



NAKIVO®

NEW

# VCP-DCV Community Study Guide

Based on vSphere 7.x

[UNOFFICIAL]



By Vladan SEGET

[www.vladan.fr](http://www.vladan.fr)

---

In order to become **VCP-DCV certified** and pass the Professional vSphere 7 exam, we follow are the guidelines from the VMware Exam guide [2V0-21.20](#)

The Professional vSphere 7 Exam (**2V0-21.20**) which leads to VMware Certified Professional – Data Center Virtualization (VCP-DCV) certification is a 70-item exam, with a passing score of 300 using a scaled scoring method. Candidates are given 130 minutes to complete the exam.

The VMware Exam prep guide is [here](#) on VMware's website. The official code for this exam is 2V0-21.20, and the cost of the exam is \$250.

# NAKIVO Backup & Replication

#1 Solution for Backup and Ransomware Recovery  
of Virtual, Physical, Cloud and SaaS environments



## Best of VMworld 2020

Finalist in the Resilience & Recovery category



All-in-one solution for backup, replication, instant granular restore, site recovery and ransomware recovery



Policy-based data protection for simplified and automated management in virtualized environments



Create a high-performance backup appliance by installing on Windows, Linux or a NAS device



Pricing starts from just \$99/socket, \$17 machine/year or \$0.75 per user/month for SaaS

## Leading brands trust NAKIVO



HONDA



SIEMENS

# Table of Contents

<a href="#">Objective 1.1 - Identify the pre-requisites and components for vSphere implementation</a>	6
<a href="#">Objective 1.2 Describe vCenter Server Topology</a>	9
<a href="#">Objective 1.3 Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.)</a>	13
<a href="#">Objective 1.3.1 Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.)</a>	15
<a href="#">Objective 1.3.2 Explain the importance of advanced storage configuration (vSphere Storage APIs for Storage Awareness (VASA), vSphere Storage APIs Array Integration (VAAI), etc.)</a>	16
<a href="#">Objective 1.3.3 Describe Storage Policies</a>	19
<a href="#">Objective 1.3.4 Describe Basic Storage Concepts in K8s, vSAN, and vSphere Virtual Volumes (vWols)</a>	23
<a href="#">Objective 1.4 Differentiate between vSphere Network I/O Control (NIOC) and vSphere Storage I/O Control (SIOC)</a>	27
<a href="#">Objective 1.5 Describe instant clone architecture and use cases</a>	34
<a href="#">Objective 1.6 Describe ESXi Cluster Concepts</a>	37
<a href="#">Objective 1.6.1 Describe Distributed Resource Scheduler (DRS)</a>	43
<a href="#">Objective 1.6.2 What is VMware Enhanced vMotion Compatibility (EVC)</a>	46
<a href="#">Objective 1.6.3 Describe how Distributed Resource Scheduler (DRS) scores virtual machines</a>	49
<a href="#">Objective 1.6.4 Describe vSphere high availability</a>	53
<a href="#">Objective 1.6.5 Describe datastore clusters</a>	58
<a href="#">Objective 1.7 Identify vSphere distributed switch and vSphere standard switch capabilities</a>	63
<a href="#">Objective 1.7.1 Describe VMkernel networking</a>	68
<a href="#">Objective 1.7.2 Manage Networking on Multiple Hosts with vSphere Distributed Switch</a>	72
<a href="#">Objective 1.7.3 Describe networking policies</a>	80
<a href="#">Objective 1.7.4 Manage Network I/O Control (NIOC) on a vSphere distributed switch</a>	89
<a href="#">Objective 1.8 Describe vSphere Lifecycle Manager concepts (baselines, cluster images, etc.)</a>	95
<a href="#">Objective 1.9 Describe the basics of vSAN as primary storage</a>	98
<a href="#">Objective 1.9.1 Identify basic VMware vSAN 7 requirements</a>	101
<a href="#">Objective 1.10 Describe the vSphere Trust Authority architecture</a>	105
<a href="#">Objective 1.11 Explain Software Guard Extensions (SGX)</a>	107
<a href="#">Objective 2.1 Describe the role of vSphere in the software-defined data center (SDDC)</a>	110
<a href="#">Objective 2.2 Identify use cases for VMware Cloud Foundation (VCF)</a>	111
<a href="#">Objective 2.3 Identify migration options</a>	113
<a href="#">Objective 2.4 Identify DR use cases</a>	116
<a href="#">Objective 2.5 Describe vSphere integration with VMware Skyline</a>	122
<a href="#">Objective 4.1 Describe single sign-on (SSO) deployment topology</a>	126
<a href="#">Objective 4.1.1 Configure single sign-on (SSO) domain</a>	128
<a href="#">Objective 4.1.2 Join an existing single sign-on (SSO) domain</a>	133

---

<a href="#">Objective 4.2 Configure VSS advanced virtual networking options</a>	136
<a href="#">Objective 4.3 Set up vCenter identity sources</a>	141
<a href="#">Objective 4.3.1 Configure Identity Federation</a>	144
<a href="#">Objective 4.3.2 Configure Lightweight Directory Access Protocol (LDAP) integration</a>	147
<a href="#">Objective 4.3.3 Configure Active Directory integration</a>	149
<a href="#">Objective 4.4 Deploy And Configure vCenter Server 7 Appliance</a>	151
<a href="#">Objective 4.5 Create and configure VMware High Availability and advanced options (Admission control, proactive HA etc.)</a>	161
<a href="#">Objective 4.6 Deploy and configure vCenter Server High Availability</a>	165
<a href="#">Objective 4.7 Setup a Content Library</a>	169
<a href="#">Objective 4.8 Configure vCenter Server file-based backup</a>	176
<a href="#">Objective 4.9 Analyze basic log output from vSphere products</a>	180
<a href="#">Objective 4.10 Configure vSphere Trust Authority</a>	184
<a href="#">Objective 4.11 Configure vSphere certificates</a>	186
<a href="#">Objective 4.11.1 Describe Enterprise PKIs role for SSL certificates</a>	188
<a href="#">Objective 4.12 Configure vSphere 7 Lifecycle Manager/VMware Update Manager (VUM)</a>	191
<a href="#">Objective 4.13 Securely Boot ESXi hosts</a>	196
<a href="#">Objective 4.14 Configure different network stacks</a>	197
<a href="#">Objective 4.15 Configure Host Profiles</a>	199
<a href="#">Objective 4.16 Identify boot options</a>	207
<a href="#">Objective 4.16.1 Configure Quick Boot</a>	212
<a href="#">Objective 5.1 Identify Resource pools use cases</a>	212
<a href="#">Objective 5.1.1 - Explain shares, limits, and reservations (resource management)</a>	216
<a href="#">Objective 5.2 - Monitor resources of vCenter Server Appliance and vSphere environment</a>	219
<a href="#">Objective 5.3 - Identify and use tools for performance monitoring</a>	223
<a href="#">Objective 5.4 – Configure Network I/O control</a>	229
<a href="#">Objective 5.5 – Configure Storage I/O Control (SIOC)</a>	235
<a href="#">Objective 5.6 – Explain the performance impact of maintaining virtual machine snapshots</a>	240
<a href="#">Objective 5.7 – Plan for upgrading various vSphere components</a>	244
<a href="#">Objective 7.1 - Create and manage virtual machine snapshots</a>	247
<a href="#">Objective 7.2 and 7.3 - Create virtual machines using different methods (Open Virtual Machine Format (OVF) templates, content library, etc.)</a>	251
<a href="#">Objective 7.4 – Manage Storage (datastores, storage policies, etc.)</a>	253
<a href="#">Objective 7.4.1 – Configure and modify datastores</a>	267
<a href="#">Objective 7.4.2 Create virtual machine storage policies</a>	274

---

<a href="#">Objective 7.4.3 - Configure storage cluster options</a>	280
<a href="#">Objective 7.5 - Create Distributed Resource Scheduler (DRS) affinity and anti-affinity rules for common use cases</a>	285
<a href="#">Objective 7.6 – Perform different types of migrations</a>	291
<a href="#">Objective 7.7 - Configure role-based user management</a>	294
<a href="#">Objective 7.8 - Configure and manage the options for securing a vSphere environment (certificates, virtual machine encryption, virtual Trusted Platform Module, lock-down mode, virtualization-based security, etc.)</a>	300
<a href="#">Objective 7.9 - Configure and manage host profiles</a>	305
<a href="#">Objective 7.9 - Utilize baselines to perform updates and upgrades</a>	305
<a href="#">Objective 7.11 - Utilize vSphere Lifecycle Manager</a>	308
<a href="#">Objective 7.11.1 - Describe Firmware upgrades for ESXi</a>	310
<a href="#">Objective 7.11.2 – Describe ESXi Updates</a>	312
<a href="#">Objective 7.11.3 – Describe Component and Driver Updates for ESXi</a>	314
<a href="#">Objective 7.11.4 – Describe Hardware Compatibility Check</a>	314
<a href="#">Objective 7.11.5 - Describe ESXi cluster image export functionality</a>	316
<a href="#">Objective 7.12 – Configure Alarms</a>	322

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

**VMware ESXi Server** - Only supported hardware should be used to install VMware ESXi. If you don't use supported hardware, you most likely won't find some components such as NICs, storage controllers, etc. after installation. Pretty annoying if you ask me, but that's the way it is. VMware cannot support ALL the server (or PC) hardware that exists. The VMware hardware compatibility guide (HCL) page is [here](#).

System Requirements:

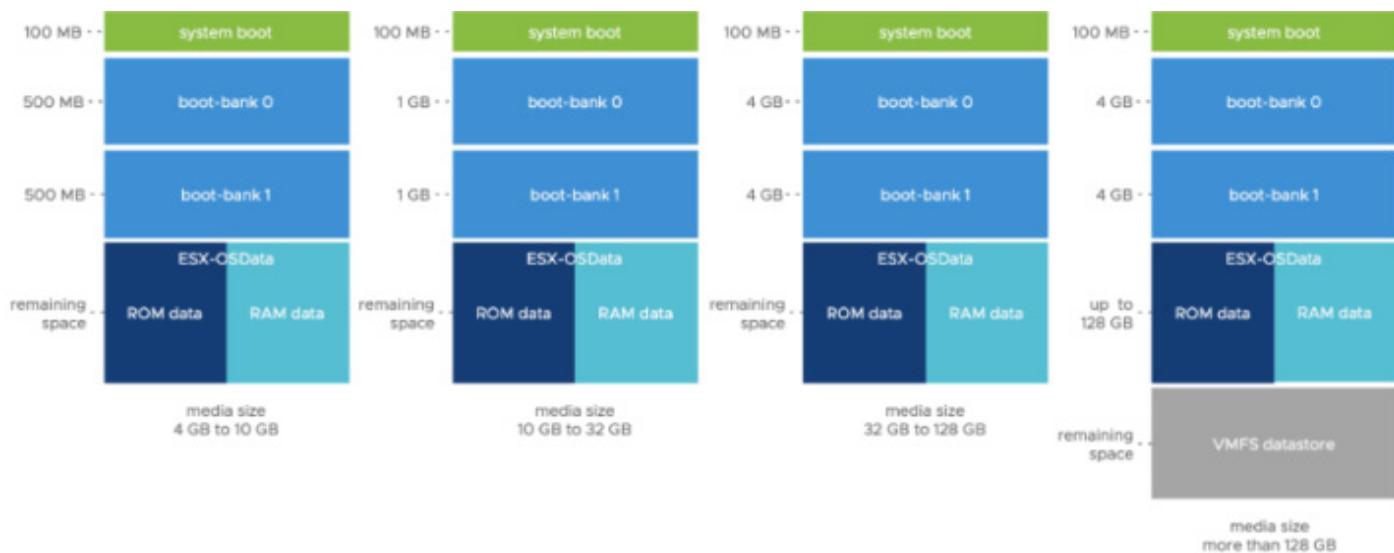
- ESXi 7 requires a host machine with at least 2 CPU cores.
- ESXi 7 supports 64-bit x86 processors released after September 2006. This includes a broad range of multi-core processors. For a complete list of supported processors, see the VMware compatibility guide [here](#).
- ESXi 7 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi 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.

VMware ESXi 7.0 has a completely new partition layout. As such, you **can't revert back** (via [Shift-R] to initiate the recovery mode and eventually recover the previous ESXi version. ESXi 7.0 has only 4 different partitions compared to the previous release, which had 8.

You can still revert back from ESXi 7.0b to 7.0GA.

VMware limits the number of cores per license to 32 (unlimited before) so if you buy a 1 CPU license you will only be able to have CPU with 32 cores, otherwise, you'll need 2 licenses. If the CPU has more than 32 cores, additional (per-CPU) licenses are required. For example, for a 48 core CPU, you'll need 2 licenses.

This affects not only paid VMware vSphere/ESXi, as the ESXi 7.0 free version raises these requirements to more than 3 GB of disk space (3.72 GB to be exact). The recommended size is actually 32 Gb. What's interesting is that while the size of the boot partition (100 MB) does not change, the other partitions sizes change depending on the size of media used for the installation.

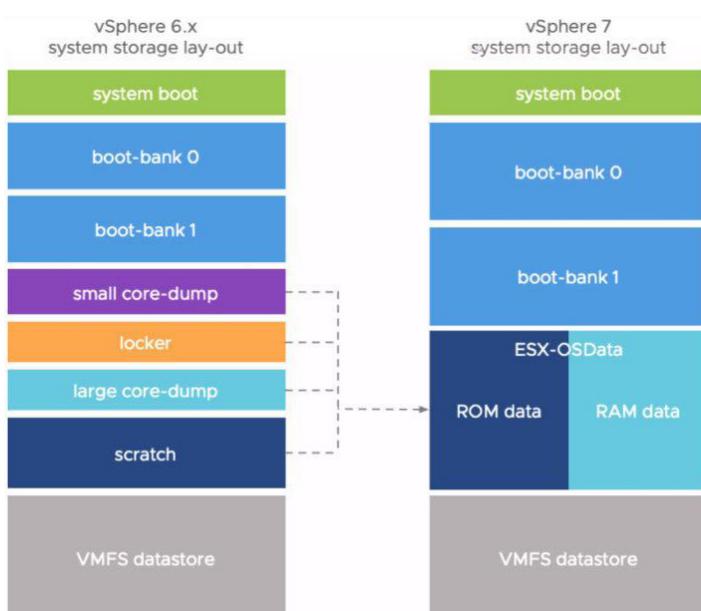


Apart from HDD, SSD, and NVMe, you can also use boot from a SAN LUN.

### Minimal ESXi 7 Storage requirements for installation:

- 8GB for USB sticks or SD devices (4Gb if you're upgrading from ESXi 6.7).
- 32GB for other boot devices like hard disks, or flash media like SSD or NVMe devices.
- A boot device must not be shared between ESXi hosts.

The partition layout has changed as well. There is an increase in the boot bank sizes where the system partitions are consolidated and are expandable. See this image from VMware.



## vCenter Server - The managing piece.

When your environment is bigger than 2-3 hosts, you'll want to have vCenter.

VMware vCSA is a Linux distribution based on Photon OS. For some of you who do not follow VMware at all and know only ESXi, then we could say that yes, VCSA is a management VM for ESXi hosts.

In order to understand vSphere management, a while back, we have put a simple article that 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, real basic, real simple explanation to people who do not deal with VMware.

The vCSA VM runs PhotonOS 3.0, which is a Linux distro maintained by VMware. The machine runs several services, such as vSphere authentication services, PostgreSQL database, vSphere Lifecycle Manager (previously vSphere Update Manager), etc.

There are a lot of services for authentication, such as vSphere Single Sign-on (SSO), vSphere license services, Certification authority.

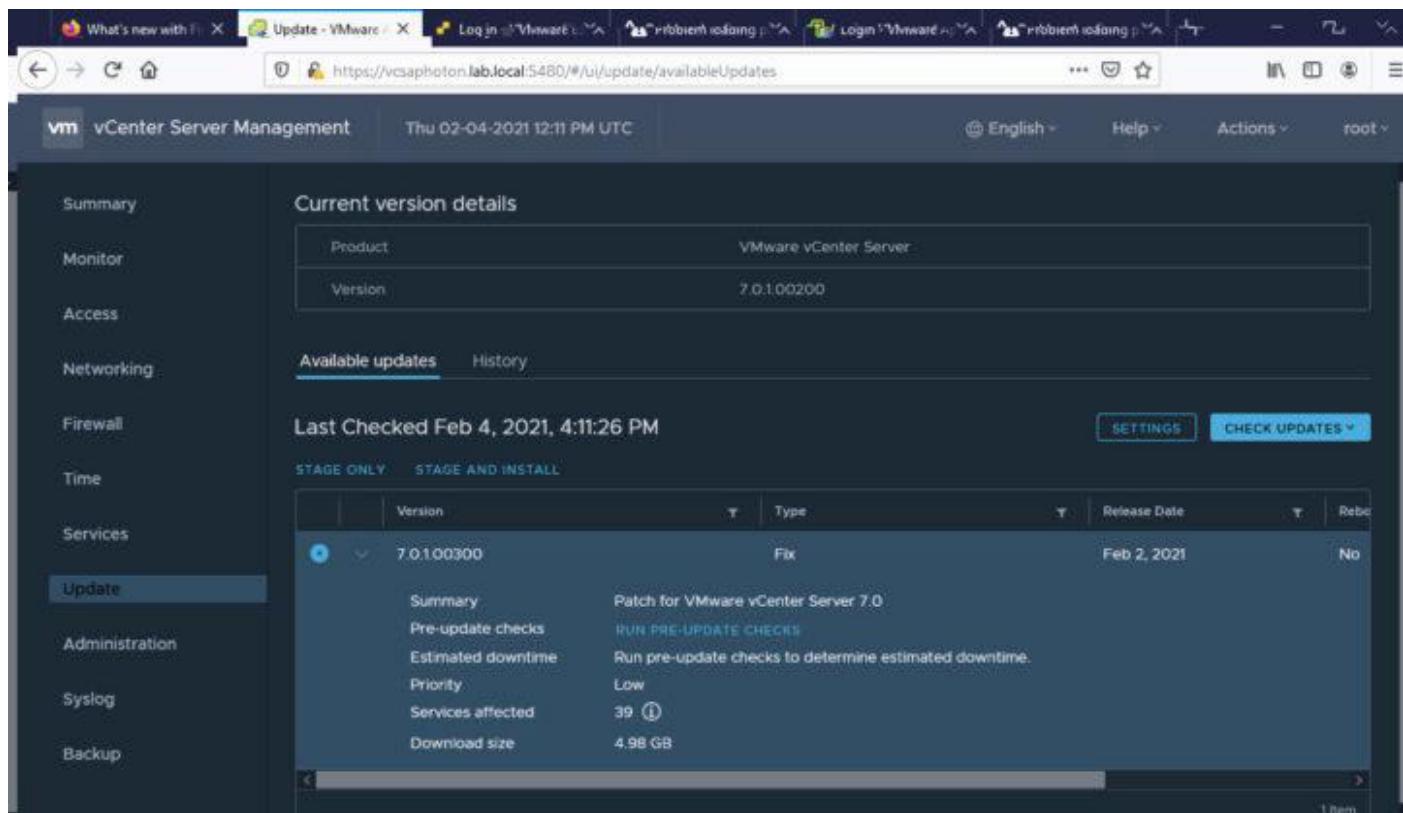
Other services such as vSphere Auto-deploy or ESXi dump collector.

Only HTML5 web-based client is now used. No more Flash.

The deployment of vCSA can be done via GUI or via CLI. There are examples of .json files available within the installation directory.

[https://IP\\_or\\_FQDN\\_VCSA/](https://IP_or_FQDN_VCSA/)

Overview of the web-based access for vCenter Server Appliance for VMware vSphere. The updates of the VCSA are now quite easy too.



The screenshot shows the vCenter Server Management interface. On the left, there's a sidebar with tabs for Summary, Monitor, Access, Networking, Firewall, Time, Services, Update (which is selected), Administration, Syslog, and Backup. The main content area has a header "Current version details" showing "Product: VMware vCenter Server" and "Version: 7.0.1.00200". Below this, under "Available updates", it says "Last Checked Feb 4, 2021, 4:11:26 PM". There are two tabs: "SETTINGS" and "CHECK UPDATES". A table lists one update: "7.0.1.00300" (Patch for VMware vCenter Server 7.0). The table columns are Version, Type, Release Date, and Reboot. The row shows: Version 7.0.1.00300, Type Fix, Release Date Feb 2, 2021, and Reboot No. Below the table, it says "1 item".

VMware Platform services controller (PSC) is now integrated into the same VM. The architectures with external PSCs are phased out, and vCenter 7 allows you to do easy migration via assistant.

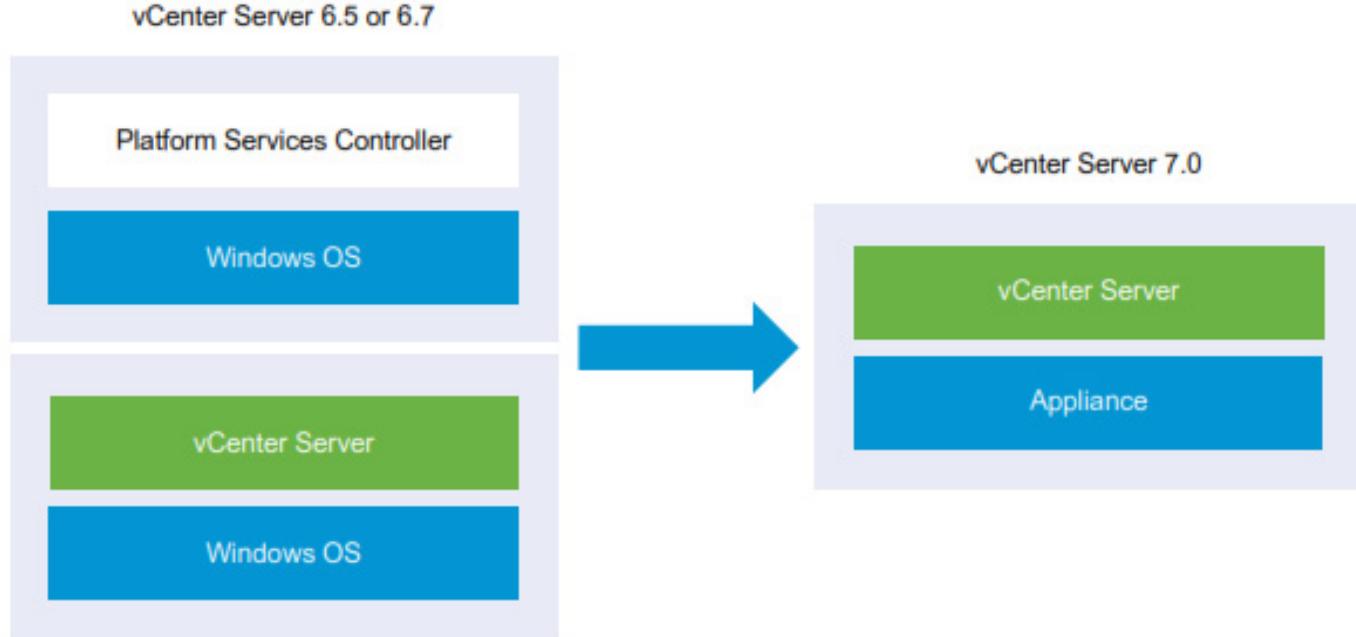
## Objective 1.2 Describe vCenter Server Topology

It is important to know what the supported and deprecated topologies are for VMware vCenter Server 7. Many admins when they inherit a vSphere installation, want to make sure that the system is supported by VMware and upgrade to the latest release.

There has been a vCenter server architecture transition since a couple of years. In the past, VMware supported an external Platform Services Controller (PSC) that was running as a separate VM and providing certain vSphere services, such as SSO, license, certificates or directory services, and it was the recommended architecture for multi-site or large-scale deployments.

Luckily, the external Platform Services Controller (PSC) deployment model from versions 6.0 and 6.5 has been removed a while ago. So vSphere 7 only uses the embedded model, where the same VM runs the vCenter server and PSC services on the same virtual machine (VM).

If you are using an external PSC, then the upgrade process now automatically converges the deployment into the embedded model.



## vCenter server converge utility

Make sure to check the [VMware Product Interoperability Matrices](#) and the [VMware Compatibility Guide](#) for the latest paths.

Before you upgrade or migrate your environment to vSphere 7.0, you must move any deprecated deployment topology to a supported deployment topology.

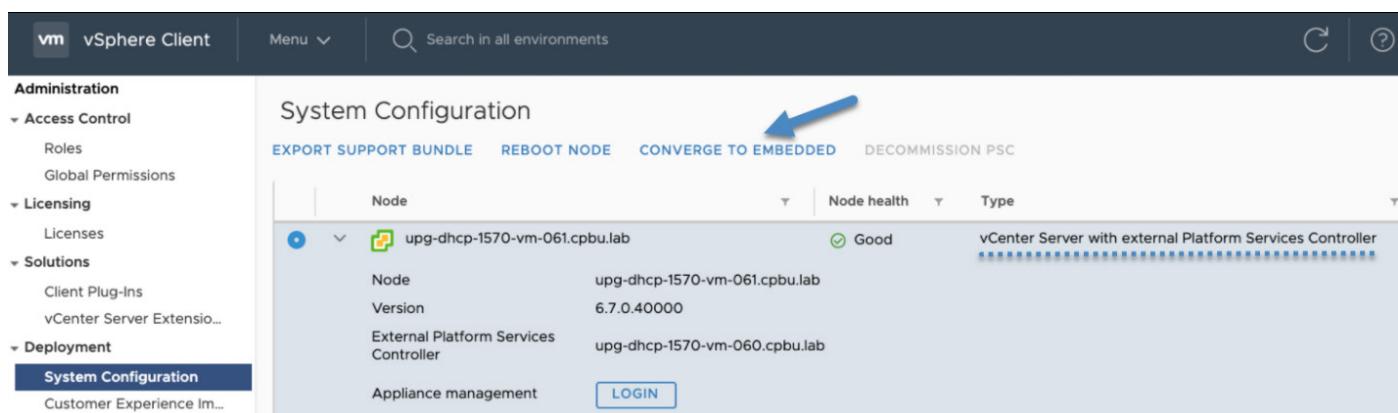
## Deprecated topologies and vCenter upgrade paths

We can sum up the vCenter version and upgrade possibilities in five major points. Note that some of those versions are no longer supported by VMware.

- vCenter 5.0 or 5.1 with updates cannot be directly upgraded to 6.5; an intermediate upgrade to 5.5 or 6.0 is required. So, if you still have vCenter server 5, make sure to upgrade it to vCenter 5.5 first.
- vCenter 5.5 or later can be directly upgraded to 6.5 or U1. This one is easy as from here you can easily upgrade to 6.5 and then to 6.7.
- vCenter 5.x cannot be directly upgraded to 6.7; an intermediate upgrade to 6.0 is required. (See the above).
- vCenter 6.0 or later can be directly upgraded to 6.7
- vCenter server on Windows is no longer available in vSphere 7, so any previous versions must be converted via the assistant. (There is an option for "Migrate" when you run the VCSA installer). Windows VCenter Server must be v5.5 or v6.0 (any build/patch) to migrate to vCenter Server appliance 6.5. If windows based vCenter is v5.0 or 5.1, upgrade to 5.5 first and then migrate to VCSA 6.5.

During the upgrade to the latest vCenter server 7, there is a tool called **vCenter server converge tool** allowing you to migrate the external PSCs into the embedded. When executed, the Converge Tool checks whether you'll need any additional components via internet access (if you have one), and those components will be automatically downloaded from the VMware Online Repository.

For topologies with multiple vCenter servers and the transition to embedded PSCs, VMware has developed a new UI within vCenter server where selected vCenter server(s) can be converged into embedded topology.



The screenshot shows the vSphere Client interface with the 'System Configuration' tab selected. On the right, a table lists a single node named 'upg-dhcp-1570-vm-061.cpbu.lab'. A blue arrow points to the 'CONVERGE TO EMBEDDED' button located above the table. The table columns include Node, Node health, and Type. The node is listed as 'Good' and 'vCenter Server with external Platform Services Controller'.

When running this utility, your External PSC will be shut down and unregistered from the Single Sign-On (SSO) domain.

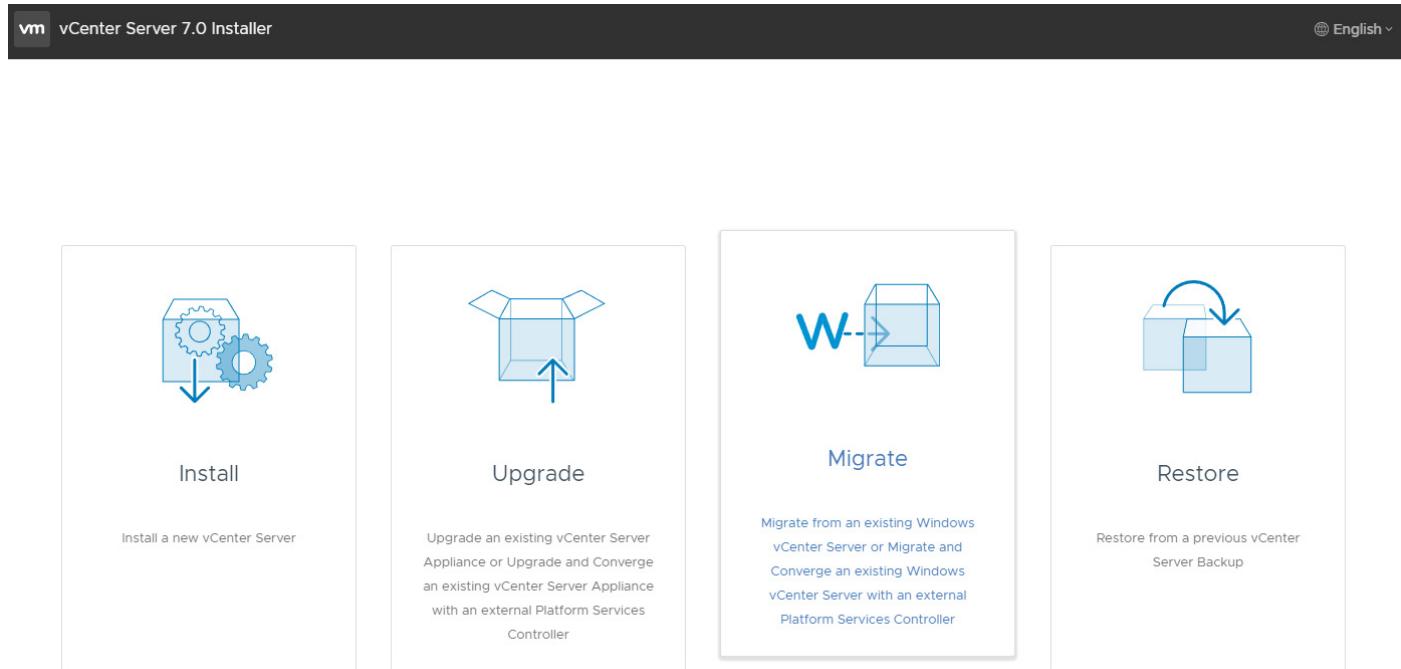
The Embedded PSC doesn't only simplify the vCenter architecture and patching, but you also have less VMs to manage and less consumption of RAM, CPU, and storage. If you have a large-scale architecture with many PSCs, then the conversion can save a good amount of resources.

## Migrating Windows-based vCenter and Windows-based PSC

When running vCenter server and PSC on Windows as separate VMs, you can migrate an external PSC instance from Windows to appliance.

It is a two-stage process:

- You'll need to deploy a new vCenter Server to the target ESXi host or a compute resource in the target vCenter Server.
- The second stage completes the vCenter Server setup and copies data from the source vCenter Server for Windows to the deployed vCenter Server



Mount the VCSA installer CD on the Windows VM which you're converting and run the VMware Migration Assistant on the Windows machine. It's a CLI utility you'll find in a subfolder. Just follow the instructions from the assistant. At the end you can decommission the external PSC after making sure it is unregistered from SSO. It is important to leave the Migration Assistant window open until you complete the upgrade or the migration process of your vCenter Server deployment.

**Note:** If anything goes wrong, you should know that you can do a rollback by reverting the source appliance or vCenter server on Windows. If that's needed, check the VMware [KB 2146453](#) article.

## What can be migrated?

During the migration assistant process, you can monitor the migration and manage what you want to bring over with you. The previous version of vCenter had also perhaps an external database. You have the possibility to migrate the data from an external DB to the embedded PostgreSQL database in vCenter server 7.0. You can also migrate vCenter tasks and history. The progress of the migration is shown in the browser window.

## Final thoughts

VMware has finally simplified vCenter Server 7. We no longer have to deal with two versions (Windows and VCSA) and we no longer have to deal with external PSCs.

vCenter server 7 runs on a single VM. But If necessary, we can add more resiliency with vCenter server HA where 3 nodes of vCenter server instances running at the same time, are able to make sure that you don't lose a hand when one instance of your vCenter server becomes unavailable.

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

vSphere can use several types of storage, and we'll see the details of what you need to know here.

**Local and Networked storage** – while local storage is pretty obvious (direct-attached disks or DAS), the networked storage can be of 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. ESXi supports SCSI, IDE, SATA, USB, SAS, flash, and NVMe devices. You cannot use IDE/ATA or USB to store your VMs.

vSphere and ESXi support network storage based on NFS 3 and 4.1 protocol for file-based storage. This type of storage is presented as a share to the host instead of block-level raw disks.

The main problem with DAS is that only the server where the storage is physically installed can use it - not any other machine within your cluster. That's why it is far better to use shared storage with NFS, iSCSI, or FC.

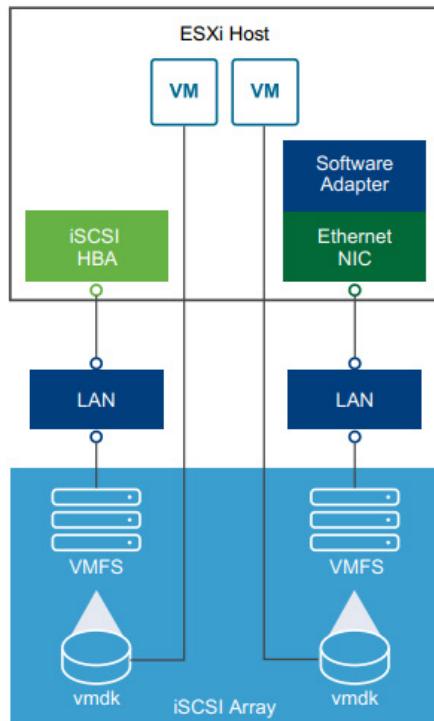
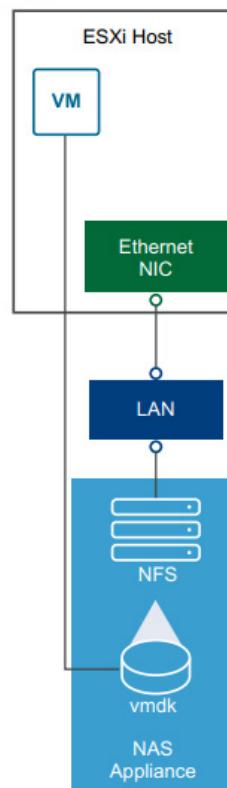
**Fibre Channel (FC) storage** – FC SAN is a specialized high-speed network that connects your hosts to high-performance storage devices. The network uses the Fibre Channel protocol to transport SCSI traffic from virtual machines to the FC SAN devices. The host should have Fibre Channel host bus adapters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

**Network storage** – This type of storage is usually based on dedicated enclosures that have controllers usually running Linux or another specialized OS on it. Now they're starting to be equipped with 10GbE NICs, but this wasn't always the case. However, it allows multiple hosts within your environment to be connected directly to the storage and share this storage among those hosts.

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

Few more storage types:

- **VMware FileSystem (VMFS) datastores:** All block-based storage must be first formatted with VMFS to transform a block service to file and folder-oriented services.
- **Network FileSystem (NFS) datastores:** This is for NAS storage.
- **VVol:** Introduced in vSphere 6.0 and is a new paradigm to access SAN and NAS storage in a common 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. And storage hardware gains complete control over virtual disk content, layout, and management.

- **vSAN datastore:** If you are using a vSAN solution, all your local storage devices could be polled 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 that 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), which uses APIs which allow storage partners to create and deliver multipathing and load-balancing plugins that are optimized for each array. Plugins talk to storage arrays and chose the best path selection strategy to increase IO performance and reliability.

## Objective 1.3.1 Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.)

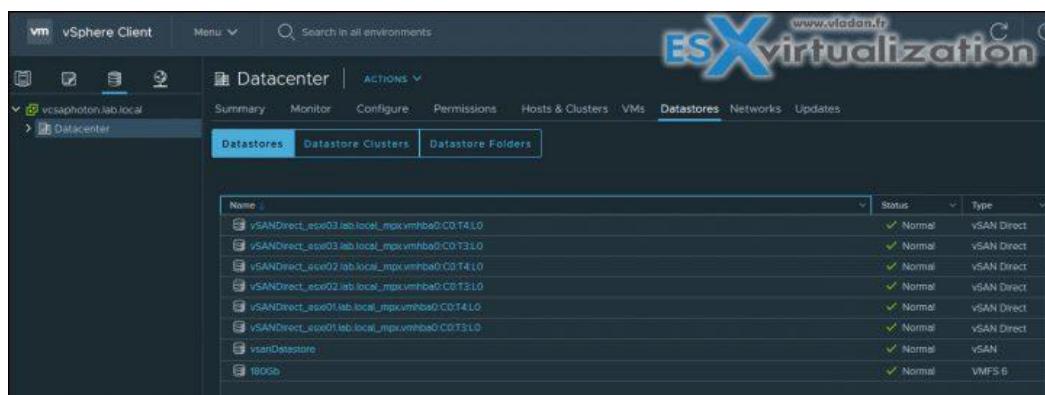
**VMFS** – you can use VMFS 5 or VMFS 6 within vSphere 7. This file system is installed on block storage devices. VMFS is a special high-performance file system format that is optimized for storing virtual machines that can be iSCSI LUNs or local (Direct Access) DAS storage.

The upgrade from 5 to 6 is not direct. You must delete and reformat the datastore. vSphere uses a locking mechanism so multiple access, from multiple hosts to files is controlled.

**NFS** – vSphere 7 supports NFS v3 and 4.1 and this file system is a file system that uses the network to access it. In the case of NFS, the access to the files is controlled by the NAS device.

**VMware vSAN** – vSAN uses local storage and SSDs from each host to create a storage pool shared within the cluster. You'll need at least 2 hosts and one witness host to create vSAN storage. Please check other chapters of our guide for more specific and detailed information about vSAN.

**vVOL** – this is another type of storage using vVol datastore that are storage containers on a block device.



From vSphere 7 documentation:

Depending on your storage type, some of the following tasks are available for the datastores.

- Create datastores. You can use the vSphere Client to create certain types of datastores.
- Perform administrative operations on the datastores. Several operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.
- Organize the datastores. For example, you can group them into folders according to business practices. After you group the datastores, you can assign the same permissions and alarms on the datastores in the group at one time.
- Add the datastore to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create the datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the vSphere Resource Management documentation.

## **Objective 1.3.2 Explain the importance of advanced storage configuration (vSphere Storage APIs for Storage Awareness (VASA), vSphere Storage APIs Array Integration (VAAI), etc.)**

Many of the storage devices are using protocols that improve the performance of vSphere storage or by offloading certain operations, the ESXi CPU usage gets lower.

**VASA** – VASA is a shortcut for vSphere APIs for Storage Awareness. VASA is important because hardware storage vendors use it to list through vCenter Server the capabilities of the storage array, health, and configurations. VASA is essential for vVols, vSAN, and Storage Policies. Using Storage Policies and VASA, you can specify that VMs need a specific performance profile or configuration, such as RAID type.

**VAAI** – VAAI stands for vSphere APIs for Array Integration. This technology allows offloading some operations to the storage hardware instead of being performed in ESXi. Though the degree of improvement is dependent on the storage hardware, VAAI can improve storage scalability, can reduce storage latency for several types of storage operations, can reduce the ESXi host CPU utilization for storage operations, and can reduce storage network traffic.

**Note:** Some software vendors support VAAI too. For Example, StarWind. Let me show you a very old pic from the lab with a StarWind datastore.

Identification	Status	Device	Drive Type	Hardware Acceleration	Capacity
02Sata1Tb	Normal	ATA Serial Attached SCSI ...	Non-SSD	Unknown	931.25 GB
64GbSSDKingston	Normal	Local ATA Disk (t10.ATA...)	SSD	Unknown	59.50 GB
drobo	Normal	Drobo iSCSIDisk (naa.60...)	Non-SSD	Not supported	1,023.75 G
hybrid	Normal	10.10.3.11:/exports/hybrid	Unknown	Supported	149.31 GB
starwind	Normal	STARWIND iSCSI Disk (eui...)	Non-SSD	Supported	199.75 GB
vsanDatastore	Normal		N/A	Not supported	

In addition, On SANs, VAAI has the following features:

- Scalable lock management (sometimes called “hardware-assisted locking,” “Atomic Test & Set,” or ATS) replaces the use of SCSI reservations on VMFS volumes when performing metadata updates. This can reduce locking-related overheads, speeding up many administrative tasks as well as increasing I/O performance for thin VMDKs. ATS helps improve the scalability of very large deployments by speeding up provisioning operations such as the expansion of thin disks, creation of snapshots, and other tasks.
- Extended Copy (sometimes called “full copy,” “copy offload,” or XCOPY) allows copy operations to take place completely on the array, rather than having to transfer data to and from the host. This can dramatically speed up operations that rely on cloning, such as Storage vMotion, while also freeing CPU and I/O resources on the host.
- Block zeroing (sometimes called “Write Same”) speeds up the creation of eager-zeroed thick disks and can improve first-time write performance on lazy-zeroed thick disks and on thin disks.
- Dead space reclamation (using the UNMAP command) allows hosts to convey to storage which blocks are no longer in use. On a LUN that is thin-provisioned on the array side this can allow the storage array hardware to reuse no-longer-needed blocks.

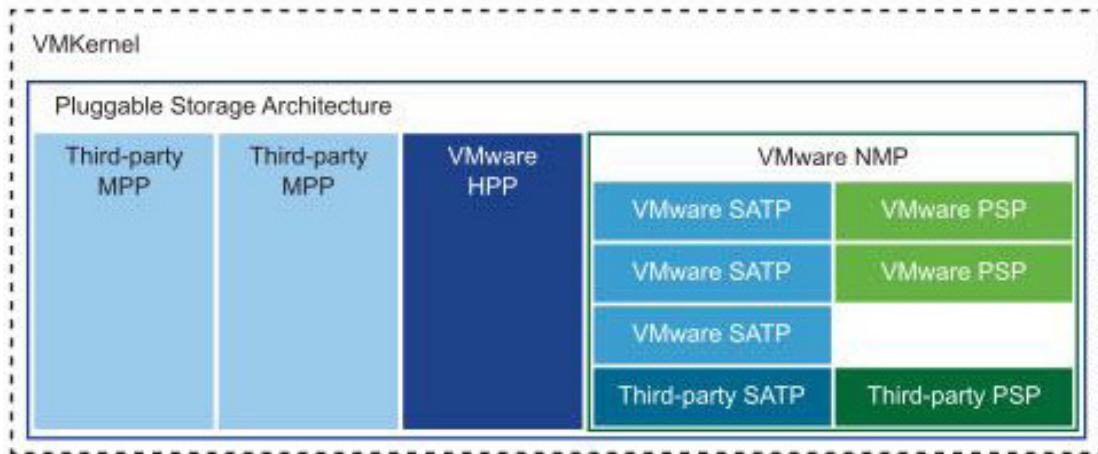
**Array Thin Provisioning APIs** – This helps monitor space usage on thin-provisioned storage arrays to prevent out of space conditions, and does space reclamation when data is deleted.

**PSA** – PSA is a shortcut for Pluggable Storage Architecture. It is a collection of APIs used by storage vendors to create and deliver specific multipathing and load-balancing plug-ins that are best optimized for specific storage arrays.

To manage storage multipathing, ESX/ESXi uses a special VMkernel layer, Pluggable Storage Architecture (PSA). The PSA is an open modular framework that coordinates the simultaneous operation of multiple multipathing plugins (MPPs).

PSA is a collection of VMkernel APIs that allow third-party hardware vendors to insert code directly into the ESX storage I/O path. This allows third-party software developers to design their own load balancing techniques and failover mechanisms for the particular storage array. The PSA coordinates the operation of the NMP and any additional third-party MPP.

**Native Multipathing Plugin (NMP)** - The VMkernel multipathing plugin that ESX/ESXi provides, by default, is the VMware Native Multipathing Plugin (NMP). The NMP is an extensible module that manages sub plugins.



There are two types of NMP sub plug-ins: Storage Array Type Plugins (SATPs) and Path Selection Plugins (PSPs). SATPs and PSPs can be built-in and provided by VMware, or can be provided by a third party.

If more multipathing functionality is required, a third party can also provide an MPP to run in addition to, or as a replacement for, the default NMP.

VMware provides a generic Multipathing Plugin (MPP) called Native Multipathing Plugin (NMP).

### What does NMP do?

- Manages physical path claiming and unclaiming
- Registers and de-registers logical devices
- Associates physical paths with logical devices
- Processes I/O requests to logical devices:
  - Selects an optimal physical path for the request (load balance)
  - Performs actions necessary to handle failures and request retries

## Objective 1.3.3 Describe Storage Policies

VMware vSphere 7 storage policies usually specify which datastores with what functions and specifications to use when placing VMs. There are several VM storage policies types that can be basically created within vSphere 7.

It is a mechanism that allows the assignment of characteristics of your storage (your datastore) to your VM. Some of your VMs might need faster storage with better DR capabilities (production VMs usually) than the others.

Usually, storage policies allow you to specify where to place your VMs according to the types of datastores you have, the performance they provide, or the DR capability they have.

**VM Storage Policies for host-based data services** - Those ones are basically rules for services provided by your ESXi host. This can be compression and encryption, for example.

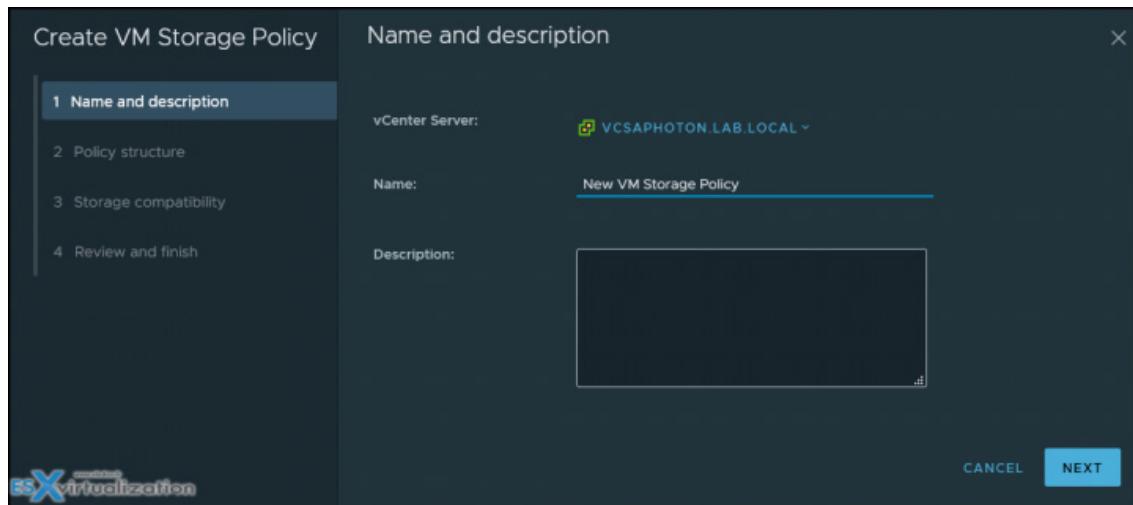
**VM Storage Policies for vVols** - With those policies, you can set rules for VMs that apply to your vVols datastores (if used). You can, for example, have different storage devices, some of them replicated for DR or different performance characteristics.

You can create policies based on the capabilities of your storage array, or you can even create ones using tags. Tag-based rules reference the tags that you assign to the datastores and can filter the datastores to be used for the placement of the VMs.

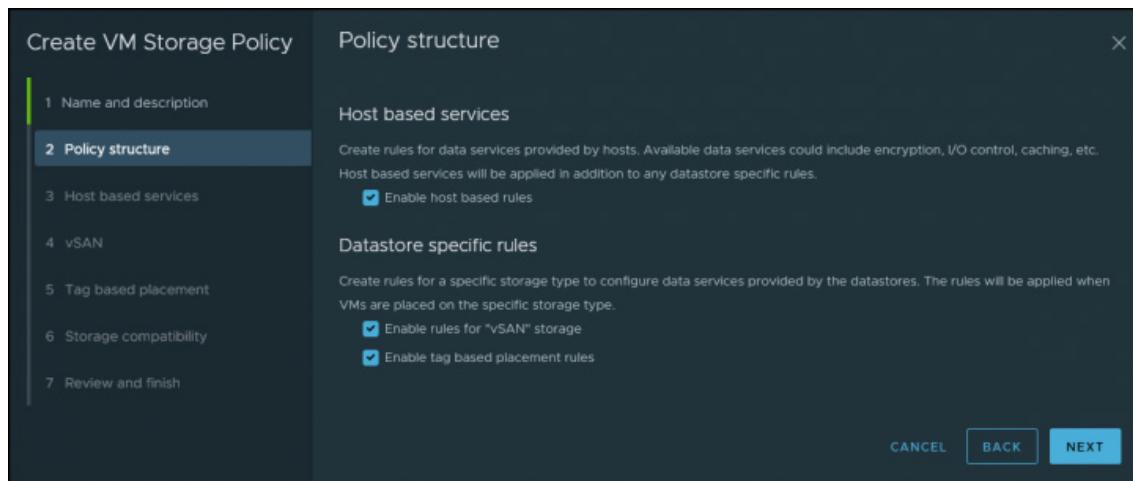
You need to create those policies by yourself to match them with your storage device. You might have a storage array that has hardware acceleration enabled or has some parameters such as minimum latency, that has to be entered concerning storage I/O control. Usually you must check this with your hardware manufacturer.

### Where do I create a storage policy?

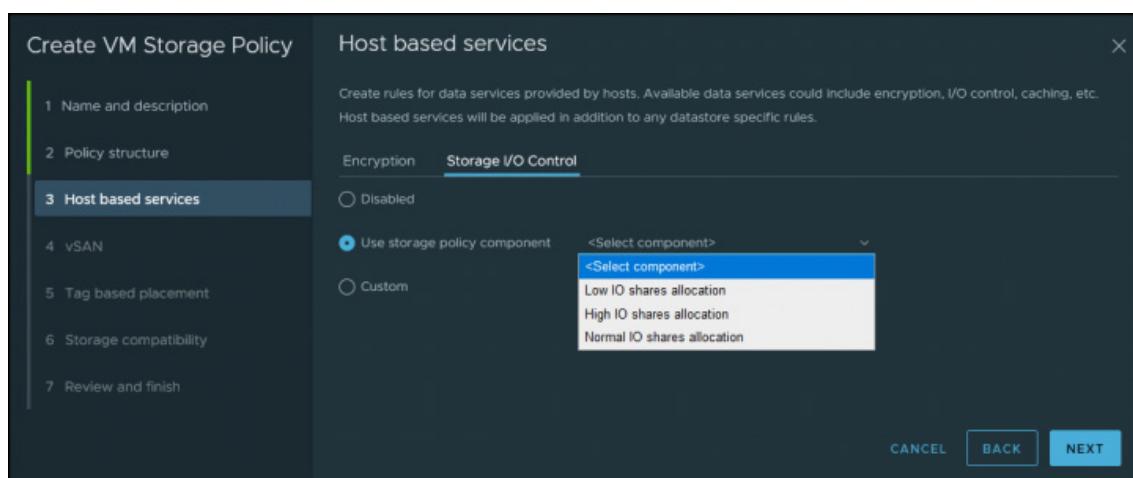
Open the Create VM Storage Policy wizard. Click **Menu > Policies and Profiles**. Under Policies and Profiles, click **VM Storage Policies > Create VM Storage Policy**.



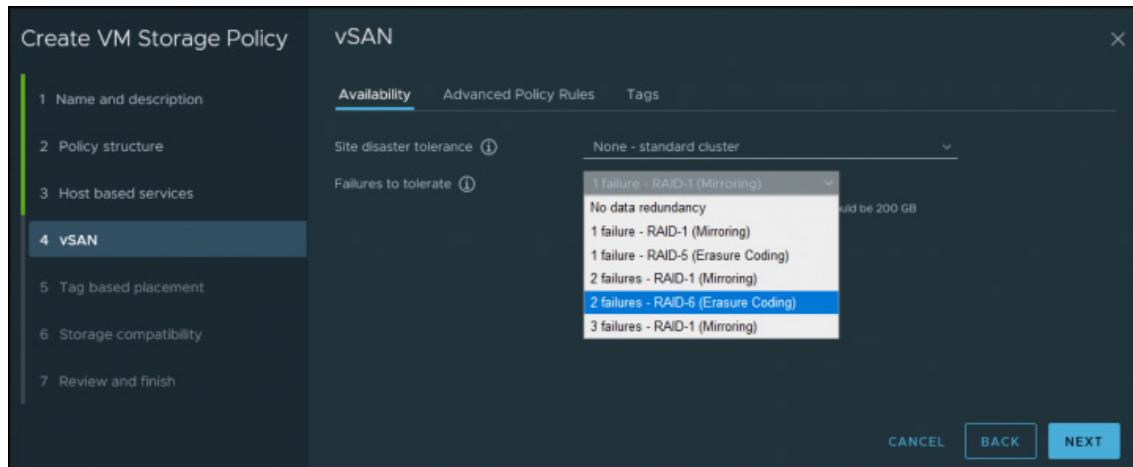
Then click **Next**, and you will be able to specify and enable host-based rules, enable rules for vSAN storage or enable tag-based placement rules.



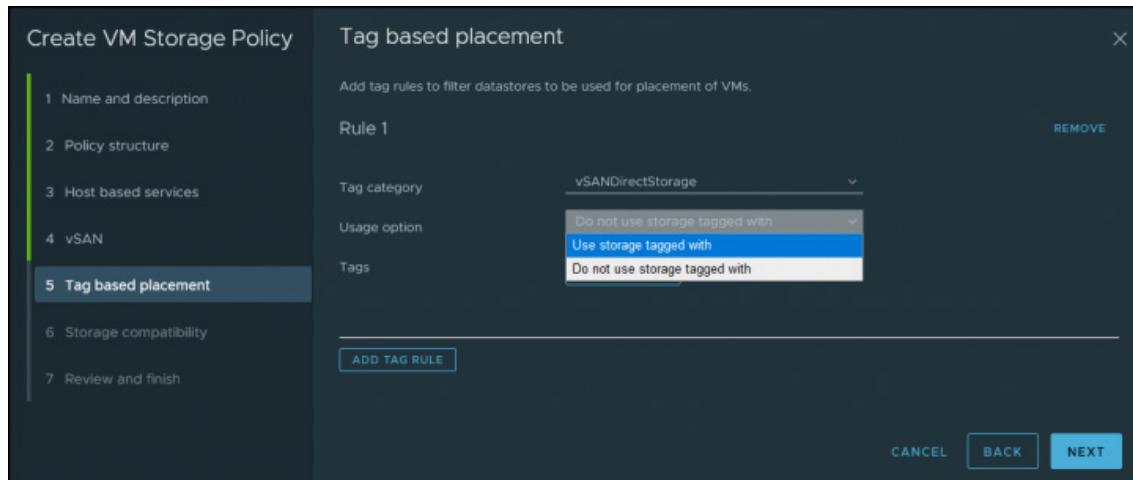
And then you can specify either Encryption or Storage I/O control-based policy creation.



The next screen shows vSAN options where you can choose options for vSAN topology (stretched clusters included) and failures to tolerate. There you can choose what redundancy you want this policy to cover. This can be Raid-1, Raid-5 with erasure coding, or Raid-6 with erasure coding. Each time with 1 or 2, see 3 hosts failures.



If you have checked the tags-based policy, the next screen shows the options there. You can use your tags already created or if you haven't created them, you should go and do that because this is the place where you can select those tags being used with the storage policy.



You can create custom policies for VMs and custom tags for storage devices. This is useful when you, for example, have a storage device that does not support VASA, so you can't see the storage characteristics inside the vSphere client. (Yes, it is VASA that does that).

As an example, you could create a tag named Diamond and use it for your storage that has the best performance.

## Virtual Disk Types

When creating your VM and specify virtual disk, you need to select and specify whether the disk will be thin disk, eager zeroed thick or lazy zeroed thick disk. Let's take a look at those differences below:

**Eager Zeroed Thick** - In this case, you have the disk space allocated and erased (we say zeroed out) during the time of the creation of the file (so it takes more time). If your storage has VAAI support, then the process is fast; if not and the disk creation process cannot be offloaded to the device, it might take a significant time, depending on the size. Best performance disk.

**Lazy zeroed thick** - Here, the disk space is allocated, but not zeroed. It only happens when needed. Each block is zeroed when there is a demand of write.

**Thin provisioned** - In this case, the disk space is not allocated or zeroed during the time of creation. But space is allocated On-Demand only. The performance isn't as good as with thick disks, but the process is immediate. Also, you save space on datastore. (Remember that you should not over-allocate space on a datastore).

## vSAN Specific storage policies

We've talked briefly about those policies during the wizard creation.

**Primary Level of Failures to tolerate (PFTT)** - This policy basically defines how many hosts and device failures VM objects can survive. For "n" failures tolerates, the data is stored in "n+1" locations. This is the default policy.

**Secondary Level of Failures to tolerate (SFTT)** - When used in stretched clusters, this policy defines how many additional host failures can be tolerated after you have a site failure. The number of additional host failures that the object can tolerate after the number of site failures defined by PFTT is reached. If PFTT = 1 and SFTT = 2, and one site is unavailable, then the cluster can tolerate two additional host failures. Default value is 1. Maximum value is 3. Check details in VMware docs [here](#).

**Data locality** - This policy has different options (none, preferred, or secondary), and it allows objects to be limited to one site or one host in a stretched clusters environment. The default setting is none.

**Failure Tolerance Method** - You can define the data replication mechanism. You specify whether you want capacity with RAID-1 (mirroring) or you want performance with Raid-5/6 (with [erasure coding](#)).

**Number of disk stripes per object** - This is the number of capacity devices where each VM replica is striped. Default is 1, but you can set max to 12; however, this consumes more resources.

**Flash Read cache reservation** - Through this policy, you define the size of flash capacity reservation for VM object caching. It's a percentage of the size of the VMDK (only for hybrid vSAN, not All flash).

**Force Provisioning** - Two values, yes/no. When set to yes, the policy forces provisioning of objects even when policy cannot be met. Default = No.

**Object Space Reservation** - Percentage of VMDK objects that must be thick provisioned on deployment.

**Disable object Checksum** - Checksum is used for integrity checks. To make sure that the copies of data spread across a vSAN cluster are identical. If there is a difference, the wrong data is overwritten with correct data. If the policy is set to Yes, the checksum is not calculated. Default = No.

## Objective 1.3.4 Describe Basic Storage Concepts in K8s, vSAN, and vSphere Virtual Volumes (vVols)

With VMware vSphere 7 and Tanzu, there is a new way of using storage. In fact, we have an additional way of using storage now within vSphere. So, I'm going to explain the basic storage concepts in K8s, vSAN, and vSphere Virtual Volumes (vVols).

Many new IT admins that learn VMware technology must face a decision point and storage is one of the areas that every admin must know pretty well, to make wise decisions. Especially with vSphere and Kubernetes, there are some areas that we'll cover.

### VMware vSphere and Kubernetes (K8s)

VMware calls it Cloud Native Storage (CNS), and it is a component that is an extension of the vCenter server management. Through the CNS, you implement the provisioning and lifecycle operations for persistent volumes.

**vSphere with Kubernetes supports three types of storage.**

- **Ephemeral virtual disks** – This storage is temporary. Virtual disk stores objects such as logs or other temporary data. Once the pod does not exist any longer, the disk is gone too. However, this type of disk persists across restarts. Each pod only has one disk.
- **Container Image virtual disks** – This disk has the software that is to be run. When the pod is deleted, the virtual disks are detached.
- **Persistent volume virtual disks** – Certain K8s workloads need persistent storage to save some data that is independent of the pod. The persistent volumes objects are backed by First Class Disks (also called Improved Virtual Disk). This First-Class Disk is identified by UUIDs, which are valid even if the disk is moved elsewhere or snapshotted.

The persistent volumes are usually used for stateful applications. vSphere 7 supports **dynamic** and **static** provisioning of persistent volumes.

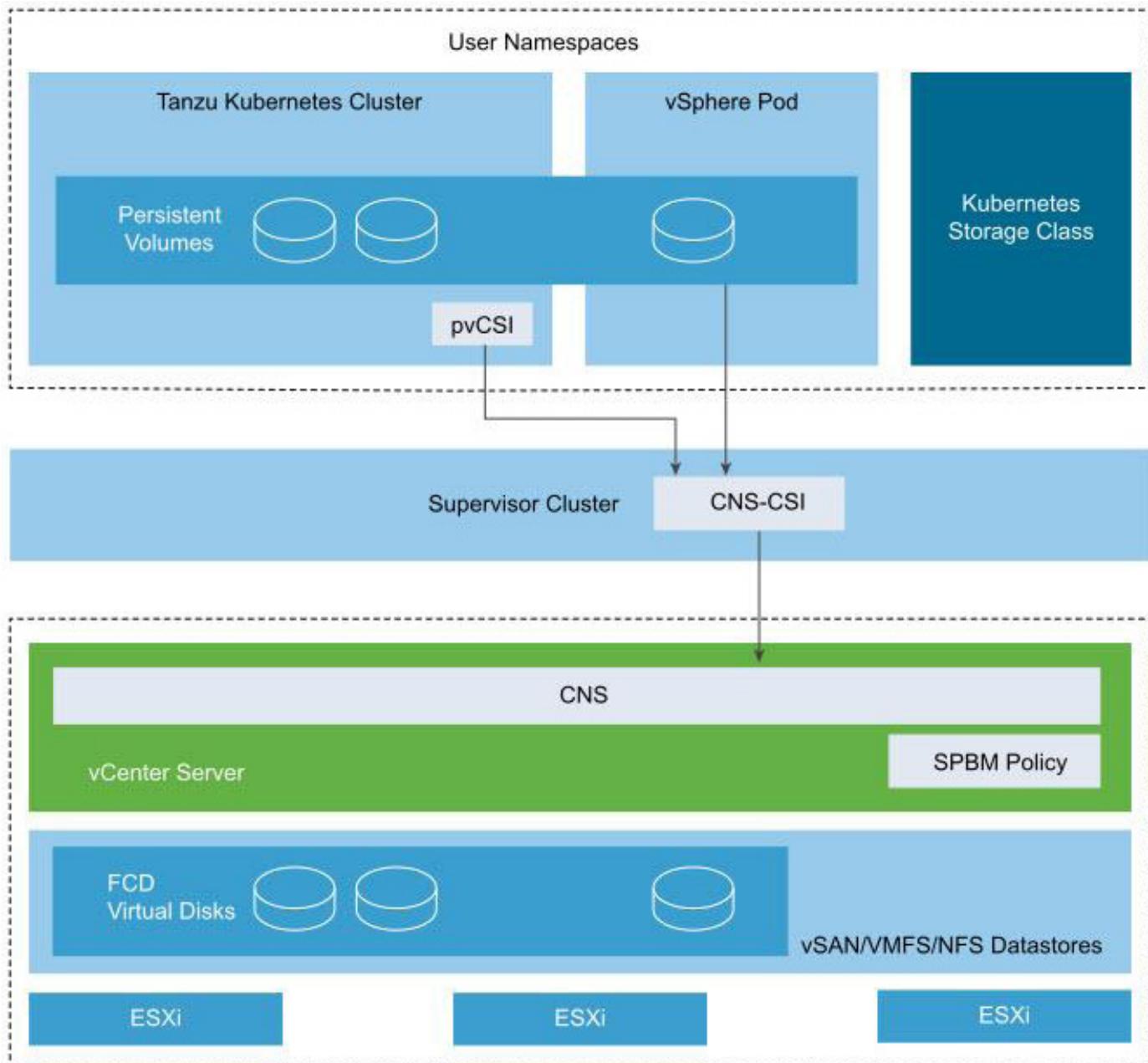
**With Dynamic Provisioning** the storage does not need to be pre-provisioned, and persistent volumes can be created on-demand.

**With Static provisioning**, you are able to use an existing storage object and make it available to the cluster. When you provision a static persistent volume, you basically manually create a virtual disk to use as backing storage for the persistent volume. Only Tanzu Kubernetes clusters support static provisioning.

Now, things get a bit more complex, at least from a terminology perspective. But it's just a new terminology, that's all.

**vSphere CNS-CSI:** Container Storage Interface (CSI) – This component provides an interface to container orchestrators such as Kubernetes on a Supervisor Namespace. The vSphere CNS-CSI is in communication directly with CNS control plane and all the storage provisioning requests that come from vSphere Pods and Tanzu Kubernetes cluster on the namespace.

**Paravirtual CSI (pvCSI)** – This is the vSphere CNS-CSI driver that has been modified for Tanzu Kubernetes clusters. The pvCSI is inside the Tanzu and manages all the storage requests from the Tanzu clusters. It is better to look at these graphics from VMware to understand the different blocks and how they interact with each other.



## vSphere CNS-CSI and pvCSI

## VMware VSAN

If you're new to VSAN, it's a hyperconverged storage system that uses local SSD/HDD to create a pool of shared storage as a single datastore that is available for all host within a vSAN cluster.

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

vSAN is object-based storage that uses policies to enable features needed to protect your VMs. You can use policies to enable multiple copies of data (raid1, etc.), performance throttling, or stripe requirements. Image from the lab shows a single disk group per host composed from a cache and capacity disk.

The screenshot shows the vSphere Web Client interface under the 'Configure' tab. The left sidebar is collapsed, and the main area is titled 'Disk Management'. A message at the top says 'All 6 disks on version 13.0.' Below this are buttons for 'CLAIM UNUSED DISKS', 'ADD DISKS', 'GO TO PRE-CHECK', and '...'. The main table displays disk groups:

Disk Group	Disks in Use	State	Health	Type	Fault Domain
esxi01.lab.local	4 of 4	Connected			
Disk group (52b2e15a-d2e2-c180-2c54-99e33...)	2	Mounted	Healthy	All flash	
vSAN Direct disks	2				
esxi02.lab.local	4 of 4	Connected			

Below the table are buttons for 'ADD DISKS', 'GO TO PRE-CHECK', 'REMOVE DISK', and '...'. A secondary table shows individual disks:

Name	Drive Type	Claimed As	Capacity
Local VMware, Disk (mpx.vmhba0:C0:T1:LO)	Flash	vSAN Cache	50.00 GB
Local VMware, Disk (mpx.vmhba0:C0:T2:LO)	HDD	vSAN Capacity	180.00 GB

## VMware VSAN disk group and cache and capacity disks

## VMware vVols

vVols is quite a different kind of storage compared to traditional types of storage you know, where you would carve storage out into LUNs, and then you would create datastores on them.

The storage administrator has a key role in meetings with the virtualization administrators. In fact, decisions had to be made in advance about storage schemas and layouts.

The traditional datastore layout is also hurting because of another problem, which is that you create a bottleneck per datastore.

When you have multiple VMs that are stored and executed on the same datastore, and if they have different IOPs required different things, you can of course use Storage IO control, but this is a per-datastore level option.

With vVols, things are different. It has granular control that helps you to bring storage functionality to the needs of individual VMs. vVols map virtual disks and different pieces, such as clones, snapshots, and replicas, directly to objects called virtual volumes, on a storage array.

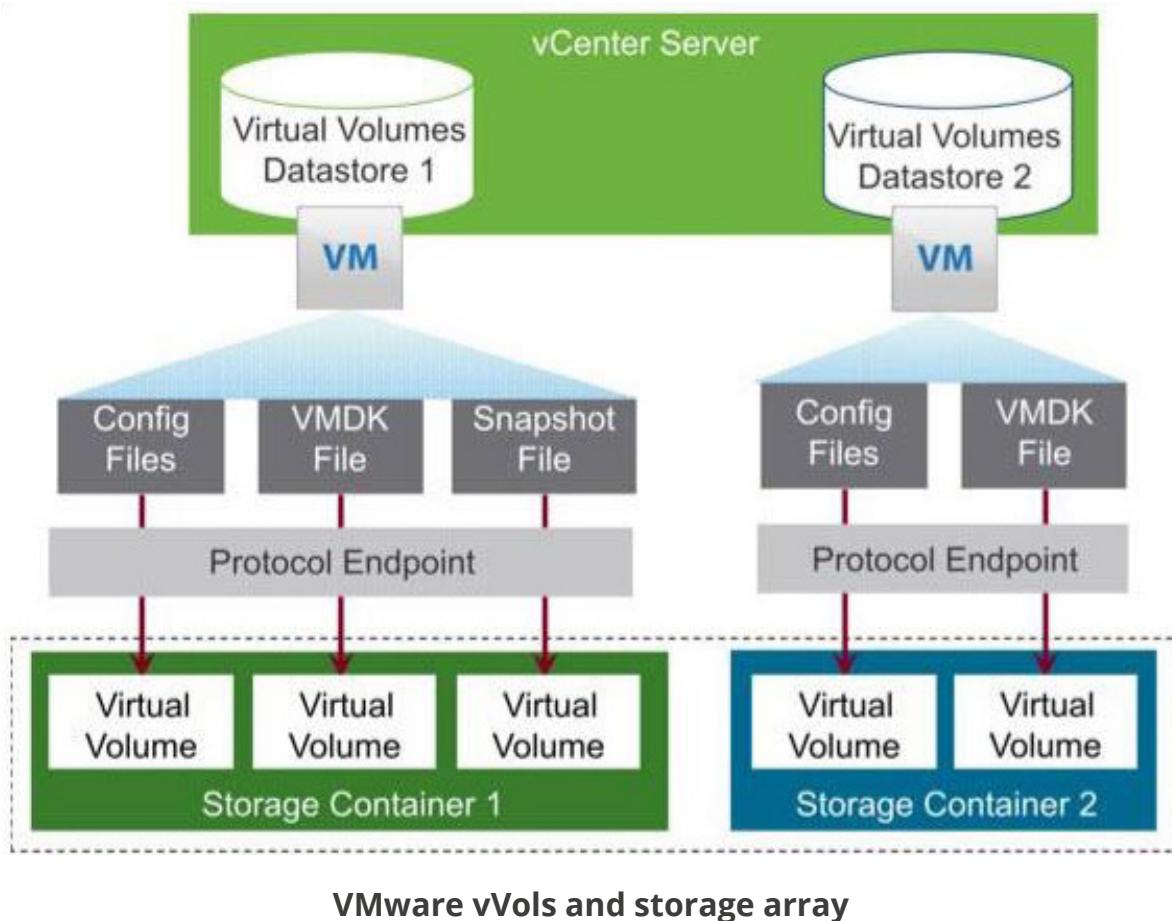
This helps vSphere to offload tasks such as cloning and snapshots to the storage array. You save some CPU cycles by doing that. And because you are creating individual volumes for each virtual disk, you have the possibility to apply policies at a very granular level. You have easier control of the performance via policies.

vVols creates a minimum of three virtual volumes: the data-vVol (virtual disk), config-vVol (config, log, and descriptor files), and swap-vVol (swap file created for VM memory pages). You can also let it create more virtual volumes, but this depends on the features you're using. Those can be features such as snapshots or read-cache, etc.

vVols start by creating a Storage Container on the storage array. The storage container is a pool of raw storage that the array is making available to vSphere. Once done, you register the storage provider with vSphere.

You can then create datastores in vCenter and create storage policies for them. All you need to do next is to deploy VMs to the vVols.

Let's find some pictures of vVols from VMware.



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

Network I/O control allows you to determine and shape the bandwidth within vSphere. You can use it together with Network Resource pools that allow you to specify the bandwidth for a specific type of network traffic. You'll need an Enterprise Plus license where you leverage vSphere Distributed Switches and NIOC.

The section of Resource allocation is divided into a System traffic and Network resource pools. You can access those sections by selecting the **vSphere Network** icon > under data center, where you have your **vDS > Configure > System traffic**.

You can use NIOC for Quality of Service (QoS) on network traffic. This can be useful for vSAN when vSAN traffic must share the physical NIC with other traffic types, such as vMotion, management, virtual machines.

Version 3 of the Network I/O Control (NIOC) feature offers improved network resource reservation and allocation across the entire switch. vSphere NIOC v3 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.

When enabled NIOC divides the traffic into resource pools. Bandwidth reservations can be used to isolate network resources for a class of traffic. For example, in VSAN cluster you would want to reserve part of the traffic only for VSAN traffic no matter what happens to the other traffic.

**Models for Bandwidth Resource Reservation** – Network I/O Control version 3 supports separate models for resource management of system traffic related to infrastructure services, such as vSphere Fault Tolerance, and of virtual machines.

**The system traffic** section - Here you can configure shares, reservations, and limits for your system-based network traffic.

- Management networking traffic
- Fault tolerance (FT)
- NFS
- vSAN
- vMotion
- vSphere replication
- vSphere data protection backup
- Virtual machine

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

**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. Each traffic 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** – This is 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, 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.

**Network Resource Pools** - This section is for controlling the VM traffic.

By clicking the Network resource pools menu link and then clicking Add, you create a new network resource pool that will have a reservation quota. You can then assign a VM to that pool.

**Bandwidth Guarantee to Virtual Machines** – Network I/O Control version 3 provisions bandwidth to the network adapters of virtual machines by using constructs of shares, reservation, and limit. Based on these constructs, to receive sufficient bandwidth, virtualized workloads can rely on admission control in vSphere Distributed Switch, vSphere DRS, and vSphere HA.

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.

You can enable Network I/O Control in the configuration properties of the vDS. Right-click the vDS in the vSphere Client, and choose menu **Settings > Edit Settings**.

You can check and monitor Network I/O Control through vSphere web client. **Networking > vDS > Manage > Resource Allocation**

Concerning the system traffic, it's possible to have a look at those metrics and details:

- Network I/O Control Status (state is Enabled/Disabled)
- NIOC Version
- Physical network adapters details
- Available bandwidth capacity
- Total bandwidth capacity
- Maximum reservation allowed
- Configured reservation
- Minimum link speed

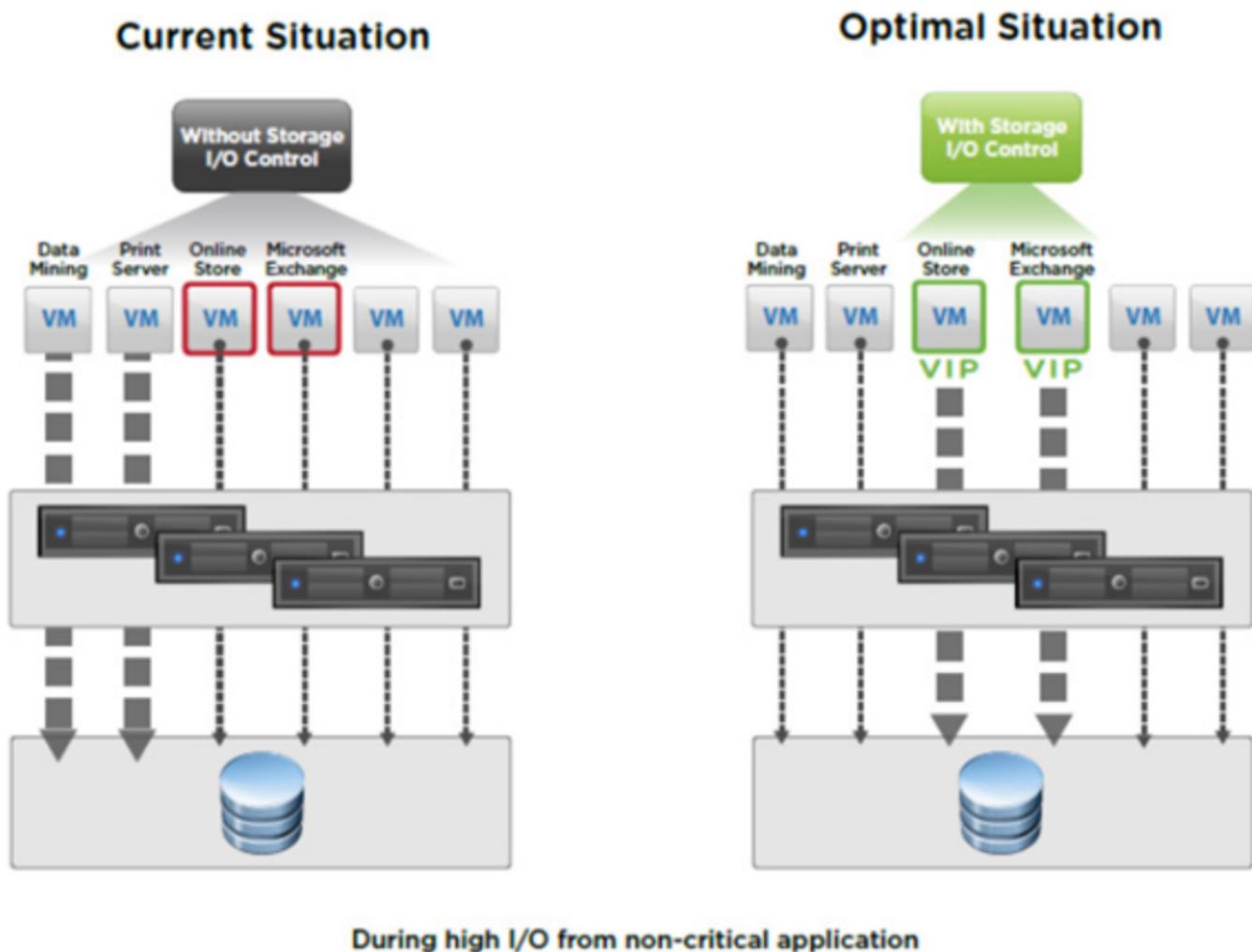
### vSphere 7 SIOC (Storage I/O control)

With SIOC enabled on a datastore, you prevent the other VMs from the "**noisy neighbour**" situation where a single VM takes all the resources. The device's latency is monitored. If latency is higher than configured values, SIOC kicks in and reduces the latency by throttling back VMs that are exceeding their consumption of IOPS.

Storage IO Control (SIOC) only kicks in when there is a 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). You know the "noisy neighbour story".

When you enable Storage I/O Control on a datastore, 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 that 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. You can adjust the number for each based-on need. The default is 1000.



### Limitations and Requirements:

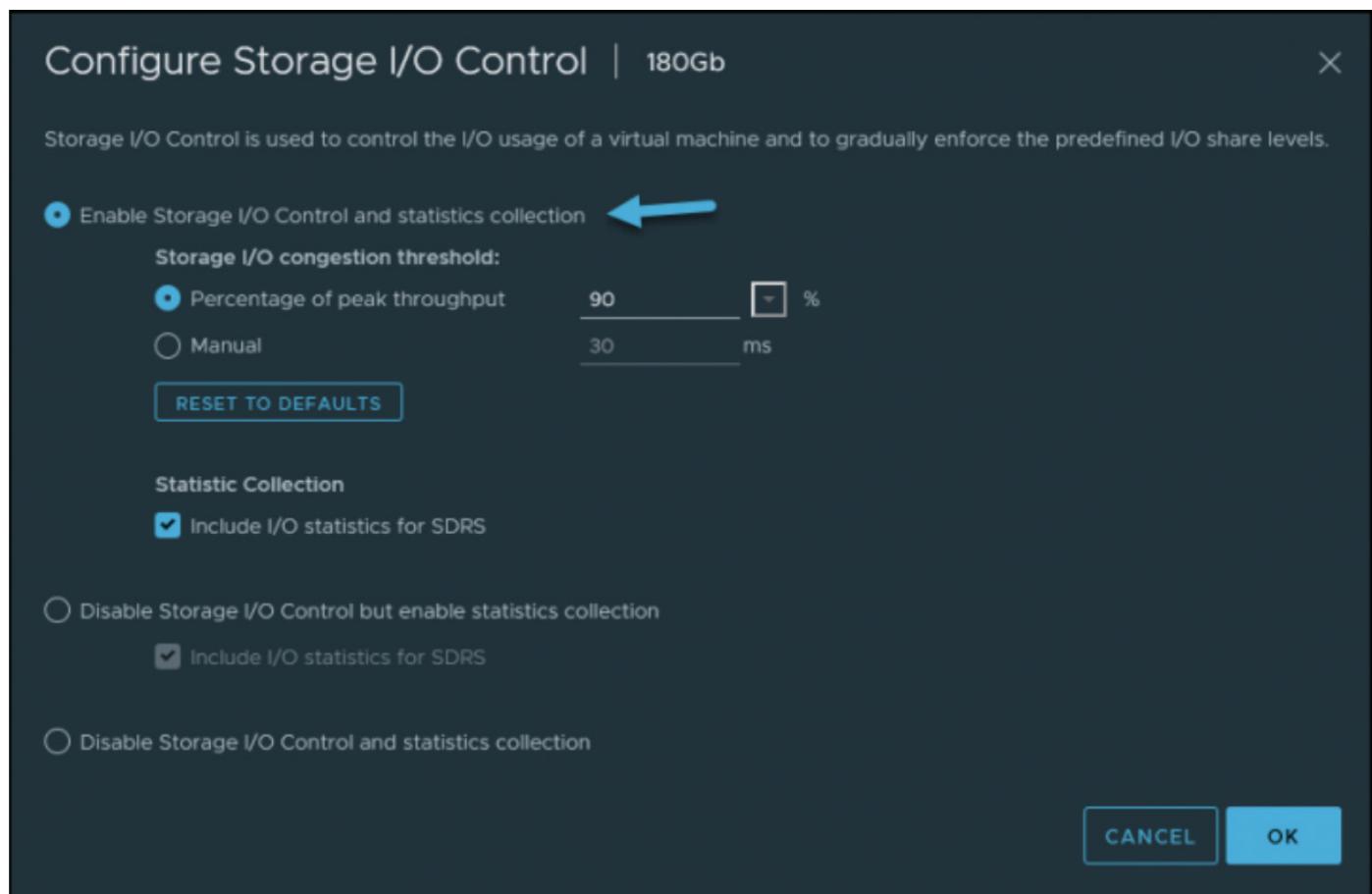
- NFS v4.1 isn't supported (it is for NFS v3).
- Storage I/O Control does not support datastores with multiple extents.
- SAN with auto-tiering has to be certified for SIOC.
- Datastores that are Storage I/O Control-enabled must be managed by a single vCenter Server system.
- Must be disabled before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

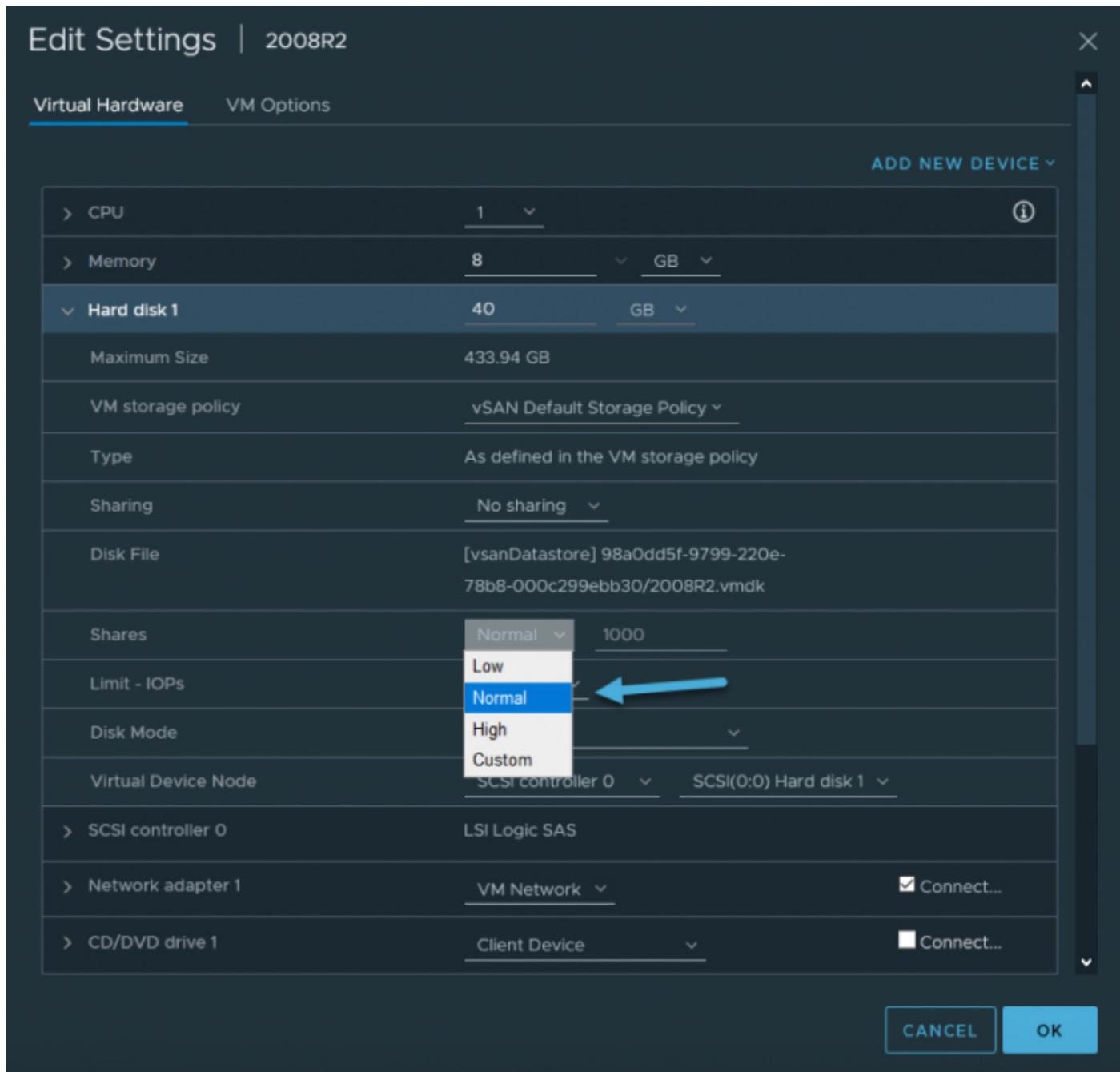
When you enable Storage I/O Control (SIOC) on a datastore, the host starts to monitor the latency. When latency on the datastore with enabled SIOC is more than the configured threshold, vSphere views the data store as “congested”, and each VM that is accessing the SIOC enabled datastore is allocated 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 with 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.

# Objective 1.5 Describe instant clone architecture and use cases

VMware Instant Clone architecture was started via Project Fargo during VMworld 2016. It slowly made it into the VMware Horizon Desktop architecture as a complementary and innovative cloning technology that is faster and more efficient than traditional cloning via VMware composer.

The first instant clone architecture release was with vSphere 6.7. However, it did not enable creating clones via the user interface. They could only be created through PowerCLI or API and via the Horizon VDI.

## Instant Clone architecture

Instant clones use a copy-on-write architecture similar to that of containers, which means that when 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.

All modifications inside the VM are isolated within this VM only. If there are some new files created within that particular VM, those files are also saved within the VM and, as such, are also stored in the child VM and not in the parent.

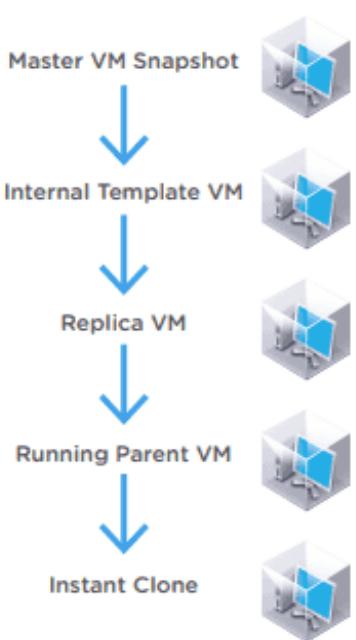
**Master VM:** Golden image of your OS, patched, and its applications installed. Once finalized, create a VM snapshot.

**Internal Template VM:** When creating a desktop pool, Horizon creates a template, which is a linked clone VM from your golden image.

**Replica:** The same as a linked clone replica. It is a thin provisioned full clone of the template VM. It will be used for read access for all the instant clone desktops.

**Parent VM:** The final copy of the original VM that will be used to “fork” (to clone) the running VMs. Parent VM exists on each ESXi host within the horizon cluster. This VM is a running VM, as we’re creating instant clones from running VMs.

**Instant Clones VM:** The final product, a running VM based on the provisioning configuration. It can be provisioned on demand because its creation takes just a couple of seconds.



### VMware Instant Clone workflow

- An instant clone is created from a running parent VM.
- Each instant clone is immediately accessible.
- Changes to the VM (its files or filesystem) don't affect the shared data and memory of the running parent VM on which all other instant clones are based.
- An instant clone is created when sharing the memory of a running parent VM (just a few secs) and then immediately powered on. The instant clone requires no boot time.
- The running parent VM can be deleted because after creation, the clone is linked to the replica VM and not to the running parent VM.

## Use cases

One of the most obvious use cases for Instant Clone technology is virtual desktop infrastructure (VDI) desktops. Administrators can quickly provision from a parent virtual machine whenever new desktops are needed.

Instant clones are also accessible via PowerCLI extensions. Extensions give PowerCLI admins access to this technology and create linked clones within VMware vSphere, without an installation of Horizon View. Instant Clone uses a private API, so admins can use PowerCLI cmdlets to explore this technology.

**Note:** Just a side note here. It's not possible to use traditional clones and instant clones side by side. It is one or the other.

## Benefits compared to View Composer clones

**No need to maintain:** When a user logs out of the desktop, that desktop always gets deleted and recreated as a fresh image from the latest patch. The admin only needs to maintain the master image patched and updated. This eliminates many previous operations that every Horizon admin knew—refreshing, recomposing, and rebalancing desktops after the master image was patched.

**Image updates scheduled during business hours:** You can schedule desktop pool image changes during business hours so that when your users log in, they receive a freshly updated desktop. Users who are logged in their desktops during the day continue to use their desktop without the need to log out. They receive the update the next day with a completely new desktop.

**No need for a database:** When traditional clones were used via View Composer, a database was required, which was usually installed on a separate VM. This component is completely eliminated from the linked clone's architecture. Less maintenance, fewer updates, less work.

**Speed:** Instant clones are fast. During testing, VMware realized that the average time to create a new VM via Instant Clone was about 10 times shorter. For example, to create a new desktop pool of 1000 VMs, compared to 170 min via traditional desktop clone technology, the instant-clone technology took only 25 min to create the same number of desktops.

## How to set up Instant Clones in VMware Horizon View?

The Instant Clones are easy to set up. Instant Clones are created in a powered-on state. The desktops are ready for users to connect to. Part of the initial workflow is also guest customization and joining the Active Directory domain.

There are two main phases:

- **Preparation of the MASTER IMAGE VM**

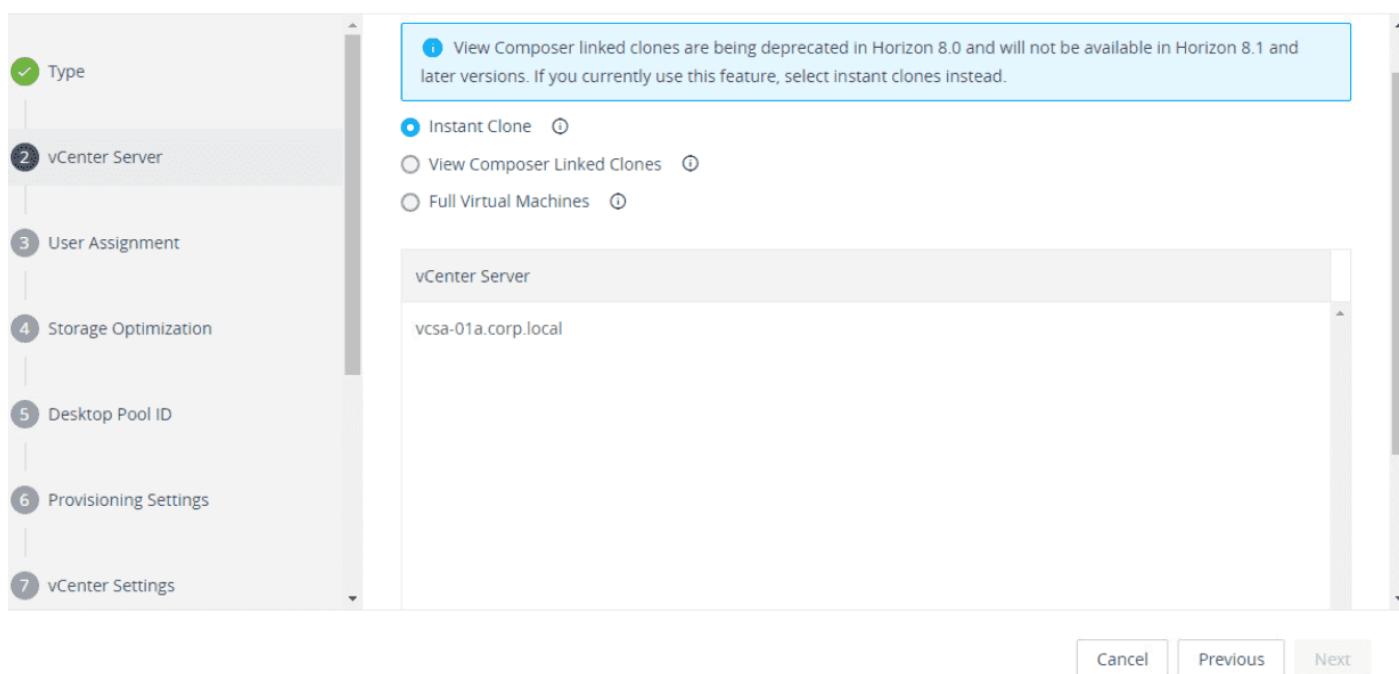
First, create the parent VM and install an operating system (Windows 7 or Windows 10). Optimize your system image following best practices, and activate with a volume license key.

Then install VMware Tools. Install the Horizon Agent, and select the Instant Clone component. Install any applications and any system updates you wish. Then shut down the parent VM and take a snapshot. Give the snapshot a meaningful name.

- **Create an Instant Linked-Clone Pool**

Connect to the View Admin UI, and select **Inventory > Desktops > Add New Desktop pool**.

Add Pool



## Create an Instant Clone Desktop Pool in Horizon View

Select your **vCenter Server** and click **Next**. Select **Floating** and click **Next**. Then continue the wizard to configure all the other required steps. I won't detail those steps here.

At the end, you should have your instant desktop pool available with the required number of desktops running.

The final result of an Instant Clone operation is basically a VM (called destination VM), which has the processor state, virtual device state, memory state, and disk state identical to those of the source VM.

The virtual hardware of the VMs, including the MAC addresses or a serial port configuration, can be customized during the cloning process.

## Objective 1.6 Describe ESXi Cluster Concepts

Now I'll cover the basics of ESXi clusters. The basics of ESXi cluster is fairly simple. Those ESXi hosts can work together as one. Their resources are shared and become part of the clusters' resources.

Within a cluster, you can configure services and enable features, such as VMware HA, vMotion, [vSphere Distributed Resource Scheduler](#) (DRS) or [vSAN](#). You manage the resources within the vSphere web client UI as single objects.

VMware Enhanced vMotion Compatibility (EVC) when enabled, can help you make sure that migrations with vMotion do not fail if the CPUs on different hosts within your cluster are not identical.

With DRS, you can allow automatic resource balancing by using the pooled resources within the cluster. With vSphere HA, you basically prevent downtime in case you have a hardware failure. In fact, when one host fails, the VMs are restarted on other hosts within the cluster automatically, without the admin needing to do anything.

With vSAN, you can use the internal disks of each host and create a shared datastore that is used by your VMs. A minimum of 2 hosts are required, with a third host hosting the witness components. You can scale up to 64 hosts.

Within your cluster you can choose to manage all hosts in the cluster with a single image. This is new in vSphere 7.

With this option, all hosts in a cluster use the same image, and that reduces variability between hosts and helps improve and ensure hardware compatibility. It also simplifies upgrades.

## 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.

### 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 HA works?

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.

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 “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 Heart beating. 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.
  - **Shutdown and restart VMs** – All affected VMs will be gracefully shutdown, 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 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

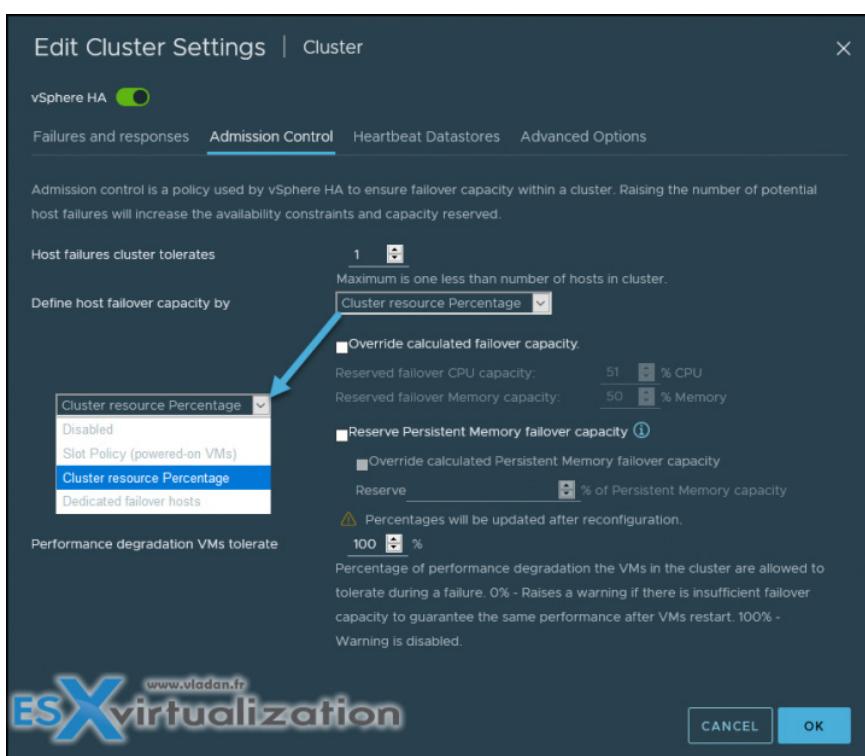
Admission control is a policy which is used by vSphere HA to make sure that there is enough failover capacity within a cluster.

- **Cluster resource Percentage (default)** – The configuring workflow for admission control is a little bit simpler. You first define a parameter for 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 host failures 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 VMs, but those would suffer from performance degradation. Now you have a warning message that informs you about it. You'll be warned if performance degradation would occur after an HA even for a particular VM(s).

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

100% – Warning is disabled

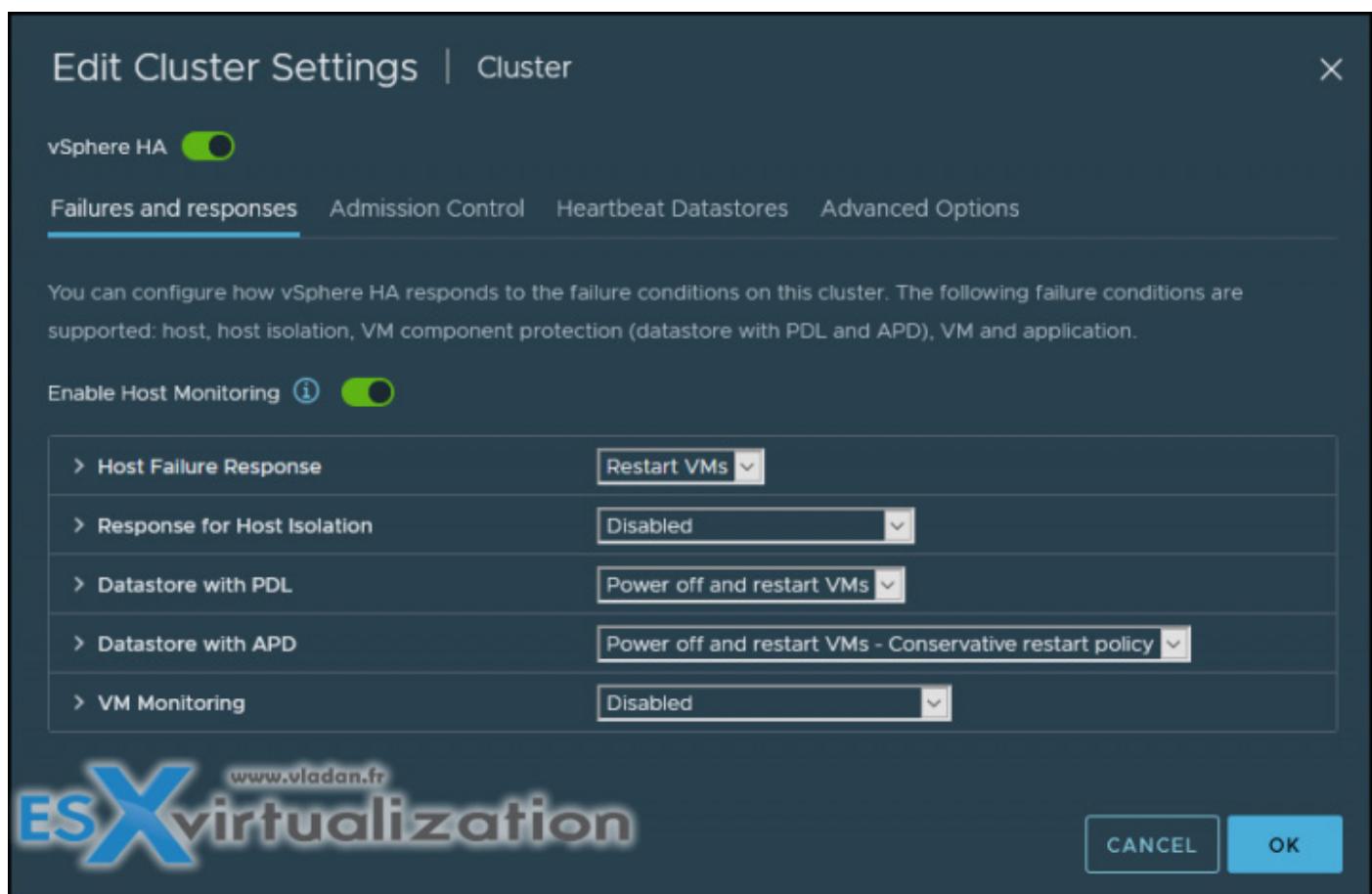


Other than cluster resource percentage policy there are “Slot policy” and “Dedicated failover host” policies.

- **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 resources.

## Enable/disable vSphere HA settings

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



## Objective 1.6.1 Describe Distributed Resource Scheduler (DRS)

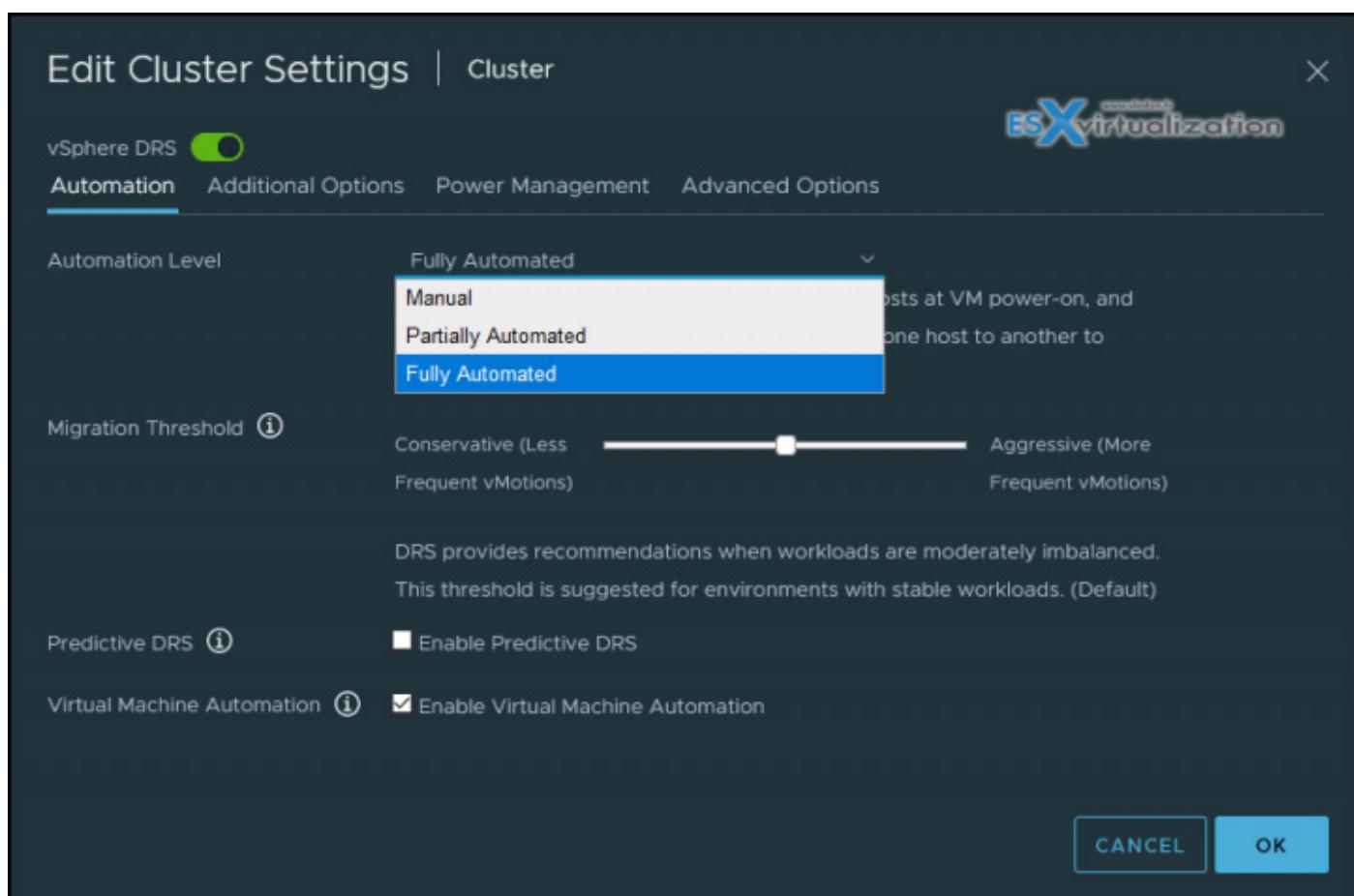
VMware vSphere has a Distributed Resource Scheduler (DRS) allowing automatic VM placement and vMotion. The purpose of DRS is to make VMs “happy” so they run smoother. DRS can be set to automatically move VMs based on its algorithms, or be set to manual and give recommendations for manually moving VMs.

In vSphere 7.0, DRS uses a new cost modelling algorithm that is flexible and balances network bandwidth together with CPU and memory usage. There is a metric called granted memory, which is used for load balancing.

DRS runs once every minute rather than every 5 minutes, as is the case in previous vSphere releases. The newer DRS versions do recommend smaller (in terms of memory) VMs for migration to facilitate faster vMotion migrations. The older DRS versions tend to recommend large virtual machines to minimize the number of migrations.

With vSphere DRS enabled cluster, you can set your DRS to Manually, Partially Automated, or Fully Automated. The configuration is accessible at the cluster level. You **select your cluster > Configure > vSphere DRS**.

You'll get to this view where you can click Edit to change the settings.



- **Manual** - DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.
- **Partially Automated** - DRS automatically places virtual machines onto hosts at VM power-on. Migration recommendations need to be manually applied or ignored.
- **Fully Automated (default)** - 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.

In the middle, you can drag the Migration threshold bar. Migration Threshold specifies how aggressively DRS recommends vMotions. Recommendations are generated automatically based on resources demanded by the virtual machines, resource allocation settings (reservations, limits, and shares), the resources provided by each host, and the cost of migrating VMs.

The more conservative the setting, the less frequent the vMotions. When you drag the button to the right it will be in Aggressive mode, and DRS provides recommendations when workloads are even slightly imbalanced, and marginal improvement may be realized. For dynamic workloads, this **may generate frequent vMotion** recommendations.

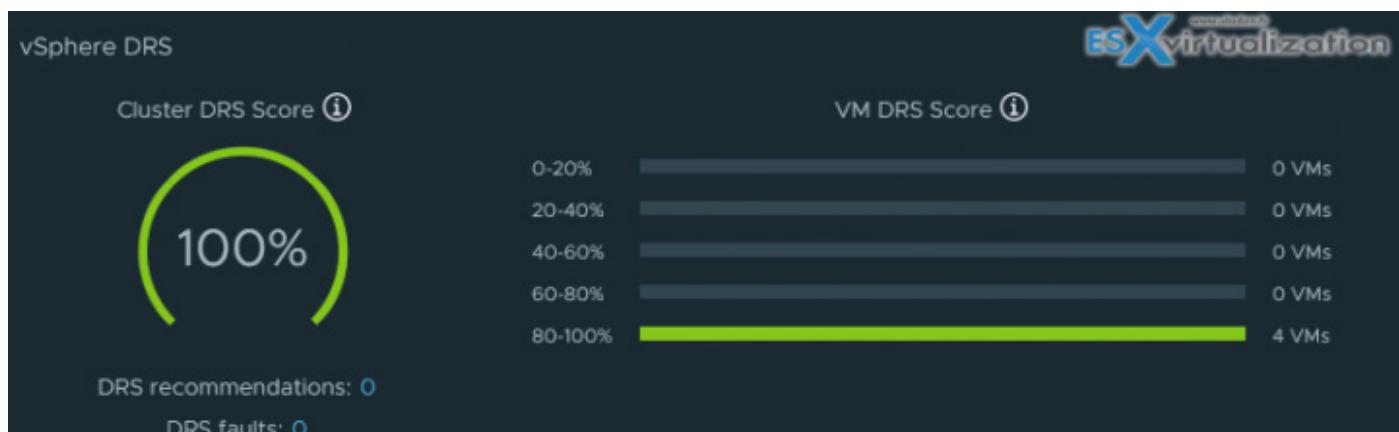
## Other Options - Predictive DRS

In addition to real-time metrics, DRS will respond to forecasted metrics provided by vRealize Operations Manager. Only forecasted metrics with high confidence will be considered by DRS to balance the cluster's workloads prior to predicted utilization spikes and resource contention. You must also configure Predictive DRS in a version of vRealize Operations that supports this feature.

**VM Automation** - Override for individual virtual machines can be set from the VM Overrides page.

## What is the VM DRS Score?

It is the execution efficiency of this virtual machine. Values closer to 0% indicate severe resource contention while values closer to 100% indicate mild to no resource contention. DRS will try to maximize the execution efficiency of each virtual machine in the cluster while ensuring fairness in resource allocation to all virtual machines.



A DRS score is a measure of the resources available for consumption by the VM(s). The higher the DRS score for a VM, the better its resource availability. DRS moves VMs to improve their DRS scores. DRS also calculates a DRS score for a cluster, which is a weighted sum of the DRS scores of all the virtual machines in the cluster. In Sphere 7.0, DRS calculates the core for each virtual machine on each ESXi host in the cluster every minute.

The calculation of an ideal throughput is executed by the DRS logic and an actual throughput for each resource (CPU, memory, and network) for each VM.

The VM's efficiency for a particular resource is a ratio of the goodness over the demand. A virtual machine's DRS score (total efficiency) is the product of its CPU, memory, and network efficiencies.

DRS applies resource costs during those calculations. There are costs for CPU cache, CPU ready, and CPU tax. Same for memory where DRS takes into account the costs for memory burstiness, memory reclamation, and memory tax.

There are also network resources costs as well as utilization involved. DRS does the comparison of the VM's DRS score for the host where the VM is currently running on. The DRS system makes sure that the host where it actually runs can provide the best DRS score for that particular VM. If not, it calculates migration costs. If all those factors match, and the system sees better DRS score on another host, it makes the vMotion recommendation.

## DRS and Affinity Rules

[The VMware documentation covering VM-Host Affinity Rules](#). You can find there how to add host affinity must rule. Basically, the VM-host affinity rule specifies whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on").

VM-VM affinity and anti-affinity rules are similar. They specify if selected VMs should run on the same host or be kept on separate hosts. These rules are typically used to create affinity or anti-affinity between individual VMs.

Watch out for conflicts here, because you can have multiple VM-VM affinity rules in different directions causing conflicts. For example, you can have one rule that keeps 2 VMs on separate hosts, while another rule puts them together. You need to select one of the rules to apply and disable or remove the rule that's in conflict.

## Objective 1.6.2 What is VMware Enhanced vMotion Compatibility (EVC)

VMware Enhanced vMotion Compatibility (EVC) is a vSphere cluster feature which allows virtual machines (VMs) to use [vMotion](#) between hosts with different processors (CPUs). The way that EVC works is basically masking the advanced capabilities of the newer CPUs in order to have the same level of instructions across the whole [VMware cluster](#).

As you know, the vMotion usually fails when a VM runs on a host with Haswell-based CPU, and the destination host is, let's say, newer Broadwell-based CPU. It is necessary to put in place VMware EVC first, and then vMotion can succeed.

### Quote from VMware:

vCenter Server's CPU compatibility checks compare the CPU features available on the source host, the subset of features that the virtual machine can access, and the features available on the target host. Without the use of EVC, any mismatch between two hosts' user-level features will block migration, whether or not the virtual machine itself has access to those features. A mismatch between two hosts' kernel-level features, however, blocks migration only when the virtual machine has access to a feature that the target host does not provide.

Interesting to know that, by default, it is **vCenter Server** component that identifies mismatches on features accessible to applications as incompatible.

### ESXi but also vCenter server

EVC capabilities of your server are based on two factors:

- The version of vCenter Server that manages the host
- The underlying CPU architecture of the host processor

### What's an Advantage of VMware Enhanced vMotion Compatibility (EVC)?

While your hardware evolves year after year, it's convenient to still be able to add a new host to the cluster and be able to vMotion your VMs across your cluster, right? It is very flexible compared to a situation where only exactly the same CPUs would be required in order to assure vMotion compatibility. You can reuse older hardware to maximize ROI and take an advantage of its resources.

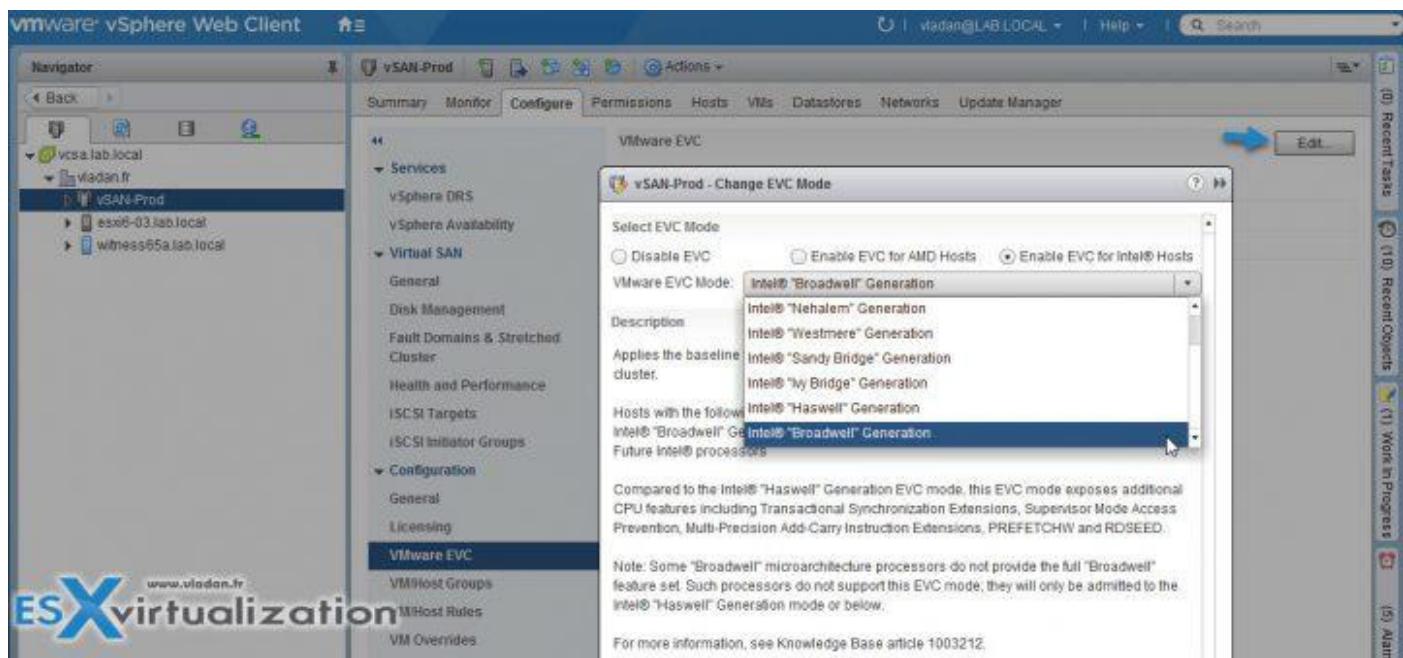
### Any Inconveniences? Drawbacks?

Usually, newer CPUs have a newer set of instructions, and are more performant and more efficient. Your applications might take a real benefit to using them perhaps, but if EVC is applied and "downgrades" the level to a point where those instructions are not showing, obviously, your applications might run a little bit slower than they would if they had the underlying CPU.

## Where to configure VMware Enhanced vMotion Compatibility (EVC)?

At the **cluster level** > **Select the cluster** > **VMware EVC** > **Edit** > **Chose a radio button** depending on your processor family (Intel/AMD) and then **drop down the menu** to choose which CPU family you want to choose from.

When you configure EVC, you configure all host processors in the cluster to present the feature set of a baseline processor. This baseline feature set is called the **EVC mode**.



Think of EVC as a “layer” that levels down all CPUs of the cluster to a level that is “acceptable” for the “lowest” equipped host within the cluster. Usually, it is the oldest host. I remember a few years back, one of my older Nehalem-based white boxes was the oldest, and I was trying to use vMotion with a [Haswell box](#).

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs.

## VMware CPU/EVC Matrix

You can check the VMware compatibility guide page related to CPU where you can find if your CPU within your cluster is compatible with a version of ESXi/vCenter server deployed. The online tool allows you to select the version of ESXi, the CPU type, and then by clicking the CPU/EVC Matrix, you can see that Haswell EVC mods aren't available for the E5-2400 v2 series of CPU.

The shortcut:

<http://www.vmware.com/resources/compatibility/search.php?deviceCategory=cpu>

## VMware Compatibility Guide

[http://www.vmware.com/resources/compatibility/search.php?  
deviceCategory=cpu](http://www.vmware.com/resources/compatibility/search.php?deviceCategory=cpu)

The screenshot shows the VMware Compatibility Guide search interface. At the top, there is a search bar with placeholder text '(e.g. compatibility or esx or 3.0)', a 'Search' button, and a 'All Listings' dropdown. Below the search bar, a message says 'Looking for a simplified search? Use the Guided Search Wizard'. The main area has four filter sections: 'Product Release Version' (with 'ESXi 6.5' selected), 'CPU Series' (with 'Intel Xeon E5-2400-v2 Series' selected), 'Enhanced vMotion Capability Modes' (with 'All'), and 'Fault Tolerant Compatible Sets' (with 'All'). Below these filters are two dropdown menus: 'CPU Capabilities' (with 'Supports SMP-FT' selected) and 'Fault Tolerant Compatible Sets' (with 'All'). At the bottom of the filter section are three buttons: 'Update and View Results', 'CPU / EVC Matrix' (which is highlighted with a blue arrow), and 'Reset'. A large blue arrow points from the 'CPU / EVC Matrix' button down to the matrix table. The matrix table has columns for Enhanced vMotion Capability Modes (Intel® Ivy-Bridge Generation, Intel® Haswell Generation, Intel® Sandy-Bridge Generation, Intel® Merom Generation, Intel® Penryn Generation, Intel® Nehalem Generation, Intel® Westmere Generation) and rows for two CPU series: Intel Xeon E5-2400-v2 Series and Intel Xeon E5-2600-v3 Series. Green checkmarks indicate compatibility across all modes for both series. The 'ESX virtualization' logo is in the bottom right corner of the matrix table.

