# VCP 2019 STUDY GUIDE

@IT_Muscle

SEPTEMBER 7, 2019

MIKE WILSON

# VCP 2019 Study Guide

It's been a while since I've done one of these. I did one for the VCP 6.0 and kind of miss it. I've decided to take a little different approach this time. I'm going to actually write it completely up as a single document and then slowly leak it out on my blog but also have the full guide available for people to use if they want. I'm not sure the usable life of this since there is a looming version on the horizon for VMware, but it will be a bit before they update the cert.

I'm also changing which certification I'm writing for. I originally did one for the delta. This time it will be the full. There shouldn't be an issue using this for the delta, however. The certification, 2V0-21.19 is for vSphere version 6.7 and is a 70-question exam. You are required to pass with a score of no less than 300 and you are given 115 minutes to take it. This gives you about 40 seconds per question. Study well and if you don't know something, don't agonize over it. Mark it and come back. It is very possible a later question will job your memory or give you possible hints to the answer.

You will need to venture outside and interact with real people to take this test. No sitting at home in your pjs, unfortunately. You will need to register for the test on Pearson Vue's Website here.

Standard disclaimer, I am sure I don't cover 100% of the topics needed on the exam, as much as I might try. Make sure you use other guides and use your own research to help out. In other words, you can't hold me liable if you fail 😊

# Table of Contents

# Section 1 – VMware vSphere Architectures and Technologies

## *Objective 1.1 – Identify the pre-requisites and components for vSphere implementation*

The first part starts with installation requirements. There are two core components that make up vSphere. ESXi and vCenter. There several requirements for ESXi and for vCenter Server. I'll cover them here one component at a time to better understand them.

**vSphere ESXi Server**

The ESXi Server is the server that does most of the work. This server is where you install virtual machines (VMs) and provides the needed resources for all your VMs to run. The documentation also talks about virtual appliances. Virtual appliances are nothing more than preconfigured VMs, usually running some variant of Linux.

There is an order to installation of vSphere, and the ESXi server is installed first. There are a number of requirements for installation. Some of them I will generalize, as otherwise this would be a Study Textbook and not a guide.

- Supported server platform. The best way to determine if your server is supported is to check against the VMware Compatibility Guide here.
- At least two CPU cores. This shouldn't be that big of an issue these days when you have companies such as AMD having mainstream 16-core processors and 64-core Server processors.
- 64-bit processor released after 2006.
- The NX/XD bit to be enabled in the BIOS. This is also known as the No-Execute bit (or eXecute Disable) and allows you to segregate areas of memory for use with code or data. Enabling this protects against certain forms of malware exploits.
- Minimum of 4 GB of RAM. You hopefully will have at least 6-8 in order to give adequate space for VMs to run.
- Support for Intel VT-x or AMD RVI. This isn't an issue for most current processors. Only extremely inexpensive or old processors would not have this option in the BIOS.
- 1+ Gigabit or faster Ethernet controllers. Same as above, make sure it is a supported model.
- SCSI disk or RAID LUN. These are seen as local drives. This allows you to use them as "scratch" partitions. A scratch partition is a disk partition used by VMware to host logs, updates, or other temporary files.
- SATA drives. You can use a SATA drive but by default these are considered "remote" not local. This prevents them from being used for that scratch partition.

You can use UEFI BIOS mode with vSphere 6.7+ or just regular BIOS mode. Once you have installed ESXi, you should not change the mode from one to the other in the BIOS, or you may need to re-install (it won't boot). The actual display message is "Not a VMware boot bank" that you might encounter.

VMware requires a minimum boot device with 1 GB of storage. When booting from a local disk, 5.2 GB is needed to allow creation for the scratch disk and the VMFS (VMware File System) volume. If you don't have enough space, or you aren't using a local drive, the scratch partition will be placed in a RAMDISK or all in RAM. This is not persistent through reboots of the physical machine, and will give you a message (nagging you) until you do provide a location for it. It actually is a good thing to have though, as any dump files (code from ESXi describing what went wrong when a crash occurs) are stored there.

You can Auto Deploy a host as well – this is when you have no local disks at all and are using shared storage to install and run ESXi software. If you do use this method, you don't need to have a separate LUN or shared disk, set aside for each host. You can share a single LUN across multiple hosts.

Actual installation of the ESXi software is straightforward. You can perform an Interactive, scripted or Auto Deploy installation. The latter requires a bit of preparation before you can do that and a number of other components. You will need to have TFTP server setup and make changes to your DHCP server to allow this to happen. There is more that goes into the Auto Deploy, but I won't cover that here as the cert exam shouldn't go too far in depth. For interactive installation you can create a customized ISO if you require specific drivers that aren't included on the standard VMware CD

**vSphere vCenter Server**

The vCenter Server component of vSphere allows you to manage and aggregate your server hardware and resources. vCenter is where a lot of the magic lies. Using vCenter Server you can migrate running VMs between hosts and so much more. VMware makes available the vCenter Server Appliance or VCSA. This is a preconfigured Linux-based VM that is deployed into your environment. There are two main group of services that run on the appliance, vCenter Server and the Platform Services Controller. You run both of those together in what is known as an "embedded" installation or you can separate the Platform Services Controller (PSC) for larger environments. While you can install vCenter on Windows as well, VMware will no longer support that model for the next major release of vSphere.

There are a few software components that make up the vCenter Server Appliance. They include:

- Project Photon OS 1.0 – This is the Linux variant used for the operating system.
- Platform Services Controller group of infrastructure services
- vCenter Server group of services
- PostgreSQL – This is the database software used.

- VMware vSphere Update Manager Extension or VUM. This is one way you can keep your vSphere software up to date.

While past versions of vCenter Server Appliance were a bit less powerful, since 6.0 they have been considerably more robust. This one is no exception, with it scaling to 2,000 hosts and 35,000 VMs.

If you do decide to separate the services it is good to know what services are included with which component. They are:

- **vCenter Platform Services Controller or PSC** - contains Single Sign On, Licensing, Lookup service, and the Certificate Authority.
- **vCenter Server** - contains vCenter Server, vSphere client, vSphere Web Client, Auto Deploy, and the Dump Collector. It also contains the Syslog Collector and Update Manager.

If you go with a distributed model, you need to install the PSC first, since that machine houses authentication services. If there is more than one PSC, you need to setup them one at a time before you create the vCenter Server/s. Multiple vCenter Servers can be setup at the same time.

The installation process consists of two parts for the VCSA when using the GUI installer, and one for using CLI. For the GUI installation, the first stage deploys the actual appliance. The second guides you through the configuration and starts up its services.

If using CLI to deploy, you run a command against a JSON file that has all the values needed to configure the vCenter Server. The CLI installer grabs values inside the JSON file and generates a CLI command that utilizes the VMware OVF Tool. The OVF Tool is what actually installs the appliance and sets the configuration.

Hardware Requirements vary depending on the deployment configuration. Here are a few tables to help guide you:

**Embedded vCenter with PSC**

| Environment | vCPUs | Memory |
|---|---|---|
| Tiny (up to 10 hosts or 100 VMs) | 2 | 10 GB |
| Small (up to 100 hosts or 1,000 VMs) | 4 | 16 GB |
| Medium (up to 400 hosts or 4,000 VMs | 8 | 24 GB |
| Large (up to 1,000 hosts or 10,000 VMs) | 16 | 32 GB |
| X-Large (up to 2,000 hosts or 35,000 VMs) | 24 | 48 GB |

If you are deploying an external PSC appliance you need 2 vCPUs and 4 GB RAM  and 60 GB  storage for each.

| Environment | Default Storage Size | Large Storage Size | X-Large Storage Size |
|---|---|---|---|
| Tiny (up to 10 hosts or 100 VMs) | 250 GB | 775 GB | 1650 GB |
| Small (up to 100 hosts or 1,000 VMs) | 290 GB | 820 GB | 1700 GB |
| Medium (up to 400 hosts or 4,000 VMs | 425 GB | 925 GB | 1805 GB |
| Large (up to 1,000 hosts or 10,000 VMs) | 640 GB | 990 GB | 1870 GB |
| X-Large (up to 2,000 hosts or 35,000 VMs) | 980 GB | 1030 GB | 1910 GB |

Both the vCenter Server and PSC appliance must be installed on a minimum ESXi 6.0 host or later.

Make sure that DNS is working and the name you choose for your vCenter Server Appliance is resolvable before you start installation.

Installation happens from a client machine and needs certain requirements. If using Windows, you can use Windows 7-10, or Server 2012-2016 (x64). Linux users can use SUSE 12 and Ubuntu 14.04. If Mac OS, 10.9-11 and Sierra are all supported.

**Installation on Microsoft Windows**

This may be covered on the test, but I can't imagine too many questions since it is being deprecated. That being said, vCPUs and Memory are the same as the appliance. Storage sizes are different. They are:

| Default Folder | Embedded | vCenter | PSC |
|---|---|---|---|
| Program Files | 6 GB | 6 GB | 1 GB |
| ProgramData | 8 GB | 8 GB | 2 GB |
| System folder (to cache the MSI installer) | 3 GB | 3 GB | 1 GB |

As far as OS's, it requires a minimum of Microsoft Windows 2008 SP2 x64. For databases you can use the built-in PostgreSQL for up to 20 hosts and 200 VMs. Otherwise you will need Oracle or Microsoft SQL Server.

## *Objective 1.2 – Identify vCenter high availability (HA) requirements*

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. This is from the Availability guide. Honestly, I'm not sure on the last one as it seems as if you are upgrading with an embedded installation, your vCenter might be unavailable for a bit but not very long (unless there is a failure). If distributed, you have other PSCs and vCenter Servers to take up the load. So, I'm not sure if it really works for me in that scenario or not. Perhaps someone might enlighten me later and I'm not thinking it all the way through. Either way…..

vCenter Server High Availability uses 3 VCSA nodes. 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 that is created when you set this up. This network is used to replicate data across and connectivity to the witness node. Requirements are:

- ESXi 5.5 or later is required. 3 Hosts are strongly recommended to house all the appliances on different physical hosts. Using DRS is also recommended.
- If using a management vCenter (for the management cluster), vCenter Server 5.5+ is required
- vCenter Server Appliance 6.5+ is required. Your Deployment size should be "Small" at a minimum. You can use VMFS, NFS, or vSAN datastores.
- Latency on the network used for the HA network must be less than 10 ms. It should be on a separate subnet than the regular Management Network.
- A single vCenter Server Standard license is required.

## *Objective 1.3 – Describe storage types for vSphere*

vSphere supports multiple types of storage. I will go over the main types. Local and Networked Storage.

**Local Storage**

Local storage is storage connected directly to the server. This can include a Direct Attached Storage (DAS) enclosure that is connected 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 the server is a single point of failure or SPOF. If the server fails, no other server can access the VM. There is a special 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

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

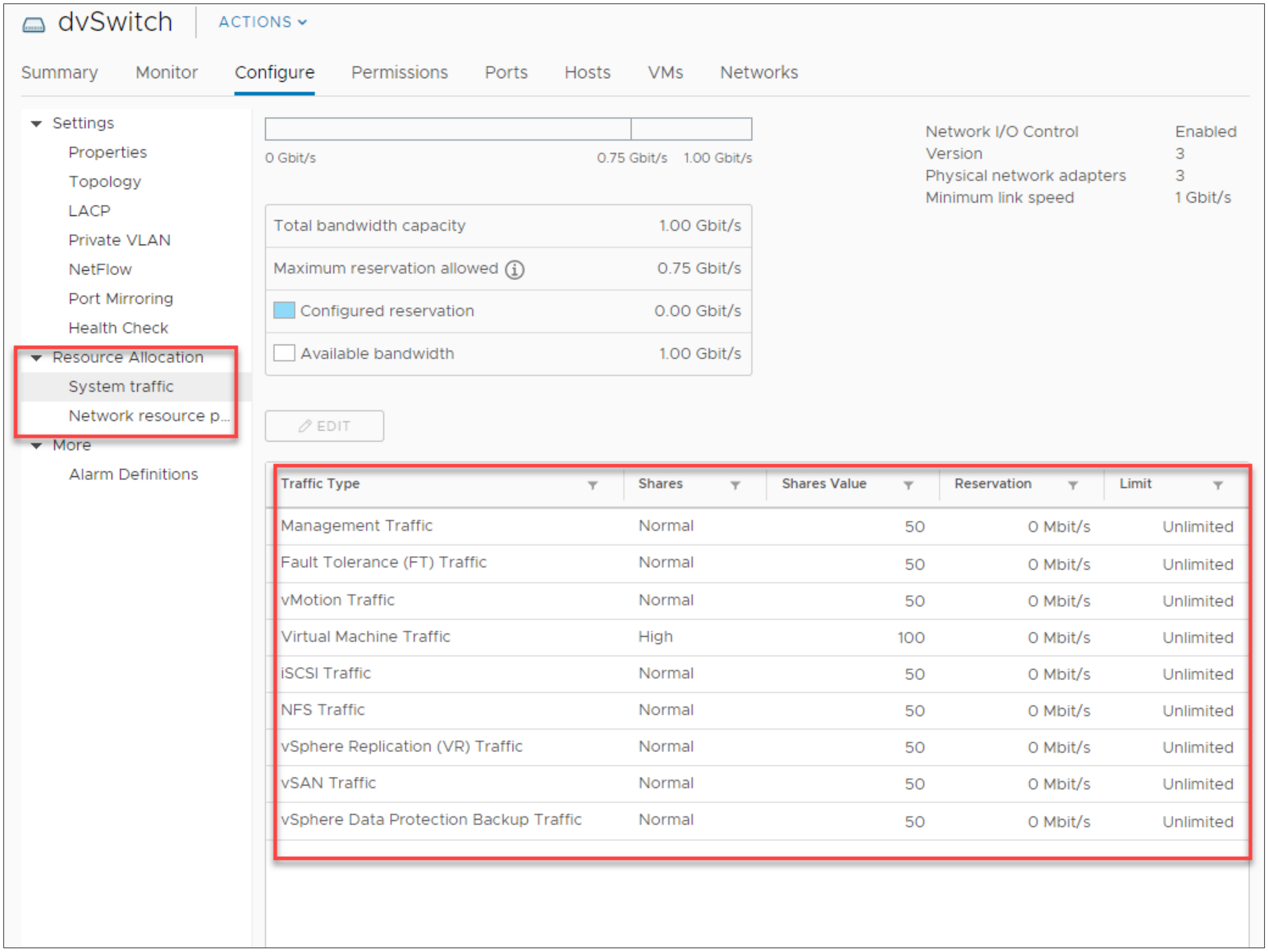
Finally, vSphere also supports the NFS 3 and 4.1 protocol for file-based storage. Unlike the rest of the storage mentioned above, this is presented as a share to the host instead of block-level raw disks. Here is a small table on networked storage for easier perusal.

| Technology | Protocol | Transfer | Interface |
|---|---|---|---|
| Fibre Channel | FC/SCSI | Block access | FC HBA |
| Fibre Channel over Ethernet (FCoE) | FCoE / SCSI | Block access | • Converged Network Adapter<br>• NIC with FCoE support |
| ISCSI | ISCSI | Block access | • ISCSI adapter (dependent or independent)<br>• NIC (Software adapter) |
| NAS | IP / NFS | File level | Network adapter |

## *Objective 1.4 – Differentiate between NIOC and 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 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.

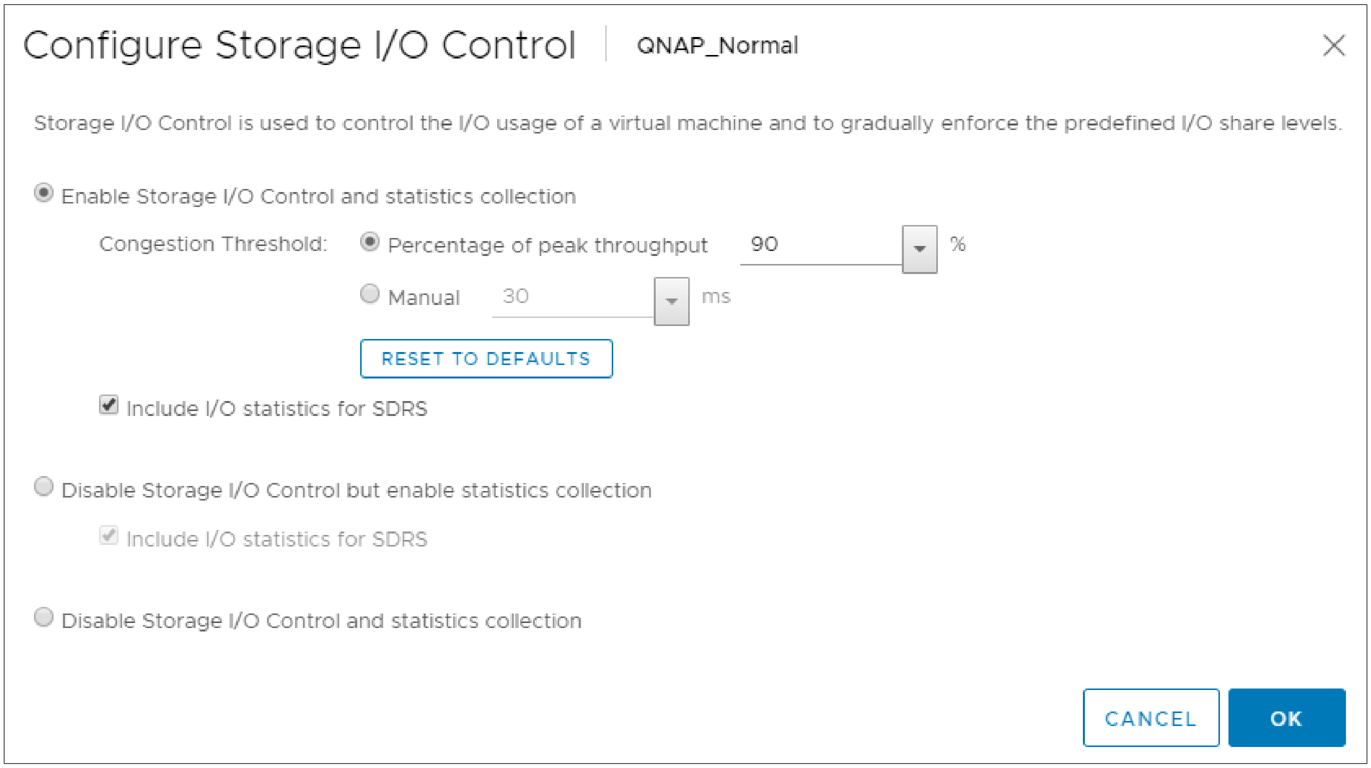


| | |
|---|---|
| Network I/O Control | Enabled |
| Version | 3 |
| Physical network adapters | 3 |
| Minimum link speed | 1 Gbit/s |

| | |
|---|---|
| Total bandwidth capacity | 1.00 Gbit/s |
| Maximum reservation allowed ⓘ | 0.75 Gbit/s |
| 🟦 Configured reservation | 0.00 Gbit/s |
| □ Available bandwidth | 1.00 Gbit/s |

| 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 important 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 | QNAP_Normal

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

Congestion Threshold: ● Percentage of peak throughput 90 %

○ Manual 30 ms

☑ Include I/O statistics for SDRS

○ Disable Storage I/O Control but enable statistics collection

☑ Include I/O statistics for SDRS

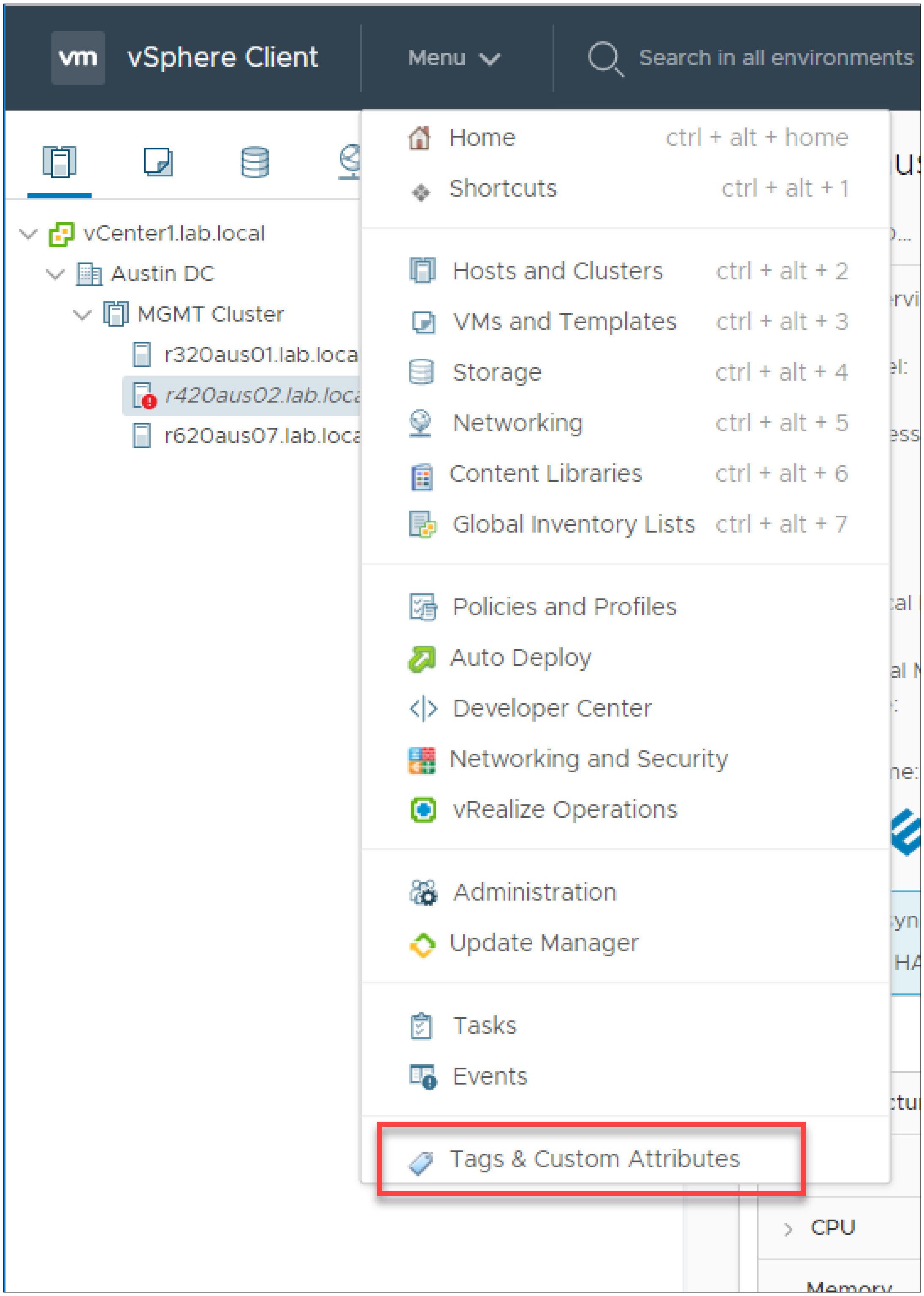
○ Disable Storage I/O Control and statistics collection

## *Objective 1.5 – Manage vCenter inventory efficiently*

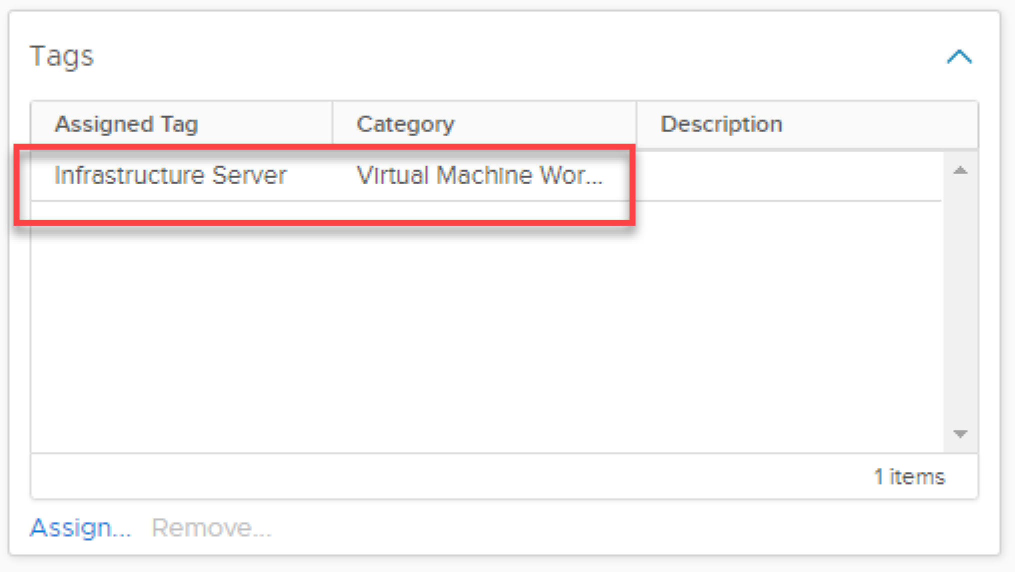
There are several tools you can use to manage your inventory easier. vSphere allows you to use multiple types of folders to hold your vCenter inventory. Folders can also be used to assign permissions and set alarms to objects. You can put multiple types of objects inside of a folder but only one type per folder. For example, if you had VMs inside a folder, you wouldn't be able to add a host to it.

vApps is another way to manage objects. They can be used to manage other attributes as well. You can assign resources and even startup order with vApps.

You can use Tags and Categories to better organize and make your inventory searchable. You create them off the main menu. There is a menu item called Tags and Custom Attributes



You can create Categories such as “Operating Systems” and then Tags such as “Window 2012” and others. This sort of action will make your VMs easier to manage and search for things. You then can see the tags on the summary of the VM as shown here.



| Assigned Tag | Category | Description |
|---|---|---|
| Infrastructure Server | Virtual Machine Wor... | |

Tags can be used for rules on VMs too. You can see this (although a bit branded) by reading a blog post I wrote for Rubrik here.

## *Objective 1.6 – Describe and differentiate among vSphere HA, DRS, and SDRS functionality*

HA is a feature designed for VM resilience. The other two, DRS and SDRS are for managing resources. HA stands for High Availability. HA works by pooling all the hosts and VMs into a cluster. Hosts are monitored and in the event of a failure, VMs are re-started on another host.

DRS stands for Distributed Resource Scheduling. This is also a feature used on a host cluster. DRS is a vSphere feature that will relocate VMs and make recommendations on host placement based on current load.

Finally, SDRS is Distributed Resource Scheduling for Storage. This is enabled on a Datastore cluster and just like DRS will relocate the virtual disks of a VM or make recommendations based on usage and I/O Load.

You can adjust whether or not DRS/SDRS takes any actions or just makes recommendations.

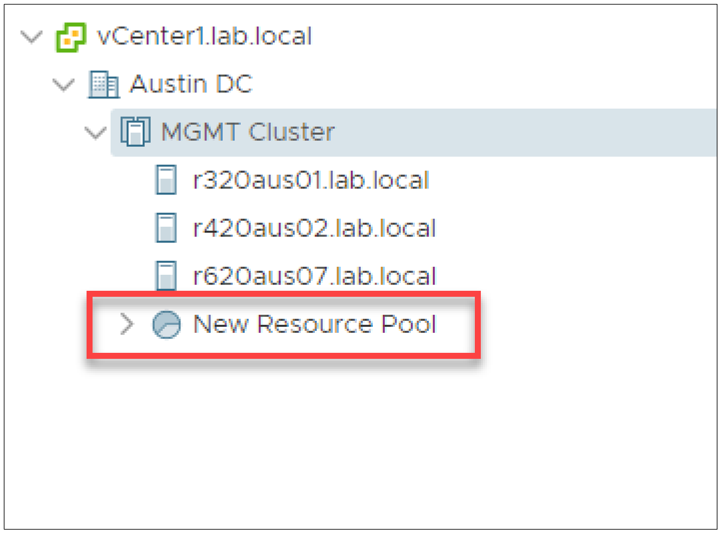
## *Objective 1.7 – Describe and identify resource pools and use cases*

The official description of a resource pool is a logical abstraction for flexible management of resources. My unofficial description is a construct inside vSphere that allows you to partition and control resources to specific VMs. Resource pools partition memory and CPU resources.

You start with the root resource pool. This is the 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 cords 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. Resources pools are abstracted from the hosts' resources. You can add and remove hosts without having to make changes to resource allocations.

You can identify resources pools by their icon.



vCenter1.lab.local
Austin DC
MGMT Cluster
r320aus01.lab.local
r420aus02.lab.local
r620aus07.lab.local
New Resource Pool

When you create a resource pool, you have a number of options you will need to make decisions on.

**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 total of the root pool. For example. If you have two pools that each have 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. Default is 0. Reserved resources are held by that pool regardless if there are VMs inside it or not.

**Expandable Reservation** is a check box 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 be able to use if there is no contention.

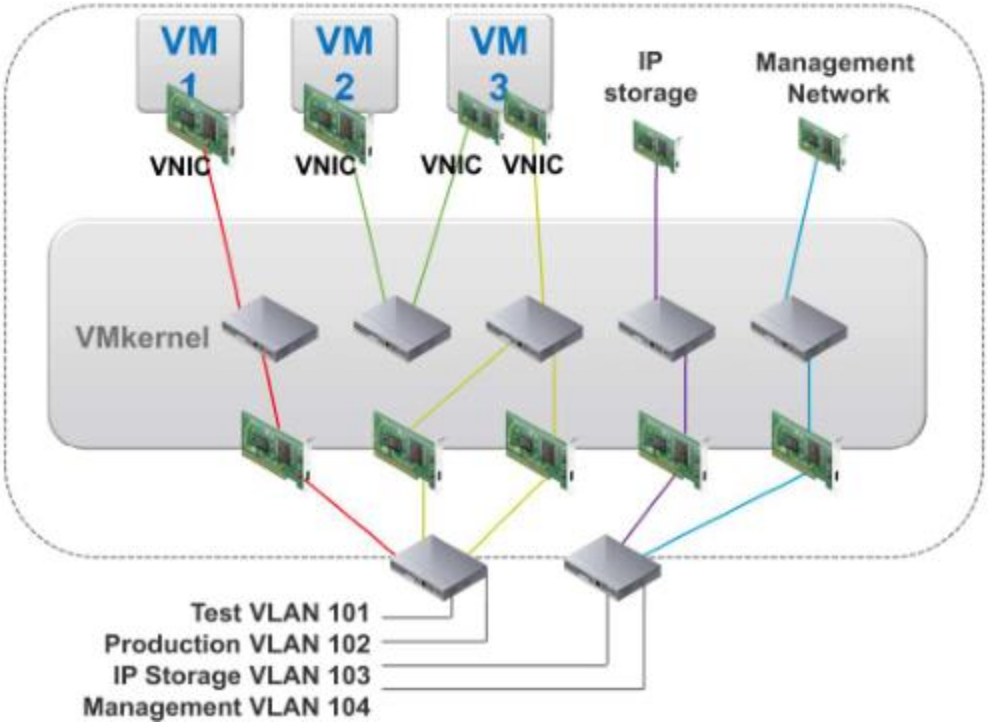
In past exams, there were questions asking you calculate resources given a number of resource pools. Make sure you go over how to do that.

## *Objective 1.8 – Differentiate between VDS and VSS*

VDS and VSS are networking constructs in vSphere. VDS is Virtual Distributed Switch and VSS is Virtual Standard Switch.

Virtual Standard Switch is the base switch. It is what is installed by default when ESXi is deployed. It has only a few features and requires you to configure a switch on every host. As you can imagine, this can get tedious and difficult to make these exactly the same. Which is what you need to do in order for VM's to seamlessly move across hosts. You could create a host profile template to make sure they are the same, but then you lose the dynamic nature of switches.

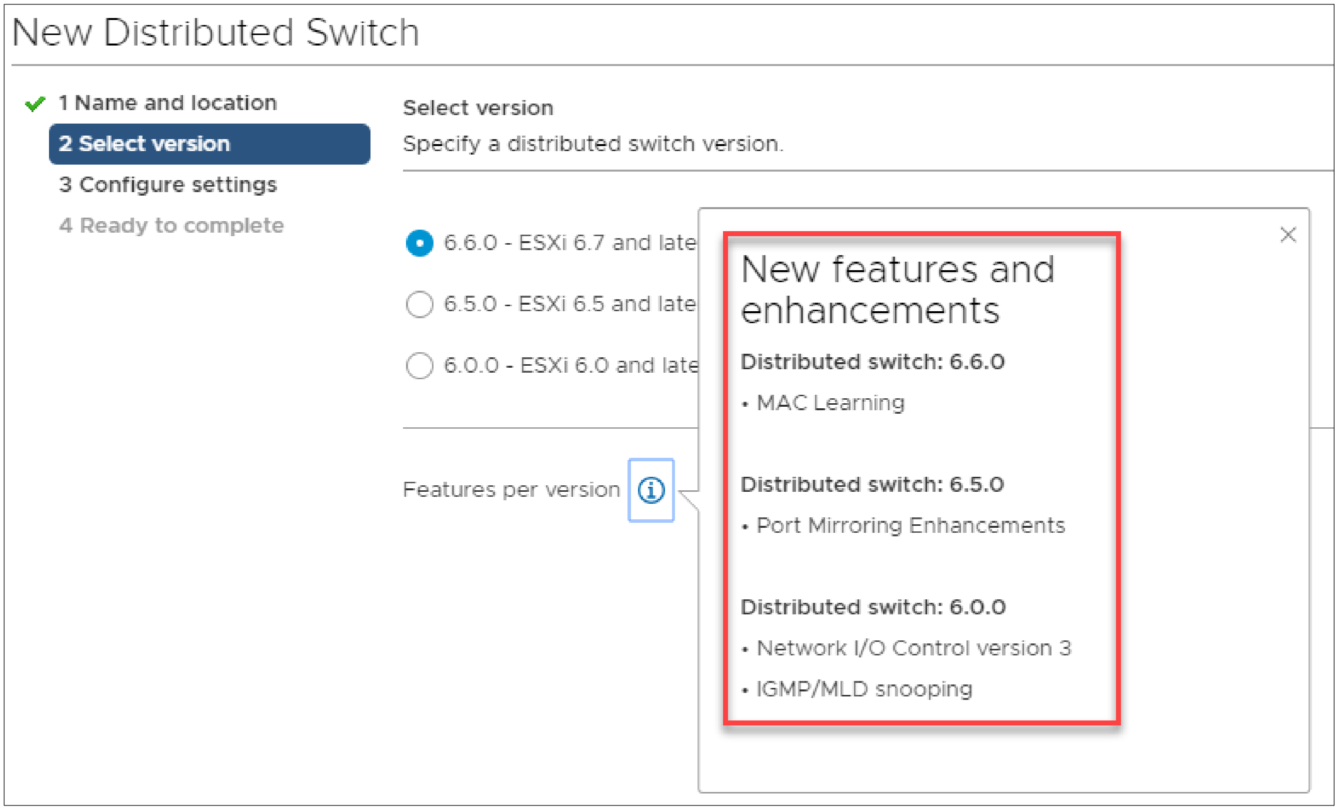
Standard Switches create a link between physical NICs and virtual NICs. You can name them essentially whatever you want, and you can assign VLAN IDs. You can shape traffic but only outbound. Here is a picture I lifted from the official documentation for a pictorial representation of a VSS.



VDSs on the other hand add a management plane to your networking. Why is this important? It allows you to control all your host networking through one UI. This does 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 and you only have to change once.

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

● 6.6.0 - ESXi 6.7 and late

○ 6.5.0 - ESXi 6.5 and late

○ 6.0.0 - ESXi 6.0 and late

Features per version

New features and enhancements

Distributed switch: 6.6.0

- MAC Learning

Distributed switch: 6.5.0

- Port Mirroring Enhancements

Distributed switch: 6.0.0

- Network I/O Control version 3
- IGMP/MLD snooping

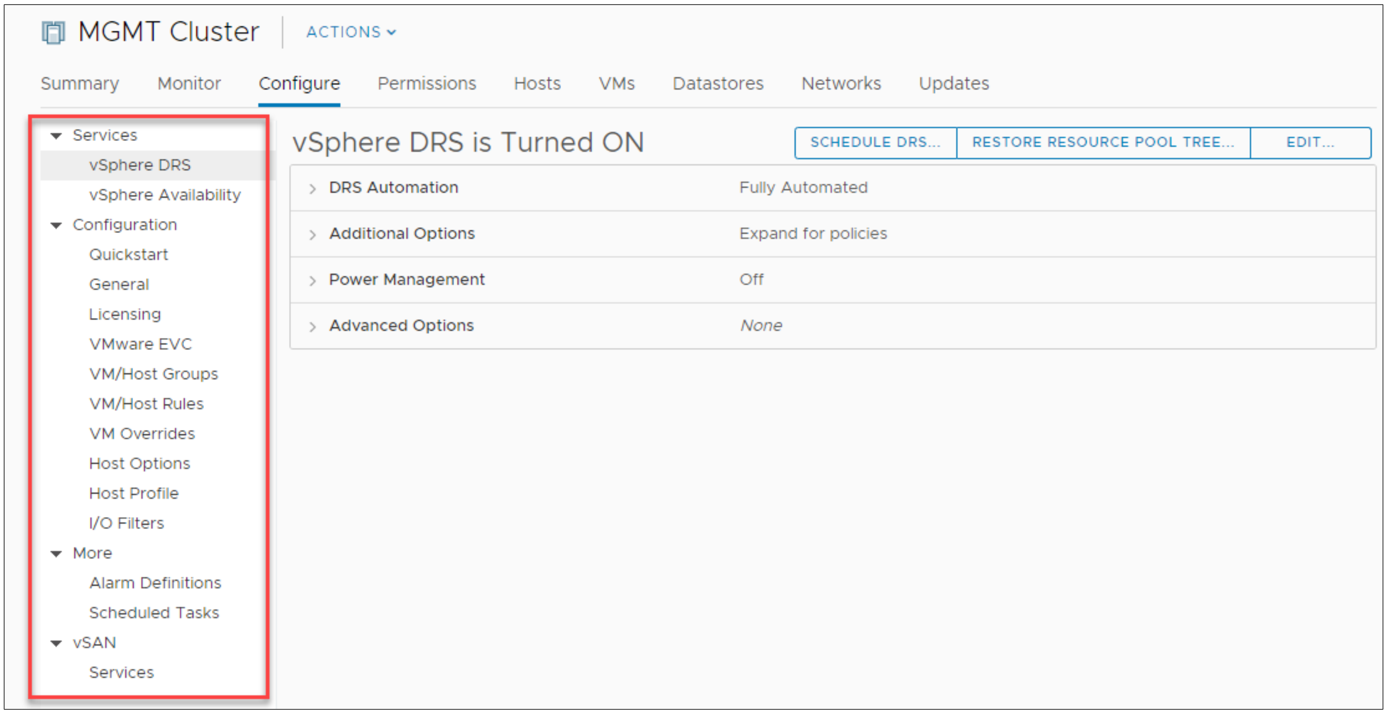
Here is a small table showing the differences between the switches.

| 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 1.9 – Describe the purpose of cluster and the features it provides*

A vSphere cluster is a group of ESXi host machines. When grouped together, vSphere aggregates all of the resources of each host and treats it like a single pool. There are a number of features and capabilities you can only do with clusters. Here is a screenshot of what you have available to you. I will now go over them.



vSphere DRS is Turned ON

| | |
|---|---|
| DRS Automation | Fully Automated |
| Additional Options | Expand for policies |
| Power Management | Off |
| Advanced Options | *None* |

Under Services you can see DRS and vSphere Availability (HA). You also see vSAN on the list, as vSAN requires a cluster as well. We've already covered HA and DRS a bit but there are more features in each.

### DRS

DRS Automation – This option lets vSphere make VM placement decisions or recommendations for placement. I trust them with Fully Automated as you can see in the window above. There are a few situations here and there where you might not want to, but 90% of the time I would say trust it. The small use cases where you might turn it off might be something like vCD deployments, but you could also just turn down the sensitivity instead. You have the following configuration options:

### Automation

- Automation Level – options are Fully Automated, Partially Automated and Manual. Fully automated provides placement at VM startup and moves VMs as needed based on Migration Threshold. Partially Automated places the VM at startup and makes recommendations for moving but doesn't actually move without approval. Manual will only make recommendations and requires you to accept them (or ignore).
- Migration Threshold – This is how sensitive the cluster is to resource imbalance. It is based on a scale of 1-5, 5 being the most sensitive. If you set it to 5, if vSphere thinks there is any benefit to moving the VM to a different host, it will do so. 1 is lazy and won't move anything unless it has to satisfy cluster constraints. 3 is default and usually a good balance.

- Predictive DRS – Using real-time metrics and metrics pulled in through vRealize Operations Manager, vSphere tried to predict (based on past performance) when additional resources might be needed by a VM and move it to a host that can provide them.
- Virtual Machine Automation – This allows you to override DRS settings for individual VMs.

**Additional Options**

- VM Distribution – This allows you to try to spread the number of VMs evenly through your cluster hosts. This prevents any host from being too heavy with VMs even though it might have the resources to support them.
- Memory Metric for Load Balancing – This load balances your VMs across hosts based on consumed memory instead of active memory. This can bite you if you overcommit a host's memory if all your hosts actually start using the memory you have assigned to them. So don't overcommit if you use this setting.
- CPU Over-Commitment – You can limit the amount of over-commitment for CPU resources. This is done on a ratio basis. (20 vCPUs : 1 physical CPU for example)

**Power Management**

- DPM – Distributed Power Management (should be Dynamic Power Management 😊). This allows you to keep the hosts turned off unless they are needed to satisfy resource needs. This saves power in your datacenter. It will use Wake-On-LAN, IPMI, iDRAC, or iLO to turn the hosts on. You can override individual hosts.
- Automation Level – You can set this to Manual or Automatic
- DPM Threshold – Just like DRS Migration Threshold, this changes sensitivity on a scale of 1-5, with 5 being the most sensitive. If resource utilization gets high, DPM will turn on another host to help with the load.

**vSphere Availability (HA)**

There are a number of configuration options to configure. Most defaults are decent if you don't 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 plugin and based on those messages will migrate VMs to a different host due to 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 will allow 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 better and give you wayyy more control than in the past.

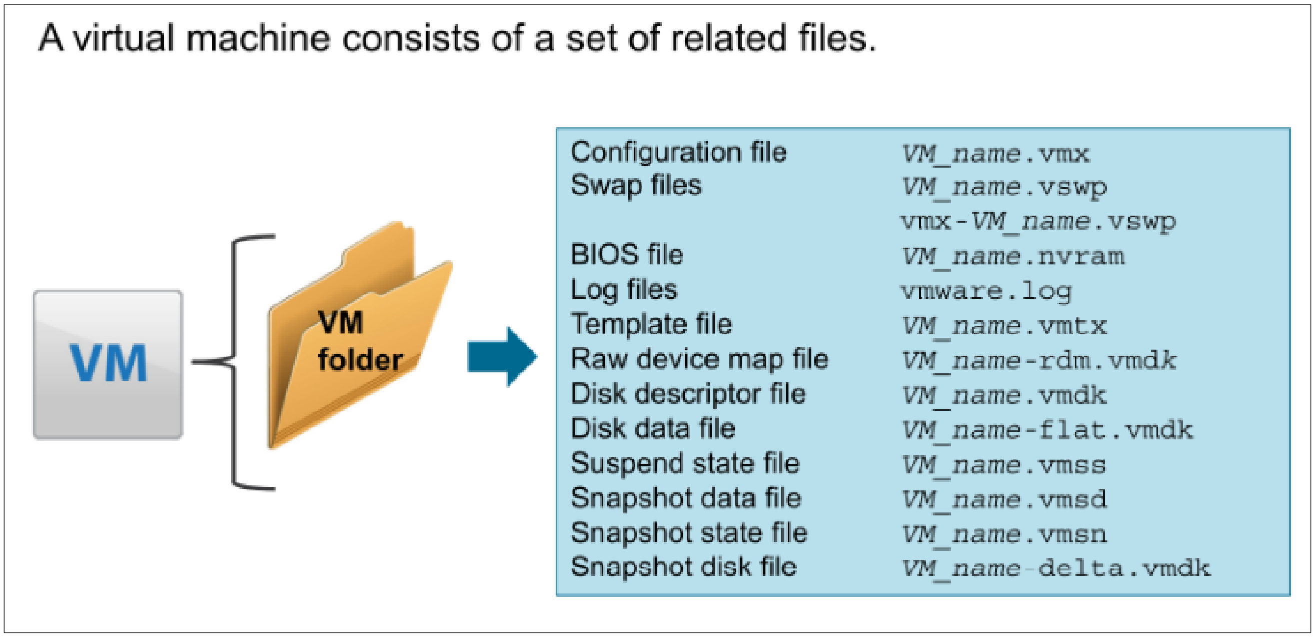
- Admission Control – What good is a feature to restart VMs if you don't have enough resources to do so? Not very. Admission Control is the gatekeeper that makes sure you have enough resources to restart your VMs in the case of host failure. You can ensure this a couple of ways. Dedicated failover hosts, 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 no VMs until there is a host failure. This is the most expensive (other than a 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. **Cluster Resources Percentage** looks at 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 will prevent new VMs from turning on.
- Heartbeat Datastores – This is used to monitor hosts and VMs when the HA network as failed. Using this it can determine if the host is still running or if a VM is still running by seeing the lock files. This automatically tries to make sure that it has at least 2 datastores that all the hosts have connectivity 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 will 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.

Clusters allow for more options then I've already listed. You can set up Affinity and Anti-Affinity rules. These are rules setup to keep VMs on certain hosts, or away from others. You might want a specific VM running on a certain host due to licensing or for a specific piece of hardware only a specific host has. Anti-affinity rules might be setup for something like Domain Controllers. You wouldn't place them on the same host for availability reasons, so you would setup an Anti-Affinity rule so that both of them would always be on different hosts.

EVC Mode is also a cool option enabled by clusters. EVC or Enhanced vMotion Compatibility allows you to take different generation hosts and still allows you to migrate them. Different generation processors have different features and options on them. EVC masks the newer ones so there is a level feature set. This means you might not receive all the benefits of a newer processors though. And a lot of newer processors are more efficient therefore lower clock speed. If you mask off those efficiencies, then you are just left with the lower clock speeds. Be mindful of that when you use it. You can enable it on a per VM basis making it more useful.

## *Objective 1.10 – Describe virtual machine (VM) file structure*

A VM is nothing more than files and software. Hardware is emulated. It makes sense to understand the files that make up a VM then. Here is a picture depicting files you might see in a VM folder lifted from VMware's book.



A virtual machine consists of a set of related files.

| | |
|---|---|
| Configuration file | VM_name.vmx |
| Swap files | VM_name.vswp |
| | vmx-VM_name.vswp |
| BIOS file | VM_name.nvram |
| Log files | vmware.log |
| Template file | VM_name.vmtx |
| Raw device map file | VM_name-rdm.vmdk |
| Disk descriptor file | VM_name.vmdk |
| Disk data file | VM_name-flat.vmdk |
| Suspend state file | VM_name.vmss |
| Snapshot data file | VM_name.vmsd |
| Snapshot state file | VM_name.vmsn |
| Snapshot disk file | VM_name-delta.vmdk |

Now as for an explanation of those files.

- .vmx file – This is the file vSphere uses to know what hardware to present. This is essentially a list of the hardware and locations of other files (like the virtual disk). It is also the file used when adding a VM to vSphere inventory.
- .vswp – This file is what vSphere uses much the same way Microsoft uses a page file. When it runs out of actual physical memory or experiences contention on the host, it will use this file to make up the difference. As expected, since this is using a disk instead of RAM, it will be much slower.
- .nvram – This file emulates a hardware BIOS for a VM.
- .log – These are log files for the individual VM. It captures actual errors from the VM such as when a Microsoft Windows machine blue screens (crashes). These can be used for troubleshooting purposes. The file name increments vSphere maintains up to 6 log files at a time. vSphere will delete the oldest file first as it needs to.
- .vmtx – This only occurs if the VM is a template. In that case the. vmx will change to a. vmtx
- .vmdk – This is the disk descriptor file. No actual data from the VM is housed here. Rather the location of the blocks of the actual disk and other information about it are found inside.
- -flat.vmdk – This is the actual data of the VM. This is hidden unless you look in the CLI.  If the VM has multiple disks there will be more than one of this and the. vmdk
- .vmsd – This is the snapshot list. If there are no snapshots, then this file is empty.
- -delta.vmdk – this file is the delta disk if there is a active snapshot. The original flat-vmdk is frozen and all I/O is routed to this -delta instead.

- -.ctk – Not shown in the graphic above, this is the Change block tracking file. This is used for programs like vSphere Data Protection or other backup programs.
- -.lck – Also not shown in the graphic, this is a lock file placed in the directory showing that the VM is turned on (or the host thinks it is).

## *Objective 1.11 – Describe vMotion and Storage vMotion technology*

There are several ways to move VMs around in your environment. vMotion and Storage vMotion are two types of migration. The first thing I do, when I taught this, was ask, what do you really need to move to move a VM? The main piece of what make up a VM is the memory. CPU resources are used briefly. When you perform a vMotion, what you are really doing is just moving active memory to a different host. The new host will then start working on tasks with the CPU.  All pointers in the files that originally point to the first host have to be changed as well. So how does this work?

1. First copy pass of the memory is moved over the new host. All users continue to use the VM on the old host and possibly make changes. vSphere will note these changes in a modified memory bitmap on the source host.
2. After the first pass happens, the VM is quiesced or paused. During this pause, the modified memory bitmap data is copied to the new host.
3. After the copy, the VM begins running on the new host. A reverse ARP is sent that notifies everyone that this is where the VM is now and forward requests to the new address.
4. Users now use the VM on the new host.

Storage vMotion is moving the VM files to another datastore. Let's go through the steps

1. Initiate the svMotion in the UI.
2. vSphere uses something called the VMkernel data mover or if you have a storage array that supports vSphere Storage APIs Array Integration or VAAI to copy the data.
3. A new VM process is started
4. Ongoing I/O is split using a "mirror driver" to be sent to the old and new vmdks while this is ongoing.
5. vSphere cuts over to the new VM files.

This is slightly different than the vMotion process as it only needs one pass to copy all the files due to using the mirror driver.

There is one other type of migration called Cross-Host vSphere vMotion or Enhanced vMotion depending on who you ask. This is a combination of vMotion and svMotion at the same time. This is also notable because this allows you to migrate a VM while using local storage.

There are limitations on vMotion and svMotion. You need to be using the same type of CPUs (Intel or AMD) and the same generation, unless you are using EVC. You should also make sure you don't have any hardware that the new host can't support. CD-ROMs etc. vMotion will usually perform checks before you initiate it and let you know if there are any issues. You can migrate up to 4 VMs at the same time on a 1Gbps or 8 VMs on a 10Gbps network per host. 128 concurrent vMotion is the limit per VMFS datastore.

# Section 2 – VMware Products and Solutions

## *Objective 2.1 – Describe vSphere integration with other VMware products*

VMware has just a few products on the market (/sarcasm), and they show no letup in acquiring other companies and expanding to new technologies. One thing I appreciate about them is their ability to take what they buy, make it uniquely theirs, and integrate it with their current solutions. While this is not always done quickly and it make take a few versions, it usually pays dividends. Other products such as their Software Defined Networking product, NSX-V and T, and vSAN (SDS storage) and more, round out their offerings making it a complete solution for their customers. While definitely not altruistic, having a single place to get a complete solution can make life easier. Let's look at some of the VMware products that are commonly used with vSphere core products.

If you look at products grouped together on VMware's download site, you'll see the core vSphere products of ESXi and vCenter. You also see Log Insight, NSX, Operations, and Orchestrator. I will try to give you a high-level of each of those products and how they fit into the vSphere world.

**vRealize Log Insight**

vRealize Log Insight is a syslog server on steroids. It is described as a Log Management and Analytics Tool by VMware. It integrates with vCenter Server and vRealize Operations. Log Insight can be used as a regular syslog server for other solutions not in VMware. Using it as a single logging repository and being able to search across your entire company's infrastructure is its true superpower. But wait… there's more.

You can also load content packs to manage specific solutions. One example of this is I am using a specially created Rubrik content pack that allows me to create specific dashboards to monitor my backups. Log Insight has the ability to have multiple users and assign them separate permissions to create their own dashboards and metrics. You can see my walkthrough on Log Insight (albeit 4.3 instead of 4.6) here. I also have a few videos to show you how you might customize dashboards here and how you can track a error in the logs here.

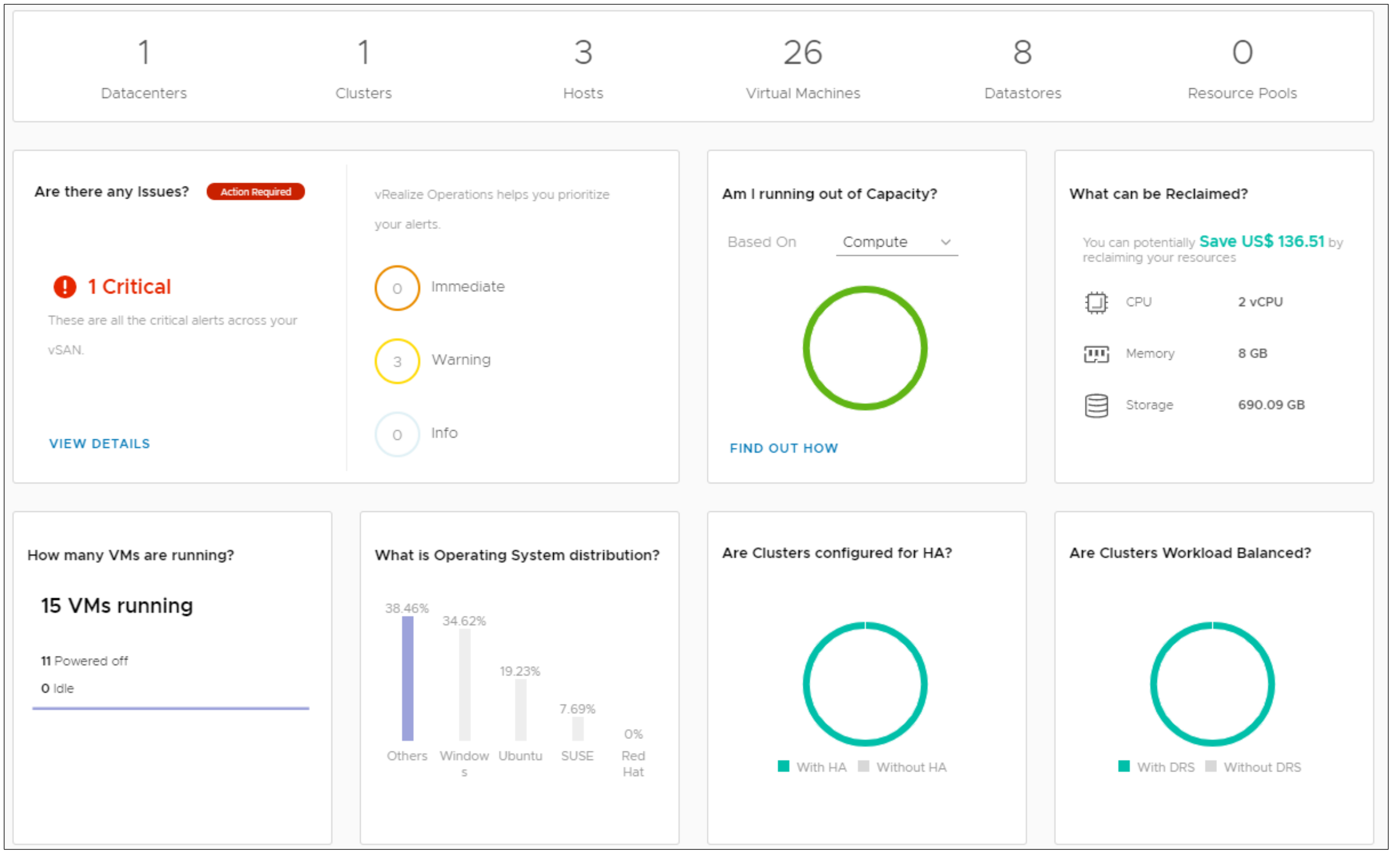
**VMware NSX**

What VMware did for Server hardware they did with Networking as well. While ESXi and vCenter Server already have VSS and VDS, this is the next step in networking evolution. Using NSX you can implement normally difficult configurations such as micro-segmentation in your datacenter with ease. Being able to do this all from a single UI makes it easy and saves time. Once the initial configuration of the physical networking is done, everything thereafter can be accomplished in VMware's HTML5 client. Creating switches, routers, load balancers, firewalling, you name it.

Because NSX's technology, ESXi essentially believes it is on a large L2 network allowing you to do things impossible before, such as vMotion over large geographic distances. NSX brings a lot to the table. There is a lot to learn about it, however and it has its own certification track.

**vRealize Operations**

vRealize Operations is a tool used to facilitate performance optimization, capacity management, forecasting, remediation, and compliance. It integrates right into the HTML5 client and keeps you constantly aware of how your environment is performing. Not only does vRealize Operations integrate with ESXi and vCenter, it also integrates with NSX and Log Insight. Here is a pic of what it looks like in the HTML5 client



1 Datacenters | 1 Clusters | 3 Hosts | 26 Virtual Machines | 8 Datastores | 0 Resource Pools

Are there any Issues? Action Required

1 Critical

These are all the critical alerts across your vSAN.

VIEW DETAILS

vRealize Operations helps you prioritize your alerts.

0 Immediate

3 Warning

0 Info

Am I running out of Capacity?

Based On: Compute

FIND OUT HOW

What can be Reclaimed?

You can potentially Save US$ 136.51 by reclaiming your resources

CPU 2 vCPU

Memory 8 GB

Storage 690.09 GB

How many VMs are running?

15 VMs running

11 Powered off

0 Idle

What is Operating System distribution?

Are Clusters configured for HA?

Are Clusters Workload Balanced?

I also have a few videos on how to perform actions in vSphere Operations here. While this is an old version it serves well to show you some of the things you can use vRealize Operations for.

You have a large number of dashboards to choose from and monitor. You can see things like disk usage and capacity graphically making it easy to pick out potential problems at a quick glance. Doing this paper vRealize notified I've been running my Plex Server on a snapshot for a long period of time… I didn't have any idea until it told me. (Snapshot was created by Update Manager upgrade). Short story, you need this in your life.

**vRealize Orchestrator**

Most people know about the app IFTTT for your phone. This is kind of like that but way more powerful. Using vRealize Orchestrator you can create workflows that can perform a plethora of different tasks. It also integrates with vRealize Automation to create even more complex jobs. Using vRealize Orchestrator, you can:

- Configure software or virtual hardware
- Update databases
- Generate work order tickets
- Initiate system backups

And much more. This integrates with all of VMware's other products and is a drag and drop worklflow solution.

## *Objective 2.2 – Describe HA solutions for vSphere*

We already went over this, but we'll touch on it again. The main High Availability solutions VMware provides are vMotion, svMotion and HA using clusters. I will include both HA parts so that you can read about HA in one fell swoop.

**High Availability**

HA works by pooling hosts and VMs into a single resource group. Hosts are monitored and in the event of a failure, VMs are re-started on another host. When you create a HA cluster, an election is held and one of the hosts is elected master. All others are slaves. 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. HA has other important jobs. One is determining priority and order that VMs will be restarted when an event occurs. HA also has VM and Application Monitoring. Using this prompts HA to restart a VM if it doesn't detect a heartbeat received from VM Tools. Application Monitoring will do the same 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. One last thing to note. In the past, VMware tried to trick people by using the old name for HA which was FDM or Fault Domain Manager

There are a several configuration options to configure. Most defaults work without drama 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 will migrate VMs to a different host due to possible impending doom of the original 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 then 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 host failure. You can ensure this a couple of ways. Dedicated failover hosts, cluster resource percentage, slot policy, or you can disable it (not good 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 a 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 off that base slot size. **Cluster Resources Percentage** looks at total resources needed and total available and tries to keep enough resources to permit you to lose the number of hosts you specify (subtracting amount 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 turning on.
- Heartbeat Datastores – Used to monitor hosts and VMs when the HA network as 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 will 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 Fault Tolerance and Disaster Recovery.

Fault Tolerance or FT creates a second live shadow copy of a VM. In the even the primary goes down, the secondary kicks in and it then creates a new shadow VM.

Disaster Recovery options include vSphere Replication and Site Recovery Manager. Both of these can be used in conjunction to replicate a site or individual VMs to another site in case of failure or disaster.

## *Objective 2.3 – Describe the options for securing a vSphere environment*

There are a number of options available to secure your vSphere environment. We will start with ESXi and move on to a few others.

**ESXi Security**

- Limit access to ESXi – this goes for both the physical box but also any other way of accessing it. SSH, DCUI, or remote console via IPMI or iDRAC/iLO etc. You can also take advantage of lockdown modes to limit access to just vCenter.
- Use named users and least privilege – If everyone is root than no one is special. Only give users that need it, access. Even then only give them the access and rights they need to do their job. Make sure they all log in as the user you give them. This allows for tracking and accounting.
- Minimize open ports – your ESXi host has a stateless firewall but if all the ports are open, it's not providing any protection for you.
- Smart Card authentication – ESXi now supports smart cards for logging on instead of user name and passwords.
- Account lockouts – After a number of incorrect tries to log in, have the account lock.
- Manage ESXi certificates – While there is a Certificate Authority in vCenter, you might want look into using third-party or enterprise CA certificates.
- VIB Integrity – try to use and only allow your ESXi hosts to accept VMware accepted or VMware Certified VIBs.

**vCenter Server Security**

- Harden all vCenter host machines – make sure all security patches and the host machines are up to date.
- Assign roles to users or groups – This allows you to better keep track of what users are allowed to do if they are part of a role.
- Setup NTP – time stamps will be accurate and allow you to better track what is going on in your environment.
- Configure Single Sign On – Keep track of the identity sources you allow to authenticate to your vSphere environment.
- vCenter Certificates – remove expired or revoked certificates and failed installations.

**VM Security**

- Protect the guest operating system – Keep your OS up to date with patches and any anti-malware or anti-spyware. Most OSs also have a firewall built-in. Use that to keep only necessary ports open.

- Disable unnecessary functionality – Turn off and disable any services not needed. Turn off things like HGFS (host-guest filesystem) that allows you to copy and paste between the VM and remote console.
- Use templates and scripted installations – After you spend all the time making an OS secure, use that as a template so that you don't have to perform the same on the next machine. This also makes sure you don't forget settings or configurations that may end up being disastrous. Script management of machines and installations for the same reason.
- Minimize use of the virtual machine console – Just like you would secure access to the physical machine, you should secure access and use sparingly the console.
- Use UEFI secure boot when possible – If the OS supports it, you can use this to prevent changes to the VM.

Network Security

- Isolate network traffic – Separation of network traffic into segments allows you to isolate important networks. A prime example of this is creating a management network that is separate from regular VM traffic. You can perform this easily using VMware NSX or even as simple as creating a separate subnet and locking that down virtually or physically to ports.
- Use firewalls – Again using NSX this becomes really simple to create firewall and micro-segmentation. Mentioned above, you can also utilize firewalls in the OS but that can get unwieldy with 1,000s of VMs. Physical firewalls are a staple as well.
- Consider Network Policies – Switches in your virtual environment have security policies you can implement to prevent malicious attacks. These are promiscuous mode, MAC address changes, and forged transmits.
- Secure VM networking – same as above with securing OSs and firewalling.
- VLANs – These can be used to segment your network and provide additional security. This also breaks up your broadcast domain which can cut down on unwanted broadcast traffic.
- Secure connection to your Storage – Usually companies setup separate networks for their storage. This is for security but also performance. You can also implement authentication on your storage array such as CHAP. Fibre Channel is particularly secure as it is difficult to tap a fibre cable.

