# Table of Contents

Lab Overview - HOL-2010-01-SDC - Virtualization 101: Introduction to vSphere ............ 2  
  Virtualization ........................................................................................................... 3  
  Lab Guidance ......................................................................................................... 14  

Module 1 - Introduction to Management with vCenter Server (60 Min)............................. 20  
  Introduction............................................................................................................. 21  
  Hands-on Labs Interactive Simulation: ESXi Installation and Configuration .............. 22  
  ESXi Host Client .................................................................................................... 23  
  vCenter 6 Overview .............................................................................................. 31  
  vCenter Server and Creating a Virtual Machine ...................................................... 37  
  Cloning Virtual Machines and Using Templates .................................................... 70  
  Using Tagging and Search to Find Objects Quickly ................................................ 84  
  Understanding vSphere Availability and Distributed Resource Scheduler (DRS) ... 98  
  vSphere 6 Fault Tolerance Provides Continuous Availability .................................. 115  
  Monitoring Events and Creating Alarms .................................................................. 118  
  Configure Shares and Resources ......................................................................... 140  
  Migrating Virtual Machines with VMware vMotion ............................................. 147  
  vSphere Monitoring and Performance .................................................................. 158  

Module 2 - Introduction to vSphere Networking and Security (60 Min) ......................... 173  
  Introduction............................................................................................................. 174  
  Adding and Configuring vSphere Standard Switch ............................................... 178  
  Working with the vSphere Distributed Switch ..................................................... 211  
  Using Host Lockdown Mode .................................................................................. 255  
  User Access and Authentication Roles ................................................................... 279  
  Understanding Single Sign On ............................................................................. 294  
  Adding an ESXi Host to Active Directory ............................................................... 314  

Module 3 - Introduction to vSphere Storage (60 Min) ..................................................... 322  
  vSphere Storage Overview ..................................................................................... 323  
  Creating and Configuring vSphere Datastores ..................................................... 327  
  Storage vMotion .................................................................................................... 368  
  Managing Virtual Machine Disks .......................................................................... 377  
  Working with Virtual Machine Snapshots ............................................................ 388  
  vSphere Datastore Cluster .................................................................................... 404  

Appendix ................................................................................................................. 413  
  For More Information .......................................................................................... 414
Lab Overview - HOL-2010-01-SDC - Virtualization 101: Introduction to vSphere
Virtualization

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

If you are familiar with virtualization or have taken this lab previously, you can jump ahead to the Lab Guidance section.

What is Virtualization:

Today's x86 computer hardware was designed to run a single operating system and a single application, leaving most machines vastly underutilized. Virtualization lets you run multiple virtual machines on a single physical machine, with each virtual machine sharing the resources of that one physical computer across multiple environments. Different virtual machines can run different operating systems and multiple applications on the same physical computer.
Virtualization is placing an additional layer of software called a hypervisor on top of your physical server. The hypervisor enables you to install multiple operating systems and applications on a single server.
Separation

Virtualization Defined

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

...by presenting a complete x86 platform to the OS.

By isolating the operating system from the hardware, you can create a virtualization-based x86 platform. VMware’s hypervisor-based virtualization products and solutions provide you the fundamental technology for x86 virtualization.
Partitioning

Key Properties of Virtual Machines

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

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

You can isolate a VM to find and fix bugs and faults without affecting other VMs and operating systems. Once fixed, an entire VM Restore can be performed in minutes.
Encapsulation simplifies management by helping you copy, move and restore VMs by treating entire VMs as files.
Hardware Independence

Key Properties of Virtual Machines: Continued

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

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

How Do I Get Those Benefits?

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

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

Availability - Introducing virtualization to increase application availability and data recoverability

...there are many more benefits of virtualization

Virtualization enables you to consolidate servers and contain applications, resulting in high availability and scalability of critical applications.
Virtualization eliminates the need for any hardware configuration, OS reinstallation and configuration, or backup agents. A simple restore can recover an entire VM.
Reduce Storage Costs

Better Storage Utilization and Efficiency

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

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

The CapEx Story: Better use of existing infrastructure

<table>
<thead>
<tr>
<th>Before VMware</th>
<th>After VMware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Servers</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Utilization</strong></td>
<td>8%</td>
</tr>
<tr>
<td><strong>Annual cost per server</strong></td>
<td>$4,000</td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td>$40,000</td>
</tr>
<tr>
<td><strong>Servers</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Utilization</strong></td>
<td>80%</td>
</tr>
<tr>
<td><strong>Annual cost per server</strong></td>
<td>$4,000</td>
</tr>
<tr>
<td><strong>Total Cost</strong></td>
<td>$12,000</td>
</tr>
</tbody>
</table>

$28,000 in cost avoidance

Source: IT Business Edge, “The Business Value of Server Virtualization” – cost for average a 2 x CPU server in three-year amortized hardware purchase, and annual support and maintenance contract costs [$07]
Lab Guidance

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

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

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

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

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

Lab Captains: Doug Baer, Dave Rollins, A.J. Ciampa

A copy of this manual can be downloaded in PDF format:


or viewed in HTML:

http://docs.hol.vmware.com/HOL-2020/hol-2010-01-sdc_html_en/

This lab may be localized. To see if this lab has been localized in your language and how to change your preferences to see it, you may review this PDF:

http://docs.hol.vmware.com/announcements/nee-localization.pdf
1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the EXTEND to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key

1. Click on the "@" key.

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes.
Module 1 - Introduction to Management with vCenter Server (60 Min)
Introduction

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

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

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

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

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

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

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

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

For additional details on the VMware Host Client, please see this PDF (https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-html-host-client-125-guide.pdf)

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

Launch Chrome

1. Launch Google Chrome from the desktop.
Select esx-03a

From the Bookmarks bar, select esx-03a.

Login

1. Login with the following credentials:
   - **User name**: root
   - **Password**: VMware1!

2. Click the **Log in** button.
ESXi Host Client

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

The initial screen shows high level details and recent tasks. There are also various power options for the host and an Actions menu for the most common tasks. Note that the server is current in Maintenance Mode, which will be discussed in a future lesson.

1. Click to minimize the Recent tasks interface to gain more room.
2. Click on Manage.
System

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

1. Click on the Hardware tab.

Hardware

1. Click Power Management.

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

2. Click the Services tab.
Services

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

1. Click on **Security and Users**.

Security & Users

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

1. Click on **Monitor**.
Monitor

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

1. Click the **Logs** tab.

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

2. Click the **Generate Support Bundle** button. This operation will take a minute or two to complete.

**Credentials?**

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

- User name: root
- Password: VMware1!
Support Bundle Completed

1. Click the Dismiss button.

Note that the bundle will be deleted after 15 minutes.

VMs, Storage and Networking

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

Since these features will be covered throughout the lab and the actions performed are identical, just at the vCenter Server level, we will not be reviewing them here.
The ESXi Host Client can be very useful in situations where a vCenter Server is not present to manage the host. However, when a vCenter Server is present, it is the preferred option and provides better tools to manage your infrastructure as a whole.
vCenter 6 Overview

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

vSphere v6 Components

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

The other component is the vSphere Web Client. The vSphere Web Client is the interface to vCenter Server and multi-host environments. It also provides console access to virtual machines. The vSphere Web Client lets you perform all administrative tasks by using an in-browser interface.
vCenter 6 Components

Starting with vSphere 5.1 there are two methods to deploy vCenter. The first method is a Windows installation. With the Windows method, you can install vCenter Single Sign On, Inventory Service, and vCenter Server on the same host machine (as with vCenter Simple Install) or on different virtual machines.

The other method is a virtual appliance. The vCenter Server Appliance (vCSA) is a single preconfigured Linux-based virtual machine optimized for running vCenter Server and associated services.

Platform Services Controller (PSC)

vCenter Server with Embedded PSC and ELM
Simplified Architecture

Enhanced Linked Mode
Greenfield deployments
Supports maximums scale
No load balancer
VCHA supported
Site boundary removed

*vCenter Server Appliance Only*
The Platform Services Controller (PSC) includes common services that are used across the suite. These include Single Sign-On (SSO), Licensing, and the VMware Certificate Authority (VMCA). You will learn more about SSO and the VMCA in the following pages.

The PSC is the first piece that is either installed or upgraded. When upgrading an SSO instance becomes a PSC. There are two models of deployment, embedded and centralized.

- **Embedded** means the PSC and vCenter Server are installed on a single virtual machine. Embedded is recommended for sites with a single SSO solution such as a single vCenter.
- **Centralized** means the PSC and vCenter Server are installed on different virtual machines. Centralized is recommended for sites with two or more SSO solutions such as multiple vCenter Servers, vRealize Automation, etc. When deploying in the centralized model it is recommended to make the PSC highly available as to not have a single point of failure, in addition to utilizing vSphere HA a load balancer can be placed in front of two or more PSC’s to create a highly available PSC architecture.

The PSC and vCenter servers can be mixed and matched, meaning you can deploy Appliance PSC’s along with Windows PSC’s with Windows and appliance-based vCenter Servers. Any combination uses the PSC’s built in replication.

**Use Case:**

- The PSC removes services from vCenter and makes them centralized across the vCloud Suite.
- This gives customers a single point to manage all their vSphere roles and permissions along with licensing.
- Reducing vCenter Server installation complexity allows customers to install or upgrade to vSphere 6 faster.
- There are only two installs options:
  - Embedded PSC which installs all components on a single virtual machine
  - Centralized, the customer must install the PSC and vCenter Server separately

- In either installation model all vCenter Server services are installed on the vCenter Server reducing the complexity of planning and installing vCenter Server.

**vCenter Single Sign On**

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

**vCenter Single Sign On - Typical Deployment**

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

Authentication with vCenter Single Sign-On makes vSphere more secure because the vSphere software components communicate with each other by using a secure token exchange mechanism, and all other users also authenticate with vCenter Single Sign-On.
Starting with vSphere 6.0, vCenter Single Sign-On is either included in an embedded deployment, or part of the Platform Services Controller. The Platform Services Controller contains all of the services that are necessary for the communication between vSphere components including vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service, and the licensing service. For example, in the image above, SSO resides within the Platform Services Controller as part of this multi-vCenter topology. Both Windows and the vCSA can participate in this topology.

**vCenter Single Sign On - Single vCenter**

In a single vCenter topology, the PSC (along with all of its associated services) can run on a single machine, also called the embedded deployment. This single machine could be a physical Windows server, a Windows VM, or the vCSA.

While vCenter Server requires a database as shown above, SSO itself does not have such a requirement.
More Information on Single Sign On

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

However, you can also refer to the vCenter 6 Deployment Guide for more in-depth requirements and considerations for SSO architecture in vCenter 6:

vCenter Server and Creating a Virtual Machine

The previous lesson reviewed the ESXi Host Client, which can be used to manage one ESXi host at a time. This lesson will introduce the vSphere Client which is used to connect to vCenter Server to manage your collective infrastructure as a whole. In addition, the process of creating a virtual machine will also be covered.

The vSphere Client is the primary method for system administrators and end users to interact with the virtual data center environment created by VMware vSphere. vSphere manages a collection of objects that make up the virtual data center, including hosts, clusters, virtual machines, data storage, and networking resources.

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

- Viewing health, status, and performance information on vSphere objects
- Issuing management and administration commands to vSphere objects
- Creating, configuring, provisioning, or deleting vSphere objects

You can extend vSphere in different ways to create a solution for your unique IT infrastructure. You can extend the vSphere Client with additional GUI features to support these new capabilities, with which you can manage and monitor your unique vSphere environment.
Launch Chrome

If you are not already in Chrome, double click the Google Chrome.

Select vSphere Client

1. Click the vSphere Client bookmark.
Login to vCenter

Log in using the following method:

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

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

1. Click on the Menu drop-down list and select **Global Inventory Lists**.

Clicking Global Inventory Lists will take you to the inventory page where you find all the objects associated with vCenter Server systems such as data centers, hosts, clusters, networking, storage, and virtual machines.
Child objects, Data Centers, and Hosts

1. Click the "Virtual Machines" inventory item. By selecting this inventory item, you are presented with a list of the VMs which are located in this environment.
Virtual Machine Summary

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

1. Click the "windows10" virtual machine.
2. Click the "Summary Tab" for that virtual machine. On this page, you are able to see all the details regarding the virtual machine. There is a "Edit Settings" link as well to modify the settings of the virtual machine.
3. Expand the VM Hardware section.
Edit the settings of a virtual machine.

