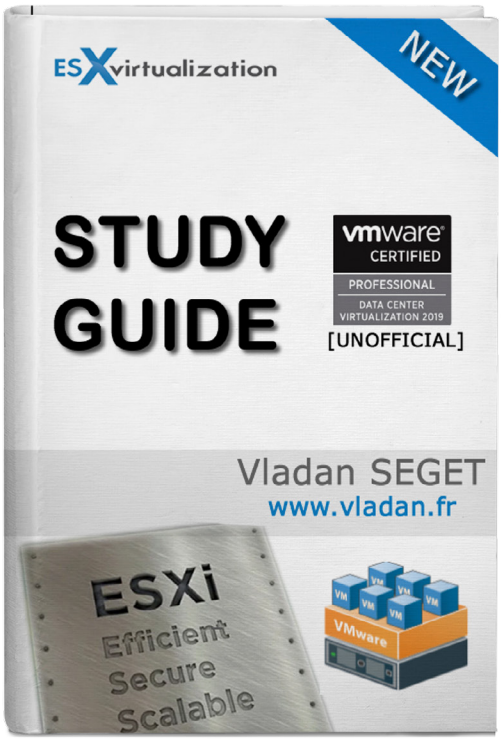
VCP-DCV 2019 Certification



[UNOFFICIAL]

By Vladan SEGET
www.vladan.fr

The VCP-DCV 2019 certification will be based on **2V0-21.19 exam number** and it will have 70 questions with a duration of 115 minutes. The passing score is 300. There is nothing really new to expect for those familiar with VMware certification process.

In order to become **VCP-DCV 2019 certified** and pass the Professional vSphere 6.7 exam, we follow the guidelines from the VMware Exam blueprint **2V0-21.19**.

The Professional vSphere 6.7 Exam 2019 (2V0-21.19) which leads to VMware Certified Professional – Data Center Virtualization 2019 (VCP-DCV 2019) certification is a 70-item exam, with a passing score of 300 using a scaled scoring method. Candidates are given 115 minutes to complete the exam.

NAKIVO Backup & Replication v9

#1 Solution for Backup and Site Recovery
of Physical, Virtual, and Cloud Workloads

Best of VMworld 2018
Gold Award for Data Protection

Single pane of glass for backup, replication, instant granular restore, and site recovery

Policy-based data protection for simplified and automated management

Can be installed on a NAS to create a high-performance backup appliance

Pricing starts from just $99 per socket or $17 machine/year

Leading brands trust NAKIVO

Coca-Cola · DHL · The University of Arizona · Honda · Verifone · China Airlines · Radisson Hotels & Resorts · ScienceLogic · FUJIFILM

Contents

The VMware Datacenter exam has become more and more difficult to master since the volume of knowledge required is higher, but I'm very confident that many of you will succeed.

And if you don't pass on your first try, don't get discouraged—you can see this as a learning experience that will help you be successful the second time.

This happened to me awhile back when taking my VCAPs (both passed the second time), and it was a lesson of humility. It took a while to prepare and learn, too.

VCP6.7-DCV Study Guide – VCP-DCV 2019 Certification

Objective 1.1- Identify the prerequisites and components needed for vSphere implementation

Since there are no special guidelines and sub-chapters like in the VCP6.5-DCV Study Guide, we basically cover what we think is important for that chapter. However, you should not rely solely on our information.

VMware vSphere is a software suite which allows you to manage and implement virtual infrastructure. The base components which run in vSphere are **ESXi hosts** and a **vCenter server(s)**. Other than that, you'll need some switches and storage to connect all these parts together.

Quote from VMware:

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform on which you can create and run virtual machines and virtual appliances. vCenter Server is a service that acts as a central administrator for ESXi hosts connected in a network. vCenter Server lets you pool and manages the resources of multiple hosts.

You'll need to meet a certain number of hardware requirements in order to successfully install ESXi.

To install or upgrade ESXi, your hardware and system resources must meet the following requirements:

- Supported server platform. For a list of supported platforms, see the VMware Compatibility Guide
- ESXi 6.7 requires a host machine with at least two CPU cores.
- ESXi 6.7 supports 64-bit x86 processors released after September 2006. This includes a broad range of multi-core processors. For a complete list of supported processors, see the VMware compatibility guide at http://www.vmware.com/resources/compatibility.

- ESXi 6.7 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi 6.7 requires a minimum of 4 GB of physical RAM. It is recommended that you provide at least 8 GB of RAM to run virtual machines in typical production environments.
- To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs.
- One or more Gigabit or faster Ethernet controllers. For a list of supported network adapter models, see the VMware Compatibility Guide
- SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers. SATA disks are considered remote, not local. These disks are not used as a scratch partition by default because they are seen as remote.

Installing ESXi 6.7 or upgrading to ESXi 6.7 requires a boot device that is a minimum of 1 GB. When booting from a local disk, SAN or iSCSI LUN, a 5.2-GB disk is required to allow for the creation of the VMFS volume and a 4-GB scratch partition on the boot device.

Here are some posts which might help:

- Top 3 Free Tools to Create ESXi 6.7 Installer USB Flash Drive
- Objective 4.4 - Set up ESXi hosts

If your infrastructure is partly virtualized, you can use the VMware converter tool to convert physical systems to virtual machines. The conversion can be “hot” or “cold.” You can either install the converter software on your management workstation and launch the conversion of powered Off VMs, or you can install VMware converter on the physical system and launch a “hot” conversion to the destination.

You must specify as a destination the ESXi or vCenter server with different options for disk layout, network adapters, services and other components. Make sure to uninstall any software which is tightened to the physical system as such (monitoring, agents, etc.).

VMware vCenter Server - vCenter Server can still be installed on Windows in this release, but this is the latest one. Make sure to familiarize yourself with VMware vCenter Server Appliance (VCSA) which is now the preferred way to run a vCenter server.

With the release of vSphere 6.7 U1, vCenter Server on Windows is enacting its last version. **In the next major release, there will be only VMware VCSA to manage vSphere**. VMware vCSA is Linux distribution based on Photon OS. For those of you who do not follow VMware at all and are only familiar with ESXi, we can state that yes, VCSA is a management VM for ESXi hosts.

In order to understand vSphere management, a while back, we submitted a simple article which explains What is The Difference between VMware vSphere, ESXi and vCenter. The posts explain the basics of VMware vSphere, which is basically a commercial name for the whole VMware Suite. Again, this is a really basic, simple explanation to people who do not have experience dealing with VMware.

VCSA Requirements (depends on the choice):

- Tiny (up to 10 hosts or 100 VMs) – 2 vCPU, 10Gb Memory, 250 GB storage
- Small (up to 100 hosts or 1000 VMs) – 4 vCPU, 16 GB Memory, 290 GB storage
- Medium (up to 400 hosts or 4000 VMs) – 8 vCPU, 24 GB RAM, 425 GB storage
- Large (up to 1000 hosts or 10000 VMs) – 16 vCPU, 32 GB RAM, 640 GB storage
- X-Large (up to 2000 hosts or 35000 VMs) – 24 vCPU, 48 Gb RAM, 980 GB storage

vCenter on Windows requirements - CPU and storage possess the same requirements. Consider joining the VM to Microsoft Domain in case you would like to use AD as an identity source. While you can use a domain admin account for full access, you might also consider creating a vSphere admin account in AD. You'll need to make this user to if you would like to:

- Be a local administrator
- Log on as service right
- Act as part of OS

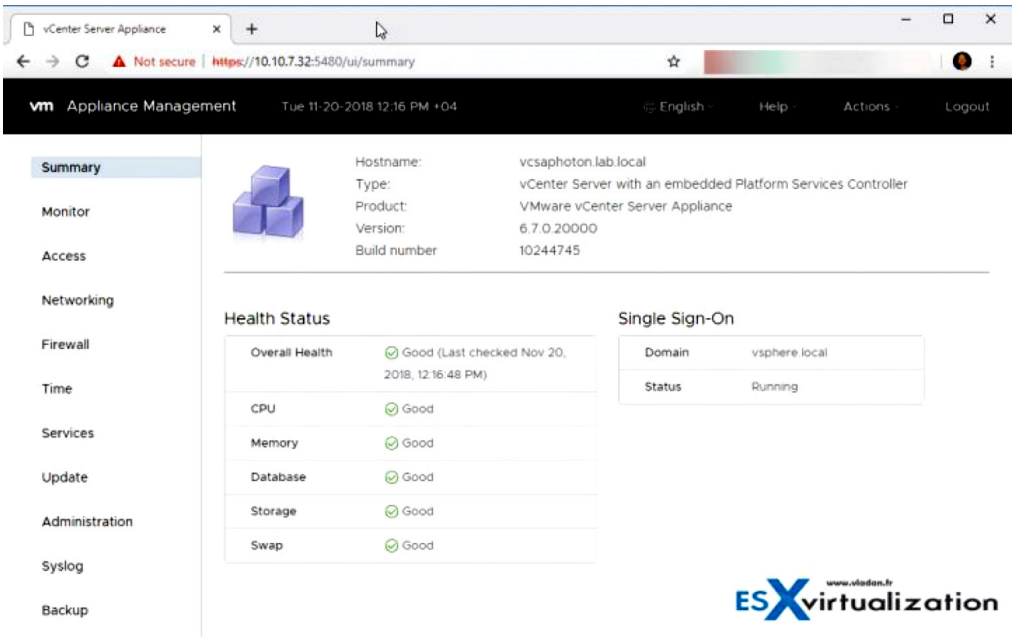
The machine should NOT be a domain controller (installation refused). The DNS resolution should be working.

DB requirements: the PostgreSQL DB bundled is fine for small installations (up to 20 host or 200 VMs). Other than that, you'll need Microsoft SQL or Oracle.

The VMware vCenter 6.7 Appliance Management Page - The VCSA appliance runs Linux Photon OS and is manageable via a web-based interface. The management page is where you set up (change) the root password, change the time zone, networking settings, configure a file backup and get an insight of how this appliance performs in terms of network, CPU, storage, etc. The latest version also has the possibility for checking that the different VMDK disks aren't filling up too much (there is a new built-in view in there).

To connect to this web-based UI, you can use your web browser to connect to a page where the 5480 is the default management port. You'll need the root user account and password which has been assigned during the installation of the appliance. Here is the connection URL.

VMware Appliance Management (https://x.x.x.x:5480)

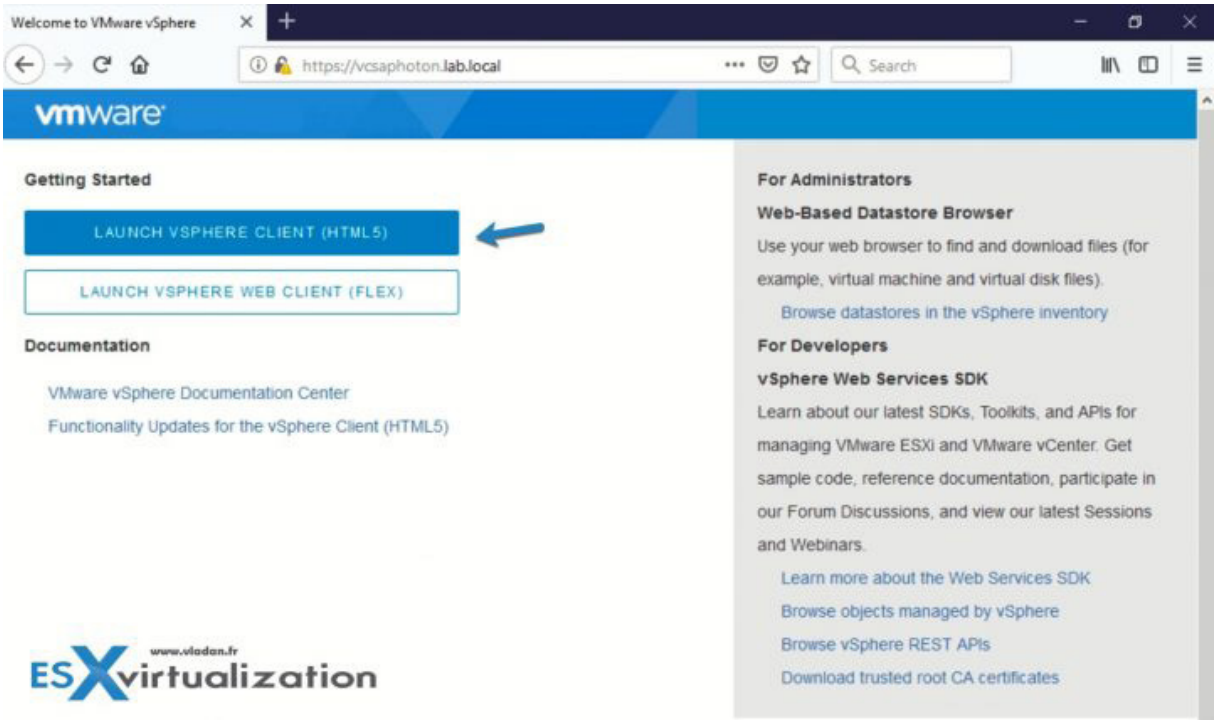


You also have the possibility, if VMware support asks you to do so, to generate and send a support bundle. You can do that via the **Actions** menu.

The vSphere management has another access URL. Also, you no longer need to purchase any software as vSphere Legacy Windows client no longer exists on vSphere 6.7. The only URL you need to know for the connection is this URL:

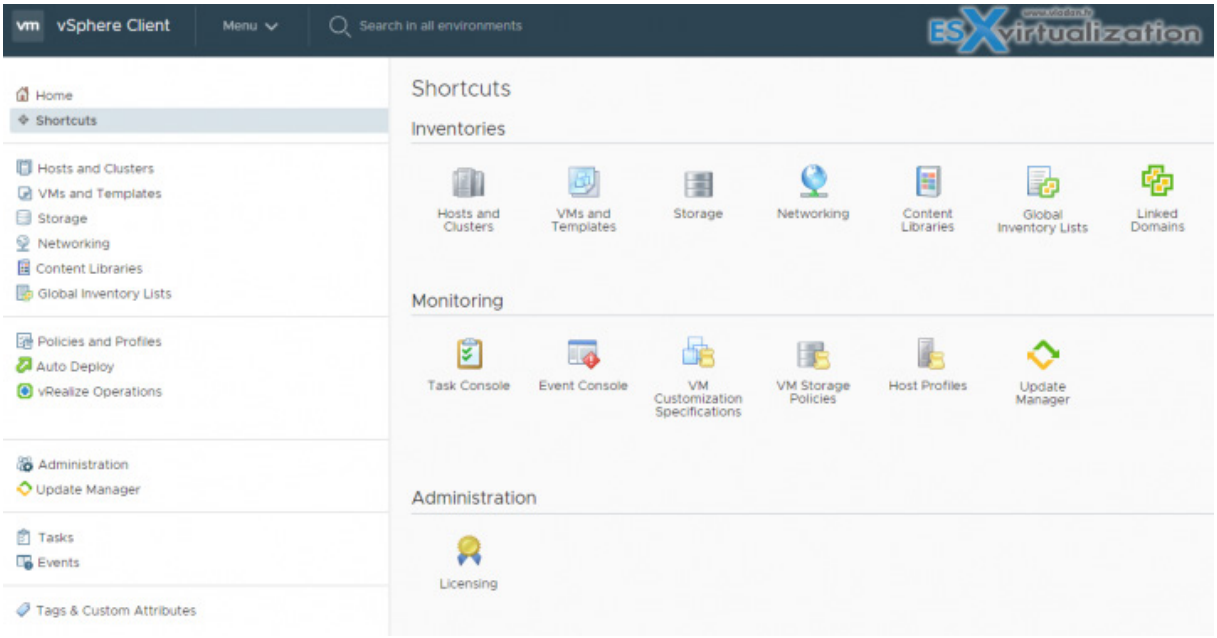
https://IP_or_FQDN_VCSA/

Overview of the web-based access for vCenter Server Appliance for VMware vSphere.



As you can see, you can still use the legacy FLEX client where you'll need to install Adobe Flash plugin as an add-on to your browser. The HTML 5 web client does not need any plugins installed. The vSphere 6.7 Update 1 has feature parity (or even more) now.

So, after connection via the HTML 5 web client, you'll end up on this page where you have all the icons and shortcuts you need to manage your vSphere infrastructure.



Part of the VCSA is also an Update Manager which is the VMware preferred method of patching and upgrading the whole infrastructure.

vCenter and Platform Services controller (PSC)

The VCSA is running **Photon OS** which is a VMware-owned lightweight distribution channel, optimized for fast booting, security, and scalability. For a number of years, VMware was using Suse Linux Enterprise Server (SLES) distribution, but the fact that VMware did not own the stack greatly incentivized its faster development.

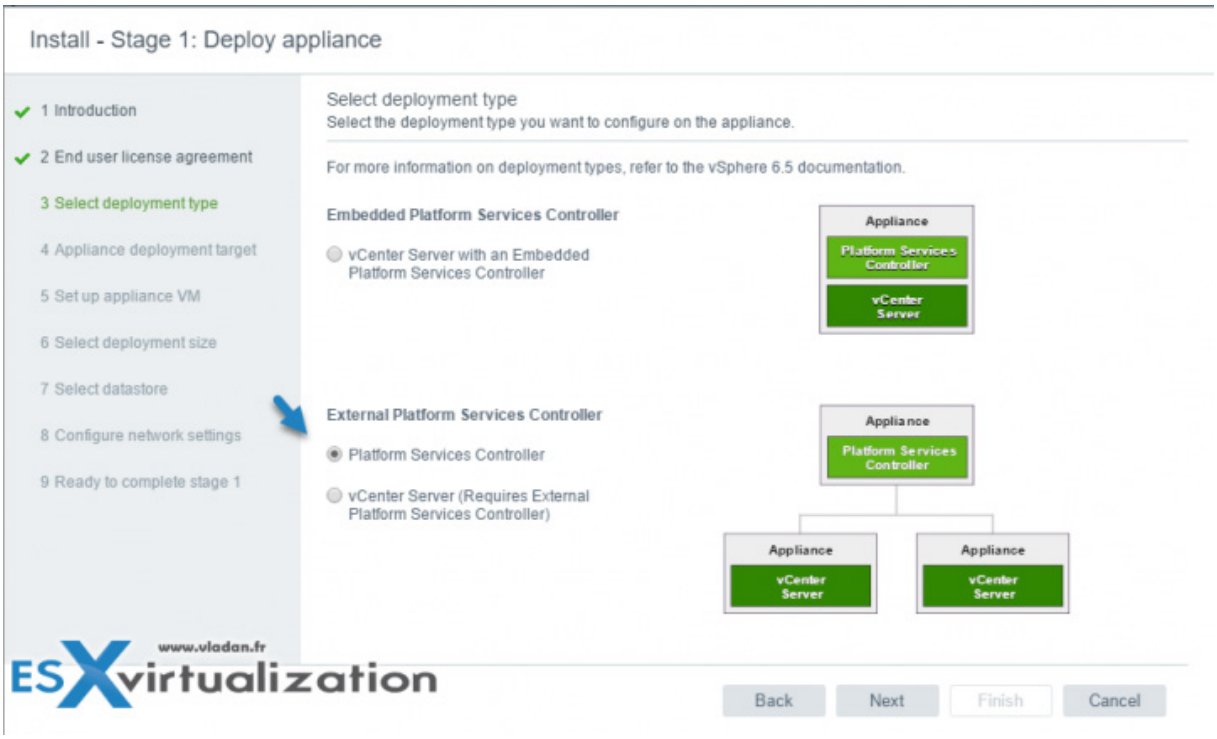
During deployment of the appliance, you select a deployment type of vCenter Server with an embedded Platform Services Controller (PSC), Platform Services Controller, or vCenter Server with an external PSC. When you deploy a PSC appliance, you can create a VMware vCenter Single Sign-On domain or join an existing domain.

VMware PSC is not new. It was a part of vSphere 6.0 where it assured a number of services already. These services include:

- VMware Appliance Management Service
- VMware License Service
- VMware Component Manager

- VMware Identity Management Service
- VMware HTTP Reverse Proxy
- VMware Service Control Agent
- VMware Security Token Service
- VMware Common Logging Service
- VMware Syslog Health Service
- VMware Authentication Framework
- VMware Certificate Service
- VMware Directory Service.

VMware PSC, when deployed separately in a separate VM, deploys only the services bundled with the PSC, not the vCenter specific services. There are different topologies which exists and have their own advantages and disadvantages, but for 6.7 and 6.7U1, the preferred way is embedded vCenter and PSC.



Within a PSC you can:

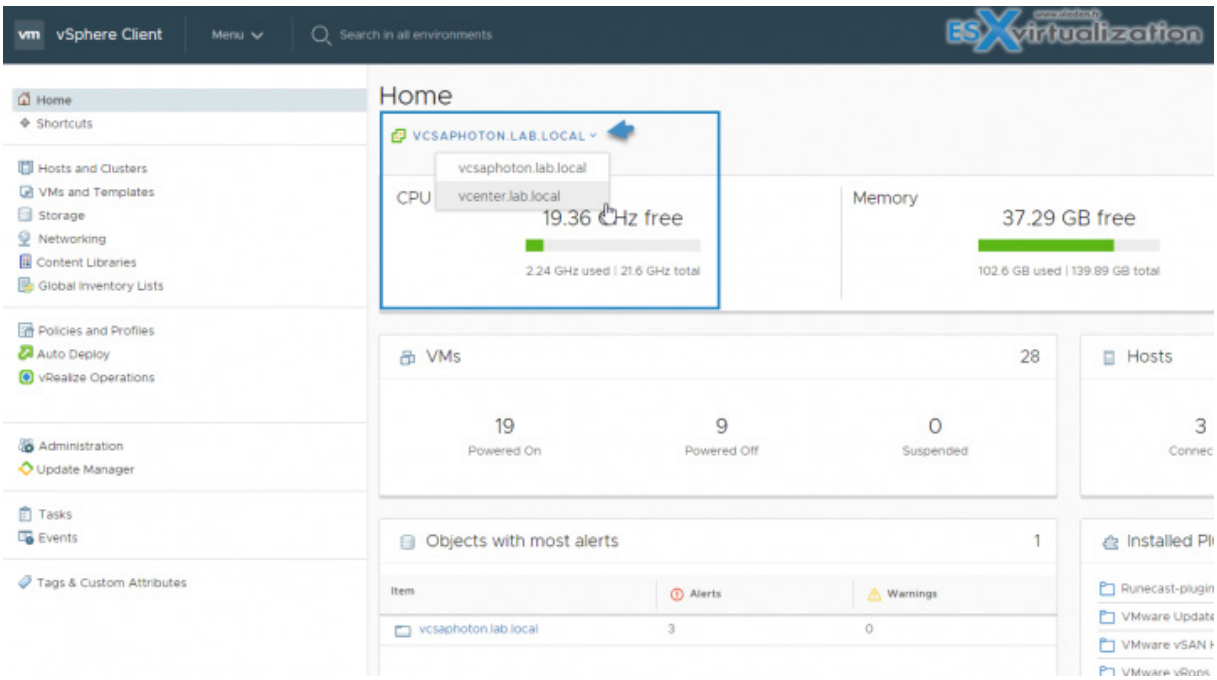
- Add and Edit Users and Groups for Single Sign-On
- Add Single Sign-On Identity Sources
- Configure Single Sign-On Policies (for example Password Policies)
- Add Certificate Stores
- Add and Revoke Certificates

PSC allows for:

- Authentication via vCenter Single Sign-On (SSO)
- Provision ESXi hosts with VMware Certificate manager (VMCA) certificates by default
- Use of custom certificates stored in VMware Endpoint Certificate store (VECS).

While you can still deploy external PSC, the question is, is it worth it? Embedded PSC now fully supports **Enhanced Linked Mode (ELM)**. Previous releases vSphere 6.0 and 6.5 needed external PSC to support ELM. Now, this is no longer the case.

For vSphere 6.5 Update 2 and vSphere 6.7 finally, the embedded deployment is fully supported.



I don't think that you'll need to know all of the information below, but I've included it to give you an idea of the importance of PSC and all the services it runs.

Platform Service Controller (PSC) services:

- **VMware Appliance Management Service** – (applmgmt) – appliance configuration and provides public API endpoints for appliance lifecycle management. It is included on the Platform Services Controller appliance.
- **VMware License Service** – (vmware-cis-license) -Each PSC includes a VMware License Service, which manages and delivers centralized licenses and has a reporting functionality to VMware products in your environment. The license service inventory replicates across all Platform Services Controller in the domain at 30-second intervals.
- **VMware Component Manager** – (vmware-cm) – offers service registration and lookup.
- **VMware PSC client** – (vmware-psc-client) – is the back end to the PSC web UI.
- **VMware Identity Management service** – (vmware-sts-idmd) – services needed for vCenter SSO, for authentication to VMware software components and users.

- **VMware Security Token Service** – (vmware-stsd) – SAML token exchange mechanism.
- **VMware HTTP Reverse proxy –** (vmware-rhttpproxy) – this proxy runs on every PSC and in each vCenter Server. It is an entry point into the node. Allows for secure communication between services running on the node.
- **VMware Service Control Agent** – (vmware-sca) – Manages service configurations. You can use the service-control CLI to manage individual service configurations.
- **VMware Appliance Monitoring Service** – (vmware-statsmonitor) – monitors vCSA Guest OS system resources utilization and performance.
- **VMware vAPI Endpoint** – (vmware-vapi-endpoint) – single point of access to vAAPI services
- **VMware Authentication Framework** – (vmafdd) – services for a client-side framework for vmdir authentication and serves the VMware Endpoint Certificate Store (VECS).
- **VMware Certificate Service** – (vmcad) – uses the VMware Endpoint Certificate Store (VECS) to serve as a local repository for certificates on every Platform Services Controller instance. **Although you can decide not to use VMCA and instead can use custom certificates, you must add the certificates to VECS.**
- **VMware Directory Service** – (vmdir) – multitenant, multimastered LDAP directory service that stores authentication, certificate, lookup, and license information.
- **VMware Lifecycle Manager API** – (vmonapi) – start and stop vCenter server services and monitor service API health.
- **VMware Service Lifecycle Manager** – (vmware-vmon) – is a centralized platform-independent service that manages the lifecycle of PSC and vCenter servers.
- **Likewise Service Manager** – (lwsmd) – enables you to join the host to a Microsoft Active Directory domain and then authenticate users through AD.
- **VMware Platform Services Controller Health Monitor** - (pschealth) - Monitors the health and status of all core Platform Services Controller infrastructure services.
- **VMware Analytics Service** (vmware-analytics) - Consists of components that gather and upload telemetry data from various vSphere components to the VMware Analytics Cloud, managing the Customer Experience Improvement Program (CEIP).

We're not sure if we've covered absolutely everything you need to know, but have included this chapter as a guideline. Your principal study material should be the Documentation Set PDF, as well as your home lab or day-to-day work with infrastructure.

Objective 1.2 - Identify vCenter high availability (HA) requirements

Today's objective to cover is Objective 1.2 – Identify vCenter high availability (HA) requirements, which is one of the core VMware vSphere functionalities.

Again, read the docs on your own, as we won't be able to cover everything – make sure to read the PDFs in particular. The VMware Exam blueprint has 41 chapters (Objectives). VCP-DCV 2019 certification is the latest certification based on vSphere 6.7.

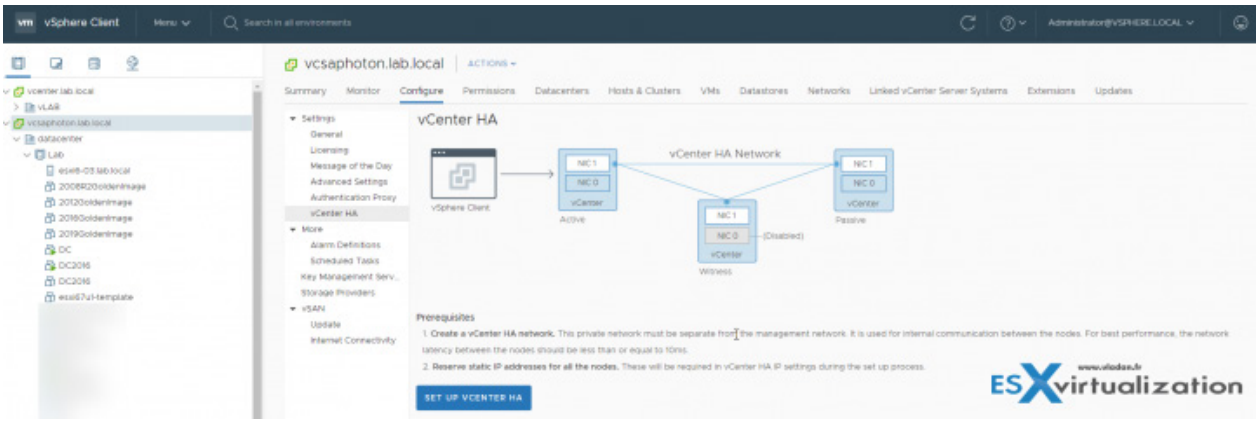
If you're new to this blog, it's worth knowing that VMware has changed the rules of re-certification recently. Our Post: VMware Certification Changes in 2019 has the details. No mandatory recertification required after 2 years. Older certification holders (up to VCP5) can pass the new exam without a mandatory course, as only recommended courses are listed).

vCenter HA for vCenter server appliance (VCSA) is the in-house VMware solution. vCenter HA for vCenter on Windows can be achieved with Microsoft failover clustering.

What about VCSA HA with embedded Platform Service Controller (PSC) or external PSC? If you are using external PSC, you can put the PSC behind load balancer and protect against failures.

A vCenter HA cluster consists of three vCenter Server Appliance instances. The first instance, initially used as the **Active node**, is cloned twice to a **Passive node** and to a **Witness node**. Together, the three nodes provide an active-passive failover solution.

Overview of how it works.



VCSA HA allows for maintaining a standby copy of the VCSA which is ready to be powered on when the primary appliance becomes unavailable. Up to date data is replicated between the active and passive nodes.

However, you'll need at least 3 hosts in your environment, managed by a vCenter server, to spread the different nodes. Remember that we have Passive VCSA as well as Witness nodes which must run on a separate ESXi host.

When vCenter HA configuration is complete, only the Active node has an active management interface (public IP). The three nodes communicate over a private network called vCenter HA network that is set up as part of the configuration.

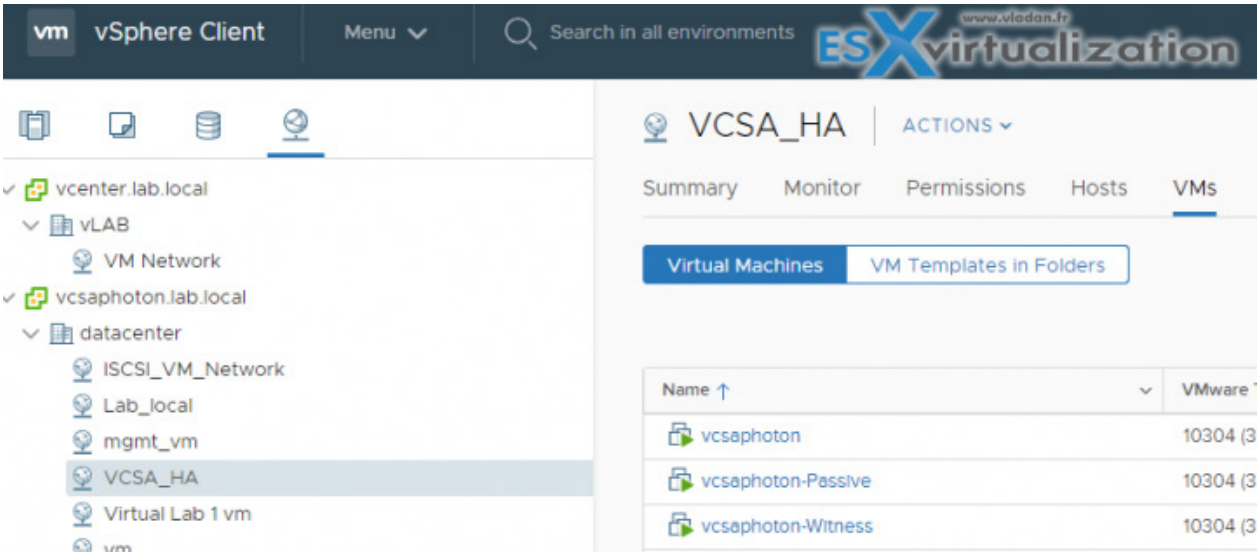
Hardware and Software Requirements:

- VMware recommends that the VCHA nodes are deployed to a DRS enabled cluster containing at minimum three ESXi hosts.
- vCenter HA was introduced with the vCenter Server Appliance 6.5, but now with 6.7, U1 the process has been even more simplified.
- The vCenter deployment size should be 4 vCPU 16 GB RAM.
- A minimum of three hosts, running at least ESXi 5.5.
- The management network should be configured with a static IP address and reachable FQDN.
- The ESXi hosts must have 2 Networks (Port Groups) attached either to a Standard or a Distributed Switch.
- The HA network must be on a **different subnet** to the management network.
- A private network or VLAN that is dedicated to vCenter HA network traffic.
- Three private static IP's for vCenter HA network traffic.
- Network latency between the nodes less than 10ms.
- vCenter HA is compatible with both embedded deployment model and external PSC.

If there is an outage to the active vCenter server VM, the passive vCenter VM automatically takes over the active role and identity, including networking.

This feature is only available for VCSA, not for vCenter On Windows.

Before starting the workflow, make sure that you create a new VM network which is on a different subnet or different VLAN than the management network. In my case, I have created a new VM network called VCSA_HA.

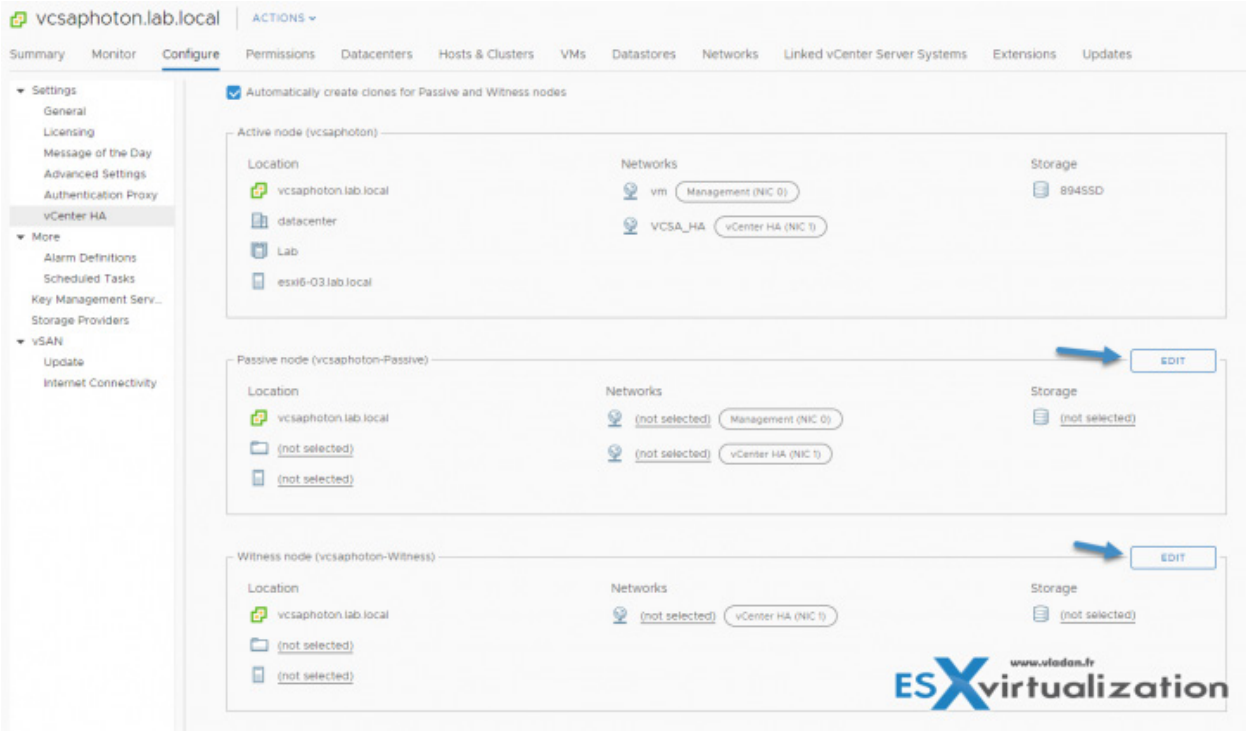


Now, let's start by **selecting vCenter > Configure > vCenter HA > SET UP VCENTER HA.**

vCenter High Availability (vCenter HA) protects not only against host and hardware failures, but also against vCenter Server application failures. Using automated failover from active to passive, vCenter HA supports high availability with minimal downtime.

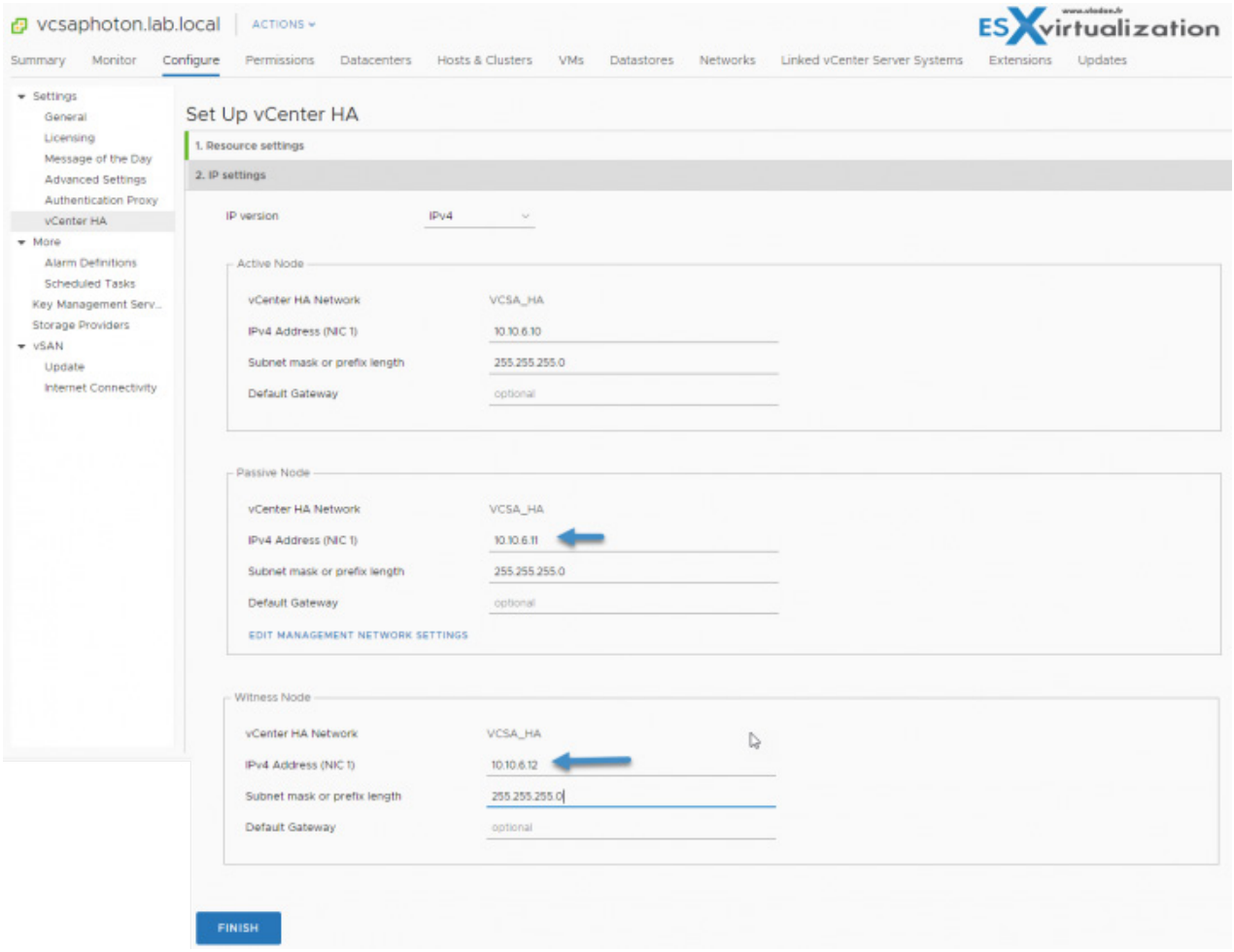
For maximum protection, place the nodes on separate hosts and datastores. If the nodes are placed on the same compute cluster that has DRS and/or SDRS enabled in automatic mode, anti-affinity rules are automatically created to keep the nodes separate. For best performance, the network latency between the nodes should be less than or equal to 10 ms.

The wizard is greatly simplified when you have the checkbox “Automatically create clones for Passive and witness nodes” checked.



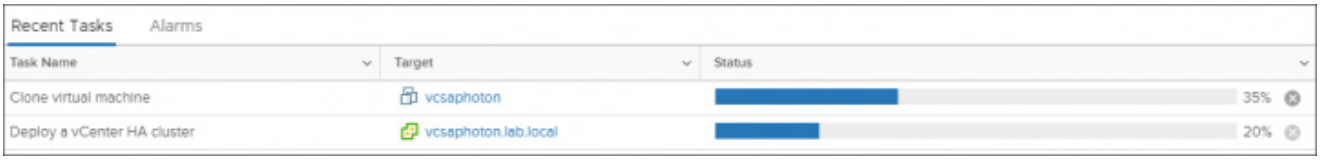
Go ahead and select the location, networking, and storage of the Passive and the Witness nodes…

Then on step 2, set the IP network for the **Passive** and **Witness** nodes. On the next page, we’ll see the networking option. You must be on a different subnet, remember. If not, the wizard will fail at the end.



Scroll down the vCenter HA resource settings, review the network and resource settings of the active node of the vCenter Server.

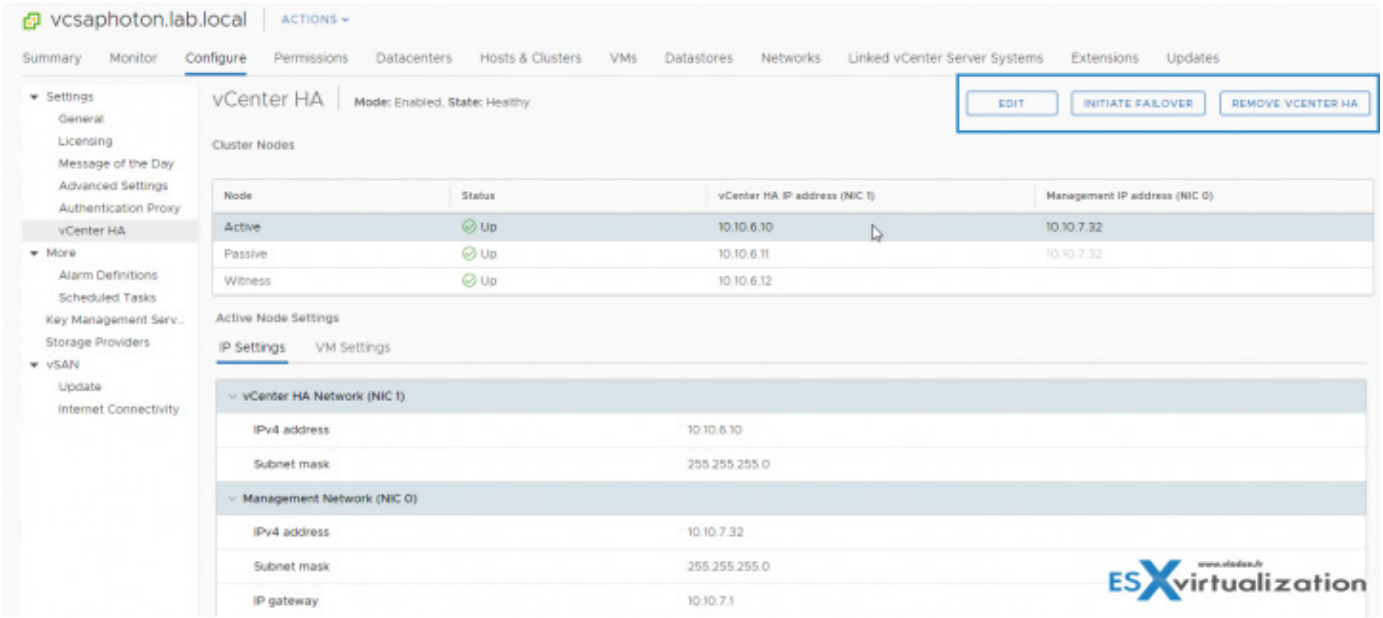
The system will automatically clone the VCSA. It takes some time depending on the performance of your infrastructure and the underlying storage. You can click the Recent tasks link to follow up on the cloning process and wait until all three nodes are up.



After roughly 10 minutes of waiting, in the end, you should see all the nodes with green checkboxes. VCSA HA is great, however, you should know that the passive and witness nodes keep running, and so continue to consume resources such as CPU and storage.

So, if you're in a really small environment, do not use this method, but rather take a regular backup with your backup software or set up a file-level backup only.

And the view of vCSA HA has now the nodes and their status with networking details...



As you can see, the configuration is pretty straightforward.

Objective 1.3 - Describe storage types for vSphere

The topic for today is called “Describe storage types for vSphere”. A very large topic, indeed, and we’ll try to stick to it. However, we don’t really have any sub-chapter guidance on what exactly VMware wants us to cover.

Follow the documentation, use your experience, study elsewhere—we’re not the only blog around. Also, the VCP6.5-DCV study guide is a good source of help as the objectives covered were guided by sub-chapters and as such the topics might be more accurately targeted.

This does not mean that the guide we’re working on is not good... -:). We’re simply saying that it is always advantageous to study from multiple sources (documentations, study guides, blogs).

Local and Networked storage - while local storage is pretty obvious (direct attached disks or DAS), networked storage can be different types, but most importantly, can be shared and accessed by multiple hosts simultaneously. VMware supports virtualized shared storage, such as VSAN. VSAN transforms internal storage resources of your ESXi hosts into shared storage.

Fiber Channel (FC) storage - FC SAN is a specialized high-speed network that connects your hosts to high-performance storage devices. The network uses Fiber Channel protocol to transport SCSI traffic from virtual machines to the FC SAN devices. The host should have Fiber Channel host bus adapters (HBAs).

Internet SCSI (iSCSI) storage - Stores virtual machine files on remote iSCSI storage devices. iSCSI packages SCSI storage traffic into the TCP/IP protocol, so that it can travel through standard TCP/IP networks instead of the specialized FC network. With an iSCSI connection, your host serves as the initiator that communicates with a target, located in remote iSCSI storage systems.

Storage Device or LUN - the terms device and LUN are used interchangeably. Typically, both terms mean a storage volume that is presented to the host from a block storage system and is available for formatting.

ESXi offers the following types of iSCSI connections:

- **Hardware iSCSI** - Your host connects to storage through a third-party adapter capable of offloading the iSCSI and network processing. Hardware adapters can be dependent and independent.
- **Software iSCSI** - Your host uses a software-based iSCSI initiator in the VMkernel to connect to storage. With this type of iSCSI connection, your host needs only a standard network adapter for network connectivity. You must configure iSCSI initiators for the host to access and display iSCSI storage devices

Figure 2-3. iSCSI Storage

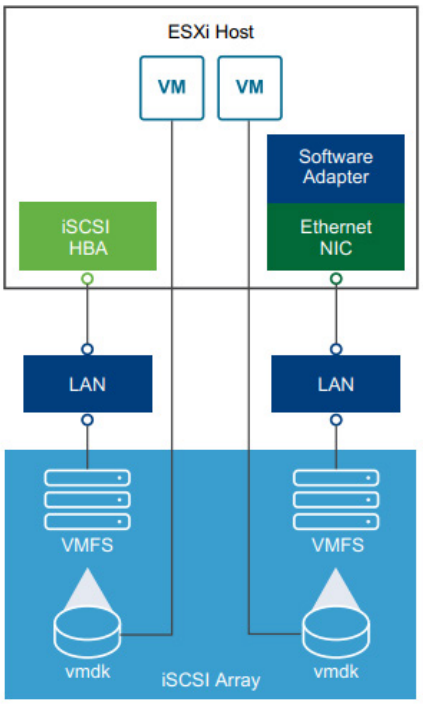
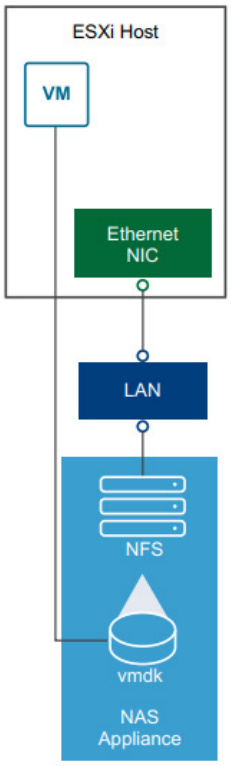


Figure 2-4. NFS Storage



Shared Serial Attached SCSI (SAS) - Stores virtual machines on direct-attached SAS storage systems that offer shared access to multiple hosts. This type of access permits multiple hosts to access the same VMFS datastore on a LUN.

- **VMware Filesystem (VMFS) datastores**: All block-based storage must be first formatted with VMFS to transform a block service to a file and folder-oriented services
- **Network Filesystem (NFS) datastores**: This is for NAS storage
- **VVol**: introduced in vSphere 6.0, it is a new paradigm for accessing SAN and NAS storage in a standardized way by better integrating and consuming storage array capabilities. With Virtual Volumes, an individual virtual machine, not the datastore, becomes a unit of storage management. Storage hardware gains complete control over virtual disk content, layout, and management.
- **VSAN datastore**: If you are using VSAN solution, all your local storage devices can be pooled together in a single shared VSAN datastore. VSAN is a distributed layer of software that runs natively as a part of the hypervisor.
- **Raw device Mapping** - RDM is useful when a guest OS inside a VM requires direct access to a storage device.

VAAI - vSphere API for Array Integration - those APIs include several components. There are Hardware Acceleration APIs which help arrays to integrate with vSphere for offloading certain storage operations to an array. This reduces CPU overhead on a host.

vSphere API for Multipathing - This is known as Pluggable Storage Architecture (PSA), uses APIs which allows storage partners to create and deliver multipathing and load-balancing plugins which are optimized for each array. Plugins communicate to storage arrays and chose the best path selection strategy to increase IO performance and reliability.

Recommended reading: *vSphere Storage PDF*

Recommended reading from VCP6.5-DCV study guide:

- Objective 3.1 Manage vSphere Integration with Physical Storage
- Objective 3.2 Configure Software-Defined Storage
- Objective 3.3 Configure vSphere Storage Multipathing and Failover
- Objective 3.4 Perform VMFS and NFS configurations and upgrades

Objective 1.4 - Differentiate between NIOC and SIOC

Storage I/O Control (SIOC) allows for throttling VMs accessing a datastore which has exceeded a certain latency. Network I/O Control, on the other hand, allows you to reserve network traffic. We'll go into further details how those two technologies work, later in this post.

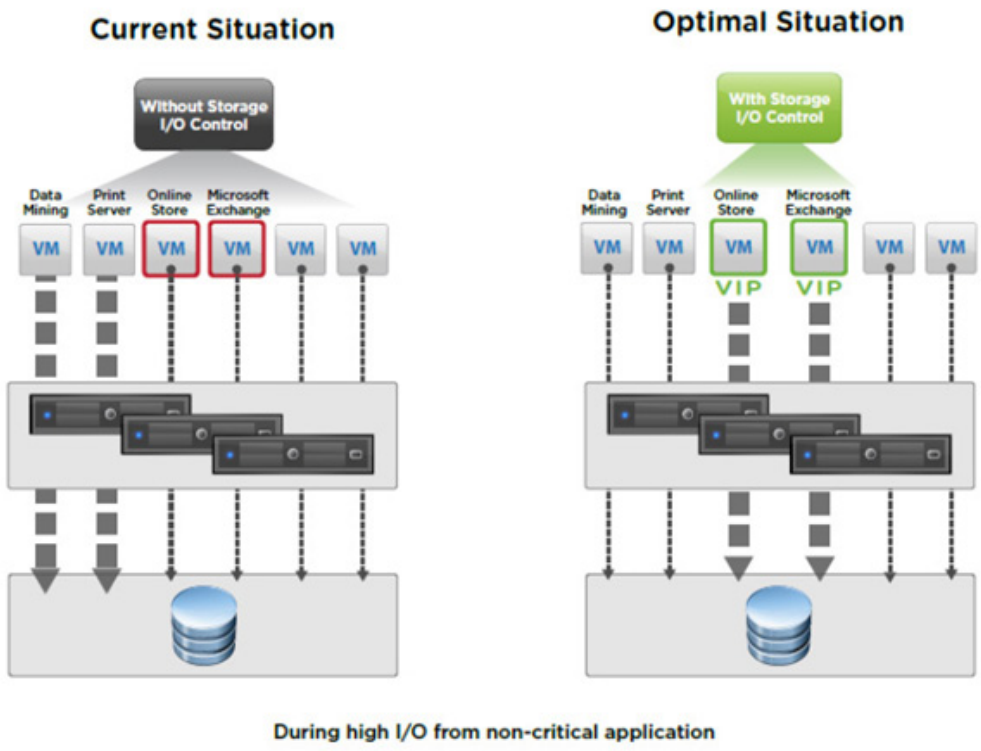
With SIOC enabled on a datastore, you prevent the other VMs from the "**noisy neighbor**" situation where a single VM monopolizes all the resources, as the device's latency is monitored.

If latency is higher than the configured values, SIOC kicks in and reduces the latency by throttling back VMs which are exceeding their consumption of IOPS.

Storage IO Control (SIOC) only kicks in when there is contention. SIOC makes sure that every VM gets its fair share of storage resources. Storage I/O control can “heal” part of your storage performance problems by setting a priority at the VM level (VMDK), avoiding the above-described “noisy neighbor story”.

When you enable Storage I/O Control on a datastore, the ESXi host starts to monitor the device latency that hosts observe when communicating with that datastore. When device latency exceeds a threshold, the datastore is considered to be congested and each VM that accesses such datastore is allocated I/O resources **in proportion to their shares**.

By default, all VMs are set to Normal (1000). You set shares per VMDK, and can adjust the number for each based-on need. The default is 1000.



Quote from VMware:

Storage I/O Control operates as a “datastore-wide disk scheduler.” Once Storage I/O Control has been enabled for a specific datastore, it will monitor that datastore, summing up the disk shares for each of the VMDK files on it. Storage I/O Control will then calculate the I/O slot entitlement per ESXi host based on the percentage of shares virtual machines running on that host have relative to the total shares for all hosts accessing that datastore.

Here are a few limitations and requirements:

- NFS v4.1 isn't supported (it is for NFS v3).
- Storage I/O Control does not support datastores with multiple extents.
- SAN with auto-tiering has to be certified for SIOC.
- Datastores that are Storage I/O Control-enabled must be managed by a single vCenter Server system.
- Must be disabled before removing a datastore.
- Raw Device Mapping (RDM) is not supported. (it is on iSCSI NFS and FC).

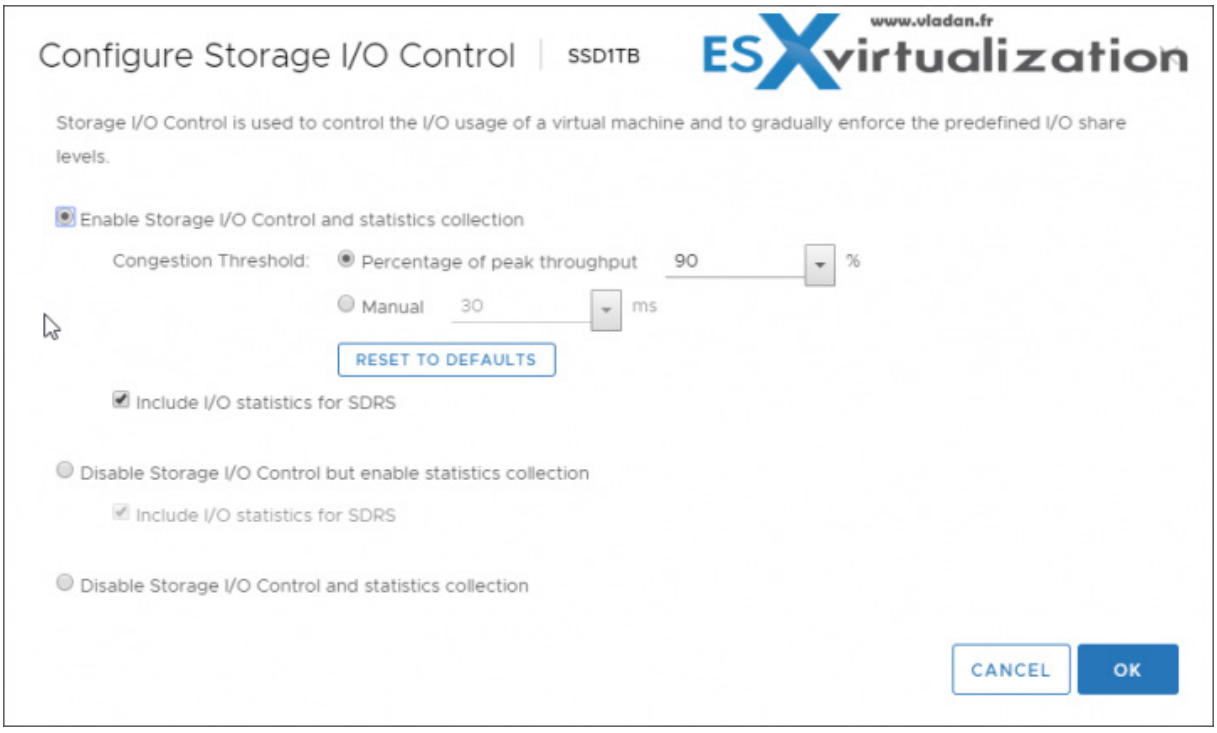
When you enable Storage I/O Control (SIOC) on a datastore, the host starts to monitor the latency. When latency on the datastore with enabled SIOC is more than the configured threshold, vSphere views the data store as "congested" and each VM that is accessing the SIOC enabled datastore is allocated I/O resources in proportion to their shares (that we'll configure on a per VMDK level).

The I/O filter framework (VAIO) allows VMware and its partners to develop filters that intercept I/O for each VMDK and provides the desired functionality at the VMDK granularity.

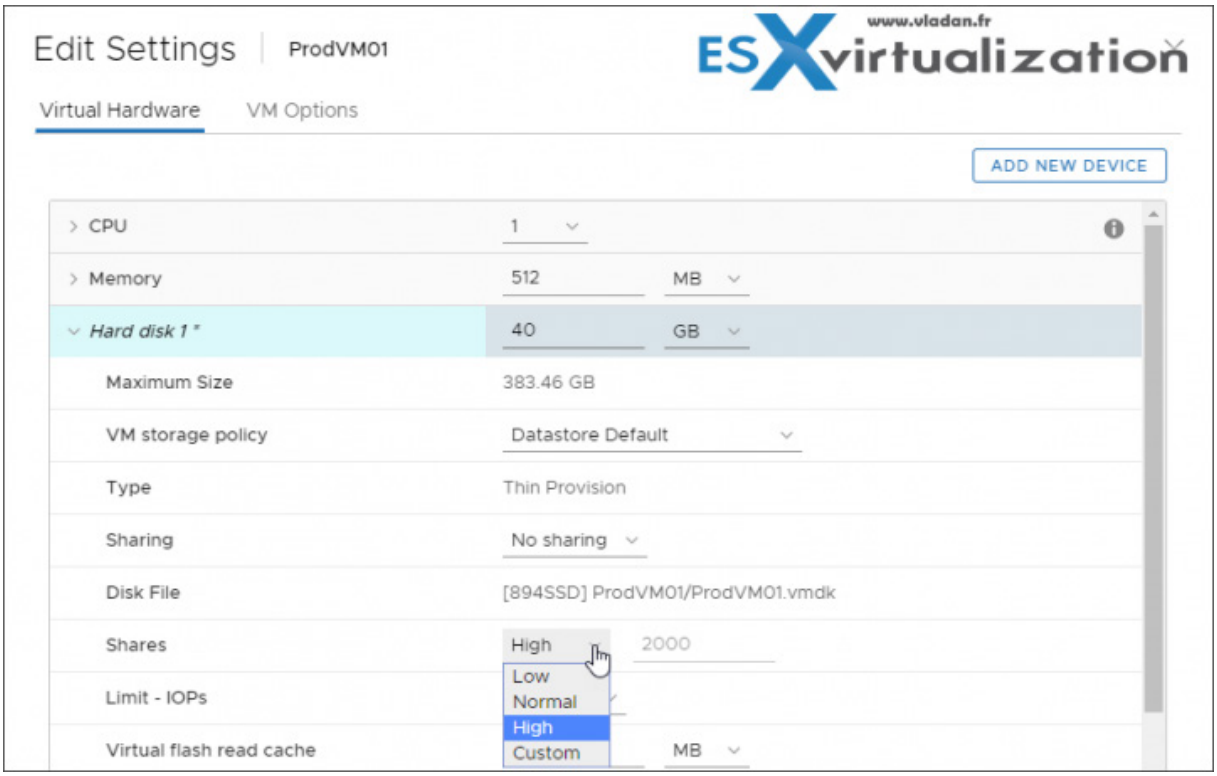
VAIO works along Storage Policy-Based Management (SPBM) which allows you to set the filter preferences through a storage policy that is attached to VMDKs.

Two-step process to activate SIOC:

Step 1. Activate SIOC at the datastore level via vSphere Client or vSphere Web client. Select **Datastore > Configure > General > Storage I/O control** section.



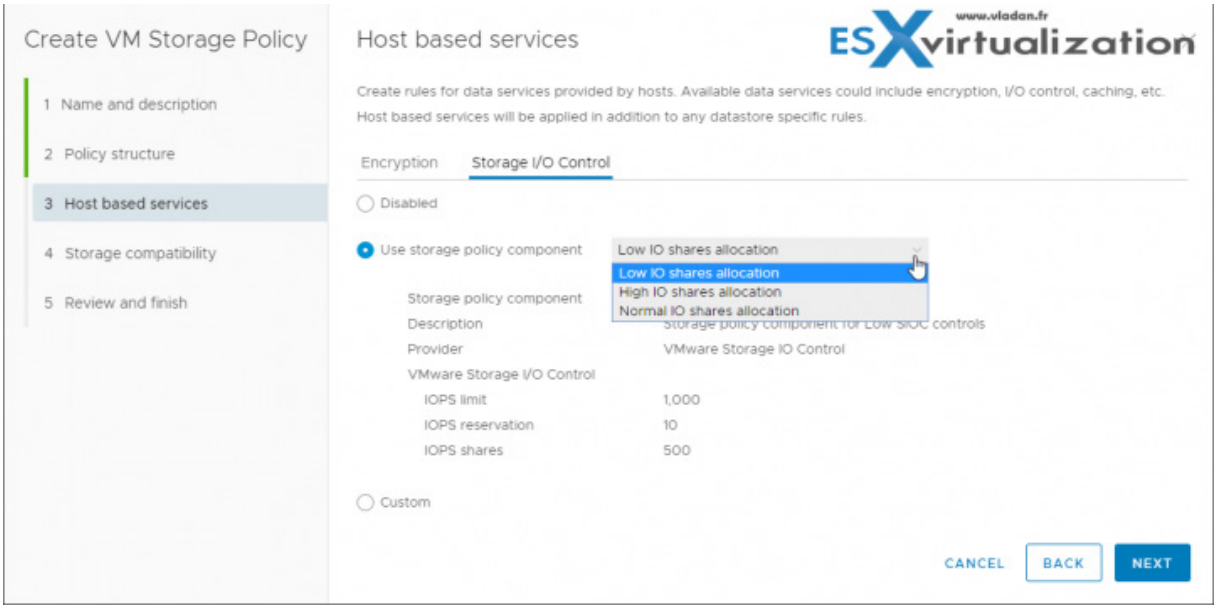
Step 2: Set the number of storage I/O shares and an upper limit of I/O operations per second (IOPS) allowed for each virtual machine. By default, all virtual machine shares are set to Normal (1000) with unlimited IOPS.



VM Storage Policies - takes control of which storage space is provided to the virtual machine, how the VM is placed within the storage space, and which data services are offered for the VM.

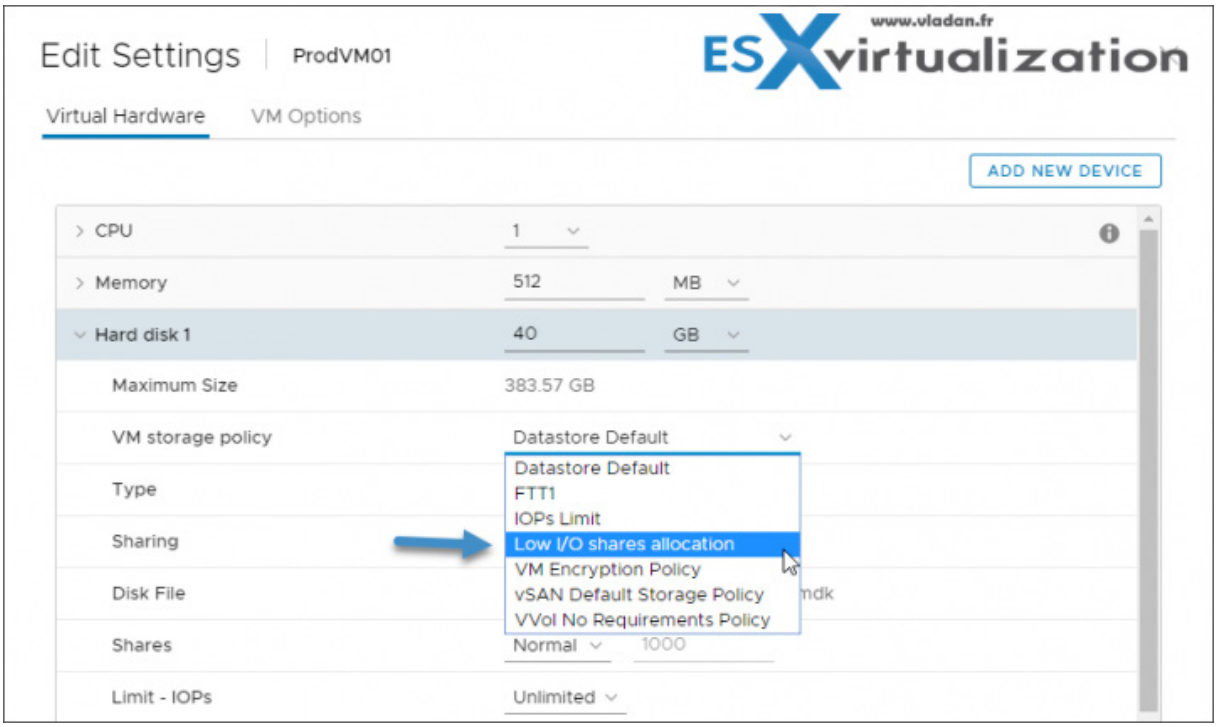
Create a VM storage policy.

Home > Policies and profiles > VM storage policies.



Once done, you can assign this VM storage policy to a virtual machine.

Select VM > Edit Settings > Hard Disk > VM Storage policy



There are few metrics which are important and are available on the datastore performance tab:

- **Average latency and aggregated IOPS** on the datastore
- **Latency** among hosts
- **Queue depth** among hosts
- **RW (Read/write) IOPS** among hosts
- **RW (Read/write) latency** among virtual machine disks
- **RW (Read/write)** IOPS among virtual machine disks

Storage IO Control Requirements

Storage I/O Control has several requirements and limitations.

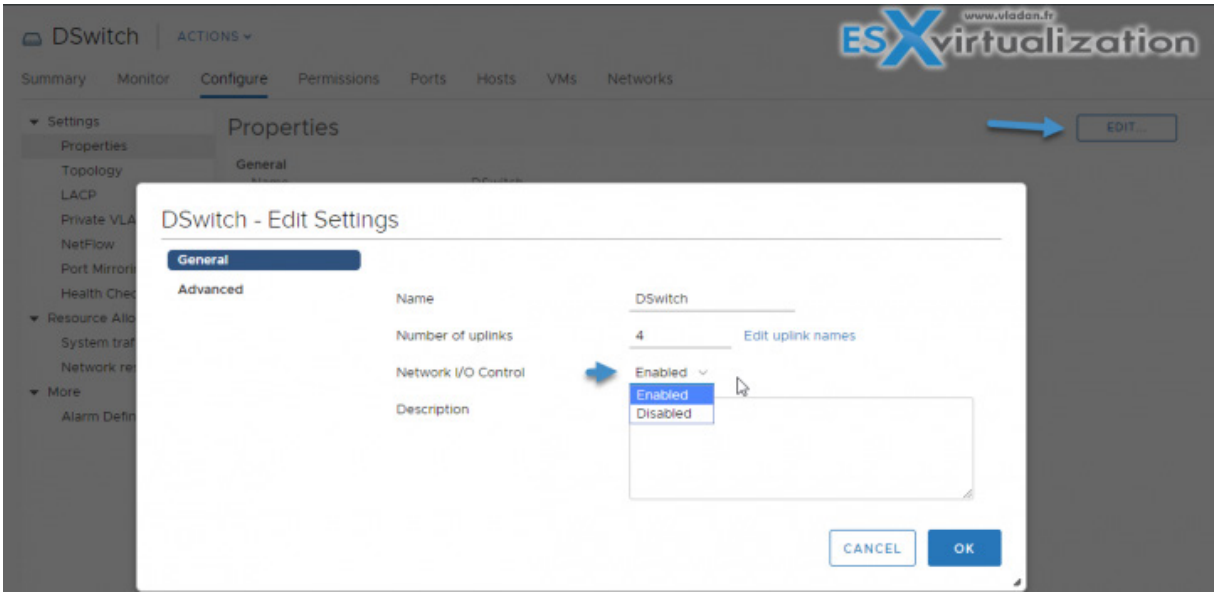
- Datastores that are Storage I/O Control-enabled must be managed by a single vCenter Server system.
- Storage I/O Control is supported on Fiber Channel-connected, iSCSI-connected, and NFS-connected storage.
- Raw Device Mapping (RDM) is not supported.
- Storage I/O Control does not support datastores with multiple extents.

Network I/O Control

Enable network resource management on a vSphere Distributed Switch to guarantee a minimal bandwidth to system traffic for vSphere features and to virtual machine traffic.

vSphere Network I/O Control version 3 introduces a mechanism to reserve bandwidth for system traffic based on the capacity of the physical adapters on a host. It enables fine-grained resource control at the VM network adapter level, similar to the model that you use for allocating CPU and memory resources.

In the vSphere Web Client, **Home > Networking >** navigate to the **distributed switch > Configure > Properties > Edit > General > Network I/O control > Enable**.



For system traffic - You can configure Network I/O Control to allocate a certain amount of bandwidth for traffic generated by vSphere Fault Tolerance, vSphere vMotion, etc.

Home > Networking > DVSwitch > Configure > Resource allocation > System traffic.

For VMs - Version 3 of Network I/O Control lets you configure bandwidth requirements for individual virtual machines.

You can also use **network resource pools** where you can assign a bandwidth quota from the aggregated reservation for the virtual machine traffic and then allocate bandwidth from the pool to individual virtual machines.

A network resource pool provides a reservation quota to virtual machines. The quota represents a portion of the bandwidth that is reserved for virtual machine system traffic on the physical adapters connected to the distributed switch. You can set aside bandwidth from the quota for the virtual machines that are associated with the pool. The reservation from the network adapters of powered on VMs that are associated with the pool must not exceed the quota of the pool.

Network I/O Control allocates bandwidth to traffic from basic vSphere system features.

Shares – Shares, from 1 to 100, reflect the relative priority of a system traffic type against the other system traffic types that are active on the same physical adapter. The amount of bandwidth available to a system traffic type is determined by its relative shares and by the amount of data that the other system features are transmitting. For example, you assign 100 shares to vSphere FT traffic and iSCSI traffic while each of the other network resource pools has 50 shares. A physical adapter is configured to send traffic for vSphere Fault Tolerance, iSCSI and management. At a certain moment, vSphere Fault Tolerance and iSCSI are the active traffic types on the physical adapter and they use up its capacity. Traffic for each receives 50% of the available bandwidth. At another moment, all three traffic types saturate the adapter. In this case, vSphere FT traffic and iSCSI traffic obtain 40% of the adapter capacity, and vMotion 20%.

Reservation – The minimum bandwidth, in Mbps, that must be guaranteed on a single physical adapter. The total bandwidth reserved among all system traffic types cannot exceed 75 percent of the bandwidth that the physical network adapter with the lowest capacity can provide. Reserved bandwidth that is unused becomes available to other types of system traffic.

However, Network I/O Control does not redistribute the capacity that system traffic does not use to virtual machine placement. For example, if you configure a reservation of 2 Gbps for iSCSI, it is possible that the distributed switch never imposes this reservation on a physical adapter because iSCSI uses a single path.

The unused bandwidth is not allocated to virtual machine system traffic so that Network I/O Control can safely meet a potential need for bandwidth for system traffic for example, in the case of a new iSCSI path where you must provide bandwidth to a new VMkernel adapter

Limit – The maximum bandwidth, in Mbps or Gbps, that a system traffic type can consume on a single physical adapter.

Final Words

You should not rely exclusively on our information, but use thse guides as a complementary resource. Perhaps it is also a good idea to download the older VCP6.5-DCV study guide PDF as it provides structure for each chapter in much more detail, and gives better support to study.

Objective 1.5 - Manage vCenter inventory efficiently

One of the lesser-known but powerful features of vSphere is **Tags**. Efficient management through tags may be one of the topics which you don't always remember to study.

Tags allow you to attach metadata to objects in the vSphere inventory, making these objects more sortable and searchable. A tag is a label that you can apply to objects in the vSphere inventory. When you create a tag, you assign that tag to a category.

VMware tags are the tags you are going to use along with the categories you are going to put them into. Categories allow you to group related tags together.

When you define a category, you can also specify which types of object its tags can be applied to and whether more than one tag in the category can be applied to an object.

For example, if you wanted to tag your virtual machines by guest operating system type, you might create a category called ‘operating system’.

You can specify that it applies to virtual machines only and that only a single tag can be applied to a virtual machine at any time.

The tags in this category might be “Windows”, “Linux”, and “Mac OS”.

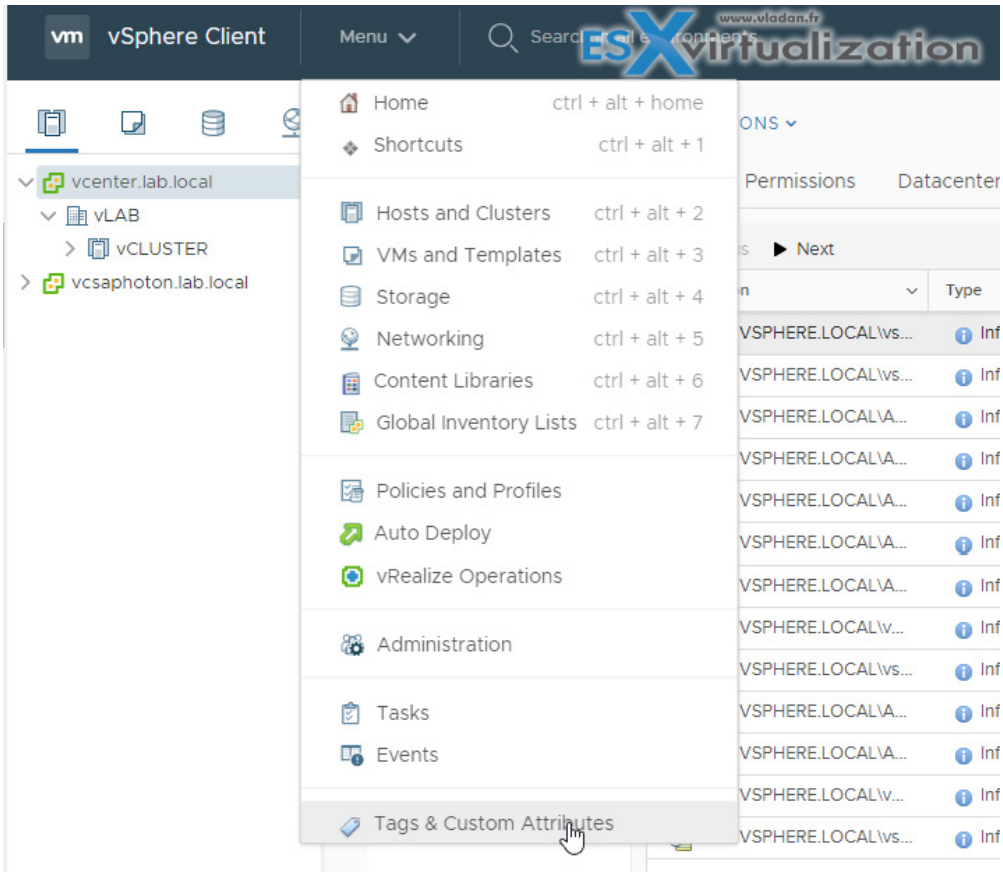
If multiple vCenter Server instances are configured to use Enhanced Linked Mode, tags and tag categories are replicated across all these vCenter Server instances. Be sure to manage vCenter inventory efficiently.

Tagging is useful in large environments but I would not bother for smaller ones. I’d say, for those with less than a hundred VMs, tagging is not especially necessary.

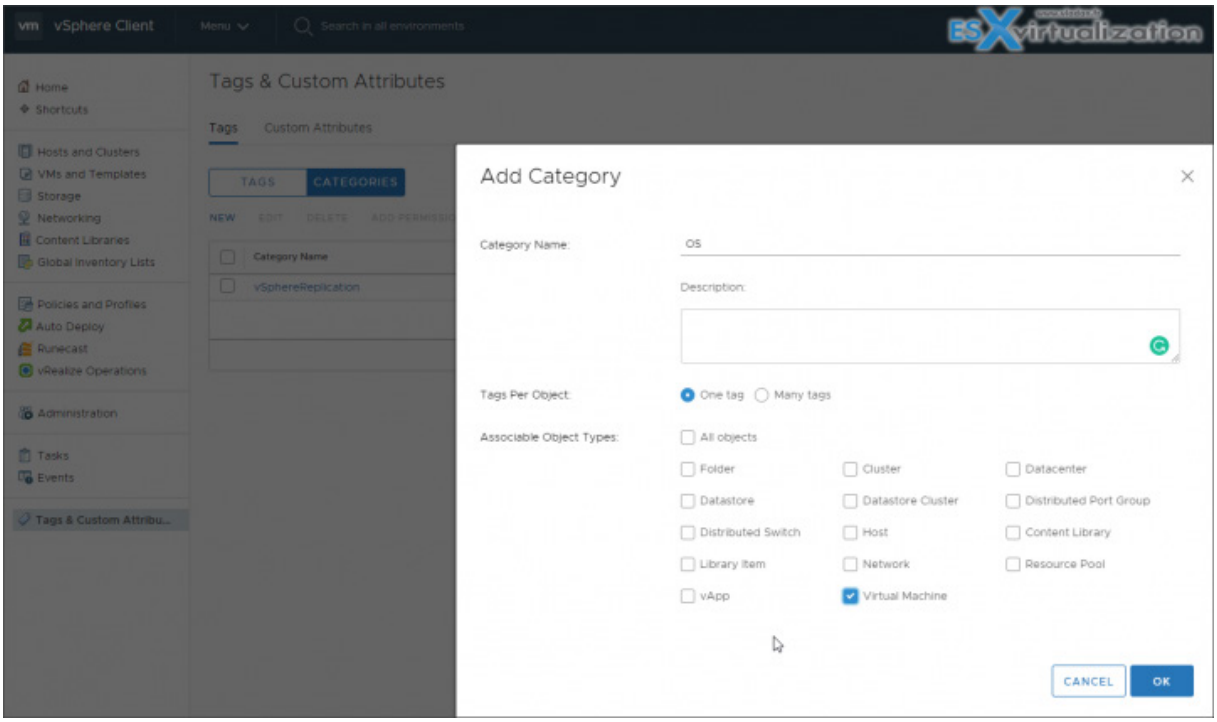
You should choose some meaningful names for your tags and categories, as they’ll continue to live with the users and the admins until otherwise changed.

Apply tagging only to those objects you consider important.

To access the Tags, Select **Menu** > **Tags** and custom categories.



Then click on the **Categories** tab > Click on the **New Category** icon > Fill in the details, specify the options and associate the category with one or more object type. Uncheck the All Object and select just Virtual Machine



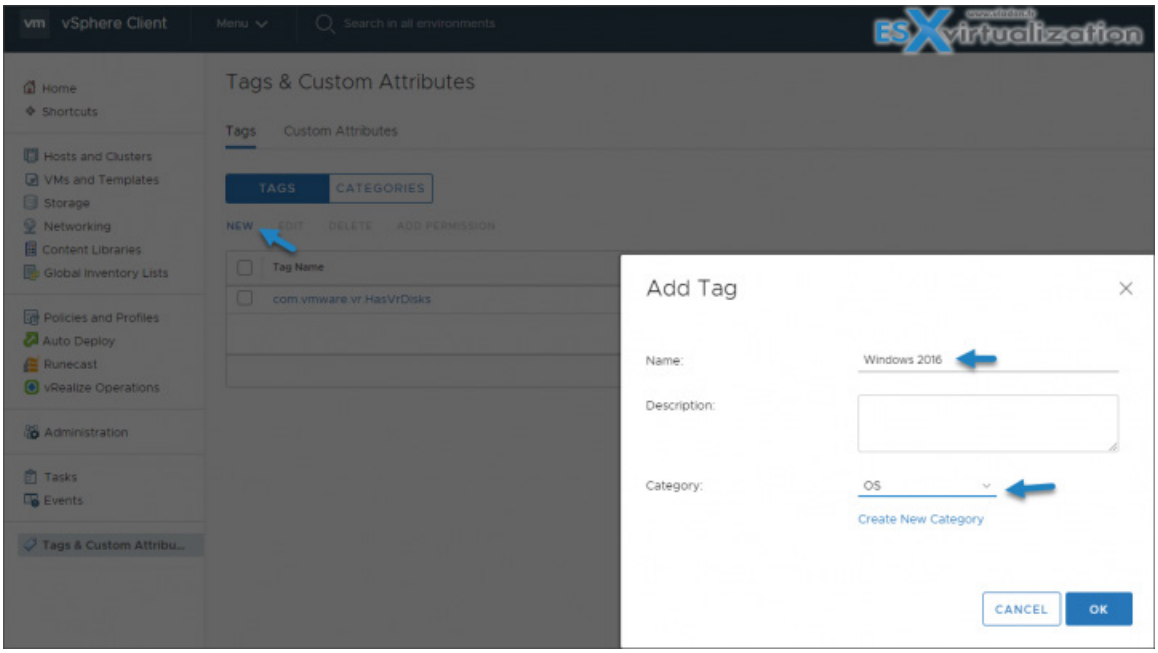
You can tag more than just VMs in your environment; my example features VMs exclusively for sake of simplicity. You can also associate a category with the following object types, or simply select All Objects.

