vembu

VMware vSphere 6.7 Update 1 Upgrade and Security Configuration

Brandon Lee

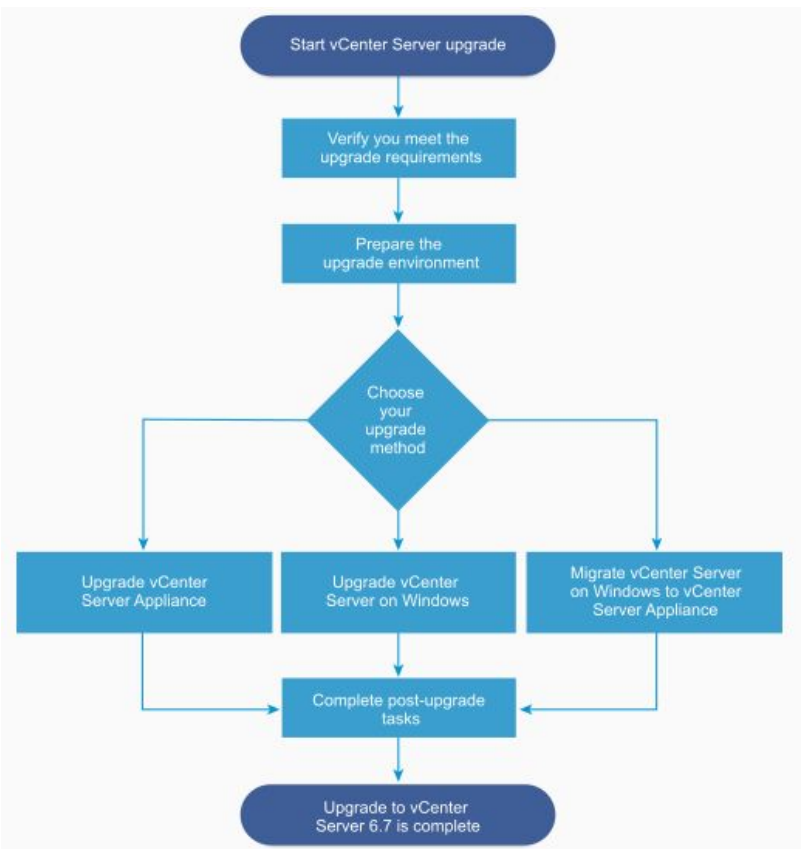
Author

Brandon Lee has been in the IT industry for over 15+ years now and has worked in various IT industries spanning education, manufacturing, hospitality, and consulting for various technology companies including Fortune 500 companies. He is a prolific blogger and contributes to the community through various blog posts and technical documentation primarily at Virtualizationhowto.com

VMware vSphere 6.7 Update 1 Upgrade and Security Configuration

1. Upgrading to VMware vSphere 6.7 Update 1 Overview
    a. Other Upgrade Considerations Before Upgrading vSphere
    b. Upgrade Process Order Overview
2. Upgrading VCSA Appliance to vCenter Server 6.7 Update 1
    a. VMware vSphere vCenter Server VCSA 6.7 Update 1 Upgrade Stage 2
3. Upgrading VMware ESXi to vSphere 6.7 Update 1
4. Implementing VMware vSphere Virtual Machine Encryption
    a. How to Enable VMware Virtual Machine Encryption
5. Virtualization-based Security Best Practices
    a. Enabling Virtualization-Based Security in VMware vSphere
6. VMware vSphere Virtual Trusted Platform Module or vTPM
    a. Differences between a Physical TPM and a Virtual TPM
    b. Adding the Virtual TPM Module to a Virtual Machine
7. What is the Virtual Networking Layer?
    a. Securing VMware vSphere Virtual Networking Layer
    b. Isolate Network Traffic
    c. Use Firewalls to Secure Virtual Network Elements
    d. Consider Network Security Policies
    e. Secure VM Networking
    f. Use VLANs to Protect Virtual Networks
    g. Secure Virtual Storage Network Traffic
    h. Use IPSec when Possible
8. Securing VMware vSphere 6.7 Update 1 Virtual machine Best Practices
    a. General Virtual Machine Protection
    b. Deploying VMs using Templates
    c. Securing the VM Console in vSphere
    d. Limiting VM Resource Usage
    e. Disabling unnecessary VM Functions
    f. Use Virtualization-Based Security and vTPM 2.0
9. White paper Takeaways

- If you are using an external Platform Services Controller, upgrade Platform Services Controller appliance 6.0 to version 6.7.
- Upgrade the vCenter Server to vSphere 6.7 Update 1 – This is an extremely important step as it allows choosing a supported upgrade method, depending on the version you are coming from.
    - You must first ensure your current deployment supports upgrading or migrating to the vCenter Server 6.7 Update 1 deployment.
    - Use the Graphical Deployment Tool – This allows upgrading vCenter Server by means of a two-step process to first deploy the new VCSA appliance as an OVA and then copying the existing data to the new appliance which then assumes the identity.
    - Use the Migration Assistant Interface – This allows migrating from the legacy SSO Platform Services Controller, or vCenter Server on Windows to the VCSA appliance.
    - Use the CLI installer – This allows advanced users the means to upgrade VCSA appliances or vCenter Server on Windows to the latest version.
    - Using the vCenter Admin VAMI interface – This is the administrative interface in VCSA that allows patching the appliance to the latest version within the major release.



High-level overview of the vCenter Server Upgrade Process (Image Courtesy of VMware)

- Upgrade your ESXi hosts – Upgrading the ESXi hypervisor on cluster hosts comes after upgrading the vCenter Server. The vCenter Server must be at the same level or higher than the ESXi hosts it manages. Typically, customers want to keep the version of ESXi in sync with the version of vCenter. However, it is worth mentioning that the latest vCenter Server 6.7 Update 1 supports managing down level ESXi hosts.
    - As shown below, vCenter Server 6.7 Update 1 supports managing ESXi hosts all the way back to version 6.0. There may be reasons a customer might choose to do this. By using the latest vCenter Server version, you have the latest HTML5 interface and all the other nice features that the new VCSA brings to the table. However, VMware has deprecated support in ESXi for legacy Windows Server versions such as 2003 starting in vSphere 6.7. If a customer is running legacy Windows Server operating systems, this might be a reason to run the latest vCenter with a down level ESXi host version.

VMware vCenter Server	6.7 U1
VMware vSphere Hypervisor (ESXi)	
6.7 U1	✓
6.7.0	✓
6.5 U2	✓
6.5 U1	✓
6.5.0	✓
6.0 U3	✓
6.0.0 U2	✓
6.0.0 U1	✓
6.0.0	✓

VMware Product Interoperability Matrix

- Upgrade Virtual Machine VMware Tools – While VMware has decoupled the VMware Tools releases from the vSphere version itself, new vSphere versions generally come with an updated version of VMware Tools if you choose this option for the ESXi hypervisor download. After upgrading your vCenter Server and ESXi hosts, you will want to roll through the virtual machines and upgrade VMware tools. This can be done manually in vSphere or can easily be done programmatically with PowerCLI.
- Upgrade Virtual Machine compatibility – This is a step that is certainly not required, however, if there are new virtual hardware features or other configuration that a new vSphere version unlocks that you want to take advantage of, you will want to upgrade your virtual hardware compatibility.

By following the steps above, upgrading vSphere environments to the latest versions including vSphere 6.7 Update 1 can be performed smoothly and effectively. What are some other considerations to make?

Other Upgrade Considerations Before Upgrading vSphere

Are there any other considerations to make before upgrading vSphere? Yes, there are. Another extremely important consideration to make before upgrading vSphere versions is to make sure your backup solution of choice supports the vSphere version. It would be extremely frustrating and dangerous for your organization's data to be able to successfully upgrade vSphere to the latest version but find that your data protection solution starts failing to backup, replicate or perform other operations with vSphere. Why do new versions often break backups?

Data protection solutions rely on being able to interact with the backup APIs that are found in vSphere. With new versions and releases, VMware at times either changes the way the API works or changes the API altogether. Once the upgrade happens, if the data protection solution is not engineered to be able to deal with the new APIs, jobs will generally start failing with miscellaneous errors. So, it is key to ensure compatibility up front with data protection solutions to make sure they are compatible with the version you are upgrading to, such as vSphere 6.7 Update 1.

Along the lines of what we have discussed with the data protection solutions interacting with vCenter Server, count on the downtime required for vCenter Server depending on the version you are coming from. Patching vCenter from the VAMI will not take as long as the Upgrade process takes with the GUI tool 2-step process. If you have monitoring solutions or other third-party products that integrate with vCenter Server, expect the downtime required for these solutions as well while vCenter is undergoing the upgrade. While the VMs themselves will still be available, make sure you can withstand the time "flying blind" if you rely on monitoring solutions with hooks into vCenter.

VMware vSphere 6.7 Update 1 Upgrade and Security Configuration

1. Upgrading to VMware vSphere 6.7 Update 1 Overview
    a. Other Upgrade Considerations Before Upgrading vSphere
    b. Upgrade Process Order Overview
2. Upgrading VCSA Appliance to vCenter Server 6.7 Update 1
    a. VMware vSphere vCenter Server VCSA 6.7 Update 1 Upgrade Stage 2
3. Upgrading VMware ESXi to vSphere 6.7 Update 1
4. Implementing VMware vSphere Virtual Machine Encryption
    a. How to Enable VMware Virtual Machine Encryption
5. Virtualization-based Security Best Practices
    a. Enabling Virtualization-Based Security in VMware vSphere
6. VMware vSphere Virtual Trusted Platform Module or vTPM
    a. Differences between a Physical TPM and a Virtual TPM
    b. Adding the Virtual TPM Module to a Virtual Machine
7. What is the Virtual Networking Layer?
    a. Securing VMware vSphere Virtual Networking Layer
    b. Isolate Network Traffic
    c. Use Firewalls to Secure Virtual Network Elements
    d. Consider Network Security Policies
    e. Secure VM Networking
    f. Use VLANs to Protect Virtual Networks
    g. Secure Virtual Storage Network Traffic
    h. Use IPSec when Possible
8. Securing VMware vSphere 6.7 Update 1 Virtual machine Best Practices
    a. General Virtual Machine Protection
    b. Deploying VMs using Templates
    c. Securing the VM Console in vSphere
    d. Limiting VM Resource Usage
    e. Disabling unnecessary VM Functions
    f. Use Virtualization-Based Security and vTPM 2.0
9. White paper Takeaways

Upgrade Process Order Overview

As covered already, there are certainly things to consider with an upgrade of VMware vSphere. How is an upgrade of vSphere carried out? When thinking about an upgrade vSphere environment, customers need to follow an order of operations in upgrading the vSphere environment. What is the order of operations when upgrading? Below is a quick listing of native VMware solutions and the order of upgrading to vSphere 6.7, found in the VMware KB article 53710. Be sure when upgrading your environment to take an inventory of all VMware solutions that are integrated into the vSphere environment along with all third-party solutions that are reliant upon connections to vSphere. Be sure to check with those third-party providers for their relevant compatibility and interoperability matrices.

1. vRealize Automation
2. vRealize Orchestrator
3. vRealize Business for Cloud
4. vRealize Operations Manager
5. vRealize Log Insight
6. vRealize Log Insight Agent
7. vRealize Operations Endpoint Agents
8. vADP-based Backup Solution
9. NSX-v
10. External PSC
11. vCenter Server
12. VUM
13. vSphere Replication
14. vSphere Site Recovery Manager
15. vSphere Update Manager Download Service
16. ESXi hypervisor
17. VMware Tools
18. Virtual Hardware
19. vSAN/VMFS

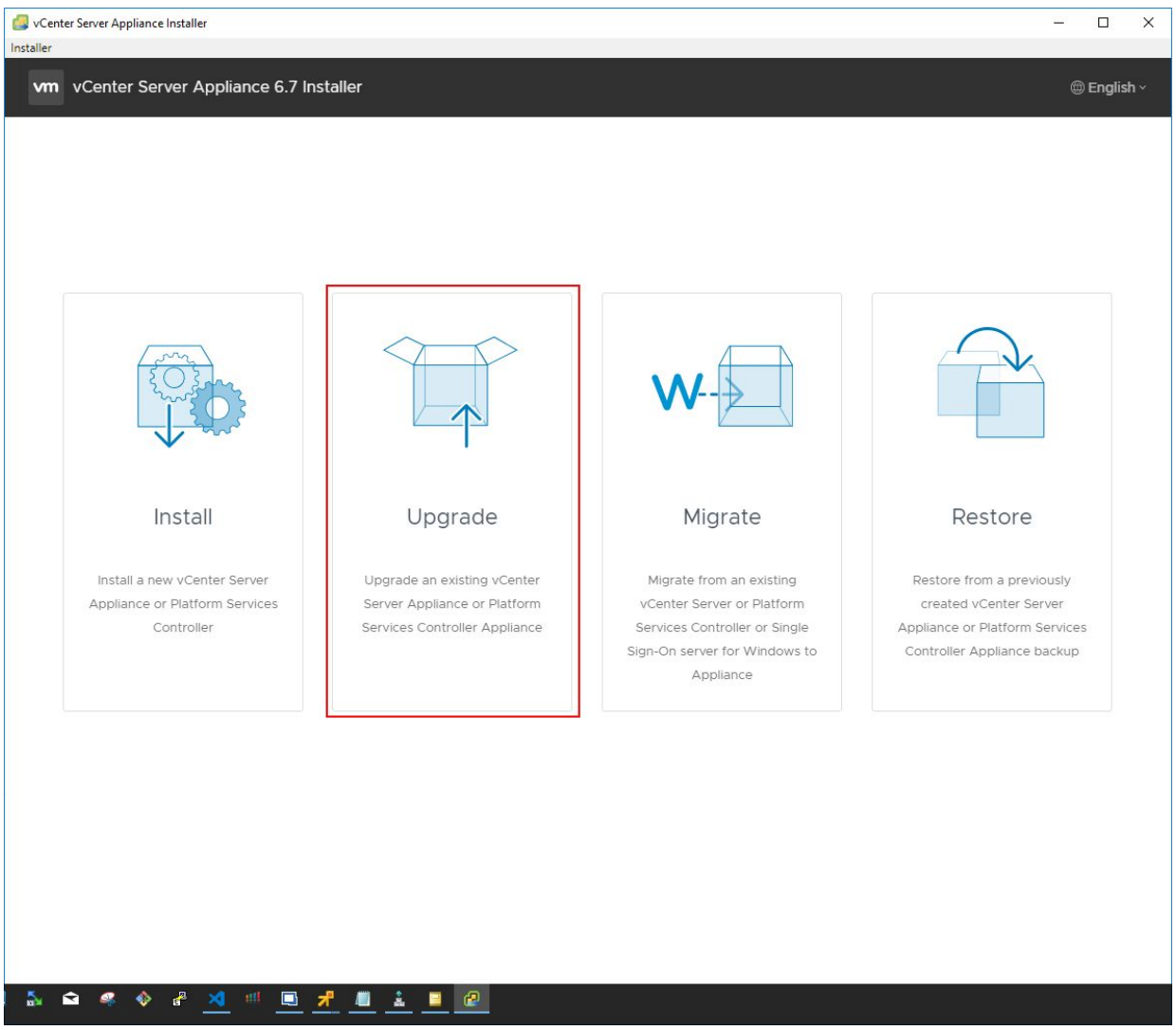
In the following walkthrough, let's take a look at upgrading a simple vSphere environment that only consists of vCenter Server and a cluster of ESXi hosts. In the above list, we have highlighted the vCenter Server and ESXi hypervisor in the list above. As you can see, these both sit in various places in the recommended order of operations from an overall VMware products standpoint. If you have any of the other solutions, you will need to look and see where it fits in the overall order of upgrade operations set forth by VMware.

When looking at a simple configuration of only vCenter Server and the ESXi hosts in the cluster, the process to upgrade the vSphere components in that configuration involves upgrading vCenter Server first, and then upgrading the ESXi hosts. In the following walkthrough, let's upgrade an existing vCenter 6.5 U2 VCSA installation to vCenter 6.7 Update 1 VCSA. The process is the same as the one established with the VCSA 6.5 upgrade process. The ISO installer that is downloaded contains the GUI installer/upgrade utility that allows deploying, upgrading, migrating from Windows vCenter, or restoring an installation.

When upgrading, the process involves deploying a **new** vCenter Server VCSA 6.7 Update 1 appliance and then copying the configuration and data from the upgrade source VCSA appliance over to the new appliance. The new appliance then assumes the identity of the source appliance and the old VCSA appliance is powered off.

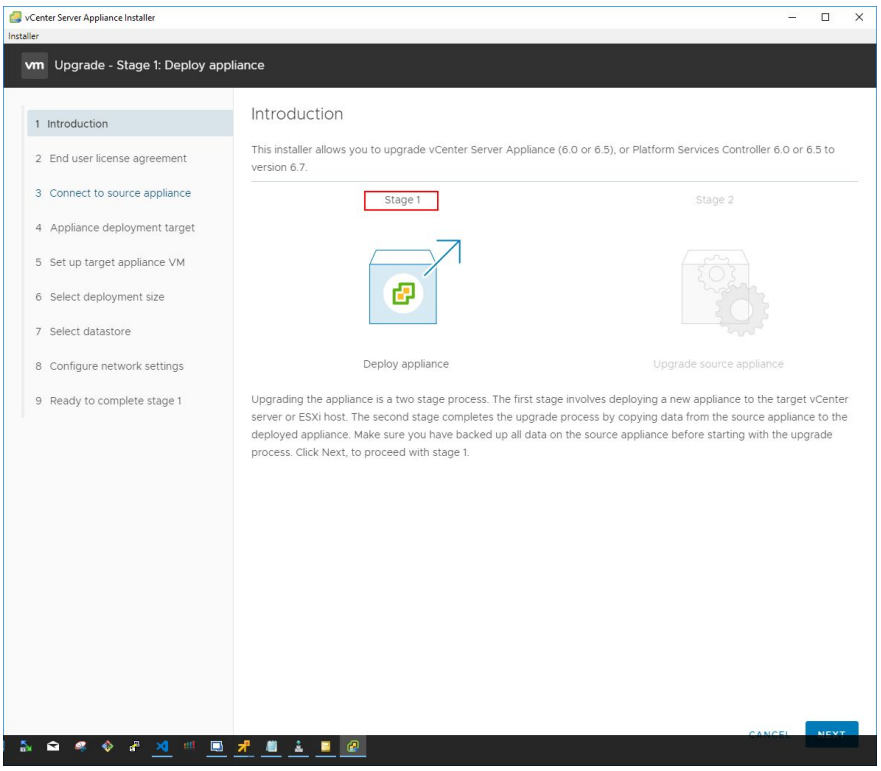
Upgrading VCSA Appliance to vCenter Server 6.7 Update 1

After downloading the new version of vCenter, which is downloadable from VMware as an ISO file, you simply mount the ISO and run the UI installer. This launches the utility that allows you to choose the operation you want to perform.



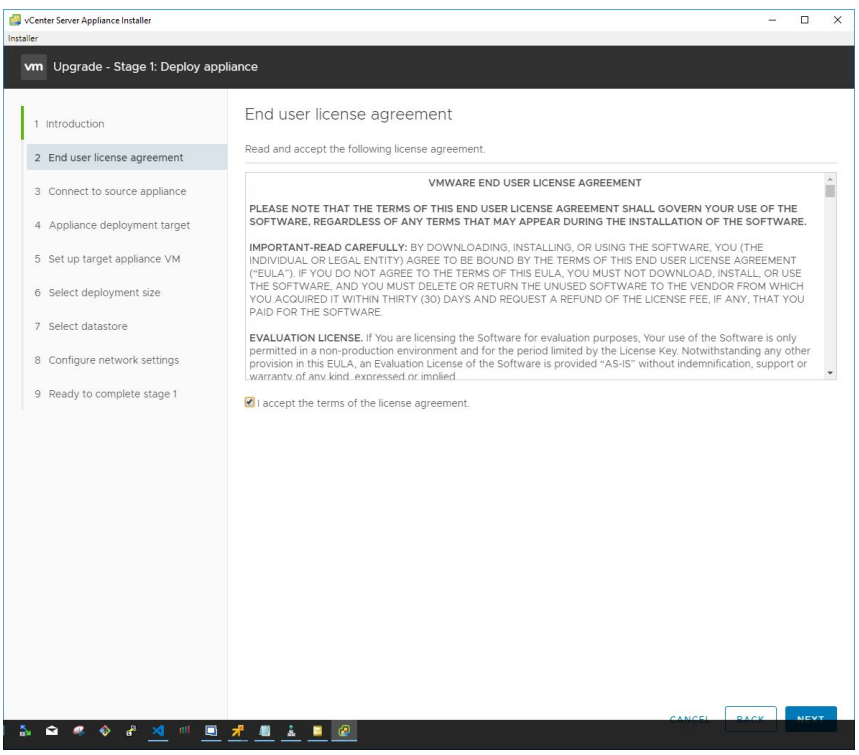
vCenter Server Appliance 6.7 Installer – Upgrade options

The installer will happen in 2 stages. The first stage is to **deploy** the appliance. The introductory screen describes the process in detail and the various steps taken in each stage.



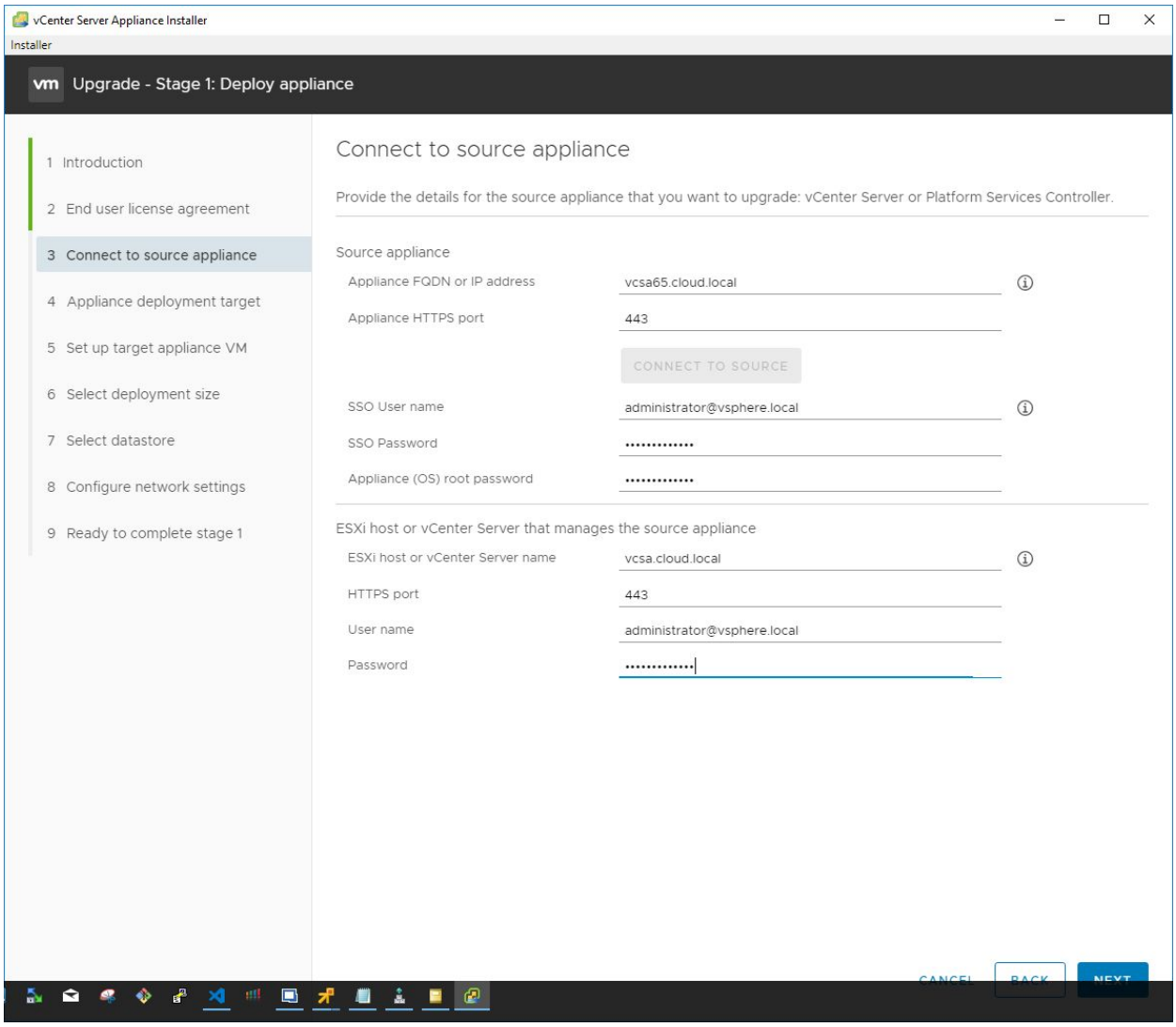
Deploying the vSphere 6.7 Update 1 appliance

Next, accept the EULA presented for the installer.



