# Table of Contents

Lab Overview - HOL-1811-01-SDC - What's New in vSphere 6.5 ........................................ 2
Lab Guidance .......................................................................................................................... 3
Module 1 - What's New in vSphere 6.5 (60 minutes) .......................................................... 9
  Introduction ......................................................................................................................... 10
vCenter Server Appliance: Overview .................................................................................. 12
vCenter Server Appliance: Management ............................................................................. 14
vCenter Server Appliance: High Availability (HA) ............................................................. 23
vCenter Server Appliance: Platform Services Controller High Availability (PSC HA) ......... 27
vCenter Server Appliance: Backup ..................................................................................... 32
vCenter Server Appliance: Restore (Interactive Simulation (iSIM)) ..................................... 42
vCenter Server Appliance: vSphere Update Manager Integration (Overview) ..................... 47
vCenter Server Appliance: vSphere Update Manager Integration (Video) ............................. 51
vCenter Server: Migration Assistant Tool ........................................................................... 53
HTML5 Host Client ................................................................................................................. 59
vSphere Web Client Enhancements ...................................................................................... 72
The NEW HTML5 vSphere Client ......................................................................................... 85
vSphere Security: Encrypted VMs & vMotion ................................................................. 116
Conclusion ............................................................................................................................ 146
Lab Overview - HOL-1811-01-SDC - What's New in vSphere 6.5
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual

Lab Module List:

• **Module 1 - What’s New in vSphere 6.5** (90 minutes) (Basic) This module provides a basic overview of some of the core enhancements made in vSphere 6.5. It starts out providing an overview of the vCenter Server Appliance and its management. We then go over the newly added native capabilities of the appliance such as High Availability, Backup/Restore, vSphere Update Manager, and the Migration Tool. Followed by a review of the new HTML5 based user interfaces for the host and web clients. Lastly, we go over the new security features such as encrypted virtual machines and encrypted vMotion.

Lab Captains:

• **Module 1 - Tim Sandy, Partner Systems Engineer, USA**

This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

Location of the Main Console

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

1. Click once in the active console window.
2. Click on the \textbf{Shift} key.

Click on the \texttt{@} key

1. Click on the \texttt{"@" 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. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - What's New in vSphere 6.5 (60 minutes)
Introduction

VMware announced vSphere 6.5, which is one of the most feature rich releases of vSphere in quite some time. The vCenter Server Appliance is taking charge in this release with several new features which we’ll cover in this blog article. Because of this, the vCenter Server Appliance is the recommended best practice over the Windows-based vCenter server. For starters, the installer has gotten an overhaul with a new modern look and feel. Users of both Linux and Mac will also be ecstatic since the installer is now supported on those platforms along with Microsoft Windows. The vCenter Server Appliance is also built on VMware’s Photon operating system now instead of the previous VMware linux-based operating system. Many of the enhancements in the vSphere 6.5 release are related to dramatically simplifying the user experience.

The vCenter Server Appliance now has features that are exclusive to it such as:

- Migration Tool
- Improved Appliance Management
- Native VMware Update Manager
- Native Host Profiles
- Native High Availability
- Native Backup / Restore

There are numerous other enhancements in vSphere 6.5 to include but not limited to:

- **Security enhancements:**
  - Virtual Machine Encryption
  - Encrypted vMotion
  - Secure boot for hosts and virtual machines
  - Enhanced Logging

- **Storage enhancements:**
  - 512e drive support
  - NFS 4.1 support
  - Automated UNMAP support

- **Networking enhancements:**
  - Dedicated Gateway for VMKernel Network adapter
  - SR-IOV provisioning

- **Availability enhancements:**
  - Proactive High Availability
  - Numerous Resource Management enhancements
  - vSphere Storage I/O Control using Storage Policies
vSphere Integrated Containers

**Application Program Interfaces (API) enhancements:**
- Industry Standard APIs for vCenter, virtual machines, etc.
- PowerCLI with cmdlets to automate almost anything

For this lab, we will walk through some of these new enhancements in vSphere 6.5. But because there are so many, we will walk through only a sub-set of them. There are other vSphere 6.5 labs that offer more detailed information and offer the ability to step through the configuration of these new or enhanced features.

**For this lab, we will go through the following items:**

- vCenter Server Overview
- vCenter Server Appliance (VCSA) Management
- vCenter Server - High Availability (HA)
- vCenter Server - Backup & Restore
- HTML5 Host Client
- vSphere Client
- vSphere Web Client

For additional resources on the enhancements in vSphere 6.5, be sure to read the **Conclusion** section of this lab which will provide some links to resources.
vCenter Server Appliance: Overview

With the release of vSphere 6.5, the vCenter Server Appliance (vCSA) has surpassed the feature set and performance of the Windows Installable vCenter server. Configuration maximums have been equal between the two since vSphere 6.0. There are two main components: vCenter and Platform Services Controller. Depending on the size or deployment model, the Platform Services Controller can be either embedded with the vCenter server or external based on your needs. These concepts and the architecture will be covered later in this module.

Why VCSA 6.5 Should Be The Default Deployment Choice

For starters, the installer received an overhaul with a new modern look and feel. Users of both Linux and Mac will also be ecstatic since the installer is now supported on those platforms along with Microsoft Windows. There is now a two-part deployment process for the vCenter Server Appliance. The first part deploys the appliance itself, and the second part sets all the configuration options you set during the deployment. The benefit of this is that we can do a snapshot of the appliance once the first step is complete. This provides a way to save time in the event that the deployment fails during step two. Simply go back to the snapshot, then start the second step again. This greatly reduces the time it takes for administrators to deploy the vCenter Server Appliance in the event of any deployment issues.

If that wasn’t enough, the vCenter Server Appliance now has features that are exclusive such as:

- Migration Assistance Tool
- Improved Appliance Management
- Native High Availability (HA)
- Native Backup / Restore

There are several other general improvements:

- The **vSphere Update Manager** is now integrated into the vCenter Server Appliance and no longer needs to be installed on a separate Windows VM.
- There has been performance improvements to the vSphere Web Client, to include a fully supported **HTML5-based** Host and vSphere Web Client.

Because of all of the previously mentioned enhancements to the vCenter Server Appliance, VMware highly recommends that the vCenter Server Appliance be used instead of the Windows-based vCenter Server. This is VMware's best practice for deploying and using the vCenter Server.
Security

Although the vCenter Server Appliance has previously been built on a customized 'VMware edition' of a SUSE Enterprise Linux appliance, the vCSA 6.5 runs PhotonOS. PhotonOS is a Linux OS that is purpose-built for virtualization by VMware. Therefore it comes pre-hardened and does not support the installation of third party software. The configuration disables unnecessary services, uses special host firewall and network interfaces and removes local accounts except for the application's administration. VMware pre-hardens the vCenter Server Appliance using the applicable guidelines of the Unix SRG STIG. Customers do not install software within the VCSA except for updates obtained from VMware. There is no general-purpose interface to the Linux operating system. Even the SSH interface, reserved for administrators, is disabled by default.

**NOTE:** Links in the lab manual are for reference only and the Hands On Lab environments **MAY NOT** be connected to the internet. So we are unable to access them in most cases, however we can save the link by taking note of the web address or taking a picture with the camera on a cellular phone.

Module Lessons

The remainder of this module focuses on lessons around these feature enhancements.
vCenter Server Appliance: Management

The vCenter Server Appliance Management user interface (formerly known as VAMI) serves as a control point to monitor and manage vCenter at the appliance level, even when the vSphere web client interface is down. In addition to configuring and editing network and time settings, we can check for appliance updates automatically, edit login credentials, and monitor resource utilization. The vCenter server database can be monitored by data type and also provide alerts when certain thresholds are reached.

The Appliance Management user interface is entirely in HTML, with no dependencies on Flash plug-ins anymore. This greatly improves the user experience due to the performance of HTML over Flash.

In this lesson, you will accomplish two primary tasks:

- Monitor the health, resource utilization, and database usage of the vCenter Server Appliance
- Edit settings of the vCenter Server Appliance
Launch Google Chrome

If Google Chrome is not already open, you can either...

1. **Double-click** the Google Chrome icon on the **Main Console Desktop**.
2. Or **single-click** the icon on the **Quick Launch bar**.

**NOTE**: If Google Chrome is already open, continue onto the next step.

**vCenter Appliance Bookmark**
1. Click on the **HOL Admin** folder in the Google Chrome Bookmarks Bar.
2. Then click on the **vcsa-01a Mgmt** bookmark.

**Log into vCenter Appliance Management Console**

1. On the bookmark toolbar, click the **HOL Admin** folder.
2. Click on the **vcsa-01a Mgmt** bookmark.
3. Type **root** in the username field.
4. Type **VMware1!** in the password field.
5. Then click the **Login** button.

**Summary: Monitor Health, Resource Utilization, and Database Usage of the vCenter Server Appliance**
Once logged in, we see the Summary page of the Appliance Management user interface.

1. The summary page shows the basic Health Status information of the appliance. The health badges in the appliance are based on capacity reached in CPU, Memory, and Database. The overall health badge will also change to yellow or orange if an appliance update is available, depending on the severity of the update.
2. We see the buttons which provide us the ability to Backup the appliance (see the Backup and Restore part of this module), Create a Support Bundle, and perform power operations such as a Reboot and Shutdown of the appliance.
3. If there are any health related messages, they would be reflected in this section of the Summary screen.
4. In this section, it provides the status of the vSphere Single Sign-On Domain.

CPU and Memory

1. Click on the CPU and Memory tab in the navigation pane on the left. We can monitor the appliance CPU and Memory utilization trends as far back as one quarter, which can be used to troubleshoot the appliance and vCenter Server resource usage.
2. Select the drop down arrow for the Overall CPU Utilization Trending graph and select 1 quarter.
3. Select the drop down arrow for the Overall Memory Utilization Trending graph and select 1 quarter.
Note: The Graph may look different depending on utilization.

Database

1. Click on the **Database** tab in the navigation pane.
2. The Appliance Management user interface provides a dashboard for the vCenter Server Appliance’s embedded Postgres database usage by data type, as well as space utilization trending with options to see any or all of the largest data types (Statistics, Events, Alarms and Tasks is known as SEAT data). We will also be alerted in the vSphere web client when certain capacity thresholds are reached.
3. Mouse over the current space utilization trending line graphs to see the breakdown of % utilization of the vCenter Postgres database by each data type.

Note: The Graph may look different depending on utilization.
Networking

1. Click on the Networking section in the left navigation pane.
2. Select the Monitor tab to see network utilization.
3. Select the drop down menu and select 1 quarter so we can see the network utilization for the quarter.

Note: The Graph may look different depending on utilization.

Syslog Configuration

The vCenter Server Appliance provides a way to send the logs to an external location. VMware recommends using VMware's vRealize Log Insight solution that collects
unstructured log data and organizes it into easily searchable log data. Think of it as a Google-like search engine for unstructured log data.

