



NAKIVO®

NEW

# VCP-DCV Community Study Guide

Based on vSphere 8.x  
VCP-DCV Certification

[UNOFFICIAL]



By Vladan SEGET

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

# NAKIVO Backup & Replication

A leading backup, ransomware protection and site recovery solution for virtual, physical, cloud, NAS and SaaS environments.



## FAST

Up to 2X faster backup. Instant recovery for anything

FILES, OBJECTS, PHYSICAL MACHINES, VMs, SITES



## AFFORDABLE

From \$2.45 workload/mo or use indefinitely from \$229/socket

UP TO 50% LOWER PRICES



## TOP RATED

5-star rating by top IT communities



High-performance, impact-free data protection; only 2 minutes to deploy across multiple platforms.

Experience up to 50% cost savings and achieve a higher ROI compared to any other solution

Exceptional support and functionality with top ratings on IT community platforms.

Comprehensive backup and recovery for business data — wherever it resides.

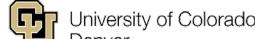
Ensure constant protection for your virtual, physical, cloud, NAS, and SaaS infrastructures.

Achieve instant recovery of critical data from any situation within minutes.

Over 25,000 businesses around the globe rely on NAKIVO to protect their data.

Exceed customer expectations with exceptional quality, technical support and rapid response times.

## Leading brands trust NAKIVO



# Table of Contents

<u>Introduction</u>	7
<u>Objective 1.1 – Identify the pre-requisites and components for a vSphere Implementation</u>	8
<u>Objective 1.2 – Describe the components and topology of a VMware vCenter architecture</u>	11
<u>Objective 1.3 – Describe storage concepts</u>	14
<u>Objective 1.3.1 – Identify and differentiate storage access protocols for vSphere (NFS, iSCSI, SAN, etc.)</u>	18
<u>Objective 1.3.2 – Describe storage datastore types for vSphere</u>	20
<u>Objective 1.3.3 Explain the importance of advanced storage configuration VASA, VAAI</u>	20
<u>Objective 1.3.4 Describe Storage Policies</u>	23
<u>Objective 1.3.5 - Describe basic storage concepts in VMware vSAN and VMware Virtual Volumes (vWOLs)</u>	28
<u>Objective 1.3.6 - Identify use cases for raw device mapping (RDM), Persistent Memory (PMem), Non-Volatile Memory Express (NVMe), NVMe over Fabrics (NVMe-oF), and RDMA (iSER)</u>	28
<u>Objective 1.3.7 - Describe Datastore Clusters</u>	32
<u>Objective 1.3.8 - Describe Storage I/O Control (SIOC)</u>	35
<u>Objective 1.4 - Describe VMware ESXi cluster concepts</u>	40
<u>Objective 1.4.1 - Describe VMware Distributed Resource Scheduler (DRS)</u>	45
<u>Objective 1.4.2 - Describe vSphere Enhanced vMotion Compatibility (EVC)</u>	48
<u>Objective 1.4.3 - Describe how DRS scores virtual machines</u>	52
<u>Objective 1.4.4 - Describe VMware vSphere High Availability (HA)</u>	56
<u>Objective 1.4.5 - Identify use cases for fault tolerance</u>	60
<u>Objective 1.5 - Explain the difference between VMware standard switches and distributed switches</u>	64
<u>Objective 1.5.1 – Describe VMkernel networking</u>	69
<u>Objective 1.5.2 – Manage networking on multiple hosts with vSphere Distributed Switch (VDS)</u>	72
<u>Objective 1.5.3 – Describe Networking Policies</u>	80
<u>Objective 1.5.4 – Manage Network I/O Control (NIOC) on a vSphere Distributed Switch (VDS)</u>	88
<u>Objective 1.5.5 – Describe Network I/O Control (NIOC)</u>	94
<u>Objective 1.6 – Describe VMware vSphere Lifecycle Manager concepts</u>	94
<u>Objective 1.7 – Describe The basics of vSAN as primary storage</u>	97
<u>Objective 1.7.1 – Identify basic vSAN requirements (networking, disk count, and type)</u>	100
<u>Objective 1.7.2 – Identify Express Storage Architecture (ESA) concepts for vSAN 8</u>	102
<u>Objective 1.8 – Describe the role of Virtual Machine Encryption in a data center</u>	106
<u>Objective 1.8.1 – Describe vSphere Trust Authority</u>	110
<u>Objective 1.8.2 – Describe the role of a Key Management Services (KMS) server in vSphere</u>	112
<u>Objective 1.9 – Recognize methods of securing virtual machines</u>	117
<u>Objective 1.9.1 – Recognize use cases for a virtual Trusted Platform Module (vTPM)</u>	119

<u>Objective 1.9.2 – Differentiate between Basic Input or Output System (BIOS) and Unified Extensible Firmware Interface (UEFI ) firmware</u>	122
<u>Objective 1.9.3 – Recognize use cases for Microsoft virtualization-based security (VBS)</u>	125
<u>Objective 1.10 – Describe identity federation</u>	129
<u>Objective 1.10.1 – Describe identity federation</u>	131
<u>Objective 1.10.2 – Recognize use cases for identity federation</u>	131
<u>Objective 1.11.1 – Describe VMware vSphere Distributed Services Engine</u>	135
<u>Objective 1.12 – Identify use cases for VMware Tools</u>	135
<u>Objective 1.13 – Describe the high-level components of VMware vSphere with Tanzu</u>	138
<u>Objective 1.13.1 – Identify the use case for a Supervisor Cluster and Supervisor Namespace</u>	139
<u>Objective 1.13.3 – Identify the use case for VMware Tanzu Kubernetes Grid (TKG) cluster</u>	141
<u>Objective 2.1 – Describe the role of VMware vpShere in the Software-Defined Data Center</u>	142
<u>Objective 2.2 – Identify use case for vSphere+</u>	144
<u>Objective 2.3 – Identify use cases for VMware vCenter Converter</u>	146
<u>Objective 2.4 – Identify disaster recovery (DR) use cases</u>	148
<u>Objective 2.4.1 – Identify VMware vCenter replication options</u>	150
<u>Objective 2.4.2 – Identify use cases for VMware Site Recovery Manager (SRM)</u>	152
<u>Objective 4.1 – Describe single sign-on (SSO)</u>	153
<u>Objective 4.1 – Configure single sign-on (SSO) Domain</u>	155
<u>Objective 4.1.2 – Join an existing single sign-on (SSO) domain</u>	161
<u>Objective 4.2 Configure vSphere distributed switches</u>	163
<u>Objective 4.2.1 - Create a distributed switch</u>	166
<u>Objective 4.2.2 - Add ESXi hosts to the distributed switch</u>	166
<u>Objective 4.3 - Configure Virtual Standard Switch (VSS) advanced virtual networking options</u>	166
<u>Objective 4.4 – Setup Identity Sources</u>	171
<u>Objective 4.4.1 – Configure identity federation</u>	174
<u>Objective 4.4.2 – Configure LDAP integration</u>	176
<u>Objective 4.5 – Deploy and configure VMware vCenter Server Appliance (VCSA)</u>	178
<u>Objective 4.6 – Create and configure VMware HA and DRS advanced options (Admission Control, Proactive HA, etc.)</u>	189
<u>Objective 4.7 – Deploy and configure VMware vCenter High Availability</u>	193
<u>Objective 4.8 – Set up content library</u>	197
<u>Objective 4.8.1 (4.8.2-4.9.2) – Content library</u>	203
<u>Objective 4.10 – Manage virtual machine (VM) template versions</u>	203
<u>Objective 4.10.1 – Update template in content library</u>	206
<u>Objective 4.11 – Configure VMware vCenter file-based backup</u>	206

<a href="#">Objective 4.12 – Configure vSphere Trust Authority</a>	209
<a href="#">Objective 4.13 – Configure vSphere certificates</a>	211
<a href="#">Objective 4.13.1 – Describe Enterprise PKI’s role for SSL certificates</a>	214
<a href="#">Objective 4.14 – Configure vSphere Lifecycle Manager</a>	216
<a href="#">Objective 4.15 – Configure different network stacks</a>	221
<a href="#">Objective 4.16 – Configure Host Profiles</a>	224
<a href="#">Objective 4.17 – Identify ESXi Boot Options</a>	231
<a href="#">Objective 4.17.1 – Configure Quick Boot</a>	236
<a href="#">Objective 4.17.2 – Securely Boot ESXi hosts</a>	239
<a href="#">Objective 4.18 – Deploy and configure clusters using the vSphere Cluster QuickStart workflow</a>	240
<a href="#">Objective 4.18.2 – Use Cluster QuickStart workflow to configure a cluster</a>	242
<a href="#">Objective 4.18.3 – Use QuickStart to expand clusters</a>	242
<a href="#">Objective 4.19.1 – Configure Time Configuration</a>	243
<a href="#">Objective 4.19.2 – Configure ESXi Services</a>	246
<a href="#">Objective 4.19.3 – Configure Product Locker</a>	246
<a href="#">Objective 4.19.4 – Configure Lockdown Mode</a>	250
<a href="#">Objective 4.19.5 – Configure ESXi Firewall</a>	256
<a href="#">Objective 4.20 – Configure vSphere with Tanzu</a>	260
<a href="#">Objective 4.20.1 – Configure a Supervisor Cluster &amp; Supervisor Namespace</a>	261
<a href="#">Objective 4.20.2 – Configure a Tanzu Kubernetes Grid Cluster</a>	262
<a href="#">Objective 4.20.3 – Configure vSphere Zones</a>	262
<a href="#">Objective 4.20.3 – Configure Namespace permissions</a>	262
<a href="#">Objective 5.1 - Identify resource pools use cases</a>	262
<a href="#">Objective 5.1 .1 - Explain shares, limits and reservations (resource management)</a>	266
<a href="#">Objective 5.2 - Monitor resources of a VMware vCenter Server Appliance (VCSA) and vSphere 8.x environment</a>	269
<a href="#">Objective 5.3 - Identify and use resource monitoring tools</a>	274
<a href="#">Objective 5.4 - Configure Network I/O Control (NIOC)</a>	279
<a href="#">Objective 5.5 - Configure Storage I/O Control (SIOC)</a>	285
<a href="#">Objective 5.6 - Configure a virtual machine port group to be offloaded to a data processing unit (DPU)</a>	290
<a href="#">Objective 5.7 - Explain the performance impact of maintaining virtual machine snapshots</a>	292
<a href="#">Objective 5.8 - Use Update Planner to identify opportunities to update VMware vCenter</a>	296
<a href="#">Objective 5.9 - Use vSphere Lifecycle Manager to determine the need for upgrades and updates</a>	300
<a href="#">Objective 5.9.1 - Update virtual machines</a>	301
<a href="#">Objective 5.9.2 - Update VMware ESXi</a>	302
<a href="#">Objective 5.10 - Use performance charts to monitor performance</a>	305

<a href="#">Objective 5.11 - Perform proactive management with VMware Skyline</a>	305
<a href="#">Objective 5.12 - Use VMware vCenter management interface to update VMware vCenter</a>	307
<a href="#">Objective 5.13 - Complete lifecycle activities for VMware vSphere with Tanzu</a>	308
<a href="#">Objective 5.13.1 - Update Supervisor cluster</a>	309
<a href="#">Objective 5.13.2 - Backup and restore VMware vSphere with Tanzu</a>	309
<a href="#">Objective 6.1 - Identify use cases for enabling vSphere Cluster Services (vCLS) retreat mode</a>	309
<a href="#">Objective 6.2 - Differentiate between the main management services in VMware ESXi and vCenter and their corresponding log files</a>	315
<a href="#">Objective 6.3 – Generate Log Bundle</a>	320
<a href="#">Objective 7.1 – Create and manage virtual machine snapshots</a>	320
<a href="#">Objective 7.2 – Create virtual machines using different methods (Open Virtualization Format (OVF) templates, content library, etc.)</a>	324
<a href="#">Objective 7.3 – Manage virtual machines (modifying virtual machine settings, VMware per-VM EVC, latency sensitivity, CPU affinity, etc.)</a>	325
<a href="#">Objective 7.4 – Manage Storage</a>	326
<a href="#">Objective 7.5 – Create DRS affinity and anti-affinity rules for common use cases</a>	339
<a href="#">Objective 7.6 – Migrate virtual machines</a>	345
<a href="#">Objective 7.6.1 – Identify requirements for Storage vMotion, Cold Migration, vMotion, and Cross vCenter Export</a>	348
<a href="#">Objective 7.7 – Configure role-based access control</a>	348
<a href="#">Objective 7.8 – Manage Host Profiles</a>	353
<a href="#">Objective 7.9 – Utilize VMware Lifecycle Manager</a>	353
<a href="#">Objective 7.9.1 – Describe firmware upgrades for VMware ESXi</a>	355
<a href="#">Objective 7.9.2 – Describe VMware ESXi Updates</a>	355
<a href="#">Objective 7.9.3 – Describe component and driver updates for VMware ESXi</a>	356
<a href="#">Objective 7.9.4 – Describe hardware compatibility check</a>	356
<a href="#">Objective 7.9.5 – Describe ESXi cluster image export functionality</a>	358
<a href="#">Objective 7.9.6 – Create VMware ESXi cluster image</a>	363
<a href="#">Objective 7.10 – Use predefined alarms in VMware vCenter</a>	363
<a href="#">Objective 7.11 – Create custom alarms</a>	368
<a href="#">Objective 7.12 – Deploy an encrypted virtual machine</a>	368
<a href="#">Objective 7.12.1 – Convert a non-encrypted virtual machine to an encrypted virtual machine</a>	368
<a href="#">Objective 7.12.2 – Migrate an encrypted virtual machine</a>	370
<a href="#">Objective 7.12.3 – Configure virtual machine vMotion encryption properties</a>	372

# Introduction

In order to become **VCP-DCV certified** and pass the Professional vSphere exam, we follow are the guidelines from the Official VMware Exam guide 2V0-21.23 (Blueprint).

The Professional vSphere Exam (**2V0-21. 23**) 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 135 minutes to complete the exam.

The VMware Exam prep guide is [here](#) on VMware's website. The official code for this exam is 2VO-21.23, and the cost of the exam is \$250.00.

# Objective 1.1 – Identify the pre-requisites and components for a vSphere Implementation

## VMware ESXi Server

Only supported hardware should be used to install VMware ESXi. If you use unsupported hardware, you most likely won't find certain components, like NICs, storage controllers, etc., after installation. For a list of all supported platforms, see the [VMware Compatibility Guide](#).

## System Requirements

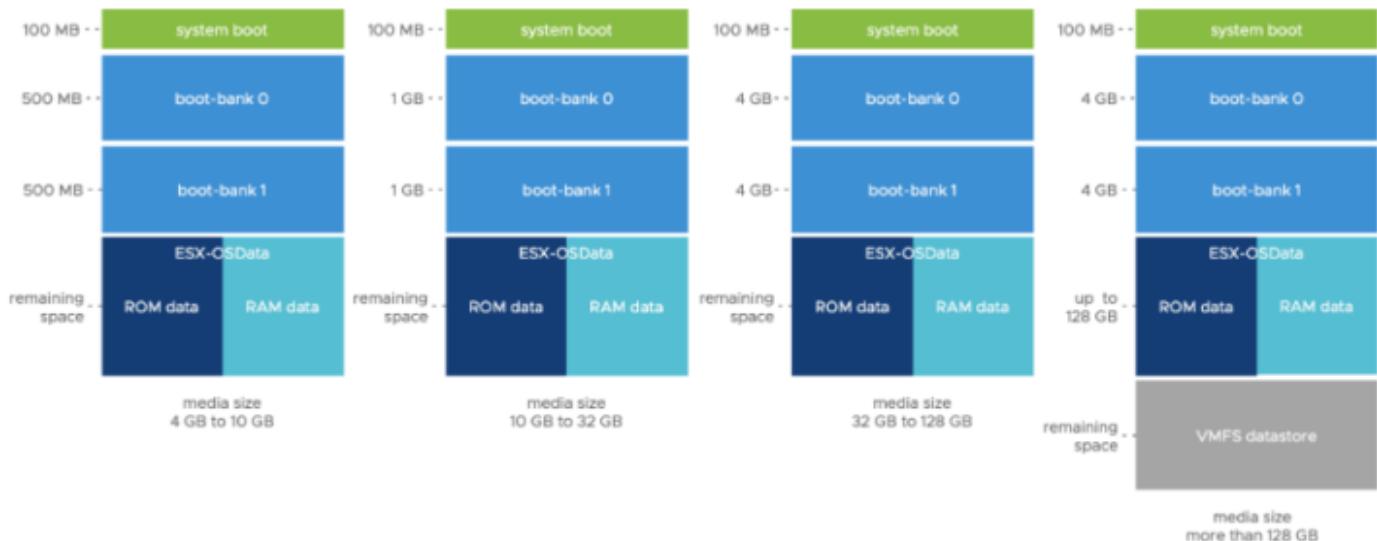
Below is an overview of system requirements:

- ESXi 8.0 requires a host with at least two CPU cores.
- ESXi 8.0 supports a broad range of multi-core of 64-bit x86 processors. For a complete list of supported processors, see the [VMware Compatibility Guide](#).
- ESXi 8.0 requires the NX/XD bit to be enabled for the CPU in the BIOS.
- ESXi 8.0 requires a minimum of 8 GB of physical RAM. For a typical production environment, provide at least 12 GB of RAM to run virtual machines.
- 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](#).
- ESXi 8.0 requires a boot disk of at least 32 GB of persistent storage such as HDD, SSD, or NVMe. A boot device must not be shared between ESXi hosts.
- 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 8.0 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. The ESXi 8.0 has only 4 different partitions compared to the previous release, which had 8.

Since vSphere 7, VMware limits the number of cores per license to 32 (it was unlimited before). If you buy a 1 CPU license, you will only be able to have a CPU with 32 cores. If the CPU has more than 32 cores, you will need additional (per-CPU) licenses. For example, for a 48-core CPU, you will need 2 licenses.

This affects not only paid VMware vSphere/ESXi licenses, as ESXi Free version 8.0 raises these requirements to more than 3 GB of disk space (3.72 GB to be precise). The recommended size is actually 32 Gb. It's interesting that while the size of the boot partition (100 MB) does not change, the sizes of the other partitions change depending on which size of media is used for the installation.



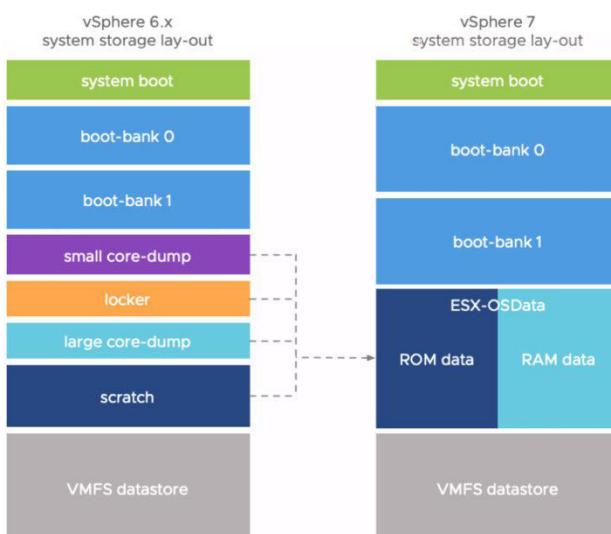
Apart from HDD, SSD, and NVMe, you can also use boot from a SAN LUN.

## Storage Requirements

The minimal ESXi 8.x storage requirements for installation are:

- 8 GB for USB sticks or SD devices (4 GB when upgrading from ESXi 6.7).
- 32 GB 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 has more than 2 or 3 hosts, you will want to have vCenter. VMware VCSA is a Linux distribution based on Photon OS. If you do not follow VMware at all and know only ESXi, then we could say that yes, VCSA is a management VM for ESXi hosts.

The VCSA VM runs PhotonOS 3.0 which is a Linux distribution 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 (VCSA) for VMware vSphere. The updates of the VCSA are now quite easy too.

The screenshot shows the vCenter Server Management interface. On the left, a sidebar lists navigation options: Summary, Monitor, Access, Networking, Firewall, Time, Services, Update, Administration, Syslog, and Backup. The 'Summary' tab is selected. In the center, there's a summary card with a purple cube icon. To its right, detailed system information is displayed:

Hostname:	vcsaphoton.lab.local
Product:	VMware vCenter Server
Version:	8.0.0.10200
Build number:	21216066
Uptime:	3 hours 37 minutes

Below this is a 'Health Status' section with a table:

Health Status	
Overall Health	Good (Last checked Feb 20, 2023, 07:02:23 PM)
CPU	Good
Memory	Good
Database	Good
Storage	Good
Swap	Good

On the right side, there's a 'Single Sign-On' section with a table:

Domain	Status
vsphere.local	Running

In the bottom right corner, there's a logo for 'ESX virtualization'.

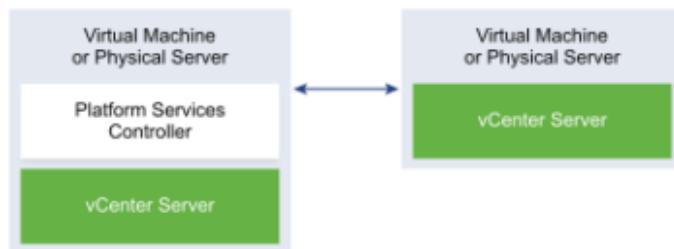
VMware Platform Services Controller (PSC) is now integrated into the same VM. The architectures with external PSCs are phased out, and vCenter 7 allows you to do easy migration via assistant.

## Objective 1.2 – Describe the components and topology of a VMware vCenter architecture

vCenter Server is the central point of vSphere. While your clusters can run and ensure High Availability (HA) in an automated matter, you need vCenter Server 8 to configure them. The same applies to vSphere distributed virtual switches and other components. All these different software components are installed on vCenter as plugins, as side-by-side products, but they need vCenter Server to function. Even your backup or monitoring software heavily relies on vCenter Server.

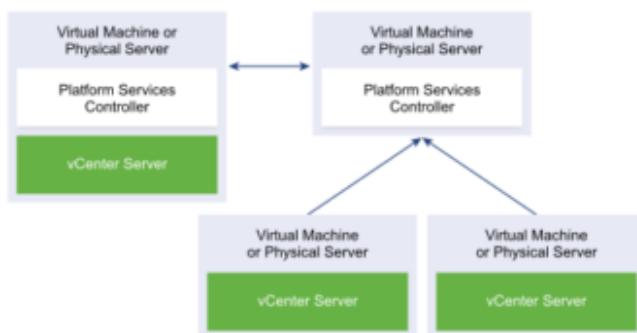
When you first install vCenter Server 6.7, your deployment includes either an embedded Platform Services Controller or an external Platform Services Controller. The installer does not validate whether the Platform Services Controller is external or embedded with vCenter Server. Although many types of join operations are possible, not all resulting topologies are supported. Before you upgrade or migrate your environment to vSphere 8.0, you must move any deprecated deployment topology to a supported deployment topology.

**Deprecated topology of a vCenter Server Pointing to an Embedded Platform Services Controller**



or like this:

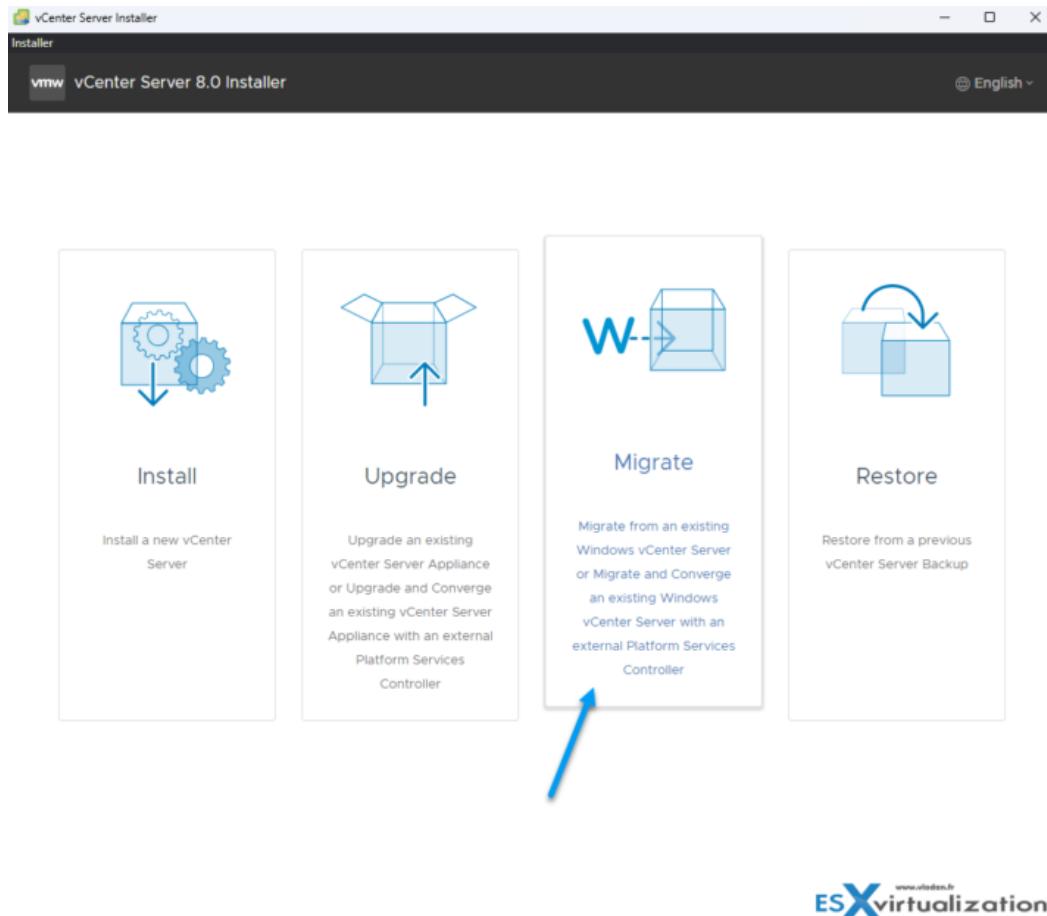
**Deprecated Topology of an Embedded Platform Services Controller and an External Platform Services Controller in Replication**



For topologies with external Platform Services Controller (PSC) instances, the PSC will be converged during the upgrade process to vCenter Server 8.0. After a successful upgrade, the external PSC is powered off can be removed from your vSphere inventory. See [Decommission the Platform Services Controller](#).

vSphere 8 (same as vSphere 7) only uses the embedded model, where the same VM runs the vCenter Server and PSC services on the same virtual machine (VM). Check the VMware Product Interoperability Matrices and the VMware Compatibility Guide for the latest paths.

Note that to upgrade vCenter Server appliance version 6.5 or earlier, you must first upgrade to version 6.7 or 7.0 and then upgrade to version 8.0.



## Deprecated Topologies and vCenter Upgrade Paths

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

1. vCenter 6.0 or later can be directly upgraded to 6.7.
2. vCenter Server on Windows is no longer available in vSphere 8, so any previous versions must be converted via the assistant. There is a Migrate option 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, the vCenter Server Converge Tool allows you to migrate the external PSCs into the embedded ones. When executed, the Converge

Tool checks whether you need any additional components via internet access (if you have one), and those components are 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 to 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 results in fewer VMs to manage and less consumption of RAM, CPU, or storage. If you have a large-scale architecture with many PSCs, this conversion can save a significant 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 the appliance.

This is a two-stage process:

- The first stage involves deploying 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.

Before starting with the migration process, make sure you have backed up all data and have started the Migration Assistant on the source vCenter Server for Windows. Click Next, to proceed with stage 1.

Mount the VCSA installer CD **on the Windows VM** where vCenter is installed, which you are converting, and run the VMware Migration Assistant on the Windows machine. It is a CLI utility you can 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. To do that, see [VMware KB 2146453](#).

## **What you can migrate and how**

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 may also have an external database. You have the possibility to migrate the data from the external DB to the embedded

PostgreSQL database in vCenter Server 8. There are checkboxes to allow you to make a choice about the data that you can or can't bring over.

You can also migrate vCenter tasks and history. The progress of the migration is shown in the browser window.

vCenter Server 8 runs on a single VM as a virtual appliance. You can add more resiliency with vCenter Server HA, with three nodes of vCenter Server instances running simultaneously. In case a host hosting one of those 3 instances goes down, another instance is automatically created on another host to make sure that the resiliency remains within the cluster. This configuration, however, consumes some resources, and that's why it is not recommended for smaller installations.

## Objective 1.3 – Describe storage concepts

### VMware vSphere and Kubernetes (K8s)

VMware calls it Cloud Native Storage (CNS), which is a component that is an extension of the vCenter server management. Through 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. The 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 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 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.

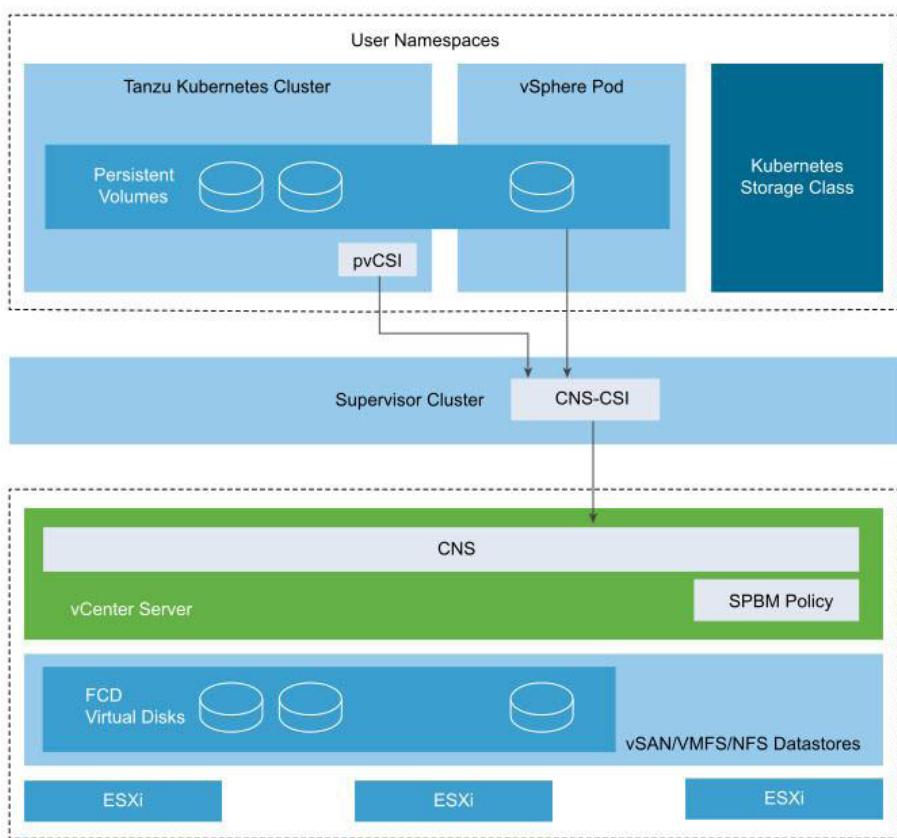
The persistent volumes are usually used for stateful applications. vSphere 8 supports dynamic and static provisioning of persistent volumes:

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

**Paravirtual CSI (pvCSI)** 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. Take a look these graphics from VMware to understand the different blocks and how they interact with each other.



