRS recommendation.

❑ **Fully automated**: This automation level takes care of automatic initial placement of the virtual machine, and migration recommendation is executed automatically to migrate the virtual machines between the ESXi hosts in the cluster to perfectly load-balance it. This is the default automation level selected when you create the DRS cluster:

6. Set the **Migration threshold** level to either **Conservative**, **Aggressive**, or inbetween that using the slider. Move the slider between 1 and 5 to adjust the various migration threshold levels that are explained as follows:

    ❑ **Migration threshold 1 (Conservative)**: This migration threshold value applies only priority 1 recommendations. The vCenter Server will only apply recommendations that must be taken to satisfy cluster constraints such as DRS affinity rules and host maintenance.

    ❑ **Migration threshold 2**: This migration threshold value applies priority 1 and priority 2 recommendations. The vCenter Server will only apply recommendations that promise a significant improvement to the cluster's load balance.

    ❑ **Migration threshold 3**: This migration threshold value applies priority 1, priority 2, and priority 3 recommendations. The vCenter Server will apply recommendations that at least promise good improvements to the cluster's load balance.

    ❑ **Migration threshold 4**: This migration threshold value applies priority 1, priority 2, priority 3, and priority 4 recommendations. The vCenter Server will apply recommendations that promise a moderate improvement to the cluster's load balance.

❑ **Migration threshold 5 (Aggressive)**: This migration threshold value applies all the priority levels, that is, priority 1, priority 2, priority 3, priority 4, and priority 5 recommendations. The vCenter Server will apply recommendations that promise even a slight improvement to the cluster's load balance.

7. Click on **OK** to create the new DRS cluster.

The following steps have to be performed in order to add ESXi hosts into the DRS cluster:

1. Browse towards your cluster in the vSphere Web Client.
2. Right-click on the DRS-enabled cluster and select **Move Hosts into cluster**.
3. Select the checkbox against the ESXi hosts to add into your DRS cluster.
4. Click on **OK**.
5. Select either one of the following options in the **What would you like to do with the virtual machines and resource pools for esxi-node2.lab.com** host's page:

   ❑ **Put all of this host's virtual machines in the cluster's root resource pool. Resource pools currently present on the host will be deleted.**

   ❑ **Create a new resource pool for this host's virtual machines and resource pools. This preserves the host's current resource pool hierarchy.** The **Resource Pool Name** will be **Grafted from esxi-node2.lab.com**.
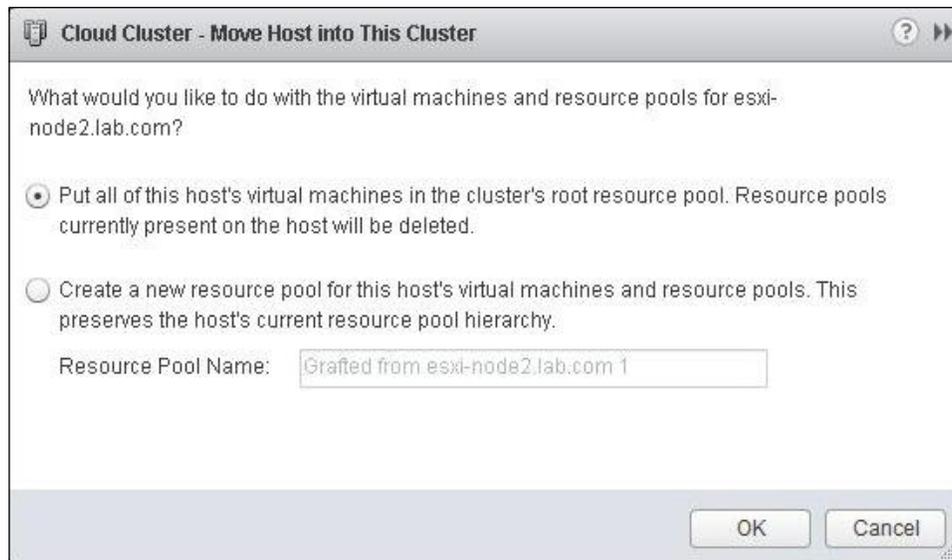
6. Click on **OK** to add the selected ESXi hosts into the DRS cluster.

ESXi hosts should be placed in the maintenance mode to remove it from the vSphere cluster. Let's take a look at the steps to remove the ESXi host from the DRS cluster:

1. Browse towards your ESXi host in the vSphere Web Client.

2. Right-click on the ESXi host and select **Enter Maintenance Mode**.

3. Confirm the maintenance mode by clicking on **OK**.

4. Once the ESXi host is entered into the maintenance mode, right-click on the ESXi host and select **Move to**.

5. Select your datacenter in the **Move To...** page to move the ESXi host out of the current cluster; then click on **OK**.

The following steps have to be performed for editing the DRS cluster settings:

1. Browse towards your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **vSphere DRS** option.

4. Click on **Edit** to edit the DRS cluster settings.

5. Click on **DRS Automation** to expand its properties.

6. Edit the settings of the DRS cluster.

7. Click on **OK** to apply the settings.

The following steps have to be performed in order to configure the custom virtual machine automation level:

1. Browse towards your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **vSphere DRS** option.

4. Click on **Edit** to edit the DRS cluster settings.

5. Select the **Enable individual virtual machine automation levels** checkbox. This option allows you to override the DRS automation level at individual virtual machine levels. An individual override for virtual machines can be configured from the **VM Overrides** page. This option is selected by default:
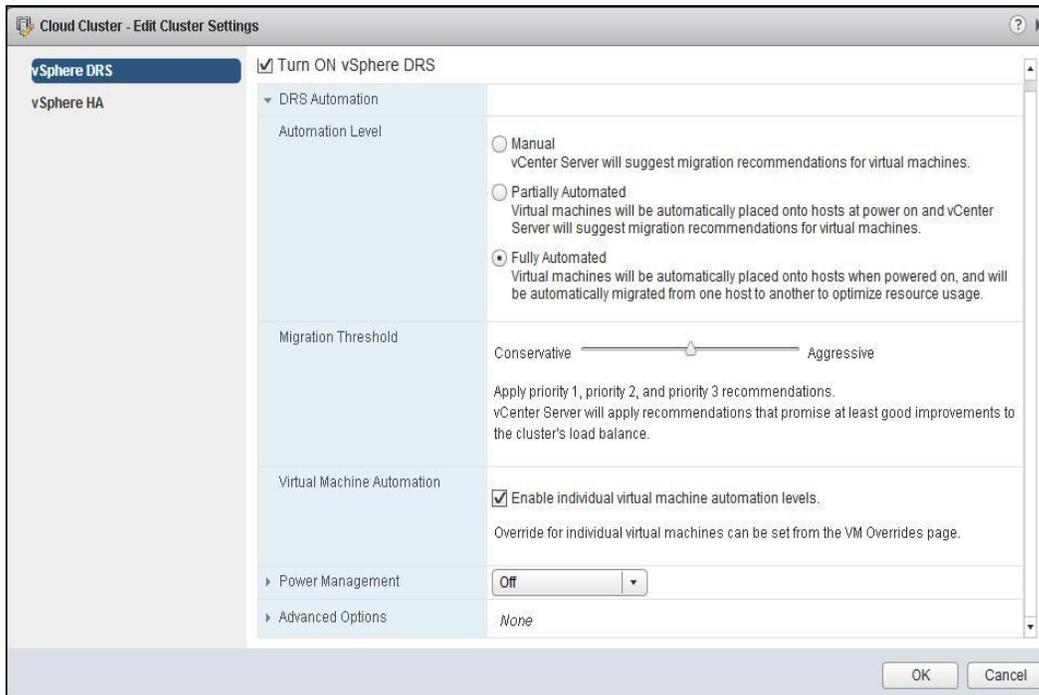
6. Click on **OK** to apply the settings.

7. To configure the individual virtual machine automation levels, click on the **VM Overrides** option under the **Settings** tab.

8. Click on **Add** to configure the custom automation level.

9. Click on the **+** symbol and select the checkbox for each of the virtual machines for which you want to configure custom cluster automation level and click on **OK**.

10. Choose one of the following cluster automation levels from the **Automation level** dropdown. By default, the **Use Cluster settings** option is selected from the following options:

    ❑ **Fully Automated**

    ❑ **Partially Automated**

    ❑ **Manual**

    ❑ **Use Cluster Settings**

    ❑ **Disabled**

The following screenshot demonstrates the preceding steps:
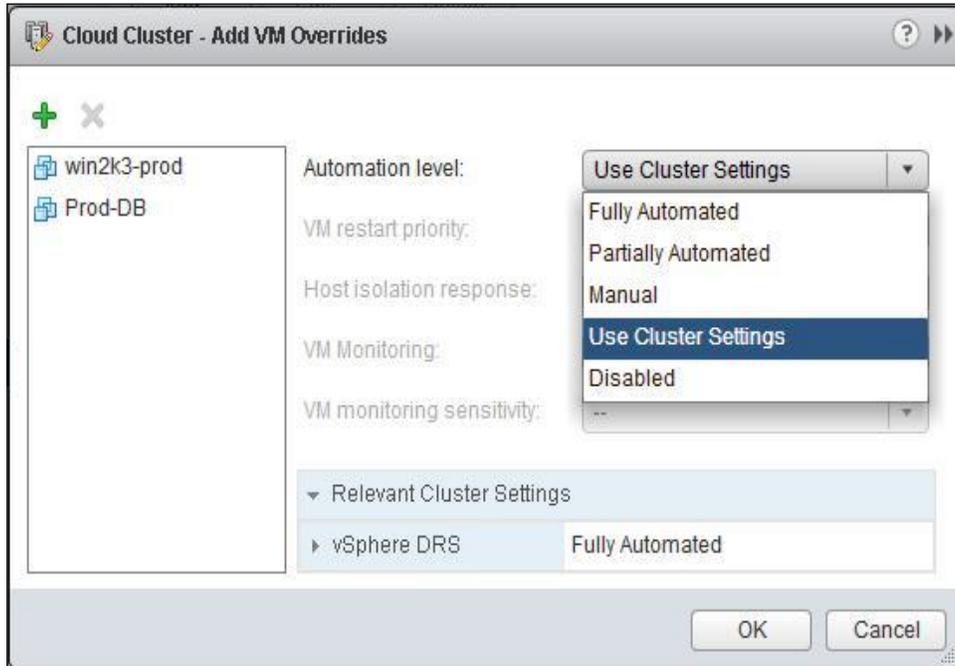
11. Click on **OK** to apply the virtual machine Custom DRS automation level.

DRS compliance will check that the vMotion NIC speed is at least 1000 Mbps, validate that vMotion is enabled, and validate that at least one shared datastore exists between the ESXi hosts in the cluster. The following steps have to be performed in order to check the DRS cluster compliance status:

1. Browse towards your cluster in the vSphere Web Client.
2. Select your DRS cluster and click on the **Monitor** tab.
3. Choose the **Profile Compliance** tab.
4. Click on the **Check Compliance Now** option.
5. Verify that all your ESXi hosts in the DRS cluster have passed the cluster requirement compliance.

Enhanced vMotion Compatibility (**EVC**) reduces the vMotion compatibility issues occurring because of different CPU generation hosts placed in the same cluster. EVC ensures that all ESXi hosts present in the cluster have the same CPU features when compared to the virtual machines in the cluster, even if the CPUs in the ESXi hosts are different from one another. EVC uses AMD-V Extended Migration technology for AMD hosts and Intel FlexMigration technology for Intel hosts to hide the processor features so that all ESXi hosts in the same cluster present the same feature set of a previous generation of processor. The following steps need to be performed in order to configure VMware EVC for DRS cluster:

1. Browse towards your cluster in the vSphere Web Client.
2. Select your DRS cluster and click on the **Manage** tab.
3. Select the **Settings** tab and click on the **VMware EVC** option.
4. Click on **Edit** to edit the VMware EVC settings.
5. By default, EVC is disabled. EVC can be enabled for either the AMD hosts or for the Intel hosts. Choose one of the following EVC mode options:

    ❑ **Enable EVC for AMD Hosts**

    ❑ **Enable EVC for Intel® Hosts**
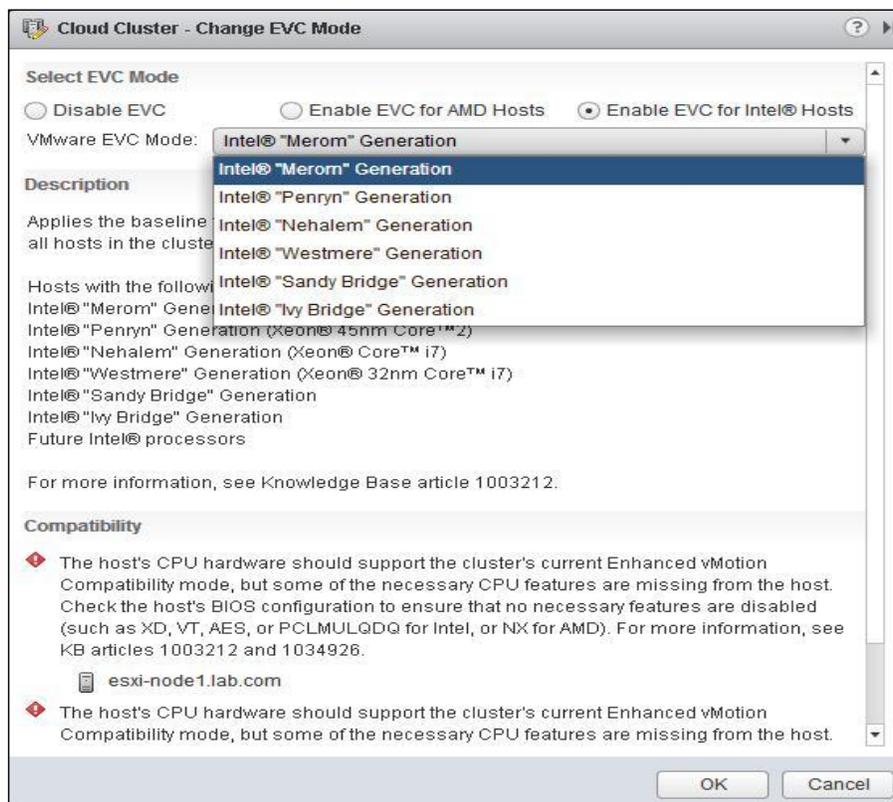
6. Choose one of the generations, whichever is applicable for your ESXi hosts, from the **VMware EVC Mode** dropdown.

7. Click on **OK** to apply the settings to the cluster.

The following steps have to be performed in order to disable DRS in vSphere cluster:

1. Browse to your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the vSphere DRS option.

4. Click on **Edit** to edit the DRS cluster settings.

5. Uncheck the **Turn ON** checkbox for the vSphere DRS.

6. Click on **OK** to apply the settings to the vSphere cluster.

How it works...

The primary function of VMware DRS is to automatically load-balance virtual machines that have imbalanced cluster using VMware vMotion. The initial placement of the virtual machine during power on is based on resource utilization of the cluster in order to properly balance the load in the cluster. DRS uses VMware vMotion for the migration of virtual machines from one ESXi host to another. So, vMotion is one of the major requirements for DRS to work:
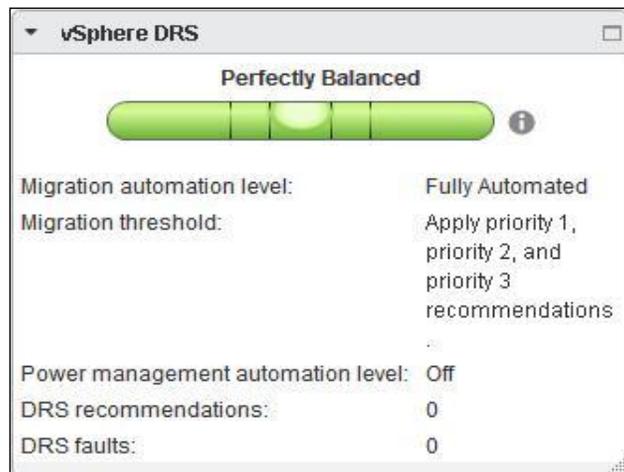
The following are the key features of VMware DRS:

▸ Automated intelligent resource allocation to the virtual machines in the cluster

▸ Resource isolation between resource pools

▸ Access control and delegation

▶ Different types of modes, either manual or automated, to initiate the DRS recommendation migrations automatically or only to provide the recommendations to administrator to best load balance the cluster

▶ DRS takes care of the initial placement of Virtual Machines during power-on by placing VMs on the right ESXi host based on current load of the cluster

▶ DRS allows a simplified way to perform ESXi host maintenance operations without downtime to the Virtual Machines running on the ESXi host by migrating the VMs to other hosts in the cluster using vMotion

▶ DRS affinity rules can be utilized to place the VMs together or keep them apart, and also to ensure that VM placement can be done only on the dedicated group of ESXi hosts based on the application and business requirements

▶ DRS along with distributed power management can perfectly handle the power management of ESXi hosts in the DPM-enabled cluster by migrating VMs out of hosts to other hosts in the same cluster and placing the ESXi hosts without virtual machines in standby mode to reduce the power consumption

There's more...

DRS rules can be used to control the virtual machine placement on ESXi hosts in the DRS clusters. There are two types of DRS rules:

▶ **VM-VM affinity rules**: This DRS rule can be used to specify the affinity or anti-affinity between individual virtual machines. With the VM-VM affinity rule, DRS ensures that it always tries to keep the virtual machines together in the same ESXi host during DRS migration. With VM-VM anti-affinity, DRS always ensures that the virtual machines are placed apart in different ESXi hosts during the DRS-initiated migrations.

▶ **VM-Host affinity rules**: This DRS rule can be used to specify affinity or anti-affinity between a group of virtual machines in the DRS cluster and a group of ESXi hosts in the cluster. With the VM-Host affinity rule, DRS ensures that the member of the selected virtual machine DRS group can or must run on the members of specific DRS host groups. The VM-Host anti-affinity rule can also be used to ensure that members of a certain virtual machine DRS group cannot run on the specific host DRS group.

VM-VM affinity rules

The VM-VM affinity rule can be used to specify whether the selected virtual machines should run on the same ESX/ESXi host or kept on separate hosts. This rule can be used to create an anti-affinity or affinity between selected virtual machines.

The following steps have to be performed in order to create VM-VM affinity rules:

1. Browse to your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **DRS Rules** option.

4. Click on **Add** to add the DRS rules.

5. Enter the name for your DRS rule.

6. Select the **Enable rule** checkbox to enable this affinity rule.

7. From the **Type** dropdown, select **Keep Virtual Machines Together**:
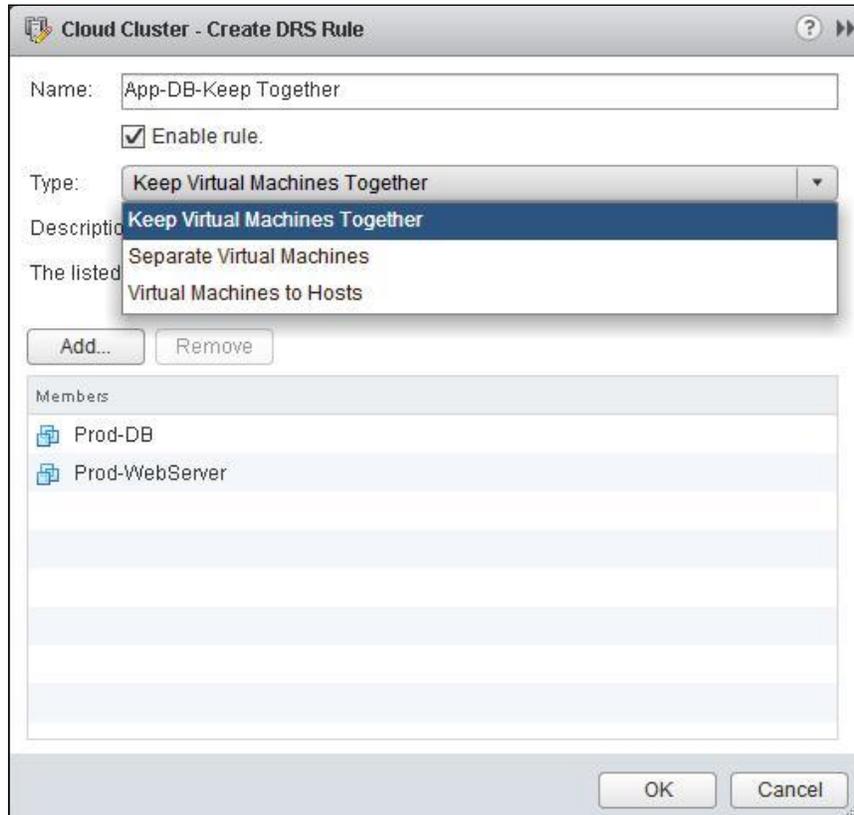
8. Click on **Add** to add the virtual machines in this rule and always keep the VMs together in the same ESXi host during DRS-initiated migrations.

9. Select the virtual machines that you want to keep together as a part of this rule.

10. Click on **OK** to create the VM-VM affinity rule.

The following steps have to be performed in order to create the VM-VM anti-affinity rule:

1. Browse to your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **DRS Rules** option.

4. Click on **Add** to add the DRS rules.

5. Enter the name for your DRS rule.

6. Select the **Enable rule** checkbox to enable this affinity rule.

7. From the **Type** dropdown, select **Separate Virtual Machines**.

8. Click on **Add** to add the virtual machines in this rule to keep the VMs on separate ESXi hosts during DRS-initiated migrations.

9. Select the virtual machines that you want to keep apart as a part of this rule.

10. Click on **OK** to create the VM-VM anti-affinity rule.

VM-Host affinity rules

To create a VM-Host affinity rule, VM DRS and Host DRS groups need to be created. Let's take a look at creating VM DRS, Host DRS, VM-Host affinity, and VM-Host anti-affinity rules.

The following steps have to be performed in order to create the VM DRS group:

1. Browse to your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **DRS Groups** option.

4. Click on **Add** to add the DRS groups.

5. Enter the name for your VM DRS group.

6. From the **Type** dropdown, select the **VM DRS** group:

7. Click on **Add** to add virtual machines as a part of this DRS group.

8. Select the virtual machines that you want as part of this VM DRS group.

9. Click on **OK** to create the VM DRS group.

The following steps have to be performed in order to create the Host DRS group:

1. Browse to your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **DRS Groups** option.

4. Click on **Add** to add the DRS groups.

5. Enter the name for your Host DRS group.

6. From the **Type** dropdown, select **Host DRS group**.

7. Click on **Add** to the ESXi hosts as a part of this DRS group.

8. Select the ESXi hosts that you want as part of this Host DRS group.

9. Click on **OK** to create the Host DRS group.

The following steps have to be performed in order to create VM-Host affinity and anti-affinity rules:

1. Browse towards your cluster in the vSphere Web Client.

2. Select your DRS cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **DRS Rules** option.

4. Click on **Add** to add the DRS rules.

5. Enter the name for your DRS rule.

6. Select the **Enable rule** checkbox to enable this affinity rule.

7. From the **Type** dropdown, select virtual machines to hosts.

8. Select the existing VM DRS group from the **VM Group** dropdown.

9. Select the existing Host DRS group from the **Host Group** dropdown:

10. Select one of the following rule types for this VM-Host rule:

    ❑ **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**

11. Click on **OK** to create the VM-Host affinity rule.

> To apply the DRS recommendation immediately based on the newly created affinity rules, manually run the DRS using the **Run DRS Now** option.

Implementing Distributed Power Management (DPM)

VMware **Distributed Power Management** (**DPM**) is a feature of VMware DRS. DPM is integrated with DRS to continuously monitor resource utilization. When the resource utilization of DRS cluster is less, VMware DPM consolidates workloads and powers off the unused ESXi hosts in the cluster to reduce the power consumption. When resource requirement of cluster is increased, DPM powers the host back on to handle the resource requirement of the cluster.

Getting ready

Connect to your vCenter Server via vSphere Web Client login.

How to do it...

We will take a look at a step-by-step procedure to configure the DPM cluster.

The following steps have to be performed in order to enable distributed power management in the DRS cluster:

1. Browse to your cluster in the vSphere Web Client.
2. Select your DRS cluster and click on the **Manage** tab.
3. Select the **Settings** tab and choose the **vSphere DRS** option.
4. Click on **Edit** to edit the DRS cluster settings.
5. Click on **Power Management** to expand the power management settings.
6. Select one the following **Automation Level** options for the DPM:
   - ❑ **Off**: With this automation level, vCenter server will not provide any power management recommendations
   - ❑ **Manual**: With this DPM automation level, vCenter server will only recommend evacuating an ESXi host's virtual machines and power off the ESXi host when the cluster's resource usage is low
   - ❑ **Automatic**: With this DPM automation level, vCenter will automatically execute power management recommendations
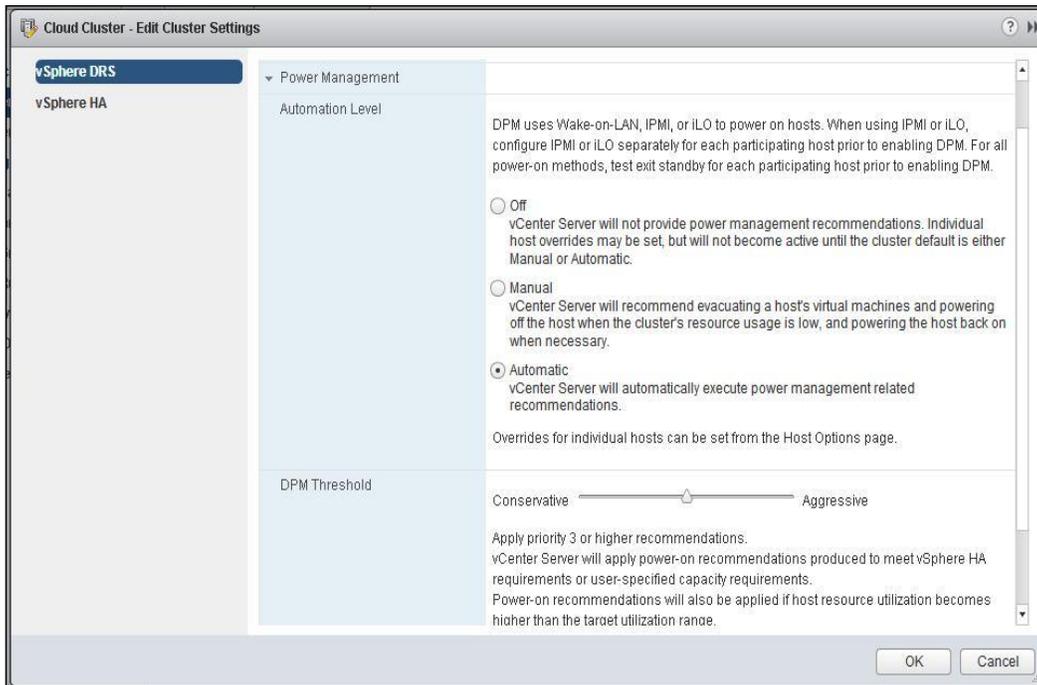
7. Set the **DPM Threshold** level to either **Conservative**, **Aggressive**, or in between that using the slider. Move the slider between 1 and 5 to adjust the migration threshold level.

8. Click on **OK** to enable the DPM on the vSphere cluster.

The following steps have to be performed in order to configure IPMI or iLO settings of the ESXi host for vSphere DPM:

1. Browse to your ESXi host in the vSphere Web Client.

2. Select the ESXi host and click on the **Manage** tab.

3. Select the **Settings** tab and choose the **Power Management** option under the **System** option.

4. Click on **Edit** to edit the power management settings of the ESXi host.

5. Enter **User name** and **Password** for the Baseboard Management Controller (BMC) of the ESXi host.

6. Enter **BMC IP address** of the ESXi host.

7. Enter the MAC address of the network adapter associated with the BMC of the ESXi host:

8. Click on **OK** to update the details.

How it works...

Distributed Power Management puts the ESXi host into powered-off state whenever there is low resource requirement in the cluster. DPM integrates with DRS to monitor the resource requirement and makes use of vMotion to migrate the VMs from one host to another to free up the ESXi host to power down. DPM uses the following power management protocols to bring the ESXi host out of standby mode:

▸ Intelligent Platform Management Interface (IPMI)

▸ Hewlett-Packard Integrated Lights-Out (iLO)

▸ Wake on LAN (WOL)

ESXi hosts powered off by VMware DPM will be marked as standby mode by vCenter server. ESXi hosts are always available to power on whenever resource requirement shoots up. VMware DPM uses **Wake on Lane** (**WOL**) to awake the ESXi hosts in powered-off state.

There's more...

DPM (Distributed Power Management) settings configured at cluster level applied to all the ESXi hosts are part of the DPM cluster. However, you can override the DPM cluster settings at the ESXi host level. Let's take a look at how to configure custom DPM automation levels for ESXi hosts.

The following steps have to be performed in order to configure custom host DPM automation levels:

1. Browse to your cluster in the vSphere Web Client.
2. Select your DRS cluster and click on the **Manage** tab.
3. Select the **Settings** tab and choose **Host Options**.
4. Select the ESXi host from the list to edit the DPM automation level.
5. Click on **Edit**.
6. In the **Edit Host** option, select one of the following automation levels from the **Power Management** dropdown:
   - **Default** (which is taken from cluster settings)
   - **Disabled**
   - **Automatic**
   - **Manual**
7. Click on **OK** to apply the settings.

Implementing High Availability (HA)

vSphere HA (**High Availability**) provides high availability for virtual machines in case of ESXi host failures in the cluster. ESXi hosts in the HA cluster are monitored, and if the ESXi host failure occurs, virtual machines running on the failed host will be restarted on the alternate hosts in the HA cluster.

Getting ready

Connect to your vCenter server via vSphere Web Client login and browse to your cluster in the vSphere Web Client.

How to do it...

vSphere HA provides high availability for virtual machines in case of ESXi host failures in the cluster. Enabling vSphere HA is possible during cluster creation or after creating the cluster. We will look into a detailed step-by-step procedure to enable vSphere HA and HA settings on the vSphere cluster.

The following steps have to be performed in order to enable High Availability in vSphere cluster:

1. Select your existing cluster and click on the **Manage** tab.
2. Select the **Settings** tab and choose vSphere HA.
3. Click on **Edit** to enable the HA on the cluster.
4. Select the **Turn ON vSphere HA** checkbox.
5. Click on **OK** to enable the HA on the cluster:

6. Once HA is enabled on the cluster, all the ESXi hosts in the cluster will be automatically reconfigured by the HA.
7. To reconfigure the host for HA, right-click on the ESXi host and select **All vCenter Actions**.
8. Select **Reconfigure for vSphere HA**. Once it is done, HA cluster will initiate the HA agent installation on the ESXi host to prepare the host for HA cluster.

The following steps have to be performed in order to edit HA cluster settings:

1. Browse to your cluster in the vSphere Web Client.
2. Select your HA cluster and click on the **Manage** tab.
3. Select the **Settings** tab and choose vSphere HA.
4. Click on **Edit** to edit the HA cluster settings.
5. Edit the following HA cluster settings:
    - ❑ **Host Monitoring**
    - ❑ **Admission Control**
    - ❑ **VM Monitoring**
    - ❑ **Datastore Heartbeating**
    - ❑ **Advanced options**
6. Click on **OK** to apply the settings.

Configuring host monitoring

The Host Monitoring feature allows the vSphere HA master ESXi host to react to the ESXi host failures, ESXi host management network isolation, and virtual machine failures. When the Host Monitoring option is enabled, each ESXi host in the cluster is checked to ensure it is up and running. If ESXi host failure occurs in the cluster, virtual machines are restarted on another running ESXi host as a part of HA. If you are performing maintenance activity at network level, it may cause the ESXi host to trigger host isolation responses. In that case, you can disable the Host Monitoring option for your HA cluster to avoid unwanted restart of virtual machines in the HA cluster. Once network change is completed, you can re-enable the **Host Monitoring** option for your cluster. The following steps have to be performed in order to configure host monitoring:

1. Browse to your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose vSphere HA.

4. Click on **Edit** to edit the HA cluster settings.

5. Select the **Enable Host Monitoring** checkbox to enable host monitoring for the HA cluster.

6. Click on **Host Monitoring** to expand its configuration options.

7. Select the checkbox to enable **Host Monitoring** for your HA cluster.

8. Configure one of the VM restart priorities under virtual machine options from the dropdown:

   - **Disabled**
   - **High**
   - **Medium (Default)**
   - **Low**

   The VM restart priority determines how vSphere HA should react to ESXi host failures when restarting the virtual machines. This option, configured at cluster level, can be overridden for individual virtual machines on the **VM Overrides** page. Higher priority virtual machines will be starting first during the HA-initiated restarts followed by medium priority and low priority virtual machines restart. If you select disabled for any virtual machine, vSphere HA will be disabled for the virtual machine and it will not be restarted on the other ESXi host in case the parent ESXi host fails.

9. Select one of the following **Host isolation response** options under **Virtual Machine Options**:

   - **Leave powered on**
   - **Power off then failover**
   - **Shutdown then failover**

The ESXi host declares it as isolated when it is unable to communicate with the HA agents running on the other ESXi hosts in the cluster; also, it is unable to reach to its isolation addresses via ping. The ESXi host performs its configured isolation response action when it is isolated. The host monitoring options need to be enabled to configure the host isolation response. This option configured at the cluster level can be overridden for individual virtual machines on the VM Overrides page. VMware Tools need to be installed on the guest operating system to perform the shutdown of a virtual machine as a part of the host isolation option.
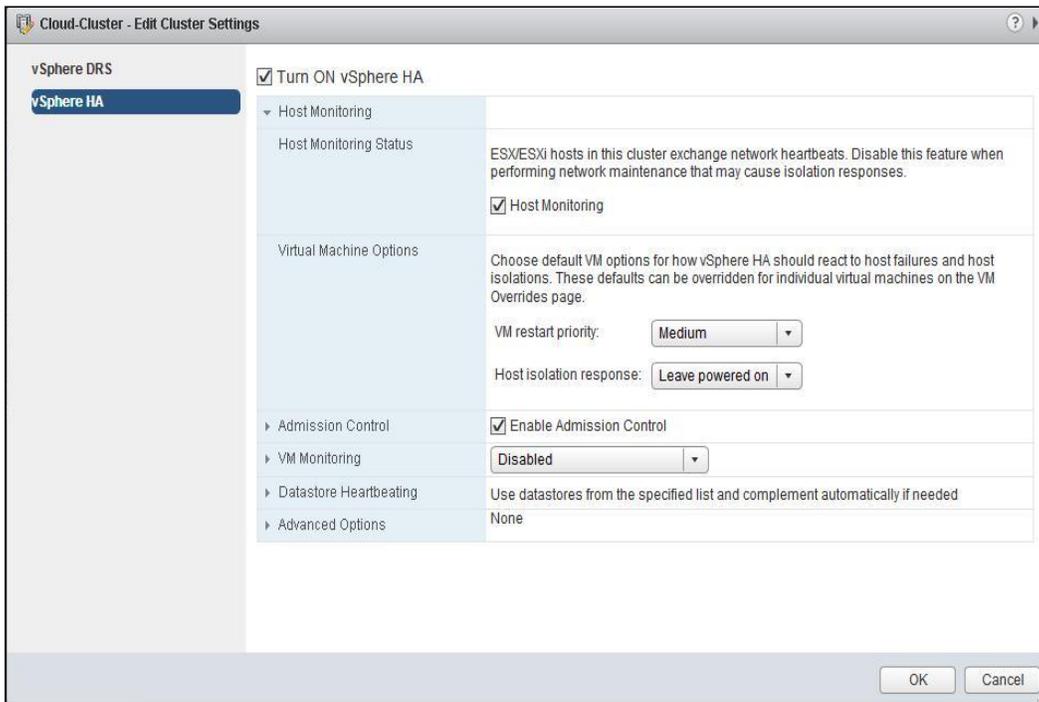
10. Click on **OK** to apply the settings.

Configuring HA admission control

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the proportion of ensured host failures increases the availability constraints and capacity reserved in the cluster. The following steps have to be performed in order to configure HA admission control:

1. Browse towards your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose vSphere HA.

4. Click on **Edit** to edit the HA cluster settings.

5. Click on **Admission Control** to expand its configuration options. Choose one of the Admission Control policies from the following available options:

   ❑ **Define failover capacity by static number of hosts**: With this admission control policy, you can choose the maximum number of hosts for reserved failover capacity. This policy ensures the maximum number of the host's failures that you can recover from or guarantee to for the failover of resources in case of host failures. With this admission control policy, you can choose one of the slot size policies; either choose cover all powered-on virtual machines or a fixed slot size.

   ❑ **Define failover capacity by reserving a percentage of the cluster resources**: With this admission control policy, you can define the percentage of the cluster's Memory and CPU resources to reserve for a spare capacity to support failover incase of ESXi host failures in the cluster. You can choose a certain percentage for **Reserved failover capacity** for CPU and **Reserved failover capacity** for memory to configure this admission control policy.

   ❑ **Use dedicated failover hosts**: Select the ESXi hosts to use as dedicated failover hosts for HA cluster. This host will not be used to run virtual machines in the cluster. If the dedicated failover hosts do not have enough resources to satisfy the failover capacity, failover will happen to other ESXi hosts in the cluster. Click on the **+** symbol to add the dedicated failover host:
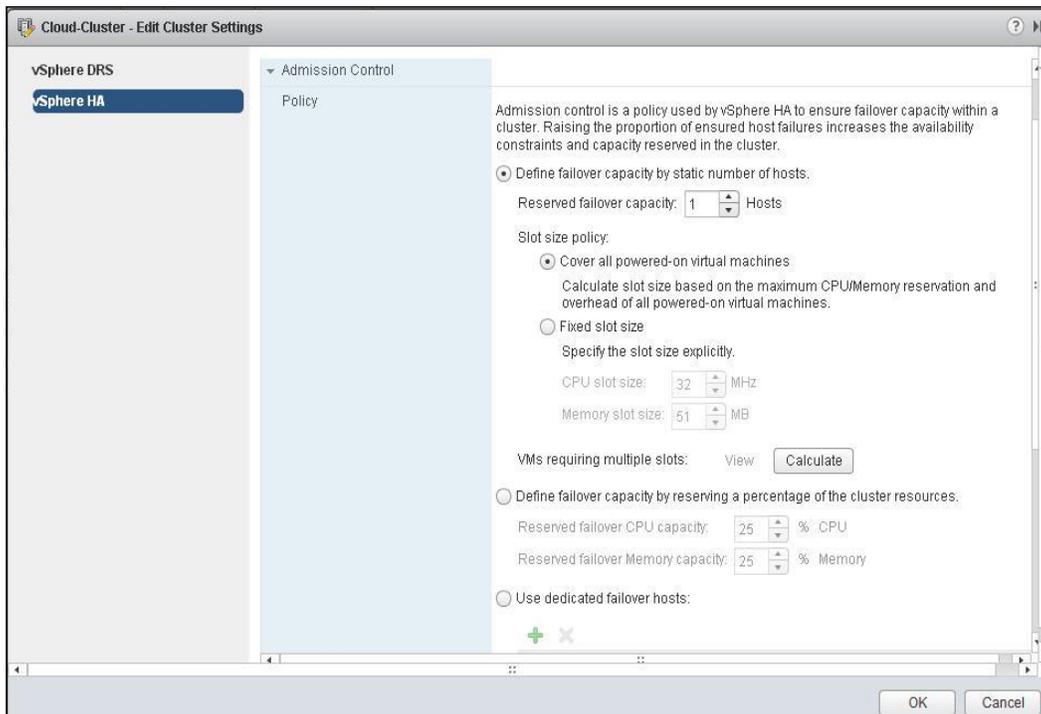
6. Click on **OK** to apply the settings.