1. Click on the **Syslog Configuration** section in the left navigation pane.
2. As we see, the vCenter Server Appliance is already configured to send **ALL (*)** of its log data to **log-01a.corp.local** which is a vRealize Log Insight virtual appliance. The default port to connect to it uses **Port 514** and uses the **UDP protocol**.
3. Select the **Edit** button to see all the different options for the **Common Log Levels** (all (*), info, warning, error, etc.), **Remote Syslog Port**, and **Remote Syslog Protocol** (TCP, UDP, TLS, and RELP).

**Syslog Configuration - Edit Settings**

The Access section allows you to enable or disable the SSH Login and the Bash Shell.
1. Click on the **Access** section in the left navigation pane.

### Time

The Time section allows you to set the appropriate Time Zone and point to an internal or external Time Server. It lets you know if the NTP Daemon is up and running or not as well.

1. Click on the **Time** section in the left navigation pane.

### Update

The Update section allows you to set the update options to manually or automatically check and download updates for the vCenter Server Appliance. It provides what the current version that is installed as well as if a new one is available and its associated information.

1. Click on the **Update** section in the left navigation pane.
Administration

The Administration section is where you can change the vCenter Server Appliance "root" password. We can also set the associated password expiration settings such as if it expires, number of days valid, and an email notification of expiring passwords.

1. Click on the Administration section in the left navigation pane.

vCenter Appliance Management Overview - Complete

We have completed the overview of the vCenter Server Appliance management options in the new HTML5 interface. Hopefully we have provided a useful overview so that a virtual administrator would be comfortable managing the appliance.
vCenter Server Appliance: High Availability (HA)

The vCenter Server Appliance sits at the heart of a vSphere environment and provides services to manage various components of a virtual infrastructure such as ESXi hosts, virtual machines, and storage and networking resources. As large virtual infrastructures are built using vSphere, vCenter Server becomes a critical element in ensuring the business continuity of an organization. It is highly recommended that the vCenter Server must be protected from potential hardware and/or software failures while also recovering transparently from such failures. The vCenter Server Appliance version 6.5 provides a brand new high availability solution known as vCenter Server High Availability, or VCHA. VCHA is an available feature for the vCenter Server Appliance ONLY, and is not available for the Windows-based version of the vCenter Server.

vCenter Server High Availability protects vCenter Server Appliance against host and hardware failures. The active-passive architecture of the solution can also help you reduce downtime significantly when you patch the vCenter Server Appliance.

vCenter High Availability is a three-node cluster that contains an Active, Passive, and Witness node much like any other clustering technology. Two different configuration paths are available called Basic and Advanced. What you select depends on your existing configuration, but both Basic and Advanced result in exact same capabilities. In other words, use Basic whenever possible. If the vCenter Server being enabled for vCenter High Availability is being managed by a different vCenter Server in a separate SSO Domain or the Active, Passive, and Witness nodes are going to be managed by different vCenter Servers, the Advanced workflow will be required.
Architecture Overview

A vCenter Server High Availability cluster consists of three vCenter Server Appliance instances.

- The first instance that is initially deployed is the **Active node**, which is then cloned twice to create the:
- **Passive node** and
- **Witness node**

Together, the three nodes provide an active-passive failover solution for the vCenter Server.

As a best practice, we recommend that you deploy each of the nodes on a different ESXi instance to protect against hardware failures. Adding the three ESXi hosts to a Distributed Resource Scheduler (DRS) cluster can further protect your environment. If using the Basic workflow to enable vCenter High Availability, then the workflow will automatically place the nodes on different hosts and create anti-affinity rules for it if DRS is already enabled. If the Advanced workflow is being used, then the node placement is manual and would then need to create the anti-affinity DRS rules manually.

When the vCenter Server High Availability configuration is complete, only the Active node has an active management interface (public IP). The three nodes communicate
over a private network called **vCenter HA network** that is automatically set up as part of the configuration. The Active node and Passive nodes are continuously replicating data between them.

**NOTE:** The screen shot assumes that we are using embedded Platform Services Controllers and not external ones. Because they are embedded to the vCenter Server Appliance, when the appliances are configured in high availability, the Platform Services Controllers will be as well.

### Roles for Each Type of Node in a vCenter High Availability Cluster

**Active Node:**

- Node that runs the active instance of the vCenter server.
- Enables and uses the public IP address of the cluster.

**Passive Node:**

- Node that runs as the passive instance of vCenter server.
- Constantly receives state updates from the Active node via both PostgreSQL replication (synchronous) and rsync file-based replication (near synchronous).
- Equivalent to the Active node in terms of resources.
- Takes over the role of Active Node in the event that the Active node fails.

**Witness Node:**

- Serves as a quorum node.
- Used to break a tie in the event of a network partition causing a situation where the Active and Passive nodes cannot communicate with each other.
- A light-weight virtual machine utilizing a reduced set of hardware resources (1 vCPU & 1 GB RAM and the same disk footprint as the original vCenter server).
- It does not take over the role of either the Active or Passive nodes.

### How Does vCenter Server High Availability Work?

Availability of the vCenter Server Appliance works as follows under the following failure conditions:

1. **Active node fails:** As long as the Passive node and the Witness node can communicate with each other, the Passive node will promote itself to Active and start serving client requests.
2. **Passive node fails:** As long as the Active node and the Witness node can communicate with each other, the Active node will continue to operate as Active and continue to serve client requests.
3. **Witness node fails:** As long as the Active node and the Passive node can communicate with each other, the Active node will continue to operate as Active
and continue to serve client requests. The Passive node will continue to watch the Active node for failover.

4. **More than one node fails or is isolated:** This means all three nodes - Active, Passive, and Witness - cannot communicate with each other. This is more than a single point of failure and when this happens, the cluster is assumed non-functional and the vCenter server application shuts down to protect itself from data corruption.

5. **Isolated node behavior:** When a single node gets isolated from the cluster, it is automatically taken out of the cluster and all services are stopped. For example, if an Active node is isolated, all services are stopped to ensure that the Passive node can take over as long as it is connected to the Witness node. Isolated node detection takes into consideration intermittent network glitches and resolves to an isolated state only after all retry attempts have been exhausted.

**Note:** The **Return To Operation (RTO)** time for a failover is approximately 5 minutes in most cases, but can vary depending on various circumstances such as the size of your environment, size of the database, etc.

**vCenter Server Appliance High Availability Overview - Complete**

We have completed the overview of the vCenter Server Appliance 6.5 High Availability overview. After reviewing this, we hope that we stressed the importance that the use of the vCenter Server Appliance over the Windows based vCenter Server is now VMware's best practice, especially because of the High Availability capabilities.
vCenter Server Appliance: Platform Services Controller High Availability (PSC HA)

The vCenter Server Appliance 6.5 introduces a native option to protect a vCenter Server deployment from failures in hardware, hosts, and vCenter Appliance services.

The Platform Services Controllers (PSC) will also support High Availability natively, but do require an external load balancer when configuring external Platform Services Controllers for High Availability. In this lab, we have provided an Interactive Simulation (iSIM) on configuring High Availability for the vCenter Server Appliance. Also configuring the Platform Services Controllers for High Availability is an advanced task, so we have only provided some basic architectural information about this configuration.
Platform Services Controller High Availability (PSC HA)

In a few pages from this one, we have an Interactive Simulation (iSIM) on configuring vCenter Server High Availability, it contains the previous version of the vSphere Web Client. So be aware in the simulation after clicking on the vCenter server, we then click on the Manage tab instead of the Configuration tab that is in the new version. There will be some name differences as well as what is in the pages that will look different between the old and newer version of the vSphere Web Client. But the setup is essentially the same process.

We are also providing Platform Services Controller High Availability (PSC HA) which means you will need to use a third-party load balancer to get High Availability (HA) for your Platform Services Controller (PSC) infrastructure.

The PSC will operate more like DNS, where each vCenter will now know where all the Platform Services Controllers are in its domain. In the event that any Platform Services Controllers service fails, then the vCenter will automatically fail over to the next Platform Services Controller. The diagram above shows how this works. The large arrows
are where the vCenter is affinitized to (where it was installed against). If a Platform Services Controller fails, the vCenter can fail over through one of the dotted lines to another Platform Services Controller.

The High Availability mode is realized when the vCenters and Platform Services Controllers are all at the same functional level (everything is at same major build level). You can operate in mixed mode but PSC HA won’t be operational.

For more detailed information on how to configure High Availability for the Platform Services Controllers along with the vCenter Server Appliance 6.5, refer to this VMware KB article here.

**NOTE:** Links in the lab manual are for reference only and the Hands On Lab environments **MAY NOT** be connected to the internet. So we are unable to access them in most cases, however we can save the link by taking note of the web address or taking a picture with the camera on a cellular phone.

### vSphere Web Client (Newest Version)

![vSphere Web Client](image)

**NOTE:** In this lesson, we are only referring the screen captures and not actually looking at and manipulating anything in the lab environment you are currently working in.

Depending on what version of the vSphere Web Client we may be looking at, we will see some slight differences such as names of tabs and buttons in the main content pane. In this particular lesson where we are discussing the configuration of High Availability for the vCenter Server:

1. We see that the tab name is called **Configure** to get to the configuration section for vCenter Server High Availability. (in the new version the tab is called **Manage**)
2. Then once we click on **vCenter HA**, we then click on the **Configure** button. (in the old client the button is called **New Configuration**)

---

**HOL-1811-01-SDC**
In the Interactive Simulation (iSIM) that we will watch shortly, we have the previous version of the vSphere Web Client than what is currently in the lab environment:

1. The simulation has us click on the vCenter Server and then the Manage tab. (in the new client the tab is called the Configure tab)
2. Then we will select vCenter HA and click on the New Configuration button to start to configure High Availability. (in the new client the button is called Configure)

Hands On Labs - Interactive Simulation (iSIM): vCenter Server High Availability

Now we are going to launch the Interactive Simulation (iSIM). This simulation will walk us through the configuration of vCenter Server High Availability. Once finished with the Interactive Simulation (iSIM), please return to this page of the lab manual to continue with this module.

NOTE: The current video was recorded with the previous version of the vSphere Web Client. So you will see some the tab names and screens are slightly different from the most current version of the vSphere Web Client. Also, when in the Interactive Simulation (iSIM) where it has you type something into a text field, it will enter in the proper text for you no matter what you try to type into the text fields.
vCenter Server Appliance and Platform Services Controller
High Availability Overview Complete

Although this was a brief overview of the architecture associated to setting up external Platform Services Controllers in High Availability, we hope that the options for vCenter Server architecture makes more sense now as to why and how you may architect a vSphere environment based on individual needs.
vCenter Server Appliance: Backup

In vSphere 6.5, the vCenter Server Appliance (VCSA) has an out-of-the-box file-based backup and restore solution. You can back up to a single folder all of vCenter Server’s core configuration, inventory, and historical data. All of this data is streamed over FTP (or SFTP / FTPS) or HTTP / HTTPS. When it is time to restore to a previous backup, you can deploy a fresh appliance, point to the folder location of the vCenter Server backup files, and restore all of vCenter Server's configuration and inventory data (with optional historical data) from the backup.