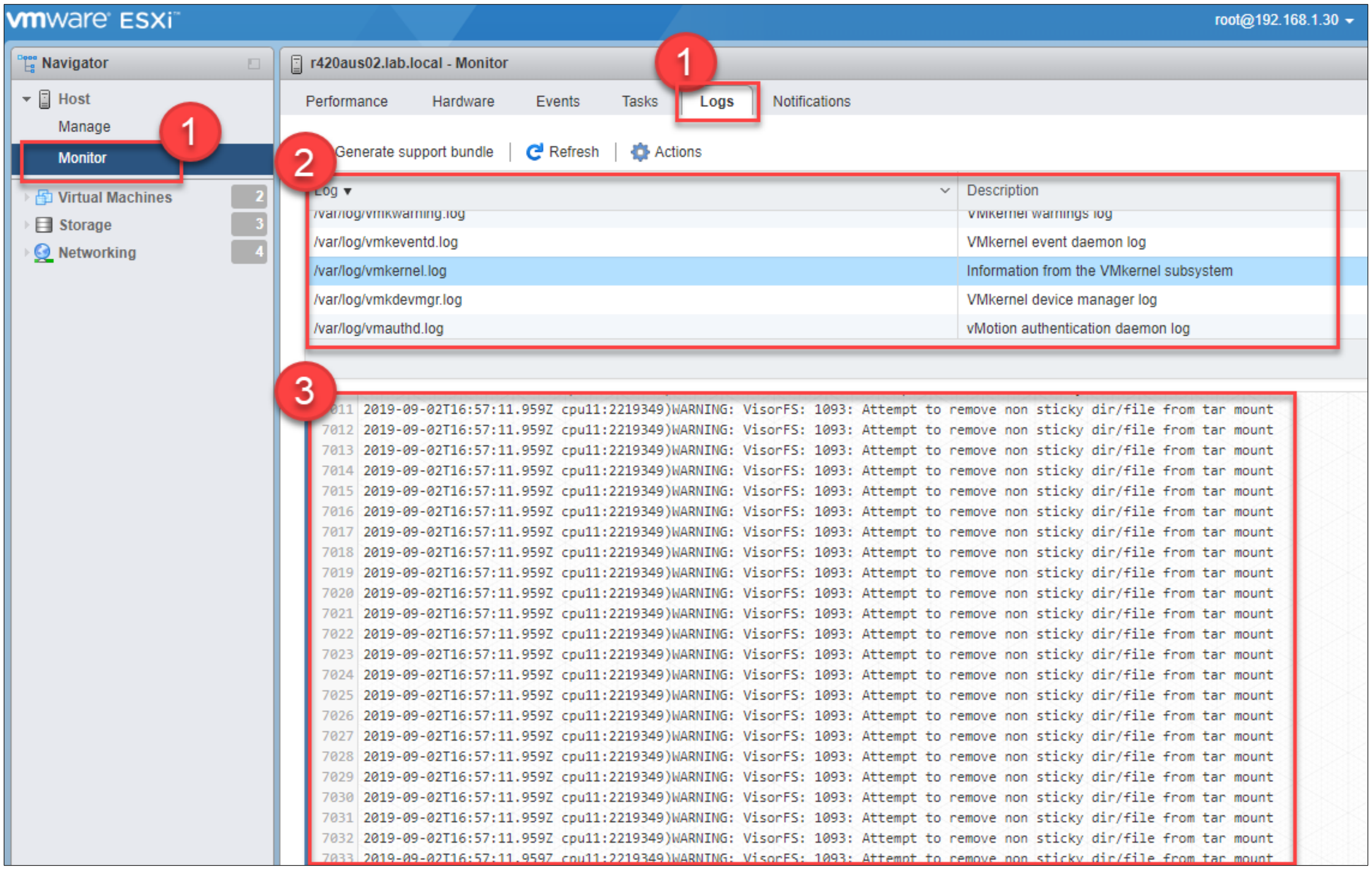
# Section 4 – Installing, Configuring, and Setting Up a VMware vSphere Solution

## *Objective 4.1 – Understand 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

Where before the easiest option was to open a 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.



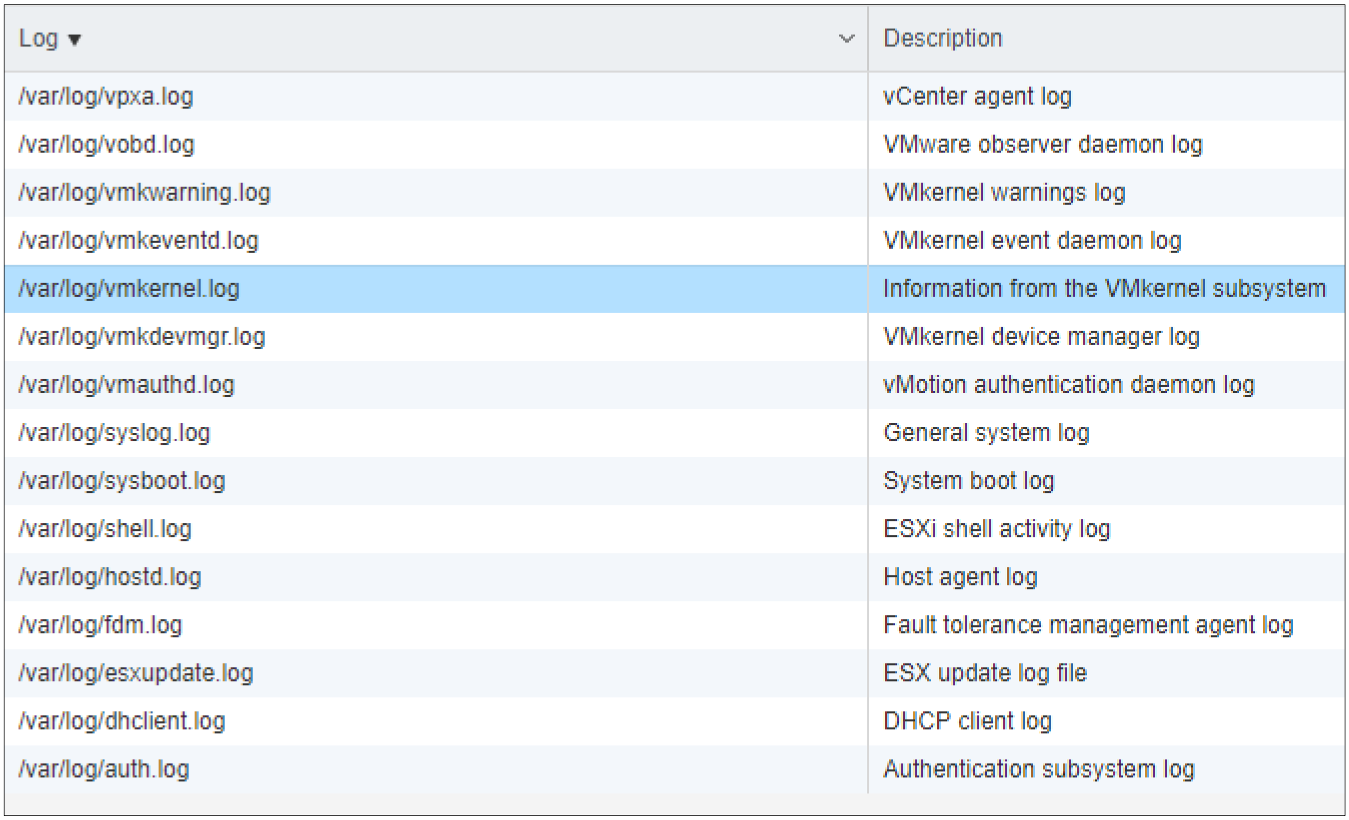
| Log ▾ | Description |
|---|---|
| /var/log/vmkwarning.log | VMkernel warnings log |
| /var/log/vmkeventd.log | VMkernel event daemon log |
| /var/log/vmkernel.log | Information from the VMkernel subsystem |
| /var/log/vmkdevmgr.log | VMkernel device manager log |
| /var/log/vmauthd.log | vMotion authentication daemon log |

```
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
2019-09-02T16:57:11.959Z cpu11:2219349)WARNING: VisorFS: 1093: Attempt to remove non sticky dir/file from tar mount
```

Here in the screenshot, you can see

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

And here is a list of the logs on the ESXi host along with a description for what the log keeps track of.



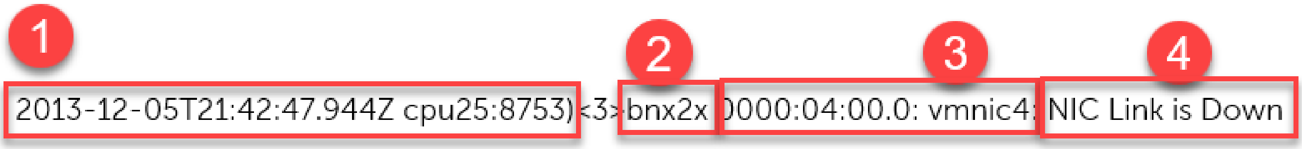
| Log ▾ | Description |
|---|---|
| /var/log/vpxa.log | vCenter agent log |
| /var/log/vobd.log | VMware observer daemon log |
| /var/log/vmkwarning.log | VMkernel warnings log |
| /var/log/vmkeventd.log | VMkernel event daemon log |
| /var/log/vmkernel.log | Information from the VMkernel subsystem |
| /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 a SSH session as well.