1. Review the VM Hardware for the windows10 virtual machine. Note that there is currently only one network adapter.
2. Use the scroll bar to move to the bottom of the VM Hardware section.
3. Click "Edit Settings" so a second network adapter can be added to the virtual machine.
Add a second network adapter

Add another network adapter to the windows10 machine.

1. In the Edit Setting window, click the **Add New Device** button.
2. Select **Network Adapter** from the drop-down list.
Configure the Second Network Card.

1. Click the arrow next to the New Network card to expand and view its settings. Notice that the MAC address is blank at this point. A new MAC address will be generated once this NIC is added or we are able to specify (with some rules) our own MAC address.

2. Click "OK" to add the device to the VM. When you select "OK" a new task is created.

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

### Recent Tasks List

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

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

### Create a Virtual Machine

In the next steps, we will walk through the process of creating a virtual machine and then installing an operating system.

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

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

Start the New Virtual Machine Wizard
1. Right click on Site A Datacenter.
2. Click New Virtual Machine to start the new virtual machine wizard.

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

**Virtual Machine wizard**

1. Since the Create a new virtual machine wizard is highlighted, just click Next.
1. Enter **web-serv01** for the name of the new virtual machine.
2. Click **Next**
Virtual Machine Placement

Because Distributed Resource Scheduler (DRS) is enabled, you just have to select a cluster and DRS will determine which host to use for the VM. More details on DRS will be covered later in this module.

1. Click **Site A Cluster 1**
2. Click **Next**
Select Storage

New Virtual Machine

1. Ensure the *ds-iscsi01* datastore is selected
2. Click **Next**
1. Click **Next** to accept the default **ESXi 6.7 and later**
In this step, we will be selecting what operating system we will be installing. When we select the operating system, the supported virtual hardware and recommended configuration is used to create the virtual machine. Keep in mind this does not create a virtual machine with the operating system installed, but rather creates a virtual machine that is tuned appropriately for the operating system you have selected.

1. For the **Guest OS Family**, select **Linux** from the drop-down menu.
2. For the **Guest OS Version**, select **VMware Photon OS (64-bit)**.
3. Click **Next** to continue.
Change Virtual Disk Size.

The recommended virtual hardware settings are shown as the default. These can be modified if needed.

1. Leave the default settings and click **Next**
Ready to complete

The settings for the virtual machine can be verified prior to it being created.

1. Click **Finish** to create the virtual machine
Congratulations on creating your first virtual machine!

In the next steps, Photon OS will be installed on the virtual machine.
Attaching an ISO to a Virtual Machine

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

1. To attach an ISO image to the virtual machine we just created, make sure web-serv01 is selected.
2. Right click on web-serv01 and select Edit Settings...
1. From the **CD/DVD drive 1** drop-down menu, select **Content Library ISO File**. This will open a file explorer to select that file.
Select Photon

Choose an ISO image to mount

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

Connect the drive

1. Click **Connect...**
2. Click **OK**

Finally, we want to attach or connect the ISO image to the virtual machine.
1. Click the **Connected** check box next to **CD/DVD drive 1**.
2. Click **OK**.

**Power on web-serv01**

![Power on web-serv01](image)

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

**Launch Console**

![Launch Console](image)

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

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

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

1. Press the **Enter** key to start the installation process.
After the boot process is complete, you will be presented with a license agreement.

1. Press Enter to accept
Select Disk

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

Confirm

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

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

Linux Kernel

1. Use the arrow key to select **2. Generic**
2. Press the **Enter** key.

**NOTE:** If 1. Hypervisor optimized is selected, the virtual machine will not boot. This is due to the unique environment the Hands-on Labs are running in.
**Rename Host**

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

**Password**

1. For the password, use `VMware1!VMware1`!

Note that Photon requires a complex, non-dictionary password, which is why the typical password is being repeated.

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

## Installation Complete

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

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

### vSphere Tab

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

1. Select the vSphere- web-serv01 tab.
Make sure **web-serv01** is still highlighted

1. Right click on **web-serv01**
2. Select **Edit Settings...**
**Disconnect CD/DVD**

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

**web-serv01 Console**

1. Click the 'X' to close the console window for web-serv01.
Cloning Virtual Machines and Using Templates

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

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

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

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

Navigate to the VMs and Templates management pane
1. Select **VMs and Templates** from the **Menu**.

**Launch the Clone Virtual Machine to Template wizard**

1. Right-click the Virtual Machine **tinyLinux2**.
2. Select **Clone**
3. Select **Clone to Template...**
Select a name and folder

**tinyLinux2** - Clone Virtual Machine To Template

1. In the Clone Virtual Machine to Template wizard, provide a name for the Template - **tinyLinux2 Template**

   Please leave the location as **Site A Datacenter** for this lab.

2. Click **Next**
Select Compute Resource

tinyLinux2 - Clone Virtual Machine To Template

Select a compute resource:

1. Choose **Site A Cluster 1**
2. Click **Next**
Select Storage

tinyLinux2 - Clone Virtual Machine To Template

1. Select **ds-nfs01** for the datastore
2. Press the **Next** button.
Review the VM Template Settings

**tinyLinux2 - Clone Virtual Machine To Template**

<table>
<thead>
<tr>
<th>Provisioning type</th>
<th>Clone virtual machine to template</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source virtual machine</td>
<td>tinyLinux2</td>
</tr>
<tr>
<td>Template name</td>
<td>tinyLinux2 Template</td>
</tr>
<tr>
<td>Folder</td>
<td>Site A Datacenter</td>
</tr>
<tr>
<td>Cluster</td>
<td>Site A Cluster 1</td>
</tr>
<tr>
<td>Datasstore</td>
<td>ds-nfs01</td>
</tr>
<tr>
<td>Disk storage</td>
<td>Thin Provision</td>
</tr>
</tbody>
</table>

1. Review the VM Template settings and press the **Finish** button.
Monitor task progress

1. Once the task has been completed, you will see the new `tinyLinux2 Template` object in the inventory pane.
Launch the Deploy From Template wizard

1. Select the Template, tinyLinux2 Template
2. Right click on tinyLinux2 Template and select New VM from This Template.
Select a name and folder

1. Enter **app-serv01** for the name of the new virtual machine
2. Leave the default location of **Site A Datacenter**
3. Click the **Next** button
Select compute resource

tinyLinux2 Template - Deploy From Template

1. Select **Site A Cluster 1**.
2. Click **Next**
Select storage

tinyLinux2 Template - Deploy From Template

1. Leave the default datastore selected, **ds-iscsi01**
2. Click **Next**
When cloning a virtual machine from a template, the guest operating system and virtual hardware can be modified. For this example, we will not customize the operating system or hardware.

1. Click "Next"
1. Review the deployment options and then click **Finish**.
Monitor task progress

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

The vSphere Client provides some powerful search options. This lesson will guide you through the different search options to find the inventory of interest quickly. Also, the vCenter Inventory Service enables users to create custom defined tags that can be categorized and added to any inventory objects in the environment. These tags are searchable metadata and reduce the time to find inventory object information. This lab will cover how to create tags and use the tags for a search.

Search for Virtual Machines

At the top of the vSphere Client is a search bar that can be used to find objects quickly. This can an object's name, like app-serv01 or an ESXi host. Tags can also be attached to objects and the search feature can be used to find them as well.

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

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

2. Press the Enter key.
Search Results

On this page, you can see all the results for objects that contain the word **tiny**. If you have a large inventory, the results can be narrowed down further by selecting the object type you are looking for. Tags or Custom Attributes could be used to narrow the search results down. Selecting the object type can help you quickly find the object you are looking for.

1. Click on **Virtual Machines**.
Filter Results

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

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

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

The search field is updated with the results.
Save the Search

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

1. Click the **Save Search** button.

Name Search

1. Name the search **not-powered-on**
2. Click the **Save** button.

Note that the name must be in lowercase with no spaces between words.
View Saved Search

1. To view a saved search, click in the Search field.
2. Click on the drop-down arrow to see the previously saved search results.
3. Click on #tiny-vms

Tiny-VMs
This was a previously created saved search and shows the results for objects that contain tiny.

1. Note that in the Actions menu, this search can be saved as another name and modified. It can also be renamed or deleted.

**Tags and Custom Attributes**

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

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

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

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

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

Add Category

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

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

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

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web tier</td>
<td>All objects in the web tier.</td>
</tr>
</tbody>
</table>

---

HOL-2010-01-SDC

Page 92
1. Click **New**
2. Name the tag **Web Server version 2**
3. Click the tag category **web tier** in the drop-down box.
4. Select **OK**
New Tag

1. The newly created tag has now been added.

In order for these tags to be useful, they need to be assigned to objects. In the next steps, the tag will be assigned to virtual machines.

2. Click on **VMs and Templates**.
Select a Virtual Machine

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

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

Search Using Tags

1. In the Search field enter "**we**".
2. Select the Tag **Web Server version 2**.
1. Click on the **Objects** tab to find the list of objects which have been assigned the **Web Server version 2** tag.
Understanding vSphere Availability and Distributed Resource Scheduler (DRS)

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

What is vSphere Availability?

vSphere Availability provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

When you create a vSphere Availability cluster, a single host is automatically elected as the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of the slave hosts. Different types of host failures are possible, and the master host must detect and appropriately deal with the failure. The master host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The master host uses network and datastore heartbeating to determine the type of failure. Also note that vSphere Availability is a host function which means there is not a dependency on vCenter in order to effectively fail over VMs to other hosts in the cluster.
vSphere Availability Primary Components

- Every host runs an agent.
  - Referred to as 'FDM' or Fault Domain Manager
  - One of the agents within the cluster is chosen to assume the role of the Master
    - There is only one Master per cluster during normal operations
    - All other agents assume the role of Slaves
- There is no more Primary/Secondary concept with vSphere HA
The Master Role

- An FDM master monitors:
  - ESX hosts and Virtual Machine availability.
  - All Slave hosts. Upon a Slave host failure, protected VMs on that host will be restarted.
  - The power state of all the protected VMs. Upon failure of a protected VM, the Master will restart it.

- An FDM master manages:
  - The list of hosts that are members of the cluster, updating this list as hosts are added or removed from the cluster.
  - The list of protected VMs. The Master updates this list after each user-initiated power on or power off.
The Slave Role

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

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

Enable and Configure vSphere Availability

1. First, click on **Menu**
2. Select **Hosts and Clusters**
Settings for vSphere Availability

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

1. Click **vSphere Availability** under **Services** to bring up the settings for high availability. Note that you may need to scroll to the top of the list.
2. Click the **Edit** button next to vSphere HA is Turned OFF.
Enable vSphere HA

1. Click the toggle next to vSphere HA to enable it.
2. From the VM Monitoring drop-down list, select VM and Application Monitoring.

By selecting VM and Application Monitoring, a VM will be restarted if heartbeats are not received within a set time, the default is 30 seconds.

3. Click the Admission Control tab.
Admission Control

Edit Cluster Settings | Site A Cluster 1

vSphere HA

Failures and responses  Admission Control  Heartbeat Datastores  Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Define host failover capacity by

- Disabled
- Slot Policy (powered-on VMs)
- Cluster resource Percentage
- Dedicated failover hosts
1. In the **Define host failover capacity by** drop-down menu, select **Cluster resource percentage**.

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

2. Click **Heartbeat Datastores**.
Heartbeat Datastores

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 2 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:
- Automatically select datastores accessible from the hosts
- Use datastores only from the specified list
- Use datastores from the specified list and complement automatically if needed
1. Select **Automatically select datastores accessible from the hosts.**

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

2. Click ‘**OK**’ to enable vSphere HA.

![Image of browser interface with zoom options]

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

**Monitor the task**

![Image of recent tasks with vSphere HA configurations]
It will take a minute or two to configure vSphere HA. You can monitor the progress in the Recent Tasks window.

