

VCP 2020 v7 Edition Study Guide

Introduction	4
Section 1 – Architectures and Technologies	4
Objective 1.1 – Identify the pre-requisites and components for a vSphere Implementation	4
ESXi Server	4
vCenter Server	6
Objective 1.2 Describe vCenter Topology.....	7
Objective 1.3 - Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.) .	8
Objective 1.3.1 – Describe datastore types for vSphere	9
Objective 1.3.2 – Explain the importance of advanced storage configuration (VASA, VAAI, etc.).....	10
Objective 1.3.3 – Describe Storage Policies.....	10
Objective 1.3.4 – Describe basic storage concepts in K8s, vSAN, and vSphere Virtual Volumes (vVols)	10
Objective 1.4 – Differentiate between vSphere Network I/O Control (NIOC) and vSphere Storage I/O Control (SIOC)	12
Objective 1.5 – Describe instant clone architecture and use cases.....	14
Objective 1.6 – Describe Cluster Concepts	14
A vSphere cluster is a group of ESXi host machines. When grouped, vSphere aggregates all of the resources of each host and treats it as a single pool. There are several features and capabilities you can only do with clusters.	14
Objective 1.6.1 – Describe Distributed Resource Scheduler	15
Objective 1.6.2 – Describe vSphere Enhanced vMotion Compatibility (EVC)	15
Objective 1.6.3 – Describe how Distributed Resource Scheduler (DRS) scores virtual machines.....	15
Objective 1.6.4 – Describe vSphere High Availability	15
Objective 1.7 – Identify vSphere distributed switch and vSphere standard switch capabilities	16
Objective 1.7.1 – Describe VMkernel Networking.....	19
Objective 1.7.2 – Manage networking on multiple hosts with vSphere distributed switch.....	20
Objective 1.7.3 – Describe Networking Policies	30
Objective 1.7.4 – Manage Network I/O Control on a vSphere distributed switch	33
Objective 1.8 – Describe vSphere Lifecycle Manager concepts (baselines, cluster images, etc.)	34
Objective 1.9 – Describe the basics of vSAN as primary storage.....	36
Objective 1.9.1 – Identify basic vSAN requirements (networking, disk count, type)	36
Objective 1.10 – Describe vSphere Trust Authority Architecture.....	37
Objective 1.11 – Explain Software Guard Extensions (SGX)	37
Section 2 – VMware Products and Solutions	37
Objective 2.1 – Describe the role of vSphere in the software-defined data center (SDDC).....	37

Objective 2.2 – Identify use cases for vCloud Foundation.....	38
Objective 2.3 – Identify migration options	39
Objective 2.4 – Identify DR use cases	41
Objective 2.5 – Describe vSphere integration with VMware Skyline	43
Section 4 – Installing, Configuring, and Setup	43
Objective 4.1 – Describe single sign-on (SSO) deployment topology.....	43
Objective 4.1.1 – Configure a single sign-on (SSO) domain.....	44
Objective 4.1.2 – Join an existing single sign-on (SSO) domain	44
Objective 4.2 – Configure VSS advanced virtual networking options.....	45
Objective 4.3 – Setup identity sources	47
Objective 4.3.1 – Configure Identity Federation	56
Objective 4.3.2 – Configure Lightweight Directory Access Protocol (LDAP) integration.....	60
Objective 4.3.3 – Configure Active Directory integration.....	62
Objective 4.4 – Deploy and configure vCenter Server Appliance	62
Objective 4.5 – Create and configure VMware High Availability and advanced options (Admission Control, Proactive High Availability, etc.)	75
Objective 4.6 – Deploy and configure vCenter Server High Availability.....	81
Objective 4.7 – Set up a content library	86
Objective 4.8 – Configure vCenter Server file-based backup	92
Objective 4.9 – Analyze basic log output from vSphere products.....	97
Objective 4.10 – Configure vSphere Trust Authority	102
Objective 4.11 – Configure vSphere certificates.....	103
Objective 4.11.1 – Describe Enterprise PKIs role for SSL certificates	106
Objective 4.12 – Configure vSphere Lifecycle Manager/VMware Update Manager (VUM)	106
Objective 4.13 – Securely Boot ESXi hosts.....	110
Objective 4.14 – Configure different network stacks	111
Objective 4.15 – Configure Host Profiles	115
Objective 4.16 – Identify boot options	123
Objective 4.16.1 – Configure Quick Boot.....	126
Section 5 – Performance-tuning, Optimization, Upgrades	128
Objective 5.1 – Identify resource pools use cases	128
Objective 5.1.1 – Explain shares, limits, and reservations (resource management).....	133
Objective 5.2 – Monitor resources of vCenter Server Appliance and vSphere environment	134
Objective 5.3 – Identify and use tools for performance monitoring	137
Objective 5.4 – Configure Network I/O Control (NIOC).....	140

Objective 5.5 – Configure Storage I/O Control (SIOC)	141
Objective 5.6 – Explain the performance impact of maintaining virtual machine snapshots.....	143
Objective 5.7 – Plan for upgrading various vSphere components.....	144
Section 6 – Troubleshooting and Repairing - There are no testable objectives for this section.....	144
Section 7 – Administrative and Operational Tasks	144
Objective 7.1 – Create and manage virtual machine snapshots.....	144
Objective 7.2 – Create virtual machines using different methods (Open Virtual Machine Format (OVF) templates, content library, etc.)	148
Objective 7.3 – Manage virtual machines.....	149
Objective 7.4 – Manage storage (datastores, storage policies, etc.).....	150
Objective 7.4.1 – Configure and modify datastores (expand/upgrade existing datastore, etc.)	158
Objective 7.4.2 – Create virtual machine storage policies	159
Objective 7.4.3 – Configure storage cluster options	159
Objective 7.5 – Create Distributed Resource Scheduler (DRS) affinity and anti-affinity rules for everyday use cases.....	167
Objective 7.6 – Configure and perform different types of migrations	169
""Objective 7.7 – Configure role-based user management	174
'Objective 7.8 – Configure and manage the options for securing a vSphere environment (certificates, virtual machine encryption, virtual Trusted Platform Module, lockdown mode, virtualization-based security, etc.).....	179
Objective 7.9 – Configure and manage host profiles.....	186
""Objective 7.10 – Utilize baselines to perform updates and upgrades	193
Objective 7.11 – Utilize vSphere Lifecycle Manager.....	200
Objective 7.11.1 – Describe Firmware upgrades for ESXi.....	204
Objective 7.11.2 – Describe ESXi updates.....	204
Objective 7.11.3 – Describe component and driver updates for ESXi	205
Objective 7.11.4 – Describe hardware compatibility check	207
Objective 7.11.5 – Describe ESXi cluster image export functionality	208
Objective 7.12 – Configure alarms.....	210

Introduction

Hello again. My 2019 VCP Study Guide was well received, so, to help the community further, I decided to embark on another exam study guide with vSphere 7. This guide is exciting for me to write due to the many new things I'll get to learn myself, and I look forward to learning with everyone.

I am writing this guide pretty much how I talk and teach in real life with a bit of Grammarly on the back end, to make sure I don't go completely off the rails. You may also find the formatting a little weird. This is because I plan on taking this guide and binding it in a single guide at the end of this blog series. I will try to finish a full topic per blog post unless it gets too large. I don't have a large attention span to read huge technical blogs in one sitting and find most people learn better with smaller chunks of information at a time. (I wrote this before I saw the first section.)

In these endeavors, I personally always start with the Exam Prep guide. That can be found on VMware's website [here](#). The official code for this exam is 2V0-21.20, and the cost of the exam is \$250.00. There is a total of 70 questions with a duration of 130 minutes. The passing score, as always, is 300 on a scale of 1-500. The exam questions are presented in a single and multiple-choice format. You can now take these exams online, in the comfort of your own home. A webcam is required, and you need to pan your webcam at the beginning of the session, and it needs to be on the whole time.

The exam itself focuses on the following topics:

- Section 1 – Architecture and Technologies
- Section 2 – Products and Solutions
- Section 3 – Planning and Designing
- Section 4 – Installing, Configuring, and Setup
- Section 5 – Performance-tuning, Optimization, and Upgrades
- Section 6 – Troubleshooting and Repairing
- Section 7 – Administrative and Operational Tasks

Each of these topics can be found in the class materials for Install, Configure, and Manage, or Optimize and Scale classes, or supplemental papers by VMware on the web. Let's begin with the first topic.

Section 1 – Architectures and Technologies

Objective 1.1 – Identify the pre-requisites and components for a vSphere Implementation
A vSphere implementation or deployment has two main parts. ESXi server and vCenter Server.

ESXi Server

The first is the virtual server itself or ESXi server. The ESXi host server is the piece of the solution that allows you to run virtual machines and other components of the solution (such as NSX kernel modules). It provides the compute, memory, and in some cases, storage resources for a company to run. There are requirements the server needs to meet for ESXi. They are:

- A supported hardware platform. VMware has a compatibility guide they make available [here](#). If running a production environment, your server should be checked against that.
- ESXi requires a minimum of two CPU cores.
- ESXi requires the NX/XD or No Execute bit enabled for the CPU. The NX/XD setting is in the BIOS of a server.

- ESXi requires a minimum of 4 GB of RAM. It would be best if you had more to run a lot of the workloads a business requires, however.
- The Intel VT-x or AMD RVI setting in the BIOS must be enabled. Most of the time, this is already enabled on servers, and you won't need to worry about it.
- 1+ Gigabit network controller is a requirement. Using the compatibility guide above, make sure your controller is supported.
- SCSI disk or RAID LUN. Because of their higher reliability, ESXi calls them "local drives," and you can use them as a "scratch" volume. A scratch partition is a disk partition used by VMware to host logs, updates, or other temporary files.
- SATA drives. You can use these but are labeled "remote" drives. Because of being labeled "remote," you can't use them for a scratch partition.

vSphere 7.0 can be installed using UEFI BIOS mode or regular old BIOS mode. If using UEFI, you have a wider variety of drives you can use to boot. Once you use one of those modes (UEFI or Legacy) to boot from, it is not advisable to try to change after installed. If you do, you may be required to reinstall. The error you might receive is "Not a VMware boot bank."

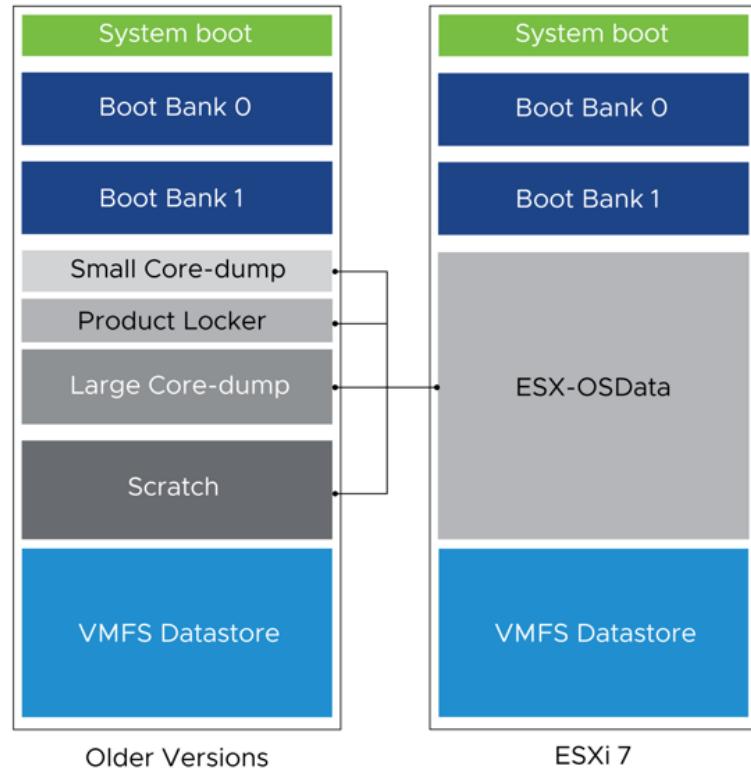
One significant change in vSphere 7.0 is system storage requirements. ESXi 7.0 system storage volumes can now occupy up to 138 GB of space. A VMFS datastore is only created if there is an additional 4 GB of space. If one of the "local" disks aren't found, then ESXi operates in a degraded where the scratch disk is placed in a RAMDISK or all in RAM. This is not persistent through reboots of the physical machine and displays an unhappy message until you specify a location for the scratch disk.

Now that being said, you CAN install vSphere 7 on a USB as small as 8 GB. You should, if at all possible, use a larger flash device. Why? ESXi uses the additional space for an expanded core dump file, and it uses the other memory cells to prolong the life of the media. So try to use a 32 GB or larger flash device.

With the increased usage of flash media, VMware saw fit to talk about it in the install guide. In this case, it specifically called out using M.2 and other Non-USB low-end flash media. There are many types of flash media available on the market that have different purposes. Mixed-use case, high performance, and more. The use case for the drive should determine the type bought. VMware recommends you don't use low-end flash media for datastores due to VMs causing a high level of wear quickly, possibly causing the drives to fail prematurely.

While the guide doesn't ask to call this out, I thought it would be a good thing to show a picture of how the OS disk layout differs from the previous version of ESXi. You should know that when you upgrade the drive from the previous version, you can't rollback.

New OS Disk Layout



vCenter Server

The ESXi has the resources and runs the virtual machines. In anything larger than a few hosts, management becomes an issue. vCenter Server allows you to manage and aggregate all your server hardware and resources. But, vCenter Server allows you to do so much more. Using vCenter Server, you can also keep tabs on performance, licensing, and update software. You can also do advanced tasks such as move virtual machines around your environment. Now that you realize you MUST have one, let's talk about what it is and what you need.

vCenter is deployed on an ESXi host. So, you have to have one of those running first. It is deployed using its included installer to the ESXi host, not as you would an OVA. The machine itself is upgraded from previous versions. It now contains the following:

- Photon OS 3.0 – This is the Linux variant used by VMware
- vSphere authentication services
- PostgreSQL (v11.0) – Database software used
- VMware vSphere Lifecycle Manager Extension
- VMware vSphere Lifecycle Manager

But wait... there used to be the vSphere vCenter Server and Platform Services? You are correct. In the future, due to design flows and simplicity, etc., VMware combined all services into a single VM. So what services are actually on this machine now? I'm glad you asked.

- Authentication Services – which includes
 - vCenter Single Sign-On
 - vSphere License Service
 - VMware Certificate Authority
- PostgreSQL
- vSphere Client -HTML5 client that replaces the previous FLEX version (Thank God)
- vSphere ESXi Dump Collector – Support tool that saves active memory of a host to a network server if the host crashes
- vSphere Auto Deploy – Support tool that can provision ESXi hosts automatically once setup for it is completed
- VMware vSphere Lifecycle Manager Extension – tool for patch and version management
- VMware vCenter Lifecycle Manager – a tool to automate the process of virtual machines and removing them

Now that we have covered the components let's talk deployment. You can install vCenter Server using either the GUI or CLI. If using the GUI install, there are two stages. The first stage installs the files on the ESXi host. The second stage configures parameters you feed into it. The hardware requirements have changed from the previous version as well. Here is a table showing the changes in green.

Deployment Size	6.7 CPU	7.0 CPU	6.7 RAM	7.0 RAM	6.7 DISK	7.0 DISK
Tiny	2	2	10 GB	12 GB	300 GB	315 GB
Small	4	4	16 GB	19 GB	340 GB	380 GB
Medium	8	8	24 GB	28 GB	525 GB	600 GB
Large	16	16	32 GB	37 GB	740 GB	965 GB
X-Large	24	24	48 GB	56 GB	1180 GB	1705 GB

Objective 1.2 Describe vCenter Topology

Topology is a lot simpler to talk about going forward because there is a flat topology. There is no vCenter Server service and Platform Controllers anymore. Everything is consolidated into one machine. If you are running a previous version and have broken vCenter Server out into those roles, don't despair! There are tools VMware has created that allow you to consolidate them back. There are a few things to add to that.

First, Enhanced Link Mode. This is where you can log into one vCenter and manage up to 15 total vCenter instances in a Single Sign-On domain. This is where the flat topology comes in. Enhanced Link Mode is set up during the installation of vCenter. Once you exceed the limits of a vCenter, you install a new one and link it. There is also vCenter Server High Availability. Later on, in this guide, we cover how its configured. For now, here is a quick overview of what it is.

vCenter High Availability is a mechanism that protects your vCenter Server against host and hardware failures. It also helps reduce downtime associated with patching your vCenter Server. It does this by using 3 VMs. It uses two full VCSA nodes and a witness node. One VCSA node is active and one passive. They are connected by a vCenter HA network, which is created when you set this up. This network is used to replicate data across and connectivity to the witness node.

For a quick look at vCenter limits compared to the previous version:

Metric	vCenter Server 6.7	vCenter Server 7.0
Hosts per vCenter Server	2,000	2,500
Hosts per cluster	64	64
Powered on VMs per vCenter Server	25,000	40,000
Registered VMs per vCenter Server	35,000	45,000
VM per cluster	8,000	8,000
Linked vCenter Server instances	15	15

Objective 1.3 - Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.)

The section I wrote in the previous guide still covers this well, so I am using that.

Local Storage

Local storage is storage connected directly to the server. This includes a Direct Attached Storage (DAS) enclosure that connects to an external SAS card or storage in the server itself. ESXi supports SCSI, IDE, SATA, USB, SAS, flash, and NVMe devices. You cannot use IDE/ATA or USB to store virtual machines. Any of the other types can host VMs. The problem with local storage is that the server is a single point of failure or SPOF. If the server fails, no other server can access the VM. There is a unique configuration that you can use that would allow sharing local storage, however, and that is vSAN. vSAN requires flash drives for cache and either flash or regular spinning disks for capacity drives. These are aggregated across servers and collected into a single datastore or drive. VM's are duplicated across servers, so if one goes down, access is still retained, and the VM can still be started and accessed.

Network Storage

Network Storage consists of dedicated enclosures that have controllers that run a specialized OS on them. There are several types, but they share some things in common. They use a high-speed network to share the storage, and they allow multiple hosts to read and write to the storage concurrently. You connect to a single LUN through only one protocol. You can use multiple protocols on a host for different LUNs

Fiber Channel or FC is a specialized type of network storage. FC uses specific adapters that allow your server to access it, known as Fiber Channel Host Bus Adapters or HBAs. Fiber Channel typically uses cables of glass to transport their signal, but occasionally use copper. Another type of Fiber Channel can connect using a regular LAN. It is known as Fiber Channel over Ethernet or FCoE.

iSCSI is another storage type supported by vSphere. This uses regular ethernet to transport data. Several types of adapters are available to communicate to the storage device. You can use a hardware iSCSI adapter or software. If you use a hardware adapter, the server offloads the SCSI and possibly the network processing. There are dependent hardware and independent hardware adapters. The first still needs to use the ESXi host's networking. Independent hardware adapters can offload both the iSCSI and networking to it. A software iSCSI adapter uses a standard ethernet adapter, and all the processing takes place in the CPU of the hosts.

VMware supports a new type of adapter known as iSER or iSCSI Extensions for RDMA. This allows ESXi to use RDMA protocol instead of TCP/IP to transport iSCSI commands and is much faster.

Finally, vSphere also supports the NFS 3 and 4.1 protocol for file-based storage. This type of storage is presented as a share to the host instead of block-level raw disks. Here is a small table on networked storage for more leisurely perusal.

Technology	Protocol	Transfer	Interface
Fiber Channel	FC/SCSI	Block access	FC HBA
Fiber Channel over Ethernet (FCoE)	FCoE / SCSI	Block access	Converged Network Adapter NIC with FCoE support
iSCSI	iSCSI	Block access	iSCSI adapter (dependent or independent) NIC (Software adapter)
NAS	IP / NFS	File level	Network adapter

Objective 1.3.1 – Describe datastore types for vSphere

vSphere supports several different types of datastores. Some of them have features ties to particular versions, which you should know. Here are the types:

- VMFS – VMFS can be either version 5 or 6. VMFS is the file system installed on a block storage device such as an iSCSI LUN or local storage. You cannot upgrade a datastore to VMFS 6 from 5. You have to create new and migrate VMs to it. On VMFS, vSphere handles all the locking of files

and controls access to them. It is a clustering file system that allows access of files to more than one host at a time.

- NFS – Version 3 and 4.1 are supported. NFS is a NAS file system accessed over a TCP/IP network. You can't access the same volume using both versions at the same time. Unlike VMFS, the NAS device controls access to the files.
- vSAN – vSAN aggregates local storage drives on a server into a single datastore accessible by the nodes in the vSAN cluster.
- vVol – A vVol datastore is a storage container on a block device.

Objective 1.3.2 – Explain the importance of advanced storage configuration (VASA, VAAI, etc.)

This is the first time I've seen this covered in an objective. I like that some of the objectives are covering more in-depth material. It's hard to legitimize the importance of them without describing them and what they do a bit. I will explain what they are and then explain why they are essential.

- VASA - VASA stands for vSphere APIs for Storage Awareness. VASA is extremely important because hardware storage vendors use it to inform vCenter Server about their capabilities, health, and configurations. VASA is essential for vVols, vSAN, and Storage Policies. Using Storage Policies and VASA, you can specify that VMs need a specific performance profile or configuration, such as RAID type.
- VAAI – VAAI stands for vSphere APIs for Array Integration. There are two APIs or Application Programming Interfaces, which are:
 - Hardware Acceleration APIs – This is for arrays to offload some storage operations directly to the array better. In turn, this reduces the CPU cycles needed for specific tasks.
 - Array Thin Provisioning APIs – This helps monitor space usage on thin-provisioned storage arrays to prevent out of space conditions, and does space reclamation when data is deleted.
- PSA – PSA stands for Pluggable Storage Architecture. These APIs allow storage vendors to create and deliver specific multipathing and load-balancing plug-ins that are best optimized for specific storage arrays.

Especially with some of the technology VMware offers (vSAN), these APIs are undoubtedly helpful for sysadmins and your infrastructure. Being able to determine health and adequately fit and apply a customer's requirements for a VM is essential for business.

Objective 1.3.3 – Describe Storage Policies

Storage Policies are a mechanism by which you can assign storage characteristics to a specific VM. Let me explain. Say you have a critical VM, and you want to make sure it sits on a datastore that is backed-up every 4 hours. Using Storage Policies, you can assign that to that VM. You can ensure that the only datastores that it can use are ones that satisfy that requirement. Or you need to limit a VM to a specific performance. You can do that via Storage Policies. You can create policies based on the capabilities of your storage array, or you can even create ones using tags. To learn even more, you can read about it in VMware's documentation [here](#).

Objective 1.3.4 – Describe basic storage concepts in K8s, vSAN, and vSphere Virtual Volumes (vVols)

K8s

I couldn't find this in the materials listed, so I went hunting. For anyone wanting to read more about it, I found the info [HERE](#).

vSphere with Kubernetes supports three types of storage.

- Ephemeral virtual disks – As the name signifies, this storage is very much temporary—this type of virtual disk stores objects such as logs or other temporary data. Once the pod ceases to exist, so does this disk. This type of disk persists across restarts. Each pod only has one disk.
- Container Image virtual disks – This disk contains the software that is to be run. When the pod is deleted, the virtual disks are detached.
- Persistent volume virtual disks – Certain K8s workloads require persistent storage to save data independent of the pod. Persistent volumes objects are backed by First Class Disks or an Improved Virtual Disk. This First Class Disk is identified by UUIDs, which remain valid even if the disk is relocated or snapshotted.

vSAN

vSAN is converged, software-defined storage that uses local storage on all nodes and aggregates them into a single datastore. This is usable by all machines in the vSAN cluster.

A minimum of 3 disks is required to be part of a vSphere cluster and enabled for vSAN. Each ESXi host has a minimum of 1 flash cache disk and 1 spinning or 1 flash capacity disk. A max of 7 capacity disks can be in a single disk group, and up to 5 disk groups can exist per host.

vSan is object-based, uses a proprietary VMware protocol to communicate over the network, and uses policies to enable features needed by VMs. You can use policies to enable multiple copies of data, performance throttling, or stripe requirements.

vVols

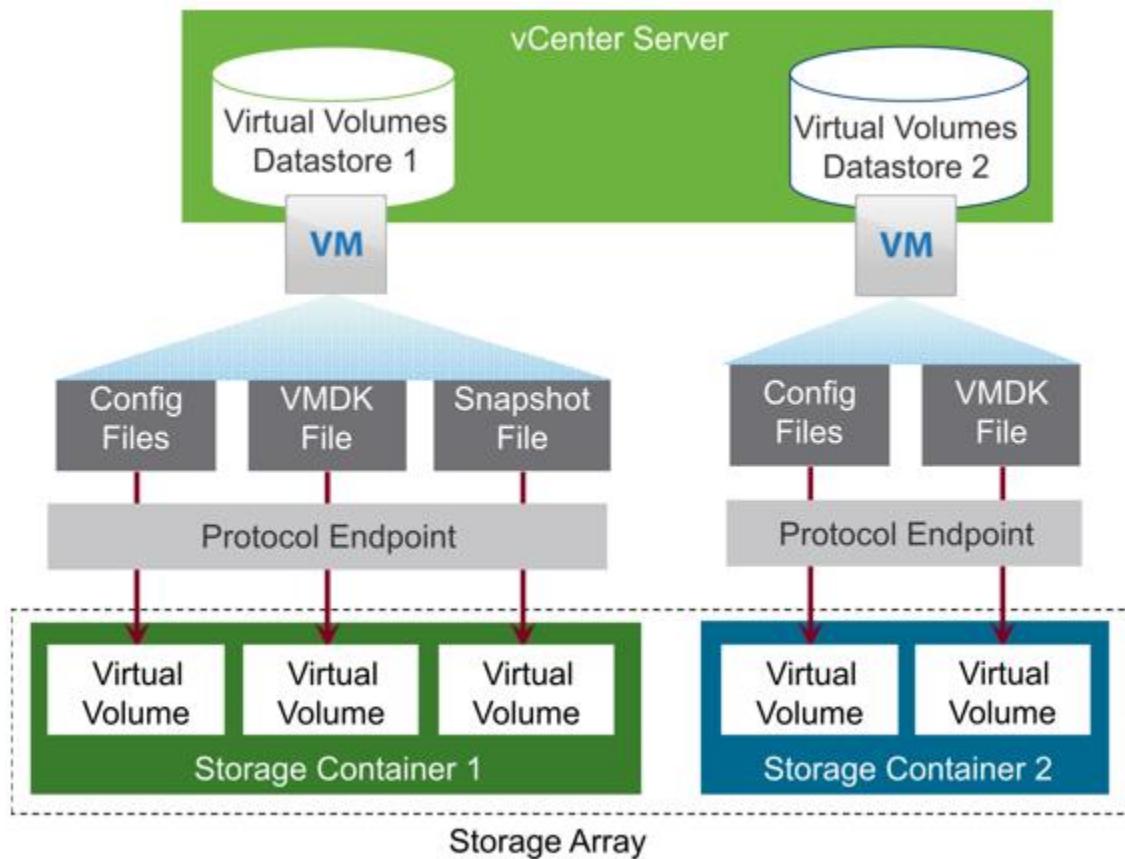
vVols shakes storage up a bit. How so? Typically, you would carve storage out into LUNs, and then you would create datastores on them. The storage administrator would be drawn into architectural meetings with the virtualization administrators to decide on storage schemas and layouts. This had to be done in advance, and it was difficult to change later if something different was needed.

Another problem was that management such as speeds or functionality was controller at a datastore level. Multiple VMs are stored on the same datastore, and if they required different things, it would be challenging to meet their needs. vVols helps change that. It improves granular control, allowing you to cater storage functionality to the needs of individual VMs.

vVols map virtual disks and different pieces, such as clones, snapshots, and replicas, directly to objects (virtual volumes) on a storage array. Doing this allows vSphere to offload tasks such as cloning, and snapshots to the storage array, freeing up resources on the host. Because you are creating individual volumes for each virtual disk, you can apply policies at a much more granular level—controlling aspects such as performance better.

vVols creates a minimum of three virtual volumes, the data-vVol (virtual disk), config-vVol (config, log, and descriptor files), and swap-vVol (swap file created for VM memory pages). It may create more if there are other features used, such as snapshots or read-cache.

vVols start by creating a Storage Container on the storage array. The storage container is a pool of raw storage the array is making available to vSphere. Then you register the storage provider with vSphere. You then create datastores in vCenter and create storage policies for them. Next, you deploy VMs to the vVols, and they send data by way of Protocol Endpoints. The best picture I've seen I'm going to lift and use here from the Fast Track v7 course by VMware.



Objective 1.4 – Differentiate between vSphere Network I/O Control (NIOC) and vSphere Storage I/O Control (SIOC)

NIOC = Network I/O Control

SIOC = Storage I/O Control

Network I/O Control allows you to determine and shape bandwidth for your vSphere networks. They work in conjunction with Network Resource Pools to allow you to determine the bandwidth for specific types of traffic. You enable NIOC on a vSphere Distributed Switch and then set shares according to needs in the configuration of the VDS. This is a feature requiring Enterprise Plus licensing or higher. Here is what it looks like in the UI.

dvSwitch | ACTIONS ▾

- Summary
- Monitor
- Configure**
- Permissions
- Ports
- Hosts
- VMs
- Networks

Settings

- Properties
- Topology
- LACP
- Private VLAN
- NetFlow
- Port Mirroring
- Health Check

Resource Allocation

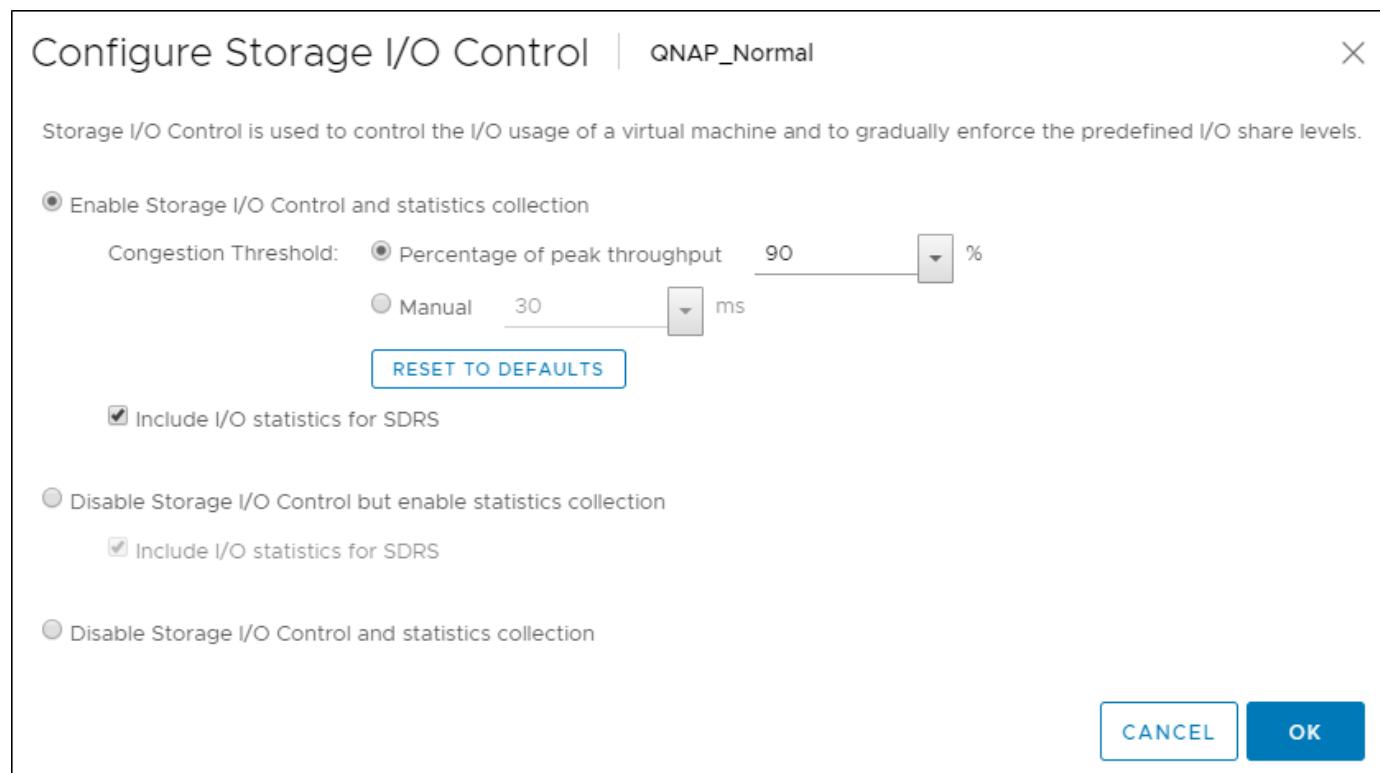
- System traffic
- Network resource p...**

More

Alarm Definitions

Traffic Type	Shares	Shares Value	Reservation	Limit
Management Traffic	Normal	50	0 Mbit/s	Unlimited
Fault Tolerance (FT) Traffic	Normal	50	0 Mbit/s	Unlimited
vMotion Traffic	Normal	50	0 Mbit/s	Unlimited
Virtual Machine Traffic	High	100	0 Mbit/s	Unlimited
iSCSI Traffic	Normal	50	0 Mbit/s	Unlimited
NFS Traffic	Normal	50	0 Mbit/s	Unlimited
vSphere Replication (VR) Traffic	Normal	50	0 Mbit/s	Unlimited
vSAN Traffic	Normal	50	0 Mbit/s	Unlimited
vSphere Data Protection Backup Traffic	Normal	50	0 Mbit/s	Unlimited

Storage I/O Control allows cluster-wide storage I/O prioritization. You can control the amount of storage I/O that is allocated to virtual machines to get preference over less critical virtual machines. This is accomplished by enabling SIOC on the datastore and set shares and upper limit IOPS per VM. SIOC is enabled by default on SDRS clusters. Here is what the screen looks like to enable it.



Objective 1.5 – Describe instant clone architecture and use cases

Instant Clone technology is not new. It was initially around in vSphere 6.0 days but was initially called VMFork. But what is it? It allows you to create powered-on virtual machines from the running state of another. How? The source VM is stunned for a short period. During this time, a new Delta disk is created for each virtual disk, a checkpoint created and transferred to the destination virtual machine. Everything is identical to the original VM. So identical, you need to customize the virtual hardware to prevent MAC address conflicts. You must manually edit the guest OS. Instant clones are created using API calls.

Going a little further in-depth, using William Lam's and Duncan Epping's blog posts [here](#) and [here](#), we learn that as of vSphere 6.7, we can use vMotion, DRS, and other features on these instant clones. Transparent Page Sharing is used between the Source and Destination VMs. There are two ways instant clones are created. One is Running Source VM Workflow where a delta disk is created for each of the destination VMs created on the source VM. This workflow can cause issues the more of them created due to an excessive amount of delta disks on the source VM. The second is the Frozen Source VM Workflow. This workflow uses a single delta on the source VM and a single delta disk on each of the Destination VMs. This workflow is much more efficient. If you visit their blogs linked above, you can see diagrams depicting the two workflows.

Use cases (per Duncan) are VDI, Container hosts, Hadoop workers, Dev/Test, and DevOps.

Objective 1.6 – Describe Cluster Concepts

A vSphere cluster is a group of ESXi host machines. When grouped, vSphere aggregates all of the resources of each host and treats it as a single pool. There are several features and capabilities you can only do with clusters.

Objective 1.6.1 – Describe Distributed Resource Scheduler

vSphere's Distributed Resource Scheduler is a tool used to keep VMs running smoothly. It does this, at a high level, by monitoring the VMs and migrating them to the hosts that allow them to run best. In vSphere 6.x, DRS ran every 5 minutes and concentrated on making sure the hosts were happy and had plenty of free resources. In vSphere 7, DRS runs every 60 seconds and is much more concentrated on VMs and their "happiness." DRS scores each VM and, based on that, migrates or makes recommendations depending on what DRS is set to do. A bit more in-depth in objective 1.6.3.

Objective 1.6.2 – Describe vSphere Enhanced vMotion Compatibility (EVC)

EVC or Enhanced vMotion Compatibility allows you to take different processor generation hosts and still combine them and their resources in a cluster. Different generation processors have different features sets and options on them. EVC masks the newer ones, so there is a level feature set. Setting EVC means you might not receive all the benefits of newer processors. Why? A lot of newer processors are more efficient, therefore lower clock speed. If you mask off their newer feature sets (in some cases how they are faster), you are left with lower clock speeds. Starting with vSphere 6.7, you can enable EVC on a per VM basis allowing for migration to different clusters or across clouds. EVC becomes part of the VM itself. To enable per-VM EVC, the VM must be off. If cloned, the VM retains the EVC attributes.

Objective 1.6.3 – Describe how Distributed Resource Scheduler (DRS) scores virtual machines

VM "Happiness" is the concept that VMs have an ideal or best-case throughput, or resource usage, and actual throughput. If there is no contention or competition on a host for a resource, those two should match, which makes the VM's "happiness" 100%. DRS takes a look at the hosts in the cluster to determine if another host can provide a better score for the VM; it takes steps to migrate or recommend it to another host. Several costs are determined to see if it makes sense to move it. CPU costs, Memory costs, Networking Costs, and even Migration costs. A lower score does not necessarily mean that the VM is running poorly. Why? Some costs taken into account include if the host can accommodate a burst in that resource. The actual equation (thanks [Niels Hagoort](#))

- Goodness (actual throughput) = Demand (ideal throughput) – Cost (loss of throughput)
- Efficiency = Goodness (actual throughput) / Demand (ideal throughput)
- Total efficiency = EfficiencyCPU * EfficiencyMemory * EfficiencyNetwork
- Total efficiency on host = VM DRS score

Keep in mind that the score is not indicative of a health score but an indicator of resource contention. A higher number indicates less resource contention, and the VM is receiving the resources it needs to perform.

Objective 1.6.4 – Describe vSphere High Availability

vSphere HA or High Availability, is a feature designed for VM resilience. Hosts and VMs are monitored, and in the event of a failure, VMs restart on another host.

There are several configuration options to configure. Most defaults work well unless you have a specific use case. Let's go through them:

- Proactive HA – This feature receives messages from a provider like Dell's Open Manage Integration plug-in and, based on those messages, migrate VMs to a different host due to the impending doom of the original host. It can make recommendations on the Manual mode or

Automatically. After all VMs are off the host, you can choose how to remediate the sick host. You can either place it in maintenance mode, which prevents running any workloads on it. You can also put it in Quarantine mode, which allows it to run some workloads if performance is affected. Or a mix of those with.... Mixed Mode.

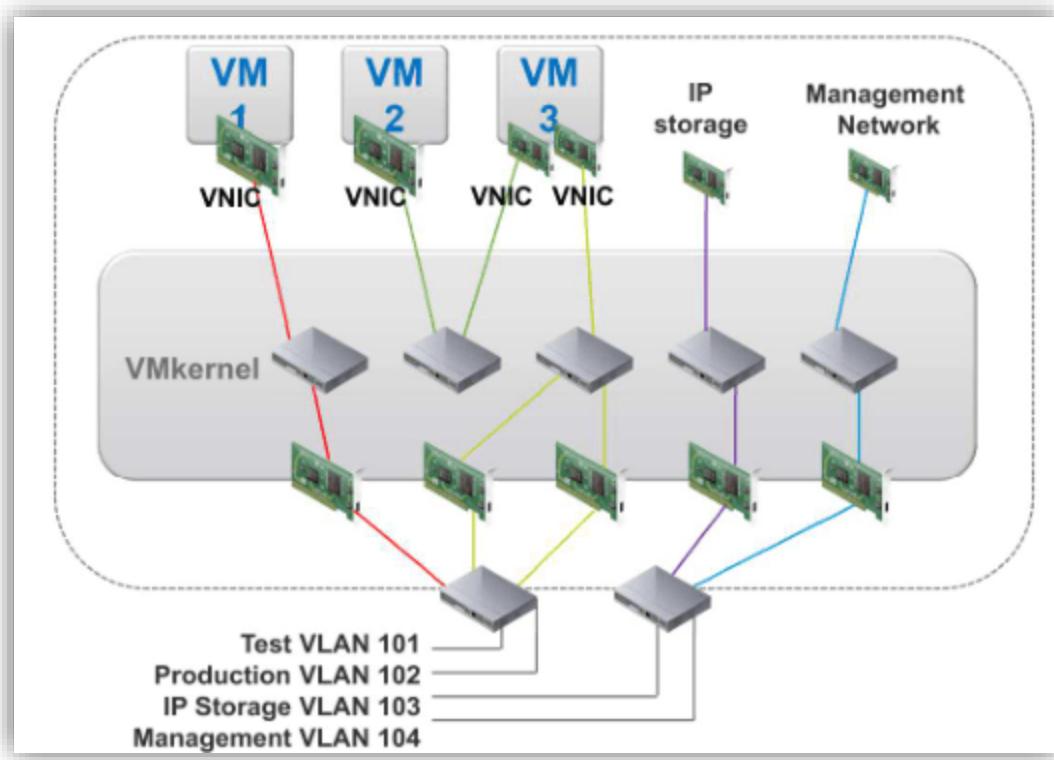
- Failure Conditions and responses – This is a list of possible host failure scenarios and how you want vSphere to respond to them. This is expanded and gives you wayyy more control than in the past.
- Admission Control – What good is a feature to restart VMs if you don't have enough resources to do so? Not very. Admission Control is the gatekeeper that makes sure you have enough resources to restart your VMs in the case of a host failure. You ensure this a couple of ways. Dedicated failover hosts, cluster resource percentage, slot policy, or you can disable it. Dedicated hosts are like a dedicated hot spare in a RAID. They do no work or run VMs until there is a host failure. This is the most expensive option (other than failure itself). Slot policy takes the largest VM's CPU and the largest VM's memory (can be two different VMs) and makes that into a "slot." It then determines how many slots your cluster can satisfy. Next, it looks at how many hosts can fail and keep all VMs powered on. Cluster Resources percentage looks at the total resources needed and total available and tries to keep enough to lose a certain number of hosts you specify. You can also override and set a specific percentage to reserve. For any of these policies, if the cluster can't satisfy needed VMs, it prevents new VMs from turning on.
- Datastore for Heartbeating – This is to monitor hosts and VMs when the HA network has failed. Using a datastore heartbeat can determine if the host is still running or if a VM is still running, by looking at the lock files. This setting automatically tries to make sure that it has at least 2 datastores connected to all the hosts. You can specify more or specific datastores to use.
- Advanced Options – This option is to set advanced options for the HA Cluster. One such setting might be setting a second gateway to determine host isolation. To enable you need to set two options. 1) `das.usedefaultisolationaddress` and 2) `das.isolationaddress[...]` The first specifies not to use the default gateway, and the second sets additional addresses.

Objective 1.7 – Identify vSphere distributed switch and vSphere standard switch capabilities

VDS and VSS are networking objects in vSphere. VDS stands for Virtual Distributed Switch, and VSS is Virtual Standard Switch.

Virtual Standard Switch is the default switch. It is what the installer creates when you deploy ESXi. It has only a few features and requires you to configure a switch on every host manually. As you can imagine, this is tedious and difficult to configure the same every time, which is what you need to do for VM's to move across hosts seamlessly. (You could create a host profile template to make sure they are the same.)

Standard Switches create a link between physical NICs and virtual NICs. You can name them essentially whatever you want, and you can assign VLAN IDs. You can shape traffic but only outbound. Here is a picture I lifted from the official documentation for a pictorial representation of a VSS.



VDSs, on the other hand, add a management plane to your networking. Why is this important? It allows you to control all host networking through one UI. Distributed switches require a vCenter and a certain level of licensing—Enterprise Plus or higher unless you buy vSAN licensing. Essentially you are still adding a switch to every host, just a little bit fancier one that can do more things, that you only have to change once to change all hosts.

There are different versions of VDS you can create, which are based on the version they were introduced. Each newer version adds features. A higher version retains all the features of the lower one and adds to it. Some features include Network I/O Control (NIOC), which allows you to shape your bandwidth incoming and outgoing. VDS also includes a rollback ability, so if you make a change and it loses connectivity, it reverts the changes automatically.

Here is a screenshot of me making a new VDS and some of the features that each version adds:

New Distributed Switch

✓ 1 Name and location

2 Select version

3 Configure settings

4 Ready to complete

Select version

Specify a distributed switch version.

7.0.0 - ESXi 7.0 and later

6.6.0 - ESXi 6.7 and later

6.5.0 - ESXi 6.5 and later

(i) The multicast filtering
continue with the sele

Features per version

New features and enhancements

Distributed switch: 7.0.0

- NSX Distributed Port Group

Distributed switch: 6.6.0

- MAC Learning

Distributed switch: 6.5.0

- Port Mirroring Enhancements

X

ou

NEXT

Here is a small table showing the differences between the switches.

Feature	vSphere Standard Switch	vSphere Distributed Switch
VLAN Segmentation	Yes	Yes
802.1q tagging	Yes	Yes
NIC Teaming	Yes	Yes
Outbound traffic shaping	Yes	Yes
Inbound traffic shaping	No	Yes

VM port blocking	No	Yes
Private VLANs	No	Yes (3 Types – Promiscuous, Community, Isolated)
Load Based Teaming	No	Yes
Network vMotion	No	Yes
NetFlow	No	Yes
Port Mirroring	No	Yes
LACP support	No	Yes
Backup and restore network configuration	No	Yes
Link Layer Discovery Protocol	No	Yes
NIOC	No	Yes

Objective 1.7.1 – Describe VMkernel Networking

VMkernel adapters are set up on the host, for the host itself to interact with the network. Your management and other functions of the host are taken care of by VMkernel adapters. The roles specifically are:

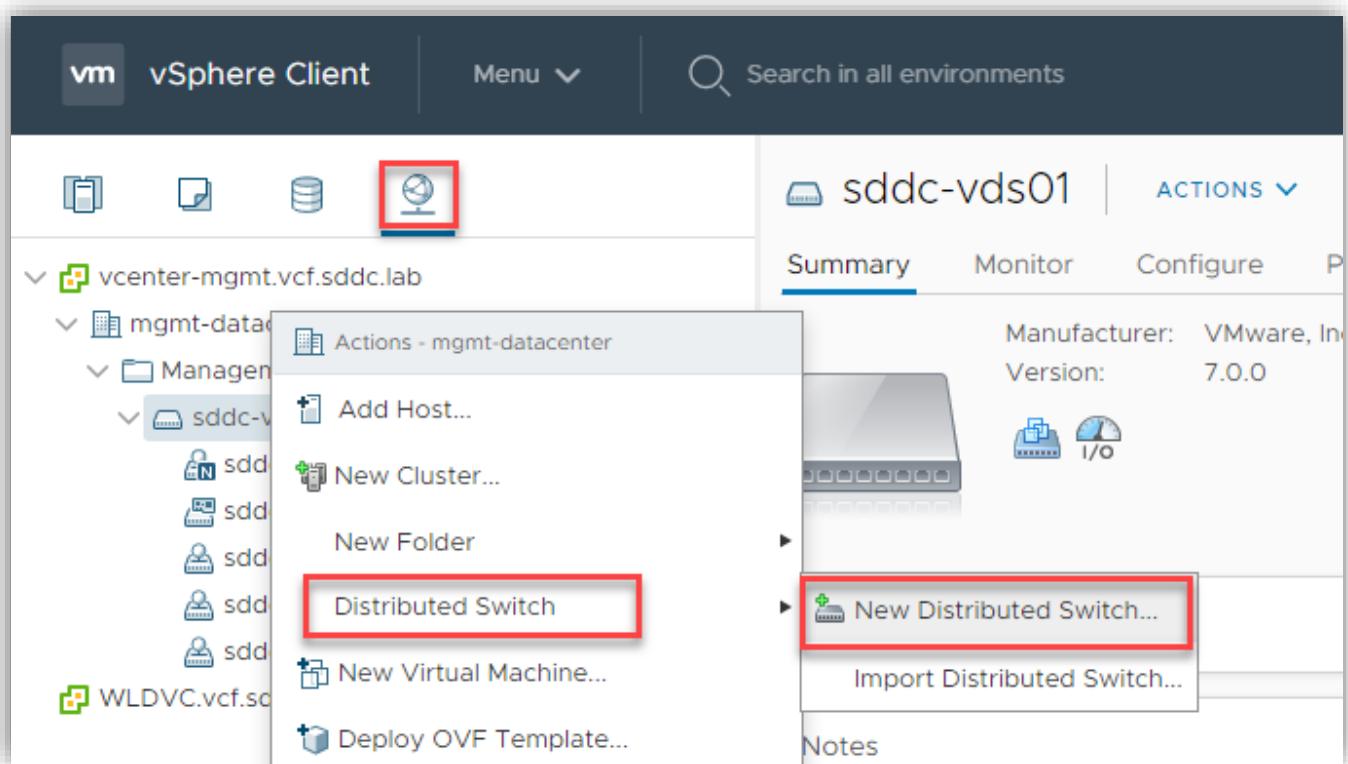
- Management traffic – Using the VMkernel for this by selecting the checkbox, carries configuration and management communication for the host, vCenter Server, and HA traffic. When ESXi is first installed, a VMkernel adapter is created with management selected on it. You should have more than one VMkernel to carry management traffic for redundancy.
- vMotion traffic – Selecting this enables you to migrate VMs from one host to another. Both hosts must have vMotion enabled. You can use multiple physical NICs for faster migrations. Be aware that vMotion traffic is not encrypted – separate this network for greater security.
- Provisioning traffic – This is used for you to separate VM cold migrations, cloning, and snapshot migration. A use case could be VDI for this, or just using a slower network to keep live vMotions separated and not slowed by migrations that don't need the performance.

- IP Storage and discovery – This is not a selection box when you create a VMkernel, but still an important role. This role allows you to connect to iSCSI and NFS storage. You can use multiple physical NICs and “bind” each to a single VMkernel. This enables multipathing for additional throughput and redundancy.
- Fault Tolerance traffic – One of the features you can enable, Fault Tolerance, allows you to create a second mirror copy of a VM. To keep both machines precisely the same requires a lot of network traffic. This role must be enabled and is used for that traffic.
- vSphere Replication traffic – As it sounds like, this role handles the replication traffic sent to a vSphere Replication server.
- vSAN traffic – If you have a vSAN cluster, every host that participates must have a vSAN VMkernel to handle and separate the large amount of traffic needed for vSAN. Movement of objects and retrieval requires a large amount of network bandwidth, so it would be best to have this on as fast of a connection as you can. vSAN does support multiple VMkernels for vSAN but not on the same subnet.

Objective 1.7.2 – Manage networking on multiple hosts with vSphere distributed switch

You should have a decent idea now of what a vSphere distributed switch is and what it can do. The next part is to show you what the pieces are and describe how to use them.

First, you need to create the vSphere distributed switch. Go to the networking tab by clicking on the globe in the HTML5 client. Then right-click on the datacenter and select Distributed Switch > New Distributed Switch



You must now give the switch a name – you should make it descriptive, so it’s easy to know what it does

New Distributed Switch

1 Name and location

2 Select version

3 Configure settings

4 Ready to complete

Name and location

Specify distributed switch name and location.

Name

Test

Location



mgmt-datacenter

CANCEL

BACK

NEXT

Choose the version corresponding to the features you want to use.

New Distributed Switch

✓ 1 Name and location

2 Select version

3 Configure settings

4 Ready to complete

Select version

Specify a distributed switch version.

7.0.0 - ESXi 7.0 and later

6.6.0 - ESXi 6.7 and later

6.5.0 - ESXi 6.5 and later

i The multicast filtering mode on the switch will be set to IGMP/MLD snooping if you continue with the selected version.

CANCEL

BACK

NEXT

You need to tell VMware how many uplinks per host you want to use. This is the number of physical NICs that are used by this switch. Also, select if you want to enable Network I/O Control and if you want vSphere to create a default port group for you – if so, give it a name.

New Distributed Switch

✓ 1 Name and location

✓ 2 Select version

3 Configure settings

4 Ready to complete

Configure settings

Specify number of uplink ports, resource allocation and default port group.

Number of uplinks

4



Network I/O Control

Enabled ▾

Default port group

Create a default port group

Port group name

DPortGroup

[CANCEL](#)

[BACK](#)

NEXT

Finish the wizard.

New Distributed Switch

- ✓ 1 Name and location
- ✓ 2 Select version
- ✓ 3 Configure settings

4 Ready to complete

Ready to complete

Review your settings selections before finishing the wizard.

Name	Test
Version	7.0.0
Number of uplinks	4
Network I/O Control	Enabled
Default port group	DPortGroup

Suggested next actions

- New Distributed Port Group
- Add and Manage Hosts

i These actions will be available in the Actions menu of

CANCEL

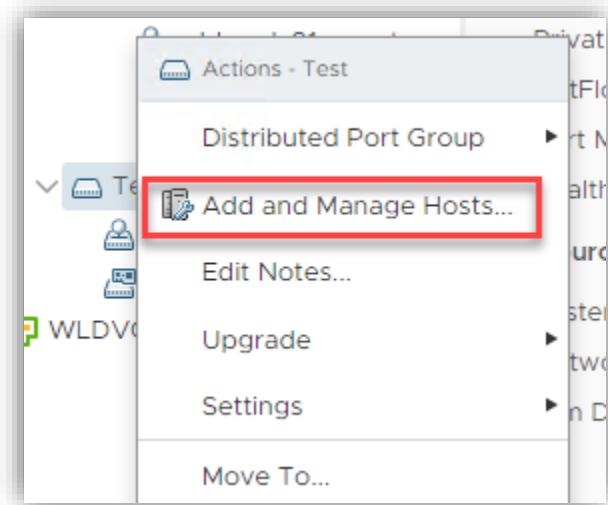
BACK

FINISH

You can now look at a quick topology of the switch by clicking on the switch, then Configure and Topology.

The screenshot shows the vSphere Client interface with the 'Test' switch selected. The 'Configure' tab is active, and the 'Topology' section is highlighted. The topology diagram illustrates a single DPortGroup connected to four physical NICs (Uplinks). A tooltip for the DPortGroup shows its configuration: VLAN ID: -- and Virtual Machines (0).

After creating the vSphere distributed switch, hosts must be associated with it to use it. To do that, you can right-click on the vSphere distributed switch and click on Add and Manage Hosts.



You now have a screen that has the following options: Add Hosts, Manage host networking, and Remove hosts.

