VMware vCenter Cookbook

Over 65 hands-on recipes to help you efficiently manage your vSphere environment with VMware vCenter

Foreword by Michael Bauer, Professor, Department of Computer Science, The University of Western Ontario

Konstantin Kuminsky
In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 1 'vCenter Basic Tasks and Features'
- A synopsis of the book’s content
- More information on VMware vCenter Cookbook

About the Author

**Konstantin Kuminsky** is a VMware-, Microsoft-, and Cisco-certified IT professional with over 10 years of experience in different areas of the IT industry, including virtualization, networking, and security. His experience includes the support of Tier 3 Data Centre, the management of private Clouds, the administration of second- and third-level help desk and on-call support, as well as the deployment and support of various redundant systems and environments with high security requirements.

Konstantin is also the author of Implementing vCenter Server, published by Packt Publishing, which covers general aspects of vCenter implementation and usage.
VMware vCenter Cookbook

This book will become your assistant in the day-to-day administration of the VMware virtual environment with vCenter Server.

My goal was to make this book as practical as possible. Each chapter is focused on detailed steps on how to perform administrative tasks and implement solutions. The intention was to provide the minimum amount of theory, just enough to understand what a feature does and why it can be useful.

While there is no lack of literature about vCenter, this topic is quite broad and can't be completely covered in one book. The selection of advice and solutions included here has been made based on daily tasks I was challenged with during my work. So with high probability, most of these tasks will be useful for other administrators who work with vSphere and vCenter.

Also, one of the goals of this book was to make each recipe self-sufficient so that there is no need to read a bunch of other articles and tips to implement a particular feature or setting. That's why you will not be required to read each chapter from top to bottom. A reader should be able to open a particular device and implement the solution if it suits their requirements.

Easier recipes will be useful for administrators who are just starting to work with vCenter. More advanced administrators may benefit from solutions related to scripting and new features introduced in vSphere 5.

With Web Client, this became available in vSphere 5 and many administrators are just starting to learn it. As this transition is happening, I have focused my attention on both Web Client and traditional vSphere Client, unless it's a new feature that can be configured only in Web Client.

Finally, beside recipes with step-by-step instructions, there is general advice about NUMA and virtual CPUs more related to planning. The principles described here are important to keep in mind each time you create a new virtual machine.

Enjoy reading!
What This Book Covers

Chapter 1, vCenter Basic Tasks and Features, covers some basic solutions administrators may need to implement while working with vCenter.

Chapter 2, Increasing Environment Availability, covers availability solutions offered by vCenter, including High Availability (HA), Fault Tolerance (FT), Admission Control, backup, and replication.

Chapter 3, Increasing Environment Scalability, describes vCenter features that can improve an administrator's efficiency. These features include templates, customizations, and host profiles.

Chapter 4, Improving Environment Efficiency, covers enhancements designed to improve an environment's efficiency.

Chapter 5, Optimizing Resource Usage, discovers options available to administrators to improve resource usage. These include Distributed Resource Scheduler (DRS) and Storage DRS, VM shares, limits and reservations, and network and storage I/O control.

Chapter 6, Basic Administrative Tasks, covers administrative tasks that allow increasing an administrator's control and visibility in the environment.

Chapter 7, Improving Environment Manageability, includes advice to improve an environment's manageability by utilizing tags, new commands, netdump, virtual switch backup, and PowerCLI.
vCenter Basic Tasks and Features

In this chapter, we will cover the follow recipes:

- Choosing the right vSphere and vCenter edition
- Booting a VM from a virtual CD-ROM
- Using hosts with different CPUs in one cluster
- Fixing VMware tools to autostart after Linux updates
- Running vCenter on a VM
- Managing several vCenter Servers from one client
- Accessing new vCenter features
- Accessing hosts via SSH
- Securing host management access
- Storing host logs on a shared datastore
- Configuring remote logging

Introduction

This chapter covers some basic tasks and features administrators may need to use while working with vCenter. Most of the tips and advices in this chapter as well as in this book assume that you already have vCenter deployed and that it already has some hosts and datastores connected. You may be running vCenter with a trial license, which will work just fine if you decide to try some of the how-tos in this chapter. All features and settings described in this chapter exist in any vSphere 5 version unless otherwise noted.
Choosing the right vSphere and vCenter editions

The vCenter edition required for a particular environment is very much determined by the vSphere edition in use. The vSphere edition in turn is chosen based on the size of the environment and features that will be used.