Once the three tasks have been completed, you can move on to the next step.
Use the Summary Tab to Verify that HA Is Enabled

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

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

Notice the bars that display resource usage in blue, protected capacity in light gray, and reserve capacity using stripes.
Enable Distributed Resource Scheduler (DRS)

1. Click on the **Configure** tab to start the process of enabling Distributed Resource Scheduler.
2. Click **vSphere DRS**.
3. Click on the **Edit** button to modify the DRS settings.
Enable Distributed Resource Scheduler (DRS)

1. Verify that vSphere DRS is enabled. -- note that this is already enabled in the lab
2. Click the drop-down box and select **Fully Automated**
3. Click **OK**

**Automation Levels**

<table>
<thead>
<tr>
<th>Automation Level</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Initial placement: Recommended host(s) is displayed.</td>
</tr>
<tr>
<td></td>
<td>Migration: Recommendation is displayed.</td>
</tr>
<tr>
<td>Partially Automated</td>
<td>Initial placement: Automatic</td>
</tr>
<tr>
<td></td>
<td>Migration: Recommendation is displayed.</td>
</tr>
<tr>
<td>Fully Automated</td>
<td>Initial placement: Automatic</td>
</tr>
<tr>
<td></td>
<td>Migration: Recommendation is executed automatically</td>
</tr>
</tbody>
</table>

---

---

---

---
The chart shown above is showing how DRS affects placement and migration according to the setting Manual, Partially Automated or Fully Automated.

**Use the Cluster's Summary Tab to Check Cluster Balance**

1. Click the **Summary** tab to display the current status of the cluster.
2. The Summary tab of the Cluster Site A shows the current balance of the cluster. Also shown in the DRS section is how many recommendations or faults that have occurred with the cluster. (You may have to scroll down to see the vSphere DRS widget).
vSphere 6 Fault Tolerance Provides Continuous Availability

vSphere 6 HA provides a base level of protection for your virtual machines by restarting virtual machines in the event of a host failure. vSphere 6 Fault Tolerance provides a higher level of availability, allowing users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.

Fault Tolerance provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in the instruction execution of the virtual machine. This is done using the VMware vLockstep technology on the ESXi host platform. vLockstep accomplishes this by having the Primary and Secondary VMs execute identical sequences of x86 instructions. The Primary VM captures all inputs and events (from the processor to virtual I/O devices) and replays them on the Secondary VM. The Secondary VM executes the same series of instructions as the Primary VM, while only a single virtual machine image (the Primary VM) executes the workload.

If the host running the Primary VM fails, an immediate and transparent failover occurs. The functioning ESXi host seamlessly becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. After a transparent failover occurs, a new Secondary VM is respawned and redundancy is re-established. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.
VMware vSphere Fault Tolerance

**vSphere 6.0 VMware Fault Tolerance**

**Additional new features**
- Enhanced virtual disk format support
- Ability to hot configure FT
- Greatly increased FT host compatibility

**Benefits**
- Protect mission critical, high performance applications regardless of OS; No application-specific management and learning
- Continuous availability – zero downtime and zero data loss for infrastructure failures; no loss of TCP connections
- Fully automated response

The benefits of Fault Tolerance are:

- Protect mission critical, high performance applications regardless of OS
- Continuous availability - Zero downtime, zero data loss for infrastructure failures
- Fully automated response

Use cases

Any workload that has up to 4 vCPUs and 64GB Memory that is not latency sensitive (e.g. VOIP & High-Frequency trading are not good candidates for FT). Note that vSphere 6.0 introduces the capability to use FT to protect VMs with more than 1 vCPU. In vSphere 5.5 and prior versions, only VMs with 1 vCPU could be protected by FT. For vSphere v6.5 the Standard and Enterprise editions allow for up to 2 vCPUs, where the Enterprise Plus edition allow for up to 4 vCPUs.

There is VM/Application overhead to using FT and that will depend on a number of factors like the application, number of vCPUs, number of FT protected VMs on a host, Host processor type, etc. See the [Performance Best Practices for VMware vSphere](#) for more information.

The new version of Fault Tolerance greatly expands the use cases for FT to approximately 90% of workloads.
The new technology used by FT is called Fast Checkpointing and is basically a heavily modified version of an vMotion that never ends and executes many more checkpoints (multiple/sec). Also note that in versions prior to 6.0, FT required shared storage where both the Primary and Secondary copies of the FT-protected VM would share the same VMDK files. However, in vSphere 6.0 in order to add additional protection to the FT-protected VM, the Primary & Secondary VM use unique VMDK's.

FT logging (traffic between hosts where primary and secondary are running) is very bandwidth intensive and is recommended that a dedicated 10G NIC is used on each host. This isn’t required, but highly recommended as at a minimum an FT protected VM will consume more bandwidth. Slower NICs on the ESXi hosts will impact performance on the secondary VM.

**Video: Protecting Virtual Machines with FT (2:51)**

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

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

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

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

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

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

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

Alarms have the following severity levels:

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

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

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

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

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

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

Alarms can be defined at different levels. In the case of the highlighted alarm, you can see it is defined at the top level. Alarms that are defined at the top level are then inherited by the objects below.
Alarms can be defined at different levels. In the case of the highlighted alarm, you can see it is defined at the top level (vCenter Server). Alarms that are defined at the top level are then inherited by the objects below.
1. Click on the **Alarm Name** field and type **cpu** in the search field.
2. Select the **Host CPU usage** alarm
3. Click the **Edit** button
Name and Targets

The Name and Targets screen defines the name of the alarm (Host CPU usage), what object it applies to (Hosts) and where the objects are located.

1. Click Next.
1. Change the percentage of 75% to 80%.
2. Use the scroll bar to scroll to the bottom.

Notice this will trigger a Warning alarm.
Add Advanced Action

1. Click on **Add Advanced Action**.
2. From the drop-down menu (Select an advanced action), select **Enter maintenance mode**.
3. Click **Next**

When a Host's CPU runs at or above 80% for more than 5 minutes, a Warning alarm will be triggered, and the Host will be put in Maintenance mode. Maintenance mode is covered in Module 3, but when a host is in this state, it is taken offline and any virtual machines that are running on it will be moved to other hosts in the cluster. This lets maintenance be performed on hosts without suffering downtime.
On this screen we can set additional actions based on when a Host's CPU is about 90% for 5 minutes. In this case, it would trigger a Critical alarm. Additional actions could be taken when a Host is in this state.

1. Click **Next**.
Reset Rule 1

If the conditions that originally triggered the alarm are no longer present, additional actions can take place. As an example, once a Host's CPU is no longer at 80% for more than 5 minutes, an email notification could be sent.

1. Click Next.
The Review screen shows what was configured.

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

1. To add a new alarm, click **Add**.
New Alarm Definition

We will be creating an alarm that will migrate a VM if CPU Ready exceeds an average of 8000ms over the course of 5 minutes.

1. Enter **Virtual Machine CPU Ready** for the Alarm name.
2. Change **Monitor** from vCenter Server to **Virtual Machines**
3. Click **Next** to move to the Alarm Rule 1 screen.
Define CPU Ready Time

1. Click in the field under IF and select **VM CPU Ready Time**.
2. Change the **select an operator** filed to **is above**.
3. Type **8000** in the ms field
4. In the last field, use the drop-down menu to select **5 min**.
5. Use the scroll bar to scroll to the Add advanced actions section.
Add Advanced Action

1. Click **Add Advanced Actions**
Migrate VM

1. Select **Show as Warning** in the Trigger the alarm menu
2. From the drop-down menu, select **Shutdown guest on VM**.

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

3. Click **Next**.
Additional options could be specified once the conditions are clear.

1. Click **Next**
Review

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

1. Click Create.
New Alarm Created

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

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

Shares are typically specified as High, Normal, or Low

**Video: Configuring Shares and Reservations (4:00)**

This video shows how to use the VMware vSphere web client to configure shares, reservations, and limits in order to effectively distribute compute and memory resources among virtual machines.
Shares, Limits and Reservations

Resource Management

Shares: relative importance of a virtual machine (VM)

Reservation: guaranteed minimum allocation for a VM

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

1. Right click the **windows10** virtual machine.
2. Select **Edit Settings...**
The above example shows 2 VM's, one a development VM and the other a Production VM. On the left-hand side of the diagram, you can see the CPU shares are equal. We want to make sure the Production VM gets the majority of the CPU resources when there is contention for those resources in the environment. Changing the shares for the production VM from 1000 shares to 2000 shares accomplishes this goal. The new settings are shown on the right side of the diagram.
Changing Resource Allocation of CPU shares.

1. Expand the **CPU** section of the settings.
2. From the Shares drop down box, Click **High** to change the setting of the CPU shares.
3. Click **OK**

Note the current setting for **Shares** is set to 1000.
Review Settings

1. The new Shares setting of 2000 is now shown in the VM Hardware section.
2. You may have to expand the VM Hardware section to see it.
Limits and Reservations are set with the same procedure. When you click on the "edit" settings for a VM, you will find the ability to set the Limit and Reservations. Limit restricts a VM from using more than the limit setting. Reservations guarantee a minimum amount of a resource be available for the virtual machine. Try out some settings for Limits and Reservations. One note is that if you try to reserve more of a resource such as memory or CPU than is available, the VM may not power on.
Migrating Virtual Machines with VMware vMotion

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

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

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

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

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

**Edit Cluster Settings**

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

1. Select **Site A Cluster 1**
2. Click the **Configure** tab
3. Click the **Edit** button

## Disable DRS

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

By disabling DRS, this will prevent the virtual machines from being migrated back to esx-02a.corp.local.
esx-02a.corp.local

1. Select esx-02a.corp.local
2. Click the VMs tab

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

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

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

1. Select all the virtual machines (click the first one on the list, hold the shift key, click the last one on the list).
2. Right click and select **Migrate...**

**Migrate**

Click **Yes** to start the migration process.
Migration Type

1. Leave the default setting and click **Next**

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

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

Since we want to move all the virtual machines to esx-01a.corp.local, we are selecting a specific host. We could also place it in a Cluster and let DRS decide the best host to move it to.
Networks

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

1. Click **Next**.
A priority can be set for the vMotion task. In most cases, the default option is OK.

1. Leave the default setting and click **Next**.
Ready to Complete

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

<table>
<thead>
<tr>
<th>Migration Type</th>
<th>Change compute resource. Leave VM on the original storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>Migrating 3 VMs</td>
</tr>
<tr>
<td>Cluster</td>
<td>Site A Cluster 1</td>
</tr>
<tr>
<td>Host</td>
<td>esx-01a.corp.local</td>
</tr>
<tr>
<td>vMotion Priority</td>
<td>High</td>
</tr>
<tr>
<td>Networks</td>
<td>No network reassignments</td>
</tr>
</tbody>
</table>

Review the settings and click **Finish** to migrate the virtual machines to **esx-01a.corp.local**.
Monitor Progress

You can monitor progress using Recent Tasks.

Migration Complete

When the task has been completed successfully, you should see all of the virtual machines moved over to esx-01a.corp.local.
vSphere Monitoring and Performance

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

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

Select esx-01a

1. Select esx-01a.corp.local
2. Click the Monitor tab
3. Click Overview under the Performance section.
1. Ensure **Real-time** has been selected from the Time Range drop-down menu.

Here we can see in real time the CPU usage in percent for esx-01a.corp.local. By default, the chart will refresh every 20 seconds. The amount of data you see will depend on how long you have been taking the lab.
Virtual Machine CPU Usage

1. Now click the View drop-down box and select Virtual Machines.
Combined CPU Usage

This chart shows the real-time CPU usage of each virtual machine. Each VM is represented by a different color in the graph and you can see at the bottom, which VM is represented by what color. Combined, they give you an idea of overall CPU usage on the host.
Other Available Graphs

There are other graphs available to show host and virtual machine memory usage, network (Mbps) and disk (KBps).

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

The graphs we have looked at so far will give you an overview of the four main components, CPU, memory, disk and storage. The advanced graphs will give you more detailed information on each of these.

Before we look at these charts, let's generate some CPU activity on esx-01a.corp.local by restarting all of the virtual machines it hosts.
Select the VMs to be Restarted

To generate some activity on esx-01a.corp.local, the virtual machines will be rebooted.