In this lesson we will go through the steps to create a backup of the vCenter Server Appliance (VCSA) and then verify the back up. In the interest of time and resources for the Hands On Lab environment, we will go through another Interactive Simulation (iSIM) for the next lesson to show the steps associated to doing a restore.
Launch Google Chrome

If Google Chrome is not already open, you can either...

1. **Double-click** the Google Chrome icon on the **Main Console Desktop**.
2. Or click the Google Chrome icon on the **Quick Launch bar**.

**NOTE:** If Google Chrome is already open, continue onto the next step.
We will backing up the vCenter Server Appliance (VCSA) configuration files, inventory, and selected historical data to a folder of files placed on an FTP server.

If still logged into the vCenter Server Appliance from the previous lesson, we can skip the below steps. Otherwise, we will log in to the Appliance Management user interface to begin the vCenter Server backup process.

1. Click the **HOL Admin** bookmark.
2. Click on the **vcsa-01a Mgmt** shortcut in the drop-down.
3. Type **root** for the username.
4. Type **VMware1!** for the password.
5. Click on the **Login** button.

**Back up the vCenter Server Appliance (vCSA) using the Backup Appliance Wizard**
Backing up the vCenter Server Appliance (VCSA) starts on the summary page of the Appliance Management user interface (https://vCenter-FQDN-IP:5480).

To begin the process of backing up the appliance:

1. Click the **Summary** tab in the left Navigation Pane if not there already.
2. Click the **Backup** button in the upper right corner of the Appliance Management user interface.

**Backup Appliance Wizard - Enter backup details**

![Backup Appliance Wizard - Enter backup details](image)

The first set of information you will need to enter is the backup protocol (FTP, FTPS, SFTP, HTTP, HTTPS), the backup location or path, and a username/password for accessing that backup location. You also have the option of encrypting your data before any of it is transferred to the backup location, by checking the **Encrypt Backup Data** box. Note that the password you set here would be needed during the Restore process to access the vCenter Server Appliance backup. For this lab, we will not be encrypting the backup.

You will need to access this FTP server to place your vCenter Server backup files. You can create a new folder on the FTP path by adding to the path name after the IP address of the FTP server. Be sure if you create a folder for the backups on a server, that you ensure the folder name is the same when filling in the location path in the backup wizard.
1. Click the **Protocol** drop-down and select **FTP**. The drop-down does show you all the possible protocols such as HTTPS, HTTP, SCP, FTPS, and FTP.
2. In the **Backup Location** field, type **192.168.110.60/vcsa01a-backup**.
3. Keep the default value of **Port 21**.
4. In the **Username** field, type **root**.
5. In the **Password** field, type **VMware1!**.
6. Click the **Next** button to continue.

**Note:** The path in the Backup user interface should be entered without "ftp://", so that the Backup location should start with the FTP server’s IP address itself. You will also notice that you can **Encrypt** the backup and it will warn you when you are using the unsecure FTP/HTTP protocols. This is a fenced lab, so the need for a secured protocol is not necessary.

**Backup Appliance Wizard - Select parts to backup**

Next, you’ll want to select whether you choose to back up optional Stats, Events, Alarms, and Tasks (SEAT) data from the vCenter Server database. A core set of data (VC inventory, services, and OS) will be backed up by default. If we select to backup all types of data, then the backup file size will be larger than if we selectively chose to only backup say just the VC inventory data.

1. Leave the check box marked **Stats, Events, Alarms, and Tasks** checked to include this data in the backup.
2. Type **vCenter Backup Primary DC** in the **Description** field to help identify this backup.
3. Click the **Next** button to continue.

**NOTE:** The size of this backup will show a different size than what is showing in the screen capture.

**Backup Appliance Wizard - Ready to complete**

The third and last step provides a backup summary which gives you a confirmation of your backup protocol, location, credentials, encryption, and optional data.

1. Confirm the selections are correct.
2. Begin the backup by clicking the **Finish** button.
Backup Appliance Wizard - Progress Window

A pop-up window with the backup status will be displayed.

1. Verify the backup says **Backup job finished successfully** and reflects **100%**.
2. Once completed, click the **OK** button to close the Backup Progress window.

**NOTE:** The backup process should take less than two minutes, but could take longer due to various factors.

**Open New Tab**

1. Click on the **New tab** button next to the vSphere Web Client tab that is already open in Google Chrome.

**Connect to FTP Server**

1. Click on the new Google Chrome browser tab.
2. Type in the **ftp://192.168.110.60** into the address text field.
Authenticate to the FTP Server

1. An **Authentication Required** pop-up will be displayed, type **root** into the **User Name:** field.
2. Type **VMware1!** in the **Password:** field.
3. Then click the **Log In** button.

Verify vcsa01a-backup Folder Exists

1. Verify that **vcsa01a-backup** folder exists and click on the **vcsa01a-backup** link.

**NOTE:** The dates associated to the backup files in the screen capture will not be the same as yours. Once you have completed a backup during the lab, it should reflect the current date of when you completed the backup job.
Review vcsa01a-backup Files

1. We now see the contents of the **vcsa01a-backup** folder from the backup we just performed.

**NOTE:** The dates associated to the backup files in the screen capture will not be the same as yours. Once you have completed a backup during the lab, it should reflect the current date of when you completed the backup job.

Close FTP Server Tab

At this time, we are finished verifying the vcsa-01a.corp.local appliance backup job and can close the FTP Server and the vCenter Server Appliance Google Chrome tabs.

1. Click on the "X" of the **FTP Server Google Chrome tab** to close it.
2. Click on the "X" of the **vCenter Server Appliance Google Chrome tab** to close it.

What is Actually Backed Up (Content Library)

To add some clarification for the vCenter Server Appliance backup, let’s look at an existing content library that resides within the vCenter Server Appliance. Content Library stores it's metadata (the library’s description) in the vCenter Server embedded
Postgres database and has its services running in a vCenter Server. It stores its content (OVF, VMDK, ISO, etc.) in a Datastore outside the vCenter Server Appliance. That means that the vCenter Server Appliance backup only captures the metadata of the library.

**vCenter Server Appliance: Backup Overview Complete**

We have completed this overview on how to use the new backup feature that is native to the vCenter Server Appliance only. Backing up a vCenter Server is a critical part of a virtual administrators job to ensure that there is a valid backup in the event of a vCenter Server failure or possible corruption of data in the database. Now administrators can feel good knowing that they have a native mechanism to provide good backups of their most important virtual machine in their vSphere environment.
vCenter Server Appliance: Restore (Interactive Simulation (iSIM))

This is a **Hands-on Labs - Interactive Simulation (iSIM)**.

An Interactive Simulation (iSIM) presents content that is either too time consuming or too complex to include in a traditional Hands-on Labs experience. The user interface does not attach to a live software system, but instead creates a user interface that mimics the behavior of a live environment. You will follow instructions and click on interface elements in a manner similar to a traditional lab.

The orange boxes provide guidance for each click and action that will progress you to the next step. You may also use the left and right arrow keys to navigate the simulation in forward or in reverse.

The **vCenter Server Appliance Restore process consists of two stages:**

- Stage 1: Deploy a fresh appliance (OVF)
- Stage 2: Setting up the vCenter Server Appliance (configuration settings)

Follow the below steps to complete the vCenter Server Appliance restore processes using the Interactive Simulation (iSIM).

1. [CLICK HERE TO START THE INTERACTIVE SIMULATION (iSIM)](#). (opens either in a new browser window or tab)
2. When finished with the simulation, click the **Return to the lab** link or close the windows to continue with this lab.

**NOTE:** We have **ALSO** provided the individual guided steps that we will be performing in the Interactive Simulation (iSIM) for your reference. **These steps ARE NOT meant to be performed in the Hands On Lab environment!** If satisfied with just watching the Interactive Simulation (iSIM) only, feel free to skip to the next lesson.
Start the vCenter Server Appliance Installer

REMINDER: The below and remaining steps are for REFERENCE ONLY and NOT to be performed by you in the Hands On Lab environment. If satisfied with just watching the Interactive Simulation (iSIM) only, feel free to skip to the next lesson.

1. Click installer.exe to open the vCenter Server Appliance Installer.
2. Click on the Restore button.

Stage 1. Deploy OVF - Introduction

1. Review the different stages of restoring the vCenter Server Appliance and Click on the Next button.

Stage 1. Deploy OVF - Accept EULA

1. Review and Accept the License Agreement Terms.
2. Click on the Next button.

Stage 1. Deploy OVF - Enter Backup Details

Here we provide the location of the backup files created as part of the previous lesson vCenter Server Appliance Backup.
1. Backup location type: **FTP**.
2. Provide the Backup location: **192.168.110.60/vcsa01a-backup**.
3. Port should be **21**.
4. Username is **root**.
5. Password is **VMware1!**.
6. Encryption should be left blank.
7. Click on the **Next** button.

**Stage 1. Deploy OVF - Review Backup Information**

1. Review the back up information and Click on the **Next** button.

**Stage 1. Deploy OVF - Connect To Target**

1. Provide Target sever or hostname **esx-01a.corp.local**.
2. HTTPS default port is **443**.
3. User name is **root**.
4. Password is **VMware1!**.
5. Click on the **Next** button and click on the **Yes** button for the Certificate Warning.

**Stage 1. Deploy OVF - Set Up Target Appliance VM**

Here we provide a name for the appliance virtual machine. This name will be displayed within vSphere. The identity of the appliance will be restored to the host name of the backed up vCenter Server Appliance once the restore is completed.

1. The target appliance virtual machine should be **vcsa01a-backup**.
2. The root password is **VMware1!**.
3. Confirm the password is correct.
4. Click on the **Next** button.

**Stage 1. Deploy OVF - Select Deployment Size**

For the purposes of this lab, we chose to use the smallest footprint for the recovered vCenter Server Appliance.

1. We will select the deployment size of "**Tiny vCenter Server**" and then click on the **Next** button.

**Stage 1. Deploy OVF - Select Datastore**

This simulation contains only one datastore. In typical environments there would be multiple datastores available.

1. **RegionA01-ISCSI01-COMP01** datastore is already selected.
2. Select **Enable Thin Disk Mode**.
3. Click on the **Next** button.

### Stage 1. Deploy OVF - Configure Network Settings

Since our source vCenter Server Appliance had a static IP configured, we want that same IP to be used during the restore process. Typical vCenter Server Appliance installations will have a static IP assigned.

1. Click **DHCP** and change it to **static** instead (The original IP settings will populate automatically from the backup).
2. Click on the **Next** button.

### Stage 1. Deploy OVF - Review Settings

1. Review that the settings are correct and click on the **Finish** button to the vCenter Server Appliance deployment.

### Stage 1. Deploy OVF

This process was sped up as part of the simulation. In a typical environment this could take several minutes to complete.