[vSphere CNS-CSI and pvCSI](#)

## VMware vSAN

vSAN is 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.

The image from the lab shows a single disk group per host composed from a cache and capacity disk:

Name	Drive Type	Claimed As	Capacity
Local VMware, Disk (mpx.vmhba0:CO:T1:LO)	Flash	vSAN Cache	50.00 GB
Local VMware, Disk (mpx.vmhba0:CO: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, where you would carve storage out into LUNs and then create datastores on them.

With traditional storage, the storage administrator has a key role in meetings with the virtualization administrators. Decisions about storage schemas and layouts have to be made in advance. The traditional datastore layout has another disadvantage: 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. vVols offers granular control, which helps you 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.

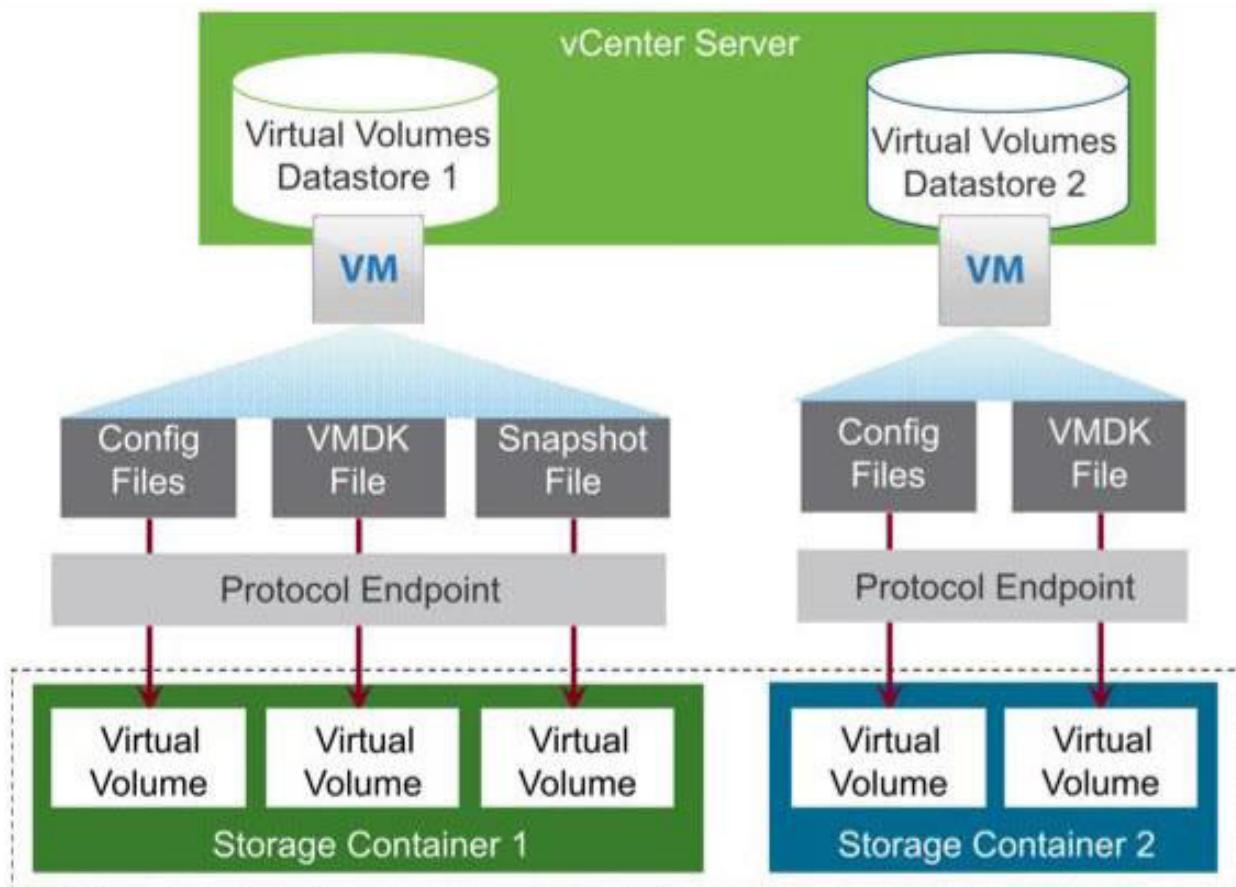
This helps vSphere to offload tasks such as cloning and snapshots to the storage array. You save some CPU cycles by doing that. And because you are creating individual volumes for each virtual disk, you have the possibility to apply policies at a very granular level. You can control the performance via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

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, 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 take a look at some graphics of vVols from VMware.



VMware vVols and storage array

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

**Local and Networked storage.** While local storage is pretty obvious (direct-attached disks or DAS), the networked storage can be of different types. Most importantly, networked storage 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 the NFS 3 and NFS 4.1 protocols 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 on which the storage is physically installed can use it and not other machines within your cluster. That's why it is far better to use shared storage with NFS, iSCSI, or FC.

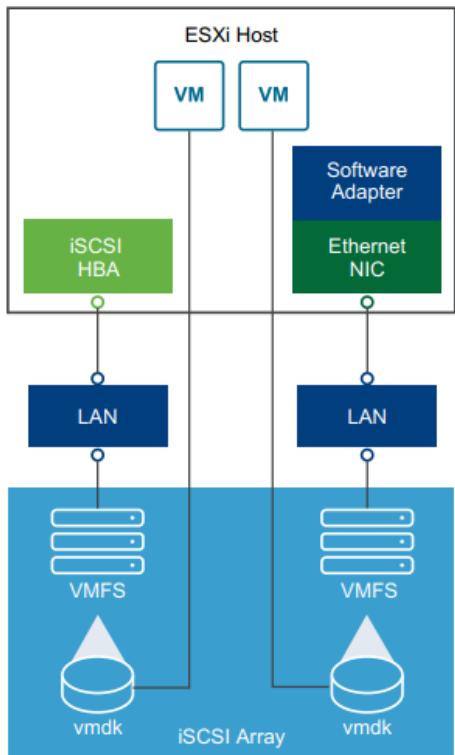
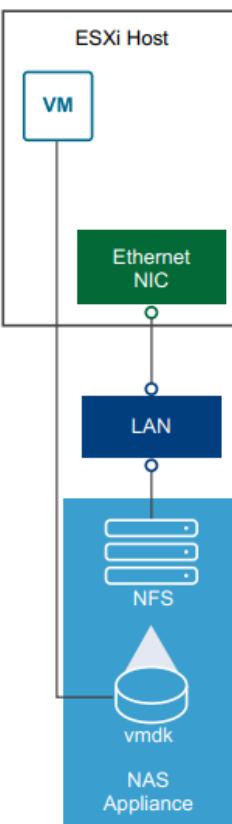
**Fibre Channel (FC)** storage. FC SAN is a specialized high-speed network that connects your hosts to high-performance storage devices. The network uses Fibre Channel protocol to transport SCSI traffic from virtual machines to the FC SAN devices. The host should have Fibre Channel host bus adapters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

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

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

ESXi offers the following types of iSCSI connections:

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

**Figure 2-3. iSCSI Storage****Figure 2-4. NFS Storage**

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

**Network storage** is usually based on dedicated enclosures that have controllers running usually Linux or other specialized OS on it. Now they are 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.

Here are a few more storage types:

- **VMware FileSystem (VMFS) datastores:** All block-based storage must be first formatted with VMFS to transform a block service to a file and folder oriented services.
- **Network FileSystem (NFS) datastores:** This is for NAS storage.
- **VVol:** Introduced in vSphere 6.0, it is a new paradigm 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). It uses APIs that allow storage partners to create and deliver multipathing and load-balancing plugins that are optimized for each array. Plugins talk to storage arrays and choose the best path selection strategy to increase IO performance and reliability.

## Objective 1.3.2 – Describe storage datastore types for vSphere

**VMFS.** you can use VMFS 5 or VMFS 6 within vSphere 8. 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 8 supports NFS v3 and 4.1, and this file system uses the network to access it. In the case of NFS, the access to the files is controlled by a NAS device.

**VMware vSAN.** vSAN uses local storage and SSDs from each host to create a storage pool shared within the cluster. You need at least 2 hosts and one witness host to create vSAN storage. Check other chapters in this guide for more specific and detailed information about vSAN.

**vVOL** is another type of storage using vVol datastore, which are storage containers on a block device.

Name	Status	Type
vSANDirect_eox03.lab.local_mpvmhba0:0:T4:L0	Normal	vSAN Direct
vSANDirect_eox03.lab.local_mpvmhba0:0:T2:L0	Normal	vSAN Direct
vSANDirect_evo02.lab.local_mpvmhba0:0:T4:L0	Normal	vSAN Direct
vSANDirect_evo01.lab.local_mpvmhba0:0:T4:L0	Normal	vSAN Direct
vSANDirect_evo01.lab.local_mpvmhba0:0:T3:L0	Normal	vSAN Direct
vsanDatastore	Normal	vSAN
180Gb	Normal	VMFS 6

## From vSphere 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 in bulk.
- 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 1.3.3 – Explain the importance of advanced storage configuration (VASA, VAAI, etc.)

**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. By using Storage Policies and VASA, you can specify that VMs need a specific performance profile or configuration, such as RAID type.

**VAAI** stands for vSphere APIs for Array Integration. This technology allows the offloading of 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, reduce storage latency for several types of storage operations, reduce the ESXi host CPU utilization for storage operations, and reduce storage network traffic.

**Note:** Some software vendors supports 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 iSCSI Disk (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:

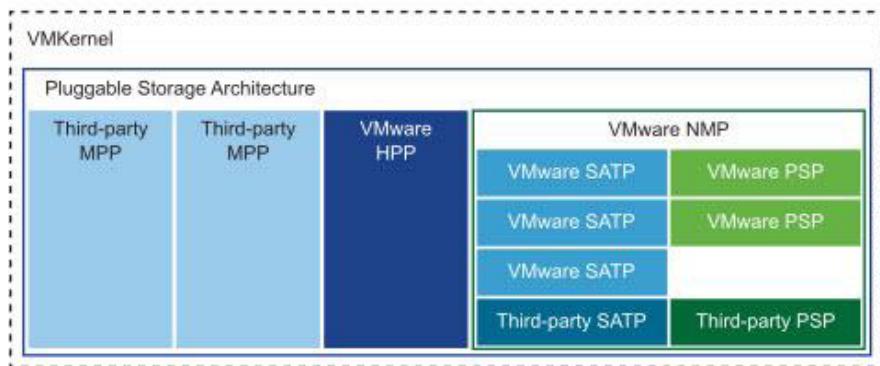
- Scalable lock management (sometimes called “hardware-assisted locking”, “Atomic Test & Set”, or ATS) replaces the use of SCSI reservations on VMFS volumes when performing metadata updates. This can reduce locking-related overheads, speeding up many administrative tasks as well as increasing I/O performance 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** help monitor space usage on thin-provisioned storage arrays to prevent out of space conditions and do space reclamation when data is deleted.

**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 1.3.4 Describe storage policies

vSphere 8 storage policy has 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 DR capability they have.

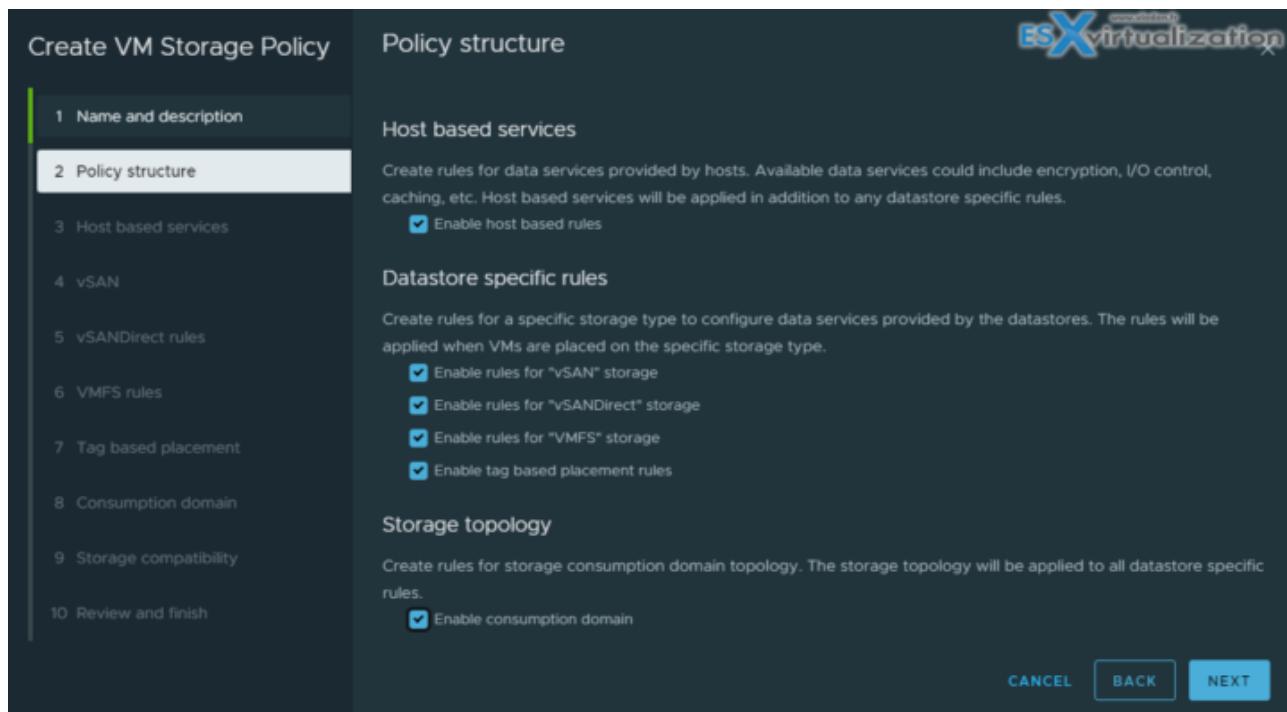
**VM Storage Policies for host-based data services** are basically rules for services provided by your ESXi host. This can be for example compression and encryption.

**VM Storage Policies for vVols** allow you to 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.

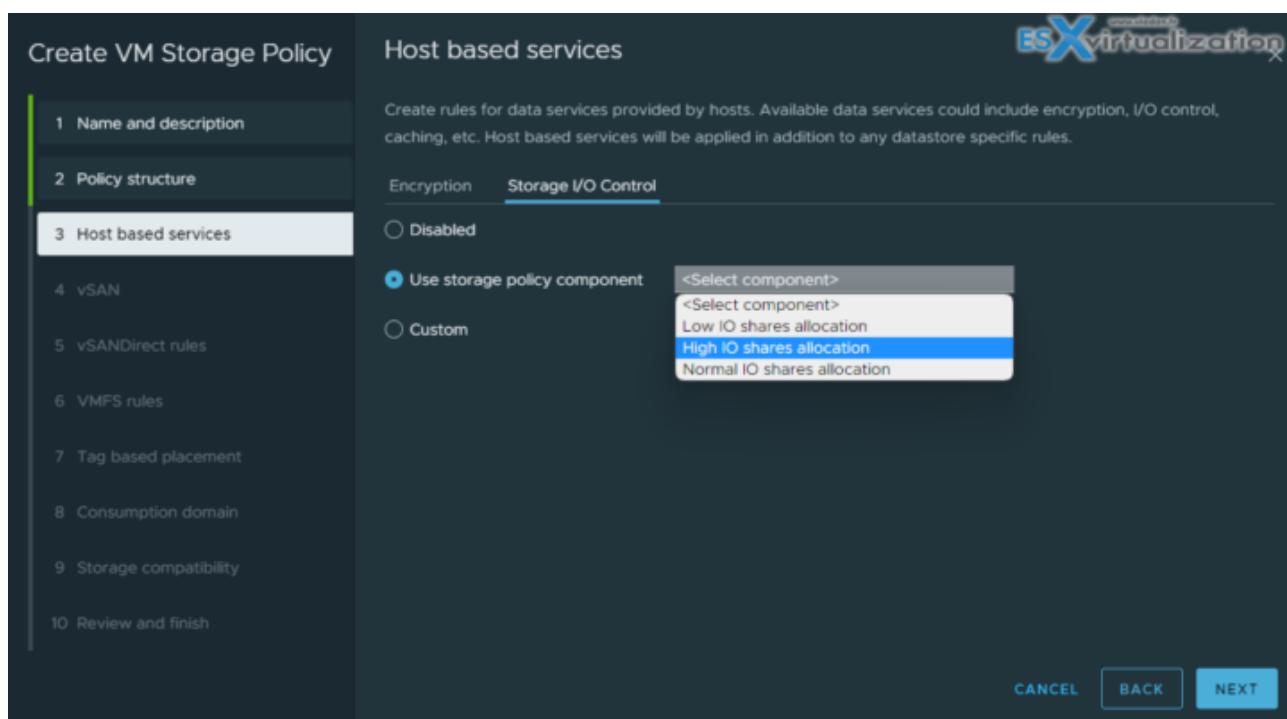
Tag-based rules reference the tags that you assign to the datastores and can filter the datastores to be used for the placement of the VMs.

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 have to be entered concerning storage I/O control. Usually, you have to check this with your hardware manufacturer.

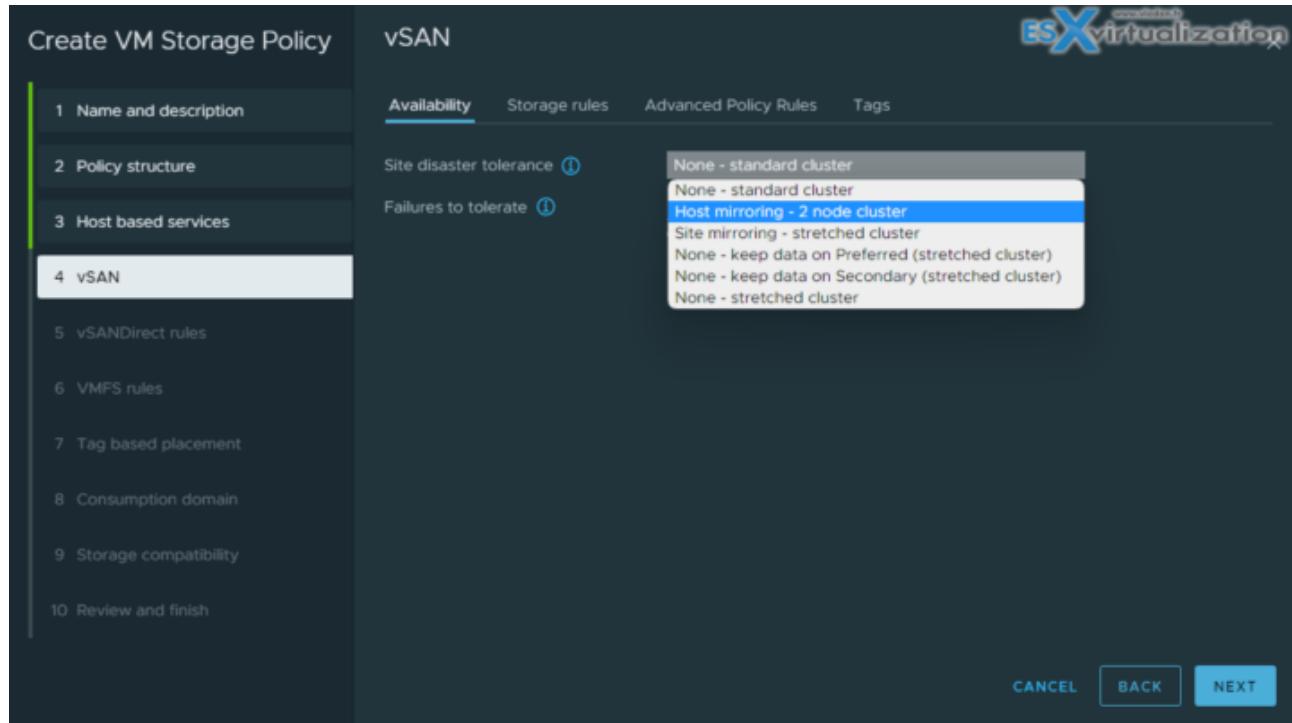
Open the **Create VM Storage Policy** wizard. Click **Menu > Policies and Profiles > VM Storage Policies > Create VM Storage Policy**.



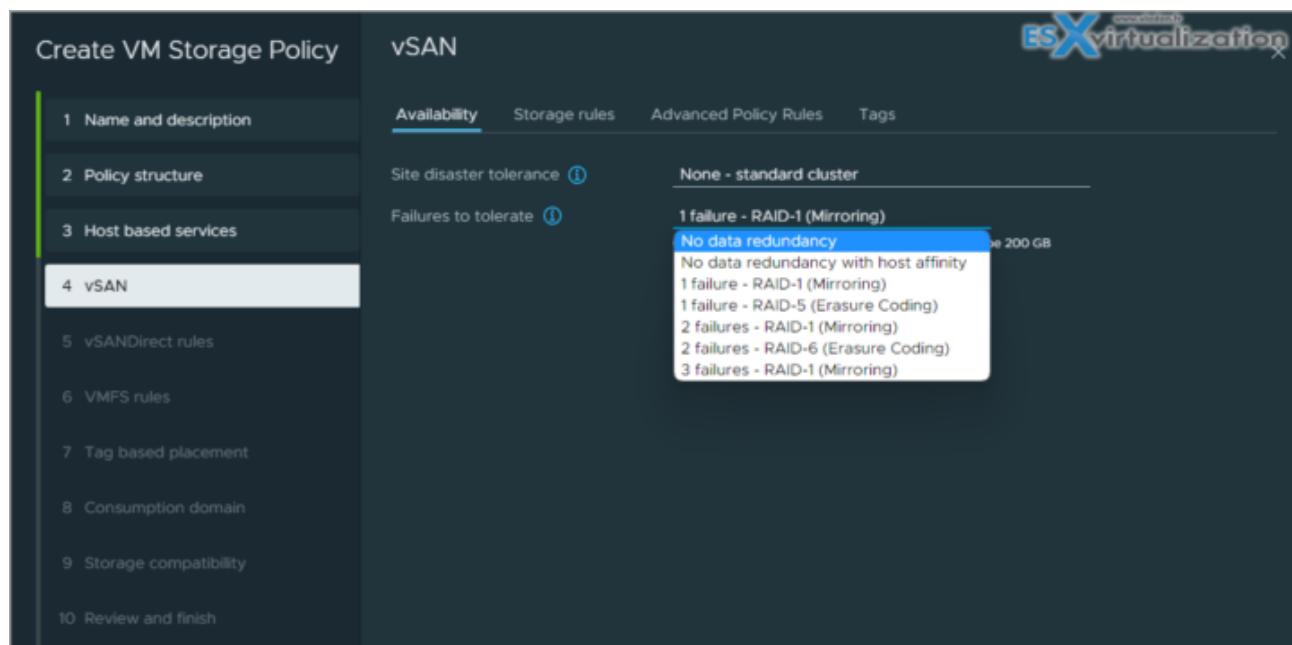
The click Next. You will be able to specify and enable host-based rules, enable rules for vSAN storage or enable tag-based placement rules.



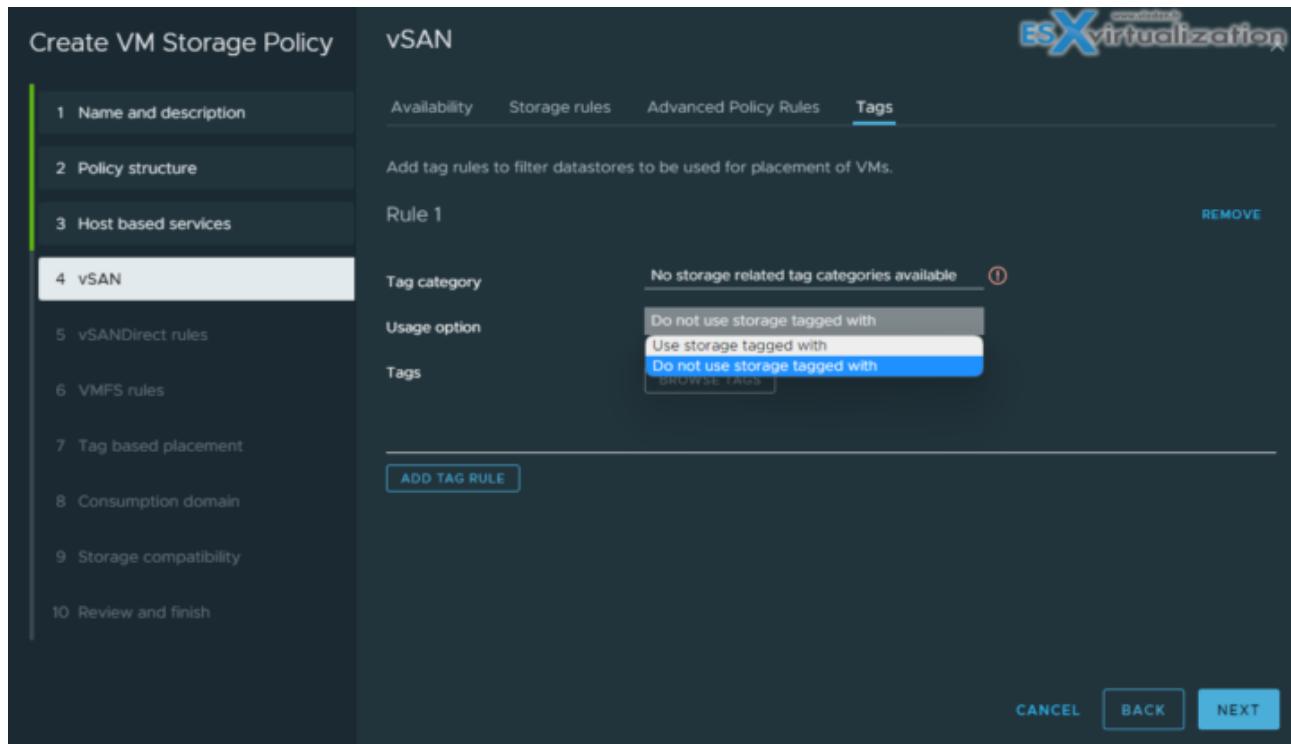
And then you can specify either Encryption or Storage I/O control-based policy creation.



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. Pretty neat.



If you have checked the tags-based policy, the next screen shows the options there. You can use your tags already created. If you haven't created them, you should 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 which does that).

As an example, you could create a tag named Diamond and use it for the storage with 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 have a look at those differences below:

- **Eager Zeroed Thick.** The disk space is allocated and erased (that is, 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.** 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.** 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 – don't over allocate space on datastore).

## vSAN Specific Storage Policies

We talked briefly about those policies during the wizard creation.

**Primary Level of Failures to tolerate (PFTT).** This policy defines the number of hosts and device failures VM objects can survive. For “n” failures tolerates, the data is stored in “n+1” locations. It’s the default policy.

**Secondary Level of Failures to tolerate (SFTT).** When used in stretched clusters, this policy defines the number of additional host failures that can be tolerated after you have a site failure. 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 documentation](#).

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

**Failure Tolerance Method.** you can define a 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. Note that the higher the number, the more resources are consumed.

**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 are available: yes/no. When set to yes, the policy forces provisioning of objects even when policy cannot be met. The default is 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 the data spread across 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. The default is no.

## Objective 1.3.5 – Describe basic storage concepts in VMware vSAN and VMware Virtual Volumes (vVOLs)

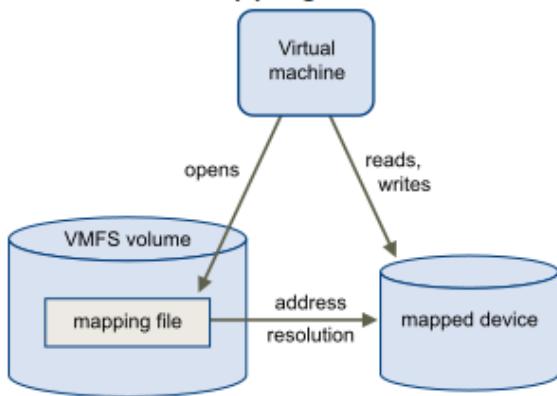
Covered in 1.3.

## Objective 1.3.6 – Identify use cases for raw device mapping (RDM), Persistent Memory (PMem), Non-Volatile Memory Express (NVMe), NVMe over Fabrics (NVMe-oF), and RDMA (iSER)

### What Is RDM?

VMware VMFS filesystem supports feature that is called an RDM. This file, an RDM, is a special mechanism for a VM to have direct access to a LUN on the SAN. This mechanism is done via a symbolic link. The LUN can be formatted in any way you want, and it does not have to be formatted as VMFS with VMDKs, etc. This kind of mechanism actually simplifies a bit and removes two layers of complexity, which are VMFS and VMDKs sitting on the top.

#### Raw Device Mapping



### How Does RDM Work?

RDM is a symbolic link (raw device mapping) from a VMFS volume to a raw LUN. The mapping has a sort of that it makes those LUNs appear as files in a VMFS volumes. Think of the mapping file as a proxy for a raw physical device.

At certain moments, you might find it more likely to use raw LUNs or logical disks located in a SAN. However, traditional VMFS volumes are still recommended by VMware as a default volume creation.

RDM has 2 modes:

- **Virtual Compatibility Mode.** The RDM acts like a virtual disk file. The RDM can use snapshots.
- **Physical Compatibility Mode.** The RDM offers direct access to the SCSI device for those applications that require lower-level control.

## RDM Use Cases

- **Hardware Specific SCSI.** For any application running in VMs that needs to access a device using hardware-specific SCSI commands.
- **Clustered VMs.** For Microsoft cluster configuration (MSCS) in a VM (virtual-to-virtual or physical-to-virtual).
- **SAN Management Software.** For running SAN management software (Storage resource management software, storage array snapshot software, replication software) inside a virtual machine.
- **NPIV Virtualization.** For configuring a virtual machine to use N-Port ID Virtualization (NPIV).
- **Conversions.** RDM is useful in physical-to-virtual conversion operations by avoiding migration of a large data LUN to a VMDK.

## VMware Persistent Memory (PMem)

PMem is non-volatile. It is capable of retaining data after any planned or unplanned power events. In essence, persistent memory fills the gap between DRAM and traditional storage when it comes to performance and cost, by bringing the data closer to the CPU.

PMem is located very close to the CPU compared to traditional storage, resulting in lower latency and faster performance.

PMem modules are available from major hardware manufacturers such as Dell or Intel. Intel's Optane DC persistent memory has been designed to improve performance and give you almost RAM speed. The latency is a little higher than RAM but still within nanoseconds.

You can have PMem configured to allow failover on another host for all NVDIMM devices. During host failure, HA will restart the virtual machine on another host with new empty NVDIMMs.



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

## Non-Volatile Memory Express (NVMe)

Virtual NVMe Device is new virtual storage host bus adapter (HBA) which has been designed to lower IO overhead and scalable IO for all flash SAN/vSAN storages.

With hardware NVMe SSDs taking significant advantage over old SATA/SAS flash-based devices, the mass adoption and the storage revolution is happening at present.

The main benefit of the NVMe interface over SCSI is overhead reduction and fewer CPU cycles. Also, there is a reduction of IO latency for VMs. Which Guest OS are supported?