- Cluster
- Content Library
- Datacenter
- Datastore
- Datastore Cluster
- Distributed Port Group
- Distributed Switch
- Folder
- Host
- Library Item
- Network
- Resource Pool
- vApp
- Virtual Machine

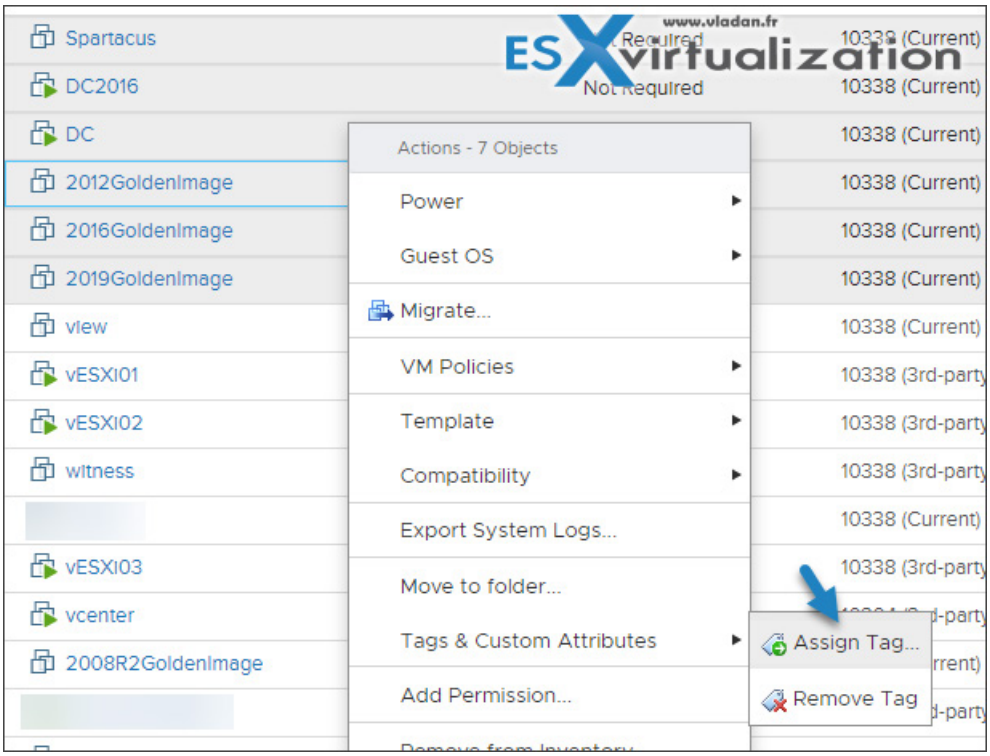
You can change the object types later, too.

After you have set the associable object types for a category, you can change the category that is associable with a single object type to be associable with all object types, but you cannot restrict a category that is associable to all object types to become associable only to a single object type.

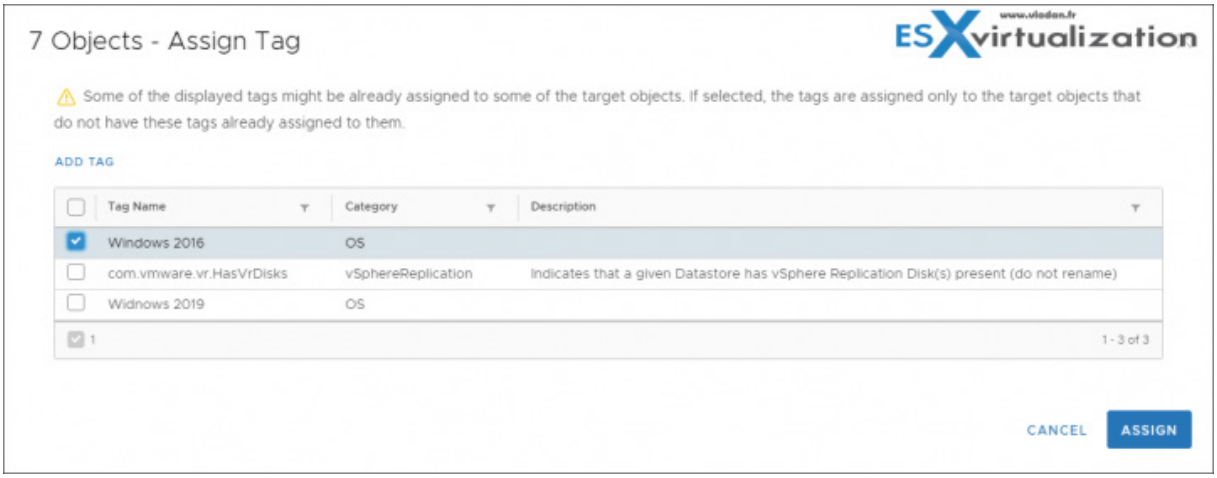
Next, click on the **Tags** tab > Click on the **New Tag icon** > Fill in the details for the tag and assign it to an existing category from the drop-down menu.



Assigning Tags to objects – I've applied a Windows OS tag to all my Windows VMs. To begin, change the view to either Hosts and Clusters or VMs and Templates and select the Virtual Machines tab



and then click the **Assign** button.



To remove tags, just simply repeat the same process but choose **Remove Tag** instead.

Searching using Tags

Many methods can be used to search for and display tagged objects.

Let's try this - Using Quick Filters.

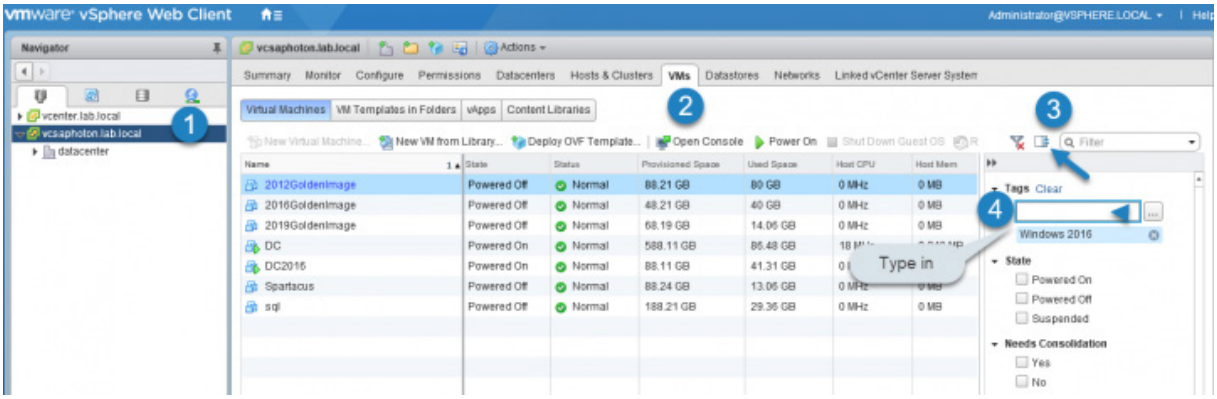
A simple way of doing this is to use the Quick Filters in vSphere.

This method works in both views.

vSphere web client (Flash).

Click on the Quick filter button. This brings the filter web component into view.
Click on the More Options button. This should load a tag selection window.

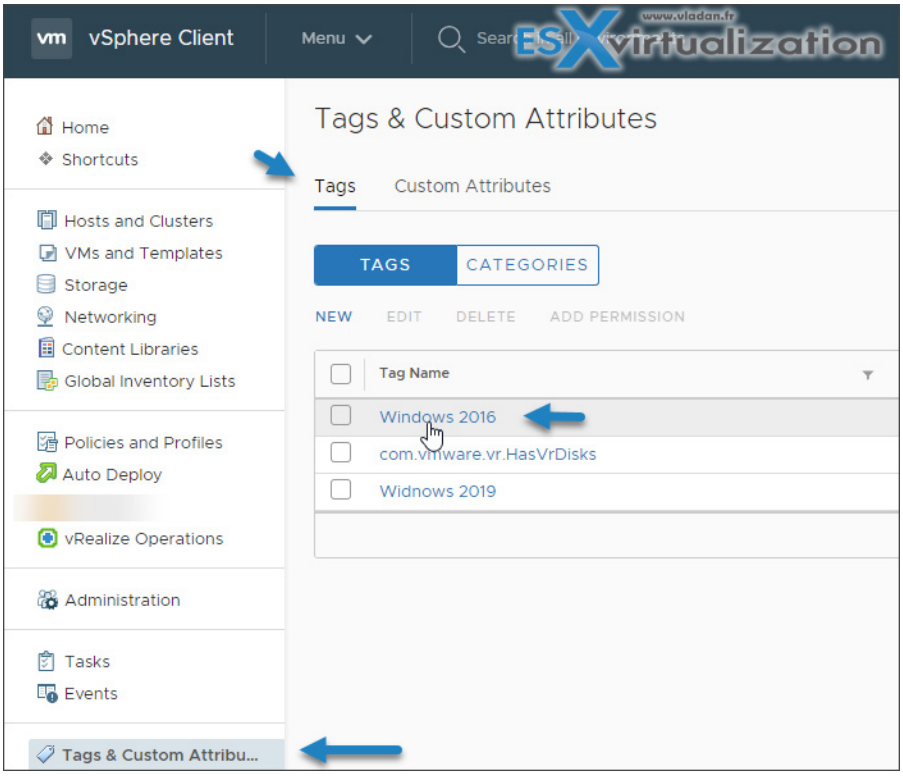
Select a tag from the list and press OK.



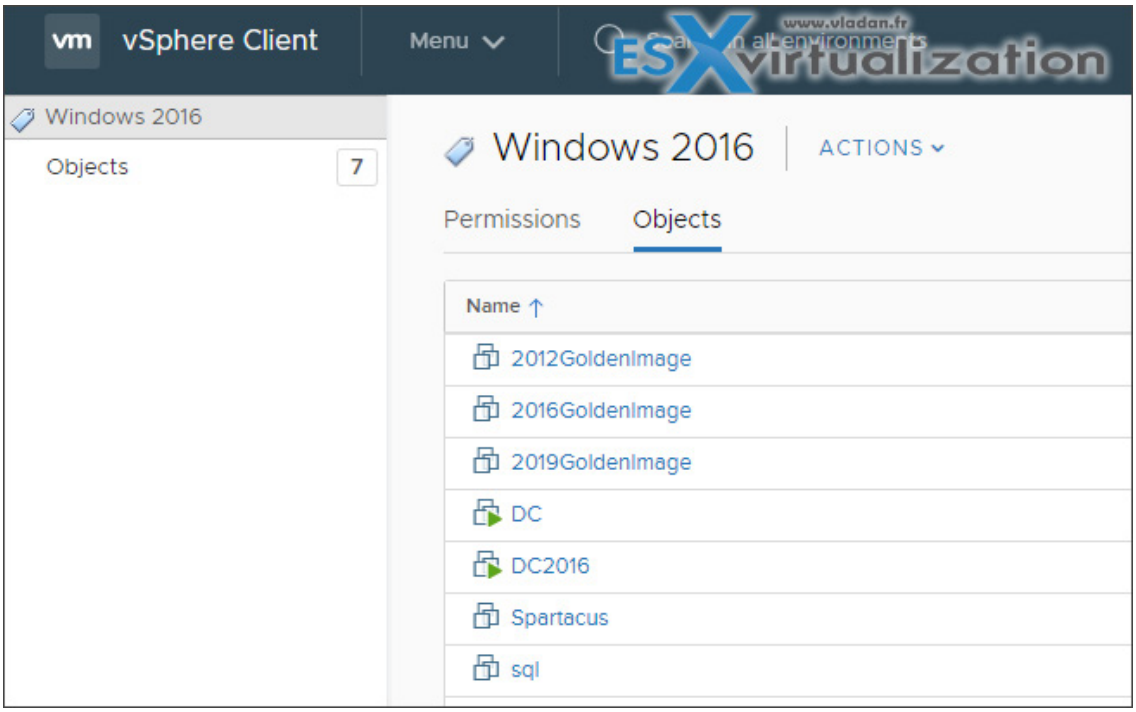
Once the filter is applied, you'll only see the VMs carrying the selected tag. You can also type in the tag name to let the tag be filled.

To remove the applied filter, just click on the Clear All Filters icon or on the cross displayed next to the filtering tag name when highlighted. That's all.

List tagged objects - If you've been wondering where to list the tagged objects, you'll have to go again to **Menu** > **Tags** and there **click the actual Tag** you created.



There, simply clicking on an individual tag from the Tags & Custom Attributes page shows you which objects are associated for this or that particular tag.



Using tags is simple. Once you've created the categories and tags, all you have to do is associate them with the objects you want. If you haven't used tags before, you should at least try them out—it might or might not be useful for the exam.

Objective 1.6 - Describe and differentiate among vSphere, HA, DRS, and SDRS functionality

There are very few guidelines about what should be covered in this chapter. We don't have any sub-chapter topic to stick to, so we'll just see what we think that should be covered and what we can put into this post without exploding the word count.

Note: You should check our VCP6.5-DCV study guide which has had a better internal structure in each objective and the technology between vSphere 6.5 and 6.7 did not change that much.

VMware vSphere - Comparing ESXi and vSphere? Possibly. VMware ESXi = Standalone host. Many ESXi hosts require a central management = vCenter server. vCenter and ESXi hosts are basically the two principal components which form a VMware vSphere Infrastructure.

VMware vSphere is the commercial name for the whole VMware Suite. vCenter itself is just one part of the licensing puzzle. You need to have a license for each of your connected ESXi hosts in order to manage them from a single central location.

Those licenses have basically 3 different flavors (Standard, Enterprise, vSphere with Operations Management Enterprise, Platinum) and are counted per physical CPU.

VMware High Availability (HA) - VMware HA protects against host or storage failures. If there is an unplanned hardware failure, vSphere High Availability (HA) can automatically restart VMs which failed when the host failed. Those VMs are automatically restarted on other hosts which are part of VMware cluster.

There is little downtime during which the system figures out how the host has failed and which hosts are able to start the failed VMs. Those hosts must have enough available capacity in terms of memory or CPU. Once this automatic decision is taken, the VM boots up. The whole process is completely automatic and acts without the admin's intervention.

A single host within vSphere HA cluster is automatically elected as the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of slave hosts.

When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster.

The master host and its responsibilities:

- To Monitor the state of slave hosts. If there is a slave host which fails or is unavailable, the master host knows which VMs needs to be restarted on other hosts.
- The master host also monitors the power state of all protected VMs. If one VM fails, then the master host makes sure that this particular VM is restarted and monitors the progress. The master also knows the resources available, letting it make a decision where to restart that VM (on which host).
- Master host manages a list of cluster hosts and protected VMs.

The slave hosts provide secondary, passive tasks, where they report on the state of VMs which are running on the slave hosts, updates the master with its availability and its resources.

The master host is able to "orchestrate" restarts of protected VMs.

If the master fails, there is a re-election process and the host which has access to the greatest number of datastores is elected as a master. This is due to the fact that the secondary communication channel operates through datastores. There are other considerations for a Slave to become elected as a Master as well.

HA can protect you against host or network failure. In the case that the host gets isolated, the response to this event can be configured differently so the VM can stay up and running (instead of killed and restarted elsewhere). Let's explore this now for more details.

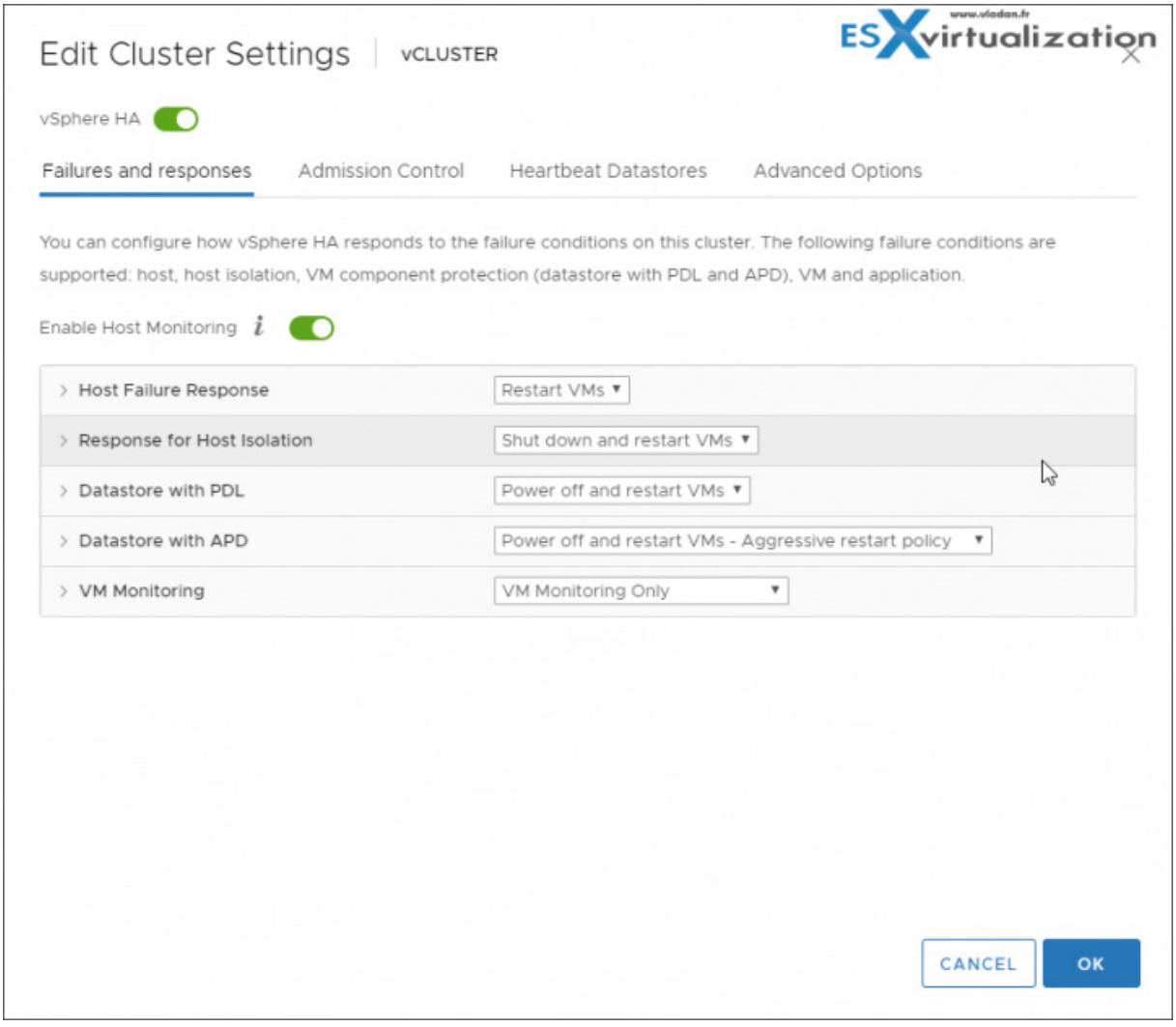
In a vSphere HA cluster, three types of host failures can be detected:

- **Failure** – When a host stops functioning.
- **Isolation** – When a host becomes network isolated.

- **Partition** – When a host loses network connectivity with the master host (A "Master" host is the only one within the cluster, and it's the one who is responsible for monitoring the "slave" hosts within the cluster).

The secondary channel through datastores is known as a **Heartbeat Datastores**. However, this secondary network is not used in normal situations—only in the event that the primary network goes down.

This secondary channel permits the Master to be aware of all Slave hosts and also the VMs running on those hosts. The Heartbeat datastores can also determine if the host has become isolated or network partitioned. The secondary channel can determine if the host is failed (PSOD) or if it's just isolated.



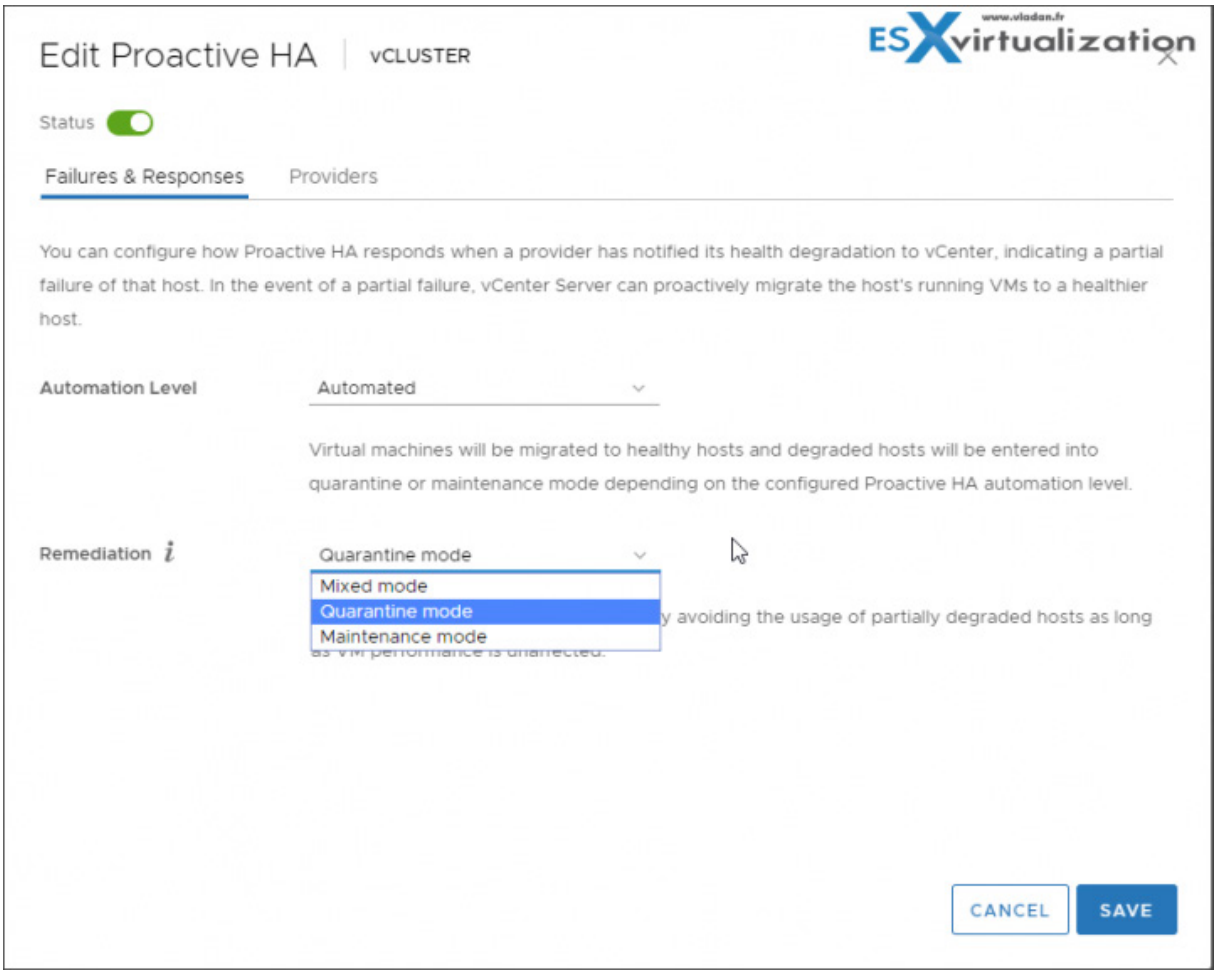
VM Restart Priority

Quote:

VM restart priority determines the relative order in which virtual machines are allocated resources after a host failure. Such virtual machines are assigned to hosts with unreserved capacity, with the highest priority virtual machines placed first and continuing to those with lower priority until all virtual machines have been placed or no more cluster capacity is available to meet the reservations or memory overhead of the virtual machines.

Proactive HA - If you have a component failure, which affects the redundancy. This does not officially count as failure yet. You can configure how Proactive HA responds when a provider has notified its health degradation to vCenter, indicating a partial failure of that host.

In this case, the VMs residing on that host can be evacuated to other hosts and the host where is the failure is placed in Quarantine mode or Maintenance Mode.



VMware Distributed Resource Scheduler (DRS) - VMware vSphere Distributed Resource Scheduler (DRS) is a resource scheduler. It monitors and can react to changes in VM workloads. The system can migrate VMs to other hosts in order to distribute the load.

DRS automatically places virtual machines onto hosts at VM power-on, and virtual machines are automatically migrated from one host to another to optimize resource utilization.

Started in VMware vSphere 6.5, vSphere DRS can predictively migrate workloads based on existing patterns in those workloads.

Note: If you're using VMware FT, then you should know that vSphere DRS do not load balance FT protected VMs (unless they're using Legacy FT managed by vCenter server 6.0). As such, you might end up with an FT VMs being unevenly distributed across your cluster.

Screenshot from VMware documentation ("*vSphere ESXi vCenter Server 6.7 resource management guide*" - *Page 69*):

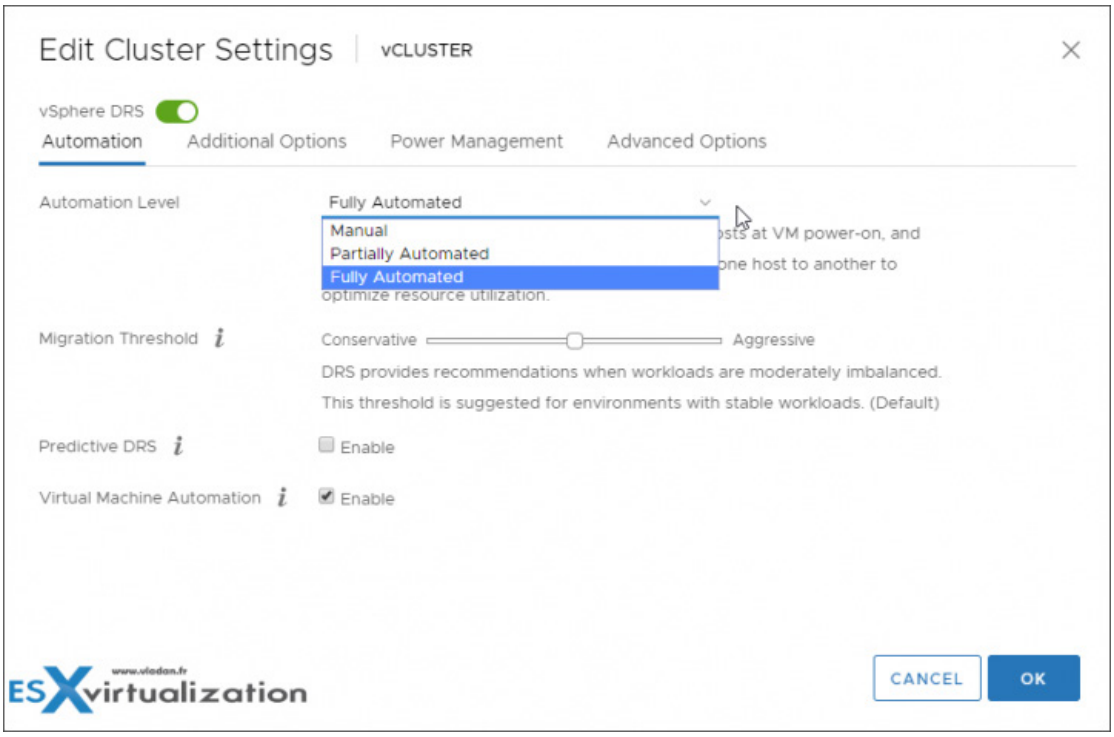
Table 11-1. DRS Behavior with vSphere FT Virtual Machines and EVC

EVC	DRS (Load Balancing)	DRS (Initial Placement)
Enabled	Enabled (Primary and Secondary VMs)	Enabled (Primary and Secondary VMs)
Disabled	Disabled (Primary and Secondary VMs)	Disabled (Primary VMs) Fully Automated (Secondary VMs)

vSphere DRS Requirements:

- Minimum of 3 hosts and activated DRS in the cluster.
- VMware vCenter Server
- vMotion network enabled on all hosts within your cluster
- Enterprise Plus licensing
- Shared Storage connected to all hosts within the cluster.
- If using predictive DRS, you will need vRealize Operations (vROPs). - Note you must also configure Predictive DRS in a version of vRealize Operations that supports this feature.

vSphere HA and DRS - Better together - If you're using HA with DRS, you're basically getting automatic failover with load balancing. You get your cluster more balanced after HA has moved VMs to a different host.



We have just scratched a surface on DRS... Read the doc to learn more.

VMware Storage DRS - A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create a datastore cluster, you can use vSphere Storage DRS to manage storage resources.

Storage DRS allows you to manage the aggregated resources of a datastore cluster, which means that you can balance a space and I/O load between different datastores within a datastore cluster. Also, SDRS manages the initial placement of virtual disks based on space and I/O workload.

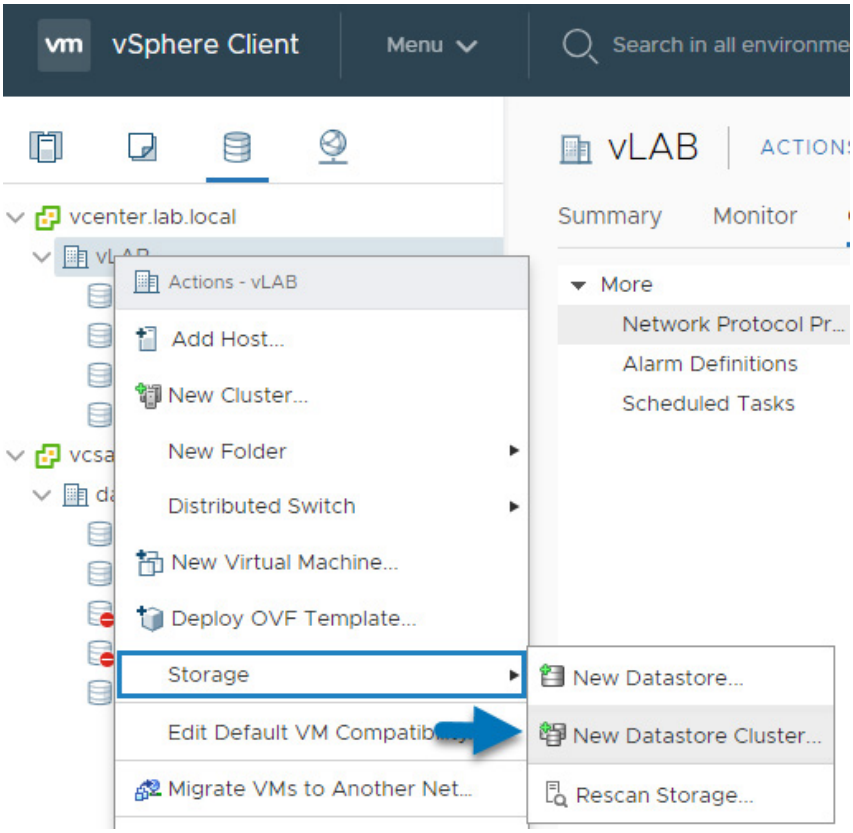
What is an initial placement? The initial placement is a process in which you select a datastore within datastore cluster where you want to place a virtual machine disk and the system will propose you the best possible place. SDRS and initial placement occur when, for example, you create a new virtual machine (VM) or clone VM.

This also happens when a virtual machine disk (VMDK) is migrated to another datastore cluster, or when you add a disk to an existing VM. SDRS enables or disables all of these components (I/O, initial placement, and space load balancing) at once. If necessary, you can disable I/O-related functions of Storage DRS independently of space balancing functions.

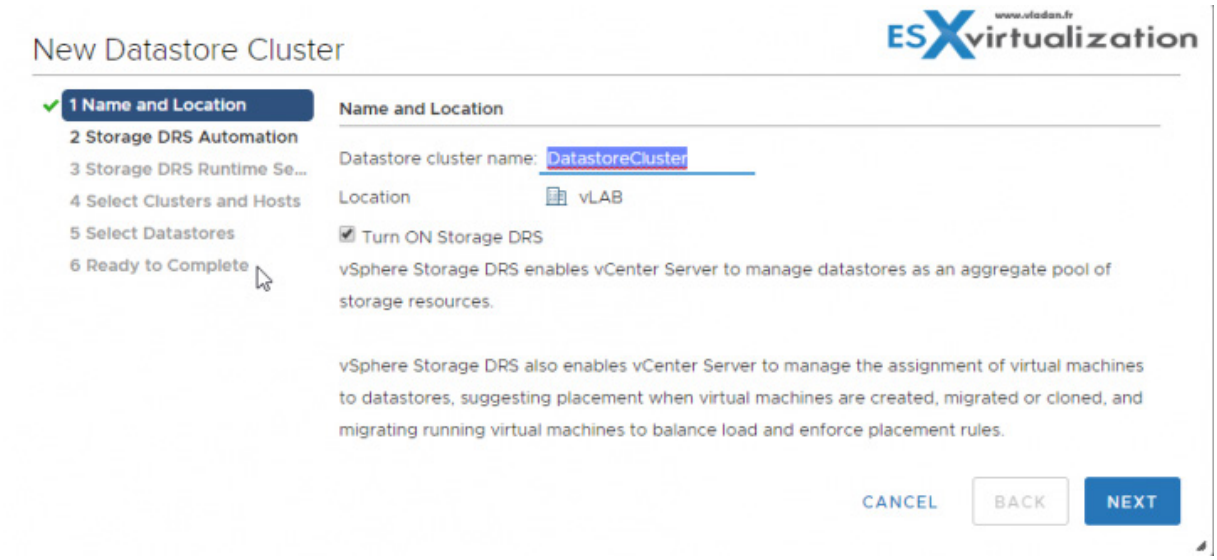
There is a **manual mode** which shows only recommendations, and there is **automation mode** which does move VMDKs around. SDRS recommend the placements of VM(s), their VMDKs, from which datastore (source) to which datastore (destination), also showing you the reason for the recommendation. It may be that the source datastore is running out of space or anti-affinity rules are violated or the datastore is entering maintenance mode.

Datastore clusters must contain similar or interchangeable datastores. A datastore cluster can contain a mix of datastores with different sizes and I/O capacities, and can be from different arrays and vendors.

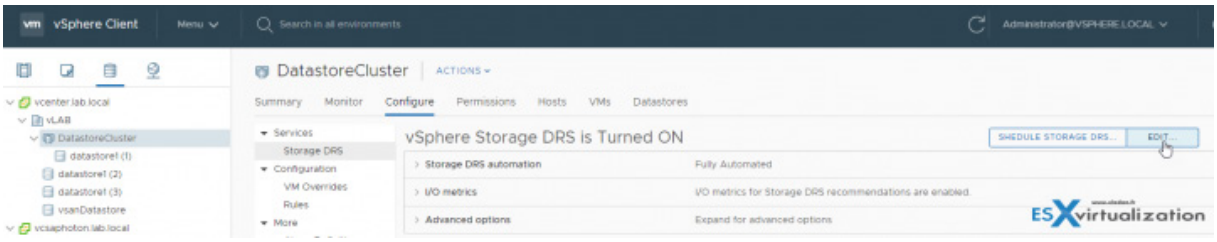
Where to enable SDRS? - Right-click the data center object and select New Datastore Cluster.



A wizard will walk you through...



Once finished, you can come back to modify those settings. Simply select the datastore cluster > **Edit**.



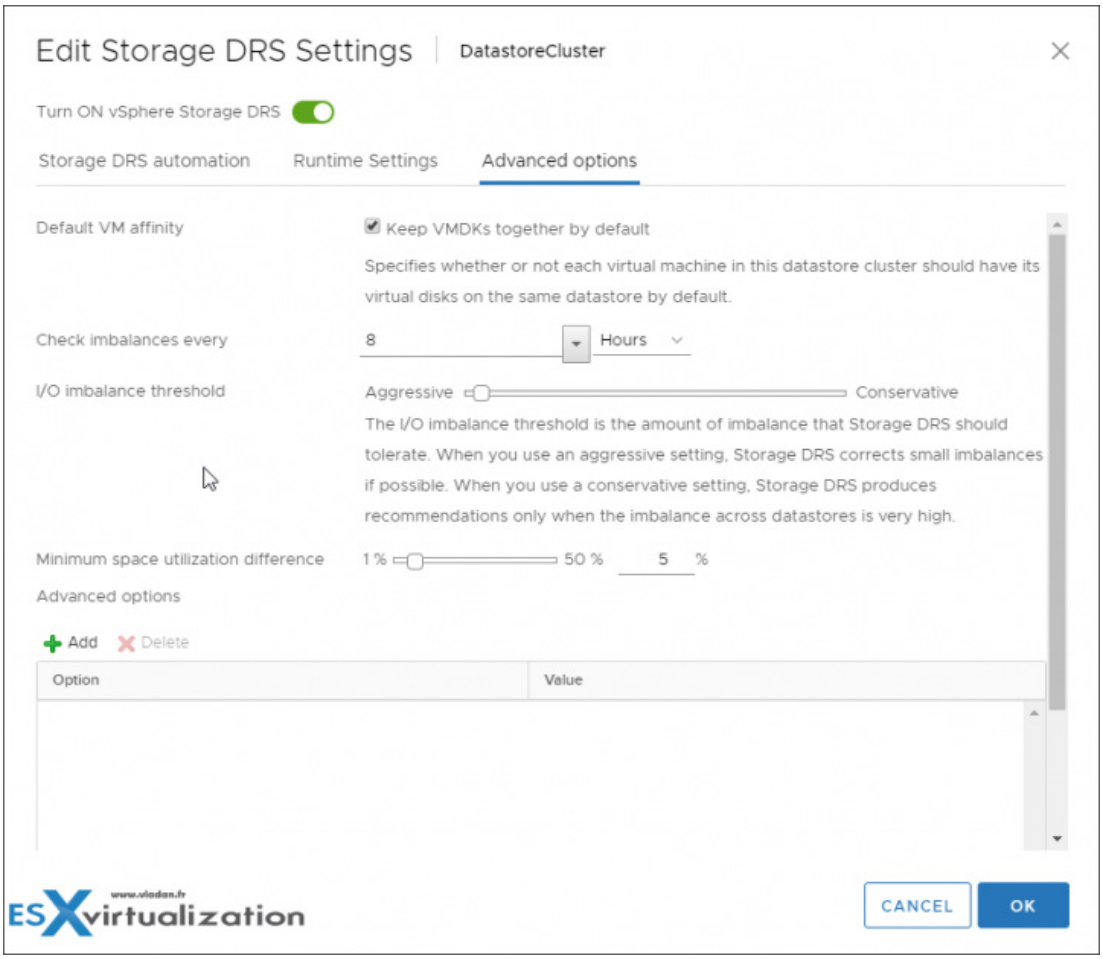
Note: "Keep VMDKs together" by default is selected. It specifies whether or not each virtual machine in this datastore cluster should have its virtual disks on the same datastore by default.

What are VMware Storage DRS Requirements?

- The use of similar or interchangeable datastores for a datastore cluster is allowed.
- There can be a mix of datastores with different sizes and I/O capacities and can be from different arrays and vendors.
- You cannot use NFS and VMFS within the same datastore cluster.
- There cannot be used – Replicated datastores with non-replicated datastores in the same Storage-DRS-enabled datastore cluster.
- Datastores which are shared across multiple datacenters are not allowed.
- All hosts must be at least ESXi 5.0
- Best practice – do not include datastores with hardware acceleration enabled with datastores without hardware acceleration enabled.

***Advanced Options*.**

The I/O imbalance threshold is the amount of imbalance that Storage DRS should tolerate. When you use an aggressive setting, Storage DRS corrects small imbalances if possible. When you use a conservative setting, Storage DRS produces recommendations only when the imbalance across datastores is very high.



At the end of each chapter, I often have the feeling that I have just scratched the surface—that is to say, that there is more to learn and more to know for the exam. I hope you have the same feeling and that you continue to study more, not simply relying solely on our study guide.

Objective 1.7 - Describe and identify resource pools and use cases

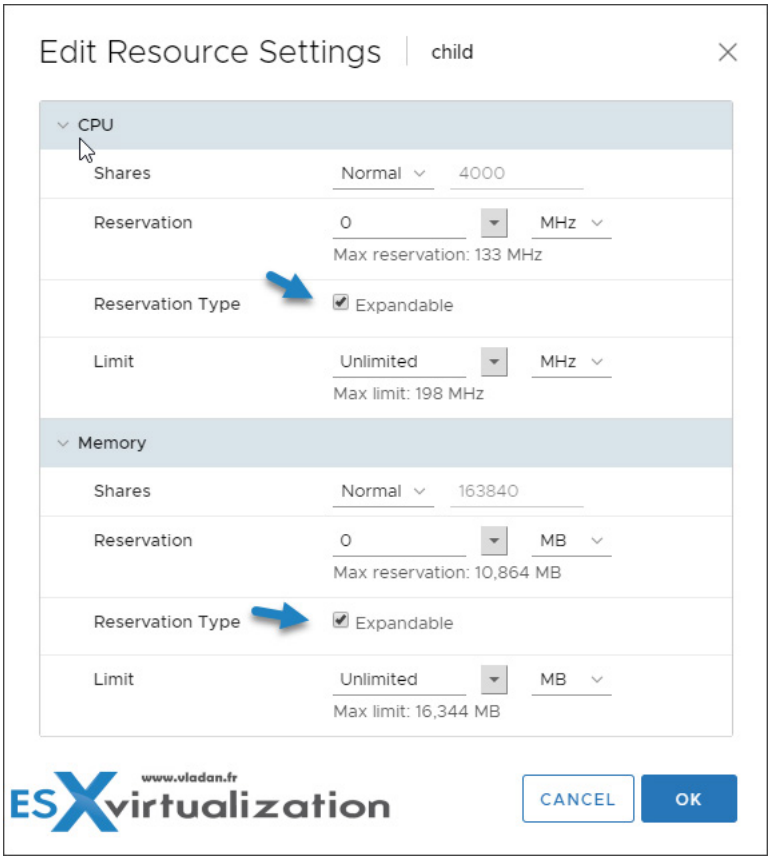
Resource Pools (RP) can be grouped into hierarchies and used to partition available CPU and memory resources, based on hierarchies. Each host and DRS cluster has a root resource pool (invisible) which does not appear as RP because it's always the same, as it sits at the root of each host/cluster.

You can create child resource pools out of the resource pool, which owns some resources of the parent RP. Your RP can contain other RPs, VMs or both. You can create a hierarchy of shared resources.

Determine the effect of the Expandable Reservation parameter on resource allocation

Expandable Resource Pool – The system considers the resources available in the selected resource pool and its direct parent resource pool. If the parent resource pool also has the Expandable Reservation option selected, it can borrow resources from its parent resource pool.

Borrowing resources occur recursively from the ancestors of the current resource pool as long as the Expandable Reservation option is selected. Leaving this option selected offers more flexibility, but, at the same time provides less protection. A child resource pool owner might reserve more resources than you anticipate.



Create a Resource Pool hierarchical structure - Resource pools always start at the root level. Each standalone host and DRS cluster has its own (invisible) root resource pool. You must **enable DRS first** in order to create a resource pool.

Note: DRS is available in vSphere Enterprise and Enterprise Plus editions.

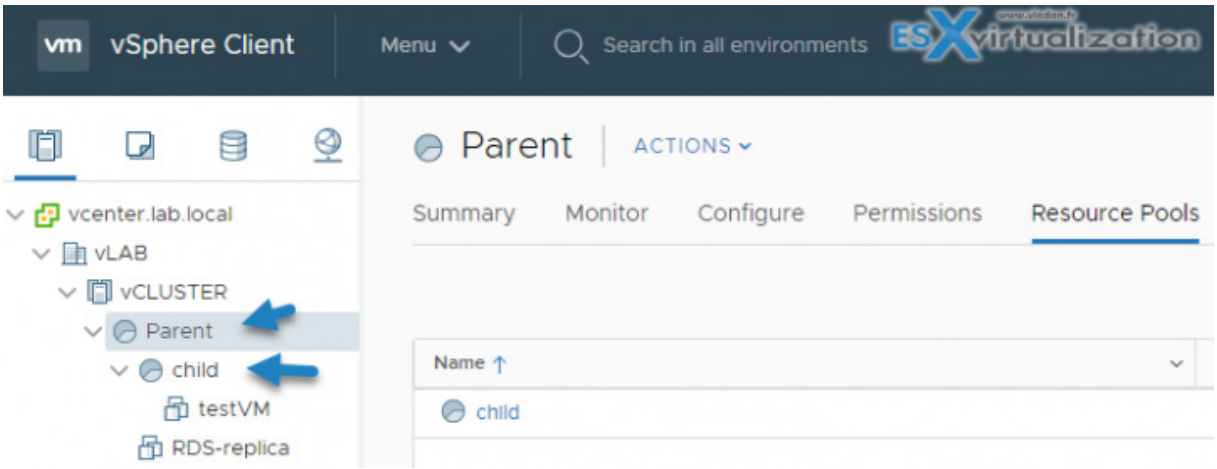
Resource Pools should be used when you need to limit or guarantee resources to VMs. By having a resource pool, you don't have to guarantee the resources to VMs individually, but only at the pool level.

When you power on a virtual machine in a resource pool or try to create a child resource pool, the system performs additional admission control to ensure the resource pool's restrictions are not violated.

Before you power on a virtual machine or create a resource pool, ensure that sufficient resources are available using the Resource Reservation tab in the vSphere Web Client. The Available Reservation value for CPU and memory displays resources that are unreserved.

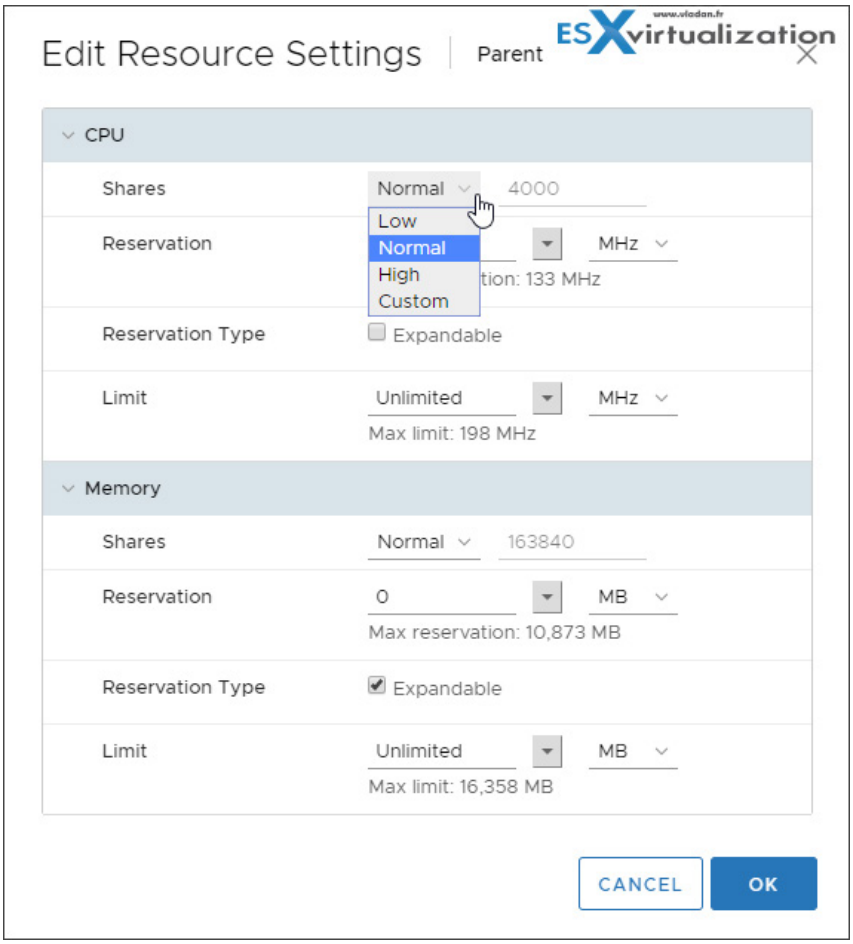
How available CPU and memory resources are computed and whether actions are performed depends on the Reservation Type, **Fixed** or **Expandable**.

The system does not allow you to violate preconfigured Reservation or Limit settings. Each time you reconfigure a resource pool or power on a virtual machine, the system validates all parameters so all service-level guarantees can still be met.



Configure custom Resource Pool attributes

- Navigate to the Host and Clusters view (**View** > **Inventory** > **Hosts and Clusters**)
- Right-click on the resource pool you would like to edit and select **Edit Settings...**
- Change the name if desired
- Change the **CPU Shares**, **Reservation**, **Expandable Reservation** and **Limit** if desired
- Change the **Memory Shares**, **Reservation**, **Expandable Reservation** and **Limit** if desired



CPU Resources

Normally, you accept the default and let the host handle resource allocation.

Shares – Specify shares for this resource pool with respect to the parent's total resources. The quantity of shares you allocate to a resource pool is relative to the shares of any sibling (virtual machine or resource pool) and relative to its parent's total resources. Sibling resource pools share resources according to their relative share values, bound by the reservation and limit.

Different types of shares – Low **(1)**, **Normal (2)**, or **High (4)** which specify share values in a ratio**.** Or you can select **Custom** to give each RP a specific number of shares, which are expressed in a proportional weight.

Reservation – Specify a guaranteed CPU or memory allocation for this resource pool. Defaults to 0. A nonzero reservation is subtracted from the unreserved resources of the parent (host or resource pool). The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool.

Limit – the upper limit for this resource pool's CPU allocation. Select Unlimited to specify no upper limit.

Memory Resources

Shares – Memory shares for this resource pool with respect to the parent's total. Sibling resource pools share resources according to their relative share values bound by the reservation and limit. Select **Low (1)**, **Normal (2)**, or **High (4)**, which specify share values in a ratio.

Select **Custom** to give each virtual machine a specific number of shares, which express a proportional weight.

Reservation – Guaranteed memory allocation for this resource pool.

Limit – the upper limit for this resource pool's memory allocation. If you give RP limit 32 GB RAM, it will never receive more RAM even if the host/cluster is able to allocate more. Select Unlimited to specify no upper limit.

Expandable Reservation – When the checkbox is selected (default), expandable reservations are considered during admission control. If you power on a virtual machine in this resource pool, and the combined reservations of the virtual machines are larger than the reservation of the resource pool, the resource pool can use resources from its parent or ancestors.

Determine how Resource Pools apply to vApps

You can configure the CPU and memory resource allocation for the vApp, but first, make sure that you know which privilege you require.

Required privilege: vApp > vApp resource configuration on the vApp.

Reservations on vApps and all their child resource pools, child vApps, and child virtual machines count against the parent resources only if those objects are powered on.

Navigate to a vApp in the inventory and click **Edit vApp Settings >** In the Deployment section, click **CPU resources** to allocate CPU resources to this vApp.

Shares – CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bound by the reservation and limit. Select Low, Normal, or High, which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.

Reservation – Guaranteed CPU allocation for this vApp.

- **Reservation Type** – Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
- **Limit** – the upper limit for this vApp's CPU allocation. Select Unlimited to specify no upper limit.
- **Shares** – Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bound by the reservation and limit. Select Low,

Normal, or High, which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.

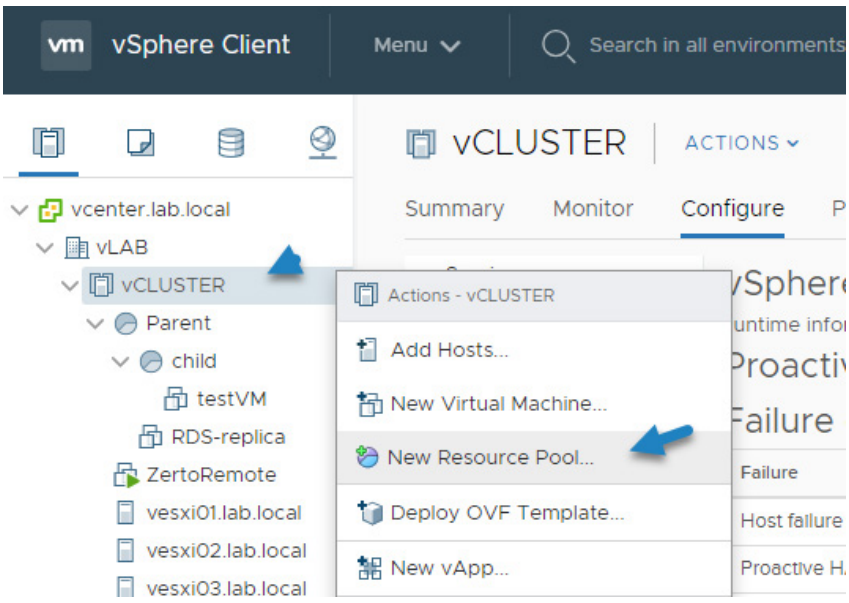
- **Reservation** – Guaranteed memory allocation for this vApp.
- **Reservation Type** – Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
- **Limit** – the upper limit for this vApp's memory allocation. Select Unlimited to specify no upper limit.

Option	Description
Shares	Defines the CPU or memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares that expresses a proportional weight.
Reservation	Defines the guaranteed CPU or memory allocation for this vApp.
Reservation Type	Defines whether the reservation is expandable. Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Defines the upper limit for this vApp's CPU or memory allocation. Select **Unlimited** to specify no upper limit.

Create/Remove a Resource Pool - To be able to create a Resource pool, you must enable DRS.

Select **Hosts and clusters** > **Manage** > **vSphere DRS** > **Edit** > **Check the Turn ON.**

The easiest way to create a resource pool is perhaps the **Right click** at the cluster > **New resource pool**...



Add/Remove virtual machines from a Resource Pool

Drag and drop... -:) Alternatively, when creating a new VM, during the wizard creation, you're asked whether you want to place the VM into a specific resource pool.

If the resource pool does not have enough resources to guarantee the virtual machine reservation(s), then the move into the resource pool will fail (for a powered-on virtual machine).

Resource Pool Admission Control

Prevents you from powering on VMs which violate RP restrictions. Before you power on a virtual machine or create a resource pool, ensure that sufficient resources are available using the Resource Reservation tab in the vSphere Client. The Available Reservation value for CPU and memory displays resources that are unreserved.

How available CPU and memory resources are computed and whether actions are performed depend on the Reservation Type.

The reservation type can be:

- **Fixed** - The system checks whether the selected resource pool has sufficient unreserved resources. If it does, the action can be performed. If it does not, a message appears and the action
  cannot be performed.
- **Expandable** - The system considers the resources available in the selected resource pool and its direct parent resource pool. If the parent resource pool also has the Expandable Reservation option selected, it can borrow resources from its parent resource pool. Borrowing resources occurs recursively from the ancestors of the current resource pool as long as the Expandable Reservation option is selected. Leaving this option selected offers more flexibility, while at the same time providing less protection. A child resource pool owner might reserve more resources than you anticipate.

I highly recommend getting the PDF series called *vSphere Resource Management* when studying for the exam.

Example of Expandable reservation from the PDF:

Let's assume an administrator manages pool P, and defines two child resource pools, S1 and S2, for two different users (or groups).

The administrator knows that users want to power on virtual machines with reservations, but does not know how much each user will need to reserve. Making the reservations for S1 and S2 expandable allows the administrator to more flexibly share and inherit the common reservation for pool P.

Without expandable reservations, the administrator needs to explicitly allocate a specific amount to S1 and S2. Such specific allocations can be inflexible, especially in deep resource pool hierarchies and can complicate setting reservations in the resource pool hierarchy.

Expandable reservations cause a loss of strict isolation in that S1 can start using all of P's reservation so that no memory or CPU is directly available to S2.

Objective 1.8 - Differentiate between VDS and VSS

Today, we'll cover another objective from VCP-DCV 2019 certification and will talk about the difference between vSphere standard switches (vSS) and vSphere Distributed Switches (vDS).

A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port group.

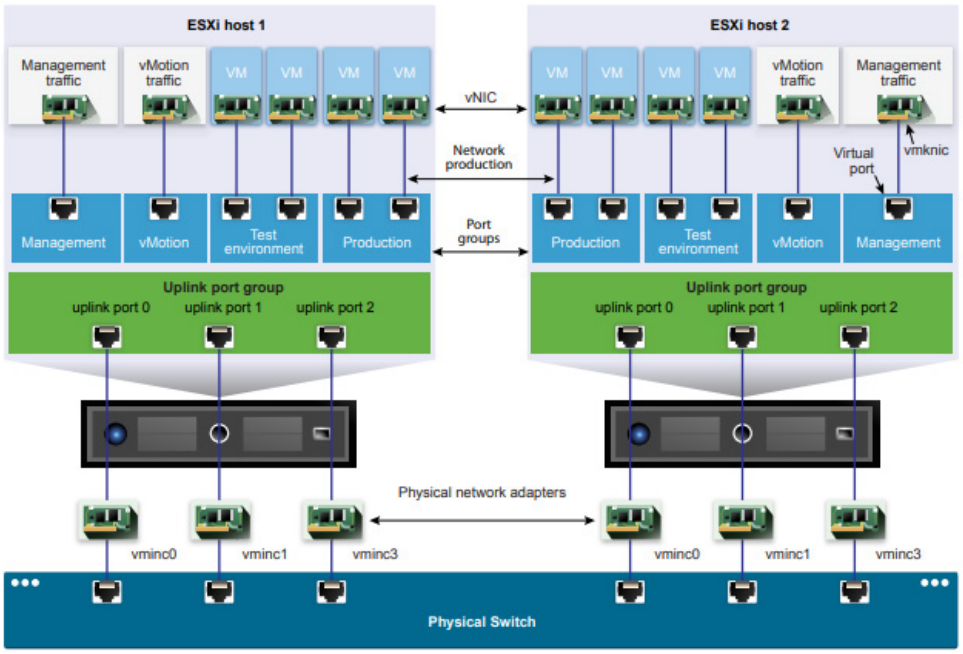
When it is connected to the physical switch using a physical Ethernet adapter (also known as uplink), you can have a connection between your virtual infrastructure and the physical (outside) world.

vSphere Standard Switch (VSS) - It works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines.

A vSphere standard switch can be connected to physical switches by using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks.

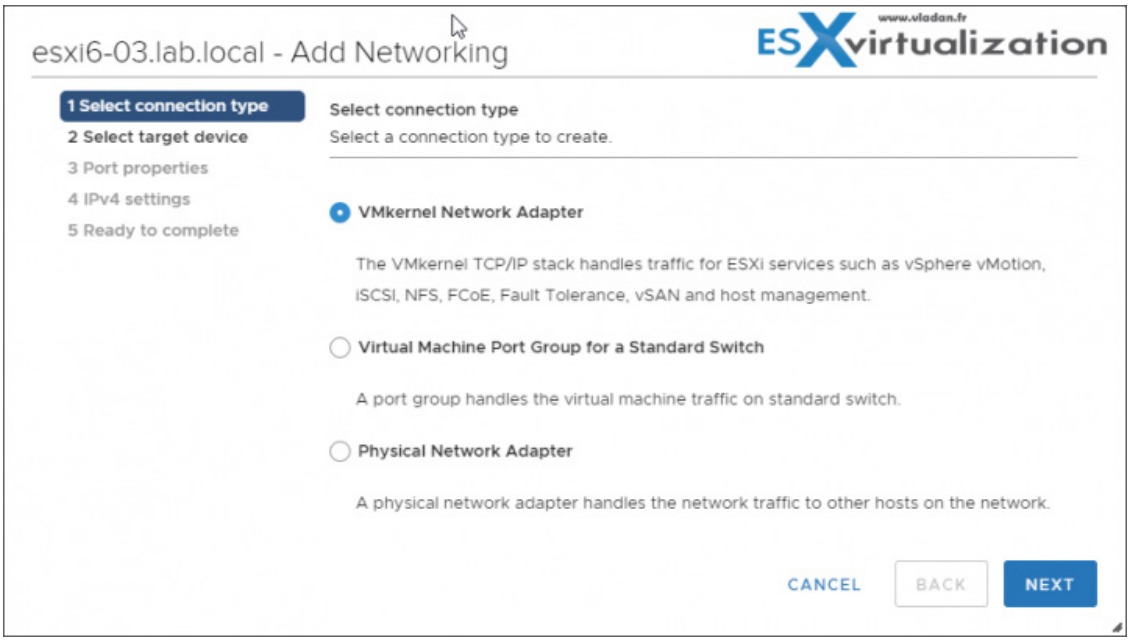
This type of connection is similar to connecting physical switches together to create a larger network. Even though a vSphere standard switch works much like a physical switch, it does not have some of the advanced functionality of a physical switch.

Figure 2-1. vSphere Standard Switch architecture



How to create a standard vswitch?

Select **Host > Configure > Networking > Virtual Switches > Add**. At the same time, the assistant proposes you to create either VMkernel network adapter, VM port group or Physical network adapter.

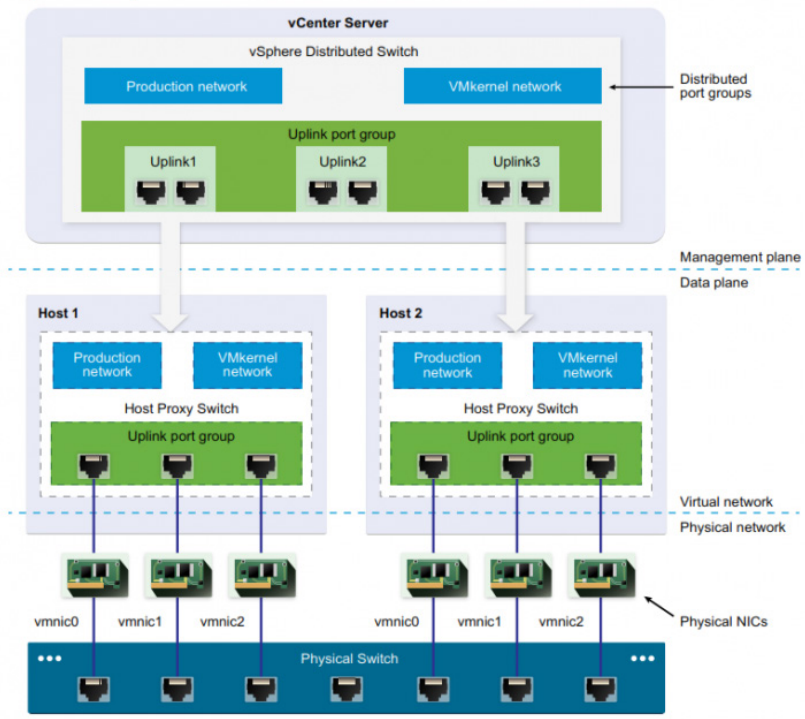


vSphere Distributed Switch - A vSphere distributed switch acts as a single switch across all associated hosts in a data center to provide centralized provisioning, administration, and monitoring of virtual networks.

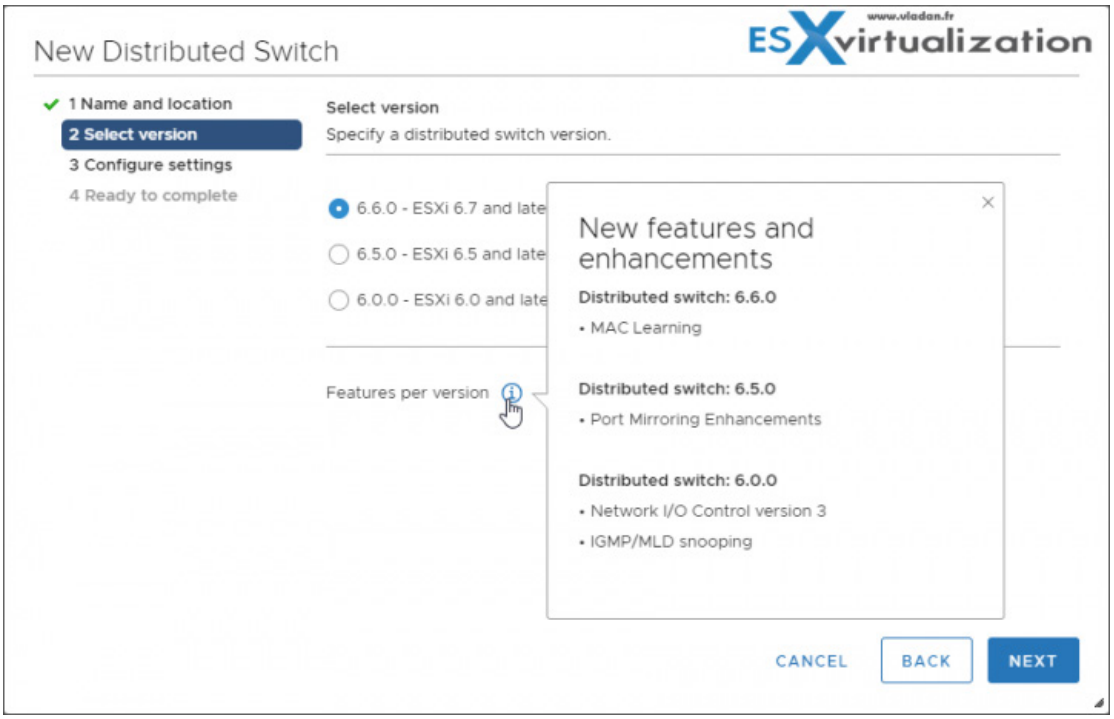
You configure a vSphere distributed switch on the vCenter Server system and the configuration is propagated to all hosts that are associated with the switch.

This lets virtual machines maintain consistent network configuration as they migrate across multiple hosts.

Figure 3-1. vSphere Distributed Switch Architecture



Where to? Right-click Datacenter > Create new distributed switch.



VLAN - VLAN enables a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments. The standard is 802.1Q.

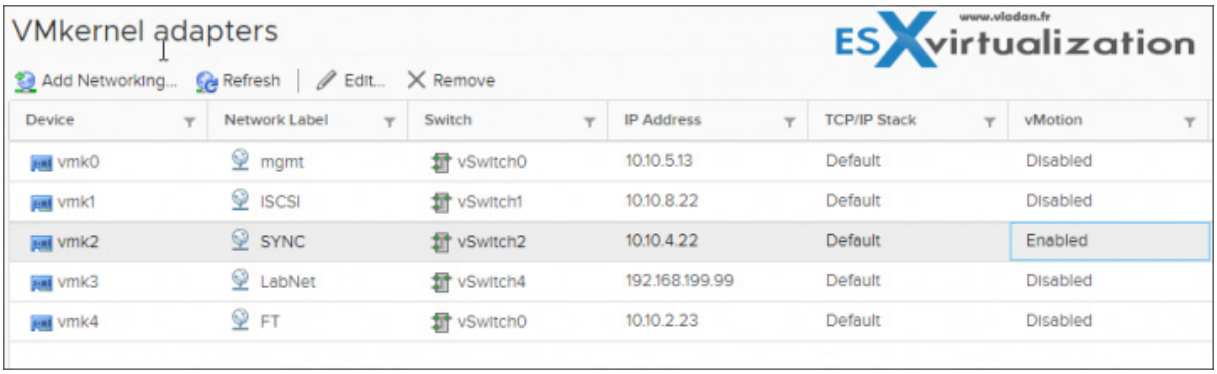
vSphere Standard Port Group - Network services connect to standard switches through port groups. Port groups define how a connection is made through the switch to the network. Typically, a single standard switch is associated with one or more port groups. A port group specifies port configuration options such as bandwidth limitations and VLAN tagging policies for each member port.

Each port group on a standard switch is identified by a network label, which must be unique to the current host. You can use network labels to make the networking configuration of virtual machines portable across hosts. You should give the **same label** to the port groups in a data center that use physical NICs connected to one broadcast domain on the physical network.

vSphere Distributed Port Group - A port group associated with a vSphere distributed switch that specifies port configuration options for each member port. Distributed port groups define how a connection is made through the vSphere distributed switch to the network.

NIC Teaming - NIC teaming occurs when multiple uplink adapters are associated with a single switch to form a team. A team can either share the load of traffic between physical and virtual networks among some or all of its members, or provide passive failover in the event of a hardware failure or a network outage.

VMkernel port - VMkernel networking layer provides connectivity to hosts and handles the standard infrastructure traffic of vSphere vMotion, IP storage, Fault Tolerance, and VSAN.



Uplink port - ethernet adapter connected to the outside world. To connect with physical networks.

I invite you to read the **vSphere Networking PDF** for more details.

Further reading of the document will give you details on:

- Managing networking on multiple hosts on a VDS
- Migrating VMKernel adapters to VDS

- Creating VMkernel adapters on VDS
- Using Host as a template to create a uniform networking configuration on VDS

Networking Policies

Policies set at the standard switch or distributed port group level apply to all of the port groups on the standard switch or to ports in the distributed port group. The exceptions are the configuration options that are overridden at the standard port group or distributed port level.

Teaming and Failover Policy - NIC teaming lets you increase the network capacity of a virtual switch by including two or more physical NICs in a team. To determine how the traffic is rerouted in case of adapter failure, you include physical NICs in a failover order. To determine how the virtual switch distributes the network traffic between the physical NICs in a team, you select load balancing algorithms depending on the needs and capabilities of your environment.

NIC Teaming Policy - You can use NIC teaming to connect a virtual switch to multiple physical NICs on a host to increase the network bandwidth of the switch and to provide redundancy. A NIC team can distribute the traffic between its members and provide passive failover in case of adapter failure or network outage. You set NIC teaming policies at **virtual switch** or **port group level** for a vSphere Standard Switch and at a **port group** or **port level** for a vSphere Distributed Switch.

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

Check the **vSphere Networking PDF** for more details. You'll learn more about:

- VLAN policy
- Security policy
- Traffic shaping policy
- Resource allocation policy
- Monitoring policy
- Traffic filtering and marking policy
- Port blocking policy

We simply can't squeeze all the networking knowledge into a single post or single study guide. I'd recommend also consulting the VCP6.5-DCV Study Guide page (or get the full PDF here) where you can find other chapters concerning networking in vSphere, further detailed:

- Configure policies/features and verify vSphere networking
- Configure Network I/O control (NIOC)
- Troubleshoot vSphere Storage and Networking

Some best practices - Dedicate a separate physical NIC to a group of virtual machines, or use Network I/O Control and traffic shaping to guarantee bandwidth to the virtual machines.

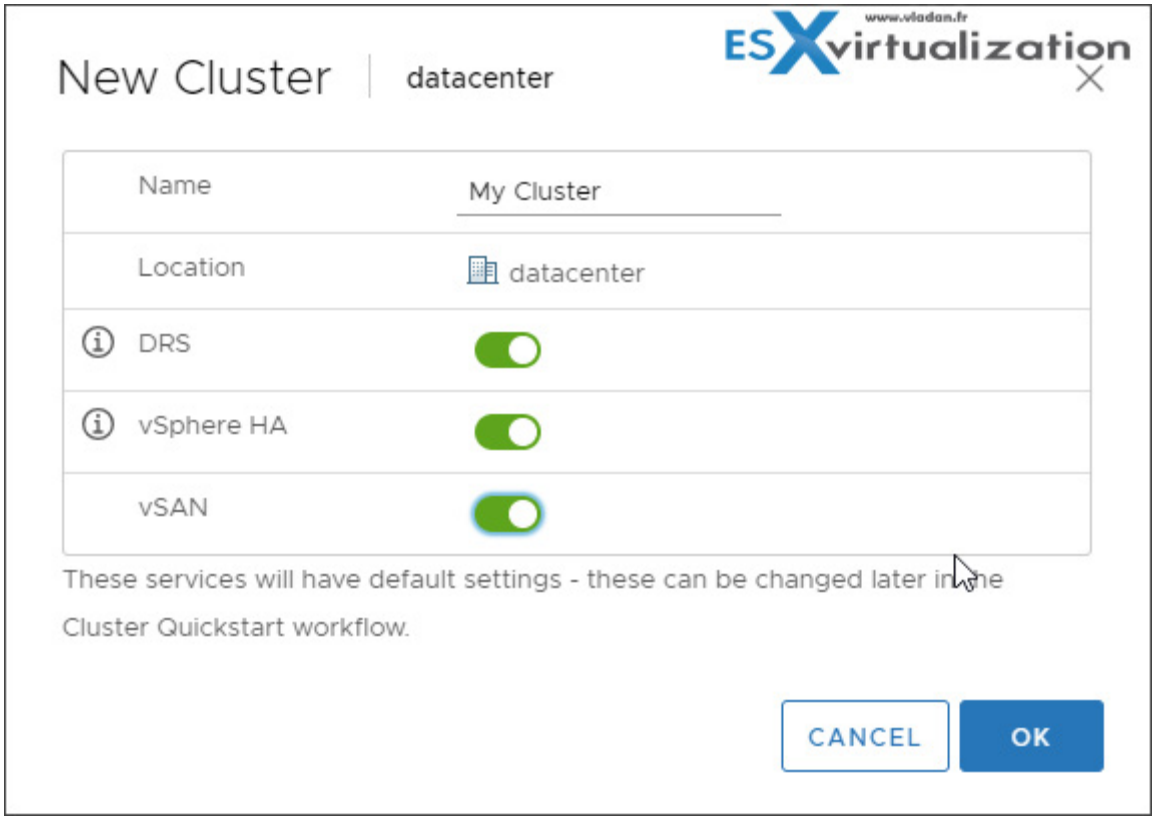
To physically separate network services and to dedicate a particular set of NICs to a specific network service, create a vSphere Standard Switch or vSphere Distributed Switch for each service. If this is not possible, separate network services on a single switch by attaching them to port groups with different VLAN IDs.

Keep the vSphere vMotion connection on a separate network. When migration with vMotion occurs, the contents of the guest operating system's memory are transmitted over the network. You can do this either by using VLANs to segment a single physical network or by using separate physical networks (the latter is preferable).

Objective 1.9 - Describe the purpose of a cluster and the features it provides

A cluster is basically a group of hosts which manage the resources of all hosts within it. When a host is added to a cluster, the host's resources become part of the cluster's resources. Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.

As said earlier, a cluster is created at the datacenter level. One vCenter can manage several datacenters, and inside of each datacenter you can have several clusters, each active with different services (DRS, HA, VSAN, etc.).



VMware High Availability (HA) - VMware HA continuously monitors all servers in a resource pool and detects server failures. An agent placed on each server maintains a “heartbeat” with the other servers in the resource pool and a loss of “heartbeat” initiates the restart process of all affected virtual machines on other servers.

VMware HA makes sure that sufficient resources are available in the resource pool at all times to be able to restart virtual machines on different physical servers in the event of server failure. Restart of virtual machines is made possible by the Virtual Machine File System (VMFS) clustered file system which gives multiple ESXi Server instances read-write access to the same virtual machine files, concurrently.

VMware HA is easily configured for a resource pool through vCenter.

Key Features of VMware HA

- Automatic detection of server failures. Automate the monitoring of physical server availability. HA detects server failures and initiates the virtual machine restart without any human intervention.
- Resource checks. Ensure that capacity is always available in order to restart all virtual machines affected by server failure. HA continuously monitors capacity utilization and “reserves” spare capacity to be able to restart virtual machines.

VMware High Availability (HA) provides easy to use, cost-effective high availability for applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other production servers with spare capacity.

By activating HA, you basically minimize downtime and IT service disruption while eliminating the need for dedicated stand-by hardware and installation of additional software. You also provide uniform high availability across the entire virtualized IT environment without the cost and complexity of failover solutions tied to either operating systems or specific applications.

How does HA work?

When you create a vSphere HA cluster, a single host is automatically selected as the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and slave hosts.

When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster. Each host in the cluster functions as a master host or a subordinate host (often called a “slave”).

HA protects against downtime. Which kind of problems are you protected from?

In a vSphere HA cluster, three types of host failure are detected:

- **Failure** - A host stops functioning.
- **Isolation** - A host becomes network isolated.
- **Partition** - A host loses network connectivity with the master host.

This communication happens through the exchange of network heartbeats every second. When the master host stops receiving these heartbeats from a subordinate host, it checks for host liveness before declaring the host failed. The liveness check that the master host performs is to determine whether the subordinate host is exchanging heartbeats with one of the datastores (see Datastore Heartbeating). Also, the master host checks whether the host responds to ICMP pings sent to its management IP addresses.

Failures and responses – you can configure how vSphere HA responds to failure conditions on a cluster.

There are 4 Failure conditions:

- **Host** – allows you to configure host monitoring and failover on the cluster. ("**Disabled**" or "**Restart VMs**" – VMs will be restarted in the order determined by their restart priority).
- **Host Isolation** – allows you to configure the cluster to respond to host network isolation failures:
  - **Disabled** – No action will be taken on the affected VMs.
  - **Shut down and restart VMs** – All affected VMs will be gracefully shut down and vSphere HA will attempt to restart the VMs on other hosts online within the cluster.
  - **Power Off and Restart VMs** – All affected VMs will be powered Off and vSphere HA will attempt to restart the VMs on the hosts which are still online.
- **VM component protection** – datastore with Permanent Device Lost (PDL) and All paths down (APD):
  - **Datastore with PDL** – allows you to configure the cluster to respond to PDL datastore failures.
    - *Disabled* – no action will be taken to the affected VMs.
    - *Issue events* – no action to the affected VMs. Events will be generated only.
    - *Power Off and restart VMs* – All affected VMs will be terminated and vSphere HA will attempt to restart the VMs on hosts that still have connectivity to the datastore.
  - **Datastore with APD** – allows you to configure the cluster to APD datastore failures.
    - *Disabled* – no action will be taken to the affected VMs.
    - *Issue Events* – no action taken to the affected VMs. Events will be generated only.
    - *Power Off and restart VMs* – All affected VMs will be terminated and vSphere HA will attempt to restart the VMs if another host has connectivity to the datastore.
    - *Power Off and restart VMs – Aggressive restart policy* – All affected VMs will be powered Off and vSphere HA will **always** attempt to restart VMs.
  - **VM and application monitoring** – VM monitoring hard restarts of individual VMs if their VM tools heartbeats are not received within a certain time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

Admission Control

Admission control is a policy which is used by vSphere HA to make sure that there is enough failover capacity within a cluster.

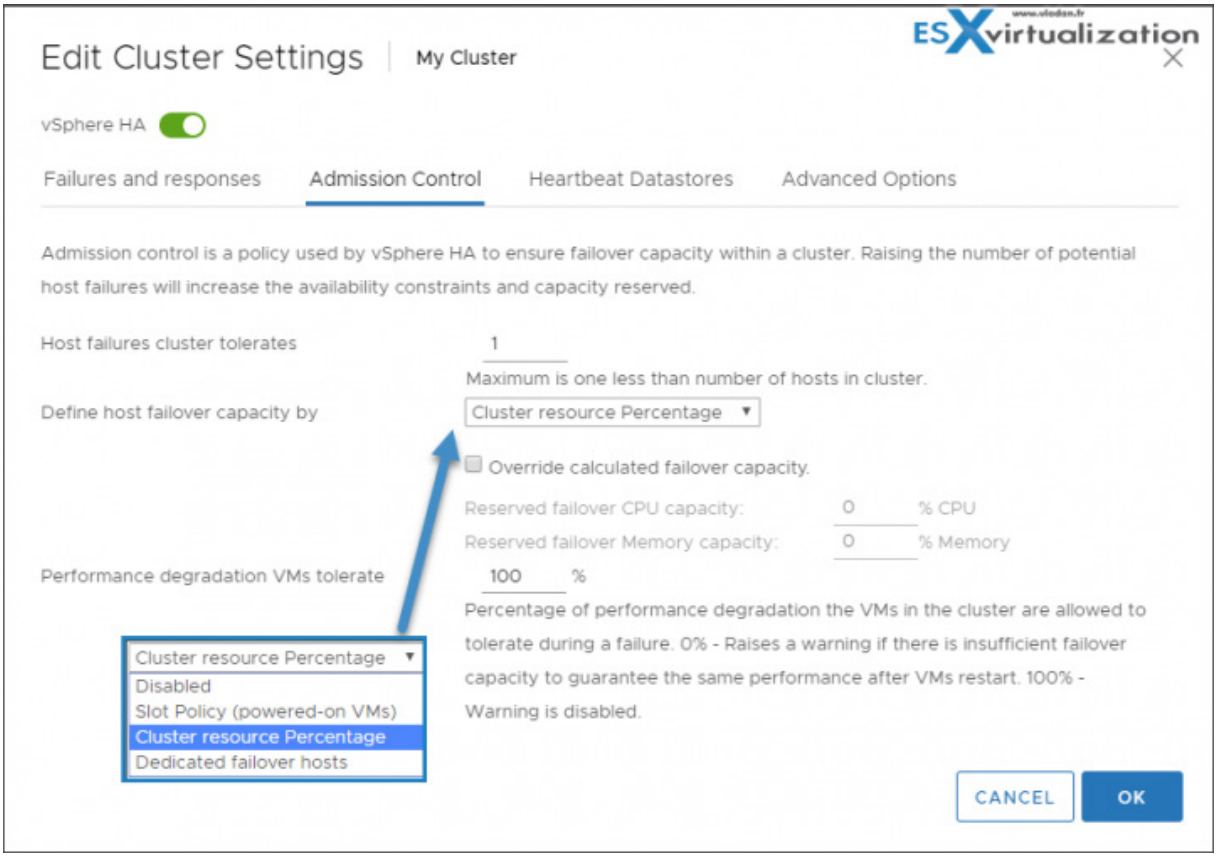
- **Cluster resource Percentage** (default) – The configuring workflow for admission control is a little bit simpler. You first define the parameter of how many failed hosts you want to tolerate within

your cluster, and the system will do the math for you. As default HA cluster admission policy, VMware will use the **cluster resource Percentage** now (previously, the cluster tolerates policy was used).

- **Override Possible** – You can override the default CPU and memory settings if needed (25% as in previous releases).

Performance degradation Warning message – Previously HA could restart a VM, but those would suffer from performance degradation. Now you have a warning message which informs you about it. You'll be warned if performance degradation would occur after an HA even for particular VM(s).