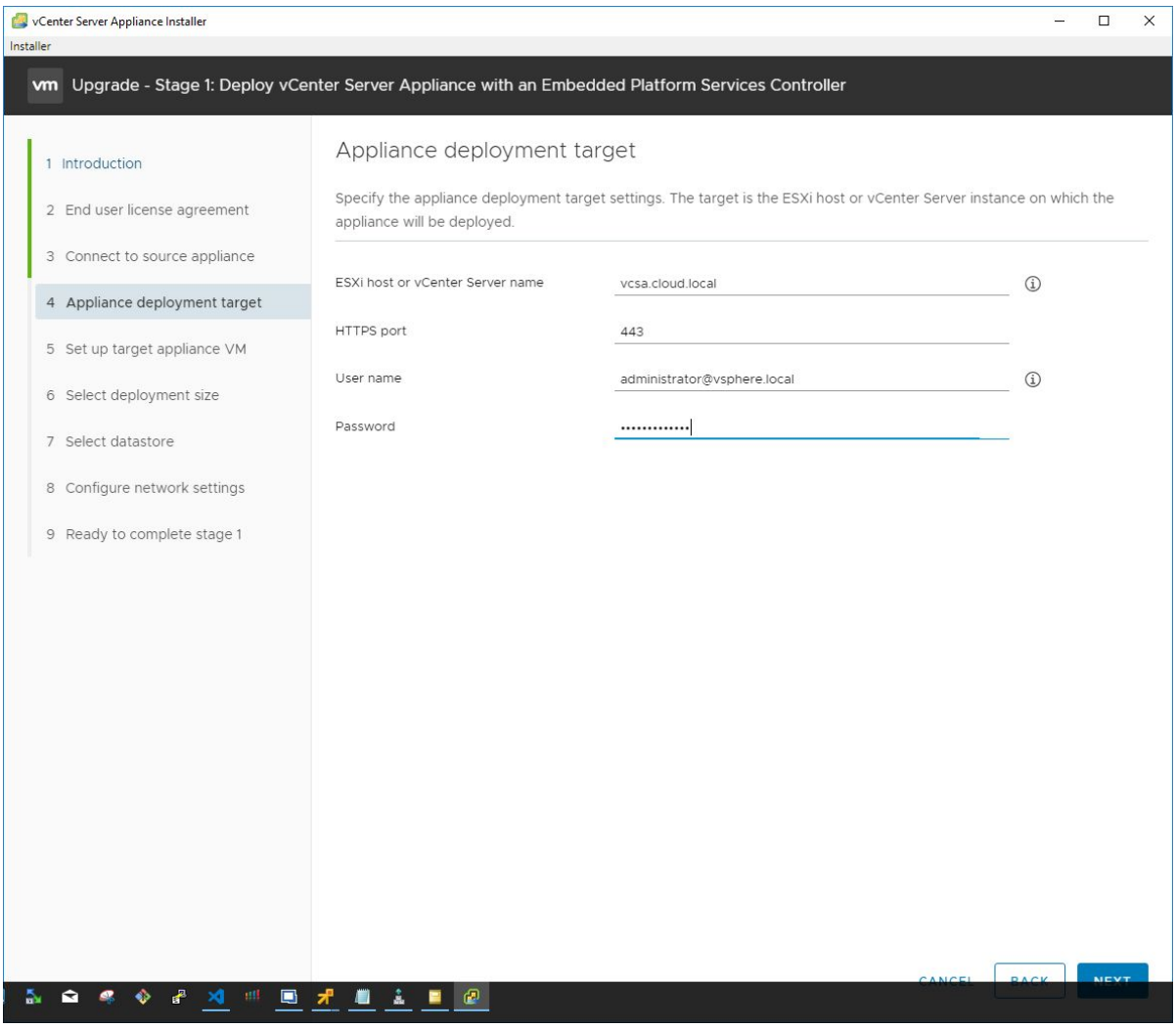
Accept the EULA for the vSphere 6.7 Update 1 upgrade

Now, we connect to the source appliance by providing the credentials for connectivity. Additionally, you connect to the source ESXi host or vCenter Server that manages the source appliance.



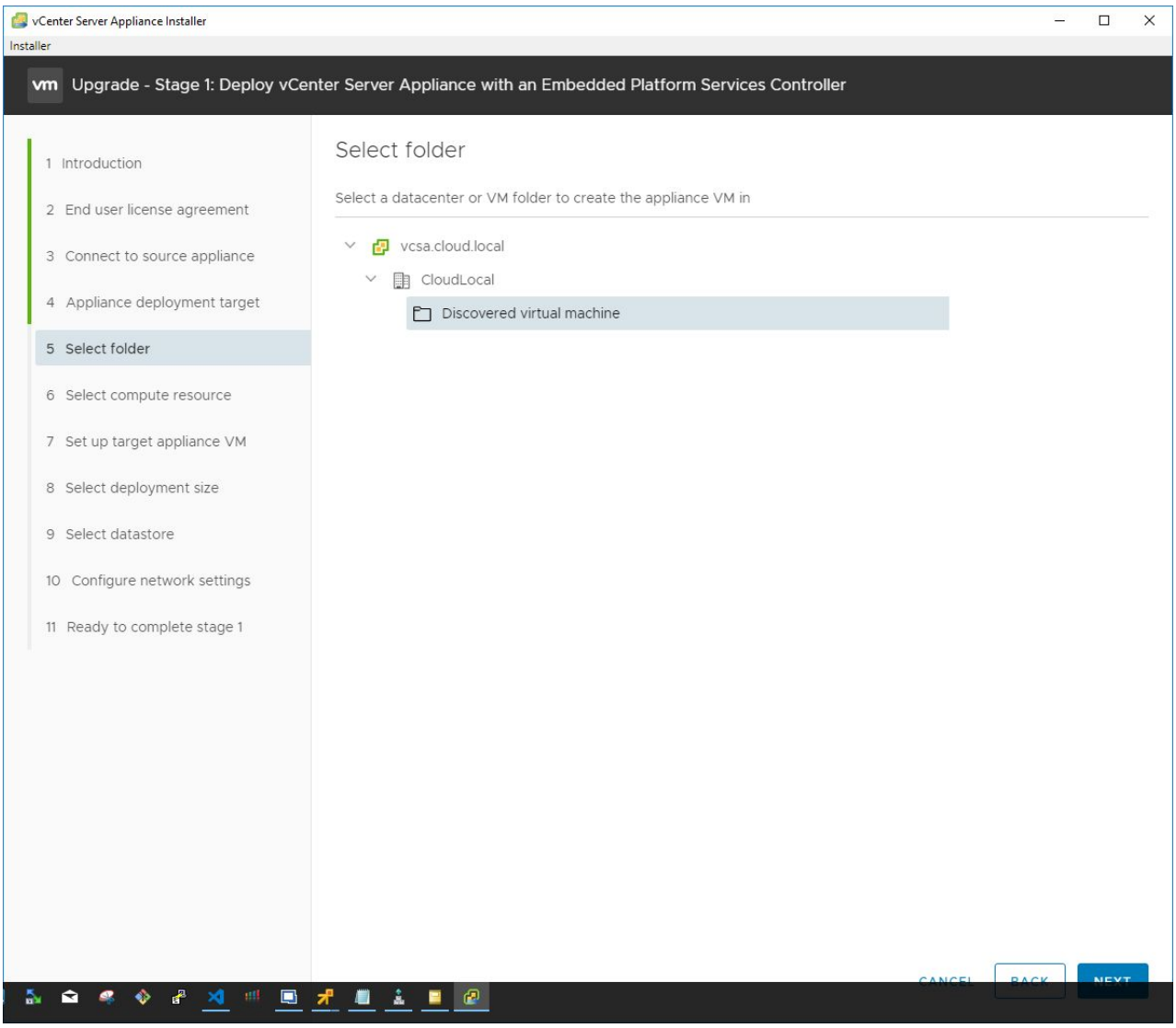
Connect to the source appliance using the installer

Next, connect to the appliance deployment target by providing the hostname and the credentials. This allows the installer to create the new appliance.



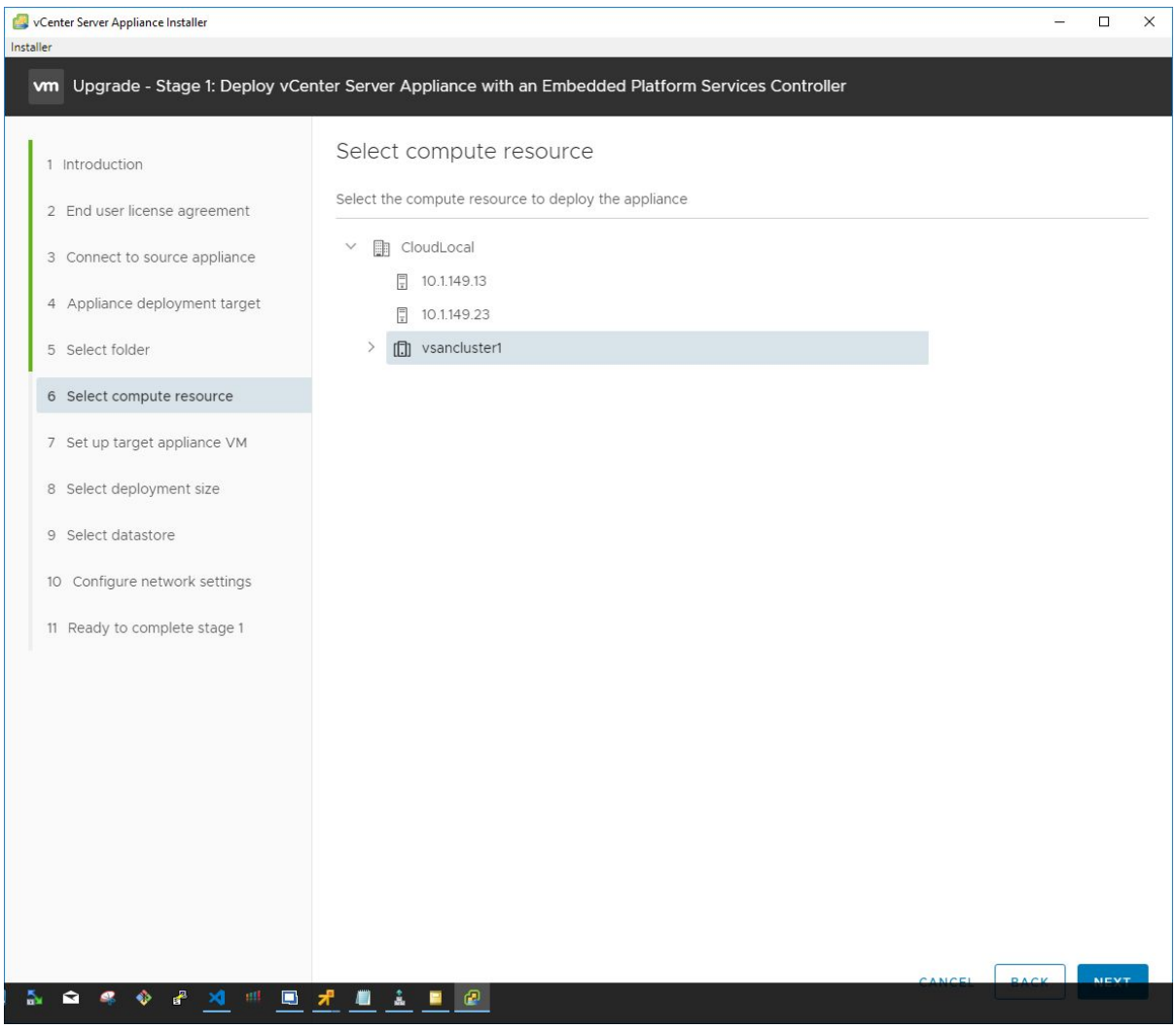
Connect to the appliance deployment target so the new appliance virtual machine can be created and managed

Select the folder for the new appliance creation in the target vSphere infrastructure.



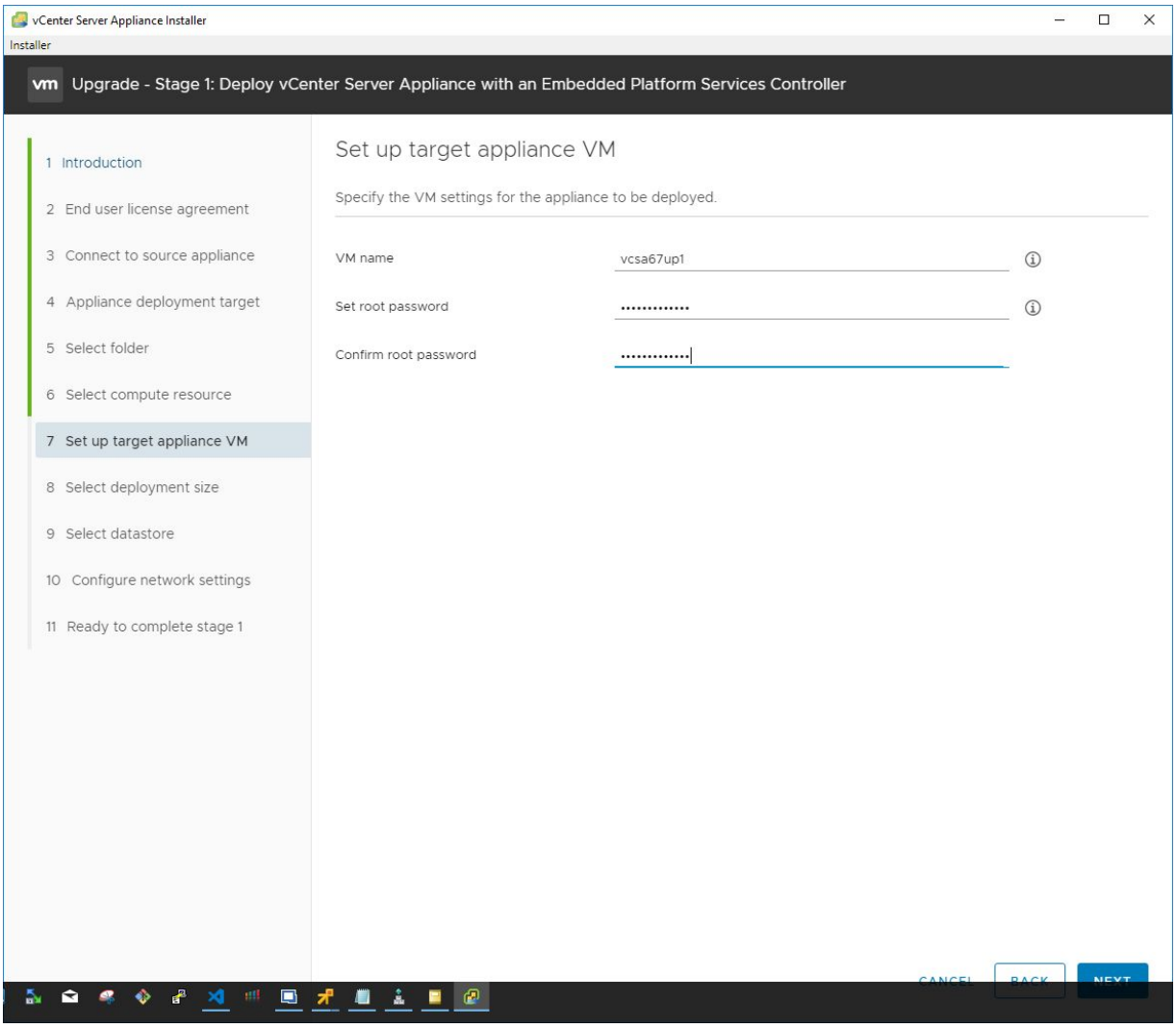
Select the vSphere folder where the new appliance will be created

Select the compute resource such as a standalone host or vSphere cluster to house the new vCenter Server Appliance.



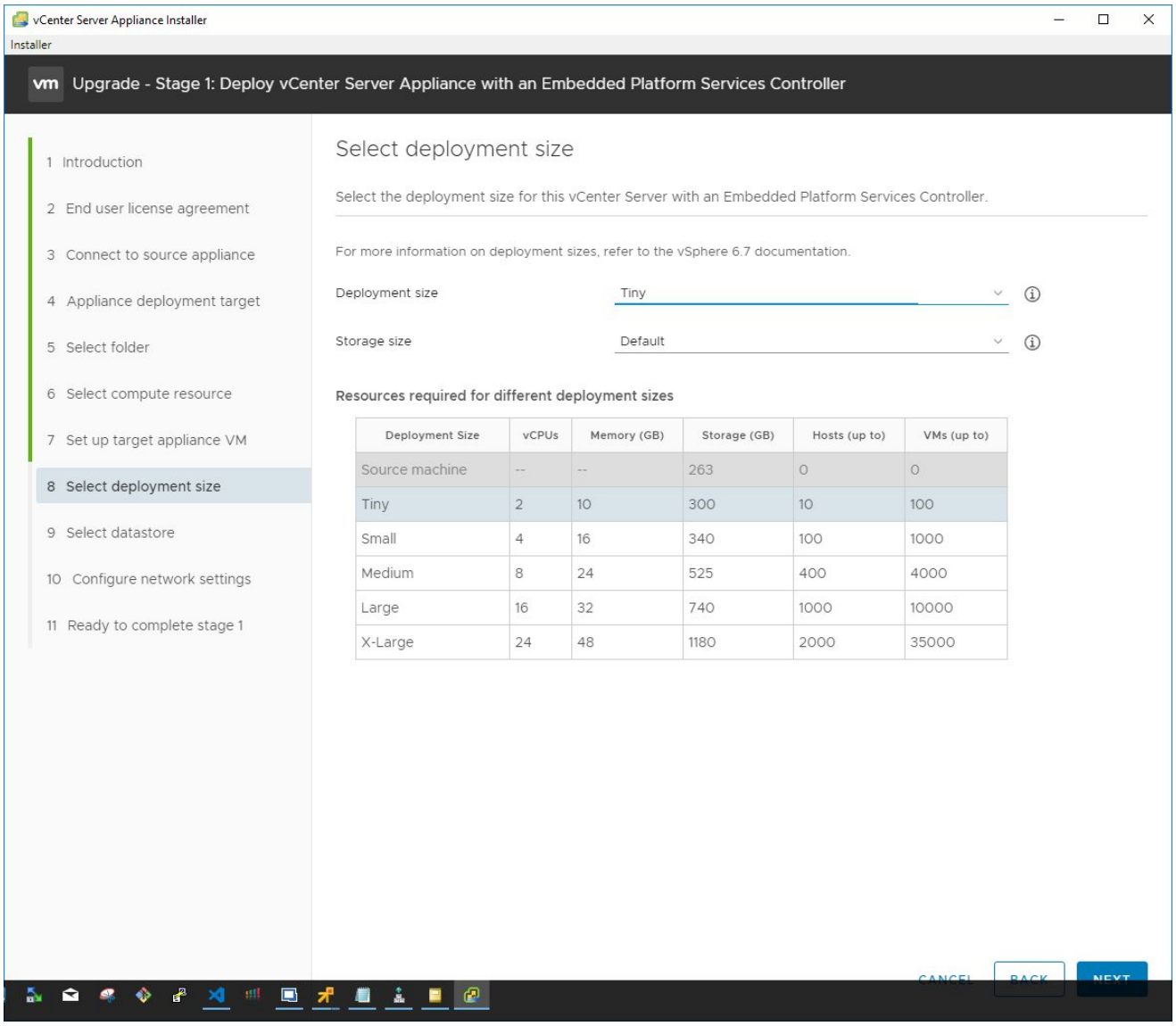
Selecting the compute resource to house the resulting appliance that is created

After configuring the vSphere connection to the target environment, you are asked to set up the target appliance virtual machine by providing a name, root password and confirming the root password.



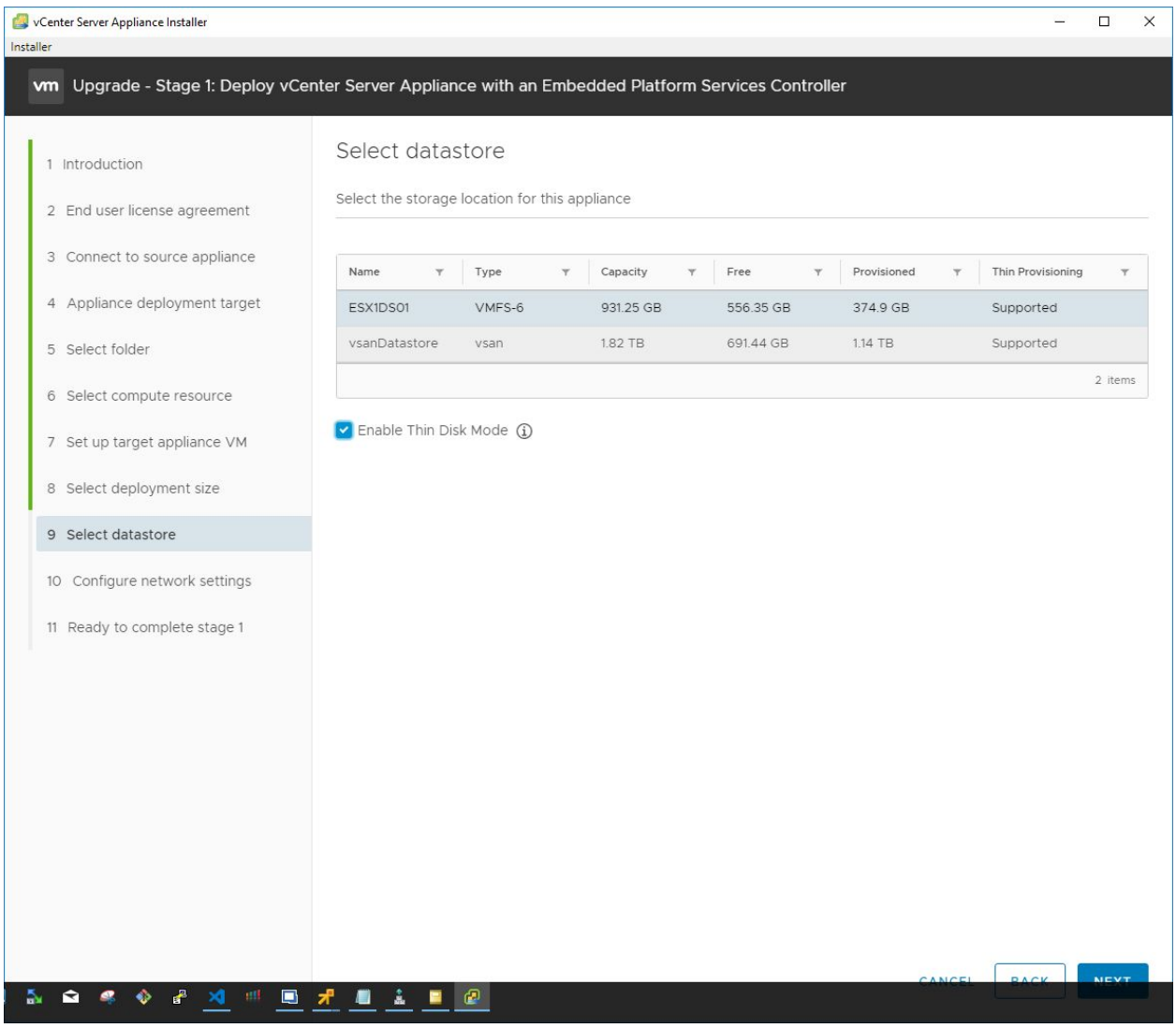
Setup the target appliance VM

Configure the deployment size for the resulting VCSA appliance. The installer provides great information right on the installer GUI configuration page for the deployment size options.



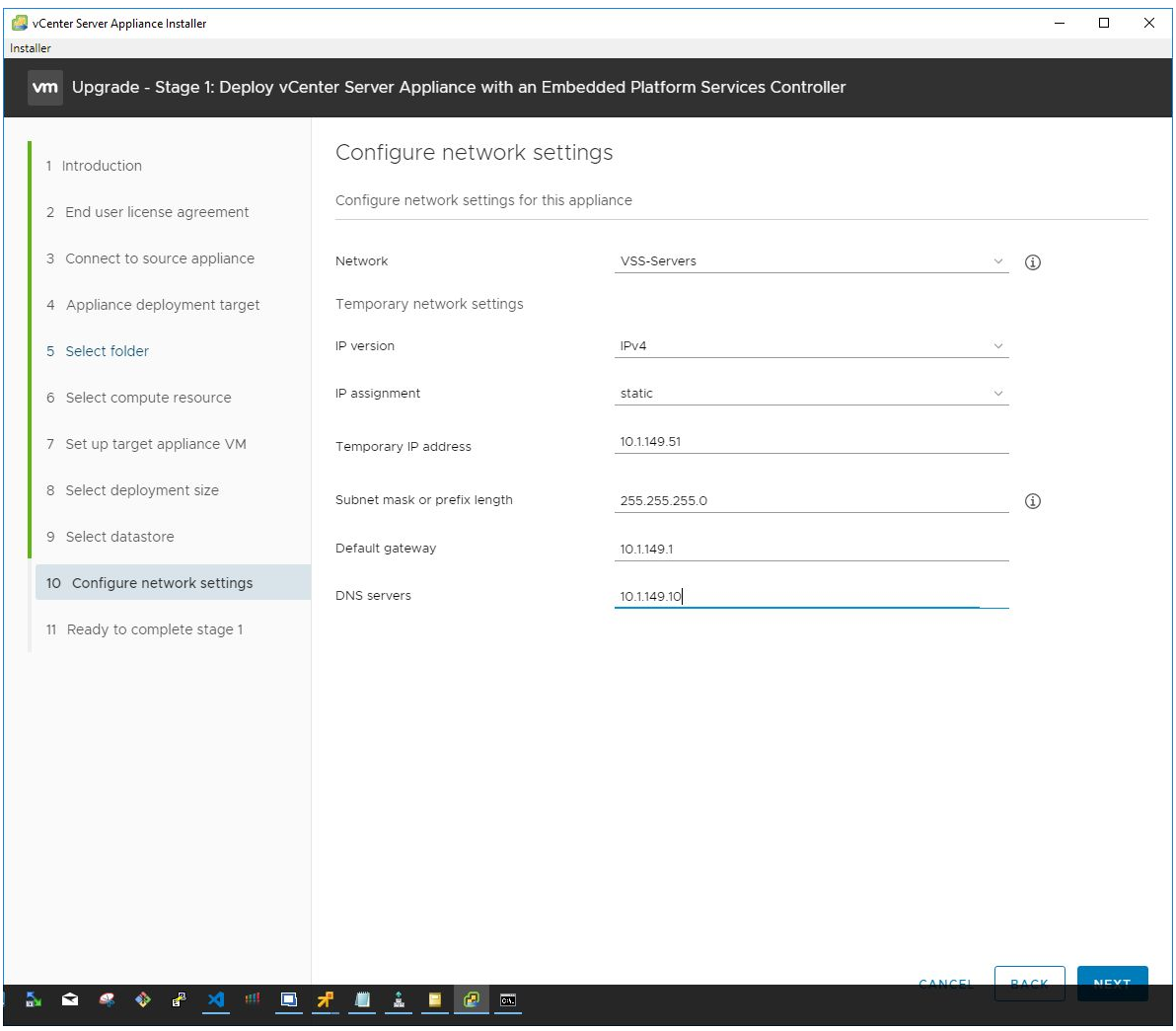
Select the deployment size for the resulting VCSA appliance

Select the datastore the new VCSA appliance will be housed in. You also have the option to select the Enable Thin Disk Mode which thin provisions the resulting VCSA appliance disks on the datastore. This means that blocks are only zeroed out when they are written to. This saves a tremendous amount of space since space is only claimed on the datastore as the blocks are written to.