1. Click the **Continue** button when the deployment is complete.

**NOTE**: It is highly recommended that you take a snapshot of the virtual machine before proceeding to Step 2 of the deployment process. Then if Step 2 fails, you can quickly and easily recover by using the snapshot instead of re-deploying the VCSA from scratch.

### Stage 2. Transfer Data - Introduction

Stage 2 involves configuring the newly deployed vCenter Server Appliance using the backup files from the FTP server we provided earlier.

1. Click on the **Next** button to start "**Stage 2**" of the restore process

### Stage 2. Transfer Data - Ready to Complete

1. Review the "**Backup details**" and click the **Finish** button to start the data transfer.
2. Click on the **OK** button to continue.
Stage 2. Transfer Data - Restore Complete

This process was sped up as part of the simulation. In a typical environment this could take several minutes to complete.

1. Click the "X" in upper right-hand corner to close the window when the restore is complete.

Verify vCenter Server Appliance is Ready

1. Click on Google Chrome to open the browser to confirm the vCenter Server Appliance login screen is active.
2. This concludes this interactive simulation, click on the "Return to the lab" link or close the windows to continue with this lab.

vCenter Server Appliance: Restore (Interactive Simulation) - Complete

We have successfully completed this lesson which showed the appropriate steps to restore a vCenter Server Appliance using the new native restore function. This represents the second half of restoring a backup job to ensure a quick and valid backup of a vCenter Server Appliance to ensure that a vSphere environment can be effectively backed up as well as restored quickly and efficiently with minimal administrative effort.
vCenter Server Appliance: vSphere Update Manager Integration (Overview)

The vSphere Update Manager is now integrated with the vCenter Server Appliance. When you deploy the vCenter Server Appliance, the VMware vSphere Update Manager Extension service starts automatically. We can no longer connect a vSphere Update Manager instance that is installed on a Windows Server with the vCenter Server Appliance. Attempts to connect vSphere Update Manager during installation on a Windows operating system to a vCenter Server Appliance will fail with an error.

The vSphere Update Manager deployed with the vCenter Server Appliance uses a PostgreSQL database. While vSphere Update Manager and the vCenter Server Appliance share the same PostgreSQL database instance, they use separate PostgreSQL databases which run on the vCenter Server Appliance. We are then able to reset/restore the vSphere Update Manager database separately from the vCenter Server Appliance database so we do not disrupt the data for the appliance.

vSphere Update Manager enables centralized, automated patch and version management for vSphere and offers support for ESXi hosts, virtual machines, and virtual appliances (Upgrade and patch operations of virtual appliances will be deprecated in a future release).

With vSphere Update Manager, we can perform the following tasks:

- Upgrade and Patch ESXi hosts.
- Install and update third-party software on hosts.
- Upgrade virtual machine hardware, VMware Tools, and Virtual Appliances.

vSphere Update Manager Web Client

- vSphere Update Manager Web Client for the vSphere Web Client - View scan results and compliance states for vSphere Inventory.

NOTE: Links in the lab manual are for reference only and the Hands On Lab environments MAY NOT be connected to the internet. So we are unable to access them in most cases, however we can save the link by taking note of the web address or taking a picture with the camera on a cellular phone.

What's New in vSphere Update Manager 6.5

- vSphere Update Manager 64-bit application support: The vSphere Update Manager server 6.5 and UMDS 6.5 are now supported 64-bit applications.
• **vSphere Update Manager as a service in the vCenter Server Appliance:** The vSphere Update Manager server is fully integrated with the vCenter Server Appliance and is enabled by default with the deployment of the vCenter Server Appliance.

• **Support for vSphere Update Manager Download Service (UMDS) Installation on Linux:** You can install the UMDS on a 64-bit Linux-based operating system. UMDS 6.5 installer is delivered with the ISO file of the vCenter Server Appliance.

• **Support for vSphere Update Manager Utility installation on Linux:** You can install the vSphere Update Manager Utility on a 64-bit Linux-based operating system.

• **Support for migration of vSphere Update Manager on Windows to vCenter Server Appliance 6.5:** VMware provides supported paths for migrating vSphere Update Manager from a Windows operating system to a vCenter Server Appliance.

• **vSphere Update Manager tab changed position in the vSphere user interface:** The vSphere Update Manager tab is now a top-level tab, same as the Monitor tab, the Configure tab, the Datacenters tab, the Host & Clusters tab, etc.

---

**vSphere Update Manager Web Client**

The client component of vSphere Update Manager is a plug-in to the vSphere Web Client. The vSphere Update Manager client component provides the full set of capabilities needed to perform patch and version management for a vSphere inventory.

The vSphere Update Manager plug-in for the vSphere Web Client requires no installation. After starting the vSphere Update Manager service in the vCenter Server Appliance, the vSphere Update Manager client component is automatically enabled in the vSphere Web Client. An vSphere Update Manager icon appears on the Home screen, and the vSphere Update Manager appears amongst the top-level tabs in the vSphere Web Client.

You can access the Administration view of vSphere Update Manager from vSphere Web Client Home screen. You can access the Compliance view of the vSphere Update Manager by selecting an object from the vSphere inventory and navigating to the Update Manager tab.

---

**vSphere Update Manager Download Service**

vSphere Update Manager Download Service (UMDS) is an optional module of Update Manager that you can use to download patch definitions on a system that is separate from the vSphere Update Manager server. Use Update Manager Download Service (UMDS) in case your vSphere Update Manager deployment system is secured and the machine on which the vSphere Update Manager server is installed has no access to the Internet.
You have two options for installation of the vSphere Update Manager Download Service (UMDS.) You can install vSphere Update Manager Download Service (UMDS.) on a 64-bit Windows operating systems. You must not install the vSphere Update Manager Download Service (UMDS.) on the same Windows machine where the Update Manager server is installed. You can also install the UMDS on a Linux-based system. In vSphere 6.5 release, an installer for Update Manager Download Service (UMDS) 6.5 is delivered with the ISO file of the vCenter Server Appliance. As a prerequisite to install the vSphere Update Manager Download Service (UMDS.) on Linux, the Linux server with a pre- configured PostgreSQL database and a 64-bit DSN is required. Mount the ISO file of the vCenter Server Appliance to the Linux machine, and install and configure vSphere Update Manager Download Service (UMDS.) 6.5.

**NOTE:** To use vSphere Update Manager Download Service (UMDS.), the download service must be of a version that is compatible with the Update Manager server. For more information about the compatibility between vSphere Update Manager and the UMDS, see the [Installing and Administering VMware vSphere Update Manager](#) documentation.

**vSphere Update Manager Utility**

The vSphere Update Manager Utility allows you to change the database password and proxy authentication, re-register vSphere Update Manager with vCenter Server, and replace the SSL certificates for Update Manager. For more information about reconfiguring the vSphere Update Manager settings by using the utility, see the [Reconfiguring VMware vSphere Update Manager](#) documentation.

When you install vSphere Update Manager or vSphere Update Manager Download Service (UMDS.), vSphere Update Manager Utility is silently installed on your system as an additional component.

**Migration Options**

VMware provides supported paths for migrating vSphere Update Manager from a Windows operating system to run in the vCenter Server Appliance.

vSphere Update Manager can be migrated to vCenter Server Appliance in the following vCenter Server deployment models:

- vCenter Server and vSphere Update Manager run on the same Windows machine
- vCenter Server and vSphere Update Manager run on different Windows machines
- vSphere Update Manager runs on a Windows machine and is connected to a vCenter Server Appliance (vCSA)

**NOTE:** For detailed information how to perform migration, see the [Installing and Administering VMware vSphere Update Manager](#) and the [vSphere Upgrade](#) documentation.
vCenter Server Appliance: vSphere Update Manager Integration (Overview) - Complete

This completes our vCenter Server Appliance: vSphere Update Manager Integration (Overview). The process of using vSphere Update Manager has not really changed, but is integrated into the vCenter Server Appliance rather than having to have another virtual machine with Windows server operating system and database on it. This saves money not having to license another operating system and database as well as reduce the workload associated to managing a vSphere environment. Also, when the vCenter Server Appliance is backed up, we know that the database for vSphere Update Manager is also backed up.
vCenter Server Appliance: vSphere Update Manager Integration (Video)

Due to the length of time it would take to perform the actions of updating hosts, virtual machines, or virtual appliances in the Hands On Lab environment, we won't be performing the actual steps in the lab. Instead, please watch this short (4:14 minutes) video which provides a brief overview of the steps involved in performing updates with the newly integrated vSphere Update Manager within the vCenter Server Appliance.

Video: VMware vSphere 6.5 Embedded vSphere Update Manager Demo (4:14 minutes)

NOTE: Click on the play button within the video player to watch the overview video on the new vSphere Update Manager Integration within the vCenter Server Appliance (vCSA) 6.5.

vCenter Server Appliance: vSphere Update Manager Integration (Video) - Complete

That completes the vCenter Server Appliance: vSphere Update Manager Integration overview. Again, vSphere Update Manager has not really changed from a functionality perspective. The fact that it is now integrated into the vCenter Server Appliance is the primary difference.
The benefits of integrating vSphere Update Manager (VUM) into the vCenter Server Appliance (vCSA) are:

- Automatically backs up the vSphere Update Manager (VUM) database located in the appliance during the appliance backup process.
- We no longer require a separate Microsoft Windows server for the vSphere Update Manager (VUM) database.
  - This also means one less virtual machine and associated resources (vCPU, vRAM, and disk space) that is needed for it.
  - One less Microsoft Server licenses needed.
vCenter Server: Migration Assistant Tool

VMware provides numerous supported paths for migrating and upgrading from vCenter Server version 5.5.x and version 6.0.x installations on Windows to the vCenter Server 6.5 Appliance. This section will provide a brief overview of these migration paths and the Migration Assistant Tool for vSphere 6.5. Keep in mind there are numerous architectures and configurations when migrating, the below information is just some examples of the potential migration paths. The ones listed are for those migrating from a older versions (5.5.x, 6.0.x) of the Windows-based vCenter Server to the vCenter Server Appliance.

**NOTE:** If you would like to see the full list of potential migration options, refer to the VMware vSphere 6.5 Documentation Center located here.

**ADDITIONAL NOTE:** Links in the lab manual are for reference only and the Hands On Lab environments **MAY NOT** be connected to the internet. So we are unable to access them in most cases, however we can save the link by taking note of the web address or taking a picture with the camera on a cellular phone.

**Supported vSphere Migration Paths**

**vCenter Server 5.5.x with Embedded vCenter Single-Sign-On Installation Before and After Migration.**

![Diagram showing vCenter Server 5.5.x migration to vCenter Server Appliance 6.5](image)
You can migrate a vCenter Server instance with an external vCenter Single Sign-On (SSO) version 5.5 or Platform Services Controller (PSC) version 6.0 to a vCenter Server Appliance 6.5 instance with an external Platform Services Controller (PSC) appliance. In this case you must first migrate the external vCenter Single Sign-On (SSO) instance or Platform Services Controller (PSC) instance and then the vCenter Server instance.

vCenter Server 5.5.x with External vCenter Single Sign-On (SSO) Installation Before and After Migration.
vCenter Server 6.0.x with External Platform Services Controller (PSC) Installation Before and After Migration.