Alright so you got the log now... How do you use it? Here is a sample taken from a VMKernel.log. This 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 [ISID: 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.
```

Let’s decipher this a bit more.



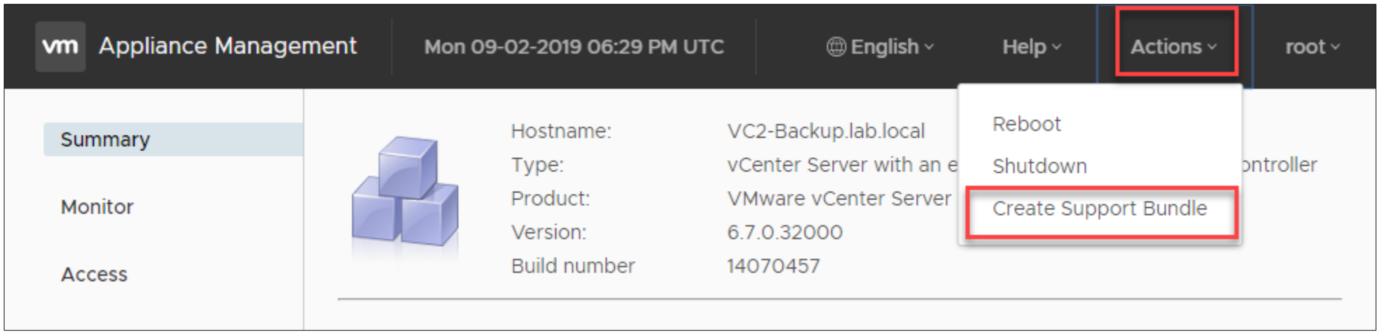
```
2013-12-05T21:42:47.944Z cpu25:8753)<3>bnx2x 0000:04:00.0: vmnic4: NIC Link is Down
```

1. This part is the time stamp of the log entry.
2. This is what is the reporter. In this case it is the bn2x 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 difficult 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 though.



Hostname: VC2-Backup.lab.local
Type: vCenter Server with an e... ontroller
Product: VMware vCenter Server
Version: 6.7.0.32000
Build number 14070457

This is accessing the Appliance Config at port 5480.

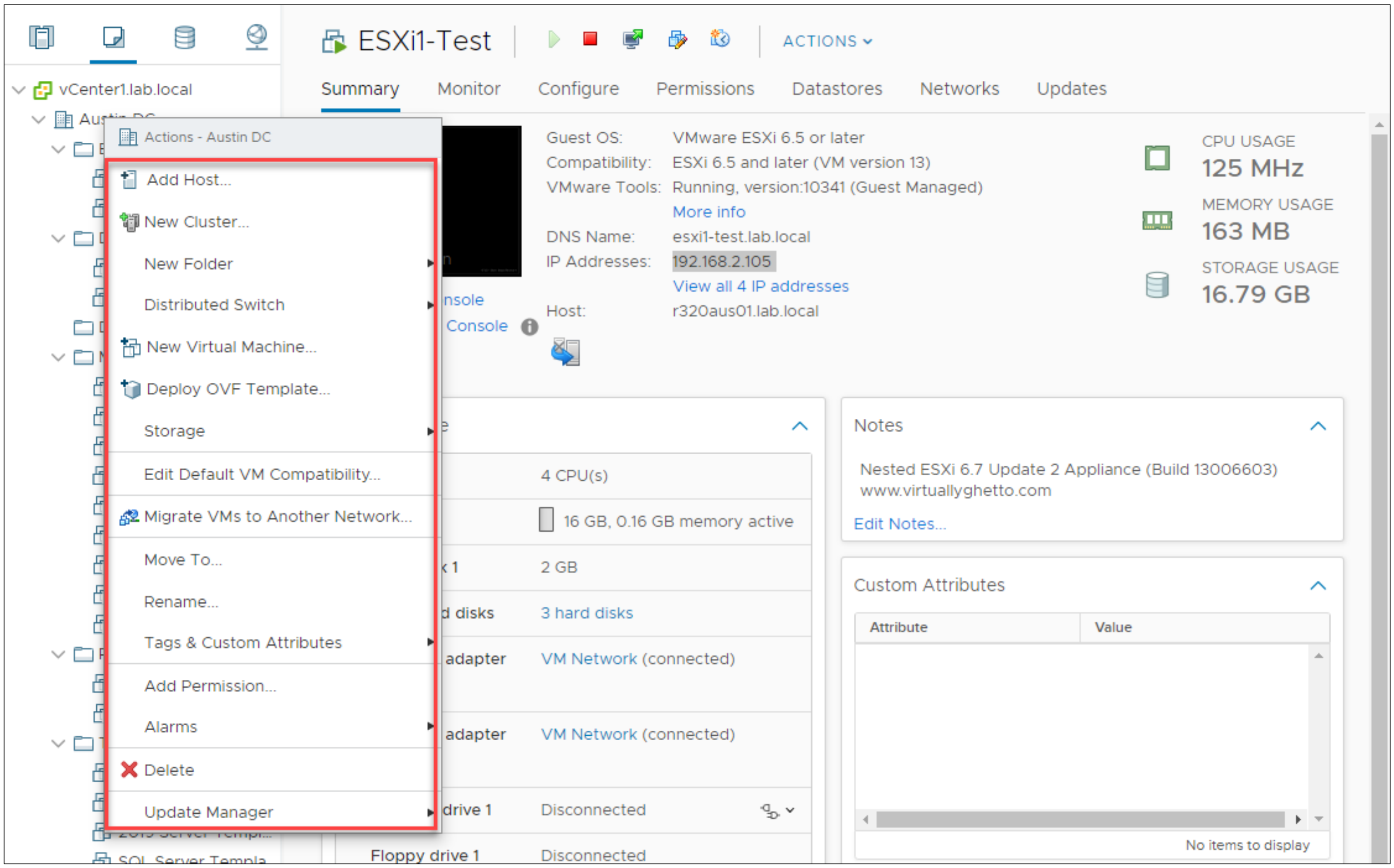
Once this is done downloading you have a decent size .tar file. You will need to unzip this a couple times. When you finally have a regular directory structure all the logs will be under the `/var/log/vmware` folder. Here is a list of the files and locations and what they do.

| Windows **vCenter Server** | **vCenter Server Appliance** | **Description** |
|---|---|---|
| **vmware-vpx\vpxd.log** | vpxd/vpxd.log | The main vCenter Serverlog |
| **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 vpxd 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 being streamed to Log Insight. You'll see output similar to what I mentioned above.

## *Objective 4.2 – Create and configure vSphere objects*

Creating and configuring objects can be done several ways. You can do this through the HTML5 client, or you can do this from the CLI using PowerCLI or use commands at the ESXi SSH prompt. Inside the HTML5 client it is as simple as right clicking on the parent object (such as a cluster) and then selecting Add Host or New Virtual Machine. This is the window you may see when you right click on the parent object:



Guest OS: VMware ESXi 6.5 or later
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Running, version:10341 (Guest Managed)
More info
DNS Name: esxi1-test.lab.local
IP Addresses: 192.168.2.105
View all 4 IP addresses
Host: r320aus01.lab.local

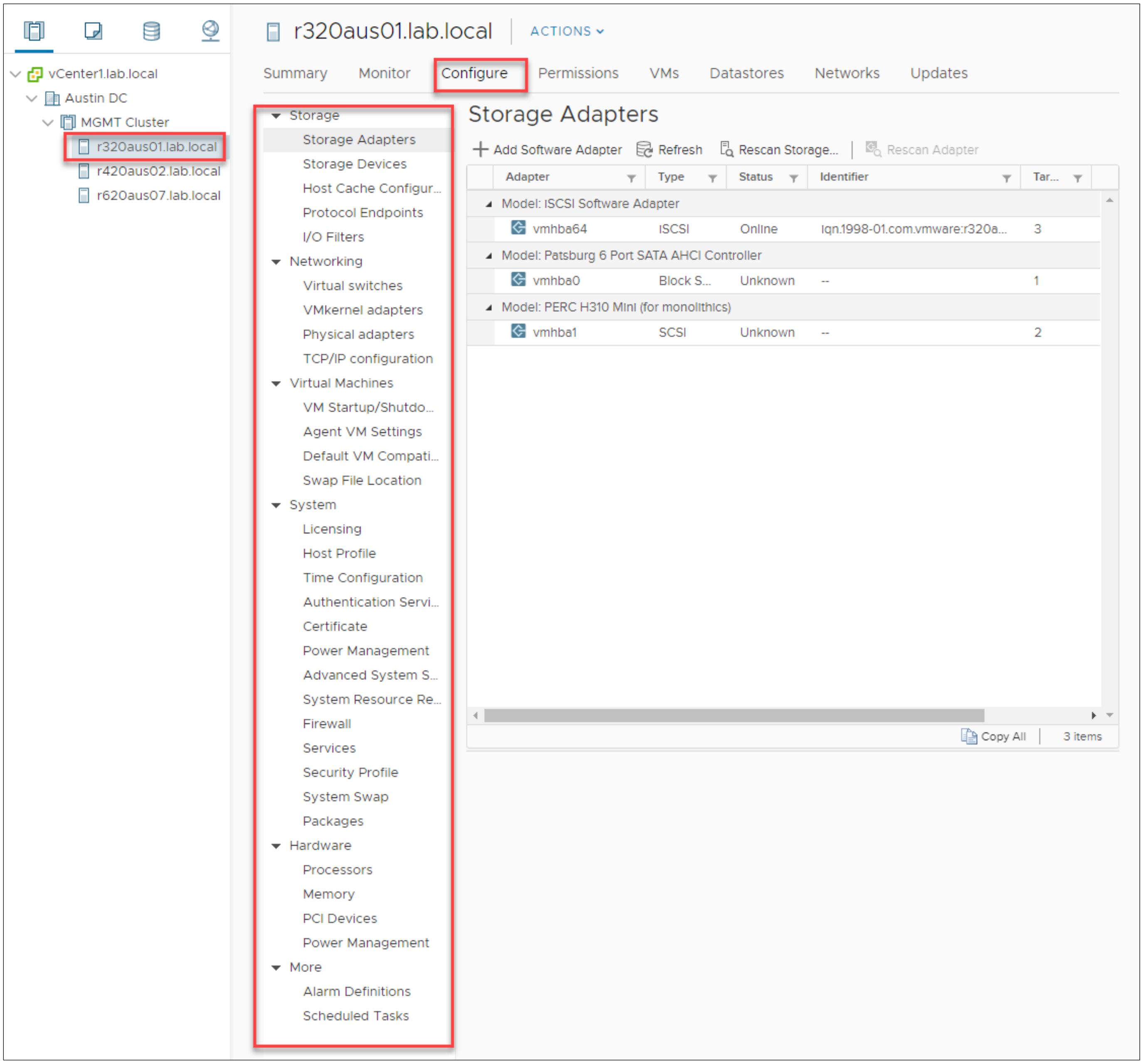
CPU USAGE 125 MHz
MEMORY USAGE 163 MB
STORAGE USAGE 16.79 GB

4 CPU(s)
16 GB, 0.16 GB memory active
k 1 2 GB
d disks 3 hard disks
adapter VM Network (connected)
adapter VM Network (connected)
drive 1 Disconnected
Floppy drive 1 Disconnected

Nested ESXi 6.7 Update 2 Appliance (Build 13006603)
www.virtuallyghetto.com

| Attribute | Value |
|---|---|

Configuring an object depends on the object. Configuring a VM is as simple as right clicking on it and Configuring Settings. You can also select the object and then use the center pane to bring up the Configure pane. This may give you different options to configure based on the object. Here is a screenshot of the Configure pane for a ESXi host.



Storage Adapters

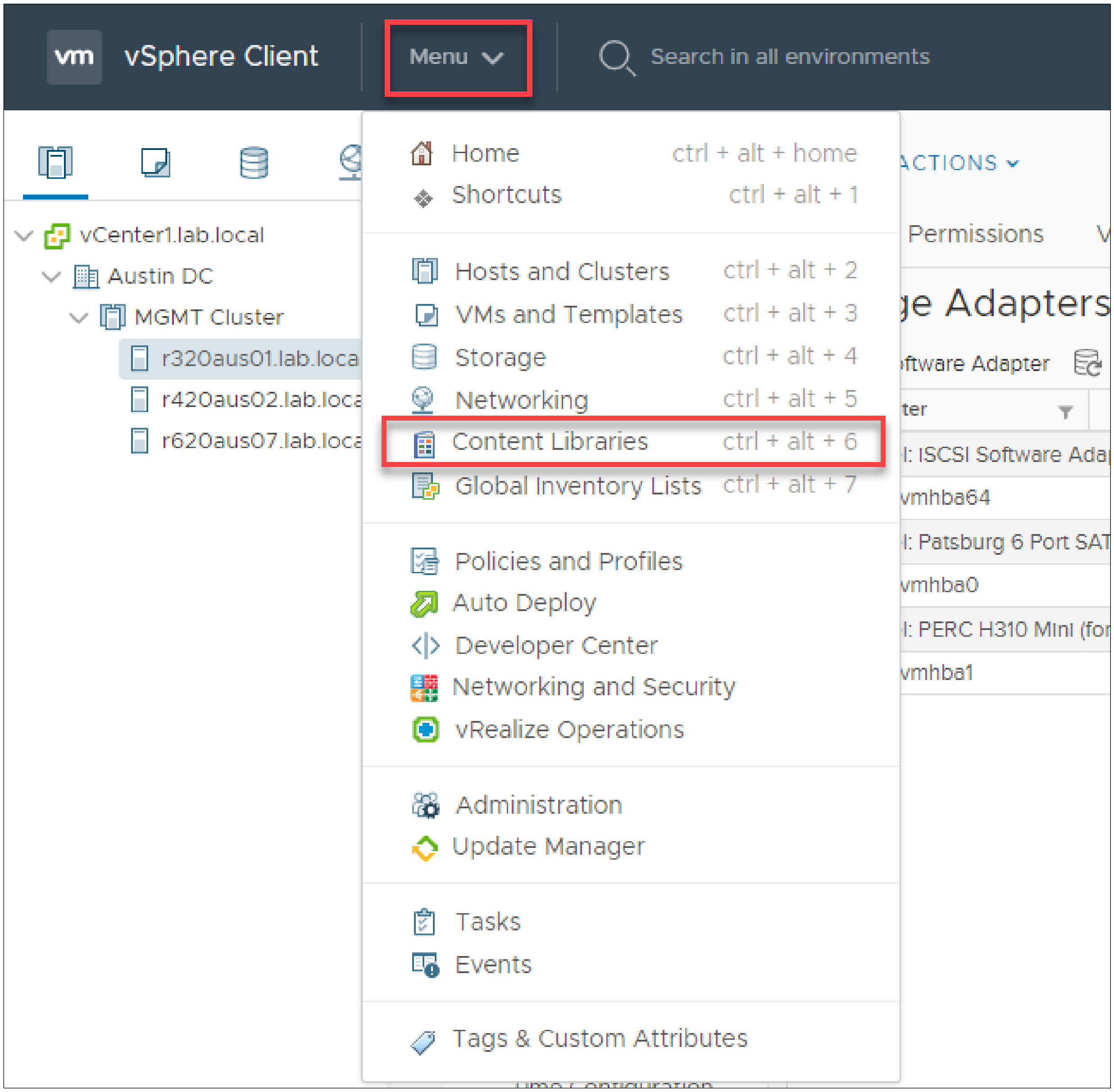
| Adapter | Type | Status | Identifier | Tar... |
|---|---|---|---|---|
| Model: iSCSI Software Adapter | | | | |
| vmhba64 | iSCSI | Online | iqn.1998-01.com.vmware:r320a... | 3 |
| Model: Patsburg 6 Port SATA AHCI Controller | | | | |
| vmhba0 | Block S... | Unknown | -- | 1 |
| Model: PERC H310 Mini (for monolithics) | | | | |
| vmhba1 | SCSI | Unknown | -- | 2 |

As you can see there are a number of ways to accomplish this task.

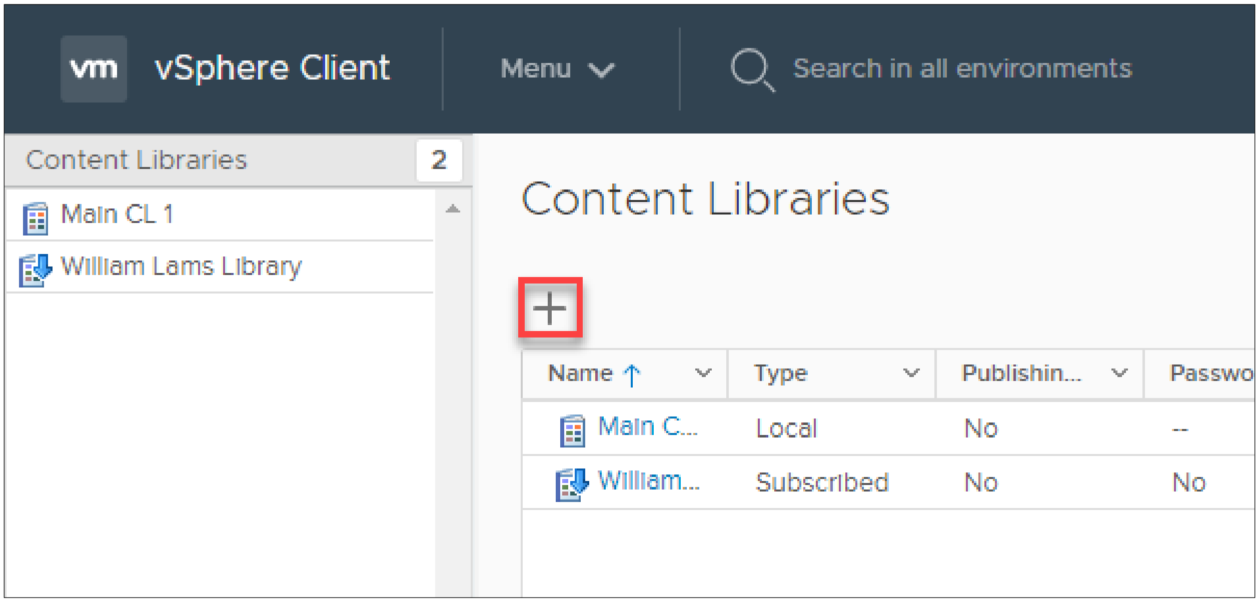
## *Objective. 4.3 – Set up a content library*

Setting up a content library is straightforward. To do this:

1. Click on Menu at the top of your screen and then select Content Libraries

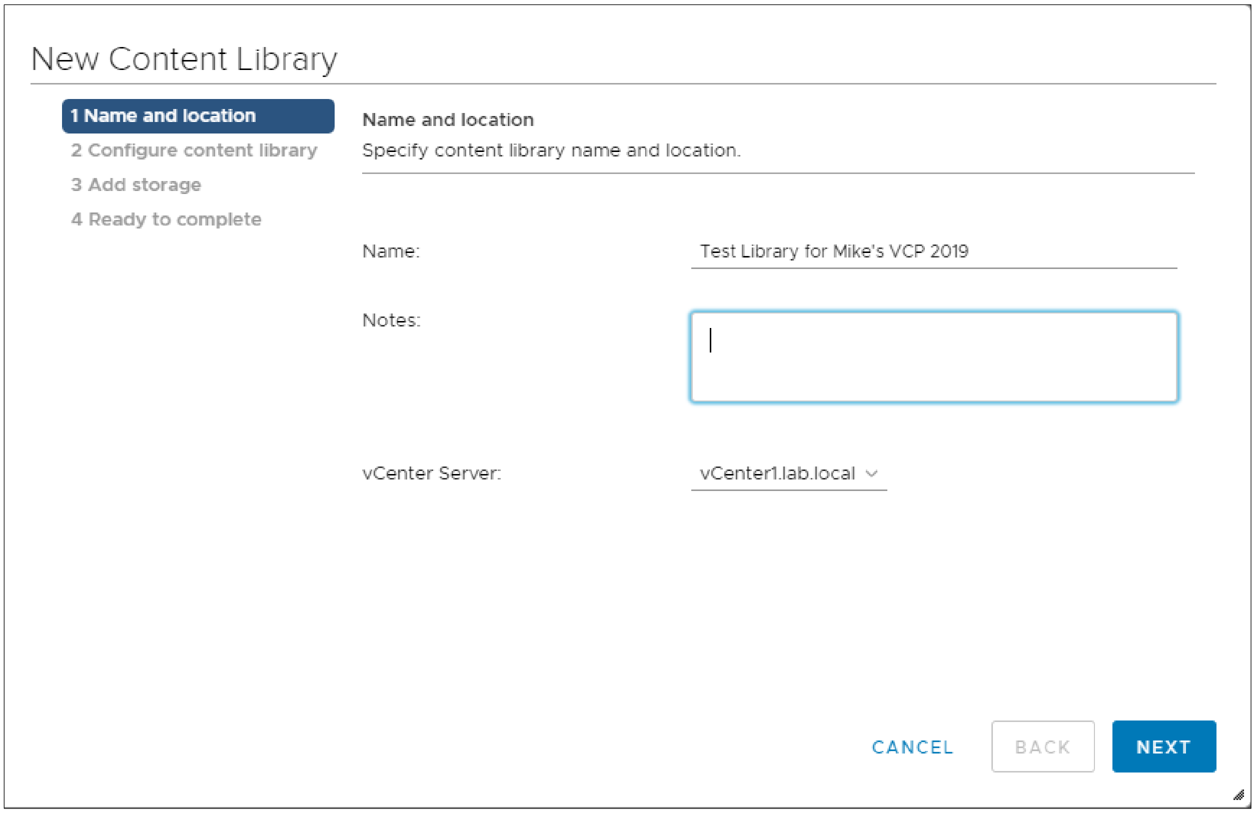


2. Click on the '+' to add a new Content Library



| Name | Type | Publishin... | Passwo |
|---|---|---|---|
| Main C... | Local | No | -- |
| William... | Subscribed | No | No |

3. Specify a Name for the library and any notes. Also if needed change what vCenter Server you will host this off of.



Name and location

Specify content library name and location.

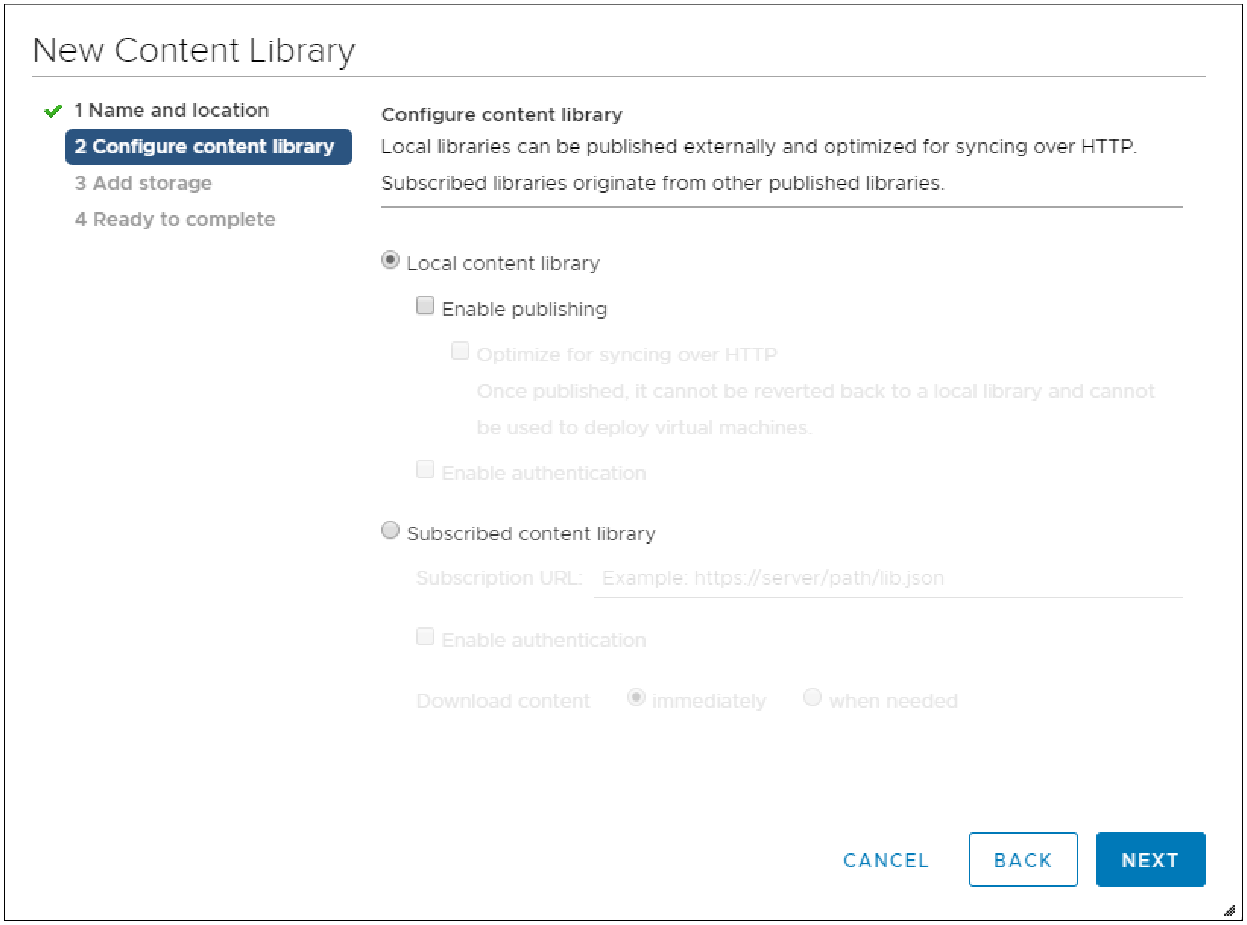
Name: Test Library for Mike's VCP 2019

Notes:

vCenter Server: vCenter1.lab.local

4. This screen has options for how you want to use it. This can be setup as a Local or you can Subscribe to someone else's library. If you do create a local library, do you want others to be able to subscribe

to it. If publishing, will they need to authenticate.



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

□ Optimize for syncing over HTTP

Once published, it cannot be reverted back to a local library and cannot be used to deploy virtual machines.

□ Enable authentication

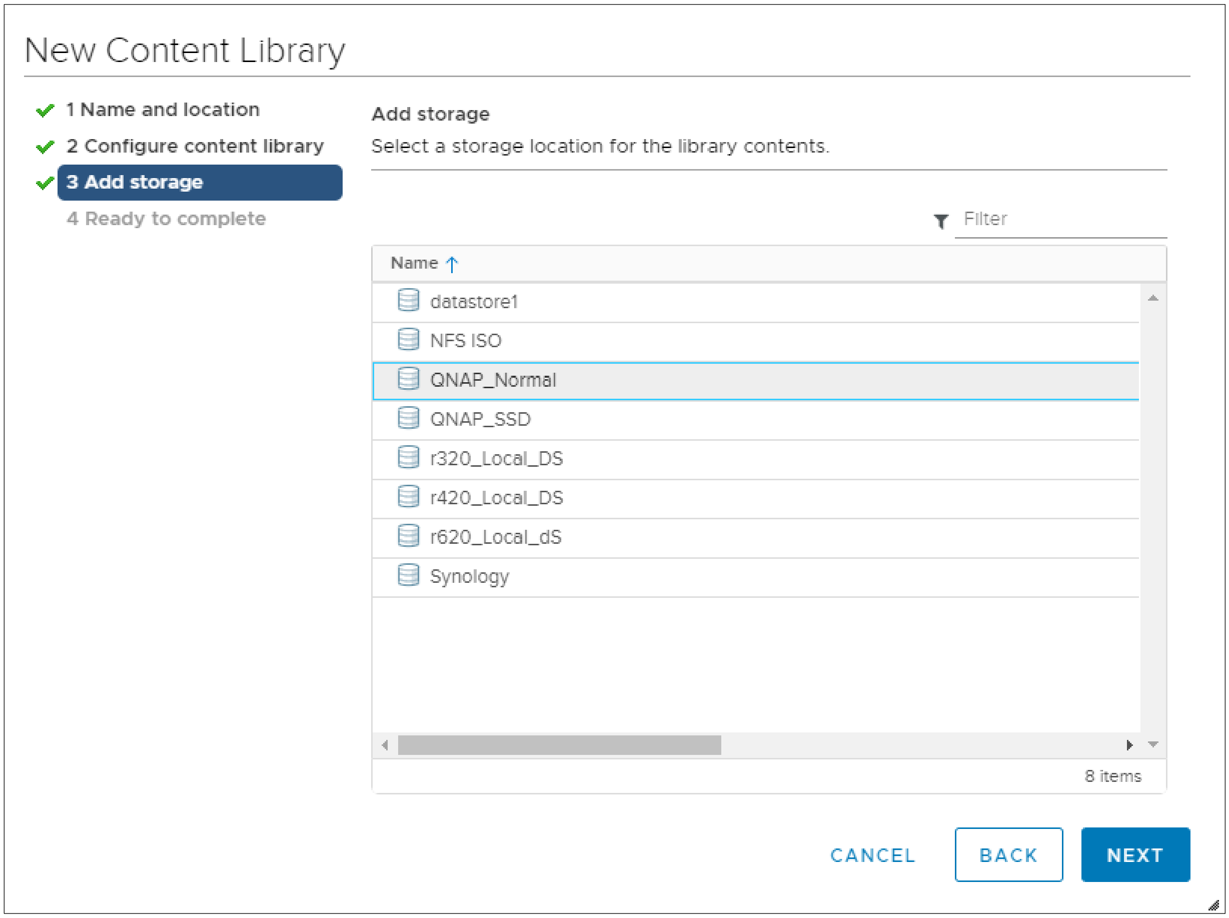
○ Subscribed content library

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

□ Enable authentication

Download content ● immediately ○ when needed

5. You need to store the Content Library somewhere. You do that on this screen.



New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library
- ✓ 3 Add storage
- 4 Ready to complete

Add storage

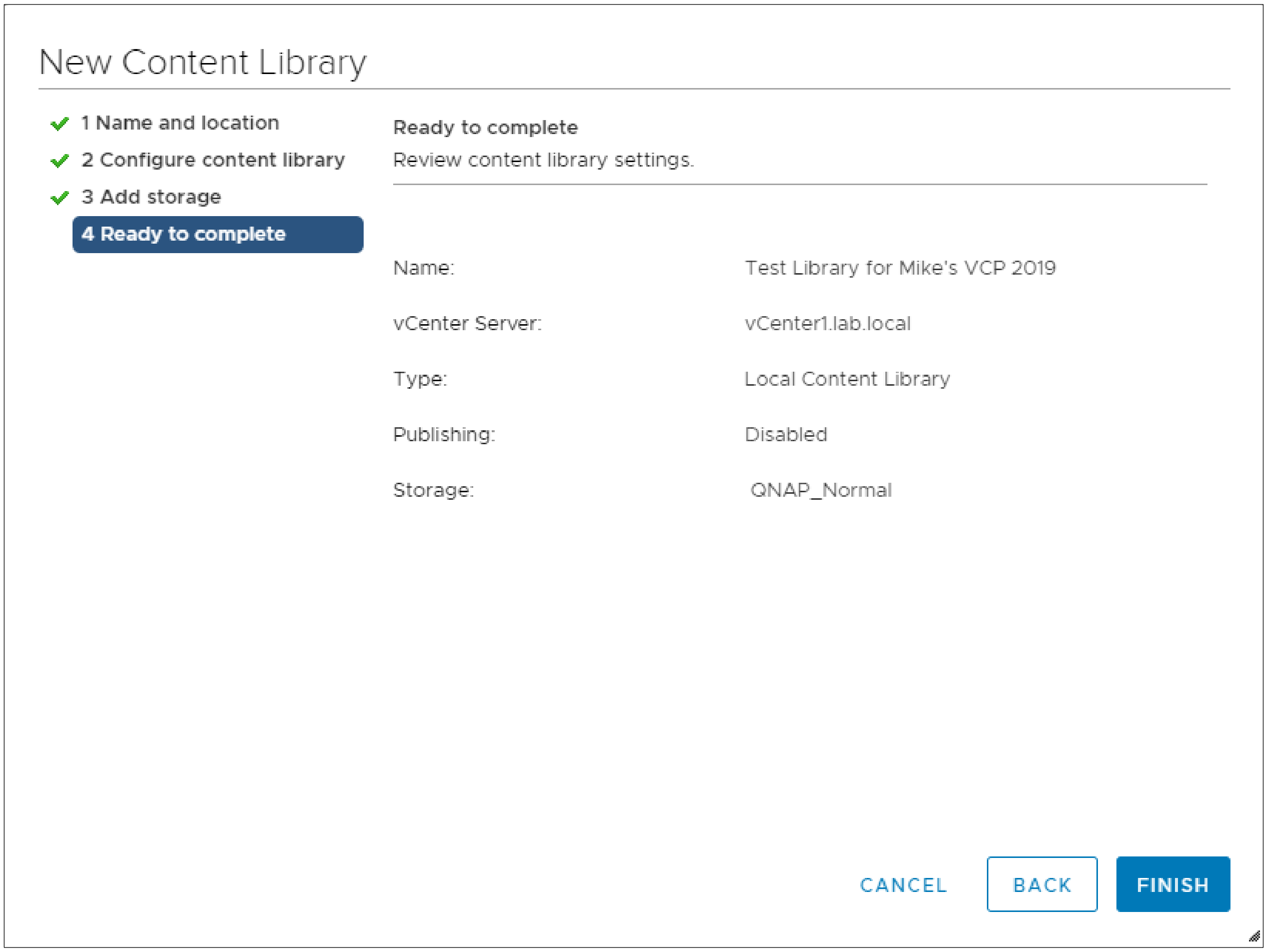
Select a storage location for the library contents.

Filter

| Name ↑ |
|---|
| datastore1 |
| NFS ISO |
| QNAP_Normal |
| QNAP_SSD |
| r320_Local_DS |
| r420_Local_DS |
| r620_Local_dS |
| Synology |

8 items

6. That's it! Click Finish



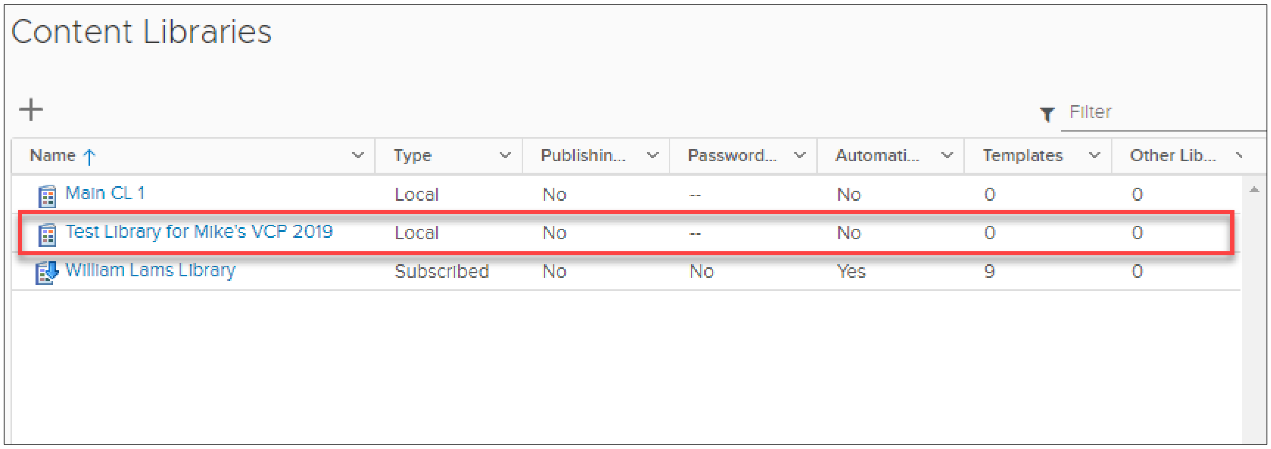
New Content Library

- ✓ 1 Name and location
- ✓ 2 Configure content library
- ✓ 3 Add storage
- 4 Ready to complete

**Ready to complete**

Review content library settings.

|  |  |
|---|---|
| Name: | Test Library for Mike's VCP 2019 |
| vCenter Server: | vCenter1.lab.local |
| Type: | Local Content Library |
| Publishing: | Disabled |
| Storage: | QNAP_Normal |



Content Libraries

| Name ↑ | Type | Publishin... | Password... | Automati... | Templates | Other Lib... |
|---|---|---|---|---|---|---|
| Main CL 1 | Local | No | -- | No | 0 | 0 |
| Test Library for Mike's VCP 2019 | Local | No | -- | No | 0 | 0 |
| William Lams Library | Subscribed | No | No | Yes | 9 | 0 |

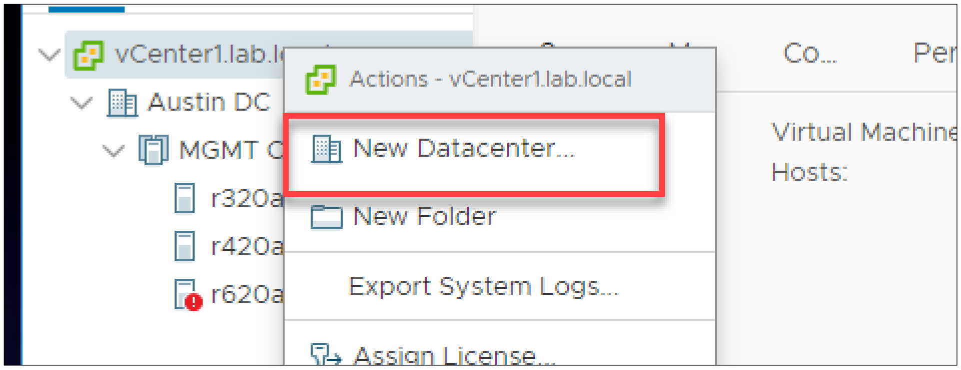
## *Objective 4.4 – Set up ESXi hosts*

Pre-requisites was gone over in Section 1, so I imagine if you got to this point you already know those. You can install ESXi several different ways.

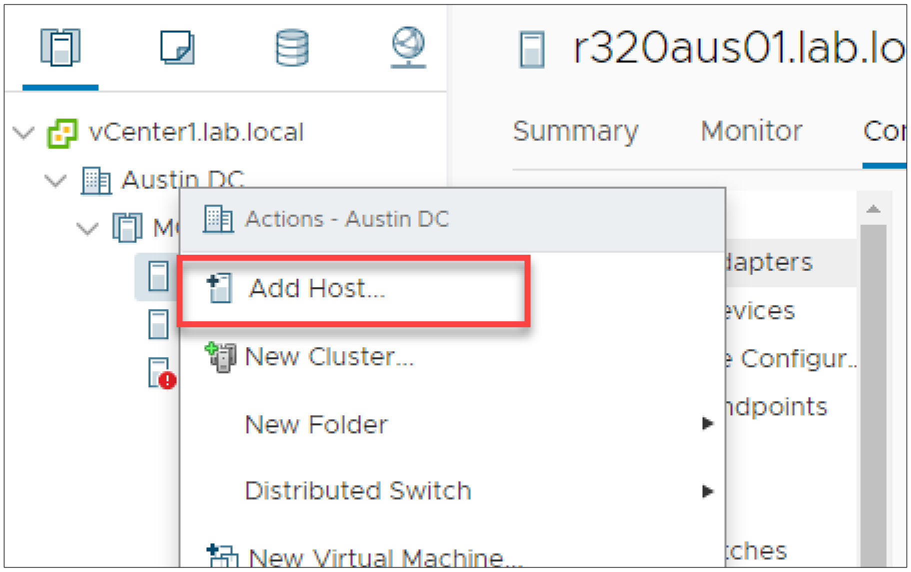
- Interactive Installation – this is you sitting at a console or in front of the server and running the installation. This can be installed from an ISO file, USB stick, CD-ROM, or PXE. The actual installation is fast and straightforward, taking about 15 min or so.
- Scripted Installation – This is more efficient than the interactive as you can do many more at the same time and you aren't required to answer prompts. The prompts are filled out automatically by an unattended file. The installation script needs to be stored in a location that the host can access with HTTP, HTTPS, FTP, NFS, CD-ROM, or USB.
- Auto Deploy Installation – This can provision hundreds of machines at the same time. This can be setup to use a remote disk and can store that setup locally or pull it down every time the machine boots. These options are known as Stateless Caching and stateful installations. With Auto Deploy you create a host profile that allows you to configure the host with specific things like Virtual Standard Switches with a specific name etc. This is great for enterprise because it allows you to keep a standard image and settings.

Once the machine is setup you can further configure it using the configure pane as we saw in Objective 4.2 (screenshot). This allows you to change options such as NTP and more. These settings could be setup if using host profiles.

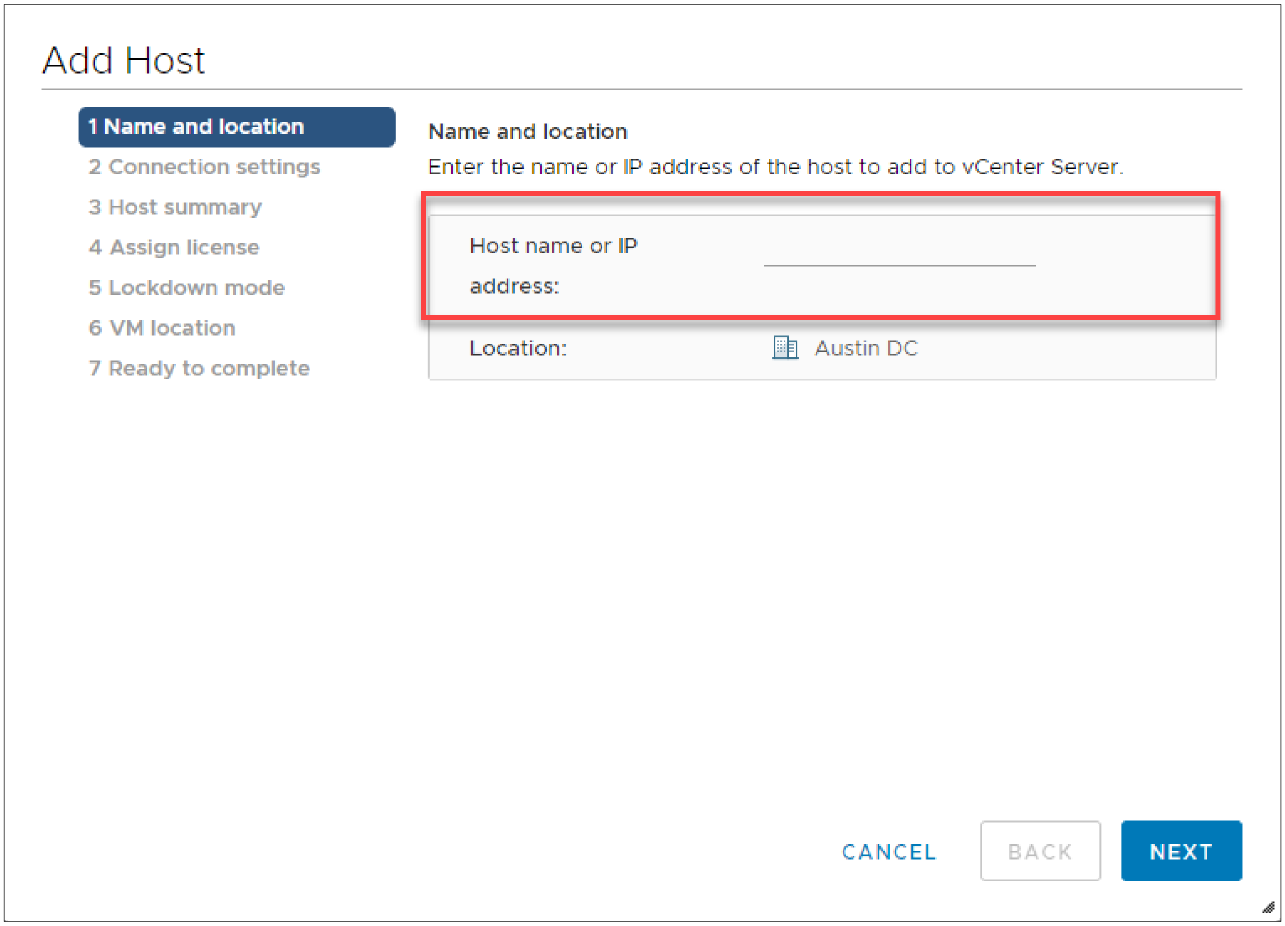
1. To add hosts in vCenter Server, you first must have a Datacenter. You create that by right clicking on the vCenter Server and choose New Datacenter



2. After that is created, you can right click on the Datacenter and Add Host.



3. Enter the IP or Fully Qualified Domain Name (FQDN). Make sure it can be resolved by DNS


Add Host

1 Name and location
2 Connection settings
3 Host summary
4 Assign license
5 Lockdown mode
6 VM location
7 Ready to complete

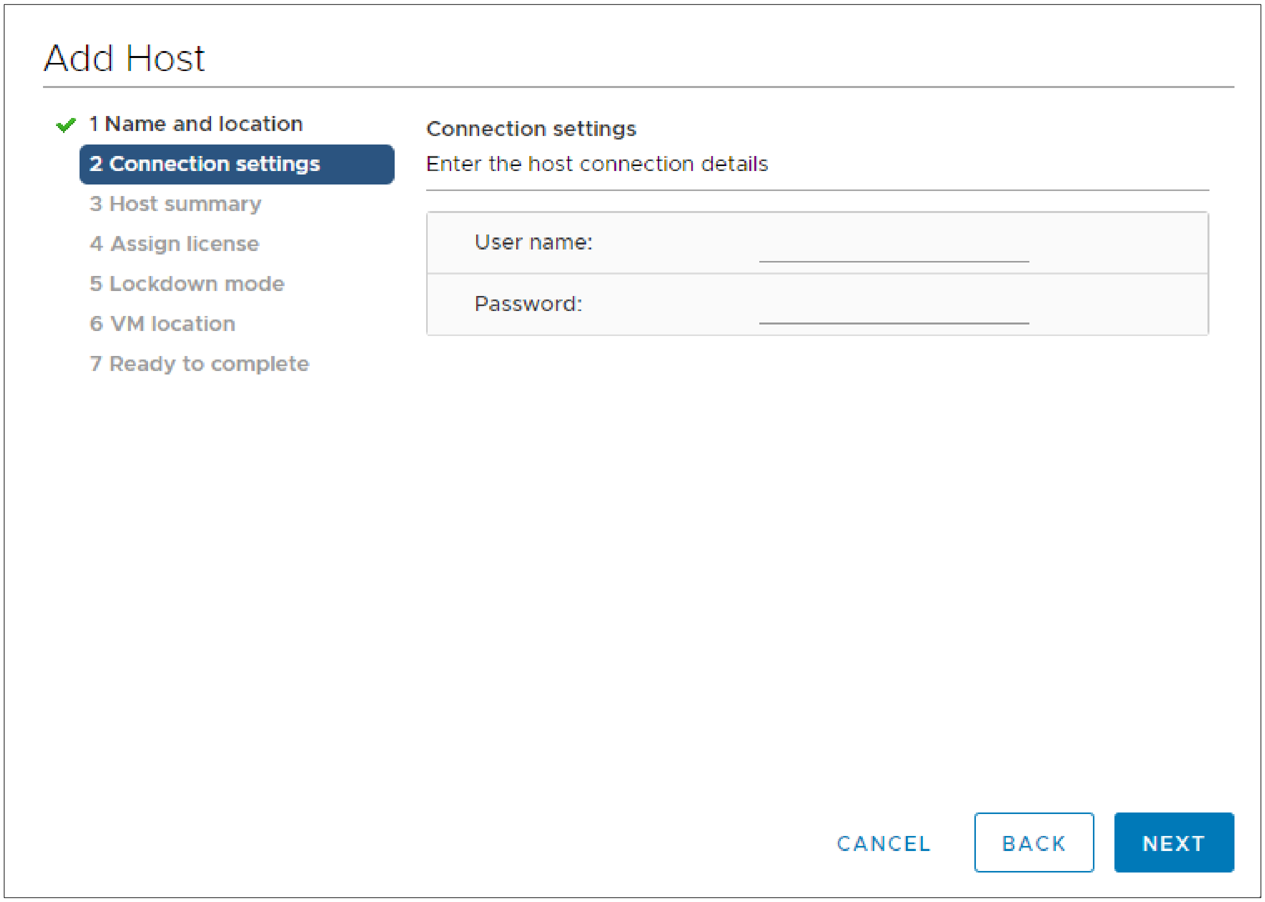
Name and location

Enter the name or IP address of the host to add to vCenter Server.

Host name or IP address:

Location: Austin DC

4. Enter connection details for username and password



Add Host

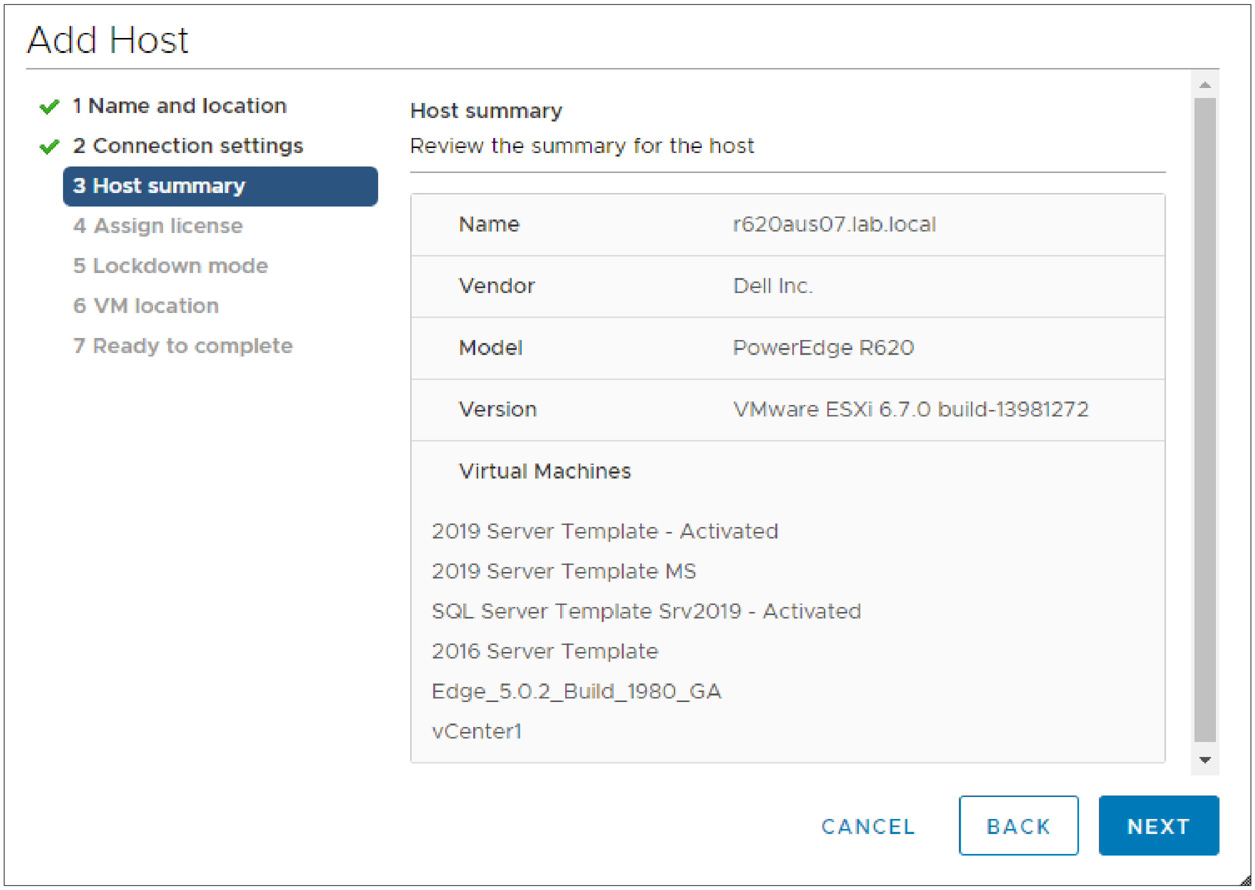
Connection settings

Enter the host connection details

User name: ____

Password: ____

5. You are asked to check the certificate and after approving it, you will be given a summary



Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- 3 Host summary
- 4 Assign license
- 5 Lockdown mode
- 6 VM location
- 7 Ready to complete

Host summary

Review the summary for the host

| | |
|---|---|
| Name | r620aus07.lab.local |
| Vendor | Dell Inc. |
| Model | PowerEdge R620 |
| Version | VMware ESXi 6.7.0 build-13981272 |

Virtual Machines

2019 Server Template - Activated

2019 Server Template MS

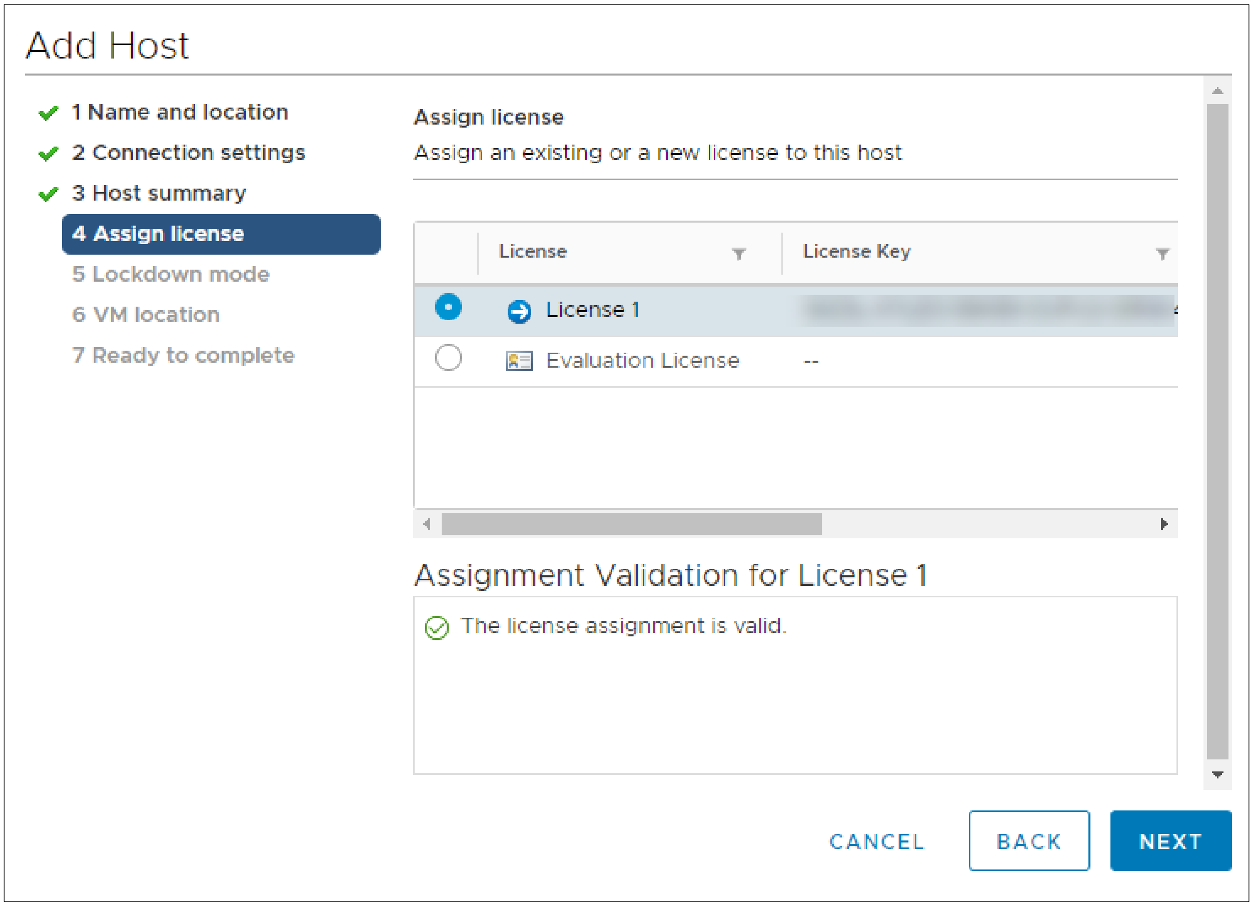
SQL Server Template Srv2019 - Activated

2016 Server Template

Edge_5.0.2_Build_1980_GA

vCenter1

6. Assign a license to it



## Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- 4 Assign license
- 5 Lockdown mode
- 6 VM location
- 7 Ready to complete

**Assign license**

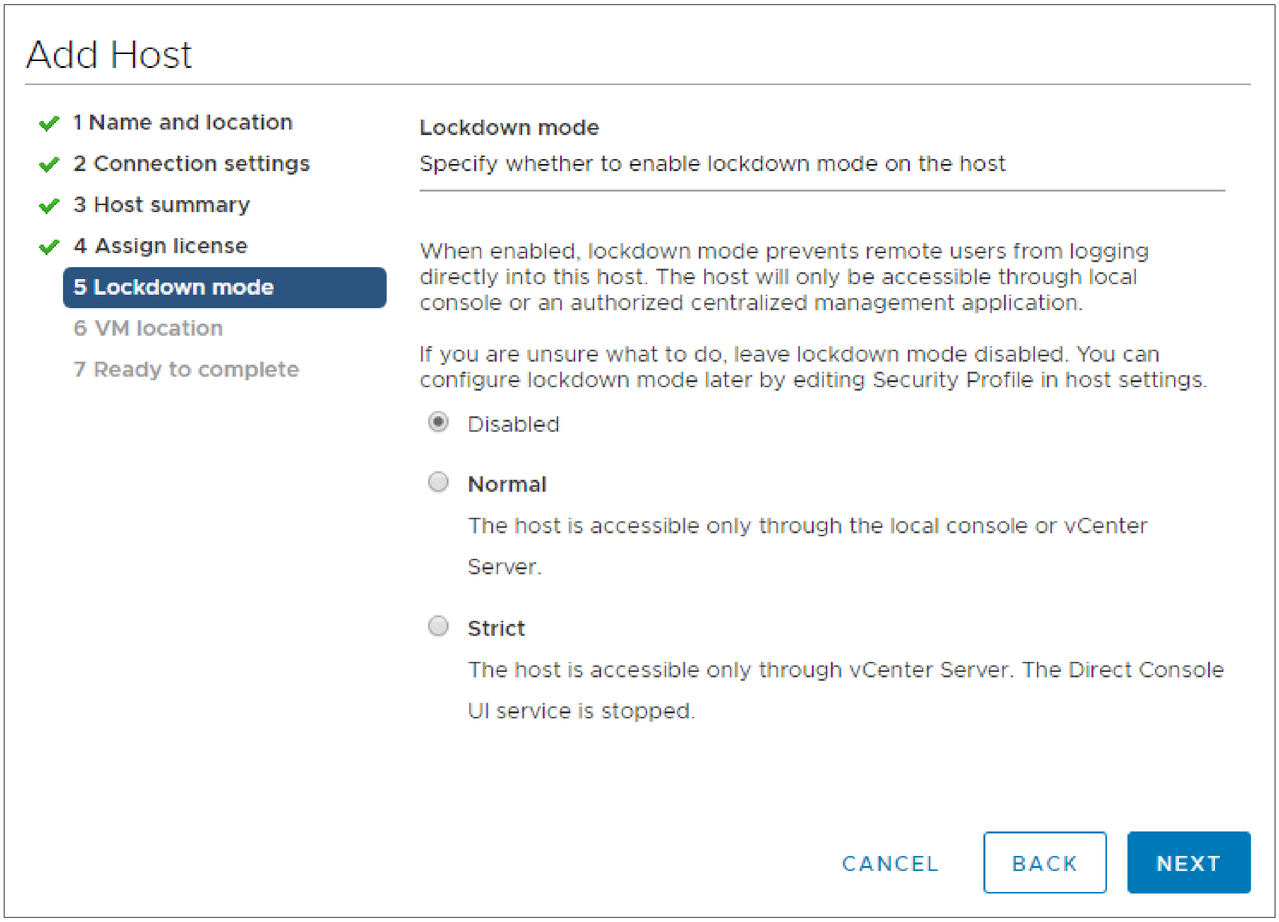
Assign an existing or a new license to this host

| | License | License Key |
|---|---|---|
| ● | License 1 | [redacted] |
| ○ | Evaluation License | -- |

Assignment Validation for License 1

✓ The license assignment is valid.

7. Assign a lockdown mode if you want to use it



Add Host

Lockdown mode

Specify whether to enable lockdown mode on the host

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.

If you are unsure what to do, leave lockdown mode disabled. You can configure lockdown mode later by editing Security Profile in host settings.

● Disabled

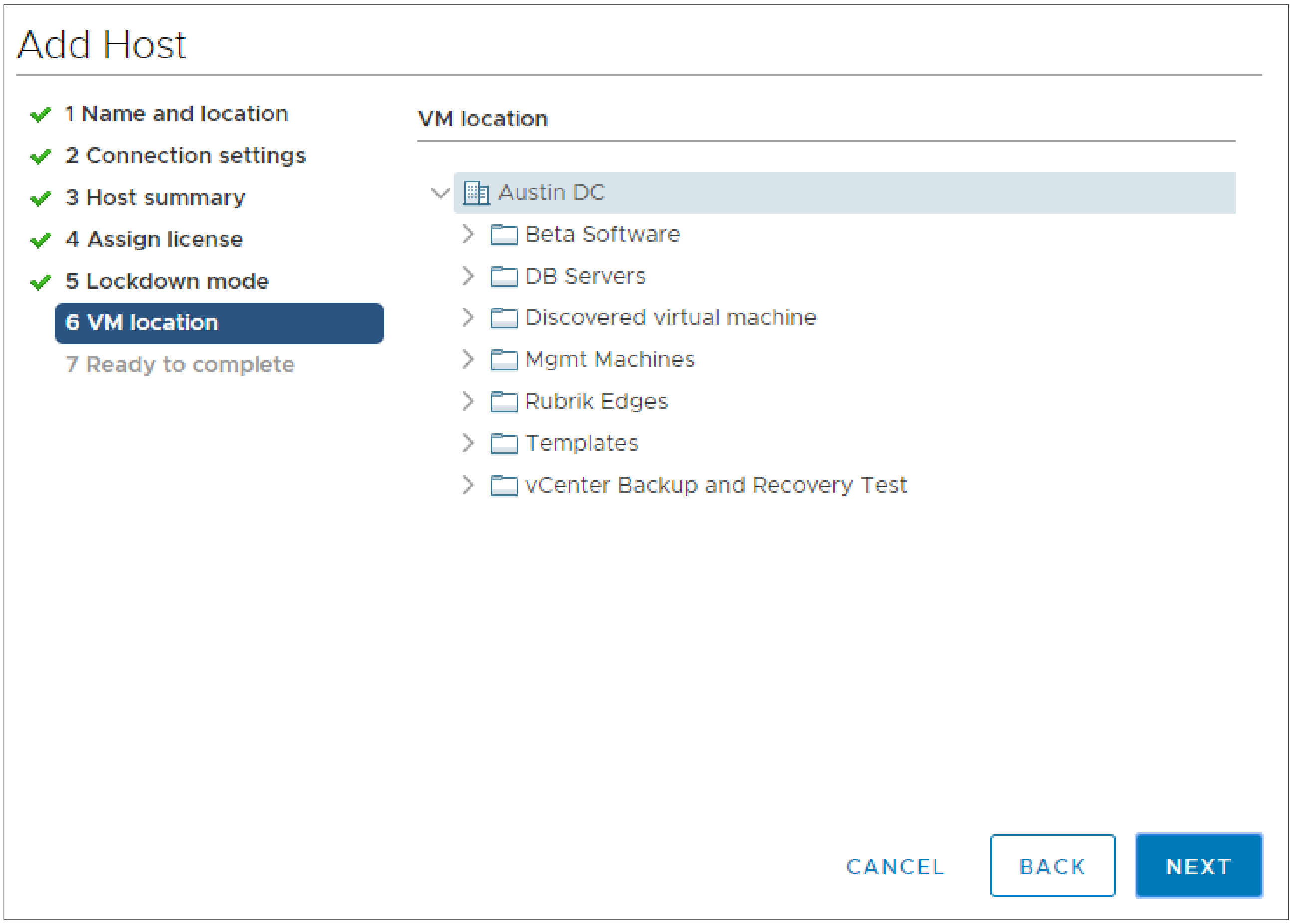
○ **Normal**

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.

8. Assign where you want to put the VMs from this host (if there are any on it)



Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- ✓ 4 Assign license
- ✓ 5 Lockdown mode
- 6 VM location
- 7 Ready to complete

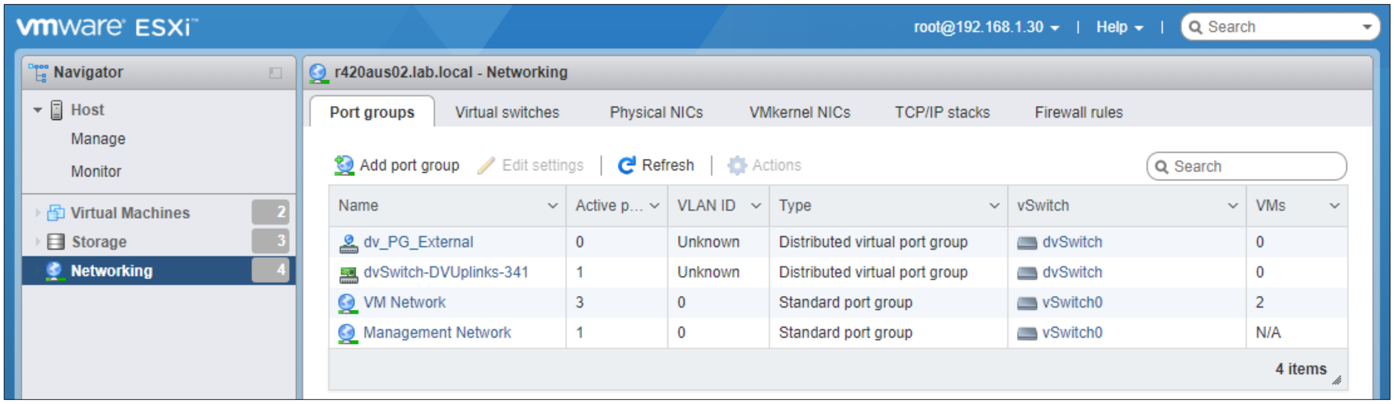
VM location

- Austin DC
  - Beta Software
  - DB Servers
  - Discovered virtual machine
  - Mgmt Machines
  - Rubrik Edges
  - Templates
  - vCenter Backup and Recovery Test

9. Click Finish and Complete it.

## *Objective 4.5 – Configure virtual networking*

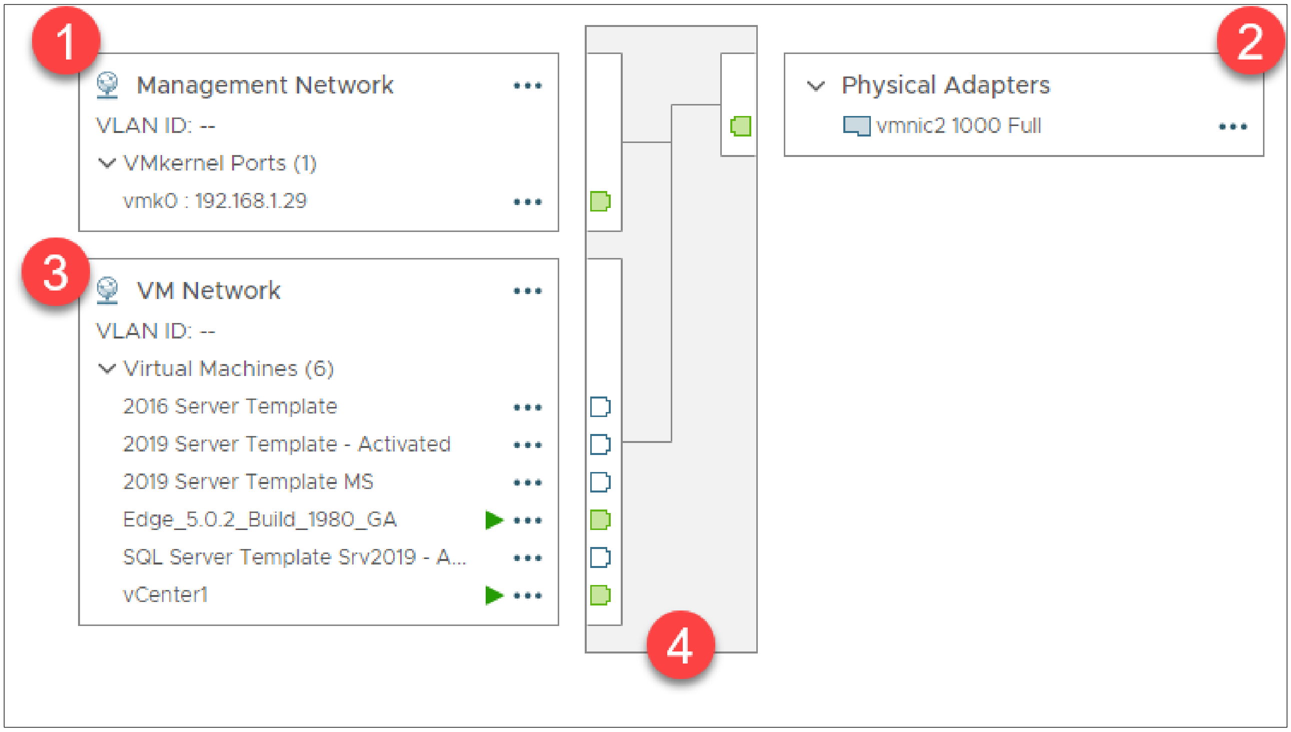
You configure virtual networking different ways, depending on your environment. Configuring VSSs can be done using the ESXi HTML5 client as seen here



| 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 |

4 items

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 together. 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.



Management Network

VLAN ID: --

VMkernel Ports (1)

vmk0 : 192.168.1.29

VM Network

VLAN ID: --

Virtual Machines (6)

2016 Server Template

2019 Server Template - Activated

2019 Server Template MS

Edge_5.0.2_Build_1980_GA

SQL Server Template Srv2019 - A...

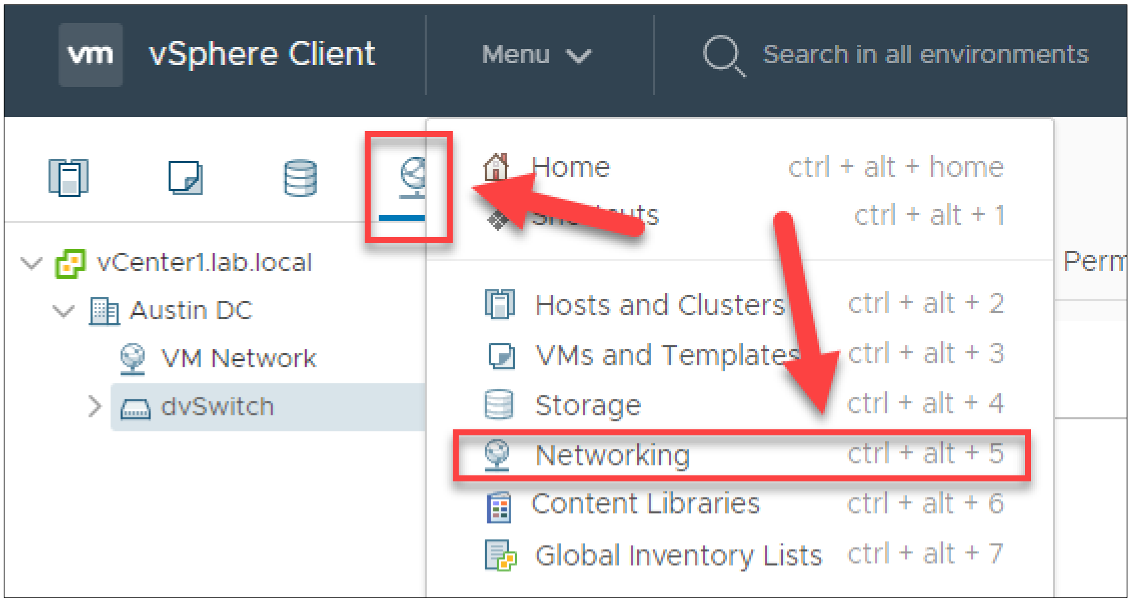
vCenter1

Physical Adapters

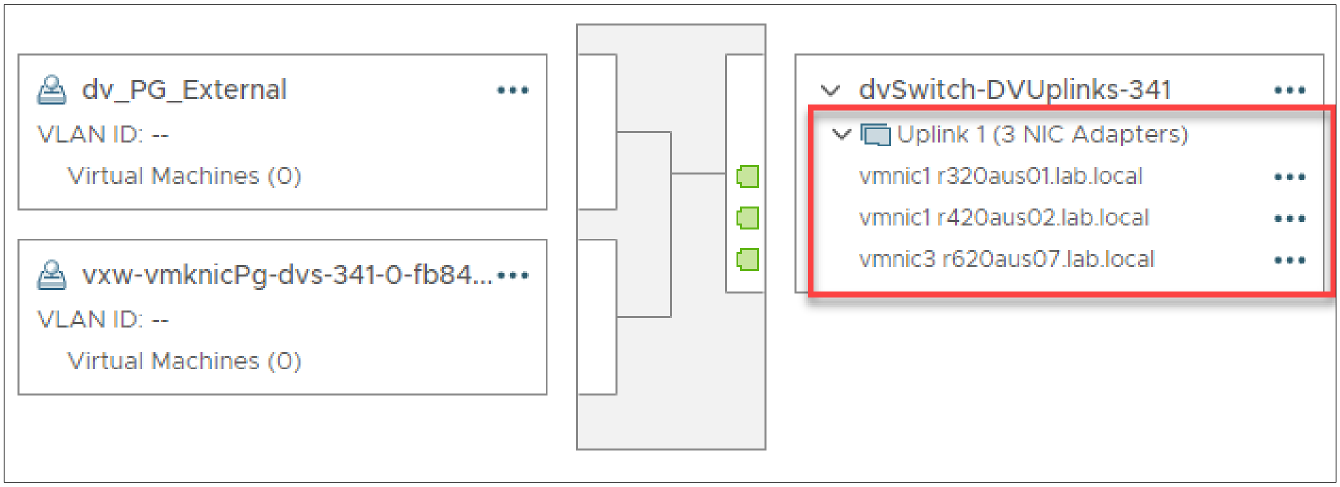
vmnic2 1000 Full

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 easier perform tasks on all of them.
4. The construct in the middle is my Virtual Switch. This one is a VSS

The picture above can be accessed on the host page under the configure tab. You can also make changes there. A VDS is accessed under the sub category networking by using the menu up top or corresponding icon.


vm
vSphere Client
Menu
Search in all environments
vCenter1.lab.local
Austin DC
VM Network
dvSwitch
Home ctrl + alt + home
Shortcuts ctrl + alt + 1
Hosts and Clusters ctrl + alt + 2
VMs and Templates ctrl + alt + 3
Storage ctrl + alt + 4
Networking ctrl + alt + 5
Content Libraries ctrl + alt + 6
Global Inventory Lists ctrl + alt + 7
Perm

The picture for VDS looks much like the one for VSS but will mention all the different uplinks on each host.


dv_PG_External
VLAN ID: --
Virtual Machines (0)

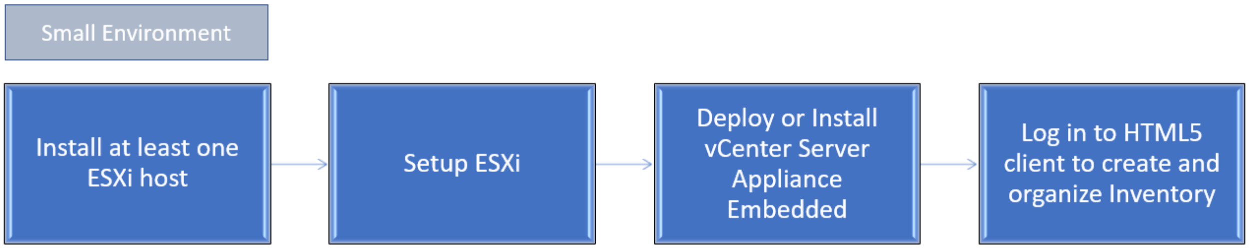
vxw-vmknicPg-dvs-341-0-fb84...
VLAN ID: --
Virtual Machines (0)

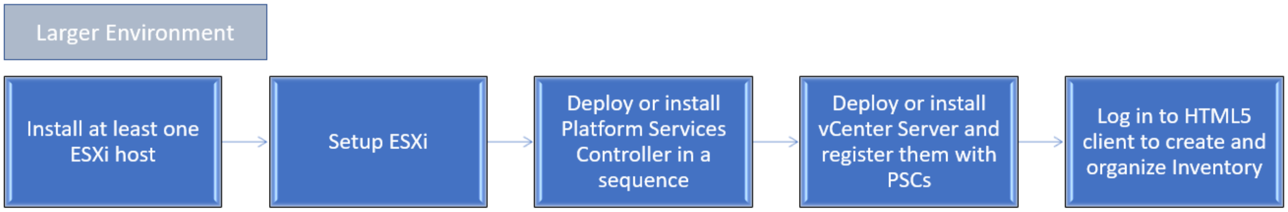
dvSwitch-DVUplinks-341
Uplink 1 (3 NIC Adapters)
vmnic1 r320aus01.lab.local
vmnic1 r420aus02.lab.local
vmnic3 r620aus07.lab.local

You can make changes there as well. Or by right-clicking on the actual switch on the navigation pane on the left.

## *Objective 4.6 – Deploy and configure VMware vCenter Server Appliance (VCSA)*

This objective is the installation and configuration of vCenter Server Appliance. The installation may vary a tad depending on the type of installation you do. Here is a workflow. I am going to assume you already have at least one ESXi host setup since we covered that a couple of objectives ago. 😊 There are two workflows. One for large environments and one for smaller.


Small Environment
Install at least one ESXi host
Setup ESXi
Deploy or Install vCenter Server Appliance Embedded
Log in to HTML5 client to create and organize Inventory

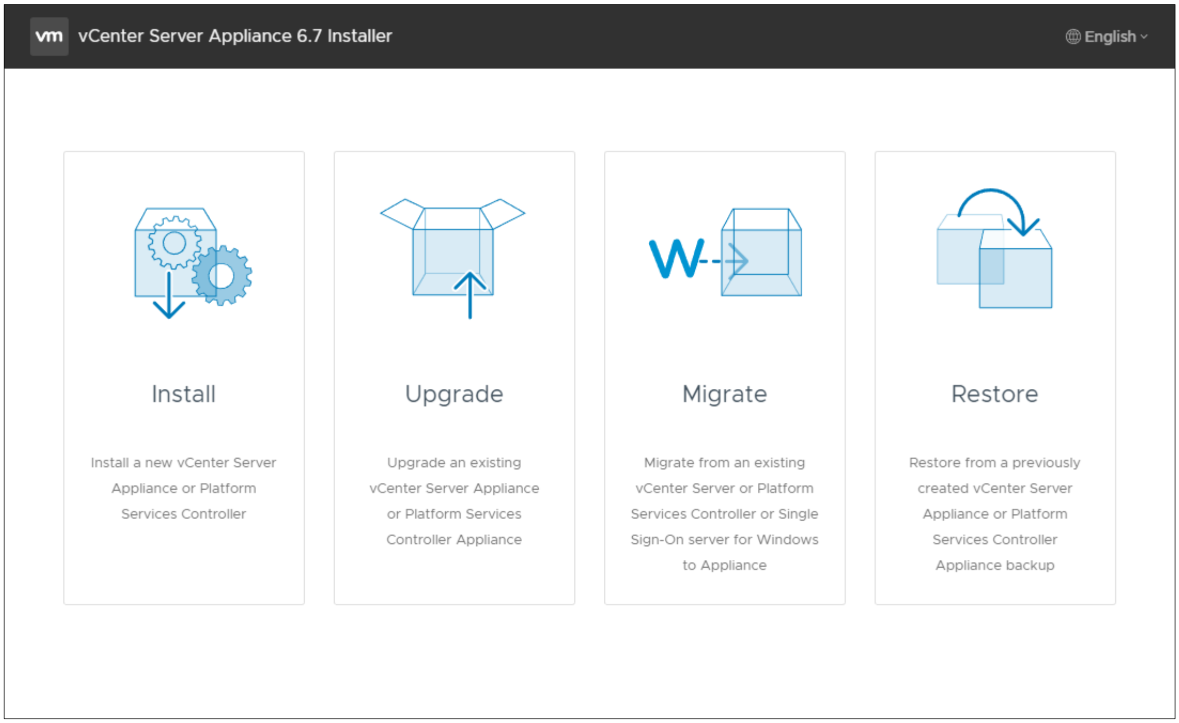

Larger Environment
Install at least one ESXi host
Setup ESXi
Deploy or install Platform Services Controller in a sequence
Deploy or install vCenter Server and register them with PSCs
Log in to HTML5 client to create and organize Inventory

The vCenter Server UI install, whether for a vCenter Server or PSC, is a two-stage process. The installer contains files for both GUI and CLI deployments so you only need the one ISO. The first stage is deployment of the OVA file into your environment. The second stage configures and starts all the services of your shiny new appliance. The CLI is slightly different. You run a CLI command against a JSON file you have inputted your configuration parameters in. This in turn creates an OVF Tool command that deploys and configures the appliance in one go.

Once setup, you log into the appliance with the username “root” and whatever password you set while deploying. Single Sign On comes later. Lets see what the install looks like.

1. For a Microsoft Windows admin station, you will mount the ISO and go to <CD-ROM Drive Letter>\vcsa-ui-installer\win32\installer.exe and double-click.

2. You are then presented with this screen