1. Select **esx-01a.corp.local**
2. Click on the **VMs** tab
3. Click on the **first VM** that is listed, hold down the **Shift key** and select the **last VM** on the list
4. Click the **Restart** button

**Confirm Restart**

1. Click **Yes** to continue.

Note: You may also receive a warning that only X of X virtual machines will be restarted. This depend on what other modules and/or lessons have been completed in the lab previously.
Manually Start VMs

If tinyLinux, tinyLinux2, or app-serv01 did not restart, but instead shut down, select all and power them on manually.
Monitor Performance

1. Click on the Monitor tab
2. Click Advanced in the Performance section.

Chart Options

1. Click the Chart Options link

This will bring up options to customize the chart.
Stacked Graph per VM

From the Chart Type drop-down menu, select **Stacked Graph per VM**.
Select Objects

1. Under the Select objects for this chart box, verify all the virtual machines are selected.
2. Click the OK button to see the newly customized chart.

CPU Usage in Real-time

Here we can see the CPU usage of each virtual machine and esx-01a.corp.local.
Performance Chart Legend

Scroll down and you will see the Performance Chart Legend. You can click on any of the virtual machines or esx-01a.corp.local to highlight it on the chart.
Exporting a Chart Image

1. You can export the chart in multiple formats, either as a graphic or CSV file by clicking the **Export** button
2. Click the **Chart Options** link

**Chart Metrics**

On the left-hand side, you will see a list of all the available chart metrics that can be viewed. The counters will update based on what metric you select.
1. Select **Memory** under Chart metrics
2. Select **Active, Ballooned memory** and **Compressed** for Counters to add.

Notice the counters section updates and now we have additional counters to view for this chart.

3. Click **OK**

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

This chart shows the memory counters relative to memory for esx-01a.corp.local. Scroll down the Performance Chart Legend to see the counter each line represents.

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

Enable DRS

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

1. Select **Site A Cluster 1**
2. Click the **Configure** tab
3. Click on **vSphere DRS**
4. Click the **Edit** button
Turn ON vSphere DRS

Check the Turn ON vSphere DRS box to enable DRS and click OK.

Further Information

For more information on performance charts, you can view the vSphere Monitoring and Performance guide.
Module 2 - Introduction to vSphere Networking and Security (60 Min)...
Introduction

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

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

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

Types of virtual switches

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

vNetwork Standard Switch (vSwitch, vSS)

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

vSwitches are configured on each ESXi/ESX host.

vNetwork Distributed Switch (dvSwitch, vDS)

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

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

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

These features are available with both types of virtual switches:

- Can forward L2 frames
- Can segment traffic into VLANs
- Can use and understand 802.1q VLAN encapsulation
- Can have more than one uplink (NIC Teaming)
- Can have traffic shaping for the outbound (TX) traffic

These features are available only with a Distributed Switch:

- Can shape inbound (RX) traffic
- Has a central unified management interface through vCenter Server
- Supports Private VLANs (PVLANs)
- Provides potential customization of Data and Control Planes

vSphere 5.x provides these improvements to Distributed Switch functionality:

- Increased visibility of inter-virtual machine traffic through Netflow.
- Improved monitoring through port mirroring (dvMirror).
- Support for LLDP (Link Layer Discovery Protocol), a vendor-neutral protocol.
- The enhanced link aggregation feature provides choice in hashing algorithms and also increases the limit on number of link aggregation groups.
- Additional port security is enabled through traffic filtering support.
- Improved single-root I/O virtualization (SR-IOV) support and 40GB NIC support.

vSphere 6.x provides these improvements to Distributed Switch functionality:

- Network I/O Control New support for per virtual machine Distributed vSwitch bandwidth reservations to guarantee isolation and enforce limits on bandwidth.
- Multicast Snooping - Supports IGMP snooping for IPv4 packet and MLD snooping for IPv6 packets in VDS. Improves performance and scale with multicast traffic.
- Multiple TCP/IP Stack for vMotion - Allows vMotion traffic a dedicated networking stack. Simplifies IP address management with a dedicated default gateway for vMotion traffic.

vSS vs vDS architecture

Spend a few minutes reviewing the differences between the Standard vSwitch and Distributed vSwitch architectures.

Pay special attention to how the port groups and uplinks are designed.
vSphere Standard Switch Architecture
Let's get started!

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

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

Adding a Virtual Machine Port Group with the vSphere Client

If you are not already logged in, launch the Chrome browser from the desktop and log in to the vSphere Web Client.

1. Click the "Use Windows session authentication" check box
2. Click "Login"
Select Hosts and Clusters

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

1. Under vcsa-01a.corp.local, expand Site A Datacenter and then Site A Cluster.
2. Next, right-click on esx-02a.corp.local in the Navigator.
3. Select Add Networking....
Connection Type

When asked to select connection type, choose **Virtual Machine Port Group for a Standard Switch**
2. Click **Next**
1. When asked to select a target device, choose **New Standard Switch**. Note that a larger MTU size can be specified if needed.
2. Click **Next**.
Create a Standard Switch

esx-02a.corp.local - Add Networking

1. Click the '+' button.

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

Add Physical Adapters to the Switch

1. Select **vmnic3** under Network Adapters
2. Click 'OK'
Add Physical Adapter

esx-02a.corp.local - Add Networking

1. Click **Next** to continue.
Connection Settings

At the Connection settings step of the wizard, for Network label, leave the default name of **VM Network 2**.

Do not change the VLAN ID; leave this set to **None (0)**.
1. Review the port group settings in Ready to complete and click **Finish**.
Virtual Switches

Next, we will verify the switch has been created.

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

**Standard Switch: vSwitch1**
1. Scroll down until you see **Standard Switch: vSwitch1**.
2. If needed, expand the section.

You should see the above diagram showing a virtual port group (VM Network 2) that is on vSwitch1 and it is using vmnic3 as an uplink.

**Editing a Standard Switch in the vSphere Web Client**

In this lesson, we will review the various properties of a Standard Switch.

vSphere Standard Switch settings control switch-wide defaults and switch properties such as the uplink configuration.

**Select esxi-01a.corp.local**

1. Select **esxi-01a.corp.local**.
2. Ensure the **Configure** tab is selected.
3. Click **Virtual switches**.
Select vSwitch0

1. You will need to scroll down until you reach the **Standard Switch: vSwitch0** section.
2. Expand the section to view the layout of the switch.
Edit vSwitch1

1. Click **Edit**.

Properties (MTU Setting)

vSwitch0 - Edit Settings

<table>
<thead>
<tr>
<th>Properties</th>
<th>Number of ports</th>
<th>Elastic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>MTU (Bytes)</td>
<td>1500</td>
</tr>
<tr>
<td>Teaming and failover</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Click **CANCEL** or **OK**.
If you are using jumbo frames in your environment and want to leverage this on a vSphere Standard Switch, you can change the MTU setting here.

You can change the size of the maximum transmission unit (MTU) on a vSphere Standard Switch to increase the amount of payload data transmitted with a single packet, that is, enabling jumbo frames. **Be sure to check with your Networking team prior to making any modifications here.** To realize the benefit of this setting and prevent performance issues, compatible MTU settings are required across all virtual and physical switches and end devices such as hosts and storage arrays.

You will also notice the Security, Traffic shaping, and Team and Failover options. This is where the default settings for the virtual switch would be set. As you will see later, these defaults may be overridden at the port group level as required.

1. Click the **Cancel** button.

Next, an additional uplink will be added to the switch and the other options will be reviewed.

**Add Uplink Adapters in the vSphere Web Client**

You can associate multiple adapters to a single vSphere standard switch to increase throughput and provide redundancy should a link fail. This is known as "NIC Teaming."
Select Virtual switches

1. Click **Add Networking**
Select Connection Type

Select connection type
Select a connection type to create.

- VMkernel Network Adapter
  The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

- Virtual Machine Port Group for a Standard Switch
  A port group handles the virtual machine traffic on standard switch.

- Physical Network Adapter
  A physical network adapter handles the network traffic to other hosts on the network.

1. Select **Physical Network Adapter**.
2. Click **Next**.
Select Target Device

Select target device
Select a target device for the new connection.

- Select an existing switch
  - vSwitch0

- New standard switch
  - MTU (Bytes) 1500

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

1. Click **Next**.
Add Networking

Add physical network adapter
Assign physical network adapters to the switch.

Assigned adapters

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

1. Click the green '+' to add the adapter.
1. Click on **vmnic3**
2. Click **OK**
Assigned Adapters

The new adapter has been added in the Active Adapters section. An adapter could also be moved to the Standby Adapters section to be used for failover. The Unused Adapters section can be used when there are multiple portgroups on a switch and you would like the ability to control what traffic flows through which physical adapter. It can be used to segment traffic or be used for individual VLAN traffic.

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

**Editing a Standard Switch Port Group**

Once the vSwitch has been configured and its defaults have been set, the port group can be configured. The port group is the construct that is connected to virtual machine NICs and usually represents a VLAN or physical network partition such as Production, Development, Desktop or DMZ.
1. In the Physical Adapters section, vmnic3 has been added to the switch.

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

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

**Port Group Properties**

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

**There is no need to modify these settings for this part of the lab.**
1. Click **Security**.

**Port Group Security**

<table>
<thead>
<tr>
<th>Properties</th>
<th>Promiscuous mode</th>
<th>MAC address changes</th>
<th>Forged transmits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Traffic shaping</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Teaming and failover</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By ticking the Override box, you can override the default setting of the Standard Switch for just this port group.

In this section, you can configure the following:

**Promiscuous Mode**

- **Reject** — Placing a guest adapter in promiscuous mode has no effect on which frames are received by the adapter.
- **Accept** — Placing a guest adapter in promiscuous mode causes it to detect all frames passed on the vSphere standard switch that are allowed under the VLAN policy for the port group that the adapter is connected to.

**MAC Address Changes**

- **Reject** — If you set the MAC Address Changes to Reject and the guest operating system changes the MAC address of the adapter to anything other than what is in the .vmx configuration file, all inbound frames are dropped. If the Guest OS changes the MAC address back to match the MAC address in the .vmx configuration file, inbound frames are passed again.
- **Accept** — Changing the MAC address from the Guest OS has the intended effect: frames sent to the altered MAC address are received by the virtual machine.

**Forged Transmits**

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

**No changes are needed here.**

1. Click **Traffic shaping**.
Traffic Shaping

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

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

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

**Average Bandwidth**

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

**Peak Bandwidth**

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

**Burst Size**

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

No changes are needed here.
1. Clicking **Teaming and failover**.

## Teaming and Failover

### VM Network - Edit Settings

<table>
<thead>
<tr>
<th>Properties</th>
<th>Load balancing</th>
<th>Override</th>
<th>Route based on originating virtual port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Network failure detection</td>
<td>Override</td>
<td>Link status only</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>Notify switches</td>
<td>Override</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Fallback</td>
<td>Override</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Failover order**

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

Select active and standby adapters. During a failover, standby adapters activate in the order specified above.

Again, we have the option to override the default virtual switch settings.

**Load Balancing Policy** - The Load Balancing policy determines how network traffic is distributed between the network adapters in a NIC team. vSphere virtual switches load balance only the outgoing traffic. Incoming traffic is controlled by the load balancing policy on the physical switch.

- **Route based on the originating virtual port** - Select an uplink based on the virtual port IDs on the switch. After the virtual switch selects an uplink for a virtual machine or a VMkernel adapter, it always forwards traffic through the same uplink for this virtual machine or VMkernel adapter.
- **Route based on IP hash** - Select an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, the switch uses the data at those fields to compute the hash. IP-based teaming requires that the physical switch is configured with EtherChannel.
- **Route based on source MAC hash** - Select an uplink based on a hash of the source Ethernet.
- **Route based on physical NIC load** - Available for distributed port groups or distributed ports. Select an uplink based on the current load of the physical network adapters connected to the port group or port. If an uplink remains busy
at 75 percent or higher for 30 seconds, the host proxy switch moves a part of the virtual machine traffic to a physical adapter that has free capacity.

- **Use explicit failover order** - From the list of active adapters, always use the highest order uplink that passes failover detection criteria. No actual load balancing is performed with this option.