If you have multiple systems configured for high availability, vCenter Server enables you to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process. If you have a multi-site setup configured with replication, you can use vCenter Server to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process.

For more information on mixed version transitional environments, see Upgrade or Migration Order and Mixed-Version Transitional Behavior for Multiple vCenter Server Instance Deployments.
Overview of Migration from vCenter Server on Windows to an Appliance

The Migration Assistant contains the following characteristics:

- Windows console application (see screen capture).
- Guides the user with the migration process.
- Enables target vCenter Server Appliance to run remote commands on the source vCenter Windows machine.
- Delivered as part of the vCenter Server Appliance ISO.
- No installation is required.
- Migration through Graphical User Interface (GUI) or Command-Line Interface (CLI).

The Migration Assistant contains the following characteristics:

- Windows console application (see screen capture).
- Guides the user with the migration process.
- Enables target vCenter Server Appliance to run remote commands on the source vCenter Windows machine.
- Delivered as part of the vCenter Server Appliance ISO.
- No installation is required.
- Migration through Graphical User Interface (GUI) or Command-Line Interface (CLI).
Migration Workflow

VMware provides many options to upgrade to vCenter Server 6.5. You can upgrade or migrate your vCenter Server version 5.5 or version 6.0 installation to version 6.5 using the method that best addresses your deployment goals and requirements.

High-level steps for upgrading or migrating vCenter Server:

1. Select the upgrade goal.
   - Upgrading the vCenter Server Appliance and Platform Services Controller Appliance
   - Upgrading vCenter Server for Windows
   - Migrating vCenter Server for Windows to vCenter Server Appliance

2. Verify that the system meets the hardware and software requirements.
3. Prepare the environment for the upgrade or migration.
4. Upgrade or migrate the vCenter Server for Windows or vCenter Server Appliance deployment.
5. Complete any required post-upgrade or post-migration tasks.

Additional Resources

**NOTE**: Links in the lab manual are for reference only and the Hands On Lab environments **MAY NOT** be connected to the internet. So we are unable to access them in most cases, however we can save the link by taking note of the web address or taking a picture with the camera on a cellular phone.

For more information on migrating the vCenter Server from versions 5.5.x and 6.0.x to 6.5, please see these resources...


**vCenter Server: Migration Assistant Tool - Complete**

That completes the overview on the various potential migration options that are available now when migrating from a previous version (5.5.x or 6.0.x) of vCenter Server to include the windows-based version. The Migration Tool as we see makes migration much easier than ever before by reducing issues associated to migrating as well as the time it takes to complete a migration. This tool has been well welcomed from many of our customers!
HTML5 Host Client

The HTML5 Host Client is a new product designed to replace the host client functionality of the original C# (called C Sharp) Client. The layout of the HTML5 user interface is generally similar to the vSphere Web Client to remain consistent in administrative workflow navigation. Yet, we have simplified areas where vCenter functionality is not required. However, since this is the "host" client, the functions that are available in this new interface are related to functions related to when connected to an individual host. This means we can't perform administrative tasks that are only typically available from within vCenter.

In the following tasks, we will go through some of the main areas of the new Host Client in order to get familiar with the new HTML5-based user interface.

Open Google Chrome Browser

If Google Chrome is not already open, you can either:
1. **Double-click** the Google Chrome icon on the **Main Console Desktop**.
2. Or click the icon on the **Quick Launch bar**.

**NOTE**: If Google Chrome is already open, continue onto the next step.

### Connect to HTML5 Host User Interface

1. In the Google Chrome bookmark tool bar, click on the **HOST-HTML5** folder.
2. Then click on the **esx-01a** bookmark.

### Log Into Host HTML5 Client

1. Type **root** into the User name text field.
2. Type **VMware1!** into the Password text field.
3. Then click on the **Log in** button.
Confirmation Page

1. For lab purposes, we will leave the default selection for the **Join the VMware Customer Experience Improvement Program** check box.
2. Click on the "OK" button

**NOTE:** In your vSphere environment, you can choose to keep this selected or to deselect it to opt out of the VMware Customer Experience Improvement Program.

Inventory Tree

You will see the basic Host resources displayed in a tree format on the left hand side of the user interface, listing: Host, Virtual Machines, Storage, and Networking.
• Left-Clicking on each resource type (Host, Virtual Machines, Storage, and Networking) in the navigation pane will display information regarding each resource in the main-context menu on the right.

For example, the host resource pane describes information about the CPU type, memory configuration, and basic performance information. Similarly, left clicking the Virtual Machine resource type will bring up a list of the virtual machines currently being hosted on that host.

Managing Resource Types

There are several options to manipulate the host such as creating virtual machines, shut down or reboot the host, and several others that can be selected by right clicking on the host.

1. **Right-click** the **Host** in the Navigator Pane.
2. We see that there is a selection when right-clicking the Host that says "Manage with vCenter Server". This selection will open a new tab in the browser and take us directly to the vSphere Web Client to manage the vCenter server making it quick and easy to get to it from the new HTML5 Host Client.

Troubleshooting Tasks

One of the main use cases for the Host Client is for troubleshooting the virtual infrastructure, particularly when vCenter Server and the vSphere Web Client are unavailable to do the remediation. In these situations, the key task is to examine the host running critical applications, examine associated logs and events, and potentially act on the host or virtual machine to bring it back online.
Minimize the Recent Tasks Pane

In order to see more of the information located in the bottom half of the Content Pane:

1. Click on the **Minimize icon** to minimize the Content Pane.

Monitor

1. Click on **Monitor** in the Navigator Pane.
Monitoring Performance

Monitoring the vCenter Server and its resources is an important task for most vSphere administrators to ensure that the vCenter Server is running optimally. If there are issues with the vCenter server, it will greatly impact how the vCenter server performs causing issues managing the vSphere environment. In the vSphere Host client, the Performance tab allows us to view how vCenter is performing as far as its resources, hardware status, events, tasks, logs, and notifications.

1. Click on the **Performance** tab in the Navigator Pane.
2. Hover your mouse over one of the performance spikes in the graph. We see it provides statistics for the time period where we are hovered over.
3. Change some of the perimeters in the drop-down menu to see performance data for Memory, Network, and Disk.

**NOTE:** The performance graph and data will be different in the lab environment than what is in the screen capture.
Reviewing Host Logs

Reviewing the host logs is also an important part of a virtual administrators job to look for the root causes of problems. Logs can provide very detailed information related to issues, and the logs in vSphere 6.5 are more detailed than any previous vSphere versions.

In order to review the host logs in the new vSphere host client:

1. Click on Monitor located under Host in the left navigation pane.
2. Click on the Logs tab at the top of the content pane.
3. Select the /var/log/vpxa.log log to see messages regarding the vCenter daemon.

**NOTE:** As a user interface aid, you can right-click any log and select Open in new window to see additional rows of the log. This screen can now also be searched by using the browser’s search capabilities (ie: Control-F).

Events Tab

1. Click on the Events tab at the top of the Content Pane.
Reviewing Host Events

Similar to Logs, a list of Events related to the Host can also be displayed.

1. Select the down arrow icon in the Event column.
2. Click on Filter in the drop-down menu.
3. Change the criteria drop-down menu to contains.
4. Type logged in into text box to filter for logged in events.
5. Click on the Filter button.

Filtered Host Events

1. We now see the filtered host events related to logged in events. We can easily filter for many different types of events using the filter option as we just did. This assists the virtual administrators quickly find specific events.

NOTE: The list of events may or may not be different in the lab environment than what we see in the screen capture.
Hardware Tab

1. Click on the **Hardware** tab at the top of the Content Pane.
2. We see we have a warning that says "**This system has no IPMI capabilities, you may need to install a driver to enable sensor data to be retrieved**". This hardware message is due to the nature of our lab environment having virtual nested hosts.

**NOTE:** The list of hardware messages may or may not be different in the lab environment than what we see in the screen capture.

Tasks Tab

1. Click on the **Tasks** tab at the top of the Content Pane.
2. We see that it provides a list of tasks that have been performed. Being a test lab environment, there is only a task related to the initial install.

**NOTE:** The list of tasks may or may not be different in the lab environment than what we see in the screen capture.
Notifications Tab

1. Click on the Notifications tab in the Content Pane.
2. We see the list of notifications such as "SSH is enabled on this host".

NOTE: The list of notifications may or may not be different in the lab environment than what we see in the screen capture.

Generating the GSS Support Bundle

Often, GSS (VMware Technical Support) will ask that a support bundle be generated to help troubleshoot Service Request (SR). The support bundle includes a snapshot of the current host state, configuration parameters, and relevant logs.

To create a support bundle to provide to VMware technical support:

1. Select the Monitor tab from the Navigator Pane.
2. Select the Logs tab in the Content Pane.
3. Then select Generate support bundle icon.

Note: It may take several minutes to generate the large bundle of log files, so please be patient.
Maximize Recent Tasks Pane

1. Click anywhere on the minimized Recent tasks pane to maximize it again.

Processing the GSS Support Bundle

1. As it creates the support bundle, the progress will be displayed in the Recent Tasks screen at the bottom of the user interface.

Confirmation of Support Bundle

Once the Support bundle has been created and is complete, we are prompted to either Download it now or we can Dismiss it and download later. For the sake of this lab, we are NOT going to download the support bundle.

1. Click on the Dismiss button.
Virtual Machines

1. Click on **Virtual Machines** in the Navigator Pane.
2. We see it lists all the virtual machines on the host we are connected to. We have basic functions that can be performed here such as:
   - Create/Register virtual machines
   - Power On/Off virtual machines
   - Open a console
   - Edit a virtual machine
   - Misc. other administrative tasks

**NOTE**: The list of virtual machines may be different in the lab environment than what you see in the screen capture.

Storage

1. Click on **Storage** in the Navigator Pane.
2. We see the list of currently connected storage devices. Within the storage area, we can do some of the following tasks:
   - Create a new datastore
   - Browse datastores
   - Create and modify storage adapters
   - See detailed information on storage devices
   - Misc. other storage related tasks
1. Click on **Networking** in the Navigator Pane.
2. We see that we can manage the following network tasks related to managing:
   - Port Groups
   - Virtual Switches
   - Physical NICs
   - VMkernel NICs
   - TCP/IP Stacks
   - Firewall rules

**HTML5 Host Client - Complete**

In this lesson, we walked through all the major areas of the new HTML5 Host Client user interface. We see that administrators have the ability to do the majority of the configurations and monitoring of a host when the vCenter server is not available. The ease of use and performance of this new client interface is because of it being based off of HTML rather than the older Java or C Sharp (C#) application programming. We look forward to these benefits in our other updated clients as well as we transition all of them over to HTML5.
vSphere Web Client Enhancements

From a user interface perspective, probably the most used interface is the vSphere Web Client. This interface continues to be based on the Adobe Flex platform and requires Adobe Flash to use. However, VMware has continued to identify areas for improvement that will help improve the user experience until it is completely retired. Through several outreach efforts over the past year we’ve identified some high-value areas where we think customers are looking most for improvements. This small list of high-impact improvements will help with the overall user experience with the vSphere Web Client while development continues with the HTML5-based vSphere Client:

- Inventory tree is the default view
- Home screen reorganized
- Renamed “Manage” tab to “Configure”
- Removed “Related Objects” tab
- Performance improvements (VM Rollup at 5000 instead of 50 VMs)
- Live refresh for power states, tasks, and more!
Launch Google Chrome

If Google Chrome is not already open, you can either:

1. **Double-click** the Google Chrome icon on the **Main Console Desktop**.
2. Or click the Google Chrome icon on the **Quick Launch bar**.