0% – Raises a warning if there is insufficient failover capacity to guarantee the same performance after VMs restart.
100% – Warning is disabled



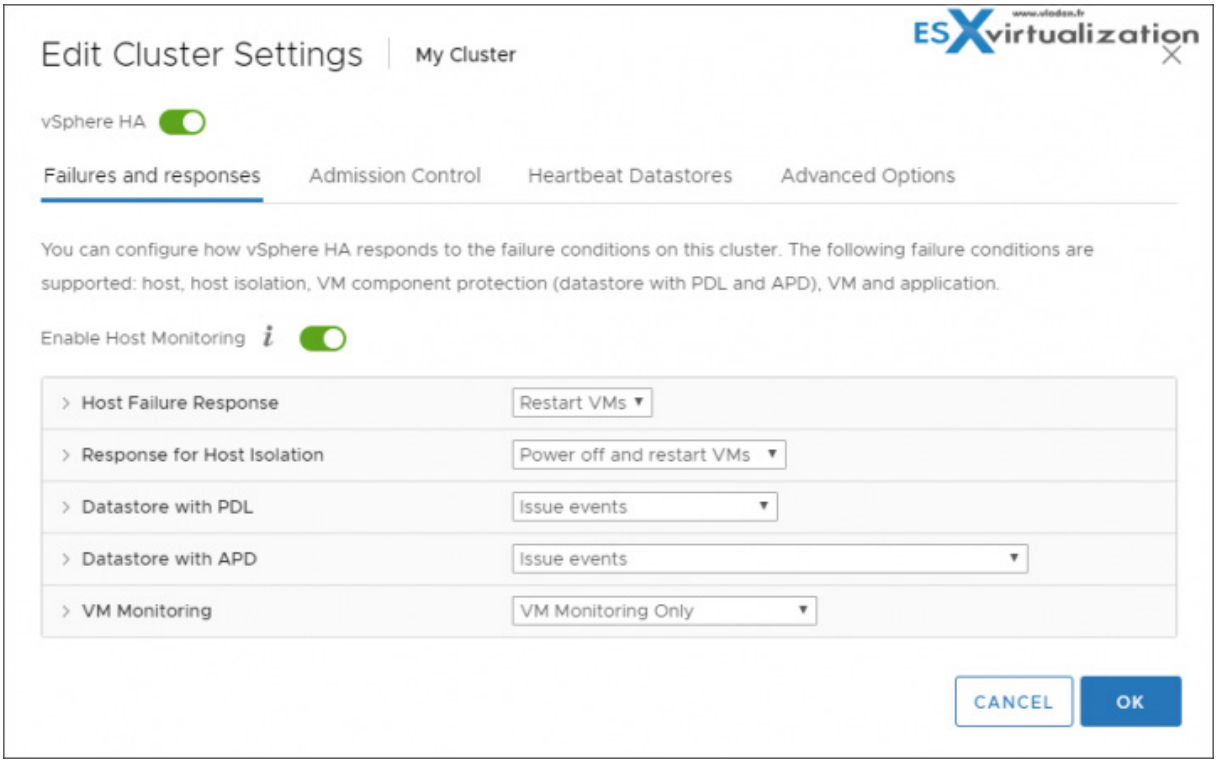
Apart from the cluster resource percentage policy, there are "Slot policy" and "Dedicated failover host" policies.

- **Slot policy** – the slot size is defined as the memory and CPU resources that satisfy the reservation requirements for any powered-on VMs in the cluster.

- **Dedicated Failover Host** – You pick a dedicated host which comes into play when there is a host failure. This host is a "spare" so it does not have running VMs during normal operations. Waste of ressources.

Enable/disable vSphere HA settings

To enable vSphere HA, open vSphere Client > **Select cluster** > Configure > **vSphere Availability** > Click **Edit** button.



vSphere DRS

VMware vSphere Distributed Resource Scheduler (DRS) is a resource scheduler. It monitors and can react to changes in VM workloads. The system can migrate VMs to other hosts in order to distribute the load.

DRS automatically places virtual machines onto hosts at VM power-on, and virtual machines are automatically migrated from one host to another to optimize resource utilization.

DRS affinity rules

You can control the placement of virtual machines on hosts within a cluster by using affinity rules. Certainly, this is useful if you wish for two or more VMs to run on the same host(s).

You can create two types of rules.

VM-Host affinity rule – specifies an affinity relationship between a group of virtual machines and a group of hosts. There are **required** rules (designated by "**must**") and 'preferential' rules (designated by "**should**".)

An affinity rule specifies that the members of a selected virtual machine DRS group can or must run on the members of a specific host DRS group. An anti-affinity rule specifies that the members of a selected virtual machine DRS group cannot run on the members of a specific host DRS group.

A VM-Host affinity rule includes the following components:

- One virtual machine DRS group.
- One host DRS group.

VM-VM affinity rule – determines whether VMs should run on the same host or be kept on separate hosts.

With an anti-affinity rule, DRS tries to keep the specified virtual machines apart. You can use such a rule if you want to guarantee that certain virtual machines are always on different physical hosts. In that case, if a problem occurs with one host, not all virtual machines will be placed at risk.

A rule specifying affinity causes DRS to try and keep the specified virtual machines together on the same host, for example, for performance reasons. With an anti-affinity rule, DRS tries to keep the specified virtual machines apart, for example, so that when a problem occurs with one host, you do not lose both virtual machines.

When you add or edit an affinity rule, and the cluster's current state is in violation of the rule, the system continues to operate and tries to correct the violation. For manual and partially automated DRS clusters, migration recommendations based on rule fulfillment and load balancing are presented for approval. You are not required to fulfill these rules, but the corresponding recommendations remain until the rules are fulfilled.

To check whether any enabled affinity rules are being violated and cannot be corrected by DRS, select the cluster's DRS tab and click Faults. Any rule currently being violated has a corresponding fault on this page. Read the fault to determine why DRS is unable to satisfy the particular rule. Rules violations also produce a log event.

Starting vSphere 6.5, DRS no takes into consideration also the network utilization. It takes into account the network utilization of host and network usage requirements of VMs during initial placement and load balancing. As a result, load balancing and DRS is more "intelligent".

DRS does the initial placement in two steps:

- It compiles a list of possible hosts based on cluster constraints and computes resource availability and ranks them.
- Then, from the list of hosts, it picks the host with the best rank and best network resource availability

Predictive DRS - Predictive DRS happens when a vCenter server proactively rebalances the VMs based on predictive patterns in the cluster workload. Predictive DRS bases its data provide by vRealize Operations Manager.

vROPS monitor VMs running within a vCenter server and analyzes the historical data. Based on this, it can forecast data, and predictable patterns of resources usage.

This data is used by predictive DRS, which moves VMs around based on the patters.

Objective 1.10 - Describe a virtual machine (VM) file structure

Today we'll detail another objective of **VCP-DCV 2019 Certification** – **Objective 1.10 - Describe a virtual machine (VM) file structure**.

So, let's get started. For this lesson, we're using the "Virtual Machine Administration" PDF. Check the **VCP6.7-DCV Study Guide Page** for the whole documentation set.

Here are the principal files contained in each VM.

Table 1-1. Virtual Machine Files

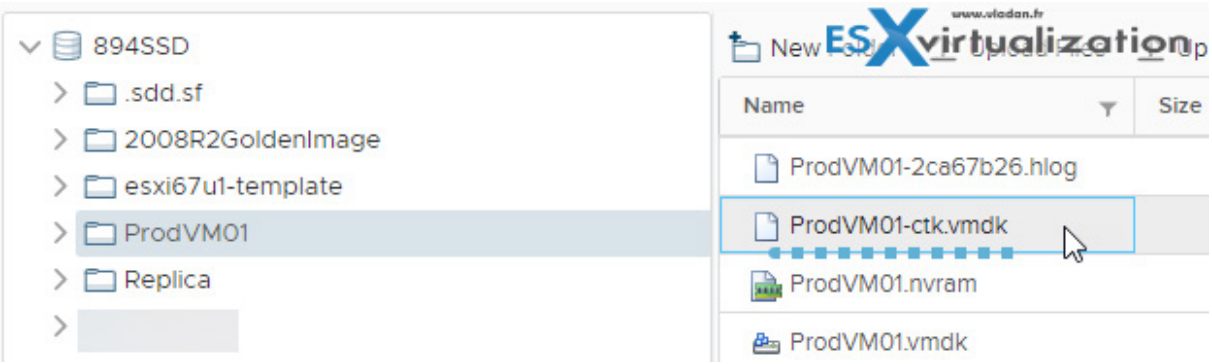
File	Usage	Description
.vmx	*vmname*.vmx	Virtual machine configuration file
.vmxf	*vmname*.vmxf	Additional virtual machine configuration files
.vmdk	*vmname*.vmdk	Virtual disk characteristics
-flat.vmdk	*vmname*-flat.vmdk	Virtual machine data disk
.nvram	*vmname*.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmsd	*vmname*.vmsd	Virtual machine snapshots
.vmsn	*vmname*.vmsn	Virtual machine snapshot data file
.vswp	*vmname*.vswp	Virtual machine swap file
.vmss	*vmname*.vmss	Virtual machine suspend file
.log	vmware.log	Current virtual machine log file
-#.log	vmware-#.log (where # is a number starting with 1)	Old virtual machine log files

You then have some additional files created after VM runs for a while.

- A file called **.hlog file** is a log file that is used by vCenter Server to keep track of virtual machine files which must be removed after a certain operation a complete.
- Another file called **.vmtx file** is created when you convert a virtual machine to a template. The .vmtx file replaces the virtual machine configuration file (.vmx file).

What is VMware CTK, and what's inside the file?

CTK file is also inside the VM folder. The CTK file is used by Changed Block Tracking (CBT). It lists the block changes made since the last backup. The first backup of a VM has to be a full backup—only then onwards does the CBT read the content of the CTK file, and back up changed blocks only instead of a full VM backup. Every block has got a time stamp which says where the location of the modified block is.



The size of this file is fixed and does not grow beyond its initial size. Only if you grow the size of a virtual disk can the size of CTK file change. The real size of this CTK file depends on the size of a virtual disk, but it's about .5MB for every 10 GB of virtual disk size.

The CTK's file content stores the state of each block, for tracking purposes, and uses sequence numbers. Those sequence numbers are used by a backup application, to see if a block has changed its state or not.

A file with extension CTK can be found by using the VMware datastore browser, in the same folder as the other VMDK file, where the VM stores all its files (VMDK, VMX, VMSD, NVRAM....).

If you don't see the CTK file, it means that the CBT just isn't activated. The CBT functionality is available for VMs with the virtual hardware version isn't 7 and higher.

The CBT is usually activated by backup products, like Veeam or VDP automatically during the first backup. The CBT can also be activated manually, through the vSphere web client and Advanced settings of the VM, OR, editing directly the configuration file of a particular VM (VMX file).

The Snapshot Structure

When a virtual machine snapshot is created, all attached disks are snapshotted simultaneously. So there will be one delta disk per virtual machine disk, per snapshot.

The files on the datastore look like this (represents a VM with 3 snapshots):
/vmfs/volumes/datastore1/examplevm/examplevm-000001.vmdk
/vmfs/volumes/datastore1/examplevm/examplevm-000002.vmdk
/vmfs/volumes/datastore1/examplevm/examplevm-000003.vmdk
...
/vmfs/volumes/datastore1/examplevm/examplevm.vmdk
/vmfs/volumes/datastore1/examplevm/examplevm.vmx

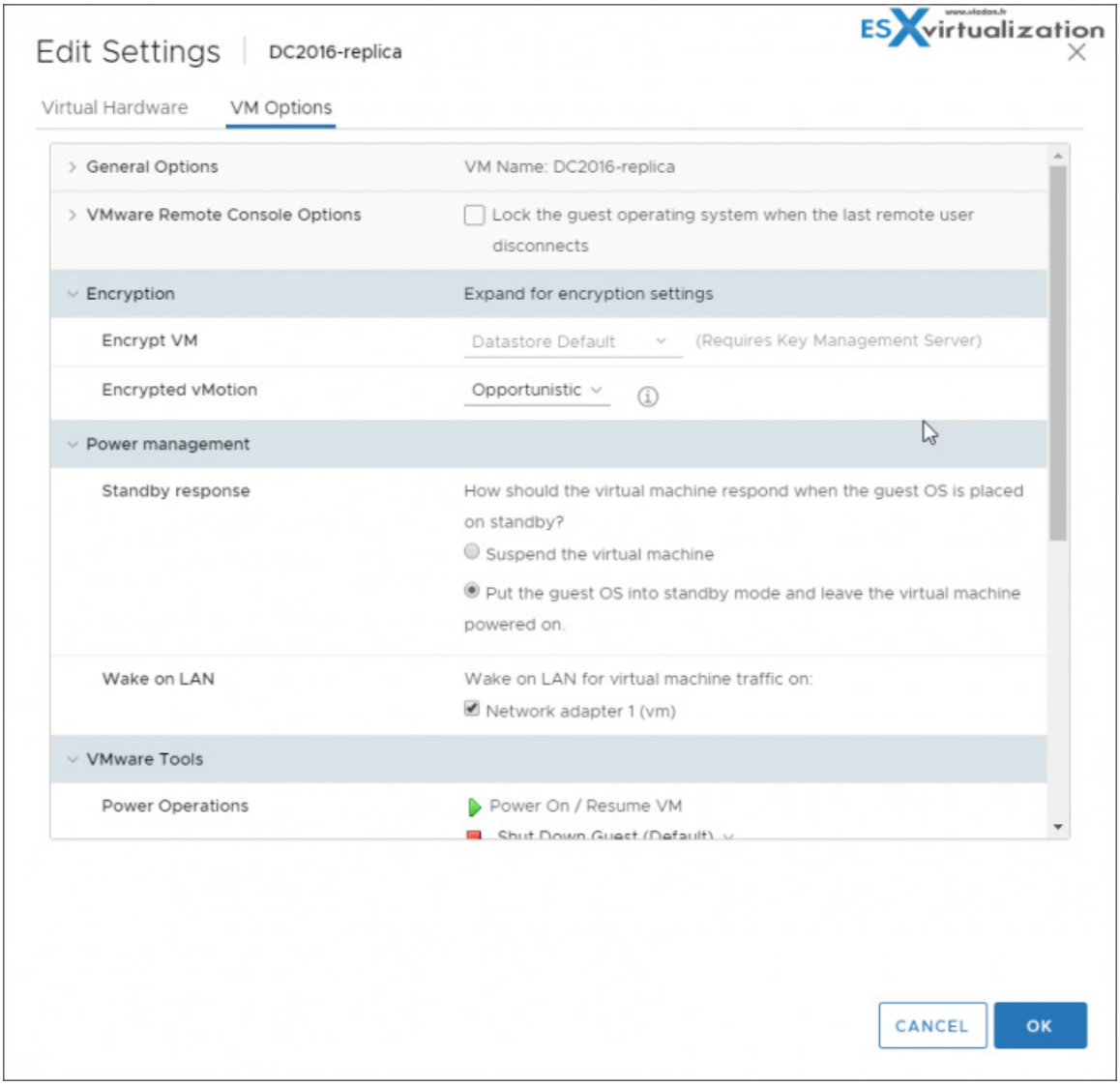
Virtual Machine Hardware Available to vSphere Virtual Machines

Check vSphere “Virtual Machine Administration” PDF page 13.

Virtual Machine Options

Virtual machine options will allow you to fine-tune the settings and behavior of your virtual machine to ensure maximum performance.

- **General Options** - modify the name, check the config file and working location.
- **Encryption Options** - you can enable encryption for the VM (which needs a Key management server not available from VMware, but through a partner).
- **Power management** - Suspend the virtual machine or leave the virtual machine powered on when you put the guest operating system into standby.
- **VMware Tools** - power controls for the virtual machine and run VMware Tools scripts. You can also upgrade VMware Tools during power cycling and synchronize guest time with the host.
- **Virtualization-based security** - you can enable VBS to add an additional level of protection



- **Boot Options** - you can set the boot delay when powering ON.
- **Advanced Options** - Disable acceleration and enable logging, configure debugging and statistics, and change the swap file location. You can also change the latency sensitivity and add configuration parameters. Also, you can enable or disable Change block tracking (CTK).
- **Fibre channel NPIV** - control VMs access to LUNs on a per-VM basis.
- **vApp Options** - enable or disable vApp Options. You can view and edit vApp properties, vApp Deployment options, and vApp Authoring options.

Objective 1.11 - Describe vMotion and Storage vMotion technology

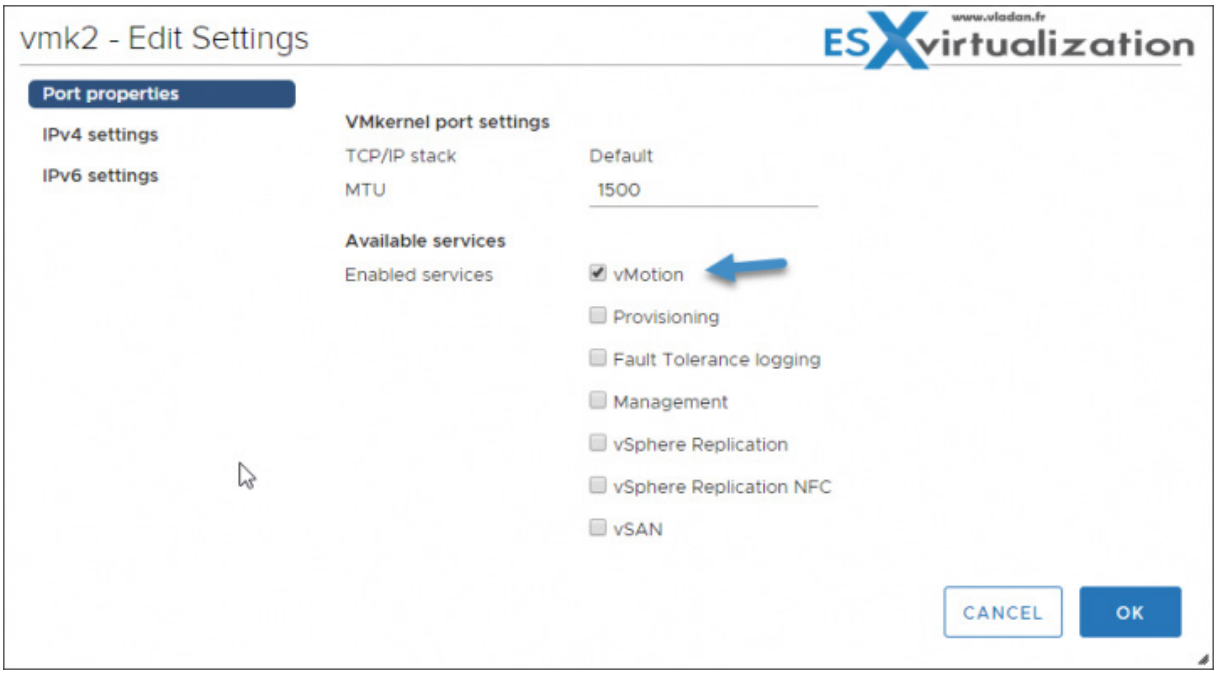
As you know, these two technologies allow you to move workloads from one host to another, from one datastore type to another, without downtime.

Both need to be properly licensed and configured. The configuration can vary depending on many parameters (networks, hardware, etc).

Migration of VMs powered ON is called vMotion. (hot migration). Depending on the power state of the virtual machine that you migrate, migration can be cold or hot.

You should make sure that VMware vSphere vMotion traffic does not travel over networks where virtual machines are located. It should be either separated by VLANs or on a dedicated network. vSphere infrastructure networks are used for features such as vSphere vMotion, VMware vSphere Fault Tolerance, and storage. Isolate these networks for their specific functions.

Example of activation of vMotion traffic on a vmkernel port.



VMware vMotion - with vSphere vMotion, you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to collocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements so that the migration can proceed.

We often talk about hot migration, but there is also cold migration which allows you to simply move the VM which is powered OFF.

vMotion has 3 Phases:

- **Phase 1** - vMotion is requested. vCenter server checks whether the existing VM is in a stable state with its current host.
- **Phase 2** - VM state info (memory, registers and network connections) are copied to the target host.
- **Phase 3** - VM resumes its activities on the new host.

vMotion Requirements:

- The host must be licensed for vMotion.
- The host must meet shared storage requirements.
- The Host must meet networking requirements for vMotion.

vMotion Migration Types

vMotion (traditional) - you change computer resource only. When you migrate virtual machines with vMotion and choose to change only the host, the entire state of the virtual machine is moved to the new host. The associated virtual disk remains in the same location on storage that must be shared between the two hosts.

Long-distance vMotion - sites that are separated by high network roundtrip latency times. vMotion across long distances is enabled when the appropriate license is installed. No user configuration is necessary. Round trip < 150 ms, License for vMotion Long distance.

Migrate to another datacenter - by using cold or hot migration. For destination networking, you can select a dedicated port group on a distributed switch.

Migrate to another vCenter server - via vCenter Enhanced Linked Mode (ELM). Across a long distance too.

Storage vMotion - You move your VM from one storage to another without downtime, and change the datastore. The virtual machine state, its VMDKs and associated files, are moved to another datastore; a proper license is required. The host on which the virtual machine is running must have access to both the source and target datastores.

Note: Regarding storage vMotion limitations, virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thin-provisioned disks during migration if the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.

vMotion without shared storage - you can vMotion VMs to a different host and storage. This is useful for performing cross-cluster migrations when the target cluster machines might not have access to the source cluster's storage.

Transferred State Information - Includes current memory content and the info about the VM. Memory content has transaction data and the parts of OS and applications which are currently running in the memory. The defining and identification information stored in the state includes all data that maps to the virtual machine hardware elements. This information includes BIOS, devices, CPU, MAC addresses for the Ethernet cards, chipset states, registers etc.

Limits on simultaneous migrations - vCenter places limits on the number of simultaneous VM migrations. Those limits apply on **a host, network and datastore**.

Host Migration Limits and Resource Costs for vMotion, Storage vMotion, and Provisioning Operations

Operation	ESXi Version	Derived Limit Per Host	Host Resource Cost
vMotion	5.0, 5.1, 5.5, 6.0	8	1
Storage vMotion	5.0, 5.1, 5.5, 6.0	2	4
vMotion Without Shared Storage	5.1, 5.5, 6.0	2	4
Other provisioning operations	5.0, 5.1, 5.5, 6.0	8	1

- **Network limit** - On 1GbE it is 4, and on 10GbE it is 8. Network limits depend on the version of ESXi and the network type.
- **Datastore limit** - 128 per datastore. Apply to migrations with vMotion and with Storage vMotion.
- **Host Limit** - apply to migrations with vMotion, Storage vMotion, and other provisioning operations such as cloning, deployment, and cold migration. All hosts have a maximum cost per host of 8.

Migrations of suspended virtual machines are also possible. However, the VM has to be able to resume execution on the target host using equivalent instructions.

When you initiate a migration with vMotion or migration of a suspended virtual machine, the Migrate Virtual Machine wizard checks the destination host for compatibility. If compatibility problems prevent migration, the wizard displays an error message.

vMotion might need Enhanced vMotion Capability (EVC) configured at the cluster level when your cluster has different hardware (and CPU). Every new processor, for example, Intel, releases a new set of instructions that are not, as you can imagine, backward compatible with previous generations of CPUs. This is why we need to "mask" these new capabilities within our cluster to retain our vMotion capability. We hide the newer instructions within vCenter Server.

As a result, EVC presents a homogeneous processor front to all the virtual machines (VMs) in a cluster. This allows us to take vMotion from, for example, Intel's Sandy Bridge-based host into a Haswell-based host.

However, do note that CPUs must be from a single vendor, for example, only from Intel or only from AMD. You cannot mix and match both and still expect to configure EVC for vMotion to work—it simply does not.

Objective 2.1 - Describe vSphere integration with≈other VMware products

This topic can be interpreted in a number of different ways. An integration of different VMware products usually means that vSphere has integration modules with other VMware products such as VMware Horizon, VMware VSAN, VMware Site Recovery Manager (SRM) and others. In keeping, these products work in conjunction with vCenter in some way.

VMware vSphere and the management, administration, VM's creation and backup, is all done through vCenter server. However, other products in the vSphere suite can do other tasks that vCenter server itself cannot or else they use the vCenter server for executing tasks.

vRealize Orchestrator (vRO) - is a development- and process-automation platform that provides an extensive library of workflows and a workflow engine. Workflows achieve step-by-step process automation for greater flexibility in automated server provisioning and operational tasks across VMware and third-party applications. By using the workflow editor, the built-in Mozilla Rhino JavaScript scripting engine, and the Orchestrator and vCenter Server APIs, you can design custom workflows in just a few clicks.

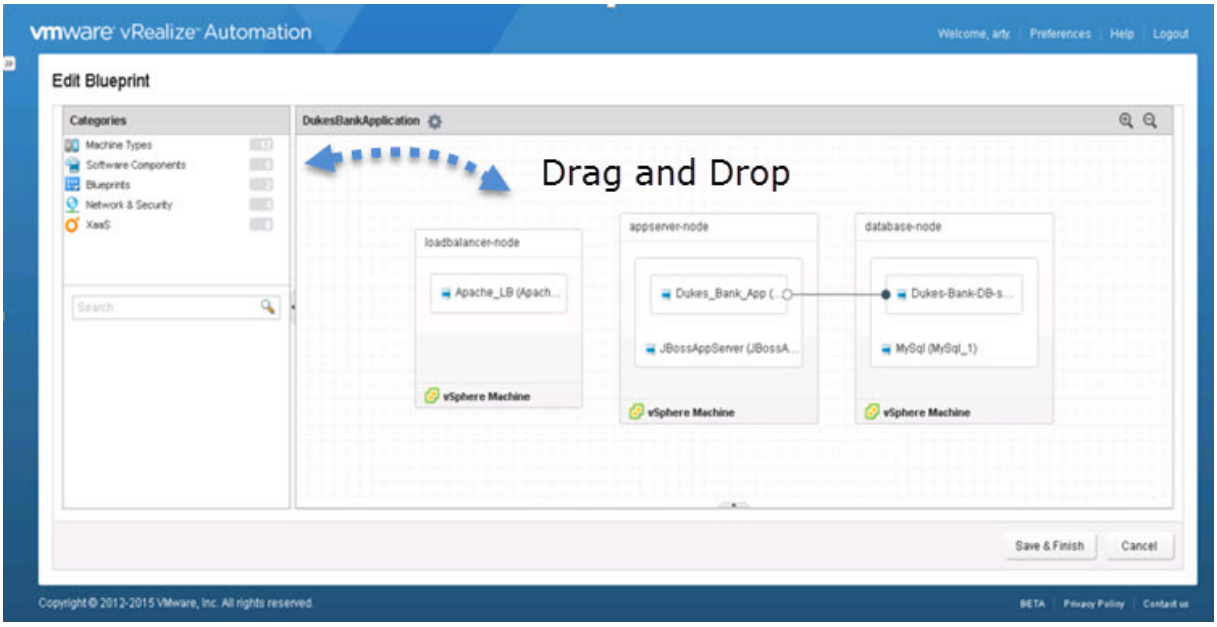
vRO allows for IT automation in vSphere and makes the automation process more user-friendly. With a few mouse clicks, you can build a new workflow. There are also pre-built workflows as well. Moreover, vRO allows for launching workflows within the VMware Cloud Suite.

vRealize Automation (vRA) - VMware vRealize Automation provides a secure portal where authorized administrators, developers, or business users can request new IT services. In addition, they can manage specific cloud and IT resources that enable IT organizations to deliver services that can be configured to their lines of business in a self-service catalog.

Check out more at the product's **documentation page**.

There is a Converged Blueprint Designer, which is simplified blueprint authoring for IaaS and Applications, allowing for drag-and-drop operations. On the left, you choose the category, and within the category, you choose what you wish to drag on the canvas.....

App services which have been a separate appliance are now incorporated into the blueprint designer.



vRealize Automation and vRealize Orchestrator are separate products, but they work so well in tandem. In essence, vRA and vRO allow you to fulfill requests for infrastructure resources in an automated fashion. The step-by-step process can be broken down by which technology fulfills that portion of the request.

VMware NSX for vSphere (NSX-V) - NSX for vSphere offers logical switching, in-kernel routing, in-kernel distributed firewalling, and edge-border L4-7 devices that offer VPN, load balancing, dynamic routing, and FW capabilities.

With the same principle as for the server virtualization – by creating a new **abstraction layer**. In fact, to provision networking, the configuration of physical switches has to be done manually, via the CLI, GUI etc...

The abstraction layer, which is the **network virtualization layer**, has objects like logical ports, logical switches, routers, distributed logical firewalls or virtual load balancers. VMware NSX makes those objects to be seen to the outside world similarly as in the compute virtualization you can see the virtual memory, virtual CPU or virtual storage.

VMware has **NSX-V** and **NSX-T**. Where NSX-V is tailored for environments running VMware vSphere, NSX-T is designed for multi-hypervisor environments. NSX-V is part of a software-defined data center and it requires a VMware vCenter server into which it is tightly integrated.

Moving forward, VMware recommends, especially for green fields deployments, opting for NSX-T. The new release also introduces a new set of wizards, allowing you to transition from NSX-V -o NSX-T and do in-place migrations.

One of the best use cases for NSX is Micro-segmentation. It allows your organization to move from a perimeter-centric security posture to a micro-segmented architecture with enhanced security and visibility.

VMware Site Recovery Manager (SRM) - You can create and perform **Test Recovery, Failover and also a Cleanup of recovery plans**. It uses policy-based protection and allows you to protect thousands of virtual machines (VMs) via centralized recovery plans managed from the vSphere Web Client. Use policy-driven automation and the SDDC architecture to simplify ongoing management.

SRM with Stretched Storage support allows:

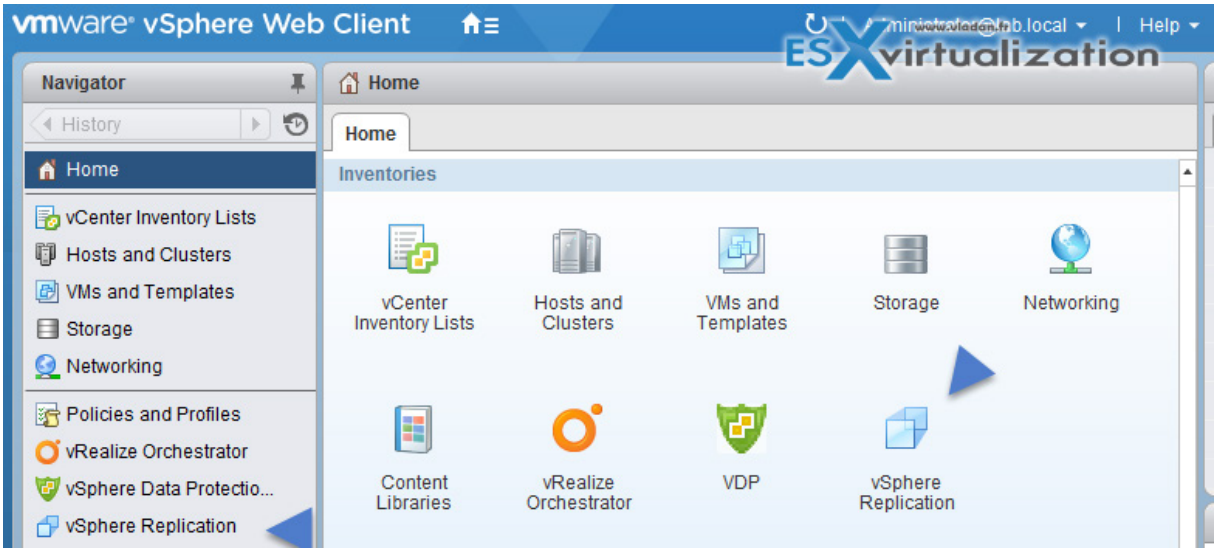
Planned maintenance downtime avoidance – using orchestrated cross-site vMotion and recovery plans.

Zero-downtime disaster avoidance – SRM 6.1 workflows + cross-site vMotion > VM is moved to another site to avoid upcoming disaster.

vSphere DATA Protection - phased out with vSphere 6.5.

vSphere Replication (VR) - used in conjunction with SRM, but can also be used separately from SRM. It is included with vSphere Essentials Plus and higher licensing, and allows replicate VMs from one datacenter onto another and has VMs ready to be powered ON in case of disaster on the primary site.

Screenshot from the previous release of vSphere.... vSphere 6.0



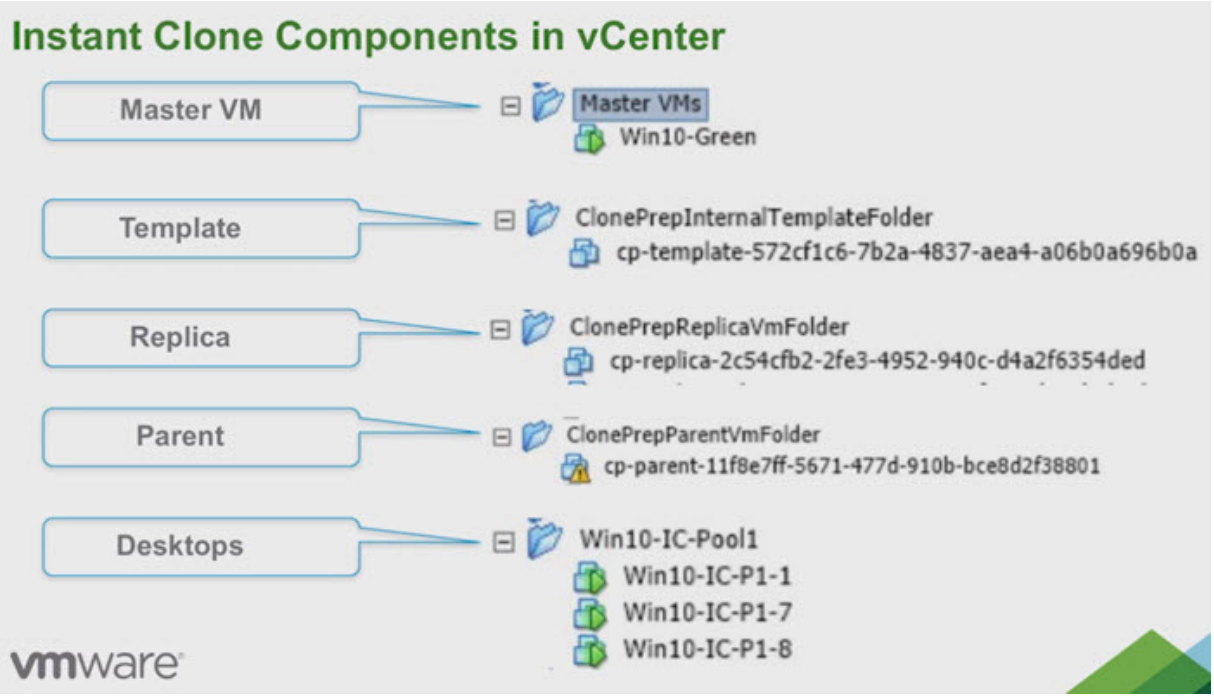
Failback is manual, meaning that after performing a successful recovery on the target vCenter Server site, you can perform failback. You log in to the target site and **manually configure a new replication in the reverse direction, from the target site to the source site.**

The disks on the source site are used as replication seeds, so that vSphere Replication only synchronizes the changes made to the disk files on the target site. Before you configure a reverse replication, you must unregister the virtual machine from the inventory on the source site.

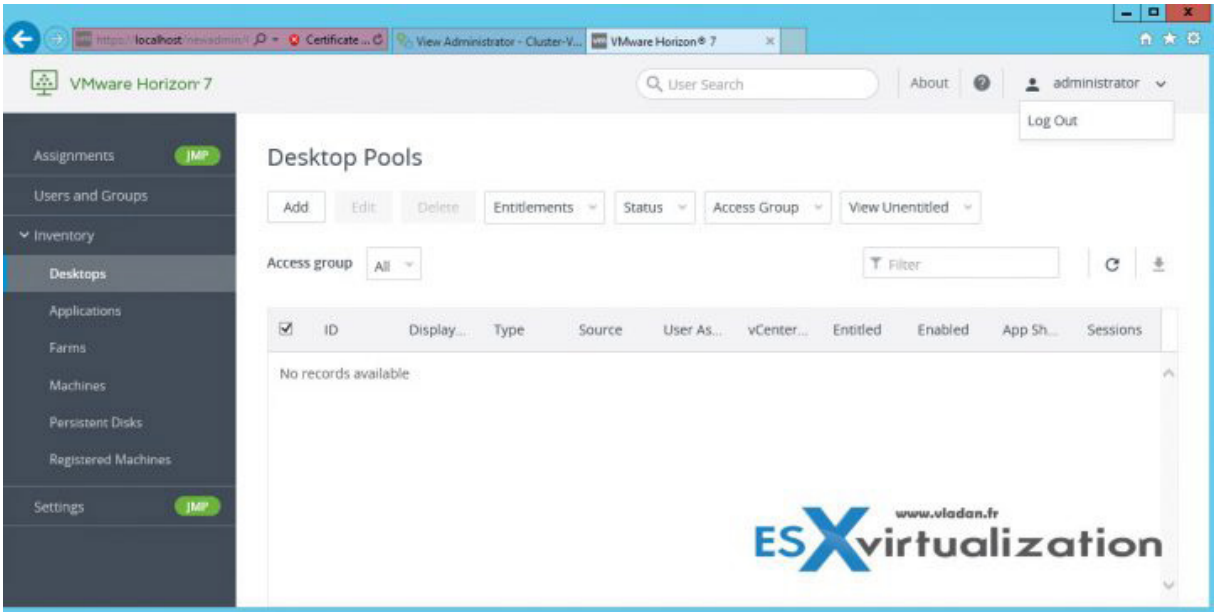
VMware Horizon Suite - a VMware VDI suite. This is the year of VDI, right? Horizon View is updated on a regular basis. VMware Horizon 7.7 has been released and we haven't reported on it yet. New support for **Windows Server 2019 for desktop and RDSH** VMs is here. It's been certainly functionality that many were waiting to start doing POC and testing. VMware Horizon 7.7 adds support for VMware vSphere 6.7 Update 1 and VSAN 6.7U1 as well.

Instant clone technology was announced as project Fargo back during VMworld 2014 and the first production systems began using it within Horizon View 7, with its new name – Instant Clones. Project Fargo uses a **copy-on-write architecture** similar to that of containers, meaning that if an application running in a child VM **tries to change a shared OS file**, a **copy of the shared file is created and stored in the child VM**. This way, all modifications made by the VM are isolated and unique only to it. Any newly created files that are saved by the VM would also be stored in the child VM and not in the parent.

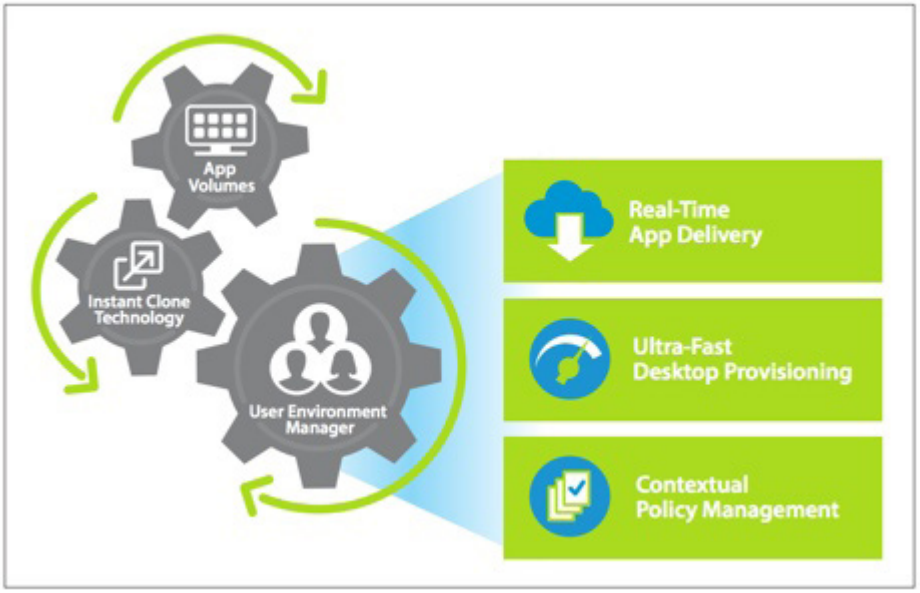
Instant Clone Technology is basically delivering VDI desktops "just in time," which is to say, instantly. Instant Clone Technology allows administrators to rapidly clone and deploy a virtual machine in much less time—just 1-2 seconds. The provisioning compared to traditional pool powered on by Composer server is also about 5-8 times faster.



Here is a screenshot from my **lab**.



Note: Horizon 7 Enterprise Edition includes all the same features as the Standard and Advanced Editions, and adds the JMP technologies: Instant Clone Technology, App Volumes, and User Environment Manager.



VMware Instant clone technology for VDI workloads and VDI environments allows for faster delivery of desktops combined with technologies such as App Volumes for fast application access without the need to install them. Overview from VMware PDF called Deploying VMware JMP

VMware Horizon Cloud Service integrates with Horizon 7 using the Horizon 7 Cloud Connector for on-premises and VMware Cloud on AWS deployments. With this integration, Horizon Cloud Service

provides a unified view into the health status and connectivity metrics for all of your cloud-connected pods. For more information, see the Horizon Cloud Service documentation.

Instant clones are supported on VMware Cloud on AWS. For a list of Horizon 7 features supported on VMware Cloud on AWS, see the VMware Knowledge Base article 58539.

VMware vSphere Integrated Containers – by now, you obviously know some things about containers technology, like how VMware has integration with Kubernetes. VMware has had fully supported Kubernetes with VMware Integrated OpenStack since 2017, where we reported on VMware Integrated Openstack 4.0 during VMworld 2017. However, this time the offering is more complete after their Heptio acquisition in November 2018 (we heard the announcement during last VMworld).

Heptio's technology orchestration and management has been renamed and now is part of **VMware Essential PKS**. So, you have basically 3 components – Kubernetes from Google, Heptio's technology (Contour, Sonobuoy, Velero) and VMware Support, all in the same package.

VMware vRealize Log Insight - a product which can ease some pain when searching through logs.

Objective 2.2 - Describe HA solutions for vSphere

In this post, we'll try to describe HA solutions for vSphere. It's here that VMware wants us to give an overview of High Availability and its usage within the enterprise, describing how this process works and what happens when a HA event gets triggered.

However, there might be another point which can apply to this chapter, and it is the vCenter Server appliance high availability (VCSA HA), since without vCenter, it's not possible to configure HA and other cluster functions. For this reason, we'll briefly cover this functionality of VCSA as well.

Moreover, vSphere HA is fully automatic, meaning that no admin or user interaction is necessary; vCenter is used only for configuration options. HA agents communicate without the need of having vCenter active or on-line.

VMware High Availability (HA) was first launched along with vCenter Server in 2003, the same year as other features such as VMotion, and Virtual SMP technology. The 64-bit support came in 2004.

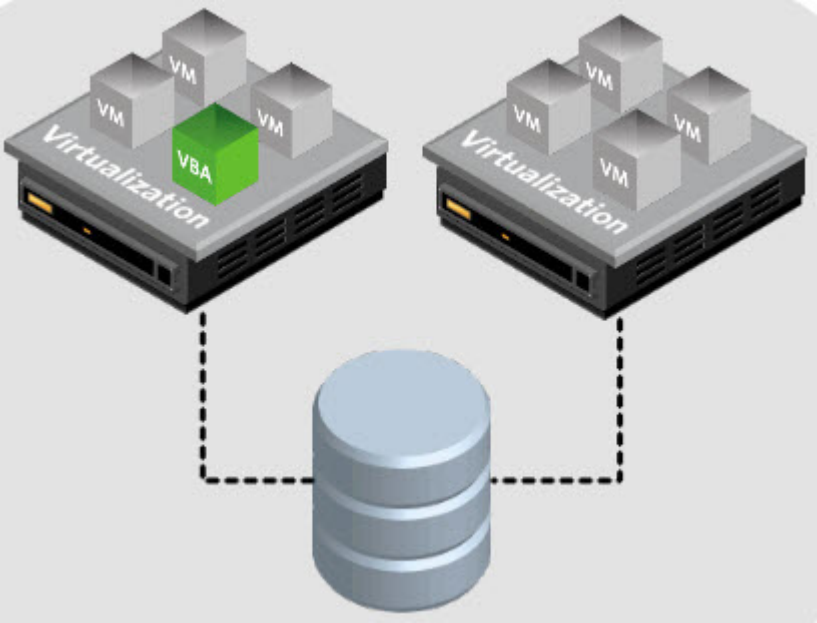
When a hardware problem occurs, it would be great to have some kind of mechanism that the VM can start on another host, right? That's exactly what VMware HA is all about. It provides an automatic start for VMs which were running on the failed host. Those VMs are started in sequences.

Let's assume we have two hosts and one external storage (this can be a SAN/NAS device) where those servers are connected to and you can see the shared storage from both servers at the same time.

The servers see the shared storage, access it at the same time, and read or write at the same time to the shared storage. (However, they cannot not write to individual VMs at the same time, because each

VM uses a locking mechanism. A long time ago, VMware invented a clustered storage system called VMFS which allows several servers to read and write to the shared storage at the same time.

We have our VM running on Server 1, connected to shared storage, and we also have Server 2 which is connected to that same shared storage. You can get a simple overview on the image below...



How Does VMware HA Work?

Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

The minimum number of hosts within a cluster is two. The VM which runs on the left (on our picture) will be able to be restarted automatically by VMware HA on the host which is on the right. All the files which the VM is composed, such as virtual disks (VMDK), a configuration file (VMX) and others **stay located on the shared storage** and do not move anywhere.

The only thing which happens after the host on the left crashes or experiences a hardware problem is that the VM starts automatically on the host on the right. (it's very simplified as explication though...)

Before you create a vSphere HA cluster, you should know how vSphere HA identifies host failures and isolation and how it responds to these situations. All hosts which are part of the HA cluster are monitored and in the case of a failure, the VMs on a failed host are restarted on surviving hosts within the cluster. The goals are to have more than 2 hosts, so the load can spread through the whole cluster, and that the VMs which will start on those hosts do not suffer from underperformance.

HA can protect you against host or network failure. Should the host get isolated, the response to this event can be configured distinctly so the VM can stay up and running (instead of killed and restarted elsewhere). Let's explore this for more details.

In a vSphere HA cluster, **three types of host failures** can be detected:

- **Failure** – When a host stops functioning.
- **Isolation** – When a host becomes network isolated.
- **Partition** – When a host loses network connectivity with the master host (there is only one "Master" host within the cluster, and it's who is responsible for monitoring the "slave" hosts within the cluster).

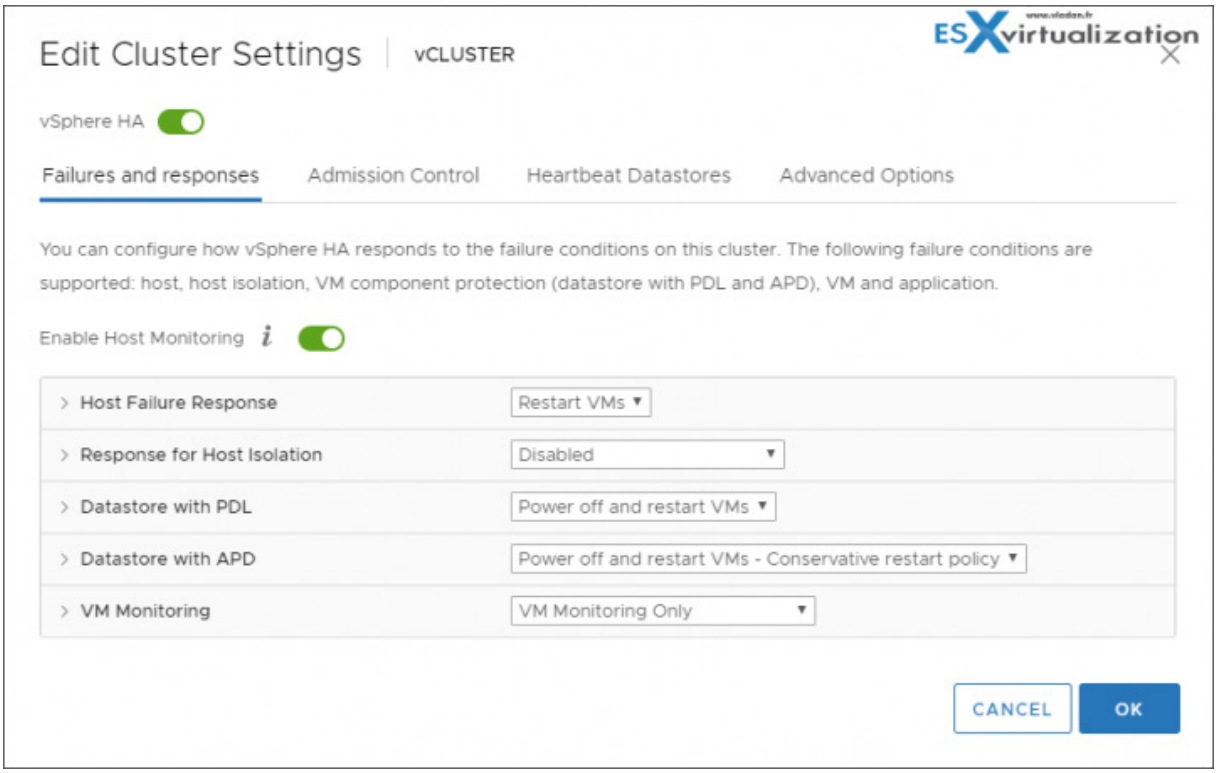
A Master and Slave concept.

There is one master host in the cluster. The master host verifies if a host responds to ICMP pings that were sent to its management IP addresses. If a master host cannot communicate directly with the agent on a slave host, the slave host does not respond to ICMP pings. If the agent is not issuing heartbeats, it is viewed as failed.

Quote:

When you create a vSphere HA cluster, a single host is automatically elected as the master host. The master host communicates with vCenter Server and monitors the state of all protected virtual machines and of the slave hosts. Different types of host failures are possible, and the master host must detect and appropriately deal with the failure. The master host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The master host uses network and datastore heartbeats to determine the type of failure.

The host's virtual machines are restarted on alternate hosts. If such a slave host is exchanging heartbeats with a data store (yes, you can configure datastore heart beating as a secondary channel), the master host assumes that the slave host is in a network partition or is network isolated. So, the master host continues to monitor the host and its virtual machines.



What are the Licensing Costs for HA?

The lowest cost edition which allows you to stay protected by VMware HA is **VMware Essentials Plus Term edition**. It is a Time limited license and contains the same features as in "Essentials Plus" but for 12 months only. As such, the price is much lower than the Essentials Plus (standard) edition.

VMware HA is configurable through an assistant, allowing you to specify several options. You'll need a VMware vCenter server running in your environment.

vCenter server High Availability (VCSA HA)

In order to protect vCenter Server, VMware has introduced a concept of vCenter Server appliance High Availability (VCSA HA). Do note that it's only for a vCenter server running on VCSA, not on Windows.

A vCenter HA cluster consists of three vCenter Server Appliance instances. The first instance, initially used as the **Active node**, is cloned twice to a **Passive node** and to a **Witness node**. Together, the three nodes provide an active-passive failover solution. The Witness VM is a lightweight VM maintaining just the witness components.

Things that are replicated between active and standby node:

- **Database** – The VCSA vPostgres database uses synchronous replication. It is a native vPostgres replication mechanism.
- **Flat files** – All configuration files, certificates, licensing info, etc. are replicated

Further reading from our VCP-DCV 2019 Study guide:

- VCP6.7-DCV Objective 1.9 – Describe the purpose of cluster and the features it provides
- VCP6.7-DCV Objective 1.6 – Describe and differentiate among vSphere, HA, DRS, and SDRS functionality

Objective 2.3 - Describe the options for securing a vSphere environment

This post will teach us about some security hardening features that vSphere possesses. Newly in vSphere 6.7 U2, a password history and reuse limits can now be applied.

This chapter can be broken down into a few main sub-chapters, where each one examines a different part of the infrastructure. There are best practices for securing ESXi, vCenter server, virtual machines or networking.

The fact that vSphere is secure by default is good to know, but further security settings are also possible. The ESXi hypervisor can further be configured and enabled by using lockdown mode and other features. You can also set up a host profile with security settings and then apply this to all your hosts in order to have a homogenous security environment.

By default, ESXi shell and SSH services are not running is for something. Risk increases when you use ESXi shell and SSH access to log in in remotely. You should always set timeouts to limit the risk of unauthorized access.

Also, the root user can do everything. You should not give the root access to everyone, but instead, you should create a named administrator user from the vCenter server and assign those users the Administrator (or a custom) role.

Check this chapter: VCP6.7-DCV Objective 7.4 – Configure host security

Securing ESXi Hypervisor

(check the post above) is one of the first options for securing a vSphere environment.

Securing vCenter Server Systems and Associated Services

One option for securing a vSphere environment is vCenter server itself. Let's talk about vCenter server accounts. If the local Windows administrator account currently has the Administrator role vCenter Server, remove that role and assign the role to one or more named vCenter Server administrator accounts.

Grant the Administrator role only to those administrators who are required to have it. You can create custom roles or use the No cryptography administrator role for administrators with more limited privileges. Do not apply this role to any group whose membership is not strictly controlled.

Not all administrator users need to have the Administrator role. Instead, you should create a custom role with the appropriate set of privileges and assign it to other administrators. Users with the vCenter Server Administrator role have privileges on all objects in the hierarchy. For example, by default the Administrator role allows users to interact with files and programs inside a virtual machine's guest operating system. Assigning that role to too many users can lessen virtual machine data confidentiality, availability, or integrity. Create a role that gives the administrators the privileges they need, but remove some of the virtual machine management privileges.

Minimize access to vCenter server machine.

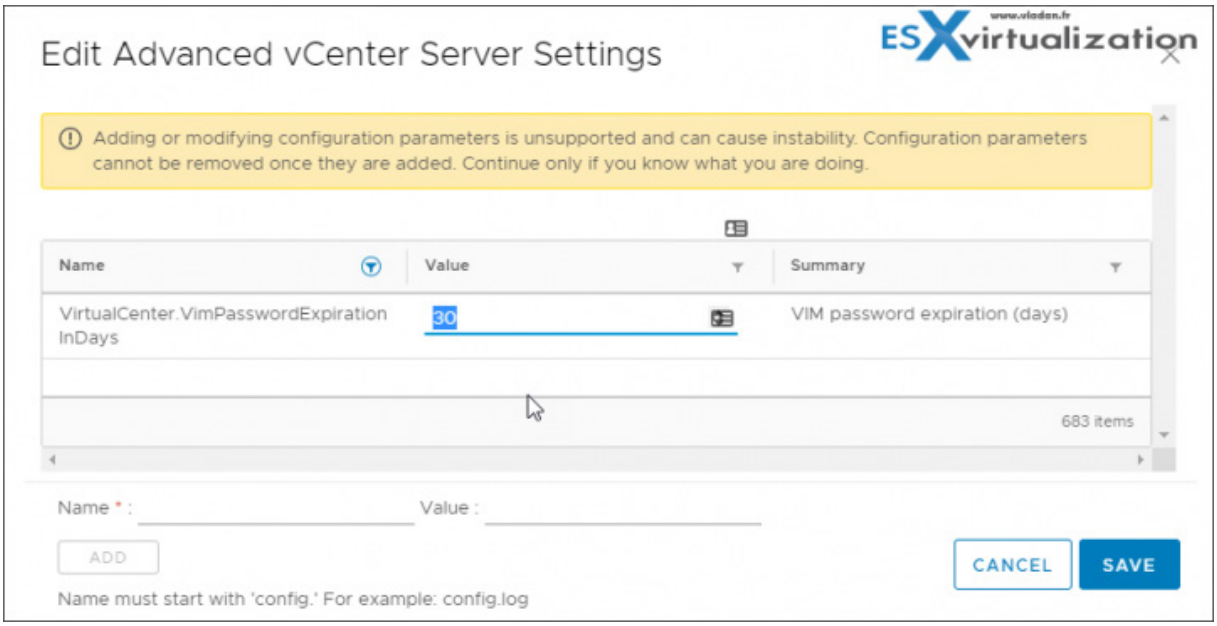
Restrict Datastore Browser Access - Assign the **Datastore.Browse** datastore privilege only to users or groups who really need those privileges. Users with this privilege can view, upload, or download files on datastores associated with the vSphere deployment through the Web browser or the vSphere Web Client.

By default, vCenter Server changes the vpxuser password automatically every 30 days. Ensure that this setting meets company policy, or configure the vCenter Server password policy.

Set the vCenter Server Password Policy - By default, vCenter Server changes the vpxuser password automatically every 30 days. You can change that value from the vSphere Web Client.

Log in to a vCenter Server system using the **vSphere Web Client** > **Select the vCenter Server system** in the object hierarchy > **Configure** > **Advanced Settings** and enter *VimPasswordExpirationInDays* in the filter box.

Then Set VirtualCenter.VimPasswordExpirationInDays to comply with your requirements.



Protect the vCenter server Windows host

- Maintain a supported operating system, database, and hardware for the vCenter Server system. If vCenter Server is not running on a supported operating system, it might not run properly, making vCenter Server vulnerable to attacks.
- Keep the vCenter Server system properly patched. By staying up-to-date with operating system patches, the server is less vulnerable to attack.
- Provide operating system protection on the vCenter Server host. Protection includes antivirus and anti-malware software.
- On each Windows computer in the infrastructure, ensure that Remote Desktop (RDP) Host Configuration settings are set to ensure the highest level of encryption according to industry-standard guidelines or internal guidelines.

Securing Virtual Machines

VMs can be secured for threads trying to sneak in through the boot process. You can enable UEFI Secure boot. UEFI Secure Boot is a security standard that helps ensure that your PC boots using only software that is trusted by the PC manufacturer.

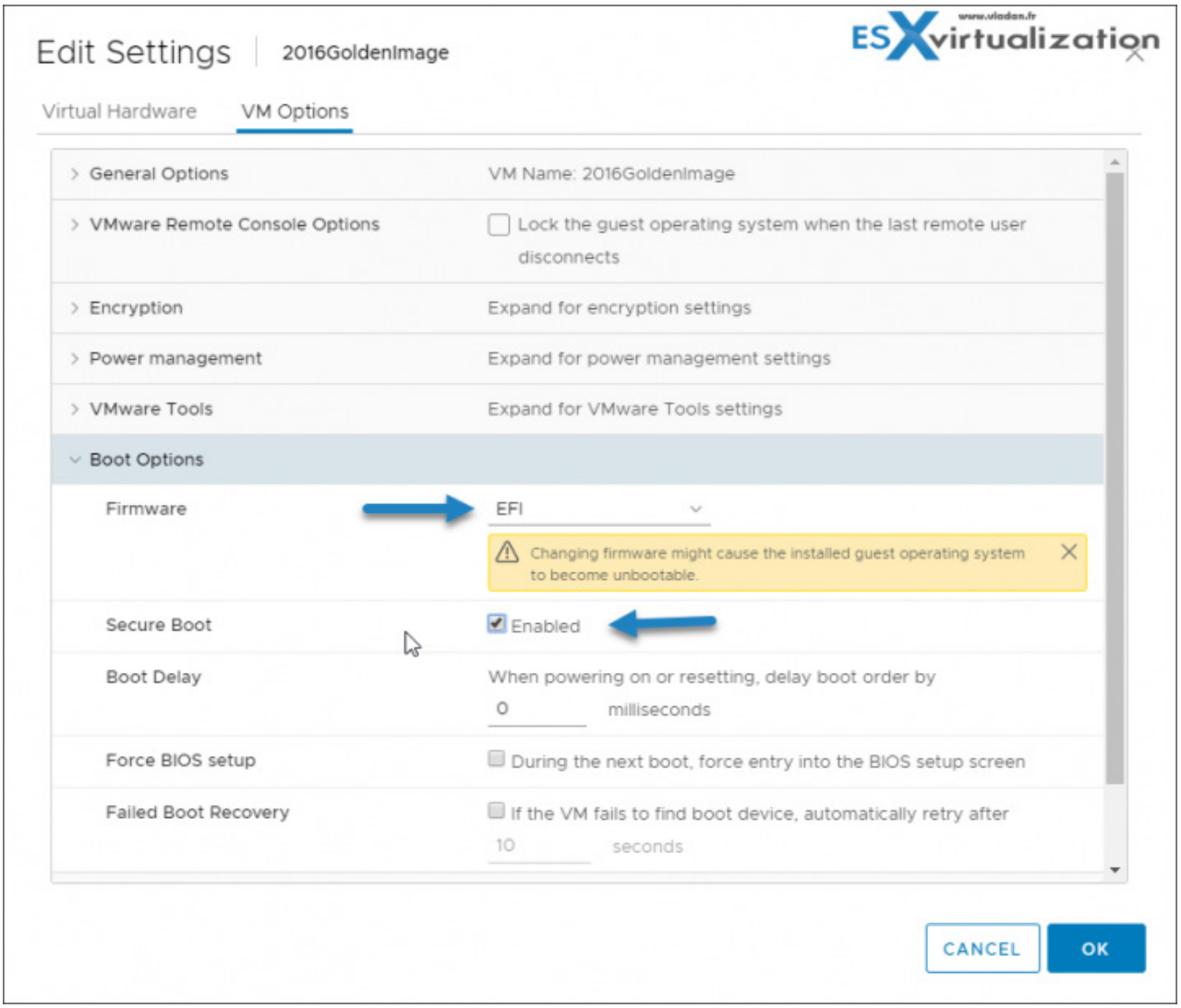
For certain virtual machine hardware versions and operating systems, you can enable secure boot just as you would for a physical machine. In an operating system that supports UEFI secure boot, each piece of boot software is signed, including the bootloader, the operating system kernel, and operating system drivers. The virtual machine's default configuration includes several code signing certificates.

VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot.

For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode. Remove VMware Host-Guest Filesystem from VMware Tools before you enable secure boot.

Right-click a VM and select **Edit Settings** > Click the **VM Options tab**, and expand **Boot Options > Boot Options, ensure that firmware is set to EFI >** Select the Secure Boot check box to enable secure boot.

Deselect the Secure Boot check box to disable secure boot.



When the virtual machine boots, only components with valid signatures are permitted. The boot process stops with an error if it encounters a component with a missing or invalid signature.

VMs best practices:

- Use the same security measures in virtual machines that you do for physical systems.
- Use Templates to Deploy Virtual Machines
- Minimize Use of the Virtual Machine Console
- Prevent Virtual Machines from Taking Over Resources
- Disable Unnecessary Functions Inside Virtual Machines

Use Encryption in your vSphere environment:

- Set up a key management server (not provided by VMware)
- Create an encryption storage policy
- Enable host encryption mode

- Create an encrypted VMs
- Change the encryption policy for VMDKs

Secure your environment with virtual Trusted Platform module:

- Add a Virtual Trusted Platform Module (vTPM) to a VM
- Enable vTPM for an existing VM
- Identify vTPM enabled VMs
- View vTPM module device certificates

Securing the Virtual Networking Layer

Network security in the vSphere environment shares many characteristics of securing a physical network environment, but also includes some characteristics that apply only to virtual machines.

Segmentation - Keep different virtual machine zones within a host on different network segments. If you isolate each virtual machine zone on its own network segment, you minimize the risk of data leakage from one zone to the next. Segmentation prevents various threats, including Address Resolution Protocol (ARP) spoofing.

Use VLANs - Set up virtual local area networks (VLANs) to help safeguard your network. VLANs provide almost all the security benefits inherent in implementing physically separate networks without the hardware overhead.

Secure the physical switch - ensure that spanning tree protocol is disabled or that Port Fast is configured for all physical switch ports that are connected to ESXi hosts.

Secure Standard switch ports with security policies - You can use this security policy to ensure that the host prevents the guest operating systems of its VMs from impersonating other machines on the network. The guest operating system that might attempt impersonation does not detect that impersonation was prevented.

Reference PDF: *vSphere Security*

Also read: *Security of the VMware vSphere Hypervisor* PDF

Be secured but not too “locked,” have a good balance between security and manageability. Making any changes to the security of the vSphere environment can have large impacts on the manageability of the environment for you and your team.

You should always analyze your needs, your risks, and your requirements before changing the security of your environment.

Objective 4.1 - Understand basic log output from vSphere products

Today, we'll have a look at different possibilities for logs in VMware vSphere products. vSphere records events in the vCenter Server database. System log entries include such information as who generated the event, when the event was created, and the type of event. You have the possibility to view, export or redirect those logs to a remote syslog server.

The default ESXi log file location is /scratch/log directory if there is local storage. However, many ESXi hosts are often deployed so that they redirect to a shared location and only use shared storage instead of local storage. As such, it's often a remote syslog server which is configured as a destination for collecting logs.

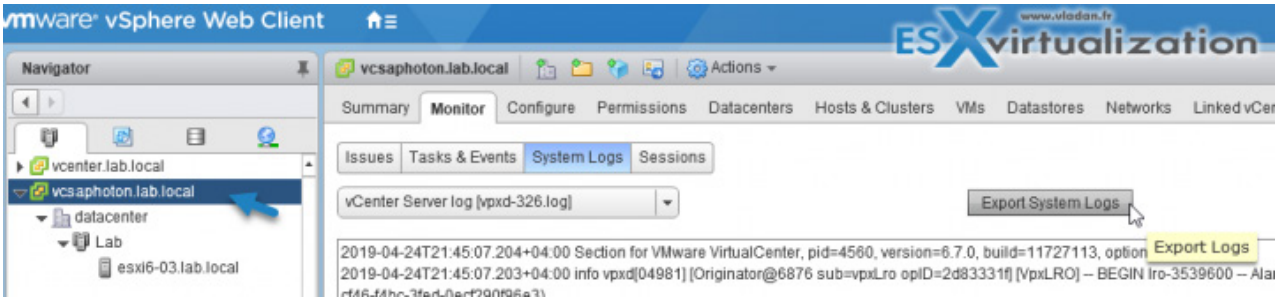
You can check for logs through vSphere Web client.

Select a vCenter Server instance in the vSphere Web Client navigator. Click **Monitor**, and click **System Logs.**

From the drop-down menu, select the log. You can export those logs if you need to send them to VMware support as well. Click Show All Lines or Show Next 2000 Lines to see additional log entries.

Note: I'm using vSphere Flash version of Web client as apparently the HTML5 Web client in this release did not arrive on time. Stay tuned!

Looking below, you can select which log you want to look at via the drop-down menu (in my example, I selected vCenter server log).



Remote syslog server

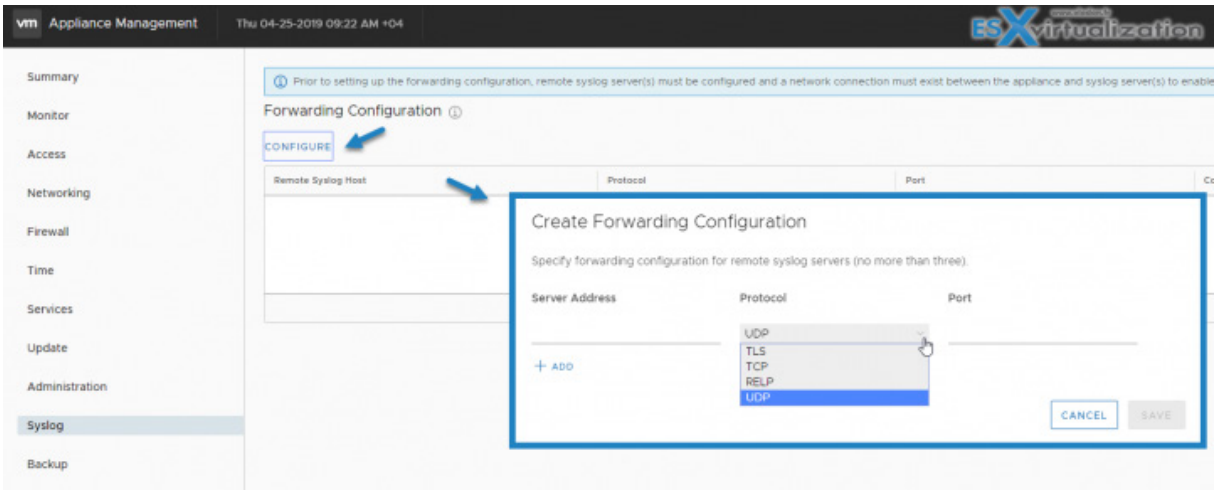
After you enable remote streaming, vCenter Server Appliance starts streaming and only the newly generated events are streamed to the remote syslog server. All syslog messages begin with a specific prefix. You can distinguish the vCenter Server Appliance events from other syslog messages by their Event prefix.

The syslog protocol limits the length of syslog messages to 1024 characters. Messages that are longer than 1024 characters split into multiple syslog messages.

Redirect vCenter Server Appliance Log Files to Another Machine

You can redirect the vCenter Server Appliance log files to another machine, for example, if you want to preserve storage space on the vCenter Server Appliance.

After login via https://IP_or_FQDN:5480 go to **Syslog > Configure**



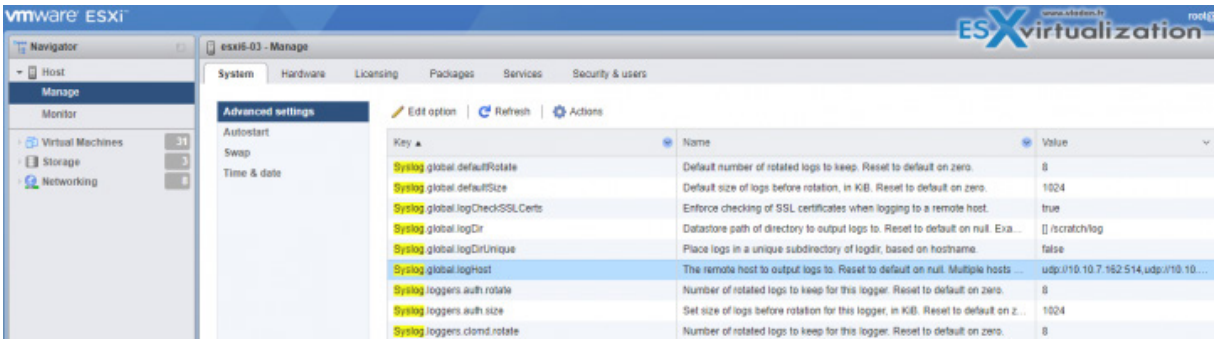
In the **Server Address** text box, enter the FQDN or IP address of the machine on which you want to export the log files.

In the **Port** text box, enter the port number you wish to use for communication with the machine on which you want to export the log files.

From the **Protocol** drop-down menu, select the protocol to use.

Configure ESXi host to send logs to a remote location.

In theory, any syslog compatible software can do the job. However, you have to configure the advanced parameter **Syslog.global.logHost** to expose the log files through either TCP or UDP. Depending on your syslog application, you should set the parameter to either tcp://hostname:514 or udp://hostname:514.



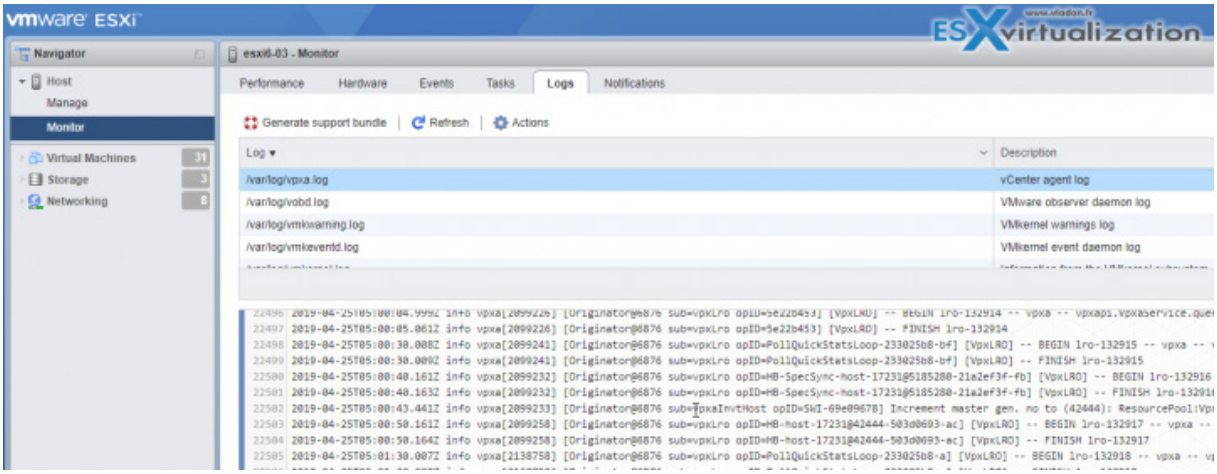
In large environments, you can use host profiles to deploy this configuration to all of your hosts, but there is also a product which can remotely configure that for you (VMware vRealize Log Insight, Runecast Analyzer etc…)

The different options are listed below

Option	Description
Syslog.global.defaultRotate	Maximum number of archives to keep. You can set this number globally and for individual subloggers.
Syslog.global.defaultSize	Default size of the log, in KB, before the system rotates logs. You can set this number globally and for individual subloggers.
Syslog.global.LogDir	Directory where logs are stored. The directory can be located on mounted NFS or VMFS volumes. Only the `/scratch` directory on the local file system is persistent across reboots. Specify the directory as *[datastorename] path_to_file*, where the path is relative to the root of the volume backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.
Syslog.global.logDirUnique	Selecting this option creates a subdirectory with the name of the ESXi host under the directory specified by **Syslog.global.LogDir**. A unique directory is useful if the same NFS directory is used by multiple ESXi hosts.
Syslog.global.LogHost	Remote host to which syslog messages are forwarded and port on which the remote host receives syslog messages. You can include the protocol and the port, for example, `ssl://hostName1:1514`. UDP (default), TCP, and SSL are supported. The remote host must have syslog installed and correctly configured to receive the forwarded syslog messages. See the documentation for the syslog service installed on the remote host for information on configuration.

Monitor individual ESXi

You can also access directly to ESXi to check the logs, in case vCenter is unavailable or it is a host not managed by vCenter.

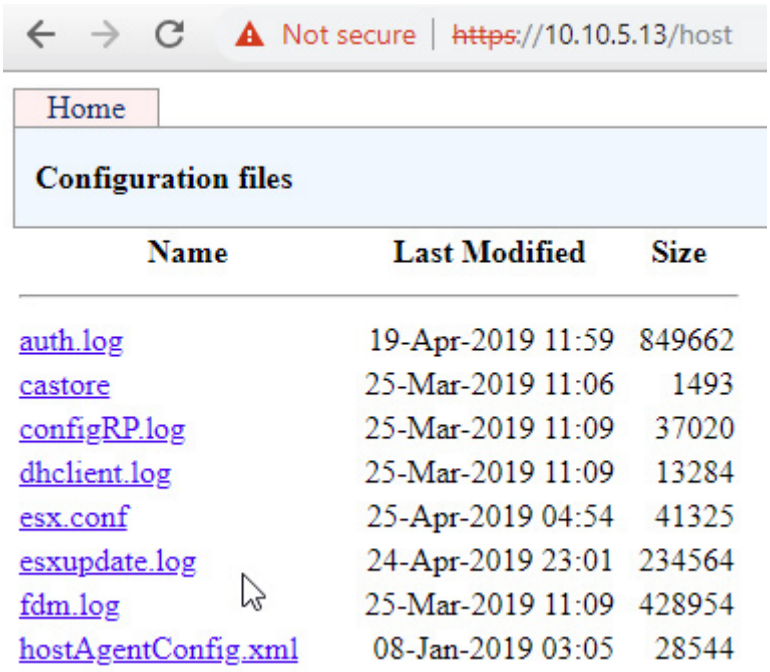


Access logs via a web browser through alternative URL

This might be a handful when there is a problem with the ESXi host client. There is a short url to access logs:

https://ip_or_fqdn/host

and you'll get access to logs directly via a web browser.



Objective 4.2 - Create and configure vSphere objects

This post, **VCP6.7-DCV Objective 4.2 – Create and configure vSphere objects**, will detail the configuration of vSphere objects (clusters, datacenters....).

Let's get back to our objective, based on the If you have VMware ESXi cluster configuration, managed by a vCenter server, multiple ESXi hosts provide compute, memory, and network resources to the cluster environment as a whole, as well as protect cluster-housed VMs against physical server failures.

Once a cluster is created, a vSphere cluster can have some "cluster only" features such as HA (high availability) or DRS (distributed resource scheduler). We'll review it in details further in this post.

A large vSphere implementation might contain several virtual data centers with a complex arrangement of hosts, clusters, resource pools, and networks. It might involve multiple vCenter Server systems connected using Enhanced Linked Mode. Smaller implementations may require a single virtual data center with a much less complex topology.

Tasks for Organizing Your Inventory

You can execute different tasks:

- Create data centers.
- Add hosts to the data centers.
- Organize inventory objects in folders.

- Set up networking by using vSphere Standard Switches or vSphere Distributed Switches. To use services such as vMotion, TCP/IP storage, VMware VSAN, and Fault Tolerance, set up VMkernel networking for these services.
- Configure storage systems and create datastore inventory objects to provide logical containers for storage devices in your inventory.
- Create clusters to consolidate the resources of multiple hosts and virtual machines. You can enable vSphere HA and vSphere DRS for increased availability and more flexible resource management.
- Create resource pools to provide logical abstraction and flexible management of the resources in vSphere. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources.

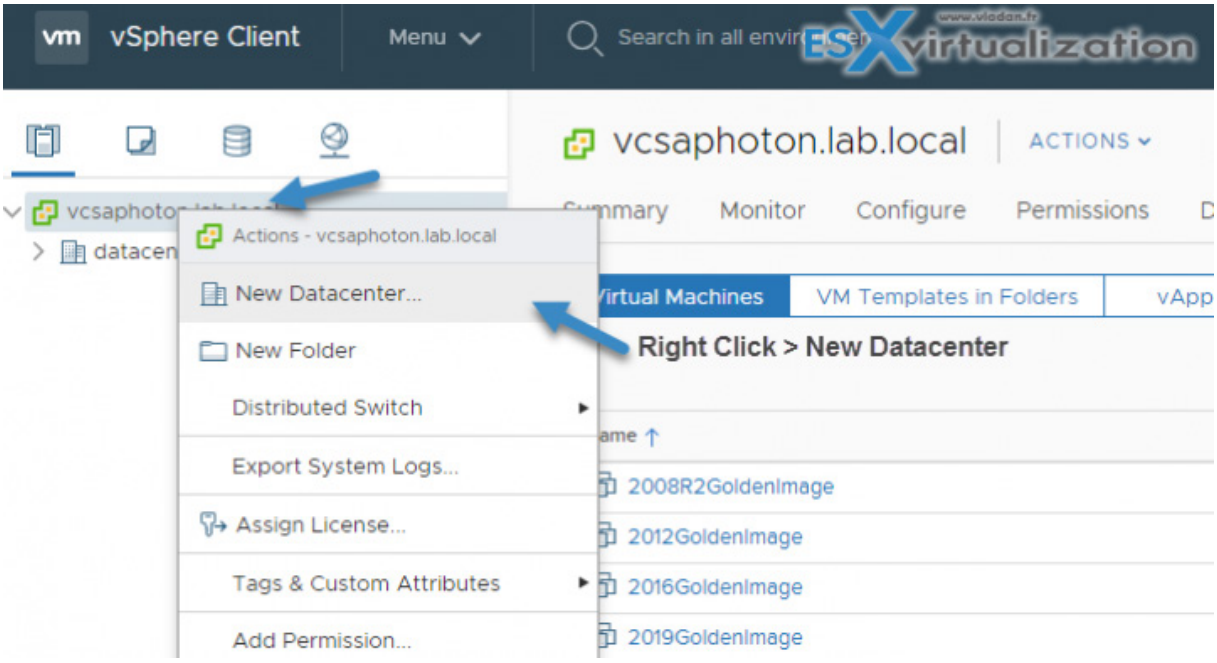
Let's start with a Creation of a Datacenter object

Quote:

A data center is a container for all the inventory objects required to complete a fully functional environment for operating virtual machines. You can create multiple data centers to organize sets of environments.

In the vSphere Client, navigate to the **vCenter Server object**, Select **Actions** > **New Datacenter** > Rename the data center and click **OK**.

You can also use **right-click action** by clicking the vCenter server in your inventory.



Add Host to Datacenter, folder, cluster

It is then possible to add hosts under a **data center object**, **folder object**, or **cluster object**. If a host contains virtual machines, those virtual machines are added to the inventory together with the host.

There is not a single or preferred way to proceed. You can either start created cluster object and then add hosts there, or you can add hosts to your datacenter first and then only create cluster(s) objects.

Required privileges:

- **Host** > **Inventory** > **Add host to cluster**.
- **Resource** > **Assign virtual machine to resource pool.**
- **System** > **View** on the virtual machines folder where you want to place the virtual machines of the host.

So, in order to add a host to the inventory, do a right-click action to the data center, cluster, or folder and select **Add Host >** Type the IP address or the name of the host > Type administrator credentials > Review the host summary > License the host.

What are folders for?

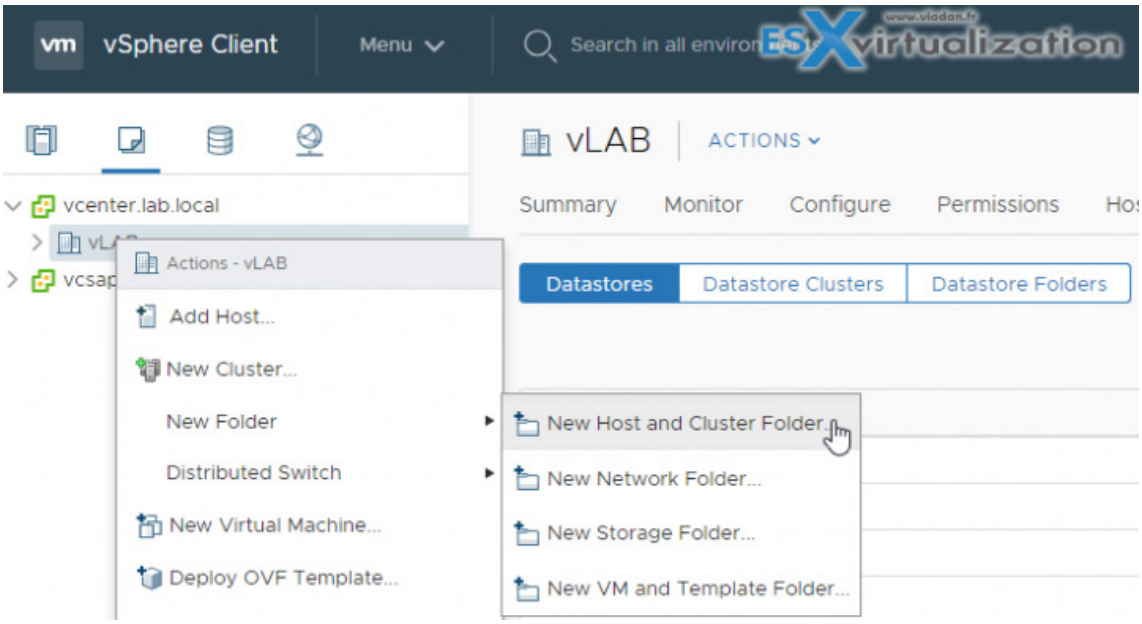
Folders are for grouping objects of the same type for easier management. You can then apply a set of permissions to folders.

A folder can have other folders inside, and a group of objects of **the same type**, as is the case for Windows Explorer. As an example, a single folder can have VMs and another folder containing other VMs.

However, you **cannot have hosts inside a folder and then a folder with VMs.**

Types of folders:

- Host and Cluster folders
- Network folders
- Storage folders
- VM and Template folders.