**Network Failure Detection** - The method the virtual switch will use for failover detection.

- **Link Status only** - Relies only on the link status that the network adapter provides. This option detects failures such as removed cables and physical switch power failures.
- **Beacon Probing** - Sends out and listens for beacon probes on all NICs in the team, and uses this information, in addition to link status, to determine link failure. ESXi sends beacon packets every second. The NICs must be in an active/active or active/standby configuration because the NICs in an unused state do not participate in beacon probing.

**Notify Switches** - specifies whether the virtual switch notifies the physical switch in case of a failover.

**Failover** - specifies whether a physical adapter is returned to active status after recovering from a failure.

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

You can also override the default virtual switch setting for the Failover order of the physical adapters.

**No changes are needed here and you may proceed to the next step.**
Cancel the Changes

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

Removing a Physical Adapter

1. Click Manager Physical Adapters for vSwitch0.
Remove vmnic3

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

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

**Clear Alerts**

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

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

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

1. Click on **esx-02a.corp.local**.
Deleting a Standard Switch

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

Virtual Switches

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

1. Click the `Configure` tab.
2. Select `Virtual switches` in the Networking section.
Standard Switch: vSwitch1

1. Scroll down until you see the Standard Switch: vSwitch1 section
2. Expand the section, if needed.
3. Click the '...' menu and select Remove

Remove Standard Switch

1. Click Yes to remove vSwitch1.

Conclusion

The vSphere Standard Switch is a simple virtual switch configured and managed at the host level. This switch provides access, traffic aggregation and fault tolerance by allowing multiple physical adapters to be bound to each virtual switch.

The VMware vSphere Distributed Switch builds on the capabilities of the vSS and simplifies management in large deployments by appearing as a single switch spanning
multiple associated hosts. This allows changes to be made once and propagated to every host that is a member of the switch.
Working with the vSphere Distributed Switch

Before we walk through the process of building our own Distributed vSwitch, let's take a minute to explore an existing vDS.

In this lab we will see how a Distributed vSwitch compares to a Standard vSwitch, how it is configured, and how it is connected to a running virtual machine.

Navigate to networking

1. Click on the **Networking** icon.
View Standard vSwitch

1. Expand **Site A Datacenter**.
2. Select **VM Network**.

**VM Network**

1. Click on **VMs** tab.

Take note of the virtual machines that are connected to this vSwitch. You should see a VM called **tinyLinux2**.
Note: You may see different results based on what lessons or modules you have already completed.

**Hosts**

1. Click on **Hosts** tab.

Take note of the hosts connected to the **VM Network** vSwitch. You should see `esx-01a.corp.local` and `esx-02a.corp.local`.
View Distributed Switch

1. Click on RegionA01-vDS-COMP.
2. Select the Configure tab.
Review vDS configuration

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

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>RegionA01-VDS-COMP</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>Version</td>
<td>6.6.0</td>
</tr>
<tr>
<td>Number of uplinks</td>
<td>4</td>
</tr>
<tr>
<td>Number of ports</td>
<td>520</td>
</tr>
<tr>
<td>Network I/O Control</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1500 Bytes</td>
</tr>
<tr>
<td>Multicast filtering mode</td>
<td>Basic</td>
</tr>
<tr>
<td><strong>Discovery protocol</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Cisco Discovery Protocol</td>
</tr>
<tr>
<td>Operation</td>
<td>Listen</td>
</tr>
<tr>
<td><strong>Administrator contact</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
</tr>
<tr>
<td>Other details</td>
<td></td>
</tr>
</tbody>
</table>

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

1. Click **Edit**
General Settings

RegionA01-vDS-COMP - Edit Settings

General

Name: RegionA01-vDS-COMP
Number of uplinks: 4
Network I/O Control: Disabled
Description:

Click General to view the vSphere distributed switch settings. Here you can modify the following:

**Name:** You can modify the name of your distributed switch.

**Number of Uplinks:** Increase or decrease the number uplink ports attached to the distributed switch. Note that you can also click the Edit uplink names button to give the uplinks meaningful names.

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

**Network I/O Control:** You can use the drop-down menu to enable or disable Network I/O Control on the switch.

**Description:** You can use this field to give a meaningful description of the switch.
### Advanced Settings

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

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

#### Multicast filtering mode

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

#### Discovery Protocol

- **Type** - Cisco Discovery Protocol, Link Layer Discovery Protocol, or disabled.
- **Operation** - to Listen, Advertise, or Both.
**Administrator Contact:** Type the name and other details of the administrator for the distributed switch.

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

---

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

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

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

1. Click on the **Health check** tab for Distributed Switch.

We can see that Health check is disabled for VLAN and MTU as well as Teaming and failover.

2. Click the **Edit** button.
Edit Health Check Settings

Select Enabled for both and click OK.

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

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

**Select name and location section**

**New Distributed Port Group**

1. Name the new port group **WebVMTraffic**.
2. Click **Next**.
Configure settings

New Distributed Port Group

Configure settings
Set general properties of the new port group.

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

VLAN
VLAN type: None

Advanced
Customize default policies configuration

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

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

- **Static binding** - Assign a port to a virtual machine when the virtual machine connects to the distributed port group.
- **Ephemeral** - No port binding. You can assign a virtual machine to a distributed port group with ephemeral port binding also when connected to the host.

**Port allocation**

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

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

**Network resource pool:** If you have created network pool to help control network traffic, you can select it here.
**VLAN**: Use the Type drop-down menu to select VLAN options:

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

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

1. **Just accept the defaults and click Next to continue.**

**Ready to complete**

**New Distributed Port Group**

1. Review your settings and click **Finish** to create the Distributed Port Group.
View the new Distributed Port Group

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

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

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

1. Click on tinyLinux

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

Creating a new Distributed Switch

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

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

1. In the vSphere Web Client, click on Site A Datacenter.

Create a new Distributed Switch
1. In the navigator, right-click the Site A Datacenter.
2. Select Distributed Switch > New Distributed Switch.

This will open the New Distributed Switch wizard.

**Name the Distributed Switch**

1. Type **New-vDS** in the Name field.
2. Click **Next**.
1. Leave the default setting of **6.6.0 - ESXi 6.7 and later**
2. Click **Next**.
1. On the Configure Settings page, leave the default options and click **Next**.
Complete the build

1. Review your settings on the Ready to Complete page and click Finish if everything looks good.
Add hosts to new Distributed Switch

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

New vDS - Add and Manage Hosts

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

Select hosts
1. On the Select hosts page, click **New hosts.**

**Select New Hosts**

1. Click the check box on the left to select both hosts in the datacenter,
2. Click **OK.**
1. Verify the two hosts are listed, then click **Next**.
Assign physical adapters

New vDS - Add and Manage Hosts

On the Manage physical network adapters page, we want to configure which physical NICs will be used on the distributed switch.

1. From the **On other switches/unclaimed** list, highlight **vmnic3**
2. Click **Assign uplink**.

---

HOL-2010-01-SDC
Assign uplinks to hosts

1. From the Select an Uplink page, select **Uplink 1**.
2. Check the box next to **Apply this uplink assignment to the rest of the hosts**.
3. Click **OK**.

This will automatically configure any other hosts that you are adding to this distributed switch with the same vmnic and uplink settings.
1. Review vmnic and uplink settings for the hosts you are adding and click **Next** if everything is correct.
1. Since we will not be using this distributed switch for any VMkernel functions, just click **Next** here.
The add hosts wizard also gives us the ability to migrate VMs from one distributed switch to another on this page. While this action can be done here, we will be doing this in the next lesson.

1. Click **Next**.

Also note that this wizard is not the typical place where you would migrate VMs from one virtual switch to another. The process we will be using later is the recommended method.
Complete the host add wizard

1. On the Ready to Complete page, click Finish.

Explore your new vDS

<table>
<thead>
<tr>
<th>New vDS</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Monitor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>State</th>
<th>Status</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>esx-01a.corp.local</td>
<td>Connected</td>
<td>Normal</td>
<td>Site A Cluster1</td>
</tr>
<tr>
<td>esx-02a.corp.local</td>
<td>Connected</td>
<td>Normal</td>
<td>Site A Cluster1</td>
</tr>
</tbody>
</table>
With your new Distributed Switch highlighted, feel free to explore the associated tabs to get a feel for the setup and configuration.

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

**Topology**

1. Click **Configure**
2. Click **Topology**
3. Note that your distributed port group DPortGroup does not have any VMs connected to it.

The next lesson will walk through the process of migrating VMs to the new vDS.

**Migrating VMs from vDS to vDS**

Now that we have created a new vDS, we want to take advantage of its capabilities. In this lab we will migrate a running virtual machine from a virtual standard switch to the newly created distributed virtual switch.

In the vSphere Client, there are numerous ways to accomplish the task of VM network migration. However, we will be walking through the procedures specifically outlined in the vSphere product documentation.
Navigate to your datacenter

To get started, click on **Site A Datacenter**.
Migrate VMs

1. Right click on Site A Datacenter
2. Select Migrate VMs to Another Network
1. In the Select source and destination networks section, click on **Browse** under **Source network**.
1. Select **VM Network**.
2. Click **OK**.

This is the network associated with the virtual standard switch where our VM is currently connected that we want to migrate.
1. Under Destination network select **Browse**.
1. Select **DPortGroup**.
2. Click **OK**.

This is the port group on the new Distributed Switch that you created. This is the new port group that will be used to connect the VM being migrated to the network.
Migrate VMs

1. Click **Next**.
1. On the Select VMs to migrate page, click on the expand arrow of the tinyLinux2 VM to show the network adapters associate with this virtual machine.

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

2. Select the check box for **Network adapter 1**.
3. Click **Next**.
1. Click **Finish** to migrate the VM from a Standard Switch to the new Distributed Switch.
Explore your changes

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

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

Select the **tinyLinux2** VM and note the highlighted path through the new vDS and Uplink.
Using Host Lockdown Mode

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

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

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

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

NOTES:

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

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

Enabling or disabling lockdown mode affects which types of users are authorized to access host services, but it does not affect the availability of those services. In other words, if the ESXi Shell, SSH, or Direct Console User Interface (DCUI) services are enabled they will continue to run whether or not the host is in lockdown mode.
First, you will enable Host Lockdown Mode with the Normal setting on esx-01a.corp.local. This will mean the host will be accessible from vCenter and through the DCUI, but not remotely over SSH.

1. From the Navigator, select the Hosts and Clusters tab.
2. Next, select esx-01a.corp.local.
Before we configure Host Lockdown Mode, let's verify the SSH service is running on esx-01a.corp.local.

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

1. We can see that the **SSH service** is enabled and **Running** on esx-01a.corp.local.

Open an SSH session to esx-01a

First, verify you can login to esx-01a using an SSH connection.
1. From the Windows Taskbar, click on the PuTTY icon.

**Connect to esx-01a**

1. Under Saved Sessions, click on `esx-01a.corp.local`
2. Click the Open button.
Logged into esx-01a

You will be automatically logged in to esx-01a.corp.local because we have configured public-key authentication from the Main Console machine to the ESXi host.
Close the PuTTY Session

Close the PuTTY session by typing 'exit' and pressing Enter. Once you hit Enter, the PuTTY window will disappear.
Enabling Lockdown Mode

Go back to the vSphere Client

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

esx-01a.corp.local - Lockdown Mode

Lockdown Mode is currently disabled. If we set it to Normal, we will not be able to access the host over SSH and only through vCenter or the local console (physically in front of the host). Lockdown Mode can also be set to Strict, meaning only vCenter can access the host and SSH and the local console are disabled.

1. Click the Normal radio button.
2. Click on Exception Users
Exception Users

As previously noted, when Lockdown Mode is enabled, remote access to the host is disabled. Some third-party applications rely on this access and it can be granted by adding the accounts they use to the Exception List. This should not be a way for specific users to bypass security and should only be used for applications that require access.

1. Click **OK** to enable Lockdown Mode.
Lockdown Mode Enabled

Wait for the vSphere Client to refresh to see that Lockdown Mode has been enabled.
PuTTY Session to esx-01a

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

1. Click on esx-01a.corp.local under Saved Sessions
2. Click Open.
Denied!

You should receive an error when trying to connect to esx-01a.corp.local. The host has been configured with Host Lockdown Mode and will refuse any remote connections, unless those users were added to the Exception User list.