Test - Add and Manage Hosts

1 Select task

2 Select hosts
3 Manage physical adapters
4 Manage VMkernel adapt...
5 Migrate VM networking
6 Ready to complete

Select task
Select a task to perform on this distributed switch.

Add hosts
Add new hosts to this distributed switch.

Manage host networking
Manage networking of hosts attached to this distributed switch.

Remove hosts
Remove hosts from this distributed switch.

CANCEL BACK NEXT

Since your switch is new, you need to Add hosts. Select that and on the next screen, click on New Hosts.

Test - Add and Manage Hosts

✓ 1 Select task

2 Select hosts

- 3 Manage physical adapters
- 4 Manage VMkernel adapt...
- 5 Migrate VM networking
- 6 Ready to complete

Select hosts

Select hosts to add to this distributed switch.

 New hosts...

 Remove

Host	Host Status
No items to display	

CANCEL

BACK

NEXT

Select the hosts that you want to be attached to this switch and click OK and then Next again.

Select New Hosts

Test



[SHOW INCOMPATIBLE HOSTS](#)

Filter

<input type="checkbox"/>	Host	Host State	Cluster	Compatibility
<input checked="" type="checkbox"/>	esxi-1.vcf.sddc.lab	Connected	mgmt-cluster	Compatible
<input checked="" type="checkbox"/>	esxi-2.vcf.sddc.lab	Connected	mgmt-cluster	Compatible
<input type="checkbox"/>	esxi-3.vcf.sddc.lab	Connected	mgmt-cluster	Compatible
<input type="checkbox"/>	esxi-4.vcf.sddc.lab	Connected	mgmt-cluster	Compatible

4 items

CANCEL

OK

Now assign the physical NICs to an uplink and click Next

Test - Add and Manage Hosts

✓ 1 Select task

✓ 2 Select hosts

3 Manage physical adapters

4 Manage VMkernel adapt...

5 Migrate VM networking

6 Ready to complete

Manage physical adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
esxi-1.vcf.sddc.lab			
On this switch			
vmnic0 (Assigned)	sddc-vds01	Uplink 1	Test-DVUplinks-7...
On other switches/unclaimed			
vmnic1	sddc-vds01	--	--
esxi-2.vcf.sddc.lab			
On this switch			
vmnic0 (Assigned)	sddc-vds01	Uplink 1	Test-DVUplinks-7...
On other switches/unclaimed			
vmnic1	sddc-vds01	--	--

CANCEL

BACK

NEXT

You can now move any VMkernel adapters over to this vSphere distributed switch if desired.

Test - Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Manage physical adapters
- 4 Manage VMkernel adapt...**
- 5 Migrate VM networking
- 6 Ready to complete

Manage VMkernel adapters

Manage and assign VMkernel network adapters to the distributed switch.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Gr...
Assign port group Reset changes View settings			
On this switch			
On other switches/unclaimed			
vmk0	sddc-vds01	sddc-vds01-mgmt	Do not migrate
vmk1	sddc-vds01	sddc-vds01-vmoti...	Do not migrate
vmk2	sddc-vds01	sddc-vds01-vsan	Do not migrate
vmk10	sddc-vds01	Port ID: ee09fa50...	Do not migrate
vmk11	sddc-vds01	Port ID: a4e0bfe3...	Do not migrate
vmk50	sddc-vds01	Port ID: 017c9799...	Do not migrate
On this switch			

CANCEL

BACK

NEXT

Same with VM networking

Test - Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Manage physical adapters
- ✓ 4 Manage VMkernel adapt...
- 5 Migrate VM networking**
- 6 Ready to complete

Migrate VM networking

Select virtual machines or network adapters to migrate to the distributed switch.

Migrate virtual machine networking

 Assign port group  Reset changes  View settings

Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group	Destination Port Group
No records to display			

CANCEL

BACK

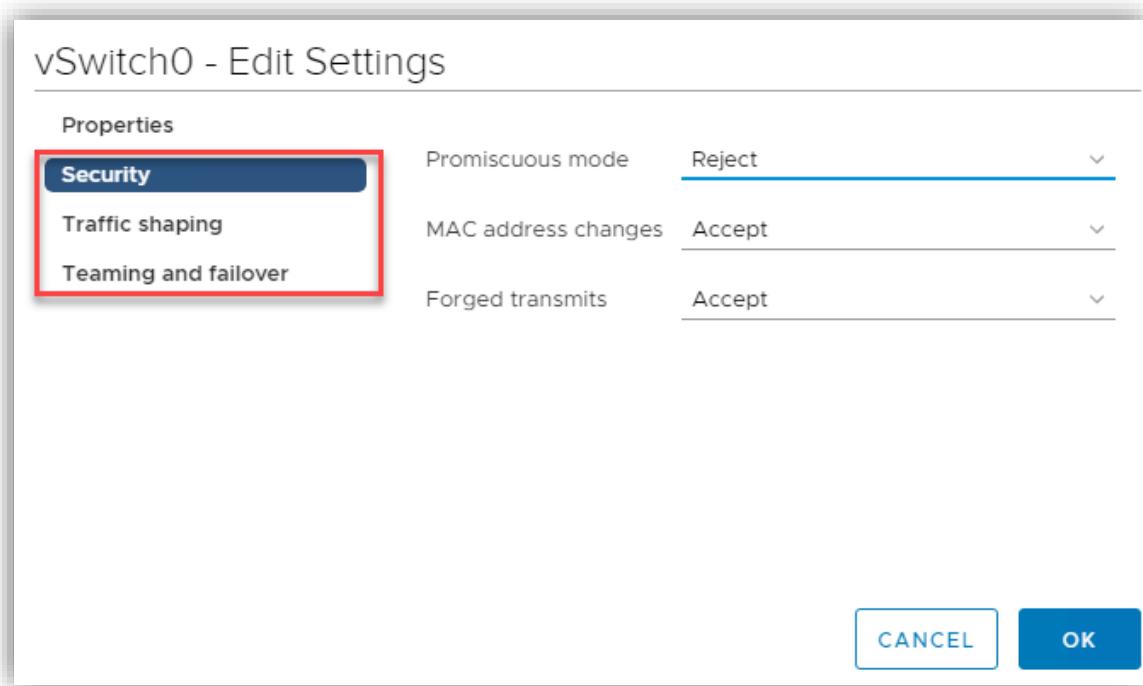
NEXT

You now complete it. And of course, you notice you can make changes to all the hosts during the same process. This is one part of what makes vSphere distributed switches great.

Objective 1.7.3 – Describe Networking Policies

Networking policies are rules on how you want virtual switches, both standard or distributed, to work. Several policies can be configured on your switches. They apply at a switch level. If needed, however, you CAN override them at a port group level. Here is a bit of information on them:

Virtual Standard Switch Policies:



vSphere Distributed Switch Policies:

Policies	
Security	Promiscuous mode Reject MAC address changes Reject Forged transmits Reject
Ingress traffic shaping	Status Disabled Average bandwidth -- Peak bandwidth -- Burst size --
Egress traffic shaping	Status Disabled Average bandwidth -- Peak bandwidth -- Burst size --
VLAN	Type VLAN VLAN ID 10
Teaming and failover	Load balancing Route based on physical NIC load Network failure detection Link status only Notify switches Yes Fallback Yes Active uplinks uplink1, uplink2 Standby uplinks -- Unused uplinks --
Monitoring	NetFlow Disabled

- Traffic Shaping – This is different depending on which switch you are using. Standard switches can only do Egress (outgoing), and vSphere distributed switches can do ingress as well. You can establish an average bandwidth over time, peak bandwidth in bursts, and burst size.
- Teaming and Failover – This setting enables you to use more than one physical NIC to create a team. You then select load balancing algorithms and what should happen in the case of a NIC failure
- Security – Most homelabbers know this setting due to needing to set Promiscuous Mode to allow nested VMs to talk externally. Promiscuous mode rejects or allows network frames to the VM. Mac Address Changes will either reject or allow MAC addresses different than the one assigned to the VM. Forged Transmits drop outbound frames from a VM with a MAC address different than the one specified for the VM in the .vmx configuration file.
- VLAN – enables you to specify a VLAN type (VLAN, VLAN trunking, or Private PLAN) and assigns a value.

- Monitoring – Using this, you can turn on NetFlow monitoring.
- Traffic Filtering and marking – This policy lets you protect the network from unwanted traffic and apply tags to delineate types of traffic.
- Port Blocking – This allows you to block ports from sending or receiving data selectively.

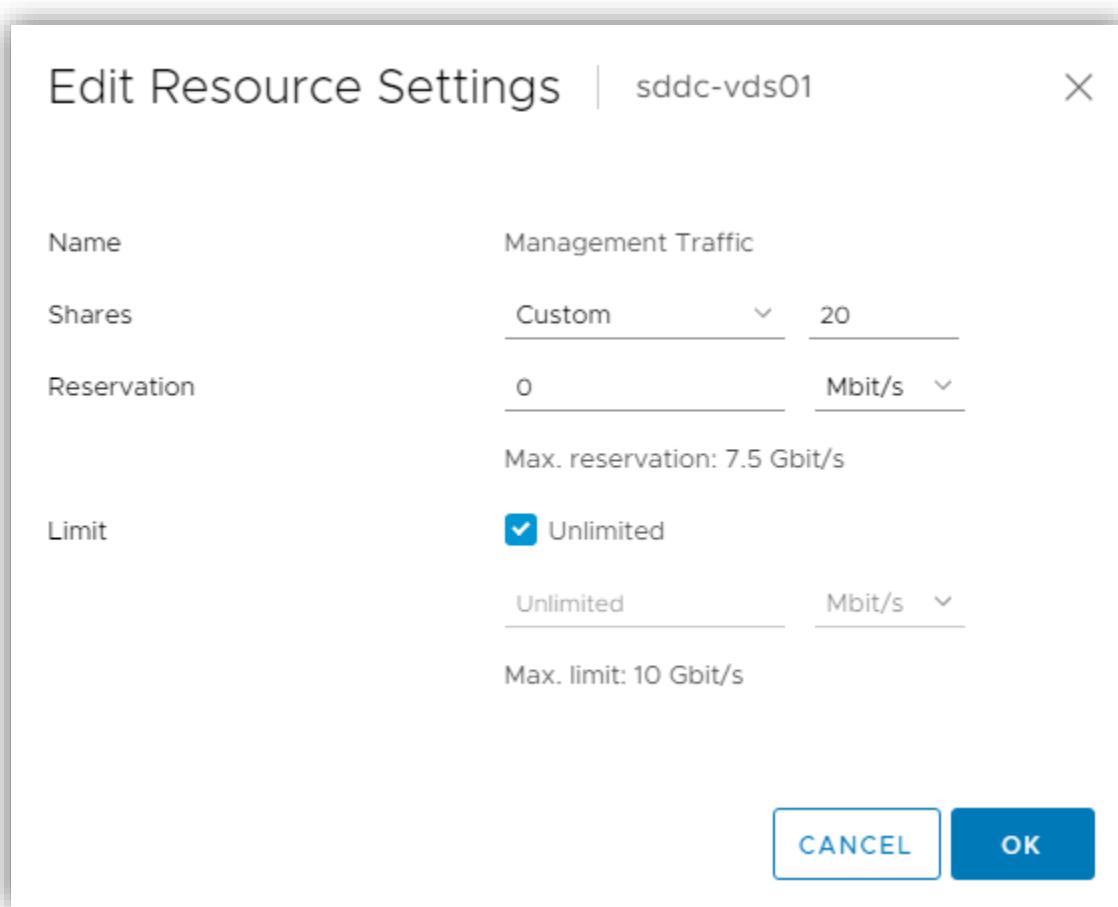
Objective 1.7.4 – Manage Network I/O Control on a vSphere distributed switch

One of the features that you can take advantage of on a vSphere distributed switch is NIOC or Network I/O Control. Why is this important? Using NIOC, you control your network traffic. You set shares or priorities to specific types of traffic, and you can also set reservations and hard limits. To get to it, select the vSphere distributed switch and then in the center pane, Configure, then Resource Allocation. Here is a picture of NIOC:

The screenshot shows the 'Resource Allocation' section of the vSphere Web Client. On the left, a sidebar lists various settings like Properties, Topology, LACP, Private VLAN, NetFlow, Port Mirroring, and Health Check. Below that is a 'Resource Allocation' dropdown menu with 'System traffic' and 'Network resource pools' selected. A red box highlights the 'Network resource pools' option. The main pane displays bandwidth capacity details and a table for traffic type allocation.

Traffic Type	Shares	Shares Value	Reservation	Limit
Management Traffic	Custom	20	0 Mbit/s	Unlimited
Fault Tolerance (FT) Traffic	Normal	50	0 Mbit/s	Unlimited
vMotion Traffic	Normal	50	0 Mbit/s	Unlimited
Virtual Machine Traffic	Custom	30	0 Mbit/s	Unlimited
iSCSI Traffic	Normal	50	0 Mbit/s	Unlimited
NFS Traffic	Normal	50	0 Mbit/s	Unlimited
vSphere Replication (VR) Traffic	Normal	50	0 Mbit/s	Unlimited
vSAN Traffic	High	100	0 Mbit/s	Unlimited
vSphere Data Protection Backup Traffic	Normal	50	0 Mbit/s	Unlimited

If you edit one of the data types, this is the box for that.



There are several settings to go through here. Let's discuss them.

- **Shares** – This is the weight you associate with the type of network traffic when there is congestion. You can assign Low, Normal, High, or Custom. Low = 25, Normal = 50, High = 100 shares. Custom can be any number you want it to be from 1-100. Shares do not equal percentage; in other words, the total doesn't add up to 100%. If you have one with Normal shares of 50 and another with 100, the one with 100 will receive twice as much bandwidth as the one with 50. Again this only comes into play when there is network congestion.
- **Reservation** – This is a guarantee that vSphere makes available to this type of traffic. If not needed, this bandwidth becomes available to other types of system traffic (not VM.) A maximum of 75% of the total bandwidth can be reserved
- **Limit** – The maximum bandwidth allowed for that type of traffic. If the system has plenty of extra, it still won't allow a limit to be exceeded.

You can also set up a custom type of traffic with the Network Resource Pool.

Objective 1.8 – Describe vSphere Lifecycle Manager concepts (baselines, cluster images, etc.)

Managing a large number of servers gets difficult and cumbersome quickly. In previous versions of vSphere, there was a tool called VUM or vSphere Update Manager. VUM was able to do a limited

number of things for us. It could upgrade and patch hosts, install and update third-party software on hosts, and upgrade virtual machine hardware and VMware Tools. This was useful but left a few important things out. Things like hardware firmware and maintain a baseline image for cluster hosts. Well, fret no more! Starting with vSphere 7, a new tool called Lifecycle Manager was introduced. Here are some of the things you can do:

- Check hardware of hosts against the compatibility guide, and vSAN Hardware Compatibility List
- Install a single ESXi image on all hosts in a cluster
- Update the firmware of all ESXi in a cluster
- Update and Upgrade all ESXi hosts in a cluster together

Just as with VUM, you can download updates and patches from the internet, or you can manually download them for dark sites. Keep in mind to use some of these features, you need to be using vSphere 7 on your hosts. Here is a primer just for those that are new to this or those needing a refresh.

Baseline – this is a group of patches, extensions, or an upgrade. There are 3 default baselines in Lifecycle Manager: Host Security Patches, Critical Host Patches, and Non-Critical Host Patches. You cannot edit or delete these. You can create your own.

Baseline Group – is a collection of non-conflicting baselines. For example, you can combine Host Security Patches, Critical Host Patches, and Non-Critical Host Patches into a single Baseline Group. You then attach this to an inventory object, such as a cluster or a host. You can then check the object for compliance. If it isn't in compliance, remediation installs the updates. If the host can't be rebooted, staging the software to it first loads the software and waits to install until a time of your choosing.

In vSphere 7, there are now Cluster baseline images. You set up an image and use that as the baseline for all ESXi 7.0 hosts in a cluster. Here is what that looks like:

NewCluster | ACTIONS ▾

Summary Monitor Configure Permissions Hosts VMs Datastores Networks **Updates**

Hosts ▾

- Image
- Hardware Compatibility
- VMware Tools
- VM Hardware

Edit Image

Select the version of ESXi and other components that you want for the hosts in this cluster. The same image will be applied consistently to all these hosts.

ESXi Version: 7.0b - 16324942 (released 06/15/2020)

Vendor Addon ⓘ: SELECT (optional)

Firmware and Drivers Addon ⓘ: SELECT (optional)

Components ⓘ: No additional components Show details

SAVE VALIDATE CANCEL

In the image, you can see you load an image of ESXi (the .zip file, not ISO), and you can add a vendor add-on and firmware and drivers. Components allow you to load individual VIBs (VMware Installation Bundles) for hardware or features.

From the above, you can deduce that the new Lifecycle Manager will be a great help in managing the host's software and hardware.

Objective 1.9 – Describe the basics of vSAN as primary storage

vSAN is VMware's in-kernel software-defined storage solution that uses local storage and aggregates them into a single distributed datastore to be used by cluster nodes. vSAN requires a cluster and hardware that has been approved and on the vSAN hardware compatibility guide. vSAN is object-based, and when you provision a VM, its pieces are broken down into specific objects. They are:

- VM Home namespace - stores configuration files such as the .vmx file.
- VMDK – virtual disk
- VM Swap – this is the swap file created when the VM is powered on
- VM memory – this is the VM's memory state if the VM is suspended or has snapshots taken with preserve memory option
- Snapshot Delta – Created if a snapshot is taken

VMs are assigned storage policies that are rules applied to the VM. Policies can be availability, performance, or other storage characteristics that need to be assigned to the VM.

A vSAN cluster can be a "Hybrid" or "All-Flash" cluster. A hybrid cluster is made up of flash drives and rotational disks, whereas an all-flash cluster consists of just flash drives. Each host, or node, contributes at least one disk group to storage. Each disk group consists of 1 flash cache drive, and 1-7 capacity drives, rotational or flash. A total of 5 disk groups can reside on a node for a total of 40 disks. The cache disk on a hybrid cluster is used for read caching and write buffering (70% read, 30% write.) On an all-flash cluster, the cache disk is just for write buffering (up to 600GB.)

vSAN clusters are limited by vSphere maximums of 64 nodes per cluster but typically use a max of 32. You can scale up, out, or back and supports RAID 1, 5, and 6. Different VM's can have different policies and different storage characteristics using the same datastore.

Objective 1.9.1 – Identify basic vSAN requirements (networking, disk count, type)

We went over a few of them above but let's list vSAN's requirements entirely.

- 1 Flash drive for cache per disk group– can be SAS, SATA, or PCIe
- 1-7 drives per disk group – can be SAS, SATA, or PCIe flash
- 1 GB NIC for Hybrid or 10 Gbe + for all-flash clusters with a VMkernel port tagged for vSAN
- SAS / SATA / NVMe Controller – must be able to work in pass-thru or Raid 0 mode (per disk) to allow vSAN to control it
- IPv4 or IPv6 and supports Unicast
- Minimum of 32 GB RAM per host to accommodate a maximum of 5 disk groups and 7 disks per disk group.

Although typically you need 3 nodes minimum for a vSAN cluster, 4 is better for N+1 and taking maintenance into account. In other cases, 2-node clusters also exist for smaller Remote Branch Office or ROBO installations.

Objective 1.10 – Describe vSphere Trust Authority Architecture

Starting with vSphere 6.7, VMware introduced support for Trusted Platform Module or TPM 2.0 and the host attestation model. TPMs are that little device can be installed in servers that can serve as a cryptographic processor and can generate keys. It can also store materials, such as keys, certificates, and signatures. They are tied to specific hardware (hence the security part), so you can't buy a used one off eBay to install in your server. The final feature of TPMs is what we are going to use here or determining if a system's integrity is intact. It does this by an act called attestation. Using UEFI and TPM, it can determine if a server booted with authentic software.

Well, that's all great, but vSphere 6.7 was view-only; there were no penalties or repercussions if the software wasn't authentic. What's changed?

Now, introduced in vSphere 7, we have vSphere Trust Authority. This reminds me of Microsoft's version of this called Hyper-V Shielded Installs. Essentially you would create a hyper-secure cluster called Host Guardian Service, and then you would have 1 or more guarded hosts and shielded VMs. This is essentially the same concept.

You create a vSphere Trust Authority which can either establish its own management cluster apart from your regular hosts. The better way is to have a completely separate cluster, but to get started, it can use an existing management cluster. They won't be running any normal workload VMs so they can be small machines. Once established, it has two tasks to perform:

- Distribution of encryption keys from the KMS (taking over this task for the vCenter server)
- Attestation of other hosts

If a host fails attestation now, the vTA will withhold keys for it, preventing secure VMs from running on that host until it passes attestation. Thanks to Bob Plankner's blog [here](#) for explaining it.

Objective 1.11 – Explain Software Guard Extensions (SGX)

Intel's Software Guard Extensions or SGX were created to meet the needs of the trusted computing industry. How so? SGX is a security extension on some modern CPUs. SGX allows software to create private memory regions called enclaves. The data in enclaves is only able to be accessed by the intended program and is isolated from everything else. Typically this is used for blockchain and secure remote computing.

vSphere 7 now has a feature called vSGX or virtual SGX. This feature allows the VMs to access Intel's technology if it's available. You can enable it for a VM through the HTML5 web client. For obvious reasons (can't access the memory), you can't use this feature with some of vSphere's other features such as vMotion, suspend and resume, or snapshots (unless you don't snapshot memory).

That ends the first section. Next up, we will go over VMware Products and Solutions, which is a lot lighter than this one was. Seriously my fingers hurt.

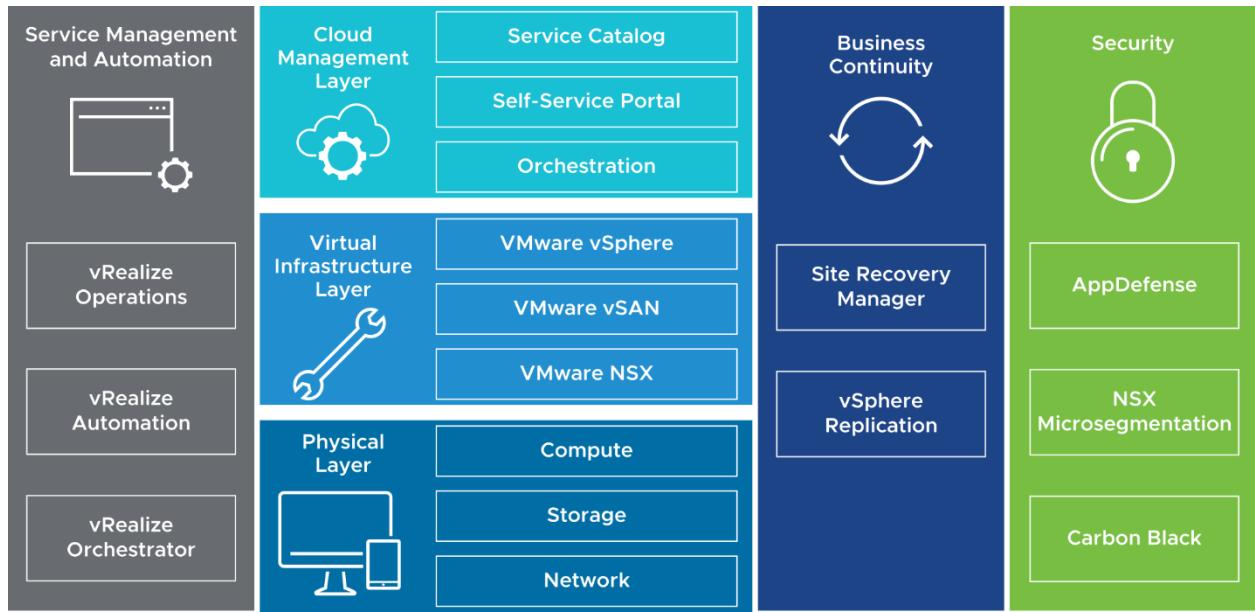
Picking up where we left off, here is Section 2. Once again, this version has been shaken up quite a bit from previous VCP objectives; this section is a bit lighter than Section 1. Let's dig in.

Section 2 – VMware Products and Solutions

Objective 2.1 – Describe the role of vSphere in the software-defined data center (SDDC)

While I think most are acquainted with what VMware is referring to when they say SDDC or Software-Defined Data Center, let us do a quick refresh for anyone that may not be aware.

VMware's vision is a data center that is fully virtualized and completely automated. The end goal is where all these different pieces are delivered as a service. vSphere is one of the main cornerstones and what makes the rest of this vision possible. What does this look like? Here is a picture (credit to VMware)



The bottom layer is hardware. From there, the next layer is vSphere, which provides software-defined compute and memory. Next, we see vSAN, which provides software-defined storage—finally, NSX, which provides software-defined networking. Cloud Management is the next layer up.

Becoming cloud-like is the goal. Why? Cloud services are mobile, easy to move around as needed, and are easy to start up and scale, both up and down. With a self-service portal and cloud-like services, requests that previously took weeks or months to fulfill now take hours or even minutes. Using automation to deliver these services ensure it's done the same way, every time. Using automation also makes sure it's easy to track requestors and do appropriate charge-backs. vRealize Operations ensure that you quickly see and are notified if low on resources and when to plan for more. Site Recovery Manager and vSphere Replication enable you to continue offering those services even in the case of disaster. But it all begins with vSphere.

Objective 2.2 – Identify use cases for vCloud Foundation

vCloud Foundation is a large portion of that SDDC picture above, but instead of needing to install each piece manually, it gives you that easy install button. This easy button comes in two ways - first from an appliance called VMware Cloud Builder. This appliance initially was a way to help VMware professional services to implement VMware Validated Designs. It released to the general public in January of 2019. The appliance itself can deploy the full SDDC stack, including:

- VMware ESXi
- VMware vCenter Server
- VMware NSX for vSphere

- VMware vRealize Suite Lifecycle Manager
- VMware vRealize Operations Manager
- VMware vRealize Log Insight
- Content Packs for Log Insight
- VMware vRealize Automation
- VMware vRealize Business for Cloud
- VMware Site Recovery Manager
- vSphere Replication

The second easy button is an appliance that is installed in vCloud Foundations called SDDC Manager. This tool automates the entire lifecycle management from bring-up, to configuration and provisioning, and updates and patching. Not only for the initial management cluster but infrastructure and workload clusters as well. It also makes deploying VMware Kubernetes much easier. For VMware vCloud Foundations, the Cloud Builder appliance only installs the following:

- SDDC Manager
- VMware vSphere
- VMware vSAN
- NSX for vSphere
- vRealize Suite

We now have a better understanding of what vCloud Foundations is, let us talk use cases. VMware has highlighted the main ones [here](#). Those use cases are:

- Private and Hybrid Cloud
- Modern Apps (Development)
- VDI (Virtual Desktop Infrastructure)

It's an exciting product, and VMware says that it simplifies management and deployment and reduces operational time. If you want to take a look at it, there are free Hands-On Labs VMware has made available [here](#).

Objective 2.3 – Identify migration options

One of the coolest, in my opinion, features of vSphere is the ability to migrate VMs. The first iteration of this was in VMware Virtual Center 1.0 in 2003. Specifically, this was a live migration. A live migration is a virtual machine running an application that could move to another host, with no interruption. This was amazing for the time, and it's still a fantastic feature today. There are several different types of migrations. They are:

- Cold Migration – This migration is moving a powered-off or suspended VM to another host
- Hot Migration – This migration involves moving a powered-on VM to another host.

Additionally, different sub-types exist depending on what resource you want to migrate. Those are:

- Compute only – This is migrating a VM (compute and memory), but not its storage to another host.
- Storage only – This is migrating a VM's storage, but not compute and memory to another datastore.

- Both compute and storage – This is how it sounds. Moves both compute memory and storage to a different location.

Previously these migrations were known as a vMotion (compute only), svMotion (storage only), and xvMotion or Enhanced vMotion (both compute and storage). To enable hosts to use this feature, hosts on both sides of the migration must have a VMkernel network adapter enabled for vMotion. Other requirements include:

- If a compute migration, both hosts must be able to access the datastore where the VM's data resides.
- At least a 1 Gb Ethernet connection
- Compatible CPUs (or Enhanced vMotion Compatibility mode enabled on the cluster.)

Another type of migration is a cross vCenter Migration. This migrates a VM between vCenter Systems that are connected via Enhanced Link Mode. Their vCenter's times must be synchronized with each other, and they must both be at vSphere version 6.0 or later. Using cross vCenter Server migration, you can also perform a Long-Distance vSphere vMotion Migration. This type of migration is a vMotion to another geographical area within 150 milliseconds latency of each other, and they must have a connection speed of at least 250 Mbps per migration.

Now that we have identified the types of migrations, what exactly is vSphere doing to work this magic? When the administrator initiates a compute migration:

- A VM is created on the destination host called a “shadow VM.”
- The source VM's memory is copied over the vMotion network to the destination's host VM. The source VM is still running and being accessed by users during this, potentially updating memory pages.
- Another copy pass starts to capture those updated memory pages.
- When almost all the memory has been copied, the source VM is stunned or paused for the final copy and transfer of the device state.
- A Gratuitous ARP or GARP is sent on the subnet updating the VM's location, and users begin using the new VM.
- The source VM's memory pages are cleaned up.

What about a storage vMotion?

- Initiate the svMotion in the UI.
- vSphere uses something called the VMkernel data mover or if you have a storage array that supports vSphere Storage APIs Array Integration (VAAI) to copy the data.
- A new VM process is started
- Ongoing I/O is split using a “mirror driver” to be sent to the old and new virtual disks while this is ongoing.
- vSphere cuts over to the new VM files.

Migrations are useful for many reasons. Being able to relocate a VM off one host or datastore to another enables sysadmins to perform hardware maintenance, upgrade or update software, and redistribute load for better performance. You can enable encryption for migration as well to be more secure—a massive tool in your toolbox.

Objective 2.4 – Identify DR use cases

Many types of disasters can happen in the datacenter. From something smaller such as power outage of a host to large, major scale natural disasters, VMware tries to cover you with several types of DR protection.

High Availability (HA):

HA works by pooling hosts and VMs into a single resource group. Hosts are monitored, and in the event of a failure, VMs are restarted on another host. When you create a HA cluster, an election is held, and one of the hosts is elected master. All others are subordinates. The master host has the job of keeping track of all the VMs that are protected and communication with the vCenter Server. It also needs to determine when a host fails and distinguish that from when a host no longer has network access. Hosts communicate with each other over the management network. There are a few requirements for HA to work.

- All hosts must have a static IP or persistent DHCP reservation
- All hosts must be able to communicate with each other, sharing a management network

HA has several essential jobs. One is determining priority and order that VMs are restarted when an event occurs. HA also has VM and Application Monitoring. The VM monitoring feature directs HA to restart a VM if it doesn't detect a heartbeat received from VM Tools. Application Monitoring does the same task with heartbeats from an application. VM Component Monitoring or VMCP allows vSphere to detect datastore accessibility and restart the VM if a datastore is unavailable. For exam takers, in the past, VMware tried to trick people on exams by using the old name for HA, which was FDM or Fault Domain Manager

There are several options in HA you can configure. Most defaults will work fine and don't need to be changed unless you have a specific use case. They are:

- Proactive HA – This feature receives messages from a provider like Dell's Open Manage Integration plugin. Based on those messages, HA migrates VMs to a different host due to the possible impending doom of a host. It makes recommendations in Manual mode or automatically moves them in Automatic mode. After VMs are off the host, you can choose how to remediate the sick host. You can place it in maintenance mode, which prevents running any future workloads on it. Or you could put it in Quarantine mode, which allows it to run some workloads if performance is low. Or a mix of those with.... Mixed Mode.
- Failure Conditions and responses - This is a list of possible host failure scenarios and how you want vSphere to respond to them. This is better and gives you way more control than in past versions (5.x).
- Admission Control – What good is a feature to restart VMs if you don't have enough resources to do so? Admission Control is the gatekeeper that makes sure you have enough resources to restart your VMs in case of a host failure. You can ensure resource availability in several ways. Dedicated failover hosts, cluster resource percentage, slot policy, or you can disable it (not useful unless you have a specific reason). Dedicated hosts are dedicated hot spares. They do no work or run VMs unless there is a host failure. This is the most expensive (other than failure itself). Slot policy takes the largest VM's CPU and the largest VM's memory (can be two different VMs) and makes that into a "slot" then it determines how many slots your cluster can satisfy. Then it looks at how many hosts can fail and still keep all VMs powered on based on that base slot size. Cluster Resources Percentage looks at total

- resources needed and total available and tries to keep enough resources free to permit you to lose the number of hosts you specify (subtracting the number of resources of those hosts). You can also override this and set aside a specific percentage. For any of these policies, if the cluster can't satisfy resources for more than existing VMs in the case of a failure, it prevents new VMs from powering on.
- Heartbeat Datastores – Used to monitor hosts and VMs when the HA network has failed. It determines if the host is still running or if a VM is still running by looking for lock files. This automatically uses at least 2 datastores that all the hosts are connected to. You can specify more or specific datastores to use.
 - Advanced Options – You can use this to set advanced options for the HA Cluster. One might be setting a second gateway to determine host isolation. To use this, you need to set two options.
 - 1) *das.usedefaultisolationaddress* and
 - 2) *das.isolationaddress[...]*

The first specifies not to use the default gateway, and the second sets additional addresses.

There are a few other solutions that touch more on Disaster Recovery.

Fault Tolerance

While HA keeps downtime to a minimum, the VM still needs to power back on from a different host. If you have a higher priority VM that can't withstand almost any outage, Fault Tolerance is the feature you need to enable.

Fault Tolerance or FT creates a second running “shadow” copy of a VM. In the event the primary VM fails, the secondary VM takes over, and vSphere creates a new shadow VM. This feature makes sure there is always a backup VM running on a second, separate host in case of failure. Fault Tolerance has a higher resource cost due to higher resilience; you are running two exact copies of the same VM, after all. There are a few requirements for FT.

- Supports up to 4 FT VMs with no more than 8 vCPUs between them
- VMs can have a maximum of 8vCPUs and 128 GB of RAM
- HA is required
- There needs to be a VMkernel with the Fault Tolerance Logging role enabled
- If using DRS, EVC mode must be enabled.

Fault Tolerance works essentially by being a vMotion that never ends. It uses a technology called Fast Checkpointing to take checkpoints of the source VM every 10 milliseconds or so and send that data to the shadow VM. This data is sent using a VMkernel port with Fault Tolerance logging enabled. There are two files behind the scenes that are important. One is *shared.vmft* and *.ft-generation*. The first is to make sure the UUID or identifier for the VM's disk stays the same. The second is in case you lose connectivity between the two. That file determines which VM has the latest data and that VM is designated the primary when they are both back online.

vSphere Replication

Remote site Disaster Recovery options include vSphere Replication and Site Recovery Manager. You can use vSphere Replication or both in conjunction to replicate a site or individual VMs in case of failure or disaster. While I'm not going to delve deep into vSphere Replication or SRM, you should know their capabilities and, at a high level, how they work.

vSphere Replication is configured on a per-VM basis. Replication can happen from a primary to a secondary site or from multiple sites to a single target site. It uses a server-client model with appliances on both sides. A VMkernel with the vSphere Replication and vSphere Replication NFC (network file copy) role can exist to create an isolated network for replication.

Once you have your appliances setup and you choose which VMs you want to be replicated, you need to figure out what RPO to enable. RPO is short for Recovery Point Objective. RPO is how often you want it to replicate the VM and can be as short as 5 minutes or as long as every 24 hours.

Site Recovery Manager uses vSphere Replication but is much more complex and detailed. You can specify runbooks (recovery plans), how to bring the other side up, test your failovers, and more.

The above tools are in addition to VMware's ability to integrate with many companies to do backups.

Objective 2.5 – Describe vSphere integration with VMware Skyline

VMware Skyline is a product available to VMware supported customers with a current Production or VMware Premier Support contract. What is it? A proactive support service integrated with vSphere, allowing VMware support to view your environment's configurations and logs needed to speed up the resolution to a problem.

Skyline does this in a couple of ways. Skyline has a Collector appliance and a Log Assist where it can upload log files directly to VMware (with customer's permission). Products supported by Skyline include vSphere, NSX for vSphere, vRealize Operations, and VMware Horizon. If you want to learn even more, visit the datasheet [here](#).

Section 4 – Installing, Configuring, and Setup

Objective 4.1 – Describe single sign-on (SSO) deployment topology

In the previous version of vSphere, you could deploy vCenter Server on a single server, which included the SSO components, or you could break it into multiple components. Sign-ons were serviced by the Platform Services Controller, and you could set more than one up to help with a massive load or multiple sites. With vSphere 7, this has been changed. You now only have the embedded vCenter Server, which has all components in a single appliance. You can scale out for larger loads. For resiliency, you can deploy vCenter High Availability. For multiple sites, you can leave the single vCenter in place, or you can have a second vCenter for the other sites and connect them with Enhanced Link Mode. Enhanced Link Mode enables you to manage all vCenters from a single HTML5 client.

vCenter Single Sign-On

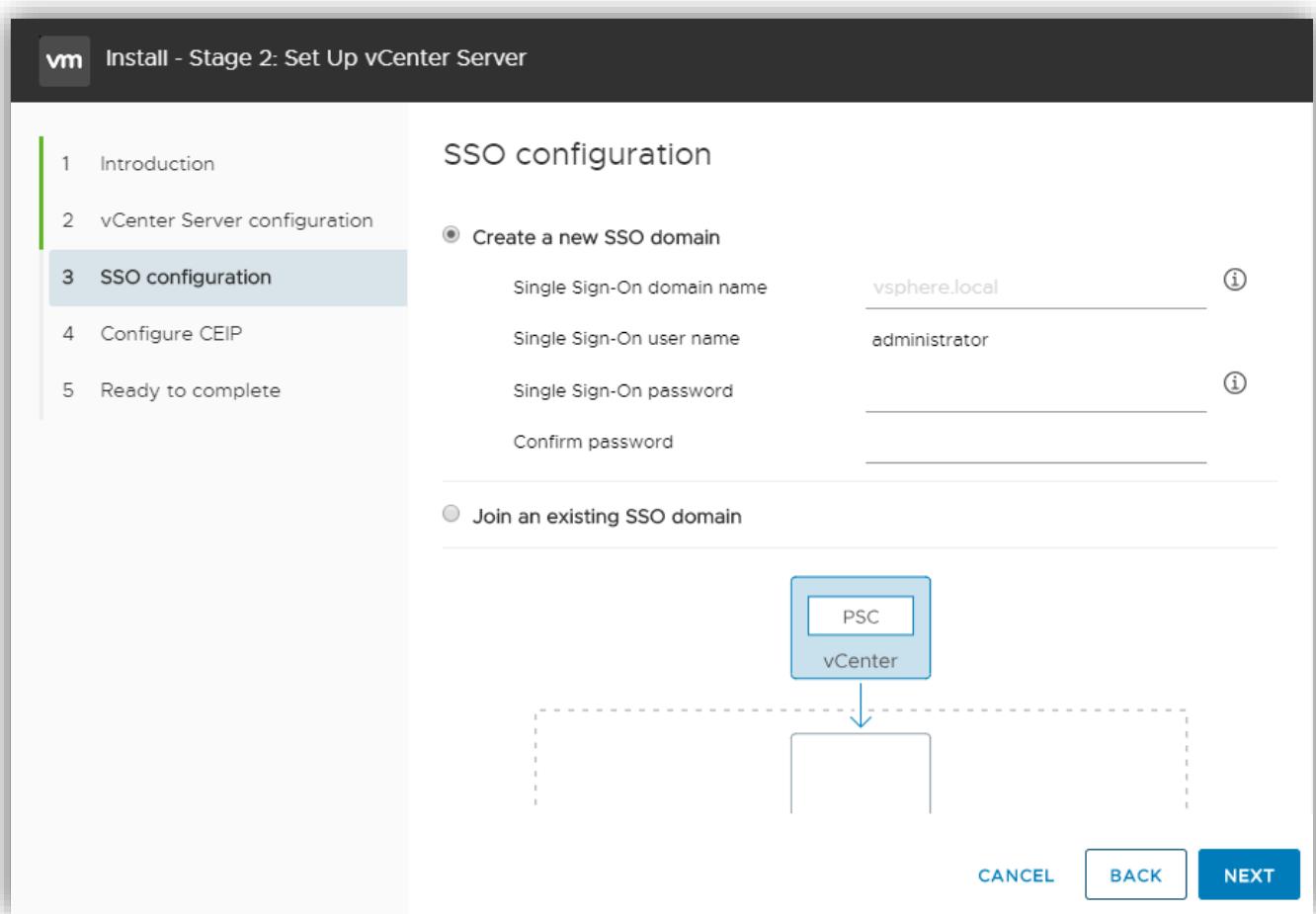
This service provides authentication services for vSphere software components, not just vCenter Server. It allows communication between the components via a secure token exchange, and all communication is encrypted. The default domain is vsphere.local, but can be changed during setup. It is also good to note that you don't want to have your single sign-on domain be the same as your Active Directory domain name. This can cause authentication problems if you do. Single sign-on can also authenticate from other identity sources, as well cover in Objective 4.3.2 and .3. Components of SSO include:

- STS (Security Token Service) – This component issues SAML tokens to represent the identity of a user. These tokens allow authentication to any service that uses SSO without needing to sign on to each individually. All tokens are signed with a certificate that is stored on disk.

- Administration Service – This component allows administrators or those with administrator services to configure SSO.
- VMware Directory Service (vmdir) – This component stores and manages SSO accounts and passwords. It also is an LDAP directory that replicates to peers and is available on port 389. If you have multiple vCenters in Enhanced Link Mode, this directory is replicated between all vCenters included.
- Identity Management Service – This component handles managing identity sources and STS authentication requests.

Objective 4.1.1 – Configure a single sign-on (SSO) domain

Configuring a single sign-on (SSO) domain is done during the initial setup of the vCenter Server Appliance. The vCenter Server Appliance install has two stages. Single sign-on installation happens in the second stage. Here is the screen to set up SSO. You have the option of creating a new SSO or joining an existing one.



To create a new, you will need to supply a domain name and password. Once again, make sure the domain name chosen is not the same as your Active Directory domain. After created, you will need to add users and groups or configure an identity source to enable other users.

Objective 4.1.2 – Join an existing single sign-on (SSO) domain

As with previous versions of vSphere, vCenter Server can be joined to an already existing SSO domain. This can be done both during the setup of the vCenter Server appliance, or it can be performed via command line later by repointing an appliance to the domain. Reasons to do this include:

- Simplified backup and restore process
- Single inventory view – ease of management
- Separation of resources or the ability to manage more resources than a single vCenter Server appliance can

Up to 15 vCenter Server appliances can be connected and displayed using a single-window view.

Objective 4.2 – Configure VSS advanced virtual networking options

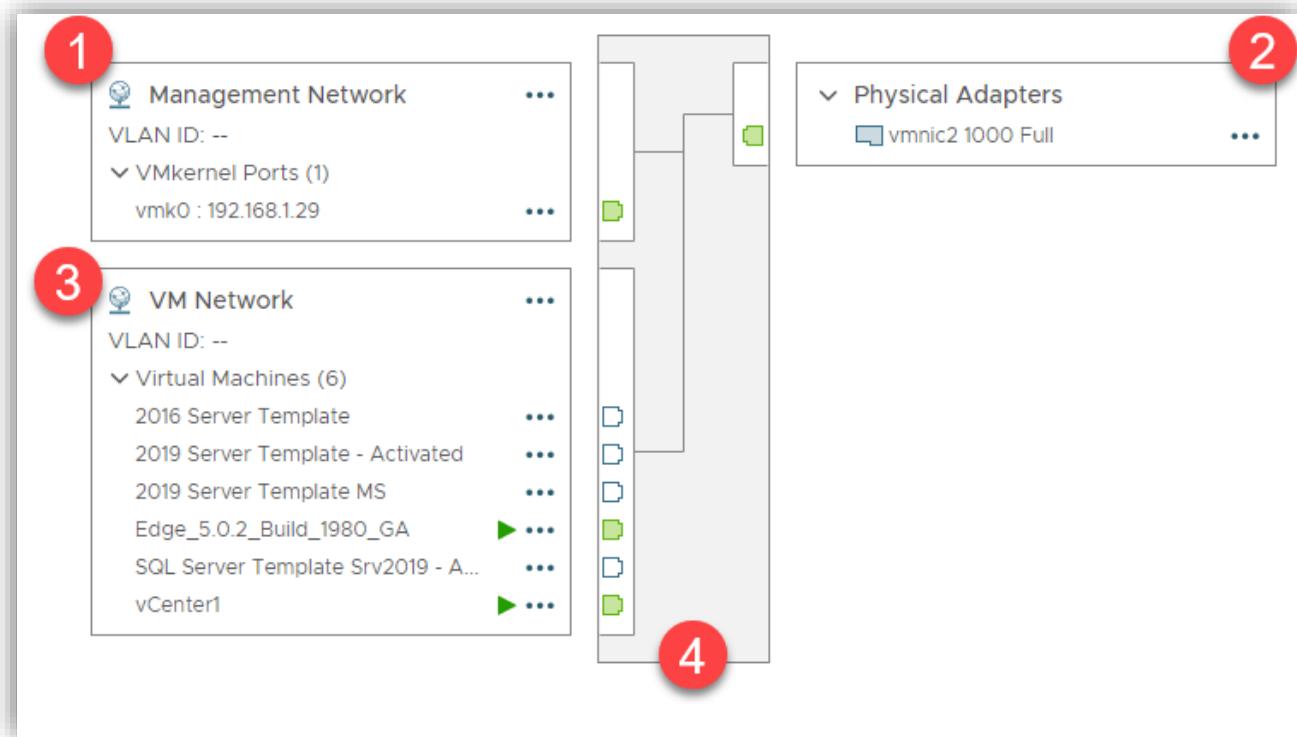
You configure virtual networking in different ways, depending on your environment. Configuring VSSs can be done using the ESXi HTML5 client as seen here

Name	Active p...	VLAN ID	Type	vSwitch	VMs
dv_PG_External	0	Unknown	Distributed virtual port group	dvSwitch	0
dvSwitch-DVUplinks-341	1	Unknown	Distributed virtual port group	dvSwitch	0
VM Network	3	0	Standard port group	vSwitch0	2
Management Network	1	0	Standard port group	vSwitch0	N/A

Physical NICs are how you access your Physical Network. You create VMKernel ports, which are how ESXi accesses the internal switch for management tasks, and you have Virtual switches to connect both. Finally, you have port groups, which is a grouping of vNICs or the virtual machine NICs. A better way to show this is with a picture.

1. These are the VMKernel ports – These are used for management tasks such as vMotion etc.
2. pNICs or Physical Network cards are on the other side and how you reach the physical network.
3. VM Network is the name of my Port Group, which is how I group all the NICs from the VMs underneath. I group them to perform tasks on all of them easier.

- The construct in the middle is my Virtual Switch. This one is a VSS



- These are the VMKernel ports – These are used for management tasks such as vMotion, etc.
- pNICs or Physical Network cards are on the other side and how you reach the physical network.
- VM Network is the name of my Port Group, which is how I group all the NICs from the VMs underneath. I group them to perform tasks on all of them easier.
- The construct in the middle is my Virtual Switch. Objective 4.3 – Set up identity sources

Advanced options for virtual standard switches are:

- MTU Size – Change the size of the IP packets being sent.
- Security – There are three options under here. Promiscuous Mode, MAC Address Changes, and Forged Transmits
- Traffic Shaping – on a VSS, you can only shape outgoing traffic
- Teaming and Failover – Control the path, load balancing algorithm, and what happens when the physical NICs fail.

The options we need to cover a bit more are Security and Teaming. Security settings include:

- Promiscuous Mode – This can be defined at the switch or port group level. If this is enabled, the VMs on that virtual switch can see all traffic traversing it.
- MAC Address changes – If this setting is set to accept, ESXi will allow requests to change the MAC address to something other than the original assigned to that virtual NIC. It will then accept traffic for the new MAC address. This is for inbound traffic.

- Forged Transmits – ESXi, by default, will check to make sure that the MAC address is transmitted by the guest OS is the same that as the source MAC address. This affects outbound traffic.

The last one we cover is Teaming and failover. You have 3 types of load balancing available + 1 failover:

- Route based on Originating Port ID – In this load balancing, each VM will take the next physical NIC in line as they transmit data.
- Route based on Source MAC Hash – In this load balancing method, each VM NICs MAC address is mapped to a specific physical NIC. This wont change unless the physical NIC fails.
- Route based on IP Hash – This method must be chosen if you want to use LACP or Etherchannel. With this load balancing method, you can link multiple physical NICs to form a single logical channel.
- Explicit Failover Order – No load balancing, just follows the failover order assigned.

Failover can use either link status or beaconing to detect a failure. You can decide what you want ESXi to do in case of failure. Failback will check to see if a failed NIC has recovered and, if so, return it to active duty. The notify switch option allows the host, if it has another physical NIC attached and active, to notify the switch of the failure.

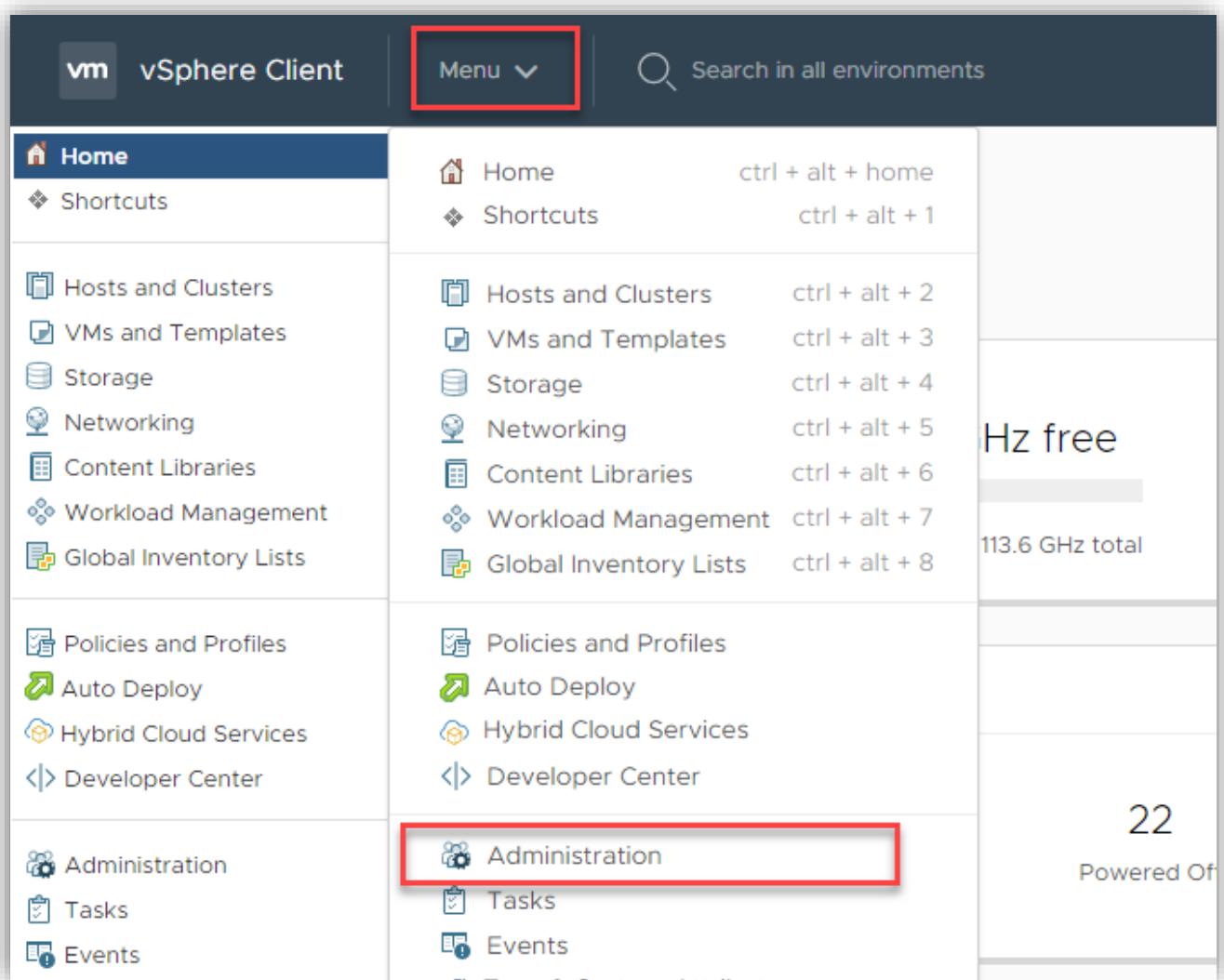
Objective 4.3 – Setup identity sources

Identity sources in vCenter Server allow users from other places, such as Active Directory, to log in to vCenter Server using the same username and password. Supported identity sources include

- Active Directory over LDAP
- Native Active Directory
- OpenLDAP directory

In this example, I add my Windows AD as an identity source. To add the identity source, do the following:

Click on the Menu and select Administration



Click on Configuration underneath Single Sign-On

Administration

▼ Access Control

- Roles
- Global Permissions

▼ Licensing

- Licenses

▼ Solutions

- Client Plugins
- vCenter Server Extensions

▼ Deployment

- System Configuration
- Customer Experience Improvement Pro...

▼ Support

- Upload File to Service Request

▼ Certificates

- Certificate Management

▼ Single Sign On

- Users and Groups

Configuration

If you haven't done so already, you must join the Active Directory Domain before adding it as an identity source. You do that by selecting the Active Directory Domain in the center pane. Click on Join AD.