vm vCenter Server Appliance 6.7 Installer

Install

Install a new vCenter Server Appliance or Platform Services Controller

Upgrade

Upgrade an existing vCenter Server Appliance or Platform Services Controller Appliance

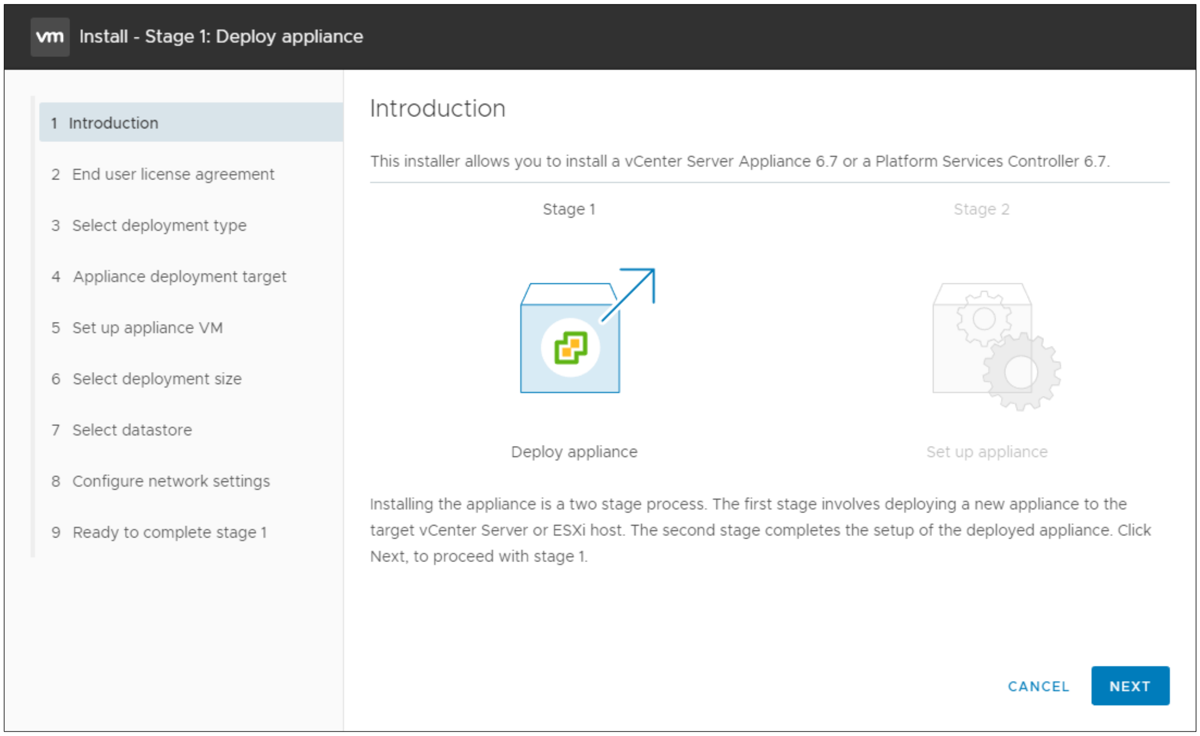
Migrate

Migrate from an existing vCenter Server or Platform Services Controller or Single Sign-On server for Windows to Appliance

Restore

Restore from a previously created vCenter Server Appliance or Platform Services Controller Appliance backup

3. We are going to Install so click on that box. The first stage then begins.



vm Install - Stage 1: Deploy appliance

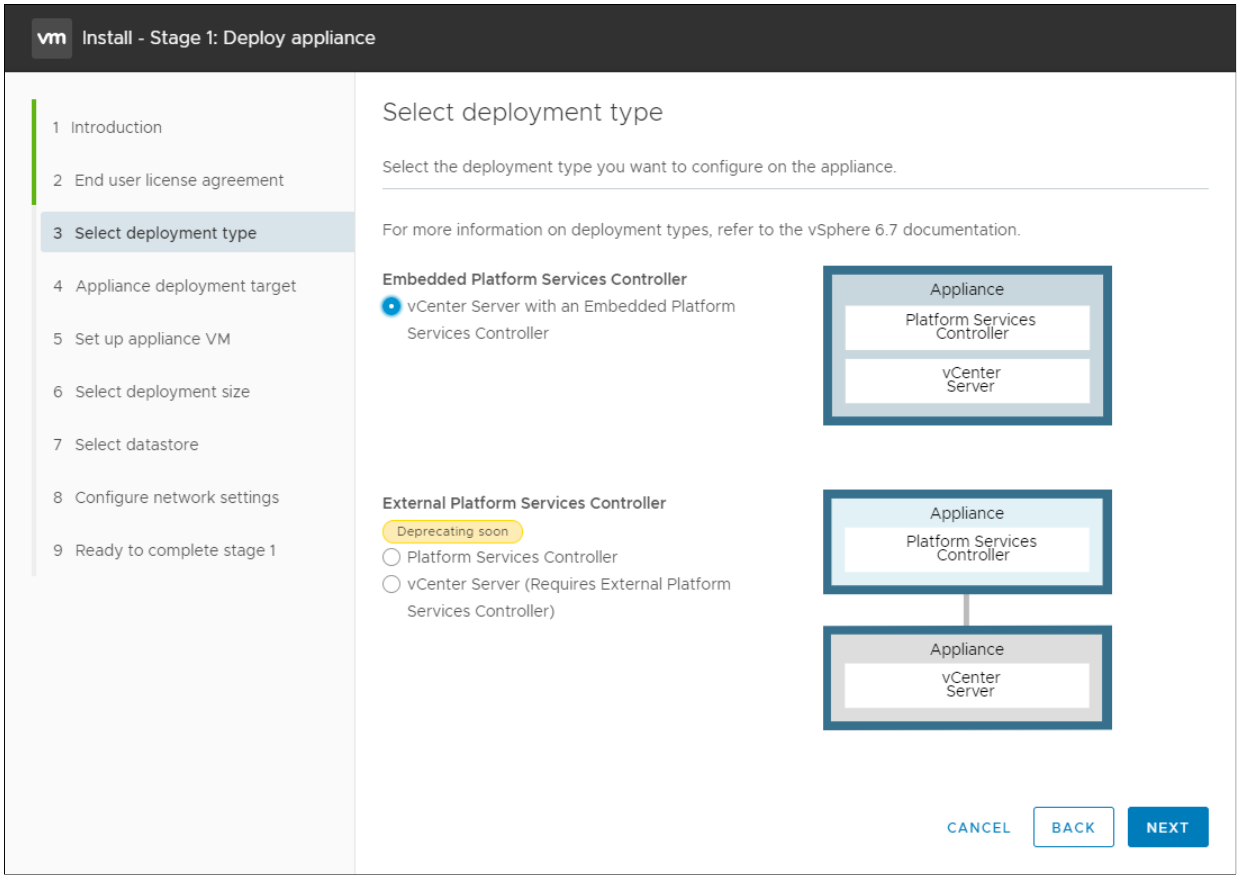
1 Introduction
2 End user license agreement
3 Select deployment type
4 Appliance deployment target
5 Set up appliance VM
6 Select deployment size
7 Select datastore
8 Configure network settings
9 Ready to complete stage 1

Introduction

This installer allows you to install a vCenter Server Appliance 6.7 or a Platform Services Controller 6.7.

Installing the appliance is a two stage process. The first stage involves deploying a new appliance to the target vCenter Server or ESXi host. The second stage completes the setup of the deployed appliance. Click Next, to proceed with stage 1.

4. Click Next and Accept the End User Agreement. The next screen is where we decide what type of installation we want to perform.



Install - Stage 1: Deploy appliance

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

Select deployment type

Select the deployment type you want to configure on the appliance.

For more information on deployment types, refer to the vSphere 6.7 documentation.

Embedded Platform Services Controller

● vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

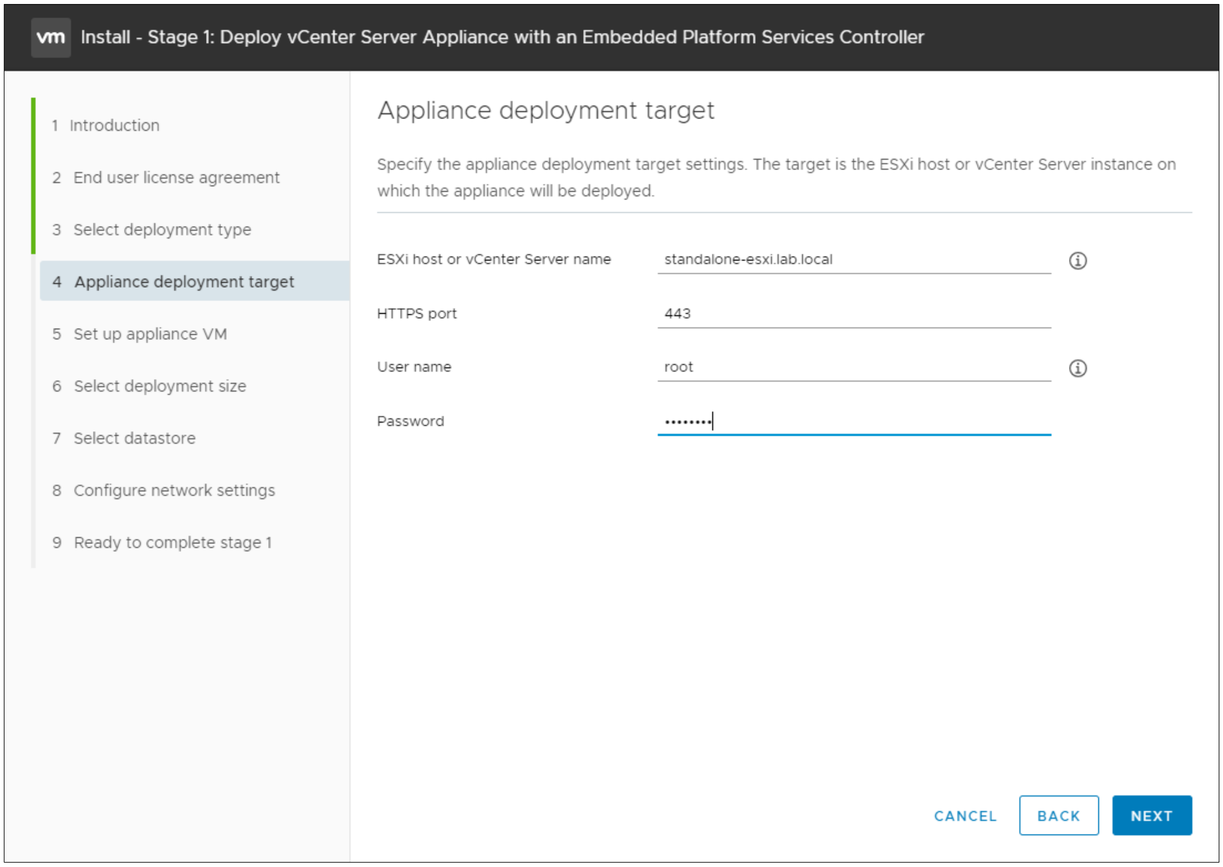
Deprecating soon

○ Platform Services Controller

○ vCenter Server (Requires External Platform Services Controller)

5. I am going to choose embedded. Notice the External PSC model will soon not be supported.

6. We now need to choose the ESXi host to install to (or vCenter Server). Generally the port will be 443 unless you have changed your environment.



Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

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

Appliance deployment target

Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

ESXi host or vCenter Server name: standalone-esxi.lab.local

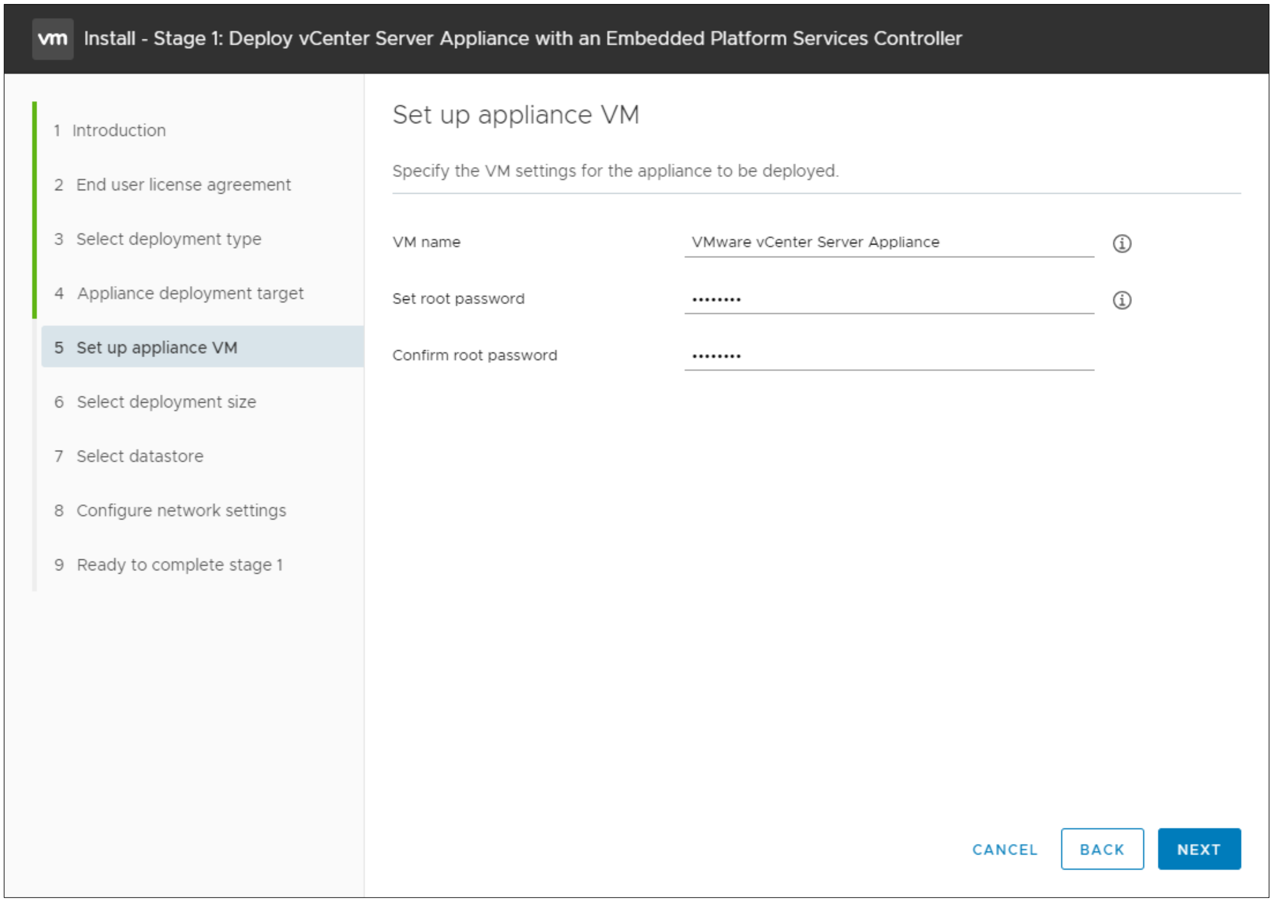
HTTPS port: 443

User name: root

Password: ••••••••

7. Accept the Certificate warning

8. Enter in the name you want to give your vCenter Server that will appear in the VM inventory. Type in a password that you want to use for the vCenter Server.



Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

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

Set up appliance VM

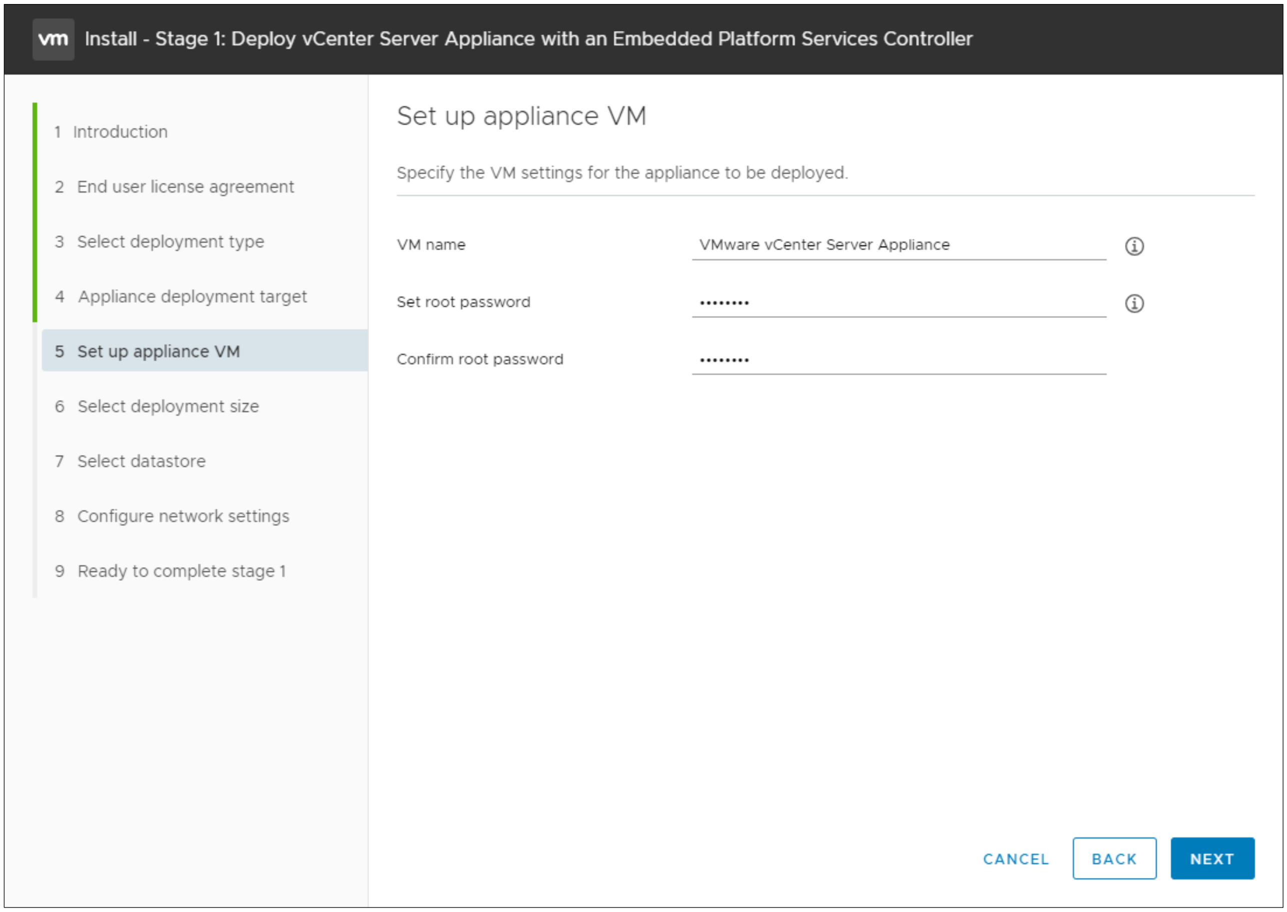
Specify the VM settings for the appliance to be deployed.

VM name: VMware vCenter Server Appliance

Set root password: •••••••••

Confirm root password: •••••••••

9. Decide on Deployment Size and Storage Size. Keep in mind if this vCenter will be doing heavy processing you may want to upsize it. This will give it more vCPUs and memory to use.



Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

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

Set up appliance VM

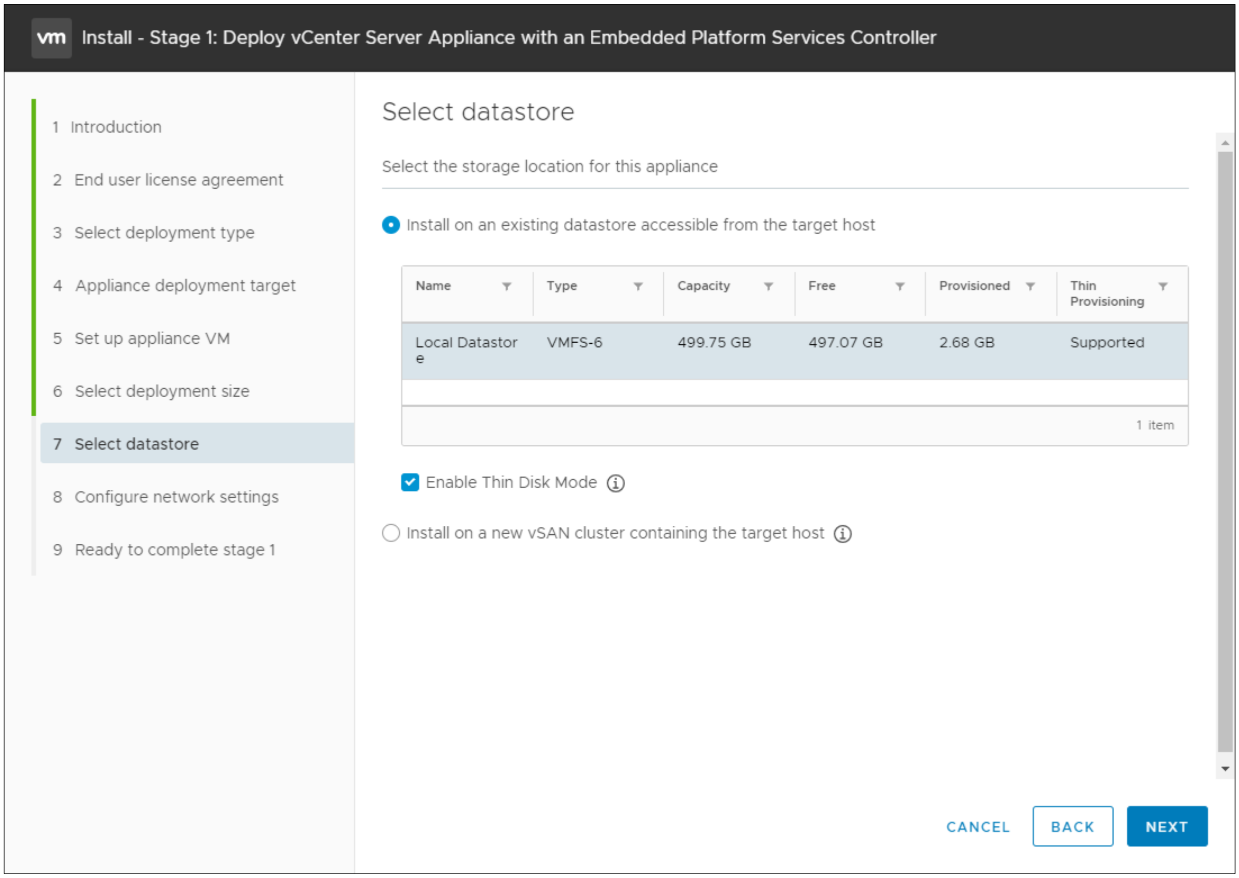
Specify the VM settings for the appliance to be deployed.

VM name: VMware vCenter Server Appliance

Set root password: ••••••••

Confirm root password: ••••••••

10. Select the datastore you want to install to and if you want to use Thin Disk Mode or Thick. You can also create a vSAN datastore to install to.



Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

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

Select datastore

Select the storage location for this appliance

● Install on an existing datastore accessible from the target host

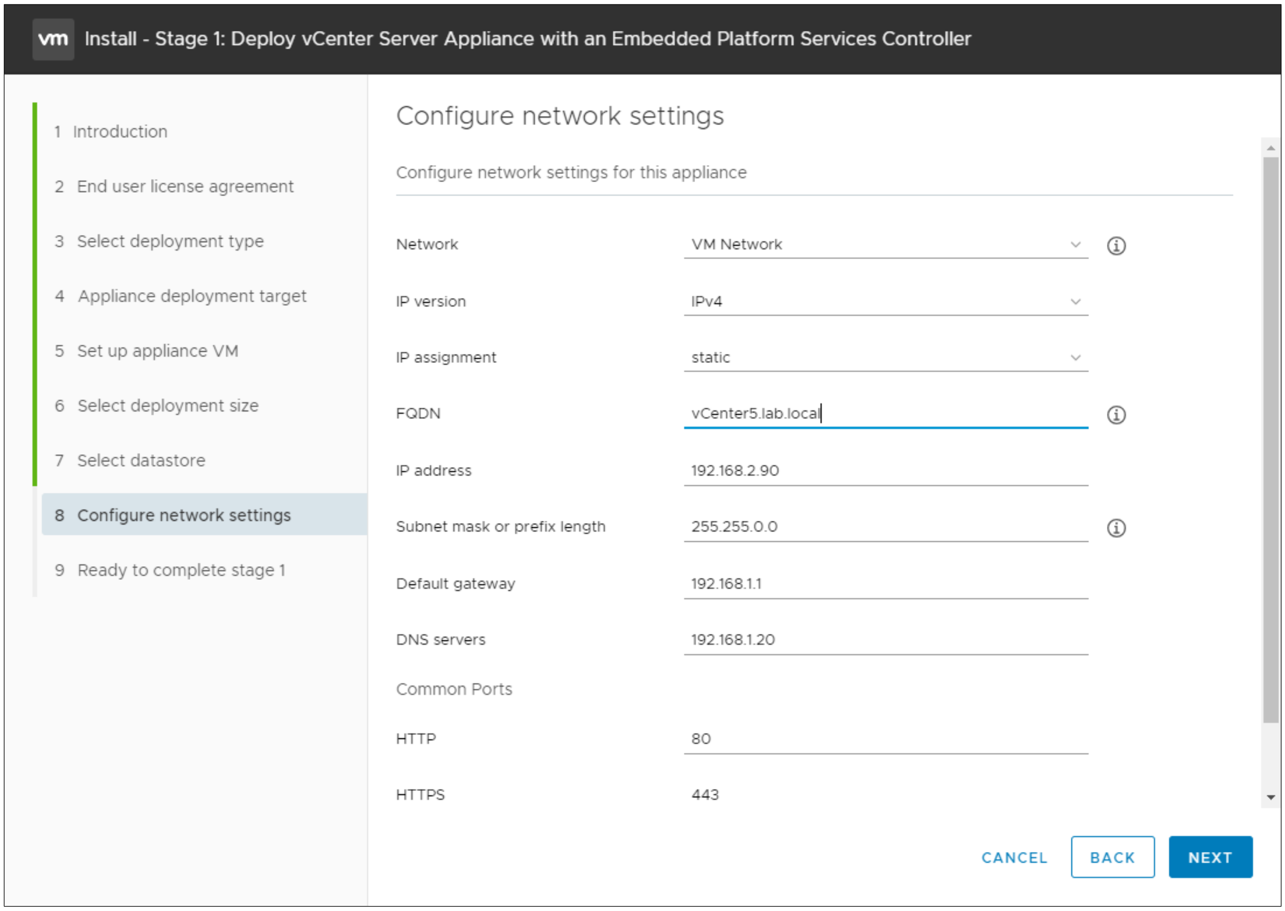
| Name | Type | Capacity | Free | Provisioned | Thin Provisioning |
|---|---|---|---|---|---|
| Local Datastore | VMFS-6 | 499.75 GB | 497.07 GB | 2.68 GB | Supported |

1 item

☑ Enable Thin Disk Mode

○ Install on a new vSAN cluster containing the target host

11. Network settings now need to be entered in.



Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

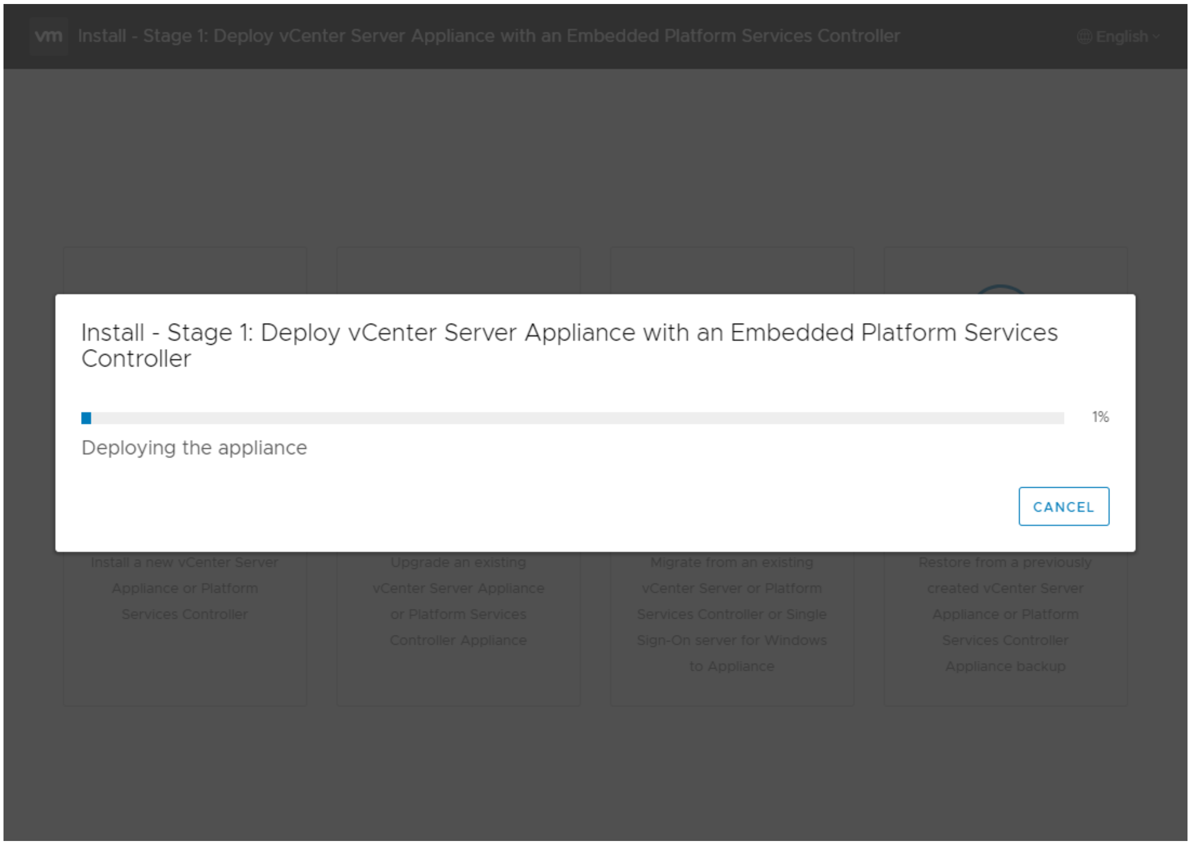
1 Introduction
2 End user license agreement
3 Select deployment type
4 Appliance deployment target
5 Set up appliance VM
6 Select deployment size
7 Select datastore
8 Configure network settings
9 Ready to complete stage 1

Configure network settings

Configure network settings for this appliance

| | |
|---|---|
| Network | VM Network |
| IP version | IPv4 |
| IP assignment | static |
| FQDN | vCenter5.lab.local |
| IP address | 192.168.2.90 |
| Subnet mask or prefix length | 255.255.0.0 |
| Default gateway | 192.168.1.1 |
| DNS servers | 192.168.1.20 |
| Common Ports | |
| HTTP | 80 |
| HTTPS | 443 |

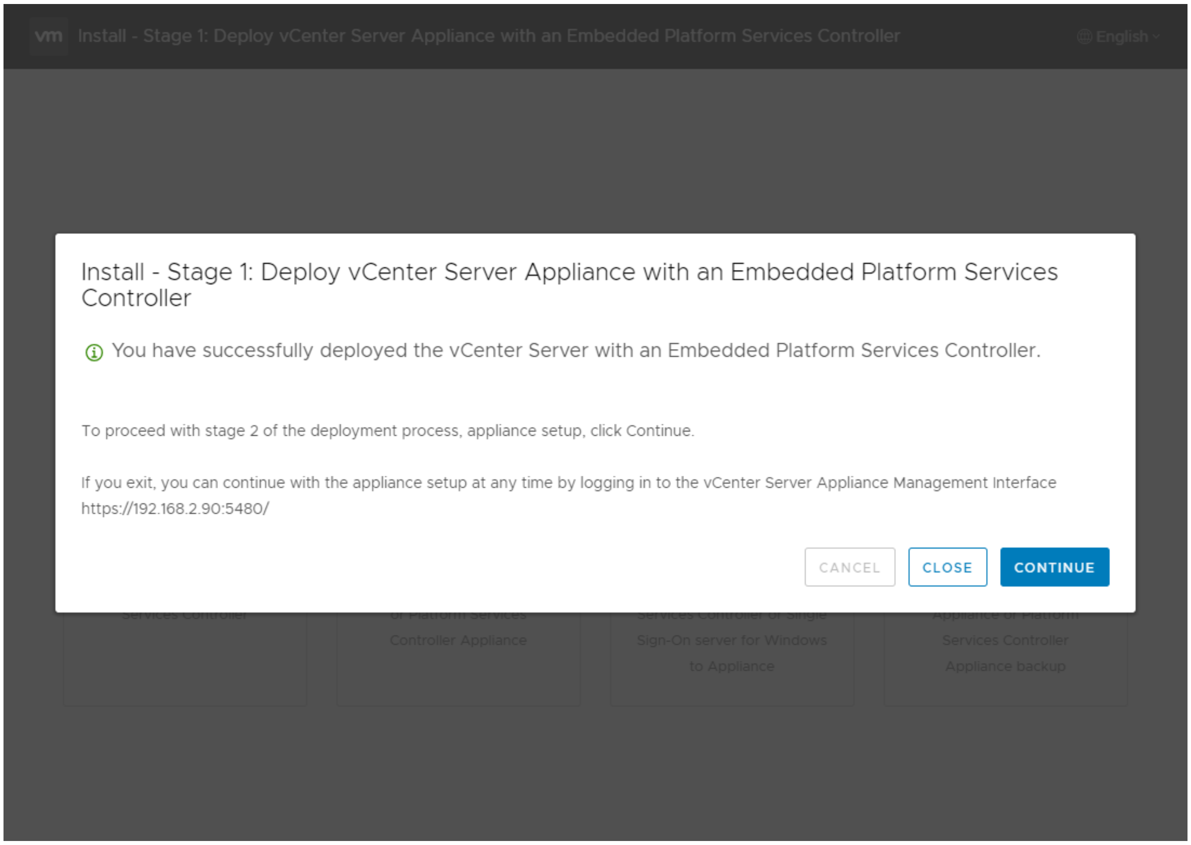
12. It is now ready to complete stage 1. Let it finish.


vm Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller
English
Install a new vCenter Server Appliance or Platform Services Controller
Upgrade an existing vCenter Server Appliance or Platform Services Controller Appliance
Migrate from an existing vCenter Server or Platform Services Controller or Single Sign-On server for Windows to Appliance
Restore from a previously created vCenter Server Appliance or Platform Services Controller Appliance backup

Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

1%

Deploying the appliance


vm Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller
English
Services Controller
or Platform Services Controller Appliance
Services Controller or Single Sign-On server for Windows to Appliance
Appliance or Platform Services Controller Appliance backup

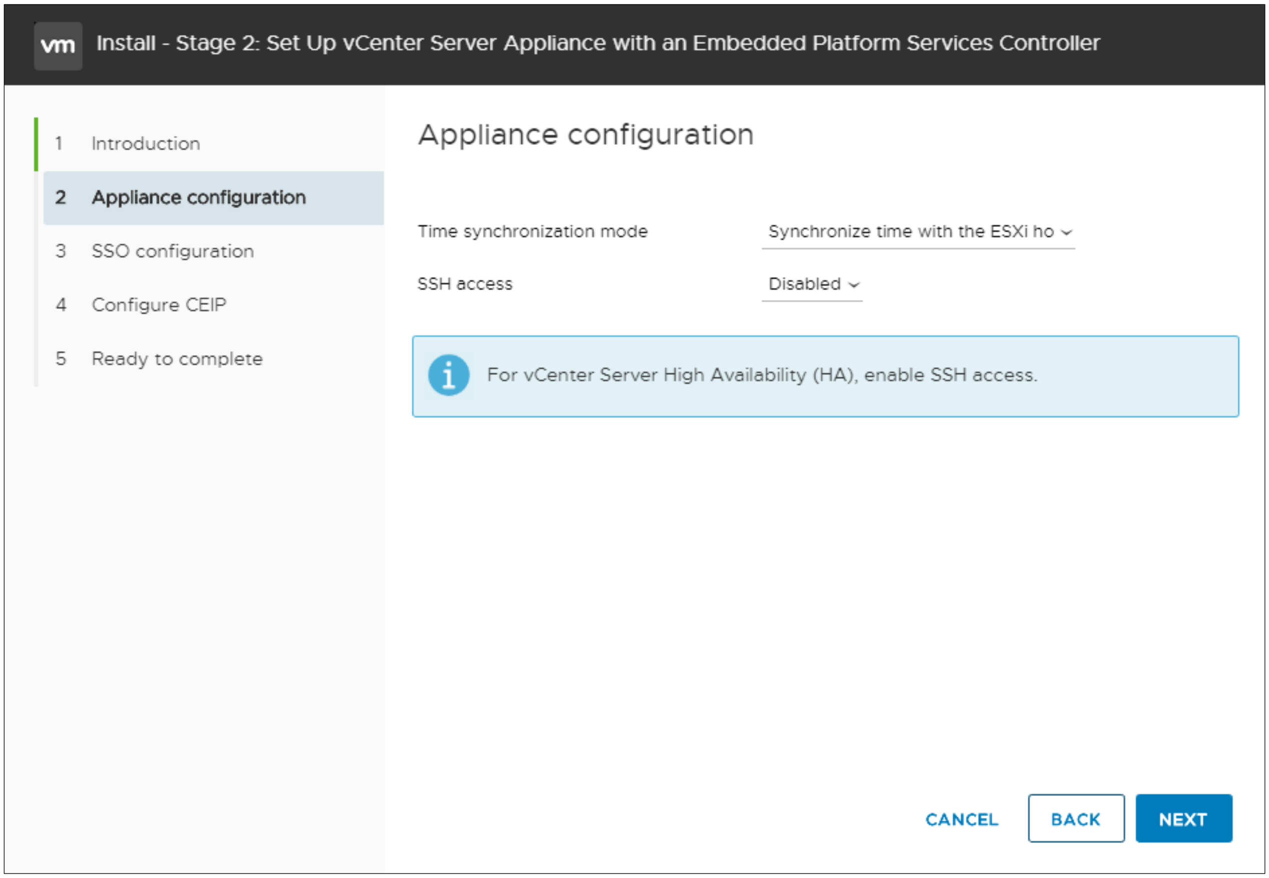
Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

ⓘ You have successfully deployed the vCenter Server with an Embedded Platform Services Controller.

To proceed with stage 2 of the deployment process, appliance setup, click Continue.

If you exit, you can continue with the appliance setup at any time by logging in to the vCenter Server Appliance Management Interface https://192.168.2.90:5480/

13. Stage 2 begins. You need to decide how to synchronize time and if SSH access will be open.



Install - Stage 2: Set Up vCenter Server Appliance with an Embedded Platform Services Controller

Appliance configuration

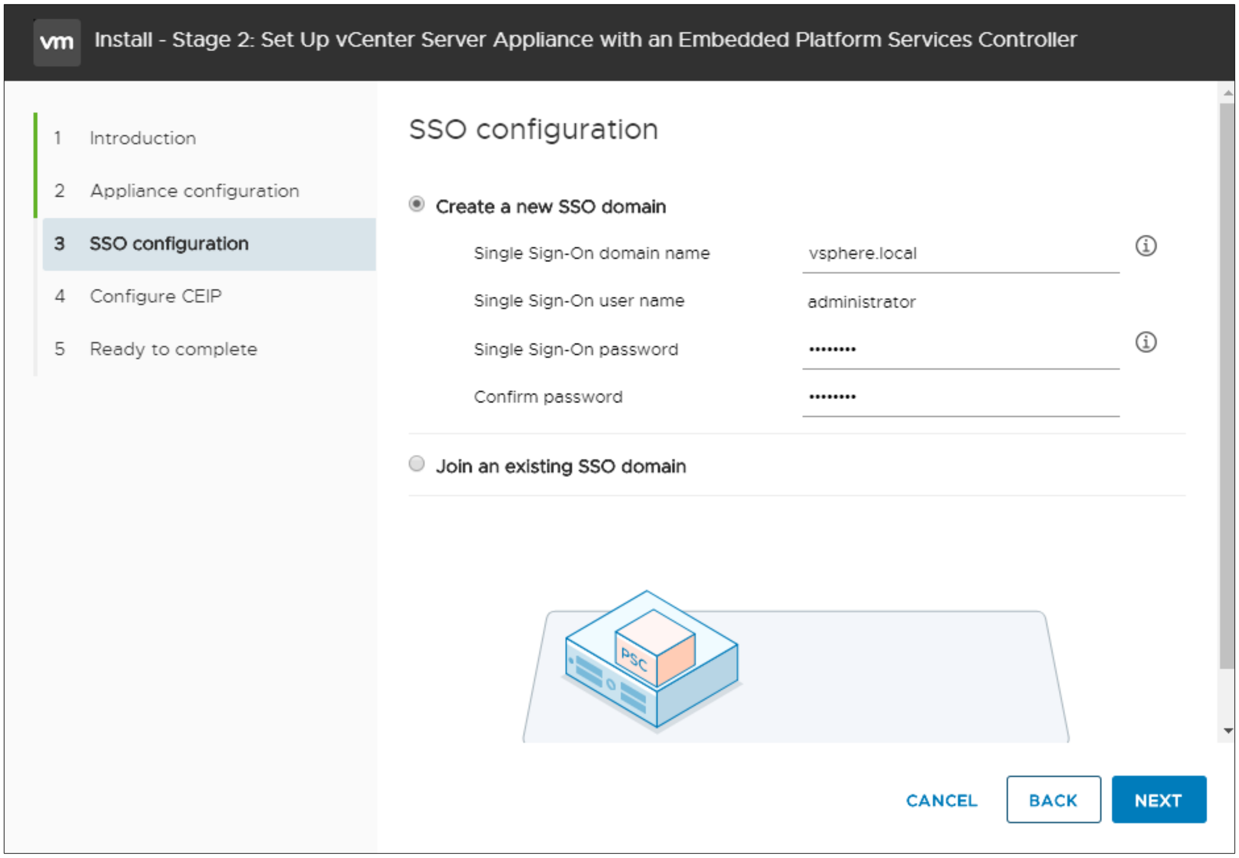
Time synchronization mode: Synchronize time with the ESXi ho

SSH access: Disabled

For vCenter Server High Availability (HA), enable SSH access.

14. You then need to create a SSO domain or join an existing one. If you create one, make sure it is not the same name as your Windows Domain as that can cause all sorts of issues. This is

also where to set the password for Administrator@SSODomainyoumakeup.something.



Install - Stage 2: Set Up vCenter Server Appliance with an Embedded Platform Services Controller

1 Introduction

2 Appliance 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

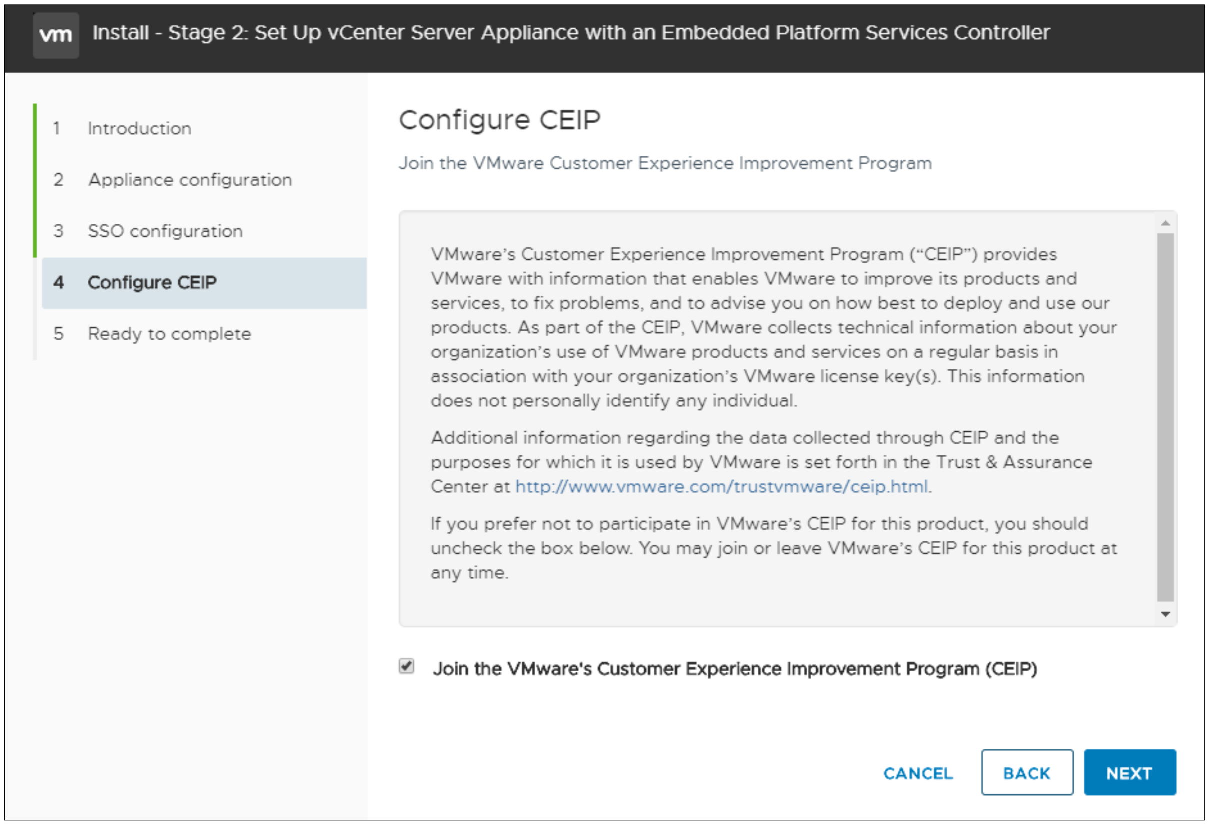
Single Sign-On user name: administrator

Single Sign-On password: ••••••••

Confirm password: ••••••••

○ Join an existing SSO domain

15. Decide if you and your company want to share anonymized data with VMware.



Install - Stage 2: Set Up vCenter Server Appliance with an Embedded Platform Services Controller

Configure CEIP

Join the VMware Customer Experience Improvement Program

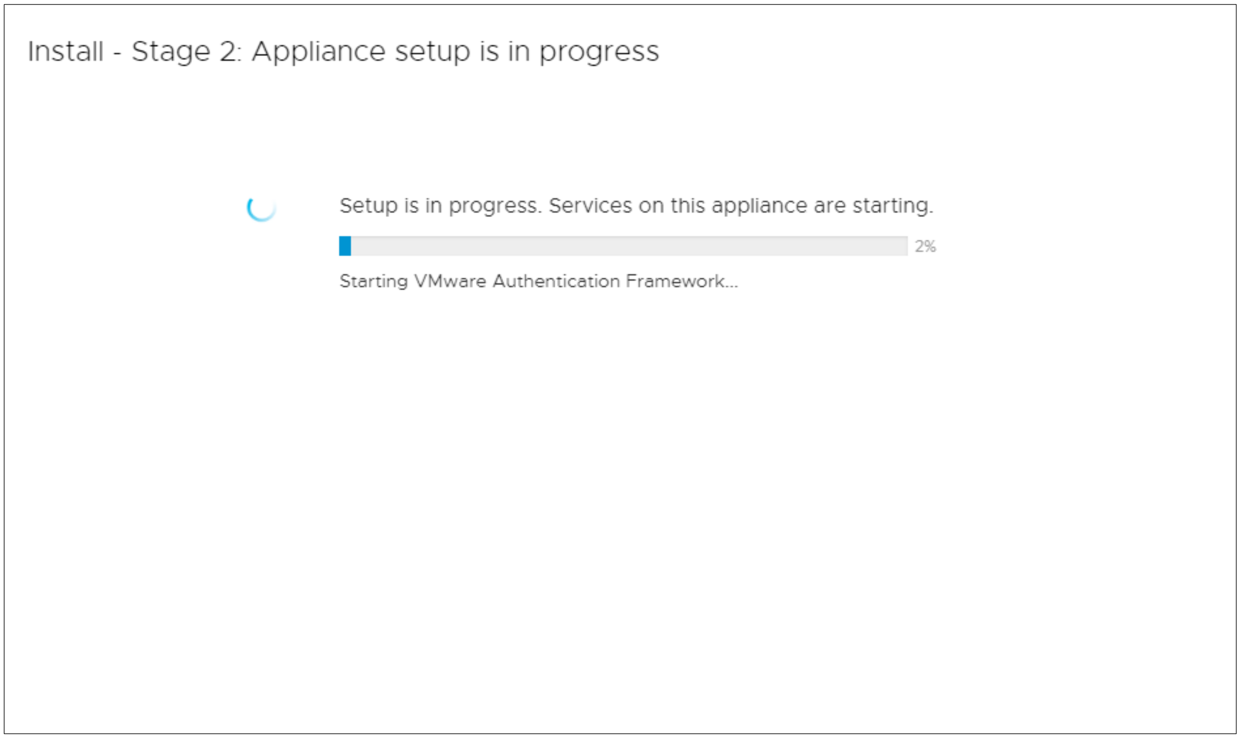
VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.

Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

If you prefer not to participate in VMware's CEIP for this product, you should uncheck the box below. You may join or leave VMware's CEIP for this product at any time.

☑ Join the VMware's Customer Experience Improvement Program (CEIP)

16. Finish and watch it work.



Install - Stage 2: Appliance setup is in progress

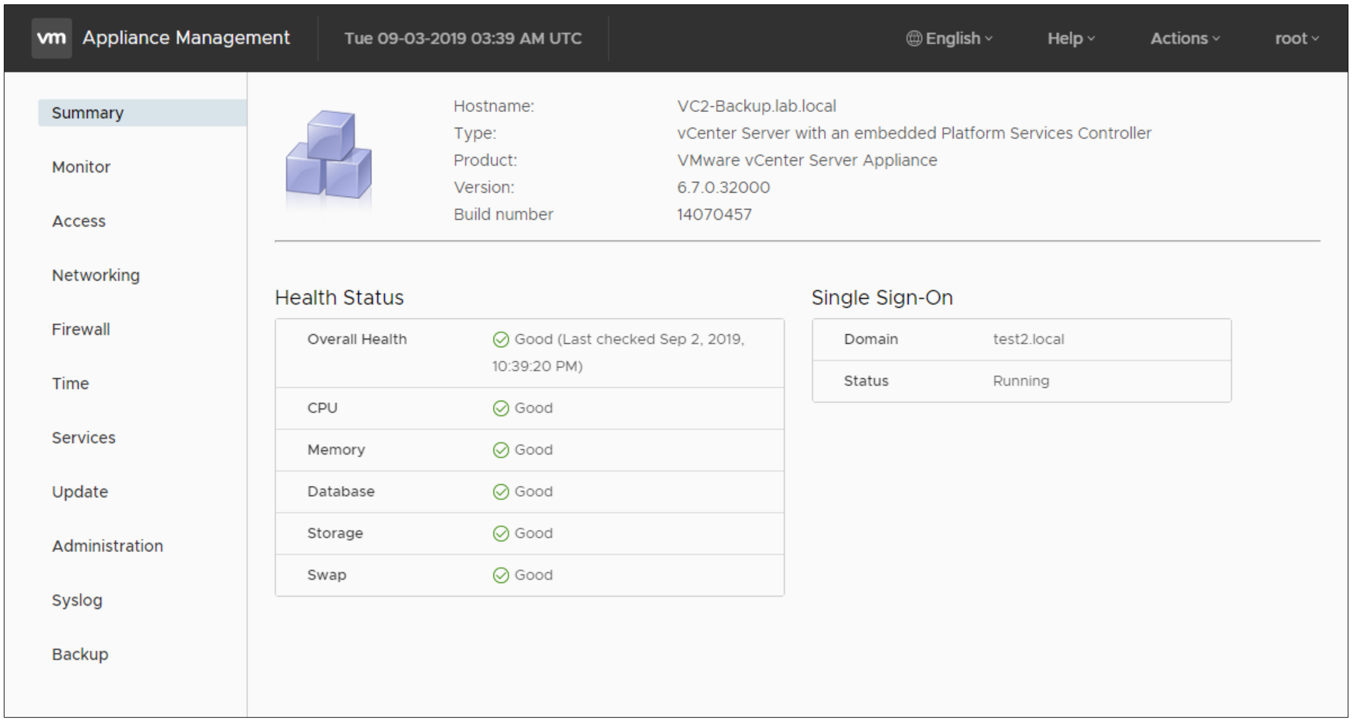
Setup is in progress. Services on this appliance are starting.

2%

Starting VMware Authentication Framework...

That's all there is to the setup. You can configure it when its done through the appliance setup page. This is the normal address for the vCenter Server but put :5480 at the end. For example https://vCenter.vsphere.local:5480

That page will allow you make changes to many of the parameters as you can see here.



| | |
|---|---|
| Hostname: | VC2-Backup.lab.local |
| Type: | vCenter Server with an embedded Platform Services Controller |
| Product: | VMware vCenter Server Appliance |
| Version: | 6.7.0.32000 |
| Build number | 14070457 |

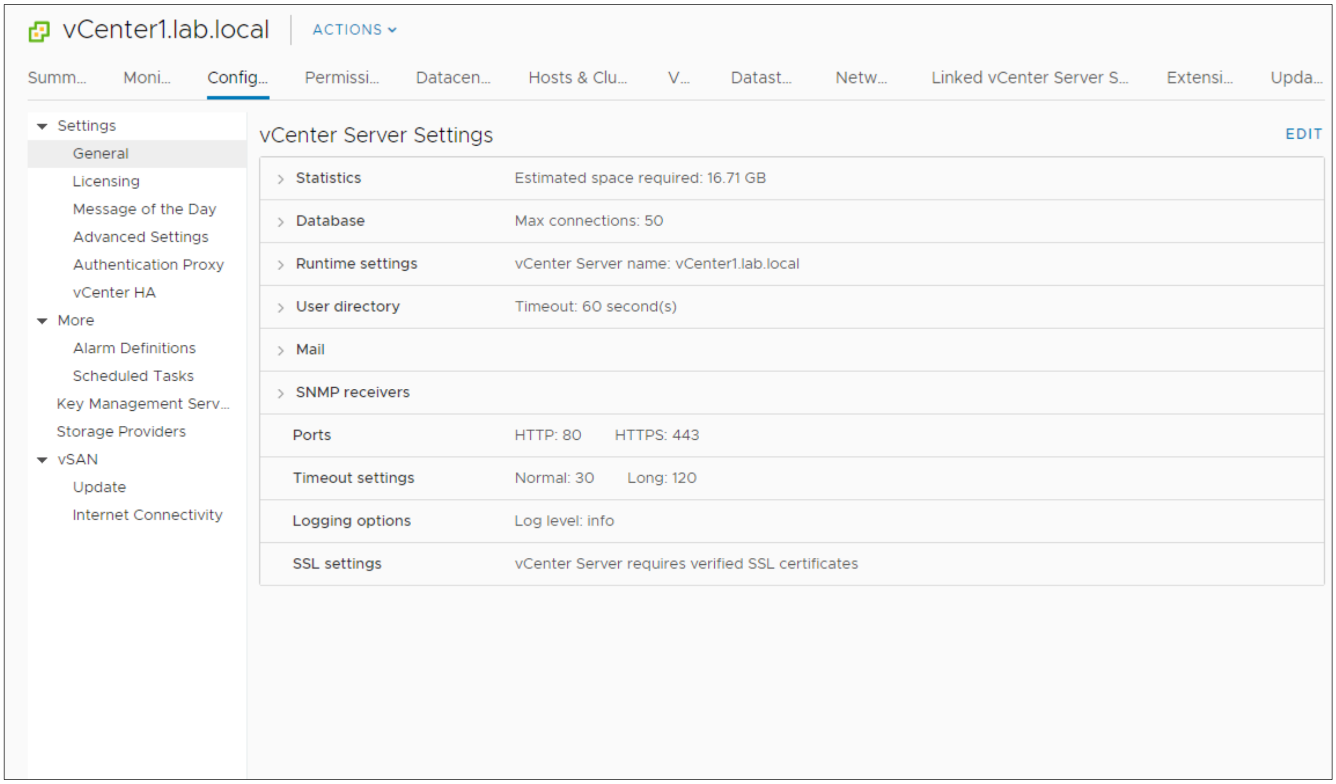
Health Status

| | |
|---|---|
| Overall Health | ✓ Good (Last checked Sep 2, 2019, 10:39:20 PM) |
| CPU | ✓ Good |
| Memory | ✓ Good |
| Database | ✓ Good |
| Storage | ✓ Good |
| Swap | ✓ Good |

Single Sign-On

| | |
|---|---|
| Domain | test2.local |
| Status | Running |

There are quite a few setting you can set through the HTML5 UI as well as seen here.

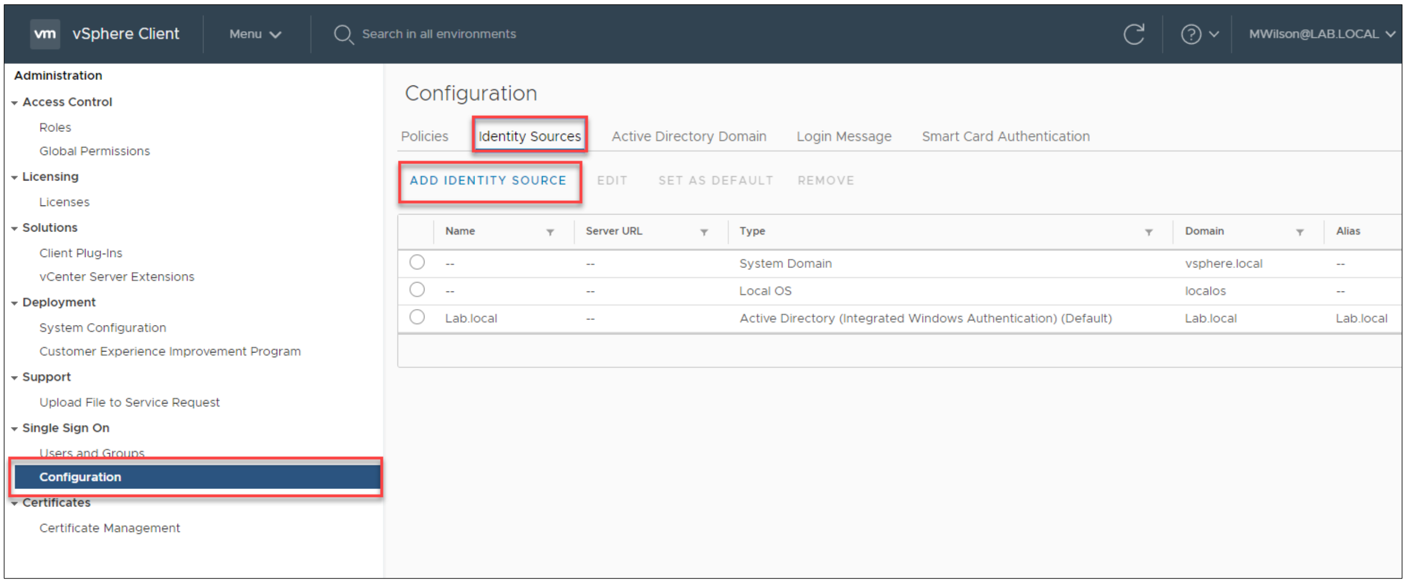


vCenter Server Settings

| | |
|---|---|
| Statistics | Estimated space required: 16.71 GB |
| Database | Max connections: 50 |
| Runtime settings | vCenter Server name: vCenter1.lab.local |
| User directory | Timeout: 60 second(s) |
| Mail | |
| SNMP receivers | |
| Ports | HTTP: 80 HTTPS: 443 |
| Timeout settings | Normal: 30 Long: 120 |
| Logging options | Log level: info |
| SSL settings | vCenter Server requires verified SSL certificates |

## *Objective 4.7 – Set up identity sources*

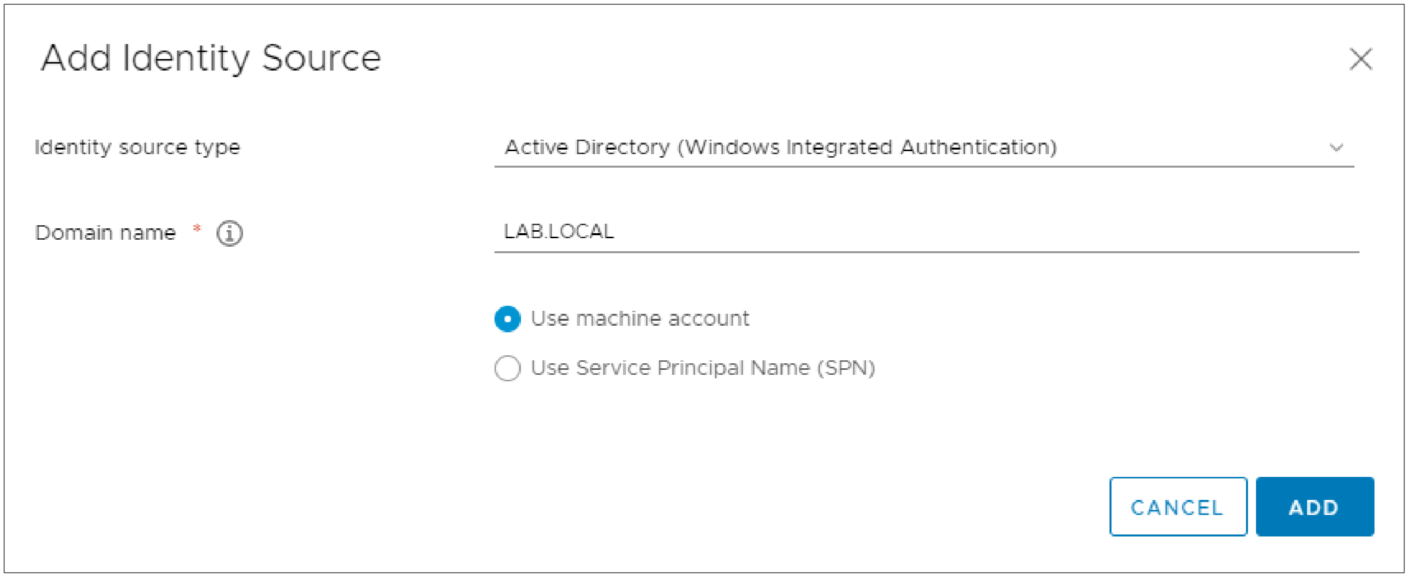
You can setup additional identity sources in your VMware environment to allow more granular control of permissions and for better management. You can set them up by going to the Menu at the top and clicking on Administration. Then going to configuration and adding the identity source.



Configuration

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

An Active Directory, AD over LDAP, or OpenLDAP identity source can be used. You can use a machine account in Active Directory or a Service Principle Name to authenticate.


Add Identity Source

Identity source type: Active Directory (Windows Integrated Authentication)

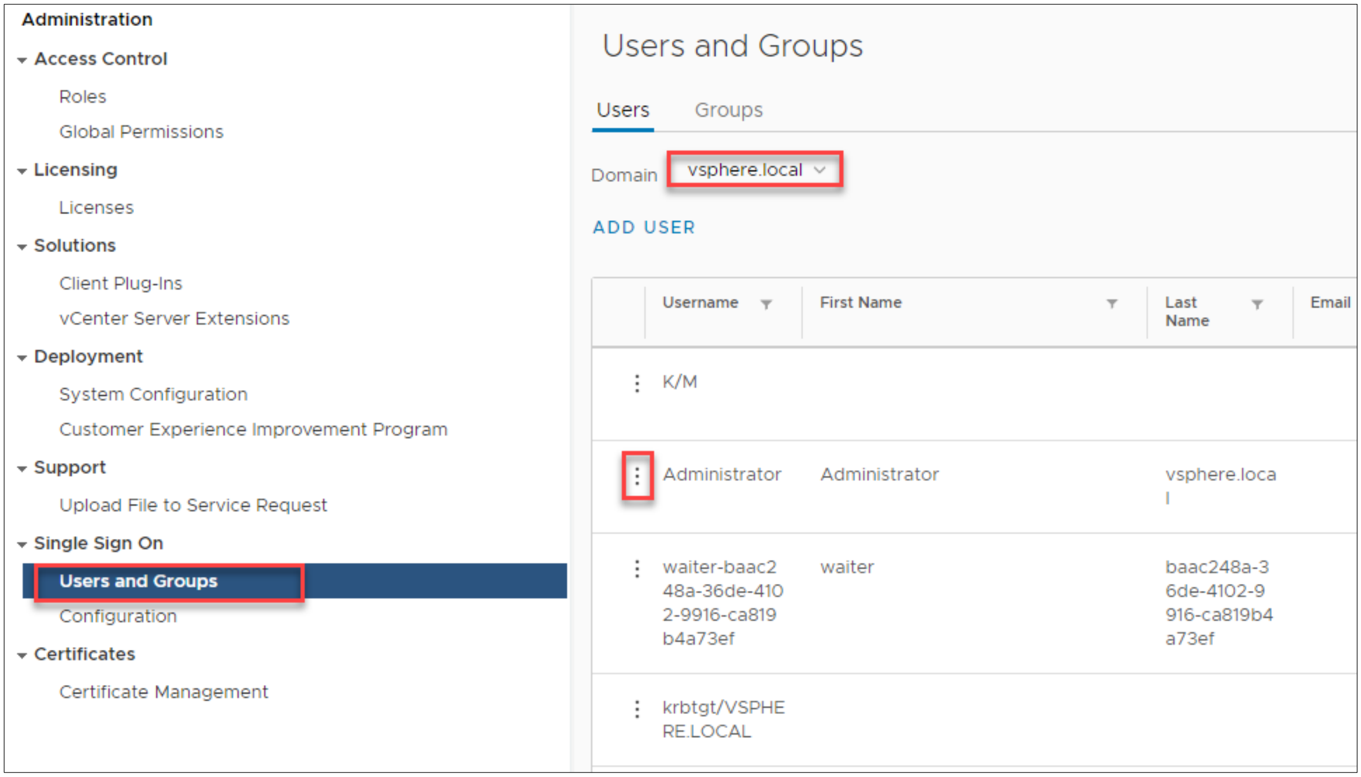
Domain name *: LAB.LOCAL

● Use machine account

○ Use Service Principal Name (SPN)

## *Objective 4.8 – Configure an SSO domain*

The only real way of configuring SSO that I can find is just users. This is done from within the same place as our identity sources. Instead of configuration menu item, you click on Users and Groups right above that. This allows you to see the Users for your SSO. You then click on the 3 dots in front of the user to change/edit/delete them.



Users and Groups

Domain: vsphere.local

| Username | First Name | Last Name | Email |
|---|---|---|---|
| K/M | | | |
| Administrator | Administrator | vsphere.local | |
| waiter-baac248a-36de-4102-9916-ca819b4a73ef | waiter | baac248a-36de-4102-9916-ca819b4a73ef | |
| krbtgt/VSPHERE.LOCAL | | | |

That’s it. Moving on!

# Section 5 – Performance-tuning and Optimizing a VMware vSphere Solution

## *Objective 5.1 – Determine effective snapshot use cases*

Many companies use the term snapshot. There are numerous definitions for snapshots that vary on the company. We should first define what VMware does with snapshots.

VMware preserves 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 more 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 be used for reverting back to the original (if needed) after small changes. Most backup tools DO use snapshots as part of their process, but it is only used 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.

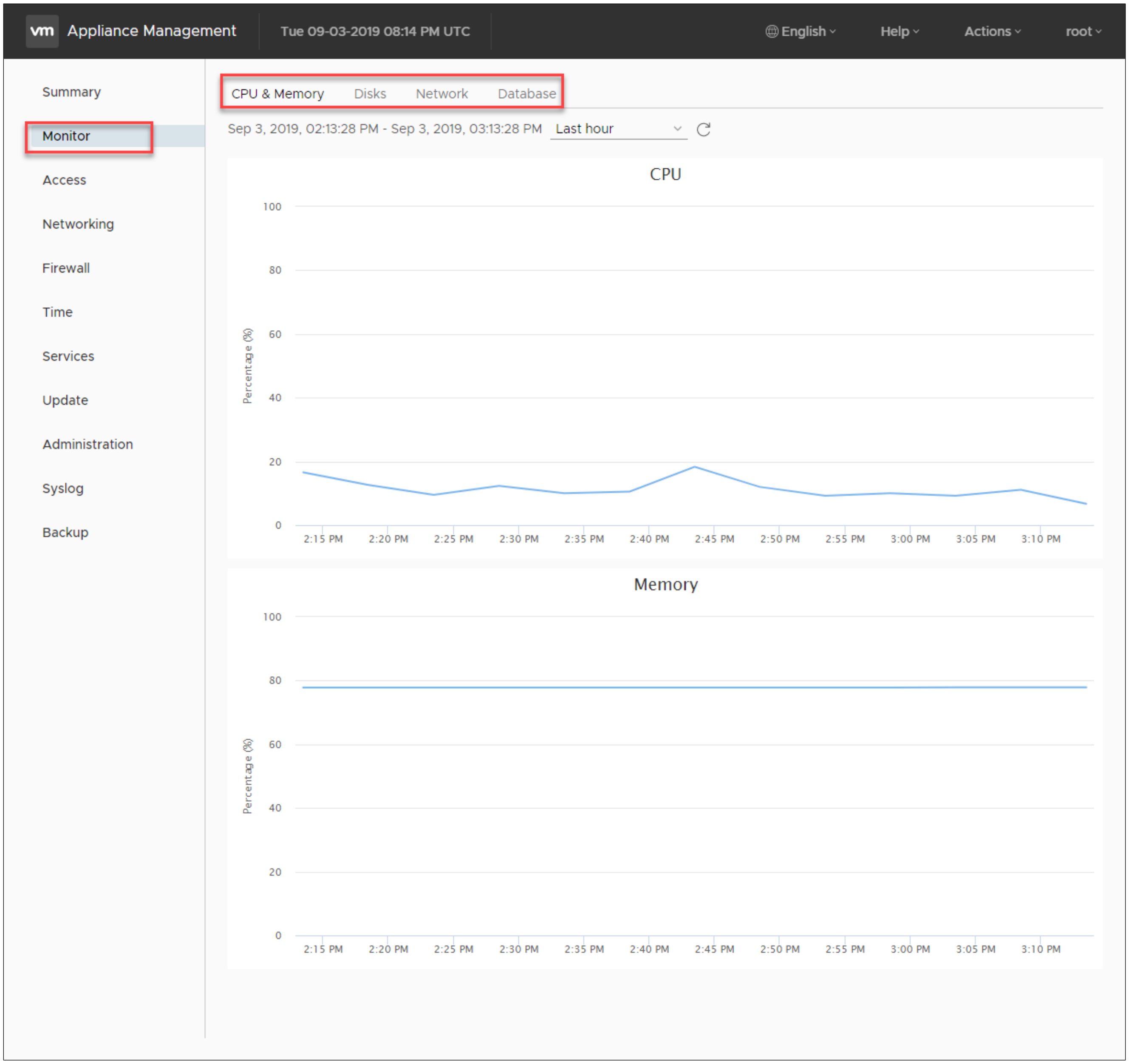
- Don’t use snapshots as backups – major performance degradation can occur and I have seen people lose months of data or more when the chain got too long.
- 32 snapshots are supported, but it’s better not to test this.
- Don’t use a snapshot longer than 72 hrs.
- Ensure if you are using a 3rd Party backup 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.

Most use cases involve you changing the VM or upgrading and once you find out it does or doesn’t work, you remove the snapshot. A good example of this is Microsoft Windows Updates. Create a snapshot, install the updates and test. If the updates haven’t broken anything, consolidate. Another use case might be installation or upgrade of an important program. Or a Dev use case of changing code and executing to determine if it works. The common thread between all the use cases is temporariness. These use cases are for snapshots running a very short period of time.

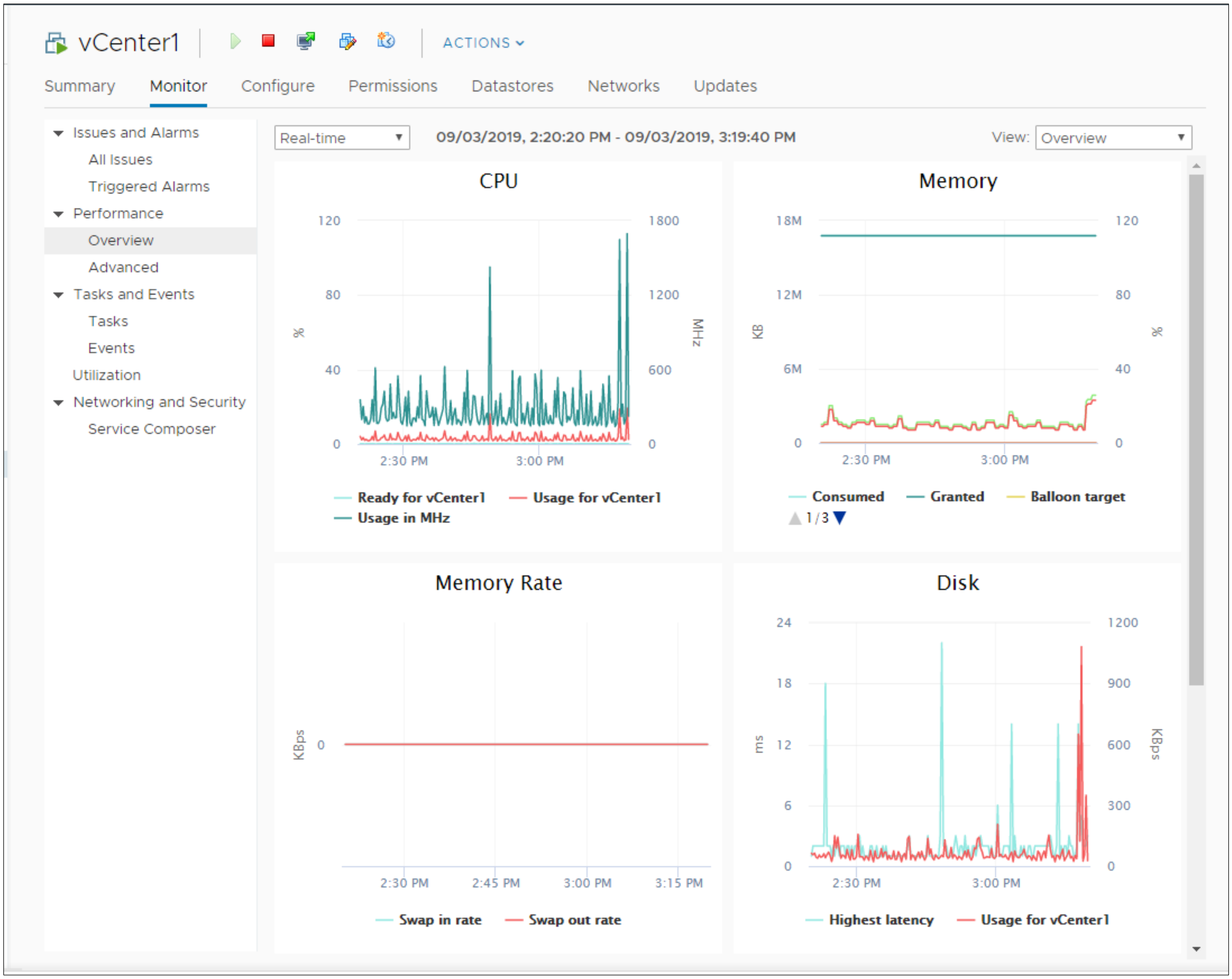
Storytime. 😊 I had a company that called in once that was creating snapshots for their Microsoft Exchange Server. They were taking one every day and using it as a backup. When I was called, they were at about a year of snapshots. Their server wasn't turning on and trying to remove the snapshots wasn't working. Consolidation takes time and a bit more space. We tried to consolidate but you can only merge 32 snapshots at a time. They got impatient about 25% through the process and tried to turn it on again. When that didn't work, they had to restore from tape backup and lost a decent amount of data.

## *Objective 5.2 – Monitor resources of VCSA in a vSphere environment*

Monitoring resources can be done from more than one place. The first place is in the vCenter appliance management page at :5480. After you log into it, you have the option on the navigation pane called Monitor. This is what it looks like:

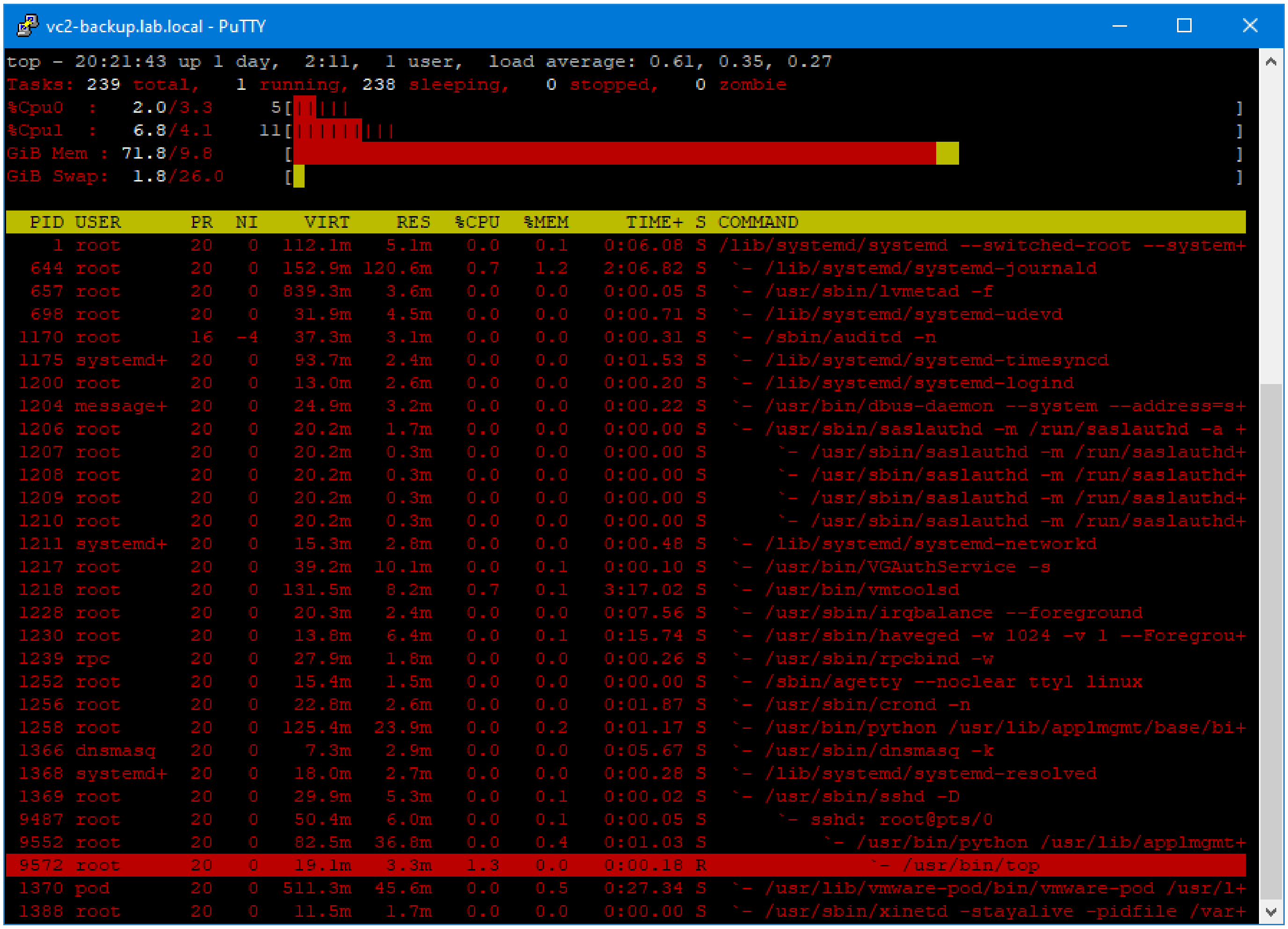


Notice the subheadings. You can monitor CPU and Memory, Disks, Networking, and the database. You can change the time period to include metrics up to the last year. Since the VCSA is also a VM, you can view this from inside the vSphere HTML5 client. This view allows you to get a bit more granular. You are looking at it from the hosts perspective whereas the Appliance Management page is from within the VM. Both are important places to give you a full look at how the vCenter is performing. Here is a screenshot of inside the HTML5 client of my vCenter Appliance.



09/03/2019, 2:20:20 PM - 09/03/2019, 3:19:40 PM

You can attach to the vCenter via SSH or console and run TOP for a per process view of the appliance. Here is what that looks like