**NOTE**: If Google Chrome is already open, continue onto the next step.
vSphere Web Client and vSphere Client (HTML5) Links

A quick way to find the links to the vSphere Web Client (Flash) and the new vSphere Client (HTML5) is to open a browser and type in the IP address of Fully Qualified Domain Name (FQDN) of the vCenter Server. The page as you see in the screen shot provides the links to both of them in case you don't know them or have forgotten. As always, this page also provides links to vSphere documentation, the ability to browse datastores in the vSphere inventory, and much more.

To find the links to the vSphere Web Client (Flash) or the new vSphere Client (HTML5):

1. You can either type the IP Address or Fully Qualified Domain Name (FQDN) of the vCenter Server, in our case, type **https://vcsa-01a.corp.local** into the browser path.
2. Then click on the **vSphere Web Client (Flash)** link to go to the old Flash-based version of the vSphere Web Client.
vSphere Web Client (Flash) Overview

First, we will look at the older Flash-based version vSphere Web Client, to do that:

1. Once the page loads fully, type **administrator@vsphere.local** into the User name text box.
2. Type **VMware1!** into the Password text box.
3. Then click on the **Login** button.

**Use Keyboard Short Cuts for Navigation and View Them in Home Menu**

Keyboard shortcuts are present in the 5.5 and 6.0 vSphere Web Client, but were not visible. We can view these objects in the vSphere environment using the key combinations to quickly navigate between Home, Hosts and Clusters, Storage, Networking, etc.

We can see these shortcuts by hovering the mouse over the **Home** menu.
1. **Hover the mouse** over the Home icon to bring up the drop-down menu of options.

2. Use some of the Ctrl+Alt+# key combinations out to see how the shortcut keys work:
   - Ctrl+Alt+1 – Home screen
   - Ctrl+Alt+2 – vCenter Inventory Lists (Object Navigator)
   - Ctrl+Alt+3 – Hosts and Clusters tree
   - Ctrl+Alt+4 – VMs and Templates tree
   - Ctrl+Alt+5 – Storage tree
   - Ctrl+Alt+6 – Networking tree

   **Note:** Use the Ctrl+Command+Number key combination if using Mac.

### Close Panes (if needed)

If the vSphere Web Client has the default view with all four panes maximized, perform the following steps. Otherwise, we can skip these steps:

1. Click on the **Pin** icon for the **Work In Progress** pane.
2. Click on the **Pin** icon for the **Alarms** pane.
3. Click on the **Pin** icon for the **Recent Tasks** pane.
4. Click on the **Pin** icon for the **Recent Objects** pane.
Object Tabs

In prior releases, all objects within a container, or related to an object, appeared under the Related Objects tab. This tab has been replaced with top-level tabs that categorize the related objects as: Hosts, VMs, Datastores, and Networks. This change has been made for all vSphere objects, and only the applicable categories are shown for each object type (for a VM, the tabs are Datastores, and Networks).

1. This example shows "vcsa-01b.corp.local" is the selected object.
2. Here we see all the new tabs in the enhanced vSphere Web Client.

Object Details Titlebar: Action Icons

1. We see in the Object Details title bar, it displays the selected object’s icon and name, action icons, and the Actions menu. Using the action icons, you can now perform common actions with a single click.

NOTE: This example shows "vcsa-01b.corp.local" is the selected object.
1. Click the **Home** icon and select **Home** from the drop-down menu.
2. Click on **Tags & Custom Attributes** in the left Navigation Pane.
Creating Custom Attributes using the Global Custom Attributes View

1. Select the **Custom Attributes** tab.
2. To create a new Custom Attribute, click the **Add** icon and the **New Custom Attribute** dialog appears.

**New Custom Attribute**

1. Type **VM_Custom** for the name in the **Attribute**: field.
2. Scroll to the bottom of the list and select **Virtual Machine** from the **Type: drop-down menu.**
3. Click **OK** to finish creating the new attribute. The new attribute now appears in the list.

**NOTE:** The list of custom attributes may be different than what you see in the screen capture.

**Creating Custom Attributes using the Global Custom Attributes View**

1. To create another new Custom Attribute, click the **Add** icon and the **New Custom Attribute** dialog appears.

**NOTE:** The list of custom attributes may be different than what you see in the screen capture.
New Custom Attribute

1. Type **vApp_Custom** for the name in the **Attribute:** field.
2. Scroll to the bottom of the list and select **Virtual App** from the **Type: drop-down menu.**
3. Click **OK** to finish creating the new attribute. The new attribute now appears in the list.
Renaming Custom Attributes Using the Global Custom Attributes View

1. Select **vApp_custom** attribute that we created in the list.
2. Click the **Edit** button. The **Edit Custom Attribute** dialog appears.

Renaming Custom Attributes Using the Global Custom Attributes View
1. Rename the attribute to **vApp_Custom**.
2. Click the **OK** button. In the list, the selected attribute’s name now reflects the changed name.

### Deleting Custom Attributes using the Global Custom Attributes View

Since we won't be using these custom attributes and were just intended to show how to create them, we will delete both of them.

1. Select **vApp_Custom_Upd** and the **VM_Custom** tags while holding down the **CTRL** (Command for Mac) key.
2. Click the **Delete** button.
3. A confirmation appears, click the **Yes** button.

**NOTE:** The list of custom attributes may be different than what you see in the screen capture.
Confirm Deletion

1. Click on the **Yes** button to delete the custom attributes.

**vSphere Web Client Enhancements - Complete**

That completes the overview of the enhancements we have made to the vSphere Web Client that is based on Adobe Flash. The web client performs much better than previous versions and we have added more capabilities to it that were only available in the old C# client. This was in part due to integrating vSphere Update Manager and other features into the new vCenter Server Appliance. This is also what allowed us to decommission the old C# client.
The NEW HTML5 vSphere Client

With vSphere 6.5 I’m excited to say that we have a fully supported version of the HTML5-based **vSphere Client** that will run alongside the vSphere Web Client. The vSphere Client is built right into vCenter Server 6.5 (both Windows and Appliance) and is enabled by default. While the vSphere Client doesn’t yet have full feature parity the team has prioritized many of the day to day tasks of administrators and continue to seek feedback on what’s missing that will enable customers to use it full time. The vSphere Web Client will continue to be accessible via “http://<vcenter_fqdn>/vsphere-client” while the vSphere Client will be reachable via “http://<vcenter_fqdn>/ui”. VMware will also be periodically updating the vSphere Client outside of the normal vCenter Server release cycle. To make sure it is easy and simple for customers to stay up to date the vSphere Client will be able to be updated without any effects to the rest of vCenter Server.

Now let’s take a look at some of the benefits to the new vSphere Client:

- Clean, consistent UI built on VMware’s new Clarity UI standards (to be adopted across our portfolio).
- Built on HTML5 so it is truly a cross-browser and cross-platform application.
- No browser plugins to install/manage.
- Integrated into vCenter Server for 6.5 and fully supported.
- Fully supports Enhanced Linked Mode.
- Users of the Fling have been extremely positive about its performance.

Keep in mind when clicking on objects in the left Navigation Pane, depending on what "type" of object we clicked will determine what kind of information is presented in the Content Pane on the right side of the user interface.

**UPDATE:** On **July 27th, 2017**, VMware released an updated version of **vSphere version 6.5 Update 1**. With this update, the vCenter server HTML5 web interface was updated. The update greatly enhanced the new HTML5 interface making it approximately 90% feature parity to the vSphere Web Client. When customers update to vSphere 6.5 Update 1, they can then use the new HTML5 interface for most of their day-to-day administrative tasks for the most part.
Launch Google Chrome

If Google Chrome is not already open, you can either:

1. **Double-click** the Google Chrome icon on the **Main Console Desktop**.
2. Or click the Google Chrome icon on the **Quick Launch bar**.

**NOTE:** If Google Chrome is already open, continue onto the next step.
HTML5-Based vSphere Client

A quick way to find the new HTML5 vSphere Client is to open a browser and type in the IP address of Fully Qualified Domain Name (FQDN) of the vCenter Server. The page as you see in the screen shot provides the links to both of them in case you don't know them or have forgotten. As always, this page also provides links to vSphere documentation, the ability to browse datastores in the vSphere inventory, and much more.

To use the new HTML5-based vSphere Client:

1. Type https://vcsa-01a.corp.local into the address bar.
2. Click on the vSphere Client (HTML5) - partially functionality link.
Login to the HTML5 vSphere Client

If it doesn’t automatically log you into the new HTML5 client, log in with the below information:

1. Type `administrator@corp.local` for the User name field.
2. Type `VMware1!` in the Password field.
3. Click on the Login button.

Recent Tasks and Alarms

1. The Recent Tasks and Alarms have been moved to the bottom of the interface to offer more real estate for the users. Like previous versions, we can also minimize it to gain even more real estate when working in the interface.
2. We also have a More Tasks link in the lower right-hand corner that we can select to see a full list of tasks and alarms.
Minimize Recent Tasks And Alarms

1. Click on the with the **two down arrows icon** to minimize the **Recent Tasks and Alarms** widget in the lower right-hand corner of the interface.

**NOTE:** Once it is minimized, we can maximize it again by simply clicking on the two up arrows icon that will be in the very lower right-hand corner of the user interface.

**HTML5 vSphere Client Overview**

Let's take a look at the new HTML5 interface and where to find some of the items that you may have used in the past:
1. Click on the VM icon in the upper left-hand corner of the interface.

**Shortcuts: Inventories and Monitoring**

As we see here, this looks familiar and has the shortcuts to the **Inventories** and **Monitoring** items. As mentioned previously, the new HTML5 vSphere client is not at full feature parity with the older Flash based vSphere Web Client. So that is why we don’t see as many items as you would in the vSphere Web Client.