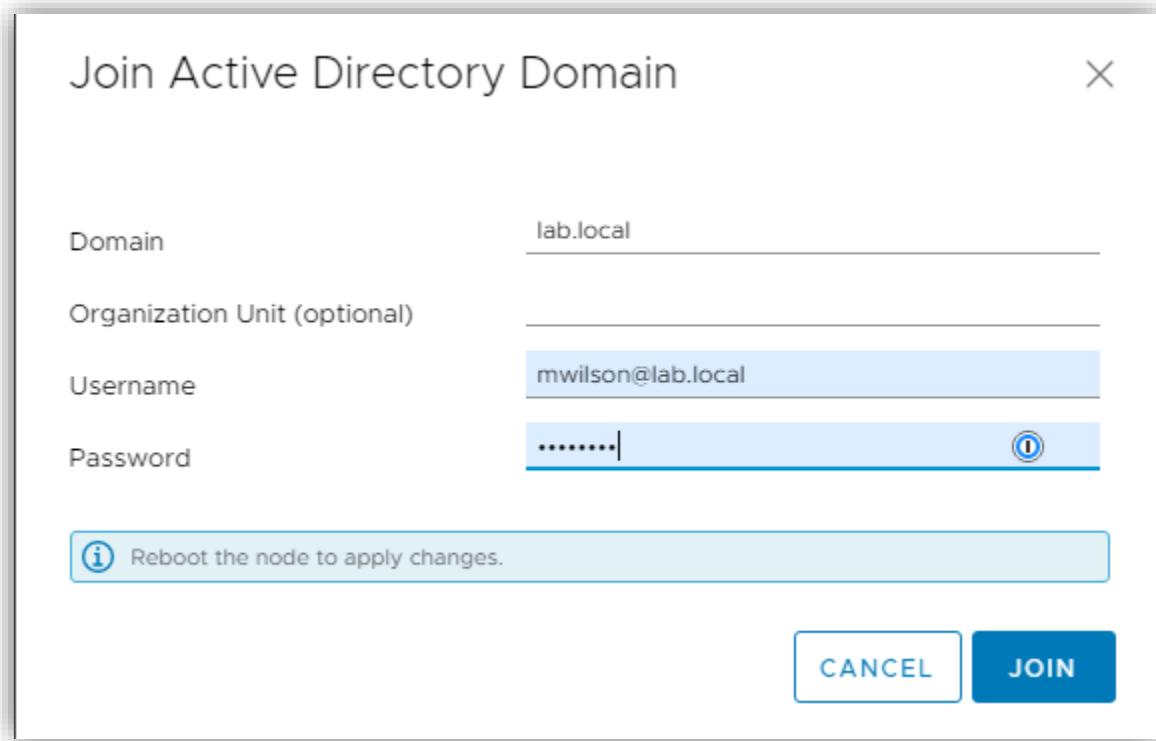
Configuration

Identity Provider Local Accounts Login Message

Type	Embedded
Identity Sources	
Active Directory Domain	JOIN AD LEAVE AD
Smart Card Authentication	

The node didn't join any Active Directory.

Fill out the needed information and select Join. You will need to reboot the vCenter Server node after this is done (just like a Windows machine, eh?)



You can reboot the node afterward, by selecting System Configuration from the left and then highlight the node, and click Reboot Node. Enter a reason on the popup and click reboot. You will lose connectivity to the vCenter Server during the reboot process.

The screenshot shows the vSphere Web Client interface. On the left, the navigation menu is visible with the following items:

- Administration
 - Access Control
 - Licensing
 - Solutions
 - Deployment
 - System Configuration** (highlighted with a red box)
 - Customer Experience Improve...

The main pane is titled 'System Configuration' and contains the following elements:

- Buttons: EXPORT SUPPORT BUNDLE and REBOOT NODE (REBOOT NODE is highlighted with a red box).
- A table with a single row:

	Node	Node Health
	mgmtVC.lab.local	Good

When the system comes back up, login and navigate to administration and Single sign-on again, now you should be able to add the Identity Source. Click on Add.

Configuration

Identity Provider

Local Accounts

Login Message

Type

Embedded

Identity Sources

Active Directory Domain
Smart Card Authentication

ADD

EDIT

SET AS DEFAULT

REMOVE

Name	Server URL	Type
--	--	System Domain
--	--	Local OS (Default)

In my case, I added a Windows Active Directory Domain, so it is already filled out for me. I can choose if I want to use a Machine Account (vCenter Server becomes a computer account in the domain) or if I want to use an SPN. I will leave it as a machine account. You could use SPN if you expect to change the computer name of vCenter at some point.

Add Identity Source

Identity Source Type

Active Directory (Integrated Windows Authentication)

Domain name * 

LAB.LOCAL

Use machine account

Use Service Principal Name (SPN)

CANCEL

ADD

I will now change the default authentication source to be the AD domain. If you set this, instead of needing to use your username@domain.com, you only have to use username.

Configuration

Identity Provider Local Accounts Login Message

CHANGE

Type

Embedded

Identity Sources

Active Directory Domain
Smart Card Authentication

ADD

EDIT

SET AS DEFAULT

REMOVE

Name	Server URL	Type	Domain
---	--	System Domain	vsphere.local
---	--	Local OS (Default)	localos
●	--	Active Directory (Integrated Windows Authentication)	LAB.LOCAL

You may need to add access to a user. To do this, click on users and groups on the left and then click on Groups and the group you want to edit. Click the ellipsis in front and click Edit.

Administration

- Access Control
 - Roles
 - Global Permissions
- Licensing
 - Licenses
- Solutions
 - Client Plugins
 - vCenter Server Extensions
- Deployment
 - System Configuration
 - Customer Experience Improve...
- Support
 - Upload File to Service Request
- Single Sign On
 - Users and Groups**
 - Configuration
- Certificates
 - Certificate Management

Users and Groups

Users **Groups**

ADD GROUP

Group Name	Description
ExternalIDPUsers	Well-known external IDP
RegistryAdministrators	Allows members to man...
ComponentManager.Administrators	Component Manager Adm...
ServiceProviderUsers	Users allowed to manag...
AutoUpdate	Users allowed to perform...
NsxViAdministrators	SSO group to manage N...
Administrators	
DCClients	

Then select the domain you will be pulling the user from and then type in the username. It should auto finish for you and then click Save

Edit Group

X

Group Name *

Administrators

Description

Add Members *

LAB.LOCAL

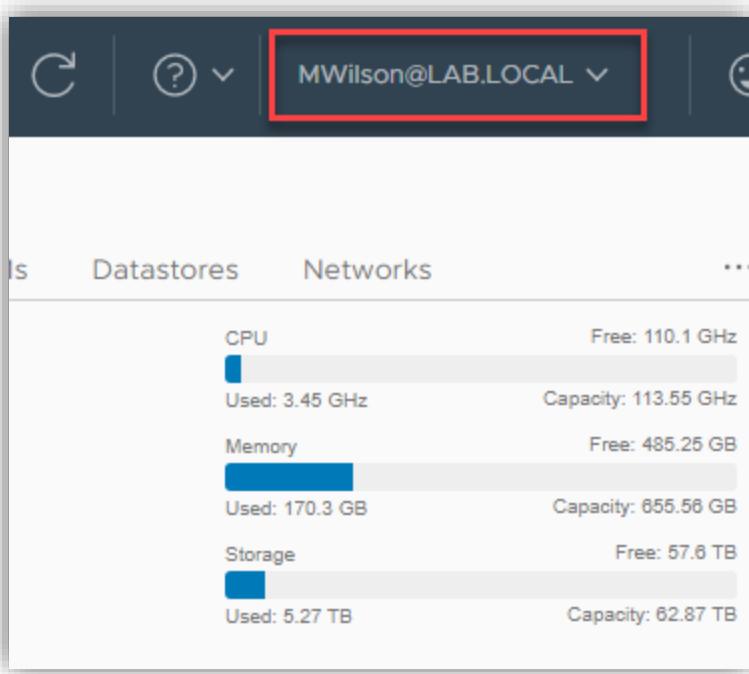
Mwilson

Administrator X

CANCEL

SAVE

Now log out and try again. Success!



Objective 4.3.1 – Configure Identity Federation

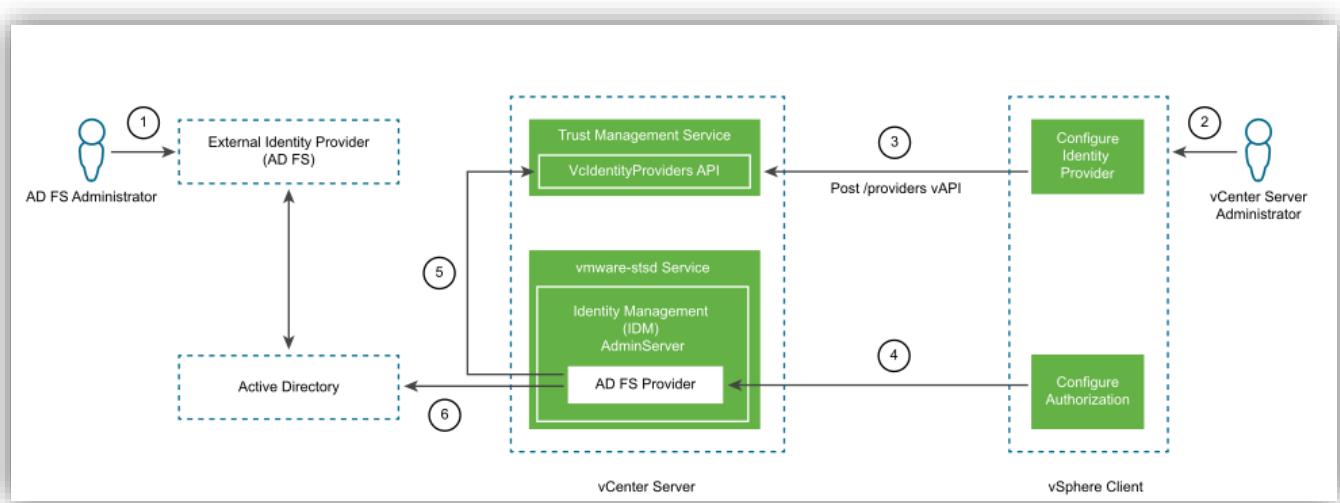
With vCenter Server federation, you are authenticating with Active Directory. How is this different from regular? With federation in place, you aren't providing your credentials to vCenter Server at all. vCenter Server trusts Active Directory, and it redirects the credentials to AD. How is this better?

- You can use SSO with existing apps and infrastructure you've already set up.
- Security is better since vCenter doesn't handle credentials
- You can use additional authentication mechanisms such as Multi-Factor Authentication

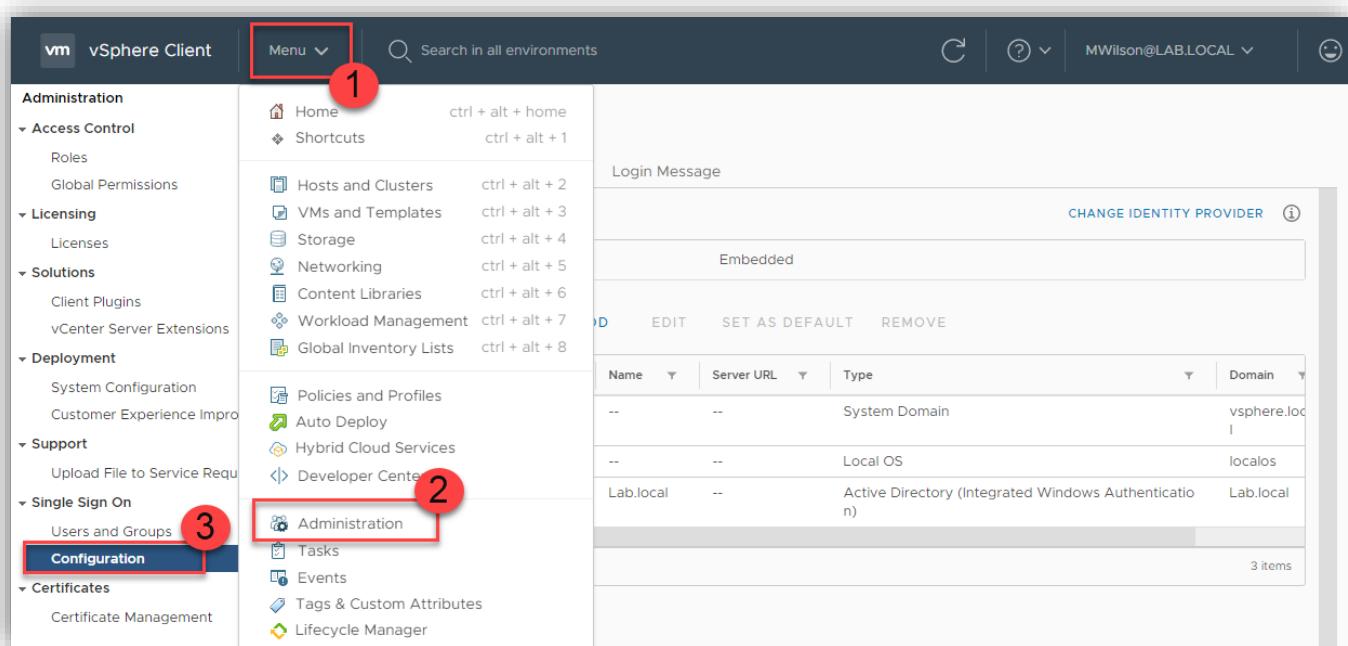
Currently, vCenter Server only supports Microsoft Active Directory Federation Services. The components needed are:

- vCenter Server
- The identity provider service configured on the vCenter Server
- An AD FS server and AD domain
- An AD FS Application Group
- AD groups and users that map to the vCenter Server

To configure it, you need to follow the flow set here. Here is the flow chart VMware provides for this.



I'm only going to cover the vCenter piece of this. To do this, you will need to go back to the Administration > Configuration.



Click on the **I** next to Change Identity Provider on the right side. Copy both of the links that pop up. You will need these later.

Configuration

Identity Provider Local Accounts Login Message

CHANGE IDENTITY PROVIDER (1)

Type
Active Directory Domain
Smart Card Authentication

Change Identity Provider

vCenter Server supports external identity providers to manage your users and groups. You can migrate from using the embedded vCenter Server identity provider to an external identity provider. For more information, see the vSphere documentation.

Redirect URIs

`https://mgmtVC.lab.local/ui/login` COPY URI

`https://mgmtVC.lab.local/ui/login/oauth2/authcode` COPY URI

You need to create an OpenID Connect configuration in AD FS and configure it for vCenter. Follow the directions [here](#) to do that in Windows 2016. Record the following when you created the AD FS group.

- Client Identifier
- Shared Secret
- OpenID address of the AD FS server

When that is complete, go back to your vCenter Server and click on the Change Identity Provider link on the right side.

Configuration

Identity Provider Local Accounts Login Message

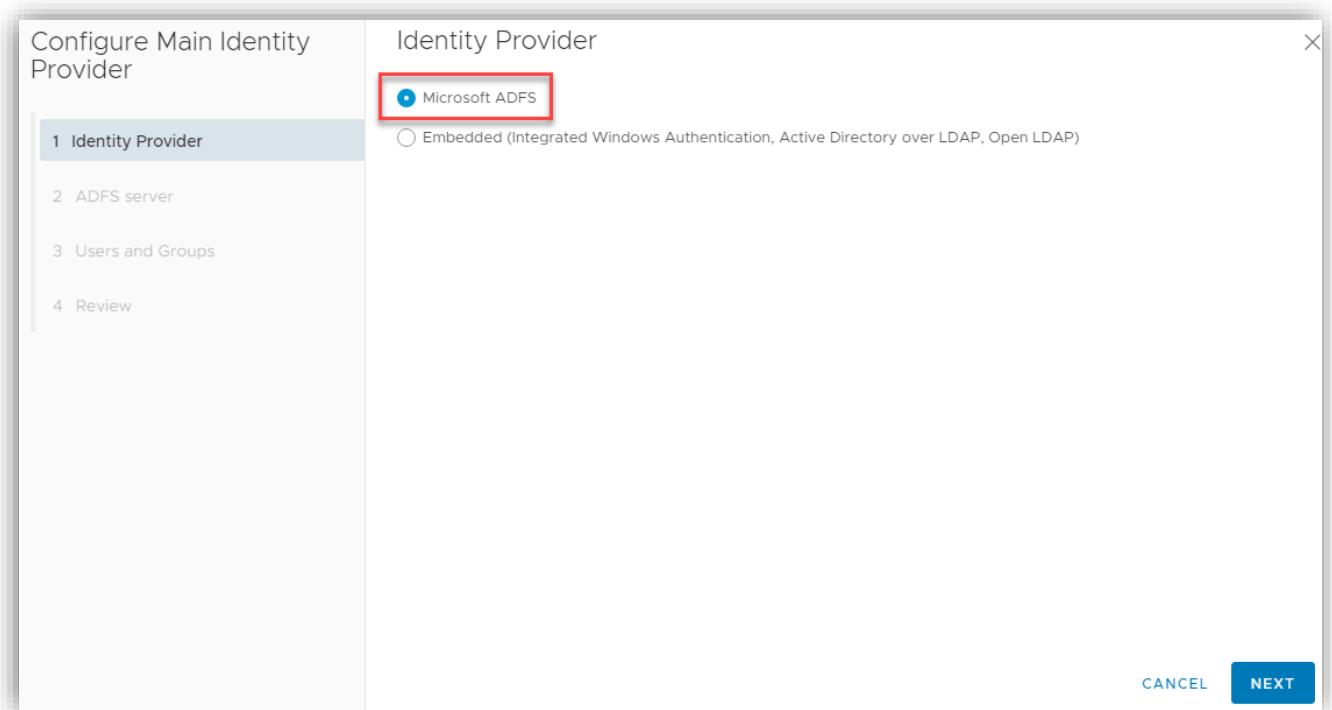
CHANGE IDENTITY PROVIDER (1)

Type	Embedded
Active Directory Domain	
Smart Card Authentication	

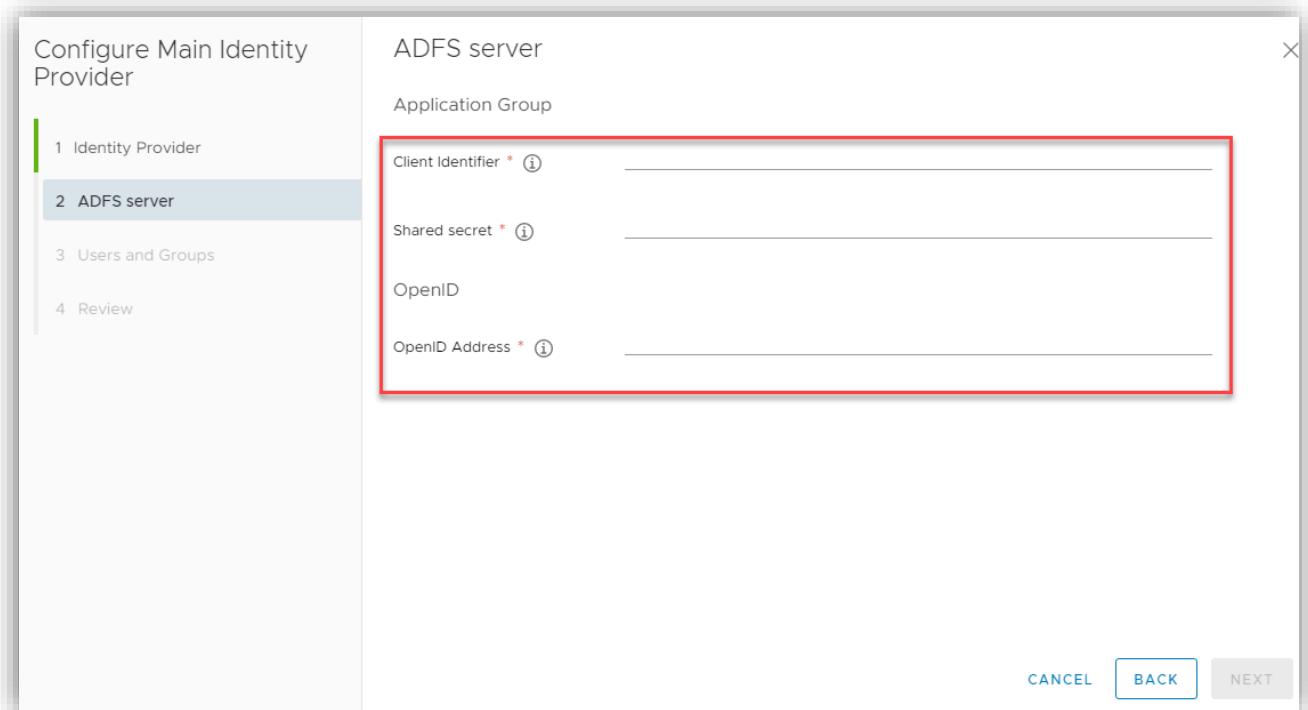
ADD EDIT SET AS DEFAULT REMOVE

Name	Server URL	Type	Domain	Alias
--	--	System Domain	vsphere.local	--
--	--	Local OS	localos	--
Lab.local	--	Active Directory (Integrated Windows Authentication)	Lab.local	Lab.local

This link brings up a wizard to configure the Main Identity Provider. Select Microsoft ADFS and click Next



This step, you will enter the information you wrote down from the AD FS server above.



For the next screen, enter user and group information for AD over LDAP connection.

The screenshot shows a configuration dialog titled 'Configure Main Identity Provider'. On the left, a vertical navigation bar lists four steps: 1. Identity Provider, 2. ADFS server, 3. Users and Groups (which is selected and highlighted in blue), and 4. Review. The main right panel is titled 'Users and Groups' and contains the following fields:

- Base distinguished name for users: [text input field]
- Base distinguished name for groups: [text input field]
- Username ⓘ: [text input field]
- Password: [text input field]
- Primary server url ⓘ: [text input field]
- Secondary server url: [text input field]
- SSL certificates ⓘ: [button labeled 'BROWSE']
A message box below says 'No certificates added.'

At the bottom right are three buttons: 'CANCEL', 'BACK' (in a blue box), and 'NEXT'.

Definitions for the fields are as follows:

- Base Distinguished name for users – This will be in the form `DC=example, DC=com`
- Base Distinguished name for groups – This looks something like this
`CN=Users, CN=BuiltIn, DC=example, DC=com`
- Username – ID of a user with a minimum of read access to the Base DN for the users and groups.
- Password – Password for the above user
- Primary Server URL – Primary domain controller LDAP server for the domain. Use the format `ldap://hostname:port` or `ldaps://hostname:port`
- Secondary Server URL – Second LDAP domain controller used for failover
- SSL certificates – if you want to use secure LDAP with your LDAP server

Finish that up and then assign users using that domain as you would for other identity providers

Objective 4.3.2 – Configure Lightweight Directory Access Protocol (LDAP) integration
LDAP has two supported options. Active Directory over LDAP and OpenLDAP. To choose one of these options, go back to the same place in Menu > Administration > Configuration and click on Add

Add Identity Source

X

Identity Source Type

Open LDAP

Identity source name *

Active Directory (Integrated Windows Authentication)

Active Directory over LDAP

Open LDAP

Local operating system of SSO server

Base distinguished name for users *

Base distinguished name for groups *

Domain name * ⓘ

Domain alias ⓘ

Username * ⓘ

Password *

Primary server url * ⓘ

Secondary server url

SSL certificates ⓘ

BROWSE

No certificates added.

CANCEL

ADD

Here are your options. If you click on Open LDAP, you must fill out the above information. The definitions and syntax will be the same as shown above – here it is again, so you don't need to click up.

- Base Distinguished name for users – This will be in the form `DC=example,DC=com`
- Base Distinguished name for groups – This looks something like this
`CN=Users,CN=BuiltIn,DC=example,DC=com`
- Domain Name – This is the fully qualified domain name. Do not provide an IP address.
- Domain Alias – This is also known as the NETBIOS name.
- Username – ID of a user with a minimum of read access to the Base DN for the users and groups.
- Password – Password for the above user
- Primary Server URL – Primary domain controller LDAP server for the domain. Use the format
`ldap://hostname:port` or `ldaps://hostname:port`
- Secondary Server URL – Second LDAP domain controller used for failover
- SSL certificates – if you want to use secure LDAP with your LDAP server

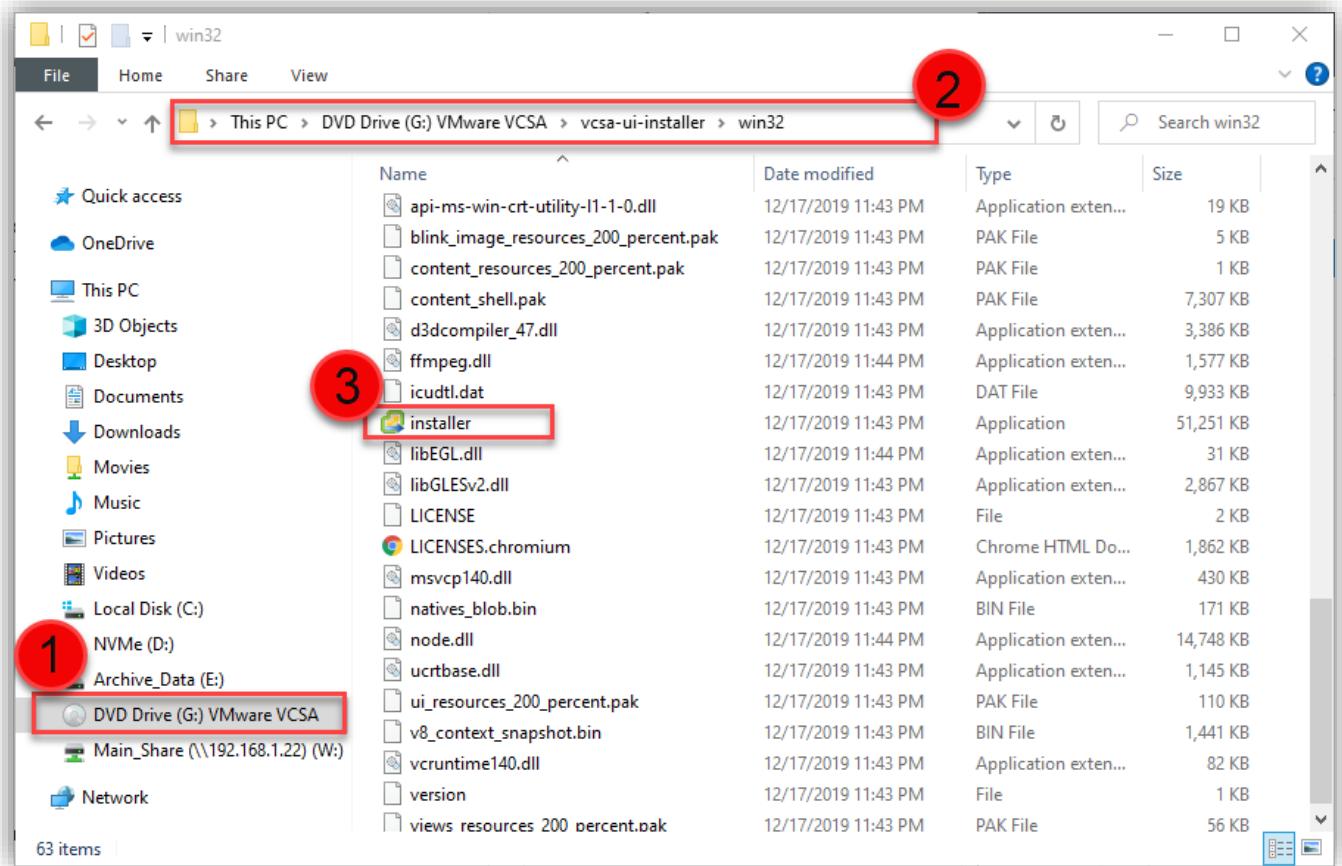
Objective 4.3.3 – Configure Active Directory integration

For this one, see above Objective 4.3, as that is the one I chose to do first.

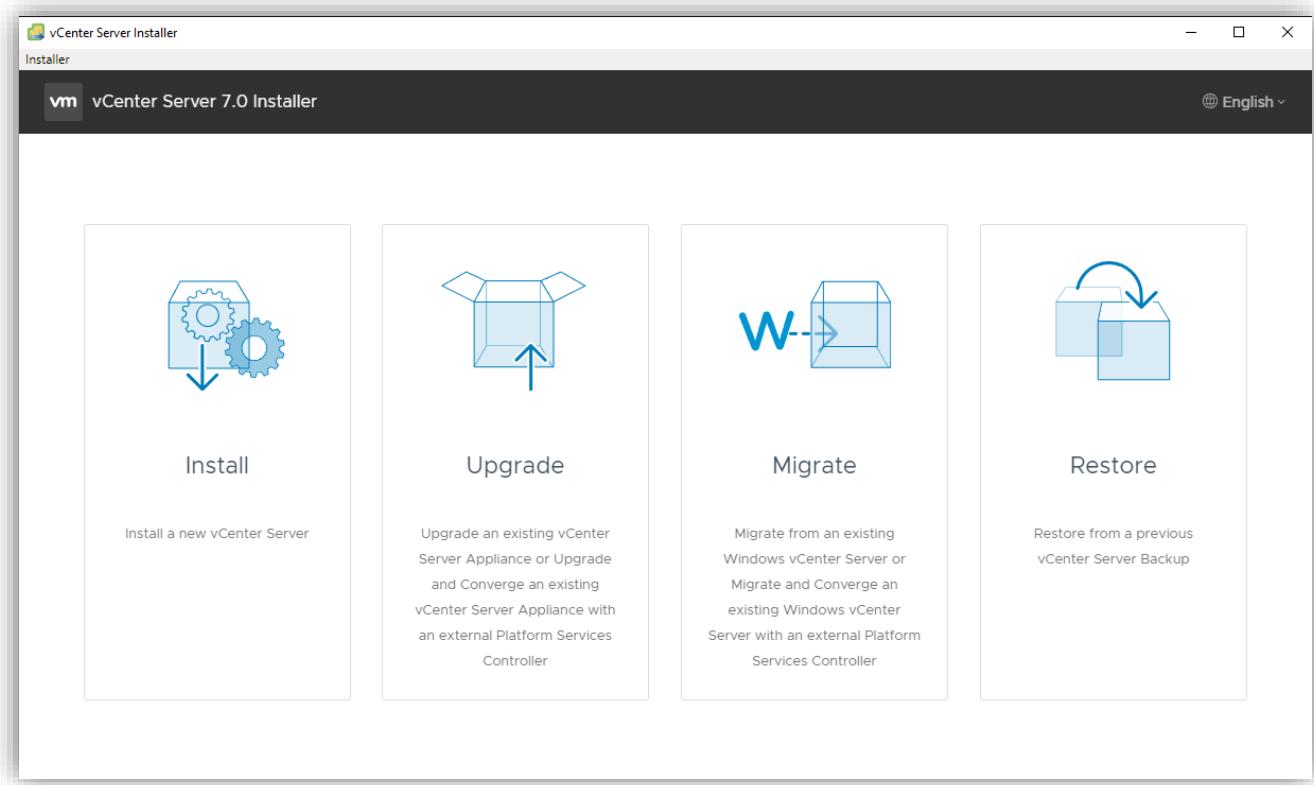
Objective 4.4 – Deploy and configure vCenter Server Appliance

The vCenter Server Appliance can be configured both from a GUI and CLI. The steps I show here will be using the GUI.

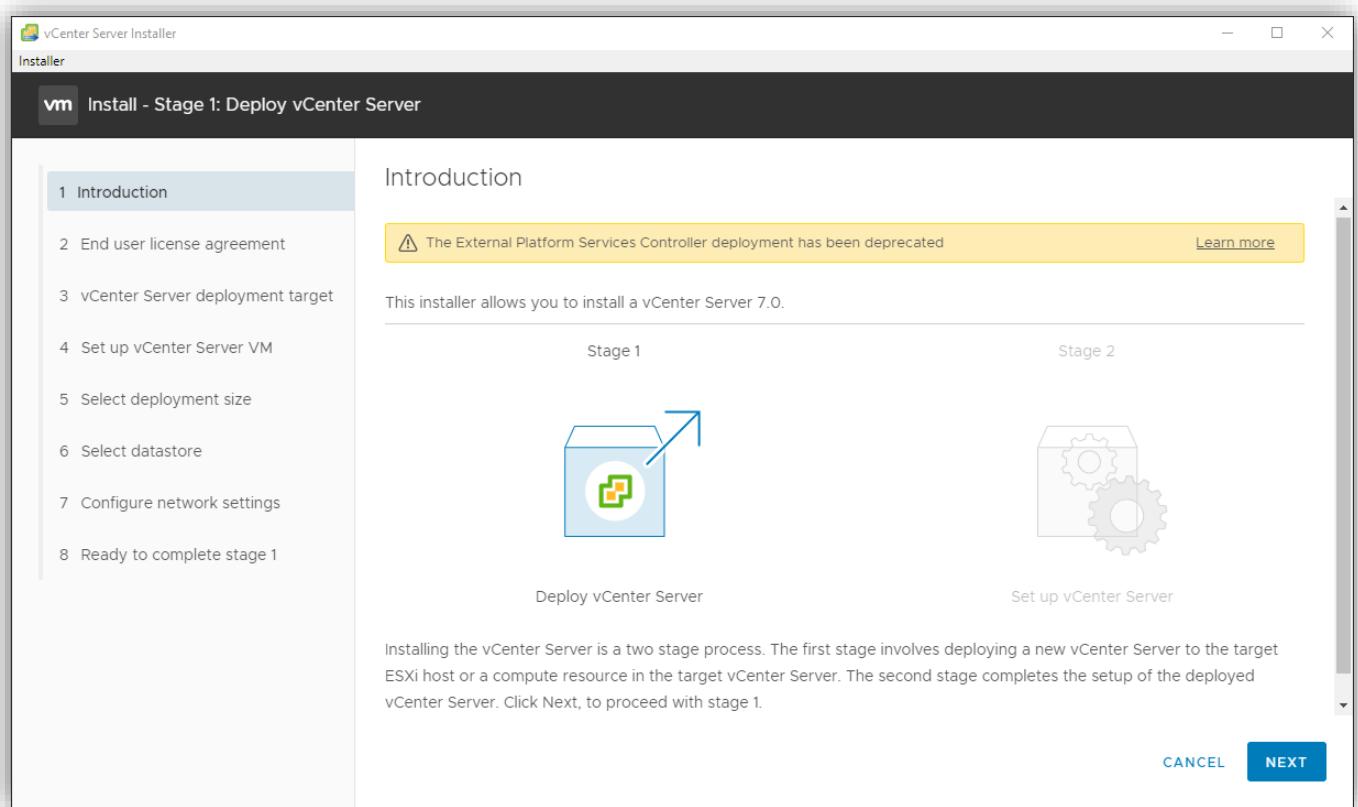
The download from VMware is an ISO file. This ISO can either be unzipped or, using Windows 10, and you can double click on it to mount the CD on your computer. Then navigate down to the following folder (this is different if you are using Linux or Mac)



Run the executable shown in the picture. Once this is run, you have the following screen appear.

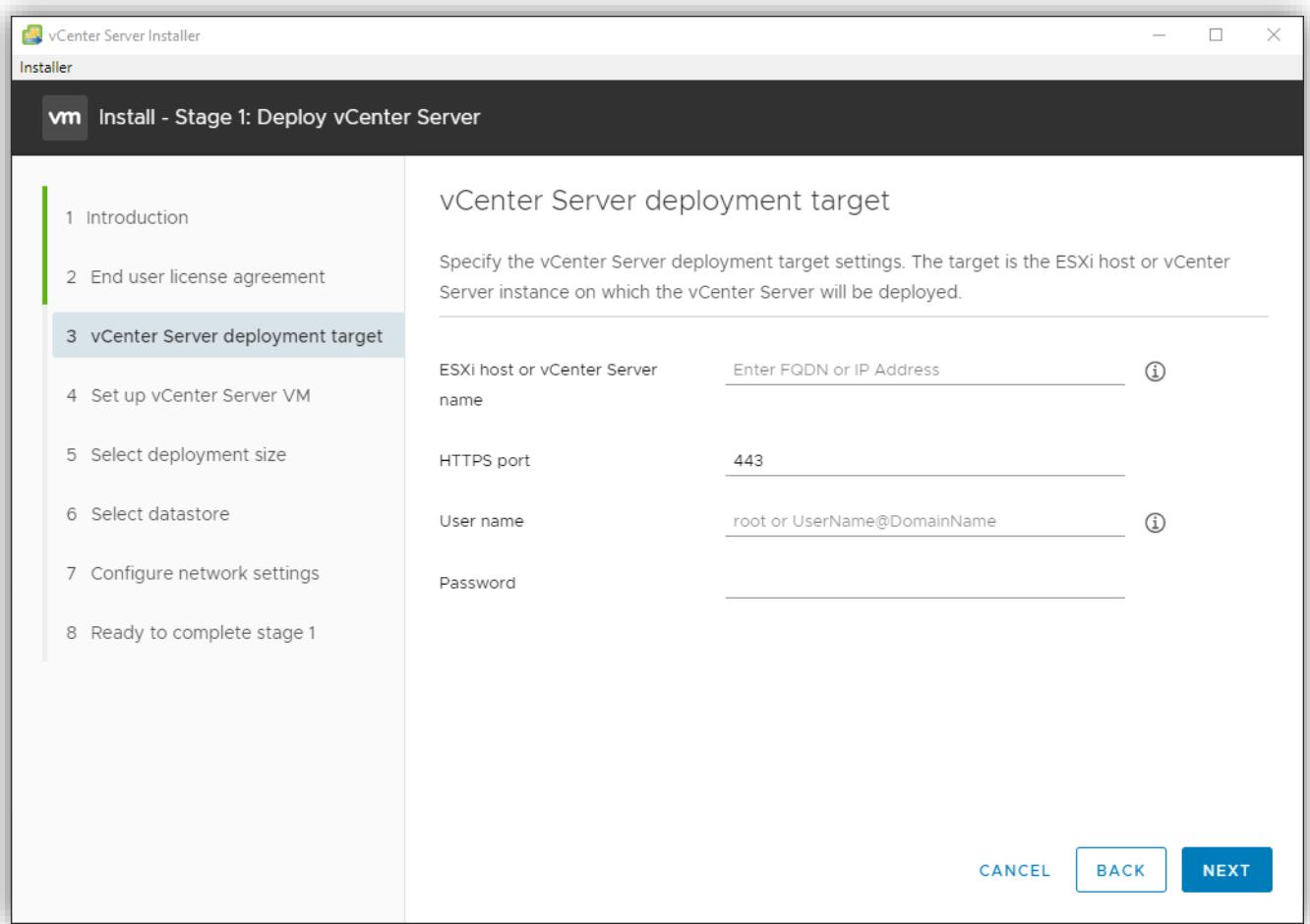


To install a new vCenter Server Appliance, click on Install. The following screen appears. It describes the first of two stages for the vCenter Server Appliance install.



Select Next. Accept the terms of the License Agreement and click Next.

You need to enter the ESXi host or vCenter Server you will install this vCenter to. You also need to tell it the port (default is 443) and then enter the username and password for the resource you want to use.



Accept the Certificate Warning and give the vCenter Server a name and password.



Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM**
- 5 Select deployment size
- 6 Select datastore
- 7 Configure network settings
- 8 Ready to complete stage 1

Set up vCenter Server VM

Specify the VM settings for the vCenter Server to be deployed.

VM name ⓘ

Set root password

Confirm root password

CANCEL

BACK

NEXT

You now need to decide the size of your vCenter Server. This will be dictated by the number of hosts and services you are using.

vm Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM
- 5 Select deployment size
- 6 Select datastore
- 7 Configure network settings
- 8 Ready to complete stage 1

Select deployment size

Select the deployment size for this vCenter Server.

For more information on deployment sizes, refer to the vSphere 7.0 documentation.

Deployment size Medium ▾
Storage size Default ▾ (i)

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	12	415	10	100
Small	4	19	480	100	1000
Medium	8	28	700	400	4000
Large	16	37	1065	1000	10000
X-Large	24	56	1805	2000	35000

CANCEL

BACK

NEXT

Select the datastore you will use for the vCenter Server files.

vm Install - Stage 1: Deploy vCenter Server

- 1 Introduction
- 2 End user license agreement
- 3 vCenter Server deployment target
- 4 Set up vCenter Server VM
- 5 Select deployment size
- 6 Select datastore**
- 7 Configure network settings
- 8 Ready to complete stage 1

Select datastore

Select the storage location for this vCenter Server

Install on an existing datastore accessible from the target host

Show only compatible datastores

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
 0 item					

Install on a new vSAN cluster containing the target host (i)

CANCEL

BACK

NEXT

Configure your network settings.

vm Install - Stage 1: Deploy vCenter Server

Step	Description
1	Introduction
2	End user license agreement
3	vCenter Server deployment target
4	Set up vCenter Server VM
5	Select deployment size
6	Select datastore
7	Claim disks for vSAN
8	Configure network settings
9	Ready to complete stage 1

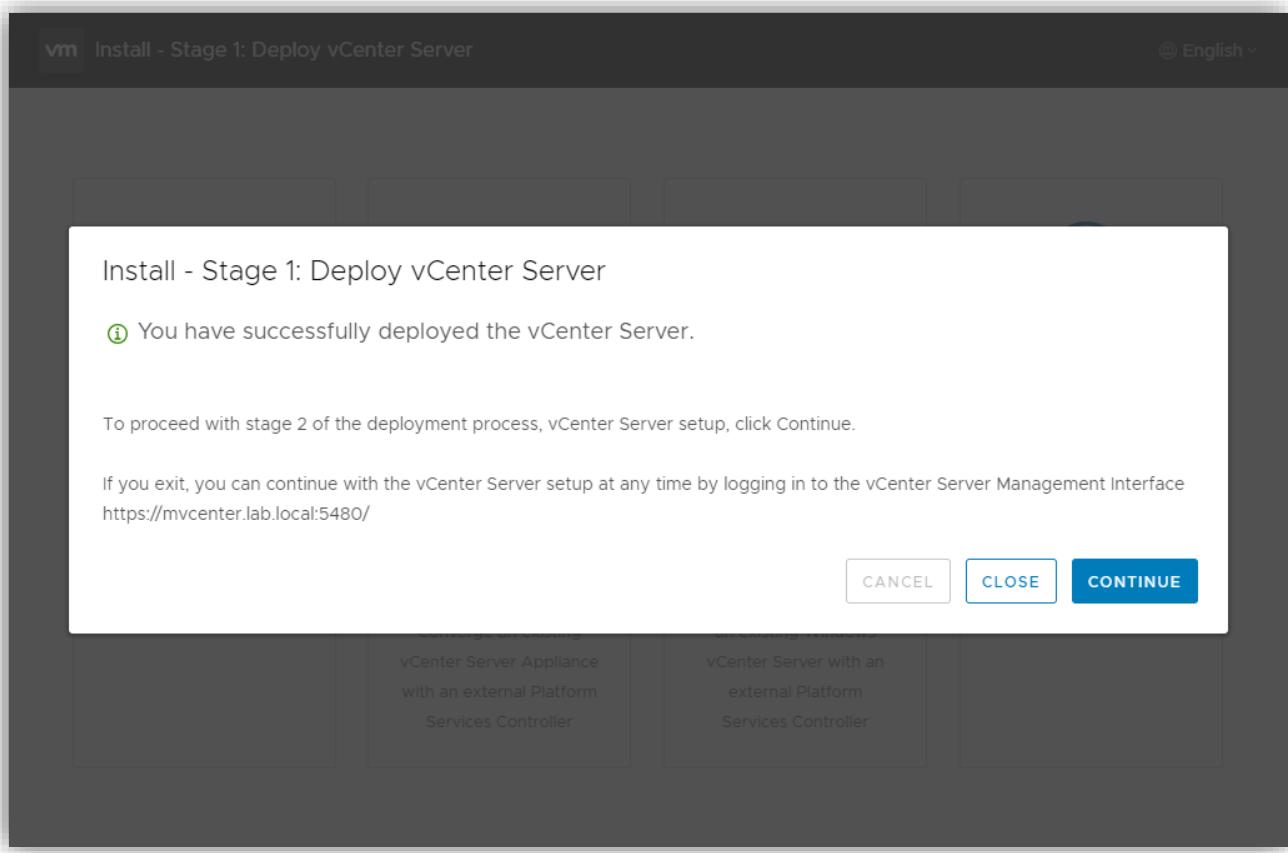
Configure network settings

Configure network settings for this vCenter Server

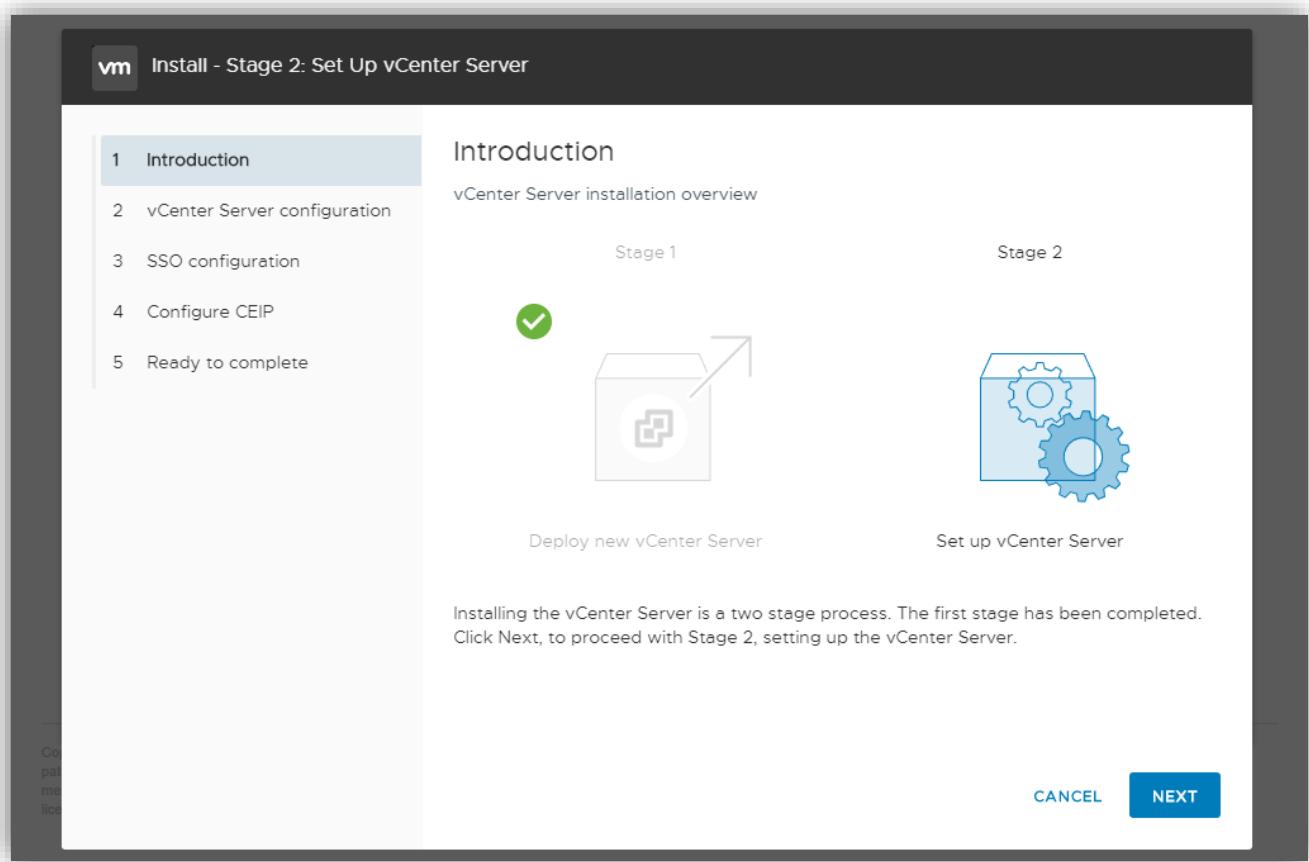
Network	VM Network	(i)
IP version	IPv4	
IP assignment	static	
FQDN	mvccenter.lab.local	(i)
IP address	192.168.1.12	
Subnet mask or prefix length	255.255.255.0	(i)
Default gateway	192.168.1.1	
DNS servers	192.168.1.20,192.168.1.16	

CANCEL **BACK** **NEXT**

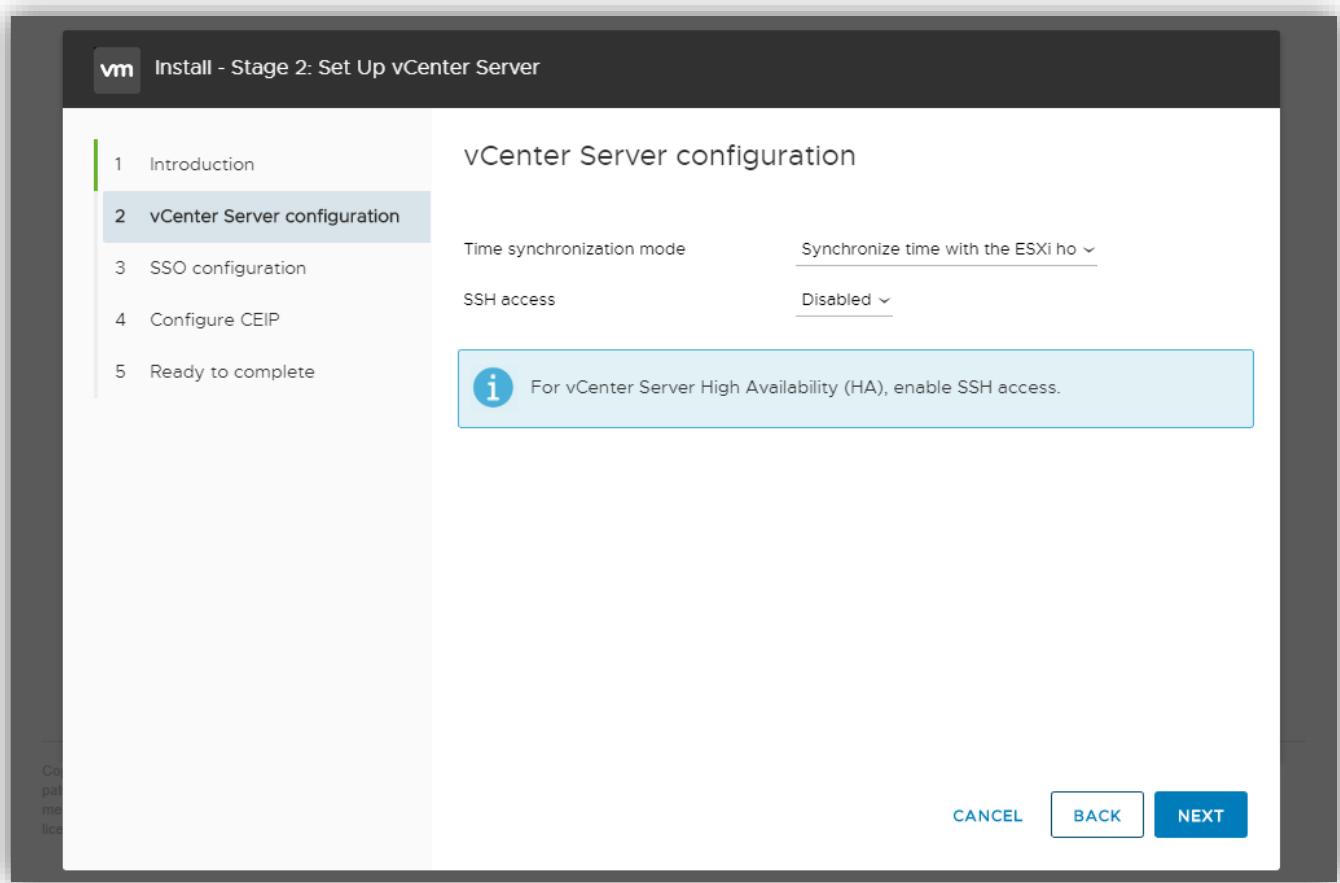
Review and start the install. When Stage 1 is complete, you will get the following screen.



Continue on to the Second Stage – this is where you configure the vCenter Server.



First step, set up time synch and SSH access.