**NVM Express (NVMe)** is a method for connecting and transferring data between a host and a target storage system. NVMe is designed for use with faster storage media equipped with non-volatile memory, such as flash devices. This type of storage can achieve low latency, low CPU usage, and high performance, and generally serves as an alternative to SCSI storage.

**NVMe Transports.** NVMe storage can be directly attached to a host using a PCIe interface or indirectly through different fabric transports. VMware NVMe over Fabrics (NVMe-oF) provides a distance connectivity between a host and a target storage device on a shared storage array.

Check the requirements of NVMe storage at [VMware documentation](#).

NVM Express (NVMe) is a standardized protocol designed specifically for high-performance multi-queue communication with NVM devices. ESXi supports the NVMe protocol to connect to local and networked storage devices.

## NVMe over Fabrics (NVMe-oF)

The NVMe storage can be directly attached to a host using a PCIe interface or indirectly through different fabric transports. VMware NVMe over Fabrics (NVMe-oF) provides a distance connectivity between a host and a target storage device on a shared storage array.

vSphere 8 NVMeoF Enhancements:

- Support for 256 Namespace and 4k paths
- Extend reservation support for NVMe devices
- Auto-discovery of NVMe Discovery Service support in ESXi

Check this page about all different [resources about NVMe-Of](#).

## VMware RDMA (iSER)

In addition to traditional iSCSI, ESXi supports the iSCSI Extensions for RDMA (iSER) protocol. When the iSER protocol is enabled, the iSCSI framework on the ESXi host can use the Remote Direct Memory Access (RDMA) transport instead of TCP/IP. You can configure iSER on your ESXi host.

See [Using iSER Protocol with ESXi](#).

Storage Adapters

Adapter		Type	Status	Identifier	Targets	Devices	Paths
vmhba33	Block SCSI	Unknown	--	1	2	2	
Model: VMware iSCSI over RDMA (iSER) Adapter							
vmhba64	iSCSI	Unbound	iser-vmnic9(iqn.1998-01.com.vmware:prime)	0	0	0	
vmhba65	iSCSI	Unbound	iser-vmnic10(iqn.1998-01.com.vmware:prime)	0	0	0	
vmhba66	iSCSI	Unbound	iser-vmnic4(iqn.1998-01.com.vmware:prime)	0	0	0	
vmhba67	iSCSI	Unbound	iser-vmnic5(iqn.1998-01.com.vmware:prime)	0	0	0	
Model: Wellsburg AHCI Controller							
vmhba1	Block SCSI	Unknown	--	0	0	0	
vmhba2	Block SCSI	Unknown	--	1	1	1	

Properties   Devices   Paths   Dynamic Discovery   Static Discovery   Network Port Binding   Advanced Options

**General**

Name	vmhba64	Edit...
Model	VMware iSCSI over RDMA (iSER) Adapter	
ISCSI Name	iqn.1998-01.com.vmware:prime-fcoe-005.eng.vmw	
ISCSI Alias	iser-vmnic9	
Target Discovery	Send Targets, Static Targets	

**Authentication**

Method	None	Edit...
--------	------	---------

## Objective 1.3.7 – Describe datastore clusters

Storage cluster configuration with Storage DRS (SDRS) in vSphere 8 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.

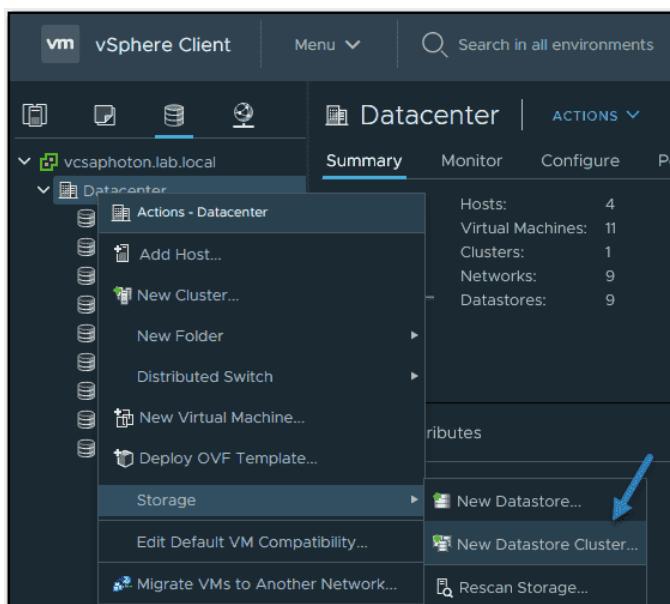
SDRS allows you to put a datastore into maintenance mode, allowing you to evacuate your VMDKs off to another datastore to enable decommissioning.

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.

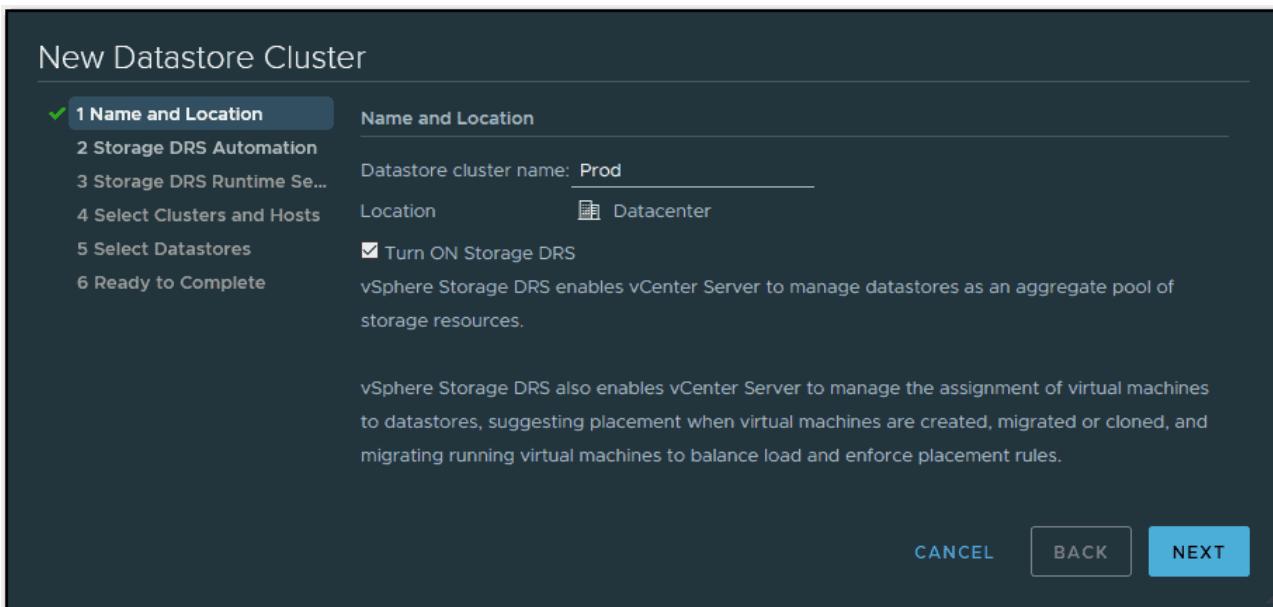
If you have some storage arrays that support hardware acceleration, you should not mix them with other arrays that don't have it. As a good practice, the datastore cluster should remain homogeneous.

## How to create new datastore clusters

You need to log in via your vSphere web client. Select the relevant datacenter object. Right-click it and select **Datacenter > Storage > 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](#)

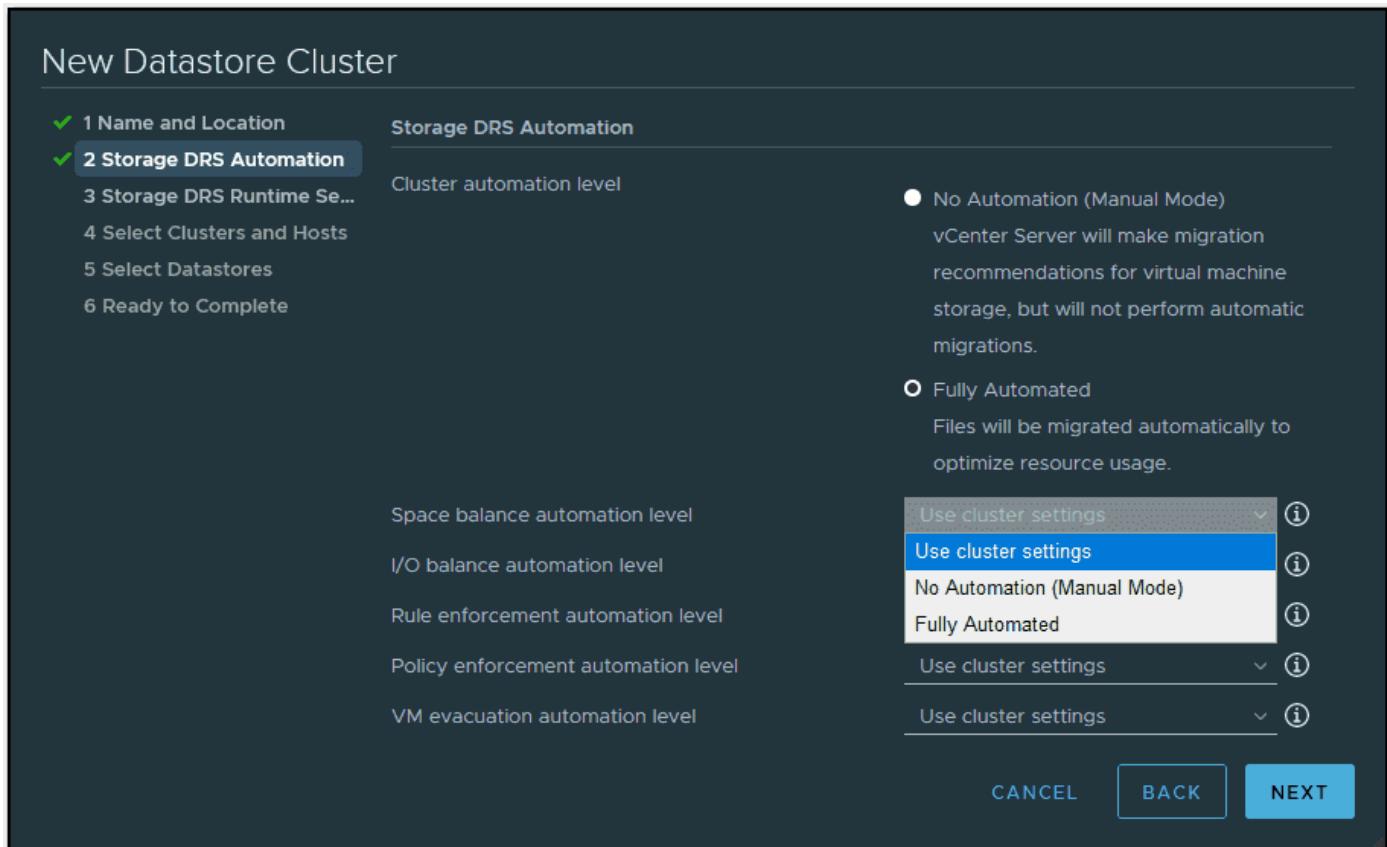
Then, on the next page, you can choose between *Fully Automated* or *No Automation (Manual mode)*.

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.

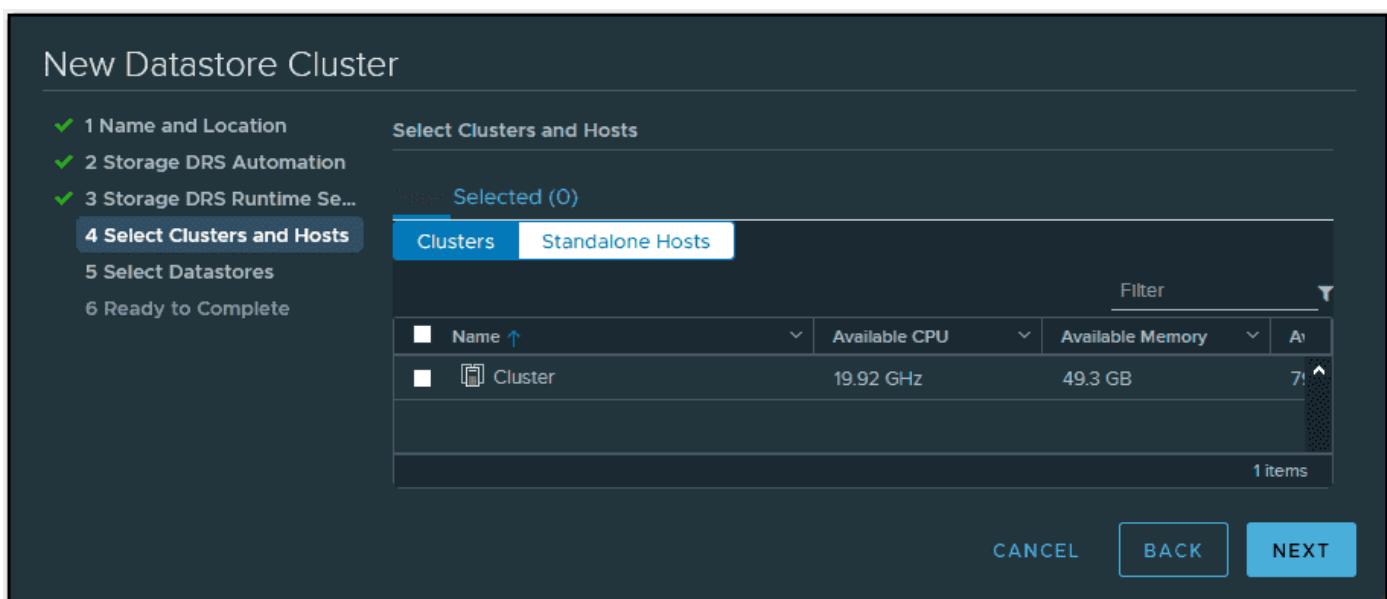
- **Space balance automation level** shows what to do when there is a recommendation to correct a space load imbalance in a datastore cluster.
- **I/O balance automation level** allows you to choose what happens when it generates recommendations for correcting an I/O load imbalance in a datastore cluster.
- **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.

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.

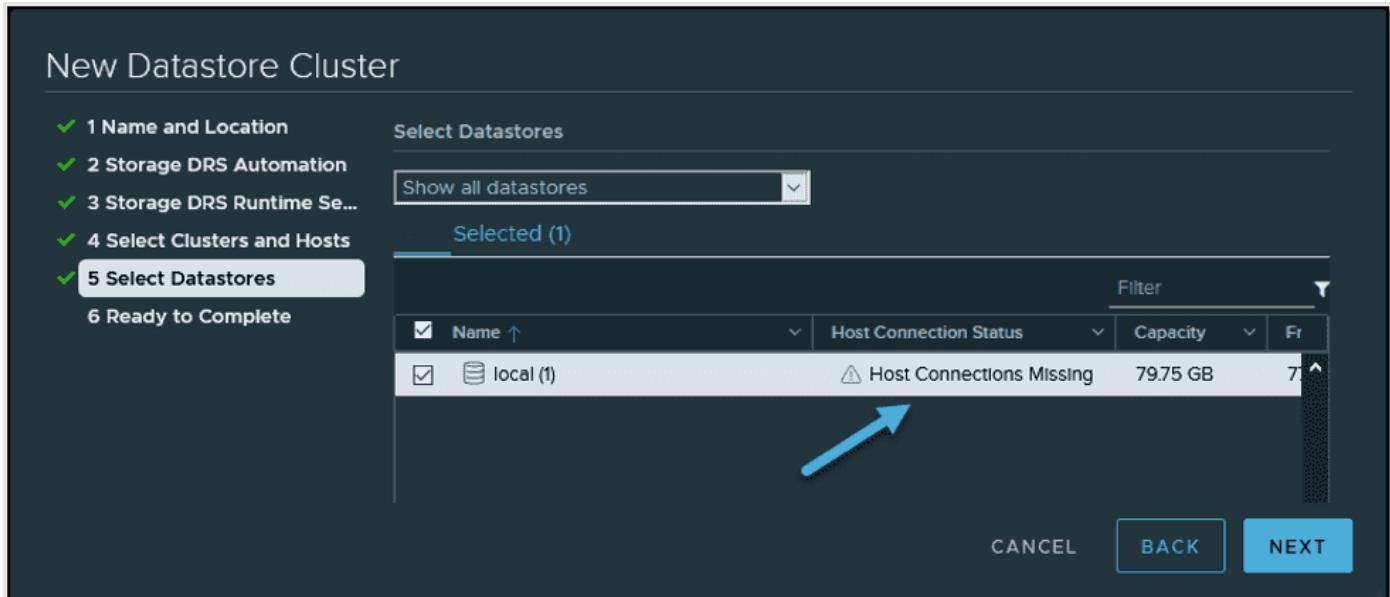
You can also set the I/O latency threshold and space threshold, such that you can set a minimum level of free space per datastore. Those settings allow you to migrate VMDKs from a datastore when the low space threshold kicks in.



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



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: *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 1.3.8 – Describe Storage I/O Control (SIOC)

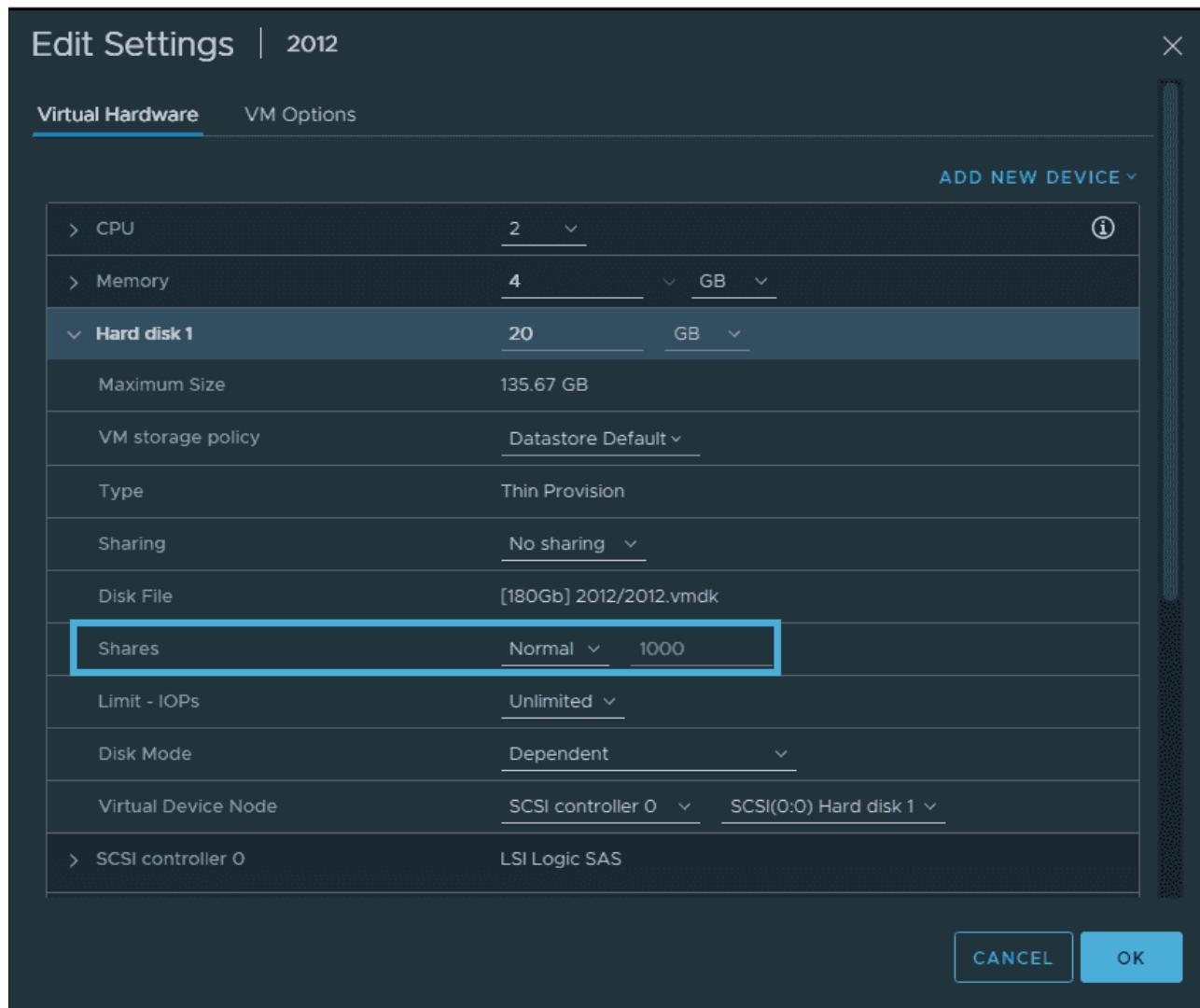
When managing and maintaining a VMware vSphere environment, keeping an eye on storage and storage I/O is extremely important. In most virtualization environments where shared SAN storage is in place, it is not uncommon to see storage I/O resources exhausted before CPU and, in many cases, memory are exhausted.

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 monitoring 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 (SIOC) 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 (it's not supported).

Some arrays might be using automated storage tiering, and 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

1. Connect to your vCenter Server via vSphere Client.
2. Browse to the **datastore** icon in vSphere Client.
3. Select **Configure > Datastore capabilities > Edit**.

The screenshot shows the vSphere Client interface for managing a datastore. The left sidebar lists tabs: Summary, Monitor, Configure (which is selected), Permissions, Files, Hosts, and VMs. Under the 'Configure' tab, there are sections for Alarm Definitions, Scheduled Tasks, General (selected), Device Backing, Connectivity and Multipathing, Hardware Acceleration, and Capability sets. The main panel displays the properties of the '180Gb' datastore, including its Name (180Gb), File system (VMFS 6.82), and Drive type (Flash). It also shows capacity details: Total Capacity (179.75 GB), Provisioned Space (545.16 GB), and Free Space (115.68 GB). The 'Datastore Capabilities' section is expanded, showing 'Thin Provisioning' is supported and 'Storage I/O Control' is disabled. A large blue arrow points downwards from the top of the page towards the 'Edit' button for 'Storage I/O Control'.

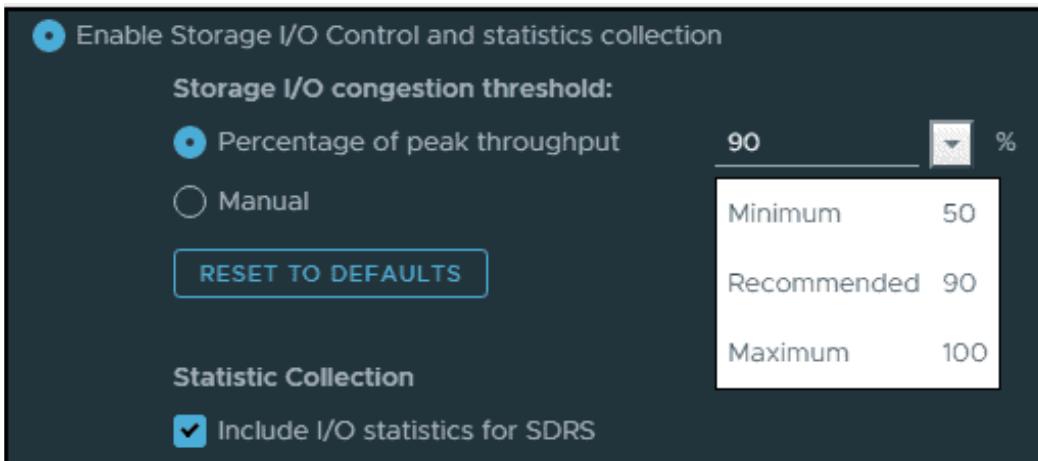
On the next screen, you'll see three radio buttons:

- **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.** Select this 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.



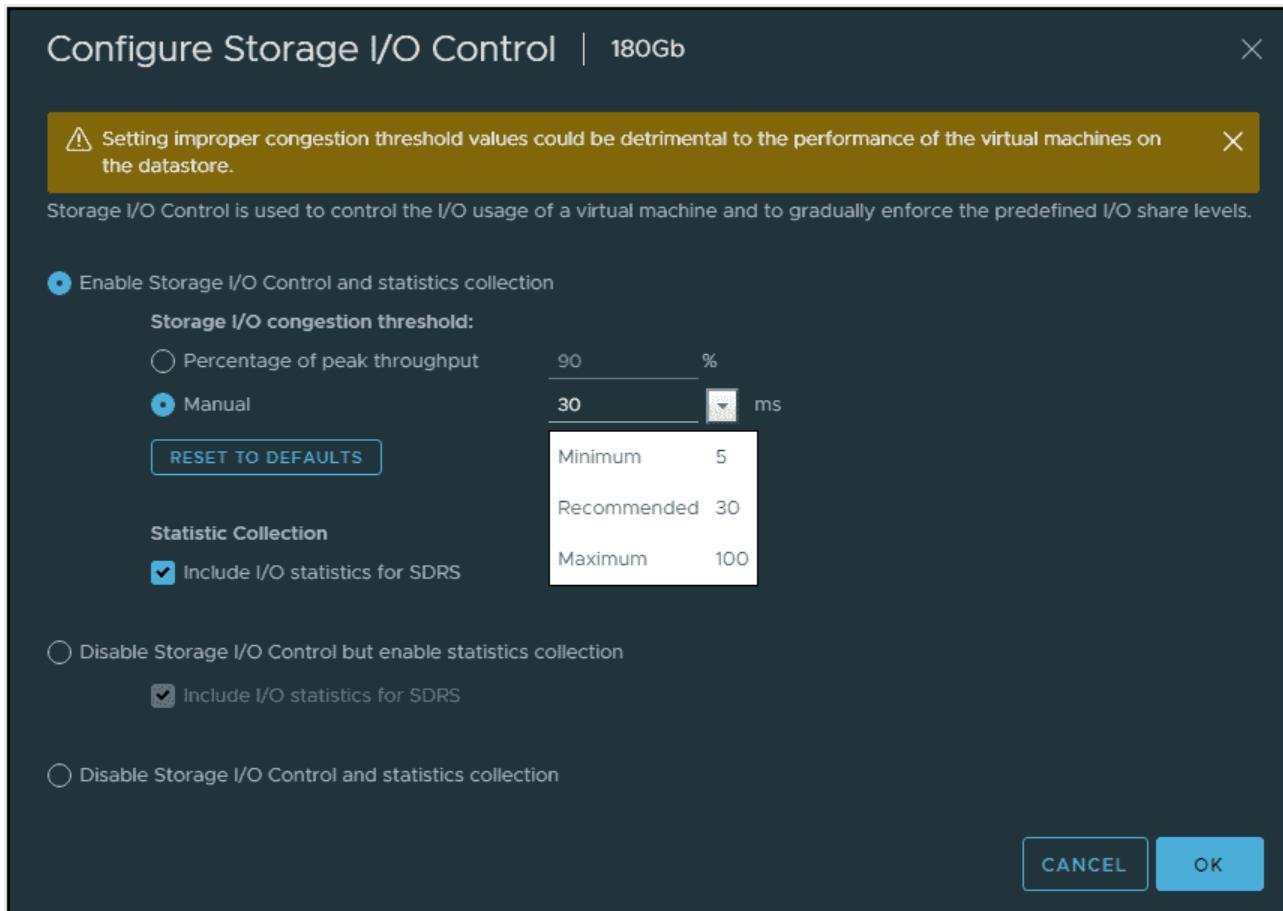
Adjust the percentage of peak thresholds if you like. The defaults are set to 90%, which is a recommended value, but there are other values you can choose from.



There is also the option to enter another number, but you'll get the 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 percentage points but in milliseconds (ms). When you click it, you see that you can choose from three different predefined 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 are using the correct values and that those values have not been modified. You should enter 30 ms, which is the recommended value.

To check VM shares/limits at the cluster level, navigate and select your **cluster > Monitor > Storage**. Then view the shares and shares value columns there.

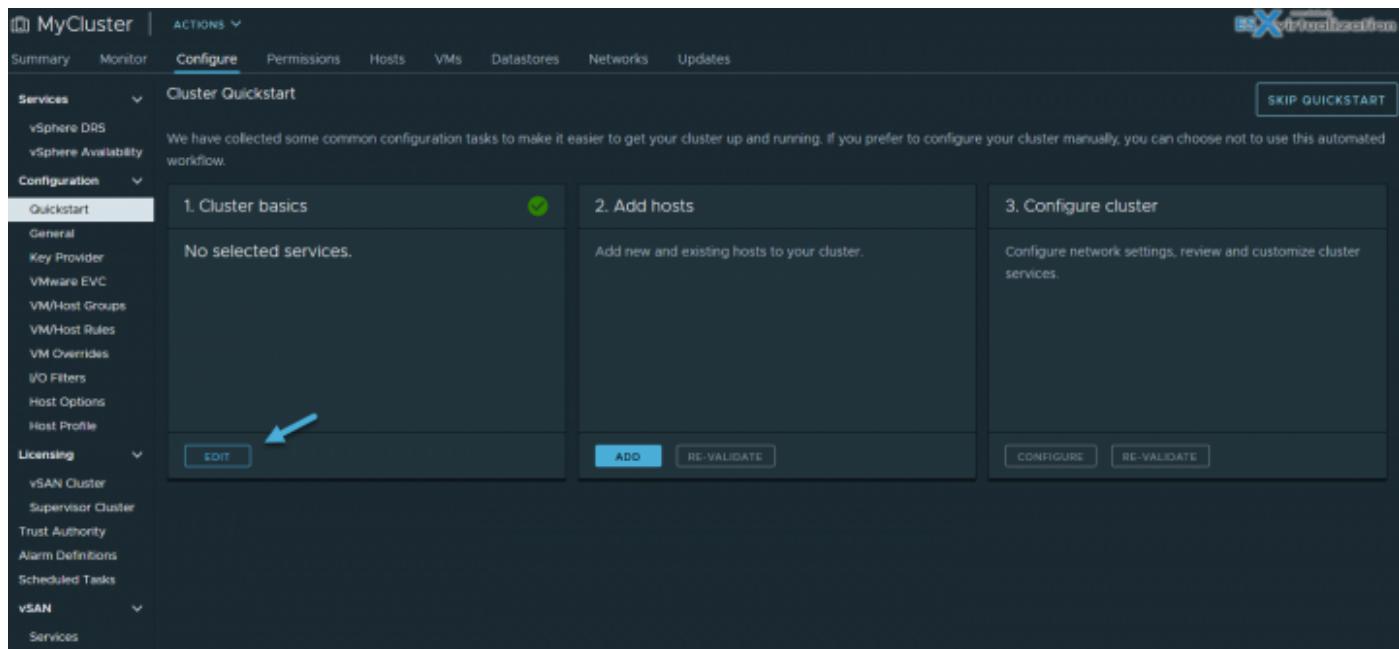
## Objective 1.4 – Describe VMware ESXi cluster concepts

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.