1. Click **OK**
2. Close PuTTY by clicking the 'X' in the top right-hand corner of the window.

**Disable Lockdown Mode**
Go back to the vSphere Client.

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

**Lockdown Mode**

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

- **Disabled**
  - Lockdown mode is disabled.
- **Normal**
  - The host is accessible only through the local console or vCenter Server.
- **Strict**
  - The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

1. Check the **Disabled** radio button
2. Click **OK** to continue.
Host Lockdown Mode Disabled

Lockdown Mode for the host should now be disabled.

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

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

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

Enable Lockdown Mode

1. Click on the Edit... button.
Lockdown Mode - Strict

1. Click button next to **Strict**.
2. Click **OK**.

Again, note that users can be added to the exception list. This will only apply to SSH and not the DCUI.

Strict Mode - Enabled

1. Notice Lockdown Mode is now Enabled.
1. Click on **Services**.

You can see the Direct Console UI (DCUI) service has been stopped. Note that the SSH service is still running in case users have been added to the Exception List.
1. On the far, right-hand side of the web page, look for the **Consoles** tab and click on it.

This will give us access to the DCUI on esx-02a-corp.local.
Select ESX-02A

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

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

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

Press F2

1. Now press the F2 key to log in to the DCUI.

You should receive an error that access to the DCUI has been disabled.

2. Press the Enter key to dismiss the message.
Main Console

1. Go back to the Console and click **MAIN CONSOLE** to return to the Windows desktop.
2. After the Main Console loads, click the X to close the Console panel.

Disable Lockdown Mode
Go back to the vSphere Client.

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

**Lockdown Mode**

When enabled, lockdown mode prevents remote users from logging directly to this host. The host is accessible only through the local console or vCenter Server.

Specify host lockdown mode:

1. **Disabled**
   - Lockdown mode is disabled.

2. **Normal**
   - The host is accessible only through the local console or vCenter Server.

3. **Strict**
   - The host is accessible only through vCenter Server. The Direct Console UI service is stopped.

1. Check the **Disabled** radio button
2. Click **OK** to continue.
Host Lockdown Mode Disabled

Lockdown Mode for the host should now be disabled.

Host Lockdown Mode provides an excellent way to further secure your vSphere hosts.
User Access and Authentication Roles

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

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

Create a Role in the vSphere Client

In the following steps, we will create a role in the vSphere Client that we can assign rights for the role.
1. In the vSphere Client, click **Menu**
2. Select **Administration**.
1. Verify the **Roles** tab is selected.

**Roles Overview**
1. The Roles panel shows various roles that already exist or are provided as sample to use or create your own roles from.
2. When a role clicked, the Description of the role, where the role is used and what privileges the role has is will be displayed by clicking the appropriate button.

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

Add A Role

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

Click on the '+ ' to add a new role.
1. Use the scrollbar to scroll down until you see **Network**.
2. Click **Network**.
3. Tick the box for **All Network Privileges**.
4. Click **Next**.
1. Name the role **Network Contractor**.
2. Click the **Finish** button to create the new role.

**Edit a Role in the vSphere Client**

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role. In Linked Mode, the changes you make are propagated to all other vCenter Server systems in the group. However, assignments of roles to specific users and objects are not shared across linked vCenter Server systems.
Sometimes a role may need to be updated for access to additional objects or tasks in vCenter. As an example, say the Network Contractor now needs access to the ESXi Hosts.

1. Click on the role **Network Contractor** to select it
2. Click the **pencil** button to edit the role.
Add Permissions

1. Click on Host.
2. Tick the box next to All Host Privileges.
3. Click Next.
We will keep the same Role name.

1. Click Finish.

**Clone a Role in the vSphere Client**

You can make a copy of an existing role, rename it, and edit it. When you make a copy, the new role is not applied to any users, groups or objects -- it does not inherit anything from the parent except the settings. In Linked Mode, the changes are propagated to all other vCenter Server systems in the group, but assignments of roles to specific users and objects are not shared across linked vCenter Server systems.
Clone a Role

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

1. Click on the Administrator role to select it.
2. Click the Clone button.

Clone Role

As an example, a new vSphere Admin is hired and they only need access to the compute and storage infrastructure, with no access to networking components.
1. For the Role name, type **vSphere Administrator**.
2. In the Description field, type **Full rights to all but Networking**.
3. Click **OK**.

**New Role Cloned**

1. Scroll to the bottom of the list to find the newly created role.
2. Click on **vSphere Administrator**.
3. Click the **pencil** button to edit the role.
1. Scroll down until you see **Network**.
2. Click on **Network**.
3. Untick **All Network Privileges**.
4. Click **Next**.
Edit Role

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

Remove a Role in the vSphere Client

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

**NOTE:**

Before removing a role from a vCenter Server system that is part of a connected group in Linked Mode, check the use of that role on the other vCenter Server systems in the group. Removing a role from one vCenter Server system also removes that role from all other vCenter Server systems in the group, even if you reassign permissions to another role on the current vCenter Server system.
Delete Role

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

Confirm Deletion

1. Click **OK** to confirm you want to delete this role.
We can see that the role named **Network Contractor** has been deleted.

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

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

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

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

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

Single Sign-On Identity Sources

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

In this section, we will look at the configured Identity Sources within Single Sign-on.
Log out as Administrator@CORP.LOCAL

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

Log into vSphere Web Client as SSO Admin

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

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

**Navigate to Administration**

1. Click **Menu**.
2. Select **Administration**.
Minimize Recent Tasks

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

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

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

1. Notice that the corp.local domain is listed as an Active Directory identity source. Users in the domains listed here can be granted permissions within vSphere.

Add a vCenter Single Sign On User with the vSphere Client

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

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

Add User

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>holadmin</td>
</tr>
<tr>
<td>Password</td>
<td>VMware1!</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>VMware1!</td>
</tr>
<tr>
<td>First Name</td>
<td>HOL</td>
</tr>
<tr>
<td>Last Name</td>
<td>Admin</td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:holadmin@regionA.local">holadmin@regionA.local</a></td>
</tr>
</tbody>
</table>

1. Fill out the New User form as follows:

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

2. Click **ADD** to create the user.

**NOTE**: You cannot change the user's name after you create the user. First and Last name are optional parameters.
Here we can see the new user has been added.

1. Clicking on the three dots next to the username, allows for editing, deleting or disabling the user.

**Add a vCenter Single Sign On Group with the vSphere Client**

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

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

1. Click **Groups**.
2. Click **Add Group**.
Create the new group

Add Group

1. For the Group Name, type **HOL Group**.
2. Add the user that was previously created by typing **holadmin**.
3. Click **holadmin** from the drop-down list.
4. Click the **Add** button.
New Group Added

1. Click on the 2 to move to the second page of Groups.
2. Here is the group, HOL Group that was just created.

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

Members of a vCenter Single Sign On group can be users or other groups from one or more identity sources. Members of a group are called principals. Groups listed on the Groups tab in the vSphere Client are internal to Single Sign On and are part of the identity source System-Domain. You can add group members from other domains to a local group. You can also nest groups.
1. Click on 1 to return to the first page of Groups.

Add Members to Users and Groups
1. Click on the **Administrators** group under the Group Names table.

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

### Add Members

![Add Members](image)

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

1. Click **Add Members**.
Edit Group

Group Name

Description

Add Members

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

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

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

**Assign Global Permissions**

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

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

SSO provides the ability to grant Global Permissions to an account by specifying the required access here. In the lab, this list represents the default permissions granted, with the exception of the **CORP.LOCAL\Administrator** user that we have added with Administrator permissions to the entire vSphere infrastructure.

Add New Global Permission

The members of the HOL Group will need to manage all virtual machines in the environment, so we will configure permissions here.
1. Click the (+) to open the Add New Permission window
2. Click the Add... button

**Locate the HOL Group**

1. Ensure that the **regionA.local** domain is selected.
2. Type **HOL Group** in the search field.
3. For the Role, select the **vSphere Administrator** group.
4. Click the **OK** button.
New Global Permission

1. The newly created Global Permission has been created.

Conclusion

Typically, user accounts will not be managed naively within the SSO domain, but will be handled by an external directory source like Microsoft Active Directory or OpenLDAP. Understanding how SSO handles accounts and where to look for account-to-permission binding is useful for managing a vSphere implementation.
Adding an ESXi Host to Active Directory

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

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

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

Hosts and Clusters

1. Click on **Menu**.
2. Select **Hosts and Clusters**.
1. Click on `esx-01a.corp.local`.

**Note:** You may need to expand Site A Datacenter and/or Site A Cluster 1 to see the host.
TCP/IP Configuration

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

**Edit Default System Stack**

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

1. Verify that the host name (esx-01a) and DNS server information (192.168.110.10) for the host are correct.
2. Click OK.
Add a Host to a Directory Service Domain in the vSphere Client

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

1. Click on **Authentication Services** under the System section. You may need to scroll down to see it.
Join Domain

1. Click the **Join Domain** button.

Join Domain Settings

1. Enter **corp.local** for the Domain.

2. Enter the **User name** and **Password**.

3. Click **OK**.
2. In the Using Credentials section enter:

- **Username**: administrator
- **Password**: VMware1!

3. Click **OK**.

**Recent Tasks**

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

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

Log out

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

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

Conclusion

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

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

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

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

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

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

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

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

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

Local Storage

![Diagram showing Local VMFS and VMware ESX connections to virtual machines]
The illustration above depicts virtual machines using Local VMFS storage directly attached to a single ESXi host.

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

**Networked Storage**

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

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

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

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

**Thin Provision**

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

**Thick Provision Lazy Zeroed**

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

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

**Thick Provision Eager Zeroed**

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

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

Launch Google Chrome web browser

1. Select **Google Chrome** from the Main Console desktop
Enter credentials and log in

VMware® vSphere

example@domain.local
Password

1. Select **Use Windows session authentication**

2. Select **Login**

Note: Selecting "Use Windows session authentication" will pass the same credentials as entering them as username "CORP\Administrator" and password "VMware1!"

1. Select **Use Windows session authentication**

2. Select **Login**
Navigate to Storage Management

1. Select the **Storage** tab.

Expand Site A Datacenter

There are 2 storage datastores configured, an iSCSI datastore and an NFS datastore.

1. Select the **ds-iscsi01** datastore

2. Click on **Summary** for summary details of the datastore.

Repeat the steps for the **ds-nfs01** datastore.
Create a vSphere NFS Datastore

In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select **Site A Datacenter**

New Datastore

In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select **Site A Datacenter**
In this section, you will create a new vSphere NFS Datastore using a pre-provisioned NFS mount.

1. Select **Actions**
2. Select **Storage**
3. Select **New Datastore**

**New Datastore - Type**

- **VMFS**: Create a VMFS datastore on a disk/LUN.
- **NFS**: Create an NFS datastore on an NFS share over the network.
- **VVol**: Create a Virtual Volumes datastore on a storage container connected to a storage provider.
1. Select **NFS** for the new Datastore type
2. Click **Next**

Note: You may need to zoom out in order to see the **Next** button.

**New Datastore - NFS Version**

1. Verify NFS Version - **NFS 3**
2. Click **Next**

**New Datastore**

- **NFS 3**
  - NFS 3 allows the datastore to be accessed by ESX/ESXi hosts of version earlier than 6.0

- **NFS 4.1**
  - NFS 4.1 provides multihosting for servers and supports the Kerberos authentication protocol
New Datastore - Name and configuration

1. Give the new Datastore a name, **ds-nfs02**
2. Enter the Folder `/mnt/NFS02` in the NFS Share Details area.
3. Enter the Server **10.10.20.60** in the NFS Share Details area.
4. Click **Next**
New Datastore - Host accessibility

1. Select the **check box** to include all hosts.
2. Click **Next**.
New Datastore - Ready to complete

1. Review New Datastore configuration and click Finish.
Monitor task progress

Recent Tasks

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Target</th>
<th>Status</th>
<th>Initiator</th>
<th>Queued For</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create NAS datastore</td>
<td>esx-02a.corp.local</td>
<td>Completed</td>
<td>CORP\Administrator</td>
<td>6 ms</td>
</tr>
<tr>
<td>Create NAS datastore</td>
<td>esx-02a.corp.local</td>
<td>Completed</td>
<td>CORP\Administrator</td>
<td>9 ms</td>
</tr>
</tbody>
</table>
1. You can follow the progress in the **Recent Tasks** pane (by clicking on **Recent Tasks**)
2. When complete, you should see the new **ds-nfs02** Datastore available for use.