```
top - 20:21:43 up 1 day,  2:11,  1 user,  load average: 0.61, 0.35, 0.27
Tasks: 239 total,   1 running, 238 sleeping,   0 stopped,   0 zombie
%Cpu0  :   2.0/3.3     5[|||||                                                                    ]
%Cpu1  :   6.8/4.1    11[|||||||||||                                                              ]
GiB Mem : 71.8/9.8      [                                                                         ]
GiB Swap:  1.8/26.0     [                                                                         ]

  PID USER      PR  NI    VIRT    RES  %CPU  %MEM     TIME+ S COMMAND
    1 root      20   0  112.1m   5.1m   0.0   0.1   0:06.08 S /lib/systemd/systemd --switched-root --system+
  644 root      20   0  152.9m 120.6m   0.7   1.2   2:06.82 S  `- /lib/systemd/systemd-journald
  657 root      20   0  839.3m   3.6m   0.0   0.0   0:00.05 S  `- /usr/sbin/lvmetad -f
  698 root      20   0   31.9m   4.5m   0.0   0.0   0:00.71 S  `- /lib/systemd/systemd-udevd
 1170 root      16  -4   37.3m   3.1m   0.0   0.0   0:00.31 S  `- /sbin/auditd -n
 1175 systemd+  20   0   93.7m   2.4m   0.0   0.0   0:01.53 S  `- /lib/systemd/systemd-timesyncd
 1200 root      20   0   13.0m   2.6m   0.0   0.0   0:00.20 S  `- /lib/systemd/systemd-logind
 1204 message+  20   0   24.9m   3.2m   0.0   0.0   0:00.22 S  `- /usr/bin/dbus-daemon --system --address=s+
 1206 root      20   0   20.2m   1.7m   0.0   0.0   0:00.00 S  `- /usr/sbin/saslauthd -m /run/saslauthd -a +
 1207 root      20   0   20.2m   0.3m   0.0   0.0   0:00.00 S      `- /usr/sbin/saslauthd -m /run/saslauthd+
 1208 root      20   0   20.2m   0.3m   0.0   0.0   0:00.00 S      `- /usr/sbin/saslauthd -m /run/saslauthd+
 1209 root      20   0   20.2m   0.3m   0.0   0.0   0:00.00 S      `- /usr/sbin/saslauthd -m /run/saslauthd+
 1210 root      20   0   20.2m   0.3m   0.0   0.0   0:00.00 S      `- /usr/sbin/saslauthd -m /run/saslauthd+
 1211 systemd+  20   0   15.3m   2.8m   0.0   0.0   0:00.48 S  `- /lib/systemd/systemd-networkd
 1217 root      20   0   39.2m  10.1m   0.0   0.1   0:00.10 S  `- /usr/bin/VGAuthService -s
 1218 root      20   0  131.5m   8.2m   0.7   0.1   3:17.02 S  `- /usr/bin/vmtoolsd
 1228 root      20   0   20.3m   2.4m   0.0   0.0   0:07.56 S  `- /usr/sbin/irqbalance --foreground
 1230 root      20   0   13.8m   6.4m   0.0   0.1   0:15.74 S  `- /usr/sbin/haveged -w 1024 -v 1 --Foregrou+
 1239 rpc       20   0   27.9m   1.8m   0.0   0.0   0:00.26 S  `- /usr/sbin/rpcbind -w
 1252 root      20   0   15.4m   1.5m   0.0   0.0   0:00.00 S  `- /sbin/agetty --noclear tty1 linux
 1256 root      20   0   22.8m   2.6m   0.0   0.0   0:01.87 S  `- /usr/sbin/crond -n
 1258 root      20   0  125.4m  23.9m   0.0   0.2   0:01.17 S  `- /usr/bin/python /usr/lib/applmgmt/base/bi+
 1366 dnsmasq   20   0    7.3m   2.9m   0.0   0.0   0:05.67 S  `- /usr/sbin/dnsmasq -k
 1368 systemd+  20   0   18.0m   2.7m   0.0   0.0   0:00.28 S  `- /lib/systemd/systemd-resolved
 1369 root      20   0   29.9m   5.3m   0.0   0.1   0:00.02 S  `- /usr/sbin/sshd -D
 9487 root      20   0   50.4m   6.0m   0.0   0.1   0:00.05 S      `- sshd: root@pts/0
 9552 root      20   0   82.5m  36.8m   0.0   0.4   0:01.03 S          `- /usr/bin/python /usr/lib/applmgmt+
 9572 root      20   0   19.1m   3.3m   1.3   0.0   0:00.18 R              `- /usr/bin/top
 1370 pod       20   0  511.3m  45.6m   0.0   0.5   0:27.34 S  `- /usr/lib/vmware-pod/bin/vmware-pod /usr/l+
 1388 root      20   0   11.5m   1.7m   0.0   0.0   0:00.00 S  `- /usr/sbin/xinetd -stayalive -pidfile /var+
```

These are the most common ways you would monitor resources of your VCSA.

## *Objective 5.3 – Identify impacts of VM configurations*

There much to unpack with this objective. I will work through best practices and try to stay brief.

- While you want to allocate the resources that your VM needs to perform, you don't want to over-allocate as this can actually perform worse. Make sure there are still enough resources for ESXi itself as well.
- Unused or unnecessary hardware on VM can affect performance of both the host and all VMs on it.
- As mentioned above, over allocation of vCPU and memory resources will not necessarily increase performance and it might lower it.

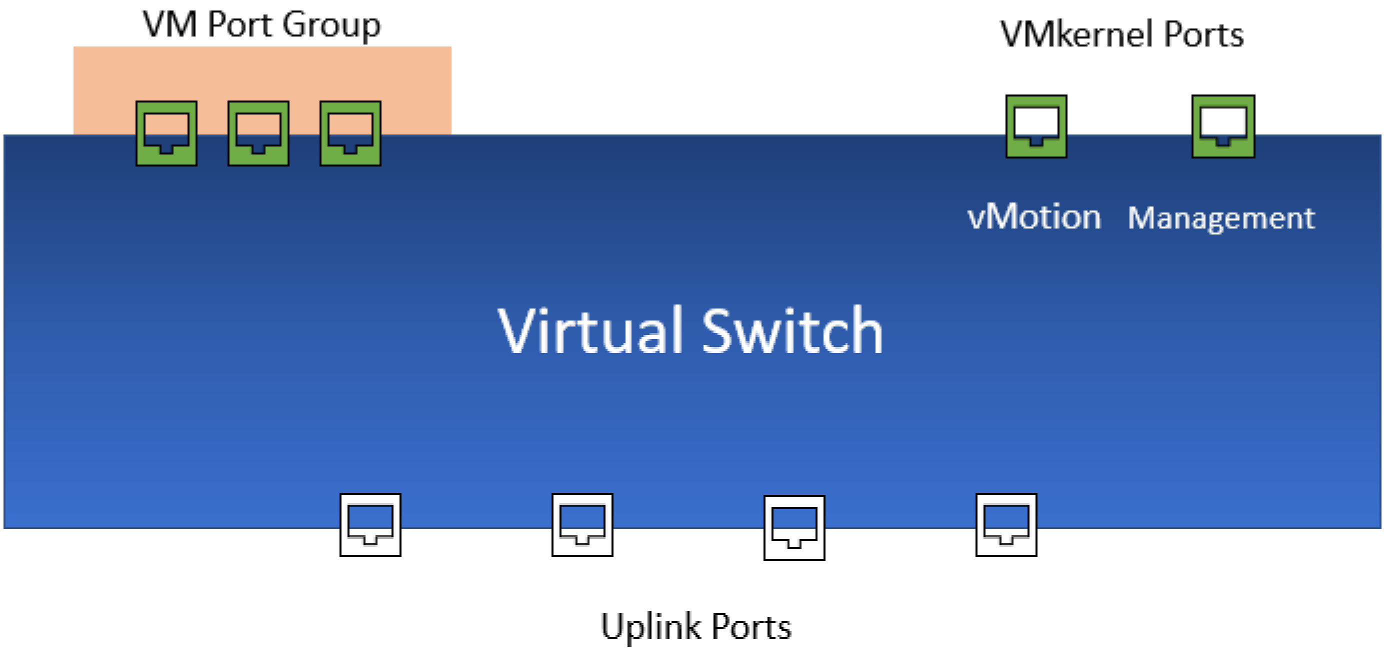
- For most workloads, hyperthreading will increase performance. Hyperthreading is like a person trying to eat food. You have one mouth to consume the food, but if you are only using one arm to put the food in, it isn't as fast as it could be. If you use both arms (enabling hyperthreading) you still only have one mouth (one core) but you aren't waiting for more food and just keep constantly chewing. Certain workloads that keep CPU utilization high, benefit less from hyperthreading.
- Be aware of NUMA (Non-Uniform Memory Access). Memory is "owned" by sockets. If you use more memory than that socket owns, you need to use memory from the other socket (if available). This causes a small delay because it has to move across the bus vs right next to the processor. This can add up. (Oversimplified but the idea is there). There are policies that can be set that could help if needed. Not in the scope of this certification though.
- Not having enough physical memory can cause VMs to use slower methods of memory reclamation all the way to disk caching. This causes performance degradation.
- Creating shares and limits on your machine may not have the result you believe. Weigh those options carefully before you apply them.
- Make sure you use VM Tools in your VMs as they add a number of useful and performance increasing solutions.
- The hardware you use in the configuration can also change performance. For example, using PVSCSI vs LSI SAS or using VMXNET vs E1000 NICs can make a decent performance jump.
- Make sure you use VMware snapshots how they were intended and not for long periods of time.
- There are different types of VMDKS you can create. They include thin provisioned, thick (lazy zeroed), and thick (eager zeroed). There are reasons you might utilize them. Thin disks are the best in a scenario where you may not have all the space yet. You may need to buy more disks or they may be already on their way. Eventually you will have this space. It is important that you monitor your space to make sure you don't consume it before you have it. If you do, the VM will be suspended best case, worst case you can lose data. Thick (lazy zero) is when you fence all that space off for that disk up front. You can't over-provision this, you have to already have the disk space. The "lazy zero" comes in play when you go to use the space. VMware will need to format the disk block before using it. This can potentially be a slow down if there are a high number of writes to the disk. If the VM is more read heavy, you are just fine. Thick (eager zero) will take more time to create, because it formats the whole disk up front before use. This type if best for a VM with heavy writes and reads such as a DB server etc.

Keep these in mind when creating VMs and also take a look at the VMware Performance Best Practices guide here.

# Section 7 – Administrative and Operational Tasks in a VMware vSphere Solution

## *Objective 7.1 – Manage virtual networking*

I've gone over virtual networking a bit already. But there are two basic types of switches to manage in vSphere. Virtual Standard Switches and Virtual Distributed Switches. They both have the same components. Virtual Ports Groups, VMkernel Ports, and Uplink Ports. Here is a diagram depicting how it might look on a host



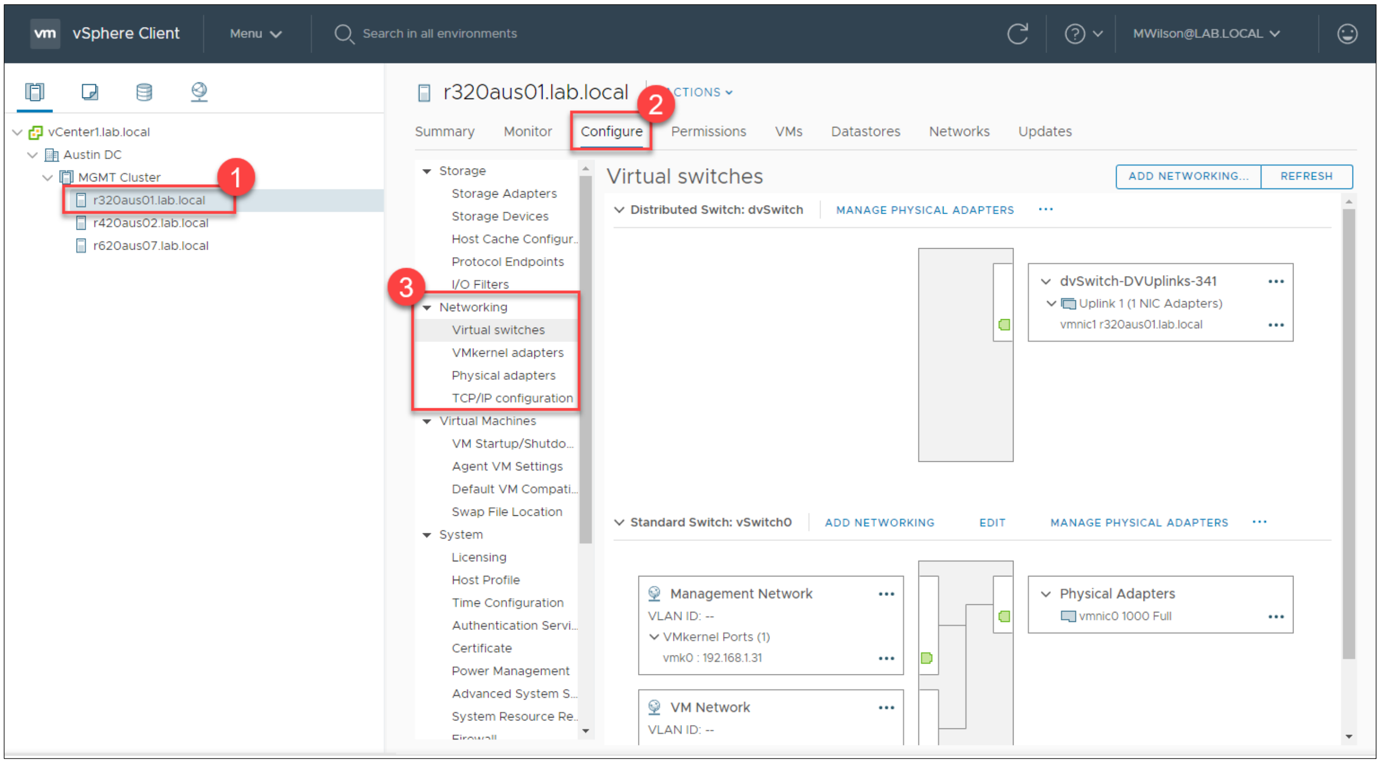
VMkernel ports are used for management purposes. When you set it up, you can choose using it for the following purposes

- vMotion – this is used to migrate VMs
- Provisioning – used for VM cold migration, cloning, and snapshot migration.
- Fault Tolerance logging – enables Fault Tolerance logging on the host (you can only have one per host)
- Management - management communication between hosts (should have minimum of two for redundancy)
- vSphere Replication – Handles outgoing replication data sent to the vSphere Replication Server
- vSphere Replication NFC – Handles incoming replication data on the target replication site.
- vSAN – allows for vSAN traffic, every host that is part of a vSAN cluster must have one.

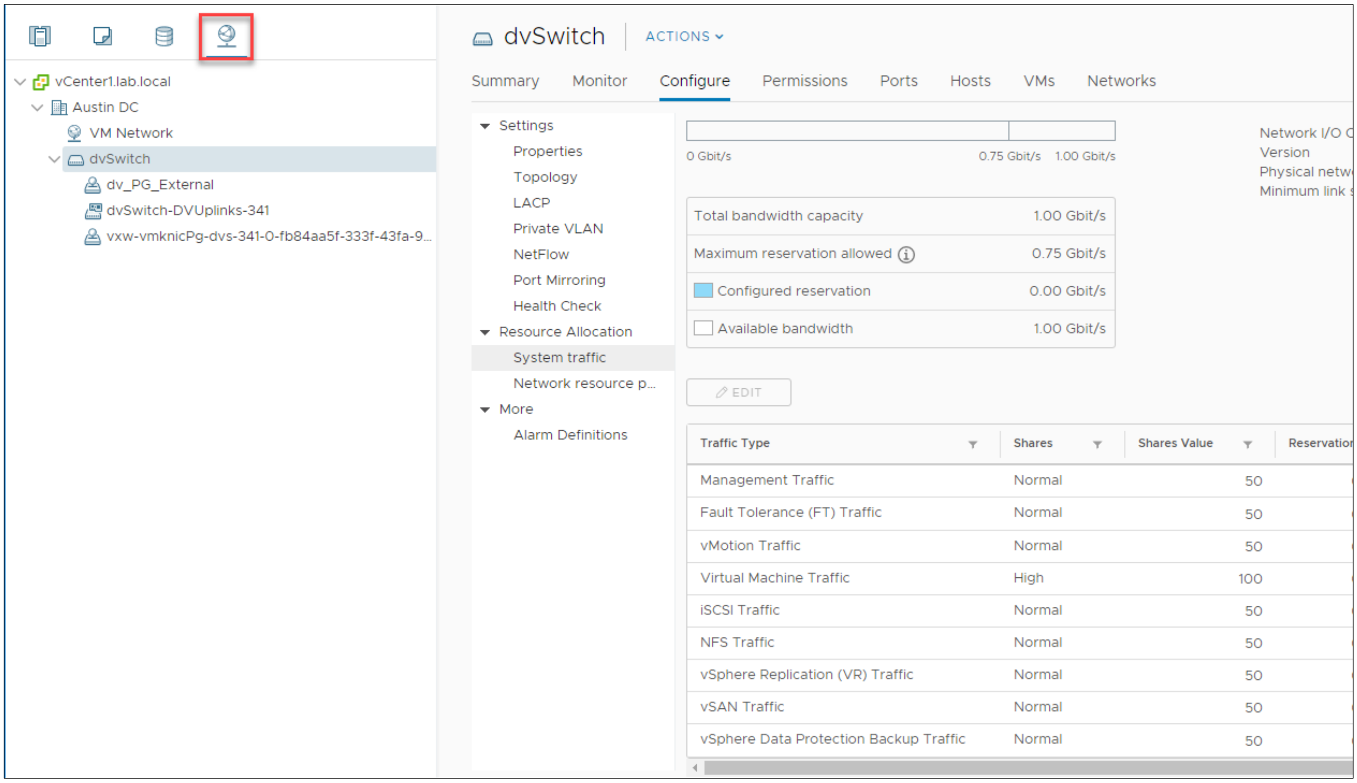
VM Port Groups are for VM network traffic. Each of the VMs have a virtual NIC which will be part of a VM port group.

Uplink ports are connected to physical NICs. A Virtual Distributed Switch will have an uplink port group that physical NICs from multiple hosts.

You can manage your networking from a few locations in the HTML5 client. You can also manage hosts from the host HTML5 client. In the HTML5 client you manage networking from Host > Configure > Networking shown here.



You can then change manage the components as needed. If you need to manage a Virtual Distributed Switch you can do that there as well or you can create a VDS on the networking tab in the navigation pane.

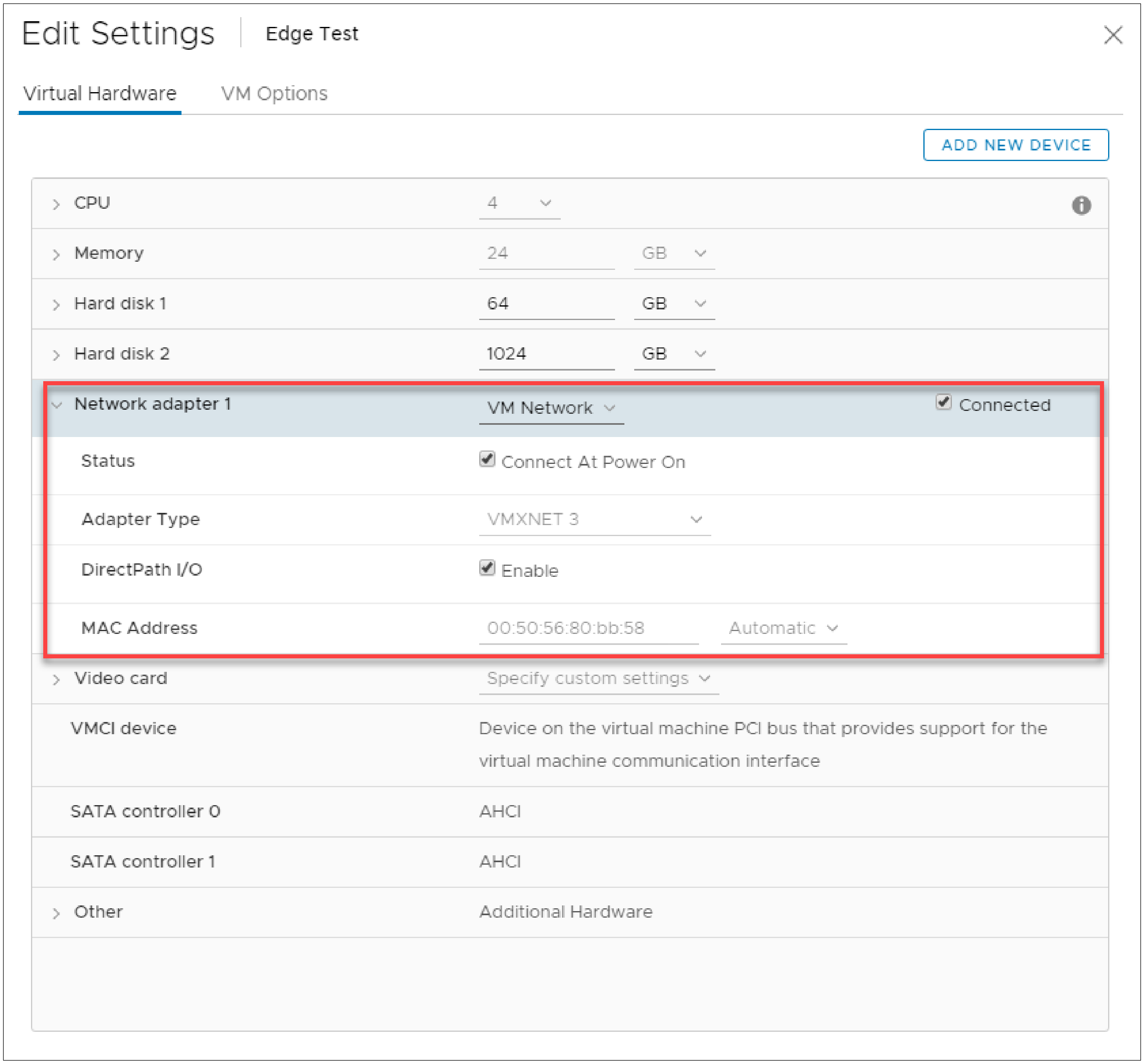


| | |
|---|---|
| Total bandwidth capacity | 1.00 Gbit/s |
| Maximum reservation allowed ⓘ | 0.75 Gbit/s |
| 🟦 Configured reservation | 0.00 Gbit/s |
| □ Available bandwidth | 1.00 Gbit/s |

| Traffic Type | Shares | Shares Value | Reservatio |
|---|---|---|---|
| Management Traffic | Normal | 50 | |
| Fault Tolerance (FT) Traffic | Normal | 50 | |
| vMotion Traffic | Normal | 50 | |
| Virtual Machine Traffic | High | 100 | |
| iSCSI Traffic | Normal | 50 | |
| NFS Traffic | Normal | 50 | |
| vSphere Replication (VR) Traffic | Normal | 50 | |
| vSAN Traffic | Normal | 50 | |
| vSphere Data Protection Backup Traffic | Normal | 50 | |

You can configure shares and other settings here as well as you can see. You can find more info here if needed.

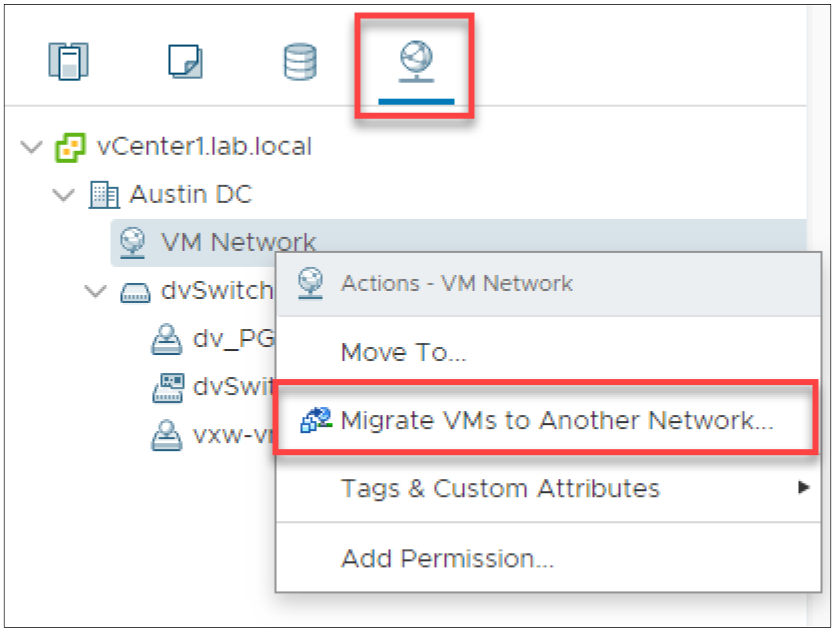
There is also managing the virtual networking of the VM. If you right click on the VM and then select Edit Settings. You can edit the networking adapter type and what virtual network the VM is connected to.



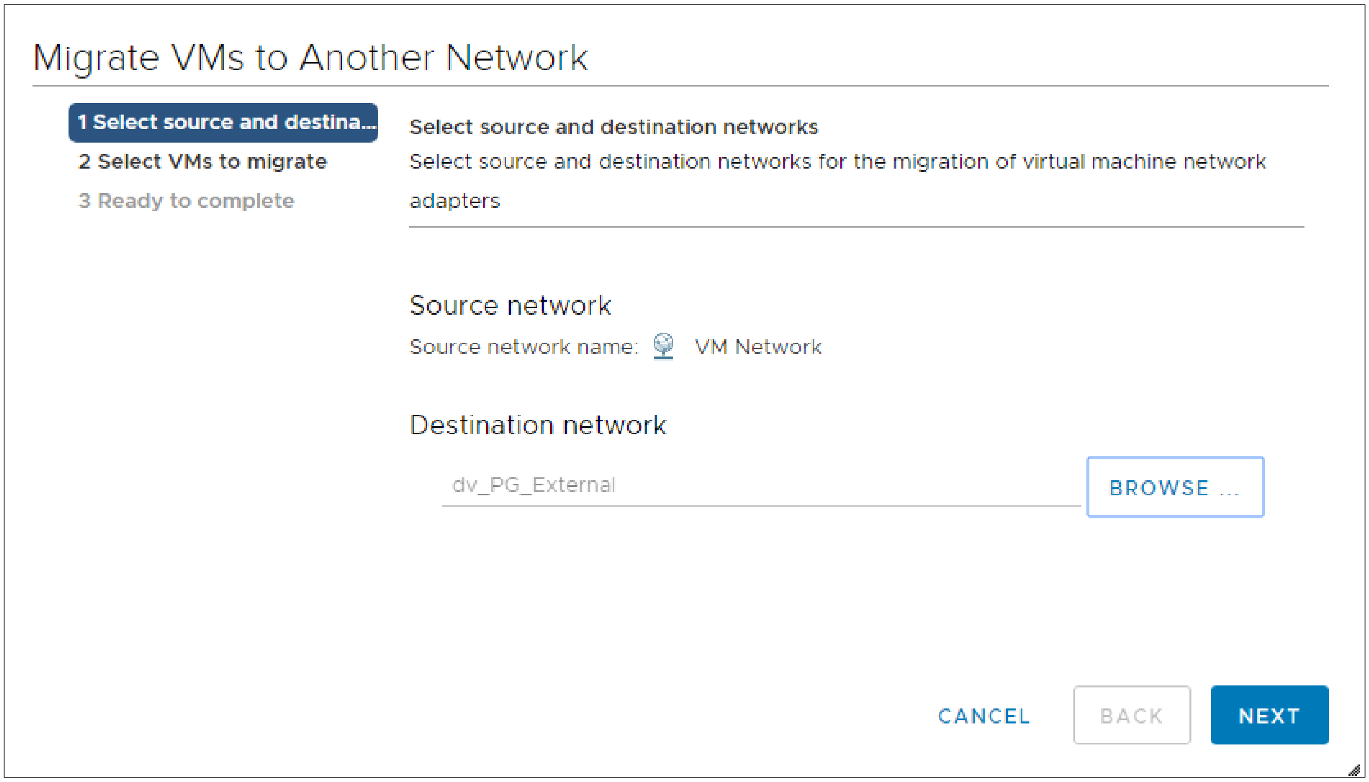
Edit Settings | Edge Test

| | | |
|---|---|---|
| CPU | 4 | |
| Memory | 24 | GB |
| Hard disk 1 | 64 | GB |
| Hard disk 2 | 1024 | GB |
| Network adapter 1 | VM Network | ☑ Connected |
| Status | ☑ Connect At Power On | |
| Adapter Type | VMXNET 3 | |
| DirectPath I/O | ☑ Enable | |
| MAC Address | 00:50:56:80:bb:58 | Automatic |
| Video card | Specify custom settings | |
| VMCI device | Device on the virtual machine PCI bus that provides support for the virtual machine communication interface | |
| SATA controller 0 | AHCI | |
| SATA controller 1 | AHCI | |
| Other | Additional Hardware | |

You can also migrate multiple VMs to another network if you go to the network tab in the navigation pane. Clicking the following will pop up a wizard.



In the wizard you select the destination network.



Migrate VMs to Another Network

Select source and destination networks

Select source and destination networks for the migration of virtual machine network adapters

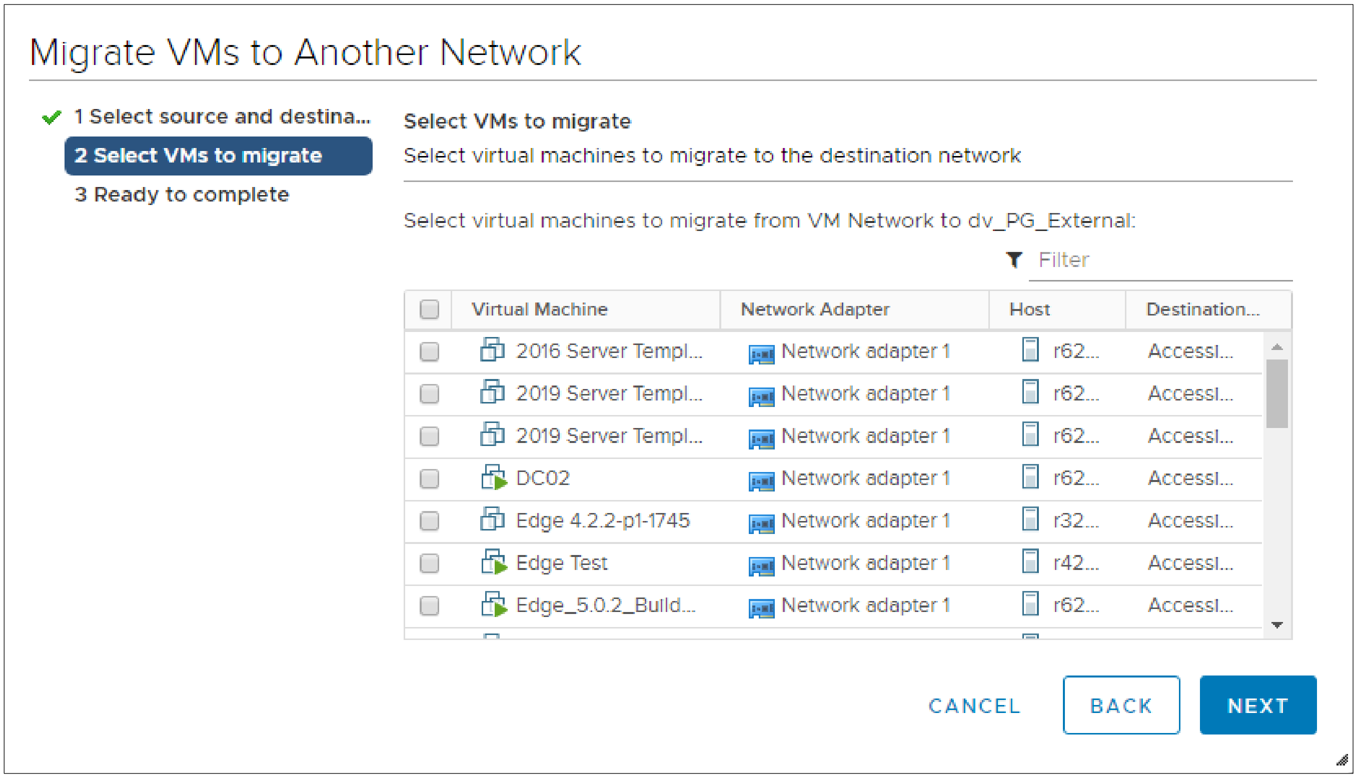
Source network

Source network name: VM Network

Destination network

dv_PG_External

Then you select all the VMs you want to migrate.



Migrate VMs to Another Network

✓ 1 Select source and destina...
2 Select VMs to migrate
3 Ready to complete

Select VMs to migrate

Select virtual machines to migrate to the destination network

Select virtual machines to migrate from VM Network to dv_PG_External:

| □ | Virtual Machine | Network Adapter | Host | Destination... |
|---|---|---|---|---|
| □ | 2016 Server Templ... | Network adapter 1 | r62... | Accessi... |
| □ | 2019 Server Templ... | Network adapter 1 | r62... | Accessi... |
| □ | 2019 Server Templ... | Network adapter 1 | r62... | Accessi... |
| □ | DC02 | Network adapter 1 | r62... | Accessi... |
| □ | Edge 4.2.2-p1-1745 | Network adapter 1 | r32... | Accessi... |
| □ | Edge Test | Network adapter 1 | r42... | Accessi... |
| □ | Edge_5.0.2_Build... | Network adapter 1 | r62... | Accessi... |

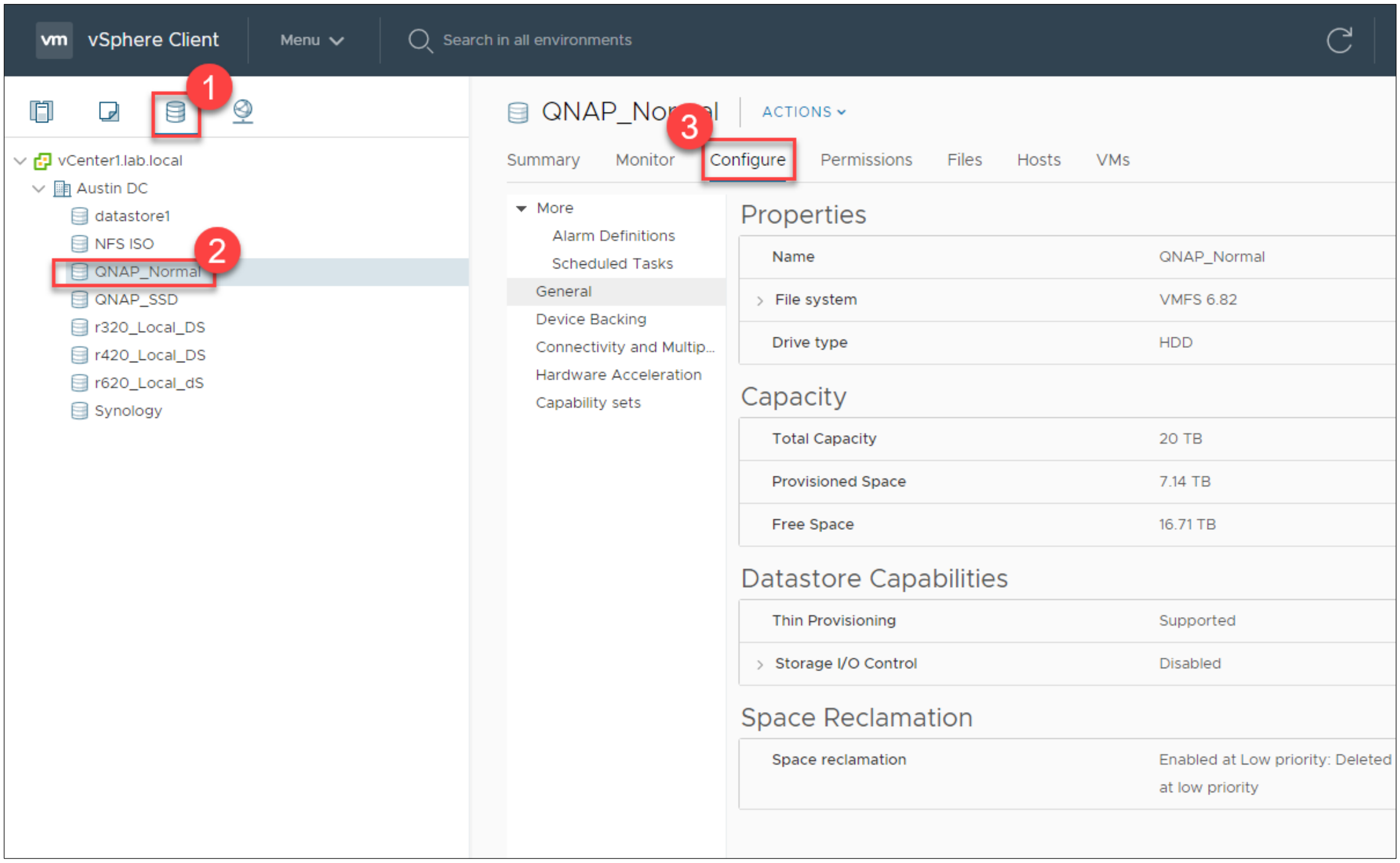
Then you complete it.

## *Objective 7.2 – Manage datastores*

Datastores are logical storage units that can use disk space on one disk or span several. There are multiple types of datastores:

- VMFS
- NFS
- vSAN
- vVOLs

To manage them, you can navigate to the Datastores tab on the navigation pane and select the datastore you want to manage. Then click on Configure on the object pane in the middle.



Properties

| | |
|---|---|
| Name | QNAP_Normal |
| File system | VMFS 6.82 |
| Drive type | HDD |

Capacity

| | |
|---|---|
| Total Capacity | 20 TB |
| Provisioned Space | 7.14 TB |
| Free Space | 16.71 TB |

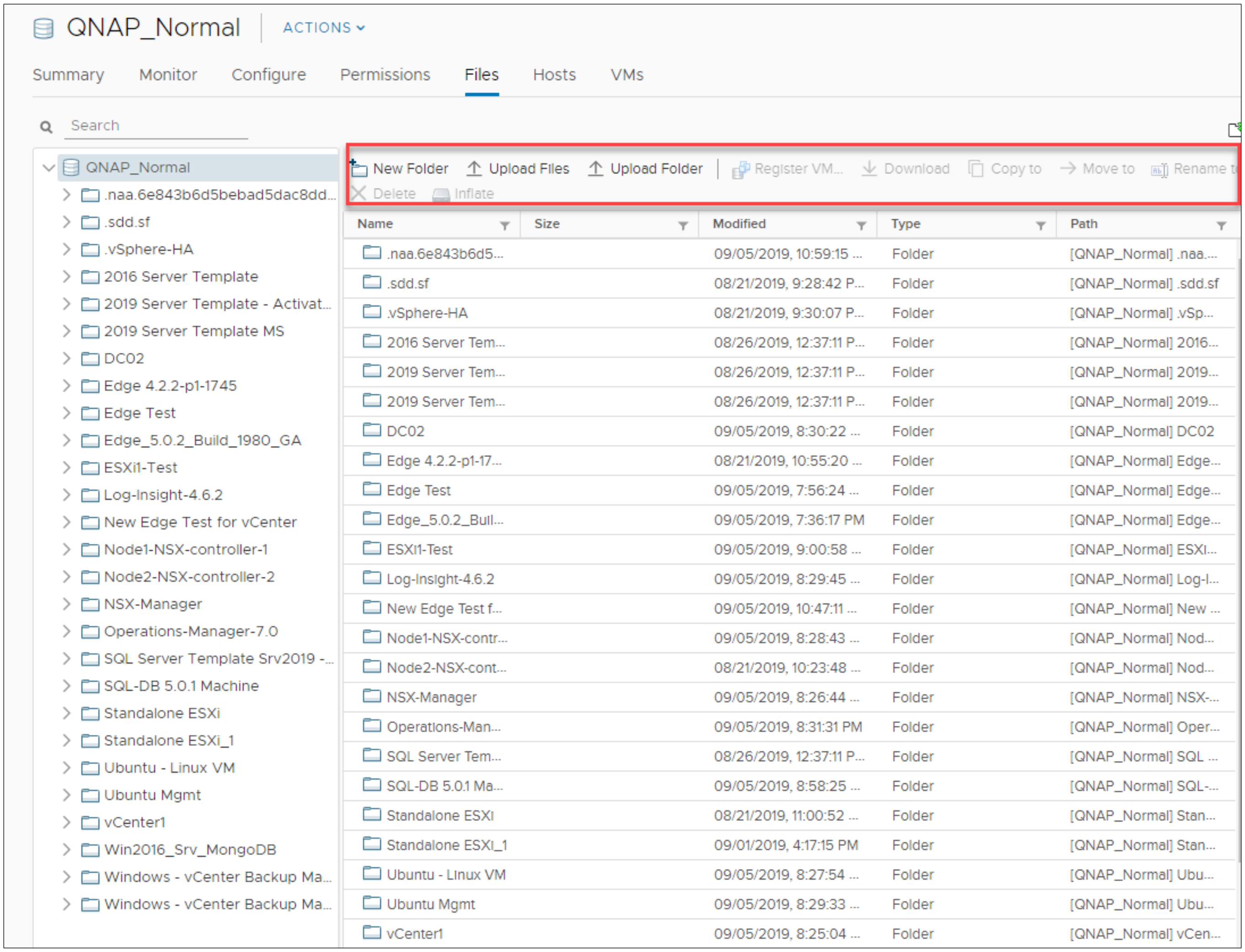
Datastore Capabilities

| | |
|---|---|
| Thin Provisioning | Supported |
| Storage I/O Control | Disabled |

Space Reclamation

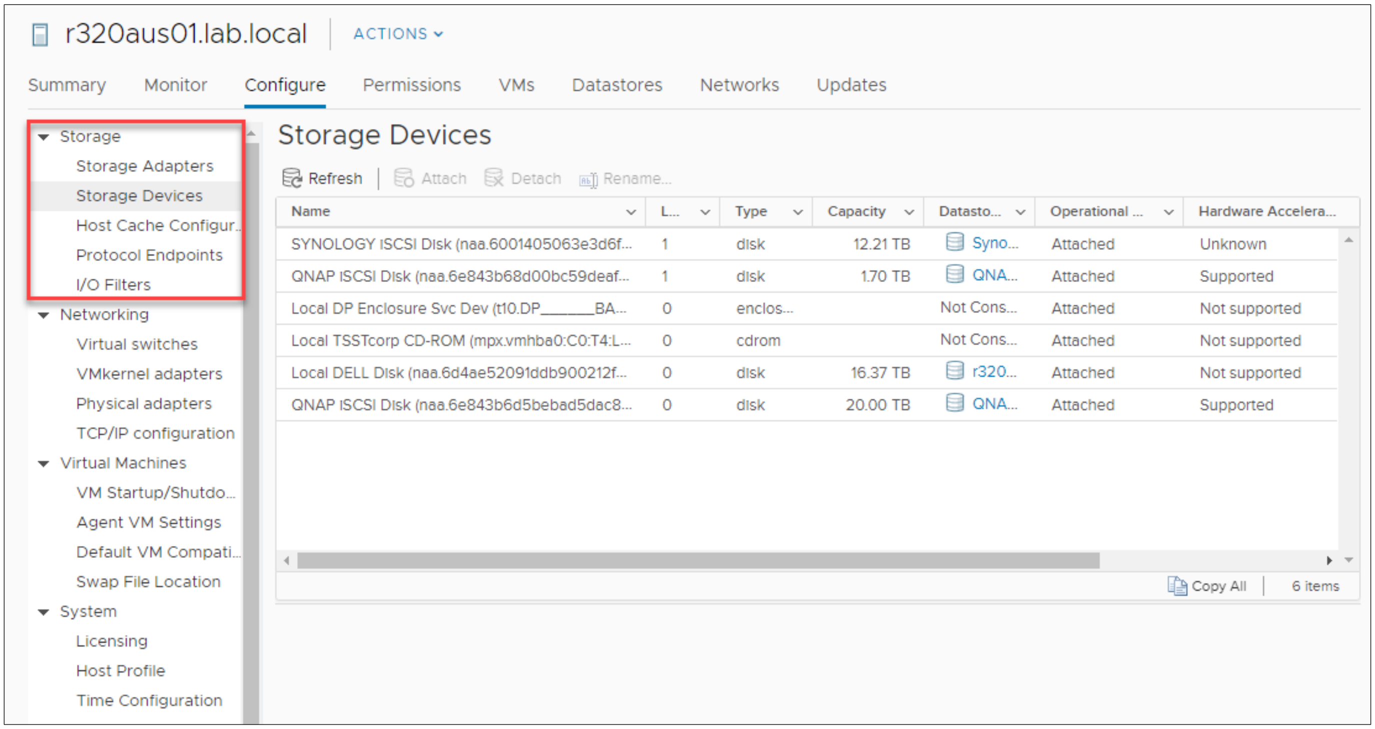