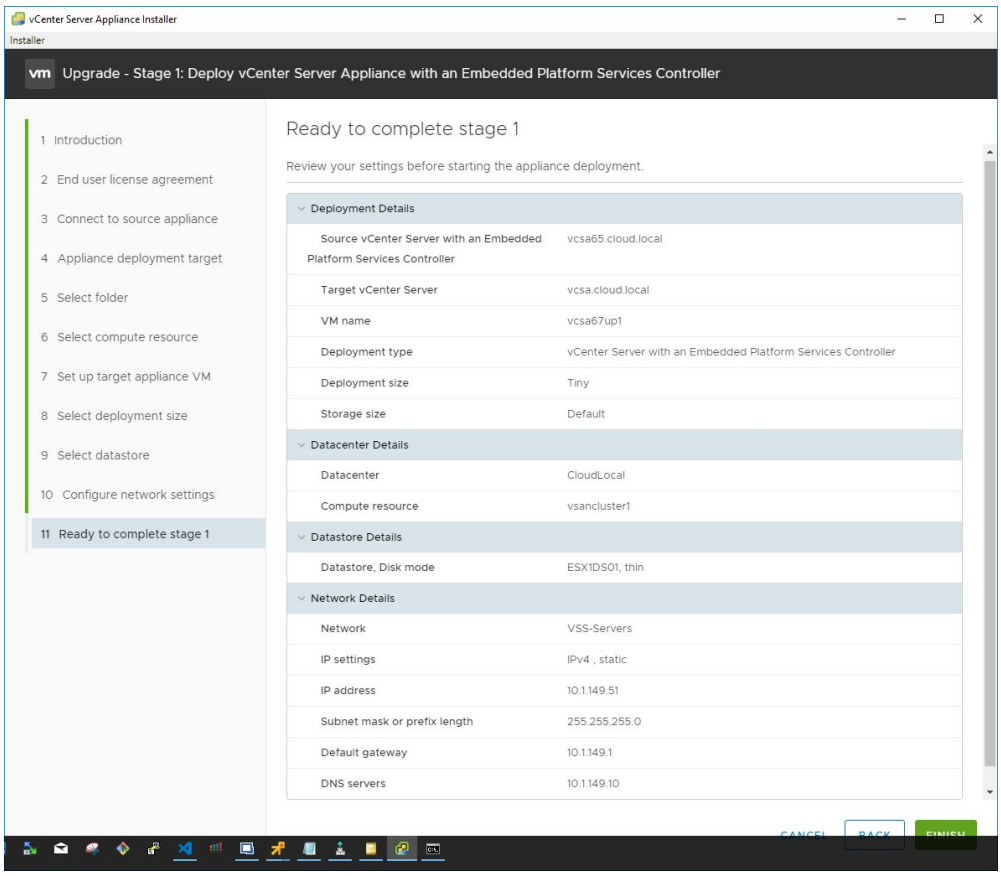
Selecting the target datastore for the resulting VCSA appliance and choosing thin disk mode options

On the network settings configuration, choose the port group to attach the resulting VCSA appliance to as well as the **temporary IP address** for the appliance. Keep in mind that ultimately, the installer is going to assume the IP address of the source appliance. So here, we are simply giving it an IP address that will allow it to communicate with the source appliance during the upgrade process to copy data across.



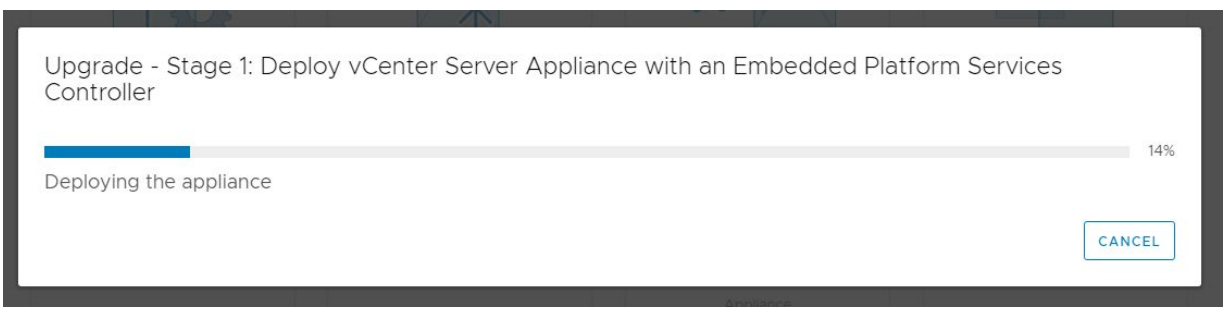
Configuring network settings for the new VCSA appliance

The Stage 1 process is now ready to begin the actual configuration of the VCSA appliance in line with the parameters configured during the wizard. Click Finish.



The configuration is ready to begin using the parameters chosen for the new VCSA appliance

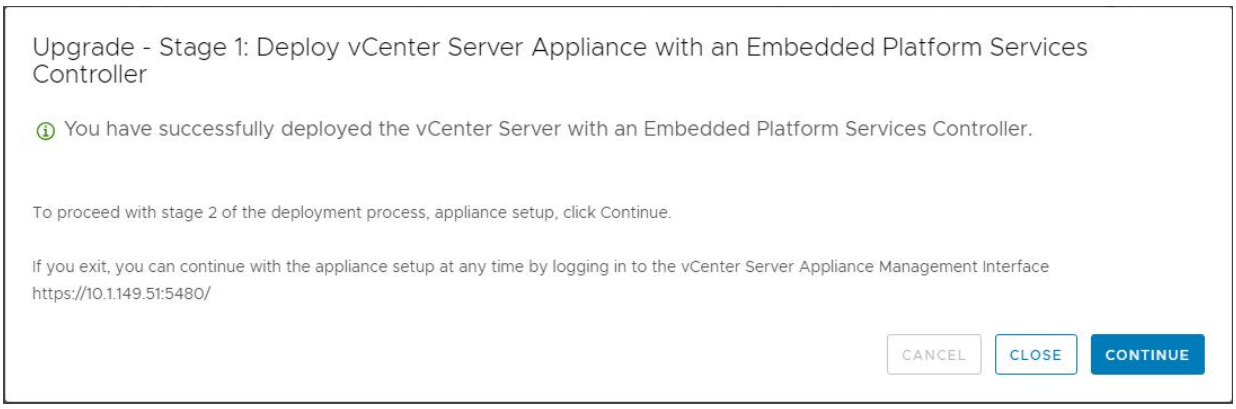
Stage 1 – Deploy vCenter Server Appliance with an Embedded Platform Services Controller begins. The new appliance VM is deployed into the vSphere inventory.



VMware vSphere 6.7 Update 1 VCSA appliance deployment begins

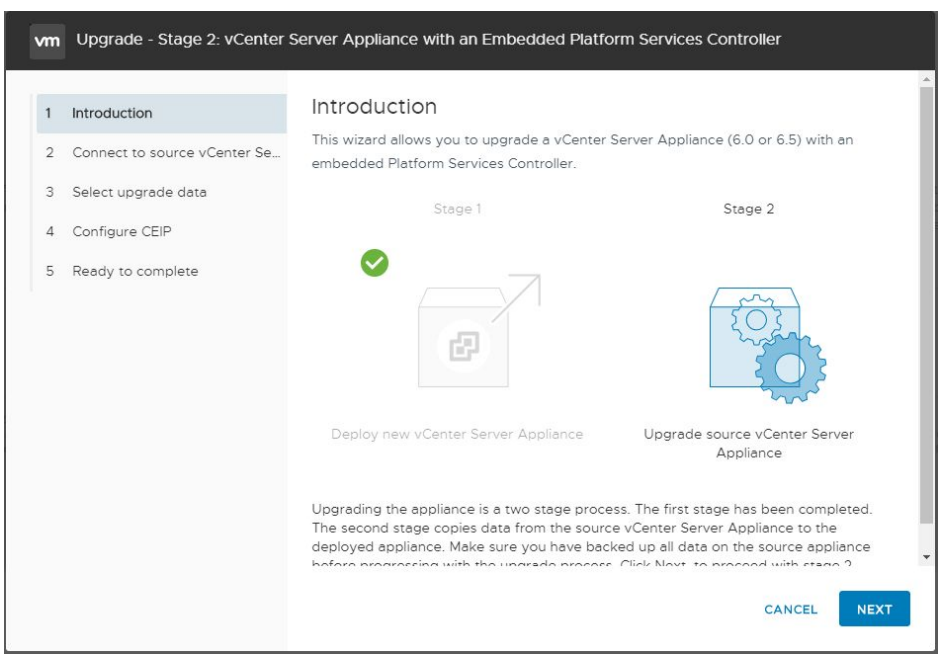
Stage 1 of the deployment finishes. Stage 2 begins.

VMware vSphere vCenter Server VCSA 6.7 Update 1 Upgrade Stage 2



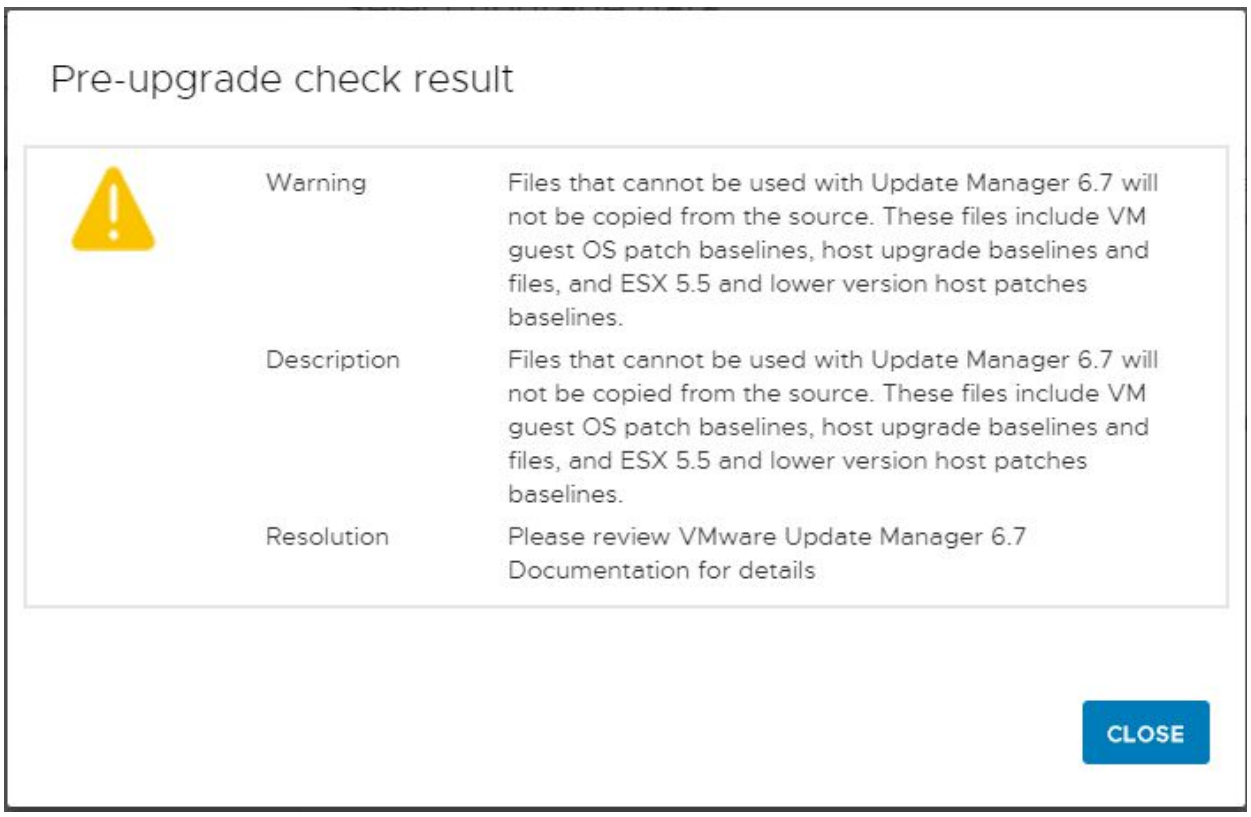
Stage 2 of the vSphere 6.7 Update 1 VCSA upgrade begins

In Stage 2, the installer copies data from the source vCenter Server Appliance to the deployed appliance. In the introduction screen, the process details are displayed.



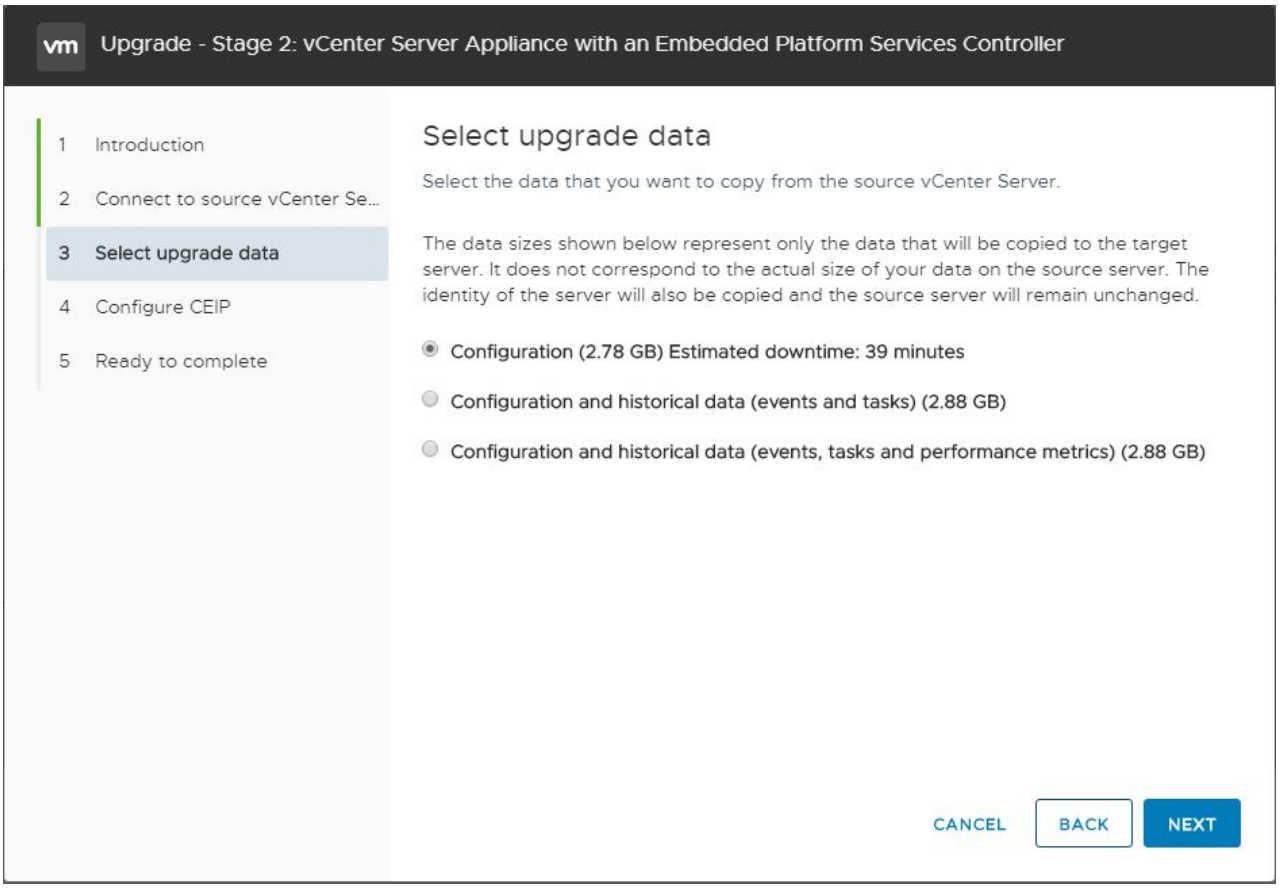
Overview of Stage 2 in the vSphere 6.7 Update 1 upgrade process

The Pre-upgrade check result will display any warning or other errors that are found. Below, we have warnings about legacy patch baselines, etc.



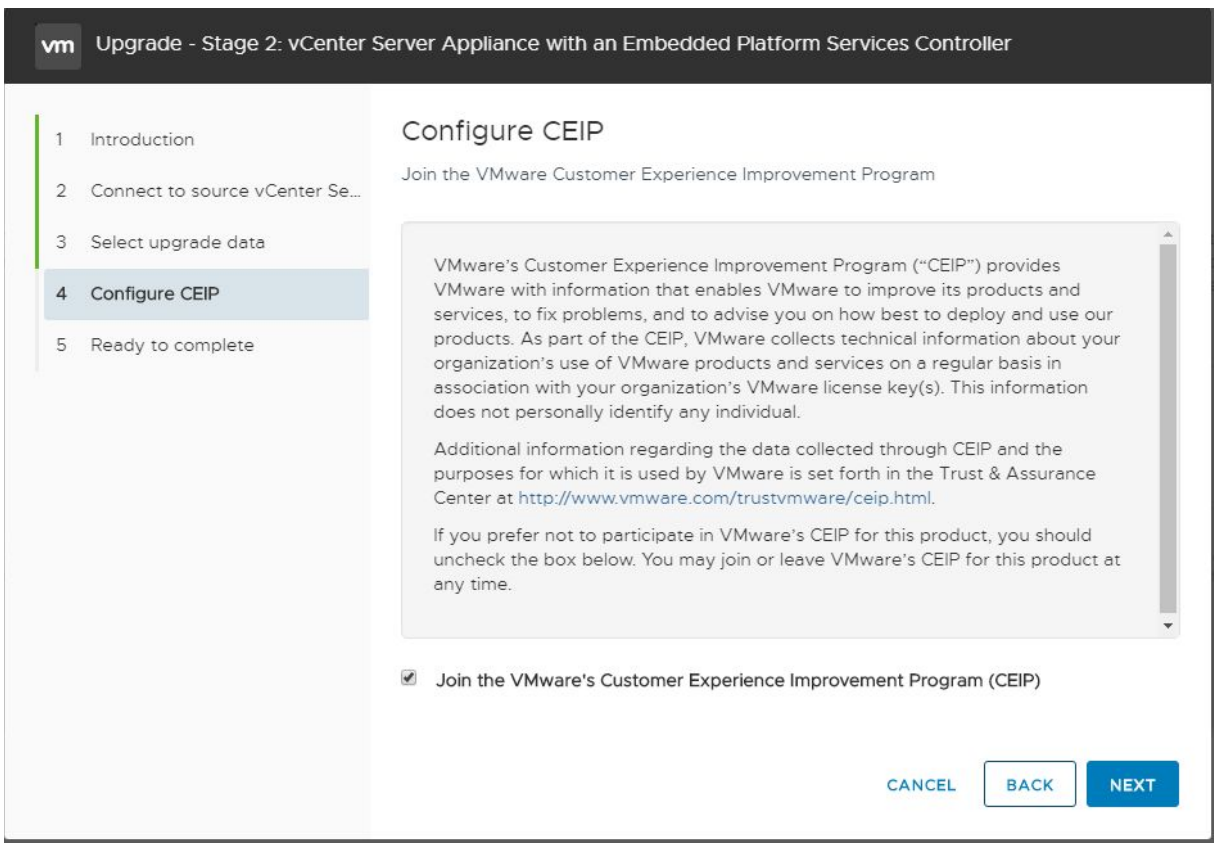
Pre-upgrade check warnings displayed before the deployment of the new appliance begins

After connecting to the source vCenter Server, the Select Upgrade data screen displays. Here you can choose which data is copied to the new appliance. The various data sizes are displayed for each option.



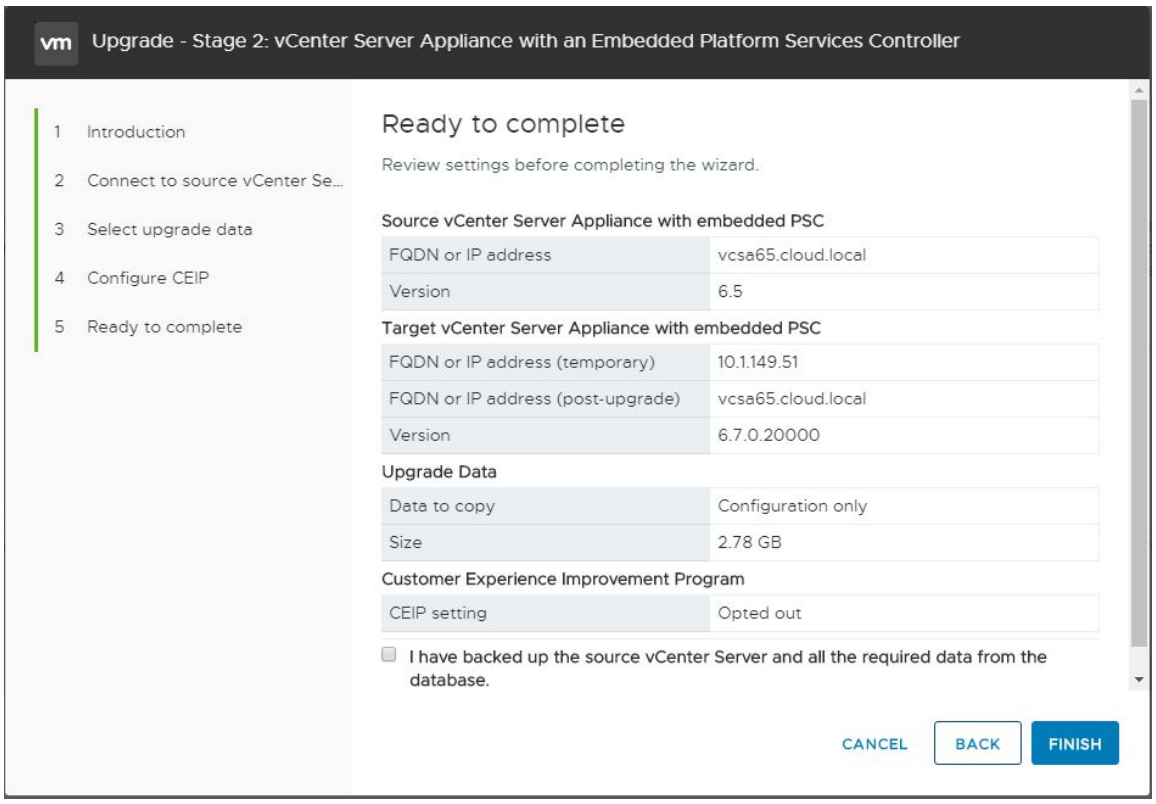
Choose the upgrade data option during the vSphere 6.7 Update 1 upgrade process

Next, choose whether or not to participate in the CEIP program by checking or unchecking the box.



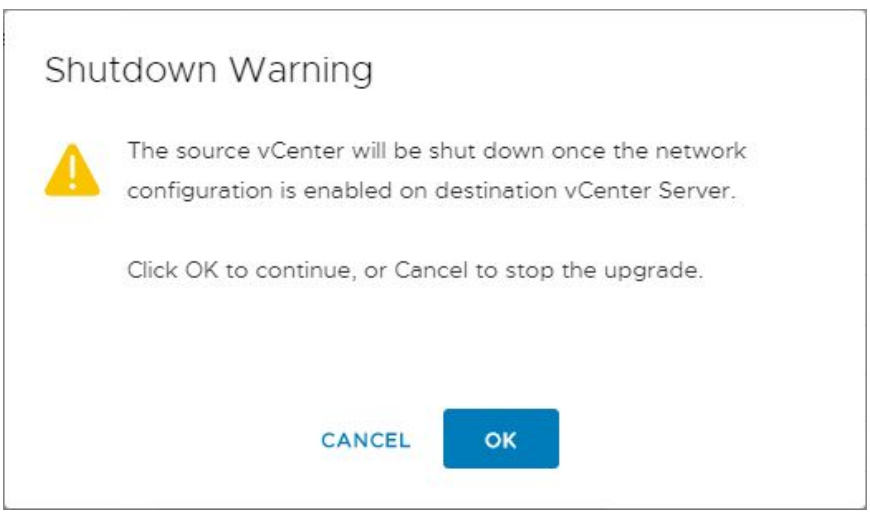
Configure CEIP options screen

Stage 2 of the upgrade process is ready to begin. The chosen options are displayed on the screen along with the option to either go back or Finish the process.