Configuring VM monitoring

VM monitoring restarts individual virtual machines if their VMware Tools heartbeats are not received within a configured time; application monitoring restarts the individual virtual machines if their VMware Tools application heartbeats are not received within a configured time. The following steps have to be performed in order to configure VM monitoring:

1. Browse to your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose vSphere HA.

4. Click on **Edit** to edit the HA cluster settings.

5. Click on VM monitoring to expand its configuration options. Choose one of the options for VM monitoring status from the dropdown:

   ❑ **Disabled**: Select this option to disable the VM Monitoring. It is disabled by default.

   ❑ **VM Monitoring Only**: Select this option to monitor the Virtual Machines and restart the Virtual Machines if heartbeats are not received within a configured time.

   ❑ **VM and Application Monitoring**: Select this option to monitor the application running on top of the guest operating system along with virtual machine monitoring.

6. Adjust the **Monitoring Sensitivity** option by moving the slider between **Low** and **High**. Choose one of the following monitoring sensitivity values from the slider:

   ❑ **Low**: vSphere HA will restart the virtual machine if the heartbeat between the host and the virtual machine has not been received within a 2-minute interval. vSphere HA restarts the virtual machine after each of the first three failures every seven days.

   ❑ **Medium**: vSphere HA will restart the virtual machine if the heartbeat between the host and the virtual machine has not been received within a 60-second interval. vSphere HA restarts the virtual machine after each of the first three failures every 24 hours.

   ❑ **High**: vSphere HA will restart the virtual machine if the heartbeat between the host and the virtual machine has not been received within a 30-second interval. vSphere HA restarts the virtual machine after each of the first three failures every hour.

❑ **Custom**: You can configure custom value for **Failure interval**, **Minimum uptime**, **Maximum per-VM resets**, and **Maximum resets time window** value:
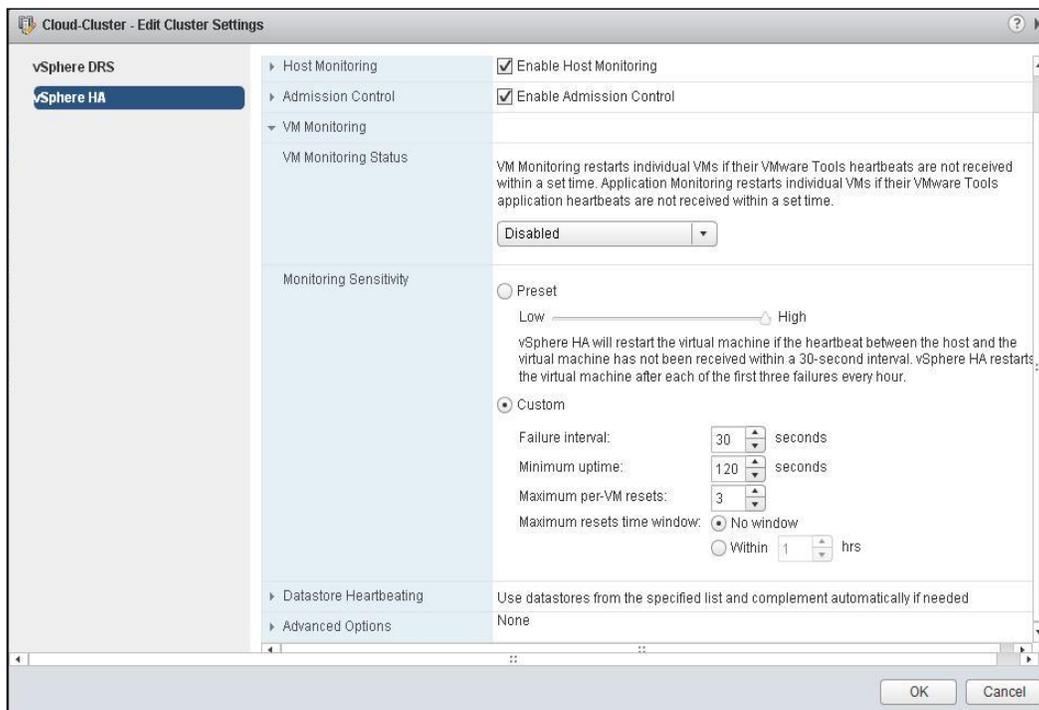
7. Click on **OK** to apply the settings.

Configuring datastore heartbeating

vSphere HA uses datastores to monitor hosts and virtual machines when management network has failed. Datastore heart beating is used by vSphere HA to distinguish between ESXi host failure and hosts with network isolation. Datastore heartbeating allows vSphere HA cluster to monitor hosts when a management network isolation occurs; this helps to continue to respond to failures that occur.

1. Browse towards your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose vSphere HA.

4. Click on **Edit** to edit the HA cluster settings.

5. Click on **Datastore Heartbeating** to expand its configuration options. Choose one of the following heartbeat datastore selection policies:

❑ Automatically select datastores accessible from the host

❑ Use datastore only from the specified list

❑ Use datastore from the specified list and complement automatically if needed
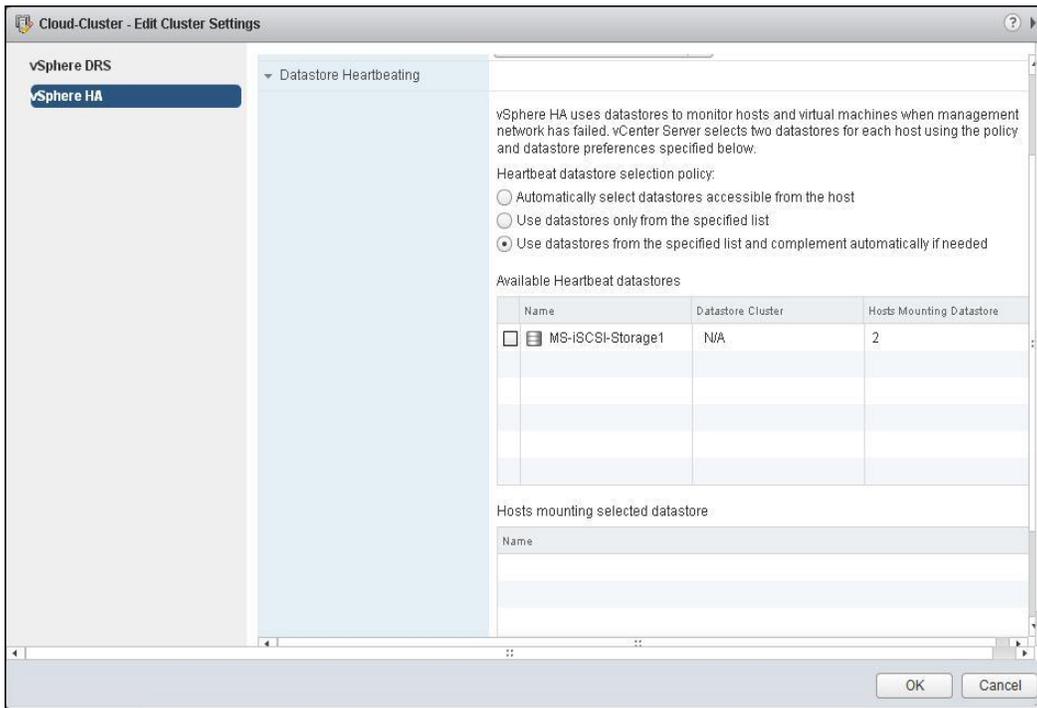
6. Click on **OK** to apply the settings.

Configuring HA advanced options

You can customize the default behavior of the HA cluster by adding advanced options of the HA.

1. Browse towards your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Manage** tab.

3. Select the **Settings** tab and choose vSphere HA.

4. Click on **Edit** to edit the HA cluster settings.

5. Click on **Advanced Options** to expand its configuration parameters.

6. Click on **Add** to add advanced HA options.

7. Enter the **Option** and **Value** options:
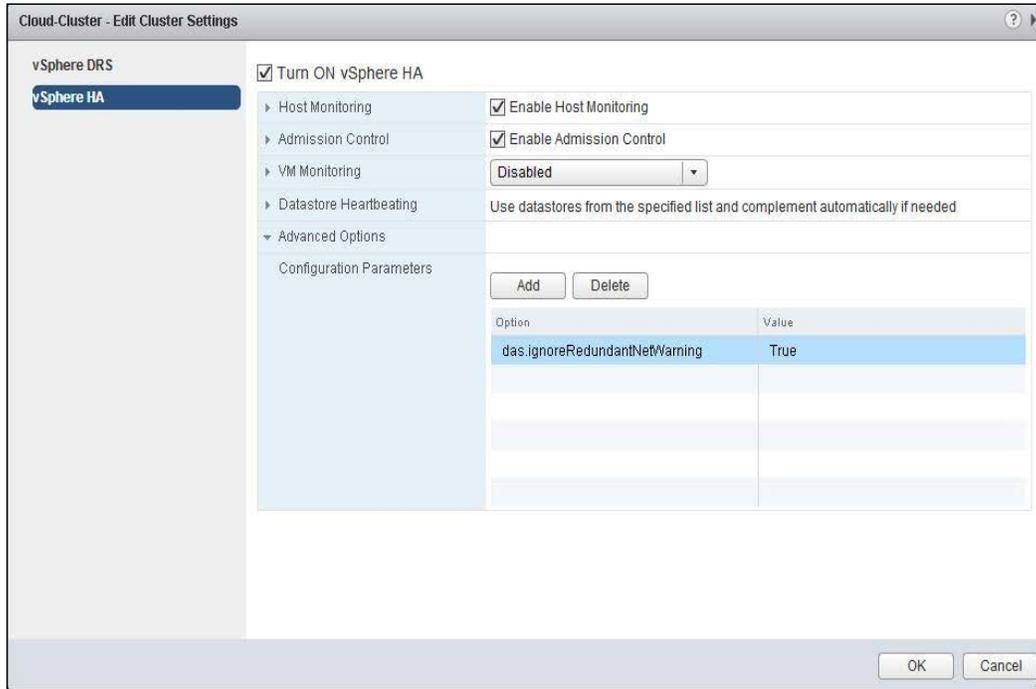
8. Click on **OK** to apply the settings.

> Please refer the following link to know the various available HA advanced options:
>
> `http://kb.vmware.com/selfservice/microsites/search.`
> `do?language=en_US&cmd=displayKC&externalId=2033250`

How it works...

vSphere HA provides high availability for the virtual machines during ESXi hosts failures. The first ESXi host added in the HA cluster will be automatically elected as the master host in the cluster and the remaining host will act as a slave. The master ESXi host communicates with the vCenter Server and actively monitors the state of the slave hosts and all protected virtual machines. Different types of ESXi host failures are the failures occurring due to hardware issues; another failure is in the network partition or when network becomes isolated. To handle these failures efficiently, vSphere HA has been introduced with datastore heartbeating from vSphere 5.0. The master ESXi host uses network and datastore heartbeating to efficiently determine the failure type.

When ESXi hosts are added to vSphere HA cluster, HA agent will be installed to the host and configured to communicate with other host agents in the same cluster. When HA is enabled on the existing cluster, all the active ESXi hosts will participate in an election to choose the cluster's master host. A host which holds the maximum number of datastores will be elected as the master and the remaining hosts will act as slave hosts. Only one host in the cluster will be elected as master and all remaining hosts will acts as slaves. When a master ESXi host fails or is taken out for maintenance, a new election process will take place to elect the new master host for the cluster.

The responsibilities of the master host are as follows:

- ▸ The master host will manage the list of clustered hosts and protected virtual machines in the cluster.

- ▸ The master hosts will actively monitor the state of the slave hosts in the cluster. If the slave host in the cluster fails or is unreachable, the master host will restart the virtual machines on the failed host. A similar process will be followed for the other hosts in the cluster.

- ▸ The master host also monitors the state of the virtual machine using its monitoring feature. It will restart the failed virtual machine to fix the issue.

- ▸ The master host will report the cluster health state to the vCenter server.

- ▸ The master host receives the reporting status updates and runtime stats from the slave hosts.

The master host monitors the health of slave hosts in the cluster by exchanging network heartbeats every second. If the master host stops receiving the heartbeat from the slave host, it checks for the exchange of datastore heartbeating. The master host also checks whether the slave host responds to ICMP pigs sent to its management IP address. If the master host is unable to communicate to the slave host with the use of the HA agent, the slave host does not respond via ICMP pings; if the agent is not receiving the heartbeat, then ESXi host will be considered as failed. The virtual machines in the failed host will restart on the alternate hosts in the cluster. In case the slave host is exchanging the datastore heartbeats, the master host assumes that it is network partitioned or network isolated and continues to monitor the host and its virtual machine.

There's more...

Let's take a look at how to configure virtual machines' override options.

Configuring virtual machine override options

The following steps have to be performed in order to configure virtual machine override options:

1. Browse to your cluster in the vSphere Web Client.
2. Select your HA cluster and click on the **Manage** tab.
3. Click on **Settings** and choose **VM Overrides**.
4. Click on **Add** to configure the VM override settings.
5. Click on the **+** symbol to add the virtual machines.
6. Select the checkbox against the virtual machines to be added to configure the VM override options.
7. By default, all the virtual machines in the HA clusters use the cluster settings. Configure the HA options to override the cluster settings:
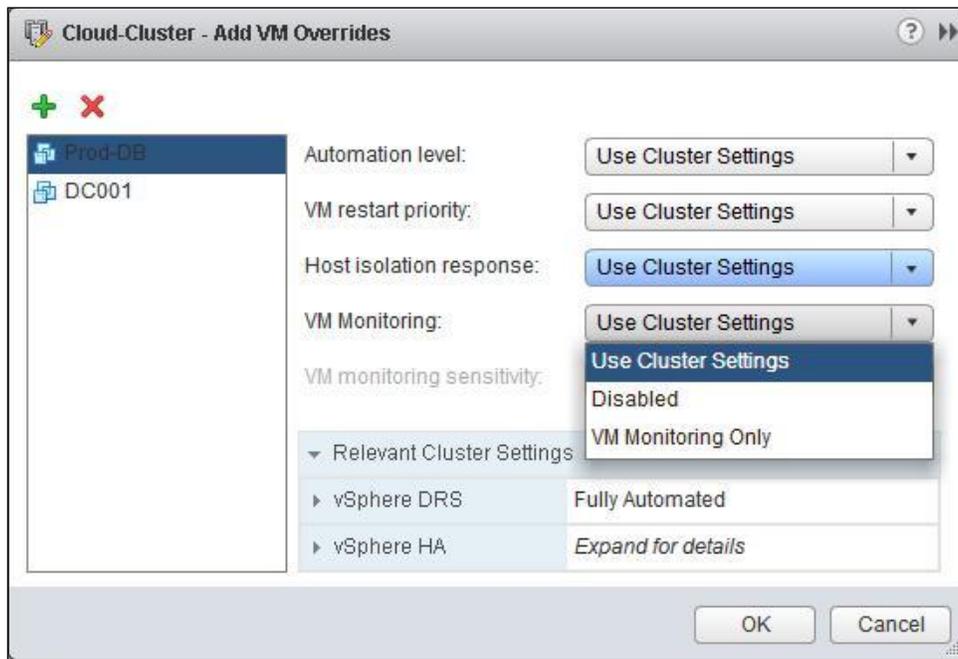
8. Click on **OK** to apply the settings.

The following steps have to be performed in order to monitor HA cluster configuration issues:

1. Browse to your cluster in the vSphere Web Client.

2. Select your HA cluster and click on the **Monitor** tab.

3. Select the **vSphere HA** tab and choose **Configuration Issues**.

4. It will display the configuration issues for the ESXi hosts in the HA cluster. You can manually fix each of these issues:
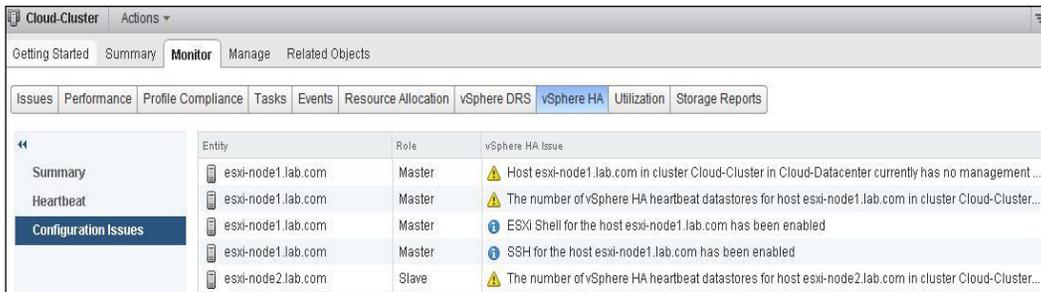
Implementing Storage Dynamic Resource Scheduling (SDRS)

With vSphere 5.0, a new feature called **Storage Dynamic Resource Scheduling** (**SDRS**) provides smart placement and load balancing of virtual machine disks based on space capacity and I/O of the datastore. Storage DRS provides effective initial placement of virtual machine disks on the datastore with least I/O latency and more free disk space in the storage cluster. This SDRS feature will only be available with the Enterprise plus license of vSphere.

Getting ready

Connect to your vCenter server via vSphere Web Client login.

How to do it...

SDRS allows you to manage the datastore cluster. SDRS provides recommendation for placement of Virtual Machine disks and migration to balance the I/O and space allocation across the datastores, which is a part of the datastore cluster.

The following steps have to be performed in order to create an SDRS:

1. Browse to the datacenter in the vSphere Web Client.

2. Right-click on **Datacenter** and select **New Datastore Cluster**.

3. Enter the name of your datastore cluster.

4. Select the **Turn ON Storage DRS** checkbox. It is selected by default.

5. Select either of the following storage DRS Automation levels:

   ❑ **No Automation (Manual Mode)**: With this automation level, vCenter Server will make migration recommendations for Virtual Machine storage, but will not perform automatic migrations

   ❑ **Fully Automated**: With this automation level, files will be migrated automatically to optimize resource usage:
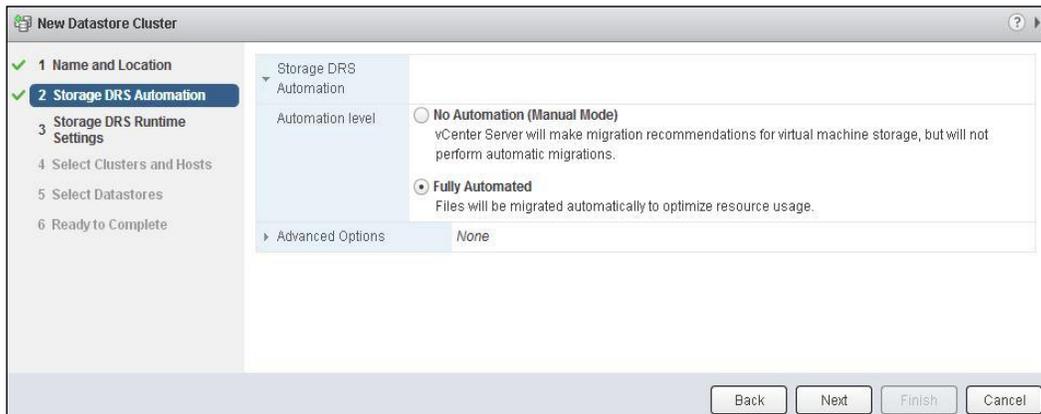
6. Configure the following options under **Storage DRS Runtime Settings**:

   ❑ **I/O Metric Inclusion**: This option is selected if you want I/O metrics considered as a part of any SDRS recommendation or automated migration in this datastore cluster. Select the **Enable I/O metric** checkbox for SDRS recommendations. I/O load functionality is only available when all hosts connected to the datastore in this datastore cluster are of Version 5.0 or later.

❑ **Storage DRS Thresholds**: This option governs when storage DRS performs or recommends migrations (based on the selected automation level). Utilized space dictates the minimum level of consumed space that is the threshold for action. I/O latency dictates the minimum I/O latency below which I/O load balancing moves are not considered. Adjust **Utilized Space** and **I/O Latency** using the slider:
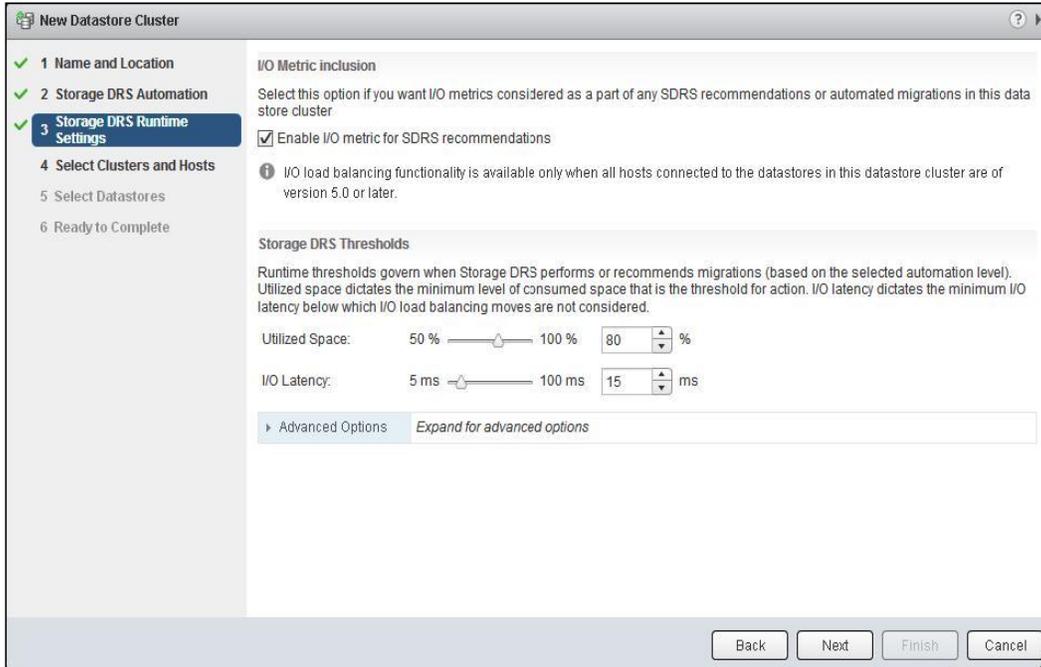
7. Select **Clusters and Hosts**.

8. Select the datastores to be added as a part of this datastore cluster:
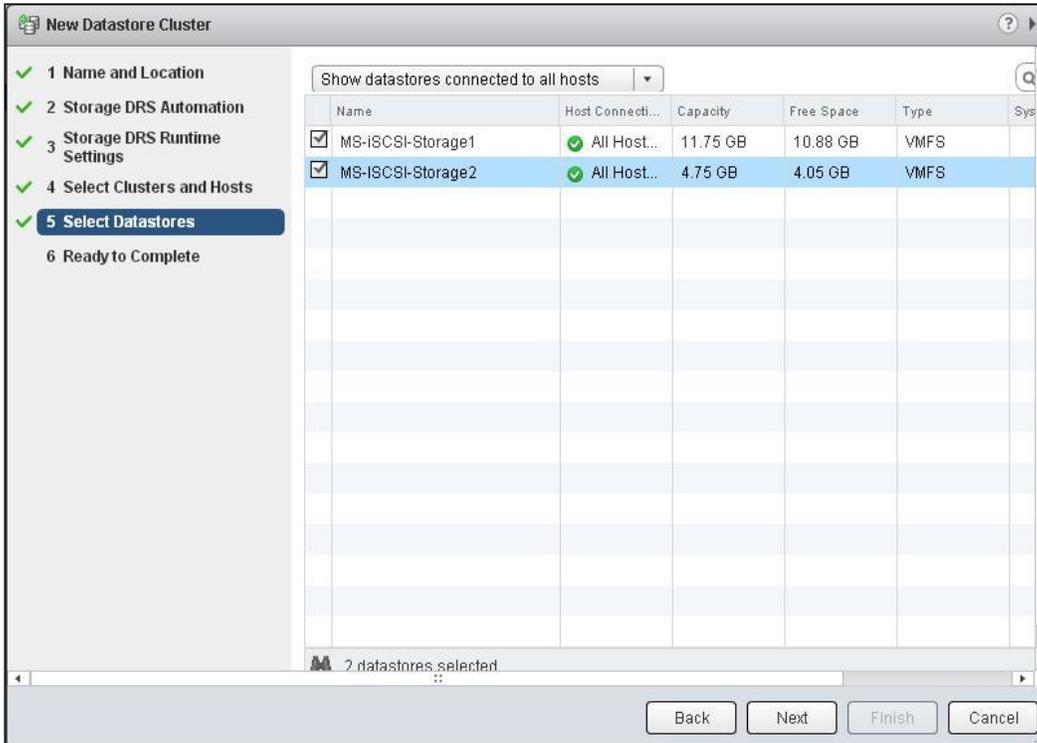
9. Review the selected options and click on **Finish** to create the datastore cluster.

The following steps have to be performed in order to configure storage DRS advanced options:

1. Browse towards your storage DRS cluster in the vSphere Web Client.

2. Click on the **Manage** tab and select **Settings**.

3. Select **Storage DRS** and click on **Edit**.

4. Click on **Advanced Options** to expand its configuration options.

5. Configure VM Default affinity. Select the **Keep VMDKs together by default** checkbox. This setting is used to specify whether each virtual machine in the datastore cluster should have its virtual disks on the same datastore by default.

6. Enter the number of minutes, hours or days to check the imbalance of storage DRS cluster by configuring the **Check Imbalance every** option.

7. Select the **I/O imbalance Threshold** option by adjusting the slider between **Aggressive** and **Conservative**.

8. Configure the **Minimum Space utilization Difference** option using the slider.

9. You can add additional configuration parameters to control the default behavior of the storage DRS cluster. To add additional **Configuration Parameters**, click on **Add** and enter **Option** and **Value**:
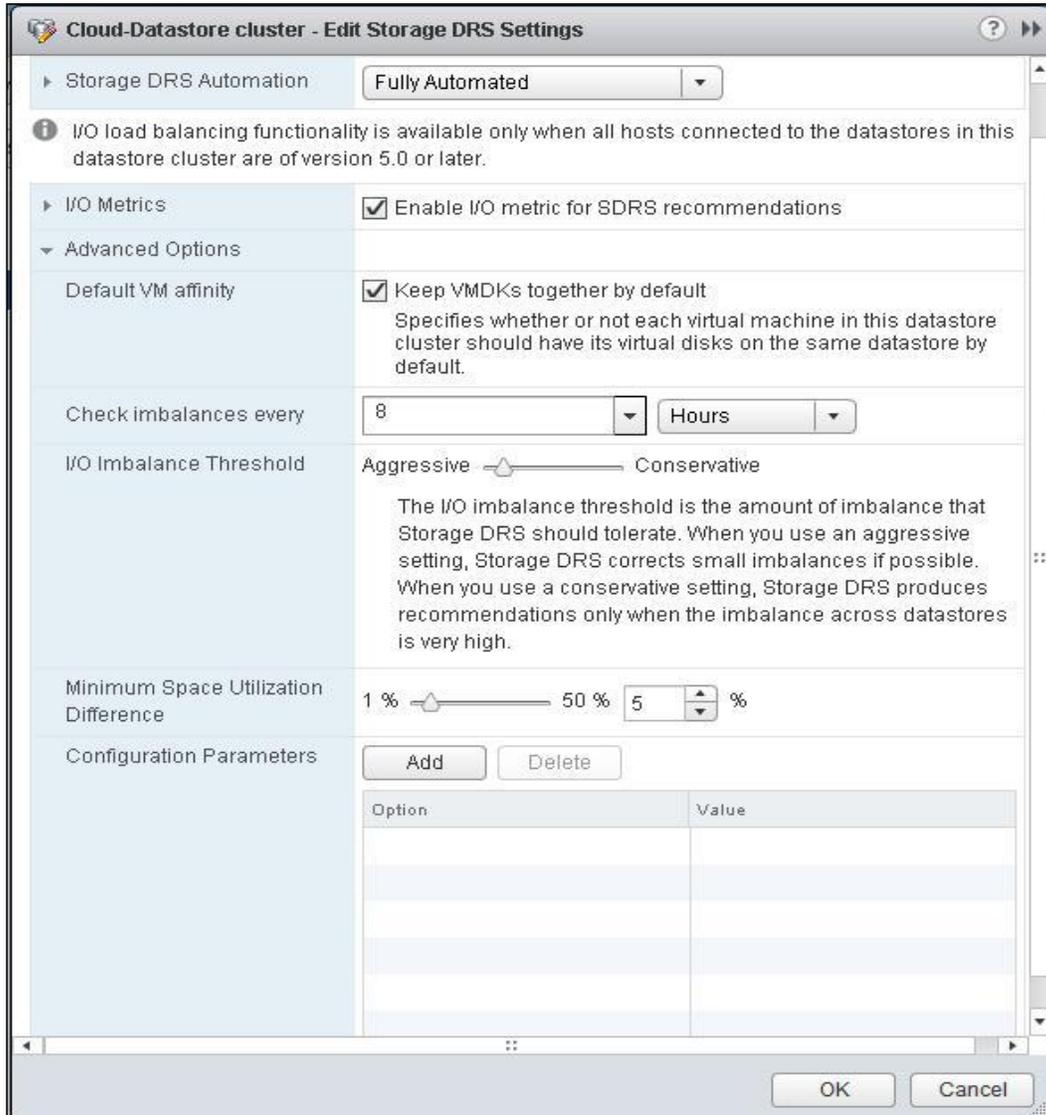
10. Click on **OK** to apply the settings to the storage DRS cluster.

The following steps have to be performed in order to place Datastore in storage DRS maintenance mode:

1. Browse towards your storage DRS cluster in the vSphere Web Client.
2. Select **Datastore** in the storage DRS cluster to place it in maintenance mode.
3. Right-click on the **Datastore** option and select **All vCenter Actions**.
4. Select **Enter Storage DRS Maintenance Mode**. Virtual machines in the particular datastore will be stored to other datastores in the SDRS cluster by using vMotion.
5. Once maintenance on the datastore is completed, you can exit from the maintenance mode by selecting **Exit Storage DRS Maintenance Mode**.

The following steps have to be performed in order to configure virtual machine override options:

1. Browse towards your storage DRS cluster in the vSphere Web Client.
2. Click on the **Manage** tab and select **Settings**.
3. Select **VM Overrides** and click on **Add**.
4. Click on the **+** symbol to add the virtual machine to override the cluster settings.
5. Select the virtual machines from the list and click on **OK**.
6. Configure the following **Storage DRS Automation Level** options for the selected virtual machine from the dropdown:
   - **Fully Automated**
   - **Manual**
   - **Disabled**
7. Select **Yes** or **No** from the dropdown to override the **Keep VMDKs together** option:
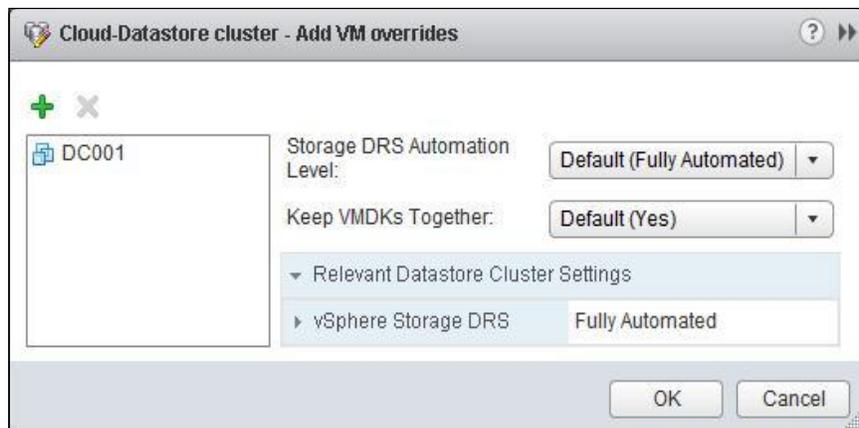
8. Click on **OK** to apply the virtual machine override settings.

Disabling storage DRS

The following steps have to be performed to disable storage DRS:

1. Browse towards your storage DRS cluster in the vSphere Web Client.
2. Click on the **Manage** tab and select **Settings**.
3. Select the **Storage DRS** option and click on **Edit**.
4. Uncheck the tick mark for the **Turn on vSphere Storage DRS** option.
5. Click on **OK** to disable the **Storage DRS** option.

How it works...

Datastore cluster is an aggregate of group of datastore. You can enable the SDRS on a similar datastore cluster to enable DRS in the vSphere cluster. SDRS will provide smart placement and load balancing of virtual machine disks based on space capacity and I/O of the datastore in the datastore cluster. SDRS will try to move virtual machines to other datastores using **storage vMotion** to load-balance the VM between datastores in the SDRS cluster. When the automation level of the cluster is set to **Automatic**, SDRS uses storage vMotion to automatically migrate virtual machines to different datastores in the datastore cluster, only if the configured threshold value is exceeded. The vSphere administrator will be given the recommendations to balance the space usage of a datastore if the cluster automation level is set to **Manual**.

There's more...

Just like DRS, SDRS also has affinity rules. SDRS affinity rules can be used to configure the placement of virtual machines on the ESXi hosts within a vSphere cluster.

Storage DRS affinity rules

There are two types of storage DRS affinity rules: VMDK anti-affinity rule and VM anti-affinity rule. Let's take a look at the step-by-step procedure to configure each type of affinity rule.

The following steps have to be performed in order to configure VMDK anti-affinity rules:

1. VMDK anti-affinity rules ensure that selected virtual disks of the virtual machine should be placed on different datastores.
2. Browse to your storage DRS cluster in the vSphere Web Client.
3. Click on the **Manage** tab and select **Settings**.
4. Select the **Rules** option and click on **Add**.
5. Select the **Enable Rule** checkbox.
6. Enter the name for your VMDK affinity rule name.
7. Select VMDK anti-affinity from the **Type** dropdown.

8. Click on **Browse** to add the virtual machine to configure for VMDK anti-affinity rule.

9. Select the **Virtual machine** type and click on **OK**.

10. Select the **Virtual Disks** type of the virtual machine to be placed on a separate datastore:
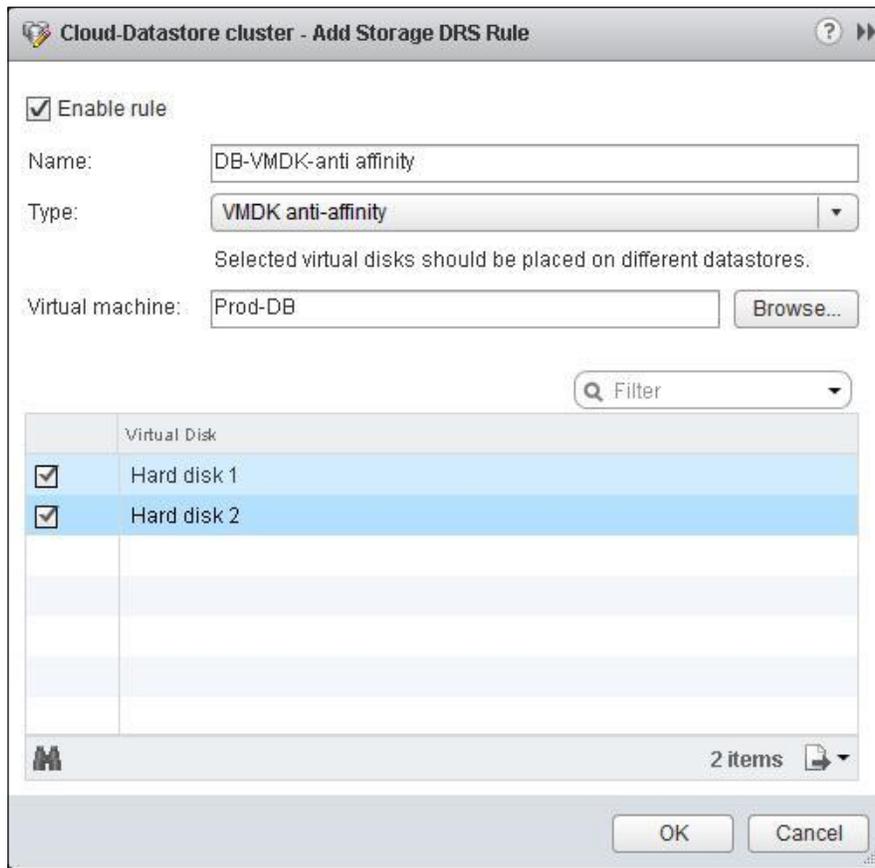
11. Click on **OK** to apply the rule.

Configuring VM anti-affinity rules

VM anti-affinity rules ensure that all the virtual disks of selected virtual machines should be placed on different datastores. Let's take a look at a step-by-step procedure to create VM anti-affinity rules:

1. Browse towards your storage DRS cluster in the vSphere Web Client.

2. Click on the **Manage** tab and select **Settings**.

3. Select the **Rules** option and click on **Add**.

4. Select the **Enable Rule** checkbox.

5. Enter the name for your VM affinity rule name.

6. Select VM anti-affinity from the **Type** dropdown.

7. Click on **Add** to add the virtual machine to configure for VM anti-affinity rule.

8. Select the **Virtual Machine** type and click on **OK**.
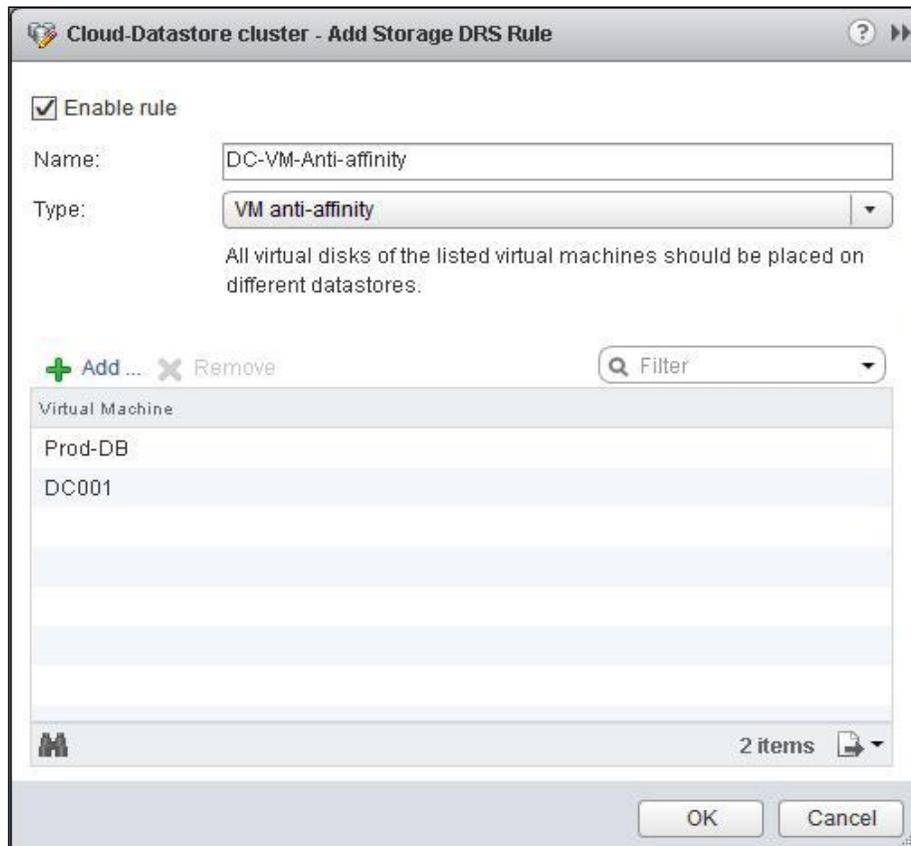
9. Click on **OK** to apply the rule.