| | |
|---|---|
| Space reclamation | Enabled at Low priority: Deleted at low priority |

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 basic file functions through this as well.



| Name | Size | Modified | Type | Path |
|---|---|---|---|---|
| .naa.6e843b6d5... | | 09/05/2019, 10:59:15 ... | Folder | [QNAP_Normal] .naa.... |
| .sdd.sf | | 08/21/2019, 9:28:42 P... | Folder | [QNAP_Normal] .sdd.sf |
| .vSphere-HA | | 08/21/2019, 9:30:07 P... | Folder | [QNAP_Normal] .vSp... |
| 2016 Server Tem... | | 08/26/2019, 12:37:11 P... | Folder | [QNAP_Normal] 2016... |
| 2019 Server Tem... | | 08/26/2019, 12:37:11 P... | Folder | [QNAP_Normal] 2019... |
| 2019 Server Tem... | | 08/26/2019, 12:37:11 P... | Folder | [QNAP_Normal] 2019... |
| DC02 | | 09/05/2019, 8:30:22 ... | Folder | [QNAP_Normal] DC02 |
| Edge 4.2.2-p1-17... | | 08/21/2019, 10:55:20 ... | Folder | [QNAP_Normal] Edge... |
| Edge Test | | 09/05/2019, 7:56:24 ... | Folder | [QNAP_Normal] Edge... |
| Edge_5.0.2_Buil... | | 09/05/2019, 7:36:17 PM | Folder | [QNAP_Normal] Edge... |
| ESXi1-Test | | 09/05/2019, 9:00:58 ... | Folder | [QNAP_Normal] ESXi... |
| Log-Insight-4.6.2 | | 09/05/2019, 8:29:45 ... | Folder | [QNAP_Normal] Log-I... |
| New Edge Test f... | | 09/05/2019, 10:47:11 ... | Folder | [QNAP_Normal] New ... |
| Node1-NSX-contr... | | 09/05/2019, 8:28:43 ... | Folder | [QNAP_Normal] Nod... |
| Node2-NSX-cont... | | 08/21/2019, 10:23:48 ... | Folder | [QNAP_Normal] Nod... |
| NSX-Manager | | 09/05/2019, 8:26:44 ... | Folder | [QNAP_Normal] NSX-... |
| Operations-Man... | | 09/05/2019, 8:31:31 PM | Folder | [QNAP_Normal] Oper... |
| SQL Server Tem... | | 08/26/2019, 12:37:11 P... | Folder | [QNAP_Normal] SQL ... |
| SQL-DB 5.0.1 Ma... | | 09/05/2019, 8:58:25 ... | Folder | [QNAP_Normal] SQL-... |
| Standalone ESXi | | 08/21/2019, 11:00:52 ... | Folder | [QNAP_Normal] Stan... |
| Standalone ESXi_1 | | 09/01/2019, 4:17:15 PM | Folder | [QNAP_Normal] Stan... |
| Ubuntu - Linux VM | | 09/05/2019, 8:27:54 ... | Folder | [QNAP_Normal] Ubu... |
| Ubuntu Mgmt | | 09/05/2019, 8:29:33 ... | Folder | [QNAP_Normal] Ubu... |
| vCenter1 | | 09/05/2019, 8:25:04 ... | Folder | [QNAP_Normal] vCen... |

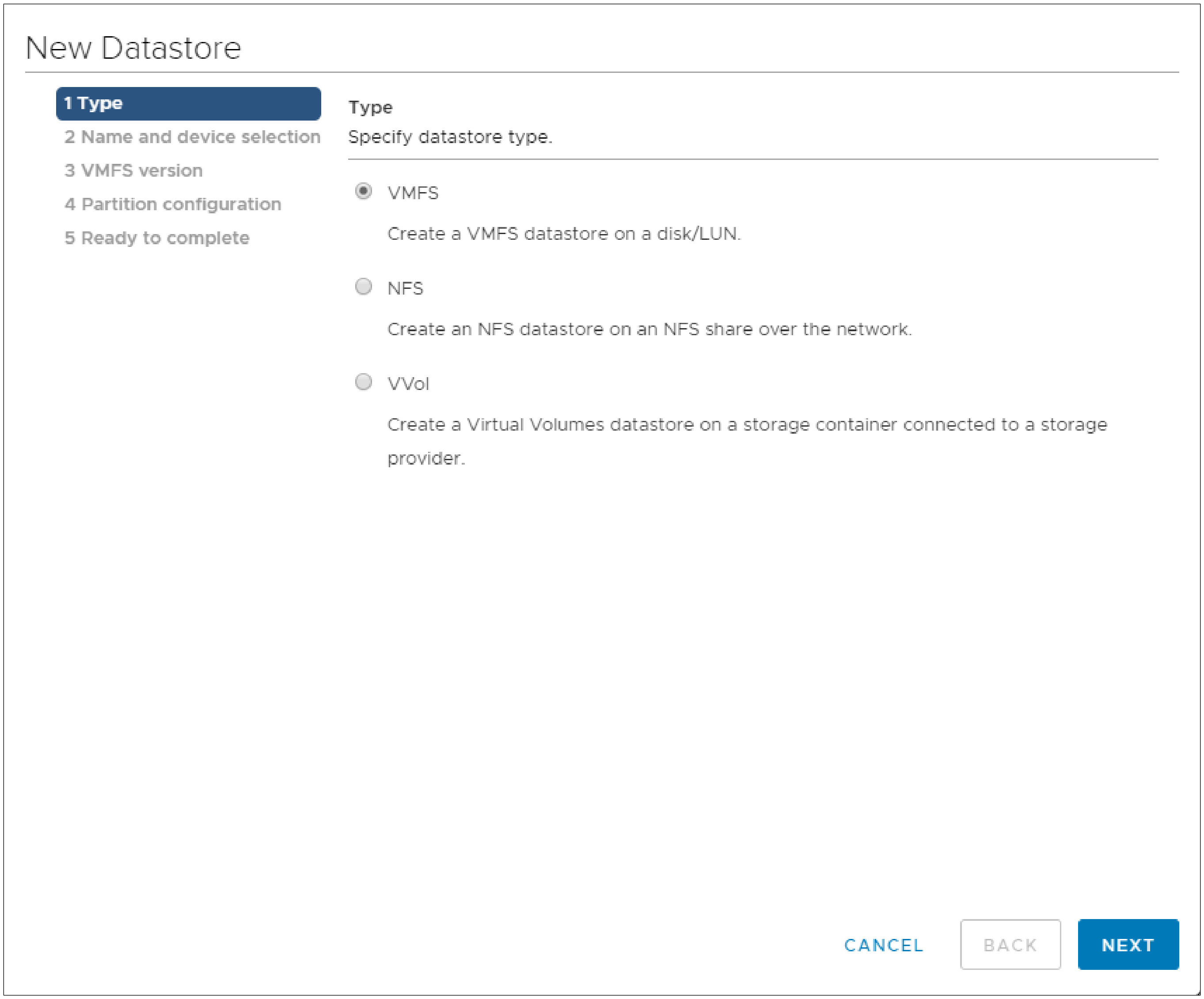
To dig a little deeper though. How did we get here? How do we see the original device? To do that we have to go back to the host configuration. There we look at two main things. Storage Adapters and Storage Devices



Storage Devices

| Name | L... | Type | Capacity | Datasto... | Operational ... | Hardware Accelera... |
|---|---|---|---|---|---|---|
| SYNOLOGY ISCSI Disk (naa.6001405063e3d6f... | 1 | disk | 12.21 TB | Syno... | Attached | Unknown |
| QNAP ISCSI Disk (naa.6e843b68d00bc59deaf... | 1 | disk | 1.70 TB | QNA... | Attached | Supported |
| Local DP Enclosure Svc Dev (t10.DP______BA... | 0 | enclos... |  | Not Cons... | Attached | Not supported |
| Local TSSTcorp CD-ROM (mpx.vmhba0:C0:T4:L... | 0 | cdrom |  | Not Cons... | Attached | Not supported |
| Local DELL Disk (naa.6d4ae52091ddb900212f... | 0 | disk | 16.37 TB | r320... | Attached | Not supported |
| QNAP ISCSI Disk (naa.6e843b6d5bebad5dac8... | 0 | disk | 20.00 TB | QNA... | Attached | Supported |

This will show us what our host is able to get to. If we don't have access to something we may need to either add it if it's ISCSI or NFS or Protocol Endpoint if its a vVOL. Once we can see the RAW device or we have finished setting up the share or protocol endpoint, we can right click on a host and select Storage > New Datastore. This pops up a wizard that looks like this



New Datastore

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.

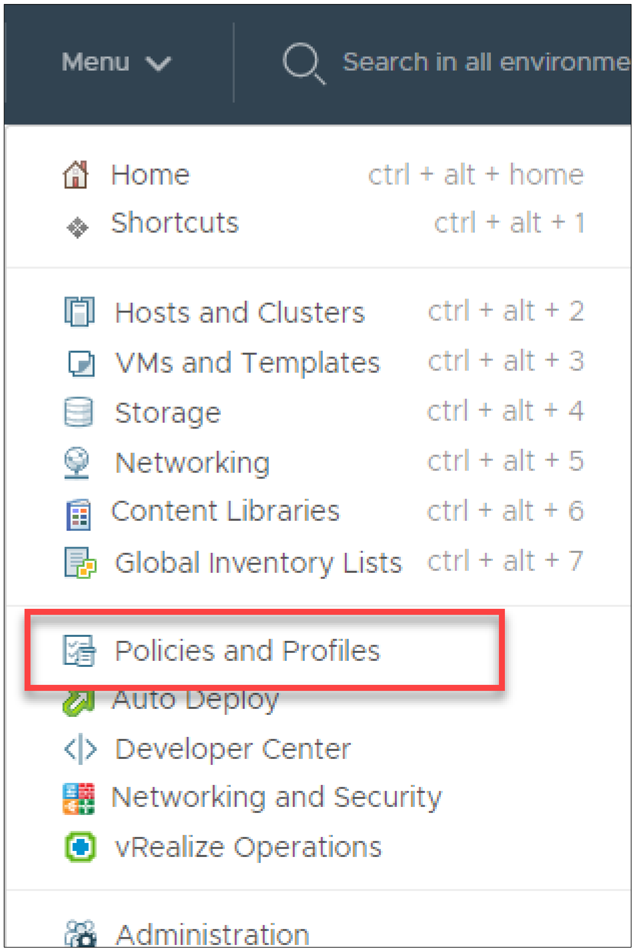
○ VVol

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

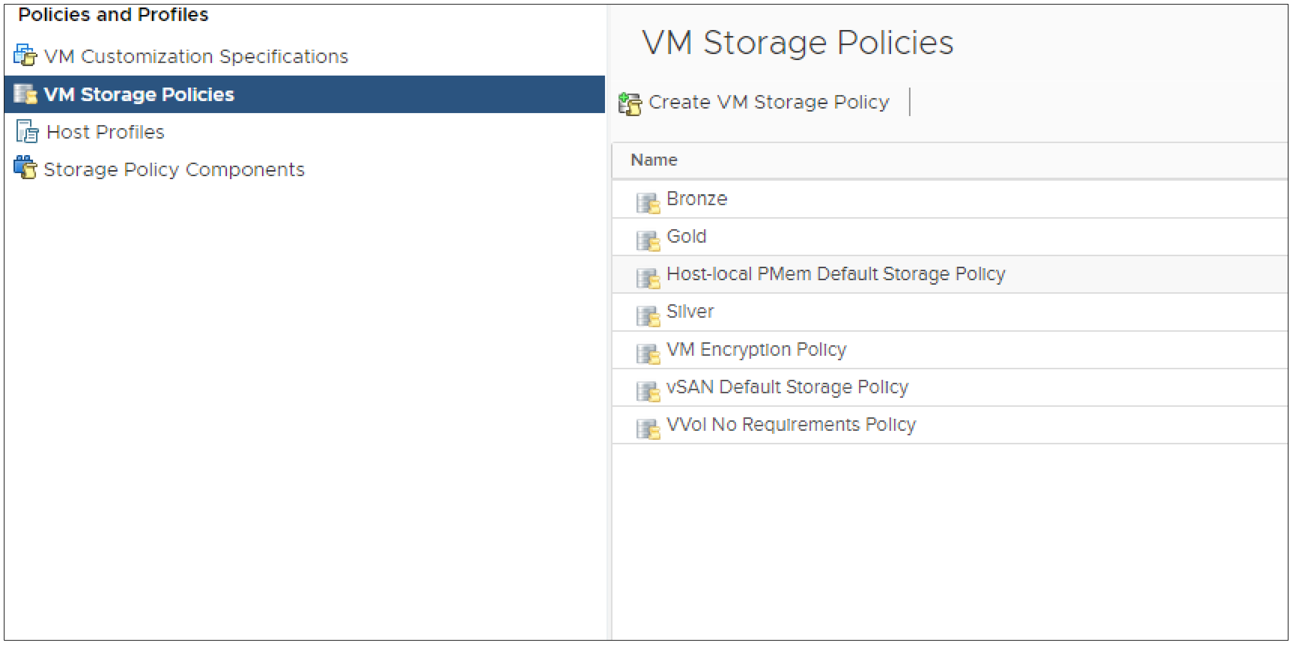
The next screen will allow us to give the datastore a name and what device we want to use for it. Then we choose a VMFS version. We would choose 5 if we still had older hosts running older vSphere. We would choose 6 if we had all 6.5 or 6.7. Why would you want to use it? Look here for a nice table. You can then partition it if desired and finish.

## *Objective 7.3 – Configure a storage policy*

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

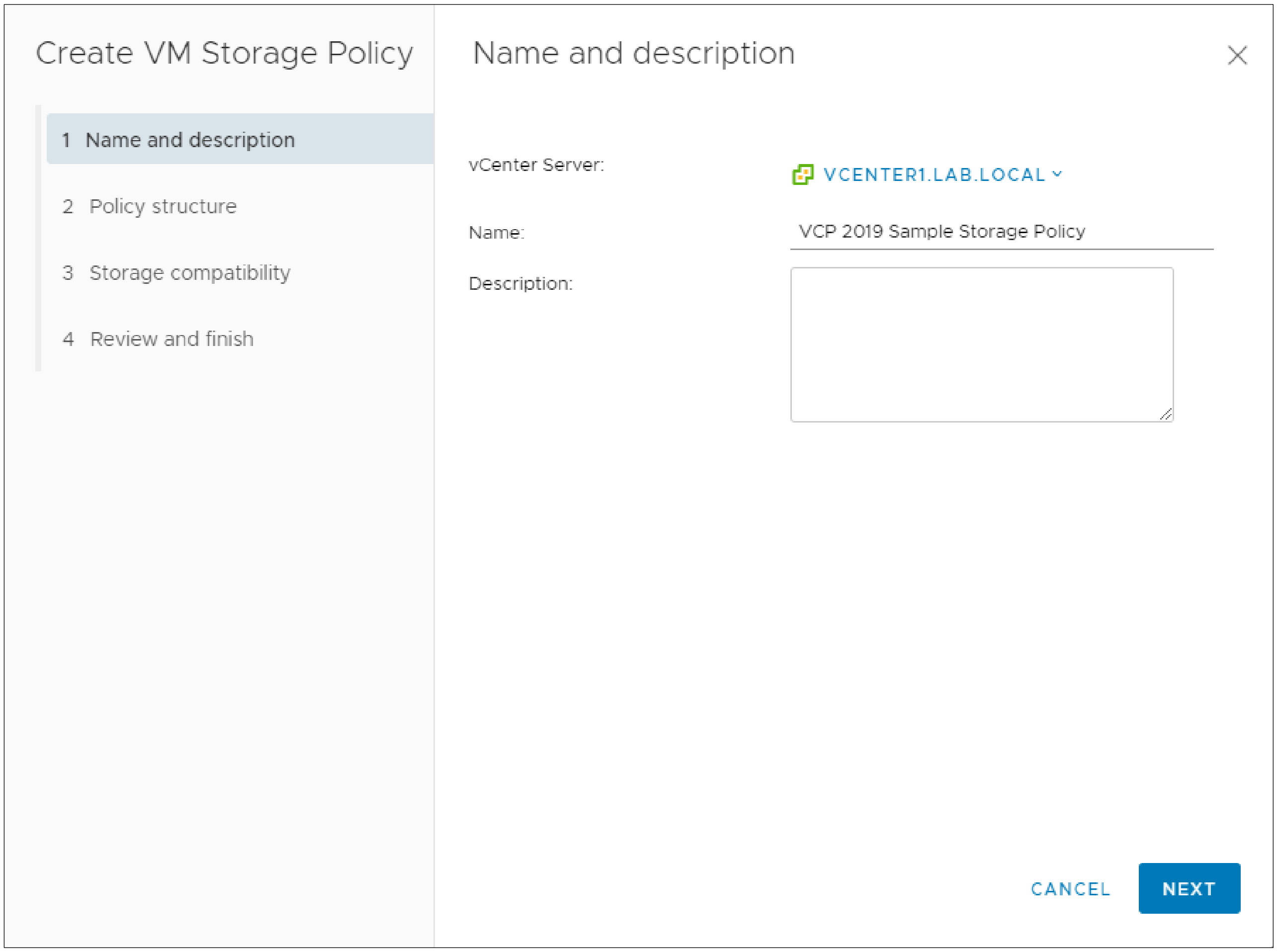


2. Click on VM Storage Policies



| 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.



Create VM Storage Policy

Name and description

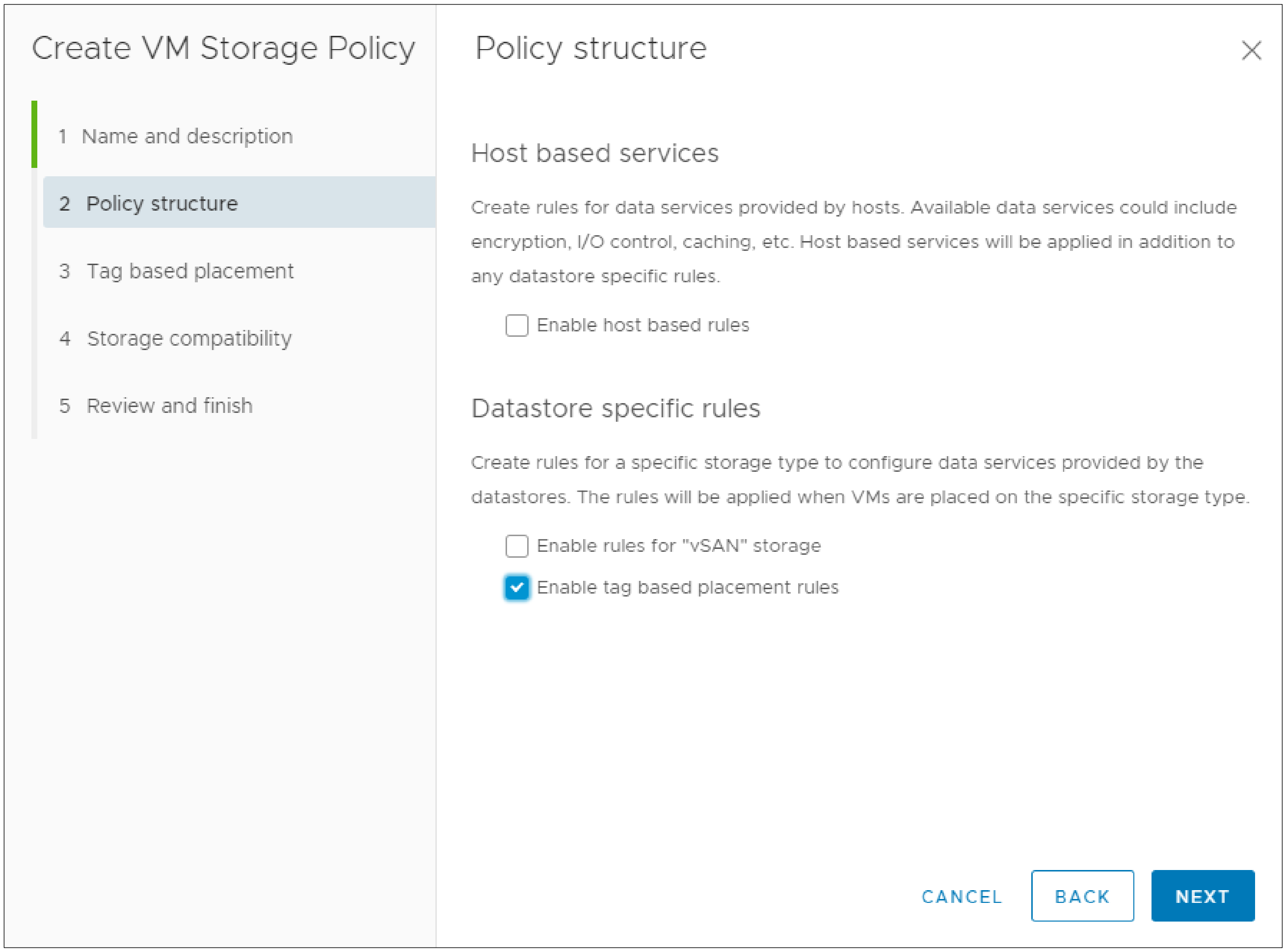
vCenter Server: VCENTER1.LAB.LOCAL

Name: VCP 2019 Sample Storage Policy

Description:

4. This screen allows you to choose between Host Based Services or Datastore Specific rules. Host based are specific services that 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. Such as I tag a specific datastore as "Gold" storage and I create a Storage policy that requires a VM to use "Gold" storage. I am going to use the tag-based placement

option.



Create VM Storage Policy

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

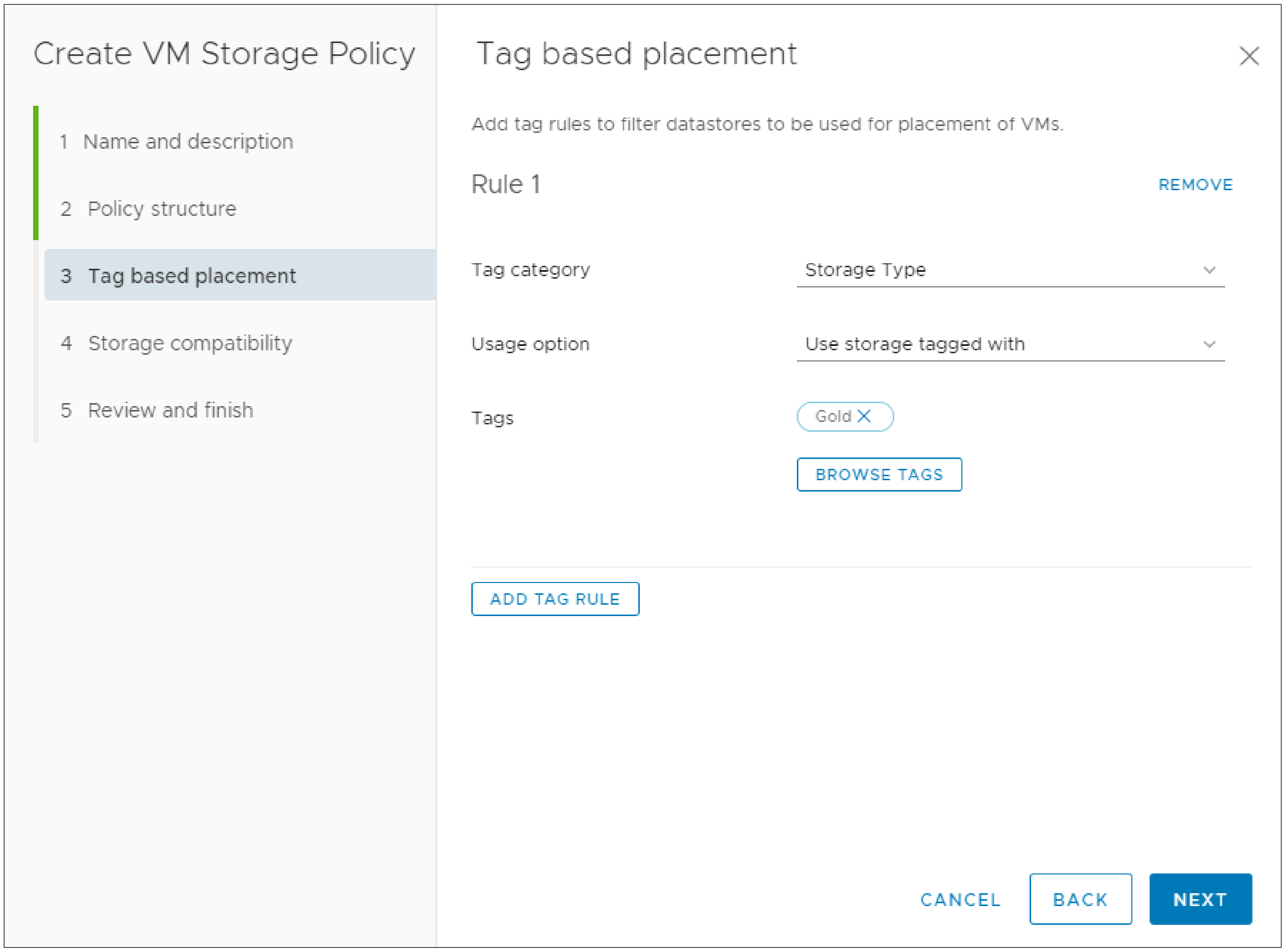
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

□ Enable rules for "vSAN" storage

☑ Enable tag based placement rules

5. I have already created a Tag category called Storage Type and I am going to tell it to Use storage tagged with the “Gold” tag. I could tell it to not 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.

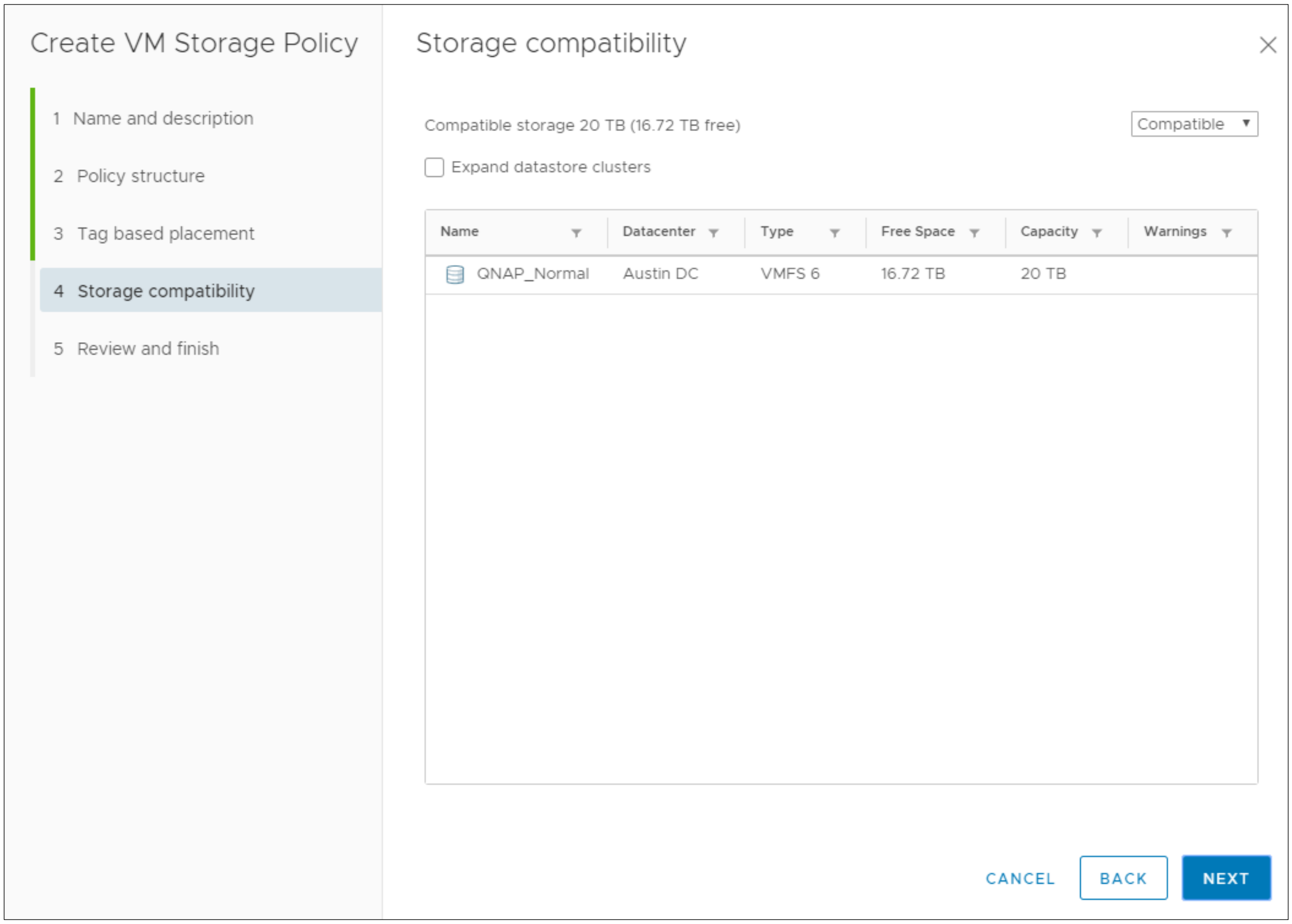
Rule 1

Tag category: Storage Type

Usage option: Use storage tagged with

Tags: Gold

6. I have one Datastore tagged as “Gold” Storage.



Create VM Storage Policy

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

Storage compatibility

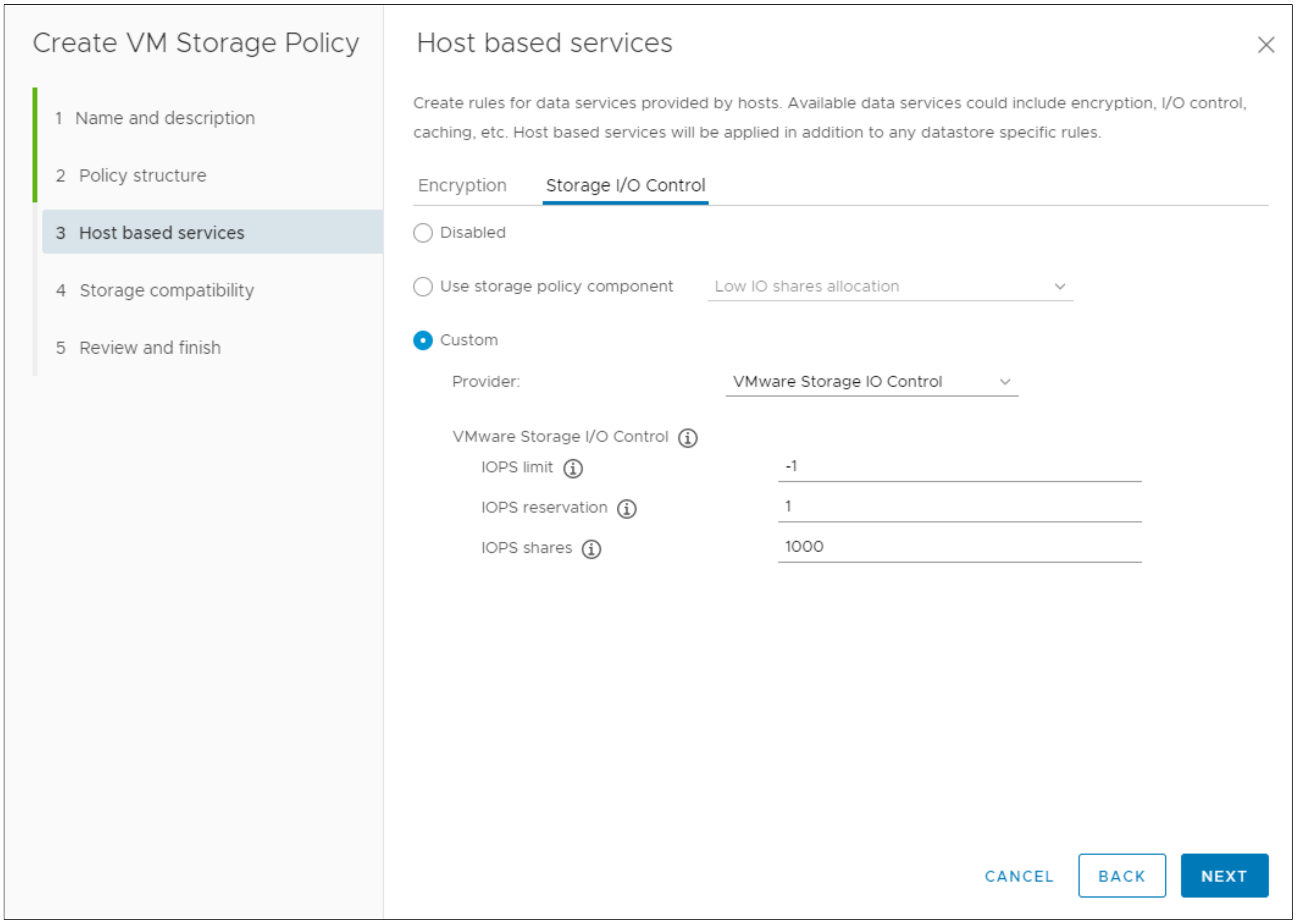
Compatible storage 20 TB (16.72 TB free)

Compatible ▾

□ Expand datastore clusters

| Name | Datacenter | Type | Free Space | Capacity | Warnings |
|---|---|---|---|---|---|
| QNAP_Normal | Austin DC | VMFS 6 | 16.72 TB | 20 TB | |

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



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.

○ Disabled

○ Use storage policy component: Low IO shares allocation

● Custom

Provider: VMware Storage IO Control

VMware Storage I/O Control

IOPS limit: -1

IOPS reservation: 1

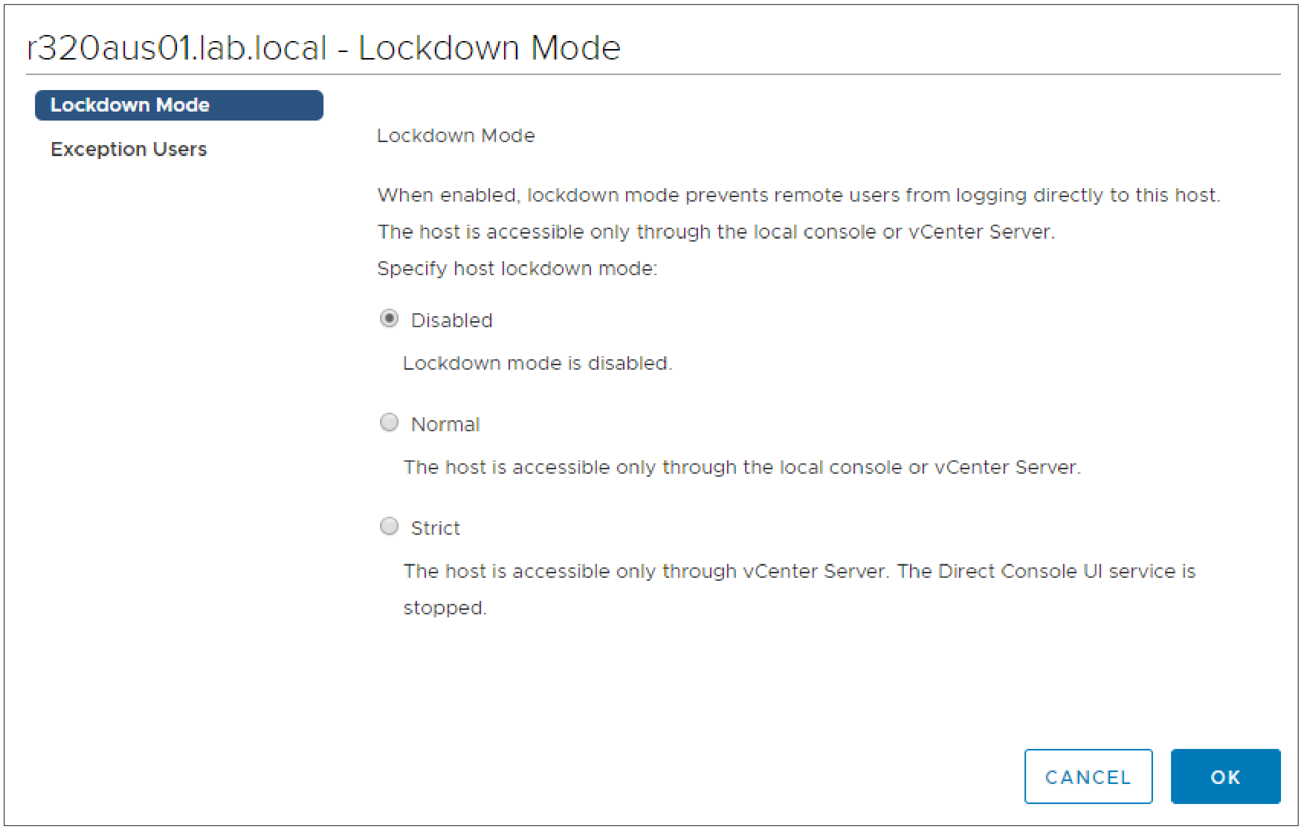
IOPS shares: 1000

## *Objective 7.4 – Configure host security*

There are several built-in features that can secure a host. Let's go over them

- Lockdown Mode – When enabled this prevents users from logging directly into the host. It will only be accessible through the local console if you are on an accepted user list or vCenter. You can also turn off the Direct Console UI completely. This can be found under

Configure > Security Profile



r320aus01.lab.local - Lockdown Mode

Lockdown Mode

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

Specify host lockdown mode:

● Disabled

Lockdown mode is disabled.

○ Normal

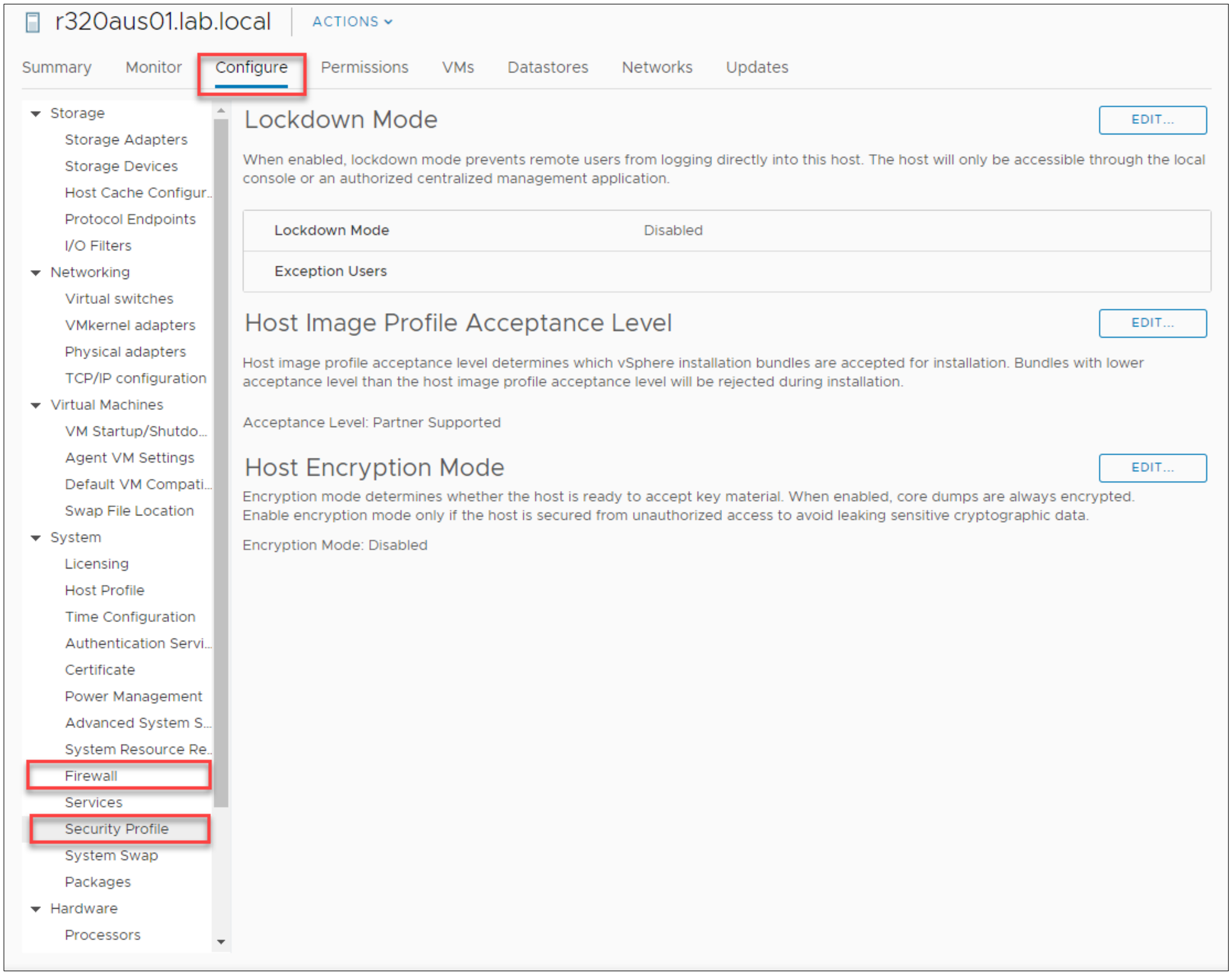
The host is accessible only through the local console or vCenter Server.

○ Strict

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

- Host Image Profile Acceptance Level – This is like driver signing on a Microsoft Windows machine. This will only allow bundles or drivers with an acceptance level you set.
- Host Encryption Mode – This setting encrypts any core dumps from the host.

- Firewall – There is a stateless firewall included in ESXi. Most ports are locked by default. If you want to add a new port not already in the list you will need to do it at command line.



Lockdown Mode

When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through the local console or an authorized centralized management application.

| | |
|---|---|
| Lockdown Mode | Disabled |
| Exception Users | |

Host Image Profile Acceptance Level

Host image profile acceptance level determines which vSphere installation bundles are accepted for installation. Bundles with lower acceptance level than the host image profile acceptance level will be rejected during installation.

Acceptance Level: Partner Supported

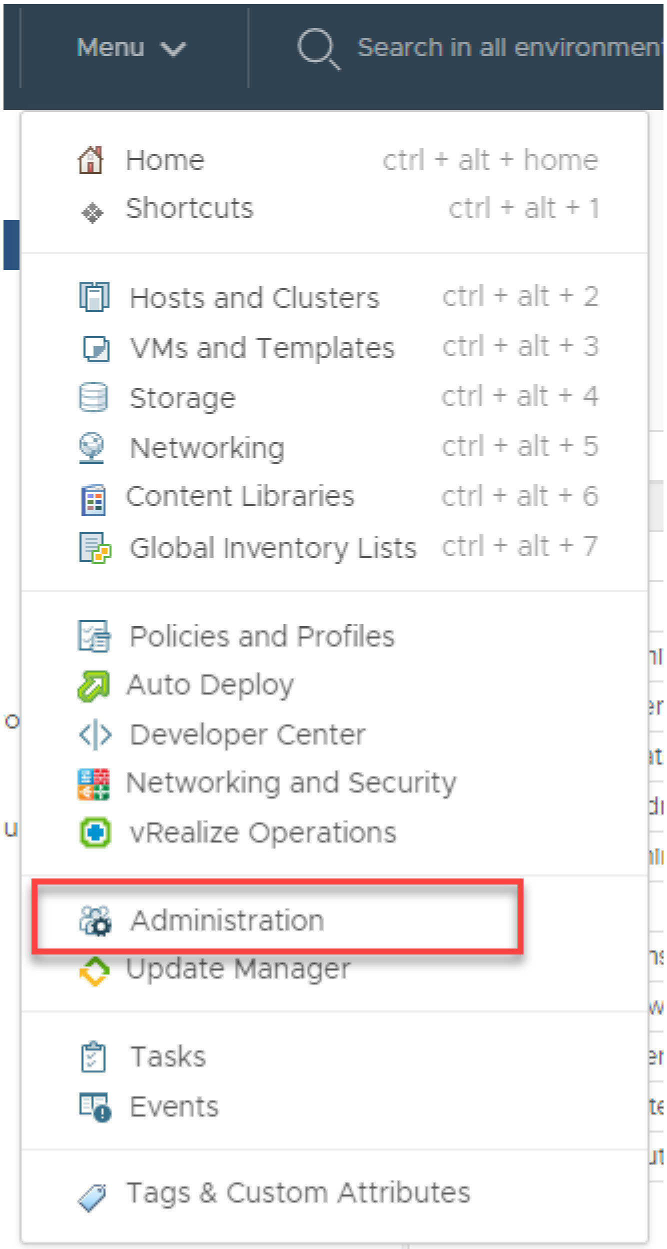
Host Encryption Mode

Encryption mode determines whether the host is ready to accept key material. When enabled, core dumps are always encrypted. Enable encryption mode only if the host is secured from unauthorized access to avoid leaking sensitive cryptographic data.

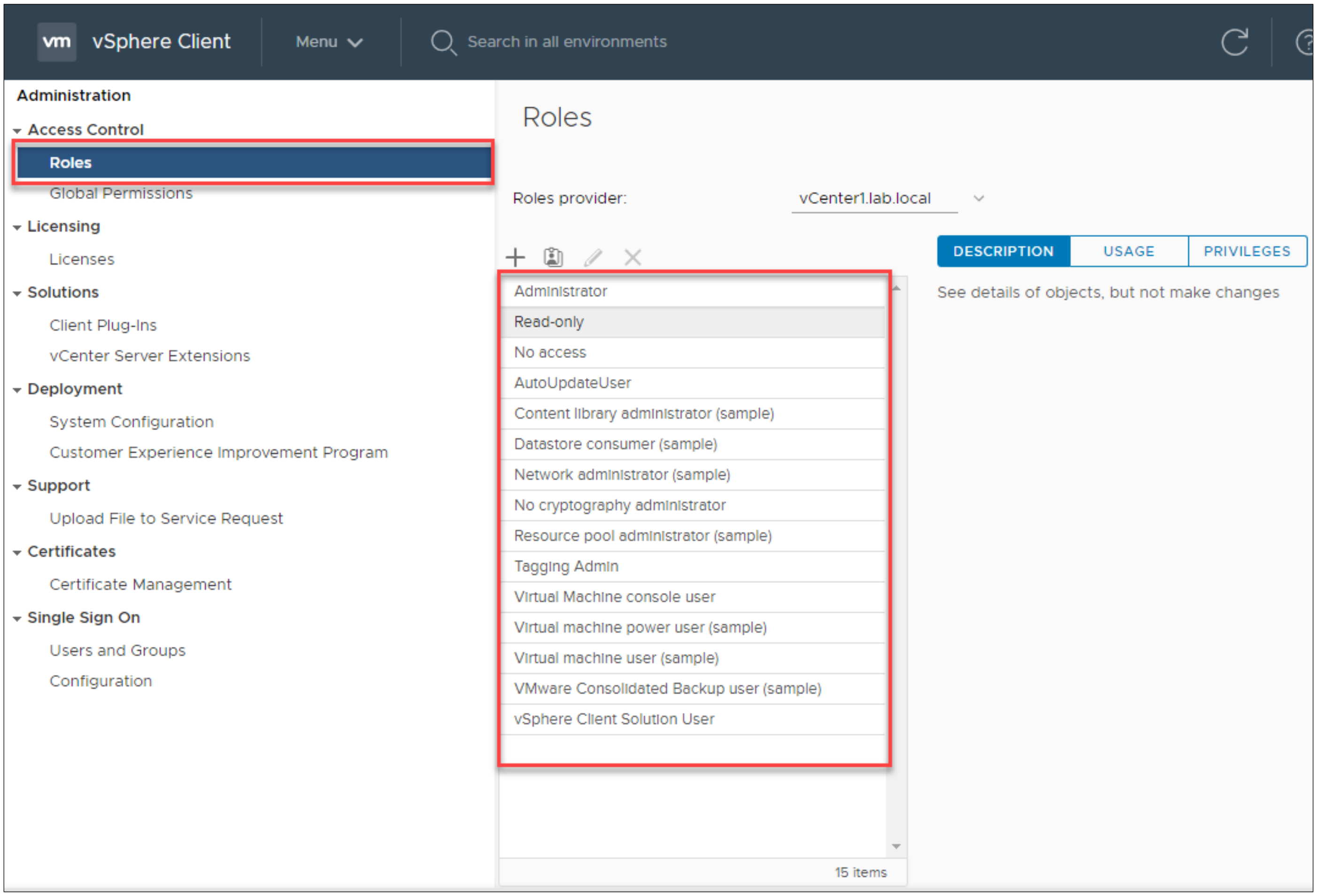
Encryption Mode: Disabled

## *Objective 7.5 – Configure role-based user management*

Role-based management allows you to assign a set of permissions to a user or group. This is great as this makes it easier to assign just the permissions you need to a user and no more. This is great for security. VMware provides a number of Roles pre-configured. These can't be changed. What you can do, is clone them and change the clones. You can also create your own custom role. In order to do this, you click on the Menu and go to Administration



You can see the predefined roles when you select Roles under Access Control



Roles

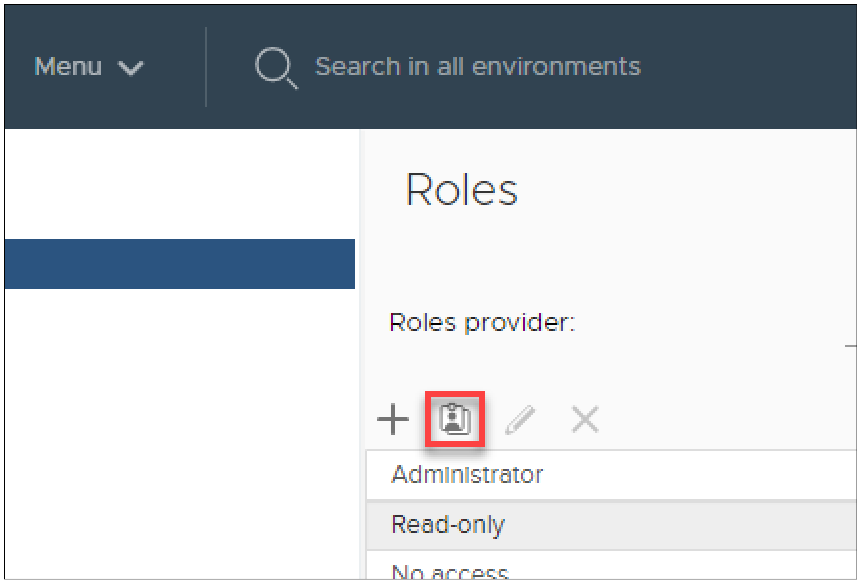
Roles provider: vCenter1.lab.local

- Administrator
- Read-only
- No access
- AutoUpdateUser
- Content library administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- No cryptography administrator
- Resource pool administrator (sample)
- Tagging Admin
- Virtual Machine console user
- Virtual machine power user (sample)
- Virtual machine user (sample)
- VMware Consolidated Backup user (sample)
- vSphere Client Solution User

15 items

See details of objects, but not make changes

To clone you select one and then click the Clone icon

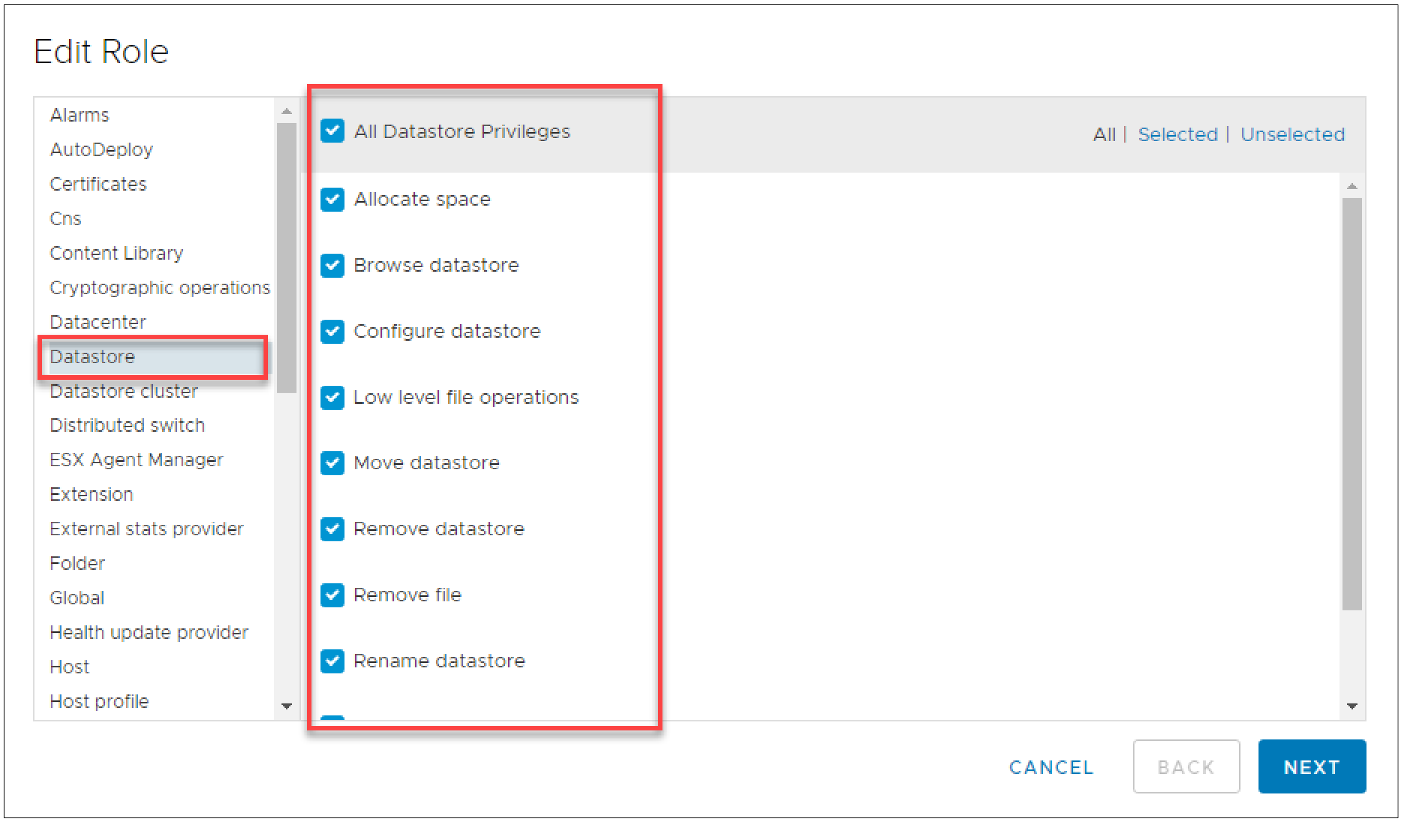


Roles

Roles provider:

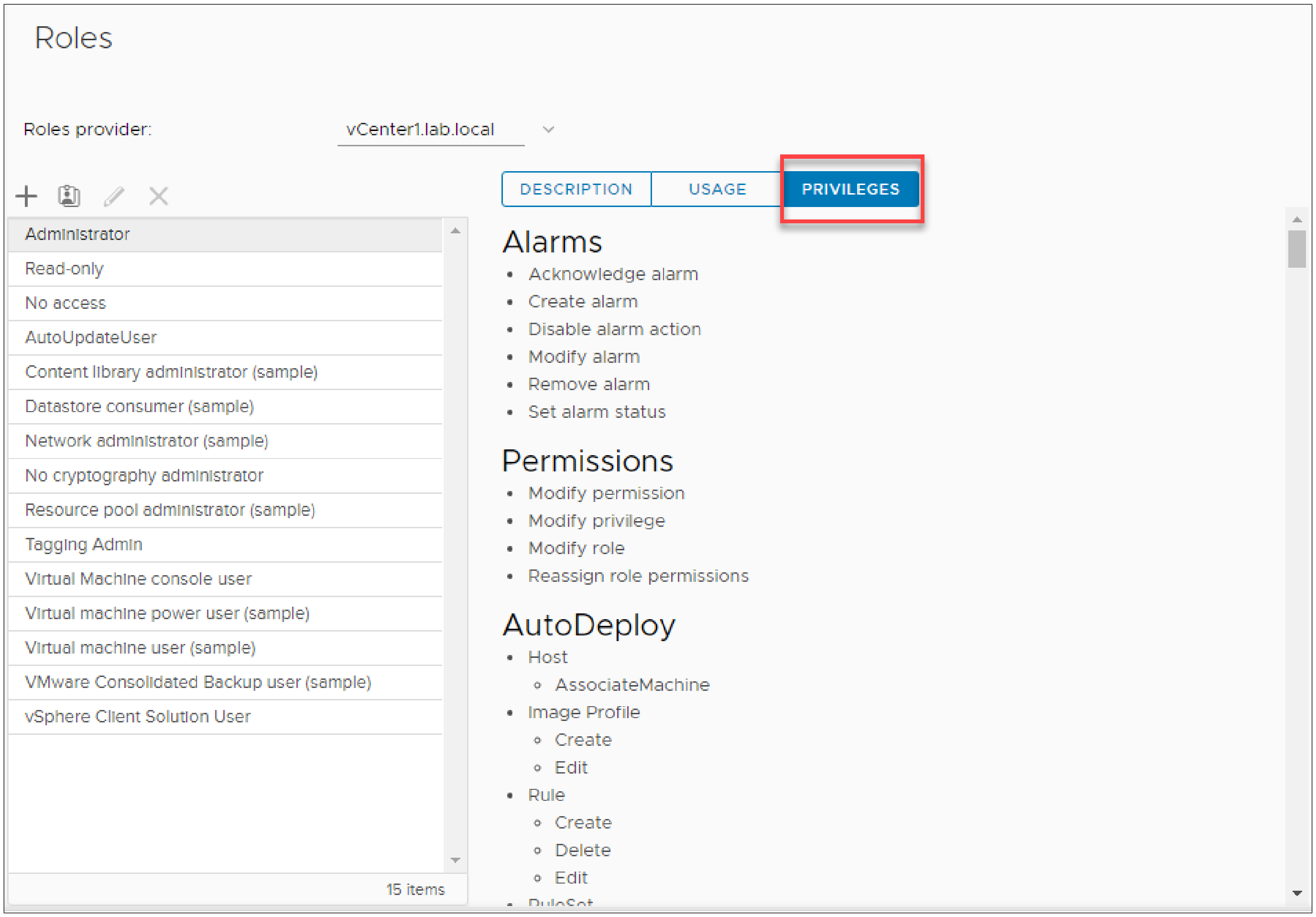
- Administrator
- Read-only
- No access

You need to name it and click ok on the window the pops up. To edit the clone you just made, click on the Pencil icon after selecting the new role. Then select the privileges you want to allow or disallow by clicking on the check boxes.


Edit Role

☑ All Datastore Privileges
☑ Allocate space
☑ Browse datastore
☑ Configure datastore
☑ Low level file operations
☑ Move datastore
☑ Remove datastore
☑ Remove file
☑ Rename datastore

You can see the privileges already assigned to a role by clicking on the Privileges button on the side.



Roles provider: vCenter1.lab.local

- Administrator
- Read-only
- No access
- AutoUpdateUser
- Content library administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- No cryptography administrator
- Resource pool administrator (sample)
- Tagging Admin
- Virtual Machine console user
- Virtual machine power user (sample)
- Virtual machine user (sample)
- VMware Consolidated Backup user (sample)
- vSphere Client Solution User

15 items

Alarms

- Acknowledge alarm
- Create alarm
- Disable alarm action
- Modify alarm
- Remove alarm
- Set alarm status

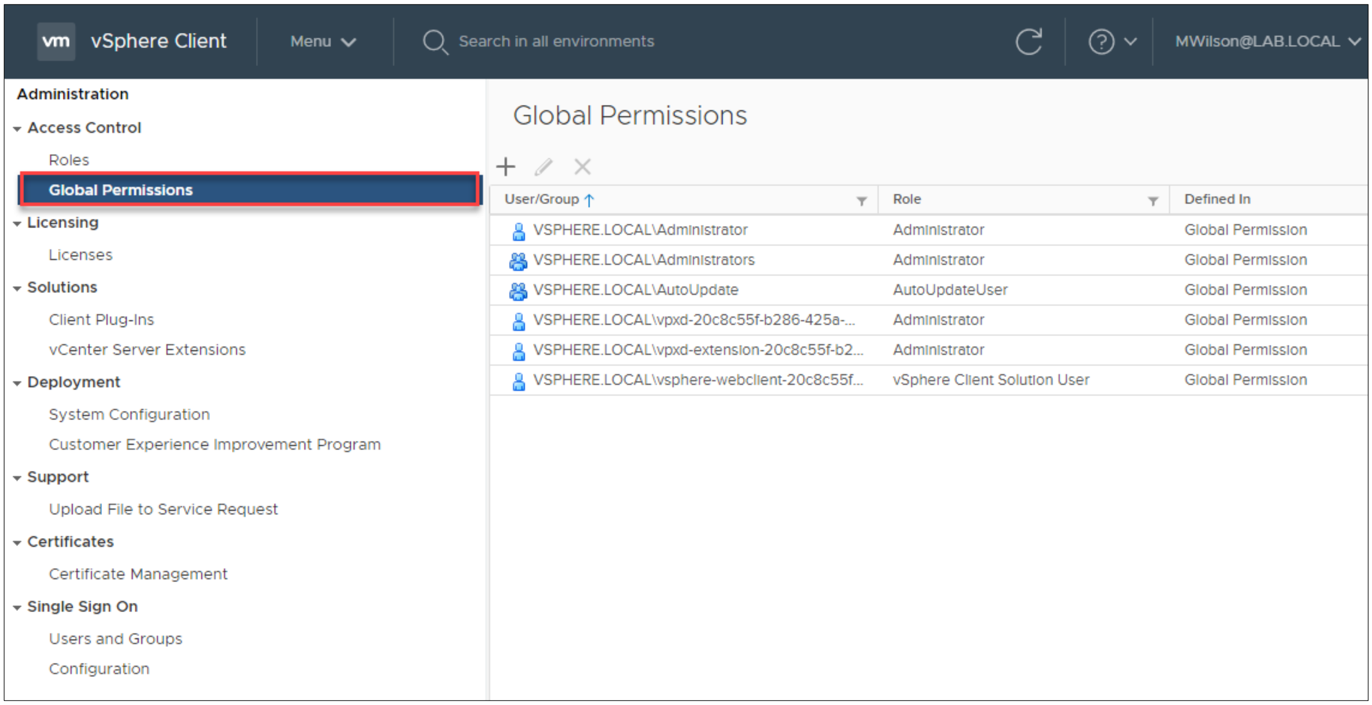
Permissions

- Modify permission
- Modify privilege
- Modify role
- Reassign role permissions

AutoDeploy

- Host
  - AssociateMachine
- Image Profile
  - Create
  - Edit
- Rule
  - Create
  - Delete
  - Edit
- RuleSet

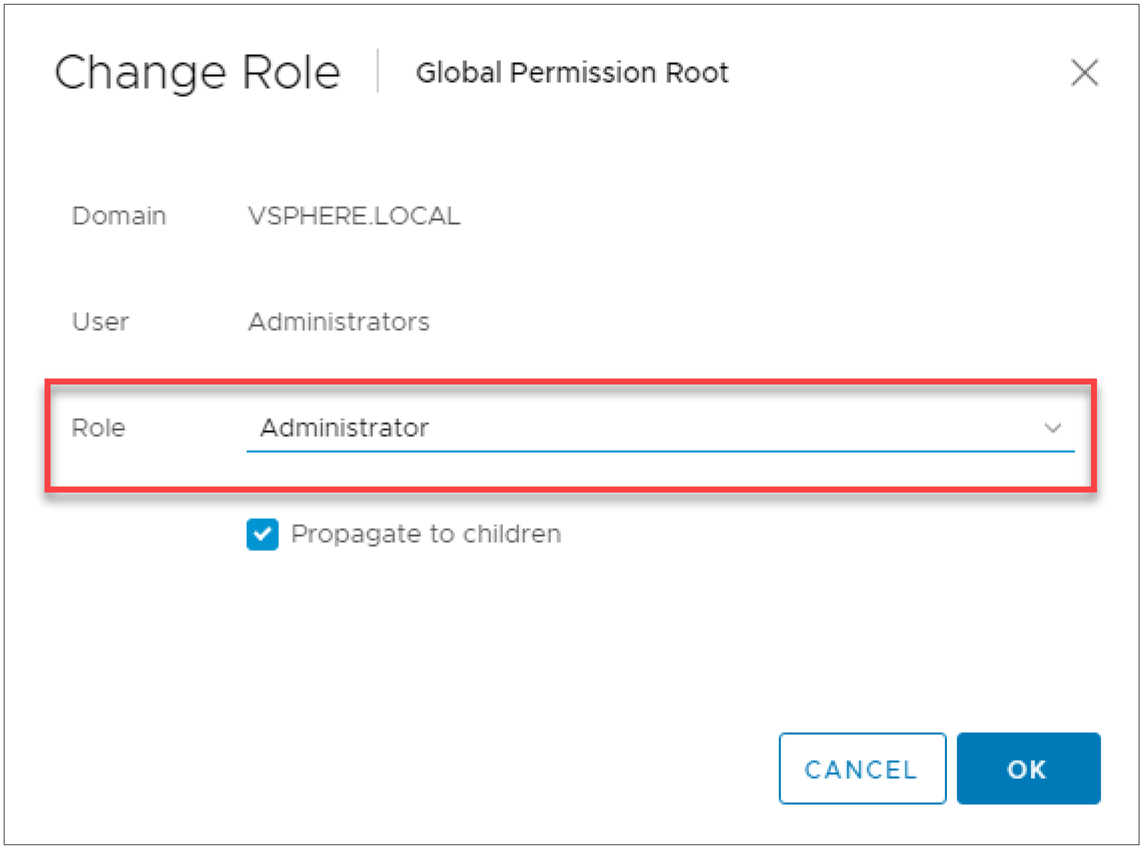
You then assign the roles under the Global Permissions item. You can use one of the built-in user or groups or you can add a new user/group. You can add the group from any of the Identity sources you have setup already.



Global Permissions

| User/Group | Role | Defined In |
|---|---|---|
| VSPHERE.LOCAL\Administrator | Administrator | Global Permission |
| VSPHERE.LOCAL\Administrators | Administrator | Global Permission |
| VSPHERE.LOCAL\AutoUpdate | AutoUpdateUser | Global Permission |
| VSPHERE.LOCAL\vpxd-20c8c55f-b286-425a-... | Administrator | Global Permission |
| VSPHERE.LOCAL\vpxd-extension-20c8c55f-b2... | Administrator | Global Permission |
| VSPHERE.LOCAL\vsphere-webclient-20c8c55f... | vSphere Client Solution User | Global Permission |

When you add or edit the permissions you set the role.



Change Role | Global Permission Root

Domain VSPHERE.LOCAL

User Administrators

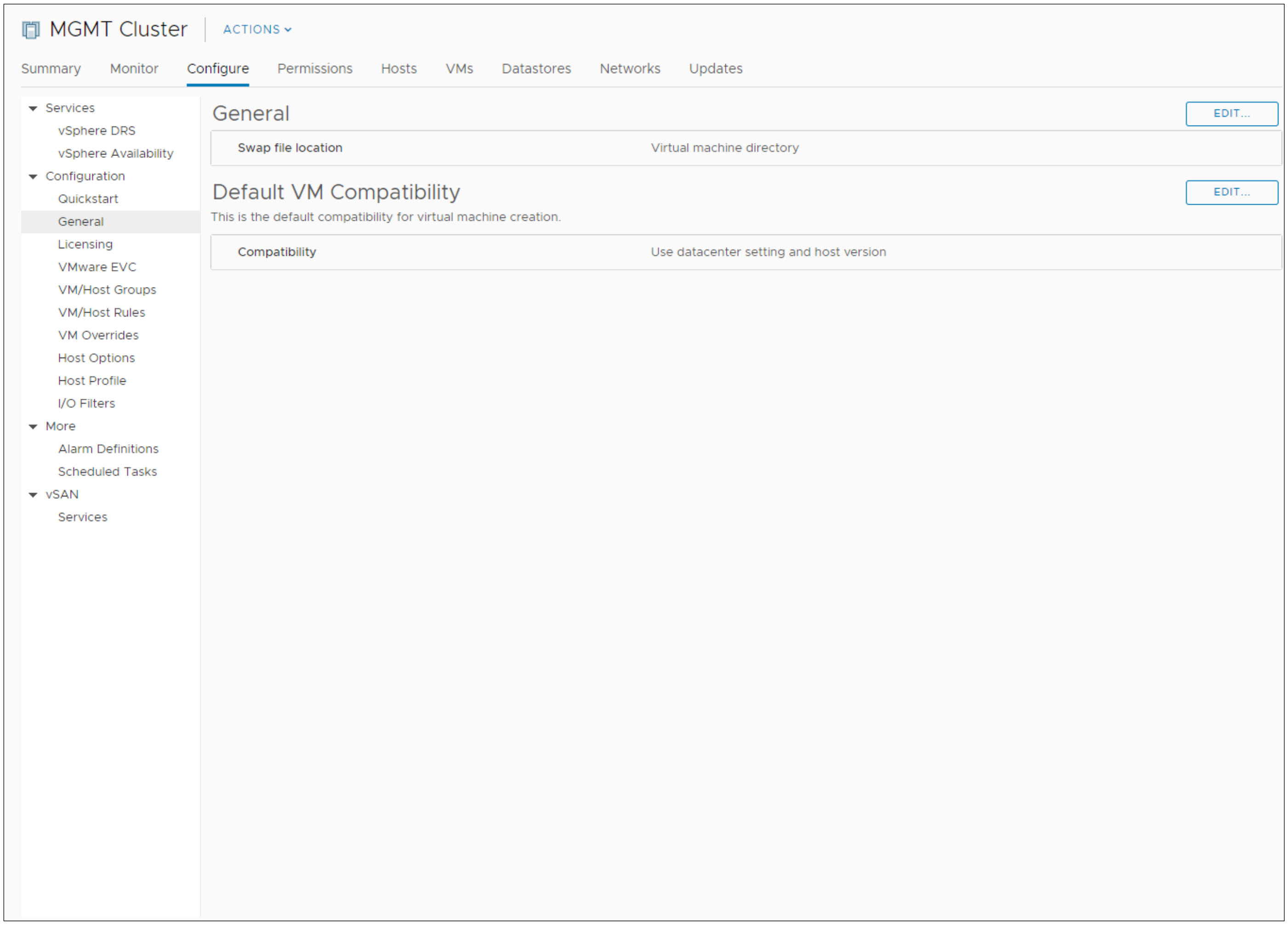
Role Administrator

☑ Propagate to children

There is a special role called No Access as well that you can assign to a user to keep them from accessing specific objects or privileges.

## *Objective 7.6 – Configure and use vSphere Compute and Storage cluster options*

After you create a cluster, you can right click on it and select settings, or click on the configure tab in the center, object pane



General

Swap file location: Virtual machine directory

Default VM Compatibility

This is the default compatibility for virtual machine creation.

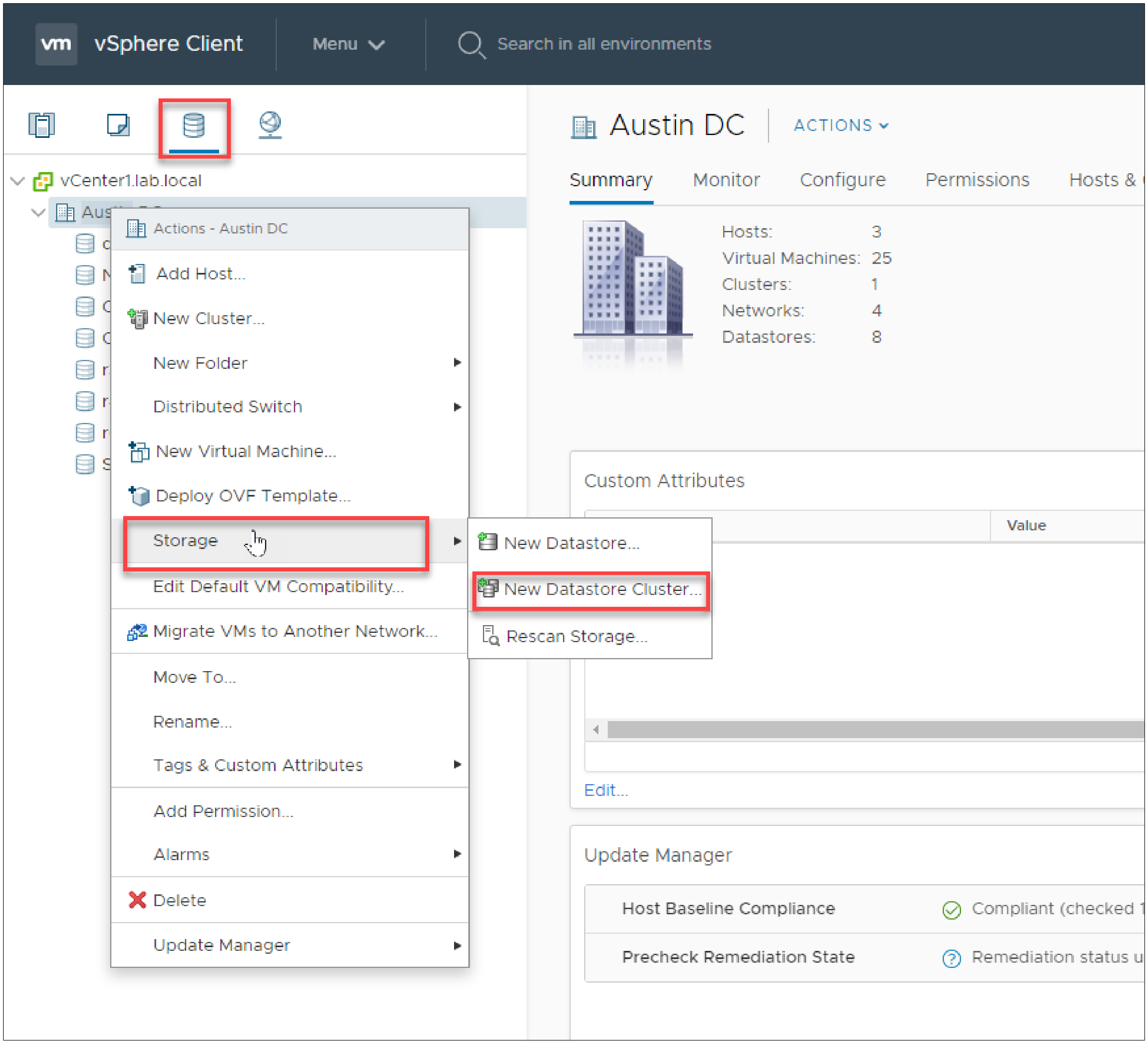
Compatibility: Use datacenter setting and host version

Quickly going through the options available. There is DRS and HA we've already gone over. We then have:

- QuickStart - is a wizard to help you configure your cluster.