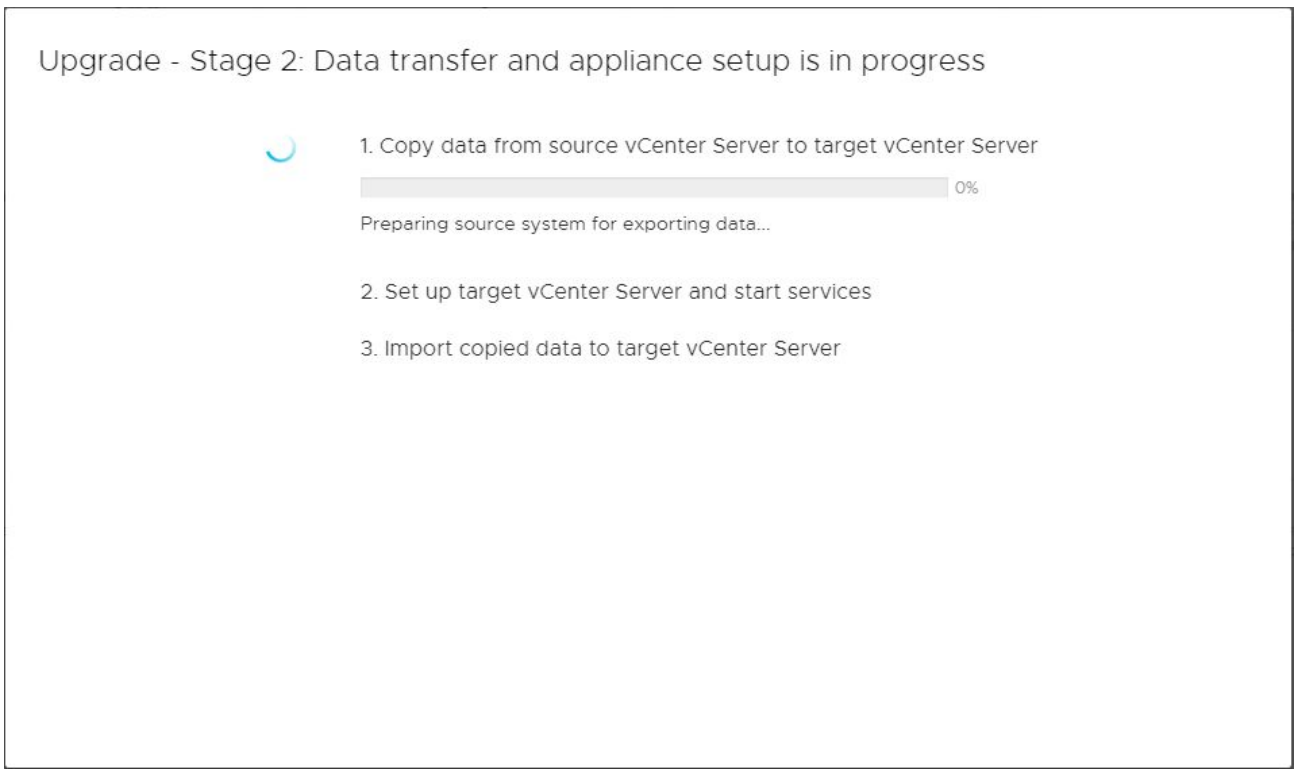
The Ready to Complete screen displays the options chosen for Stage 2

You will see a warning displayed indicating the source VCSA appliance will be shut down during the process. Click OK to continue with the process.



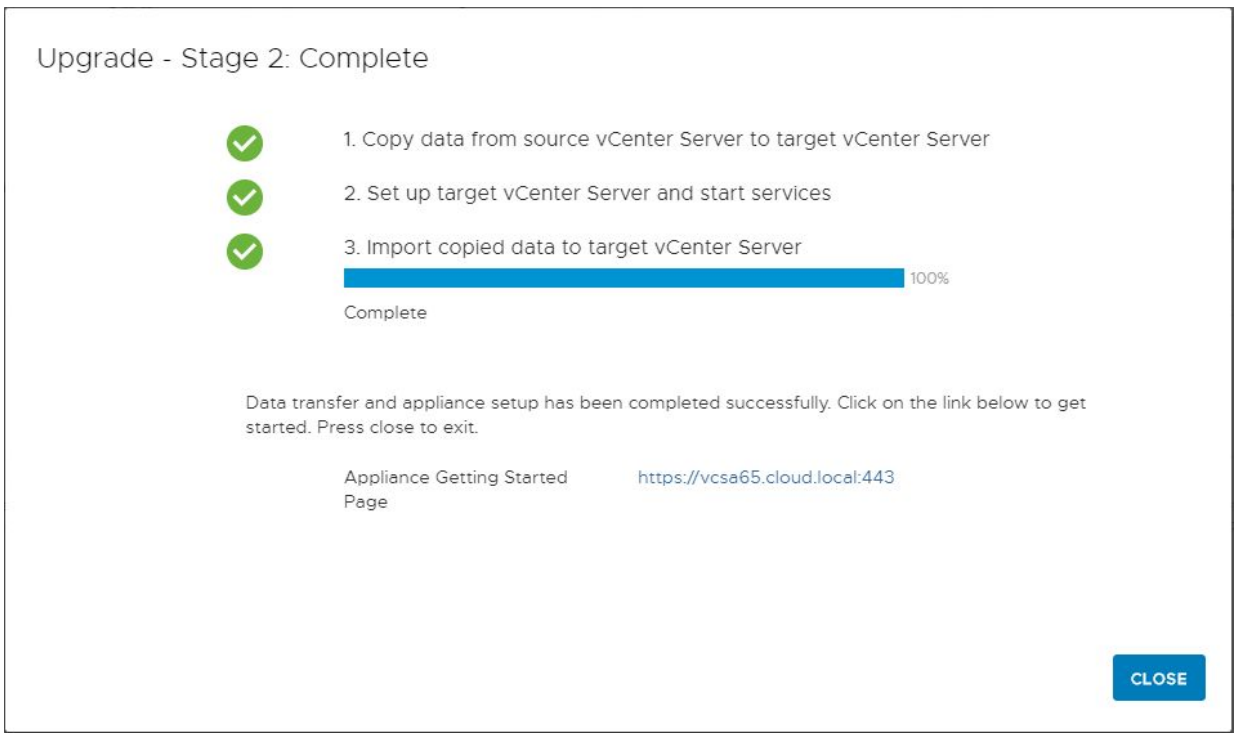
Acknowledge the shutdown warning for the source VCSA appliance VM

The Data transfer and appliance setup begin in the Stage 2 process.



Stage 2 process begins with the data copy from the source appliance

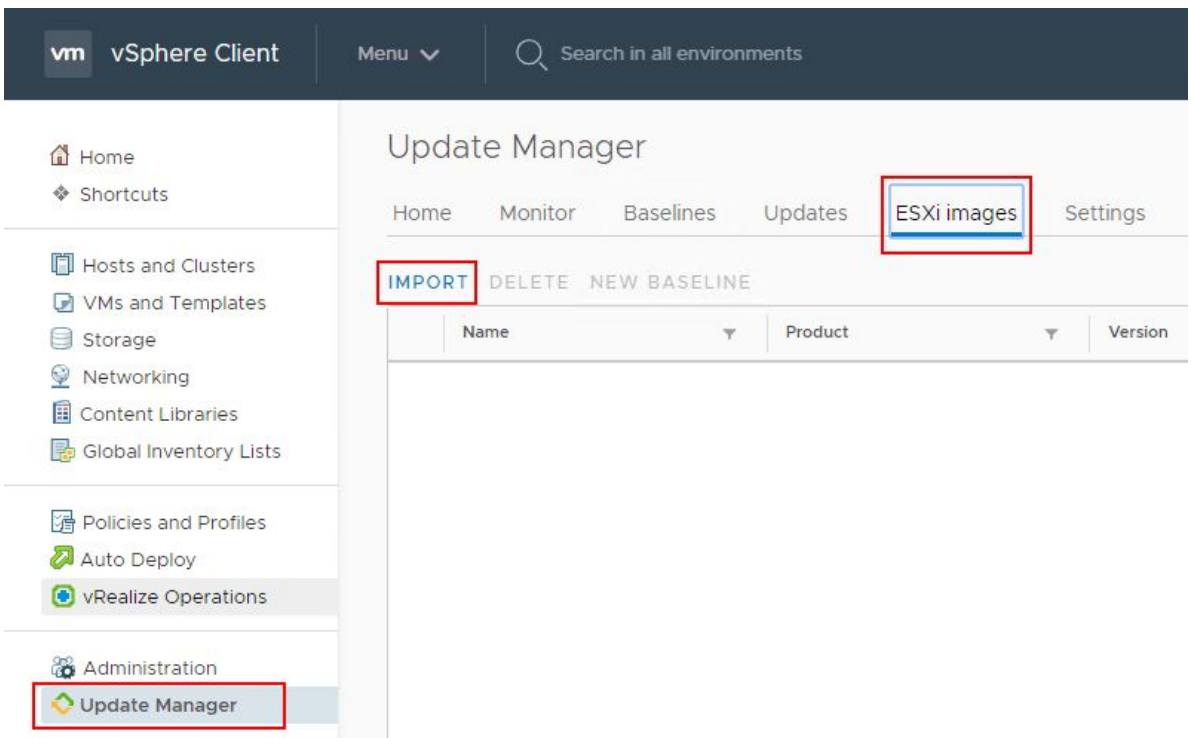
After some time, the Stage 2 process will complete. As you can see the three steps as defined are to copy data, set up the target vCenter Server and start processes, and then import copied data to the target vCenter Server. After a successful upgrade process, you will see the link to the appliance displayed on Stage 2 complete screen.



Upgrading VMware ESXi to vSphere 6.7 Update 1

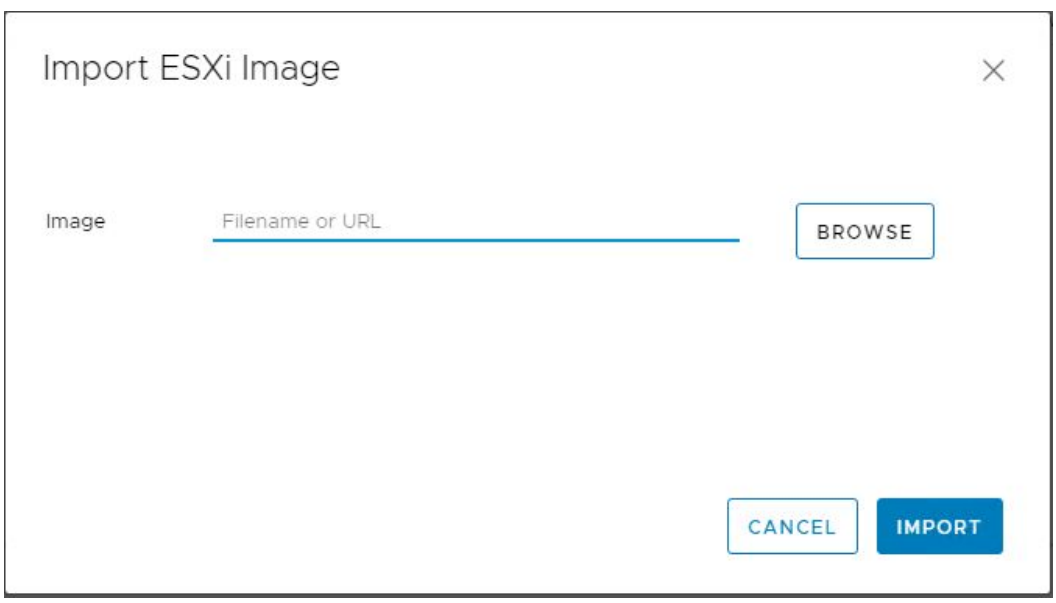
One of the major achievements of vSphere 6.7 Update 1 is the introduction of the fully functional HTML 5 UI. The new HTML 5 interface is a joy to work with. This is certainly evident when working with the Update Manager component of the vSphere client. The process to work with the Update Manager interface, uploading images, creating baselines, attaching baselines, and remediating hosts are extremely easy and intuitive. Let's step through the process and screens of the normal process to upload the vSphere 6.7 Update 1 ESXi image, create the baseline, attach the baseline to the ESXi hosts in our environment, and then remediate the hosts per the attached upgrade baseline.

The first thing that we need to do is upload the new ESXi 6.7 ISO. To do this navigate in the HTML5 client to **Update Manager >> ESXi Images >> Import**.



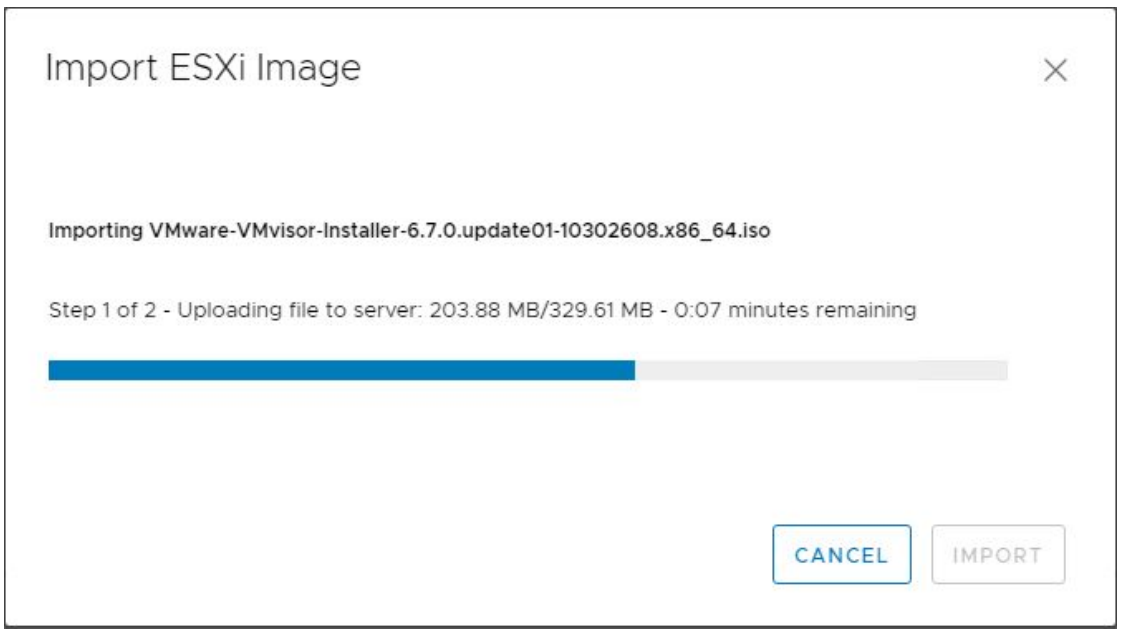
Importing and uploading the vSphere 6.7 Update 1 ISO to Update Manager

Choose to import an ESXi Image and Browse to the ISO file for ESXi 6.7 Update 1. As soon as you select it, it will start to import and then upload the image.



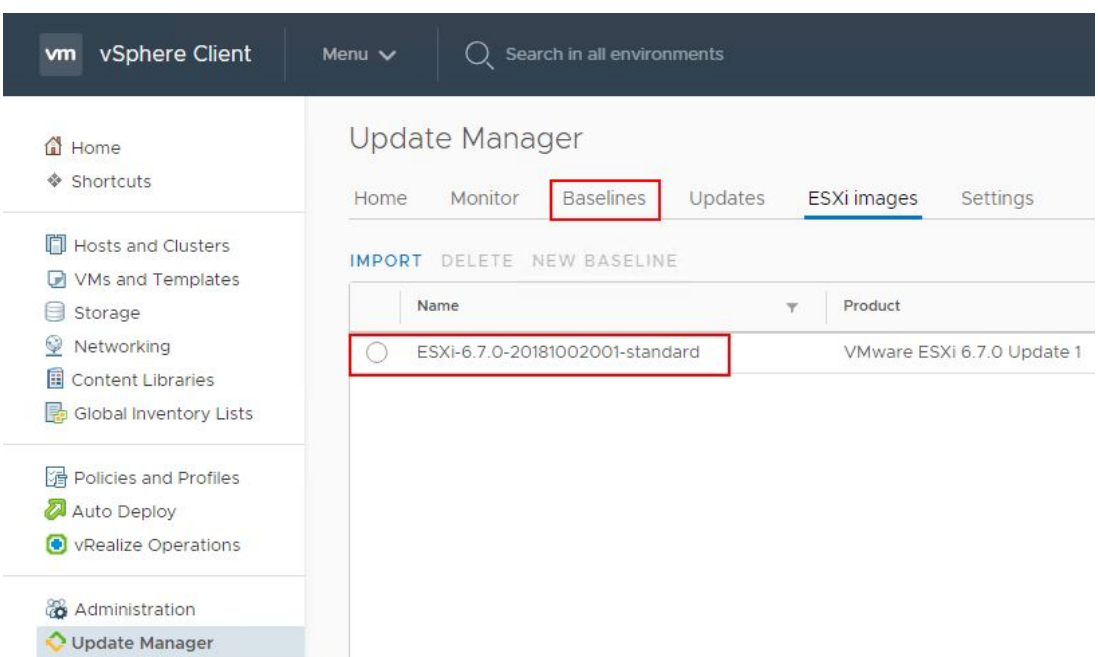
Choose the ESXi 6.7 Update 1 ISO image to import to Update Manager

Below, the process to import the ESXi image has begun. The first step uploads the image and step 2 imports the image into the Update Manager images catalog.



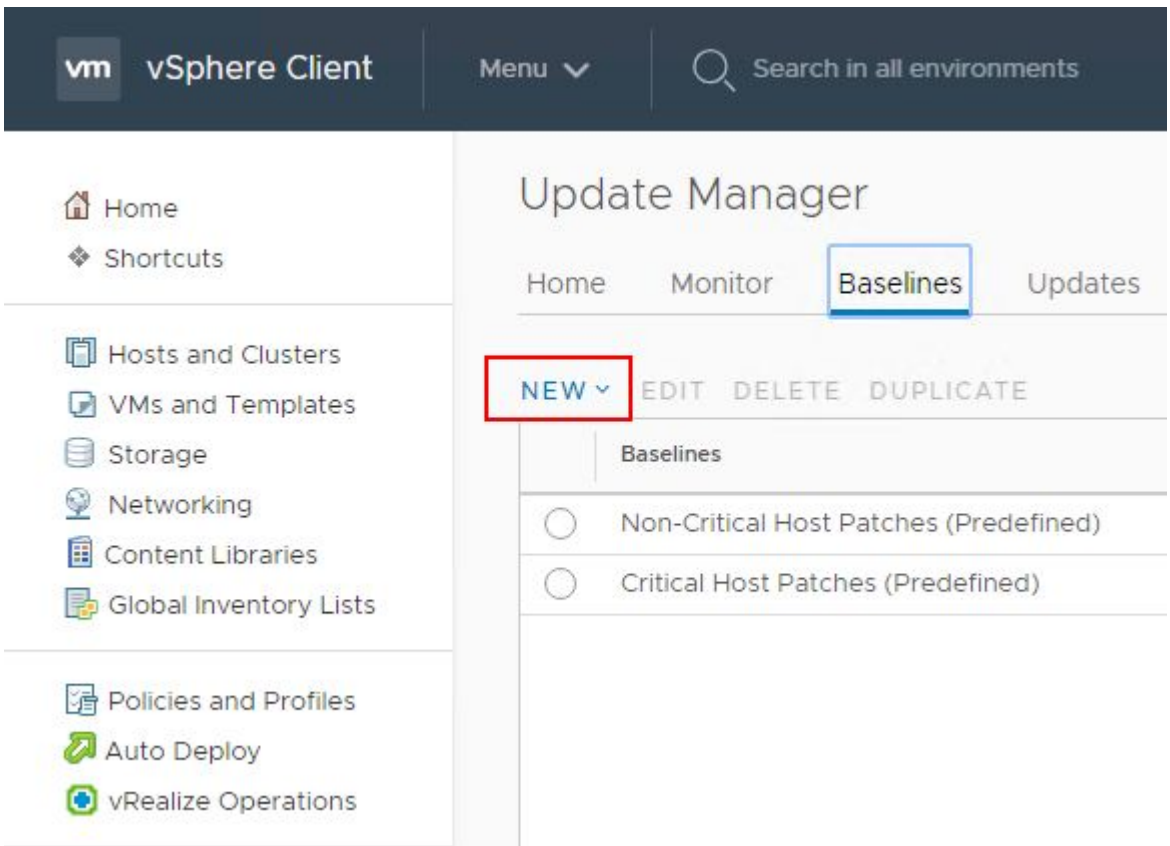
The ESXi 6.7 Update 1 ISO image uploads via the Update Manager Import ESXi Image wizard

After the upload and import finishes, you should be able to see the ESXi image that was just uploaded under the ESXi Images tab.



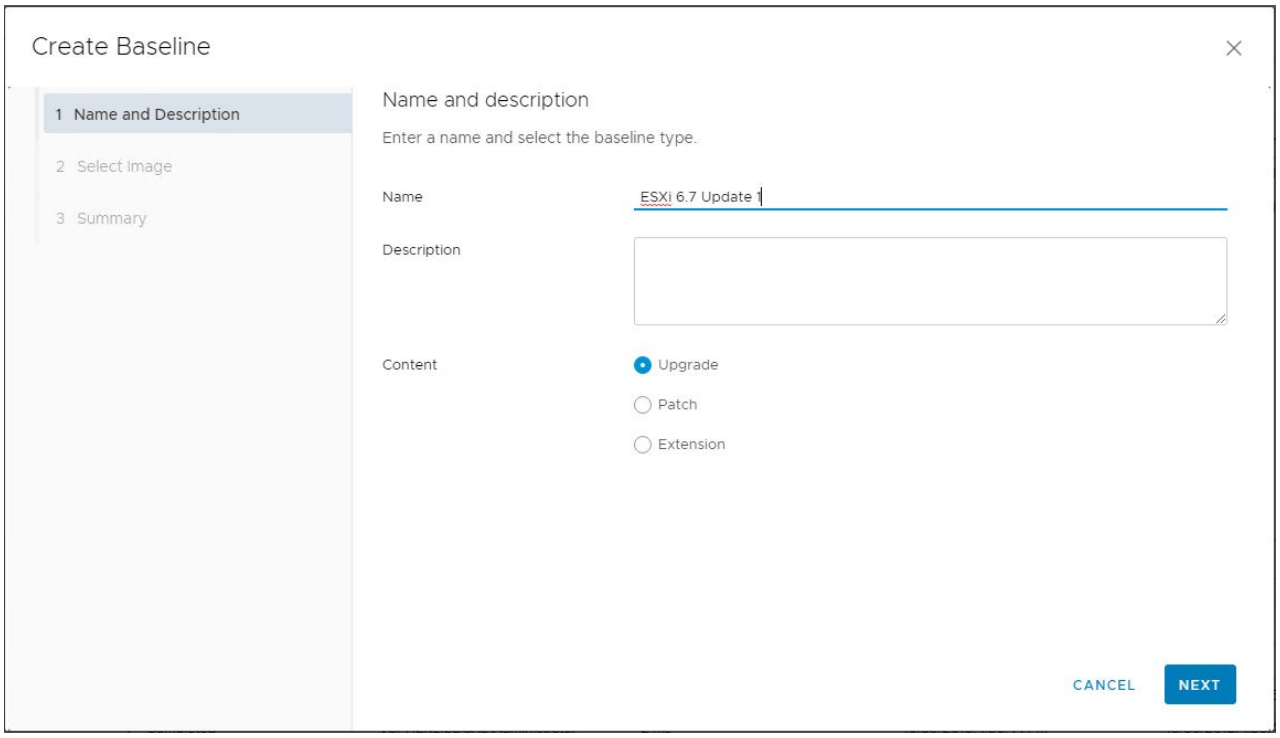
Verifying the ESXi 6.7 Update 1 ISO file was uploaded to Update Manager

Now that the image is uploaded, we can create a new Baseline which allows assigning the action to a “template” of sorts for upgrading, updating, etc. The host has to meet the baseline by the scan operation or it will show out of compliance. Click Baselines >> New.