Enhanced vMotion Capability Modes	Intel® Ivy-Bridge Generation	Intel® Haswell Generation	Intel® Sandy-Bridge Generation	Intel® Merom Generation	Intel® Penryn Generation	Intel® Nehalem Generation	Intel® Westmere Generation
Intel Xeon E5-2400-v2 Series	✓		✓	✓	✓	✓	✓
Intel Xeon E5-2600-v3 Series	✓	✓	✓	✓	✓	✓	✓

VMware EVC was introduced a long time ago, but it still adds a great value to VMware clusters which are able to use vMotion operations within hosts with different types of CPUs (Intel or AMD, not boths). The EVC feature makes sense for licensing packages using vMotion, which is the case of VMware [vSphere Essentials PLUS](#) or Essentials Plus Term (cheaper but limited in time for 12 months).

### Sources:

- Enabling EVC on a cluster when vCenter is running in a virtual machine (1013111).
- vMotion CPU compatibility requirements for Intel processors

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

With the release of VMware vSphere 7, there has been a new, redesigned Distributed Resource Scheduler (DRS) release as well. It completely changes the way it previously worked by introducing scoring for virtual machines (VMs). This scoring is a determinant value for the DRS system.

Based on the score of each VM running on a particular host, the DRS can move the VM to another host, where the score might be better and the workload would be “happier”—yes, the workload’s actual happiness, meaning that the workloads can consume the resources they are entitled to.

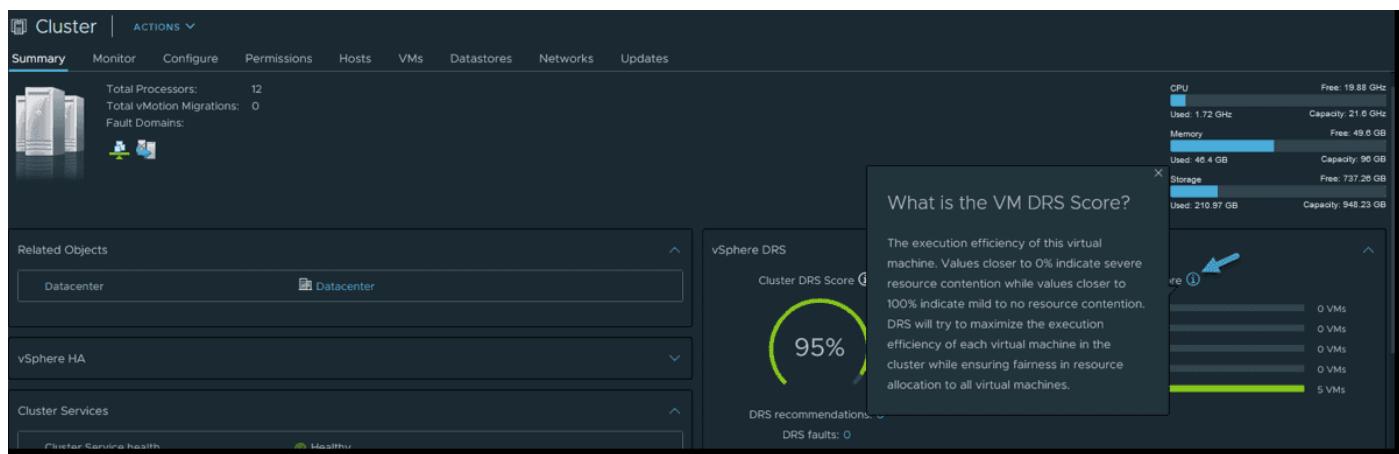
The DRS calculates intelligent workload placement and balancing across clusters by vMotioning VMs to hosts that can ensure better DRS scores. Internally, the DRS uses a placement decision and evaluates current performance. The DRS calculates a what-if scenario on a different host and verifies the cost of VM migration.

If the result is positive, and the VM could benefit from a better host that is run more efficiently, the DRS performs a vMotion to the new host. The new focus of these calculations is for the highest VM DRS score—the highest instance on which the VM’s resource requirements are being met.

vSphere 6.x and earlier releases used a different model that was cluster-centric. The focus was on hosts and the utilization of host resources.

### Cluster DRS score vs. VM DRS score

In fact, vSphere 7 has two notions. There is a VM DRS score and a cluster DRS score. What is the cluster DRS score? It is the average DRS score of all the virtual machines in the cluster. You can see an overview of the cluster DRS score and the VM DRS score in the summary of each of your clusters.



vSphere 7 VM DRS Score

## VM DRS score details

The VM DRS score is calculated every minute (compared to every 5 min in previous releases of vSphere). It takes a more granular approach to balancing workloads because it considers other hosts that are able to provide a better score for a particular VM.

The VM DRS score uses metrics such as CPU %ready time, memory swap metrics, and good CPU cache behaviour. It uses goodness modelling, which uses an ideal throughput and actual throughput for CPU, memory, and network. During periods of no contention, the ideal throughput of a particular VM is equal to the actual throughput.

Then there are resource costs that lower the VM throughput. The VM DRS score is a combination of how efficient each resource is. The resource cost is used to determine efficiency. The costs of each resource, such as CPU, memory, or network, are added to the cost. One last cost that is considered is the migration cost—when a VM is migrated to another host, it will use some CPU cycles for the operation.

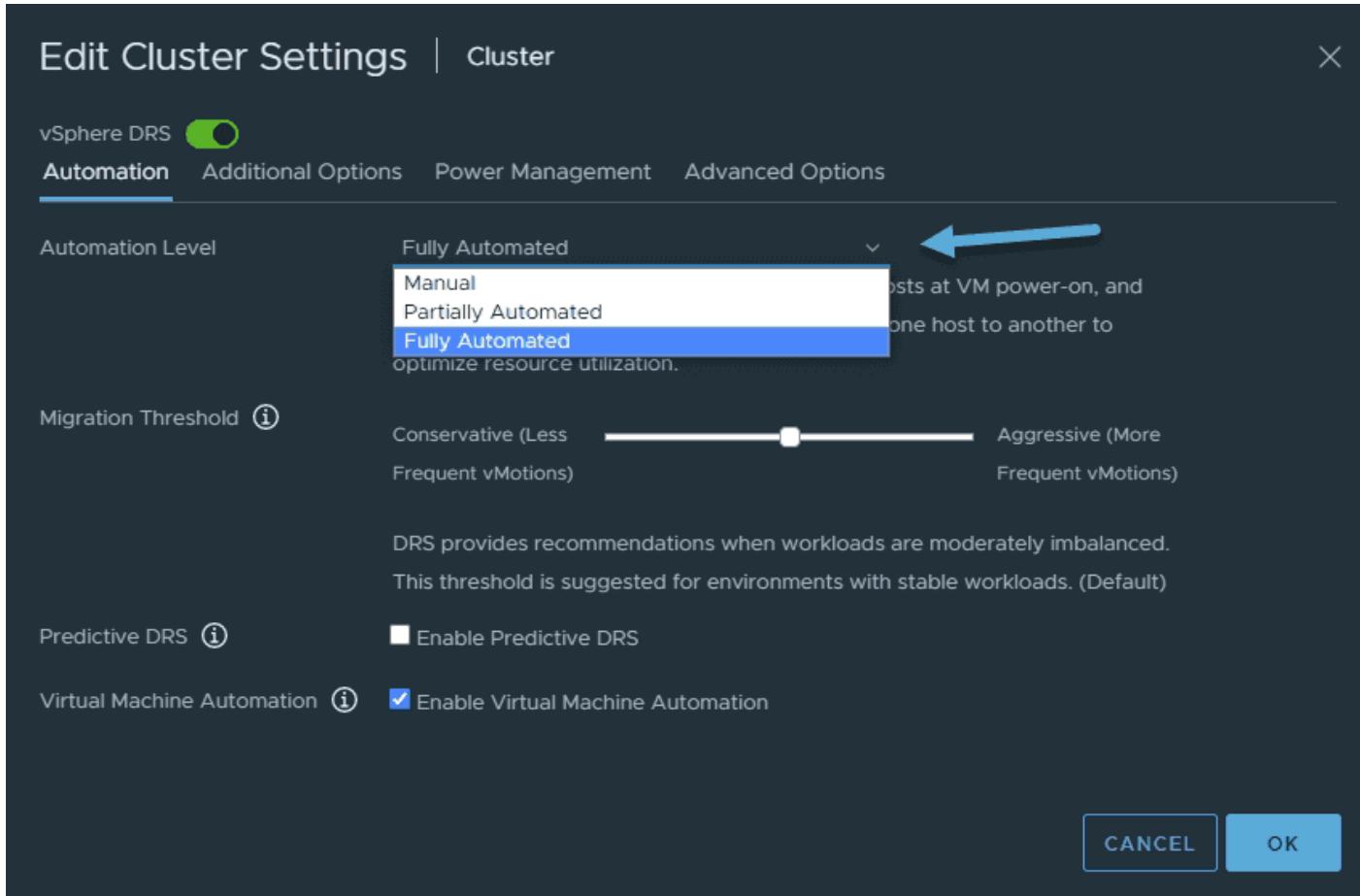
You may not know this, but vMotion can be an “expensive” operation, depending on how many VM memory pages have to be copied to the destination host. vMotion usually consumes a large amount of CPU, memory, and network resources. And don’t forget, this is on both the source and destination hosts.

**Note:** After you migrate from vSphere 6.x to vSphere 7, you might see more vMotion operations due to the new DRS behaviour.

## vSphere 7 DRS configuration

The three different vSphere DRS automation levels look the same in vSphere 7, but let’s quickly recap what they’re actually used for. Here are the DRS automation levels that are accessible via the drop-down menu:

- **Fully automated**—vSphere fully automates the VM placement and migrations. The 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.
- **Partially automated**—vSphere places the VMs, but you must click a button to initiate vMotion and PowerON. The DRS automatically places virtual machines onto hosts at VM power-on. Migration recommendations need to be manually applied or ignored.
- **Manual**—vSphere shows notifications only of recommendations. The DRS generates both power-on placement recommendations and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.



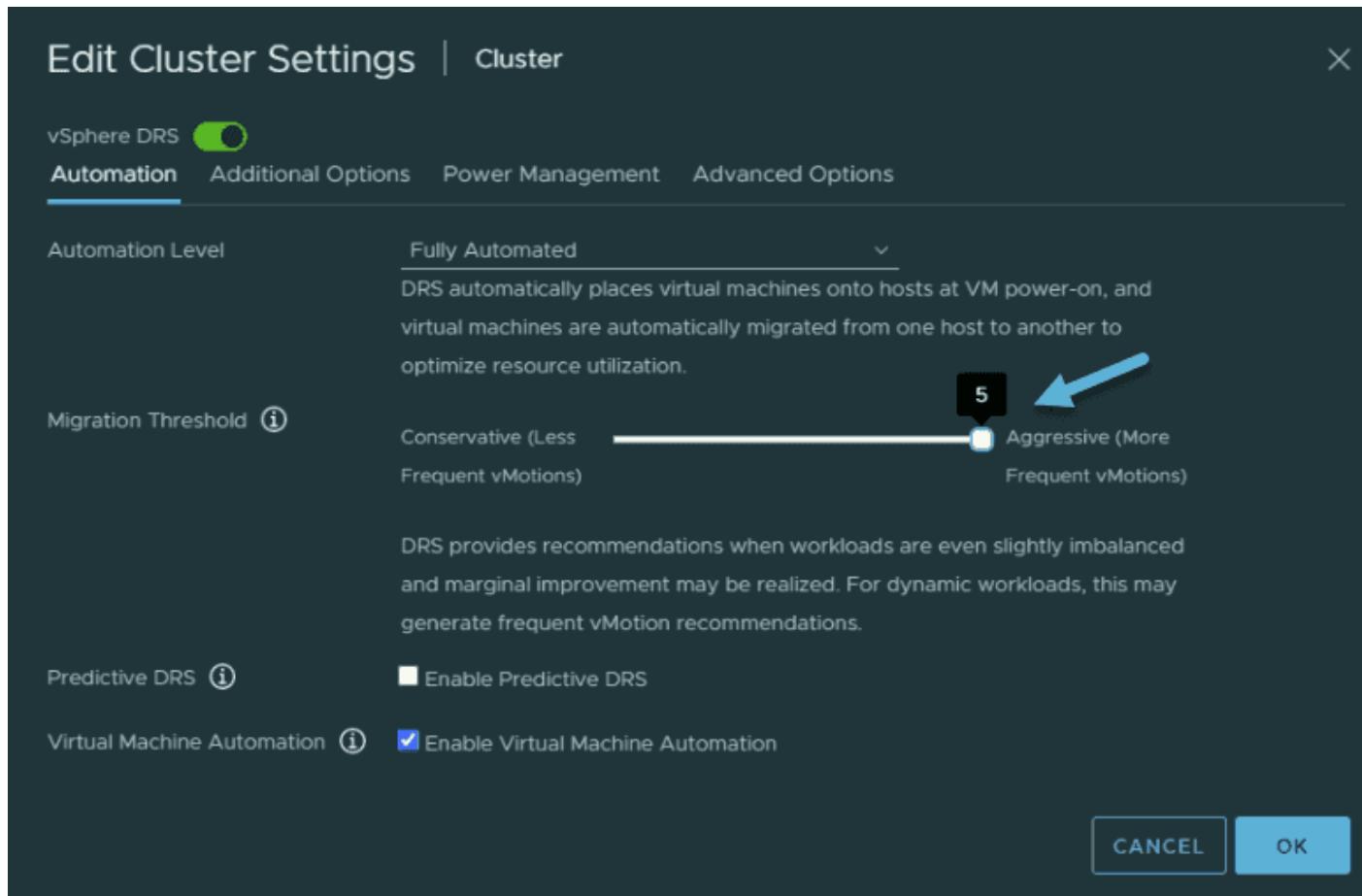
### vSphere 7 DRS automation levels

#### Configuring the migration threshold

The threshold can be set from 1 to 5. Just drag the bar from **Conservative** to **Aggressive** mode.

The default (3) is in the middle.

- The DRS will only apply recommendations that must be accepted to satisfy cluster constraints, such as affinity rules and host maintenance. The DRS will not try to correct host imbalance at this threshold.
- The DRS only gives recommendations when workloads are extremely imbalanced or virtual machine demand is not being satisfied on the current host.
- Default - The DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads.
- The DRS provides recommendations when workloads are fairly imbalanced. This threshold is suggested for environments with bursty workloads.
- The DRS provides recommendations when workloads are even slightly imbalanced and marginal improvement may be realized. For dynamic workloads, this may generate frequent vMotion recommendations.



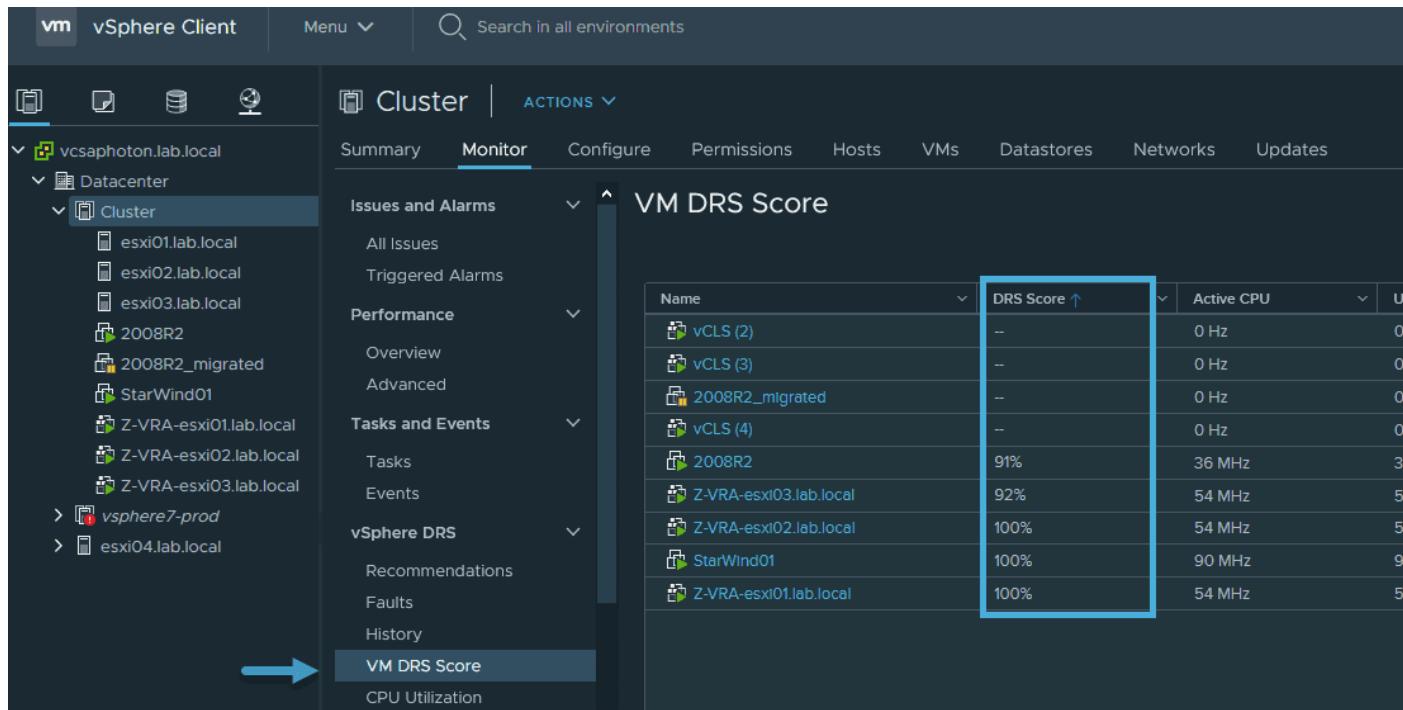
### Configure the DRS migration threshold in vSphere 7

## Viewing the VM DRS score

I was wondering whether there was some detailed VM DRS score information visible within the vSphere UI when navigating via the vSphere client. Yes, there are.

You must go and select your cluster. Then select **Monitor > VM DRS score** under the vSphere DRS section. There is a column that shows the DRS score for the VMs.

**Note:** The vCLS VMs in my example do not use the DRS and vMotion, so they do not show VM DRS scores at all.



The screenshot shows the vSphere Client interface with the 'Monitor' tab selected for the 'Cluster' view. On the left, the navigation tree shows a Datacenter with multiple Clusters (esxi01.lab.local, esxi02.lab.local, esxi03.lab.local, 2008R2, 2008R2\_migrated, StarWind01, Z-VRA-esxi01.lab.local, Z-VRA-esxi02.lab.local, Z-VRA-esxi03.lab.local). A blue arrow points from the 'vSphere7-prod' cluster entry to the 'VM DRS Score' section at the bottom of the left sidebar. The main content area displays the 'VM DRS Score' table:

Name	DRS Score ↑	Active CPU	U
vCLS (2)	–	0 Hz	0
vCLS (3)	–	0 Hz	0
2008R2_migrated	–	0 Hz	0
vCLS (4)	–	0 Hz	0
2008R2	91%	36 MHz	3
Z-VRA-esxi03.lab.local	92%	54 MHz	5
Z-VRA-esxi02.lab.local	100%	54 MHz	5
StarWind01	100%	90 MHz	9
Z-VRA-esxi01.lab.local	100%	54 MHz	5

### Where to find the VM DRS score for a particular VM

While a VM DRS score close to 0 means poor efficiency, a VM DRS score between 80% and 100% means that there is almost no resource contention.

The VM DRS score is transparent, and you don't need to make any adjustments or special configuration compared to vSphere 6.7 or earlier.

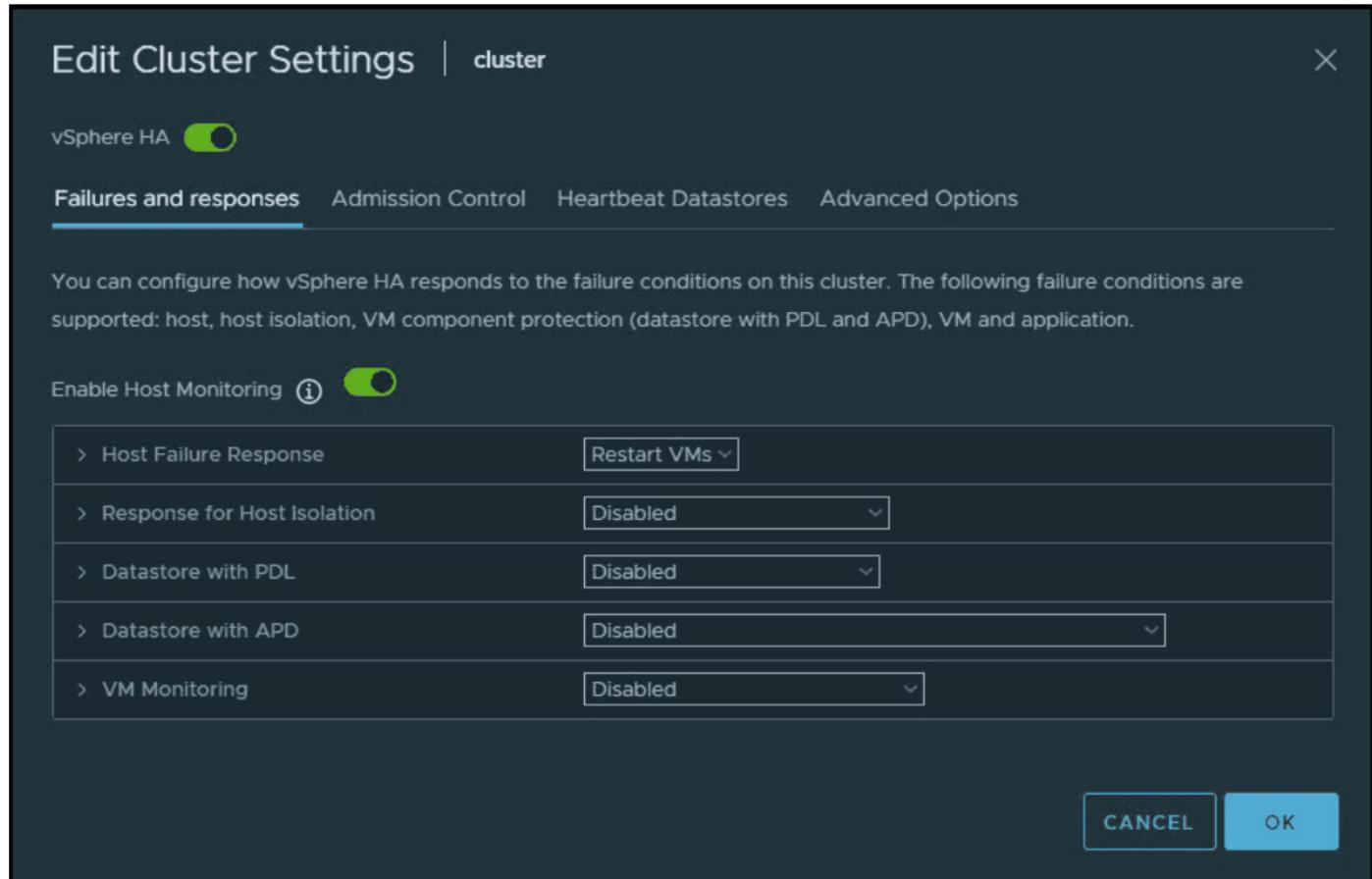
## Objective 1.6.4 Describe vSphere high availability

### vSphere high availability (HA) overview

VMware vSphere high availability (HA) is able to protect virtual machines (VMs) during hardware failures. If you have a VMware vSphere cluster configured and you activate HA, then if any of your hosts has a hardware problem, the VMs running on that host will be restarted automatically on the remaining hosts in the cluster.

vSphere HA can also protect against application failure by continuously monitoring a virtual machine and resetting it in the event a failure is detected.

If you have a datastore problem, vSphere HA protects against datastore accessibility failures by restarting affected virtual machines on other hosts that still have access to their datastores.



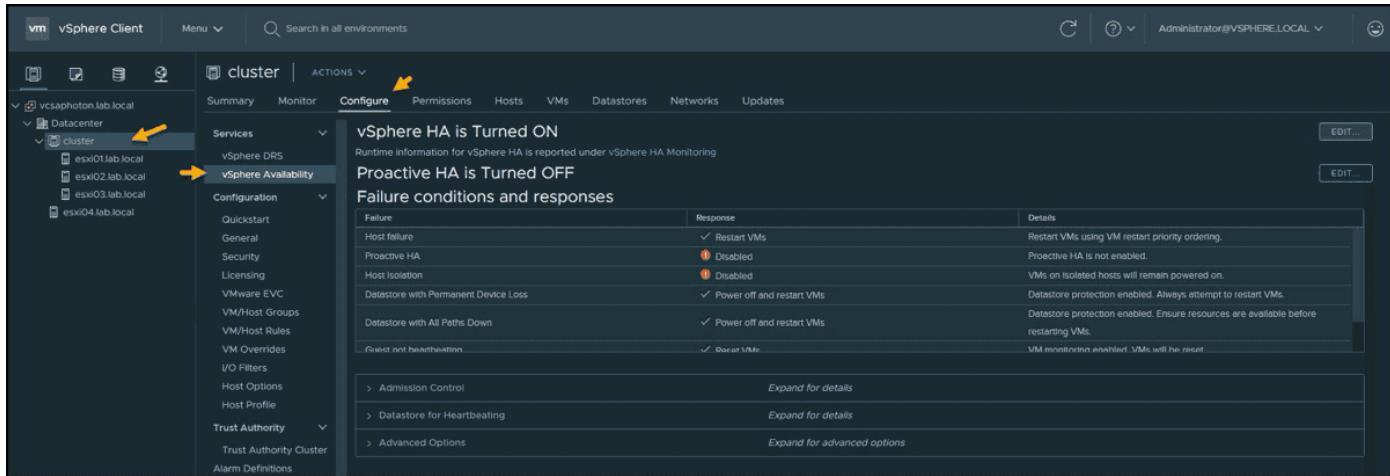
## VMware vSphere HA Edit cluster settings

vSphere HA has another capability that can protect virtual machines against network isolation by restarting them if their host becomes isolated.

### Activating vSphere high availability (HA)

You do not need to install special software in the application or virtual machine. All workloads are automatically protected by vSphere HA. After vSphere HA is configured, no actions are required to protect new VMs.

You can activate vSphere HA by selecting the cluster, and then selecting **Configure > vSphere Availability > Edit**.



## Where to configure vSphere HA

When you activate vSphere HA, there are a couple of things going on in the background. The HA agent is installed on each host in the cluster. The agents can communicate with each other.

There is an election process where one host from the cluster will become a primary host. This depends on a couple of things, such as the total number of mounted datastores, etc. Once the primary host is elected, all the other hosts become “secondary hosts” that listen to the primary host. If the primary host has a problem and becomes unavailable, a new election takes place, and a new primary host is elected.

The primary host receives information from vCenter Server on a regular basis. It pulls information which it then passes to the secondary hosts. If there is a host failure, the primary host uses network and datastore heartbeats to verify that a secondary host is offline.

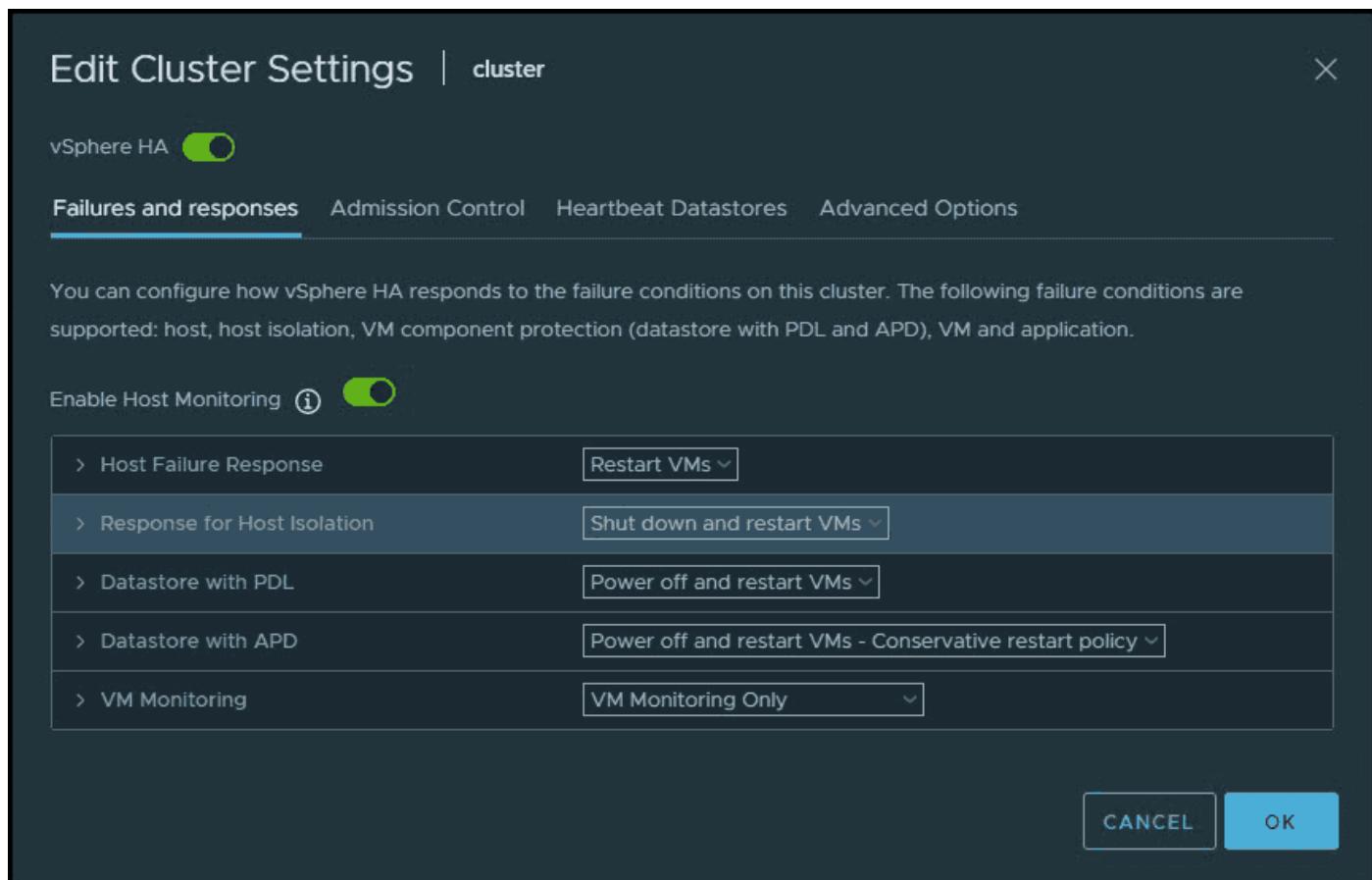
It monitors both network and shared datastores, so it basically double-checks that there is some kind of problem with one of the secondary hosts. It then triggers an HA event, and VMs that were running on the failed secondary hosts are restarted on other hosts in the cluster.

## vSphere high availability (HA) host failures

- **Failure** — The host stops functioning. This can be a power supply, motherboard, or CPU problem, or the host has a purple screen of death (PSOD).
- **Isolation** — The host becomes isolated from the network. In this case, the host is running but cannot communicate with other hosts. vSphere HA has detected this because the datastore heartbeat is working.
- **Partition** — The host loses network connectivity with the primary host but is still connected to other secondary hosts.

When there is a failure, the HA must know what to do. We can configure different options in the case of host failure. Many failure conditions are supported, including host failure, host isolation, VM component protection (datastore with PDL and APD), VM, and application. The

different configuration options and settings are available through the Failures and responses tab via the drop-down lists. Then there are check boxes for each option. For the case of datastore Permanent Device Loss (PDL) or All Paths Down (APD), check with your hardware manufacturer to see whether those options are supported.

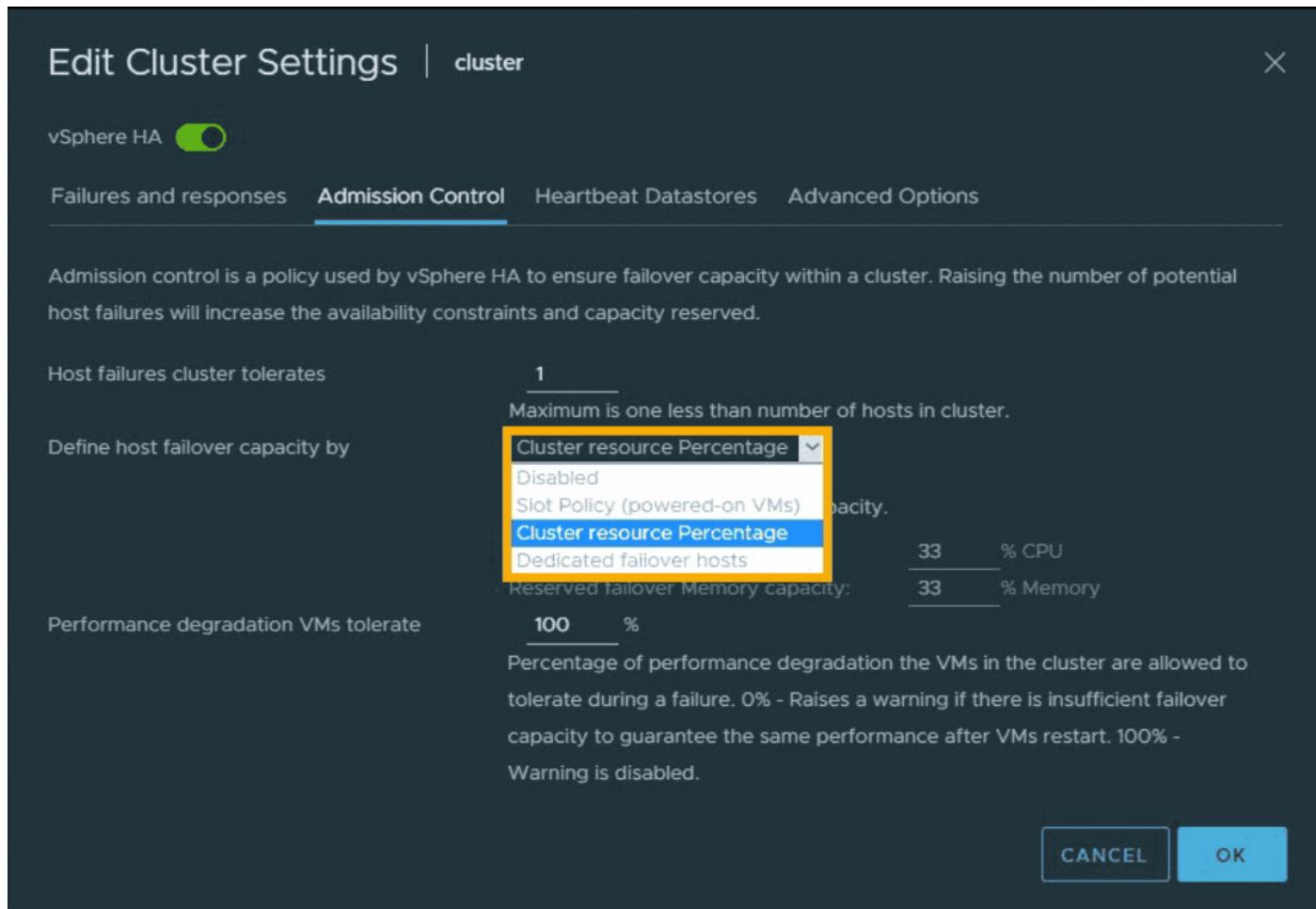


## vSphere HA failures and responses

### vSphere admission control

What is vSphere admission control? It is a configuration policy that enables ensuring that vSphere has enough failover capacity in the cluster. By default, a cluster can tolerate one host failure at a time. The maximum is one less than the number of hosts in the cluster.

So, for example, you have a cluster with five hosts. You can set the maximum number of host failures to 4.



## vSphere admission control

You can define the host failover capacity by:

**Cluster resource percentage** — This takes into account a specified percentage of aggregate CPU and memory resources that are reserved for failover.

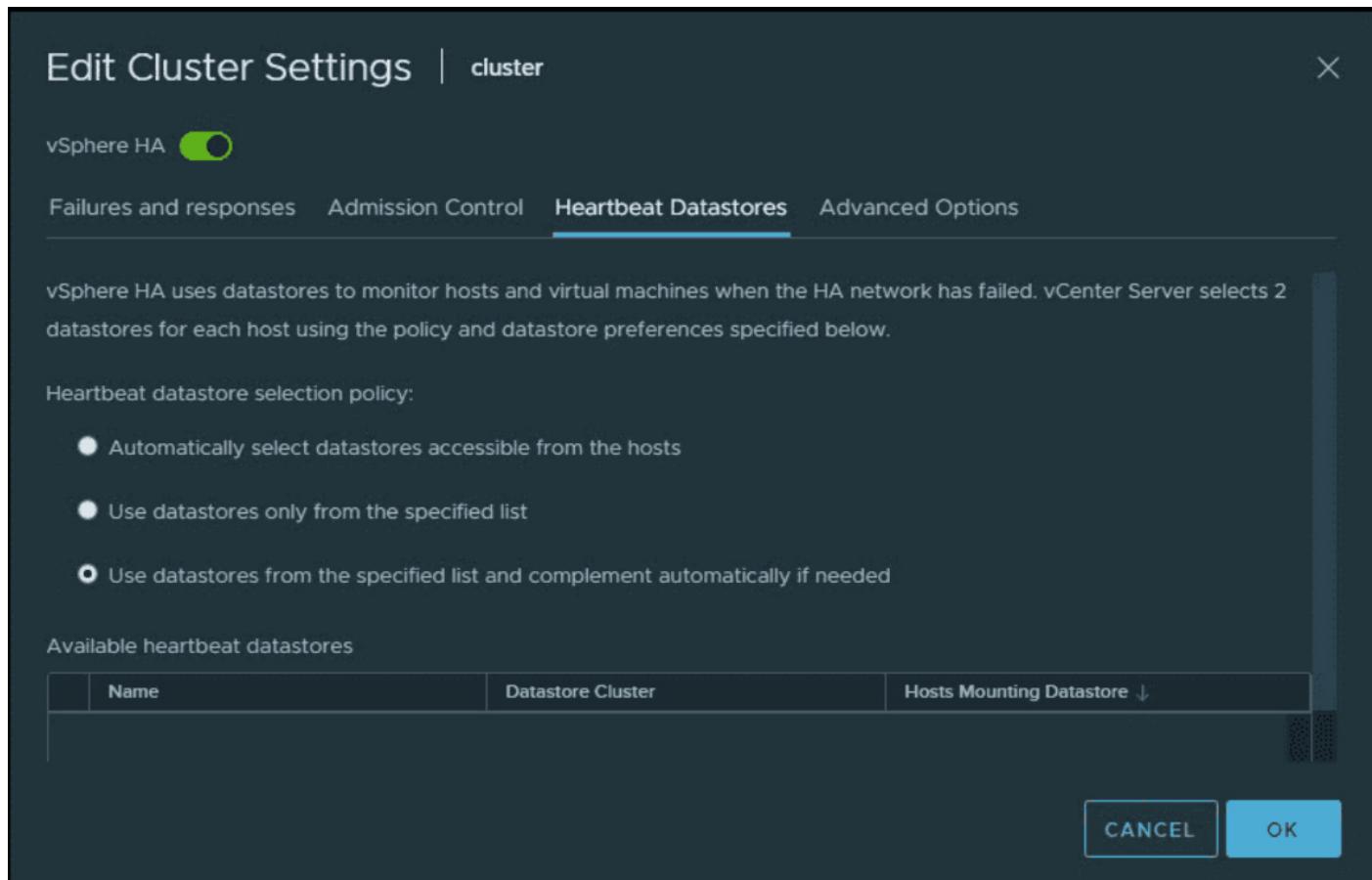
**Slot policy admission control** — vSphere HA admission control makes sure that host(s) can fail, and there are still sufficient resources in the cluster to failover all the VMs from those hosts.

**Dedicated failover hosts** — This policy is the least efficient. It reserves host(s) as «spare» host(s). No VMs can run on them because they are used **only** if an HA event is triggered. vSphere HA works with other features, such as VMware vSAN or Distributed Resources Scheduler (DRS).

If you are using vSphere HA with vSAN, the pooled vSAN datastore and its separated network traffic are used to detect HA failure. There is only one small issue: You must disable HA to activate VMware vSAN. And vice versa: You can enable vSAN only if vSphere HA is disabled.

There are three policies to choose from in the heartbeat datastores. You can let vSphere automatically select the datastore that will be used for the datastore heartbeats (default), you

can use a datastore from a specific list, or you can use datastores from the specified list and complement automatically if needed.



### vSphere HA heartbeat datastores

In the last option, if one of the datastores becomes unavailable, vSphere HA will choose a different datastore. If there is no preferred datastore available, vSphere HA picks any available cluster datastore.

## Objective 1.6.5 Describe datastore clusters

VMware Distributed Resource Scheduler (DRS) is a VMware feature that optimizes the performance and resources of your vSphere cluster. Storage DRS was introduced in vSphere several releases ago, and it is still a key feature of vSphere 7.

Storage cluster configuration with Storage DRS (SDRS) in vSphere 7 allows you to balance virtual machine disk files (VMDK) between datastores in the datastore cluster.

In the same way as traditional DRS, where VMs are placed initially onto the healthiest host, the initial placement is manual with SDRS. After the VM is placed onto a datastore, the SDRS function keeps an eye on those datastores and makes sure none of them becomes completely filled.

If the utilization of the datastore rises above a predefined threshold, the DRS will issue a recommendation to move some VMDKs off this datastore and place them on a datastore with sufficient free space.

SDRS also monitors I/O latency and checks what has happened in the last 24 hours. There might have been a datastore with some heavy I/O over the past 24 hours, which might mean the system won't move VMDKs onto it.

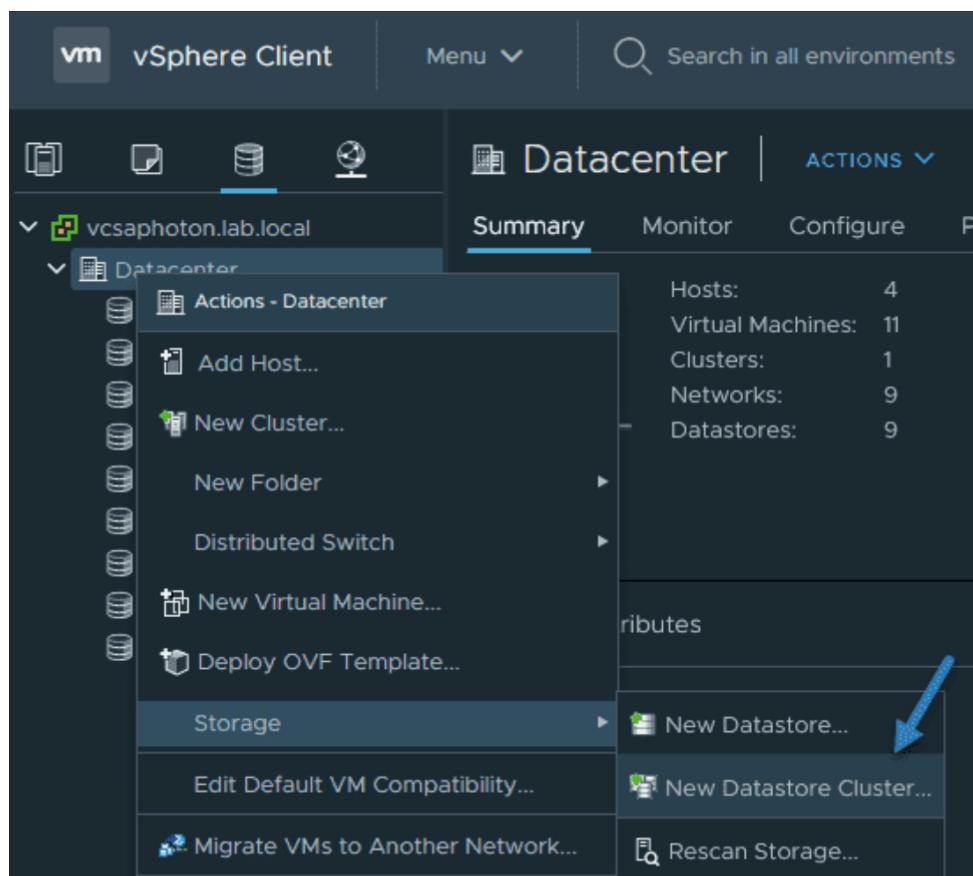
SDRS allows you to put a datastore into maintenance mode, allowing you to evacuate your VMDKs off to another datastore to enable decommissioning.

You can use VMFS or NFS-based datastores, but you can't combine VMFS with NFS in the same SDRS cluster. In this case, simply create separate SDRS clusters.

If you have some storage arrays that support hardware acceleration, you should not mix them with other arrays that don't have it. As a good practice, the datastore cluster should remain homogeneous.

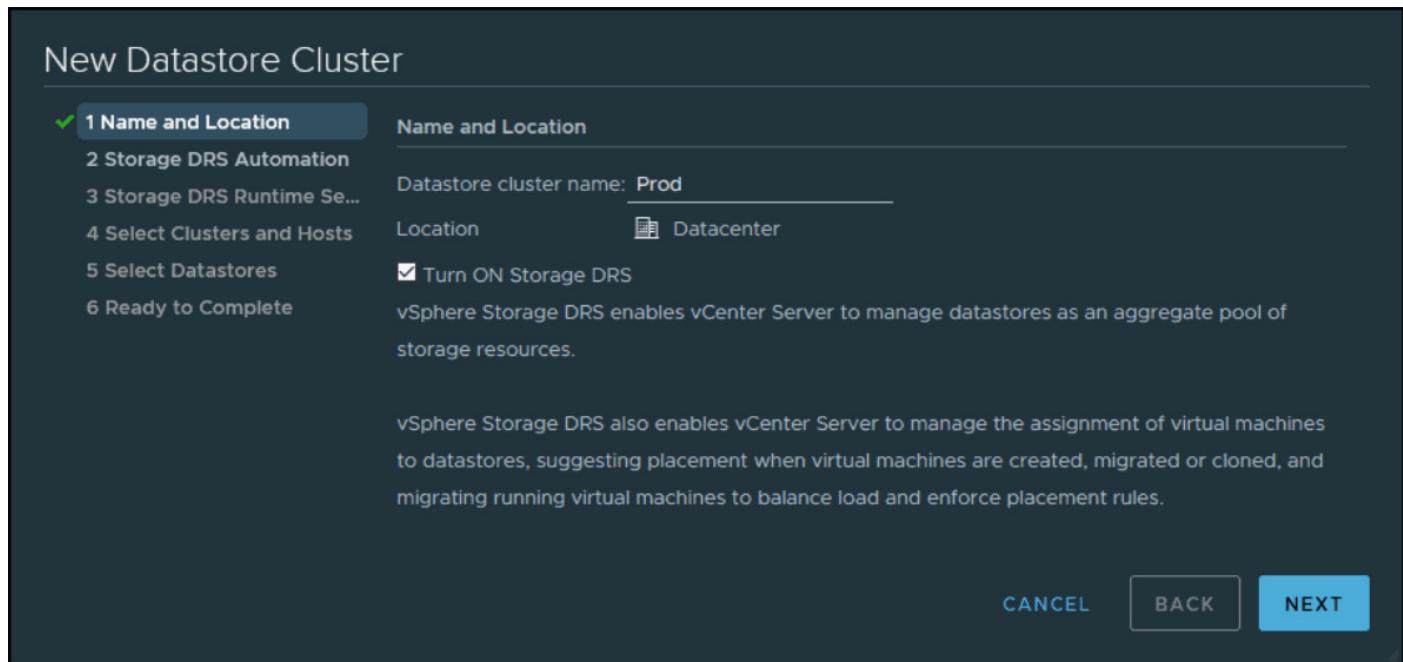
## How to create new datastore clusters

You'll need to log in via your vSphere web client. Select the relevant datacenter object. Right-click it and select **Datacenter > Storage > New Datastore Cluster**.



Create a new datastore cluster

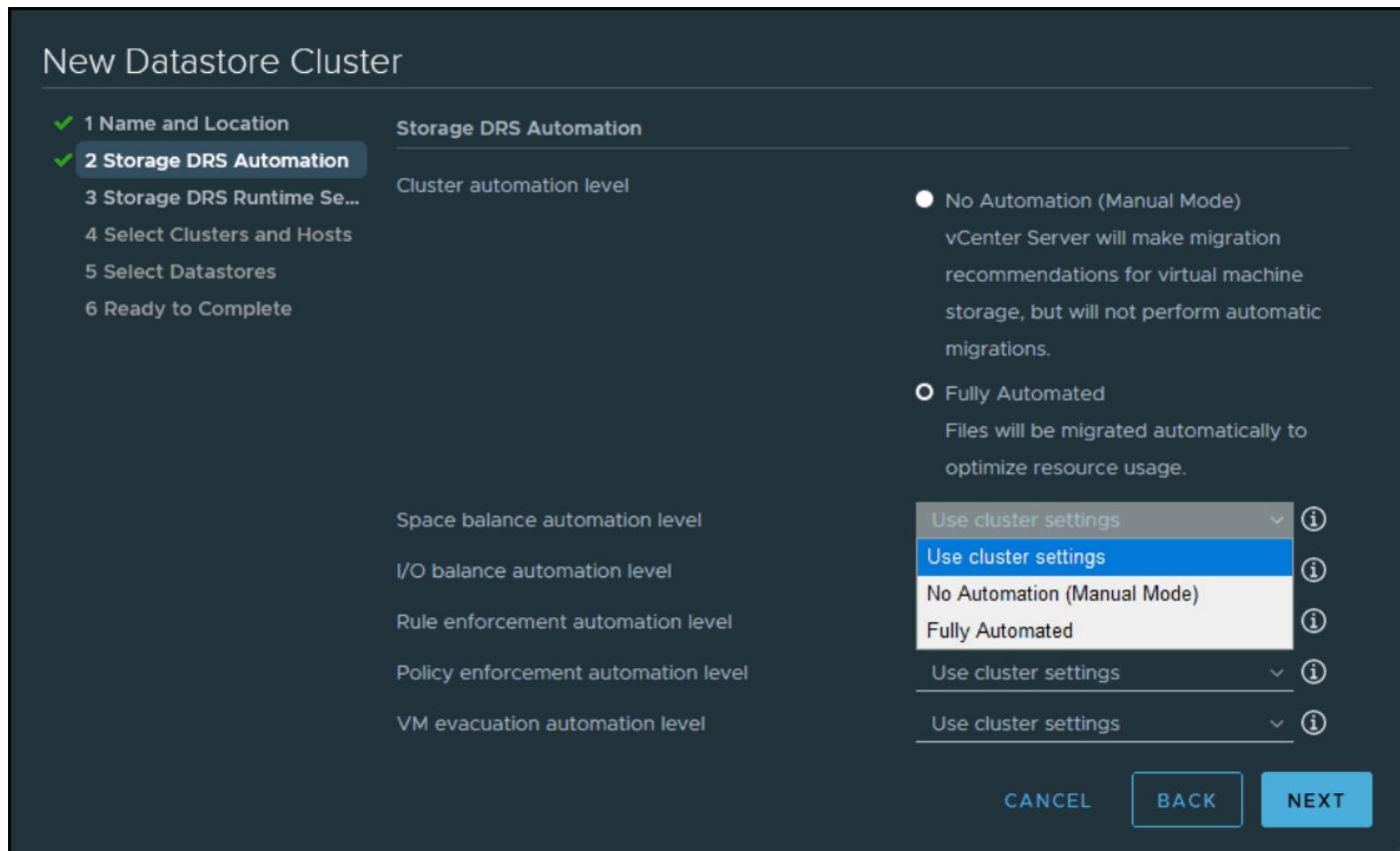
Then, on the next page, give it a meaningful name so you recognize which SDRS cluster you're working with. You can create several SDRS clusters within your datacenter.



### Turn On Storage DRS checkbox

Then, on the next page, you can choose between Fully Automated or No Automation (Manual mode). This is a one-or-the-other choice.

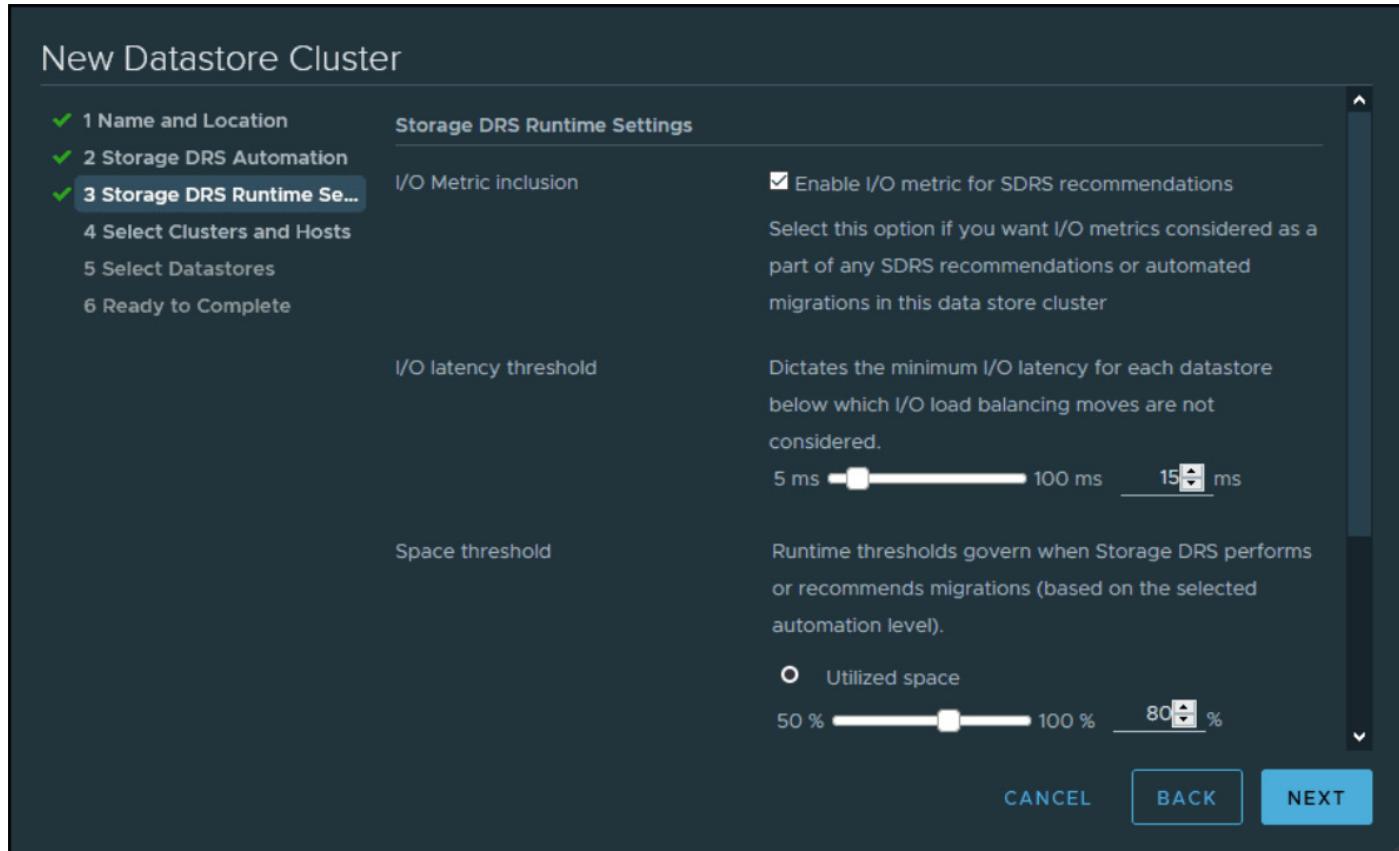
- You have different granularity options available that allow you to override the cluster settings. This means that you can have cluster settings on fully automatic, but individual options can be set as needed.
- **Space balance automation level** — Shows what to do when there is a recommendation to correct a space load imbalance in a datastore cluster.
- **I/O balance automation level** — Allows you to choose what happens when it generates recommendations for correcting an I/O load imbalance in a datastore cluster.
- **Rule enforcement automation level** — Specifies SDRS behaviour when it generates recommendations for correcting affinity rule violations in a datastore cluster. Affinity rules allow you to place different VMDKs on different datastores. Useful for Microsoft clustered applications, for example.
- **Policy enforcement automation level** — Specifies SDRS behaviour when it generates recommendations for correcting storage and VM policy violations in a datastore cluster.
- **VM evacuation automation level** — Specifies SDRS behaviour when it generates recommendations for VM evacuations from datastores in a datastore cluster.



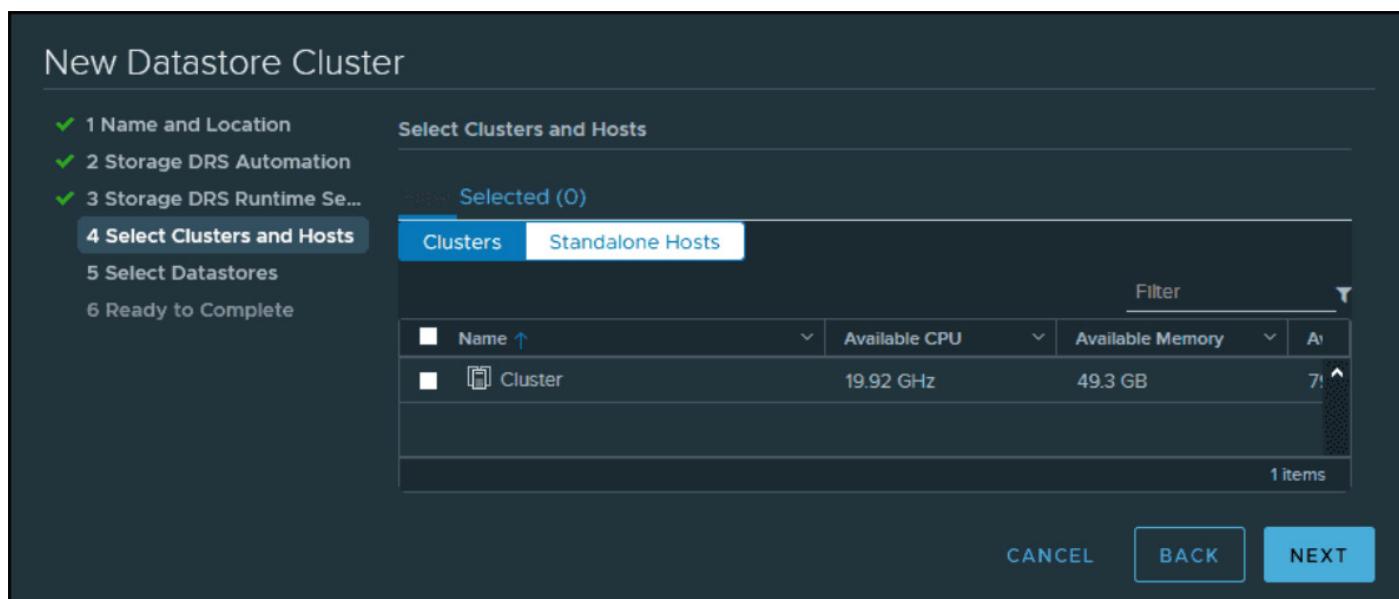
### Choose Fully Automated or Manual Mode

The next page of the wizard presents you with Storage DRS Runtime Settings. You can set the different options for I/O where the I/O metrics are considered as a part of any SDRS recommendation or automated migration in this datastore cluster.

You can also set the I/O latency threshold and space threshold, such that you can set a minimum level of free space per datastore. Those settings allow you to migrate VMDKs off a datastore when the low space threshold kicks in.

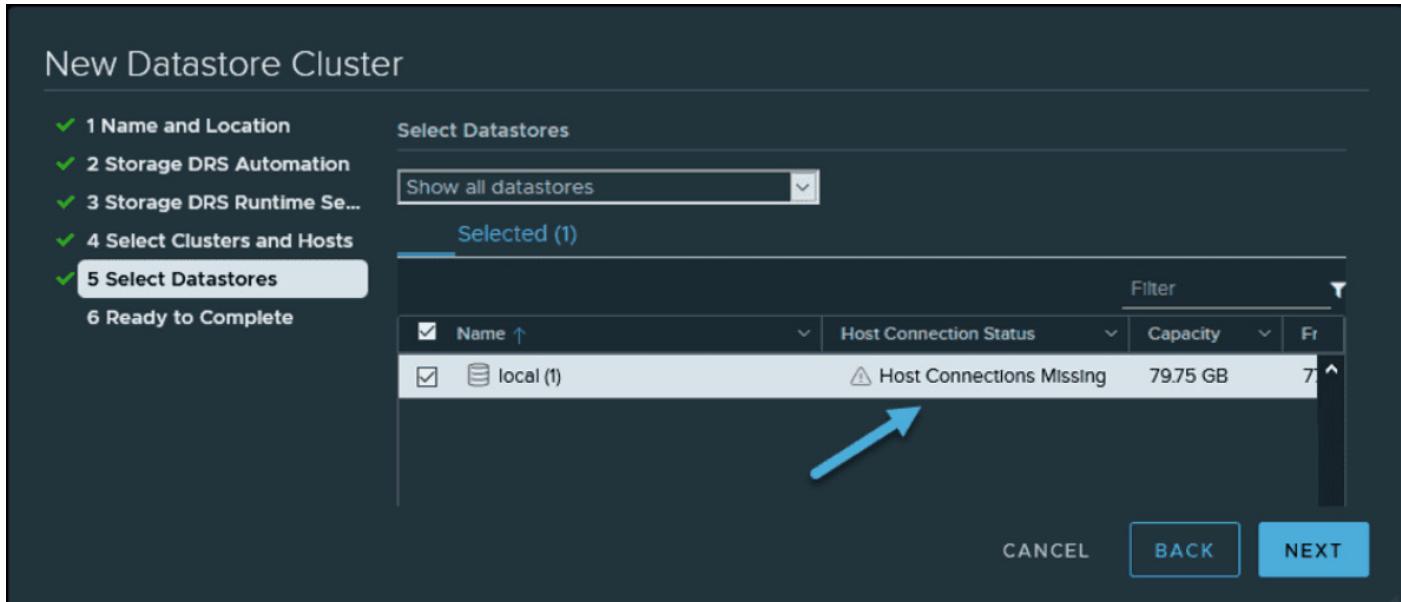


The next page of the wizard allows you to select the cluster and hosts that will be part of the cluster.



### Select clusters and hosts that will be part of the SDRS cluster

The last page of the wizard shows us which datastores can be used. In our small lab case, we only have a local datastore, and as you can see, there is a warning telling us *Host Connections Missing*. This is because we only have a local datastore here, no shared datastores.



### Host Connection Missing warning

This concludes the creation of the datastore cluster in which we activated SDRS.

SDRS is an intelligent vCenter Server system that automatically and efficiently manages VMFS and NFS storage. It is very similar to DRS, which optimizes the performance and resources of your vSphere cluster.

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

Virtual networking can become complex in VMware vSphere 7. Let's look at the differences between vSphere Standard Switch (VSS) and vSphere Distributed switch (VDS) in vSphere 7.

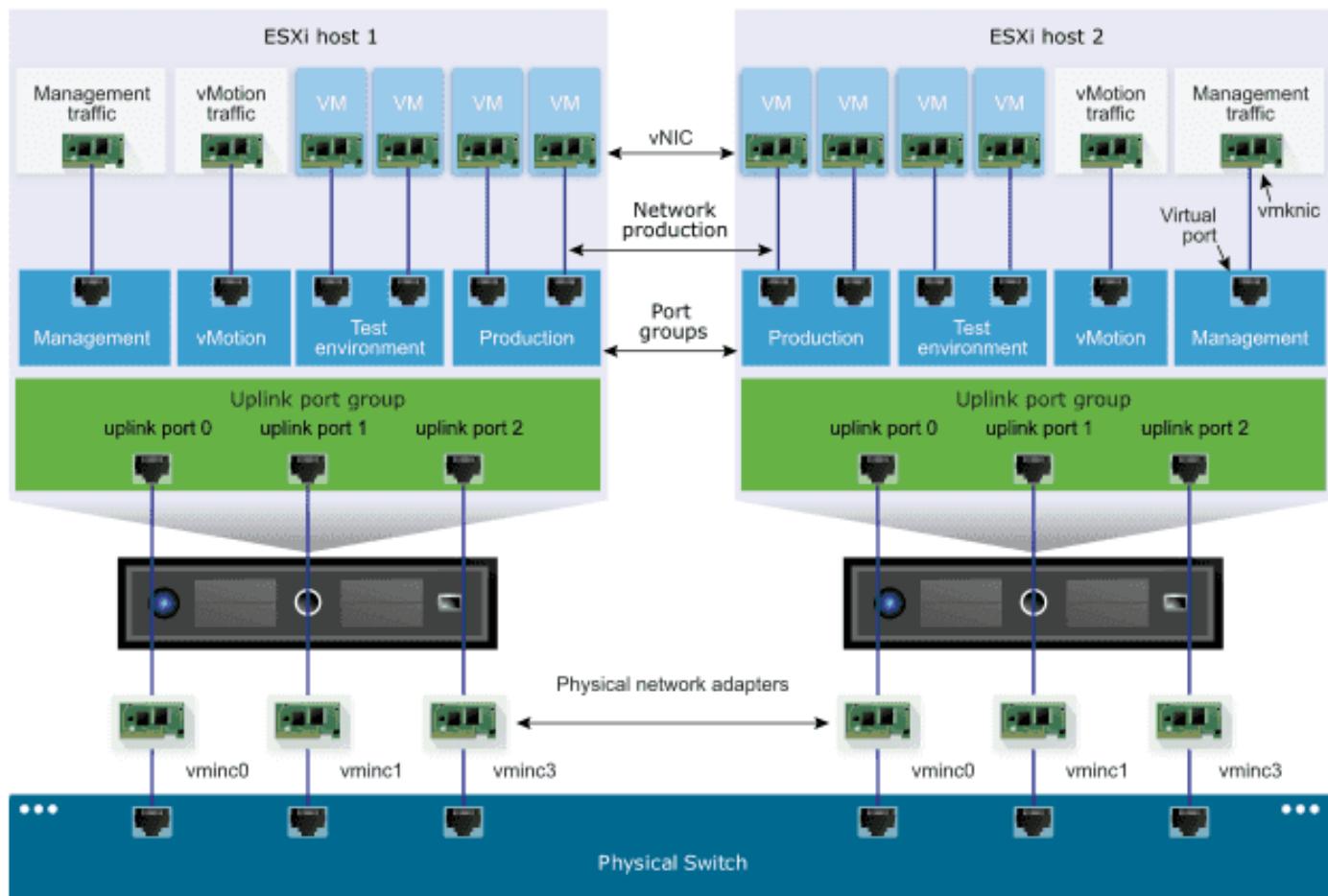
While vSphere 7 does not offer any significant changes or new networking capabilities, it does offer the ability to run vSphere with Kubernetes, which previously involved NSX-T installation. However, NSX-T is not required to run Kubernetes clusters with vSphere 7.

As you know, NSX-T has some network requirements that need to be met before installation. vSphere 7, or rather vCenter Server 7, offers a new capability called multi-homed NICs, which allow having multiple management interfaces for vCenter and fulfilling different network configuration and segmentation needs.

Let's start with the basics first and compare some VSS and VDS features.

## vSphere Standard Switch

This works pretty much the same as a physical Ethernet switch. VSS knows which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. VSS can be connected to physical switches by using physical Ethernet adapters. These adapters are called uplinks, and their important function is to connect the virtual network into a physical network as they are connected to a physical switch.

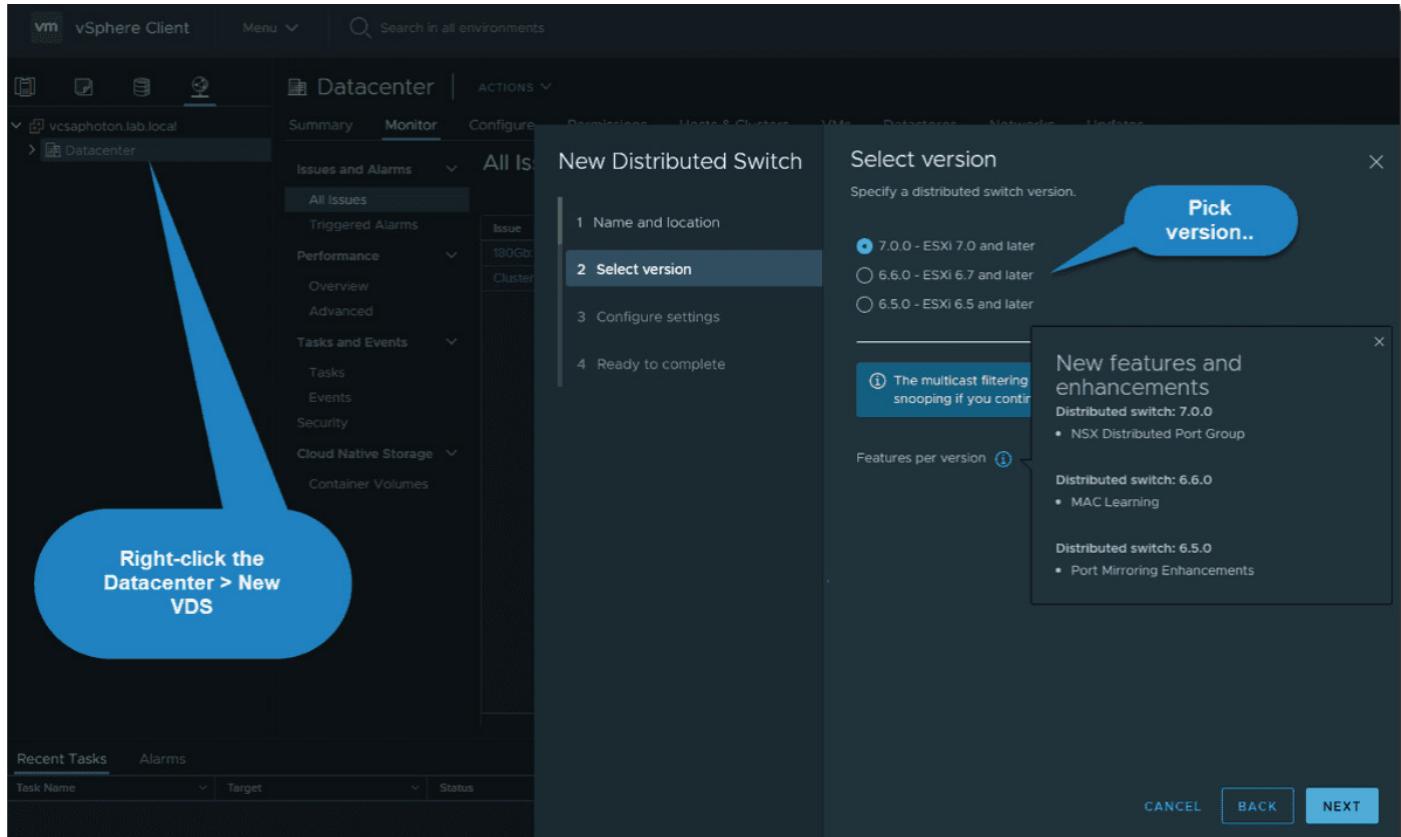


Connectivity with the vSphere Standard Switch

## vSphere Distributed Switch

Imagine VDS as a single switch connected with all associated hosts in a datacenter. The VDS has the role of providing centralized provisioning, administration, and monitoring of virtual networks. When you configure VDS, you can choose the ESXi host to which you attach and propagate this configuration. In this way, you don't have to go one-by-one to each of your ESXi hosts to replicate the configuration.

As you can see, with the evolution of vSphere versions, the VDS has evolved as well. You can see all the versions you can still create on vCenter Server 7. vSphere 6 is no longer on the list.



## Create a new VDS at the datacenter level

### Standard Port Group

When you want to connect network services that are active on your network, you do it through standard port groups. Port groups basically define how a connection is made through the switch to the network. Usually, you have a single standard switch that is associated with one or more port groups. But this is not a limit. You can also create multiple VSSs on your host, each of which can carry multiple port groups.

### Distributed Port Group

This is a port group that is associated with a vSphere distributed switch. Distributed port groups define how a connection is done through the vSphere distributed switch to the network.

### vSphere 7 Standard Switch advanced networking options

Some advanced options that are available when you configure a VSS are the possibility of having two or more physical NICs in a team to increase the network capacity of the VSS or a standard port group. You can also configure failover to create network traffic routing in the event of adapter failure.

Another feature within VSS is that you can select a load balancing algorithm to determine how the standard switch distributes the traffic between the physical NICs in a team.

## Configure load balancing on VSS

Remember, those are per-vSwitch settings. So if you have three hosts in the cluster, you must replicate those settings manually across all your hosts. Hence, the advantage of distributed vSwitch.

You have several options here:

**Route based on originating virtual port** - The VSS selects uplinks that are based on the VM port IDs on the VSS or VDS. Default load balancing method. Each VM running on the ESXi host has a virtual port ID on the vSwitch. VSS uses the virtual machine port ID and the number of uplinks in the NIC team. Once the uplink is selected, it always forwards traffic through the same uplink for this VM (while the VM is still running on the same port). Once the VM is migrated or deleted, the port ID on vSwitch is freed.

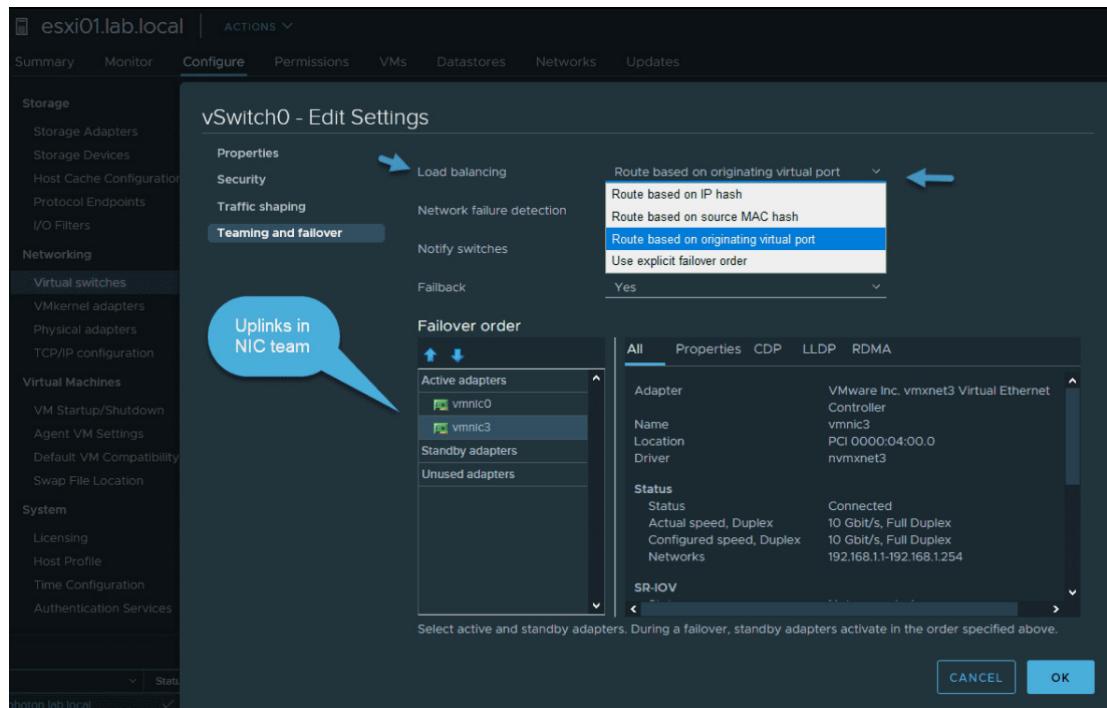
**Route based on source MAC hash** - The vSwitch selects uplinks for VMs based on the source and destination IP address of each packet. The system calculates an uplink for the VM based on the VM's MAC address and the number of uplinks in the NIC team.

The advantage is that there is a more even distribution of the traffic than Route Based on Originating Virtual Port. The virtual switch calculates an uplink for every packet. However, this policy consumes somewhat more resources. Another disadvantage is the fact that the vSwitch does not know if the uplink is saturated.

**Route based on IP hash** - This policy is used when the vSwitch selects uplinks for VMs based on the source and destination IP of each packet. Any VM can use any uplink in the NIC team. The route depends only on the source and destination IP address. The advantage is that each VM can use the bandwidth of any uplink in the team, and the traffic is spread evenly among all uplinks in the NIC team.

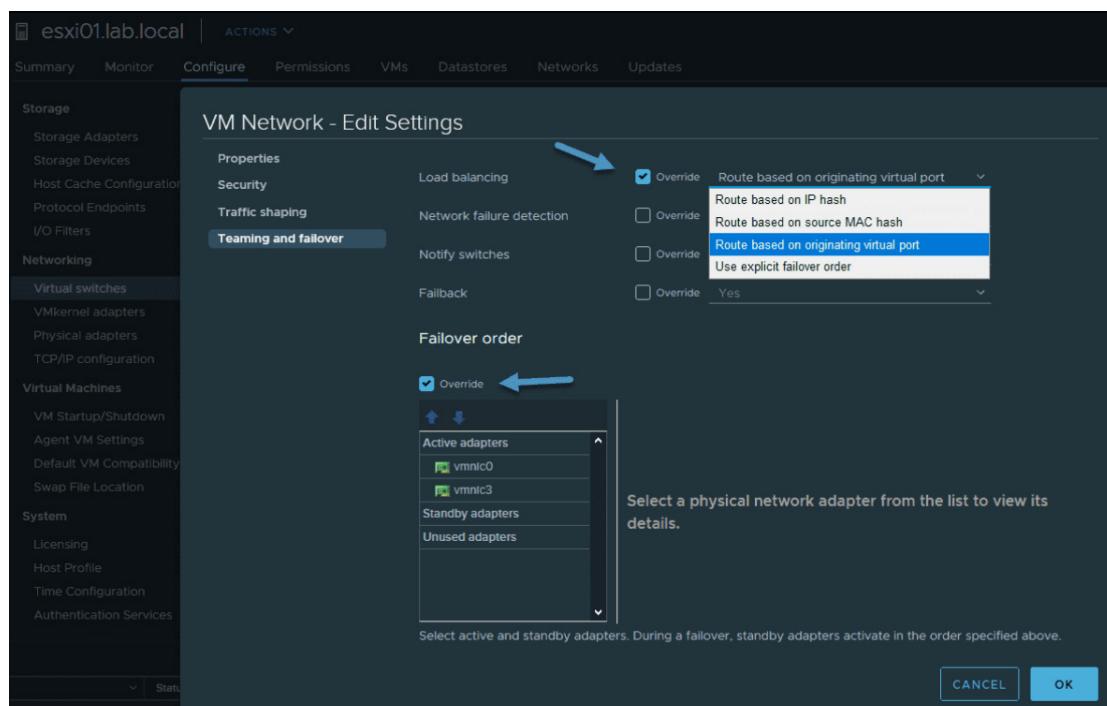
**Route based on physical (only available for VDS)** - The best option. This load balancing policy is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks.

**Use Explicit Failover Order** - No real load balancing is done with this policy. The vSwitch always uses the uplink that is the first in the list of active adapters. If no adapters are available in the "Active" list, then the vSwitch picks the adapter from the "Standby" adapters list.



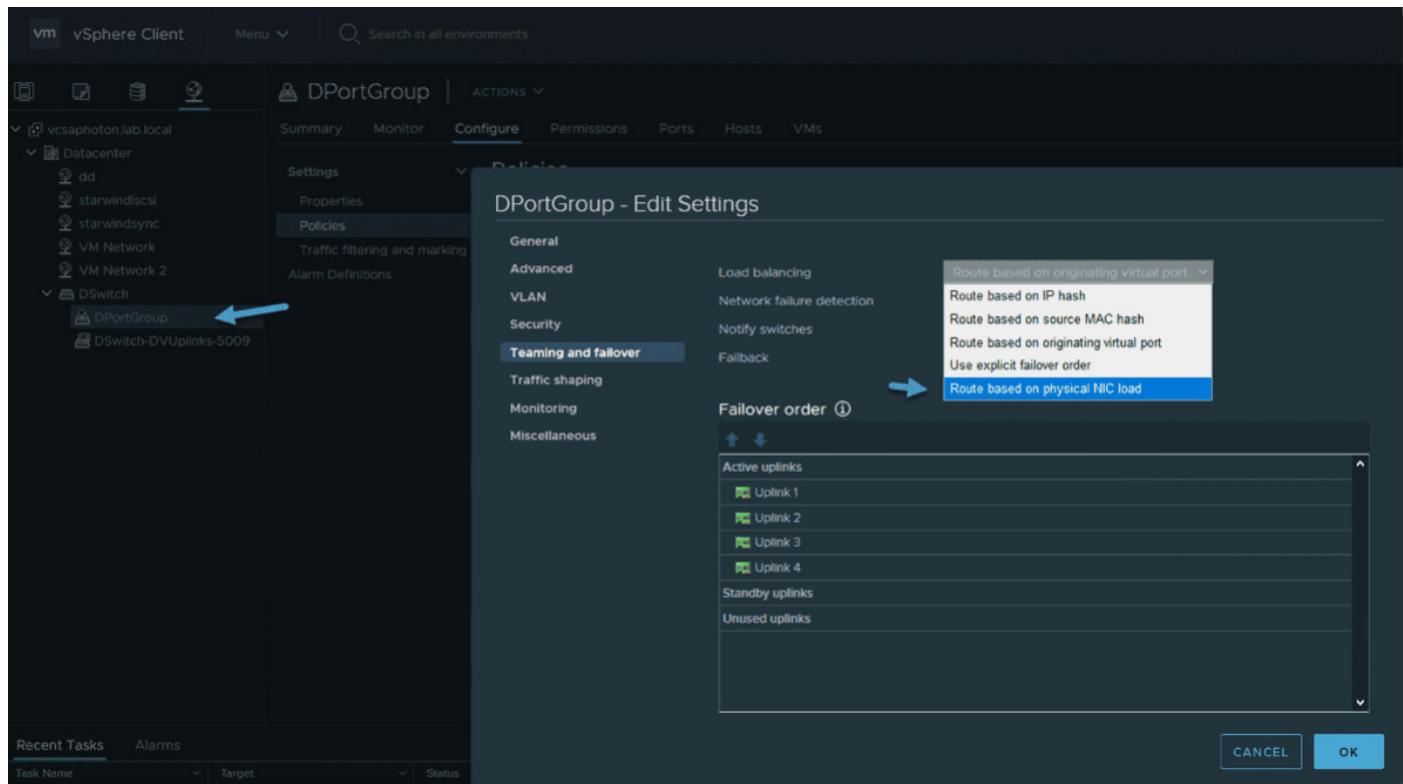
## Changing load balancing policy on vSwitch

Contrary to settings at the vSwitch level, we can have a look at the port group level. Remember, each vSwitch can have several port groups. The same load balancing options apply there, too. The only thing that changes is that little checkbox “override”, allowing us to have a different policy on the port group level than at the vSwitch level.



## Changing load balancing policy on port group

Now let's see what it looks like at the distributed port group. You see that we have the option to choose a network load balancing policy based on the Route based on physical NIC load here.



**Changing load balancing policy on a distributed port group**

## Objective 1.7.1 Describe VMkernel networking

Here are a few words and definitions that 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.

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.

### Terminology:

We assume that you know already the networking terminology. Things such as TCP/IP, MAC address, IP address, Ether Channel, LACP, etc.

Let's describe some networking creation concepts, for vSphere standard switch (vSS).

- **vSphere Standard Switch (vSS)** – It's like a physical Ethernet switch where you have VMs connected and those can communicate with each other as the switch forwards traffic to each of those VMs.
- **Standard Port group** – Portgroup specifies port configuration options (VLAN, bandwidth limitation). A single standard switch has usually one or more portgroups.
- **Uplink** – Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks.

Name	Type	VLAN	Connectees
Management Network	Standard Network	VLAN ID: --	VMkernel Adapters 1
VM Network	Standard Network	VLAN ID: --	Virtual Machines 2
vsan	Standard Network	VLAN ID: --	VMkernel Adapters 1
Physical Adapters	Physical Adapter	VLAN ID: --	Physical Adapters 1

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.

## To Create VSS

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

**esxi01.lab.local - Add Networking**

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select connection type  
Select a connection type to create.

VMkernel Network Adapter  
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

Virtual Machine Port Group for a Standard Switch  
A port group handles the virtual machine traffic on standard switch.

Physical Network Adapter  
A physical network adapter handles the network traffic to other hosts on the network.

CANCEL BACK NEXT

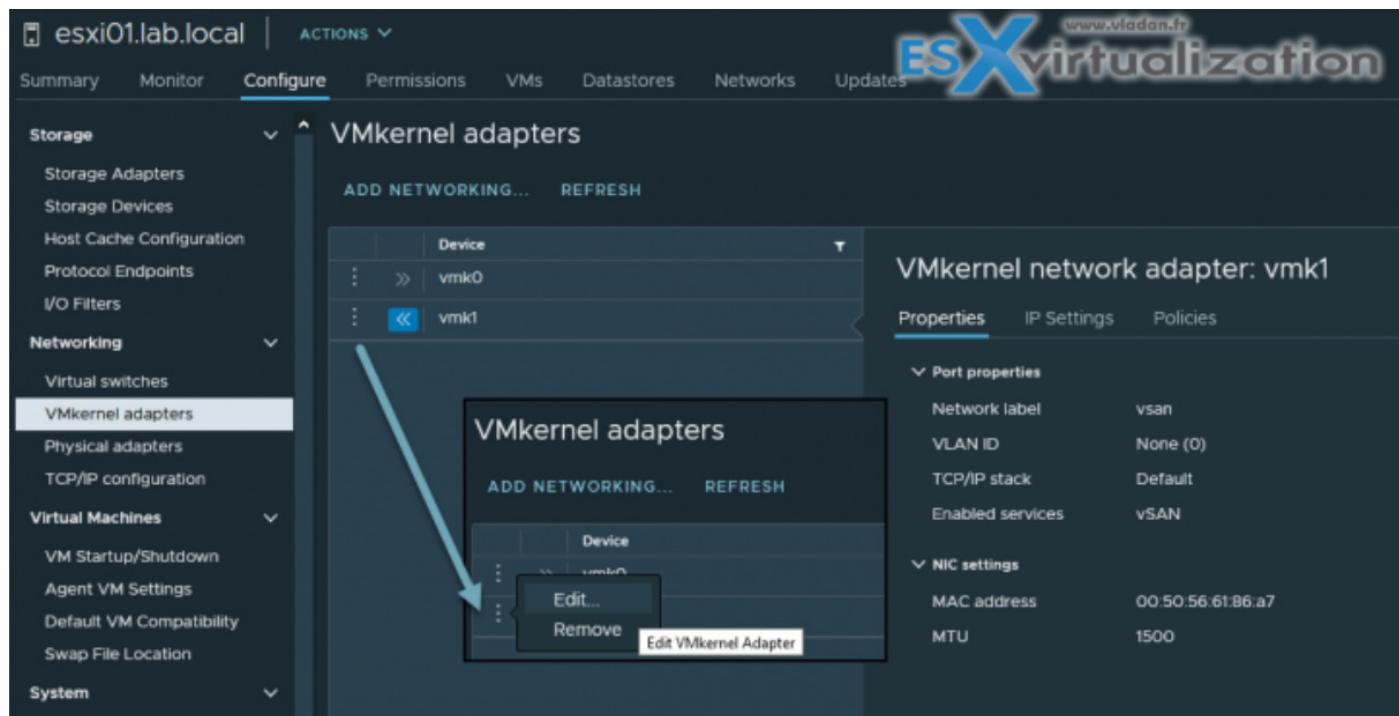
You'll need to select one of the 3 different options:

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

Continue the assistant to create your vSS and network.

VMkernel adapters are part of every host. The management network, for example, is essentially based on VMkernel networking, but this is not the only one. VMkernel network adapters have, or can have, several functions:

**Management Traffic** - configuration and management communication for the host, vCenter Server, and HA traffic. When ESXi is first installed, a VMkernel adapter is created with management-selected checkbox.



**vMotion Traffic** - When you check this box, the VMkernel adapter is able to be used for vMotion. You can use multiple physical NICs for faster migration. By default, vMotion traffic is not encrypted.

**Provisioning traffic** – Basically, this type of traffic is used for VM cold migrations, cloning, and snapshot migration.

**IP Storage and discovery** – This is an important role for VMkernel adapter, as this role allows you to connect to iSCSI and NFS storage. You can use several physical NICs and “bind” each to

a single VMkernel to enable multipathing for additional throughput and redundancy. This role is not a checkbox you simply activate though.

**Fault Tolerance traffic** – One of the features you can enable, Fault Tolerance, allows you to create a second mirror copy of a VM. To keep both machines precisely the same requires a lot of network traffic. This role must be enabled and is used for that traffic.

**vSphere Replication traffic** – As it sounds like, this role handles the replication traffic sent to a vSphere Replication server.

**vSAN traffic** – Mandatory to check if you configured vSAN. The resync of VSAN objects and retrieval needs a very high amount of network bandwidth, so it would be best to have this on as fast of a connection as you can. vSAN does support multiple VMkernels for vSAN but not on the same subnet.

## Recap

The VMkernel port is a virtual adapter, which means it is a special device with which the vSphere host communicates with the outside world. Thus, any service at the second or third level is delivered to the vSphere host.

The VMkernel Networking Layer allows you to connect to the host. Also, it processes the system traffic of IP storage, vSphere vMotion, vSAN, Fault Tolerance, and others. As an example, for vSphere replication: You can create many different VMkernel adapters use them on the source and target vSphere Replication hosts in order to isolate replication data traffic. So, basically vSphere supports different TCP/IP stacks each of them isolated from each other.

- **Default TCP/IP Stack** - This default stack provides networking support for management traffic between vCenter Server and ESXi hosts, and other system services such as FT or iSCSI.
- **vMotion TCP/IP stack** - Use the vMotion TCP/IP to provide better isolation for the vMotion traffic. After you create a VMkernel adapter on the vMotion TCP/IP stack, you can use only this stack for vMotion on this host.
- **Provisioning TCP/IP stack** - Supports the traffic for virtual machine cold migration, cloning, and snapshot migration. You can use the provisioning TCP/IP to handle Network File Copy (NFC) traffic during long-distance vMotion
- **Custom TCP/IP stacks** - You can add custom TCP/IP stacks at the VMkernel level to handle the networking traffic of custom applications.

## Objective 1.7.2 Manage Networking on Multiple Hosts with vSphere Distributed Switch

VMware vSphere 7 has the possibility to use vSphere Distributed Switch to manage multiple hosts at the same time and “push” the configuration to multiple hosts at the same time. With the traditional vSphere Standard Switch (vSS), you have to repeat the configuration on a per-host basis.

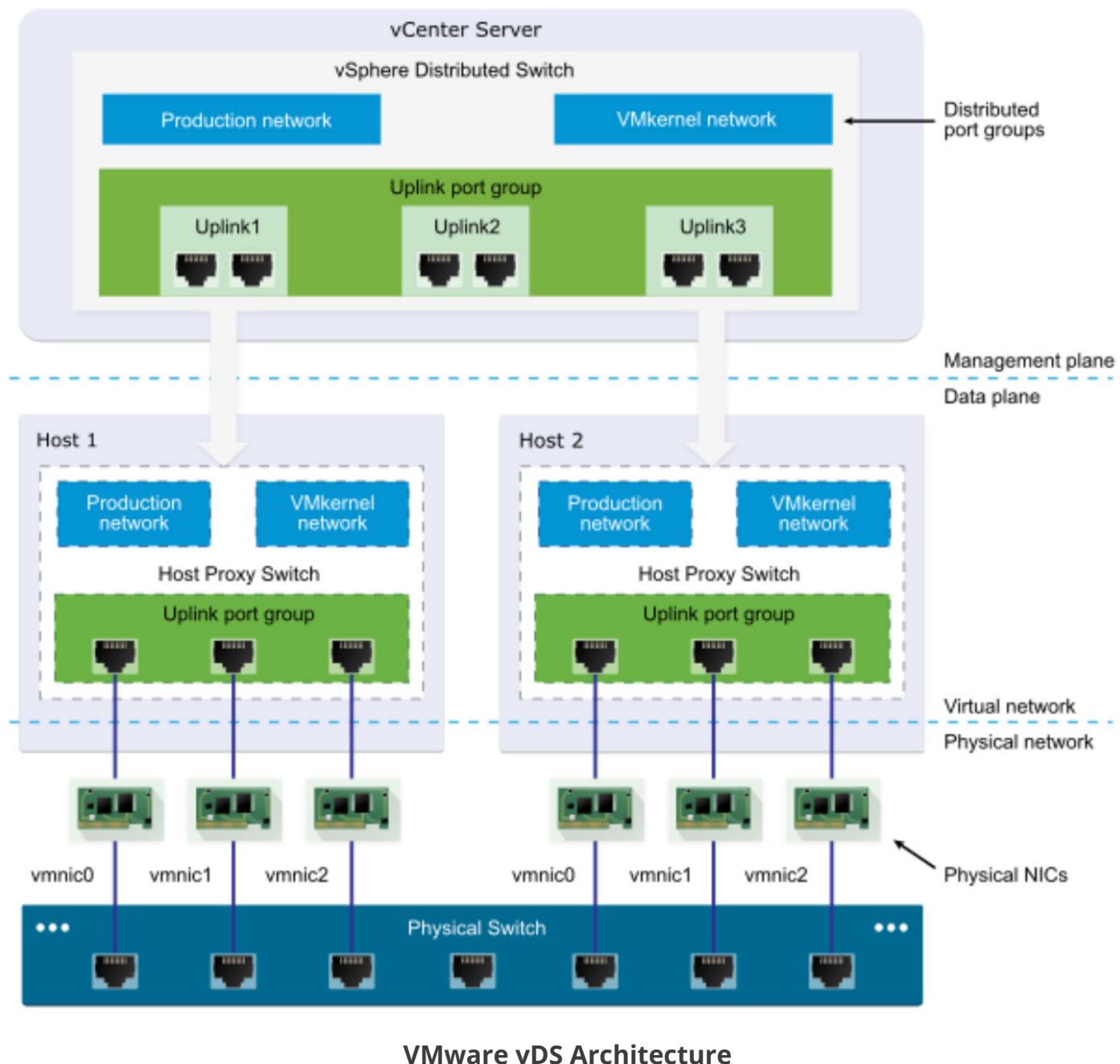
A vSphere Distributed Switch (vDS) acts as a single virtual switch that is associated with selected hosts in your datacenter. You can pick a host that is part of vDS but you don’t have to “attach” all the hosts from your environment.

vDS provides centralized provisioning, monitoring, and management of virtual networks for your hosts and virtual machines (VMs). You can create and configure distributed switches on a vCenter Server system, so you need as a hard requirement vCenter Server.

Another hard requirement is licensing. You’ll need an Enterprise Plus license or a vSAN license. It’s because VMware has made this configuration available only for customers who have purchased a vSAN license.

The vCenter Server propagates the vDS configuration to each connected ESXi host in the form of a host proxy switch. The ESXi host provides the data plane for the I/O traffic. The data plane implements the packet switching, filtering, tagging, and other features for the Ethernet packet. However, the management plane is provided only via vCenter Server.

If your vCenter server is down for some reason, it does not matter for the normal functioning of VMs and hosts, but it matters for configuration. Without vCenter Server, you can’t configure vDS.



## Distributed Port groups

As in vSS, vDS has port groups. They're called distributed port groups. There are connections from VMkernel network adapters and also VMs NICs that connect there. A set of distributed ports is called a distributed port group.

VMware has created those distributed port groups to simplify the configuration and management of distributed ports. You can basically apply unique network labels to each distributed port group and they are propagated to all hosts.

You can configure NIC teaming, VLAN, security, traffic shaping, and other policies to a distributed port group which then applies the policies to the underlying distributed ports. It's very powerful.

## Uplink port groups

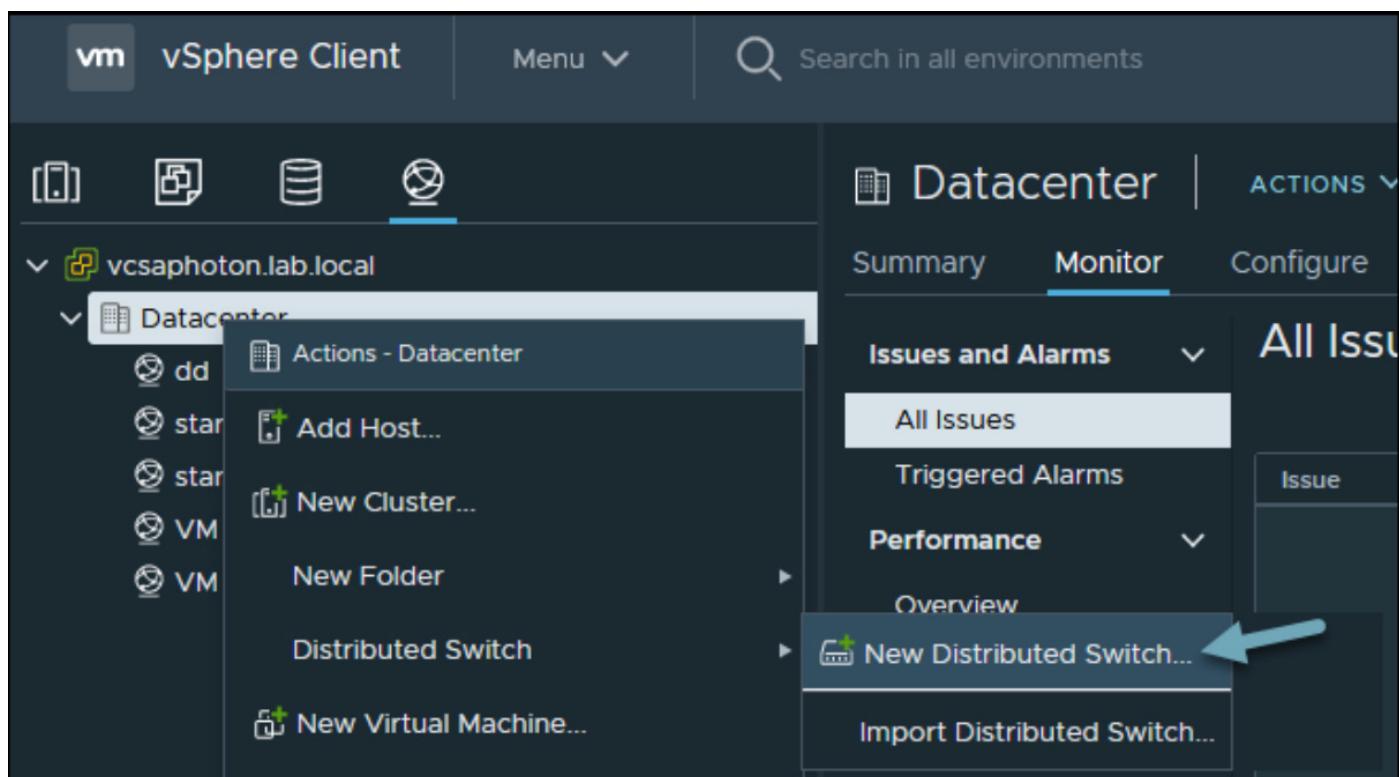
As with standard switches, there are uplinks that are providing connectivity to the physical world. An uplink port group has one or more uplinks. By default, there are 4 uplinks created when you first create a vDS.

Again, changing settings on the uplink port group, those settings are replicated to all the connected hosts.

vDS does have features that vSS does not. Private VLANs are one of those. You can also use vDS network policies that allow you to manage traffic shaping.

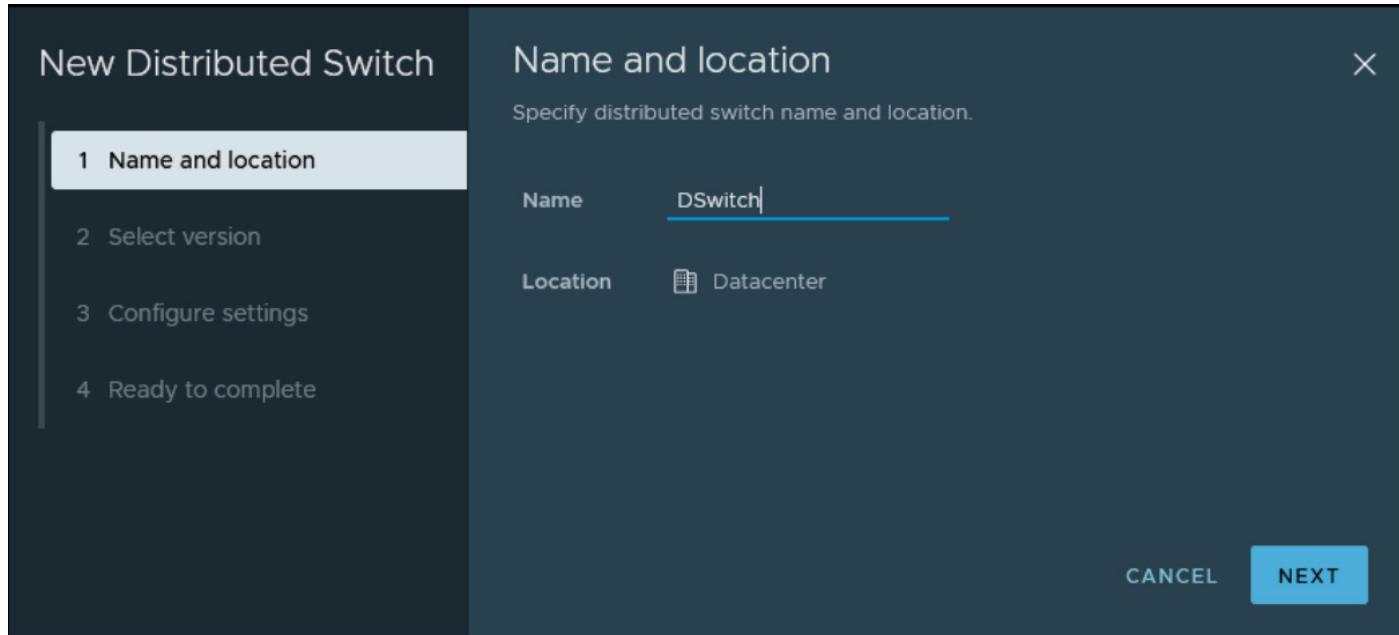
Now we're going to show you how to create a VMware vDS. First, you need to create the vSphere distributed switch. Go to the networking tab by clicking on the globe in the HTML5 client.

Then right-click on the datacenter and select **Distributed Switch > New Distributed Switch**



Create new vSphere Distributed Switch

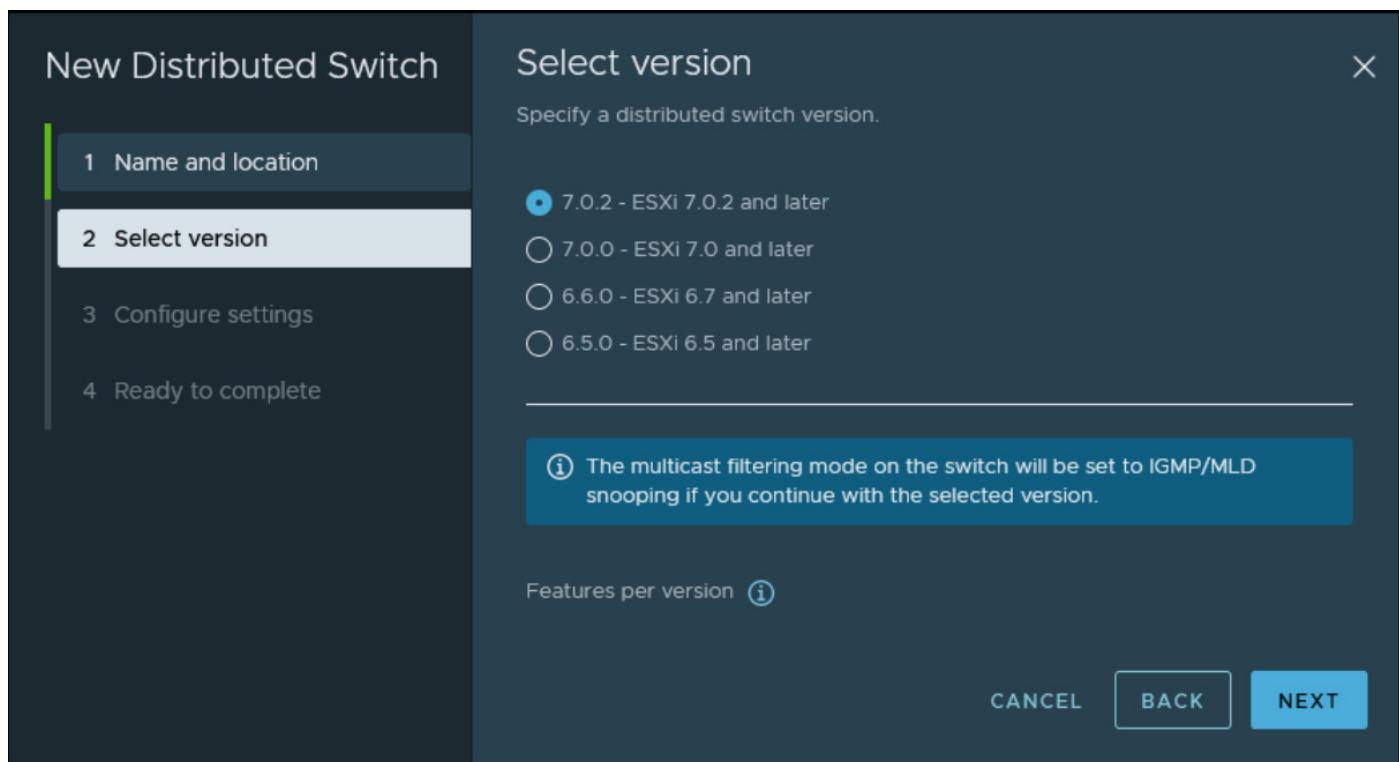
Next, enter some meaningful name for your switch. Note that within your datacenter you might be creating several vDS, so a proper naming convention is probably a good idea.



### Create a new vSphere Distributed Switch Wizard

We can choose which version of vDS we'll be creating. This is obviously for compatibility reasons. You might be running some older ESXi hosts that aren't migrated to vSphere 7 so you'd be obviously picking up the older version of the vDS.

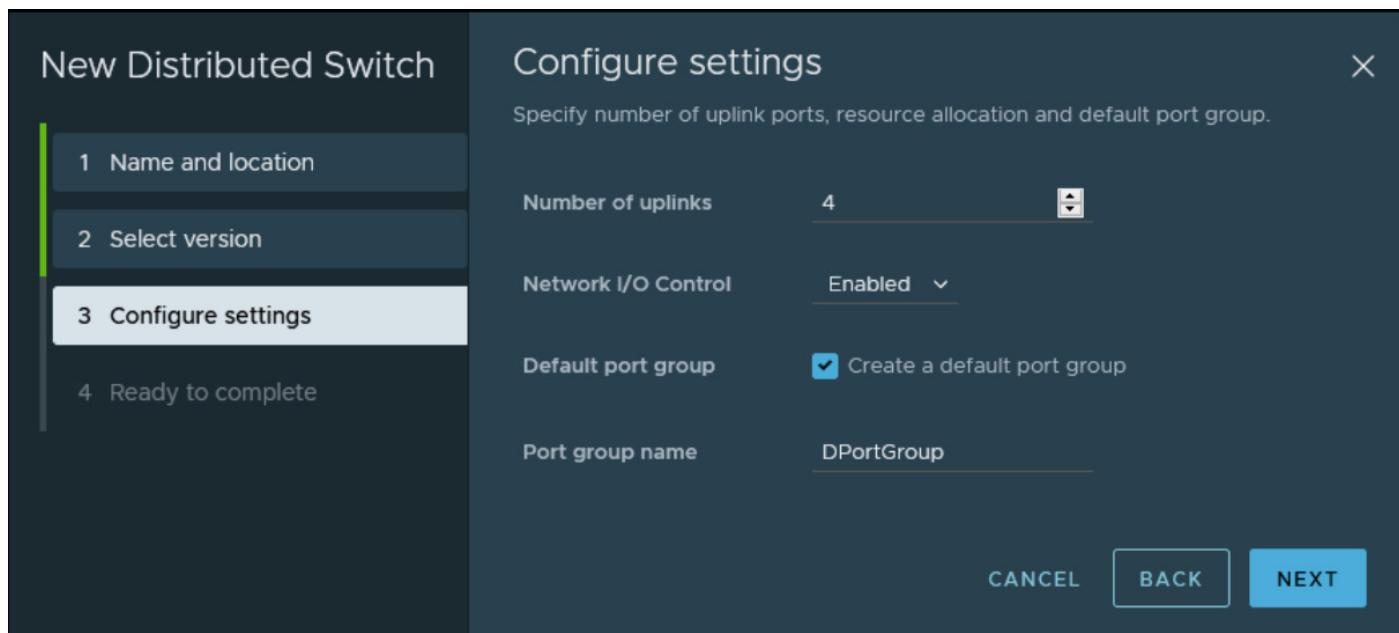
The vDS has evolved since vSphere 6.x to 7.0.2 by adding additional features and options. Let's move on with the wizard.



### Create new vSphere Distributed Switch Wizard – Select version

Next, we need to select how many uplinks we'll connect to this switch and whether we want to enable Network I/O control (by default, it's enabled).

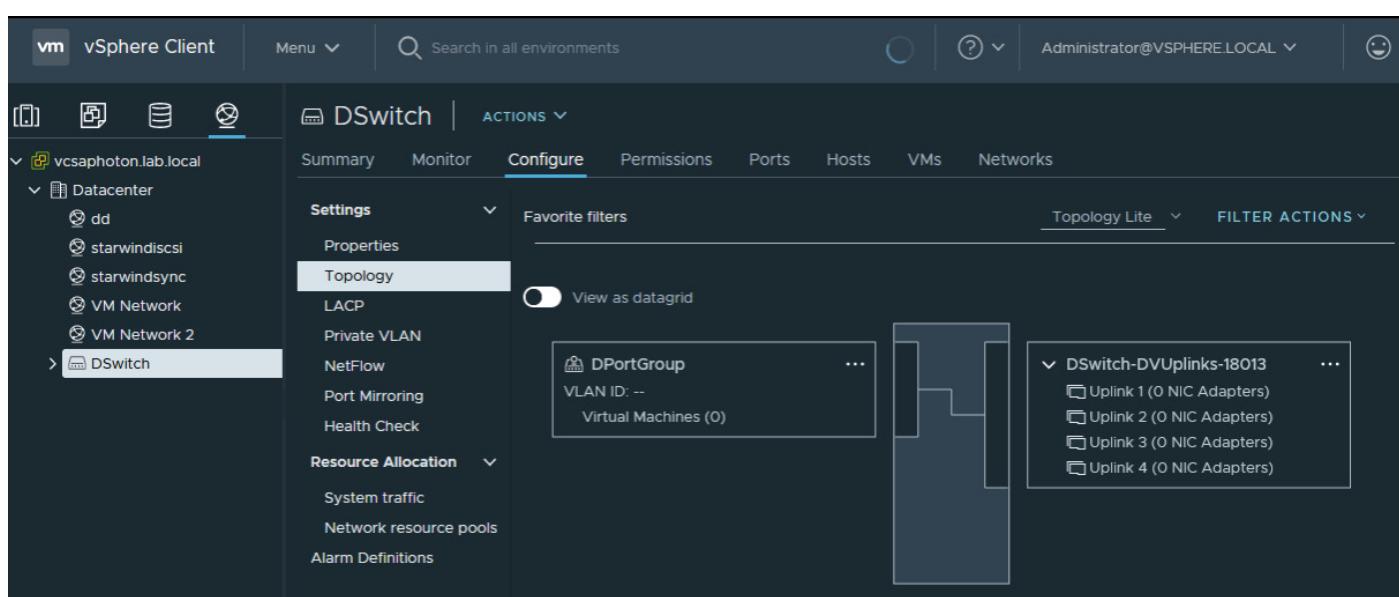
Also, on this page, we're asked to create the default port group. You can pick a name for this distributed port group here or rename it later.



### Create new vSphere Distributed Switch Wizard – Uplinks and port group

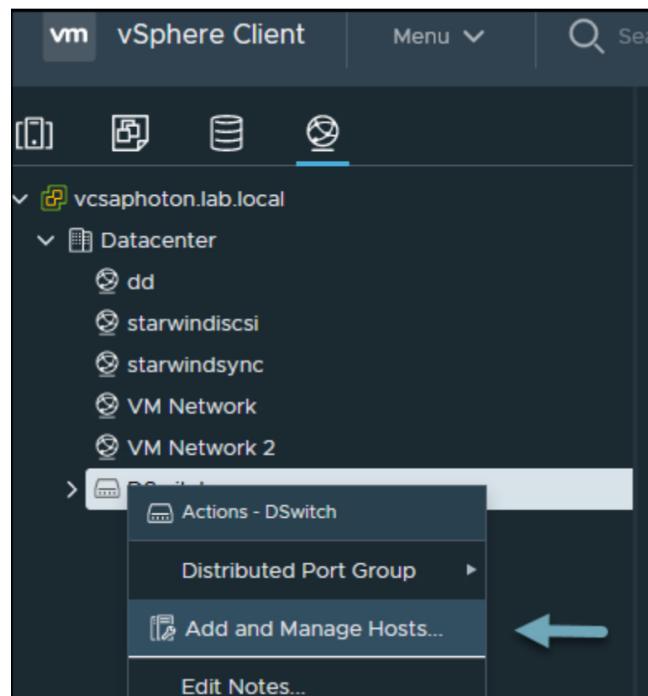
On the next page, you'll see the summary. Click the finish button to create your vDS. You can have a look at the vDS topology. You're still in the networking section, and you should see your vDS here.

Click on the vDS and select **Configure > Topology**.



**VMware vDS Topology**

Next, we need to associate some of our hosts with vDS. To do that, you can right-click the vSphere distributed switch and click **Add and Manage Hosts**.



### Add and manage hosts

Then we have another wizard where we can either Add hosts, manage host networking or remove hosts.

The screenshot shows the "DSwitch - Add and Manage Hosts" wizard. On the left, a vertical navigation bar lists steps: 1 Select task, 2 Select hosts, 3 Manage physical adapters, 4 Manage VMkernel adapt..., 5 Migrate VM networking, and 6 Ready to complete. Step 1 is highlighted. The main area is titled "Select task" with the sub-instruction "Select a task to perform on this distributed switch." Three radio buttons are available: "Add hosts" (selected), "Manage host networking", and "Remove hosts". The "Add hosts" option has a description: "Add new hosts to this distributed switch." The "Manage host networking" option has a description: "Manage networking of hosts attached to this distributed switch." The "Remove hosts" option has a description: "Remove hosts from this distributed switch." At the bottom are "CANCEL", "BACK", and "NEXT" buttons.

### Add hosts to vDS

Next, select your hosts that you want to connect to your vDS.

Select New Hosts | DSwitch 1 X

SHOW INCOMPATIBLE HOSTS

Filter

	Host	Host State	Cluster	Compatibility
<input checked="" type="checkbox"/>	esxi01.lab.local	Connected	Cluster	<span style="color: green;">✓ Compatible</span>
<input checked="" type="checkbox"/>	esxi02.lab.local	Connected	Cluster	<span style="color: green;">✓ Compatible</span>
<input checked="" type="checkbox"/>	esxi03.lab.local	Connected	Cluster	<span style="color: green;">✓ Compatible</span>
<input type="checkbox"/>	esxi04.lab.local	Connected	N/A	<span style="color: green;">✓ Compatible</span>

4 items

CANCEL OK

### Select your hosts

Next, you'll need to assign the physical NICs to an uplink and click Next again.

DSwitch 1 - Add and Manage Hosts

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

**Manage physical adapters**  
Add or remove physical network adapters to this distributed switch.

Assign uplink Unassign adapter View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
▼ esxi01.lab.local			
▲ On this switch			
▼ vmnic3 (Assigned)	--	Uplink 1	DSwitch 1-DVUpli...
▶ On other switches/unclaimed			
▼ esxi02.lab.local			
▲ On this switch			
▼ vmnic3 (Assigned)	--	Uplink 1	DSwitch 1-DVUpli...
▶ On other switches/unclaimed			
▼ esxi03.lab.local			
▲ On this switch			
▼ vmnic3 (Assigned)	--	Uplink 1	DSwitch 1-DVUpli...
▶ On other switches/unclaimed			

CANCEL BACK NEXT

### Assign an uplink

Next, we have an option to migrate any VMkernel adapters if we want to (not mandatory).

**DSwitch 1 - Add and Manage Hosts**

**Manage VMkernel adapters**  
Manage and assign VMkernel network adapters to the distributed switch.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Gr...
esxi01.lab.local			
On this switch			
On other switches/unclaimed			
vmk0	vSwitch0	Management Net...	Do not migrate
vmk1	vSwitch0	vsan	Do not migrate
esxi02.lab.local			
On this switch			
On other switches/unclaimed			
vmk0	vSwitch0	Management Net...	Do not migrate
vmk1	vSwitch0	vsan	Do not migrate
esxi03.lab.local			
On this switch			

**CANCEL** **BACK** **NEXT**

## Migrate VMkernel adapters if you want to

And we have an option to migrate VM networking as well.

**DSwitch 1 - Add and Manage Hosts**

**Migrate VM networking**  
Select virtual machines or network adapters to migrate to the distributed switch.

Migrate virtual machine networking

Host/Virtual Machine/Network Adapter	NIC Count	Source Port Group	Destination Port Group
esxi01.lab.local			
2008R2	1		Reassigned
Z-VRA-esxi01.lab.local	1		
esxi02.lab.local			
StarWind01	3		
Z-VRA-esxi02.lab.local	1		
esxi03.lab.local			
Z-VRA-esxi03.lab.local	1		

**CANCEL** **BACK** **NEXT**

## Migrate VM networking

Next, just click Finish to close the assistant. We're done. You can now make changes to all hosts connected to your vDS. This is the main advantage over the standard vSwitches.

## Objective 1.7.3 Describe networking policies

VMware vSphere 7 has networking policies that can be applied to both vSphere Standard Switch (vSS) and vSphere Distributed Switch (vDS).

You set networking policies on virtual switches to configure different properties of the virtual network such as connectivity to virtual machines (VMs) and VMkernel services, VLAN tagging, security, and others.

You can use NIC teaming policy to connect a virtual switch to multiple physical NICs on a host to increase the network bandwidth of the switch and to provide redundancy. Several physical NIC adapters in a NIC team can distribute the traffic between its members and provide passive failover in case of adapter failure or if the network is down.

You can 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.

### vSphere Standard Switch

On VSS, you set the networking policies on the entire VSS or on the individual port groups. If you set the policies on the entire switch, the policies apply on all the port groups present within this switch. If you want to apply different policies to specific port group, you need to apply the policy to that particular port group and check "override" policies set on the switch on the per-portgroup level.

As an example, we can show you that you can specify which physical network adapters handle the network traffic for the VSS.

Connect to vCenter server via vSphere client, select your **host > Configure > Networking > Virtual Switches**.

The screenshot shows the vSphere Web Client interface for host 'esxi01.lab.local'. The 'Configure' tab is selected. In the left sidebar under 'Networking', 'Virtual switches' is highlighted with a blue arrow. The main pane displays 'Virtual switches' with three entries: 'Management Network', 'VM Network', and 'vsan'. Each entry has a '... More' button. To the right, a 'Physical Adapters' section lists 'vmnic0' and 'vmnic7' with status '10000 Full'. A blue arrow points from the top right towards the 'Management Network' entry.

### Edit properties of vSphere Standard Switch

Then select the vmnic7 and click the up arrow to move this adapter to the "Active adapters" section.