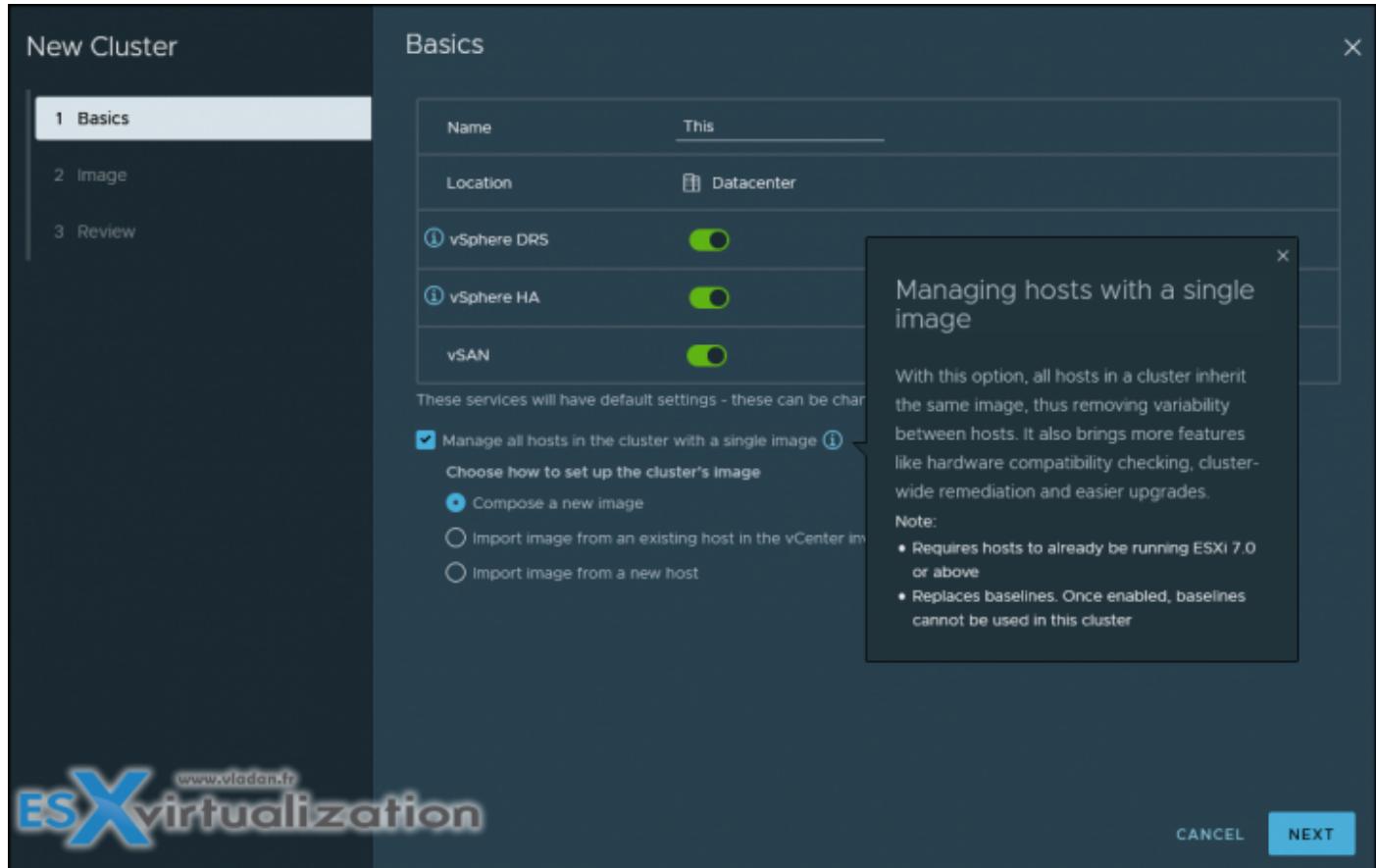
When enabled, VMware Enhanced vMotion Compatibility (EVC) can help you make sure that migrations with vMotion do not fail if the CPUs on different hosts within your cluster are not identical.

With DRS, you can allow automatic resource balancing by using the pooled resources within the cluster. With vSphere HA you basically prevent downtime if 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 needed to do anything.

With vSAN you can use the internal disks of each host and create a shared datastore for your VMs. A minimum of two hosts is 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 8. With this option, all hosts in a cluster use the same image, and this reduces variability between hosts and helps improve and ensure hardware compatibility. This also simplifies upgrades.



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. 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. 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 aims to determine whether the subordinate host is exchanging heartbeats with one of the datastores. See Datastore Heartbeating. Also, the master host checks whether the host responds to ICMP pings sent to its management IP addresses.

## Failures and responses

You can configure how vSphere HA responds to failure conditions on a cluster. There are 4 failure conditions:

- **Host** – allows you to configure host monitoring and failover on the cluster. (“**Disabled**” or “**Restart VMs**” – VMs will be restarted in the order determined by their restart priority).
- **Host Isolation** – allows you to configure the cluster to respond to host network isolation failures:
  - **Disabled** – No action will be taken on the affected VMs.
  - **Shut down and restart VMs** – All affected VMs will be gracefully 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.

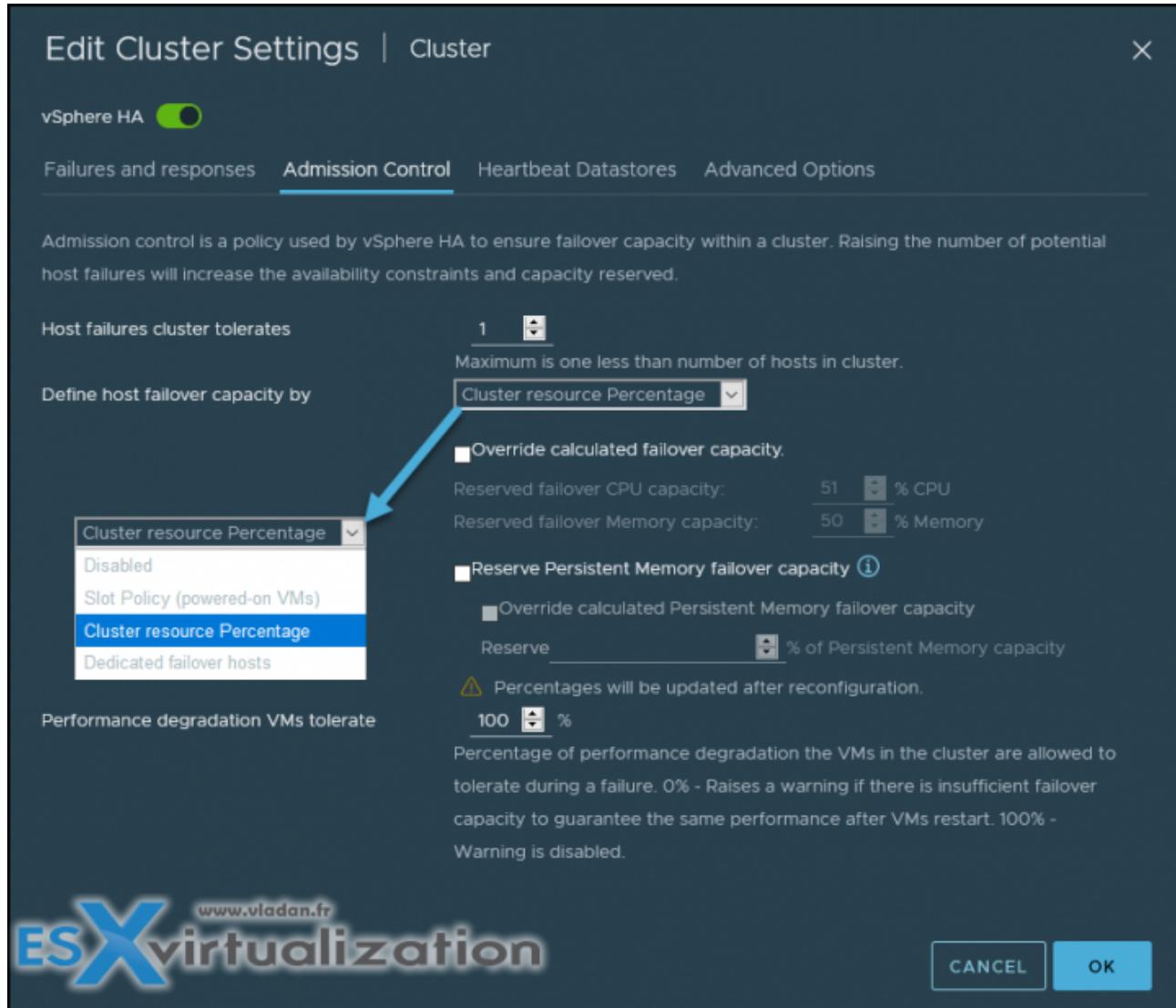
- **VM component protection** – datastore with Permanent Device Lost (PDL) and All Paths Down (APD):
  - **Datastore with PDL** – allows you to configure the cluster to respond to PDL datastore failures.
    - **Disabled** – No action will be taken to the affected VMs.
    - **Issue events** – No action 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 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 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 VM, but those would suffer from performance degradation. Now you have a warning message which informs you about it. You'll be warned if performance degradation would occur after an HA even for a particular VM(s):

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

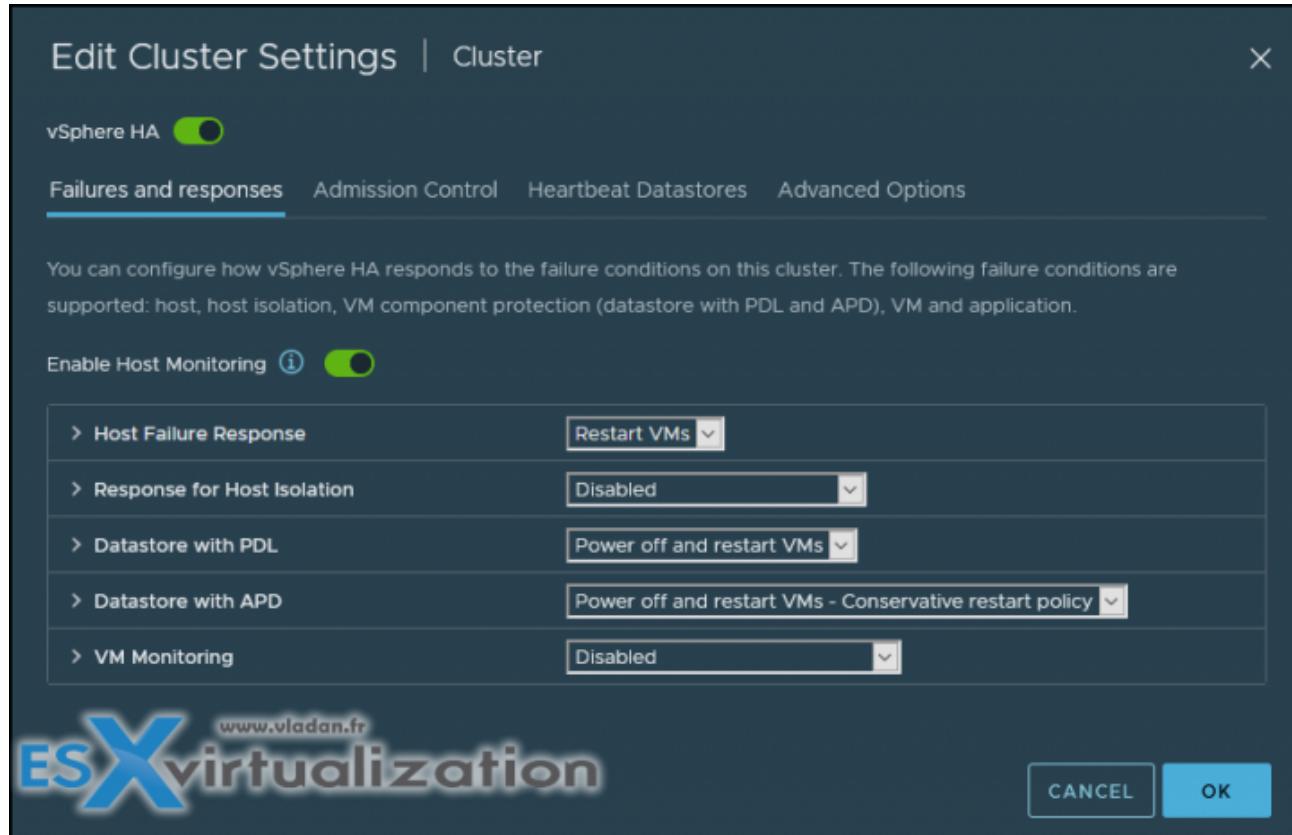


Other than cluster resource percentage policy there are “Slot policy” and “Dedicated failover host” policies.

- **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 > Edit**.

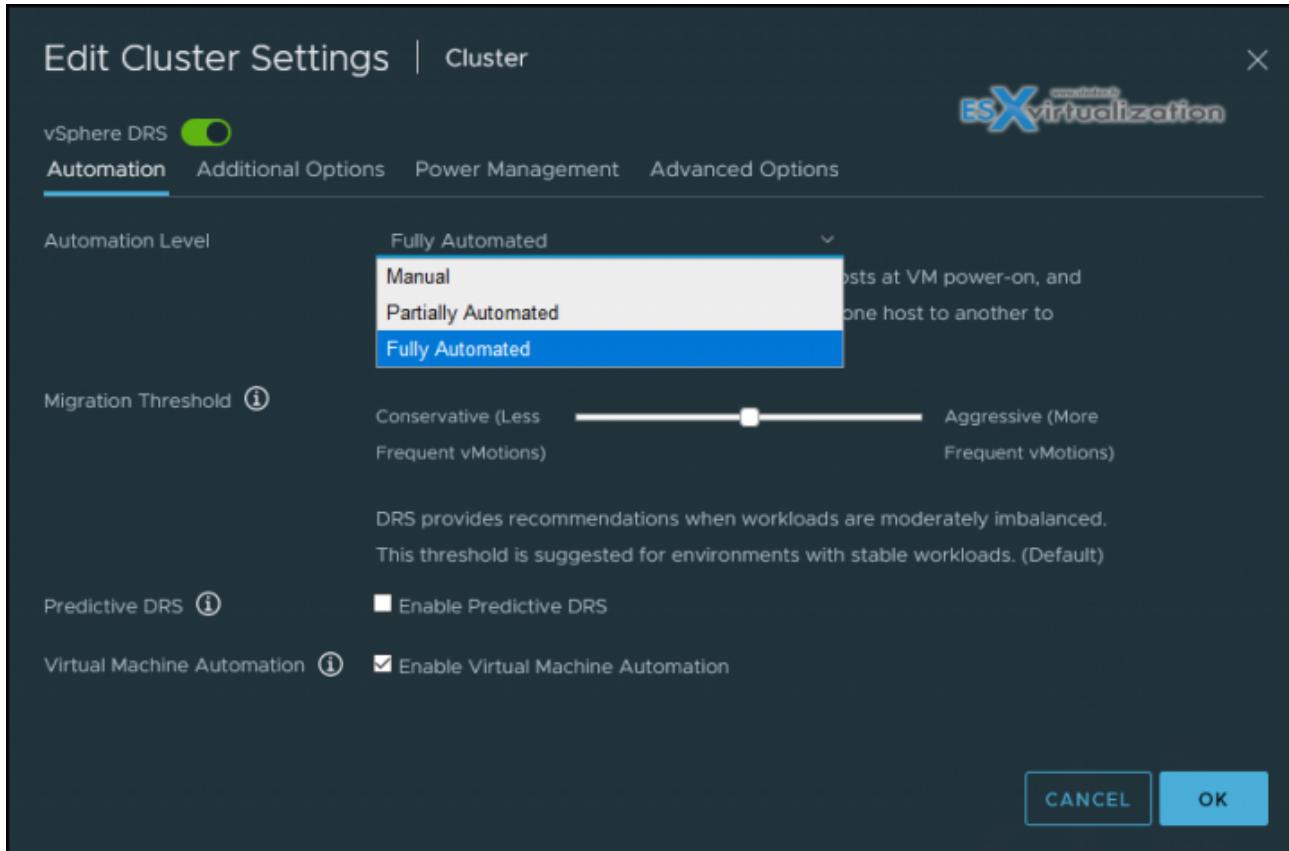


## Objective 1.4.1 – Describe VMware Distributed Resource Scheduler (DRS)

DRS runs once every minute rather than every 5 minutes, as was 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: Select your cluster > **Configure > vSphere DRS**. And you'll see the following 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

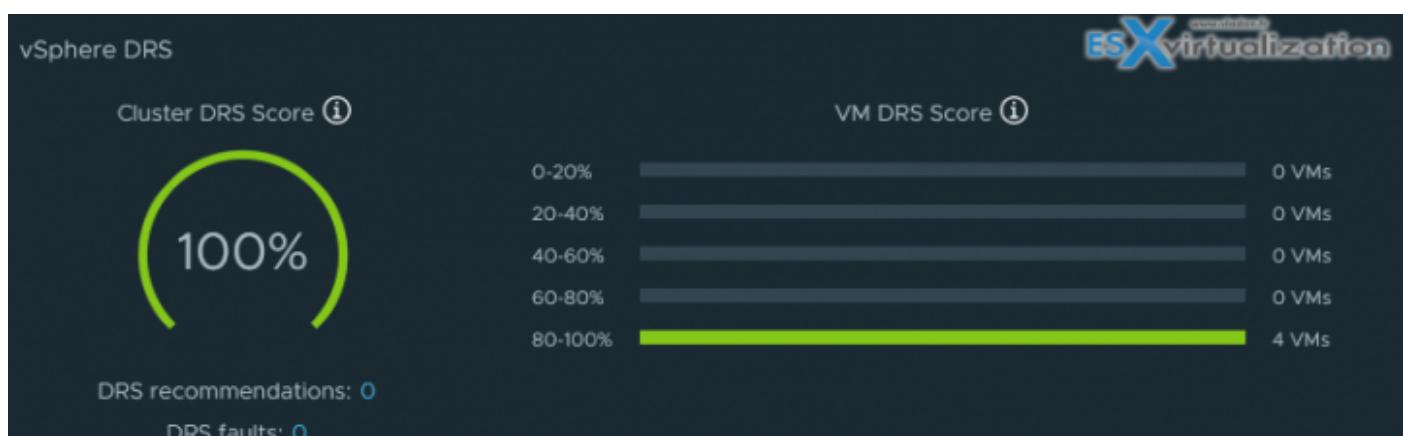
In addition to real-time metrics, DRS will respond to forecasted metrics provided by vRealize Operations Manager. Only forecasted metrics with high confidence will be considered by DRS to balance the cluster's workloads prior to predicted utilization spikes and resource contention. You must also configure 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 VM DRS Score

The VM DRS Score represents 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 accounts the costs for memory burstiness, memory reclamation, and memory tax. There are also network resources costs as well as utilization.

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**

See [VMware documentation on 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. These specify whether 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 two VMs on separate hosts, while another rule that puts them together. You need to select one of the rules to apply and disable or remove the rule that is in conflict.

## **Objective 1.4.2 – Describe vSphere Enhanced vMotion Compatibility (EVC)**

If you're an experienced VMware admin, you probably won't find anything here that you don't already know. VMware Enhanced vMotion Compatibility (EVC) is a vSphere cluster feature that 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.

vMotion usually fails when a VM runs on a host with a Haswell-based CPU and the destination host is a newer Broadwell-based CPU, for example. It is necessary to put in place VMware EVC first, and then vMotion can succeed.

A 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.*

Interestingly, by default, it is the 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

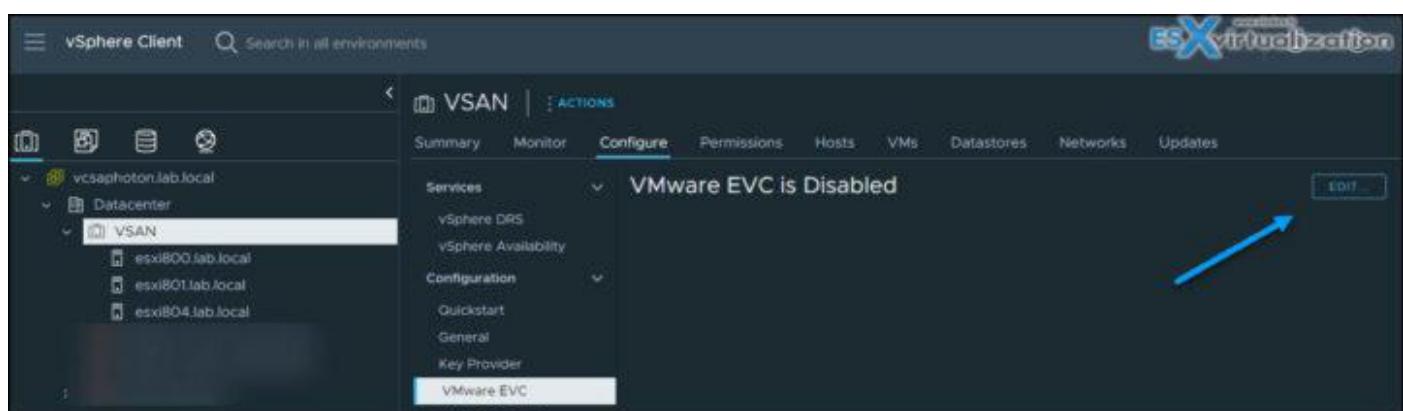
## Advantages of VMware Enhanced vMotion Compatibility (EVC)

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.

## Inconveniences and drawbacks

Usually, newer CPUs have newer sets of instructions and are more performant and efficient. Your applications may greatly benefit from using them. 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.

## Configuring VMware Enhanced vMotion Compatibility (EVC)



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

Disable EVC     Enable EVC for AMD Hosts     Enable EVC for Intel® Hosts

**CPU Mode**

AMD Opteron™ Generation 1

- AMD Opteron™ Generation 1
- AMD Opteron™ Generation 2
- AMD Opteron™ Gen. 3 (no 3DNow!™)
- AMD Opteron™ Generation 3
- AMD Opteron™ Generation 4
- AMD Opteron™ "Piledriver" Generation
- AMD Opteron™ "Steamroller" Generation
- AMD Zen Generation
- AMD Zen 2 Generation
- AMD Zen 3 Generation

**Description**

**CPU Mode**  
Applies the baseline feature set of AMD Opteron™ Generation 1 ("Rev. E") AMD Opteron™ Generation 2 ("Rev. F") AMD Opteron™ Generation 3 ("Greyhound") For more information, see Knowledge Base article 1003212.

**Graphics Mode (vSGA)**  
Applies the baseline feature set for graphics that includes features through D3D 10.1/OpenGL 3.3. This is compatible with the features provided by ESXi 7.0 (and earlier).

**Compatibility**

ⓘ The host's CPU hardware does not support the cluster's current Enhanced vMotion Compatibility mode. The host CPU lacks features required by that mode.  
 esxi800.lab.local  
 esxi801.lab.local  
 esxi802.lab.local

**CANCEL** **OK**

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**.

Disable EVC     Enable EVC for AMD Hosts     Enable EVC for Intel® Hosts

**CPU Mode**

Intel® "Merom" Generation

- Intel® "Merom" Generation
- Intel® "Penryn" Generation
- Intel® "Nehalem" Generation
- Intel® "Westmere" Generation
- Intel® "Sandy Bridge" Generation
- Intel® "Ivy Bridge" Generation
- Intel® "Haswell" Generation
- Intel® "Broadwell" Generation
- Intel® "Skylake" Generation
- Intel® "Cascade Lake" Generation
- Intel® "Ice Lake" Generation

**Description**

**CPU Mode**  
Applies the baseline feature set of Intel® "Merom" Generation (Xeon® Core™2) Intel® "Penryn" Generation (Xeon® Core™ i7) Intel® "Westmere" Generation (Xeon® 32nm Core™ i7) Intel® "Sandy Bridge" Generation Intel® "Ivy Bridge" Generation Intel® "Haswell" Generation Intel® "Broadwell" Generation Intel® "Skylake" Generation Future Intel® processors For more information, see Knowledge Base article 1003212.

**CANCEL** **OK**

Think of EVC as a “layer” which 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.

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'll 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 modes 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>

The screenshot shows the VMware Compatibility Guide search interface. At the top, there's a search bar with placeholder text '(e.g. compatibility or esx or 3.0)', a dropdown for 'All Listings', and a 'Search' button. Below the search bar, there's a link 'Looking for a simplified search? Use the Guided Search Wizard'. The main area has four sections: 'What are you looking for: CPU Series', 'Product Release Version' (set to 'ESXi 6.5'), 'CPU Capabilities' (set to 'Supports SMP-FT, Capable of Legacy FT, ALL CPUs'), and 'Compatibility Guides' (dropdown). Below these are three lists: 'Enhanced vMotion Capability Modes' (including All, AMD Opteron™ Generation 1, etc.), 'Fault Tolerant Compatible Sets' (including All, AMD Bulldozer Generation, etc.), and a table titled 'CPU / EVC Matrix'. The 'CPU / EVC 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 CPU Series (Intel Xeon E5-2400-v2 Series, Intel Xeon E5-2600-v3 Series). The 'CPU / EVC Matrix' button is highlighted with a blue arrow. The bottom right corner features the 'ESX virtualization' logo.

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 that are able to use vMotion operations within hosts with different types of CPUs (Intel or AMD, not boths).

## Objective 1.4.3 – Describe how DRS scores virtual machines

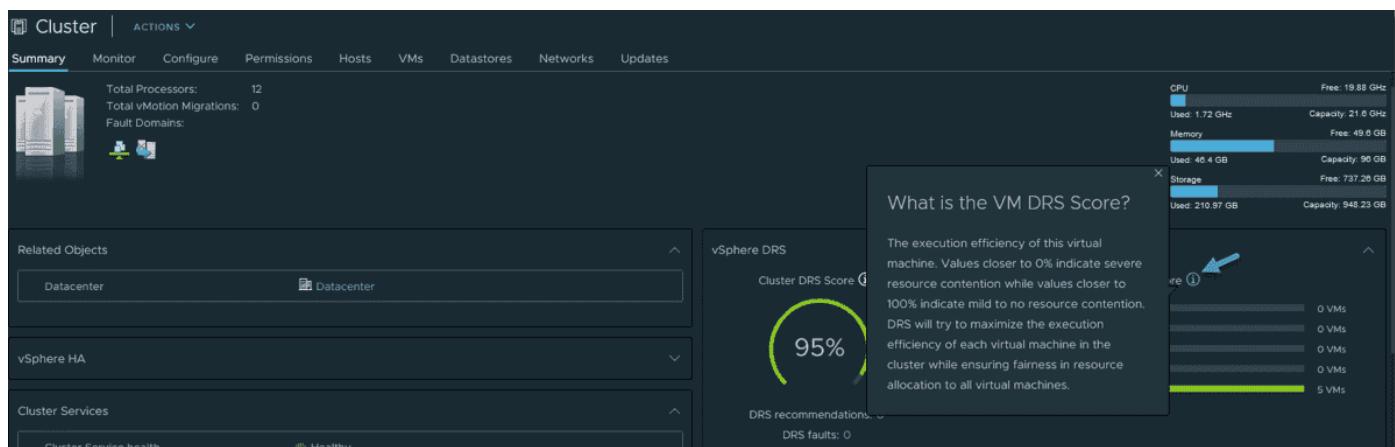
Based on the score of each VM running on a particular host, the DRS can move the VM to another host where the score might be better and the workload would be “happier”. Yes, the workload’s actual happiness, meaning that the workloads can consume the resources they are entitled to.

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 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.



### 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 behavior. It uses goodness modeling, 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.

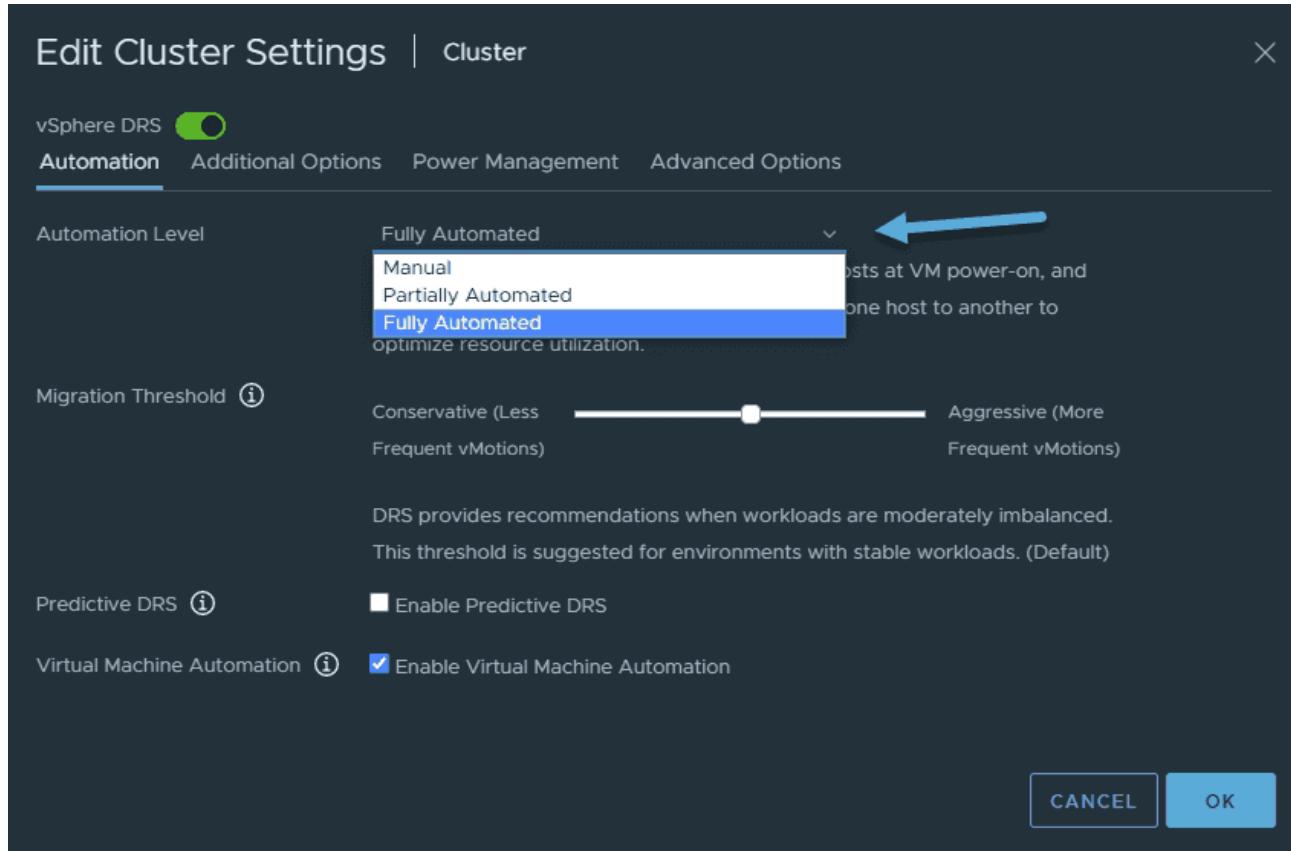
You may not know this, but vMotion can be an «expensive» operation, depending on how many VM memory pages have to be copied to the destination host. vMotion usually consumes a large amount of CPU, memory, and network resources. And don't forget, this is on both the source and destination hosts.

**Note:** After you migrate from vSphere 6.x to vSphere 8, you might see more vMotion operations due to the new DRS behavior.

## vSphere DRS configuration

The three different vSphere DRS automation levels look the same in vSphere 8, 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.