6
Managing Virtual Machines

In this chapter, we will cover the following:

- ▸ Deploying virtual machines
- ▸ Installing and customizing a guest operating systems
- ▸ Configuring the ESXi host and VM for Fault Tolerance
- ▸ Configuring virtual machine's hardware
- ▸ Configuring virtual machine options
- ▸ Creating snapshots, templates, and clones

Introduction

A virtual machine is the collection of different sets of specification and configuration files. Virtual machines are similar to the physical computer that runs the operating system and applications. VMware virtual machine shares the resources such as processor and memory from the ESX/ESXi hosts. A virtual machine can be deployed or run on an isolated ESX/ESXi host and also on the ESXi hosts that is managed by the vCenter Server. virtual machines have an operating system, virtual resources, virtual hardware, and VMware tools. Virtual machines can be managed in the same way as the physical servers.

Deploying virtual machines

A virtual machine can be deployed in multiple ways, such as creating a new virtual machine, deploying a virtual machine from the template, or clone an existing virtual machine. Creating a new virtual machine involves a lot of manual tasks such as creating a new virtual machine with memory, CPU, and disk configuration followed by guest OS installation, configuration, and application installation. It will be a bit of a time consuming task as compared to other deployment methods. Deploying a virtual machine from the template is suitable for mass deployment for quicker provisioning of virtual machine. Templates are also referred to as a golden image, which is nothing but a preconfigured virtual machine with guest OS and application. New virtual machine can be easily and quickly deployed from templates. Cloning an existing virtual machine creates an exact copy of the virtual machine. It can be useful if you want an identical virtual machine, to create a same setup to test the development activities in the test environment.

Getting ready

Connect to your VMware vCenter Server using vSphere Web Client and browse to your cluster or ESXi host in the vSphere Web Client.

How to do it...

We'll see a step-by-step procedure of different methods to deploy a virtual machine using the vSphere Web Client.
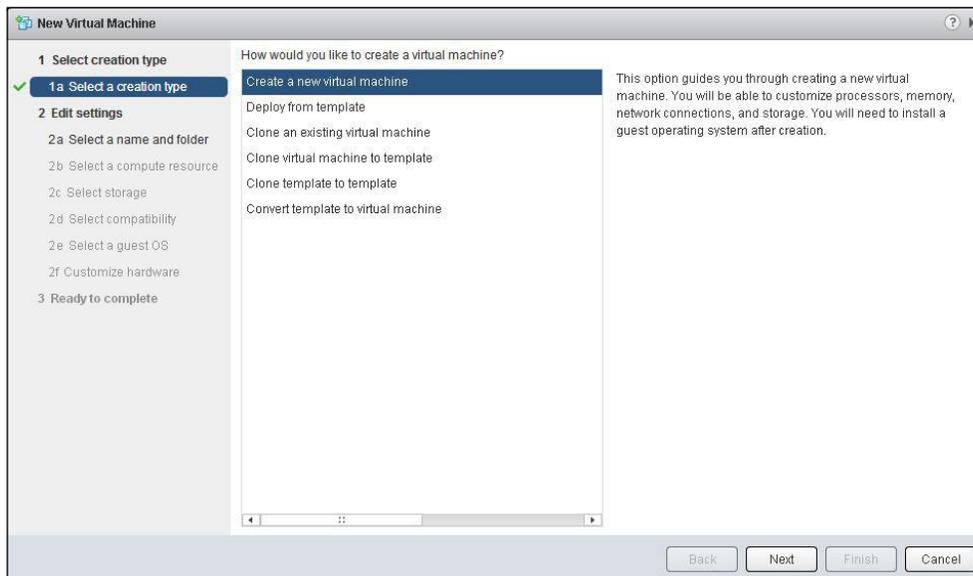
The steps for creating a new virtual machine are as follows. This option allows you to create a new virtual machine and also you will be able to customize the virtual hardware such as processor, memory, network connection, and storage.

1. Right-click on the cluster or the ESXi host and select **New virtual machine**.
2. Select the **Create a new virtual machine** option under the **Select a creation type** option.
3. Enter a name for your virtual machine.
4. Select a **datacenter** or **VM folder** location for the new virtual machine.
5. Select a computing resource such as **cluster**, **host**, **vApp**, or **resource pool** to run this virtual machine.
6. Select the **Datastore** to store the virtual machine.
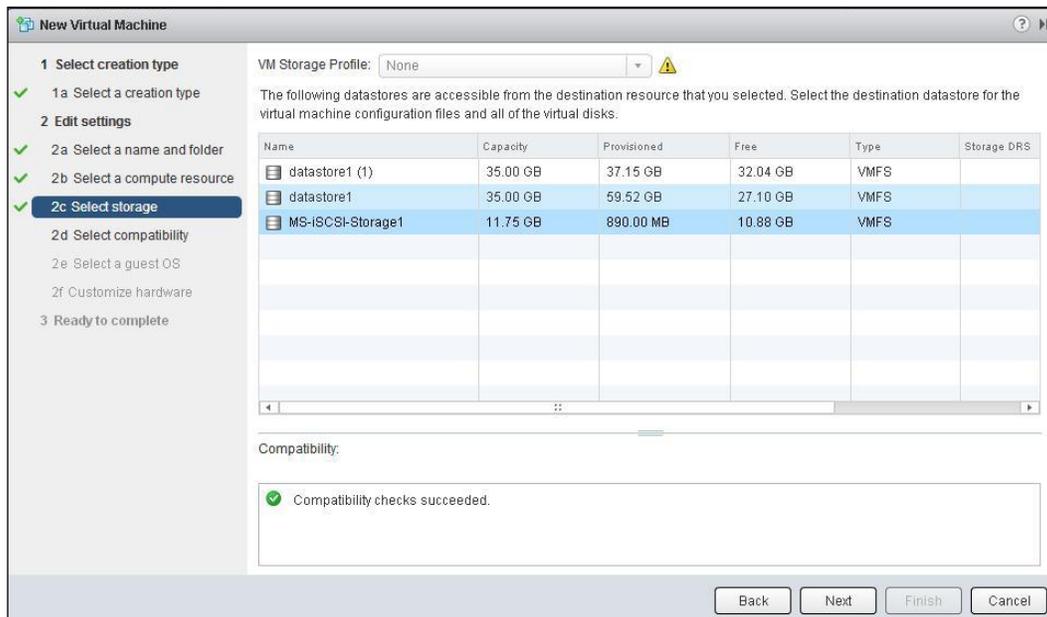
7. Select one of the following compatibilities for the virtual machine from the drop-down menu:

   ❑ **ESX 3.x and later**: This virtual machine (VM Version 4) is also compatible with ESXi 4.X, ESXi 5.0, and ESXi 5.1. Some of the hardware features of the virtual machine are unavailable with this option.
   ❑ **ESX 4.x and later**: This virtual machine (VM Version 7) is also compatible with ESXi 5.0 and ESXi 5.1. Some of the hardware features of the virtual machine are unavailable with this option.

❑ **ESX 5.0 and later**: This virtual machine (VM Version 8) is also compatible with ESXi 5.1. Some of the hardware features of the Virtual Machine are unavailable with this option.

❑ **ESX 5.1 and later**: This virtual machine (VM Version 9) provides best performance and latest features in ESXi 5.1.
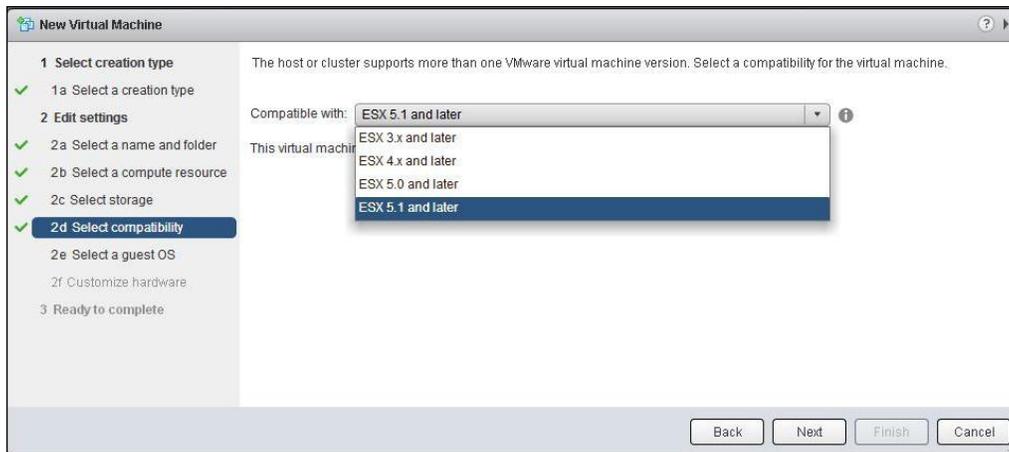
8. Select the guest OS family and the guest OS version for the virtual machine.

9. When creating the virtual machine, you will have an option to configure the virtual hardware. You can edit the virtual hardware or you can add a new virtual hardware by selecting the device from the **New device** drop-down menu and clicking on **Add**.
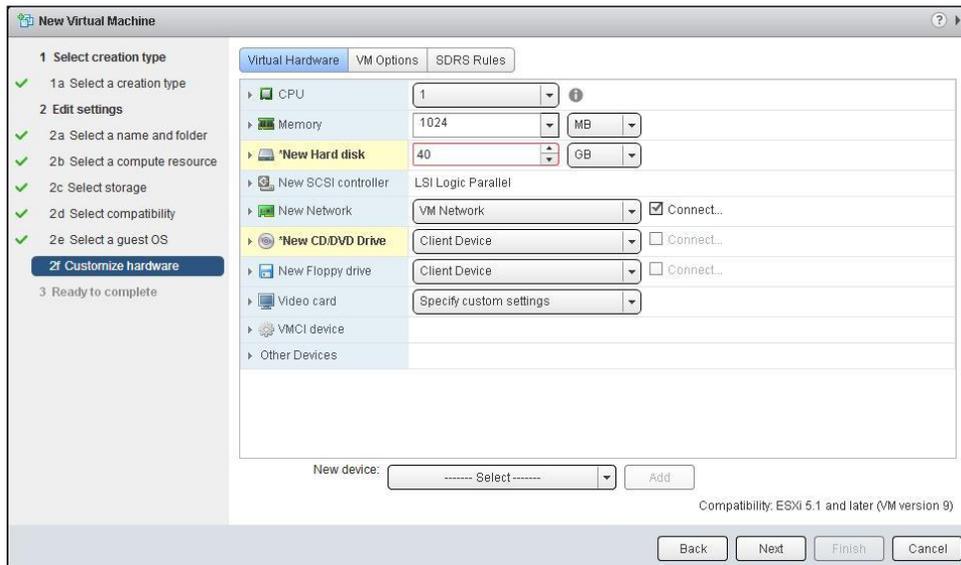
10. Review the selected options and click on **Finish** to create the new virtual machine.

The steps to deploy a virtual machine from the template are as follows. This option allows you to create a new virtual machine from the existing template. A template is a golden image of a preconfigured virtual machine as per your organization's needs. It allows you to easily deploy virtual machines very quickly.

1. Right-click on the cluster or the ESXi host and select **New virtual machine**.
2. Select the **Deploy from template** option from the **Select a creation type** page.
3. Select a template to deploy the virtual machine from. Optionally, you can also choose from the following options:

   ❑ **Customize the operating system**: This option is to customize the guest operating system of the virtual machine

   ❑ **Customize this virtual machine hardware (Experimental)**: This option is used to configure the virtual machine's hardware before the virtual machine deployment

   ❑ **Power on virtual machine after creation**: Select this option to power on the virtual machine after the creation of the virtual machine is complete.
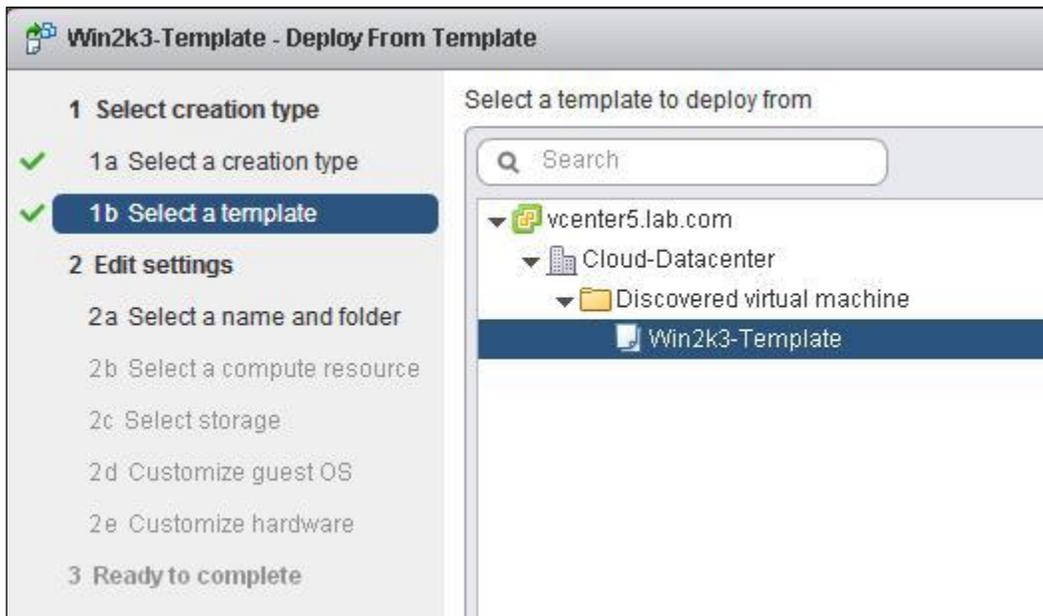
4. Enter the name for the virtual machine and choose the **Inventory location** for the virtual machine.
5. Select a computer resource such as **cluster**, **host**, **vApp**, or **resource pool** to run this virtual machine.

6. Select the **Datastore** to store the virtual machine. All the virtual machine related files are stored under the folder with the same as the VM name on the datastore selected.

7. Customize **Guest OS** and **virtual hardware** if required.

8. Review the selected options and click on **Finish** to create the new virtual machine.

Cloning an existing virtual machine allows you to create a copy of the existing virtual machine. The steps to clone an existing virtual machine are as follows:

1. Right-click on the cluster or the ESXi host and select **New virtual machine**.

2. Select the **Clone an existing virtual machine** option from the **Select a creation type** page.

3. Select a **virtual machine** to clone the New virtual machine from and optionally choose one of the options: **Customize the operating system**, **Customize this virtual machine hardware**, or **Power on virtual machine after creation**.

4. Enter the name for the virtual machine and choose the **Inventory location** for the virtual machine.

5. Select a compute resource, such as **cluster**, **host**, **vApp**, or **resource pool** to run this virtual machine on.

6. Select the **Datastore** to store the virtual machine.

7. Customize **Guest OS** and **virtual hardware** if required.

8. Review the selected options and click on **Finish** to create the new virtual machine.

Cloning a virtual machine to a template will allow you to create a copy of an existing virtual machine and making it a template. A template is a golden image of a preconfigured virtual machine that allows you to easily deploy virtual machines from a preconfigured virtual machine. The steps for cloning a virtual machine to Template are as follows:

1. Right-click on the cluster or the ESXi host and select **New virtual machine**

2. Select the **Clone virtual machine to Template** option from the **Select a creation type** page.

3. Select a virtual machine to clone to the template.

4. Enter a name for the Template and choose the **Inventory location** for the template.

5. Select a **cluster or host** to store this template. If host is selected, the template is directly placed on that host or the template will be placed on any one of the hosts in cluster, if cluster is selected.

6. Select the **Datastore** to place the template. All the template-related files are stored on the datastore.

7. Review the selected options and click on **Finish** to clone a template from a virtual machine.

Cloning a template to template allows you to create a copy of an existing template. Steps for cloning a template to template are as follows:

1. Right-click on the cluster or the ESXi host and select **New virtual machine**.
2. Select the **Clone a Template to Template** option from the **Select a creation type** page.
3. Select a template to clone the template from.
4. Enter a name for the Template and choose the **location** for the template.
5. Select a **cluster or host** to store this template in.
6. Select the **Datastore** to place the template in.
7. Review the selected options and click on **Finish** to clone a template from an existing template.

You can update the virtual machine with the latest software and patches and then convert the virtual machines back to template to continue the virtual machine's deployment from the template. The steps to convert a template to virtual machine are as follows:

1. Right-click on the cluster or the ESXi host and select **New virtual machine**.
2. Select the **Covert template to virtual machine** option from the **Select a creation type** page.
3. Select a template to convert to virtual machine.
4. Select a compute resource such as **cluster, host, vApp or resource pool** to run this virtual machine on.
5. Review the selected options and click on **Finish** to convert a template to a virtual machine.

How it works...

Virtual machines comprise multiple files that will be stored on the datastore. These files make up the virtual machine. The following is the list of file types which the virtual machine comprises:

▶ `.vmx`: This is a virtual machine configuration file that contains the settings specified while creating a new virtual machine wizard or while editing the virtual machine settings.

▶ `.vmxf`: This is an additional virtual machine configuration file for the VMs in the team.

▶ `.vmdk`: This is a virtual disk file that contains the virtual machine's hard disk characteristics.

- ▶ `-flat.vmdk`: This is a virtual disk file that contains the virtual machine disk data.
- ▶ `.nvram`: This file contains the virtual machine BIOS or EFI configuration.
- ▶ `.vswp`: This is the virtual machine swap file. It will be created when the virtual machine will be powered on. The size of the file is equal to the memory assigned to the virtual machine. This file will be used as memory overflow in case of memory contention of the ESXi host.
- ▶ `.vmsd`: This file is the virtual machine's snapshot.
- ▶ `.vmsn`: This file is the virtual machine snapshot data file.
- ▶ `.vmss`: This is the virtual machine's suspend file.
- ▶ `.log`: This file is the current virtual machine log file.
- ▶ `-#.log`: This file is the compressed old log entries.
- ▶ `-delta.vmdk`: This file will be created only when snapshots are created. A delta file will be created for each snapshot that you create for the VM. This file will be deleted once snapshot of the virtual machine is deleted.
- ▶ `-rdm.vmdk`: This file will be created when the virtual machine is assigned with RDM raw file. This is the mapping file for the RDM.

There's more...

The **Open virtual machine Format** (**OVF**) template can be used to deploy a preconfigured virtual machine to your vCenter Server or the ESXi host. vSphere client or vSphere Web Client allows you to deploy and export virtual machines with preinstalled guest operating system and preconfigured software into OVF format. You can also export the preconfigured virtual machine with preinstalled software applications from your inventory to use as virtual appliance. An OVF file allows faster deployments of the virtual machine with preconfigured guest operating system and applications. OVF can encapsulate more than one virtual machine and also multi-tiered applications.

The steps for deploying an OVF template are as follows:

1. Right-click on the cluster or the ESXi host and select **Deploy OVF Template**.
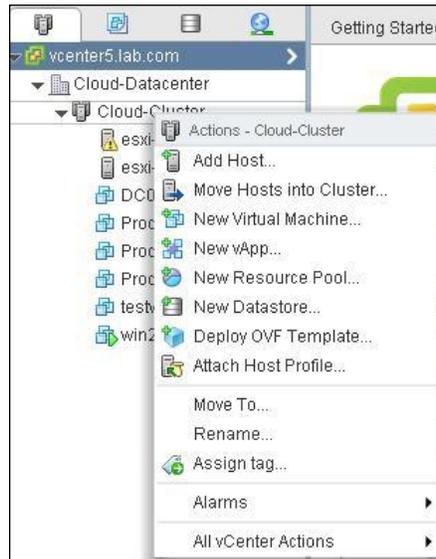
2. Select either deploy from the URL or local file option to deploy the OVF template from.

3. Enter a URL to download and install the OVF package from the Internet, or browse to a location file accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. Click on **Next**.

4. Review the OVF template details and click on **Next**.

5. Click on **Accept** to accept the OVF license agreement and click on **Next**.

6. Edit or enter the OVF template Name and specify the folder location for the OVF. Click on **Next**.

7. Select one of the **Datastores** listed to store the files for this deployed template and click on **Next**.

8. Select one of the virtual machines port groups from the **Destination** networks drop-down for the deployed OVF template.

9. Select one of the IP allocation methods either **Static-Manual** or **DHCP** from the **IP Allocation** drop-down and Enter **DNS Servers**, **Net Mask** and **Gateway information**. Click on **Next**.
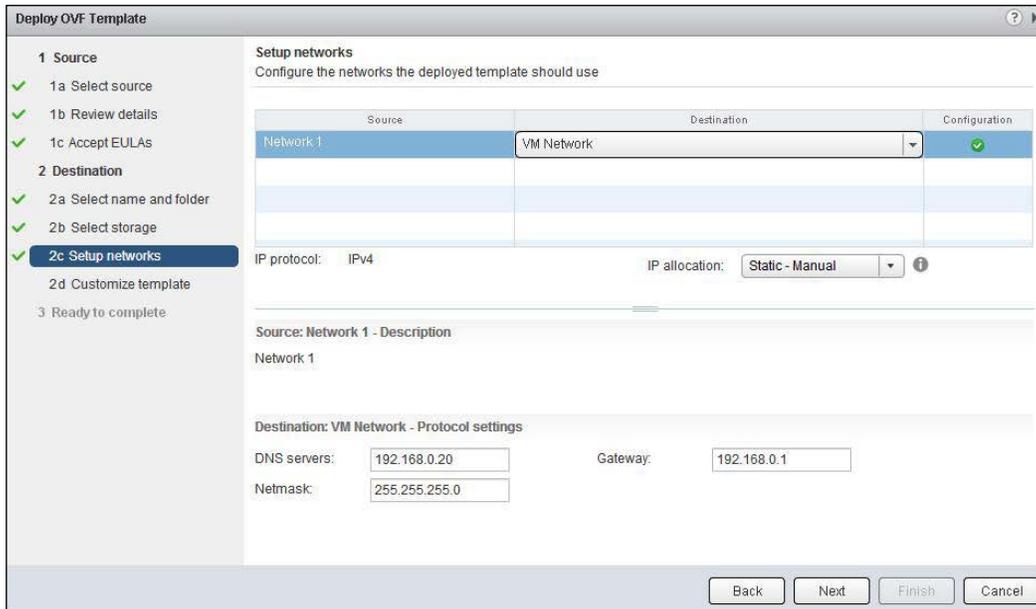
10. Enter all the required properties to customize the deployed OVF and click on **Next**.

11. Review your selected settings and click on **Finish** to complete the OVF template deployment. Optionally, you can choose the checkbox **Power on after deployment** to power on the OVF template once deployment completes.

The steps for exporting an OVF template from the virtual machine are as follows:

1. Browse to your virtual machine in the vSphere Web Client.

2. Right-click on the powered-off virtual machine and select **All vCenter Actions**.

3. Select **Export OVF Template**.

4. Enter the name for the OVF template.

5. Click on **Choose** to browse to the location to save the exported OVF template.

6. Select the checkbox **Overwrite existing files** if you want to overwrite files with the same name on the desktop location.

7. Select one of the following format from the drop-down for the OVF Template:

    ❑   **Folder of Files (OVF):** Select this option to store the OVF templates as a set of files (`.OVF`, `.VMDK`, and `.mf`) and also if you plan to publish this OVF on a web server or image library. This OVF package can be deployed using the URL from the vSphere Web Client.

    ❑   **Single File (OVA):** Select this option to package the OVF template into a single file (`.OVA` file). This can be downloaded from the website and used as a single file. This OVF package can be deployed using the file location option from the vSphere Web Client.

8. Type the description for the OVF Template in the **Annotation** field.

9. Select **Enable advanced options**, if you want to include additional options for this exported OVF template.
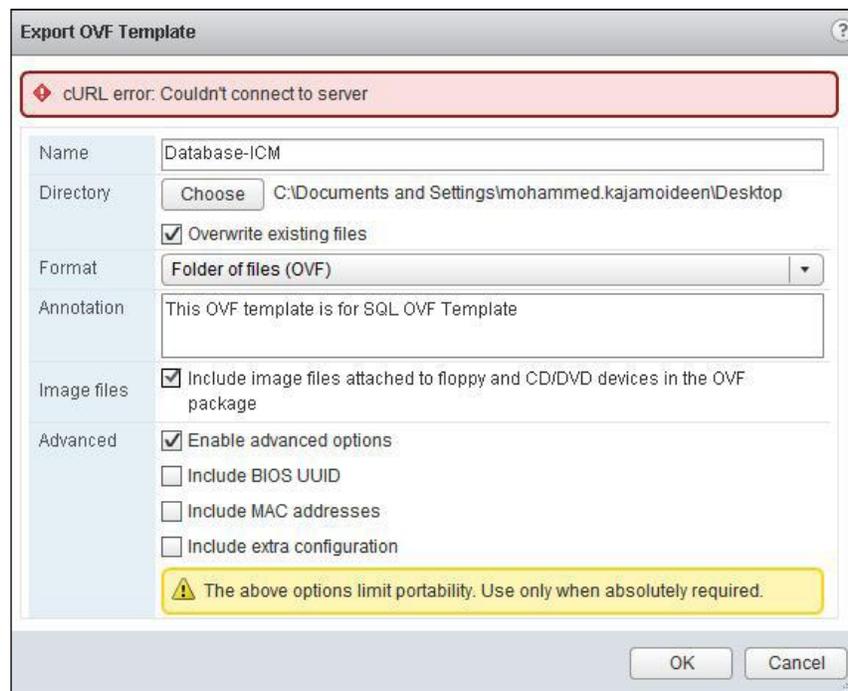
10. Click on **OK** to complete the export of the OVF template.

Installing and customizing a guest operating system

Once the virtual machine is created, the next step will be to install the guest operating system on the virtual machine. But when you deployed a virtual machine from the template or a clone from an existing virtual machine, you can customize the guest operating system of the virtual machine to avoid conflicts. Conflicts may happen when identical virtual machines are deployed either via the template or clone.

Getting ready

Connect to your VMware vCenter Server using the vSphere Web Client. Browse to your virtual machine in the vSphere Web Client.

How to do it..

We'll demonstrate a step-by-step procedure to configure, install, and customize the guest operating system of the virtual machine. The steps for configuring a virtual machine BIOS to boot from the CD/DVD drive are as follows:

1. Right-click on the virtual machine and select **Edit Settings**.

2. Click on the **VM Options** tab and select **Boot Options**.

3. Click on **Boot Options** to expand its configuration options.

4. Select the checkbox **Force BIOS Setup** to force the virtual machine to enter into the BIOS setup screen next time the virtual machine boots. Click on **OK** to apply the settings.
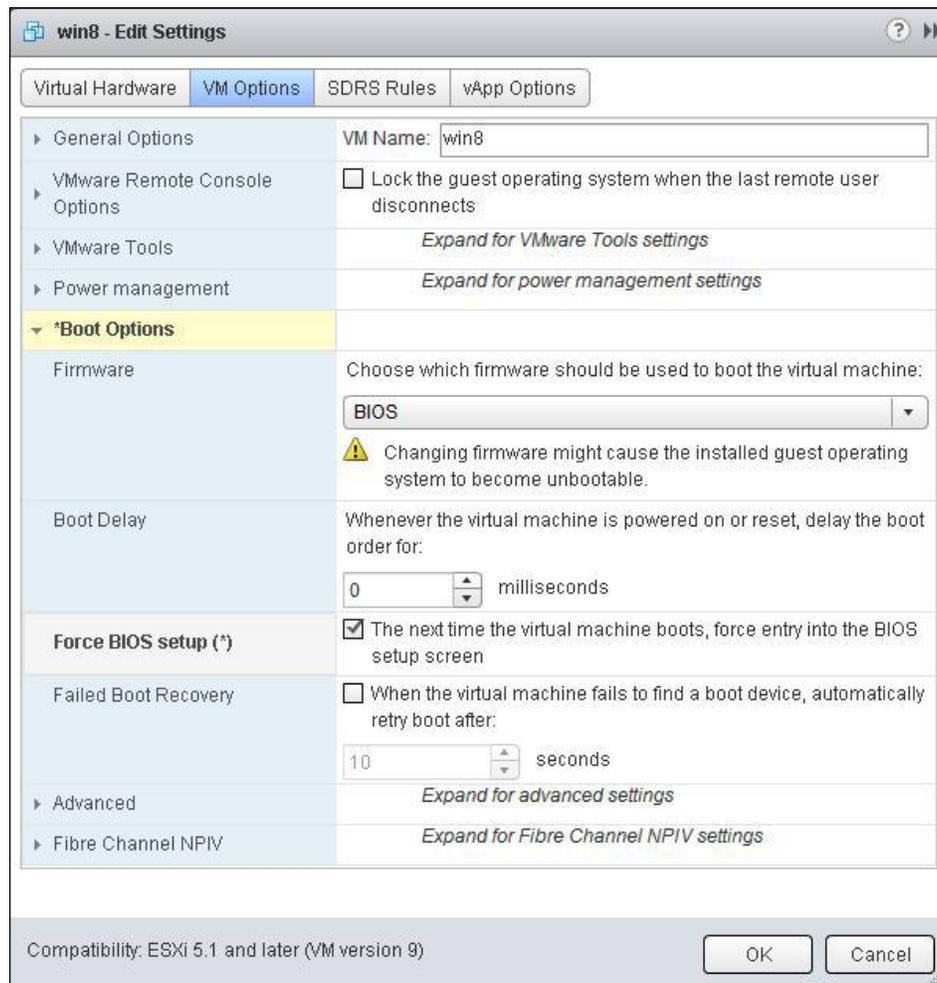
5. Power on the virtual machine and click on **Launch Console** under the **Summary** tab.

6. Once the virtual machine boots into the BIOS screen select the **Boot** tab.

7. Expand on the plus symbol to bring the **CD-ROM Drive** to the top.

```
                    PhoenixBIOS Setup Utility
   Main      Advanced     Security     Boot     Exit

                                            ┌─────────────────────────┐
                                            │    Item Specific Help    │
                                            │                          │
      CD-ROM Drive                          │                          │
     +Hard Drive                            │ Keys used to view or     │
     +Removable Devices                     │ configure devices:       │
      Network boot from Intel E1000e        │ <Enter> expands or       │
                                            │ collapses devices with   │
                                            │ a + or -                 │
                                            │ <Ctrl+Enter> expands     │
                                            │ all                      │
                                            │ <+> and <-> moves the    │
                                            │ device up or down.       │
                                            │ <n> May move removable   │
                                            │ device between Hard      │
                                            │ Disk or Removable Disk   │
                                            │ <d> Remove a device      │
                                            │ that is not installed.   │
                                            └─────────────────────────┘

   F1   Help    ↑↓  Select Item   -/+   Change Values    F9   Setup Defaults
   Esc  Exit    ↔   Select Menu   Enter Select ▶ Sub-Menu F10  Save and Exit
```

8. Press *F10* to save the configuration and exit from the BIOS screen.

The steps for installing the guest operating system are as follows:

1. Right-click on the virtual machine and select **Edit Settings**.
2. Click on the **Virtual Hardware** tab.
3. Select **CD/DVD drive** and click on **CD/DVD drive** to expand its configuration options.
4. Select one of the following **CD/DVD device** from the drop-down:
    - **Client Device**: Select this option to install the guest operating system from the CD/DVD device connected to the physical DVD or CD device on the system from which you are using the vSphere Web Client to connect to your vCenter Server.
    - **Host Device**: Select this option to install the guest operating system from the CD/DVD device connected to the physical ESXi host.
    - **Datastore ISO File**: Select this option to install the guest operating system from the CD/DVD device attached to an ISO file that is stored on a datastore accessible to the ESXi host.

5. Select **Connect At Power On** for CD/DVD device status.

6. Click on **OK** to apply the settings.

7. Once the CD/DVD drive is connected to the virtual machine, **power on** the virtual machine

8. The virtual machine will boot from the attached CD/DVD media.

Now, follow the operating system installation instructions. The steps for installing VMware tools on Windows guest operating system are as follows:

1. Make sure your virtual machine is powered on and a guest operating system is running.

2. Right-click on your virtual machine and select **All vCenter Actions**.

3. Choose **Guest OS** and select **Install/Upgrade VMware Tools**.

4. In the confirmation window, click on **Mount** to install VMware Tools.
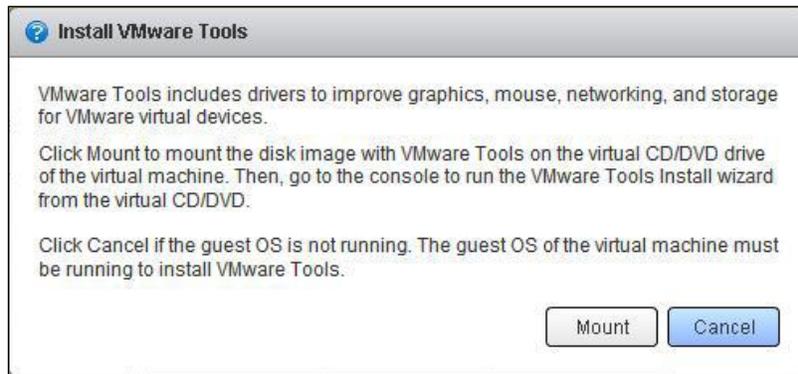
5. To open the virtual machine console, click on **Launch Console** in the **Summary** tab of the virtual machine

6. Log in to the guest operating system and open **My Computer**.

7. Double-click on the VMware tools mounted on your virtual machine CD/DVD drive.

8. Follow the installation instructions as per the VMware tools installation wizard and click on **Finish** to complete the VMware tool's installation.

9. Restart your virtual machine to apply the settings.

The steps for using customization specification manager to customize the guest OS are as follows:

1. From the vSphere Web Client home page, click on **Rules and Profiles**.

2. Select **Customization Specification Manager**.

3. Expand the plus symbol to create a new specification.

---

4. Select either **Windows** or **Linux** from the **Target VM Operating system** drop-down.

5. Enter the name for this customization specification and click on **Next**.

6. Enter the registration information for this copy of the guest operating system.

7. Choose one of the following options to enter the computer name that will identify this virtual machine on a network:

   ❑ **Enter a name**: This option allows you to manually enter the computer name for the virtual machine. The name cannot exceed 15 characters. You choose the checkbox **Append a numeric value to ensure uniqueness** to append the hostname with the numeric value. The name will be truncated if combined with the numeric value; the name cannot exceed fifteen characters.

   ❑ **Use the virtual machine name**: This option will use the virtual machine name as the computer name for the guest operating system.

   ❑ **Enter a name in the Clone/Deploy Wizard**: With this option, you can enter a computer name for the virtual machine, when it is deployed from the clone/deploy wizard.

   ❑ **Generate a name using the custom application configured with the vCenter Server**: You can use the custom application to enter a computer name for the virtual machine.
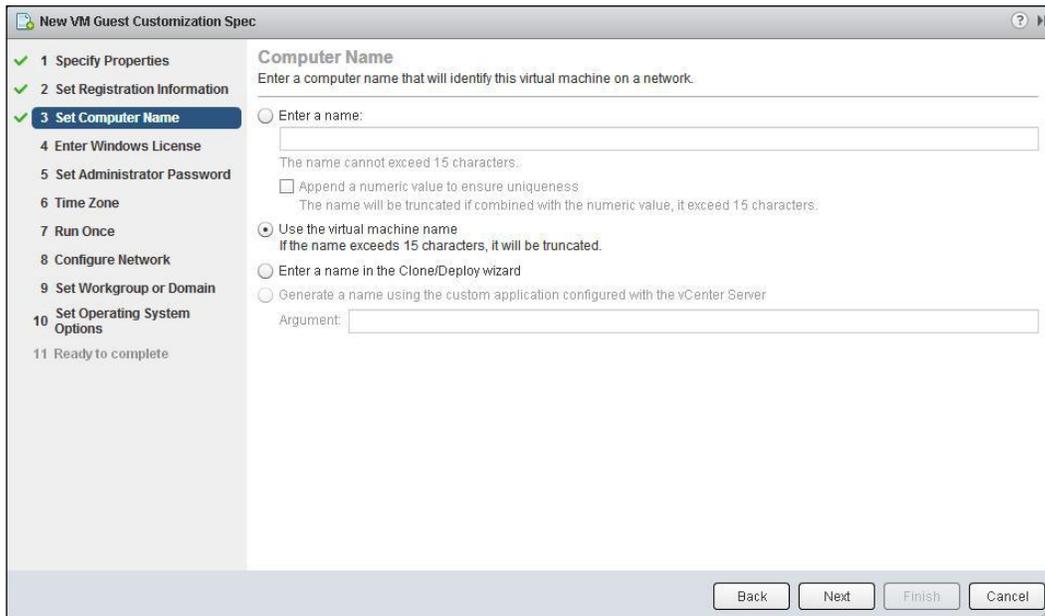
8. Enter the Windows Licensing information for this copy of the guest operating system. If this virtual machine does not require licensing information, leave these fields blank. Select Licensing Mode **Per seat or Per server** for the windows guest operating system and enter the number of Max connections for every server licensing mode. Click on **Next**.

9. Enter the **Administrator Password** for the autolog on option of the administrator account. Select the checkbox, **Automatically logon as Administrator** and enter the number of times to logon automatically and click on **Next**.

10. Select the **Time Zone** for this virtual machine from the drop-down and click on **Next**.

11. Specify the commands to be executed the first time a user logs in to the guest operating system. Click on **Add** to add the commands.

12. Configure the network for the virtual machine either using default or custom network settings.

13. Select the option **How will this virtual machine participate in a network?**. Choose either **workgroup or Domain** and enter Workgroup name or domain name, username, and password for the user account that has permission to add the computer to the domain. Click on **Next**.

14. Select the checkbox **Generate New Security ID (SID)** to generate a new security identity for the virtual machine and click on **Next**.

15. Review the selected options and click on **Finish** to create a new guest customization specification for the Windows operating system.

The steps for customizing the virtual machine deployed from the template or clone are as follows:

1. Browse to your VMs and templates in the vSphere Web Client.

2. Right-click on your template and select **Deploy VM from this Template**.

3. Enter a name for a virtual machine and select the location to place the deployed virtual machine. Click on **Next**.

4. Select a **Cluster, host ,vApp, or resource pool** to run this virtual machine and click on **Next**.

5. Select a **Datastore** and choose the disk format from the **select virtual disk format** drop-down if you want to change the virtual machine's disk format. Click on **Next**.