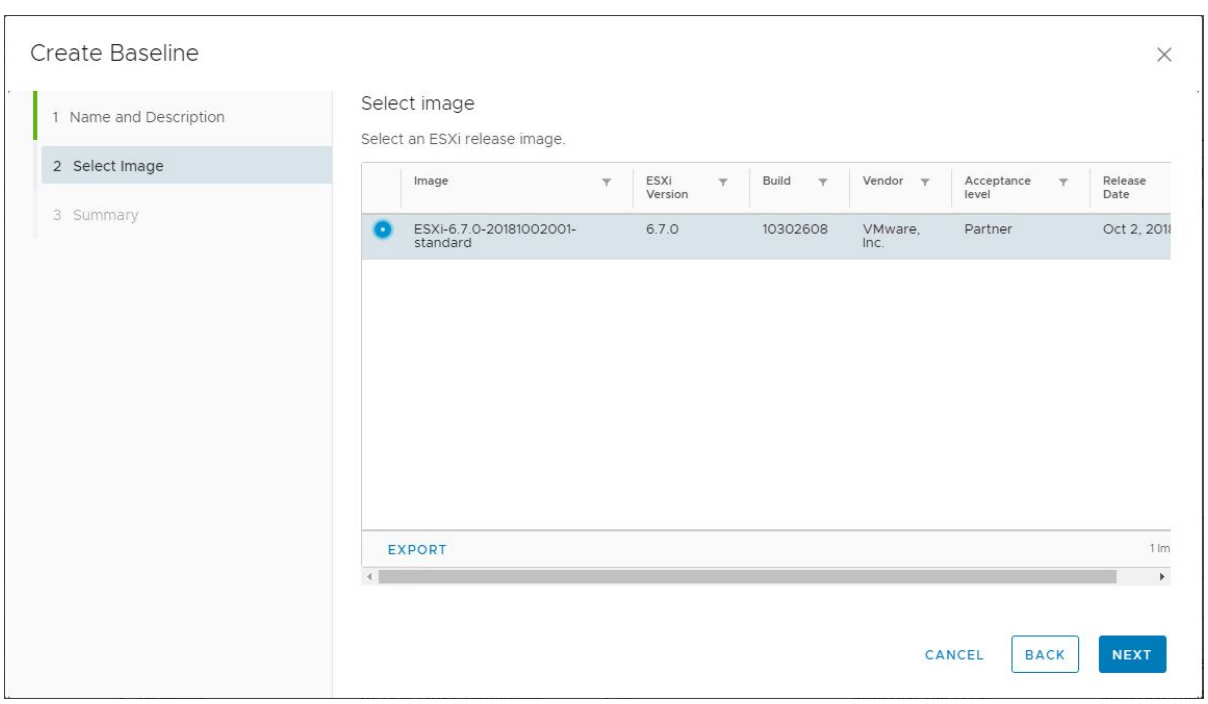
Creating a new baseline for the upgrade process to ESXi 6.7 Update 1

This will launch the Create Baseline wizard. The Create Baseline wizard is a 3-step process that will allow naming and setting the description for the baseline, selecting an image, and finalizing the baseline. Below, the Name for the Baseline is configured and the Content type is set to Upgrade.



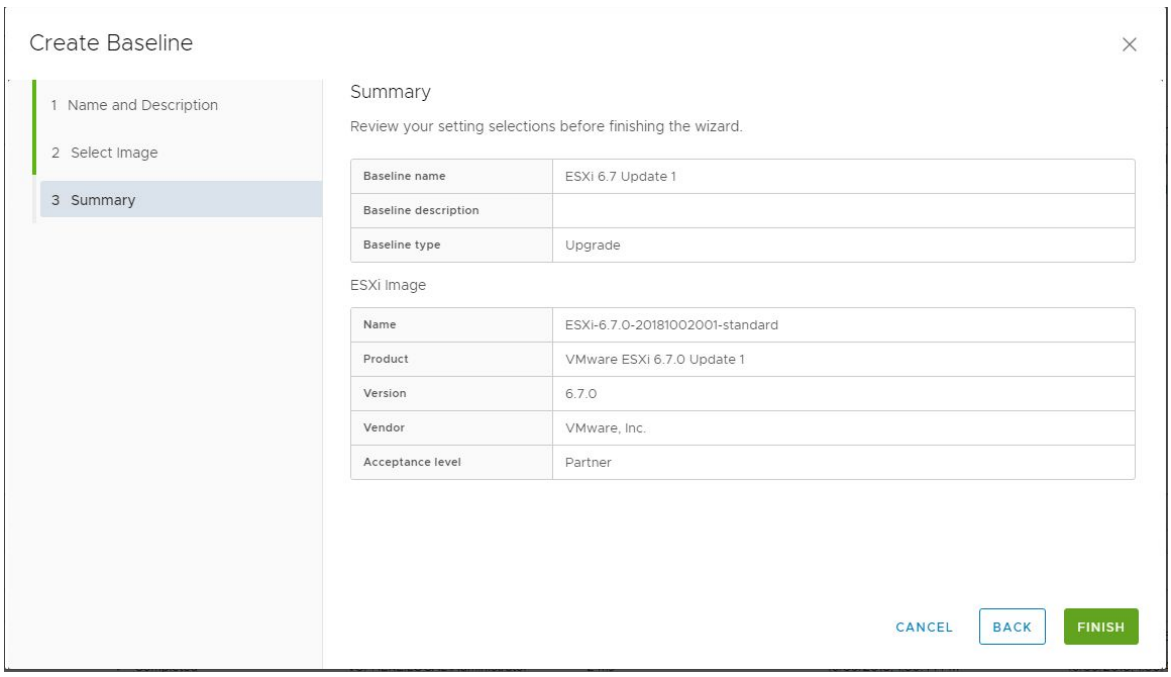
Name and Classify the new Baseline in Update Manager

One step 2, select the image that was uploaded previously for ESXi 6.7 Update 1. You can identify this is Update 1 by the Build version which is 10302608.



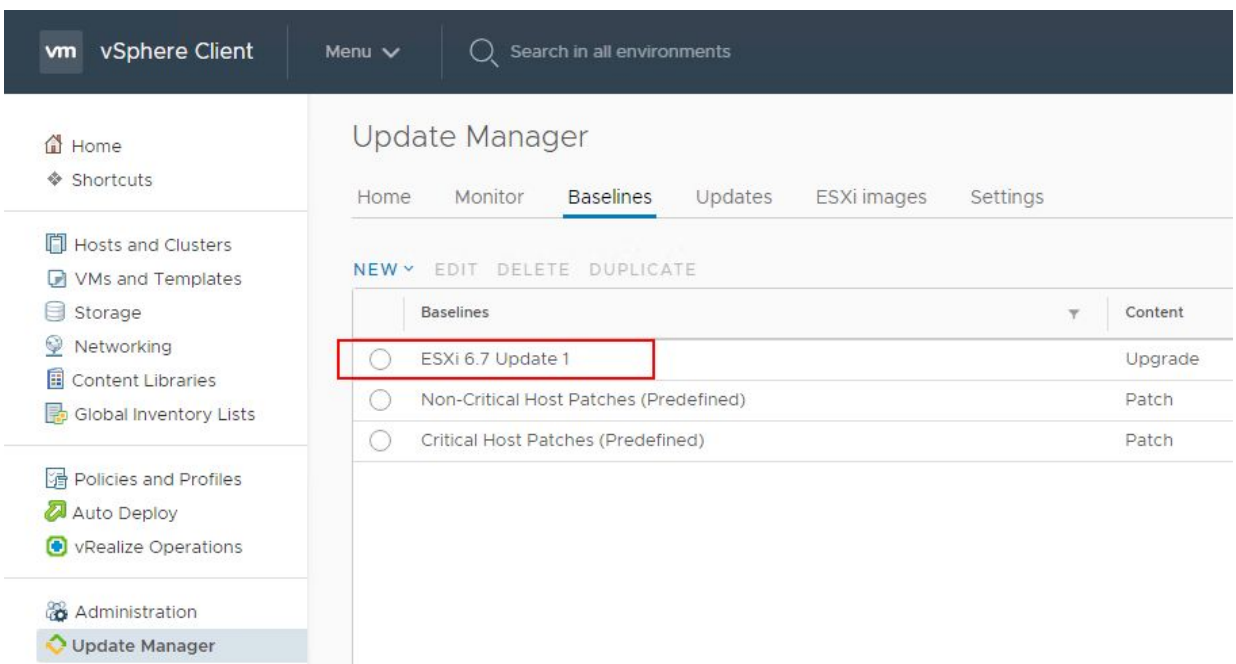
Choose the vSphere 6.7 Update 1 ESXi image file

On the **Summary** screen, you can verify the baseline is configured correctly and then **Finish** the wizard to finalize the baseline creation.



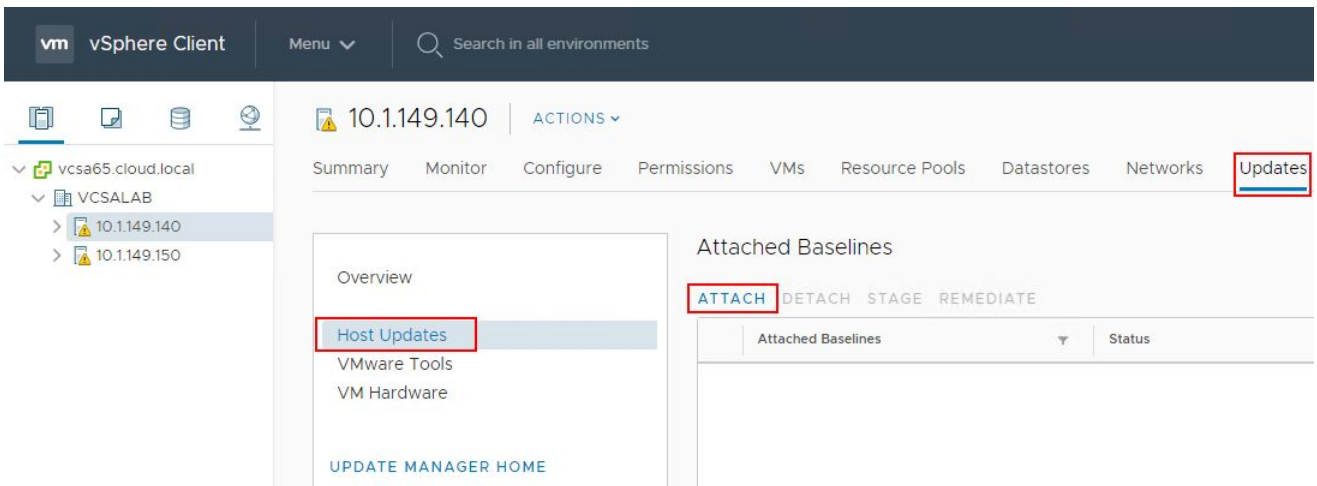
Finalizing the new Upgrade Baseline to vSphere 6.7 Update 1

After the Baseline is created, you should be able to see the new Baseline listed in the Baselines listing.



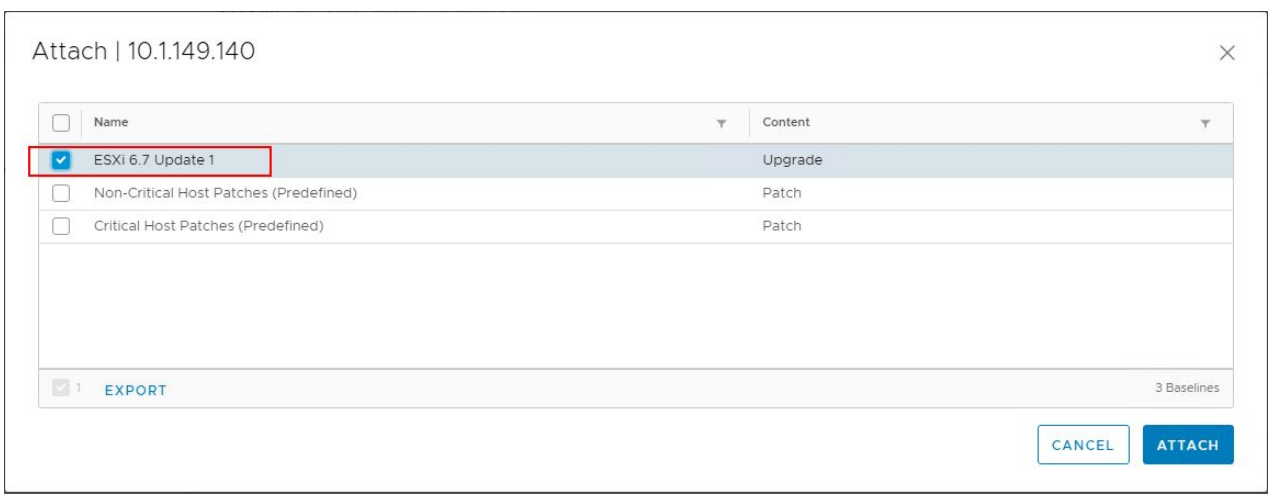
Verifying the new vSphere 6.7 Update 1 Upgrade Baseline was created successfully

Now that the vSphere ESXi 6.7 Update 1 ISO image has been uploaded and the new upgrade baseline for ESXi 6.7 Update 1 has been created, you can attach the baseline to the ESXi host that is to be remediated. To do this, select the host click Updates >> Host Updates >> Attach to select the newly created baseline.



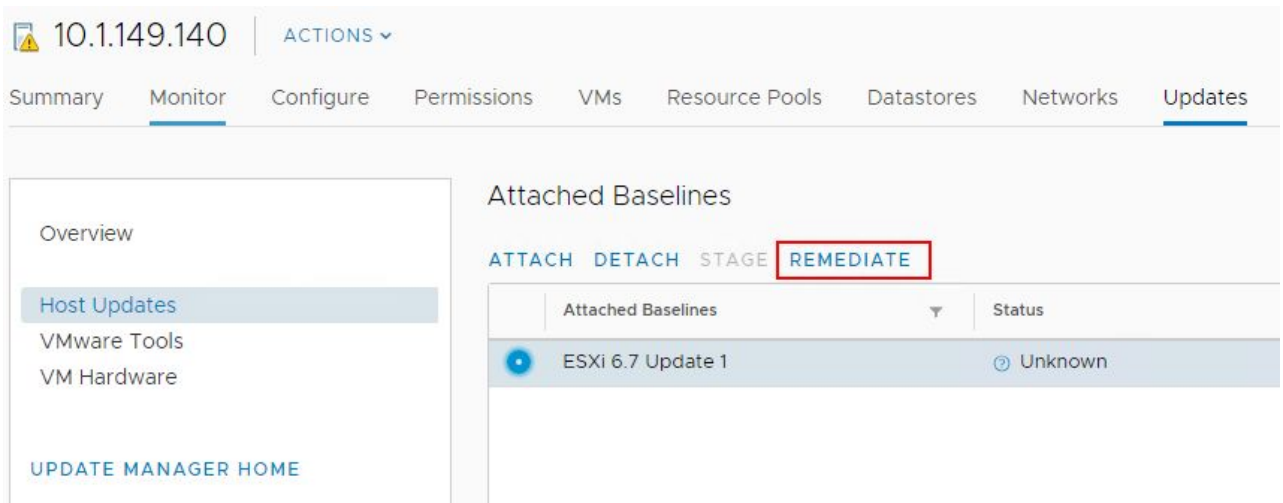
Attach the Upgrade Baseline to the ESXi host you want to upgrade to vSphere 6.7 Update 1

On the Attach screen, select the newly created baseline that contains the Upgrade action to ESXi 6.7 Update 1.



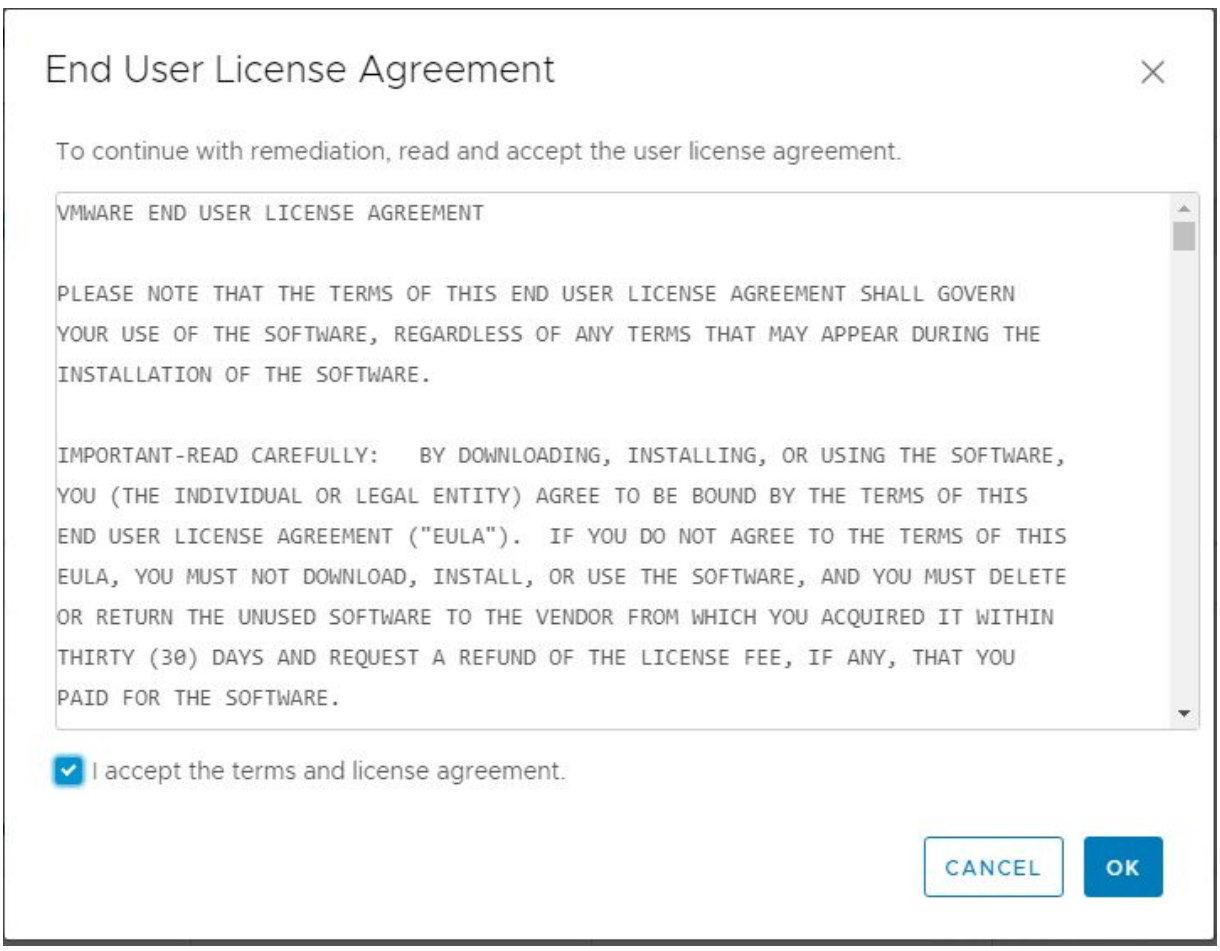
Choose the new ESXi 6.7 Update 1 Upgrade Baseline

Next, choose the Remediate button under Updates >> Host Updates. This will allow the host to be scanned and remediated based on the attached baselines.



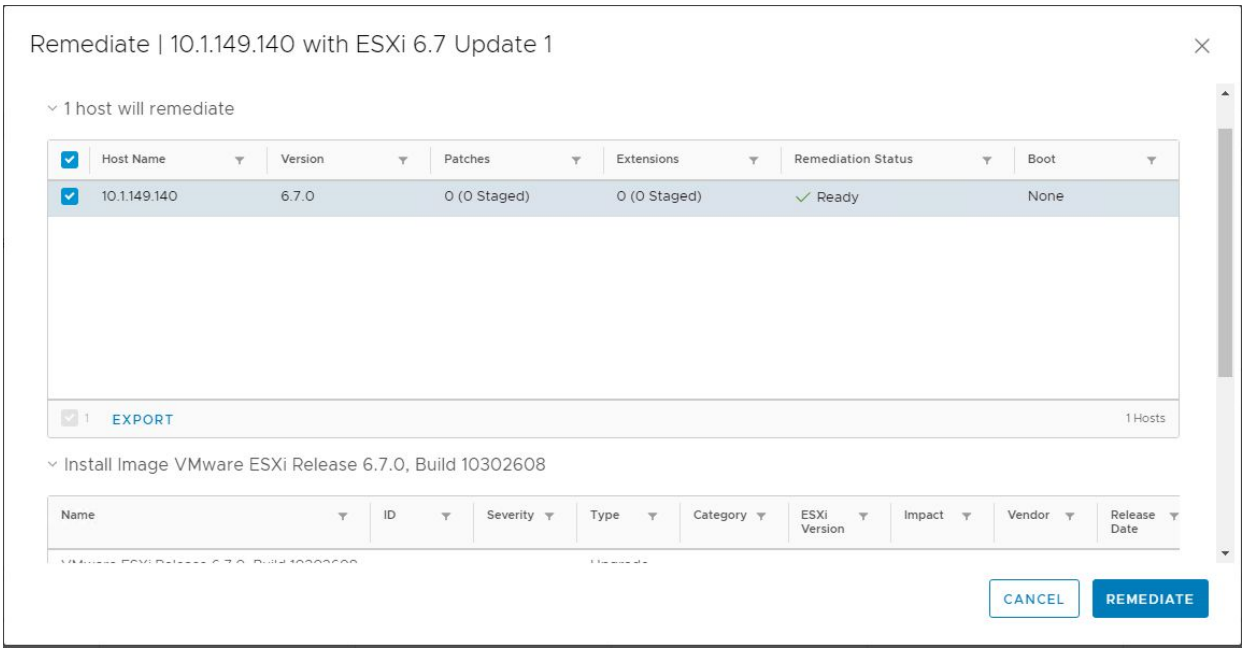
Choose to Remediate the ESXi host

Once Remediate is clicked, the EULA for ESXi 6.7 Update 1 is displayed. Place a check in the box to accept the EULA and click OK.



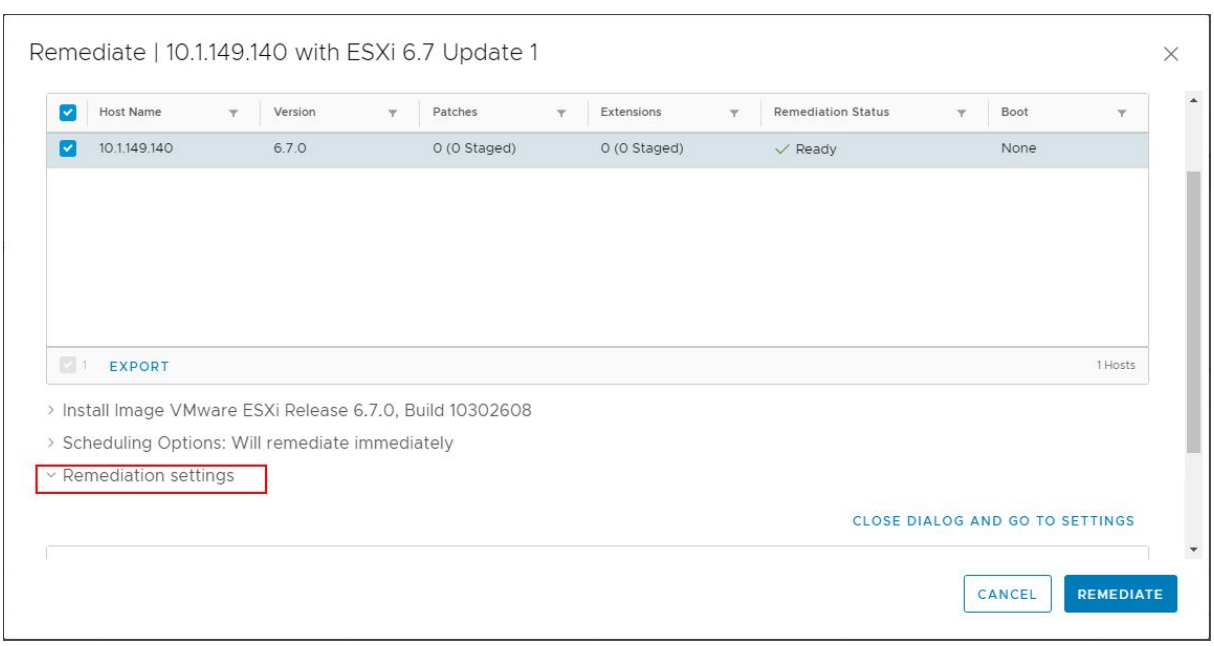
Accept the EULA for the upgrade to vSphere 6.7 Update 1

The Remediate screen is displayed for the host. The host will automatically be checked for remediating. At this point, you can simply click the Remediate button to begin the upgrade process or customize the remediate action further.



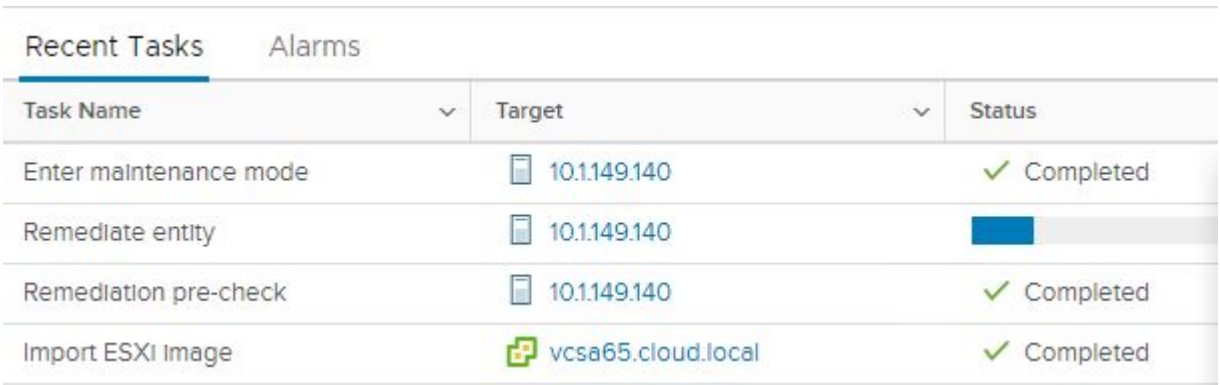
Verify the host to remediate and configure any additional remediation options

You can expand the various options on the bottom of the Remediate screen such as Scheduling Options and Remediation Settings. These allow configuring the scheduling of the upgrade as well as other remediation settings on the host itself.