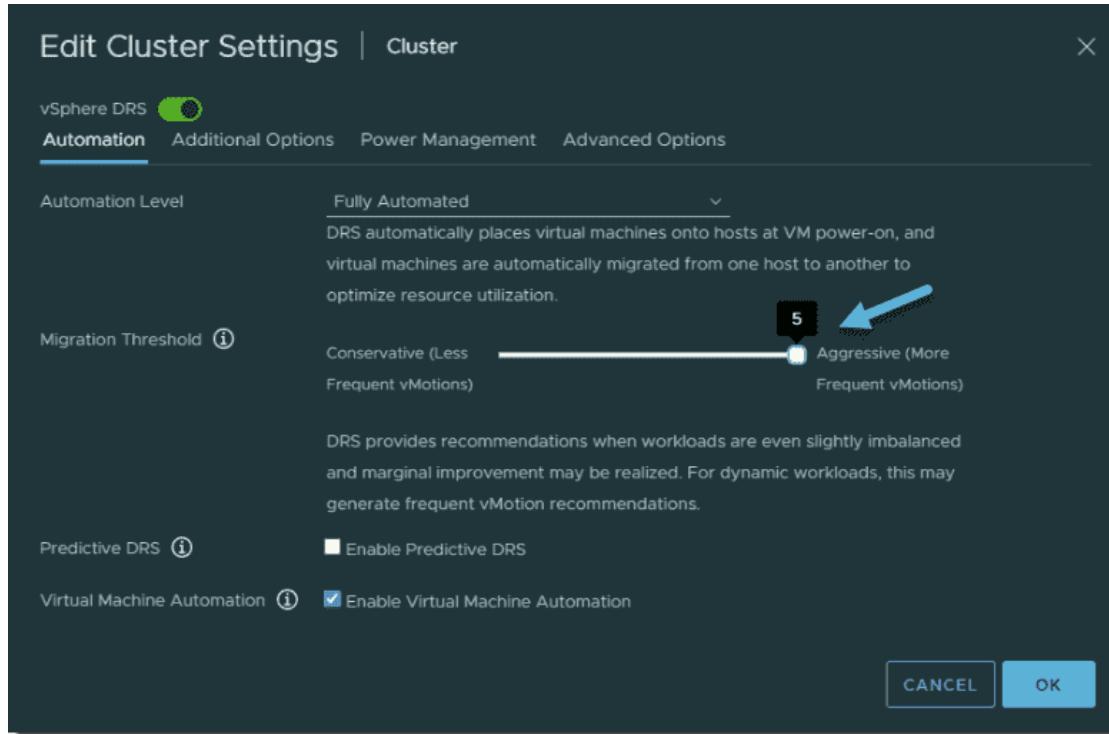


vSphere DRS automation levels

## 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.

1. 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.
2. The DRS only gives recommendations when workloads are extremely imbalanced or virtual machine demand is not being satisfied on the current host.
3. Default—The DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads.
4. The DRS provides recommendations when workloads are fairly imbalanced. This threshold is suggested for environments with bursty workloads.
5. 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.



## 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.

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

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.

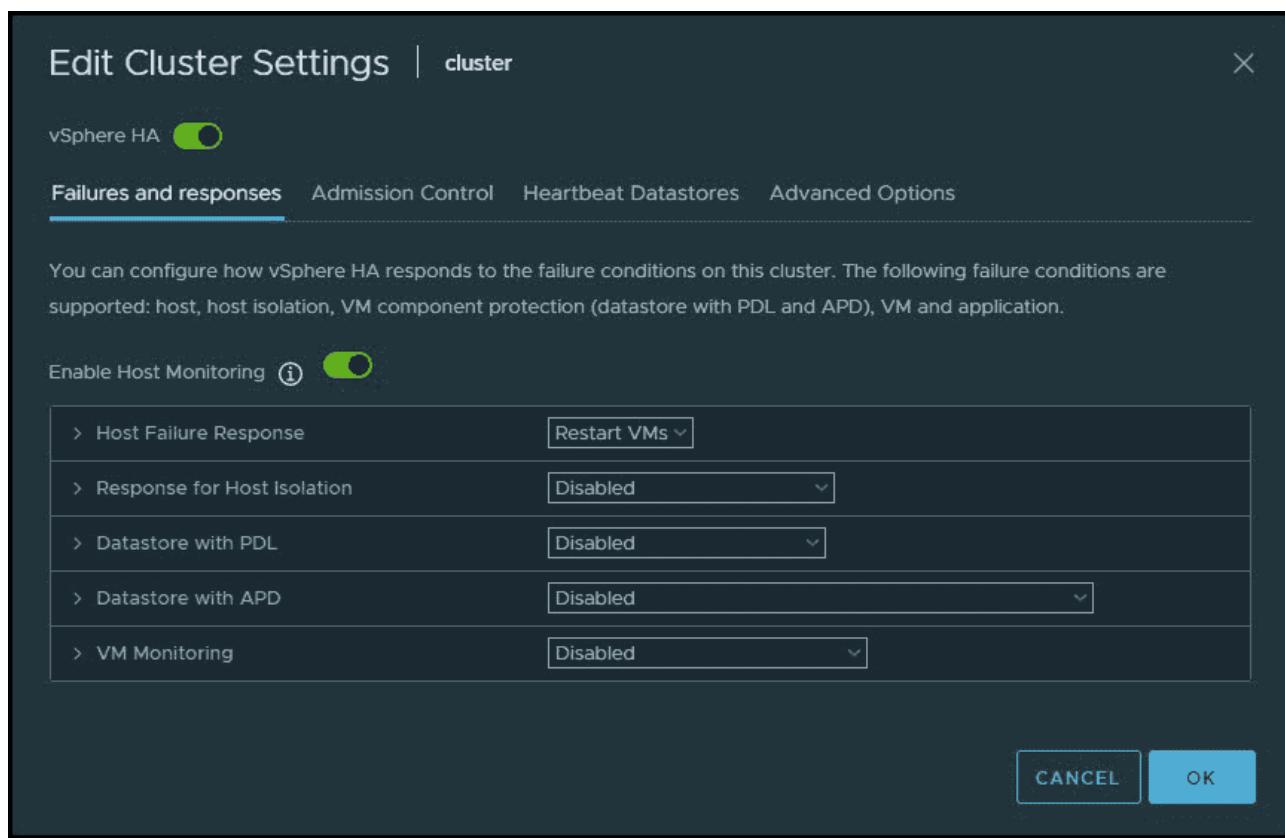
## Objective 1.4.4 - Describe VMware vSphere High Availability (HA)

### 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.



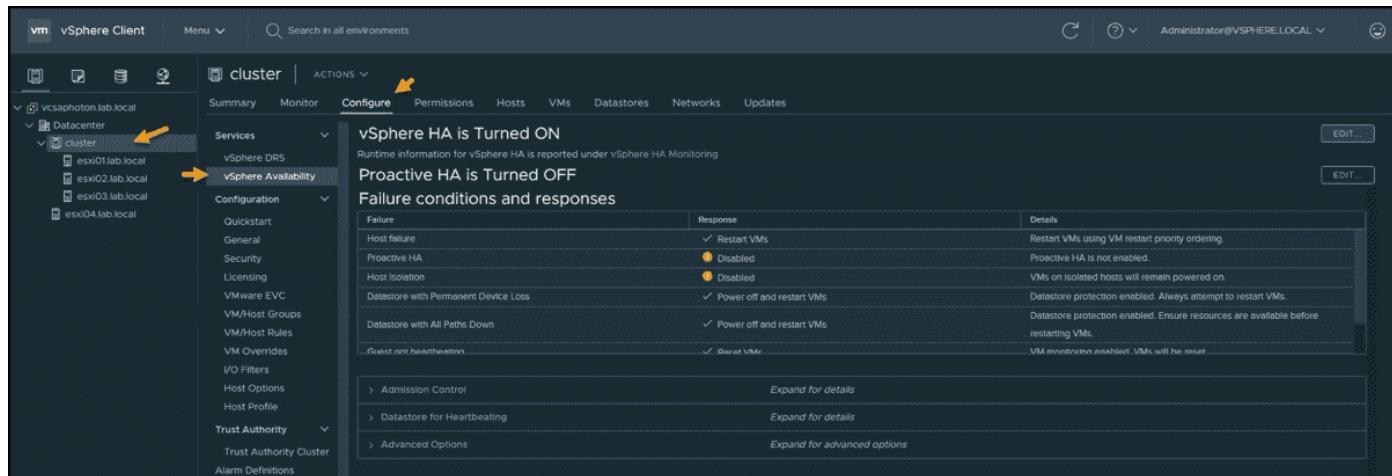
VMware vSphere HA Edit cluster settings

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**.



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.

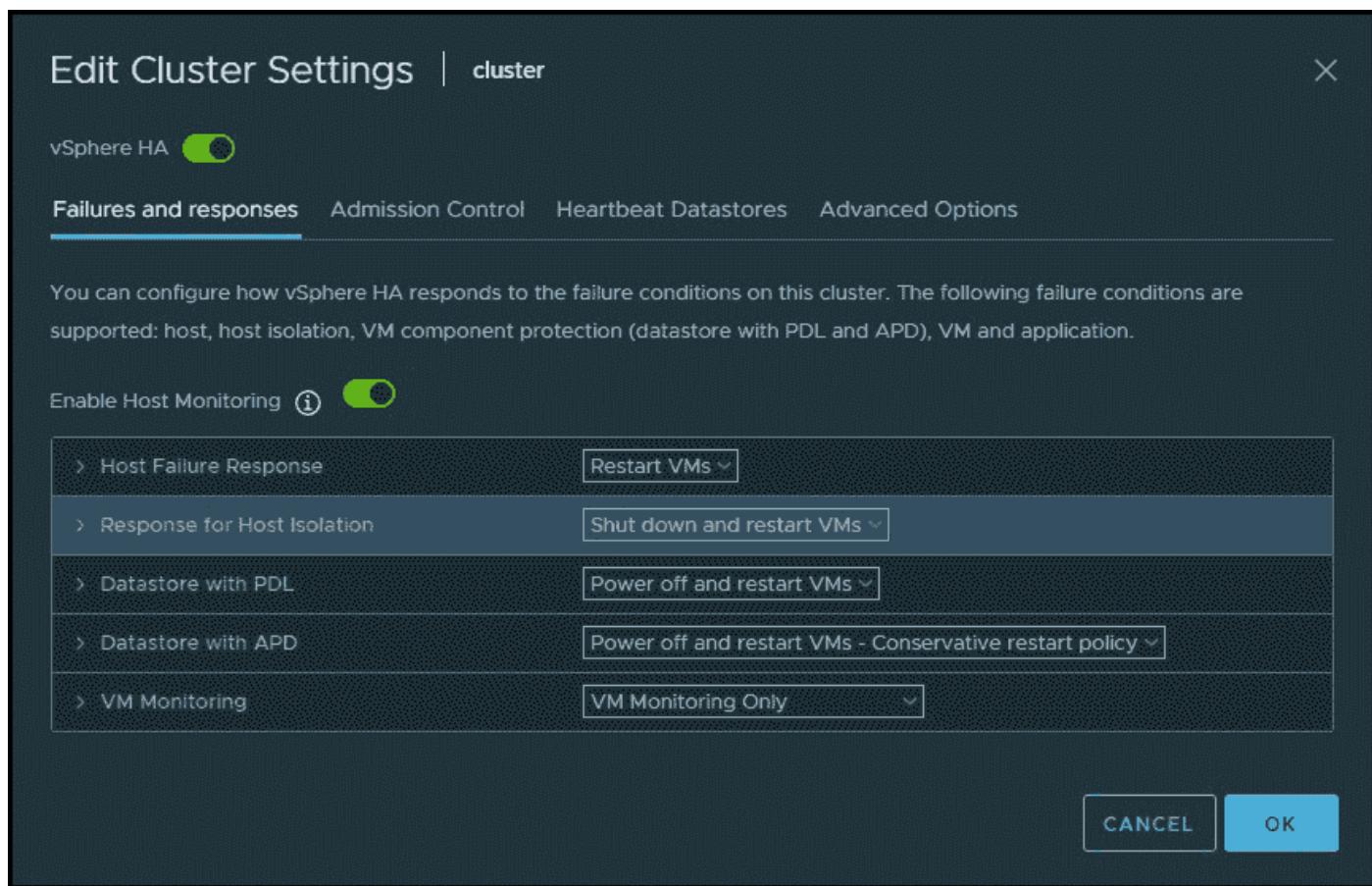
## vSphere high availability (HA) host failures

**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.

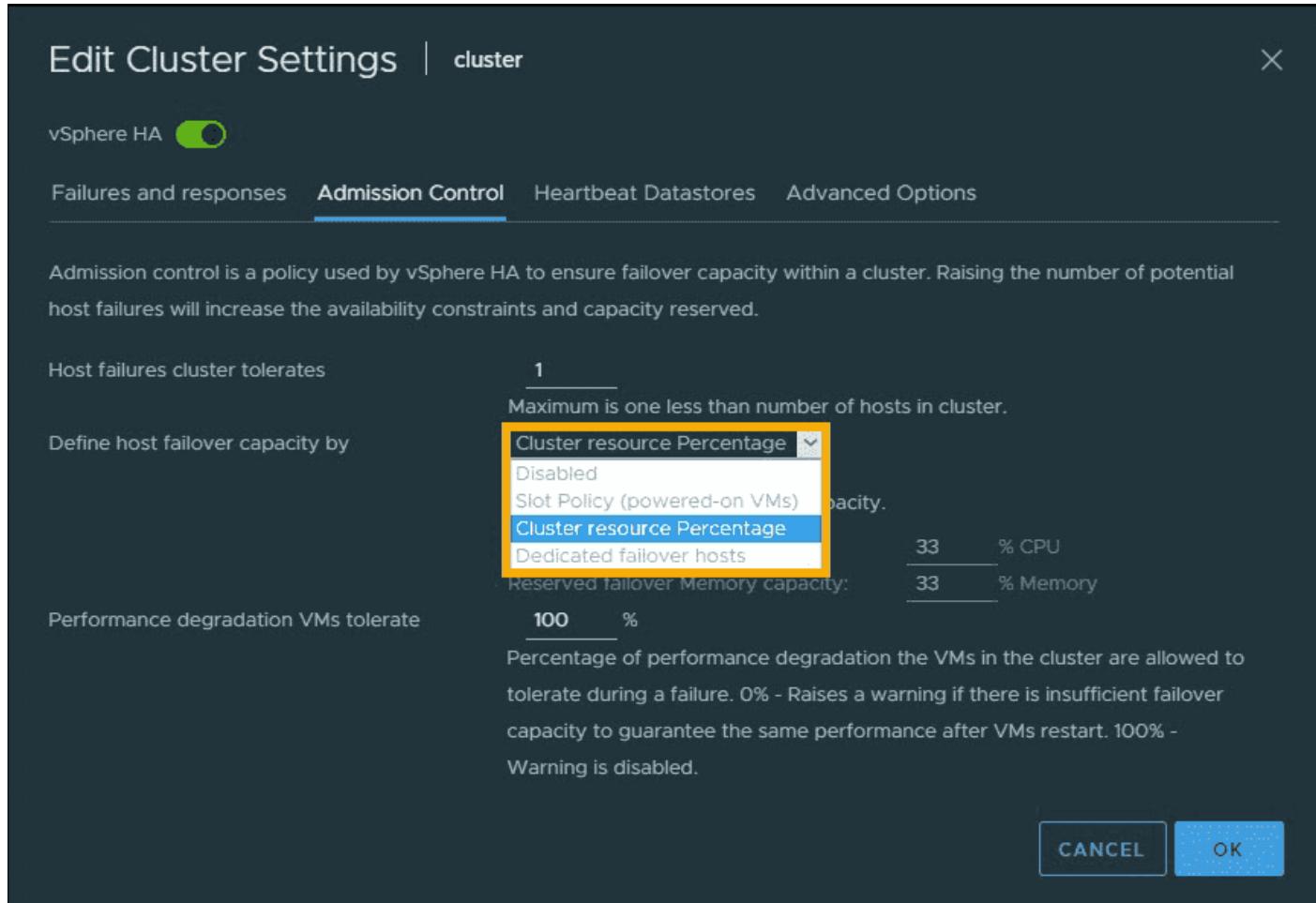
**Partition**—The host loses network connectivity with the primary host but is still connected to other secondary hosts.

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 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 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.



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.

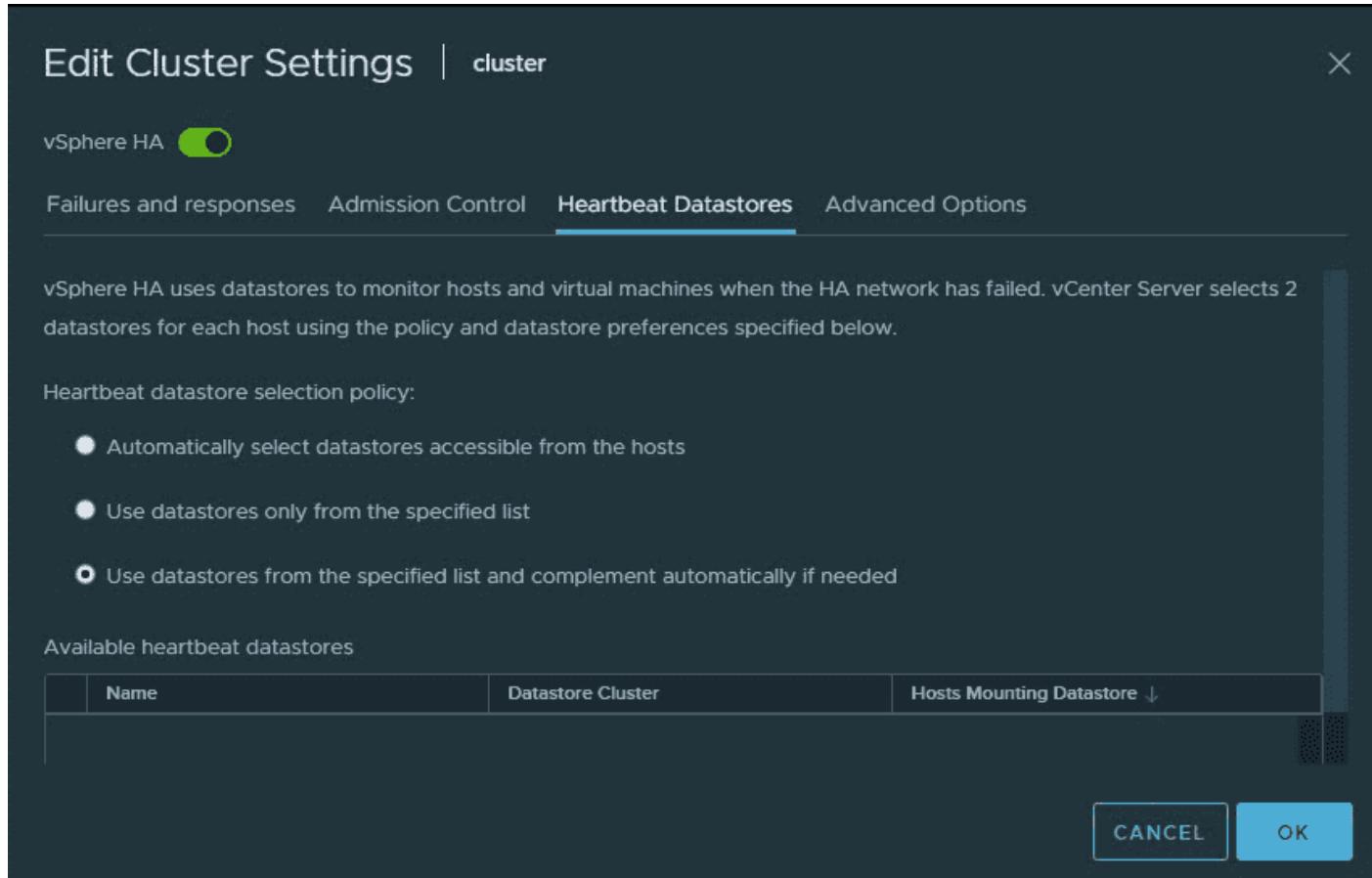
**Slot policy admission control**—vSphere HA admission control makes sure that host(s) can fail and there are still sufficient resources in the cluster to failover all the VMs from those hosts.

**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](#)  
[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 1.4.5 - Identify use cases for fault tolerance

VMware Fault Tolerance (FT) is a very emblematic feature which provides an ultimate VM protection **without any downtime** for the application(s) running within the VM. You can lose the underlying host, but the VM which runs with her identical copy on another, host, is fully resilient.

When a Secondary VM is called upon to replace its Primary VM because of a failure, the Secondary VM immediately takes over the Primary VM's role with the entire state of the virtual machine preserved. Applications are already running, and data stored in memory does not need to be reentered or reloaded. Failover provided by vSphere HA restarts the virtual machines affected by a failure.

The protected virtual machine is called the Primary VM. The duplicate virtual machine, the Secondary VM, is created and runs on another host. The primary VM is continuously

replicated to the secondary VM so that the secondary VM can take over at any point, thereby providing Fault Tolerant protection.

The Primary and Secondary VMs continuously monitor the status of one another to ensure that Fault Tolerance is maintained. A transparent failover occurs if the host running the Primary VM fails, or encounters an uncorrectable hardware error in the memory of the Primary VM, in which case the Secondary VM is immediately activated to replace the Primary VM. A new Secondary VM is started and Fault Tolerance redundancy is reestablished automatically. If the host running the Secondary VM fails, it is also immediately replaced. In either case, users experience **no interruption in service and no loss of data**.

A fault tolerant virtual machine and its secondary copy are not allowed to run on the same host. This restriction ensures that a host failure cannot result in the loss of both VMs.

Applications which must always be available, especially applications that have long-lasting client connections that users want to maintain during hardware failure.

- **Custom Apps** – Custom applications that have no other way of doing clustering.
- **Too complicated solutions** – Cases where high availability might be provided through custom clustering solutions, which are too complicated to configure and maintain.
- **On-Demand FT** – Another key use case for protecting a virtual machine with Fault Tolerance can be described as On-Demand Fault Tolerance. In this case, a virtual machine is adequately protected with vSphere HA during normal operation. During certain critical periods, you might want to enhance the protection of the virtual machine. For example, you might be running a quarter-end report which, if interrupted, might delay the availability of critical information. With vSphere Fault Tolerance, you can protect this virtual machine before running this report and then turn off or suspend Fault Tolerance after the report has been produced. You can use On-Demand Fault Tolerance to protect the virtual machine during a critical time period and return the resources to normal during non-critical operation.

## Limits of FT

In a cluster configured to use Fault Tolerance, two limits are enforced independently.

### *das.maxftvmsperhost*

The maximum number of fault tolerant VMs allowed on a host in the cluster. The default value is 4. There is no FT VMs per host maximum, you can use larger numbers if the workload performs well in FT VMs. You can deactivate checking by setting the value to 0.

### *das.maxftvcpusperhost*

The maximum number of vCPUs aggregated across all fault tolerant VMs on a host. The default value is 8. There is no FT vCPU per host maximum, you can use larger numbers if the workload performs well. You can deactivate checking by setting the value to 0.

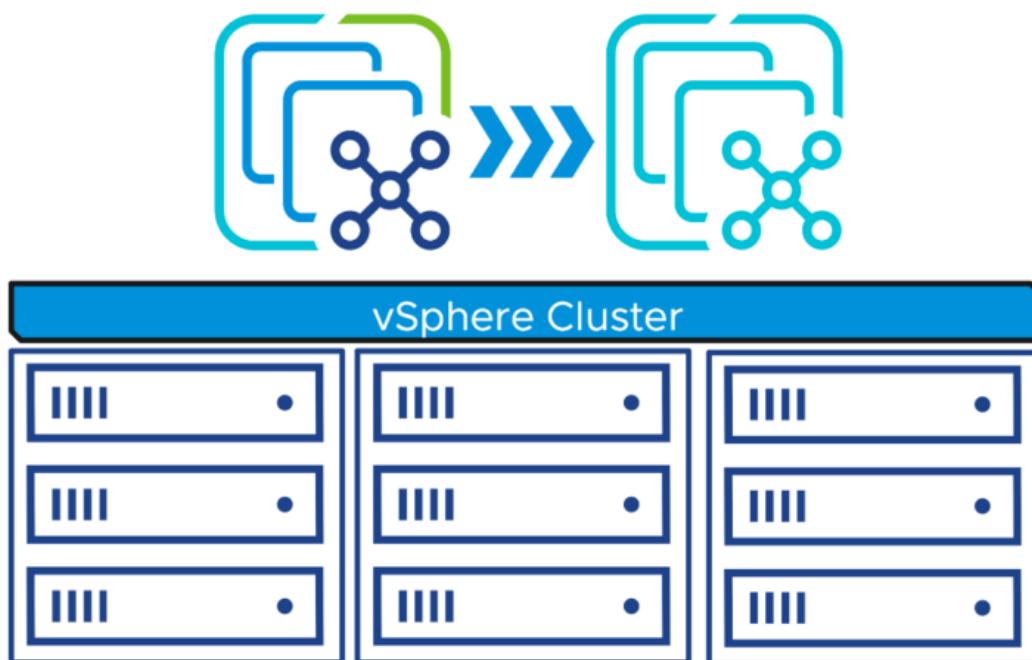
## Licensing

The number of vCPUs supported by a single fault tolerant VM is limited by the level of licensing that you have purchased for vSphere. Fault Tolerance is supported as follows:

- vSphere Standard and Enterprise. Allows up to 2 vCPUs
- vSphere Enterprise Plus. Allows up to 8 vCPUs

vSphere FT requires a 10-Gbit network between ESXi hosts in the cluster, a dedicated 10-Gbit network exclusively for FT is recommended. vSphere FT supports up to 8 vCPUs on a single VM, which means vCenter Server instances of size Large or greater cannot be protected using vSphere FT.

## Screenshot from VMware



## Unsupported Features of FT

I thought it might be interesting to add which features are not supported with VMware FT.

- **Snapshots** – Snapshots must be removed or committed before Fault Tolerance can be enabled on a virtual machine. In addition, it is not possible to take snapshots of virtual machines on which Fault Tolerance is enabled.
- Note: Disk-only snapshots created for vStorage APIs – Data Protection (VADP) backups are supported with Fault Tolerance. However, legacy FT does not support VADP.

- **Storage vMotion** – You cannot invoke Storage vMotion for virtual machines with Fault Tolerance turned on. To migrate the storage, you should temporarily turn off Fault Tolerance, and perform the storage vMotion action. When this is complete, you can turn Fault Tolerance back on.
- **Linked clones** – You cannot use Fault Tolerance on a virtual machine that is a linked clone, nor can you create a linked clone from an FT-enabled virtual machine. Virtual Volume datastores.
- **Storage-based policy management** – Storage policies are supported for vSAN storage.
- I/O filters.
- TPM.
- VBS enabled VMs.

Some Fault Tolerance configuration and failover issues

How to resolve FT problems.

- **Hardware Virtualization Not Enabled** – You must enable Hardware Virtualization (HV) before you use vSphere Fault Tolerance.
- **Compatible Hosts Not Available for Secondary VM** – If you power on a virtual machine with Fault Tolerance enabled and no compatible hosts are available for its Secondary VM, you might receive an error message.
- **Secondary VM on Overcommitted Host Degrades Performance of Primary VM** – If a Primary VM appears to be executing slowly, even though its host is lightly loaded and retains idle CPU time, check the host where the Secondary VM is running to see if it is heavily loaded.
- **Increased Network Latency Observed in FT Virtual Machines** – If your FT network is not optimally configured, you might experience latency problems with the FT VMs.
- **Some Hosts Are Overloaded with FT Virtual Machines** – You might encounter performance problems if your cluster's hosts have an imbalanced distribution of FT VMs.
- **Losing Access to FT Metadata Datastore** – Access to the Fault Tolerance metadata datastore is essential for the proper functioning of an FT VM. Loss of this access can cause a variety of problems.
- **Turning On vSphere FT for Powered-On VM Fails** – If you try to turn on vSphere Fault Tolerance for a powered-on VM, this operation can fail.
- **FT Virtual Machines not Placed or Evacuated by vSphere DRS** – FT virtual machines in a cluster that is enabled with vSphere DRS do not function correctly if Enhanced vMotion Compatibility (EVC) is currently disabled.

- **Fault-Tolerant Virtual Machine Failovers** – A Primary or Secondary VM can fail over even though its ESXi host has not crashed. In such cases, virtual machine execution is not interrupted, but redundancy is temporarily lost. To avoid this type of failover, be aware of some of the situations when it can occur and take steps to avoid them.

## Objective 1.5 - Explain the difference between VMware standard switches and distributed switches

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

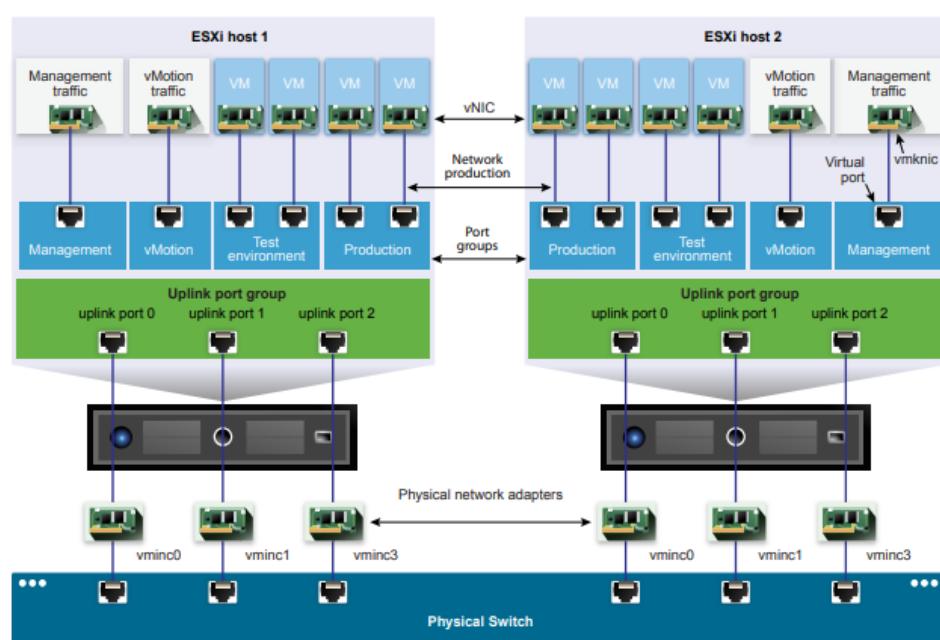
When it is connected to the physical switch using a physical Ethernet adapter also called uplink, you can have a connection between your virtual infrastructure and the physical (outside) world.

### vSphere Standard Switch (VSS)

It works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. A vSphere standard switch can be connected to physical switches by using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks.