6. Select the checkbox **Customizing the operating system** in **Select clone options** and click on **Next**.
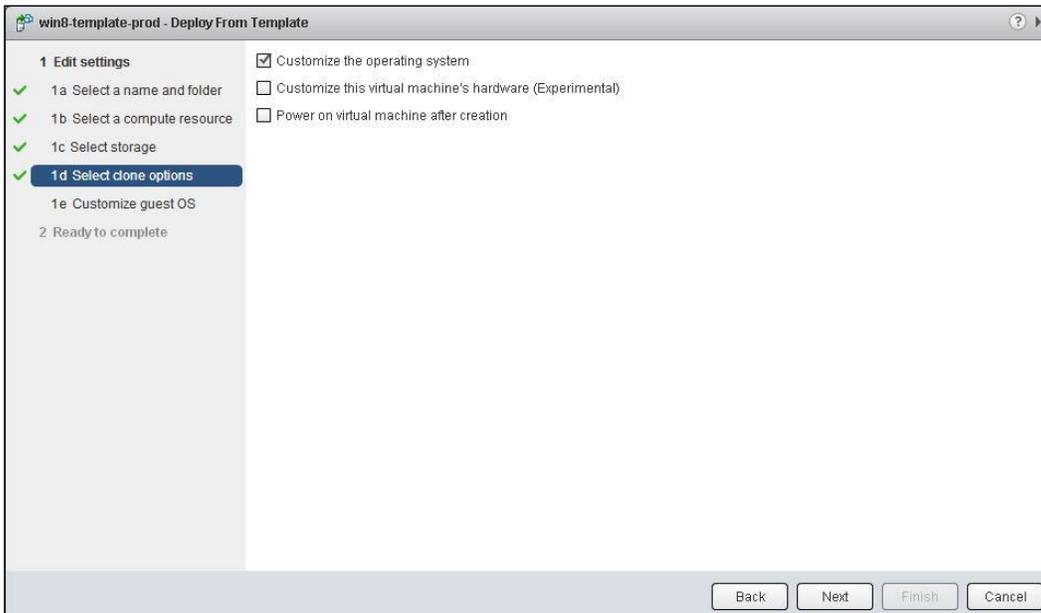
7. Choose customization specification that is suitable for this operating system deployment and click on **Next**.
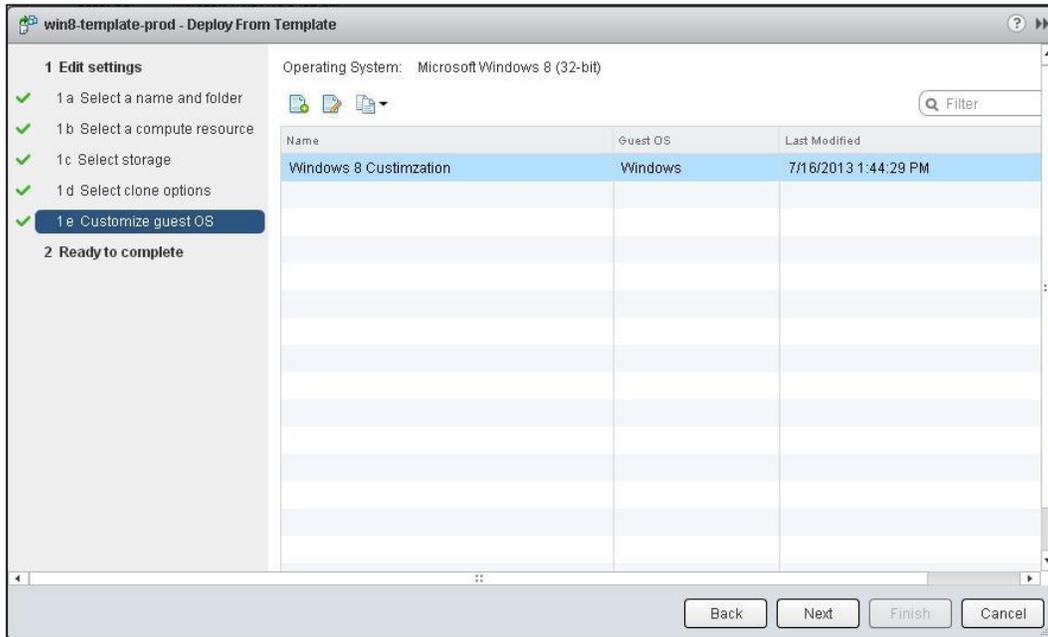
8. Enter the values that are required as input for this customization specification and click on **Next**.
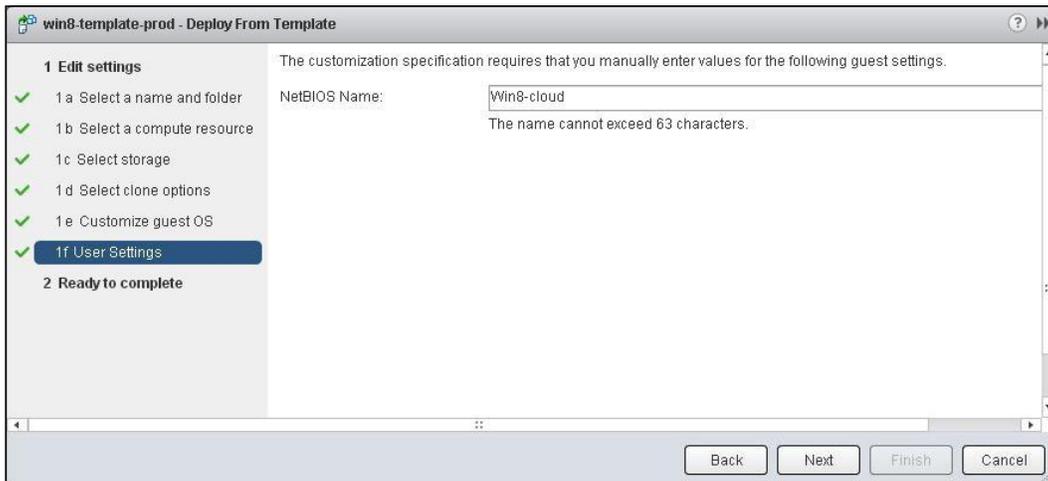
9. Review the options selected for the virtual machine deployment and click on **Finish**.

There's more...

The client integration plug-in provides access to perform vSphere infrastructure tasks such as accessing the virtual machine's console, deploying OVF or OVA templates and also uploading and downloading files from the datastore browser. Apart from that, the client integration plug-in allows you to connect to the virtual devices from the client computer to a virtual machine. The client integration plug-in can be installed from the vSphere Web Client.

The steps for installing the client integration plug-in are as follows:

1. Open your web browser and enter the URL of your vSphere Web Client.
2. In the left corner of your vSphere Web Client, click on **Download the Client Integration Plug-in**.
3. Once the download is complete, start the installation by double-clicking on the **Client Integration Plug-in installer**.
4. In the welcome screen, click on **Next** to continue the installation of the client integration plug-in.
5. Follow the installer instructions and click on **Finish** to complete the installation.

Configuring the ESXi host and VM for Fault Tolerance

vSphere Fault Tolerance (**FT**) is also called as super high availability. vSphere Fault Tolerance provides continuous availability to the virtual machines even during the ESXi host failures by eliminating the downtime to the virtual machine and applications running in it. **vSphere High availability** (**HA**) provides high availability to virtual machines in case of ESXi host failures but the downtime to the virtual machines will be the time the virtual machine restarted on the other hosts. In vSphere Fault Tolerance, there will be zero downtime even in case of ESXi host failure. FT-protected virtual machines are continuously available even when the parent ESXi host is down.

Getting ready

Connect to your vCenter Server via the vSphere Web Client login.

How to do it...

We will take a look at a step-by-step procedure to prepare and configure the ESXi host and virtual machine for Fault Tolerance. The steps for preparing the host and cluster for Fault Tolerance are as follows:

1. vSphere HA must be enabled on the vSphere cluster and the ESXi hosts to place the Fault tolerance virtual machine on the cluster.

2. At least two ESXi hosts that are FT-certified with same build number or Fault Tolerance version should be in the HA cluster.

3. The ESXi hosts BIOS must have enabled with HV.

4. The ESXi hosts should have one of the processors that is compatible with FT and also compatible with one another.

5. The ESXi hosts must have access to same networks and datastores attached.

6. The ESXi hosts must be licensed and certified for the Fault Tolerance feature.

7. The ESXi hosts VMkernel network must be enabled with vMotion and Fault Tolerance logging. It is a good practice to separate the different VMkernel networks using different NICs.
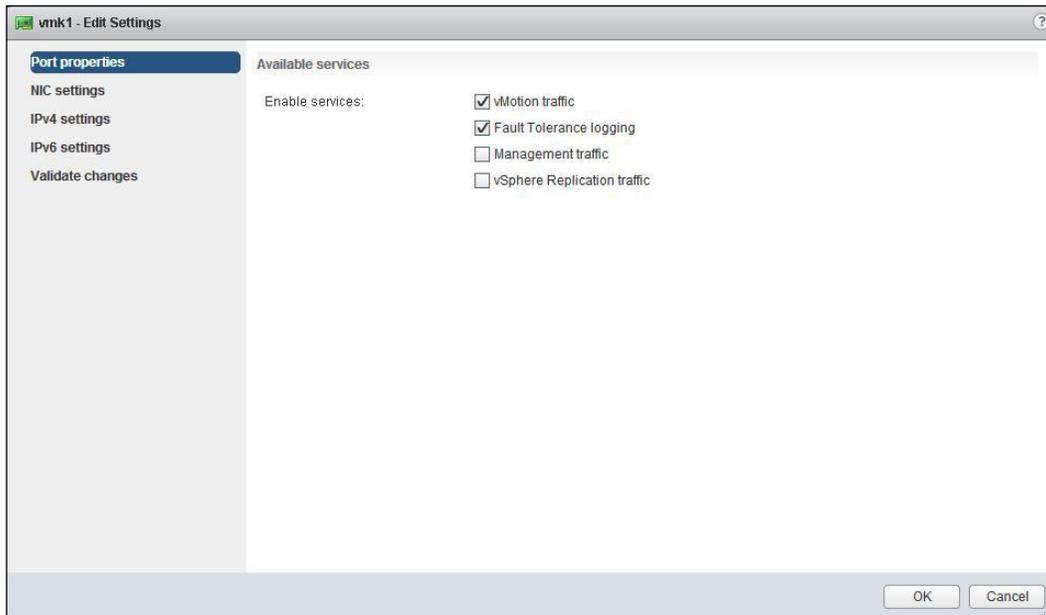
The steps to modify the requirements and limitations of the virtual machine for Fault Tolerance are as follows:

1. Virtual machines must have **Virtual RDM** or **VMDK** (**Virtual Machine DISK**) with thick provision eager zeroed format. Virtual machines with other disk formats should be converted to supported disk format to enable Fault Tolerance. When you try to enable Fault Tolerance on the virtual machine with thin format, it will display the message that the VMDK file must be converted. The virtual machine must be powered off to proceed with this disk format conversion.

2. FT-enabled virtual machines should be stored on shared storage such as Fibre Channel, iSCSI, NFS, and NAS.

3. Virtual machines must be running with the supported guest operating system.

4. Virtual machines must not have snapshots to enable the Fault Tolerance.

5. Fault tolerance cannot be enabled on the virtual machine with a linked clone.

6. A virtual machine enabled for Fault Tolerance cannot be migrated with Storage vMotion. To migrate the virtual machine with storage vMotion, Fault Tolerance should be temporarily turned off.

7. A virtual machine with only one vCPU is compatible with Fault Tolerance. **Symmetric Multiprocessor** (**SMP**) virtual machines are not supported for Fault Tolerance.

8. vSphere features such as **Physical Raw Device Mapping** (**RDM**), Para virtualized guests, IPv6 for FT logging, Extended Page Tables/Rapid Virtualization Indexing, Virtual EFI firmware, NIC passthrough, N_pord ID Virtualization, and devices such as USB devices, sound devices, Vlance network drivers, hot-plugging devices, serial ports, parallel ports, video devices with 3D enabled, virtual hard disk with thin-provisioned format and thick-provisioned have clustering feature but are not supported for Fault Tolerance.

9. Virtual machines must not have HA disabled from VM override options.

The steps for enabling Fault Tolerance for virtual machines are as follows:

1. Browse to your virtual machine in the vSphere Web Client.
2. Right-click on your virtual machine and select **All vCenter Actions**.
3. Select **Fault Tolerance** and choose **Turn On Fault Tolerance**.
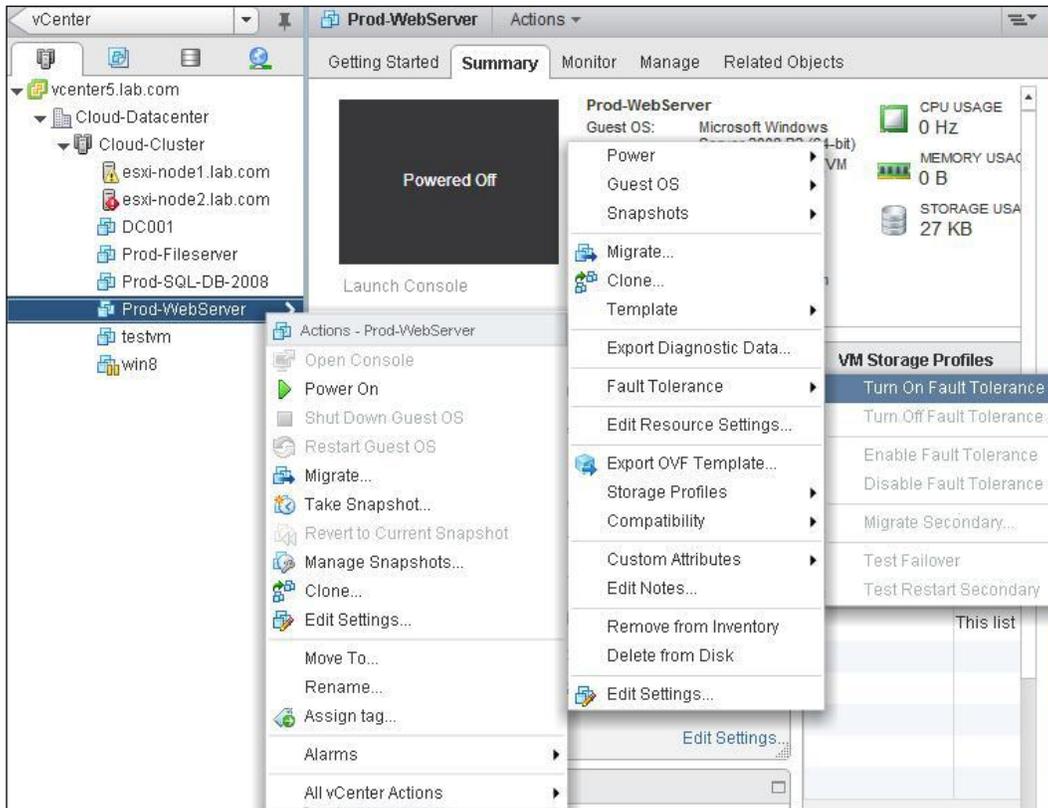
4. Click on **Yes** to turn on Fault Tolerance.
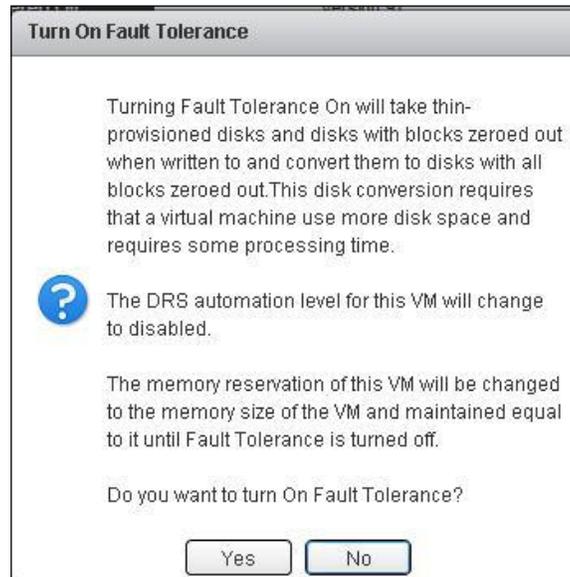
The steps for disabling Fault Tolerance for virtual machines are as follows. Disabling Fault Tolerance will remove Fault Tolerance protection from this virtual machine but will keep historical information about Fault Tolerance performance.

1. Browse to your virtual machine in the vSphere Web Client.
2. Right-click on your FT protected virtual machine and select **All vCenter Actions**.
3. Select **Fault Tolerance** and choose **Disable Fault Tolerance**.
4. Click on **Yes** to disable the Fault Tolerance.

Turning off Fault Tolerance will remove Fault Tolerance protection from this virtual machine and delete all historical Fault Tolerance data. The steps for turning off Fault Tolerance for virtual machine are as follows:

1. Browse to your virtual machine in the vSphere Web Client.
2. Right-click on your FT protected virtual machine and select **All vCenter Actions**.
3. Select **Fault Tolerance** and choose **Turn off Fault Tolerance**.
4. Click on **Yes** to turn off the Fault Tolerance.

How it works...

Fault tolerance can be enabled for mission critical virtual machines. When Fault Tolerance is enabled for the virtual machine, a duplicate virtual machine will be created called secondary virtual machine. vSphere Fault tolerance uses a technology called **vLockstep technology**. vLockstep technology captures all inputs and events that happened in the primary virtual machine and will be sent to, and repeated on, the secondary virtual machine.

When you enable Fault Tolerance on the virtual machine, the secondary virtual machine will be created on another ESXi host in the same cluster. Fault tolerance uses FT logging network to transfer traffic between primary and secondary virtual machines. Both primary and secondary FT protected virtual machines will continuously exchange heartbeats. The exchange of heartbeats will be used to monitor the status of each other to ensure that the Fault Tolerance of the virtual machine is maintained. If the ESXi host hosting the primary virtual machine fails, immediately the secondary virtual machine will be activated and take the control of the primary virtual machine. A new secondary virtual machine will be created in other ESXi host in the cluster. The primary virtual machine and secondary virtual machine are not allowed to run on the same ESXi host. This ensures that both the primary and secondary VM will not fail in case of host failure, so it always ensures that the Fault Tolerance of the virtual machine is maintained.

There's more...

VMware site survey is a plug-in for vSphere client, which analyzes the ESX/ESXi hosts managed by the vCenter Server and it reports whether the current configuration of both software and hardware is compatible for use with the vSphere Fault Tolerance.

The steps for using site survey to check Fault Tolerance Compliance are as follows:

1. Log in to your vCenter Server using vSphere client.
2. Select your cluster or the ESXi host and click on the **Site Survey** tab.
3. Click on **Run Site Survey**.
4. Click on **Add** to add the DRS rules.

5. It will display the compatibility of your selected ESXi hosts or host in the cluster and virtual machines for Fault Tolerance Compliance.

Refer to the following link to understand the installation of VMware Site Survey:

```
http://www.vmwarearena.com/2012/08/fault-tolerance-vmware-site-
survey.html
```

> As per VMware, Site Survey is no longer supported as of vSphere 5.1.
> Versions prior to 5.1 will continue to be supported. However, I have
> explained the feature of Site Survey to understand its features and benefits.

Configuring virtual machine hardware

A virtual machine has virtual devices that are similar to physical hardware and provide the same functionality as that of the physical servers along with additional benefits, such as manageability, portability, and high level of security. The following is the list of virtual hardware devices that can be added to the virtual machines, but not all hardware is available to every VM. It is based on the ESXi host it is running, guest operating system installed on the virtual machine, and also on the vSphere license.

- CPU
- Memory
- Virtual Network Adapter
- Virtual hard disk
- Chipset
- DVD/CD-ROM drive
- Floppy drive
- USB device
- USB controller
- SCSI device
- SCSI controller
- Serial port
- Parallel port
- Keyboard
- Pointing device
- PCI device
- PCI controller
- IDE controller

Getting ready

Connect to your vCenter Server via the vSphere Web Client and browse to your virtual machine in the vSphere Web Client.

How to do it...

We will take a look at the step-by-step procedure to create and configure the virtual hardware for the virtual machine.

The steps for configuring the virtual CPU options are as follows:

1. Right-click on your VM and click on **Edit Settings**.
2. Click on **CPU** to expand its configuration options.
3. Select the **Number of Processors** from the **CPU** drop-down menu. The virtual CPUs available to a virtual machine depend on the number of licensed CPUs on the ESXi host and the number of CPUs supported by the selected guest operating system of the virtual machine.
4. From the **Cores per Socket** drop-down, select **number of cores per socket**.
5. Allocate the CPU capacity for the virtual machine by configuring **Reservation, Limits and Shares** if required.
6. Select one of the **CPUID Mask** options from the drop-down menu. The CPU identification mask specifies the CPU capabilities that this virtual machine requires so that vCenter Server can determine if a destination host is viable for vMotion or cold migration. In some cases, values need to be different for AMD processors. The following settings can be set in the AMD override tab:

    □ **Hide the NX/XD flag to guest**: With this automation level, vCenter Server will not provide any power management recommendations.

    □ **Expose the NX/XD flag to guest**: With this manual DPM automation level, vCenter Server will only recommend evacuating an ESXi host's virtual machines, and power off the ESXi host when the cluster's resource usage is low.

7. Select the **Expose hardware assisted virtualization to the guest OS** checkbox to expose the full CPU virtualization to the guest operating system. Applications that require **Hardware Virtualization** (**HV**) can run on virtual machines without binary translation or paravirtualization.

8. Select the **Enable Virtualized CPU performance counters** checkbox to use performance-tuning tools in the guest operating system for software profiling. This feature will be useful to identify the performance problems of the processor and improve the processor's performance. This capability is useful for software developers who optimize the software running on the virtual machines.

9. Select one of the following **Hyper threaded** (**HT**) **Sharing** options from the **HT sharing** drop-down menu. The HT sharing option allows you to control the sharing of a physical core within and among the virtual machine and virtual machine's Virtual CPUs.

    ❑ **Any**: With this **HT Sharing** option, the virtual CPUs of the virtual machine can share the physical core with other virtual CPUs of this virtual machine or other virtual machines.

    ❑ **None**: With this **HT Sharing** option, virtual CPUs of the virtual machine use a processor core whenever they are scheduled for it.

    ❑ **Internal**: With this **HT Sharing** option, virtual CPUs are allowed to share a physical core within the CPUs of this virtual machine but never share a core with any other virtual machine.

10. Choose one of the following **CPU/MMU Virtualization** types from the drop-down menu. ESXi can automatically determine if a virtual machine should use hardware support for virtualization based on the processor type and the virtual machine. However, overriding the automatic selection for some workloads can provide better performance. If a selected setting is not supported by the host, Automatic selection will be used.

    ❑ Automatic
    ❑ Software CPU and MMU
    ❑ Hardware CPU and software MMU

❑ Hardware CPU and MMU
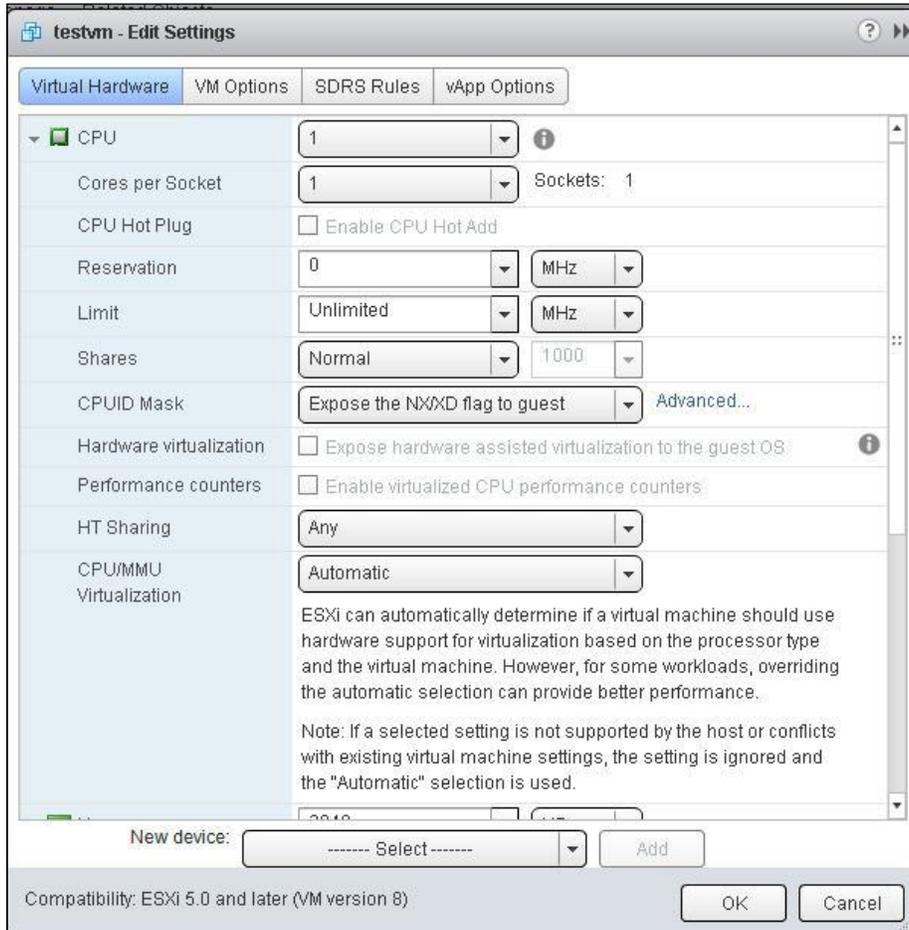
11. Click on **OK** to apply the settings.

The steps for configuring the virtual machine's memory options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Click on **Memory** to expand its configuration options.
3. Enter the virtual machine's memory size in MB or GB in the **RAM** option.

4. Allocate the memory capacity for the virtual machine by configuring **Reservation, Limits and Shares** if required.
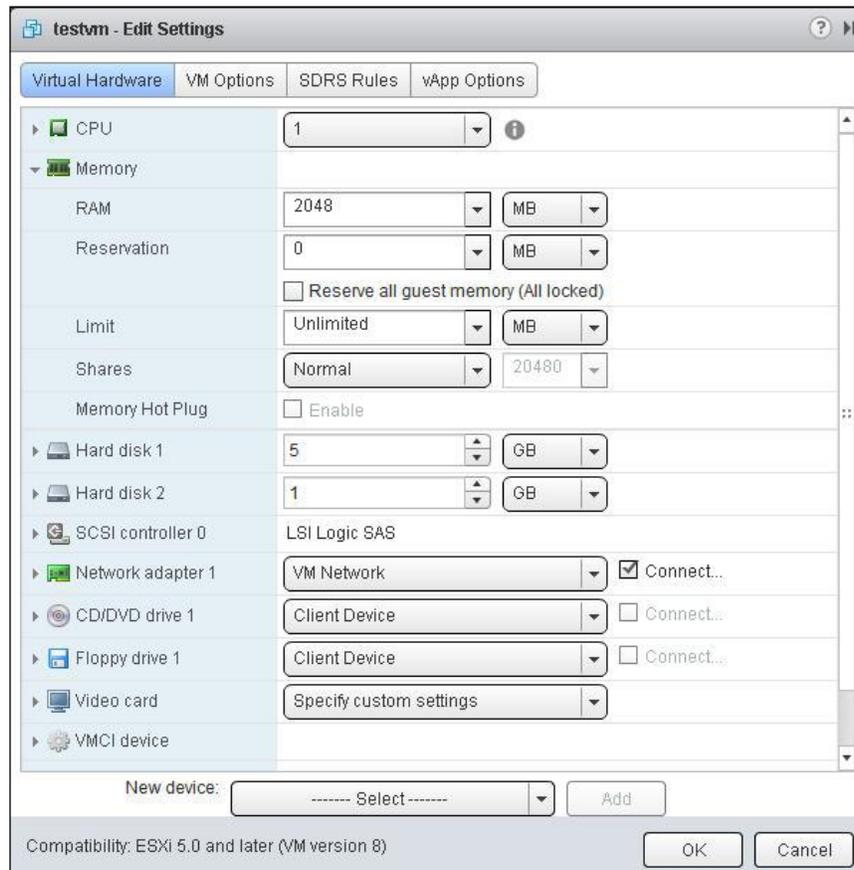
5. Click on **OK** to apply the settings.

The steps for reconfiguring the virtual machine's hard disk are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Click on **Hard disk** to expand its configuration options.
3. Enter the size of the virtual machine's hard disk in MB or GB if you want to change the size of the hard disk.
4. Configure the shares for your virtual hard disk. Choose **High**, **Normal**, **Low**, or **Custom** from the **Shares** drop-down menu.
5. You can enter the value in **Limit–IOPs** for the virtual disk.

6. You can choose the **virtual device node** from the drop-down for your virtual disk.

7. Choose one of the following disk modes for your virtual disk from the **Disk Provisioning** option:

   ❑ **Dependent**: This disk type is included in snapshots. It is the default option.

   ❑ **Independent-Persistent**: With this disk type, changes are written immediately and permanently to the disk. Persistent disks are not affected by snapshots.

   ❑ **Independent-Nonpersistent**: When power off or revert to the snapshot takes place, changes to this disk are discarded.

8. Click on **OK** to apply the settings.

The steps for adding a new virtual machine hard disk to a virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **New Hard disk** device from the device's drop-down and click on **Add**.

3. Enter the size of the new hard disk in MB or GB.

4. Select the **Store with the virtual machine or Browse** option to change the datastore location from the **Location** drop-down menu.

5. Select one of the following disk formats from the **Disk Provisioning** options:

   ❑ **Thick provision lazy zeroed**: This is the default disk format. With this disk format, the space required for the virtual disk is allocated during the disk creation. This disk is not zeroed during disk creation, which means any data on the physical storage device is not erased during the disk creation but is zeroed out on demand.

   ❑ **Thick provision eager zeroed**: This disk format is supported for clustering features such as the MSCS cluster and Fault Tolerance. The space required for the virtual disk is allocated during the disk creation. This disk will be zeroed during disk creation, which means any data on the physical storage device is erased during the disk creation. It takes a longer time to create this disk type as compared to other disk types.

   ❑ **Thin provision**: With this disk format, the virtual disk only utilizes the space required in the datastore. If the disk needs more space later, it can grow to the maximum capacity allocated to the virtual disk.

6. You can enter the value to **Limit - IOPs** for the virtual disk.

7. Choose one of the disk modes (**Dependent**, **Independent - Persistent**, or **Independent-Nonpersistent**) for your virtual disk in the **Disk Provisioning** option.
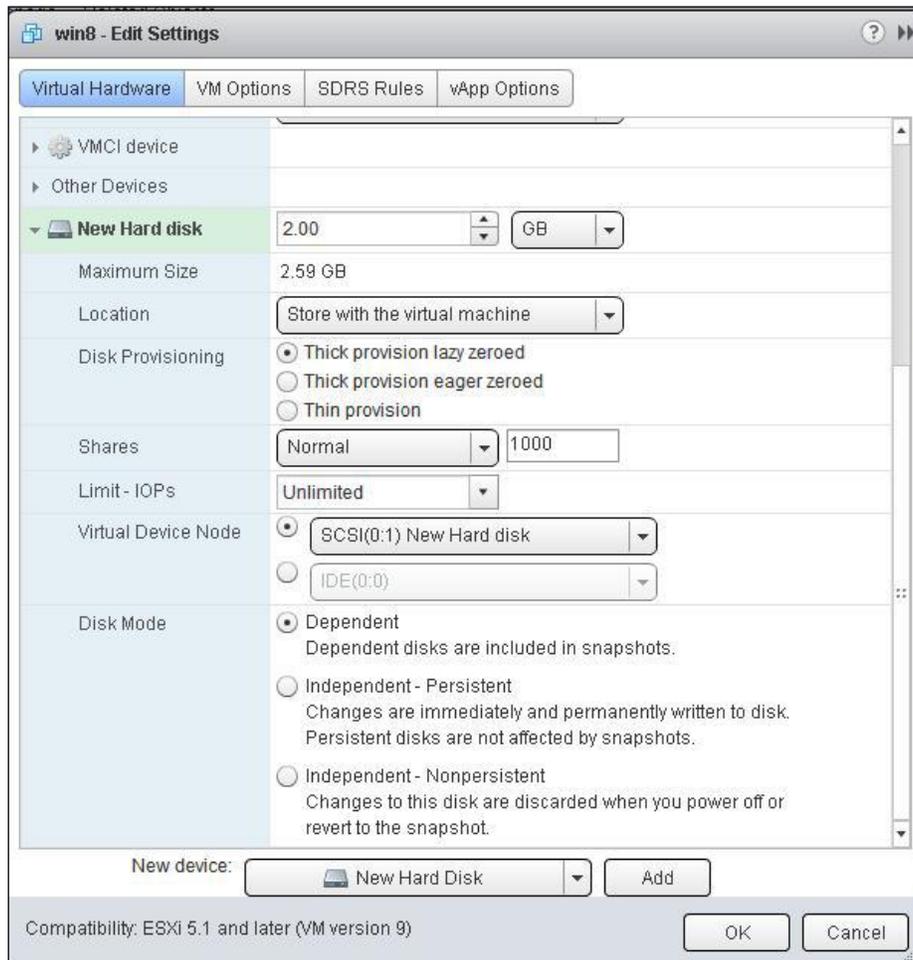
8. Click on **OK** to apply the settings.

The steps for adding the hard disk of an existing virtual machine to a virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **Existing Hard disk** from the device's drop-down menu and click on **Add**.
3. Select the datastore from the list where the existing virtual disk (`*.vmdk`, `*.raw`, or `*.dsk`) is stored.
4. Select the virtual disk and click on **OK**.
5. Click on **OK** to add an existing virtual hard disk.

The steps for adding an RDM disk to a virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **RDM disk** from the device's drop-down and click on **Add**. This option is enabled only when an unused LUN is presented in the ESXi host.
3. Select the **Physical LUN** from the list available under **Select Target LUN** and click on **OK**.
4. Select **Store with the virtual machine** or **Browse** to change to a different datastore location from the **Location** drop-down.
5. Select one of the following compatibility modes from the **Compatibility Mode** drop-down menu:
   - **Virtual Compatibility**: This compatibility allows the virtual machine to use snapshots and other advanced functionalities.
   - **Physical Compatibility**: This compatibility allows the guest operating system to access the hardware directly. A snapshot of this virtual machine will not include this RDM disk. This compatibility can be used to leverage array-based tools for protecting the virtual machine's data.
6. Configure the shares for your virtual hard disk. Choose **High**, **Normal**, **Low**, or **Custom** from the **Shares** drop-down.
7. You can enter the value to **Limit–IOPs** for the virtual disk.

8. You can choose the **Virtual Device Node** from the drop-down menu for your virtual disk.
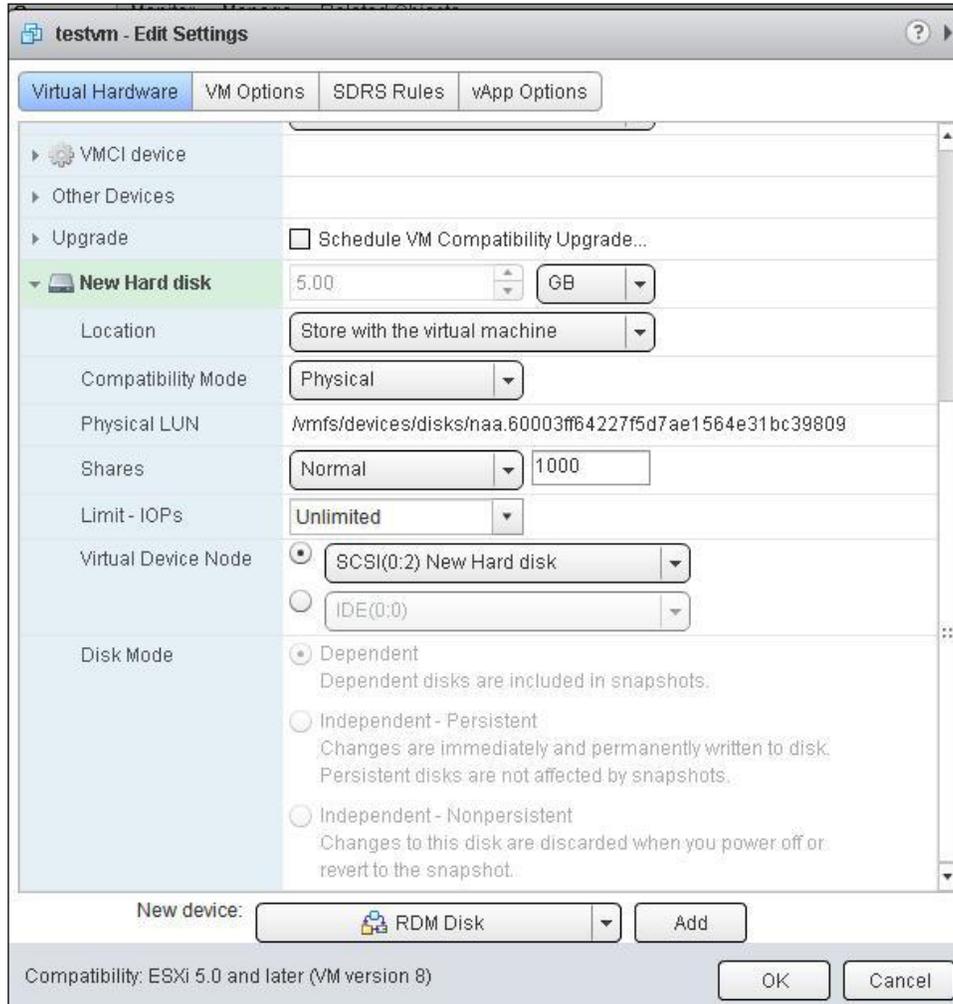
9. Click on **OK** to add an RDM disk to your virtual machine.