The screenshot shows the 'vSwitch0 - Edit Settings' dialog. The 'Teaming and failover' tab is selected. In the 'Failover order' section, 'vmnic0' is listed under 'Active adapters' and 'vmnic7' is listed under 'Unused adapters'. A blue arrow points from the left towards the 'Teaming and failover' tab. Another blue arrow points from the top left towards the 'Failover order' section. On the right, a detailed adapter properties table shows information for 'vmnic7': Adapter: VMware Inc. vmxnet3 Virtual Ethernet Controller; Name: vmnic7; Location: PCI 0000:05:00.0; Driver: nvmxnet3; Status: Connected; Actual speed, Duplex: 10 Gbit/s, Full Duplex; Configured speed, Duplex: 10 Gbit/s, Full Duplex; Networks: 192.168.30.1-192.168.30.1. At the bottom, a note says 'Select active and standby adapters. During a failover, standby adapters activate in the order specified above.' with 'CANCEL' and 'OK' buttons.

Select the unused adapter and move it up to the active adapters section

And now we have two active uplinks configured for this vSwitch.

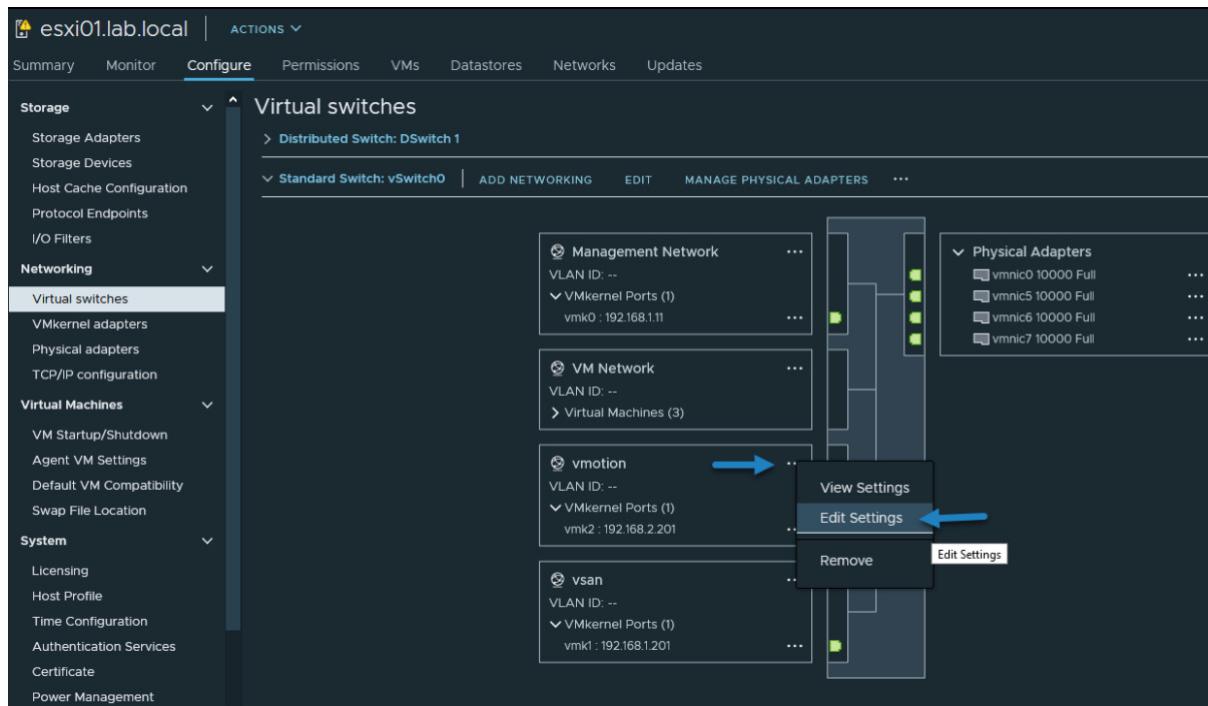
The screenshot shows the 'vSwitch0 - Edit Settings' dialog. In the 'Teaming and failover' section, 'Load balancing' is set to 'Route based on originating virtual port', 'Network failure detection' is set to 'Link status only', 'Notify switches' is set to 'Yes', and 'Fallback' is set to 'Yes'. The 'Failover order' section lists 'Active adapters' as vmnic0 and vmnic7, with vmnic7 currently selected. The right panel displays adapter details for vmnic7, including Adapter (VMware Inc. vmxnet3 Virtual Ethernet Controller), Name (vmnic7), Location (PCI 0000:05:00.0), Driver (nvmxnet3), Status (Connected), Actual speed, Duplex (10 Gbit/s, Full Duplex), Configured speed, Duplex (10 Gbit/s, Full Duplex), and Networks (192.168.30.1-192.168.30.1). Below the adapter list, a note says 'Select active and standby adapters. During a failover, standby adapters activate in the order specified above.' At the bottom are 'CANCEL' and 'OK' buttons.

### Two active NICs as uplinks are now configured for the VSS

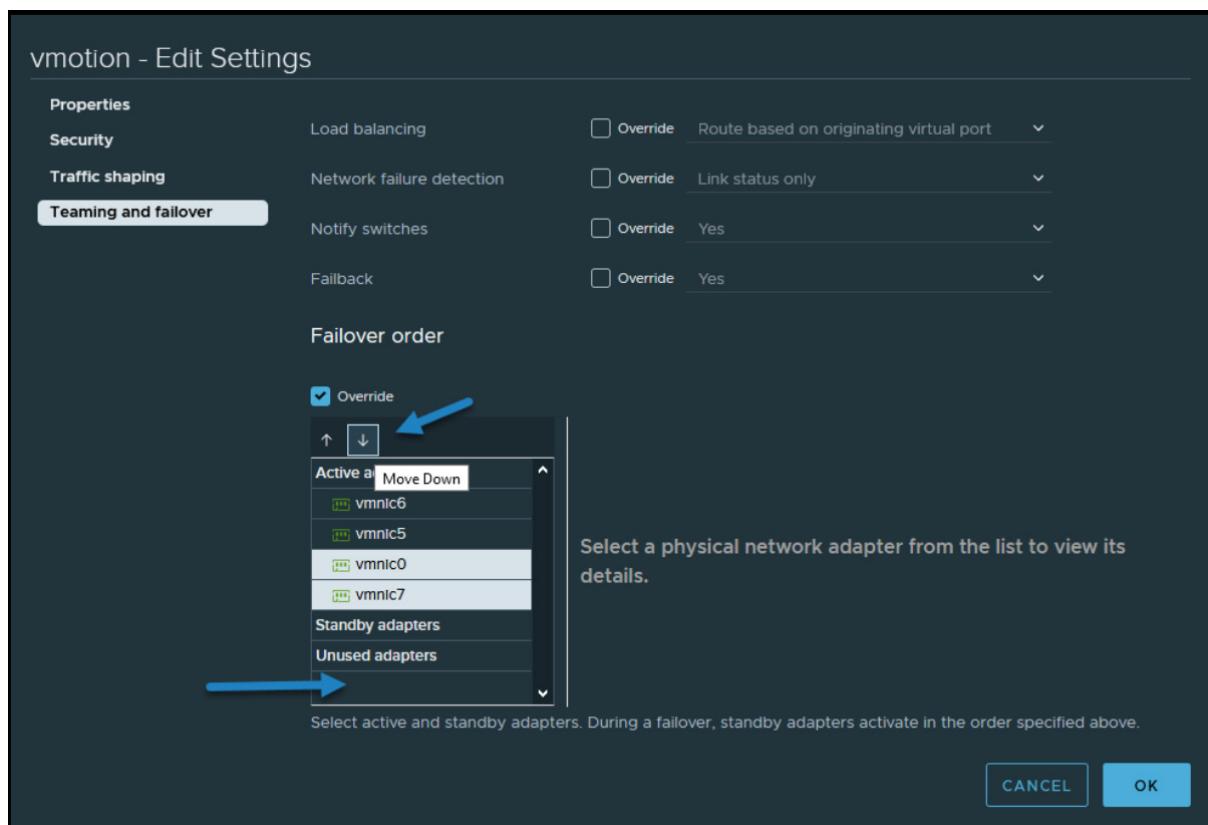
Click OK to validate the configuration.

If you want to apply a network policy to a portgroup level we can show you another example. Let's say that you have added 2 other physical NICs to your ESXi host, and you want to use those adapters only for vMotion traffic and experience faster vMotion.

Go back to the **VSS > select vMotion > Edit settings > Teaming and Failover**.

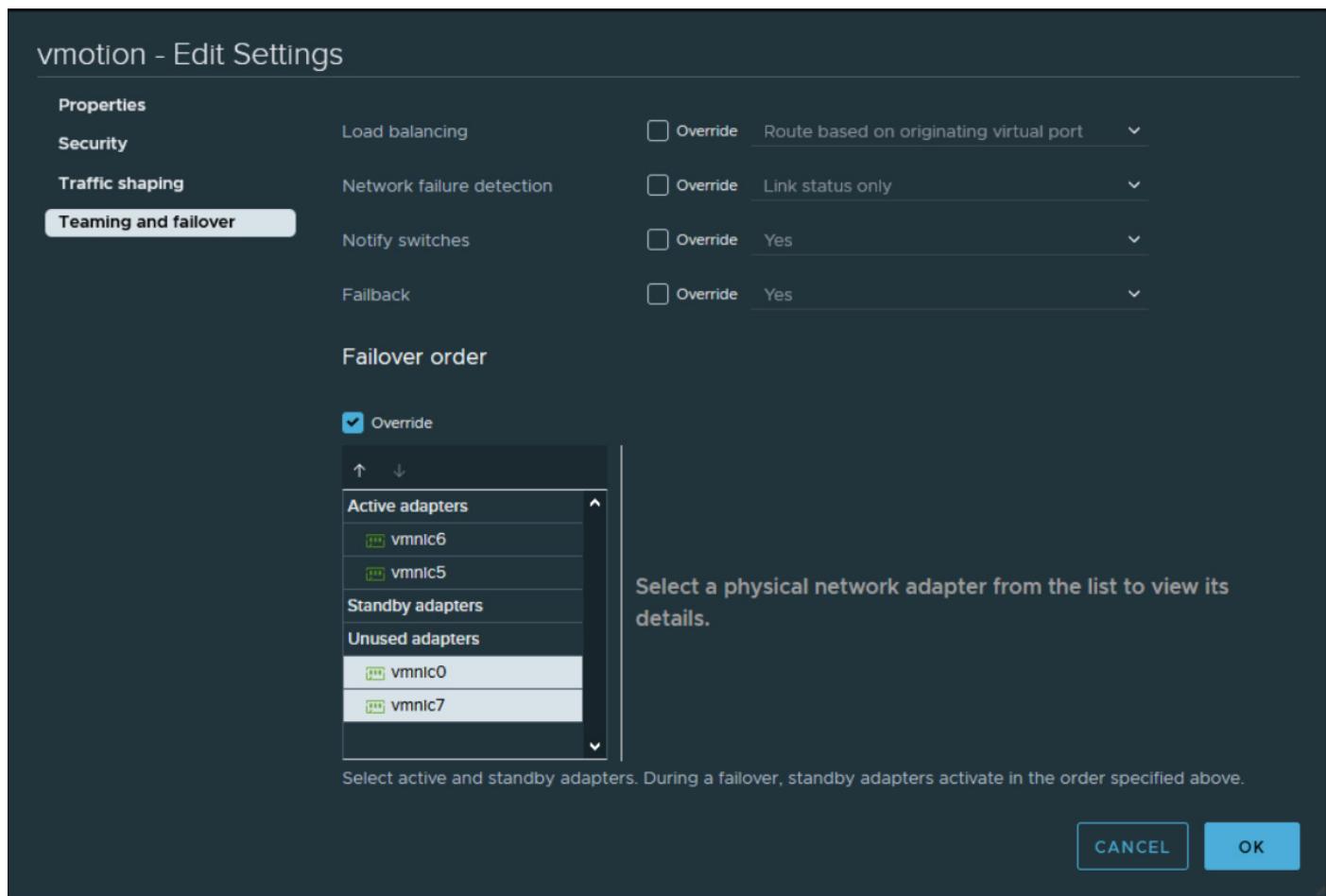


First, check the “**override**” checkbox. Leave the NICs that you plan to use for vMotion traffic, select the other two NICs, and click the down arrow to move them to the unused section. The override option simply allows you to override the global VSS network policy applied at the switch level above.



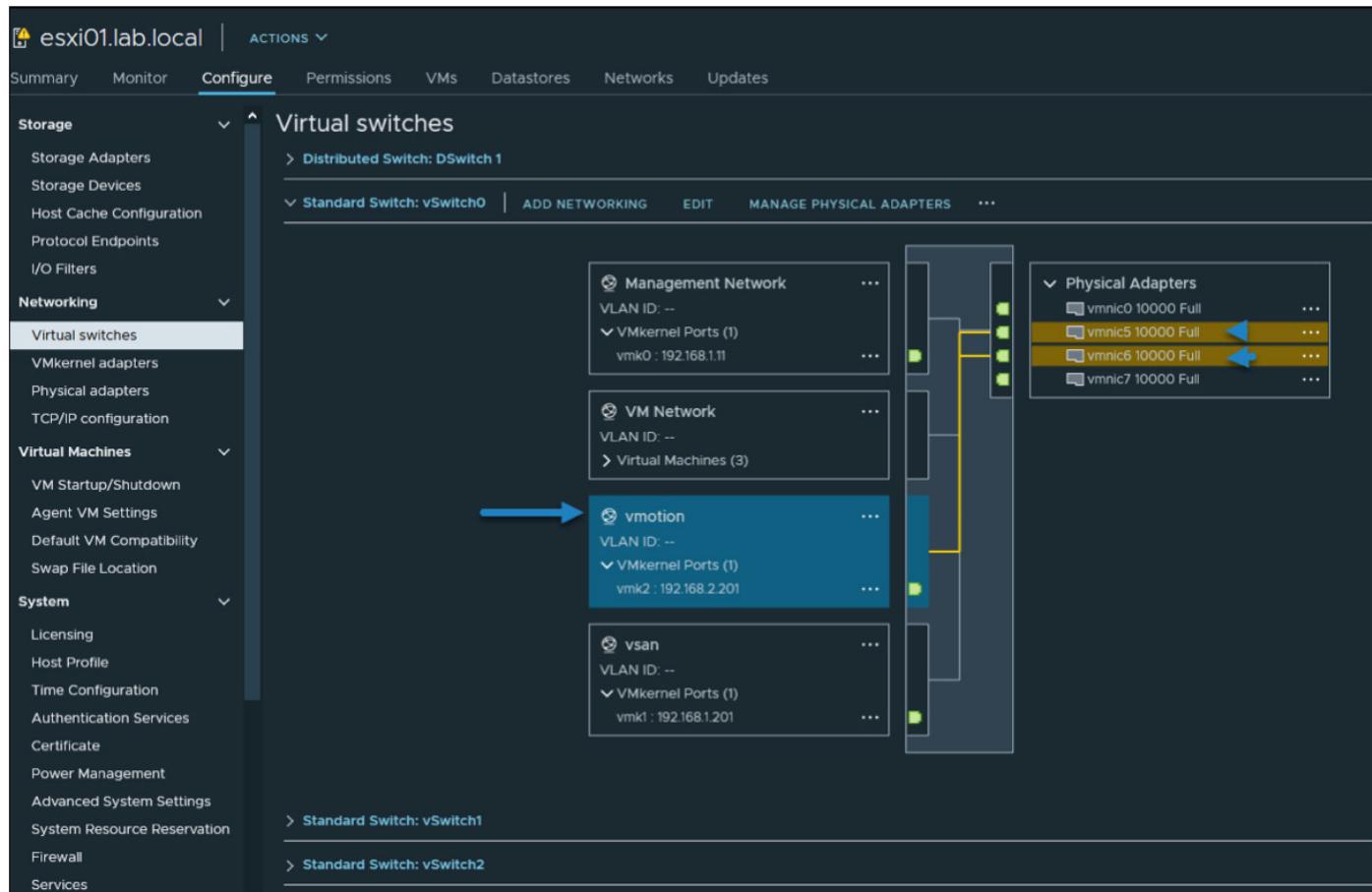
Select the other two uplinks and move them to the unused section

You can click OK to validate the configuration. Your vMotion port group should now look like this. You have two NICs dedicated to vMotion and two NICs that are unused (they're used for other services already).



**Click validate to save the configuration**

If you want to check which NICs are used for each of the port groups, simply click on the link in each port group and you'll have a visual. In our example, we can see that when we click the vMotion link on the port group, we can see visually which NICs are used for vMotion traffic.



When you click the vMotion link you should see which NICs are used for vMotion traffic

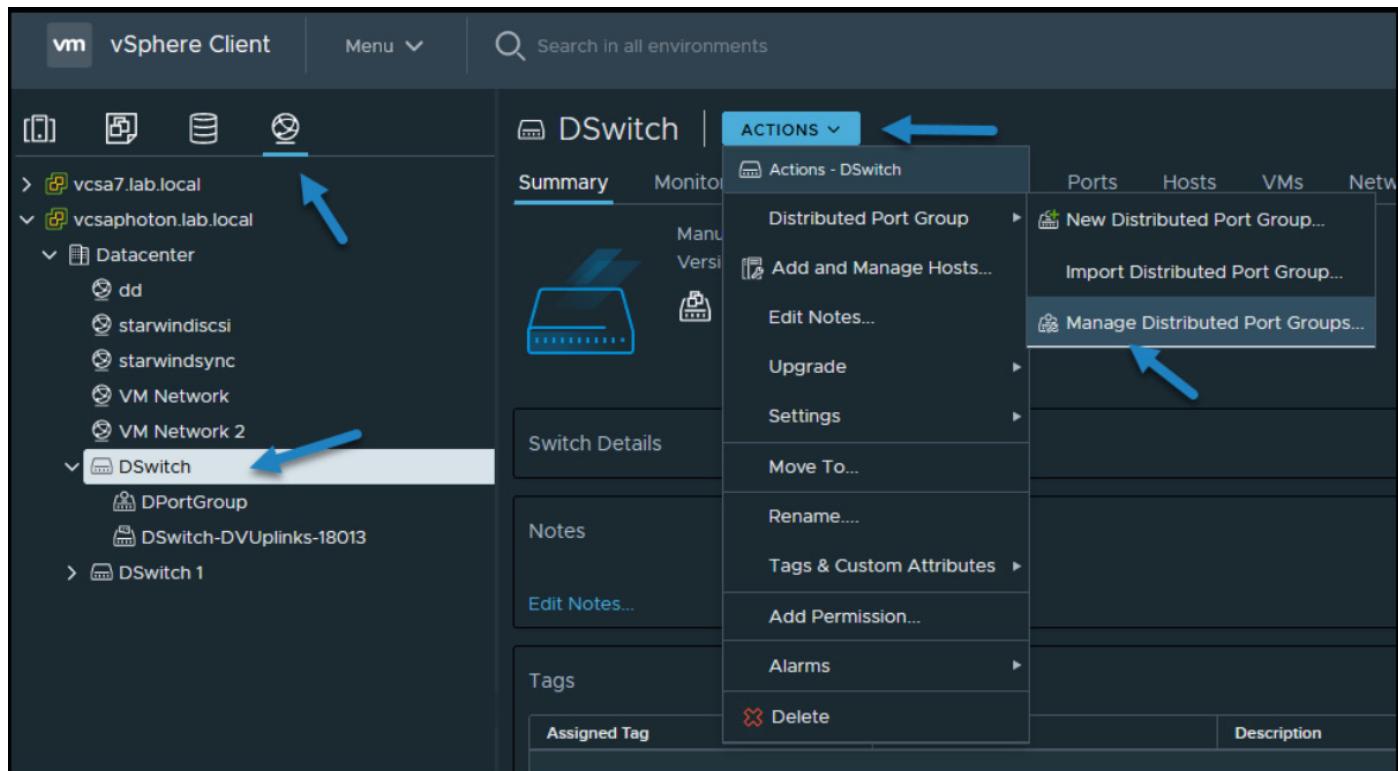
## vSphere Distributed Switch (vDS)

If you're lucky and have an Enterprise Plus license, or if you're running VMware vSAN, you can configure networking policies on vDS.

In vDS, you set networking policies on distributed port groups or uplink port groups. Policies apply to all ports in the group.

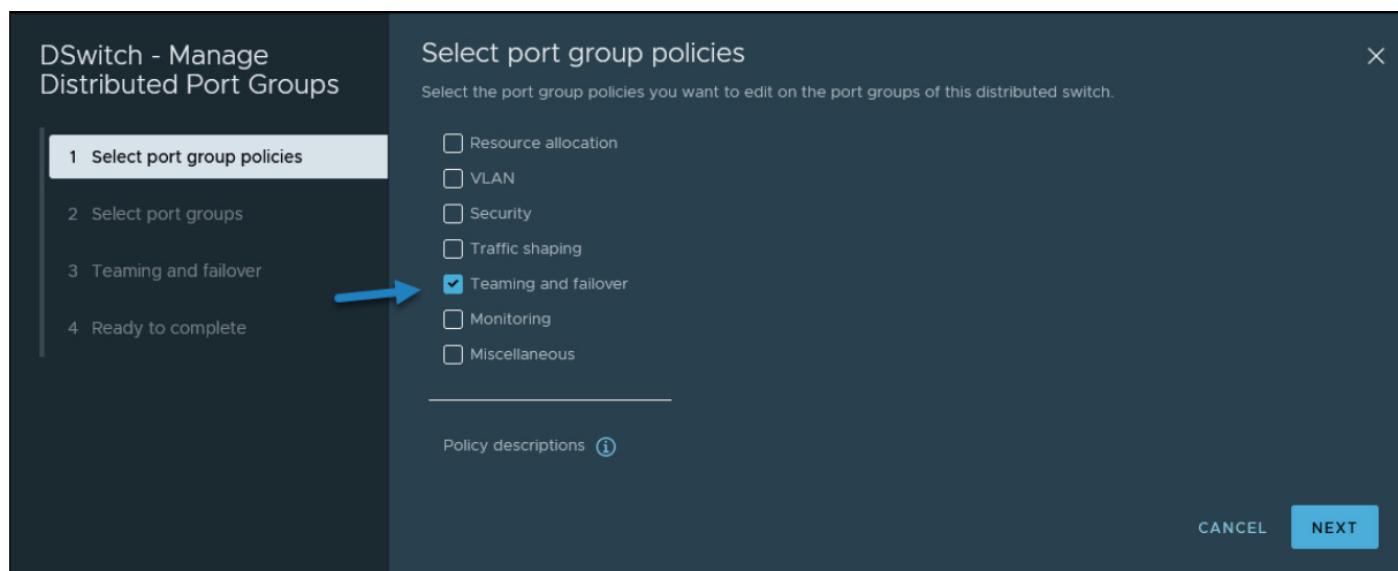
To have different policies per specific port, you can override the policies set on the port group on a per-port level. This is useful when you want to set a specific policy for individual VMs or physical network adapters.

Go to **Networking**, select your **vDS** > **Actions** > **Manage Distributed Port Groups**



## Manage Distributed Port groups on vDS

You'll have a new assistant that will show up. Select Teaming and Failover.



## Select Teaming and Failover

Click next to select the port groups. In our example, we select all three port groups.

**Select port groups**

Select the port groups on this distributed switch that you want to edit.

Filter Selected (3)

Name	VLAN ID
DPortGroup	VLAN access: 0
DPortGroup2	VLAN access: 0
DPortGroup3	VLAN access: 0

3 items

CANCEL BACK NEXT

### Select all three port groups

Then on the next page select the uplink 3 and 4 and click the **Move Down** button to “push” them to the **Unused uplinks** section.

**Teaming and failover**

Controls load balancing, network failure detection, switch notification, fallback and uplink failover order.

Load balancing: Route based on originating virtual port

Network failure detection: Link status only

Notify switches: Yes

Fallback: Yes

**Failover order ⓘ** ↓

MOVE UP MOVE DOWN SELECT ALL DESELECT ALL

Active uplinks: Move Down  
 Uplink 1  
 Uplink 2  
 Uplink 3  
 Uplink 4

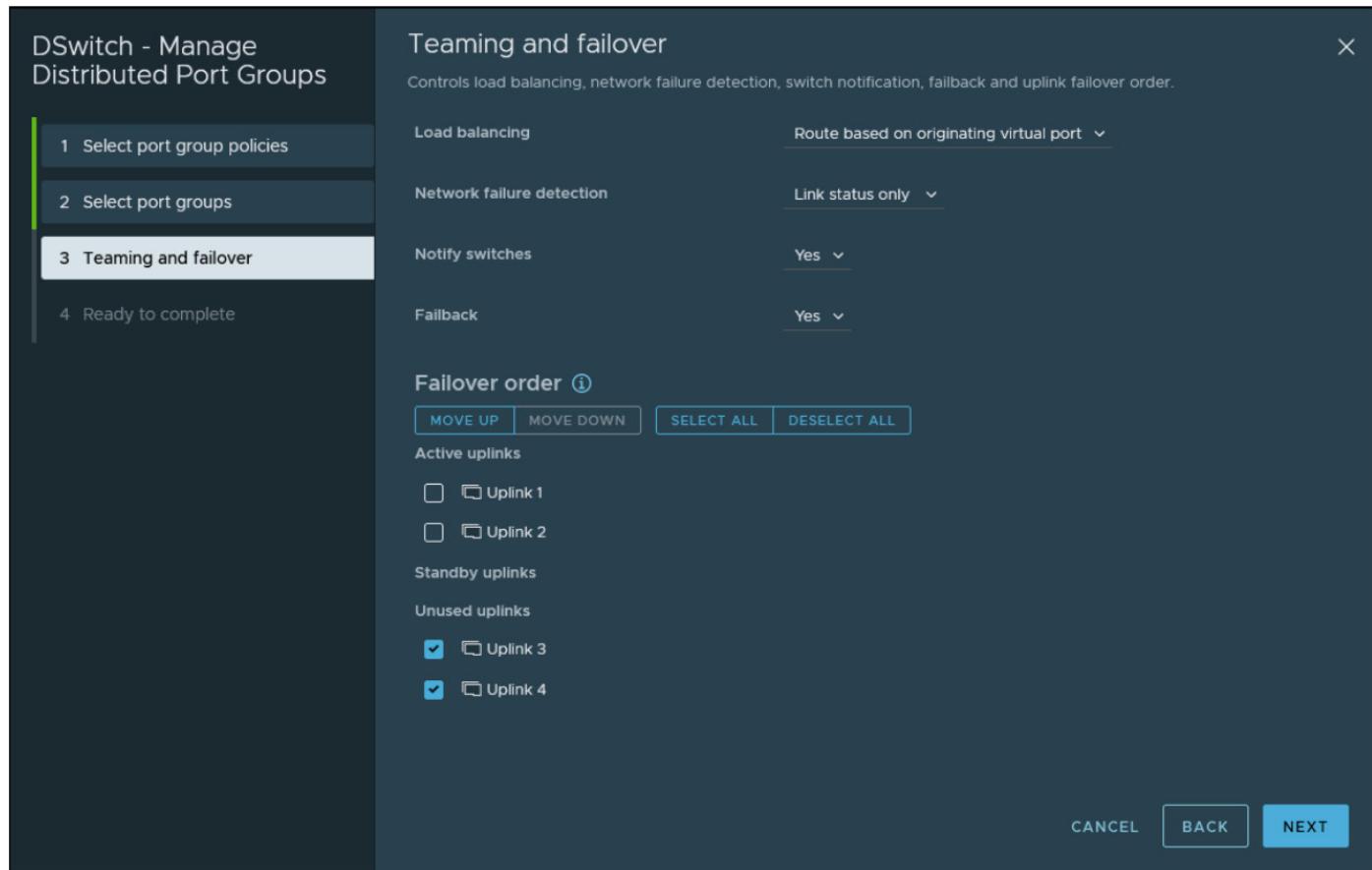
Standby uplinks

Unused uplinks

CANCEL BACK NEXT

### Select uplink 3 and 4 and click the Move down button

Then click OK to validate and save your settings.



### Click validate to save your settings

You're done. You have just configured simultaneously 3 different port groups with a single networking policy. This is the power of distributed switches. You can apply your configuration to all your hosts that are attached to the VDS within your cluster. If you use only VSS, you would have to go and do this host-by-host.

If you're studying for VMware VCP-DCV exam, make sure to read the networking section where you can also find more information about VLAN policies, Security policies, Traffic shaping policies or resource allocation policies.

You'll also need to learn about Monitoring, traffic filtering, and port blocking policies. Those all are the sections that you'll be asked about in the exam.

vSphere 7 has improved the UI of the vSS and vDS. VMware did this by streamlining the steps and adding many visual assistants to make it easier to navigate the networking sections and make changes to the configurations.

## Objective 1.7.4 Manage Network I/O Control (NIOC) on a vSphere distributed switch

With Network I/O control (NIOC), you can adjust the bandwidth of your vSphere 7 networks. You can set different bandwidths for specific types of traffic. Once you enable NIOC on vSphere Distributed vSwitch, you'll be able to set shares according to your needs.

There are separate models for **system traffic** (vMotion, fault tolerance, vSAN, etc.) and for **VM traffic**. The main goal of NIOC is to ensure that you have enough bandwidth for your virtual machines (VMs) and that you can control their resource allocation while still preserving sufficient resources for your system traffic.

I'm sure you already know this, but in order to use NIOC and vDS, you'll need vSphere Enterprise Plus licensing.

VMware vSphere 7 Distributed vSwitch (vDS) is version 7 of vDS. Version 7 of vDS introduced a new feature for VMware NSX product integration—NSX Distributed Port group. The previous version of vDS, 6.6.0, introduced the MAC Learning capability.

To create a new vDS, click the Networking icon (the globe). Then right-click **Datacenter object** and select **New vDS**. Select **Configure > Properties** to check the properties.

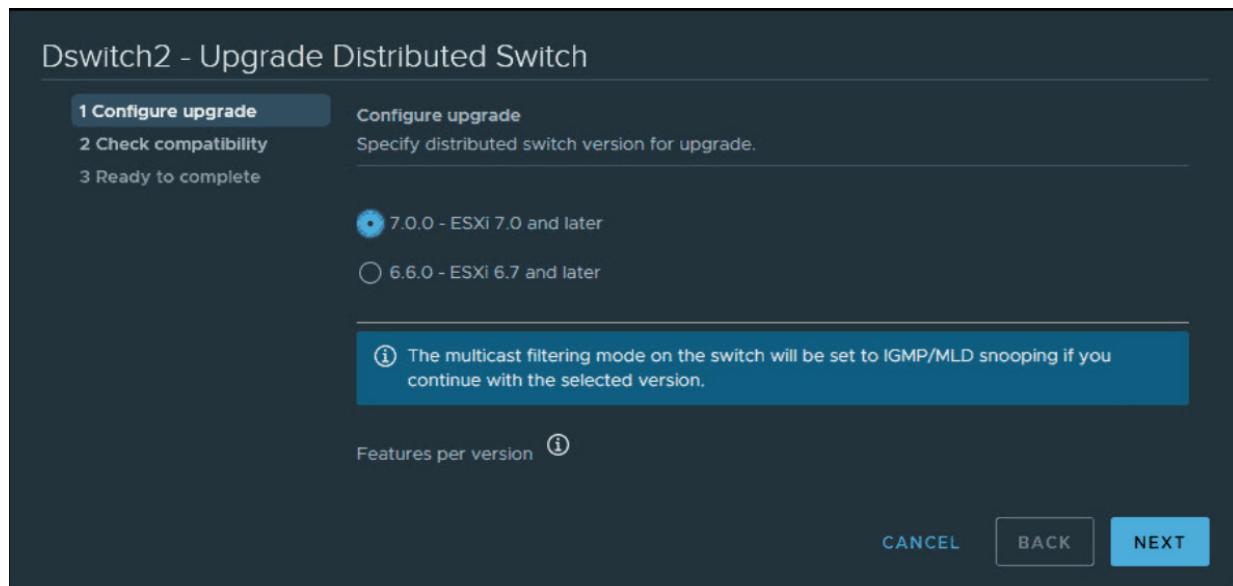
General	
Name	DSwitch
Manufacturer	VMware, Inc.
Version	7.0.0
Number of uplinks	4
Number of ports	20
Network I/O Control	Enabled

VMware vSphere 7 Distributed Switch properties

## How can vDS be upgraded from the previous release?

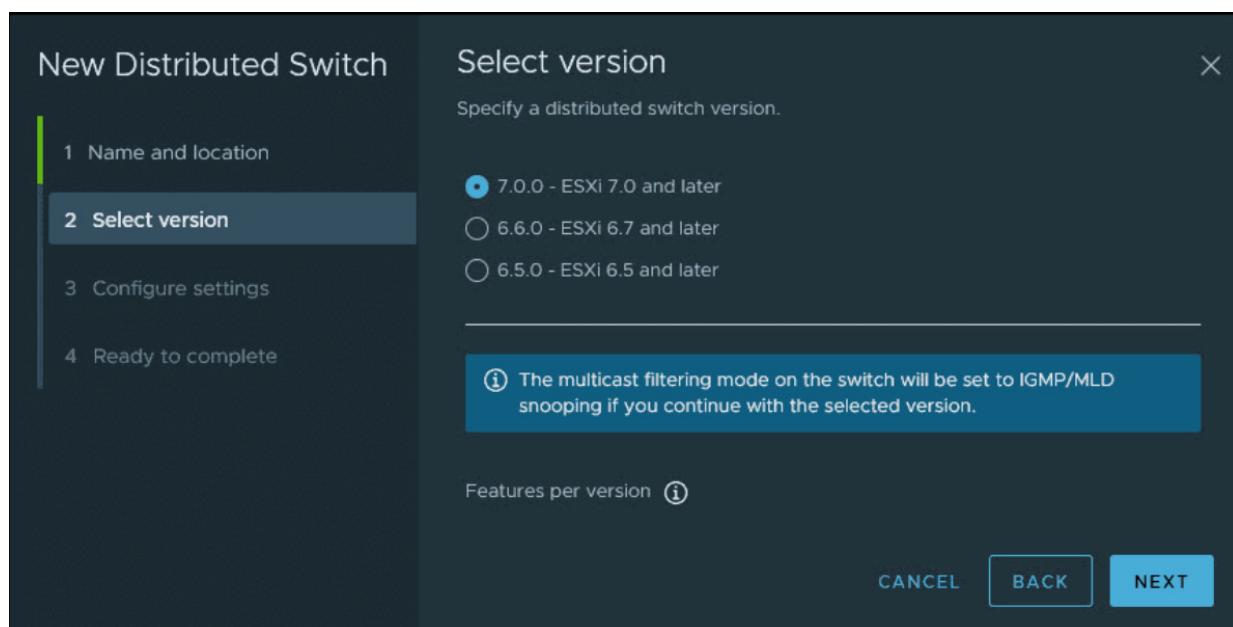
If you have upgraded recently from the previous release of vSphere, you can upgrade your vDS via the UI. We'll show you that later. Note that there is short downtime for the VMs attached to the switch.

Right-click your vDS and select > **Upgrade > Upgrade Distributed Switch**.



## Upgrade VMware Distributed Switch

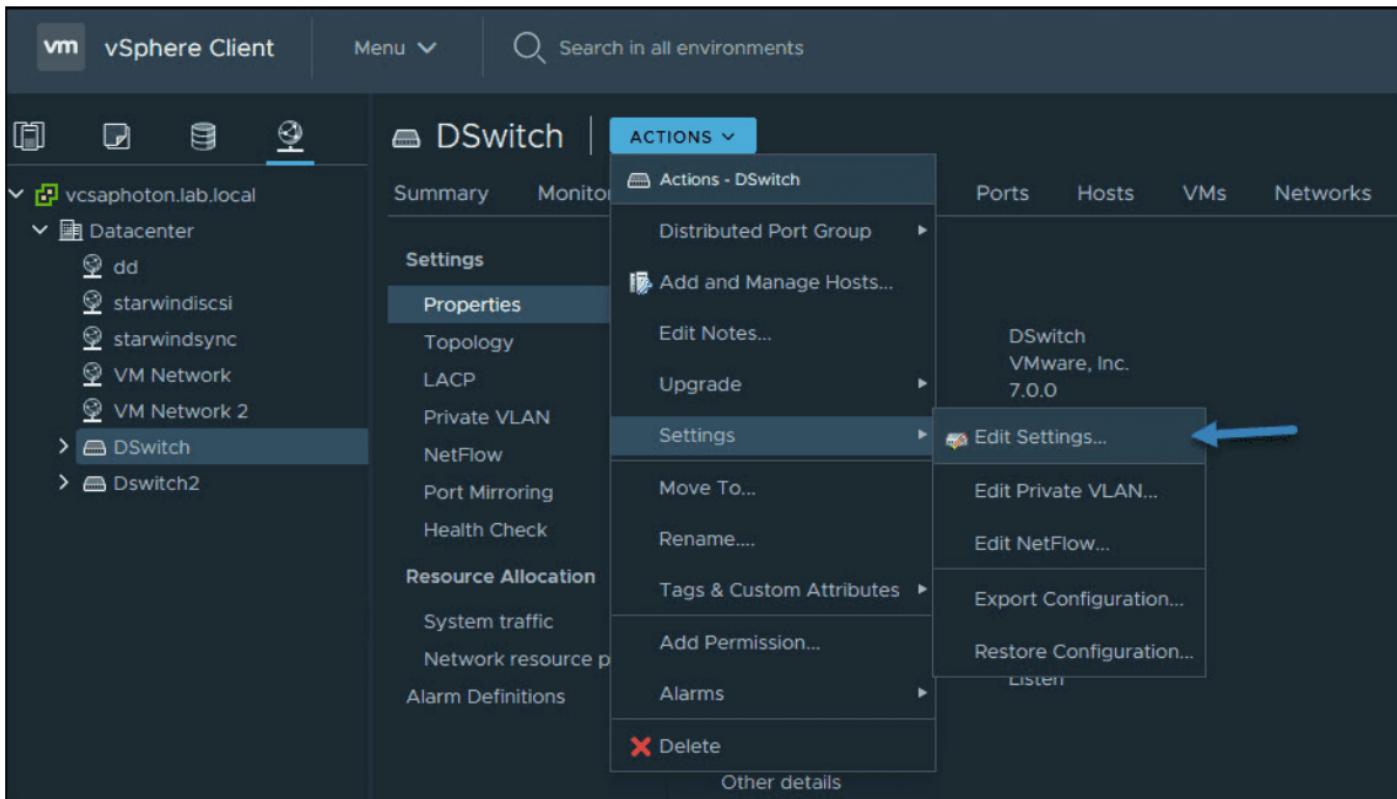
If you're running a fresh installation of vSphere 7 and creating a new vDS, you still have the option of creating previous versions of vDS, such as vSphere 6.5 or 6.7. You may need to ensure compatibility with the rest of your infrastructure, which might still be running older versions of vSphere.



## vSphere 7 and the option to create a different version of vDS

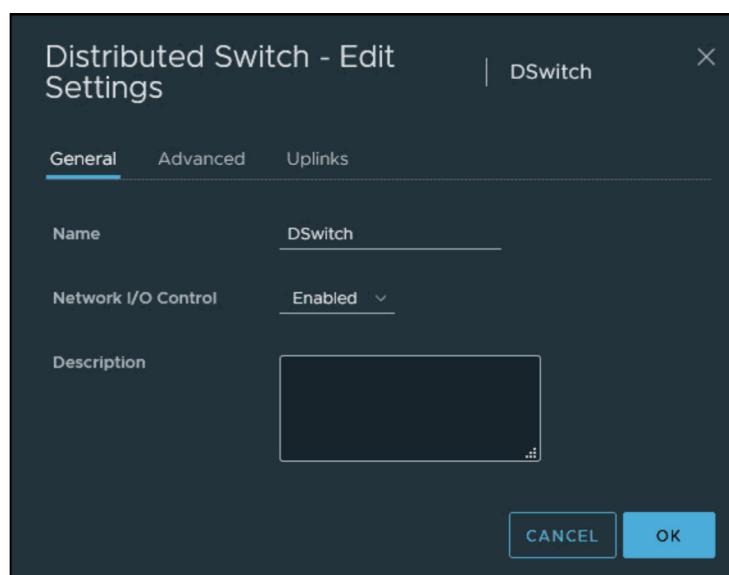
## Where should you enable NIOC?

You need to enable NIOC on each vDS. From Networking, select the vDS. Then select **Actions > Settings > Edit Settings**.



### Enable NIOC on vSphere 7 vDS

This opens a pop-up window where you can use the drop-down menu to enable or disable NIOC. NIOC is enabled by default.



### Enable NIOC drop-down menu

The traffic types are all set to 50 shares except the VM traffic. No reservation or limits are set by default.

The main vSphere features for which network traffic can be configured are:

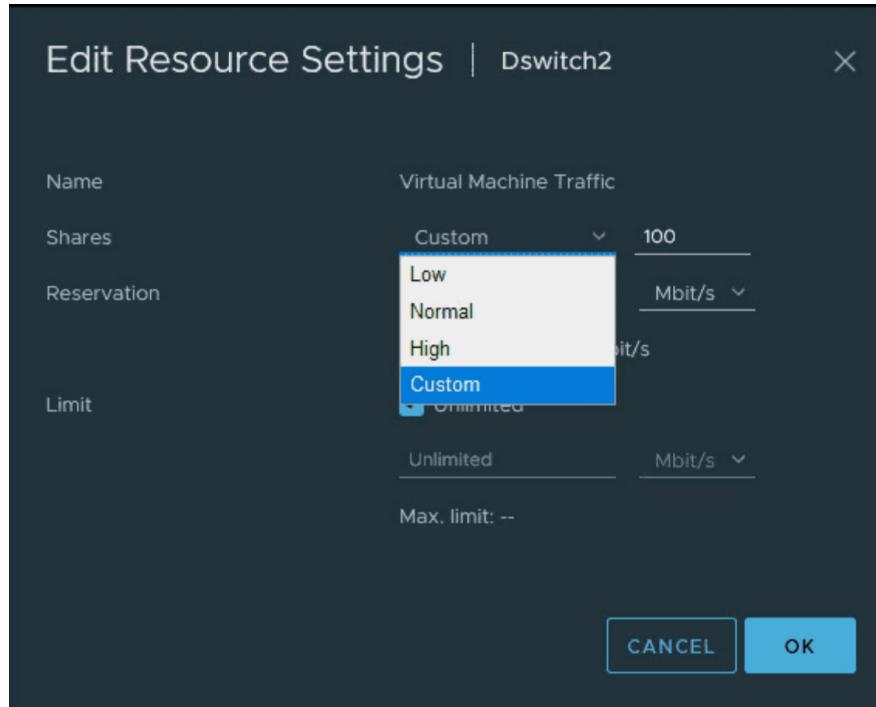
- Management networking traffic
- Fault tolerance (FT)
- NFS
- vSAN
- vMotion
- vSphere replication
- vSphere data protection backup
- Virtual machine

Here is the view of the system traffic and the default values. You can see that by default, all system types are at 50, while the VM value is at 100.

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

### VMware vDS system traffic default values

You can click the **Edit** button after selecting the type of traffic, and then modify the values by selecting **Custom**.



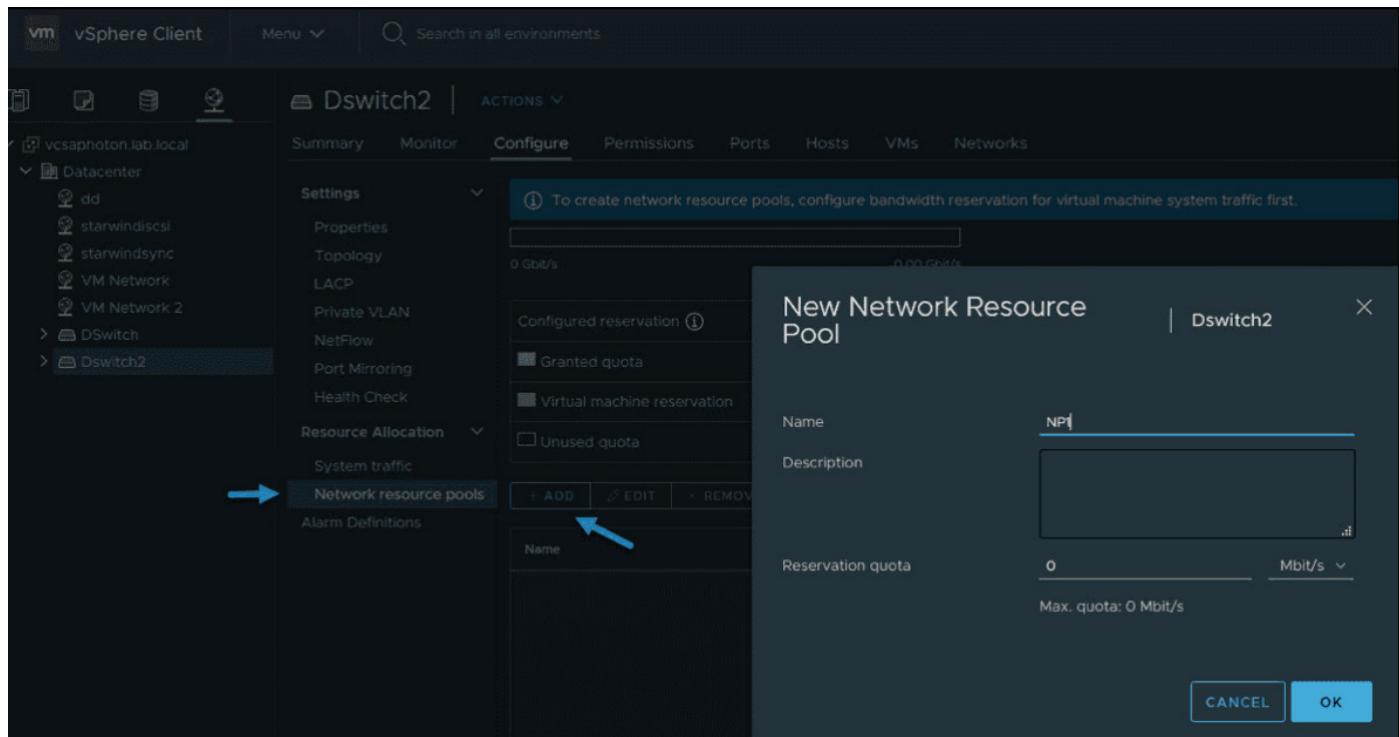
### Configure shares reservations and limits for different traffic types

The allocation parameters for the different traffic types are:

- **Shares** — Value from 1 to 100, where the maximum 100 is the priority of a traffic type compared to the other traffic types that are active on the same physical adapter.
- **Reservation** — Minimum bandwidth is in Mbps. This is the bandwidth guaranteed on a simple physical adapter.
- **Limit** — Sets the maximum allowed bandwidth, in Mbps or Gbps, that the traffic type can consume on a single physical adapter.

You can also create new resource types via the menu just below system traffic. Click the **Network resource pools** menu link and then click **Add**. This will create a new network resource pool that will have a reservation quota. You can then assign a VM to that pool.

This group basically takes off bandwidth from the Virtual Machine system type, so you would need to set up a bandwidth reservation for that group first.



### Create new network resource pool in vSphere 7

This is the main principle of NIOC in vSphere 7. NIOC has been around since vSphere 5. The latest version is version 3, which has improved network resource reservation and allocation across the entire switch.

NIOC version 3 lets you configure bandwidth requirements for VMs. 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.

While the configuration of the vDS and NIOC is only possible via vCenter Server, in case of a problem on your vCenter Server appliance (vCSA), the system functions and the rules are deployed on the individual ESXi hosts.

If you don't want to use NIOC for certain physical adapters, you can configure it as needed. It might be the case where this particular adapter is low capacity or low speed. You can do this in the advanced system settings.

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

During the boot sequence, each server or each host must test the hardware, initialize RAID storage cards, video, chipsets, etc. So the traditional boot process of a server is pretty long compared to a PC, for example.

VMware came out with something called **Quick boot** that you can activate via vSphere Lifecycle manager (previously vSphere Update Manager). The Quick boot is some kind of a warm reboot that allows booting much quicker. The regular reboot involves a full power cycle that requires firmware and device initialization. Quick Boot optimizes the reboot path to avoid this.

Now, why might this be interesting since you don't have to reboot your hosts that frequently? Well, it depends. In large infrastructures you have clusters of hosts that need to be patched. vSphere Lifecycle manager (vLCM) does the patching the hosts one by one and each time it evacuates the VMs running on that host, to other hosts within the cluster. vSphere uses vMotion technology to evacuate the VMs.

VMware Quick Boot is very useful when working hand-in-hand with vSphere Lifecycle Manager and allows the patching process to be faster because each host does not have to go through all of the hardware initialization phases each boot.

The things slightly changed since vSphere 6.7 as now in vSphere 7.0 U1c (starting vSphere 7) there is no option within the UI on whether to activate quick boot or not. It is the system itself that determines whether quick boot is supported on the host or not.

Screenshot from the lab shows that the selected host is supported for Quick Boot.

The screenshot shows the vSphere Lifecycle Manager interface under the 'Updates' tab. The 'Image' section is active. A host named 'esxi02.lab.local' is highlighted in blue and has a yellow warning icon next to it. A tooltip for this host states: 'Host is out of compliance with the image' and 'Quick Boot is supported on the host. The host will be rebooted during remediation.' An arrow points to the 'Quick Boot is supported on the host.' part of the tooltip. Below the host list, there is a 'Software compliance' table:

Image	Host Version	Image Version
ESXi Version	7.0 Update 1 - 16850804	7.0 U1c - 17325551

Quick Boot support in vSphere 7

This is one thing less to worry about when managing vSphere clusters. In vSphere 6.7, this was a manual action that needed your attention. You had to go through all your hosts and check if the host was compatible or not, and then activate quick boot only. It was a manual step as the quick boot was not activated by default.

## Quick Boot Requirements and limitations

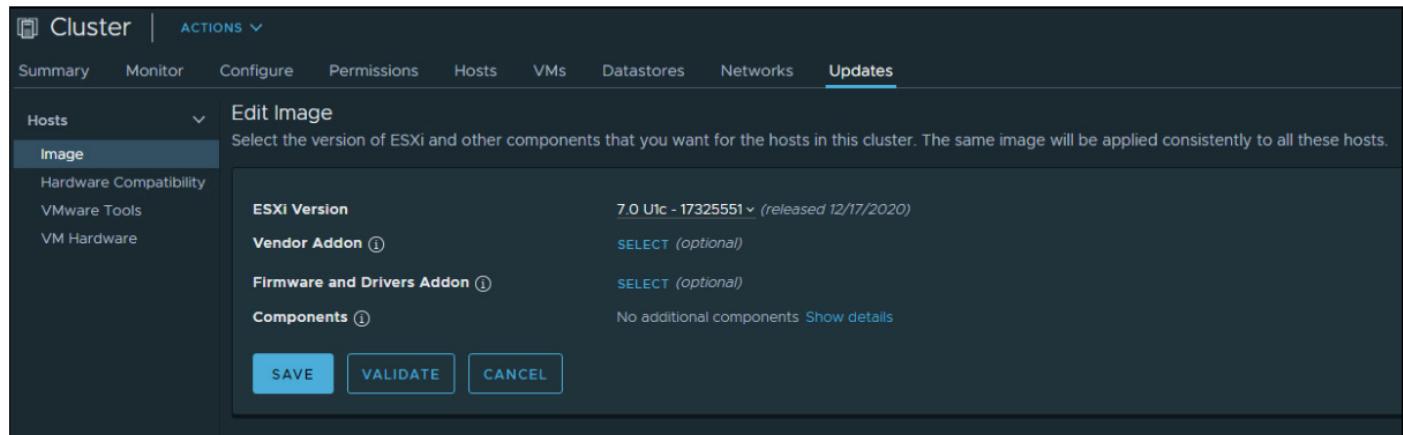
- Supported server hardware (currently some Dell, Fujitsu, Cisco, Lenovo and HPE systems)
- Native device drivers only – no vmklinux driver support
- No Secure boot – Secure boot not supported
- Only available for ESXi 6.7 and later so If you have hosts running older versions, you must upgrade them first.
- Supported on limited hardware only
- No Pass Through – if you have your host configure with a passthrough, you cannot use quick boot
- No Trusted Platform Module (TPM) – if you are using TPM, you cannot use quick boot. You must disable.

As you can see, quite a few limitations when you enable some security features, such as TPM and secure boot within vSphere. As I said earlier, the vSphere Update manager has been renamed to vSphere Lifecycle Manager.

There have been quite a few changes in vSphere lifecycle manager and we have detailed this in our article here – [VMware vSphere Lifecycle manager Improvements](#).

Let me focus on particular feature and this is the new **Image management feature**. This concept is quite different than what traditional baselines-based updates does.

Once we have our vLCM and cluster image management enabled for our cluster, there is what's known as a **desired state** that is set up. All the ESXi hosts adhere to this desired state and when for some reason, there is a host which has been installed with some new component or software that differs from the desired state, the host is remediated in order to stay compliant to the desired state and have the cluster uniformized.



## Edit the content of the image and validate

### What is an image?

Do you remember when in the past, you have been creating slipstreamed ISO images for Windows 2000 or 2003 servers? This slipstreaming process where you could add drivers, software and patches to the base image? Yes, this is basically the same here. Made by VMware.

The vLCM image has 4 composing elements:

- **ESXi Base Image** – This is an ESXi ISO file, it has a version that has an image of VMware ESXi Server. The base image from VMware.
- **Vendor Add-on** – This is a collection of software components for the ESXi hosts that OEM manufacturers create and distribute in order to maintain the infrastructure. This vendor add-on can contain drivers, patches, and software solutions that are used for the cluster management, monitoring, etc.
- **Firmware and Driver Add-on** – This is a special type of vendor add-on which helps for example maintain same firmware/drivers across the cluster. Usually those depends on the type of server that needs to be maintained.
- **Component** – This is the smallest discrete unit in the vSphere Lifecycle manager image. This is basically a third-party software vendor that create and publish those components. Those are usually drivers or adapters. They are completely independent. You can add such independent components to your image.

Setting up an image is easy when you have the hardware compatible. In the lab I'm working right now, this is not the case. But let's talk about transportation or export. Yes, you can export your image, and this can be in different formats.

vLCM image export possibilities:

- **JSON** – Yes, JSON is well known type of configuration file. This option exports an **image specification only**, not the actual source files. You won't be able to remediate clusters just with the JSON. However, you can import the image specification to other clusters.
- **ISO** – This one has the image as an ESXi image (an ISO), that can be imported into other clusters. You can also use the exported ISO file to boot/build new ESXi hosts using your image. It has everything, the drivers, firmware driver add-ons or components that you have added during the image creation.
- **ZIP** – Well known option. Offline bundle that has all of the image components and can be used directly within the vLCM. You can use the ZIP file to import the components into a different vCenter Server.

## Objective 1.9 Describe the basics of vSAN as primary storage

VMware vSAN is a software solution from VMware allowing you to configure local direct-attached storage (DAS) in each host to create a shared storage pool visible by all the hosts within the vSAN cluster. Each host participates in the pool with some storage, but there can also be hosts part of the cluster, that don't participate with any storage. A single datastore per vSAN cluster is created.

vSAN can be configured as a hybrid or All-Flash where the hybrid solution uses SSD for caching and All-Flash uses usually fast NVMe for caching and SATA/SAS for the capacity tier. You can easily expand the vSAN datastore by adding to the cluster hosts with capacity devices or by adding local drives to the existing hosts in the cluster.

vSAN, and also VMware clusters in general, works best when all ESXi hosts in the cluster are with similar or identical storage configurations. A consistent configuration enables vSAN to balance virtual machine storage components across all devices and hosts in the cluster. vSAN is particularly sensitive to homogenous storage controllers, their firmware, and drivers.

**Don't even try to using the storage controller not listed on vSAN HCL.** Not only you won't be supported, but most likely your solution will have poor performance and stability.

vSAN does not require a dedicated storage network, such as on an FC network or SAN. With vSAN, you do not have to pre-allocate and preconfigure storage volumes (LUNs). vSAN does not behave like traditional storage volumes based on LUNs or NFS shares. You do not have to apply standard storage protocols, such as FC, and you do not need to format the storage directly.

vSAN management is done through the vSphere web client so you don't need to install any other software to manage the vSAN storage. With vSAN you can assign storage policies automatically.

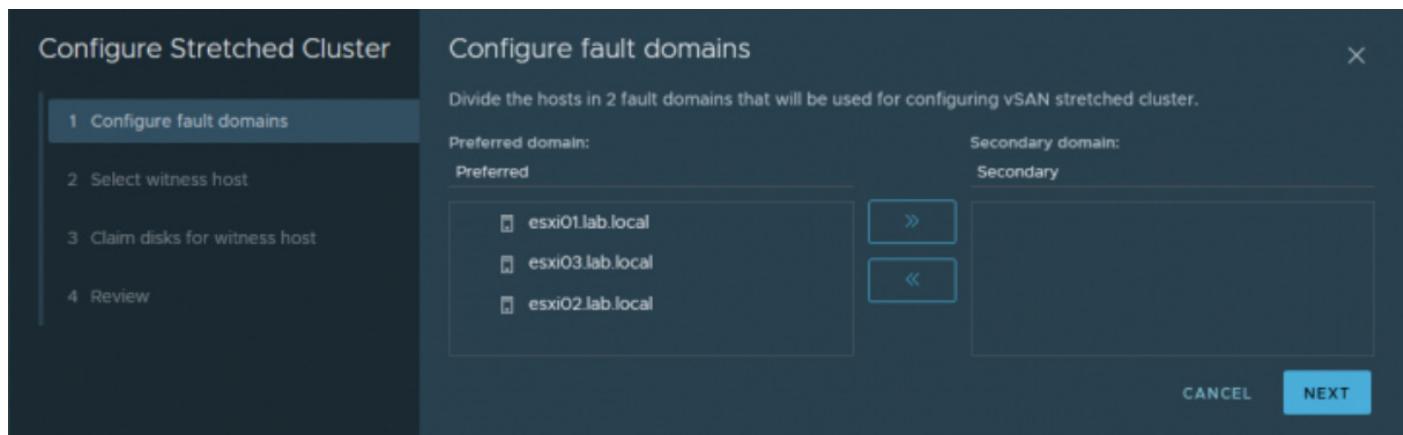
Imagine vSAN as a network distributed RAID storage where local disks are used as shared storage. vSAN uses copies of the VM data where one copy is local and another copy is on one of the other nodes in the cluster. You can configure the number of copies for data protection or performance.

Some other VMware vSAN characteristics:

**Fault domains** - Fault domains can be configured to protect against rack or chassis failures. vSAN intelligently places copies of the data to different hosts/racks to prevent all copies of VM disk data from sitting in the same rack.

**iSCSI target service** - The vSAN datastore can now be visible outside of the vSAN cluster. You can connect other ESXi hosts or VMs to the iSCSI target exported by vSAN and consume the vSAN storage.

**Stretched cluster** - vSAN supports stretching a cluster across physical geographic locations. You can connect to two remote datacenters, and have your Witness host in a third datacenter.



**Support for Windows Server failover clusters (WSFCs)** - SCSI-3 Persistent Reservations (SCSI3-PR) is supported on virtual disks, which are required for shared disks and WSFCs. Microsoft SQL 2012 or later is supported on vSAN (Some limitations here: There is a maximum of 6 application nodes in each vSAN cluster. Maximum of 64 shared disks per ESXi host vSAN).

**Health service** - This service includes health checks for monitoring and troubleshooting purposes.

**vSAN performance service** - This service shows stats for monitoring vSAN performance metrics. You can monitor the cluster level, ESXi host, disk group, disk, or VM level.

**Integration with vSphere storage features** - Snapshots, linked clones, and vSphere Replication (VR) are all supported on vSAN datastores. Also, all third-party backup solutions, such as NAKIVO Backup & Replication, are fully supported.

**Virtual machine storage policies** - Policies can be defined for VMs on vSAN. When you define no policies, you have a default vSAN policy that is applied.

**Deduplication and compression** - Block-level deduplication and compression are available space-saving mechanisms on vSAN, and they can be configured at the cluster level and applied to each disk group.

**Data at rest encryption** - Data at rest encryption is encryption of data that is not in transit and on which no processes are being done (for example, deduplication or compression). If drives are removed, the data on those drives is encrypted.

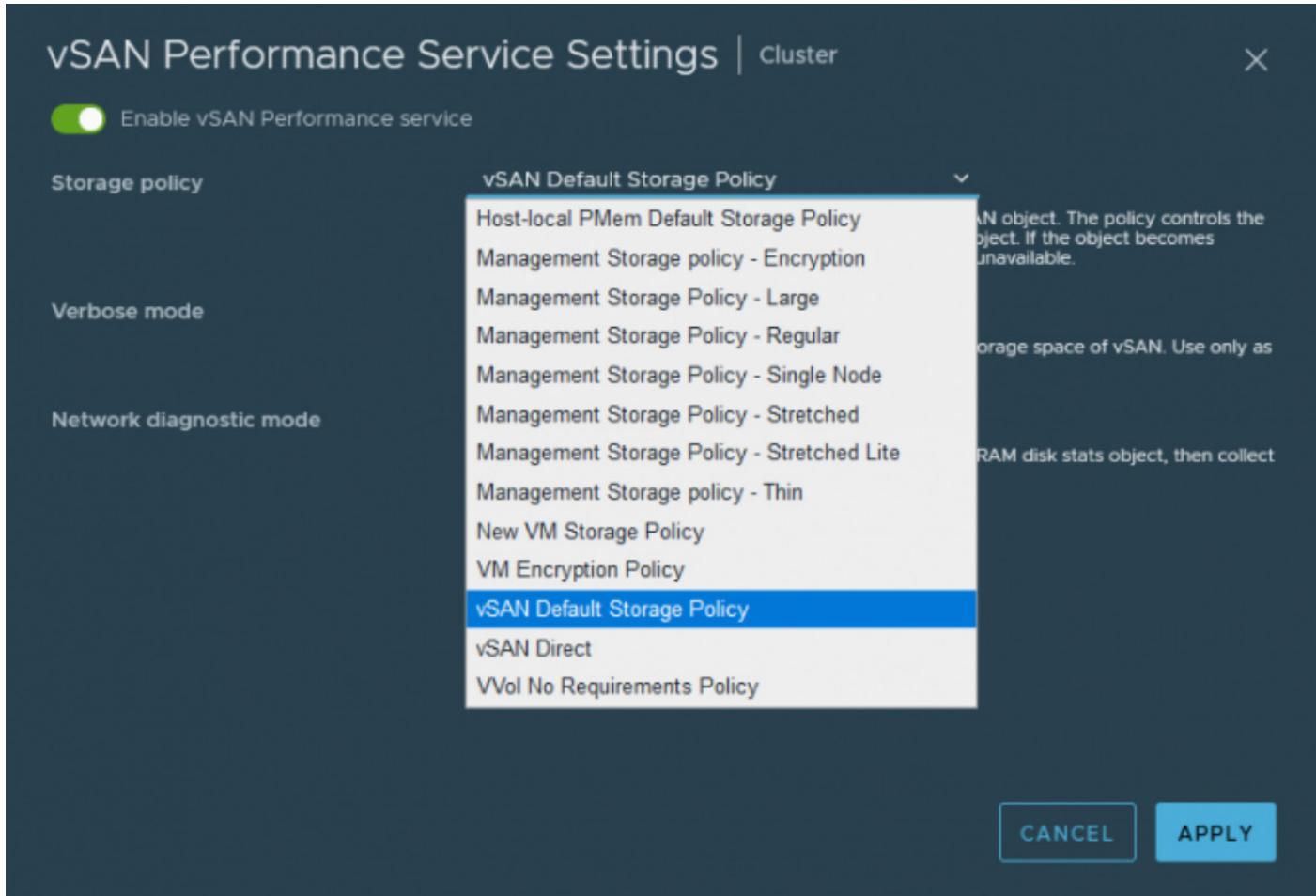
**vSAN Disk Group** - Each host participating in a vSAN cluster with local storage has the local disks configured in disk group(s). It's a kind of container, where the SSD for cache and capacity devices (SSD or HDDs) are in relation. The VMs are placed on the capacity tier but accelerated through the SSD cache tier. The SSD or PCIe flash device that is used for that I/O acceleration is the one that is in the same disk group as the capacity devices on which the VM is placed.

Disk Group	Disk in Use	Status	Health	Type	Fault Domain	Network Partition Group	Disk Format Version
Host01.lab.local	4 of 4	Connected	Healthy	All Flash	Group 1		14
Disk group (520d9bfa-d2c2-4f80-2c54-99e33...)	2	Mounted	Healthy	All Flash			14
vSAN Direct disks	2						
Host02.lab.local	4 of 4	Connected	Healthy	All Flash	Group 1		14
Disk group (520d9b07-0df7-4626-aed0-7d923...)	2	Mounted	Healthy	All Flash			14
vSAN Direct disks	2						
Host03.lab.local	4 of 4	Disconnected	Healthy	All Flash			

Name	Drive Type	Claimed As	Capacity	Health	State
Local VMware Disk (mpx:vmhba0:C0:T1L0)	Flash	vSAN Cache	50.00 GB	Healthy	Mounted
Local VMware Disk (mpx:vmhba0:C0:T2L0)	Flash	vSAN Capacity	160.00 GB	Healthy	Mounted

On each ESXi host, disks are organized into disk groups. A disk group is a main unit of storage on a host. Each disk group includes one SSD and one or multiple HDDs (magnetic disks). Up to **seven magnetic disks**.



## Objective 1.9.1 Identify basic VMware vSAN 7 requirements

When it comes to storage, VMware vSAN is one of the options you have when going through the process of choosing the right storage for your vSphere environment. In this post, we'll look at the basic VMware vSAN 7 requirements you might not be aware of.

While the VMware vSAN concept is pretty simple and cool, using local direct-attached storage (DAS) in each host with an SSD cache tier to create a shared storage pool where all the hosts are connected, many admins do not know what all the requirements and perhaps drawbacks are.

There are many environments where VMware vSAN is simply not the best option, and using other storage options gives a better deal.

### Hardware Requirements

While you can still create and use hybrid vSAN clusters, it's preferable to go All-Flash. At a minimum, a vSAN cluster must include three hosts with capacity devices. The best is to have identical hardware.

In hybrid clusters, magnetic disks are used for capacity, and flash devices have a read cache and a write buffer function. If you're running a VMware vSAN hybrid cluster, 70% of the flash space is used for the read cache, and 30% is used for the write buffer.

If you have an all-flash cluster, one SSD disk is used as a write cache, and additional flash devices are used for capacity. There is no read cache. All read requests come directly from the flash pool capacity.

Each host participating in a vSAN cluster with local storage has the local disks configured in disk group(s). It's a kind of container where the SSD for cache and capacity devices (SSD or HDDs) are in relation.

The VMs are placed on the capacity tier but accelerated through the SSD cache tier. The SSD or PCIe flash device that is used for that I/O acceleration is the one that is in the same disk group as the capacity devices on which the VM is placed.

On each ESXi host, disks are organized into disk groups. A disk group is a main unit of storage on a host. Each disk group includes one SSD and one or multiple HDDs (magnetic disks; up to seven magnetic disks).

**Disk Management**

- All 6 disks on version 13.0.

Disk Group	Disks in Use	State	Health	Type
esxi01.lab.local	4 of 4	Connected	Healthy	All flash
Disk group (52b2e15a-d2e2-c180-2c54-99e33...)	2	Mounted	Healthy	All flash
vSAN Direct disks	2			
esxi02.lab.local	4 of 4	Connected	Healthy	
esxi03.lab.local	4 of 4	Connected	Healthy	

Name	Drive Type	Claimed As
Local VMware, Disk (mpx.vmhba0:C0:T1L0)	Flash	vSAN Cache
Local VMware, Disk (mpx.vmhba0:C0:T2L0)	Flash	vSAN Capacity

## VMware vSAN Disk Groups

All capacity devices, drivers, and firmware versions in your vSAN configuration **must be certified and listed in the vSAN section of the VMware Compatibility Guide**.

This is good in general to prevent you from using storage controllers without enough queue depth that are not suitable for VMware vSAN environments.

For cache tier, you can use one SATA or SAS SSD or also PCIe Flash device. The cache flash devices must not be formatted with VMFS or another file system.

For the capacity tier, you'll need at least one SSD or spinning media disk. Note that usually, you'll try to get more disks to create a disk group for the capacity tier.

## **Networking requirements**

A 1Gbps network can be used, but 10Gbps or higher capacity networks are highly recommended. If you're planning to use All-Flash vSAN, you must use 10Gbps or higher capacity networks.

Each host in the vSAN cluster, regardless of whether it contributes capacity, must have a VMkernel network adapter for vSAN traffic.

**Network latency** is an important factor as the network can have a maximum of 1 ms RTT for standard (non-stretched) vSAN clusters between all hosts in the cluster. Maximum of 5 ms RTT between the two main sites for stretched clusters and a maximum of 200 ms RTT from one main site to the vSAN witness host.

## **Cluster requirements**

You'll need to have a cluster created with at least 3 ESXi hosts because this is the bare minimum. VMware recommends 4 hosts where the 4th host is useful in scenarios when you have a host failure and need some time to rebuild the vSAN components. If you have only 3 hosts and you have a host failure, there is no host where those components can basically rebuild.

However, you can have a scenario where you have two data hosts and one witness host. Unfortunately, if you do have a host failure, there is no other host where vSAN can rebuild its components.

## **Software requirements**

vCenter server is one of the requirements. Without a vCenter server, you can't configure and activate VMware vSAN.

## **Licensing Requirements**

In order to be able to use VMware vSAN in your environment, you'll need to buy an additional license from VMware. vSAN has 4 licensing options (Standard, Advanced, Enterprise, and Enterprise Plus). Each one of those has its feature sets that are tied to the version you want to use.

Advanced features include RAID 5/6 erasure coding and deduplication and compression. An enterprise license is required for encryption and stretched clusters.

As you can see, the more advanced features you want to use, the more you'll have to spend on licensing. For example, RAID-5/6 erasure coding that allows you to save space on your vSAN shared storage is only present in the "Advanced" version.

Another example is the Stretched cluster version of vSAN, where your vSAN datastore is spanned across two remote sites.

And if you want to have an iSCSI and file services to export the files to the outside world, you'll need an "Enterprise" license.

Editions	Standard	Advanced	Enterprise	Enterprise Plus
<b>vSAN 7 U2</b>				
Storage Policy Based Mgmt.	✓	✓	✓	✓
Virtual Distributed Switch	✓	✓	✓	✓
Rack Awareness	✓	✓	✓	✓
Software Checksum	✓	✓	✓	✓
All-Flash Hardware	✓	✓	✓	✓
iSCSI Target Service	✓	✓	✓	✓
QoS - IOPS Limit	✓	✓	✓	✓
Cloud Native Storage (CNS) Control Plane	✓	✓	✓	✓
vSphere Container Storage Interface (CSI) Driver	✓	✓	✓	✓
Shared Witness	✓	✓	✓	✓
Deduplication & Compression		✓	✓	✓
RAID-5/6 Erasure Coding		✓	✓	✓
vRealize Operations within vCenter		✓	✓	✓
Data-at-Rest and Data-In-Transit			✓	✓
Stretched Cluster with Local Failure			✓	✓
File Services			✓	✓
HCI Mesh <sup>1</sup>			✓	✓
Data Persistence Platform for Modern Stateful Services			✓	✓
<b>vRealize Operations 8 Advanced</b>				✓

License editions and product features

## Objective 1.10 Describe the vSphere Trust Authority architecture

VMware is introducing a new feature that is very important for an organization's security. VMware Trust Authority (vTA) will be able to establish a trust relationship with the ESXi host configuration to ensure there are no alterations from malware, etc. VTA creates a separate cluster with three hosts, in which the key manager communicates with trusted hosts among the management hosts.

The management hosts are pretty much "locked down", which means that a very small group of people can access those hosts, where the workload hosts (green) can be accessed by a larger group. The management cluster runs management software, such as vCenter Server or other monitoring solutions.

The architecture basically relies on the principle of least privilege, whereby the admin should really only have privileges to do what needs to be done. A separation of roles is essential when planning security.

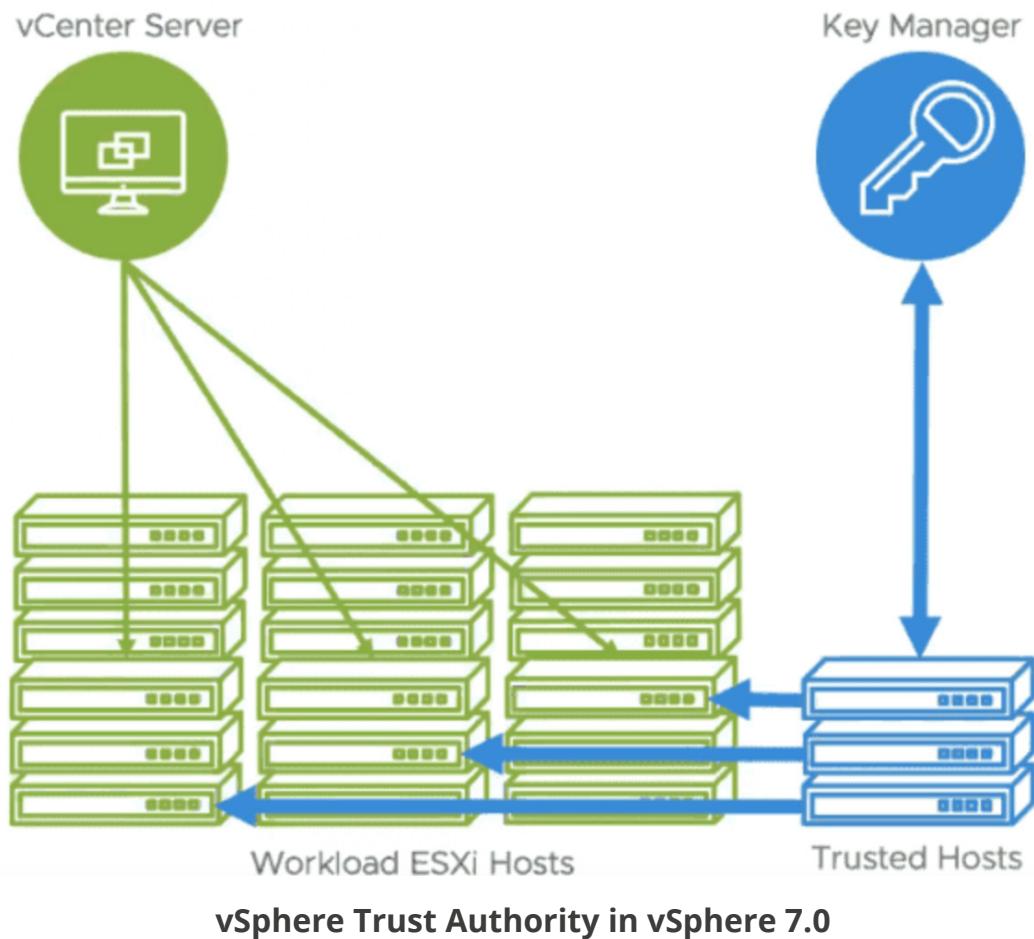
VMware is trying to work toward a better security model, and the introduction of vTA is the first step. vTA represents the foundation to which VMware will add more functions in future releases. In this release, VMware is building the base block of the architecture.

### The main vSphere Trust Authority (vTA) features

**VMware vTA creates a hardware root of trust using a separate ESXi host cluster:** This might be a problem for certain clients since, as you can see, the management cluster is used only for management, not for running workloads. Explain this to a client who is on a budget, and who does not have the money to spend on three hosts that do not directly run his production environment. The trusted hosts will be running the corporate workloads, which are encrypted and cannot be moved to hosts that are not trusted.

**Key manager and attestation requirement:** The VMware Key Management Server was introduced in vSphere 6.5 to allow encryption of VMs. You set up a trusted connection between the vCenter Server and a Key Management Server (KMS). The vCenter Server can then retrieve keys from the KMS as needed. The vSphere Trust Authority will enable setting that attestation can be a requirement for access to encryption keys. This will further reinforce security to prevent a potential intruder from getting the encryption keys to decrypt your encrypted VMs and gain access to the company's data. The Key Manager only talks to trusted hosts, not to the vCenter Server like in previous releases.

vSphere 6.7 and its attestations were "view only", so there were no repercussions for failing. The secure workloads could still run-on untrusted hosts. vTA and vSphere 7 allow the Key Manager to talk to trusted hosts instead of the vCenter Server (which is a VM).



**Can encrypt workload vCenter server instances:** In 6.5 and 6.7, you cannot encrypt the vCenter Server VM as there are many dependencies. vSphere 7.0 will be able to encrypt vCenter Server instances.

**Principle of Least Privilege:** You can restrict access such that a very small group of admins can access the trusted hosts. Again, separation of roles and privileges is important. The “green” hosts in the diagram above can be accessed and managed by a wider group of admins, whereas access to “blue” hosts remains restricted.

**Trusted Platform Module (TPM 2.0):** This is a \$20 trusted platform module chip that can be ordered from your hardware manufacturer and which is cryptographically signed and attached to the host when you first plug it in. (Note: Don’t buy these on eBay since they are usually used and are worthless.)

## Objective 1.11 Explain Software Guard Extensions (SGX)

Intel SGX is a processor-specific technology for application developers who seek to protect select code and data from disclosure or modification. So, it is not a protection for a VM but rather protection at the CPU level. With VMware Virtual Software Guard Extensions (vSGX), your applications are able to define private areas of memory (enclaves) that store protected data.

vSGX is implemented via software programs that can create private memory regions that are called enclaves. The enclaves can store cryptographic keys, HR records, or any other kind of secret. In order to use vSGX, the ESXi host has to have an SGX-capable CPU, and the BIOS of the system must support SGX. The enclave is encrypted or decrypted via CPU on-the-fly.

vSGX allows the VMs to see Intel SGX technology only if the hardware supports it. The option can be switched on or off in the web browser.

The official definition:

*Intel Software Guard eXtensions (SGX) is a modern Intel processor security feature that enables apps to run within protected software containers known as enclaves, providing hardware-based memory encryption that isolates the applications' code and data in memory.*

Virtual SGX (vSGX) is implemented as part of the vSphere. The vSGX creation/implementation happens between the VMkernel, the Virtual Machine Manager (VMM), and the management layer, where you can find the principal services

(VPX/hostd/VMX). It is the VMkernel that is basically in charge of initializing SGX support on the ESXi host, after validation that the hardware and BIOS support it.

### What are the requirements for vSGX?

Well, as said, the underlying hardware, the motherboard with a BIOS, and the CPU must support it. If not, you simply won't be able to proceed with the activation, which happens at the VM level. Intel Coffee Lake CPUs and higher are supported.

Open the virtual hardware edit options via the vSphere web client to view the security devices.

- EFI firmware
- Virtual hardware version 17 and above
- vCenter Server 7.0
- ESXi 7.0

### Guest OS support

Not all OSs are supported, so you must pick a supported guest OS if you want to use this feature. Supported guest OSs are:

- Linux
- Windows Server 2016 (x64) and higher
- Windows 10 (x64) and later

## What are the restrictions for vSGX?

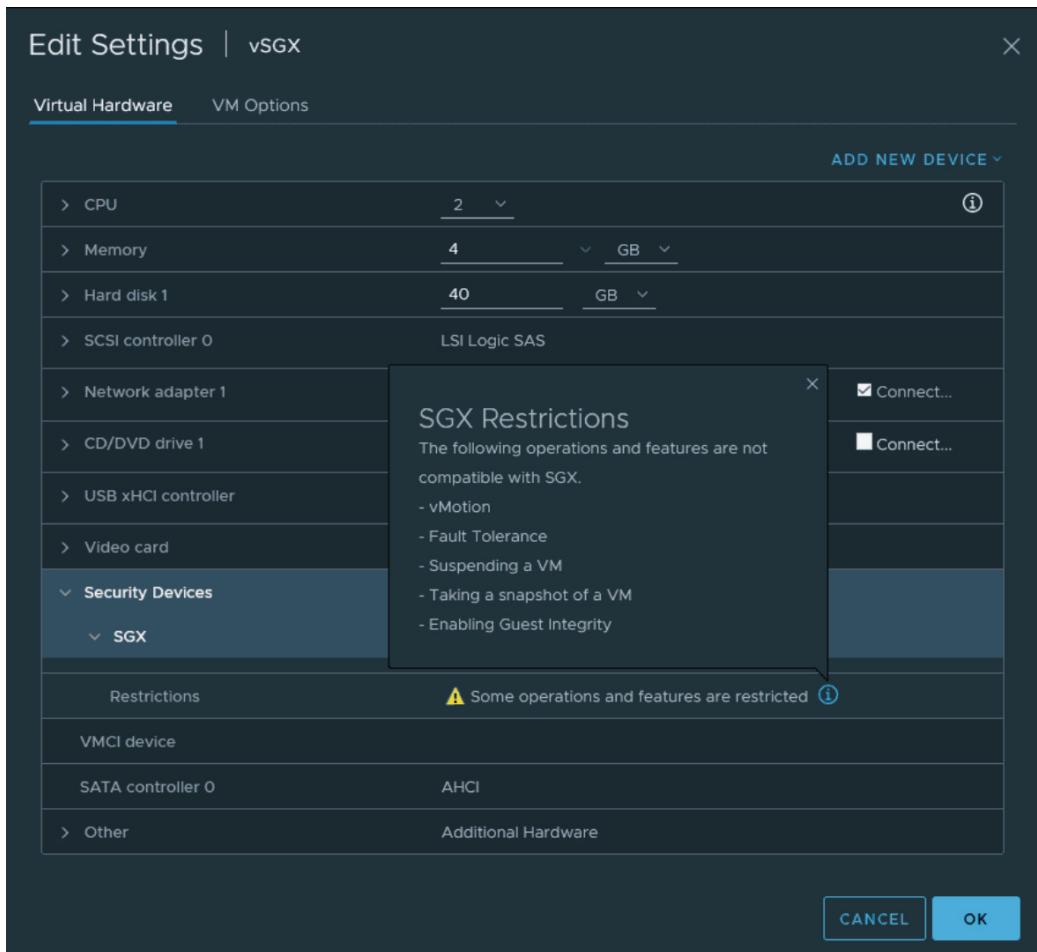
As you can see in the image, there are some restrictions to our vSphere infrastructure. We won't be able to use vMotion or DRS, or activate fault tolerance (FT) on a VM that has been enabled for vSGX.

Also, some operations simply won't work, such as suspending a VM, taking snapshots of a VM, or enabling guest integrity.

Note that virtual machine snapshots are supported if you do not snapshot the virtual machine's memory (there is a checkbox to deactivate).

You'll have to back up the data inside those VMs via some software that uses an agent, so the agent installed in the VM does an image level backup that is sent to a remote backup server.

Lastly, you'll need one of the latest versions of vSphere 7.



## VMware vSGX restrictions

## BIOS settings—Three options to choose from

**Enabled** — You simply enable, so Intel Software Guard Extensions (Intel SGX) is enabled and available for use in applications.

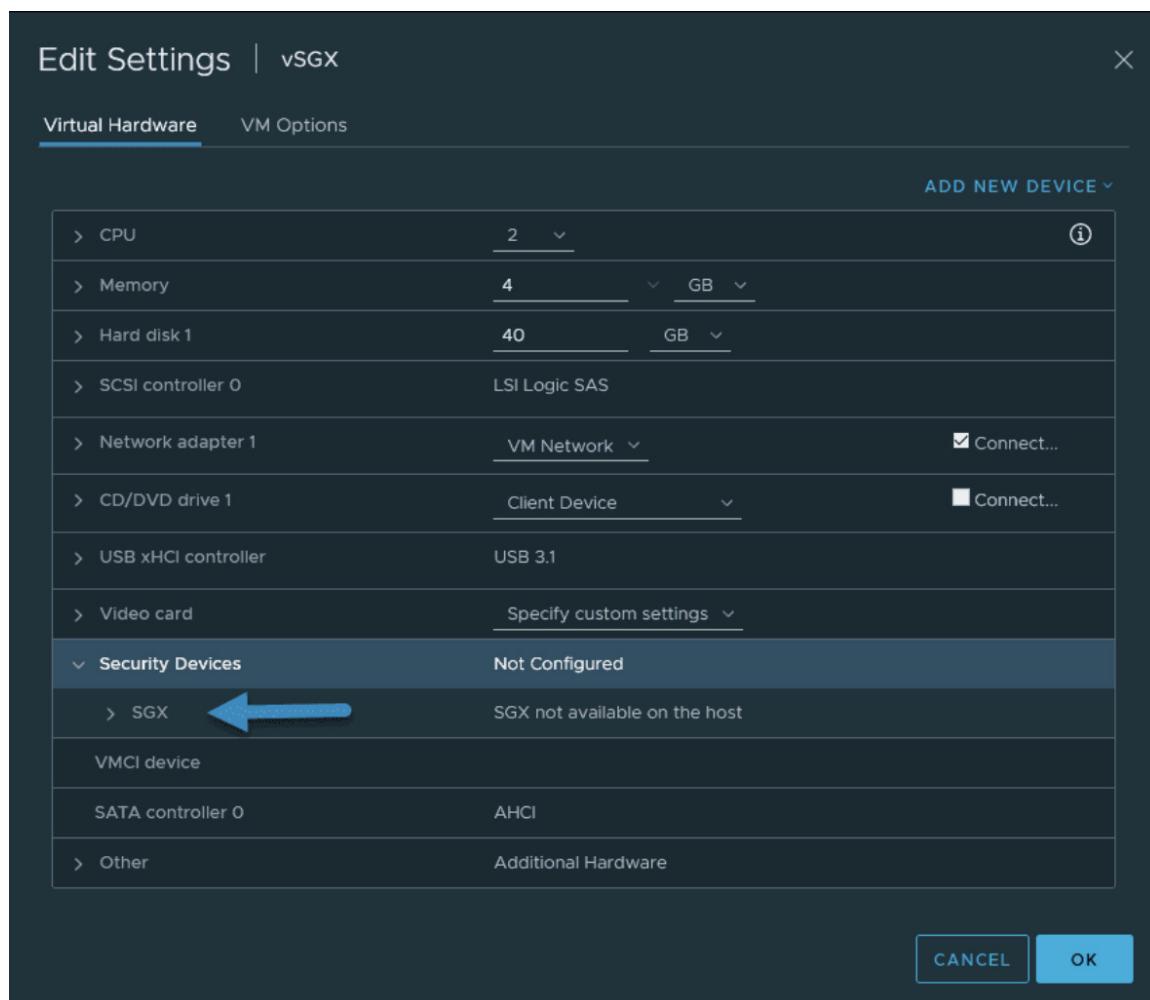
**Software Controlled** — In this case, the Intel SGX can be enabled by software applications, but it is not available until it is triggered. Note that in this case, when the app enables the feature, the guest OS might need to reboot.

**Disabled** — In this case, the feature is disabled. Intel SGX is disabled, and it cannot be enabled through software applications or via the Virtual Hardware assistant. This setting can only be changed again in the BIOS setup screen.

## Where do I enable vSGX in vSphere Client?

Open the vSphere client. Then navigate to and select one of your VMs. Under **Security devices**, select the **Enable** checkbox for SGX.

Unfortunately, my virtual lab does not have the hardware support.



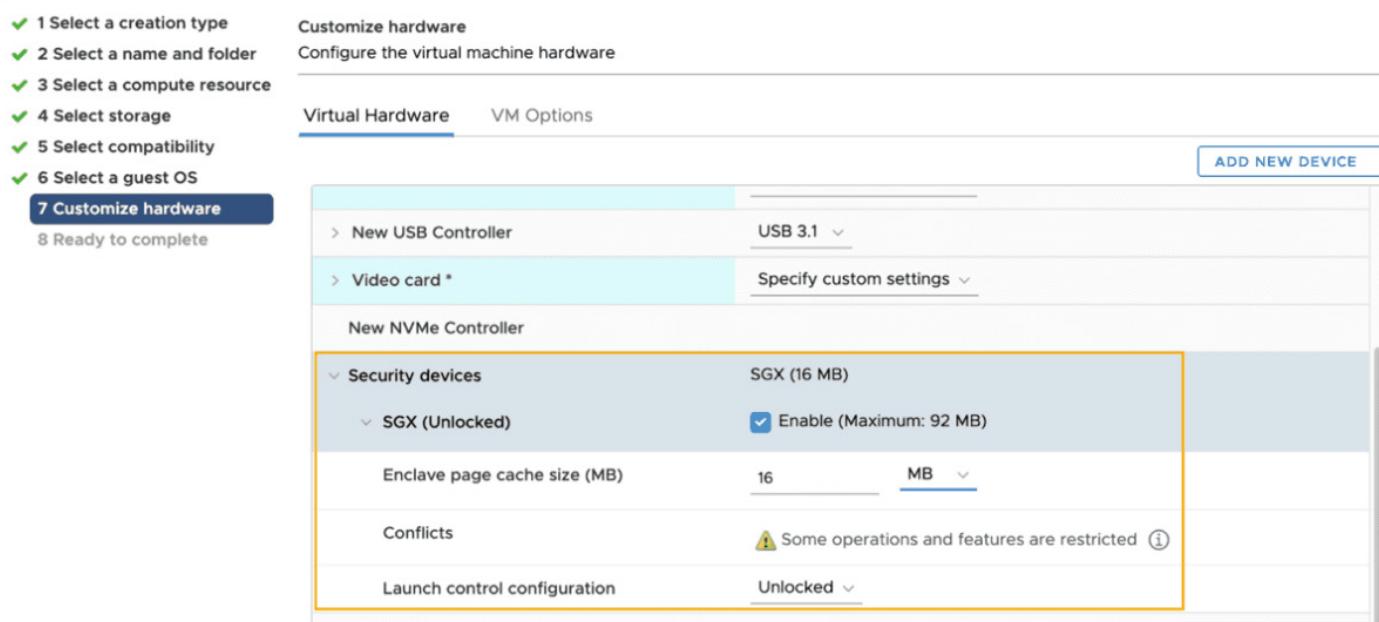
**VMware vSGX not available**

Under **VM Options > Boot Options > Firmware**, verify that **EFI** is selected. Also, you can enter the enclave page cache (EPC) size and select Flexible Launch Control (FLC) mode accordingly.

**Note:** If the VM is not set up with EFI firmware, you may need to reinstall the OS.

This screenshot is from VMware. You can see that you can allocate a certain amount of memory to the feature and also an enclave page cache size.

### New Virtual Machine



VMware vSGX activation

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

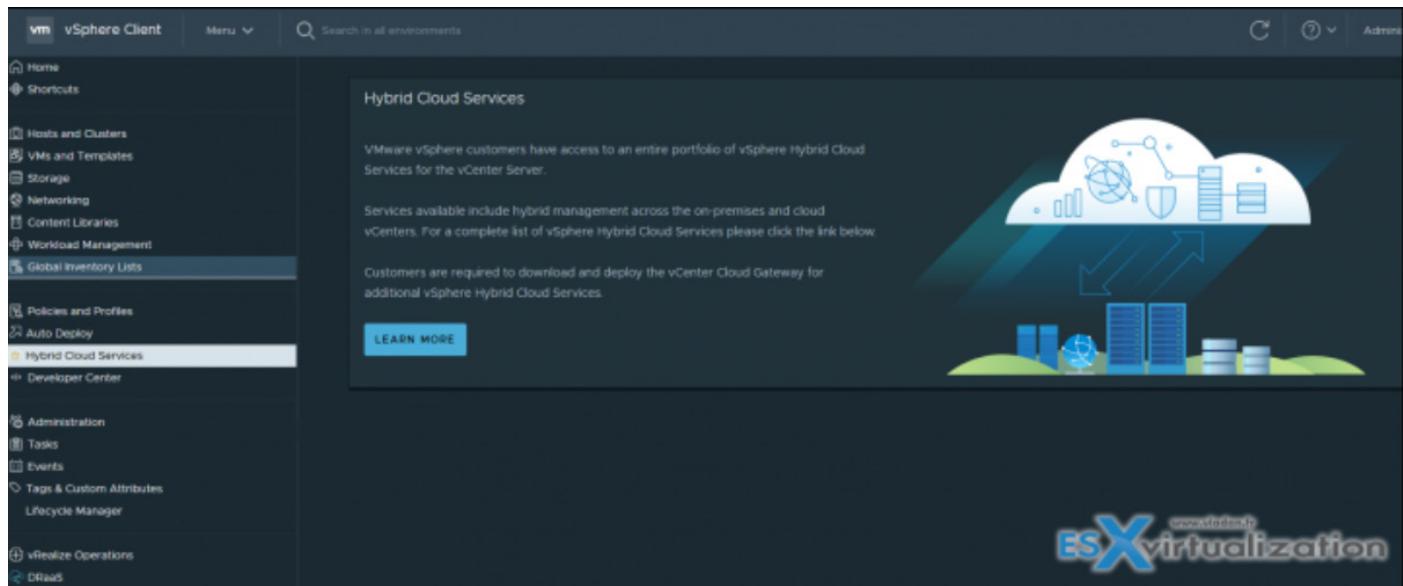
Describing the role of vSphere in the software-defined data center (SDDC) is a large topic.

VMware Software-Defined Datacenter (SDDC) is a data center that uses local infrastructure services that are abstracted from the underlying physical infrastructure. It allows any apps to run on a virtual platform that uses underlying physical hosts, physical servers. SDDC is a perfect architecture for private, public, and hybrid clouds.

VMware SDDC includes vSphere and compute virtualization, NSX with network virtualization, as well as software-defined storage (vSAN or vVOLs). SDDC gives us abstraction, pooling, and automation of the compute, network, and storage services. There is also vRealize Automation, vRealize Operations, which gives us other services such as policy-based automated management of the whole datacenter, apps, or VMs.

**VMware vCloud Suite** is an enterprise application, a software suite with vSphere for data center virtualization, and also VMware vRealize Suite for cloud management.

**VCF and Hybrid cloud environment** is a cloud that includes private cloud, public cloud, and also on-premises infrastructure. It's a combination of your home (in-house) data center with cloud environments.



VMware Cloud Foundation (VCF) is a set of software tools with an integrated installer. It has not only vSphere, ESXi, but also VMware vSAN and NSX or vRealize suite.

It brings a simple path to the hybrid cloud by using common infrastructure and a consistent operational model for on-premises and off-premises data centers.

**VMC on Amazon Web Services (AWS)** is an integrated cloud offering that has been developed in common with VMware and Amazon. It has a highly scalable and secure service that offers to businesses to expand their own on-premises infrastructure to AWS cloud. You can not only expand, but also migrate back and forth your VMs and make DR plans.

**VMware vCloud Director** - vCD is a cloud service delivery software used usually by cloud providers. It allows the automatic provision of secure, efficient, and elastic cloud resources to many customers via self-service portals.

## Objective 2.2 Identify use cases for VMware Cloud Foundation (VCF)

VMware Cloud Foundation (VCF) is a **hybrid cloud platform**. There are two pre-packaged workload domain types, Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). VMware VCF provides a simple and easy-to-use architecture that allows consistent and secure infrastructure operations between private and public clouds.

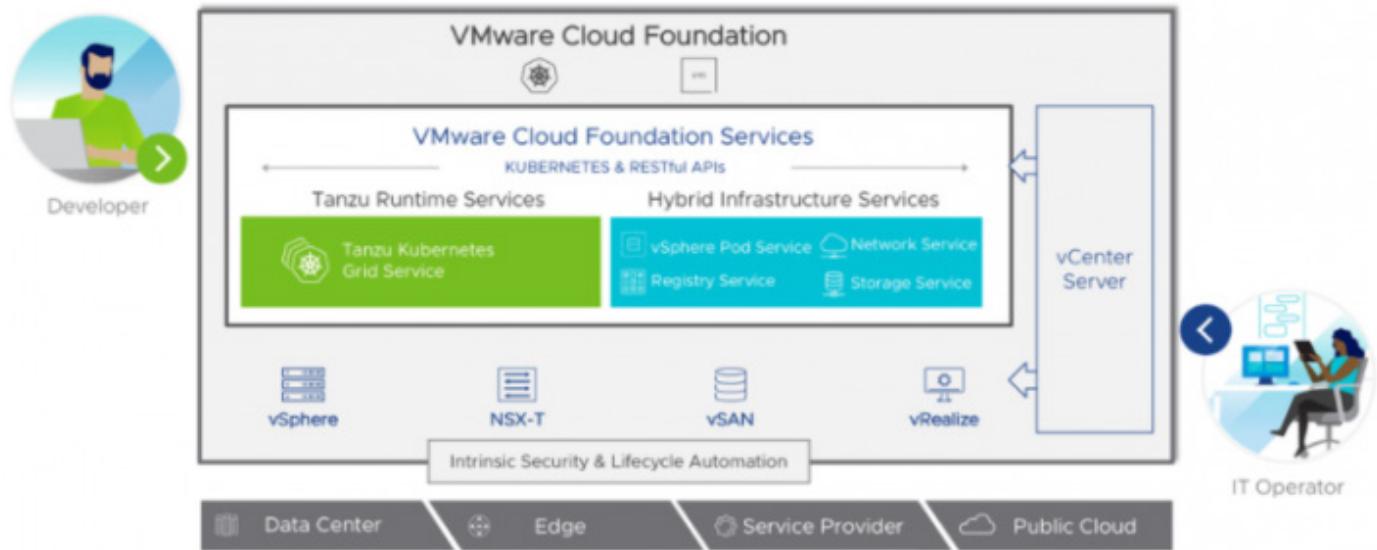
VCF has an automated way to install vSphere and all the necessary components (vCenter, vSAN, NSX-T and vRealize suite). The latest release also supports vSphere with Tanzu in order to support VMs and containers on the same platform.

You don't need to install each piece manually, but instead, it gives you the possibility to install the solution automatically. There are two appliances: VMware Cloud Builder and SDDC Manager. So the vCloud builder gives you this:

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

The SDDC Manager automates the lifecycle management. It means the configuration and provisioning, and updates and patching. The Cloud Builder appliance installs the following components:

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



Use cases are for vCloud Foundation:

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

You can test it via free Hands-On Labs [here](#).

## Objective 2.3 Identify migration options

VMware vSphere can do different types of migrations of VMs. In this section, we'll be identifying migration options under vSphere.

You can migrate virtual machines (VMs) from one compute resource or storage location to another while the virtual machine is stopped (cold) or running (hot). That's the definition. Hot migration is known as vMotion.

As an example, if you want to balance the workload, you can migrate some virtual machines from busy ESXi hosts or datastores (or both) to other hosts and datastores. Or you want to perform maintenance (such as an upgrade), you can migrate all VMs from an ESXi host or datastore, perform the maintenance, and then migrate VMs back to the original location.

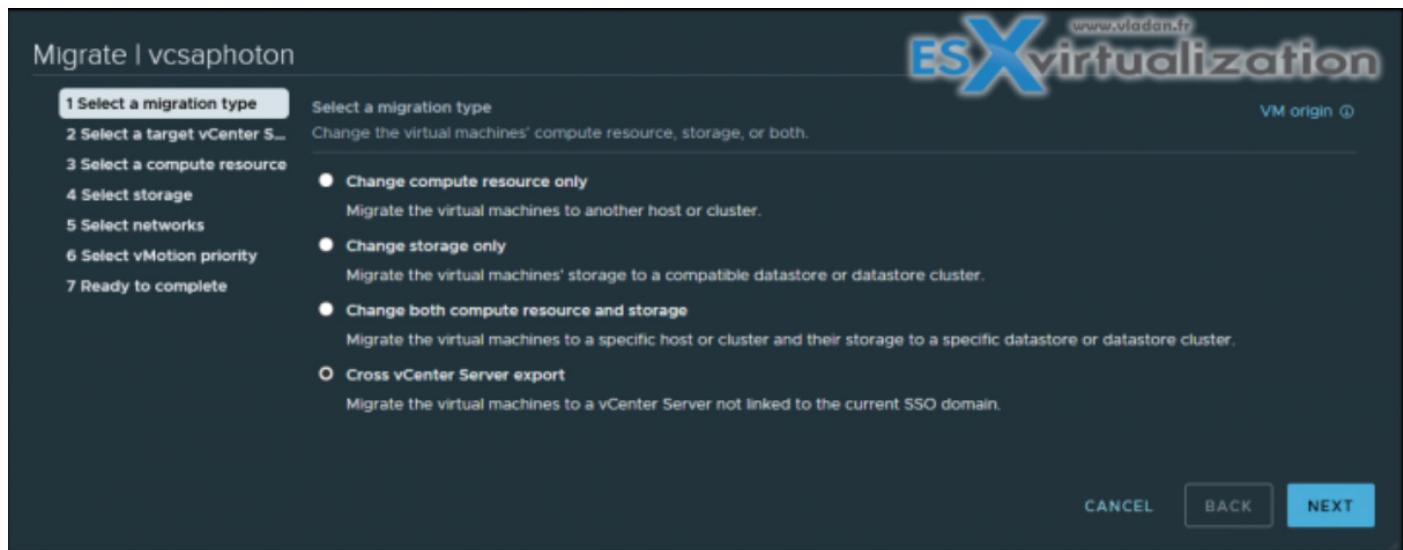
**Cold Migration** - when moving powered-off or suspended VMs to another host, another datastore.

**Hot migration** - when moving powered-on VM from one host to another or from one datastore to another.

**Cross-Host migrations** - In vSphere Client, there are wizards that allow you to initiate cross-host migrations and you can choose a destination host. You can also choose a DRS cluster, resource pool, or vApp as the destination.

**Cross-Datastore migrations** - when moving VM (hot or cold) to a new datastore.

**Cross vCenter Migration** - when moving VM (hot or cold) from one vCenter server to another vCenter server. There are some requirements, as for example, you'll have to use vCenter Server and ESXi 6.0 and later. And also, you'll need an **Enterprise Plus license**.



Also, vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification. And also, both vCenter Server instances must be in Enhanced Linked Mode, and they must be in the same vCenter Single Sign-On domain.

### Limitations of VM migrations

vCenter Server uses a costing method by which each migration and provisioning operation is assigned a cost per resource. Operations whose costs cause resources to exceed their limits are queued until other operations finish.

**Note:** The below limits, I don't really think that those topics will show up on the exam, but I've found it documented pretty well through VMware documentation, and quite interesting. Limits depend on the resource type, ESXi version, migration type, and other factors, such as network type. ESXi Versions 5.0 to 7.0 have consistent limits:

**Network limits** - Network limits are considered for vMotion migrations. Each vMotion migration has a network resource cost of 1. The network limit depends on the network bandwidth for the particular VMkernel adapter enabled for vMotion migration. For 1 Gig the limit is 4, and for 10 GigE it is 8.

**Datastore limits** - Datastore limits counts for vMotion and Storage vMotion migrations. Each vMotion migration has a resource cost of 1 against the shared datastore. Each Storage

vMotion migration has a resource cost of 16 against both the source and destination datastores. The datastore limit per datastore is 128.

**Host limits** - Host limits apply to vMotion, Storage vMotion, and cold migrations. They also apply to virtual machine provisioning operations, including new deployments, and cloning. Provisioning and vMotion operations have a host cost of 1. Storage vMotion operations have a host cost of 4. The host limit per host is 8.

As an example of limitations, let's say that you do nine vMotion migrations at the same time. The ninth migration is queued due to the network limit, even if different hosts are involved. If you do nine simultaneous hot cross-host and cross-datastore migrations with the same datastore, the ninth migration is queued due to the datastore limit, even if the migrations are split as to whether the datastore is the source or the target.

## Storage vMotion

Storage vMotion migration is a hot cross-datastore migration. Storage vMotion enables you to migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running.

## Limitations

Virtual disks in nonpersistent mode are not supported for Storage vMotion. For virtual compatibility mode RDMs, you can migrate just the mapping file or include the migration of the data to a virtual disk file. For physical compatibility mode RDMs, you can only migrate the mapping file.

- Storage vMotion migration is not supported during VMware Tools installation.
- You cannot use Storage vMotion to migrate virtual disks larger than 2 TB from a VMFS Version 5 datastore to a VMFS Version 3 datastore.
- The source host that is running must have a license that includes Storage vMotion.
- ESXi 4.0 and later hosts do not require vMotion configuration to perform Storage vMotion migrations.
- The host on which the virtual machine is running must have access to both the source and target datastores.

## VM Cloning

You'll need vCenter server to clone VMs. vCenter Server creates a virtual machine that is a copy of the original virtual machine. The virtual disk files, configuration file, and other files are copied from the original virtual machine to the new virtual machine.

You can choose to make some configuration changes and customizations during the cloning process. The contents of some of the files, such as the configuration file, are modified.

**Cold and Hot Clones** - Cold clone is for VMs powered-off. Hot clones are for when VMs are running. vCenter server must avoid disrupting the execution of the VM and takes snapshot of the VM before starting to copy. At the end when the clone is done, the snapshot is removed.

**Linked Clones** - It shares its virtual disk files with the original virtual machine (parent). The shared files are static. Much like a virtual machine that has a snapshot, a linked clone writes its virtual disk changes to separate data files.

**Note:** Linked clones can only be used via PowerCLI with -LinkedClone parameter.

### Templates and usage

You can convert a VM to a template and vice versa. Templates are used for rapid deployment of new similar VMs from a single template. In this case, you are actually cloning the templates so the template can be reused again.

**Instant Clones** - Instant clone technology is new and came in with vSphere 6.7. You can use instant clones to hot clone a running VMs. It's like a combination of vMotion and linked clone technology. The result of an instant clone operation is a new VM that is basically identical to the source VM. The processor state, virtual device state, memory state, and disk state of the destination VM match those of the source VM. Instant clones are used with VMware Horizon and completely eliminate the use of VMware Horizon Composer server.

During an instant clone (vmFork) operation the system quiesces and stuns the source VM, creates and transfers a checkpoint, customizes the destination MAC address and UUID, and forks the memory and disk.

The destination VM then shares the parent virtual machine's disk and memory for reads. For writes, the destination VM uses copy on write (COW) to direct disk and memory changes to delta files and private memory space.

Instant cloned VMs are fully independent vCenter Server inventory objects. You can manage instant clone destination virtual machines as you would regular virtual machines, without any restrictions. The creation of instant cloned VMs can't be done via UI in vSphere client, but it's rather API driven.

## Objective 2.4 Identify DR use cases

VMware vSphere is a software data center suite that has one main function: disaster recovery. Whenever you have a small power outage in your local data center or a hurricane flooding your entire server room, you can use vSphere 7 to protect your IT environment. Let me show you how different technologies and products within the vSphere 7 suite can help.

## High Availability

VMware High Availability (HA) is the first technology that VMware offered. It allows automatic restart of virtual machines (VMs) on other hosts in the event of host failure. HA basically pools hosts and VMs into a single resource group where all hosts are monitored.

In the event of host failure, which can be CPU, motherboard, storage controller, or network internet card (NIC), different actions can be triggered that allow VMs running on the failed host to be restarted elsewhere.

Hosts can be declared failed when either they are not reachable over the management network or not reachable via a second communication channel, which is a storage network. Yes, we need a shared storage where all the hosts are connected at the same time and all the VMs run and are stored on shared storage datastores.

At first, when you enable vSphere HA, one of the hosts becomes the master and all the other hosts become slaves. The master host holds a list of all the VMs that are protected and communicate securely with the vCenter Server.

HA needs hosts to have static IP or persistent DHCP reservations. The hosts communicate over the management network.

HA is responsible for restarting VMs in different priorities and orders if there is a host failure.

There is also a VM monitoring feature that tells vSphere HA to restart a VM if it doesn't detect a heartbeat received from VM Tools, which is installed within the VM.

One last more granular option, called Application Monitoring, is able to do the same but with heartbeats from an application.

On the other hand, there is something called VM Component Monitoring, or VMCP. This is a function that allows vSphere to detect datastore accessibility and restart the VM if a datastore is unavailable.

## vSphere 7 HA and various configuration options

There are several options in HA that can be configured. Once you enable HA, the defaults are good for most environments.

One such option is **Proactive HA**, which is able to receive messages from a provider plugin (Dell, HP, etc.). vSphere 7 HA is able to migrate VMs to a different host because of a failure detected by the provider's plugin. The host might still be able to run VMs, but the hardware being monitored by the manufacturer's component gives you more fine-grained ability to mitigate risks.

There are two options:

- **Manual** — DRS will suggest recommendations for VMs and hosts.
- **Automated** — VMs will be migrated to healthy hosts, and degraded hosts will be entered into quarantine or maintenance mode depending on the configured proactive HA automation level.

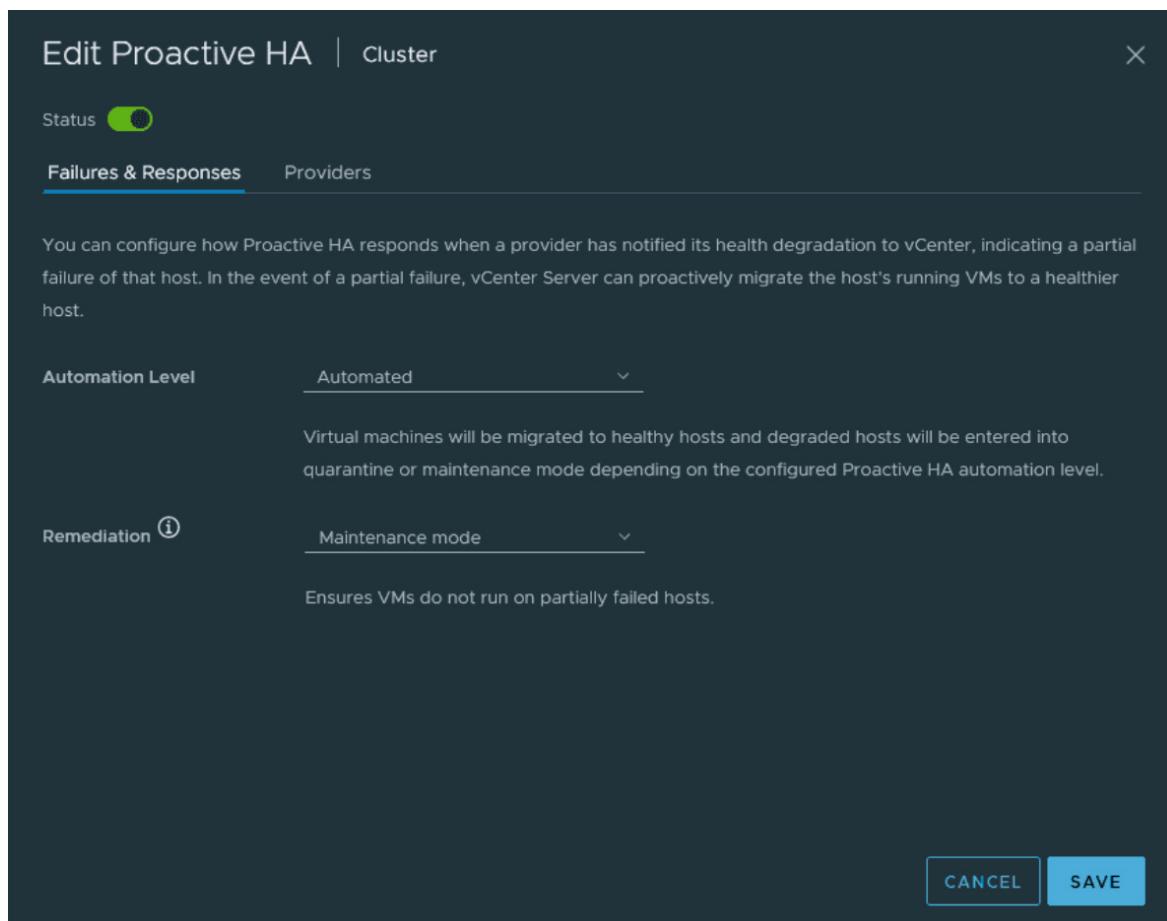
After VMs are migrated to other hosts within the cluster, the failed host can be placed in maintenance mode.

However, there are other options too:

**Maintenance mode** — Ensures VMs do not run on partially failed hosts.

**Quarantined mode** — Balances performance and availability by avoiding the use of partially degraded hosts as long as VM performance is unaffected.

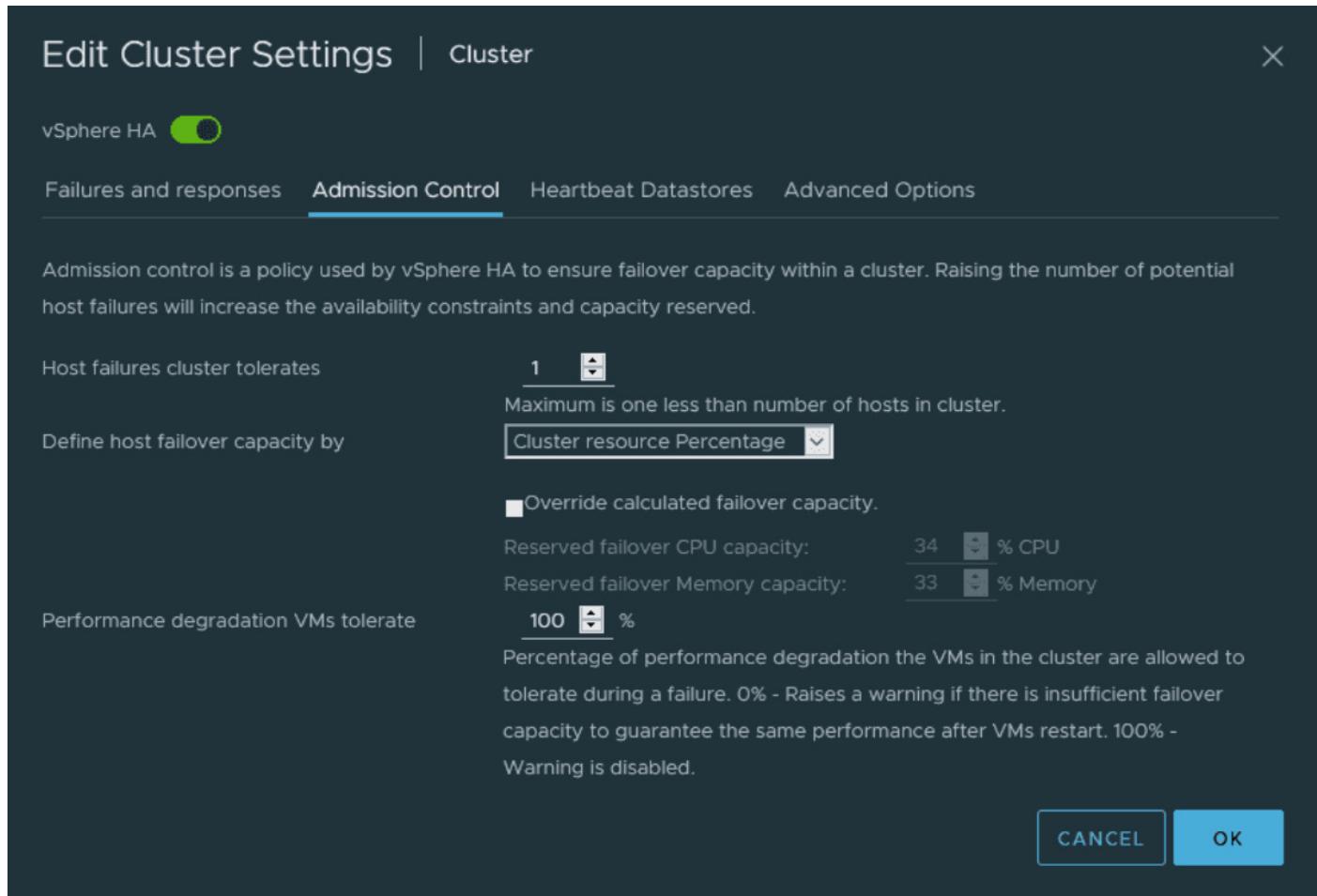
Selecting either quarantine or maintenance mode will apply the same response for both moderate and severe failures. Selecting mixed mode will enforce quarantine mode for moderate failures and maintenance mode for severe failures.



## vSphere Proactive HA configuration options

We're not done with vSphere HA. There is more, and we'll look at it. Next, we'll talk about failure conditions and responses, which is a list of possible host failure scenarios and how you want vSphere to respond to them.

**vSphere 7 HA Admission Control** — Allows you to make sure that you have enough resources to restart your VMs in the event of a host failure. You can configure admission control and resource availability in several ways.



### vSphere 7 HA admission control option

You can use the default (preferred), which is **Cluster resource percentage**. This option determines the percentage of resources available on each host.

You can also use dedicated failover hosts or slot policy in some cases, but those waste more resources. Imagine running a dedicated spared host that sits in the data center and waits for failure. This is quite expensive, isn't it?

The option with slot policy takes the largest VM's CPU and the largest VM's memory and creates a slot. Once done, the system is capable of calculating how many slots the cluster can handle. The best (and the default) is cluster resources percentage. It simply takes a look at

total resources needed and total available within the cluster. It keeps enough resources free to allow you to adjust the number of specified hosts.

If your cluster can't satisfy all resources and you have more VMs to be restarted, they are simply not restarted. Hence, the name—admission control.

**Heartbeat Datastores** — As I mentioned earlier, if the host's management network fails, HA will use the datastore network to try to reach the host. vSphere HA can see if the host or a VM is still running by looking for lock files on a particular datastore. The heartbeat datastore function is used on two or more datastores.

**Advanced Options** — There are some advanced options that help to determine if the host is isolated on the network. You can set a second gateway, because it is the gateway that is pinged at regular intervals to determine the host's state. In order to use this, you need to set two options, **das.usedefaultisolationaddress** and **das.isolationaddress**, which are found in the advanced configuration options.

The first option enables you to configure not using the default gateway, and the second enables you to set an additional gateway address.

## Fault Tolerance

With Fault Tolerance (FT), your VMs run all the time even if the underlying host fails. FT creates a secondary VM that runs as a shadow copy of the primary VM. Both VMs run in sync on two different hosts.

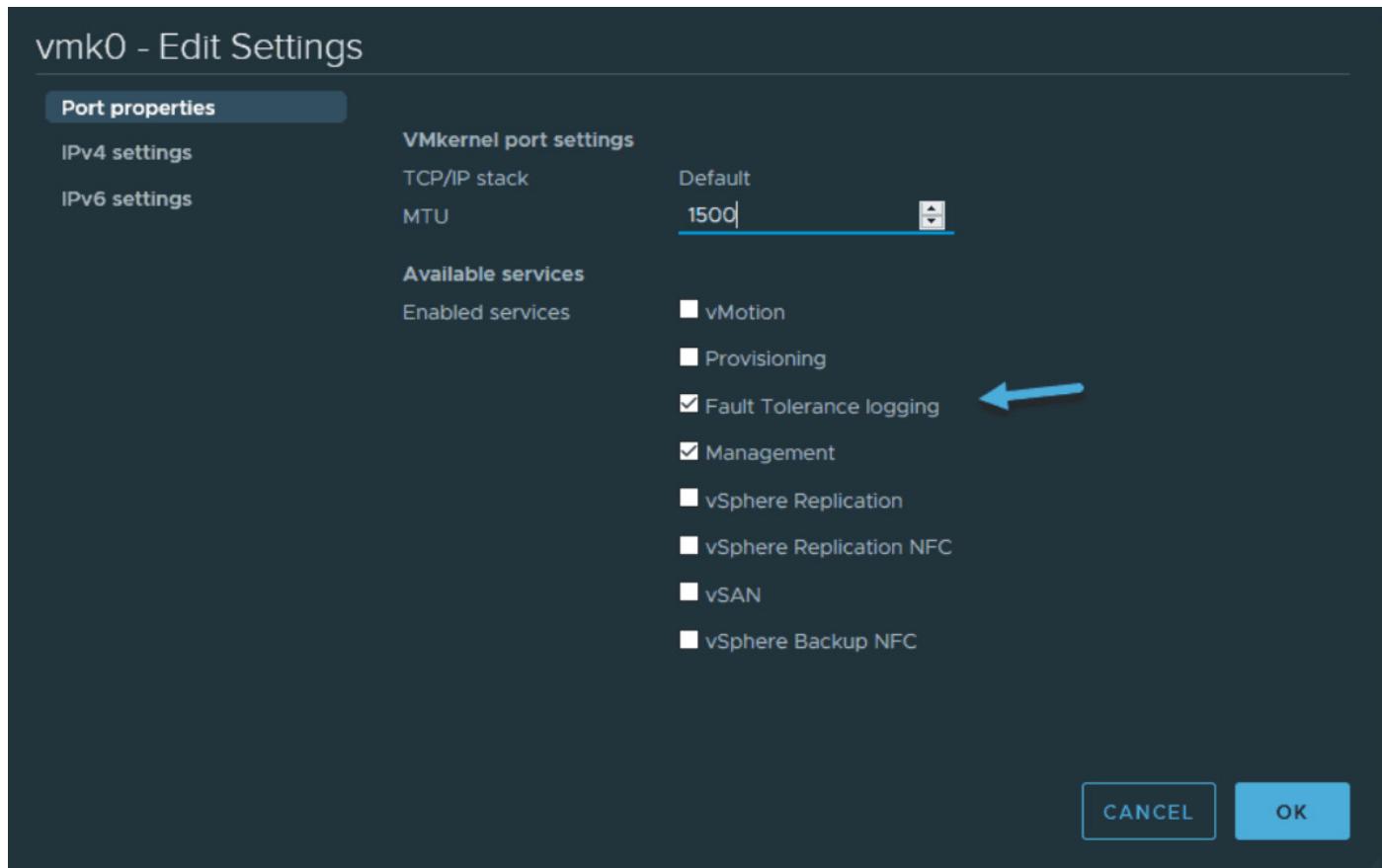
If the primary VM fails, the secondary VM takes over, and vSphere creates a new shadow VM. If the secondary VM fails, vSphere also creates a new shadow VM.