Next, we need to create a new SSO domain or join an existing SSO domain.

vm Install - Stage 2: Set Up vCenter Server

1 Introduction
2 vCenter Server configuration
3 SSO configuration
4 Configure CEIP
5 Ready to complete

SSO configuration

Create a new SSO domain

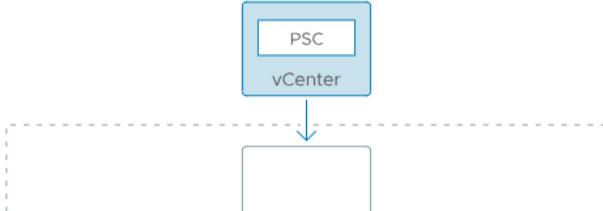
Single Sign-On domain name: vsphere.local (i)

Single Sign-On user name: administrator (i)

Single Sign-On password: (i)

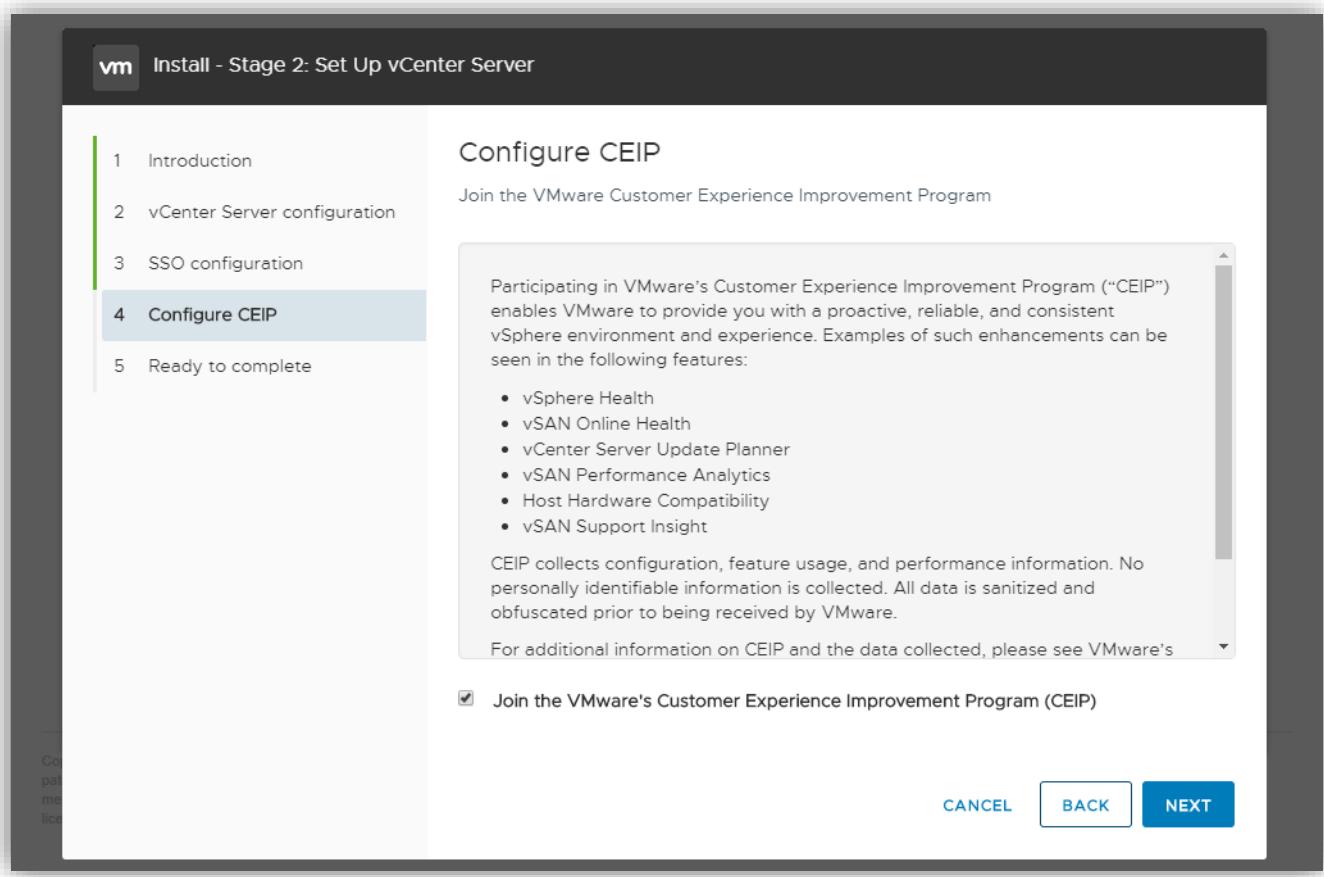
Confirm password: (i)

Join an existing SSO domain

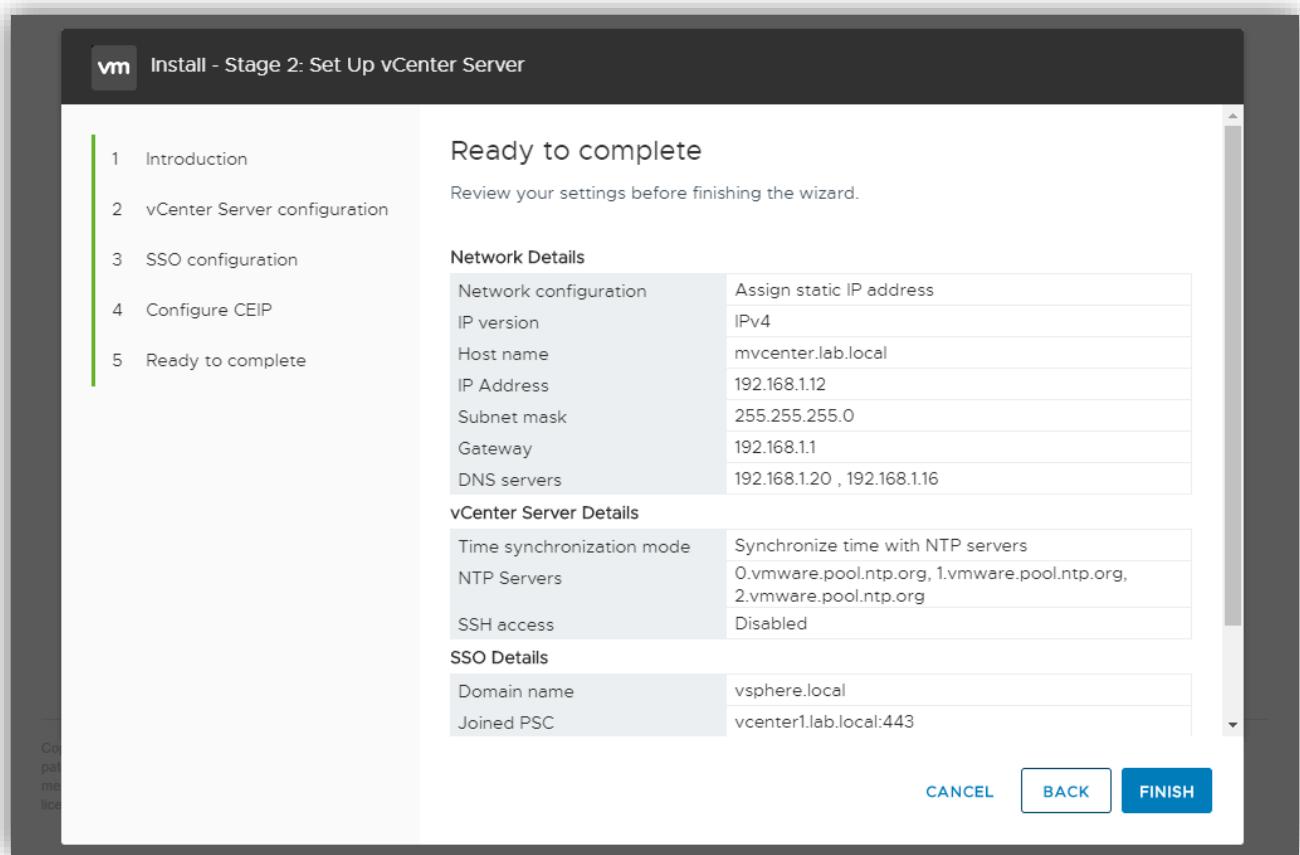


CANCEL BACK NEXT

You now need to decide if you want to join the VMware Customer Experience Improvement Program. This means you will be sending information back to VMware, although it is scrubbed of identifying data.



Review the information and then click Finish.

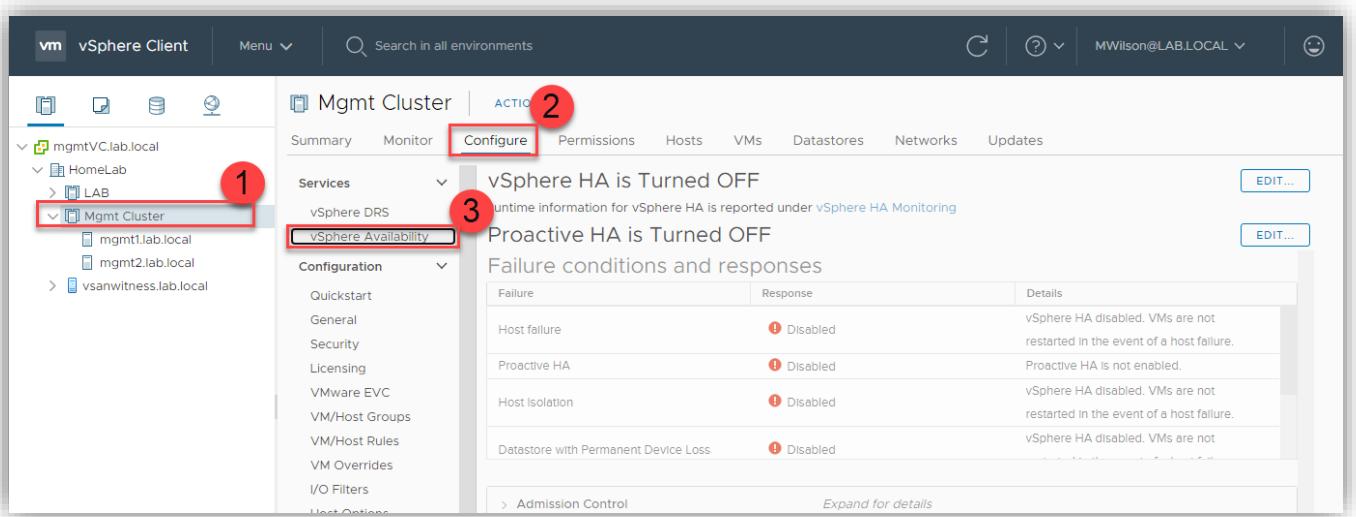


There are more configuration options you can do, such as backups, but that will be later.

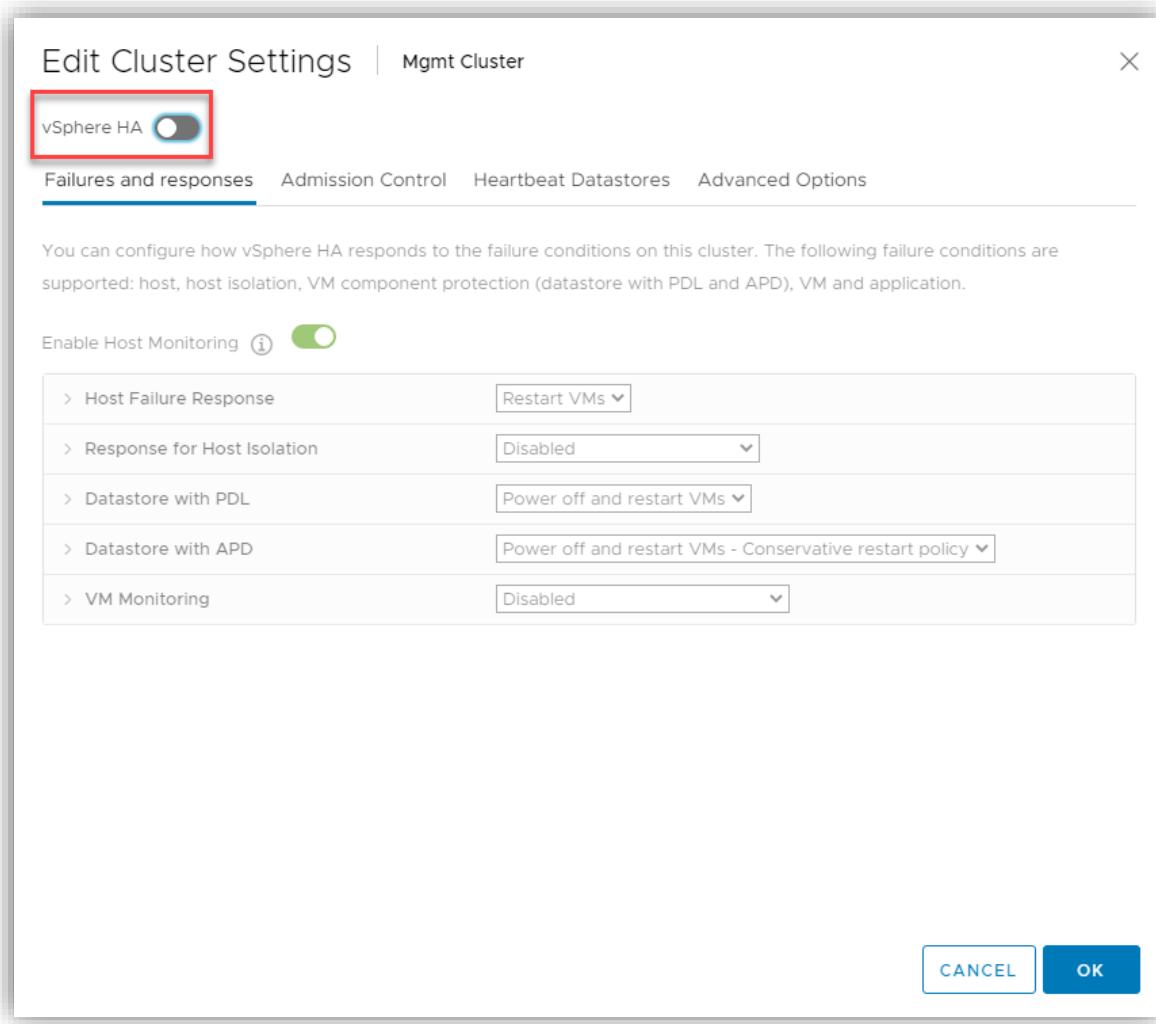
Objective 4.5 – Create and configure VMware High Availability and advanced options (Admission Control, Proactive High Availability, etc.)

We've already covered what VMware HA and its advanced options are/do. Let's discuss how to configure it.

First, click on the cluster you want to work on. Next click on Configure, then on vSphere Availability



Then click on Edit for vSphere HA.



To activate HA, you will need to click on the toggle shown. This enables the rest of the options on here. You can configure them as your environment needs. Again, if you need to, go back to the first section (Objective 1.6.4) to remind yourself what those options do. The screens look like this

Admission Control

Edit Cluster Settings | Mgmt Cluster

X

vSphere HA

Failures and responses **Admission Control** Heartbeat Datastores Advanced Options

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

Host failures cluster tolerates

1

Maximum is one less than number of hosts in cluster.

Define host failover capacity by

Cluster resource Percentage

Override calculated failover capacity.

Reserved failover CPU capacity: % CPU

Reserved failover Memory capacity: % Memory

Performance degradation VMs tolerate

%

Percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure. 0% - Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart. 100% - Warning is disabled.

CANCEL

OK

Heartbeat Datastores

Edit Cluster Settings | Mgmt Cluster X

vSphere HA ON

Failures and responses Admission Control **Heartbeat Datastores** Advanced Options

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

Heartbeat datastore selection policy:

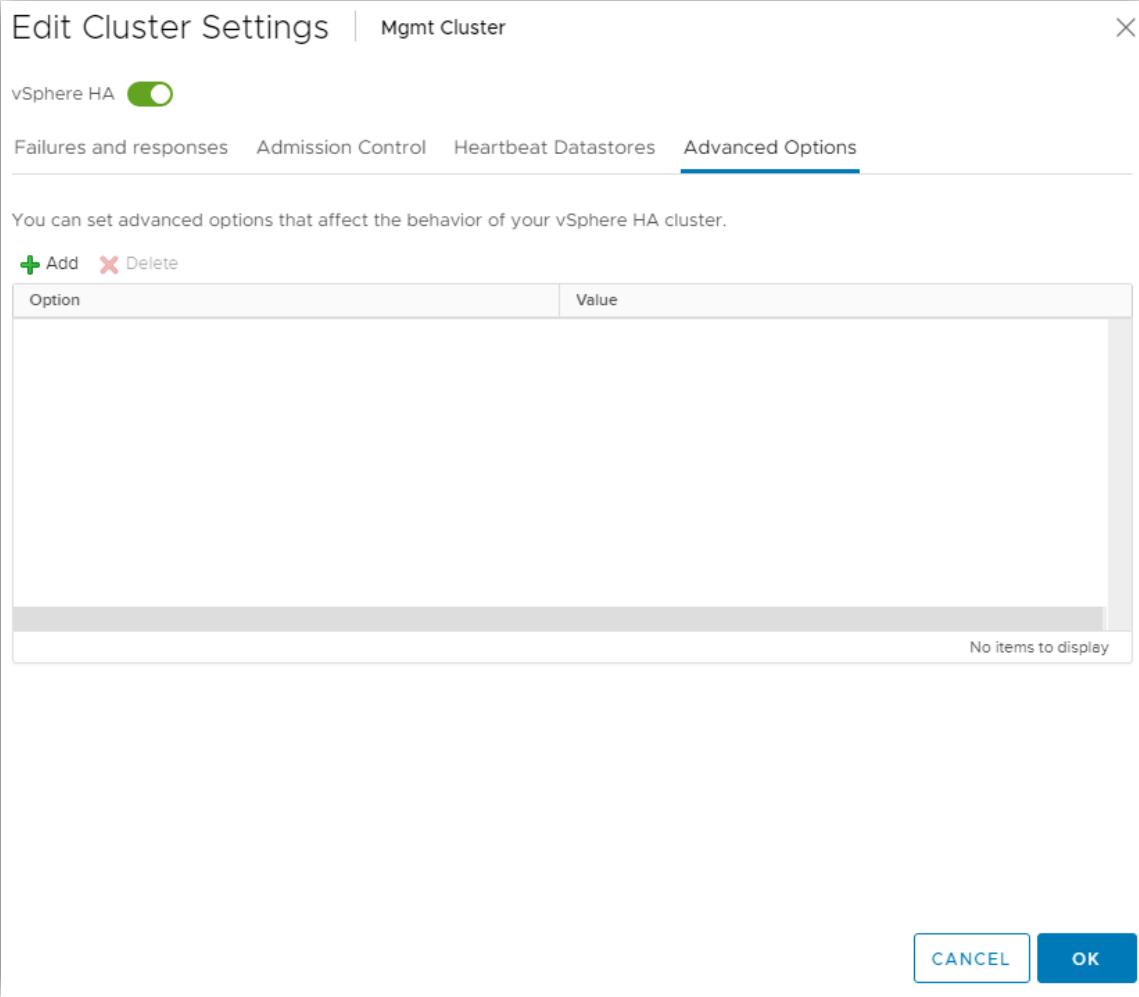
Automatically select datastores accessible from the hosts
 Use datastores only from the specified list
 Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

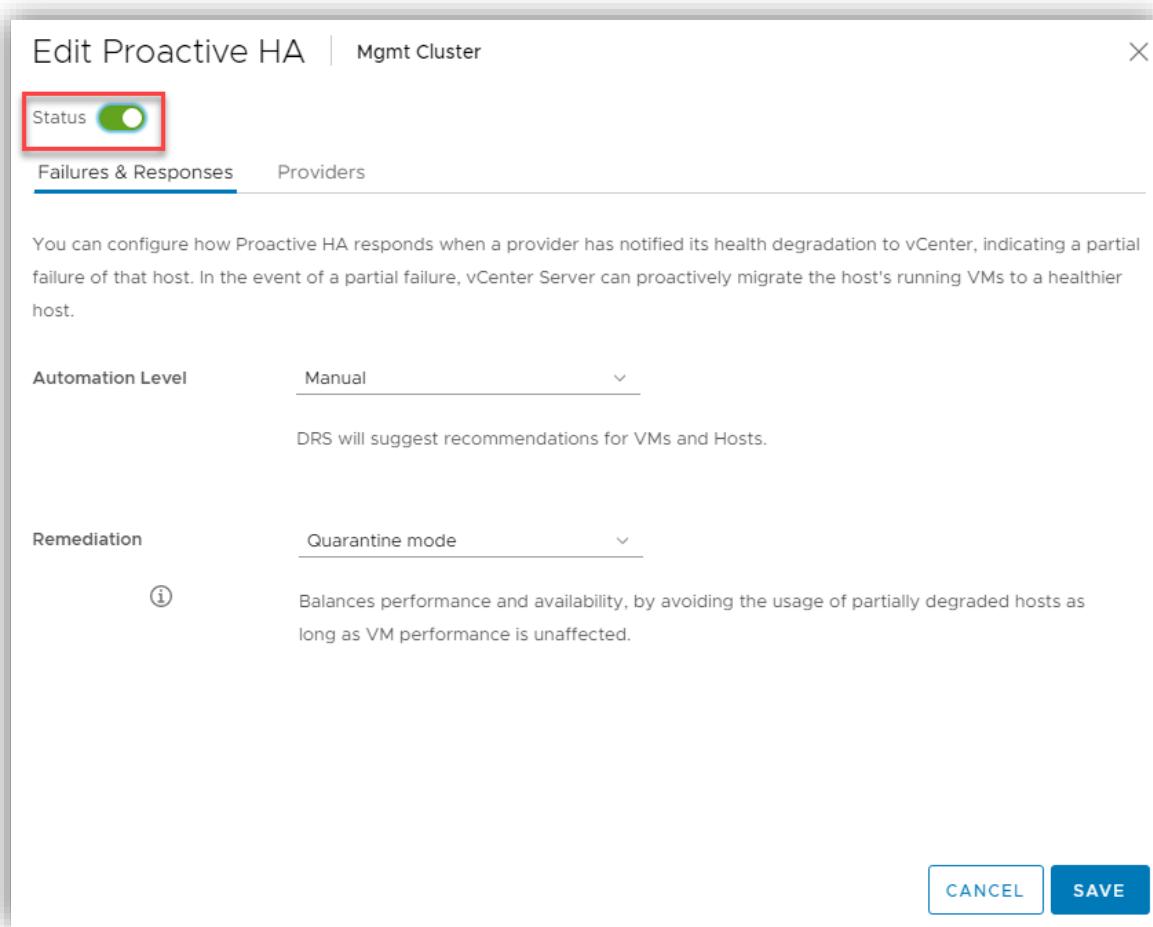
Name	Datastore Cluster	Hosts Mounting Datastore ↓

CANCEL OK

Advanced Options



To enable Proactive HA, click on the Edit button on Proactive HA.



You will need to click on the toggle to enable this as well. Keep in mind that if no provider is found, it won't have any automated response.

Objective 4.6 – Deploy and configure vCenter Server High Availability

We covered the concept of vCenter HA back in Objective 1.2. Quick refresher for you though. vCenter Server HA works by using a total of 3 nodes. One Active, one passive, and one witness nodes. The active node is the only machine the admin will interact with. All the nodes communicate with each other in the background over a separate HA network to continually replicate data to the passive node and the witness provides quorum in case of split-brain scenarios (network connection loss). If something happens to the active node, the passive will automatically switch and pick up the slack.

What do we need for vCenter Server HA? A few things.

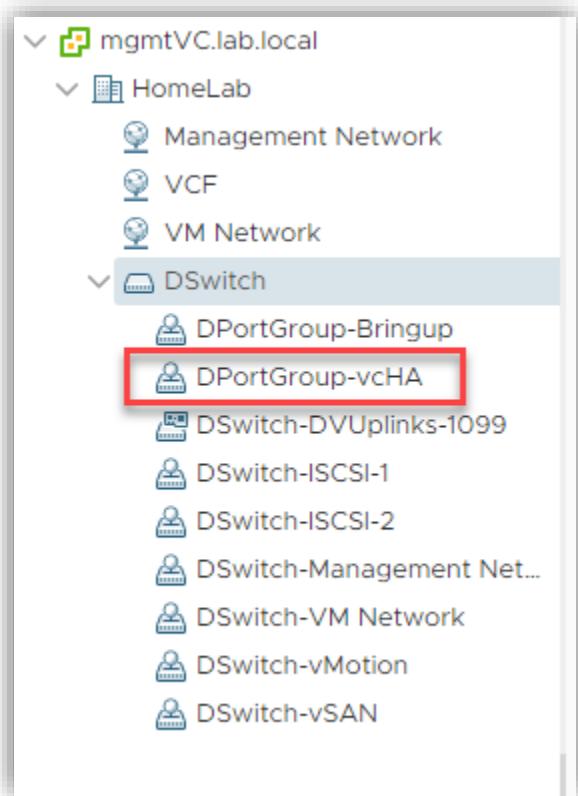
- SSH needs to be enabled
- Network latency must be less than 10ms for all the nodes
- HA network must be on a separate subnet than management
- HA requires a standard vCenter Server license
- While not required, a minimum of 3 hosts is recommended. (There are affinity rules created and if you try to do this all on a single host, it won't work)
- ESXi 6.0 and vCenter 6.5 minimum

If you use the automatic configuration you will

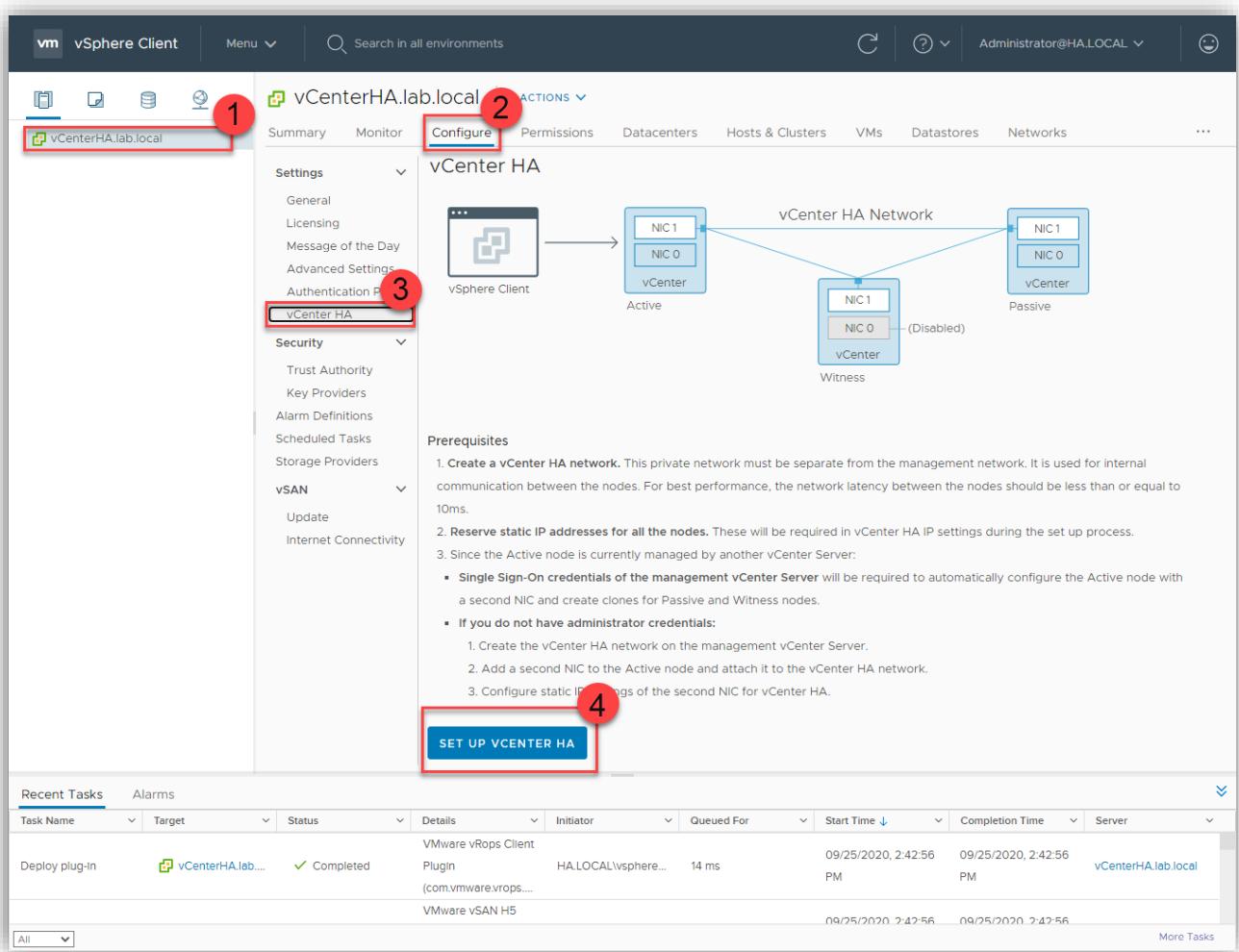
1. Add a port group or network on each ESXi host for HA traffic
2. Start the HA configuration and specify IP address, hosts used, and datastores
3. The installer will perform the rest of the steps (creating 2 more nodes, setup the network and exchange heartbeats)

What does this look like? I thought you'd never ask...

Setting up the network



Getting to the configuration page for vCenter Server HA



This next step is where you need to enter in information on the resources and networking

Select vCenter HA network for Active node

DPortGroup-vcHA

BROWSE ...

Automatically create clones for Passive and Witness nodes

Active node (vCenterHA_1)

Location

-  mgmtVC.lab.local
-  HomeLab
-  LAB
-  r730.lab.local

Networks

-  DPortGroup-Bringup Management (NIC 0)
-  DPortGroup-vcHA vCenter HA (NIC 1)

Storage

-  VirtualSynology

Passive node (vCenterHA_1-Passive)

EDIT

Location

-  mgmtVC.lab.local
-  (not selected)
-  (not selected)

Networks

-  (not selected) Management (NIC 0)
-  (not selected) vCenter HA (NIC 1)

Storage

-  (not selected)

Witness node (vCenterHA_1-Witness)

EDIT

Location

-  mgmtVC.lab.local
-  (not selected)
-  (not selected)

Networks

-  (not selected) vCenter HA (NIC 1)

The last step here is to put in the network configuration.

3. IP settings

IP version ▾

Active Node

vCenter HA Network	DPortGroup-vcHA
IPv4 Address (NIC 1)	<input type="text"/>
Subnet mask or prefix length	<input type="text"/>
Default Gateway	<input type="text"/> optional

Passive Node

vCenter HA Network	DPortGroup-vcHA
IPv4 Address (NIC 1)	<input type="text"/>
Subnet mask or prefix length	<input type="text"/>
Default Gateway	<input type="text"/> optional

[EDIT MANAGEMENT NETWORK SETTINGS](#)

Witness Node

vCenter HA Network	DPortGroup-vcHA
IPv4 Address (NIC 1)	<input type="text"/>
Subnet mask or prefix length	<input type="text"/>
Default Gateway	<input type="text"/> optional

FINISH

After completed, click Finish. The installer will now begin its work. When complete, the config page will look something like this.

The screenshot shows the vCenter HA configuration page. At the top, it displays "vCenter HA" with "Mode: Enabled, State: Healthy". Below this are three buttons: "EDIT", "INITIATE FAILOVER", and "REMOVE VCENTER HA".

The main section is titled "Cluster Nodes" and contains a table:

Node	Status	vCenter HA IP address (NIC 1)	Management IP address (NIC 0)
Active	Up	172.16.1.10	192.168.3.10
Passive	Up	172.16.1.11	192.168.3.10
Witness	Up	172.16.1.12	

Below the table is a section titled "Active Node Settings" with tabs for "IP Settings" and "VM Settings". The "IP Settings" tab is selected, showing the following details:

- vCenter HA Network (NIC 1)**
 - IPv4 address: 172.16.1.10
 - Subnet mask: 255.255.255.0
- Management Network (NIC 0)**
 - IPv4 address: 192.168.3.10
 - Subnet mask: 255.255.0.0
 - IP gateway: 192.168.1.1

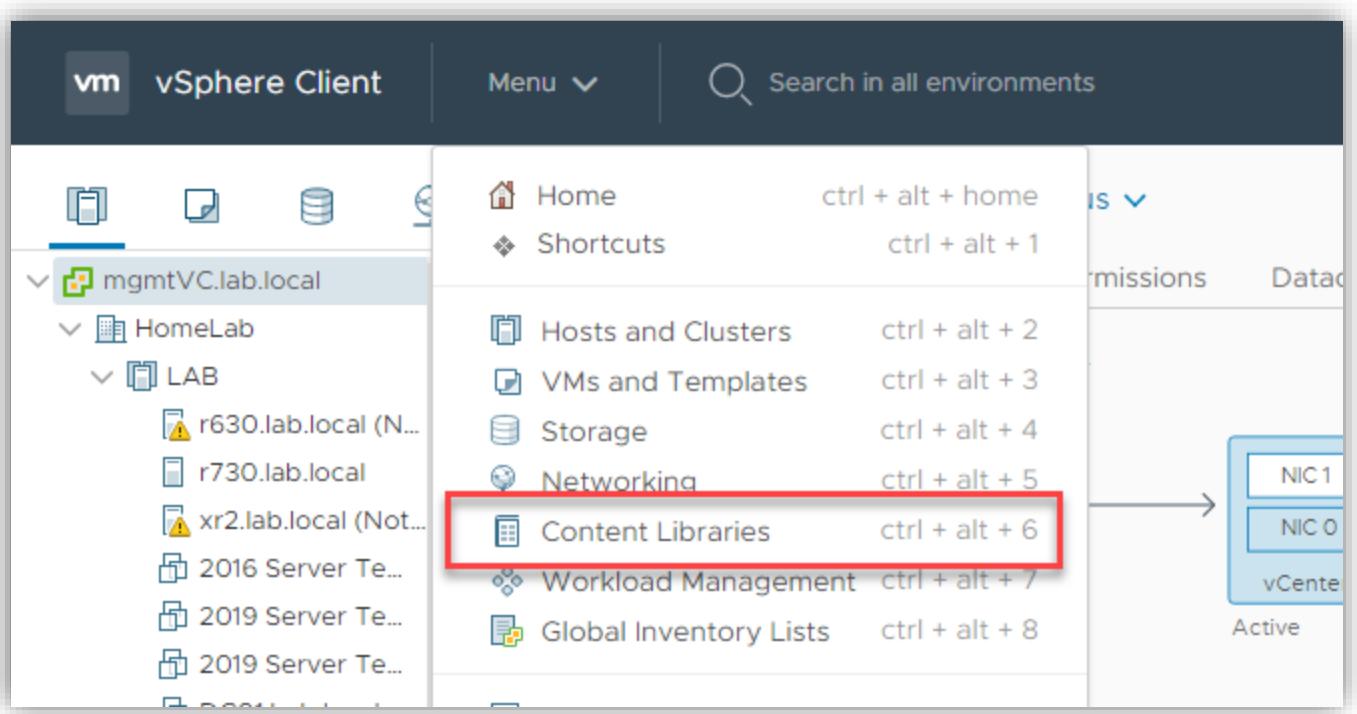
Objective 4.7 – Set up a content library

Content Libraries are containers for VMs, templates, and other types of files used for the vSphere infrastructure, such as ISOs. You can distribute this content to other vCenters if allowed. There are two types of content libraries you can create:

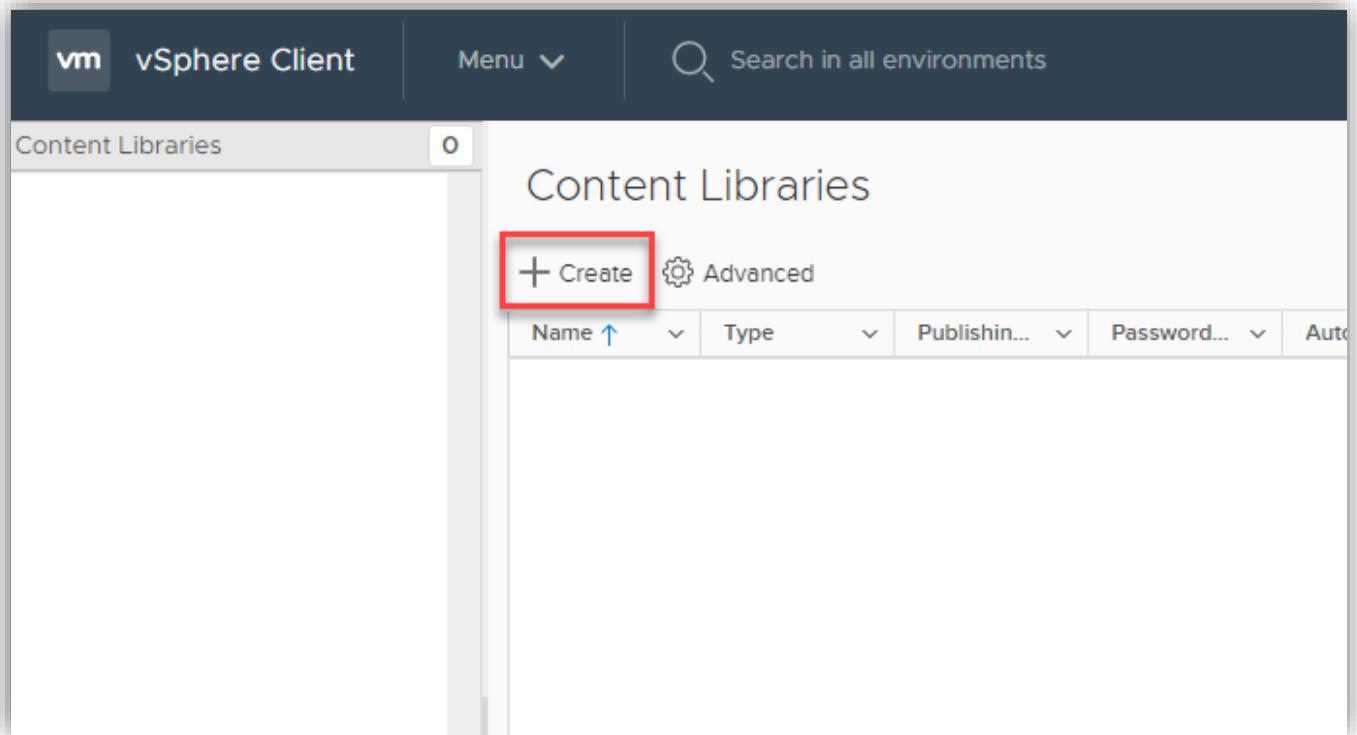
- Local Content Library – This is managed on the local vCenter Server. You can enable publishing however, which allows you to share this library with other vCenter Servers.
- Subscribed Content Library (or remote). This enables you to use another content library's files. You can't upload or import or modify, but you can pull them down and use them.

Before we dive into how to set up a Content Library, I did want to point out a major feature of vSphere 7 Content Libraries. And that is the ability to check out and save a history of all changes made to a template. This is awesome and allows you even revert if needed. Version control. Yes, ok back to set up.

Click Menu at the top bar and then click on Content Libraries



Click on Create



Type in a name and any notes you want to include. You also need to choose which vCenter to host it. Then click next.

New Content Library

1 Name and location

2 Configure content library

3 Add storage

4 Ready to complete

Name and location

Specify content library name and location.

Name:

VCP 2020 Content Library

Notes:

This is a test CL for my study guide|

vCenter Server:

mgmtVC.lab.local ▾

CANCEL

BACK

NEXT

Select if this content library will be local or subscribed. You also need to decide if local, do you want to allow publishing.

New Content Library

✓ 1 Name and location

2 Configure content library

3 Add storage

4 Ready to complete

Configure content library

Local libraries can be published externally and optimized for syncing over HTTP. Subscribed libraries originate from other published libraries.

Local content library

Enable publishing

Enable authentication

Subscribed content library

Subscription URL: Example: https://server/path/lib.json

Enable authentication

Download content immediately when needed

CANCEL

BACK

NEXT

The next step is deciding where the files will be held. Specifically, which datastore you will use. (I don't have all mine currently running, hence the red)

New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library

3 Add storage

4 Ready to complete

Add storage

Select a storage location for the library contents.

Name ↑	Status	Type	Datastore... ▾
Datastore	✓ Normal	VMFS 6	
R730_Local_DS2	✓ Normal	VMFS 6	
R730_Local_SSD_DS1	✓ Normal	VMFS 6	
VirtualSynology (Inaccessible)	✓ Normal	VMFS 6	
vsanDatastore	✓ Normal	vSAN	
XR2_Local_NVMe_SSD (Inacces...)	✓ Normal	VMFS 6	

6 items

CANCEL

BACK

NEXT

At this point, you are done. Look over the parameters and if they look correct, click finish.

New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library
- ✓ 3 Add storage

Ready to complete
Review content library settings.

4 Ready to complete

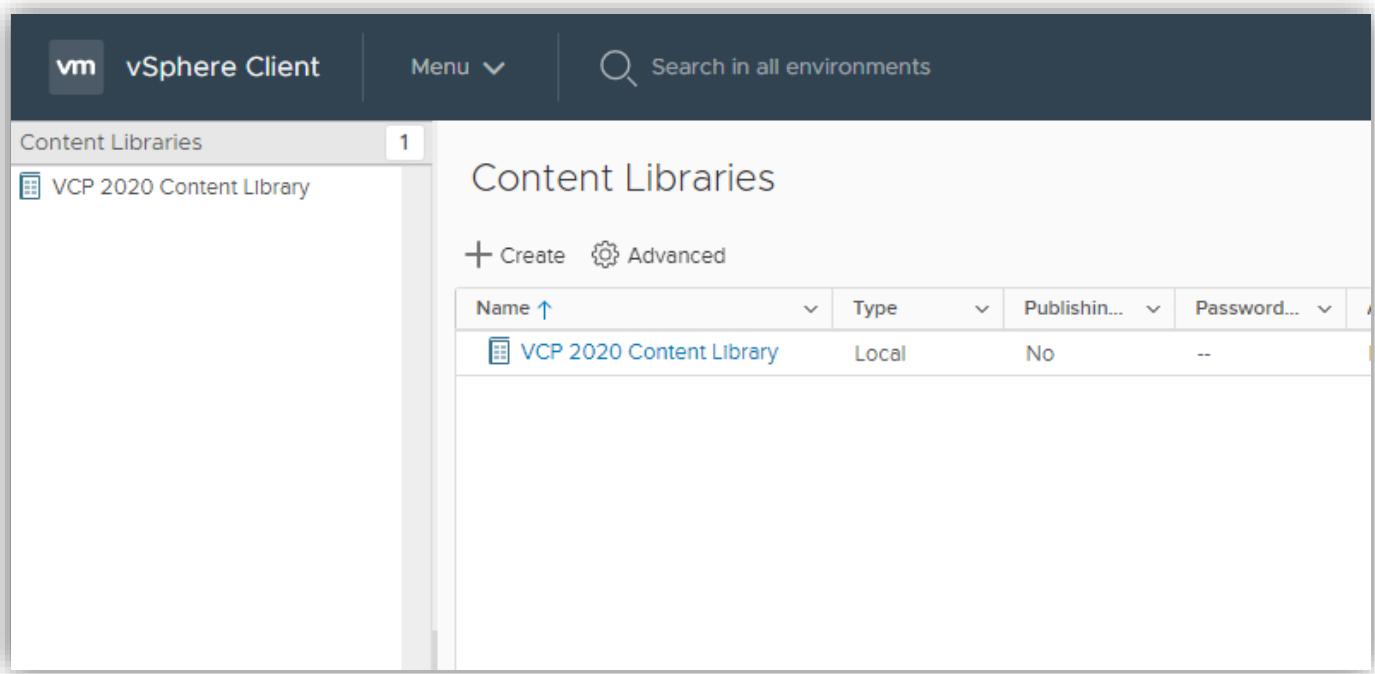
Name:	VCP 2020 Content Library
Notes:	This is a test CL for my study guide.
vCenter Server:	mgmtVC.lab.local
Type:	Local Content Library
Publishing:	Disabled
Storage:	Datastore

CANCEL

BACK

FINISH

You can now start adding templates and ISOs to your content library!



Objective 4.8 – Configure vCenter Server file-based backup

vCenter Servers are important data that should have backups. Fortunately, VMware has given us a utility to take backups of its important data. VMware supports FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB files share to store the backup. Keep in mind that in order to restore this data, you would have to use either the CLI or GUI install tool to install a new appliance. The second stage of the install is where it would take your information and restore it to the new appliance. Now let's show how to configure it.

The first step is logging into the vCenter Server administration web UI. This is at [https://\[vCenter Server FQDN or IP address\]:5480](https://[vCenter Server FQDN or IP address]:5480).

vCenter Server Management Sun 09-20-2020 02:12 AM UTC English ▾ Help ▾ Actions ▾ root ▾

Summary

Hostname: mgmtVC.lab.local
Type: vCenter Server with an embedded Platform Services Controller
Product: VMware vCenter Server Appliance
Version: 7.0.0.10700
Build number: 16749653

Health Status

Overall Health	Good (Last checked Sep 19, 2020, 09:12:15 PM)
CPU	Good
Memory	Good
Database	Good
Storage	Good
Swap	Good

Single Sign-On

Domain	vsphere.local
Status	Running

Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup

Click Backup on the left pane.

Administration	Storage	Good
Syslog	Swap	Good
Backup		

Click on Configure.

VM vCenter Server Management Sun 09-20-2020 02:14 AM UTC English Help Actions root

Summary
Monitor
Access
Networking
Firewall
Time
Services
Update
Administration
Syslog
Backup

Before taking a backup, a backup server must be set up and configured such that the vCenter server has access to it. The protocols supported for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB and HTTP.

Backup Schedule

Status Not configured **CONFIGURE**

Activity **BACKUP NOW**

Backup Location	Type	Status	Data Transferred	Duration	End Time
No items to display					

This allows us to create a schedule for our backups. If we only wanted to perform a single backup, we could just click on Backup Now. If we setup a schedule, we can perform a one-off backup using that configuration however. Put in the configuration you wish to use. You can also tell it how many backups to retain, as some of these can get quite large. I am going to say 5 backups. It lists the size there at the end.

Create Backup Schedule

Backup location (i)	smb://192.168.1.22/main_share/vcenter_backup		
Backup server credentials	User name	admin	
	Password	*****	
Schedule (i)	Daily	11 : 59 P.M.	Etc/UTC
Encrypt backup (optional)	Encryption Password		
	Confirm Password		
DB Health Check (i)	<input checked="" type="checkbox"/> Disable		
Number of backups to retain	<input type="radio"/> Retain all backups <input checked="" type="radio"/> Retain last <input type="text" value="5"/> backups		
Data	<input checked="" type="checkbox"/> Stats, Events, and Tasks	50 MB	
	<input checked="" type="checkbox"/> Inventory and configuration	283 MB	
	Total size (compressed)	333 MB	
CANCEL CREATE			

When you click create it creates that schedule. It won't automatically create a backup immediately. If you want to test it, click Backup Now and select at the top, Use backup location and username from backup schedule. When you click start it will attempt to take the backup. You do not have to have the folder created if using a user that has create rights. Once done, it will look like this.

The screenshot shows the vCenter Server Management interface. On the left, a sidebar lists various management categories: Summary, Monitor, Access, Networking, Firewall, Time, Services, Update, Administration, Syslog, and Backup. The 'Backup' category is currently selected and highlighted in blue. The main content area is divided into two sections: 'Backup Schedule' and 'Activity'. The 'Backup Schedule' section contains a table with one row, showing a backup task that has completed successfully. The 'Activity' section contains a table with four rows, providing detailed information about the backup task, including its location, type, status, transferred data, duration, and end time. A prominent 'BACKUP NOW' button is located at the top of the 'Activity' section.

Backup Location	Type	Status	Data Transferred	Duration	End Time
smb://192.168.1.22/main_sh...	Manual	Complete	1.01 GB	00:02:28	Sep 19, 2020, 09:22:04 PM

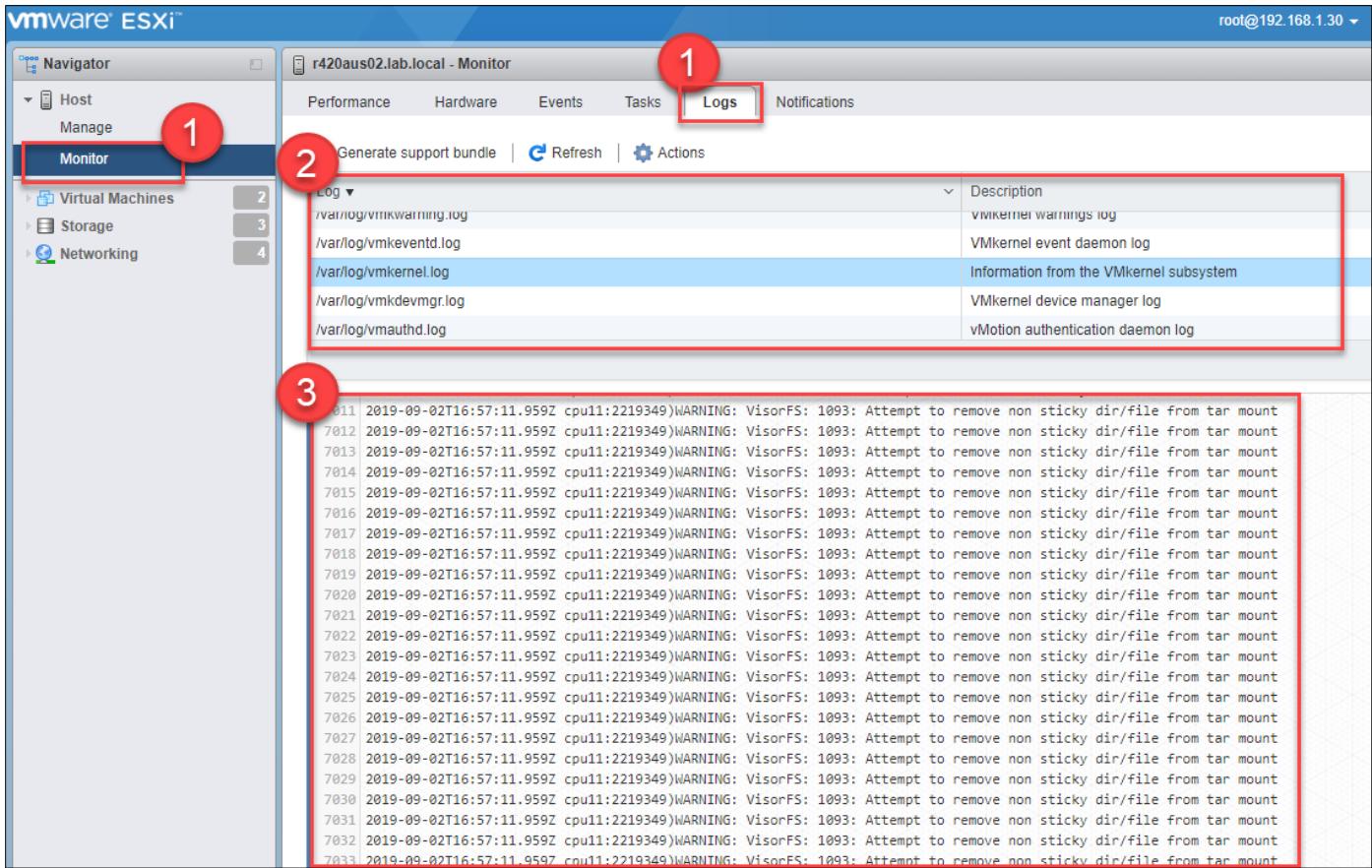
Backup Location	Version
smb://192.168.1.22/main_share/vcenter_backup/vCenter/sn_mgmtVC.lab.local/M_7.0.0.10700_20200920-021937_JJSWO2LONZUW4ZY=	VC-7.0.0 ⓘ
Backup server user name	admin
Start Time	Sep 19, 2020, 09:19:37 PM

Objective 4.9 – Analyze basic log output from vSphere products

VMware has come a long way from when I started troubleshooting their products. Their logs have gotten easier to get to and improved in their quality. What I will do here is give you a quick overview of where to find the logs and how to read them.

ESXi Logs

Before, the most straightforward option was to open an SSH session to the host and look at the logs; you can easily do that from within the host UI now. If you go to Monitor, you can see a list of all the logs available to peruse.



Here in the screenshot, you can see

1. Monitor menu and the tab for logs
2. Logs available
3. Log output

Here is a list of logs on the ESXi host and a description of what the log does.

Log ▾	Description
/var/log/vpxa.log	vCenter agent log
/var/log/vobd.log	VMware observer daemon log
/var/log/vmkwarning.log	VMkernel warnings log
/var/log/vmkeventd.log	VMkernel event daemon log
/var/log/vmkernel.log	Information from the VMkernel subsystem
/var/log/vmkdevmgr.log	VMkernel device manager log
/var/log/vmauthd.log	vMotion authentication daemon log
/var/log/syslog.log	General system log
/var/log/sysboot.log	System boot log
/var/log/shell.log	ESXi shell activity log
/var/log/hostd.log	Host agent log
/var/log/fdm.log	Fault tolerance management agent log
/var/log/esxupdate.log	ESX update log file
/var/log/dhclient.log	DHCP client log
/var/log/auth.log	Authentication subsystem log

You can still access these logs through the DCUI or an SSH session as well.

All right, so you have the log now... How do you use it? Here is a sample taken from a VMKernel.log. This sample was after shutting down a switch port using a Software iSCSI controller to a SAN LUN.

```
2013-12-05T21:42:47.944Z cpu25:8753)<3>bnx2x 0000:04:00.0: vmnic4: NIC Link is Down
```

```
2013-12-05T21:43:12.090Z cpu16:8885)WARNING: iscsi_vmk: iscsivmk_StopConnection: vmhba45:CH:0 T:0 CN:0: iSCSI connection is being marked "OFFLINE" (Event:4)
```

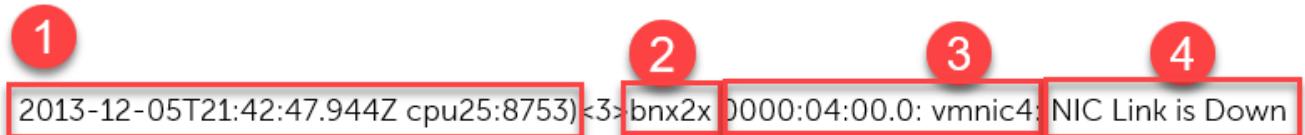
```
2013-12-05T21:43:12.090Z cpu16:8885)WARNING: iscsi_vmk: iscsivmk_StopConnection: Sess [SID: 00023d000001 TARGET: iqn.2001-05.com.equallogic:0-8a0906-0f6407f09-1173c8a93ab4f0f6-aim-2tb-1 TPGT: 1 TSIH: 0]
```

```
2013-12-05T21:43:12.090Z cpu16:8885)WARNING: iscsi_vmk: iscsivmk_StopConnection: Conn [CID: 0 L: 192.168.3.123:61632 R: 192.168.3.3:3260]
```

```
2013-12-05T21:43:22.093Z cpu31:8261)StorageApdHandler: 248: APD Timer started for ident [naa.6090a098f007640ff6f0b43aa9c87311]
```

2013-12-05T21:43:22.093Z cpu31:8261)StorageApdHandler: 395: Device or filesystem with identifier [naa.6090a098f007640ff6f0b43aa9c87311] has entered the All Paths Down state.

Lets decipher this a bit more.



1. This part is the timestamp of the log entry.
2. This is what the reporter is. In this case, it is the bnx2x driver
3. This is what it is reporting on, specifically vmnic4 at the hardware address referenced 0000:04:00:0
4. This is data about what it saw. Namely, the NIC link went down.

Some entries are a bit more challenging to read than others, but the structure stays pretty close. You can also use something like Log Insight to help search through the logs and decipher them.

vCenter Server Logs

We have logs we may need to retrieve for vCenter Server as well. Unfortunately, it doesn't have a browser like the hosts. (Hint Hint VMware) Here is where you can get to them, in any case.

The screenshot shows the vCenter Server Management interface. The left sidebar has tabs for Summary, Monitor, Access, and Networking. The main area displays server details: Hostname: vcenter-mgmt.vcf.sddc.lab, Type: vCenter Server with an embedded database, Product: VMware vCenter Server Appliance, Version: 7.0.0.10600, and Build number: 16620007. A context menu is open over the server icon, with the 'Actions' option highlighted. The menu includes options: Reboot, Shutdown, Create Support Bundle (which is highlighted with a red box), and Switch Theme.

This picture shows accessing the Appliance Config at port 5480.

Once this is done downloading, you have a decent size .tar file. You have to unzip this a couple of times. When you finally have a typical directory structure, all the logs are under the /var/log/vmware folder. Here is a list of the files and locations and what they do.