How to do it...

To choose the vCenter edition that's right for your environment you need to:

1. Determine the vSphere features required.
2. Choose the vSphere edition based on environment size, features required, and growth expected.
3. Select the vCenter edition if it's not included in the chosen vSphere edition.

vSphere editions

A vSphere license can be bought as part of a kit or separately. Kits include a vCenter license while other vSphere editions require a separate vCenter license. When choosing a vSphere edition, it may be a good idea to take a look at its kits first. An included vCenter license will save costs. If you determine that none of the available kits include the required features and capacity, select one of the separate vSphere editions.

The following table compares five main kits available and shows the features that are included in each kit:

<table>
<thead>
<tr>
<th>Features</th>
<th>Essentials kits</th>
<th>Operations management kits (vSOM)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Essentials</td>
<td>Essentials Plus</td>
</tr>
<tr>
<td>Physical CPUs included</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vMotion</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>High Availability (HA)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Data Protection (DP)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vSphere Replication (VR)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Operations monitoring, optimization and visibility</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Kit editions are meant for smaller environments and have their limitations. Six processors included determine that the environment cannot be larger than three servers with two physical processors each. As a result, if there is a plan to grow the environment in the near future, choose one of the separate vSphere editions.

The following table shows the available vSphere editions and features included:

<table>
<thead>
<tr>
<th>Features</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Enterprise Plus</th>
<th>Standard with vSOM</th>
<th>Enterprise with vSOM</th>
<th>Enterprise Plus with vSOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical CPUs included</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(per-CPU license entitlement)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypervisor (basic virtualization capabilities)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations monitoring, optimization and visibility</td>
<td></td>
<td></td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vMotion</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>High Availability (HA)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
### vCenter Basic Tasks and Features

<table>
<thead>
<tr>
<th>Features</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Enterprise Plus</th>
<th>Standard with vSOM</th>
<th>Enterprise with vSOM</th>
<th>Enterprise Plus with vSOM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection (DP)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vSphere Replication (VR)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fault Tolerance (FT)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Storage vMotion</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Resource Scheduler (DRS)</td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Power Management (DPM)</td>
<td></td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage DRS</td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Flash Read Cache</td>
<td></td>
<td></td>
<td>+</td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

Remember that vSphere 5 is licensed per physical CPU. For instance, two physical servers with two CPUs each will require four vSphere 5 CPU licenses. If DRS is a requirement, four Enterprise licenses will be needed. To take advantage of the Storage DRS, you will need four Enterprise Plus licenses in this case.

Both the preceding tables include only the main features we believe are necessary to make a decision. A full feature comparison can be found on the Compare VMware vSphere Editions page at [http://www.vmware.com/products/vsphere/compare](http://www.vmware.com/products/vsphere/compare).

Additional information on the existing features and editions as well as upgrade paths from vSphere 4 can be found at the following link: [http://www.vmware.com/files/pdf/vsphere_pricing.pdf](http://www.vmware.com/files/pdf/vsphere_pricing.pdf)
vCenter editions
Each of the following vSphere kit editions includes one instance of vCenter:

- Essentials
- Essentials Plus
- vSOM Standard
- vSOM Enterprise
- vSOM Enterprise Plus

Other vSphere editions do not include a vCenter license, and if a separate vSphere edition has been chosen, there are two options for the vCenter edition:

- vCenter Server Foundation
- vCenter Server Standard

It is important to know that according to the End User License Agreement, customers licensed under Essentials or Essentials Plus are not allowed to purchase any other vCenter addition. If you need to manage more hosts, then the solution is to upgrade the existing license to vSphere Standard or above and purchase vCenter Standard.