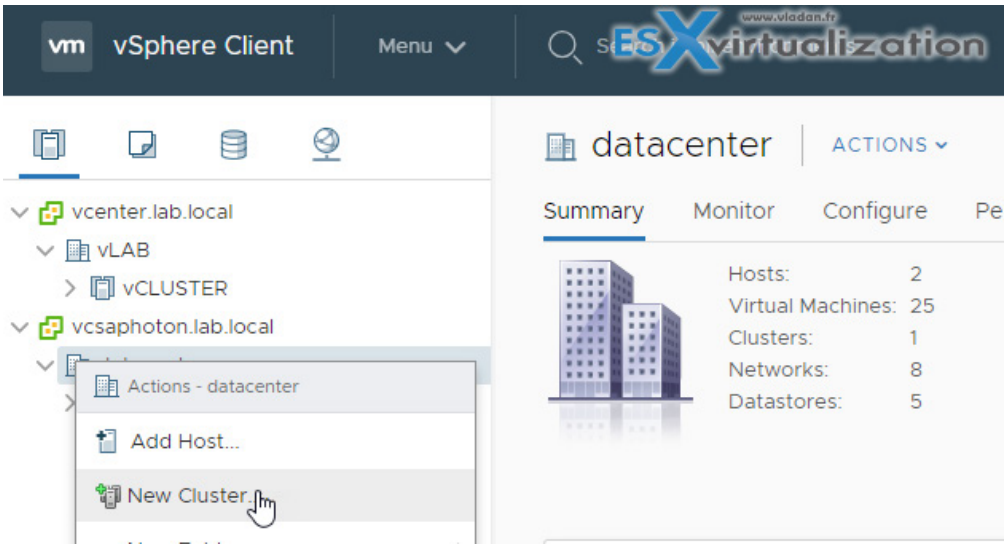


Create a cluster

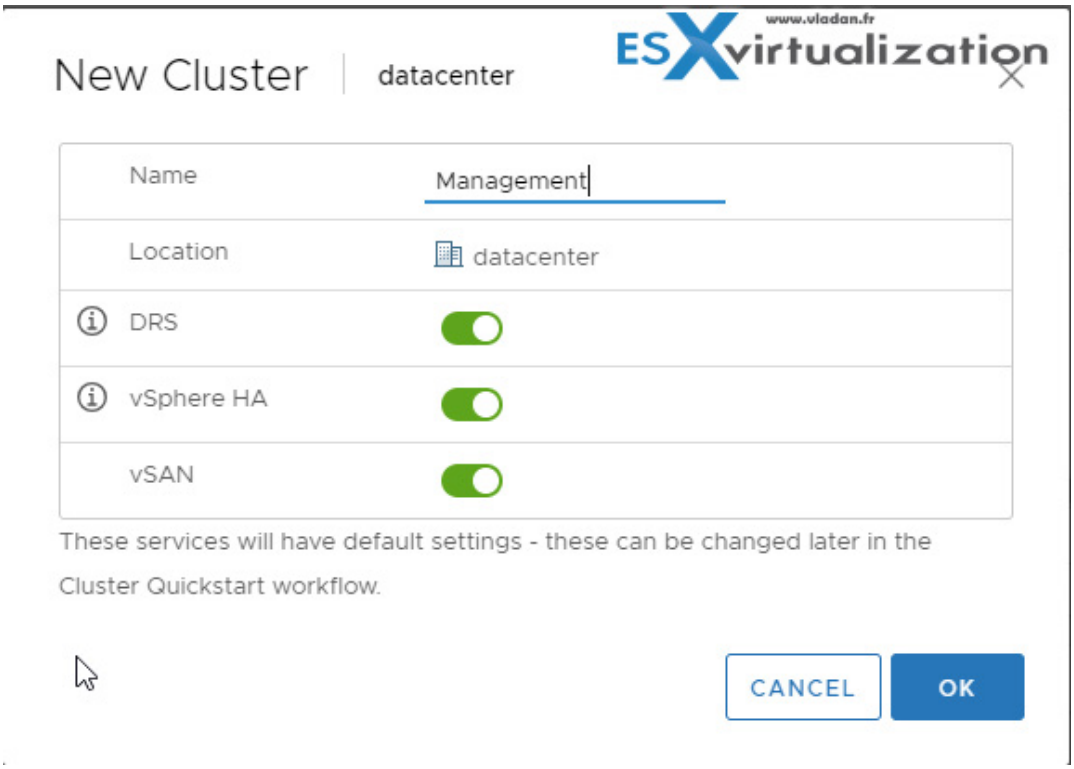
After you have created your datacenter, you can create clusters. Clusters are usually based on your type of workload used, geographical location, etc.

You can create an empty cluster, activate certain services (VSAN, HA, DRS) and then add hosts into that cluster.

The steps: Right click **Datacenter Object** > **New Cluster**.



Assign a distinct and meaningful name and activate the services you want the cluster to assure. In our case, we're activating all cluster services.



The different individual cluster services, such as HA, VSAN or DRS shall be studied through **vSphere Availability** PDF. You'll find topics about vSphere HA, the concepts, how it works, what the master and slave nodes are, host failure types, VM and application monitoring or Network partitions.

However, there are other chapters from the blueprint which will cover those technologies in details. For example, the Objective 1.6 – Describe and differentiate among vSphere, HA, DRS, and SDRS functionality.

We also have the Objective 2.2 – Describe HA solutions for vSphere or Objective 7.6 – Configure and use vSphere Compute and Storage cluster options.

Below are a few basic concept articles and guides from vSphere 6.5 which might be useful as well.

- What is VMware DRS (Distributed Resource Scheduler)?
- VCP6.5-DCV Objective 7.5 - Troubleshoot HA and DRS Configurations and Fault Tolerance
- VCP6.5-DCV Objective 9.1 - Configure vSphere HA Cluster Features

Objective 4.3 - Set up a content library

With vCenter Server 6.7 Update 2, you can publish your .vmtx templates directly from a published library to multiple subscribers in a single action instead of performing sync from each subscribed library individually.

The published and subscribed libraries must be in the same linked vCenter Server system, regardless if on-prem, in the cloud, or a hybrid. Work with other templates in content libraries does not change.

With vCenter 6.7 Update 2, you can now publish your VM templates managed by Content Library from a published library to multiple subscribers. You can trigger this action from the published library, which gives you greater control over the distribution of VM templates. The published and subscribed libraries must be in the same linked vCenter Server system, regardless if on-prem, in the cloud or a hybrid. Work with other templates in content libraries does not change.

VMware has introduced VM Template (VMTX) syncing in **vSphere 6.7 U2**. A VM template will now be automatically synchronized between on-prem and on-prem vCenter Servers and also from on-prem to VMware Cloud on AWS.

Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in the same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

Starting with **vSphere 6.7 Update 1**, content libraries also support VM templates. As such, templates in the content library can either be of the **OVF Template** type or the V**M Template type**. vApp templates are still converted to OVF files when you upload them to a content library.

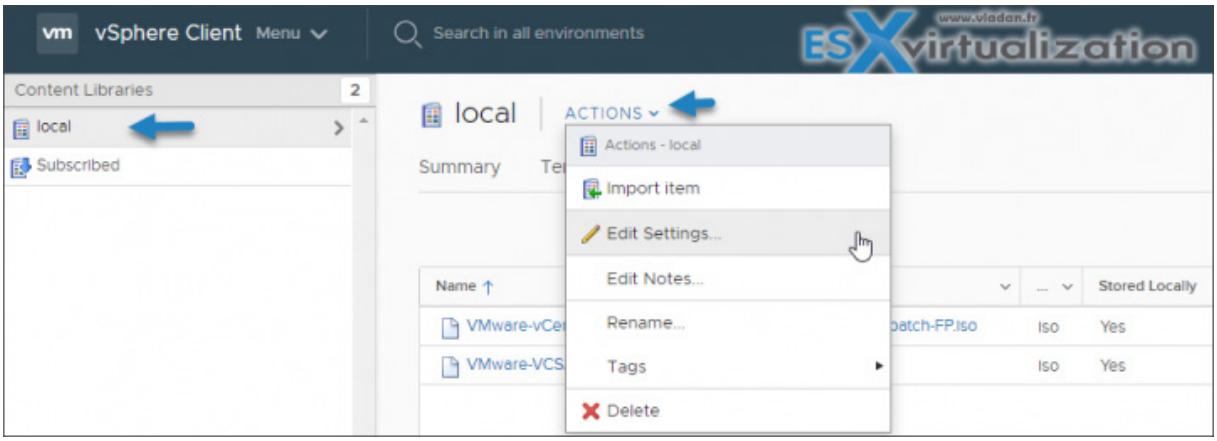
Open Virtual Appliance (OVA) templates can now be imported from some HTTPS endpoint or your local storage. You also can just sync the content of OVA templates to other vCenter Servers.

The distribution of VM templates additionally requires that the respective vCenter Server instances are in Enhanced Linked Mode or Hybrid Linked Mode and that the respective hosts are connected through a network.

You create and manage a content library from a single vCenter Server instance, but you can share the library items to other vCenter Server instances if HTTP(S) traffic is allowed between them.

Two Types of Libraries:

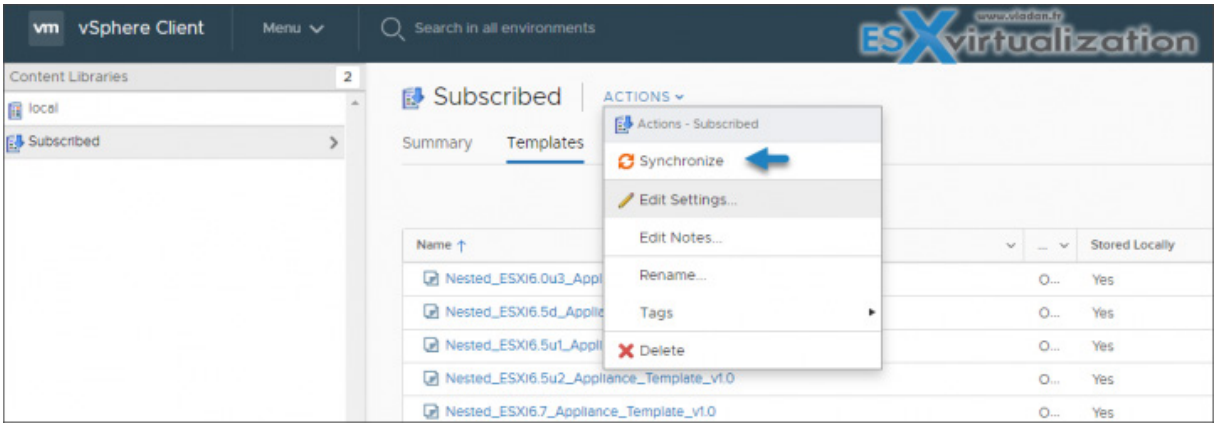
Local Libraries - store items in a single vCenter Server instance. You can publish the local library so that users from other vCenter Server systems can subscribe to it. When you publish a content library externally, you can configure a password for authentication.



Subscribed Libraries - You subscribe to a published library by creating a subscribed library. You can create the subscribed library in the same vCenter Server instance where the published library is, or in a different vCenter Server system.

In the Create Library wizard, you have the option to download all the contents of the published library immediately after the subscribed library is created, or to download only metadata for the items from the published library and later to download the full content of only the items you intend to use.

vSphere web client > Menu > Content Libraries > Right-click (or Actions) > Synchronize.



Content Library Roles

Content Library Administrator role is a predefined role that gives a user privileges to monitor and manage a library and its contents.

A user who has this role can:

- Create, edit, and delete local or subscribed libraries.
- Synchronize a subscribed library and synchronize items in a subscribed library.
- View the item types supported by the library.
- Configure the global settings for the library.

- Import items to a library.
- Export library items.

When you create a subscription for a local library, the result is a subscribed library. A publisher library is aware of its subscriptions. Subscriptions enable the administrator of the publisher library to control the content distribution. With subscriptions, content is distributed either when the subscriber initiates synchronization, or when the administrator of the local library publishes the library items to one or more of the existing subscriptions.

When you use subscriptions, you have the flexibility to decide how much of the library content you want to share with the subscribers. For example, you can publish some or all library items. You can also publish content to selected subscribers or to all subscribers.

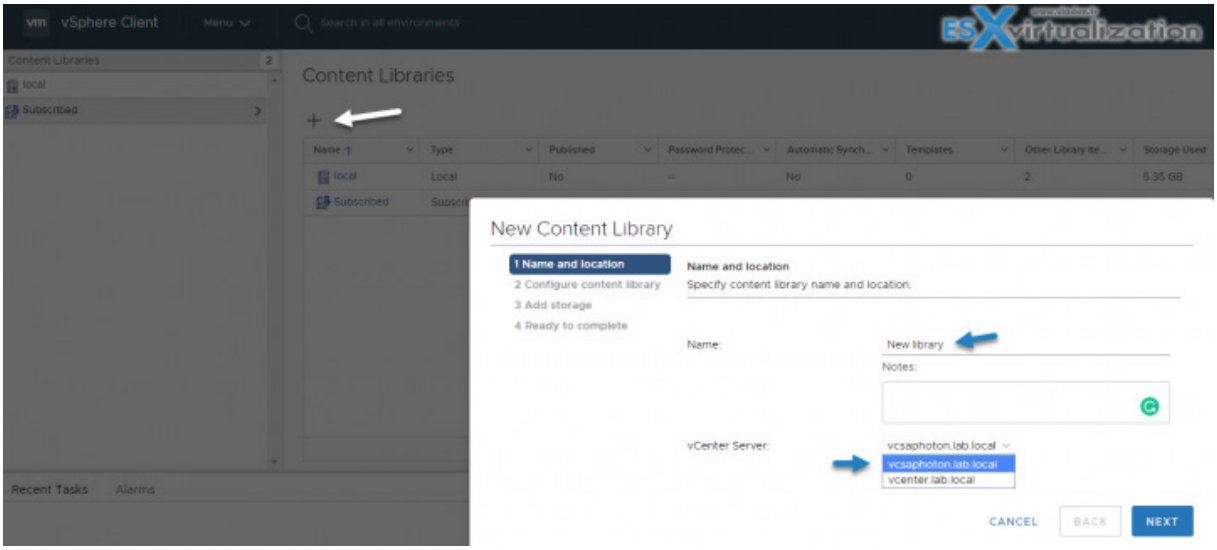
The use of subscriptions allows for content distribution between a publisher and a subscriber in the following scenarios:

- The publisher and subscriber are in the same vCenter Server instance.
- The publisher and subscriber are in vCenter Server instances that are in Enhanced Linked Mode.
- The publisher and subscriber are in vCenter Server instances that are in Hybrid Linked Mode.

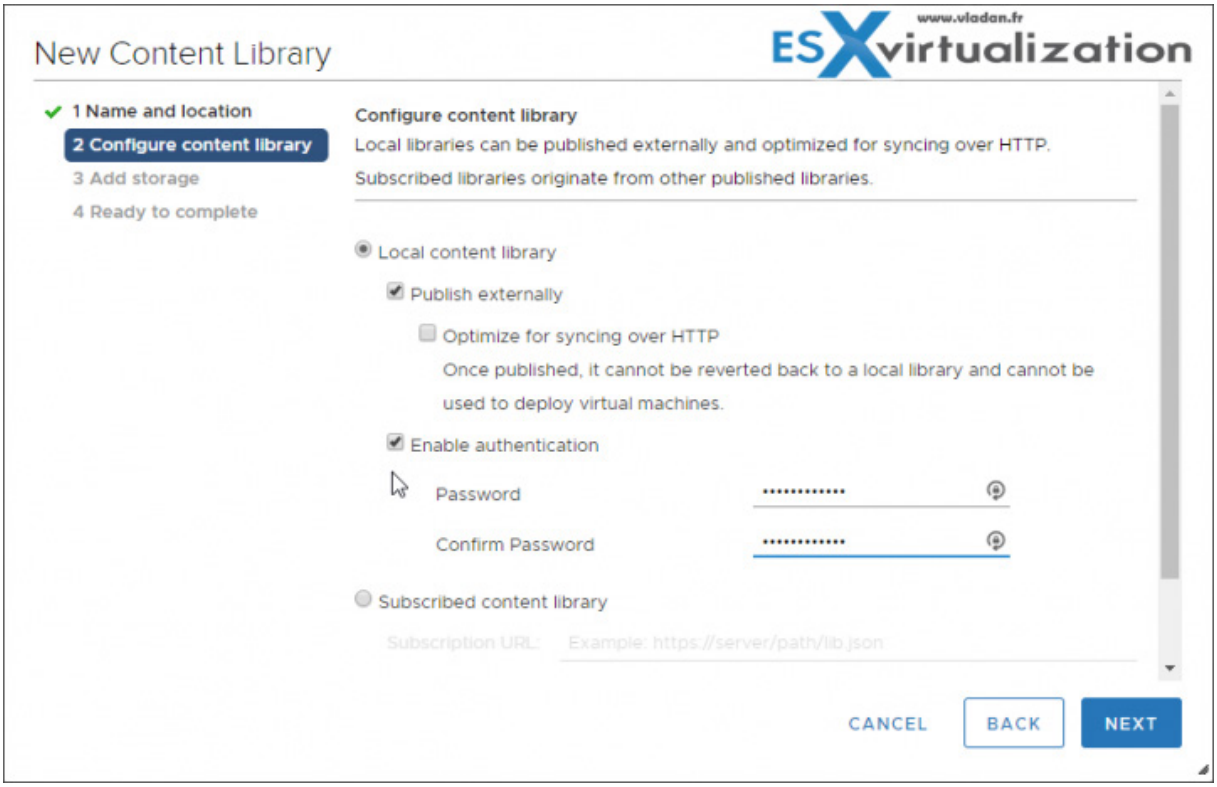
Create New content Library with authentication

You'll need to provide a Name, description and select vCenter server to which this library will be attached; the other options you'll have are whether it is:

- Local content library
- Subscribed content library
- Select datastore



Next, identify whether you want to create a Local content library or Subscribed content library, and if you wish to enable authentication.



Now, finally you'll see this library added to the list of existing content libraries on your vCenter server system.

You can edit items only in a local library, regardless of whether it is published or not. Library items in subscribed libraries cannot be modified.

You can edit both VM templates and OVF templates. In a content library, an OVF template is either a template of a virtual machine or a template of a vApp. When you clone a virtual machine into a template in a content library, you must choose whether to create an OVF template or a VM template.

However, if you clone a vApp into a template in a content library, the resulting content library item is always an OVF template. Since the OVF format is actually a set of files, if you export the template, all the files in the OVF template library item (.ovf, .vmdk, .mf) are saved to your local system.

Objective 4.4 - Set up ESXi hosts

This post's title is **VCP6.7-DCV Objective 4.4 – Set up ESXi hosts** and we'll have a look at how to setup ESXi.

Note that it's impossible to cover **all knowledge** for this topic in a single blog post.

ESXi requirements:

You'll need to check VMware compatibility guide and check your hardware if it›s compatible with ESXi 6.7. ESXi needs at least:

- Double-core CPU
- 64 bit CPU
- ESXi needs the NX/XD bit to be enabled for the CPU in the BIOS
- Minimum 4GB of RAM (8 recommended)
- Intel VT-x or AMD RVI if you want to use x64 virtual machines
- At least one 1GBE physical Network interface card (NIC)
- SCSI disk or local, non-network, RAID LUN with unpartitioned space for virtual machines

ESXi supports a boot from UEFI (Unified Extensible Firmware Interface).

From ESXi 6.7 VMware supports UEFI also for auto deploy (network booting and provisioning).

Storage requirements:

ESXi 6.7 needs a boot device which is at least 1GB in size. If you're booting from USB stick, local disk, SAN or iSCSI LUN, you'll need 2-5 GB of space due to VMFS volume and scratch partition (4 GB) on the boot device.

While 1 GB is sufficient, VMware recommends using a 4 GB or larger device due to core dump partition location. The best option to use are 16 GB high-quality USB sticks.

For USB and SD, the ESXi does not create the scratch partition automatically because those devices are IO sensible and can wreck faster than traditional storage. The ESXi installer tries to find a local disk and if a local disk is not found, the scratch partition is placed on the ramdisk.

For configs "Boot from SAN" or Autodeploy, you can allocate a shared LUN for scratch partitions of many ESXi hosts.

You should NOT use local datastore and VMFS partition to run VMs for M2 and non-USB low-end and low-quality flash media. It's because the high I/Os generated by VMs will destroy those devices in no time. It's recommended **to delete this local datastore right after the end of the installation**.

Required Firewall ports:

Check pages 14-15 of the "*vSphere ESXi Installation PDF*" for required firewall ports. This is the PDF we're working with which you'll still need to read if you want to get all the information about setting up ESXi hosts. This blog post gives you the guidance and the main info, but we cannot cram in everything…

Required free space for System Logging

While hosts deployed with AutoDeploy stores logs on a RAM disk, the configuration may vary for hosts configured to boot from local storage.

VMware recommends redirecting logs for hosts deployed with Auto Deploy like this:

- Redirect logs to a remote collector
- Redirect logs to a NAS or NFS datastore

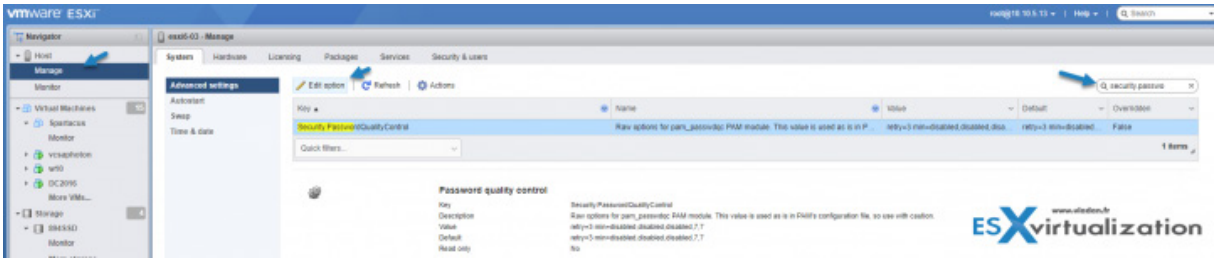
Table 5-6. Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

ESXi Password and Account Lockout

You have to use a password with predefined requirements, which can be changed in the advanced option ***Security.PasswordQualityControl***

Click to enlarge…



- By default, you have to include a mix of characters from four-character classes: lowercase letters, uppercase letters, numbers, and special characters such as underscore or dash when you create a password.
- By default, password length must be more than 7 and less than 40.
- Passwords cannot contain a dictionary word or part of a dictionary word.

ESXi account lockout behavior

Account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of ten failed attempts is allowed before the account is locked. The account is unlocked after two minutes by default.

Configuring Login Behavior - You can configure the login behavior for your ESXi host with the following advanced options:

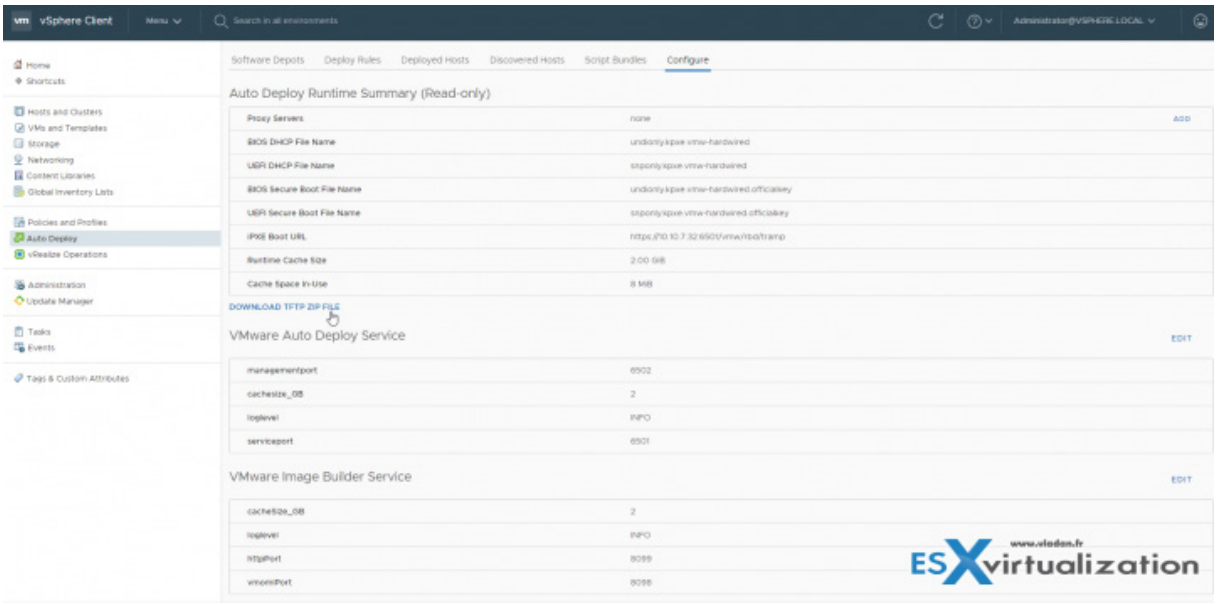
- **Security.AccountLockFailures** - Maximum number of failed login attempts before a user›s account is locked. Zero disables account locking.
- **Security.AccountUnlockTime** - Number of seconds that a user is locked out.

Prepare for Installing ESXi

- Get the ISO for installation of ESXi at VMware. You'll need a myVMware account.

Several Ways of installing ESXi include:

- **Interactive ESXi installation** (CD/DVD, Bootable USB or PXE booting the installer over the network.
- **Scripted ESXi installation** (the installation script must be stored in a location that the host can access by HTTP, HTTPS, FTP, NFS, CDROM, or USB. You can PXE boot the ESXi installer or boot it from a CD/DVD or USB drive.)
- **Autodeploy ESXi installation** - you can provision a lot of hosts by using a single image. You can specify host profiles to apply to the hosts and store the ESXi image configuration on local disk, remote disk or USB drive. vCenter Server loads the ESXi image directly into the host memory. vSphere Auto Deploy does not store the ESXi state on the host disk. The vSphere Auto Deploy server continues to provision this host every time the host boots. We have covered Autodeploy in details in our post - VCP6.5-DCV Objective 8.1 – Configure Auto Deploy for ESXi Hosts.



ESXi installer can boot from:

- USB flash drive - (check the steps and procedure of creating USB boot installer on a Linux machine on the “VMware ESXi Installation and Setup - VMware vSphere 6.7” PDF.)
- Boot from CD/DVD drive

TIP: Top 3 Free Tools To Create ESXi 6.7 Installer USB Flash Drive

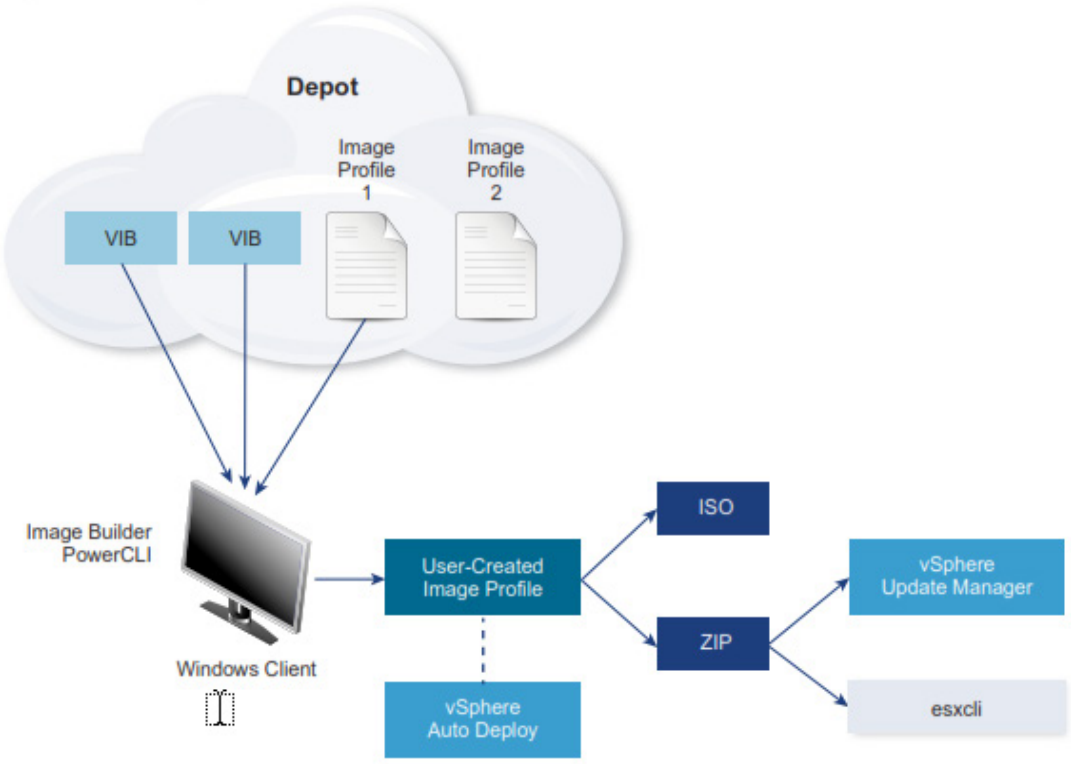
PXE Booting the ESXi installer - setup a DHCP server which sends the address of the TFTP server and the filename of the Initial boot loader to the ESXi host.

Note: PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

If your TFTP server runs on a Microsoft Windows host, use tftpd32 version 2.11 or later. Linux distros also have a copy of tftp-hpa server.

ESXi Image Builder - You can use vSphere ESXi Image Builder with the vSphere Client or with PowerCLI to create an ESXi installation image with a customized set of ESXi updates and patches. You can also include third-party network or storage drivers that are released between vSphere releases.

Figure 5-2. Image Builder Architecture



You can watch a video from VMware tech marketing here.

Different types of VIBs?

Quote:

VIB – A VIB is an ESXi software package. VMware and its partners package solutions, drivers, CIM providers, and applications that extend the ESXi platform as VIBs. VIBs are available in software depots. You can use VIBs to create and customize ISO images or to upgrade ESXi hosts by installing VIBs asynchronously onto the hosts.

Image Profile – An image profile defines an ESXi image and consists of VIBs. An image profile always includes a base VIB, and might include more VIBs. You can examine and define an image profile using the Image Builder PowerCLI.

Software Depot – A software depot is a collection of VIBs and image profiles. The software depot is a hierarchy of files and folders and can be available through an HTTP URL (online depot) or a ZIP file (offline depot). VMware and VMware partners make depots available. Companies with large VMware installations might create internal depots to provision ESXi hosts with vSphere Auto Deploy, or to export an ISO for ESXi installation.

There are VIBs that needs a reboot (base ESXi patches, drivers or esxcli extensions) and there are ones that don't.

Some examples of VIBs which do not require reboot are:

- CIM providers
- Cisco Nexus
- vShield Plugins
- Lab Manager
- HA agents

A VIB has 3 parts:

- **File Archive** – the main file. The file which gets deployed to the ESXi host.
- **XML descriptor file** – has important info about requirements for installing the VIB, namely relating to dependencies, compatibility, and whether a reboot is necessary
- **Signature File** – a signature which verifies the level of trust (Integrity, Information about the creator and verifications that it has been done).

The different VIBs can be installed in a different way, as you will see. In addition, there are VIBs that are **VMware certified**, **VMware accepted**, **Partner supported,** or **community supported**

Read more about image builder cmdlets at **page 35-42.**

Required space for System Logging

Table 5-6. Recommended Minimum Size and Rotation Configuration for hostd, vpxa, and fdm Logs

Log	Maximum Log File Size	Number of Rotations to Preserve	Minimum Disk Space Required
Management Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

The default values for log capacity in this infrastructure vary, depending on the amount of storage available and on how you have configured system logging. Hosts that are deployed with Auto Deploy store logs on a RAM disk, which means that the amount of space available for logs is small.

If your host is deployed with Auto Deploy, reconfigure your log storage in one of the following ways:

- Redirect logs over the network to a remote collector.
- Redirect logs to a NAS or NFS store.

By default, ESXi hosts use the default configuration, which stores logs in a scratch directory on the VMFS volume. For these hosts, ESXi 6.7 configures logs to best suit your installation and provides enough space to accommodate log messages.

Make sure that you read the whole PDF *vSphere ESXi Installation PDF* as we won't be able to squeeze all the information contained on the 214-page PDF here.

Objective 4.5 - Configure virtual networking

Virtual networking and vSphere infrastructure is a very large topic. In this post, we'll focus on fundamentals where through a series of examples, we'll explain how virtual machines can communicate to each other and how ESXi hosts has to be configured.

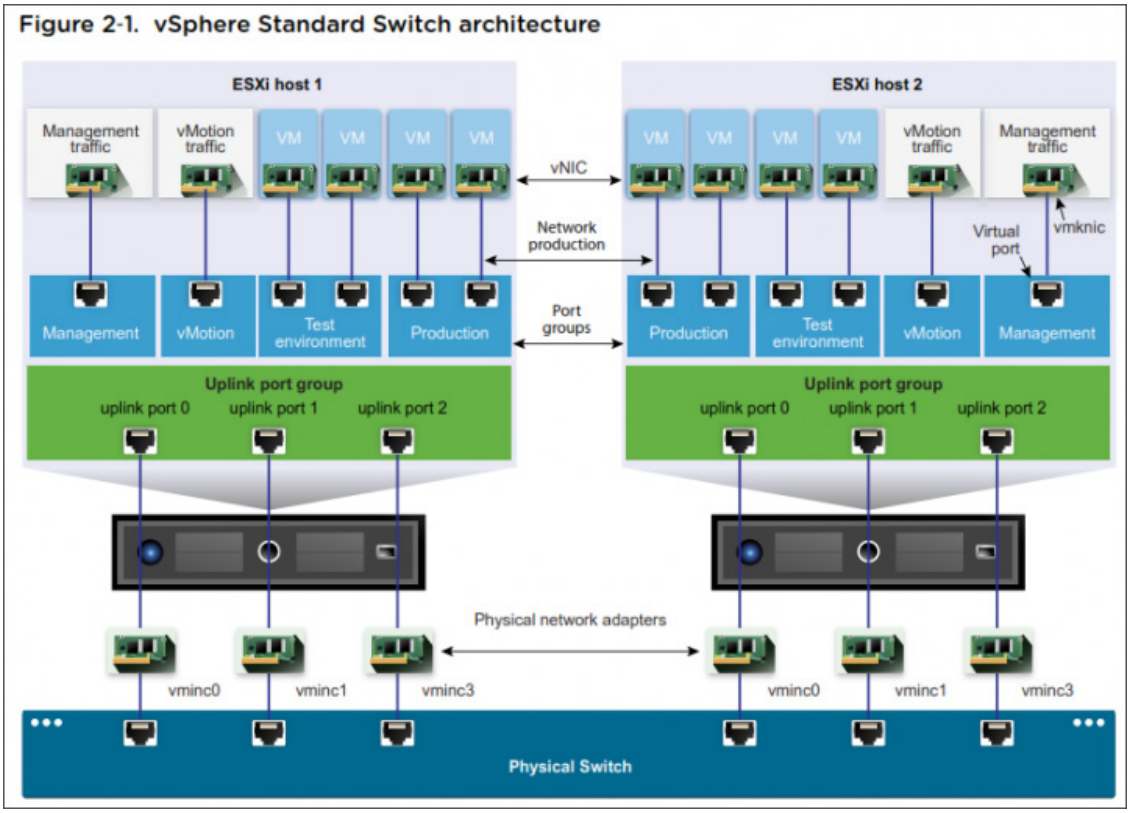
Here are a few words and definitions which you'll hear quite often:

Physical network - A network of physical machines that are connected so that they can send data to and receive data from each other. VMware ESXi runs on a physical machine.

Virtual Network - virtual machines running on a physical machine that are connected logically to each other so that they can send data to and receive data from each other. The VMs are also connected to the physical world. The virtual network also provides services such as vmkernel services which are necessary to maintain management connections, vMotion, VSAN, iSCSI, Fault Tolerance (FT) etc.

You don't have to have vCenter server installed in order to configure the standard switch. However, to configure a distributed switch, you will need a vCenter server.

A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port group.



vSphere Standard Switch (vSS) - it's like a physical Ethernet switch where you have VMs connected which can communicate with each other as the switch forward traffic to each of those VMs.

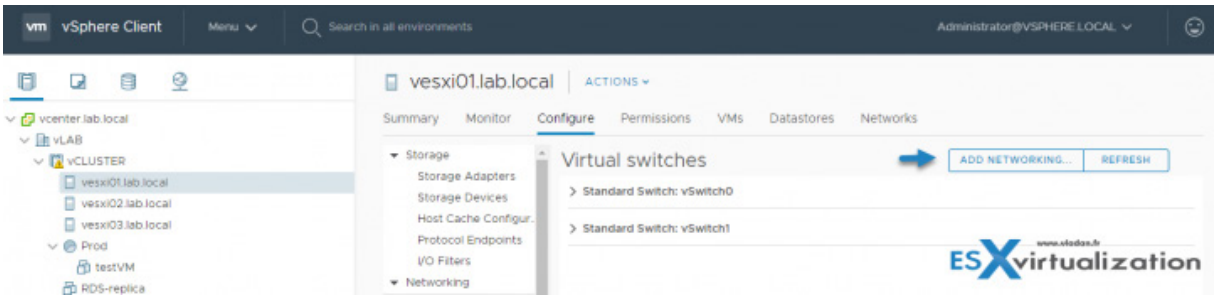
Standard Port group - port group specifies the port configuration options (VLAN, bandwidth limitation). A single standard switch usually has one or more port groups.

Uplink - Ethernet adapters, also referred to as uplink adapters, are used to join virtual networks with physical networks.

A VLAN ID, which restricts port group traffic to a logical Ethernet segment within the physical network, is optional. For port groups to receive the traffic that the same host sees, but from more than one VLAN, the VLAN ID must be set to virtual guest tagging (VGT) VLAN 4095.

Creating a VSS

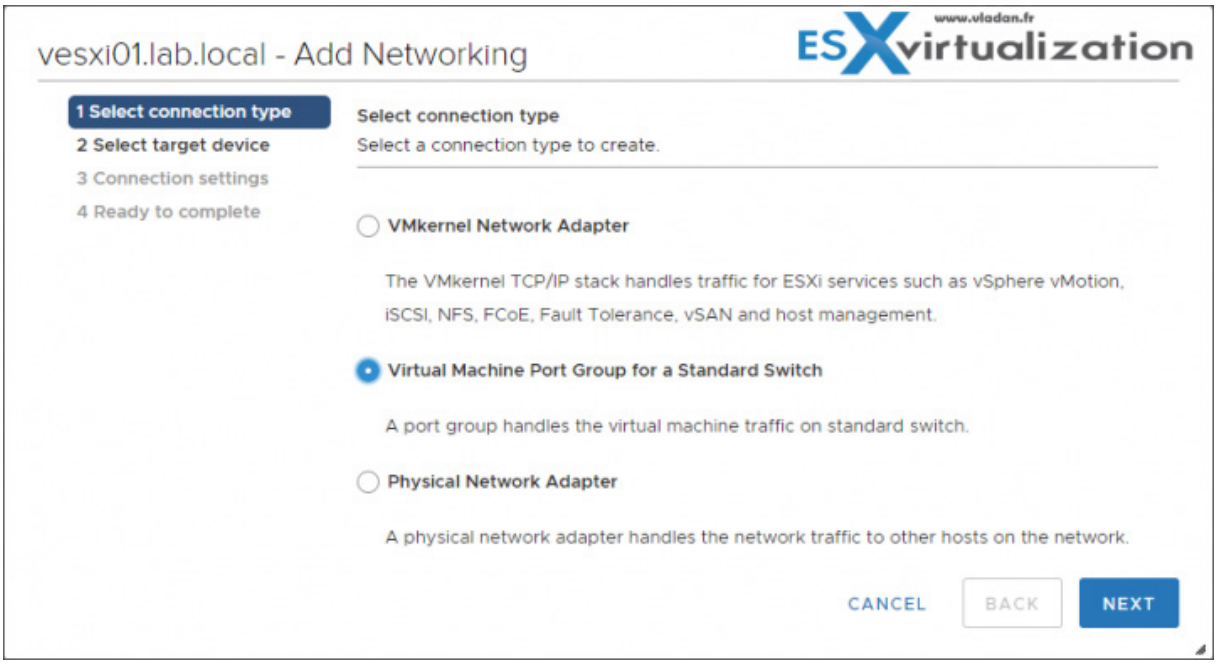
Open vSphere **Web client > Hosts and clusters, select host > Configure > Networking > Virtual Switches > Add Networking**



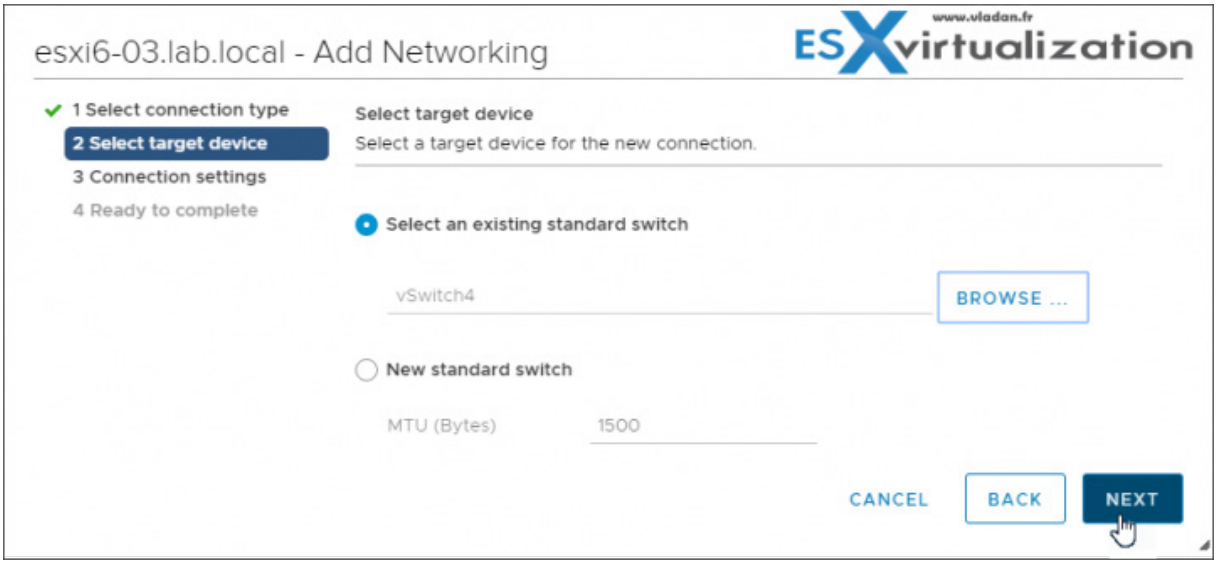
A new wizard will appear.

You'll need to select one of the 3 different options:

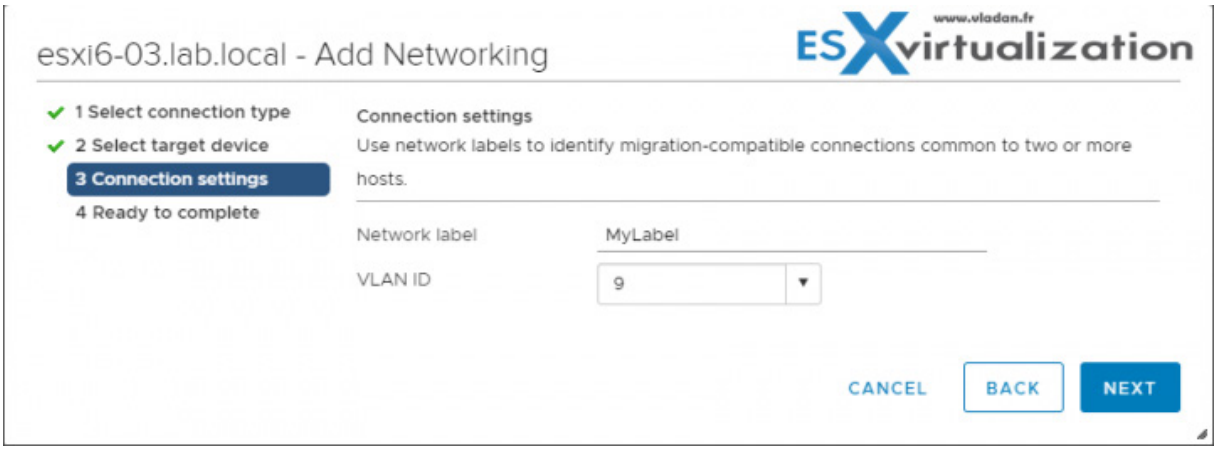
- **VMkernel Network Adapter** – Chose this option if you want to create a new VMkernel Adapter and associate some services (VSAN, FT, VMOTION)
- **VM Port Group** – Chose this option if you want to create a virtual machine port group
- **Physical Network Adapter** – Chose this option if you want to create and manage physical adapters on ESXi host.



This workflow creates connections according to your needs, allowing you to create either a **new standard switch** or **use an existing standard switch**.

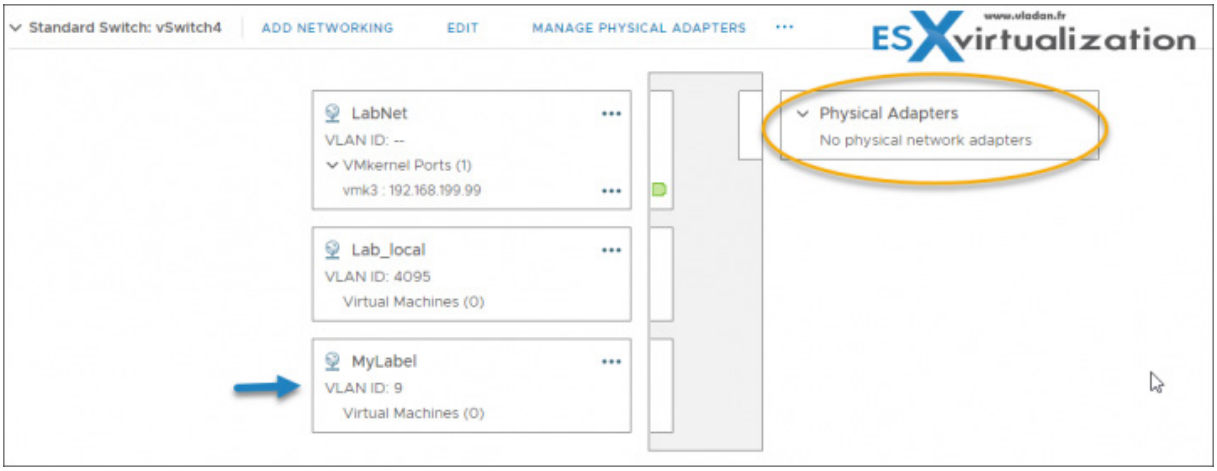


The next step allows us to specify the **Network Label** and **VLAN ID**.

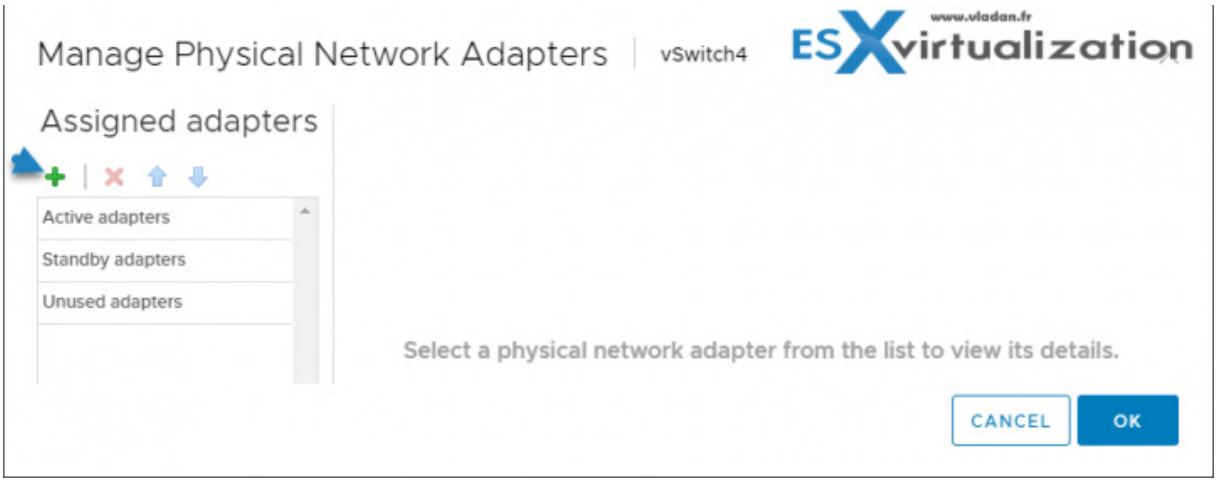


Once you hit finish and check the vSwitch, you'll see that the VM port group has been created and VLAN successfully assigned.

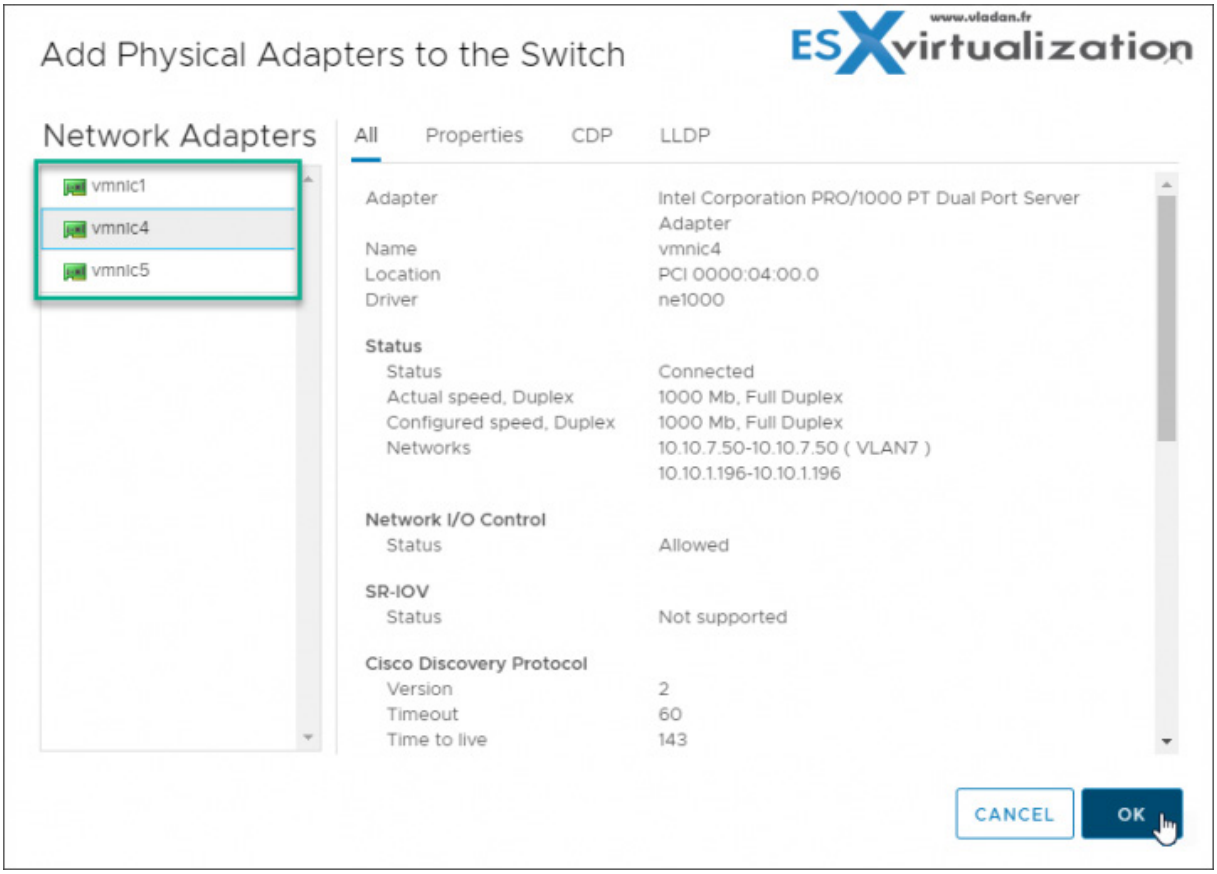
But as you can see, we don't have any physical adapters connected to our vSwitch, so no VMs will be able to communicate to the outside world.



We can add some physical adapters to a vswitch any time. Just click the **Manage Physical Adapters** button and then the **Green PLUS sign.**



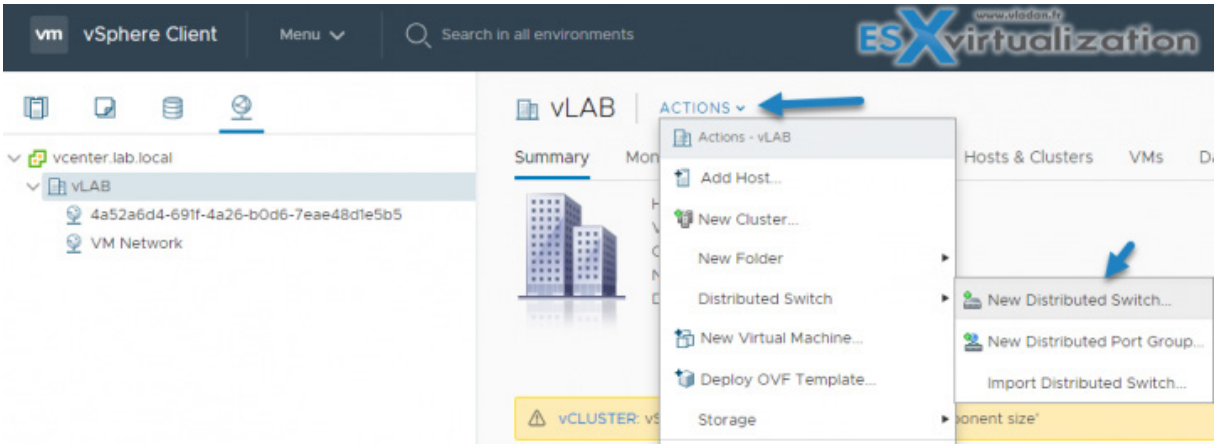
Then choose from the physical adapters you have available on the host.



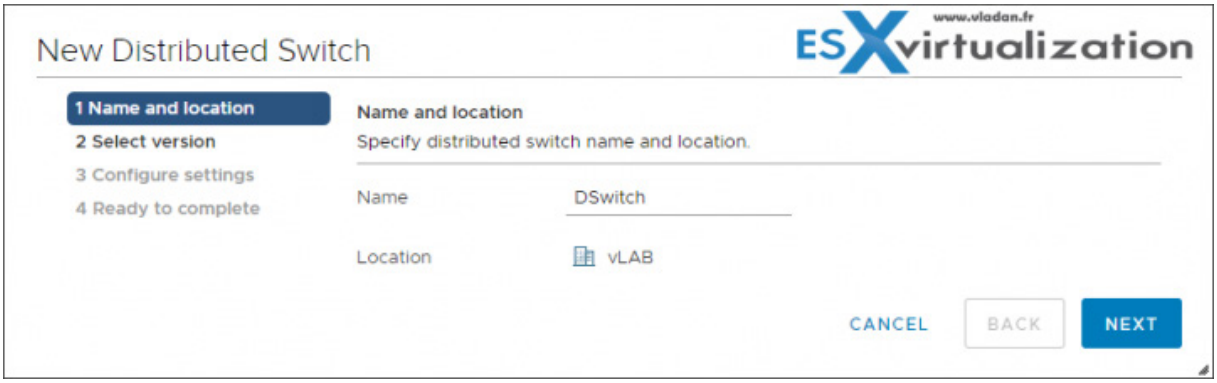
vSphere Distributed Switch (vDS) - is a single switch where all hosts share the config. It provides centralized provisioning, administration, and monitoring of virtual networks, and is configured at the vCenter level, not at the host level like in the case of vSS. This is an advantage as you can change the config on a single place instead of going to each ESXi individually.

Distributed port group – is a port group associated with a vSphere distributed switch that specifies port configuration options for each member port.

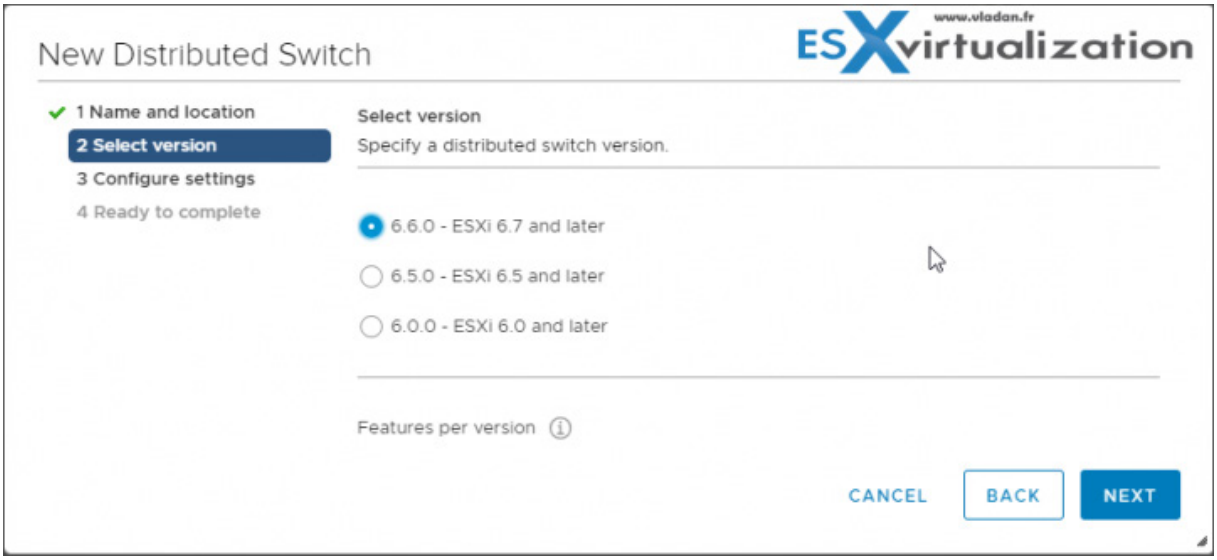
How do you create vDS?



A new wizard will pop up. You'll need to put in a name for the dvSwitch.

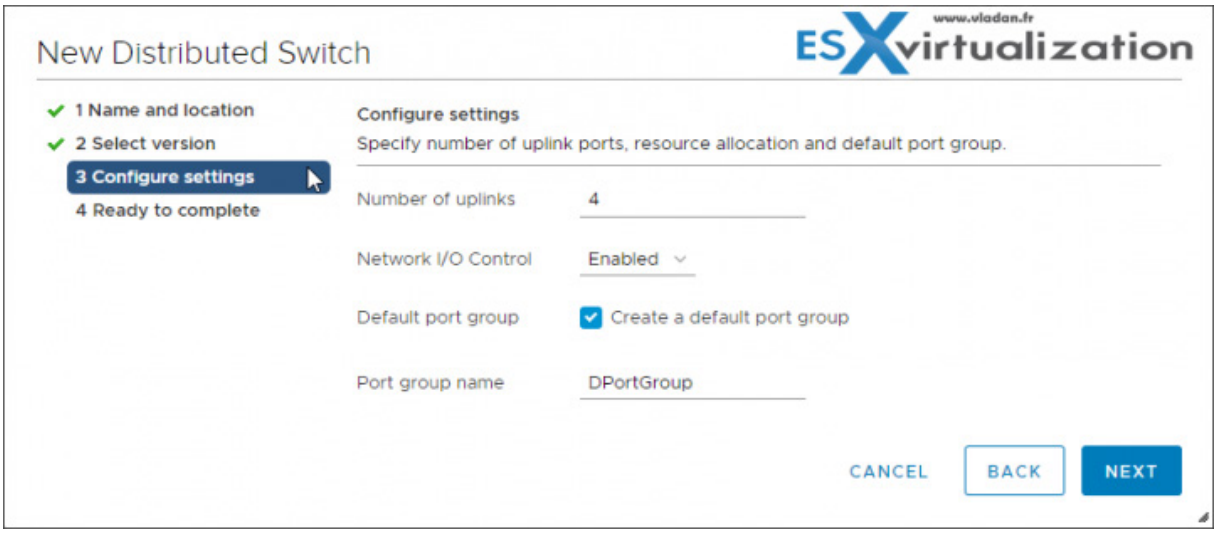


And also chose a version.



The next screen allows you to add the **Number of Uplinks** you like and choose to **Enable Network IO control (NIOC) at the dvSwitch level**. Also, as is the case during the VSS creation, you have the possibility to create a **default port group** and name it.

Uplink ports connect the distributed switch to physical NICs on associated hosts. The number of uplink ports is the maximum number of allowed physical connections to the distributed switch per host.

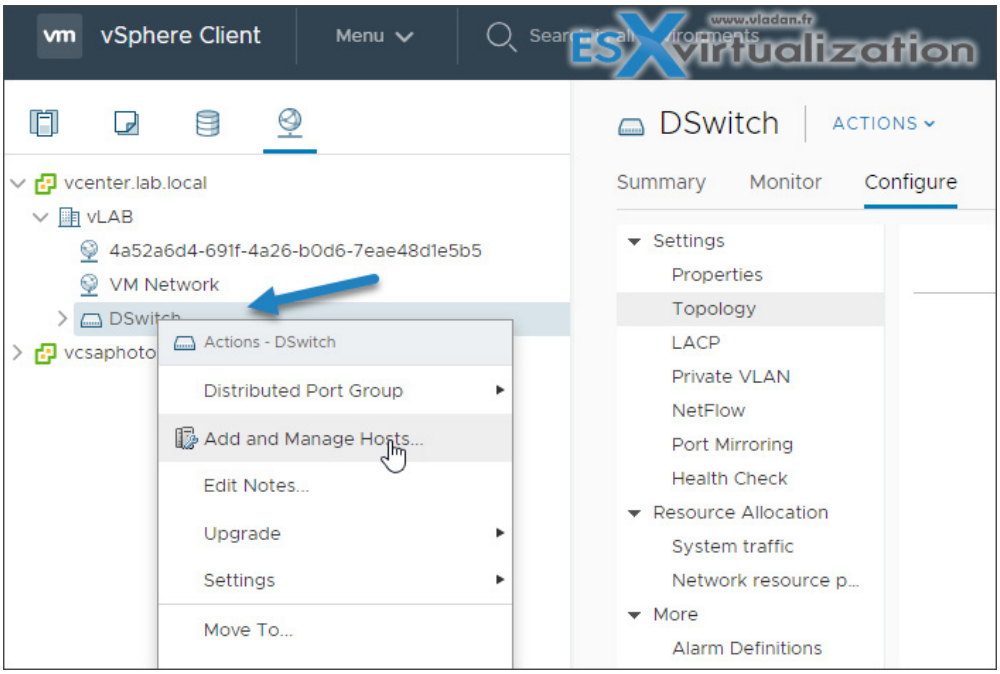


A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

Once your vDS is created, you can see the view and the configuration options here. Next would be to attach hosts to your dvSwitch.

There you can:

- Edit settings – change number of uplinks, change the name of VDS, enable/disable Network I/O control (In Advanced: change MTU, change Multicast filtering mode, Change Cisco discovery protocol settings)
- Edit Private VLAN
- Edit Netflow
- Edit Health Check
- Export Configuration
- Restore Configuration



You can use the Add and Manage Hosts wizard in the vSphere Web Client to add multiple hosts at a time.

In order to connect your host to a vSphere Distributed Switch (vDS) you should think twice and prepare ahead.

Ahead of time, you might want to do the following:

- Create distributed port groups for VM networking
- Create distributed port groups for VMkernel services, such as vMotion, VSAN, FT etc...
- Configure a number of uplinks on the distributed switch for all physical NICs that you want to connect to the switch

Removing Hosts from a vSphere Distributed Switch – Before you remove hosts from a distributed switch, you must migrate the network adapters that are in use to a different switch.

To add hosts to a different distributed switch, you can use the Add and Manage Hosts wizard to migrate the network adapters on the hosts to the new switch altogether. You can then remove the hosts safely from their current distributed switch.

To migrate host networking to standard switches, you must migrate the network adapters in stages. For example, remove physical NICs on the hosts from the distributed switch by leaving one physical NIC on every host connected to the switch to keep the network connectivity up. Next, attach the physical NICs to the standard switches and migrate VMkernel adapters and virtual machine network adapters to the switches. Lastly, migrate the physical NIC that you left connected to the distributed switch to the standard switches.

I'd like to invite you to check our detailed post on vSphere networking from our VCP6.5-DCV Study Guide. **VCP6.5-DCV Objective 2.1 – Configure policies/features and verify vSphere networking**. There are several sub-chapters which go quite deep in the different vDS configuration options which we won't be able to cover in this post.

Also, you'll have the possibility to download and study from the official VMware PDF called *vSphere Networking.*

Objective 4.6 - Deploy and configure VMware vCenter Server Appliance (VCSA)

In this objective, we'll show you how to set up the main piece of VMware infrastructure - a vCenter server running on Linux Photon OS - VMware vCenter Server Appliance (VCSA). For the past several years, VMware has been trying to break out from Windows dependency since 6.5 and now with 6.7, the feature set of VCSA is even larger than vCenter server on Windows.

Also, the 6.7 is also the last version where admins still have the possibility to install vCenter server on Windows platform. Next major release of vSphere will only be running on Linux.

The VCSA is running **Photon OS** which is a VMware own lightweight distribution, optimized for fast booting, security, and scalability. During a long time, VMware was using Suse Linux Enterprise Server (SLES) distribution, but the fact that VMware did not own the stack was a hinderance to faster development.

During the deployment of the appliance, you select a deployment type of vCenter Server with an embedded Platform Services Controller (PSC), Platform Services Controller, or vCenter Server with an external PSC. When you deploy a PSC appliance, you can create a VMware vCenter Single Sign-On domain or join an existing domain.

VMware vCenter Server Appliance (vCSA) 6.7 supports embedded deployment where vCenter Server and Platform Service Controller (PSC) are on the same node. So you can join another node with the VCSA + PSC. This architecture is called an **Embedded Linked Mode (ELM).**

What are the advantages? You can manage all vCenters which are linked within the same SSO Domain. You don't have to re-log in with your browser session to multiple vCenter server sessions. The vCenter Servers appear all within the same browser window session.

System Requirements for VCSA deployments

Check system requirements, hardware requirements, storage requirements, required ports for vCenter server and PSC. Documentation Set PDF: "*vCenter Server Installation and Setup Update 1*", **Pages 25-34.**

VMware delivers a single ISO which does it all, with built-in tools. This single ISO has everything so you can **Install, Upgrade, Migrate or Restore.** Mount the ISO to see the file structure.

We'll need at least one ESXi host, and then no matter which OS you are on, (Linux, Windows or Mac OS) you simply chose the one corresponding for your environment, and execute the installer.

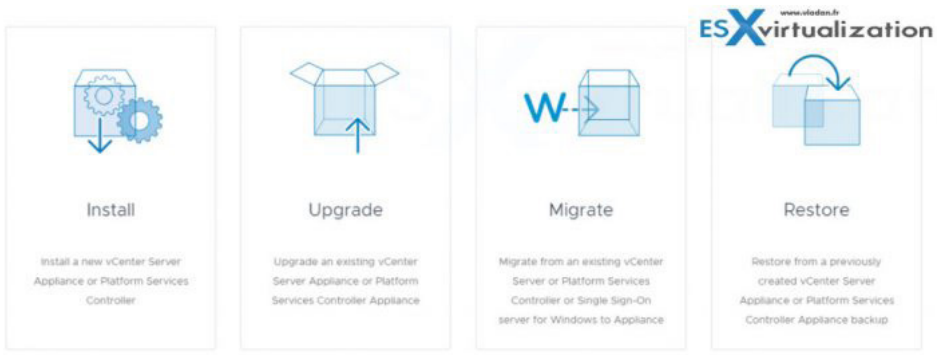
If you're looking at the folder structure, you'll see that there is a vcsa-ui-installer and inside we have 3 folders:

lin64

mac

win32

With that in mind, let's kick the tires and execute the host from win32 as we're right now on Windows workstation. You'll see the four operations which are available. Click the first one – Install, and let's follow the necessary steps.



We'll be doing a clean install.

Note: Before we get started, observe that we have created a forward and reverse DNS records on our DNS server.

All you need is an ESXi host, and to download the VCSA ISO.

Note that you can also use VMware Workstation which now has the possibility of installing VCSA for lab training.

The process consists of two phases:

- Deployment
- Configuration

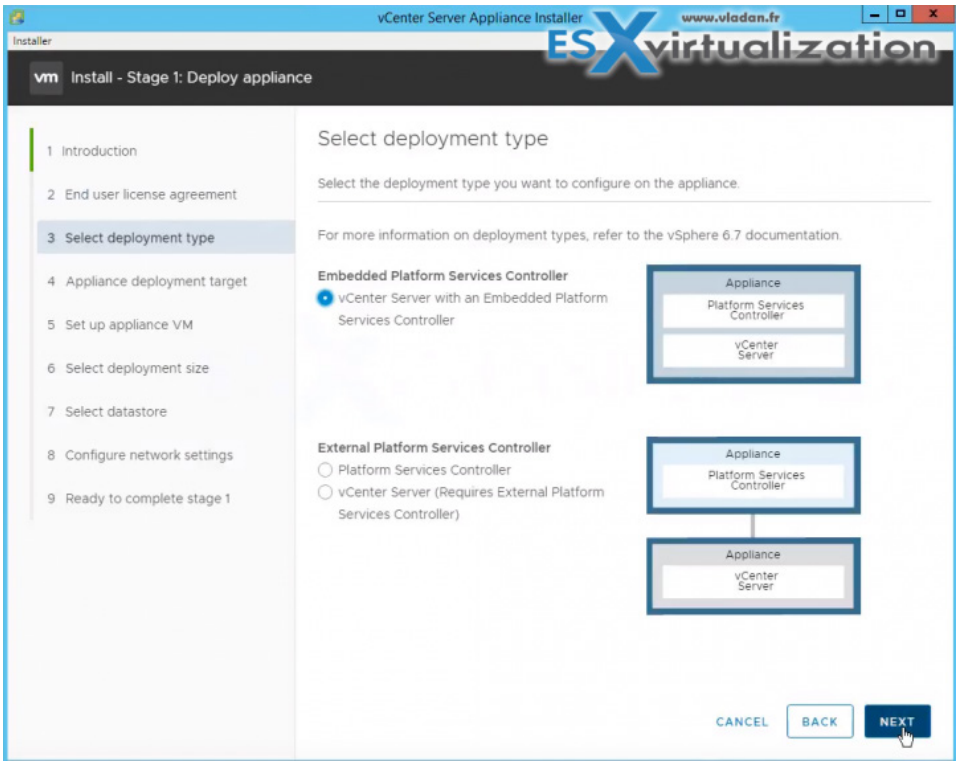
One of the initial choices is the choice between **embedded** or **separate PSC** deployment types.

With vCenter Embedded Linked Mode, you can connect a vCenter Server Appliance with an embedded Platform Services Controller together to form a domain. vCenter Embedded Linked

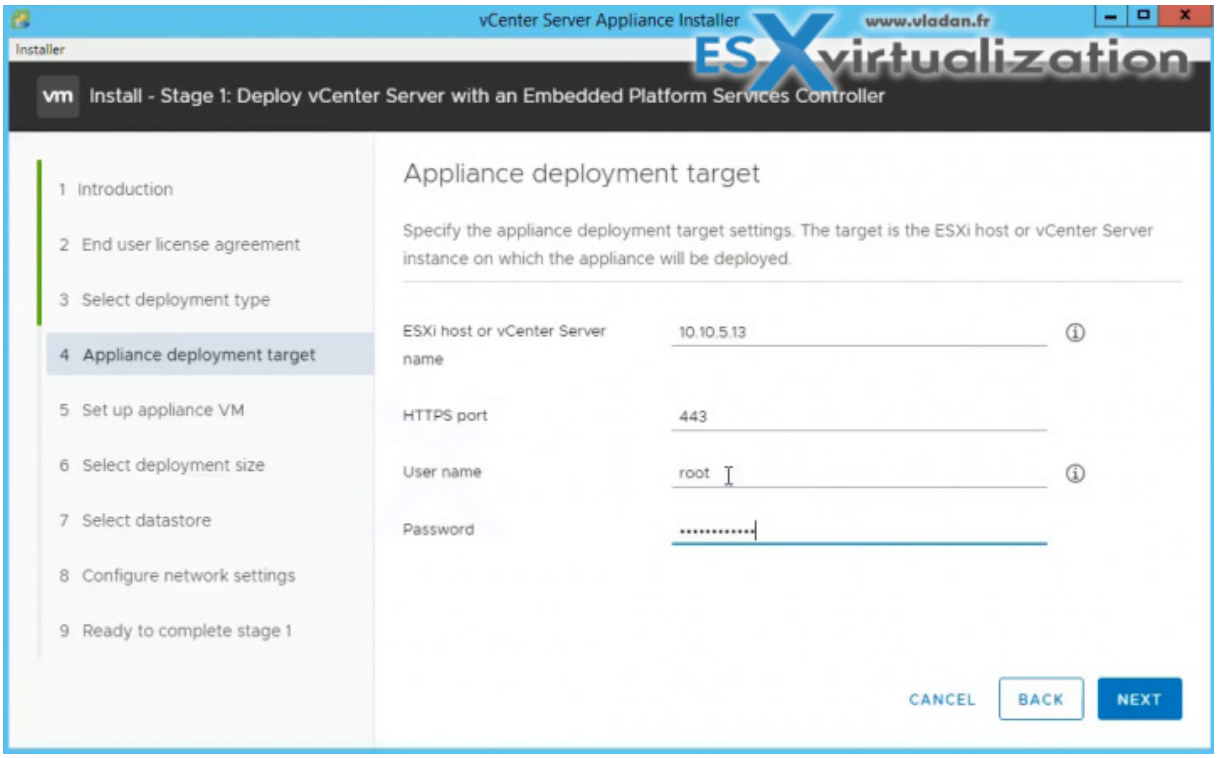
Mode is not supported for Windows vCenter Server installations. vCenter Embedded Linked Mode is supported starting with vSphere 6.5 Update 2 and is suitable for most deployments.

Embedded Linked Mode has:

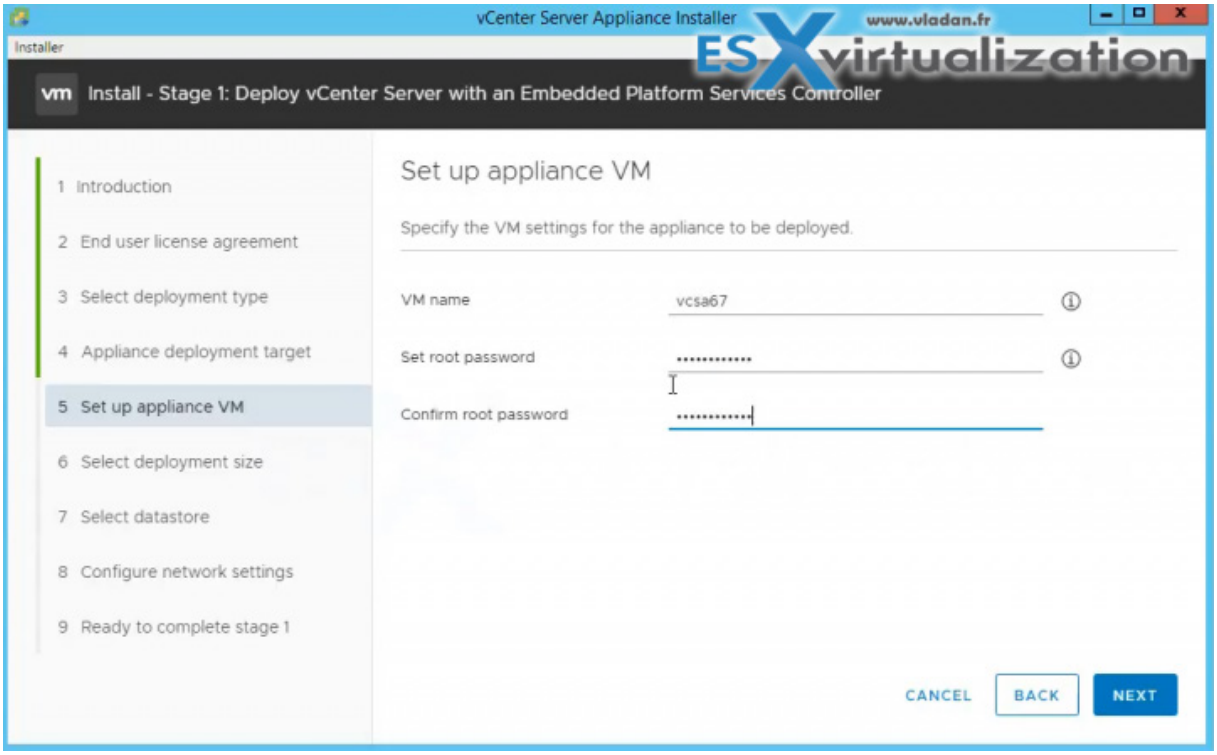
- No external PSC
- Simplified backup and restore
- Simplified HA process
- **Up to 15** vCSA's can be linked together using vCenter Embedded Linked Mode and displayed in a single inventory view.



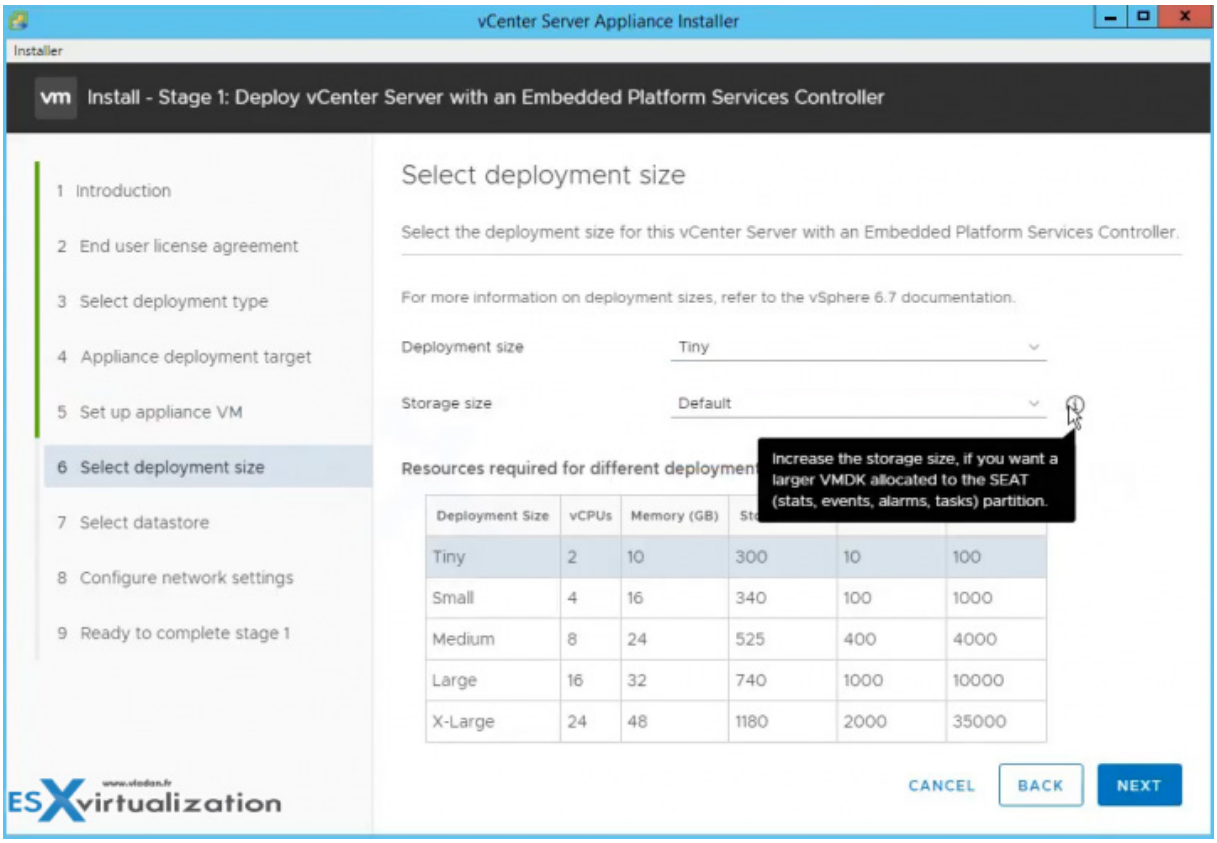
Specify a target - ESXi or an existing vCenter Server.



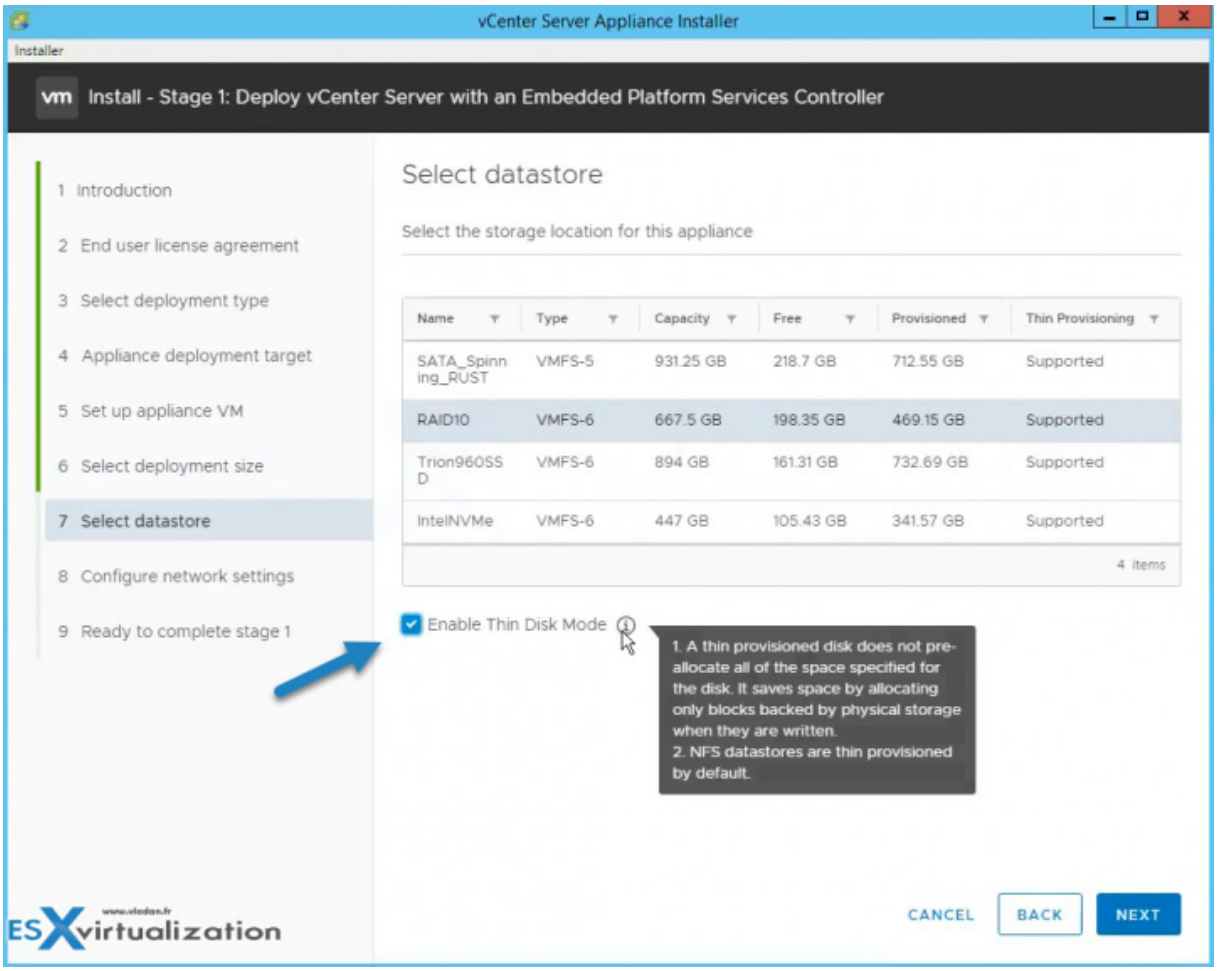
Set up the appliance VM (VM name, root password…).