- General – lets you change the swap file location for your VMs. This will be the default setting for the cluster. Default VM compatibility is the default VM Hardware version for the cluster.
- Licensing – This is only used if you vSAN

- VMware EVC – This was mentioned previously as well. Enhanced vMotion Compatibility. This allows you to use disparate versions of processors and vMotion between them.
- VM/Host Groups – This is the VM Groups and Host groups you can setup to create Affinity or Anti-Affinity rules
- VM Host Rules – These are the Affinity or Anti-Affinity rules.
- VM Overrides – This allows you to override cluster settings for DRS/HA restart or response for individual VMs.
- Host Options – Allows for host power management. You enter in your IPMI settings per Server
- Host Profile – This will be gone over in a few objectives, but creates a settings template for all hosts in the cluster.
- I/O filters – You can install I/O filters here (VAIO) This can be a plugin such as backup or disaster recovery filters.
- Alarm Definitions – This is where you can add/enable/disable/delete alarms for your cluster (applies to objects in the cluster)
- Scheduled Tasks – You can schedule certain tasks for off hours. New Virtual Machine, Add Host, or Edit DRS.
- vSAN – This won’t say much here unless it’s turned on.

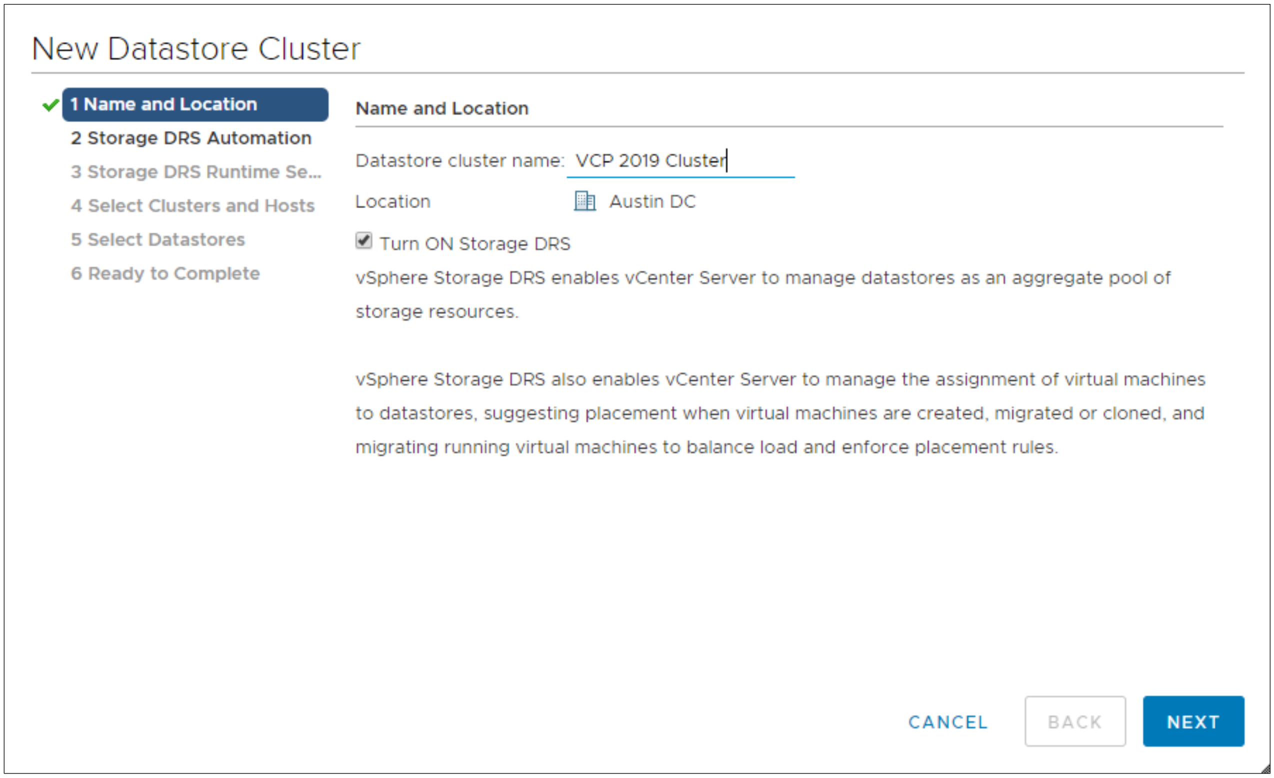
A Datastore Cluster or Storage Cluster (unless referring to VSAN cluster) is created by right-clicking on the datacenter in the Storage heading on the object pane.



Hosts: 3
Virtual Machines: 25
Clusters: 1
Networks: 4
Datastores: 8

| | |
|---|---|
| Host Baseline Compliance | Compliant (checked 1 |
| Precheck Remediation State | Remediation status u |

1. This launches a wizard to go through. You will need to enter a Datastore Cluster name and you should turn on Storage DRS



New Datastore Cluster

Name and Location

Datastore cluster name: VCP 2019 Cluster

Location: Austin DC

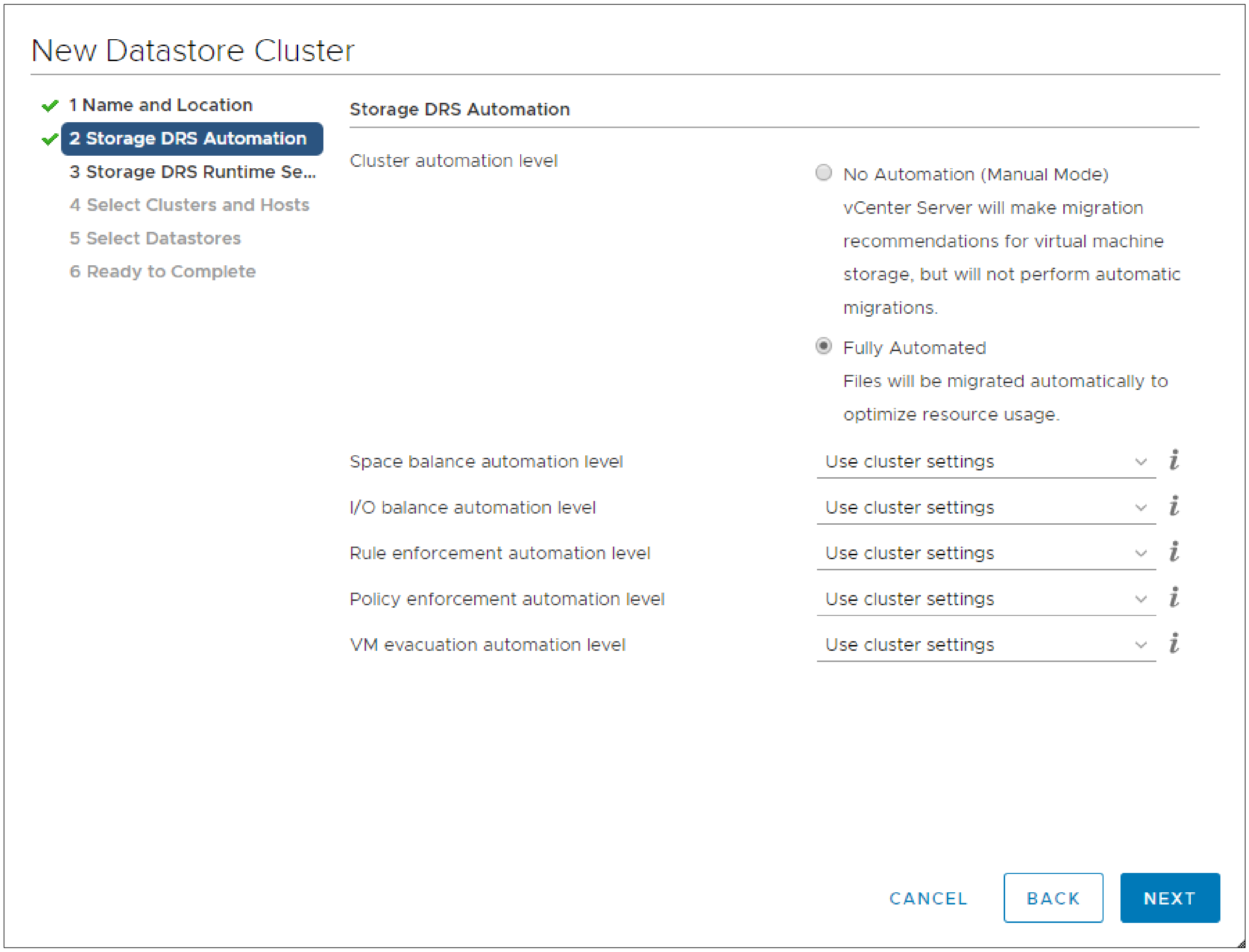
☑ Turn ON Storage DRS

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.

2. You then are presented with more options than anyone should be. The first is what level of automation would you like, but then you have all these other options which I will leave at cluster default. Each one of them will check certain metrics or alarms and move the VM

storage based on what it sees.



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

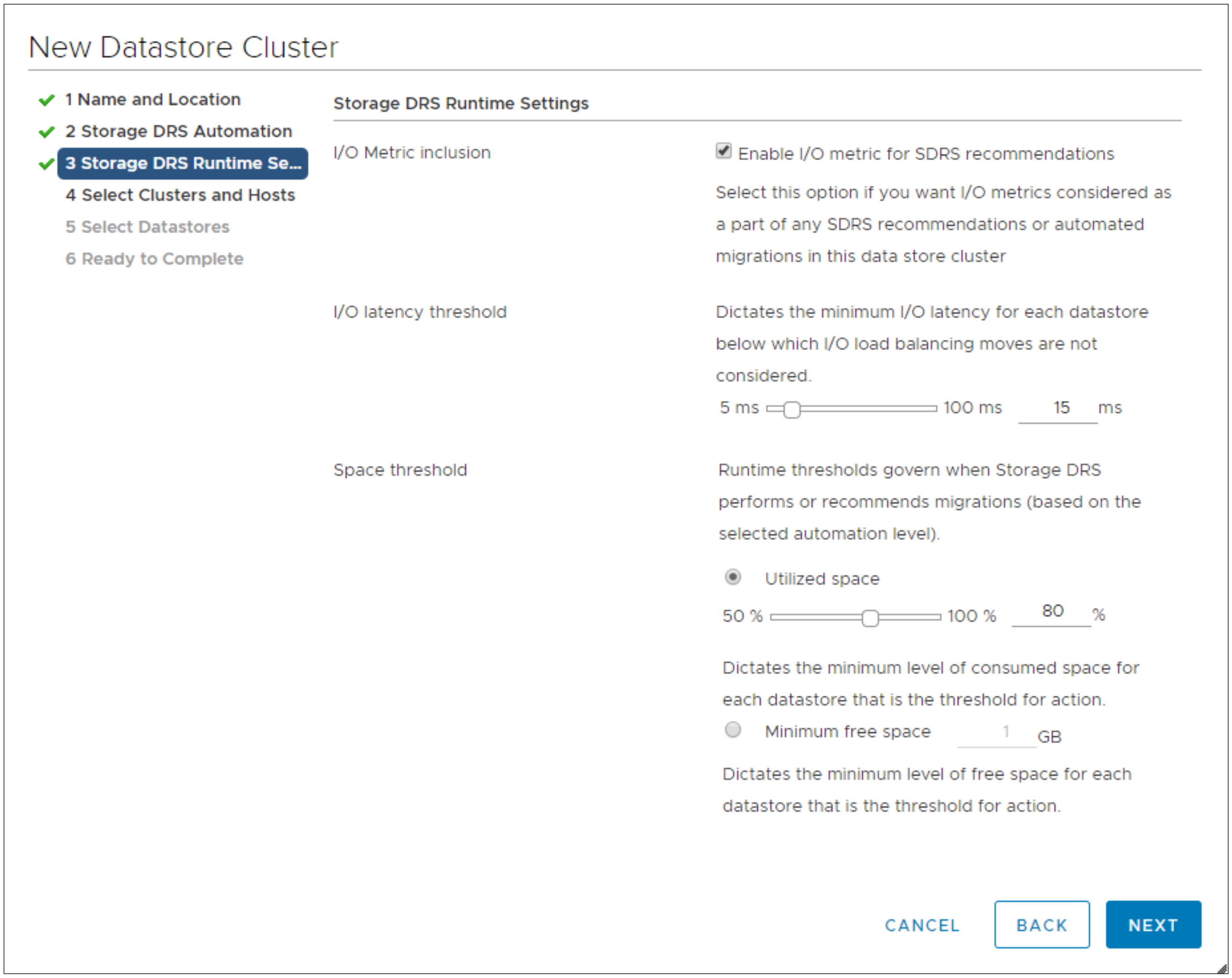
I/O balance automation level: Use cluster settings

Rule enforcement automation level: Use cluster settings

Policy enforcement automation level: Use cluster settings

VM evacuation automation level: Use cluster settings

3. Now you need to decide storage DRS runtime settings. These are thresholds you set before it takes action to move data around. I'm leaving defaults again.



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 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 15 ms

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

● Utilized space

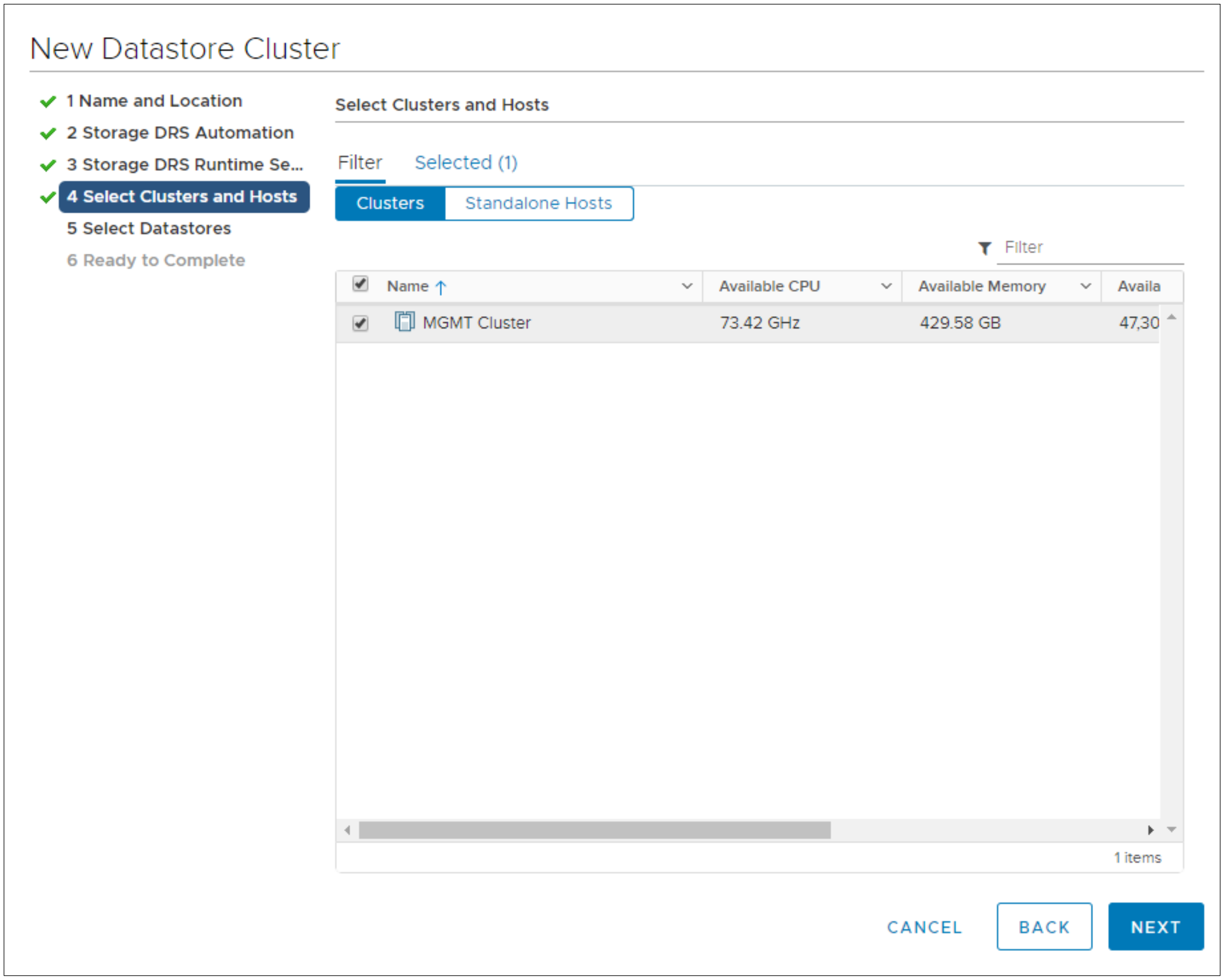
50 % — 100 % 80 %

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

○ Minimum free space 1 GB

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

4. You then select your cluster and / or hosts that will participate in sharing their datastores in this.

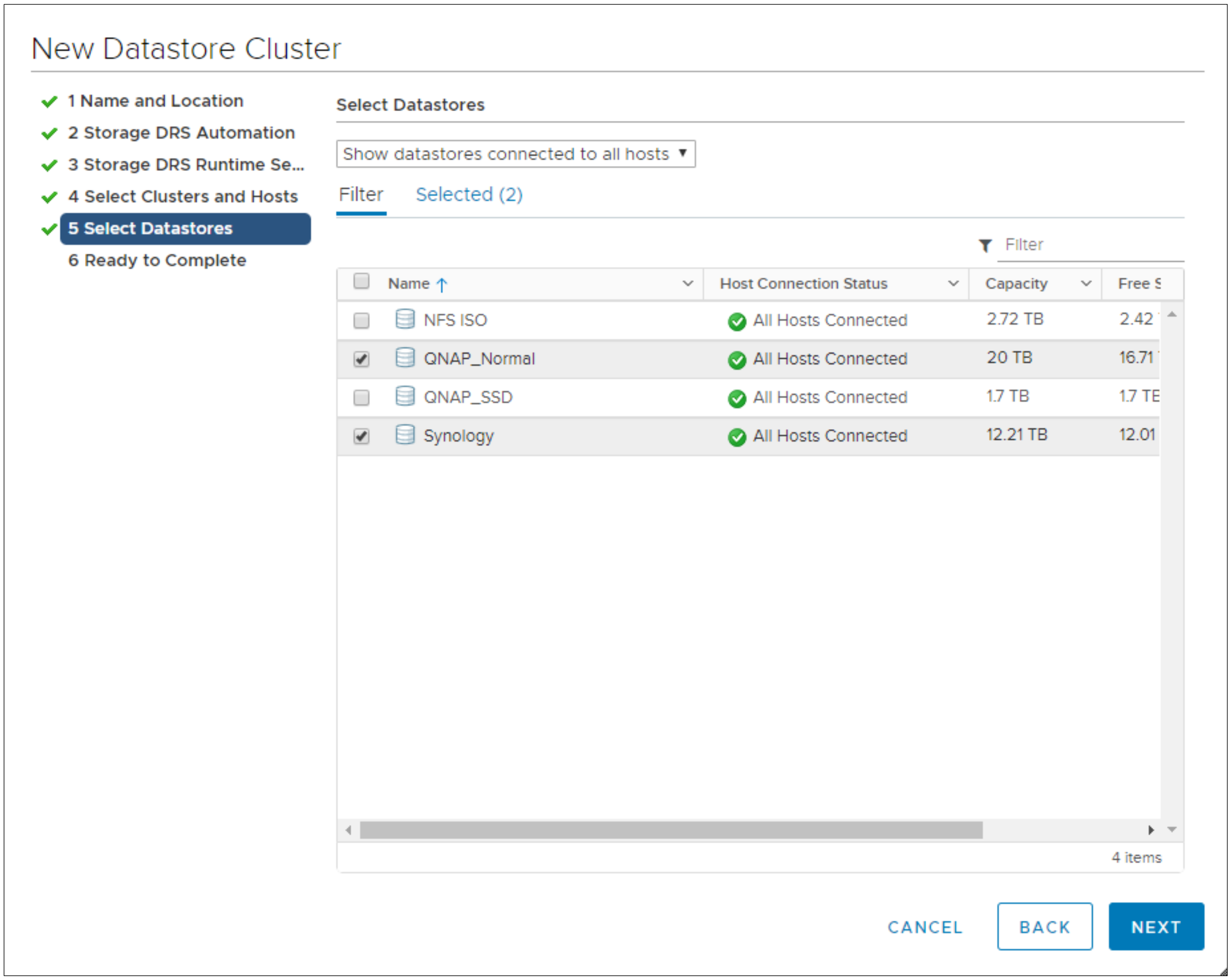


Select Clusters and Hosts

| ☑ | Name ↑ | Available CPU | Available Memory | Availa |
|---|---|---|---|---|
| ☑ | MGMT Cluster | 73.42 GHz | 429.58 GB | 47,30 |

1 items

5. Select the datastores that will make up this Datastore 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 (2)

| □ | Name ↑ | Host Connection Status | Capacity | Free S |
|---|---|---|---|---|
| □ | NFS ISO | ✓ All Hosts Connected | 2.72 TB | 2.42 |
| ☑ | QNAP_Normal | ✓ All Hosts Connected | 20 TB | 16.71 |
| □ | QNAP_SSD | ✓ All Hosts Connected | 1.7 TB | 1.7 TE |
| ☑ | Synology | ✓ All Hosts Connected | 12.21 TB | 12.01 |

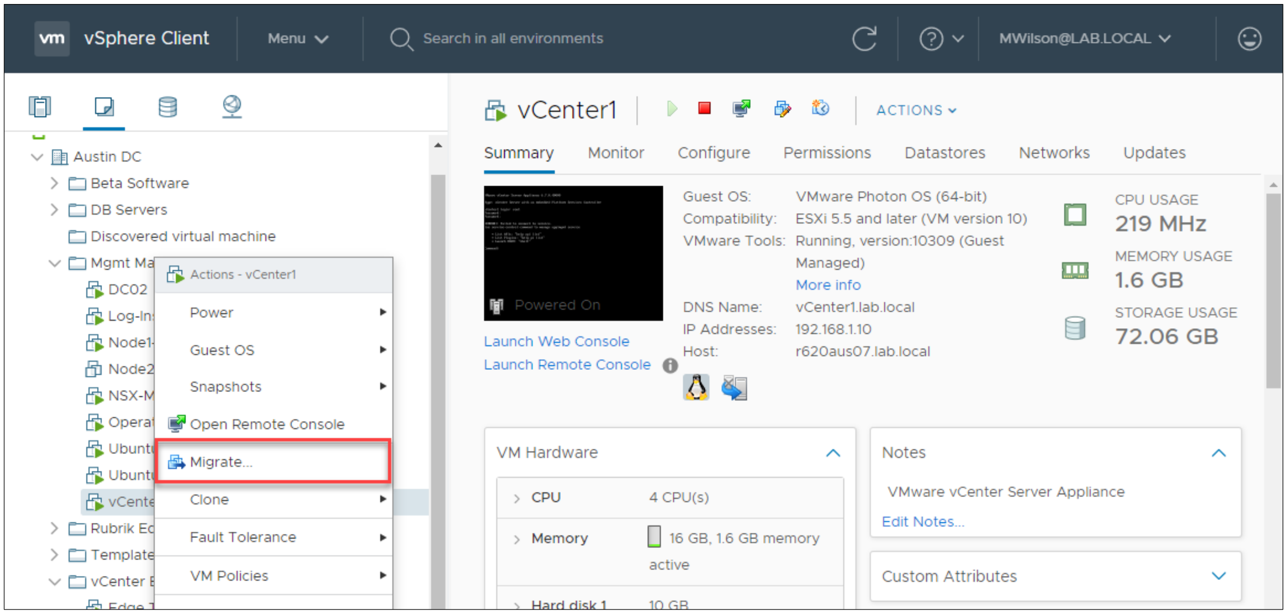
4 items

6. It gives you final summary screen and you click Finish.

## *Objective 7.7 – Perform different types of migrations*

We've already gone over the types of migrations possible. Now let's see how to accomplish them.

1. To migrate a VM, whether you migrate the VM or storage, you need to right click on the VM and choose Migrate.



Guest OS: VMware Photon OS (64-bit)
Compatibility: ESXi 5.5 and later (VM version 10)
VMware Tools: Running, version:10309 (Guest Managed)
DNS Name: vCenter1.lab.local
IP Addresses: 192.168.1.10
Host: r620aus07.lab.local

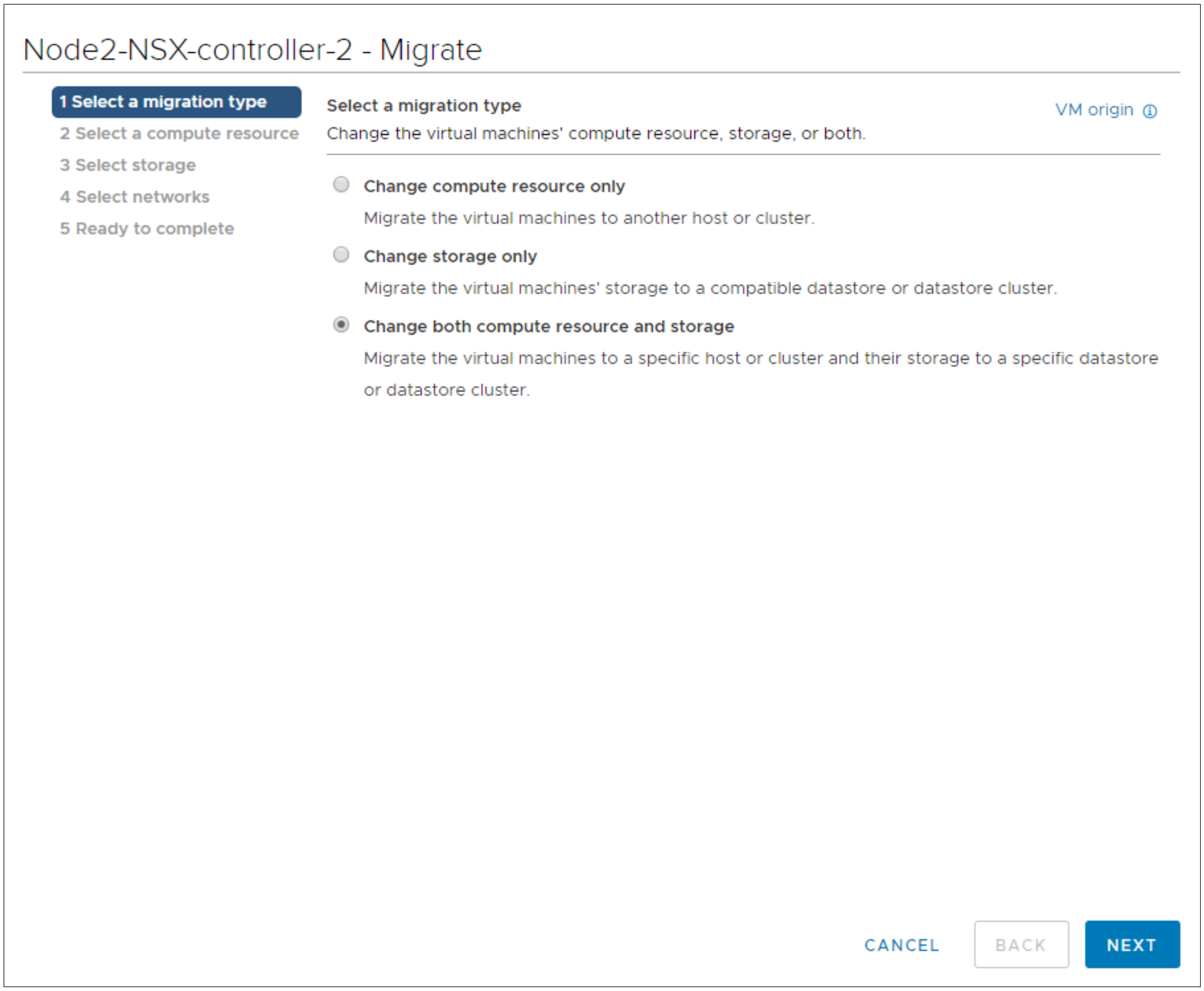
CPU USAGE 219 MHz
MEMORY USAGE 1.6 GB
STORAGE USAGE 72.06 GB

CPU 4 CPU(s)
Memory 16 GB, 1.6 GB memory active
Hard disk 1 10 GB

VMware vCenter Server Appliance

2. You are given the option of 3 types of migration. vMotion = Compute resource only, svMotion = Change storage only, or enhanced or xvMotion is both. The screens after depend

on which you choose here. I will choose both so you see both screens.



Node2-NSX-controller-2 - Migrate

1 Select a migration type
2 Select a compute resource
3 Select storage
4 Select networks
5 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

VM origin ⓘ

○ **Change compute resource only**

Migrate the virtual machines to another host or cluster.

○ **Change storage only**

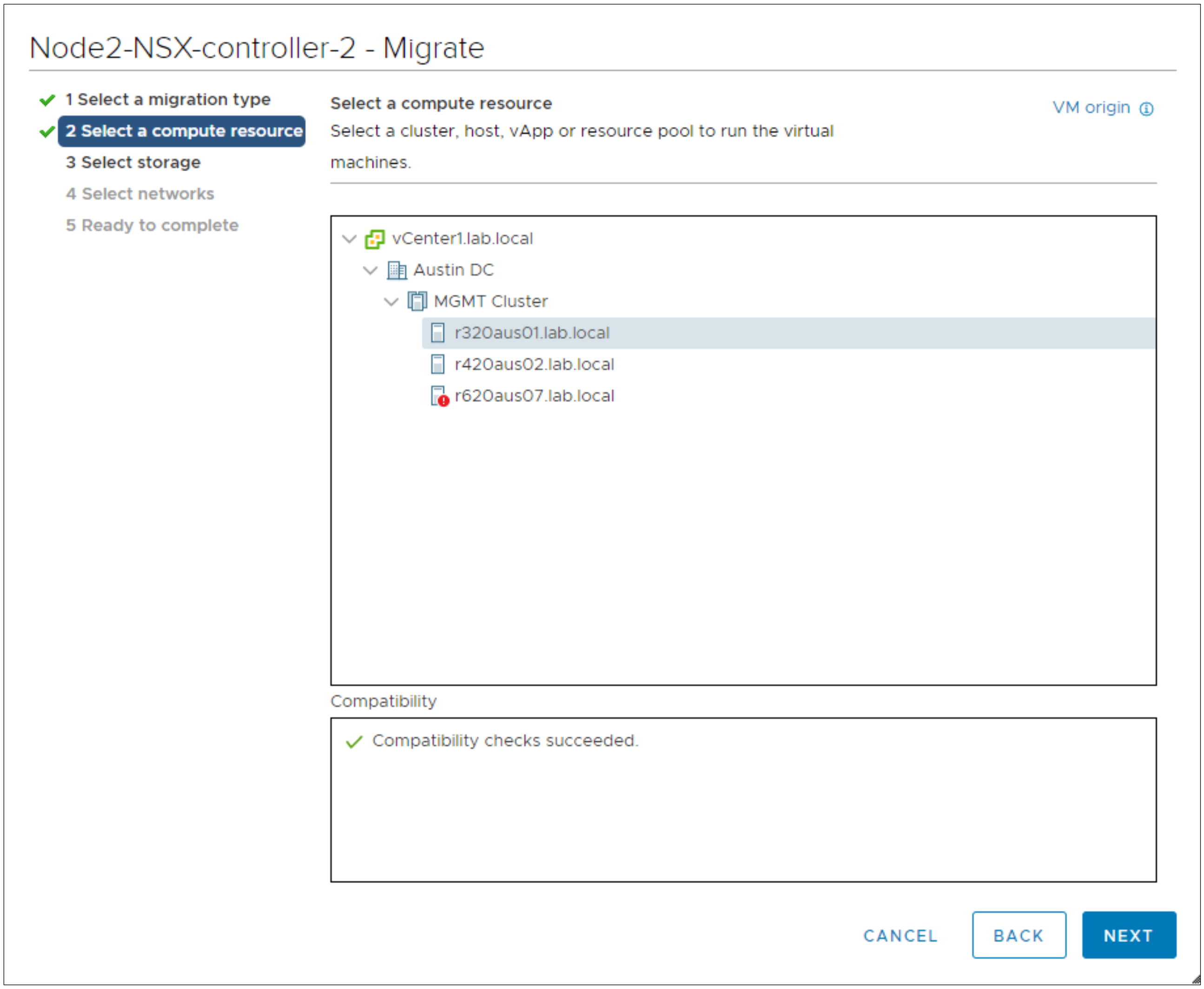
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

● **Change both compute resource and storage**

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

3. For the compute resource to migrate to, I need to choose either a cluster, or individual host. A handy little tidbit that's nice is the upper right-hand corner. VM origin tells you where this

VM is sitting right now, both host and datastore.



Node2-NSX-controller-2 - Migrate

✓ 1 Select a migration type

✓ 2 Select a compute resource

3 Select storage

4 Select networks

5 Ready to complete

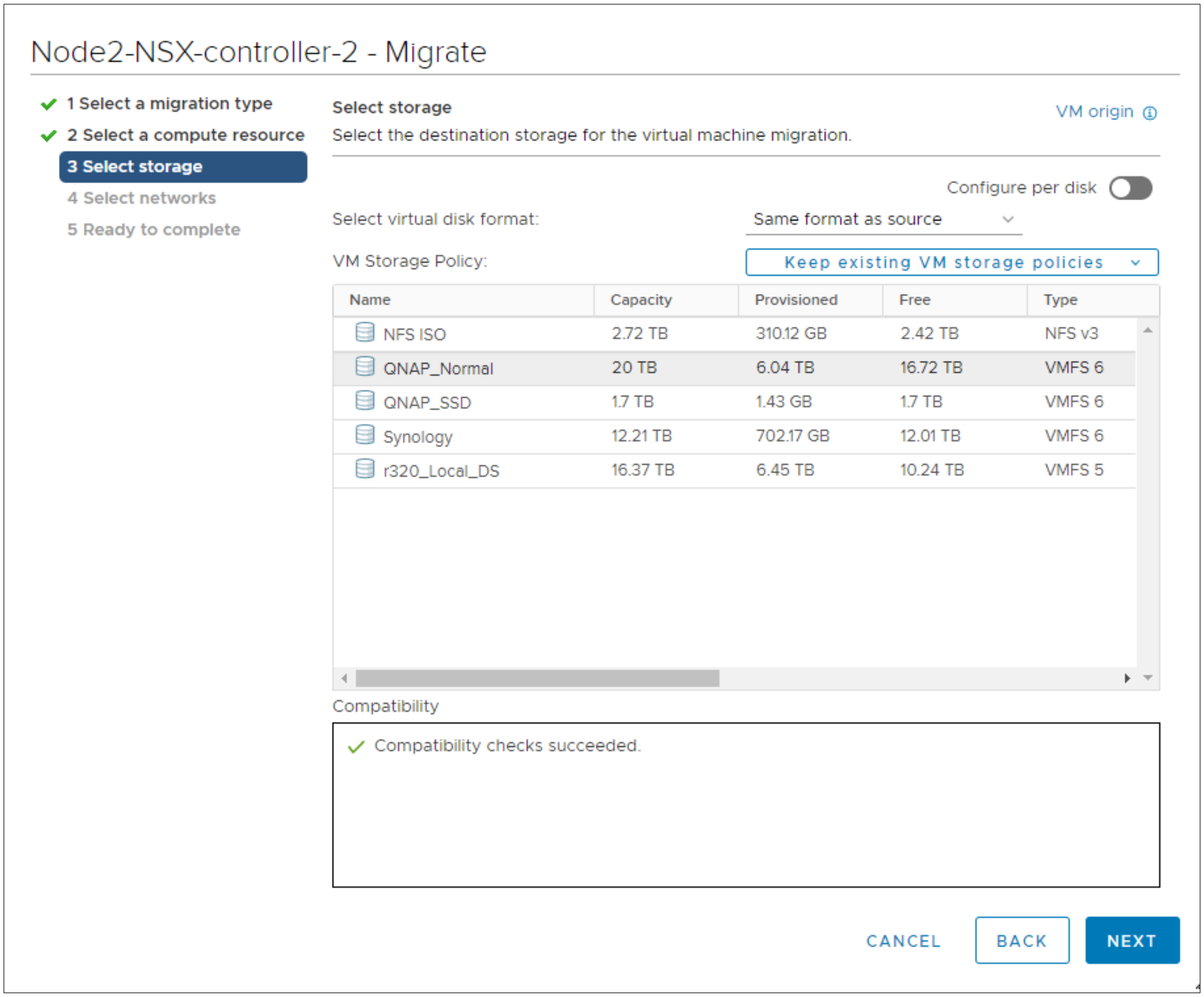
**Select a compute resource**

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

Compatibility

✓ Compatibility checks succeeded.

4. Select storage next.



Node2-NSX-controller-2 - Migrate

Select storage

Select the destination storage for the virtual machine migration.

Configure per disk

Select virtual disk format: Same format as source

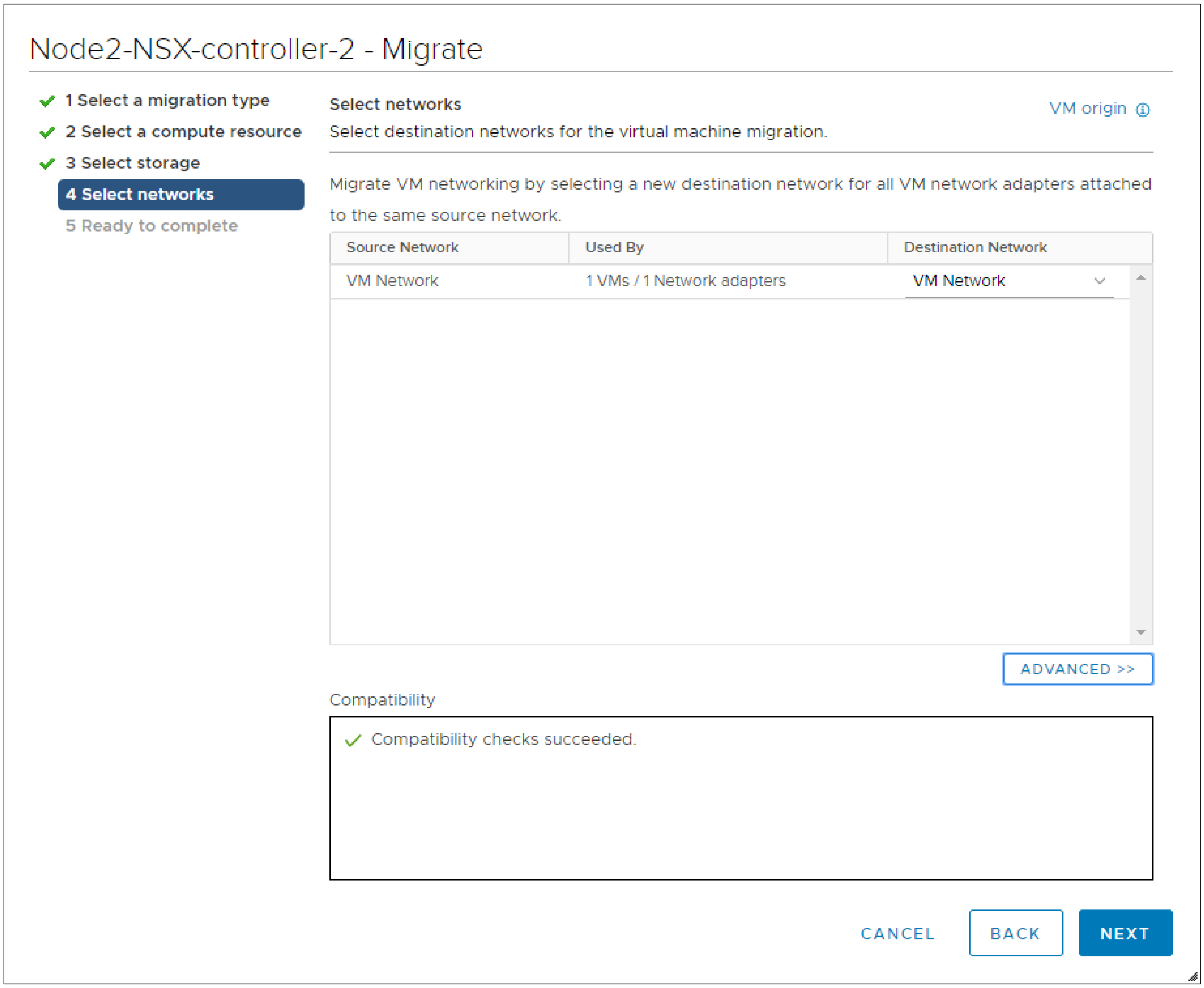
VM Storage Policy: Keep existing VM storage policies

| Name | Capacity | Provisioned | Free | Type |
|---|---|---|---|---|
| NFS ISO | 2.72 TB | 310.12 GB | 2.42 TB | NFS v3 |
| QNAP_Normal | 20 TB | 6.04 TB | 16.72 TB | VMFS 6 |
| QNAP_SSD | 1.7 TB | 1.43 GB | 1.7 TB | VMFS 6 |
| Synology | 12.21 TB | 702.17 GB | 12.01 TB | VMFS 6 |
| r320_Local_DS | 16.37 TB | 6.45 TB | 10.24 TB | VMFS 5 |

Compatibility

✓ Compatibility checks succeeded.

5. Next, select the network for this VM to use.



Node2-NSX-controller-2 - Migrate

Select networks

Select destination networks for the virtual machine migration.

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 |
|---|---|---|
| VM Network | 1 VMs / 1 Network adapters | VM Network |

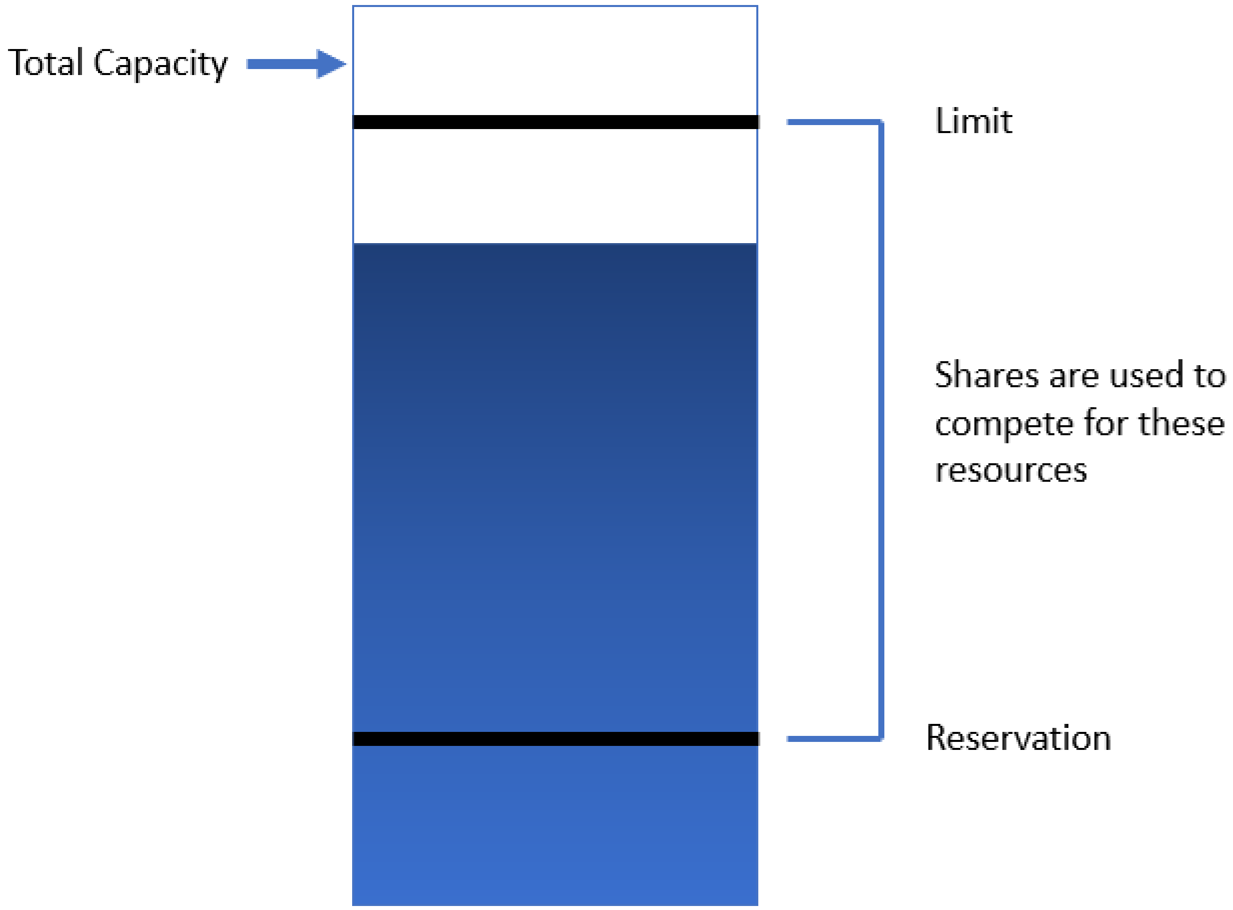
Compatibility

✓ Compatibility checks succeeded.

6. vSphere gives a summary, click Finish and it will migrate.

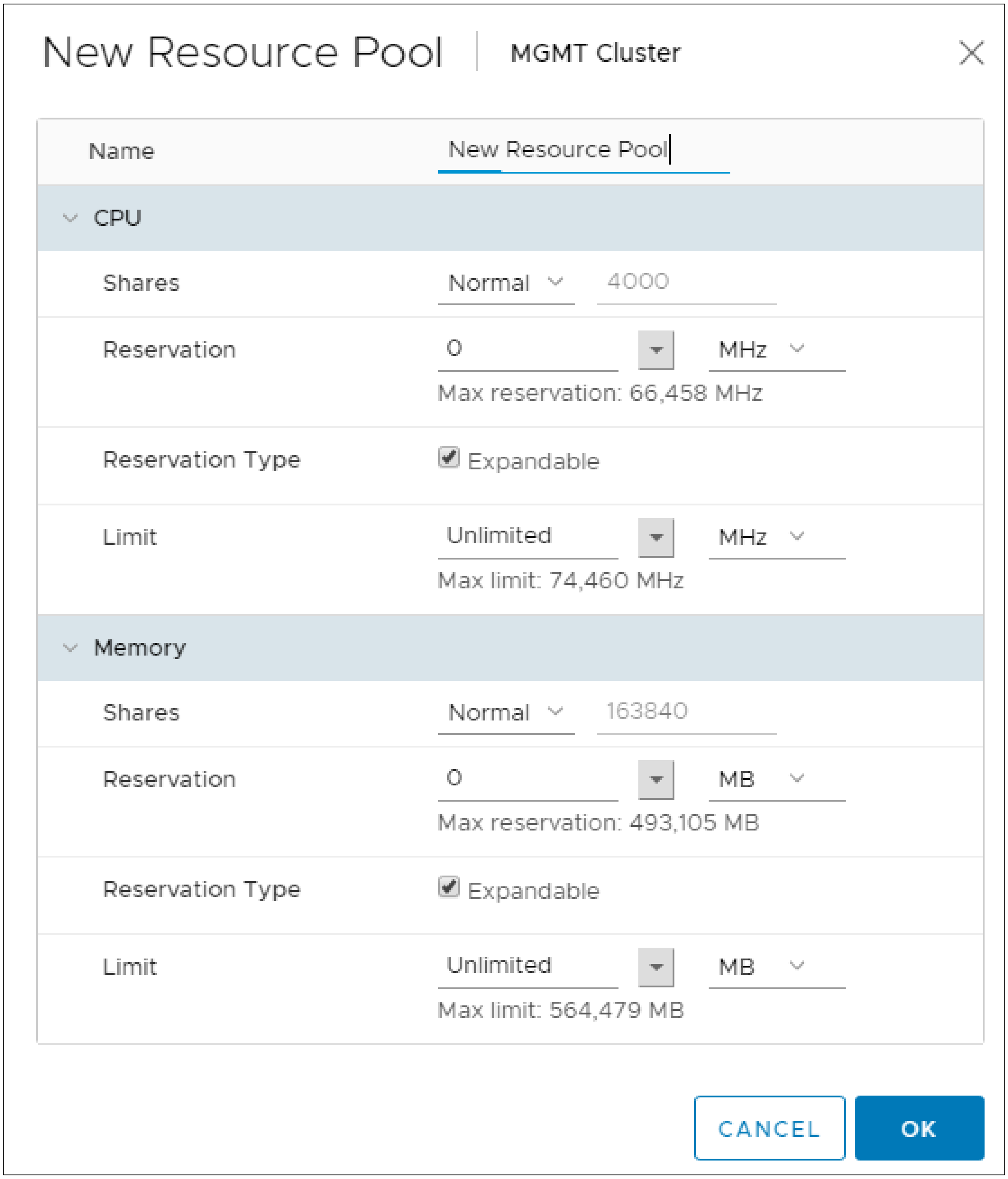
## *Objective 7.8 – Manage resources of a vSphere environment*

There are several resources that can be managed in a vSphere environment. There are mechanisms built-in to vSphere to allow that. You can create resource pools, assign shares for CPU, memory, disk, and network resources. You can also create reservations and limits. Let's define a few of those and how they work.



- Reservations – this is the amount of the resource that is guaranteed. If the resource can't be given, the VM will not power on.
- Limits – are the maximum amount of that resource you will allow for that VM. The issue with limits is if you have extra resources vSphere will still not allow that VM to have more resources.
- Shares are used to compete for the resources between. Shares will only come into play when there is contention for it. During regular periods when all the VMs are happy and there is plenty of resources, shares don't matter.

Resource Pools can also be 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 is what you need to configure when you create a CPU and Memory Resource Pool



New Resource Pool | MGMT Cluster

Name: New Resource Pool

CPU

Shares: Normal 4000

Reservation: 0 MHz

Max reservation: 66,458 MHz

Reservation Type: ☑ Expandable

Limit: Unlimited MHz

Max limit: 74,460 MHz

Memory

Shares: Normal 163840

Reservation: 0 MB

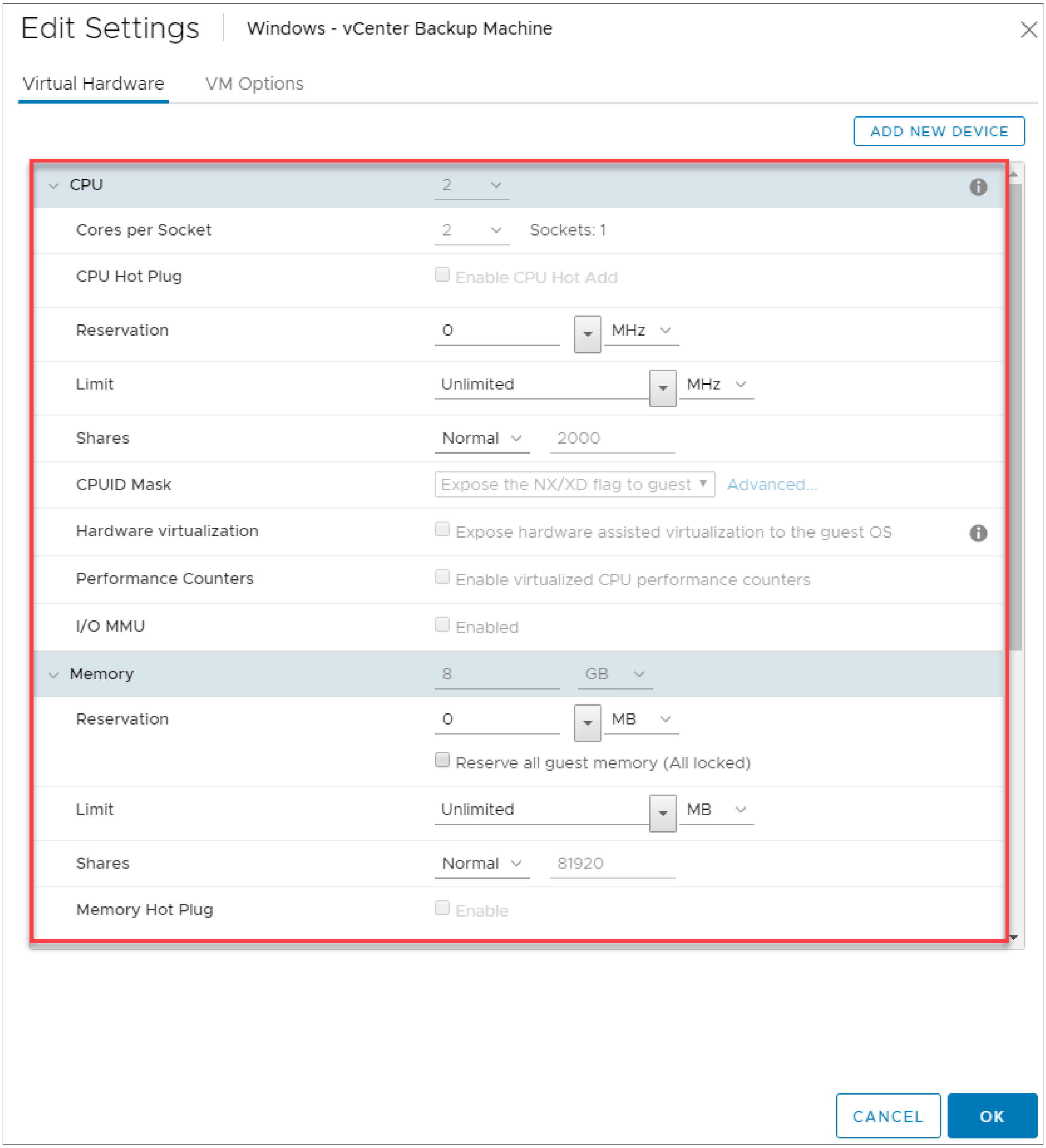
Max reservation: 493,105 MB

Reservation Type: ☑ Expandable

Limit: Unlimited MB

Max limit: 564,479 MB

You can also assign this on an individual VM basis



CPU 2

Cores per Socket 2 Sockets: 1

CPU Hot Plug ☐ Enable CPU Hot Add

Reservation 0 MHz

Limit Unlimited MHz

Shares Normal 2000

CPUID Mask Expose the NX/XD flag to guest Advanced...

Hardware virtualization ☐ Expose hardware assisted virtualization to the guest OS

Performance Counters ☐ Enable virtualized CPU performance counters

I/O MMU ☐ Enabled

Memory 8 GB

Reservation 0 MB

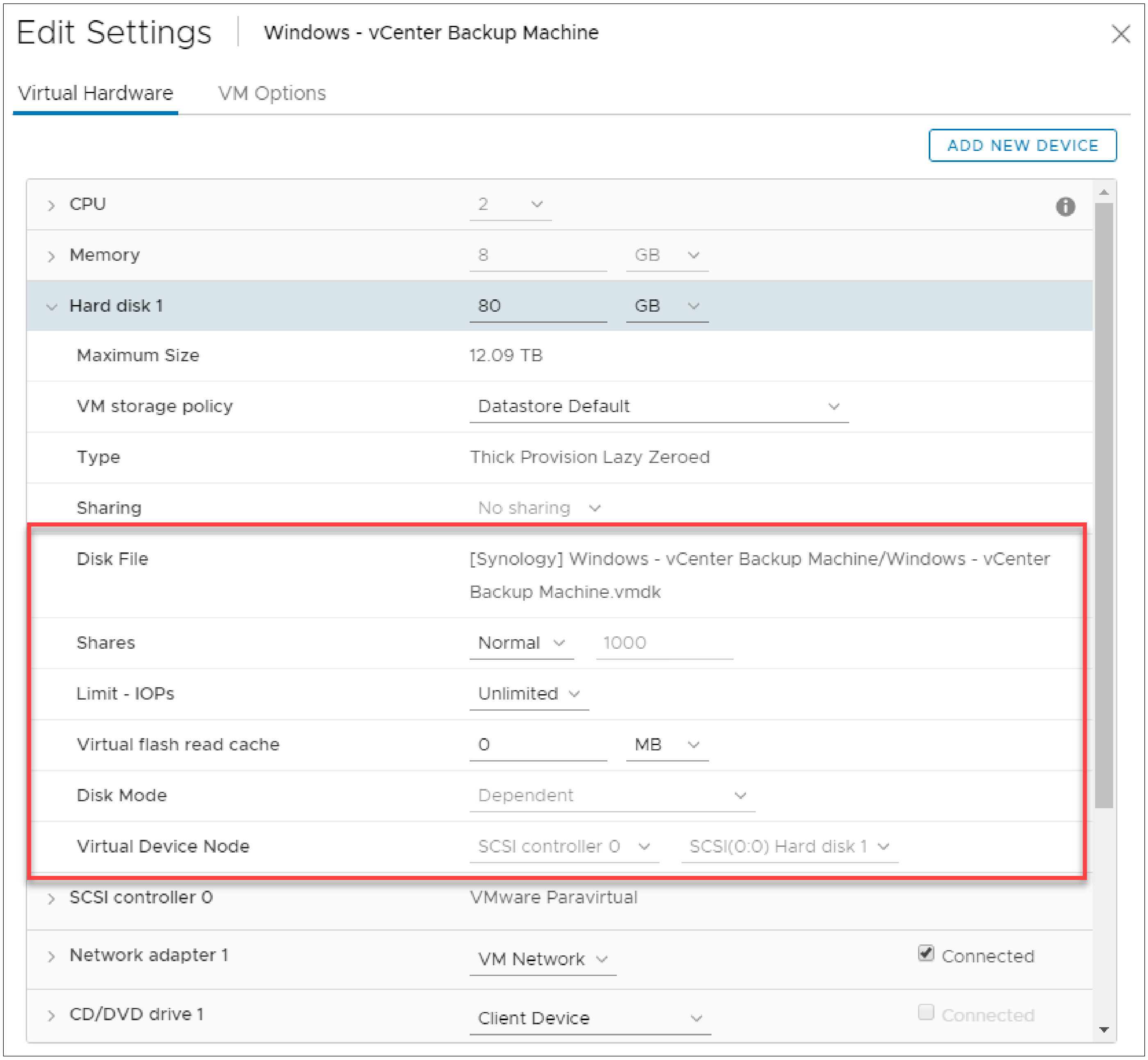
☐ Reserve all guest memory (All locked)

Limit Unlimited MB

Shares Normal 81920

Memory Hot Plug ☐ Enable

To assign disk shares you can look at the individual VM



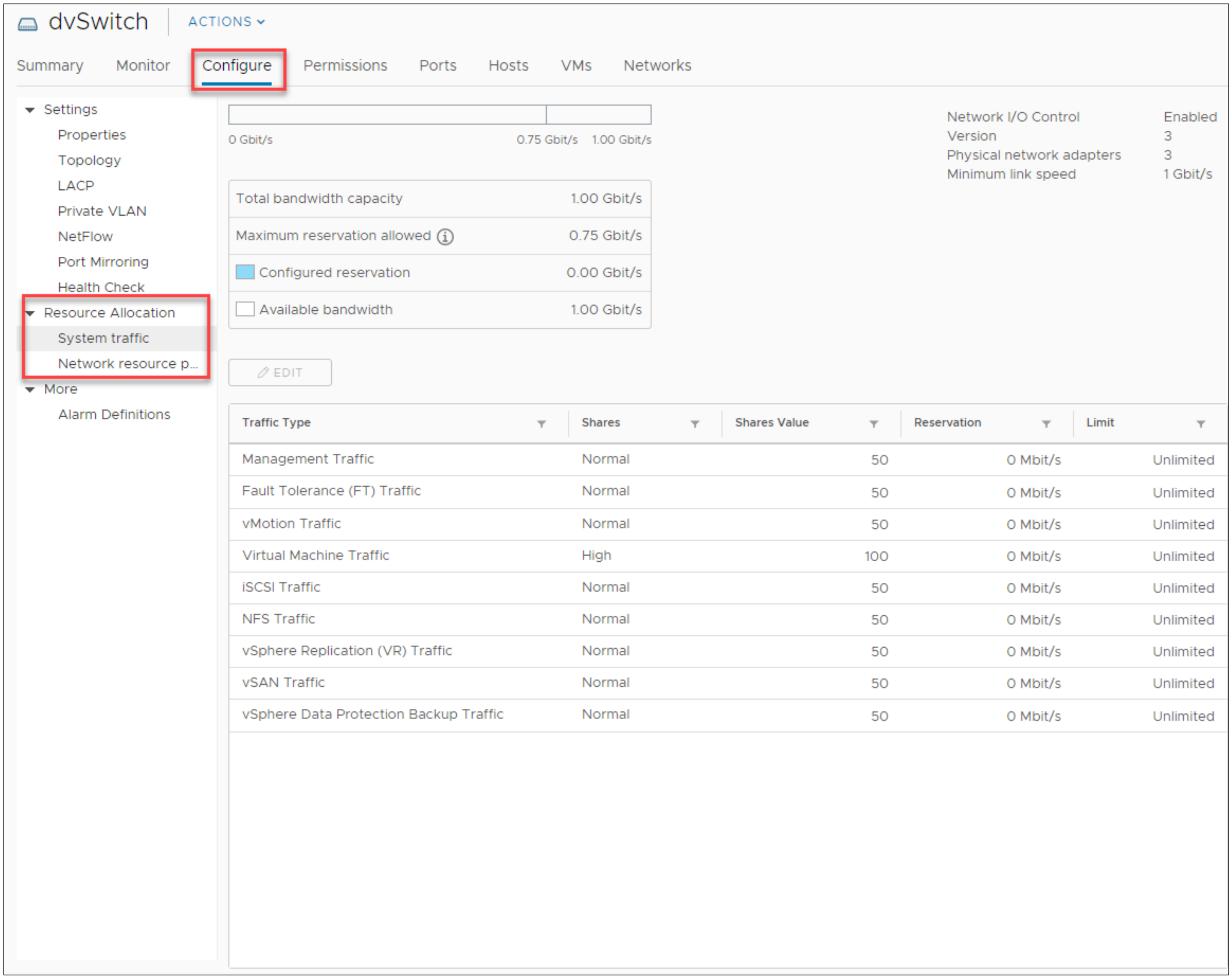
Edit Settings | Windows - vCenter Backup Machine

Virtual Hardware | VM Options

ADD NEW DEVICE

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

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



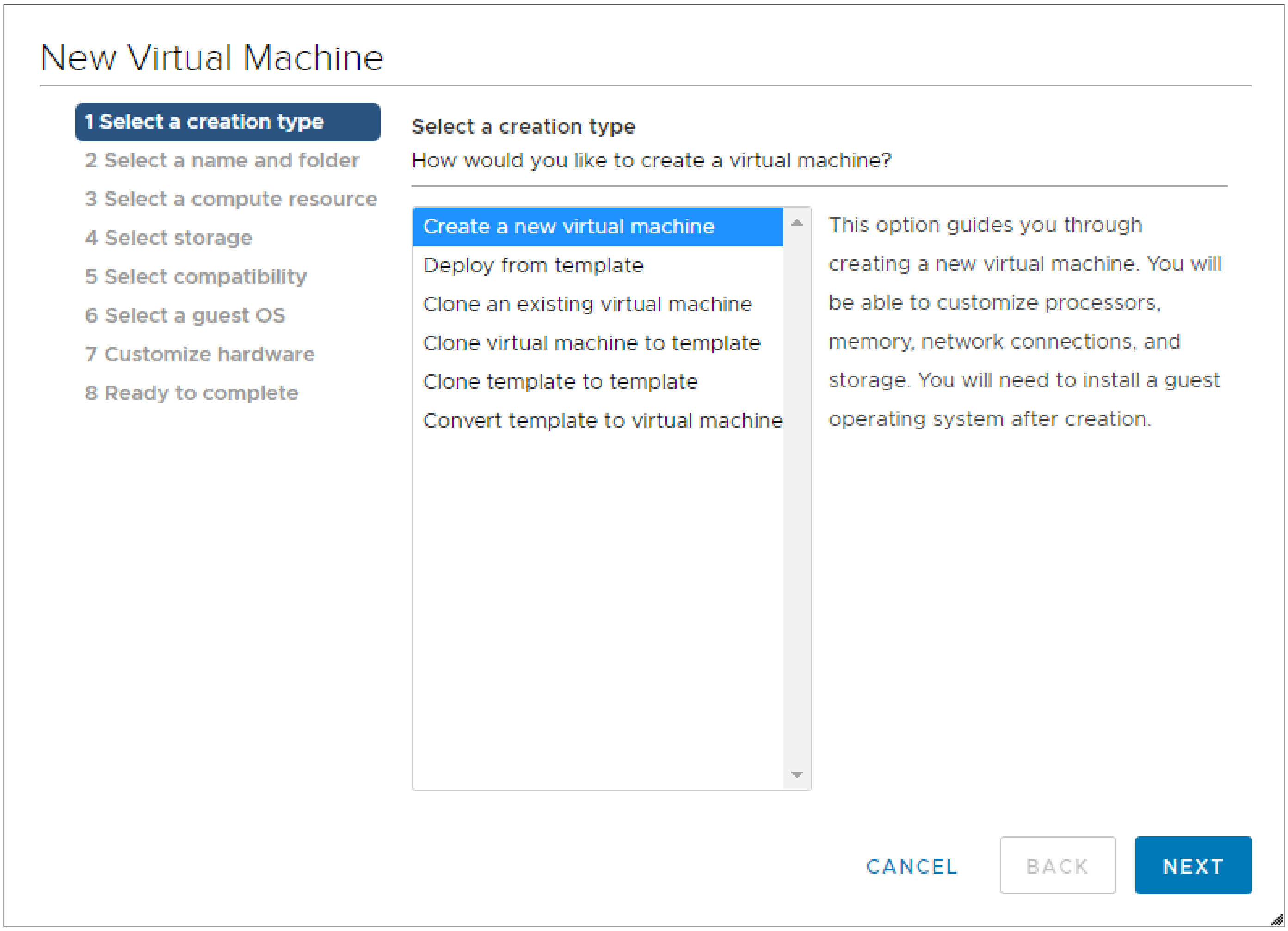
| | |
|---|---|
| Network I/O Control | Enabled |
| Version | 3 |
| Physical network adapters | 3 |
| Minimum link speed | 1 Gbit/s |

| | |
|---|---|
| Total bandwidth capacity | 1.00 Gbit/s |
| Maximum reservation allowed | 0.75 Gbit/s |
| 🟦 Configured reservation | 0.00 Gbit/s |
| □ Available bandwidth | 1.00 Gbit/s |

| 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 |

## *Objective 7.9 – Create and manage VMs using different methods*

There are several methods to create VMs. You can:



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 creation type
How would you like to create a virtual machine?

- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

You can also deploy from an OVF template, use the OVF Tool or create a VM from a physical using the P2V tool. For the purposes of the exam they more than likely just want you to know about the ones in the picture and deploying from an OVF template.

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

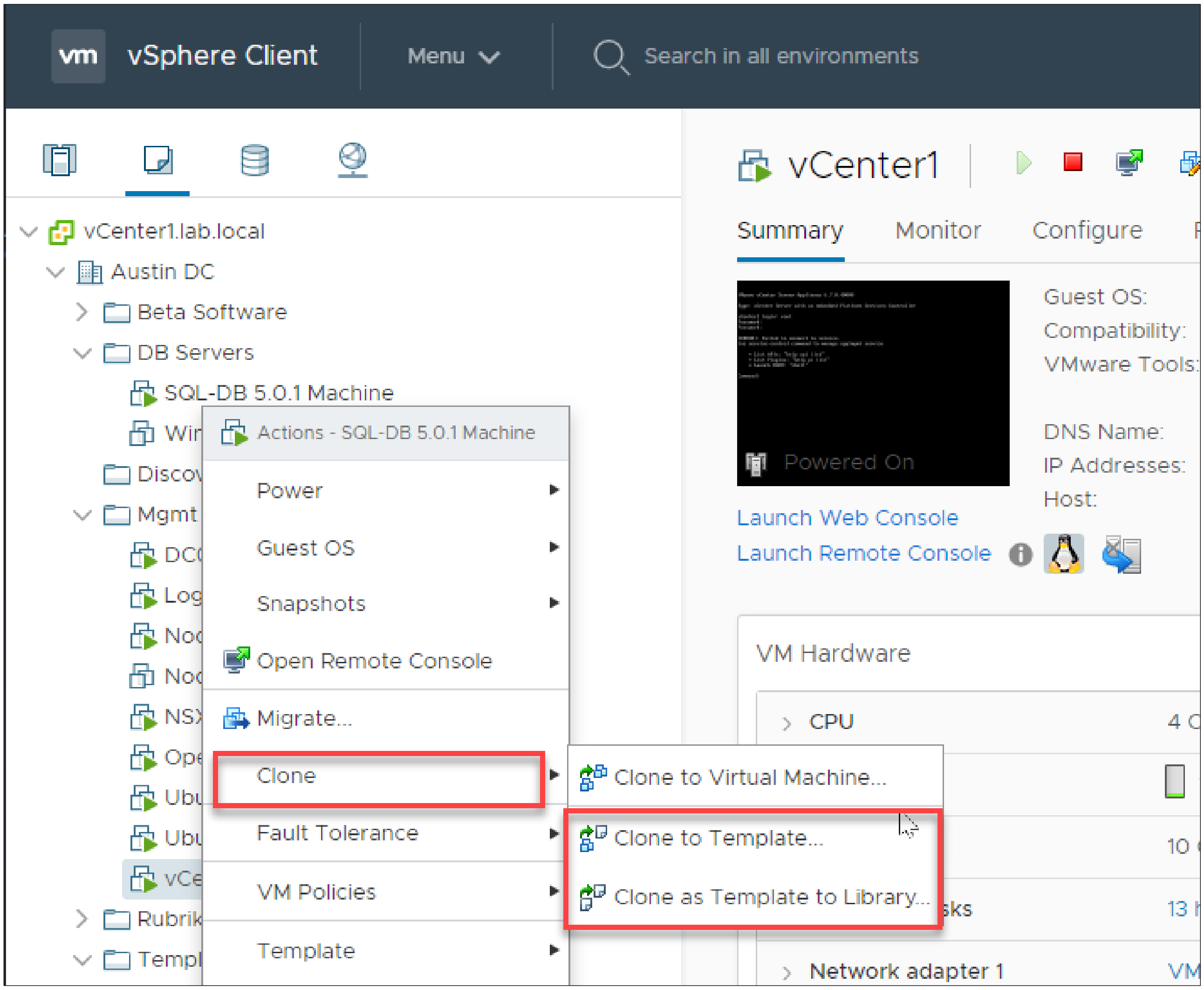
```
New-VM -Name 'TestVM' -VMHost 'VMHost-1' -Datastore 'TestDatastore' -DiskGB 40 -
MemoryGB 8 -NumCpu 2 -NetworkName 'Virtual Machine Network'
```

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

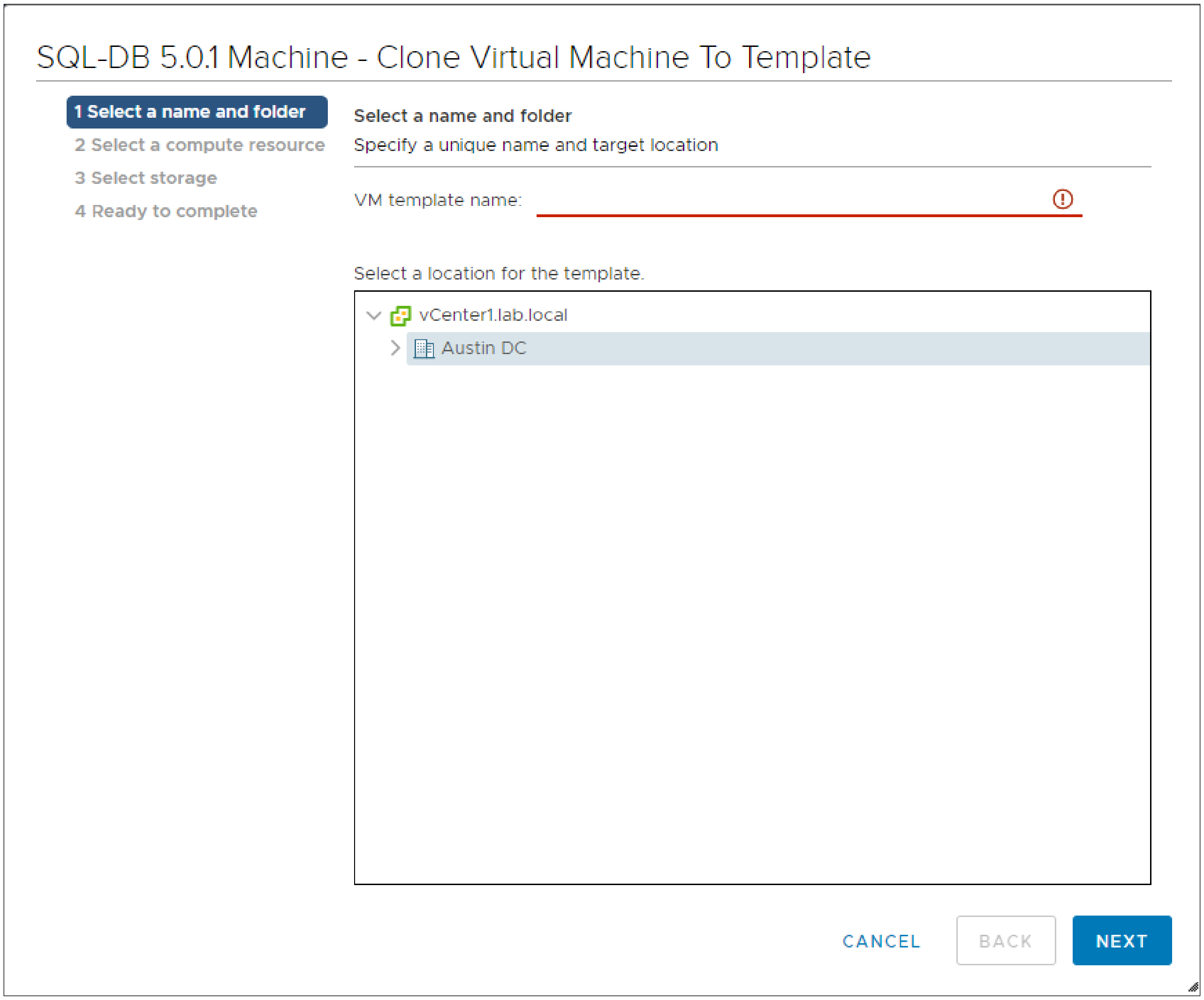
## *Objective 7.10 – Create and manage templates*

Templates are VMs that have been converted so that they can't be turned on. They are used as base server machines or VDI base workstations. Creating them is a simple process. You can do this with a running VM by cloning it (creating a copy) and making the copy a Template. If you want to convert the machine you are working on, it will need to be turned off.  I will go over both ways to do this.

1. Right click on the VM to be converted. We will start with a running VM.



2. Give the VM Template a name



SQL-DB 5.0.1 Machine - Clone Virtual Machine To Template

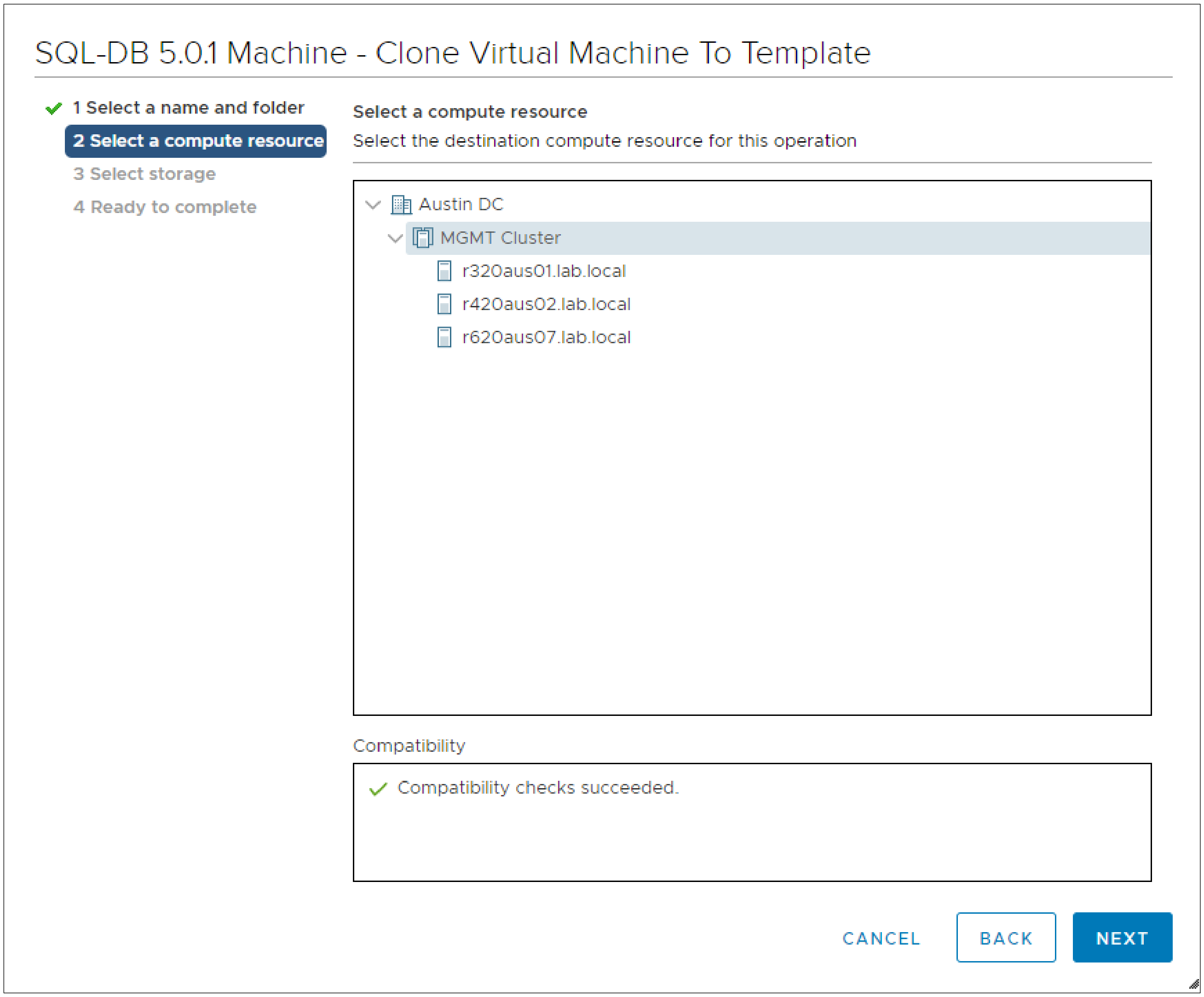
Select a name and folder

Specify a unique name and target location

VM template name:

Select a location for the template.

3. Choose a location for the template



SQL-DB 5.0.1 Machine - Clone Virtual Machine To Template

✓ 1 Select a name and folder
**2 Select a compute resource**
3 Select storage
4 Ready to complete

**Select a compute resource**

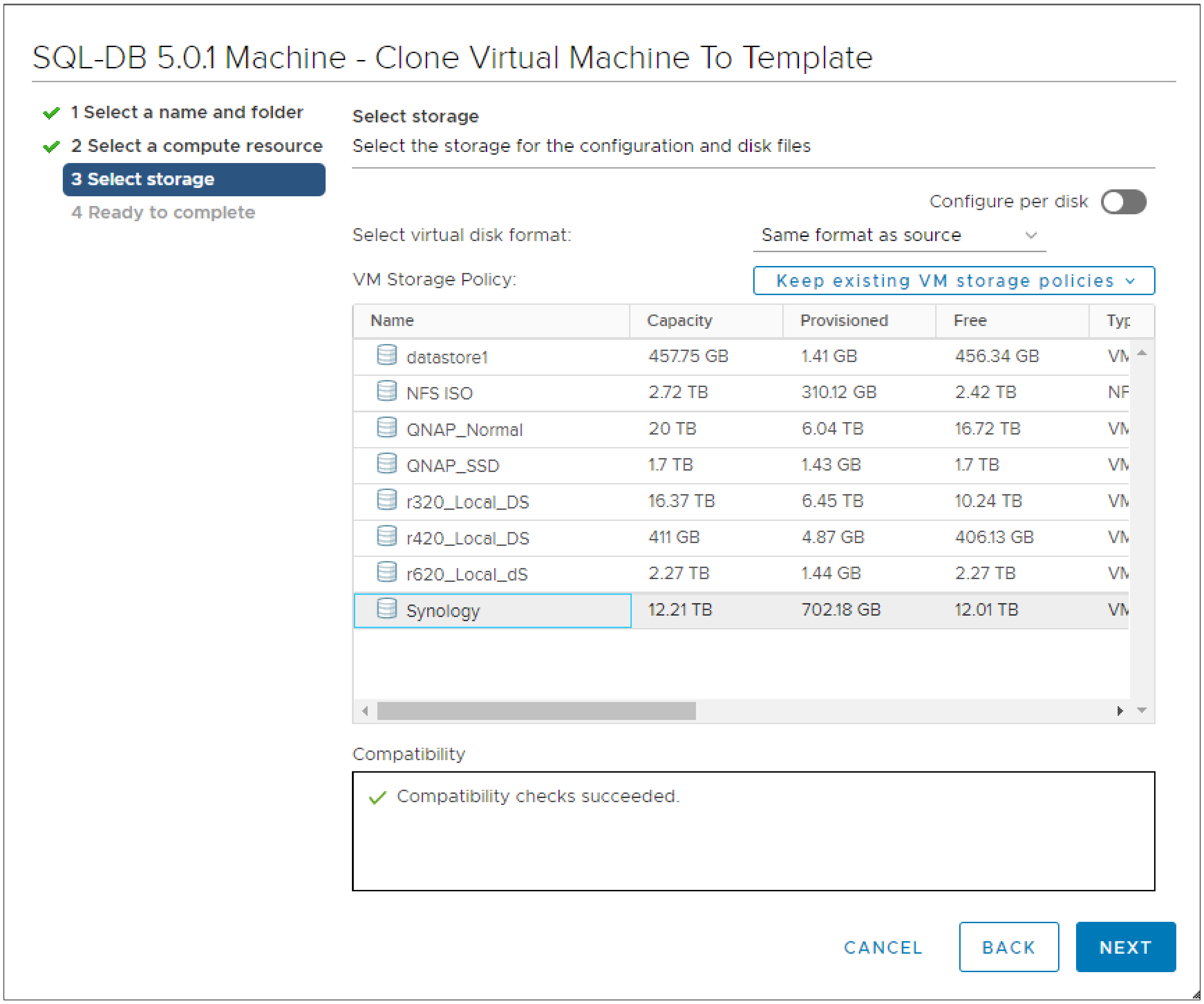
Select the destination compute resource for this operation

- Austin DC
  - MGMT Cluster
    - r320aus01.lab.local
    - r420aus02.lab.local
    - r620aus07.lab.local

Compatibility

✓ Compatibility checks succeeded.

4. Choose storage for the template



SQL-DB 5.0.1 Machine - Clone Virtual Machine To Template

Select storage

Select the storage for the configuration and disk files

Configure per disk

Select virtual disk format: Same format as source

VM Storage Policy: Keep existing VM storage policies

| Name | Capacity | Provisioned | Free | Typ |
|---|---|---|---|---|
| datastore1 | 457.75 GB | 1.41 GB | 456.34 GB | VM |
| NFS ISO | 2.72 TB | 310.12 GB | 2.42 TB | NF |
| QNAP_Normal | 20 TB | 6.04 TB | 16.72 TB | VM |
| QNAP_SSD | 1.7 TB | 1.43 GB | 1.7 TB | VM |
| r320_Local_DS | 16.37 TB | 6.45 TB | 10.24 TB | VM |
| r420_Local_DS | 411 GB | 4.87 GB | 406.13 GB | VM |
| r620_Local_dS | 2.27 TB | 1.44 GB | 2.27 TB | VM |