Windows vCenter Server	vCenter Server Appliance	Description
vmware-vpx\vpxd.log	vpxd/vpxd.log	The main vCenter Server log
vmware-vpx\vpxd-profiler.log	vpxd/vpxd-profiler.log	Profile metrics for operations performed in vCenter Server
vmware-vpx\vpxd-alert.log	vpxd/vpxd-alert.log	Non-fatal information logged about the vpdx process
perfcharts\stats.log	perfcharts/stats.log	VMware Performance Charts
eam\eam.log	eam/eam.log	VMware ESX Agent Manager
invsvc	invsvc	VMware Inventory Service
netdump	netdumper	VMware vSphere ESXi Dump Collector
vapi	vapi	VMware vAPI Endpoint
vmdird	vmdird	VMware Directory Service daemon
vmsyslogcollector	syslog	vSphere Syslog Collector
vmware-sps\sps.log	vmware-sps/sps.log	VMware vSphere Profile-Driven Storage Service
vpostgres	vpostgres	vFabric Postgres database service
vsphere-client	vsphere-client	VMware vSphere Web Client
vws	vws	VMware System and Hardware Health Manager
workflow	workflow	VMware vCenter Workflow Manager
SSO	SSO	VMware Single Sign-On

It would be simpler again to use a program like Log Insight to help you parse through the logs. And you wouldn't need to download them as they are streamed directly to Log Insight. You'll see output similar to what I mentioned above.

Objective 4.10 – Configure vSphere Trust Authority

We've covered VMware attestation and the security piece of this earlier. The Trust Authority is enabled on a dedicated vCenter Server cluster (known as the vSphere Trust Authority Cluster) in order to attest VMware ESXi hosts are secure. There are Pre-Reqs required ([here](#)) before you can set up the Trust Authority. There are a number of tasks (10 in fact), each with their own respective steps that need to be accomplished to make this work. Those tasks are as follows

1. On a system that has access to your Trust Authority environment (for example, a jumpbox)
 - a. Install PowerCLI 12.0.0
 - b. Make sure MS .NET 4.8 or greater is installed
 - c. Create a local folder to save the information that will be exported as files
2. Add the Trust Authority administrator to the TrustedAdmins group on the vCenter Server of the Trust Authority Cluster – This is done by navigating to Menu > Administration > Users and Groups and then click on the ellipsis in front of Trusted Admins and then add the user to that group.

The screenshot shows the vSphere Client interface. The left sidebar has a tree view with 'Administration' selected, which is highlighted with a red box. Under 'Administration', 'Users and Groups' is also highlighted with a red box. The main pane shows a table titled 'Users and Groups' with the 'Groups' tab selected. The table has columns for 'Group Name' and 'Description'. A new row is being added, indicated by an 'ADD GROUP' button and a table row with a single cell containing 'TrustedAdmins'. To the right of this cell is a red box with three dots (...), indicating where to click to add the user to the group.

Group Name	Description
DCAdmins	
LicenseService.Administrators	License Service Administrators
ActAsUsers	Act-As Users
NsxAuditors	SSO group to view NSX configuration.
CAAdmins	
SolutionUsers	Well-known solution users' group, which contains all solution users as members.
SyncUsers	Sync Users
NsxAdministrators	SSO group to view and modify NSX configuration.
WorkloadStorage	Workload Storage
TrustedAdmins	Administrators who manage the trusted hosts

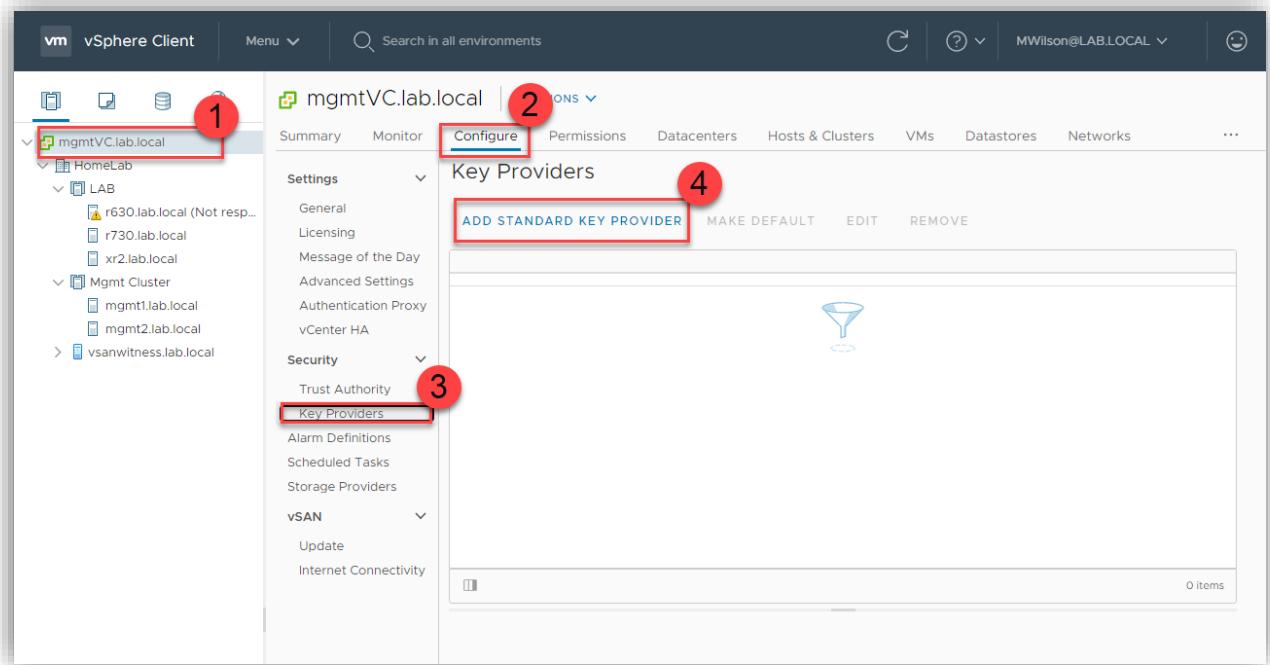
3. Perform the same action (add the same user) to the TrustedAdmins to the cluster you will be trusting.
4. Enable the Trust Authority State – To do this you will need to run a command at the CLI on your jumpbox. First you will need to connect to the Trust Authority cluster. Check status of it by running:

```
Get-TrustAuthorityCluster
```

Then to enable it run the following command (change 'vTA cluster' to the name of your authority cluster)

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -  
State Enabled
```

5. You will now need to compile information on the ESXi hosts you are going to trust (background check HA!) You need to run a number of PowerCLI commands to get this information and export it to a file. You can look [here](#) for guidance.
6. Once you have this information, you need to import it into the Trust Authority Cluster (check [here](#) for how)
7. Now you need to create the Trusted Key Provider from the Trust Authority Cluster. You can see how [here](#).
8. You then need to export information about the Trust Authority to the trusted cluster. Proving it is an authority that can be trusted. Again this is done via PowerCLI and can be found [here](#).
9. This information needs to be imported into the trusted cluster now. How can be found [here](#).
10. Last you need to configure the Trusted Key Provider to the Trusted Hosts. This can be done either by command line or by HTML client. You can do that here.



11. You can find all these steps and explanations in VMware's documentation [here](#).

Objective 4.11 – Configure vSphere certificates

In 5.x and even in 6.x days configuring certificates wasn't very easy. Matter of fact it was downright painful in some cases. In vSphere 7 there have been improvements made to try to make this simpler for admins. To be clear, the VMware Certificate Management (VMCA) is not a full-fledged PKI solution, so you can't request certs for other purposes. For your VMware environment it is just enough.

There are a number of ways for you to manage your vCenter Server certificates. You can use

- vSphere HTML5 client – This allow for command tasks to be performed within the client
- vSphere Automation API –
- Certificate Manager utility – uses command line tools on the vCenter Server to perform certificate tasks
- Certificate management CLIs – uses the dir-cli, certool, and vecs-cli tools to perform tasks

- Sso-config utility – perform STS (Security Token Service) certificate management from the vCenter Server command line.

There are 4 modes you can run certificates through vCenter Server.

In the first mode, Fully Managed Mode, the vCenter Server generates a root certificate at first install and uses that to manage intra-cluster certificates as well as the certificate we use when we log on, the machine certificate. You can regenerate that root cert using your own company information if desired.

In Hybrid Mode, you replace the machine certificate that the vSphere client uses so that it can be accepted without intervention by default browsers. Something like a GoDaddy certificate for example. The VMCA still manages internal certificates making this simple and easy.

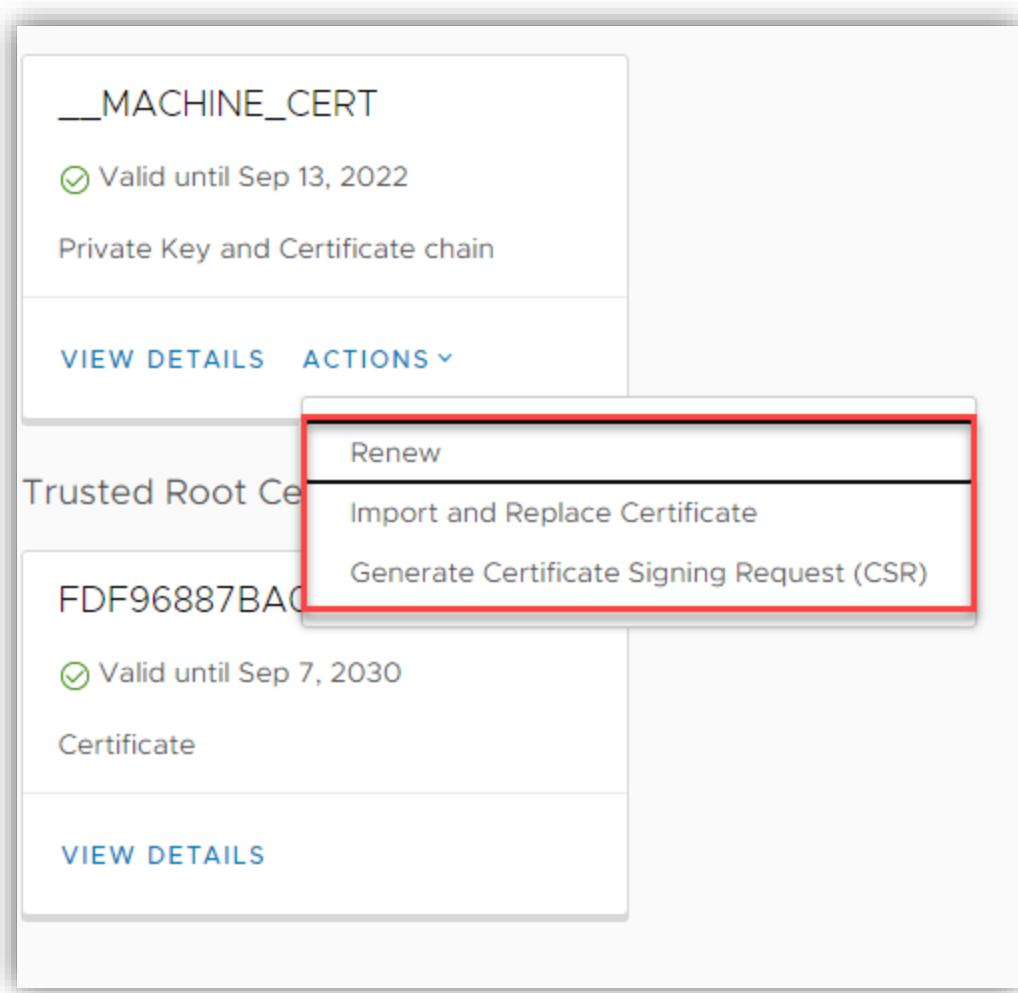
In subordinate mode, the VMCA will act as a subordinate CA. The vCenter Server still generates certificates but it generates them as part of the larger organization's.

The last mode is Full Custom. In this mode, the VMCA isn't used at all, and all certs must be installed and managed by a person.

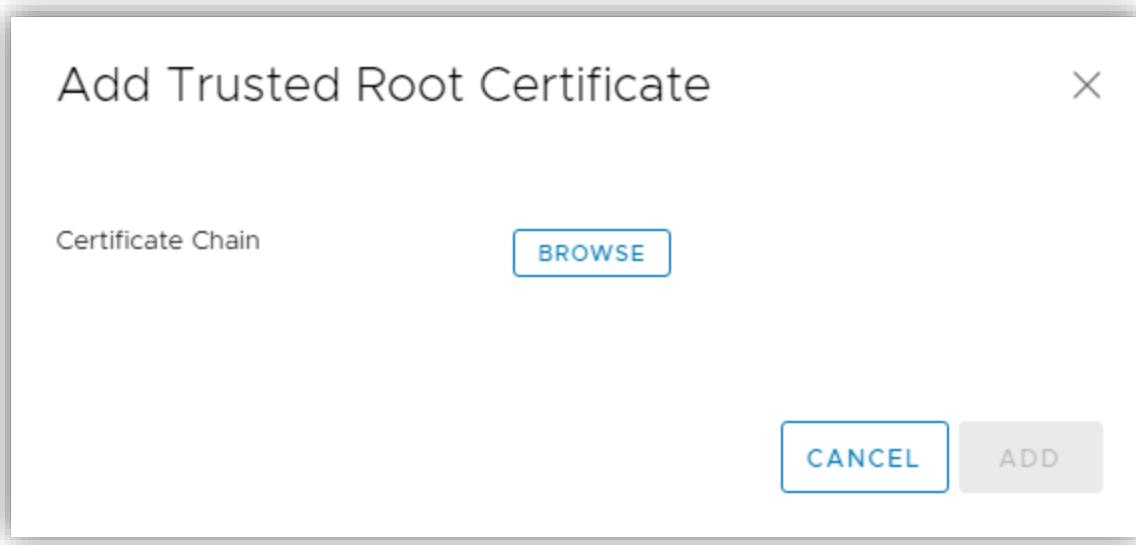
To work with the certificates, you can go through the HTML5 client by going to Menu > Administration > Certificate Management. This is what that screen looks like.

The screenshot shows the vSphere Client HTML5 interface. The left sidebar has a dark blue header with 'vm' and 'vSphere Client'. Below it is a navigation menu with sections like 'Administration', 'Access Control', 'Licensing', 'Solutions', 'Deployment', 'Support', 'Single Sign On', and 'Certificates'. Under 'Certificates', 'Certificate Management' is selected and highlighted in blue. The main content area has a dark header with a search bar 'Search in all environments'. Below the header, there are two main sections: 'Machine SSL Certificate' and 'Trusted Root Certificates'. The 'Machine SSL Certificate' section shows a certificate named '__MACHINE_CERT' that is valid until Sep 13, 2022. It also includes a link to 'Private Key and Certificate chain'. Below this is a 'VIEW DETAILS' and 'ACTIONS' button. The 'Trusted Root Certificates' section shows a certificate for FDF96887BA0CF95... that is valid until Sep 7, 2030. It includes a link to 'Certificate' and a 'VIEW DETAILS' button. The top right corner shows the user 'MWilson@LAB.LOCAL' and a connection status icon.

To work with it, you can choose the Actions menu



Using the machine cert menu, you can renew, change, or generate a new one to replace an expired certificate. Under Trusted Root Certificates, you can select Add to import a certificate chain.



If you want to run the Certificate Manager Utility, the location is as follows.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

When you run that, it will present you options to choose from. You follow the options to complete the workflow.

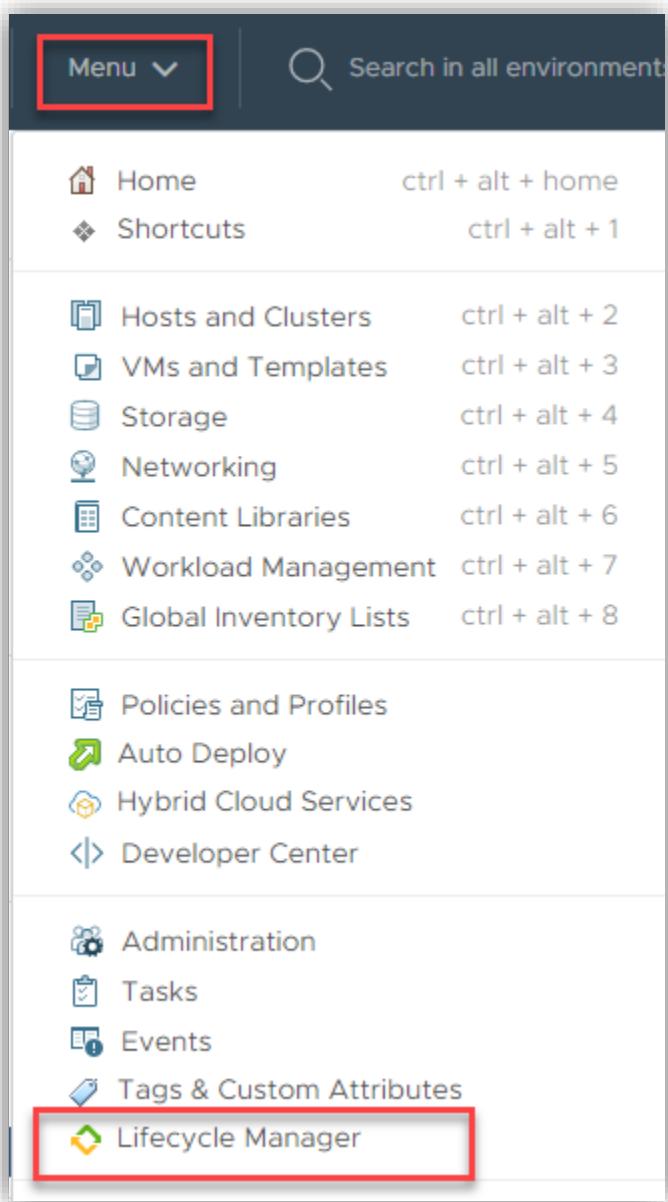
Objective 4.11.1 – Describe Enterprise PKI's role for SSL certificates

In vSphere, certificates are used for, encryption of communication, authentication of vSphere services, and internal actions such as signing tokens. The internal VMware Certificate Authority can supply all the certificates needed for VMware services, but a company might institute a PKI or Public Key Infrastructure. A PKI can include, hardware, software, policies, processes, and procedures to manage certificates and their lifecycle and public keys.

A smaller business might decide to not use a full infrastructure, but should still have some sort of policies and procedures around how certificates are dealt with. VMware can work within a PKI to create certificates for an organization. It is suggested the best way to accomplish most business' tasks would be to setup a Hybrid Mode VMware vCenter Server. This setup allows you to replace the machine certificate, or the one used to login to VMware vCenter Server and allows the VMCA to manage all the other certificates with its own self-signed certificates. VMware created a blog with some suggestions on how to implement certificates [here](#).

Objective 4.12 – Configure vSphere Lifecycle Manager/VMware Update Manager (VUM)

In vSphere 7 Lifecycle Manager is a service that enables updating and upgrades for ESXi hosts. To setup Lifecycle Manager Click on Menu > Lifecycle Manager



There are a number of things you can do from there. Image Depot allows you to setup a base image for clusters and even add vendor drivers or installation bundles. The Updates tab allows you to remove updates from baselines. Imported ISOs allows you to import a ESXi ISO image to use for an update baseline. Baselines is one or more patch, extensions, or updates that you want to apply to your vSphere infrastructure. Settings allows you to configure LCM.

vSphere Client | Menu ▾ | Search in all environments | C | ? | MWilson@LAB.LOCAL | ☺

Home
Shortcuts

Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Workload Management
Global Inventory Lists

Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center

Administration
Tasks
Events
Tags & Custom Attributes

Lifecycle Manager

Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Workload Management
Global Inventory Lists

Lifecycle Manager | ACTIONS ▾

Image Depot Updates Imported ISOs Baselines Settings

ESXI VERSIONS VENDOR ADDONS COMPONENTS

Last Sync: 57 minutes ago. Next Sync: in 23 hours

ESXI Versions

Name	Version	Release Date	Category
ESXi	7.0b - 16324942	06/15/2020	Enhancement
ESXi	7.0bs - 16321839	06/15/2020	Enhancement
ESXi	7.0 GA - 15843807	03/16/2020	Enhancement

Vendor Addons

Name	Version	Release Date	Category
DellEMC addon for PowerEdge Servers running ESXi 7.0	A02	06/22/2020	Enhancement
DellEMC addon for PowerEdge Servers running ESXi 7.0	A00	04/01/2020	Bug Fix
HPE Customization for HPE Synergy Servers	700.0.0.10.5.6-19	08/01/2020	Enhancement
HPE Customization for HPE Servers	700.0.0.10.5.5-46	06/16/2020	Enhancement
htc-custom-addon	7.0.0.11-03	07/21/2020	Enhancement
FJT-Addon-for-FujitsuCustomImage	7.0.0-500.1.0	05/14/2020	Enhancement
Lenovo Customization Addon for Lenovo System x and ThinkSystem	LVO.700.10.1	07/20/2020	Bug Fix
NEC-addon-GEN	7.0.0-01	06/28/2020	Enhancement
NEC-addon	7.0.0-01	06/29/2020	Enhancement

The screenshot shows the Lifecycle Manager interface with the 'Settings' tab selected. On the left, there's a navigation tree with 'Administration' expanded, showing 'Patch Downloads' (which is selected) and 'Patch Setup'. Under 'Host Remediation', there are 'Images', 'Baselines', and 'VMs'. The main panel displays 'Automatic Download Settings' with the following configuration:

Automatic Download Settings	
Automatic downloads	Enabled
Automatic download task name	VMware vSphere Lifecycle Manager Update Download
Automatic download task description	A predefined scheduled task to download software updates.
Send email to	

An 'EDIT' button is located in the top right corner of the settings panel.

- Administration Settings
 - Patch Downloads concerns itself with getting your updates.
 - Patch Setup concerns itself with where it is getting them from. Do you need a proxy?
- Remediation Settings
 - Images – When you applying images, how do you want vSphere to handle VMs and migration of them
 - Baselines – Same thing with Baselines
 - VMs – If you are remediating VMs do you want to take a snapshot automatically and how long do you want to keep them.

Once you have baselines and everything how you want them, you can apply them to hosts at an individual level or at a cluster level. Checking compliance will check the host against the baseline. If the host doesn't have the updates on it, it will show out of compliance. You can then choose to stage, to download the updates to the host and then reboot at your leisure, or you can remediate the host immediately. If there is a new baseline, you can attach it to check compliance.

The screenshot shows the vSphere Client interface for managing a cluster named 'LAB'. The left sidebar lists various clusters and hosts under 'mgmtVC.lab.local' and 'HomeLab'. The main pane displays 'Baselines' information for the 'LAB' cluster. It shows '3 Host(s)' running 'ESXi version 6.7.0'. In the 'Hosts' section, it indicates that '3 of 3 Hosts are unknown' regarding their compliance status. A 'CHECK COMPLIANCE' button is highlighted with a red box. Below this, a section titled 'Ready to remediate' includes a 'Remediation Pre-check' link. At the bottom, there's a table for 'Attached Baselines' with columns for Status, Content, Type, ESXi version, and Last Modified. The table shows two entries: 'Host Security Patches (Predefined)' and 'Critical Host Patches (Predefined)'. The table header has four buttons: 'ATTACH', 'DETACH', 'STAGE', and 'REMEDIATE', which are also highlighted with a red box.

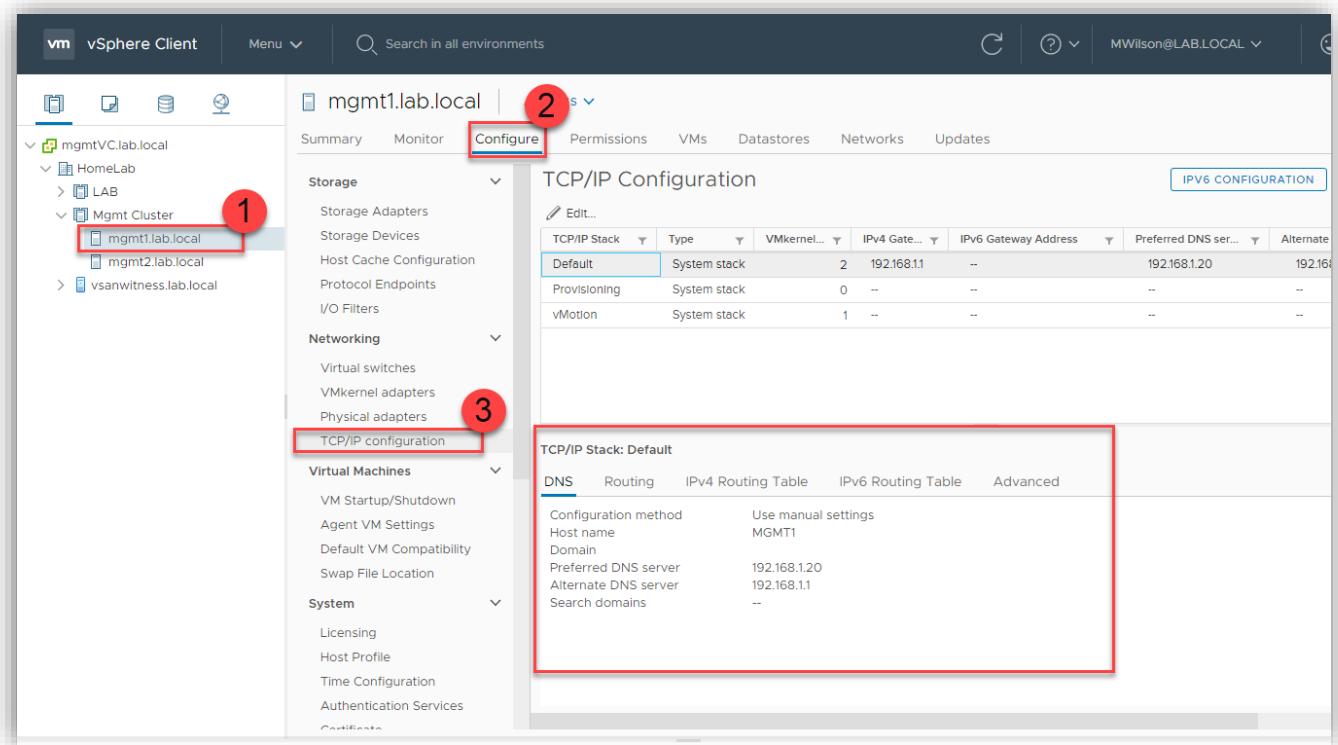
Objective 4.13 – Securely Boot ESXi hosts

With the advent of UEFI firmware, Secure Boot is a feature that will refuse to load any driver or app unless it is cryptographically signed. You might be more familiar with operating systems such as Windows 10 or Ubuntu using this to prevent unwanted modification to the boot drive. Starting with vSphere 6.5 VMware has been able to use this as well. The host needs to be compatible and you can run validation script to check. Once enabled, you must use an ESXi bootloader that contains VMware's public key. Trying to upgrade a system using esxcli commands with Secure Boot enabled will fail to update the bootloader and won't work.

If a physical host has a TPM included, you can use host attestation to authenticate and securely boot the host as well.

Objective 4.14 – Configure different network stacks

TCP/IP stacks allow you to change DNS and gateway configuration for a specific traffic. You can also change congestion control, the number of connections allowed, and even the name of the stack. To do this, click on the host, and then click Configure > Networking > and TCP/IP configuration. You can see current settings below.



To change them, click on the one you want to change and then edit. The first screen allows you to either obtain settings from an existing VMkernel or manual

Default - Edit TCP/IP Stack Configuration

DNS configuration

Routing

Obtain settings automatically from a VMkernel network adapter

Name

VMkernel network adapter



Advanced

Enter settings manually

Host name

MGMT1

Domain

Preferred DNS server

192.168.1.20

Alternate DNS server

192.168.1.1

Search domains

CANCEL

OK

The next screen allows you to set a IPv4 or 6 gateway for routing. It mentions if you change this, you might lose connectivity between the host and vCenter.

Default - Edit TCP/IP Stack Configuration

DNS configuration

Routing

VMkernel gateway

192.168.1.1

Name

Advanced

⚠ Changing the default gateway might cause loss of connectivity between the host and vCenter Server.

IPv6 VMkernel gateway

⚠ One or more VMkernel ports are using IPv6 addresses but an IPv6 gateway has not been specified.

CANCEL

OK

The next screen allows you to name the stack.

Default - Edit TCP/IP Stack Configuration

DNS configuration

Routing

Name

Default

Name

Advanced

CANCEL

OK

And the last screen allows you to set connection limit and congestion algorithm type.

Default - Edit TCP/IP Stack Configuration

DNS configuration

Routing

Congestion control algorithm

New Reno ▾

Name

Max. number of connections

11000

Advanced

CANCEL

OK

Finally, you CAN create a brand-new stack if you need to. This is done by using the following CLI command on a host.

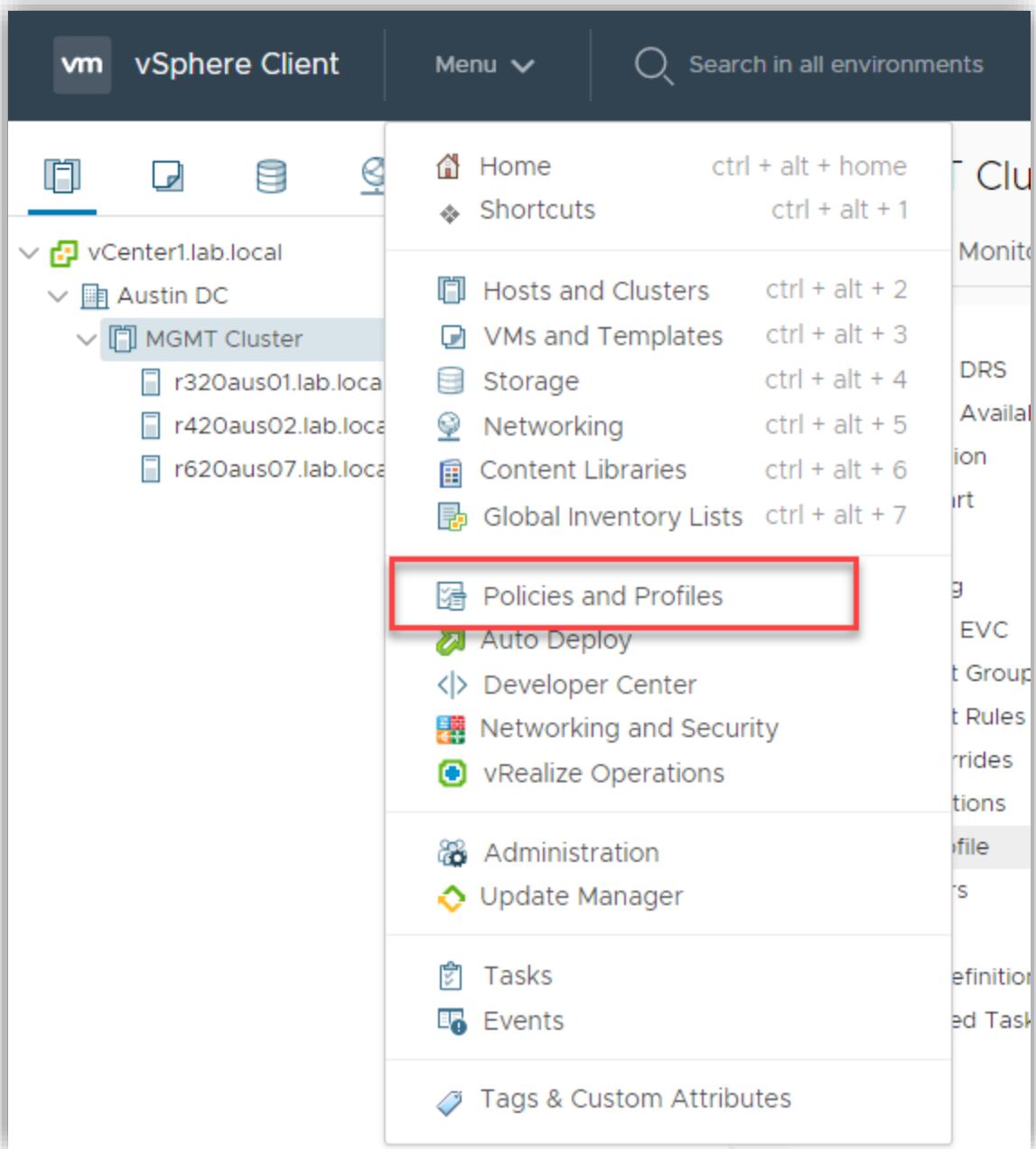
```
esxcli network ip netstack add -N="stack_name"
```

Objective 4.15 – Configure Host Profiles

I will recycle this heading from my previous study guide since I don't see any differences.

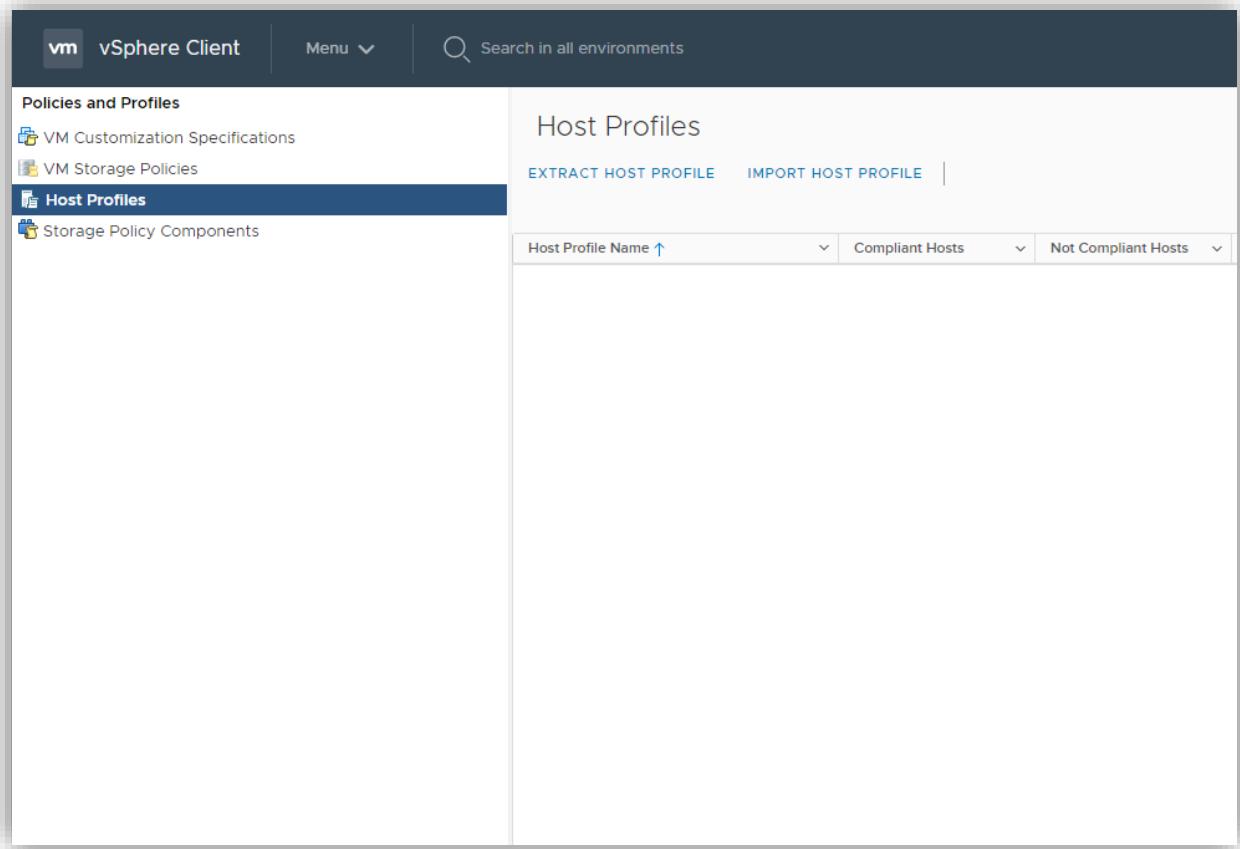
Host profiles provide a mechanism to automate and create a base template for your hosts. Using host profiles, you can make all your hosts the same. VMware will inform you if your host is not in compliance yet, and then you can take steps to remediate it.

You access it under Policies and Profiles

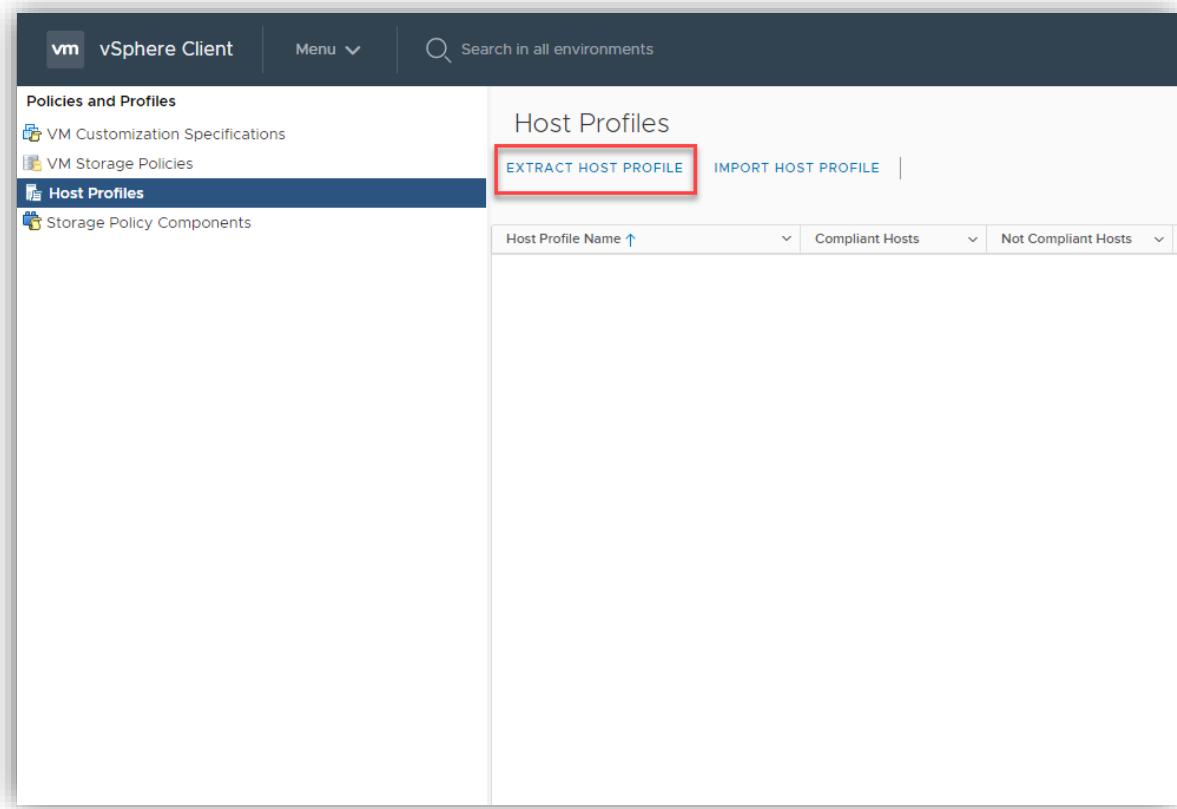


There is a process to it. Here it is:

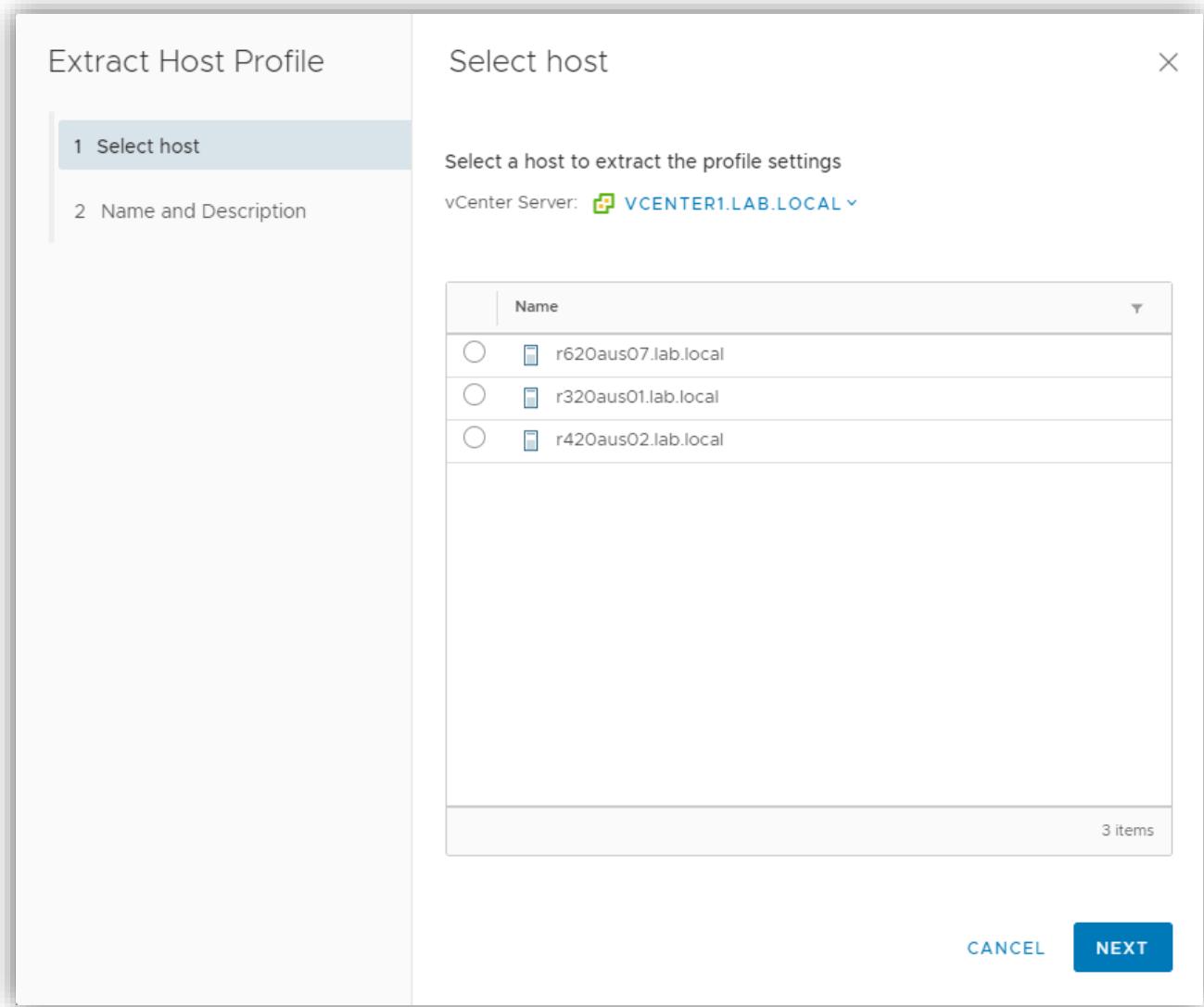
1. Click on Host Profiles on the navigation pane on the left.



2. Next is Extract Host Profile. This will take a host you select, and that will be the "baseline."



3. This will pop up a wizard. This is where you select the host.



4. Give it a name and a description and then Finish

The screenshot shows a dialog box titled "Extract Host Profile". On the left, a vertical navigation bar lists two steps: "1 Select host" and "2 Name and Description", with the second step being the active one. The main area is titled "Name and Description" and contains instructions: "Enter the name and description for the selected profile settings". It has two input fields: "Name" (containing "VCP 2019 Host Profile") and "Description" (an empty text area). At the bottom right, there are three buttons: "CANCEL", "BACK" (in a blue box), and "FINISH" (in a green box).

Extract Host Profile

1 Select host

2 Name and Description

Name and Description

Enter the name and description for the selected profile settings

Name

VCP 2019 Host Profile

Description

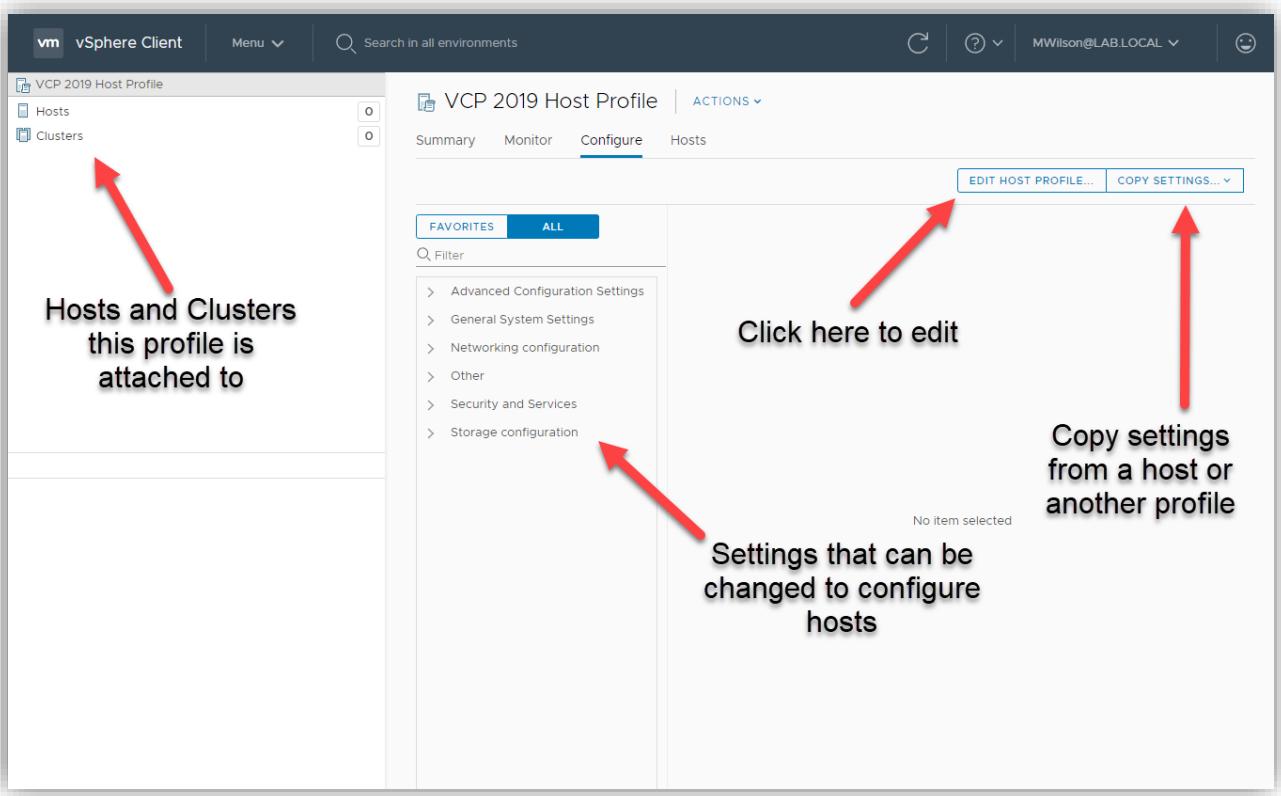
CANCEL BACK FINISH

5. Once that is done, you now have a window that looks like this

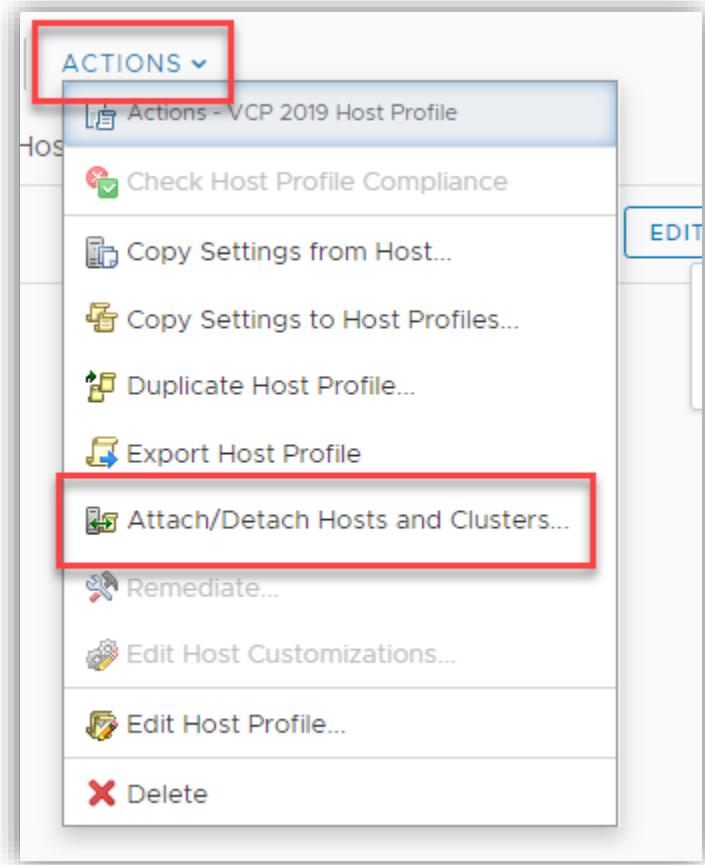
The screenshot shows the 'Host Profiles' section of the vSphere Client interface. The left sidebar lists 'Policies and Profiles' with options for VM Customization Specifications, VM Storage Policies, Host Profiles (which is selected and highlighted in blue), and Storage Policy Components. The main pane is titled 'Host Profiles' and contains a table with the following data:

Host Profile Name	Compliant Hosts	Not Compliant Hosts	Unknown State Hosts	Last Edited	Hosts	VC
VCP 2019 Host Profile	0	0	0	Sep 6, 2019 3:19 AM	0	vCenter1.lab.loc

6. Yes, it's small. The point is when you click on the host profile, you now have additional options above. Notice as well that the profile is also a hyperlink. Click on it.



7. Click on the Actions to attach to hosts or clusters.



Objective 4.16 – Identify boot options

At first, I believed they were looking for installation types, but after further study, I believe they are looking for boot options at the boot command line. This is accomplished by pressing Shift + O in the ESXi installer screen shown below.



At the command prompt that is displayed, enter in

```
ks=[location of installation script] boot command line options
```

location of installation script	boot options
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg	nameserver=00.00.0.0 ip=00.00.00.000 netmask=255.255.255.0 gateway=00.00.00.000

Some of the boot options include (image grabbed from VMware documentation)

Boot Options for ESXi Installation

Boot Option	Description
<code>BOOTIF=hwttype-MAC address</code>	Similar to the <code>netdevice</code> option, except in the PXELINUX format as described in the IPAPPEND option under SYSLINUX at the syslinux.org site.
<code>gateway=ip address</code>	Sets this network gateway as the default gateway to be used for downloading the installation script and installation media.
<code>ip=ip address</code>	Sets up a static IP address to be used for downloading the installation script and the installation media. Note: the PXELINUX format for this option is also supported. See the IPAPPEND option under SYSLINUX at the syslinux.org site.
<code>ks=cdrom:/path</code>	Performs a scripted installation with the script at <i>path</i> , which resides on the CD in the CD-ROM drive. Each CDROM is mounted and checked until the file that matches the path is found.
Important:	
If you have created an installer ISO image with a custom installation or upgrade script, you must use uppercase characters to provide the path of the script, for example, <code>ks=cdrom:/KS_CUST.CFG</code> .	
<code>ks=file://path</code>	Performs a scripted installation with the script at <i>path</i> .
<code>ks=protocol://serverpath</code>	Performs a scripted installation with a script located on the network at the given URL. <i>protocol</i> can be <code>http</code> , <code>https</code> , <code>ftp</code> , or <code>nfs</code> . An example using NFS protocol is <code>ks=nfs://host/porturl-path</code> . The format of an NFS URL is specified in RFC 2224.
<code>ks=usb</code>	Performs a scripted installation, accessing the script from an attached USB drive. Searches for a file named <code>ks.cfg</code> . The file must be located in the root directory of the drive. If multiple USB flash drives are attached, they are searched until the <code>ks.cfg</code> file is found. Only FAT16 and FAT32 file systems are supported.
<code>ks=usb:/path</code>	Performs a scripted installation with the script file at the specified path, which resides on USB.
<code>ksdevice=device</code>	Tries to use a network adapter <i>device</i> when looking for an installation script and installation media. Specify as a MAC address, for example, <code>00:50:56:C0:00:01</code> . This location can also be a <code>vmnicNN</code> name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
<code>nameserver=ip address</code>	Specifies a domain name server to be used for downloading the installation script and installation media.
<code>netdevice=device</code>	Tries to use a network adapter <i>device</i> when looking for an installation script and installation media. Specify as a MAC address, for example, <code>00:50:56:C0:00:01</code> . This location can also be a <code>vmnicNN</code> name. If not specified and files need to be retrieved over the network, the installer defaults to the first discovered network adapter that is plugged in.
<code>netmask=subnet mask</code>	Specifies subnet mask for the network interface that downloads the installation script and the installation media.
<code>vlanid=vlanid</code>	Configure the network card to be on the specified VLAN.

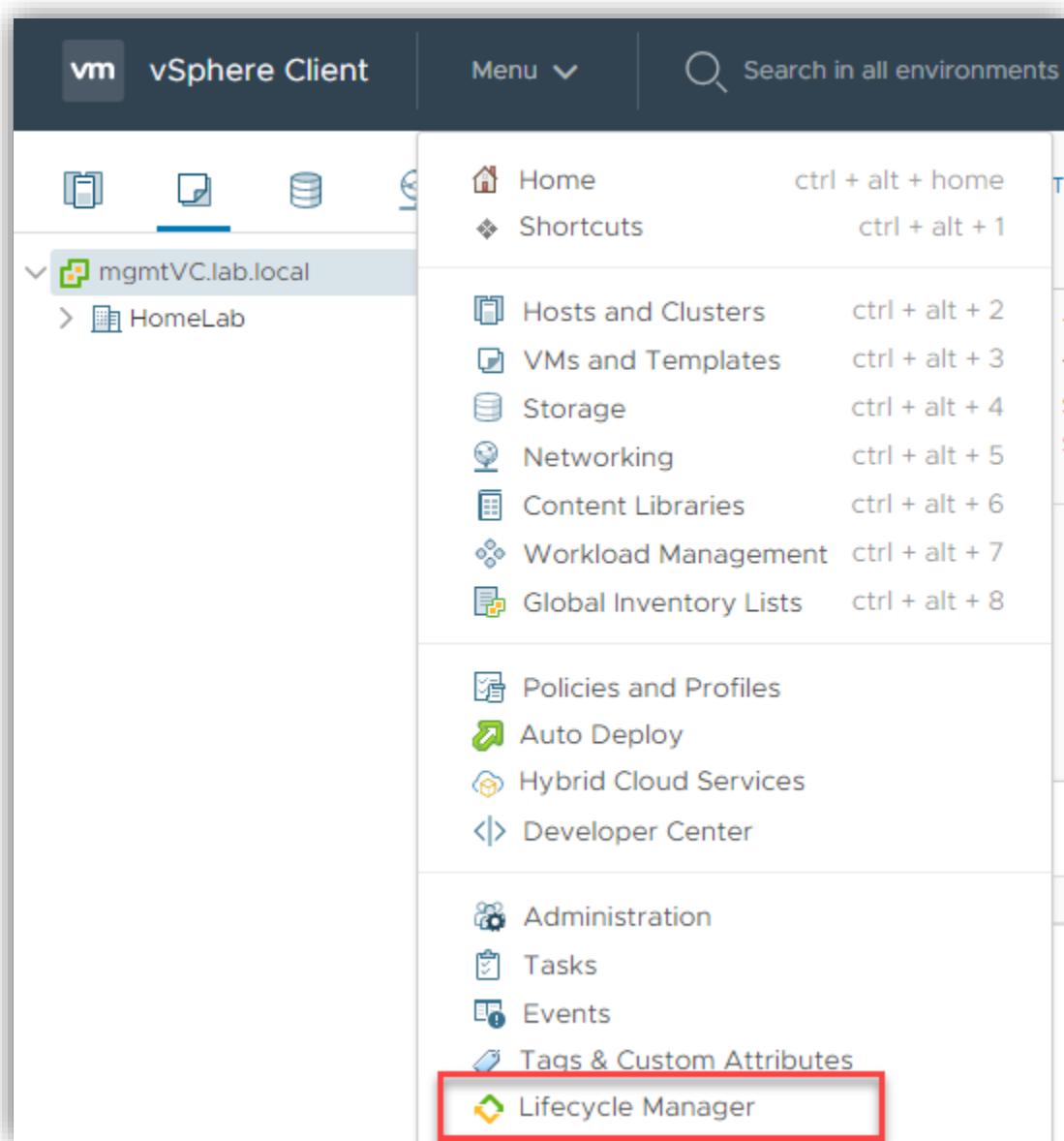
As shown, the location can be in several different places, including a USB drive or CD-ROM.

Objective 4.16.1 – Configure Quick Boot

vSphere Quick Boot is pretty amazing. If you have a server that supports it, instead of doing a lengthy hardware reboot, where the server tests memory etc., it will just skip hardware initialization and just restarts the software. To determine if your host is compatible, check [here](#) or you can run this command at CLI on the host:

```
/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py
```

To configure vSphere to use it, click Update Manager or Lifecycle manager from the Menu.



Next click on Settings then Images under Host Remediation.

The screenshot shows the Lifecycle Manager interface. At the top, there are tabs: Image Depot, Updates, Imported ISOs, Baselines, and Settings. The Settings tab is highlighted with a red box and a red number '1' above it. In the left sidebar, under Host Remediation, the 'Images' option is selected and highlighted with a red box and a red number '2' above it. On the right, the 'Images Remediation Settings' section is displayed. It contains a note: 'Remediation settings are set to VMware-provided settings. They will change if VMware updates their provided settings.' Below this are several configuration items:

Setting	Description
VM Power state	Do not change VM power state
Retry entering maintenance mode in case of failure	3 attempts every 5 minutes
VM Migration	Do not migrate powered off and suspended VMs to other hosts in the cluster
Quick Boot	Quick Boot is disabled
HA Admission Control	Do not disable HA admission control during remediation
Distributed Power Management	Disable DPM on the cluster during remediation

A red box and a red number '3' above it highlight the 'EDIT' button in the top right corner of the settings section.

Now click Enable Quick Boot. – That's it.

Edit Cluster Settings

X

Your changes will override VMware default settings and will apply to all images.

Do not change VM power state ▾

Leave virtual machines and virtual appliances in their current power state

Retry entering maintenance mode in case of failure.

Retry delay 5 minutes

Number of retries 3

Migrate powered off and suspended VMs to other hosts in the cluster, if a host must enter maintenance mode.

Disable HA admission control during remediation.

Disable DPM on the cluster during remediation.

Enable Quick Boot.

CANCEL

SAVE

Section 5 – Performance-tuning, Optimization, Upgrades

Objective 5.1 – Identify resource pools use cases

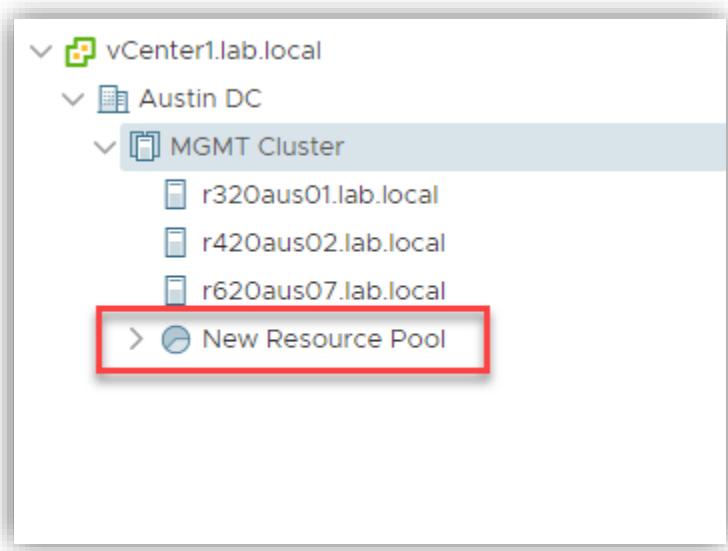
The official description of a resource pool is a logical abstraction for the flexible management of resources (same exact definition as vSphere 6.x). My unofficial description is an object inside of vSphere that allows you to partition and control resources to specific VMs. Resource pools partition memory and CPU.

Everyone starts with the root resource pool. This is a pool of resources that exists at the host level. You don't see it, but it's there. You create a resource pool under that that slices off resources. It's also possible to nest resource pools. For example, if you had a company and inside that company you had departments, you could partition resources into the company and departments. This works as a hierarchy. When you create a child resource pool from a parent, you are further diminishing your resources - unless you allow it to draw more from further up the hierarchy.

Why use resource pools? You can delegate control of resources to other people. There is isolation between pools, so resources for one doesn't affect another. You can use resource pools to delegate permissions and access to VMs. Resource pools are abstracted from the hosts' resources. You can add and remove hosts without having to make changes to resource allocations.

You can also use resource Pools to divide resources to departments that have paid for them. If a department has paid for 50% of a new server, you can set up a resource pool to guarantee that the department receives those resources.

You can identify resources pools by their icon.



Resource Pools are created to slice off resources. You can have reservations on Resource Pools as well, but you can do a bit more. You can have expandable reservations to borrow resources from its parent if it needs to. This picture shows what you can configure when you create a CPU and Memory Resource Pool

New Resource Pool | MGMT Cluster X

Name	New Resource Pool		
CPU			
Shares	Normal	4000	
Reservation	0	MHz	▼
Max reservation: 66,458 MHz			
Reservation Type	<input checked="" type="checkbox"/> Expandable		
Limit	Unlimited	MHz	▼
Max limit: 74,460 MHz			
Memory			
Shares	Normal	163840	
Reservation	0	MB	▼
Max reservation: 493,105 MB			
Reservation Type	<input checked="" type="checkbox"/> Expandable		
Limit	Unlimited	MB	▼
Max limit: 564,479 MB			

CANCEL OK

You can also assign shares on an individual VM basis

Edit Settings | Windows - vCenter Backup Machine

Virtual Hardware VM Options

ADD NEW DEVICE

CPU	
Cores per Socket	2 <input type="button" value="▼"/>
CPU Hot Plug	<input type="checkbox"/> Enable CPU Hot Add
Reservation	0 <input type="button" value="▼"/> MHz <input type="button" value="▼"/>
Limit	Unlimited <input type="button" value="▼"/> MHz <input type="button" value="▼"/>
Shares	Normal <input type="button" value="▼"/> 2000
CPUID Mask	<input type="button" value="Expose the NX/XD flag to guest"/> Advanced...
Hardware virtualization	<input type="checkbox"/> Expose hardware assisted virtualization to the guest OS i
Performance Counters	<input type="checkbox"/> Enable virtualized CPU performance counters
I/O MMU	<input type="checkbox"/> Enabled
Memory	
Reservation	8 GB <input type="button" value="▼"/> MB <input type="button" value="▼"/>
Limit	0 <input type="button" value="▼"/> MB <input type="button" value="▼"/>
Shares	Normal <input type="button" value="▼"/> 81920
Memory Hot Plug	<input type="checkbox"/> Enable

CANCEL

OK

To assign disk shares, you can look at the individual VM

Edit Settings | Windows - vCenter Backup Machine

X

Virtual Hardware VM Options

ADD NEW DEVICE

> CPU	2	v
> Memory	8	GB v
Hard disk 1	80	GB v
Maximum Size	12.09 TB	
VM storage policy	Datastore Default v	
Type	Thick Provision Lazy Zeroed	
Sharing	No sharing v	
Disk File	[Synology] Windows - vCenter Backup Machine/Windows - vCenter Backup Machine.vmdk	
Shares	Normal v	1000
Limit - IOPs	Unlimited v	
Virtual flash read cache	0	MB v
Disk Mode	Dependent v	
Virtual Device Node	SCSI controller 0 v	SCSI(0:0) Hard disk 1 v
> SCSI controller 0	VMware Paravirtual	
> Network adapter 1	VM Network v	<input checked="" type="checkbox"/> Connected
> CD/DVD drive 1	Client Device v	<input type="checkbox"/> Connected

You can also assign shares and manage network resources on Virtual Distributed Switches with Network I/O Control enabled.

Edit Settings | nsx-mgmt-1

> CPU	6	v	(i)
> Memory	24	GB	v
> Hard disk 1	200	GB	v
> Hard disk 2	100	GB	v
> SCSI controller 0	LSI Logic Parallel		
Network adapter 1		sddc-vds01-mgmt v	<input checked="" type="checkbox"/> Connected
Status	<input checked="" type="checkbox"/> Connect At Power On		
Port ID	54		
Adapter Type	VMXNET 3 v		
DirectPath I/O	<input checked="" type="checkbox"/> Enable		
Shares	Normal	v	50
Reservation	0	v	Mbit/s v
Limit	Unlimited	v	Mbit/s v
MAC Address	00:50:56:ac:4d:5e		Automatic v
> Video card	Specify custom settings v		
VMCI device			
> Other	Additional Hardware		

CANCEL

OK

Objective 5.1.1 – Explain shares, limits, and reservations (resource management)

Shares - Shares can be any arbitrary number you make up. All the shares from all the resource pools added up will equal to a total number. That total number will be a total of the root pool, for example. If you have two pools that each has 8000 shares, there are a total of 16,000 shares, and each resource pool makes up half of the total, or $8,000/16,000$. There are default options available as well in the form of Low, Normal, and High. Those will equal $1,000/2,000$ and $4,000$ shares, respectively.

Reservations - This is a guaranteed allocation of CPU or memory resources you are giving to that pool. The default is 0. Reserved resources are held by that pool regardless if there are VMs inside it or not.

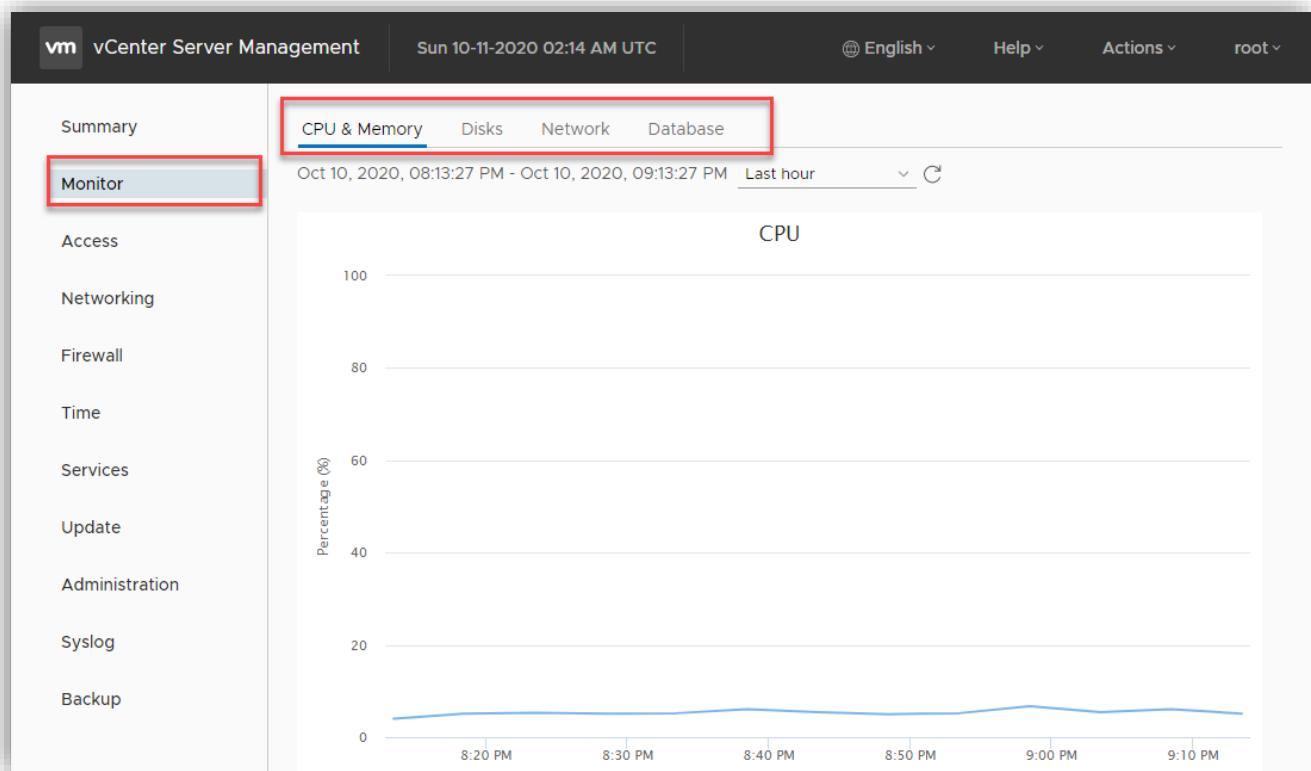
Expandable Reservation is a checkbox that allows the pool to “borrow” resources from its parent resource pool. If this is the parent pool, then it will borrow from the root pool.

Limits - specify the upper limit of what a resource pool can grab from either CPU or memory resources. When teaching VMware’s courses, unless there is a definite reason or need for it, you shouldn’t use limits. While shares only work when there is contention (fighting among VMs for resources), limits create a hard stop for the VM even if resources are high. Usually, there is no reason to limit how much resources a VM would use if there is no contention.

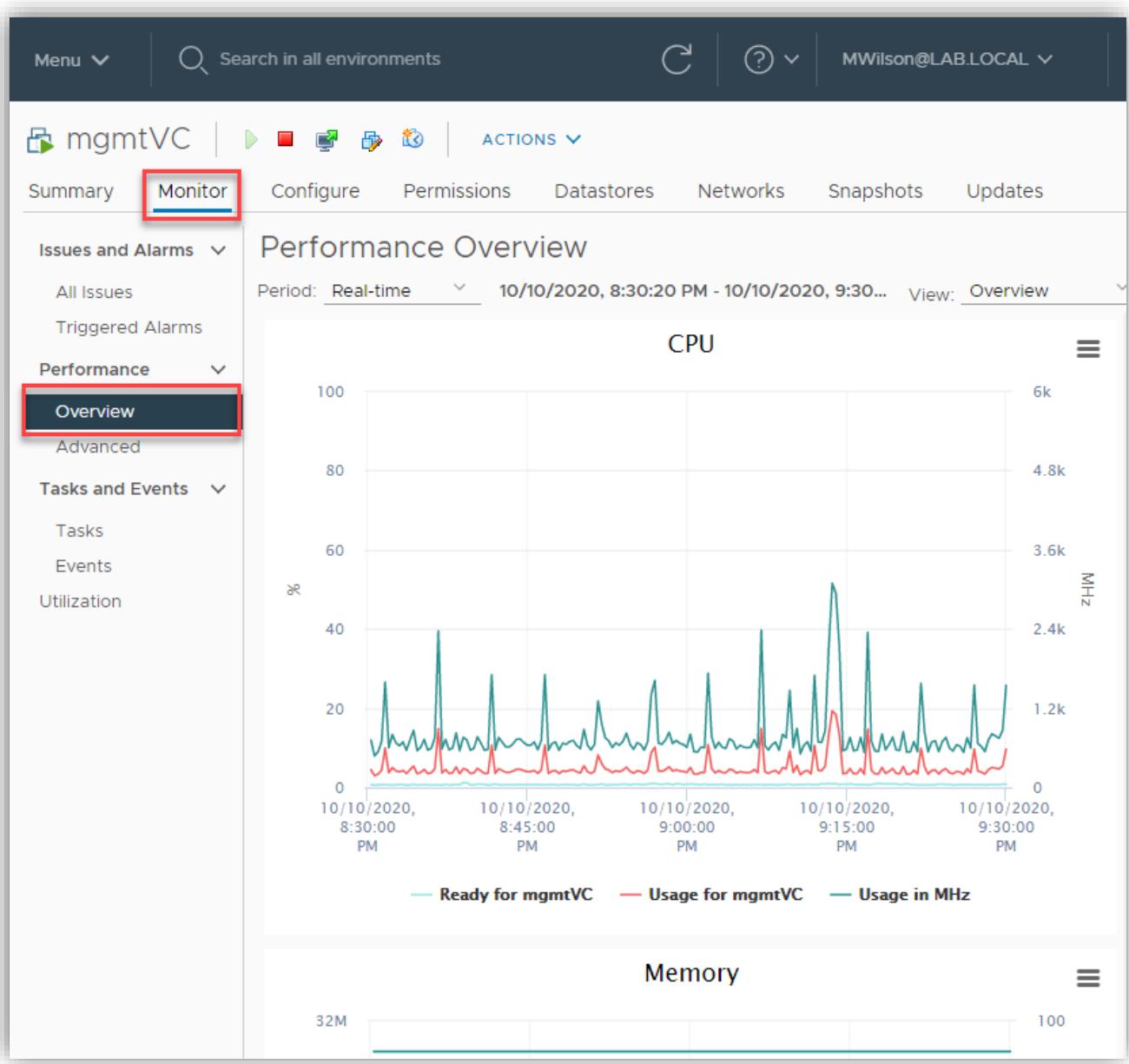
In past exams, exam questions were asking you to calculate resources given several resource pools. Make sure you go over how to do that.

Objective 5.2 – Monitor resources of vCenter Server Appliance and vSphere environment
Monitoring resources of both your vCenter Server Appliance and vSphere appliance is done from several places. There are many different products out there besides to do this as well. vRealize Operations Manager is one such tool. From within vSphere itself, there are several tools to do this. First, let’s cover the vCenter Server Appliance.

From within the VCSA VAMI (on port 5480), there is a Monitoring pane you can use to see resources your vCenter is consuming.



As shown in the screenshot above, you can monitor CPU, memory, disks, network, and even the database. From within the HTML5 client, you can monitor the vCenter VM by going to the VM and then clicking on Monitor, as shown here.



You can look at the different resources for the VM and change time periods. You can also monitor the vCenter Server by using “top” on the VM console, as shown here.

To monitor resources on the rest of the environment, this is accomplished by clicking on the VM and then clicking the monitor tab. Just like for the vCenter Server. This can be done for any of the VMs, cluster, or host. If you want to monitor the hosts via CLI, you can use 'esxtop' to do that. This is what that looks like.

```

xr2.lab.local - PuTTY
2:56:46am up 8 days 2:27, 1576 worlds, 20 VMs, 88 vCPUs; CPU load average: 0.22, 0.22, 0.23
PCPU USED(%): 11 1.2 3.9 0.8 5.5 1.6 6.4 2.1 6.2 0.9 4.7 0.1 1.7 5.1 3.1 8.3 3.1 3.2 0.0 0.0 4.1 2.5 6.7
4.8 6.8 8.6 1.3 10 7.0 1.3 2.5 7.7 1.3 8.5 2.2 0.3 3.1 3.4 2.6 0.8 11 6.0 7.5 15 10 11 7.2 9.3 15 1
4 25 7.4 5.8 13 27 8.1 17 9.7 11 7.6 19 7.0 8.1 38 10 31 12 30 17 9.6 13 32 16 17 12 13
39 9.4 25 15 AVG: 9.8
PCPU UTIL(%): 15 2.8 8.2 1.7 10 3.5 10 4.6 9.7 1.9 7.1 0.1 2.7 7.2 5.2 9.4 4.5 6.1 0.1 0.0 6.1 5.4 10
7.6 7.8 10 2.9 15 11 2.9 5.3 7.6 2.4 10 3.4 0.7 6.7 7.3 5.5 1.8 23 14 17 24 20 21 16 19 22 2
1 30 14 14 23 32 16 25 18 20 15 28 14 13 40 15 36 18 35 25 18 15 34 22 22 19 20
41 14 28 21 AVG: 14
CORE UTIL(%): 18 9.7 13 14 11 7.6 9.5 13 10 1.2 12 17
17 18 13 12 12 3.7 13 7.2 33 36 36 36 31 39 36
41 33 42 38 32 38 47 46 48 38 46 39 36
49 45 AVG: 26

```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT	%VMWAIT	%RDY	%IDLE	%OVRLP
289669	289669	vcf-esxi-2	22	385.27	395.58	0.53	1818.08	0.23	1.40	413.73	0.69
288478	288478	vcf-esxi-1	22	111.38	178.47	1.38	2033.92	0.00	3.31	630.99	0.70
188703	188703	mgmtVC	33	92.40	133.89	0.31	3185.60	0.00	0.76	671.48	0.27
289701	289701	vcf-esxi-3	22	60.45	118.17	0.82	2093.00	1.08	3.25	689.56	0.52
289661	289661	vcf-esxi-4	22	43.26	74.00	0.46	2137.78	0.00	3.63	729.23	0.40
136227	136227	Element 12.0	15	19.64	22.17	0.06	1485.92	0.08	0.23	179.37	0.04
30388	30388	Synology_DS3615	22	17.80	34.76	1.02	2177.33	0.00	1.45	369.86	0.70
137393	137393	SolidFire VCSA	24	17.55	16.26	0.02	2398.56	0.00	0.11	185.87	0.03
393604	393604	esxtop.2188847	1	10.97	8.51	0.00	91.95	-	0.00	0.00	0.00
15232	15232	vROperations	15	9.46	15.93	0.13	1494.46	0.00	0.59	387.97	0.07
140048	140048	SolidFire ESXi	13	8.33	15.31	0.13	1291.65	0.24	2.02	385.71	0.16
289677	289677	vcf-esxi-12	17	7.90	15.39	0.13	1693.57	0.13	2.41	385.54	0.12
289685	289685	vcf-esxi-10	17	7.76	14.90	0.16	1694.01	0.00	2.36	385.92	0.13
289693	289693	vcf-esxi-11	17	7.37	14.85	0.12	1694.05	0.00	2.37	385.83	0.12
1	1	system	757	4.56	6956.83	0.00	67952.22	-	1114.91	0.00	10.61
290887	290887	vcf-infra1	11	4.15	8.66	0.03	1097.79	0.06	0.67	195.31	0.04
136242	136242	mNode 12.0	15	3.53	6.69	0.05	1500.00	0.00	0.27	598.68	0.02

Objective 5.3 – Identify and use tools for performance monitoring

Tools used for performance monitoring are precisely the ones shown above. Other tools can be used, as well. These include vRealize Operations Manager. vROPs integrates intimately with vSphere and shows much information on your environment. From within your HTML5 client, you can find info like this:

vm vSphere Client | Menu ▾ | Search in all environments | C | ? | MWilson@LAB.LOCAL | ☺

Home | Shortcuts

Hosts and Clusters | VMs and Templates | Storage | Networking | Content Libraries | Workload Management | Global Inventory Lists

Policies and Profiles | Auto Deploy | Hybrid Cloud Services | Developer Center

Administration | Tasks | Events | Tags & Custom Attributes | Lifecycle Manager

vRealize Operations | DRaaS

vRealize Operations

You can manage vCenter- mgmtVC.lab.local here. To manage multiple vCenters, use [vRealize Operations](#)

mgmtVC.lab.local Last Updated - 10:02 PM Quick Links

1 Datacenters	2 Clusters	5 Hosts	34 Virtual Machines	6 Datastores	0 Resource Pools
---------------	------------	---------	---------------------	--------------	------------------

Are there any Issues? Action Required

12 Critical

These are all the critical alerts across your vCenter.

VIEW DETAILS

vRealize Operations helps you prioritize your alerts.

- 3 Immediate
- 4 Warning
- 1 Info

Am I running out of Capacity?

Based On Compute ▾

FIND OUT HOW

What can be Reclaimed?

You can potentially **Save 0.00** by reclaiming your resources

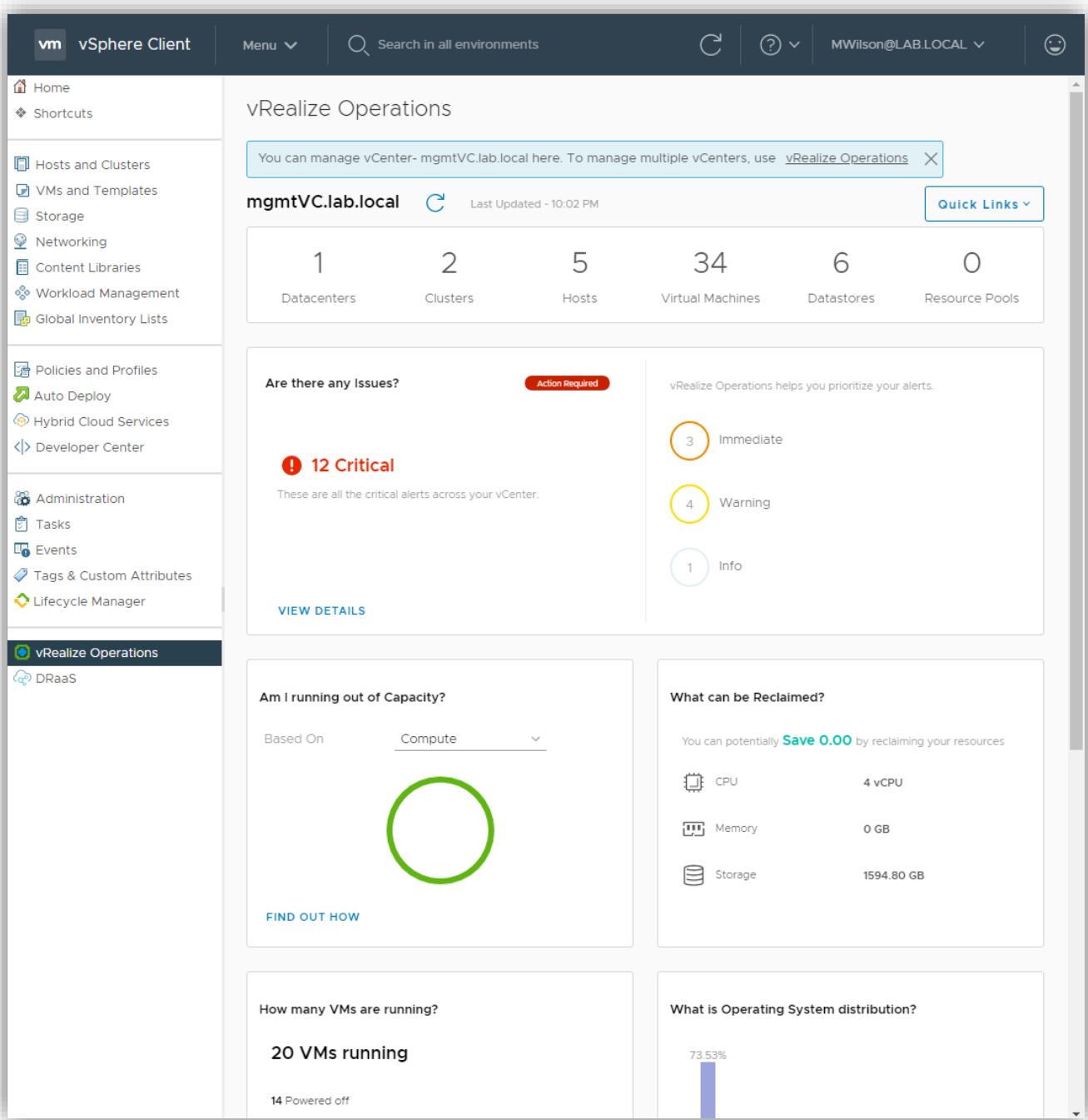
CPU	4 vCPU
Memory	0 GB
Storage	1594.80 GB

How many VMs are running?

20 VMs running

14 Powered off

What is Operating System distribution?



When you bring up vRealize Operations Manager, you get a lot more info.

vRealize Operations Manager Dashboards vSphere Compute Inventory Actions All Dashboards 1H 6H 24H 7D CUSTOM Locked

BACK

Relationships

Quick filter (Name)

Properties

CPU Capacity 24 GHz 3... GB

Disk Capacity 27 TB 34 VM

Metrics

CPU Demand 24 GHz

RAM Demand 237.4 GB

Disk IOPS 3,547.8

Powered-on VM 20

Relationships diagram:

```

graph LR
    A[vSphere World] --- B[VC_VROPS_Unity]
    B --- C[HomeLab]
  
```

Clusters

Name	CPU Capacity
LAB	79.81 GHz
Mgmt Cluster	0 GHz

1 - 2 of 2 items

ESXi Hosts

Name	Model
r730.lab.local	Pivot3 Inc. P
mgmt1.lab.local	Nutanix NX
mgmt2.lab.local	Nutanix NX
r630.lab.local	Dell Inc. Pow
xr2.lab.local	

1 - 5 of 5 items

Virtual Machines

Name	CPU
2016 Server Template	2
DC01.lab.local	1
DC02.lab.local	2
Element 12 - 2	2
Element 12.0	2
Windows	2

1 - 27 of 27 items

Objective 5.4 – Configure Network I/O Control (NIOC)

Network I/O Control allows you to determine and shape bandwidth for your vSphere networks. They work in conjunction with Network Resource Pools to allow you to determine the bandwidth for specific types of traffic. You enable NIOC on a vSphere Distributed Switch and then set shares according to needs in the configuration of the VDS. This is a feature requiring Enterprise Plus licensing or higher. Here is what it looks like in the UI.

The screenshot shows the vSphere Client interface with the navigation bar at the top. The left sidebar shows a tree view of network resources under 'mgmtVC.lab.local' and 'HomeLab'. A red box highlights the 'DSwitch' node under 'VM Network'. The main pane shows the 'DSwitch' configuration page. A red box highlights the 'Configure' tab. Below it, a red box highlights the 'System traffic' section of the 'Resource Allocation' table. The table lists various traffic types with their current settings:

Traffic Type	Shares	Shares Value	Reservation	Limit
Management Traffic	Normal	50	0 Mbit/s	Unlimited
Fault Tolerance (FT) Traffic	Normal	50	0 Mbit/s	Unlimited
vMotion Traffic	Normal	50	0 Mbit/s	Unlimited
Virtual Machine Traffic	High	100	0 Mbit/s	Unlimited
iSCSI Traffic	Normal	50	0 Mbit/s	Unlimited
NFS Traffic	Normal	50	0 Mbit/s	Unlimited
vSphere Replication (VR) Traffic	Normal	50	0 Mbit/s	Unlimited
vSAN Traffic	High	100	0 Mbit/s	Unlimited
vSphere Data Protection Backup Traffic	Normal	50	0 Mbit/s	Unlimited

The traffic types that are shown here are there by default. You can make changes to them by clicking on one of the types and then clicking 'Edit'. When you click edit, a screen appears where you can choose shares, reservations, and limits.

Edit Resource Settings | DSwitch X

Name	Management Traffic	
Shares	Normal	50
Reservation	0	Mbit/s
Max. reservation: 7.5 Gbit/s		
Limit	<input checked="" type="checkbox"/> Unlimited	
	Unlimited	Mbit/s
Max. limit: 10 Gbit/s		

CANCEL OK

You can create new network resource types by clicking on Network Resource Pool and then ‘Add.’ This allows you to create a new pool that has a Reservation quota. You then would assign a VM to that pool. This group slices off bandwidth from the Virtual Machine system type, so you need to setup bandwidth reservation for that group first.

Objective 5.5 – Configure Storage I/O Control (SIOC)

Storage I/O Control allows cluster-wide storage I/O prioritization. You can control the amount of storage I/O allocated to virtual machines to get preference over less critical virtual machines. This is accomplished by enabling SIOC on the datastore and set shares and upper limit IOPS per VM. SIOC is enabled by default on SDRS clusters. Here is what the screen looks like to enable it.

Configure Storage I/O Control | VirtualSynology X

Storage I/O Control is used to control the I/O usage of a virtual machine and to gradually enforce the predefined I/O share levels.

Enable Storage I/O Control and statistics collection

Storage I/O congestion threshold:

Percentage of peak throughput

90 %

Manual

30 ms

[RESET TO DEFAULTS](#)

Statistic Collection

Include I/O statistics for SDRS

Disable Storage I/O Control but enable statistics collection

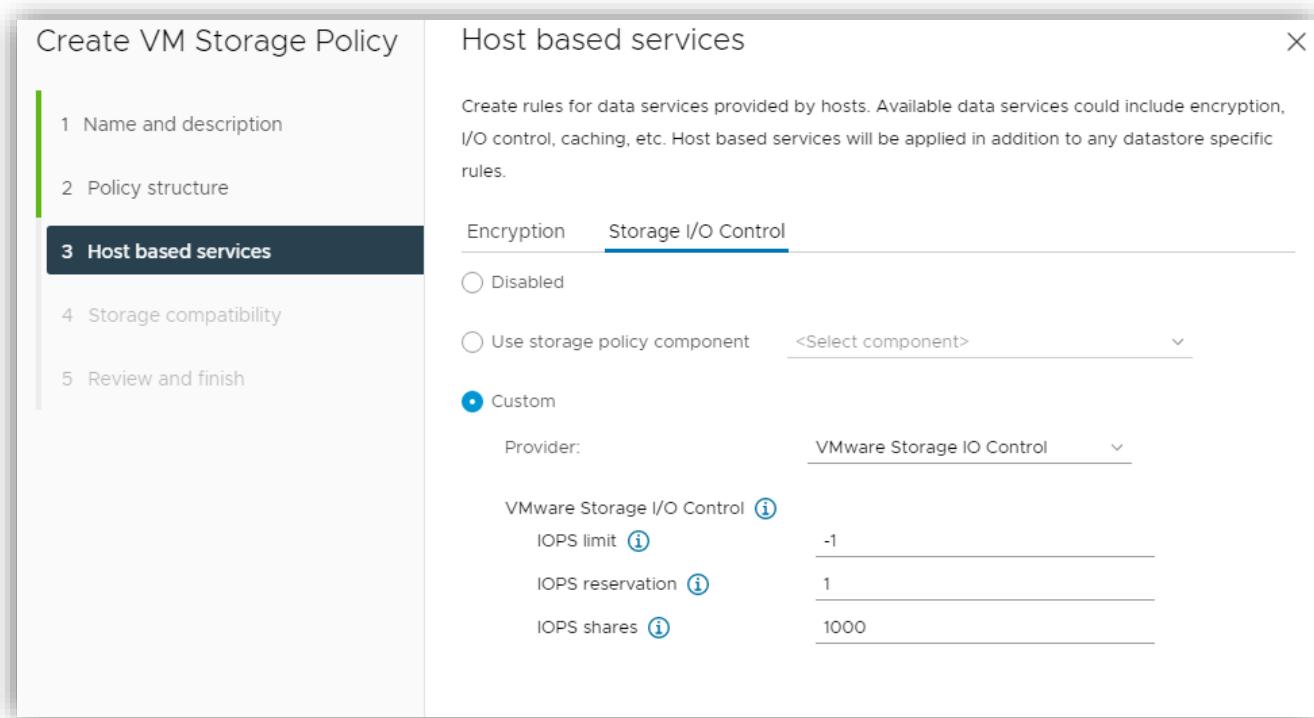
Include I/O statistics for SDRS

Disable Storage I/O Control and statistics collection

[CANCEL](#)

[OK](#)

Once SIOC is enabled on the datastore, you can either set shares and limits on individual VM disks, or you can set up a Storage Policy and apply it to VMs to control performance. Here is a picture of one way you might set up a storage policy.



Objective 5.6 – Explain the performance impact of maintaining virtual machine snapshots

VMware can preserve a Point in Time or PIT for a VM. This process freezes the original virtual disk and creates a new Delta disk. All I/O is now routed to the Delta disk. If data is needed that still exists on the original disk, it will need to go back to that to retrieve data. So now, you are accessing two disks. Over time you can potentially double the size of the original disk as you make changes and new I/O. The original 10 GB disk becomes 20 GB over 2 disks. If you create additional snapshots, you create new Delta disks, and it continues.

Now that we understand a bit more about them, we see the limitations inherent. This tool was never meant to be a backup. It was designed to revert the VM to the original (if needed) after small changes. Most backup tools DO use snapshots as part of their process, but only for the amount of time needed to copy the data off, and then the snapshot is consolidated back again. Here are a few Best Practices from VMware on how to use them.

- Don't use snapshots as backups – significant performance degradation can occur, and I have seen people lose months of data or more when the chain got too long.
- 32 snapshots are supported, but it's better not to test this.
- Don't use a snapshot longer than 72 hrs.
- Ensure if you are using a 3rd Party backup that utilizes the snapshot mechanism, they are getting consolidated and removed after the backup is done. This may need to be checked via CLI
- Don't attempt to increase disk size if the machine has a snapshot. You risk corrupting your snapshot and possible data loss.

Objective 5.7 – Plan for upgrading various vSphere components

Depending on what version you are starting from, this can be a significant undertaking. One major hurdle could be hardware compatibility. VMware has made several tools available to navigate your upgrade. The first is the vSphere Assessment Tool. You can find more about that tool and also how to download it [here](#).

Once you have checked your hardware and workloads and they can move, the next step is making sure all your VMware products are compatible with each other. You can find that information using the VMware Product Interoperability Matrix [here](#).

The next step is figuring out the order of upgrading. If it's just a simple VMware environment with no additional products, there are very few steps needed. They are

1. Backup vCenter Server and configuration
2. Upgrade your vCenter Server
3. Upgrade ESXi Hosts
4. Upgrade VMs (vSphere tools and/or VMware Hardware version)

And you're done. If there are additional products in the environment, you should look at the Knowledge Base Article VMware has made available to determine the update sequence [here](#).

Section 6 – Troubleshooting and Repairing - There are no testable objectives for this section.

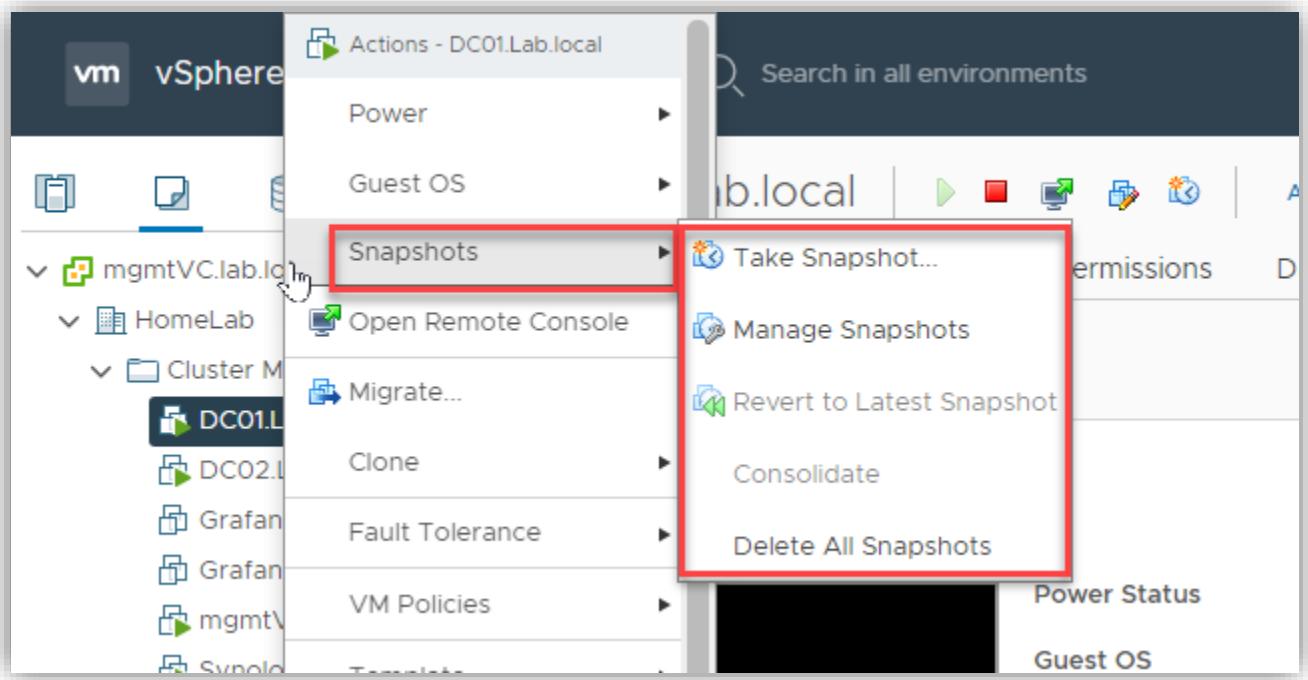
Since this isn't a testable section, we won't cover this. If there is enough of an ask, I may add a bit in here.

Section 7 – Administrative and Operational Tasks

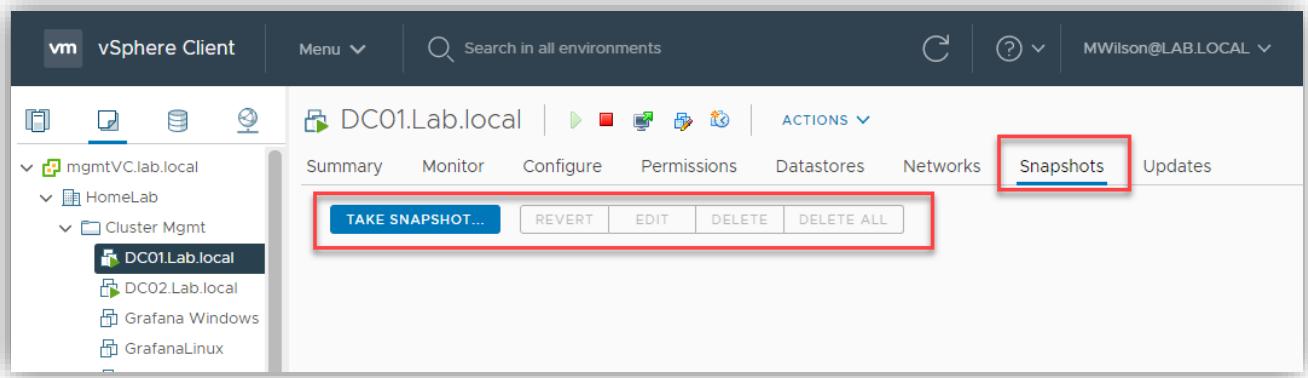
Objective 7.1 – Create and manage virtual machine snapshots

We've already discussed use cases and why you might utilize snapshots. Now let's take a look at how to create and manage snapshots. There are several ways we can access snapshots. One is by right-clicking

on the VM and then choosing "Snapshots."



Another way you can access snapshots is to go to the Snapshot Tab for the VM



The method for taking a snapshot is pretty straightforward. You click on the "Take Snapshot" button in either of those, and it will prompt you with a new window. That window looks like this.

Take snapshot

X

Name

VM Snapshot 10/22/2020, 3:42:56 PM

Description

Include virtual machine's memory

Quiesce guest file system(requires VM tools)

CANCEL

CREATE

You should fill in a descriptive name for it (perhaps outlining why and the date and time) and then decide if you want to include the VM's memory contents. If you decide to include the memory, there is no need to quiesce the guest file system so that that option will remain grayed out. If you uncheck the memory box, the other will become available. Quiescing will allow you to stun or pause the VM briefly to ensure there is no data in-flight that is not snapshotted. Once you finish, this is what the tab will look like (if you notice, I took 2 snapshots to show the tree effect)

DC01.Lab.local

ACTIONS

Summary Monitor Configure Permissions Datastores Networks Snapshots Updates

TAKE SNAPSHOT... REVERT EDIT DELETE DELETE ALL

VCP 2020 Test 10%2f22%2f2020, 3:44:15 PM

VCP 2020 Test 2 10%2f22%2f2020, 3:47:40 PM

You are here

Name	Description
VCP 2020 Test 2 10%2f22%2f2020, 3:47:40 PM	VCP 2020 Test 2 10%2f22%2f2020, 3:47:40 PM
	Timestamp 10/22/20, 3:47 PM
	Size 23.03 MB
	Snapshot the virtual machine's memory No
	Quiesce guest file system No

You can see the first one on top, then one more I made underneath. On the right side, you can see the details about the snapshot. I can do several things now with the snapshots. I can revert and delete it. If I revert to the first one, That will change where I am in the timeline. Here is what happens.

vSphere Client

DC01.Lab.local

ACTIONS

Summary Monitor Configure Permissions Datastores Networks

TAKE SNAPSHOT... REVERT EDIT DELETE DELETE ALL

VCP 2020 Test 10%2f22%2f2020, 3:44:15 PM

You are here

VCP 2020 Test 2 10%2f22%2f2020, 3:47:40 PM

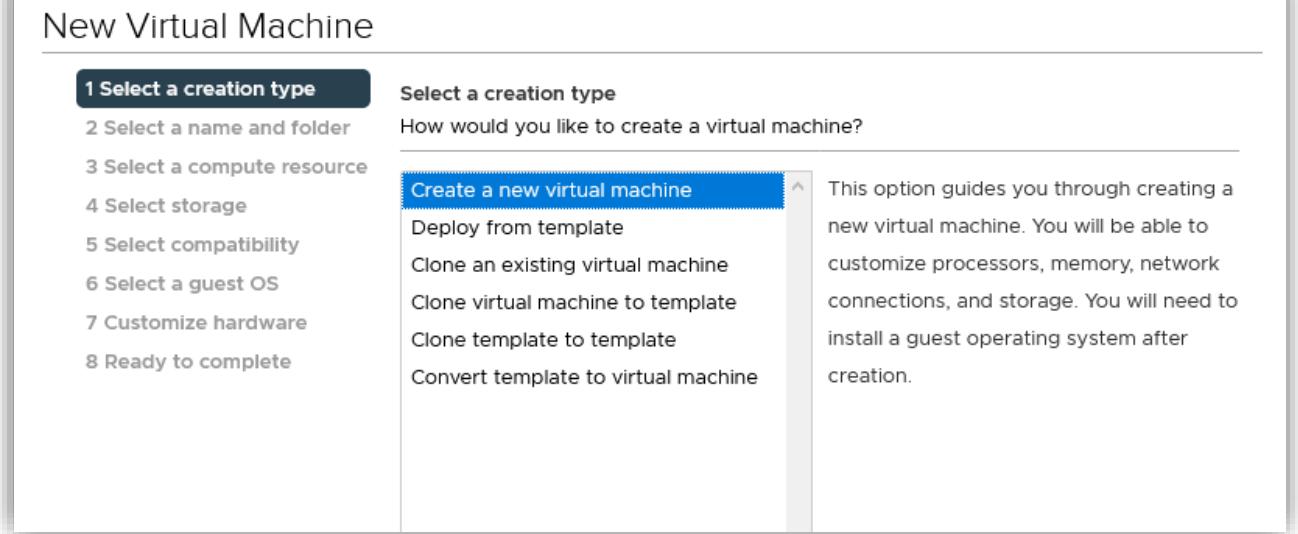
If I had deleted the first one, I would have stayed in the same place, but it would have merged the next snapshot changes, if any. If I delete the second one while I am reverted to the first, the second one just goes away. And if I delete all, it will just merge all changes. Keep in mind, if you hadn't snapshotted the memory and you revert, it will turn the machine off to revert. This is the same as deleted. Here is a handy table from VMware to tell if the machine will be powered off or not.

Virtual Machine Power State After Restoring a Snapshot	
Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Again, you don't want to have snapshots running too long, and make sure you name them descriptively so that if you do have to come back at some point, you know what has been snapshotted.

Objective 7.2 – Create virtual machines using different methods (Open Virtual Machine Format (OVF) templates, content library, etc.)

There are several options available to you to create a new virtual machine. When you right-click on a cluster, host, or Folder and select New Virtual Machine, you will be presented with the following Menu.



There are several options to create a new VM there. You can also right-click and select Deploy OVF template, or you can create a preconfigured VM appliance. You also create a VM from a physical machine using the P2V tool.

As you go throughout the wizard above, you need to select a location, host, datastore, and what you will run on it. (An OVF template, you don't need to select what will run on it, but still need to choose a location, host, and storage for it.

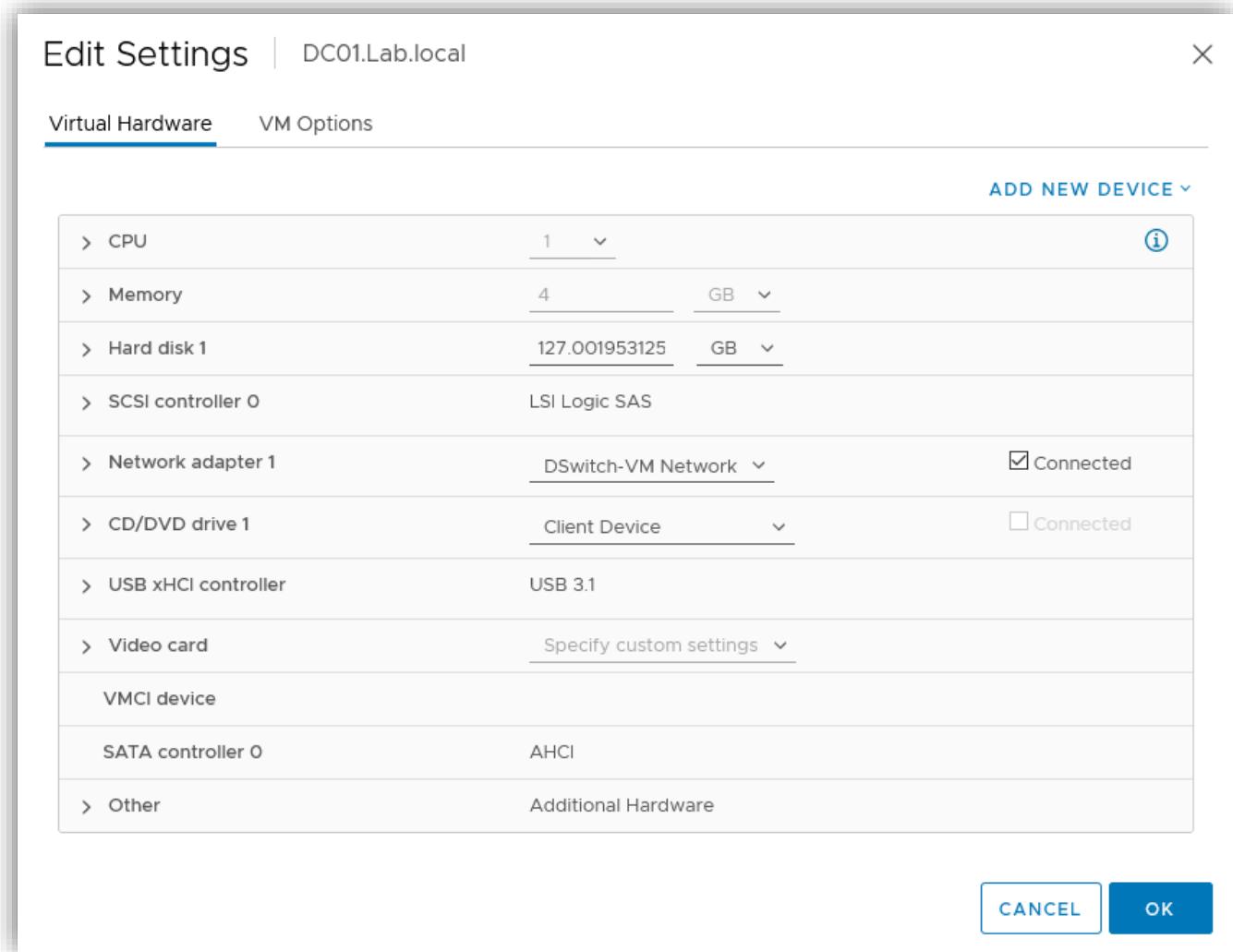
Creating a new VM via PowerCLI isn't hard either; it can be done with a command like the following:

```
New-VM -Name 'TestVM' -VMHost 'VMHost-1' -Datastore 'TestDatastore' -  
DiskGB 40 -MemoryGB 8 -NumCpu 2 -NetworkName 'Virtual Machine Network'
```

That creates a new VM with the name TestVM on VMHost-1 storing its 40 GB VMDK on the TestDatastore. A lot simpler than going through a long wizard to me.

Objective 7.3 – Manage virtual machines

You can manage VMs through the HTML5 client, API, PowerCLI (PowerShell), or even through the ESXi host console. There are even some options you can only do using PowerCLI. You are presented with a large number of options when you right-click on a VM. To change the VM's settings, you can click on "Edit Settings" and get the following screen.



Keep in mind that some options can only be changed when the VM is powered off.

Objective 7.4 – Manage storage (datastores, storage policies, etc.)

There are numerous places for you to manage storage, depending on what you need to do. For example, when setting up iSCSI adapters, you can accomplish this by clicking on the host. Then select the Configure tab and then Storage Adapters and iSCSI Adapter. From there, you can add iSCSI targets by clicking on the Dynamic Discovery or Static.

The screenshot shows the vSphere Client interface for host `r630.lab.local`. The left sidebar shows the inventory tree with nodes like `mgmtVC.lab.local`, `LAB`, and `r630.lab.local`. The main pane is titled "Storage Adapters" under the "Configure" tab. The "Dynamic Discovery" tab is selected, displaying a list of three iSCSI targets:

Target IP	Port	Protocol
192.168.10.4	3260	iSCSI
192.168.10.10	3260	iSCSI
192.168.1.22	3260	iSCSI

As you can see, I already have several targets inputted. Once you add them, you rescan storage for the host to query for devices. Those devices will show up under devices, as shown here.

Properties Devices Paths Dynamic Discovery Static Discovery Network Port Binding Advanced Options						
<input type="button" value="Refresh"/> <input type="button" value="Attach"/> <input type="button" value="Detach"/> <input type="button" value="Rename..."/>						
Name	L...	Type	Capacity	Datastore	Operational ...	
FreeNAS iSCSI Disk (naa.6589fc000000a68...)	0	disk	20.00 TB	FreeNas_dS	Attached	
SYNOLOGY iSCSI Disk (naa.6001405e363d66...)	0	disk	6.08 TB	VirtualSynology	Attached	
SYNOLOGY iSCSI Disk (naa.60014053920ea5...)		disk	3.97 TB	Synology-Main	Attached	

If there isn't already a datastore on the device, you can format it by right-clicking on one of the hosts and selecting storage and then New Datastore. You can then choose to format it with VMFS. Likewise, if you are mounting an NFS export or creating a vVol, you can use the same action.

New Datastore

1 Type
Type

Specify datastore type.

VMFS
Create a VMFS datastore on a disk/LUN.

NFS
Create an NFS datastore on an NFS share over the network.

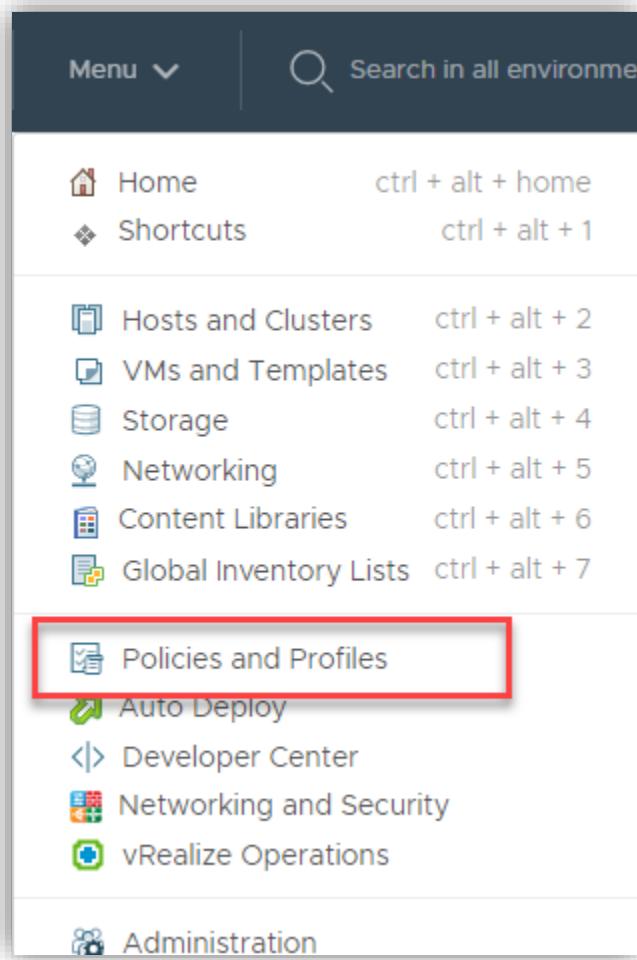
vVol
Create a Virtual Volumes datastore on a storage container connected to a storage provider.

2 Name and device selection
3 VMFS version
4 Partition configuration
5 Ready to complete

You will need to supply a name for the datastore and select what device will back it. Then, if VMFS, select if you want to use VMFS 6 or 5. Some of the reasons you would want to choose VMFS 6 would be automatic space reclamation or if you are using 4Kn storage devices.

Storage policies enable an administrator to make it simpler to choose storage when creating or moving VMs. You can specify characteristics or even resilience types if using vSAN.

1. To create a storage policy, click on the Menu drop-down at the top of your HTML5 client and choose Policies and Profiles



2. Click on VM Storage Policies

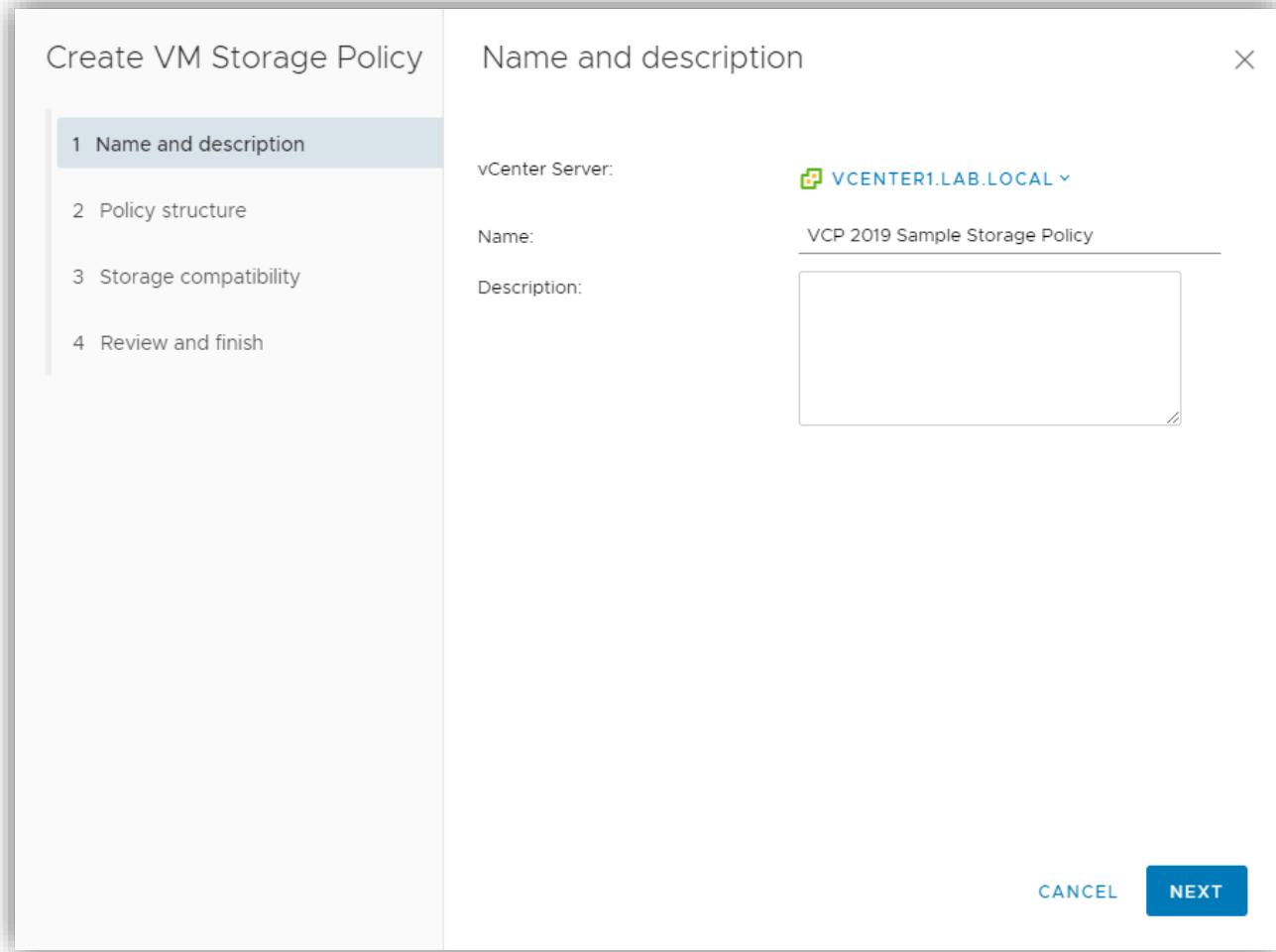
The screenshot shows the vSphere Web Client interface. On the left, there is a sidebar titled "Policies and Profiles" with the following options:

- VM Customization Specifications
- VM Storage Policies** (selected)
- Host Profiles
- Storage Policy Components

The main pane is titled "VM Storage Policies" and contains a list of existing policies:

- Create VM Storage Policy
- Name
- Bronze
- Gold
- Host-local PMem Default Storage Policy
- Silver
- VM Encryption Policy
- vSAN Default Storage Policy
- VVol No Requirements Policy

3. Select Create VM Storage Policy and on the popup wizard, give it a name.



4. This screen allows you to choose between Host-Based Services or Datastore Specific rules. Host-based are specific services that a particular host may provide, such as caching, encryption, etc. These can be used in conjunction with Datastore specific rules, which are directed to specific datastores. I tag a specific datastore as "Gold" storage and create a Storage policy that requires

a VM to use "Gold" storage. I am going to use the tag-based placement option.

The screenshot shows the 'Create VM Storage Policy' wizard. The left sidebar lists steps 1 through 5. Step 2, 'Policy structure', is selected and highlighted in blue. The main content area is titled 'Policy structure' and contains two sections: 'Host based services' and 'Datastore specific rules'. Under 'Host based services', there is an unchecked checkbox for 'Enable host based rules'. Under 'Datastore specific rules', there are two checkboxes: one for 'Enable rules for "vSAN" storage' (unchecked) and one for 'Enable tag based placement rules' (checked). At the bottom right are buttons for 'CANCEL', 'BACK', and 'NEXT'.

Create VM Storage Policy

1 Name and description

2 Policy structure

3 Tag based placement

4 Storage compatibility

5 Review and finish

Policy structure

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

Enable rules for "vSAN" storage

Enable tag based placement rules

CANCEL BACK NEXT

5. I have already created a Tag category called Storage Type, and I will tell it to Use storage tagged with the "Gold" tag. I could tell it not to use that tag as well. Multiple Rules can be used at the

same time.

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 Tag based placement**
- 4 Storage compatibility
- 5 Review and finish

Tag based placement

Add tag rules to filter datastores to be used for placement of VMs.

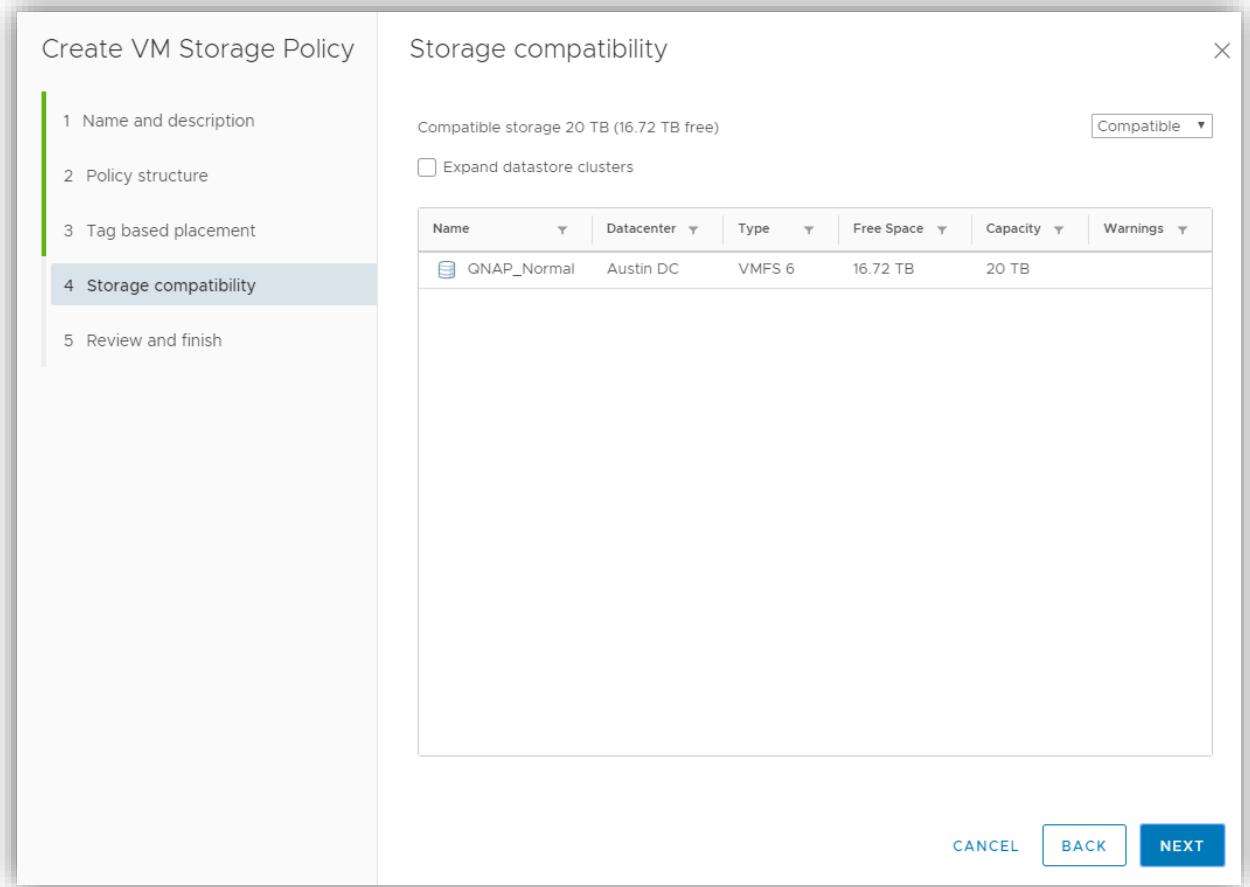
Rule 1 REMOVE

Tag category	Storage Type
Usage option	Use storage tagged with
Tags	Gold X BROWSE TAGS

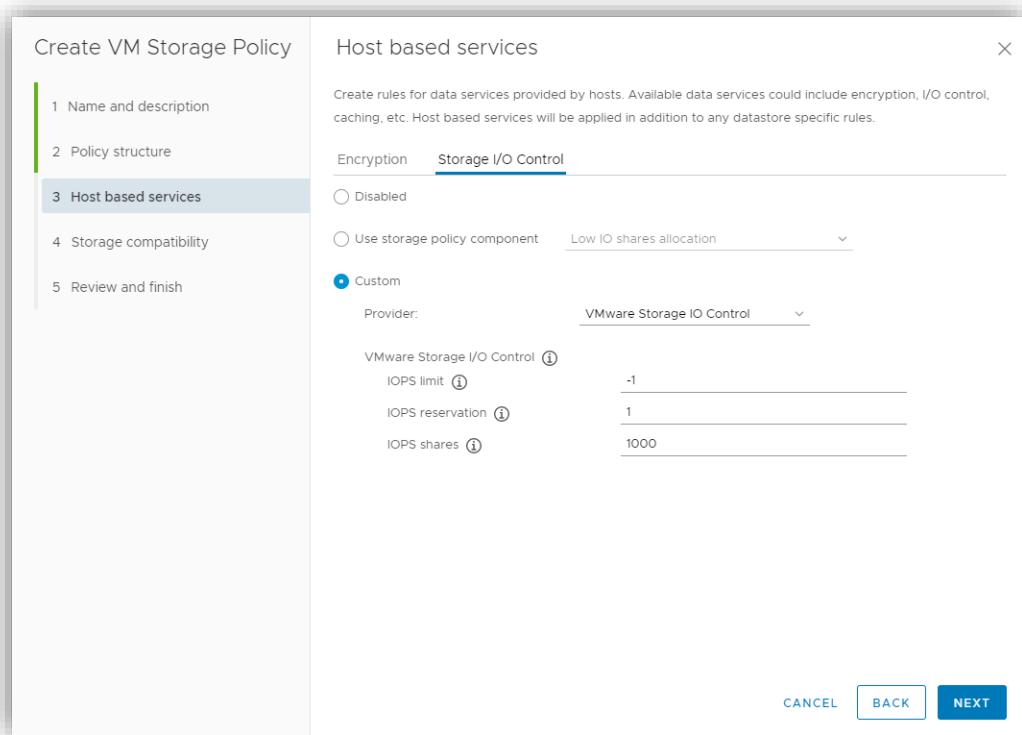
[ADD TAG RULE](#)

[CANCEL](#) [BACK](#) **NEXT**

6. I have one Datastore tagged as "Gold" Storage.



7. That's it. Click Finish, and you have created a Storage Policy. Just to show you what host-based services might look like, here is a screenshot



Objective 7.4.1 – Configure and modify datastores (expand/upgrade existing datastore, etc.)

Datastores are logical storage units that can use disk space on one disk or span several. You can navigate to the Datastores tab on the navigation pane to manage them and select the datastore you want to manage. Then click on Configure on the object pane in the middle.

Name	Value
Total Capacity	20 TB
Provisioned Space	6.91 TB
Free Space	16.91 TB

From this screen, you can increase the capacity. Enable SIOC, and edit Space Reclamation priority. Using the Connectivity and Multipathing, you can edit what hosts have access to this datastore. You can also see what files and VMs are on this datastore. You can perform essential file functions through this as well.

The screenshot shows the vSphere Datastore Management interface for a datastore named 'FreeNas_dS'. The 'Files' tab is selected. The left sidebar lists various folders and files within the datastore. The right panel displays a detailed list of files with columns for Name, Size, Modified, Type, and Path. A toolbar at the top provides actions like New Folder, Upload Files, Register VM..., Copy to, Move to, and Rename to. A search bar is also present.

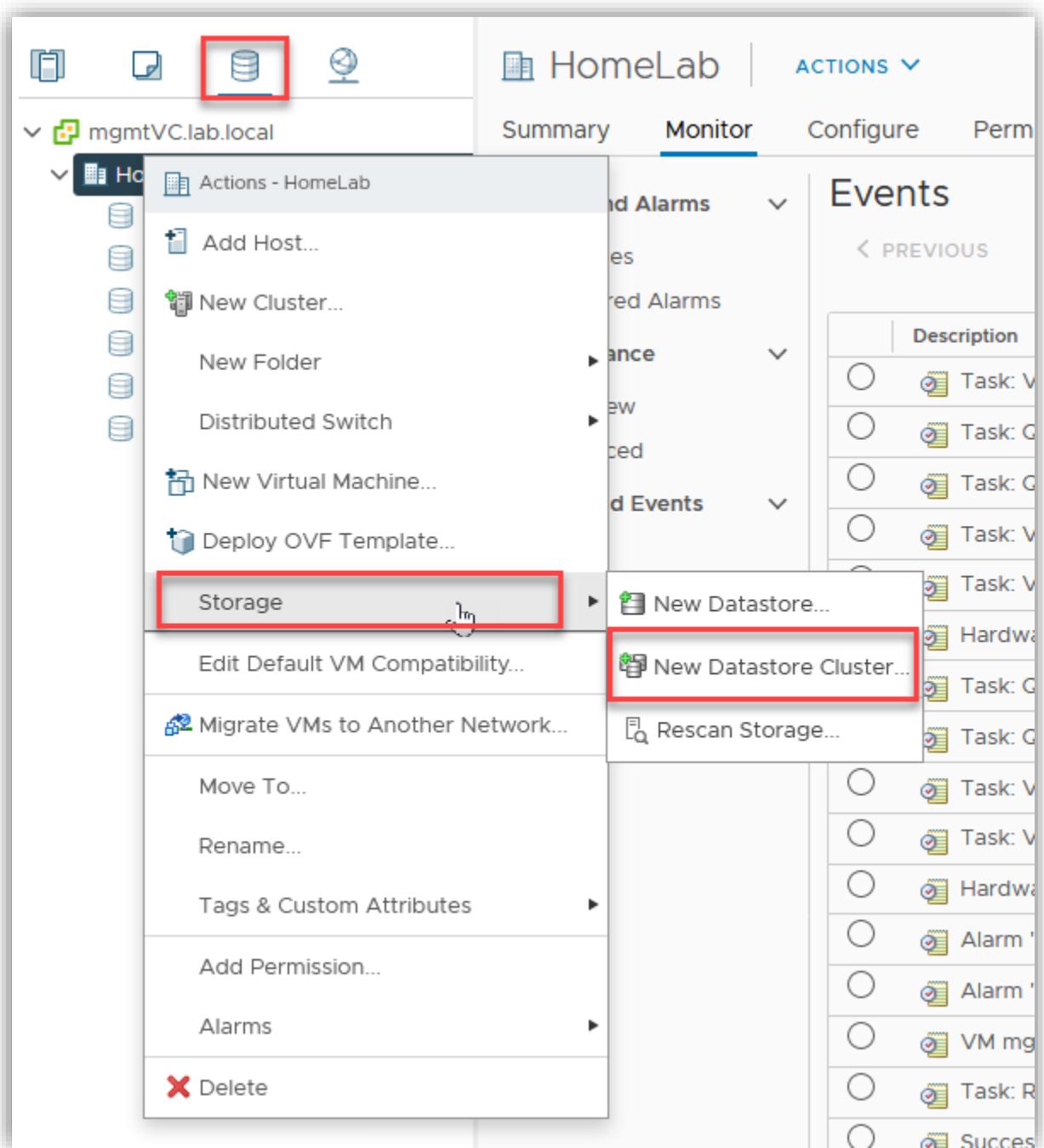
Name	Size	Modified	Type	Path
.dvsData		10/18/2020, 6:16:06 PM	Folder	[FreeNas_dS].dvsData
.sdd.sf		10/18/2020, 6:13:19 PM	Folder	[FreeNas_dS].sdd.sf
.vSphere-HA		10/23/2020, 1:48:56 PM	Folder	[FreeNas_dS].vSphere-HA
DC01.Lab.local		10/24/2020, 7:14:03 PM	Folder	[FreeNas_dS] DC01.Lab.local
ISO		10/23/2020, 2:19:53 PM	Folder	[FreeNas_dS] ISO
mgmtVC		10/24/2020, 6:59:57 PM	Folder	[FreeNas_dS] mgmtVC
Nutanix Install Test		10/23/2020, 2:45:53 PM	Folder	[FreeNas_dS] Nutanix Install Test
Nutanix_CE_Template		10/18/2020, 7:07:45 PM	Folder	[FreeNas_dS] Nutanix_CE_Template
VCF-CB-01a		10/24/2020, 11:21:34 PM	Folder	[FreeNas_dS] VCF-CB-01a
VCF-esxi-1		10/24/2020, 11:30:10 PM	Folder	[FreeNas_dS] VCF-esxi-1
VCF-esxi-2		10/24/2020, 12:01:44 PM	Folder	[FreeNas_dS] VCF-esxi-2
VCF-esxi-3		10/24/2020, 12:02:17 PM	Folder	[FreeNas_dS] VCF-esxi-3
VCF-esxi-4		10/24/2020, 12:02:52 PM	Folder	[FreeNas_dS] VCF-esxi-4
vCLS (8)		10/23/2020, 2:46:33 PM	Folder	[FreeNas_dS] vCLS (8)
vCLS (9)		10/23/2020, 2:46:30 PM	Folder	[FreeNas_dS] vCLS (9)
VMware-vRealize-Log-Insight-8...		10/24/2020, 4:35:24 PM	Folder	[FreeNas_dS] VMware-vRealize-Log-Insight-8...
vRealize-Operations-Manager		10/24/2020, 4:36:11 PM	Folder	[FreeNas_dS] vRealize-Operations-Manager
vsim-NetAppDOT-simulate		10/23/2020, 2:45:56 PM	Folder	[FreeNas_dS] vsim-NetAppDOT-simulate
xray		10/18/2020, 6:16:04 PM	Folder	[FreeNas_dS] xray

Objective 7.4.2 – Create virtual machine storage policies

Check objective 7.4 for the creation of virtual machine storage policies.

Objective 7.4.3 – Configure storage cluster options

To create a storage cluster, right-click on the datacenter under the datastore tab and click on storage > New Datastore Cluster.



You then need to go through a wizard to configure the storage cluster options. First, give it a name, and select if you want to turn on Storage DRS. This will allow you to manage all the datastore inside as one aggregate pool of storage. It will also suggest placement or move VMs as needed, depending on what automation level you have set up.

New Datastore Cluster

✓ **1 Name and Location**

2 Storage DRS Automation

3 Storage DRS Runtime Se...

4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Name and Location

Datastore cluster name: **VCP 2020 Cluster**

Location  HomeLab

Turn ON Storage DRS

vSphere Storage DRS enables vCenter Server to manage datastores as an aggregate pool of storage resources.

vSphere Storage DRS also enables vCenter Server to manage the assignment of virtual machines to datastores, suggesting placement when virtual machines are created, migrated or cloned, and migrating running virtual machines to balance load and enforce placement rules.

CANCEL

BACK

NEXT

The next screen gives you options to configure for SDRS. You can check on the 'I' at the end of each for more information about that setting.

New Datastore Cluster

✓ 1 Name and Location

✓ 2 Storage DRS Automation

3 Storage DRS Runtime Se...

4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Storage DRS Automation

Cluster automation level

No Automation (Manual Mode)

vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.

Fully Automated

Files will be migrated automatically to optimize resource usage.

Space balance automation level

Use cluster settings (i)

I/O balance automation level

Use cluster settings (i)

Rule enforcement automation level

Use cluster settings (i)

Policy enforcement automation level

Use cluster settings (i)

VM evacuation automation level

Use cluster settings (i)

CANCEL

BACK

NEXT

The next screen allows you to configure latency threshold settings to start moving VMs if experienced.

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Se... **(Current Step)**
- 4 Select Clusters and Hosts
- 5 Select Datastores
- 6 Ready to Complete

Storage DRS Runtime Settings

I/O Metric inclusion

Enable I/O metric for SDRS recommendations

Select this option if you want I/O metrics considered as a part of any SDRS recommendations or automated migrations in this data store cluster

I/O latency threshold

Dictates the minimum I/O latency for each datastore below which I/O load balancing moves are not considered.

5 ms  100 ms ms

Space threshold

Runtime thresholds govern when Storage DRS performs or recommends migrations (based on the selected automation level).

Utilized space

50 %  100 % %

Dictates the minimum level of consumed space for each datastore that is the threshold for action.

Minimum free space GB

Dictates the minimum level of free space for each datastore that is the threshold for action.

CANCEL

BACK

NEXT

Next, you select clusters that will be given access to the Storage Cluster (or hosts)

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Se...

4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Select Clusters and Hosts

Filter Selected (0)

[Clusters](#) [Standalone Hosts](#)

Filter

<input type="checkbox"/> Name ↑	Available CPU	Available Memory	Avai
<input type="checkbox"/> LAB	139.1 GHz	407.92 GB	27,7
<input type="checkbox"/> Mgmt Cluster	76.53 GHz	476.44 GB	14,E

2 items

CANCEL

BACK

NEXT

Next, add the datastores that will be in the storage cluster.

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Se...
- ✓ 4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Select Datastores

Show datastores connected to all hosts

Filter Selected (0)

<input type="checkbox"/> Name ↑	Host Connection Status	Capacity	Free
<input type="checkbox"/> FreeNas_dS	✓ All Hosts Connected	20 TB	16.9
<input type="checkbox"/> Synology-Main	✓ All Hosts Connected	3.97 TB	3.8

CANCEL

BACK

NEXT

Check over the summary and then finish.

New Datastore Cluster

- ✓ 1 Name and Location
- ✓ 2 Storage DRS Automation
- ✓ 3 Storage DRS Runtime Se...
- ✓ 4 Select Clusters and Hosts
- ✓ 5 Select Datastores
- 6 Ready to Complete**

Storage DRS: Enabled

Storage DRS Automation

Cluster automation level:	Fully Automated
Space balance automation level:	Use cluster settings
I/O balance automation level:	Use cluster settings
Rule enforcement automation level:	Use cluster settings
Policy enforcement automation level:	Use cluster settings
VM evacuation automation level:	Use cluster settings

Storage DRS Runtime Settings

Storage I/O load balancing:	Enabled
Space threshold:	80 % utilized space per datastore
I/O latency threshold:	15 ms

Datastores

Name	Capacity	Free Space	Type
Synology-Main	3.97 TB	3.8 TB	VMFS 6

Clusters and Hosts

Name	Datastore Connection ...	Selected	I/O Load Balance Capa...
LAB	<input checked="" type="checkbox"/> All Datastores ...	Yes	<input checked="" type="checkbox"/> Yes

CANCEL

BACK

FINISH

If you need to configure the cluster afterward, you can click on the cluster and select the middle panes configure.

vSphere Storage DRS is Turned ON

Storage DRS automation

- Cluster automation level: Fully Automated
- Space balance automation level: Use cluster settings
- I/O balance automation level: Use cluster settings
- Rule enforcement automation level: Use cluster settings
- Policy enforcement automation level: Use cluster settings
- VM evacuation automation level: Use cluster settings
- Space threshold: 80 % utilized space per datastore

I/O metrics

- I/O metric inclusion: I/O metrics for Storage DRS recommendations are enabled.
- I/O latency threshold: 15 ms

Advanced options

- Default VM affinity: Keep VMDKs together by default
- Check imbalances every: 8 Hours
- I/O imbalance threshold: 5
- Minimum space utilization difference: 5 %

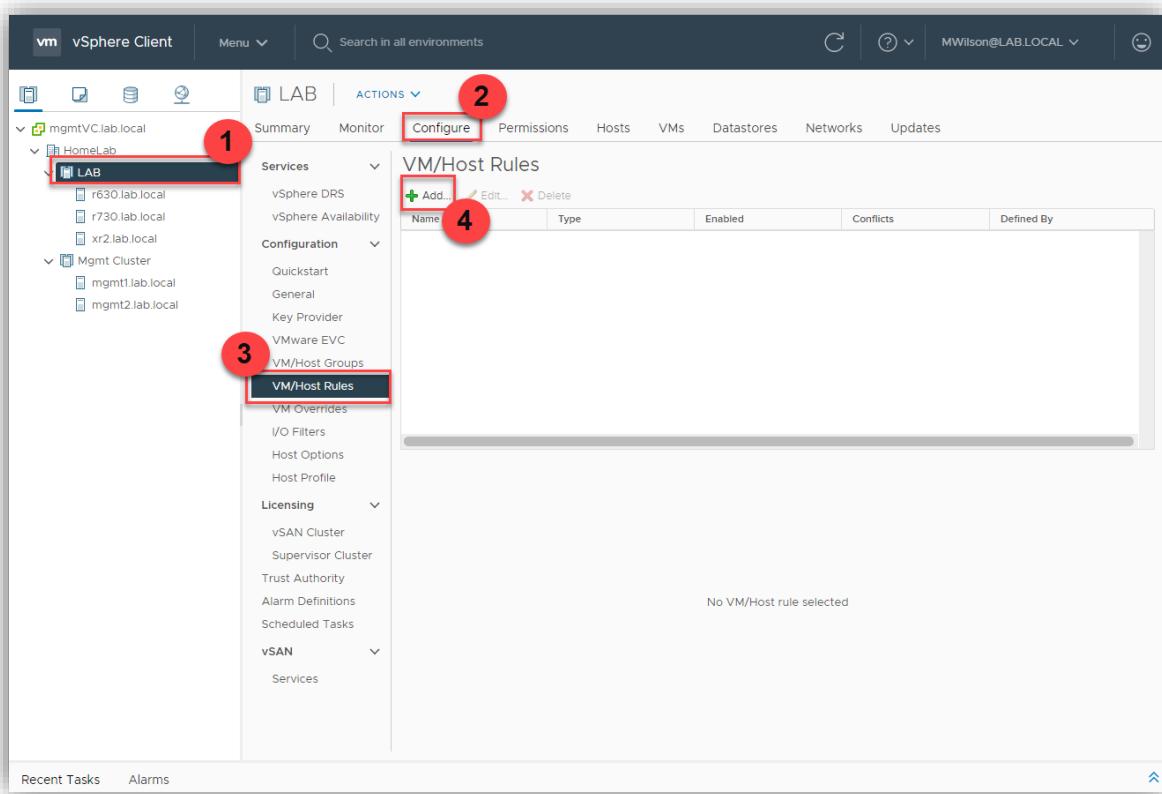
Option	Value
No items to display	

Objective 7.5 – Create Distributed Resource Scheduler (DRS) affinity and anti-affinity rules for everyday use cases

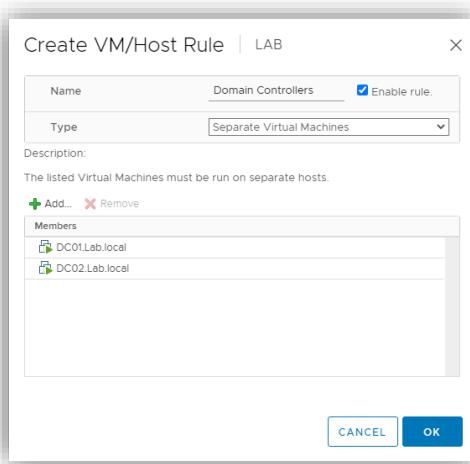
Some everyday use cases for affinity and anti-affinity rules will be if a VM needs to stay on a specific host due to a specific hardware key or license restriction. Another would be if you have multiple domain controllers for resilience, you wouldn't want a scenario where both of them would be on the same physical host. This would be an example of a VM-VM anti-affinity rule. Another might be if you have a multi-tiered app that needs to be kept together on the same host for some reason. That would be a VM-Host affinity rule.

These rules are set up under the cluster configuration under VM/Host Groups and VM/Host Rules. There are two pieces to setup. You have to either make a VM group or Host group depending on which type of rule you want to use. I will take the Active Directory use case and create a VM to VM anti-affinity rule. First, I need to define the VMs.

Cluster > Configure > VM/Host Rules > Add



Give it a name and then choose the type "Separate Virtual Machines." Next, select both the VMs that will be in this group.



When finished, it will look like this.

The screenshot shows the vSphere Web Client interface for a cluster named "LAB". The "Configure" tab is selected. In the left sidebar, under "VM/Host Rules", the "VM/Host Rules" option is highlighted. The main content area displays a table titled "VM/Host Rules" with one entry:

Name	Type	Enabled	Conflicts	Defined By
Domain Controllers	Separate Virtual Machi...	Yes	0	User

Below this, the "VM/Host Rule Details" section shows two hosts listed under "Rule Members":

Rule Members	Conflicts
DC02.Lab.local	0
DC01.Lab.local	0

The "Conflicts" panel on the right is currently empty.

Notice the rule is enabled, and there are no conflicts. That's all there is to it!

Objective 7.6 – Configure and perform different types of migrations

We've already covered the type of migrations that are possible. Let's now go over how to perform them. There are several ways to initiate the migration. You can drag the VM over to the host or datastore you want to put it on. How would you do that? If you are in either the hosts and cluster or datastore section, you can click on the VMs tab. (like in the example picture)

The screenshot shows the vSphere Client interface. On the left, there's a navigation bar with icons for Home, Hosts & Clusters, Datastores, VMs (which is highlighted with a red box), and Network. Below this is a tree view under 'mgmtVC.lab.local' showing various datastores: FreeNas_dS, R730_Local SSD_DS1, Synology-Main, VirtualSynology, vsanDatastore, and XR2_Local_NVMe_SSD. In the center, the 'HomeLab' cluster is selected. At the top right, there are tabs for Summary, Monitor, Configure, Permissions, Hosts & Clusters, and Datastores. Below these are four sub-tabs: Virtual Machines (selected and highlighted with a red box), VM Templates, vApps, and VM Folders. The main area displays a table of virtual machines:

Name	State	Status	Provisioned Space
2016 Server Template	Powered Off	Normal	108.61 GB
DC01.lab.local	Powered On	Normal	152.31 GB
DC02.lab.local	Powered On	Normal	208.1 GB
Element 12 - 2	Powered Off	Normal	256.59 GB
Grafana Windows	Powered Off	Normal	84.61 GB
GrafanaLinux	Powered Off	Normal	110.99 GB
Linux_Template_CentOS7	Powered Off	Normal	40.61 GB
mgmtVC	Powered On	Normal	741.14 GB
Nutanix Install Test	Powered Off	Normal	1.41 TB
Nutanix_CE_Template	Powered Off	Normal	1.42 TB
SolidFire vVOL	Powered On	Normal	256.08 GB
Synology_DS3615xs_6.1.7	Powered On	Normal	7.09 TB
VCF-CB-01a	Powered On	Normal	154.08 GB

From there, click on one of the VMs or multiple and drag it where you want to migrate it to. It will then pop up the wizard to finish. You can also right-click on a VM and then select migrate. If you do the latter, you have to choose the type of migration. Next, you click where you want the VM to migrate to, either host or datastore. You also need to select the network to attach to and vMotion priority. That's all!

Migrate | DC01.Lab.local

✓ 1 Select a migration type

2 Select a compute resource

3 Select networks

4 Select vMotion priority

5 Ready to complete

Select a compute resource

VM origin ⓘ

Select a cluster, host, vApp or resource pool to run the virtual machines.

Hosts Clusters Resource Pools vApps

Filter

Name ↑	State	Status	Cluster	Consumed C
r630.lab.local	Connected	✓ Normal	LAB	1%
r730.lab.local	Connected	✓ Normal	LAB	2%
xr2.lab.local	Connected	✓ Normal	LAB	12%

3 items

Compatibility

CANCEL

BACK

NEXT

Migrate | DC01.Lab.local

- ✓ 1 Select a migration type
- ✓ 2 Select a compute resource

3 Select networks

4 Select vMotion priority
5 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM origin ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
DSwitch-VM Network	1 VMs / 1 Network adapters	DSwitch-VM Network

DSwitch-VM Network is in use at:

VM	Network Adapter	Network
DC01.Lab.local	Network adapter 1	DSwitch-VM Network

[ADVANCED >>](#)

Compatibility

- ✓ Compatibility checks succeeded.

[CANCEL](#) [BACK](#) [NEXT](#)

Migrate | DC01.Lab.local

✓ 1 Select a migration type

✓ 2 Select a compute resource

✓ 3 Select networks

4 Select vMotion priority

5 Ready to complete

Select vMotion priority

Protect the performance of your running virtual machines by prioritizing the allocation of CPU resources.

VM origin ⓘ

Schedule vMotion with high priority (recommended)

vMotion receives higher CPU scheduling preference relative to normal priority migrations. vMotion might complete more quickly.

Schedule normal vMotion

vMotion receives lower CPU scheduling preference relative to high priority migrations. You can extend vMotion duration.

CANCEL

BACK

NEXT

Migrate | DC01.Lab.local

- ✓ 1 Select a migration type
- ✓ 2 Select a compute resource
- ✓ 3 Select networks
- ✓ 4 Select vMotion priority

5 Ready to complete

Ready to complete

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

VM origin ⓘ

Migration Type	Change compute resource. Leave VM on the original storage
Virtual Machine	DC01.Lab.local
Cluster	LAB
Host	r630.lab.local
vMotion Priority	High
Networks	No network reassignments

CANCEL

BACK

FINISH

"Objective 7.7 – Configure role-based user management

We've covered what roles are already, but a short refresher is that a role is just a container for a group of privileges. Each object in the vSphere world has permissions associated with it. This is how you control who can do what. You assign a user a role, and that allows them to have specific privileges and do tasks.

vCenter has built-in system roles that cannot be changed. However, they CAN be cloned, and you can modify the clone to have more or fewer privileges. To find those roles, Click on Menu > Administration > Access Control > Roles. If you click on a role and then click on privileges, you can see what each role can do. Choose the one with the least amount of privileges needed for the task and then clone that.

The screenshot shows the vSphere Client interface with the 'Access Control' section selected in the navigation bar. The main pane displays a list of roles, each with a red box highlighting it. The roles listed include:

- Administrator
- Read-only
- No access
- AppdApplianceUser
- AutoUpdateUser
- Content library administrator (sample)
- Content Library Registry administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- No cryptography administrator
- No Trusted Infrastructure administrator
- NSX Administrator
- NSX Auditor
- NSX VI Administrator
- Resource pool administrator (sample)
- SupervisorService Cluster Operator
- SupervisorService Operator
- SupervisorService RootFolder Operator
- SyncUsers
- Tagging Admin
- Trusted Infrastructure administrator
- Virtual Machine console user
- Virtual machine power user (sample)
- Virtual machine user (sample)

Below the role list, there are sections for Alarms, Permissions, AutoDeploy, and Certificates, each with a list of items. The entire list of roles is enclosed in a red box.

To clone, click on the role you want to use; for example, I chose Virtual Machine User. Then you can click on the clone. You can just create a new role if you know all the privileges needed for that role.

The screenshot shows the vSphere Client interface with the 'Roles' section selected in the navigation menu. The main pane displays a list of roles, with 'Virtual machine user (sample)' highlighted and surrounded by a red box. A second red box highlights the '+' icon at the top left of the list. The right side of the screen shows tabs for 'DESCRIPTION', 'USAGE', and 'PRIVILEGES'.

Roles provider: VS SPHERE.LOCAL

DESCRIPTION USAGE PRIVILEGES

Global

- Cancel task

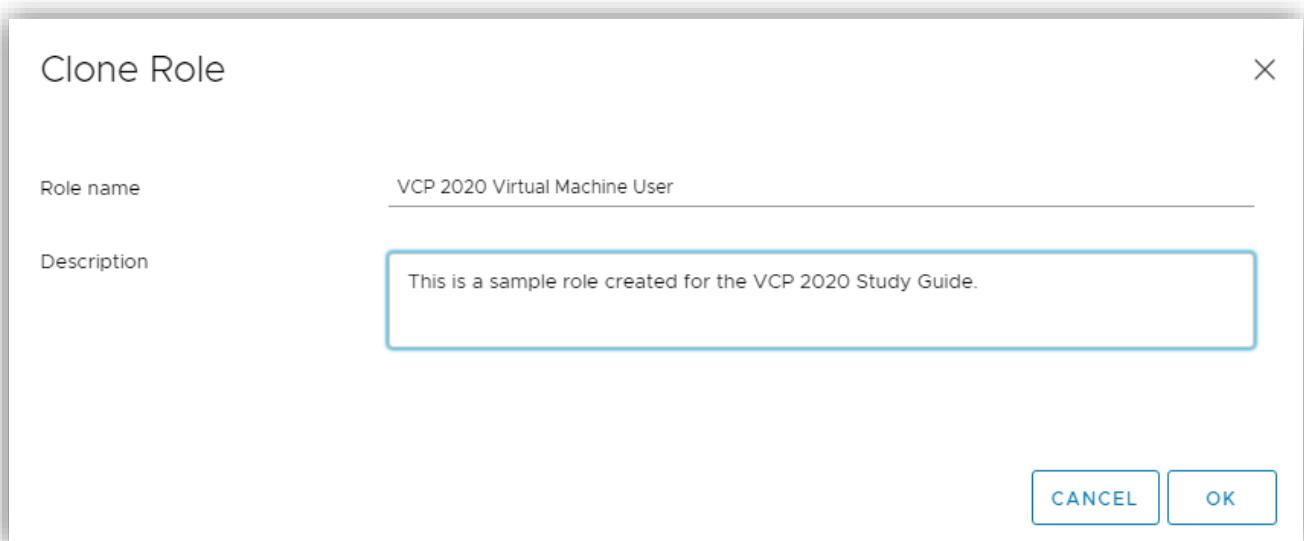
Scheduled task

- Create tasks
- Modify task
- Remove task
- Run task

Virtual machine

- Interaction
 - Answer question
 - Configure CD media
 - Configure floppy media
 - Connect devices
 - Console interaction
 - Install VMware Tools
 - Power off
 - Power on
 - Reset
 - Suspend

When you click clone, the Clone Role window comes up and asks you to give it a name and optionally a description.



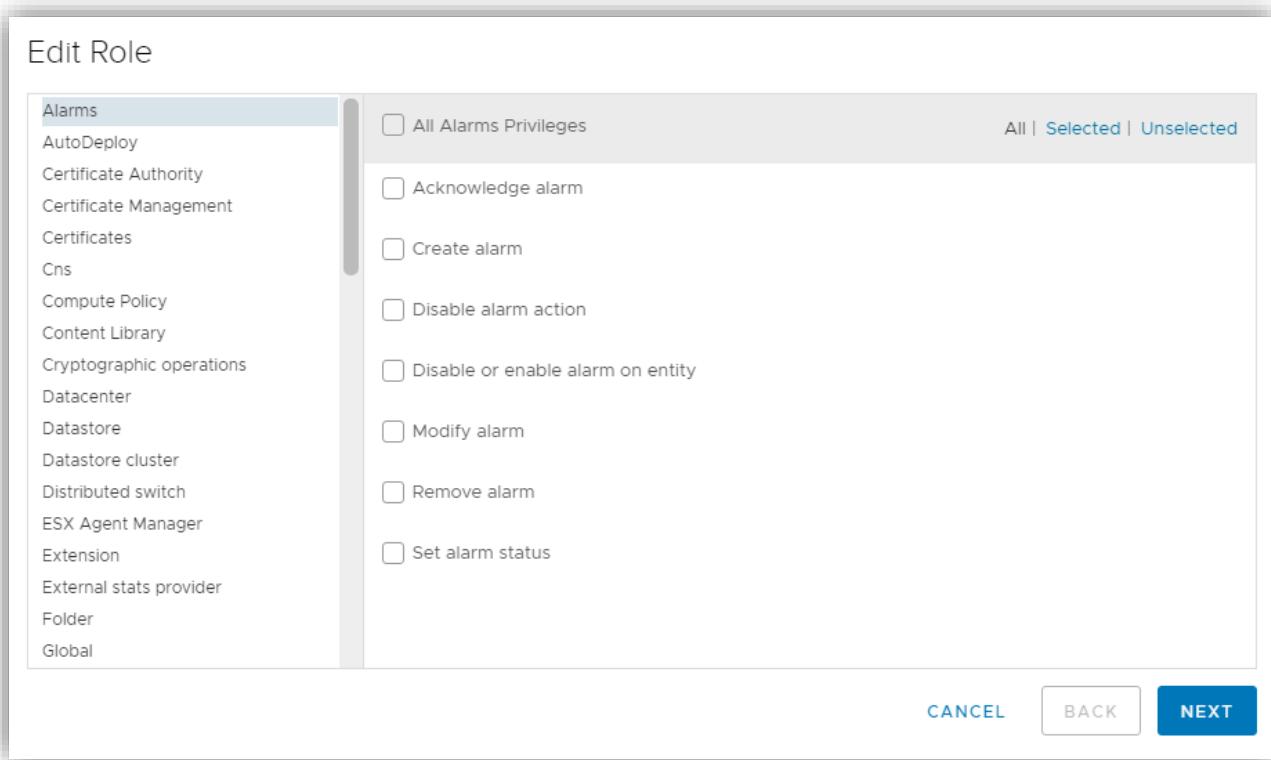
Click, OK, and your role has been created. We now need to modify it to add permissions, however. So, we select the role and then click on the pencil icon.

The screenshot shows the vSphere Client interface with the title bar "vm vSphere Client". The left sidebar menu is open, showing the "Roles" option under "Access Control" is selected. The main pane is titled "Roles" and shows a list of roles. A red box highlights the "Edit" icon (pencil) next to the "VCP 2020 Virtual Machine User" role, which is also highlighted with a red box. The list includes:

- No cryptography administrator
- No Trusted Infrastructure administrator
- NSX Administrator
- NSX Auditor
- NSX VI Administrator
- Resource pool administrator (sample)
- SupervisorService Cluster Operator
- SupervisorService Operator
- SupervisorService RootFolder Operator
- SyncUsers
- Tagging Admin
- Trusted Infrastructure administrator
- VCP 2020 Virtual Machine User** (highlighted with a red box)
- Virtual Machine console user
- Virtual machine power user (sample)
- Virtual machine user (sample)

On the right side, there are three tabs: DESCRIPTION, USAGE, and PRIVILEGES. Below the tabs, there are sections for Global, Scheduled task, and Virtual machine, each listing specific permissions.

We are now given a plethora of options to edit the role.



After adding the privileges, we then click on next and then finish. If we need to, we can give a user role access to a specific object. To do that, navigate to the object. Then click on the permissions tab.

User/Group	Role	Defined In
VSPPHERE.LOCAL\Administrator	Administrator	mgmtVC.lab.local
VSPPHERE.LOCAL\Administrators	Administrator	Global Permission
VSPPHERE.LOCAL\AutoUpdate	AutoUpdateUser	Global Permission
VSPPHERE.LOCAL\NsxAdministrators	NsxAdministrator	Global Permission
VSPPHERE.LOCAL\NsxAuditors	NsxAuditor	Global Permission
VSPPHERE.LOCAL\NsxVIAAdministrators	NsxVIAdministrator	Global Permission
VSPPHERE.LOCAL\RegistryAdministrators	Content Library Registry administrator (sample)	Global Permission
VSPPHERE.LOCAL\SyncUsers	SyncUsers	Global Permission
VSPPHERE.LOCAL\TrustedAdmins	Trusted Infrastructure administrator	Global Permission
VSPPHERE.LOCAL\vpd-0b94dc3f-c6ee-430c-86a8-6c9346...	Administrator	Global Permission
VSPPHERE.LOCAL\vpd-extension-0b94dc3f-c6ee-430c-86a8...	Administrator	Global Permission
VSPPHERE.LOCAL\vsphere-webclient-0b94dc3f-c6ee-430c-8...	vSphere Client Solution User	Global Permission
VSPPHERE.LOCAL\vsphereClientSolutionUsers	vSphere Client Solution User	Global Permission
VSPPHERE.LOCAL\WorkloadStorage	WorkloadStorageManagement	Global Permission

Then click on the plus icon and add in the user and choose the role you want them to have.

Add Permission

DC01.Lab.local



Domain

LAB.LOCAL



User/Group

MWilson

Role

VCP 2020 Virtual Machine User



Propagate to children

CANCEL

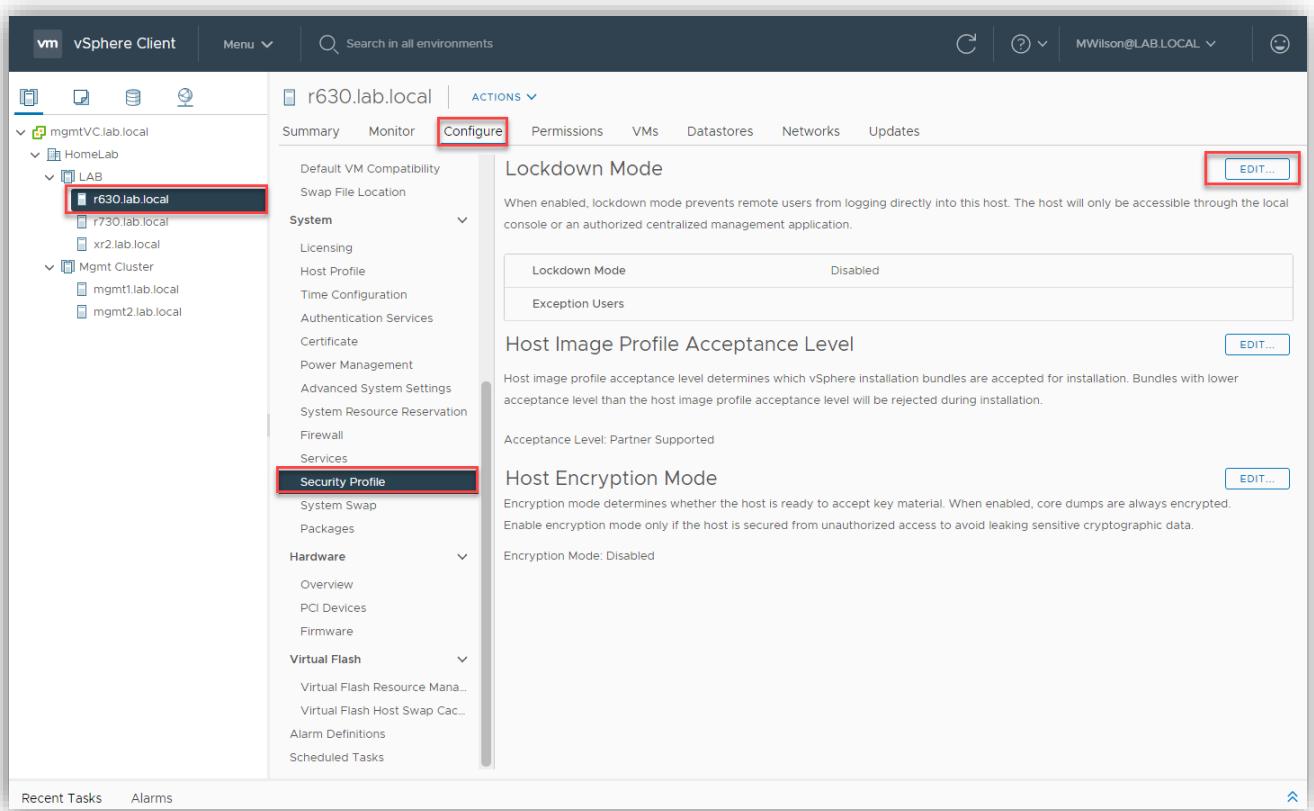
OK

Click OK, and that user should have access to that specific object now.

'Objective 7.8 – Configure and manage the options for securing a vSphere environment (certificates, virtual machine encryption, virtual Trusted Platform Module, lockdown mode, virtualization-based security, etc.)

There are many options for securing your vSphere environment. We will now show you where to find those and how to enable them.