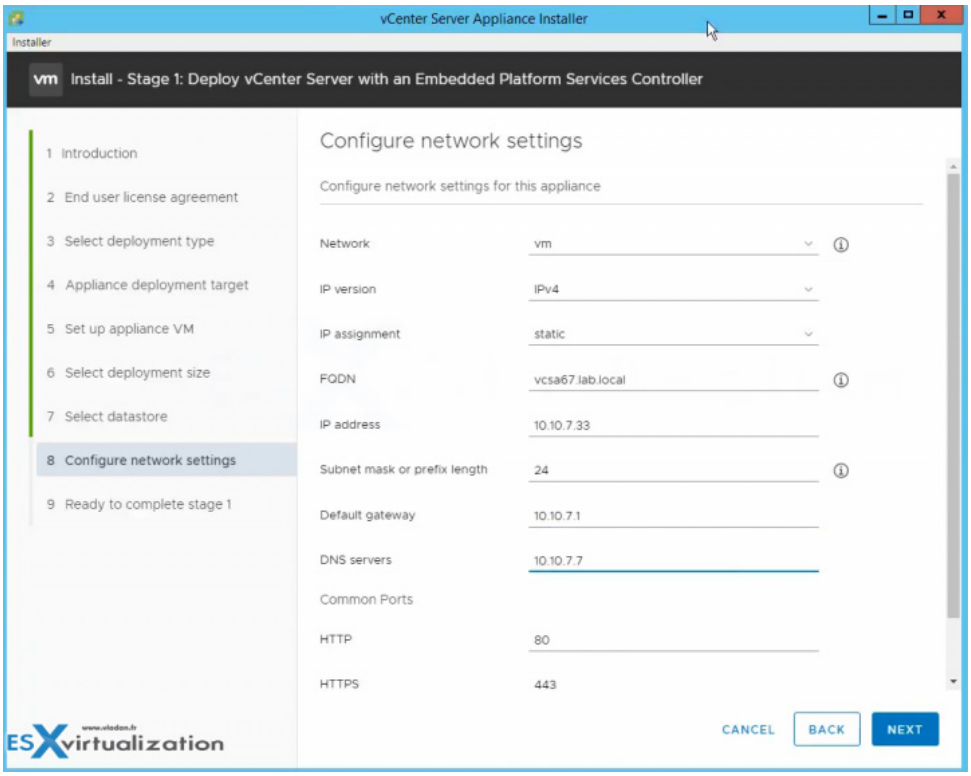
And the deployment size. Note that you can also adjust the disk sizes.



The next step is to choose a datastore location where the VM will be stored; you can also tick “use thin disks” which allows you to save some disk space.

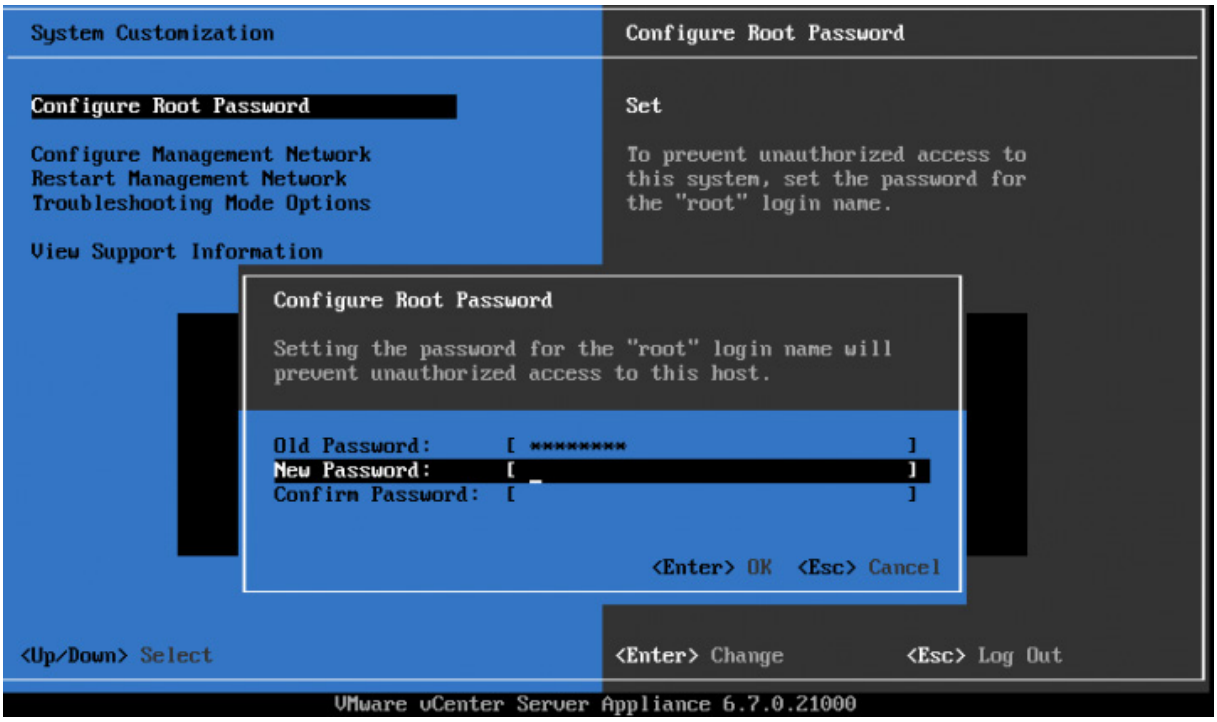


Next we need to configure networking. Make sure to double check before validating. If not, your deployment might fail.

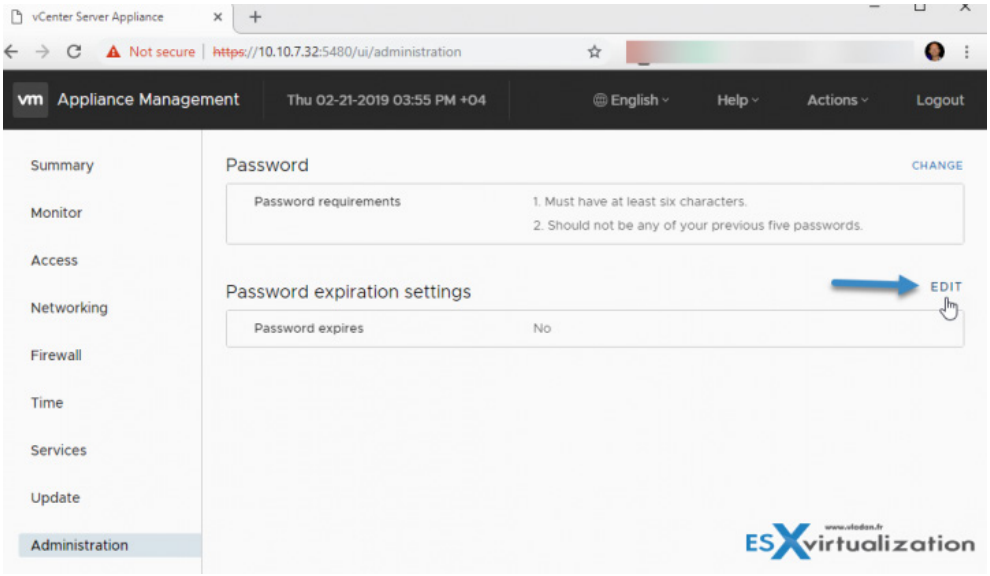


Then you'll have one final page where you just need to check whether everything is configured as it should be for the 1st phase - deployment.

After a while, when you see that on the console, you have a message saying that you must configure a root password, just log in to the console and configure the root password.



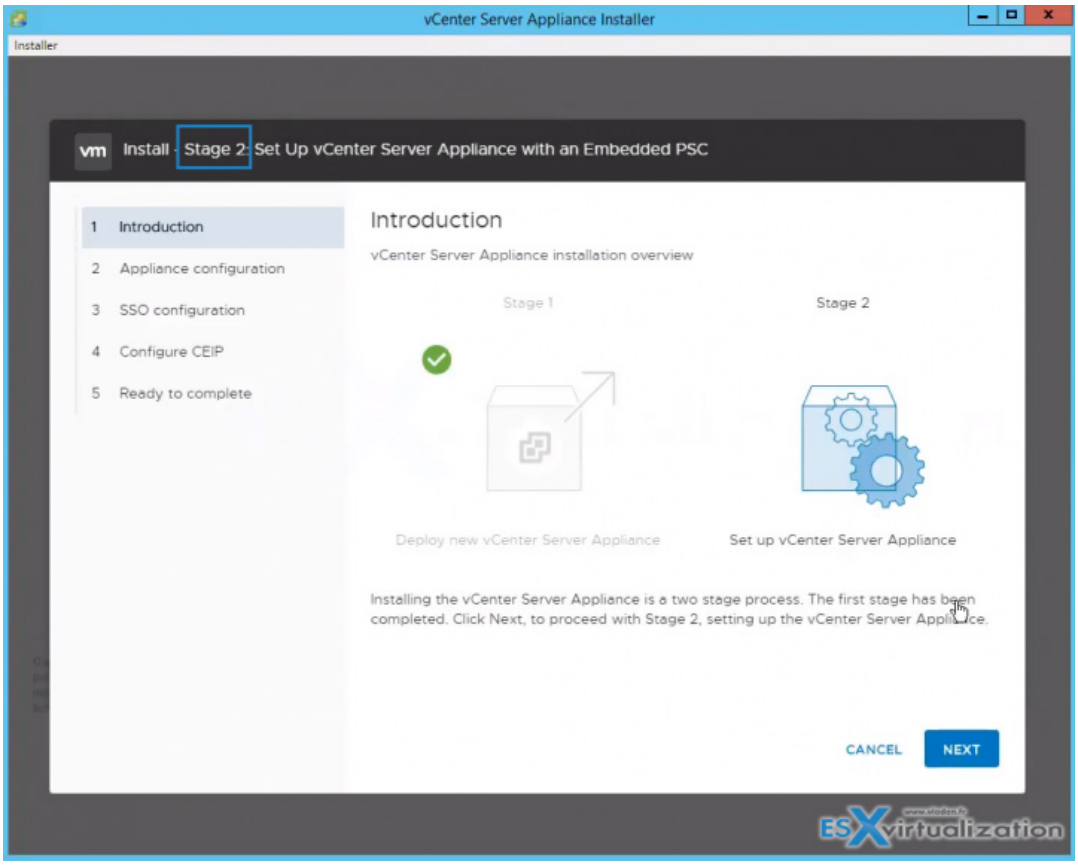
Please note that this root password **will expire in 365 days**. In case you do not want this password to expire, wait until the VCSA appliance is configured and go to the VAMI user interface via https://FQDN_or_IP_VCSA:5480 > login > Administration > Click **Edit** next to the **Password expiration settings**.



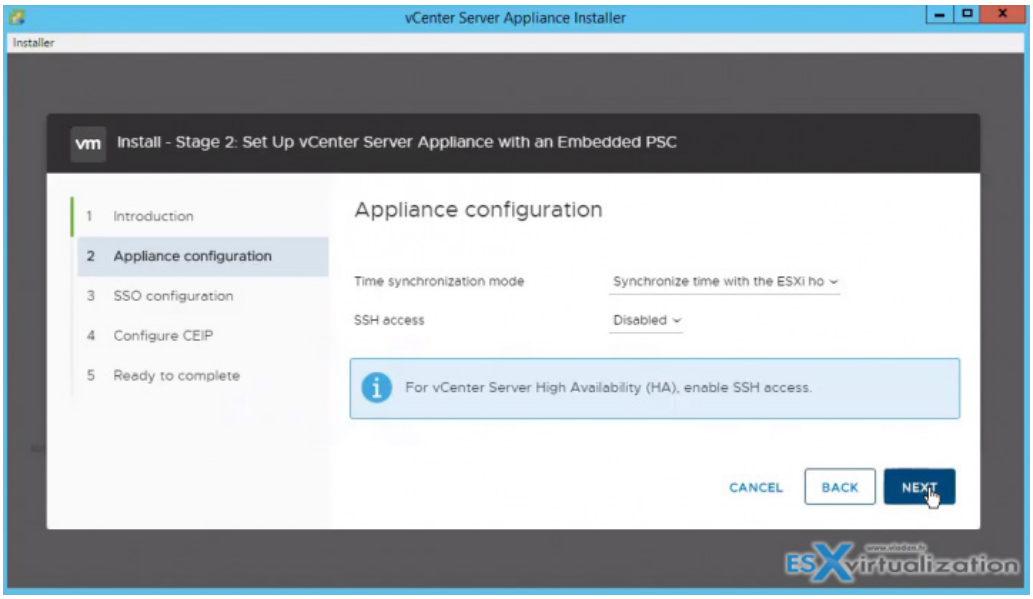
While there, you can also set Networking, Time servers (NTP), check services and/or update to the latest version.

- VMware vCenter Server Appliance (VCSA) – Manage Firewall Settings
- vSphere 6.7 Configuration Maximums

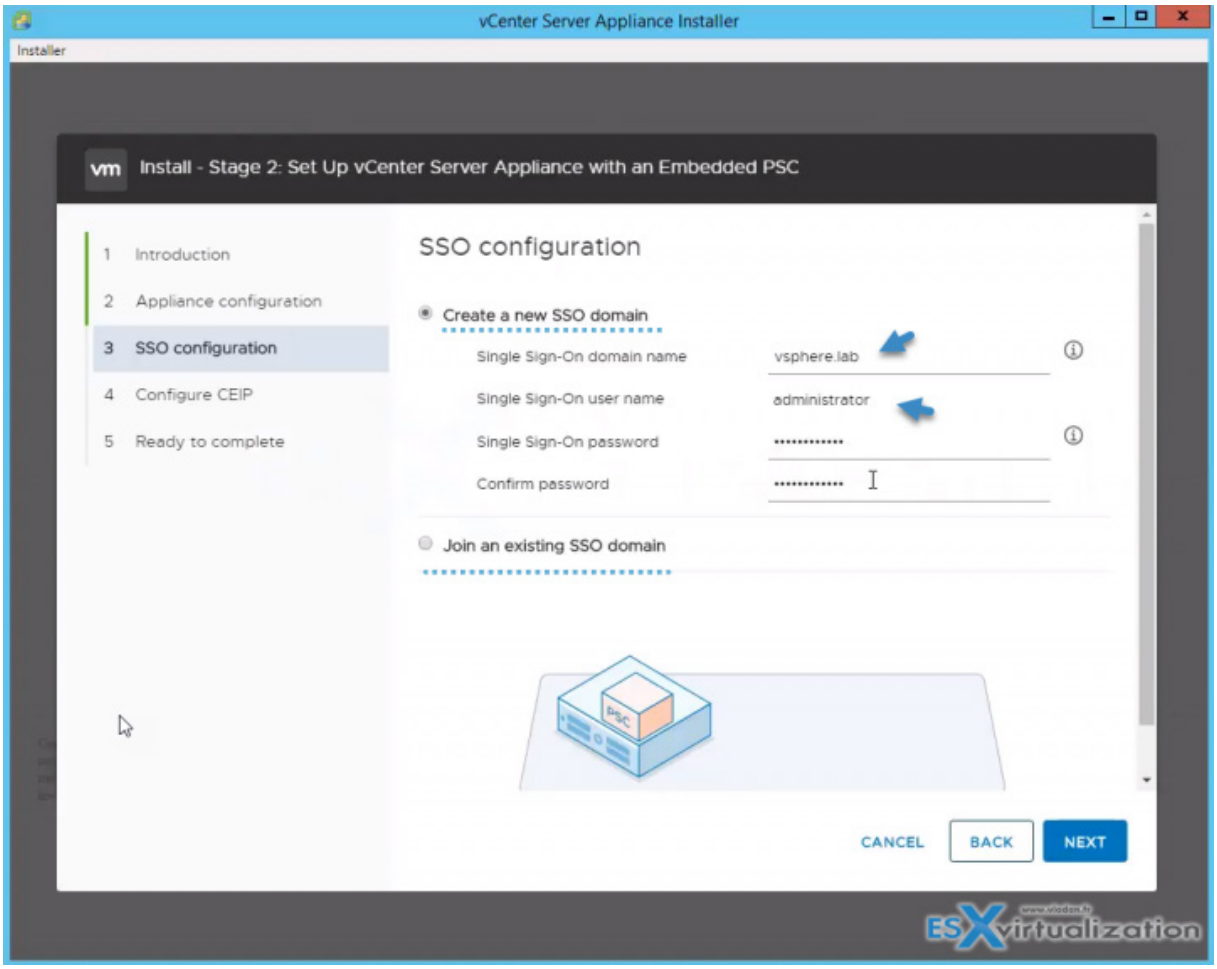
Phase 2 - Setup vCenter Server Appliance



And then we have some options concerning Time synchronization mode which can be either via ESXi or external (via NTP servers).



The Next screen shows the SSO configuration, where we can either create a new SSO domain or join an existing SSO domain. You'll need to create a new domain name and password if that you are creating a new SSO domain.



You can join CEIP on the next page (Optional) and then, you're ready to launch the Phase 2: Configuration. Once it is done, you can log in at

https://IP_or_FQDN/UI

CLI Deployment of VMware VCSA

The CLI deployment process includes downloading the vCenter Server Appliance installer on a network virtual machine or physical server from which you want to perform the deployment, preparing a JSON configuration file with the deployment information, and running the deployment command.

The ISO file contains templates of JSON files that contain the minimum configuration parameters that are required for deploying the vCSA or PSC.

For a complete list of the configuration parameters and their descriptions, navigate to the installer subdirectory for your operating system and run this command:

- vcsa-deploy install --template-help command

In the vCenter Server Appliance installer, navigate to the vcsa-cli-***installer*** directory, and open the templates subfolder.

Check the full syntax at Documentation Set PDF: "*vCenter Server Installation and Setup Update 1*", **Pages 79-80.**

We can't say for sure if we covered everything that's needed but have included this chapter as a guideline. Your principal study material should be the Documentation Set PDF: "*vCenter Server Installation and Setup Update 1,* as well as your home lab.

Objective 4.7 - Set up identity sources

Today we'll continue configuring our VMware vCenter Server Appliance (VCSA), and cover a topic from **Professional vSphere 6.7 Exam 2019** - **VCP6.7-DCV Objective 4.7 – Set up identity sources**.

Setup Identity sources

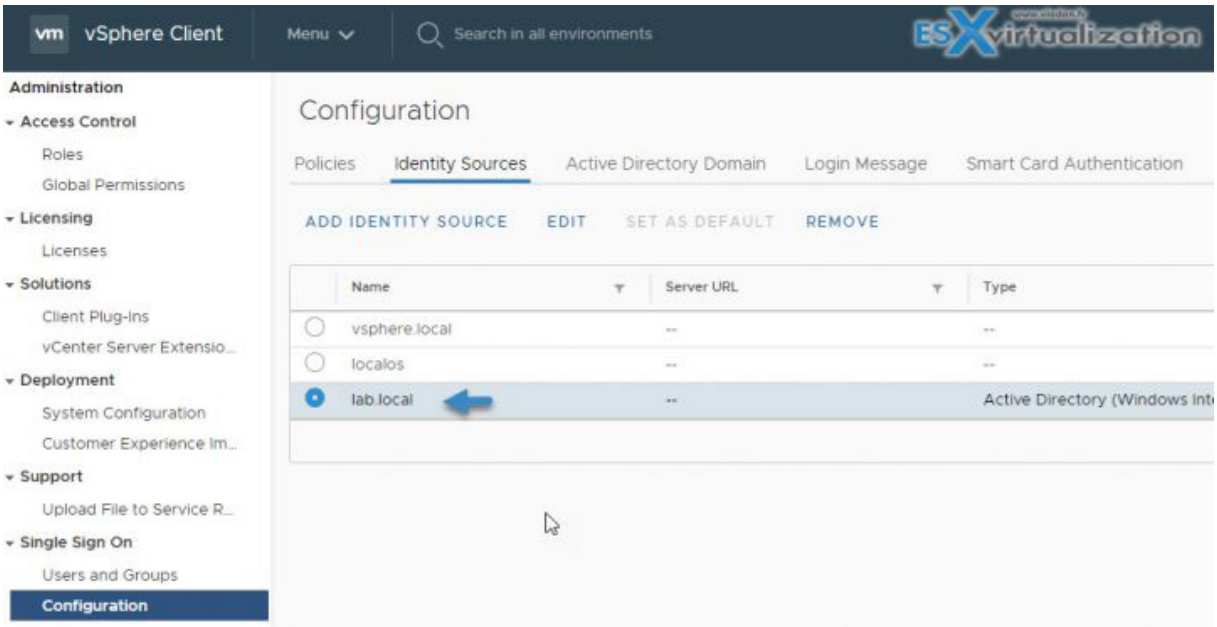
In our case, we'll explore the vCenter and embedded Platform Service Controler (PSC).

After installation of VCSA, you connect to the UI as administrator@vsphere.local and go to **Administration,> Single Sign-On > Configuration > Identity Sources > Add Identity Source**.

As you can see, there are 4 different options:

- Active Directory Windows Integrated Identification
- Active Directory Over LDAP
- Open LDAP
- Local operating system of SSO server

In our example, we use our Microsoft Active Directory (AD) domain for the lab. This is the most common scenario since Microsoft AD is the de facto standard when it comes to authentication and user's access to resources.



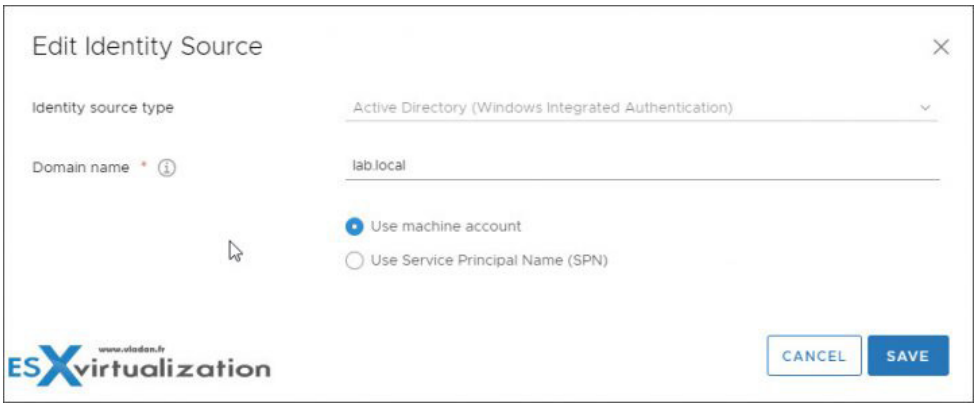
Whether you are installing your PSC as an embedded component together with vCenter server or a separate PSC, you'll have to set up SSO and Identity sources.

When you install a PSC, you are invited to create a vCenter SSO domain or join an existing domain. The vSphere domain name is used by the VMware Directory Service (vmdir) for all Lightweight Directory Access Protocol (LDAP) internal structuring.

With vSphere 6.0 and later, you can give your vSphere domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services. You cannot change the domain to which a Platform Services Controller or vCenter Server instance belongs.

If you are upgrading from vSphere 5.5, your vSphere domain name remains the default (vsphere.local). For all versions of vSphere, you cannot change the name of a domain.

After you specify the name of your domain, you can add users and groups. It usually makes more sense to add an Active Directory or LDAP identity source and allow the users and groups in that identity source to authenticate. You can also add vCenter Server or Platform Services Controller instances, or other VMware products, such as vRealize Operations, to the domain.

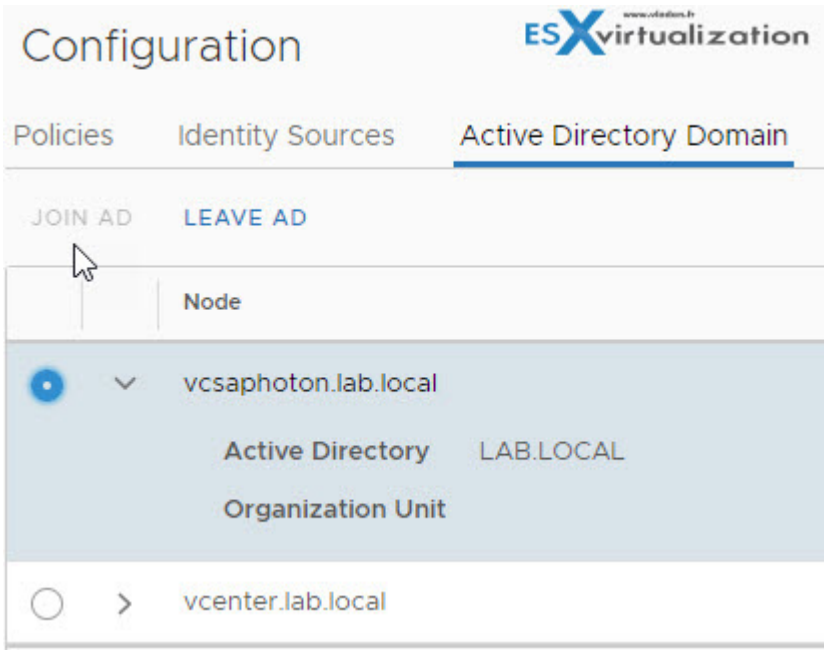


- **Service Principal Name (SPN)** - Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
- **Use Machine account** - you'll use this option to use the local machine account (computer acount in AD) as Service principal name (SPN). In this case, you'll need to specify only the domain name (do not select this option if you planning to rename this machine).

However, please note that:

Before you add the AD as an Identity source you'll have to **join the VM to Microsoft AD and reboot.** You'll do that on the Active Directory Domain TAB.

You can see the screenshot here:



After that, you'll have to configure permission for AD users, so that users and groups from the joined Active Directory domain can access the vCenter Server components.

Objective 4.8 - Configure an SSO domain

Today we'll cover another objective from VCP-DCV 2019 certification and we'll talk about VMware clusters.

You should not rely on our information only but use those guides as a complementary resource. Perhaps it is also a good idea to download the older **VCP6.5-DCV study guide PDF** as the structure of each chapter is much more detailed and, quite frankly, gives better support to study.

vCenter SSO allows vSphere components to communicate with each other through a secure token mechanism. vCenter SSO uses:

- Security Token Service (STS)
- SSL for secure traffic
- Authentication of users through Microsoft AD or OpenLDAP
- Authentication of solution through certificates

Check vSphere ***Platform Services Controler Administration PDF*** for further explanation on how SSO and handshakes works.

Each Platform Services Controller (PSC) is associated with a vCenter Single Sign-On domain. The domain name defaults to vsphere.local, but you can change it during the installation of the first Platform Services Controller.

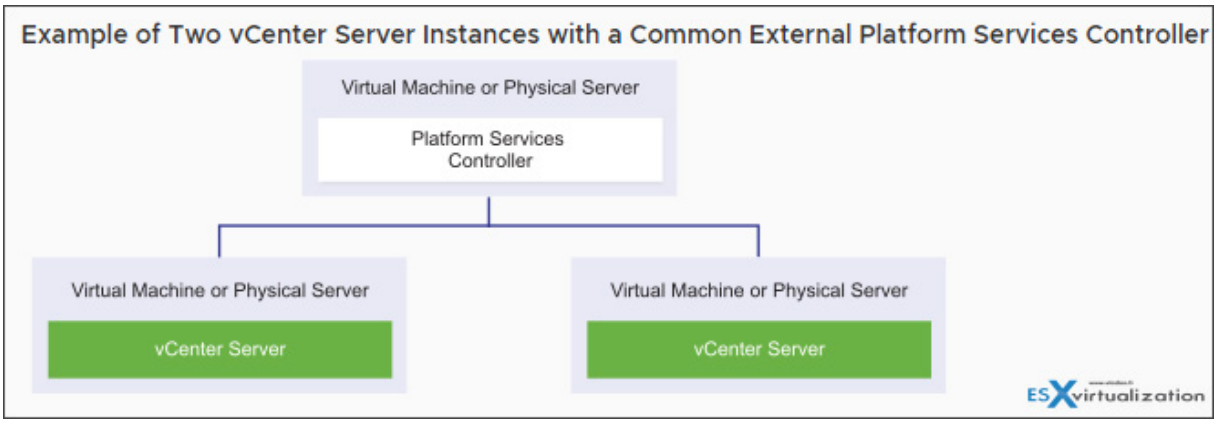
Tip: What is the VMware Platform Services controller (PSC) ?

The domain determines the local authentication space. You can split a domain into multiple sites and assign each Platform Services Controller and vCenter Server instance to a site. Sites are logical constructs, but usually, correspond to geographic location.

You can organize Platform Services Controller domains into logical sites. A site in the VMware Directory Service is a logical container for grouping Platform Services Controller instances within a vCenter Single Sign-On domain.

Deployment types:

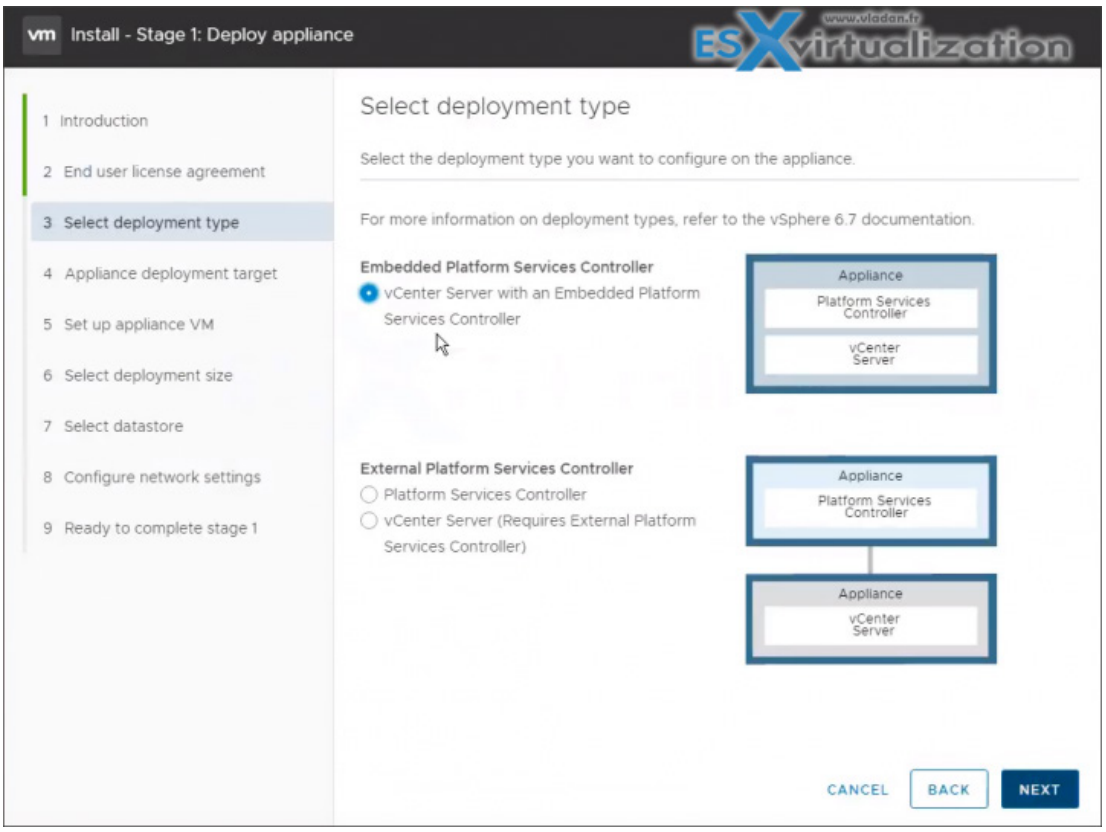
- **Embedded** - All services that are bundled with the Platform Services Controller are deployed together with the vCenter Server services on the **same virtual machine** or **physical server.**
- **External** - Only the vCenter Server services are deployed on the virtual machine or physical server. You must register such a vCenter Server instance with a Platform Services controller instance that you previously deployed or installed.



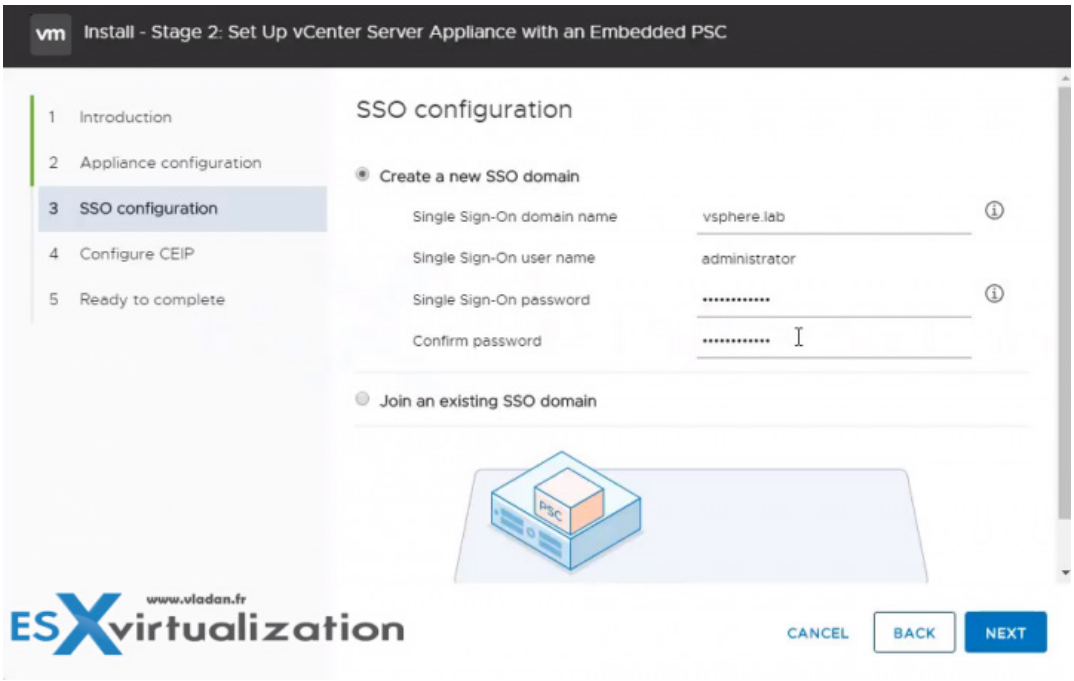
It is worth noting that:

With vSphere 6.7 Update 2, VMware is announcing the deprecation of external PSCs. With VMware vCenter Server enhanced link mode introduced in vSphere 6.7, infrastructure teams can link up to fifteen vCenter Server instances in the embedded PSC topology, eliminating the need for load balancers and simplifying architectures.

When deploying a new VCSA, you have the choice to deploy embedded or external PSC.



During the configuration phase, you have to specify the SSO domain, or join an existing SSO domain. Also, you have to create or enter the administrator's password.

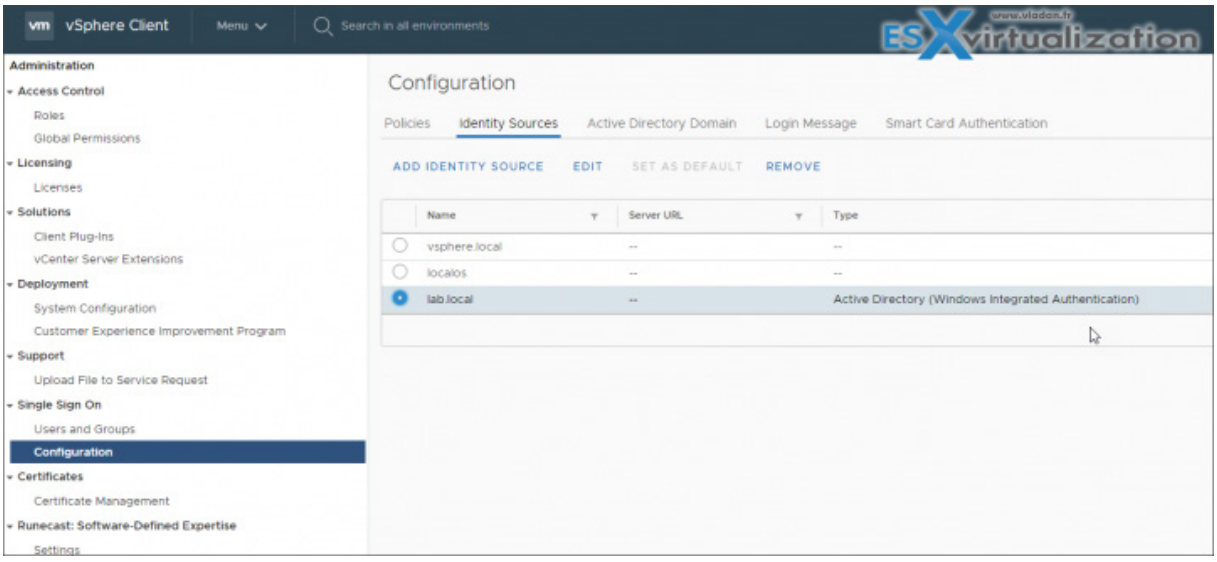


Once the VCSA is deployed, you can access the SSO config through **Administration > SSO**

Once there, you must join the PSC to Microsoft AD and only then add AD as an identity source.

Using the vSphere Client, log in to a vCenter Server associated with the Platform Services Controller (PSC) as a user with administrator privileges in the local vCenter Single Sign-On domain.

Select Administration > Expand Single Sign-On and click Configuration > Click Active Directory Domain > Click Join AD, specify the domain, optional organizational unit, and user name and password, and click Join.



Other than Microsoft AD (starting with version WS 2003) you can configure the identity source as OpenLDAP in vSphere client.

If you select the Active Directory (Integrated Windows Authentication) identity source type, you can use the local machine account as your SPN (Service Principal Name) or specify an SPN explicitly. You can use this option only if the vCenter Single Sign-On server is joined to an Active Directory domain, as is the case in our example.

vCenter SSO Components

STS (security token service) - This service issues security assertion markup language (SAML) tokens. Those tokens represent the identity of a user in one of the identity source types supported by vCenter SSO. The vCenter Single Sign-On service signs all tokens with a signing certificate and stores the token signing certificate on a disk. The certificate for the service itself is also stored on the disk.

Administration Server - allows users with admin privileges to vCenter SSO to configure the SSO server and manage users and groups from the vSphere web client.

Do not name the domain name with your Microsoft Active Directory or OpenLDAP domain name.

VMware Directory Service (vmdir) - the VMware Directory service (vmdir) is associated with the domain you specify during installation and is included in each embedded deployment and on each Platform Services Controller. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available on port 389. The service still uses port 11711 for backward compatibility with vSphere 5.5 and earlier systems. It stores SSO information as well as certificate information.

Identity Management Service - handles identity sources and STS authentication requests.

To configure vCenter Single Sign-On and manage vCenter Single Sign-On users and groups, the user administrator@vsphere.local or a user in the vCenter Single Sign-On Administrators group must log in to the vSphere Client. After authentication, that user can access the vCenter Single Sign-On administration.

Authenticated users can view all vCenter Server instances or other vSphere objects for which their role gives them privileges. No further authentication is required. After installation, the administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, has administrator access to both vCenter Single Sign-On and vCenter Server.

That user can then add identity sources, set the default identity source, and manage users and groups in the vCenter Single Sign-On domain.

There are some advantages when installing PSC on the same machine over having a separate PSC within your environment. The connection between vCenter Server and the Platform Services

Controller is not over the network, and vCenter Server is not prone to outages caused by connectivity and name resolution issues between vCenter Server and the Platform Services Controller.

You'll configure SSO during the installation of the vCenter server and PSC (if installing embedded PSC). When you install a Platform Services Controller, you are prompted to create a vCenter Single Sign-On domain or join an existing domain.

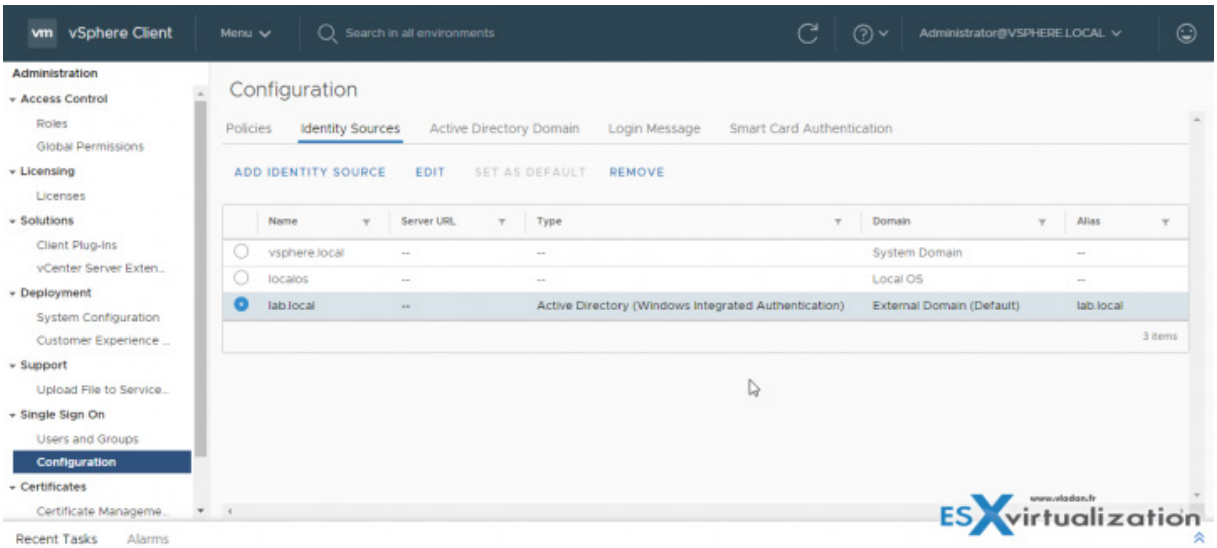
The domain name is used by the VMware Directory Service (vmdir) for all Lightweight Directory Access Protocol (LDAP) internal structuring. With vSphere 6.0 and later, you can give your vSphere domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

Note: You cannot change the domain to which a Platform Services Controller or vCenter Server instance belongs.

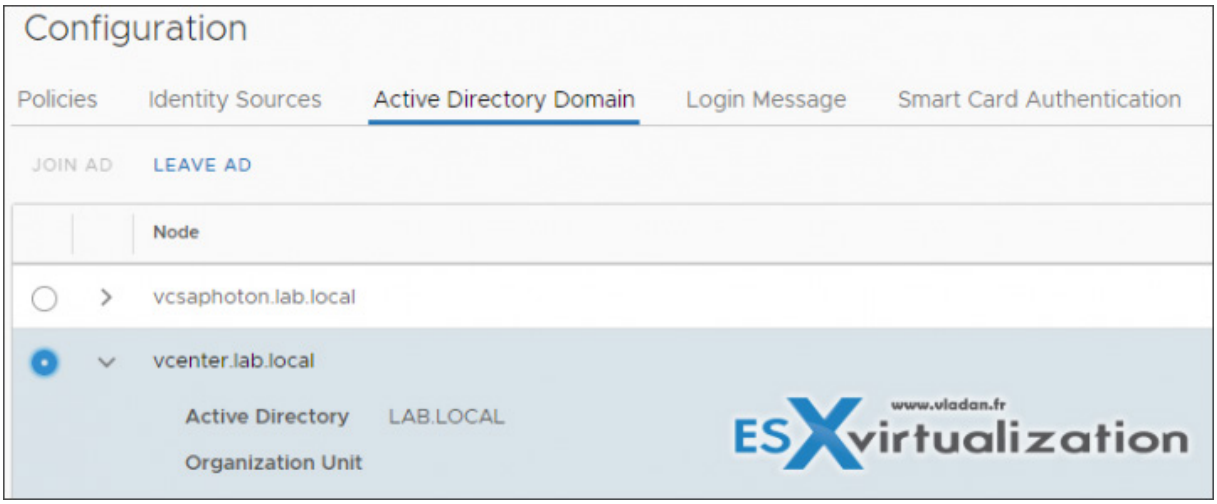
After installation, the administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, has administrator access to both vCenter Single Sign-On and vCenter Server. That user can then add identity sources, set the default identity source, and manage users and groups in the vCenter Single Sign-On domain.

The SSO and identity sources can be found when you go to **Menu > Administration > Single Sign-On > Configuration**

Where to set a default SSO domain?



There you can add other identity sources. As you can see, I have added my Microsoft Active Directory (AD). However, you must add the Platform services controller in advance to an active directory domain.



Groups in vCenter SSO Domain

The vCenter Single Sign-On domain has some predefined groups. If you add users to one of those groups, they will be able to perform the corresponding actions.

For all objects in the vCenter Server hierarchy, you can assign permissions by pairing a user and a role with the object. For example, you can select a resource pool and give a group of users reading privileges to that resource pool object by giving them the corresponding role. For some services that are not managed by vCenter Server directly, membership in one of the vCenter Single Sign-On groups determines the privileges.

For example, a user who is a member of the Administrator group can manage vCenter Single Sign-On. A user who is a member of the CAAdmins group can manage the VMware Certificate Authority, and a user who is in the LicenseService.Administrators group can manage licenses.

Groups in the vsphere.local Domain

Privilege	Description
Users	Users in the vCenter Single Sign-On domain (vsphere.local by default).
SolutionUsers	Solution users group vCenter services. Each solution user authenticates individually to vCenter Single Sign-On with a certificate. By default, VMCA provisions solution users with certificates. Do not add members to this group explicitly.
CAAdmins	Members of the CAAdmins group have administrator privileges for VMCA. Do not add members to this group unless you have compelling reasons.
DCAdmins	Members of the DCAdmins group can perform Domain Controller Administrator actions on VMware Directory Service. **Note** Do not manage the domain controller directly. Instead, use the `vmdir` CLI or vSphere Client to perform corresponding tasks.
SystemConfiguration.BashShellAdministrators	This group is available only for vCenter Server Appliance deployments. A user in this group can enable and disable access to the BASH shell. By default a user who connects to the vCenter Server Appliance with SSH can access only commands in the restricted shell. Users who are in this group can access the BASH shell.
ActAsUsers	Members of Act-As Users are allowed to get Act-As tokens from vCenter Single Sign-On.
ExternalIPDUsers	This internal group is not used by vSphere. VMware vCloud Air requires this group.
SystemConfiguration.Administrators	Members of the SystemConfiguration.Administrators group can view and manage the system configuration in the vSphere Client. These users can view, start and restart services, troubleshoot services, see the available nodes, and manage those nodes.
DCClients	This group is used internally to allow the management node access to data in VMware Directory Service. **Note** Do not modify this group. Any changes might compromise your certificate infrastructure.
ComponentManager.Administrators	Members of the ComponentManager.Administrators group can invoke component manager APIs that register or unregister services, that is, modify services. Membership in this group is not necessary for read access on the services.
LicenseService.Administrators	Members of LicenseService.Administrators have full write access to all licensing-related data and can add, remove, assign, and unassign serial keys for all product assets registered in the licensing service.
Administrators	Administrators of the VMware Directory Service (vmdir). Members of this group can perform vCenter Single Sign-On administration tasks. Do not add members to this group unless you have compelling reasons and understand the consequences.

vCenter Single Sign-On allows vSphere components to communicate with each other through a secure token mechanism. vCenter Single Sign-On uses the following services:

- STS (Security Token Service).
- SSL for secure traffic.
- Authentication of human users through Active Directory or OpenLDAP.
- Authentication of solution users through certificates

Please have a further look at *Platform Services controller Administration* PDF.

Objective 5.1 - Determine effective snapshot use cases

Today's topic is about snapshots, snapshot formats, and effective snapshot use cases. Today's post name is - VCP6.7-DCV Objective 5.1 - Determine effective snapshot use cases.

Snapshots let you capture the state of the virtual machine, including the virtual machine memory, settings, and virtual disks. You can roll back to the previous virtual machine state when needed. However, snapshots aren't backups. You should use a backup software leveraging snapshots to create first full and then incremental backups allowing you to restore.

When you take a snapshot, the state of the virtual disk is preserved, which prevents the guest operating system from writing to it, after which a delta or child disk is created. The delta represents the difference between the current state of the VM disk and the state that existed when you took the previous snapshot. On the VMFS datastore, the delta disk is a sparse disk.

Sparse disks use the copy-on-write mechanism, in which the virtual disk contains no data until the data is copied there by a write operation. This optimization saves storage space.

Depending on the type of your datastore, delta disks use different sparse formats.

Snapshot Formats	VMFS5	VMFS6
VMFSsparse	For virtual disks smaller than 2 TB.	N/A
SEsparse	For virtual disks larger than 2 TB.	For all disks.

ESXvirtualization

VMs with snapshots can be migrated. However, there are some considerations depending on the type of snapshot:

- If you migrate a VM with the VMFSsparse snapshot to VMFS6, the snapshot format changes to SEsparse.
- When a VM with a vmdk of a size smaller than 2 TB is migrated to VMFS5, the snapshot format changes to VMFSsparse.
- You cannot mix VMFSsparse redo-logs with SEsparse redo-logs in the same hierarchy

VMFSsparse - is a newer format which is implemented on the top of VMFS.

Quote:

VMFSsparse is implemented on top of VMFS. The VMFSsparse layer processes I/Os issued to a snapshot VM. Technically, VMFSsparse is a redo-log that starts empty, immediately after a VM snapshot is taken. The redo-log expands to the size of its base vmdk, when the entire vmdk is rewritten with new data after the VM snapshotting. This redo-log is a file in the VMFS datastore. Upon snapshot creation, the base vmdk attached to the VM is changed to the newly created sparse vmdk.

SEsparse - supports NMAP.

Quote:

SEsparse is a default format for all delta disks on the VMFS6 datastores. On VMFS5, SEsparse is used for virtual disks of the size 2 TB and larger. SEsparse is a format similar to VMFSsparse with some enhancements. This format is space efficient and supports the space reclamation technique. With space reclamation, blocks that the guest OS deletes are marked. The system sends commands to the SEsparse layer in the hypervisor to unmap those blocks. The unmapping helps to reclaim space allocated by SEsparse once the guest operating system has deleted that data. Snapshots are not available when RDM in physical compatibility mode is used. They are, however, available for RDM in virtual compatibility mode.

So, what's the use case for snapshots?

One of the use cases is, for example, an upgrade of VMware virtual hardware version (AKA VM compatibility). Before an upgrade, you take a VM snapshot, then you upgrade the VM hardware version. If everything works as expected, you can delete your snapshot. If something is not working, you can revert back.

Leave enough space on your datastore for snapshots - Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes.

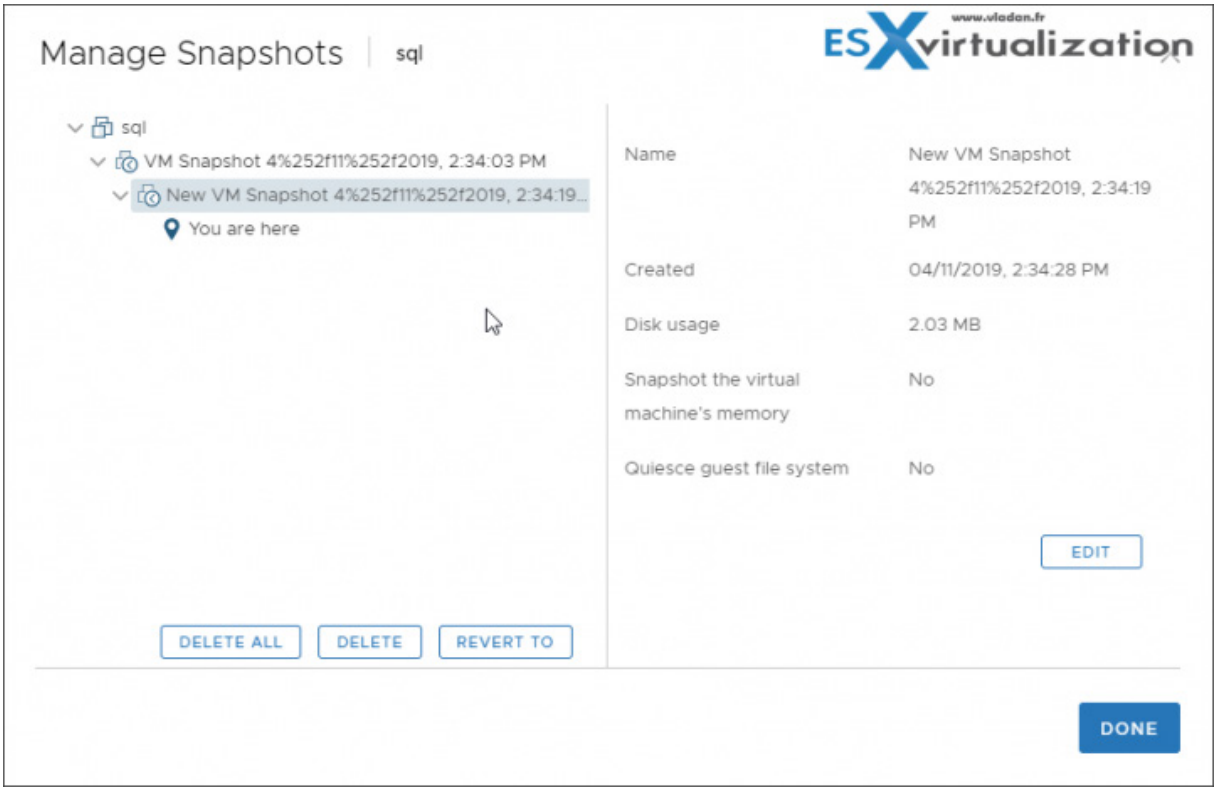
Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking a snapshot of a VM for each member of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short-term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline. With snapshots, you can preserve a baseline before making changes to a virtual machine.

Parent Snapshot – is the first snapshot in the hierarchy, and the most recently saved version of the current state of the VM.

Child Snapshot – is a snapshot of the VM taken after the parent snapshot. Each child snapshot contains delta files of each attached VMDK. Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

Recommended readings: *vSphere Virtual Machine Administration PDF (page 253)*



A Take Snapshot operation creates .vmdk, -delta.vmdk, .vmsd, and .vmsn files. By default, the first and all delta disks are stored with the base .vmdk file. The .vmsd and .vmsn files are stored in the virtual machine directory.

- **Delta disk files** - a VMDK file to which the OS can write. Delta disk is the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken.
- **Flat File** - A -flat.vmdk file that is one of two files that comprise the base disk. The flat disk contains the raw data for the base disk (not visible in the datastore browser).
- **Database file** - A .vmsd file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager.
- **Memory File** - A .vmsn file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state.

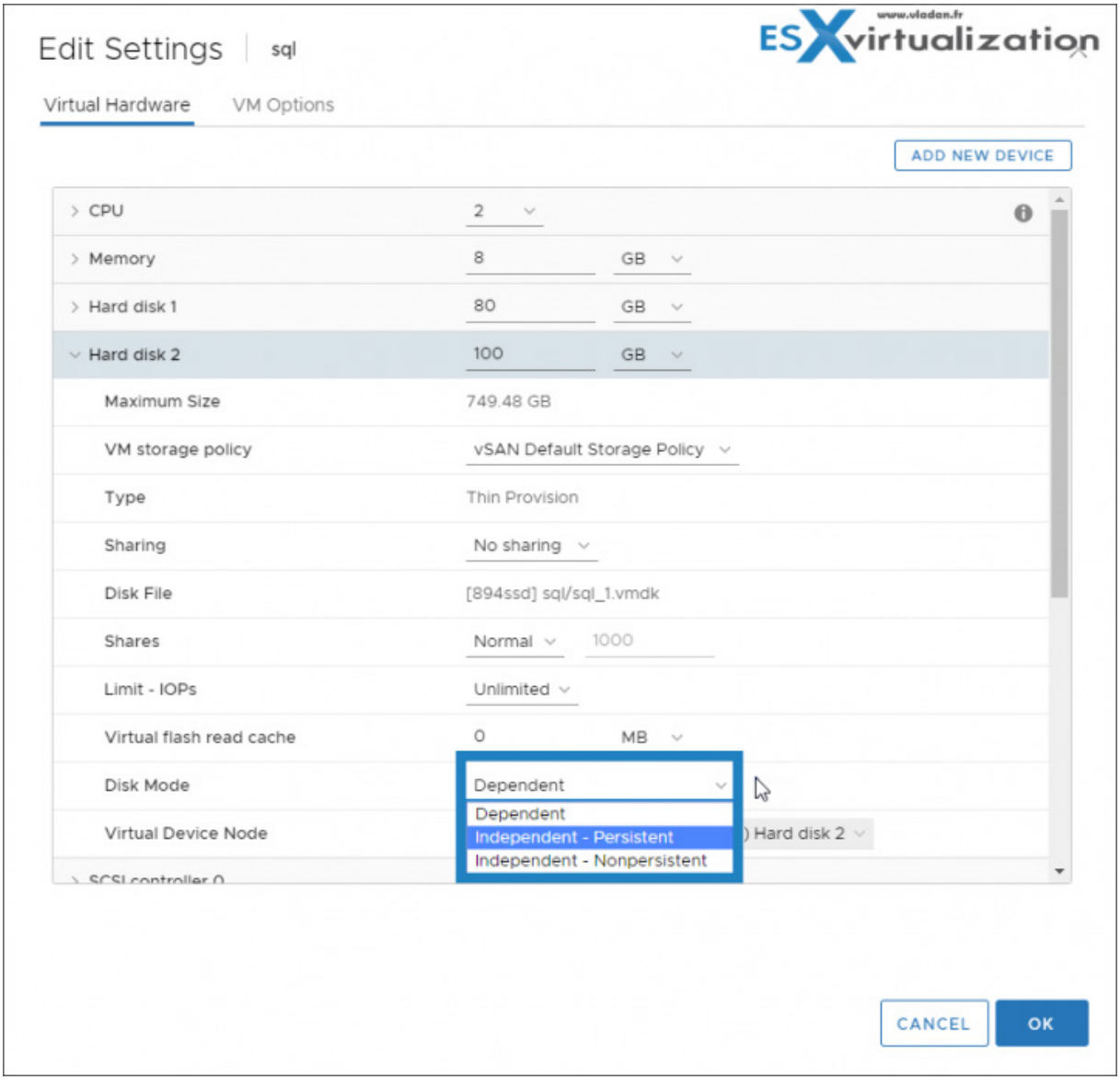
What is preserved with Snapshots?

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

Quiesced snapshots - When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems.

Independent disks allow you to **exclude** VM's disks from snapshots. There are two different types:

1. **Independent - persistent** - Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
2. **Independent Nonpersistent** - Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time.



You can either **delete** a single snapshot within the snapshot tree or you can **Delete All** snapshots.

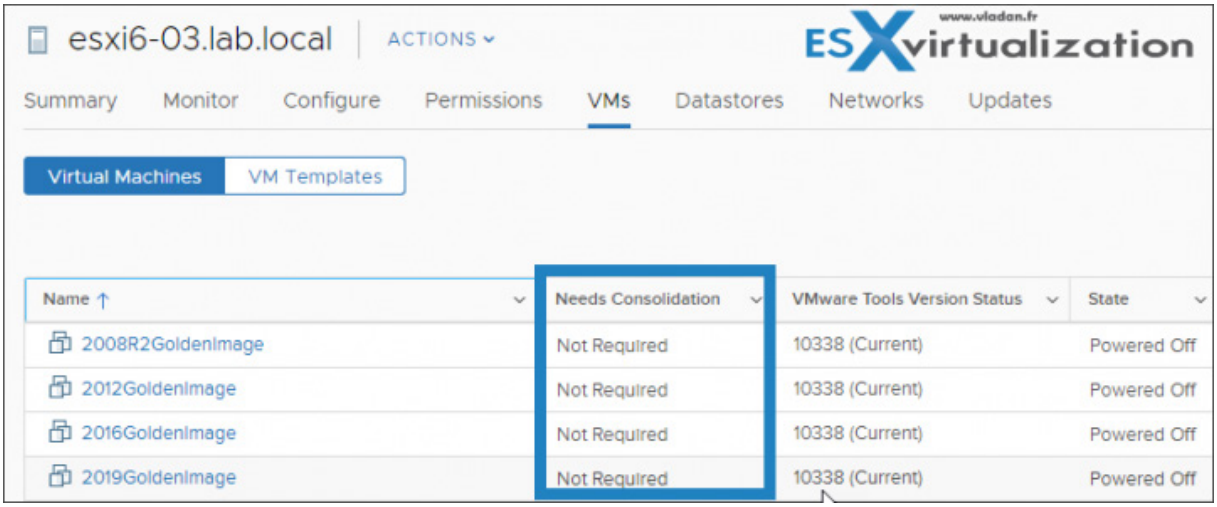
Delete - remove single parent or child snapshot from the snapshot tree. Delete writes disk changes that happen between the stat of the snapshot and the previous disk state to the parent snapshot.

Note: Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other snapshot.

Delete All - consolidates and writes the changes that occur between snapshots and the previous delta disk states to the base parent disk and merges them with the base virtual machine disk.

Snapshot consolidation

The **Needs Consolidation column** in the vSphere Client shows which virtual machines to consolidate.

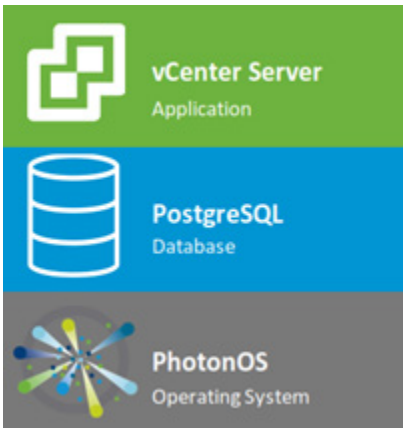


The presence of redundant delta disks can adversely affect virtual machine performance. You can combine such disks without violating data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compress after a Delete or Delete All operation. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

Objective 5.2 - Monitor resources of VCSA in a vSphere environment

VMware vCenter Server Appliance (VCSA) has regular updates which bring new features. Not so long ago it was just a black box which you could only monitor with CLI or via console session. Today, VCSA has its own management and offers the monitoring of several components like CPU, disks, network, or even services through UI.



VCSA is composed of Photon OS, PostgreSQL database and vCenter server application. Feature parity has been a goal for VMware for several vSphere releases which has since been achieved. The Linux-based appliance has HTML5 management of all functions that Flash-based client. The vCenter on Windows is still possible in vSphere 6.7 but it is the last release. Future major releases will be in VCSA only.

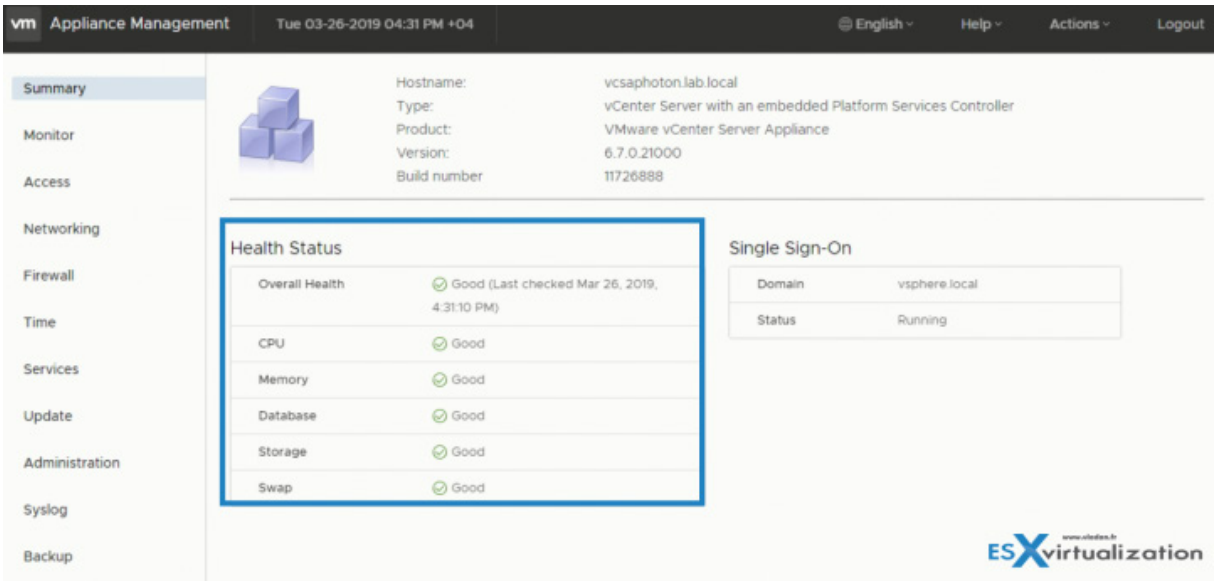
Services can be restarted within the UI as well.

Right after logging in to the management interface of VCSA through port 5480, you get the overview of the health status. You can verify if any of the components (CPU, memory, database, storage swap) are in good condition. If any of the mentioned components are in a poor state, you'll see a yellow icon.

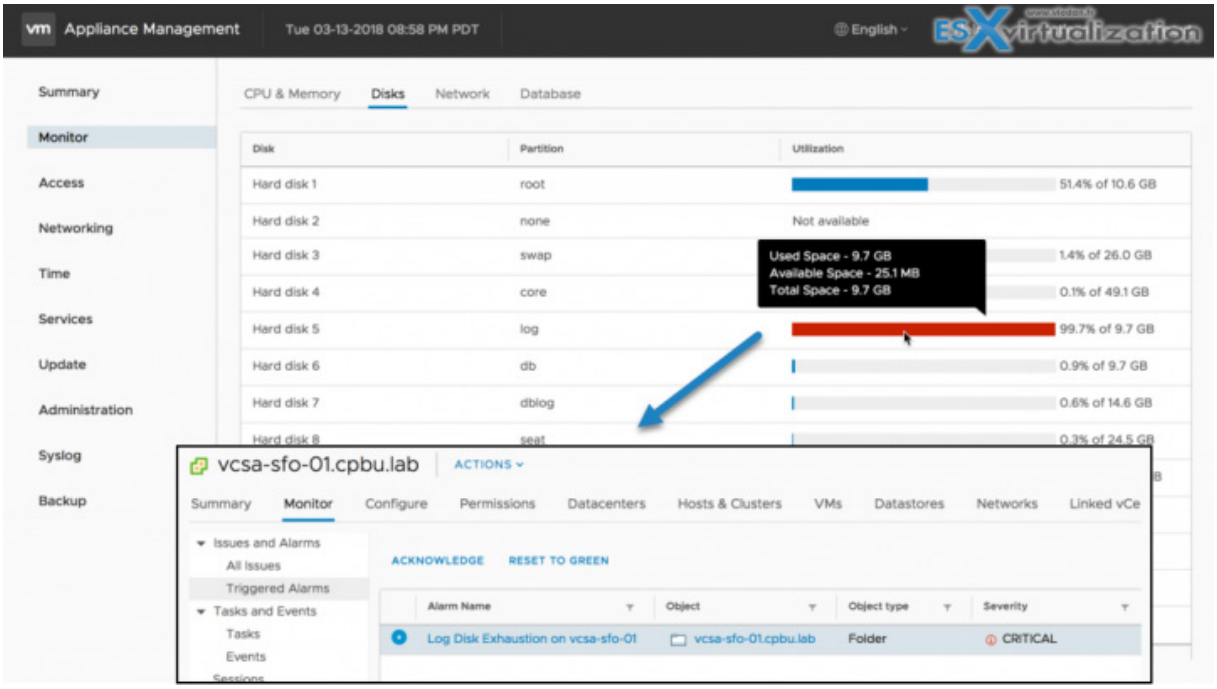
The connection to VCSA management:

https://ip_or_fqdn:5480

Here is the summary tab view.



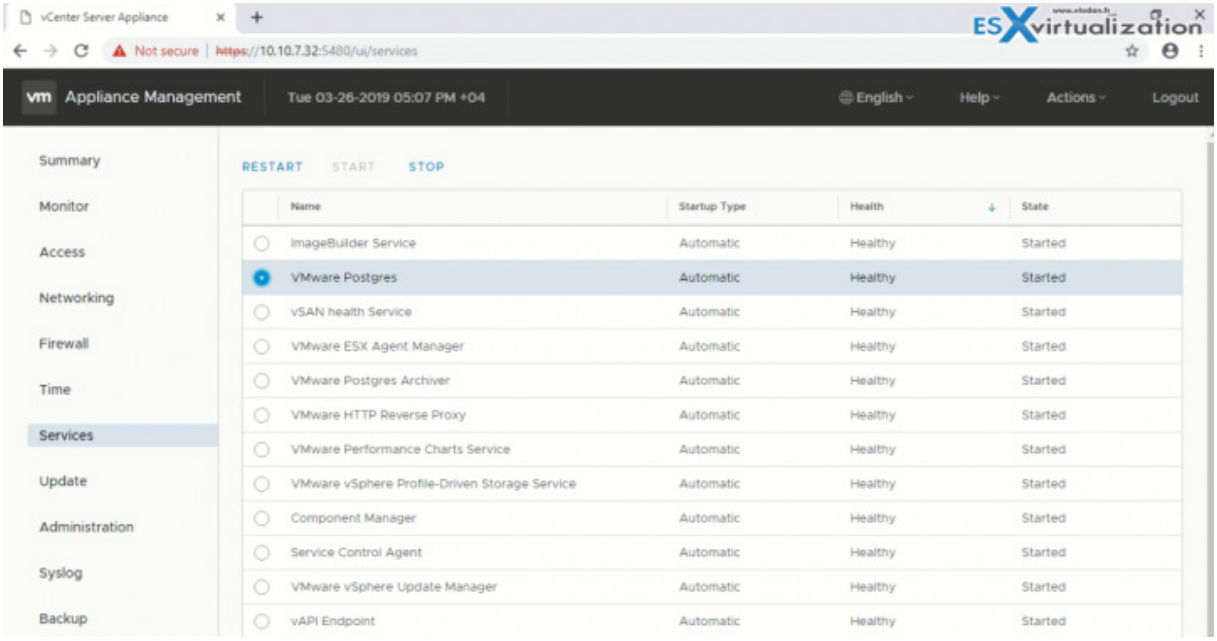
When clicking the **Monitor** menu, you'll get full details of each. This single menu item has all the monitoring you need: CPU and Memory, Disks, Network and Database. With the new improvements in monitoring, there are also improvements in alerting. For example, you'll receive a vCenter alert when one of the disks is getting low on space.



The alerts are triggered for warning and critical when reaching thresholds:

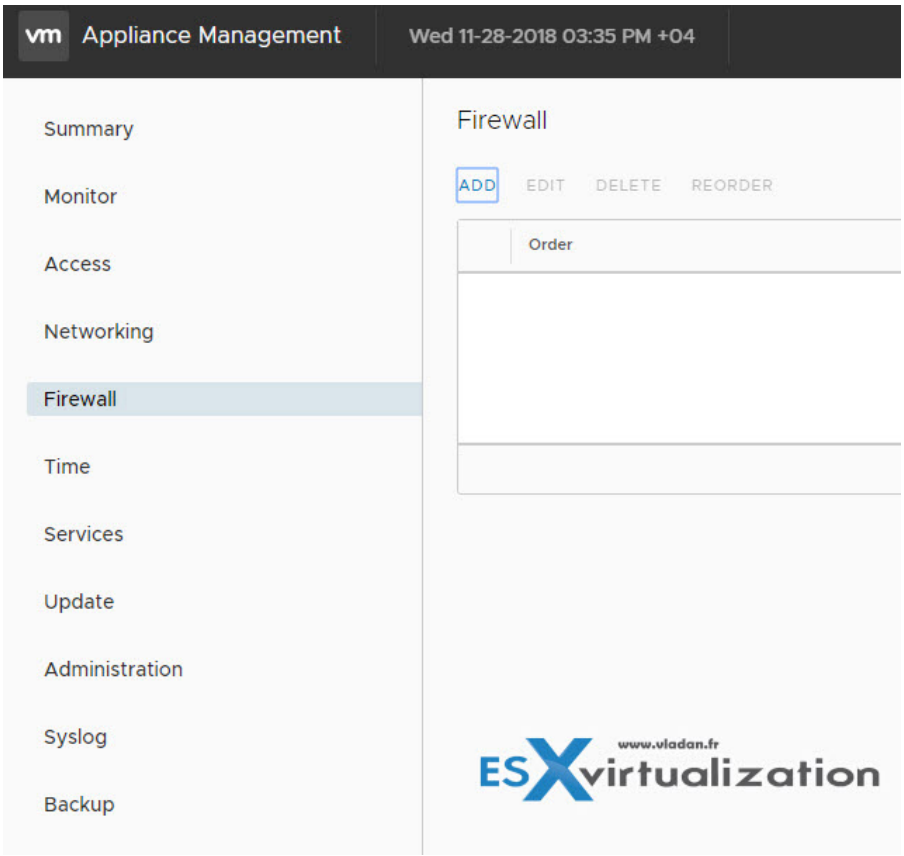
- **Disks** - Warning 75%, Critical 85%
- **Memory** - Warning 85%, Critical 95%
- **CPU** - Warning 75%, Critical 90%

The services Menu provides us with the possibility to manage VCSA services. We can start, stop or restart individual services; you can sort individual columns.



Firewall Management

VMware VCSA allows you to create custom rules. You can access the firewall via the menu on the left, and navigate to **Firewall**. After that, click on the **Add** menu button to add a new rule.

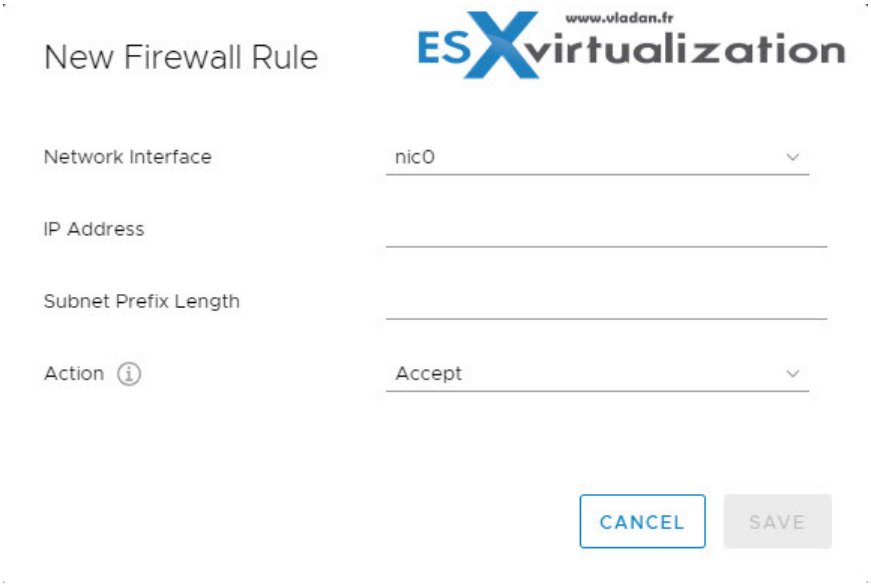


You'll see an overlay pop-up window appear, inviting you to fill certain details.

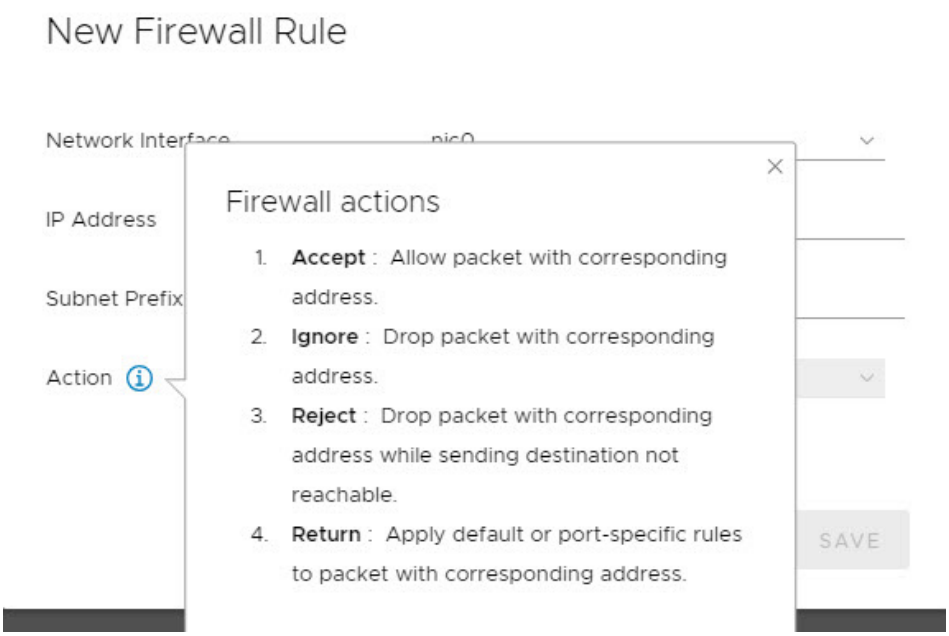
Here are the details.

You have the choice of:

- **Network Interface** – a drop-down menu allowing you to select the vNIC you want to add the rule for.
- **IP address** – address from which you want to allow/block traffic
- **Subnet Prefix Length** – subnet details
- **Action** – accept or refuse traffic

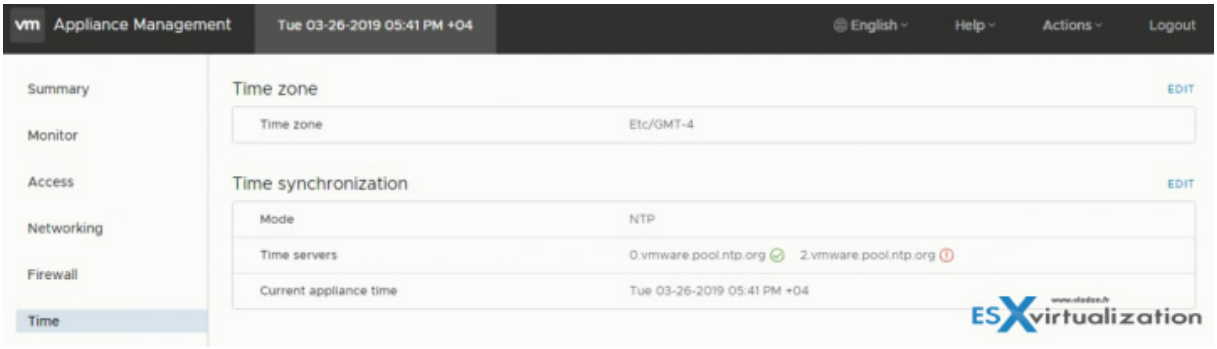


Here is a screenshot of when you hover the mouse over the "**i**" next to the Action.



Time management

You can access the time management through the Time menu and configure the time zone and add NTP servers. All this is accessible through a web browser without any plugin.



I won't go through all the tabs, but you get the idea. You have all the appliance configuration options, including self-backup, accessible through the appliance management interface through the port 5480.

While we try to cover everything that's needed, we do not always know what exactly VMware will require you to know for the exam. Use this chapter as a guideline, however, your principal study material should be the Documentation Set PDF, as well as your home lab or day-to-day work with the infrastructure.

Objective 5.3 - Identify impacts of VM configurations

Configuration of VMs and the different virtual hardware options have a direct impact on performance. In this post, we'll try to have a look at different options available.

Before going further, make sure that you know the composition of VM files. There is a dedicated lesson in our guide - **Objective 1.10** **Describe a virtual machine (VM) file structure.**

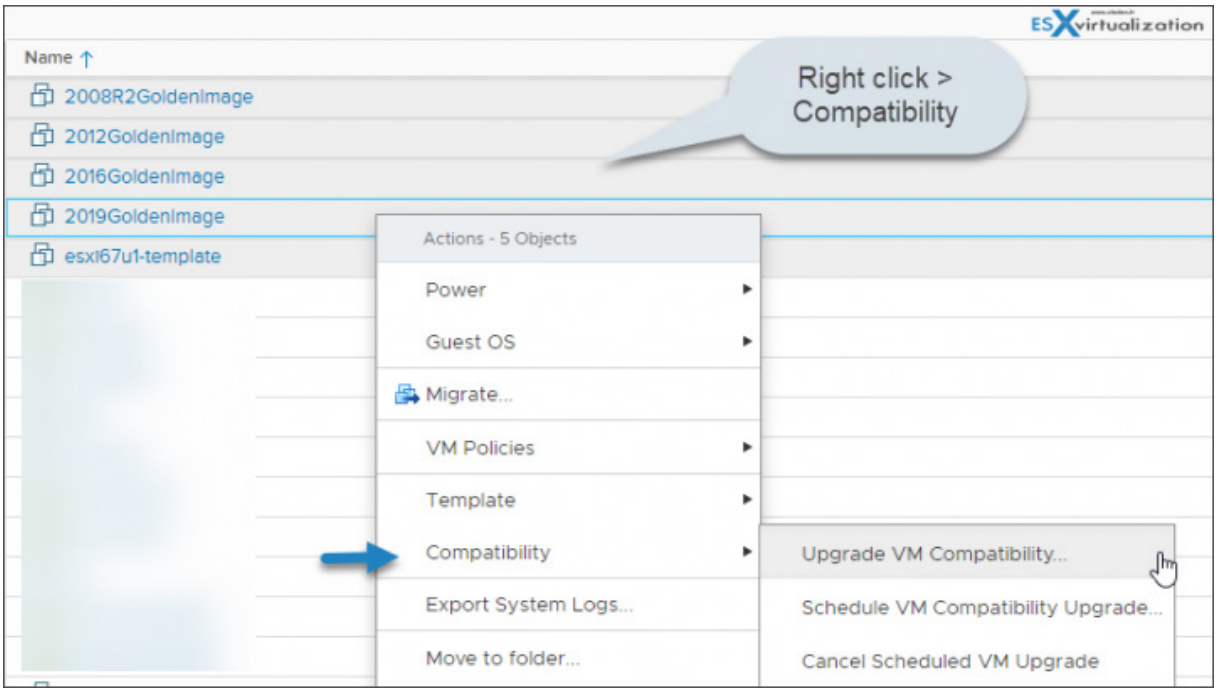
It's a fairly difficult lesson, as identifying impacts of VM configurations isn't easy to document in a single blog post, though let's give it a try, shall we?

VM's full components are usually necessary for each VM to run. Each VM has typically an **OS, VMware Tools, and virtual resources and hardware**. VMware tools are an essential part of every VM. VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. It includes device drivers and other software that is essential for your VM. With VMware Tools, you have more control over the virtual machine interface.