The steps for adding a network adapter to a virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **Network** from the device's drop-down menu and click on **Add**.
3. Select one of the virtual machine port groups from the **Network** drop-down menu.
4. Select the checkbox **Connect At power on** in the **Status** option.
5. Select one of the following types for the virtual adapter from the **Adapter type** drop-down menu:
   - ❑ **E1000**: This network adapter is the emulated version of Intel 8245EM Gigabit Ethernet NIC. These drivers are available in the most recent guest operating systems including Windows XP and later.
   - ❑ **Vlance**: This adapter type is the emulated version of AMD 79c970 PCnet32 LANCE NIC. These network adapter drivers are available in most 32-bit guest operating systems except Windows Vista and later.
   - ❑ **Flexible**: This adapter will appear as a vlance adapter when a virtual machine boots. When the VMware tools are installed, it will be transformed to a high-performance VMXNET adapter.
   - ❑ **VMXNET**: This adapter will only be available after VMware tools are installed on the virtual machine. This adapter type is optimized for performance.
   - ❑ **VMXNET 2 (Enhanced)**: This adapter is a high-performance one that provides advanced network features such as jumbo frames and hardware offloads. This adapter type is available for the virtual machines on ESX/ESXi 3.5 and later.
   - ❑ **VMNET 3**: This adapter is the paravirtualized NIC designed for higher performance. This adapter provides all the advanced features as in VMXNET2 and adds additional features such as IPv6 offloads, multiqueue support, and MST/MST-X interrupt delivery.
6. Select either **Automatic** or **Manual** from the MAC address assignment in the **MAC Address** drop-down menu.
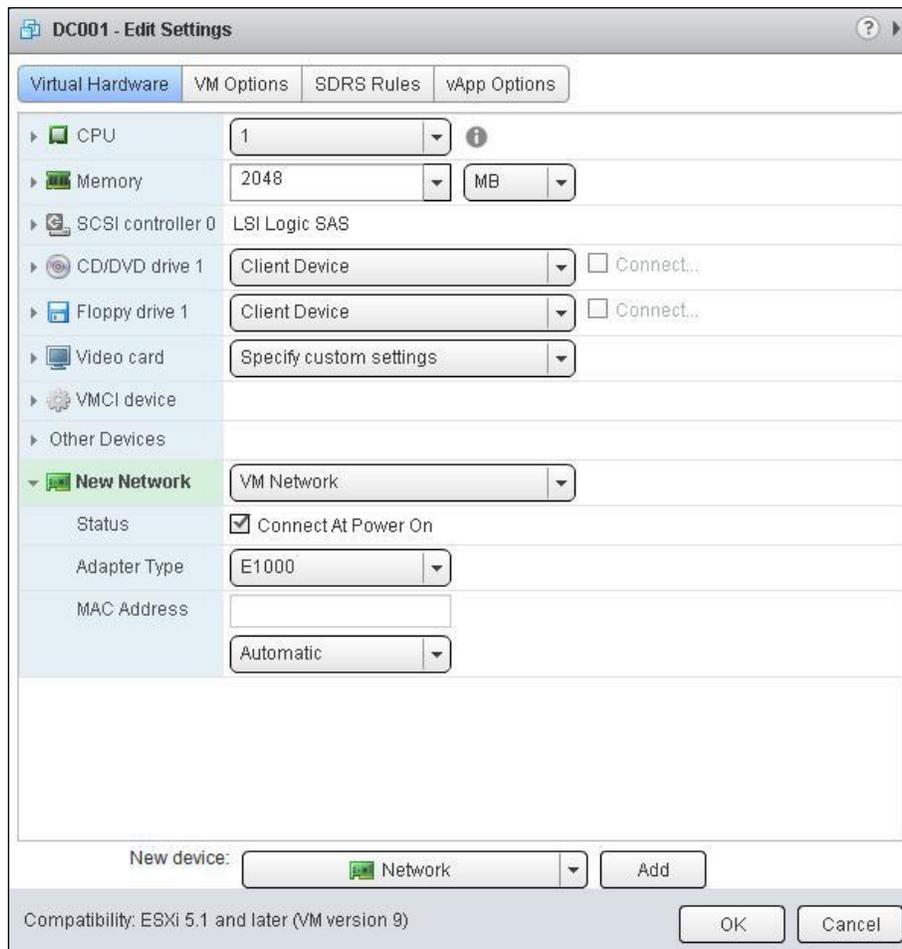
7. Click on **OK** to create the new network adapter for the virtual machine.

The steps for adding a CD/DVD drive to a virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **CD/DVD drive** from the device's drop-down and click on **Add**.
3. Select the type of CD/DVD device from the **New CD/DVD drive** drop-down menu:
   - ❑ **Client Device**
   - ❑ **Host Device**
   - ❑ **Datastore ISO file**

4. Select the **Checkbox Connect At Power on** status option.
5. Select the device type as either **Emulated IDE** or **Passthrough IDE** from the **Device Mode** drop-down menu.
6. Select the **Virtual Device Node** from the drop-down menu and click on **OK** to create the CD/DVD drive for the virtual machine.
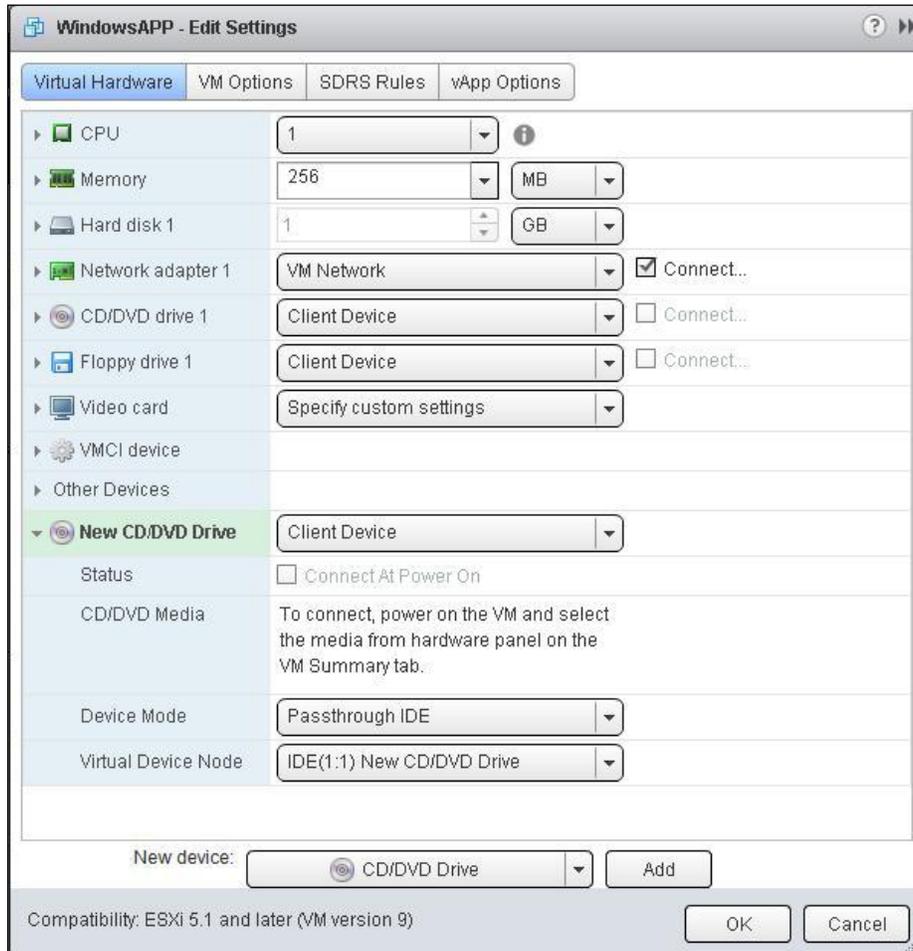
7. Click on **OK** to create the new CD/DVD drive for the virtual machine.

There's more...

vSphere DirectPath I/O allows the virtual machine's guest operating system to directly access the physical PCI and PCIe devices connected to the ESXi host. This feature gives you direct access to devices such as sound cards, graphics cards, and so on. Six PCI devices can connect to each virtual machine. The physical ESXi server's PCI device that needs to connect to the virtual machine should be made available for passthrough to a virtual machine. If the virtual machine that is connected with PCI devices using vSphere Direct I/O, you will not be able to suspend or migrate with vMotion and cannot take a snapshot of that virtual machine.

The ESXi host should have **Intel Virtualization for Directed I/O** (**VT-d**) or **AMD I/O virtualization technology** (**IOMMU**) enabled in BIOS to use the DirectPath I/O feature. Also, PCI devices should be marked as available for passthrough from the ESXi host. The virtual machine should be placed in the ESX/ESXi Version 4.x and later versions.

The steps for adding a PCI device to the virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **PCI Device** from the device's drop-down menu and click on **Add**.
3. Click on **New PCI device** to expand its configuration options.
4. Select the passthrough device from the drop-down menu to connect to the virtual machine.
5. Click on **OK** to connect the selected PCI device to the virtual machine.

Configuring virtual machine's options

The virtual machine's options can be used to configure VMware tools' scripts, startup behavior, boot options, user access to the remote console, and many more options. The following are the virtual machine's options that can be configured as part of its options' settings:

- **General options**: This option can be used to configure the virtual machine display name and to view the guest OS type, OS version, location of the virtual machine configuration file and working location.

- **VMware remote console options**: This option can be used to lock the guest operating system when the last remote user disconnects and also to limit the number of simultaneous connections to the virtual machine.

- **VMware Tools option**: This option can be used to configure power control behavior, VMware tools, automatic upgrade of VMware tools, and also to configure time synchronization between the guest and the host.

- **Power Management options**: This option can be used to configure the standby response and also the Wake on LAN feature of the virtual machine.

- ▶ **Virtual machine boot option**: This option can be used to configure boot delay, forcing BIOS setup, and failed boot recovery of the virtual machine.

- ▶ **Virtual machine advanced option**: This option can be used to configure acceleration, debugging and statistics, and also the swap file location. This option can be used to add additional configuration parameters and also latency sensitivity of the virtual machine.

- ▶ **Fibre channel NPIV options**: This option can be used to configure the fibre channel virtual WWNs.

Getting ready

Connect to your vCenter Server via the vSphere Web Client and browse to your virtual machine in the vSphere Web Client.

How to do it...

Virtual machine options can be used to define the general options, VMware remote console options, the VMware tools option, power management options, boot options, and advanced and fibre channel NPIV settings. Let's see the step-by-step procedure to configure each option available under virtual machine options.

The steps for configuring the virtual machine's general options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **VM Options** tab and click on **General Options** to expand its configuration options.
3. Enter the virtual machine's name in the **VM Name** option if you want to edit the virtual machine.
4. Verify **VM Config File** and **VM Working Location**.
5. Verify **Guest OS** and **Guest OS Version** of the virtual machine.
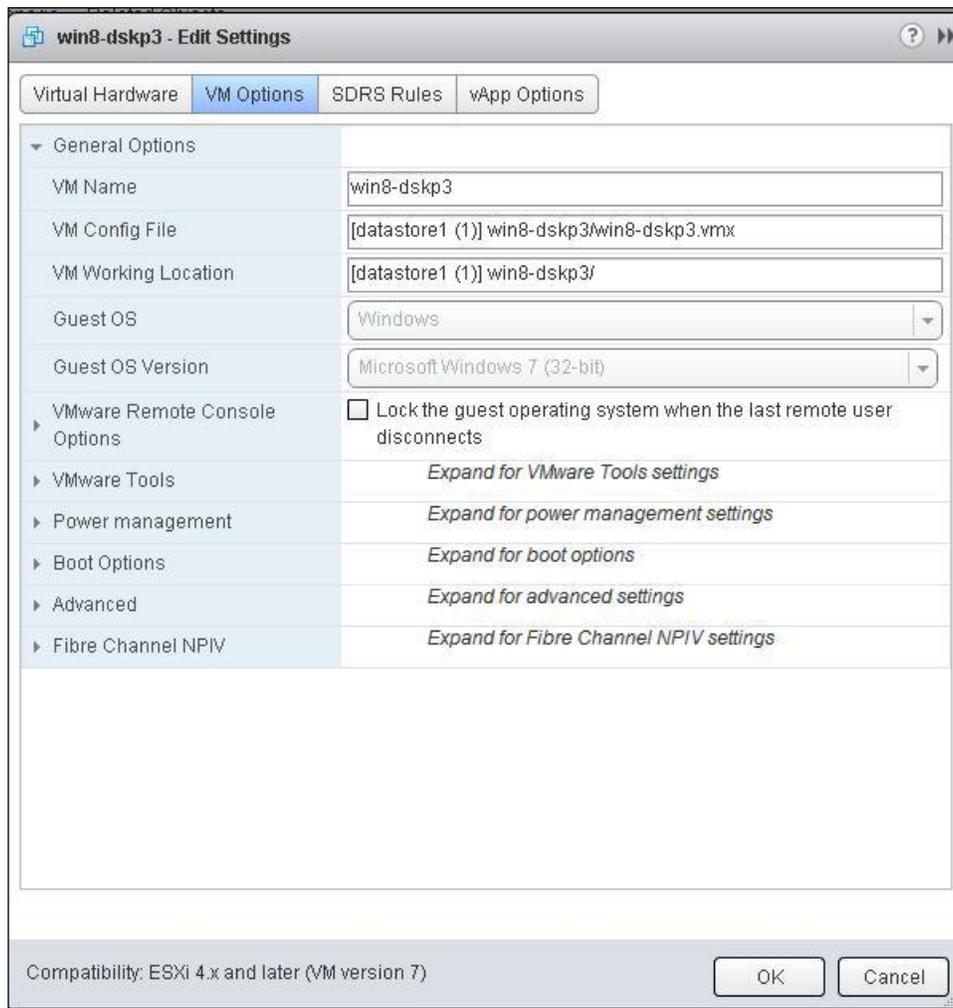
6. Click on **OK** to apply the settings.

The steps for configuring VMware remote console options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **VMware Remote Console options** to expand its configuration options.

3. Select the **Lock the guest operating system when the last remote user disconnects** checkbox in the **Guest OS lock** option if you want to configure this option.

4. Select the checkbox named **Limit the number of simultaneous connections to this virtual machine** and enter the value for the simultaneous connection in the **Maximum number of sessions** option.
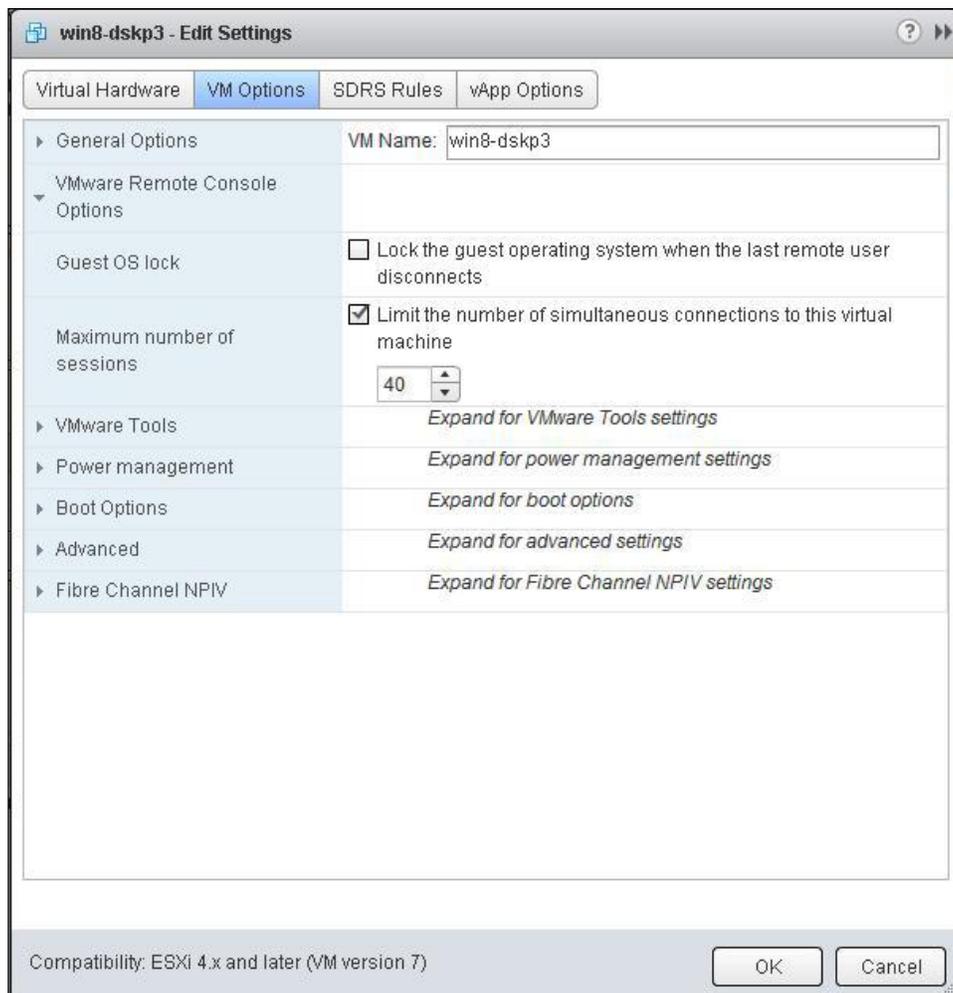
5. Click on **OK** to apply the settings.

The steps for configuring the VMware tools' options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **VM Options** tab and click on the **VMware Tools** option to expand its configuration options.
3. Select one of the following actions from the drop-down menu when you click on the **Power Off** button:
    - ❑ **Power Off**
    - ❑ **Shutdown Guest**
    - ❑ **Default (The current value of the system settings appears in parentheses)**
4. Select one of the following actions from the drop-down menu when you click on the **Suspend** button:
    - ❑ **Suspend**
    - ❑ **Default (The current value of the system settings appears in parentheses)**
5. Select one of the following actions from the drop-down menu when you click on the **Reset** button:
    - ❑ **Reset**
    - ❑ **Restart Guest**
    - ❑ **Default (The current value of the system settings appears in parentheses)**
6. Select the following checkboxes to control when the VMware tools script runs in the **Run VMware Tools Scripts** option:
    - ❑ **After powering on**
    - ❑ **After resuming**
    - ❑ **Before suspending**
    - ❑ **Before shutting down guest**
7. Select the **Check and upgrade VMware Tools before each power on** checkbox in the **Tools upgrades** option if you want to configure the virtual machines to automatically update VMware tools before the virtual machines start.

8. Select the **Synchronize guest time with host** checkbox if you want to synchronize the guest operating system's time with your ESXi host using the help of VMware tools installed on the guest operating system.
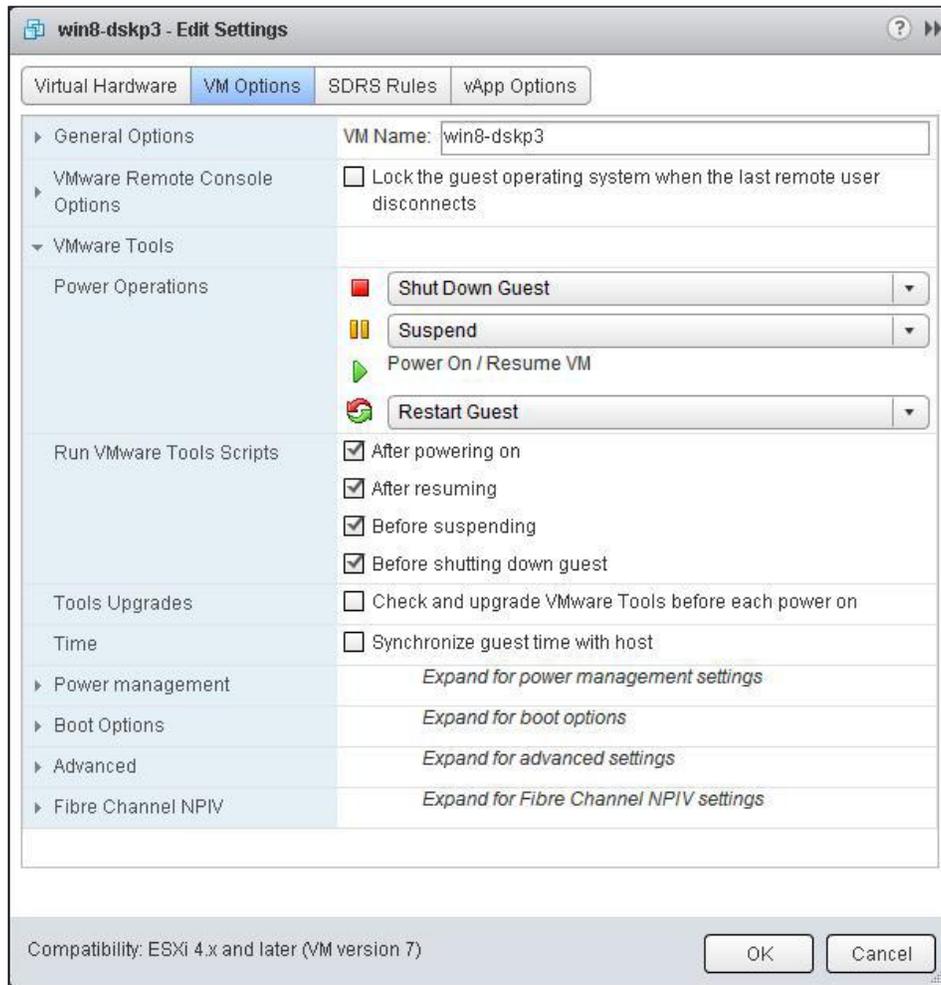
9. Click on **OK** to apply the settings.

The steps for configuring the Power management options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on the **Power Management** option to expand its configuration options.

3. Select one of the following options for **How should the virtual machine respond when the guest is** under the **Standby response** option:

   ❑ **Suspend the virtual machine.**

   ❑ **Put the guest OS into standby mode and leave the virtual machine powered on.**

4. Select the **VM Options** tab and click on the **Power Management** option to expand its configuration options.

5. Select the **Wake on LAN for virtual machine traffic on:** option and the virtual network adapter to trigger this action.
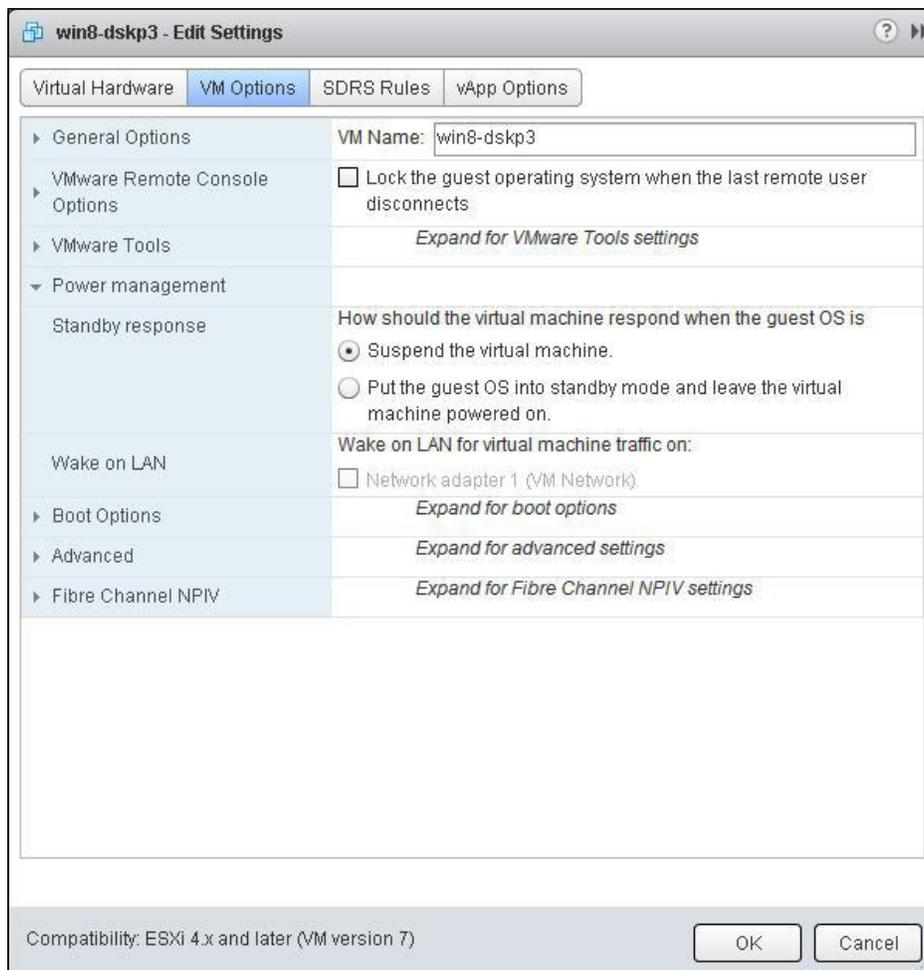
6. Click on **OK** to apply the settings.

The steps for configuring the virtual machine boot options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **VM Options** tab and click on **Boot Options** to expand its configuration options.
3. Select the **Choose which firmware should be used to boot the virtual machine** option from the drop-down in the **Firmware** option.
4. Enter the value in milliseconds to delay the boot order whenever the virtual machine is powered on or reset in the **Boot Delay** option.
5. Select the **The next time the virtual machine boots, force entry into the BIOS setup screen** checkbox in the **Boot Delay** option if you want the virtual machine to boot into BIOS setup during the next boot time.
6. Select the **When the virtual machine fails to find a boot device, automatically retry boot after** checkbox if you want to restart the virtual machine to fix the boot failures. Enter the value in seconds to retry after a specific time.
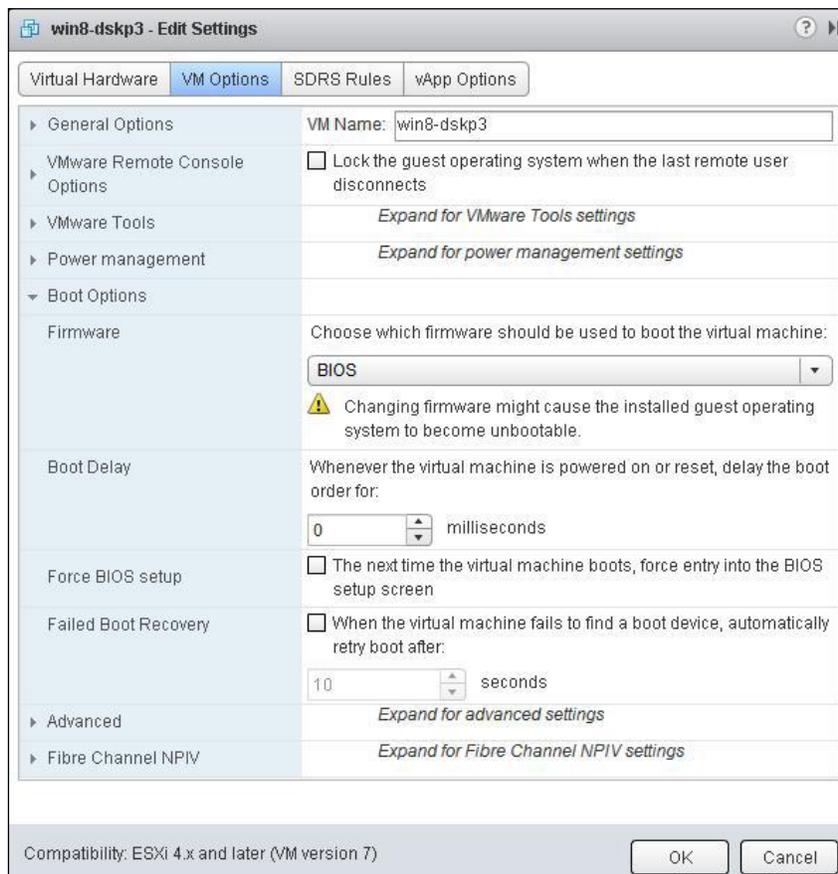
7. Click on **OK** to apply the settings.

The steps for configuring the virtual machine's advanced options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **Advanced Options** to expand its configuration option.

3. Select the **Disable acceleration** checkbox in the settings option. VMware server appears to be hung when you install or run software inside a virtual machine.

4. Select the **Enable logging** checkbox to collect log-files to help in troubleshooting the virtual machine.

5. Select one of the following options from the drop-down menu to configure the virtual machine to collect the additional debugging information in the **Debugging and statistics** option:

   ❑ Run normally

   ❑ Record debugging information

   ❑ Record statistics

   ❑ Record statistics and debugging information

6. Select one of the following options to choose the virtual machine's **swap file location**:

   ❑ **Virtual machine directory**: This option allows you to store the swap files of the virtual machine in the same directory as that of the virtual machine.

   ❑ **Datastore specified by host**: With this option, the virtual machine's swap files can be stored in the datastore specified by the host to be used for swap files. If not possible, you can store the swap files in the virtual machine's directory.

> Using a datastore that is not visible to both the hosts during vMotion might affect the vMotion's performance for the affected virtual machines.
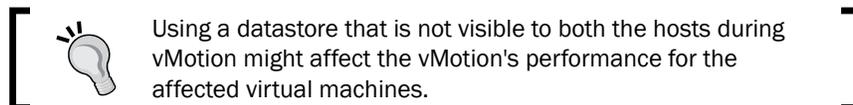
7. Click on **Edit Configuration** in the configuration parameters. Click on **Add row**, and enter the name and value to add the virtual machine's advanced configuration options.

8. Select one of the following options from the drop-down menu in the **Latency Sensitivity** option. This option can be used to adjust the latency sensitivity of a virtual machine, which is used to optimize the scheduling delay for latency sensitive applications.

   ❑ **Low**

   ❑ **Normal**

   ❑ **Medium**

❑ **High**

❑ **Custom**

The advanced VM options are shown in the following screenshot:
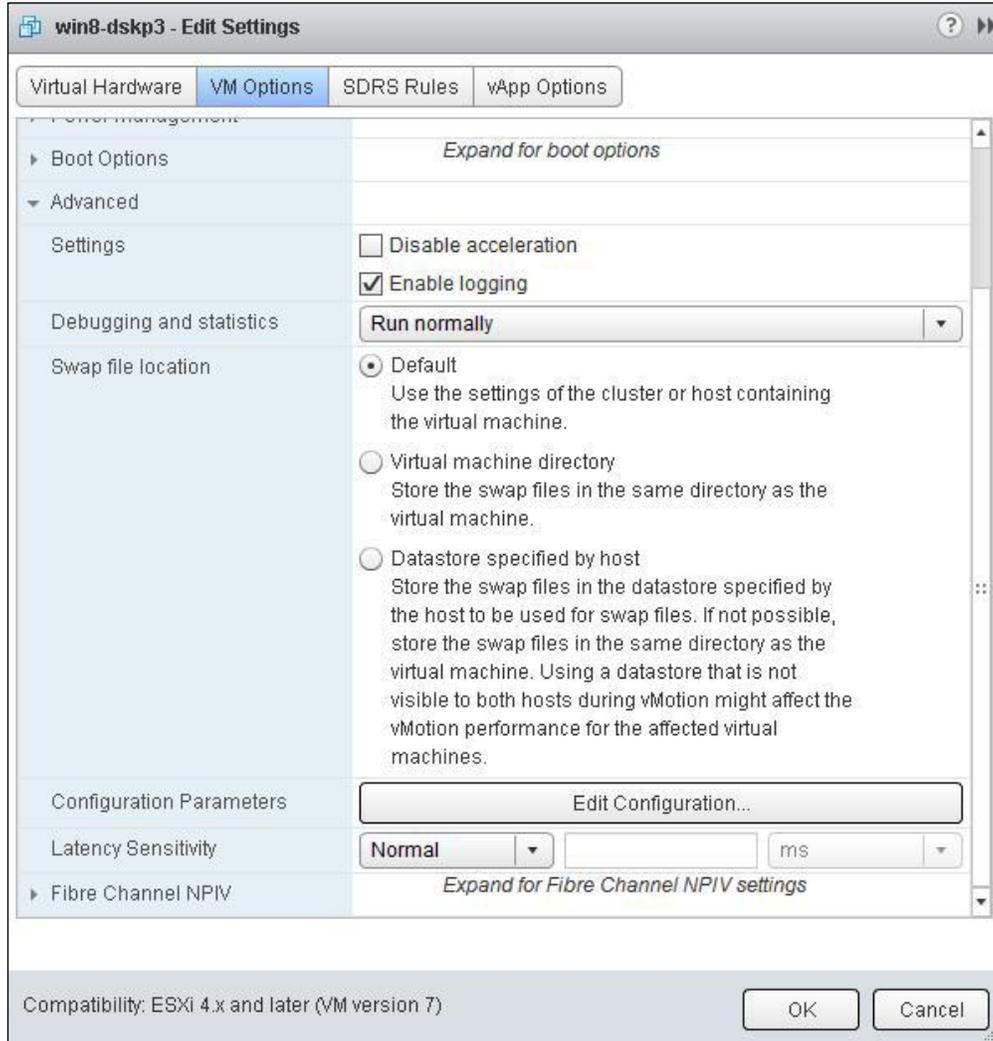
9. Click on **OK** to apply the settings.

There's more...

The steps for configuring the fibre channel NPIV options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **Fibre Channel NPIV** to expand its configuration options.

3. Unselect the **Temporarily disable NPIV for this virtual machine** checkbox.

4. Select **Generate WWNs** and specify the number of WWNs and WWPNs.

5. Click on **OK**. Note down the WWNs generated to provide storage access to the virtual machine.

6. Configure your storage to provide access to the virtual WWNs so that the virtual machine can access the storage LUNs directly with the use of virtual WWNs.

7. Click on **OK** to apply the settings.
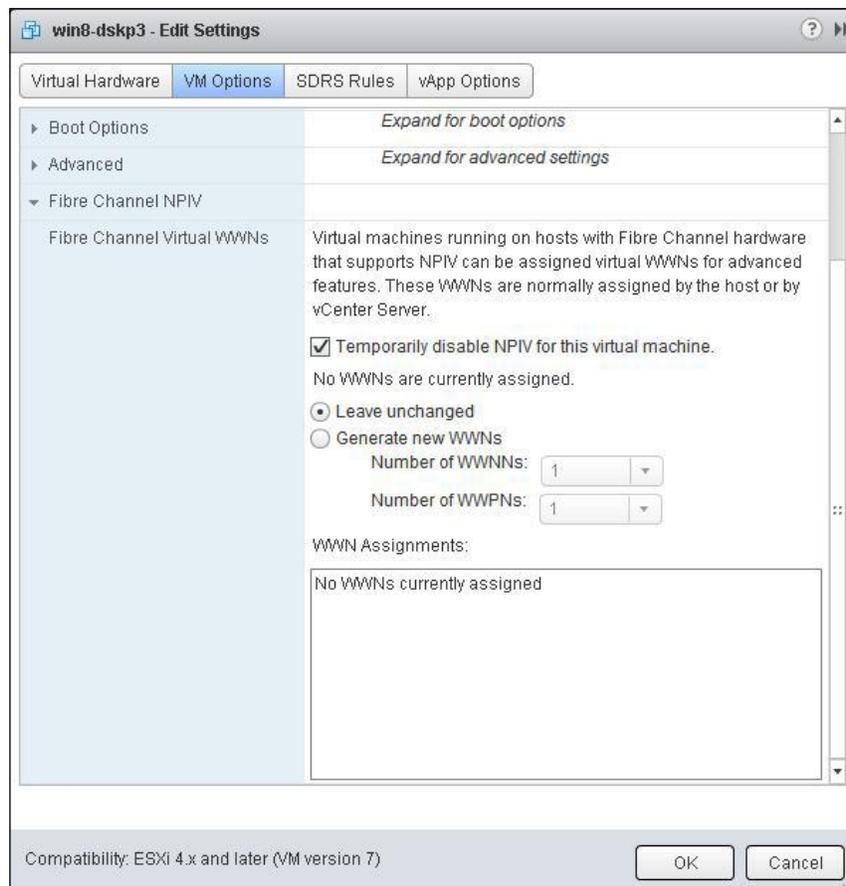
Creating snapshots, templates, and clones

Snapshots of the virtual machine can be used to preserve the state and data of the virtual machine at the time you take the snapshot. Snapshots are most useful when you want to revert back to the original state of the virtual machine in case of its failure due to software or patch installation. You can take multiple snapshots to create multiple restoration points, but it is not recommended to use snapshots as a backup of the virtual machine.

Templates can be used to deploy a fully configured virtual machine to avoid the repetitive installation and configuration of the guest OS and applications. You can configure one of the virtual machines with the guest OS application, and install all the required software such as monitoring, antivirus, backup, and other management software including required patches and software updates. This fully configured virtual machine can be converted to a template. This virtual machine template can act as a golden image, which can be used to deploy multiple virtual machines as per your organization requirements very quickly.

A **clone** is an exact copy of the virtual machine including all its settings, virtual devices, installed software, and contents of the virtual machine disks. Cloning a virtual machine saves a lot of time if you want to deploy many similar virtual machines. You can use a guest customization wizard to customize the deployed virtual machine's guest operating system settings such as computer name and network settings to avoid conflicts due to identical network settings.

Getting ready

Connect to your vCenter Server via the vSphere Web Client and browse to your virtual machine in the vSphere Web Client.

How to do it...

One of the important operational tasks of a virtual machine is to manage the virtual machine's snapshots. We will see a step-by-step procedure to manage various virtual machine snapshot operations such as creating, reverting, deleting, and consolidating snapshots.

The steps for taking a snapshot of the virtual machine are as follows:

1. Right-click on your virtual machine and select **Take Snapshot** to open **Snapshot Manager**.
2. Enter the name for the virtual machine's snapshot.

3. Type the description for this virtual machine's snapshot.

4. Select the **Snapshot the virtual machine's memory** checkbox to capture the memory of the virtual machine. This option is only available when the virtual machine is powered on.

5. Select the **Quiesce the guest file system (Needs VMware Tools installed)** checkbox. This option pauses all the running processes on the guest operating system so that the file system's contents in the guest operating system are aware about when you take the snapshot. This option is only available when the virtual machine is powered on.
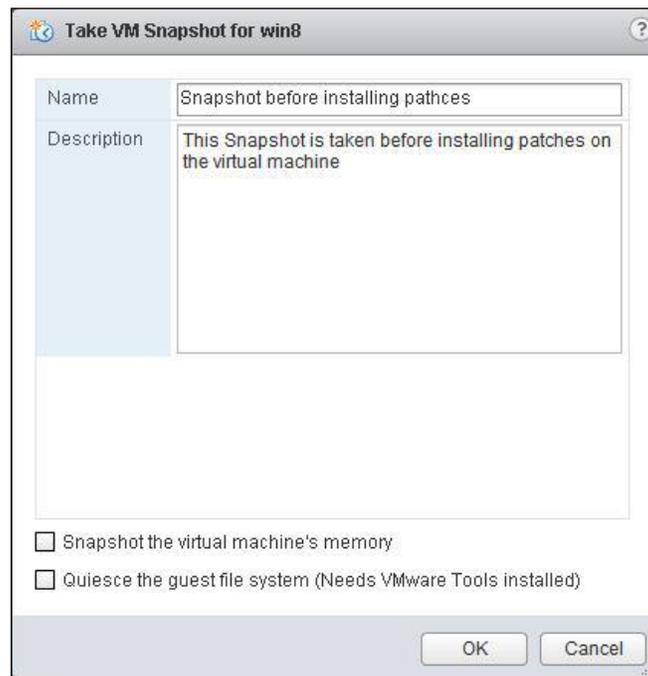
6. Click on **OK** to create a snapshot.

The steps for reverting to a snapshot of the virtual machine are as follows:

1. Right-click on your virtual machine and select **Manage Snapshots** to open the Snapshot Manager.

2. Select one of the snapshots from the Snapshot Manager to revert to.

3. Click on **Go to** in order to revert the virtual machine to the selected snapshot.

4. Click on **Yes** to confirm going to the snapshot. It will display the message **Current state of the virtual machine will be lost unless it is saved in a snapshot. Revert to snapshot "Snapshot name"?**.