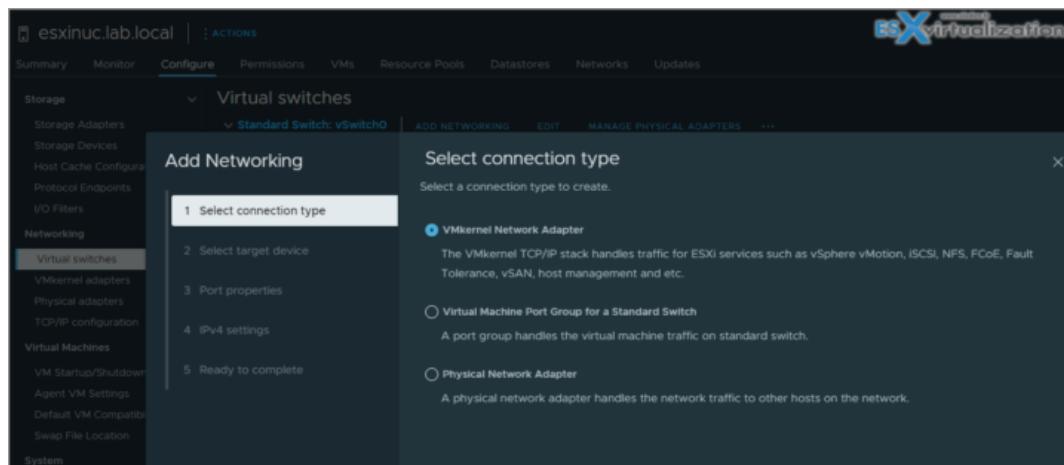
This type of connection is similar to connecting physical switches together to create a larger network. Even though a vSphere standard switch works much like a physical switch, it does not have some of the advanced functionality of a physical switch.

**Figure 2-1. vSphere Standard Switch architecture**



## How to create a standard vSwitch?

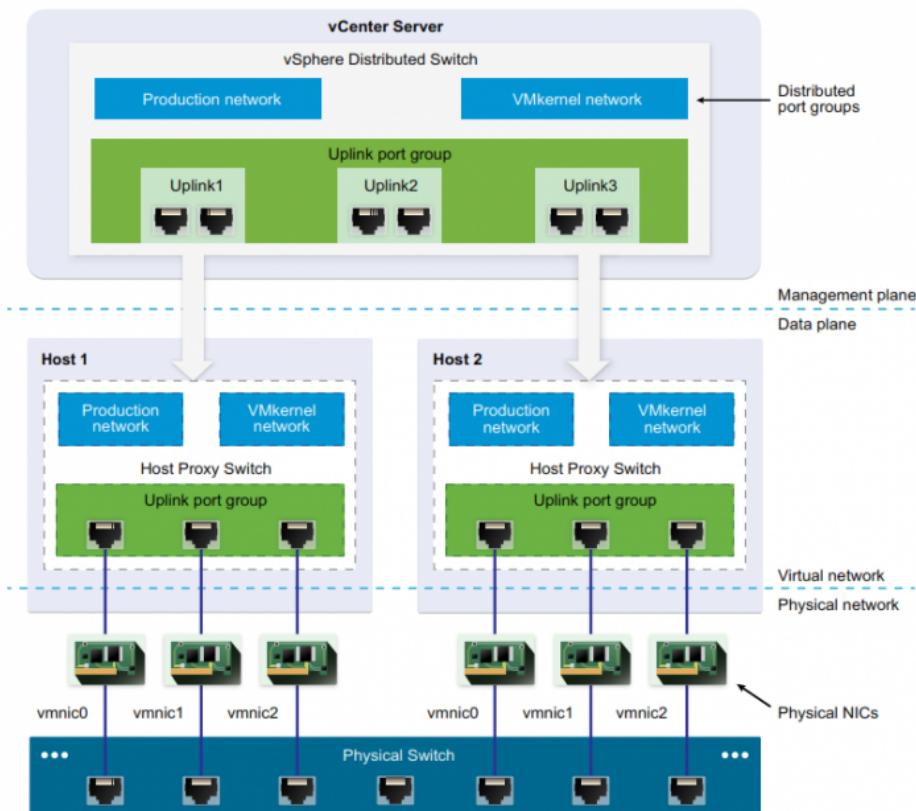
Select Host > Configure > Networking > Virtual Switches > Add. At the same time, the assistant proposes you to create either VMkernel network adapter, VM port group or Physical network adapter.



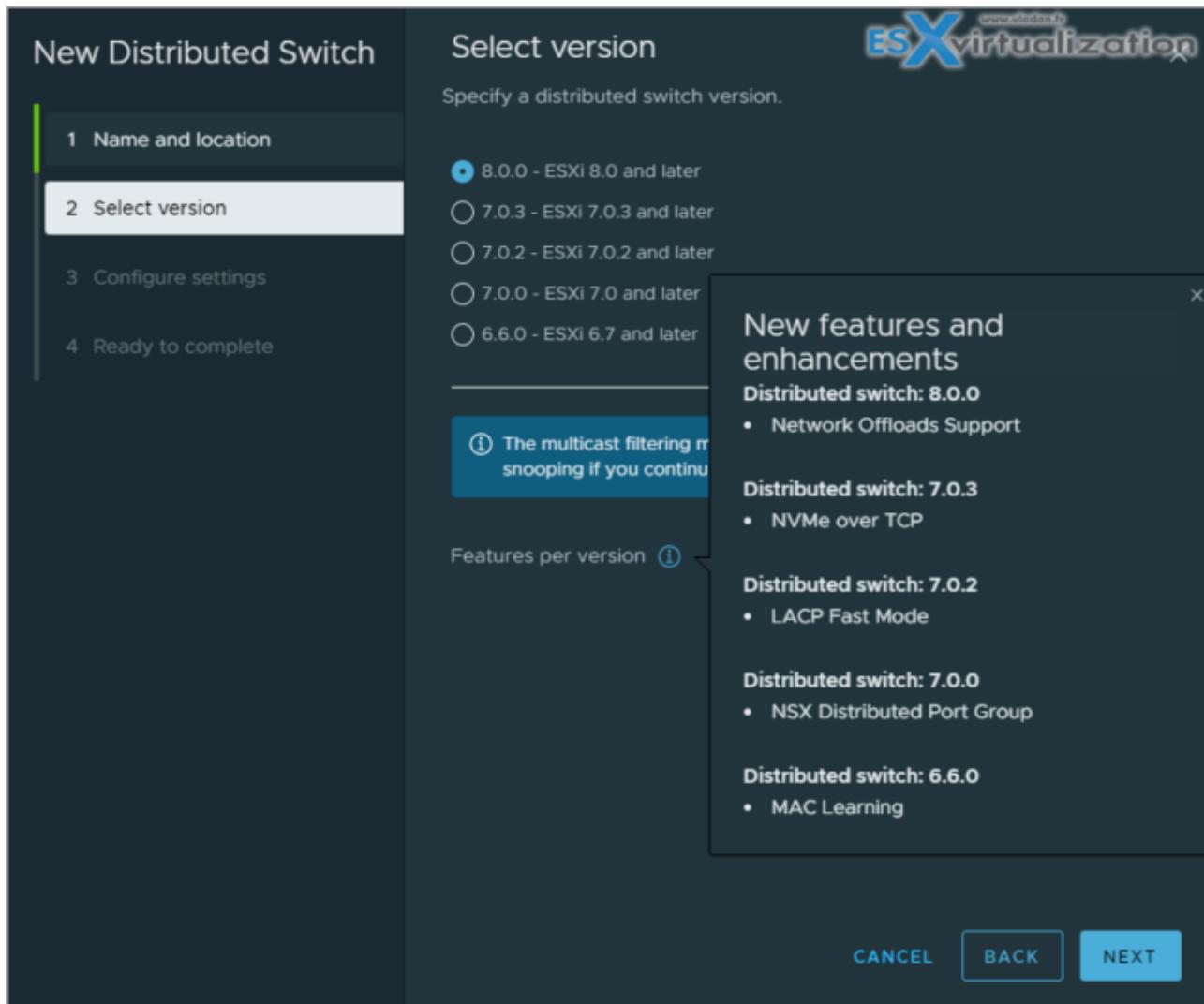
A vSphere distributed switch acts as a single switch across all associated hosts in a data center to provide centralized provisioning, administration, and monitoring of virtual networks. You configure a vSphere distributed switch on the vCenter Server system and the configuration is propagated to all hosts that are associated with the switch.

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

**Figure 3-1. vSphere Distributed Switch Architecture**



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



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

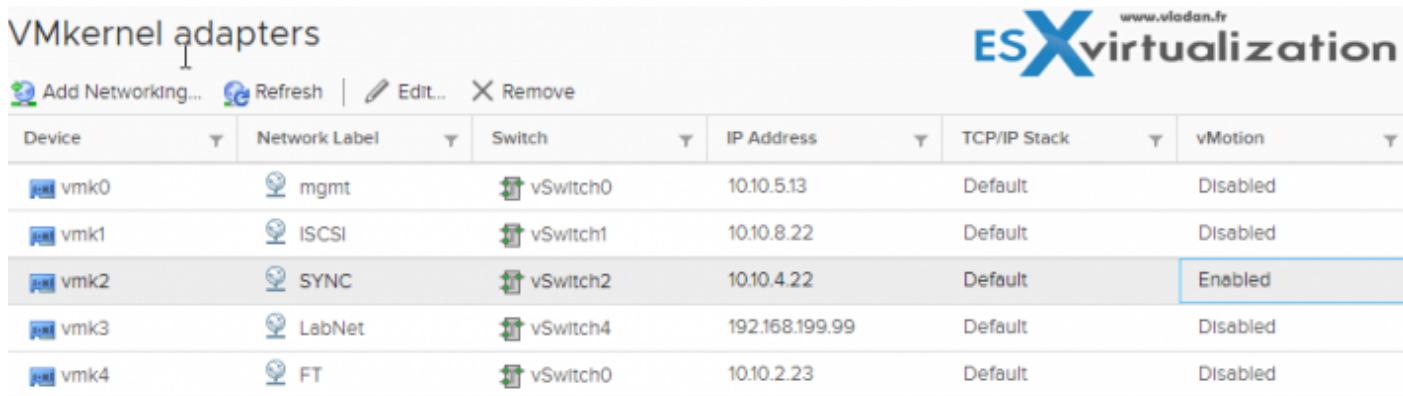
**vSphere Standard Port Group** – Network services connect to standard switches through port groups. Port groups define how a connection is made through the switch to the network. Typically, a single standard switch is associated with one or more port groups. A port group specifies port configuration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

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

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

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

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



Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion
vmk0	mgmt	vSwitch0	10.10.5.13	Default	Disabled
vmk1	iSCSI	vSwitch1	10.10.8.22	Default	Disabled
vmk2	SYNC	vSwitch2	10.10.4.22	Default	Enabled
vmk3	LabNet	vSwitch4	192.168.199.99	Default	Disabled
vmk4	FT	vSwitch0	10.10.2.23	Default	Disabled

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

Further reading of the document will give you details on:

- Managing networking on multiple hosts on a VDS
- Migrating VMKernel adapters to VDS
- Create VMkernel adapters on VDS
- Use Host as a template to create a uniform networking configuration on VDS

## Networking Policies

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

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

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

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

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

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

We simply can't squeeze all the networking knowledge into a single post. Check also:

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

### **Some best practices:**

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

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

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

## Objective 1.5.1 – Describe VMkernel networking

Few words and definitions which you'll hear quite often.

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

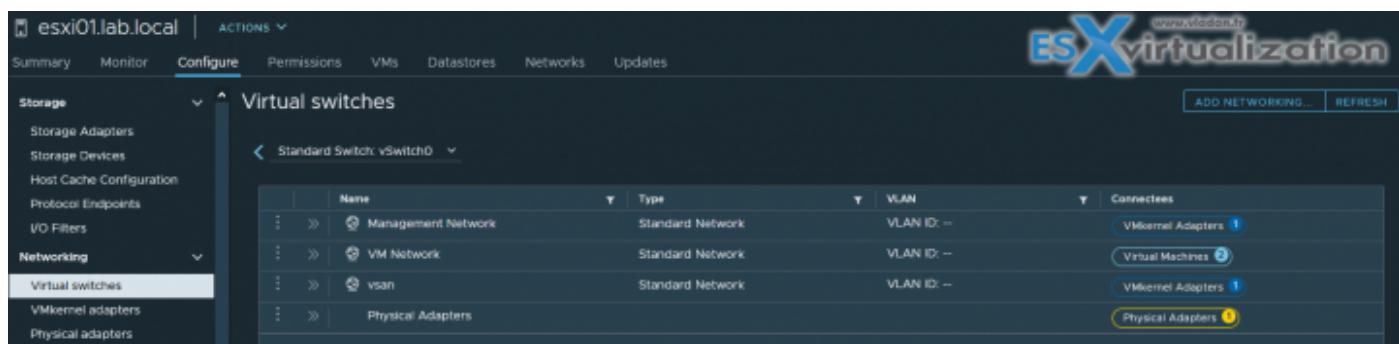
A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port group.

### Terminology:

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

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

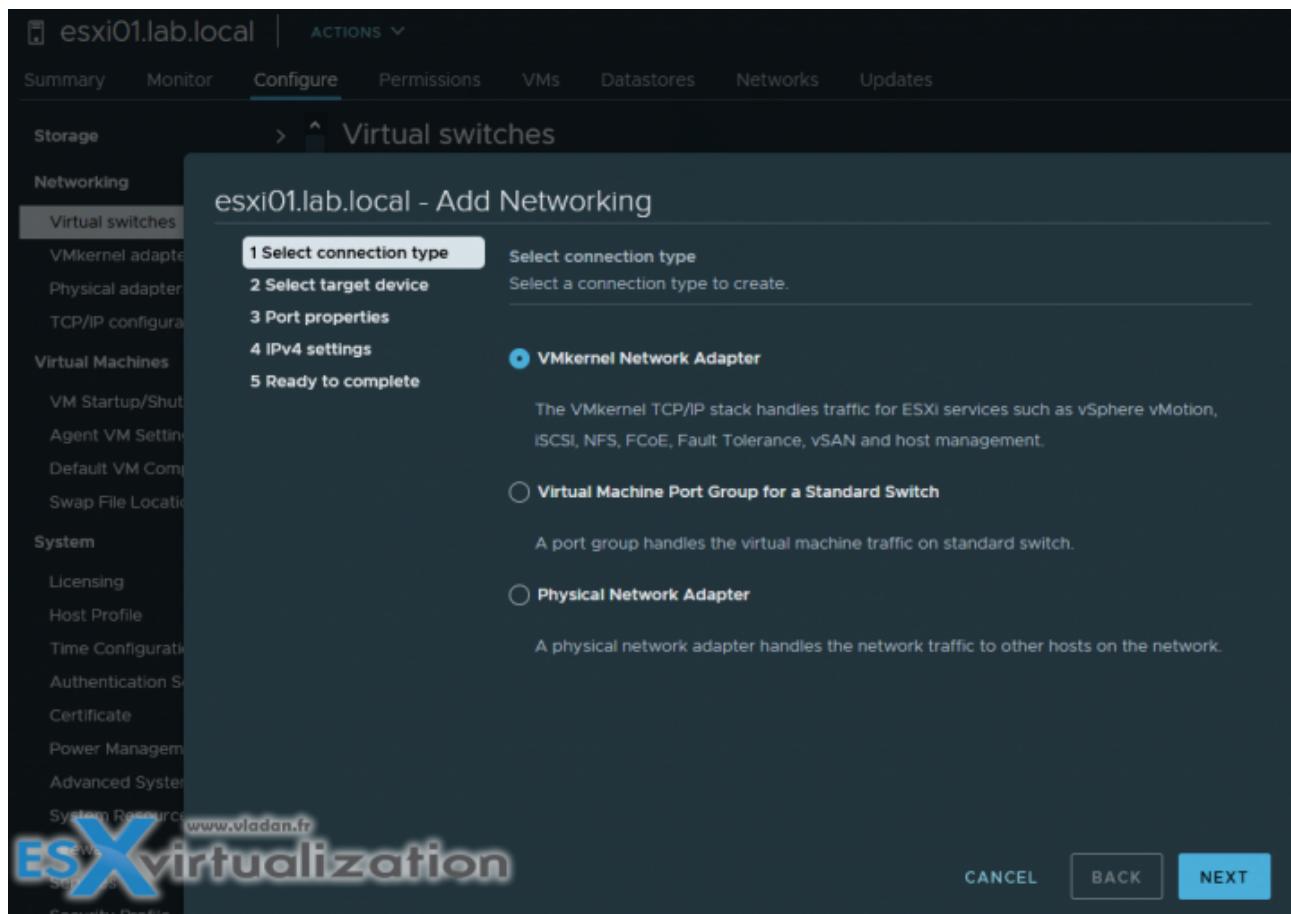
- **vSphere Standard Switch (vSS)** – it's like a physical Ethernet switch where you have VMs connected and those can communicate with each other as the switch forward traffic to each of those VMs.
- **Standard Port group** – portgroup specifies port configuration options (VLAN, bandwidth limitation). 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.



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



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

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

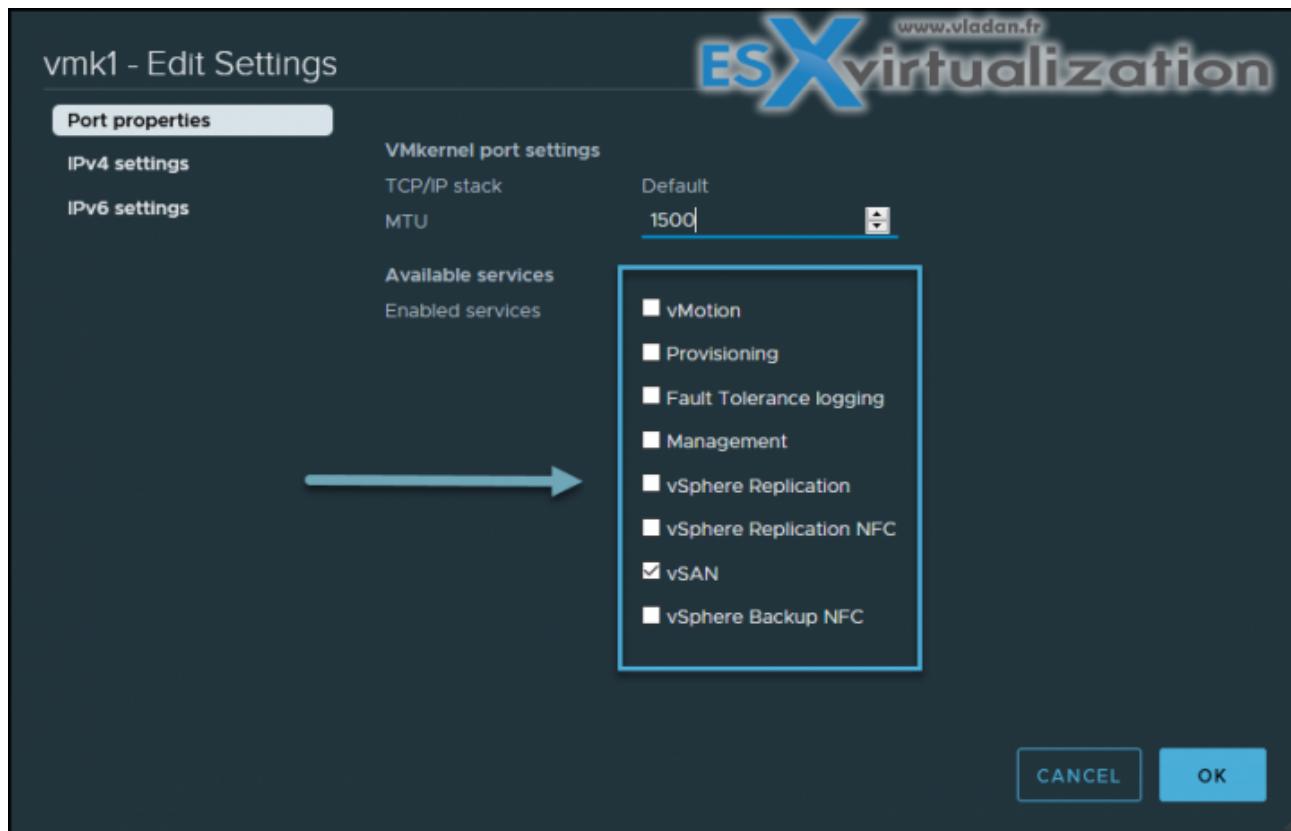
Continue the assistant to create your vSS and network.

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 1.5.2 – Manage networking on multiple hosts with vSphere Distributed Switch (VDS)

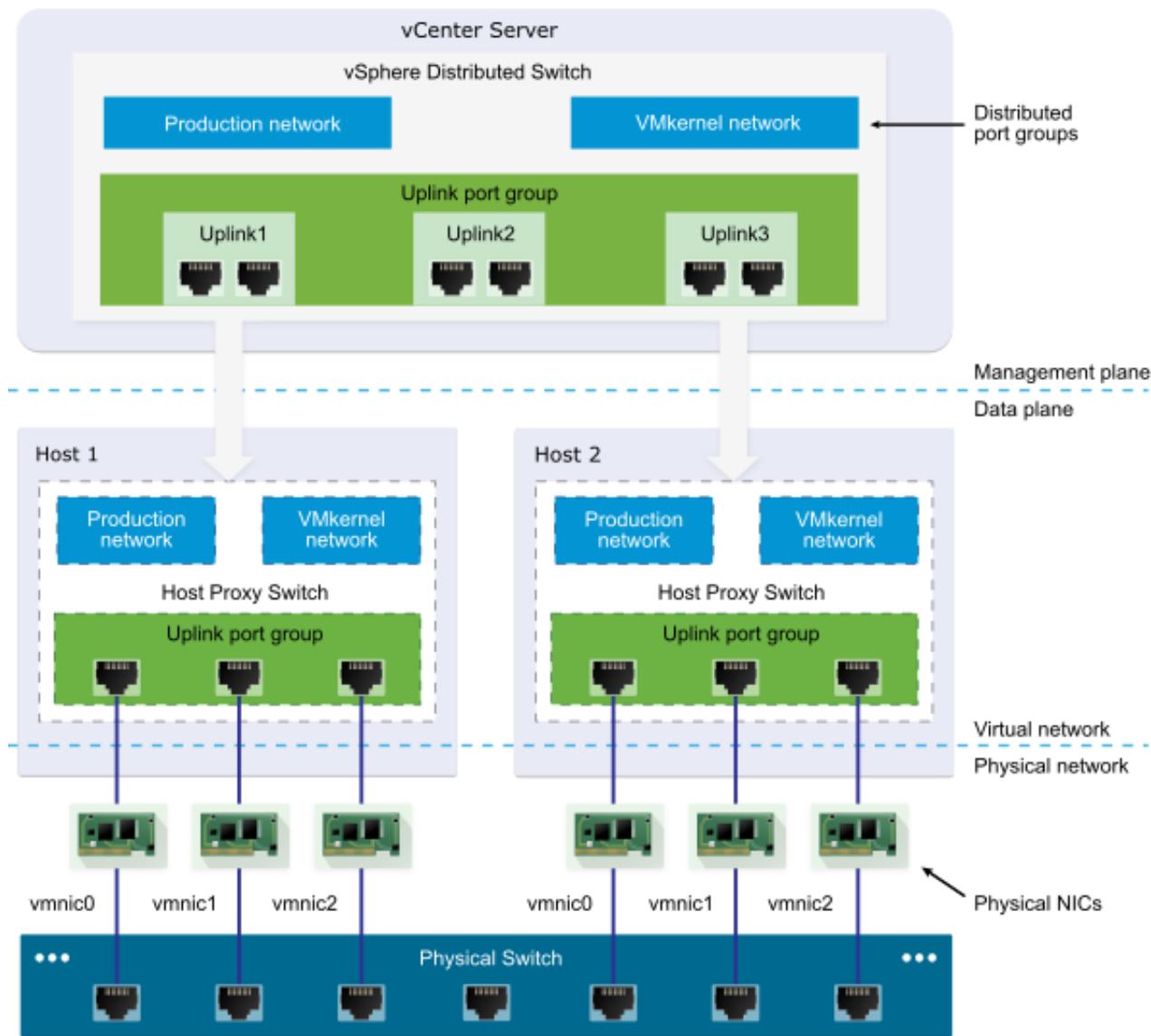
A vSphere Distributed Switch (vDS) acts as a single virtual switch that is associated with selected hosts in your datacenter. You can pick a host that is part of vDS but you don't have to "attach" all the hosts from your environment.

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 said configuration available only for clients that 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.



VMware vDS Architecture

## 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 very powerful.

## Uplink port groups

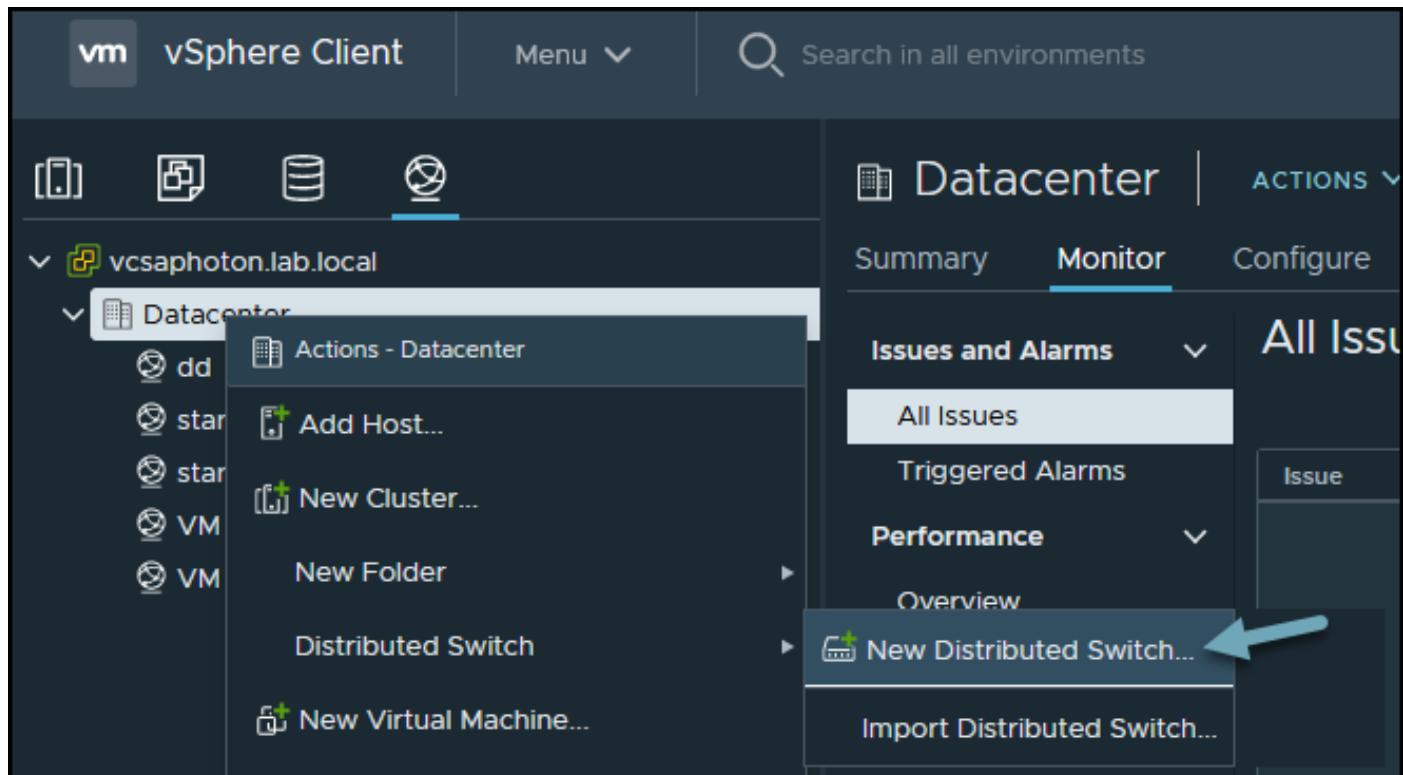
As with standard switches, there are uplinks that are providing connectivity to the physical world. An uplink port group has one or more uplinks. By default, there are 4 uplinks created when first create a vDS.

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.

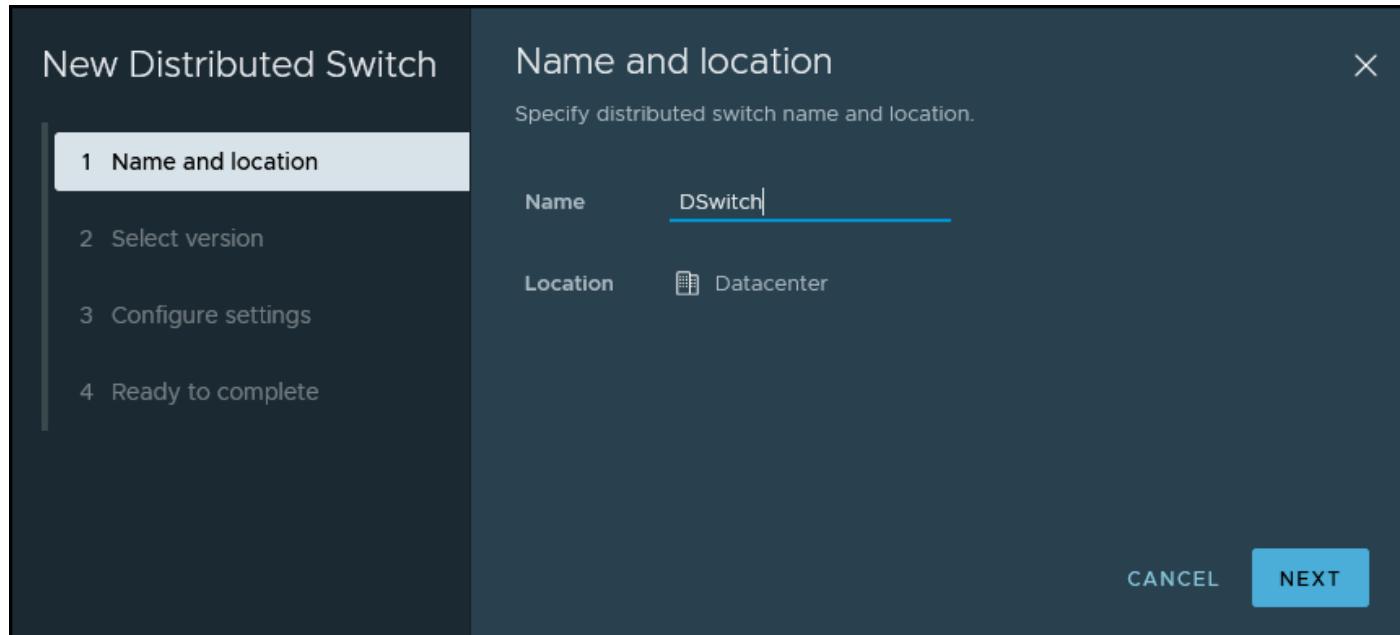
Now we're going to show you how to create a VMware vDS. First, you need to create the vSphere distributed switch. Go to the networking tab by clicking on the globe in the HTML5 client.