The following table compares vCenter editions:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Essentials (part of Essentials or Essentials Plus kit)</th>
<th>Foundation</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of hosts that can be managed</td>
<td>3</td>
<td>3</td>
<td>1,000</td>
</tr>
<tr>
<td>Management service</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Database server</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Inventory service</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vSphere Clients</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vCenter APIs</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>vCenter Orchestrator</td>
<td></td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>Linked Mode</td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>
There's more...

There is also an option to purchase a support plan from VMware along with the software. The two available options include:

- **Basic**: Provides support during business hours
- **Production**: Provides 24 x 7 support

The production support plan is recommended for critical environments. Both plans include an unlimited number of support cases. Any of the preceding subscriptions are required for at least one year.

VMware also offers an option for per incident support, which can be purchased in 1, 3, or 5-incident packs. This option is available for vSphere Essentials kit only.

**Booting a VM from a virtual CD-ROM**

If a VM has just been created and you are trying to install the operating system from a virtual CD-ROM, you can turn the VM on, connect the ISO image to the operating system, and reboot the VM. It will start booting from the CD-ROM right away.

If the operating system has already been installed and you need to boot this VM from the CD-ROM, it may be challenging, as the option to press Esc for **Boot Menu** is displayed for a very short period of time:
How to do it...

To increase the time for which this option is displayed so that you can press Esc, you’ll need to change the **Power On Boot Delay** value. To do that, perform the following steps:

1. Go to **VM Settings** | **Options** | **Boot Options**.
2. Select the **Power On Boot Delay** option.
3. Set the value to **3,000** so that the VM waits for 3 seconds for Esc.

   4. The location of this setting in vCenter Web Client is similar:
      - Right-click on a VM
5. Go to VM Options | *Boot options.

6. Adjust the Boot Delay (*) setting.
Once Esc has been pressed, you'll get the **Boot Menu** options to choose from. Connect the ISO image, host or local CD-ROM in **VM Settings**, and choose **CD-ROM drive** from the **Boot Menu**:

Using hosts with different CPUs in one cluster

One of the core vSphere features is vMotion. It allows administrators to move a running virtual machine from one host to another without interruption.

Unfortunately, one of the requirements for vMotion is to use hosts with the same processors so that the virtual machine that has been moved can keep running on a new host. This is due to the fact that newer processors, even within the same family, typically have additional features. New generations of processors can also have a different set of instructions. When features or instructions an application is using are not available, the application will crash.

Clusters consisting of hosts with different CPU generations can use **Enhanced vMotion Compatibility (EVC)** mode. In this mode, vCenter hides CPU features and instructions that are not available on older hosts. This way, it makes all hosts' CPUs in the cluster look like they are the same.

The obvious downside of using this feature is that the cluster's processors will all be the same or lower than the oldest host's CPU.
Getting ready

Things to consider before enabling the feature are as follows:

- All hosts must have either Intel or AMD processors.
- All cluster VMs running on hosts where EVC mode will be enabled must be shut down before the feature can be turned on.

How to do it...

To enable EVC:

1. Switch to the **Hosts and Clusters** view.
2. Right-click on your cluster and choose **Edit Settings**.
3. Go to **VMware EVC** and click on **Change EVC Mode**.
4. Choose **AMD** or **Intel** depending on the host's CPU.
5. Choose the best available option for processor generation.
6. In vCenter Web Client, this setting can be found by going to **vCenter | Cluster | Manage | Settings | VMware EVC:**
7. Press the **Edit...** button next to the **VMware EVC** section to change EVC mode:

![vCenter EVC Mode Change](image)

**There's more...**

Virtual machines always have to be off when changing EVC mode to an older processor generation. This is not a requirement when EVC mode is being raised. Unfortunately, in this case, new CPU features will not be available to VMs until they are powered off and back on. Suspending or restarting VMs is not sufficient because virtual machine EVC mode is determined when it's turned on.

**Fixing VMware tools to autostart after Linux updates**

From time to time, VMware tools that have been working fine before refuse to start automatically when the Linux guest is rebooted. VMware tools can be started manually using the following command:

```
# /etc/vmware-tools/services.sh start
```
The preceding command and other commands in this book assume RHEL or CentOS and can be different for Debian or other Linux distributions.