5. Click on **Close** to exit from the snapshot manager.

Deleting the snapshot option will remove a single parent or child snapshot of the virtual machine from the snapshot tree. The delete operation writes the disk changes between the snapshot and the previous delta disk state to the parent snapshot. Deleting snapshot can be used to remove a corrupted snapshot from the snapshot tree without merging them with the parent snapshot. The steps for deleting a snapshot of the virtual machine are as follows:

1. Right-click on your virtual machine and select **Manage Snapshots** to open the Snapshot Manager.

2. Select one of the snapshots from the snapshot manager to delete.

3. Click on **Delete** to delete that particular snapshot.

4. Click on **Yes** to confirm the delete operation. It will display the message **Are you sure want to delete the snapshot "snapshot name"?**

5. Click on **Close** to exit from the snapshot manager.

The **Deleting All** option will delete all the snapshots of the virtual machine from the Snapshot Manager. The **Delete All** option consolidates and writes the changes between snapshots and previous delta disk states to the base parent disk of the virtual machine and merges them with the base virtual machine disk. The steps for deleting all snapshots of the virtual machine are as follows:

1. Right-click on your virtual machine and select **Manage Snapshots** to open the Snapshot Manager.

2. Select one of the snapshots from the snapshot manager to delete.

3. Click on **Delete** to delete that particular snapshot.

4. Click on **Yes** to confirm the delete operation. It will display the message **Are you sure you want to delete the snapshot "snapshot name"?**.
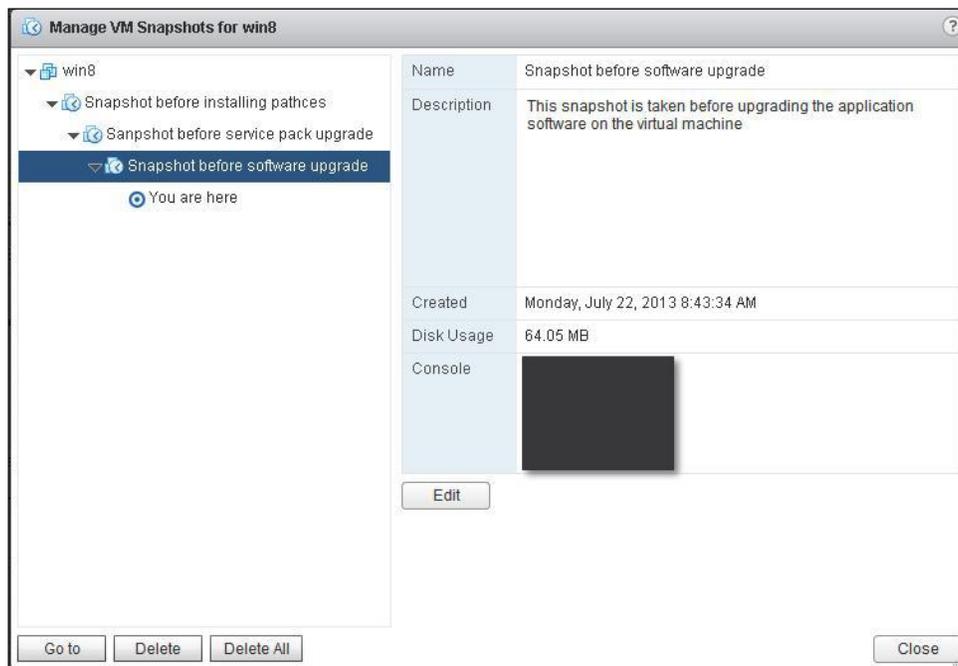
5. Click on **Close** to exit from the snapshot manager.

The **Consolidate** snapshot option removes the redundant disks by combining redundant delta disks without violating a data dependency. After the snapshot consolidation, redundant disks are removed, which improves the virtual machine's performance. The **Consolidation** option is useful when snapshot disks fail to compress after the delete or delete all operation. The steps for consolidating a snapshot of the virtual machine are as follows:

1. Right-click on your virtual machine and select **All vCenter Actions**.
2. Click on **Snapshots** and select **Consolidate**.
3. Verify the **Needs Consolidation** column to verify the task status.

How it works...

Snapshot preserves the disk state of the virtual machine taken at a specific time by creating delta disks for each attached virtual disk. Snapshot can be optionally used to preserve the memory and power state of the virtual machine by creating a memory file. Snapshot creates a `delta.vmdk` disk file. Snapshot prevents the virtual machine's guest operating system from writing to the base `.vmdk` file; instead, it redirects all the write requests to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time the virtual machine's previous snapshot was taken. When you create a snapshot, the list of files such as `.vmdk`, `-delta.vmdk`, `.vmsd`, and `.vmsn` will be created in the virtual machine directory.

There's more...

You can create an exact copy of the existing virtual machine as a template using this **Clone to Template...** option, as shown in the following steps. This can be used to modify the cloned template by installing software or upgrading the guest OS without disturbing the actual virtual machine or template.

1. Right-click on your virtual machine and select **All vCenter Actions**.
2. Select **Template** and click on **Clone to Template**.
3. Enter the name for the template and select a **location either datastore or VM folder** location for the new template.
4. Select either **cluster** or **host** to store this template in.
5. Select the **Datastore** to place this template.
6. Review the selected settings and click on **Finish** to create a clone of the template.

You can convert a virtual machine to a template. This option can be used to convert your virtual machine after installing the software and configure the guest OS as per your organization policy to a template. This template will act as a golden image to deploy virtual machines as per the organization's requirements. The steps for converting a VM to a template are as follows:

1. Right-click on your virtual machine and select **All vCenter Actions**.
2. Select **Template** and click on **Convert to Template**.
3. Verify that **Mark virtual machine as Template task** is completed in **Recent tasks**.

The **Clone a virtual machine** option allows you to create an exact copy of the existing virtual machine. The steps for cloning a virtual machine are as follows:

1. Browse to your cluster or ESXi host in the vSphere Web Client.
2. Right-click on the cluster or the ESXi host and select **New virtual machine**.

3. Select the **Clone an existing virtual machine** option from the **Select a creation type** page.

4. Select a virtual machine to clone the new virtual machine from and optionally choose the following options **Customize the operating system, Customize this virtual machine hardware and Power on virtual machine after creation**.

5. Enter the name for the virtual machine and choose the **location** option for the virtual machine.

6. Select a compute resource such as **cluster, host, vApp, or resource pool** to run this virtual machine.

7. Select the **Datastore** option to store the virtual machine.

8. Customize **Guest OS** and **virtual hardware** if required.

9. Review the selected options and click on **Finish** to create the new virtual machine.

7

Securing the ESXi Server and Virtual Machines

In this chapter, we will cover the following topics:

- ▶ Configuring the ESXi firewall
- ▶ Enabling the Lockdown mode
- ▶ Managing the ESXi authentication
- ▶ Managing the ESXi certificates
- ▶ Configuring logging for virtual machines
- ▶ Configuring security settings for virtual machines

Introduction

The ESXi hypervisor is designed and developed by keeping strong security in mind. ESXi is designed with very limited services and small attack surface compared to the ESX hypervisors. You can even customize the ESXi host to match with the compliance of your organization by performing additional hardening. Virtual machines are like the containers that hold guest operating systems and applications. All virtual machines are isolated from one another. This isolation ensures that multiple virtual machines can run securely while sharing the physical hardware. A virtual machine configuration file can be tweaked to disable unnecessary features and also to improve the security layer of the virtual machine.

Configuring the ESXi firewall

The ESXi firewall acts as a firewall between the management interface (VMkernel) and the external network. The ESXi firewall is enabled by default. The ESXi firewall will block incoming and outgoing traffic except the traffic for the default services. **Internet Control Message Protocol** (**ICMP**), **Domain Name System** (**DNS)**, and **Dynamic Host Configuration Protocol** (**DHCP)** communications are allowed in the ESXi firewall by default.

A Firewall Configuration file called `Service.xml` is stored at `/etc/vmware/firewall/`. This file contains the firewall rules and its relationship with ports and protocols. The supported services and agents that are required to operate the ESXi host are described in the rule-set configuration file.

Getting ready

Connect to your VMware vCenter Server using vSphere Web Client and browse to your ESXi host in vSphere Web Client.

How to do it...

We'll see a step-by-step procedure on how to configure the ESXi firewall from vSphere Web Client.

The steps for configuring the ESXi firewall to allow or deny access to services and agents are as follows:

1. Select your ESXi host from the vSphere Web Client.
2. Click on the **Manage** tab and select the **Settings** option.
3. Select **Security Profile** and click on **Edit** under the **Firewall** section. A list of active incoming and outgoing connections with the corresponding firewall ports will be displayed in vSphere Web Client.

4. Select the checkbox to provide access to a service or client or uncheck the checkbox to disable the rule-sets. The **Incoming Ports** column indicates the ports that vSphere Web Client opens for the service for incoming connections and **Outgoing ports** indicates the ports that vSphere Web Client opens for the service for outgoing connections. The **Protocols** column indicates the protocol that the service uses. The **Daemon** column indicates the status of the service daemons associated with the service:

5. Click on **OK** to apply the settings.

The steps for configuring service or client startup options in the ESXi host are as follows. These steps allow you to control the service startup options for the services in the ESXi host.

1. Select your ESXi host in vSphere Web Client.
2. Click on the **Manage** tab and select the **Settings** option.
3. Select **Security Profile** and click on **Edit** under the **Services** section.
4. Select the service or management agent to configure the startup options.
5. Click on **Service Details** to expand its configuration options.
6. You will be able to **Start**, **Stop**, or **Restart** the selected **Service Status** option.

7. Select a **Startup policy** for the service from the drop-down menu:

    ❑ **Start and stop with host**: This options allows you to start and stop the service along with the ESXi host.

    ❑ **Start and stop manually**: This option allows you to start and stop the service manually.

    ❑ **Start and stop with port usage**: This option ensures that the service starts automatically if any ports are open, and stops when all ports are closed.
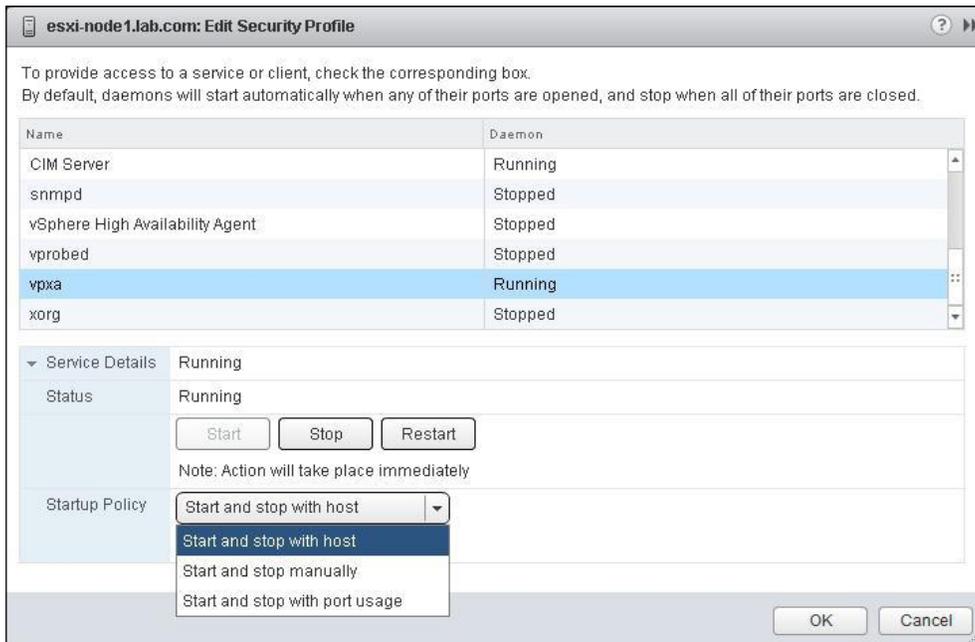
8. Click on **OK** to apply the settings.

The steps for configuring the allowed IP address for services in the ESXi firewall are as follows. This option allows you to specify the range of IP addresses or any specific IP address as the allowed IP address for services in the ESXi firewall.

1. Select your ESXi host in vSphere Web Client.

2. Click on the **Manage** tab and select the **Settings** option.

3. Select **Security Profile** and click on **Edit** under the **Firewall** section.

4. Select the Service or management agent to configure the startup options.

5. Click on **Allowed IP Addresses** to expand its configuration options.

6. Select one of the following options to configure **Allowed IP address** for the selected service:

   ❑ **Allow connections from any IP address checkbox**: This option allows connections from any IP address to connect to the selected service of the ESXi host.

   ❑ **Allow connections from any IP address**: With this option, connections are not allowed from any IP address. You can manually specify the IP address to allow connections from.
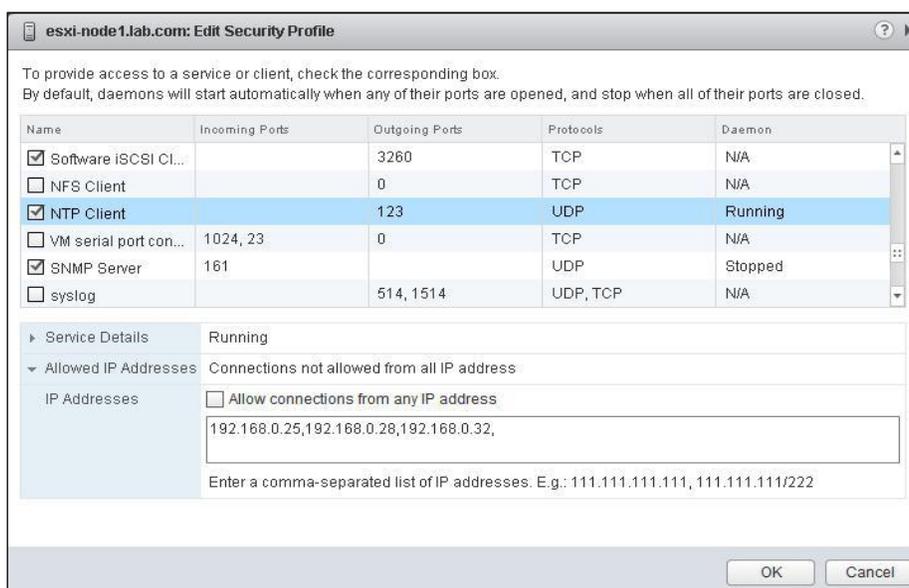
7. Click on **OK** to apply the settings.

The steps for creating custom firewall rules in the ESXi server are as follows. You can add the custom firewall rules for the ESXi host in the rule-set configuration file. We'll see the step-by-step procedure of how to add a custom firewall rule in the firewall rule-set configuration file:

1. Connect to your ESXi host using the SSH connection.

2. Before editing the firewall configuration file, back up the `service.xml` file by running the following command:

   ```
   cp /etc/vmware/firewall/service.xml /etc/vmware/firewall/service.xml.bak
   ```

3. Modify the permission for the `service.xml` file to allow writes to the file using the following command:

   ```
   chmod 644 /etc/vmware/firewall/service.xml
   ```

4. Edit the `service.xml` file using text editor:

   ```
   vi /etc/vmware/firewall/service.xml
   ```

5. Add the rule for your custom service named `Myservice` in the `service.xml` file in the following format. The following command is only an example. You can add the rule for your required custom service in the ESXi firewall in the following format along with the inbound and outbound ports for your service:

   ```
   <service id='0033'>
     <id>Myservice</id>
     <rule id='0000'>
       <direction>inbound</direction>
       <protocol>tcp</protocol>
       <porttype>dst</porttype>
       <port>922</port>
     </rule>
     <rule id='0001'>
       <direction>inbound</direction>
       <protocol>tcp</protocol>
       <porttype>dst</porttype>
       <port>933</port>
     </rule>
     <enabled>true</enabled>
     <required>true</required>
   </service>
   ```

6. Save the `service.xml` file after the edit.

7. Enter the following command to refresh the firewall rules for the changes to take effect:

   ```
   esxcli network firewall refresh
   ```

There's more...

The steps for managing the ESXi firewall using command line are as follows:

▸ The following is the command to list the status of the firewall whether it is enabled or disabled, loaded or not loaded:

```
esxcli network firewall get
```

▸ To enable the ESXi firewall use the following command:

```
esxcli network firewall set -e true
```

▸ To disable the ESXi firewall use the following command:

```
esxcli network firewall set -e false
```

▶ To load the firewall module and rule-set configuration files use the following command:

```
esxcli network firewall load
```

▶ To unload the firewall module and destroy the filters use the following command:

```
esxcli network firewall unload
```

▶ To list the rule-sets information use the following command:

```
esxcli network firewall ruleset list
```

▶ To enable the specific ruleset named `ntpclient` use the following command :

```
esxcli network firewall ruleset set -r ntpClient -e true
```

▶ To disable the specific ruleset named `ntpclient` use the following command:

```
esxcli network firewall ruleset set -r ntpClient -e false
```

▶ To configure all the allowed IP address for rule-set named `ntpclinet`, set allowed all IP list to `true` and set it to `false` to use the allowed IP list:

```
esxcli network firewall ruleset set -r ntpClient -a true
esxcli network firewall ruleset set -r ntpClient -a false
```

▶ To specify the IP address or range of IP address to allow access to the rule-set named `ntpclient` use the following command:

```
esxcli network firewall ruleset allowedip add -i 192.168.0.22 -r
ntpClient
```

▶ To list the allowed IP addresses for the specific rule-set `ntpClient` use the following command:

```
esxcli network firewall ruleset allowedip list -r ntpClient
```

Enabling the Lockdown mode

The ESXi Lockdown Mode increases the security by preventing all users other than vpxuser to have authentication permission for performing operations against the ESXi host directly. The Lockdown Mode enforces to perform all the operations through vCenter Server. You will not even be able to manage the ESXi host from vSphere CLI commands, from a script, or from **VMware Management Assistant** (**vMA**) when Lockdown Mode is enabled. When Lockdown Mode is enabled, external monitoring or management tools might also be unable to retrieve the information of the ESXi hosts that are not managed by the vCenter Server.

Getting ready

Connect to your VMware vCenter Server using the vSphere Web Client. Browse to your ESXi host in the vSphere Web Client.

How to do it...

We'll see the step-by-step procedure of various methods to enable the ESXi Lockdown mode.

The steps for enabling Lockdown mode in the ESXi host from vSphere Web Client are as follows:

1. Select your ESXi host in the vSphere Web Client.
2. Click on the **Manage** tab and select the **Settings** option.
3. Select **Security Profile** and click on **Edit** in the **Lockdown Mode** section.
4. Select the checkbox **Enable Lockdown Mode**:
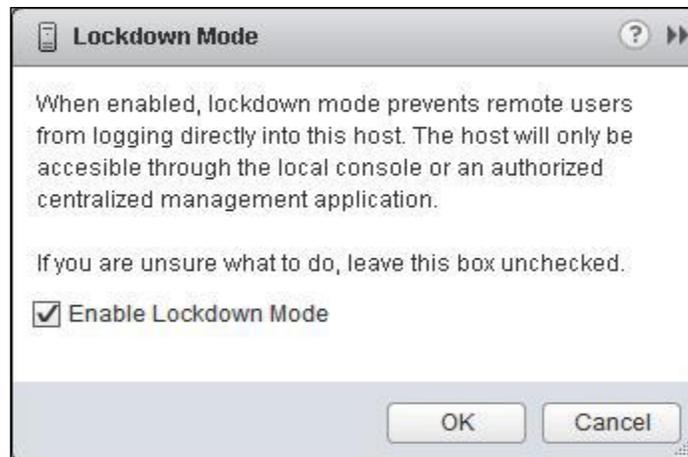
5. Click on **OK** to apply the settings.

The steps for enabling **Lockdown Mode from Direct Console User Interface** (**DCUI**) are as follows:

1. Connect to the physical console of your ESXi server.
2. Press *F2* to log in to your ESXi from DCUI.
3. Scroll down and select **Configure Lockdown Mode**.
4. Press *Enter* to enable or disable the Lockdown Mode.

```
System Customization                        Configure Lockdown Mode

Configure Password                          Disabled
Configure Lockdown Mode
                                            When enabled, lockdown mode prevents users from logging
Configure Management Network                directly into this host. The host will only be accessible
Restart Management Network                  through this local console or an authorized centralized
Test Management Network                     management application.
Network Restore Options

Configure Keyboard
Troubleshooting Options

View System Logs

View Support Information

Reset System Configuration




<Up/Down> Select                            <Enter> Change                        <Esc> Log Out
                      VMware ESXi 5.1.0 (VMKernel Release Build 799733)
```

5. Press *Esc* to log out from the DCUI.

How it works...

The ESXi Lockdown Mode controls which users are authorized to access the host services. Users who were connected to the ESXi host before the Lockdown Mode was enabled, will remain logged in and able to execute the commands; however, these users cannot disable the Lockdown Mode during that time. No other users including root users and users with administrative roles on the host can use the ESXi shell to log in to an ESXi host in Lockdown Mode. Users who have administrative privileges on the vCenter Server can disable the Lockdown Mode for the ESXi hosts that are managed by that vCenter Server using vSphere Client or vSphere Web Client. Apart from that, only users assigned with DCUI access to the ESXi host can log in directly to the ESXi host via DCUI to disable the Lockdown Mode.

There's more...

The steps for enabling Lockdown mode from the command line are as follows:

▶ The command to check the status of Lockdown mode is as follows:

```
vim-cmd -U dcui vimsvc/auth/lockdown_is_enabled
```

▸ The command to enable the Lockdown mode in the ESXi server is as follows:

```
vim-cmd -U dcui vimsvc/auth/lockdown_mode_enter
```

▸ The command to disable the Lockdown mode in the ESXi server is as follows:

```
vim-cmd -U dcui vimsvc/auth/lockdown_mode_exit
```

Managing ESXi authentication

Handling user authentication and user permissions of local users of the ESXi host can be managed directly by the ESXi host. vCenter single sign-on cannot handle the authentication of the local user accounts of the ESXi host. Also, you will not be able to create a local user account of the ESXi host from the vCenter Server. You must connect to the ESXi host directly using the vSphere client to create a local user account because the vCenter Server is not aware of the local user account of the ESXi host. However, you can configure your ESXi host to authenticate with the Windows Active Directory Domain by joining the ESXi host to the windows domain. This option allows you to maintain the same group of users to be available to the ESXi host and also to the vCenter Server.

Getting ready

Connect to your ESXi host directly using the vSphere client.

How to do it...

We will take a look at creating local user accounts of the ESXi host and also how to configure active directory authentication for the ESXi host.

The steps for creating the local ESXi user account is as follows:

1. Click on **Local Users & Groups** and select **Users**.
2. Right-click on the empty space and select **Add**.
3. Enter the login name information for the local user account.
4. Provide the username. The UID is optional.
5. Enter the password for the local user account.
6. Select the checkbox **Grant shell access to this user**, if you want to provide the user shell access to your ESXi host.

7. Click on **OK** to create the user account.

The steps for modifying the local ESXi user account are as follows;

1. Click on **Local Users & Groups** and select **Users**.
2. Right-click on the user account to modify and select **Edit**.
3. Modify user **Properties & password** for the user account.
4. Click on **OK** to apply the settings.

The steps for removing the local ESXi user account are as follows:

1. Click on **Local Users & Groups** and select **Users**.
2. Right-click on the user account to remove and select **Remove**.
3. Click on **Yes** to remove the user account from the ESXi host.

The steps for configuring DNS and routing for the ESXi host are as follows:

1. Connect to your vCenter Server using the vSphere Web Client.
2. Browse to your ESXi host in the vSphere Web Client.
3. Select the ESXi host and click on the **Manage** tab.

4. Select the **DNS and Routing** tab and click on **Edit**.

5. Select one of the options: **Obtain settings automatically from the virtual network adapter** or **Enter Settings Manually**.

6. Enter the following settings manually for the ESXi host:

   ❑ **Host name**

   ❑ **Domain**

   ❑ **Preferred DNS server**

   ❑ **Alternate DNS server**

   ❑ **Search domains**
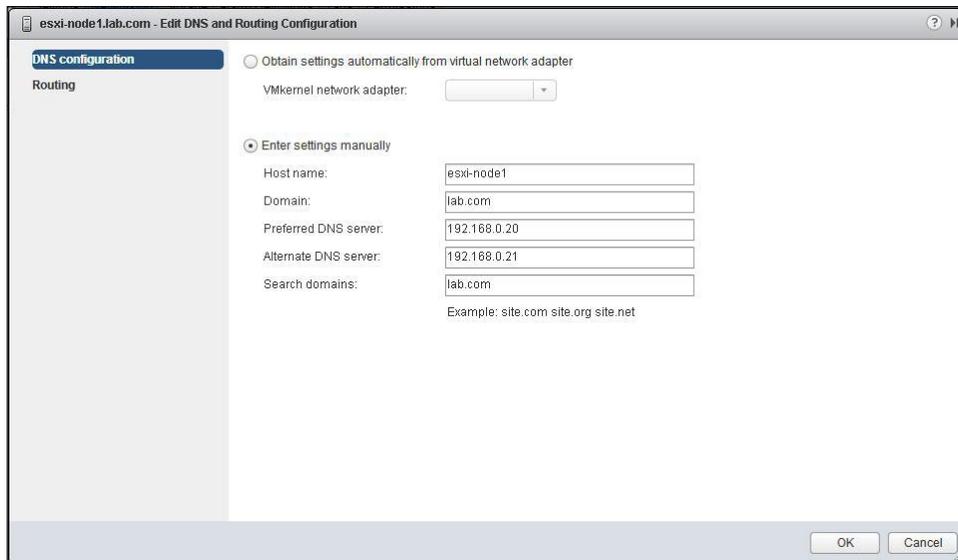
7. Click on **OK** to apply the settings.

The steps for adding the ESXi host to the Active Directory Domain are as follows:

1. Browse to your ESXi host in the vSphere Web Client.

2. Select the ESXi host and click on the **Manage** tab.

3. Select the **Settings** tab and choose **Authentication Services**.

4. Click on **Join Domain** and enter the **Domain name**.

5. Enter the `Username and password` for all the user accounts that have permission to join the host to the domain.

6. Click on **OK** to join the ESXi host to the Active Directory Domain.

7. Once the **Join Windows Domain** task is completed, verify whether the **Directory Services type** has changed to **Active Directory**.

There's more...

DCUI access can be used to specify which users can log in to an ESXi host that is in Lockdown Mode. Users with DCUI access do not need to have administrative privileges on the ESXi host. Root users can log in to DUCI on the ESXi host with the Lockdown Mode enabled in earlier versions of vSphere. In vSphere 5.1, you can specify which local ESXi users can log in to the DCUI when the host is in the Lockdown Mode. This ensures that the users with DCUI access can perform operations on the ESXi host with Lockdown Mode enabled.

The steps for providing user access to DCUI of the ESXi host are as follows:

1. Browse to your ESXi host in the vSphere Web Client.
2. Select the ESXi host and click on the **Manage** tab.
3. Select the **Settings** tab and choose **Advanced System Settings**.
4. Select the settings **DCUI.Access** and click on **Edit**.

5. Enter one or more comma-separated local users next to **DCUI Access:** which are granted unconditional access to DCUI, even if they don't have administrator role on the host:

6. Click on **OK** to apply the settings.

Managing ESXi certificates

Certificates play a major role in encrypting the session information. ESXi and vCenter Server support **Standard X.509 Version 3** (**X.509v3**) certificates, which is used to encrypt the session information between the connections sent over **Secure Socket Layer** (**SSL**) protocol. If SSL is enabled, the data sent over will be protected and cannot be modified during transit. SSL certificates are used to encrypt the network traffic. Certificate checking is enabled by default. vCenter Server uses the default automatically generated certificates that are created and stored with the servers during the installation. These certificates are unique but they are not verified and signed by a trusted **certificate authority** (**CA**). Default certificates may be vulnerable to possible man-in-the-middle attacks. To overcome this issue, you can generate the certificates from the certificate authority and replace the default certificates of the ESXi hosts and vCenter Server with the certificates generated.

Getting ready

Connect to your vCenter Server via the vSphere Web Client login.

How to do it...

We will take a look at the step-by-step procedure to generate certificates and enable certificate checking for the ESXi hosts.

The steps for generating new certificates for the ESXi host are as follows. This option will allow you to regenerate the default ESXi host certificates.

1. Connect to your ESXi host using the SSH connection with root credentials.

2. Browse to the location `/etc/vmware/ssl` using the following command:

   ```
   cd /etc/vmware/ssl
   ```

3. Make sure you have taken a backup of the existing certificates by renaming them using the following command:

   ```
   mv rui.crt backup.rui.crt
   mv rui.key backup.rui.key
   ```

4. Generate the new certificates by executing the following command:

   ```
   /sbin/generate-certificates
   ```

5. Make sure the new certificates are generated and verify `rui.crt` and `rui.key` exist at `/etc/vmware/ssl`. Confirm the timestamp of certificates created.

   ```
   ls -l
   ```

6. Restart the ESXi host after new certificates are generated.

> Generating certificates from Trusted Certificate Authority for the ESXi hosts and vCenter Server is out of the scope of this chapter. Once it is generated, replacing the trusted certificates with default certificates can be performed by renaming the default certificates and placing the CA certificates on the ESXi host directory at `/etc/vmware/ssl`.

The steps for enabling certificate checking are as follows:

1. Browse to your vCenter Server in the vSphere Web Client.

2. Click on the **Manage** tab and select the **Settings** option.

3. Under settings, select **General** and click on **Edit**.

4. Select the **SSL Settings** in the **Edit vCenter Server settings** page.

5. Select the checkbox **vCenter requires verified host SSL certificates**. When this option is selected, the vCenter Server will verify the validity of the SSL certificates of the remote hosts when establishing SSL connections. This affects operations such as adding a host to the vCenter Server, connecting to a VM, and making the VM devices remotely available.

6. Select the **Verify** checkbox next to the host, if there are any hosts that require manual validation.
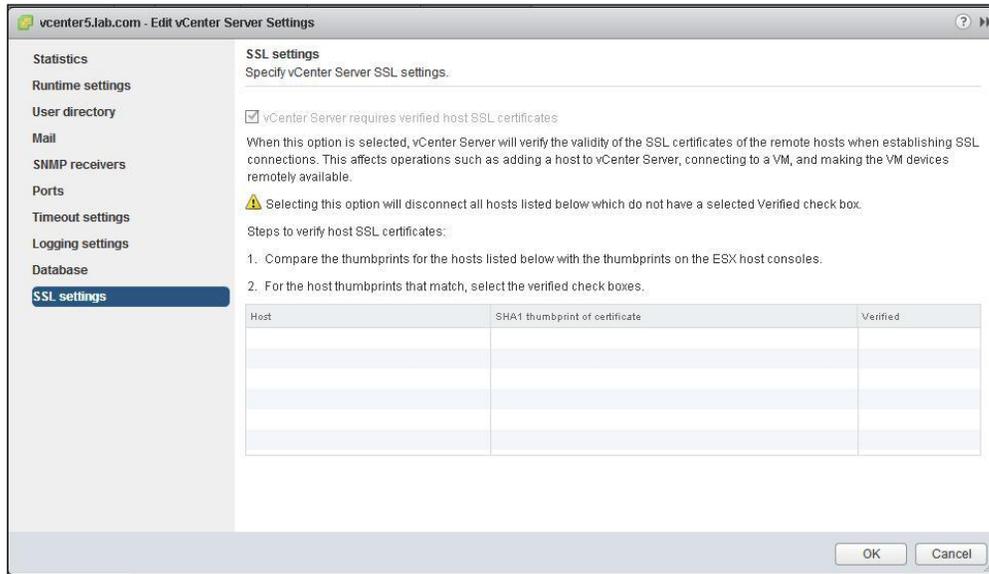
7. Click on **OK**.

There's more...

SSL timeout can be configured to disconnect the idle connections after the timeout period. By default, established SSL connections have a timeout value of infinity. The **Read timeout** settings applies to the connections that have completed the SSL handshake process with port 443 of the ESXi host and the **Handshake timeout** settings applies to connections that have not completed the SSL handshake process with port 443 of the ESXi host.

The steps for configuring SSL timeouts are as follows:

1. Connect to your ESXi host using the SSH connection with root credentials.

2. Browse to `/etc/vmware/rhttpproxy` using the following command:

   ```
   cd /etc/vmware/rhttpproxy/
   ```

3. Edit the `config.xml` file using the text editor:

   ```
   vi config.xml
   ```

4. Configure the read timeout value in milliseconds using the following command. For a 30-second timeout, enter 30000 in the following format:

   ```
   <readTimeoutMs>30000</readTimeoutMs>
   ```

5. Configure the **handshake timeout** value in milliseconds using the following command. For a 30-second timeout, enter 30000 in the following format:

   ```
   <handshakeTimeoutMs>30000</handshakeTimeoutMs>
   ```

6. Save the changes by pressing ESC and type: `wq!`.

7. Restart the `rhttpproxy` process for the changes to take effect using the following command:

   ```
   /etc/init.d/rhttpproxy restart
   ```

Configuring logging for virtual machines

Virtual machine log files are used by virtual machines to write troubleshooting information. Virtual machine log files are stored on the same VMFS volumes as the virtual machine files are stored. Virtual machines may write a large amount of data to log files that can consume a large amount of disk space on the datastores, which leads to the denial of service. This behavior can be controlled by modifying the logging settings of virtual machines.

Getting ready

Connect to your vCenter Server via the vSphere Web Client and browse towards your virtual machine in the vSphere Web Client.

How to do it...

We will take a look at the step-by-step procedure to configure the logging settings of the virtual machine.

The steps for configuring the virtual machine log file and log size limit are as follows:

1. Right-click on your powered off virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **Advanced** to expand its configuration options.

3. Click on **Edit Configurations** and select **Add Row**.

4. Type `log.rotatesize` in the name field and enter the value for maximum size of log files in bytes. For 200 KB, enter 20000.

5. Type `log.keepOld` number in the name field and enter the value for the number of log files to keep. It will delete the oldest files as new log files are created.

Configuration Parameters

Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name	Value
pciBridge7.virtualDev	pcieRootPort
pciBridge7.functions	8
vmware.tools.internalversion	9216
vmware.tools.requiredversion	9216
vmware.tools.installstate	none
vmware.tools.lastInstallStatus	unknown
migrate.hostLogState	none
migrate.migrationId	0
log.rotatesize	20000
log.keepOld	8

Add Row

OK   Cancel

6. Click on **OK** to apply the settings.

The steps for configuring a virtual machine's guest operating system logging options are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **Advanced** to expand its configuration options.

3. Select or deselect the checkbox **Enable Logging** to enable or disable the guest operating system logging option.

4. Click on **OK** to apply the settings.

How it works...

The virtual machine's logging settings can be used to limit the total size and number of log files. Normally, a new log file of the virtual machine will be created each time you reboot a host and this can end up occupying a large amount of space. You can modify the behavior by limiting the maximum size of the log file and also the maximum number of log files to create. This ensures that the space utilized by the log files of the virtual machines can be kept under control. VMware's recommendation is to save 10 log files and limit each to 100 KB. These values are more than enough to capture sufficient information. If you configured the virtual machine with the logging limit, each time an entry is written to a log, the size of the log files is checked. If it reaches the limit of maximum log file size, the new entry is written to a new log file and also once the maximum number of log files is reached, the oldest log files will be deleted to create new log files.

There's more...

The steps for configuring the virtual machine log file and log size limit from the command line are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select the **VM Options** tab and click on **General** to expand its configuration option.
3. Note down the location of the virtual machine's configuration file location.

Prod-WebServer - Edit Settings	⑦ ▶▶

Virtual Hardware	VM Options	SDRS Rules	vApp Options

▼ General Options

VM Name	Prod-WebServer
VM Config File	[datastore1] Prod-WebServer/Prod-WebServer.vmx
VM Working Location	[datastore1] Prod-WebServer/
Guest OS	Windows

4. Log in to the ESXi host with the SSH where the virtual machine is residing.
5. Browse to the virtual machine's location using the following command:

```
cd /vmfs/volumes/datastore1/Prod-WebServer
```

6. Edit the virtual machine `.vmx` file using the following command:

   ```
   vi Prod-WebServer.vmx
   ```

7. Enter the following lines to configure the log size and log file limit:

   ```
   log.rotateSize=200000
   log.keepOld=8
   ```

8. Save your changes and exit the file.

Configuring security settings for virtual machines

Securing virtual machines is necessary in the same way it is for physical servers. Securing a virtual machine using tools including antivirus, anti-spyware, and protection are enabled for the virtual machine. Keep virtual machines up-to-date with the security updates and patches. Apart from that, you can secure the virtual machines against attacks by disabling unnecessary services and features of the virtual machine which are not necessary for the applications or guest applications. You can find the complete details on securing a virtual machine from the vSphere 5.1 Hardening Guide.

Please refer to the following link for vSphere 5.1 Hardening Guide:

```
http://communities.vmware.com/docs/DOC-22981
```

Getting ready

Connect to your vCenter Server via the vSphere Web Client login and browse to your virtual machine in the vSphere Web Client.

How to do it...

We will take a look at the step-by-step procedure to configure a few of the important security settings of virtual machines.

The steps for disabling copy and paste operations in the remote console of the virtual machine are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.
2. Select **VM Options** tab and click on **Advanced** to expand its configuration options.
3. Click on **Edit Configurations** and select **Add Row**.

4. Type `isolation.tools.copy.disable` in the name field and enter the value as `True` to disable the copy operation.

5. Type `isolation.tools.paste.disable` in the name field and enter the value as `True` to disable the paste operation.

6. Click on **OK** to apply the settings.

The steps for preventing virtual machine disk shrinking are as follows:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select the **VM Options** tab and click on **Advanced** to expand its configuration option.

3. Click on **Edit Configurations** and select **Add Row**.

4. Type `isolation.tools.diskWiper.disable` in the name field and enter the value as `True`.

5. Type `isolation.tools.diskShrink.disable` in the name field and enter the value as `True`.

6. Click on **OK** to apply the settings. You cannot shrink virtual machine disks if a datastore runs out of space when you disable this feature.

There's more...

The steps for preventing other users on spying the virtual machine remote console sessions are explained here. More than one user can connect to the virtual machine remote console sessions at a time by default. If more than one user connects to a remote console of the virtual machine, users can observe the actions performed by the other remote console users. These settings can be used to limit the number of remote console connections to the virtual machine:

1. Right-click on your virtual machine and click on **Edit Settings**.

2. Select **VM Options** tab and click on **Advanced** to expand its configuration options.

3. Click on **Edit Configurations** and select **Add Row**.

4. Type `RemoteDisplay.maxConnections` in the name field and enter the value as `1` to limit console sessions of the virtual machine to only one.

5. Click on **OK** to apply the settings.

8

Performance Monitoring and Alerts

In this chapter we will cover:

- ▶ Running vCenter performance monitoring graphs
- ▶ Configuring SNMP for ESXi and vCenter
- ▶ Running performance monitoring using ESXTOP
- ▶ Configuring vCenter alarms
- ▶ Managing log files

Introduction

The vSphere statistics system collects data on the resource utilization of the vSphere inventory objects managed by the vCenter Server. The vCenter Server database stores the data of the collected metrics that is collected at frequent intervals. Collected data will be processed and archived in the vCenter database. This stored statistical information can be accessed through the command-line monitoring tools or via the performance charts in the vSphere Windows Client and Web Client.

Running vCenter performance monitoring graphs

Advanced performance charts can be useful to analyze the performance problem that requires more statistical data to understand the source of the trouble. Advanced charts provide more statistical information. It displays the specific data point information when you hover over a data point in the performance chart. An advanced chart can be customizable, and chart settings can be changed and saved to create your own charts for future purpose. Performance chart data can be exported to a spread sheet and can also be saved to an image file.

Getting ready

Connect to your VMware vCenter Server using vSphere Web Client. Select your inventory object in vSphere Web Client. Click on the **Monitor** tab and select the **Performance** option.

How to do it...

We'll see a step-by-step procedure of how to view and configure advanced performance charts using the vSphere Web Client.