**Requirements and limits** — vSphere FT supports up to four FT VMs with no more than eight vCPUs between them.

VMs can have a maximum of 8 vCPUs and 128 GB of RAM, and you have to have a VMkernel adapter configured with the Fault Tolerance logging checkbox enabled.

If you are using DRS, you must enable Enhanced vMotion Compatibility (EVC) mode.

FT uses a technology called fast checkpointing, which takes checkpoints of the source VM every 10 milliseconds. Those checkpoints are sent to the shadow VM via the VMkernel port with the Fault Tolerance logging checkbox enabled.



### vSphere and FT logging enabled on the VMkernel adapter

## vSphere Replication

This is an add-on product that is installed as a virtual appliance (VM). It allows you to configure replication of VMs to remote data centers. In conjunction with the Site Recovery Manager (SRM) product, you can automate disaster recovery (DR) plans and have a failure under control.

vSphere Replication is configured on a per-VM basis. The replication allows you to copy VMs from a primary to a secondary site, where those VMs are in stand-by mode. The system first does a full copy and then only an incremental one.

You can have one or more primary sites that are replicated to the secondary (DR) site. It uses a server-client model with appliances on both sides.

You can configure the recovery point objective (RPO), which is how often you want it to replicate the VM disks. The settings can be as low as 5 minutes or as long as every 24 hours.

You can also set up replication with your preferred third-party backup software programs, such as NAKIVO Backup & Replication. This disaster recovery product allows setting replicas and other options as well.

## Objective 2.5 Describe vSphere integration with VMware Skyline

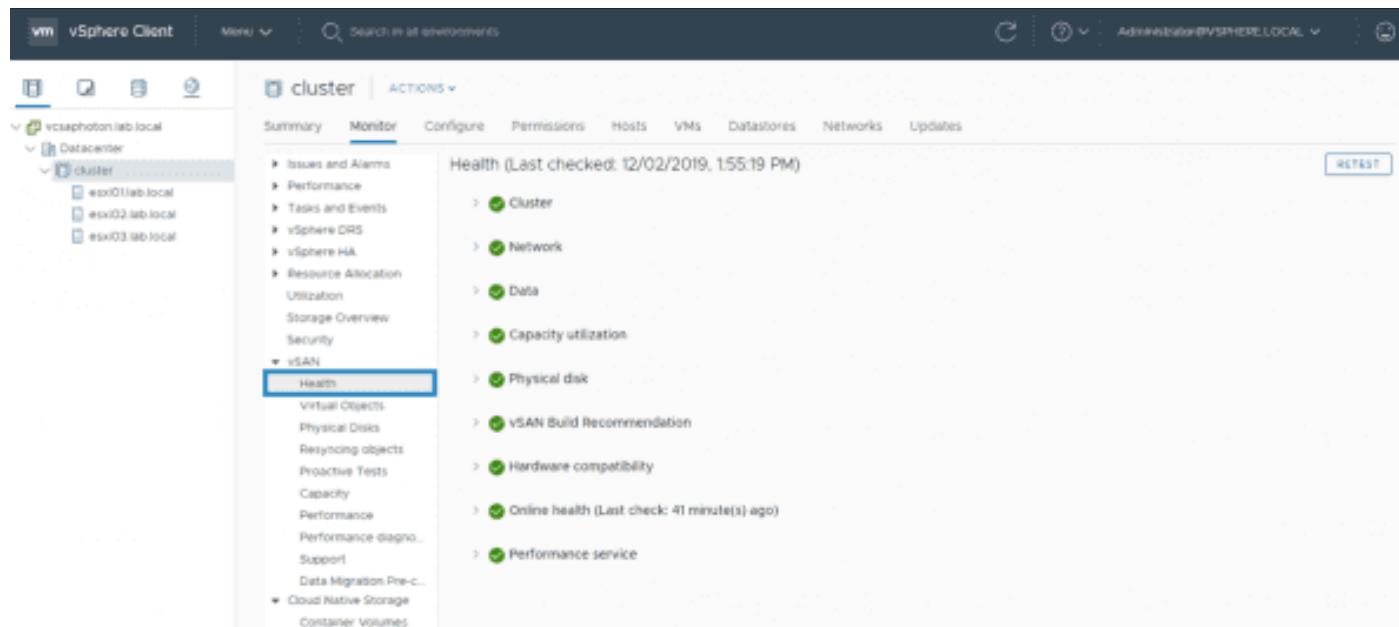
Skyline Health discovers environmental issues and recommends solutions before the actual problems happen. Skyline is a proactive VMware support solution that is available to all customers who have subscribed to Basic, Production, or Premier Support.

Skyline covers vSphere and VSAN Health, in addition to NSX-V, Horizon 7, and vRealize Operations Manager (vROPS). Skyline also includes SkylineLog Assist, which reduces customer effort in uploading support log bundles to VMware Global Support Services (GSS); with the customer's permission, the upload is performed automatically on a periodic basis.

VMware Skyline offers different sets of services depending on which support level you subscribe to. For example, customers who subscribe to the Premier support level can benefit from advanced troubleshooting findings, advanced reporting, and tailored remediation plans.

Customers with Production support can get support for the products mentioned above, starting with vSphere 5.5. They can get help via automated log uploading with Log Assist and have shorter times to resolution than customers with just Basic support.

Skyline Health is accessible through the vSphere Dashboard in vCenter Server. In fact, since vSphere 6.7 Update 3b there is a new menu entry called Skyline Health. The current release of vSphere 6.7 U3a has this menu entry, but the name is either vSphere Health or vSAN Health, depending on which part of the infrastructure you select (vCenter Server object or vSAN object).



VMware vSAN Health will become VMware Skyline Health

To monitor your vSphere infrastructure with Skyline Health, you must meet certain requirements. One such requirement is to enable the Customer Experience Improvement Program (CEIP); the other is to have internet connectivity.

**Note:** You can enable CEIP at any time if you didn't do so when installing your vCenter. You can check this in the vSphere Client by selecting Administration > Deployment > Customer Experience Improvement Program.

The screenshot shows the vSphere Client interface with the navigation bar at the top. On the left, there's a sidebar with various administration categories like Access Control, Roles, Global Permissions, Licensing, Licenses, Solutions, Client Plug-ins, vCenter Server Extensions, Deployment, System Configuration, and Customer Experience Improvement. The 'Customer Experience Improvement' link is highlighted. The main content area is titled 'Customer Experience Improvement Program'. It shows the 'Program Status' as 'Joined' with a joined icon. A descriptive text explains that the product participates in VMware's Customer Experience Improvement Program (CEIP), providing VMware with information to improve their products. It also states that VMware collects technical information about the organization's use of VMware products and services on a regular basis but does not personally identify any individual. Below this, there's a note about internet connectivity status and a table showing a single node entry: 'vcsaphoton.lab.local' with a 'VAMI link' button next to it. At the bottom, a message says leaving CEIP will disable all CEIP-based analytics programs, and a 'Leave CEIP' button is highlighted with a blue box.

## Change settings for the Customer Experience Improvement Program

The use of VMware Skyline might be a problem for customers running highly secure environments without internet access, since the system needs to send some data to VMware.

To start with VMware Skyline, you must connect to the VMware cloud site at <https://cloud.vmware.com/skyline> and create a Cloud Services Organization.

The screenshot shows the VMware Skyline Overview page. At the top, there's a navigation bar with links for 'Products', 'I Need To', 'Find a Partner', 'Events', 'Community', 'Why Our Cloud', 'Log In', and a search icon. Below the navigation is a 'Overview' section with a 'GET STARTED' button. The main content area features a large blue cloud graphic containing a smaller white cloud with a magnifying glass icon. The text 'VMware Skyline' is prominently displayed, followed by a subtext: 'Increase productivity and reliability by identifying and resolving issues before they occur.' There are three numbered steps: 1. Select or create an organization, 2. Set up Skyline Collector, and 3. Access Skyline Advisor. Each step has a corresponding blue number and a brief description.

## VMware Skyline at VMware

After this, you can download Skyline Collector. This is a virtual appliance that runs in your on-prem environment, collecting logs and analyzing your environment. The organization owner must grant access for users to Skyline Advisor. You must possess the Skyline Advisor service role. If you don't, then you won't have access to Skyline Advisor.

### Which services are covered and what's on the roadmap?

The first two products covered by VMware Skyline will be VMware vSAN and VMware vCenter Server, as they are the most critical core products that VMware wants to have covered. If something happens with vSAN, then the more data VMware technicians have for analysis, the better. The same goes for vCenter.

Even though much has been done to mitigate problems, nothing is problem-free. In the past, there were several areas in vCenter Server where things could go wrong. From a failed virtual disk, to a DB problem, or vSAN partition corruption.

VMware is working on enhancements and will be covering more products in the future via Skyline. A new Dell integration will be available for customers using Dell PowerEdge Server

hardware. Customers will see a notification in Skyline Advisor, informing them they can download Dell EMC SupportAssist Enterprise (SAE) to monitor and support Dell hardware proactively. If you're already using Dell EMC SAE, you'll see a new notification link to download VMware Skyline, so this new offering will work both ways.

## Skyline Advisor benefits

Skyline Advisor, which is basically the high-end assistance and support app, will cover vSphere, vSAN, NSX-V, Horizon, and vRealize Operations Manager (vROPS). You'll benefit from proactive findings and health checks, as well as on-demand analysis that can be scheduled and automated. Notifications can be sent via an alerting system that can be SNMP-based, through email, or through in-product alerts.

The screenshot shows the vSphere Client interface with the 'Brooklyn' cluster selected. The 'Monitor' tab is active. On the left, there's a navigation tree with categories like New York, APP, DB, WEB, and others. Under 'vSAN', the 'Skyline Health' option is highlighted. In the main pane, a section titled 'Skyline Health (Last checked: 10/28/2019, 2:21:09 PM)' lists several items with yellow warning icons. One item, 'Advisor', is highlighted with a blue arrow. To the right, a sidebar titled 'Advisor' contains an 'Info' section with text about Skyline Health and a link to 'Set up Skyline Advisor.' Another blue arrow points to this link. At the bottom of the sidebar, it says 'Already have an account? Log into Skyline Advisor.'

## VMware vSphere tech preview

When you click the Skyline Advisor, you're taken to your online account at <https://skyline.vmware.com>, where you can connect. If you don't have an account yet, you can create one.

Within the portal, you can access your inventory and view proactive findings and recommendations. You'll be advised about potential risks if you don't take any actions to correct the problems you might have.

Skyline Advisor is included in the proactive support package that you subscribed to. It is included with the Production and Premier support contracts. Skyline proactive support

gathers some data about your installation, which is necessary, and uploads the data via a secure channel. VMware uses an encrypted channel and stores those data at its US facility.

Sections 3 has no testable objectives.

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

VMware vSphere 7 and higher only supports vCenter Server Appliance (VCSA) based architecture where a conversion utility is provided for Windows-based vCenter server and also for external Platform Service Controllers (PSC). Starting vCenter server 7 the deployment topology is fairly simpler than in previous releases as external PSCs are no longer supported.

The services provided by PSC in prior vCenter Server versions are directly integrated into vCenter Server Appliance 7.0. vCenter Single Sign-On that is part of the vCenter server, is an authentication service that utilizes a secure token exchange mechanism rather than requiring components to authenticate users per component.

Single Sign-On domain is basically a local domain for authentication. The default name is vsphere.local but it's not mandatory as during the deployment you can override the default and choose a different name. The SSO authentication is able to authenticate also other products such as vRealize Operations etc.

When you deploy the vCenter server appliance you must create a new SSO domain or join an existing SSO domain. You should give your domain a unique name that is not used by Microsoft AD or OpenLDAP (if used within your environment).

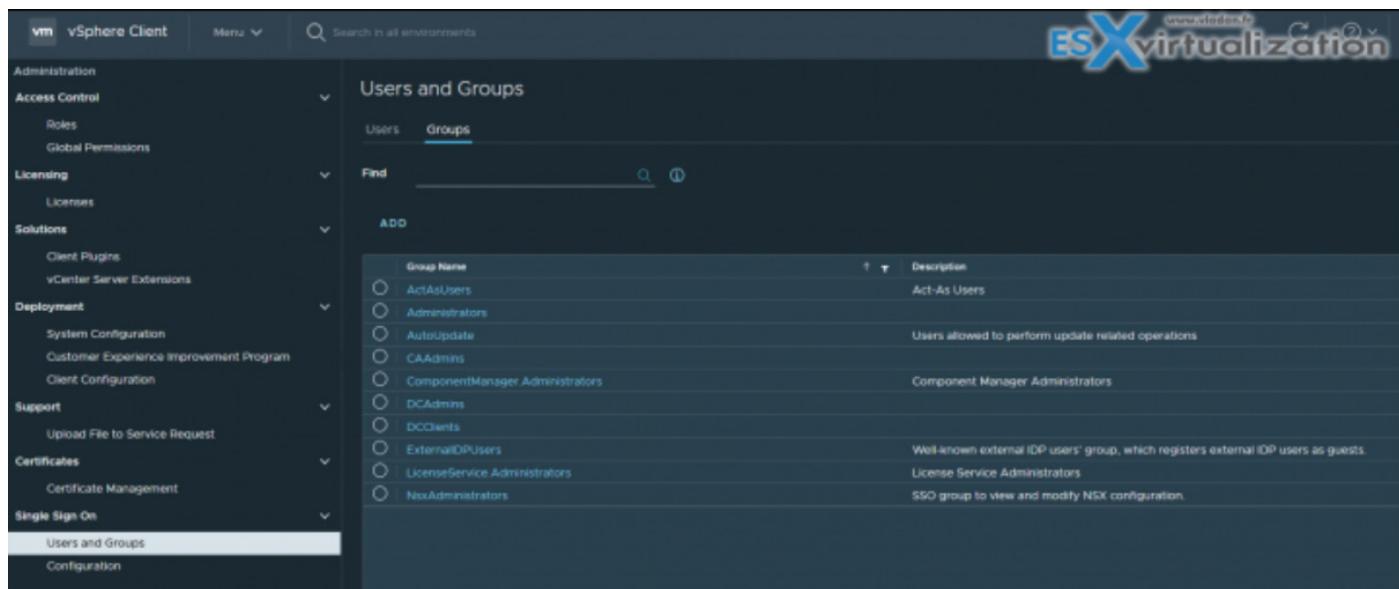
vCenter SSO allows vSphere components to communicate with each other through a secure token mechanism.

vCenter SSO uses:

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

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

**Predefined groups** - VMware has predefined groups defined. Add users to one of those groups to enable them to perform the corresponding actions. Do not delete any of the predefined groups in the vsphere.local domain. If you do, errors with authentication or certificate provisioning might result.



Once there you can join the PSC to Microsoft AD and then only to 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.

For topologies with multiple vCenter Servers and the transition to embedded PSCs, VMware has developed a new UI within vCenter Server where selected vCenter Server(s) can be converged to the embedded topology.

When running this utility, your external PSC will be shut down and unregistered from the single sign-on (SSO) domain.

The embedded PSC doesn't only simplify the vCenter architecture and patching, but you also have fewer VMs to manage and less consumption of RAM, CPU, or storage. If you have large-scale architecture with many PSCs, then the conversion can save a good amount of resources.

You also can seamlessly migrate from Windows-based vCenter server to VCSA.

During the Migration Assistant process, you can monitor the migration and manage what you want to bring over with you. The previous version of vCenter might also have had an external database. You have the possibility to migrate the data from the external DB to the embedded PostgreSQL database in vCenter Server 7. You can also migrate vCenter tasks and history. The progress of the migration is shown in the browser window.

## 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 disk. The certificate for the service itself is also stored on 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 and also certificates information.

**Identity Management Service** – handles identity sources and STS authentication requests.

## Objective 4.1.1 Configure single sign-on (SSO) domain

vCenter Server 7 has an internal user database that allows you to add and manage users very easily. User management and Single Sign-On are provided by the embedded Platform Service Controller (PSC). The PSC runs other services, such as licensing, certificate services, authentication framework, or appliance management.

You can also configure vCenter Server 7 to authenticate the connection via your Microsoft Active Directory (AD), so any users that you'll grant access to part of your vSphere infrastructure will not need to remember new login/password combination, but will use the Windows session credentials.

Single Sign-On allows different vSphere components to communicate with each other via a secure token mechanism (SAML).

The SSO domain that you create when you first install vCenter Server is the default identity source of the vSphere environment. You can set the Microsoft AD integration afterwards. VMware SSO allows not only Active Directory authentication, but also any other Security Assertion Markup Language (SAML) 2.0-based authentication source.

New in vSphere 7.0, vCenter Server supports [federated authentication](#) to sign in to vCenter Server.

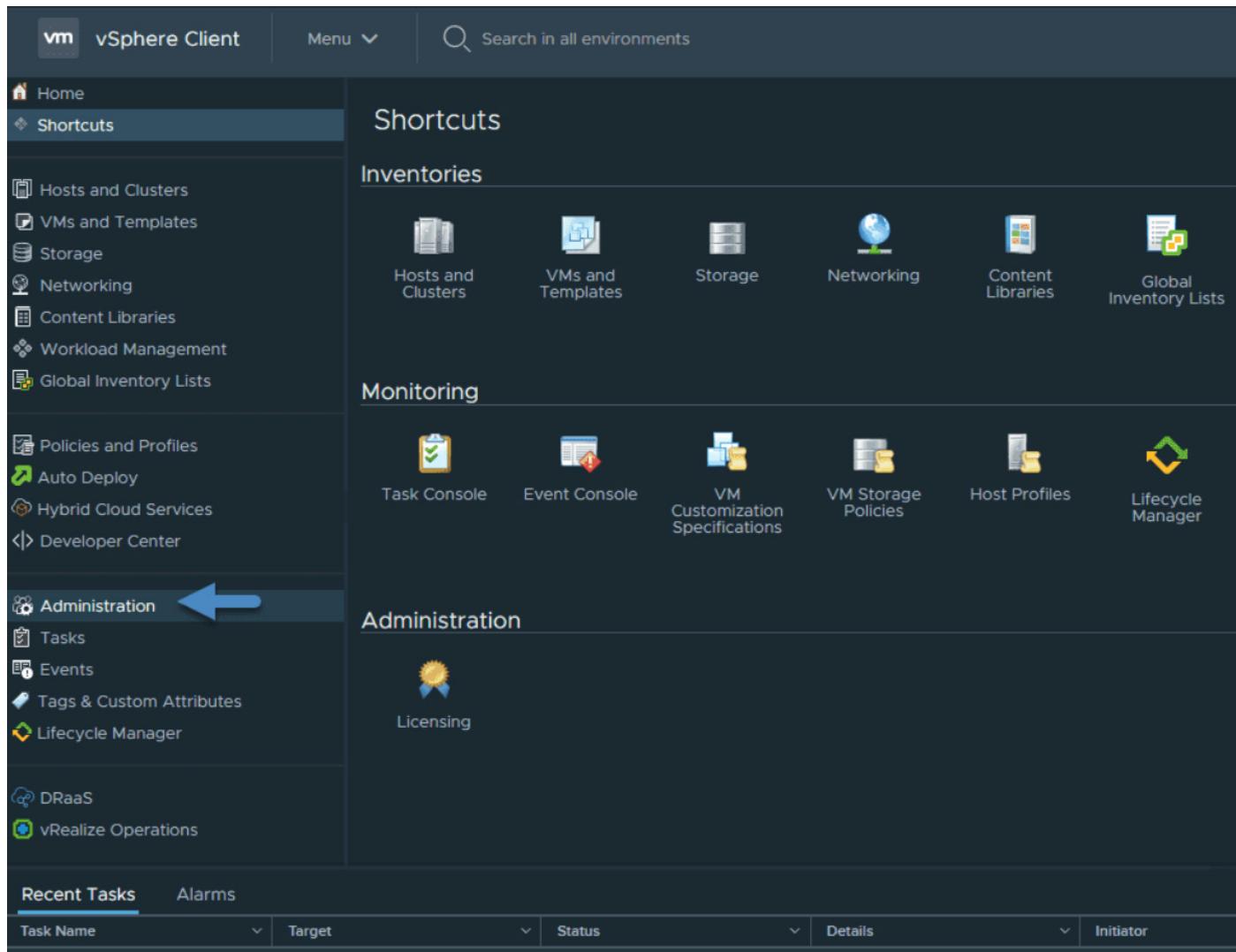
### Single Sign-on uses several services

- **Authentication of users** — Users are authenticated through either an external identity provider federation or the vCenter Server built-in identity provider. The built-in identity provider supports local accounts, Active Directory or OpenLDAP, integrated Windows authentication (IWA), and other authentication systems such as smart card, RSA SecurID, and Windows session authentication.
- Authentication of solution users through certificates.

- **Security Token Service (STS)** — This service issues the SAM tokens representing a user's identity.
- SSL for secure traffic.

## SSO Configuration: Identity providers and sources

Open your vSphere web client and connect to your vCenter Server 7, then go to **Shortcuts > Administration**.



### Access VMware SSO via Administration

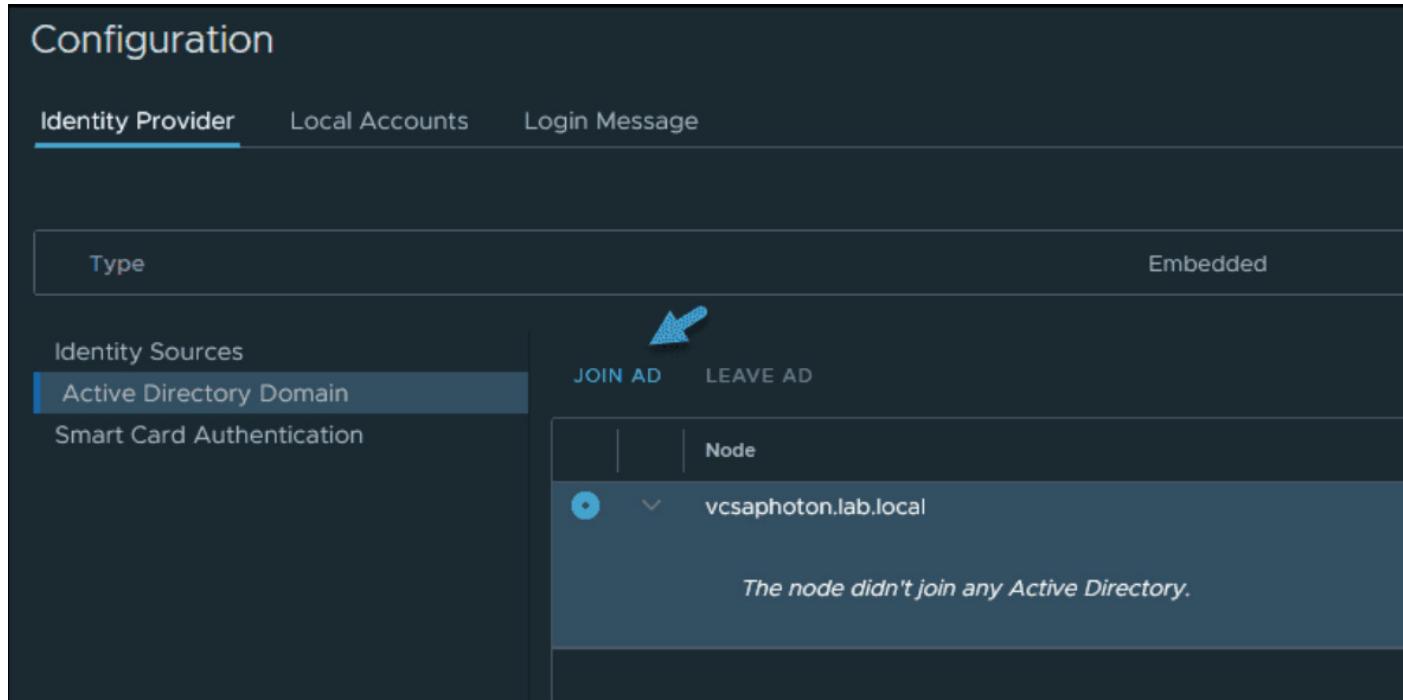
Click the **Single Sign-On** section and **Configuration**. On the **Identity provider tab**, click **Active Directory Domain > Join AD**.

## Configuration

Identity Provider   Local Accounts   Login Message

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

The node didn't join any Active Directory.



### Join Microsoft AD

Enter your Microsoft domain and OU (optional). After entering your Microsoft AD credential, you'll need to reboot.

I thought that VMware is better than Microsoft, but both vendors' products need a reboot when changing Microsoft AD specifications, changing domain, going from workgroup to domain, etc.

### Join Active Directory Domain

Domain: lab.local

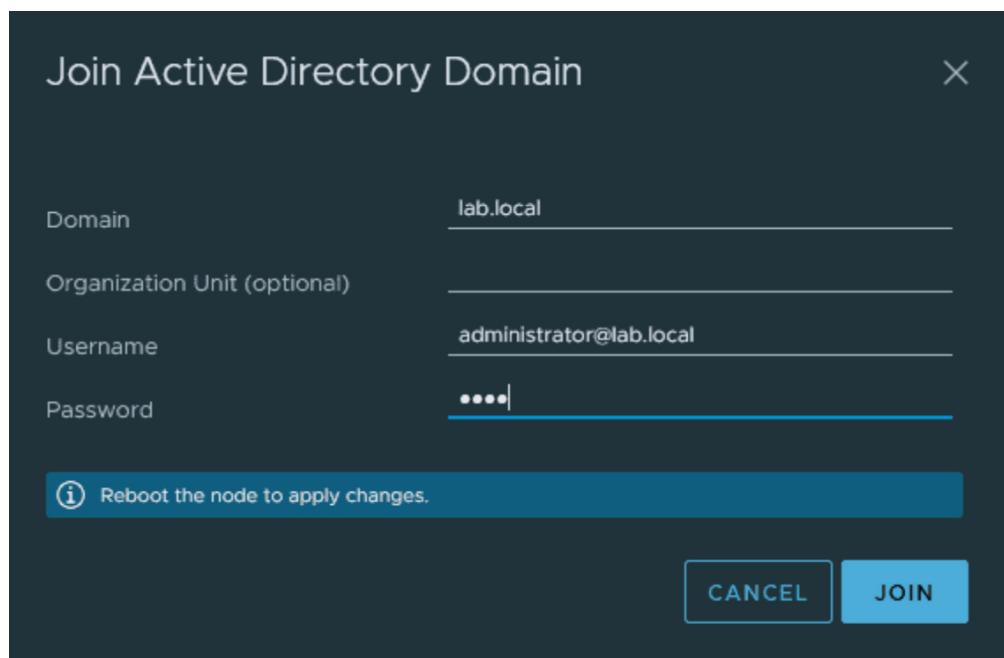
Organization Unit (optional):

Username: administrator@lab.local

Password:

**(i) Reboot the node to apply changes.**

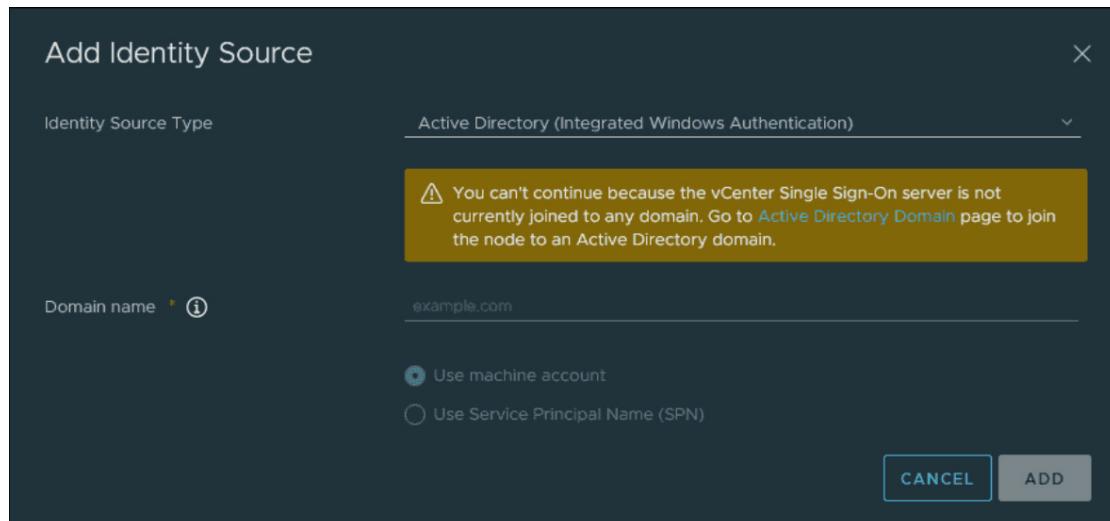
**CANCEL** **JOIN**



### Join Microsoft AD and reboot the appliance

If you do not join the VCSA to Microsoft AD, you'll get the following message when you want to change the identity source:

*You can't continue because the vCenter Single Sign-On server is not currently joined to any domain.*

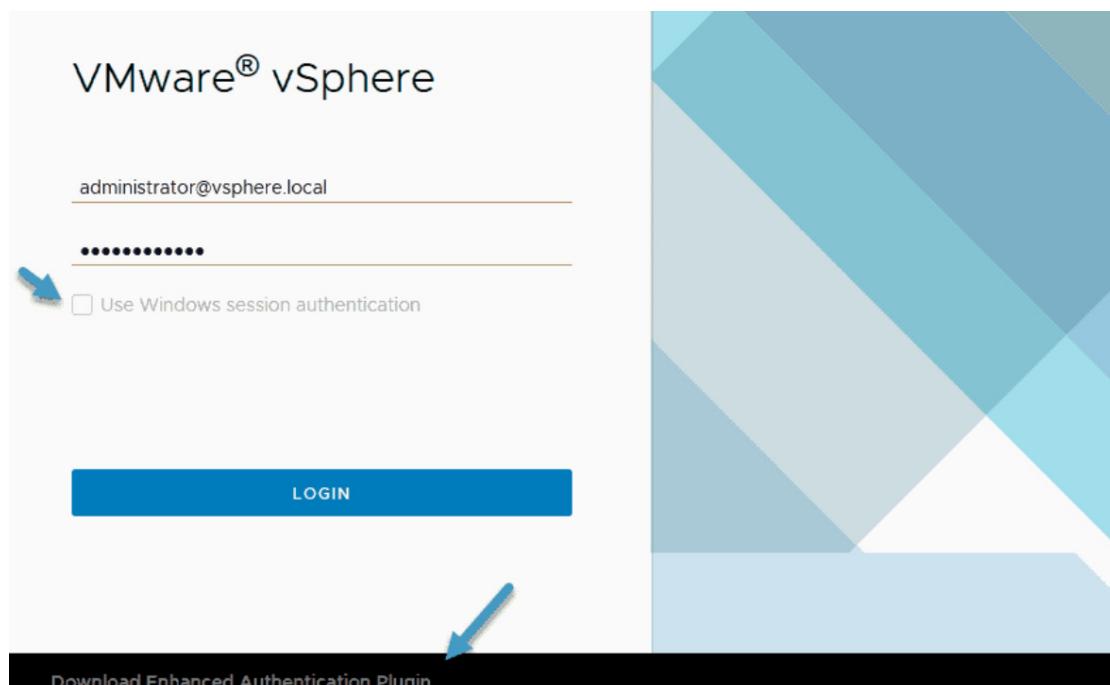


### Change identity source type

After a reboot, go back to the identity sources. You should now be able to pick the Microsoft AD.

I found it quite convenient when working on a Windows workstation attached to a Microsoft domain to simply select the checkbox Use Windows session authentication when connecting to vCenter Server.

If the checkbox is greyed out, you need to install the **Enhanced Authentication Plug-in**.



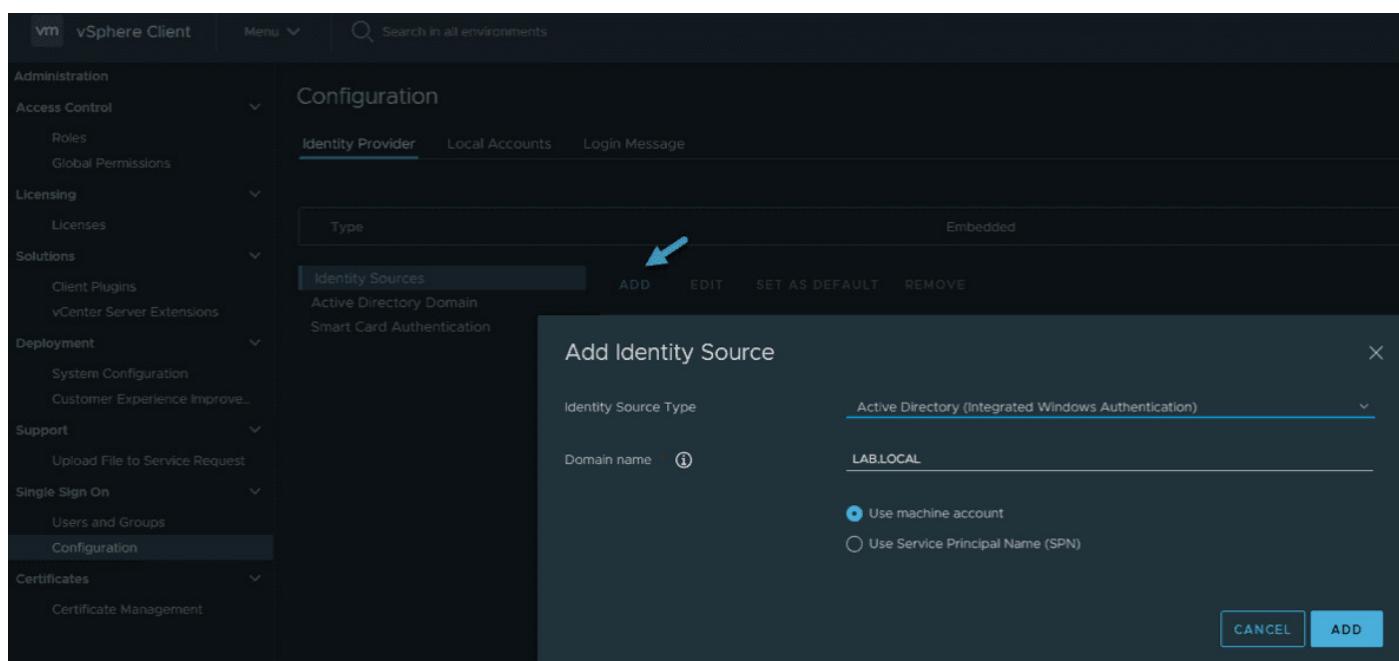
**Use Windows session authentication is greyed out**

The Enhanced Authentication Plug-in enables:

- Accessing the VM console
- Deploying OVF or OVA templates
- Transferring files with the datastore browser
- Using Windows session authentication

**Note:** If you configure vCenter Server to use federated authentication with Active Directory Federation Services, the Enhanced Authentication Plug-in only applies to configurations where vCenter Server is the identity provider (Active Directory over LDAP, integrated Windows authentication, and OpenLDAP configurations).

Back to our SSO identity provider configuration, where you can see how I'm adding the Microsoft AD as the identity source type.



### Add Microsoft AD as the identity source type

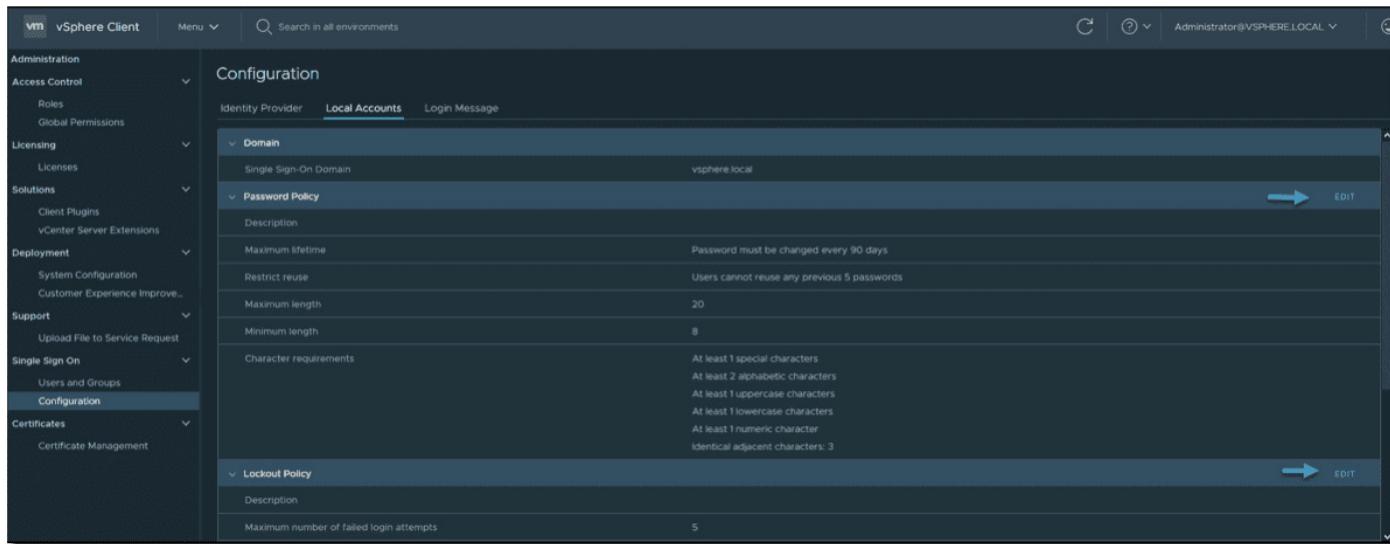
## Users and groups

Users and groups are also found in the same section. Let's have a look at the Local Accounts tab. On the Local Accounts tab, you'll see different options where you can change the password policy or password expiration lifetime.

By default, users are locked out after five consecutive failed attempts in three minutes, and a locked account is unlocked automatically after five minutes. You can change these defaults using the vCenter Single Sign-On lockout policy.

You should know that many of these groups are internal to vsphere.local domain or give users high-level administrative privileges. You should only consider adding users to those groups after cautious consideration of the risks.

You should never delete any predefined user or group.



### Possibility to change local password policy

## vCenter Server object hierarchy

All objects in the vCenter Server hierarchy can carry permissions that are assigned by you. You can pair a user and a role with the object. For example, you can select a resource pool and give a group of users read privileges to that resource pool object by assigning them a specific role.

However, for some services that are not managed by vCenter Server directly, you'll need to be a member of certain SSO groups that determine the privilege. For example, a user who is a member of the Administrators group can manage vCenter Single Sign-On. A user who is a member of the CAAdmins group can manage the VMware Certificate Authority, etc.

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

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

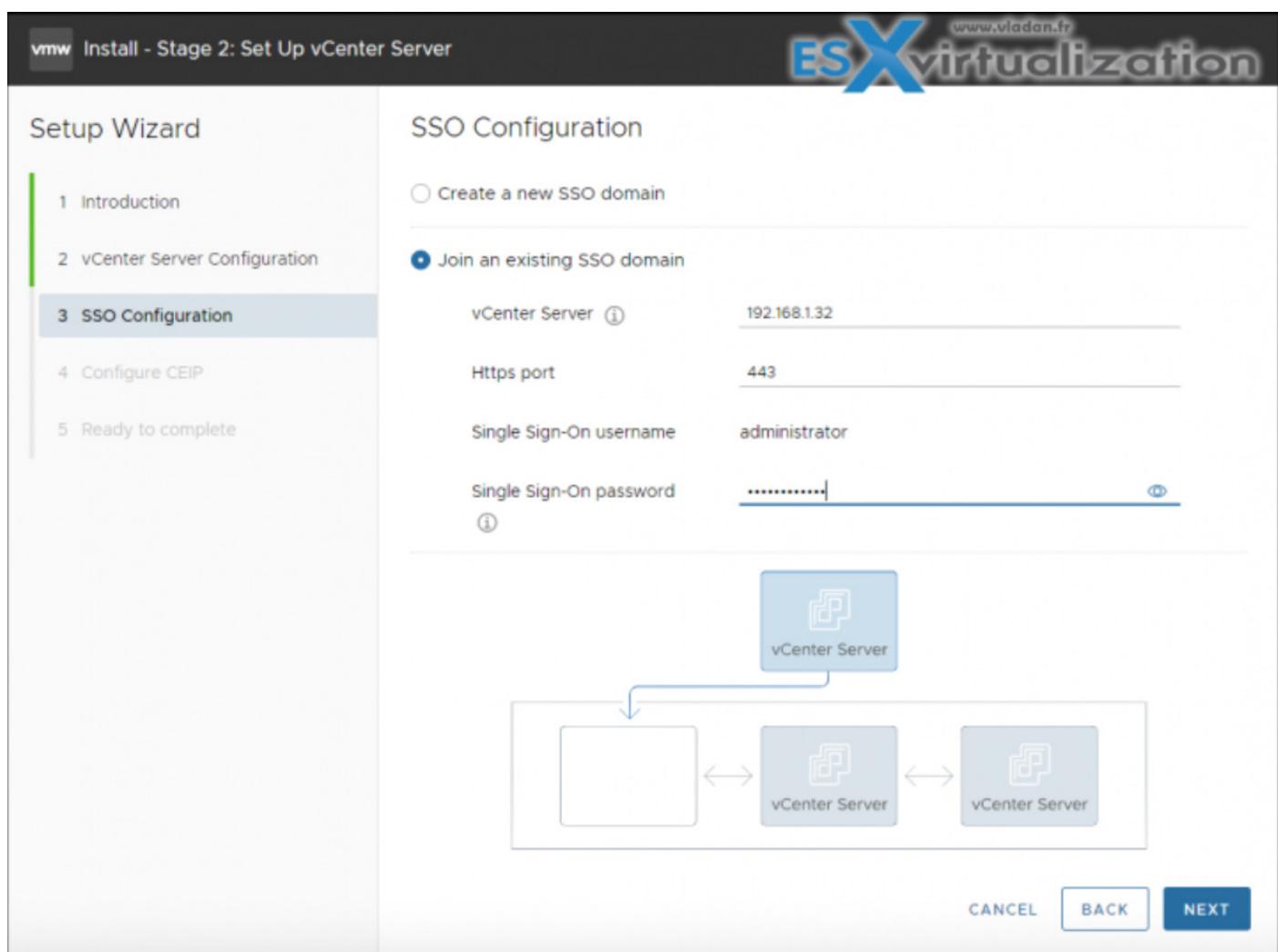
- Security Token Service (STS)
- SSL for secure traffic

- Authentication of users through Microsoft AD or OpenLDAP
- Authentication of solution through certificates

The domain name defaults to vsphere.local, but you can change it during the installation.

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.

During the deployment of an additional Center server within your organization, you can add it to the existing SSO domain.



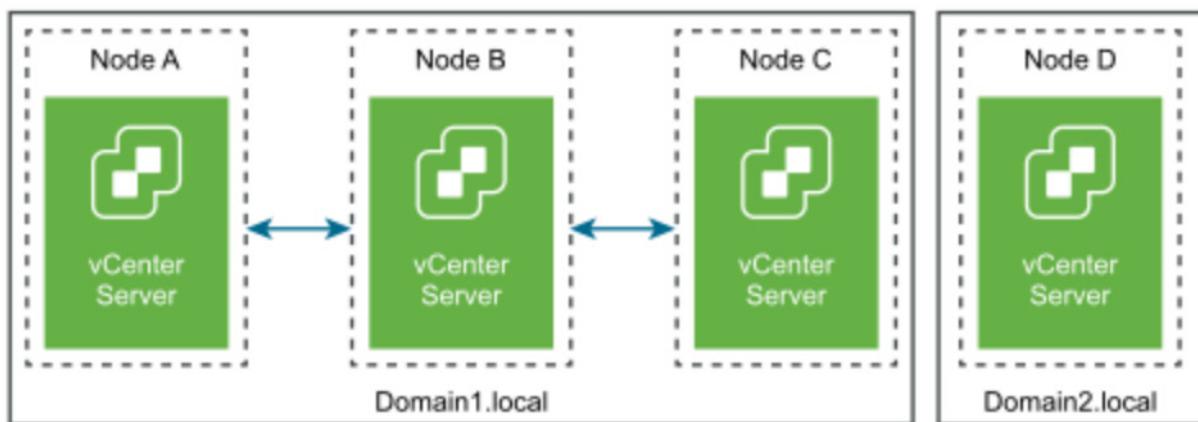
SSO Domain Repointing was introduced in vSphere 6.7 to allow the repointing of a vCenter Server from one SSO Domain to another. Let's say you have an environment with a couple of vCenter Servers, each within one site. One day, your boss tells you that your company just bought another company and that you need to manage the new environment.

By repointing the other company's SSO domain to your company's SSO domain, you'll be able to «join» that other vCenter Server to your organization and manage all the vCenter Servers with **Enhanced Linked Mode** (ELM).

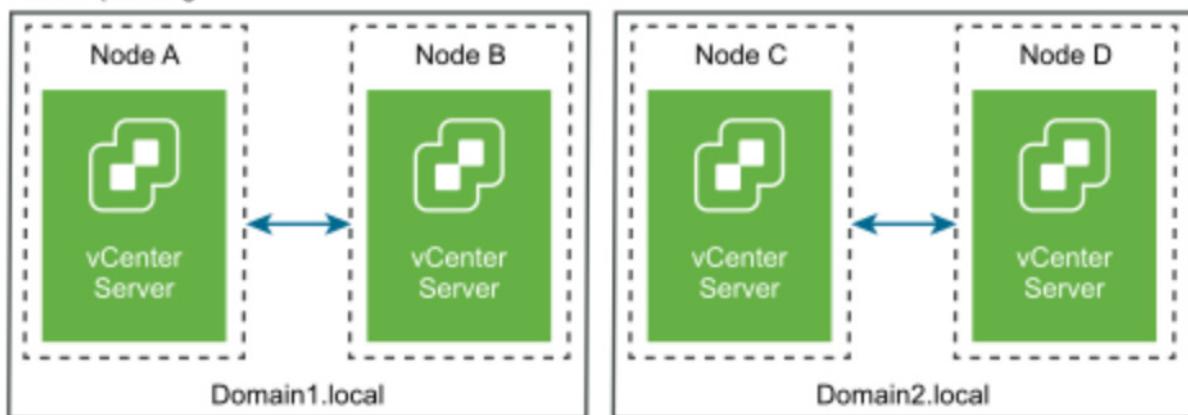
Here's how it is depicted in VMware documentation:

## Repointing a vCenter Server from One Domain to an Existing Domain

Before repointing



After repointing



←→ Represents vCenter Server nodes connected by linked mode

Quote from VMware documentation on the reporting process :

- Shut down the node (for example, Node C) that is being repointed (moved to a different domain).
- Decommission the vCenter Server node that is being repointed. For example, to decommission Node C, log into Node B (on the original domain) and run the following command:

```
cmsso-util unregister --node-pnid Node_C_FQDN --username Node_B_sso_administrator@sso_domain.com --passwd Node_B_sso_adminuser_password
```

After unregistering Node C, services are restarted. References to Node C are deleted from Node B and any other nodes that were linked with Node C on the original domain.

- Power on Node C to begin the repointing process.
- Run the execute command. In execute mode, the data generated during the pre-check mode is read and imported to the target node. Then, the vCenter Server is repointed to the target domain.

For example, run the execute command with the following:

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

We're using the **cmsso-util domain-repoint** command.

If you want, you can check the detailed [how-to article we've done for vSphere 6.7](#), which is still valid for vSphere 7.

## Objective 4.2 Configure VSS advanced virtual networking options

In this section you will learn about the difference between vSphere Standard Switch (VSS) and vSphere Distributed switch (VDS) in vSphere 7.

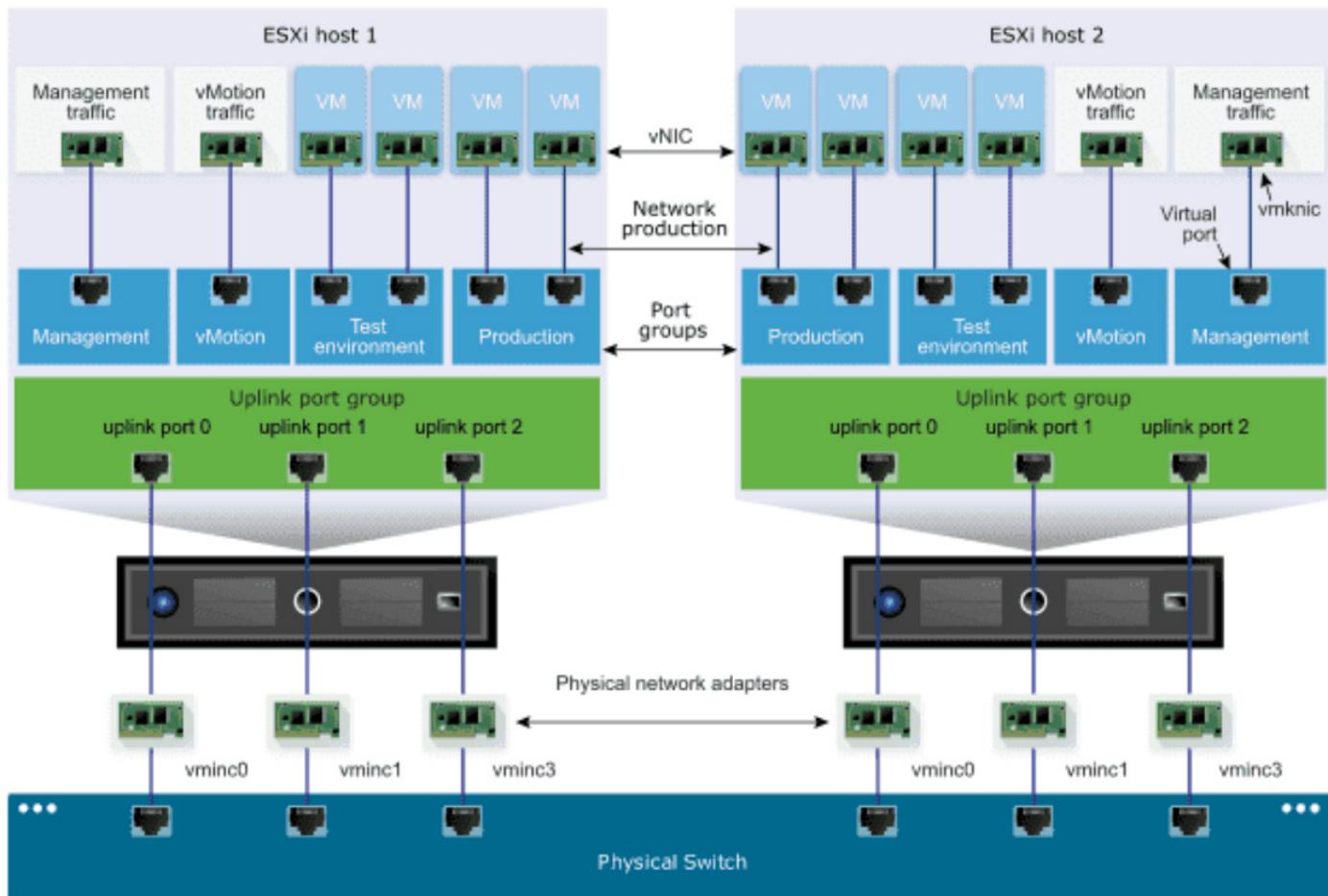
While vSphere 7 does not offer any significant changes or new networking capabilities, it does offer the ability to run vSphere with Kubernetes, which previously involved NSX-T installation. However, NSX-T is not required to run Kubernetes clusters with vSphere 7.

As you know, NSX-T has some network requirements that need to be met before installation. vSphere 7, or rather vCenter Server 7, offers a new capability called Multi-homed NICs, which allow having multiple management interfaces for vCenter and fulfilling different network configuration and segmentation needs.

Let's start with the basics first and compare some VSS and VDS features.

### vSphere Standard Switch

This works pretty much the same as a physical Ethernet switch. VSS knows which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. VSS can be connected to physical switches by using physical Ethernet adapters. These adapters are called uplinks, and their important function is to connect the virtual network into a physical network as they are connected to a physical switch.

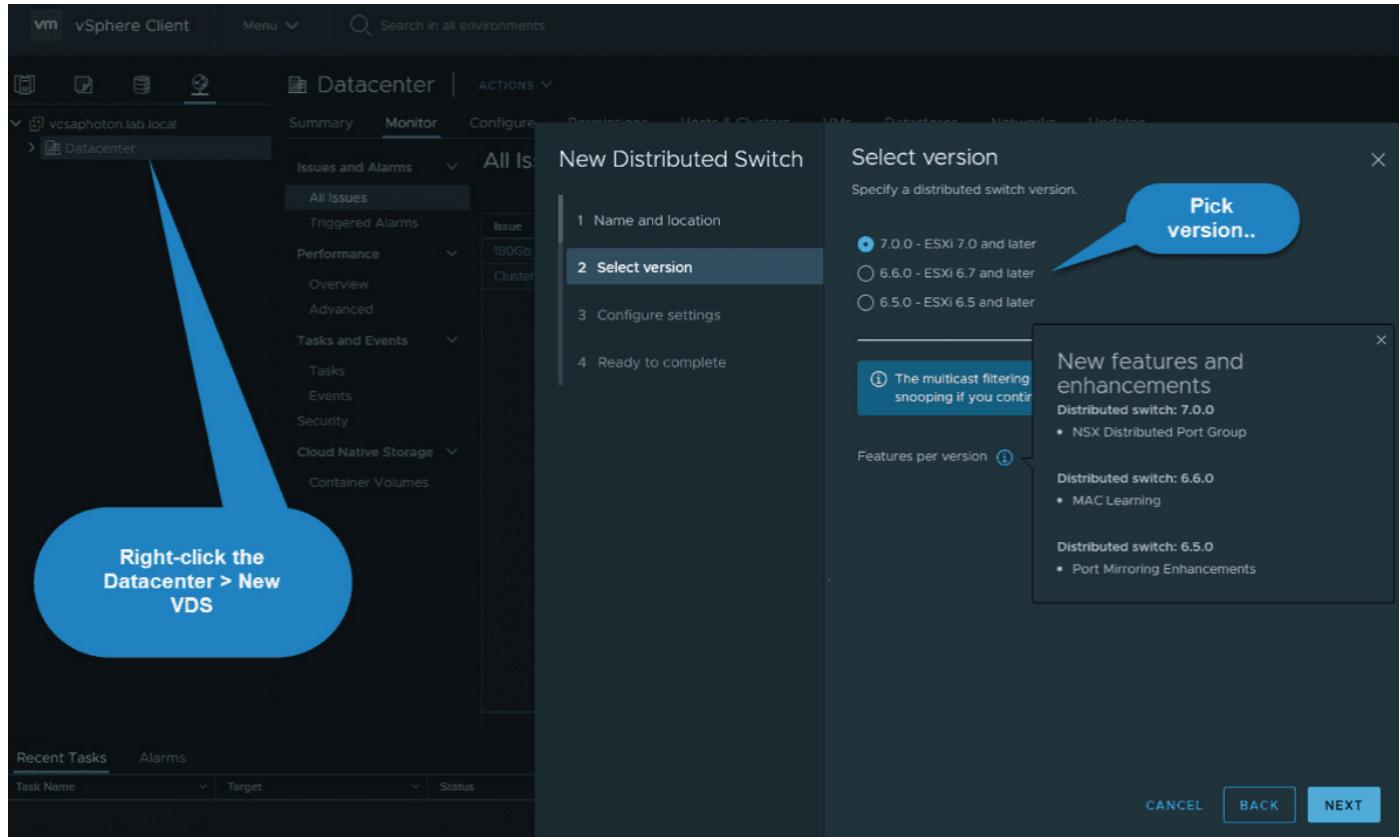


### Connectivity with the vSphere Standard Switch

#### vSphere Distributed Switch

Imagine the VDS as a single switch connected with all associated hosts in a data center. The VDS has the role of providing centralized provisioning, administration and monitoring of virtual networks. When you configure the VDS, you can choose the ESXi host to which you attach and propagate this configuration. This way, you don't have to go one-by-one to each of your ESXi hosts to replicate the configuration.

With the evolution of vSphere versions, the VDS has evolved as well. You can see all the versions you can still create on vCenter Server 7. vSphere 6 is no longer on the list.



## Create a new VDS at the datacenter level

### Standard Port Group

When you want to connect network services that are active on your network, you do it through standard port groups. Port groups basically define how a connection is made through the switch to the network. Usually, you have a single standard switch that is associated with one or more port groups, although this is not the limit. You can also create multiple VSSs on your host, each of which can carry multiple port groups.

### Distributed Port Group

This is a port group that is associated with a vSphere distributed switch. Distributed port groups define how a connection is made through the vSphere distributed switch to the network.

### vSphere 7 Standard Switch advanced networking options

Some advanced options that are available when you configure a VSS are the possibility of having two or more physical NICs in a team to increase the network capacity of the VSS or a standard port group. You can also configure failover order to create network traffic routing in the event of an adapter failure.

Another feature within VSS is that you can select a load balancing algorithm to determine how the standard switch distributes the traffic between the physical NICs in a team.

## Configure load balancing on VSS

An important thing to remember is that these are per-vSwitch settings, so if you have three hosts in the cluster, you must replicate those settings manually across all your hosts. Hence the advantage of distributed vSwitch.

You have several options here:

**Route based on originating virtual port** - The VSS selects uplinks that are based on the VM port IDs on the VSS or VDS. This is the default load balancing method. Each VM running on the ESXi host has a virtual port ID on the vSwitch. VSS uses the virtual machine port ID and the number of uplinks in the NIC team. Once the uplink is selected, it always forwards traffic through the same uplink for this VM (while the VM is still running on the same port). Once the VM is migrated or deleted, the port ID on vSwitch is freed.

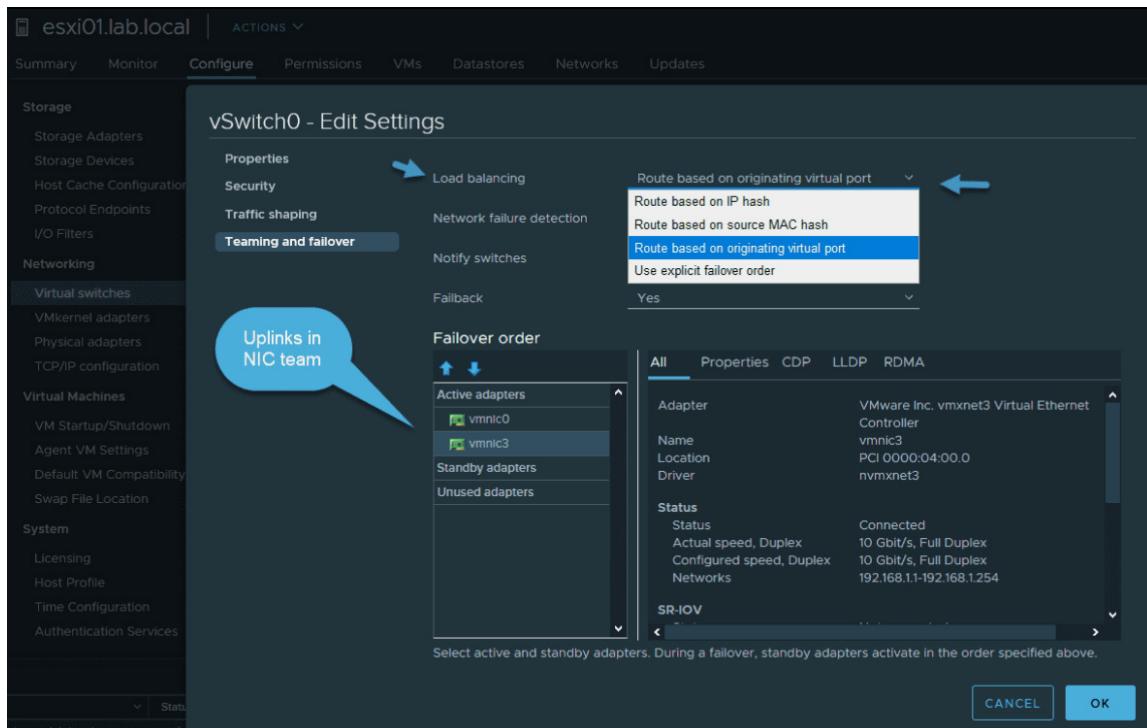
**Route based on source MAC hash** - The vSwitch selects uplinks for VMs based on the source and destination IP address of each packet. The system calculates an uplink for the VM based on the VM's MAC address and the number of uplinks in the NIC team.

The advantage is that there is a more even distribution of the traffic than Route Based on Originating Virtual Port. The virtual switch calculates an uplink for every packet. However, this policy consumes somewhat more resources. Another disadvantage is the fact that the vSwitch does not know if the uplink is saturated.

**Route based on IP hash** - This policy is used when the vSwitch selects uplinks for VMs based on the source and destination IP of each packet. Any VM can use any uplink in the NIC team. The route depends only on the source and destination IP address. The advantage is that each VM can use the bandwidth of any uplink in the team, and the traffic is spread evenly among all uplinks in the NIC team.

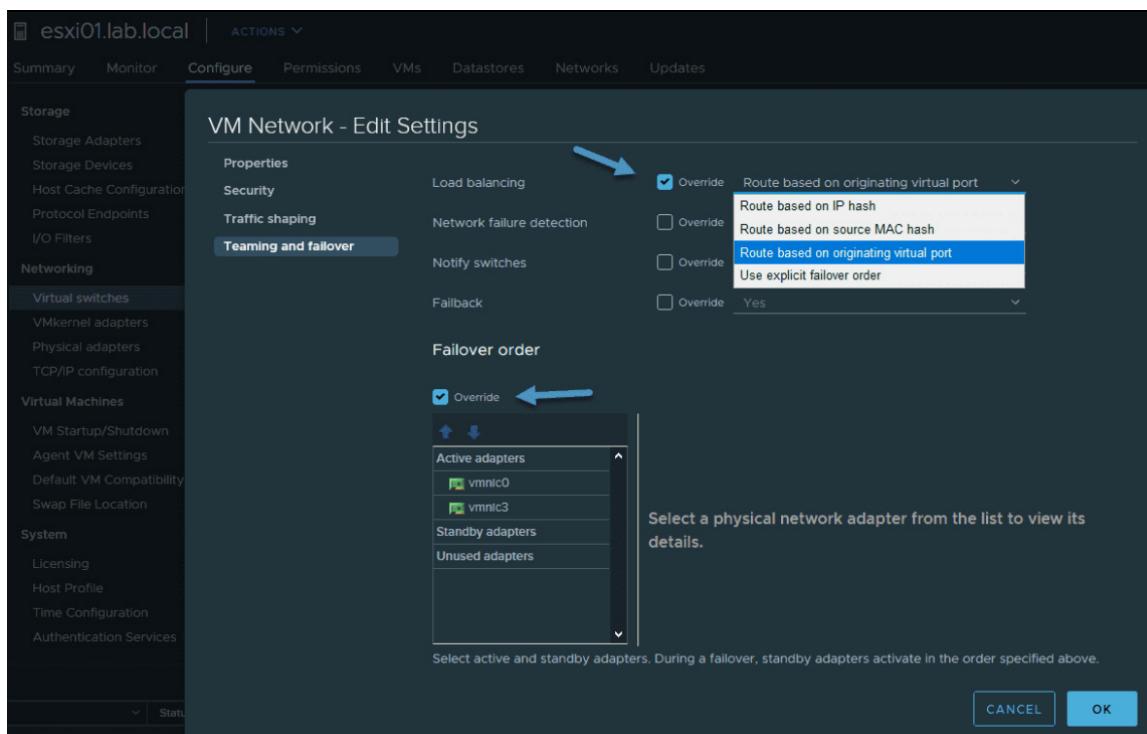
**Route based on physical (only available for VDS)** - The best option. This load balancing policy is based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks.

**Use Explicit Failover Order** - No real load balancing is done with this policy. The vSwitch always uses the uplink that is the first in the list of active adapters. If no adapters are available in the «Active» list, then the vSwitch picks the adapter from the «Standby» adapters list.



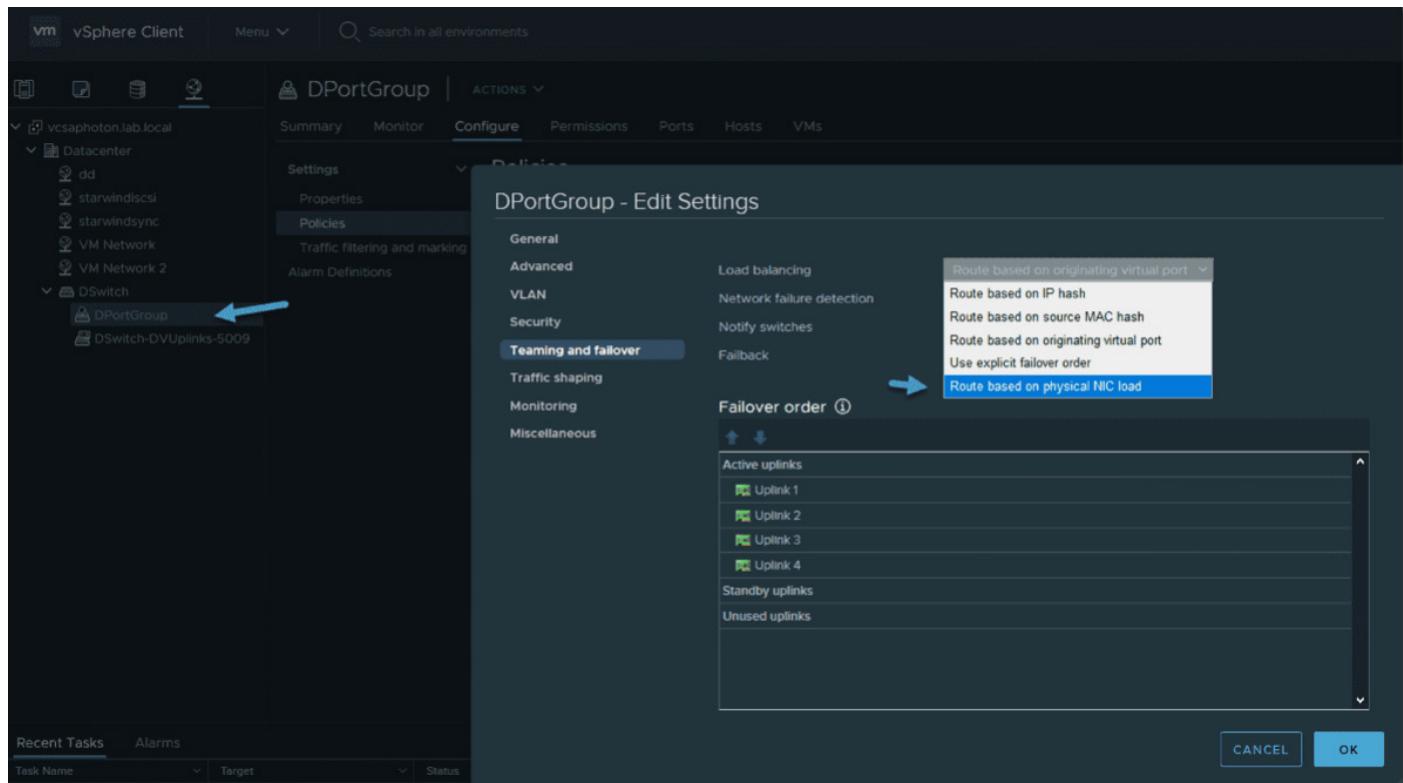
## Changing load balancing policy on vSwitch

Next to the settings at the vSwitch level, we can have a look at the port group level. Remember, each vSwitch can have several port groups. The same load balancing options apply here. The only thing that changes is the «override» checkbox, which allows us to have a different policy on the port group level and at the vSwitch level.



## Changing load balancing policy on port group

Now let's see what it looks like at the distributed port group. You see that we have the option to choose a network load balancing policy based on the «Route Based on Physical NIC Load» here.



**Changing load balancing policy on a distributed port group**

## Objective 4.3 Set up vCenter identity sources

During a vCenter Server login process, when a user logs in with a username, vCenter single sign-on (SSO) verifies the default identity source and determines whether the user has the right to connect. If the user tries to log in with a domain name on the login screen, vCenter Server 7 and SSO check whether the specific domain has been added as an identity source.

Adding and removing vCenter identity sources or setting up the default one is done through the vSphere web client by connecting to vCenter Server. SSO can have several domains attached to identity sources, depending on the one set as the default.

All the data about groups and users are either stored locally in the SSO database or retrieved and searched through Microsoft Active Directory (AD)/Open LDAP systems, if those are configured.

**Note:** There is only one default domain at any given time. You cannot have two default domains at the same time.

Think of the identity provider as a service that manages identity sources and authenticates users. Examples of an identity provider include Microsoft AD Federation Services (ADFS) or vCenter SSO.

## Which type of identity sources are supported in vCenter Server 7?

- **Microsoft AD over LDAP** — SSO supports multiple AD over LDAP identity sources
- **AD over LDAPS** — secure connection by using SSL to the LDAP (LDAP secure)
- **Microsoft IWA (Integrated Windows Authentication)** – You're allowed to specify a single AD as an identity source. This option allows users to log in to the vCenter Server using your AD accounts.
- **Open LDAP** — vCenter SSO supports Open LDAP 2.4 and later; multiple Open LDAP identity sources are supported.

The different options are available through the options in the Administration section > SSO config. This section offers different identity provider options.

### How to set up a default identity source via vSphere client

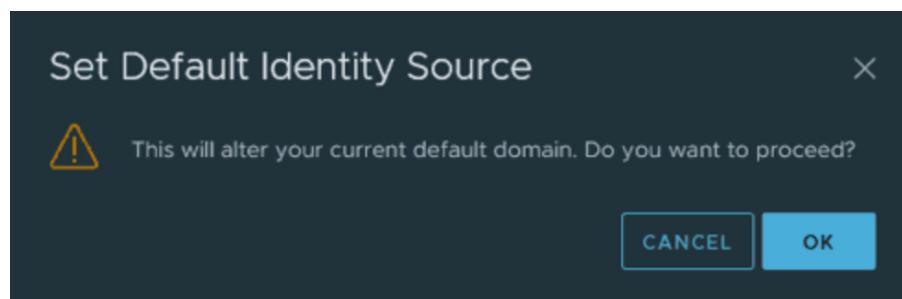
Connect to the vCenter Server with the default administrator@vsphere.local login and password. This is the default that you created during the installation process. (Note: if you created a different domain during the installation, connect via administrator@yourdomain.)

Go to **Home > Administration > Single Sign-On > Configuration > Identity Provider** tab.

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

How to set up default identity source

When you click the button, an overlay window opens where you'll be asked whether you want to proceed.



### Set default identity source validation

You have the details about the domain, alias, type, server URL, or name. After selecting one of the connections via the radio button, you can edit, set as default, or remove the connection.

Outside the Identity Provider tab, there is also a Local Accounts tab where you can specify and change password policy or account lockout policy. These policies are for the local SSO accounts only.

### A word about the upcoming Microsoft AD security changes

The **Integrated Windows Authentication** option is used by many admins, as this is the easiest way of integrating with existing Microsoft AD environments. However, Microsoft plans to change the default behaviour of AD to require strong authentication and encryption.

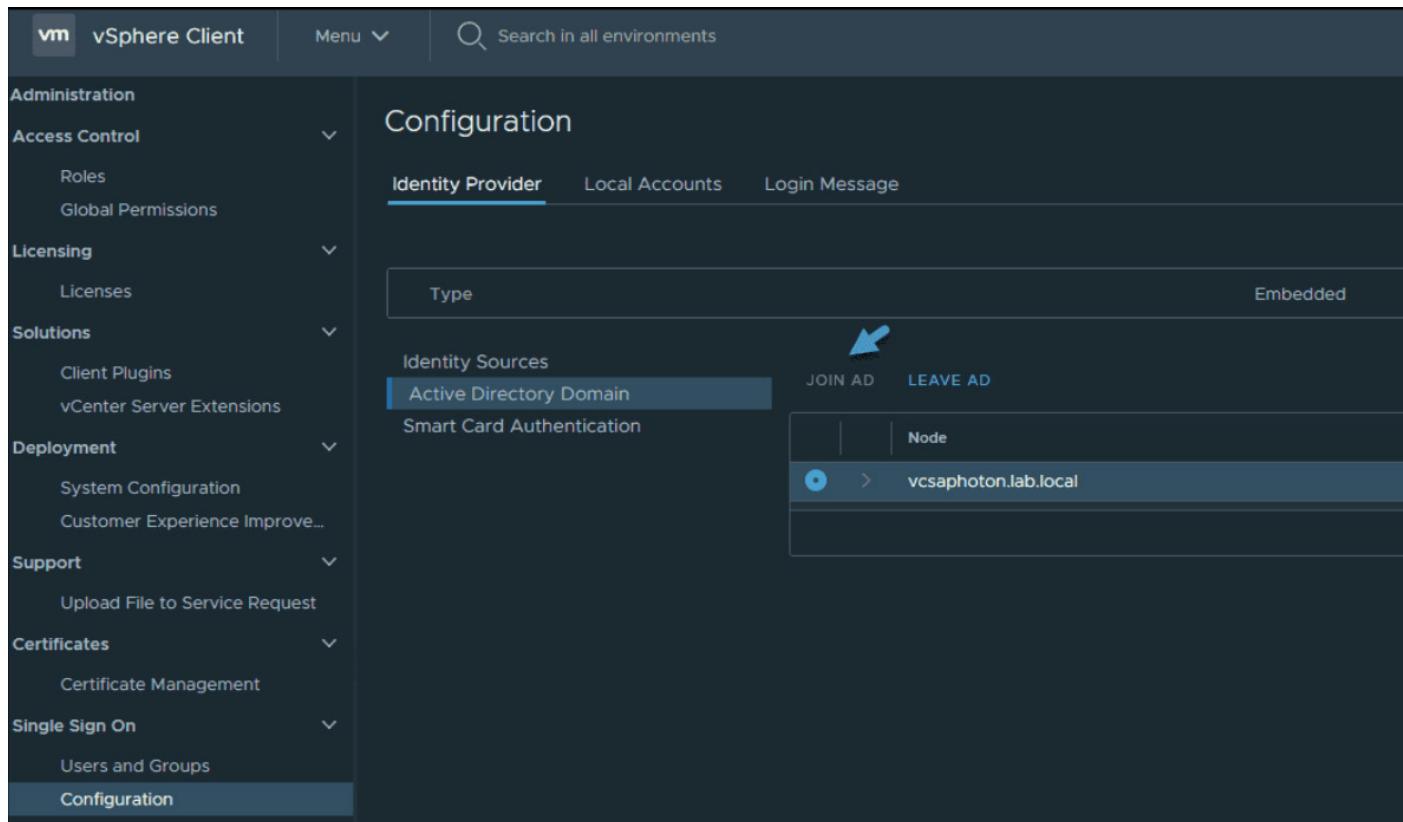
After the changes, the Integrated Windows Authentication won't work as expected. You won't be able to search for users and groups to SSO, and there may be some other incompatibilities.

While Integrated Windows Authentication works for now, Microsoft plans to secure AD further. This will affect VMware configurations, as there will be a hard requirement to use strong authentication and encryption. If you are using unencrypted LDAP (ldap://, not ldaps://), you'll need to implement a couple of changes. You'll need to plan and enable LDAPS or use identity federation.

VMware is sending a message here—Integrated Windows Authentication (IWA) is deprecated in vSphere 7. It is still supported but deprecated. Microsoft AD over LDAPS and Identity Federation are the two primary recommended approaches for connecting vSphere to Active Directory.

Note that **if you've added your vCenter Server to your Microsoft AD domain, you're not affected** by this upcoming change. You're only affected when using LDAP without adding the vCenter Server to AD.

As you can see, we have already joined our vCenter Server to Microsoft AD, so we should be fine.



**Our vCenter Server is joined to AD 1**

## How do I move from LDAP to LDAPS?

If for some reason you operate on a vCenter Server system that is not joined to AD, the move from LDAP to LDAPS needs a complementary configuration and setup on your DC, as you'll need to install enterprise CA and deal with certificates. I invite you to go through [this video](#) from VMware if you need to do so.

## Using scripts to manage authentication services

vCenter Server Appliance (VCSA) has a built-in command called **sso-config** for managing configuration services. You can have a look at different options by running **sso-config -help**. Another useful command, **service-control**, allows you to start, stop, and list services. Use **service-control --list-services** to show all services and their state. Use **service-control --help** for further details.

## Objective 4.3.1 Configure Identity Federation

The release of VMware vSphere 7 has introduced many new features. Many things have been improved over the previous release, and some completely new concepts have been introduced. In this section, we'll detail vCenter Identity Federation which will be available in vCenter server 7.0.

If we look at the corporate environment, we can see that there are users and external workers using mobile devices that are present within the corporate workspace. Secure authentication must be available for these devices. It is important both that users can authenticate themselves and that the organization can be certain that a particular user is authenticated and can be granted access to secure documents and corporate emails.

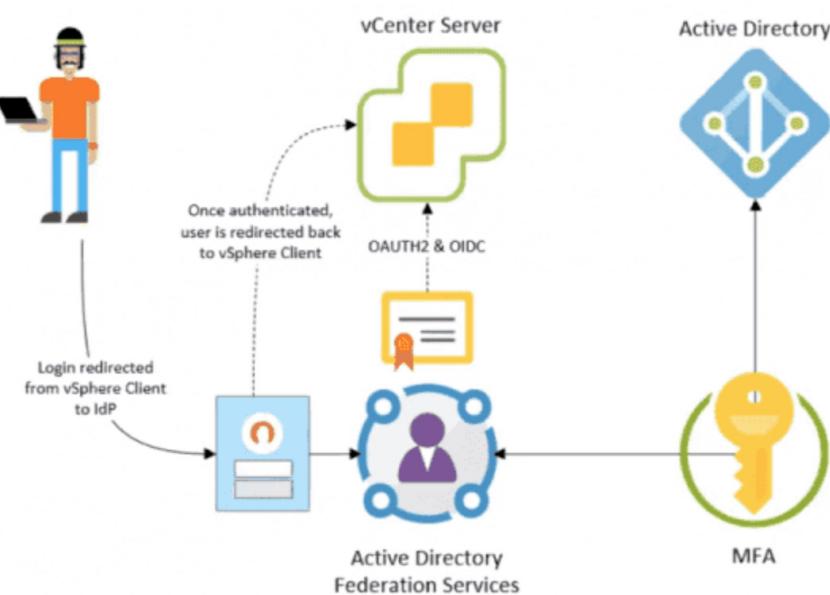
Identity management is one of the key elements needed for each organization to remain secure. Organizations are looking to consolidate their authentication into dedicated identity providers with flexible options, such as Multi-Factor Authentication (MFA). Another consideration is the reduction of risk via federated solutions, in which the applications do not have to handle credentials directly.

vSphere Identity Federation (VIF) uses industry standard protocols such as OIDC and OAuth 2.0 to connect to these systems and to participate in the corporate and identity solution. OpenID Connect (OIDC) is an authentication protocol based on the OAuth 2.0 specifications. It uses simple JSON Web Tokens (JWT). OAuth 2.0 is a protocol that allows a user to grant limited access to their resources on one site or to a different site without the need to expose their credentials at any time.

The traditional link between vCenter Server and Microsoft Active Directory (AD) is no longer used if you use vCenter Identity Federation.

When Active Directory Federation Services (ADFS) are configured and users try to connect to vCenter, they are redirected to ADFS, which prompts the users for login credentials. After successful authentication, the users receive a token that enables them to do their work as before. The token-based service is an industry standard now, so vCenter will be able to use the same system as other applications and systems.

The process looks like this:



## vSphere Identity Federation overview

vSphere Identity Federation basically allows you to connect your vCenter Server to an external identity provider that supports OAuth 2.0, so you can log in to vCenter Server with the corporate identity using this enhanced single sign-on (SSO) and multi-factor authentication (MFA) method.

Starting from this release, vSphere and ADFS support some additional providers, such as Azure AD, PingID, Okta, vIDM, and others.

## How to configure vCenter with ADFS

The configuration of vCenter Identity federation has three principal phases:

- Creating an application group on the Microsoft ADFS server and configuring it for vCenter Server
- Creating an identity provider via the vCenter SSO Administration configuration page
- Configuring group membership in vCenter to provide authorization for users within the ADFS domain

After all this is done, users will be able to log in to vCenter and be redirected for authentication via ADFS and the corporate portal.

There is a new wizard that allows you to configure identity federation with Microsoft ADFS. To configure vCenter identity federation, you must go to the Single Sign-On configuration page and add a new identity source in the Identity Sources pane.

The screenshot shows the vSphere Client interface with the 'Configuration' section selected. The left sidebar shows various administrative categories like Access Control, Licensing, Solutions, Deployment, Support, Hybrid Cloud, and Single Sign On. The 'Configuration' category is currently active. In the main pane, the 'Identity Provider' tab is selected. Below it, the 'Identity Sources' table displays two entries:

Name	Type	Domain	Alias
--	System Domain	vsphere.local	--
--	Local OS	localos	--

At the bottom of the table, it says '2 items'. There are buttons for 'ADD', 'EDIT', 'SET AS DEFAULT', and 'REMOVE'.

vSphere Identity Federation Configuration wizard

In order to make the configuration work, you'll need to configure the ADFS server before you start the wizard in your vCenter.

You'll need to create an OpenID Connect configuration, which is known as an application group. This group comprises a server application and API components, which together specify the connection details for vCenter Server. vCenter Server then uses those details as a trust and can communicate with the ADFS server.

After you create the application group on the ADFS server, you can return to the vCenter Server and launch the wizard. Note that the detailed configuration of the vCenter identity federation and ADFS is outside the scope of this section.

Other configurations are also needed, such as users and group configuration, as well as permission configuration within the vCenter SSO Administration section.

## Objective 4.3.2 Configure Lightweight Directory Access Protocol (LDAP) integration

The Active Directory over LDAP identity source is preferred over the Active Directory (Integrated Windows Authentication) option. The OpenLDAP Server identity source is available for environments that use OpenLDAP.

If you are configuring an OpenLDAP identity source, see the VMware knowledge base article at <http://kb.vmware.com/kb/2064977> for additional requirements.

- **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 need this option to use the local machine account (computer account 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 are 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.

Note that OpenLDAP is also supported, but there are some requirements that need to be met:

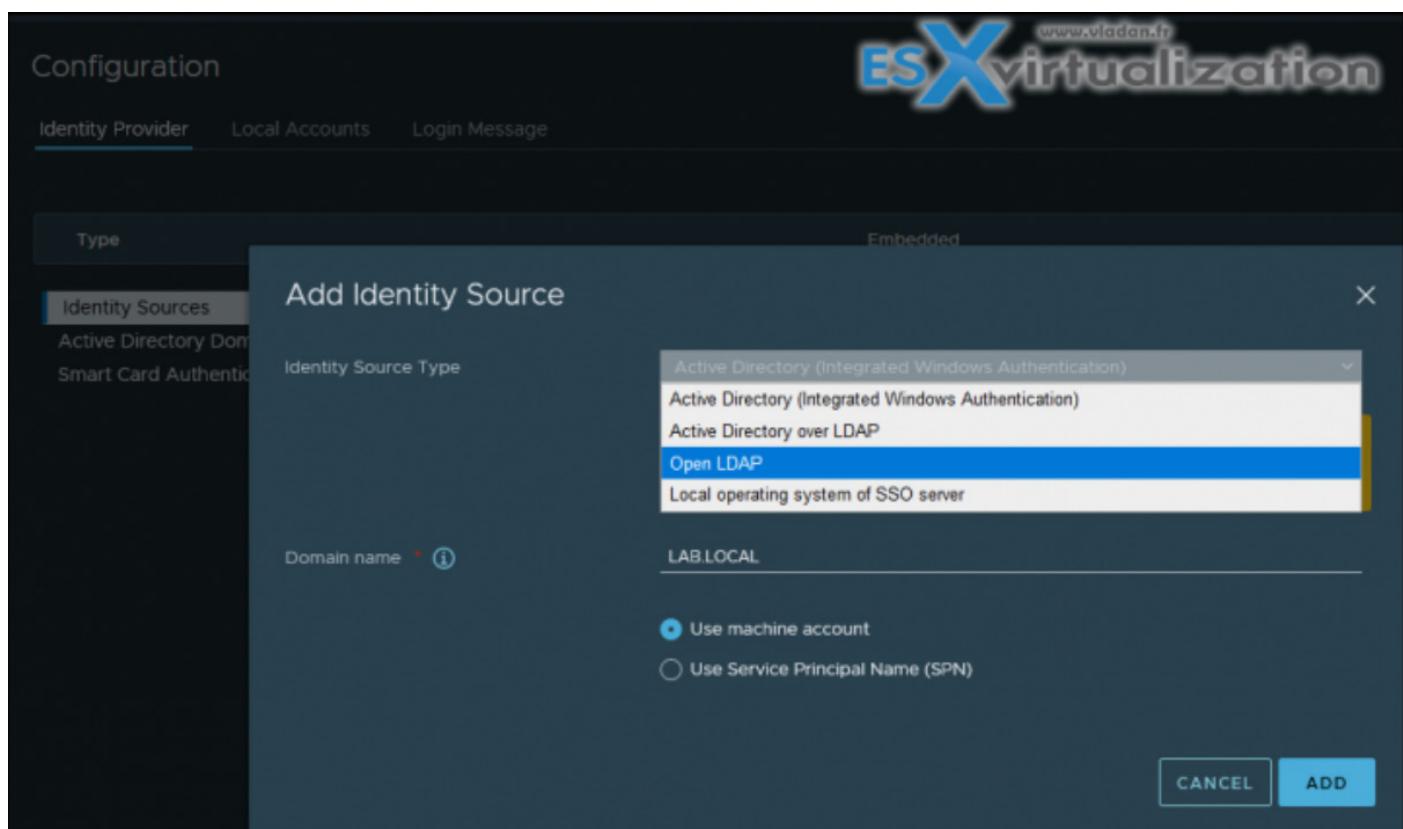
Currently, vCenter Single Sign-On supports the use of OpenLDAP as an identity source only if it satisfies all of these requirements:

- OpenLDAP versions 2.4 and later
- The OpenLDAP schema is RFC4519 compliant.

- All users have an objectClass of inetOrgPerson.
- All groups have an objectClass of groupOfUniqueNames.
- All groups have a group membership attribute of uniqueMember.
- All users and group objects have entryUUID configured (The objects have a unique GUID and should not be changing)

Also note that:

Starting from vSphere 7.0 Update 2, you can enable FIPS on vCenter Server. See the *vSphere Security* documentation. AD over LDAP and IWA are not supported when FIPS is enabled. Use external identity provider federation when in FIPS mode.



Important note:

A future update to Microsoft Windows will change the default behavior of Active Directory to require strong authentication and encryption. This change will impact how vCenter Server authenticates to Active Directory. If you use Active Directory as your identity source for vCenter Server, you must plan to enable LDAPS.

## Objective 4.3.3 Configure Active Directory integration

VMware vSphere 7 and VCSA allow to configure Active Directory (AD) integration. You can join the Microsoft AD vCenter server appliance (VCSA) and your ESXi hosts. In this section, we'll learn how it is done and go over its main advantages.

To access vCenter Server, users must log in using SSO domain user accounts or user accounts from identity sources registered in SSO. After a fresh deployment of VCSA you only have the local OS identity source available. If you want to add an external Identity source you have to configure it.

The default SSO domain name is vSphere.local, which is the only one predefined. However, it's not hard coded like in 5.5, so during the initial installation you can use a different name instead.

vSphere 7 supports different types of identity sources.

- **Microsoft AD over LDAP** — SSO supports multiple AD over LDAP identity sources
- **AD over LDAPS** — secure connection by using SSL to the LDAP (LDAP secure)
- **Microsoft IWA (Integrated Windows Authentication)** – You're allowed to specify a single AD as an identity source. This option allows users to log in to the vCenter Server using your AD accounts.
- **Open LDAP** — vCenter SSO supports Open LDAP 2.4 and later; multiple Open LDAP identity sources are supported.

Before you can add an integrated Active Directory identity source, you need to ensure that the server where SSO is installed is in the domain. If not, you'll not be able to add an AD. To do so, simply go to **Administration > system configuration > nodes**. Then select the node > **Manage tab > select Active directory > Join**.

After that, you can add your AD as an identity source. To do so, just go to **Shortcuts > Administration**.

Click the **Single Sign-On** section and **Configuration**. On the **Identity provider tab**, click **Active Directory Domain > Join AD**.

You'll need to enter:

**Domain name** - FQDN

**Use Machine account** - the easier option. Select this to use the local machine account as the server principal name. However, if you're planning to rename your VCSA, don't use this option.

**Use Service Principal Name (SPN)** - use this if you prefer to specify a unique SPN instead of using the machine name. You must also provide an SPN name and password.

The screenshot shows the vSphere Client Configuration interface. On the left, a sidebar lists various management categories like Administration, Access Control, Licensing, Solutions, Deployment, Support, Certificates, Single Sign On, and Configuration. The Configuration tab is selected. In the main area, the Identity Provider tab is active. Under 'Identity Sources', 'Active Directory Domain' is selected. Below this, there are buttons for 'JOIN AD' and 'LEAVE AD'. To the right, a panel titled 'Node' shows a single entry: 'vcsaphoton.lab.local' with 'Active Directory' set to 'LAB.LOCAL' and 'Organization Unit' set to 'CN=Computers,DC=lab,DC=local'.

You'll need to reboot your VCSA. You can configure a default domain for SSO. The default SSO domain allows users to authenticate without identifying a domain name. Users from other identity sources must identify the domain name during authentication.

The screenshot shows the Configuration screen with the Identity Provider tab selected. The top toolbar has buttons for ADD, EDIT, SET AS DEFAULT, and REMOVE. The table below lists identity sources: 'Active Directory Domain' (selected), 'Smart Card Authentication', and 'lab.local' (highlighted with a blue border). The 'lab.local' row shows 'Name: lab.local', 'Server URL: ...', 'Type: Active Directory (Integrated Windows Authentication)', 'Domain: lab.local', and 'Alias: lab.local'.

You can also add an LDAP authentication source. In order to use OpenLDAP for authentication, you'll need one or more LDAP authentication sources to be added to the vCenter server. There are quite a few requirements, such as that the OpenLDAP schema must be RFC 4519 compliant. All users must have the object class `inetOrgPerson`, or all groups must have the object class `groupOfUniqueNames`.

You can use the `sso-config` utility to add or remove an identity source.

- Use SSH or another remote console connection to start a session on the vCenter Server system.
- Log in as root.
- Change to the directory where the `sso-config` utility is located.

```
cd /opt/vmware/bin
```

- Refer to the sso-config help by running sso-config.sh -help, or see the VMware knowledge base article at <https://kb.vmware.com/s/article/67304> for usage examples.

## Objective 4.4 Deploy And Configure vCenter Server 7 Appliance

### System Requirements for VCSA deployments

The VMware vCenter Server appliance can be deployed on ESXi 6.5 hosts or later, or on vCenter Server instances 6.5 or later.

There is a single ISO file which you'll download from MyVMware. (you can use the 60-day trial for learning, you just need to give your email to VMware).

This single ISO has everything you need to **Install, Upgrade, Migrate or Restore**.

The installation order is as follows:

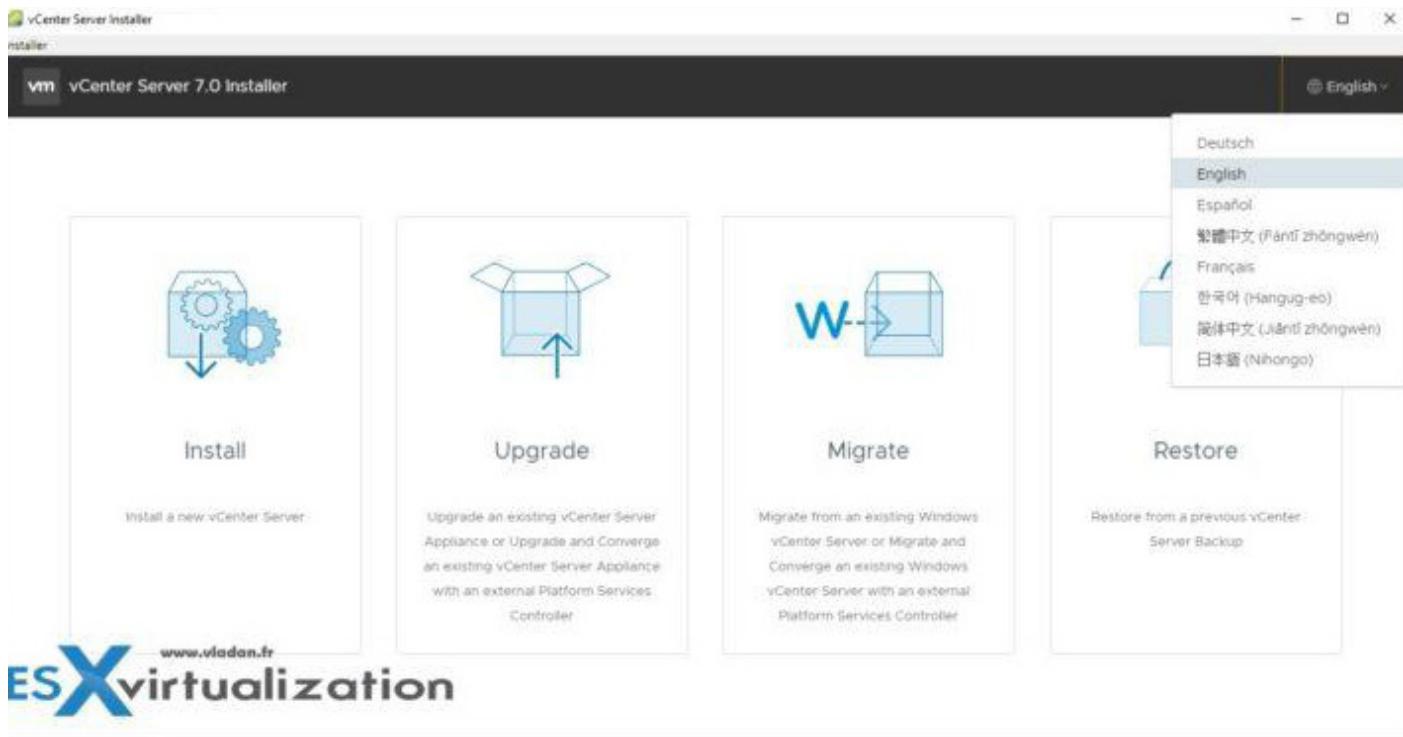
Install ESXi on at least one host, then setup ESXi, deploy vCenter Server Appliance (VCSA). Login to vSphere client to create and organize your vCenter server inventory.

In order to start the installer that is located within the file structure of the ISO, just mount the ISO.

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

- lin64
- mac
- win32

Since we are on a Windows workstation, let's execute the one from win32. We are presented with the four options. Click the first one – Install, and let's follow the necessary steps.



As you can see, there are different languages available for installation.

The GUI deployment is a two-stage process. The first stage is the deployment wizard that deploys the OVA file of the appliance on the target ESXi host or the vCenter Server instance.

After the OVA deployment is over, you are redirected to the second stage of the process that sets up and starts the services of the newly deployed appliance.

The CLI deployment method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that automatically deploys and sets up the appliance. The CLI deployment automatically runs both stage 1 then stage 2, with no user interaction required.

Before we get started, we need to create forward and reverse DNS records on our DNS server. The authentication services contain vCenter Single Sign-On, License service, Lookup Service, and VMware Certificate Authority.

The vCenter Server group of services contains vCenter Server, vSphere Client, vSphere Auto Deploy and vSphere ESXi Dump Collector. The vCenter Server appliance also contains the VMware vSphere Lifecycle Manager Extension service and the VMware vCenter Lifecycle Manager.

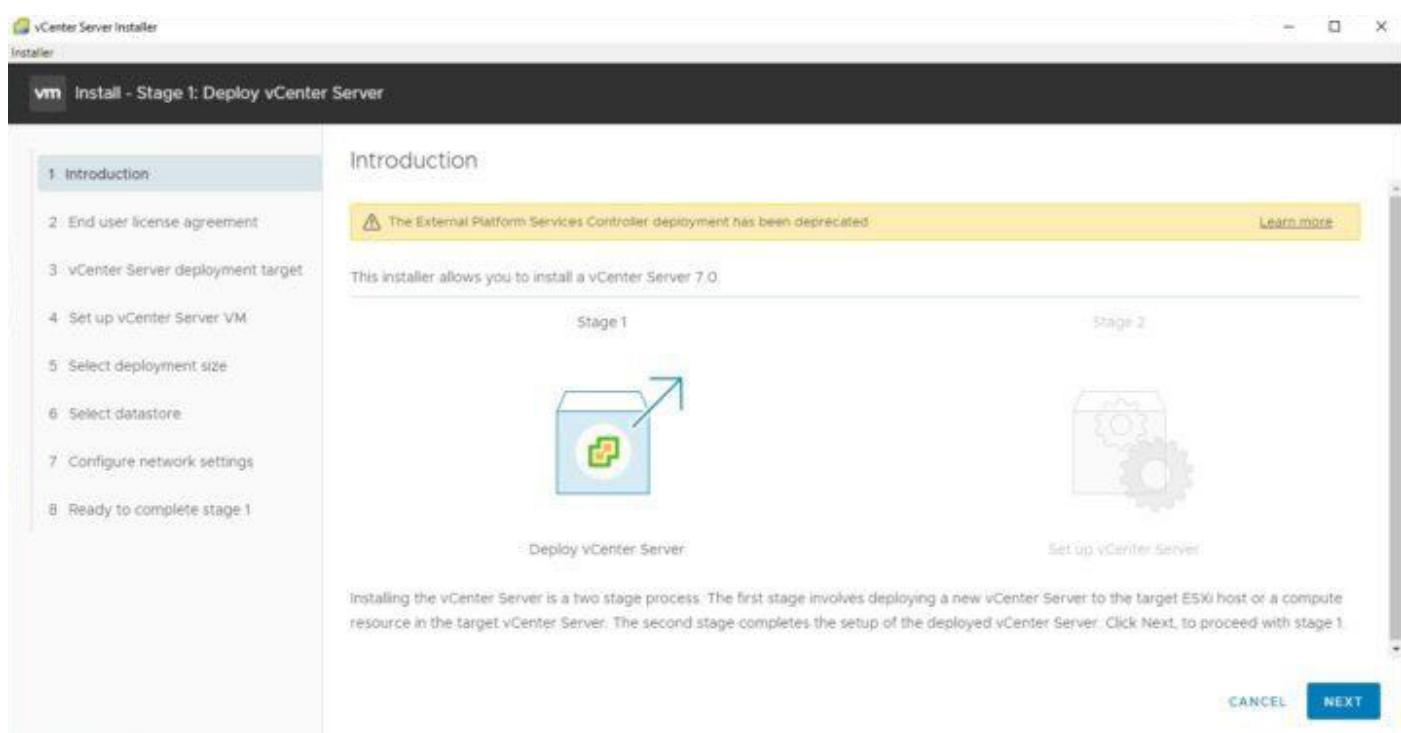
Version 7.0 of vCenter Server is deployed with virtual hardware version 10, which supports 64 virtual CPUs per virtual machine in ESXi.

## Where is the Platform Service Controller (PSC)?

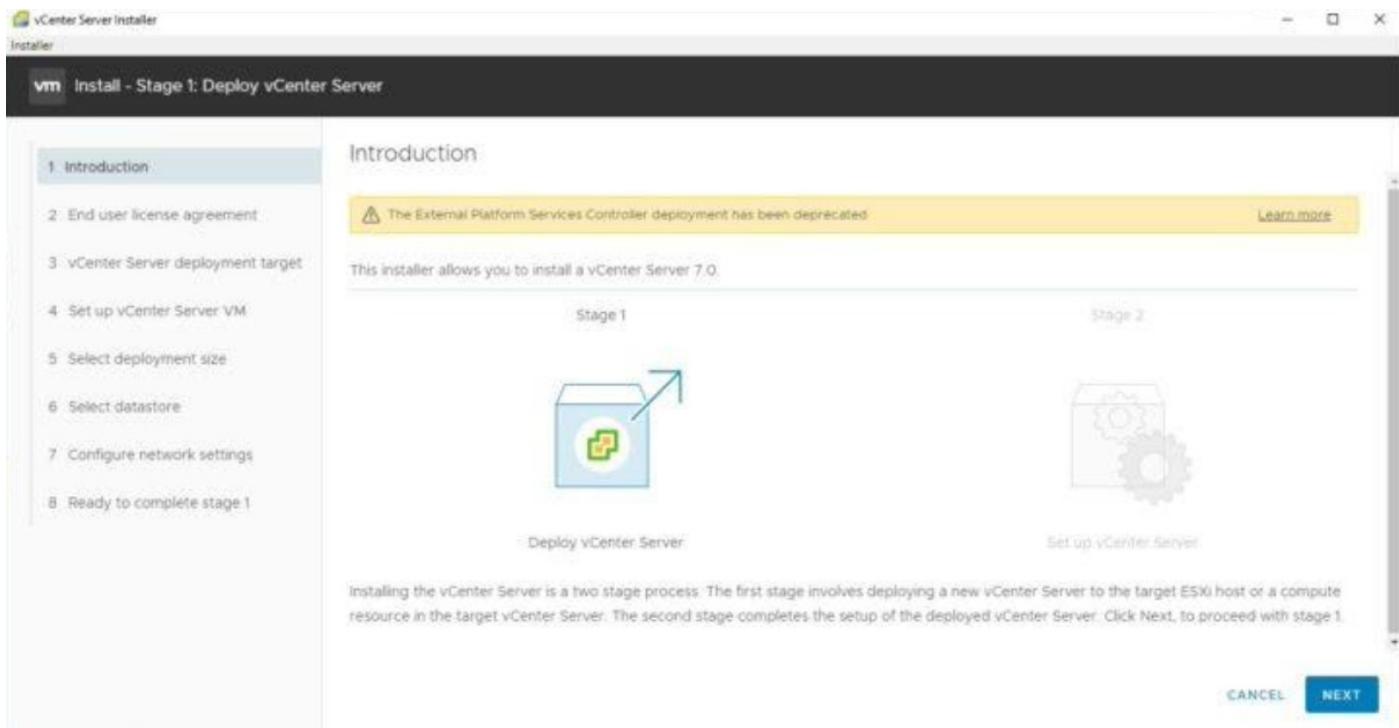
No more external PSC. vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary (or possible) to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into the vCenter Server.

## Which services are installed with vCenter server?

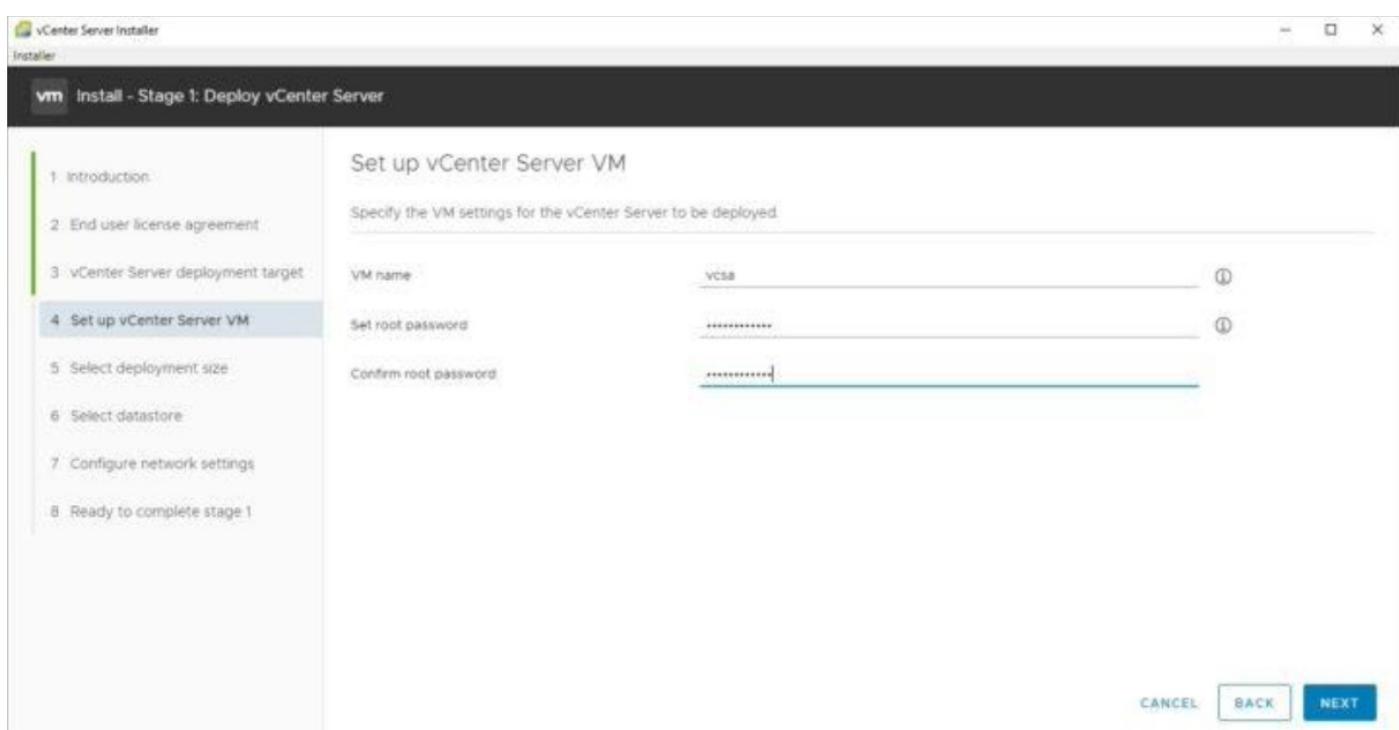
- **PostgreSQL** - a DB bundled and preinstalled. It is a VMware distribution of the PostgreSQL database for vSphere and vCloud Hybrid Services.
- **vSphere Client** - HTML 5 UI which can be accessed through a web browser. No more Macromedia/Adobe Flash.
- **ESXi Dump Collector** - The vCenter Server support tool. You can configure ESXi to save the VMkernel memory to a network server, rather than to a disk, when the system encounters a critical failure. The vSphere ESXi Dump Collector collects such memory dumps over the network.
- **vSphere Auto Deploy** - Allows deployment of stateless hosts. You can specify the image to deploy and the hosts to provision with the image. Optionally, you can specify host profiles to apply to the hosts and a vCenter Server location (folder or cluster) for each host.
- **vSphere LifeCycle Manager Extension** - New in vSphere 7. enables centralized, automated patch and version management for VMware vSphere and offers support for VMware ESXi hosts, virtual machines and virtual appliances.
- **vCenter Lifecycle Manager** - vCenter Lifecycle Manager automatically places servers based on their location, organization, environment, service level, or performance levels.



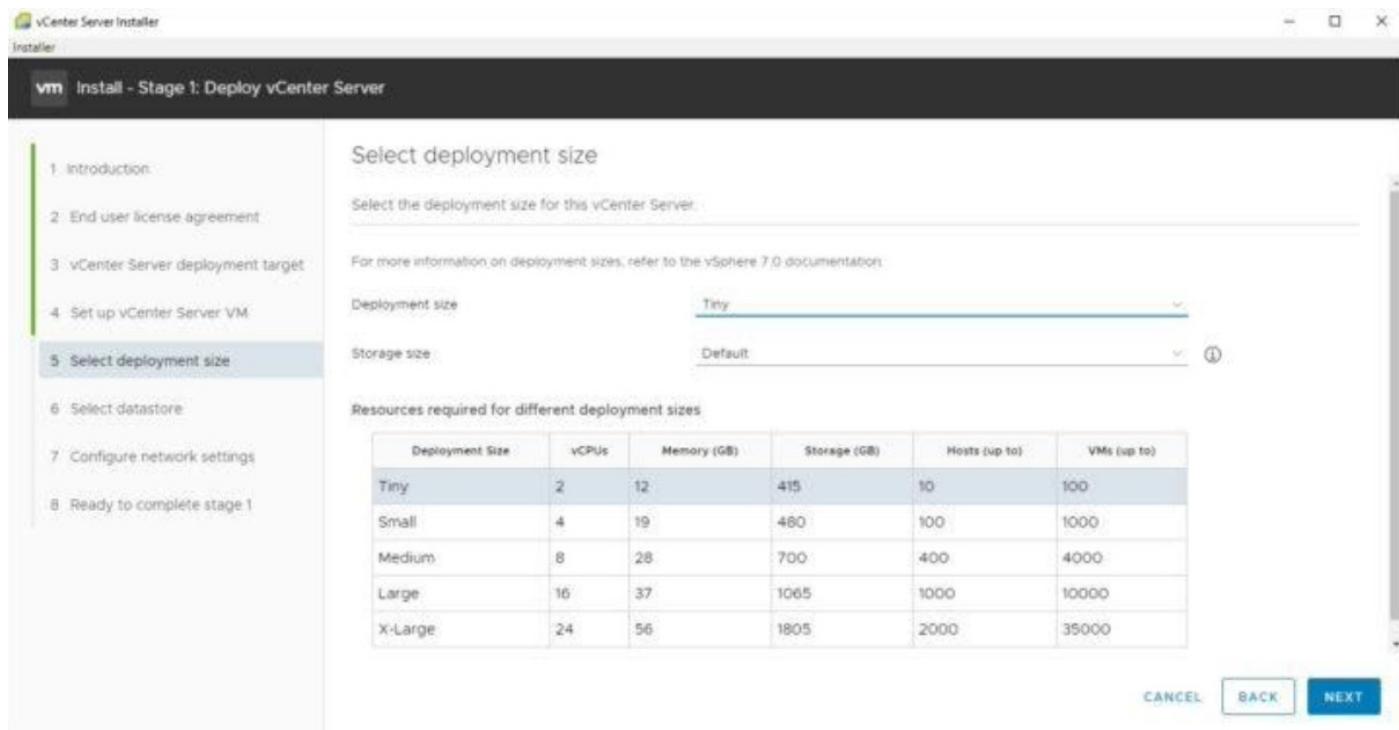
then



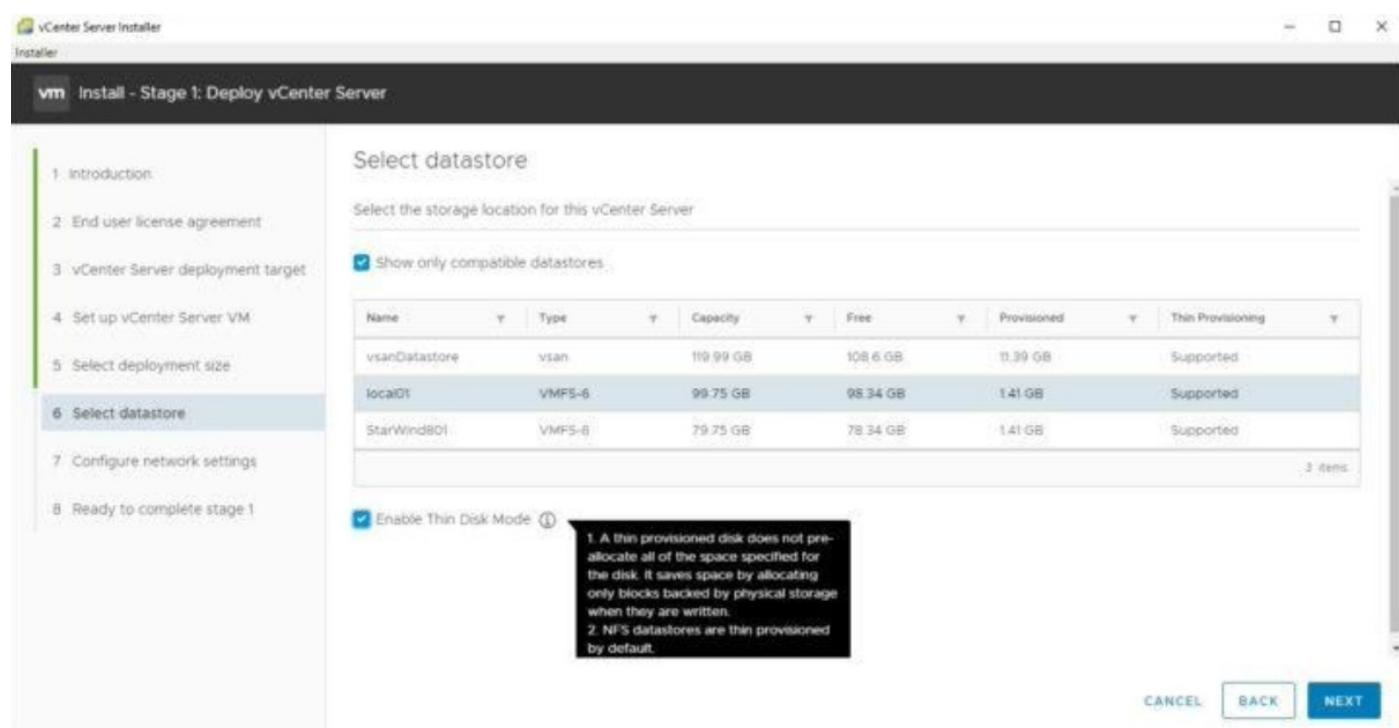
then



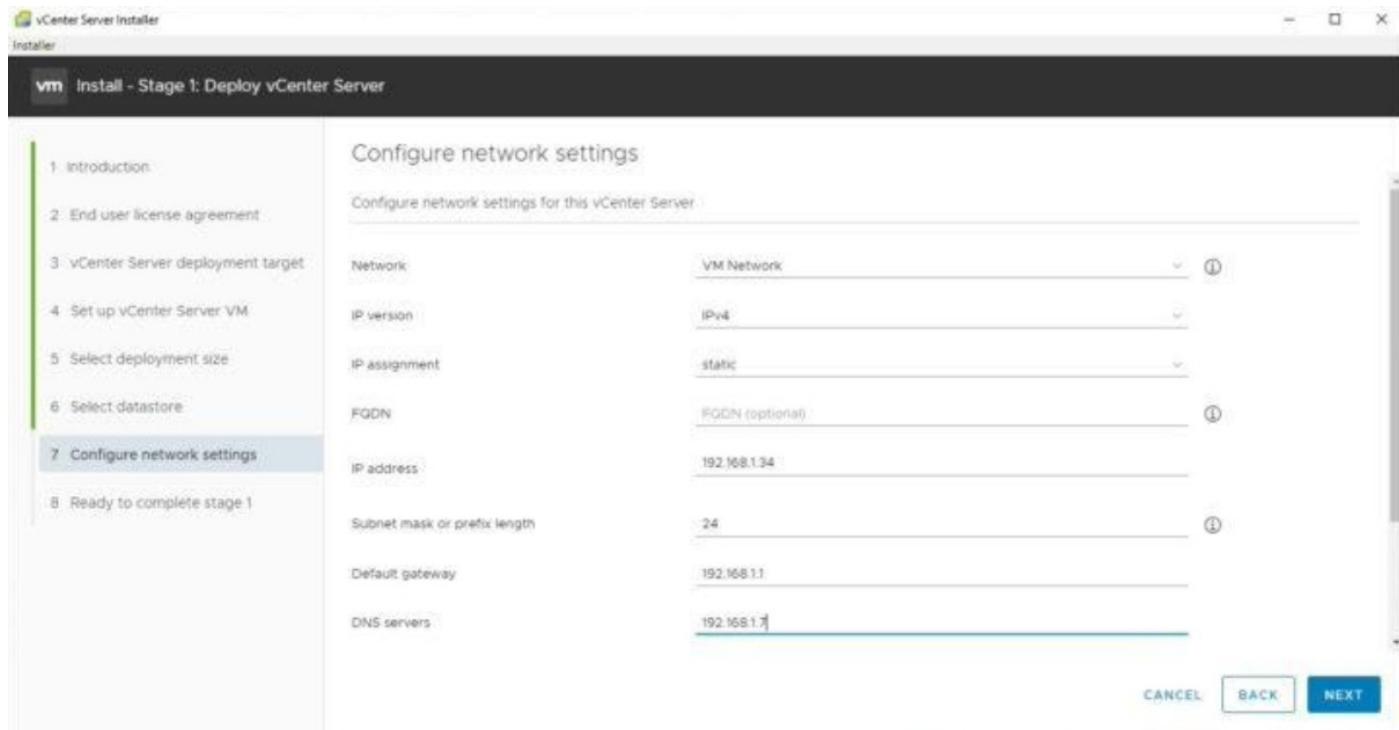
then



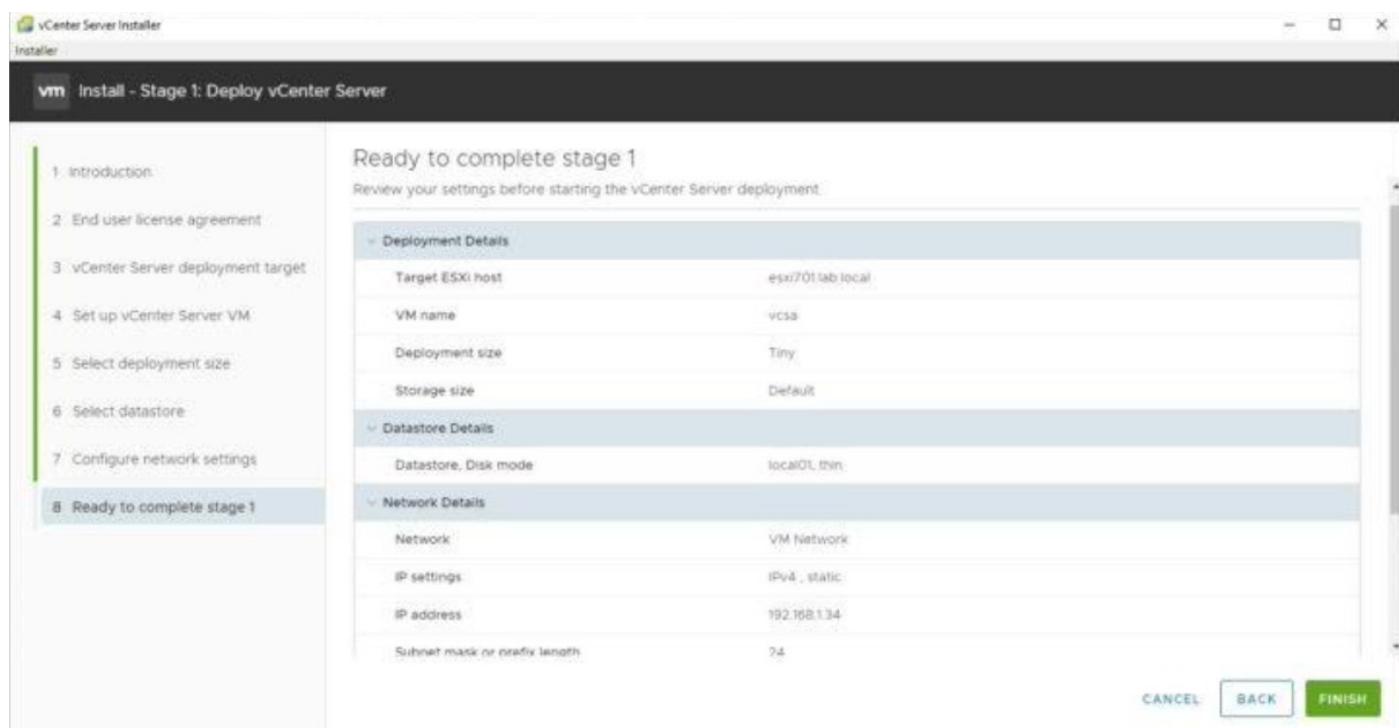
then



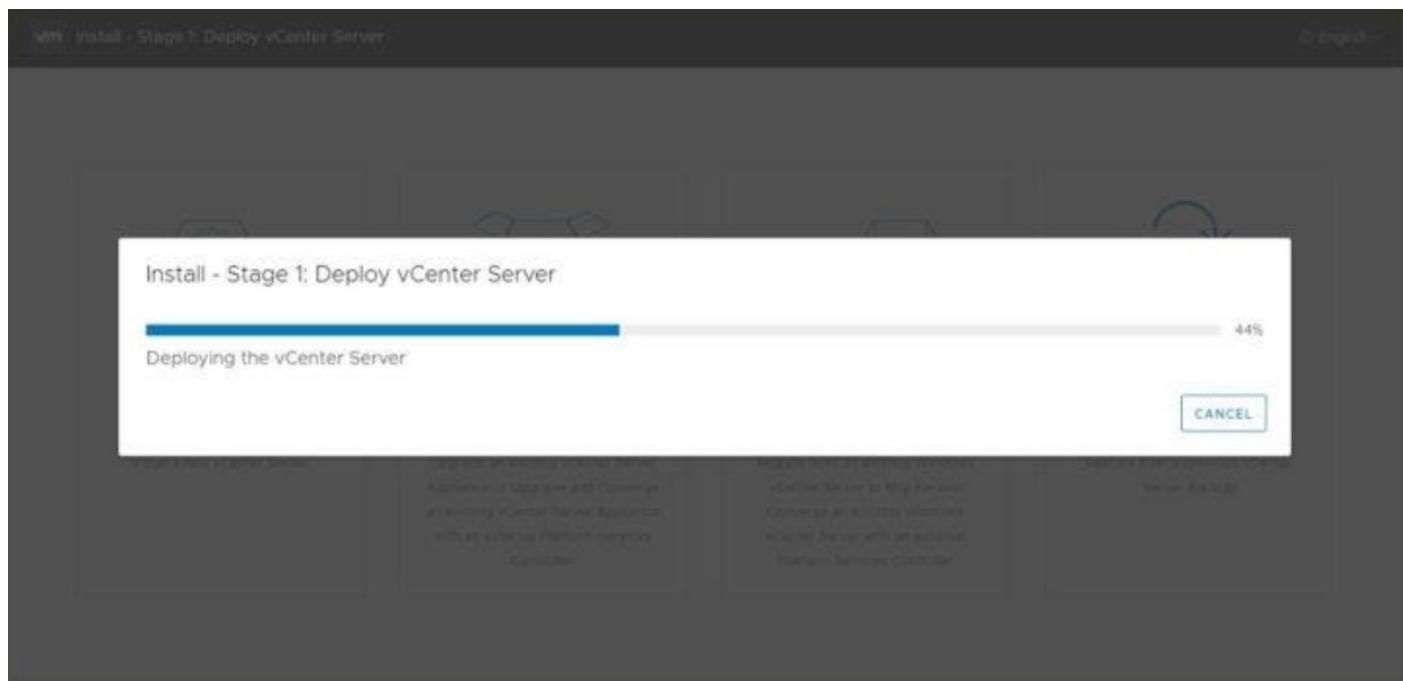
then



then



And you'll see the progress screen which indicates the Part 1 (deployment) progress.