The following error message may be displayed:

In most cases, this issue is related to recent OS updates; in particular, the Linux kernel update, which breaks the existing VMware tools installation.

As servers are not rebooted often, it may be hard to correlate the issue of VMware tools not starting automatically and OS updates.

How to do it...

To fix the issue, simply reinstall VMware tools the same way they were installed the first time. The following commands have been tested on CentOS 5 and depending on the Linux distribution, the commands you use and their sequence may be different.

1. Initiate the VMware tools installation by going to VM menu and then navigating to Guest | Install/Upgrade VMware Tools:

2. For Linux guest, the Automatic option will not be available. Click on OK.
3. The VMware tools ISO image from the ESXi host will be connected to the virtual CD-ROM of the VM.

4. Mount the image as follows:
   
```
   # mount /dev/cdrom /mnt/cdrom
   ```

5. Extract the archive with VMware tool's installation files:
   
```
   # tar xzvf /mnt/cdrom/VMwareTools-<x.x.x-xxxx>.tar.gz -C /tmp/
   ```

6. Start the installation. Switch –d is for the unattended installation with default settings:
   
```
   # cd /tmp/vmware-tools-distrib/
   # ./vmware-install.pl -d
   ```

7. Reboot the virtual machine. VMware tools should start automatically as soon as the guest OS is back up:

```
   # shutdown -r now
   ```

There's more...

Additional details about the issue can be found in the VMware KB 2050592 article on the VMware Knowledge Base website at http://kb.vmware.com/kb/2050592.

Running vCenter on a VM

Administrators have three options when it comes to deploying the vCenter Server. vCenter can be imported as a Linux-based virtual appliance or it can be installed on a physical or virtual Windows Server.

How to do it...

For smaller environments, it makes sense to choose a vCenter appliance. Its installation and configuration is easier than deploying your own vCenter Server:

1. Download the vCenter Server Appliance from my.vmware.com.
2. Deploy the appliance from a template using the **Deploy OVF Template...** option from the **File** menu.

![Deploy OVF Template... menu option]

3. Open your web browser and go to `http://<ip address of virtual appliance>:5480`.

4. Log in using the default credentials to configure vCenter:
   - Username: `root`
   - Password: `vmware`

5. After logging in, go through the steps of the configuration wizard to start using the appliance.

**There's more...**

vCenter Appliance has its limitations. First of all, if an embedded database is used, this server will be able to manage only up to five hosts and up to 50 virtual machines. In vSphere 5.5, this limit has been increased to 100 hosts and 3,000 virtual machines.

Also, this solution doesn't support the Linked Mode configuration. More information about the supported services and limitations can be found in the Knowledge Base article KB2002531 at `http://kb.vmware.com/kb/2002531`.

**vCenter Server on a VM**

Running the vCenter Server on a virtual machine offers all virtualization advantages:

- No additional hardware is needed, which means savings and flexibility.
- Administrators can take advantage of using high availability features offered by vSphere—HA or FT.
- vMotion offers additional flexibility and higher uptime.
- Snapshots can be utilized as a rollback option.
Virtual machines are easier to manage but at the same time, there are a few concerns related to this approach:

1. The main concern is that issues with the vSphere environment potentially can affect the vCenter Server and as a result, the administrator’s ability to manage the environment and troubleshoot issues.
   
   For example, if a host where vCenter VM is running becomes unavailable, vCenter is not accessible until it’s restarted and comes back online. In certain cases, HA fails to restart some VMs so vCenter may become unavailable for a longer time.
   
   The administrator can connect to hosts directly using the vSphere Client but in this case, the core features offered by vCenter will not be available.

2. Another concern is related to environments that have only one host. Certain tasks such as ESXi updates require host maintenance mode, which means that all VMs need to be turned off. In this case, the vCenter Server has to be shut down and thus, Update Manager can’t be used.

   Updating ESXi from the command line can be more time consuming and challenging in certain cases. In other words, running the vCenter Server on a VM in environments with only one ESXi host can introduce some administrative difficulties.

   In general, a single ESXi host with vCenter Server VM is not a recommended design option for the enterprise environment.