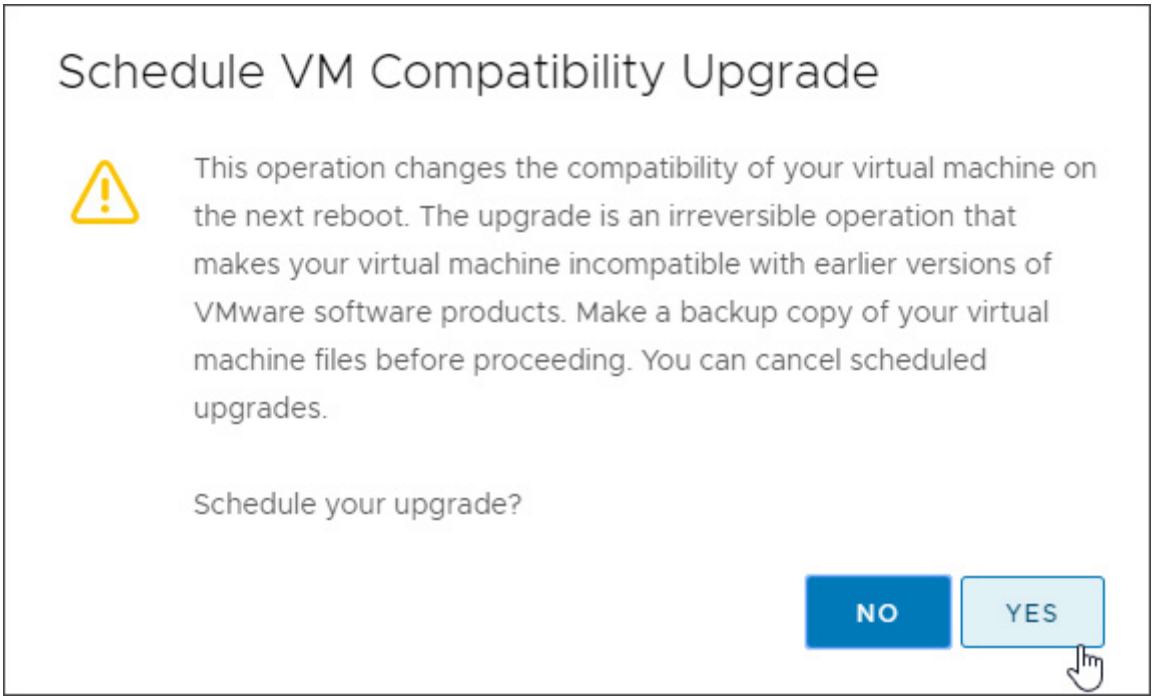
Compatibility Settings - you assign each virtual machine to a compatible ESXi host version, cluster, or datacenter by applying a compatibility setting. The compatibility setting determines which ESXi host versions the virtual machine can run on and the hardware features available to the virtual machine.

You can schedule compatibility upgrade for a single VM or for multiple VMs.

- Create a backup or snapshot of the virtual machines.
- Upgrade to the latest version of VMware Tools. On Microsoft Windows virtual machines, if you upgrade the compatibility level before you upgrade VMware Tools, the virtual machine runs the risk of losing its network settings.

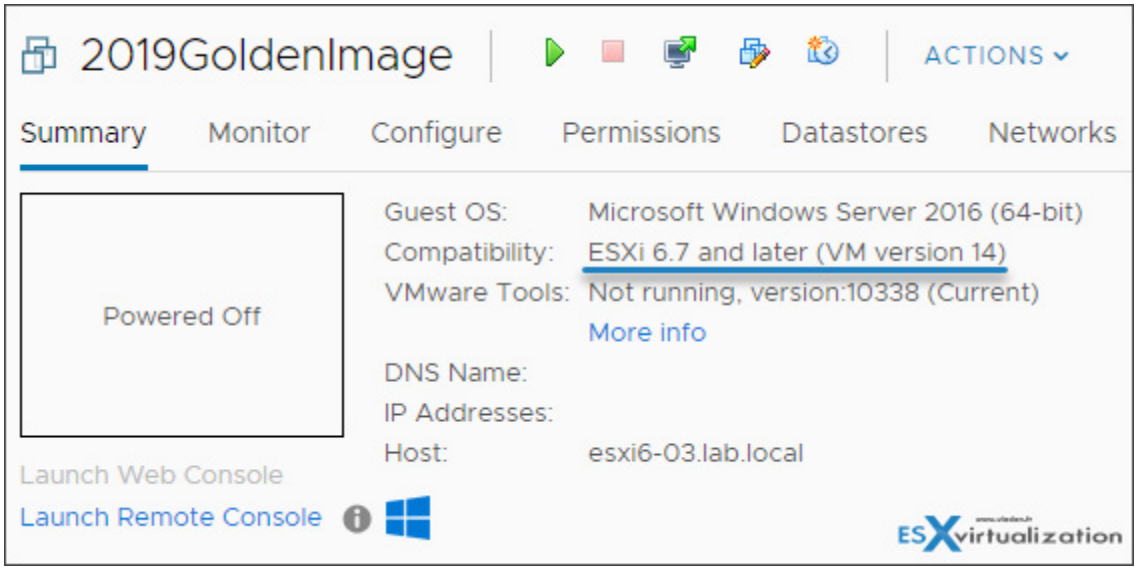


- Right-click a virtual machine and select **Compatibility** > **Schedule VM Compatibility Upgrade**.
- In the Schedule VM Compatibility Upgrade dialog box, confirm that you want to schedule a compatibility upgrade by clicking **Yes**.



From the Compatible with drop-down menu, select the compatibility to upgrade to.

The virtual machine compatibility is upgraded the next time you restart the virtual machine. Once the virtual machine compatibility is upgraded, the new version appears on the virtual machine Summary tab.



Check ***vSphere Virtual Machine*** *Administration PDF*, **page 93** for all details about Supported Features for Virtual Machine Compatibility.

Hardware Device - Each VM has CPU, Memory, and disk. All recent operating systems provide support for virtual memory, allowing the software to use more memory than the machine physically possesses.

Virtual Machine Options

Use the available virtual machine options to fine-tune the settings and behavior of your virtual machine and to ensure maximum performance.

VMware virtual machines have the following options.

General Options	View or modify the virtual machine name, and check the location of the configuration file and the working location of the virtual machine.
Encryption Options	Enable or disable encryption for the virtual machine if the vCenter Server instance is in a trusted relationship with a KMS server. For more information, see the *vSphere Security* documentation. You can also enable or disable encrypted vMotion for virtual machines that are not encrypted. You can set encrypted vMotion to the disabled, opportunistic, or required state. You can enable encrpyted vMotion during virtual machine creation. Alternatively, you can change the encrypted vMotion state at a later time. For more information, see the *vCenter Server and Host Management* documentation.
Power Management	Manage guest power options. Suspend the virtual machine or leave the virtual machine powered on when you put the guest operating system into standby.
VMware Tools	Manage the power controls for the virtual machine and run VMware Tools scripts. You can also upgrade VMware Tools during power cycling and synchronize guest time with the host.
Virtualization Based Security (VBS)	Enable VBS to provide an additional level of protection to the virtual machine. VBS is available on the latest Windows OS versions. For more information, see the *vSphere Security* documentation.
Boot Options	Set the boot delay when powering on virtual machines or to force BIOS setup and configure failed boot recovery.
Advanced Options	Disable acceleration and enable logging, configure debugging and statistics, and change the swap file location. You can also change the latency sensitivity and add configuration parameters.
Fibre Channel NPIV	Control virtual machine access to LUNs on a per-virtual machine basis. N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers.
vApp Options	Enable or disable the vApp functionality in a virtual machine. When you enable vApp options, you can view and edit vApp properties, vApp Deployment options, and vApp Authoring options. For example, you can configure an IP allocation policy or a network protocol profile for the vApp. A vApp option that is specified at the level of a virtual machine overrides the settings specified at the level of the vApp.

Virtual CPU configuration

You can add, change or configure CPU resources to improve VM performance.

Some terminology from VMware:

CPU socket - A CPU socket is a physical connector on a computer motherboard that connects to a single physical CPU. Some motherboards have multiple sockets and can connect multiple multicore processors (CPUs).

Core - A core contains a unit containing an L1 cache and functional units needed to run applications. Cores can independently run applications or threads. One or more cores can exist on a single CPU.

Resource sharing - Shares specify the relative priority or importance of a virtual machine or resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when the two virtual machines are competing for resources.

Resource allocation - You can change CPU resource allocation settings, such as shares, reservation, and limit, when available resource capacity does not meet demands. For example, if at year-end, the workload on accounting increases, you can increase the accounting resource pool reserve.

vSphere Virtual Symmetric Multiprocessing (Virtual SMP) - Virtual SMP or vSphere Virtual Symmetric Multiprocessing is a feature that enables a single virtual machine to have multiple processors.

The latest virtual hardware 15 (vmx-15) introduced in vSphere 6.7 U2, brought the possibility to allocate **up to 256 vCPUs to VMs** (previous versions of virtual hardware were capable of allocating up to 128 vCPUs).

Check VMware KB article 1003746.

Quote:

ESXi 6.7u2 introduces hardware version 15. This new hardware version allows for the creation of a VM with up to 256 vCPUs. It is important to note that a hardware version 15 VM cannot be vMotioned to a host on a prior version of ESXi, including ESXi 6.7u1, ESXi 6.7, ESXi 6.0 etc, as these prior ESXi versions are not compatible with the new hardware version.

Similarly, vCenter 6.7 or vCenter 6.7u1 can be used to manage ESXi 6.7u2 hosts as long as hardware version 15 VMs are not in use. For customers looking to create, run, and manage hardware version 15 VMs, both the ESXi hosts in the cluster and vCenter need to be upgraded to at least 6.7u2.

Multicore vCPUs - VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU's cores, which increases overall performance.

Note: Make sure to comply with the EULA of the guest OS.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs means the number of physical processor cores or twice that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

For more information about multicore CPUs, see the *vSphere Resource Management* PDF.

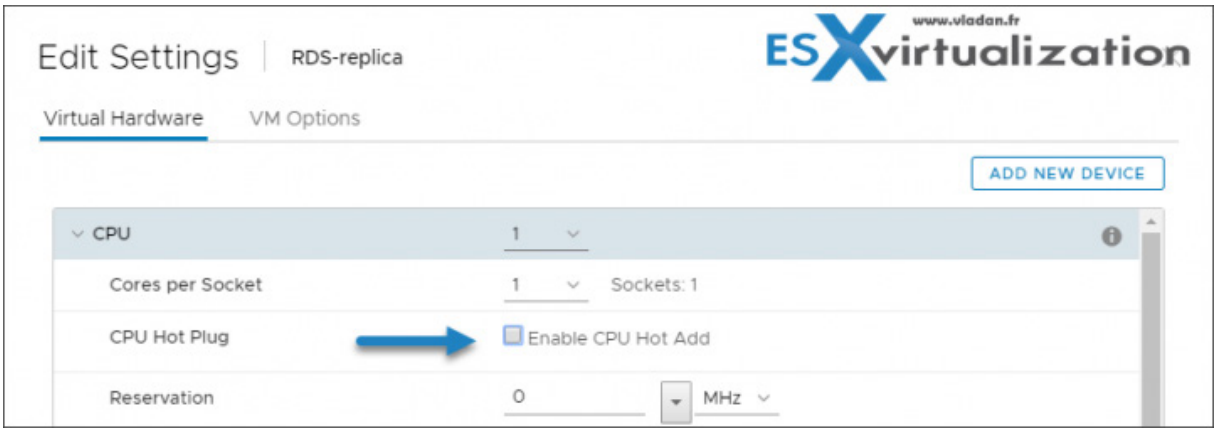
You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hotplug is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

CPU Hot Add - The CPU hot add option lets you add CPU resources to a running virtual machine. There are some requisites to enable the CPU hot-add option, and you need to verify that the VM is running and is configured as follows:

- The virtual machine is turned off.
- Virtual machine compatibility is ESX/ESXi 4.x or later.
- The latest version of VMware Tools is installed.
- A guest operating system that supports CPU hotplug (with all recent OS, for Windows from Windows Server 2012 or W7).

To enable the CPU hot-add option:

Right-click a virtual machine in the inventory and select **Edit Settings > Virtual Hardware tab**, **expand CPU**, and select **Enable CPU Hot Add**.

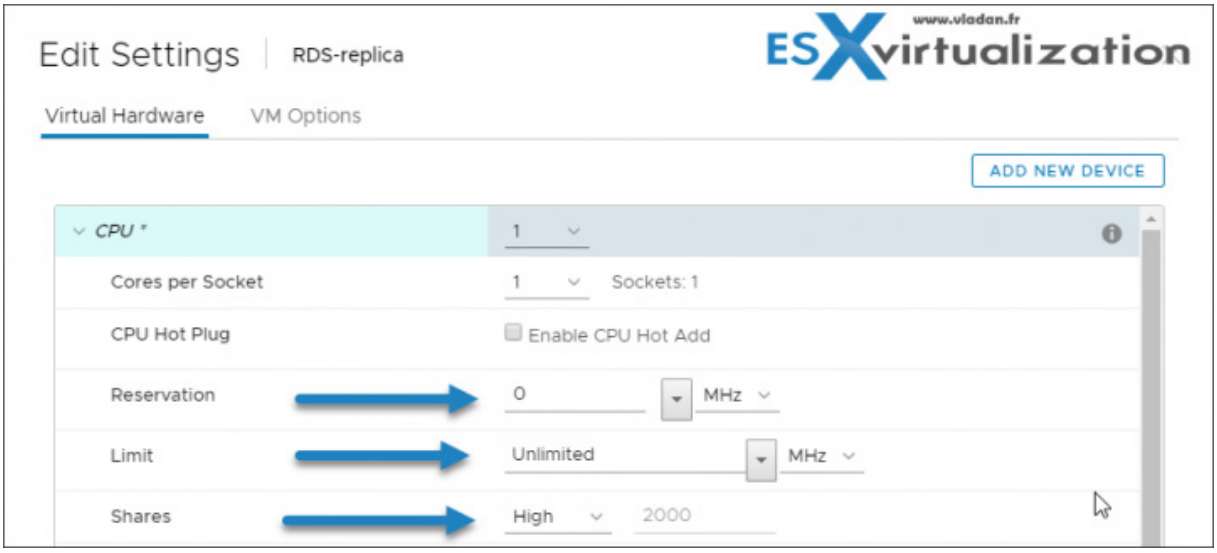


Allocate CPU Resources

While you can allocate CPU resources directly on a per-VM basis, it's recommended to use resource pools. You can change the amount of CPU resources allocated to a virtual machine by using the shares, reservations, and limits settings.

- **Limit** - Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz or GHz.

- **Reservation** - Specifies the guaranteed minimum allocation for a VM. The reservation is in MHz or GHz.
- **Shares** - Each VM is granted a number of CPU shares. The more shares a VM has, the more often it gets a time slice of a CPU when there is no CPU idle time. Shares are the relative metric for allocating CPU capacity.



Enable Virtual CPU Performance Counters - You can identify and improve processor performance problems. This capability is useful for software developers who optimize or debug software that runs in the virtual machine.

Right-click a virtual machine in the inventory and select **Edit Settings** > On the **Virtual Hardware** tab, expand CPU and select the Enable virtualized CPU performance counters checkbox. Click **OK**.

Virtual Memory Configuration - You can change the default RAM settings for a VM to enhance performance. Virtual machines that use EFI firmware require at least 96MB of RAM or they cannot power on. The maximum memory size for a virtual machine depends on the host's physical memory and the virtual machine's compatibility setting.

Table 5-3. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 6.7	ESXi 6.7 and later	6128GB
ESXi 6.5	ESXi 6.5 and later	6128GB
ESXi 6.0	ESXi 6.0 and later	4080GB
ESXi 5.5	ESXi 5.5 and later	1011GB
ESXi 5.1	ESXi 5.1 and later	1011GB
ESXi 5.0	ESXi 5.0 and later	1011GB
ESX/ESXi 4.x	ESX/ESXi 4.0 and later	255GB
ESX/ESXi 3.x	ESX/ESXi 3.5 and later	65532MB

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance.

The maximum for best performance represents the threshold above which the host's physical memory is insufficient to run the virtual machine at full speed.

Check also:

Tip: VMware Hot Add RAM and How to use

Persistent Memory

Persistent memory is an amazing technology that multiplies the storage performances of servers. It was developed as a RAM module that retains its content (across reboots, too) and vSphere supports **Two different modes of access** to those modules, as a vPMEM disk (exposed to a VM as datastore) or as vPMEM (direct and uninterrupted access to the NVDIMM hardware).

When you add a physical PMem device to a host, ESXi detects the PMem resource and exposes it as a host-local PMem datastore to the virtual machines that run on the host. Each host can have only one local PMem datastore that pools and represents all PMem resources of the host.

So, virtual machines can consume the PMem resources of the ESXi host **as memory** (through virtual NVDIMM devices) **or as storage** (through virtual PMem hard disks).

In summary, persistent memory features:

- DRAM-like latency and bandwidth
- Regular load/store CPU instructions
- Paged/mapped by operating system just like DRAM
- Data is persistent across reboots

NVDIMs

Read more on page 109 of ***vSphere Virtual Machine*** *Administration PDF.*

This post could go on and on, and still not answer all of your questions! Instead, you should check out the PDF mentioned above as there are some essential information about:

- Large Capacity Virtual Disk Conditions and Limitations
- Virtual Disk Provisioning Policies
- Virtual disk configuration
- Large Capacity Virtual Disk Conditions and Limitations
- Changing the Virtual Disk Configuration
- Using Disk Shares to Prioritize Virtual Machines

- Configuring Flash Read Cache for a Virtual Machine (please note that vFlash read cache is currently becoming phased out).
- Determining the Virtual Disk Format and Converting a Virtual Disk from the Thin Provision Format to a Thick Provision Format
- Adding a Hard Disk to a Virtual Machine
- Adding an Existing Hard Disk to a Virtual Machine
- Adding an RDM Disk to a Virtual Machine
- SCSI and SATA Storage Controller Limitations, and Compatibility

This is a major chapter which needs to be studied from the PDF (or at least read through briefly to get some basics). We simply can't write everything here.

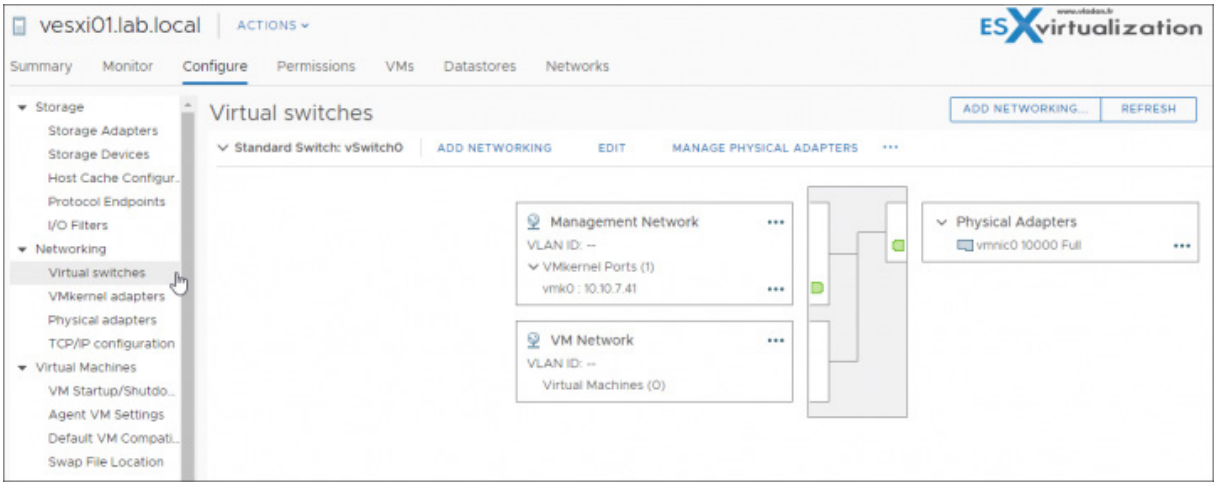
We haven't even touched on network configuration or network adapter types, as it is just too involved for this post. In this lesson, which was about identifying impacts of VM configurations, we tried to list a maximum of options for VM configuration, but it's definitely not an all-encompassing blog post (chapter) option. Alas, that is all we can offer you at this time. There are always risks of failure when you go for the exam.

Objective 6 - There are no testable objectives for this section

Objective 7.1 - Manage virtual networking

VMware vSphere has by default all of its hosts configured with vSphere standard switch (VSS). vSphere Distributed Switch (VDS) can be created and configured through vCenter server only for customers which have the appropriate licensing or are running VMware VSAN.

To manage virtual networking, you'll first need to configure and use vSphere Standard Switch (VSS). This is because VDS config can be done through vCenter server only. vSphere Standard switch configuration is accessible via the vSphere Web client. **Select host > configure > networking**



Network Policies:

Policies which are applied at the switch level propagate to all standard port groups.

The virtual standard switches (VSS) can have the following policies and settings:

- Traffic shaping (outbound only)
- VLANs (none, VLAN ID, All) – at the portgroup level config
- MTU
- Teaming and failover
- Security

If you set VLAN policy to 4095 (All), it allows you to pass All VLANs, and the tagging is done at the Guest OS level.

vSphere features the following distributed switches (vDS) policies and settings:

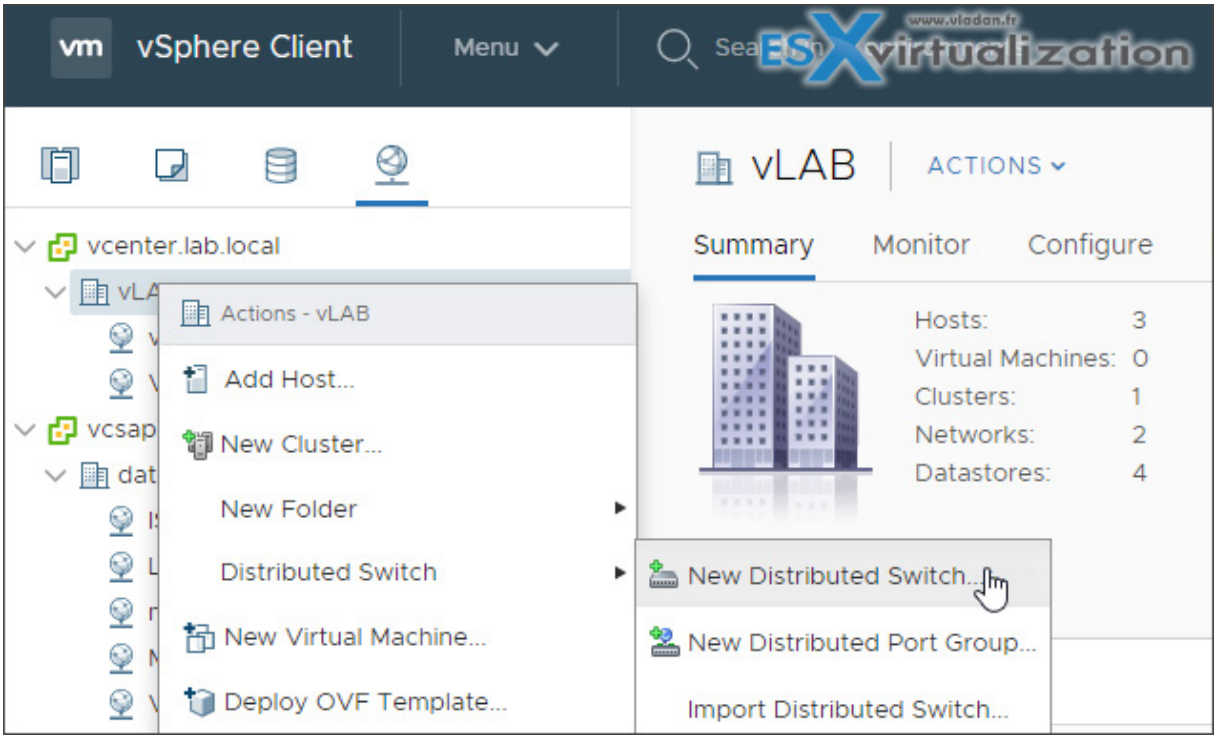
- Traffic filtering and marking
- MTU
- VLANs (none, VLAN ID, VLAN trunking, PVLANs)
- Monitoring (NetFlow)
- Security
- Traffic Shaping – inbound and outbound (ingress/egress)
- LACP
- Port mirroring
- Health check for VLAN and MTU, teaming and failover – allows for checking the status of the overall config.
- Teaming and failover as is the case on VSS switch.

Check it out: I highly recommend reading our post from previous study guide - VCP6.5-DCV Objective 2.1 – Configure policies/features and verify vSphere networking

Note: Policies for vSwitches differ. Not all policies for vSphere Distributed Switch (vDS) are available for vSphere Standard Switch (vSS).

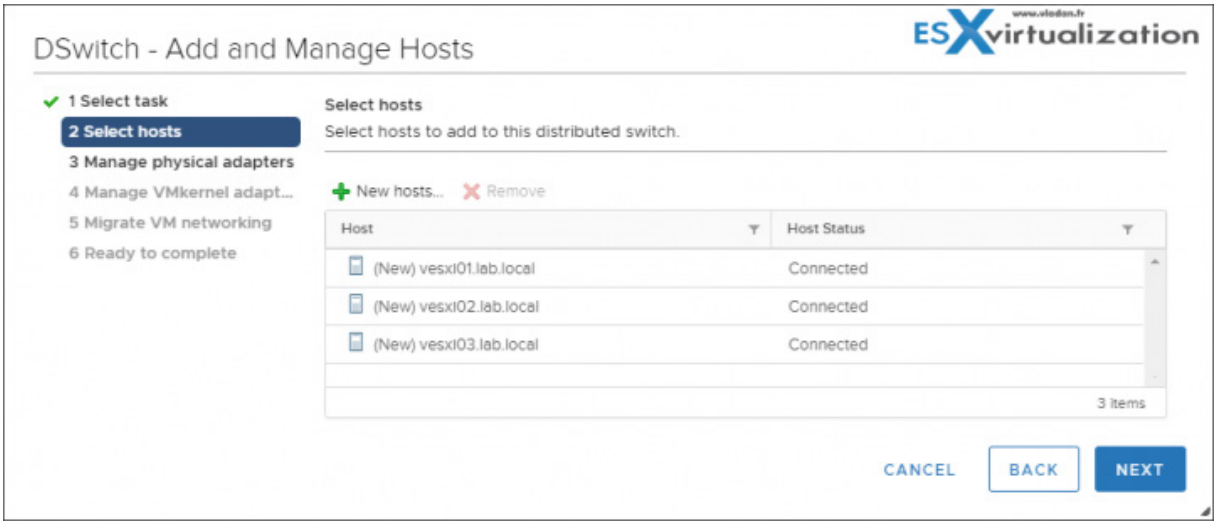
vSphere Distributed Switch

You need to go to **Networking TAB > Right click Datacenter > Distributed Switch > New Distributed Switch**



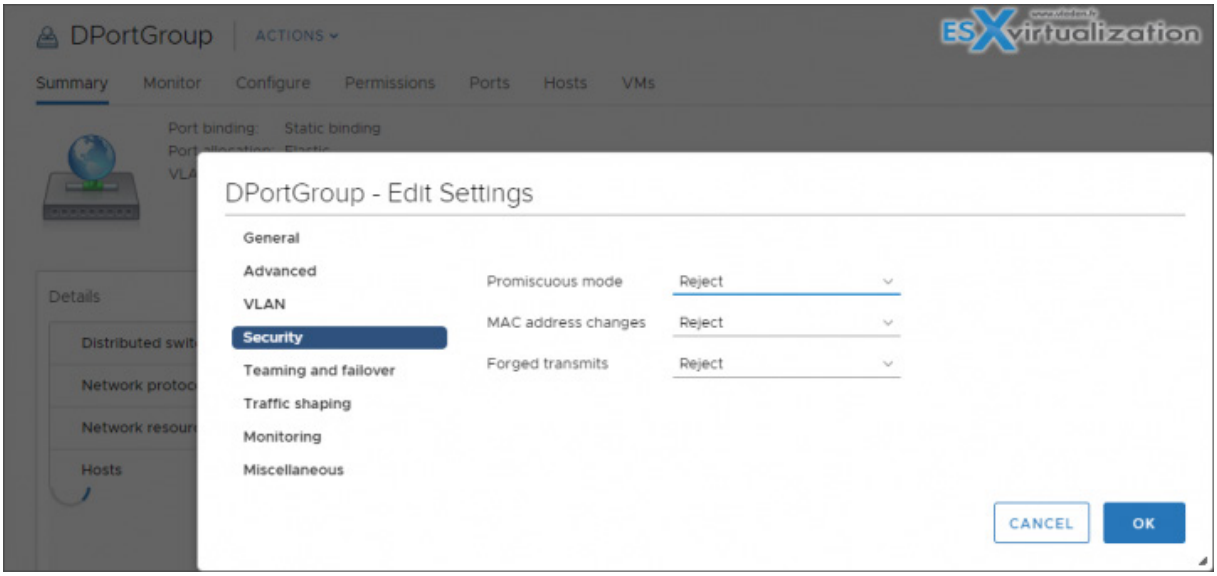
After you create VDS, you need to add hosts. But before doing that, you should:

- Create distributed port groups for VM networking
- Create distributed port groups for VMkernel services, such as vMotion, VSAN, FT etc.
- Configure a number of uplinks on the distributed switch for all physical NICs that you want to connect to the switch



VDS has 3 different network security policies:

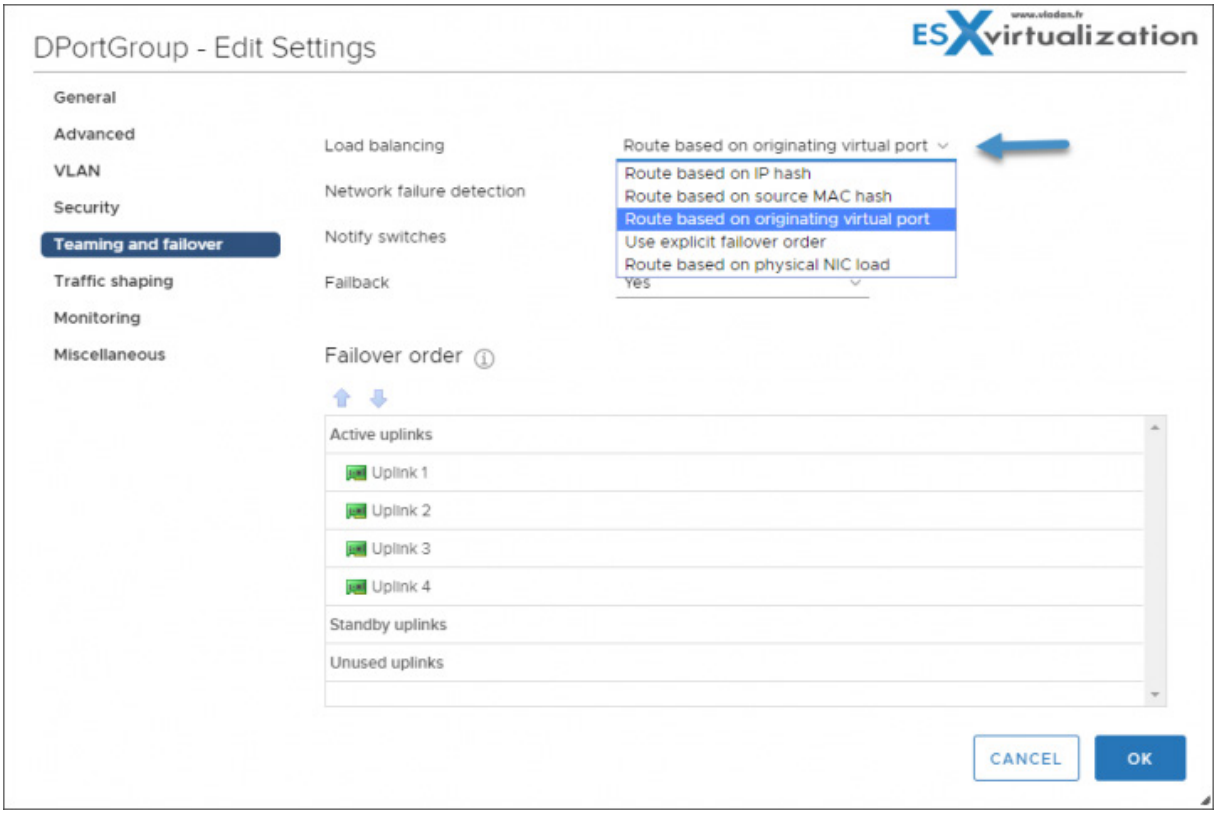
- **Promiscuous mode** – Reject is by default. Should you set it to **Accept** >, the guest OS will receive all traffic observed on the connected vSwitch or PortGroup.
- **MAC address changes** – Reject is by default. Should you set it to **Accept** >, then the host will accept requests to change the effective MAC address to a different address from the initial MAC address.
- **Forged transmits** – Reject is by default. Should you set it to **Accept** >, then the host will not compare sources and effective MAC addresses transmitted from a virtual machine.



vDS load balancing (LNB):

- **Route based on IP hash** – The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.
- **Route based on source MAC hash** – The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.
- **Route based on originating virtual port** – Each virtual machine running on an ESXi host has an associated virtual port ID on the virtual switch. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine port ID and the number of uplinks in the NIC team. After the virtual switch selects an uplink for a virtual machine, it always forwards traffic through the same uplink for this virtual machine as long as the machine runs on the same port. The virtual switch calculates uplinks for virtual machines only once, unless uplinks are added or removed from the NIC team.
- **Use explicit failover order** – No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.

- **Route based on physical NIC load (Only available on vDS)** – based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. This is available only for vSphere Distributed Switch. The distributed switch calculates uplinks for virtual machines by taking their port ID and the number of uplinks in the NIC team. The distributed switch tests the uplinks every 30 seconds, and if their load exceeds 75 percent of usage, the port ID of the virtual machine with the highest I/O is moved to a different uplink.



I highly recommend getting a *vSphere 6.7 Networking PDF* and studying from it as our blog post here isn't really complete. You should also practice in the lab, heavily, as networking is one of the core vSphere components. While networking and VSS might not be as difficult to configure and use, VDS, on the other hand, has far more option and configuration parameters.

Objective 7.2 - Manage datastores

A very large chapter today is based on the theme of managing datastores. The vSphere web client is our principal tool. There is a *vSphere Storage 6.7 Update 2 PDF* as documentation present at the VCP-DCV 2019 Study Guide Wordpress page. Use it for the study of this chapter.

Datastores are logical containers, analogous to file systems, that hide specifics of physical storage and provide a uniform model for storing virtual machine files.

There are different types of datastores in vSphere and we'll have a look at their differences and possibilities.

Types of Datastore:

- **VMFS** - version 5 and 6 are supported. VMFS is a special high-performance file system format that is optimized for storing virtual machines.
- **NFS** - An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume. The volume is located on a NAS server. The ESXi host mounts the volume as an NFS datastore, and uses it for storage needs. ESXi supports versions 3 and 4.1 of the NFS protocol.
- **VSAN** - VSAN aggregates all local capacity devices available on the hosts into a single datastore shared by all hosts in the VSAN cluster. See the Administering VMware VSAN documentation.
- **Virtual Volumes** - Virtual Volumes datastore represents a storage container in vCenter Server and vSphere Client.

There are some differences between VMFS 5 and VMFS 6. Here is a screenshot from VMware documentation PDF which summarizes this:

Table 17-3. Comparing VMFS5 and VMFS6

www.vladan.fr ESXvirtualization

Features and Functionalities	VMFS5	VMFS6
Access for ESXi hosts version 6.5 and later	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	Yes	No
Datastores per host	512	512
512n storage devices	Yes	Yes (default)
512e storage devices	Yes. Not supported on local 512e devices.	Yes (default)
4Kn storage devices	No	Yes
Automatic space reclamation	No	Yes
Manual space reclamation through the esxcli command. See Manually Reclaim Accumulated Storage Space.	Yes	Yes
Space reclamation from guest OS	Limited	Yes
GPT storage device partitioning	Yes	Yes
MBR storage device partitioning	Yes For a VMFS5 datastore that has been previously upgraded from VMFS3.	No
Storage devices greater than 2 TB for each VMFS extent	Yes	Yes

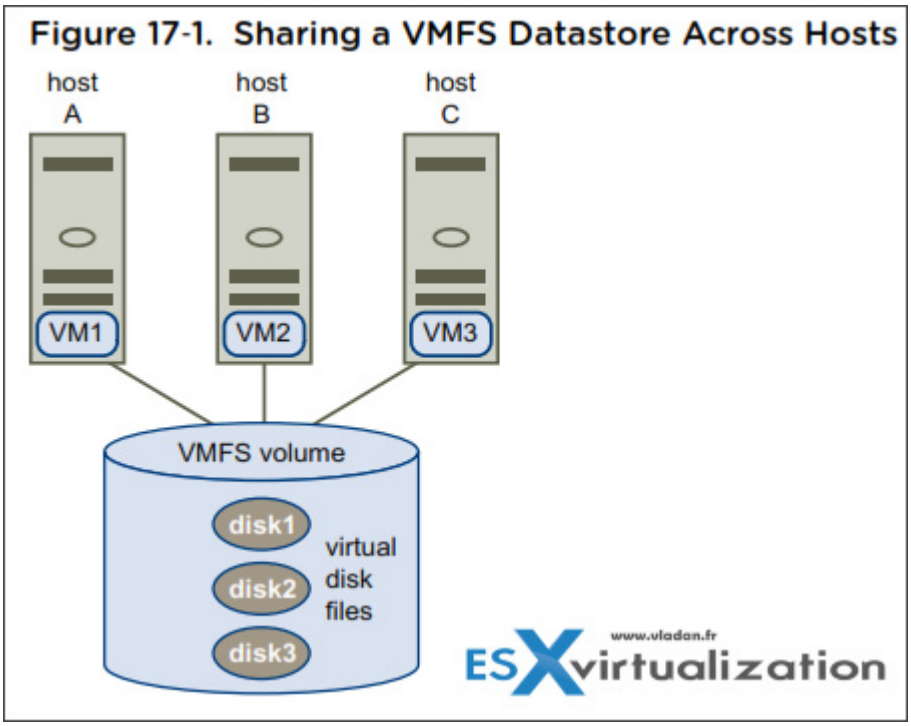
And for your convenience, we've also included a second part:

Table 17-3. Comparing VMFS5 and VMFS6 (Continued)

Features and Functionalities	VMFS5	VMFS6
Support for virtual machines with large capacity virtual disks, or disks greater than 2 TB	Yes	Yes
Support of small files of 1 KB	Yes	Yes
Default use of ATS-only locking mechanisms on storage devices that support ATS. See VMFS Locking Mechanisms.	Yes	Yes
Block size	Standard 1 MB	Standard 1 MB
Default snapshots	VMFSsparse for virtual disks smaller than 2 TB. SEsparse for virtual disks larger than 2 TB.	SEsparse
Virtual disk emulation type	512n	512n
vMotion	Yes	Yes
Storage vMotion across different datastore types	Yes	Yes
High Availability and Fault Tolerance	Yes	Yes
DRS and Storage DRS	Yes	Yes
RDM	Yes	Yes

VMFS Locking Mechanisms - In a shared storage environment when multiple hosts access the same VMFS datastore, specific locking mechanisms are used. These locking mechanisms prevent multiple hosts from concurrently writing to the metadata and ensure that no data corruption occurs.

Depending on its configuration and the type of underlying storage, a VMFS datastore can use different types of locking mechanisms. It can exclusively use the atomic test and set locking mechanism (ATSonly), or use a combination of ATS and SCSI reservations (ATS+SCSI).



VMFS Sparse - VMFS5 uses the VMFSsparse format for virtual disks smaller than 2 TB. VMFSsparse is implemented on top of VMFS. The VMFSsparse layer processes I/Os issued to a snapshot VM.

SEsparse - SEsparse is a default format for all delta disks on the VMFS6 datastores. On VMFS5, SEsparse is used for virtual disks of a size 2 TB and larger.

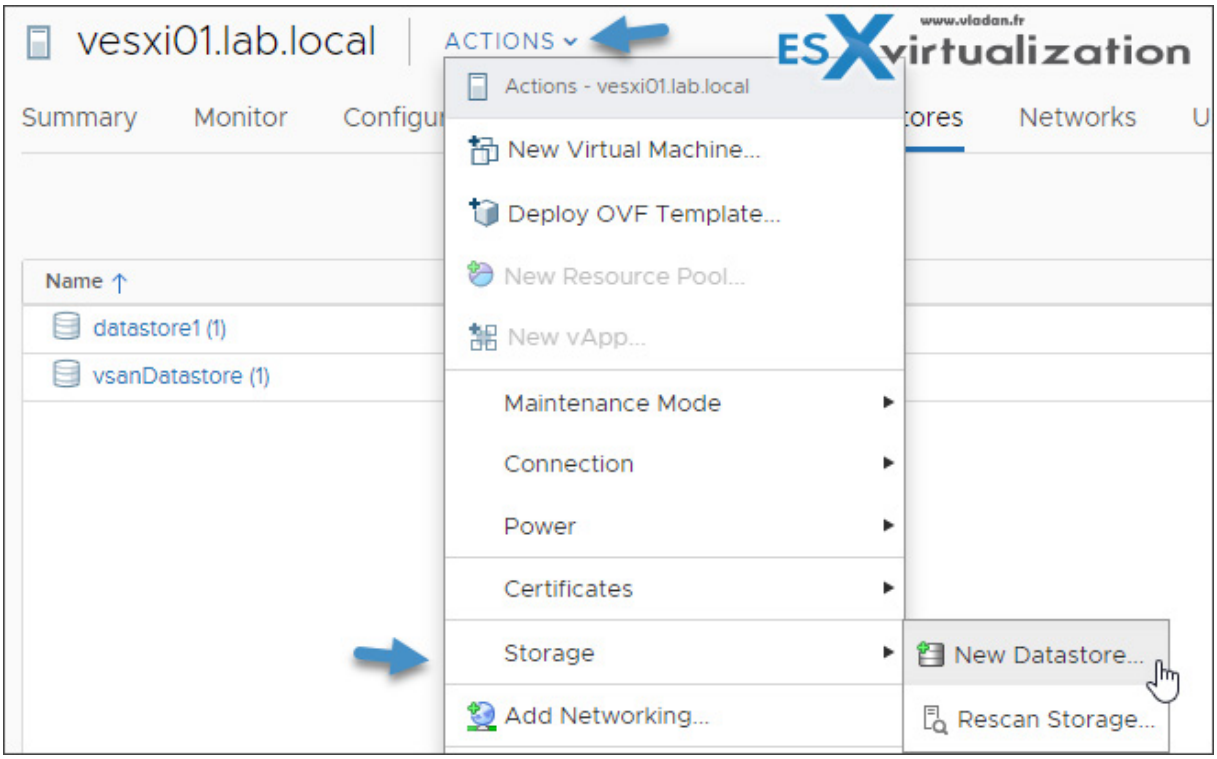
Snapshot Migration

You can migrate VMs with snapshots from one datastore to another. There are some limitations and considerations:

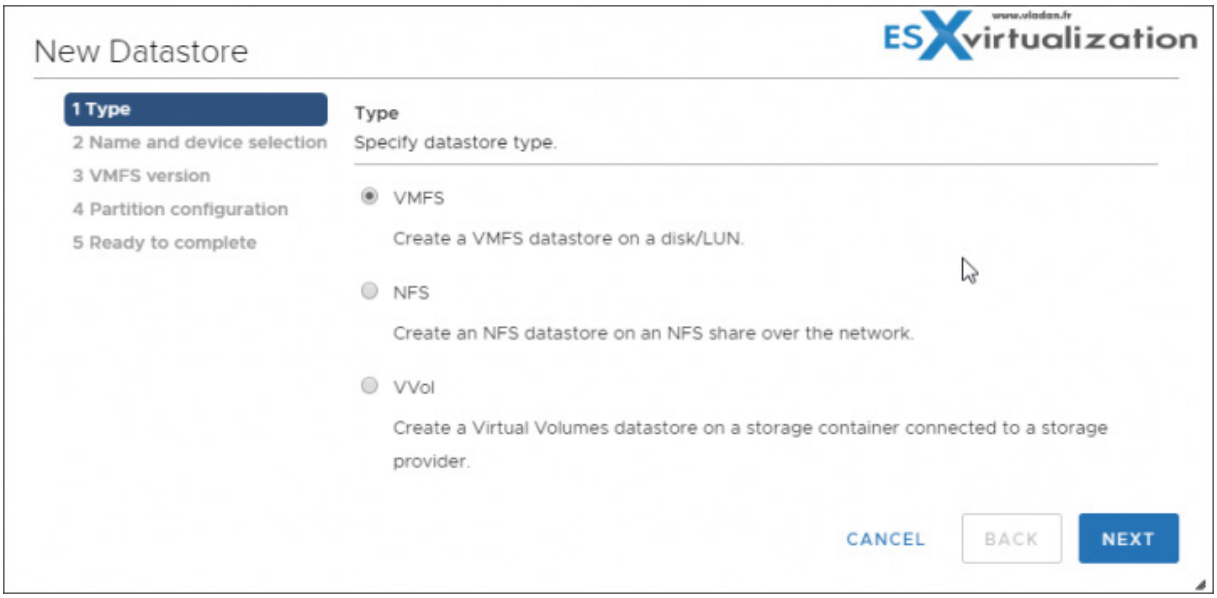
- If you migrate a VM with the VMFSsparse snapshot to VMFS6, the snapshot format changes to SEsparse.
- When a VM with a vmdk of a size smaller than 2 TB is migrated to VMFS5, the snapshot format changes to VMFSsparse.
- You cannot mix VMFSsparse redo-logs with SEsparse redo-logs in the same hierarchy.

What Operations can you do on datastores?

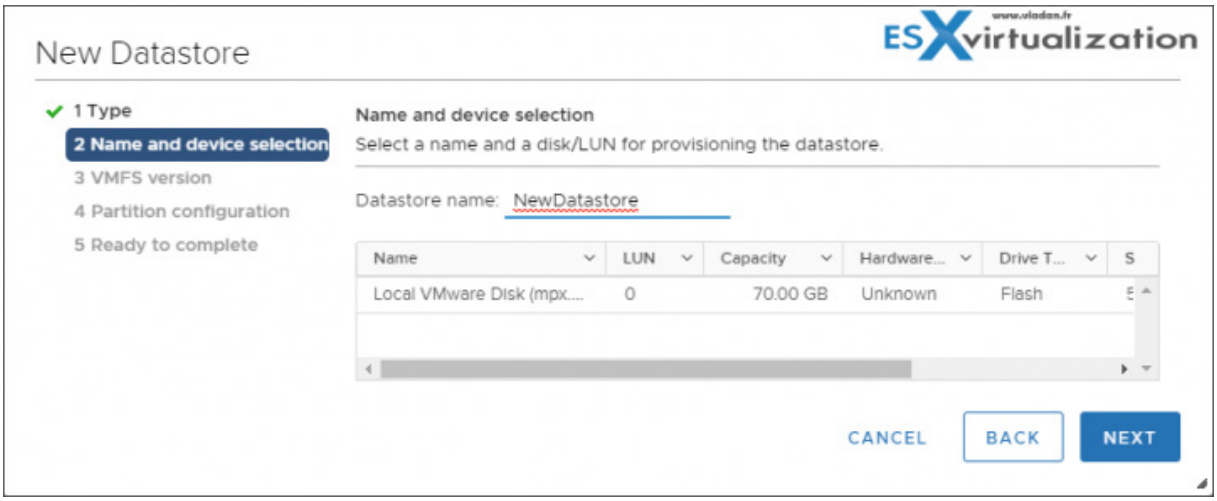
Create Datastores - The usual datastore creation workflow looks like this.



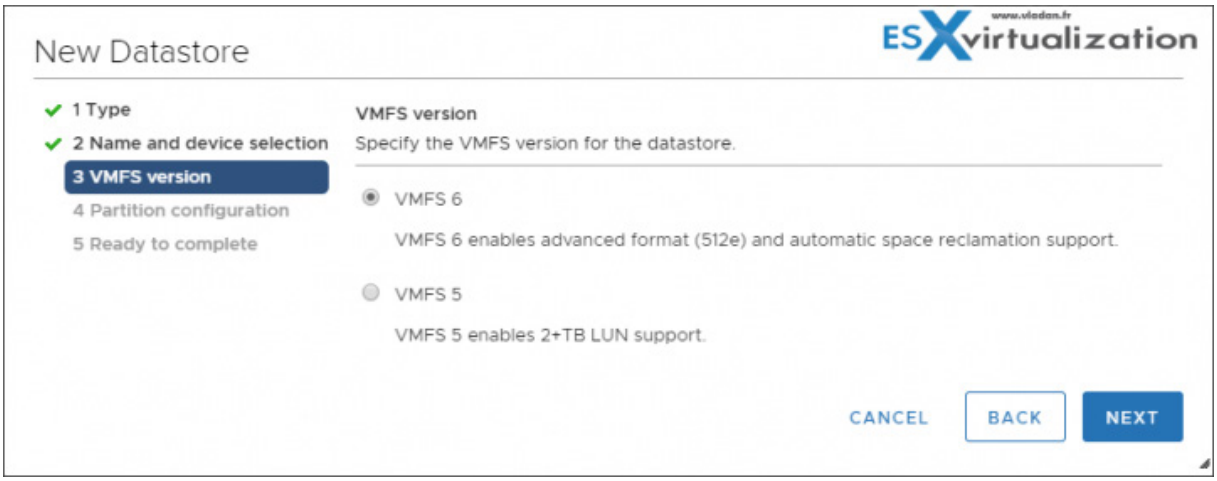
Then a new wizard will start. Chose the type of datastore you wish to create.



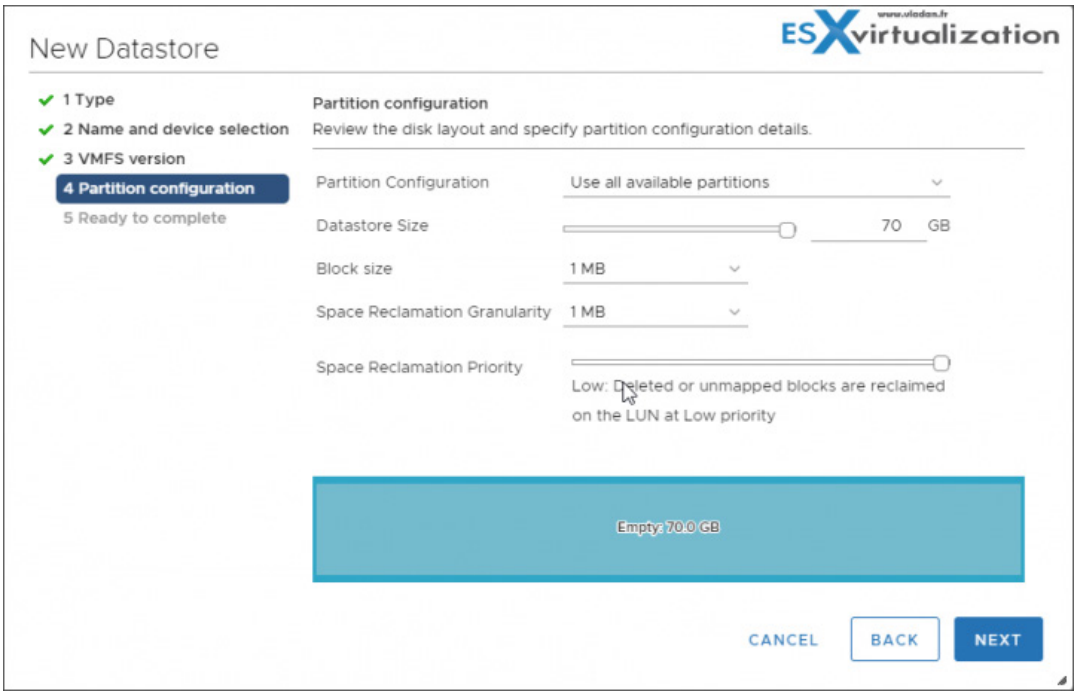
and then select the device.



And then chose VMFS 6 (or VMFS 5 if older ESXi hosts will be accessing this datastore).



and then chose the option most useful for your environment.



Administrative operations - operations such as renaming as well as other operations (Mount, unmount, remove, use datastore browser, rename datastore files) depending on the type of datastore.

Organize datastores - you can organize datastores into folders depending on usage.

Add datastore do datastore cluster - you can put datastores into a datastore cluster.

Check Metadata consistency with VOMA - It is possible to use vSphere On-disk Metadata Analyzer (VOMA) to identify and fix incidents of metadata corruption that affect file systems or underlying logical volumes.

In case you're having problems (storage outages, after rebuilding a RAID or disk replacement, metadata consistency errors in vmkernel.log file) with VMFS datastores or a virtual flash resource, VOMA can be used from CLI of an ESXi host and you can check and fix minor consistency issues for VMFS datastore or virtual flash resource.

Make sure that the VMFS datastore does not span multiple extents (VOMA can be run only against a single extent). Also, you need to evacuate running VMs to another datastore or shut them down.

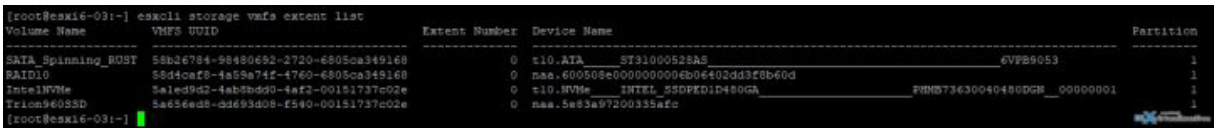
Check both KB articles for best practices. Basically, you should make sure that:

1. There are no VMs on the datastore you wish to analyze.
2. For VMFS5 datastores, the datastore is unmounted on all ESXi hosts (I haven't done that, so I have a message saying that one ESXi uses this datastore for heart beating)
3. For VMFS3, the LUN masking has to be in place by using claim rules.
4. The volume does not have multiple extents.

Step 1. Connect via SSH and enter this command to obtain the name and partition number of the device which contains the VMFS datastore.

esxcli storage vmfs extent list

You'll see an output like this



Step 2. Run this command by providing an absolute path to the device partition you want to check. You'll also need to give a partition number with the device name.

Example below:

voma -m vmfs -f check -d /vmfs/devices/disks/t10.ATA_ST31000528AS__6VPB9053:1

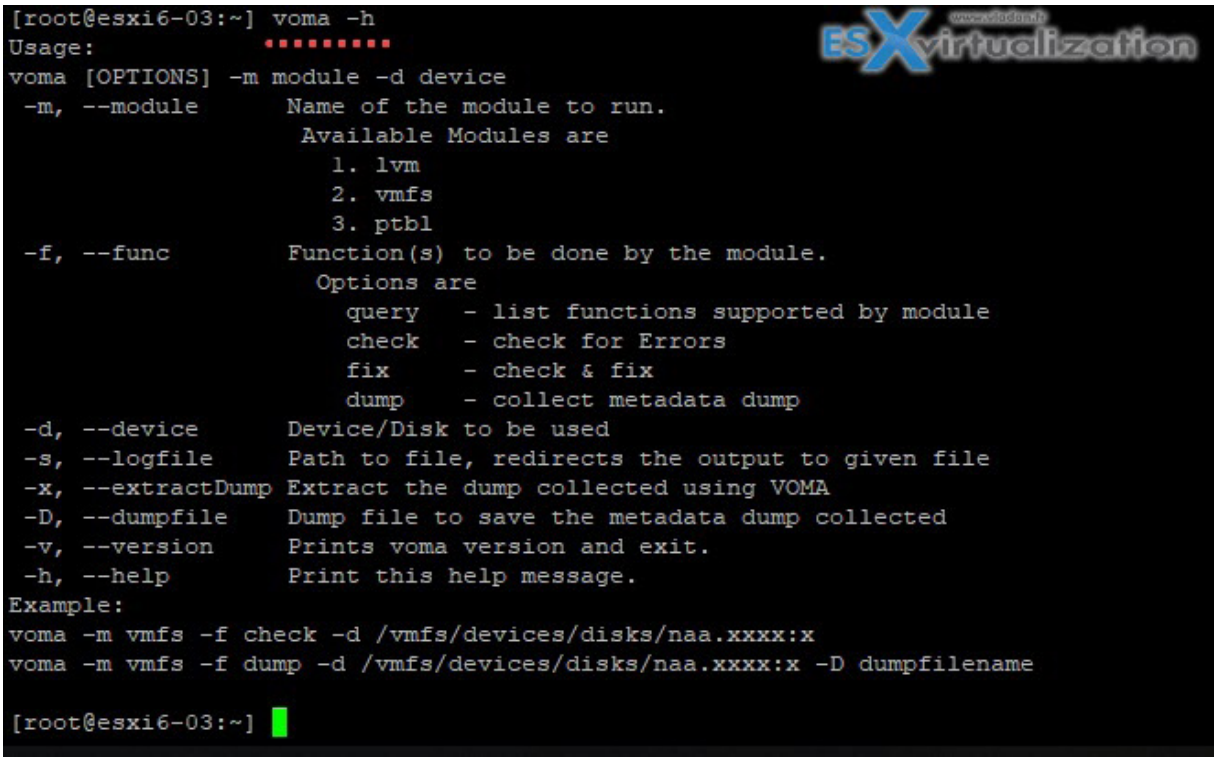
Gives us just a notification that the datastore heart beating is taking place on this datastore, but does not identify errors.

The options:

You can find all options by typing:

voma -h

The output looks like this:



You can log the output to a file with the **-s** option or further display a help message with each VOMA command

VOMA on our testing system (ESXi 6.5) has 4 options:

query - list functions supported by module
check - check for errors
fix - check & fix
dump - collect metadata dump

Below are two VMware KB articles which you may find interesting and useful. One of them helps you via the aid of VOMA, recreate missing partition tables.

- Using VMware vSphere On-disk Metadata Analyzer to re-create missing partition tables on VMware ESXi

The other one gives you some further guidance on the VOMA tool with some words of caution as well.

Quote:

Shutting down a virtual machine running on files possessing certain types of corrupt metadata may make the virtual machine and its data permanently unavailable. Because of this, it is always advisable to have current backups of the virtual machines in the environment. If you suspect that the virtual machine may become unavailable because, for example, there are read/write errors in the guest OS, or the virtual machine is unresponsive, you should open a support request.

Here is the link:

- Using vSphere On-disk Metadata Analyzer (VOMA) to check VMFS metadata consistency

Use the official documentation as well as your home lab for the study.

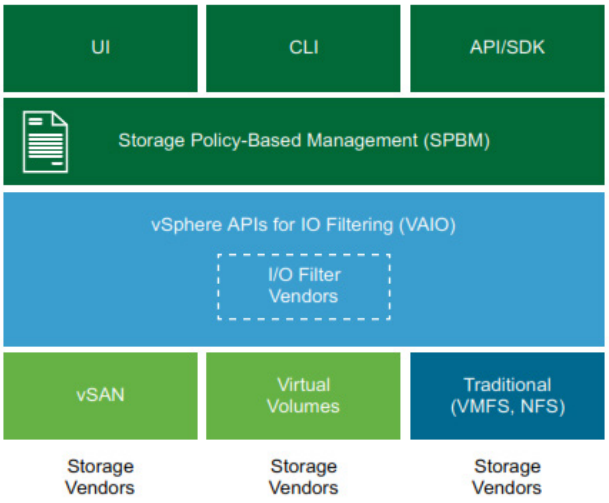
Objective 7.3 - Configure a storage policy

VMware vSphere Storage Policy Based Management (SPBM) provides a storage policy framework that serves as a single unified control panel across a broad range of data services and storage solutions.

As an abstraction layer, SPBM abstracts storage services delivered by Virtual Volumes, VSAN, I/O filters, or other storage entities.

Instead of integrating with each individual type of storage and data services, SPBM provides a universal framework for different types of storage entities.

VM Storage policies control which type of storage is provided for the virtual machine and to which storage the virtual machine is placed. They also determine data services that the virtual machine can use.



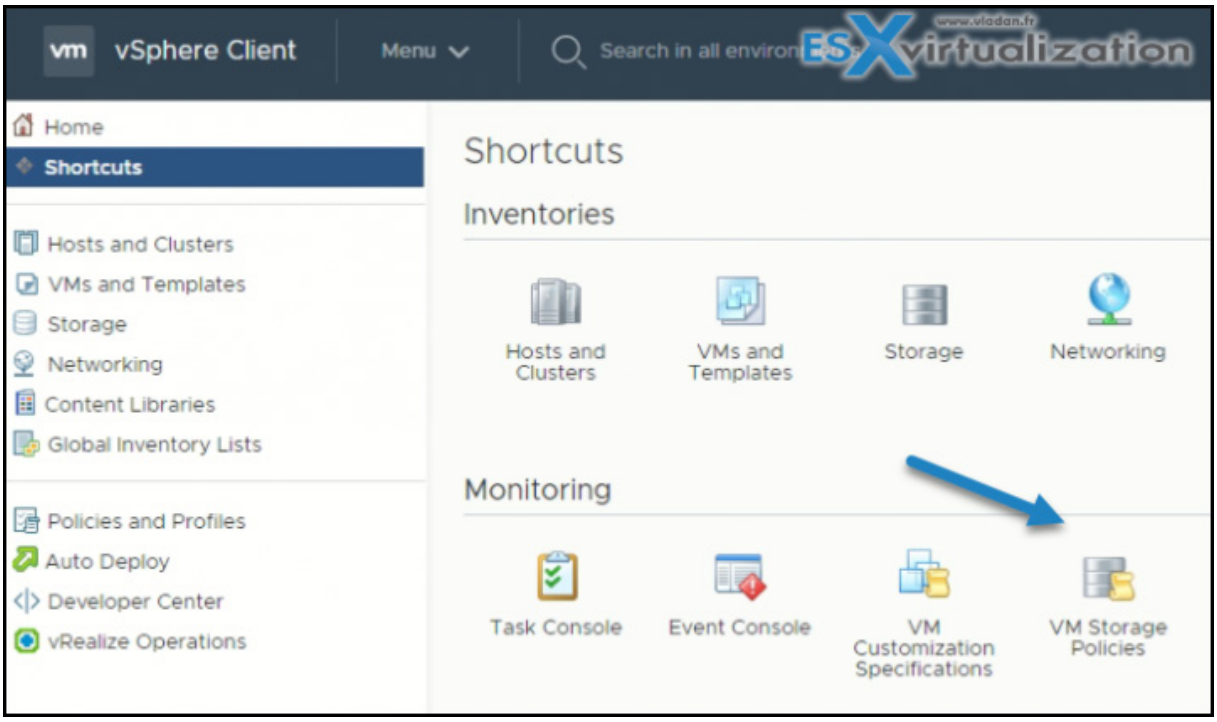
You use the VM Storage Policies interface to create a storage policy. When you define the policy, you specify various storage requirements for applications that run on virtual machines. You can also use storage policies to request specific data services, such as caching or replication for virtual disks.

You apply the storage policy when you create, clone, or migrate the virtual machine. After you apply the storage policy, the SPBM mechanism assists you with placing the virtual machine in a matching datastore. In certain storage environments, SPBM determines how the virtual machine storage objects are provisioned and allocated within the storage resource to guarantee the required level of service. The SPBM also enables requested data services for the virtual machine and helps you to monitor policy compliance

SPBM offers the following mechanisms:

- Advertisement of storage capabilities and data services that storage arrays and other entities, such as I/O filters offer.
- Bidirectional communications between ESXi and vCenter Server on one side, and storage arrays and entities on the other.
- Virtual machine provisioning based on VM storage policies.

Virtual Machine Storage Policies - VM storage policies control which type of storage is provided for the virtual machine and how the virtual machine is placed within the storage. They also determine data services that the virtual machine can use. vSphere offers default storage policies. In addition, you can define policies and assign them to the VMs.



The entire process of creating and managing storage policies typically includes several steps. Whether you must perform a specific step can depend on the type of storage or data services that your environment offers.

The whole process is done in 5 steps:

1. Populate the VM Storage Policies interface with appropriate data.
2. Create predefined storage policy components.
3. Create VM storage policies.
4. Apply the VM storage policy to the virtual machine.
5. Check compliance for the VM storage policy.

Before you start creating VM storage policies, you must populate the VM Storage Policy interface with information about storage entities and data services that are available in your storage environment. This info is coming from storage providers, also called VASA providers. Another source is datastore tags.

Storage Capabilities and Services - Virtual Volumes and VSAN are represented by the storage providers. Through the storage providers, the datastores can advertise their capabilities in the VM Storage Policy interface.

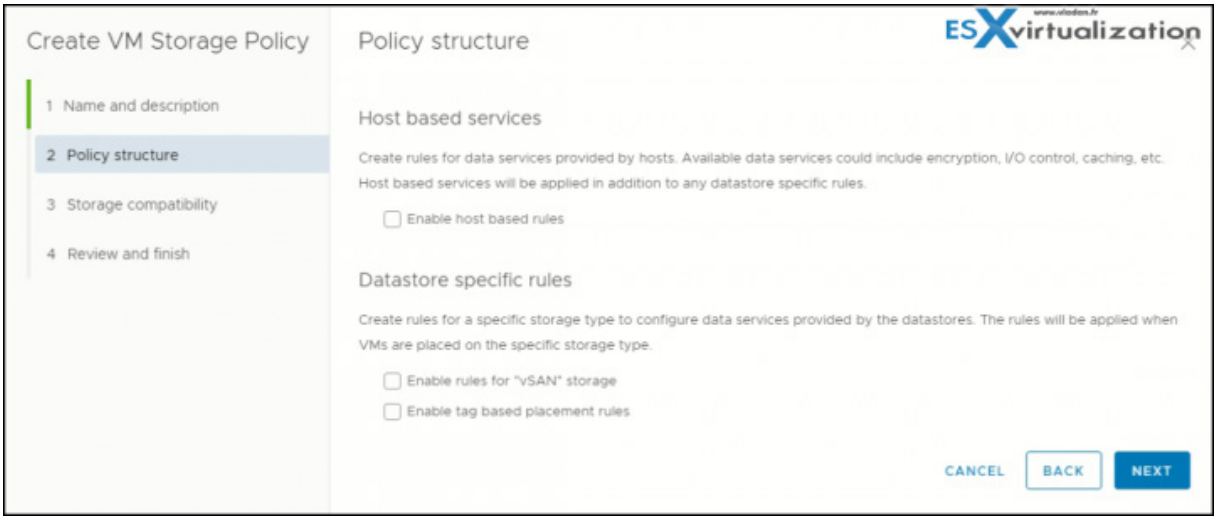
Data Services - I/O filters on your hosts are also represented by the storage providers. The storage provider delivers information about the data services of the filters to the VM Storage Policy interface. You can use this information when defining the rules for host-based data services, also called common rules. They activate the requested I/O filter data services for the virtual machine.

Tags - VMFS and NFS datastores are not represented by a storage provider. They do not display their capabilities and data services in the VM Storage Policies interface. You can use tags to encode information about these data stores. For example, you can tag your VMFS datastores as VMFS-Gold and VMFS-Silver to represent different levels of service.

Create a VM Storage Policy for Tag-Based Placement

Open the Create VM Storage Policy wizard. Click **Menu** > **Shortcuts** > **VM Storage Policies** > Click **Create VM Storage Policy**.

Enter the policy **name and description,** and click **Next**



On the **Tag-based** placement page, create the tag rules. Click **Add Tag Rule** and define tag-based placement criteria. Use the following as an example.

Tag category - Level of Service
Usage option - Use storage tagged with
Tags – Gold

All datastores with the Gold tag become compatible as the storage placement target.

On the Storage compatibility page, review the list of datastores that match this policy. On the Review and finish page, review the storage policy settings and click Finish.

Check also the vSphere online documentation about how to Define a VM Storage Policy in the vSphere Web Client VMware vSphere 6.7.

Final Words

Stay consistent with the study. Use our study guide but not exclusively—the more you read, the better. Don't use a single source for the study, but rather multiple sources at the same time. We try to give as many details as possible with screenshots and the like, but we are not able to cover everything.

Objective 7.4 - Configure host security

The ESXi hypervisor architecture has many built-in security features such as CPU isolation, memory isolation, and device isolation. You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.

Risks to the hosts are mitigated out of the box as follows:

- ESXi Shell and SSH are disabled by default.
- Only a limited number of firewall ports are open by default. You can explicitly open additional firewall ports that are associated with specific services.
- ESXi runs only services that are essential to managing its functions. The distribution is limited to the features required to run ESXi.
- By default, all ports that are not required for management access to the host are closed. Open ports if you need additional services.
- By default, weak ciphers are disabled and communications from clients are secured by SSL. The exact algorithms used for securing the channel depend on the SSL handshake. Default certificates created on ESXi use PKCS#1 SHA-256 with RSA encryption as the signature algorithm.
- A Tomcat Web service is used internally by ESXi to support access by Web clients. The service has been modified to run only functions that a Web client requires for administration and monitoring. As a result, ESXi is not vulnerable to the Tomcat security issues reported in broader use.
- VMware monitors all security alerts that can affect ESXi security and issues a security patch if needed.
- Insecure services such as FTP and Telnet are not installed

You can tighten security on hosts further by:

- Enabling/Disabling services in the ESXi firewall
- Change default account access
- Adding a VMware ESXi host to a directory service (Microsoft AD or other LDAP capable)
- Apply permissions to the ESXi hosts using host profiles
- Enable Lockdown Mode
- Control access to hosts (DCUI/Shell/SSH/MOB) - via console or vCenter.

Harden ESXi hosts

Only a limited set of services run by default on each ESXi host:

- ESXi Shell and SSH are disabled by default.
- You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.
- An ESXi host is also protected with a firewall. You can open ports for incoming and outgoing traffic as needed but should restrict access to services and ports.
- Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment.
- Hosts are provisioned with certificates that are signed by the VMware Certificate Authority (VMCA) by default.
- You might consider using UEFI Secure Boot for your ESXi system.
- Join ESXi hosts to an Active Directory (AD) domain to eliminate the need to create and maintain multiple local user accounts. Using AD for user authentication simplifies the ESXi host configuration, and ensures password complexity; reuse policies are enforced and there is a reduced risk of security breaches and unauthorized access. (Note: if the AD group “ESX Admins” (default) exists then all users and groups that are assigned as members to this group will have full administrative access to all ESXi hosts the domain).
- **Use ESXi lockdown mode** – Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server and features two modes available (normal and strict). Tip: What is ESXi Lockdown Mode? Users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host and if these services are enabled. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option
- **ESXi.set-shell-timeout** – sets a timeout to limit how long the ESXi shell and SSH services are allowed to run.

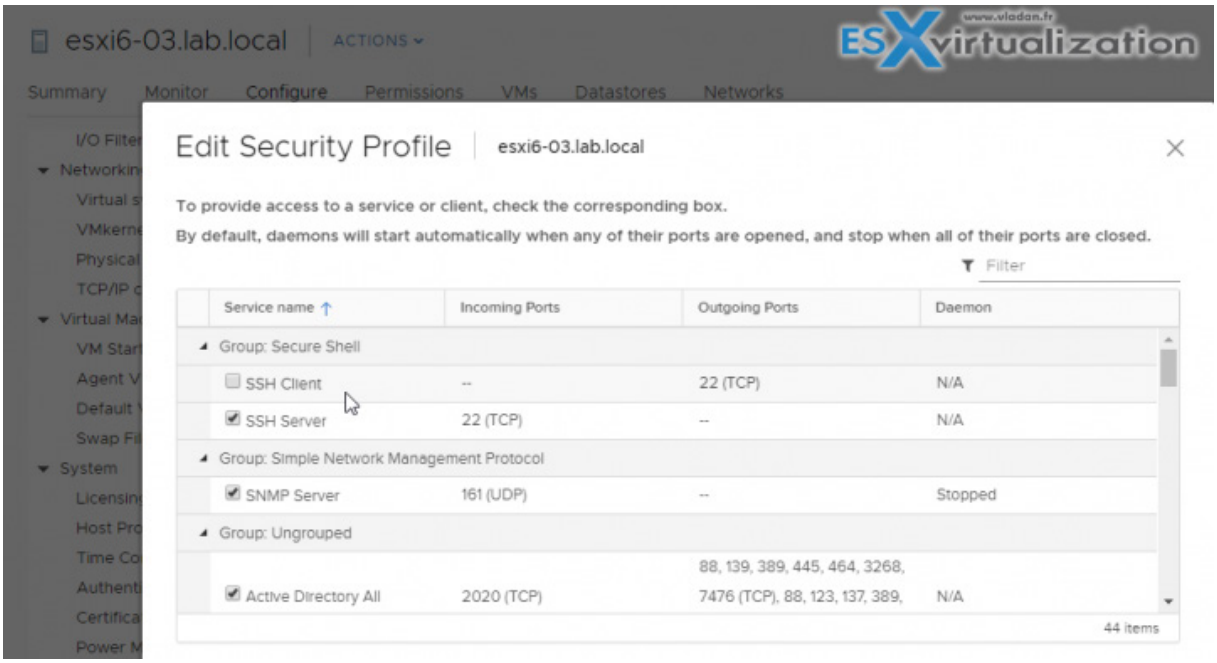
Check the VMware Security Hardening guides at VMware Blog.

Enable/Configure/Disable services in the ESXi firewall

For each ESXi host, you can create firewall rules.

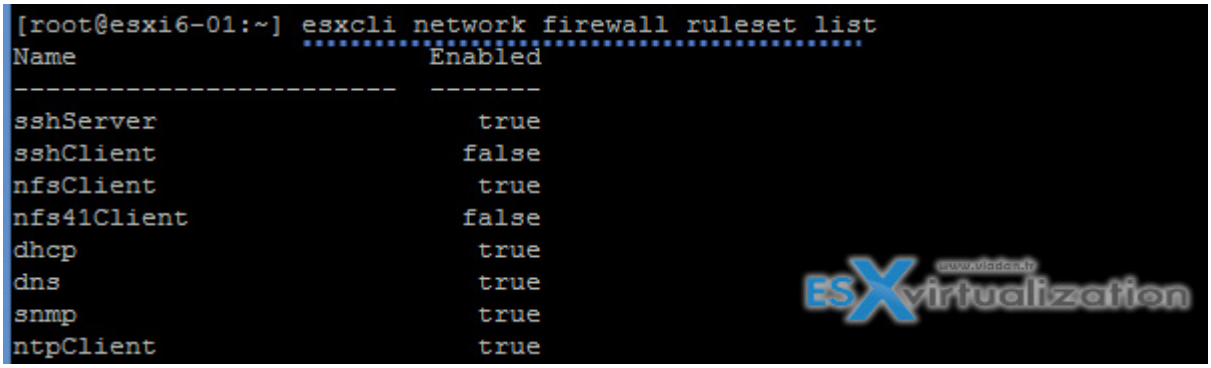
Connect via vSphere web client > Configure > System > Firewall section > Edit > Select Rule > Enable/disable.

Select the rule sets to enable or deselect the rule sets to disable. You can change startup policy to have a service started with the host or by port usage. Some services allow for configuring IP address from which connections are permitted.



Check which services are active

esxcli network firewall ruleset list



Open firewall port via CLI:

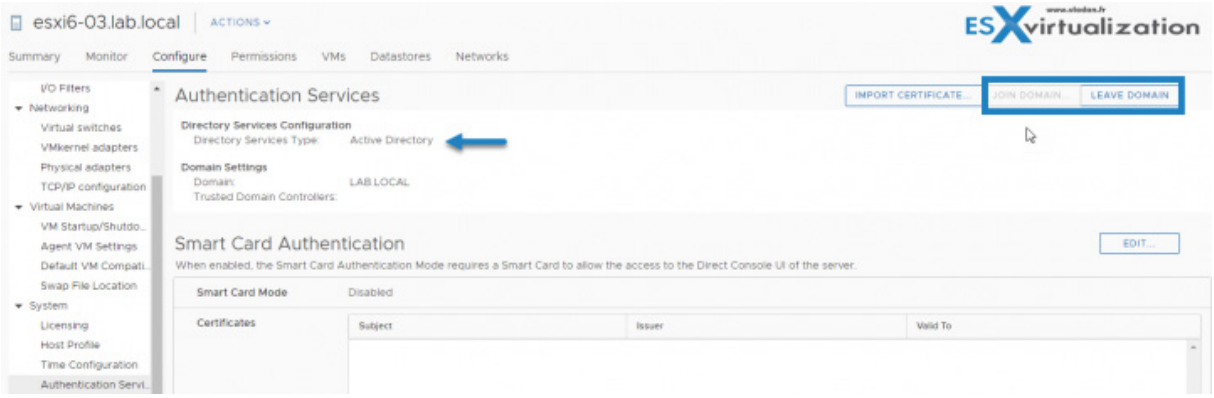
esxcli network firewall ruleset set -e true -r httpsClient

Add an ESXi Host to a directory service

You can configure a host to use a directory service such as Active Directory to manage users and groups. When you add an ESXi host to Active Directory, the DOMAIN group 'ESX Admins' is assigned full administrative access to the host if it exists.

A special AD group known as "**ESX Admins**" shall be manually created before a host is joined to Microsoft AD. **Why?** Because all members of this group (ESX admins) are automatically assigned to the **Administrator role** on the host when this host is joined to an AD. If not, the permissions have to be **applied manually.**

Select your host > **Configure > System > Authentication Services > Join Domain > Enter your Microsoft domain name > Use a user and password who has** permission **to join the host to the domain > Click OK.**



Apply permissions to ESXi Hosts using Host Profiles

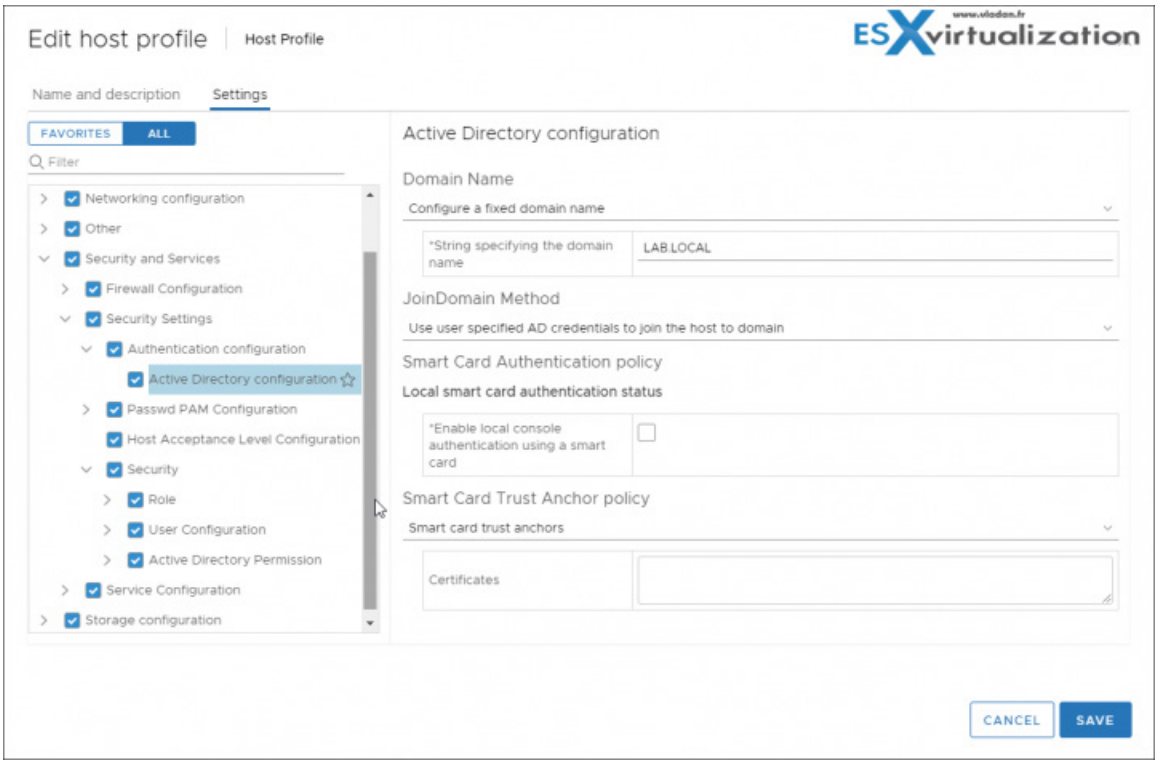
Host profiles allow you to "standardize" configurations for ESXi hosts and automate compliance for settings you have set on a reference host. Host profiles allow you to control many aspects of host configuration including memory, storage, networking, and so on. But most importantly, it's possible to apply the same security settings for all hosts within a cluster for example, without configuring those host after host.

In some cases, host profiles can be also useful when, for example, you need to reset esxi root password on a host.

1. Set up the reference host with necessary specifications and create a host profile.
2. Attach the profile to a host or cluster.
3. Apply the host profile of the reference host to other hosts or clusters.

If you haven't done so yet, go to Home > Host profiles > Extract profile from a host. Once you have that profile you can apply it to a host.

- **Click** the host profile > Click **Configure** > **Edit Host profile**

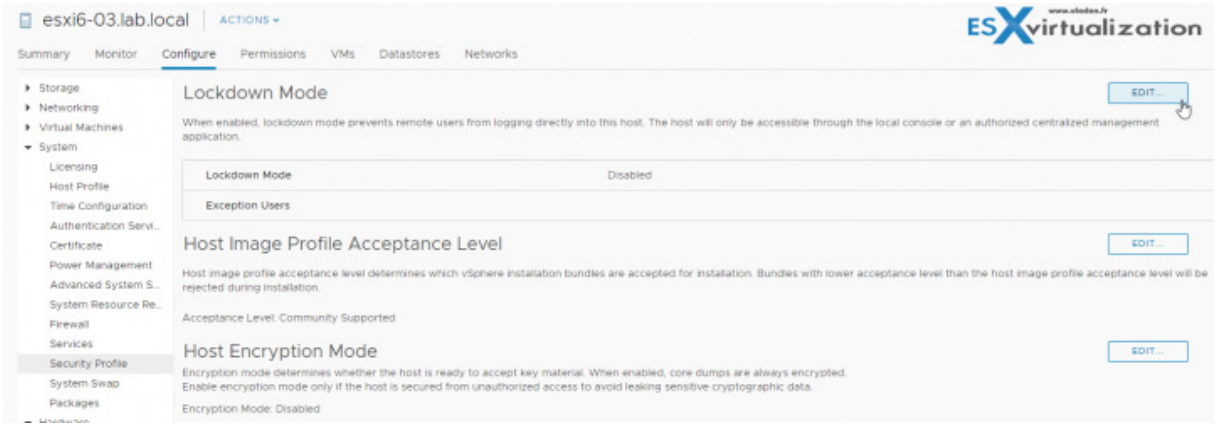


Enable Lockdown Mode

Lockdown Modes:

- **Disabled** – Lockdown mode is disabled.
- **Normal** – The host can be accessed through vCenter Server. Only users who are on the **Exception Users list** and have administrator privileges can log in to the Direct Console User Interface. If SSH or the ESXi Shell is enabled, access might also be possible.
- **Strict** – The host can only be accessed through vCenter Server. If SSH or the ESXi Shell is enabled, running sessions for accounts in the *DCUI.Access* advanced option and for Exception User accounts that have administrator privileges remain enabled. All other sessions are terminated. **DCUI is stopped.**

Select your host > Configure > System > Security Profile > Lockdown mode > Edit.