We'll start with host lockdown mode. If enabled, lockdown mode prevents users from logging directly into the host itself. There are multiple levels of lockdown. Normal allows access through either the local console (in front of the machine) or vCenter Server. Strict locks down the host so that it can only be accessed through vCenter Server. To enable one of those modes, navigate to the host in Clusters and Hosts. Then select Configure, then Security Profile.



Once there, click "Edit."

r630.lab.local - Lockdown Mode

Lockdown Mode

Exception Users

Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly to this host.

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

Specify host lockdown mode:

Disabled

Lockdown mode is disabled.

Normal

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

Strict

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

CANCEL

OK

There are your options. You also have the option to select exception users. You will need to click on that on the left to enter them in.

r630.lab.local - Lockdown Mode

Lockdown Mode

Exception Users

Exception Users

A list of user accounts that keep their permissions when the host enters lockdown mode. The accounts are used by third-party solutions and external applications that must continue their function in lockdown mode. To keep lockdown mode uncompromised, you should add only user accounts that are associated with applications.

[ADD USER](#) [REMOVE USER](#)

User	⋮

0 items

[CANCEL](#)

[OK](#)

Exemptions should be made sparingly. Under the security profile, you also have the option for Host Encryption mode and Host Image Profile Acceptance Level. The latter prevents software from running if they don't have a certain acceptance level from VMware. The host encryption mode must be enabled to create Encrypted VMs or other encryption type tasks. It becomes enabled most of the time when performing a task, such as creating an encrypted VM.

To create an encrypted VM, you need to first have a Key Management Server, or KMS, in place. Once you do, you can go to the VM settings and then VM Options to perform encryption tasks.

Edit Settings | DC01.Lab.local

X

Virtual Hardware

VM Options

> General Options

VM Name: DC01.Lab.local

> VMware Remote Console Options

Lock the guest operating system when the last remote user disconnects

Encryption

Expand for encryption settings

Encrypt VM

Datastore Default

(Requires Key Management Server)

Encrypted vMotion

Opportunistic



> Power management

Expand for power management settings

> VMware Tools

Expand for VMware Tools settings

Virtualization Based Security

Enable

> Boot Options

Expand for boot options

> Advanced

Expand for advanced settings

> Fibre Channel NPIV

Expand for Fibre Channel NPIV settings

CANCEL

OK

You might also notice an option there for Virtualization Based Security. I can't use it on this VM because it requires Windows 10 or Server 2016+ OSs. You also need to enable

- UEFI firmware
- Secure Boot
- Hardware version 14
- IOMMU turned on

ESXi will then create a virtual TPM 2.0 and allow that to be installed and used in Windows just like a real Trusted Platform Module device. This can also be enabled on the VM during creation here.

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility

6 Select a guest OS

7 Customize hardware
8 Ready to complete

Select a guest OS

Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Windows

Guest OS Version: Microsoft Windows Server 2019 (64-bit)

Enable Windows Virtualization Based Security (i)

Compatibility: ESXi 7.0 U1 and later (VM version 18)

CANCEL

BACK

NEXT

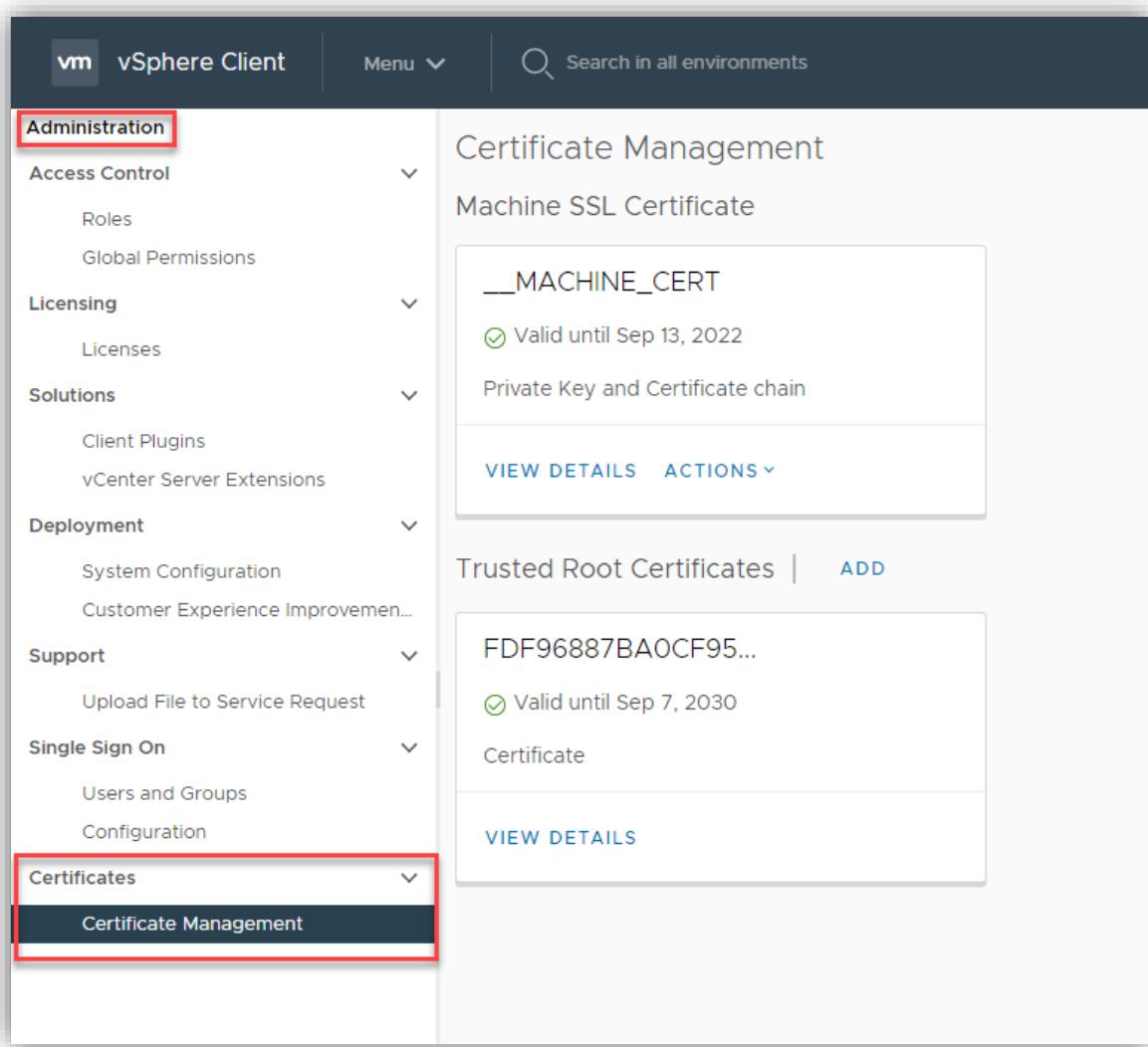
You can then see it enabled on the VM Options screen.

Edit Settings | VCP 2020 Encryption Test

Virtual Hardware VM Options

> General Options	VM Name: VCP 2020 Encryption Test
> VMware Remote Console Options	<input type="checkbox"/> Lock the guest operating system when the last remote user disconnects
> Encryption	Expand for encryption settings
> Power management	Expand for power management settings
> VMware Tools	Expand for VMware Tools settings
Virtualization Based Security	<input checked="" type="checkbox"/> Enable
Boot Options	
Firmware	EFI (recommended) 
Secure Boot	<input checked="" type="checkbox"/> Enabled 
Boot Delay	When powering on or resetting, delay boot order by 0 milliseconds.

The last subject we'll cover here is certificates. To get to certificates in the HTML5 web client, you click on Menu> Administration > Certificate Management

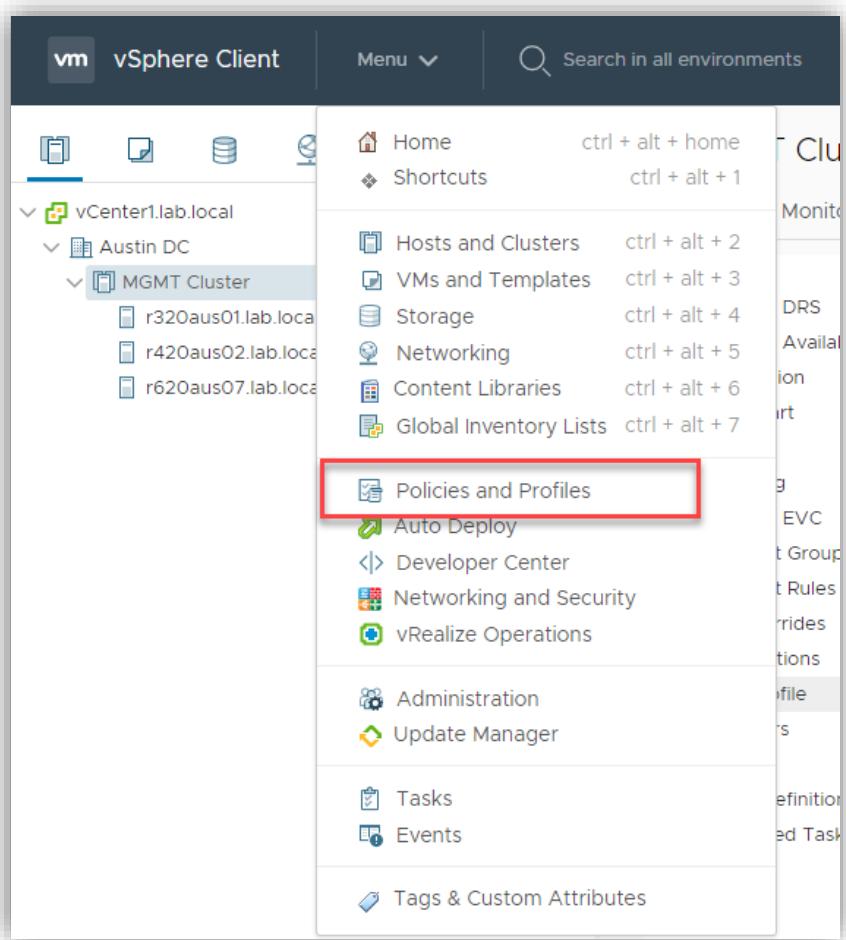


You can see two certificates there currently. We've already covered the different practices for certificates, so we just need to cover how to change them here. To add a new Trusted Root Certificate, just click on the Add and then tell vSphere where it is located. To replace the Machine certificate, click on Actions, and you can renew, import and replace, or generate a certificate signing request for a certificate authority. If you want to read more on that subject, head to VMware's site [here](#).

Objective 7.9 – Configure and manage host profiles

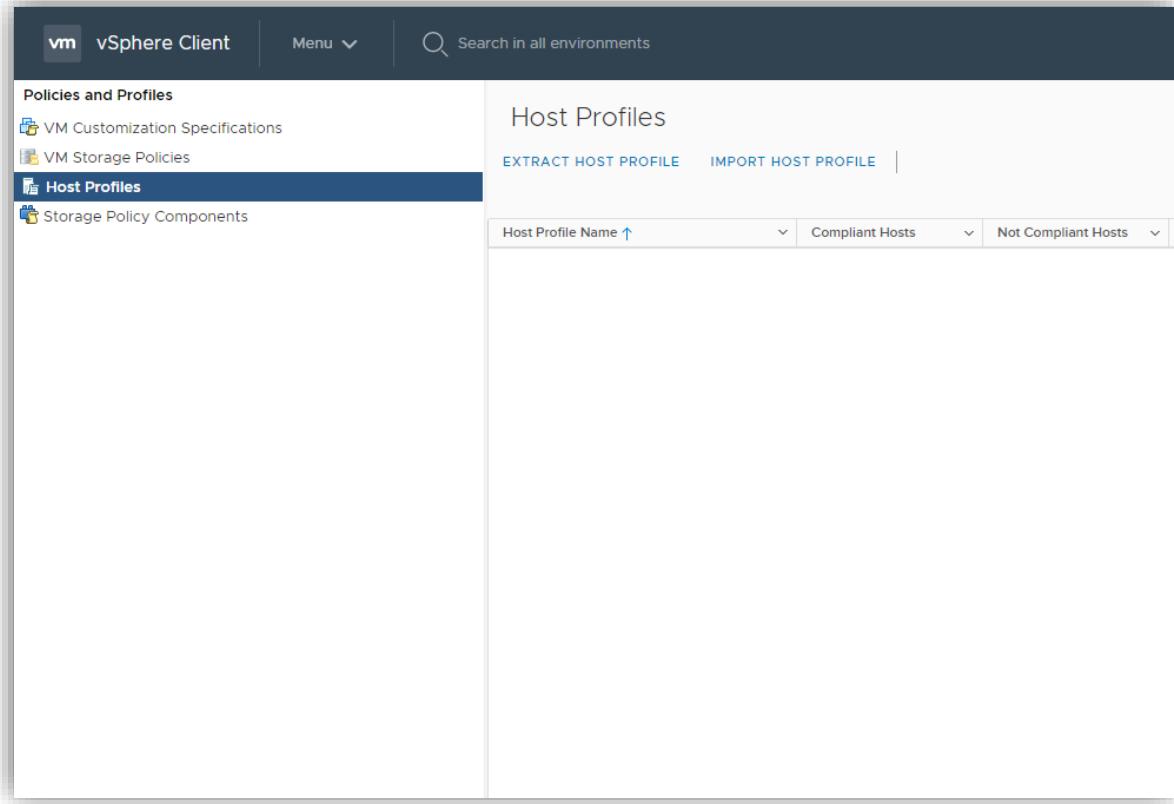
Host profiles provide a mechanism to automate and create a base template for your hosts. Using host profiles, you can create host uniformity. VMware will inform you if your host is not in compliance yet, and then you can take steps to remediate it.

It's accessed under Policies and Profiles



There is a process to it. Here it is:

8. Click on Host Profiles on the navigation pane on the left.



9. Next is extracting the original host profile. This is going to take a host you select and make that the baseline

The screenshot shows the vSphere Client interface with the title bar "vSphere Client". In the top navigation bar, there are tabs for "VM", "Policies and Profiles", "Menu", and a search bar. The "Policies and Profiles" tab is selected, and its sub-menu includes "VM Customization Specifications", "VM Storage Policies", "Host Profiles" (which is highlighted with a blue background), and "Storage Policy Components". On the right side of the screen, under the "Host Profiles" heading, there is a button labeled "EXTRACT HOST PROFILE" which is highlighted with a red box. Below this button is a table header with columns: "Host Profile Name ↑", "Compliant Hosts", and "Not Compliant Hosts". The table body is currently empty.

10. Select the host.

Extract Host Profile

1 Select host

2 Name and Description

Select host

Select a host to extract the profile settings

vCenter Server:  VCENTER1.LAB.LOCAL ▾

Name
<input type="radio"/> r620aus07.lab.local
<input type="radio"/> r320aus01.lab.local
<input type="radio"/> r420aus02.lab.local

3 items

CANCEL **NEXT**

11. Give it a name and a description, and then Finish

Extract Host Profile

1 Select host

2 Name and Description

Name and Description

X

Enter the name and description for the selected profile settings

Name: VCP 2020 Host Profile

Description:

CANCEL BACK FINISH

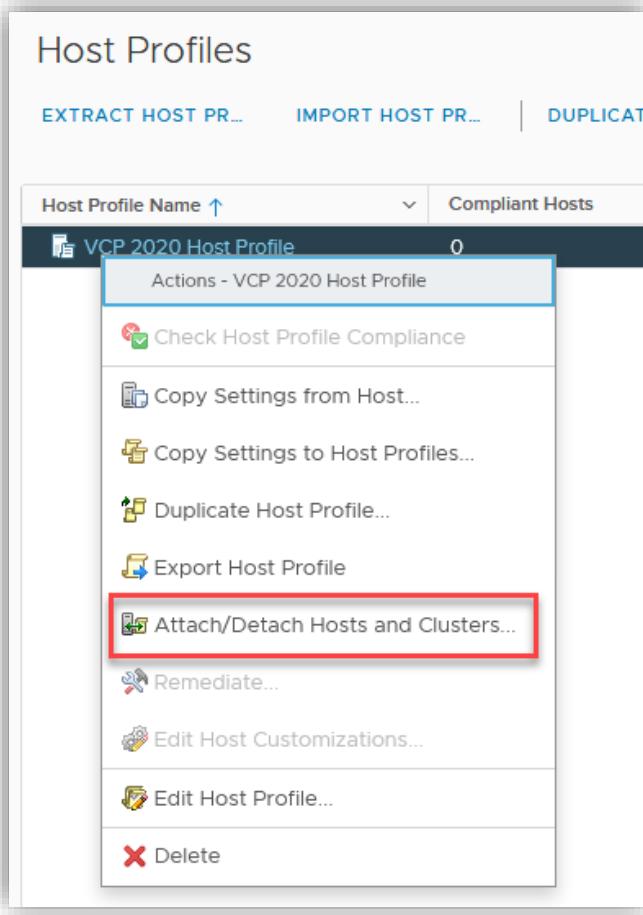
12. Once that is done, you now have a window that looks like this

The screenshot shows the vSphere Client interface with the title bar "vSphere Client". In the top left, there's a "vm" icon. The main navigation menu on the left lists "Policies and Profiles", "VM Customization Specifications", "VM Storage Policies", "Host Profiles" (which is selected and highlighted in blue), and "Storage Policy Components". The central pane is titled "Host Profiles" and contains two buttons: "EXTRACT HOST PROFILE" and "IMPORT HOST PROFILE". Below these buttons is a table with the following columns: "Host Profile Name", "Compliant Hosts", "Not Compliant Hosts", "Unknown State Hosts", "Last Edited", and "Hosts". A single row is visible, showing "VCP 2020 Host Profile" with values 0, 0, 0, 09/14/2020, 9:27:23 PM, and 0. There is also a "Filter" button at the top right of the table.

13. Yes, it's small. The point is when you click on the host profile, you now have additional options above. Notice as well that the profile is also a hyperlink. Click on it.

This screenshot shows the "VCP 2020 Host Profile" configuration screen. At the top, there's a breadcrumb trail: "vSphere Client" → "VCP 2020 Host Profile". The top navigation bar includes "Menu", "Search in all environments", and user information "MWilson@LAB.LOCAL". Below the search bar are three buttons: "EDIT HOST PROFILE...", "COPY SETTINGS...", and "HOSTS". The main content area has tabs: "Summary", "Monitor", "Configure" (which is selected and highlighted in blue), and "Hosts". On the left, there's a sidebar with "Clusters" and "Hosts" sections, each with a count of 0. A red arrow points from this sidebar to the text "Hosts and Clusters this profile is attached to". The main pane displays a list of configuration settings under the "Configure" tab, with "Advanced Configuration Settings" expanded. Other items listed include "General System Settings", "Networking configuration", "Other", "Security and Services", and "Storage configuration". A red arrow points from the "Edit Host Profile" button to the text "Click here to edit the profile". Another red arrow points from the "Copy Settings" button to the text "Copy settings from a host or another profile". A red arrow also points from the "Hosts" tab to the text "Configuration settings for the hosts". At the bottom right, it says "No item selected".

14. Right-click on the host profile and use the Actions menu to attach to hosts or clusters.



"Objective 7.10 – Utilize baselines to perform updates and upgrades

You can use baselines to update and upgrade hosts or clusters, or other objects. First, you will need a baseline. You can use one of the two default baselines that VMware has included for you, or you can create a new one. To create a new one, click on Menu and select Lifecycle Manager. Under Lifecycle Manager, go to the Baseline tab and then click New.

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected in the left sidebar. The main pane displays the 'Baselines' tab of the Lifecycle Manager. A red box highlights the 'Baselines' tab header and the 'NEW' button below it. Another red box highlights the 'Content' column header in the table. The table lists four baseline entries:

Baselines	Content	Type	ESXi version	Last Modified
7.0.1	Upgrade	Custom	7.0.0	1 week ago
Non-Critical Host Patches (Predefined)	Patch	Predefined	7.0, 7.*, 6.5.0, 7.0.1, 6.7.0, 7.0.1, 7.0.0, 6.*, 7.1	1 month ago
Critical Host Patches (Predefined)	Patch	Predefined	7.0, 6.5.0, 6.7.0	1 month ago
Host Security Patches (Predefined)	Patch	Predefined	7.0, 6.5.0, 6.7.0	1 month ago

At the bottom of the table, there are 'EXPORT' and '4 Baselines' buttons. The left sidebar also shows other management categories like 'Hosts and Clusters' and 'Policies and Profiles'.

Next, give it a name and optionally a description. Select what type of content it will contain. Upgrade, Patch, or Extension.

Create Baseline

X

1 Name and Description

2 Select ISO

3 Summary

Name and description

Enter a name and select the baseline type.

Name

VCP 2020 Upgrade

Description

Content

Upgrade

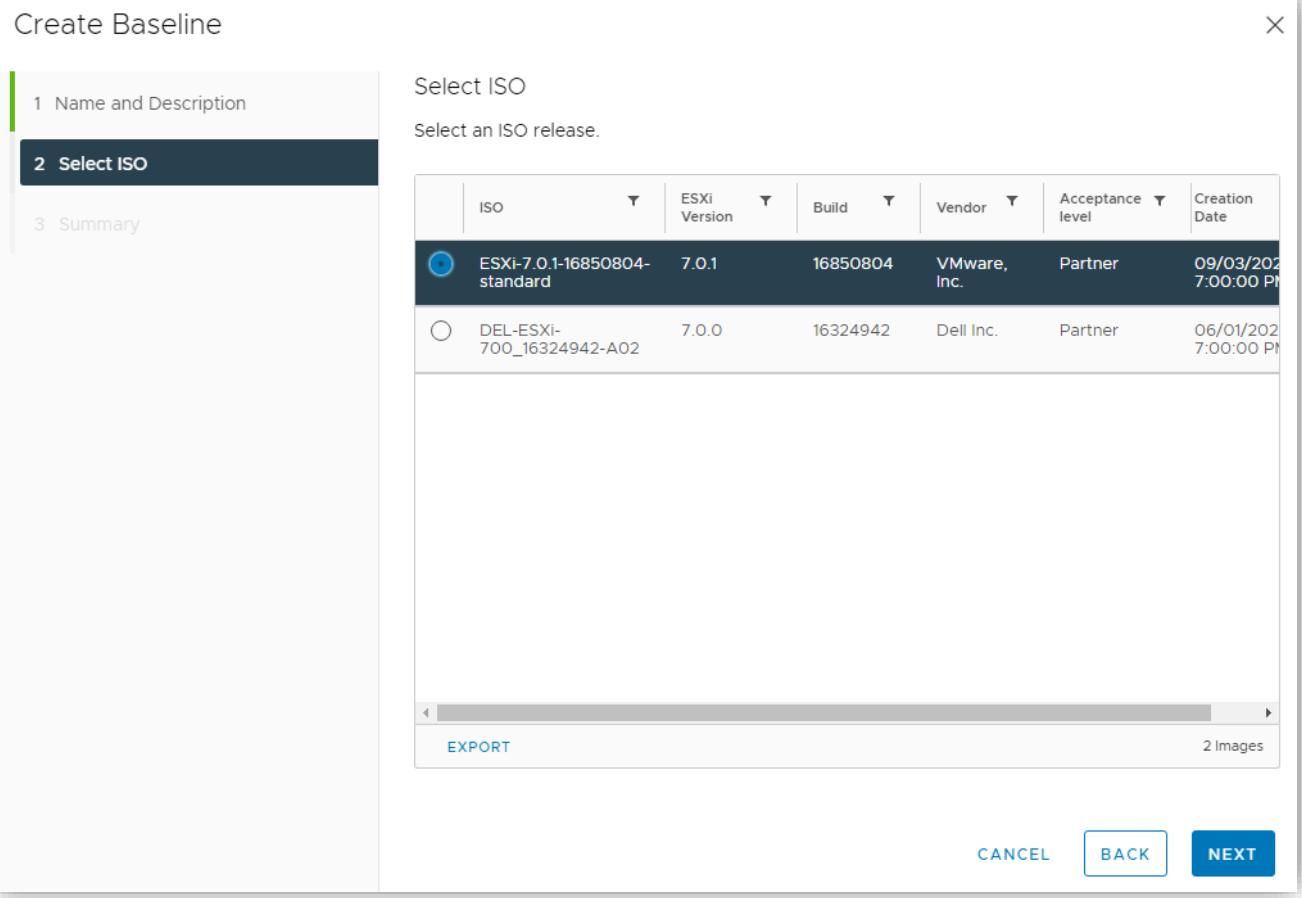
Patch

Extension

CANCEL

NEXT

I have a couple of ISOs already installed (I chose to upgrade), and I will use this to upgrade the host to the new 7.0 Update 1.



Then click Finish on the summary page.

Create Baseline

X

1 Name and Description

2 Select ISO

3 Summary

Summary

Review your setting selections before finishing the wizard.

Baseline name	VCP 2020 Upgrade
Baseline description	
Baseline type	Upgrade

ISO

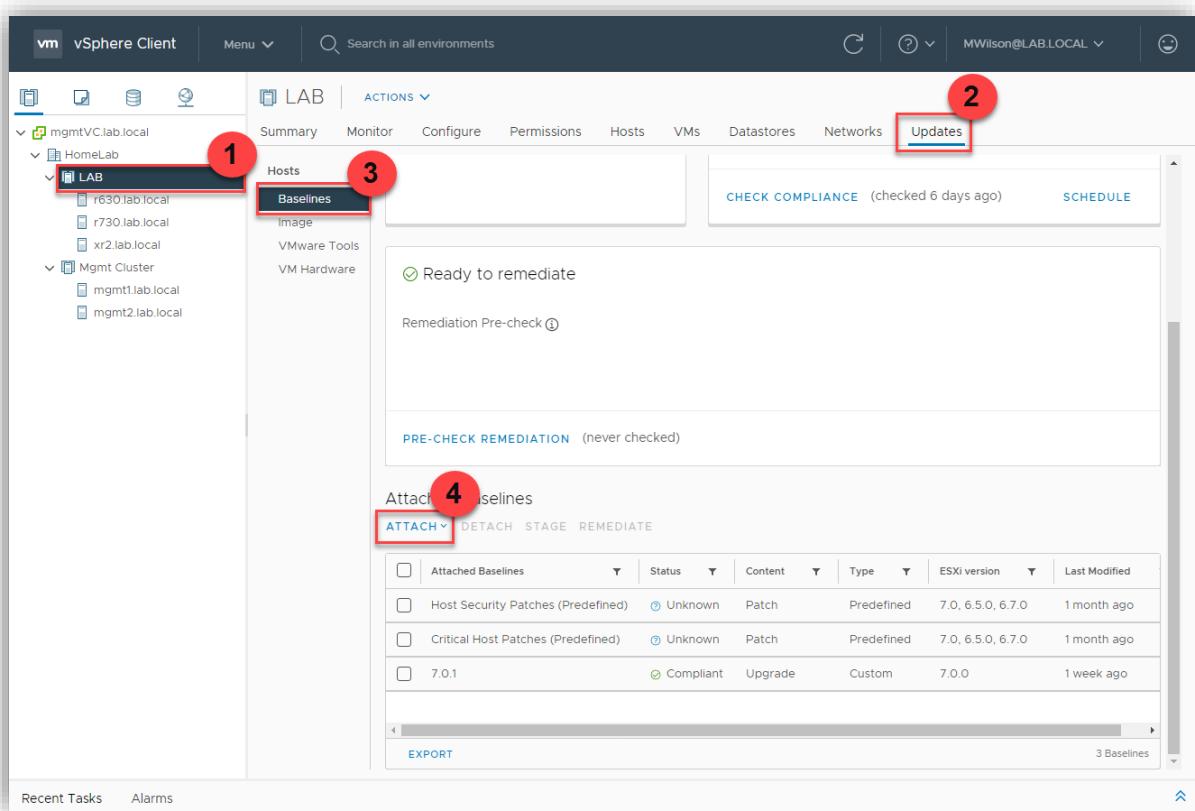
Name	ESXi-7.0.1-16850804-standard
Product	VMware ESXi 7.0.1 Update 1
Version	7.0.1
Vendor	VMware, Inc.
Acceptance level	Partner

CANCEL

BACK

FINISH

That's only half of the story, however. We now need to tell it to apply this baseline to an object. We do that by going back to Hosts and Clusters. Click on the object we want to manage, select Updates and Baselines, and scroll down and click Attach.



Select Attach Baseline. If you notice, we could have created the baseline from here as well. Select the VCP 2020 Upgrade (or whatever one you created) and click on Attach.

Attach | LAB

X

<input type="checkbox"/>	Name	Content
<input checked="" type="checkbox"/>	VCP 2020 Upgrade	Upgrade
<input type="checkbox"/>	7.0.1	Upgrade
<input type="checkbox"/>	Non-Critical Host Patches (Predefined)	Patch
<input type="checkbox"/>	Critical Host Patches (Predefined)	Patch
<input type="checkbox"/>	Host Security Patches (Predefined)	Patch
<input checked="" type="checkbox"/> 1 EXPORT		5 Baselines
		<input type="button" value="CANCEL"/> <input type="button" value="ATTACH"/>

It will now show up in the attached baselines for the object. You can now select just that one, and you can use either stage or remediate. Stage will load the software or patches to the host/s and then wait for your reboot. Remediate will do everything now. It will utilize DRS or wait until all running VMs are powered off or moved before proceeding.

Remediate | LAB with VCP 2020 Upgrade

X

Cluster is ready to remediate

3 hosts will remediate

<input checked="" type="checkbox"/>	Host Name	Version	Patches	Extensions	Remediation Status
<input checked="" type="checkbox"/>	r730.lab.local	7.0.1	0 (0 Staged)	0 (0 Staged)	✓ Ready
<input checked="" type="checkbox"/>	xr2.lab.local	7.0.1	0 (0 Staged)	0 (0 Staged)	✓ Ready
<input checked="" type="checkbox"/>	r630.lab.local	7.0.1	0 (0 Staged)	0 (0 Staged)	✓ Ready

3 EXPORT

3 Hosts

- › Install ISO VMware ESXi Release 7.0.1, Build 16850804
- › Scheduling Options: Will remediate immediately
- › Remediation settings

CANCEL

REMEDIATE

It will then kick-off and remediate the hosts unless you need to move some VMs first.

Objective 7.11 – Utilize vSphere Lifecycle Manager

We've already utilized parts of the vSphere Lifecycle Manager to perform updates and upgrades. There are a few more things we could go over, however. The Image Depot we've already covered a bit. This shows the ESXi versions, drivers, and components available to us to use. The Updates tab will show us a list of all the updates included in the baselines we've created and VMware's default baselines. You can filter them if you are looking for specific patches. You can also create a baseline that only has a subset of the updates or patches in them if you've determined that one or more may be detrimental to your environment.

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected. The 'Updates' tab is active, displaying a list of ESXi patch releases. The table includes columns for Name, ID, Severity, Type, Category, ESXi Version, and Impact. The first row is highlighted with a blue background.

Name	ID	Severity	Type	Category	ESXi Version	Impact
VMware ESXi 6.5 Patch Release	ESXi650-201806001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201808001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201810001	Critical	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201810002	Critical	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201811001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201811002	Critical	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201901001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201903001	Critical	Rollup	Security	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201905001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201908001	Important	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201910001	Important	Rollup	Security	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201911001	Moderate	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201912001	Critical	Rollup	Security	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-201912002	Critical	Rollup	BugFix	6.5.0	Reboot, Maintenance
VMware ESXi 6.5 Patch Release	ESXi650-202005001	Important	Rollup	Security	6.5.0	Reboot, Maintenance

The Imported ISOs tab is where you can import whole ISOs of ESXi to use for upgrades. You can also use an ISO if the OEM has made one available to upgrade a driver.

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected in the sidebar. The main pane displays a table of imported ISOs.

Lifecycle Manager | **ACTIONS** ▾

Image Depot Updates **Imported ISOs** Baselines Settings

IMPORT ISO **DELETE** **NEW BASELINE**

Name	Product	Version	Build	Vendor	Acceptance Level	Creation Date
ESXi-7.0.1-16850804-standard	VMware ESXi 7.0.1 Update 1	7.0.1	16850804	VMware, Inc.	Partner	09/03/2020, 7:00:00 PM
DEL-ESXI-700_16324942-A02	VMware ESXi 7.0.0	7.0.0	16324942	Dell Inc.	Partner	06/01/2020, 7:00:00 PM

EXPORT 2 Images

Recent Tasks Alarms

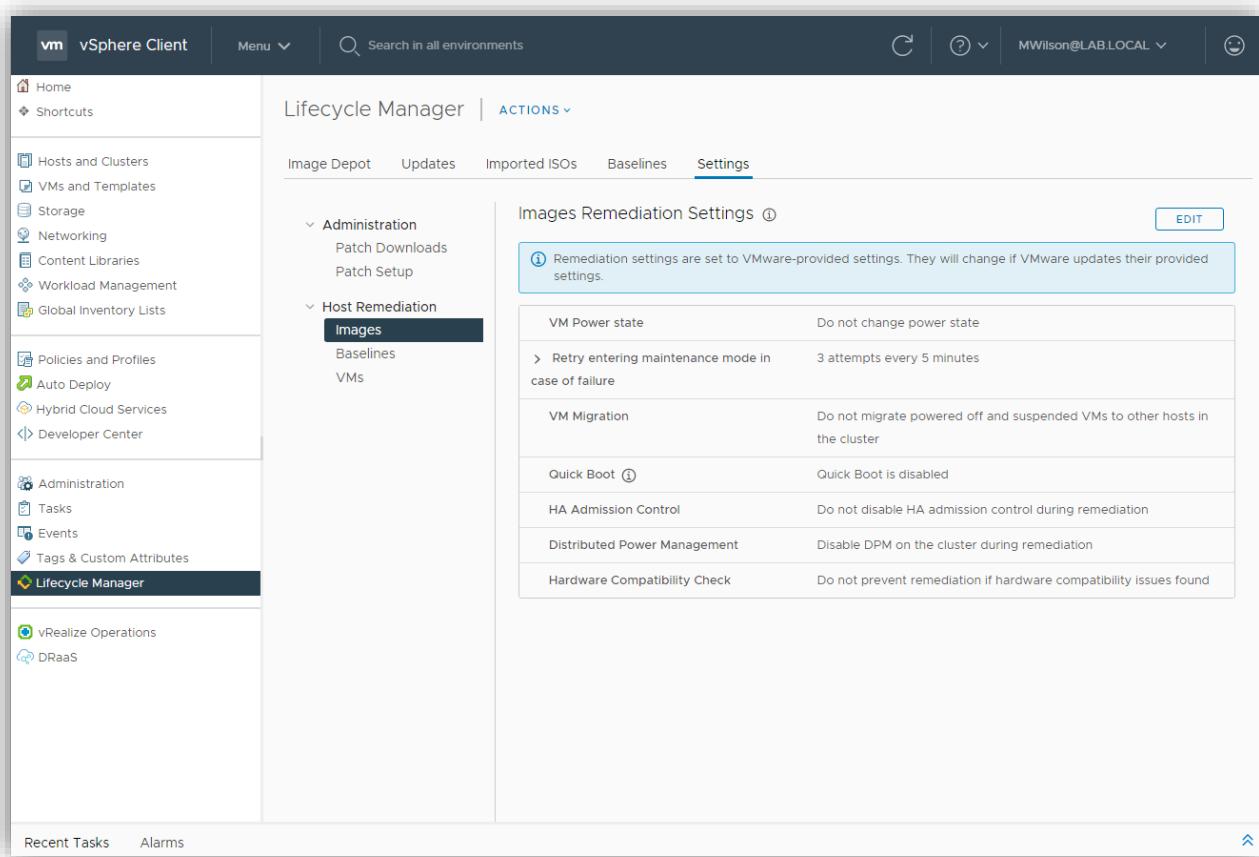
In the next tab, baselines we've used in the previous objective. We can also duplicate one if we need to change one slightly for a specific host.

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected. The left sidebar has a tree view with 'Lifecycle Manager' expanded. The main area shows a table of host baselines:

Baselines	Content	Type	ESXi version	Last Modified
VCP 2020 Upgrade	Upgrade	Custom	7.0.1	28 minutes ago
7.0.1	Upgrade	Custom	7.0.0	1 week ago
Non-Critical Host Patches (Predefined)	Patch	Predefined	7.0, 7.*, 6.5.0, 7.0.1, 6.7.0, 7.0.*, 7.0.0, 6.*, 7.1	1 month ago
Critical Host Patches (Predefined)	Patch	Predefined	7.0, 6.5.0, 6.7.0	1 month ago
Host Security Patches (Predefined)	Patch	Predefined	7.0, 6.5.0, 6.7.0	1 month ago

Buttons at the bottom include 'EXPORT' and '5 Baselines'.

The final tab is settings. This tab controls when vSphere checks for new patches and downloads them. It also controls the depots where it looks. Under Host remediation, it controls the VMs and behavior while attempting to remediate the hosts or VMs.



Objective 7.11.1 – Describe Firmware upgrades for ESXi

Firmware upgrades can be accomplished in vSphere 7, but there are caveats. Firmware and driver add-ons are not distributed through VMware channels. They must be done using a particular vendor depot, which works in conjunction with a hardware support manager. So, while vLCM will let you know if the host is in compliance and can kick off the remediation process, the actual firmware upgrade is accomplished by the hardware support manager. Open Manage Integration for VMware vCenter from Dell is an example of a hardware support manager. It is distributed by Dell and deployed as an appliance (not free). Dell, HPE, and Lenovo hardware support managers are supported. Once installed, you register the appliance as a vCenter Server extension. In the case of Dell's tool, it will interact with the iDRAC or remote access card to deploy the firmware.

Objective 7.11.2 – Describe ESXi updates

VMware differentiates between updates and upgrades as: Upgrades are significant software changes, whereas updates make smaller updates to the software. Anything that involves a numbered release, such as 6.5 to 6.7 or 6.7 to 7.0, is an upgrade. A change going from vSphere 7.0 to 7.0 Update 1 is just an update or smaller change. An upgrade may make configuration changes to the host, whereas updates will not affect host configuration.

vSphere will, if allowed, periodically check VMware's depot for new updates and will download them if configured to do so. You can see the configuration options here in the screenshot.

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected. The 'Patch Downloads' tab is active under the 'Administration' category. A red box highlights the 'Settings' tab at the top of the main content area, which is currently displaying the 'Automatic Download Settings' configuration. The settings table includes:

Automatic downloads	Enabled
Automatic download task name	VMware vSphere Lifecycle Manager Update Download
Automatic download task description	A predefined scheduled task to download software updates.
Send email to	[Empty field]

Objective 7.11.3 – Describe component and driver updates for ESXi

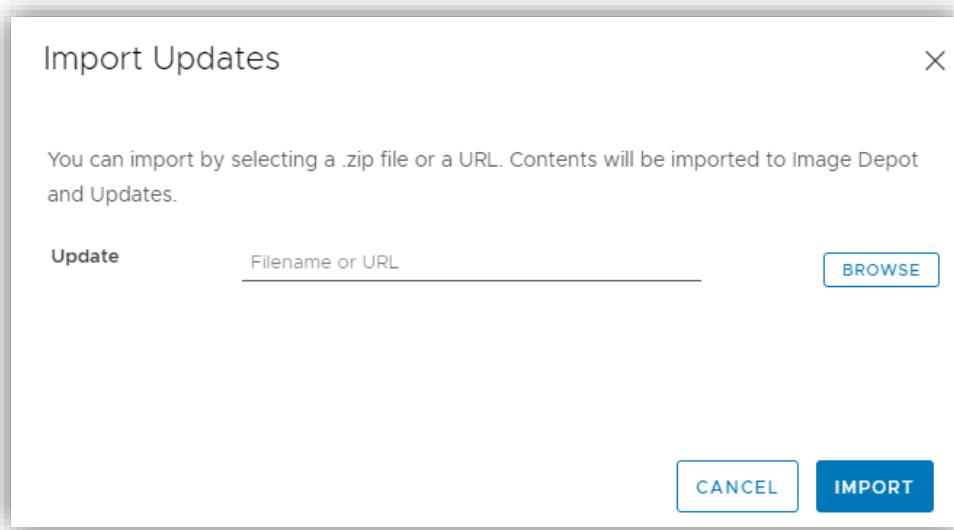
Driver and component updates can also be performed through the Lifecycle Manager in vSphere 7. Drivers are code to let vSphere know how to interact with hardware and utilize it. Components can be solutions, tools, or drivers. VMware has both downloaded from the VMware depot, but if you need to insert one that wasn't included, you can do that too. Vendor add-ons usually are driver packs meant to support an OEM's servers such as Dell or HP's. Here you can see a screenshot of the listing of available vendor add-ons and components in Lifecycle Manager

The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' section selected in the sidebar. The main area displays two tables: 'Vendor Addons' and 'Components'. The 'Vendor Addons' table lists various software add-ons with columns for Name, Version, Release Date, and Category. The 'Components' table lists hardware components with similar columns. Both tables include sorting and filtering options.

If you need to add either a driver or component, you can do that at the top via "Actions" and then Import Updates.

The screenshot shows the 'Lifecycle Manager' section with the 'Actions' dropdown menu open. The 'Import Updates' option is highlighted with a red box. Other options visible in the menu include 'Updates', 'Sync Updates', 'Hardware Compatibility List', and 'Sync HCL'.

It will then ask you for the location of the .zip or URL. It then adds the new update to the list.



Objective 7.11.4 – Describe hardware compatibility check

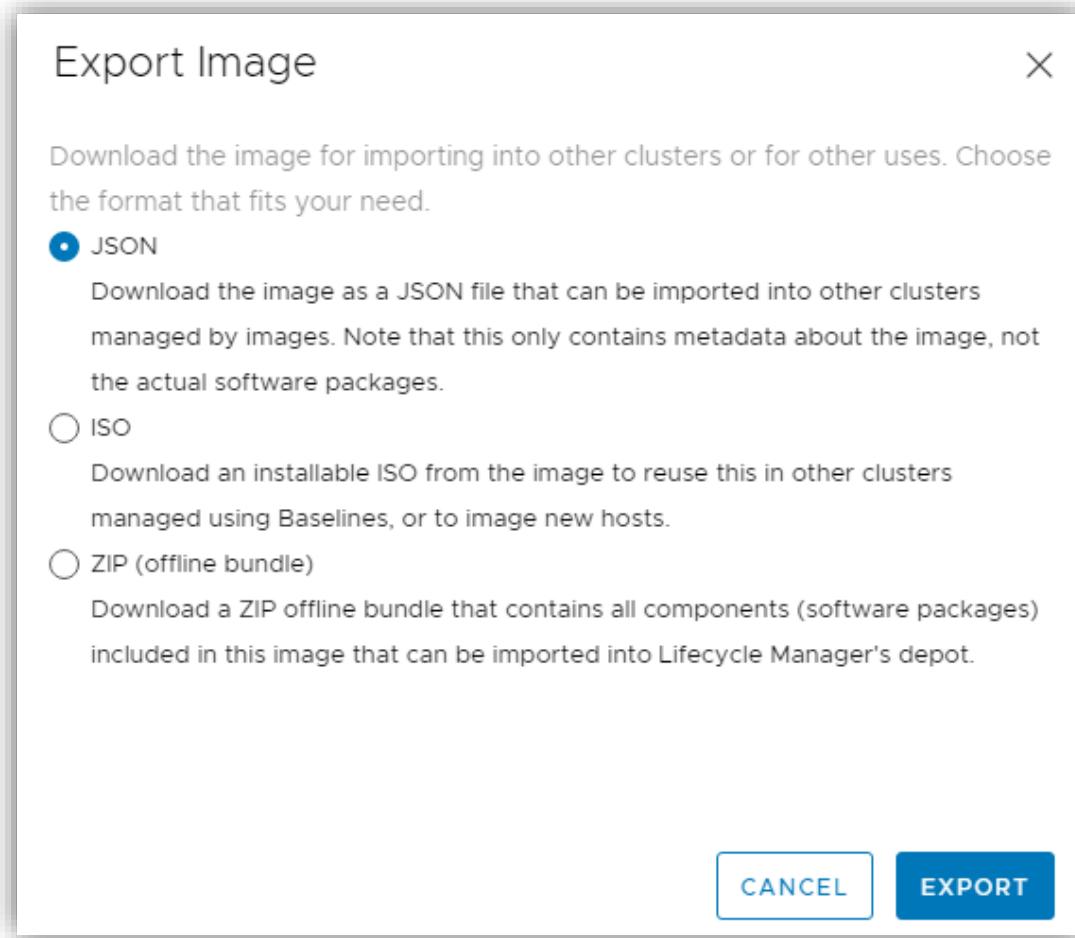
The hardware compatibility check is a tool that allows you to choose a host and see if it is capable of running a particular ESXi version. More specifically - if that host is certified to run it. It will take the hardware it finds on the host and checks it against the VMware HCL (Hardware Compatibility List) or vSAN HCL if the host participates in a vSAN cluster. At the end of the scan, the tool will give you the results to export to a CSV file. Here is where it is and what it looks like below.

You would select a host, click on the Update tab, and then Hardware Compatibility. You can then select which version of ESXi you want to check.

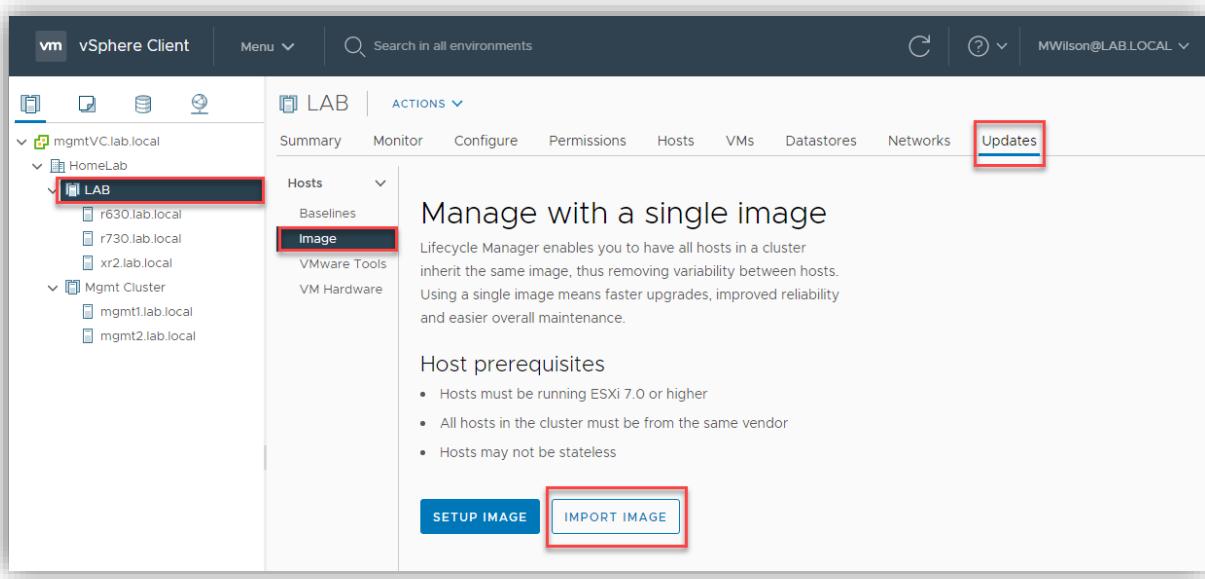
Objective 7.11.5 – Describe ESXi cluster image export functionality

One of the new abilities that vSphere 7 brought was using a single image for the whole cluster. This was able to promote uniformity and made the hosts easier to maintain and troubleshoot. Once you setup an image for a cluster, you can also export it to be imported and used in another cluster. This would be done for the same reasons as described above. The export process is done in the following location.

Go to the cluster > Updates > Image > ellipsis > export. This is assuming you have already set this up. You then are presented with a box that asks you what you want to export. JSON, ISO, or ZIP. If using for another cluster to import, you will need the JSON and zip.



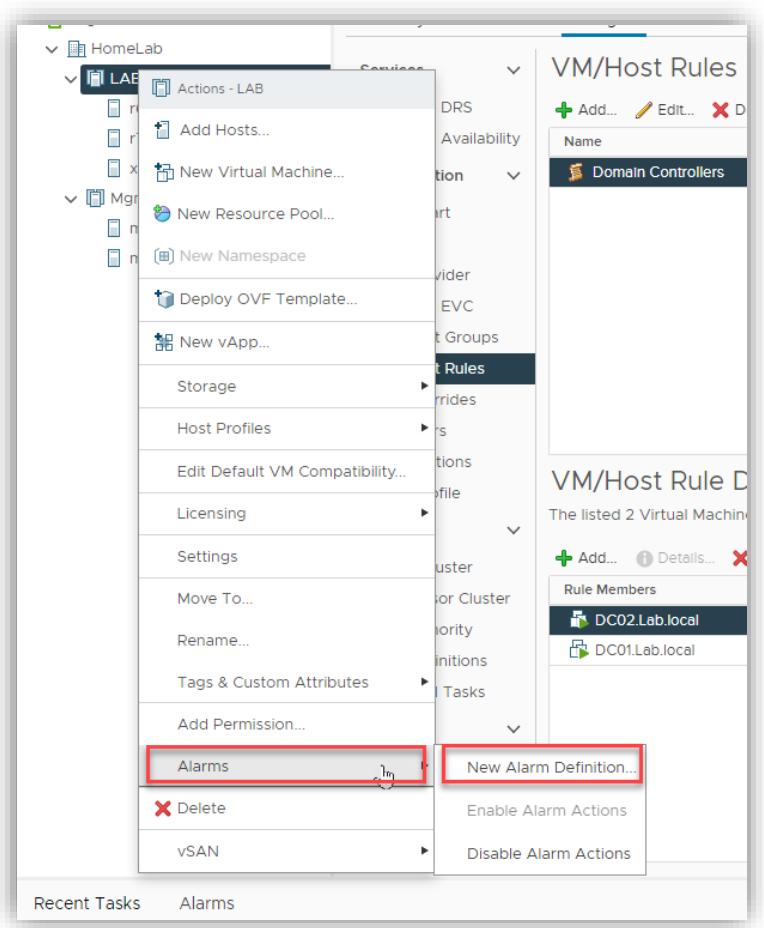
To import, you will go to the same place on a cluster that has not been set up yet.



It will then ask you for the JSON file and zip.

Objective 7.12 – Configure alarms

An alarm can be set up for many different objects in vSphere. There are many predefined alarms, and you can create and configure new ones. To create a new alarm, Right-click on an object and select Alarms > New Alarm Definition.



Give the alarm a name and then click Next.

New Alarm Definition

1 Name and Targets

- 2 Alarm Rule 1
- 3 Reset Rule 1
- 4 Review

Name and Targets

Alarm Name * VCP 2020 Test Alarm

Description

Target type * Clusters

Targets LAB

CANCEL NEXT

Now you need to select what the trigger will be. In this case, I want an alarm to happen if someone creates a resource pool. I then tell vSphere what I want it to do. In this case, I want a warning to appear and send me an email.

New Alarm Definition

2 Alarm Rule 1

- 1 Name and Targets
- 3 Reset Rule 1
- 4 Review

Alarm Rule 1

IF Resource pool created ADD ARGUMENT

THEN Trigger the alarm and * Show as Warning

Send email notifications Repeat ⓘ Subject * Alarm {Alarm name} on Cluster : {Target Name} is {New status}

Email to * Mike@IT-Muscle.com

Send SNMP traps

Run script

ADD ANOTHER RULE DUPLICATE RULE REMOVE RULE

CANCEL BACK NEXT

Next, I will add that if the resource pool is deleted, it can reset it to green.

The screenshot shows the 'Reset Rule 1' configuration screen within the 'New Alarm Definition' wizard. The left sidebar lists steps: 1. Name and Targets, 2. Alarm Rule 1, 3. Reset Rule 1 (selected), and 4. Review. The main area displays the rule configuration:

Reset Rule 1

Reset the alarm to green

IF

Resource pool deleted

THEN

Reset the alarm to * Normal

Send email notifications

Send SNMP traps

Run script

Buttons at the bottom: ADD ANOTHER RESET RULE, DUPLICATE RULE, REMOVE RULE, CANCEL, BACK, NEXT.

Make sure the alarm is enabled and then click create.

The screenshot shows the 'Review' screen for the new alarm definition. The left sidebar lists steps: 1. Name and Targets, 2. Alarm Rule 1, 3. Reset Rule 1, and 4. Review (selected). The main area displays the alarm details:

New Alarm Definition

1. Name and Targets
2. Alarm Rule 1
3. Reset Rule 1
4. Review (selected)

Review

Alarm Name: VCP 2020 Test Alarm

Description:

Targets: LAB

Alarm Rules:

IF Resource pool created
THEN Trigger the alarm as Warning
Send emails to Mike@IT-Muscle.com
with subject Alarm {Alarm name} on Cluster : {Target Name} is {New status}

Reset Rules:

IF Resource pool deleted
THEN Trigger the alarm as Normal

Enable this alarm

Buttons at the bottom: CANCEL, BACK, CREATE.

I can now find this alarm if I go to the object > Configure > Alarm Definitions

The screenshot shows the vSphere Client interface. The left sidebar shows a tree view of the vSphere environment, with 'LAB' selected. The main pane has a 'Configure' tab selected, which is highlighted with a red box. Below it is a 'Alarm Definitions' section, also highlighted with a red box. A table lists various alarms, with the first one, 'VCP 2020 Test Alarm', also highlighted with a red box. The table columns are: Alarm Name, Object type, Defined In, and Enabled.

	Alarm Name	Object type	Defined In	Enabled
1	> VCP 2020 Test Alarm	Cluster	This Object	Enabled
2	> alarm.vsan.health.test.ditencryption...	Cluster	mgmtVC.lab...	Enabled
3	> alarm.vsan.health.test.diagnostics...	Cluster	mgmtVC.lab...	Enabled
4	> vSAN File Service 'Infrastructure H...	Cluster	mgmtVC.lab...	Enabled
5	> vSAN health alarm 'Unexpected n...	Cluster	mgmtVC.lab...	Enabled
6	> alarm.vsan.health.test.diagnostics.t...	Cluster	mgmtVC.lab...	Enabled
7	> alarm.vsan.health.test.diagnostics...	Cluster	mgmtVC.lab...	Enabled
8	> vSAN health alarm 'Server cluster ...	Cluster	mgmtVC.lab...	Enabled
9	> vSAN health alarm 'No hosts in re...	Cluster	mgmtVC.lab...	Enabled
10	> vSAN health alarm 'Shared witness...	Cluster	mgmtVC.lab...	Enabled
11	> vSAN online health alarm 'vSAN co...	Cluster	mgmtVC.lab...	Enabled
12	> vSAN online health alarm 'Audit C...	Cluster	mgmtVC.lab...	Enabled
13	> vSAN online health alarm 'vSAN m...	Cluster	mgmtVC.lab...	Enabled
14	> vSAN online health alarm 'Importa...	Cluster	mgmtVC.lab...	Enabled
15	> vSAN online health alarm 'HPE SA...	Cluster	mgmtVC.lab...	Enabled
16	> vSAN online health alarm 'Custom...	Cluster	mgmtVC.lab...	Enabled

You notice I can disable alarms under the same place, but I can't edit the default alarms. I CAN edit mine, however. As you can see, I can set alarms for all sorts of events and have many things that will happen if the alarm's criteria are met.

Conclusion

Well, that brings us to the end of another Study Guide. I hope it helped in some way, and I'm happy you were along for the ride! Till next time.

Mike