**Managing several vCenter Servers from one client**

There is a way to manage more than one vCenter Server from the same vCenter client. This is accomplished by using Linked Mode groups. Linked Mode group is a group of vCenter Servers that allows managing other members by connecting to any one of them.

**Getting ready**

This feature is available only in vCenter Server Standard edition and cannot be used with vCenter Server Appliance (vCSA).
Chapter 1

The main requirement is that all group members must run the same version of vCenter. Other requirements are as follows:

- Members must belong to the same Active Directory domain or different domains that have two-way trust relationships with each other.
- DNS has to be operational for Linked Mode groups to work properly.
- vCenter must be licensed or in evaluation mode.
- The domain account is the local administrator on both vCenter Servers—the one that is being joined to the group and the target server.

How to do it...

To be able to manage additional vCenter Servers, they need to be joined to the Linked Mode group.

Joining vCenter to a group

The vCenter Server can be joined to a group either during installation or any time after. The Linked Mode group is created when the first member is being joined to a group that doesn’t exist.

To join the running vCenter Server to the existing Linked Mode group, follow the ensuing steps:

1. On the vCenter Server, go to Start | All Programs | VMware.
2. Run vCenter Server Linked Mode Configuration.
3. Select Modify linked mode configuration.
4. Click on Join this vCenter server instance to an existing linked mode group or another instance.
5. Click on Next.
6. Enter the FQDN of an existing member and LDAP port.
7. In case role conflict has been detected, choose a way to resolve it. You can either let vCenter rename the group or you can rename it yourself.
8. Restart the vCenter Server.

If a member that is being joined to the Linked Mode group is running an older version of vCenter than other members of the group it has to be upgraded. Also, if vCenter on a member is upgraded, it will be disconnected from the group.
Removing vCenter from a group

To remove vCenter from a Linked Mode group, execute the following steps:

1. On the vCenter Server, go to Start | All Programs | VMware.
2. Run vCenter Server Linked Mode Configuration.
3. Choose Modify linked mode configuration.
4. Select Isolate this vCenter server instance from linked mode group and click on Next.
5. Click on Continue and then on Finish.
6. Reboot the vCenter Server.

Accessing new vCenter features

vSphere 5 introduced a new web client, which can be used to manage the environment along with the traditional vSphere Client we used before.

vCenter Web Client is just another way to access the environment using a web browser. Three major browsers—Internet Explorer, Firefox, and Chrome—are supported.

Web Client becomes the main administrative interface starting with vSphere 5.1 and while vSphere Client can still be used, a lot of new features introduced in vSphere 5 are available only through Web Client.

Some of these new features are:

- Datastore cluster and Storage DRS
- vSphere Replication
- vSphere Data Protection
- Enhanced vMotion
- Drag-and-drop actions as well as bulk operations for vSphere objects

How to do it...

1. To access your vSphere environment using Web Client, open your web browser and point it to https://<vCenter Server IP address>:9443/vsphere-client.
2. On the VMware vSphere welcome page, click on the Log in to vSphere Web Client link.
3. From this page, you will be able to log in to vCenter using the same credentials that work for older clients.

**There's more...**

Take a look at the following error message:
If the preceding error message is displayed, add port 9443 after the vCenter Server address or name in the URL: https://<vcenter-server>:9443/vsphere-client/. This will take you to the same login page, assuming vCenter was installed with default port settings.

**Accessing hosts via SSH**

In certain cases, you may need to access the ESXi host via SSH. This may be needed to run a script, troubleshoot an issue, or use a command or a feature not available via vSphere Client.

**How to do it...**

SSH access to ESXi hosts is disabled by default and can be enabled using the ESXi console and command line or through vCenter. To enable it from vCenter:

1. Allow SSH port through the host's firewall.
2. Start the SSH service on the host.

**Opening the SSH port on the firewall**

To allow the SSH port through the firewall on the ESXi host, execute the following steps:

1. Go to the *Hosts and Clusters* view.
2. Select the host and go to the *Configuration* tab.
3. Click on *Security Profile* on the left.
4. Click on the **Properties...** link next to the **Firewall** section.
5. The Firewall Properties window will open. Check **SSH Server** under the **Secure Shell** section.
6. Click on the **Firewall** button to allow only certain IP addresses to connect. Click on **OK** when finished to apply the changes.