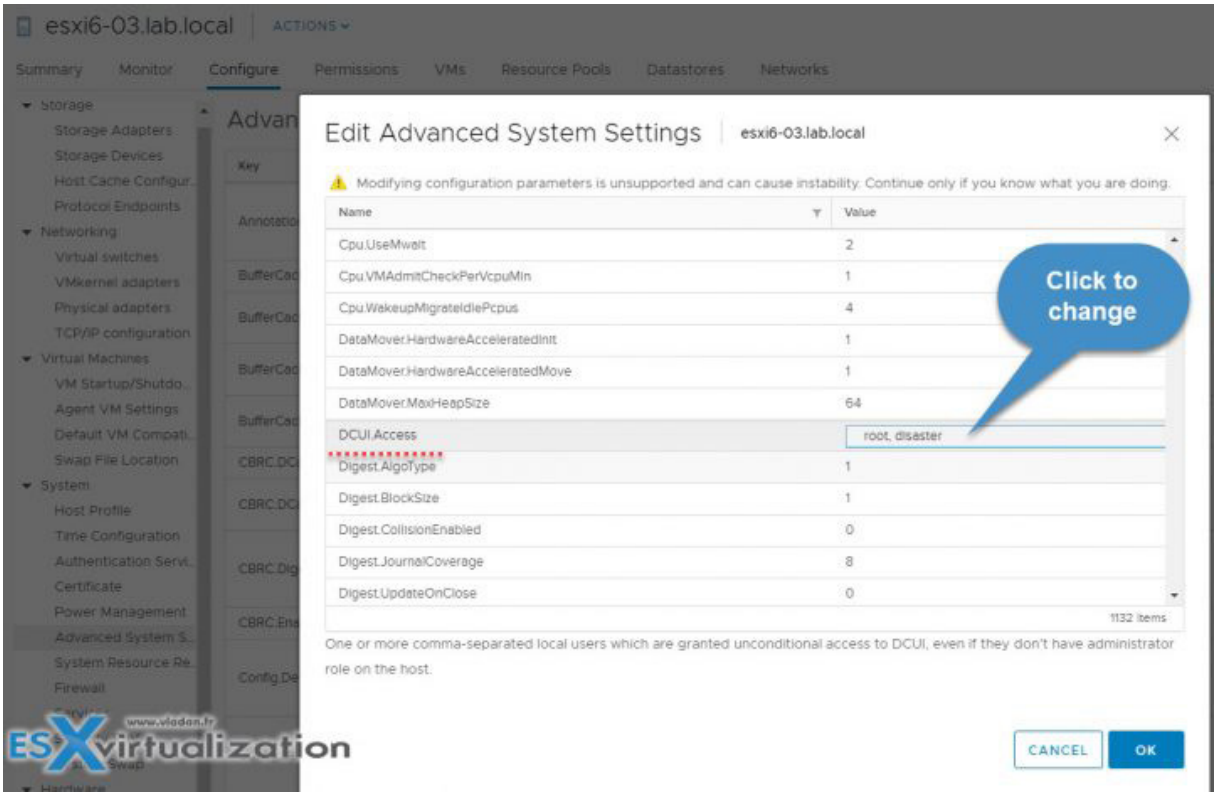


Let us consider accounts in the Exception User list for lockdown mode who have administrative privileges on the host. The Exception Users list is meant for service accounts that perform very specific tasks. Adding ESXi administrators to this list defeats the purpose of lockdown mode.

Where to add an account to the Exception Users list?

You'd have to first create a local ESXi user and then specify this advanced setting on a per-host base. So, in my case, I created a sample local ESXi user called "disaster" through ESXi host client which is a local ESXi user.

In order to modify the Exception users list, you'll have to use the vSphere HTML5 client of vSphere Web Client. To access this setting, you **Select your host > System > Advanced System Settings >** within the list find the **DCUI.Access** > click to add another local ESXi user there. The root user is already present there by default.



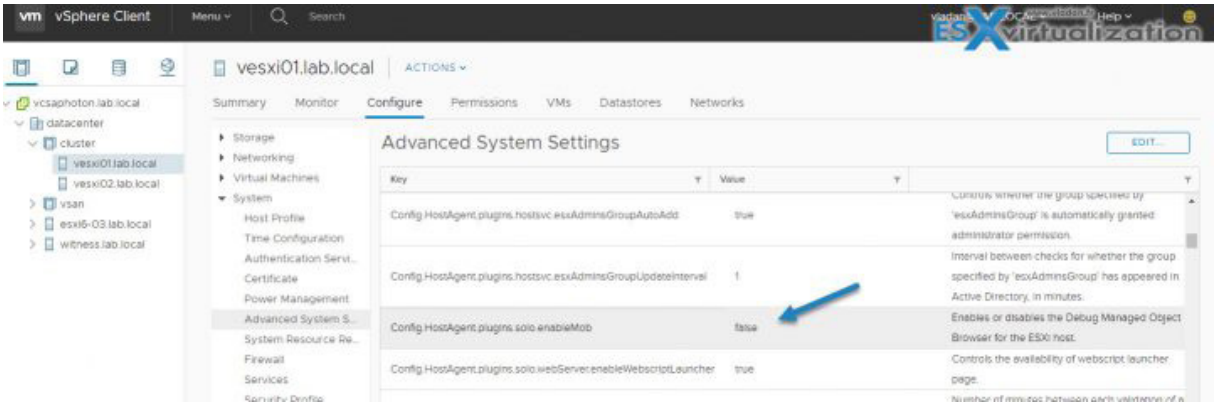
The exception users can only perform tasks for which they have privileges. So even if you create your local user and put them on the Exceptions list, the user won't be able to connect unless you give them a privilege.

Control access to hosts (DCUI/Shell/SSH/MOB)

You can control the access to the DCUI/Shell and SSH. The MOB is the managed object browser (MOB) and provides a way to explore the VMkernel object model. vSphere 6.0 and later have the MOB is disabled by default because it could be exploited by hackers.

To Enable MOB:

Select host > Advanced System Settings > Advanced > Config.HostAgent.plugins.solo. enableMob > modify the value.



The security of ESXi hosts is manageable through vCenter server, but also on a per-host basis if you have hosts which are not attached to vCenter.

Restrict administrative privileges

Not all administrator users must have the Administrator role. You might want to create a **custom role** with the appropriate set of privileges and assign it to other administrators. Users with the vCenter Server Administrator role have privileges on all objects in the hierarchy.

Follow the principle of least privilege. Clone and customize role for nodes you need, and then assign this role to administrators.

Being secured but not too “locked,” you can have a good balance between security and manageability. Making any changes to the security of the vSphere environment might have potentially large impacts on the manageability of the environment for you and your team. You should always analyze your needs, your risks, and your requirements. Then change the security of your environment.

Objective 7.5 - Configure role-based user management

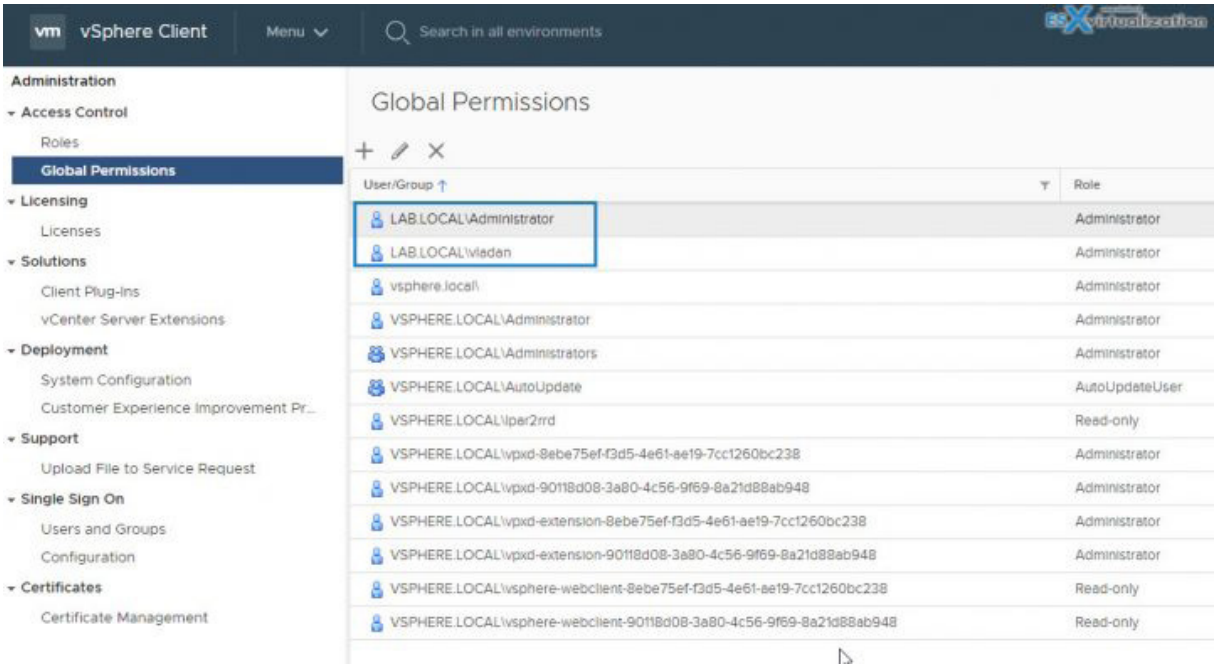
In this post, **VCP6.7-DCV Objective 7.5 - Configure role-based user management**, we’ll be detailing vCenter management, roles structure, permissions, etc.

VMware vSphere has predefined roles. A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc. are predefined roles.

vCenter Server Permissions - The permission model for vCenter Server systems basically allows you to assign permissions to objects in the object hierarchy. Each permission gives one user or group a set of privileges, that is, a role for a selected object. For example, you can select a virtual machine and

select Add Permission to assign a role to a group of users in a domain that you select. That role gives those users the corresponding privileges on the VM.

Global Permissions - Global permissions are applied to a global root object that spans solutions. For example, if both vCenter Server and vRealize Orchestrator are installed, you can use global permissions. For example, you can give a group of users Read permissions to all objects in both object hierarchies. Global permissions are replicated across the vsphere.local domain. Global permissions do not provide authorization for services managed through vsphere.local groups.



To check the propagated and explicit permission assignments, we have to connect to our **vCenter server** > Global Administration. But before doing this, it's important to know the difference between Permissions, Users and Groups.

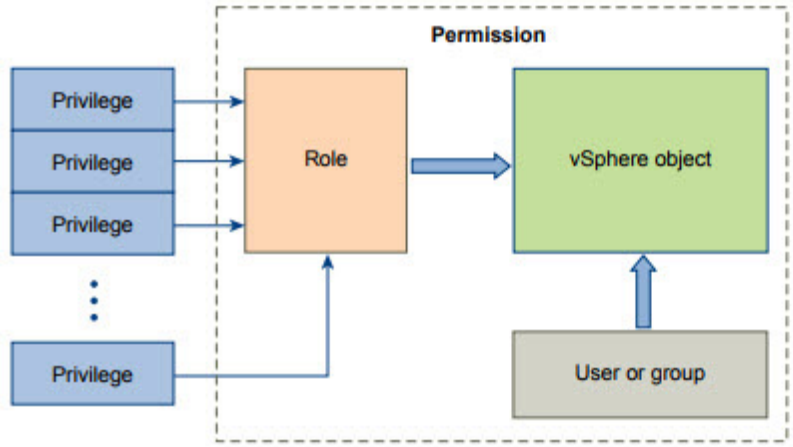
- **Permissions** – each object in the vCenter hierarchy has associated permissions.
- **Privileges** – Each permission has access controls to the resource. From there, group privileges into roles, which are mapped to users or groups.
- **Users and groups** – this part is pretty obvious. Only users authenticated through Single Sign-ON (SSO) can be given particular privileges. Users must be defined within the SSO or users from external identity sources such as Microsoft AD.
- **Roles** – what is a role? A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc. are predefined roles. You can clone them or change them (except Administrator).

When you assign permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission.

Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

The image below (from vSphere 6.7 Security guide) illustrates the inventory hierarchy and the paths by which permissions can propagate.

Figure 2-1. vSphere Permissions



To assign permissions to an object, you follow these steps:

1 Select the object to which you want to apply the permission in the vCenter object hierarchy.

2 Select the group or user that should have privileges on the object.

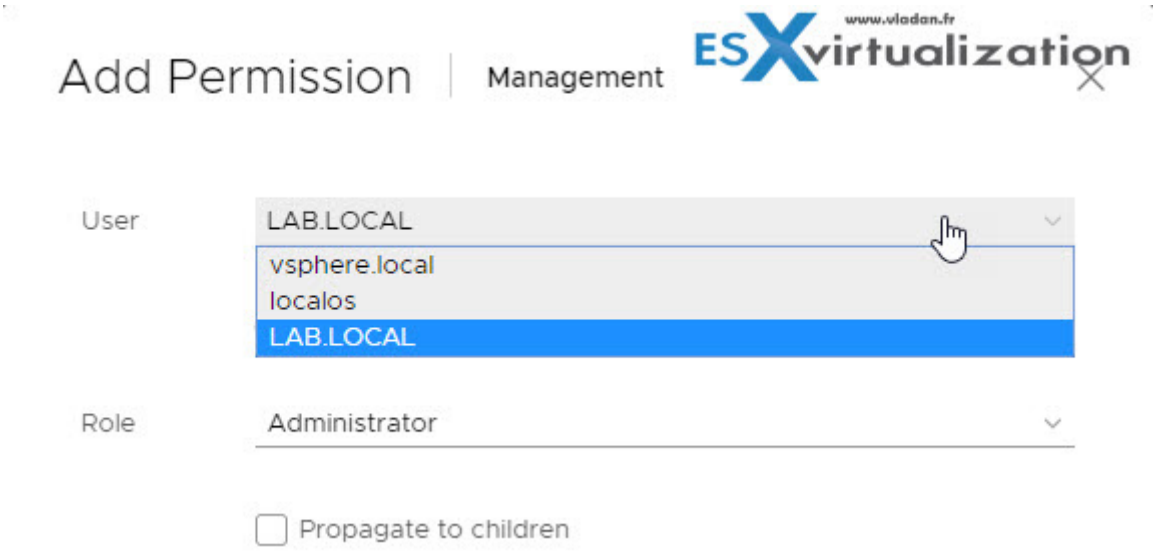
3 Select individual privileges or a role, that is a set of privileges, that the group or user should have on the object.

By default, permissions propagate, that is the group or user has the selected role on the selected object and its child objects.

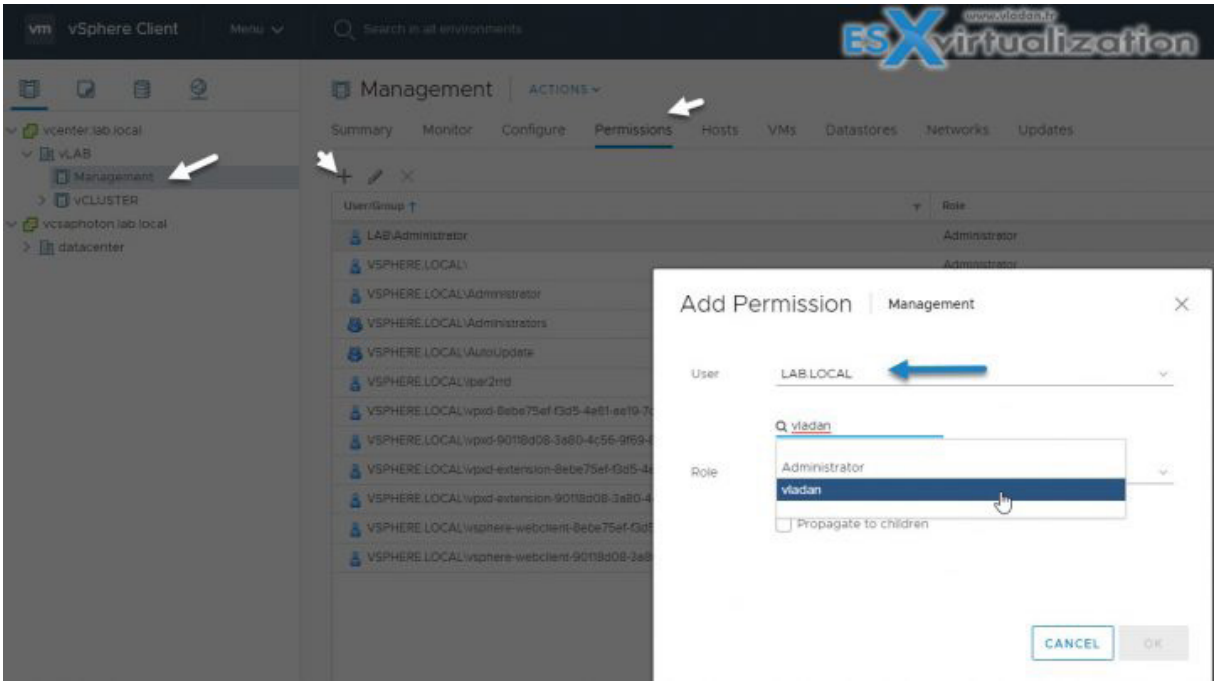
Add/Modify/Remove permissions for users and groups on vCenter Server inventory objects

To Add/Modify/Remove permission for a user and group from vCenter inventory you have to **Select an object from the inventory** > click **Permissions TAB >** there you can add, edit, and remove permissions.

From the drop-down select the identity source (in our case our Lab.local AD domain)

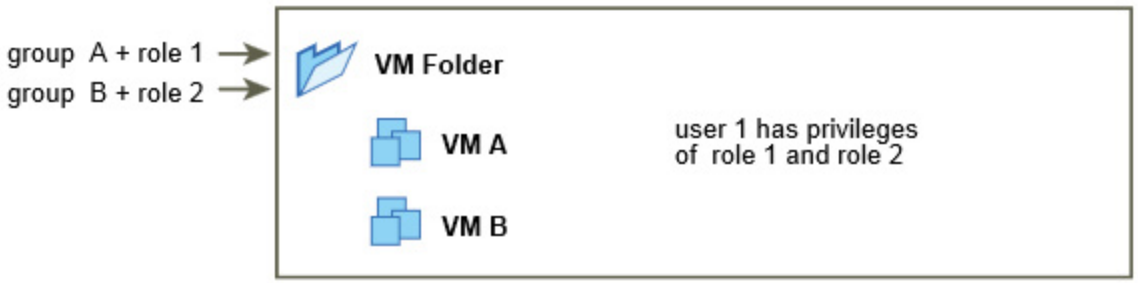


And then start typing the name of the person.... (my name, in my case).



Inheritance, Parent and Child permissions

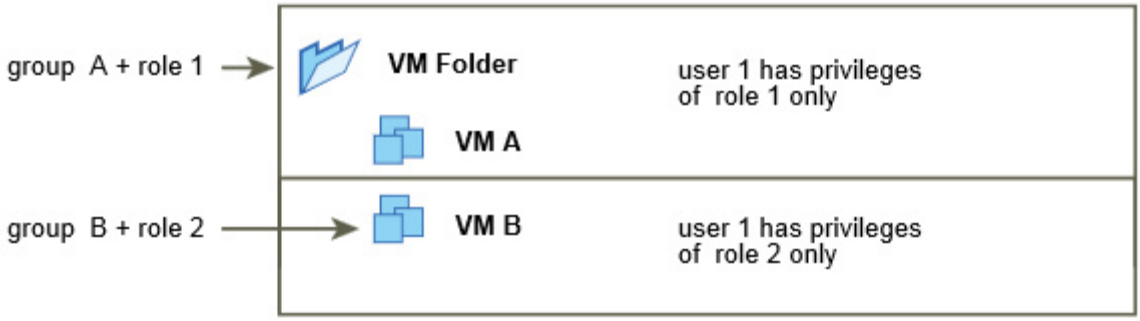
- **Inheritance of Multiple Permissions** – what if the user is member of **more than one group**? Then **combined** privileges within the roles apply. The example below shows user member of both groups.



- **Child permissions override Parent permissions** – Permissions applied on a child object always override permissions that are applied on a parent object. See examples P. 119 of vSphere Security Guide.

Ex. Role 1 can power on VMs and Role 2 can take snapshots.
Group A is granted Role 1 on VM folder and permissions propagate to child objects
Group B is granted Role 2 on VM B

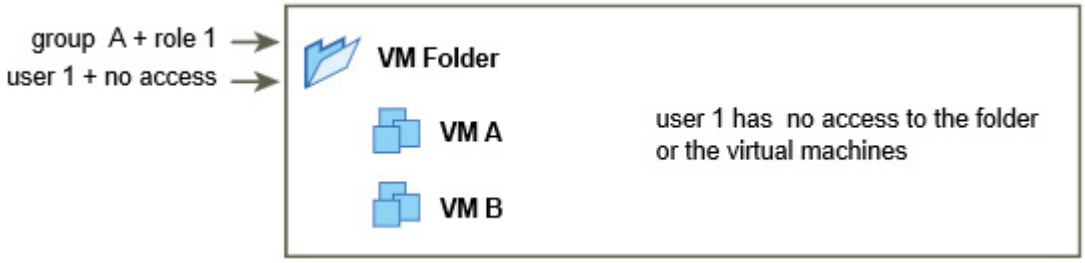
User 1, who belongs to groups A and B, logs on. Because Role 2 is assigned at a lower point in the hierarchy than Role 1, it overrides Role 1 on VM B. User 1 can power on VM A, but not take snapshots. User 1 can take snapshots of VM B, but not power it on.



- **User role overriding group role** – this is the case if two permissions are defined on the same object.

One permission is granted to a group, the other to a user which at the same time is a member of the group. Role 1 can power VMs Group A is granted Role 1 on VM folder and at the same time, User 1 is granted No Access role on VM folder.

User 1, who belongs to group A, logs on. The No Access role granted to User 1 on VM Folder overrides the role assigned to the group. User 1 has no access to VM Folder or VMs A and B.



Where possible, assign a role to a group rather than individual users to grant privileges to that group. Grant permissions only on the objects where they are needed and assign privileges only to users or groups that must have them.

If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges.

The best is to group objects into folders, (including hosts). Then you can assign permissions to folders containing hosts and other objects.

In most cases, enable propagation when you assign permissions to an object. This ensures that when new objects are inserted into the inventory hierarchy, they inherit permissions.

Tip**: To **Mask specific areas of the vCenter hierarchy – Use the ***No Access role*** to mask specific areas of the hierarchy if you do not w*ish for certain users or groups to have access to the objects in that part of the object hierarchy.*

vCenter Server extensions might define additional privileges not even listed in the PDF. Check the vSphere 6.7 security guide.

Permissions defined for a child object **always override** the permissions that are propagated from parent objects.

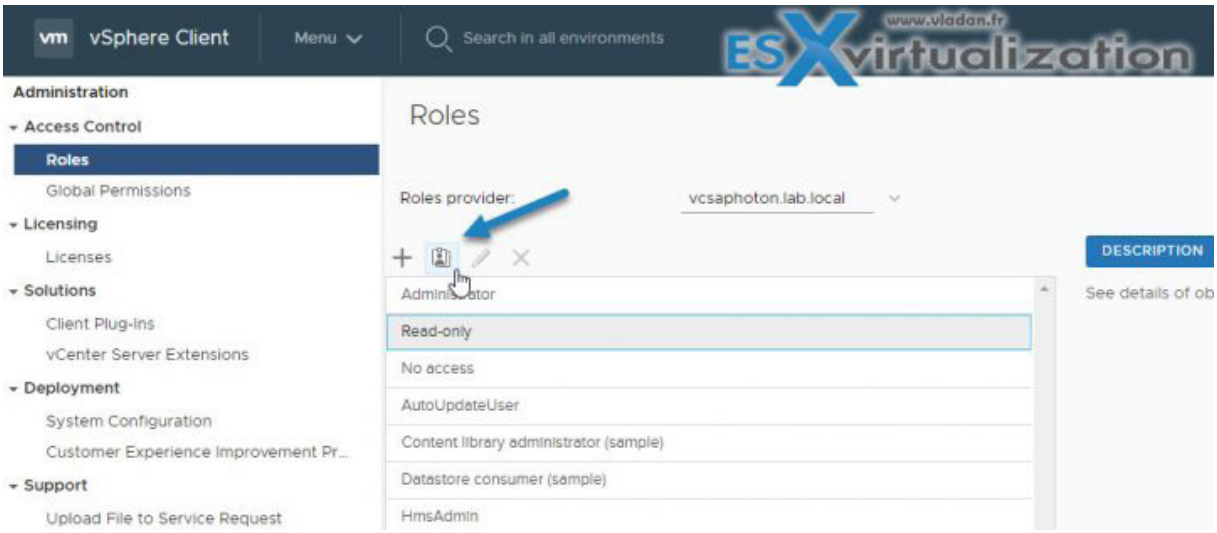
Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent data center. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously.

Create/Clone/Edit vCenter Server Roles

To edit, create or clone vCenter roles, it's necessary to use vSphere Web client > Administration > Roles OR Home > Roles. Default roles are:

- Administrator
- Read-Only
- No Access

To clone a role, click the icon, as seen below.



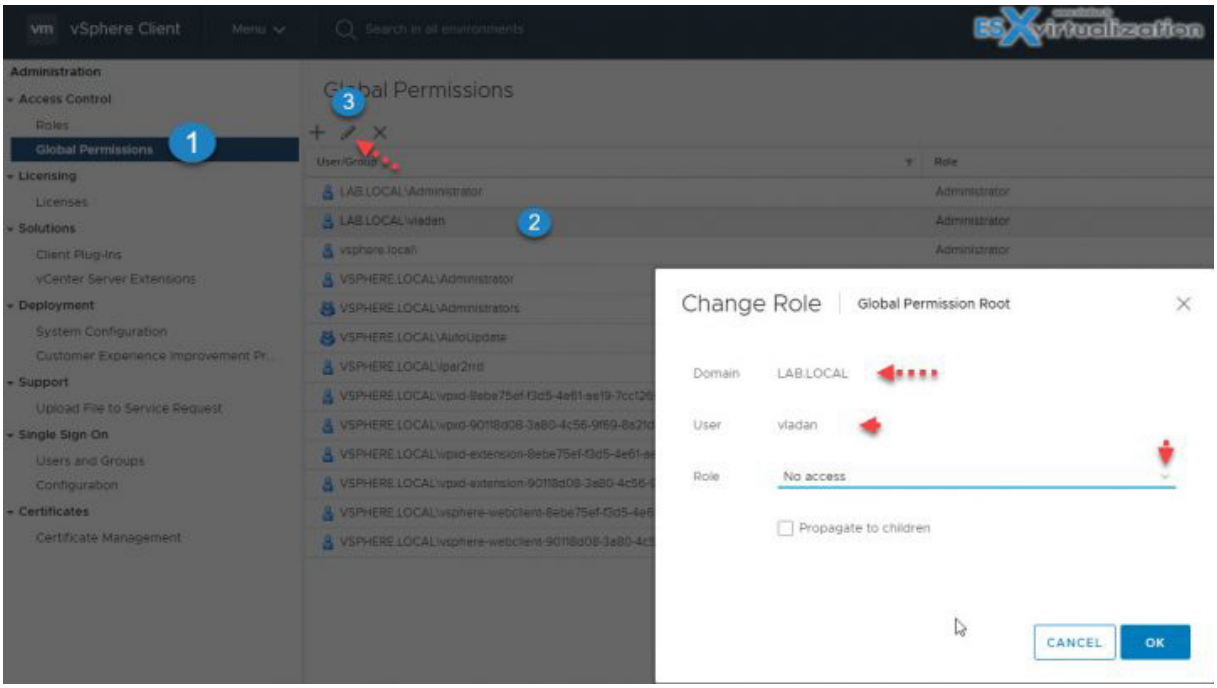
1. Log in to vCenter Server with the vSphere Web Client.
2. Select Home, click **Administration** and click **Roles**.
3. **Select** a role and click the **Clone** role action icon.
4. Type a **name** for the cloned role.
5. **Select or deselect privileges** for the role and click **OK**.

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role.

Apply a role to a User/Group and to an object or group of object

A role is a predefined set of privileges. A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc. are predefined roles. Privileges define rights to perform actions and read properties. For example, the **Virtual Machine Administrator** role allows a user to read and change virtual machine attributes.

You can change the role of a user by going to **Global permissions** > **Select User** > Click **Edit icon** > The user comes preselected > In the drop-down menu, choose **a different role** for the user.



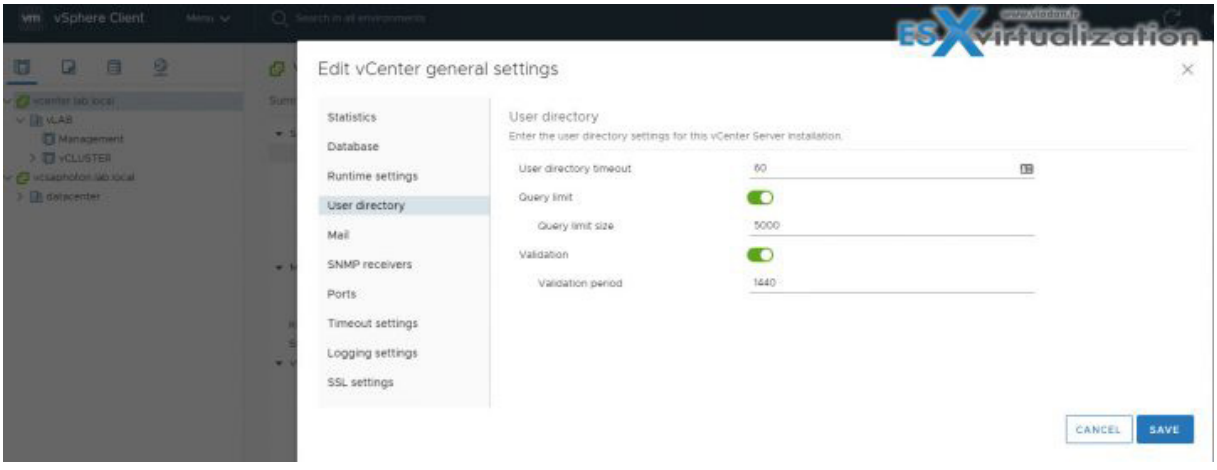
Change role

vCenter Server has certain system roles and some sample roles you can play with.

- **System Roles** – System roles are permanent, not editable. You cannot edit the privileges associated with these roles.
- **Sample roles** – Sample roles are useful because they have been created for frequently performed tasks. Those roles are modifiable, so you are allowed to **clone, modify, or remove** these roles

vCenter Server systems that use a directory service regularly validate users and groups against the user directory domain. Validation occurs at regular intervals specified in the vCenter Server settings.

Home > Hosts and clusters > Select vCenter > server > Configure > Settings> General > Edit and select User directory > Change the values as needed.



The Options:

- **User directory timeout –** Timeout interval, in seconds, for connecting to the Active Directory server. This value specifies the maximum amount of time vCenter Server allows a search to run on the selected domain. Searching for large domains can take a long time.
- **Query limit** – Select the checkbox to set a maximum number of users and groups that vCenter Server displays.
- Query limit size – This is the maximum number of users and groups from the selected domain that vCenter Server displays in the Select Users or Groups dialog box. If you enter 0 (zero), all users and groups appear.
- **Validation** – Deselect the checkbox to disable validation
- **Validation Period** – Specifies how often vCenter Server validates permissions, in minutes.

Many tasks require permissions on multiple objects in the inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot complete successfully.

Any operation that consumes storage space requires the Datastore.Allocate Space privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.

Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.

Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the Resource.Assign Virtual Machine to Resource Pool privilege.

Screenshot directly from the vSphere 6.7 security guide (see in PDF).

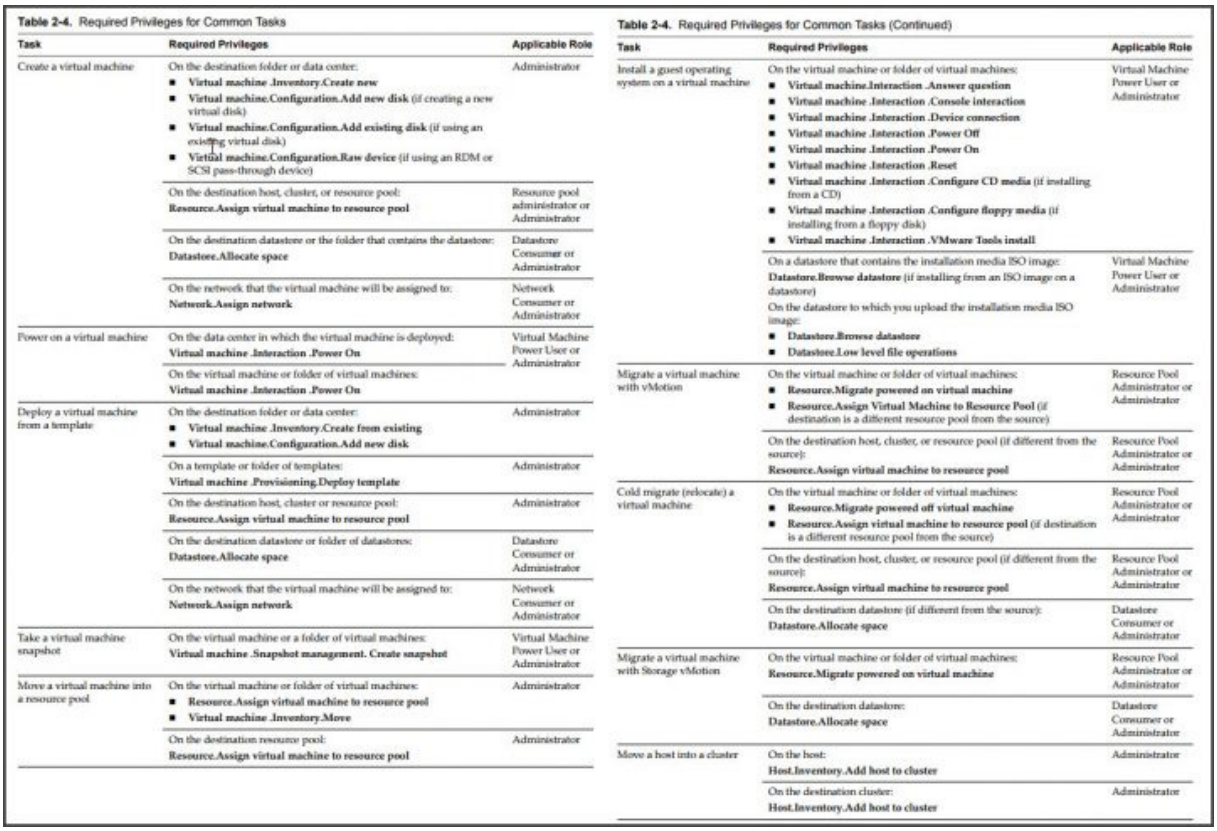


Table 2-4. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: ■ **Virtual machine .Inventory.Create new** ■ **Virtual machine.Configuration.Add new disk** (if creating a new virtual disk) ■ **Virtual machine.Configuration.Add existing disk** (if using an existing virtual disk) ■ **Virtual machine.Configuration.Raw device** (if using an RDM or SCSI pass-through device)	Administrator
	On the destination host, cluster, or resource pool: **Resource.Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or the folder that contains the datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Power on a virtual machine	On the data center in which the virtual machine is deployed: **Virtual machine .Interaction .Power On**	Virtual Machine Power User or Administrator
	On the virtual machine or folder of virtual machines: **Virtual machine .Interaction .Power On**	
Deploy a virtual machine from a template	On the destination folder or data center: ■ **Virtual machine .Inventory.Create from existing** ■ **Virtual machine.Configuration.Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine .Provisioning.Deploy template**	Administrator
	On the destination host, cluster or resource pool: **Resource.Assign virtual machine to resource pool**	Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine .Snapshot management. Create snapshot**	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: ■ **Resource.Assign virtual machine to resource pool** ■ **Virtual machine .Inventory.Move**	Administrator
	On the destination resource pool: **Resource.Assign virtual machine to resource pool**	Administrator

Table 2-4. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: ■ **Virtual machine.Interaction .Answer question** ■ **Virtual machine .Interaction .Console interaction** ■ **Virtual machine .Interaction .Device connection** ■ **Virtual machine .Interaction .Power Off** ■ **Virtual machine .Interaction .Power On** ■ **Virtual machine .Interaction .Reset** ■ **Virtual machine .Interaction .Configure CD media** (if installing from a CD) ■ **Virtual machine .Interaction .Configure floppy media** (if installing from a floppy disk) ■ **Virtual machine .Interaction .VMware Tools install**	Virtual Machine Power User or Administrator
	On a datastore that contains the installation media ISO image: **Datastore.Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: ■ **Datastore.Browse datastore** ■ **Datastore.Low level file operations**	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered on virtual machine** ■ **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered off virtual machine** ■ **Resource.Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore.Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource.Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a host into a cluster	On the host: **Host.Inventory.Add host to cluster**	Administrator
	On the destination cluster: **Host.Inventory.Add host to cluster**	Administrator

Compare and contrast default system/sample roles

vCenter Server provides a few default roles. You cannot change the privileges associated with the default roles. The default roles are organized as a hierarchy. Each role inherits the privileges of the previous role.

For example, the Administrator role inherits the privileges of the Read Only role. Roles that you create do not inherit privileges from any of the system roles.

Administrator Role – Users with the Administrator role for an object are allowed to view and perform all actions on the object. This role also includes all privileges inherent in the Read Only role. If you are acting in the Administrator role on an object, you can assign privileges to individual users and groups. If you are acting in the Administrator role in vCenter Server, you can assign privileges to users and groups in the default vCenter Single Sign-On identity source. Supported identity services include Windows Active Directory and OpenLDAP 2.4.

By default, the administrator@vsphere.local user has the Administrator role on both vCenter Single Sign-On and vCenter Server after installation. That user can then associate other users with the Administrator role on vCenter Server.

No Cryptography Administrator Role – Users with the No cryptography administrator role for an object have the same privileges as users with the Administrator role, **except for Cryptographic operations privileges**. This role allows administrators to **designate other administrators that**

cannot encrypt or decrypt virtual machines or access encrypted data, but that can perform all other administrative tasks.

Where possible, assign a role to a group rather than individual users to grant privileges to that group.

Use caution when adding permission to the root vCenter Server objects. Users with privileges at the root level have access to global data on vCenter Server, such as roles, custom attributes, vCenter Server settings.

Today we covered another topic from Professional vSphere 6.7 Exam 2019. Stay tuned for more!

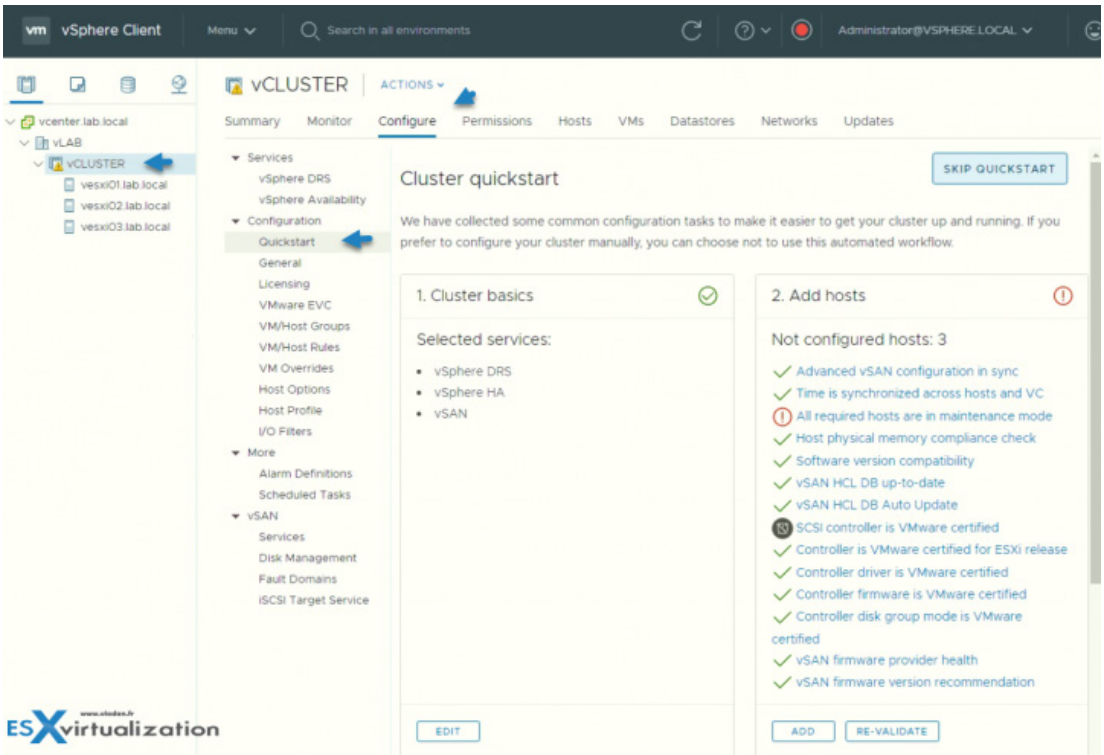
Objective 7.6 - Configure and use vSphere Compute and Storage cluster options

After you create your first datacenter object in vSphere client you can start adding more objects inside. You can add hosts, clusters, resource pools, vApps, networking, datastores, and virtual machines to the data center.

To enable your cluster for vSphere HA, you must first create an empty cluster. After you plan the resources and networking architecture of your cluster, use the vSphere Web Client to add hosts to the cluster and specify the cluster's vSphere HA settings.

Note: A vSphere HA-enabled cluster is a prerequisite for vSphere Fault Tolerance.

The best for configuring cluster options is to use the **Quickstart** wizard which is new in vSphere 6.7.



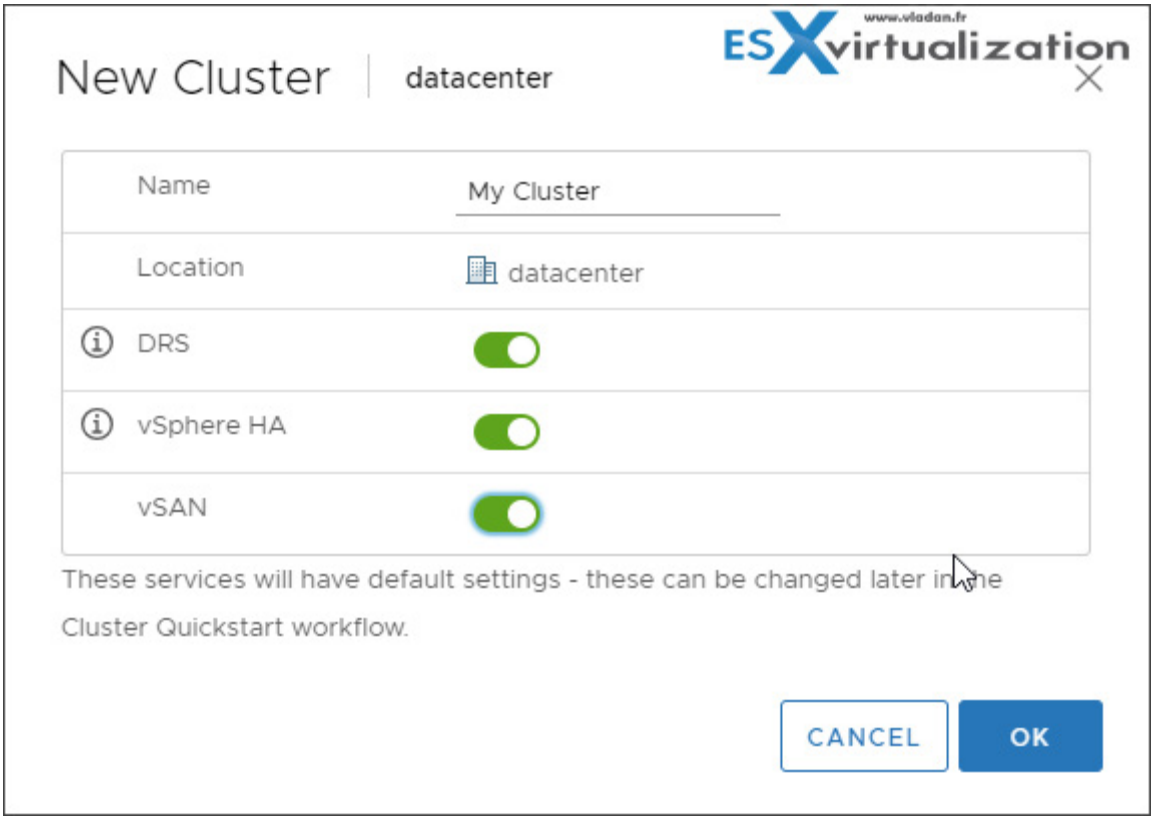
However, you should check whether you have adequate permissions to create a cluster.

- Verify that you have sufficient permissions to create a cluster object.
- Verify that a data center, or folder within a data center, exists in the inventory.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual VSAN or networking configuration.

You can have several clusters, each active with different services (DRS, HA, VSAN, etc).

In the vSphere Web Client, browse to the data center in which you want the cluster to reside and click **New Cluster** > Complete the **New Cluster wizard** > Do not turn on vSphere HA (or DRS).

Click OK to close the wizard and create an empty cluster.



After activating those services, you'll need to configure the appropriate vSphere HA settings for your cluster:

- Failures and responses
- Proactive HA Failures and Responses
- Admission Control
- Heartbeat Datastores
- Advanced Options

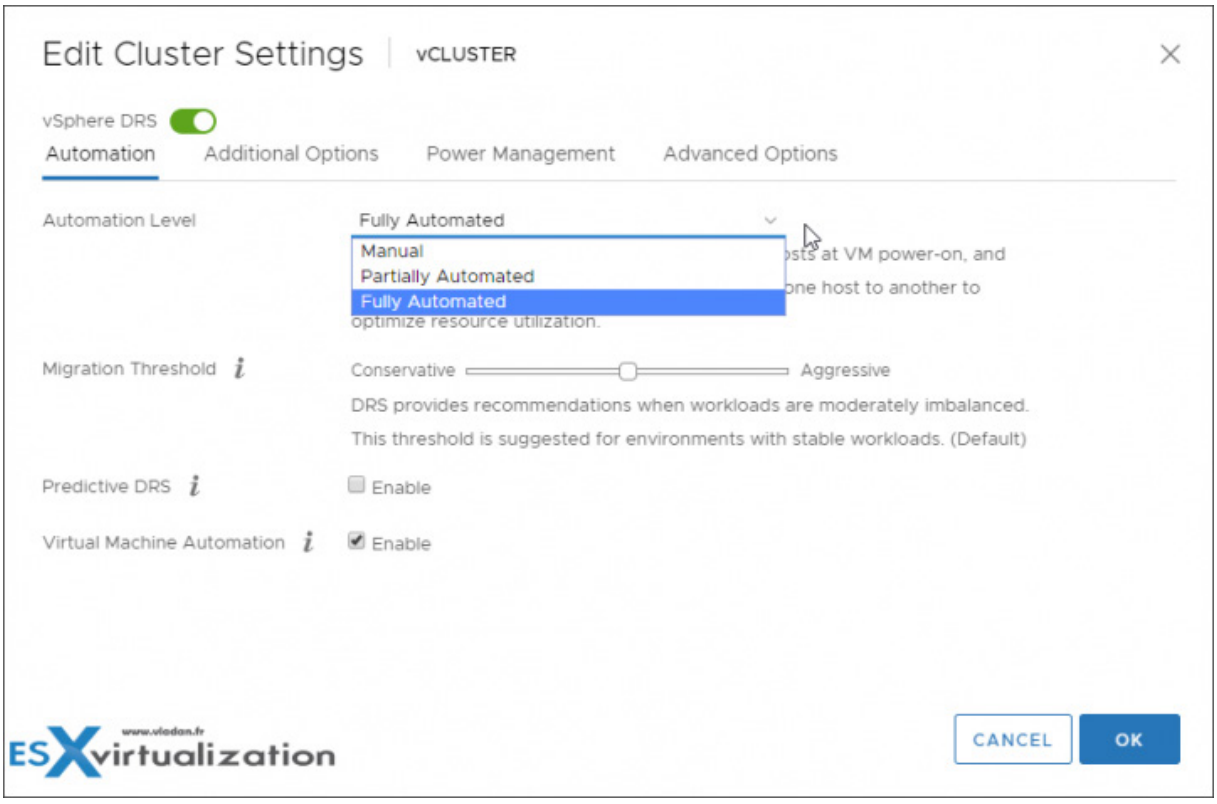
Based on your plan for the resources and networking architecture of the cluster, use the vSphere Web Client to add hosts to the cluster. Browse to the cluster and enable vSphere HA. Click the **Configure tab >** Select vSphere Availability and click Edit > Select Turn ON vSphere HA.

Select Turn ON Proactive HA to allow proactive migrations of VMs from hosts on which a provider has notified a health degradation. Under Failures and Responses, select Enable Host Monitoring.

With Host Monitoring enabled, hosts in the cluster can exchange network heartbeats, and vSphere HA can take action when it detects failures.

Host Monitoring is required for the vSphere Fault Tolerance recovery process to work properly.

If you're using HA with DRS, you're basically getting automatic failover with load balancing. You get your cluster more balanced after HA moved VMs to a different host.



After you have configured your cluster, you can scale it out by adding more hosts.

You must specify the network configuration for the new hosts in the cluster. If during the initial configuration of the cluster, you have postponed configuring the host networking, no configuration, as for the existing hosts, is applied to the newly added hosts.

Objective 7.7 - Perform different types of migrations

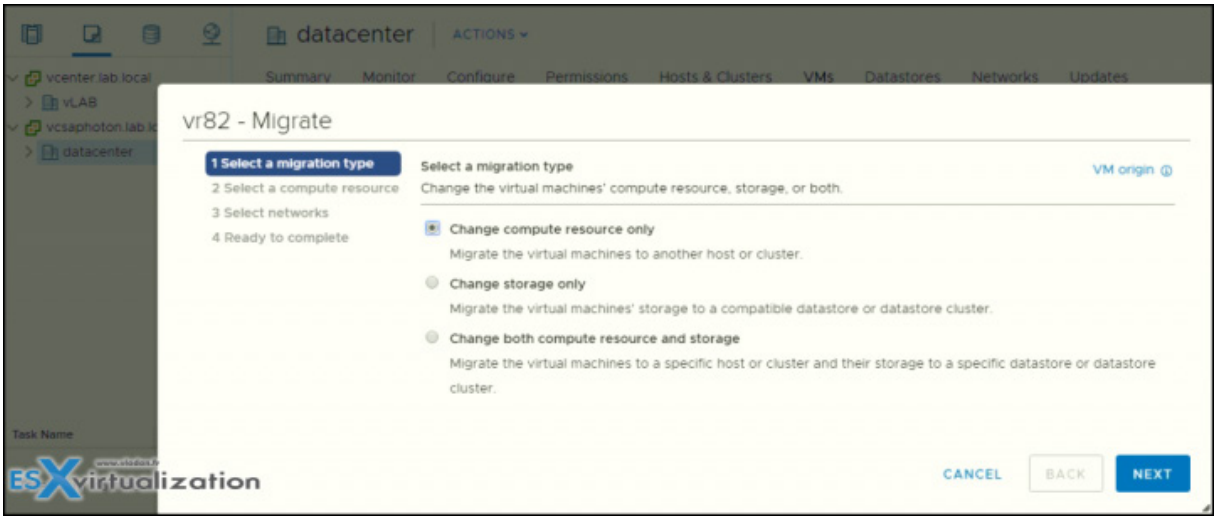
Depending on the power state of the virtual machine that you migrate, migration can be cold or hot. Hot migration is usually known as vMotion where cold migration.... is simply moving the VM during its power OFF state.

Cold Migration - Moving a powered off or suspended virtual machine to a new host. Additionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one virtual switch to another, and from one data center to another. You can perform cold migration manually or you can schedule a task.

Hot Migration - Moving a powered on virtual machine to a new host. Optionally, you can also move the virtual machine disks or folder to a different datastore. Hot migration is also called live migration or vMotion. With vMotion, you migrate the virtual machine without any interruption in its availability.

Depending on the virtual machine resource type, you can perform three types of migration:

1. **Change compute resource only** - Moving a virtual machine, but not its storage, to another compute resource, such as a host, cluster, resource pool, or vApp. You can move the virtual machine to another compute resource by using cold or hot migration. If you change the compute resource of a powered on virtual machine, you use vMotion.
2. **Change storage only** - Moving a virtual machine and its storage, including virtual disks, configuration files, or a combination of these, to a new datastore on the same host. You can change the datastore of a virtual machine by using cold or hot migration. If you move a powered on virtual machine and its storage to a new datastore, you use Storage vMotion.
3. **Change both compute resource and storage** - Moving a virtual machine to another host and at the same time, moving its disk or virtual machine folder to another datastore. You can change the host and datastore simultaneously by using cold or hot migration.



In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between the following types of objects.

Migrate to another virtual switch - Moving the network of a virtual machine to a virtual switch of a different type. You can migrate virtual machines without reconfiguring the physical and virtual network. By using cold or hot migration, you can move the virtual machine from a standard to a standard or distributed switch, and from a distributed switch to another distributed switch. When you move a virtual machine network between distributed switches, the network configuration and policies that are associated with the network adapters of the virtual machine are transferred to the target switch.

Migrate to another data center - Moving a virtual machine to a different data center. You can change the data center of a virtual machine by using cold or hot migration. For networking in the target data center, you can select a dedicated port group on a distributed switch.

Migrate to another vCenter Server system - Moving a virtual machine to a vCenter Server instance that is connected to the source vCenter Server instance through vCenter Enhanced Linked Mode. You can also move virtual machines between vCenter Server instances that are located across a long distance from each other.

Note: If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, the compatibility check fails, and you cannot proceed further with the migration. If the virtual machine that you migrate does not have an NVDIMM device, but has virtual PMem hard disks, the destination host or cluster must have available PMem resources so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks will use the storage policy and datastore selected for the configuration files of the virtual machine.

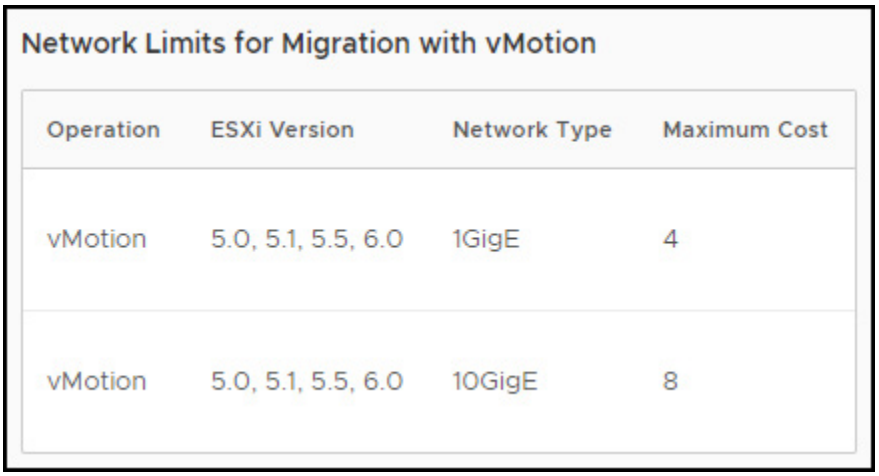
Limits on Simultaneous Migrations

vCenter Server places limits on the number of simultaneous virtual machine migration and provisioning operations that can occur on each host, network, and datastore.

Each operation, such as migration with vMotion or cloning a virtual machine, is assigned a resource cost. Each host, datastore, or network resource, has a maximum cost that it can support at any one time. Any new migration or provisioning operation that causes a resource to exceed its maximum cost does not proceed immediately but is queued until other operations complete and release resources. Each of the network, datastore, and host limits must be satisfied for the operation to proceed.

vMotion without shared storage, and migrating virtual machines to a different host and datastore simultaneously, are a combination of vMotion and Storage vMotion. This migration inherits the network, host, and datastore costs associated with those operations. vMotion without shared storage is equivalent to a Storage vMotion with a network cost of 1.

Network Limits - Network limits apply only to migrations with vMotion. Network limits depend on the version of ESXi and the network type. All migrations with vMotion have a network resource cost of 1.



Network Limits for Migration with vMotion

Operation	ESXi Version	Network Type	Maximum Cost
vMotion	5.0, 5.1, 5.5, 6.0	1GigE	4
vMotion	5.0, 5.1, 5.5, 6.0	10GigE	8

Datastore Limits - Datastore limits apply to migrations with vMotion and with Storage vMotion. A migration with vMotion has a resource cost of 1 against the shared virtual machine's datastore. A migration with Storage vMotion has a resource cost of 1 against the source datastore and 1 against the destination datastore.

vMotion:

- Maximum Cost Per Datastore: 128
- Datastore Resource Cost: 1

Storage vMotion:

- Maximum Cost Per Datastore: 128
- Datastore Resource Cost: 16

Host Limits - Host limits apply to migrations with vMotion, Storage vMotion, and other provisioning operations such as cloning, deployment, and cold migration. All hosts have a maximum cost per host of 8. For example, on an ESXi 5.0 host, you can perform 2 Storage vMotion operations, or 1 Storage vMotion and 4 vMotion operations.

vMotion:

- Derived Limit Per Host: 8
- Host Resource Cost: 1

Storage vMotion:

- Derived Limit Per Host: 2
- Host Resource Cost: 4

vMotion Without Shared Storage

- Derived Limit Per Host: 2
- Host Resource Cost: 4

Other provisioning operations

- Derived Limit Per Host: 8
- Host Resource Cost: 1

Objective 7.8 - Manage resources of a vSphere environment

The best option for studying this objective is to read the *vSphere Resource Management PDF*. It is a 150 pages PDF which explains in detail all which you need to know for this chapter.

As you might imagine, we'll cover a few topics from this PDF, but you'll definitely want to refer to the PDF as our space for individual blog post is fairly limited.

Resource management is the allocation of resources from resource providers to resource consumers.

Here are few definitions:

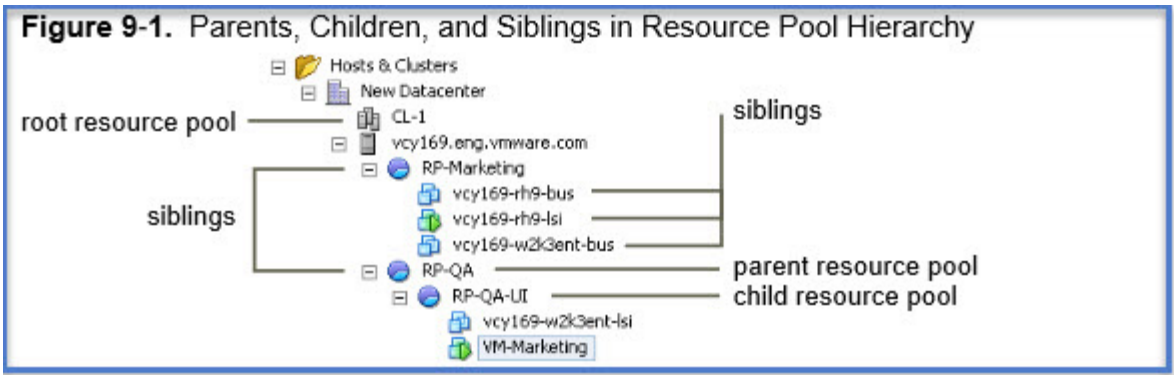
Resource Providers - Hosts and clusters, including datastore clusters, are providers of physical resources. For hosts, available resources are the host's hardware specification, minus the resources used by the virtualization software.

Resource Consumers - Virtual machines are resource consumers. The default resource settings assigned during creation work well for most machines. You can later edit the virtual machine settings to allocate a share-based percentage of the total CPU, memory, and storage I/O of the resource provider or a guaranteed reservation of CPU and memory. When you power on that virtual machine, the server checks whether enough unreserved resources are available and allows power on only if there are enough resources. This process is called admission control.

Resource pools - A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources.

Note: You should definitely check the individual chapter VCP6.7-DCV Objective 1.7 – Describe and identify resource pools and use cases.

We also talk about reservations, shares, and limits. Resource Pools should be used when you need to limit or to guarantee resources to VMs. By having a resource pool, you don't have to guarantee the resources to VMs individually, but only at the pool level.



When you power on a virtual machine in a resource pool or try to create a child resource pool, the system performs additional admission control to ensure the resource pool's restrictions are not violated.

Before you power on a virtual machine or create a resource pool, ensure that sufficient resources are available using the Resource Reservation tab in the vSphere Web Client. The Available Reservation value for CPU and memory displays resources that are unreserved.

How available CPU and memory resources are computed and whether actions are performed depends on the Reservation Type, Fixed or Expandable.

The system does not allow you to violate preconfigured Reservation or Limit settings. Each time you reconfigure a resource pool or power on a virtual machine.

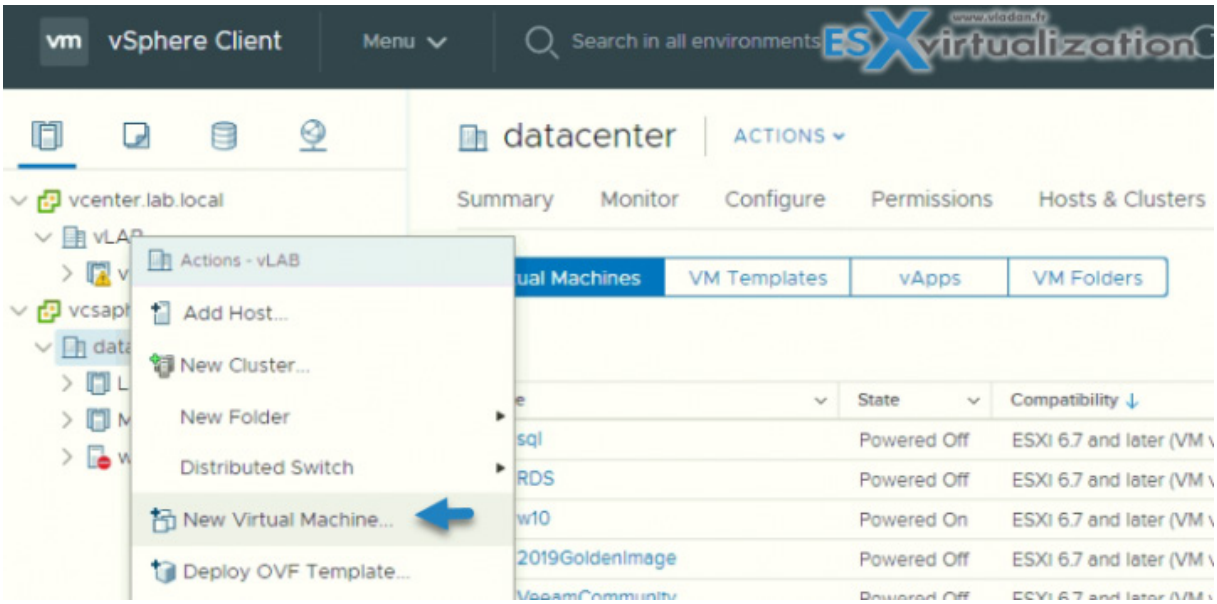
The chapter should include more information, I'm well aware. Honestly, your best bet is to check out the PDF. In addition, you'll get further information about vSphere Distributed Resource Scheduler (DRS) problems for categories: cluster, host, and virtual machine problems.

Objective 7.9 - Create and manage VMs using different methods

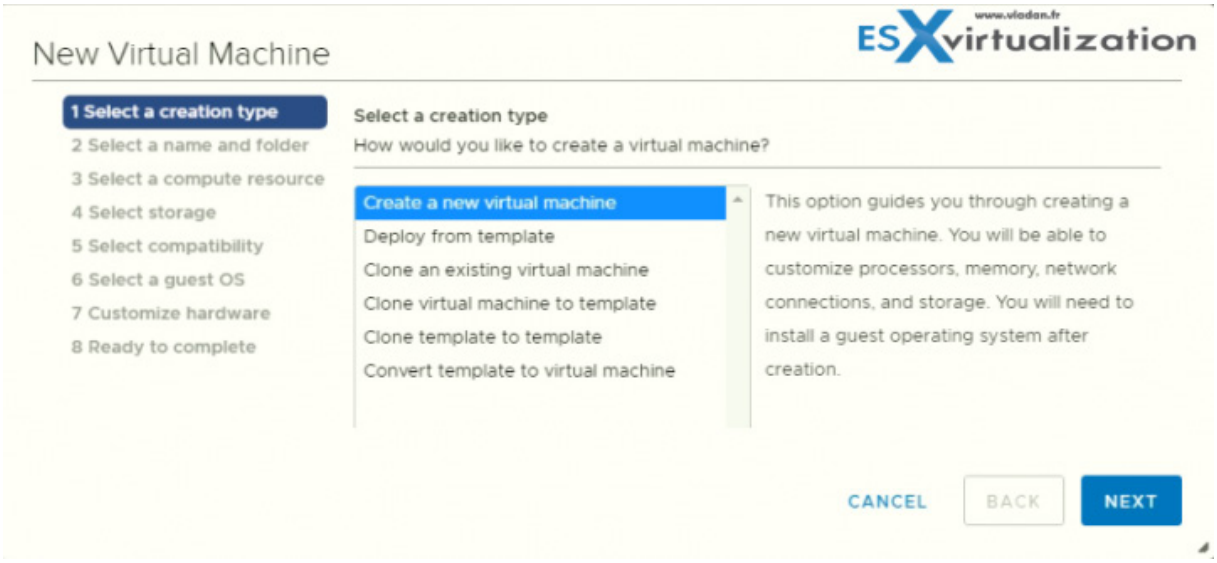
Open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine. If you right-click any part of the inventory, you can start the new VM wizard.

You can create a single virtual machine if no virtual machines in your environment meet your needs, for example, of a particular operating system or hardware configuration. When you create a virtual machine without a template or clone, you can configure the virtual hardware, including processors, hard disks, and memory.

During the creation process, a default disk is configured for the virtual machine. You can remove this disk and add a new hard disk, select an existing disk, or add an RDM disk on the Virtual Hardware page of the wizard.



The new VM wizard gives you different options, from which you should choose the way you would like to proceed.



Create a new VM - Create a new VM with the possibility to customize CPUs, memory, network, and storage.

Deploy VM from template - This option guides you through the process of creating a virtual machine from a template. A template is a golden image of a virtual machine that lets you easily create ready-for-use virtual machines. You must have a template to proceed with this option.

Clone a VM - This option guides you through creating a copy of an existing virtual machine.

Clone VM to template - This option guides you through creating a copy of an existing virtual machine and making it a template. A template is a golden image of a virtual machine that allows you to easily create ready-for-use virtual machines.

Clone template to template - Another option which guides you through creating a copy of an existing template.

Convert Template to VM - This option guides you through the process of converting a template into a virtual machine. Converting a template to a virtual machine allows you to update the virtual machine software and settings. After doing this, you can convert the virtual machine back to a template or keep it as a virtual machine if you no longer need to use it as a golden image.

If the template that you convert does not have an NVDIMM device, but has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

You can export virtual machines, virtual appliances, and vApps in Open Virtual Format (OVF) and Open Virtual Appliance (OVA). You can then deploy the OVF or OVA template in the same environment or in a different environment.

You can deploy an OVF or OVA template from a local file system or from a URL. Some of the pages in the Deploy OVF Template wizard only appear if the OVF template that you deploy requires additional customization, contains deployment options or has one or multiple service dependencies.

Make sure to check the VMware PDF called *vSphere Virtual Machine Administration* for further details, particularly for permissions necessary for the VM operations.

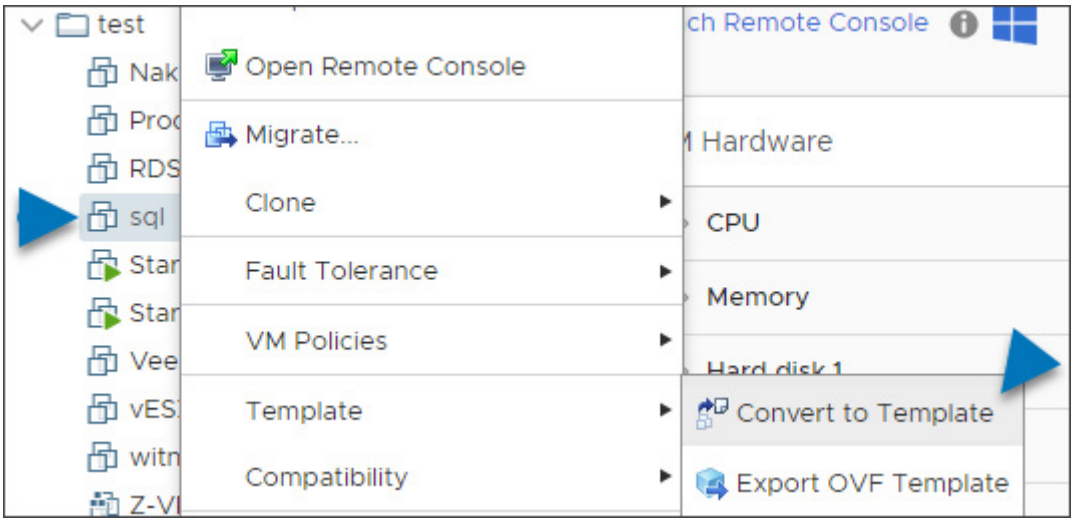
Objective 7.10 - Create and manage templates

Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has virtual hardware, installed software, and other properties that are configured for the template.

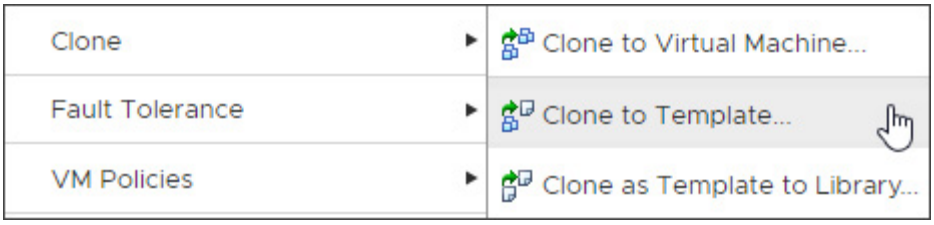
How do you create a template?

Two possibilities:

1. From VM simply do a **Right Click** > **Template** > **Convert to a template**.



1. By Cloning. Simply **Right click a VM** > **Clone** > **Clone to Template**



To Deploy a VM from a Template Prerequisites

You must have the following privileges to deploy a virtual machine from a template:

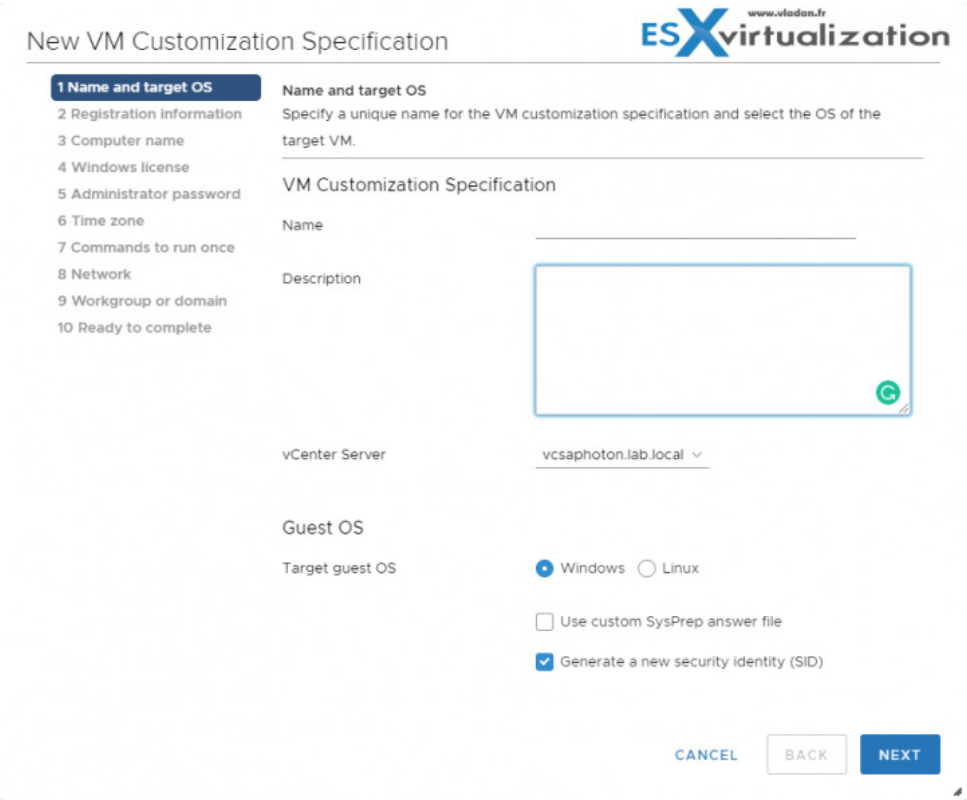
- Virtual machine > Inventory > Create from existing on the data center or virtual machine folder.
- Virtual machine > Configuration > Add a new disk on the data center or virtual machine folder. Required only if you customize the original hardware by adding a new virtual disk.
- Virtual machine > Provisioning > Deploy template on the source template.
- Resource > Assign virtual machine to resource pool on the destination host, cluster, or resource pool.
- Datastore > Allocate space on the destination datastore.
- Network > Assign network on the network to which the virtual machine is assigned. Required only if you customize the original hardware by adding a new network card.
- Virtual machine > Provisioning > Customize on the template or template folder if you are customizing the guest operating system.
- Virtual machine > Provisioning > Read customization specifications on the root vCenter Server if you are customizing the guest operating system.

Note: If the VM that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource.

Using VM Customization specification with Templates and VM cloning

VM customization specification is a workflow wizard allowing you to prepare an answer file which is used during the cloning process. This is what's needed to be done first. You can customize Windows or Linux VMs. Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system.

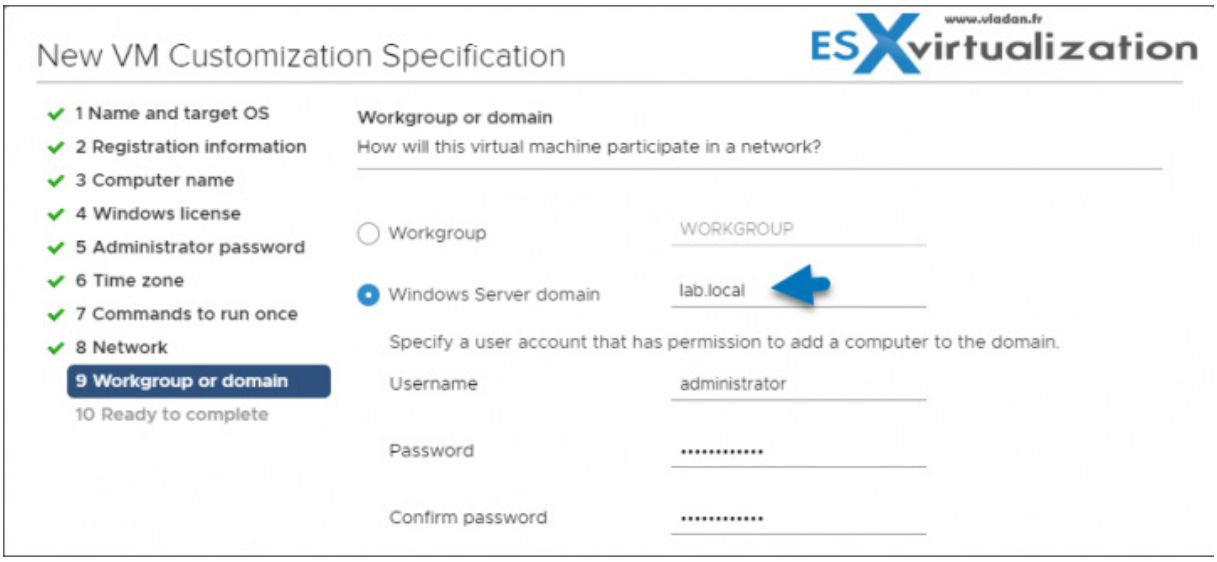
From the **Menu** > go the **Policies and Profiles** and click the **New** button to add a new Customization Specification.



You'll need to specify a computer name or entering a virtual machine name during the clone/deploy wizard. You can also hard code a name you want for the machine to take.

All this workflow is basically a **Virtual machine personalization**, which will be executed after the clone is done.

If you would like to join a Microsoft domain, you can do that as well.



While Cloning Existing VM – VM Customization specification needs to be created before you can use this specification to clone and personalize the Guest OS.

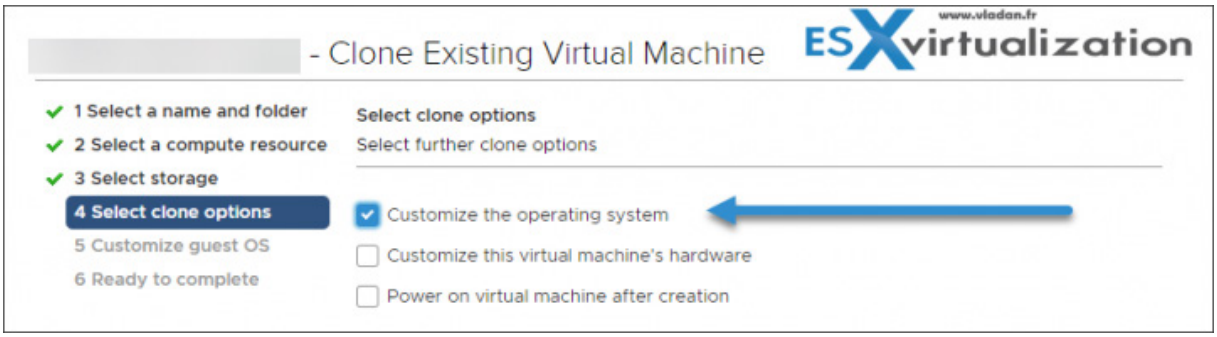
When Personalizing OS of a VM deployed from Template – Template is not a VM. It is a special object which serves as a model, and you can only use this object to deploy new VMs from.

The third option is a customization of an existing VM, which can be any VM (Windows or Linux at this time).

Right-click a VM in the vSphere inventory, and select **Guest OS** > **Customize Guest OS**. The Customize Guest OS wizard opens. Apply a customization specification to the VM.

So How do I clone and Customize a VM?

Select any **VM > Clone to Virtual Machine.** A new wizard will start. You are asked to specify a name for your new VM; pick a datastore where this VM will be stored, and here you have the "Customize the Guest OS" option which you must check in order to launch an overlay window which will bring the list of Guest OS specification.



Content Library Templates - You can store an OVF based template in the content library. It is a convenient way to deploy VMs from OVF template which is accessible through a global vCenter access.

You can use an OVF template from a content library to deploy a virtual machine to a host or a cluster in your vSphere inventory. You can also apply a customization specification to the virtual machine.

Customization Specification for Windows Using a Custom Sysprep Answer File - Yes, it's also possible to have a custom Sysprep answer file. It stores licensing information, and workgroup or domain settings. You can supply a custom Sysprep answer file as
an alternative to specifying many of the settings in the Guest Customization wizard.

It seems that this chapter was shorter than the others, which is good as there are 41 chapters to cover (compared to 31 in VCP6.5-DCV Study guide).

Objective 7.11 - Manage different VMware vCenter Server objects

The inventory is a collection of virtual and physical objects on which you can place permissions, monitor tasks, and events, and set alarms. You can group most inventory objects by using folders to more easily manage them. All inventory objects, except for hosts, can be renamed to represent their purposes.

For example, they can be named after company departments or locations or functions.

vCenter Server monitors and manages the following inventory objects:

Datacenters - Is an aggregation of all the different types of objects used to work in a virtual infrastructure.

Within each data center, there are four separate hierarchies.

1. Virtual machines (and templates)
2. Hosts (and clusters)
3. Networks
4. Datastores

The names for these objects must be unique within a data center. You cannot have two datastores with the same name within a single data center, but you can have two datastores with the same name in two different data centers.

Clusters - Are collections of hosts and associated VMs. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit.

If you enable vSphere DRS on a cluster, the resources of the hosts in the cluster are merged to allow resource balancing for the hosts in the cluster. If you enable vSphere HA on a cluster, the resources of the cluster are managed as a pool of capacity to allow rapid recovery from host hardware failures.

Datastores - A datastore is the storage location for virtual machine files. Physical storage resources can come from the local SCSI disk of the ESXi host, the Fiber Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays.

Folders - You can use folders to **set permissions** across objects, to **set alarms** across objects, and to organize objects in a meaningful way. A folder can contain other folders, or a group of objects of the same type: data centers, clusters, datastores, networks, virtual machines, templates, or hosts.

For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines.

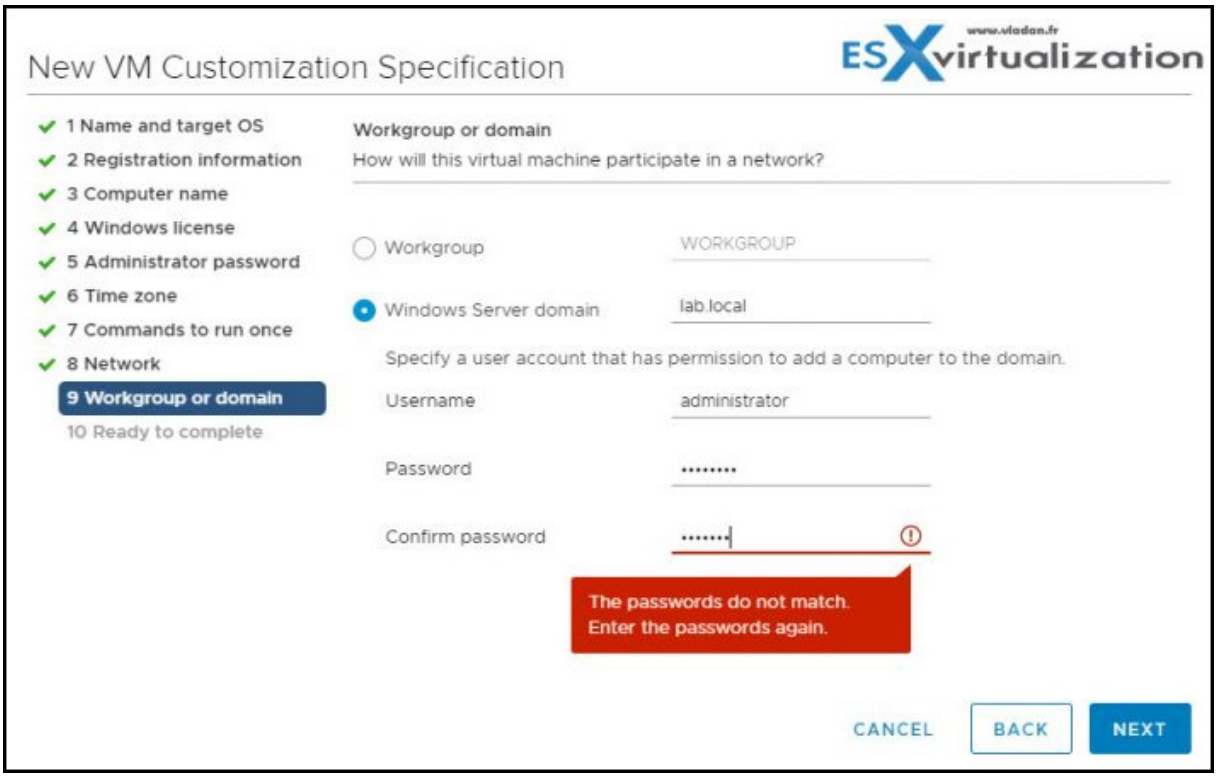
Hosts - Servers which run ESXi software. All VMs run on physical hosts or clusters.