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



Create new vSphere Distributed Switch

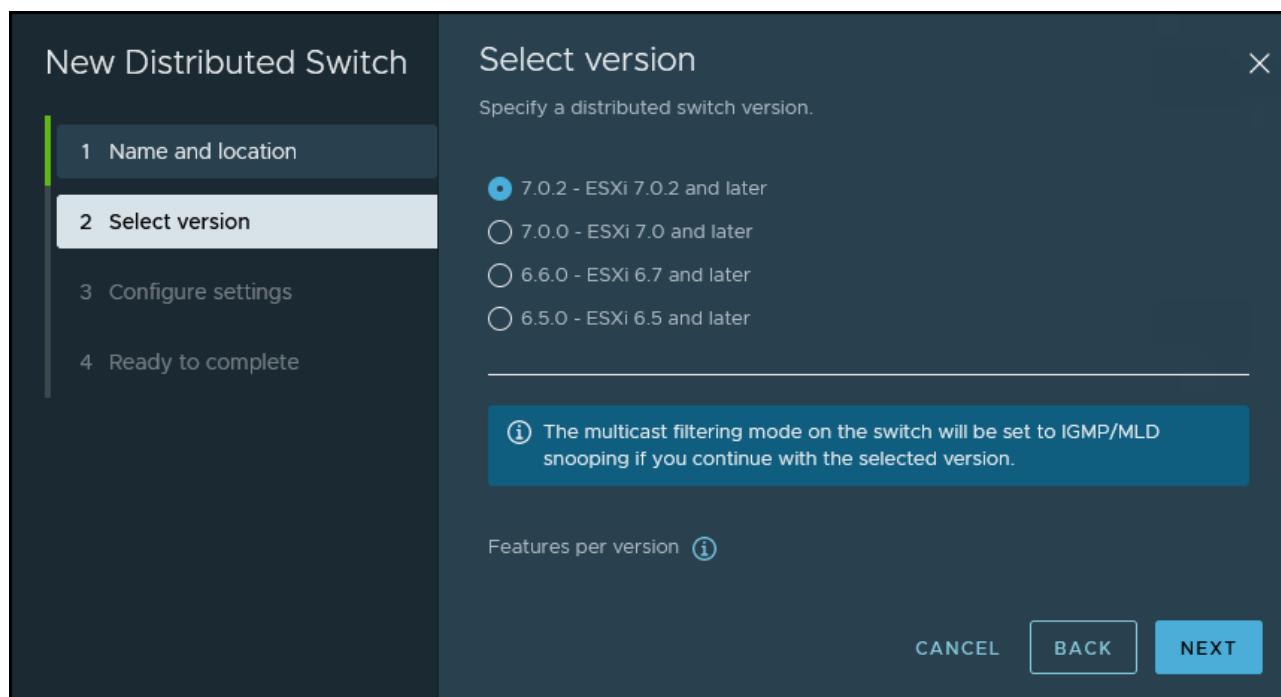
Next, put some meaningful name for your switch. Note that within your datacenter you might be creating several vDS so a proper naming convention is probably not a bad idea.



#### 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 8 so you'd be obviously picking up the older version of the vDS.

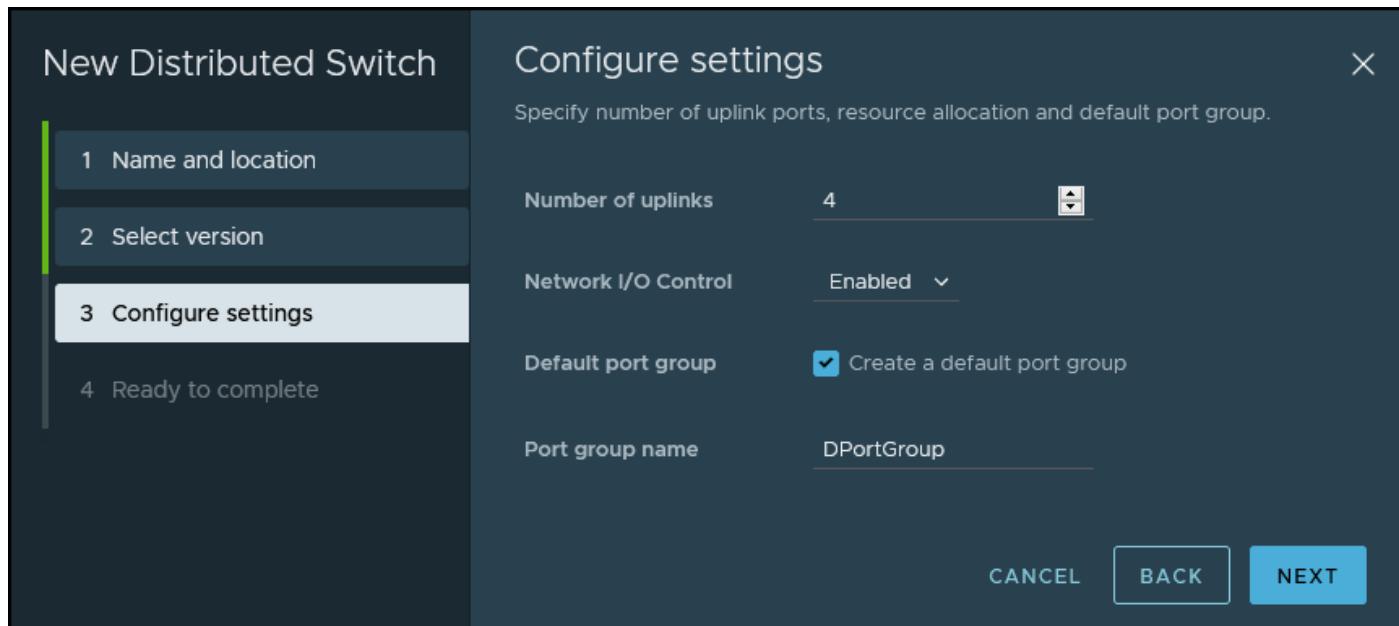
The vDS has evolved since vSphere 6.x to 7.0.2 by adding additional features and options. Let's move on with the wizard.



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

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

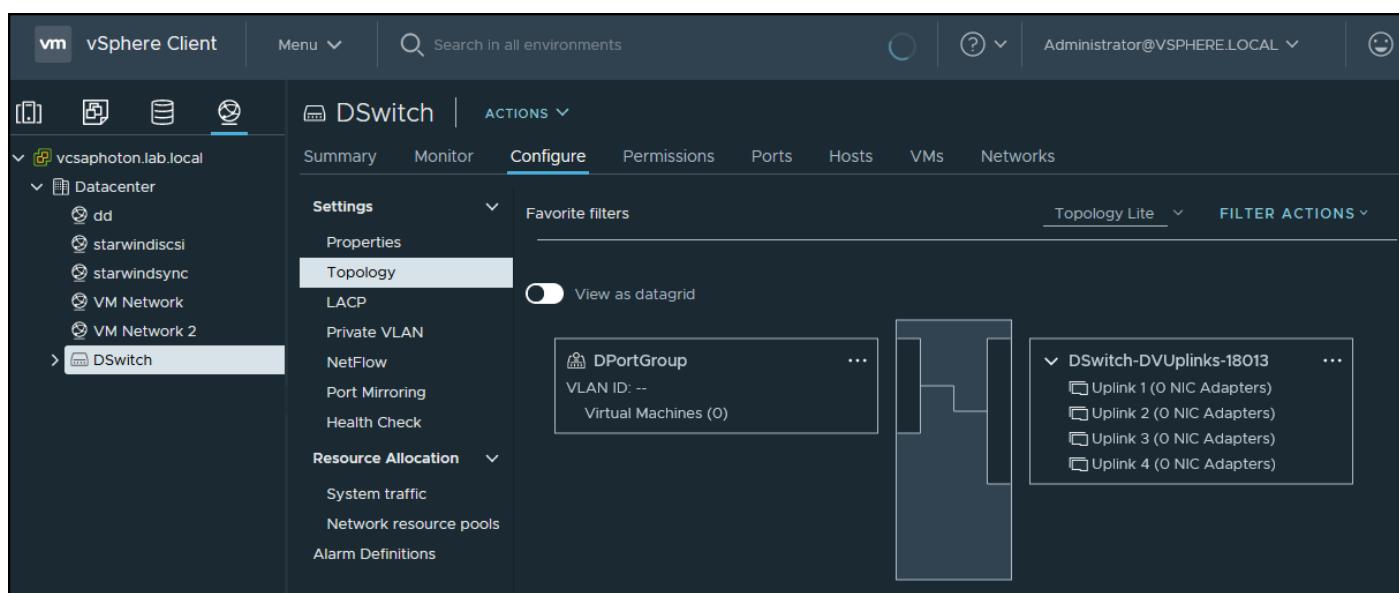
Also, on this page, we're asked to create the default port group. You can pick a name for this distributed port group here or rename it later.



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

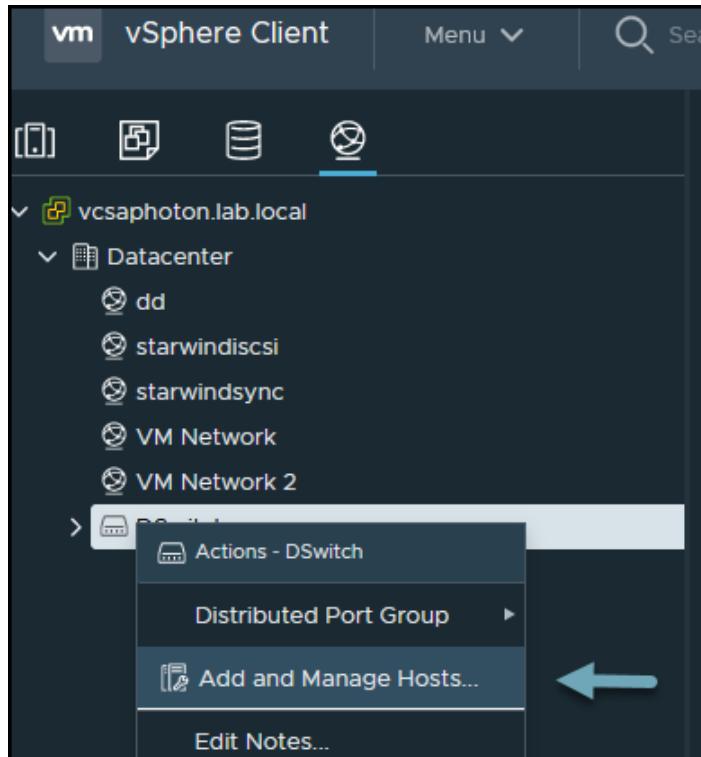
On the next page, you'll see the recapitulation. Click the finish button to create your vDS. You can have a look at the vDS topology. You're still in the networking section and you should see your vDS here.

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



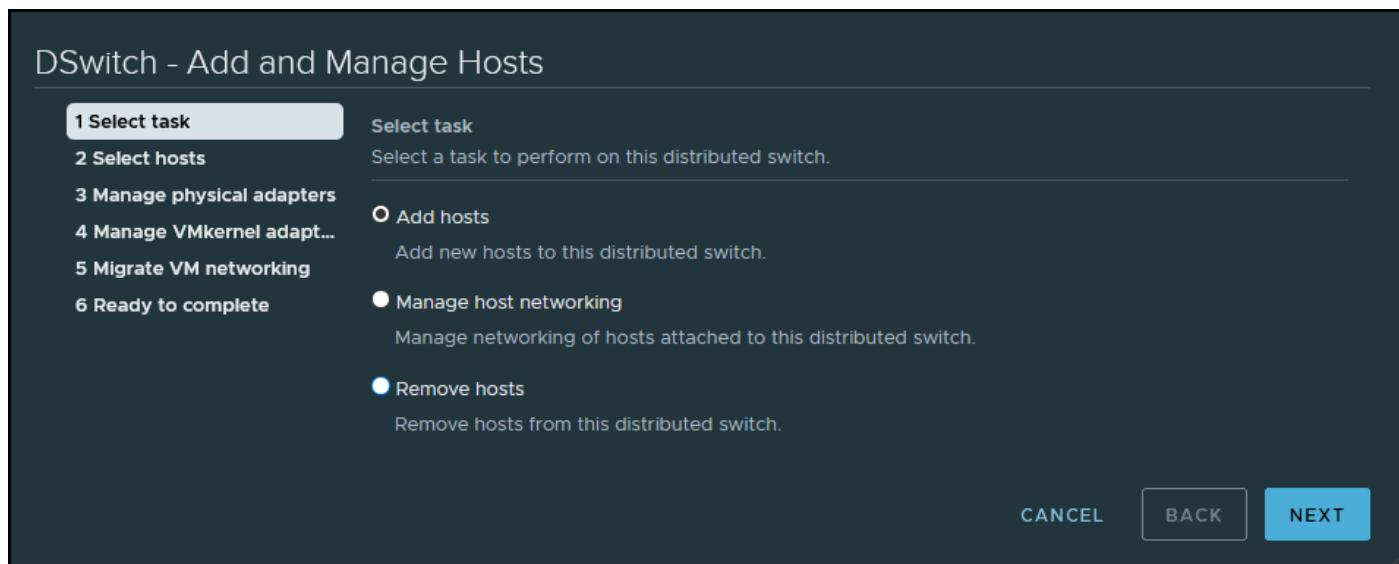
VMware vDS Topology

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



#### 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	✓ Compatible
<input checked="" type="checkbox"/>	esxi02.lab.local	Connected	Cluster	✓ Compatible
<input checked="" type="checkbox"/>	esxi03.lab.local	Connected	Cluster	✓ Compatible
<input type="checkbox"/>	esxi04.lab.local	Connected	N/A	✓ Compatible

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

**1 Select task**

**2 Select hosts**

**3 Manage physical adapters**

**4 Manage VMkernel adapt...** (selected)

**5 Migrate VM networking**

**6 Ready to complete**

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

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Gr...
<ul style="list-style-type: none"> <li>On this switch</li> <li>On other switches/unclaimed</li> </ul>			
esxi01.lab.local	vSwitch0	Management Net...	Do not migrate
vmk0	vSwitch0	vsan	Do not migrate
esxi02.lab.local	vSwitch0	Management Net...	Do not migrate
vmk0	vSwitch0	vsan	Do not migrate
esxi03.lab.local	vSwitch0	Management Net...	Do not migrate
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

**1 Select task**

**2 Select hosts**

**3 Manage physical adapters**

**4 Manage VMkernel adapt...**

**5 Migrate VM networking** (selected)

**6 Ready to complete**

**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
<ul style="list-style-type: none"> <li>On this switch</li> <li>On other switches/unclaimed</li> </ul>			
esxi01.lab.local	1	Reassigned	
2008R2	1		
Z-VRA-esxi01.lab.local	1		
esxi02.lab.local	3		
StarWind01	3		
Z-VRA-esxi02.lab.local	1		
esxi03.lab.local	1		
Z-VRA-esxi03.lab.local	1		
On this switch			

**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 1.5.3 – Describe Networking Policies

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 more.

You can use the 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 the virtual switch or port group level for a VSS and at the port group or port level for a VDS.

### VSS

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 to all the port groups present in the switch. If you want to apply different policies to a specific port group, you need to apply the policy to that particular port group and check that **Override Policies** is set on the switch for each port group.

For example, you can configure which physical network adapters handle the network traffic for the VSS.

Connect to the vCenter Server via the vSphere client, select your host, and then select **Configure > Networking > Virtual Switches**.

esxi01.lab.local | ACTIONS ▾

Summary Monitor Configure Permissions VMs Datastores Networks Updates

**Storage**

- Storage Adapters
- Storage Devices
- Host Cache Configuration
- Protocol Endpoints
- I/O Filters

**Networking**

- Virtual switches** (highlighted)
- VKernel adapters
- Physical adapters
- TCP/IP configuration

**Virtual Machines**

- VM Startup/Shutdown
- Agent VM Settings
- Default VM Compatibility
- Swap File Location

**System**

- Licensing
- Host Profile
- Time Configuration
- Authentication Services
- Certificate

Distributed Switch: DSwitch 1

Standard Switch: vSwitch0 | ADD NETWORKING EDIT MANAGE PHYSICAL ADAPTERS ...

Management Network  
VLAN ID: --  
VMkernel Ports (1)  
vmk0 : 192.168.1.11

VM Network  
VLAN ID: --  
Virtual Machines (3)

vsan  
VLAN ID: --  
VMkernel Ports (1)  
vmk1 : 192.168.1.201

Physical Adapters  
vmnic0 10000 Full  
vmnic7 10000 Full

Standard Switch: vSwitch1

Standard Switch: vSwitch2

Edit properties of vSphere Standard Switch

Then select vmnic7 and click the Up arrow to move this adapter to the **Active adapters** section.

vmotion - Edit Settings

**Properties**

**Security**

**Traffic shaping**

**Teaming and failover** (selected)

Load balancing       Override      Route based on originating virtual port

Network failure detection       Override      Link status only

Notify switches       Override      Yes

Fallback       Override      Yes

**Failover order**

Override

↑ [Move Up] ↓ [Move Down]

Active adapters	Move Down
vmnic6	
vmnic5	
vmnic0	
vmnic7	
Standby adapters	
Unused adapters	

Select a physical network adapter from the list to view its details.

Select active and standby adapters. During a failover, standby adapters activate in the order specified above.

CANCEL OK

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. The 'Teaming and failover' tab is selected. Under 'Failover order', there is a list of adapters: 'vmnic0' (Active) and 'vmnic7' (Standby). The 'vmnic7' adapter is highlighted. The right panel displays adapter details:

Adapter	
Name	VMware Inc. vmxnet3 Virtual Ethernet Controller
Location	vmnic7
Driver	PCI 0000:05:00.0 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.' There are 'CANCEL' and 'OK' buttons at the bottom right.

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 port group, we can show you another example. Let's say that you have added two others 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 and select **vMotion > Edit settings > Teaming and Failover**.

The screenshot shows the vSphere Web Client interface under the 'Configure' tab. On the left, the navigation bar includes 'Storage', 'Networking' (selected), 'Virtual machines', and 'System'. In the center, under 'Networking', 'Virtual switches' is selected. A list of virtual switches is shown: 'Management Network', 'VM Network', 'vmotion' (selected), and 'vsan'. The 'vmotion' switch has its 'Edit' context menu open, with the 'Edit Settings' option highlighted by a blue arrow.

### Configure multiple adapters for vMotion traffic

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.

The screenshot shows the 'vmotion - Edit Settings' dialog. The 'Teaming and failover' tab is active. Under 'Failover order', there is a dropdown menu for 'Active adapters' containing 'vmnic6', 'vmnic5', 'vmnic0' (highlighted), and 'vmnic7'. Below this, there are sections for 'Standby adapters' and 'Unused adapters'. A blue arrow points to the 'Move Down' button in the dropdown menu, and another blue arrow points to the 'Unused adapters' section.

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).

vmotion - Edit Settings

**Properties**

**Security**

**Traffic shaping**

**Teaming and failover**

Load balancing       Override      Route based on originating virtual port

Network failure detection       Override      Link status only

Notify switches       Override      Yes

Fallback       Override      Yes

**Failover order**

Override

↑ ↓

Active adapters
vmnic6
vmnic5
Standby adapters
Unused adapters
vmnic0
vmnic7

Select a physical network adapter from the list to view its details.

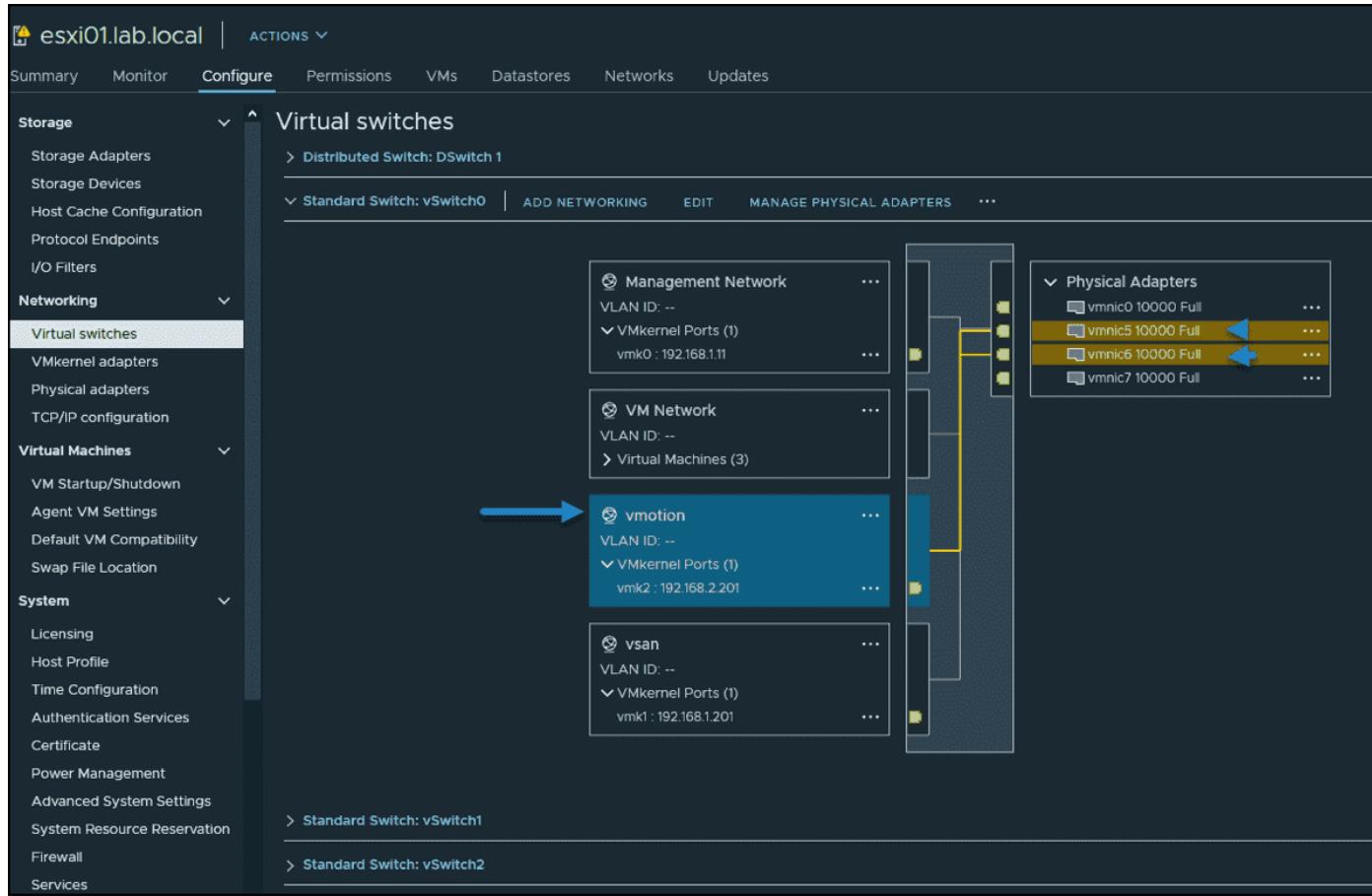
Select active and standby adapters. During a failover, standby adapters activate in the order specified above.

CANCEL      OK

Click validate to save the configuration

If you want to check which NICs are used for each of the port groups, simply click the link in each port group, and you'll have a visual.

When we click the vMotion link on the port group in our example, we can see which NICs are used for vMotion traffic.



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

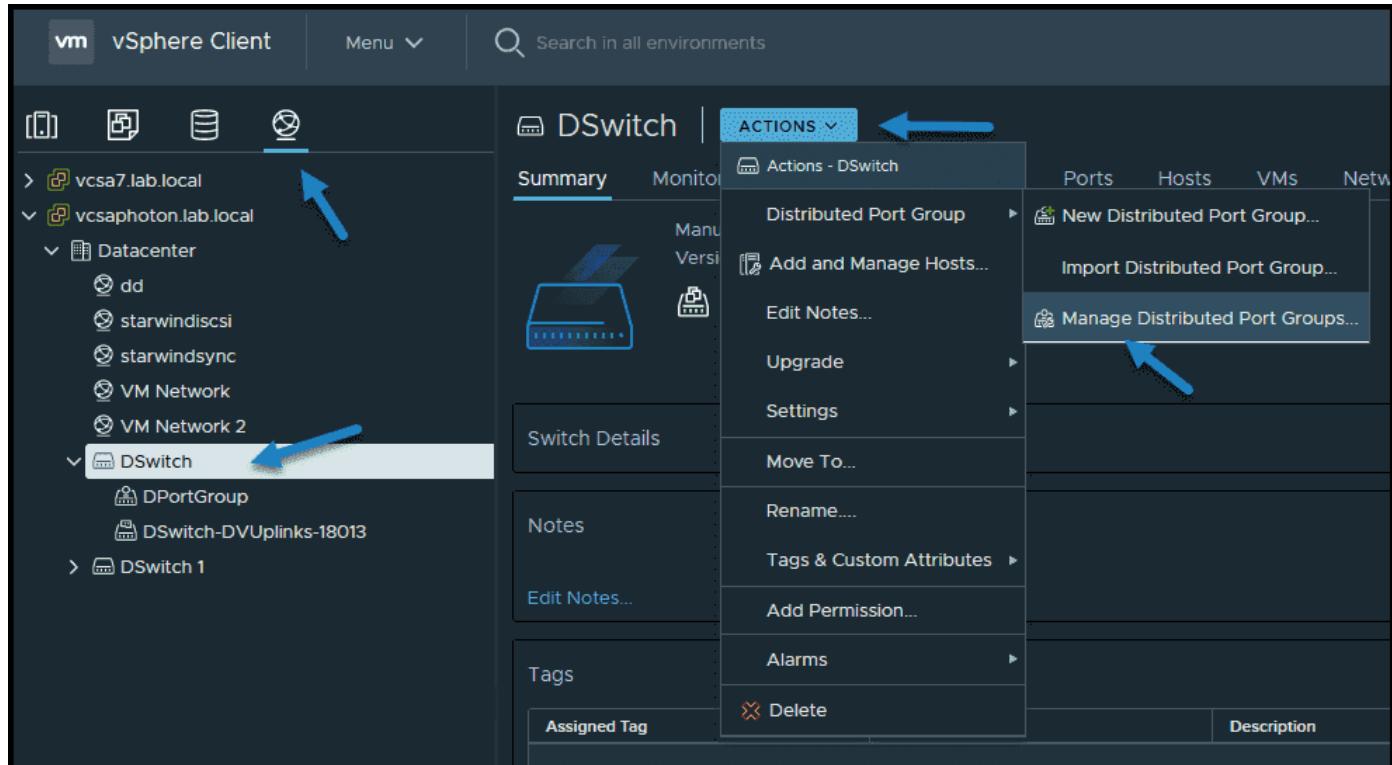
## VDS

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

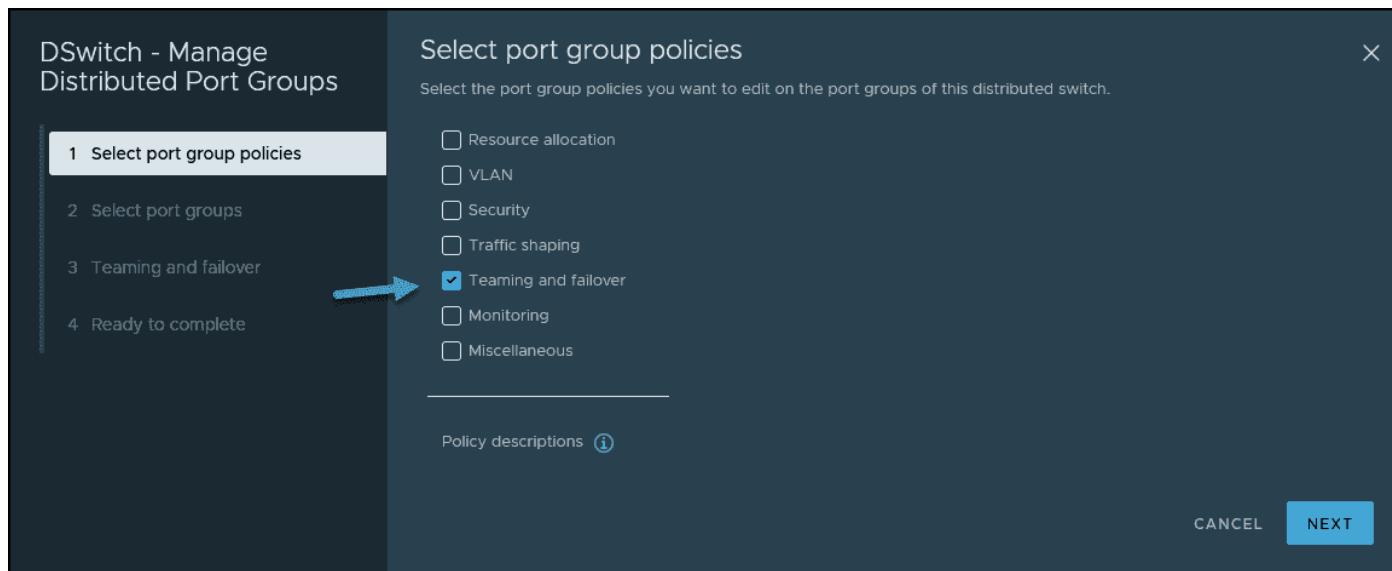
To have different policies for specific ports, you can override the policies set on the port group at a per-port level. This is useful when you want to set specific policies for individual VMs or physical network adapters.

Go to **Networking** and select your VDS. Then select **Actions > Manage Distributed Port Groups**.



Manage distributed port groups on VDS

A new assistant is displayed. Select **Teaming and failover**.



Select Teaming and failover

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

**DSwitch - Manage Distributed 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

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

Select all three port groups

On the next page, select **Uplink 3** and **Uplink 4** and click the **Move Down** button to push them to the **Unused uplinks** section.

**DSwitch - Manage Distributed Port Groups**

**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 Down

**Active uplinks** Move Down

- Uplink 1
- Uplink 2
- Uplink 3
- Uplink 4

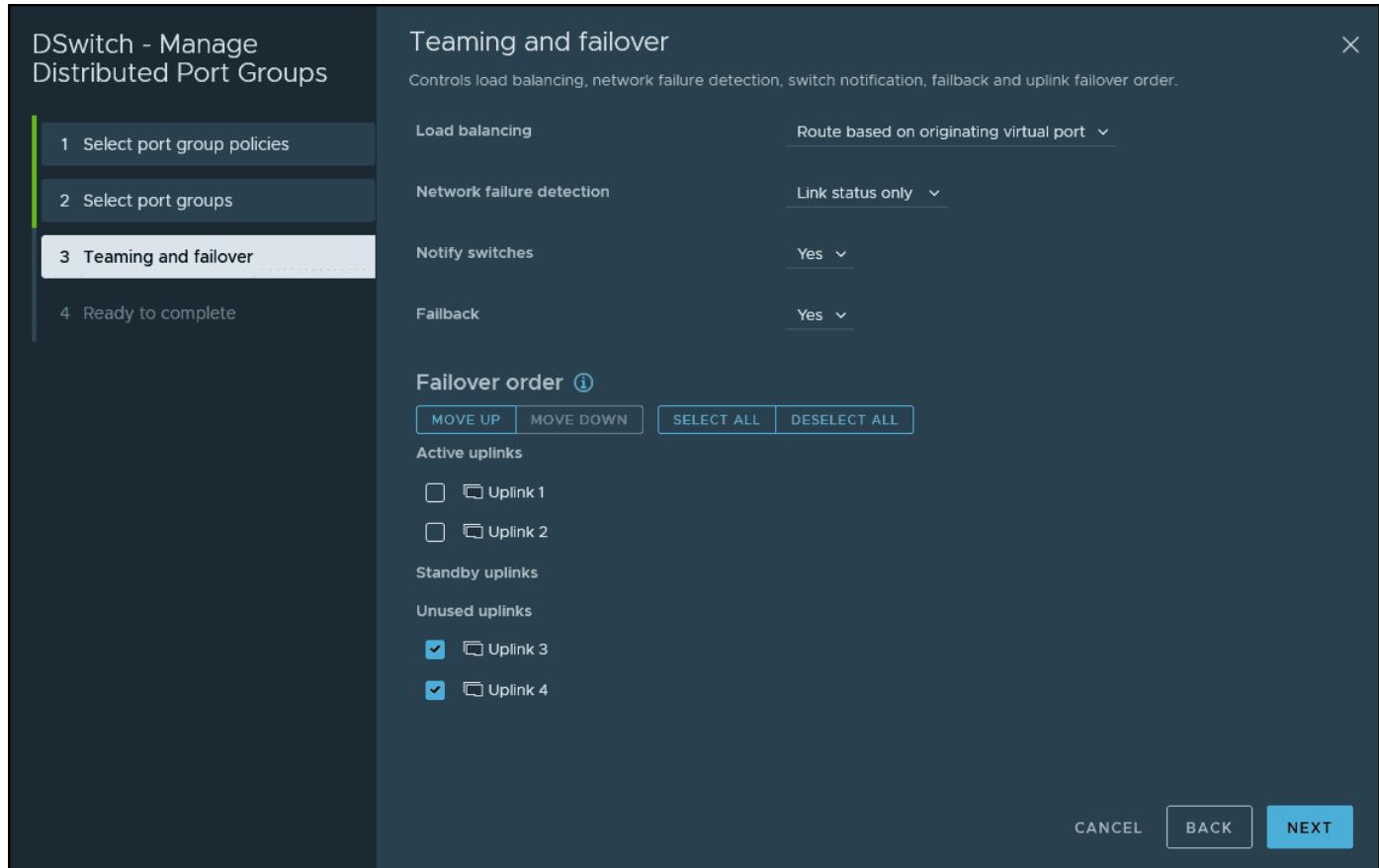
**Standby uplinks**

**Unused uplinks**

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

Select Uplink 3 and Uplink 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 three different port groups simultaneously with a single networking policy. This is the power of distributed switches. You can apply your configuration to all the hosts that are attached to the VDS within your cluster. If you had used only VSS, you'd have to do this host-by-host.