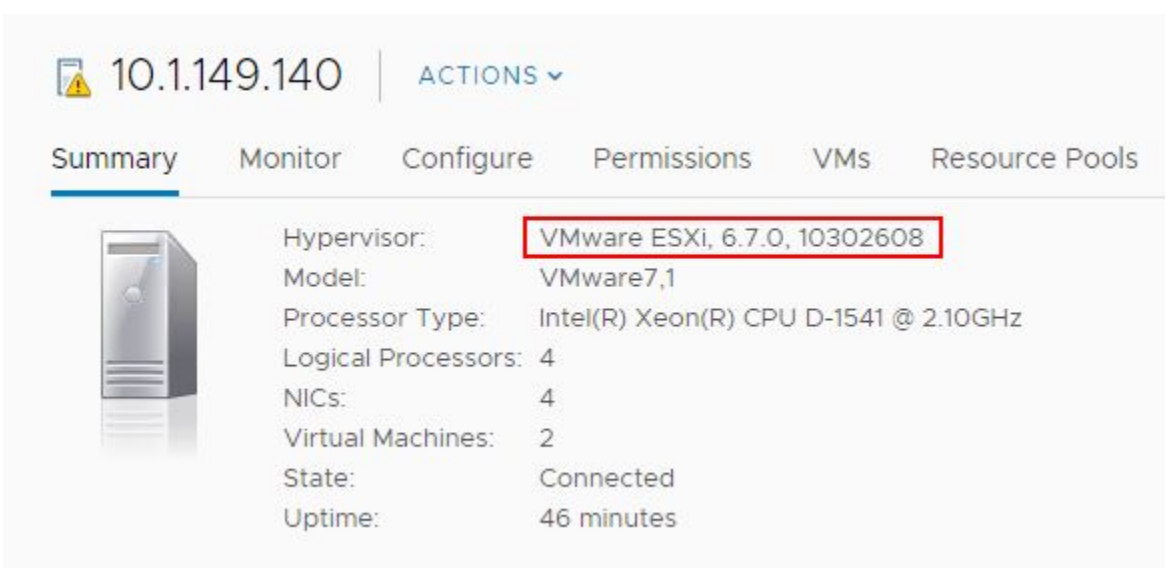
Expand the Remediation Settings to further customize the remediation process

After clicking the Remediate button, you will see the Remediate entity action kick off in the Recent Tasks pane in vCenter Server.



The Remediate entity task kicks off in the Recent tasks in vCenter

The upgrade process will automatically reboot the host in question. After the host reboots, you can take the host out of maintenance mode and verify the Hypervisor version under the Summary tab. The version should reflect VMware ESXi, 6.7.0, 10302608. This is the build version for ESXi 6.7 Update 1.



The ESXi host version and build should reflect vSphere 6.7 Update 1 after the reboot

Implementing VMware vSphere Virtual Machine Encryption

VM encryption provides security to the VMDK that stores the data for a virtual machine. The I/O operations are encrypted from a virtual machine before they are written to the VMDK disk. Other files associated with the virtual machine are not encrypted due to their non-sensitive nature. These include the VM log files, configuration files, virtual disk descriptor files, etc. How is this helpful in the realm of securing virtual machine data?

Imagine the scenario and use case of how this type of security protects your virtualized environment and perhaps, very sensitive data. If an unscrupulous system administrator or someone who has potential access to the VMware vSphere storage copied the virtual machine disk files to a removable device, they could take the disk to another VMware vSphere environment, import the virtual machine disk files into the new environment, power up the virtual machine, and have access to all the data stored on the virtual machine disk file that was copied from the source environment.

Another scenario might involve a domain controller. What if an employee or someone who gained access to VMware vSphere storage was able to copy a domain controller virtual machine to removable storage. They could then perform the same task as above and import the virtual machine into a new VMware vSphere environment, perhaps at home. Then they could run Active Directory password utilities relentlessly against the environment, completely outside the scanning, alerting, and other security mechanisms that might be running on-premises. Passwords can potentially be gathered from the “offline” Active Directory environment and provide an extremely dangerous security situation if this goes undiscovered. The employee could have access to domain admin credentials and potentially impersonate other users, compromising data, stealing data, and even other outcomes.

The above scenarios are only a couple of examples of how unencrypted data can be compromised. Virtual machine disks that are not encrypted are fully readable with no special effort on the part of the attacker outside of having access to the data. Once virtual machine encryption is introduced into the environment, it becomes exponentially more difficult to compromise data, even if you have access to the virtual machine storage.

How to Enable VMware Virtual Machine Encryption

So with all the added security benefits to encrypting VMware virtual machines, this is certainly a security feature that most will want to take a look at to secure sensitive virtual machines running in the environment. Let's take a look at the requirements for enabling virtual machine encryption in VMware vSphere. To enable virtual machine encryption, let's look at the following steps to enable this functionality.

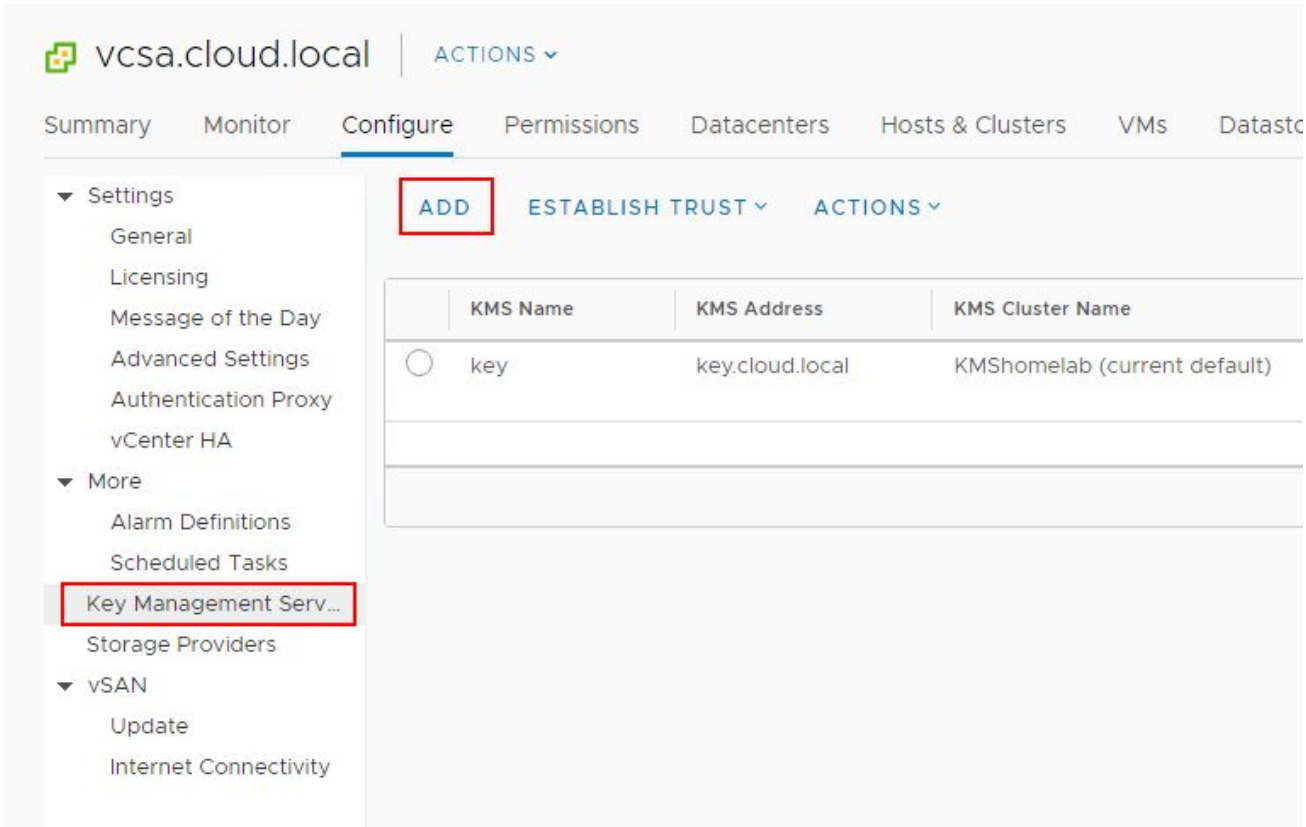
1. Provision a supported Key Management Server cluster to issue encryption keys
2. Establish trust between VMware vCenter Server and the Key Management Server cluster
3. Change the storage policy to VM Encryption for virtual disks

The process to do this is straightforward and can easily be accomplished via the new fully-featured HTML 5 vSphere client in vSphere 6.7 Update 1. The first requirement as listed is to provision a Key Management Server cluster. Most will probably provision a virtual solution running by way of a virtual appliance either in a production or management cluster. The Key Management Server cluster or KMS cluster will most likely be made up of multiple nodes for resiliency and in accord with best practice.

The Key Management Server solution must support the Key Management Interoperability Protocol (KMIP) 1.1 standard to be used as a KMS solution in VMware vSphere. You can find out more about which solutions are supported in the VMware Compatibility Guide.

In the below walkthrough, we will add a supported KMS cluster server solution to the VMware vSphere environment for use with virtual machine encryption tasks.

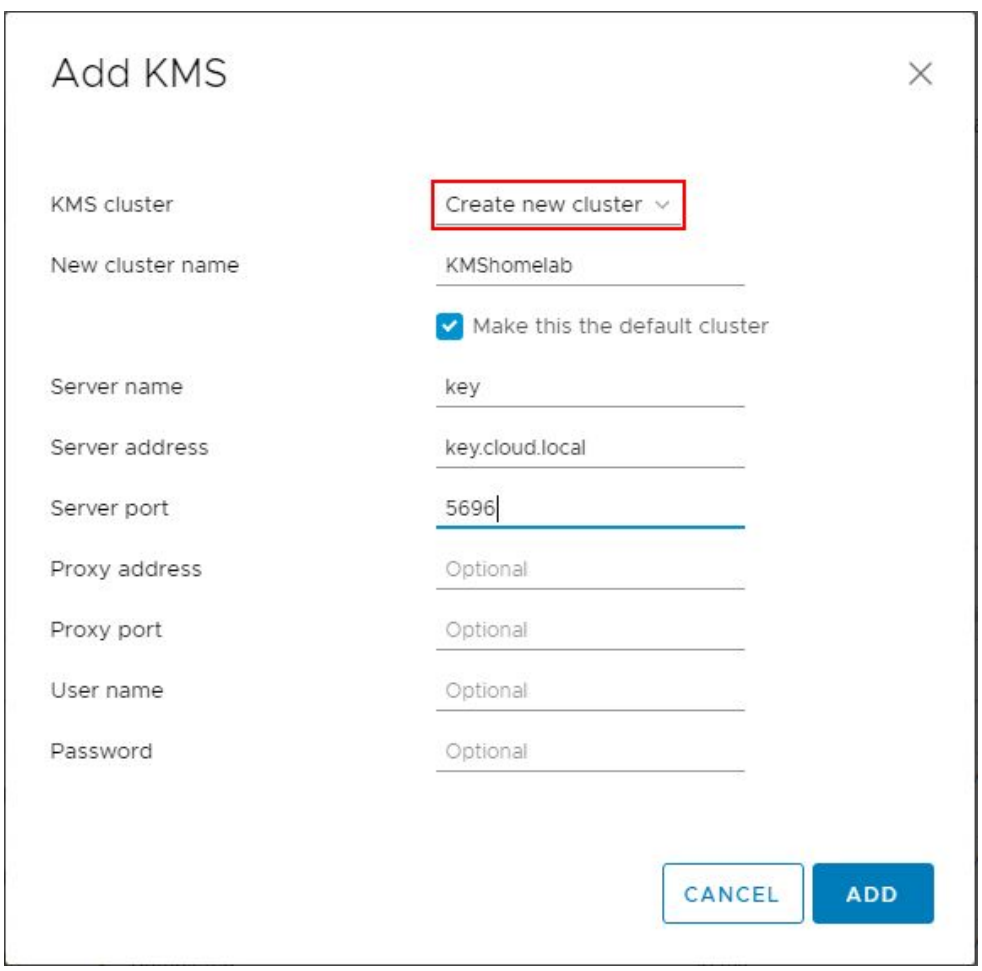
Navigate to the **Configure** menu of the vCenter Server inside of the vSphere client. Click **Key Management Servers > Add**.



Adding a new Key Management Server in the properties of the VMware vCenter Server configuration

This will launch the **Add KMS** dialog box that will allow you to **Create new cluster** or point to an existing cluster. Below we are creating a new KMS cluster inside of the vCenter Server configuration. The process gathers the necessary configuration information including:

- KMS Cluster configuration (create new or point to existing)
- New cluster name with the choice to make the KMS cluster the default configuration
- Server name – This is the friendly name in vCenter Server
- Server address – The IP or FQDN of the KMS cluster
- Server port – port the KMS server is listening on
- Proxy address – (optional)
- Proxy port - (optional)
- User name - (optional)
- Password - (optional)

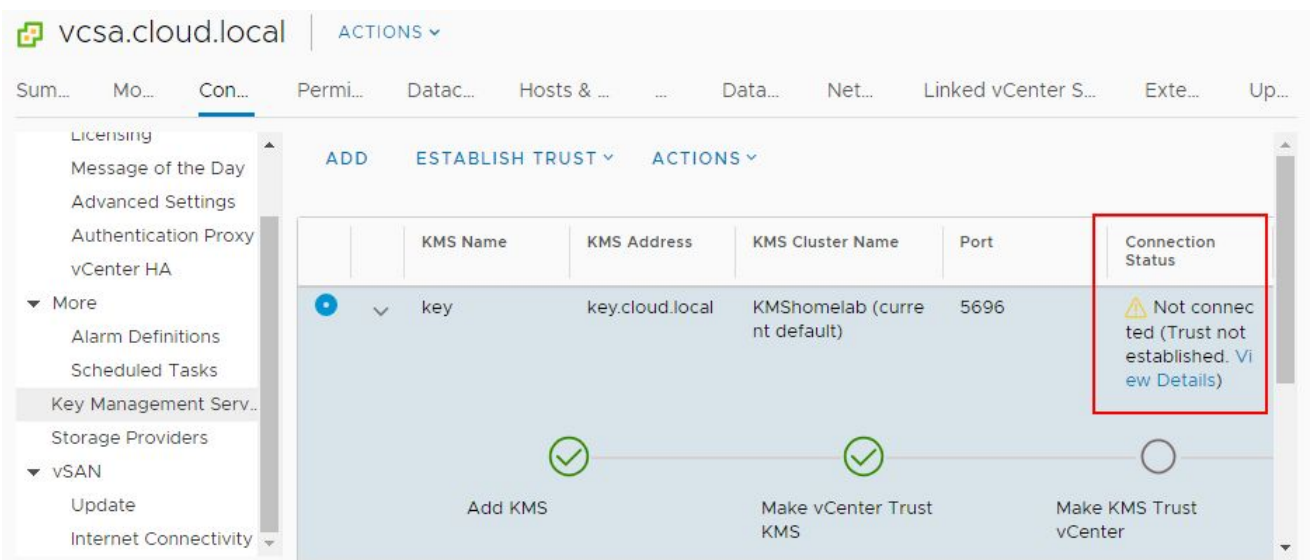


Adding a new KMS cluster in the Key Management Server properties

You will see the **Make vCenter Trust KMS** dialog box open after establishing the connection to the KMS server cluster. Even though you click **Trust** in this step, there are further steps required for establishing trust in vCenter.

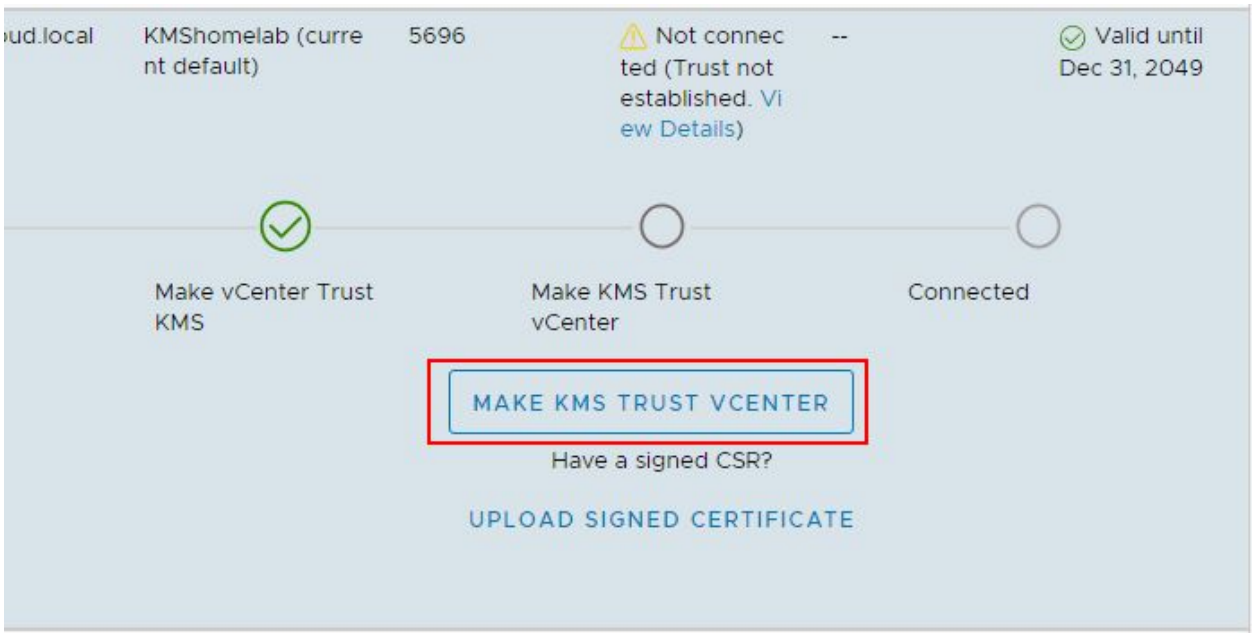
Connecting to the KMS configured

Notice the connection status shows Not connected (Trust not established View Details).



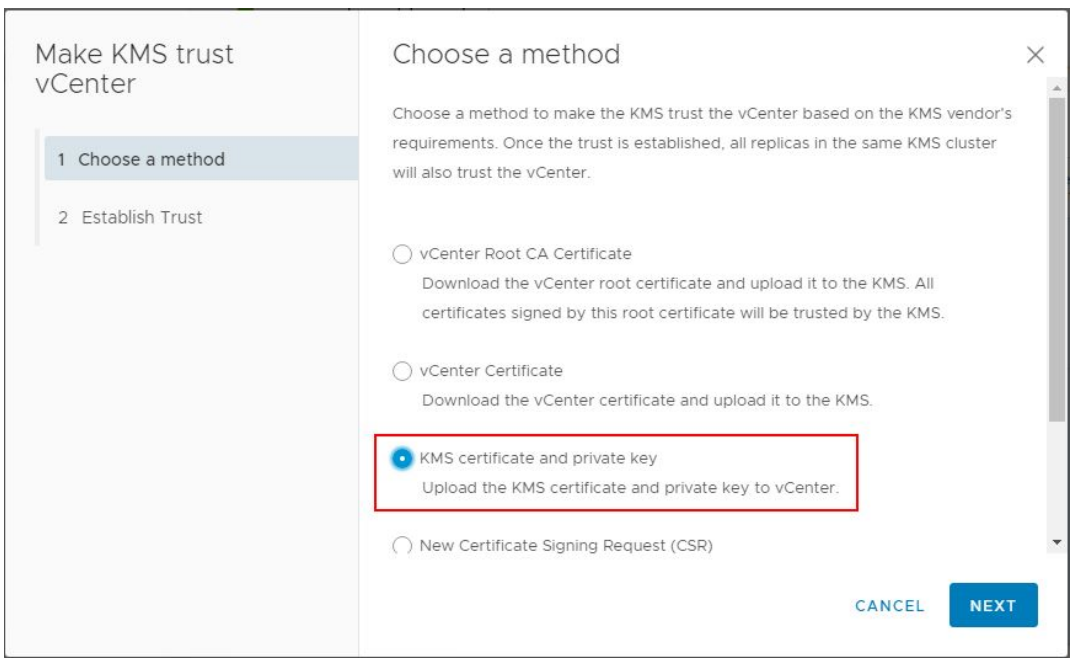
Viewing the trust status of the new KMS cluster in the vSphere client

If you click to **View Details** you will see the **MAKE KMS TRUST VCENTER** button. Click this button to open the further configuration for trusting the KMS server.



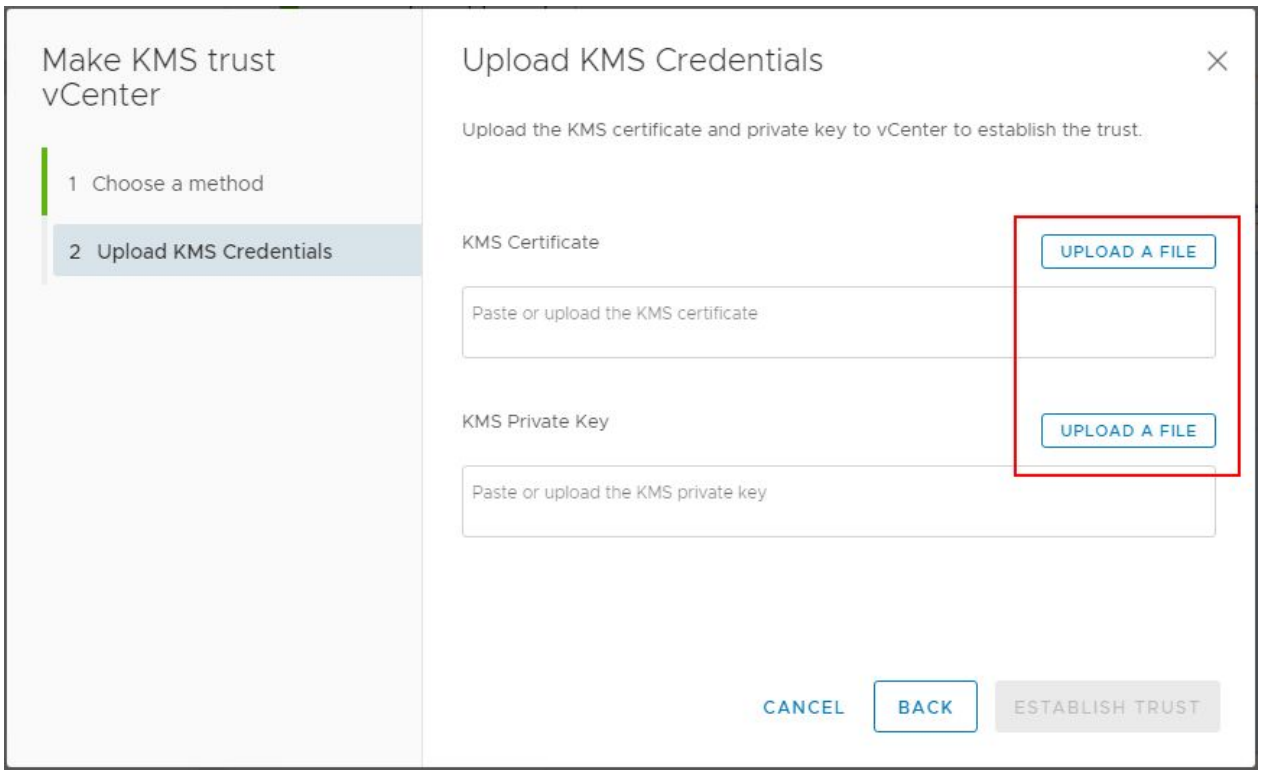
Make KMS Trust vCenter

This will launch a wizard to Make KMS trust vCenter with a few options. Since in the lab, I have a certificate downloaded from the KMS server and a private key, I will be uploading these to vCenter for establishing trust.



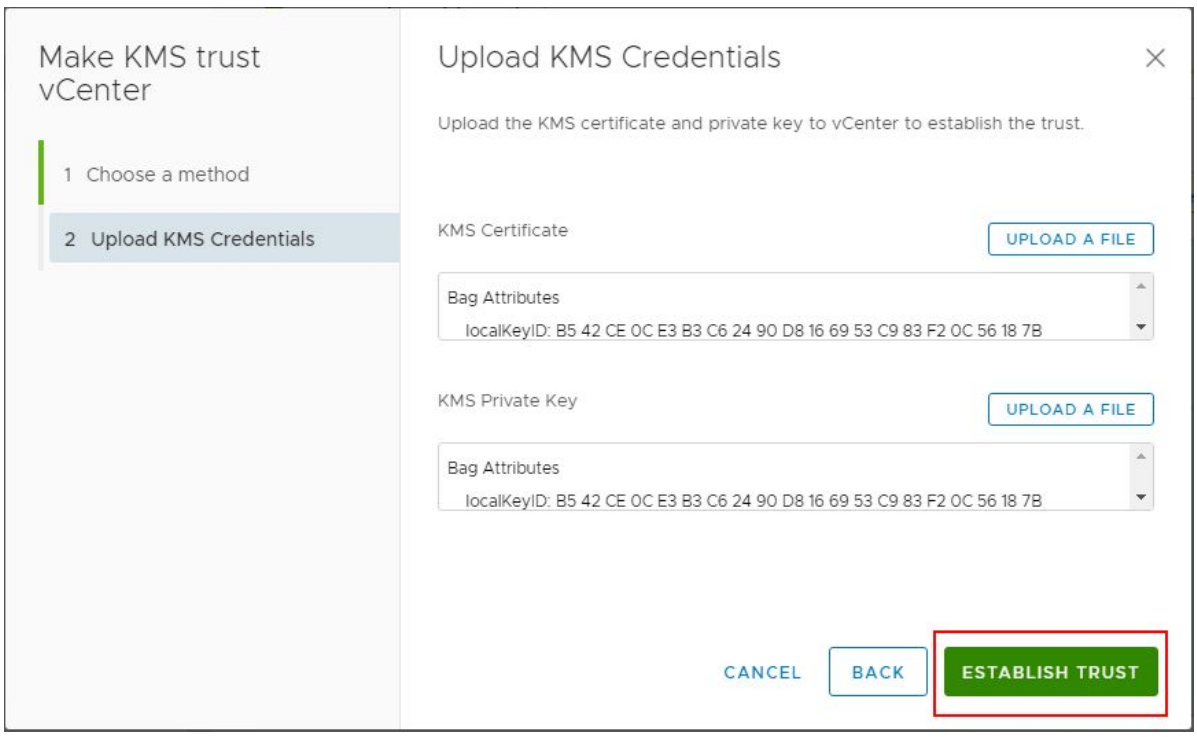
KMS certificate and private key upload to establish trust

In the **Upload KMS Credentials,** you will see the **Upload a file** button for both the **KMS Certificate** and the **KMS Private Key**.