3. Minimize the **Recent Tasks** pane before continuing to the next step.

**Review new Datastore Settings**

1. Select the datastore **ds-nfs02** from the inventory list
2. Select **Summary** to review capacity and configuration details
Create a vSphere iSCSI Datastore

1. Select Site A Datacenter

New Datastore

In this section, you will create a new vSphere iSCSI Datastore with a pre-provisioned iSCSI LUN.

1. Select Actions
2. Select **Storage**
3. Select **New Datastore**

### New Datastore - Type

**New Datastore**

<table>
<thead>
<tr>
<th>1 Type</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Name and device selection</td>
<td><strong>Specify datastore type.</strong></td>
</tr>
<tr>
<td>3 VMFS version</td>
<td></td>
</tr>
<tr>
<td>4 Partition configuration</td>
<td></td>
</tr>
<tr>
<td>5 Ready to complete</td>
<td></td>
</tr>
</tbody>
</table>

1. Verify type - **VMFS**- is selected.
2. Click **Next**
1. Give the new Datastore the name **ds-iscsi02**
2. Select a Host to view the accessible disks/LUNs and select **esx-01a.corp.local** in the drop-down box.

**Note:** Do not click Next just yet, proceed to the next step!
From this view, we can see that there are existing datastores that can be presented to our vSphere environment.

1. Select the device with LUN ID 2. In this case, it should be the only device visible with a FreeNAS prefix.
2. Click Next
New Datastore - VMFS Version

1. Leave the default of **VMFS 6** selected
2. Click **Next**
New Datastore - Partition Configuration

New Datastore

1. Select Next

We can use all available capacity for this datastore or change the size if needed. The defaults are fine for this step.
1. Review New Datastore configuration and click **Finish**.
New Datastore - Monitor task progress

1. Note the progress in the Recent Tasks pane
2. When complete, you should see the ds-iscsi02 Datastore available for use
New Datastore - Review Settings

1. Select the datastore **ds-iscsi02** from the inventory list
2. Select **Summary** to review capacity and configuration details

Add a new ESXi host

In this section, we will add a new ESXi host, **esx-03a.corp.local**, to the environment in Site A and ensure that it has the appropriate storage configured so that it can become a productive member of the cluster.
Hosts and Clusters View

1. Click on the **Hosts and Clusters** icon to return to that Inventory view.
2. Select **Site A Datacenter**

It is a best practice to bring hosts into a datacenter first before adding them to a cluster. If a host is added to a cluster first, by not having access to the cluster's storage volumes, it could impact High Availability (see Module 1 for more details on High Availability).

Begin the Add Host workflow

1. Go to the **Actions** menu
2. Select **Add Hosts...**
Enter the hostname

1. In the **Host name or IP address**, enter: `esx-03a.corp.local`
2. Click **Next**
Connection Settings

Add Host

1. Enter the following login details:
   - **User name**: root
   - **Password**: VMware1!

2. Click Next
Host Summary

Add Host

This screen shows the details of the host.

Click **Next**
Leave the default license choice and click **Next**.
Lockdown Mode

Add Host

Lockdown mode
Specify whether to enable lockdown mode on the host

- Enabled
  - The host will only be accessible through a local console or an authorized centralized management application.

- Disabled

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

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

When a host is being added to a Datacenter, it can be placed in what is called Lockdown mode. This can prevent unauthorized users from gaining access to the ESXi host either through local console access or remotely by way of SSH. If you are interested in Lockdown Mode, the details are covered in Module 1.

1. Leave the default setting and click Next.
VM Location

The virtual machines currently on the ESXi host being imported can be placed in either the Datacenter itself or in the default Discovered virtual machines folder.

1. Since there are no virtual machines on esx-03a.corp.local, leave the default setting and click Next.
Ready to Complete

Review the settings and click Finish to add the esx-03a.corp.local to the datacenter.
Host Added to Datacenter

Here you can see esx-03a.corp.loca has been added to the datacenter and is in Maintenance Mode.

Maintenance Mode is used for hosts that service. A host could enter Maintenance Mode so that it can be brought offline in order for additional memory to be added to the physical host. In our case, it is in Maintenance Mode once it has been added to the datacenter so that we can verify its settings prior to bringing it online and potentially conflicting with other hosts in the environment.
Prior to adding the new host to the cluster, an NFS datastore will be added to the host.

1. Click on the **Datastore** icon to switch to the Datastores view
2. Select the **ds-nfs01** datastore in the Inventory

**Mount NFS Datastore to New Host Wizard**

1. Click on the **Actions** drop-down menu
2. Select **Mount Datastore to AdditionalHosts**
In this case, there are two NFS datastores used by the Cluster Site A cluster. Adding an existing NFS datastore to a new host is a simple process.

1. Click on the **Actions** menu
2. Select **Mount Datastore to Additional Hosts...**

**Mount NFS Datastore - Select Host**

Mount Datastore to Additional Hosts  |  ds-nfs01

<table>
<thead>
<tr>
<th>Host</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>esx-03a.corp.local</td>
<td></td>
</tr>
</tbody>
</table>

1. Click the checkbox next to `esx-03a.corp.local`
2. Click **OK**
Mount NFS Datastore - Monitor Task

1. The mount task can be monitored using Recent Tasks
2. Once the mount completes, it can be verified by clicking on the Hosts tab.

This will show all hosts in the inventory that have mounted this datastore.

For additional practice, perform the same steps to mount the other NFS datastore, ds-nfs02 to the esx-03a.corp.local host.

Add iSCSI Target to an ESXi host

iSCSI devices are presented via an iSCSI Target. Think of this as the host for the iSCSI devices. The ESXi host needs to know where to look for the devices, so this section will
go through the process of pointing the ESXi host at the iSCSI target and discovering which LUNs are available.

**Select Hosts and Clusters**

1. Select the Hosts and Clusters icon and
2. Click on esx-03a.corp.local.
3. Finally, click the Configure tab.
Perform Dynamic Discovery

1. Select "Storage Adapters"
2. Select the "vmhba65" adapter in the iSCSI Software Adapter section.
3. Click on "Dynamic Discovery" - notice that the list of iSCSI Servers is currently empty
4. Click "Add"
Add Send Target Server

1. Enter the iSCSI Server Address: 10.10.20.60
2. Select OK
Rescan the iSCSI storage adapter

Once the new Target has been added, a message will appear in yellow to remind you of the need to tell the adapter to reach out and query the iSCSI Target.

1. Click on the \textit{vmhba65} iSCSI adapter to select it
2. Click the \textit{Rescan Storage...} icon to rescan

Rescan Storage

Leave the default options selected and click \textbf{OK}. 
Verify iSCSI Devices are Visible

1. Once the rescan is complete, Click on **Storage Devices**.
2. You should now see two iSCSI disks connected, both with 45GB of capacity.

Verify iSCSI Datastore Availability

1. Click on the **Datastores** tab.

Notice that the two iSCSI datastores are now visible to the **esx-03a.corp.local** host.
Move into the Cluster

Now that we have the storage configured, move the esx-03a-corp.local into Site A Cluster 1.

1. Right-click on esx-03a.corp.local
2. Select Move To...
1. Expand **Site A Datacenter** until you see **Site A Cluster 1** and select it.
2. Click **OK**.
We are given the option to either place all of the virtual machines hosted by esx-03a.corp.local into the Site A Cluster 1 Resource pool or create a new one.

1. Leave the default setting and click OK.

### Exit Maintenance Mode

The host has been added to the cluster. Now it can exit Maintenance Mode and participate in the cluster.
1. Right-click on esx-03a.corp.local
2. Select Maintenance Mode
3. Click Exit Maintenance Mode

**Ready to Go**

After a minute or two, the host will exit Maintenance Mode. If you enabled vSphere HA on the cluster, the HA agent will be configured and started before the host shows a Status of Normal. The process occurs fairly quickly, so a refresh of the Web Client may be required to show the current state.

Note that basic networking for virtual machines, vMotion, and IP Storage have been preconfigured on this host for the purpose of this lab exercise. Adding the new host to a distributed switch would typically be done prior to taking the host out of Maintenance Mode, but is not required for this exercise. Feel free to migrate this switch to the vDS if you would like the practice.

This host is now able to handle workloads for the cluster.
Storage vMotion

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

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

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

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

Navigate to Virtual Machines and Templates

Before the Storage vMotion, we'll verify there is no downtime for the virtual machine by constantly ping it. To ping it, we will need the IP address of the virtual machine, TinyLinux-01.
1. Click the **VMs and Templates** tab
2. Select **tinyLinux**
3. Ensure you are on the **Summary** tab
4. Note the IP Address of **tinyLinux, 192.168.120.51**

Open a Command Prompt

From the Windows Task Bar, click on the icon to open a command prompt.

**Ping TinyLinux-01**

```
C:\Users\Administrator>ping -t 192.168.120.51
```

Issue the following in the command prompt and press the Enter key:

```
ping -t 192.168.120.51
```

**Ping Results**

```
Pinging 192.168.120.51 with 32 bytes of data:
Reply from 192.168.120.51: bytes=32 time=2ms TTL=63
Reply from 192.168.120.51: bytes=32 time=1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
Reply from 192.168.120.51: bytes=32 time<1ms TTL=64
```
You should now see a continuous ping to tinyLinux.

**Storage View**

1. Click the **Storage** icon.

**List Virtual Machines on a Specified Datastore**

1. Navigate to and click on the **ds-iscsi01** datastore object in **Site A Datacenter** managed by the **vcsa-01a.corp.local** vCenter.
2. Click **VMs**
3. Click the **Virtual Machines** tab. You should now have a list of all virtual machines on the selected datastore.

*Note: depending on which lessons you have completed, the available datastores and virtual machines may be different than the images.*

**Drag and Drop Storage vMotion**

The VM tinyLinux is initially on **ds-iscsi01** and needs to be moved to **ds-nfs01**.

1. Click the tinyLinux VM and continue to hold the left mouse button while dragging the VM to the **ds-nfs01** datastore object. A green + will appear near the mouse cursor (see picture) when it is pointing at objects which are suitable targets for the object being moved. Let go of the mouse button to drop the **tinyLinux** VM onto the **ds-nfs01** object. The Migrate wizard will launch to complete the process.
Migrate Datastore

1. Select the radio button to **Change storage only**. Note that as of vSphere 6.5 (and higher) we do have the ability to change compute, network, and storage in the same vMotion operation.

2. Click **Next**
1. Note that the **ds-nfs01** datastore is already selected because that is where the VM was dropped prior to starting the wizard.
2. Click **Next** to accept the settings for the storage move.
Ready to Complete

Verify your selections on the Ready to complete screen and click **Finish** to start the migration.

Feel free to monitor the operation within the Recent Tasks pane or move on to the next step.
Confirm no packets were dropped

Go back to the command prompt and review the results of the ping. You can use the scroll bar to see if there were any dropped packets.

You may see instances where the time field increases to 2ms, but otherwise no packets should have dropped.

Stop the ping

Click the 'X' to stop the ping and close the command window.
The Storage vMotion progress can be monitored in the Recent Tasks panel

1. Once complete, click on the **ds-nfs01** datastore and notice that the **tinyLinux** virtual machine is listed.

The virtual machine's storage has been migrated from iSCSI to NFS storage without the need to take the virtual machine offline.
Managing Virtual Machine Disks

When working with Virtual Machines, you can create a virtual disk or use an existing virtual disk. A virtual disk comprises one or more files on the file system that appear as a single hard disk to the guest operating system. These disks are portable among hosts.

You use the "Create Virtual Machine" wizard to add virtual disks during virtual machine creation. However, in this lesson you will work with an existing Virtual Machine in the inventory.

This lesson will walk you through the process of adding a new virtual disk to an existing Virtual Machine. Additionally, you will extend the Virtual Machine's original disk to a larger capacity.