This part takes some time to finish.

When you deploy a vCenter Server appliance, 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.

You can give your domain a unique name. To prevent authentication conflicts, use a name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

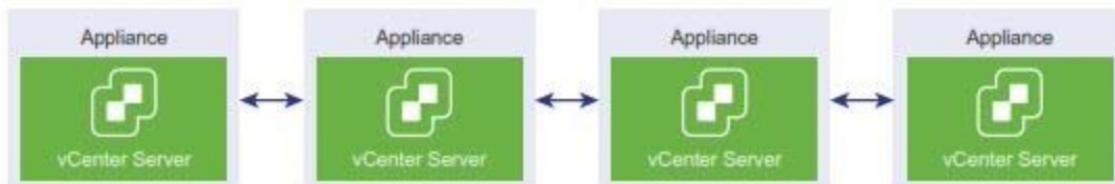
### vCenter Enhanced Linked Mode

vCenter Enhanced Linked Mode allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group.

You can join up to 15 vCenter Server appliance deployments with the vCenter Enhanced Linked Mode in a single vSphere Single Sign-On domain. You can create a vCenter Enhanced Linked Mode group during the deployment of the vCenter Server appliance.

You can also join a vCenter Enhanced Linked Mode group by moving, or repointing, a vCenter Server from one vSphere domain to another existing domain.

**Figure 1-2. Enhanced Linked Mode for vCenter Server Appliance Deployments**



## The Part 2 - configuration

### Install - Stage 1: Deploy vCenter Server

i You have successfully deployed the vCenter Server.

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

If you exit, you can continue with the vCenter Server setup at any time by logging in to the vCenter Server Management interface <https://192.168.1.34:5480/>

CANCEL CLOSE CONTINUE

Click Continue to start.

**Install - Stage 2: Set Up vCenter Server**

1 Introduction
Introduction

2 vCenter Server configuration
vCenter Server installation overview

3 SSO configuration
Stage 1
Stage 2

4 Configure CEIP

5 Ready to complete

Deploy new vCenter Server

Set up vCenter Server

Installing the vCenter Server is a two stage process. The first stage has been completed.  
Click Next, to proceed with Stage 2, setting up the vCenter Server.

CANCEL NEXT

Then

**Install - Stage 2: Set Up vCenter Server**

1 Introduction
vCenter Server configuration

2 vCenter Server configuration
Time synchronization mode
Synchronize time with the ESXi ho ▾

3 SSO configuration
SSH access
Disabled ▾

4 Configure CEIP

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

CANCEL
BACK
NEXT

Then

Install - Stage 2: Set Up vCenter Server

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

**SSO configuration**

Create a new SSO domain

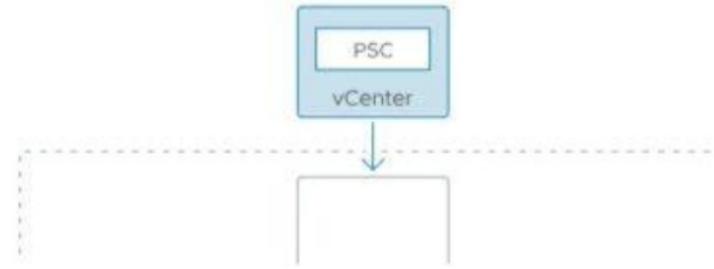
Single Sign-On domain name: vladan.lab (i)

Single Sign-On user name: administrator (i)

Single Sign-On password: (i)

Confirm password: (i)

Join an existing SSO domain



**CANCEL** **BACK** **NEXT**

Next comes the CEIP. If you check the box, VMware is allowed to collect some technical information about the infrastructure. Which firmware/driver combination you have present (important for vSAN for example as the wrong combination can impact the performance and even lead to the purple screen of death – PSOD)

The config data such as settings of the cluster environment,

**vm Install - Stage 2: Set Up vCenter Server**

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

**Configure CEIP**

Join the VMware Customer Experience Improvement Program.

Participating in VMware's Customer Experience Improvement Program ("CEIP") enables VMware to provide you with a proactive, reliable, and consistent vSphere environment and experience. Examples of such enhancements can be seen in the following features:

- vSphere Health
- vSAN Online Health
- vCenter Server Update Planner
- vSAN Performance Analytics
- Host Hardware Compatibility
- vSAN Support Insight

CEIP collects configuration, feature usage, and performance information. No personally identifiable information is collected. All data is sanitized and obfuscated prior to being received by VMware.

For additional information on CEIP and the data collected, please see VMware's [Customer Experience Improvement Program \(CEIP\)](#).

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

CANCEL BACK NEXT

Then

**vm Install - Stage 2: Set Up vCenter Server**

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

**Ready to complete**

Review your settings before finishing the wizard.

**Network Details**

Network configuration	Assign static IP address
IP version	IPv4
Host name	vcsa.lab.local
IP Address	192.168.1.34
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS servers	192.168.1.7

**vCenter Server Details**

Time synchronization mode	Synchronize time with the ESXi host
SSH access	Disabled

**SSO Details**

Domain name	vladan.lab
User name	administrator

**Customer Experience Improvement Program**

CANCEL BACK FINISH

After that, just go for a coffee. It'll take at least 15 min to complete, configure, and start all the VCSA services. You won't be able to login before all these steps are completed.

## Objective 4.5 Create and configure VMware High Availability and advanced options (Admission control, proactive HA etc).

In this section, we'll discuss how to create and configure VMware vSphere 7 High Availability (HA) advanced options. Those options are useful when you need to provide specific networking due to local network requirements or whether you need to change some behaviour which is not usually common.

All these settings are accessible via vSphere 7 web client and vCenter server. The advanced settings are applied at the cluster level (not at the individual host level) and determine how the vSphere HA behaves and give you some fine-tuning options to make it fit your needs.

We'll look at specific scenarios, like how to change an alternative address for host isolation when no heartbeats are received from other hosts or how to change the default gateway IP address which is used for isolation tests. But before we jump into it, let's recap what VMware HA is capable of and which kind of failure protection it offers for vSphere environments.

### VMware vSphere 7 HA has four protection functions:

**Server failure** - restarts VMs on remaining hosts when one of the underlying hosts has a hardware problem or the network is isolated from the rest of the hosts in the cluster.

**Application failure** – monitors VMs via VMware tools. If failure is detected, it resets the VM. This proceeds until the system receives a response from VMware tools.

**Datastore access** - HA can also protect against **datastore accessibility failures** by restarting affected VMs on other hosts which can still access their shared datastores. Datastore heartbeats are used as a secondary channel, in addition to the network heartbeat. The system uses the storage network to determine if the host has been isolated or if it's a network partition.

**Network partition** - HA has also a fourth protection function and this is a **Network isolation**. In this case we have VMs on hosts which run on hosts, but are separated by network failure between hosts. If a host becomes isolated like this, on the management or vSAN network, VMs are restarted on other hosts which can still communicate with all the other hosts within the cluster.

## vSphere HA advanced Options

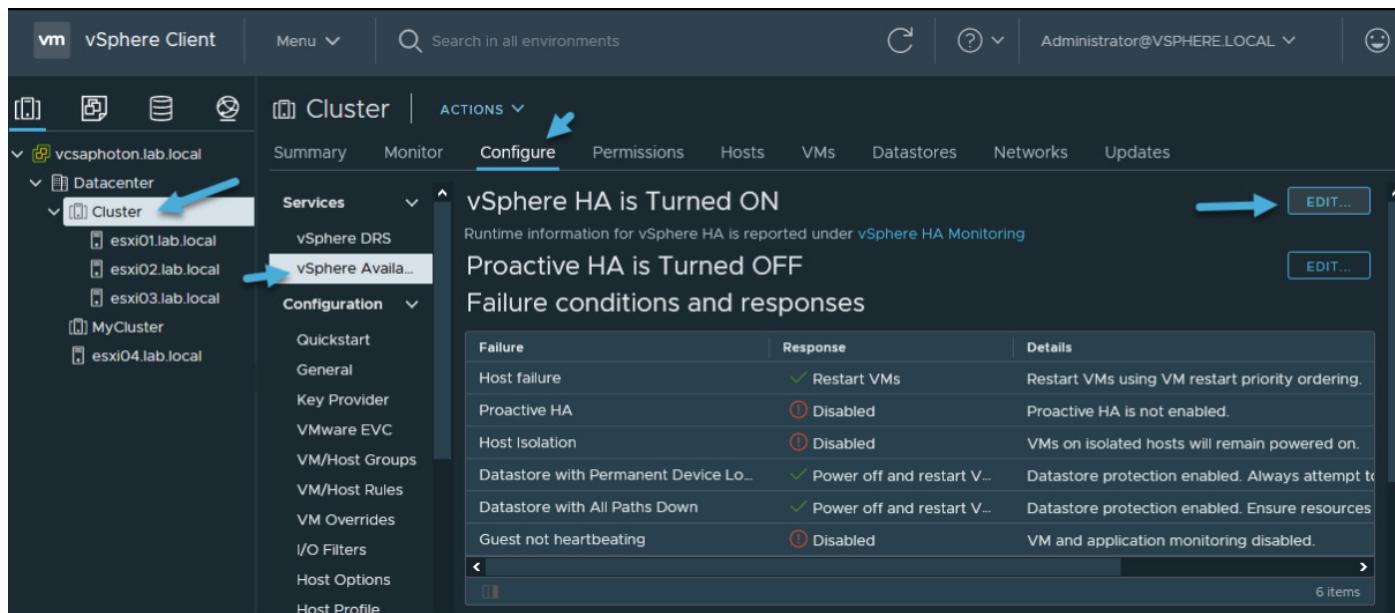
The use of multiple isolation response addresses offers VMware HA a potentially more accurate picture of the network connectivity of a host. There may be situations in which a single isolation address would indicate that a host is in a state of complete isolation from the network, but access to additional isolation addresses would show that only a partial network failure has occurred.

**das.isolationaddress** - the addresses used to test for host isolation when no heartbeats are received from other hosts in the cluster. If this option is not specified (which is the default setting), the management network default gateway is used to test for isolation.

You can use **das.isolationaddressX** where the X is a number between 0 and 9 for **testing multiple** addresses. Pretty neat.

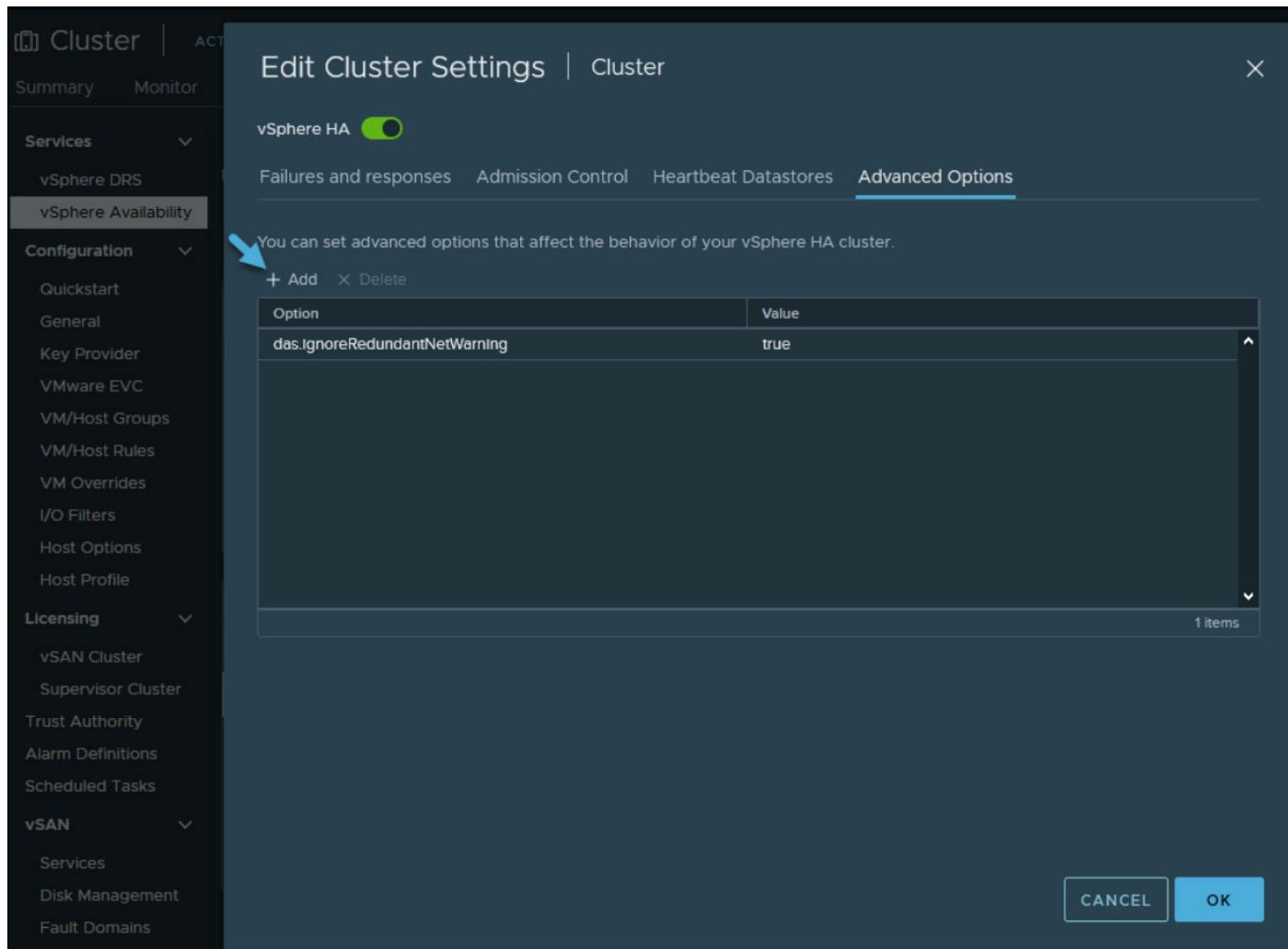
Where to change/add those vSphere 7 HA advanced Options?

In the vSphere Client, browse to **Select vSphere HA cluster** > Click the **Configure** tab > Select **vSphere Availability** and click **Edit button** on the right.



**vSphere 7 HA Advanced Options access via Web client at the cluster level**

Click Advanced Options.



### vSphere 7 HA Advanced Options

Click **Add** and type the name of the advanced option in the text box.

**Option:** *das.isolationaddress0*

**Value:** Type in a valid IP address other than the default gateway address

vSphere HA

Failures and responses   Admission Control   Heartbeat Datastores   Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

+ Add   X Delete

Option	Value
das.IgnoreRedundantNetWarning	true
das.IsolationAddress0	192.168.1.1
das.IsolationAddress1	192.168.10.1

### Different IP addresses to test host isolation

Some of those settings below are used only when you're using some specific HA policy. For example, some advanced settings won't be useful when using **Slot-based HA** policy or **Dedicated failover hosts**, but applies when used for **Cluster Resource Percentage** policy.

**das.usedefaultisolationaddress** - Specifies whether to use the default gateway IP address for isolation tests.

**das.isolationshutdowntimeout** - This type of advanced settings is used for scenarios where the host's isolation response is to shut down. You basically set the period of time that the VM is allowed to shut down before the system powers it off.

**das.slotmeminmb** - This setting specifies the maximum bound on the memory slot size for slot policy which calculates the slot size based on the maximum CPU/Memory reservation and overhead of all powered-on VMs.

**das.slotcpuinmhz** - This setting defines the maximum bound on the CPU slot size. The slot size is the smaller of this value or the maximum memory reservation plus memory overhead of any powered-on virtual machine in the cluster.

**das.vmmemoryminmb** - Defines the default memory resource value assigned to a virtual machine whose memory reservation is not specified or its value is zero.

**das.vmcpuminmhz** - The value is the default CPU resource value assigned to a VM whose CPU reservation is not specified or is zero. Usually used for the Host Failures Cluster. Tolerates admission control policy. If no value is set, the system uses the default of 32 MHz.

**das.respectvmvmantiaffinityrules** – Use this setting if you need to reinforce VM-VM anti-affinity rules for situations when DRS is not enabled.

**das.config.fdm.isolationPolicyDelaySec** - Specifies the number of seconds the system delays before executing the isolation policy after determining that a host is isolated. The minimum is 30. A lower value results in a 30-second delay.

**das.heartbeatdsperhost** – You can change the number of heartbeat datastores required per host. The default is 2. You are allowed to enter values between 2 and 5.

## Objective 4.6 Deploy and configure vCenter Server High Availability

vCenter Server availability (VCSAHA) was introduced in vSphere 6 and protects the vCenter Server appliance against host and hardware failures. It has active-passive architecture, in which a three-node cluster is configured with active, passive, and witness nodes. Note that vCenter HA can also be useful in that it reduces downtime when you patch your VCSA. Over time, the solution has been improved to provide very good protection for the vCenter Server.

During the configuration process, the first instance of VCSA will be used as an active node. This instance will be cloned twice, once to the Passive node and once to the Witness node.

We do not have to deal with external Platform Service Controller (PSC) VMs, as this architecture decision has been phased out in vSphere 7.

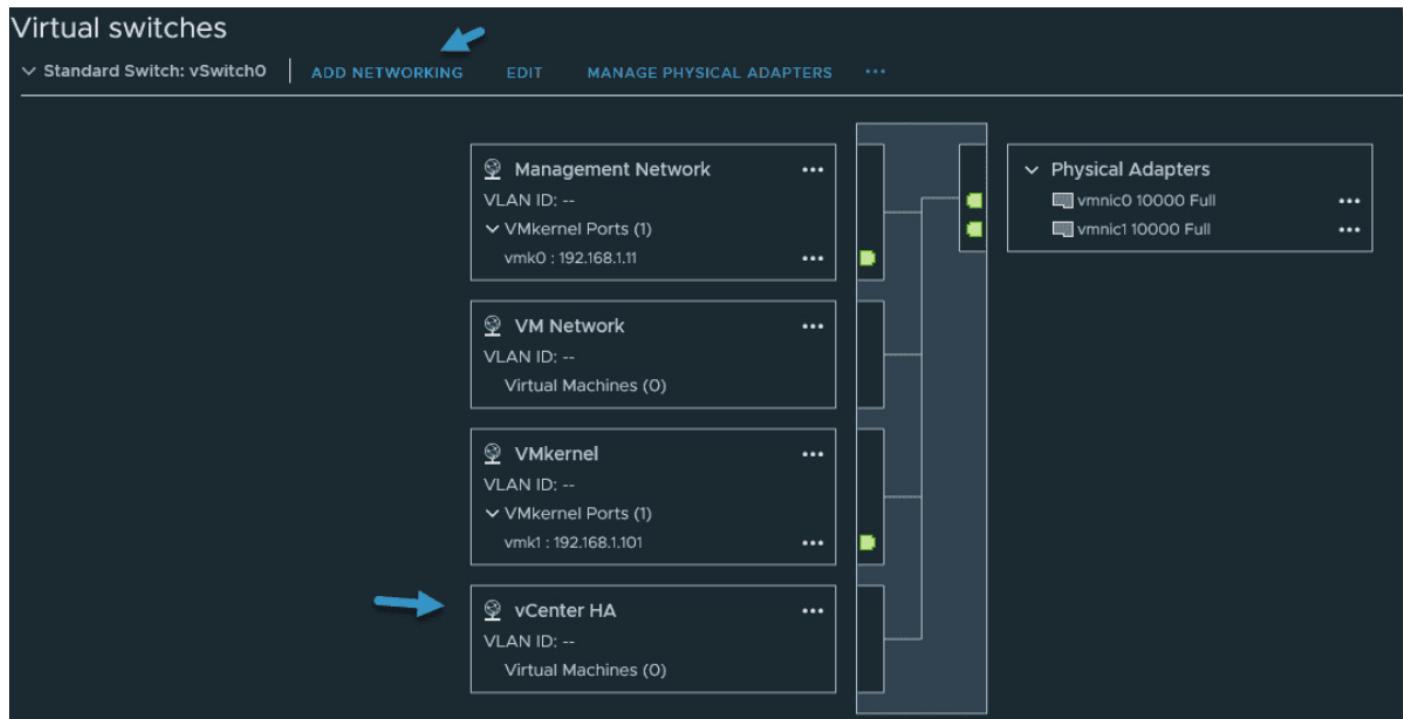
All three nodes, then, provide an additional layer of resiliency where each node is deployed on a different ESXi host. The three nodes communicate over a private network, called a vCenter HA network, which is set up as part of the configuration. The active node continuously replicates data to the passive node. The Witness is a lightweight clone of the Active node and provides a quorum to protect against a split-brain situation.

### VCSA HA Prerequisites

We need to first create a vCenter HA network. This network is separate from the management network. It is used for communication between the nodes to determine, in case of failure, which node has the latest data. For best performance, the network latency between the nodes should be less than or equal to 10 ms.

So, for each host of the cluster, add a separate port group for the vCenter HA network. The vCenter HA network must be on a different subnet than the management network. vCenter HA needs a single vCenter Server license; however, it needs to be a standard license, not an «Essentials» license that covers only three host installations.

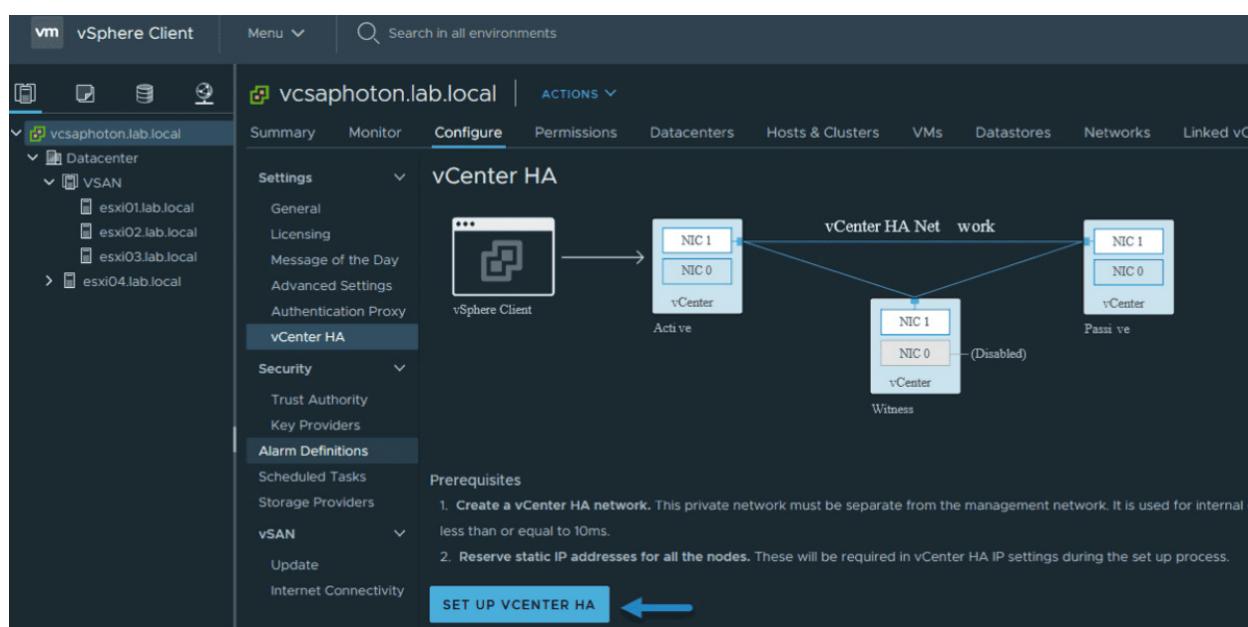
You need to enable SSH on the vCenter Server appliance. You can do that via the VAMI user interface by connecting directly to the appliance via [https://ip\\_of\\_vcsa:5480](https://ip_of_vcsa:5480) with root user and password. Then select **Access > SSH Login > Enable**, where you activate the SSH.



### Add a vCenter HA network

We should also reserve static IP addresses for all the nodes on our DNS server. These IP addresses will be required in vCenter HA IP settings during the setup process.

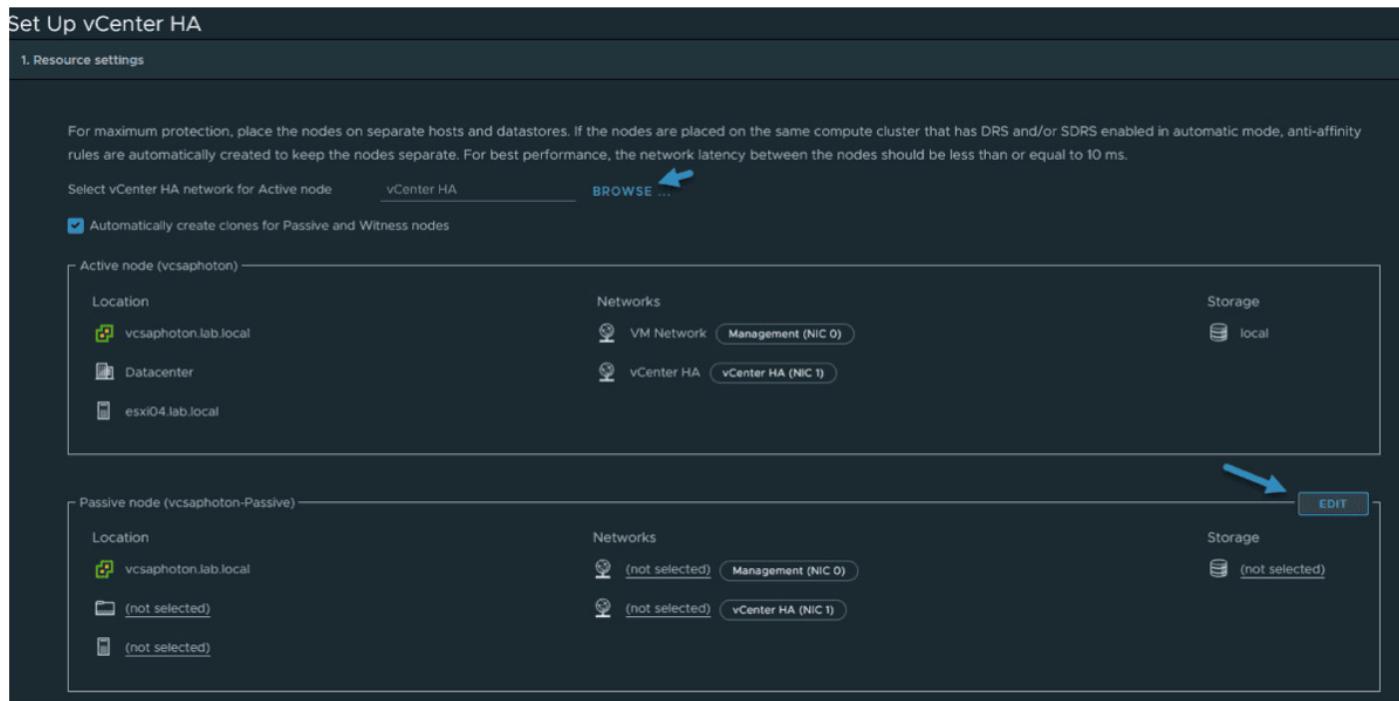
I assume that you've done this config on your DNS server.



### Start the vCenter HA configuration wizard

A new page will pop up that shows the resource settings. Here on each node, you'll have to click the **Edit** button to select the host, storage, network, etc.

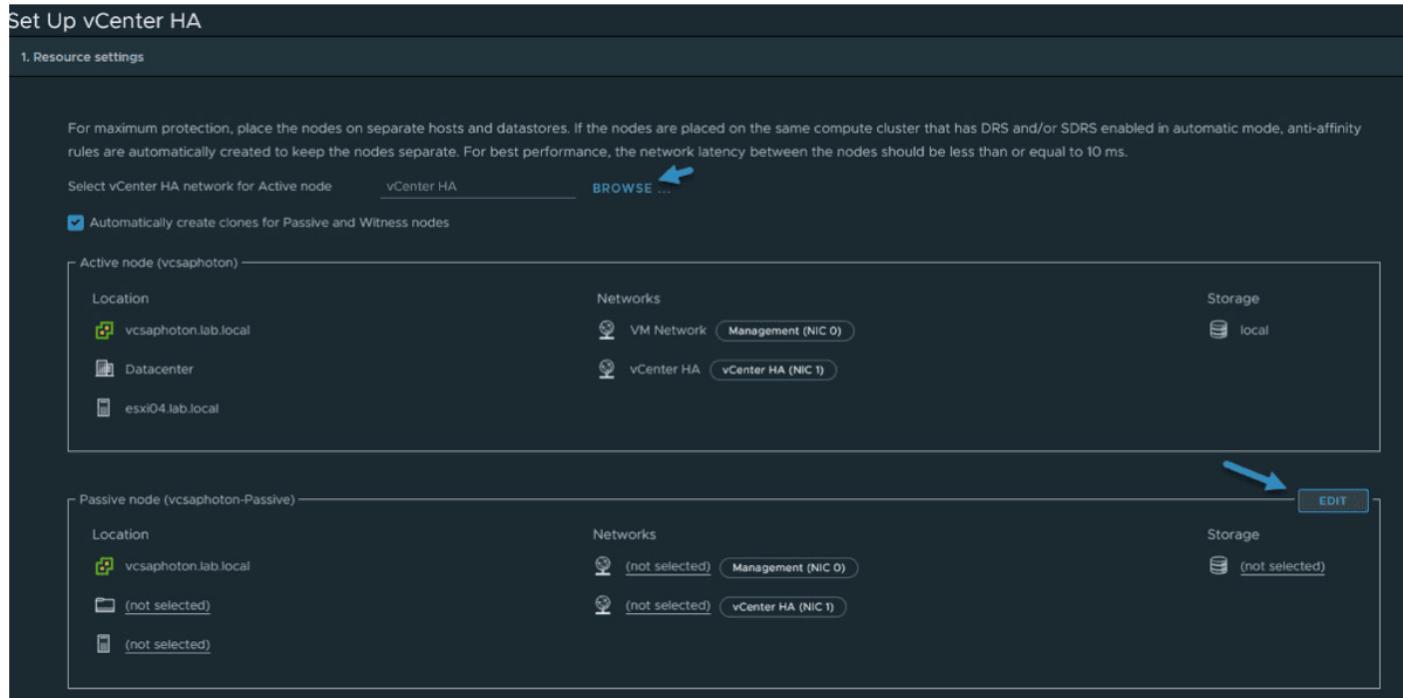
Note the check box «Automatically create clones for Passive and Witness nodes.»



### Set the HA network and the different resources

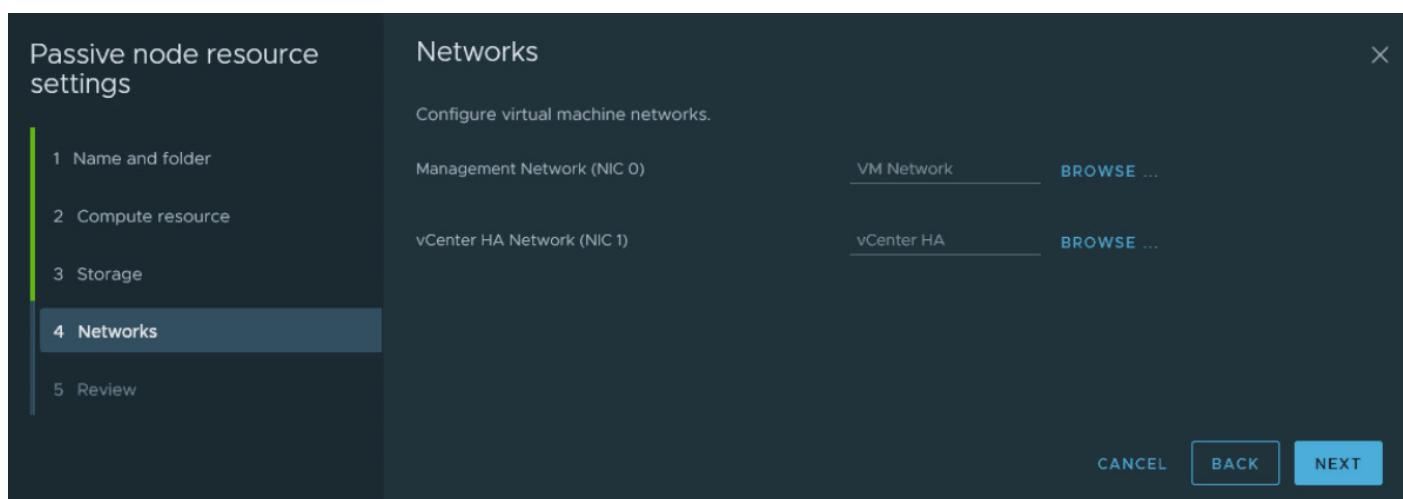
Then we must select the compute resources where the passive node will be running. When we say it's in passive node, it does not mean that the VM is powered off. It is a fully running VM, but it only receives a copy of the data from the active node.

In case of a failure, this node is «promoted» to active, and a new copy of the passive node is cloned again.



## Select compute resources

The networking for each node must be done separately for the passive and witness nodes.



## Select networking

Once all options are selected and you click the **Finish** button, the system will start the configuration. It will clone an active node and create passive and witness nodes. The process takes some time, depending on your underlying storage system.

### How can VCSA be patched when there is an HA configuration?

While it's possible to patch VCSA HA globally, you must put the VCSA HA cluster into maintenance mode and patch the witness node first. When done, patch the passive node.

After you've done this, initiate a failover manually. The passive node will become active and the current active node will become passive. Patch this passive node now. Exit maintenance mode and you're done.

While this is quite tedious, the other option is simply to destroy the HA configuration and delete the passive and witness nodes prior to patching. Once you have finished patching, simply recreate the VCSA HA.

The view on the cluster nodes looks like this. The **Edit**, **Initial Failover**, and **Remove vCenter HA** buttons are on the right.

Node	Status	vCenter HA IP address (NIC 1)	Management IP address (NIC 0)
Active	Up	192.168.2.32	192.168.1.32
Passive	Up	192.168.2.33	192.168.1.32
Witness	Up	192.168.2.34	

VCSA HA cluster nodes

## Objective 4.7 Setup a Content Library

vSphere Content Library was introduced into the VMware suite back in version 6.0. Since then, VMware has made some significant changes and enhancements to this feature. With the latest vSphere 7 version, the Content Library has matured further and now offers some new ways of working with your VMs, templates and external files, such as OVF or ISO files.

All these files can be shared within or outside of your organization. The access to content libraries can be password protected. The transfer service on the vCenter Server manages the import and export of content between the subscriber and the publisher libraries. It uses the HTTP NFC protocol.

When you enable the authentication for the Content Library, you basically set a password on the static username `vcsp`, which you cannot change. This user account, however, is not associated with vCenter Single Sign-On or Active Directory.

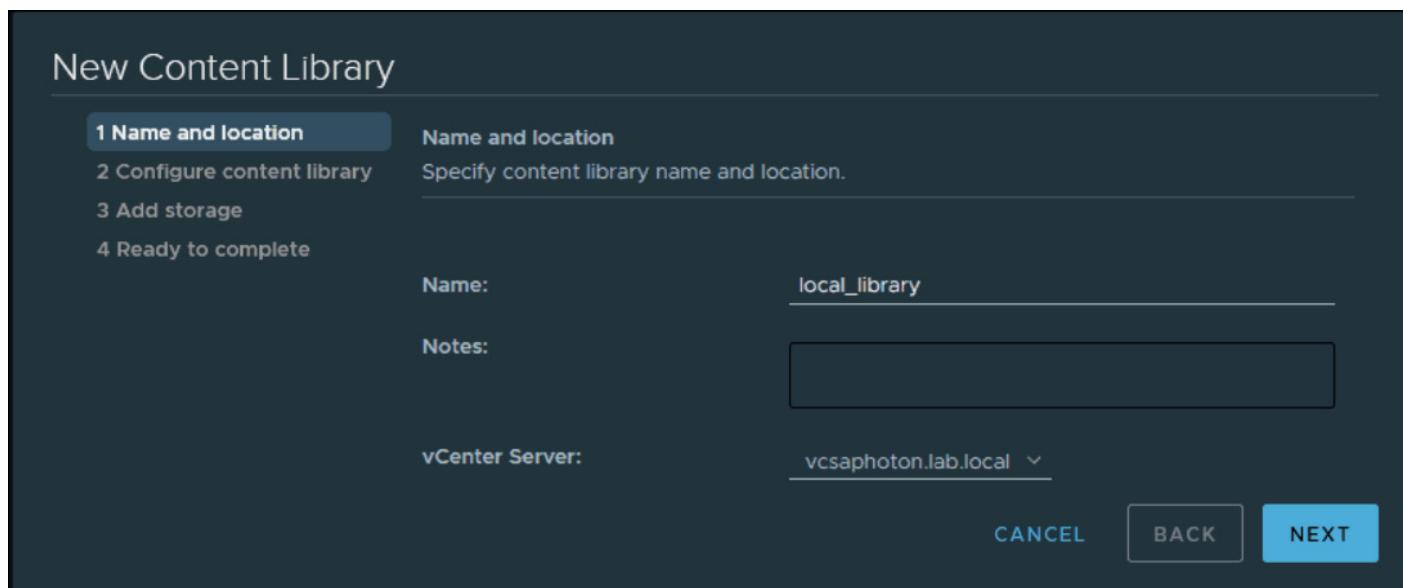
The idea is to have an efficient, centralized method to manage important data required in a vSphere environment. Note that it is possible to edit items only in a local library, no matter whether it is published or not. Library items in subscribed libraries cannot be modified.

The use of subscriptions allows content distribution between a publisher and a subscriber in some scenarios. We can consider the following:

- 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 a local or subscription Content Library in vSphere 7

Connect to your vSphere web client and select **Home > Shortcuts > Content Libraries**. Click **Create** to start the assistant.



## Create a local or subscription Content Library in vSphere 7

Give it a meaningful name and click **Next**. You'll have to choose whether you're creating a **local library** or a **Subscribed content library**. This is a library that is created in another datacenter or another vSphere environment. You'll need to know the exact address so you can connect to it.

## New Content Library

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

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

Local content library  
 Enable publishing  
 Enable authentication

Subscribed content library

Subscription URL

Enable authentication

Download content  immediately  when needed

CANCEL BACK NEXT

### Create a local Content Library in vSphere 7

The other option is the **Subscribed content library**. We'll show you what it looks like here. It's very important you do not select the «immediately» option because in this case, the system would start to download all the content from the remote library to your environment, and this is probably not what you want.

## New Content Library

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

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

Local content library  
 Enable publishing  
 Enable authentication

Subscribed content library

Subscription URL

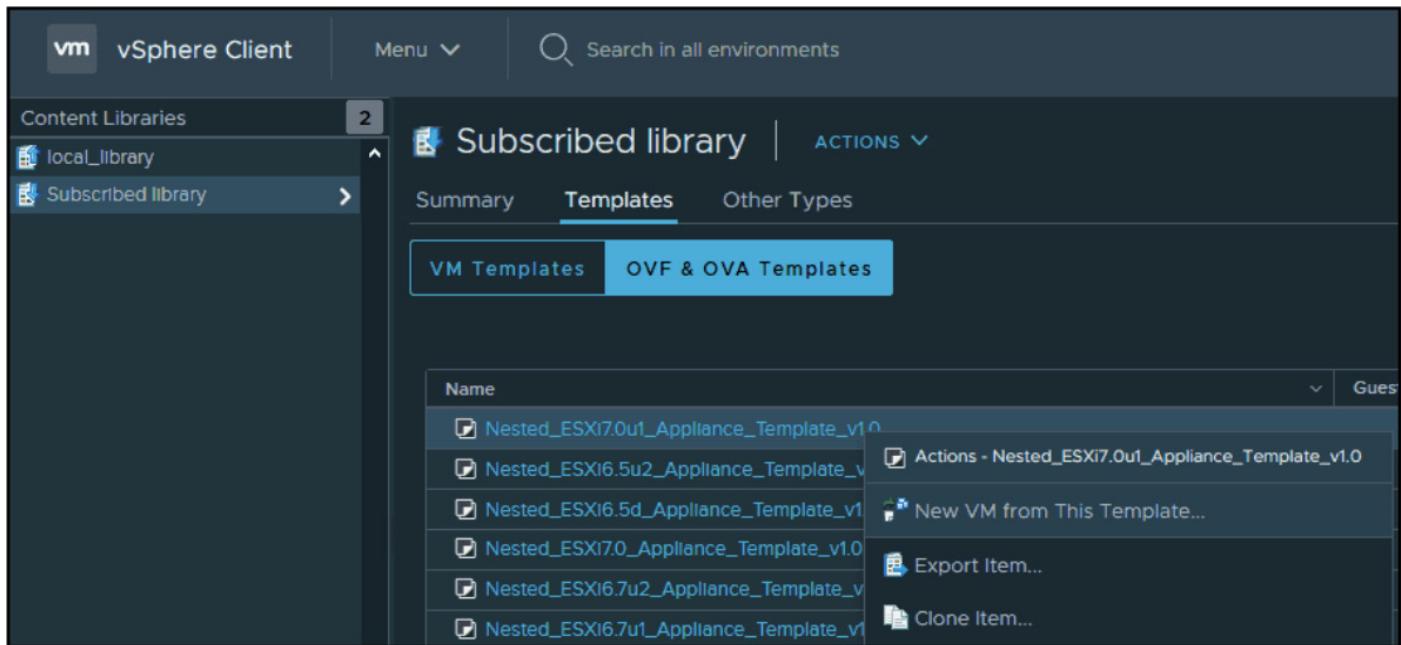
Enable authentication

Download content  immediately  when needed

CANCEL BACK NEXT

### Download content from a subscribed Content Library when needed

Once done, you can execute different actions on different objects. In our example, we can see that we have some OVA templates from which we can create a new VM or clone/export them.



### Possible actions on OVA objects in a Subscribed Content Library

When you create a local library within your vSphere environment, you basically create a space where you can store different kinds of files and enable certain new functionality that VMware calls Check-in/Check-out.

This functionality is active for VM templates in Content Libraries and can be edited with version control. You can check out a Virtual Machine from the template while you keep the template as is. You can then patch or edit the Virtual Machine. When you are ready, you can check it back in to update the VM template.

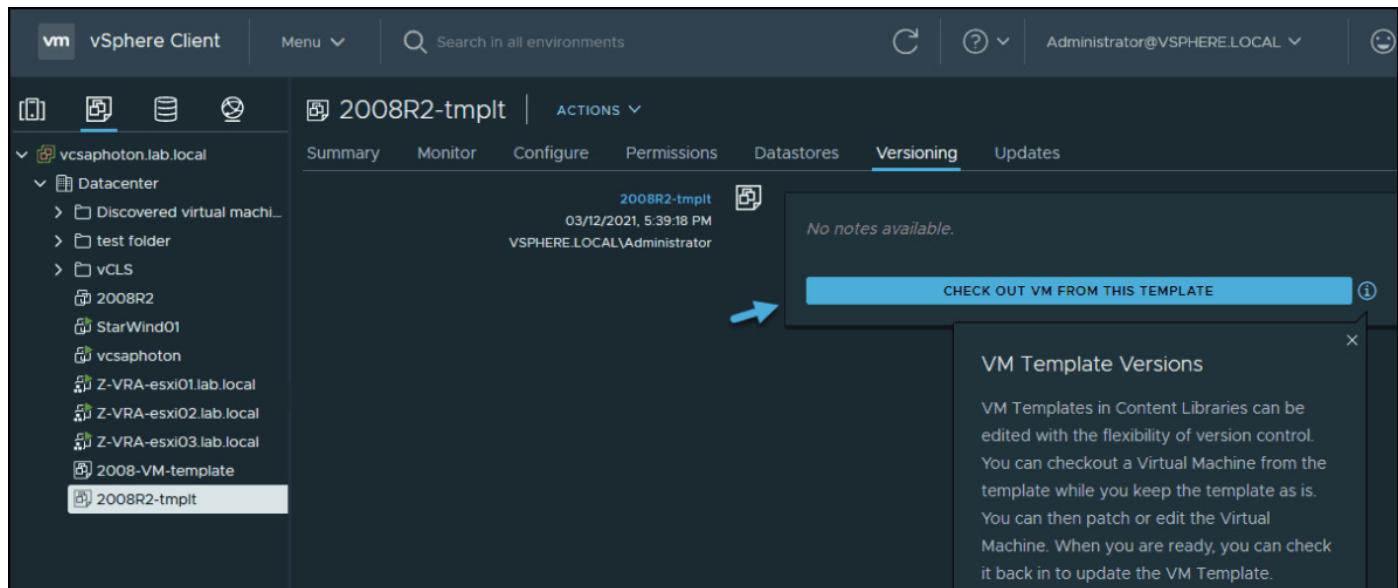
### What is Check-In/Check-Out?

Before vSphere 7, when an administrator needed to perform maintenance on a VM template (vmtx), the process consisted of multiple steps that had to be done manually. For example:

- Convert the VM template back to a VM.
- Snapshot the VM if rollback is needed.
- Update the guest OS or other VM object settings.
- Convert the VM back to a VM template.
- Copy the VM template back to a Content Library.
- Delete the old VM template(s) from the Content Library.

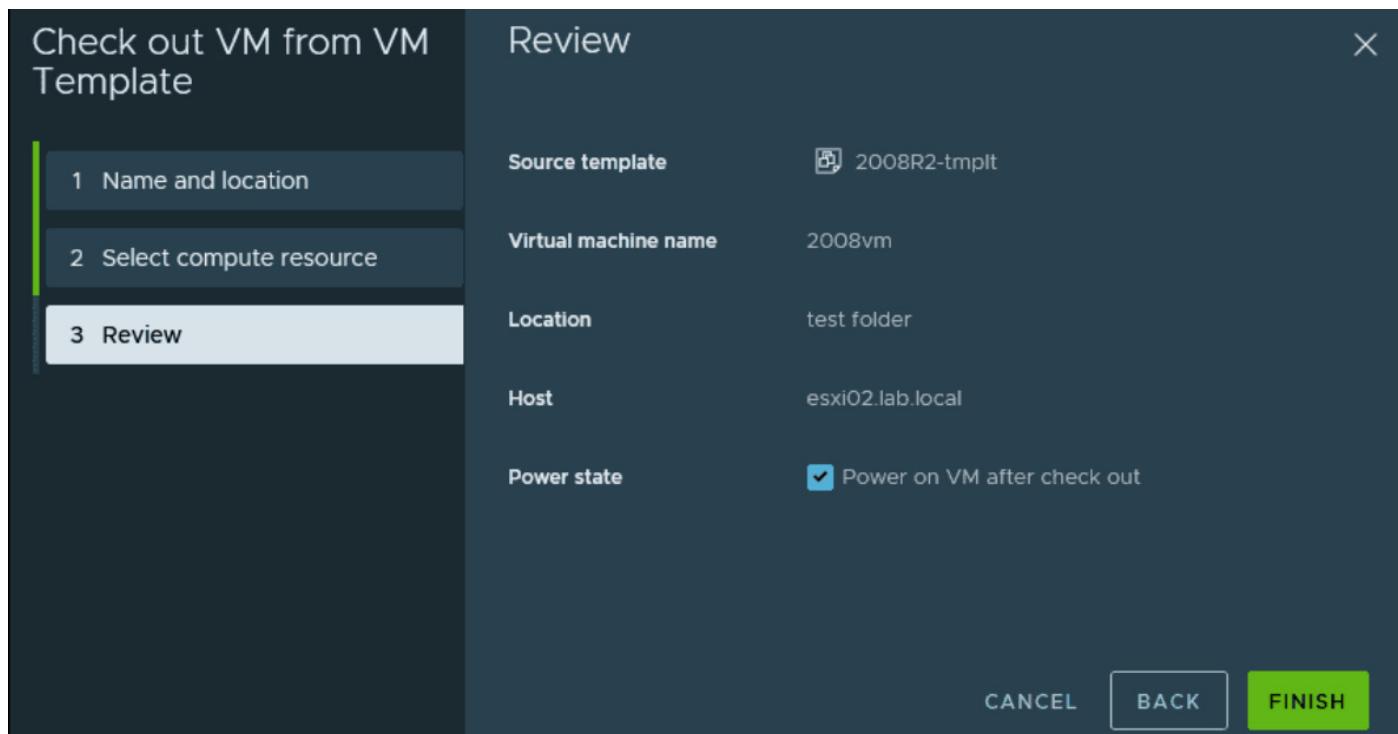
Now with the check-in/check-out function, you have versioning. You'll be able to check out the VM from this template for edits and then check in that template VM back to the Content Library to save the changes you made.

Simply select **the** template. Then go to the **Versioning** tab and click **Check out VM from this template**.



### Check out VM from this template

A new wizard will start. Follow the wizard and specify where you want to create and power on this VM.



Choose host and cluster and optionally also power on

Once you make at least one change, you'll be able to see the versioning. In our case, we edited the VM's virtual hardware and added some vCPU to test it. Be sure to add some notes so we know what we modified.

The VMTX templates will now be able to see different versions when you change the template. You may want to apply some patches to the VM or change add/remove some of the VM's virtual hardware.

## Content Library Roles

vCenter Server uses roles to protect certain areas of the infrastructure from unwanted access. When you work with a team of IT administrators, you can delegate certain roles to different team members.

The 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

## Advanced Content Library settings

The **Advanced settings** button next to **Create** on the Content Library page allows you to configure some advanced sync operations, set the auto sync refresh interval, or adjust some performance optimization settings.

Let's have a look. The auto sync, when enabled, allows you to automatically sync all items from the subscription library to your own local datacenter.

## Advanced Configuration

Auto-sync Frequency

Library Auto Sync Enabled (i)

Subscribed library automatic synchronization enabled status

true ▼

240 ▲ ▼

600 ▲ ▼

Library Auto Sync Setting Refresh Interval (seconds) (i) ⌚ Service restart required

20 ▲ ▼

7 ▲ ▼

Library Auto Sync Start Hour (i)

Library Auto Sync Stop Hour (i)

Performance Optimization

Library Maximum Concurrent Sync Items (i)

5 ▲ ▼

Max concurrent NFC transfers per ESX host (i)

8 ▲ ▼

Maximum Bandwidth Consumption (i)

0 ▲ ▼

Maximum Number of Concurrent Priority Transfers (i) ⌚ Service restart required

5 ▲ ▼

Maximum Number of Concurrent Transfers (i) ⌚ Service restart required

20 ▲ ▼

CANCEL SAVE

The screenshot shows the 'Advanced Configuration' screen for a Content Library. It's divided into two main sections: 'Auto-sync Frequency' and 'Performance Optimization'. In the 'Auto-sync Frequency' section, there's a tooltip for the 'Library Auto Sync Enabled' setting, which says 'Subscribed library automatic synchronization enabled status'. The 'Performance Optimization' section contains several numerical input fields with up/down arrows for adjusting values like concurrent sync items, NFC transfers, bandwidth consumption, and priority transfers. At the bottom right are 'CANCEL' and 'SAVE' buttons.

### Advanced configuration of Content Library

You can find other options by hovering a mouse over the information icon, as we won't be able to explain all settings in this section.

What's interesting with subscription libraries is that you can easily share your templates with a sister company and allow those two entities to put a common template together.

When relying on a high-speed fibre internet connection, you don't even need to keep all the templates locally and waste your storage space. Simply deploy a new VM from a subscribed Content Library and this template will be downloaded and transformed into a VM automatically.

## Objective 4.8 Configure vCenter Server file-based backup

When it comes to a vCenter Server Appliance (vCSA) backup, you have to make sure that the method is supported. As you know, VMware vCSA is a virtual appliance that can be backed up in two ways.

VMware vCSA holds a large amount of configuration information about your environment and has dependencies to other backup and monitoring products, with many third-party plugins installed. It is crucial to perform regular backups of vCSA and its configuration. The best practice is to separate the backup of the configuration from the backup of vCSA.

You can do an image-level backup or a file-level backup. However, there are other considerations. The image-level backup can be done via third-party backup software such as NAKIVO **as long as the vendor supports the backup and restoration of vSphere 7.0**. Not all vendors have confirmed support for vSphere 7.0 as of yet.

The vCSA has to use the fully qualified domain name (FQDN) with correct DNS resolution. Your forward and reverse DNS static records must exist at your DNS server, and the resolution must work both ways.

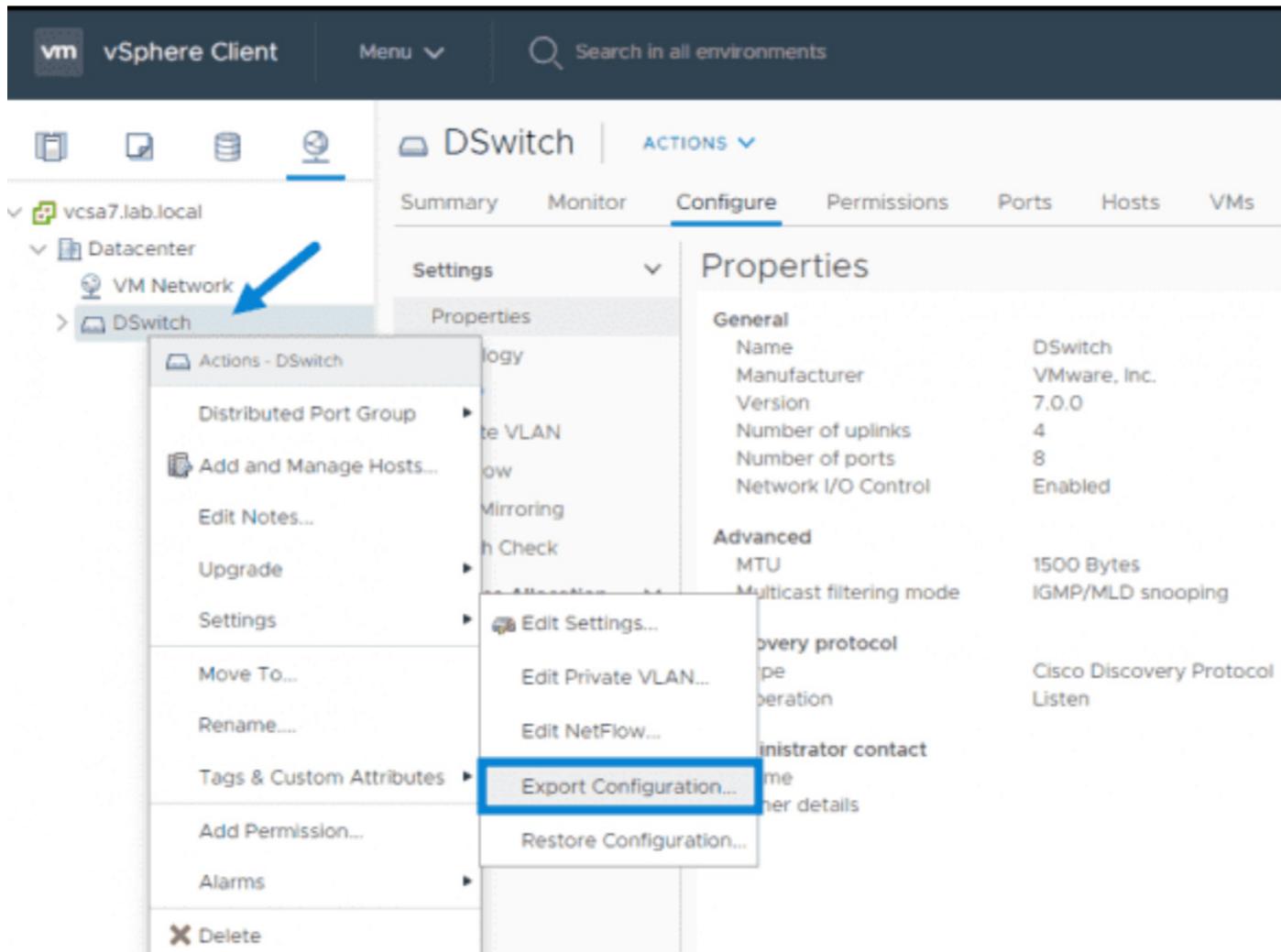
The VMware vSphere Storage APIs – Data Protection framework is used by backup software products to do a backup of all your virtual machines (VMs), including the VMware vCSA.

Basically, the software product is able to back up a vCSA VM and do a restore. In order to restore the vCenter itself, you must connect directly to an ESXi host to initiate the restore operation because vCenter is unavailable during the restore.

### Limitations and considerations

**VMware vSphere Distributed Switch:** If you're using a VMware vSphere Distributed Switch (vDS) in your environment, VMware recommends backing up the vDS separately. What you need to do, in fact, is an export of the vDS configuration before performing the backup.

In this way, you can re-import the configuration after a restore if you see some inconsistency within your network configuration. In this case, it is possible to have a separated backup of the specific vCenter networking component, which is configured via vCenter and deployed to each ESXi host.



### Export VMware vDS Configuration prior to backup

**Content Libraries:** Yes, content libraries are vCenter-dependent objects. If, for example, you delete some items or templates within the content library after you make a backup, the library item is missing when you want to restore. It's a dependency that you might want to take into consideration.

**vCenter Server HA:** You'll need to reconfigure vCenter High Availability if you know vCenter HA is a system where a second and third node of vCSA are used to ensure failover and fallback, in case vCenter becomes unavailable.

Restoring a vCenter Server requires reconfiguring vCenter HA. If you know that you'll be restoring the vCenter server, VMware recommends destroying the configuration prior to restoring, and then restoring and reconfiguring vCenter HA again.

### VMware file-level backup

The file-level backup, introduced in vSphere 6.0, is a convenient way to have an up-to-date, granular backup of your full configuration if you don't do regular image-level backups or your

software vendor does not support vSphere 7.0 just yet and you have already upgraded your vCenter Server to version 7.0.

File-level backup can be configured by connecting to the vCSA admin user interface (UI) via [https://IP\\_of\\_appliance:5480](https://IP_of_appliance:5480).

There, you can configure scheduled backups of different files, including the vPostgres DB. One interesting feature of the file-level backup is that the process verifies the DB before making the backup.

Also, if you want to restore the whole vCSA, you must use the same installer ISO, because the installer and backup versions must match.

The screenshot shows the 'Backup Schedule' section with a single backup task listed. The task details are as follows:

Backup Location	Type	Status	Data Transferred
smb://192.168.1.7/d\$/backu...	Manual	2%	0 B

Below the table, there is a tooltip message: "The restore process requires that both the installer and backup versions are identical." To the right of the tooltip, there is a timestamp: "0200605-062722\_".

The 'Activity' tab is selected, showing the status of the backup task: "Db health check in progress. This may take 3 to 10 min based on db size." A blue box highlights this message.

### DB health check prior to backup

Many options and storage protocols are supported for configuring the destination of a scheduled backup. The protocols supported for backup are FTPS, HTTPS, SFTP, FTP, NFS, SMB, and HTTP. In my lab, I simply used SMB for my file server.

Various options can be configured or disabled. For example, the DB health check and the stats, events, and tasks do not need to be backed up in some environments.

## Edit Backup Schedule

The screenshot shows the 'Edit Backup Schedule' dialog box. It includes fields for backup location (smb://192.168.1.7/d\$/backup), user name (administrator@lab.local), password, schedule (Daily at 03 : 25 P.M. Etc/GMT+4), encryption password, and confirm password. Under 'DB Health Check', 'Disable' is selected (indicated by a blue arrow). Under 'Number of backups to retain', 'Retain last 7 backups' is selected. Under 'Data', 'Stats, Events, and Tasks' is checked (indicated by a blue arrow) and 'Inventory and configuration' is unchecked. At the bottom are 'CANCEL' and 'SAVE' buttons.

Backup location <span style="font-size: small;">(i)</span>	smb://192.168.1.7/d\$/backup	
Backup server credentials	User name	administrator@lab.local
	Password	<span style="font-size: small;">(i)</span>
Schedule <span style="font-size: small;">(i)</span>	Daily	03 : 25 P.M. Etc/GMT+4
Encrypt backup (optional)	Encryption Password	<span style="font-size: small;">(i)</span>
	Confirm Password	<span style="font-size: small;">(i)</span>
DB Health Check <span style="font-size: small;">(i)</span>	<input checked="" type="checkbox"/> Disable	
Number of backups to retain	<input type="radio"/> Retain all backups <input checked="" type="radio"/> Retain last 7 backups	
Data	<input checked="" type="checkbox"/> Stats, Events, and Tasks	
	<input checked="" type="checkbox"/> Inventory and configuration	
Total size (compressed)		
<span style="border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; text-decoration: none; color: inherit;">CANCEL</span>		<span style="text-decoration: none; color: inherit;">SAVE</span>

### Backup options and ability to disable DB health check

These are the supported backups of vCSA.

**Note:** If your DB is larger and its size is greater than 300 GB, your backup will most likely fail.

Quote from VMware release notes:

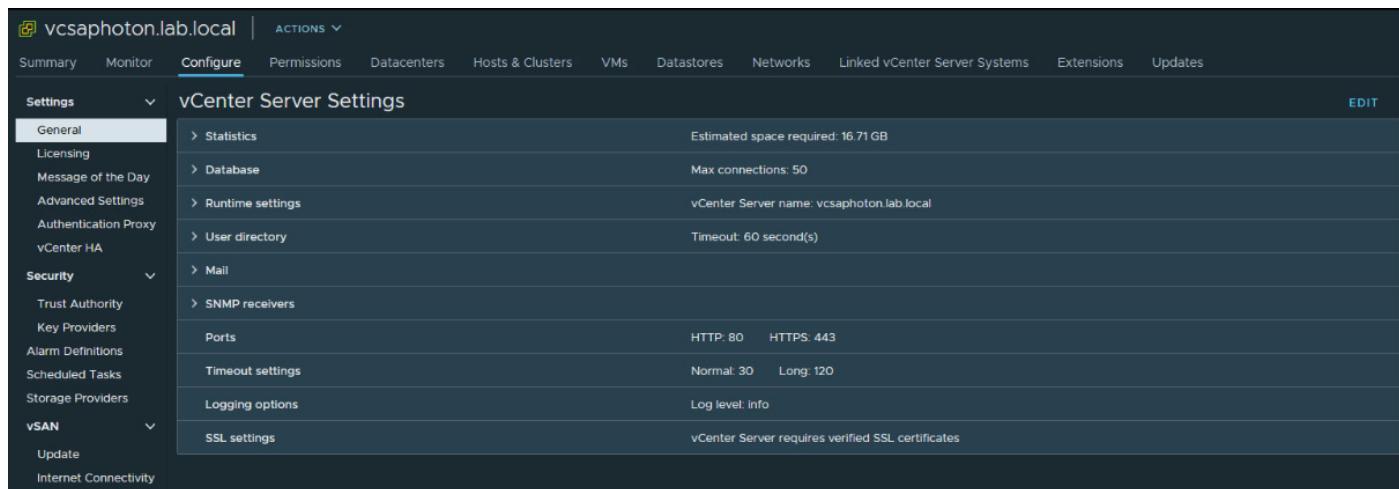
*If the vCenter database size is 300 GB or greater, the file-based backup will fail with a timeout. The following error message is displayed: Timeout! Failed to complete in 72000 seconds.*

## Objective 4.9 Analyze basic log output from vSphere products

If you're running just vSphere and ESXi, you'll only have to deal with logs from those two products. However, VMware has a rather large portfolio of products, and each of those has its own logging. Probably the best solution is to send logs from all VMware products to a remote logging server which can ingest those logs and present you with a graphical UI which provides some advanced search capabilities for specific issues.

On a vCenter server, the default log level setting is Info. This is where errors, warnings, and informational level are logged. It is possible to change it and have more detailed logs.

You can use the vSphere Client to change the logging level by **selecting the vCenter Server**, **selecting Configure > Settings > General > Edit**, and setting the logging settings to the appropriate level.



The screenshot shows the vSphere Client interface with the URL "vcsaphoton.lab.local" at the top. The navigation bar includes Summary, Monitor, Configure (which is selected), Permissions, Datacenters, Hosts & Clusters, VMs, Datastores, Networks, Linked vCenter Server Systems, Extensions, and Updates. On the left, a sidebar under the Settings section lists General, Licensing, Message of the Day, Advanced Settings, Authentication Proxy, vCenter HA, Security (with Trust Authority, Key Providers, Alarm Definitions, Scheduled Tasks, Storage Providers), and vSAN (with Update and Internet Connectivity). The main content area is titled "vCenter Server Settings" and contains the following configuration options:

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

**vCenter server logs settings**

In the logging settings you have a drop-down menu where you can choose the log level. The choices are none, error, warning, info, verbose or trivia.

However, VMware does not recommend increasing the log settings to trivia as it might cause performance degradation on vCenter Server. Only enable trivia or verbose logging for troubleshooting purposes.

The screenshot shows the 'Edit vCenter general settings' interface. On the left, a sidebar lists various settings: Statistics, Database, Runtime settings, User directory, Mail, SNMP receivers, Ports, Timeout settings, Logging settings (which is selected and highlighted in grey), and SSL settings. The main panel is titled 'Logging settings' with the sub-instruction 'Select the level of detail that vCenter Server uses for log files.' Below this, a 'Log level' dropdown menu is open, showing options: none, error, warning, info, verbose, and trivia. The 'info' option is currently selected. A small downward arrow icon is located at the top right of the dropdown.

## Edit vCenter server log settings

The main logs in a vCenter Server appliance are located in `/var/log/vmware`. The most important logs are in the `vpxd` subdirectory. Some other sibling subdirectories include `vsan-health`, `vsphere-ui`, and `vpostgres`.

The Management agent (`hostd`), VirtualCenter Agent Service (`vpxa`), and VirtualCenter (`vpxd`) logs are automatically rotated and maintained to manage their growth. If not, they will take too much storage space.

On the other hand, the information in the logs can be lost if the logs are rotated too quickly, hence the idea of changing to `trivia` only during the troubleshooting or when you want to send the logs to VMware.

### How to understand that the logs are rotating too quickly?

Rotation of logs basically means the turnover of files where the oldest gets deleted and replaced by newer ones. For example, if you set the maximum number of log files to 10, after every 10 log files, the numbering restarts at 0.

You can adjust the log rotation via two advanced parameters:

- **Syslog.global.defaultRotate** - Maximum number of logs to keep when rotating logs.
- **Syslog.global.defaultSize** - Size of log (in KB) before triggering a log rotation.

Those settings are based on per-host level, so you have to go to the advanced system settings on your host.

**Configure > System > Advanced system settings > Edit > filter for Syslog.**

Name	Value
Syslog.global.defaultRotate	8
Syslog.global.defaultSize	1024
Syslog.global.logCheckSSLCerts	true
Syslog.global.logDir	[] /scratch/log
Syslog.global.logDirUnique	false
Syslog.global.logHost	

## Configuring syslog on ESXi 7 hosts

There, you can also set up a global log directory which can be located on VMFS or NFS datastore.

You can also set up a remote syslog host via another advanced setting:

- **Syslog.global.LogHost** - Remote syslog host and port. The logs are sent to a remote host via this port. As an example, if we would like to forward to a server named syslogsvr01 and we would like to use port 1514, we could simply put `ssl://syslogsvr-1:1514`.

### How to control logs on a per-VM level?

You can change the number of logs for a single VM. Every time you power On or resume a VM on your host a log file is created.

VMware recommends saving 10 log files, each one limited to no less than 2 MB. If you need logs for a longer time span, you can set `vmx.log.keepOld` to 20.

You can do this change via vSphere web client, **Select your VM > right click > Edit Settings > VM Options > Advanced > Edit Configuration**.

**vmx.log.keepOld** – this is the setting to look for. Set this for the number you want.

You can also do it for all VMs on a particular host. In this case you'll need to edit a `/etc/vmware/config` file where you'd add or edit a line like this: `vmx.log.keepOld = "10"`

As you can see, we can configure the size of logs, their number or rotation.

## How do I upload my logs to VMware?

It is possible to export system logs from the vCenter Server and all its hosts. Start by selecting the vCenter Server instead of a specific host.

In the wizard, you can select which hosts to include, and you can optionally select Include vCenter Server and vSphere UI Client Logs.

You can export a vCenter Server instance's support bundle by using the URL shown on the DCUI home screen (<https://FQDN:443/appliance/support-bundle>).

The screenshot shows the vCenter Server Management interface. On the left, a sidebar lists various management categories: Summary (selected), Monitor, Access, Networking, Firewall, Time, Services, Update, Administration, Syslog, and Backup. The main content area displays the vCenter Server's configuration, including its name (vcsaphoton.lab.local), product (VMware vCenter Server), version (7.0.2.00100), and build number (17920168). To the right of this information is a vertical Actions menu with options: Reboot, Shutdown, Create Support Bundle (which is highlighted with a blue arrow), and Switch Theme. Below the server info, there are two sections: Health Status and Single Sign-On. The Health Status section shows the overall health as 'Good' (last checked on May 19, 2021, at 6:46:20 PM) and lists detailed status for CPU, Memory, Database, Storage, and Swap, all of which are also 'Good'. The Single Sign-On section shows the domain as 'vsphere.local' and the status as 'Running'.

### Create vCenter server appliance support bundle

## Objective 4.10 Configure vSphere Trust Authority

VMware is introducing a new feature that is very important for an organization's security. VMware Trust Authority (vTA) will be able to establish a trust relationship with the ESXi host configuration to ensure there are no alterations from malware, etc. VTA creates a separate cluster with three hosts, in which the key manager communicates with trusted hosts among the management hosts.

The management hosts are pretty much «locked down,» which means that a very small group of people can access those hosts, where the workload hosts (green) can be accessed by a larger group. The management cluster runs management software, such as vCenter Server or other monitoring solutions.

The architecture basically relies on the principle of least privilege, whereby the admin should really only have privileges to do what needs to be done. A separation of roles is essential when planning security.

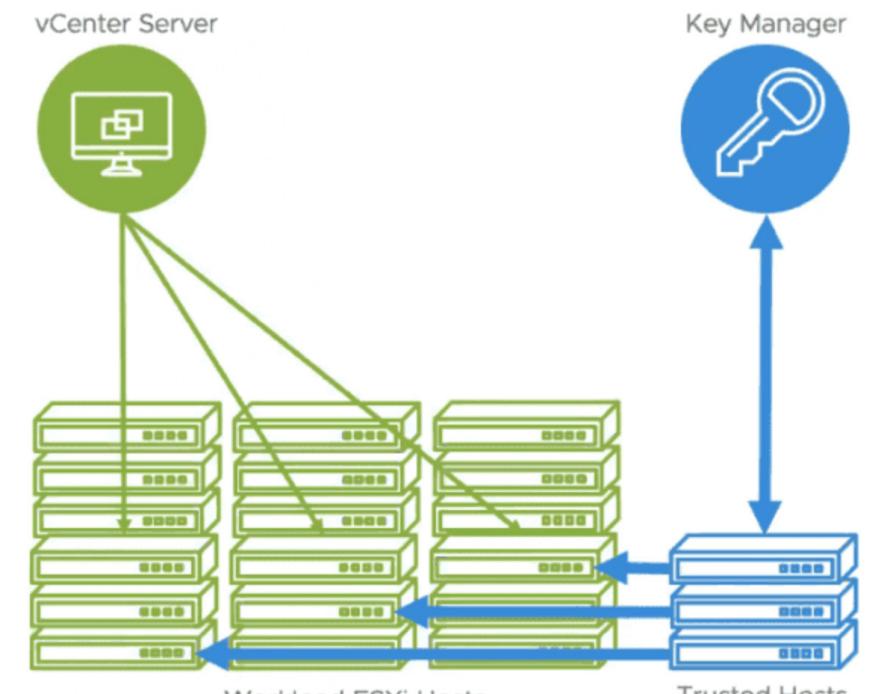
VMware is trying to work toward a better security model, and the introduction of vTA is the first step. vTA represents the foundation to which VMware will add more functions in future releases. In this release, VMware is building the base block of the architecture.

### The main vSphere Trust Authority (vTA) features

**VMware vTA creates a hardware root of trust using a separate ESXi host cluster:** This might be a problem for certain clients since, as you can see, the management cluster is used only for management, not for running workloads. Explain this to a client who is on a budget, and who does not have the money to spend on three hosts that do not directly run his production environment. The trusted hosts will be running the corporate workloads, which are encrypted and cannot be moved to hosts that are not trusted.

**Key manager and attestation requirement:** The VMware Key Management Server was introduced in vSphere 6.5 to allow encryption of VMs. You set up a trusted connection between the vCenter Server and a Key Management Server (KMS). The vCenter Server can then retrieve keys from the KMS as needed. The vSphere Trust Authority will enable setting that attestation can be a requirement for access to encryption keys. This will further reinforce the security, to prevent a potential intruder from getting the encryption keys to decrypt your encrypted VMs and gain access to the company's data. The Key Manager only talks to trusted hosts, not to the vCenter Server, as in previous releases.

vSphere 6.7 and its attestations were «view only,» so there were no repercussions for failing. The secure workloads could still run on untrusted hosts. vTA and vSphere 7 allow the Key Manager to talk to trusted hosts instead of the vCenter Server (which is a VM).



### vSphere Trust Authority in vSphere 7.0

**Encryption of workload vCenter server instances:** In 6.5 and 6.7, you cannot encrypt the vCenter Server VM as there are many dependencies. vSphere 7.0 will be able to encrypt vCenter Server instances.

**Principle of Least Privilege:** You can restrict access such that a very small group of admins can access the trusted hosts. Again, separation of roles and privileges is important. The «green» hosts in the diagram above can be accessed and managed by a wider group of admins, whereas access to «blue» hosts remains restricted.

**Trusted Platform Module (TPM 2.0):** This is a \$20 trusted platform module chip that can be ordered from your hardware manufacturer and which is cryptographically signed and attached to the host when you first plug it in. (Note: don't buy these on eBay since they are usually used and are worthless.)

## Conclusion

The VMware vSphere Trust Authority is a set of features that will reinforce your organization's security by leveraging a trusted platform module that is integrated into the hardware. There is also a set of features that enable running vCenter within a completely secured environment while leveraging encryption for the vCenter Server itself.

The possibility of separating access to the management cluster and the workload cluster reduces the audit scope and risk, which wasn't really possible with the previous vSphere design.

## Objective 4.11 Configure vSphere certificates

With vSphere certificates, you can basically stick to the defaults when it comes to provisioning vCenter server components and ESXi hosts with certificates. The certificates are managed and issued by VMware Certificate Authority (VMCA).

You have another option to use custom certificates stored in the VMware Endpoint Certificate Store (VECS). vCenter Server supports custom certificates generated and signed from your own enterprise public key infrastructure (PKI) such as Microsoft PKI. vCenter Server, however, also supports custom certificates that are generated and signed by trusted third-party certificate authorities (CAs), as for example VeriSign or GoDaddy, so there are options to choose from.

The certificates under vSphere can:

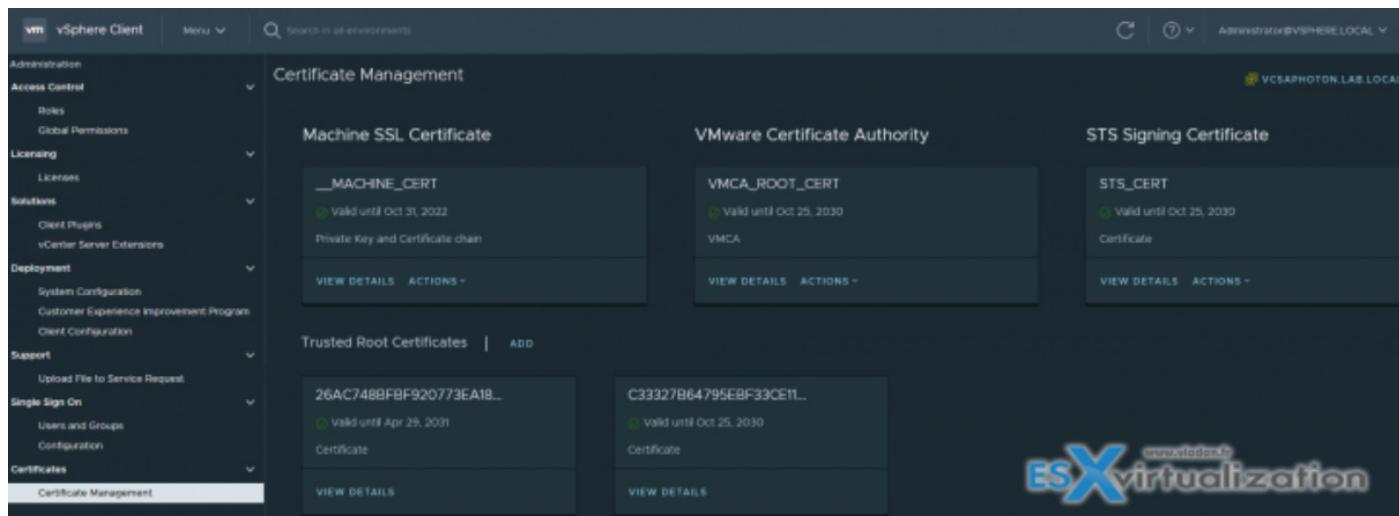
- Authenticate vSphere services
- Sign tokens (e.g., SSO)
- Encrypt communication between vCenter and ESXi

VMware VMCA runs on VCSA as a service. It provides all the required certificates for vCenter Server and ESXi, which are auto-renewed.

You can replace the VMCA root certificate with a certificate that is signed by an enterprise CA or a third-party CA, in which case VMCA signs the custom root certificate each time it provisions certificates, making VMCA an intermediate CA.

When you replace the default certificates by your own, you are then responsible for the renewal, when the time comes.

VMware recommendations for certificate management are basically the following. If you replace certificates on your own, you should replace only the SSL certificate that provides encryption between nodes. VMware does not recommend replacing either solution user certificates or STS certificates.



In fact there are two different scenarios or modes:

**Default** - VMCA provides all the certificates for vCenter Server and ESXi hosts.

**Hybrid** - You replace the vCenter Server SSL certificates and allow VMCA to manage certificates for solution users and ESXi hosts. Optionally, for high-security-conscious deployments, you can replace the ESXi host SSL certificates as well.

## Certificate requirements

- The key size is 2048 bits to 16,384 bits.
- VMware supports PKCS8 and PKCS1 (RSA key) PEM formats. When you add keys to VECS, they are converted to PKCS8.
- x509 Version 3 is required.
- SubjectAltName must contain DNS Name=machine\_FQDN.
- CRT required.

## What's not supported by VMCA?

- Certificates with wildcards
- The algorithms md2WithRSAEncryption 1.2.840.113549.1.1.2, md5With-RSAEncryption 1.2.840.113549.1.1.4, and sha1WithRSAEncryption 1.2.840.113549.1.1.5
- The algorithm RSASSA-PSS with OID 1.2.840.113549.1.1.10

If you use VMCA as an intermediate CA, you can use the vSphere Certificate Manager to create a CSR or you can create a CSR manually. You can use the vSphere Client to view the expiration date for certificates, whether they are signed by VMCA or a third party.

The vCenter Server has alarms for hosts where certificates expire shortly (expire in less than 8 months) and red alarms where certificates are in the Expiration Imminent state (expire in less than 2 months). ESXi hosts that boot from installation media have auto-generated certificates. When a host is added to the vCenter Server system, it is provisioned with a certificate that is signed by VMCA as the root CA.

**ESXi certificate** - provisioned by VMCA and stored locally on the ESXi host (in /etc/vmware/ssl) when first connected or re-connected.

**Machine SSL Certificate** - used to create SSL sockets for secure socket layer (SSL) client connections, server verification, and secure communication such as HTTPS and LDAPS. Used by the reverse proxy service, the vCenter Server service (vpxd), and the VMware Directory service (vmdir).

**Solution user certificate** - Used by solution users to authenticate to vCenter Single Sign-On through SAML token exchange.

**vCenter Single Sign-On SSL signing certificate** - Used for authentication. The SAML token is basically the user's identity. You can manage this certificate from the command line.

**VMware Directory Service (vmdir) SSL certificate** - since vSphere 6.5 (I think) the machine SSL certificate is used as the vmdir certificate.

**vSphere Virtual Machine Encryption Certificates (important when you want to encrypt your VMs)** - Used for virtual machine encryption, which relies on a key management server (KMS), now present in vSphere 7.0 U2.

## Objective 4.11.1 Describe Enterprise PKIs role for SSL certificates

Certificate management in vSphere 7 is done via vCenter Server. In general, certificates are used for encryption of communication, authentication of vSphere services, or internal actions, such as signing tokens.

VMware vSphere has an internal VMware Certificate Authority that is able to supply all the certificates that are needed for VMware services. VMCA is installed on every vCenter Server host. All communications within vSphere are protected with Transport Layer Security (TLS). There are ESXi certificates, machine SSL certificates for web-based vSphere clients, and SSO login pages.

Other types of certificates are used for add-on solutions, such as vRealize Operations Manager, vSphere Replication, and others.

Certificate management within vSphere 7

## The configuration of vSphere certificates

Previous releases of vSphere had poor usability in terms of certificate management. However, vSphere 7 has some significant improvements to make creating or replacing certificates as seamless as possible.

VMware Certificate Management (VMCA) is not as advanced as traditional PKI solutions, so you cannot request generating certificates for other purposes. The VMCA is fine for VMware environments, though.

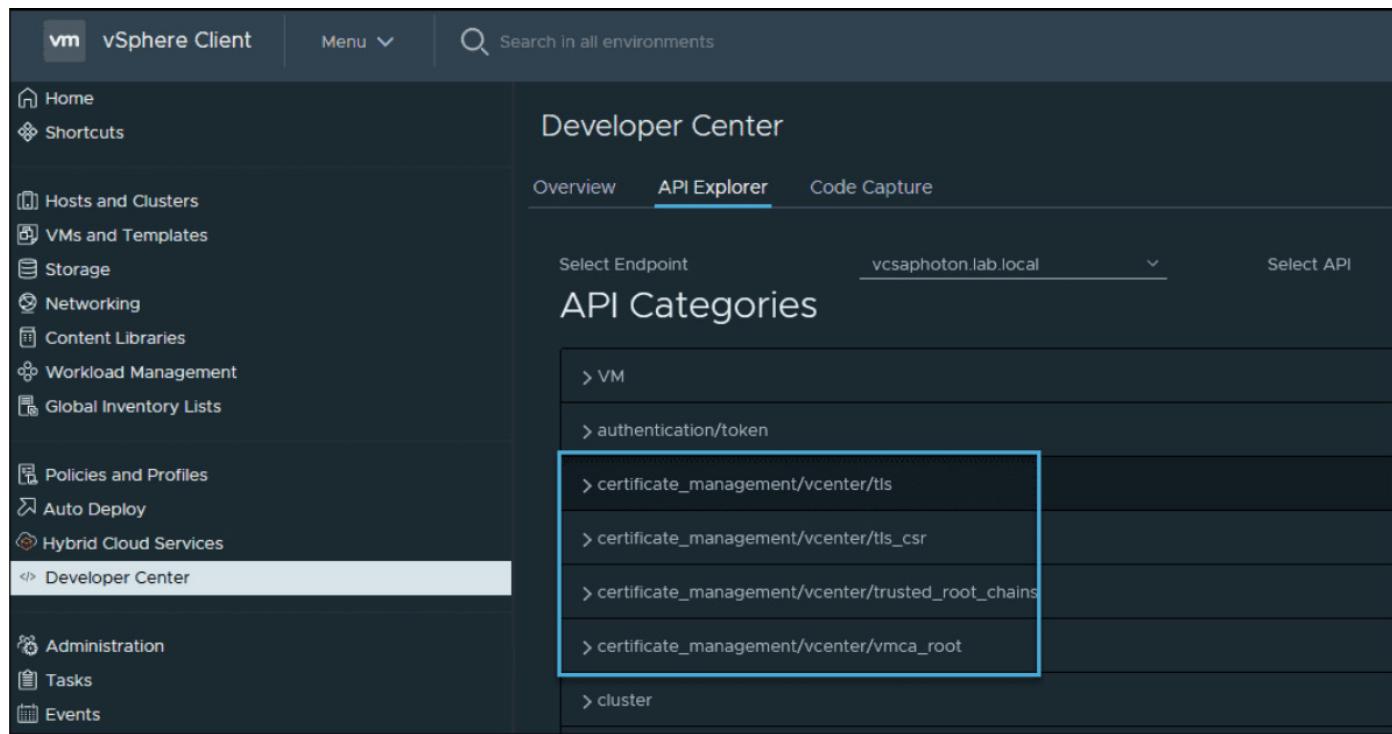
By default, vSphere comes with self-generated certificates so you don't have to lose time during the installation and deployment of the product. If you have to replace the certificates on your own, you'll do it through the certificate management menu, as shown in the above screenshot.

## How can vSphere Certificates be managed?

You can manage vSphere certificates not only via the vSphere web client, but also in many other ways.

- **Certificate Management CLIs** — This is a command line utility that uses dir-cli, certool, and vecs-cli tools that perform the tasks necessary for certificate management.
- **Certificate Manager Utility** — This uses command line tools on the vCenter Server to perform tasks.
- **vSphere REST API** — Used via the vCenter server UI.

Here is a screenshot from the UI showing an API explorer and certificate management:



vCenter API explorer and certificate management via the REST API copy

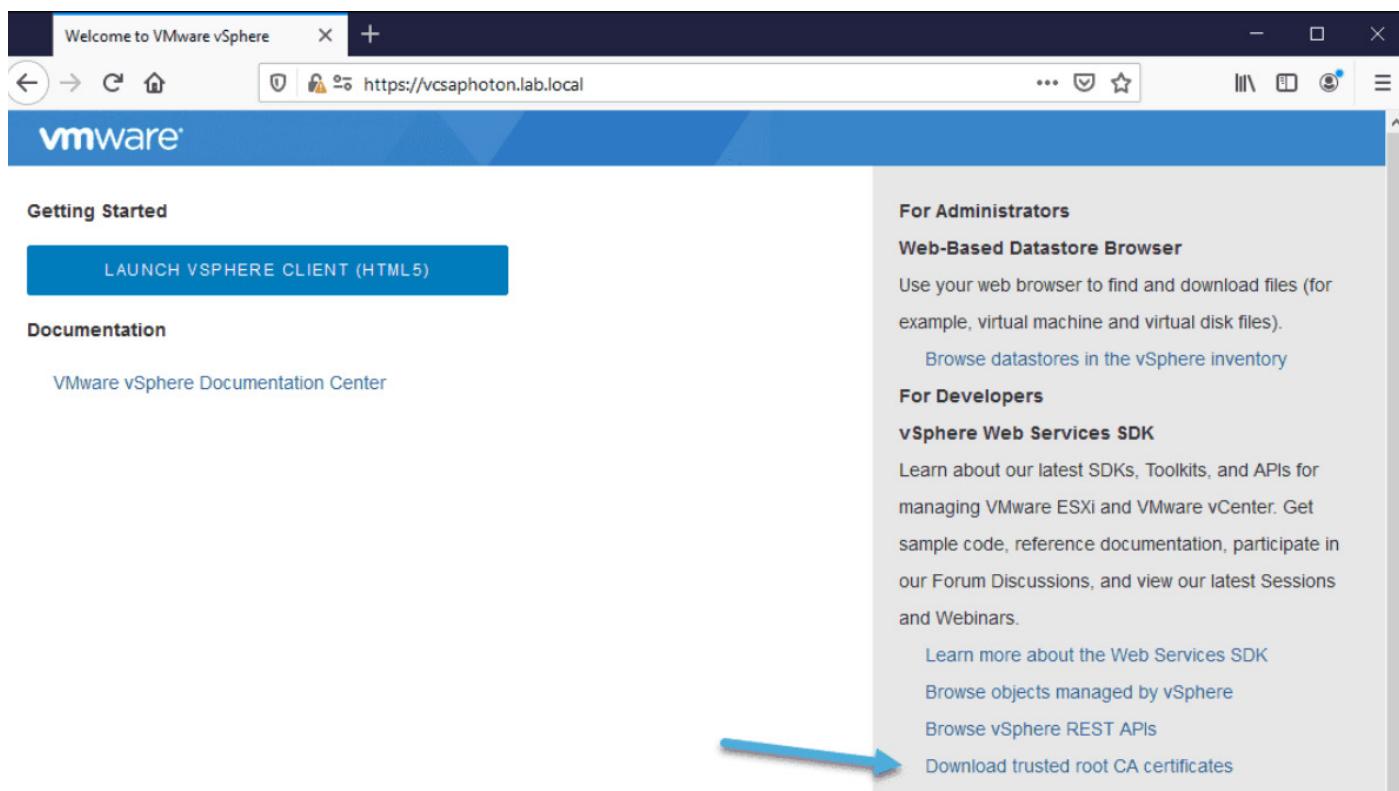
- **vSphere HTML5 Web client** — The traditional way of performing tasks within the client.
- **SSO Configuration Utility** — This uses and runs the Security Token Service (STS), which handles certificate management from the vCenter Server command line user interface.

Note that there is also a VMware Fling tool called the [SDDC Certificate Tool](#), which can automatically replace certificates across VMware products.

## Four modes of certificate management in vSphere

In vCenter Server, you can run certificate management in four different modes.

**Fully Managed Mode** — In this case, the VMCA has a new root CA certificate. With this certificate, vCenter Server manages the intra-cluster certificates where hosts communicate among themselves and back to vCenter Server. There is also a machine certificate, which serves when the user logs in to the vSphere client. The VMCA root CA certificate can be downloaded from the main vCenter Server page and imported to other PCs to establish trust. The certificate can be regenerated, and we can replace the information by default with our own information (by default, it contains only VMware information).



### Download trusted root CA certificates

**Hybrid Mode** — This mode allows the VMCA to automate certificate management. It enables automatic replacement of the certificate that the vSphere web client uses, so it is accepted by default by client browsers. The certificates that establish trusts with ESXi hosts are managed manually.

**Subordinate CA Mode** — In this case, the VMCA can operate as a subordinate CA, which is a delegated authority from a corporate CA. vCenter Server can continue to automate certificate management, but the certificates that are generated are trusted as a part of the organization.

**Full Custom Mode** — In this mode, the VMCA is not used at all. An admin has to install and manage all the certificates within the vSphere cluster—manually. This can be very time consuming for IT teams. In addition, there might be some downtime, as it needs to be disconnected and reconnected to vCenter Server when you replace certificates on a host. This might be a bit overwhelming and complicated to manage when you have distributed vSwitches or VMware vSAN, which does not like it when vCenter Server is disconnected.

VMware recommends using Hybrid mode, which provides some automation.

However, all four modes are fully supported. The security teams of most organizations are working hard to secure the control plane of the administrators, using certificates that are issued by the security team via their enterprise PKI. vSphere Hybrid mode helps in this and allows securing access to vSphere by replacing the Machine SSL certificate.

VMware's best practice says that access to ESXi management should be limited and only executed on an isolated network. To achieve this and still be able to log in directly to ESXi hosts, the VMCA CA certificate can be exported and added to the Trusted Root Certification Authorities container in an Active Directory group policy.

## Objective 4.12 Configure vSphere 7 Lifecycle Manager/VMware Update Manager (VUM)

VMware vSphere Update Manager (VUM) product has evolved into what is now called vSphere 7 Lifecycle Manager. The functionality in vSphere 7 has been expanded and there are some new configuration options as well. In this section, we'll detail the changes and see how to configure vSphere 7 Lifecycle Manager (vLCM).

In vSphere 7.0, vSphere Lifecycle Manager replaces VMware Update Manager from prior versions. Lifecycle Manager expands the functionality of Update Manager to include features and capabilities for ESXi lifecycle management at the cluster level.

Lifecycle Manager operates as a service that runs on the vCenter Server appliance. This service is available via the vSphere Client after the vCenter Server deployment and there is no special extra installation.

Installing an optional module can be done with VMware vSphere Update Manager Download Service (UMDS) which is used in scenarios where vCenter Server is installed in a secured network with no Internet access.

It is then possible to install UMDS and use it to download updates. You can also use the UMDS to export the updates to a USB drive that you then present to vSphere Lifecycle Manager.

## Fast Upgrades with vLCM

With vSphere 7 U2 a new functionality has been introduced in vLCM. You can now remediate hosts with business priorities and leverage fast upgrades to have as little downtime as possible.

You can configure **Quick Boot** where supported OEM vendors enable skipping the initialization of firmware and many other hardware devices during boot.

Fast upgrades preserve the state of VMs running on a host by suspending them to the **host's memory**. Once the host reboots, they are automatically restored from memory.

You save time by not migrating the VMs off the host.

**Image remediation Settings** - The image remediation settings also allow you to configure the quick boot. With vSphere web client, go to **Shortcuts > Lifecycle Manager > Settings >** under **Host remediation** chose **Images**.

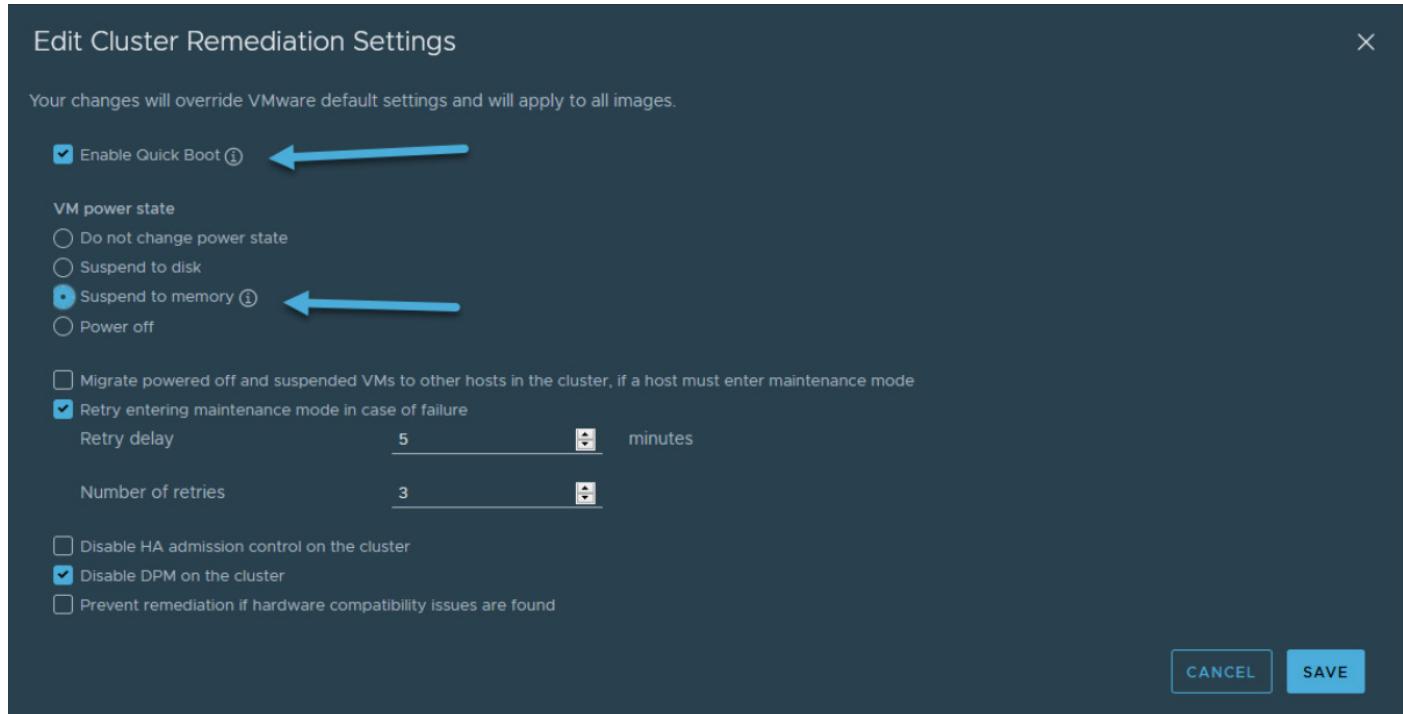
The screenshot shows the vSphere Lifecycle Manager interface. The left sidebar has sections for Administration, Image Depot, Updates, Imported ISOs, Baselines, and Settings. Under Host Remediation, the 'Images' tab is selected. The main area is titled 'Images Remediation Settings'. A note says 'Remediation settings are set to VMware-provided settings. They will change if VMware updates their provided settings.' Below are several configuration options:

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

## vSphere Lifecycle Manager Image Remediation Settings

As you can see, we can enable Quick boot at the top. This option speeds up the upgrade process of an ESXi host compared to a regular reboot, which involves a full power cycle requiring firmware and device initialization. With Quick Boot you optimize the reboot times and, if you have many ESXi hosts, it adds up to the overall time.

Here we also have different options for changing VM power state - suspend to disk, **suspend to memory** or power off.



## vSphere Lifecycle Manager and Editing cluster remediation settings

We can also change whether we want to migrate powered off and suspended VMs to other hosts in the cluster or change the retry delay or the number of retries when the host needs to enter the maintenance mode.

Lastly, we can activate the Disable HA admission control on the cluster, disable DPM or prevent remediation if hardware compatibility issues are found.

This is particularly useful for preventing new and potentially problematic updates from applying to a host.

**Baselines Remediation Settings** - You can use baselines or images to remediate individual hosts or all hosts in a cluster collectively. Some remediation settings are applicable regardless of whether you use baselines or images to initiate host remediation.

As an example, you can configure virtual machine migration settings, maintenance mode settings, and quick boot for hosts that are managed by either cluster images or baselines.

With vSphere web client go to **Shortcuts > Lifecycle Manager > Settings >** under **Host remediation** chose **Baselines**.

Lifecycle Manager | ACTIONS ▾

Image Depot   Updates   Imported ISOs   Baselines   **Settings**

Administration  
Patch Downloads  
Patch Setup

Host Remediation  
Images  
**Baselines**  
VMs

**Baselines Remediation Settings**

The settings will apply to hosts in this vCenter which are managed with Baselines during remediation.

VM power state	Do not change VM power state
> Retry entering maintenance mode in case of failure	3 attempts every 5 minutes
PXE booted hosts	Disallow installation of additional software on PXE booted hosts
VM migration	Do not migrate powered off and suspended VMs to other hosts in the cluster
Disconnect removable media devices	No
Quick Boot ⓘ	Quick Boot is enabled
> Parallel remediation ⓘ	Disabled

## vSphere Lifecycle Manager

By clicking the Edit button you'll have a pop-up window which will bring you to the configuration options. This opens a familiar page where we can (again) see the Enable quick boot check box.

Edit Settings for Host Remediation X

Enable Quick Boot ⓘ

Power off virtual machines

Suspend virtual machines

Do not change VM power state

Leave virtual machines and virtual appliances in their current power state

Retry entering maintenance mode in case of failure

Retry Delay  minutes

Number of retries

Allow installation of additional software on PXE booted hosts

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

Disconnect removable media devices that might prevent a host from entering maintenance mode

Parallel remediation

Maximum number of concurrent remediations  Automatic  Manual

CANCEL SAVE

## vSphere Lifecycle Manager configuration options

Other options below are unchecked, but we can check them. One of the options, Parallel Remediation, will allow you to remediate all ESXi selected hosts in this cluster that are in maintenance mode at the same time.

**Please Note:** Remaining hosts not in maintenance mode will be skipped when using this option.

**VM Rollback Settings** - Lastly, we can change the way VMs are protected against updates applied to them by activating VM snapshots during upgrades and specifying for how long we want to keep those snapshots before they are deleted.

The screenshot shows the Lifecycle Manager interface with the 'Settings' tab selected. On the left, there's a sidebar with 'Administration' and 'Host Remediation' sections, and a 'VMs' button which is highlighted with a blue bar at the bottom. The main area is titled 'Default Settings for VM Rollback' and contains two settings: 'Take snapshot of VMs' (set to 'No') and 'Keep snapshots' (set to '--'). An 'EDIT' button is located to the right of the settings table. A large blue arrow points from the 'VMs' button in the sidebar to the 'Edit' button in the main window.

### VM Rollback settings

In this pop-up window we can specify whether we want to have our VMs snapshotted before upgrades and how long should those snapshots be kept.

The dialog box is titled 'Edit Default Settings for VM Rollback'. It contains a message: 'Rollback will take a snapshot of the VMs before upgrading.' Below this, there are three options: 'Take snapshot of VMs' (checked), 'Do not delete snapshots' (unchecked), and 'Keep snapshots for [12] hours' (radio button selected). At the bottom are 'CANCEL' and 'SAVE' buttons.

### Default settings for VM rollback

The VM rollback settings can vary from organization to organization. By default, vSphere Lifecycle Manager takes snapshots of virtual machines before upgrading them. If the upgrade fails, you can use the snapshot to return a virtual machine to its state before the upgrade.

## Objective 4.13 Securely Boot ESXi hosts

ESXi provides the option of using UEFI Secure Boot. UEFI Secure Boot is a mechanism that makes sure that only trusted code is loaded by the EFI firmware. Then the ESXi OS is loaded and, finally, you get to the UI where you can log in.

When Secure Boot is enabled, the UEFI firmware processes the validation of the kernel which is digitally signed. It is verified and compared to a digital certificate which is stored in the UEFI firmware.

VMware supports Secure boot since ESXi 6.5, but the hardware must support it first and this feature must be enabled. ESXi version 6.5 and later supports UEFI Secure Boot at each level of the boot stack where even the vSphere Installation Bundles (VIBs) are digitally signed.

During the boot time, the ESXi file system tries to map to the content of those packages. It's basically the kernel that validates each VIB by using the Secure Boot verifier against the firmware-based certificate. The system is making sure that all VIBs are matching.

When Secure Boot is enabled, ESXi does not allow the installation of unsigned VIBs on ESXi. If you want to install unsigned VIBs such as community drivers, you must disable Secure Boot. If you enable Secure Boot, the Secure Boot verifier runs.

If the secure boot verifier detects unsigned VIBs, it basically generates a PSOD. If you still want to boot the ESXi (for testing), you need to boot the ESXi host with Secure Boot disabled, remove the VIB, and reboot with Secure Boot enabled.

### Using TPM chips

ESXi can use Trusted Platform Module (TPM) chips, which are secure cryptoprocessors that enhance host security by providing a trust assurance rooted in hardware as opposed to software. You can buy them separately from your hardware.

TPM is an industry-standard for secure cryptoprocessors. TPM chips can also be installed in laptops, desktops, and servers. vSphere 7.0 supports TPM version 2.0.

A TPM 2.0 chip basically guarantees the ESXi host's identity.

UEFI Secure Boot makes sure that only signed software is loaded during boot, so it is a requirement for successful attestation.

### TPM 2.0 establishes Hardware Root of Trust

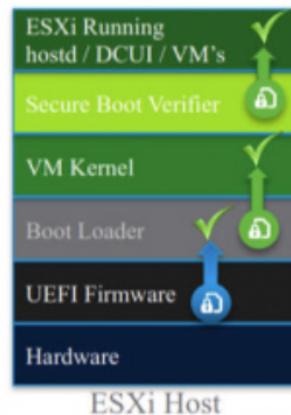
Secure Boot validates the bootloader and VMkernel.

Various measurements are written to the TPM

vCenter validates these measurements against the host event log and VIB metadata and marks the host as attested or not

Secure Boot Verifier continues and validates all remaining VIBs

### Remote Host Attestation



### TPM v2.0

The hardware chip is used by the ESXi host. The UEFI firmware within the hardware validates the bootloader and the VM kernel. In the Kernel, a number of measurements are taken, which are stored in the TPM device.

After that, the boot continues and the information is passed to vCenter, which queries the ESXi host and the TPM device and compares the hashes which have been reported by ESXi against the hashes reported by TPM.

## Objective 4.14 Configure different network stacks

You can create a custom TCP/IP stack on a host to forward networking traffic through a custom application.

Once you set a TCP/IP stack for the VMkernel adapter, you cannot change it later. If you select the vMotion or the Provisioning TCP/IP stack, you can use only these stacks to handle vMotion or Provisioning traffic on the host. All VMkernel adapters for vMotion on the default TCP/IP stack are disabled for future vMotion sessions.

If you set the Provisioning TCP/IP stack, VMkernel adapters on the default TCP/IP stack are disabled for operations that include Provisioning traffic, such as virtual machine cold migration, cloning, and snapshot migration.

If you must change the TCP/IP stack configuration, delete the existing VMkernel adapter and create a new one. You can then create a TCP/IP stack for that adapter.

## Procedure

- Open an SSH connection to the host.
- Log in as the root user.
- Run the ESXCLI command.

```
esxcli network ip netstack add -N=>stack_name»
```

## TCP/IP Stacks at the VMkernel Level

**Default TCP/IP stack** - Provides networking support for the management traffic between vCenter Server and ESXi hosts, and for system traffic such as vMotion, IP storage, Fault Tolerance, and so on.

**vMotion TCP/IP stack** - Supports the traffic for live migration of virtual machines. Use the vMotion TCP/IP to provide better isolation for the vMotion traffic. After you create a VMkernel adapter on the vMotion TCP/IP stack, you can use only this stack for vMotion on this host. The VMkernel adapters on the default TCP/IP stack are disabled for the vMotion service. If a live migration uses the default TCP/IP stack while you configure VMkernel adapters with the vMotion TCP/IP stack, the migration is completed successfully. However, the involved VMkernel adapters on the default TCP/IP stack are disabled for future vMotion sessions.

**Provisioning TCP/IP stack** - Supports the traffic for virtual machine cold migration, cloning, and snapshot migration. You can use the provisioning TCP/IP to handle Network File Copy (NFC) traffic during long-distance vMotion. NFC provides a file-specific FTP service for vSphere. ESXi uses NFC for copying and moving data between datastores. VMkernel adapters configured with the provisioning TCP/IP stack handle the traffic from cloning the virtual disks of the migrated virtual machines in long-distance vMotion. By using the provisioning TCP/IP stack, you can isolate the traffic from the cloning operations on a separate gateway. After you configure a VMkernel adapter with the provisioning TCP/IP stack, all adapters on the default TCP/IP stack are disabled for the Provisioning traffic.

## System Traffic Types

Dedicate a separate VMkernel adapter for every traffic type . For distributed switches, dedicate a separate distributed port group for each VMkernel adapter.

**Management traffic** - Carries the configuration and management communication for ESXi hosts, vCenter Server, and host-to-host High Availability traffic. By default, when you install the ESXi software, a vSphere Standard switch is created on the host together with a VMkernel adapter for management traffic. To provide redundancy, you can connect two or more physical NICs to a VMkernel adapter for management traffic.

**vMotion traffic** - Accommodates vMotion. A VMkernel adapter for vMotion is required both on the source and the target hosts. Configure The VMkernel adapters for vMotion to handle

only the vMotion traffic. For better performance, you can configure multiple NIC vMotion. To have multi-NIC vMotion, you can dedicate two or more port groups to the vMotion traffic. Every port group must have a vMotion VMkernel adapter associated with it. Then you can connect one or more physical NICs to every port group. In this way, multiple physical NICs are used for vMotion, which results in greater bandwidth .

**Note:** vMotion network traffic is not encrypted. You should provision secure private networks for use by vMotion only.

**Provisioning traffic** - Handles the data that is transferred for virtual machine cold migration, cloning, and snapshot migration.

**IP storage traffic and discovery** – connects your storage types that use standard TCP/IP networks and depend on the VMkernel networking. Storage using software iSCSI, dependent hardware iSCSI, and NFS.

If you have two or more physical NICs for iSCSI, you can configure iSCSI multipathing. ESXi hosts support NFS 3 and 4.1. To configure a software Fibre Channel over Ethernet (FCoE) adapter, you must have a dedicated VMkernel adapter. Software FCoE passes configuration information through the Data Center Bridging Exchange (DCBX) protocol by using the Cisco Discovery Protocol (CDP) VMkernel module.

**Fault Tolerance traffic** - Handles the data that the primary fault tolerant virtual machine sends to the secondary fault tolerant virtual machine over the VMkernel networking layer. A separate VMkernel adapter for Fault Tolerance logging is required on every host that is part of a vSphere HA cluster.

**vSphere Replication traffic** - Handles the outgoing replication data that the source ESXi host transfers to the vSphere Replication server. Dedicate a VMkernel adapter on the source site to isolate the outgoing replication traffic.

**vSphere Replication NFC traffic** - Handles the incoming replication data on the target replication site.

**vSAN traffic** - Every host that participates in a vSAN cluster must have a VMkernel adapter to handle the vSAN traffic.

## Objective 4.15 Configure Host Profiles

When you manage configuration of your ESXi hosts through your clusters, you should always try to make it as uniform as possible. A slightly different parameter in one of your hosts can result in hours of troubleshooting. Fortunately, with Host Profiles applying the same configuration to all your ESXi 7 hosts within the cluster is easy.

Host Profiles allow you to automate and centralize the configuration of your hosts, whether as a part of a cluster or as an individual host. They allow storing parameters that can configure networking, storage, security, and other host's settings by simply applying the Host Profile to a particular host.

Host Profiles also allow validating a host config by checking the compliance against the Host Profile. This is valid for a single host or for a whole cluster. You can clearly see the benefits of having completely uniform clusters with a 100 percent identical host configuration. This level of uniformity is difficult to achieve with manual configuration.

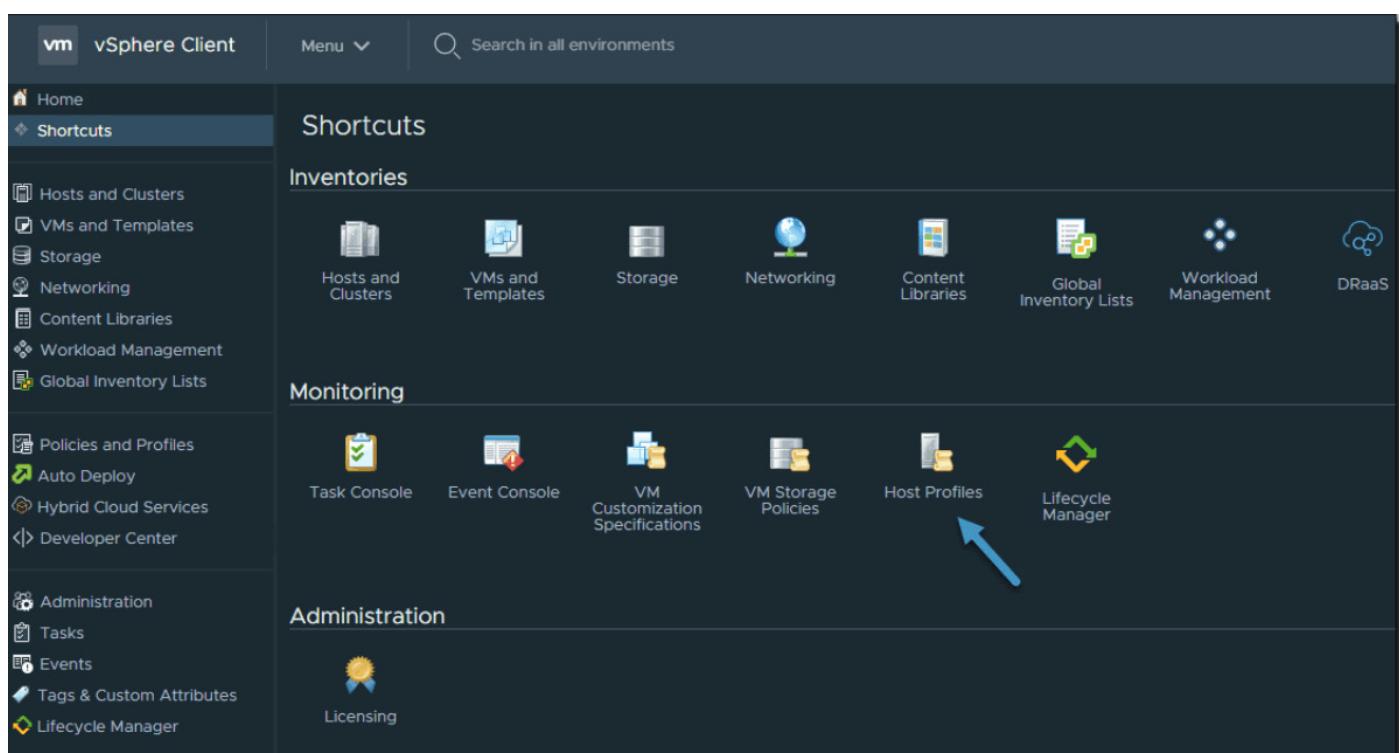
Note that Host Profiles are only included in the Enterprise Plus licensing. If you don't have Enterprise Plus, you should do a 60-day trial and create a virtual lab to see whether it would be useful for your organization or not.

## Set up and configure a reference host

In this step, which we will not cover in detail, you'll basically need to set up a reference host with all the necessary configuration. You'll install a new host and configure networking, storage, and security. We won't go too deep into these parameters as they are outside the scope of this section.

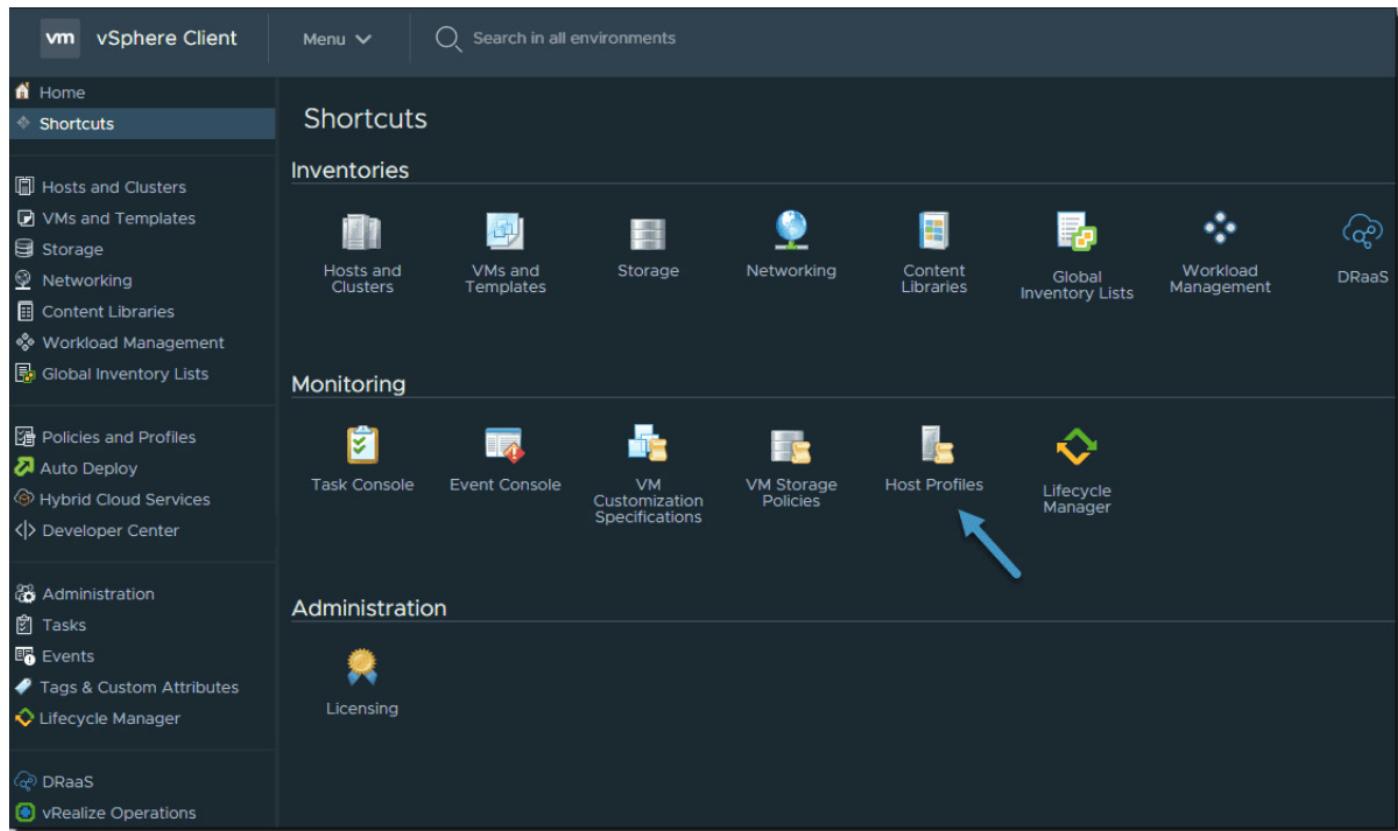
## Create a new vSphere 7 Host Profile

The best way to create a new Host Profile is to extract one **from an already configured host**. The advantage here is that you don't start from scratch. Instead, you're taking an existing config that you'll apply to the rest of the cluster. Go to Menu > Shortcuts and click the Host Profiles shortcut.