The following steps will enable you to view the advanced performance charts:

1. Click on **Advanced** to view the advanced performance charts.

2. Select an option from the **View** drop-down menu to view the different charts (**CPU**, **Datastore**, **Disk**, **Memory**, **Network**, **Power,** and so on). Available views depend on the type of inventory object selected.
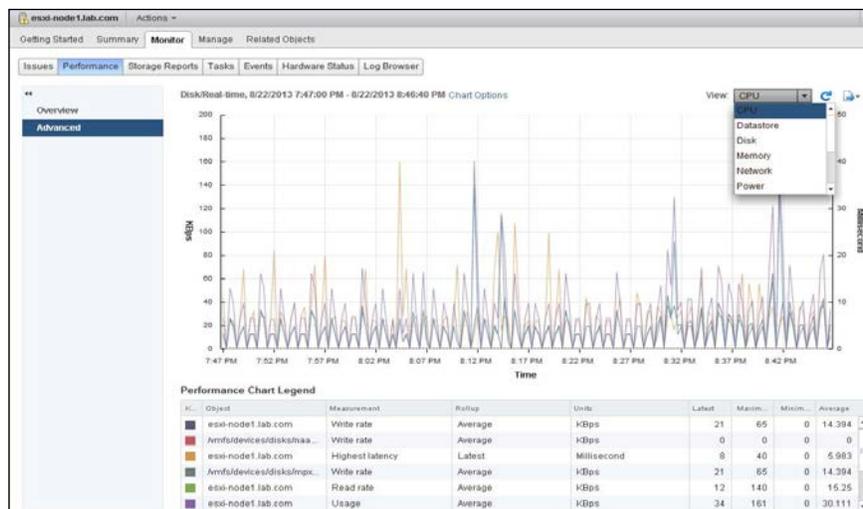
Configuring the advanced performance charts settings is done as follows:

1. Click on **Advanced** to view the advanced performance charts.

2. Click on the **Chart options** drop down to configure the advanced performance chart settings.

3. Select one of the metric group (**CPU**, **Memory**, **Network**, or any other available metric group) from the **Chart Metrics** section.

4. Select one of the available time ranges from the **Timespan** drop down:

    ❑ **Real-time**

    ❑ **Last day**

    ❑ **Last week**

    ❑ **Last month**

    ❑ **Last year**

    ❑ **Custom interval** (Specify the **From** and **To** date along with specific time)

5. Select the inventory object under the **Target Objects** section to display the statistics in the performance charts.

6. Select one of the available chart types from the **Chart Type** drop-down menu.

7. Select the counters to display in the chart under the **Select counters for this chart** option. If you hover over a counter, you can view the display of its information in the description column:

8. Click on **OK** to display the performance chart.

The following steps will create a custom advanced chart view:

1. Click on **Advanced** to view the advanced performance charts.
2. Click on **Chart options** to configure the advanced performance chart view settings. Customize the advanced chart as per your requirements.
3. Click on the **Save Options As...** option.
4. Enter the name of the chart options and click on **OK**.

The following steps will delete a custom advanced chart view:

1. Click on **Advanced** to view the advanced performance charts.
2. Click on **Chart Options** and select the chart view that you want to delete from the drop-down list.
3. Click on **Delete Options** and click on **OK** to confirm the deletion.

There's more...

Exporting or saving the performance data is a very important task for administrators. This will help administrators to share the performance report with the management about the performance of your virtual environment.

The following steps will savie the performance chart data to a file:

1. Click on **Advanced** to view the advanced performance charts.
2. Click on the **Export** icon to export the output of the performance chart.
3. Select one of the following **File type** to save the chart data:
   - **To PNG**
   - **To JPEG**
   - **To CSV**
4. Enter the filename and location to save the chart data.
5. Click on **Save**.

Configuring SNMP for ESXi and vCenter

SNMP (**Simple Network Management Protocol**) is a protocol commonly used to monitor a variety of networked devices. vSphere systems use SNMP agents to send a notification alert to notify the management system of a particular event or condition. ESXi host includes an SNMP agent that can send SNMP traps, and informs and receives `GET`, `GETBULK`, and `GETNEXT` requests. With ESXi 5.1, the SNMP agent adds support for Version 3 SNMP protocol that offers improved functionality and increased security. ESXCLI commands can be used to enable and configure the SNMP agent. Configuration methods of the SNMP agent will be different depending on the SNMP version (SNMP v1/v2c or SNMP v3) used. You can also use **Host Profiles** and the **PowerCLI** commands to configure SNMP for an ESXi host. The **Management Information Base** (**MIB**) files can be used to define the information that can be provided by managed devices.

Getting ready

Connect to the ESXi server with root credentials using SSH connection or via a console connection.

How to do it..

We'll demonstrate a step-by-step procedure to configure different types of SNMP versions traps for an ESXi host.

The following steps will configure SNMP v1 and v2c traps for an ESXi host:

1. Set the community string name as `ProdMonitor` in the ESXi host as follows. I have chosen `ProdMonitor` as the community name for this description.

   ```
   esxcli system snmp set –c ProdMonitor
   ```

2. Configure the SNMP target by specifying the SNMP target address, port number, and community name. You can specify the multiple targets by separating them with a comma. In the following example, ESXi host is configured with the target address as `snmpsrv1.lab.com`, and community as `ProdMonitor` via the port `162`. So this ESXi host will send SNMP traps to the SNMP target called `snmpsrv1.lab.com` at port `162` using the `ProdMontior` community.

   ```
   esxcli system snmp set –t snmpsrv1.lab.com@162/ProdMonitor
   ```

3. Enable the SNMP agent if it is not enabled.

   ```
   esxcli system snmp set –e true
   ```

4. Optionally, you can send a test trap to verify that the configurations are correct.

   ```
   esxcli system snmp test
   ```

The following steps will configure SNMPv3 traps for ESXi host:

1. Each and every SNMPv3 agent has an engine ID that serves as a unique identifier for the SNMP agent. This is an optional step. This SNMP engine ID is used with a hashing function to generate keys for authentication and encryption of SNMPv3 messages. You can specify the engine ID that is a hexadecimal string between 5 and 32 characters long. It will be automatically generated when the SNMP agent is enabled on the host, if you didn't manually specify:

   ```
   esxcli system snmp set –E 655d44513456
   ```

2. Configure the **SNMP authentication protocol**, which is an optional protocol. Three available authentication options are `None`, `SHA1`, and `MD5`. Authentication is used to ensure the identity of users and also to ensure the confidentiality of data. The following command will set to `SHA1`:

   ```
   esxcli system snmp set –a SHA1
   ```

3. Configure the **Privacy** protocol, which is an optional protocol. You must enable authentication in order to enable privacy. Available options are `None` and `AES128`. The following command will set the authentication type to `AES128`:

   ```
   esxcli system snmp set –x AES128
   ```

4. The authentication and privacy hash can be generated from the user supplied passwords if either privacy or authentication protocol were enabled as follows:

   ```
   esxcli system snmp hash -r -A secret5555 -X secret6666


   -A Provide filename to secret for authentication hash
   -X Provide filename to secret for privacy hash
   -r Make -A and -X flags read raw secret from command line instead
   of file.
   ```

   Output of the preceding command will be generated in the preceding format

   ```
   Authhash: 0c09ae8a2209d2364d66ac21eb096337de8a5c08
   Privhash: 6dfe0add5436aa63ab2f87034cc73a2a6b76d398
   ```

5. Configure the SNMP users, which are up to five users who can access SNMPv3 information. Before configuring the SNMP users, generate the authentication and privacy hash values as mentioned in the previous step. The security levels available for a user are `none` (no authentication or privacy) , `priv` (authentication and privacy) and `auth` (authentication only). The following is the structure of the command:

   ```
   esxcli system snmp set --users userid/authhash/privhash/security.
   esxcli system snmp set -u
   snmpusr1/0c09ae8a2209d2364d66ac21eb096337de8a5c08/6dfe0add5436aa63
   ab2f87034cc73a2a6b76d398/priv
   ```

6. Configure the SNMPv3 target by specifying the SNMP target address, port number, user ID, and security level along with the message type, either trap or inform, as follows:

```
esxcli system snmp set --v3targets
   snmpsrv1.lab.com@162/snmpusr1/priv/trap
```

7. Enable the SNMP agent, if it is not enabled, as follows:

```
esxcli system snmp set -e true
```

8. Optionally, you can send an test trap to verify that the configurations are correct.

   esxcli system snmp test

There's more...

You should configure your vCenter Server with SNMP server settings to send the SNMP traps to the monitoring server.

Configuring SNMP settings for vCenter Server

vCenter Server also included an SNMP agent that can be used to send traps, when an alarm is triggered on the vCenter Server. An SNMP agent on the vCenter Server functions only as a trap emitter and does not support other SNMP operators such as GET like ESXi host does. vCenter Server typically sends SNMP traps to other management programs. Management server needs to be configured to interpret the traps sent by vCenter Server. vCenter Server SNMP settings must be configured to use the vCenter Server SNMP traps. The traps sent by the vCenter Server are defined in the MIB file called `VMWARE-VC-EVENT-MIB.mib`.

1. Connect to your vCenter Server using vSphere Web Client.
2. Select your vCenter Server in vSphere Web Client.
3. Click on **Manage** and select **Settings**.
4. Click on **Edit** and select the **SNMP receivers** option.
5. Enter the primary receiver URL (DNS or IP address of the SNMP receiver), receiver port, and community name.

6. Optionally, you can configure the additional SNMP receivers and click on **OK** to apply the settings:
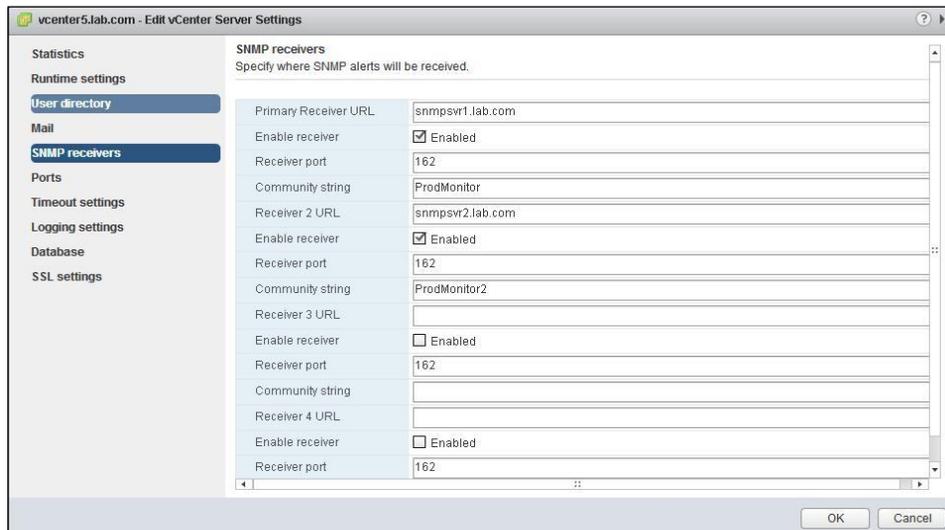
Running performance monitoring using ESXTOP

The esxtop and resxtop command-line utilities can be used to get the detailed information about real time ESX/ESXi host resource utilization. You must use root user privileges to execute the esxtop or resxtop against the ESX/ESXi host. You can start the esxtop utility in three different modes, which are interactive (default mode), batch, and replay mode. The only difference between esxtop and resxtop is that you can use resxtop to understand the resource utilization of the remote ESX/ESXi host remotely, but esxtop can only be used locally on the ESX/ESXi host. The esxtop utility reads its default configuration from the file called `.esxtop41rc`.

Getting ready

Connect to the ESXi with your root credentials host using SSH connection or via console connection.

How to do it...

We will take a look at how to use the esxtop command line in different batch modes to collect the performance data.

The following steps need to be performed to run esxtop in an interactive mode:

1. Type the command `esxtop`. It will display the real-time statistics and it refreshes every 5 seconds by default.

2. Type the following switches to switch between different statistics view in esxtop interactive mode:

   - `c` (CPU view): This displays the CPU resource utilization screen of ESXi server.
   - `m` (memory view): This displays the memory resource utilization of the ESXi server.
   - `i` (interrupt): This displays the information about the interrupt vectors of the ESXi server.
   - `d` (disk adapter view): This displays the storage disk adapter resource utilization screen of the ESXi server.
   - `u` (disk device view): This displays the storage disk device resource utilization screen of the ESXi server.
   - `v` (virtual disk view): This displays information about the Virtual Machine storage.
   - `n` (network view): This displays the network utilization screen of the ESXi server.
   - `p` (power management): This displays the information about the power utilization of the ESXi server.
   - `h` (help screen for esxtop): This displays the help options for the current view.
   - `f`: This adds or removes a field.
   - `s`: This sets the delay in seconds between updates.
   - Space: Update display.
   - `o`: This changes the order of the fields.
   - `2`: This moves down the highlighed row.
   - `8`: This moves up the highlighed row.
   - `4`: This removes a selected line.
   - `#`: This sets the number of instances to display.
   - `L`: This changes the length of the `NAME` field.
   - `l`: This limits the display to a single group.

3. Type `q` to exit the esxtop interactive mode.

The following steps need to be performed to run esxtop in the batch mode:

1. Type the following command to run esxtop in the batch mode. It will redirect the output of the esxtop command to a CSV file. You can analyze the statistics collected from the esxtop batch mode later using tools such as Microsoft Excel and Perfmon. Also ESXplot is a "fling" from VMware labs to review batch output from esxtop.

    ```
    esxtop -b > file_name.csv
    ```

2. The following are the command-line options that can be used with the esxtop batch mode:

    -   `a`: This shows all the default statistics
    -   `b`: This option runs esxtop in the batch mode
    -   `c <filename>`: This command allows you to load a user-defined configuration file to collect the statistics when running esxtop in batch mode
    -   `d`: This can be used to specify the delay between the statistics snapshots. Default is 5 seconds.
    -   `n`: This can be used to define a number of iterations or times esxtop collects and saves the statistics

3. Using the following command, the esxtop command will run for about 50 seconds, a 10 second delay with 5 iterations. It will then save the output file called `esxistats.csv` in the `/tmp` folder of the ESXi host:

    ```
    esxtop -b -d 10 -n 5 >/tmp/esxistats.csv
    ```

The esxtop replay mode can be used to replay the statistics collected using vm-support command. The following steps need to be performed to run esxtop in the replay mode:

1. Run the vm-support command in the snapshot mode. The following command will collect stats for five minutes ((30 seconds * 10 iterations) = 300 seconds). Once vm-support commands are completed, all the files are stored in the same location from where you have executed the command:

    ```
    vm-support -p  -i 10 -d 20
    ```

2. Unzip and untar the output tar file to use in the esxtop replay mode.

3. Execute the following command to reply the statistics captured by the vm-support command using the esxtop replay mode:

    ```
    esxtop -R vm-support-File_directory_path
    ```

4. Output will be similar to the esxtop interactive mode but you are replaying the stats captured using vm-support commands at that particular time. It will mostly be used to troubleshoot the performance issues that happened at a particular time.

5. The following are the command-line options that can be used during the esxtop replay mode:

  - ❏ `R`: This specifies the path to the vm-support collected snapshot's directory.
  - ❏ `a`: This shows all the default statistics.
  - ❏ `c filename`: This specifies a user-defined configuration file to collect the statistics when running esxtop in the replay mode.
  - ❏ `d`: This can be used to specify the delay between the statistics snapshots. The default value is 5 seconds.
  - ❏ `n`: This can be used to define a number of iterations; esxtop can collect and save the statistics.

There's more...

The esxtop command can be used to take a look at the resource utilization of the local ESXi host. It cannot be used to see the remote ESXi server resource utilization. The `resxtop` command can be used to understand the resource utilization of the remote ESXi host. The resxtop command belongs to the vSphere CLI and you need to download and install a vSphere CLI package or deploy the **vSphere Managenet Assistant** (**vMA**) in your ESXi host before using any vSphere CLI commands. Then you can connect to your remote ESX/ESXi hosts to execute the resxtop commands. Other than conection options, the resxtop commands and switches are exactly same. The following are the command-line options for the resxtop command:

  - ▸ `server`: This is the name of the remote ESX/ESXi host to connect to. You can use it if you are connecting directly to the host or to the vCenter Server in case of an indirect connection.
  - ▸ `vihost`: This option is used to specify the name of the ESX/ESXi host to connect, if you have made a connection to the vCenter Server.
  - ▸ `portnumber`: This option is only needed if you changed the default port number. The default port is 443.
  - ▸ `username`: This is to be used to authenticate when connecting to the remote host. Remote server prompts you for the password for the specified user account.

Configuring vCenter alarms

vSphere has a user-configurable alarm subsystem. This subsystem enables you to specify the conditions when alarms are triggered. vCenter alarms can also be used to specify the action to perfrom the automated alarm actions, when system condition changes. vCenter Alarms are the notifications that can be activated in response to an event, a set of conditions or the state of an inventory object in the vCenter Server. By default, vCenter Server provides a set of predefined alarms that are specific to the different inventory objects in the vCenter Server. You can also create a new alarm definition as per your requirement. Alarm definition consists of the following elements:

- ▶ **Name and description**: It provides an identity to the alarm definition with the label and description.
- ▶ **Alarm type**: It is used to define the alarm type and also type of the inventory object to be monitored.
- ▶ **Triggers**: It defines the event, state, or condition that will trigger an alarm and also defines the severity of the notification.
- ▶ **Tolerance thresholds**: It provides the additional restrictions on the state and condition triggers thresholds that must be exceeded before the vCenter alarm is triggered.
- ▶ **Actions**: It defines the operations that occur in response to the triggered alarms. vCenter provides the groups of predefined actions that are specific to the inventory object types.
- ▶ **Severity levels**: This specifies three Severity levels that are as follows:

  - ❑ Normal: Green
  - ❑ Warning: Yellow
  - ❑ Alert: Red

Getting ready

Connect to your vCenter Server via vSphere Web Client login.

How to do it...

We will take a look at the step-by-step procedure to create a condition and event-based alarm definition using vSphere Web Client.

The following steps will create a new condition-based alarm definition:

1. Browse to the datacenter object in vSphere Web Client. You can create alarm definitions for various objects, such as vCenter Server, datacenter, clusters, hosts, Virtual Machines, datastores, datastore clusters, distributed switches, and distributed port groups.
2. Click on the **Manage** tab and click on **Alarm Definitions**.
3. Click on **Add** to add a new alarm definition.
4. Enter the **Alarm name** and **Description** for the new alarm definition.
5. Select the object type such as vCenter Server (datacenters, clusters, hosts, Virtual Machines, datastores, datastore clusters, distributed switches, and distributed port groups) to monitor from the **Monitor** drop-down option.
6. Select one of the options under **Monitor for**. In our example, I have selected **specific condition or state, for example CPU usage** to monitor my Virtual Machine memory usage. Based on the object type you want to monitor, you can choose one of the following options:
    -   Specific conditions or state (CPU usage, Memory usage, and so on)
    -   Specific event occurring on this object (VM power on, VM power off, and so on)
7. Select the checkbox **Enable this alarm** to enable this new alarm definition and click on **Next**:

8. Click on **Add** to add a new alarm trigger on the trigger page.

9.   Select one of the trigger condition from the drop-down menu. I have chosen **VM Memory Usage**:
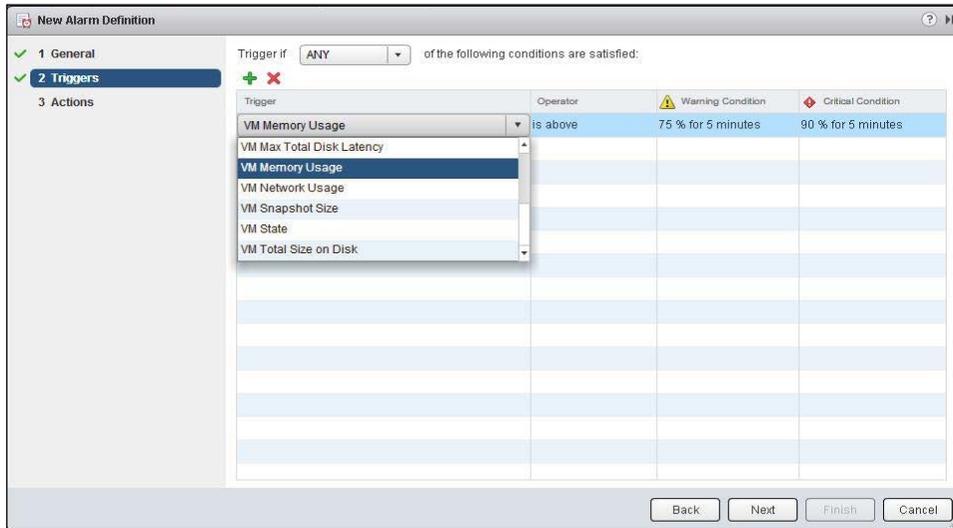
10. Select either **is above** or **is below** from the **Operator** drop down.

11. Select an option from the drop-down menu under the **Warning Condition** column to set the threshold for triggering a warning alert. In our example, I have selected VM memory usage is above **75% exists for 5 Minutes**, which will trigger a warning alert.

12. Select an option from the drop-down menu under the **Critical Condition** column. In our example, I have selected VM memory usage is above **90% exists for 5 Minutes,** which will trigger a critical alert.

13. You can specify multiple trigger condition. Select one of the following options from the **Trigger if** drop-down menu and click on **Next:**

   ❑   **ANY**: This means trigger if any of the following conditions are satisfied

   ❑   **ALL**: This means trigger if all of the following conditions are satisfied

14. Click on **Add** to add the actions to perform as part of this alarm definition.

15. Select one of the alarm actions from the drop-down under the **Action** column. In our example, I have selected alarm action as **Send a notification email**. This will send an e-mail to my vCenter Server admin group e-mail address. Enter the e-mail address of the vCenter Server admin group to receive the e-mail notification. Similar to that you can configure other alarm actions as per your organizations requirements:
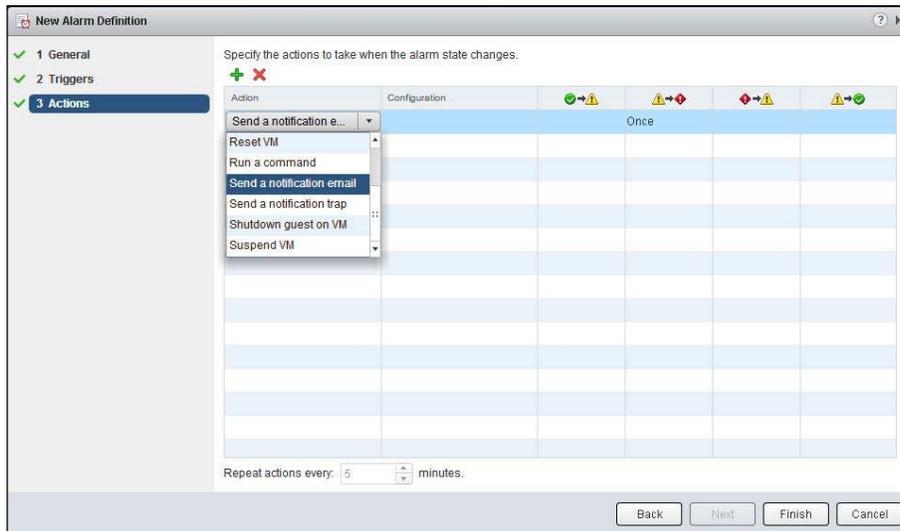
16. Select the action frequency either once or repeat for each trigger condition (green to yellow, yellow to red, red to yellow, and yellow to green).

17. Select the minutes from the drop down for the **Repeat Actions every** option:
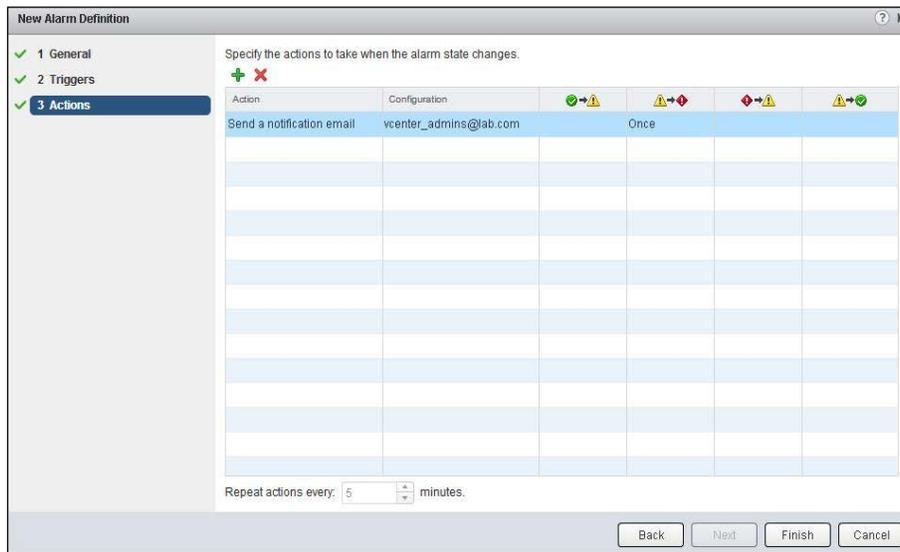
18. Click on **Finish** to create the new alarm definition.

The following steps will create a new event-based alarm definition:

1. Browse the datacenter object in vSphere Web Client. You can create an alarm definition for various objects such as (vCenter Server, datacenter, clusters, hosts, Virtual Machines, datastores, datastore clusters, distributed switches, and distributed port groups).

2. Click on the **Manage** tab and select **Alarm Definitions**.

3. Click on **Add** to add a new alarm definition.

4. Enter **Alarm name** and **Description** for the new alarm definition.

5. Select the object type (vCenter Server, datacenters, clusters, hosts, Virtual Machines, datastores, datastore clusters, distributed switches, or distributed port groups) to monitor from the **Monitor** drop-down menu.

6. Select the options **Specific event occurring on this object, for example VM Power on** under **Monitor for**.

7. Select the checkbox **Enable this Alarm** to enable this new alarm definition and click on **Next**.

8. Click on **Add** to add a new alarm trigger on the trigger page.

9. Select one of the events from the drop down under the **Events** column.

10. Select one of the status (**Unset**, **Normal**, **Warning**, or **Alert**) from the drop down under the **Status** column.

11. Click on **Add** to add the conditions that should be satisfied to be triggered.
    This step is optional.

12. Select one of the arguments from the **Argument** drop-down menu.
    This step is optional.

13. Click on the **Operator** column and select one of the operators from the drop-down menu. This step is also optional.

14. Click on **Value** and enter the value for the condition and click on **Next**. This step is optional, too.

15. Click on **Add** to add the actions to perform as part of this alarm definition.

16. Select one of the alarm actions from the Alarm drop-down menu. In our example, I have selected alarm action as **send a notification email**. Similarly, you can configure other alarm actions as per your organization requirement.

17. Select the action frequency either once or repeat for each trigger condition (green to yellow, yellow to red, red to yellow, and yellow to green).

18. Select the minutes from the drop down for the **Repeat Actions every** option.

19. Click on **Finish** to create the new alarm definition.

There's more...

Acknowledging triggered alarms:

1. Select an inventory object from the vSphere Web Client.

2. Click on the **Monitor** tab and select the **All Issues** option.

3. Click on **Triggered Alarms** and select one of the triggered alarms.

4. Right-click on the selected triggered alarm and select **Acknowledge**.

Resetting triggered alarms:

1. Select an inventory object from the vSphere Web Client.

2. Click on the **Monitor** tab and select the **All Issues** option.

3. Click on **Triggered Alarms** and select one of the triggered alarms.

4. Right-click on the selected triggered alarm and select **Reset to Green**.

Managing log files

Log files can be used to write troubleshooting information and also contains additional information about the activities performed in your vSphere environment. With vSphere Web Client, Log Browser allows you to view, search, and export vCenter Server and vSphere hosts log files. It allows you to view the different types of logs of the ESXi host and also vCenter Server and it has advanced functionality to filter the logs using filter queries.

Getting ready

Connect to your vCenter Server via vSphere Web Client login .Select your vCenter Server or ESXi host from the vSphere Web Client. Click on the **Monitor** Tab and select **Log Browser**.

How to do it...

We will take a look at the step-by-step procedure to manage and view the logs using the Log Browser from the vSphere Web Client.

The following steps will retrieve logs using Log Browser:

1. If no logs for the ESXi host or vCenter Server are available, you may see the message **The logs have not been retrieved for this object**. Click on **retrieve now** to retrieve the log files. Retrieving logs will take a few minutes to complete.

2. Once the log files are retrieved, select the type of log that you want to browse from the drop down under the **type** option.

The following steps will teach us to filter log files using Log Browser:

1. Select your vCenter Server or ESXi host from the vSphere Web Client.
2. Click on the **Monitor** tab and select **Log Browser**.
3. Select the type of log that you want to browse from the drop down under the **type** option.
4. Type the text in the **Filter** search box that you want to filter from the log files and press *Enter*.

The following steps will create Advanced Log filters using Log Browser:

1. Select your vCenter Server or ESXi host from the vSphere Web Client
2. Click on the **Monitor** tab and select **Log Browser**.
3. Click on the **Advanced Filters** option.
4. Enter the conditions that you want to include as part of this filter.
5. Type the name for this filter and click on **Save** to save this advanced filter.
6. Click on **Filter** to view the filtered results in the Log Browser.

The following steps will adjust log timings using Log Browser:

1. Select your vCenter Server or ESXi host from the Sphere Web Client.
2. Click on the **Monitor** tab and select **Log Browser**.
3. Under **Actions**, select **Adjust Time**.
4. Select **Add or Subtract and Adjust the times** from the original timestamps in the log file. You might need to modify the timestamp of a log file to adjust its time to a different time zone:

5. Click on **Apply** to apply the modified log timings to the log files.

There's more...

In many troubleshooting situations, it is necessary to export log files. You should use Log Browser to export the log files when using vSphere Web Client.

The following steps will export the log files using Log Browser:

1. Select your vCenter Server or ESXi host from vSphere Web Client.
2. Click on the **Monitor** tab and select **Log Browser**.
3. Under **Actions**, select **Export** to export the log files.
4. Select the type of file that you want to download.
5. Click on **Export**.
6. Specify the location where you want to save the log file.

9

vSphere Update Manager

In this chapter, we will cover the following topics:

- ▶ Installing Update Manager
- ▶ Configuring Update Manager
- ▶ Creating and managing baselines
- ▶ Scanning and remediating vSphere objects
- ▶ Configuring UMDS

Introduction

Update Manager helps you to manage the centralized patch management and version management for VMware vSphere. It supports automated patch installation of VMware vSphere hosts, virtual machines, and virtual appliances with any manual intervention. Using Update Manager, you can upgrade ESX/ESXi hosts to the latest version, install and update hardware drivers such as NIC drivers, storage adapter drivers, and monitoring agents on ESX/ESXi hosts. Upgrading virtual machine hardware version, VMware Tools, and virtual appliances can be also be automated using Update Manager.

Installing Update Manager

The Update Manager server component can be installed on the vCenter Server or on different computers. For production deployment, install the Update Manager on a dedicated server. Following are a few of the prerequisites for the installation of the Update Manager server:

▸ Create a database and a 32-bit system DSN if you are not using SQL Server Express Edition bundled with the installation.

▸ Verify whether the database version is supported with your Update Manager installation.

▸ Make sure that the Update Manager database and system DSN are configured with SQL Server authentication, if your database is located on the remote system. This is done because Windows authentication of the database located on a different machine is not supported by the Update Manager. The Oracle database is also supported with the Update Manager installation.

Getting ready

Log into the system where you want to install the Update Manager with administrative credentials and insert the VMware vCenter Server installation media to CD/DVD drive of the system.

How to do it...

We'll see a step-by-step procedure on how to install the Update Manager server and client:

Perform the following steps for installing the Update Manager:

1. Double-click on the vCenter Server installer's `autorun.exe` file.

2. Choose **vSphere Update Manager** and click on **Install**.

3. Select the language for the installer from the dropdown and click on **OK**.

4. Click on **Next** in the welcome page.

5. Read the end-user patent agreement and click on **Next**.

6. Read the end-user license agreement and **Accept** it. Click on **Next**.

7. Review the Update Manager support information. Select the checkbox **Download updates from default source immediately after installation** to download the updates immediately after the installation of the Update Manager. If you deselect this option, Update Manager downloads the patches and updates according to the default download schedule. Click on the **Download Now** button to initiate the download on the **Download Settings** page. The default download schedule can be modified once the installation is complete.

> Deselect this option to review the default download sources before download or to use a shared repository as a download source.
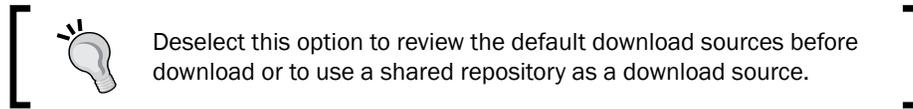
8. Enter the vCenter Server **IP address** or **Host Name**, **HTTP Port**, and the administrative account credentials (which are used by the Update Manager server to connect to the vCenter Server) and click on **Next**:

9. In the **Database Options** page, choose the type of database for your Update Manager. Select the checkbox **Install a Microsoft SQL server 2008 R2 Express instance (for small scale deployment)** if you don't have any existing database in your environment. This default database is for deployments up to 5 ESXi hosts and 50 virtual machines. Select the checkbox **Use an existing supported database** if you are using a supported database, and enter the 32-bit system DSN name. Click on **Next**:
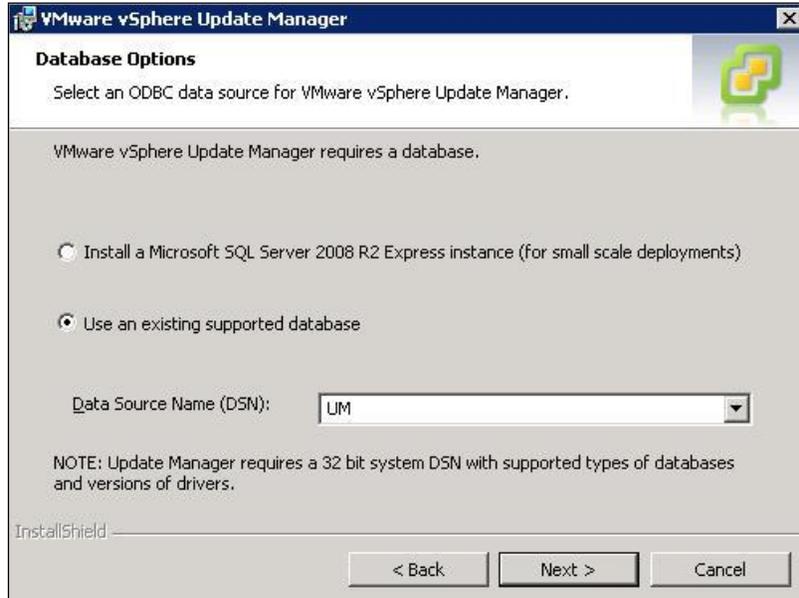
> The ODBC tool in the control panel will create a 64-bit DSN. Update Manager requires a 32-bit system DSN. You need to use the 32-bit ODBC tool located at `C:\Windows\SysWOW64\odbcad32.exe` for the Update Manager.

10. Review the additional database configuration information and click on **Next**.

11. Select the IP address or hostname of your Update Manager instance from the dropdown and review the port numbers required for the Update manager installation. The setup will open the ports in the firewall if the Windows firewall/Internet connection sharing service is running on the system:

12. Select the checkbox **Yes, I have Internet connection and I want to configure proxy settings now** if you want to configure the proxy server and provide the proxy server information, the port, and the credentials to authenticate the proxy. Click on **Next**.

13. Review the Update Manager installation and patch download location. If you want to change to a different directory, click on **Change to browser to a different directory** and then click on **Next**.

> A warning message will appear when you try to install the Update Manager on the system that has less than 120 GB free space.

14. In the **Ready to Install the Program** page, click on **Install** to begin the Update Manager installation.

15. Once the installation is complete, click on **Finish**.

Perform the following steps for installing the Update Manager Client plugin:

1. Connect to your vCenter Server system using vSphere Web Client.

2. Click on the **Plug-ins** tab and select **Manage Plug-ins**.

3. In the **Plug-in Manager**, click on **Download and Install** to install the Update Manager extension.

4. Select the language for the installer from the dropdown and click on **OK**.

5. In the welcome screen of the installation, click on **Next**.

6. Review the patent agreement and click on **Next**.

7. Read and accept the license agreement and click on **Next**.

8. Click on **Install** to start the installation.

9. Click on **Finish** once the installation is completed.

10. Once the installation is complete, you will see the status of **Enabled** for **VMware vSphere Update Manager Extension** in **Plug-in Manager**:
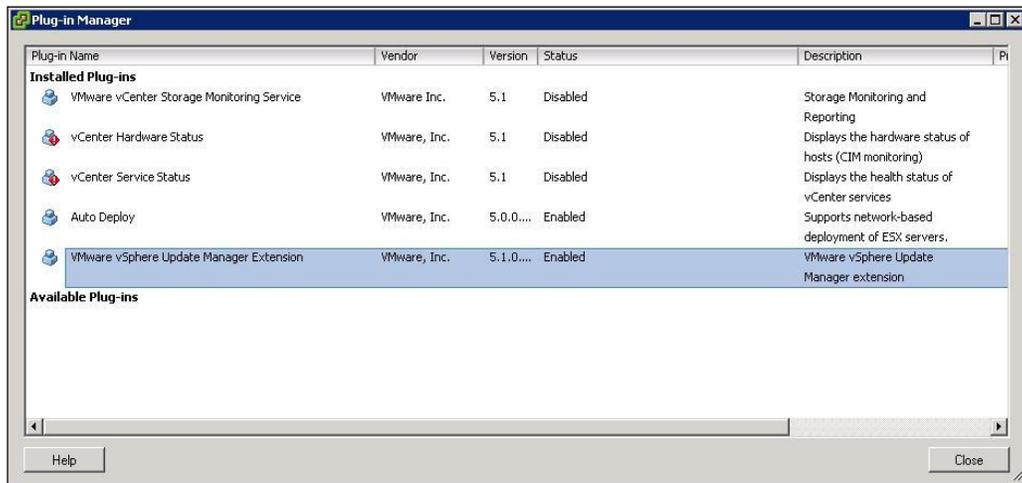
11. Click on **Close** to exit from the **Plug-in Manager**.

12. You can see the Update Manager plugin icon under **Solutions and Applications** in the home page of your Windows vSphere Client.

How it works...

The Update Manager consists of two parts: a server part and a plugin part. Both are supported only in the Windows machine. It is always recommended to install the Update Manager server on a remote machine in a large-scale environment to achieve better performance. The Update Manager Client plugin on the vSphere Client should be installed and enabled to use the Update Manager application. The Update Manager installer opens the designated ports on the Windows firewall to enable the communication.

There's more...

Perform the following steps for disabling Update Manager Client plugin:

1. In the vSphere Client, click on the **Plug-ins** tab and select **Manage Plug-ins**.
2. In the **Plug-in Manager**, right-click on **VMware vSphere Update Manager Extension**.
3. Select **Disable** to disable the Update Manager plugin.
4. Once disabled, you will see the status of **Disabled** for **VMware vSphere Update Manager Extension** in **Plug-in Manager**.
5. Click on **Close** to exit the **Plug-in Manager**.

Configuring Update Manager

The Update Manager server component is installed with the default configuration options if you have not modified it during the installation. The Update Manager settings can be modified after the installation, too. The Update Manager settings can be modified only with the required privileges to configure the Update Manager service. These privileges can be assigned on the vCenter Server system.

Getting ready

Connect to the vCenter Server using Windows vSphere Client and click on the Update Manager icon in the home page. Select the **Configuration** tab under settings to configure the Update Manager.

How to do it...

We'll see a step-by-step procedure to configure various Update Manager settings.