Navigate to the VMs and Templates management pane

1. Select VMs and Templates

From this view, we can see that there are several existing Virtual Machines in our vSphere environment. In the next step, we will add a new virtual disk to the windows10 Virtual Machine.
Verify windows10 Storage

1. Select Virtual Machine **windows10** and click the **Summary** tab.
2. If w12-core is not powered on, click the **power on** button.
3. In the VM Hardware pane, note the original disk configuration - single hard disk with a capacity of 24.00 GB. You may need to expand the VM Hardware section to see it.
1. Right-click on **windows10**
2. Select **Edit Settings**
Add New Device

1. Click the **Add New Device** button
2. Click **Hard Disk**
1. Decrease the size to **5 GB**
2. Click **OK** to create the new virtual disk
Monitor task progress

You can follow the progress in the Recent Tasks pane

1. You should now see **Hard disk 2** with a capacity of 5 GB available to the **windows10** VM.
Extend an existing Virtual Disk

In this section, you will extend an existing Virtual Disk for a Virtual Machine.

1. Right-click the Virtual Machine **windows10**
2. Select **Edit Settings**
### Hard disk 1 settings

In the Edit Settings wizard, note the capacity for Hard disk 1 is 24 GB.

<table>
<thead>
<tr>
<th>VM Hardware</th>
<th>VM Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory U</td>
<td>1</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB</td>
</tr>
<tr>
<td>Hard disk 1</td>
<td>24 GB</td>
</tr>
<tr>
<td>Hard disk 2</td>
<td>5 GB</td>
</tr>
<tr>
<td>SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
<tr>
<td>Network adapter 1</td>
<td>VM-RegionA01-vDS-COMP</td>
</tr>
</tbody>
</table>
## Extend Hard disk 1

1. Type **32** Hard disk 1 capacity field.
2. Click **OK**
Monitor task progress

You can follow the progress in the Recent Tasks pane

1. You should now see **Hard disk 1** with a capacity of 32 GB available to the **windows10** VM.
1. Note each of the configured virtual disks and associated capacity
2. Note that due to Thin Provisioning, the total consumed storage for the virtual disks is only using about half of the 32GB!
Working with Virtual Machine Snapshots

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines. You can also take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. The Snapshot Manager in the vSphere Web Client provides several operations for creating and managing virtual machine snapshots and snapshot trees. These operations let you create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more.

A Virtual Machine snapshot preserves the following information:

- **Virtual machine settings** - The virtual machine directory, which includes disks that were added or changed after you took the snapshot.
- **Power state** - The virtual machine can be powered on, powered off, or suspended.
- **Disk state** - State of all the virtual machine's virtual disks.
- **Memory state** (optional) - The contents of the virtual machine's memory.

In this section, you will create a Virtual Machine snapshot, make changes to the Virtual Machine's hardware and configuration state, and then revert back to the original state of the Virtual Machine by leveraging the vSphere Web Client Snapshot Manager.
Take a Virtual Machine Snapshot

In this step, you'll take a Snapshot of a Virtual Machine.

1. Right-click windows10
2. Select Snapshots
3. Click Take Snapshot
Enter a Name and Description for the VM Snapshot

1. In the Take Snapshot window, provide a name for the Snapshot point - **Snapshot #1**
2. Provide a description for the Snapshot point - **Snapshot taken prior to VM settings change**.
3. Uncheck the **Snapshot the virtual machine's memory** box.
4. Click "OK"

**Note:** When you take a snapshot of a powered on virtual machine, you are given the option to capture the running VMs memory state. In our case, since we are in a lab environment, this will generate unneeded I/O.
Open the Snapshots tab

Note the progress in the Recent Tasks pane. Once the snapshot task is complete:

1. Right-click windows10
2. Select Snapshots
3. Click Manage Snapshots
Snapshot Details

Here you can view the details of the snapshot and verify it was taken.

1. Click **Done** when you are finished viewing the details.

Change the Virtual Machine Settings

![Change the Virtual Machine Settings](image)
In this section, you will change the memory configuration for the Virtual Machine.

To change the memory configuration for **windows10**, we will need to shut it down.

1. From the **Actions** menu, Select **Power --> Power Off**. Select **Yes** to confirm power off.

   **NOTE**: This is not the proper way to shut the VM down gracefully, but for our lab environment, it provides a quick way to power off a machine.

2. Click the **Yes** button to power off the virtual machine.

**Launch the Edit Settings wizard**

1. Click the "**Actions**" drop down menu
2. Select "**Edit Settings...**"
Change the Virtual Machine's settings

<table>
<thead>
<tr>
<th>Virtual Hardware</th>
<th>VM Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1</td>
</tr>
<tr>
<td>Memory*</td>
<td>4</td>
</tr>
<tr>
<td>Hard disk 1</td>
<td>32</td>
</tr>
<tr>
<td>Hard disk 2</td>
<td>5</td>
</tr>
<tr>
<td>SCSI controller 0</td>
<td>LSI Logic SAS</td>
</tr>
</tbody>
</table>

1. In the Memory field, change this setting to "4".
**Review the Virtual Machine's new settings**

1. Note the new Memory configuration
2. Click **OK** to continue.
1. Make sure you are on the **Summary** tab for **windows10** and verify the memory has been updated.
Revert Virtual Machine settings using the Snapshot Manager

In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

1. Right-click **windows10**
2. Select **Snapshots**
3. Click **Manage Snapshots**
Select the VM Snapshot to Revert to

1. Make sure Snapshot #1 is selected.
2. Click the Revert To button.

Confirm Revert to Snapshot

1. Click OK to confirm action.
1. Click **Done** to close the Snapshot window.
Monitor task progress

1. Note the progress in the Recent Tasks pane.
2. Note the Memory configuration has reverted back to 1 GB.
Delete Snapshot #1

1. Click the **Delete All** button to remove the snapshot.

2. Click **OK** to confirm the deletion of all the snapshots.

It is a best practice to delete virtual machine snapshots when they are no longer needed. Over time the snapshot delta can grow to be quite large which could result in issues consolidating the virtual machine files and lead to performance issues.
Snapshot Removed

You can watch the progress of the snapshot being deleted in the Recent Tasks window.
Video: More on Virtual Machine Snapshots (2:33)

For more information on vSphere Virtual Machine Snapshots, be sure to check out this video.
vSphere Datastore Cluster

A vSphere Datastore Cluster balances I/O and storage capacity across a group of vSphere datastores. Depending on the level of automation desired, Storage Dynamic Resource Scheduler will place and migrate virtual machines in order to balance out datastore utilization across the Datastore Cluster.

In this section, you will create a vSphere Datastore Cluster using two iSCSI datastores.

Navigate to Storage

1. Click on the Storage icon.
New Datastore Cluster

1. Right Click on **Site A Datacenter**
2. Select **Storage**
3. Click **New Datastore Cluster...**
New Datastore Cluster - Name and Location

New Datastore Cluster

1. Enter DatastoreCluster-01 for the name.
2. Select Next.
### New Datastore Cluster - Storage DRS Automation

**New Datastore Cluster**

<table>
<thead>
<tr>
<th>Name and Location</th>
<th>Storage DRS Automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Name and Location</td>
<td>✓ Storage DRS Automation</td>
</tr>
<tr>
<td>✓ Location</td>
<td>Cluster automation level</td>
</tr>
<tr>
<td>✓ Select Datastores</td>
<td>Use cluster settings</td>
</tr>
<tr>
<td>✓ Ready to Complete</td>
<td>✓ Fully Automated</td>
</tr>
<tr>
<td>✓ Storage DRS Runtime Settings</td>
<td>Files will be migrated automatically to optimize resource usage.</td>
</tr>
</tbody>
</table>

1. Leave the defaults settings and select **Next**.
Storage DRS provides multiple options for tuning the sensitivity of storage cluster balancing.

1. Leave the defaults for now and select Next.
New Datastore Cluster - Select Clusters and Hosts

1. Because there are no standalone hosts, please select Site A Cluster.
2. Click the Next button.
New Datastore Cluster - Select Datastores

New Datastore Cluster

1. Select the **ds-iscsi01** and **ds-iscsi02** datastores for the new Datastore Cluster.
2. Click **Next**.
New Datastore Cluster- Ready to Complete

New Datastore Cluster

1. Review the Storage DRS settings and click the Finish button.

New Datastore Cluster- Summary

View the Recent Tasks to check the progress of the operation.

Conclusion

Leveraging vSphere Datastore Clusters in your vSphere environment can help to ensure datastores are filled evenly and I/O is spread out across the group of datastores in the cluster. Storage DRS can automate the initial placement of new virtual machines and
adjust virtual machine placement to maintain an even distribution of I/O across the datastore cluster.
Appendix
For More Information....

This section provides supplementary documentation and videos.

**Video: How to Configure a vSphere Standard Switch (VSS) (4:22)**

This video shows how to use the VMware vSphere web client to configure basic networking for your vSphere hosts using the vSphere Standard Switch (VSS).
vSphere 6.7 - vCenter Server High Availability

Lightboard illustration of the vCenter Server High Availability options for each deployment type.

**Video: Configure Alarms and Notification for VMware vSphere (5:20)**

This video shows how to use the VMware vSphere web client to configure vCenter Server alarms and alerts and how to enable email notification.
Video: Enable vSphere Host Lockdown Mode for VMware vSphere (4:48)

This video shows how to secure VMware vSphere hosts with Lockdown Mode in order to limit direct access to the host console and to require administrators manage hosts through vCenter Server.
(Optional) Video: Add VMware vSphere Hosts to Active Directory (3:40)

This video shows how to join a VMware vSphere host to a Microsoft Active Directory (AD) domain in order to allow administrators to use their Active Directory credentials to access and manage hosts.

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

This video shows how to use the VMware ESXi Firewall on the vSphere host to block incoming and outgoing communication and to manage the services running on the host.
REFERENCE - Unlock vCenter Single Sign On Users in the vSphere Web Client

A vCenter Single Sign On user account might be locked when a user exceeds the allowed number of failed login attempts. After a user account is locked, the user cannot log in to the Single Sign On system until the account is unlocked, either manually or after a certain amount of time has elapsed.

You specify the conditions under which a user account is locked in the Single Sign On Lockout Policy. Locked user accounts appear on the Users and Groups administration page. Users with appropriate privileges can manually unlock Single Sign On user accounts before the specified amount of time has elapsed. You must be a member of the Single Sign On Administrators group to unlock a Single Sign On user.

Locked Out User

By default, after three failed login attempts, the Users' account is locked.
In the lab, this policy has been disabled in order to prevent login issues that frequently occur with non-US keyboards.

This section has been included for reference purposes only.

Unlocking a User

Login to the vSphere Web Client as a user with SSO Admin privileges and navigate to the Users list.

1. Locate the locked user account -- it will show as "Yes" in the "Locked" column.
2. Right-click on the locked user and select 'Unlock'

Log out of the Web Client.

Change Your Password in the vSphere Web Client

Depending on your vCenter Single Sign On privileges, you might not be able to view or edit your Single Sign On user profile. However, all users can change their Single Sign On passwords in the vSphere Web Client. The password policy defined in the vCenter Single Sign-On configuration tool determines when your password expires. **By default, Single Sign-On passwords expire after 90 days in vSphere 6**, but your system administrator might change this depending on the policy of your organization. If you choose to keep the defaults, remember to change the password for the administrator@vsphere.local account password every 90 days or it will lock out on day 91.
Change Password

In the upper navigation pane, click your user name to pull down the menu.

Change Password Dialog

Select Change Password and type your current password.

Enter a new password.

Type a new password and confirm it.

Click the OK button to make the change.

NOTE: If you do change the password, please make sure to remember it for other activities in the lab.
In this section, you revert the Virtual Machine's configuration back to the original state using the Snapshot Manager.

1. Right-click **windows10**
2. Select **Snapshots**
3. Click **Manage Snapshots**

**What is vSphere Storage DRS? (5:08)**
This animated video shows how VMware Storage DRS reduces the time and complexity of provisioning virtual machines by aggregating data stores into a single pool, called a datastore cluster, enabling rapid placement of virtual machines and virtual machine disks.

**Creating a Datastore Cluster with Storage DRS (3:23)**

This video reviews the process of creating and managing a datastore cluster in a vSphere environment.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-2010-01-SDC

Version: 20210121-173215