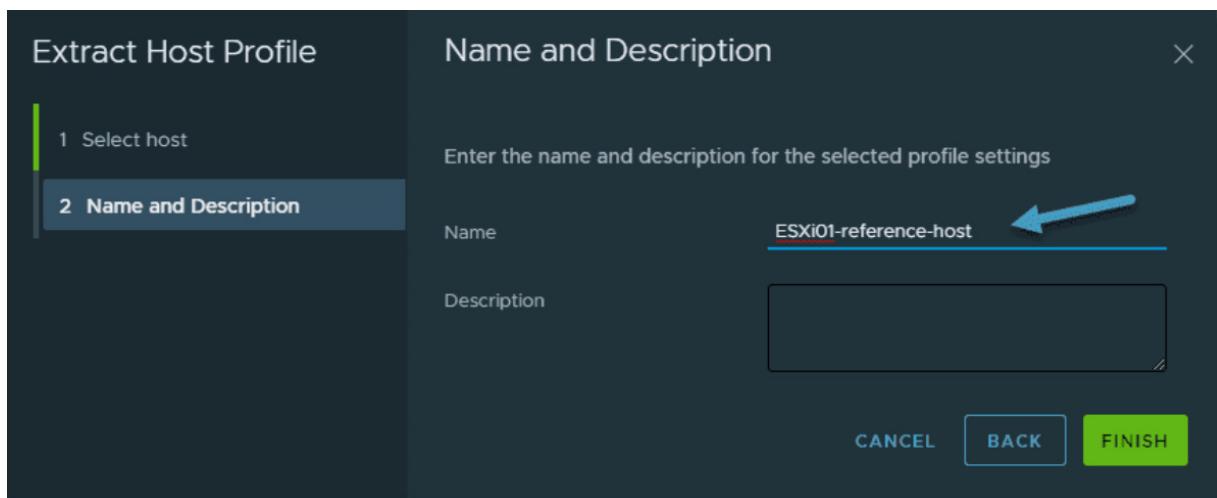
vSphere 7 Host Profiles shortcut icon

Once there, click the **Extract Host Profile** link button. On the next screen, we'll need to select the host we want to extract the profile from. This will be our reference host (source host).



vSphere 7 Host Profiles shortcut icon 1

Then simply give it a meaningful name and click the **Finish** button. It is important to correctly name your reference profile. If you're in a regulated environment, you'll probably have to respect some naming conventions. You can also add a description, where you can detail the configuration, if necessary.



Give it a meaningful name and click \_Finish

The system will start extracting and creating the profile, and after a while you should see the profile created.

That was the first part of what we have to do to successfully create and manage our ESXi 7 hosts within our cluster via Host Profiles.

Now that we have our Host Profile created, we can do many things. We can:

- Duplicate the Host Profile
- Copy settings from a host
- Copy settings to Host Profiles
- Import/export Host Profiles

The screenshot shows the vSphere Client interface with the 'Host Profiles' section selected. The left sidebar shows 'Policies and Profiles' with 'Host Profiles' highlighted. The main pane displays a table of host profiles, with one row selected for 'ESXi01-reference-host'. A blue arrow points to the 'Edit Host Profile...' option in the 'Actions' dropdown menu on the right.

Possible actions available with vSphere 7 Host Profiles

## Edit the vSphere 7 Host Profile

When you want to change the configuration of your hosts, the first step is to edit your Host Profile and apply the configuration to your hosts.

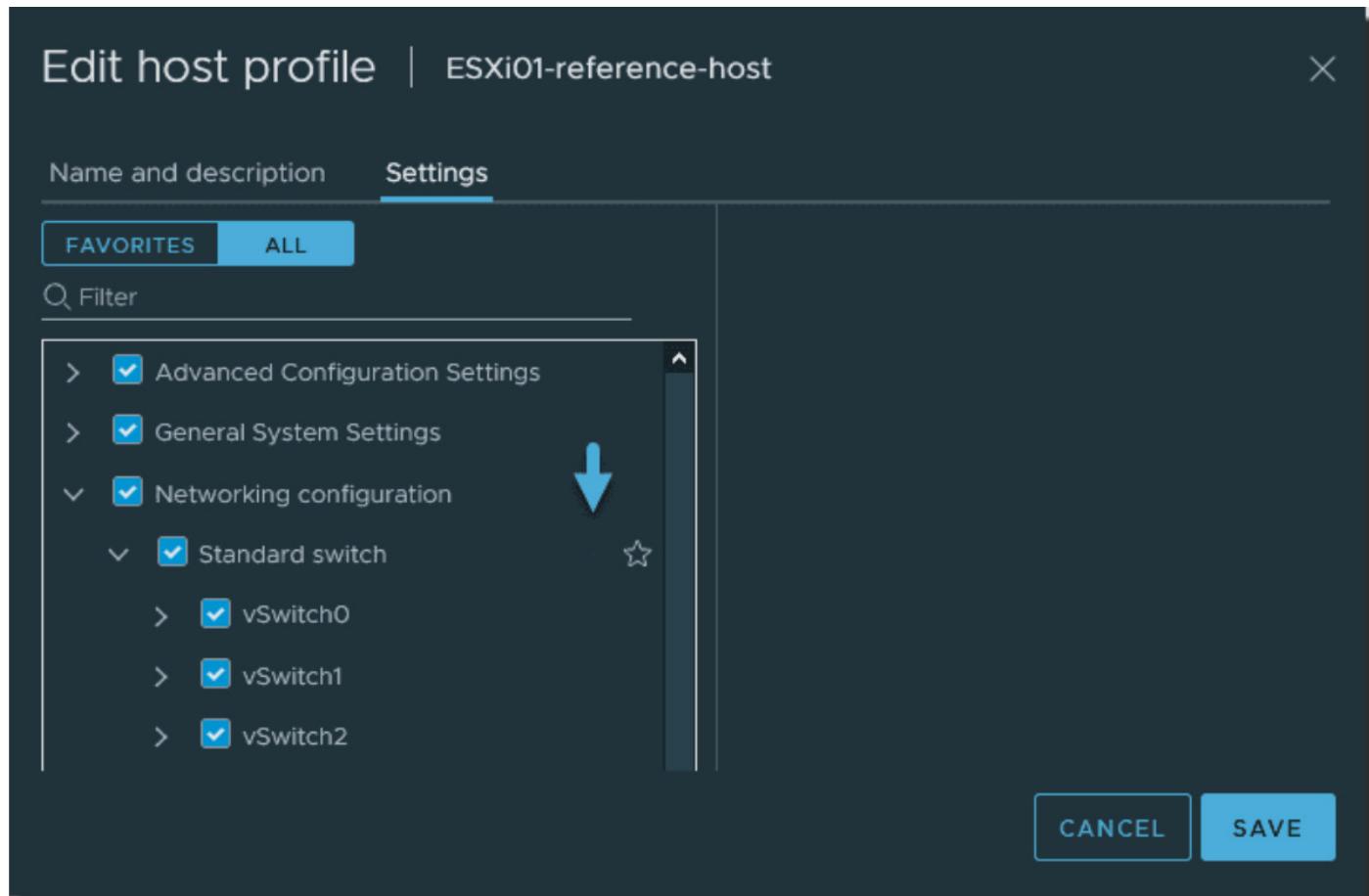
For some reason, the link to edit the Host Profile is missing on this screen, so we must click through the Host Profile. You'll see this screen where you can click **Actions > Edit Host Profile**.

The screenshot shows the vSphere Client interface with the 'Summary' tab selected for the 'ESXi01-reference-host' profile. The right pane displays host profile details and a 'Recent Compliance Failures' section. A blue arrow points to the 'Edit Host Profile...' option in the 'Actions' dropdown menu on the right.

Edit Host Profile

You can edit the existing configuration or add new configuration attributes.

For our example, we'll add another vSwitch to our profile. When you click the networking configuration > Standard switch and hover your mouse over, you'll see a green plus sign that allows you to add a component. In our case, we'll add a vSwitch.



**Click the green plus sign to create a new vSwitch**

Note that when you hover a mouse over an existing component, you can delete it.

The image shows two side-by-side screenshots of a host profile editing interface. Both screens have a header "Edit host profile | ESXi01-reference-host" and a "Settings" tab selected. On the left screen, under the "Networking configuration" section, there is a "Standard switch" entry with four vSwitches listed: vSwitch5, vSwitch0, vSwitch1, and vSwitch2. On the right screen, the same networking configuration is shown, but the "Standard switch" entry has three vSwitches: vSwitch0, vSwitch1, and vSwitch2. A large blue downward arrow is positioned between the two screens, pointing from the left configuration to the right one. In the bottom right corner of the right screen's list, there is a red "X" icon and a yellow star icon.

**When you hover a mouse you can also delete a component**

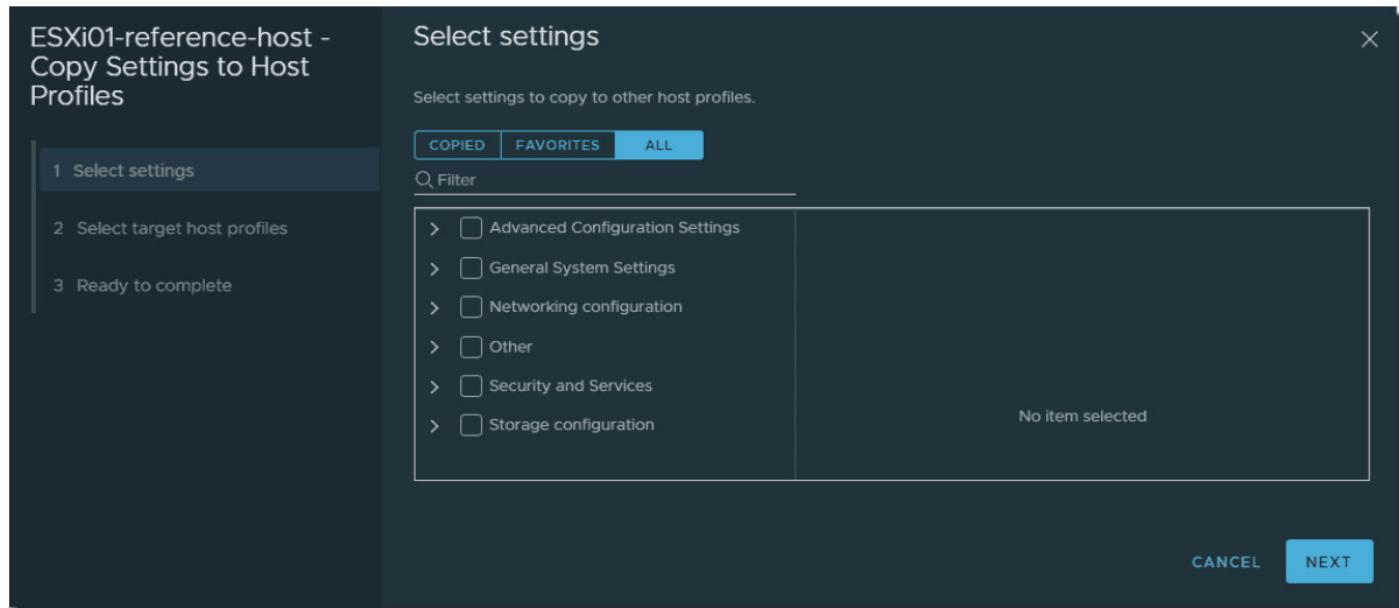
You can also add additional attributes.

When you finish editing your Host Profile, you can reapply the configuration to your hosts. Once you do, they will be automatically updated.

**Note:** If your host changed and you added some new configuration to your host, you can use the **Copy settings from host** option.

### Copy settings to Host Profile

This option allows you to modify the settings of a Host Profile from another Host Profile. You can pick a section that you want, check the box, and then update this section to your existing Host Profile.

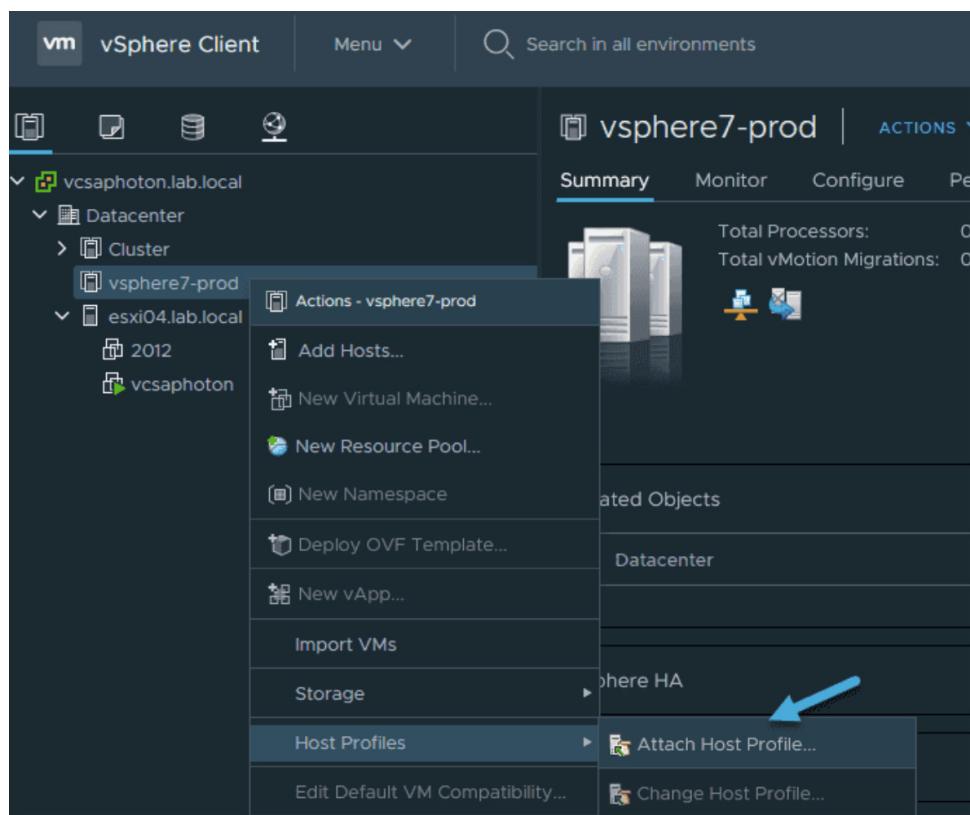


### Copy settings to a Host Profile

Then choose the destination Host Profile to apply.

### Apply a Host Profile to a host or cluster

Once you have the Host Profile created and extracted from a reference host, you can apply it to a cluster or host. Right-click the host or cluster and select **Host Profiles > Attach Host Profile**.



### Attach a Host Profile to a cluster

Pick the profile you want to attach and click OK. Now, when you select that cluster, you can see it has a profile attached.

The screenshot shows the vSphere Client interface for the cluster 'vsphere7-prod'. In the 'Host profile' section, the 'CHECK COMPLIANCE' button is highlighted with a blue arrow. Below it, a table lists hosts and their compliance status. The host 'esxi05.lab.local' is shown as 'Not Compliant' with an orange warning icon. Another blue arrow points to the 'Unknown' status next to the host name.

### Check compliance of an ESXi host in a cluster

We need to check the compliance via the **Check Compliance** button. Since the reference profile was extracted from a host that was part of a vSAN cluster, we'll most likely get some errors because we only have a single host in this cluster. In our case, this is not an issue as it was just a part of our test.

Here is how it works. When you select the check box next to the host, the lower pane shows you why it is not compliant.

The screenshot shows the vSphere Client interface for the cluster 'vsphere7-prod'. The 'Host profile' section is open, and the host 'esxi05.lab.local' is selected, indicated by a blue arrow. The status is 'Not Compliant'. Below the table, a status message says 'Status: Not Compliant, 1/24/2021, 4:57:09 PM'. A detailed list of non-compliant items is provided, categorized by setting name:

Category	Profile Path	Setting Name
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > VM Network > Network policy Configuration	Port group Configuration
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > starwindiscsi > VLAN ID configuration	Port group Configuration
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > starwindiscsi > vSwitch selection	Port group Configuration
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > starwindsync > VLAN ID configuration	Port group Configuration
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > starwindsync > vSwitch selection	Port group Configuration

### Host not compliant and details

The system will tell you exactly which part doesn't match the profile. Before you execute the remediation, you can click the **Pre-Check Remediation** button to get a preview of changes on the host.

When a host or cluster is not in compliance with the attached profile, you must remediate it. Once you remediate, you should have green everywhere, and everything should match the Host Profile configuration. You can be sure that the cluster config is the same within each of the hosts that are part of this cluster.

## Objective 4.16 Identify boot options

There are many ways to boot an ESXi 7 host from different media or from a network. The topic of boot options for VMware ESXi is one that you need to master in order to pass the datacenter certification exam. In this post, we can cover only the fundamentals.

VMware has changed the storage requirements and completely changed the partition layout in ESXi 7. VMware has increased the bootbank sizes, consolidated the system partitions and made them expandable.

The layout of system-storage boot media was changed mainly to prepare for the future, since VMware is planning to add new features and capabilities in later releases. The partition layout can now consume up to 138 GB of disk space, which limits the space available to create a VMFS datastore.

These are the media options for booting the ESXi installer:

- Boot from a CD or DVD.
- Boot from a USB device.
- Boot from a network using the Preboot Execution Environment (PXE).
- Boot from a remote location using a remote management application: HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM management module (MM), and Remote Supervisor Adapter II (RSA II).

### Boot from a CD, a DVD, or a USB device

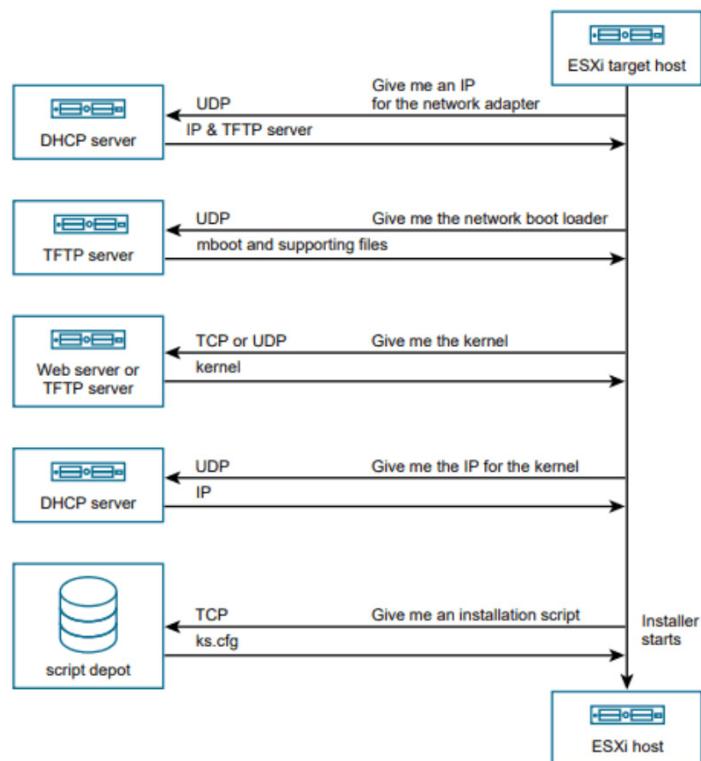
Booting from a CD or DVD is pretty straightforward. It is an interactive process in which you choose the disk or partition where you would like to install the ESXi 7 hypervisor. Other steps, like networking or password configuration, are also easy so we won't go into much detail here. You can also use a script.

You can create an installer ISO that includes the installation script. With an installer ISO image, you can execute a scripted, unattended installation when you boot the resulting installer ISO image. The installation is then completely automated.

For further details, see «VMware ESXi Installation and Setup,» a reference document that is studied to prepare for the VCP-DCV certification exam.

## Boot from PXE

In this network environment, in which you can use the TFTP server to PXE-boot the ESXi installer, you usually choose whether the target host supports a UEFI boot or just the legacy BIOS. Most environments now support UEFI, which was not always the case.



## Overview of PXE boot installation process

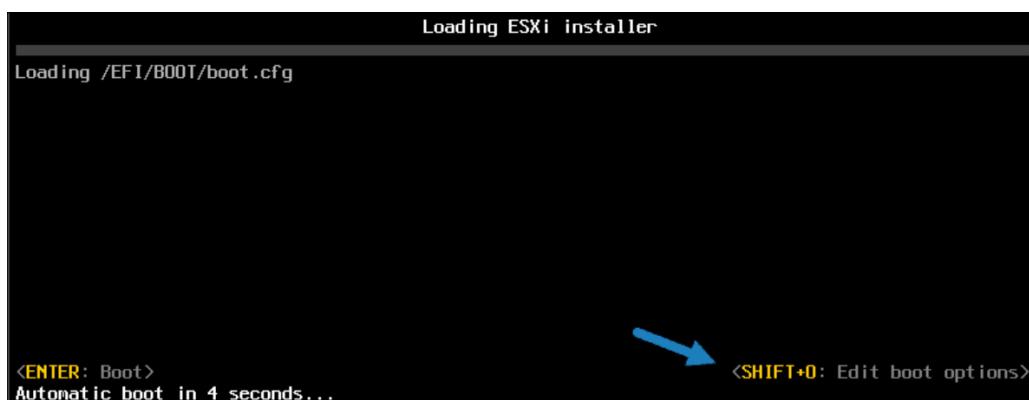
- What's happening in the background:
- The user boots the target ESXi host.
- The target ESXi host makes a DHCP request.
- The DHCP server responds with the IP information and the location of the TFTP server.
- The ESXi host contacts the TFTP server and requests the file that the DHCP server has specified.
- The TFTP server sends the network boot loader, and the ESXi host executes it. There is an additional boot loader that can be loaded after the initial boot; it is also from the TFTP server.
- The boot loader searches for a configuration file on the TFTP server, downloads the kernel and other ESXi components from the HTTP server or the TFTP server, and boots the kernel on the ESXi host.
- The installer runs interactively or by using a kickstart script, as specified in the configuration file.

This, in essence, is all the magic of the process.

## Scripted ESXi 7 installation

ESXi Installation scripts provide an efficient way to deploy multiple hosts and to deploy hosts remotely. You can use an installation script that includes the settings for installing ESXi. The script can be applied to all of the hosts that need to have the same configuration. Only supported commands can be used in the installation script. This script can be modified to specify settings that need to be unique for each host. The installation script can be stored on an FTP server, an HTTP or HTTPS server, an NFS server, or a USB flash drive.

To start the installation script, enter boot options at the ESXi installer boot command line. At boot time, press **Shift+O** in the boot loader, enter boot options, and access the kickstart file.



**Press Shift plus O during the boot process**

If you are using a PXE boot to install, options can be passed through the **kernelopts** line of the **boot.cfg** file. The location of the installation script is set with the **ks=filepath** option, where filepath is the location of the kickstart file. If ks=filepath is not included in the script, the text installer is executed.

For example, at the runweasel command prompt, you could enter ks= along with the path to the installation script and the command-line options. You could enter the following options to boot the host from a script named esxi-script residing on the server 192.168.1010.10 and

set the IP address of the host to 192.168.100.101:

```
ks=http://192.168.100.10/kickstart/esxi-script.cfg  
nameserver=192.168.1.100 ip=192.168.100.101  
netmask=255.255.255.0 gateway=192.168.100.101
```

Check the documentation to see all the different options. There is a default installation script included with the ESXi installer that can be used to install ESXi onto the first disk that is detected.

## Using Auto Deploy

VMware vSphere Auto Deploy makes it possible to install ESXi 7 on hundreds of physical hosts. By using Auto Deploy, experienced administrators can manage large environments efficiently. However, your vCenter server needs to be up; otherwise, Auto Deploy does not work.

ESXi 7 hosts use network booting to boot from a central Auto Deploy server. Hosts can be configured with a host profile created from a reference host. This host profile can be created to prompt for input. After the hosts boot and are configured, they are managed by vCenter Server, as other ESXi hosts are.

Auto Deploy can be configured for either stateless caching or stateful installations:

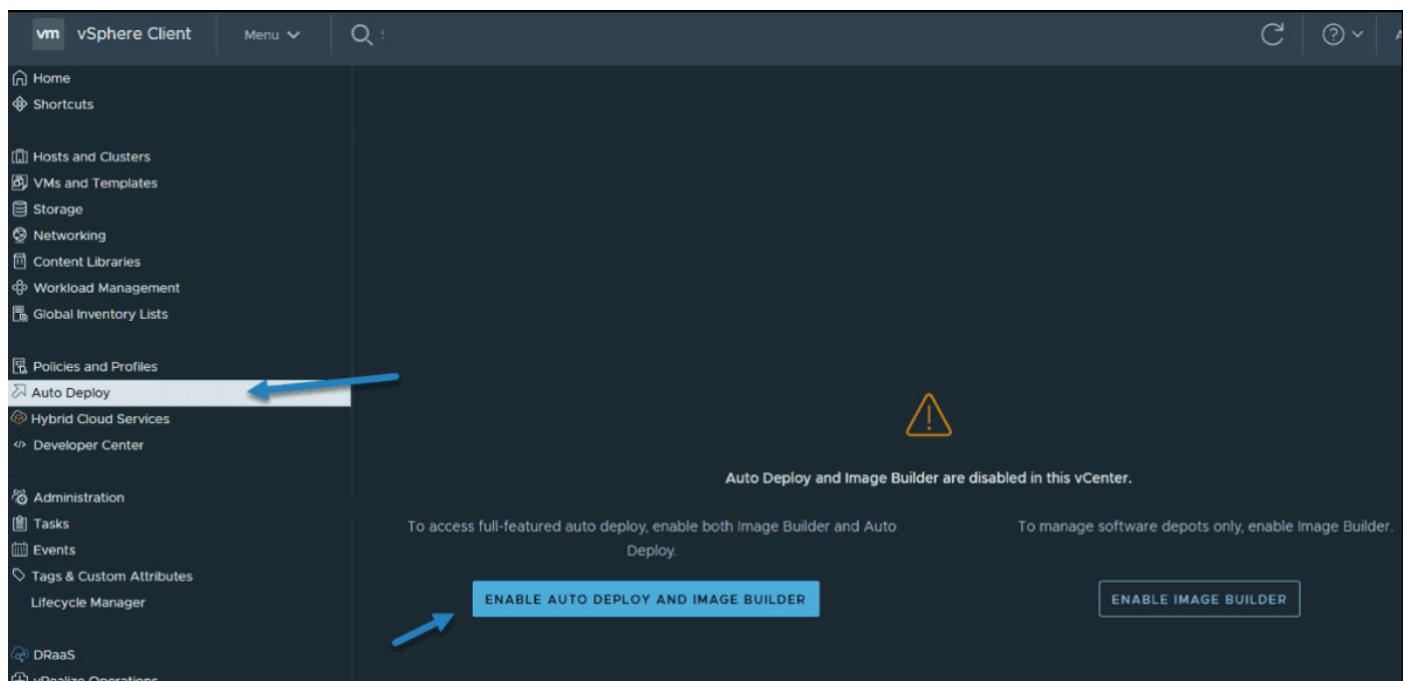
**Stateless caching.** Auto Deploy does not store ESXi config or state data within the host (which is why it is «stateless»). Auto Deploy uses image profiles and host profiles to maintain the host configuration.

If a network boot fails, the ESXi host can use a local cache to boot from the last known ESXi 7 image.

**Stateful installations.** Auto Deploy is used to boot the host, but the installation and configuration are written to a local disk. During boots, the host **boots from the local disk** where this host configuration is stored.

Auto Deploy can be configured and managed using a graphical user interface (GUI) in vSphere 6.5 and later.

There is also a PowerCLI method, but the GUI option is easier to use. You must activate Image builder and Auto Deploy services (which are disabled by default) within the vSphere client.



Enable Auto Deploy and Image Builder in vSphere 7

The Image Builder feature in the GUI enables you to download ESXi images from the VMware public repository or to upload ZIP files containing ESXi images or drivers.

You can customize the images by adding or removing components, and you can export images to ISO or ZIP files for use elsewhere.

You can compare two images to see how their contents differ. Use the **Deployed Hosts** tab to view hosts that are provisioned with Auto Deploy and to perform tests and remediations.

The screenshot shows the vSphere Client interface with the 'Auto Deploy' option selected in the left sidebar. The main content area displays three configuration sections: 'Auto Deploy Runtime Summary (Read-only)', 'VMware Auto Deploy Service', and 'VMware Image Builder Service'. The 'Auto Deploy Runtime Summary' section lists various parameters with their values. The 'VMware Auto Deploy Service' and 'VMware Image Builder Service' sections show configuration tables with parameters like 'cacheSize\_Gb', 'loglevel', and 'httpPort'.

Parameter	Value
Proxy Servers	none
BIOS DHCP File Name	unidrivenpxe.vmw-hardwired
UEFI DHCP File Name	snpnonly64.efi.vmw-hardwired
UEFI Secure Boot File Name	snpnonly64.efi.vmw-hardwired officialkey
iPXE Boot URL	https://192.168.1.32:6501/vmw/rbd/tramp
Runtime Cache Size	2.00 GiB
Cache Space In-Use	8 MiB

Parameter	Value
cacheSize_Gb	2
managementport	6502
loglevel	INFO
serviceport	6501

Parameter	Value
cacheSize_Gb	2
loglevel	INFO
httpPort	8099
vmomiPort	8098

**Auto Deploy and Image Builder configuration screen**

## Conclusion

Previous releases of vSphere included only the PowerCLI option for configuring Auto Deploy. But in vSphere 6.5 and vSphere 7, the Auto Deploy and Image Builder options are visible in the GUI, allowing you to create custom ISOs from which you can then boot ESXi 7 hosts on your network.

## Objective 4.16.1 Configure Quick Boot

Covered on Page 88.

## Objective 5.1 Identify Resource pools use cases

vSphere 7 resource pools are an integral part of clustered environments. They allow you to create different compartments within your cluster and delegate control over a cluster's resources.

Many new vSphere admins do not use resource pools because they seem complicated at first; however, they're part of vSphere. Moreover, this topic is required to pass the VCP-DCV VMware certification exam. In fact, the VCP exam has several sections on resource pools and resource management.

VMware vSphere 7 uses resource pools to separate and compartmentalize all resources in a cluster. A resource pool is a logical abstraction for the flexible management of resources, allowing you to create a hierarchy within your environment. Each part of this hierarchy can have different amounts of CPU or memory resources assigned from the total available within your cluster.

A resource pool can have child resource pools, such that each child receives part of the parent's resources. Child resource pools are smaller units compared to parents. A resource pool can contain other resource pools, as well as individual virtual machines (VMs).

The main advantage of managing resources via resource pools is that you do not need to set resources on each virtual machine individually. Instead, you can control the aggregate allocation of resources to the set of virtual machines by changing the settings on their enclosing resource pool.

vSphere 7 offers a new feature with resource pools. It is a new checkbox called **Scalable shares**.

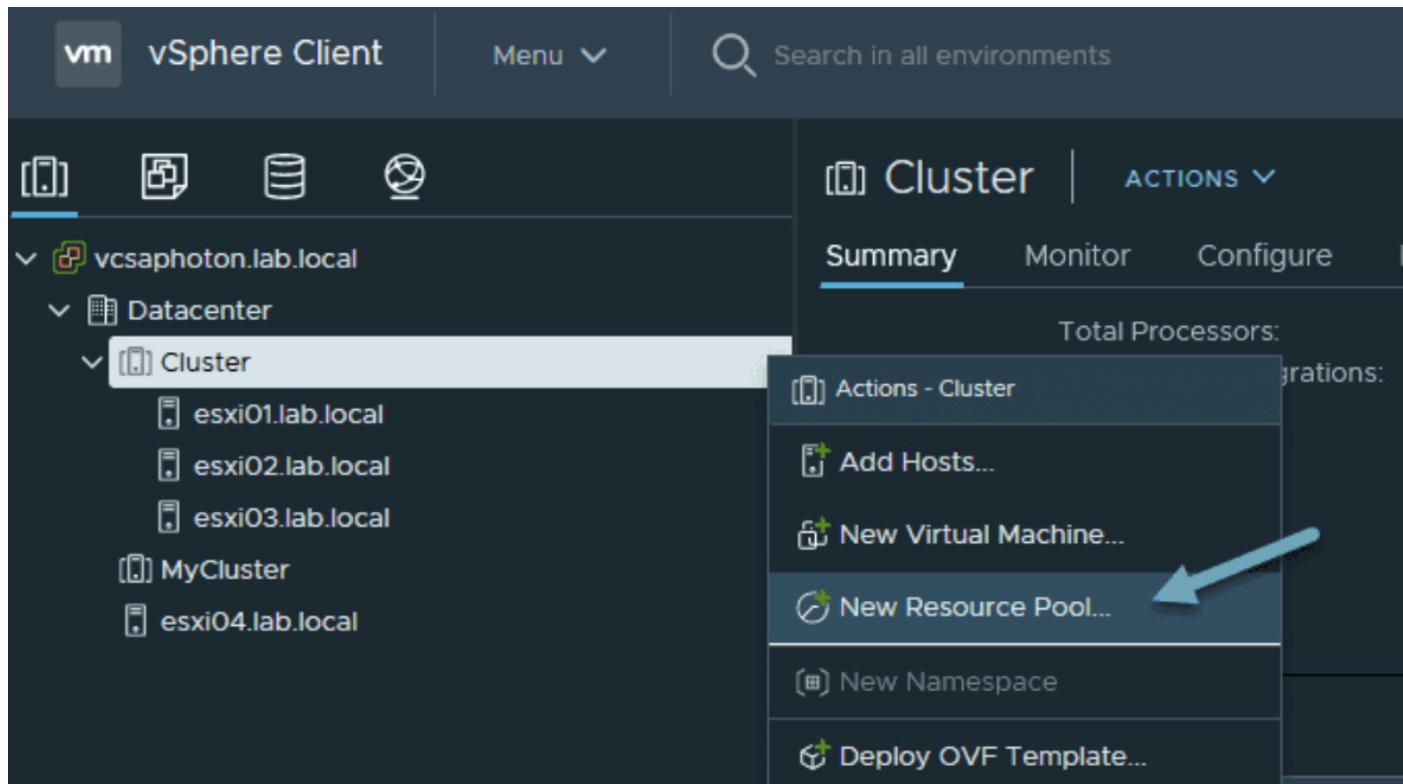
If you have more VMs that are provisioned in a resource pool, VMware vSphere 7 with scalable shares activated recalculates the entitlement for all the workloads running inside the resource pool. Scalable shares are dynamic.

In this section we'll cover the basics of resource pools, their usage, examples, and configuration. vSphere 7 resource pools enable the separation of resources from hardware. You can use them to manage resources independently from the actual hosts that contribute to the cluster.

### Where should vSphere 7 resource pools be created?

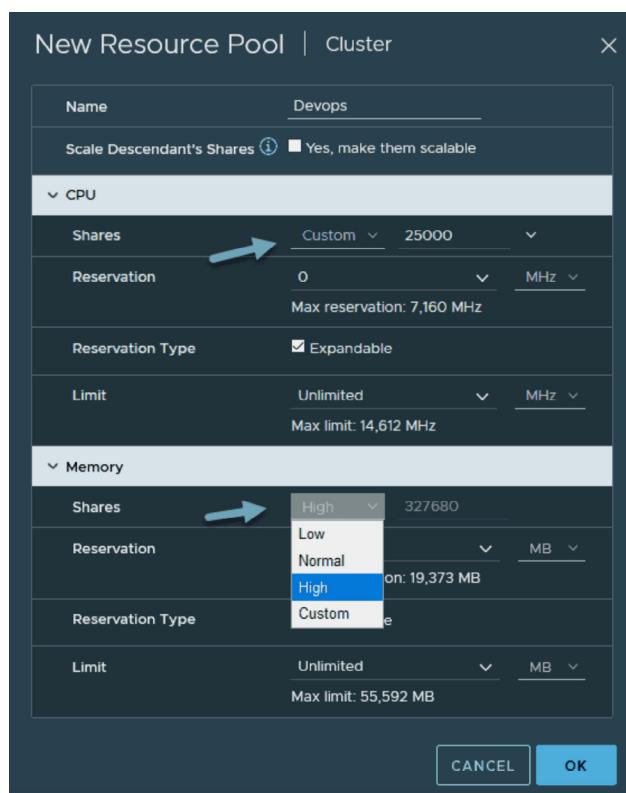
Right-click your cluster and choose **New Resource Pool** from the menu. Note that resource pools are a part of vSphere Enterprise or Enterprise Plus licensing.

To proceed, you'll need to meet a few requirements. You must have **DRS enabled** on your cluster.



### Create a new resource pool

On the next page, you'll need to give your resource pool a meaningful name and choose what CPU and memory allocation you would like to have.



### Configure CPU and memory in your resource pool

**Shares** — The Shares value indicates which virtual machine will request resources with which priority if there is a shortage of resources on an ESXi host. By default, the Shares value is 1000, but you can increase it. If you increase it, the virtual machines in this resource pool will start to prioritize the use of CPU resources, as follows: Low (2000), Normal (4000), High (8000) or custom.

**Reservation** — A virtual machine needs CPU and memory resources to run. If you do not want to be affected by the resource bottleneck on the ESXi server, you need to make a resource reservation.

**Expandable Reservation** — If the reserved resources are not provided, the virtual machine cannot be started. If this option is selected, even if there is no resource in the resource pool, you can use the resources of the resource pool located above it and power on the virtual machine.

**Limit** — If you set a limit for a resource pool, you can never exceed that limit. I do not recommend that this setting be used in a production environment. For example, if the virtual machine has 2 GHz usage and you set the limit to 1 GHz, this resource will never, ever exceed 1 GHz.

**Unlimited** — This option should always be checked if you are not setting a limit. It indicates that there is no limit on the amount of CPU you have allocated.

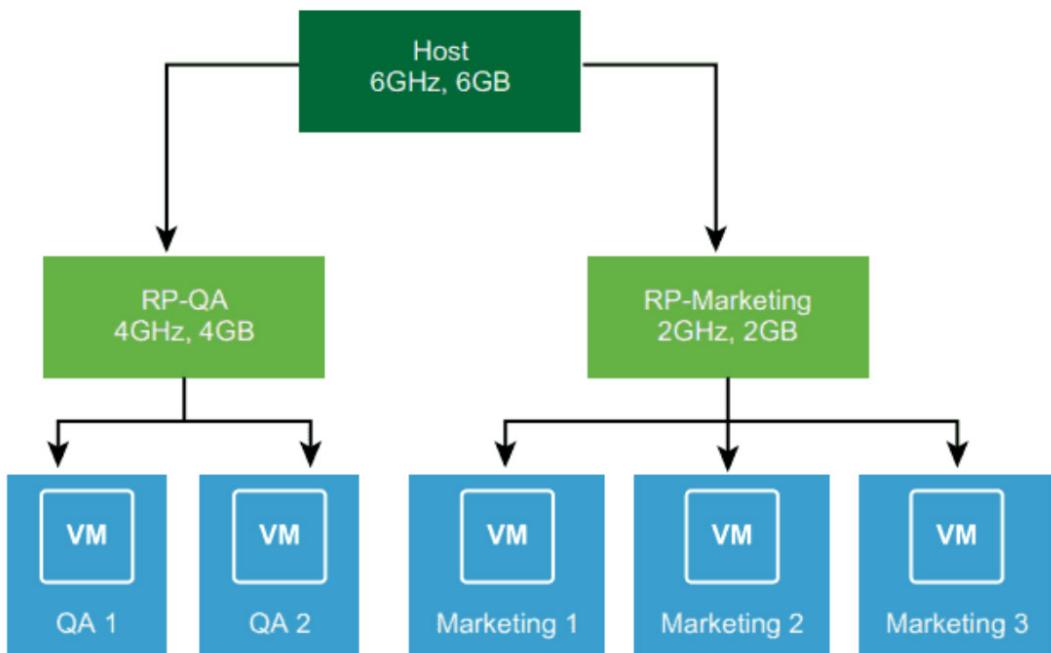
### What are some use cases for using a resource pool?

You might have more than one database and IIS servers in your infrastructure. Let's assume that you create a resource pool named Database and add Database servers into it. You can then create a resource pool named IIS and add your IIS-related virtual machines to it. This way, you can perfectly allocate how much of the overall cluster resources would be available for your Database resource pool and how much for your IIS resource pool.

You might also have VMs that are a part of different departments, such as Human Resources (HR), DevOps, CAD Design, Machine Learning etc. Each department might have different requirements when it comes to performance. For example, the Machine Learning VMs might need a lot compared to HR, and so on.

One example from the VMware documentation is where two different departments use a resource pool. The QA department needs more CPU. The admin simply **sets the CPU shares to High** for this resource pool and to **Normal** for the Marketing resource pool. This is the simplest example.

Resource pools are container objects in the vSphere 7 inventory, and they help create compartments. Each compartment has its own CPU and memory settings set as a percentage of the overall cluster resources. A delegation can be created within vSphere 7, as resource pools are objects.

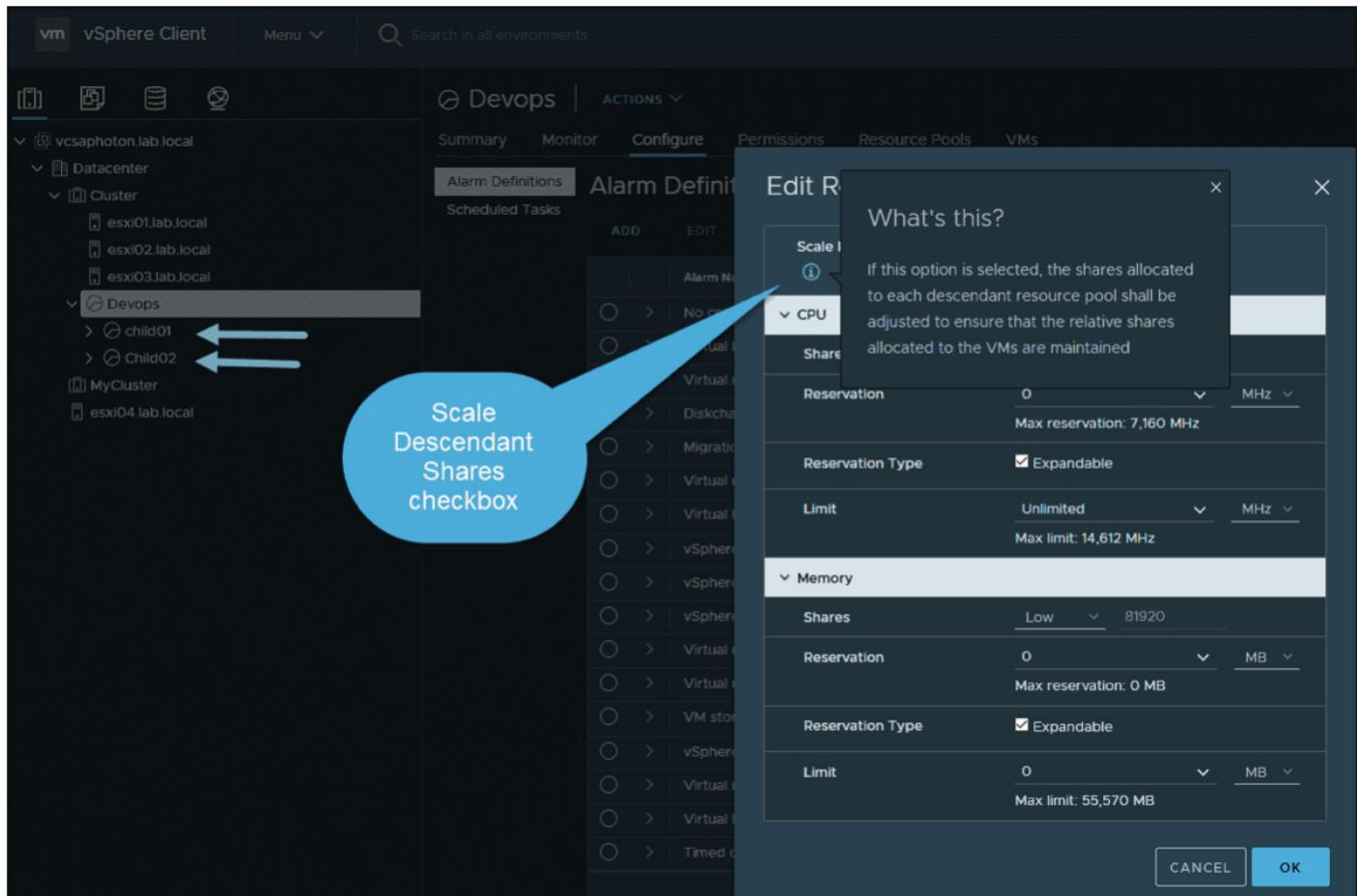


**Example of vSphere 7 resource pool**

There are also more complex cases, especially with a child resource pool. There is a checkbox called Scale Descendant Shares when you have a parent resource pool.

The **Scale Descendant Shares** option allows the shares allocated to each descendant resource pool to be adjusted to ensure that the relative shares allocated to the VMs are maintained. With scalable shares, the allocation for each pool factors in the number of objects in the pool. You can add/remove objects or VMs, and the shares for each object are adjusted automatically.

Note that this wasn't the case in previous releases of vSphere, where resource pools were only static.



Scale Descendant Shares option

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

When you do over-provisioning on an ESXi host on memory and CPU, you basically need a tool that makes sure that the VMs get the correct amount of resources. Let's say we have a VM that needs to get 3500MHz (Reservation) and make sure that another VM for testing never gets more than 1000MHz (Limit).

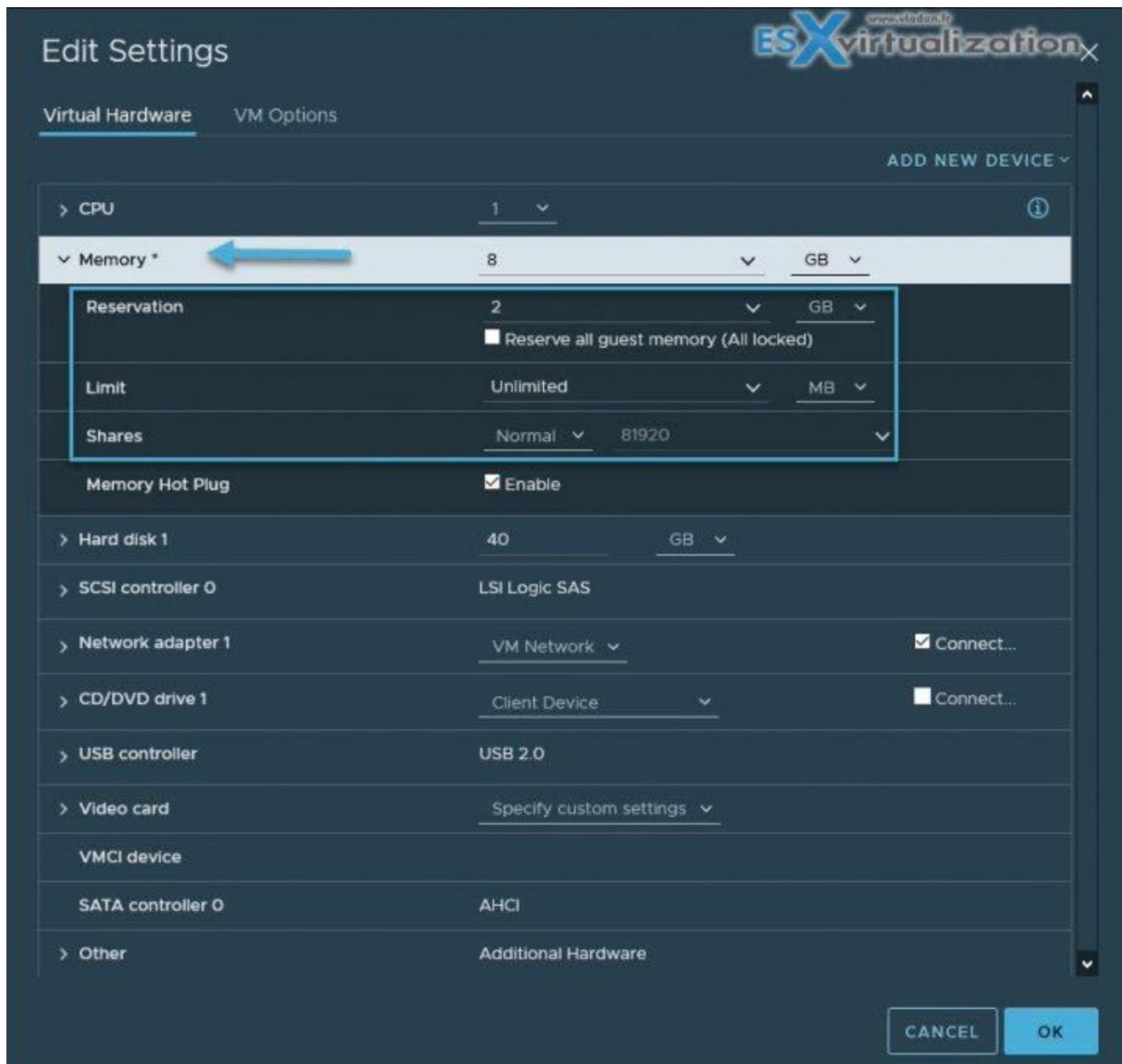
The basic understanding of reservation and limits will allow you to better understand the mechanism which vSphere uses to run your VMs. This topic is also necessary for you to pass your VCP certification exam.

**Reservations** is a resource guarantee on CPU or Memory for a VM. When you set a reservation, you basically guarantee that a particular VM gets this over a VM which does not have this reservation. You define reservation in MB or MHz depending on which resource you make reservations for.

Example 1: You have a virtual machine **configured with 4 GB** memory and you configure a **2 GB reservation**. When the virtual machine powers on, a 2 GB swap file (.vswp) is created on a

datastore. The 2 GB reservation guarantees that the VM will always at least get 2 GB of physical memory. If the ESXi host is running low the remaining 2 GB can come from the swap file on disk.

Example 2: You have a virtual machine **configured with 8 GB** memory and you configure a **8 GB reservation**. When the virtual machine powers on, a swap file with zero in size is created. The 8 GB reservation guarantees that the VM will get ALL its memory from physical memory and it will never do hypervisor swapping or ballooning.

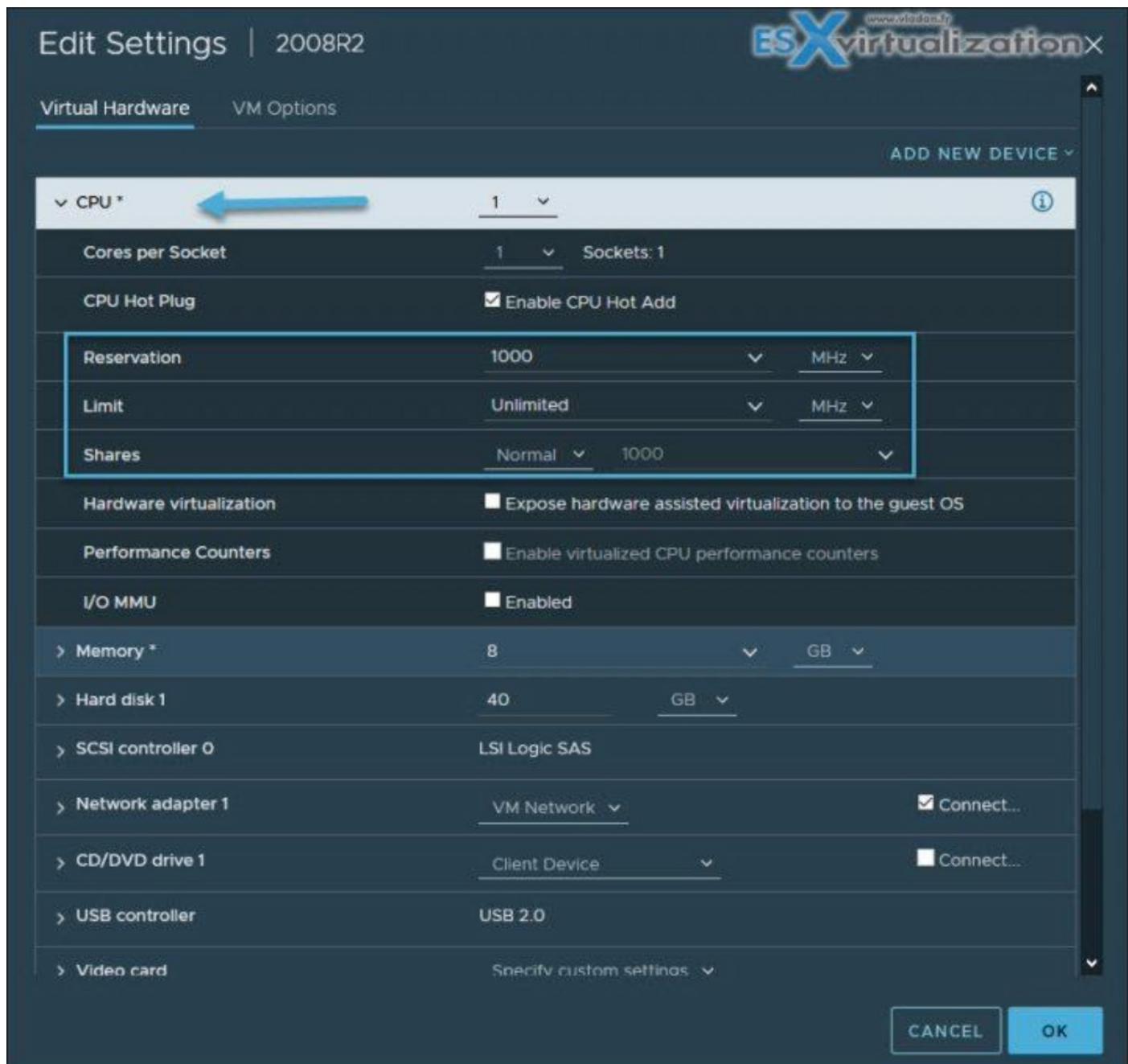


That wraps it up for memory.

For a **CPU**, you basically guarantee the clock cycles. You guarantee the reservation in MHZ. Let's say you give a VM a reservation. It basically means that the vmkernel CPU scheduler will

give it at least that amount of resources. If a VM is not using its resources, the CPU cycles are not wasted on the physical host.

Other machines can use it as well. Here's how it works: when you set CPU reservations, the system is making sure that a VM will always get access to the physical CPU in an over-committed environment.



## Limits

You set a limit - the VM will never use more than you set on the limit for memory or CPU. It's pretty restrictive and the opposite compared to a reservation. If you set the limit lower than the configured memory for a VM, the particular VM will swap and balloon to have enough memory to run. But the performance will struggle, obviously.

Let's say that you have a VM which is **configured with 8 GB** memory and you configure a **2 GB limit**. The VM guest OS will see 8GB of RAM, but the ESXi is not allowed to give it more than 2 Gigs of its physical RAM. When the VM will ask for more memory for running some apps, you'll see ballooning and swapping start happening.

When you set a limit for CPU, you basically limit the performance of a VM even if the ESXi has more than enough capacity on its CPU.

**Shares** - Shares define how much access you get to a resource compared to something else. Every virtual machine has 1000 shares configured per vCPU by default, which means you are already using them. All VMs are equal from a hypervisor perspective unless you change the shares and tell it which machines are actually more important. What is important to know about shares is that they should only be used in the case of contention. If you have enough capacity available for all machines, it does not help performance-wise to increase the shares on some machines.

Let's have a look at some examples.

Let's say that we have a VM (we'll call it a VM01) that has 1000 shares and another one, VM02, which also has 1000 shares. They are both **competing** for the same physical CPU core. In this particular case, the ESXi CPU scheduler will give each machine 1/2 (50%) access and they will have the exact same performance.

Now, let's say that we have changed the config so that VM01 has 3000 shares and VM02 has 1000 shares, and they are still **competing** for the same physical CPU core. We will see that VM01 gets 3/4 (75%) access and VM02 gets **only 1/4** (25%) access.

Let's change the config again so that our VM01 has 3000 shares and VM02 has 1000 shares, only this time they are **not competing** for the same physical CPU core. In this case, both machines will get 100% access to the physical CPU. It is because shares are only applied when we have a contention.

## Objective 5.2 - Monitor resources of vCenter Server Appliance and vSphere environment

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

VCSE is composed of Photon OS, PostgreSQL database, and vCenter server application. Feature parity was a goal for VMware for several vSphere releases. The Linux-based appliance has HTML5 management of all functions of that Flash-based client. The vCenter on Windows



is still possible in vSphere 6.7 but it is the last release.

Services can be restarted within the UI as well.

Some predefined firewall

Right after logging into the management interface of VCSA through port 5480 you get the overview of the health status. You can see whether the components (CPU, memory, database, storage swap) are in good condition. If there's an issue with any of those, you'll see a yellow icon.

The connection to VCSA management: [https://ip\\_or\\_fqdn:5480](https://ip_or_fqdn:5480)

Here is the summary tab view.

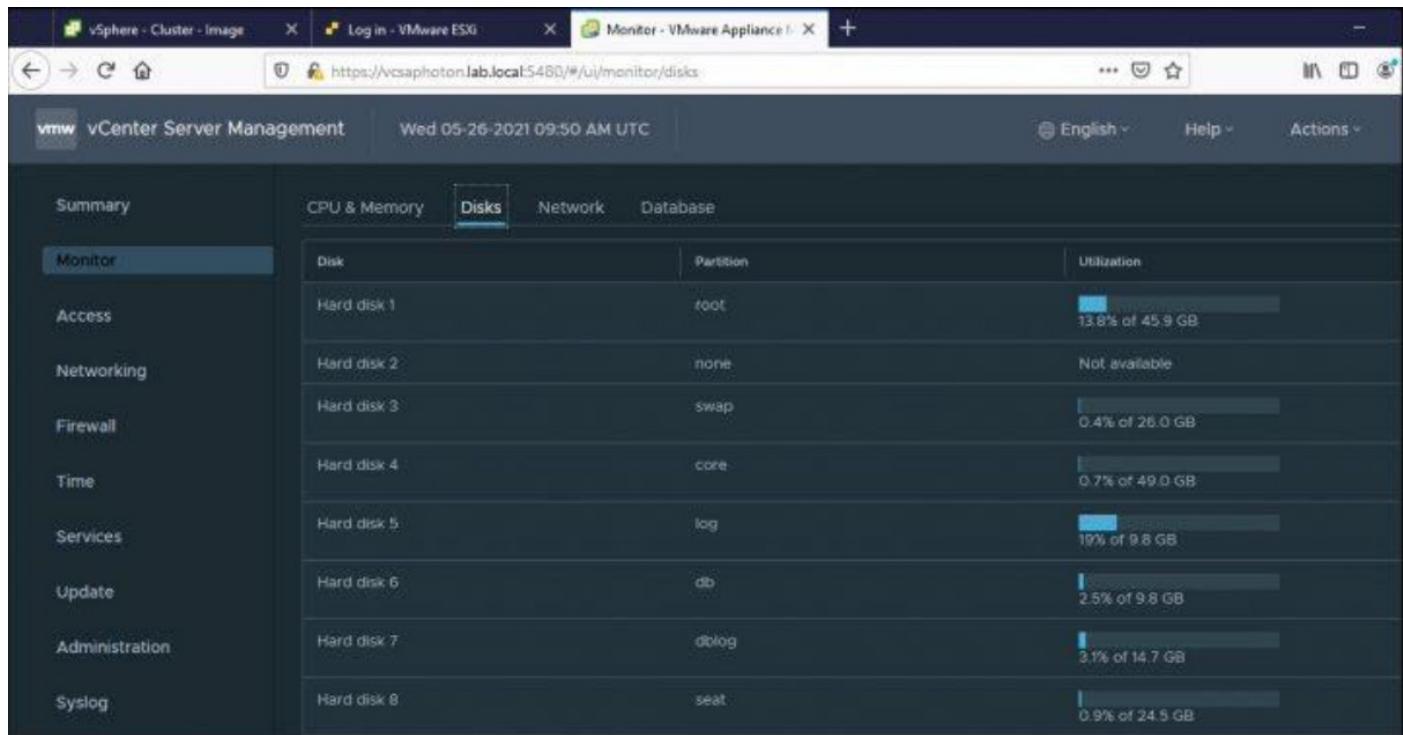
The screenshot shows the vCenter Server Management interface. On the left, a sidebar lists various tabs: Summary (selected), Monitor, Access, Networking, Firewall, Time, Services, Update, Administration, Syslog, and Backup. The main content area has a dark header bar with the title 'vCenter Server Management', the date 'Wed 05-26-2021 09:48 AM UTC', and user information 'root'. Below this is a 'Health Status' section with a table:

Health Status	
Overall Health	<span>Good</span> (Last checked May 26, 2021, 1:47:58 PM)
CPU	<span>Good</span>
Memory	<span>Good</span>
Database	<span>Good</span>
Storage	<span>Good</span>
Swap	<span>Good</span>

On the right, there is a 'Single Sign-On' section with a table:

Domain	vsphere.local
Status	Running

After clicking the **Monitor** menu, you'll get full details of each option. This menu item has all the monitoring information you need: CPU, Memory, Disks, Network and Database. With the improvement of 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.



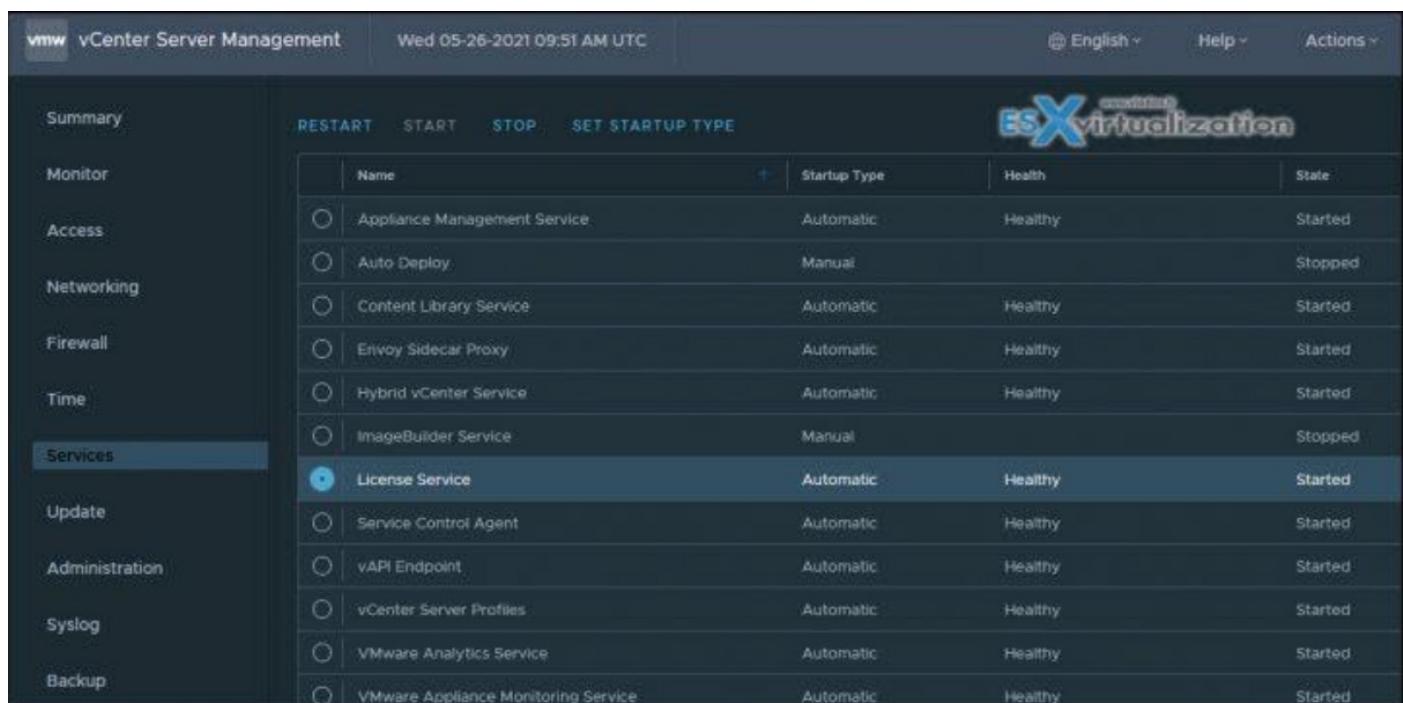
The screenshot shows the vCenter Server Management interface with the 'Monitor' tab selected. Under the 'Disks' section, a table lists eight hard disks with their utilization levels. Hard disk 1 is at 13.8% of 45.9 GB. Hard disk 2 is not available. Hard disk 3 is at 0.4% of 26.0 GB. Hard disk 4 is at 0.7% of 49.0 GB. Hard disk 5 is at 19% of 9.8 GB. Hard disk 6 is at 2.5% of 9.8 GB. Hard disk 7 is at 3.1% of 14.7 GB. Hard disk 8 is at 0.9% of 24.5 GB.

Disk	Partition	Utilization
Hard disk 1	root	13.8% of 45.9 GB
Hard disk 2	none	Not available
Hard disk 3	swap	0.4% of 26.0 GB
Hard disk 4	core	0.7% of 49.0 GB
Hard disk 5	log	19% of 9.8 GB
Hard disk 6	db	2.5% of 9.8 GB
Hard disk 7	dblog	3.1% of 14.7 GB
Hard disk 8	seat	0.9% of 24.5 GB

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%

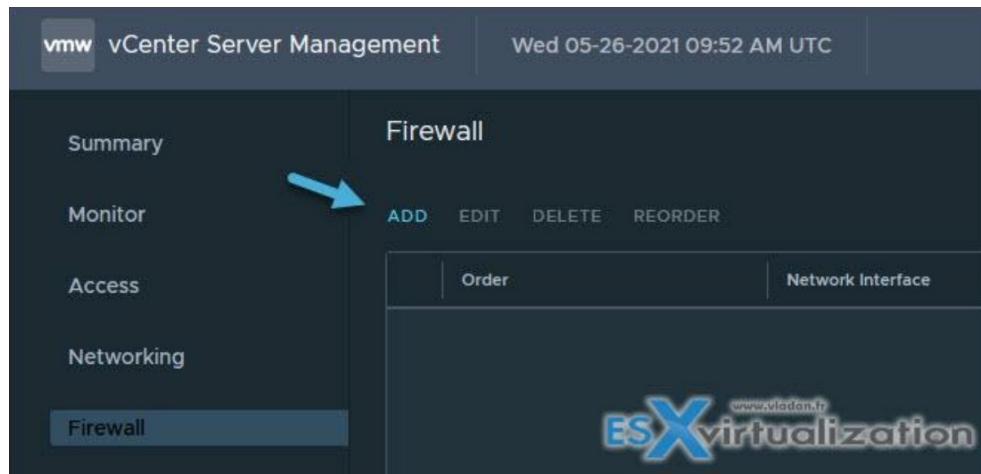
The services Menu provides us with a possibility to manage VCSA services. We can start, stop or restart individual services or sort individual columns.



The screenshot shows the vCenter Server Management interface with the 'Services' tab selected. A table lists various VCSA services with their startup types and health status. The 'License Service' is highlighted with a blue circle.

	Name	Startup Type	Health	State
Appliance Management Service	Automatic	Healthy	Started	
Auto Deploy	Manual		Stopped	
Content Library Service	Automatic	Healthy	Started	
Envoy Sidecar Proxy	Automatic	Healthy	Started	
Hybrid vCenter Service	Automatic	Healthy	Started	
ImageBuilder Service	Manual		Stopped	
<b>License Service</b>	Automatic	Healthy	Started	
Service Control Agent	Automatic	Healthy	Started	
vAPI Endpoint	Automatic	Healthy	Started	
vCenter Server Profiles	Automatic	Healthy	Started	
VMware Analytics Service	Automatic	Healthy	Started	
VMware Appliance Monitoring Service	Automatic	Healthy	Started	

**Firewall Management** - VMware VCSA allows you to create custom rules. To do that, you need to access the firewall via the menu on the left, navigate to **Firewall**, then click the **Add** menu button to add a new rule.

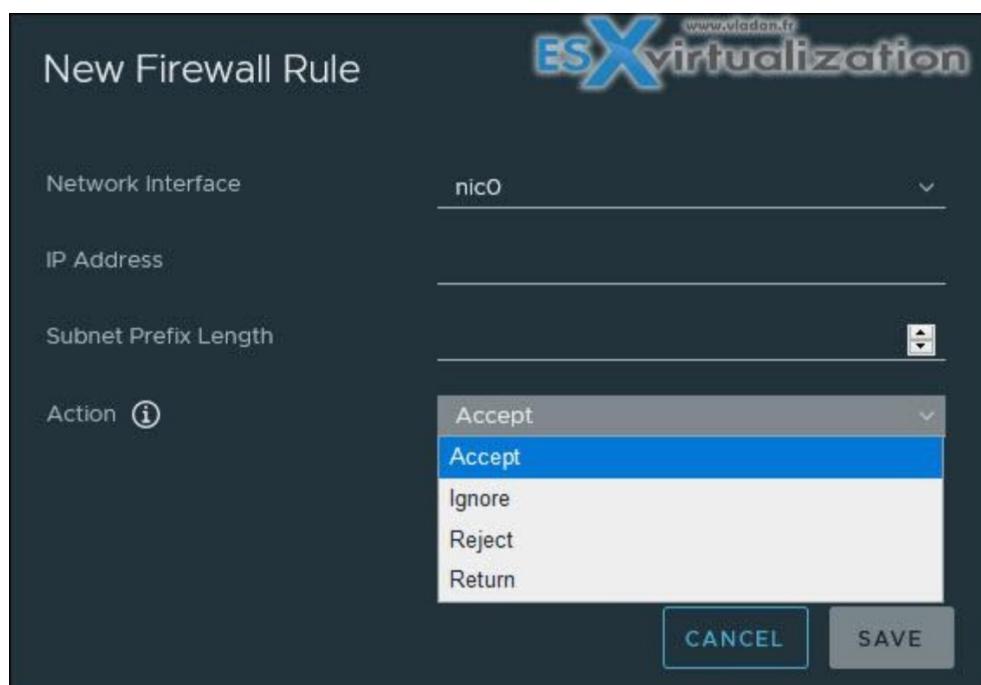


You'll see an overlay pop-up window appear inviting you to fill certain details.

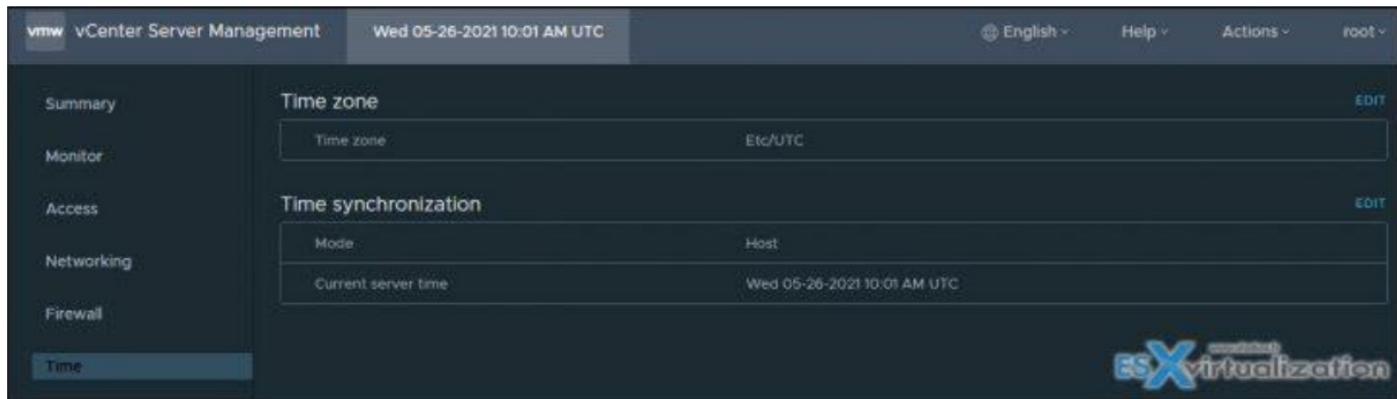
These include:

- **Network Interface** – a drop-down menu allowing you to choose 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 reject traffic

and 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 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 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 and use tools for performance monitoring

VMware vSphere 7 offers several built-in tools and utilities to monitor performance. You can use the vSphere client performance charts where you can view the compute, network, or storage resource usage for your VMs, hosts, and clusters. If you want to look deeper, tools such as the ESXTOP command line utility can give you better insights.

vSphere 7 also has many prebuilt alarms that can notify you of a problem that needs to be resolved, like low resource availability on your host, cluster, or datastore. Storage has often been and still is the place where you'll find the most bottlenecks or space problems on the datastore, causing VMs to be in a suspended state.

If you're part of a larger organization, you should definitely consider the vRealize Operations (vROPs) product suite, which offers more than just monitoring. You can spot resource consumption during the specified period, or you can intelligently automate workload management based on current conditions.

## vSphere 7 client performance charts

The built-in charts in the vSphere 7 UI can be viewed and accessed via a web browser, and you can see performance metrics in different types of charts depending on the selected object and metric type.

**Line chart** — Shows metrics for a single inventory object. The data for each metric is represented by a separate line.

**Bar chart** — Shows metrics for objects where each bar is a metric for an object.

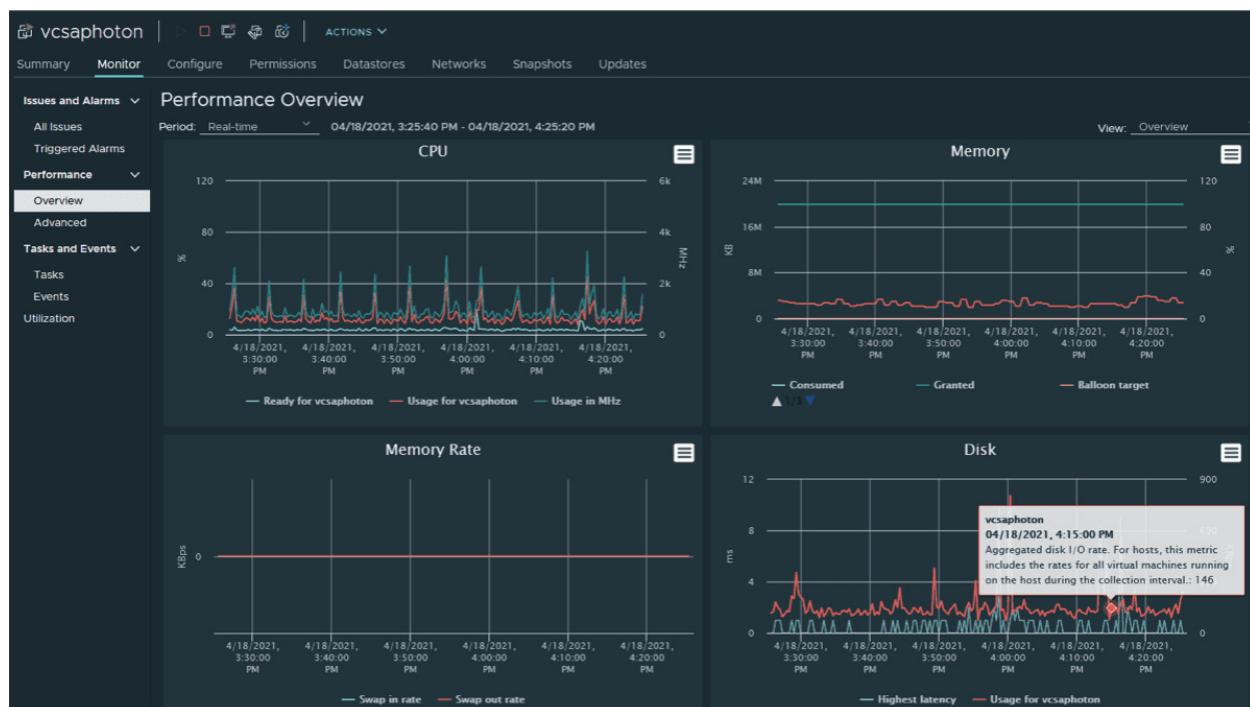
**Pie chart** — Shows metrics for a single object, such that each slice represents a category or child object. An example here would be a pie chart that shows the amount of storage space occupied by each virtual machine or by each file type.

**Stacked chart** — This type of chart displays metrics for child objects.

Different overviews and advanced performance charts exist for data centers, clusters, hosts, resource pools, vApps, and virtual machine objects.

It is also possible to display overview performance charts that are available for datastores and datastore clusters. Performance charts, however, are not available for network objects. All charts are organized into views, which you can use to see related data together on one screen.

The vSphere 7 client performance charts are easily accessible. In the vSphere client, select an appropriate object (a VM in our case) in the inventory pane and navigate to **Monitor > Performance > Overview**. Then select a predefined or custom time range.



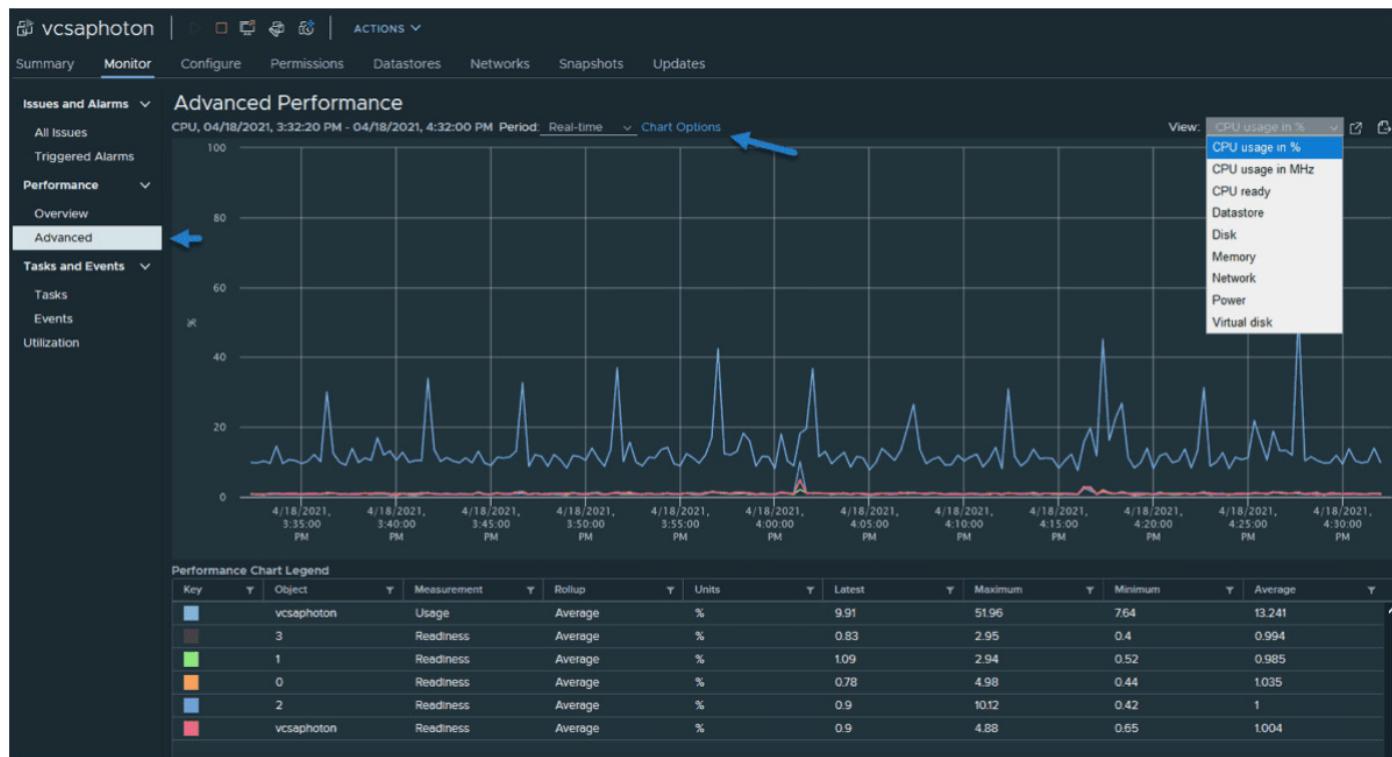
vSphere 7 performance charts

## Advanced performance charts

If you want more granular views, you can use advanced performance charts or create your own custom charts. You can also include data counters that are not integrated in other general performance charts. You can hover over a data point to see details at that point.

The charts can be exported to a file or spreadsheet.

How can advanced performance charts be accessed? **Select** the object you want > **Monitor** > **Performance** > **click Advanced**. Optionally, select an appropriate view from the View drop-down list.

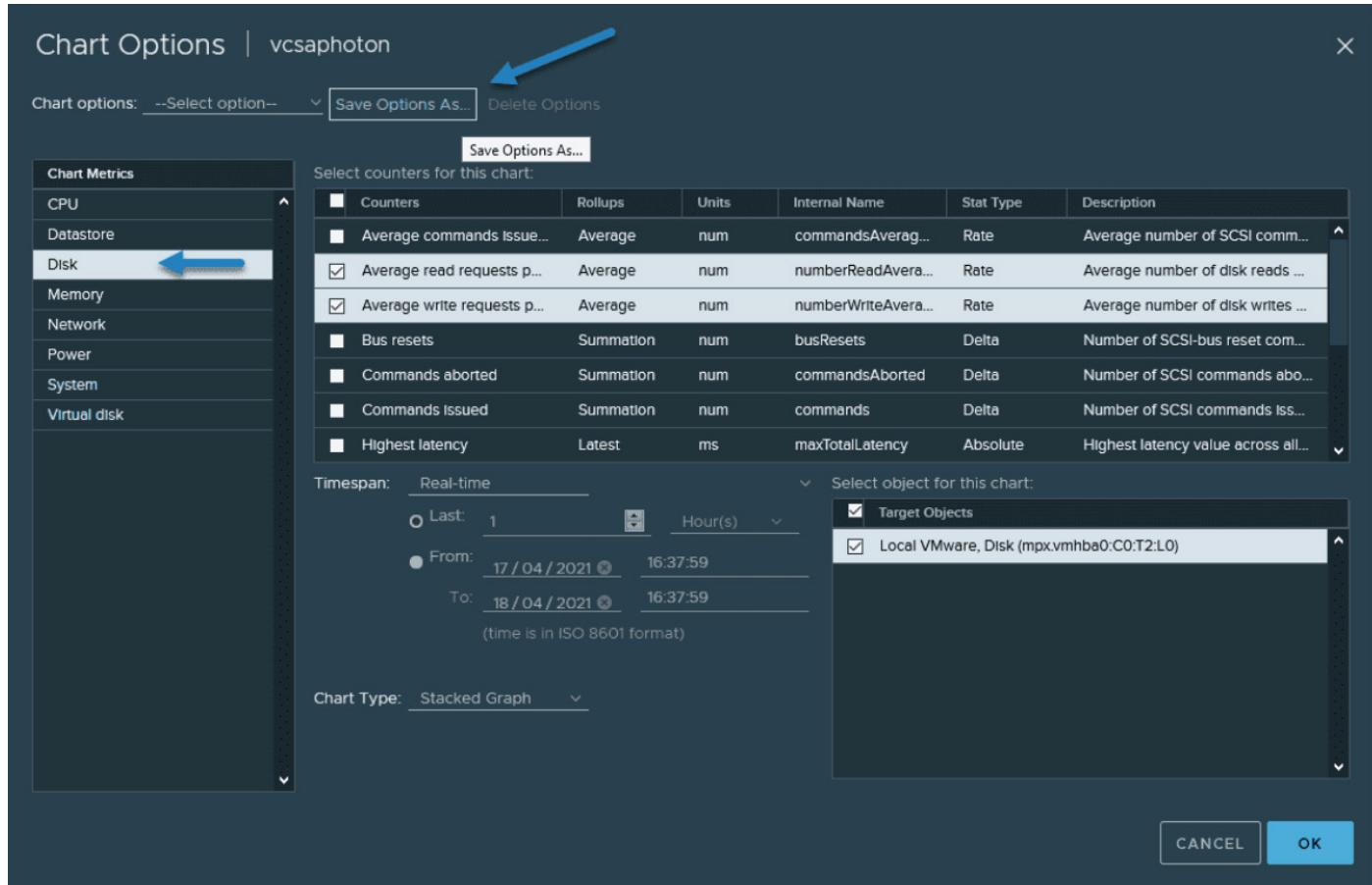


## vSphere 7 advanced performance charts

Select a timespan. If you choose Custom Interval, you must select one of the following:

- **Last** — Select the number of hours, days, weeks, or months.
- **From** — Select beginning and ending times.

If you click the **Chart Options** link, an overlay window will appear. Select the chart metrics you want to monitor and the counters you're interested in. Then click the **Save Option As** button.

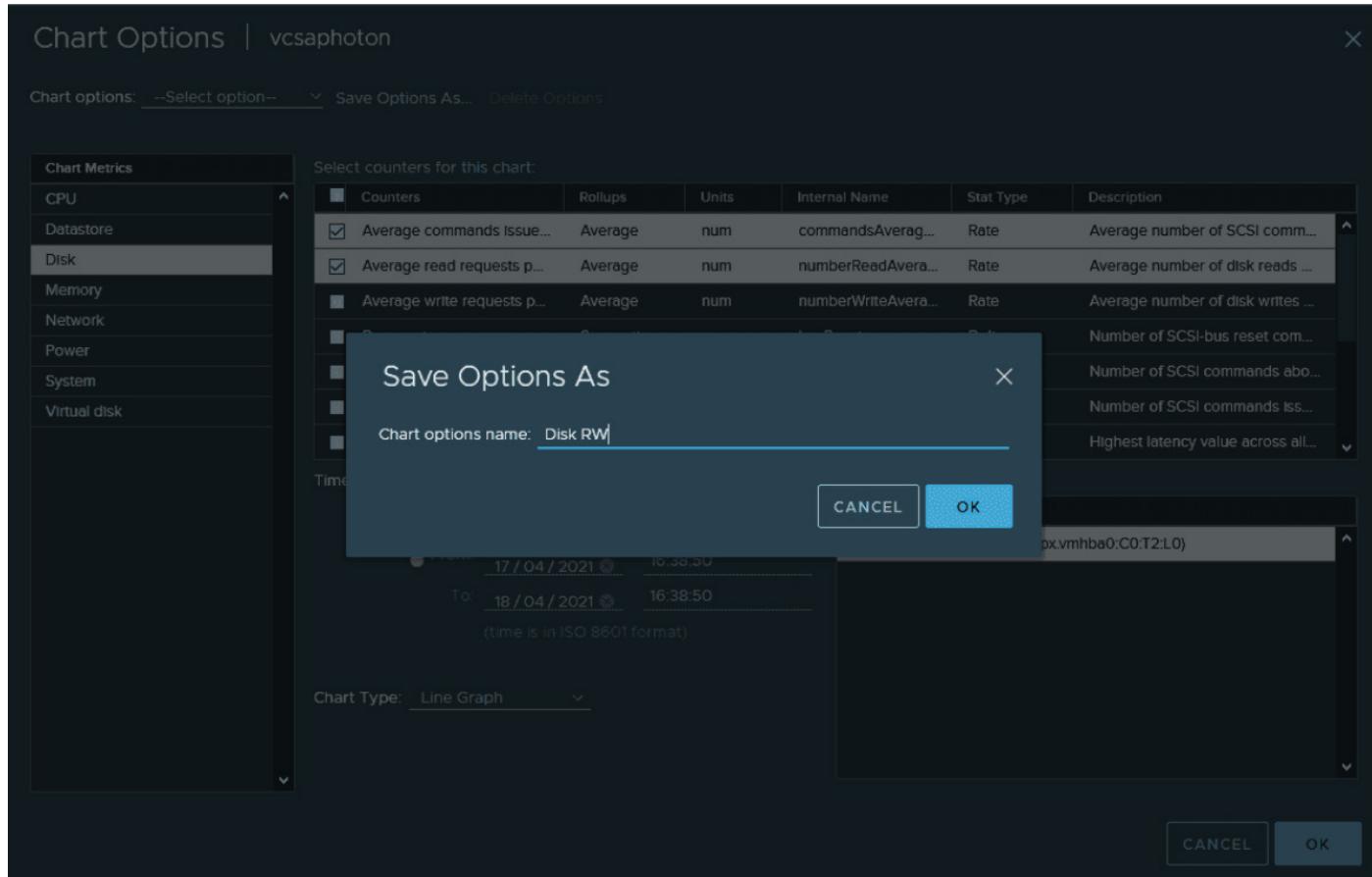


### Select chart metrics and click the Save Options As button

vSphere 7 uses metrics that are organized into logical groups based on object or object device. For example, disk metrics include I/O performance, such as latency and read/write speeds, and utilization metrics for storage as a finite resource.

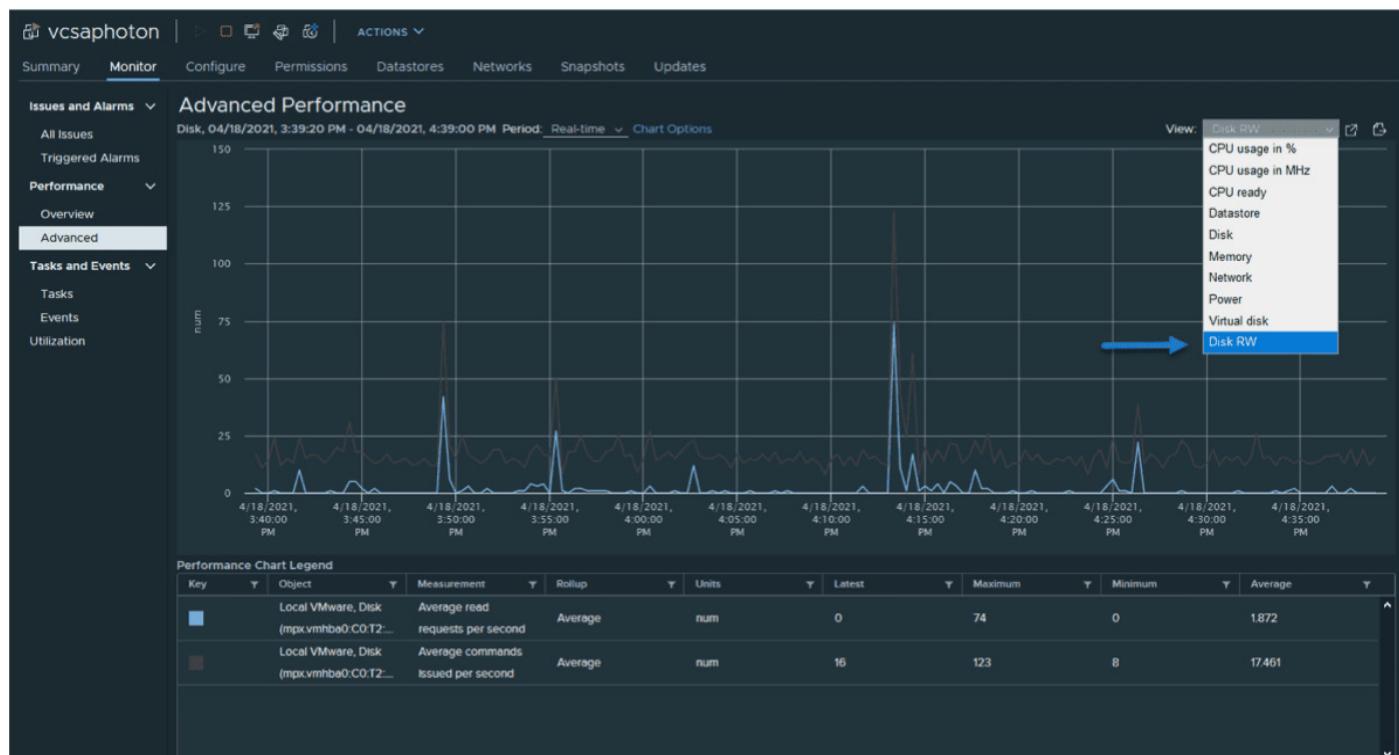
Concerning memory utilization, one of the following applies. Either memory is considered as a guest physical memory, which is the virtual memory of the hypervisor presented to the guest as physical memory.

Add a meaningful name in the pop-up window to know what you want to display.



## Name your new chart

You're done. Now you can access the chart via the drop-down menu on the right.



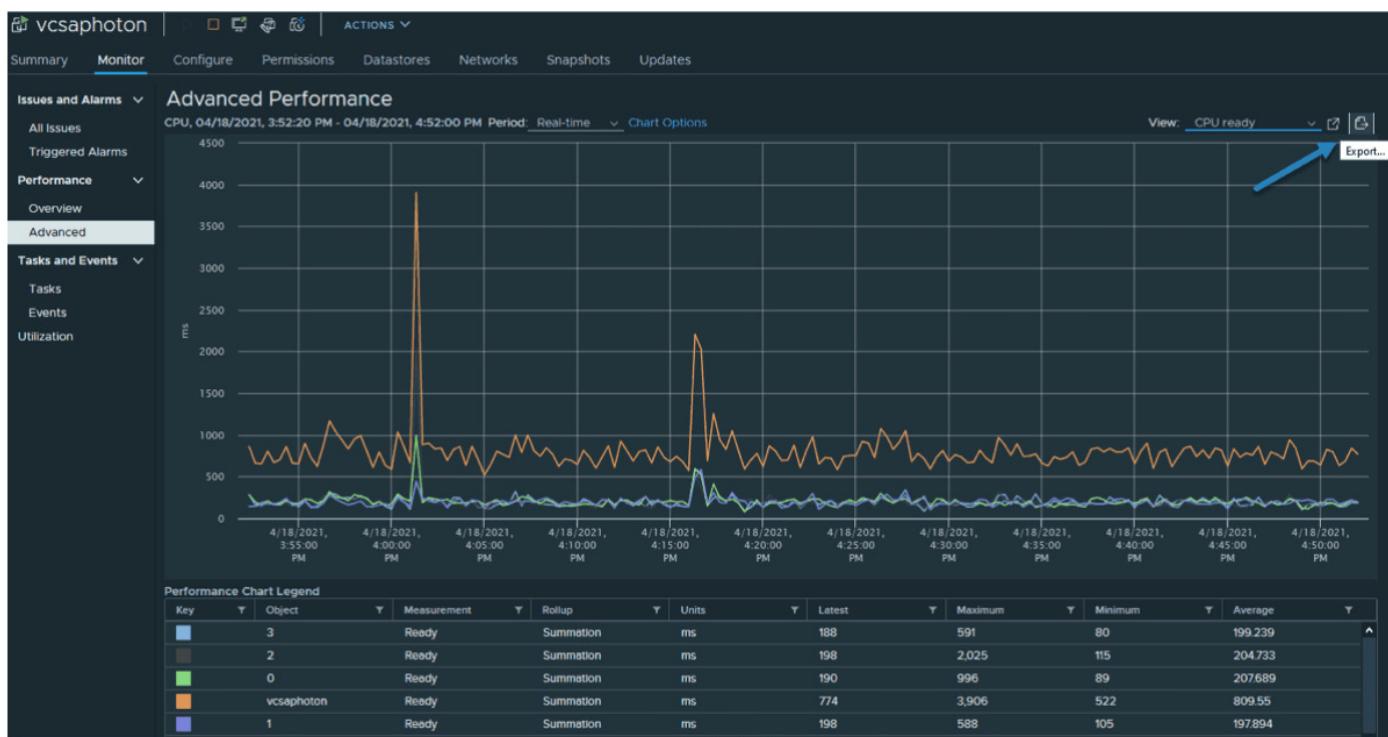
Access your new chart via drop down menu

None of these things is difficult, but you must know them for a VCP exam, and you need to practice them. While it's good that I can show you where to find them via these screenshots, nothing is better than trying the vSphere 7 client user interface and finding it by yourself.

## Save data from advanced performance charts

You can save the data by exporting it in graphic format or into a comma-separated CSV file. In the vSphere Client, select an object in the inventory pane and navigate to **Monitor > Performance > Click Advanced**.

Then select a view or change chart options as needed. Click the Export icon and select one of the options (PNG, JPEG, CSV, or SVG).



## Export your chart

Once you master those charts and you can read them and configure them properly, you can identify certain bottlenecks and find a possible solution

You can have the CPU usage of a host that is very high for several hours. This could signify that the host has insufficient CPU resources to meet the demand. As a solution, you could consider adding another host to the cluster or migrating other VMs to other hosts. Another solution would be to lower the virtual CPU allocation per VM, which may improve the performance of the host (but probably not the VM).

Users often simply over-allocate virtual CPUs to VMs, and then they have high CPU Ready spikes that indicate that the VM was ready but could not get scheduled to run on the physical CPU during the cycle.

## Objective 5.4 – Configure Network I/O control

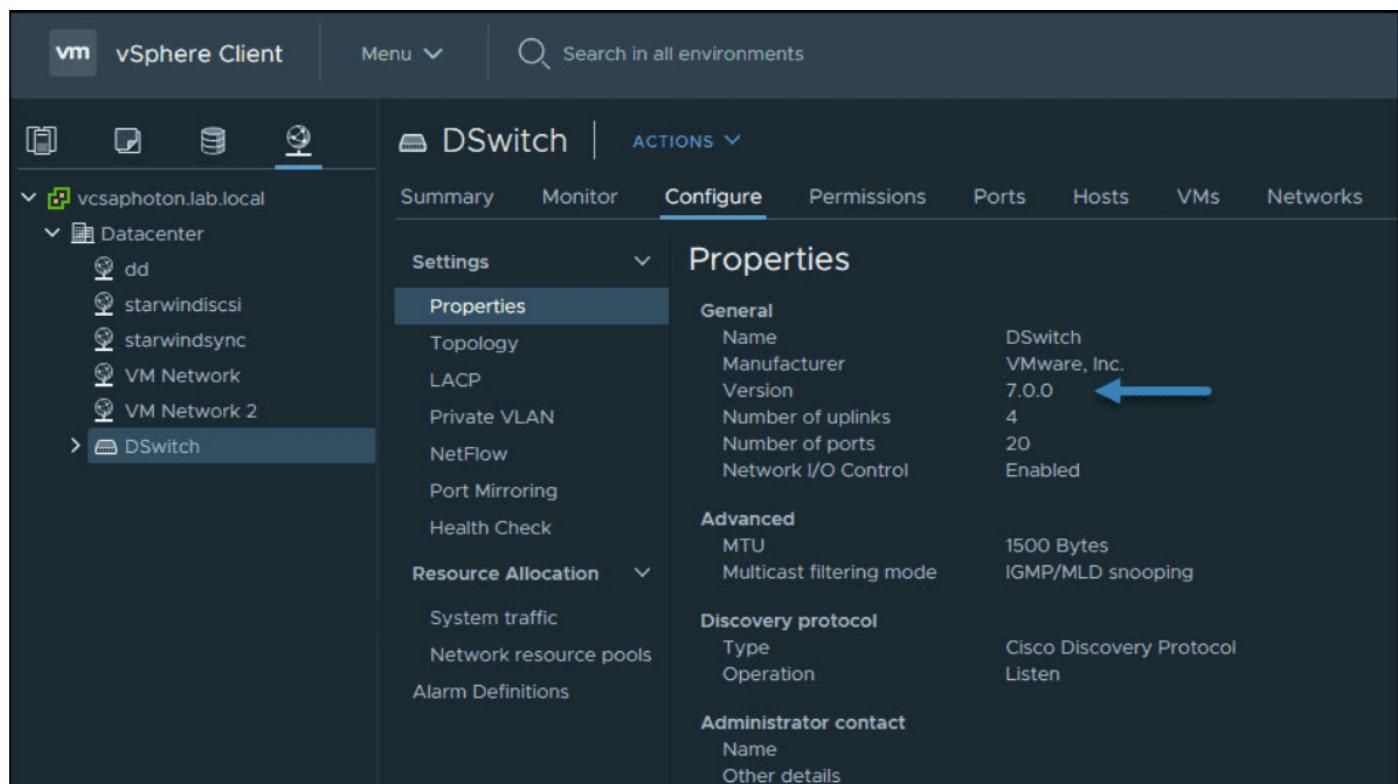
With Network I/O control (NIOC), you can adjust the bandwidth of your vSphere 7 networks. You can set different bandwidths for specific types of traffic. Once you enable NIOC on vSphere Distributed vSwitch, you'll be able to set shares according to your needs.

There are separate models for **system traffic** (vMotion, fault tolerance, vSAN, etc.) and for **VM traffic**. The main goal of NIOC is to ensure that you have enough bandwidth for your virtual machines (VMs) and that you can control their resource allocation while still preserving sufficient resources for your system traffic.

Note that in order to use NIOC and vDS, you'll need vSphere Enterprise Plus licensing.

VMware vSphere 7 Distributed vSwitch (vDS) is version 7 of vDS. Version 7 of vDS introduced a new feature for VMware NSX product integration—NSX Distributed Port group. The previous version of vDS, 6.6.0, introduced the MAC Learning capability.

To create a new vDS, click the Networking icon (the globe). Then right-click **Datacenter object** and select **New vDS**. Select **Configure > Properties** to check the properties

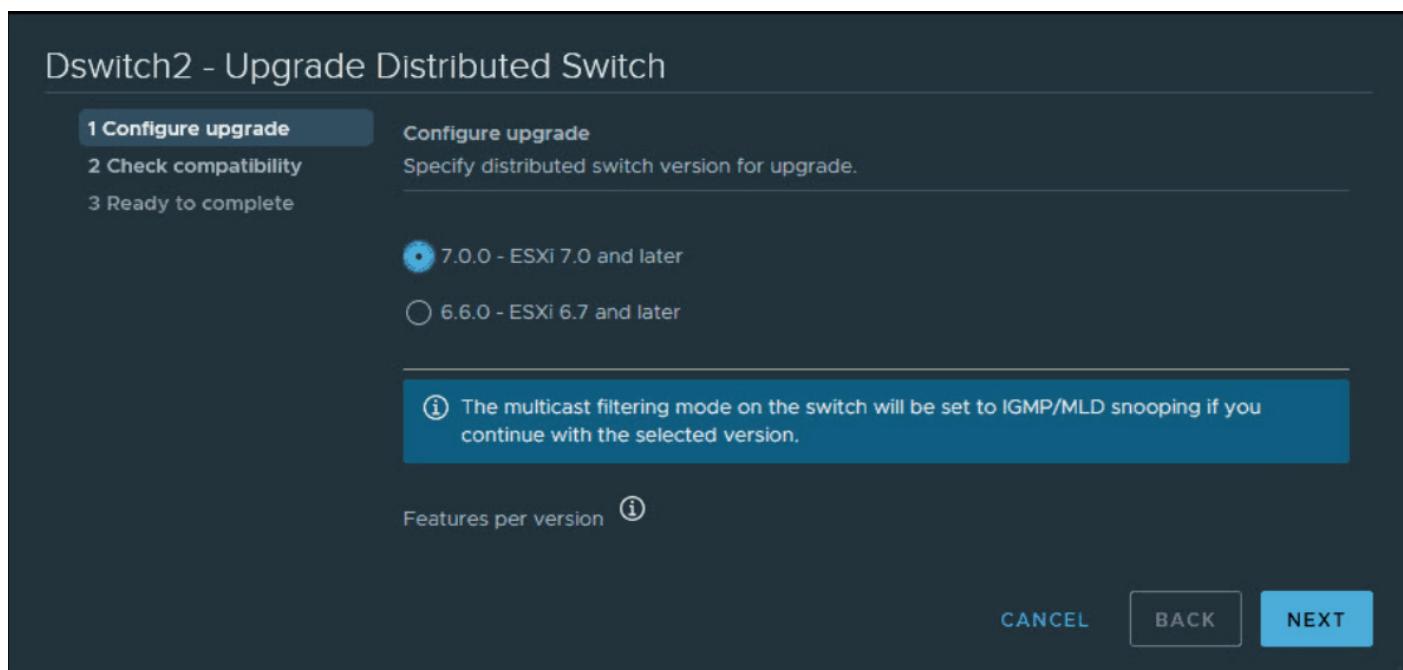


.VMware vSphere 7 Distributed Switch properties

## How can vDS be upgraded from the previous release?

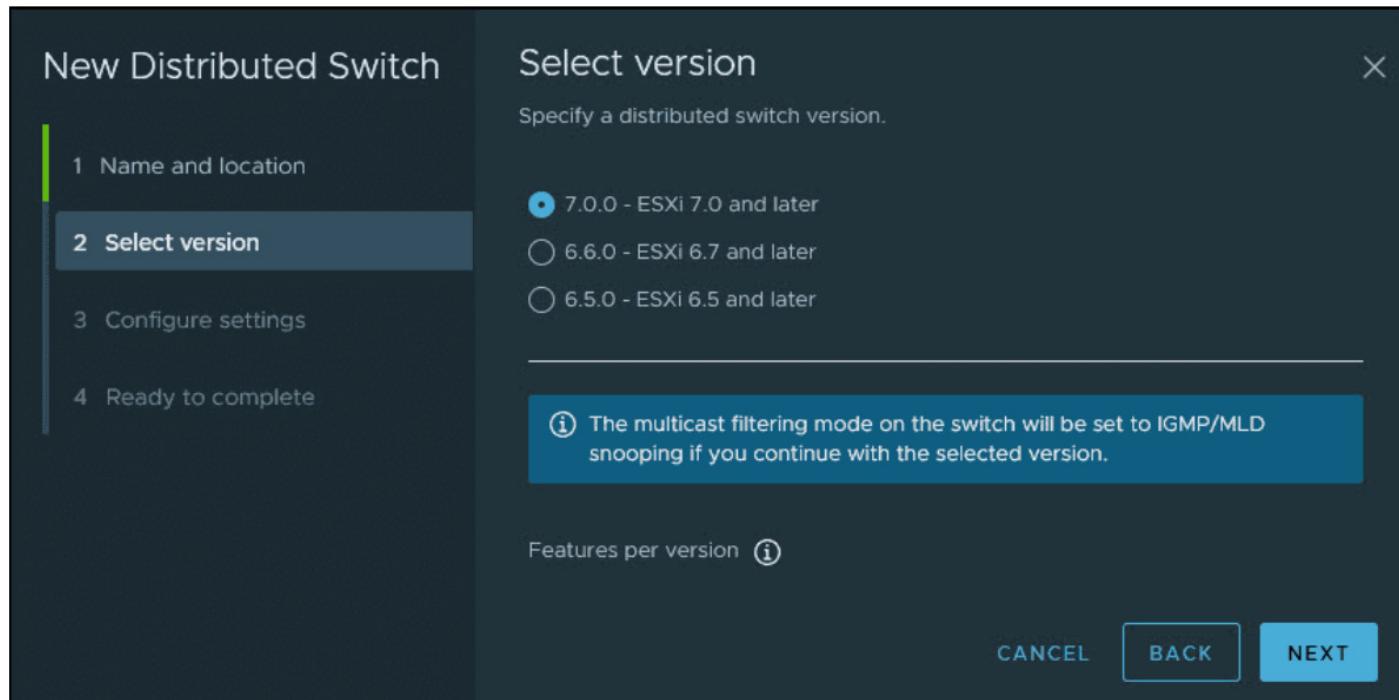
If you have upgraded recently from the previous release of vSphere, you can upgrade your vDS via the UI. We'll show you that later. Note that there is short downtime for the VMs attached to the switch.

Right-click your vDS and select > **Upgrade > Upgrade Distributed Switch**.



## Upgrade VMware Distributed Switch

If you're running a fresh installation of vSphere 7 and creating a new vDS, you still have the option of creating previous versions of vDS, such as vSphere 6.5 or 6.7. You may need to ensure compatibility with the rest of your infrastructure, which might still be running older versions of vSphere.



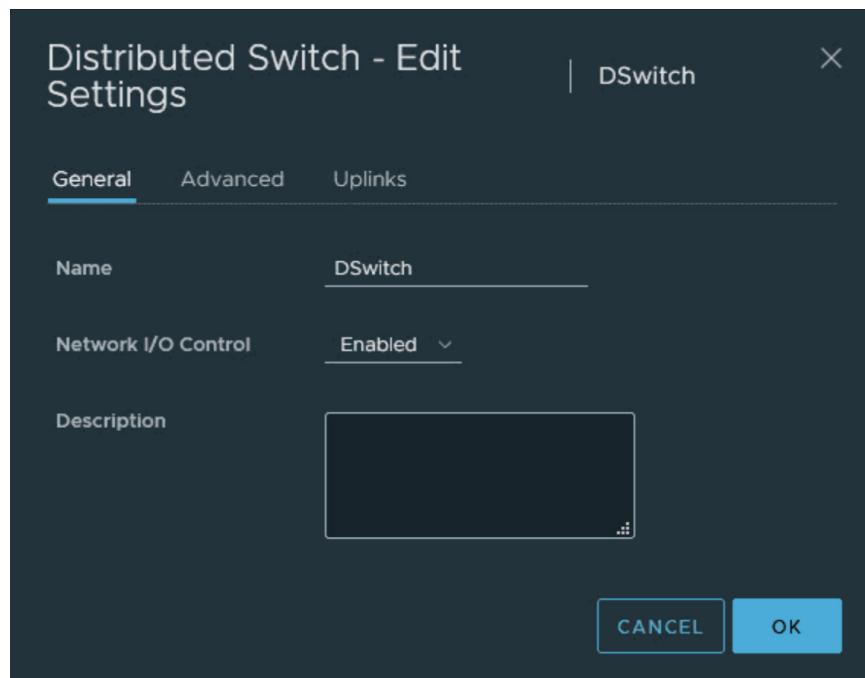
### vSphere 7 and the option to create a different version of vDS

#### Where should you enable NIOC?

You need to enable NIOC on each vDS. From Networking, select the vDS. Then select **Actions > Settings > Edit Settings**.

#### Enable NIOC on vSphere 7 vDS

This opens a pop-up window where you can use the drop-down menu to enable or disable NIOC. NIOC is enabled by default.



### Enable NIOC drop down menu

The traffic types are all set to 50 shares except the VM traffic. No reservation or limits are set by default.

The main vSphere features for which network traffic can be configured are:

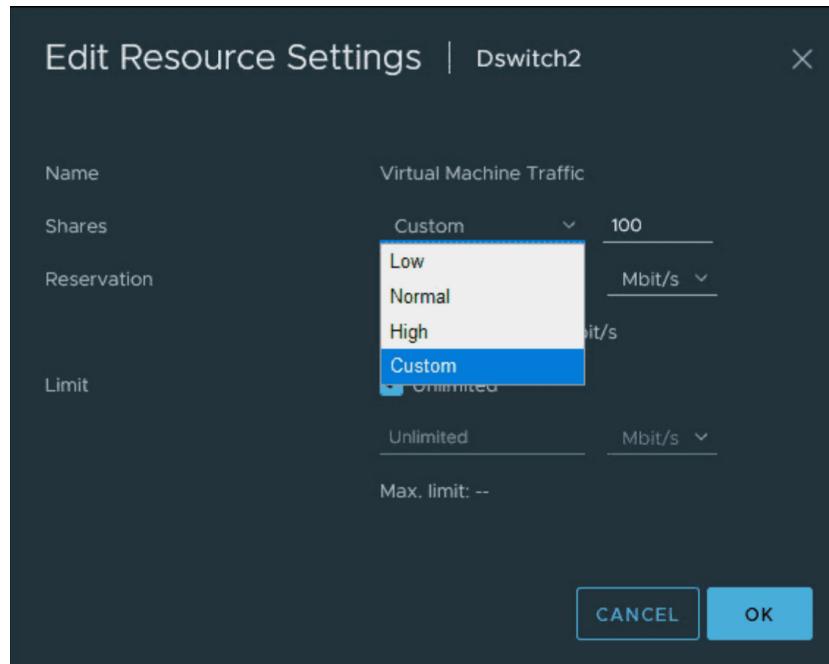
- Management networking traffic
- Fault tolerance (FT)
- NFS
- vSAN
- vMotion
- vSphere replication
- vSphere data protection backup
- Virtual machine

Here is the view of the system traffic and the default values. You can see that by default, all system types are at 50, while the VM value is at 100.

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

### VMware vDS system traffic default values

You can click the **Edit** button after selecting the type of traffic and then modify the values by selecting **Custom**.



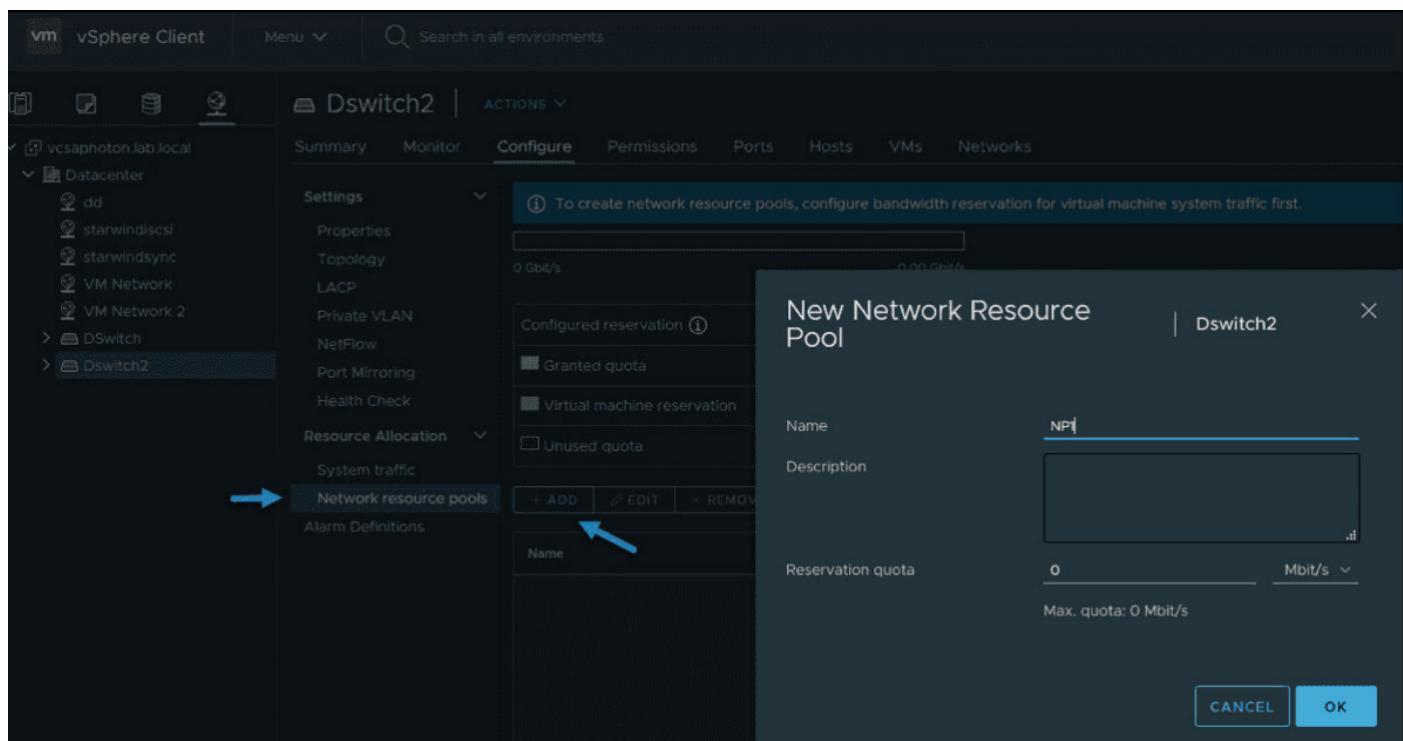
### Configure shares reservations and limits for different traffic types

The allocation parameters for the different traffic types are:

- **Shares** — Value from 1 to 100, where the maximum 100 is the priority of a traffic type compared to the other traffic types that are active on the same physical adapter.
- **Reservation** — Minimum bandwidth is in Mbps. This is the bandwidth guaranteed on a simple physical adapter.
- **Limit** — Sets the maximum allowed bandwidth that the traffic type can consume on a single physical adapter in Mbps or Gbps.

You can also create new resource types via the menu just below system traffic. Click the **Network resource pools** menu link and then click **Add**. This will create a new network resource pool that will have a reservation quota. You can then assign a VM to that pool.

This group basically takes off bandwidth from the Virtual Machine system type, so you would need to set up a bandwidth reservation for that group first.



Create new network resource pool in vSphere 7

This is the main principle of NIOC in vSphere 7. NIOC has been around since vSphere 5. The latest version is version 3, which has improved network resource reservation and allocation across the entire switch.

NIOC version 3 lets you configure bandwidth requirements for VMs. 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.

While the configuration of the vDS and NIOC is only possible via vCenter Server, in case of a problem on your vCenter Server appliance (vCSA), the system functions and the rules are deployed on the individual ESXi hosts.

If you don't want to use NIOC for certain physical adapters, you can configure it as needed. It might be the case where this particular adapter is low capacity or low speed. You can do this in the advanced system settings.

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

With VMware vSphere 7, VMware keeps storage I/O control configuration within its flagship suite. The SIOC isn't new; however, the new UI is now fully HTML based and easier to use. We'll have a look at SIOC in this lesson.

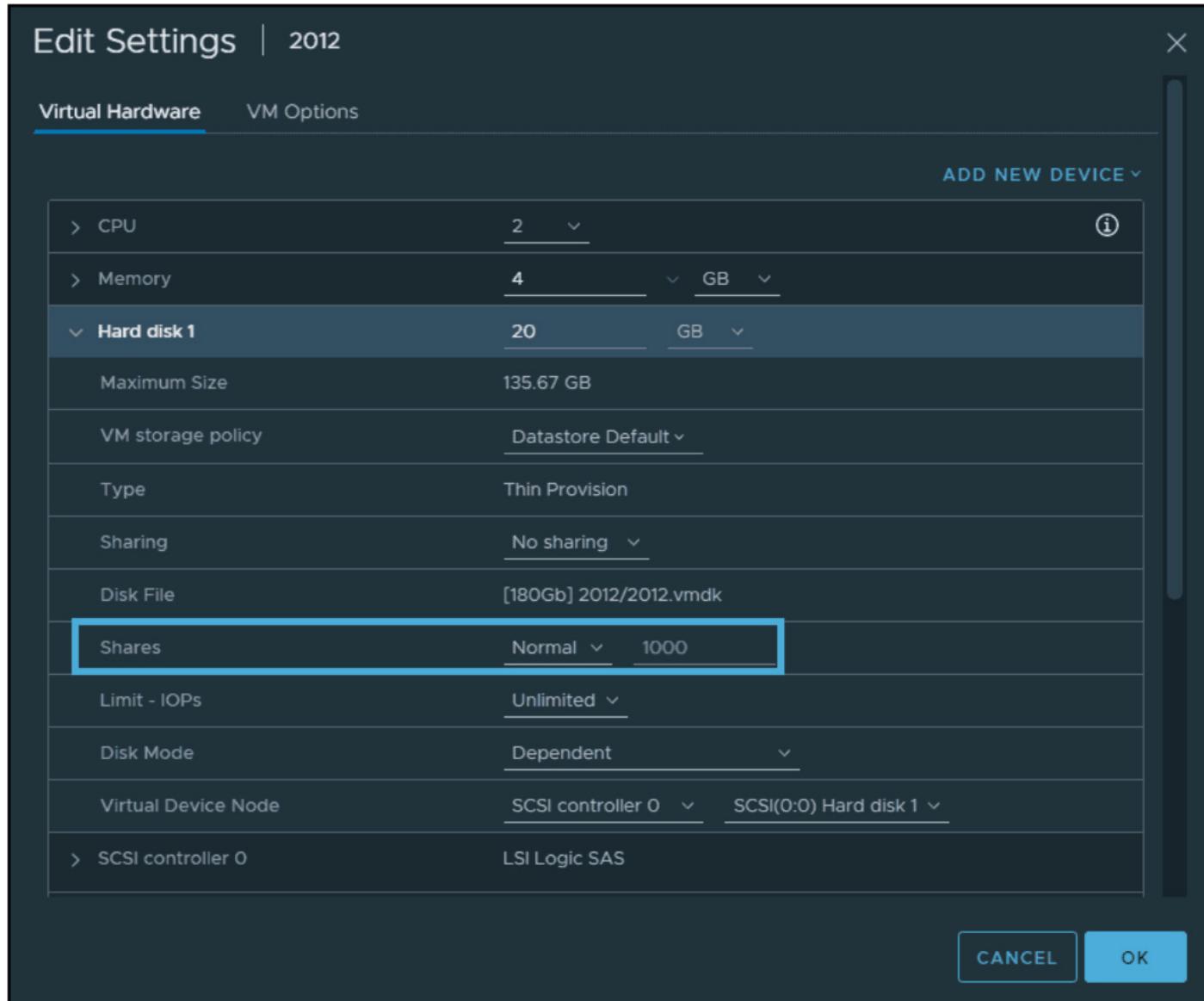
When managing and maintaining a VMware vSphere environment, keeping an eye on storage and storage I/O is extremely important. In most virtualization environments where shared SAN storage is in place, it is not uncommon to see storage I/O resources exhausted before CPU and, in many cases, memory.

SIOC allows you to prevent a single virtual machine from monopolizing I/O consumption on your datastore. SIOC is able to ensure an equal (or fair) distribution of I/Os between VMs when contention occurs. SIOC is not triggered during normal operations. There is a threshold that acts as a trigger for the I/O queue throttling mechanism that is enabled on the datastore.

In terms of performance, SIOC offers some control over the datastores where your workloads are running. If some of your VMs have a high load while others are underperforming because the storage is not able to deliver enough, SIOC is the element that can control that.

SIOC prevents your critical VMs from being affected by VMs from other hosts that access the same datastore and «steal» valuable I/O operations per second (IOPS). After SIOC is enabled on the datastore, ESXi starts to monitor the datastore for latency. If ESXi marks a datastore as congested and its latency reaches a predefined threshold, each VM on that datastore is allocated I/O resources in proportion to its shares.