In Web Client, perform the following steps:

1. Select a host.
2. Go to **Manage | Settings | Security Profile**.

3. Click on the **Edit...** button next to the **Firewall** section.
4. Select the **SSH Server** option and click on **OK** as shown in the next screenshot.

To allow connections from only certain IP addresses, uncheck the **Allow connections from any IP address** option and enter the IP addresses separated by commas.

**Starting an SSH service**

To start an SSH service on the host from the same place under **Configuration | Security Profile**:

1. Click on the **Properties...** link next to the **Services** section.
2. Select **SSH** in the list of services and click on **Options**.

![Services Properties](image)

3. Click on the **Start** button.

4. Once the service starts, both windows can be closed.

From Web Client, perform the following steps:

1. Select a host.

2. Go to **Manage | Settings | Security Profile**.
vCenter Basic Tasks and Features

3. Scroll down to the **Services** section.

4. Click on the **Edit** button.

5. Select **SSH** from the list.

6. Click on **Start**.
There's more...

Now you will be able to access the ESXi command line using the SSH client.

Note that when SSH service is running on the host, vCenter marks it with a yellow exclamation mark as it is a configuration issue. Enabling SSH is considered to be an insecure practice.

Securing host management access

When it comes to managing ESXi hosts, there are a few interfaces available to perform management tasks:

- **Common Information Model (CIM)**, which is used for vCenter Server access.
- **Direct Console User Interface (DCUI)**, which is also known as the ESXi console.
- **Tech Support Mode (TSM)**
  - Local—console access to the ESXi command line.
  - Remote—SSH access to the ESXi command line.
- **vSphere Application Programming Interface (API)** such as vSphere Client, PowerCLI, vCLI, and so on.

Remote TSM has been covered in the Accessing hosts via SSH recipe in this chapter. Local TSM and DCUI are console options available if you have physical access to the host or remote console access such as iDRAC.
All interfaces except vSphere API can be managed from vCenter under host **Configuration | Security Profile | Services:**

Both TSM options can also be configured from the DCUI console.
The following table summarizes different management interfaces and where each one can be configured:

<table>
<thead>
<tr>
<th>Management Interface</th>
<th>Description</th>
<th>Configuration from vCenter</th>
<th>Configuration from DCUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>vCenter access</td>
<td>Host's Services</td>
<td></td>
</tr>
<tr>
<td>DCUI</td>
<td>ESXi console</td>
<td>Host's Services</td>
<td></td>
</tr>
<tr>
<td>Local TSM</td>
<td>Console CLI</td>
<td>Host's Services</td>
<td>Troubleshooting menu</td>
</tr>
<tr>
<td>Remote TSM</td>
<td>SSH access to CLI</td>
<td>Host's Services</td>
<td>Troubleshooting menu</td>
</tr>
<tr>
<td>APIs</td>
<td>vSphere Client, PowerCLI, vCLI</td>
<td>Host's Services</td>
<td></td>
</tr>
</tbody>
</table>

VMware offers a way to secure management access to hosts called **Lockdown mode**.

**Lockdown mode** is a security feature, which limits the administrator's ability to manage the ESXi host only through vCenter. When a host is in this mode, the administrator cannot use the command line or run scripts. Also, any third-party software cannot get or change any settings on this host.

![User root will still be able to access DCUI but not TSM.]

The following table summarizes each management interface's behavior in Normal and Lockdown modes:

<table>
<thead>
<tr>
<th>Management Interface</th>
<th>Normal mode</th>
<th>Lockdown mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM</td>
<td>User and group permissions</td>
<td>Only vCenter server</td>
</tr>
<tr>
<td>DCUI</td>
<td>User root and users with administrator rights</td>
<td>Only root user</td>
</tr>
<tr>
<td>Local TSM</td>
<td>Only root user</td>
<td>None</td>
</tr>
<tr>
<td>Remote TSM</td>
<td>Only root user</td>
<td>None</td>
</tr>
<tr>
<td>APIs</td>
<td>User and group permissions</td>
<td>Only vCenter vpxuser</td>
</tr>
</tbody>
</table>

Additional security always means inconvenience. If the vCenter VM crashed or didn't come up after the reboot, and access to vCenter has been lost, ESXi has to be reinstalled on hosts that are in Lockdown mode to restore access.
vCenter Basic Tasks and Features

How to do it...