Networks - A set of virtual network interface cards (virtual NICs), distributed switches or vSphere Distributed Switches, and port groups or distributed port groups that connect virtual machines to each other or to the physical network outside of the virtual data center.

All VMs that connect to the same port group belong to the same network in the virtual environment, even if they are on different physical servers.

Resource Pools - Are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines run in and draw their resources from resource pools. You can create multiple resource pools as direct children of a standalone host or cluster and then delegate control over each resource pool to other individuals or organizations.

Templates - A template is a master copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed. They can be customized during deployment to ensure that the new virtual machine has a unique name and network settings.



Virtual Machines - virtualized computer environments in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same managed host machine concurrently.

vApps - vSphere vApp is a format for packaging and managing applications. A vApp can contain multiple virtual machines.

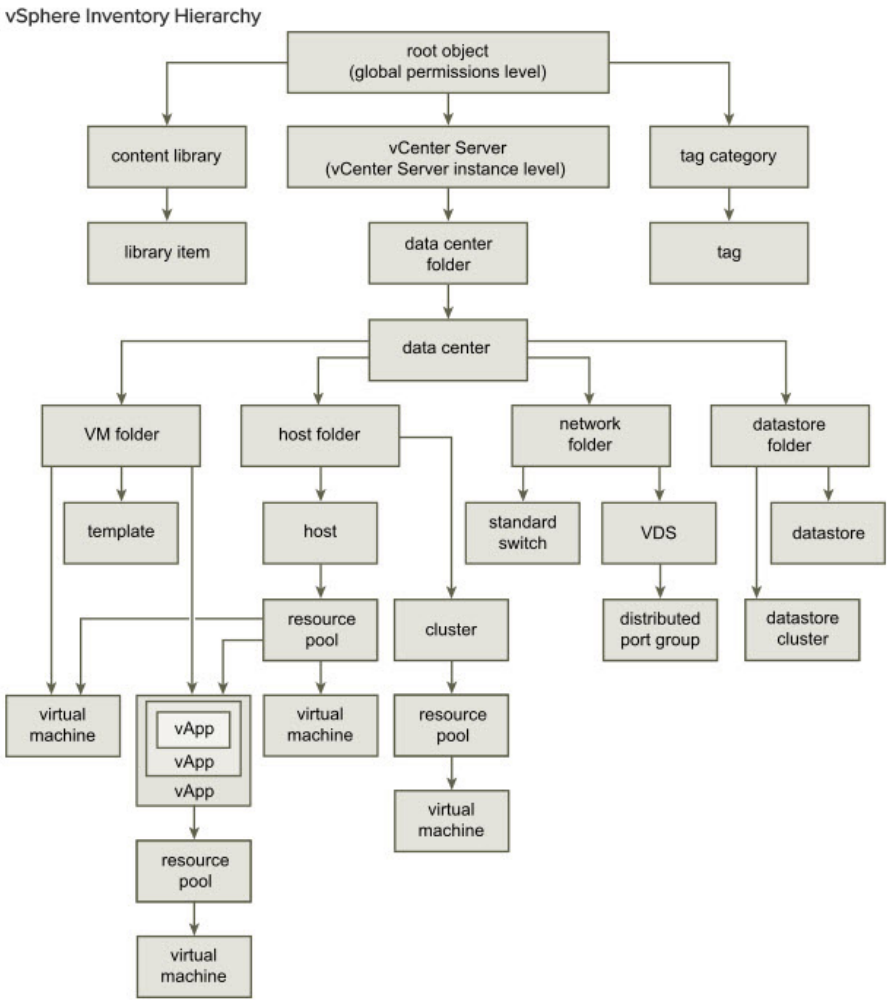
Objective 7.12 - Setup permissions on datastores, clusters, vCenter, and hosts

Each object in the vCenter Server object hierarchy has associated permissions. Each permission specifies for one group or user which privileges that group or user has on the object.

Privileges are fine-grained access controls. You can group those privileges into roles, which you can then map to users or groups.

The permission model for vCenter Server systems basically allows you to assign permissions to objects in the object hierarchy. Each permission gives one user or group a set of privileges, that is, a role for a selected object.

For example, you can select a virtual machine and select Add Permission to assign a role to a group of users in the domain that you select. That role gives those users the corresponding privileges on the VM.



After assigning permission to an object, on the same page you can check the box to propagate permissions down the object hierarchy. You have to set the propagation for each permission.

Permissions defined for a child object **always override** the permissions that are propagated from parent objects.

Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent data center. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously.

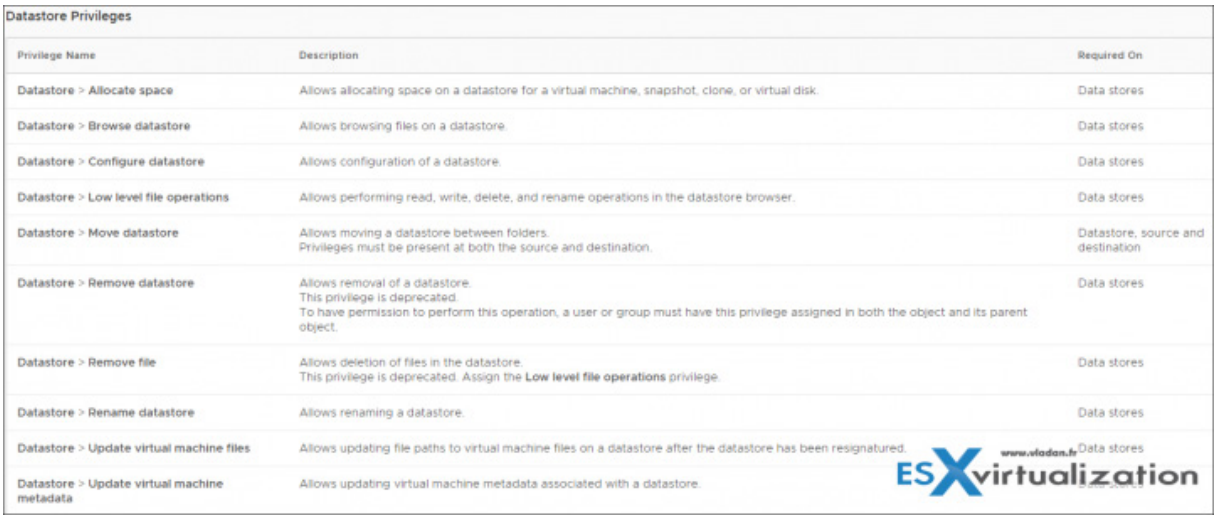
Differences between permissions, privileges, users and groups and roles.

- **Permissions** – each object in the vCenter hierarchy has associated permissions. Each permission
- **Privileges** – access controls to the resource. You group privileges into roles, which are mapped to users or groups.
- **Users and groups** – Only users authenticated through Single Sign-ON (SSO) can be given certain privileges. Users must be defined within the SSO or users from external identity sources such as Microsoft AD.

- **Roles** – what is a role? A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc. are predefined roles. You can clone them or change them (except Administrator).

When you assign permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission, though propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

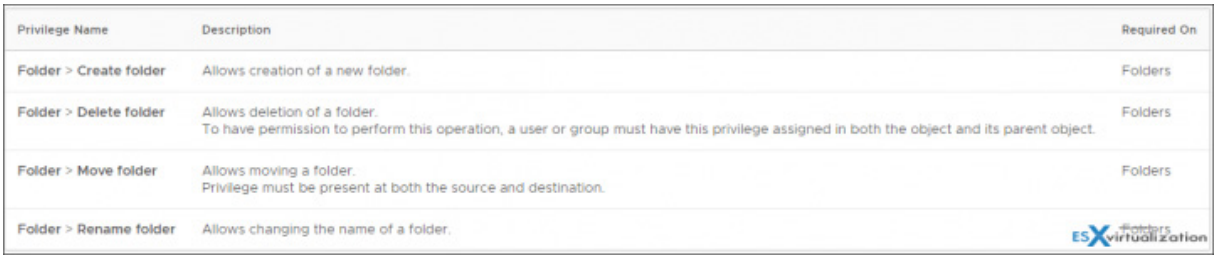
Datastore Privileges - Datastore privileges control the ability to **browse, manage, and allocate space** on datastores. You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.



Datastore Privileges

Privilege Name	Description	Required On
Datastore > Allocate space	Allows allocating space on a datastore for a virtual machine, snapshot, clone, or virtual disk.	Data stores
Datastore > Browse datastore	Allows browsing files on a datastore.	Data stores
Datastore > Configure datastore	Allows configuration of a datastore.	Data stores
Datastore > Low level file operations	Allows performing read, write, delete, and rename operations in the datastore browser.	Data stores
Datastore > Move datastore	Allows moving a datastore between folders. Privileges must be present at both the source and destination.	Datastore, source and destination
Datastore > Remove datastore	Allows removal of a datastore. This privilege is deprecated. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Data stores
Datastore > Remove file	Allows deletion of files in the datastore. This privilege is deprecated. Assign the **Low level file operations** privilege.	Data stores
Datastore > Rename datastore	Allows renaming a datastore.	Data stores
Datastore > Update virtual machine files	Allows updating file paths to virtual machine files on a datastore after the datastore has been resignatured.	Data stores
Datastore > Update virtual machine metadata	Allows updating virtual machine metadata associated with a datastore.	

Folder Privileges - Folder privileges control the ability to **create and manage folders**. You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required-On column must have the privilege set, either directly or inherited.



Privilege Name	Description	Required On
Folder > Create folder	Allows creation of a new folder.	Folders
Folder > Delete folder	Allows deletion of a folder. To have permission to perform this operation, a user or group must have this privilege assigned in both the object and its parent object.	Folders
Folder > Move folder	Allows moving a folder. Privilege must be present at both the source and destination.	Folders
Folder > Rename folder	Allows changing the name of a folder.	

Add Permission to an Inventory Object - After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same permissions to multiple objects simultaneously by moving the objects into a folder and setting the permissions on the folder.

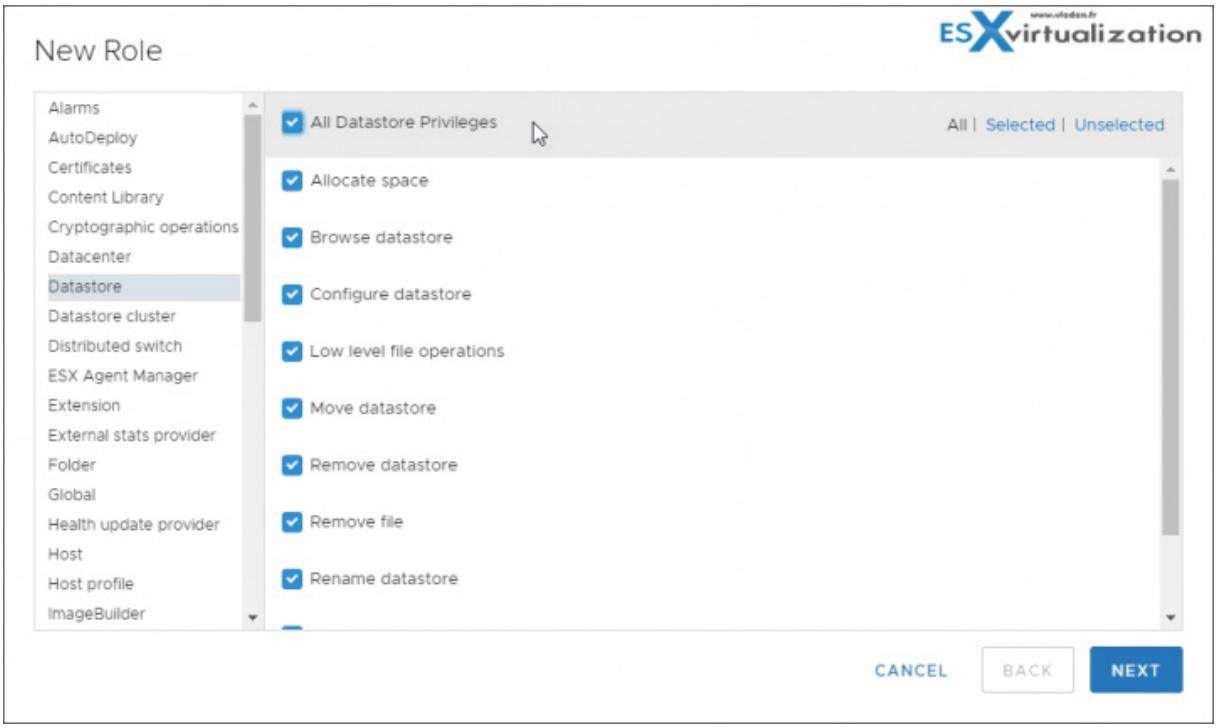
Browse to the object for which you want to assign permissions in the vSphere Client object navigator. Click the **Permissions tab >** Click the Add Permission icon > Select the user or group that will have the privileges defined by the selected role.

From the User drop-down menu, select the domain for the user or group. Type a name in the Search box. The system searches user names and group names > Select the user or group > Select a role from the Role drop-down menu.

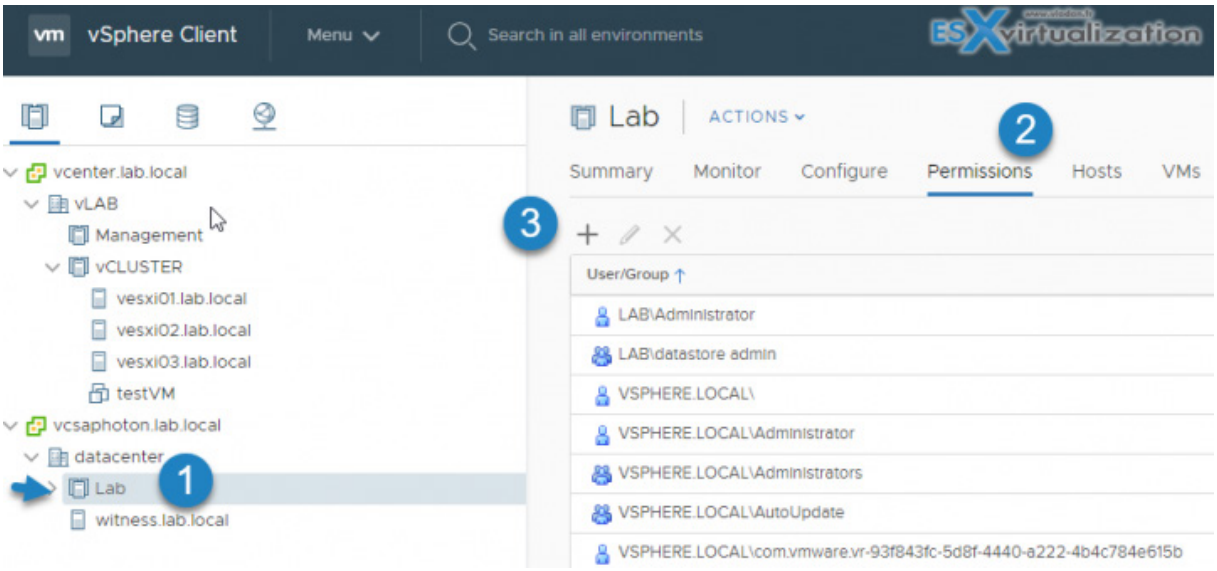
(Optional) To propagate the permissions, select the **Propagate to children** check box. The role is applied to the selected object and propagates to the child objects. Click OK to add the permission.

So here is an example of the whole process. For example, you wish to assign a role to a datastore object.

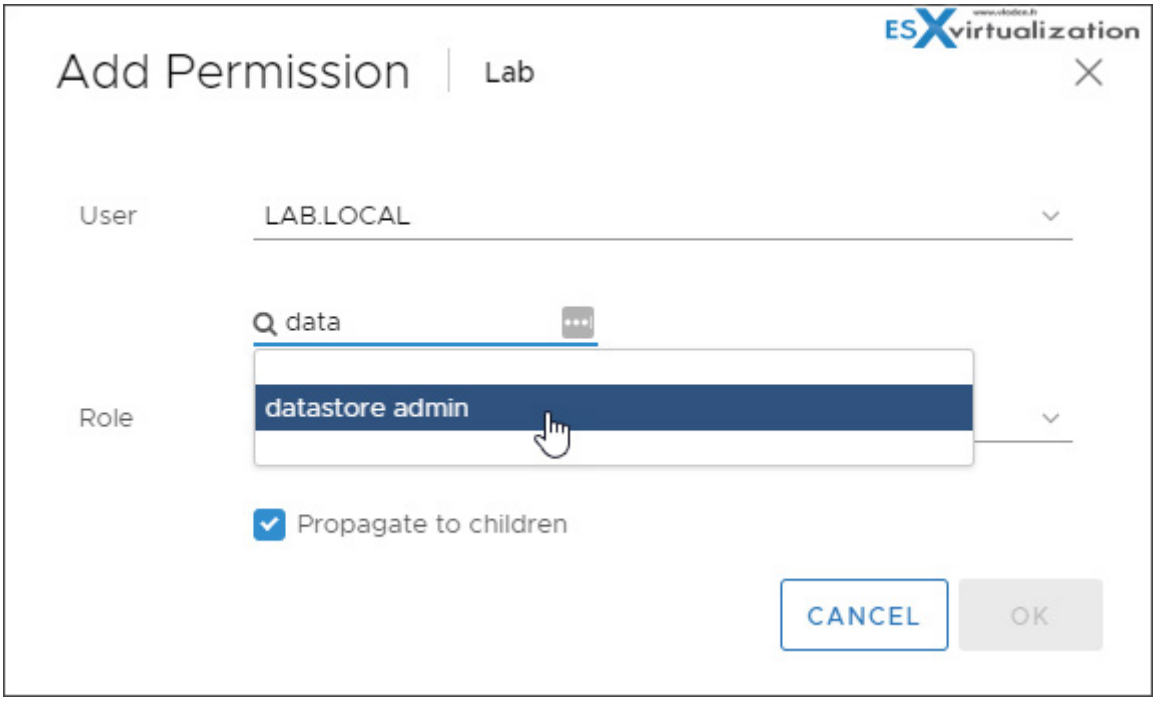
First, go to vSphere Client > **Administration** > **Roles** > **Create a role** > choose from the **categories of privileges** you would like to create a role.



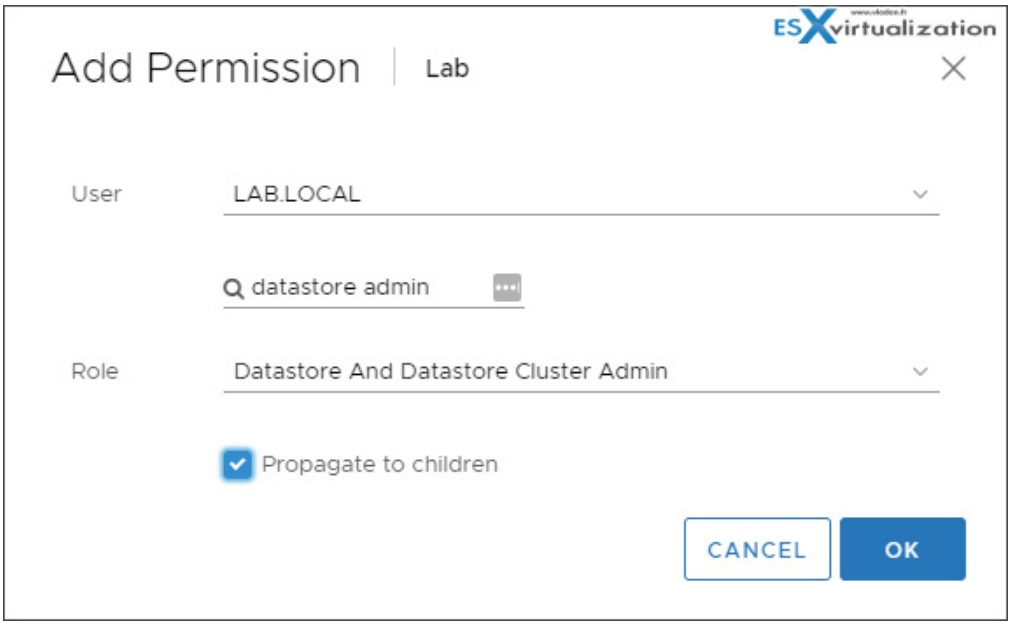
Then select the object where you want to assign permissions by selecting the role.



Chose the domain at the first drop-down menu. Start typing the name of group (in my case, I created a group called datastore admin in my Microsoft active directory (AD) first, and then added some users to this group). It populates automatically.



And then pick the role via the drop-down menu.



Check also VMware documentation here: Required Privileges for Common Tasks

Objective 7.13 - Identify and interpret affinity/anti-affinity rules

DRS in fully automated mode can misplace some VMs, which admin would clearly not like to happen. You can configure the VM placement using affinity and anti-affinity rules. If you create a DRS affinity rule for your cluster, you can specify how vSphere HA applies that rule during a virtual machine failover.

For example, you have a tier 3 application composed of multiple VMs (web frontend, application server, database backend). As is usually the case with tier 3 apps, they "talk" heavily with each other. As such, the backend traffic would be quite significant if you leave to run those VMs on different hosts. The best option is to keep them together on the same host.

The two types of rules for which you can specify vSphere HA failover behavior are the following:

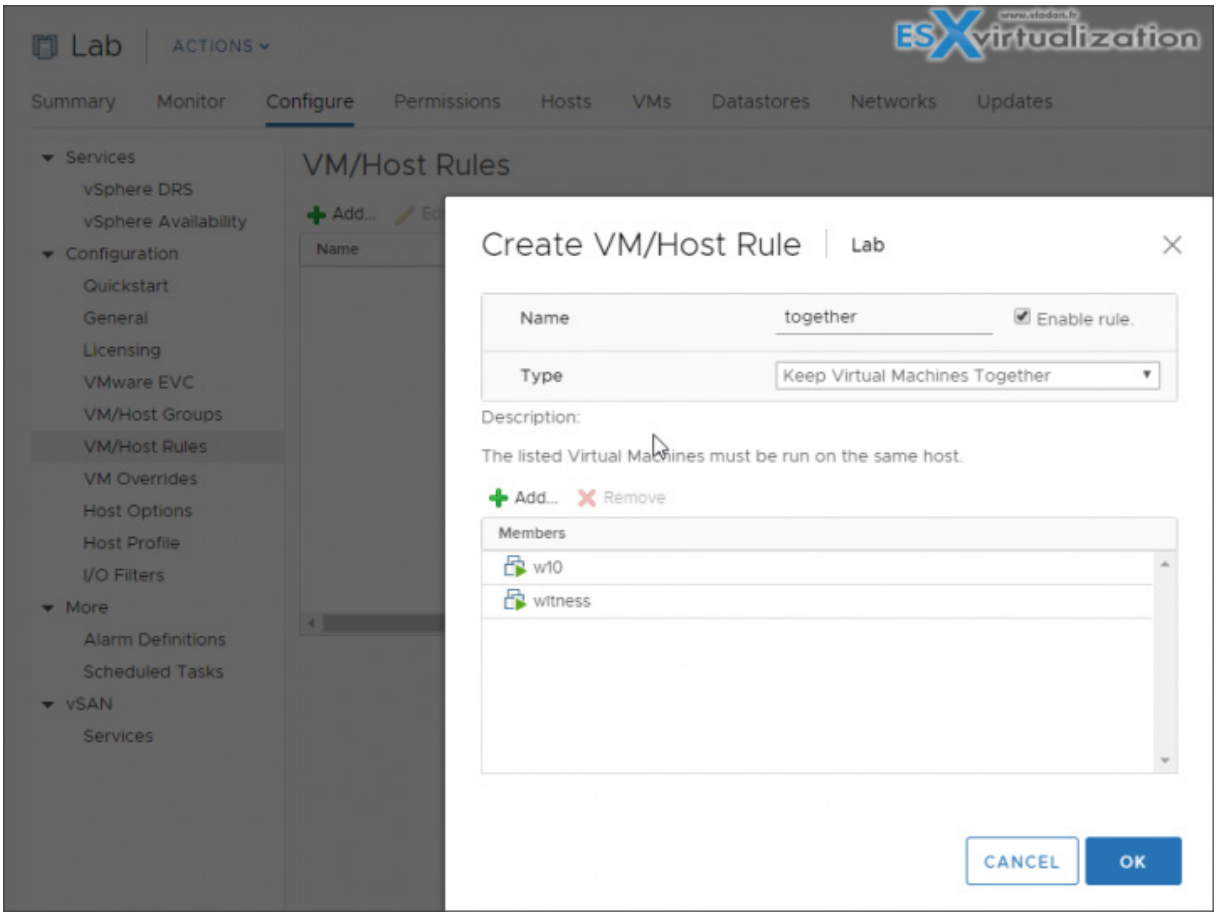
- **VM Affinity/anti-affinity rules** force specified virtual machines to remain together (or apart) during failover actions.
- **VM-Host affinity rules** place specified virtual machines on a particular host or a member of a defined group of hosts during failover actions.

When you edit a DRS affinity rule, you must use vSphere HA advanced options to enforce the desired failover behavior for vSphere HA.

HA must respect VM anti-affinity rules during failover - When the advanced option for VM anti-affinity rules is set, vSphere HA does not fail over a virtual machine if doing so violates a rule. Instead, vSphere HA issues an event reporting if there are insufficient resources to perform the failover.

HA should respect VM to Host affinity rules during failover - vSphere HA attempts to place VMs with this rule on the specified hosts if at all possible.

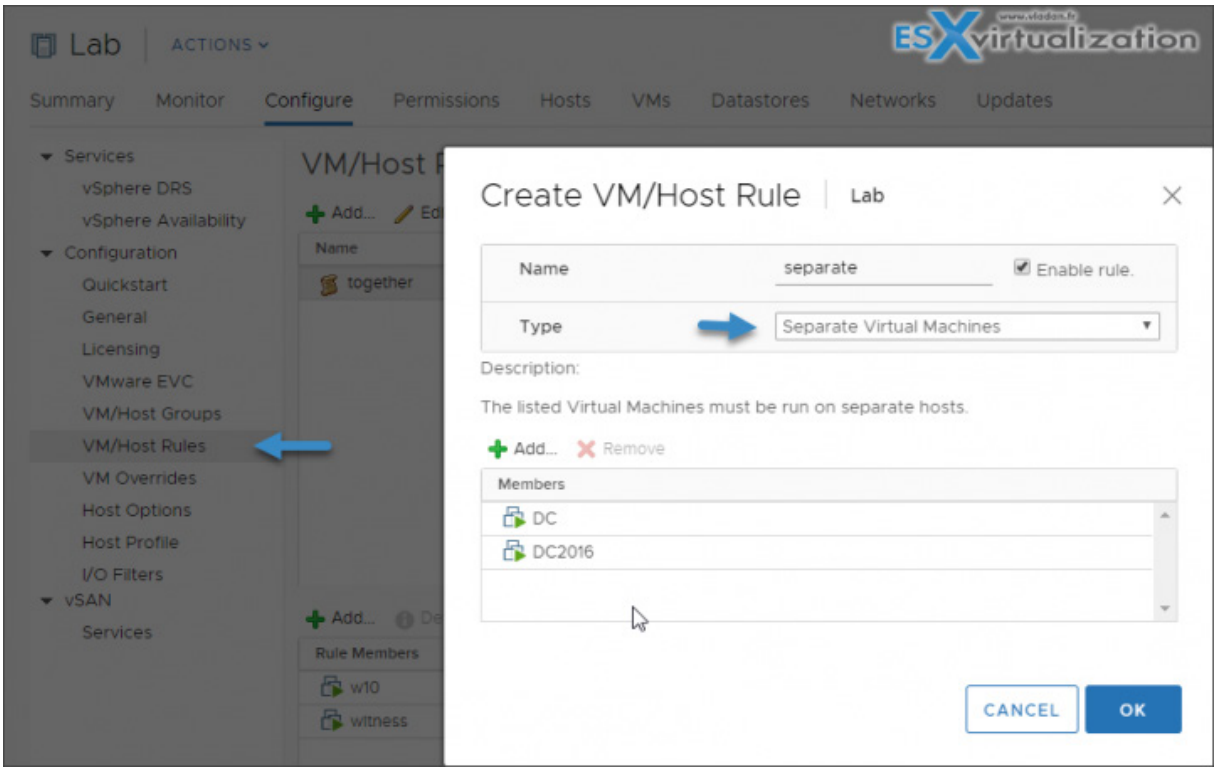
VM-VM Affinity Rule - You can create VM-Host affinity rules to specify whether or not the members of a selected virtual machine DRS group can run on the members of a specific host DRS group. When set to fully automated mode, DRS migrates the VMs to bring them together on the next run of DRS.



A partially automated DRS mode will display the migration recommendation and perform the initial placement when powering on the VM.

VM-VM Anti-Affinity rule - Let's say that we need to keep two VMs apart on different hosts. There you might have an SQL cluster for high availability or perhaps a web server farm that is composed of multiple VMs.

If you have, let's say, two SQL servers on the same physical host and the host has a hardware problem, you will lose VMs at the time HA restarts those VMs on another host. As such, you'll most likely have an interruption of service. It is a good idea to prevent somehow that DRS places those VMs on the same physical host.



A VM-Host affinity rule specifies whether or not the members of a selected virtual machine DRS group can run on the members of a specific host DRS group.

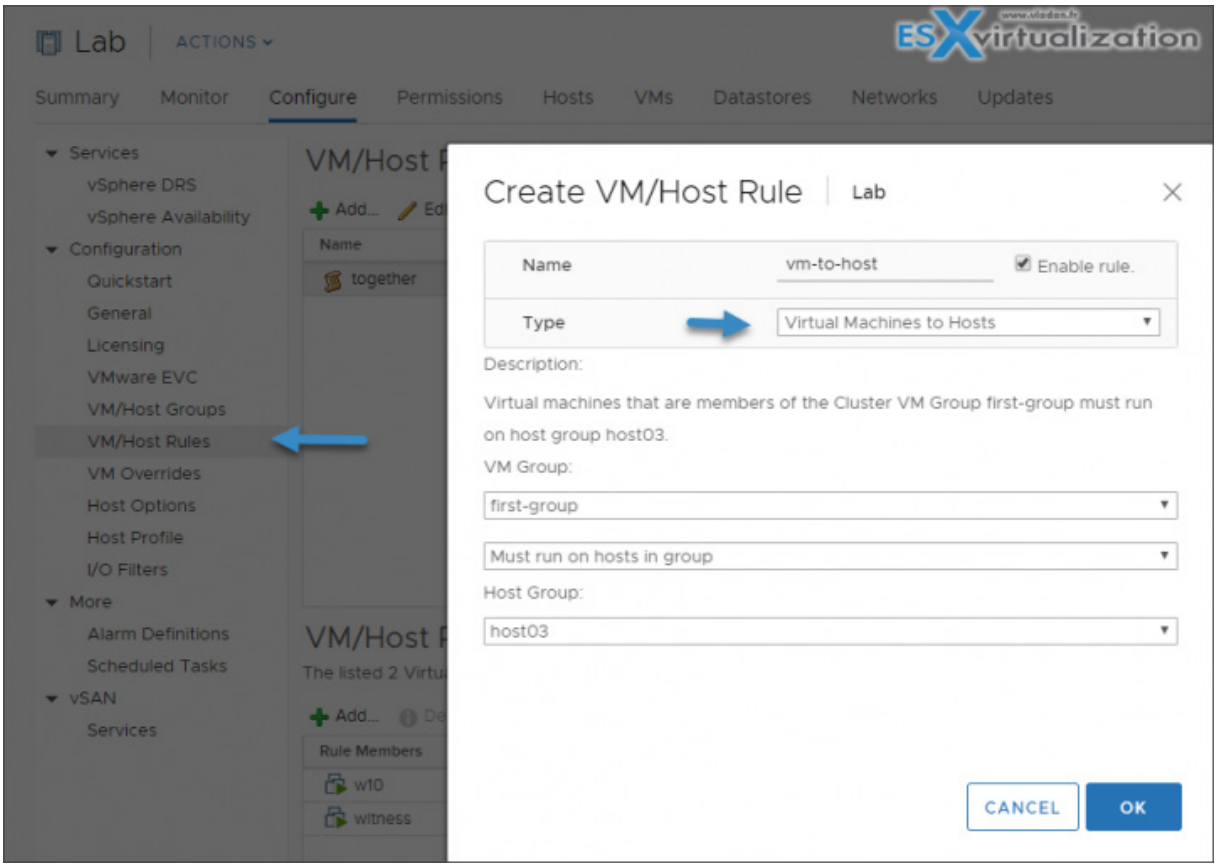
Unlike a VM-VM affinity rule which specifies an affinity (or anti-affinity) between individual virtual machines, a VM-Host affinity rule specifies an affinity relationship between a group of virtual machines and a group of hosts.

There are 'required' rules (designated by "must") and 'preferential' rules (designated by "should".)

A VM-Host affinity rule includes the following components.

- One virtual machine DRS group.
- One host DRS group.
- A designation of whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on").

You use a VM-Host affinity rule to specify an affinity relationship between a group of virtual machines and a group of hosts.



VM-VM Affinity Rule Conflicts - If you create multiple VM-VM affinity rules, they can be in conflict sometimes, depending on the situation.

If two VM-VM affinity rules are in conflict, you cannot enable both. For example, if one rule keeps two virtual machines together and another rule keeps the same two virtual machines apart, you cannot enable both rules.

You must select one of the rules to apply and you have to disable or remove the other, conflicting rule.

When two VM-VM affinity rules conflict, the **older one takes precedence** and the **newer rule is disabled**. DRS only tries to satisfy enabled rules and disabled rules are ignored. DRS gives higher precedence to preventing violations of anti-affinity rules than violations of affinity rules.

Objective 7.14 - Understand use cases for alarms

vCenter Alarms comes pre-configured out of the box, but you can add your own, personalized alarms as well.

VMware documentation teaches us that vCenter Server provides a list of default alarms which monitor the operations of vSphere inventory objects. You must only set up actions for these alarms.

Some alarms are stateless. vCenter Server does not keep data on stateless alarms, does not compute, or display their status. Stateless alarms cannot be acknowledged or reset. Stateless alarms are indicated by an asterisk next to their name.

vCenter has some great alarms built-in which can trigger alerts via email or SNMP to the IT admin. You can create alarms at the data center level, the cluster level, host level or even for a specific VM.

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

In the past, many vSphere admins did not really care about alarms and did not create any additional alarms outside of the predefined vCenter alarms. So it's important to **understand use cases for alarms** and create predefined alarms which fit your environment. Each environment is different. It's worth going through the alarms and learning a bit more about their structure, creation and different monitoring possibilities and conditions.

Alarms and vCenter hierarchy - When creating a new alarm, you should take into account that alarms created at higher levels in the vSphere hierarchy will propagate down to the underlying objects at lower levels. A top-level object in the hierarchy is the vCenter server, then there is a datacenter, ESXi hosts, and so on.

Different types of alarms - a type of alarm created depends on the type of object it has been applied to. If you, let say, create an alarm set to monitor VSAN, it won't apply to VM object. You get the picture.

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

- **Name and description** - Provides an identifying label and description.
- **Targets** - Defines the type of object that is monitored.
- **Alarm Rules** - Defines the event, condition, or state that triggers the alarm and defines the notification severity. It also defines operations that occur in response to triggered alarms.
- **Last modified** - The last modified date and time of the defined alarm.

An alarm definition consists of the following elements in the vSphere Web Client:

- **Name and description** - Provides an identifying label and description.
- **Alarm type** - Defines the type of object that is monitored.
- **Triggers** - Defines the event, condition, or state that triggers the alarm and defines the notification severity.

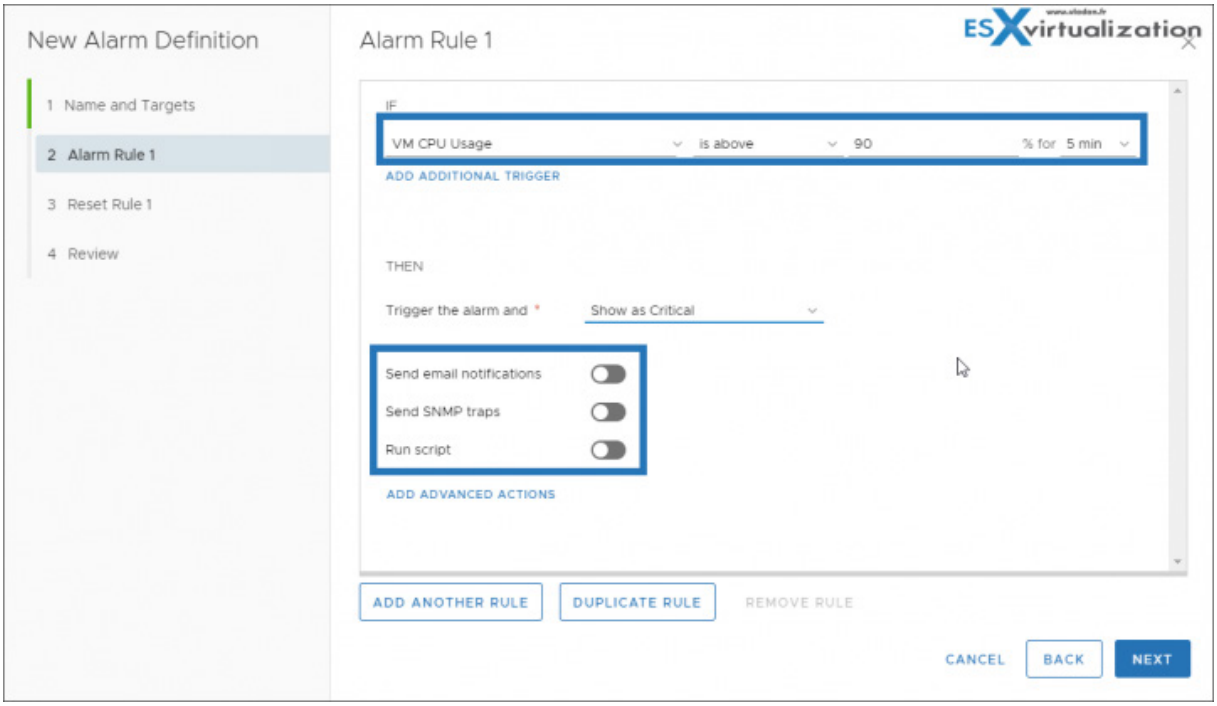
- **Tolerance thresholds (Reporting)** - Provides additional restrictions on condition and state triggers thresholds that must be exceeded before the alarm is triggered. Thresholds are not available in the vSphere Web Client.
- **Actions** - Defines operations that occur in response to triggered alarms. VMware provides sets of predefined actions that are specific to inventory object types.

Alarms have the following severity levels:

- **Normal** – green
- **Warning** – yellow
- **Alert** – red

Example

If you would like to monitor vCPU usage of all virtual machines in a specific host cluster, you can select the cluster in the inventory and add a virtual machine alarm to it. When enabled, that alarm monitors all virtual machines running in the cluster and triggers when any one of them meets the criteria defined in the alarm. To monitor a specific virtual machine in the cluster, but not others, select that virtual machine in the inventory and add an alarm to it. To apply the same alarms to a group of objects, place those objects in a folder and define the alarm on the folder.



Alarm Actions - Alarm actions are operations that occur in response to the trigger. For example, you can have an **email notification** sent to one or more administrators when an alarm is triggered.

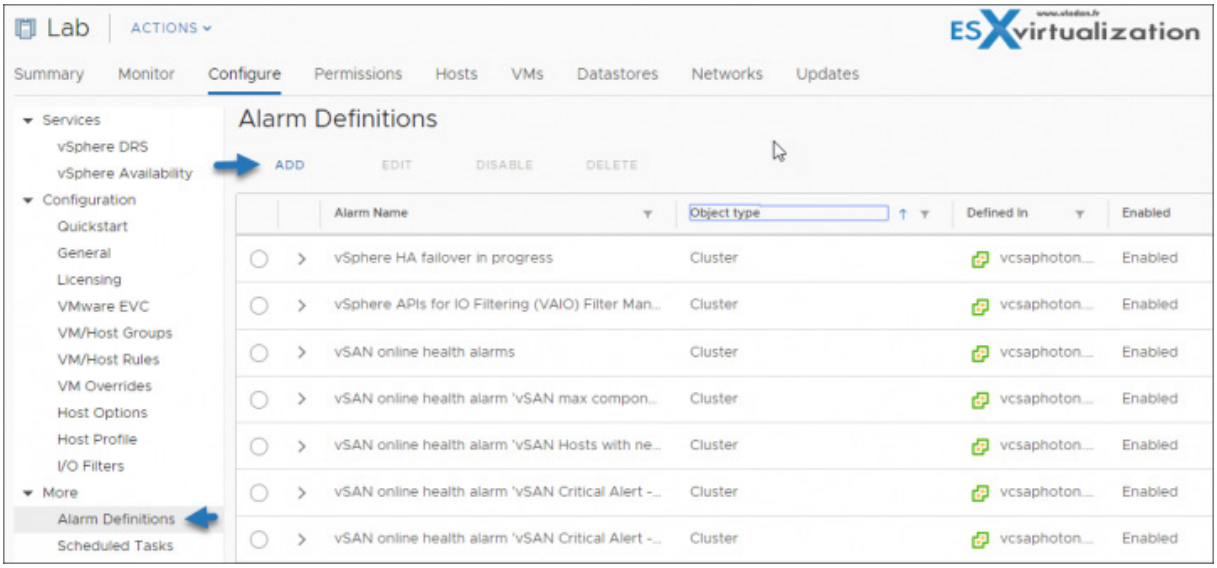
Note: If you defined an alarm in a cluster to monitor virtual machines, you can only enable, disable, or modify that alarm through the cluster. You cannot change the alarm at the individual virtual machine level.

Required Privilege: **Alarms > Create alarm or Alarms > Modify alarm**

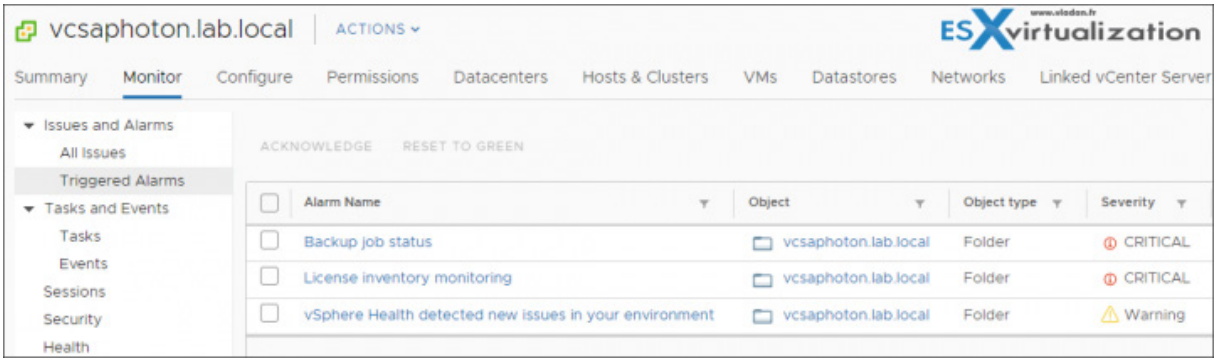
Create or edit alarms in the **Configure** tab. You can monitor inventory objects by setting alarms on them. Setting an alarm involves selecting the type of inventory object to monitor, defining when the alarm triggers, for how long the alarm is on, and defining actions that are performed as a result of the alarm being triggered. You define alarms in the alarm definition wizard.

Select an inventory object, click the **Configure** tab, and click **More** > Click **Alarm Definitions** > Right-click the list of alarms, and select to **add** or **edit** an alarm.

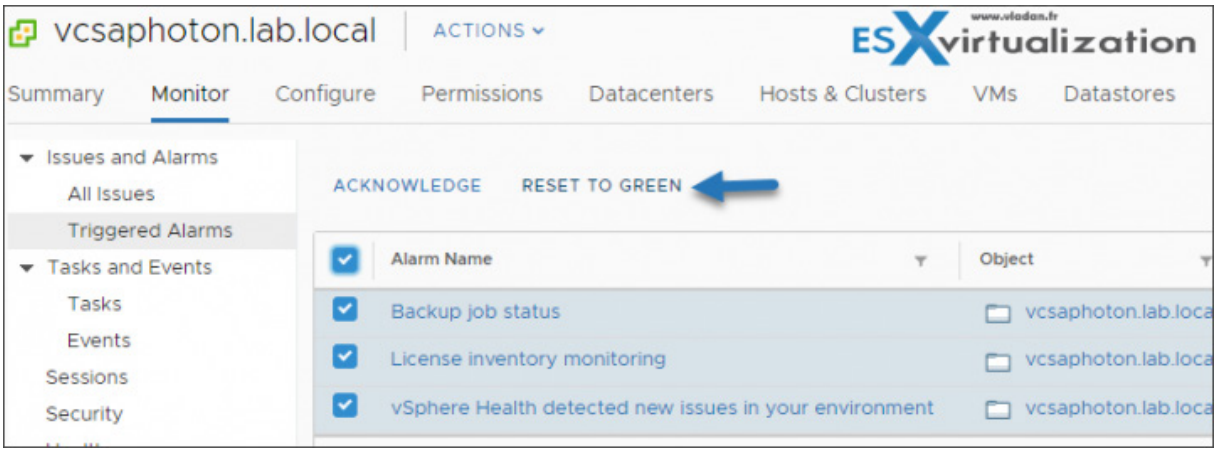
Note: You cannot edit vCenter Server **predefined** alarms.



View Triggered Alarm and Alarms definitions



An alarm triggered by an event might not reset to a normal state if vCenter Server does not retrieve the event that identifies the normal condition. In such cases, reset the alarm manually in the vSphere Client to return it to a normal state.



Final words

As you can see, alarms are useful if you want to closely monitor a group of VMs for a particular situation. You simply group them together (put into a folder) and apply an alarm on the top.

In response to certain events or conditions that occur with an object in vCenter Server, you'll get an alarm. If you create alarms for vCenter Server objects (VMs, ESXi hosts, networks, and datastores), you can get informed when something goes wrong with that object. Alarms can monitor resource consumption or the state of the object and alert you when certain conditions have been met, such as high resource usage or low disk space.

You can also create an alarm to email a notification whenever a new VM is created or have an alarm when some resources are running low on an ESXi host.

Objective 7.15 - Utilize VMware vSphere Update Manager (VUM)

In this post, we'll learn about the latest version of vSphere Update Manager (VUM) present in the vSphere 6.7 U2 recently released by VMware. The tool has been enhanced and improved for usage with HTML5 web client. Previously, not all functions were possible through this client and the use of vSphere web client (Flash) was necessary.

VUM provides centralized, automated patch and version management for ESXi hosts and virtual machines (VMs).

With Update Manager, you can perform the following tasks:

- Upgrade and patch ESXi hosts.

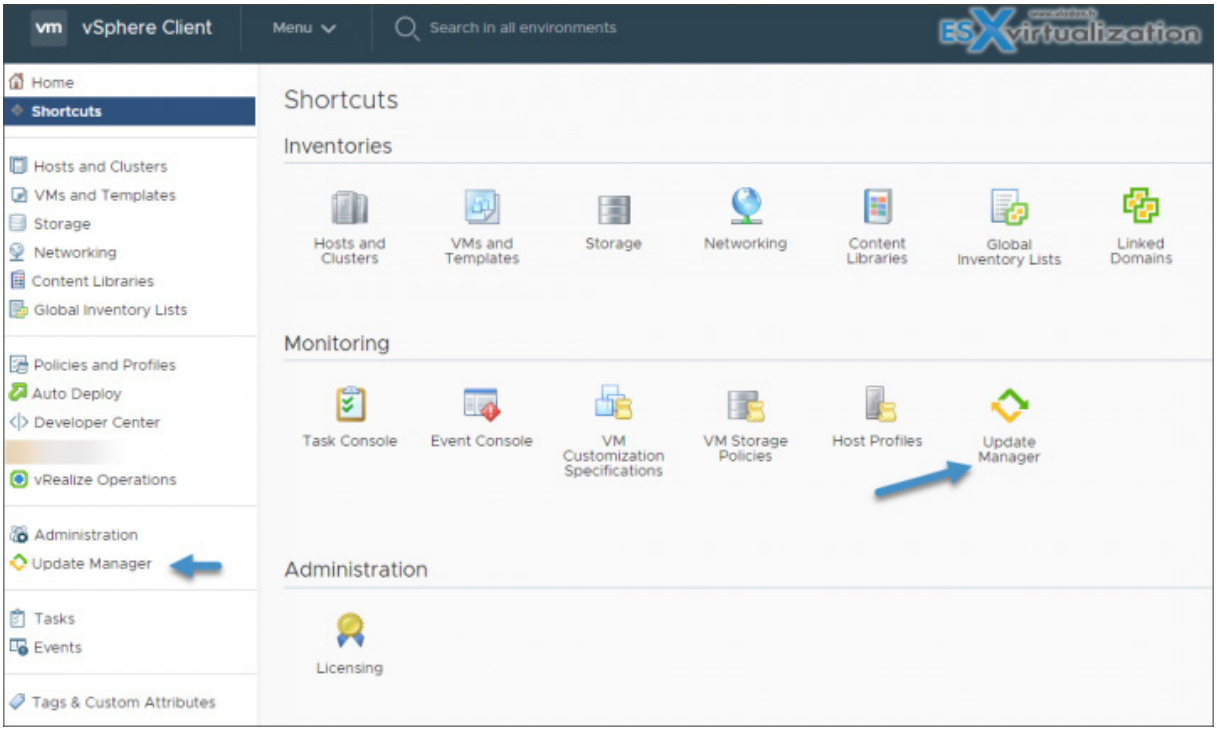
- Install and update third-party software on hosts.
- Upgrade virtual machine hardware and VMware Tools.

You can use Update Manager with either vCenter Server that runs on Windows or with the vCenter Server Appliance. While the VUM on Windows needs to be installed and configured in order to run, VUM on vCenter server appliance (VCSA) comes pre-installed and pre-configured and requires no additional effort from you.

You can install the Update Manager server component either on the same Windows server where the vCenter Server is installed or on a separate machine.

Note: If you would like to see an Install config guide, I'd recommend getting VMware PDF called "*vSphere Update Manager Installation and Administration Guide*". (Update 2).

Update Manager baselines are hosts baselines and virtual machine baselines. To upgrade objects in your vSphere inventory, you can use predefines baselines, system-managed baselines, or custom baselines that you create. When you scan hosts and virtual machines, you evaluate them against baselines and baseline groups to determine their level of compliance.



VUM has two kinds of baselines: (there are more)

System managed baselines - The Update Manager displays system managed baselines that are generated by VSAN. These baselines appear by default when you use VSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. You can see them **only** if you have VSAN in your cluster.

The system managed baselines automatically update their content periodically (needs internet connectivity). You can use the system managed baselines to upgrade your VSAN clusters to recommended critical patches, drivers, updates or latest supported ESXi host version for VSAN.

Predefined baselines - Predefined baselines cannot be edited or deleted—you can only attach or detach them to the respective inventory objects.

Under the Host Baselines tab in Update Manager Admin view, you can see the following predefined baselines:

- **Critical Host Patches (Predefined)** - Checks ESXi hosts for compliance with all critical patches.
- **Non-Critical Host Patches (Predefined)** - Checks ESXi hosts for compliance with all optional patches.

Custom Baselines - Custom baselines are the baselines you create. You can also delete them.

Baseline groups - Baseline groups are assembled from existing baselines. A baseline group might contain one upgrade baseline, and one or more patch and extension baselines, or might contain a combination of multiple patch and extension baselines. A baseline group consists of a set of non-conflicting baselines. Baseline groups allow you to scan and remediate objects against multiple baselines at the same time.

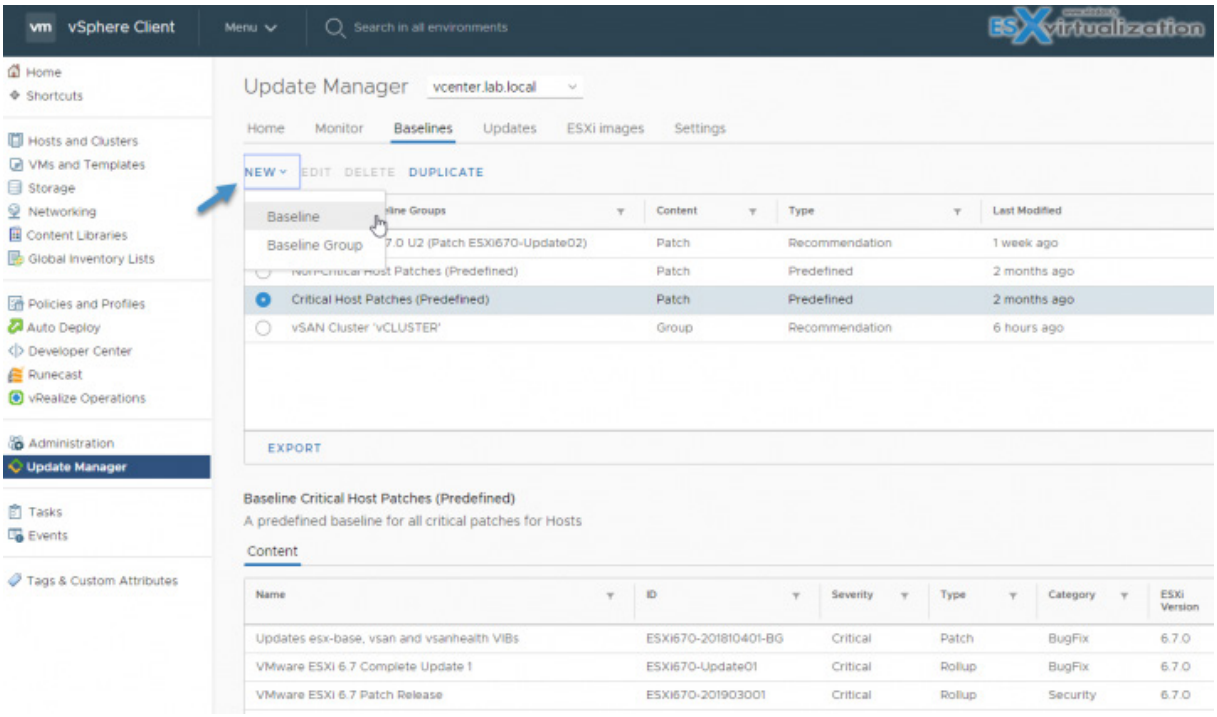
Required Privileges

You must have the **Manage Baseline** privilege. To attach baselines and baseline groups, you must have the **Attach Baseline** privilege. Privileges must be assigned on the vCenter Server system with which Update Manager is registered.

How to create a baseline

You create and manage baselines in the Update Manager Client Administration view. Use the new **Baseline wizard** via the New button.

Menu > Shortcuts > Update Manager > Baselines > New



Note: Update Manager also provides default baselines that you cannot edit or delete. Default baselines are the predefined baselines that contain patches for hosts and updates for VMs. The other type of default baselines is the system managed baselines that you can use to check if your VSAN clusters run the latest supported software.

Patch or Extensions Baselines

It is possible to remediate (update/upgrade) a host against baselines that contains patches or extension.

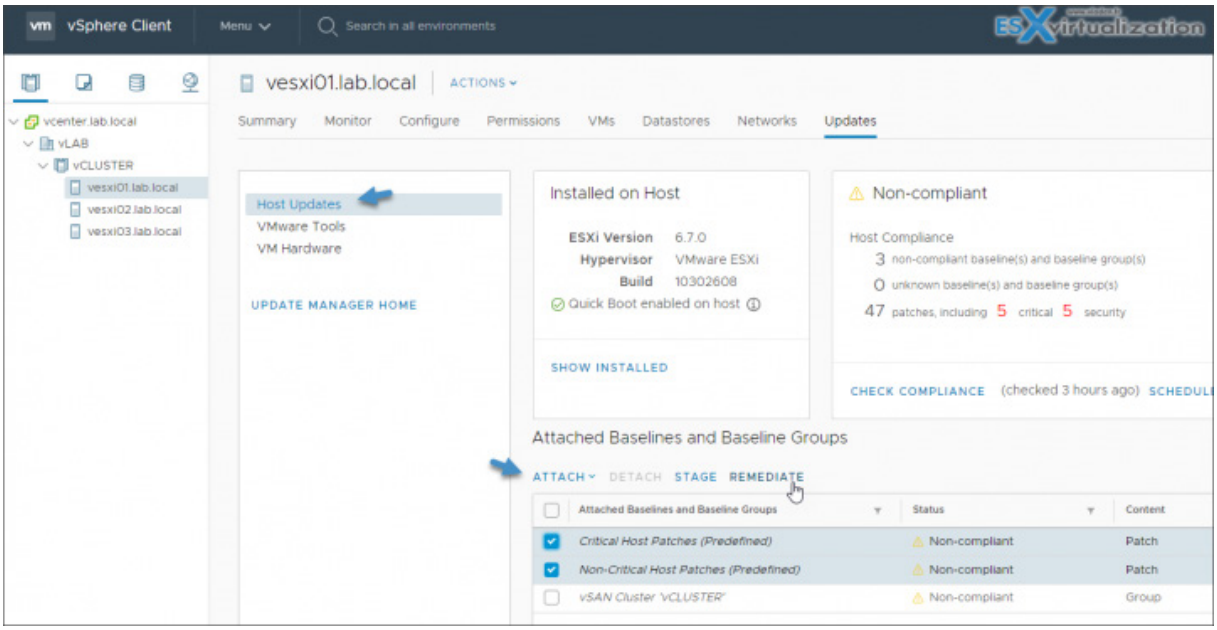
Dynamic patch baselines contain a set of patches which updates automatically according to patch availability and the criteria that you specify. Fixed baselines contain only patches that you select, regardless of new patch downloads.

Extension baselines contain additional software modules for ESXi hosts. This additional software might be VMware software or **also a third-party software**. You can install additional modules by using extension baselines and update the installed modules by using patch baselines.

Attach Baselines and Baseline Groups to Objects

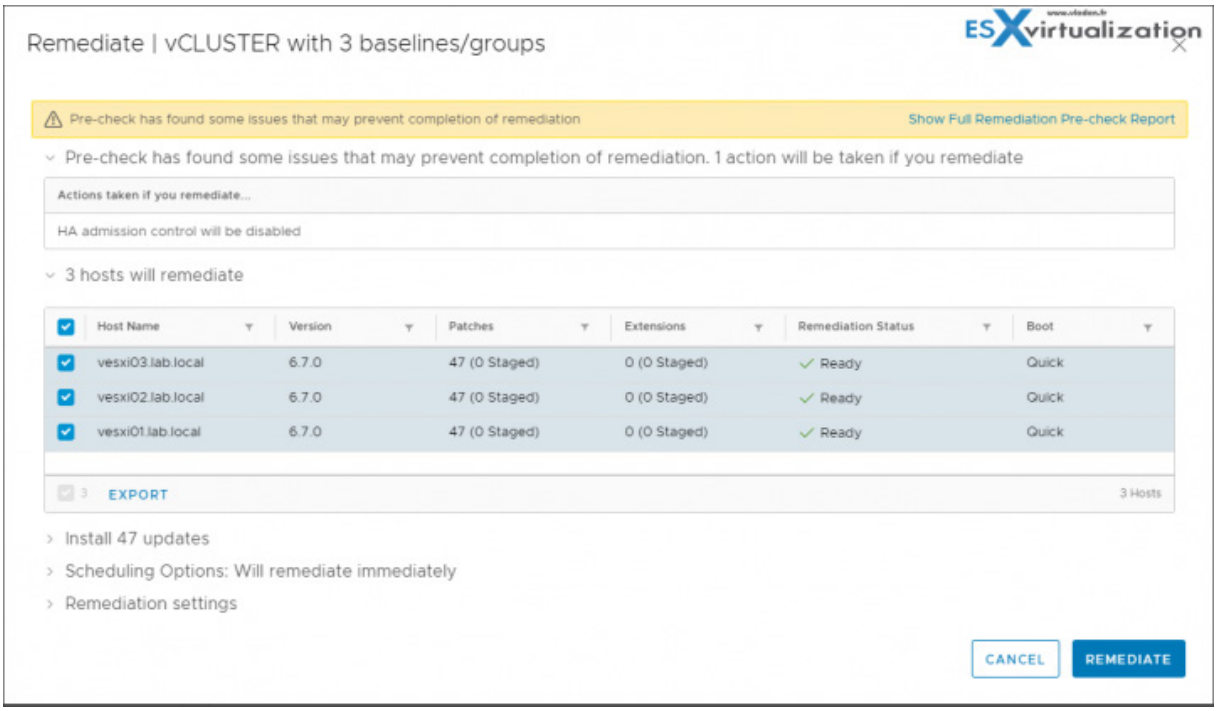
To view compliance information and scan objects in the inventory against baselines and baseline groups, you must first attach the respective baselines and baseline groups to the objects.

Select Host > go to **Updates** > Select **Host updates** > **Attach Baseline or baseline group**.



You can duplicate baselines and baseline groups to edit the copies without risk of compromising the original baseline.

Remediate vSphere Object - You can remediate virtual machines and hosts using either user-initiated remediation or scheduled remediation. To remediate vSphere objects, you need the Remediate to Apply Patches, Extensions, and Upgrades privilege.



And watch the progress...

For ESXi hosts in a cluster, the remediation process is sequential by default. With Update Manager, you can select to run host remediation in parallel. When you remediate a cluster of hosts sequentially and one of the hosts fails to enter maintenance mode, Update Manager reports an error, and the process stops and fails. The hosts in the cluster that are remediated stay at the updated level. The ones that are not remediated after the failed host remediation are not updated.

The host upgrade remediation of ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

Using VUM for Virtual Machine Upgrade - Use Update Manager to upgrade the hardware version of one or multiple virtual machines to the latest hardware version that the host supports.

You might not think of it as such, but this allows you to have additional security as VUM can roll back virtual machines and appliances to their previous state. You can manually upgrade the hardware of virtual machines immediately, or you can schedule.

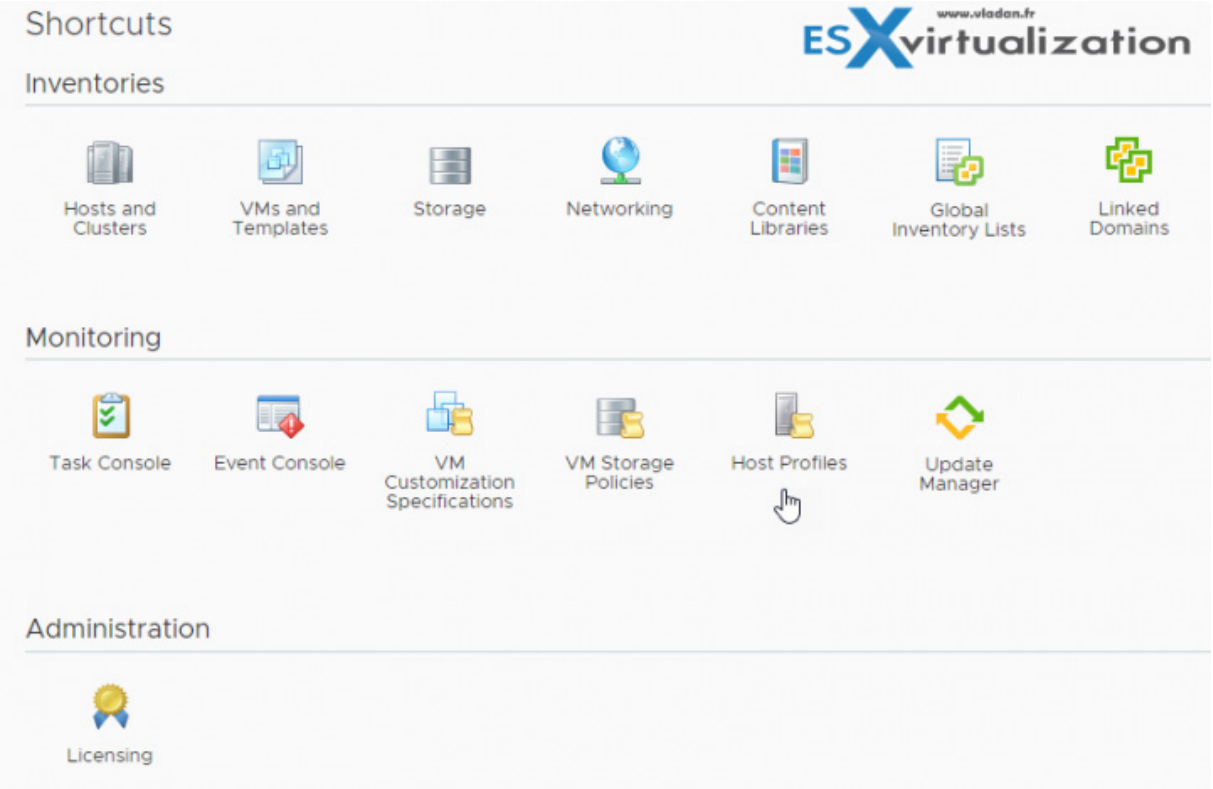
You can also use Update Manager **to upgrade VMware Tools** to the latest version that the host supports. Navigate to Menu > Hosts and Clusters > Select a host or a cluster from the inventory and click the Updates tab > The Update Overview page appears > Select VMware Tools.

We haven't covered everything here, but the essential. Use the VMware docs to read everything when studying for the exam.

Objective 7.16 - Configure and manage host profiles

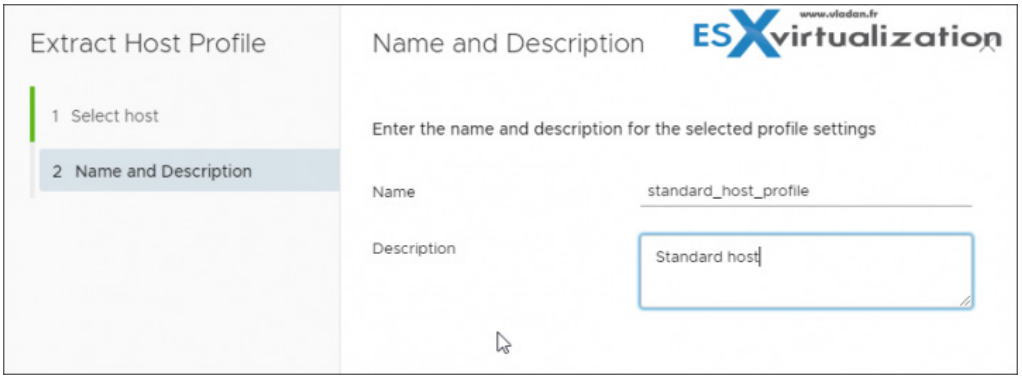
Host profiles allow us to "copy" a configuration from a reference host. The configuration of the reference host, which is extracted as a host profile, serves as a configuration template for configuring other hosts. We say that a host profile is applied to that host.

Follow the *VMware vSphere Host Profiles PDF.*



The Host Profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages multiple hosts or clusters in vCenter Server.

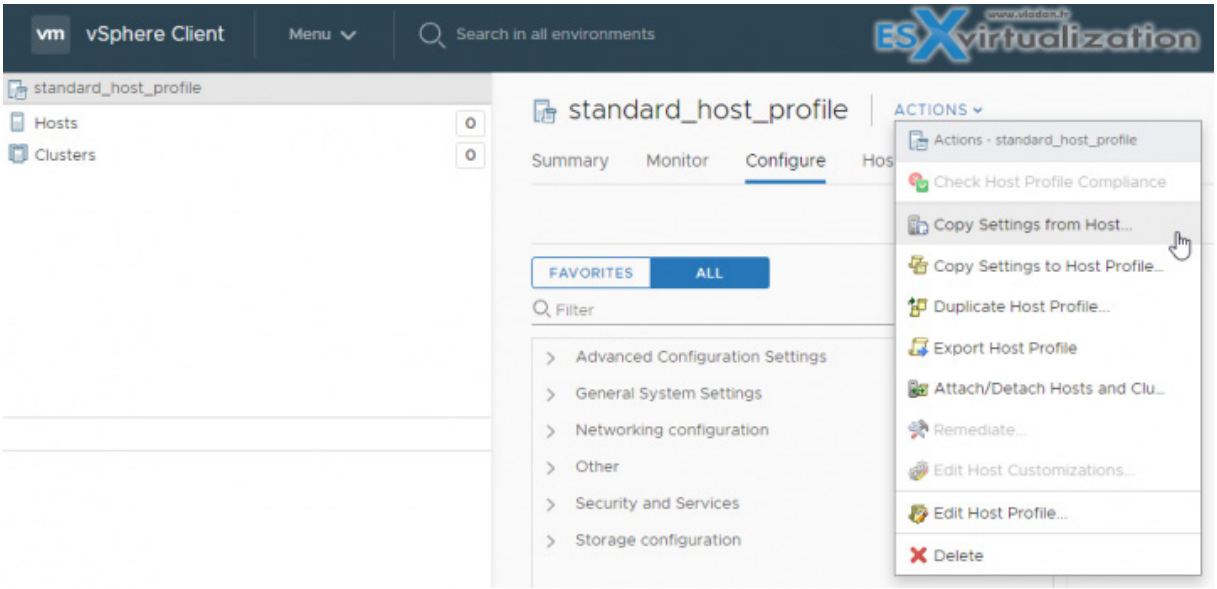
Requirements: vSphere Enterprise Plus license.



There are quite a few actions you can do with host profiles:

- **Copy Settings from Host** - If the configuration of the reference host changes, you can update the host profile so that it matches the reference host's new configuration.
- **Copy Settings to Host profile** - If you want to copy some changes to other host profiles after you made a change to host profile. Once you make changes to a host profile, you can propagate those changes to other host profiles in the inventory

- **Duplicate Host profile** - creates a copy of an existing host profile
- **Export Host Profile** - You are able to make an export of host profile in VMware profile format (.vpf). **Note**: administrator and user profile passwords are **not exported.**
- **Attach/detach hosts and clusters** - After creating a host profile from a reference host, attach the host or cluster to the host profile.
- **Remediate** - Edit Host Customization.
- **Edit Host Profile** - You can edit host Profiles policies, select a policy to be checked for compliance, and change the policy name or description
- **Check host profile compliance** - can confirm the compliance of a host or cluster to its attached host profile and determine which, if any, configuration parameters on a host are different from those specified in the host profile.



Editing a VMware host profile is a good way to do a uniform configuration change on several hosts within your environment. However, if you have a host that has changed config and you need to update your host profile from that host, you can simply use **Copy settings from host** rather than edit host profile.

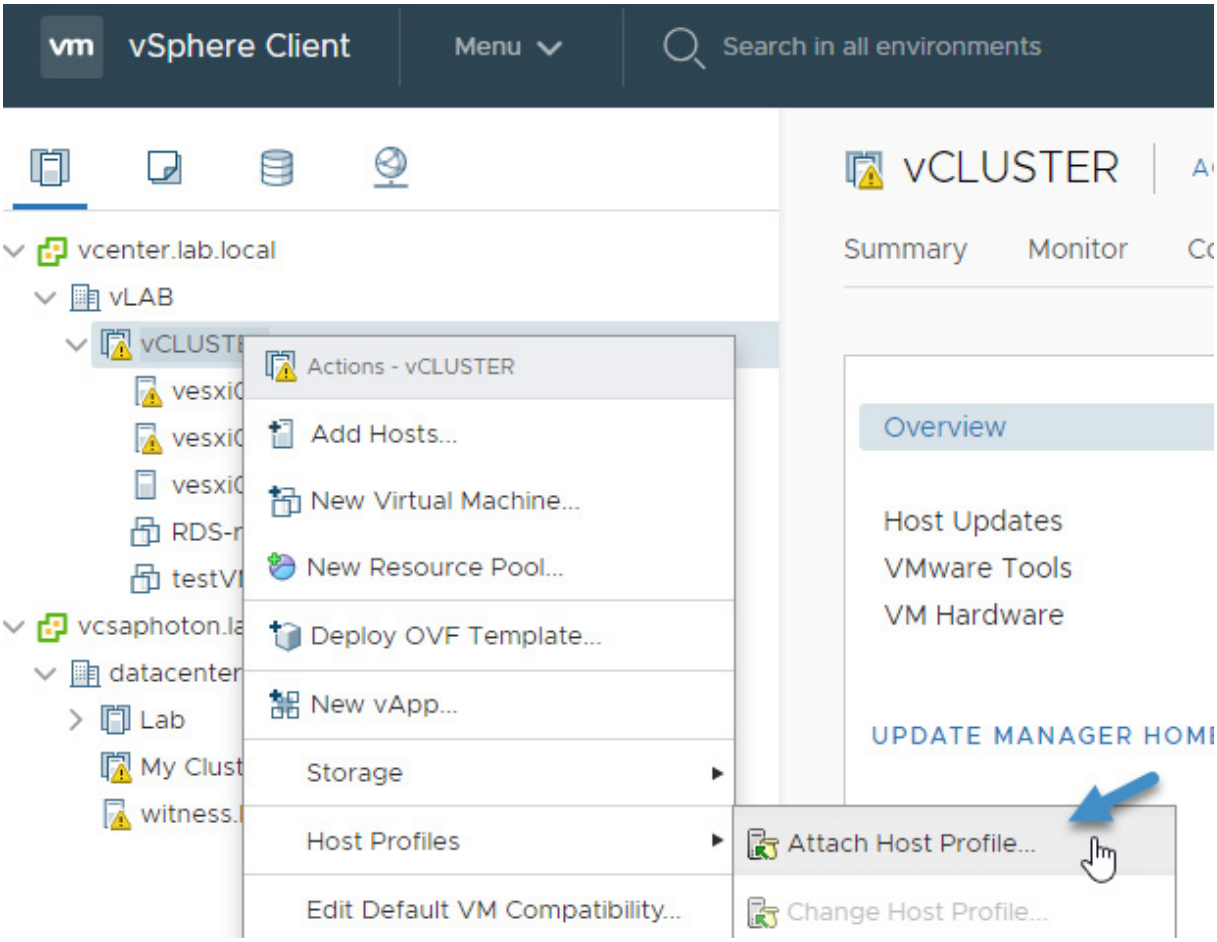
The Workflow on configuring VMware vSphere ESXi host with a VMware Host profile

First, Attach host profile to a host(s). You can attach a host profile to a host or to a cluster. If you attach host profile to a cluster, all hosts keep the same uniform configuration. Essentially, there are 3 steps to follow:

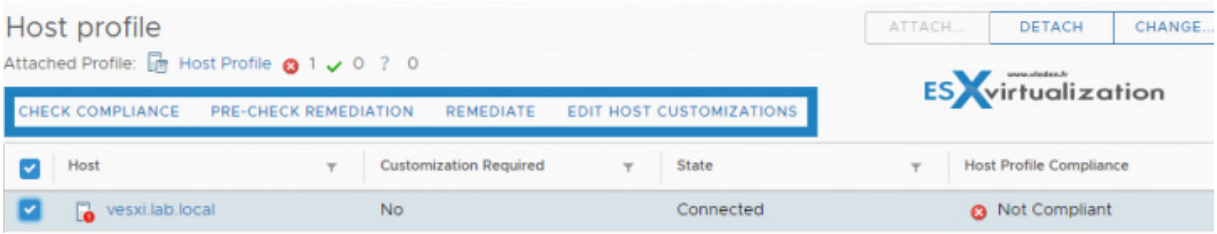
1. Attach VMware Host profile
2. Check host profile compliance
3. Remediate host with attached host profile

Here are the steps:

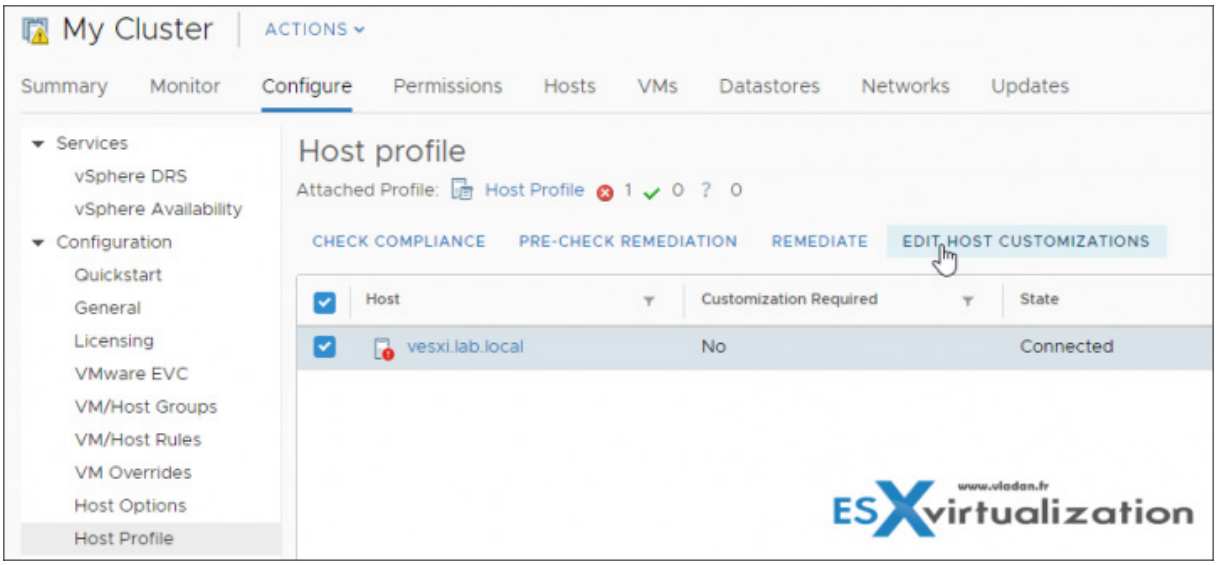
Attach VMware Host profile - Right-click the cluster from the **Hosts and Clusters view** > **Host Profiles** > select **Attach Host Profile**.



Check Compliance - when select cluster (or host) you go to Configure > Host profile. There you have different actions, including the Check compliance action.



Remediate - The remediation action is also accessible at the same menu. If host(s) is not in compliance with the attached profile, you must remediate it. Before the host(s) can be remediated, you have to edit the host customizations.

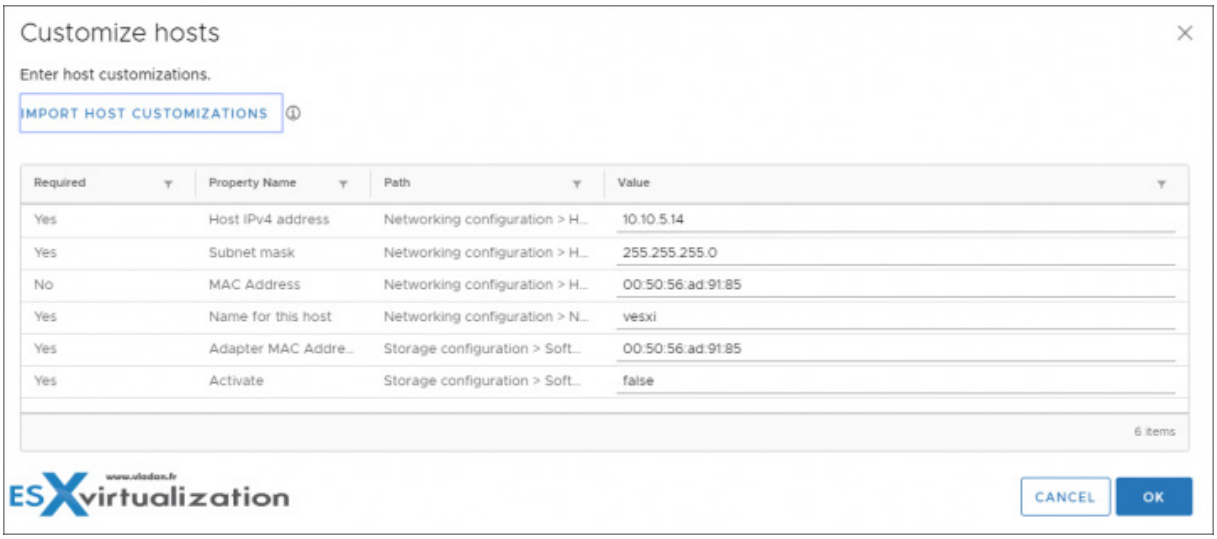


Here it really depends on the changes you're looking to make. After all, you may not even need to change anything here. So, go ahead and select the host(s) using the checkbox and then select Edit hosts customizations.

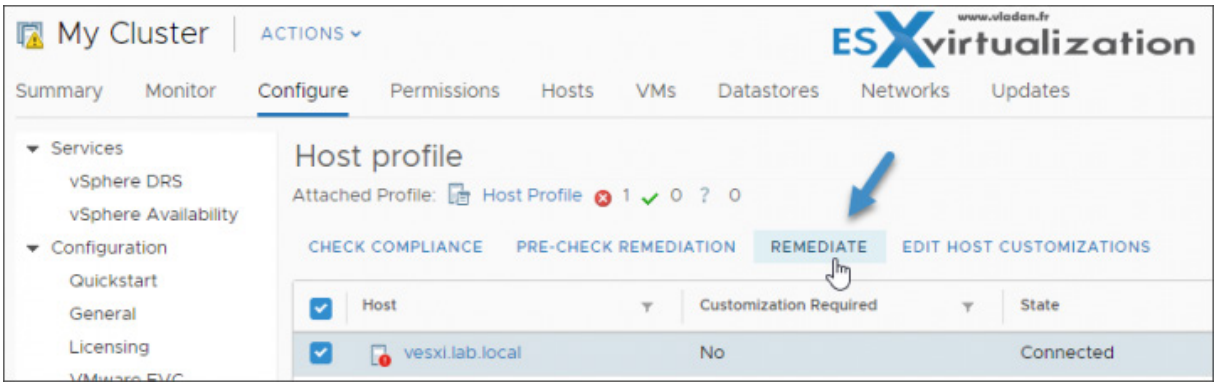
Once clicked, an overlay window will pop up, allowing us to change things here such as IP address, subnet mask, name etc. Once you review the options here you can make changes if needed. One example could be when you've created a new vmkernel port for each host. As a result, you would need to enter the IP address during this step here.

Note: you can also import a CSV file as the source for customizing host(s).

Once done, hit OK.



And this step passed you can finally hit the **remediate** button.



Certain Host Profile policy configurations require that the host be rebooted after remediation. In those cases, you are prompted to place the host into maintenance mode. You might be required to place hosts into maintenance mode before remediation.

Hosts that are in a fully automated DRS clusters are placed into maintenance mode at remediation. For other cases, the remediation process stops if the host is not placed into maintenance mode when it is needed to remediate a host.

Follow the *VMware vSphere Host Profiles PDF.*

Final Words

Stay consistent with your studying! Use our study guide, but by no means exclusively. The more you read, the better you'll fare. Don't rely completely on a single source for your exam preparation, but rather multiple sources at the same time. We try to give as many details as possible, with screenshots, and hope you have found this guide useful. We are not able to cover everything, though, and urge you to keep broad source horizons. Good luck!