Configuring shares on virtual machines sets how IOPS will be distributed between those VMs. A VM with high shares is going to get more IOPS than a VM that is configured with low or normal shares.



### Example of share settings by default on the per vm level

#### Storage I/O Control requirements and some limitations

All your datastores that are enabled with SIOC (SIOC is enabled per datastore) have to be managed by a single vCenter Server.

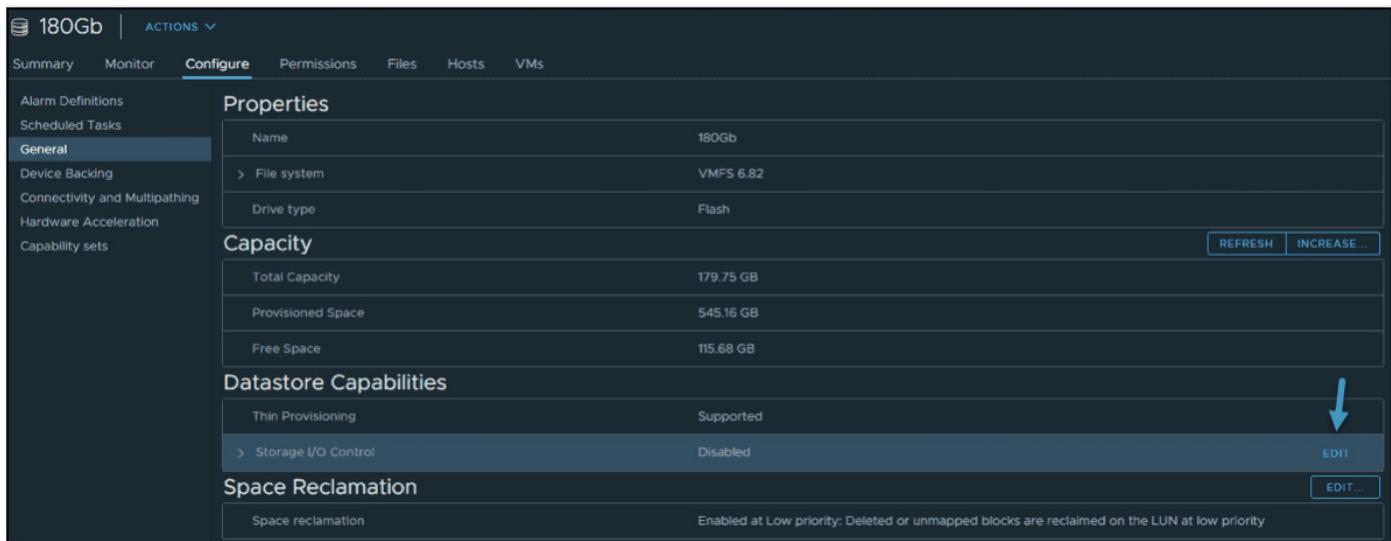
SIOC is supported on Fibre Channel, NFS, and iSCSI connected storage. Raw device mappings (RDM) are not currently supported.

If you're using extents on your datastores, then you cannot use SIOC. This is not supported.

Some arrays might be using automated storage tiering, so in this case you should check the [VMware storage compatibility guide](#) and make sure it is compatible with SIOC.

## How to activate SIOC and where?

Connect to your vCenter Server via the vSphere client and then browse to the **datastore** icon in the vSphere Client. Select **Configure > Datastore capabilities > Edit**.



### Configure Storage IO Control on a datastore

On the next screen, you'll see three radio buttons:

- **Enable Storage I/O Control and statistics collection** — Activates the feature. Note: You can uncheck the Include I/O statistics for SDRS.
- **Disable Storage I/O Control but enable statistics collection** — You can select the option to include I/O statistics for SDRS if used.
- **Disable Storage I/O Control and statistics collection** — Disables SIOC and statistics collection.

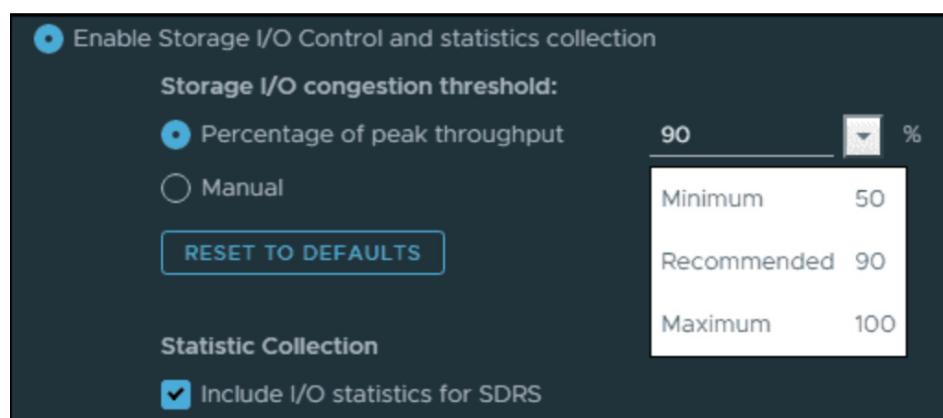
By default, the **Disable Storage I/O Control and statistics collection** option is active and selected. So, you can go ahead and select the **Enable Storage I/O Control and statistics collection** radio button.



### Set SIOC congestion threshold

Adjust the percentage of peak thresholds if you like. The defaults are set to 90%, which is a recommended value, but there are other values you can choose from.

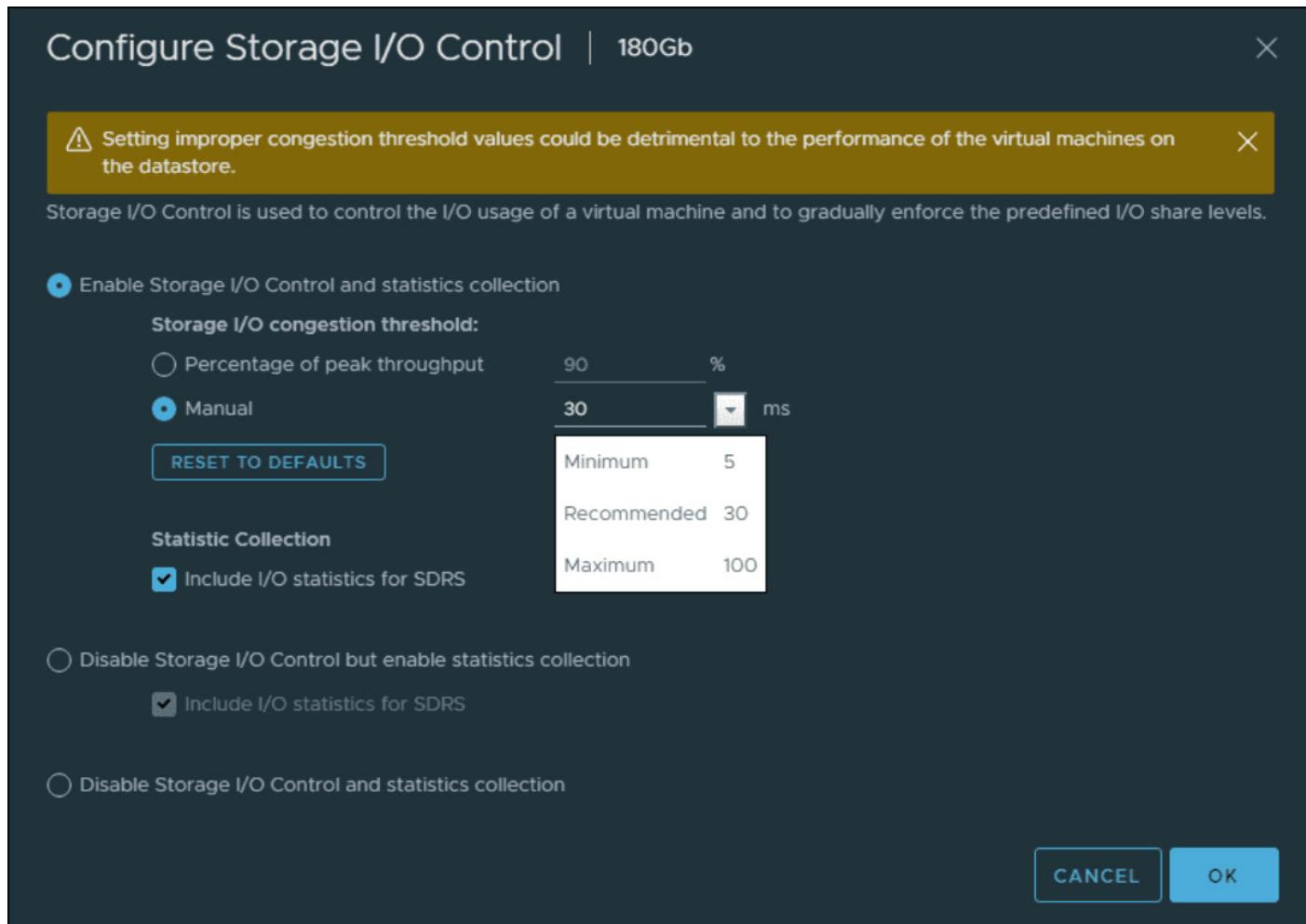
Here is the view.



### SIOC recommended values

There is also the option to enter another number, but you'll get a warning message «Setting improper congestion threshold values could be detrimental to the performance of the virtual machines on the datastore».

The manual value is not in percent but in milliseconds (ms). When you click it, you'll see that you can choose from three different predefined values as well.



### Enable SIOC manual values

Click **OK** to validate and you're done. Proceed with all the shared datastores you might have in your organization or only the ones where you have your business-critical workloads running.

### Storage I/O control troubleshooting

Each time you add a new host that is connected to a shared datastore, you have to re-enable SIOC. If you experience problems with SIOC and you have recently changed the number of hosts, simply disable and re-enable SIOC.

Make sure that you're using the correct values and that those values have not been modified. You should enter 30 ms, which is the recommended value.

Where can you check the VMs shares/limits at the cluster level? Navigate and select your **cluster > Monitor > Storage**. Then view the shares and shares value columns there.

The screenshot shows the vSphere Client interface with the 'Cluster' selected in the navigation pane. Under the 'Storage' tab, the 'Storage Reservation Details' section is displayed. A table lists various VMs along with their storage details. The 'Shares' and 'Shares Value' columns are highlighted with a blue border, indicating they are the focus of the question. The table data is as follows:

Name	Disk	Datastore	Limit - IOPs	Shares	Shares Value
vCLS (2)	Hard disk 1	vsanDatastore	Unlimited	Normal	1000
vCLS (3)	Hard disk 1	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 1	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 2	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 3	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 4	vsanDatastore	Unlimited	Normal	1000
vCLS (4)	Hard disk 1	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi03.lab.l...	Hard disk 1	vsanDatastore	Unlimited	Normal	1000
Z-VRA-esxi03.lab.l...	Hard disk 2	vsanDatastore	Unlimited	Normal	1000

**Check VMs and their shares value at the cluster level**

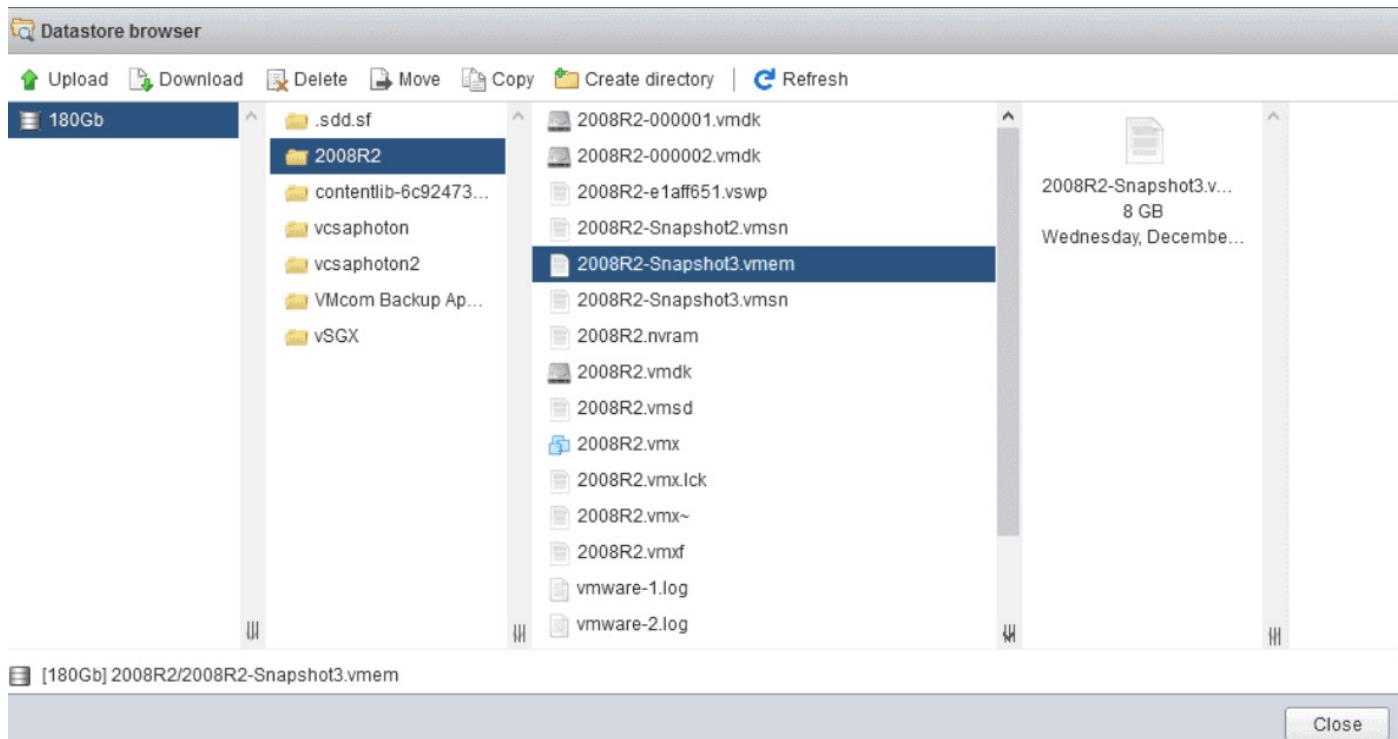
## Objective 5.6 – Explain the performance impact of maintaining virtual machine snapshots

As you know, snapshots affect the performance of virtual machines (VMs) in your VMware environment. The performance is affected by how long the snapshot or the snapshot tree is in place. The longer you have VMs running on snapshots, the more the guest OSs have changed since the time you took the snapshot.

Snapshots as such are here to preserve the state of a VM at the time you take the snapshot. When you trigger the creation of a snapshot, you create a file that contains the state of the VM at that particular point in time. The VM snapshots slow the vMotion switchover process; you should always avoid unneeded snapshots on VMs.

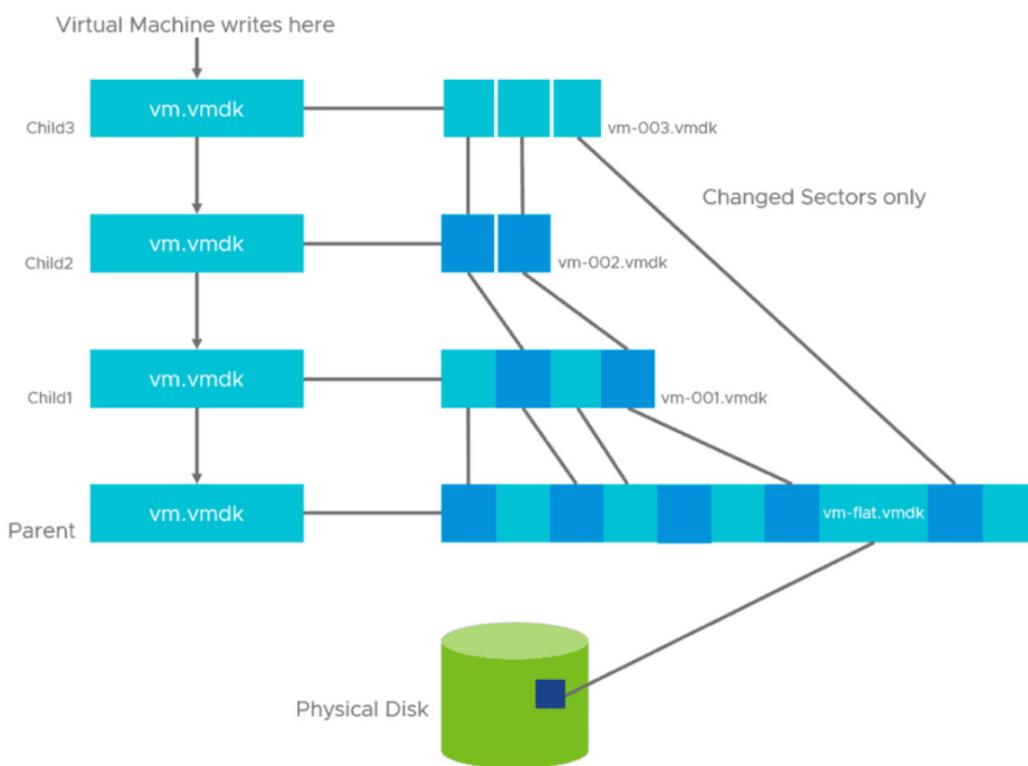
### What files are generated by a snapshot?

A snapshot comprises a number of files that you can view in the datastore browser after navigating to a folder in the VM for which snapshots have been taken. Use the vSphere web browser, or if running an individual ESXi host, use the ESXi host client.



### Example of a VM and snapshot file

We won't go into too much detail here about each of these files, as this won't teach you much that is new. However, to imagine the snapshot chain with the naming convention for child VMDKs, VMware has a nice image available in [this KB](#).



VMware snapshot architecture in vSphere 7

## Consolidating a VM's disks

Sometimes you see that you need to consolidate VM disks. You can see it in the vSphere client, and I'll show you how in a sec. What is it? It is when the VM has redundant delta disks. When the consolidation process is executed, those redundant disks are removed. This improves virtual machine performance and saves storage space.

When not using snapshots, you don't need to consolidate. Snapshot consolidation is needed when snapshot disks fail to compress after a **Delete snapshot** or **Delete all snapshots** operation. This can happen, for example, when you delete a snapshot but the associated disk does not commit back to the base disk.

The **Needs Consolidation** column in the vSphere web client shows the virtual machines to consolidate.

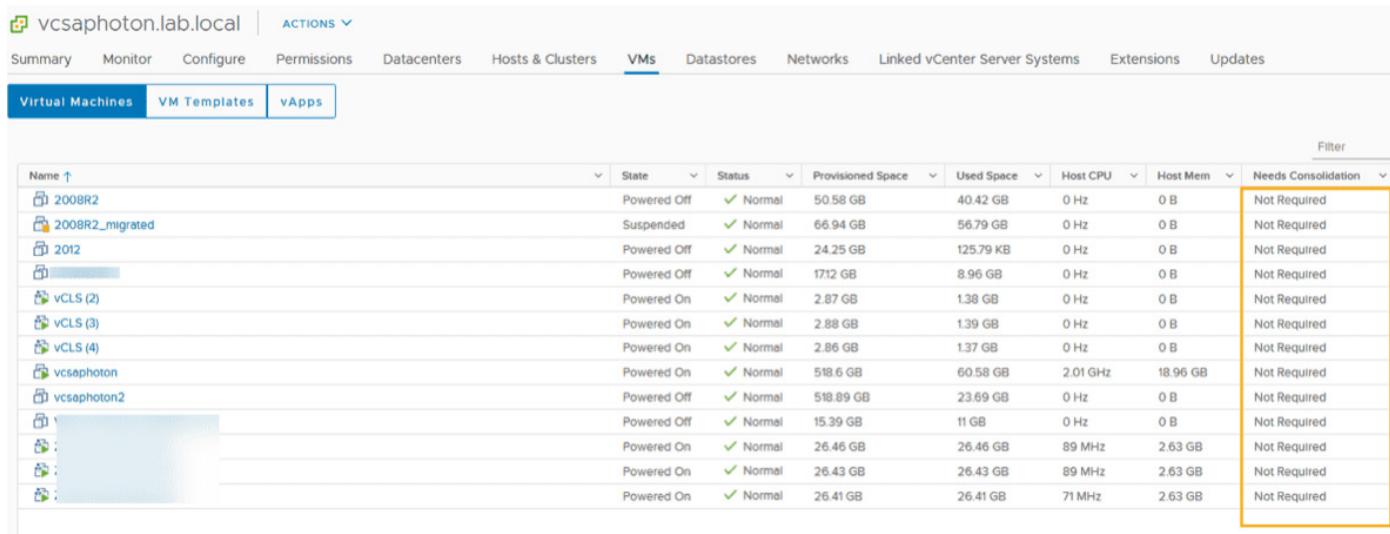
To view the **Needs Consolidation** column in the vSphere client, you'll need to:

- Select a vCenter Server instance, host, or cluster.
- Click the **VMs** tab.
- Left-click the menu bar for any virtual machine column and select **Show/Hide Columns > Needs Consolidation**.

The screenshot shows the vSphere Client interface with the 'Datacenter' selected in the navigation tree. The 'VMs' tab is active. A blue arrow points to the 'Datacenter' icon in the navigation bar. Another blue arrow points to the 'VMs' tab in the top navigation. A third blue arrow points to the 'Show/Hide Columns' button in the top right corner of the main content area. The 'Needs Consolidation' checkbox is checked, and a blue arrow points to it. The main table lists various VMs with their status, provisioned space, used space, and host details. The 'Needs Consolidation' column is visible in the table.

**The Needs Consolidation column is not shown by default**

The VM can have a status of Yes, which means that the snapshot files for the VM should be consolidated and that the VM's Tasks and Events tab indicates a configuration problem (yellow color). If there is no status saying Not Required, it means that all is good and there is no need to consolidate.



Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem	Needs Consolidation
2008R2	Powered Off	Normal	50.58 GB	40.42 GB	0 Hz	0 B	Not Required
2008R2_migrated	Suspended	Normal	66.94 GB	56.79 GB	0 Hz	0 B	Not Required
2012	Powered Off	Normal	24.25 GB	125.79 KB	0 Hz	0 B	Not Required
	Powered Off	Normal	1712 GB	8.96 GB	0 Hz	0 B	Not Required
vCLS (2)	Powered On	Normal	2.87 GB	1.38 GB	0 Hz	0 B	Not Required
vCLS (3)	Powered On	Normal	2.88 GB	1.39 GB	0 Hz	0 B	Not Required
vCLS (4)	Powered On	Normal	2.86 GB	1.37 GB	0 Hz	0 B	Not Required
vcsaphoton	Powered On	Normal	518.6 GB	60.58 GB	2.01 GHz	18.96 GB	Not Required
vcsaphoton2	Powered Off	Normal	510.89 GB	23.69 GB	0 Hz	0 B	Not Required
	Powered Off	Normal	15.39 GB	11 GB	0 Hz	0 B	Not Required
	Powered On	Normal	26.46 GB	26.46 GB	89 MHz	2.63 GB	Not Required
	Powered On	Normal	26.43 GB	26.43 GB	89 MHz	2.63 GB	Not Required
	Powered On	Normal	26.41 GB	26.41 GB	71 MHz	2.63 GB	Not Required

## Consolidation not required

### Some of VMware's best practices and recommendations for snapshots

- Snapshots are not backups, and we all know that. But not everyone knows why this is. A snapshot file is only a changelog of the original virtual disk; you'll need the base disk to fully restore. So, if the base disk is missing, lost, or damaged, it's tough luck.
- There are those delta files in the VM's folder. The delta files can grow to the same size as the original base disk file if a lot of changes are made to the VM over time. This is why the provisioned storage size of a VM with snapshots can increase by some huge number and cause problems for your datastores. Note that even to delete snapshots, you'll need free space on a datastore. If you don't have enough free space, you cannot delete your snapshot.
- A maximum of 32 snapshots is allowed. This does not mean that you have to create those 32 snapshots. In fact, VMware recommends that you use only two to three snapshots in a chain, not more.
- You should not use a single snapshot for more than 72 hours. Snapshots should not be kept over long periods of time because they grow over time with the changes to your VM.
- There are a couple of backup software products on the market that ensure there are no snapshots left behind when you back up your VMs.
- If there is a large number of delta files in a chain, a VM having many snapshots has a heavy performance impact on the applications running in those VM(s). There is also a heavy impact on host performance because the IOPS consumed by those VMs might negatively impact the performance of your storage device and hosts.

## Read IOPS and write IOPS

Imagine that when you keep a snapshot for a VM, you basically double the amount of read IOPS. For write operations, a VM that needs to write a block that has not been written before will need twice as many write operations as well.

A huge penalty indeed. This is because VMware has to update the table that keeps the reference to the block's location, either the snapshot or the base disk. This leads to a very big performance impact.

## Performance exceptions

There are situations where performance is not affected when running VMs with snapshots. This is the case with VMware vVols.

Snapshots on vVols are offloaded to the array that creates the snapshot using the array-side native operations. The snapshots are handled by the array and the copy-on-write (COW) operations that are needed to maintain the snapshot. As a result, the I/O from the VM to the disk does not have the performance penalty because the VM is running on an active snapshot.

## Objective 5.7 – Plan for upgrading various vSphere components

To upgrade a vSphere 6.5 or 6.7 environments to vSphere 7.0, you should upgrade the major components in the following order: vCenter Server ESXi hosts VMware Tools on the virtual machines Virtual machine hardware.

Note For vCenter Server 6.0 and earlier, you should upgrade to vSphere 6.5 or 6.7 and then upgrade to vSphere 7.0.

You should back up the vCenter Server prior to upgrading it. Upgrading your environment to use vCenter Server 7.0 requires you to either upgrade an existing vCenter Server Appliance or migrate from an existing Windows-based vCenter Server. When you upgrade or migrate a vCenter Server that uses an external Platform Services Controller (PSC), you converge the PSC into a vCenter Server Appliance.

Prior to upgrading to vCenter Server 7.0, you should consider its compatibility with other vSphere components.

**vCenter Server Appliance** - You can upgrade vCenter Server Appliance 6.5 and 6.7 to 7.0, except with specific build combinations that violate the back-in-time restrictions identified at <https://kb.vmware.com/s/article/67077>.

- vCenter Server for Windows - vCenter Server 7.0 uses PostgreSQL for the embedded database. It does not support external databases.
- vCenter Server database - vCenter Server 7.0 uses PostgreSQL for the embedded database. It does not support external databases.
- ESXi Hosts - vCenter Server 7.0 requires ESXi host Version 6.5 or later.
- Host profiles - vCenter Server 7.0 requires host profiles Version 6.0 or later.
- VMFS - vCenter Server 7.0 supports VMFS 3 and later but can only create VMFS 5 and VMFS 6 datastores.
- Virtual machines and VMware Tools - Review the ESXi upgrade documentation for specific upgrade options, which are dependent on the current versions.
- Auto Deploy - If you currently use Auto Deploy, when you upgrade to vCenter Server 7.0, VMware recommends that you use Auto Deploy to upgrade hosts to ESXi 7.0.
- vSphere Distributed Switch (vDS) - Upgrade to vDS 6.0 before upgrading vCenter Server.
- Network I/O Control (NIOC) - Upgrade to NIOC Version 3 before upgrading vCenter Server.
- vSAN - VMware's recommendations are that you should synchronize versions of Center server and ESXi to avoid potential faults.
- vSAN disk version - Supported versions and paths may be impacted by the current version and upgrade history. See <https://kb.vmware.com/articleview?docid=2145267>.
- Legacy Fault Tolerance (FT) - If you use Legacy FT on any virtual machines, you must turn off or upgrade the Legacy FT feature prior to vCenter Server upgrade or migration.

**vCenter Server Data Transfer** If you migrate a Windows-based vCenter Server or upgrade a vCenter Server with an external PSC, you need to transfer data to the embedded PostgreSQL database in the target vCenter Server Appliance. At a minimum, you must transfer configuration data. You can choose whether you want to transfer historical data and performance metrics data.

**Configuration data** - Transferring just configuration data minimizes downtime during the upgrade.

**Configuration and historical data** - You can choose to transfer historical data (usage statistics, tasks, and events) during an upgrade (impacting the downtime) or in the background following the upgrade.

**Configuration, historical, and performance data** - You can transfer the configuration data during the upgrade and transfer the remaining data in the background following the upgrade.

## **Upgrading vCenter server appliance (vCSA)**

**Upgrading vCenter Server Appliance** You should address the following prerequisites prior to upgrading a vCenter Server Appliance to Version 7.0:

- Check that the clocks of all the vSphere components are synchronized.
- Make sure that the system has the minimum hardware and software components.
- You should verify that the target ESXi host is not in Lockdown, Maintenance, or Standby Mode.
- Also, check that the target ESXi host is not part of a fully automated DRS cluster.
- Verify that port 22 is open on the source vCenter Server Appliance and that port 443 is open on the ESXi host on which the source vCenter Server Appliance is running. Verify that the source appliance has sufficient free space to accommodate the data that is used for the upgrade.

If the source vCenter Server uses an external database, determine its size and ensure that your account for it in the size of the new appliance.

Make sure that you have network connectivity between the vCenter Server or ESXi that hosts the source vCenter Server Appliance and the new vCenter Server Appliance. If planning to set the system name to an FQDN, **verify that forward and reverse DNS records are created**.

Upgrading a vCenter Server Appliance is a **two-stage process**. The first stage is to deploy the OVA. The second phase is to transfer the data and configure the vCenter Server Appliance.

For a vCenter Server with an external PSC, you can use the following procedure for the first stage:

- Launch the vCenter Server (GUI) installer and select Upgrade.
- Review the upgrade process on the first wizard page and click Next.
- Accept the license agreement and click Next.
- Provide the following information for the source vCenter Server:
  - Provide the address, HTTPS port, SSO credentials, and root password for the source vCenter Server. Provide the address, HTTPS port, and credentials for a user with administrative privileges for the ESXi host (or vCenter Server) that is hosting the source vCenter Server. Click Connect.
  - Follow the wizard prompts to accept the certificate and accept the plan to converge the source vCenter Server and external PSC into a single vCenter Server Appliance.
  - Follow the wizard prompts to provide the following information for the target environment that will host the new vCenter Server Appliance.

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

# Objective 7.1 - Create and manage virtual machine snapshots

VMware snapshots are important part of vSphere infrastructure. Using snapshots is very flexible way of being able to go back in time and revert changes. VMware snapshots are used by admins, developers and other IT team members who are not all VMware specialists. As such it might be a good idea to learn some good practices about snapshots and this technology, to get the most out of it.

VMware storage technology has evolved over time, including snapshots. vSphere 6.5 uses SEsparse as a default format for all delta disks on the VMFS 6 formatted datastores. The SEsparse stands for “space efficient” and supports space reclamation, which previous formats did not. The blocks deleted within VM are marked, then used by the hypervisor which issues a command within the SEsparse layer to unmap (to free) those blocks and save space on a datastore.

If you still have VMFS 5 formatted datastores in your environment and still planning to use snapshots, you might consider upgrading to VMFS 6 in order to benefit those enhancements.

You can create a snapshot of a VM when it is powered on, off or suspended. VMware snapshot stores the **complete state and data of a virtual machine** whenever a snapshot is created. It means that you can easily go back in time with the point-in-time saved state of the VM.

However, with each snapshot, there are delta files which can grow to the same size as the original base disk file. That's why the provisioned storage size of a VM increases by an amount up to the original size of the VM multiplied by the number of snapshots on the virtual machine.

## Do not use snapshots as backups

This is the number one thing not to do. I guess everyone has heard this at least once, but who knows. While it might be tempting to save your work in snapshots instead of creating a regular backup job via your backup software. However, there are some risks.

The snapshot file is only a change log of the original virtual disk, it creates a place holder disk, `virtual_machine-00000x-delta.vmdk`, to store data changes since the time the snapshot was created. If the base disks are deleted, the snapshot files are not enough to restore a virtual machine.

There is a maximum of 32 snapshots supported in a chain so imagine you have 32 snapshots and the chain breaks in the middle. Then you have problem. For best performance and best security always use only 2 to 3 snapshots.

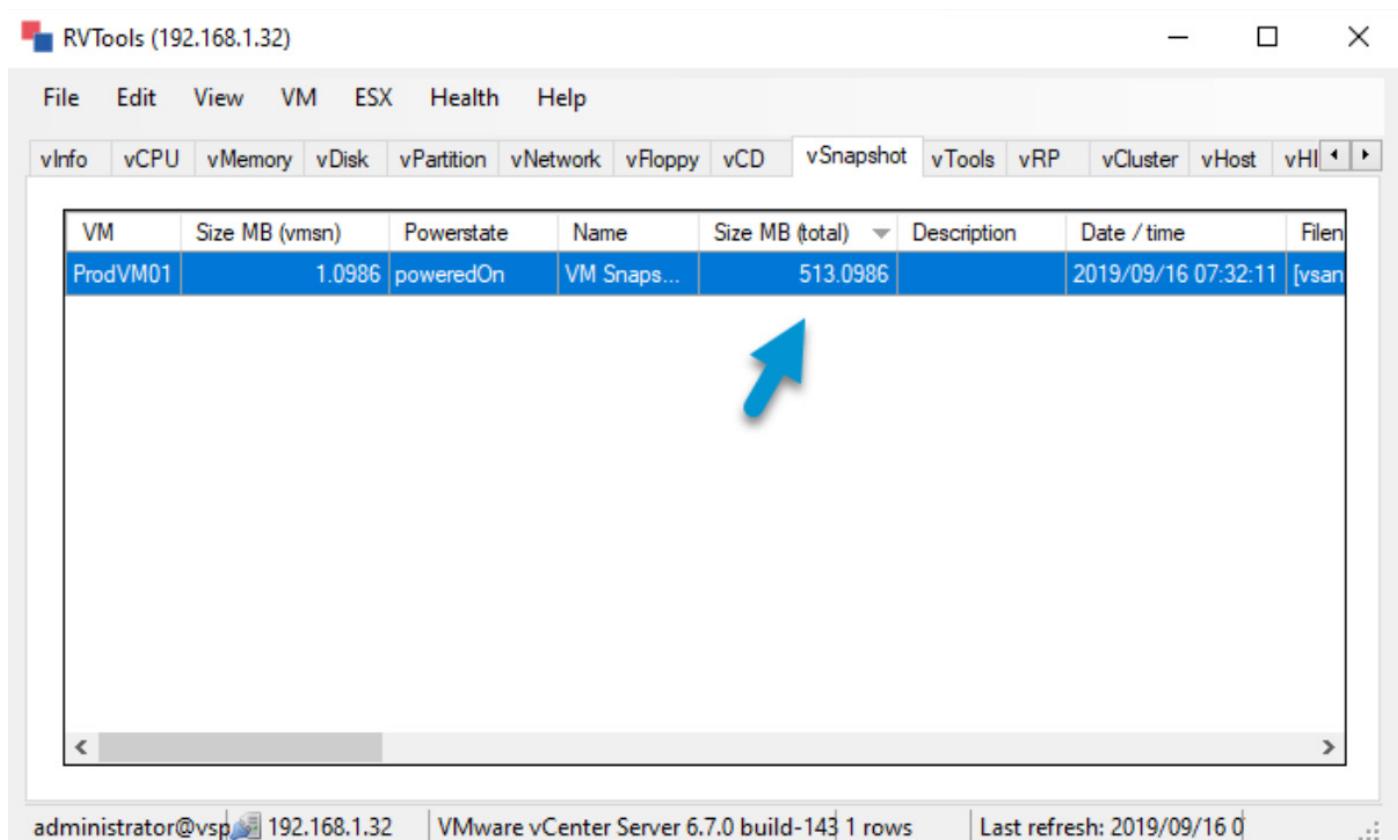
Do not use a snapshot for more than 72 hours. The snapshot files continue to grow as you keep using the VM. This can cause the snapshot storage location to run out of space and impact the system performance.

By default, the storage location is within the same folder as the VM's files, so if you're not cautious and do not have enough space on your datastore to accommodate those grows, your datastore will simply **fills up and your VMs will be suspended**.

### Backup software creates snapshots too

When using a third-party backup software, ensure that snapshots are deleted after a successful backup. In the past, there has been many backup vendors having problems with storage APIs and the problems resulted many snapshots created (and not deleted) after successful or failed backup jobs.

**Note:** Sometimes snapshots taken by third party backup software (through API) may not even appear in the Snapshot Manager, so you'll have to manually check for snapshots from time to time. Either use a command line or manually run some free tools, such as RVTools which shows all snapshots created within your organization.



The screenshot shows the RVTools application window. The title bar reads "RVTools (192.168.1.32)". The menu bar includes File, Edit, View, VM, ESX, Health, Help. The top navigation bar contains tabs: vInfo, vCPU, vMemory, vDisk, vPartition, vNetwork, vFloppy, vCD, vSnapshot, vTools, vRP, vCluster, vHost, vH. The vSnapshot tab is highlighted. Below the tabs is a table with the following data:

VM	Size MB (vmsn)	Powerstate	Name	Size MB (total)	Description	Date / time	File
ProdVM01	1.0986	poweredOn	VM Snaps...	513.0986		2019/09/16 07:32:11	[vsan]

Administrator details at the bottom: administrator@vsp 192.168.1.32 | VMware vCenter Server 6.7.0 build-143 1 rows | Last refresh: 2019/09/16 0

**RVTools shows snapshots and size on datastore**

But there are many other software tools which detects snapshots and even many modern backup vendors integrate snapshot detection (and deletion) at the end of backup job.

That's the case of for example Veeam Backup and replication which checks the datastore to discover orphaned snapshot file. Veeam has a built-in process called "Snapshot hunter".

The Snapshot Hunter is started as a separate process scheduled within every job session. If there are some orphan/phantom snapshots discovered, the Veeam Backup Service schedules the snapshot consolidation, which means that the VMware Snapshot Consolidate method is executed. It uses the same mechanism that VMware vSphere uses for VMs with the “Needs Consolidation status”.

When looking for a backup software, make sure to ensure that snapshots are handled properly.

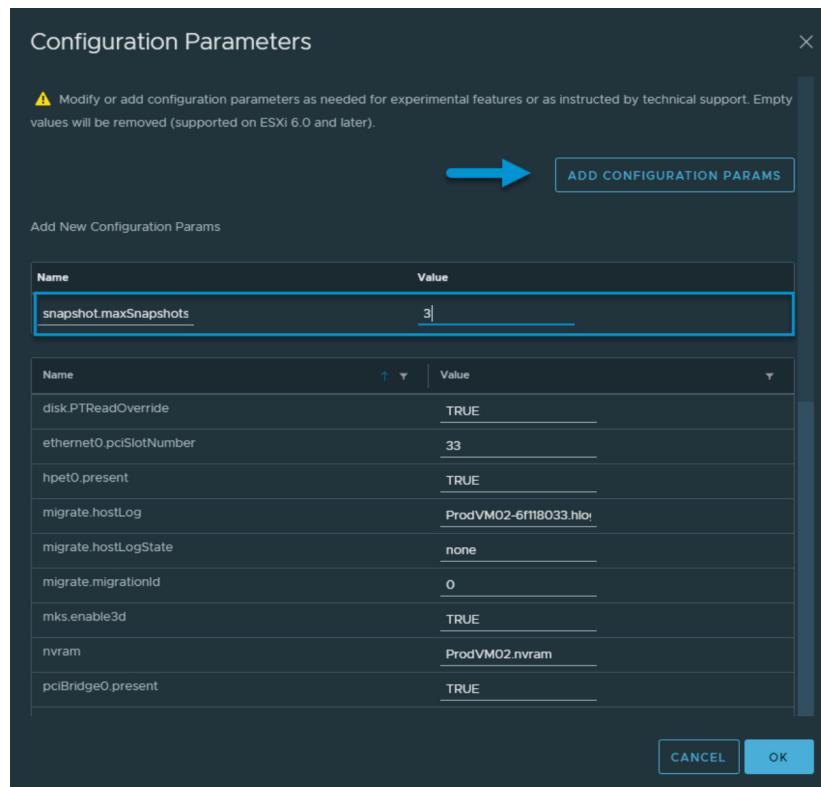
## How many snapshots to keep per VM?

When working with a team where many users have access to a possibility to create a temporary snapshot, it can go wild. Devops environments where many developers maintain their temporary work and use snapshots intensively is just one of many examples.

When multiple users have multiple snapshots on multiple VMs, storage performance might decline and more storage needs to be provisioned.

However, there is a way **to control the number of snapshots allowed per VM**. There is also VMware’s best practice for the number of VM snapshots allowed, which is 32 at maximum, but you should never go that high. I’d limit this to **2-3 snapshots maximum**.

It has to be done at per-vm level and you can do it by editing the VM’s configuration. After clicking on “Edit Configuration” button, **advanced configuration parameters** > Go to “snapshot.maxSnapshots” > “Value” column, change the default setting to 3. This will limit the number of maximum snapshots to three.



**Limit the Maximum snapshots number to three via advanced VM configuration**

This way you can also disable snapshots completely. Just enter “0” to the field and nobody will be able to snapshot the VM. (including your backup software). So actually, to stay safe and still be able to backup your VM, you should enter “1” and have a possibility to take at least one snapshot.

### Snapshot management via UI of vSphere client

This is the easiest way to manage snapshots. The snapshots tree is displayed when you open the snapshot manager.

**Right click a VM > Snapshots > Manage Snapshots.**

Name	VM Snapshot 16%252f09%252f2019 à 07:19:03
Description	another one
Created	09/16/2019, 7:19:09 AM
Disk usage	2.24 GB
Snapshot the virtual machine's memory	Yes
Quiesce guest file system	No

### Manage Snapshots via vSphere client

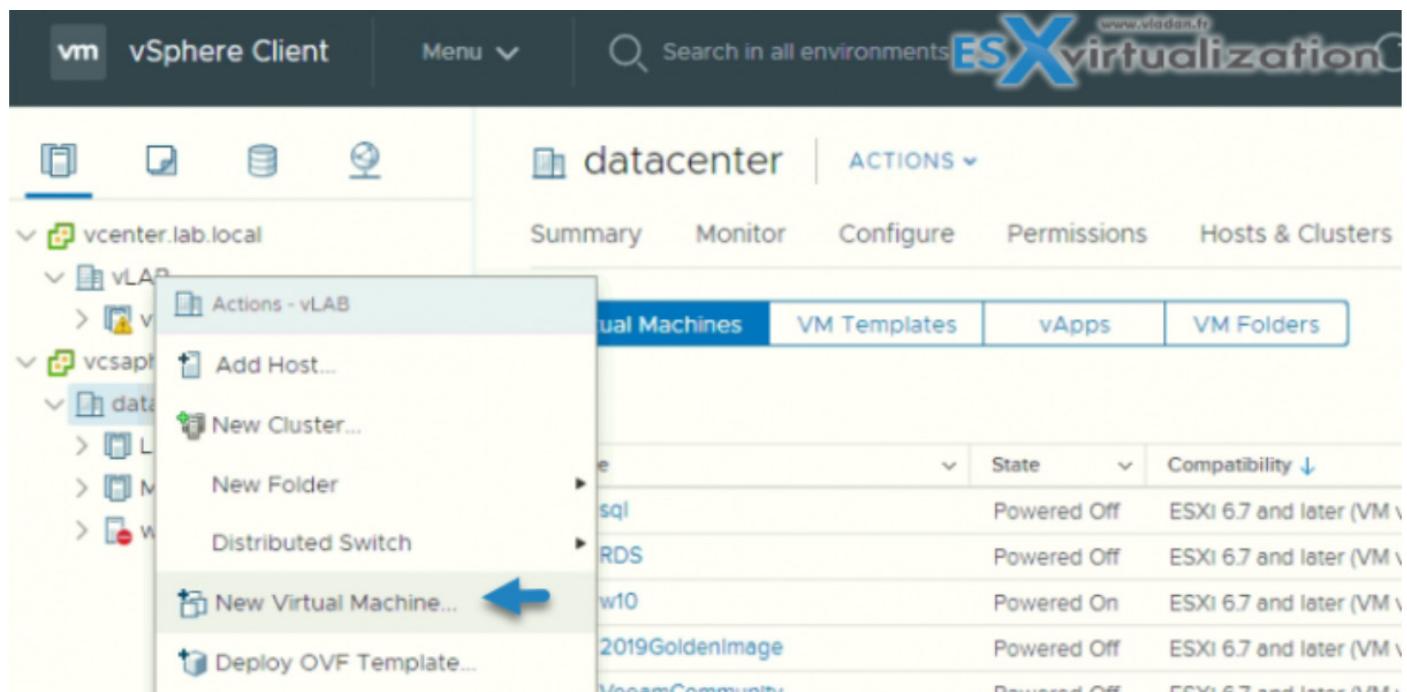
You can delete particular snapshot in a snapshot tree by first selecting it and then hit the Delete button. You can also Delete All snapshots there.

## Objective 7.2 and 7.3 - Create virtual machines using different methods (Open Virtual Machine Format (OVF) templates, content library, etc.)

You 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.



And then the new VM wizard gives you different options. You'll choose the way you would like to proceed.

## New Virtual Machine



### 1 Select a creation type

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Select a creation type

How would you like to create a virtual machine?

#### Create a new virtual machine

- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

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

[CANCEL](#)

[BACK](#)

[NEXT](#)

**Create a new VM** - Create a new VM with a 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 it 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 and especially for permissions necessary for the VM operations.

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

**Where to check storage adapters?**

**Web Client > Hosts and clusters > host > manage > storage > storage adapters**

Adapter	Type	Status	Identifier
vmhba36	Block SCSI	Unknown	
vmhba41	iSCSI	Online	iqn.1998-01.com.vmware:esxi6-01-24295aa2

Name	Type	Capacity	Operational...	Hardware Acceleration	Drive Type
Drobo iSCSI Disk (naa.6001a62...)	disk	1,024.00 GB	Attached	Not supported	HDD

You can also check storage devices there which shows basically all storage attached to the host...

### Identify storage naming conventions

When you select the device tab (as on the image above), you'll see that there is a storage device(s) that are accessible to the host. Depending of the type of storage, ESXi host uses different algorithms and conventions to generate an identifier for each storage device. There are 3 types of identifiers:

- **SCSI Inquire identifiers** - the host query via SCSI INSUIRY command a storage device. The resulting data are being used to generate a unique identifier in different formats (naa. number or t10.number OR eui.number). This is because of the T10 standards.
- **Path-based identifiers** - ex. mpx.vmhba1:C0:T1:L3 means in details - vmhbaAdapter is the name of the storage adapter. Channel - Target - LUN. MPX path is generated in case the

device does not provide a device identifier itself. Note that the generated identifiers are not persistent across reboots and can change.

- **Legacy identifiers** - In addition to the SCSI INQUIRY or mpx. identifiers, for each device, ESXi generates an alternative legacy name. The identifier has the following format: vml.number

The legacy identifier includes a series of digits that are unique to the device.

Check via CLI to see all the details:

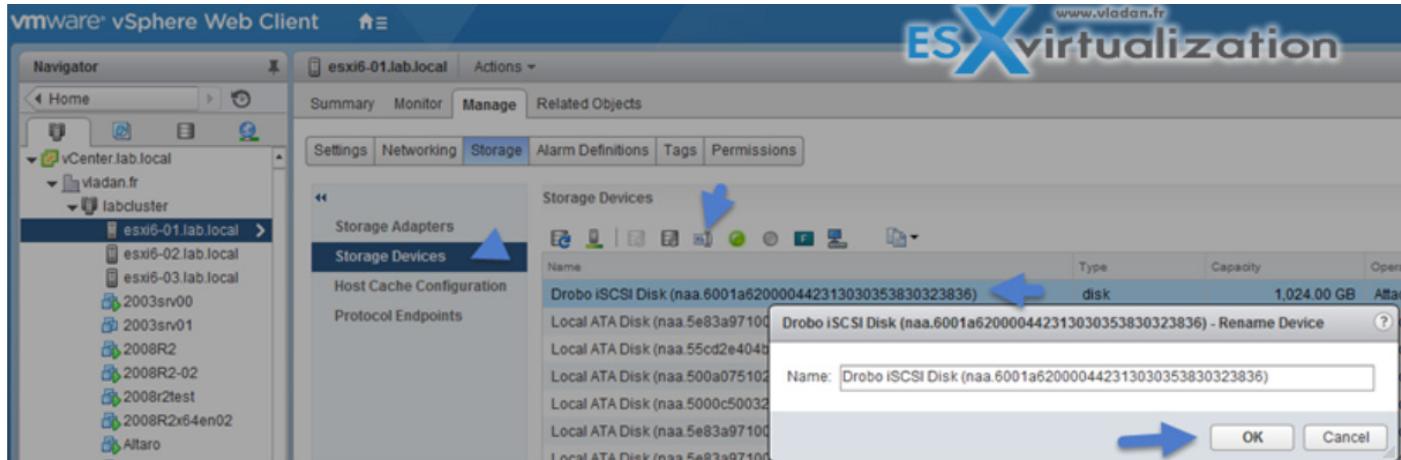
```
esxcli storage core device list
```

```
naa.500a0751095c5844
  Display Name: Local ATA Disk (naa.500a0751095c5844)
  Has Settable Display Name: true
  Size: 457862
  Device Type: Direct-Access
  Multipath Plugin: NMP
  Devfs Path: /vmfs/devices/disks/naa.500a0751095c5844
  Vendor: ATA
  Model: Crucial_CT480M50
  Revision: MU03
  SCSI Level: 6
  Is Pseudo: false
  Status: on
  Is RDM Capable: false
  Is Local: true
  Is Removable: false
  Is SSD: true
  Is VVOL PE: false
  Is Offline: false
  Is Perennially Reserved: false
  Queue Full Sample Size: 0
  Queue Full Threshold: 0
  Thin Provisioning Status: yes
  Attached Filters:
    VAAI Status: unknown
  Other UIDs: vml.0200000000500a0751095c5844437275636961
  Is Shared Clusterwide: false
  Is Local SAS Device: true
  Is SAS: true
  Is USB: false
  Is Boot USB Device: false
  Is Boot Device: false
  Device Max Queue Depth: 32
  No of outstanding IOs with competing worlds: 32
  Drive Type: physical
  RAID Level: NA
  Number of Physical Drives: 1
  Protection Enabled: false
  PI Activated: false
  PI Type: 0
  PI Protection Mask: NO PROTECTION
  Supported Guard Types: NO GUARD SUPPORT
  DIX Enabled: false
  DIX Guard Type: NO GUARD SUPPORT
  Emulated DIX/DIF Enabled: false
```



esxcli storage core device list

Note that the display name can be changed - web client **Select host > Manage > Storage > Storage Devices > select > click rename icon.**



There are also:

Fibre Channel targets which uses World Wide Names (WWN)

- World Wide Port Names (WWPN)
- World Wide Node Names (WWNN)

Check vSphere Storage Guide p.64 for iSCSI naming conventions

**Basically, similar to the WorldWide Name (WWN) for FC devices. iSCSI names are formatted in two different ways. The most common is the IQN format.**

iSCSI Qualified Name (IQN) Format

iqn.yyyy-mm.naming-authority:unique name,

where:

- *yyyy-mm* is the year and month when the naming authority was established.
- *naming-authority* is usually reverse syntax of the Internet domain name of the naming authority. For example, the `iscsi.vmware.com` naming authority could have the iSCSI qualified name form of `iqn.1998-01.com.vmware.iscsi`.
- *unique name* is any name you want to use, for example, the name of your host. The naming authority

- must make sure that any names assigned following the colon are unique, such as:
  - iqn.1998-01.com.vmware.iscsi:name1
  - iqn.1998-01.com.vmware.iscsi:name2
  - iqn.1998-01.com.vmware.iscsi:name999

iSCSI Software Adapter			
vmhba41	iSCSI	Online	iqn.1998-01.com.vmware:esxi6-01-24295aa2

OR

### Enterprise Unique Identifier (EUI) naming format

eui.16 hex digits.

Example: eui.16hexdigits ie eui.0123456789ABCDEF

### Identify hardware/dependent hardware/software iSCSI initiator requirements

Two types of iSCSI adapters.

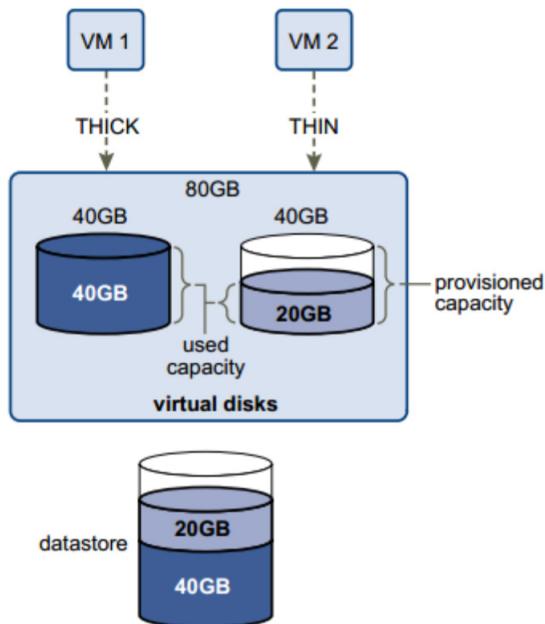
- Hardware based** - add-On iSCSI cards (can do boot-on-lan). Those types of adapters are also capable of offloading the iSCSI and network processing so the CPU activity is lower. Hardware adapters can be dependent or independent. Compared to Dependent, the Independent adapters do not use VMkernel adapters for connections to the storage.
- Software based** - activated after installation (cannot do boot-on-lan). Brings a very light overhead. Software based iSCSI uses VMkernel adapter to connect to iSCSI storage over a storage network.

Dependent adapters can use CHAP, which is not the case of Independent adapters.

### Compare and contrast array thin provisioning and virtual disk thin provisioning

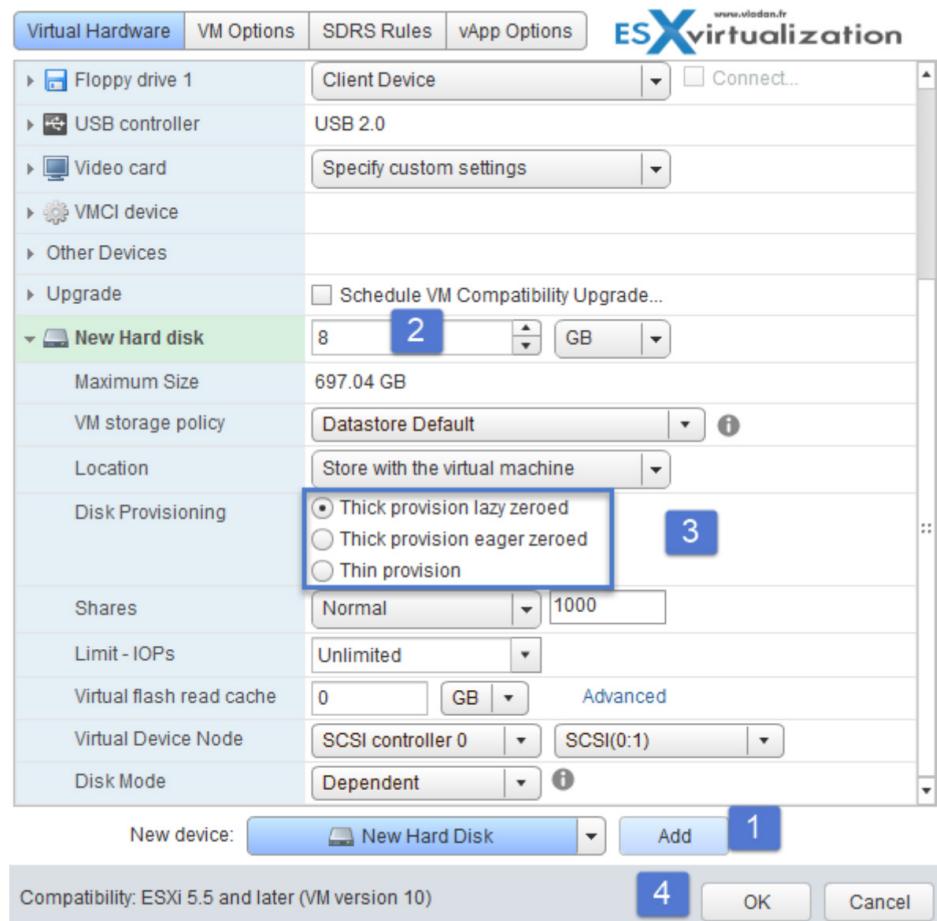
**Virtual disk thin provisioning** allows to allocate only small amount of disk space at the storage level, but the guest OS sees as it had the whole space. The thin disk grows in size when adding more data, installing applications at the VM level.

So it's possible to over-allocate the datastore space, but it brings a risks so it's **important to monitor** actual storage usage to avoid conditions when you run out of physical storage space.

**Figure 23-1.** Thick and thin virtual disks

- **Thick Lazy Zeroed** - default thick format. Space is allocated at creation, but the physical device is not erased during the creation process, but zeroed-on-demand instead.
- **Thick Eager Zeroed** - Used for FT protected VMs. Space is allocated at creation and zeroed immediately. The data remaining on the physical device is zeroed out when the virtual disk is created. Takes longer to create Eager Zeroed Thick disks.
- **Thin provision** - as on the image above. Starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin disk can be **inflated** (thin > thick) via datastore browser (right click vmdk > inflate).

Check the different VMDK disk provisioning options when creating new VM or adding an additional disk to existing VM



### Thin-provisioned LUN

Array Thin Provisioning and VMFS Datastores on p. 257.

ESXi also supports thin-provisioned LUNs. When a LUN is thin-provisioned, the storage array reports the LUN's logical size, which might be larger than the real physical capacity backing that LUN. A VMFS datastore that you deploy on the thin-provisioned LUN can detect only the logical size of the LUN.

For example, if the array reports 2TB of storage while in reality the array provides only 1TB, the datastore considers 2TB to be the LUN's size. As the datastore grows, it cannot determine whether the actual amount of physical space is still sufficient for its needs.

Via Storage API -Array integration (VAAI) you CAN be aware of underlying thin-provisioned LUNs. VAAI let the array know about datastore space which has been freed when files are deleted or removed to allow the array to reclaim the freed blocks.

Check thin provisioned devices via CLI:

```
esxcli storage core device list -d vmlxxxxxxxxxxxxxx
```

```
[root@esxi6-01:~] esxcli storage core device list -d vml.02000000005e83a9710005
20d64f435a2d5341
naa.5e83a971000520d6
  Display Name: Local ATA Disk (naa.5e83a971000520d6)
  Has Settable Display Name: true
  Size: 228936
  Device Type: Direct-Access
  Multipath Plugin: NMP
  Devfs Path: /vmfs/devices/disks/naa.5e83a971000520d6
  Vendor: ATA
  Model: OCZ-SABER1000
  Revision: 1.00
  SCSI Level: 6
  Is Pseudo: false
  Status: on
  Is RDM Capable: false
  Is Local: true
  Is Removable: false
  Is SSD: true
  Is VVOL PE: false
  Is Offline: false
  Is Perennially Reserved: false
  Queue Full Sample Size: 0
  Queue Full Threshold: 0
  Thin Provisioning Status: yes
  Attached Filters:
    VAAI Status: unknown
    Other UIDs: vml.02000000005e83a971000520d64f435a2d5341
    Is Shared Clusterwide: false
    Is Local SAS Device: true
    Is SAS: true
    Is USB: false
    Is Boot USB Device: false
    Is Boot Device: false
    Device Max Queue Depth: 32
    No of outstanding IOs with competing worlds: 32
    Drive Type: physical
    RAID Level: NA
    Number of Physical Drives: 1
    Protection Enabled: false
    PI Activated: false
    PI Type: 0
    PI Protection Mask: NO PROTECTION
    Supported Guard Types: NO GUARD SUPPORT
    DIX Enabled: false
    DIX Guard Type: NO GUARD SUPPORT
    Emulated DIX/DIF Enabled: false
[root@esxi6-01:~]
```



## Describe zoning and LUN masking practices

Zoning is used with FC SAN devices. Allow controlling the SAN topology by defining which HBAs can connect to which targets. We say that we zone a LUN. Allows:

- Protecting from access non desired devices the LUN and possibly corrupt data
- Can be used for separation different environments (clusters)
- Reduces number of targets and LUN presented to host
- Controls and isolates paths in a fabric.

Best practice? Single-initiator-single target

### LUN masking

`esxcfg-scsidevs -m` — the `-m`

`esxcfg-mpath -L | grep naa.5000144fd4b74168`

`esxcli storage core claimrule add -r 500 -t location -A vmhba35 -C 0 -T 1 -L 0 -P MASK_PATH`

```
esxcli storage core claimrule load
```

```
esxcli storage core claiming reclaim -d naa.5000144fd4b74168
```

## Unmask a LUN

```
esxcli storage core claimrule remove -r 500
```

```
esxcli storage core claimrule load
```

```
esxcli storage core claiming unclaim -t location -A vmhba35 -C 0 -T 1 -L 0
```

```
esxcli storage core adapter rescan -A vmhba35
```

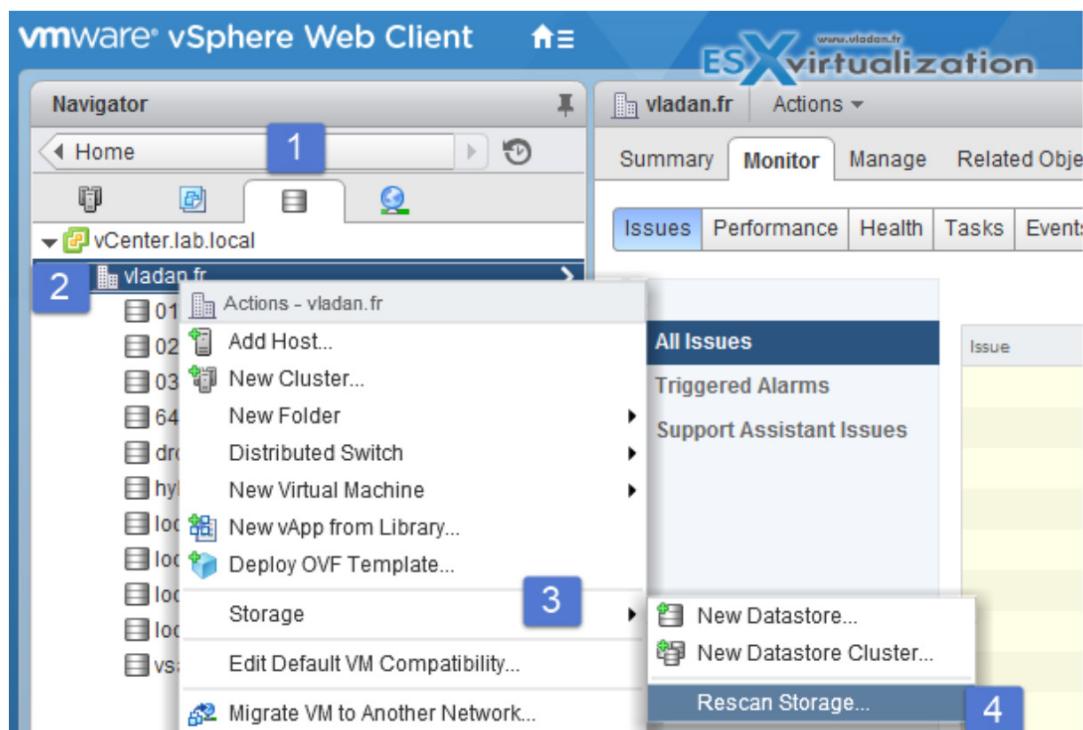
## Scan/Rescan storage

Perform the manual rescan each time you make one of the following changes.

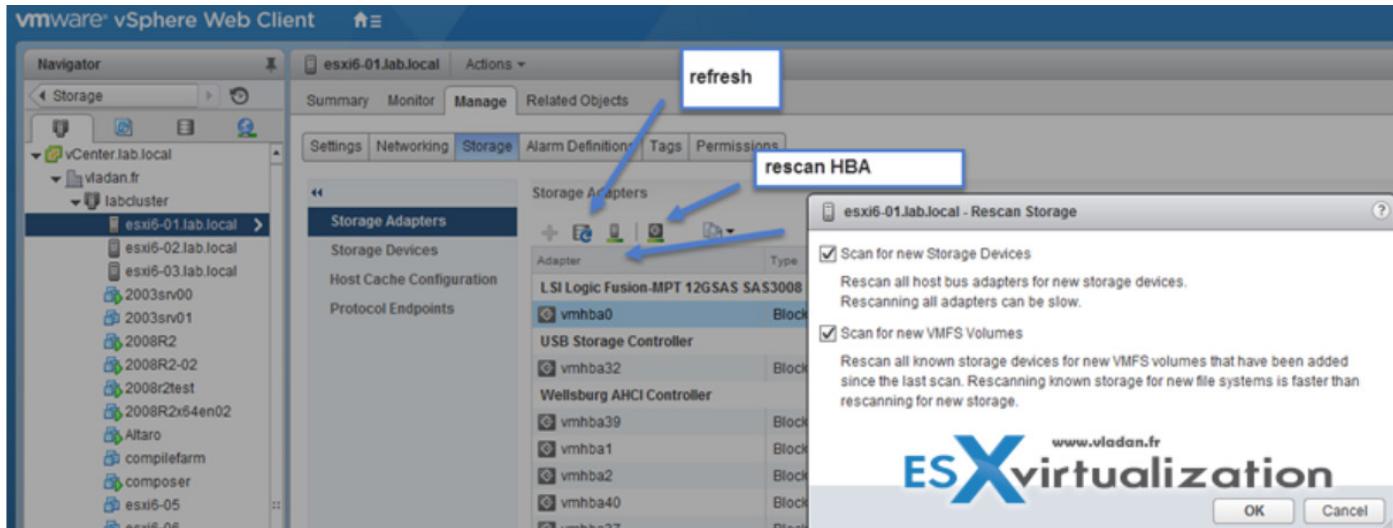
- Zone a new disk array on a SAN.
- Create new LUNs on a SAN.
- Change the path masking on a host.
- Reconnect a cable.
- Change CHAP settings (iSCSI only).
- Add or remove discovery or static addresses (iSCSI only).

Add a single host to the vCenter Server after you have edited or removed from the vCenter Server a datastore shared by the vCenter Server hosts and the single host.

You can scan at the Host level or at the datacenter level (storage > select datacenter > right click > Storage > Rescan storage).



Click host > manage > storage > storage adapters



- Scan for New Storage Device – Rescans HBAs for new storage devices
- Scan for New VMFS Volumes – Rescans known storage devices for VMFS volumes
- Configure FC/iSCSI LUNs as ESXi boot devices
- Few requirements. As being said, only the hardware iSCSI can boot from LUN.
- Boot from SAN is supported on FC, iSCSI, and FCoE.
- 1:1 ratio - Each host must have access to its own boot LUN only, not the boot LUNs of other hosts.
- Bios Support - Enable the boot adapter in the host BIOS
- HBA config - Enable and correctly configure the HBA, so it can access the boot LUN.

## Create an NFS share for use with vSphere

An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it for its storage needs. vSphere supports versions 3 and 4.1 of the NFS protocol.

**How?** By exporting NFS volume as NFS v3 or v4.1 (latest release). Different storage vendors have different methods of enabling this functionality, but typically this is done on the NAS servers by using the **no\_root\_squash** option. If the NAS server does not grant root access, you might still be able to mount the NFS datastore - but **read only**.

NFS uses VMkernel port so you need to configure one.

v3 and v4.1 compare:

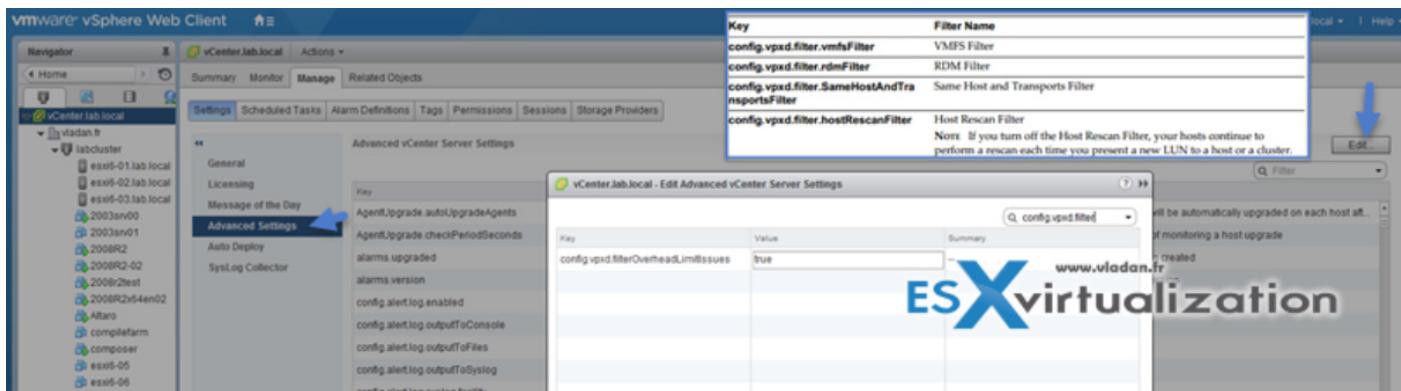
## NFS Protocols and vSphere Solutions

vSphere Features	NFS version 3	NFS version 4.1
vMotion and Storage vMotion	Yes	Yes
High Availability (HA)	Yes	Yes
Fault Tolerance (FT)	Yes	Yes
Distributed Resource Scheduler (DRS)	Yes	Yes
Host Profiles	Yes	Yes
Storage DRS	Yes	No
Storage I/O Control	Yes	No
Site Recovery Manager	Yes	No
Virtual Volumes	Yes	No

## Enable/Configure/Disable vCenter Server storage filters

When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. p. 167 of vSphere 6 storage guide.

Where? Hosts and clusters > vCenter server > manage > settings > advanced settings



In the value box type **False** for appropriate key.

From the vSphere Storage Guide:

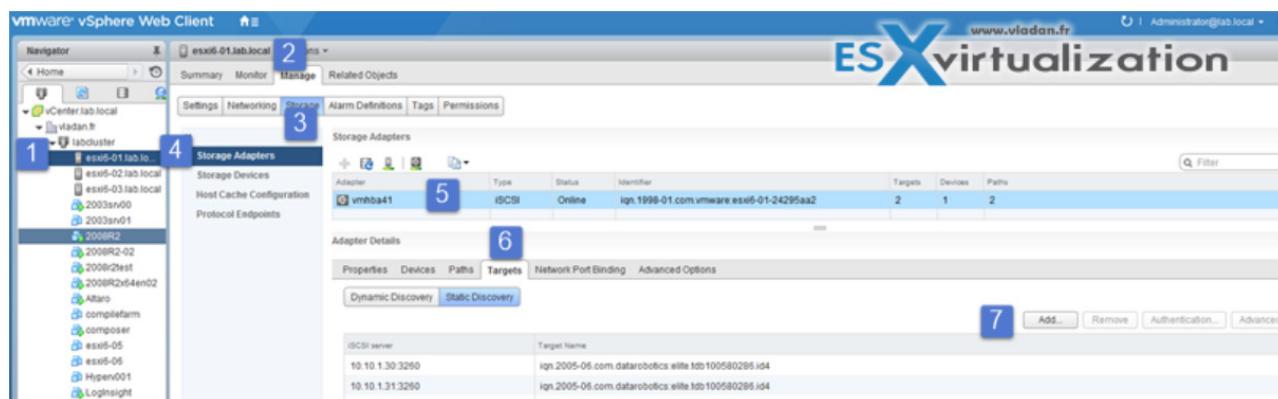
Key	Filter Name
<b>config.vpxd.filter.vmfsFilter</b>	VMFS Filter
<b>config.vpxd.filter.rdmFilter</b>	RDM Filter
<b>config.vpxd.filter.SameHostAndTransportsFilter</b>	Same Host and Transports Filter
<b>config.vpxd.filter.hostRescanFilter</b>	Host Rescan Filter <b>NOTE</b> If you turn off the Host Rescan Filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.

## Configure/Edit hardware/dependent hardware initiators

### Where?

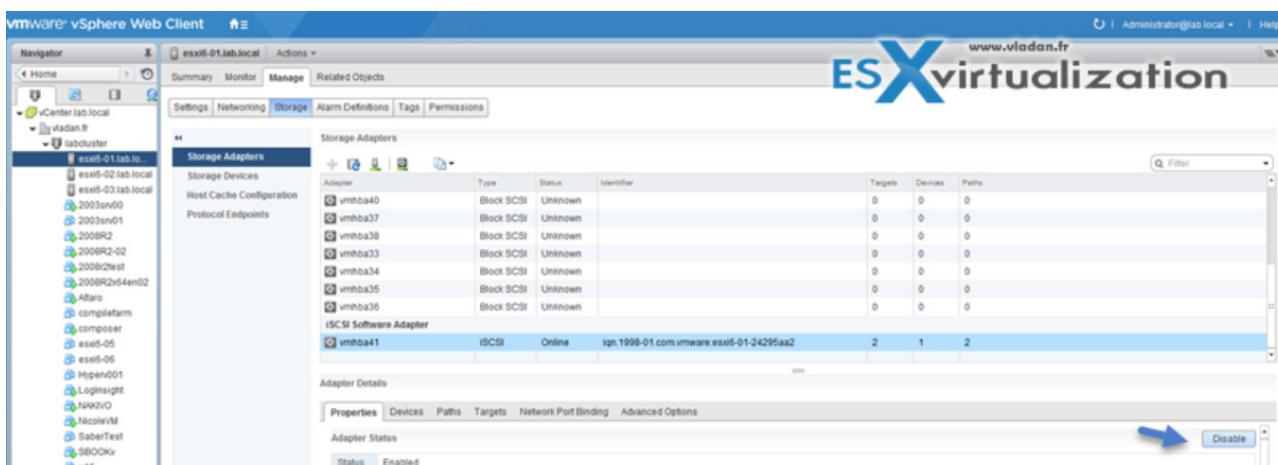
Host and Clusters > Host > Manage > Storage > Storage Adapters.

It's possible to rename the adapters from the default given name. It's possible to configure the **dynamic** and **static** discovery for the initiators.



It's not so easy to find through Web client, as before we use to do it eyes closed through a vSphere client...

## Enable/Disable software iSCSI initiator



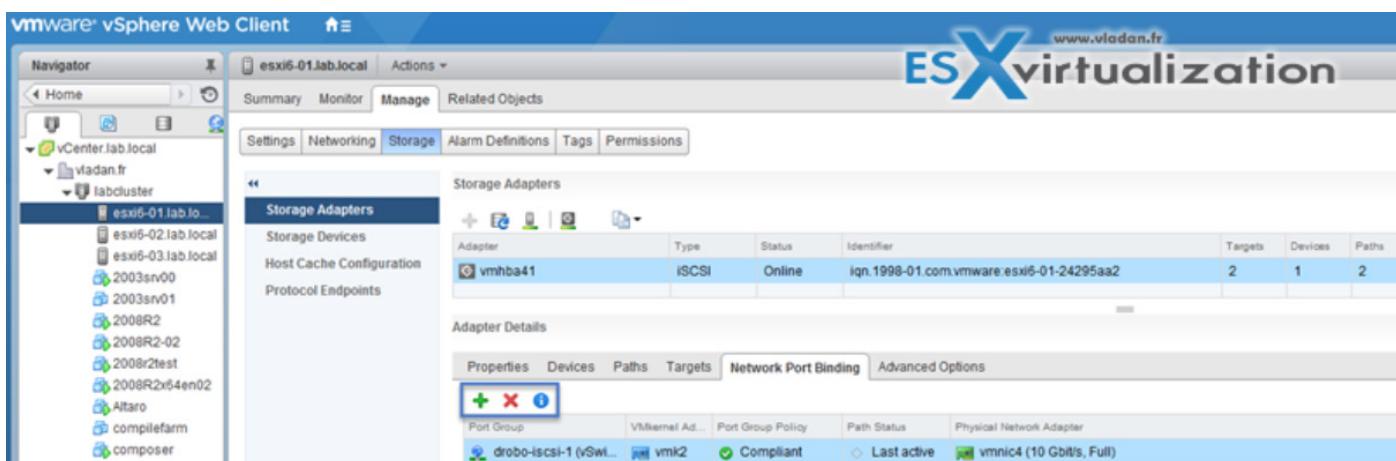
## Configure/Edit software iSCSI initiator settings

As being said above, to configure and Edit Software iSCSI initiator settings, you can use Web client or C# client. **Web Client > Host and Clusters > Host > Manage > Storage > Storage Adapters**

And there you can:

- View/Attach/Detach Devices from the Host
- Enable/Disable Paths
- Enable/Disable the Adapter
- Change iSCSI Name and Alias
- Configure CHAP
- Configure Dynamic Discovery and (or) Static Discovery
- Add Network Port Bindings to the adapter
- Configure iSCSI advanced options

## Configure iSCSI port binding



Port binding allows to configure multipathing when :

- iSCSI ports of the array target must reside in the same broadcast domain and IP subnet as the VMkernel adapters.
- All VMkernel adapters used for iSCSI port binding must reside in the same broadcast domain and IP subnet.
- All VMkernel adapters used for iSCSI connectivity must reside in the same virtual switch.
- Port binding does not support network routing.

Do not use port binding when **any** of the following conditions exist:

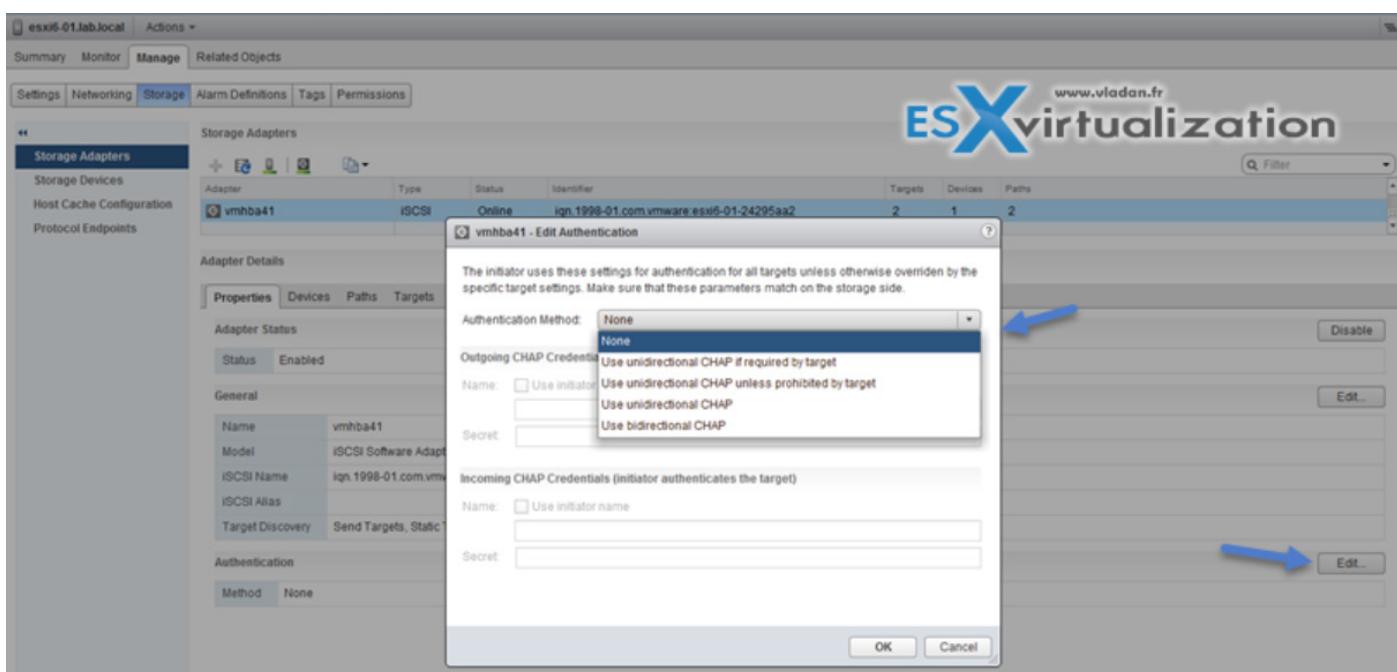
- Array target iSCSI ports are in a different broadcast domain and IP subnet.
- VMkernel adapters used for iSCSI connectivity exist in different broadcast domains, IP subnets, or use
- different virtual switches.
- Routing is required to reach the iSCSI array.

**Note:** The VMkernel adapters must be configured with single **Active uplink**. All the others as unused only (not Active/standby). If not they are not listed...

### Enable/Configure/Disable iSCSI CHAP

#### Where?

**Web Client > Host and Clusters > Host > Manage > Storage > Storage Adapters > Properties > Authentication (Edit button).**



Challenge Handshake Authentication Protocol (CHAP), which verifies the legitimacy of initiators that access targets on the network.

**Unidirectional CHAP** - target authenticates the initiator, but the initiator does not authenticate the target.

**Bidirectional CHAP** - an additional level of security enables the initiator to authenticate the target. VMware supports this method for software and dependent hardware iSCSI adapters only.

## Chap methods:

- **None** - CHAP authentication is not used.
- **Use unidirectional CHAP if required by target** - Host prefers non-CHAP connection but can use CHAP if required by target.
- **Use unidirectional CHAP unless prohibited by target** - Host prefers CHAP, but can use non-CHAP if target does not support CHAP.
- **Use unidirectional CHAP** - Requires CHAP authentication.
- **Use bidirectional CHAP** - Host and target support bidirectional CHAP.

CHAP does not encrypt, only authenticates the initiator and target.

## Determine use case for hardware/dependent hardware/software iSCSI initiator

It's fairly simple, as we know that if we use the **software iSCSI adapter** we do not have to buy additional hardware and we're still able to «hook» into iSCSI SAN.

The case for **Dependent Hardware iSCSI Adapter** which is dependant on the VMKernel adapter but offloads iSCSI processing to the adapter, which accelerates the treatment and reduces CPU overhead.

On the other hand, the **Independent Hardware iSCSI Adapter** has its own networking, iSCSI configuration, and management interfaces. So you must go through the BIOS and the device configuration in order to use it.

## Determine use case for and configure array thin provisioning

Some arrays do support thin provisioned LUNs while others do not. The benefit is to offer more capacity (visible) to the ESXi host while consuming only what's needed at the datastore level. (attention however for over-subscribing, so proper monitoring is needed). So at the datastore level it's possible to use thin provisioned virtual disk or on the array using thin provisioned LUNs.

## Tools

- vSphere Installation and Setup Guide
- vSphere Storage Guide
- [Best Practices for Running VMware vSphere® on iSCSI](#)
- vSphere Client / vSphere Web Client

## Objective 7.4.1 – Configure and modify datastores

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 Datastores:

- **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**



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 <a href="#">Manually Reclaim Accumulated Storage Space</a> .	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, there is a second part as well..

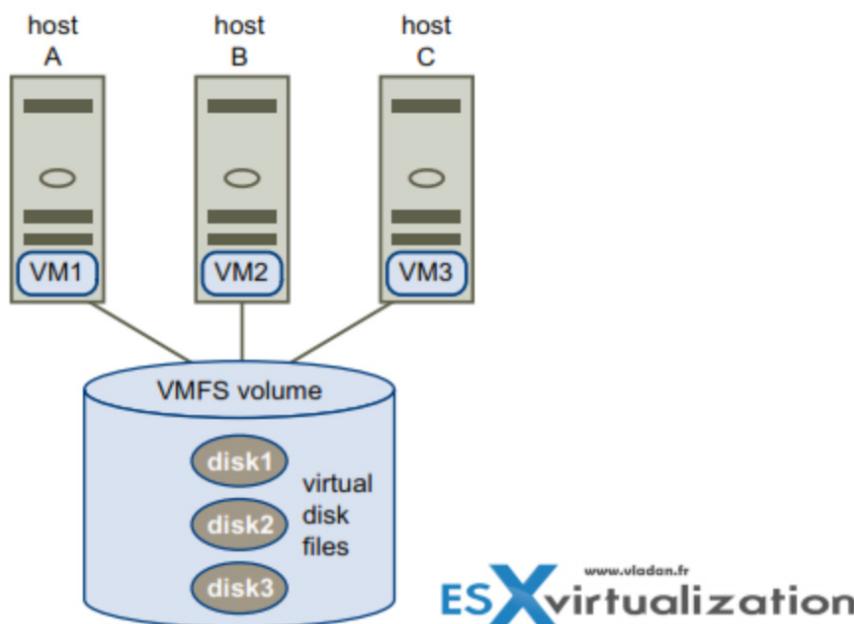
**Table 17-3. Comparing VMFS5 and VMFS6 (Continued)**

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 <a href="#">VMFS Locking Mechanisms</a> .	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 (ATSSonly), or use a combination of ATS and SCSI reservations (ATS+SCSI).

**Figure 17-1. Sharing a VMFS Datastore Across Hosts**



**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 the size 2 TB and larger.

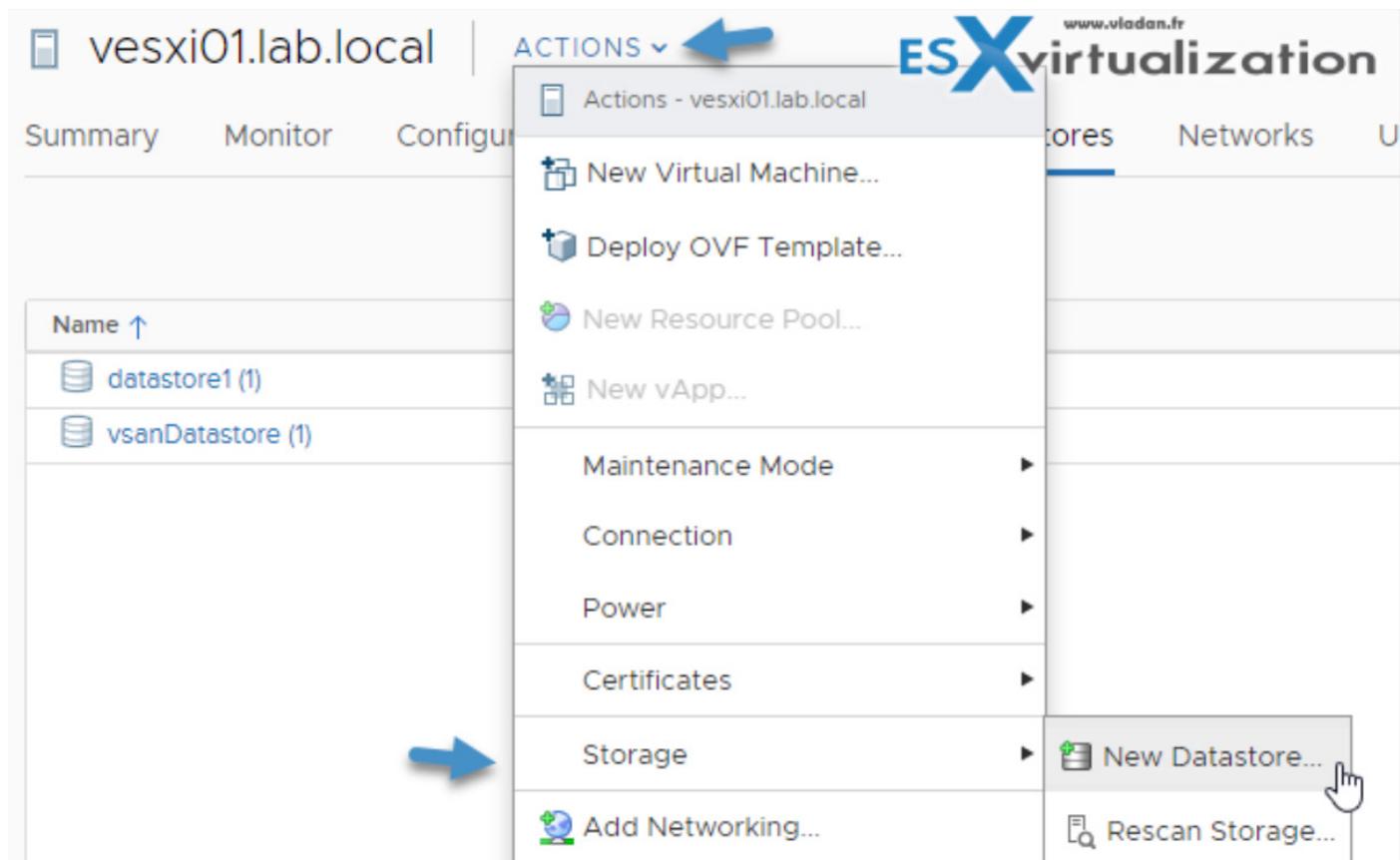
## Snapshot Migration

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 the 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. Choose the type of datastore you wish to create.

## New Datastore



**1 Type**

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

Type  
Specify datastore type.

VMFS  
Create a VMFS datastore on a disk/LUN.

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

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

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

and then select the device.

## New Datastore



**1 Type**  
**2 Name and device selection**

3 VMFS version  
4 Partition configuration  
5 Ready to complete

Name and device selection  
Select a name and a disk/LUN for provisioning the datastore.

Datastore name: NewDatastore

Name	LUN	Capacity	Hardware...	Drive T...	S
Local VMware Disk (mpx....)	0	70.00 GB	Unknown	Flash	E

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

And then chose VMFS 6 (or VMFS 5 if older ESXi hosts will be accessing this datastore).

## New Datastore



- 1 Type
- 2 Name and device selection
- 3 VMFS version**
- 4 Partition configuration
- 5 Ready to complete

### VMFS version

Specify the VMFS version for the datastore.

VMFS 6

VMFS 6 enables advanced format (512e) and automatic space reclamation support.

VMFS 5

VMFS 5 enables 2+TB LUN support.

CANCEL

BACK

NEXT

and then chose the option which are useful for your environment.

## New Datastore



- 1 Type
- 2 Name and device selection
- 3 VMFS version
- 4 Partition configuration**
- 5 Ready to complete

### Partition configuration

Review the disk layout and specify partition configuration details.

#### Partition Configuration

Use all available partitions

#### Datastore Size

70 GB

#### Block size

1 MB

#### Space Reclamation Granularity

1 MB

#### Space Reclamation Priority

Low: Deleted or unmapped blocks are reclaimed

on the LUN at Low priority

Empty: 70.0 GB

CANCEL

BACK

NEXT

**Administrative operations** - operations such as renaming, but other operations (Mount, unmount, remove, use datastore browser, rename datastore files) as well depending on the type of datastore.

**Organize datastores** - you can organize datastores into folders depending on usage or others

**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:

- There are no VMs on the datastore you wish to analyze.
- 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)
- For VMFS3 the LUN masking has to be in place by using claim rules.
- The volume does not have several extents.

**Step 1.** Connect via SSH and enter this command to obtain the name and partition number of the device which has the VMFS datastore.

`esxcli storage vmfs extent list`

You'll see an output like this

Volume Name	VMFS UUID	Extent Number	Device Name	Partition
SATA_Spinning_R0ST	58b26784-9848-0e92-2720-6805ca349160	0	t10.ATA__ST31000528AS	6VPB9053
RAID10	58d4caf8-4a19a71f-4760-6805ca349160	0	msa.600508e0000000006b0e402dd3f0b60d	1
IntelINVMe	5a1ed9d2-4ab9bd00-4af2-90151737c92e	0	t10.INVMe_INTEL_SSDEKDD1480GA	FUM5736300404800GB_00000001
Trion960SSD	5a656ed8-dd693d08-15f0-00151737e02e	0	msa.5e63a972003355afe	1

**Step 2.** Then 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 no errors.

```
[root@esxi6-03:] voma -m vmfs -f check -d /vmfs/devices/disks/t10.ATA__ST31000528AS_6VPB9053:1
Checking if device is actively used by other hosts
Scanning for VMFS-3/VMFS-5 host activity (512 bytes/HB, 2048 HBs).
Found 1 actively heartbeating hosts on device '/vmfs/devices/disks/t10.ATA__ST31000528AS_6VPB9053:1'
1) MAC address 00:15:17:87:c0:2e, IP 10.10.5.13
[root@esxi6-03:]
```

## The options:

You can find all options by typing, as usually:

```
voma -h
```

The output looks like this:

```
[root@esxi6-03:~] voma -h
Usage: .....  
voma [OPTIONS] -m module -d device  
-m, --module      Name of the module to run.  
                  Available Modules are  
                  1. lvm  
                  2. vmfs  
                  3. ptbl  
-f, --func        Function(s) to be done by the module.  
                  Options are  
                  query   - list functions supported by module  
                  check   - check for Errors  
                  fix     - check & fix  
                  dump    - collect metadata dump  
-d, --device      Device/Disk to be used  
-s, --logfile     Path to file, redirects the output to given file  
-x, --extractDump Extract the dump collected using VOMA  
-D, --dumpfile    Dump file to save the metadata dump collected  
-v, --version     Prints voma version and exit.  
-h, --help         Print this help message.  
Example:  
voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x  
voma -m vmfs -f dump -d /vmfs/devices/disks/naa.xxxx:x -D dumpfilename
```



You can log the output to a file with the -s option or further display help message with each VOMA command.

## VOMA on our testing system has 4 options:

**query** - list functions supported by module

**check** - check for Errors

**fix** - check & fix

**dump** - collect metadata dump

A two VMware KB articles which are interesting to read. One of them helps you via the help 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 cautions too.

**Quote:**

Shutting down a virtual machine running on files having 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](#)

## Objective 7.4.2 Create virtual machine storage policies

Before we start talking about VMware Storage Policy-Based Management (SPBM), we should explain what it is and how it can help admins manage vSphere environments more efficiently.

SPBM provides a universal framework for different types of storage, whether they be vSAN, virtual volumes, input/output (I/O) filters, or other storage methods. It provides a universal control plane across multiple data services and storage solutions.

On one side there are storage capabilities of storage arrays—VMware vSAN and others, and on the other side there is virtual machine (VM) provisioning based on VM storage policies.

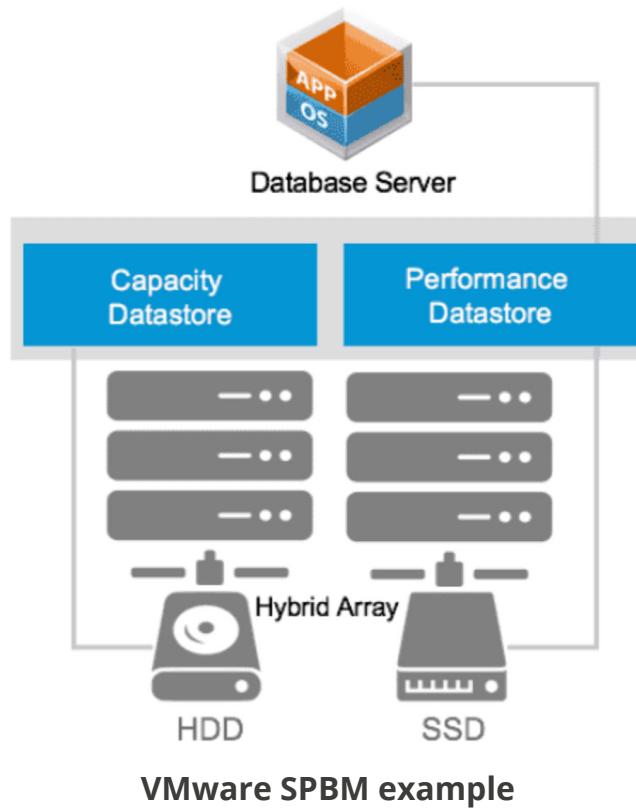
In between there is bidirectional communication between ESXi and vCenter Server (on one end) and storage arrays and entities on the other.

The admin can build different storage policies, select capabilities of the underlying storage array, and then apply the policies to VMs. It is possible to create tags and tag categories and then apply these to the storage medium to define their capabilities.

SPBM looks at the storage requirements found in policies associated with individual VMs and then places the VM on the right storage tier. The available capabilities vary by storage vendor.

After creating a storage policy, an admin can assign a VM (or just the data disk where an important database is located) to a more performant datastore or a subset of datastores without thinking of hardware that runs underneath.

Here is an example below.



## How to create a storage policy

In this post, we'll create a VM storage policy based on tags.

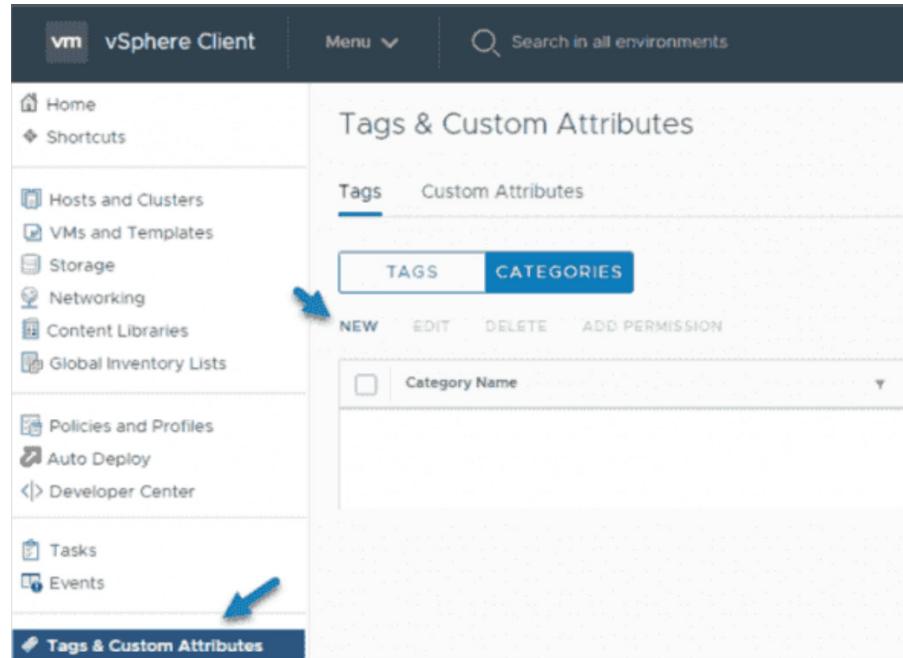
One of the first actions when starting with SPBM is to tag the available datastores within our environment with custom metadata we must define. We'll have to create tags and tag categories.

The entire process of creating and managing storage policies usually has a few steps.

- Populate the VM Storage Policies interface with appropriate data.
- Create predefined storage policy components.
- Create VM storage policies.
- Apply the VM storage policies to the VMs.
- Verify the compliance for the VM storage policies.

VMFS and NFS datastores are not represented by storage provider. These datastores show their capabilities and data services in the VM Storage Policies interface.

You can use tags to encode information about these datastores. As an example, we can tag VMFS datastores as VMFS-Gold and VMFS-Silver to differentiate different levels of service they provide.



### Tags and custom attributes

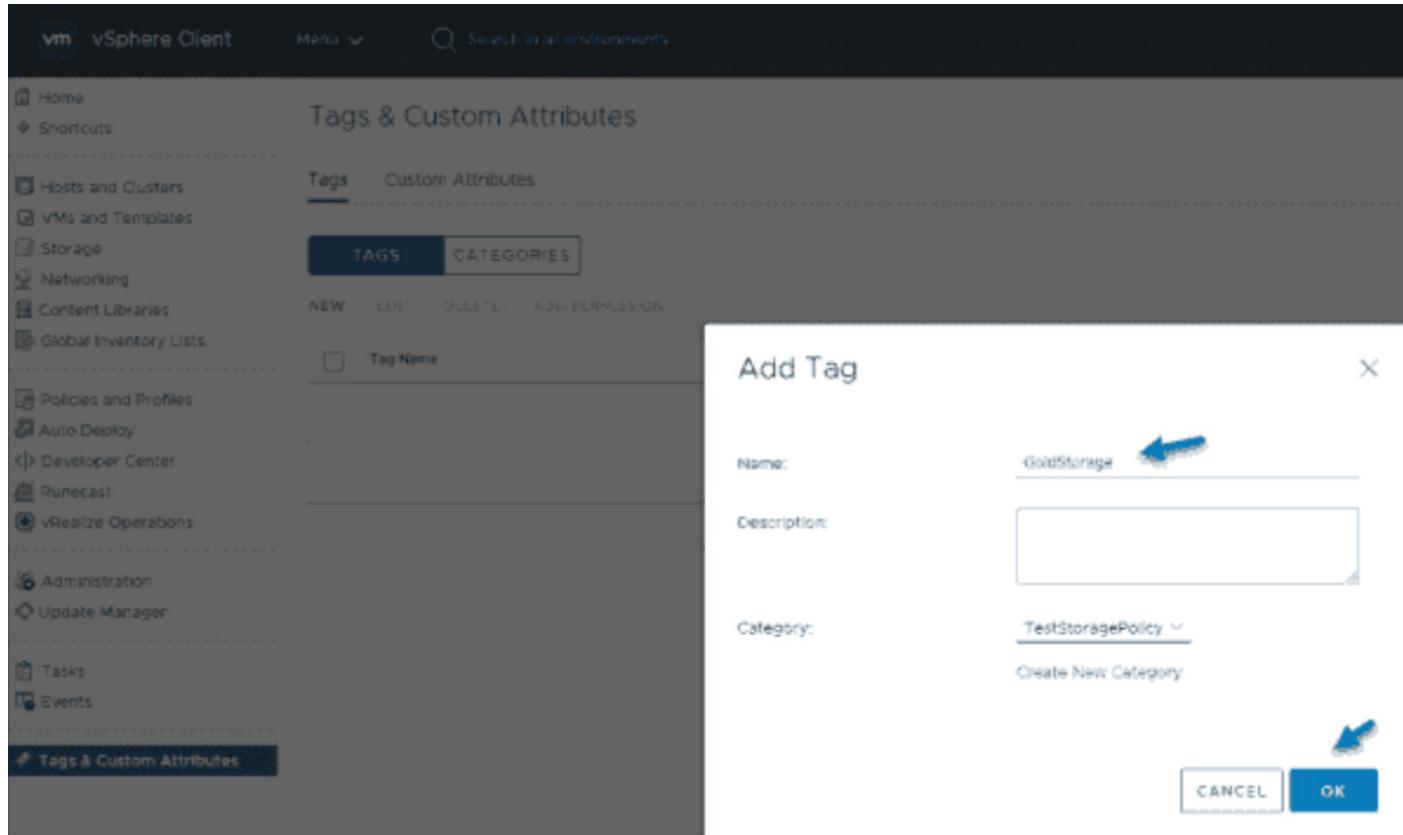
Then you enter a meaningful name for the category. As an example in our case, we can simply use *TestStoragePolicy*.

Add Category

Category Name:	TestStoragePolicy
Description:	<input type="text"/>
Tags Per Object:	<input type="radio"/> One tag <input checked="" type="radio"/> Many tags <span style="color: red;">←</span>
Associable Object Types:	<input type="checkbox"/> All objects <input type="checkbox"/> Folder <input type="checkbox"/> Cluster <input type="checkbox"/> Datacenter <span style="color: red;">→</span> <input checked="" type="checkbox"/> Datastore <input checked="" type="checkbox"/> Datastore Cluster <input type="checkbox"/> Distributed Port Group <input type="checkbox"/> Distributed Switch <input type="checkbox"/> Host <input type="checkbox"/> Content Library <input type="checkbox"/> Library Item <input type="checkbox"/> Network <input type="checkbox"/> Resource Pool <input type="checkbox"/> vApp <input type="checkbox"/> Virtual Machine
	<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">CANCEL</span> <span style="border: 1px solid #0070C0; color: white; background-color: #0070C0; padding: 2px 10px; font-weight: bold;">OK</span>

### Add objects to tag category

Once we have created the tag category, we'll need to create tags. For the sake of simplicity, let's call the tag *GoldStorage*.



### Create a new tag

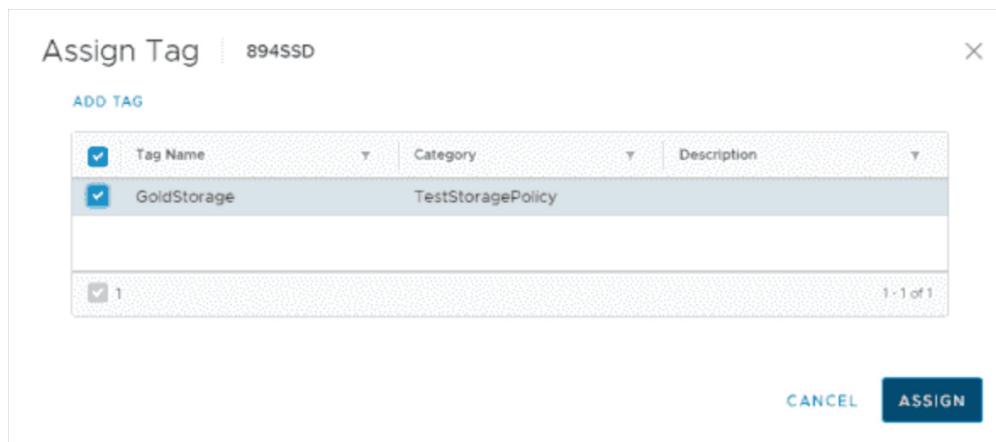
## Tag the VMware vSphere datastores

Now that we have successfully created a tag category and tags, we can tag our datastores with these tags.

We can do this by **right-clicking the datastore** and then going to **Tags & Custom Attributes**.

Click «Assign Tag»

And then select the tag from the list. You can have many tags here, but we only have one in this example.



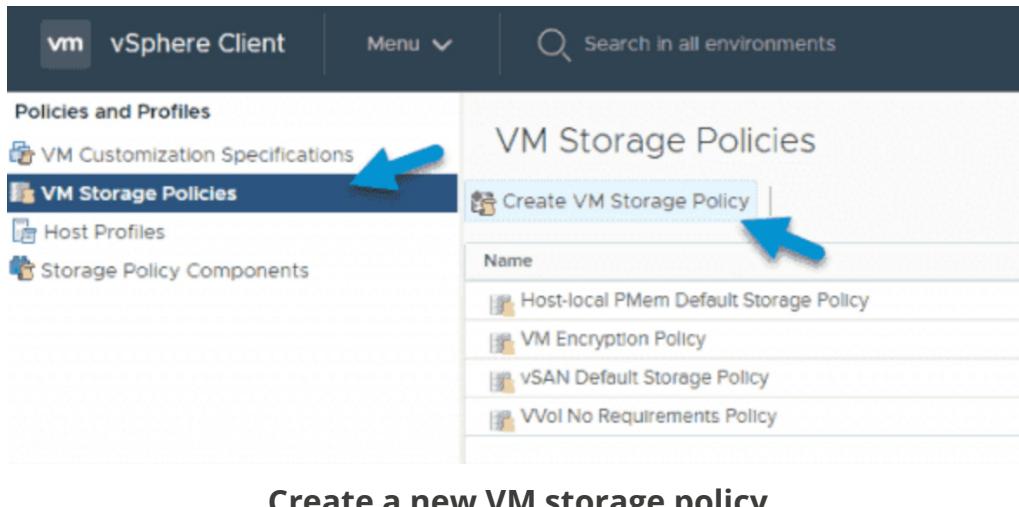
### Select the tag to assign to the datastore

## Create VMware VM storage policies

So finally, we've got to the point where all we have left is to create a VM storage policy. We'll use the shortcut from the main UI, or we can also do this via **Menu > Policies and Profiles**.

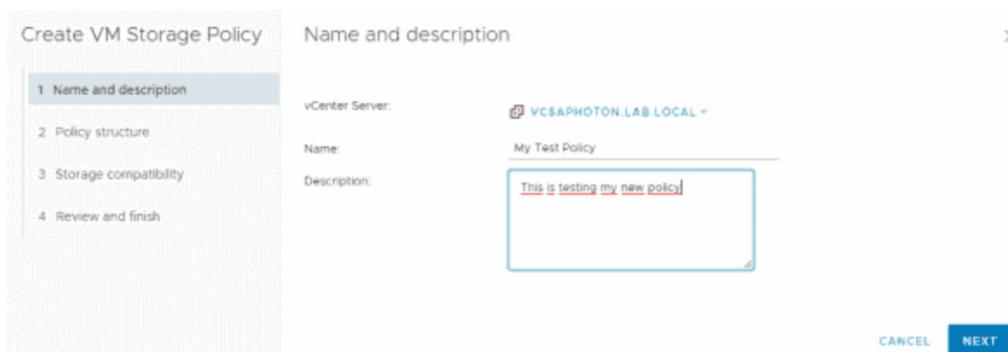
Go to «Policies and Profiles» via the menu

Then click the **VM Storage Policies** icon and click **Create VM Storage Policy**.



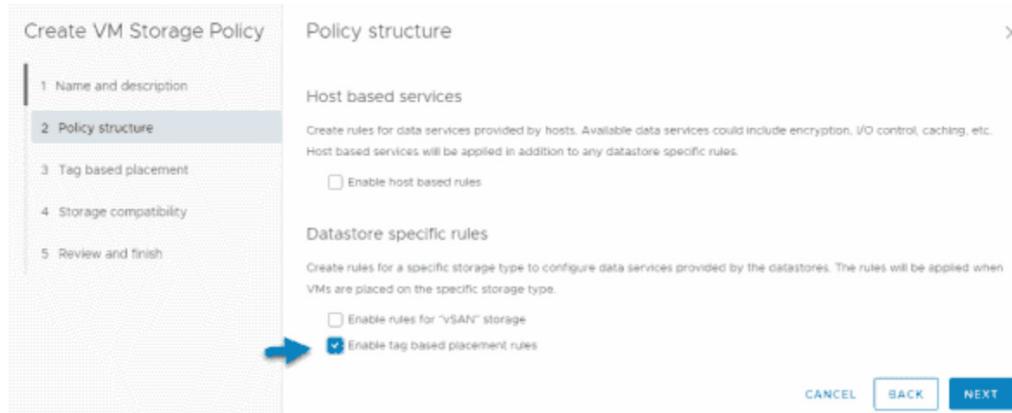
### Create a new VM storage policy

You'll get a new window where you'll have to enter some details.



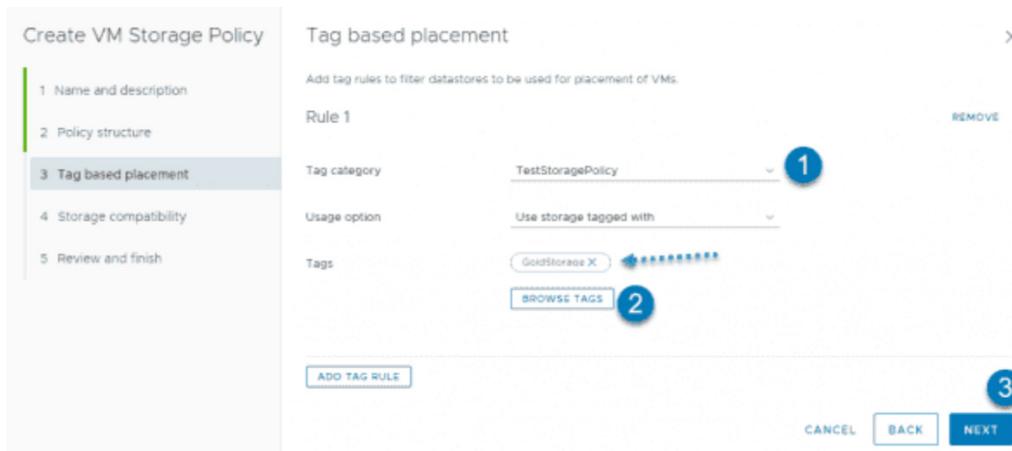
### VM storage policy wizard

Pick host-based services or datastore-specific rules or both. In our case, I've only checked the datastore-specific rules because I just want to show how to use the tag-based ones.



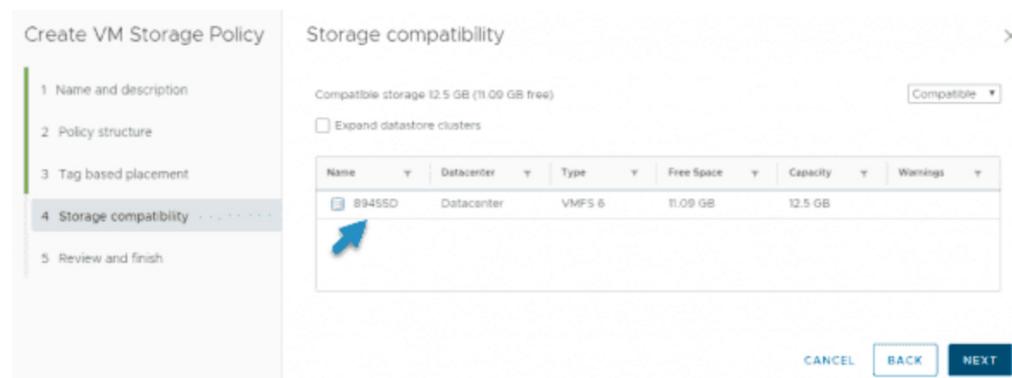
## Datastore specific and tag based placement rules

Click **Next** and pick the tag category we've created earlier.



## Add tag rules to filter datastores to use for placing VMs

Then on the next screen, you will see the datastore you have tagged during one of the earlier steps.



## Pick the compatible storage device

## Create a new VM or clone an existing VM to test the storage policy

Finally, we can test our storage policy by either creating a new VM or cloning an existing VM so we can test the storage placement based on tags.

With SPBM, upon creating a VM, the storage policy automates selecting the datastores that fulfill the requirements listed within the storage policy.

As you can see, when choosing our «test policy,» we can choose the compatible storage of our datastore that we tagged in our earlier step.

And it lists this datastore as «compatible,» so we're sure to use the datastore with a capability we specified via a tag.

**Note:** As you can see on the image below, you can even provision a new VM and separate VMDKs. Examples have different performance datastores assigned to «system» and «data» disks.

You can assign two separate policies to each of the VM's disks. You can assign a mission-critical (Gold) policy to the disk that is a database. At the same time, you can apply some other storage (Silver) policy to the VM's operating system (OS).

### ProdVM02 - Clone Existing Virtual Machine

The screenshot shows the 'ProdVM02 - Clone Existing Virtual Machine' wizard, specifically Step 3: Select storage. On the left, a progress bar indicates steps 1 through 5. Step 3 is highlighted with a blue box. The main area shows a 'Select storage' section with a dropdown menu set to 'My Test Policy'. Below it is a table of storage options. The first row, '894SSD', is highlighted with a blue arrow and has its details (Capacity: 12.5 GB, Provisioned: 1.41 GB, Free: 11.09 GB) displayed. The second row, 'vsanDatastore', is also visible. At the bottom are 'CANCEL', 'BACK', and 'NEXT' buttons.

Name	Capacity	Provisioned	Free
894SSD	12.5 GB	1.41 GB	11.09 GB
vsanDatastore	359.98 GB	188.37 GB	229.59 GB

## VM operations for initial placement

## Objective 7.4.3 - Configure storage cluster options

VMware Distributed Resource Scheduler (DRS) is a VMware feature that optimizes the performance and resources of your vSphere cluster. Storage DRS was introduced in vSphere several releases ago, and it is still a key feature of vSphere 7.

Storage cluster configuration with Storage DRS (SDRS) in vSphere 7 allows you to balance virtual machine disk files (VMDK) between datastores in the datastore cluster.

In the same way as traditional DRS, where VMs are placed initially onto the healthiest host, the initial placement is manual with SDRS. After the VM is placed onto a datastore, the SDRS function keeps an eye on those datastores and makes sure none of them becomes completely filled.

If the utilization of the datastore rises above a predefined threshold, the DRS will issue a recommendation to move some VMDKs off this datastore and place them on a datastore with sufficient free space.

SDRS also monitors I/O latency and checks what has happened in the last 24 hours. There might have been a datastore with some heavy I/O over the past 24 h, which might mean the system won't move VMDKs onto it.

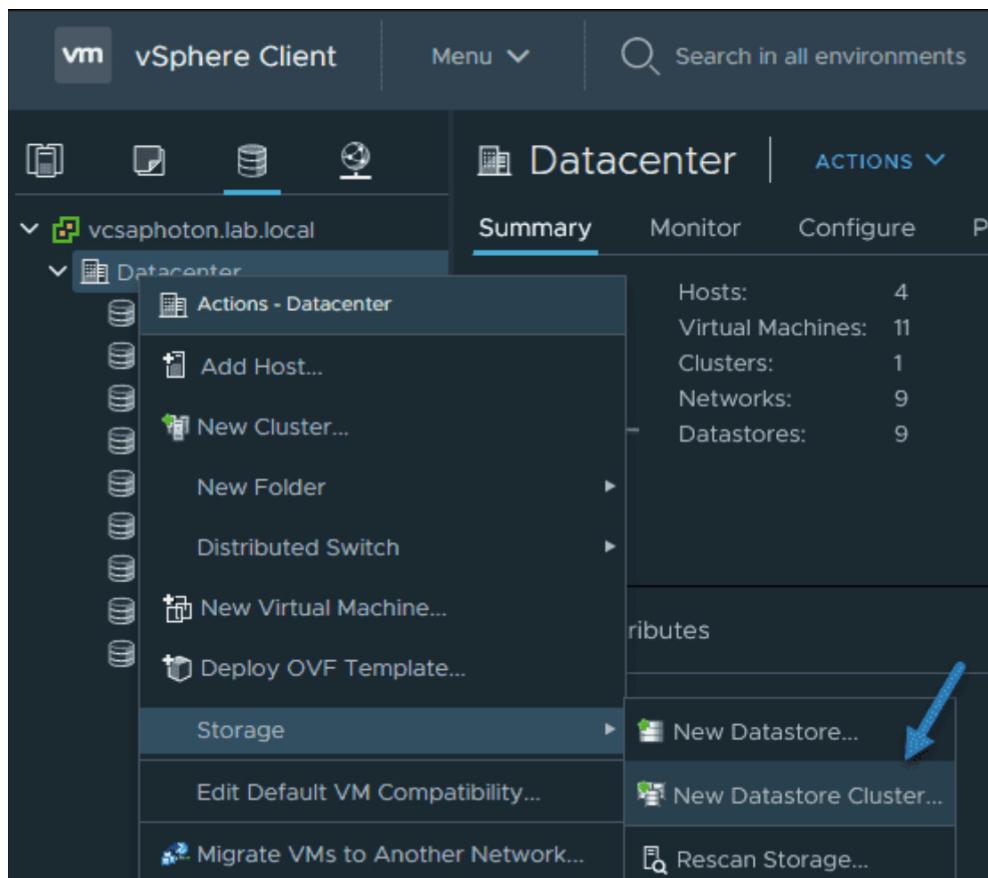
SDRS allows you to put a datastore into maintenance mode, allowing you to evacuate your VMDKs off to another datastore to enable decommissioning.

You can use VMFS or NFS-based datastores, but you can't combine VMFS with NFS in the same SDRS cluster. In this case, simply create separate SDRS clusters.

If you have some storage arrays that support hardware acceleration, you should not mix them with other arrays that don't have it. As a good practice, the datastore cluster should remain homogeneous.

### How to create new datastore clusters

You'll need to log in via your vSphere web client. Select the relevant datacenter object. Right-click it and select **Datacenter > Storage > New Datastore Cluster**.



### Create a new datastore cluster

Then, on the next page, give it a meaningful name so you recognize which SDRS cluster you're working with. You can create several SDRS clusters within your datacenter.