| Synology | 12.21 TB | 702.18 GB | 12.01 TB | VM |

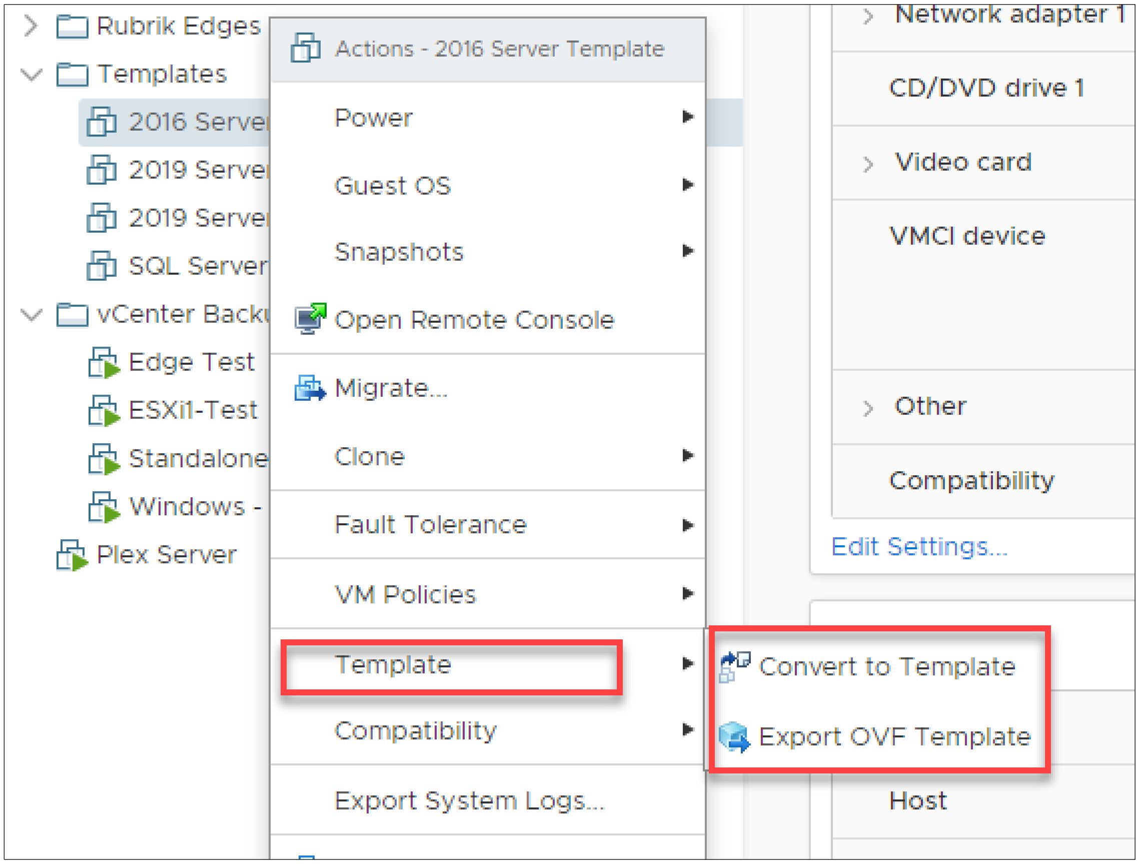
Compatibility

✓ Compatibility checks succeeded.

5. Complete by clicking Finish.

For a machine that is turned off you can clone it as well, but you have the option of turning that VM into a template. To do that:

1. Right click on the VM you want to change to a template.

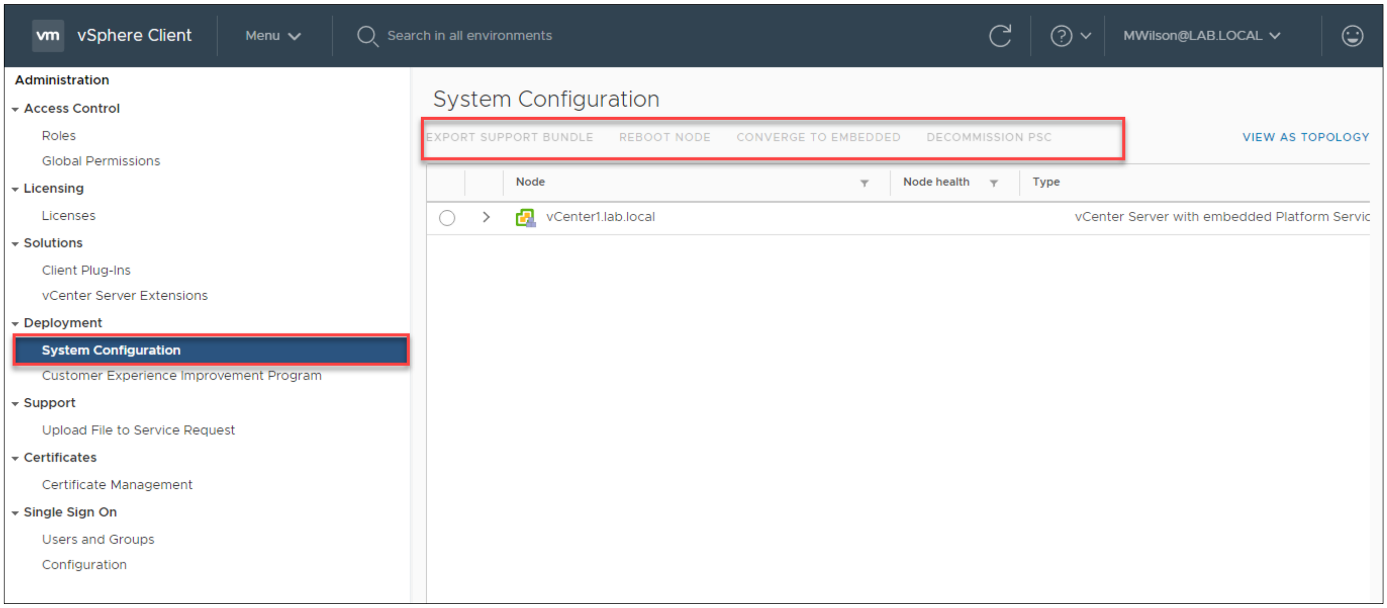


2. If you choose Convert to template, it asks you if you are sure and then does it. If you Export OVF this will save an OVF file to your desktop that is the VM in template format that you can import like an appliance.

## *Objective 7.11 – Manage different VMware vCenter Server objects*

I've gone over how to manage different types of objects so I will take a stab here and guess that they are referring to the actual vCenter Server objects and not clusters, hosts, etc.

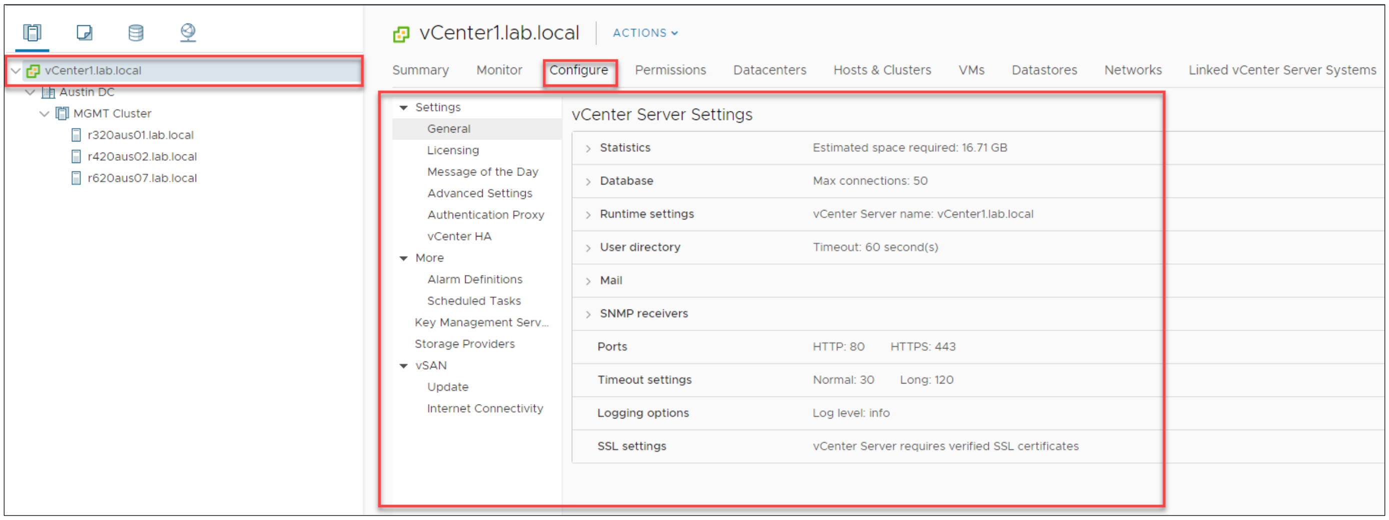
To manage the vCenter Server object, there is a couple of places to go to. The first is Administration > System Configuration. This location will allow you to export a support bundle, converge an external PSC to embedded, and decommission PSC. Oh, you can also reboot it.



System Configuration

| Node | Node health | Type |
|---|---|---|
| vCenter1.lab.local | | vCenter Server with embedded Platform Servic |

The next place you can configure the vCenter is by clicking on the vCenter in the navigation pane and then go to the configure tab in the object pane. You can see that here



vCenter Server Settings

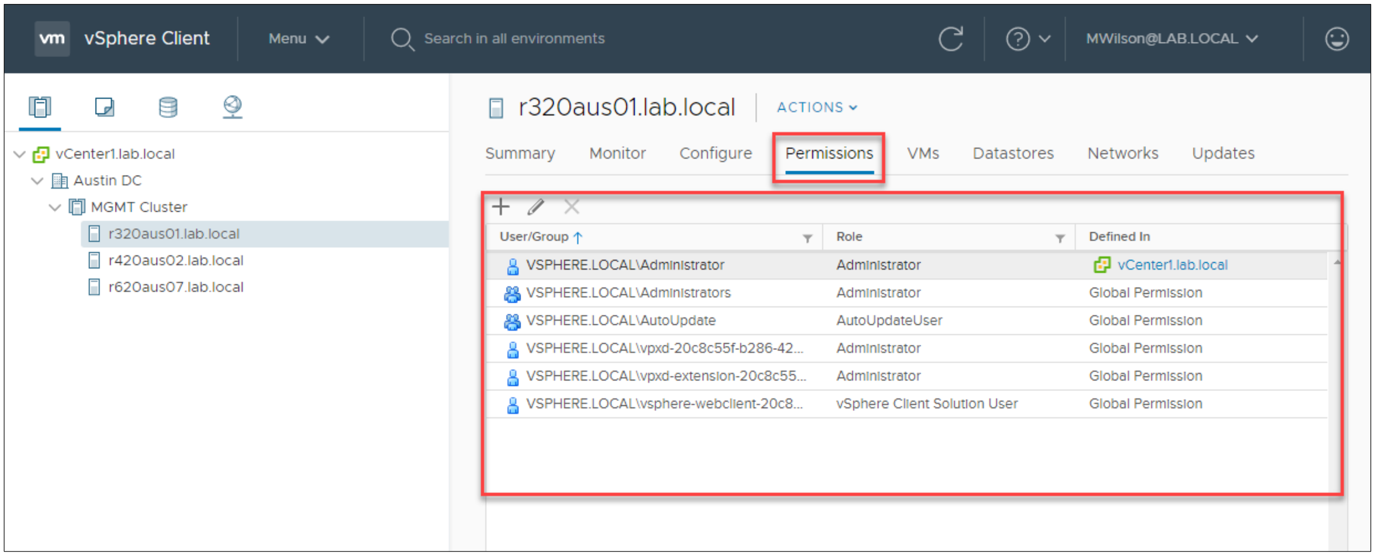
| | |
|---|---|
| Statistics | Estimated space required: 16.71 GB |
| Database | Max connections: 50 |
| Runtime settings | vCenter Server name: vCenter1.lab.local |
| User directory | Timeout: 60 second(s) |
| Mail | |
| SNMP receivers | |
| Ports | HTTP: 80 HTTPS: 443 |
| Timeout settings | Normal: 30 Long: 120 |
| Logging options | Log level: info |
| SSL settings | vCenter Server requires verified SSL certificates |

This is just changing the settings on the vCenter server itself and not the object.

If anyone has a thought on what they may be looking here if I didn't cover it, reach out to me.

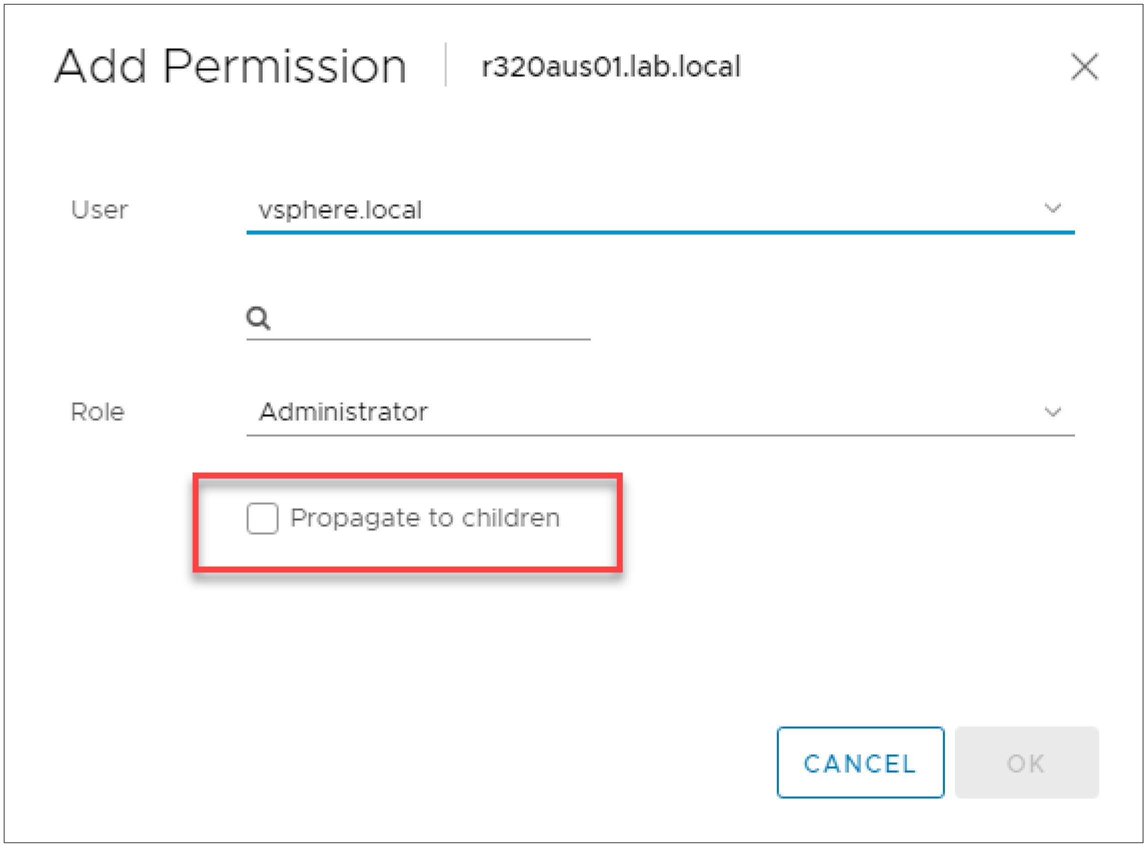
## *Objective 7.12 – Setup permissions on datastores, clusters, vCenter, and hosts*

Permissions can be set on most objects in the vSphere environment. To do that you need to navigate to the Permissions tab in the object pane. Here is an example



| User/Group | Role | Defined In |
|---|---|---|
| VSPHERE.LOCAL\Administrator | Administrator | vCenter1.lab.local |
| VSPHERE.LOCAL\Administrators | Administrator | Global Permission |
| VSPHERE.LOCAL\AutoUpdate | AutoUpdateUser | Global Permission |
| VSPHERE.LOCAL\vpxd-20c8c55f-b286-42... | Administrator | Global Permission |
| VSPHERE.LOCAL\vpxd-extension-20c8c55... | Administrator | Global Permission |
| VSPHERE.LOCAL\vsphere-webclient-20c8... | vSphere Client Solution User | Global Permission |

You can see how you can assign permissions to it. Click on the '+' in order to add another user or group to it. You can also edit an existing permission by clicking on the pencil icon. You can also propagate this permission to its children with the Propagate to children checkbox.



Add Permission | r320aus01.lab.local

User vsphere.local

Role Administrator

□ Propagate to children

If a user has conflicting permissions, the explicit permissions will win over general. This allows you to assign a user “No Access” to an object and it will win over having group rights to it.  The user documentation has this really well. (From the VMware Documentation here)

> If multiple group permissions are defined on the same object and a user belongs to two or more of those groups, two situations are possible:
>
> - No permission for the user is defined directly on the object. In that case, the user has the privileges that the groups have on that object.
> - A permission for the user is defined directly on the object. In that case, the user's permission takes precedence over all group permissions.

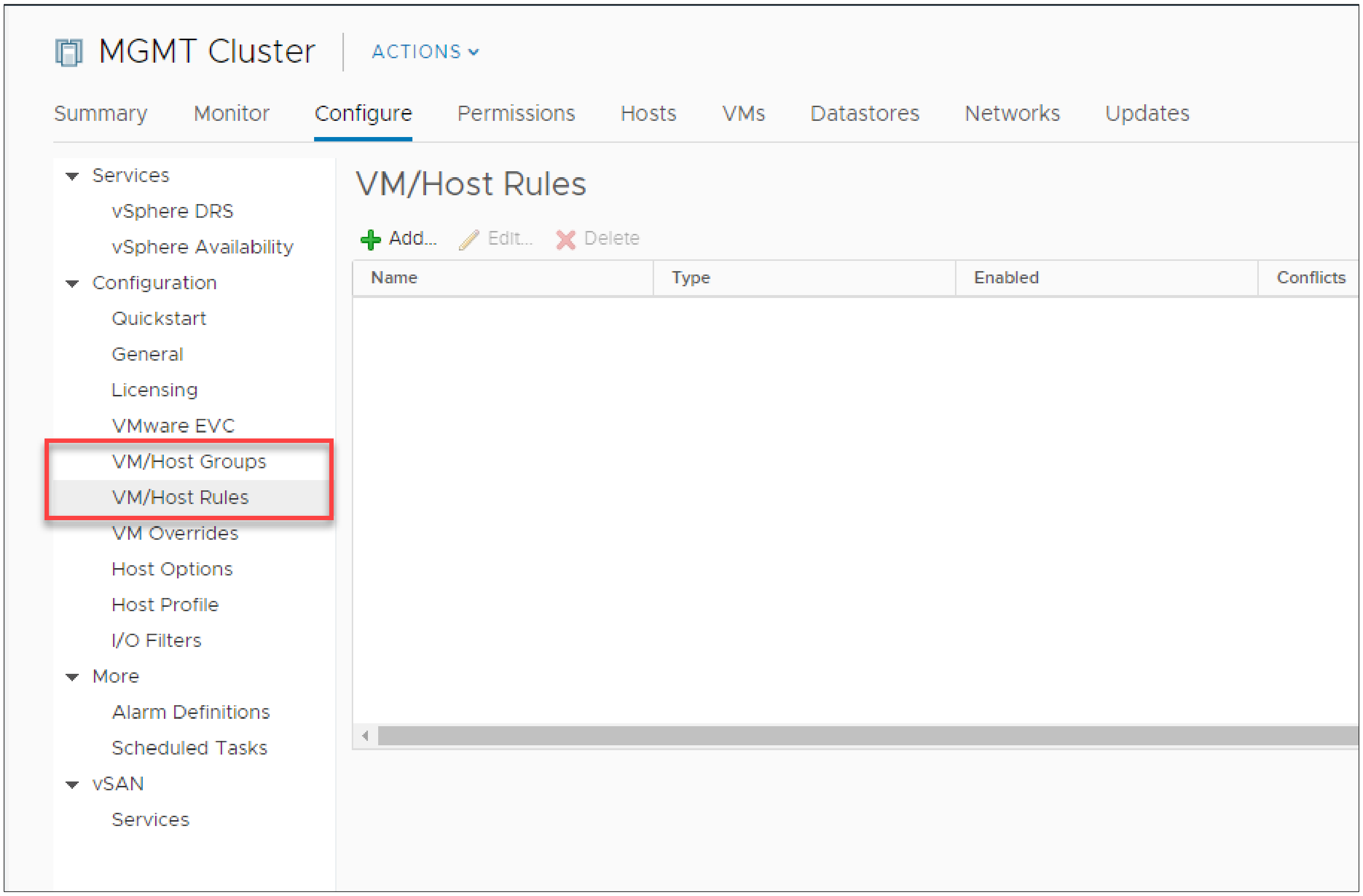
## *Objective 7.13 – Identify and interpret affinity/anti affinity rules*

Affinity and Anti-Affinity rules exist on a DRS enabled cluster. They are typically used for the following reasons:

- Affinity Rules – Used for multi-tier app VMs or other VMs that communicate heavily or depend on each other in order to run. It can also be used to keep a VM running on a specific host for licensing or other purposes.
- Anti-Affinity Rules – Use to keep VMs separate from each other or keep them from running on separate hosts.

These rules can be setup as “Must” rules or “Should” rules. Just like it sounds the Must will prevent the machines from doing what is instructed and if they can’t comply with the rule they won’t start. The Should rules will try everything they can to comply but for example, you are down to one host, the machines will still run there as that is their only option.

You create groups that are made up of either VMs or hosts and then create a rule that defines the relationship between them.  You set them up underneath the Configure tab under your cluster. Here is what that looks like:



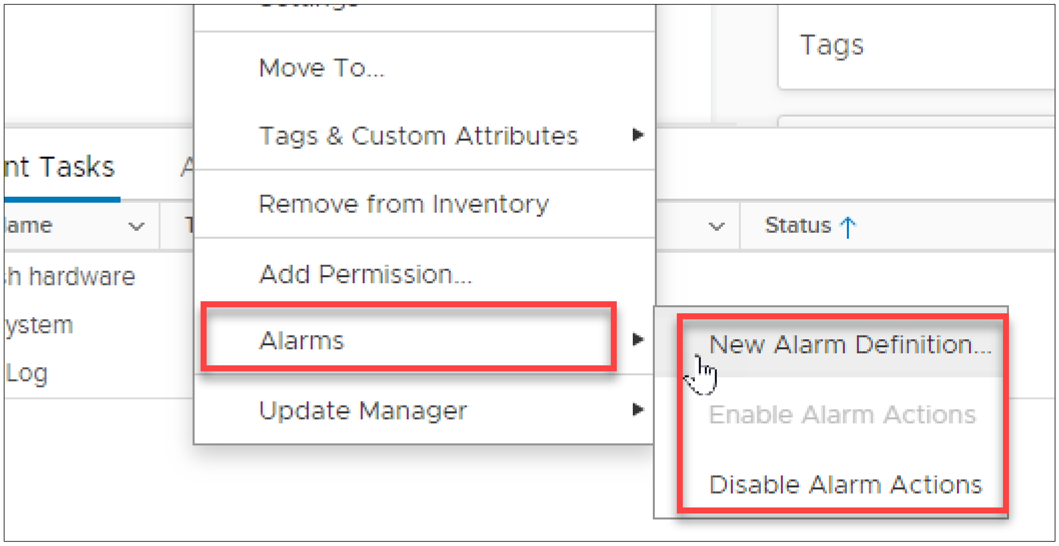
You would create the VM and/or host groups. Then you create the rules that will govern them.

## *Objective 7.14 – Understand use cases for alarms*

Use cases for alarms are plentiful. You don't want errors and issues happening in the background without you knowing. Even better, it would be great to get notice of these events before they happen. That is what alarms can do for you. They can notify you in response to events or conditions that occur to objects in your vSphere environment. There are default alarms setup for hosts and virtual machines already existing for you. You can also setup alarms for many objects. An alarm requires a trigger. This can be one of two things.

- Condition or State. This is monitoring the condition or state of an object. And example of this would be a datastore is using 80 percent of its storage. Or a host is experiencing high CPU usage.
- Event. This would be something like a host hardware changes, or leaves a cluster.

You can setup an alarm by right clicking on the object and then click on Alarms > New Alarm Definition.

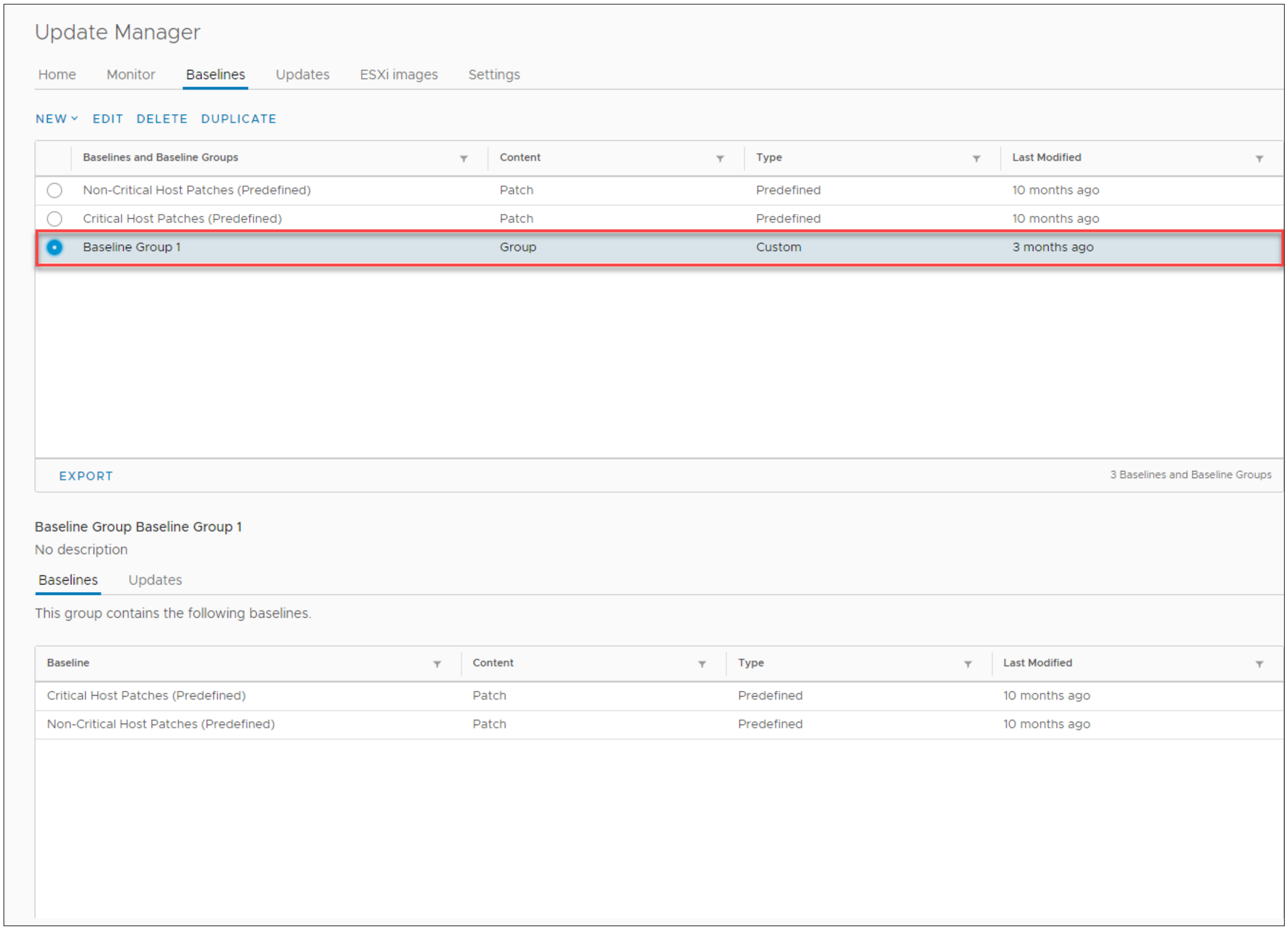


## *Objective 7.15 – Utilize VMware vSphere Update Manager (VUM)*

VUM (vSphere Update Manager) is VMware's server and management utility to patch and upgrade its software. While there were many requirements to get VUM working on previous versions of vSphere, in 6.7 its pretty easy. Though its not completely simple, it does make more sense once you use it for a little bit. First, we need to define a few terms.

Baseline – is one or more patches, extension or upgrade that you want to apply to your vSphere Infrastructure. You can have dynamic patches or static. Dynamic baselines will automatically download and add new patches. I don't necessarily recommend this as you don't know how a patch will affect your environment without testing. Now if it's a test environment go for it! VMware includes two dynamic baselines for patches predefined for you. You can create your own.

Baseline Group – Includes multiple baselines. The pre-defined ones are Non-Critical and Critical Patches. Unless one causes an issue, it would be good to have both of those. I created a group that includes both called Baseline Group 1.



Update Manager

| | Baselines and Baseline Groups | Content | Type | Last Modified |
|---|---|---|---|---|
| ○ | Non-Critical Host Patches (Predefined) | Patch | Predefined | 10 months ago |
| ○ | Critical Host Patches (Predefined) | Patch | Predefined | 10 months ago |
| ● | Baseline Group 1 | Group | Custom | 3 months ago |

3 Baselines and Baseline Groups

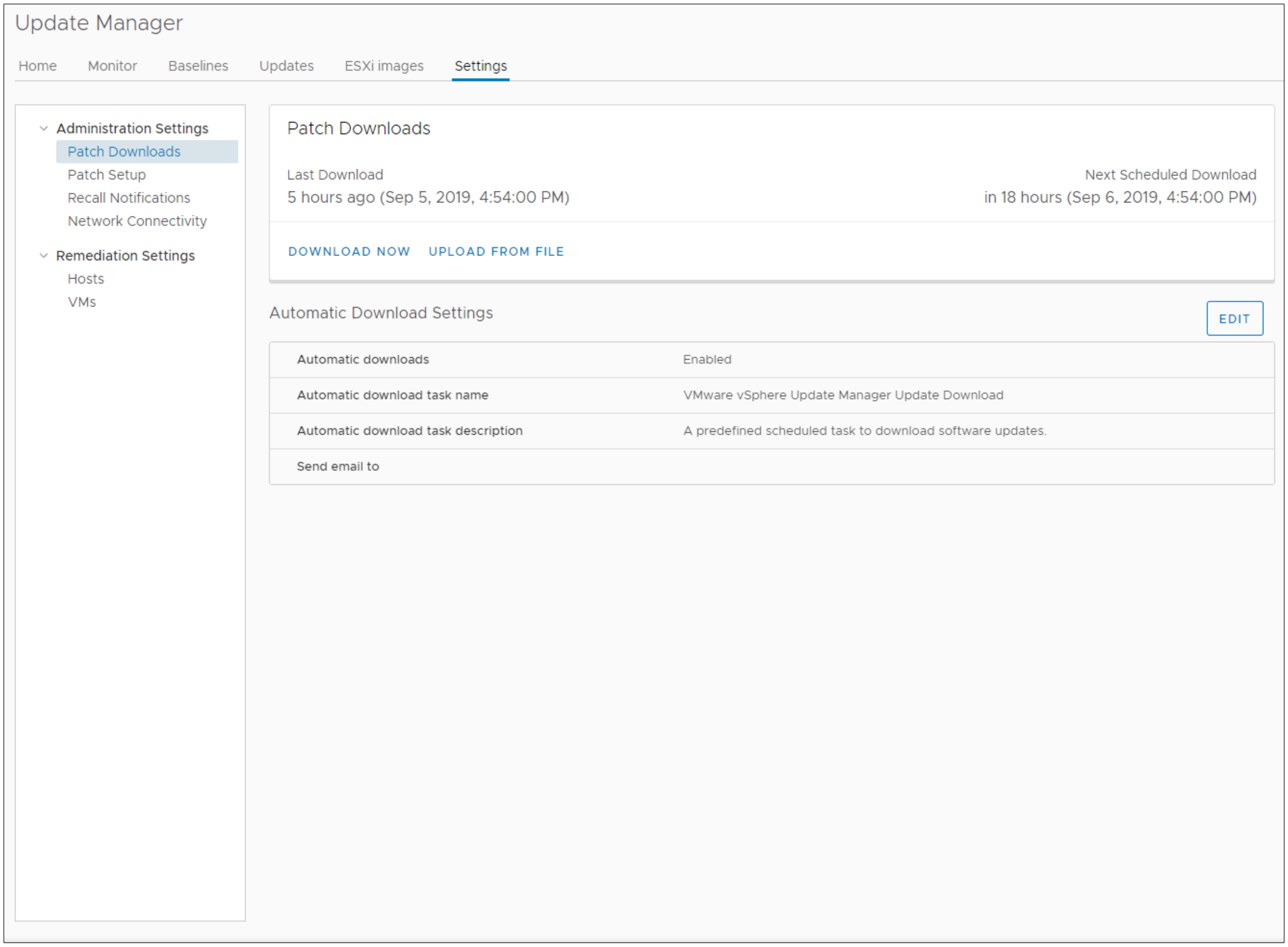
Baseline Group Baseline Group 1

No description

This group contains the following baselines.

| Baseline | Content | Type | Last Modified |
|---|---|---|---|
| Critical Host Patches (Predefined) | Patch | Predefined | 10 months ago |
| Non-Critical Host Patches (Predefined) | Patch | Predefined | 10 months ago |

You can create a baseline that includes an upgrade say from 6.5 to 6.7 as well. There are settings that go along with this service and here is what they look like.



Patch Downloads

Last Download
5 hours ago (Sep 5, 2019, 4:54:00 PM)

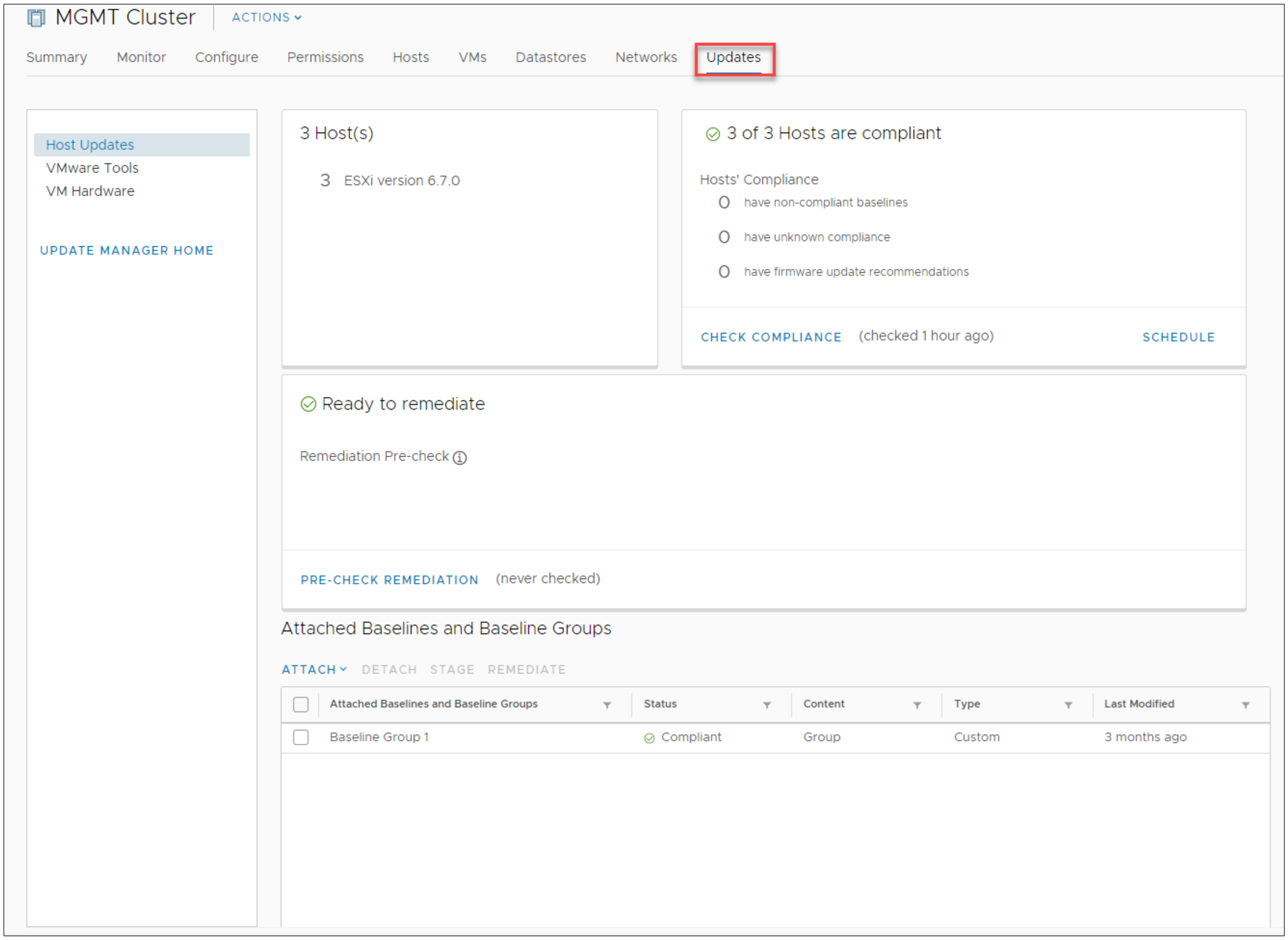
Next Scheduled Download
in 18 hours (Sep 6, 2019, 4:54:00 PM)

Automatic Download Settings

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

- 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?
    - Recall Notification. Occasionally VMware needs to recall a patch that isn't up to par. This setting will notify you there is a recall and what it is and make sure it doesn't apply that patch to any hosts.
    - Network Connectivity. Connectivity for VUM. Mainly port numbers and host name.
- Remediation Settings
    - Hosts – When you apply the baselines to a host, what do you want it with the VMs, host if it uses PXE to boot, and retries.
    - VMs – If you are remediating VMs do you want to take a snapshot automatically and how long do you want to keep them.

The setup of the server is just the first step though. You now need to get these patches to the hosts and VMs. You have two options when you apply them. You can Stage, or Remediate. Stage will just load the patches on it and wait for you to tell it to take action. Remediate takes immediate action. You can do this by going to the update tab for the object. Here is the update for the cluster.



3 Host(s)

3 ESXi version 6.7.0

3 of 3 Hosts are compliant

Hosts' Compliance

0 have non-compliant baselines

0 have unknown compliance

0 have firmware update recommendations

(checked 1 hour ago)

Ready to remediate

Remediation Pre-check

(never checked)

Attached Baselines and Baseline Groups

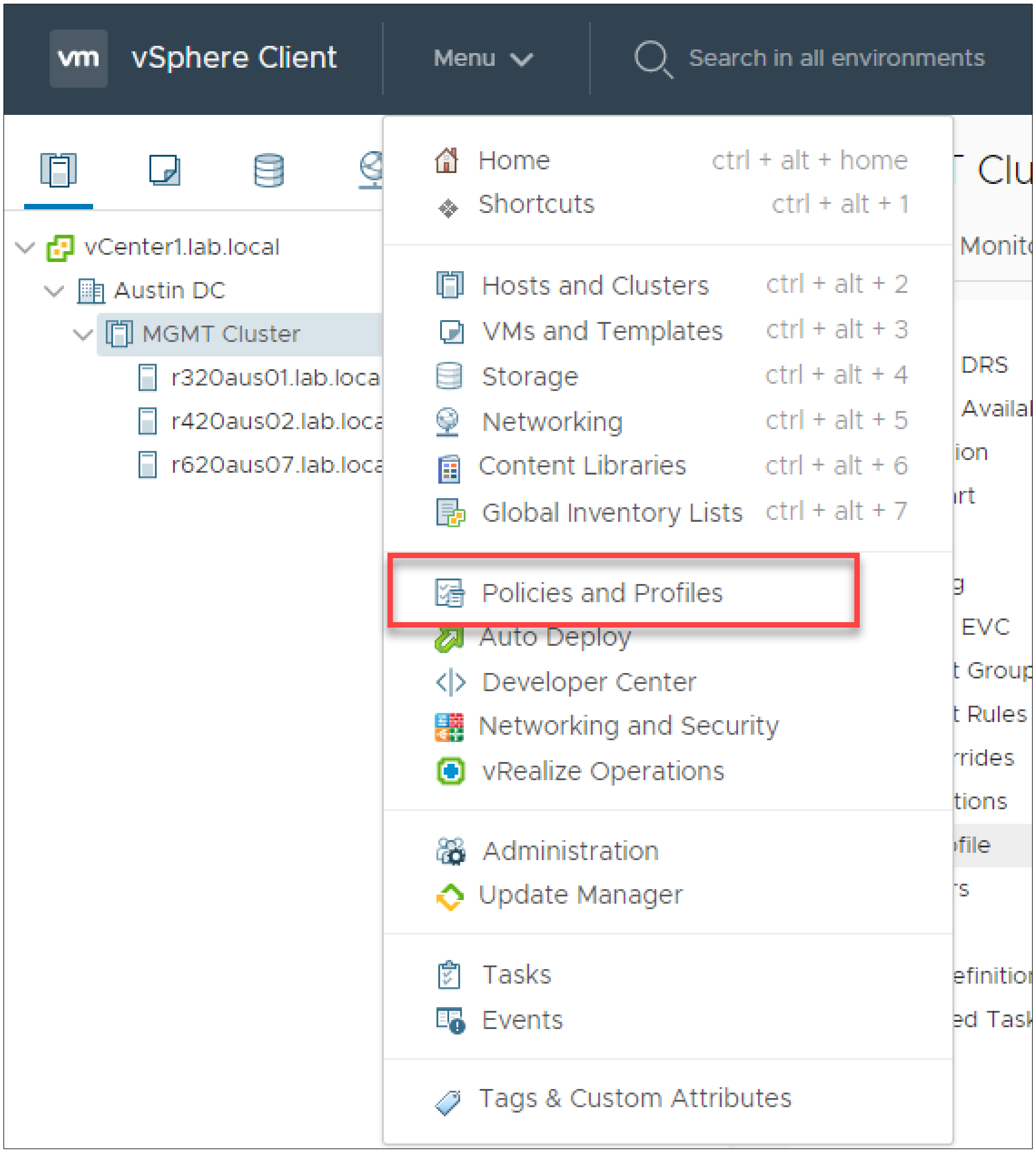
| □ | Attached Baselines and Baseline Groups | Status | Content | Type | Last Modified |
|---|---|---|---|---|---|
| □ | Baseline Group 1 | ✓ Compliant | Group | Custom | 3 months ago |

At the bottom you notice I attached the baseline. This is needed to stage or remediate your hosts and VMs. You can then check them by Checking Compliance. You may also notice you can update VMware Tools and VM Hardware versions en masse. (may require VM reboot)

## *Objective 7.16 - Configure and manage host profiles*

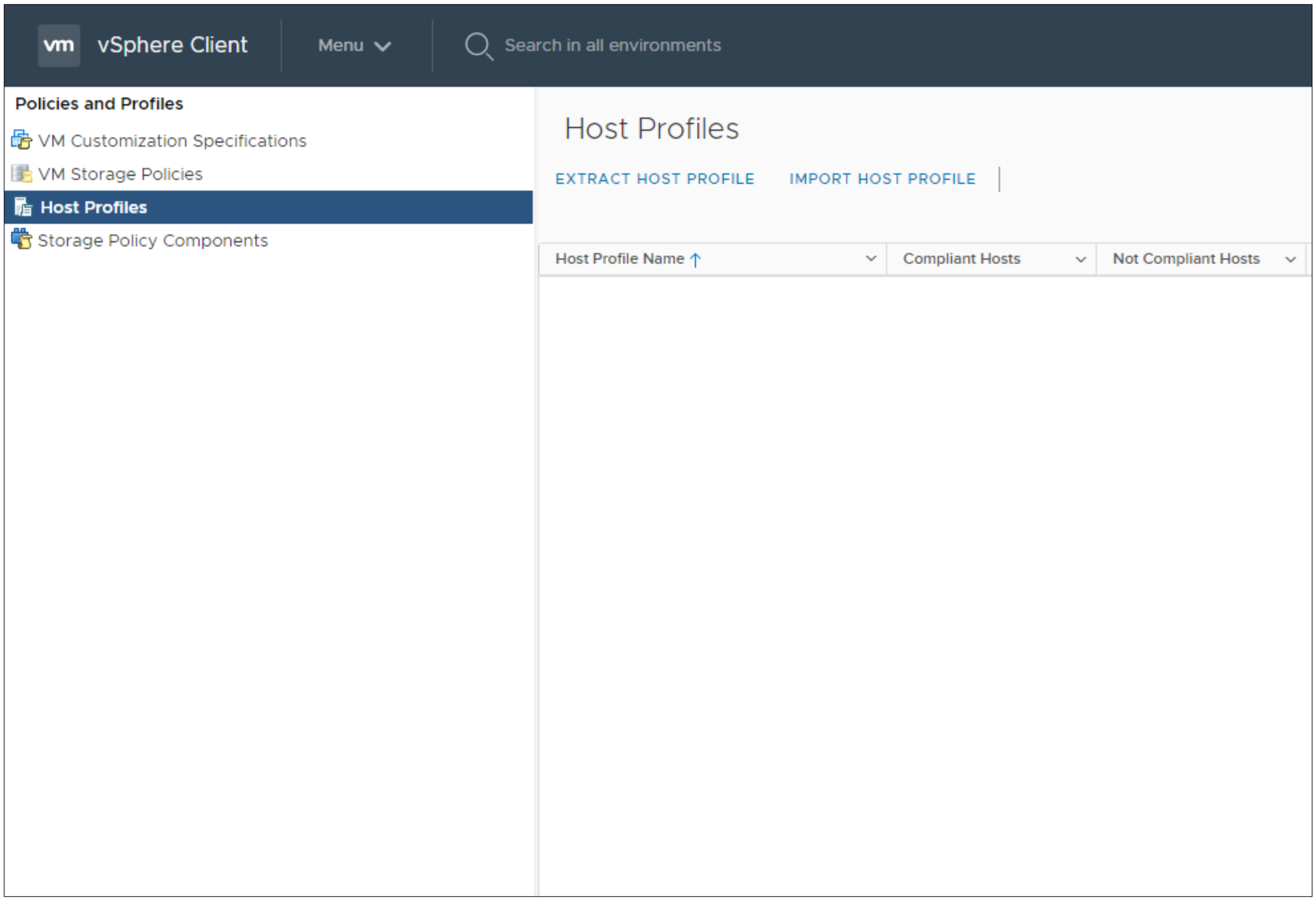
Host profiles provide a mechanism to automate and create a base template for your hosts. Using host profiles, you can make all your hosts exactly the same. VMware will inform you if your host is not in compliance yet and then you can take steps to remediate it.

You access it under Policies and Profiles

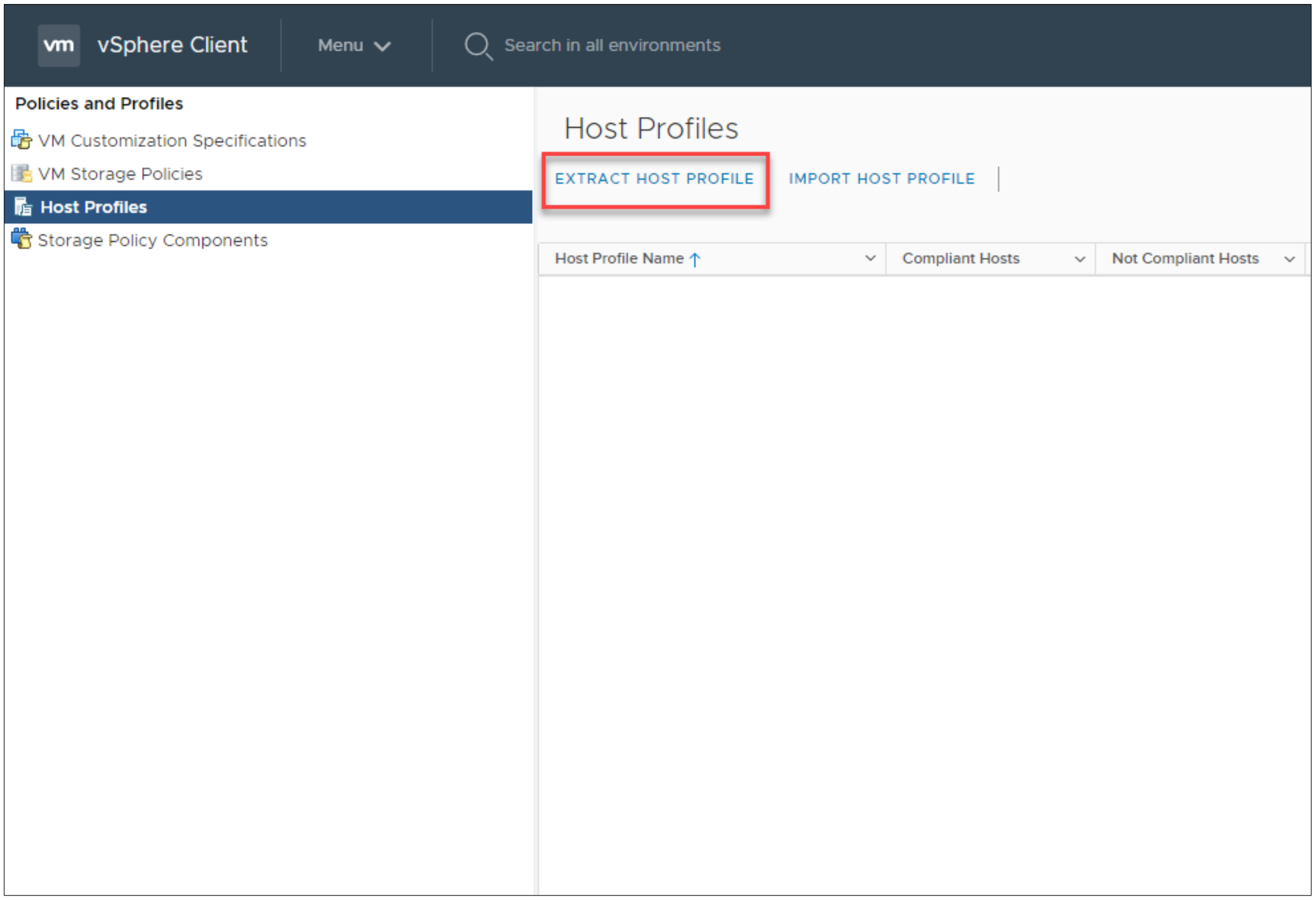


There is a process to it. Here it is:

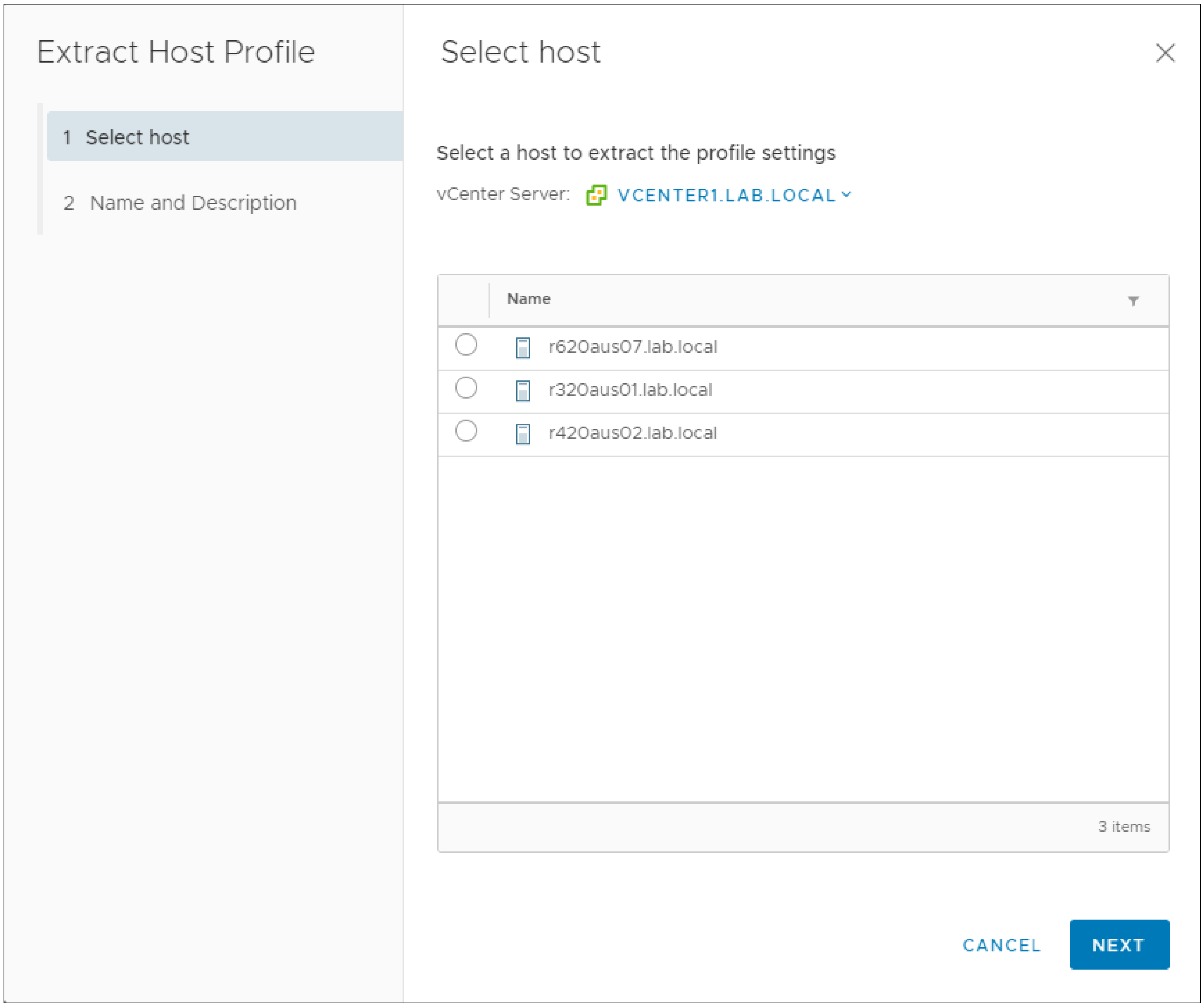
1. Click on Host Profiles on the navigation pane on the left.



2. Next is Extract Host Profile. This is going to be taking a host you select and that will be the "baseline"



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



Extract Host Profile

1 Select host

2 Name and Description

Select host

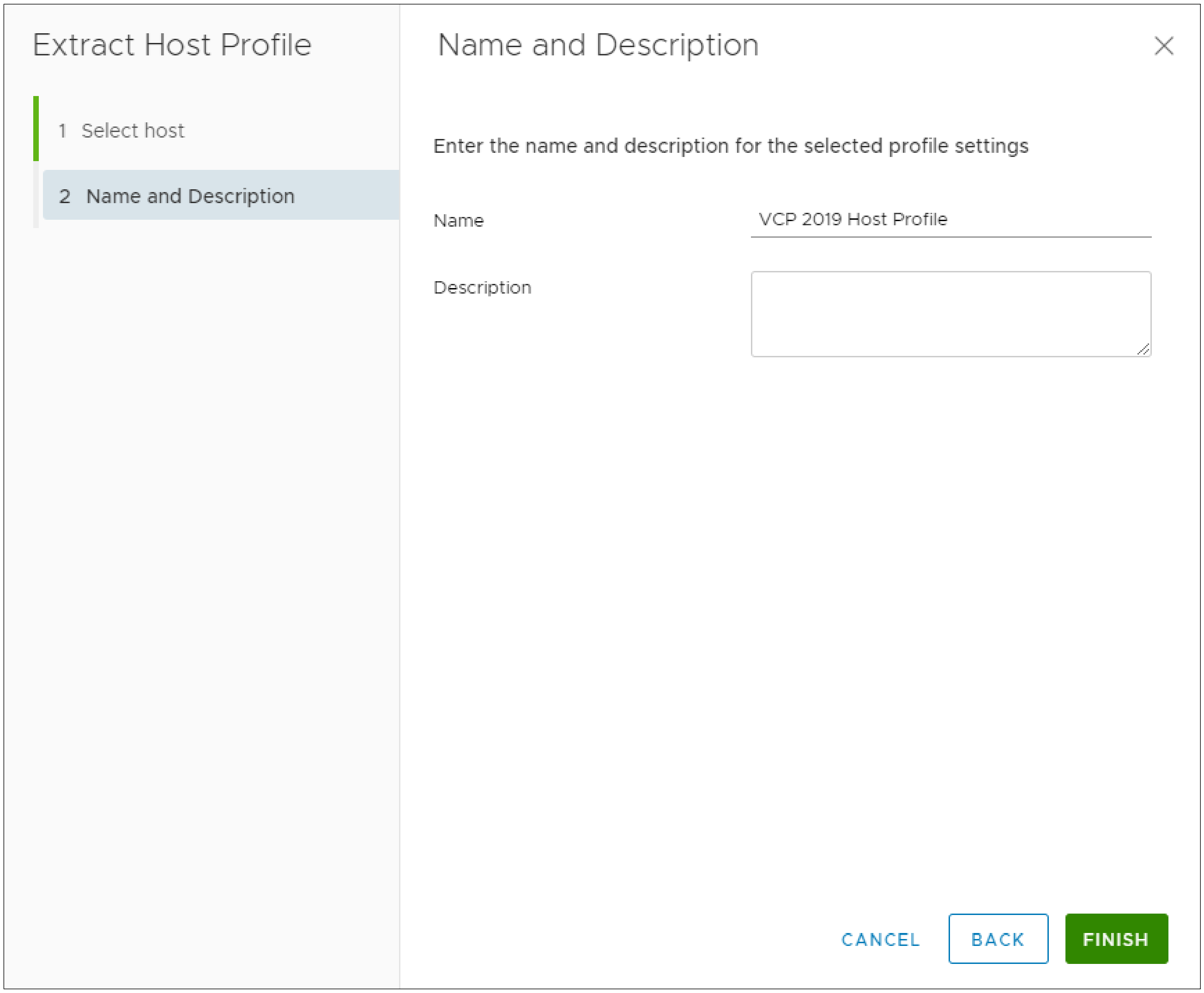
Select a host to extract the profile settings

vCenter Server: VCENTER1.LAB.LOCAL

| | Name |
|---|---|
| ○ | r620aus07.lab.local |
| ○ | r320aus01.lab.local |
| ○ | r420aus02.lab.local |

3 items

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



Extract Host Profile

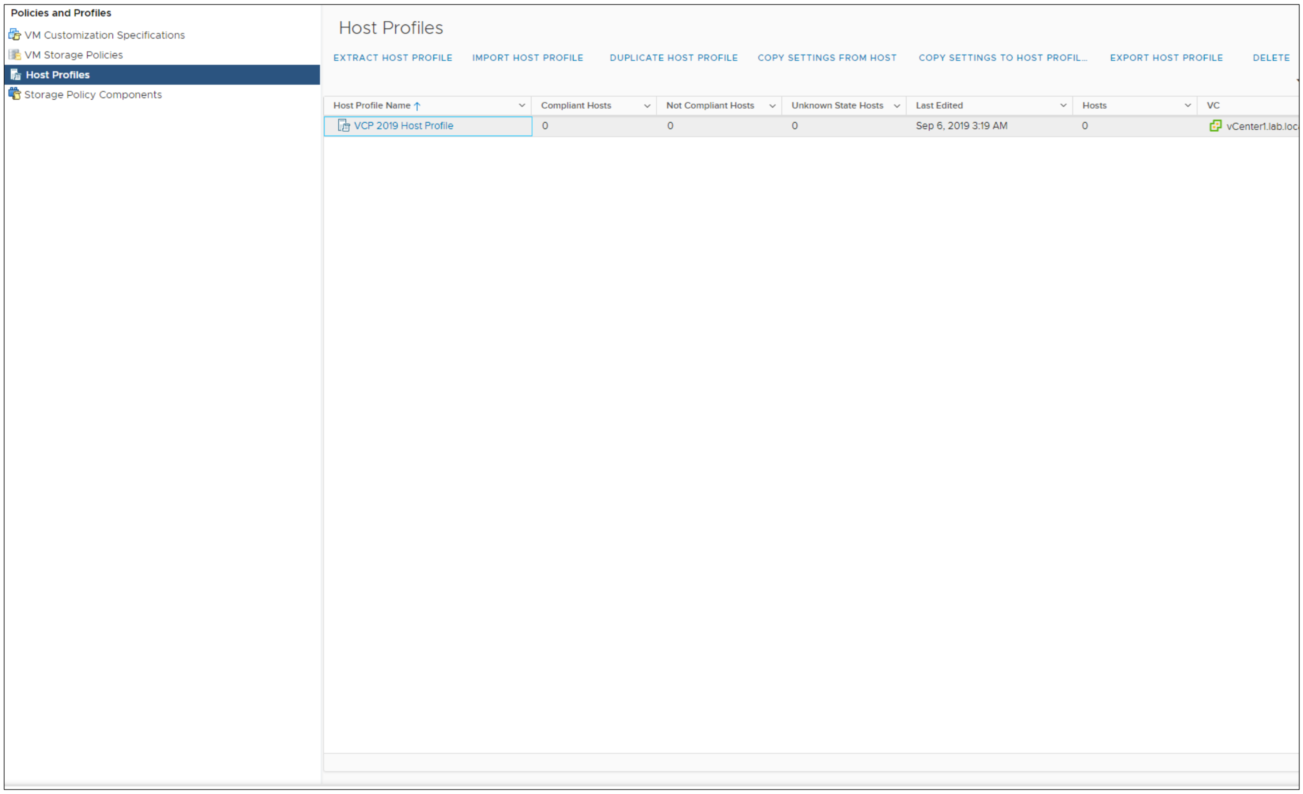
Name and Description

Enter the name and description for the selected profile settings

Name: VCP 2019 Host Profile

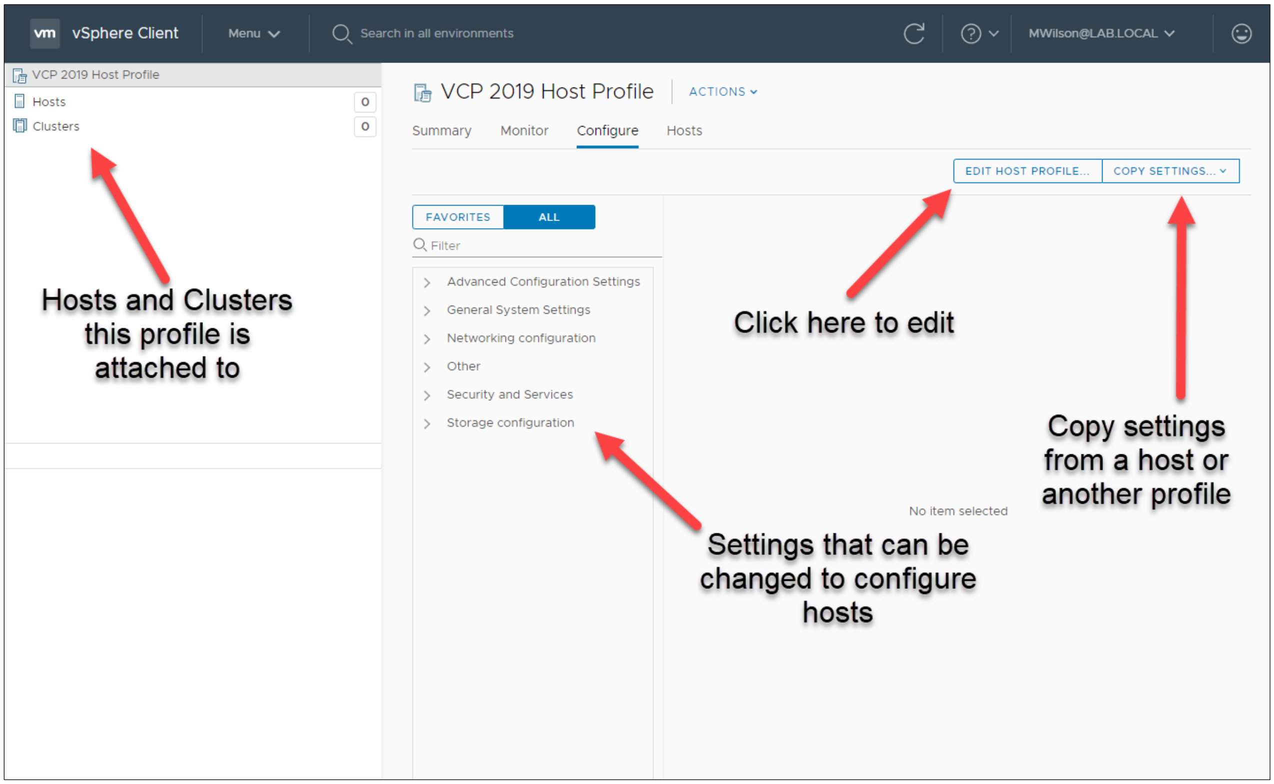
Description:

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



| 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, its 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.



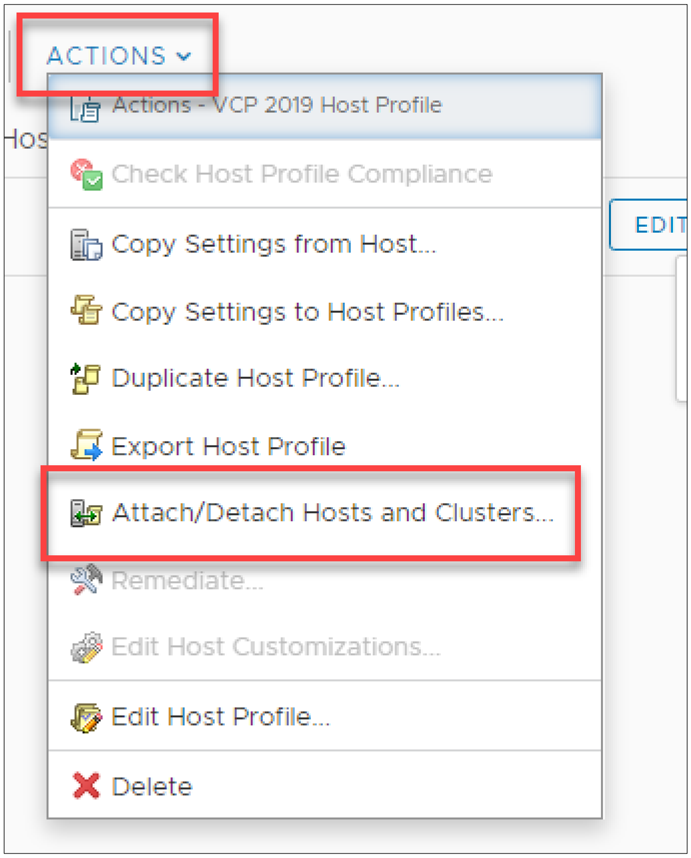
Hosts and Clusters this profile is attached to

Click here to edit

Copy settings from a host or another profile

Settings that can be changed to configure hosts

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


ACTIONS
Actions - VCP 2019 Host Profile
Hos
Check Host Profile Compliance
EDIT
Copy Settings from Host...
Copy Settings to Host Profiles...
Duplicate Host Profile...
Export Host Profile
Attach/Detach Hosts and Clusters...
Remediate...
Edit Host Customizations...
Edit Host Profile...
Delete

# Conclusion

So that is the end of this study guide. If you find something incorrect in it or I didn't understand the Blueprint from VMware, let me know. I appreciate you taking the time to read through and hope you were able to use it. I really appreciate the community and all the things its done for me, which is why I love doing things like this. Thanks!!

Mike Wilson (IT-Muscle.com / @IT_Muscle )