Perform the following steps for configuring the Update Manager network settings:

1. Click on the **Network Connectivity** option.
2. Review the port number displayed for **SOAP port** (port number **8084** which is used by the Update Manager client to establish communication with the Update Manager server) and **Server port** (the listening port for the web server that provides access to the client plugin installer) only if required.

3. Review the **IP address or host name of the server for the patch store**. Edit the IP address or hostname if more than one NIC or IP address is configured on the Update Manager server:
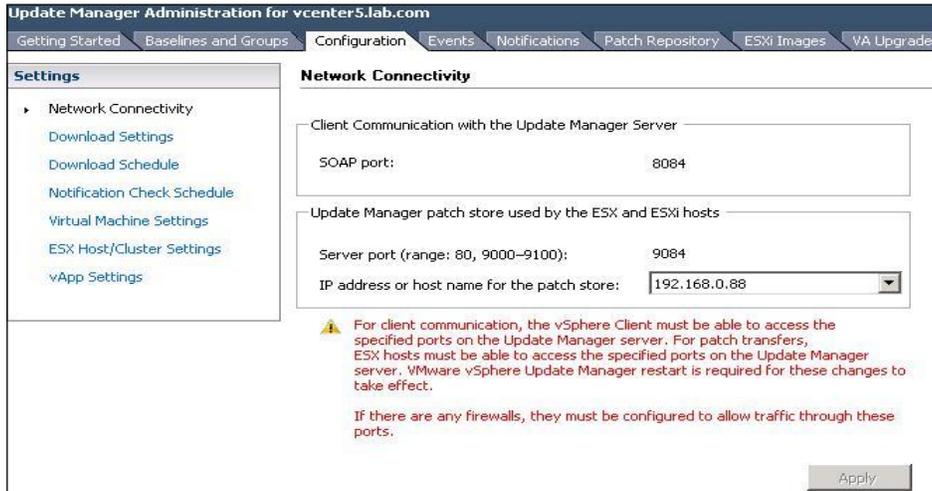
4. Click on **Apply** to save the settings.

Perform the following steps for configuring the UMDS settings:

1. Click on the **Download Settings** option.

2. If Update Manager system is directly connected to the Internet, select the checkbox **Direct Connection to Internet** in the **Download Sources** panel and select or deselect the checkbox in the **Enabled** column to choose the type of updates to download.

3. To add a new download source, click on **Add Download Source**. Type the download source URL and a URL description in the **Add Download Source** window. HTTP and HTTPS URL are supported by Update Manager. Click on **Validate URL** to verify the accessibility of the URL and click on **OK**.

> To make sure your connection is secure, specify the HTTPS URL.
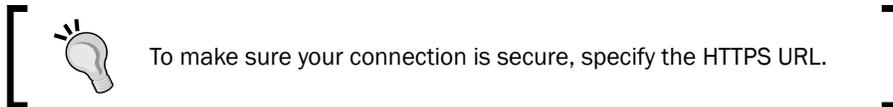
4. If you have a proxy server to connect to the Internet, select the checkbox **Use Proxy** under **Proxy Settings**. Click on the **Test Connection** button to test the Internet access through the proxy.

5. Enter the proxy and port information. If it requires authentication, select the checkbox **Proxy requires authentication** and enter the values for **Username** and **Password**:
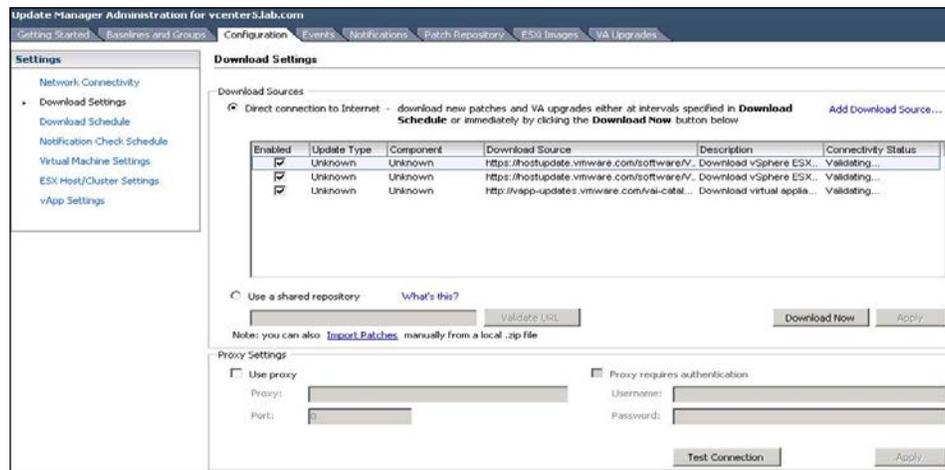
6. Click on **Apply** to apply the settings.
7. Click on **Download Now** to initiate the patch definition's download.

Perform the following steps for configuring the download schedule:

1. Click on the **Download Schedule** option.
2. Verify whether the checkbox **Enable scheduled download** is selected.
3. If you want to modify the download schedule, click on **Edit Download Schedule**.
4. Configure the download **Frequency** (**Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**), **Start time**, and **Interval**. Click on **Next**.
5. Enter one or more e-mail addresses to be notified when patches are downloaded in the e-mail notification window. The vCenter Mail Sender settings should be configured to enable e-mail notifications. Click on **Next**.
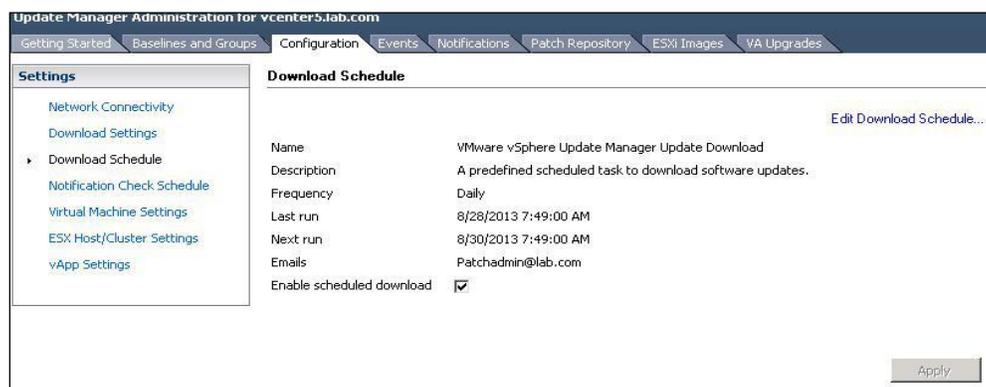
6. Review the selected settings and click on **Apply**.

Perform the following steps for configuring the Update Manager notification check schedule:

1. Click on the **Notification Check Schedule** option.

2. Verify that the checkbox **Enable scheduled download** is selected.

3. If you want to modify the notification schedule, click on **Edit Notifications**.

4. Configure the **Frequency** (**Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**), **Start time**, and **Interval**. Click on **Next**.

5. Enter one or more e-mail addresses to receive notifications from Update Manager or e-mail alerts such as when a patch is recalled in the e-mail notification window. Click on **Next**.
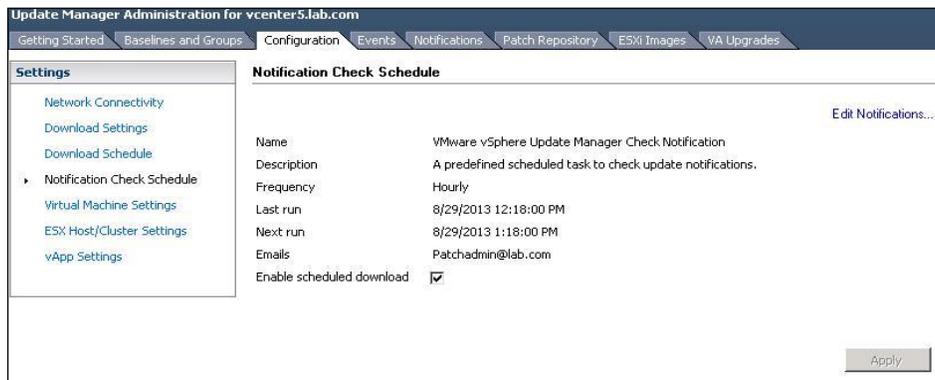
6. Review the selected settings and click on **Apply**.

Perform the following steps for configuring the virtual machine's settings:

1. Click on the **Virtual Machine Settings** option.

2. If you want to create the snapshots before remediating the virtual machines, make sure **Take a snapshot of the virtual machines before remediation** checkbox is selected. Update Manager is configured by default to take a snapshot of the virtual machines before applying updates. It will help to return the virtual machine to the previous state before the remediation, in case of a failed remediation.

3. Select either one of the following options to configure the retention of the snapshot:

   ❑ **Keep for hours**

   ❑ **Do not delete snapshots**

Snapshots reduce the performance of the virtual machine.
Delete the snapshots as soon as the remediation is validated.
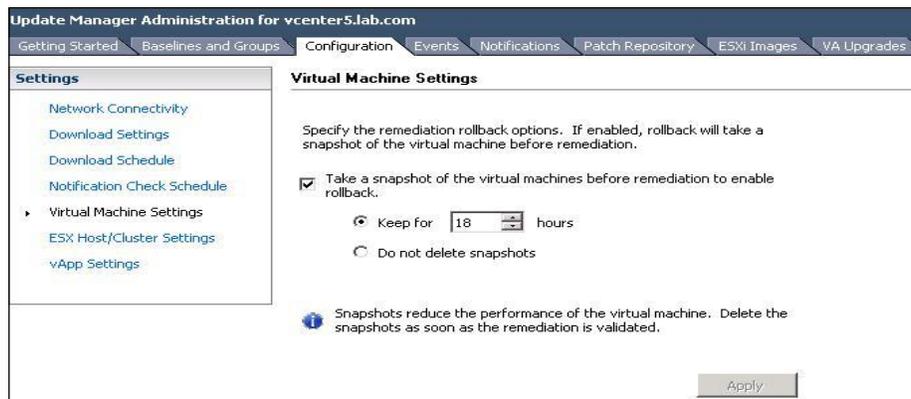
4. Click on **Apply** to apply the settings.

Perform the following steps to configure host maintenance mode settings:

1. Click on the **ESX Host/Cluster Settings** option.

2. Select any one of the following options from the drop-down menu for the **VM Power state** option to determine the power state of the virtual machines that are running on the ESX/ESXi host before remediation is applied:

   ❑ **Power off the Virtual Machines**

   ❑ **Suspend Virtual Machines**

   ❑ **Do not Change VM Power State** (default setting)

3. Select the checkbox **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode** to disable the CD/DVD or floppy drives connected to the virtual machines because Update Manager does not remediate ESX/ESXi hosts with virtual machine connected to CD/DVD or floppy drives.

4. Select the checkbox **Retry entering maintenance mode in case of failure**:
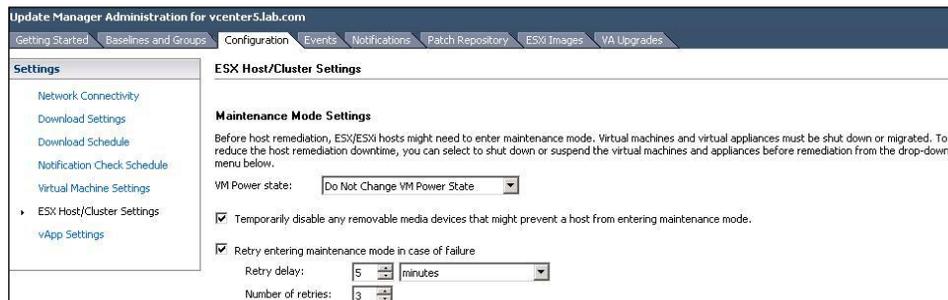
5. Specify the **Retry delay** option in minutes or hours and the **Number of retries** value. Click on **Apply**.

Perform the following steps for configuring the cluster settings:

1. Click on the **ESX Host/Cluster Settings** option.

2. Certain features might need to be temporarily disabled for the cluster updates to succeed. These features will be automatically re-enabled when the remediation is complete. Select the checkboxes for the following to enable or disable the features under the **Temporarily disable** option:

   ❏ **Distributed Power Management (DPM)**.

   ❏ **Enable parallel remediation for hosts in cluster**.

   ❏ **Fault Tolerance (FT)**.

   ❏ **Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode**. vMotion and DRS must be enabled to use this option.

   ❏ **High Availability Admission Control**.

3. Select the checkbox **Allow installation of additional software on PXE booted ESXi 5.x hosts** under **PXE Booted ESXi Host Settings** if you want to enable software installation for solutions on PXE booted hosts:

Cluster Settings

Certain features might need to be temporarily disabled for cluster updates to succeed. These features will be automatically re-enabled when remediation is complete.

Update Manager does not remediate hosts on which the features are enabled.

Temporarily disable:

☐ Distributed Power Management (DPM)

☐ High Availability Admission Control

☐ Fault Tolerance (FT)

ⓘ To ensure that FT can be re-enabled, you should remediate all hosts in a cluster with the same updates at the same time. See the documentation for more details.

☐ Enable parallel remediation for hosts in cluster

☐ Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode

PXE Booted ESXi Host Settings

☐ Allow installation of additional software on PXE booted ESXi 5.x hosts

Apply

4. Click on **Apply** to apply the settings.

Perform the following steps for configuring a smart reboot:

1. Click on the **vApp Settings** option.

2. Select the checkbox **Enable Smart reboot**. Enabling the smart reboot option will selectively reboot the virtual appliances in the vApp to maintain the start up dependencies.

3. Click on **Apply** to apply the settings.

There's more...

Perform the following steps for manually importing patches:

1. Click on the **Download Settings** option

2. Under **Download Sources** pane, click on **Import Patches**.

3. Click on **Browse** and select a compressed patch file that you want to import in the Update Manager repository. Click on **Next**.

4. Once the upload has been completed successfully, review the patches that have been imported and click on **Finish**.

Creating and managing baselines

Update Manager baselines can be upgrade, patch, or extension baselines. Baselines contain a collection of one or more patches, upgrades, or extensions. Baseline groups are created from existing baselines and might contain one upgrade baseline and one or more extension and patch baselines, or might contain a combination of multiple extension and patch baselines. You can scan the hosts, virtual appliances, and virtual machines against the baseline and baseline groups to verify their level of compliance. You must have the privilege of **Manage Baseline** to create, edit, or delete baseline and baseline groups. To attach baselines, you must have the **Attach Baseline** privilege on the vCenter Server system in which Update Manager is registered.

By default, Update Manager includes two dynamic patches and three upgrade baselines:

▶ **Critical Host Patches**: This default baseline checks the vSphere hosts for compliance with all available critical patches

▶ **Non-Critical Host Patches**: This default baseline checks vSphere hosts for compliance with all non-critical patches that are optional for the hosts

▶ **VMware Tools Upgrade to Match Host**: This default baseline checks virtual machines for the latest VMware Tools version supported by the host

▶ **VM Hardware Upgrade to Match Host**: This default baseline checks the virtual machine hardware version with the latest version supported by the host

▶ **VA Upgrade to Latest**: This default baseline checks the compliance of the virtual appliance with the latest vApp available version

Getting ready

Using Windows vSphere Client, connect to your vCenter Server and click on the Update Manager icon in the home page. Select the **Baselines and Groups** tab to create and configure the baselines.

How to do it...

We will take a look at how to create different types of baseline and baseline groups using the vSphere Client.

Perform the following steps for creating a fixed patch baseline:

1. Click on **Create** to create the baseline.
2. Enter the name and description for the baseline.
3. Select **Host Patch** under **Baseline Type** and click on **Next**:

4. In the **Patch Options** page, select the **Fixed Baseline** checkbox.
5. From the list, select the individual patches and click on the down arrow key to add them into the fixed patch list.
6. Click on **Finish**.

Perform the following steps for creating a dynamic patch baseline:

1. Click on **Create** to create the baseline.
2. Enter the name and description for the baseline.
3. Select **Host Patch** under **Baseline Type** and click on **Next**.
4. Select the **Dynamic Baseline** checkbox in the **Patch Options** page.

5. Select the specific criteria to determine the set of patches to include in the dynamic baseline. The set will only contain the patches that match all the fields.

    ❑ **Patch Vendor**

    ❑ **Product**

    ❑ **Severity**

    ❑ **Category**

    ❑ **Release Date**

6. Select the patches from the list to exclude and click on the down arrow key to exclude them on the **Patches to Exclude** page.

7. Select the patches to include them in baseline on the **Other Patches to Add** page and click on the down arrow key to add them into the list.

8. Click on **Finish**.

The extension baseline can contain additional VMware software or third-party software such as hardware drivers and Common Information Model (CIM) providers for managing third-party modules on the host for ESX/ESXi hosts. Host extension baselines are always fixed. Perform the following steps for creating a host extension baseline:

1. Click on **Create** to create the baseline.

2. Enter the name and description for the baseline.

3. Select **Host Extension** under **Baseline Type** and click on **Next**.

4. Select the patches from the list to include and click on the down arrow key to add them into the fixed patch list.

5. Click on **Advanced** to find the particular patches to include as a part of the baseline and click on **Next**.

6. Click on **Finish**.

Perform the following steps for importing host upgrade images and creating host upgrade baselines:

1. Click on the **ESXi Images** tab and select the **Import ESXi image** option.

2. Click on **Browse** in the **Import ESXi image** page, select the ESX/ESXi image to upload, and click on **Next**.

3. Once the upload is complete, review the information about the uploaded image and click on **Next**.

4. Select the checkbox **Create a baseline using the ESXi image** to create a host upgrade baseline from the uploaded ESXi image.

5. Enter the name and description for the baseline.

6. Click on **Finish** to create the host upgrade baseline.

Perform the following steps for creating a virtual appliance upgrade baseline:

1. Click on **Create** to create the baseline.

2. Enter the name and description for the baseline.

3. Select **VA Upgrade** under **Baseline Type** and click on **Next**.

4. Select the **Vendor** and **Appliance** options from the respective drop-down on the **Upgrade Options** page. Select any one of the following options from the **Upgrade To** drop-down menu:

   ❑ **Latest**

   ❑ **Do Not Upgrade**

   ❑ **A specific version number**

5. Click on **Add Rule** and then click on **Next**.

6. Click on **Finish**.

There's more...

We will look into creating a host baseline group, virtual machine and virtual appliance baseline group, and attaching baselines and baseline groups to vSphere objects in the following sections.

Creating a host baseline group

You can combine multiple patch or extension baselines with one host upgrade baseline, or combine one host upgrade in a baseline group with multiple patch and extension baselines. Perform the following steps for creating a host baseline group:

1. Click on **Create** on the **Baselines and Groups** tab.

2. Select the checkbox **Host Baseline Group** and specify the name for the baseline group. Click on **Next**.

3. Select a host upgrade baseline and click on **Next**.

4. Select the patch baselines to include in the host baseline group and click on **Next**.

5. Select the extension baselines to include as part of this baseline group and click on **Next**.

6. Review your baseline group settings and click on **Finish**.

Creating a virtual machine and virtual appliance baseline group

You can combine the virtual machine and virtual appliance baseline group in the upgrade baselines. Perform the following steps for creating a virtual machine and virtual appliance baseline group:

1. Click on **Create** and then on the **Baselines and Groups** tab.

2. Select the **Virtual Machine and Virtual Appliance Baseline Group** checkbox and specify the name for the baseline group. Click on **Next**.

3. Add one upgrade baseline per type (virtual appliance, VMware Tools, and virtual hardware) in this group:

❑ **VA Upgrades**

❑ **VMware Tools Upgrades**

❑ **VM Hardware Upgrades**
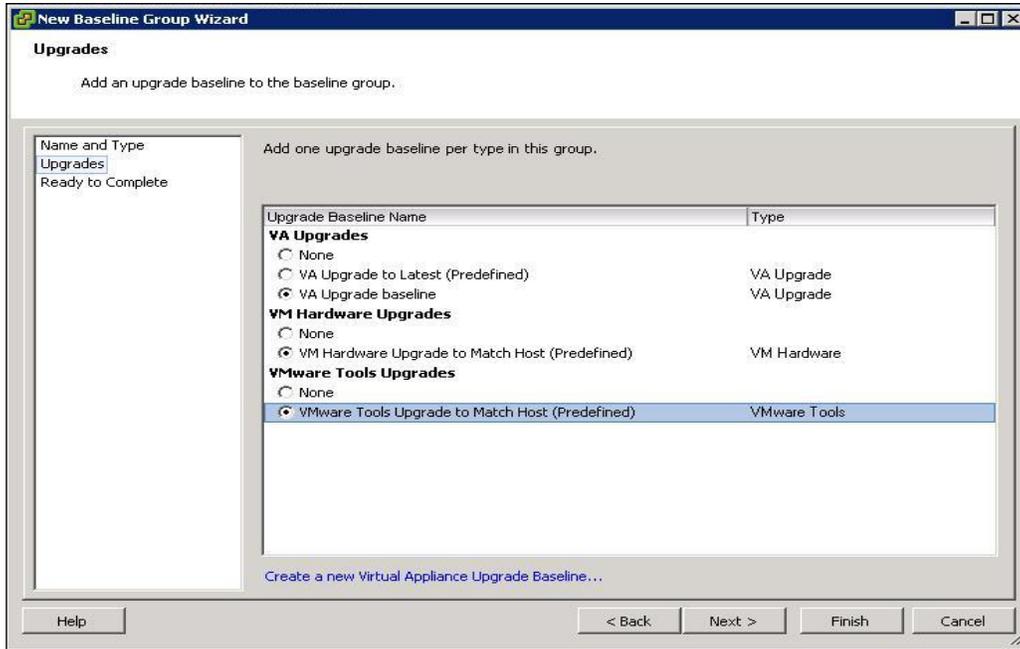
4. Review your baseline group settings and click on **Finish**.

Attaching baselines and baseline groups to vSphere objects

Perform the following steps for attaching baselines and baseline groups to vSphere objects:

1. Select the type of inventory object (**Host and Clusters** or **VMs and Templates**) that you want to attach the baseline to.

2. Select the vSphere object from the inventory, and click on the **Update Manager** tab.

3. Click on **Attach** and select one or more baselines or baseline groups to attach to the object in the **Attach Baseline or Group** window.

4. Click on **Attach** to attach the selected baseline and baseline group to the vSphere object.

Scanning and remediating vSphere objects

Scanning is the process that can be used to evaluate the vSphere hosts, virtual appliances, or virtual machines against the patches, extensions, and upgrades included in the attached baselines and baseline groups. The Update Manager's scan option can be manually initiated or scheduled to generate compliance information. Baselines and baseline groups must be attached to the ESX/ESXi hosts, virtual machine, or virtual appliances to generate compliance information about the ESX host and to view the scan results. You can manually initiate or schedule the remediation of ESX/ESXi hosts, virtual machines, and virtual appliances. Virtual machines and appliances can be remediated together.

Getting ready

Using Windows vSphere Client, connect to your vCenter Server.

How to do it...

We will take a look at the step-by-step procedure to initiate and view the scan results along with the procedure to remediate it.

Perform the following steps for initiating a scan of the ESX/ESXi hosts:

1. Select the **Hosts and Clusters** view in Windows vSphere Client.
2. Right-click a datacenter, host or cluster and select the option **Scan for Updates**.
3. Select the types of updates (**Patches and Extensions** or **Upgrades**) to scan for.
4. Click on **Scan**.

Perform the following steps for initiating a scan of virtual machine and virtual appliances:

1. Select **VMs and Templates** view in the Windows vSphere Client.
2. Right-click on the vSphere objects (a folder of Virtual Machines and appliances, virtual machine, virtual appliance, or a datacenter) and select **Scan for Updates**.
3. Select the type of updates (**VA upgrades**, **VM Hardware upgrades**, and **VMware Tools upgrades**) to scan for.
4. Click on **Scan**.

Perform the following steps for viewing the compliance information for vSphere objects:

1. Navigate to **Home | Inventory** in the Windows vSphere Client.
2. Select the type of object (**Hosts and Clusters** or **VMs and Templates**) from the inventory to view the compliance information.
3. View the results of the scan in the **Update Manager** tab.

There's more...

Perform the following steps for remediating hosts against patch or extension baseline:

1. Select the **Hosts and Clusters** view in the home page of vSphere Client and click on the **Update Manager** tab.

2. Click on **Remediate**.

3. Select the baseline group and baseline to apply in the **Remediation Selection** wizard and select the vSphere hosts to remediate and click on **Next**.

4. Deselect the specific extensions and patches to exclude them from the remediation in the **Patches and Extensions** page and click on **Next**.

5. Enter the unique name and description for the task in the **task description** field. Select **Immediately** to begin the remediation process or specify a time to begin the remediation process and then click on **Next**.

6. In the **Host Remediation Options** page, select one of the following power states from the drop-down menu under **Maintenance Mode Options**:

   ❑ **Do Not Change VM Power State**

   ❑ **Power Off Virtual Machines**

   ❑ **Suspend Virtual Machines**

7. Select the checkbox **Disable any removable media devices connected to the virtual machines on the host**. Update Manager does not remediate the vSphere hosts with the virtual machines connected to floppy or CD/DVD drives.

8. Select the checkbox **Retry entering maintenance mode in case of failure** and specify the **Number of Retries** value and **Retry delay** in minutes. Update Manager waits for the period of retry delay and retries for placing the vSphere host into maintenance mode.

9. Select the checkbox under **ESXi 5.x Patch Settings** to enable Update Manager to patch powered on PXE booted ESXi hosts, if required, and click on **Next**:

Chapter 9
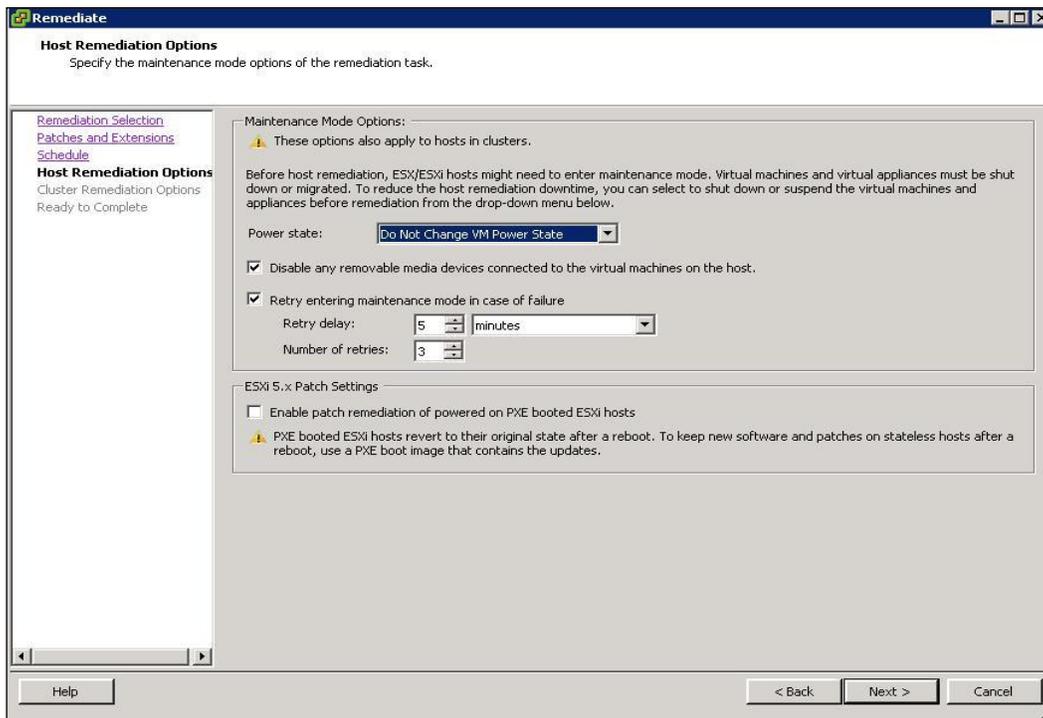
10. To remediate clusters, first you should temporarily disable certain cluster features. Update Manager automatically re-enables the features after remediation. Select the checkboxes to configure the following options in the **Cluster Remediation Options** page and click on **Next**:

    ❑ **Disable Distributed Power Management (DPM) if it is enabled for any of the selected features**.

    ❑ **Disable Fault Tolerance (FT) if it is enabled. This affects all fault tolerant virtual machines in the selected clusters.**

    ❑ **Disable High Availability admission control if it is enabled for any of the selected users.**

    ❑ **Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode**.

❑ **Enable parallel remediation for the hosts in the selected clusters.**
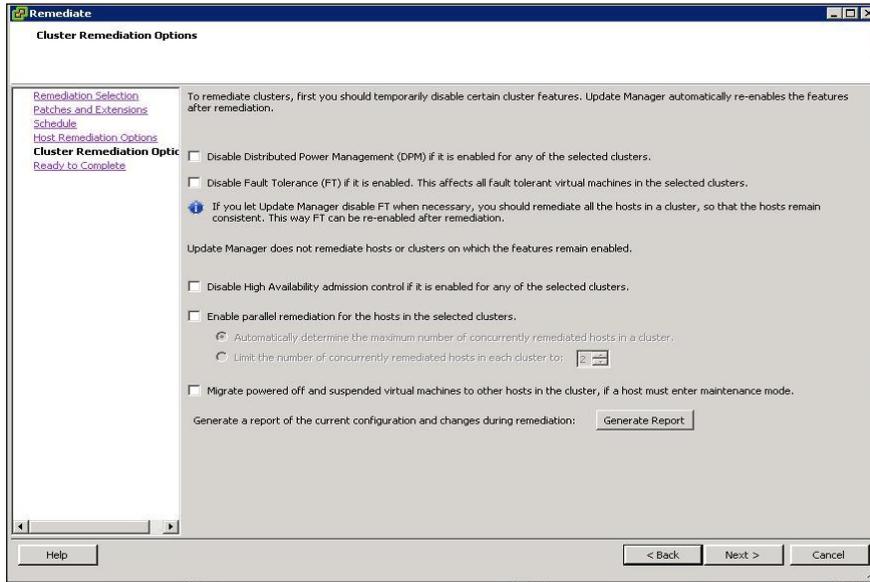
11. Review the options selected in the **Ready to complete** page and click on **Finish**.

Configuring UMDS

VMware vSphere **Update Manager Download Service** (**UMDS**) is a component of Update Manager. UMDS will download the upgrades for virtual appliances, patch binaries, and patch metadata. There are many environments in which Update Manager is deployed in a restricted and secured network which does not communicate to other local networks and the Internet. In such an environment, UMDS access to the Internet can download upgrades, patch metadata, and patch binaries. You can export the downloaded upgrades and patches to the location which is accessible to Update Manager. So those downloads become accessible to the Update Manager server. UMDS cannot be installed on the Update Manager server.

Getting ready

Log in to the system with Internet access where you want to install UMDS with administrative credentials. Insert the VMware vCenter Server installation media to the CD/DVD drive of the system. For other configuration after the installation, log in to the server where UMDS is installed. Navigate to the directory where UMDS is installed using the Windows command prompt.

How to do it...

We will take a look at the step-by-step procedure to install Update Manager Download Service along with configuration procedures.

Perform the following steps for installing Update Manager Download Service:

1. Insert the VMware vCenter installation DVD into the Windows server to proceed with the UMDS installation.

2. Browse towards the `umds` folder in the DVD and double-click on `VMware-UMDS.exe` to start the installer.

3. Select the language for the installation and click on **OK**.

4. Accept the license agreement for the UMDS installation and click on **Next**.

5. Select either one of the database options and click on **Next**.

6. Select **Install a Microsoft SQL Server 2008 R2 Express** (for small-scale deployment).

7. Select **Use an existing supported database** if you have an existing database server.

8. Enter the UMDS proxy settings and click on **Next**.

9. Select the directories for the Update Manager download service installation and patch download. Click on **Next** and then on **Change** if you want to change to a different directory.

10. Click on **Install** to begin the installation.

11. Once the installation is completed, click on **Finish**.

Perform the following steps for configuring the data to download with Update Manager Download Service:

1. Execute the following commands to specify the updates to download:

    To configure a download of all host updates and all virtual appliance upgrades, run the following command:

    ```
    vmware-umds -S --enable-host --enable-va
    ```

2. To configure a download of all ESXi 5.x updates, and to disable downloading only ESX 4.0 and ESXi 4.0 host updates, run the following commands:

    ```
    vmware-umds -S --enable-host
    vmware-umds -S -d esx-4.0.0 embeddedEsx-4.0.0
    ```

3. To configure a download of all host updates and disable the download of virtual appliance upgrades, run the following command:

```
vmware-umds -S --enable-host --disable-va
```

4. Execute the following command to initiate the download of the selected updates:

```
vmware-umds -D
```

5. Execute the following command to export the data:

```
vmware-umds -E --export-store repository_path
```

There's more...

▸ Execute the following command to change the UMDS repository location:

```
vmware-umds -S --patch-store your_new_patchstore_folder
```

▸ Execute the following commands to change the URL addresses of the hosts and virtual appliances:

   ❑ To add a URL address for patch download and notifications for ESX/ESXi 4 or ESXi 5 hosts, run the following command:

```
vmware-umds -S --add-url https://host_URL/index.xml --url-
type HOST
```

   ❑ To add a URL address for virtual appliance upgrades, download and run the following command:

```
vmware-umds -S --add-url https://virtual_appliance_URL/
index.xml --url-type VA
```

Index

C

CD/DVD drive
  adding, to virtual machine **221, 222**
certificate authority (CA) **254**
certificate check
  enabling **255**
CHAP authentication
  about **109**
  setting up **110, 111**
Check Imbalance every option **179**
Cisco Discovery Protocol (CDP) **93**
client integration plugin
  installing **204**
clone **234**
Clone a virtual machine option **238**
Clone to Template... option **238**
cluster object
  creating **52**
cluster settings
  configuring **294**
community PVLAN **90**
condition-based alarm definition
  creating, steps **275-277**
Configure Management Network **29**
Configure Management screen **27**
Configure Options screen **65**
Consolidate snapshot option **237**
Consolidation option **237**
control plane **88**
Covert template to virtual machine option **191**
Create VM storage Profiles icon **129**
custom advanced chart view
  creating **266**
  deleting **266**
custom install method **33**
Customize Configure settings screen
  Ephemeral binding option **83**
  Network resource pool option **83**
  Number of ports option **83**
  Port allocation option **83**
  Port binding option **83**
  VLAN type option **83**
Customize default policies configuration checkbox **84**

D

database settings
  configuring **56**
Datacenter object
  creating **52**
data plane **88**
datastore cluster **182**
datastore heartbeating
  configuring **171, 172**
Datastore option **239**
Debugging and statistics option **231**
deployed virtual machine
  customizing **202, 203**
deployment modes, vCenter SSO
  basic **39**
  high availability **40**
  identity source **39**
  multisite **40**
deployment rule **20**
Direct Console User Interface (DCUI) **12, 53**
Disk Provisioning options
  Thick provision eager zeroed **216**
  Thick provision lazy zeroed **216**
  Thin provision **216**
Distributed Resource Schedule (DRS) **102**
Distributed Resource Scheduler (DRS) **52**
DNS
  configuring **25-29**
DNS records
  creating, steps **25, 26**
DPM (Distributed Power Management)
  automation levels, configuring **165**
  IPMI, configuring **163**
  working **164**
DPM cluster
  configuring, steps **162**
DRS cluster
  about **149**
  Automation Level options **149**
  compliance status, checking **154**
  creating **149, 150**
  custom virtual machine automation level, configuring **152, 153**
  disabling **156**
  DPM, enabling **162**
  ESXi hosts, adding to **151**

K

L

M

N

[PACKT] PUBLISHING enterprise

professional expertise distilled

Thank you for buying
VMware ESXi Cookbook

About Packt Publishing

Packt, pronounced 'packed', published its first book "*Mastering phpMyAdmin for Effective MySQL Management*" in April 2004 and subsequently continued to specialize in publishing highly focused books on specific technologies and solutions.

Our books and publications share the experiences of your fellow IT professionals in adapting and customizing today's systems, applications, and frameworks. Our solution-based books give you the knowledge and power to customize the software and technologies you're using to get the job done. Packt books are more specific and less general than the IT books you have seen in the past. Our unique business model allows us to bring you more focused information, giving you more of what you need to know, and less of what you don't.

Packt is a modern, yet unique publishing company, which focuses on producing quality, cutting-edge books for communities of developers, administrators, and newbies alike. For more information, please visit our website: www.PacktPub.com.

About Packt Enterprise

In 2010, Packt launched two new brands, Packt Enterprise and Packt Open Source, in order to continue its focus on specialization. This book is part of the Packt Enterprise brand, home to books published on enterprise software – software created by major vendors, including (but not limited to) IBM, Microsoft and Oracle, often for use in other corporations. Its titles will offer information relevant to a range of users of this software, including administrators, developers, architects, and end users.

Writing for Packt

We welcome all inquiries from people who are interested in authoring. Book proposals should be sent to author@packtpub.com. If your book idea is still at an early stage and you would like to discuss it first before writing a formal book proposal, contact us; one of our commissioning editors will get in touch with you.

We're not just looking for published authors; if you have strong technical skills but no writing experience, our experienced editors can help you develop a writing career, or simply get some additional reward for your expertise.

VMware View 5 Desktop Virtualization Solutions

ISBN: 978-1-84968-112-4   Paperback: 288 pages

A complete guide to planning and designing solutions based on VMware View 5

1. Written by VMware experts Jason Langone and Andre Leibovici, this book is a complete guide to planning and designing a solution based on VMware View 5.

2. Secure your Visual Desktop Infrastructure (VDI) by having firewalls, antivirus, virtual enclaves, USB redirection and filtering, and smart card authentication.

3. Analyze the strategies and techniques used to migrate a user population from a physical desktop environment to a virtual desktop solution.
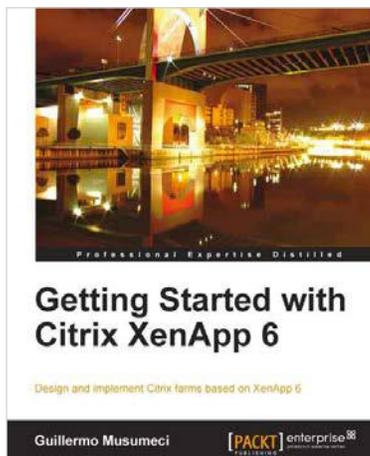
Getting Started with Citrix XenApp 6

ISBN: 978-1-84968-128-5   Paperback: 444 pages

Design and implement Citrix farms based on XenApp 6

1. Use Citrix management tools to publish applications and resources on client devices with this book and eBook.

2. Deploy and optimize XenApp 6 on Citrix XenServer, VMware ESX, and Microsoft Hyper-V virtual machines and physical servers.

3. Understand new features included in XenApp 6 and review Citrix farms terminology and concepts.
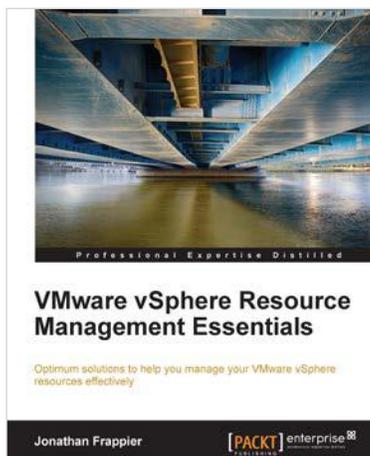
Please check **www.PacktPub.com** for information on our titles