**NOTE:** On **July 27th, 2017**, VMware released an updated version of **vSphere version 6.5 Update 1**. With this update, the vCenter server HTML5 web interface was updated. The update greatly enhanced the new HTML5 interface making it approximately 90% feature parity to the vSphere Web Client. When customers update to vSphere 6.5 Update 1, they can then use the new HTML5 interface for most of their day-to-day administrative tasks for the most part.
Menu

Instead of the old Home icon that was in the vSphere Web Client, it is now titled Menu, but still has the same list of options.

1. Click on the Menu drop-down menu, we see the list looks very much the same as the Flash-based interface.

Global Search

Next to the Menu, we have the new Global Search that allows you to search for any object type in the vSphere environment.
1. Click inside the **Global Search** field and type `linux` to do a search for anything with the name `linux` in it.

2. We see that the results come back with a VM Template called `linux-micro-01-template` and a virtual machine named `linux-micro-01a`.

No matter what type of object you are looking for, you can quickly and easily find it from the Global Search.

### User Menu

![User Menu](image)

There has been a few minor changes under the user name drop-down menu. There is now the **Change Time Format...** setting, but no longer is there the **Remove Stored Data**, **Reset To Factory Defaults**, or **Change Password** selections.

1. Click on the **Administrator@CORP.LOCAL** drop-down menu.

### Help Menu

![Help Menu](image)

1. Click on the **Help** drop-down arrow to see the Help menu items.
Feedback Icon

A new item added to the interface is the smiley face in the upper right-hand corner. As we see in the screen capture, it gives a way to send VMware feedback directly from the interface.

1. Click on the Smiley Face icon, we will see a pop-up comes up.

Provide Feedback

1. First you can select which smiley face icon represents your current situation/attitude as to the information you are submitting for feedback.
2. Type in what feedback you want to provide to VMware in the Tell us more text box.
3. We have the option to type in our email address if we desire, or we can remain anonymous by not filing in the text box.
4. We can click the Take Screenshot button to include a screenshot if desired to show VMware what we are referring to.
5. Click the CANCEL button so we don't send information to VMware at this time from a lab environment.
We see the Home page provides us a great overview of the current status of the vCenter environment.

1. Click on the **Home** icon in the left Navigation Pane.
2. It provides us the total amount of resources such as CPU, Memory, and Storage within the associated vCenter server we have selected.
3. Then how many Powered On, Off, and Suspended virtual machines (VM) and how many Disconnected/Connected hosts as well as ones in Maintenance Mode.
4. It also gives us a list of the objects with the most Alerts for quick and easy troubleshooting.
5. And finally, it shows a list of the installed Plug-ins.
1. Click on the **Menu** Drop-down menu.
2. Then click on **Hosts and Clusters** in the drop-down menu.
By selecting Hosts and Clusters from the Menu drop-down menu previously, it automatically has that view selected for us. We see that the look and the contents have not changed from the older vSphere Web Client versions. Most of the interface still has items in the same place as before making learning the new user interface extremely easy.

1. **Expand** out all areas by clicking on the **arrows** next to the objects.
1. Click on the **VMs and Templates** icon and then expand out all areas by clicking on the arrows next to the objects.
1. Click on the **Storage** icon and then expand out all areas by clicking on the arrows next to the objects.
Networking

As we have seen in the last few steps, the only thing that has really changed is how the icons look because of being based on HTML.

1. Click on the Networking icon and then expand out all areas by clicking on the arrows next to the objects.

The New Tabs
1. For the tabs, they are very similar to the new version of the vSphere Web Client. However, we see it is different than the older versions of the vSphere Web Client. But they are straightforward to understand by their names, and to know what information is contained in them. So there will be little to no learning curve for virtual administrators that are used to using the older vSphere Web Client.

**The Summary Tab**

1. We see the **Summary** tab provides us the total amount of CPU, Memory, and Storage resource being used on the vcsa-01a.corp.local vCenter server.
2. It also shows us any **Custom Attributes** we may have.
3. As well as any **Tags** that we are using.
Monitor Tab

1. Click on the **Monitor** tab.
2. Under the **Monitor** tab, we have several selections for All Issues, Triggered Alarms, Alarm Definitions, Tasks, and Events.

Configure Tab
Because of adding new tabs such as the Permissions, Datacenters, Datastores, Networks, etc., you will see that there is limited configuration items located under the Configure tab now.

To see what is listed in the Configure tab:

1. Click on the **Configure** tab.
2. Then click on the **Advanced Settings**.
3. You may have to scroll down and over to see all the various advanced settings.

We can see that now there are only the Advanced Settings and the Storage Providers sub-sections that we can configure. The bulk of configurations were located here in previous versions of the vSphere Web Client.

**Permissions Tab**

![Permissions Tab](image)

Under the Permissions tab, it lists all the users and groups, what role their account holds, and if it is a global permission or not.

1. Click on the **Permissions** tab.
Datacenters Tab

1. Click on the **Datacenters** tab.
2. **Right-click** on the **RegionA01 datacenter** to see the potential actions you can take against it.
1. Click on the **Hosts & Clusters** tab.
2. Then **Right-click** on the **esx-01a.corp.local** virtual machine to see the drop-down menu list of potential tasks to perform.
1. Click on the **VMs** tab.
2. Then **Right-click** on one of the virtual machine to see the drop-down menu list of potential tasks to perform.
1. Click on the **Datastores** tab.
2. Then **Right-click** on the datastore to see the drop-down menu list of potential tasks to perform.
Networks Tab

Now let's look at the Networks tab and see how the networking information is presented in the new interface.

To look at the networks settings such as Distributed Switches:

1. Click on the **Networks** tab.
2. Click on the **Distributed Switches** tab.
3. Right-click on the **RegionA01-vDS-COMP** Distributed Switch.

Here we see the sub-menu where we can make setting changes to this distributed switch. A nice addition we see in the menu is the ability to add notes which can be extremely useful for administrators to make notes on the purpose of this distributed switch, settings, etc. This becomes useful for others to read and understand why the settings were made by someone else, especially if the individual no longer works for the company anymore.
Navigation Pane

We see in the left Navigation Pane that its options are very similar to the Home menu. All of the items in the Navigation Pane are also listed on one of the tabs across the top of the interface when we were clicked on the vCenter server. So there is more than one way to get to these items from within the interface.

1. Click on the **Global Inventory Lists** in the Navigation Pane.
The list of items in the Global Inventory List looks the same as the normal vSphere Web Client list does, just the icons look different because of it being HTML.
Menu Drop-down

1. Click on the **Menu** drop-down menu.
2. Then click on **Administration** in the drop-down menu.
1. Under Administration, we have **Access Control** items such as **Roles** and **Global Permissions** as well as **Solutions** that has **Client Plug Ins**.
2. Then we can select between the **Description**, **Usage**, and **Privileges**.
1. The **Tasks**, **Events**, and **Tags & Custom Attributes** selections we already saw in the other primary tabs at the top of the user interface. So there is no need to review them again from the Navigation Pane.
1. Click on **New Search** in the Navigation Pane.
1. Type **kms** into the search text field.

We see that it lists the two HyTrust KMS servers and their associated information that we have on this vCenter server. Notice the virtual machine names are links in which you can click on them and take us to that virtual machine.

1. Click on the **kms-01a.corp.local** virtual machine link.
1. Notice after clicking the virtual machine link, it takes us to the **VMs and Templates** tab and shows all relevant information about the virtual machine in the Content Pane.

**HTML5 vSphere Client Overview Completed**

That completes our overview of the new HTML5 vSphere Client!

Hopefully this overview of the new client provided a valuable overview to where we can start using this easy to use and better performing interface for the virtual administrators day to day tasks.

**NOTE:** Again, keep in mind that the new HTML5 vSphere Client IS **NOT** at feature parity with the vSphere Web Client which is still based off of Adobe Flex/Flash. So there are some administrative tasks you will still need to use the Flash-based vSphere Web Client to accomplish. In a future release, the new HTML5 client will become 100% feature parity and we will retire the old Flash-based vSphere Web Client.
vSphere Security: Encrypted VMs & vMotion

vSphere 6.5 is a turning point in VMware infrastructure security. What was mostly an afterthought by many IT folks only a few short years ago is now one of the top drivers of innovation for vSphere. Security has become a front and center focus of this release and I think you’ll like what we’ve come up with.

Our focus on security is manageability. If security is not easy to implement and manage then the benefit it may bring is offset. Security in a virtual infrastructure must be able to be done “at scale”. Managing 100’s or 1000’s of security “snowflakes” is something no IT manager wants to do. She/He doesn’t have the resources to do that. The key to security at scale is automation and in these new features you’ll see plenty of that.

In this section, we will provide a brief overview of vSphere 6.5 new Security features such as:

- Add and create a trust between a Key Management Server (KMS) and a vCenter Server.
- Create an encryption storage policy.
- Encrypt an existing VM.
- Encrypted vMotion.

Because this is an introduction lab, we will not be walking through all the steps to configure for encrypted virtual machines, the associated policies, and the task of actually doing a vMotion of a virtual machine. This sections is to provide a basic information on these topics. For more detailed information and the ability to perform the actual configuration steps, be sure to go and take the "HOL-1811-04-SDC - vSphere 6.5 Security Concepts and Implementation" lab, specifically Modules 4-5 and 8.
Launch the Chrome Browser

If Google Chrome is not already open, you can either:

1. Double-click the **Google Chrome icon** on the **Main Console Desktop**.
2. Or click the **Google Chrome icon** on the **Quick Launch bar**.

**NOTE**: If Google Chrome is already open, continue onto the next step.

Connect to RegionB vCenter
1. Click on the **RegionB vCenter** bookmark,

**Log Into RegionB vCenter**

If the RegionB vCenter server is already open in a Google Chrome tab, we can skip Steps 1 - 3, otherwise complete the below steps:

1. Type **administrator@vsphere.local** into the User name text box.
2. Type **VMware1!** into the Password text box.
3. Then click on the **Login** button.

**Global Inventory Lists**
1. Click on the **Home** Icon.
2. Click on the **Global Inventory Lists**.

### Navigate to vCenter Servers List

1. Under **Resources**, click on **vCenter Servers** in the Navigation Pane.
Select vsca-01a.corp.local

1. Select the vsca-01b.corp.local vCenter server in the left Navigation Pane.
2. Click on the Configure tab.
3. Click on the Key Management Servers section.
4. Click on the Add Server Icon (has green plus sign).

Add a KMS Server

We would then Input the following examples of information associated to a KMS server:

1. Keep the default KMS cluster selection of <Create new cluster>. 
2. Type **KMS Cluster 1** in for the **Cluster name** text field.
3. Type **KMS Server 1** into the **Server alias** text field.

### Add a KMS Server (continued)

1. Type **kms-01b.corp.local** for the **Server address** text field.
2. Type **5696** for the **Server port** text field.
3. Then click on the **OK** button.
Set the Default KMS Cluster

We would then get a pop-up window asking if we want to select the newly added KMS server as the default KMS server.

1. Click on the **Yes** button to make this your Default KMS Server.

Trust the Certificate

![Certificate Trust Window](image)
We would then need to trust the certificate presented by the newly added KMS Server.