**New Datastore Cluster**

1 Name and Location

2 Storage DRS Automation

3 Storage DRS Runtime Se...

4 Select Clusters and Hosts

5 Select Datastores

6 Ready to Complete

Name and Location

Datastore cluster name: **Prod**

Location **Datacenter**

Turn ON Storage DRS

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

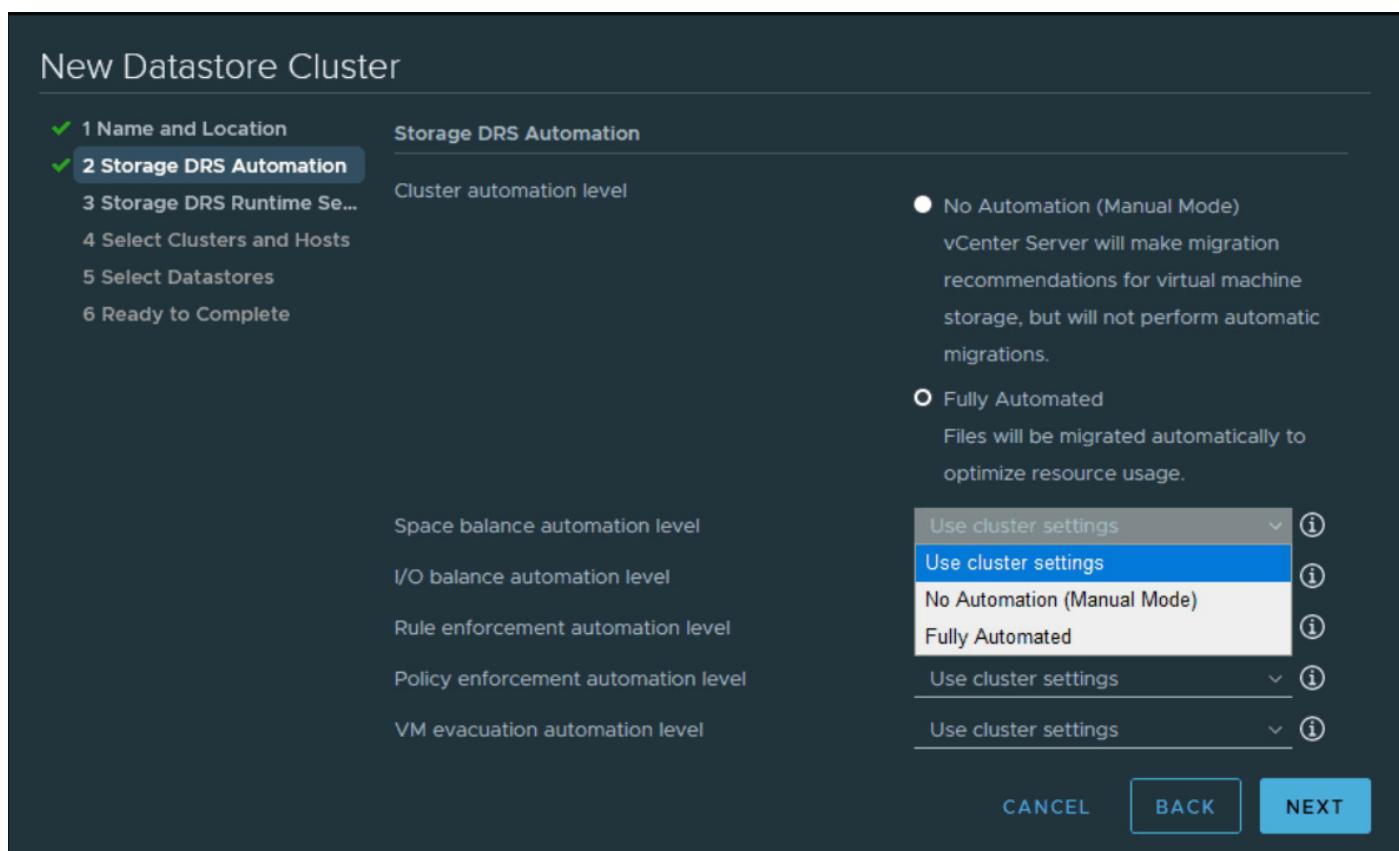
vSphere Storage DRS also enables vCenter Server to manage the assignment of virtual machines to datastores, suggesting placement when virtual machines are created, migrated or cloned, and migrating running virtual machines to balance load and enforce placement rules.

CANCEL BACK NEXT

### Turn On Storage DRS checkbox

Then, on the next page, you can choose between Fully Automated or No Automation (Manual mode). This is a one-or-the-other choice.

- You have different granularity options available that allow you to override the cluster settings. This means that you can have cluster settings on fully automatic, but individual options can be set as needed. **Space balance automation level** — Shows what to do when there is a recommendation to correct a space load imbalance in a datastore cluster.
- **I/O balance automation level** — Allows you to choose what happens when it generates recommendations for correcting an I/O load imbalance in a datastore cluster.
- **Rule enforcement automation level** — Specifies SDRS behavior when it generates recommendations for correcting affinity rule violations in a datastore cluster. Affinity rules allow you to place different VMDKs on different datastores. Useful for Microsoft clustered applications, for example.
- **Policy enforcement automation level** — Specifies SDRS behavior when it generates recommendations for correcting storage and VM policy violations in a datastore cluster.
- **VM evacuation automation level** — Specifies SDRS behavior when it generates recommendations for VM evacuations from datastores in a datastore cluster.



### Choose Fully Automated or Manual Mode

The next page of the wizard presents you with Storage DRS Runtime Settings. You can set the different options for I/O where the I/O metrics are considered as a part of any SDRS recommendation or automated migration in this datastore cluster.

You can also set the I/O latency threshold and space threshold, such that you can set a minimum level of free space per datastore. Those settings allow you to migrate VMDKs off a datastore when the low space threshold kicks in.

**New Datastore Cluster**

**Storage DRS Runtime Settings**

**I/O Metric inclusion**

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

**I/O latency threshold**  
Dictates the minimum I/O latency for each datastore below which I/O load balancing moves are not considered.  
5 ms  100 ms **15 ms**

**Space threshold**  
Runtime thresholds govern when Storage DRS performs or recommends migrations (based on the selected automation level).  
 Utilized space  
50 %  100 % **80 %**

**CANCEL** **BACK** **NEXT**

### Storage DRS runtime settings

The next page of the wizard allows you to select the cluster and hosts that will be part of the cluster.

**New Datastore Cluster**

**Select Clusters and Hosts**

**Selected (0)**

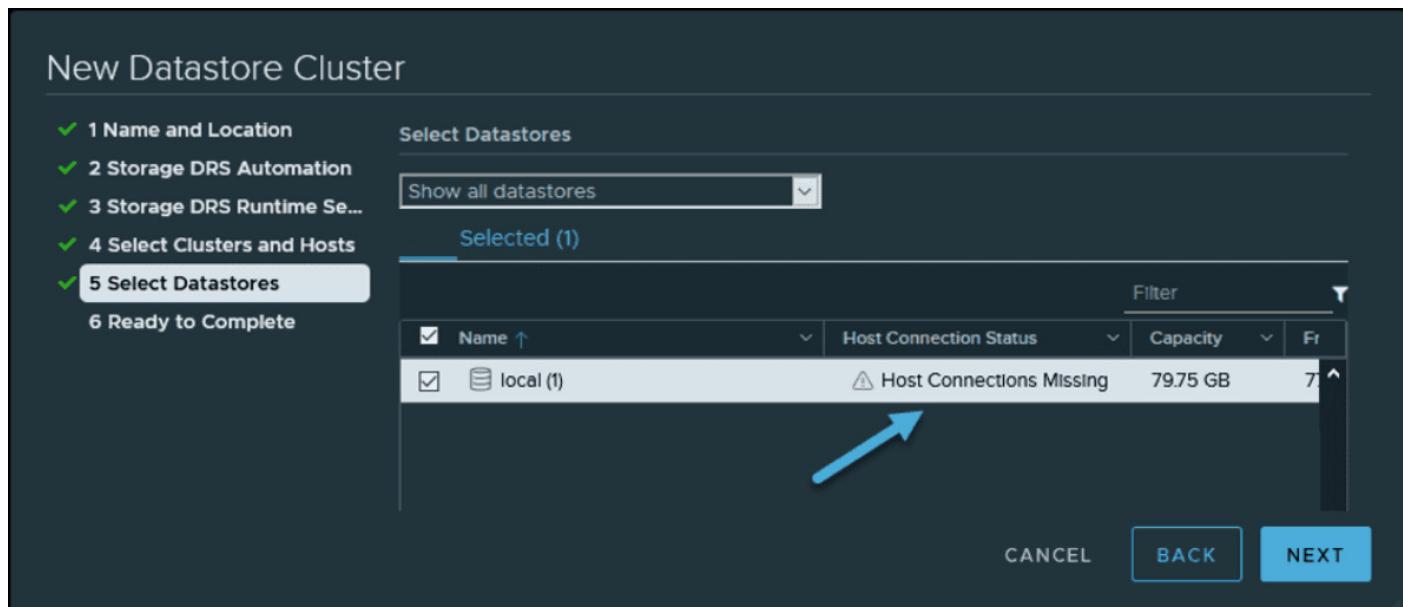
**Clusters** **Standalone Hosts**

Name	Available CPU	Available Memory
Cluster	19.92 GHz	49.3 GB

**CANCEL** **BACK** **NEXT**

### Select clusters and hosts that will be part of the SDRS cluster

The last page of the wizard shows us which datastores can be used. In our small lab case, we only have a local datastore, and as you can see, there is a warning telling us “Host connections missing.” This is because we only have a local datastore here, no shared datastores.



### Host Connection Missing warning

This concludes the creation of the datastore cluster in which we activated SDRS.

SDRS is an intelligent vCenter Server system that automatically and efficiently manages VMFS and NFS storage. It is very similar to DRS, which optimizes the performance and resources of your vSphere cluster.

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

VMware vSphere 7 has a really good system for configuring different workloads and their requirements. You might have VMs which are meant to stay together on the same host or you may have VMs which should not execute on the same host. VMware calls it VM-to-VM affinity and anti-affinity rules.

When studying to pass VMware VCP-DCV exam, the knowledge of affinity and anti-affinity rules is required.

VMware Distributed Resource Scheduler (DRS) that balances and optimizes the VM's performance and DRS score which is a measure of the resources available for consumption by the VM. The higher the DRS score for a VM, the better is the resource availability for that VM.

VMware DRS moves a VM from one host to another in order to improve this VM DRS score, however it respects the VM-to-VM affinity and anti-affinity rules.

Affinity rules are also respected by VMware High Availability (HA) which does initial placement of VMs to a host. VM Affinity/anti-affinity rules force specified virtual machines to remain together (or apart) during failover actions. If you create a DRS affinity rule for your cluster, you can specify how vSphere HA applies that rule during a VM failover.

Additionally, when your DRS is configured in fully automated mode, the system can misplace some VMs which you would not like to as you might have a special requirement (separation or keep together).

For example, if you have application composed of multiple VMs (web frontend, application server, database backend). Those 3 applications are most likely having strong network traffic between each other. So, the backend traffic would be quite significant if you leave to run those VMs on different hosts.

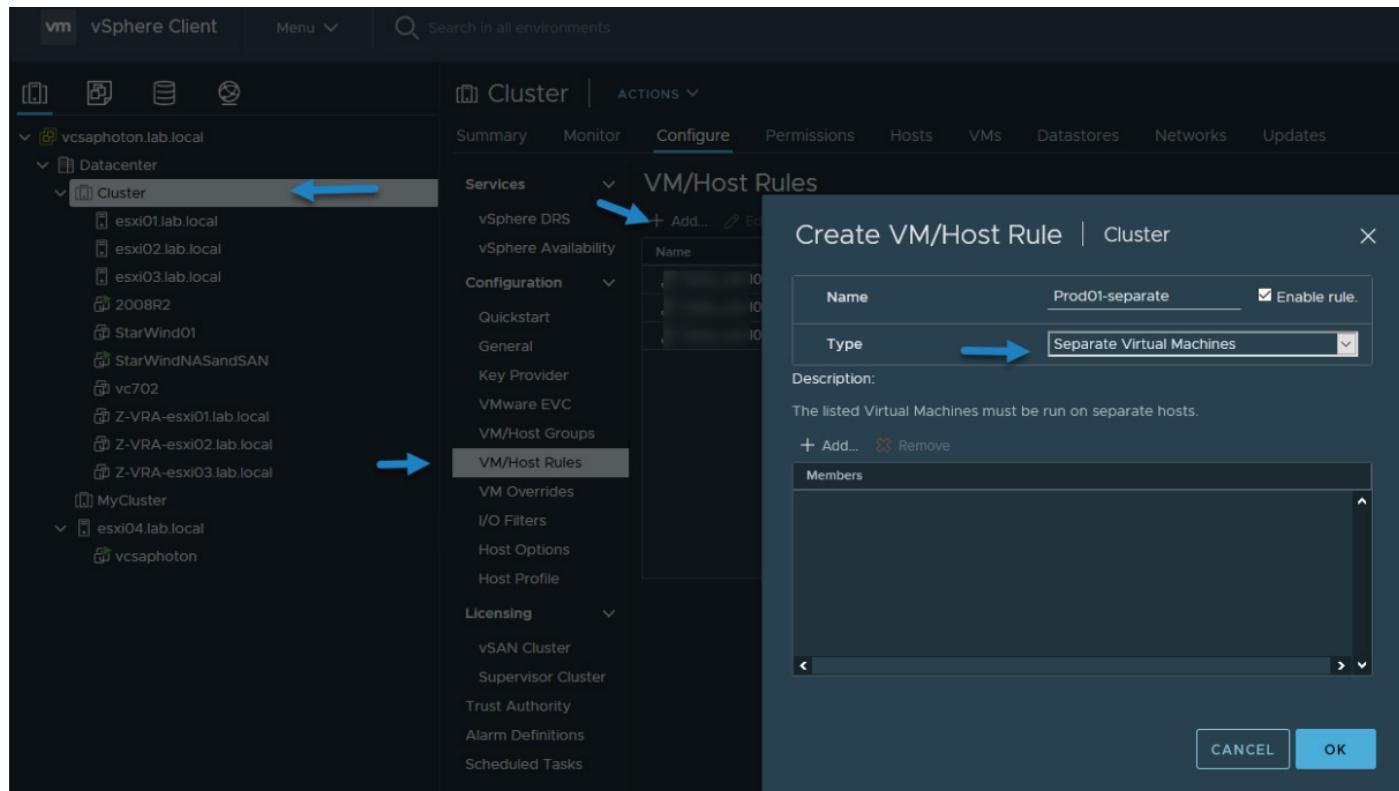
Common use cases for VM-to-VM affinity and anti-affinity rules

- **Multi-node VMs** - You need to improve application and communication performance of multi-node VMs, which are also called vApps. You can use VM-to-VM affinity rules to make sure that the VMs transferring files between them stays on the same host and the data does not traverse the physical network.
- **Disaster recovery** – When you need to improve or ensure DR for your multi-VM application, you want to make sure that you separate them so they execute each on different host.

You can have a Database server on one host while front-end web server on another host.

How to create VM-to-VM affinity or anti-affinity rules

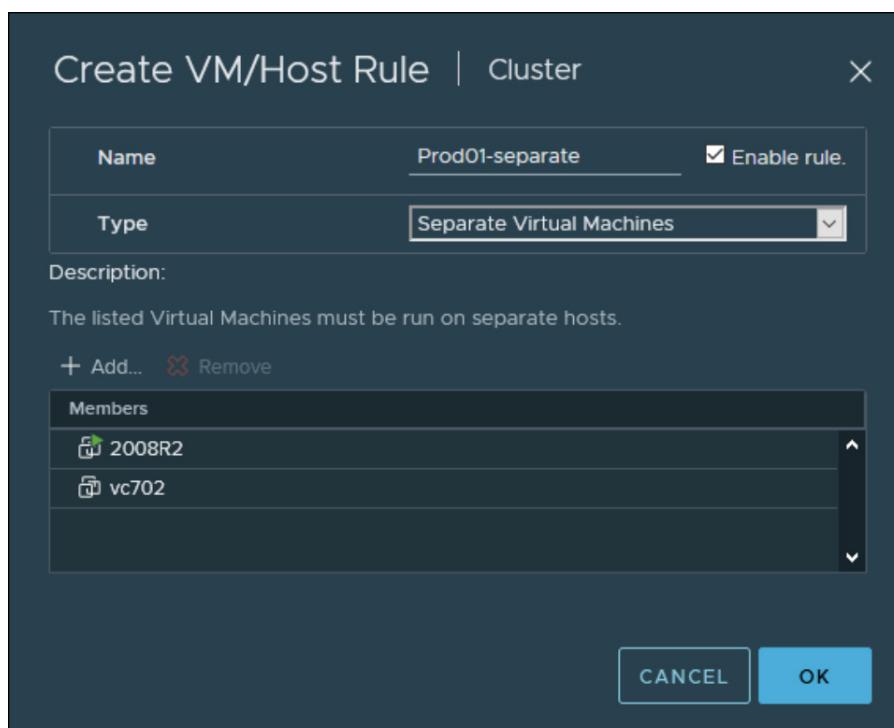
Connect via vSphere client and browse to the **Cluster level > Configure > VM/Host Rules > Add**. There you'll see **Create VM/Host Rule** dialog box, type a name for the rule.



### Create VM Host Rule in vSphere 7

From the Type drop-down menu select either Keep Virtual Machines Together (affinity) or Separate Virtual Machines (anti-affinity).

Then you'll need to select at least two virtual machines to which the rule will apply and click OK.



Select at least two VMs and click OK to create the rule

## VM-Host rules

We saw a VM-VM affinity rule that specifies affinity between individual VMs. However, a VM-Host affinity rule can define an affinity relationship between a group of VMs and a group of hosts. This will allow us to tighten certain VMs to certain hosts.

There are 'required' rules (Must) and 'preferential' rules (Should).

A VM-Host affinity rule has basically three different parts:

- One VM DRS group.
- One host DRS group.
- A specification if the rule is a requirement (must) or a preference (should) and if it is affinity (run on this host) or anti-affinity (do not run on this host).

These types of rules are usually used when setting up storage appliances where each one of those must be attached to a single host. Those type of Virtual Storage Appliances (VSAs) are not meant to be migrated or started on other hosts within cluster.

In the example below we have three VSA VMs (VSA01, VSA02 and VSA03) that runs on 3 different hosts (ESXi01, ESXi02 and ESXi03). We will make sure that each of those VMs are always starting and executing on particular hosts.

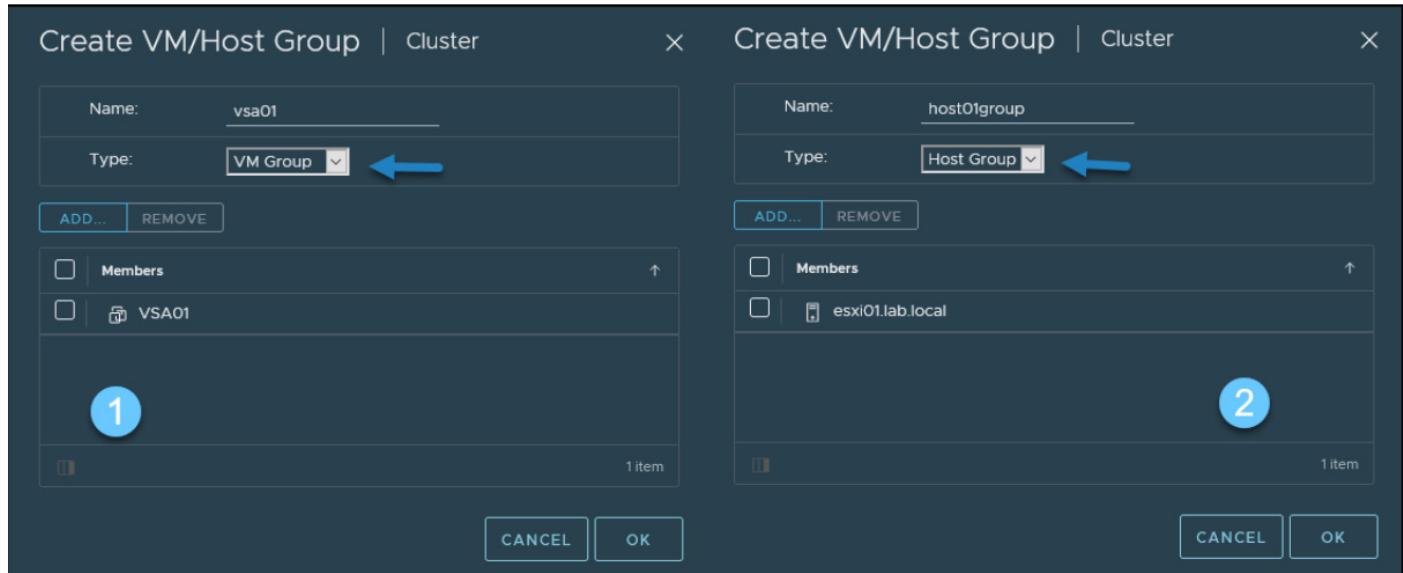
Go and select your **Cluster > VM/Host Groups > Add**

The screenshot shows the vSphere Client interface with the following details:

- Top Bar:** vm vSphere Client, Menu, Search in all environments.
- Left Navigation:** Shows a tree structure of vCenter sites, Datacenters, Clusters, and various hosts and services.
- Central Panel:**
  - Cluster View:** Summary, Monitor, **Configure** (selected), Permissions, Hosts, VMs, Datastores.
  - Services:** vSphere DRS, vSphere Availability.
  - Configuration:** Quickstart, General, Key Provider, VMware EVC.
  - VM/Host Groups:** ADD... (highlighted with a blue box and arrow), DELETE.
  - VM/Host Rules:** (List of 10 entries, each with a blue circle icon and blurred text).
  - VM Overrides:**
  - I/O Filters:**
  - Host Options:**
  - Host Profile:**

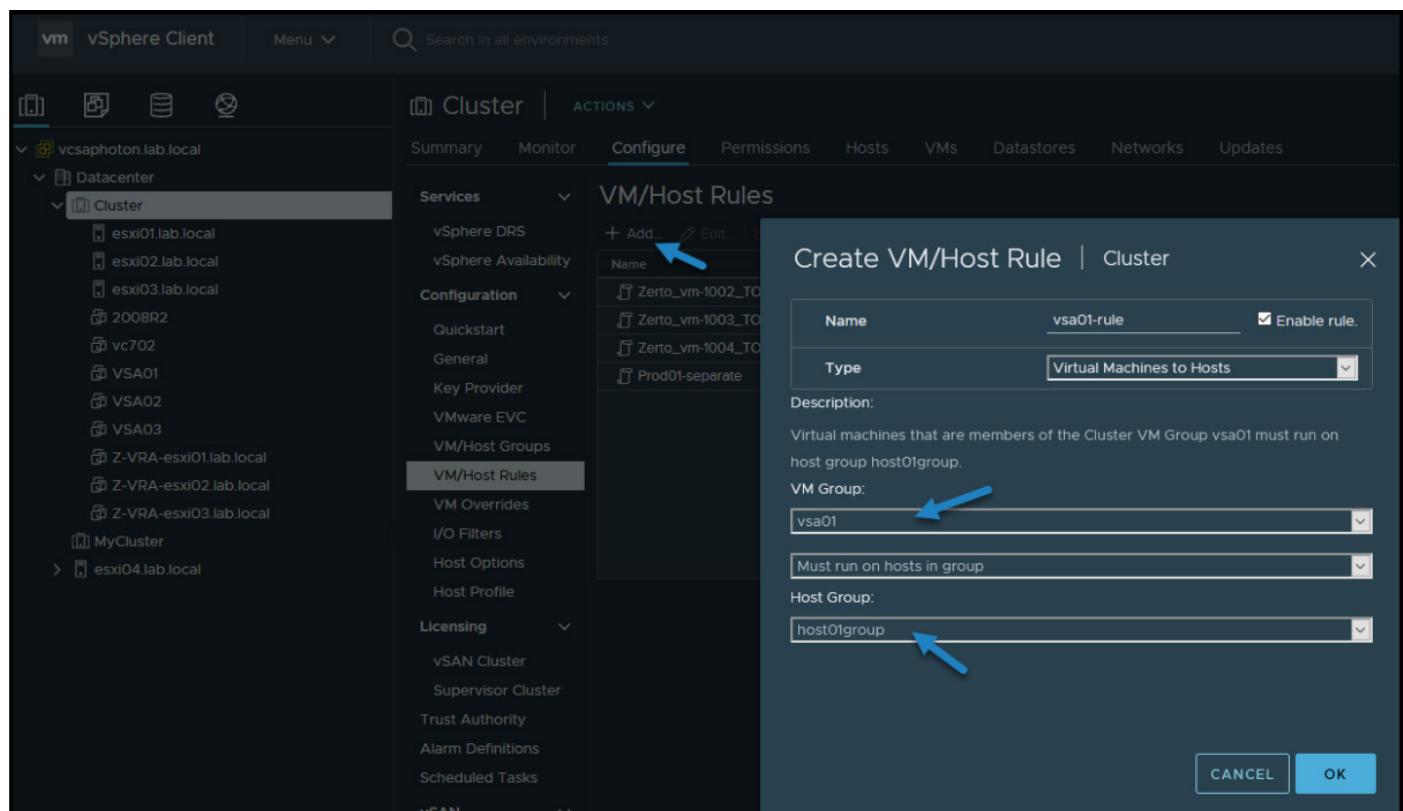
Create Two groups

Create two groups, in separate steps. **VM group** and **Host group**.



### Create VM group and Host group

Then go back to the UI VM/Host rules and **Add** a new rule.



### Create VM Host rule

For our case where we need that VSA01 runs on ESXi01 we simply pick from the drop-down menu, the **VSA01** group and **Host01** group that we have previously created.

Click validate and repeat those steps for the two other VSA. You should end up with 3 different rules, like this.

Name	Type	Enabled	Conflicts	Defined By
Zerto_vm-1002_TO_Zerto_host-40_F...	Run VMs on Hosts	Yes	0	User
Zerto_vm-1003_TO_Zerto_host-18_F...	Run VMs on Hosts	Yes	0	User
Zerto_vm-1004_TO_Zerto_host-21_F...	Run VMs on Hosts	Yes	0	User
<b>vsa01-rule</b>	Separate Virtual Machines	Yes	0	User
vsa02-rule	Run VMs on Hosts	Yes	0	User
vsa03-rule	Run VMs on Hosts	Yes	0	User

**VM/Host Rule Details**

Virtual Machines that are members of the VM Group must run on hosts that are members of the Host Group.

Group Members
vsa01 Group Members ↑ VSA01
host01group Group Members ↑ esxi01.lab.local

### Rules showing group and VM

There is different specification for the rule is like this.

- **Must run on hosts in group.** Virtual machines in VM Group 1 must run on hosts in Host Group A.
- **Should run on hosts in group.** Virtual machines in VM Group 1 should, but are not required, to run on hosts in Host Group A.
- **Must not run on hosts in group.** Virtual machines in VM Group 1 must never run on host in Host Group A.
- **Should not run on hosts in group.** Virtual machines in VM Group 1 should not, but might, run on hosts in Host Group A.

### VM-VM Affinity Rule Conflicts

vSphere 7 is able to handle conflicts between rules that would be in conflict. There are two different cases or scenarios.

**Not possibility of enable both if in conflict** - If two VM-VM affinity rules are in conflict, you cannot simply enable both. As an example, you can have one rule that keeps two VMs together and another rule keeps the same two VMs apart on two different hosts, you cannot enable both rules. The system does not allow you to.

You must select one of the rules to apply and you have to disable or remove the other which causes the conflict. Smart if you ask me.

**One rule is older than the other one** - When two VM-VM affinity rules conflict, the **older one takes precedence** and the newer rule is disabled. vSphere 7 DRS only tries to satisfy enabled rules. The disabled rules are ignored. DRS is able to recognize and prevent the violation of anti-affinity rules.

## Objective 7.6 – 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.

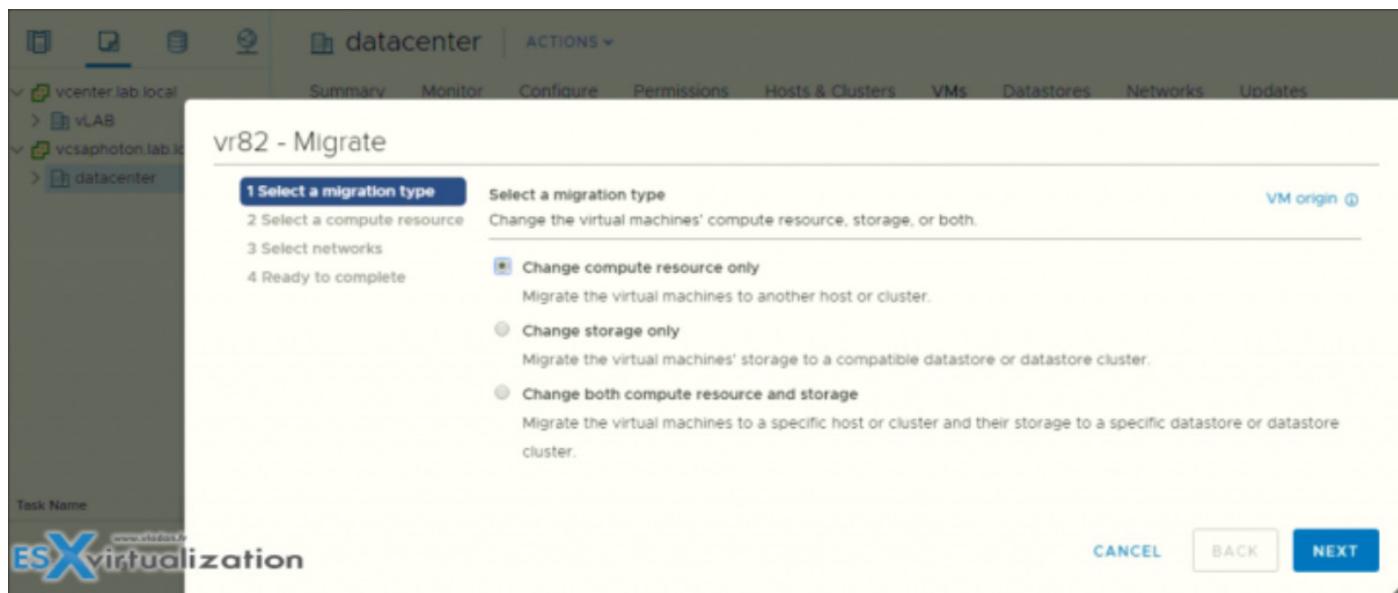
**Cold Migration** - Moving a powered off or suspended virtual machine to a new host.

Optionally, 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:

- **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.
- **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.
- **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 it has virtual PMem hard disks, the destination host or cluster must have available PMem resource, 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, migrating virtual machines to a different host and datastore simultaneously, is 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 7.7 - Configure role-based user management

While vCenter Server 7 has many users and roles predefined by default, you might need to create a custom role and add users. As you know, the vCenter Server role is a predefined set of privileges. After adding permission to an object, you can assign a role to the user or group. The default roles in vCenter are not modifiable; this means that you cannot change the privileges that are associated with those default roles. Let's have a look at a couple of roles.

**Administrator** — Can perform all actions on the object. The role also has all privileges of the Read Only role. With the Administrator role, you can assign privileges to users and groups.

**Read Only** — Users can view the state of an object, but not modify it. For example, users cannot view the remote console for a host; no action is permitted.

**No Access** — Cannot view or change object. All new users are assigned this role by default.

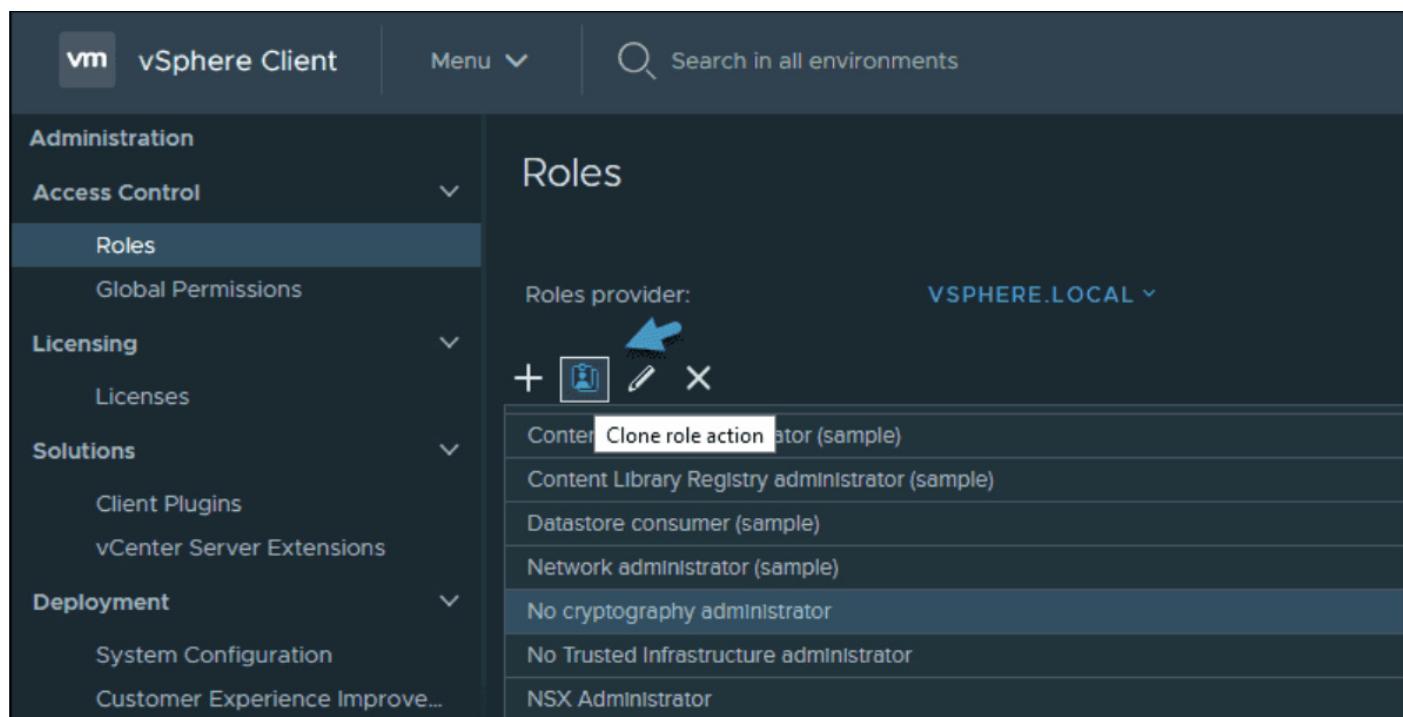
Then there are specific roles such as No Cryptography Administrator, Trusted Infrastructure Administrator (for [vSphere Trust Authority](#)), and No Trusted Infrastructure Administrator.

### Where to add new roles?

Log in to the vCenter Server by using the vSphere Client and go to **Administration > Click Roles** in the Access Control area. Select **Administration** and click **Roles** in the Access Control area.

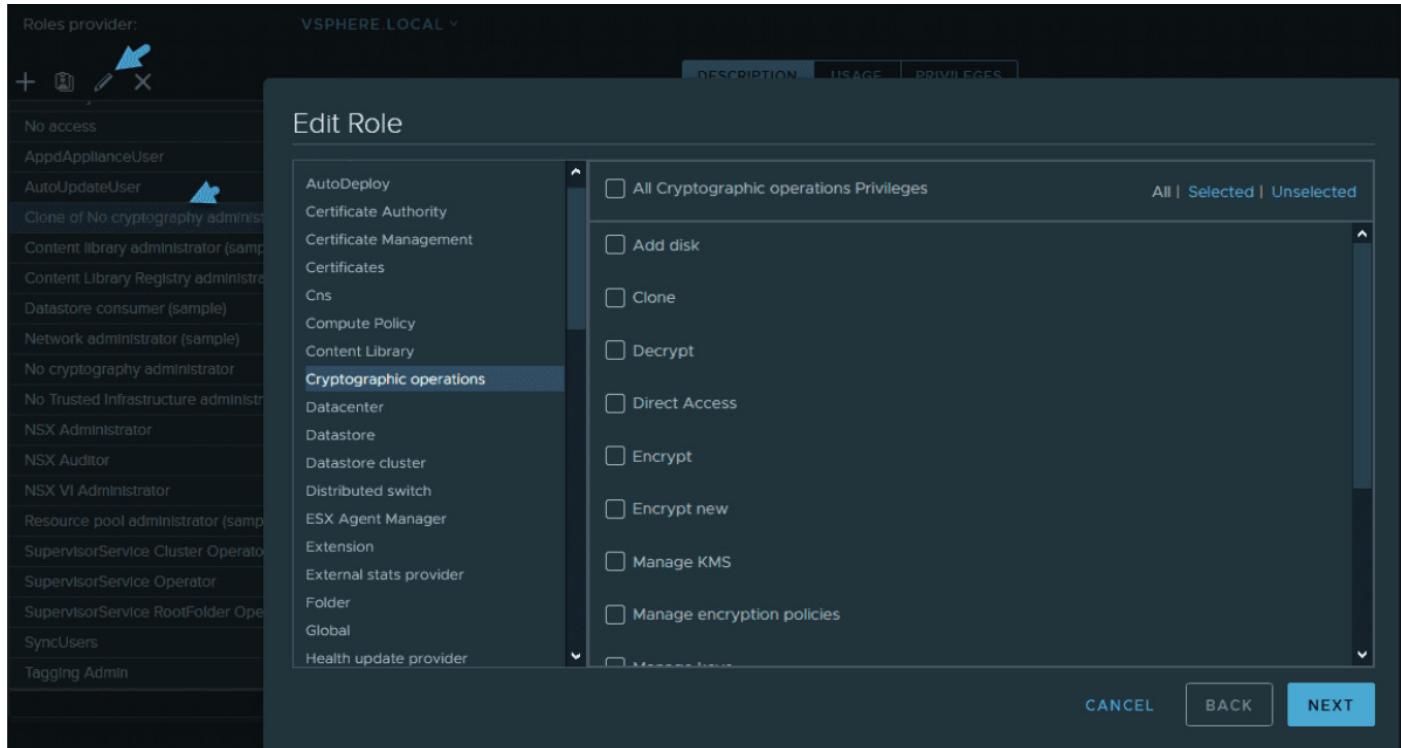
To create a role, just click the **Create Role** action icon.

To create the role by cloning, just select a role, and click the **Clone role** action icon.



### How to clone a role in vCenter Server 7

Click OK to validate. Then select the newly created role and click the **Edit** icon. As you can see, the *No cryptography administrator* role has all privileges except cryptographic operations. This role was created on purpose and is useful when you don't want to pass any of the cryptographic operations to a part of your team.



## Edit cloned role in vCenter Server 7

This is the safest way of creating a new role based on an original role. In this way, when you change something, you'll be changing the clone, not the original.

After you create a new role, you can assign privileges. The fact is that a role is a predefined set of privileges that define read properties or rights to perform actions. As an example, the Datastore role allows the creation and modification of datastores.

vCenter has two different kinds of roles:

- **System Roles** — These are permanent roles. You are not allowed to edit the privileges associated with these roles.
- **Sample Roles** — There are sample roles provided by VMware, and they are intended to be used for cloning, modifying, or removing.

Sample roles cannot be reset back to default, so in order to avoid losing the original config, simply clone the role again before making any modifications.

## What different objects exist in vCenter Server?

Let's quickly recap the different objects we can find within vCenter Server.

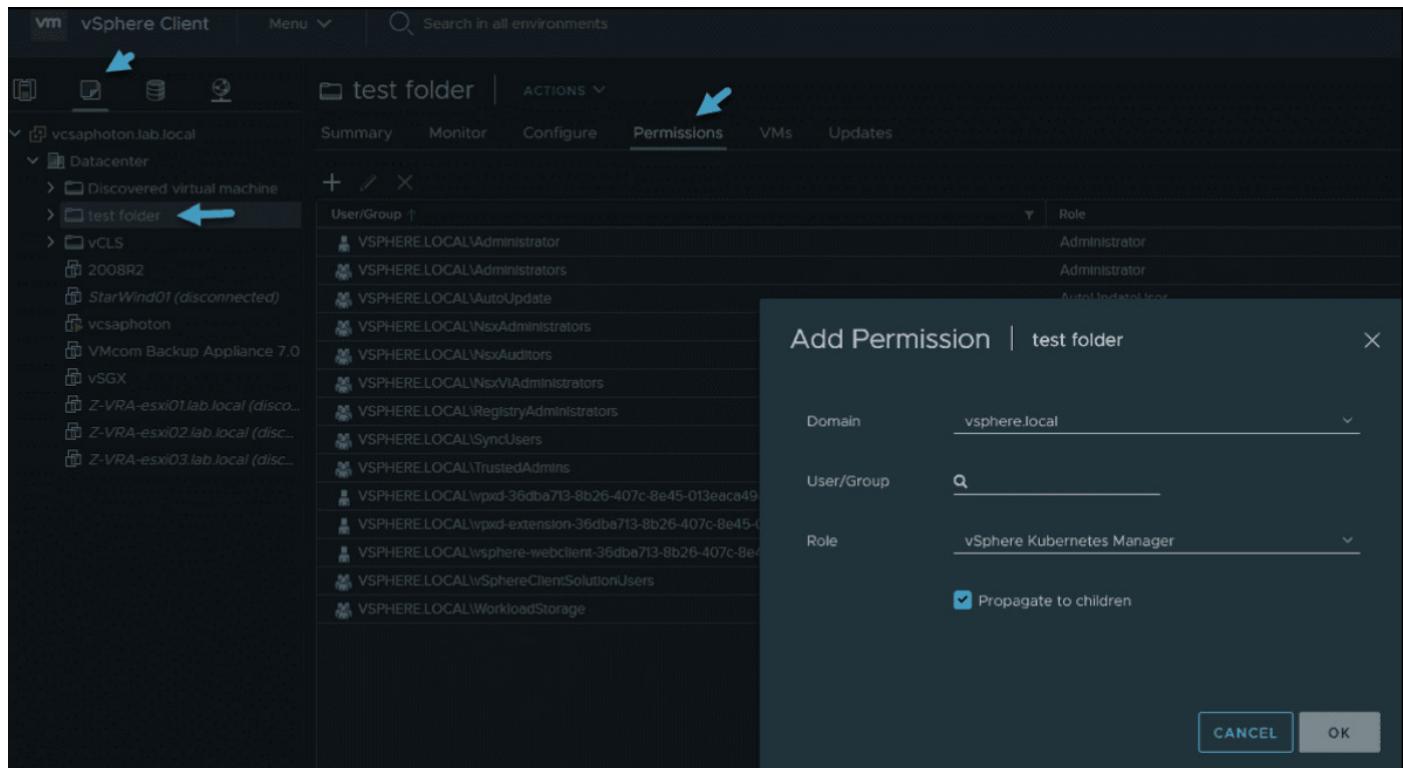
- **Permissions** — Each object in the vCenter hierarchy has associated permissions. Each permission specifies which privileges one group or user has on the object.

- **Privileges** — Access controls to the resource. Privileges are grouped into roles, which are mapped to users or groups.
- **Users and groups** — Only users authenticated through single sign-on (SSO) can be given some privileges. Users must be defined within the SSO or be users from external identity sources, such as Microsoft AD or other LDAP.
- **Roles** — A role allows you to assign permission to an object. Administrator and Resource Pool Administrator are predefined roles. You can clone or change most predefined roles (except Administrator).
- **Global Permissions** — Global permissions are special. They are applied to a global root object that spans different solutions. Imagine that you have vCenter Server and vRealize Orchestrator installed side by side. These two products 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.

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; instead, you must check a checkbox for this. Permissions defined for a child object always override the permissions that are propagated from parent objects.

Where possible, assign a role to a group rather than individual users to grant privileges to that group. This is the same logic as in Windows administration. Grant permissions only on the objects where they are needed, and assign privileges only to users or groups that must have them. A good practice is to group objects into folders. Then you can assign permissions to folders containing hosts and other objects.

Go to the **VMs and templates** view. Pick or create a new folder and add objects inside. Select the **Permissions** tab, and click the **plus sign** to add new permission.



## Assign permissions to folders

You should always enable propagation (unless it is not wanted) when you assign permissions to an object. This means when new objects are inserted into the inventory hierarchy, they inherit all permissions, as they should, so you don't have to assign them manually.

**Note:** You can use the **No Access** role to mask specific areas of the hierarchy if you do not want certain users or groups to have access to the objects in that part of the object hierarchy.

## How to create users?

Go to **Single Sign On**, and within this section, select **Users and Groups**. Then pick the domain in which you want to create your user and click **Add**.

**vSphere Client**

Menu ▾ Search in all environments

**Administration**

**Access Control**

- Roles
- Global Permissions

**Licensing**

- Licenses

**Solutions**

- Client Plugins
- vCenter Server Extensions

**Deployment**

- System Configuration
- Customer Experience Improve...

**Support**

- Upload File to Service Request

**Certificates**

- Certificate Management

**Single Sign On**

**Users and Groups** (selected)

**Configuration**

**Users and Groups**

**Users** **Groups**

Domain: vsphere.local

Find:

**ADD**

	Username	First Name	Last Name
<input type="radio"/>	K/M		
<input type="radio"/>	Administrator	Administrator	vsphere.local
<input type="radio"/>	waiter-e5ae78f7-b007-4f54-9dab-d66838a5c394	waiter	e5ae78f7-b007-4f54
<input type="radio"/>	krbtgt/VSPHERE.LOCAL		

### Add a new user to vCenter Server 7

You'll get a new popup window asking you for the details.

**Add User**

Username \*:

Password \*:

Confirm Password \*:

First Name:

Last Name:

Email:

Description:

**CANCEL** **ADD**

**Add New User** popup window

**Note:** When you set up a Microsoft AD as the identity source, you'll still need to add/remove users of your AD via the Microsoft AD Users and Objects console. Within the vSphere client, the button is greyed out.

For groups, proceed in the same manner. VMware directory service works in a similar way as Microsoft AD, where changes on one vCenter Server are propagated to other vCenter Servers connected to the same SSO. So, the VMware directory service replicates the role changes that you make to other vCenter Server systems. However, the assignments of roles to specific users and objects are not shared across vCenter Server systems.

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

The fact that vSphere is secure by default is good to know, but further security settings are 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 for something. Risk increases when you'll use ESXi shell and SSH access to login 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.

### **Securing vCenter Server Systems and Associated Services**

One of the options of options 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 must have the Administrator role. Instead, 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 the 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.

www.vladan.fr

### Edit Advanced vCenter Server Settings

**ESX virtualization**

⚠ Adding or modifying configuration parameters is unsupported and can cause instability. Configuration parameters cannot be removed once they are added. Continue only if you know what you are doing.

Name	Value	Summary
VirtualCenter.VimPasswordExpirationInDays	30	VIM password expiration (days)

683 items

Name \* : Value :

ADD CANCEL SAVE

Name must start with 'config.' For example: config.log

## 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 can 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.

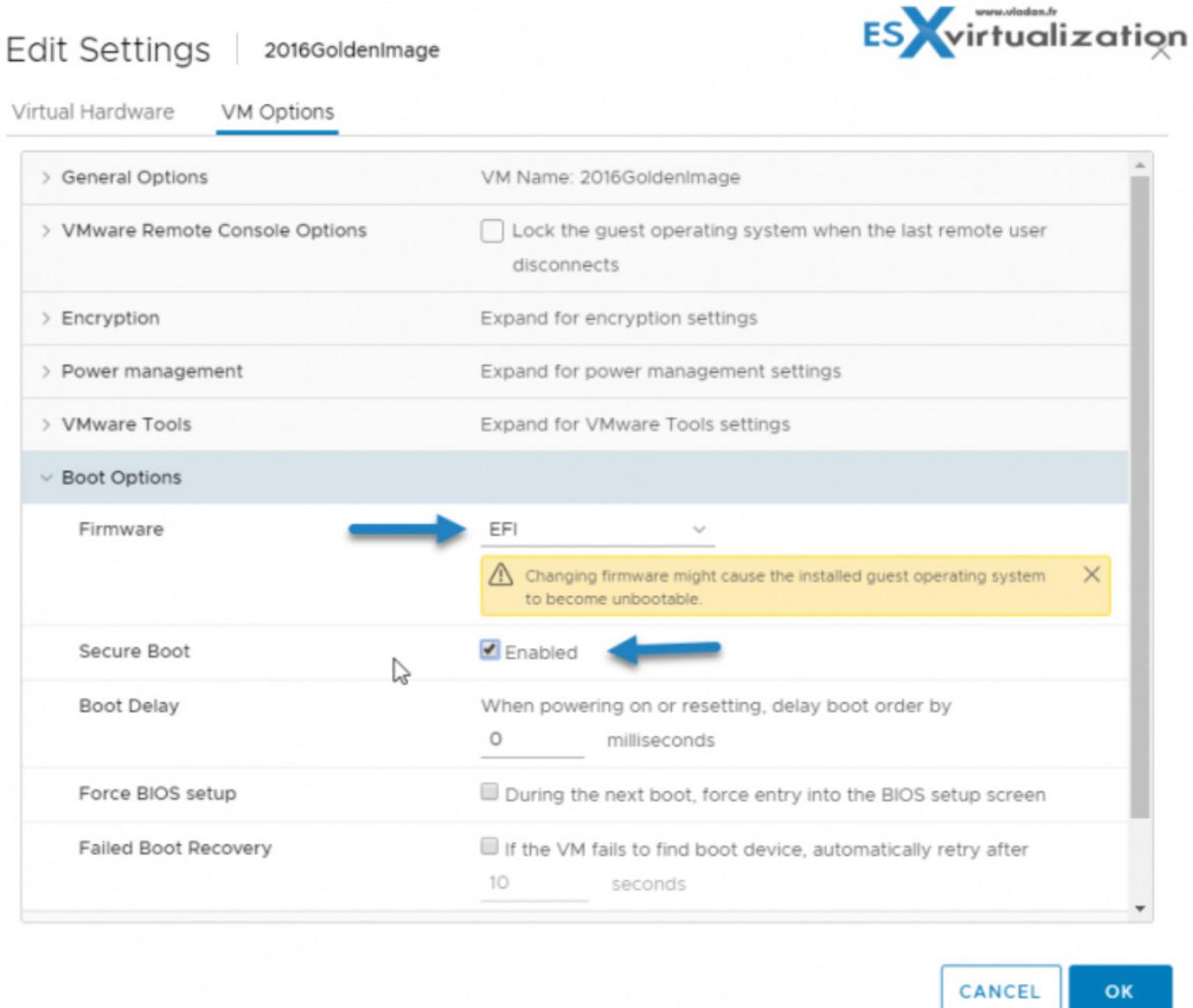
VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot.

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 allowed. The boot process stops with an error if it encounters a component with a missing or invalid signature.

### **VM's 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**

- Setup 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 the impersonation was prevented.

**Reference PDF:** *vSphere Security*

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

Being secured but not too “locked”, have a good balance between security and manageability. Making any changes to the security of the vSphere environment might have perhaps 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 7.9 - Configure and manage host profiles

Same as Objective 4.15 configure host profiles chapter. Already covered.

## Objective 7.9 - Utilize baselines to perform updates and upgrades

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. You have nothing to do.

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.

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.

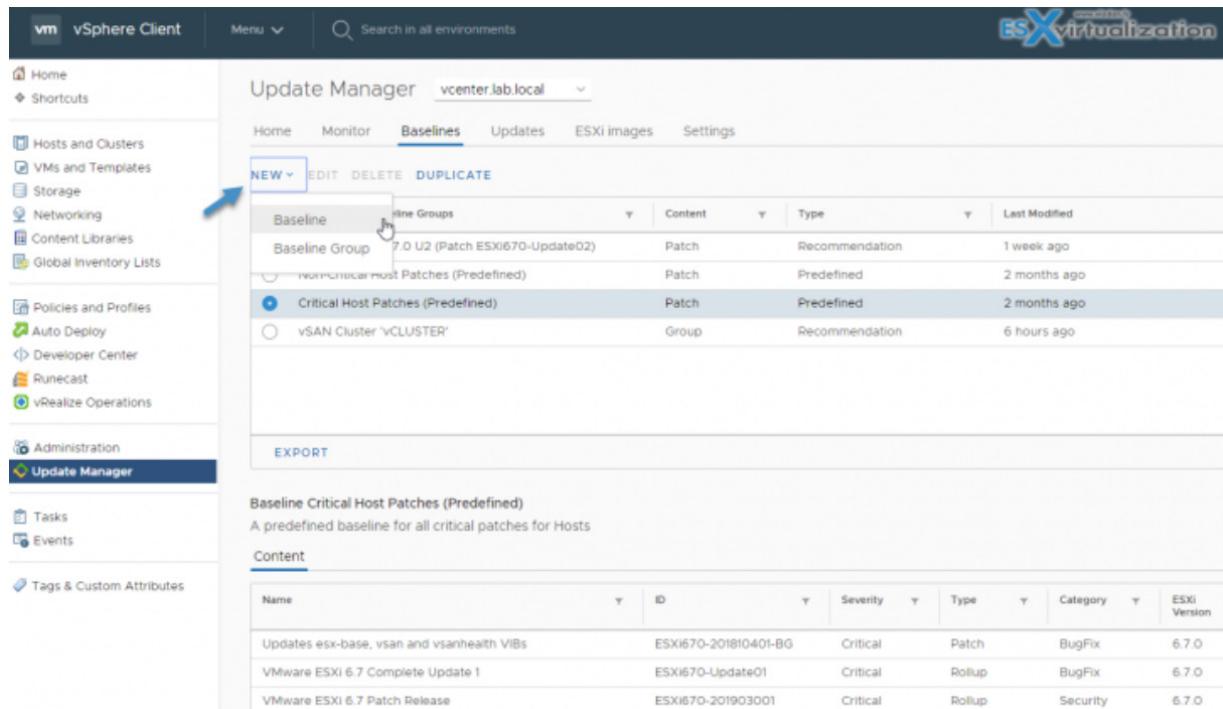
**Baseline groups** - Baseline groups are assembled from existing baselines. A baseline group might contain one upgrade baseline, and one or more patch and extension baselines, or might contain a combination of multiple patch and extension baselines. A baseline group consists of a set of non-conflicting 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 New button. **Menu > Shortcuts > Update Manager > Baselines > New**



The screenshot shows the vSphere Client interface with the 'Update Manager' section selected. The 'Baselines' tab is active. A blue arrow points to the 'NEW' button in the top-left corner of the table header. The table lists several baselines, including 'Baseline Group' (7.0 U2 (Patch ESXi670-Update02)), 'Non-Critical Host Patches (Predefined)', 'Critical Host Patches (Predefined)' (selected), and 'vSAN Cluster 'vCLUSTER''. Below the table, a detailed description of the 'Critical Host Patches (Predefined)' baseline is shown, along with its content table.

Name	ID	Severity	Type	Category	ESXi Version
Updates esx-base, vsan and vsanhealth VIBs	ESXi670-201810401-BG	Critical	Patch	BugFix	6.7.0
VMware ESXi 6.7 Complete Update 1	ESXi670-Update01	Critical	Rollup	BugFix	6.7.0
VMware ESXi 6.7 Patch Release	ESXi670-201903001	Critical	Rollup	Security	6.7.0

**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) 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.**

Attached Baselines and Baseline Groups	Status	Content
Critical Host Patches (Predefined)	Non-compliant	Patch
Non-Critical Host Patches (Predefined)	Non-compliant	Patch
vSAN Cluster 'VCLUSTER'	Non-compliant	Group

You can duplicate baselines and baseline groups in order to edit the copies without a risk of the compromise or 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.

Remediate | vCLUSTER with 3 baselines/groups



⚠️ Pre-check has found some issues that may prevent completion of remediation [Show Full Remediation Pre-check Report](#)

Pre-check has found some issues that may prevent completion of remediation. 1 action will be taken if you remediate

Actions taken if you remediate...

HA admission control will be disabled

3 hosts will remediate

<input checked="" type="checkbox"/>	Host Name	Version	Patches	Extensions	Remediation Status	Boot
<input checked="" type="checkbox"/>	vesxi03.lab.local	6.7.0	47 (0 Staged)	0 (0 Staged)	<span style="color: green;">✓ Ready</span>	Quick
<input checked="" type="checkbox"/>	vesxi02.lab.local	6.7.0	47 (0 Staged)	0 (0 Staged)	<span style="color: green;">✓ Ready</span>	Quick
<input checked="" type="checkbox"/>	vesxi01.lab.local	6.7.0	47 (0 Staged)	0 (0 Staged)	<span style="color: green;">✓ Ready</span>	Quick

EXPORT 3 Hosts

- > Install 47 updates
- > Scheduling Options: Will remediate immediately
- > Remediation settings

CANCEL REMEDIATE

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.

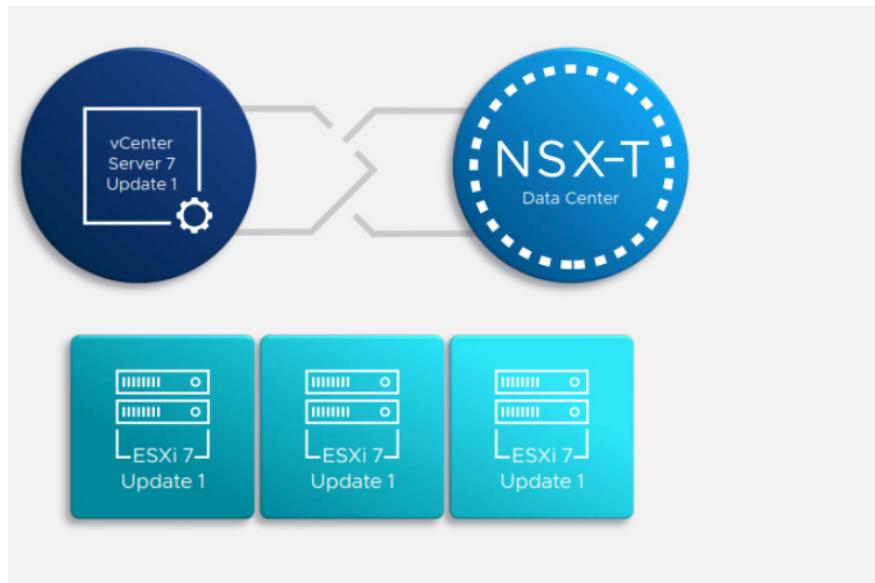
The host upgrade remediation of ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

## Objective 7.11 - Utilize vSphere Lifecycle Manager

VMware has announced recently a new major update of their flagship product – VMware vSphere 7.0 Update 1. It is not a simple update, but rather a major upgrade to already a very large upgrade from 6.7 to 7.0 release. In this post we'll have a look at new features introduced in vSphere Lifecycle Manager (vLCM) previously called vSphere Update Manager (VUM).

Many admins were still waiting for the upgrade to 7.0 because usually in the past, the major release has bugs and those bugs are ironed out in an “Update 1”. While I’m not aware of any major bugs, the number of enhancements is quite significant.

vSphere Lifecycle Manager (vLCM) is the main tool for upgrading not only ESXi hosts, but also other products you might be running within your environment. vLCM can upgrade NSX-T or vSAN going forward and this is something new.



### Manage your NSX-T lifecycle via vLCM

1. Supported in the upcoming NSX-T release
2. NSX Manager leverages vLCM Image manager to enable:
  - Installation of NSX components
  - Upgrade of NSX components
  - Un-install of NSX components
  - Add/Remove a host to a cluster
  - Move hosts to a vLCM enabled cluster

## VMware vSphere 7.0 U1 and vLCM NSX-T Management

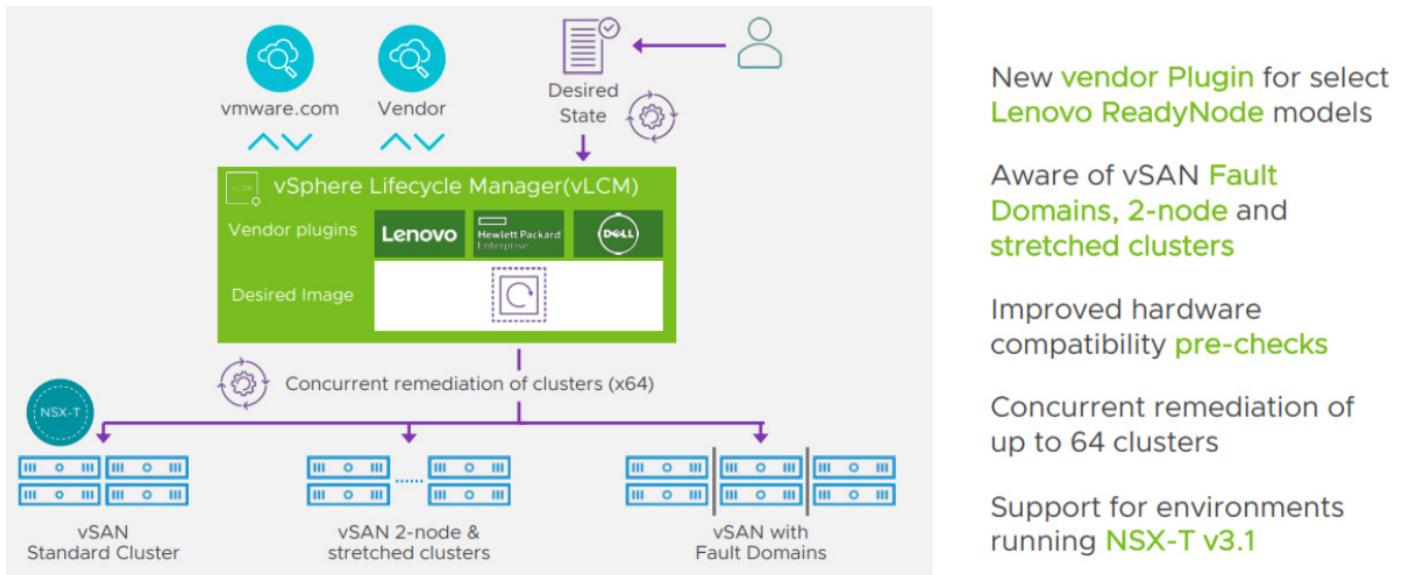
### What's new in vLCM in vSphere 7.0 U1?

- **NSX-T support** – from next major release of NSX-T (from NSX-T 3.1 onwards), you’ll be able to make deployments and upgrades of NSX-T from within vSphere UI, via vLCM. The vLCM also supports drift detection comparing the version of NSX-T within your cluster.

### Configuration of NSX-T on vLCM enabled cluster

- **VMware vSAN support** – VMware vSAN can be upgraded via vLCM which is now aware of stretched clusters configurations and as such, it is able to perform a rolling update on all hosts within a fault domain before jumping into a next cluster’s fault domain. This way, the vSAN objects will stay available during the remediation process. For example, if there are only two fault domains (FD), the system will update the Preferred FD then the Secondary FD.
- **Scalability improvements** – vLCM is able to perform parallel remediation across clusters. You can have up to 64 concurrent vSAN cluster operations running at the same time! Previously, with vSphere 7 you had possibility to run up to 15 concurrent operations. The operations will still be respecting the fault domains to keep vSAN objects available.

- **Lenovo xClarity Integrator support** – with Dell and HPE, Lenovo is third vendor to be supported concerning firmware management for Lenovo servers. It is happening via the Lenovo XClarity Integrator hardware support manager. Note that the first release supports only the ThinkAgile VX server models.

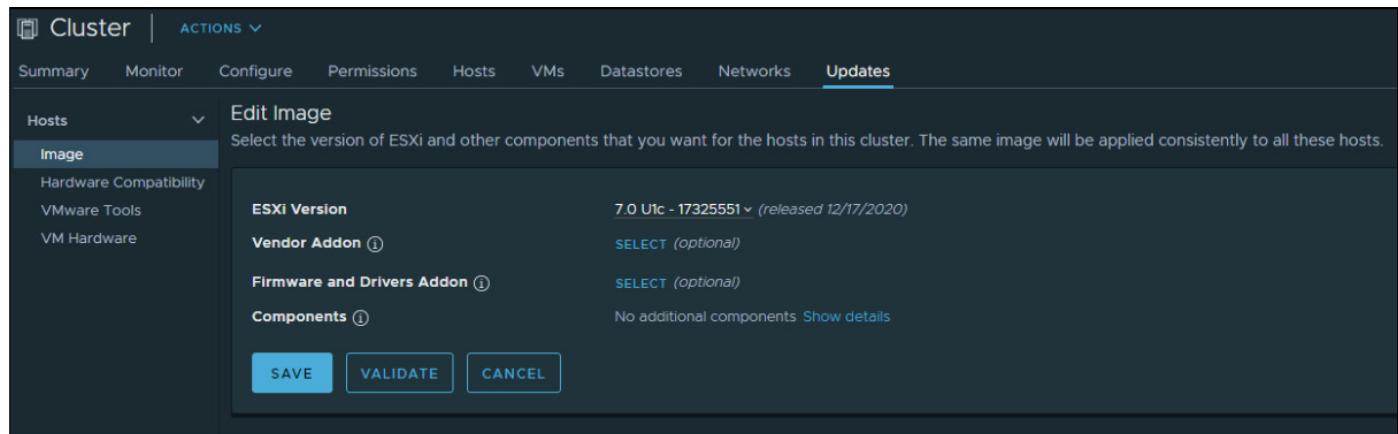


### VMware vSphere 7.0 U1 and vLCM enhancements

**Hardware compatibility checks improvements** – As you know, vSphere 7.0 brought a new way of managing clusters. You had a possibility to use image that can be applied to the entire infrastructure. In each image you'll be able to specify which software, drivers and firmware can run on the host(s) in order to keep your infrastructure in a “desired state”. vSphere 7.0 U1 and vLCM will now automatically trigger checks after you have modified the desired state image. Thos checks will then verify the HCL database on a scheduled interval for any changes. Admins will now be able to prevent remediation if hardware compatibility issues are found. They'll be able to select new option “Prevent remediation if hardware compatibility issues are found”.

## Objective 7.11.1 - Describe Firmware upgrades for ESXi

Once we have our vLCM and cluster image management enabled for our cluster, there is what's called a **desired state** that is set up. All the ESXi hosts adhere to this desired state and when for some reason, there is a host which has been installed with some new component or software that differs from the desired state, the host is remediated in order to stay compliant to the desired state and have the cluster uniformized.



## Edit the content of the image and validate

### What is an image?

Do you remember when in the past, you have been creating slipstreamed ISO images for Windows 2000 or 2003 servers? This slipstreaming process where you could add drivers, software and patches to the base image? Yes, this is basically the same here. Made by VMware.

The vLCM image has 4 composing elements:

- **ESXi Base Image** – This is an ESXi ISO file, it has a version that has an image of VMware ESXi Server. The base image from VMware.
- **Vendor Add-on** – This is a collection of software components for the ESXi hosts that OEM manufacturers create and distribute in order to maintain the infrastructure. This vendor add-on can contain drivers, patches, and software solutions that are used for the cluster management, monitoring etc.
- **Firmware and Driver Add-on** – This is a special type of vendor add-on which helps for example maintain same firmware/drivers across the cluster. Usually those depends on the type of server that needs to be maintained.
- **Component** – This is the smallest discrete unit in the vSphere Lifecycle manager image. This is basically a third-party software vendor that create and publish those components. Those are usually drivers or adapters. They are completely independent. You can add such independent components to your image.

Setting up an image is easy when you have the hardware compatible. In the lab I'm working right now, this is not the case. But let's talk about transportation or export. Yes you can export your image and this can be in different formats.

## vLCM Image export possibilities:

- **JSON** – Yes, JSON is well known type of configuration file. This option exports an image specification only, not the actual source files. You won't be able to remediate clusters just with the JSON. However, you can import the image specification to other clusters.
- **ISO** – This one has the image as an ESXi image (an ISO), that can be imported into other clusters. You can also use the exported ISO file to boot/build new ESXi hosts using your image. It has everything, the drivers, firmware driver add-ons or components that you have added during the image creation.
- **ZIP** – Well known option. Offline bundle that has all of the image components and can be used directly within the vLCM. You can use the ZIP file to import the components into a different vCenter Server.

## Objective 7.11.2 – Describe ESXi Updates

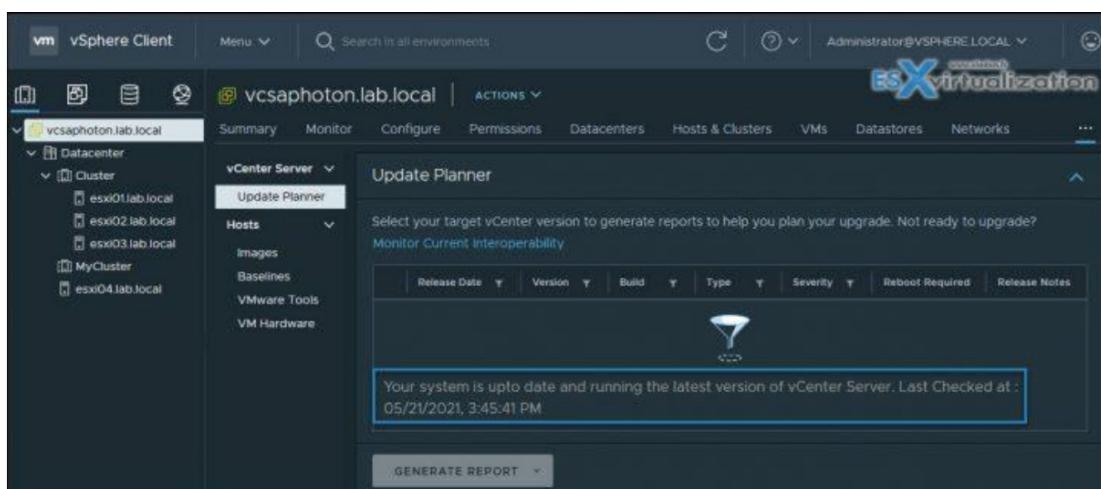
After upgrading to vCenter Server 7.0, you can use Lifecycle Manager to upgrade ESXi hosts and virtual machines. Within the lifecycle manager, there you can use the Update Planner to examine available vCenter Server updates and upgrades. You can generate interoperability reports for installed VMware products within your environment as well.

You can also compare your source (current) and target vCenter Server versions. It is possible to generate pre-update reports to make sure that your system meets the minimum software and hardware requirements. The report shows you whether there are upgrade issues before the upgrade starts and provides potential remedy actions.

In the vSphere Client, select a **vCenter Server** in the inventory pane and navigate to **Updates > Update Planner**.

Select a target vCenter Server version (major upgrade or minor update).

**Note:** My vCenter in the lab has the latest version so I can't show you what they're asking for.



## Click **Generate Report > Pre-Update Checks.**

Click Export to save the report as a comma-separated values (CSV) file. Step 5. Optionally, click Open Appliance Management or Download ISO.

However, in order to use Update Planner, you must join the VMware Customer Experience Improvement Program (CEIP), but I see no issues with this. vSphere Lifecycle Manager has more functionality than Update Manager was able to give you with earlier vSphere releases. It is a service running within your VCSA and is automatically enabled in the vSphere Client.

Starting with vSphere 7.0 it is possible to use vSphere Lifecycle Manager images to perform some tasks on a set of hosts at the cluster level. You must choose between using Images or baselines. Not both.

With Images you can:

- Install the desired ESXi version on each host
- Install and update third-party software on each ESXi host
- Update the firmware of each ESXi host

Update and upgrade each ESXi host in a cluster Check the hardware compatibility of each host against hardware compatibility lists, such as the VMware Compatibility Guide and the vSAN Hardware Compatibility List.

### **Important Note:**

When you start using Lifecycle Manager images as you create a cluster, you need to switch to this mode. Otherwise, you can switch from using baselines to images later. **However, after switching a cluster to use images, you cannot revert the cluster back to using baselines.**

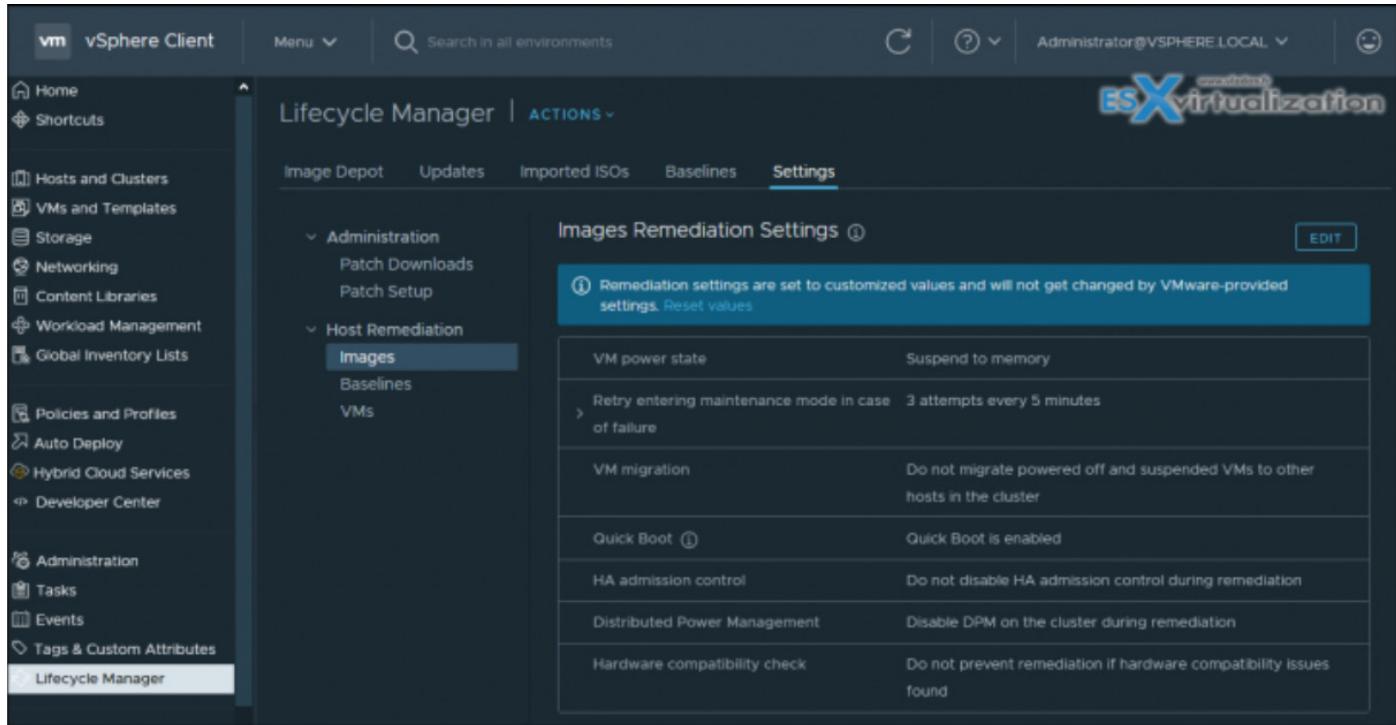
As a workaround, you can **move the hosts to another cluster** that uses baselines, there do the update, and move it back.

And another gotcha:

If you set up an image for a cluster and remediate all the hosts in the cluster, then **all standalone VIB and non-integrated agents are deleted from the hosts.**

You can leverage vSphere Lifecycle Manager for VMware Tools and virtual machine hardware upgrade operations on virtual machines running on ESXi 6.5, ESXi 6.7, and ESXi 7.0 hosts.

To get started using vSphere Lifecycle Manager, in the vSphere Client, you can navigate to **Menu > Lifecycle Manager** (which is called the Lifecycle Manager home view) and select a vCenter Server. Here you can configure Lifecycle Manager by using the **Settings tab**.



## Objective 7.11.3 – Describe Component and Driver Updates for ESXi

- **Firmware and Driver Add-on** – This is a special type of vendor add-on which helps for example maintain same firmware/drivers across the cluster. Usually those depends on the type of server that needs to be maintained.
- **Component** – This is the smallest discrete unit in the vSphere Lifecycle manager image. This is basically a third-party software vendor that create and publish those components. Those are usually drivers or adapters. They are completely independent. You can add such independent components to your image.

## Objective 7.11.4 – Describe Hardware Compatibility Check

VMware HCL and its validation is not an easy task as the compatibility information is usually spread through multiple web pages. The user needs to understand the data and validate them one by one manually.

It is possible to check HCL of a host and find out if the host hardware is certified for use with a selected ESXi version. The hardware compatibility check is performed against the VMware Compatibility Guide (VCG) or, if the host is in a vSAN cluster, against the vSAN Hardware Compatibility List (HCL).

The hardware compatibility check that you initiate for a single host checks whether the server and the physical devices on the host are Certified for use with a selected ESXi version. The check is performed against the VCG.

**Note:** If the host is in a vSAN cluster, the hardware compatibility of the I/O devices that are used by vSAN is checked against the vSAN Hardware Compatibility List (HCL). All other I/O devices are checked against the VCG.

You can do that via vSphere Lifecycle Manager (previously called vSphere Update Manager - VUM). After the check, vSphere Lifecycle Manager shows the status for the server and hardware devices. The server and devices might have one of the three different states: compatible, incompatible, and unknown.

## How to proceed with vSphere Client

- In the vSphere Client, navigate to a standalone host or a host in a cluster.
- On the Updates tab, select Hosts > Hardware Compatibility.
- In the Hardware Compatibility pane, select your task.
  - To run a hardware compatibility check for the host for the first time, select a target ESXi from the drop-down menu and click Apply.
  - To check the hardware compatibility between the host and the already selected target ESXi version, click Re-run Checks.
  - To choose a new target ESXi version for the hardware compatibility check, click Edit and select a new target ESXi version.
  - To export the hardware compatibility report in a CSV format, click the Export button.

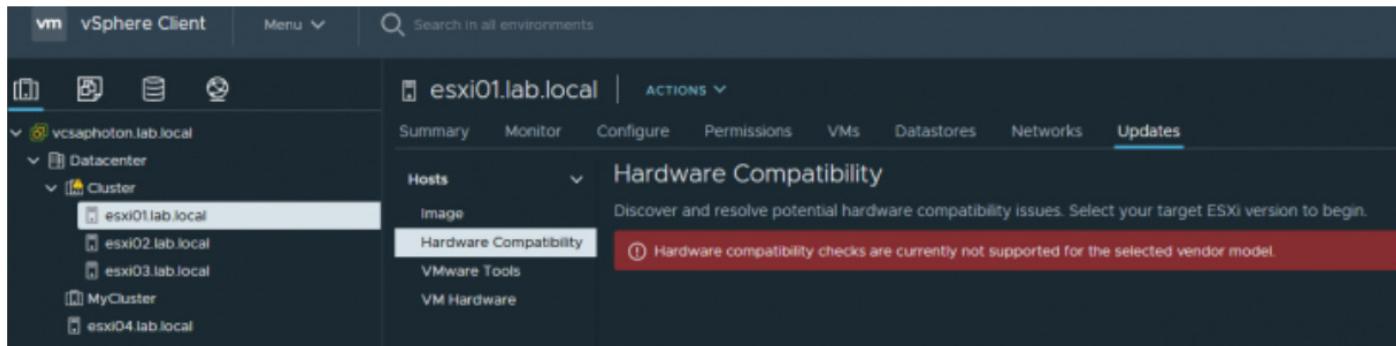
The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' tab selected. The left sidebar includes 'Hosts and Clusters', 'Storage', 'Networking', 'Content Libraries', 'Workload Management', 'Global Inventory Lists', 'Policies and Profiles', 'Auto Deploy', 'Hybrid Cloud Services', 'Developer Center', 'Administration', 'Tasks', 'Events', 'Tags & Custom Attributes', and 'Lifecycle Manager'. The main pane displays 'Lifecycle Manager' for 'vcsa7.lab.local'. It has tabs for 'Image Depot', 'Updates' (which is selected), 'Imported ISOs', and 'Baseline'. Below these are 'ESXI VERSIONS', 'VENDOR ADDONS', and 'COMPONENTS' sections. A dropdown menu under 'ACTIONS' shows 'Updates', 'Sync Updates' (highlighted with a blue arrow), 'Import Updates', 'Hardware Compatibility List', and 'Sync HCL'. A table lists ESXi versions with columns for Name, Version, and Release Date. The table includes rows for ESXi 7.0 U2a, 7.0 U1d, 7.0 U1c, 7.0 Utsc, 7.0 Utb, 7.0 Utla, 7.0 Update 1, 7.0b, 7.0bs, and 7.0 GA.

Name	Version	Release Date
ESXi	7.0 U2a - 17867351	04/29/2021
ESXi	7.0 U1d - 17551050	02/04/2021
ESXi	7.0 U1c - 17325551	12/17/2020
ESXi	7.0 Utsc - 17325020	12/17/2020
ESXi	7.0 Utb - 17168206	11/19/2020
ESXi	7.0 Utla - 17119627	11/04/2020
ESXi	7.0 Update 1 - 16850804	09/04/2020
ESXi	7.0b - 16324942	06/16/2020
ESXi	7.0bs - 16321839	06/16/2020
ESXi	7.0 GA - 15843807	03/16/2020

## Results

vSphere Lifecycle Manager displays the result from the compatibility check. You can see a list of compatible, incompatible, and unknown devices. For each device, you can see full details by clicking the expand button.

When you have a homelab or running Nested ESXi labs, your hardware compatibility checks won't work. This is what HCL will look like when you'd like to show ....



From vSphere documentation:

With vSphere Lifecycle Manager, you can perform the following tasks.

- **Check the hardware compatibility of a single host** - The hardware compatibility check for a host validates the server model and the host I/O devices against the current or future ESXi version. The check is performed against the VCG or the vSAN HCL.
- **Check the hardware compatibility of a vSAN cluster** - The hardware compatibility check for a cluster validates only the I/O devices against the software specification in the image for the cluster. Unless all hosts are remediated against that image, the hardware compatibility check might not reflect accurately their current status. The hardware compatibility check for a cluster is performed against the vSAN HCL only.

## Objective 7.11.5 - Describe ESXi cluster image export functionality

vSphere Lifecycle Manager provides new functionality in vSphere 7.0 called cluster images, which allows you to easily update and upgrade the software and firmware on the hosts within your clusters.

Once your image is created, it can be used to build new clusters with the exact same specifications (if, of course, those clusters have the same hardware characteristics). Imagine a supermarket chain with 200 shops around the country, and your task is to build and maintain those three-node vSAN clusters for all those sites. Cluster images to the rescue.

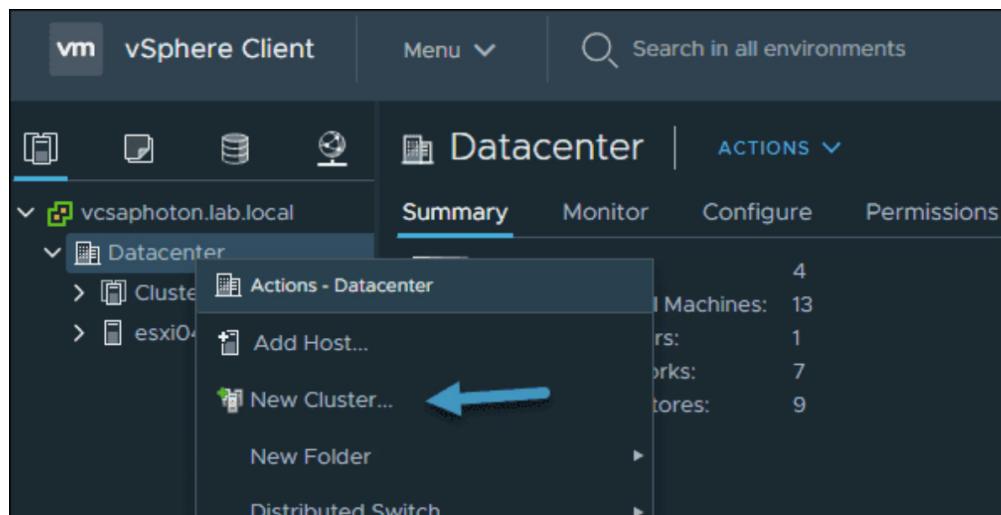
This is something that many admins were looking for. Many of us know that, for example, within a vSAN environment, it's pretty crucial to have the same level of firmware/driver combination on all HCAs within clusters. ESXi 7 with cluster imaging allows you to maintain a consistent configuration across infrastructure by bundling an ESXi base image with firmware, vendor, and driver add-ons.

## The requirements

- ESXi and vSphere 7.
- Within your inventory, you'll have to have a datacenter cluster. Normally it's obvious, but make sure they have been created.
- All ESXi 7 hosts must be on the same version.
- You must know the ESXi root account password.

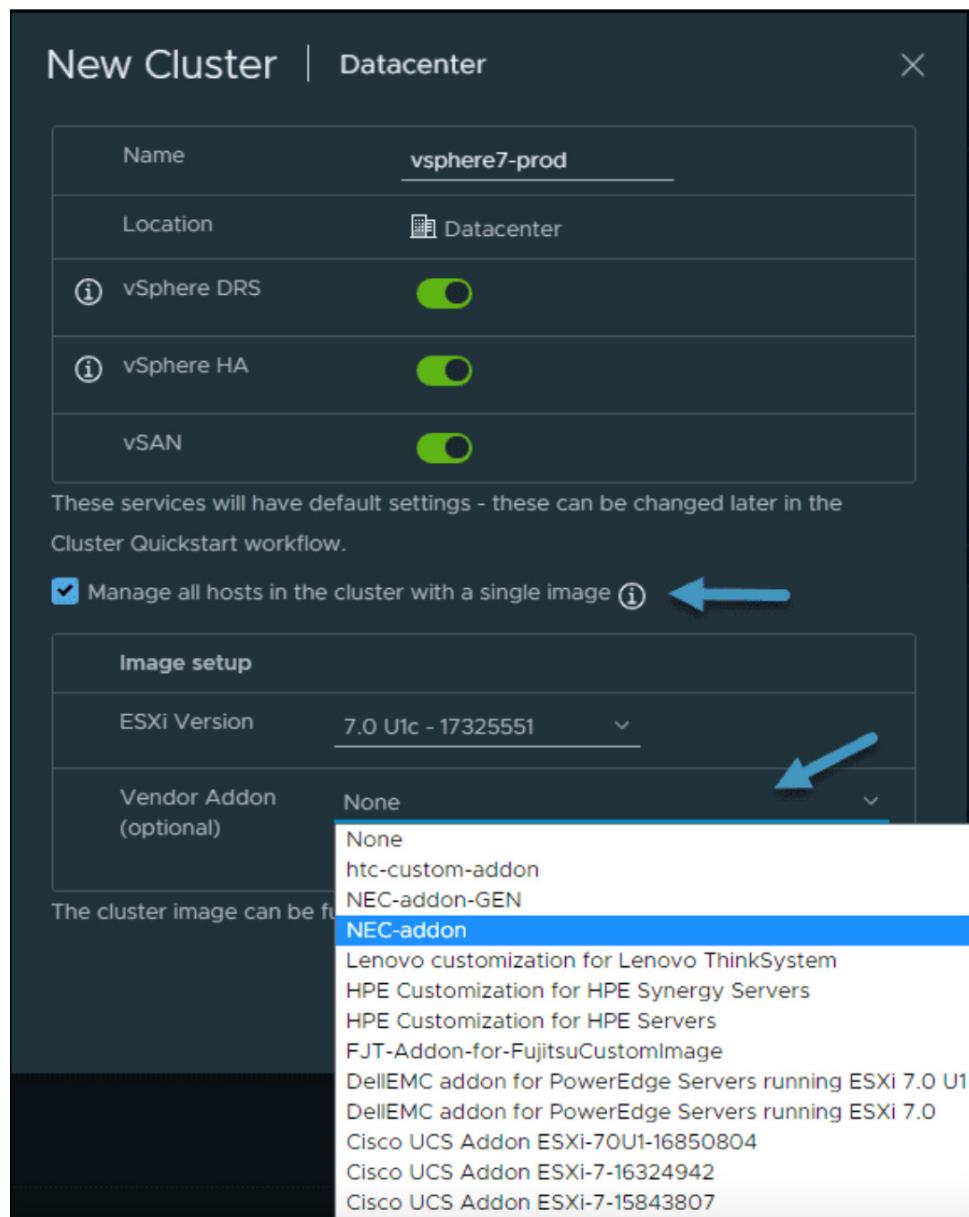
## The steps

When you open your vSphere client, go to **Home > Hosts and Clusters**. Select a data center, right-click it, and select **New Cluster**. Enter a name for the cluster.



Create a new cluster in vSphere 7

Next, pick the features that you'll be using within your cluster (DRS, HA, vMotion, vSAN, etc.), and select the checkbox for **Manage all hosts in the cluster with a single image**.



### Manage all ESXi 7 hosts with a single image

**Note:** The vendor add-on is optional. You may use this perfectly well without the server on the list too

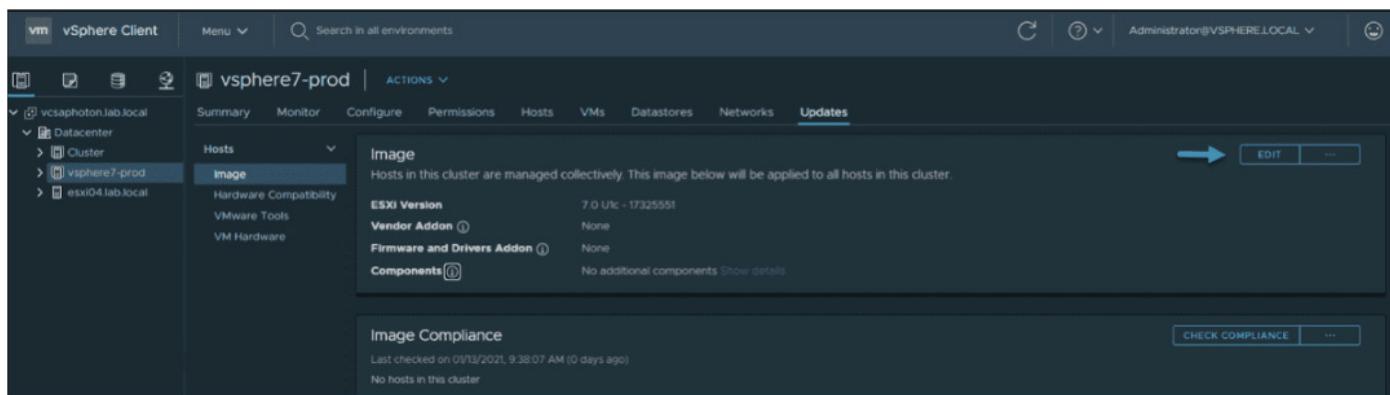
### The ESXi 7 images have four elements

**ESXi Base Image** — This is the ESXi release version ISO image which was released by VMware. It has all the necessary components of the VMware ESXi Server and additional components such as drivers and adapters that are necessary for installation.

**Vendor Add-on** — This is a collection of software components provided by the OEM manufacturer. It's the manufacturer's responsibility to provide and maintain an up-to-date version, which is usually distributed within MyVMware downloads. This vendor add-on usually has some drivers, patches, and management solutions.

**Firmware and Driver Add-on** — This one is a highly specific package that helps with the firmware updates. The firmware and driver add-on combination is crucial for specific types of hardware, such as HBAs, and usually has firmware for a specific server version.

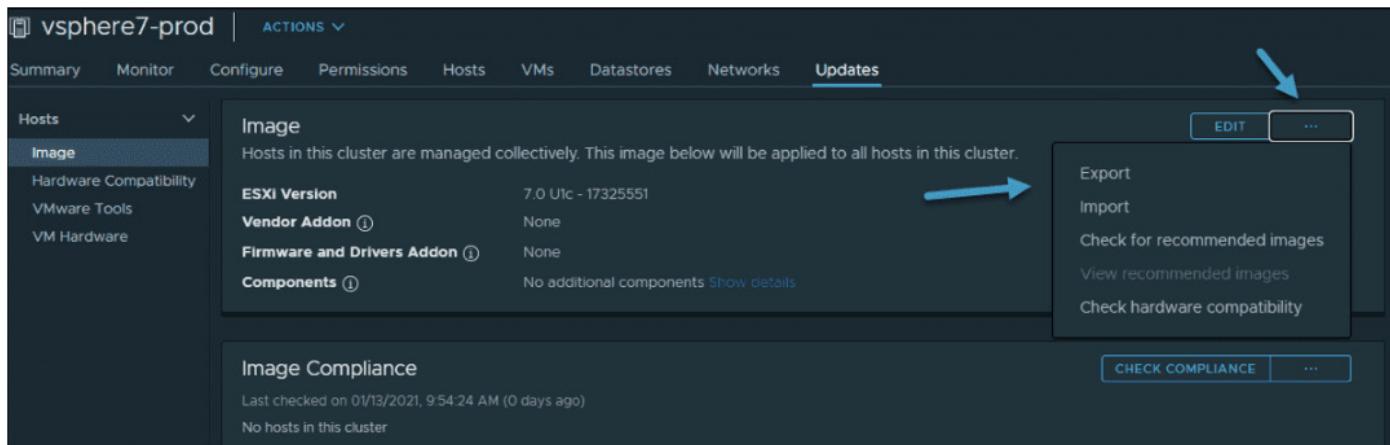
**Component** — This one is basically the smallest part of the image and is reserved for third-party software vendors. VMware and OEM manufacturers do not publish components, as they're usually very small pieces of software that contain small drivers, but independently from everything else. This enables you to fine tune your image and add even very small components to it.



Your image is now created but you can go back to edit the options

If you want to add/remove the different vendor add-ons or change them, click the **Edit** button as shown above. This will bring back the assistant.

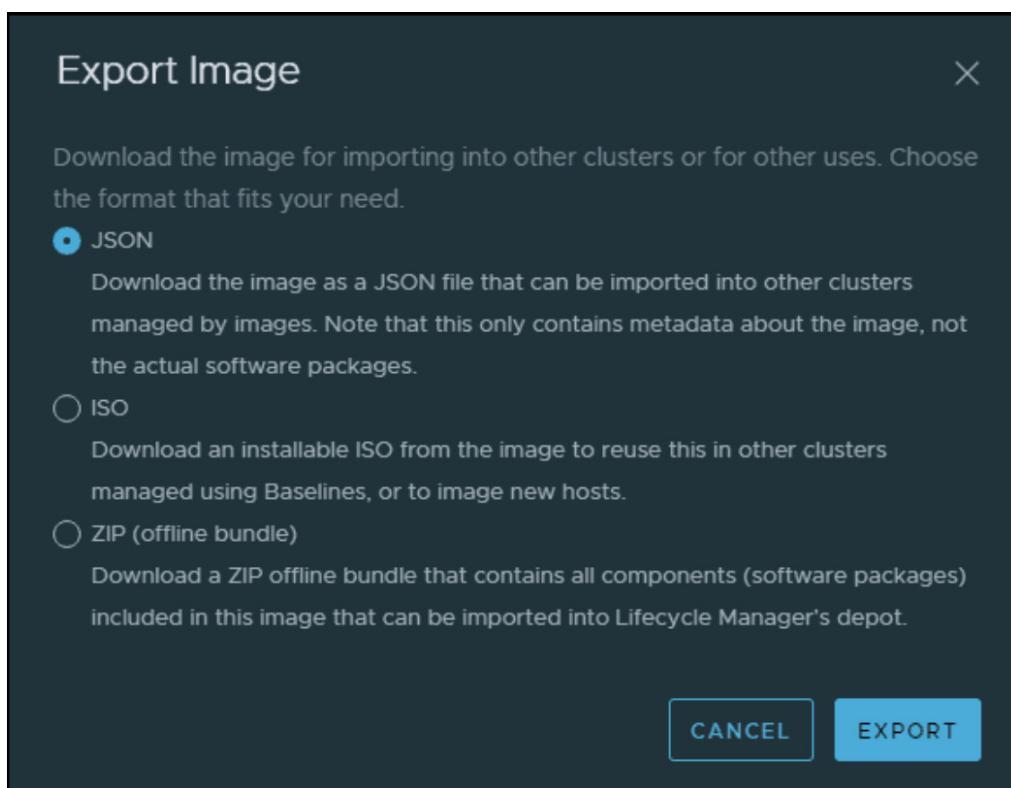
Once you're happy with your image and selection of firmware, drivers, and ESXi version, you can add hosts that you have preinstalled.



You can export the ESXi 7 cluster image

When you click the Export option, the assistant gives you three options to choose from:

- **JSON** — Allows you to use this file in other clusters that are managed by images. It does not contain all the base installation files, just the JSON configuration file. Remember that you can still have clusters that are not managed by images, but as traditional compliance levels.
- **ISO** — This gives you a full-blown ISO with everything in it. You can easily upload this to some cloud storage and use it for other clusters where you'll be able to access it from anywhere.
- **ZIP** — Create an offline bundle that can be imported by vSphere Lifecycle Manager. Similar to ISO.



### Export as JSON ISO or ZIP fil

In our lab case, we haven't added any hosts, so we cannot show you the compliance tab. But as you can imagine, this will be very easy to manage.

Next to the **Check Compliance** link, click the ellipsis button to show the menu. You can select **Edit remediation settings** to have a look at the cluster remediation options.

## Image compliance options allow you to verify whether your hosts are in compliance

The overlay window pops up with some options, which are basically the same as when you manage your cluster via baselines. These are cluster-level update settings and settings concerning your VMs, such as whether you want your VMs to be powered off, without change, or suspended.

If you have vMotion configured and you keep the default selection, **Do not change the power state**, your VMs are simply migrated via vMotion to other hosts within the cluster, and the host enters maintenance mode before starting the update.

## Edit cluster remediation settings

As you can see, we can enable [quick boot](#) functionality, which allows you to bypass the hosts' firmware boot and speed up the overall remediation on clusters.

## Objective 7.12 – Configure Alarms

As with previous releases, VMware vSphere 7 has kept alarm management. The vSphere 7 alarms are useful for day-to-day management, but as the product grows larger, with more functions and cluster-wide options, the number of predefined alarms grows.

It's important for admins to know how to effectively configure vSphere 7 alarms to help them with their daily tasks. You can create an alarm to email a notification whenever a new VM is created or alert you to resources running low on an ESXi host or cluster. This is particularly useful when you and your coworkers are creating many VMs and you want to keep track.

vSphere 7 alarms that are created at higher levels in the vSphere hierarchy will be propagated to the underlying objects at lower levels where applicable. At the very top, there is vCenter Server, then a datacenter object, ESXi hosts, and so on. You can create an alarm to monitor any object registered in the vSphere 7 inventory.

You can also create an alarm whenever some of the cluster or VM resources run low. Imagine you have a critical VM that has problems with performance. You want to be notified when this happens. Alarms are very configurable and flexible.

### Required privileges

When managing alarms, you need to have a required privilege. You as an admin can delegate this task to someone within your IT team or from among your coworkers.

The required privileges are **Alarms.Create alarm** or **Alarms.Modify alarm**.

### Where are alarms created?

In the vSphere client, select an object in the inventory pane and navigate to **Configure > More > Alarm Definitions**. Then click **Add**.

**Tip:** If you want to create an alarm for a particular VM or object, you can also **right-click that VM** or object, and then select **Alarms > New Alarm definition**.

The screenshot shows the vSphere Client interface for managing a vCenter server named 'vcsaphoton.lab.local'. The 'Configure' tab is active, and the 'Alarm Definitions' section is displayed. The table lists various alarms:

	Alarm Name	Object type
○ >	Host connection and power state	Host
○ >	No compatible host for Secondary...	Virtual Machine
○ >	Update Manager Service Health Al...	vCenter Server
○ >	vMon API Service Health Alarm	vCenter Server
○ >	Component Manager Service Healt...	vCenter Server
○ >	VMware vSphere Authentication P...	vCenter Server
○ >	vSAN Health Service Alarm	vCenter Server
○ >	PostgreSQL Archiver Service Healt...	vCenter Server
○ >	VMware vCenter-Services Health ...	vCenter Server
○ >	Hybrid vCenter Service Health Alar...	vCenter Server
○ >	Host TPM attestation alarm	Host

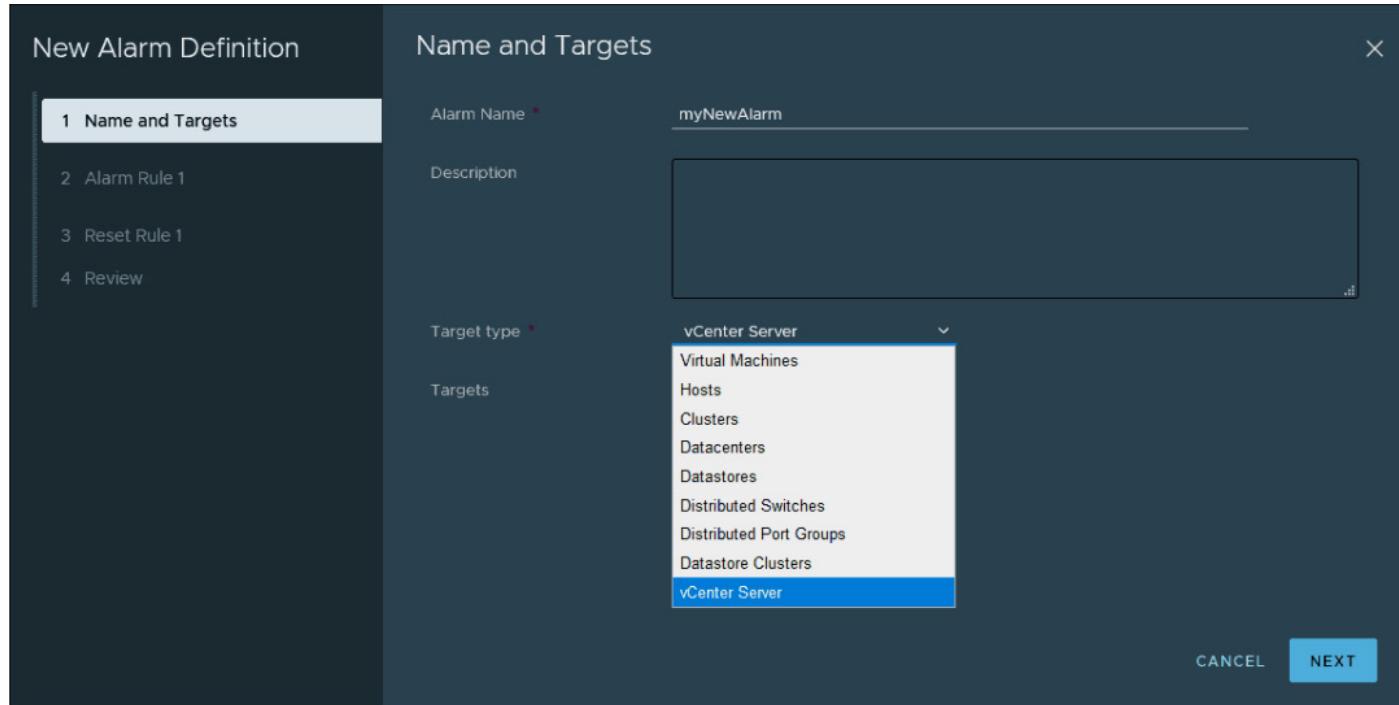
### vCenter Server alarm definitions

You'll open an assistant inviting you to provide a name, description, target type, and target.

Click next and create an alarm rule by specifying:

- **Conditions** — Options are: Trigger, Arguments, Operator, Thresholds
- **Severity** — Options are: Warning or Critical
- **Actions** — Options are: Send email notifications, SNMP traps, Run script

As you can see, there are nine different target types available.

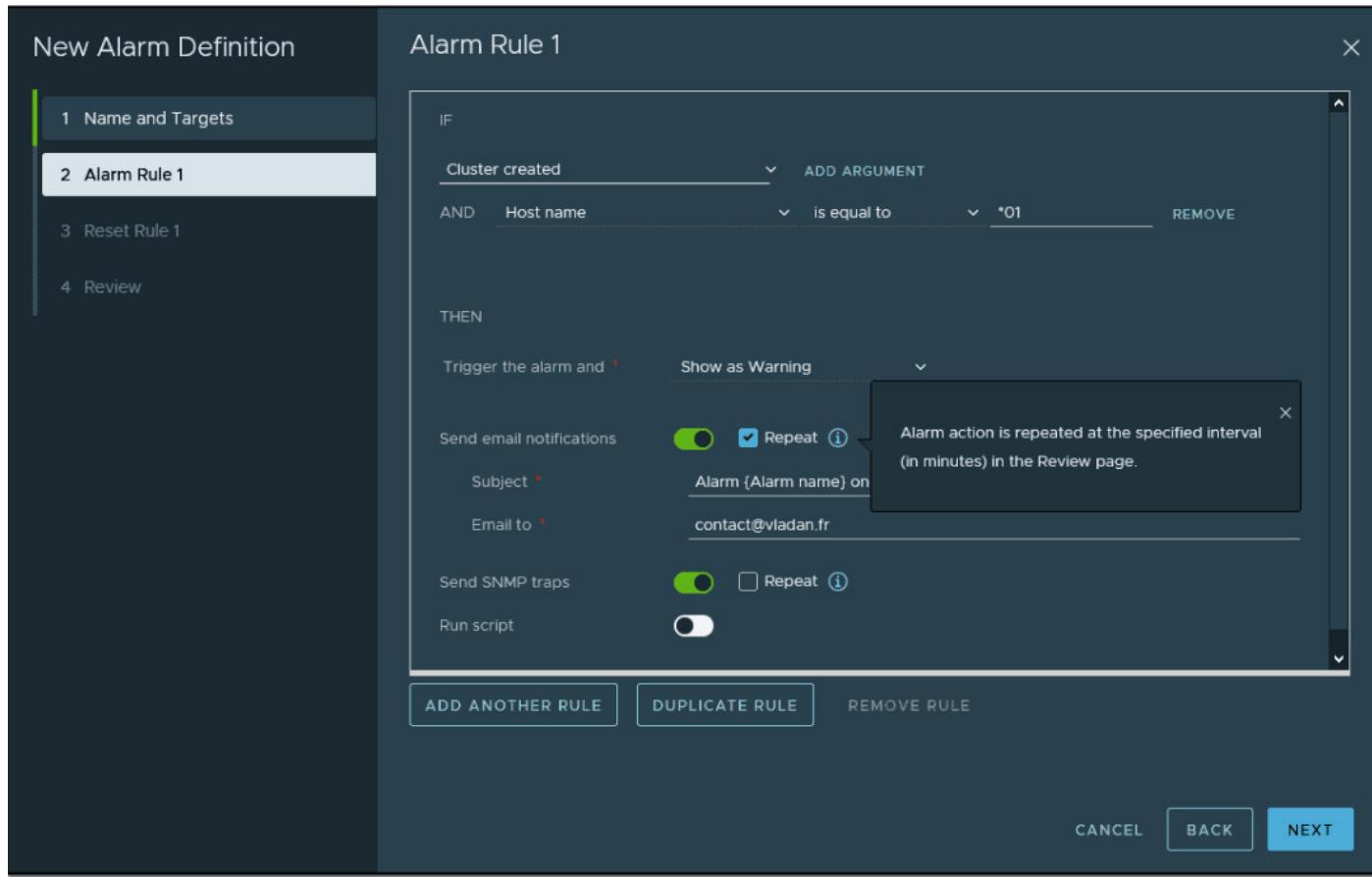


### Provide a name and specify the target type

After choosing the target type and adding a meaningful name, choose the alarm rule and arguments. Then, in the lower section, select the rule's severity. This indicates whether the alarm is a warning, is critical, or keeps the target's current state.

Then set the notification type. You can choose from email, SNMP trap, or running a script.

Note the two buttons below: **Add Another Rule** and **Duplicate Rule**. Use them to add some additional rules to the alarm.



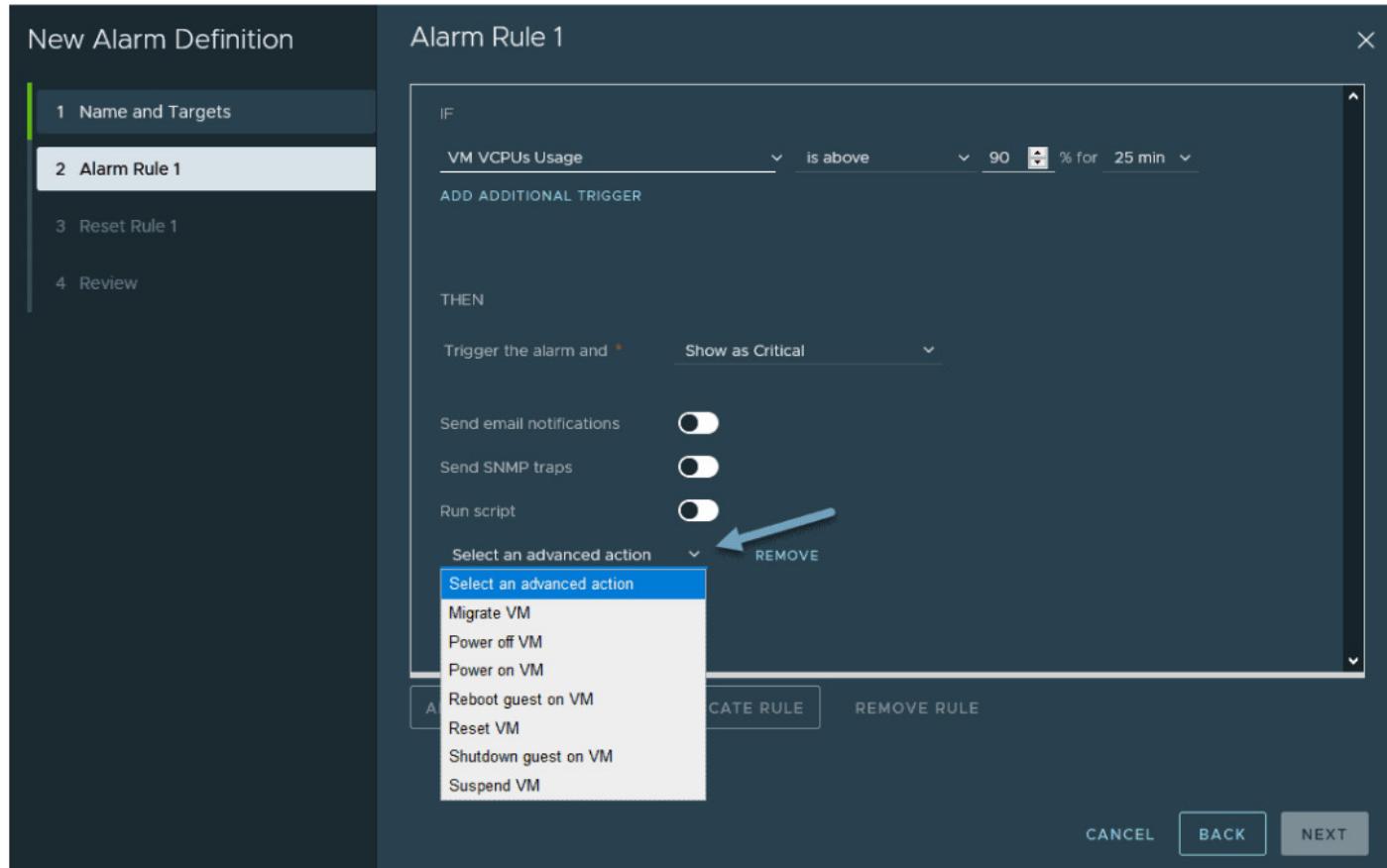
### Example of an alarm creation in vSphere 7

Note that the email and SNMP settings require that you first configure the mail settings for your vCenter Server. You must set the primary receiver URL to the DNS name or IP address of your SNMP receiver.

The **run script** option needs the full pathname of the command or script. Be sure to format it as a single string. The scripts are executed on the vCenter Server Appliance (VCSA).

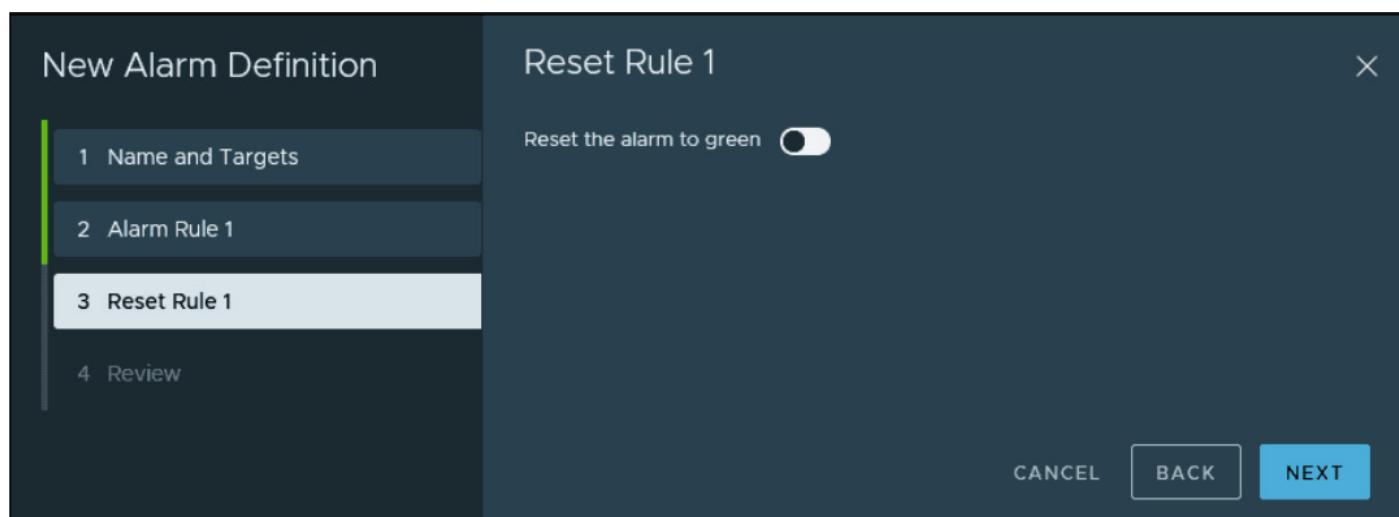
### Advanced actions

When you create an alarm that targets VMs and hosts, advanced actions are also available. Examples of host actions include **Enter Maintenance Mode** and **Exit Maintenance Mode**. Examples of virtual machine actions include **Migrate VM** and **Reboot Guest on VM**.



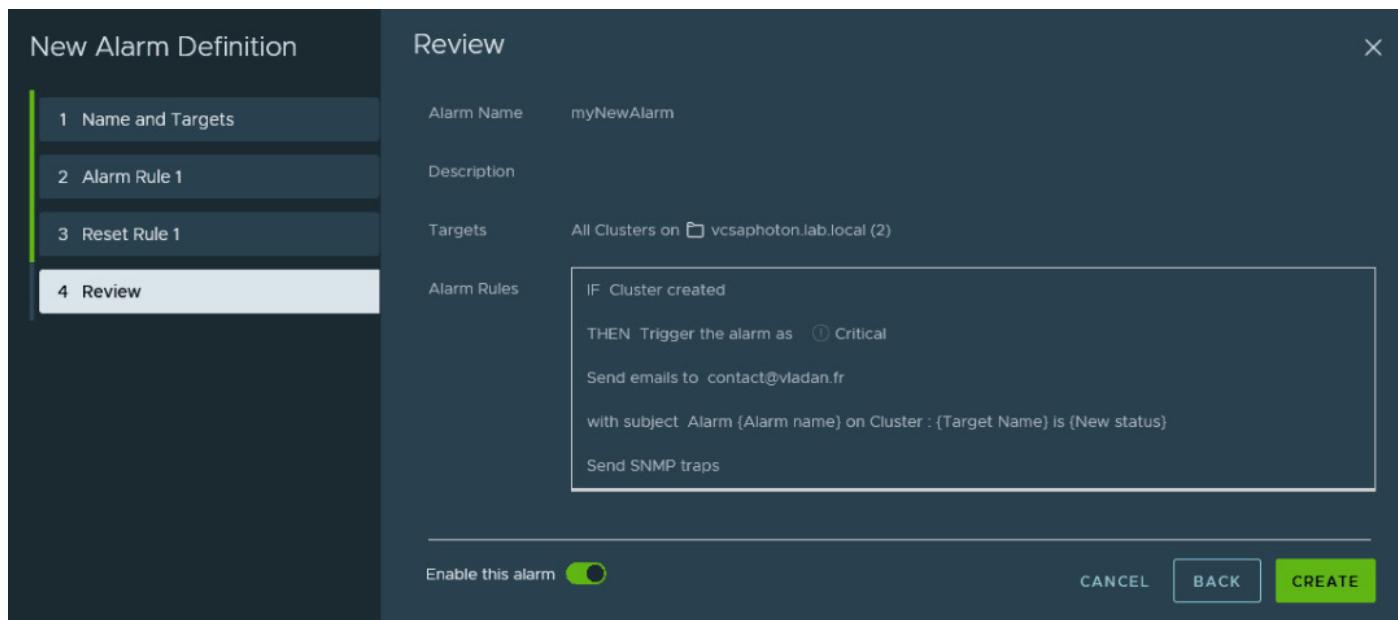
### Advanced actions for VMs and hosts

Let's continue with the assistant. On the next page, we can specify alarm reset rules by enabling the **Reset the Alarm to Green** option and providing details, such as arguments, operators, and actions.



### Specify alarm reset rules

Click **Next** to move to the review page, where you can see which alarms you've created, what the triggers are, and what notification options you picked up.



### Review page of the entire alarm creation assistant

Once done, you can sort the Last Modified column by date to find your freshly created alarm easily.

	Alarm Name	Object type	Defined In
<input checked="" type="radio"/> >	myNewAlarm	Cluster	This Object
<input type="radio"/> >	Skyline Health has detected issues...	vCenter Server	This Object
<input type="radio"/> >	vSAN cluster alarm 'vSAN Direct h...	Cluster	This Object
<input type="radio"/> >	Identity Source LDAP Certificate is ...	Host	This Object
<input type="radio"/> >	Trusted Host Attestation Failed Al...	Host	This Object
<input type="radio"/> >	TPM Encryption Recovery Key Bac...	Host	This Object

### My new alarm

As you can see, there are many options. There are nine different target types in the vSphere 7 suite. You can choose the vCenter Server, virtual machines, hosts, clusters, datacenters, datastores, distributed switches, distributed port groups, or datastore clusters. There are hundreds and hundreds of predefined alarms, so chances are that vSphere 7 already has you covered.

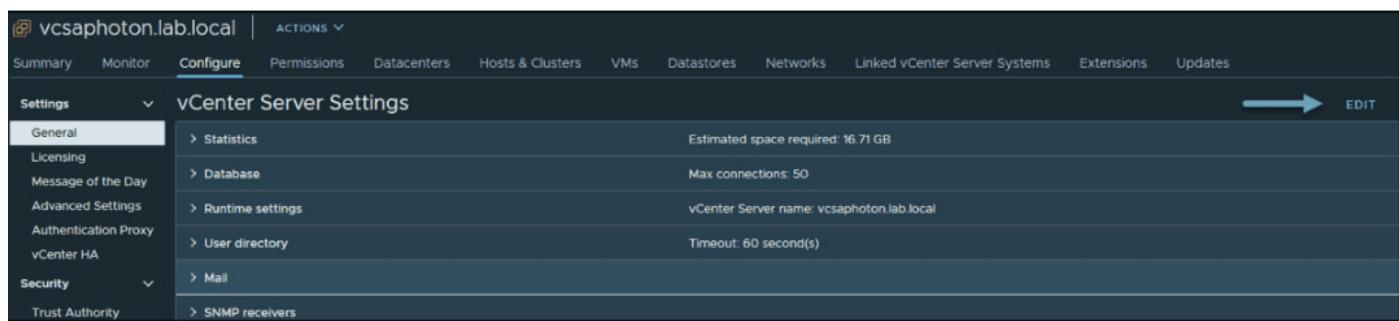
The custom alerts with notifications should help you to create your own alerts. There are numerous examples. For instance, you could create an alert to notify you when something is

not performing well, such as a lot of memory swapping, disk latency, or excessive CPU ready time metrics with high values. Another example could be notification about the poor health of vSAN objects, key management server problems, or vSphere HA cluster health issues.

The vSphere 7 alarm system is very flexible, enabling you to create your own personalized alarms that fit your own environment.

In larger environments, you'll certainly want to use a SNMP-based monitoring tool such as Nagios, vRealize Operations Manager, or vRealize Log Insight server. You won't configure email settings for your alarms because you'll most likely receive a lot of emails.

When you enable SNMP or SMTP (email), you must configure vCenter Server first so you can use one or the other. To do so, select the vCenter Server object in the vSphere Web Client and configure SNMP or SMTP from the vCenter Server Settings page.



The screenshot shows the vSphere Web Client interface for configuring vCenter Server. The navigation bar at the top includes 'vcsaphoton.lab.local', 'ACTIONS', 'Summary', 'Monitor', 'Configure' (which is selected), 'Permissions', 'Datacenters', 'Hosts & Clusters', 'VMs', 'Datastores', 'Networks', 'Linked vCenter Server Systems', 'Extensions', and 'Updates'. On the left, a sidebar menu under 'Settings' shows 'General' (selected), 'Licensing', 'Message of the Day', 'Advanced Settings', 'Authentication Proxy', and 'vCenter HA'. Under 'Security', it shows 'Trust Authority'. The main content area is titled 'vCenter Server Settings' and contains sections for 'Statistics' (Estimated space required: 16.71 GB), 'Database' (Max connections: 50), 'Runtime settings' (vCenter Server name: vcsaphoton.lab.local), 'User directory' (Timeout: 60 second(s)), 'Mail' (disabled), and 'SNMP receivers' (disabled). A large blue 'EDIT' button is located at the top right of the configuration pane.

### Configure vCenter Server 7 for SMTP and SNMP