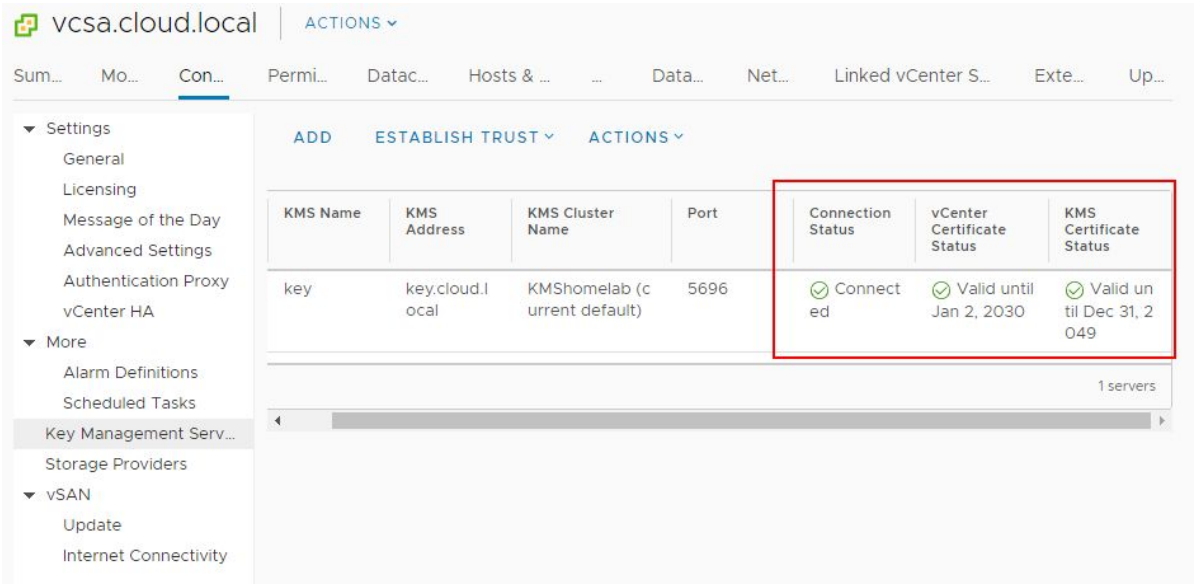
Uploading the certificate and private key

After uploading the certificate and private key, click the Establish Trust button.



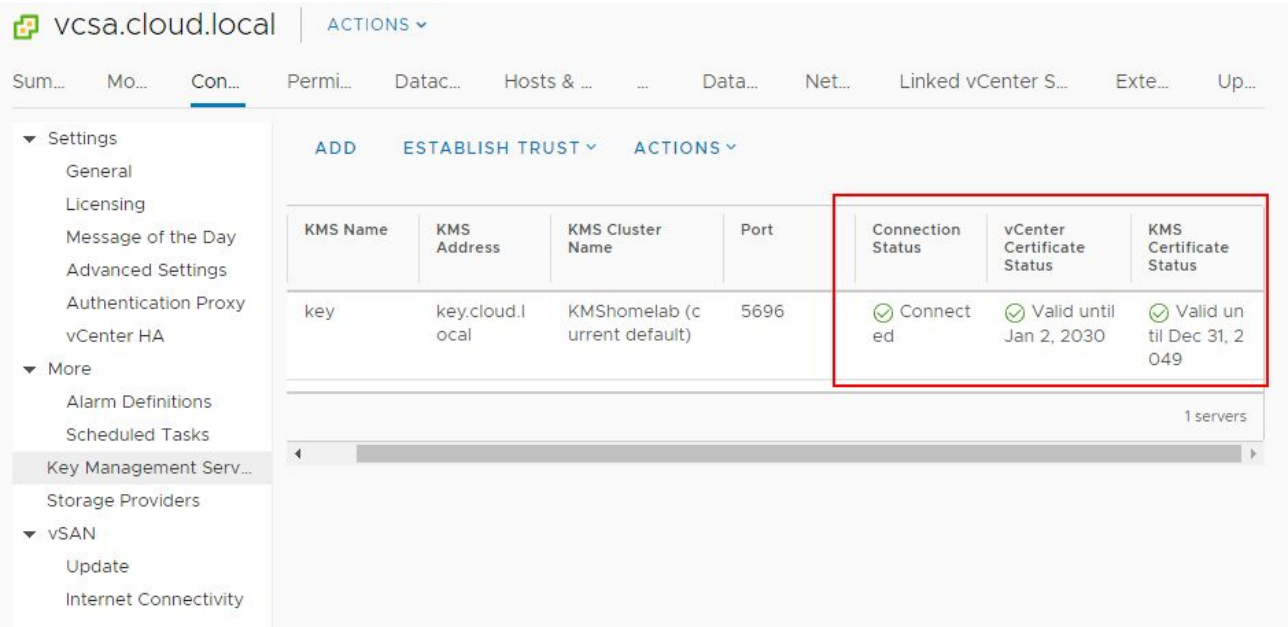
Establishing Trust with the KMS cluster by using the KMS certificate and private key

Now, after establishing trust, you will see the connection status, vCenter Certificate Status, and KMS Certificate Status all showing with a green checkmark. Trust has been established.



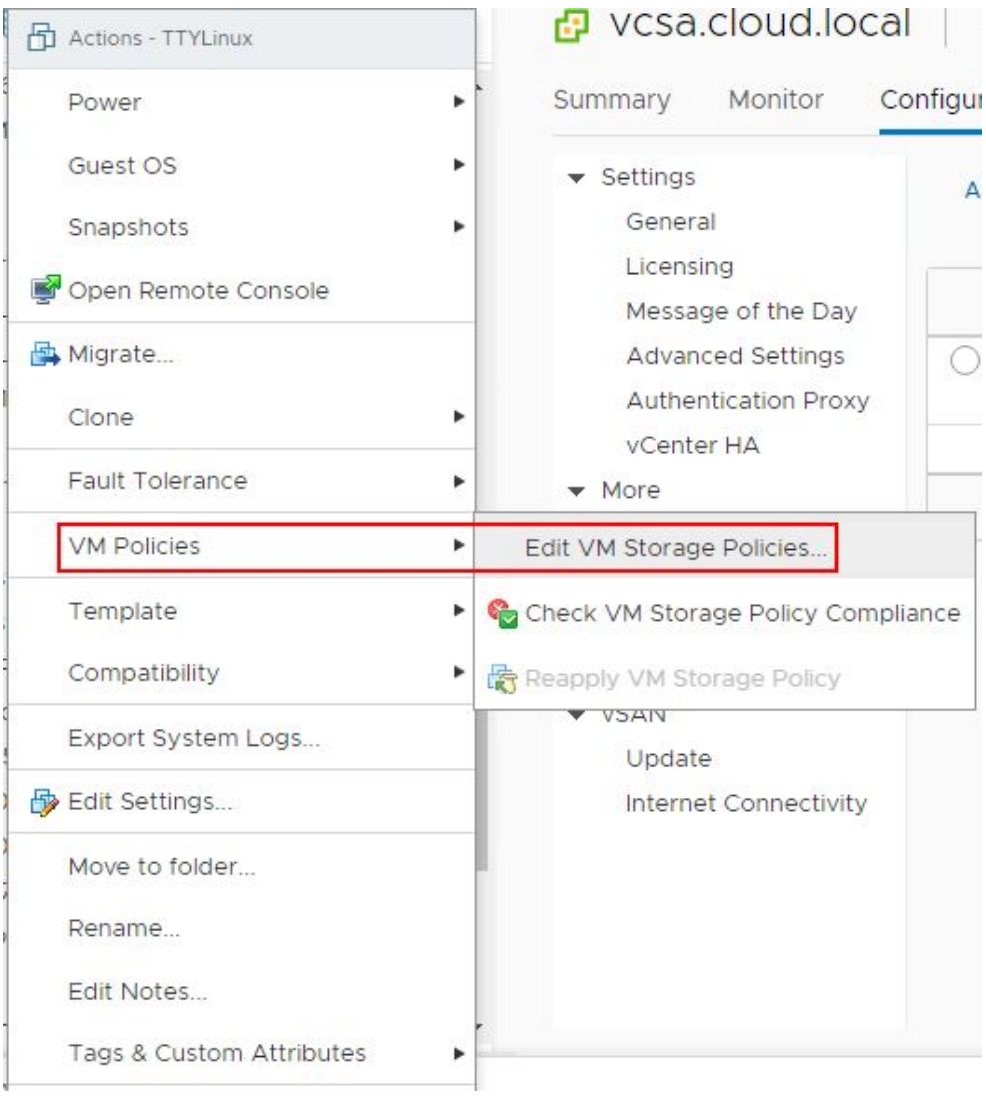
Trust successfully established with the KMS cluster and vCenter

Now, after establishing trust, you will see the connection status, vCenter Certificate Status, and KMS Certificate Status all showing with a green checkmark. Trust has been established.



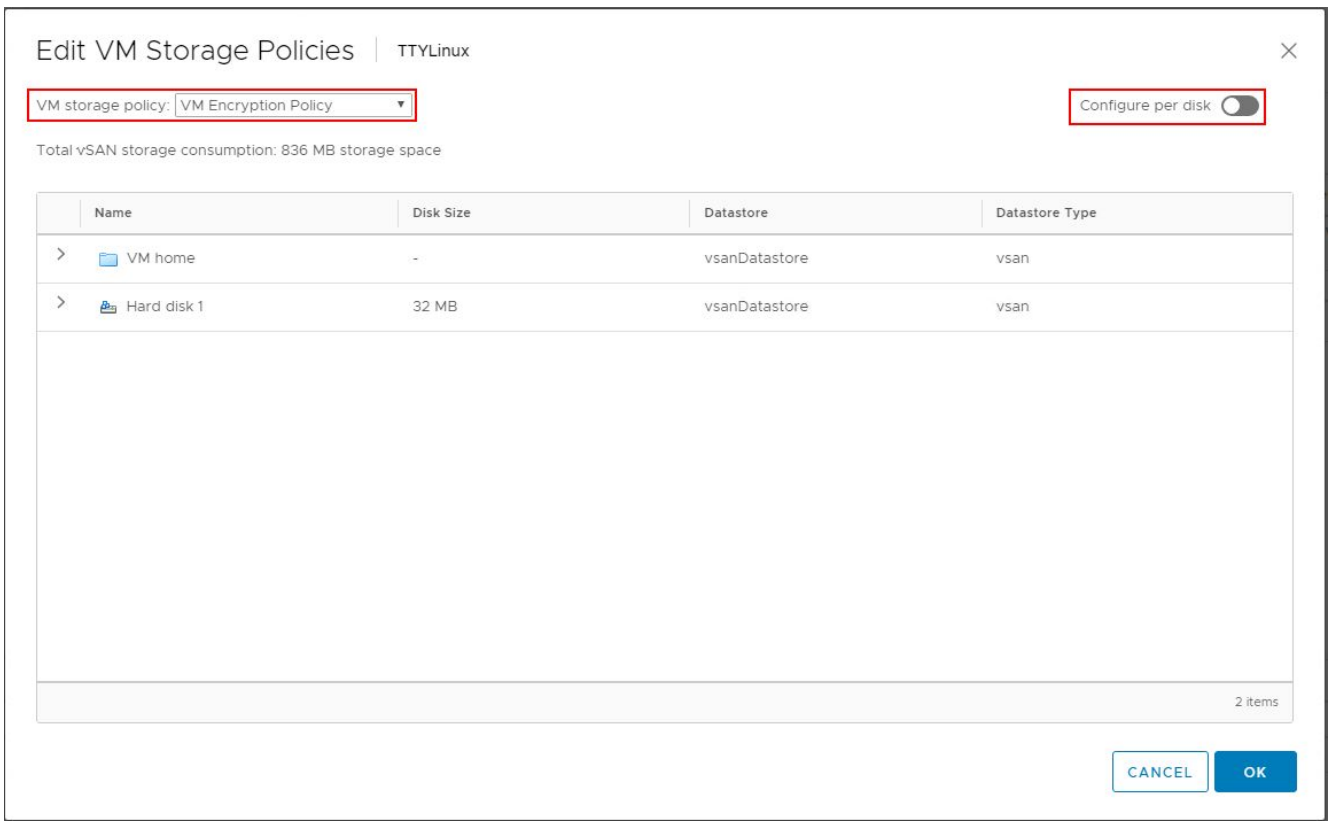
Trust successfully established with the KMS cluster and vCenter

Now that the KMS cluster is in place, we can start encrypting virtual machine disks with the new functionality enabled by the KMS server. To encrypt virtual machine disks, right-click on a virtual machine in the vSphere client inventory, and choose VM Policies > Edit VM Storage Policies.



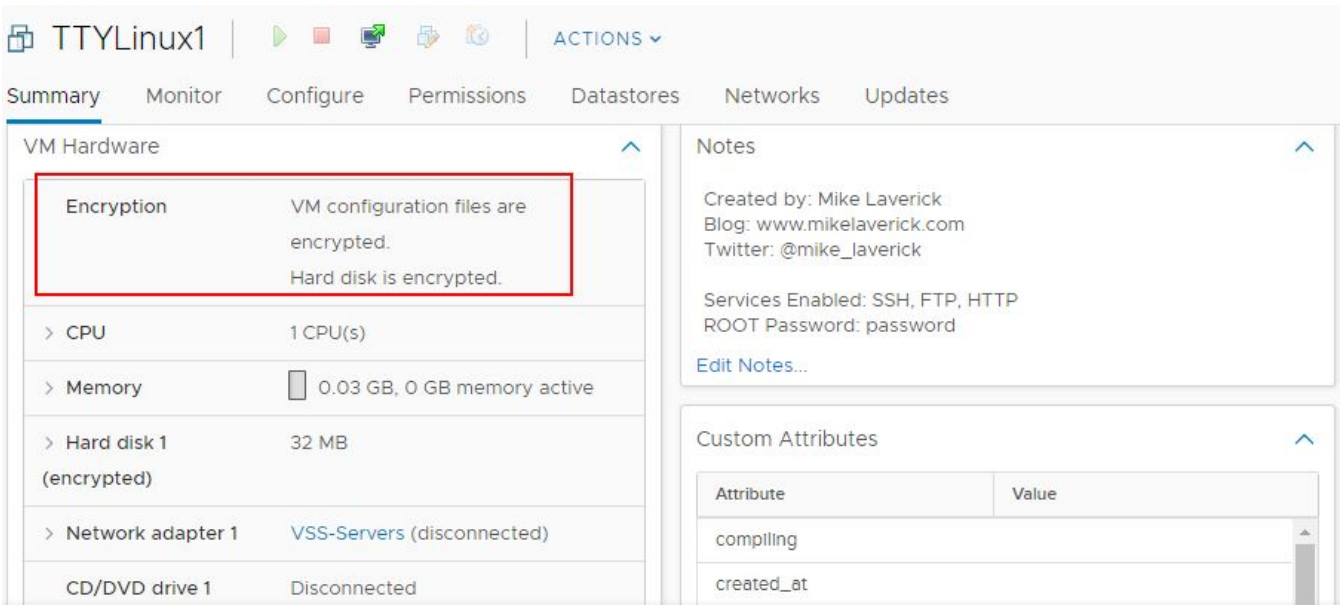
Enabling encryption with a VM Storage Policy

In the Edit VM Storage Policies dialog box, choose the VM Encryption Policy to enable encryption on the virtual machine disk(s). Note how you can granularly assign storage policies, including encryption on a per disk basis.



Assigning a VM Encryption Policy for a VM disk

After assigning the VM encryption policy, you will see the Encryption section under the virtual machine properties populated with the status of VM configuration files are encrypted. Hard disk is encrypted.



After assigning the VM encryption storage policy, the VM is now encrypted

Implementing Virtualization-based Security (VBS)

How does virtualization-based security raise the bar of security to make it more difficult for attackers to obtain this type of information? Virtualization-based security when implemented in Windows 10 or Windows Server 2016 and higher, uses hardware-assisted virtualization capabilities to create an isolated environment, separate from the operating system, to store sensitive system information.

Microsoft implements this feature in a rather ingenious way by utilizing the Hyper-V hypervisor to host the operating system to create this virtual secure mode which allows enforcing restrictions and protecting system and other operating system resources. Additionally, it is able to protect security information such as authenticated user credentials. When thinking about a system being compromised by malware or other malicious code, when virtualization-based security is being used, the damage that can be inflicted and information that can be stolen by the malware infecting the system can be greatly limited. Even if the malware has control of the OS kernel the underlying Hyper-V hypervisor can protect the sensitive areas of the system from being accessed by the malware.

VBS enables the following security mechanisms to harden your system and isolate key system resources from being compromised:

- Credential Guard – With Credential Guard, VBS can isolate and harden key system and user secrets against compromise
- Device Guard – Helps to prevent malware from being able to run on Windows operating systems
- Configurable Code Integrity
    - One mechanism that can be enabled with virtualization-based security is Hypervisor-Enforced Code Integrity (HVCI). Many of the effective security mechanisms that help to filter malicious code allow for enforcing code integrity checks. HVCI uses VBS to check all kernel-mode drivers and binaries before they are started and can prevent unsigned drivers or system files from loading into system memory. Similarly, there is a user-mode variant that enforces checks of applications before they are loaded and will only start those applications that are signed by known, approved signers.

- The Hyper-V hypervisor plays the mediator between applications and memory pages and the permissions that applications have to write across system memory. With these mechanisms in place, malware cannot modify memory and code pages cannot be modified or made executable.

The requirements for implementing Virtualization-based security are the following:

- 64-bit CPU
- Second Level Address Translation or SLAT
- Intel VT-D or AMD-Vi, ARM64 SMMUs
- TPM 2.0
- Firmware support for SMM protection
- UEFI Memory Reporting
- Secure Memory Overwrite Request
- Hypervisor Code Integrity or HVCI compatible drivers

Virtualization-based Security Best Practices

What are some best practices when it comes to implementing Windows Virtualization-based security in the context of VMware virtual machines? The following considerations need to be made.

- VBS Hardware – You need the following Intel hardware for VBS
  - Haswell CPU or later
  - Not all VBS functionality is available on AMD CPUs
- Windows Guest OS Compatibility – The following operating systems are supported in the context of VBS running inside of vSphere 6.7:
  - Windows 10 and Server 2016
- Unsupported VMware Features with Virtual Machines that have VBS enabled
  - Fault tolerance
  - PCI passthrough
  - Hot add of CPU or memory

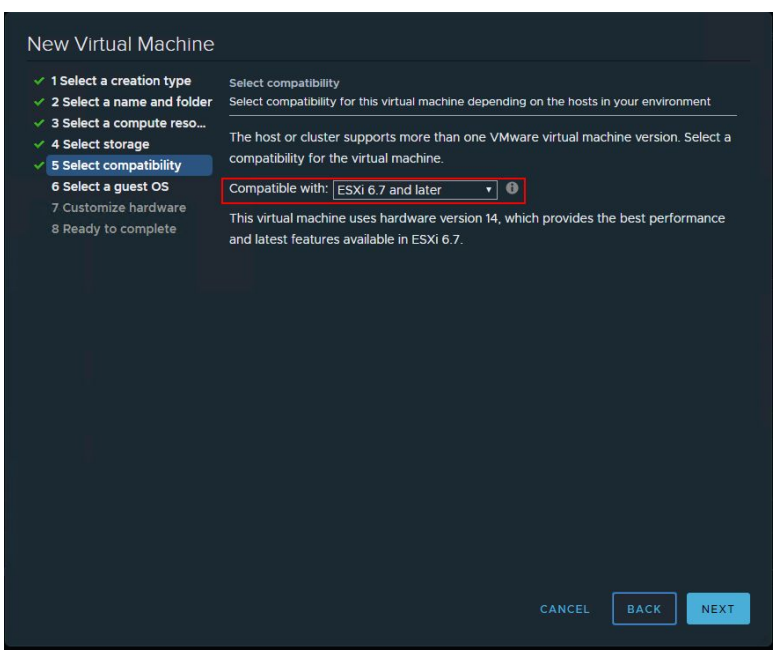
- Installation and Upgrade considerations:
  - If Virtual machine versions less than VM version 14 are used with Windows 10 and Windows Server 2016, you must reinstall the operating system if you change to UEFI from BIOS.
  - If migrating virtual machines from previous vSphere releases to vSphere 6.7 and higher and plan on enabling VBS in the future, use UEFI to avoid an OS reinstall after the upgrade.

Enabling Virtualization-Based Security in VMware vSphere

The new virtualization-based security feature that is found in VMware vSphere 6.7 and higher can be enabled at the virtual machine level inside the vSphere client. In fact, you have to enable the feature at the virtual machine level first, and then enable the feature inside of the Windows operating system.

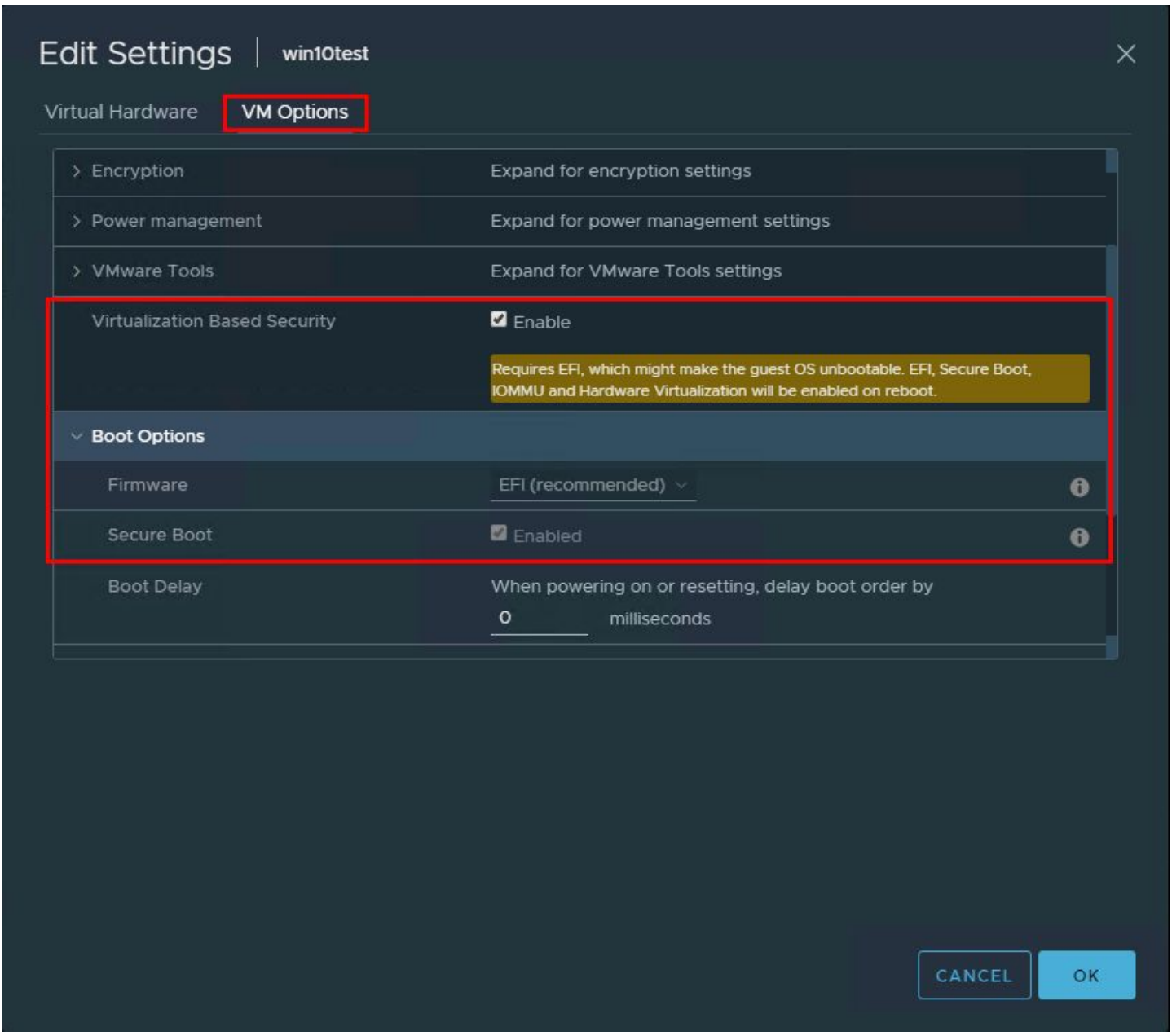
Enable Virtualization-Based Security on the VMware vSphere virtual machine:

When you create a new virtual machine, the step, **Select Compatibility** needs to be configured for **ESXi 6.7 and later** to be able to configure the virtualization-based security mechanism.