1. Click on the Trust button.

Configure vCenter Trust Relationship

1. Click on KMS Server 1 which is listed under KMS Cluster 1.
2. Click on the Establish trust with KMS icon.

Upload certificate and private key

1. Click on the Upload certificate and private key radius button.
2. Then click on the OK button.
1. Click on the **Upload file...** button at the **top** of the pop-up window.
Path

1. Browse to the path "C:\LabFiles\HOL-1811\vcsa01b\".
2. Click on the file `vcsa01b.pem`.
3. Click on the Open button.
1. Click on the **Upload file...** button at the **bottom** of the pop-up window.
vcsa01b.pem

1. Browse to the path "C:\LabFiles\HOL-1811\vcsa01b".
2. Click on the file `vcsa01b.pem`.
3. Click on the **Open** button.
1. Click on the OK button.

**KMS Server Configured**

At this point we finished configuring the new KMS servers.
1. We see the newly added KMS server with the status is **Normal** and the Certificate Status is showing valid.

## Create an Encryption Policy

The next process for configuring for encryption would be to create and configure a new Encryption Storage Policy. The new encryption policy is configured like any other storage policy with the exception that we would select the encryption selection in the rule sets.

In order to create a new Storage Policy, we would click on the **Policies and Profiles** under the Home drop-down menu. However, in this lab, we will not be performing the actual steps to create a new encryption storage policy because one has been already created (VM Encryption Policy) to save time.

**NOTE:** To perform the actual steps of configuring a new encryption storage policy, please take **Module 4** of the **HOL-1811-04-SDC - vSphere 6.5 Security Concepts and Implementation** lab.

## Virtual Machine Encryption

Encryption of virtual machines is something that’s been on-going for years. But, in case you hadn’t noticed, it just hasn’t “taken off” because every solution has a negative operational impact. With vSphere 6.5 we are addressing that head on.
Encryption will be done in the hypervisor, “beneath” the virtual machine. As I/O comes out of the virtual disk controller in the virtual machine it is immediately encrypted by a module in the kernel before being sent to the kernel storage layer. Both virtual machine Home files (VMX, snapshot, etc) and VMDK files are encrypted.

The advantages here are numerous.

1. Because encryption happens at the hypervisor level and not in the virtual machine, the Guest OS and datastore type is not a factor. *Encryption of the VM is agnostic.*
2. Encryption is managed via policy. Application of the policy can be done to many virtual machines, **regardless of their Guest OS.**
3. Encryption is not managed “within” the virtual machine. *This is a key differentiation to every other solution in the market today!* There are no encryption “snowflakes”. You don’t have to monitor whether encryption is running in the virtual machine and the keys are not contained in the virtual machines memory.
4. Key Management is based on the industry standard, **KMIP 1.1.** In vSphere vCenter is a KMIP client and works with a large number of KMIP 1.1 key managers. This brings choice and flexibility to customers. Virtual machine Keys do not persist in vCenter.
5. Virtual machine Encryption makes use of the latest hardware advances inherent in the CPU’s today. It leverages **AES-NI** for encryption.
At this point we could test out a newly created encryption policy to enable encryption for a new virtual machine. So we will walk through the steps of creating a new virtual machine and then assign the encryption policy to it afterward.

1. Click on the **Home** Button.
2. Click on the **VMs and Templates**.

### New VM from This Template

1. **Right-click** on the **Tiny-VM** template.
2. Click on the **New VM from This Template** from the drop-down menu.
1. Type **My Encrypted VM1** in the Enter a name for the virtual machine text field.
2. Under the **vcsa-01b.corp.local** vCenter server, click on **RegionB01** for the location.
3. Then click on the **Next** button.
Select a compute resource

1. Select **RegionB01-COMP01** as your compute resource (it is the only choice).
2. Verify that we have the green check mark under Compatibility.
3. Click the Next button.
1. From the **Select virtual disk format** drop-down, select **Thin Provisioning**.
2. Then click on the **Next** button.
Select clone options

1. Keep the defaults and click on the **Next** button.
Ready to Complete

1. Click on the **Finish** button.

Edit VM Policies

1. **Right-click** on the **My Encrypted VM1** virtual machine.
2. Click on **VM Policies** from the drop-down menu.
3. Then click on **Edit VM Storage Policies...** from the VM Policies drop-down menu.

**Edit VM Storage Policies**

1. From the **VM storage policy** drop-down menu, select **VM Encryption Policy**.
2. Click on the **Apply to all** button to apply the policy to the VM home folder and Hard disk 1 of the virtual machine.
3. Then click on the **OK** button.
Verify Edit Settings

1. **Right-click** on the **My Encrypted VM1** virtual machine.
2. Then click on **Edit Settings** from the drop-down settings.
1. Once the Edit Settings pop-up opens, click on the arrow next to Hard disk 1 to expand it.
2. Verify that it has VM Encryption Policy selected for the VM storage policy setting.
Verify VM Options

1. Click on the **VM Options** tab.
2. Click on the **arrow** next to **Encryption** to expand it.
3. Verify that it has **Required** selected for the **Encrypted vMotion** setting.
4. Click on the **Cancel** button.

**NOTE**: We see that if the virtual machine is encrypted, then by default encrypted vMotion is Required and can't be changed manually as long as the virtual machine is encrypted.

**Encrypted vMotion Overview**

Encrypted vMotion has been an ask for a long time and with vSphere 6.5, we delivered it. What’s unique about vMotion encryption is that we are not encrypting the network. There are not certificates to manage or network settings to make. The encryption happens on a per-VM level, enabling vMotion encryption on a VM sets things in motion.
When the VM is migrated, a randomly generated, one time use 256-bit key is generated by vCenter (it does not use the key manager for this key).

In addition, a 64-bit “Nonce” (an arbitrary number used only once in a crypto operation) is also generated. The encryption key and Nonce are packaged into the migration specification sent to both hosts. At that point all the VM vMotion data is encrypted with both the key and the Nonce, ensuring that communications can’t be used to replay the data.

vMotion encryption can be set on unencrypted VM’s and is always enforced on encrypted VM’s. Next, we will walk through the steps to perform encrypted vMotion of an unencrypted virtual machine.

**Migrate a Virtual Machine**

Performing encrypted vMotion is no different than doing vMotion with an unencrypted virtual machine. We will run through the steps for encrypted vMotion of a virtual machine, however we won't actually initiate the vMotion to limit resource utilization in the Hands On Lab environment.

1. **Right-click** on the **w10-base-01b.corp.local** virtual machine.
2. Then select **Migrate** from the drop-down menu.

**NOTE:** We had to configure the KMS server on the **vcsa-01b.corp.local** vCenter Server since both KMS servers reside under it. However, we only have one ESXi host under that vCenter Server. This means we would not be able to vMotion the virtual machine because of there being only one ESXi host. So we will just go through the motions as
though we were performing an encrypted vMotion with a virtual machine under the vcsa-01b.corp.local vCenter server.

Select the migration type

We now select whether we want to move the virtual machine to another compute resource (Host), another storage location, or both.

1. Keep the default value of Change compute resource only.
2. Click the Next button.
Select a compute resource

Now we select the compute resource that we want to move the virtual machine to. Currently, we only have one ESXi host in the cluster, so we have to select the only host. If there were more than one ESXi host, we would select a host that the virtual machine was not already residing on. So again we are simulating this for lab purposes and to show you the process of performing the vMotion action.

1. Select the radius button next to **esx-01b.corp.local**.
2. Click on the **Next** button.

**NOTE:** We have the green check mark in the Compatibility field showing we can move the virtual machine to that host with no compatibility issue.
Select networks

We select the appropriate network that we want the virtual machine to be connected to, in this case we will select the default network.

1. Keep the default Designated Network and click on the Next button.

**NOTE:** We have the green check mark in the Compatibility field showing we can assign the default networking to the virtual machine with no compatibility issue.
At this point, we are ready to start the vMotion process. But first, it is always a good idea to take a close look at the summary of settings that was selected to be sure they are correct before starting the vMotion process. *We will NOT be actually doing the vMotion of the virtual machine to not burden the Hands On Labs environment.*

1. Click on the **Cancel** button so that we do not start the vMotion process.

**vSphere Security: Encrypted VMs & vMotion- Completed**

Congratulations on completing the **VM Encryption and Encrypted vMotion** overview!

Hopefully we have provided a good overview of vSphere 6.5 security features related to encryption. If you are looking for more detailed information on the new security features that we just covered, we recommend taking the **HOL-1811-04-SDC - vSphere 6.5 Security Concepts and Implementation lab**. This lab provides a deeper dive into all the vSphere 6.5 security enhancements.
Conclusion

Congratulations on completing the HOL-1811-01-SDC "What's New in vSphere 6.5" lab!

In this lab, we showed many of the new enhancements in vSphere 6.5. We learned about the improved vCenter Server Appliance management enhancements as well as the long awaited native capabilities of High Availability, Backup/Restore, and vSphere Update Manager within the vCenter Server Appliance. Then we reviewed the new Migration Tool that makes migrating from earlier versions (5.5.x or 6.0.x) of vSphere to vSphere 6.5 no matter if migrating from a Windows-based version or the vCenter Server Appliance. We walked through the new HTML5 versions of the Host Client and vSphere Web Client which showed how well the user interface performs. And finally, we discussed the new security features that offer the ability to have encrypted virtual machines as well as encrypted vMotion.

We sincerely hope this lab provided a beneficial overview of the core enhancements in the vSphere 6.5 release. Although we did not cover the vast amount of enhancements, we feel these were some of the core highlights to begin learning vSphere 6.5. If interested in getting a deeper understanding of the vSphere 6.5 security enhancements, the HOL-1811-04-SDC vSphere 6.5: Security Concepts and Implementation lab. We also have the HOL-1811-02-SDC Getting Started with vSphere with Operations Management lab that also covers several topics on vSphere 6.5 as well.

We have also provided some vSphere 6.5 resources in the Additional Resources section to assist in providing more details on the new enhancements in vSphere 6.5.

Additional Resources

If you are looking for additional information on What's New in vSphere 6.5, see the below links:

- Feature Walkthrough - vSphere 6.5 - https://featurewalkthrough.vmware.com/#!/vsphere-6-5
- VMware vSphere Blog Site - https://blogs.vmware.com/vsphere/
- VMware vSphere YouTube Channel - https://www.youtube.com/channel/UCN8FHFshMw-15AtFKWSLczA
OPTIONAL: How to End the Lab

NOTE: Understand that when you click the END button in the lab, it will close out the lab and delete the associated virtual machines. This means when the lab is re-launched, it will create a new lab instance with new virtual machines, not the ones used previously. Any and all previous settings will be lost and they will be back to the default settings from when the lab is first deployed.

If you fully understand the warning note above and you want to end your lab:

1. To end your lab click on the END button.
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-1811-01-SDC

Version: 20180425-080214