To enable lockdown mode from vCenter, execute the following steps:

1. Lockdown mode can be enabled per host by going to Configuration | Security Profile:

   - Lockdown mode can be enabled per host by going to Configuration | Security Profile:

2. Click on Edit next to Lockdown Mode, select Enable Lockdown Mode, and click on OK:
All the existing vCenter Client connections to the host will be dropped immediately.

Users that are currently logged in to DCUI or TSM will still have access after Lockdown mode has been enabled until they log off. Logged in users will not be able to switch Lockdown mode off in this case.

All the existing user and group permissions will be restored once Lockdown mode is disabled if it was enabled from vCenter.

To enable Lockdown Mode from Web Client, execute the following steps:

1. Select a host.
2. Go to Manage | Settings | Security Profile.
3. Scroll down to the Lockdown Mode section.
4. Click on the Edit next to the section.
5. Check Enable Lockdown Mode.
6. Click on OK.
Enable Lockdown mode from the ESXi console
To enable Lockdown mode from DCUI, press F2, log in with the root user, move the cursor to the **Configure Lockdown Mode** item, and press Enter.

<table>
<thead>
<tr>
<th><strong>System Customization</strong></th>
<th><strong>Configure Lockdown Mode</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Password</td>
<td>Enabled</td>
</tr>
<tr>
<td>Configure Lockdown Mode</td>
<td></td>
</tr>
<tr>
<td>Configure Management Network</td>
<td></td>
</tr>
<tr>
<td>Restart Management Network</td>
<td></td>
</tr>
<tr>
<td>Test Management Network</td>
<td></td>
</tr>
<tr>
<td>Disable Management Network</td>
<td></td>
</tr>
<tr>
<td>Restore Standard Switch</td>
<td></td>
</tr>
<tr>
<td>View Keyboard</td>
<td></td>
</tr>
<tr>
<td>View Support Information</td>
<td></td>
</tr>
<tr>
<td>View System Logs</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Options</td>
<td></td>
</tr>
<tr>
<td>Reset System Configuration</td>
<td></td>
</tr>
<tr>
<td>Remove Custom Extensions</td>
<td></td>
</tr>
<tr>
<td>&lt;Up/Down&gt; Select</td>
<td>&lt;Enter&gt; Change &lt;Esc&gt; Log Out</td>
</tr>
</tbody>
</table>

All the existing user and group permissions will be lost once Lockdown mode is enabled from DCUI so the best practice is to use vCenter to enable Lockdown.

Storing host logs on a shared datastore
ESXi server logs are stored locally by default on each host in the /var/log directory. In certain cases, there is a requirement to store logs on a datastore.

Possible scenarios are hosts without local storage, where all locally stored logs disappear after reboot, compliance requirements where there is a requirement to store logs in an alternative location, or space concerns where there are many hosts and the administrator has to keep older logs.
How to do it...

vCenter allows redirecting ESXi logs to one of the datastores accessible to the host. This can be accomplished by going to Configuration | Advanced Settings | Syslog by changing the variable Syslog.global.logDir to an appropriate value [Datastore]/Folder:
In vCenter Web Client, these options can be found by going to **Host | Manage | Settings | Advanced System Settings**, as shown in the following figure:

![Advanced System Settings](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scsi.TimeoutITMThreadMin</td>
<td>1</td>
</tr>
<tr>
<td>Scsi.TimeoutITMThreadMax</td>
<td>1800</td>
</tr>
<tr>
<td>Scsi.TimeoutITMThreadExplicit</td>
<td>2000</td>
</tr>
<tr>
<td>Scsi.TimeoutITMThreadLatency</td>
<td>2000</td>
</tr>
<tr>
<td>Scsi.ScanDiskStalledQueueLatency</td>
<td>500</td>
</tr>
<tr>
<td>Scsi.ComportLUNNumber</td>
<td>1</td>
</tr>
<tr>
<td>Scsi.UseAdaptiveRotates</td>
<td>1</td>
</tr>
<tr>
<td>Scsi.ChangeGEOMSetting</td>
<td>1</td>
</tr>
<tr>
<td>Scsi.ScanSync</td>
<td>0</td>
</tr>
<tr>
<td>Scsi.FaultVMComCPD</td>
<td>0</td>
</tr>
<tr>
<td>SunRPC.WorldwideMin</td>
<td>2</td>
</tr>
<tr>
<td>SunRPC.MaxCommPerWP</td>
<td>4</td>
</tr>
<tr>
<td>SunRPC.SendLowlat</td>
<td>25</td>
</tr>
<tr>
<td>ScmHton.ScmMotionLogDisksPerVM</td>
<td>8</td>
</tr>
<tr>
<td>Systlog.global.defaultRollate</td>
<td>0</td>
</tr>
<tr>
<td>Systlog.global.defaultSize</td>
<td>1024</td>
</tr>
</tbody>
</table>

**Syslog.global.logDir**

- `/vmfs/log` `/vmkadms/logout/systemlogs`
- Systlog.global.logOmitUnique: false
- Systlog.global.log-host: `udp://192.168.15.51:514`
- Systlog.loggers.Xlog.retenta: 8
There's more...

Once this change is made, you will see log files created in the configured folder if you browse the datastore.

From the same Advanced Settings section, you can configure the additional logging options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog.global.logDirUnique</td>
<td>If chosen the ESXi syslog will create a separate folder for this host in the specified logging folder. The folder will be named with the ESXi hostname. This option is helpful when the logging folder is shared between more than one host.</td>
</tr>
<tr>
<td>Syslog.global.defaultRotate</td>
<td>This is the maximum number of log files to keep after rotation.</td>
</tr>
<tr>
<td>Syslog.global.defaultSize</td>
<td>This is the maximum log file size in kilobytes. Once reached, the log file will be rotated.</td>
</tr>
</tbody>
</table>

The same logging parameters can also be configured from the ESXi command line using the esxcli system syslog command.

For example, to validate logging settings configured from vCenter use:

```
esxcli system syslog config get
```

VMware KB 2003322 gives more details about configuring syslog, including CLI command sequence, which is available at [http://kb.vmware.com/kb/2003322](http://kb.vmware.com/kb/2003322).

Configuring remote logging

For compliance and security reasons, administrators may need to redirect ESXi logs to a remote syslog server.
How to do it...

This configuration is done by going to Configuration | Advanced Settings | Syslog and changing the variable Syslog.global.logHost to <protocol>://<syslog host>:<port> as shown in the following screenshot:

From Web Client, perform the following steps:

1. Go to Manage | Settings | Advanced System Settings.
2. Select the Syslog.global.logHost option in the list.
3. Click on the Edit button above the list.
4. Adjust the value of the Syslog.global.logHost option.
5. Click on OK.
In most cases, syslog uses UDP and that's why in case of high logging volume or high network utilization, some log entries may be lost. Consider this when planning the logging infrastructure.

You can configure the syslog and datastore logging mentioned in storing host logs on a shared datastore at the same time for each host.

Also, administrators may need to configure the ESXi firewall to allow outbound syslog traffic. This is done by going to Configuration | Security Profile | Firewall and performing the following steps:

1. Click on Properties next to the Firewall section.
2. Make sure syslog is chosen.
3. Click on OK.
Alternatively, from Web Client, perform the following steps:

1. Select a host.
2. Go to Manage | Settings | Security Profile.
3. Click on the Edit button next to the Firewall section.
4. Select syslog in the list.
5. Click on OK.

Once this configuration is completed the remote syslog server will start receiving logging data.
Where to buy this book

You can buy VMware vCenter Cookbook from the Packt Publishing website.
Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.
Click here for ordering and shipping details.