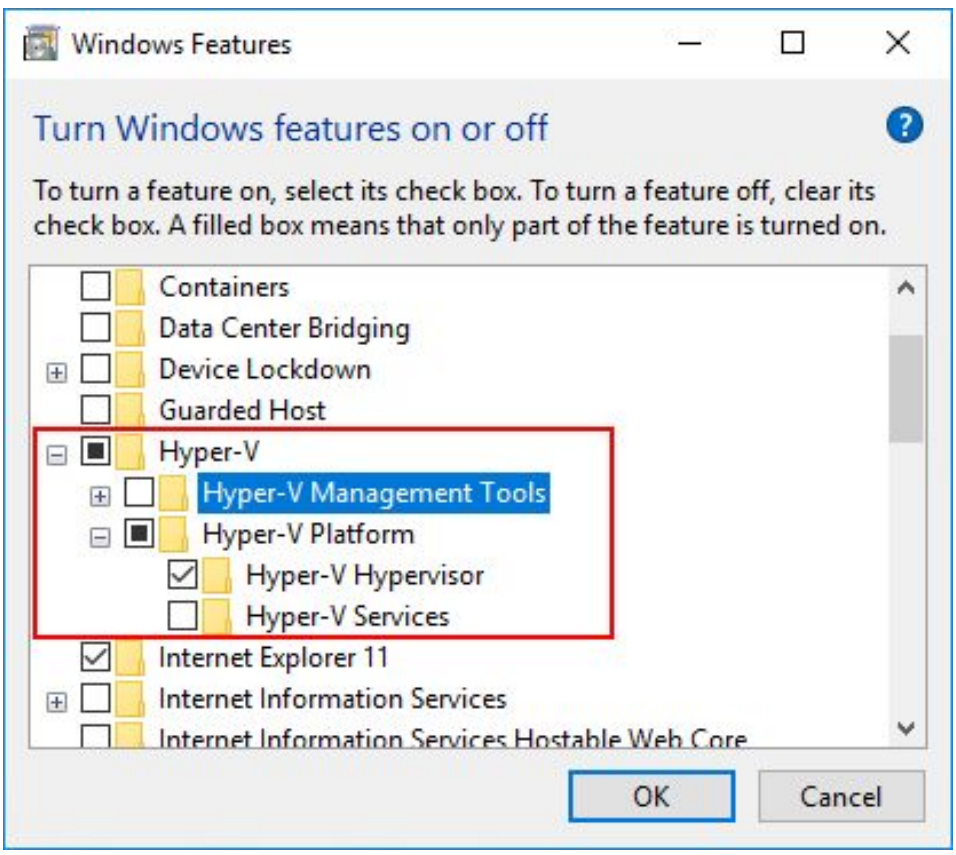
Configure the compatibility level of the vSphere virtual machine to take advantage of VBS

Once you have created a new virtual machine, go into the properties of the virtual machine and click the VM Options tab. Look for the Virtualization Based Security section. Place a checkbox in the Enable field. Also, make sure the Secure Boot is enabled and UEFI.



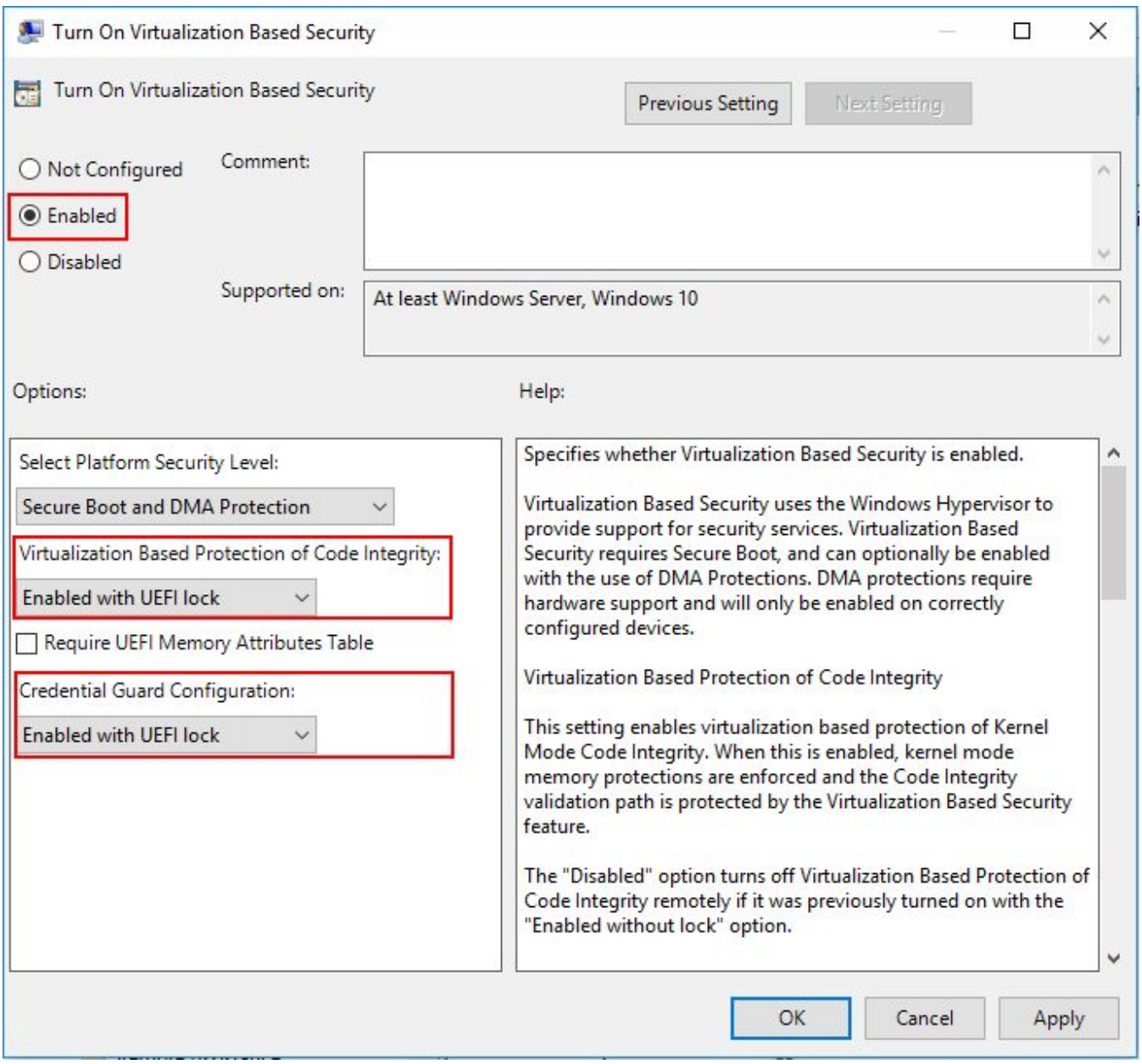
Enabling the Virtualization-Based Security feature in VM Options

Now, it is simply a matter of installing the Hyper-V feature and configuring VBS.



Install Hyper-V hypervisor in Windows

Navigate to Computer Configuration >> Administrative Templates >> System > Device Guard >> Turn On Virtualization Based Security



Configure the VBS options as needed in the policy configuration

VMware vSphere Virtual Trusted Platform Module or vTPM

How does the "virtual" Trusted Platform Module or vTPM work? The vTPMs allow performing cryptographic coprocessor capabilities in the software layer. A huge focus in security today is separating out and isolating very sensitive components in software from the operating system. Malware and other malicious code looking to steal sensitive information from a target system often achieve this by the lack of barriers implemented with some of the secure and vulnerable processes from normal operating system accessible memory. With the vTPM, a separate, secure, and isolated area exists for cryptographic keys to be stored that can be used to attest to the state of the system and the software running on it.

This technology is implemented in VMware vSphere 6.7 and can be added to a new virtual machine and even retro added to an existing virtual machine. When you add the vTPM device to a virtual machine, the VM files are encrypted as this is where the ultra-secure TPM data is housed. The disks are not encrypted as part of this process. However, disk encryption can be added at the same time or later. It is important to note, there is no special storage policy that is associated with the vTPM virtual hardware or that is implemented when this is added to a VM.

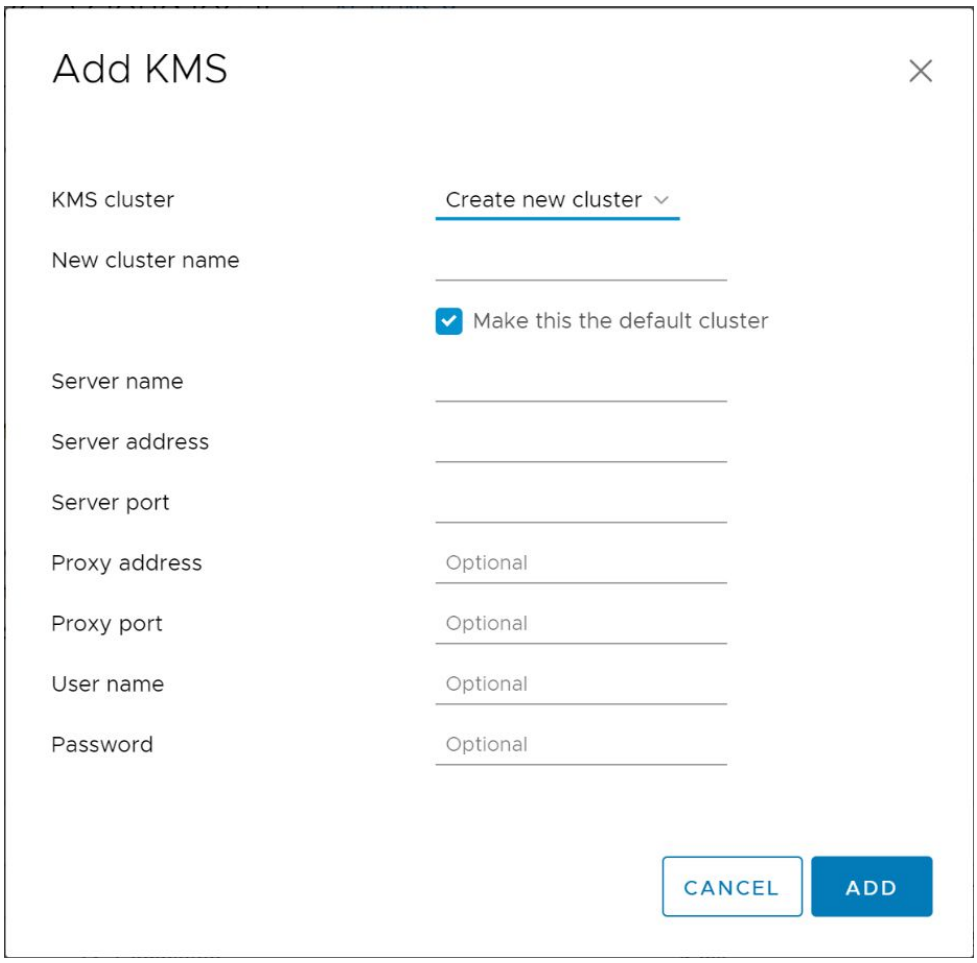
Many have had experience with some type of encryption used in conjunction with a VM in the past. This can certainly affect backups and the ability to create and restore backups. Can you backup a VM that has the vTPM module added, where the VM home files have been encrypted, as they are by default? Yes, you can. A couple of important considerations need to be made when thinking about the vTPM module and data protection. It is critical to backup all of the VM files including the *.nvram file as this contains the encryption keys used in conjunction with vTPM. Also, make sure to have the encryption key convenient when you perform a restore operation on a vTPM enabled virtual machine.

One might think that you would need a physical TPM attached to the virtual host for allowing the capability to add the vTPM. This is not the case. In fact, you can add the vTPM to a virtual machine running on a host that does not have a valid TPM module installed.

Differences between a Physical TPM and a Virtual TPM

A hardware-based TPM is well, hardware that provides the ability to provide secure storage for keys or credentials. A **virtual** TPM device provides the same functionality, except inside software. How does this work and how is it secured? The vTPM device is able to provide a secure location for storing these types of information by using the **.nvram** file to store the secure cryptographic information on disk and securing this file using virtual machine encryption. Again, the home files of the VM, including the .nvram file are encrypted and not the virtual disk files. While a physical TPM has the cryptographic information including the public and private key, the vTPM device gets the key information initially from VMware Certificate authority or from another third-party certificate authority. While the keys in the virtual TPM could be changed, this would invalidate the existing sensitive information in the vTPM and is generally not done.

The VMware encryption process for virtual machines is enabled by the use of a Key Management Server cluster. The KMS cluster is added into vSphere and then the trust with the KMS cluster is verified to allow the provisioning of encryption keys. To be able to be used, the KMS cluster needs to be able to support the Key Management Interoperability Protocol (KMIP) 1.1.



Adding a new Key Management Server cluster in VMware vSphere

Requirements for vTPM

To use a vTPM, your vSphere environment must meet these requirements:

Virtual machine requirements:

- EFI firmware
- Hardware version 14

Component requirements:

- vCenter Server 6.7 or 6.7 Update 1
- Virtual machine encryption (to encrypt the virtual machine home files).
- Key Management Server (KMS) configured for vCenter Server (virtual machine encryption depends on KMS).

Guest OS support:

- Windows Server 2019 (64 bit)
- Windows Server 2016 (64 bit)
- Windows 10 (64 bit)

Adding the Virtual TPM Module to a Virtual Machine

The process to add a vTPM to a new virtual machine is a straightforward process. You first need to make sure all the prerequisite steps have been performed with adding the KMS cluster to VMware vSphere and establishing trust. The guest operating system needs to run the required version of Windows including Windows 10, Server 2016 or 2019. Make sure the VM has also been configured to use EFI firmware.

On the **Customize Hardware** step of creating a new virtual machine process:

- Click **Add New Hardware** and select Trusted Platform Module.

The process is similar to an existing virtual machine. You will simply need to **Add New Hardware** and add the Trusted Platform Module. Remember however that the firmware will need to be EFI firmware which if not already configured this way will require a reload of the operating system.

What is the Virtual Networking Layer?

The VMware vSphere Virtual Networking Layer contains the virtual network adapters, virtual switches or vSwitches, distributed virtual switches or DVS switches, ports, and port groups. VMware vSphere ESXi uses this virtual networking layer to enable communication from the virtual layer to the physical network layer all the way up the OSI stack to the end user and their applications. Additionally, the virtual networking layer allows communication with storage devices such as iSCSI SANs, NAS storage, and so forth.

The VMware vSphere ESXi hypervisor includes extremely secure virtual networking capabilities that allow very secure network communication when configured correctly. Also, it allows for granular controls of each element of the virtual networking layer of the components listed above.

Aside from the secure nature of the VMware vSphere ESXi hypervisor and the virtual networking layer constructs that enable secure virtual network communication, there are other best practices that allow for securing the virtual networking layer. Let's take a look at these best practices and how they can be implemented.

Securing VMware vSphere Virtual Networking Layer

There are many best practices in regards to securing VMware vSphere Virtual Networking and the various components therein. Let's take a look at the following configurations and best practices that can help to secure the virtual network layer in a VMware vSphere environment.

- Isolating network traffic
- Use firewalls to secure virtual network elements
- Consider network security policies
- Secure VM networking
- Use VLANs to protect virtual networks
- Secure network communication with virtual storage
- Use IPSec when possible

We will look at each of the above security mechanisms a bit closer to see how they can help with securing VMware vSphere virtual networking for production workloads.

Isolate Network Traffic

On any network, there are generally different kinds of traffic that are traversing that network. Isolating network traffic based on the type of traffic is a great general guideline to creating good security boundaries on a network. Generally, this is accomplished by using VLANs and different subnets for various kinds of traffic. In the virtual environment, this guideline holds true as well. In any VMware vSphere environment, there are many different kinds of traffic that are needed for proper communication with the compute, storage, and networks of the configuration. Typically, you have management, storage, vMotion, and VM network traffic in a general vSphere installation. Additionally, in the VM network traffic realm, there may be many different kinds of workloads that need to be isolated from one another using different network segments, virtual switches, VLANs, subnets, etc.

Use Firewalls to Secure Virtual Network Elements

One of the common means of securing networks is using firewalls for filtering traffic. Firewalls can be used across the VMware vSphere environment. Firewalls can be used to filter VM network traffic. Also, the ESXi host itself has built-in firewall capabilities that allow allowing or disallowing communication to certain ports, IP addresses, etc. VMware vCenter Server also has the capabilities to allow communication via firewall mechanisms. All of these capabilities allow securing network traffic across the virtual networking layers.

Consider Network Security Policies

The built-in VMware vSphere virtual switches including the Standard vSwitch and the Distributed vSwitch have the ability to protect traffic against such malicious activities as unwanted port scanning, MAC address impersonation, and others. The security policy as implemented at the virtual switch layer is a Layer 2 construct that has three components: promiscuous mode, MAC address changes, and forged transmits.

Secure VM Networking

When thinking about the virtual machine running in a VMware vSphere environment, there are many features that can be used to secure virtual networking traffic. These include many of the capabilities we have already mentioned at the virtual switch layer. Additionally, the guest operating system of a virtual machine can also be used to filter traffic using built-in firewall and other security features such as Windows Firewall which can block or allow certain types of traffic. Used in conjunction with the default VMware vSphere security mechanisms, these can add to a powerful overall security stance for guest operating systems running on top of vSphere.

Use VLANs to Protect Virtual Networks

The VLAN construct in networking is defined by the 802.1q IEEE standard that serves to segment physical networks into different broadcast domains. The VLAN tag is added to the packet header and only allows communication between VMs that have the same VLAN tag. So, two different VMs can be isolated from one another by using different VLANs for each. This provides an effective way to segment and isolated various kinds of traffic. The VMware vSphere virtual networking stack is fully 802.1q aware so you can make use of VLANs all along the way. This can be done at the physical switch port, virtual switch port, or VLAN guest tagging.

Secure Virtual Storage Network Traffic

Virtual storage is where your actual data resides with virtual machines running inside of VMware vSphere. This is performed by the VMFS file system that resides on top of your LUNs. If virtual storage is compromised by an attacker, they have access to the heart of your infrastructure – your data. By using different techniques such as isolating storage traffic on separate physical and logical networks as well as using CHAP authentication in iSCSI environments, storage networks can be effectively secured.

Use IPSec when Possible

IPSec is Internet Protocol Security and is a network security mechanism that authenticates and encrypts packets of data sent over an IP network. IPSec may not be feasible or even possible in certain network segments, however, its use should be considered to provide the most secure communication possible when security is a must. Used in conjunction with all the other mechanisms and technologies listed, it can help ensure network communication is as secure as possible.

Securing VMware vSphere 6.7 Update 1 Virtual Machine Best Practices

When it comes down to the purpose of a hypervisor, it is to run virtual machines. The virtual machine generally speaking performs the primary role of serving out production data and services. These may include serving out files, databases, email services, or applications. Aside from securing the hypervisor itself, there are virtual machine security considerations to be made in VMware vSphere 6.7 that need to be taken into account and implemented to ensure the virtual machine itself is properly secured. Let's take a look at the following points for consideration with virtual machine security in VMware vSphere 6.7.

- General Virtual Machine Protection
- Deploying VMs using Templates
- Securing the VM Console in vSphere
- Limiting VM resource usage
- Disabling unnecessary VM functions
- Use Virtualization-Based Security and vTPM 2.0

Let's examine each of these in a bit more depth to understand how they allow for better security at the virtual machine level.

General Virtual Machine Protection

When we thinking about a virtual machine, there can be a misconception in perception that a VM is a totally different entity than a physical server. However, this is generally not the case when it comes to general best practices within the guest operating system. This includes making sure the following are in place:

- Guest operating system patching – The guest operating system running inside a virtual machine, like a physical server, needs to be patched regularly with Windows or Linux guest operating system patches. Applying operating system patches is one of the best protections against many exploits which tend to compromise known vulnerabilities that these patches resolve. Keeping pates up to data ensures the best security within the guest VM from an operating system perspective.
- Antimalware Software – VMs like physical nodes typically need to have some type of antimalware software in place to ensure scanning and remediation of any malware that may be found on the guest operating system. Ensuring the antimalware software is up-to-date and scanning properly is also a priority when thinking about security.
- Controlling Serial port access – Serial ports allow for connecting physical devices to virtual machines and can be connected via passing these devices through from the host to the VM. Serial port connecting can allow low-level access to a VM which may be concerning from a security standpoint. Limiting VMs that have serial port access and those to have access to connect these devices to VMs certainly is a best practice from a security st

Deploying VMs using Templates

In thinking about the security of virtual machines, deploying virtual machines via templates may not rank high on the list of security objectives. However, using templates to deploy virtual machines is a security best practice. Why? Each time an operating system is loaded by hand manually and applications are installed in this way, there is a risk that something can get missed on each subsequent system that is provisioned. In using a virtual machine template, you are creating a “master” generalized image of a VM and then deploying each subsequent VM from that master image. As long as the master image is verified from an installation and security standpoint, you can be confident that each VM provisioned from the master VM, will contain the same installed software, applications, security patches, and other configuration that makes for verifying the resulting VM is configured correctly and secured.

Securing the VM Console in vSphere

The VM Console is a powerful mechanism for managing a virtual machine inside of VMware vSphere. The VM Console is equivalent to having a monitor connected to a server. In the VMware vSphere environment, users with access to the console, also have access to the power management as well as the ability to connect and disconnect devices, media, etc. So, it can truly be a dangerous vehicle for administration in the wrong hands. What is recommended from a security best practices standpoint?

- Use remote management software to access guest operating systems running inside a virtual machine. These may include Microsoft Remote Desktop for Windows virtual machines or SSH for virtual machines running Linux.
- Grant VM Console access only when necessary and limit the access of the VM Console to only 1 connection per the security configuration best practice recommendation.

<u>Procedure to limit the number of VM Console connections:</u>

1. Find the virtual machine in the vSphere Web Client inventory.
    a. To find a virtual machine, select a datacenter, folder, cluster, resource pool, or host.
    b. Click the Related Objects tab and click Virtual Machines.
2. Right-click the virtual machine and click Edit Settings.
3. Select VM Options.
4. Click Advanced and click Edit Configuration.
5. Add or edit the parameter **RemoteDisplay.maxConnections** and set the value to 1.
6. Click OK.

Limiting VM resource usage

By default, in VMware vSphere, a virtual machine can take as many resources as needed by using the configured hardware that is contained on the virtual machine. All VMs share resources equally. If a particular virtual machine is able to consume so many resources that other virtual machines on the host have degraded performance or are no longer able to function, a Denial of Service attack using a VM could happen.

To circumvent this as a possibility, Shares and resource pools can be used to prevent a denial of service attack that could allow one virtual machine to consume all available resources. To do this:

1. Right-size virtual machines with only the needed resources in the vSphere environment
2. Use shares to guarantee resources to critical VMs
3. Group virtual machines with similar resources requirements into resource pools
4. Within each resource pool, leave the shares set to the default value to ensure each VM has the same resource priority
5. This will ensure that a single VM will not be able to monopolize resource usage on the vSphere ESXi host

Disabling unnecessary VM functions

In the context of security, disabling unnecessary VM functions serves a meaningful purpose. When looking at a virtual machine when compared to a physical server, one of the differences is a virtual machine generally does not require as many functions or services as a physical server. Eliminating anything that is not needed within a VM lessens the attack surface and the security vulnerabilities that may be attached to those unnecessary functions. What may be included in unnecessary functions?

- Unused services – Common services such as file services or web services should not be running inside a VM unless they are needed
- Unused physical devices – Attached CD/DVD drives, floppy drives, USB, serial and other ports should be disconnected or removed unless they are being used/needed
- Unused functionality – VMware shared folders and copy/paste operations should be disabled unless needed
- Screensaver – Disable screensaver
- Do not run X Windows on top of Linux if not needed – This creates security vulnerabilities unless it is needed.

By lessening the attack surface and eliminating unnecessary functions, the security posture of the virtual machine is greatly increased.

Use Virtualization-Based Security and vTPM 2.0

- New with vSphere 6.7 is the ability to utilize Virtualization-Based Security which allows vSphere virtual machines to be compatible with Microsoft's new VBS security in Windows 10 and Windows Server 2016 and higher. This allows for a hypervisor protected space where credentials and other sensitive information are stored which makes it exponentially more difficult for an attacker to steal credentials.
- Virtual TPM is now possible with vSphere 6.7 VMs which allows greatly enhancing the security features of a guest VM. The vTPM functionality allows adding a virtualized TPM 2.0 compatible module to a VM running inside vSphere 6.7. The guest OS uses the vTPM module to store sensitive information, provide cryptographic operations and attest to the integrity of the VM platform.

White Paper Takeaways

Security is one of the key elements of today's infrastructure and must be considered in each layer of today's business-critical systems. VMware vSphere 6.7 Update 1 provides key new security features that allow taking the security of today's infrastructure to the next level. In considering securing VMware vSphere 6.7 Virtual Machine Best Practices, there are many great ways to ensure the maximum-security posture of vSphere VMs running production workloads. Many of these security best practices align with traditional physical security and guest operating system security. However, there are new features in vSphere 6.7 such as virtualization-based security and Virtual TPM 2.0 that allow taking advantage of new security technology to greatly enhance security across the landscape of the virtual machines running in production. By implementing both the traditional virtual machine security methodologies and the new technology found in VMware vSphere 6.7, organizations can have a secure virtual machine platform that can bolster confidence in data security.