## Objective 1.5.4 – Manage Network I/O Control (NIOC) on a vSphere Distributed Switch (VDS)

With Network I/O control (NIOC), you can adjust the bandwidth of your vSphere 8 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.

here 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 8 Distributed vSwitch (vDS) is version 8 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

Advanced	
MTU	1500 Bytes
Multicast filtering mode	IGMP/MLD snooping

Discovery protocol	
Type	Cisco Discovery Protocol
Operation	Listen

Administrator contact	
Name	
Other details	

## 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**.

**Dswitch2 - Upgrade Distributed Switch**

**1 Configure upgrade**

**2 Check compatibility**

**3 Ready to complete**

**Configure upgrade**  
Specify distributed switch version for upgrade.

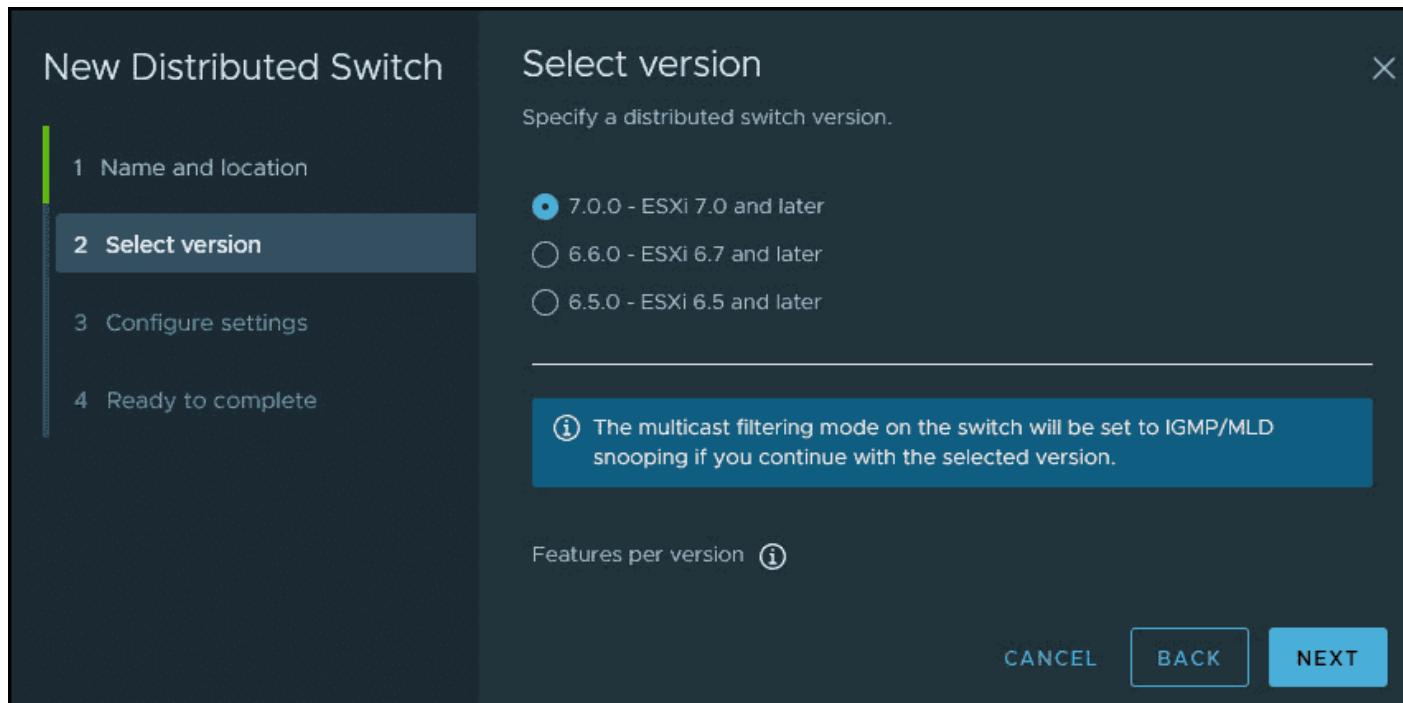
7.0.0 - ESXi 7.0 and later  
 6.6.0 - ESXi 6.7 and later

**① The multicast filtering mode on the switch will be set to IGMP/MLD snooping if you continue with the selected version.**

Features per version **①**

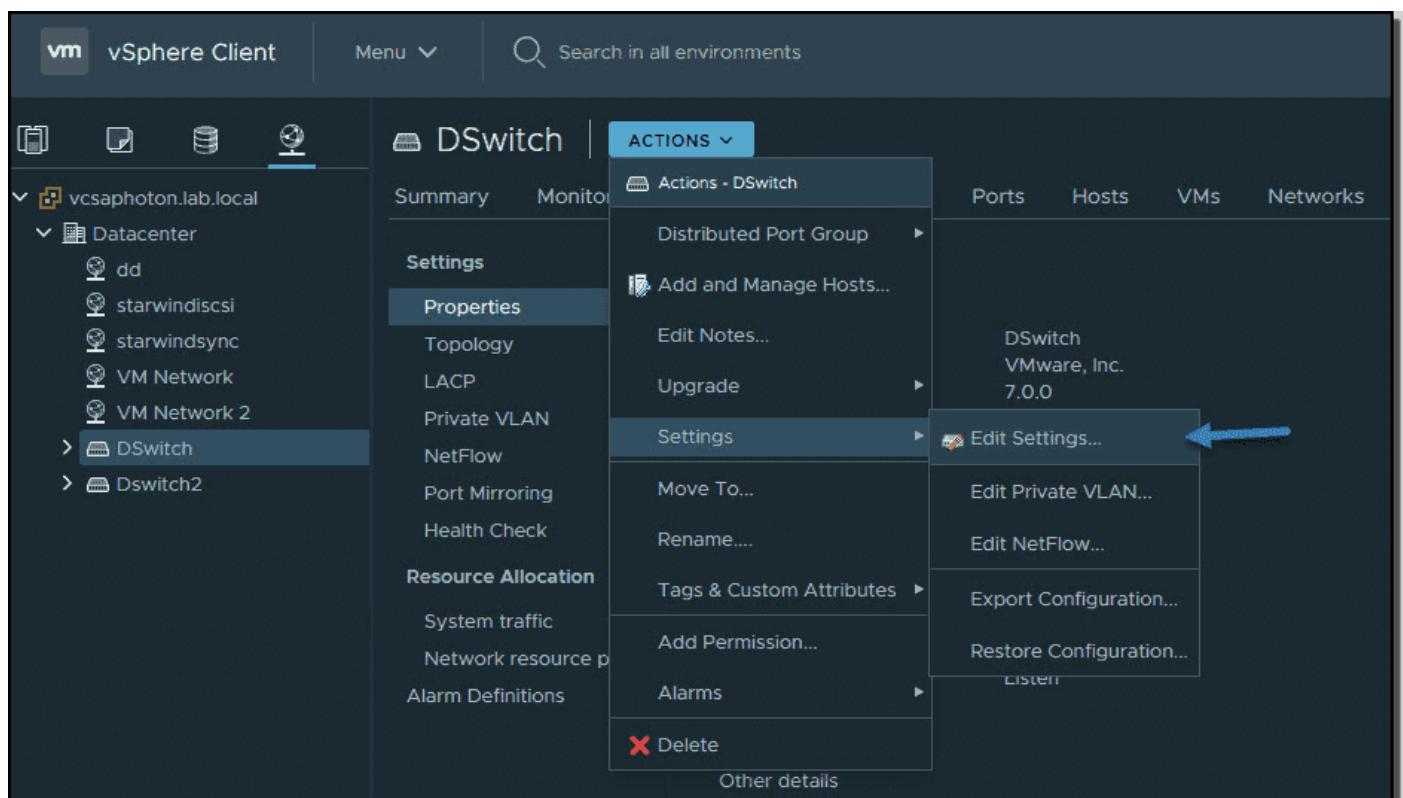
**CANCEL** **BACK** **NEXT**

If you're running a fresh installation of vSphere 8 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.

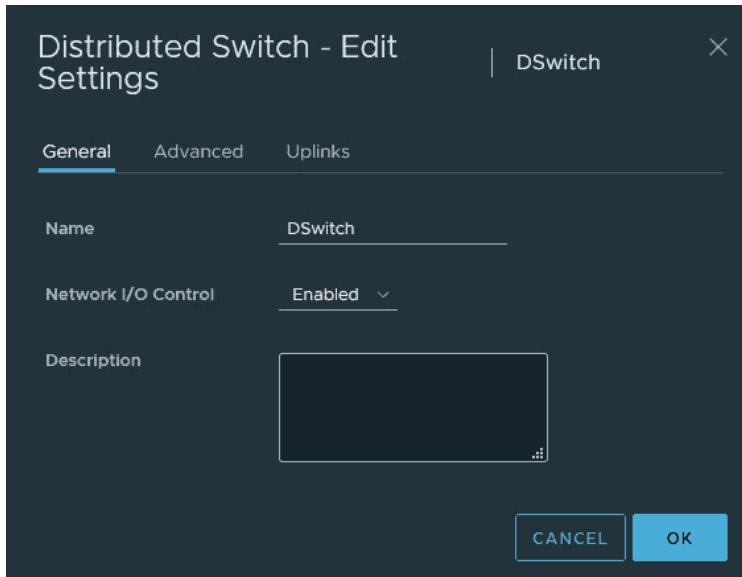


## Where should you enable NIOC?

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



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.

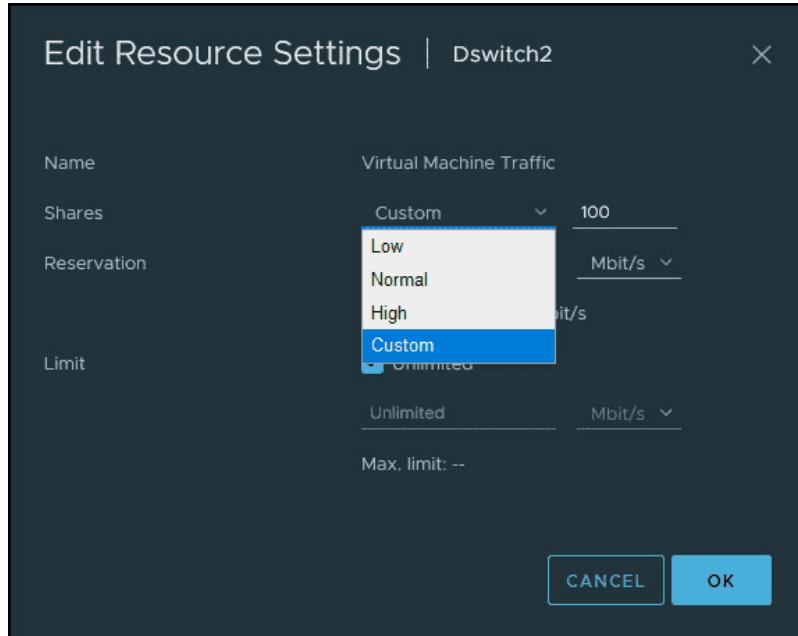
The main vSphere features for which network traffic can be configured are:

- 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

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

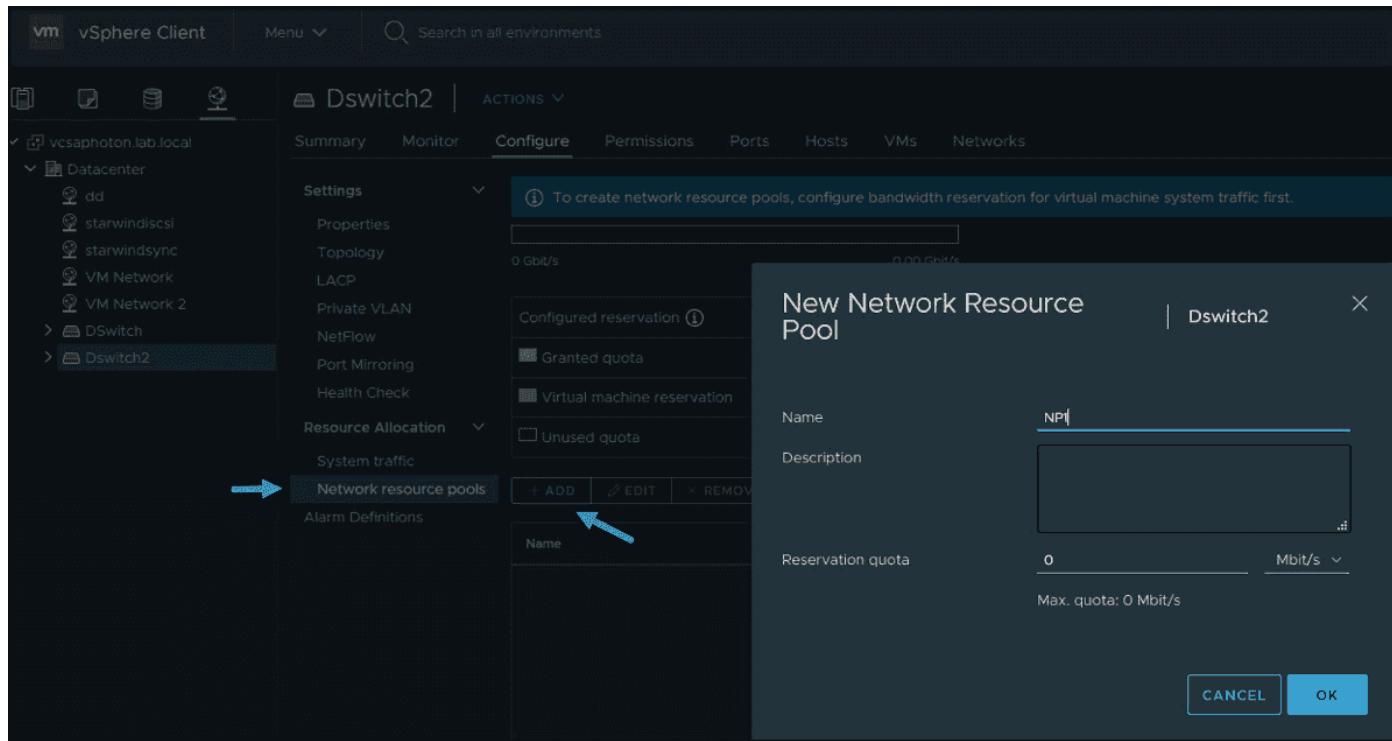


The allocation parameters for the different traffic types are:

- **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.



This is the main principle of NIOC in vSphere. 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 1.5.5 – Describe Network I/O Control (NIOC)

Explained in 1.5.4

## Objective 1.6 – Describe VMware vSphere Lifecycle Manager concepts

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 would it be interesting when it is not often when you have to reboot your hosts? 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 through all of the hardware initialization phases each boot.

The things slightly changed since vSphere 6.7 as now in vSphere 8 (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.

**Cluster** | ACTIONS ▾

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

**Hosts** ▾

- Image**
- Hardware Compatibility
- VMware Tools
- VM Hardware

**Image Compliance**  
Last checked on 01/22/2021, 4:06:05 PM (0 days ago)  
⚠️ 3 of 3 hosts are out of compliance with the cluster's image

**REMEDIEATE ALL** **RUN PRE-CHECK**

Hosts
: esxi02.lab.local
: esxi03.lab.local
: esxi01.lab.local

**esxi02.lab.local**

⚠️ Host is out of compliance with the image  
 ⓘ Quick Boot is supported on the host.  
 The host will be rebooted during remediation.

**Software compliance** **Show Only drift comparison**

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

Quick Boot support in vSphere 8

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.

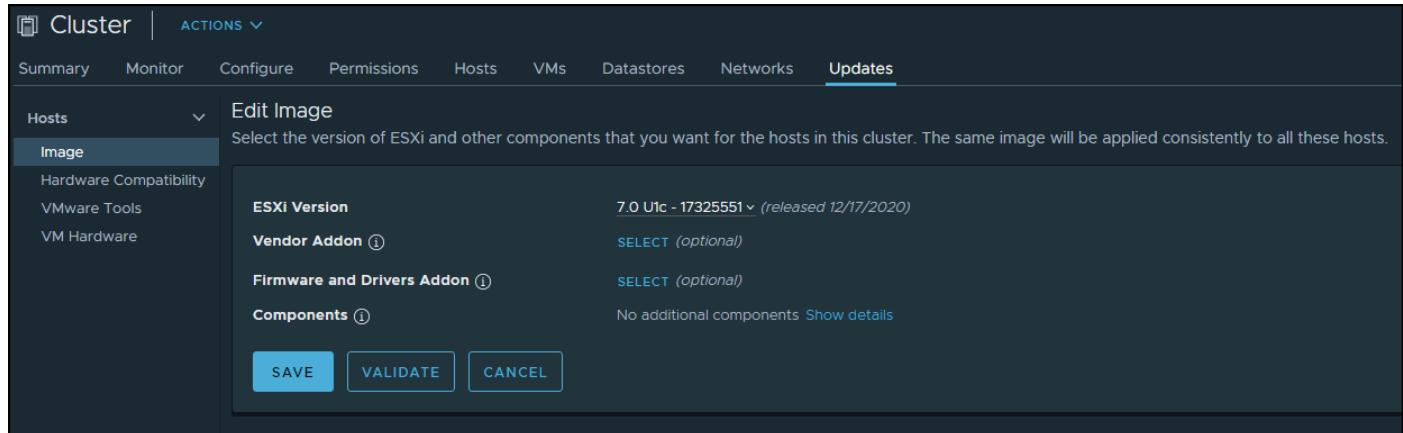
As you can see, quite a few limitations when you enable some security features, such as TPM and secure boot within vSphere.

As I said in the beginning of the post, 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 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 1.7 – 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 not using the storage controller not listed on vSAN HCL.** Not only you won't be supported, but most likely your solution will have bad 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.

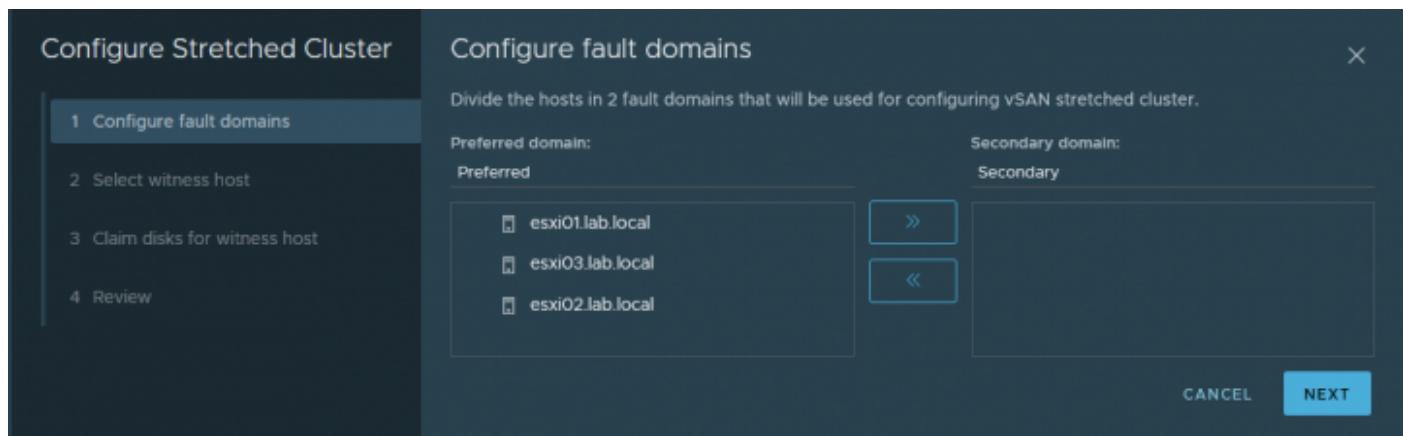
Imagine vSAN as a network distributed RAID storage where local disks are used as shared storage. vSAN uses copies of the VM data where one copy is local and another copy is on one of the other nodes in the cluster. You can configure the number of copies, for data protection or performance.

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 vSAN cluster. You can connect other ESXi hosts or VMs to 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 the third data center.



**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 from Veeam, Nakivo, [Altaro](#) or Zerto 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 kind of a 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.

Name	Drive Type	Defined As	Capacity	Health	Status
Local VMware Disk (lpm:vmhba0:C0:T1L0)	Flash	vSAN Cache	50.00 GB	Healthy	Mounted
Local VMware Disk (lpm:vmhba0:C0:T2L0)	Flash	vSAN Capacity	180.00 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 1.7.1 – Identify basic vSAN requirements (networking, disk count, and type)

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.

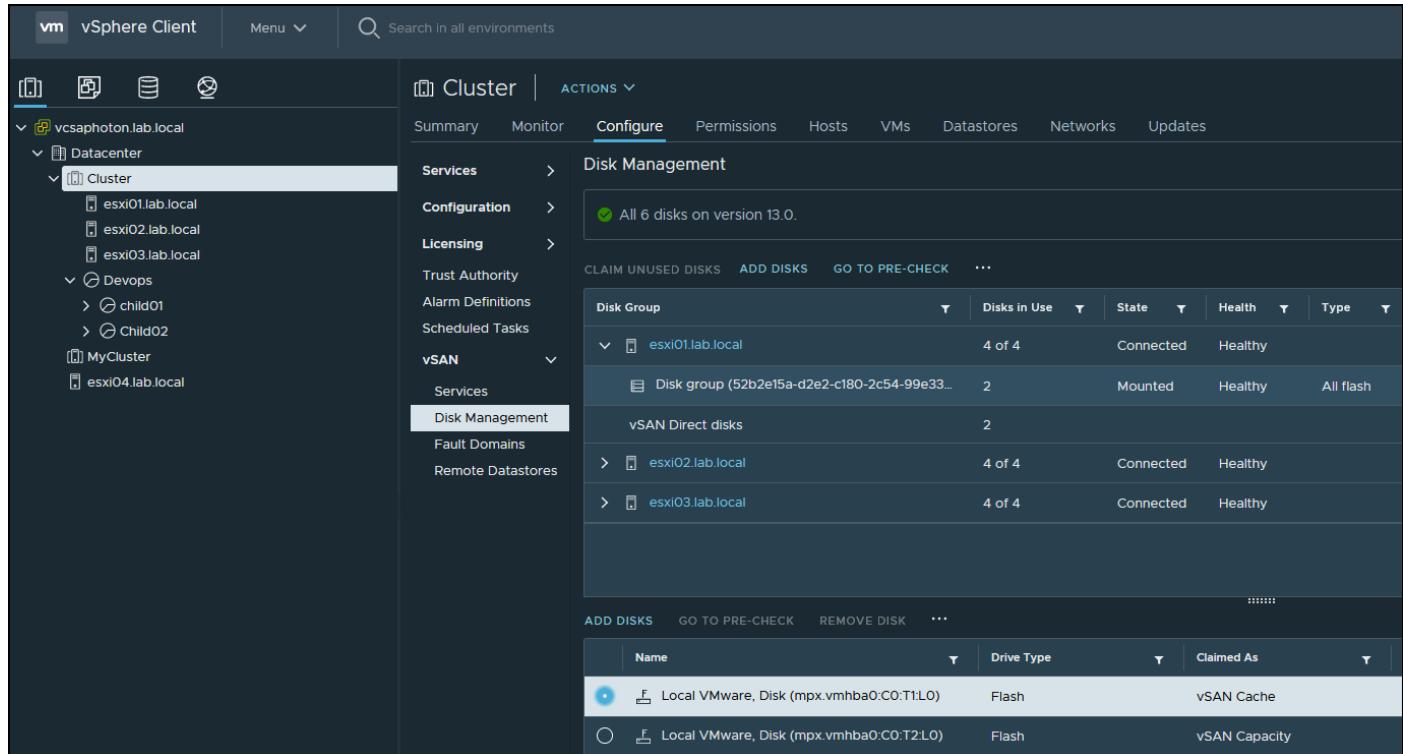
In hybrid clusters, magnetic disks are used for capacity, and flash devices have a read cache and a write buffer function. If you're running a VMware vSAN hybrid cluster, 70% of the flash space is used for the read cache, and 30% is used for the write buffer.

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 kind of a 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.



## 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

The 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 could 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 within 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 tightened 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.

## Objective 1.7.2 – Identify Express Storage Architecture (ESA) concepts for vSAN 8

VMware vSAN 8.0 ESA architecture is faster, uses less CPU and more efficient with better compression. Yes, moving forward, VMware will privilege the deployments and configuration of vSAN as a vSAN ESA. Note that the old, traditional vSAN architecture, based on group disks and caching/capacity devices, will still be supported.

So, the main reason why this evolution and transition is, according to VMware, efficiency, performance and less CPU usage. Considering the evolution in hardware during past two or three years, they're not wrong. NVMe is not the future, it's now.

### **Differences between classic vSAN storage architecture and vSAN 8.0 ESA.**

vSAN Express Storage Architecture in vSAN 8 is a single-tier architecture optimized for high performance NVMe based TLC flash devices.

With traditional vSAN, you had to make some planning and decide whether you'll use RAID 1, RAID 5 or RAID 6. As you can imagine, the workloads did not have the same performance when you selected RAID 1 or RAID 6.

With vSAN 8.0 ESA the need for caching devices has been completely removed so you don't need dedicated caching devices per disk group(s) – because there are no disk groups! There is a completely new log structured file system and IO path optimizations to the write path which further reduce write amplification and reduce write latency.

**Cost per TB has been reduced** – this is due to the change of the architecture as well. You no longer need caching devices. The default storage policy is RAID-1. VMware does however recommend to use RAID-5 or RAID-6 as the default. The compression has been improved 8 times with vSAN 8.0 ESA too which brings overall improvements 4x compared to the original vSAN architecture.

RAID-5/6 erasure coding brings huge capacity savings compared to RAID-1 mirroring. You can save capacity and reduce your TCO by upgrading with new hardware and software. The failures to tolerate (FTT) FTT=2 using RAID-6 will consume just 1.5x when compared to 3x for FTT=2 using RAID-1.

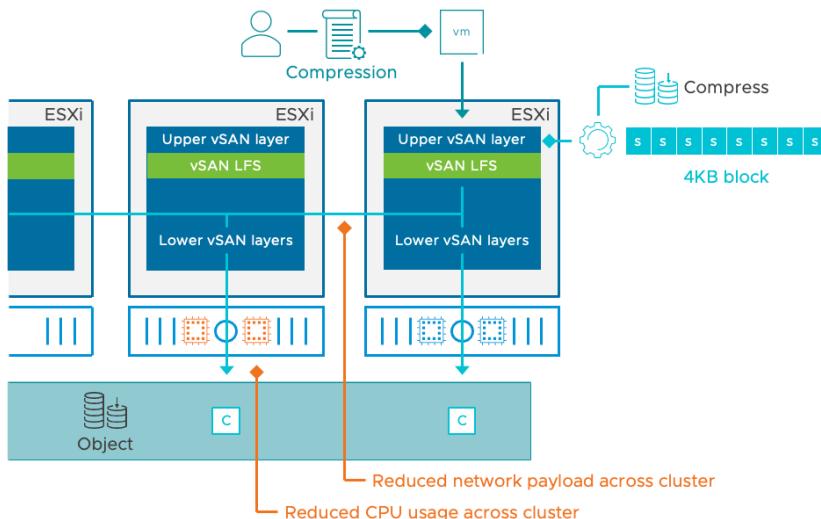
The compression process efficiency works a bit different too compared to the original architecture. During the writes, the compression process only needs to be run only once (vs once for each of the copy of the data in the old vSAN architecture). The reads are fetched compressed that allows to transfer less data when fetched over the network.

Compression is enabled by default but you can disable the feature via vCenter Storage Policy Based Management (SPBM). You can disable compression on per VM-level or even on per-VMDK level. This might be particularly useful for some VMs that uses their own compression utilities such as databases or so.

Screenshot from VMware.

## Storage Policy-based Compression Capabilities

Highly efficient data compression



### vSAN SPBM Compression Capabilities

**vSAN 8.0 performance** – There is a new, log-structured file system (LFS) introduced. It uses an optimized log-structured object manager to deliver significant efficiencies throughout the stack. The vSAN LFS allows ingesting writes quickly, efficiently and in a durable manner, while preparing the data and metadata for an efficient, full stripe write.

The new LFS in the ESA takes advantage of our approach to writing data resiliently by first quickly writing using a redundant mirror, and packages it in a way that allows vSAN to write the data to a stripe with parity, all while maintaining the metadata in a very efficient and fast manner.

**vSAN 8.0 Security improvements** – new vSAN 8.0 ESA architecture uses encryption, but the encryption process occurs only on the host where particular VM resides. Previously, the data needed to be decrypted from moved between caching tier and capacity tiers. This used additional CPU cycles. The new architecture minimizes CPU cost for encryption and also lowers the I/O's because data does not need to move between cache and capacity within the storage pool. There is not such a thing as cache and capacity now.

**Snapshot improvements** – The old architecture, starting with vSAN 6 introduced a “vsanSparse” snapshots. Those snapshots brought some improvements compared to of traditional snapshots based on redo-logs. However, this improvement did not resolve every problem, and there were still the slow and long snapshot consolidation times during which you could see some performance degradation.

Toggled by **storage policy**

- Enabled by default

Occurs high in the storage stack to minimize

- CPU costs
- Network payload

Minimal performance impact

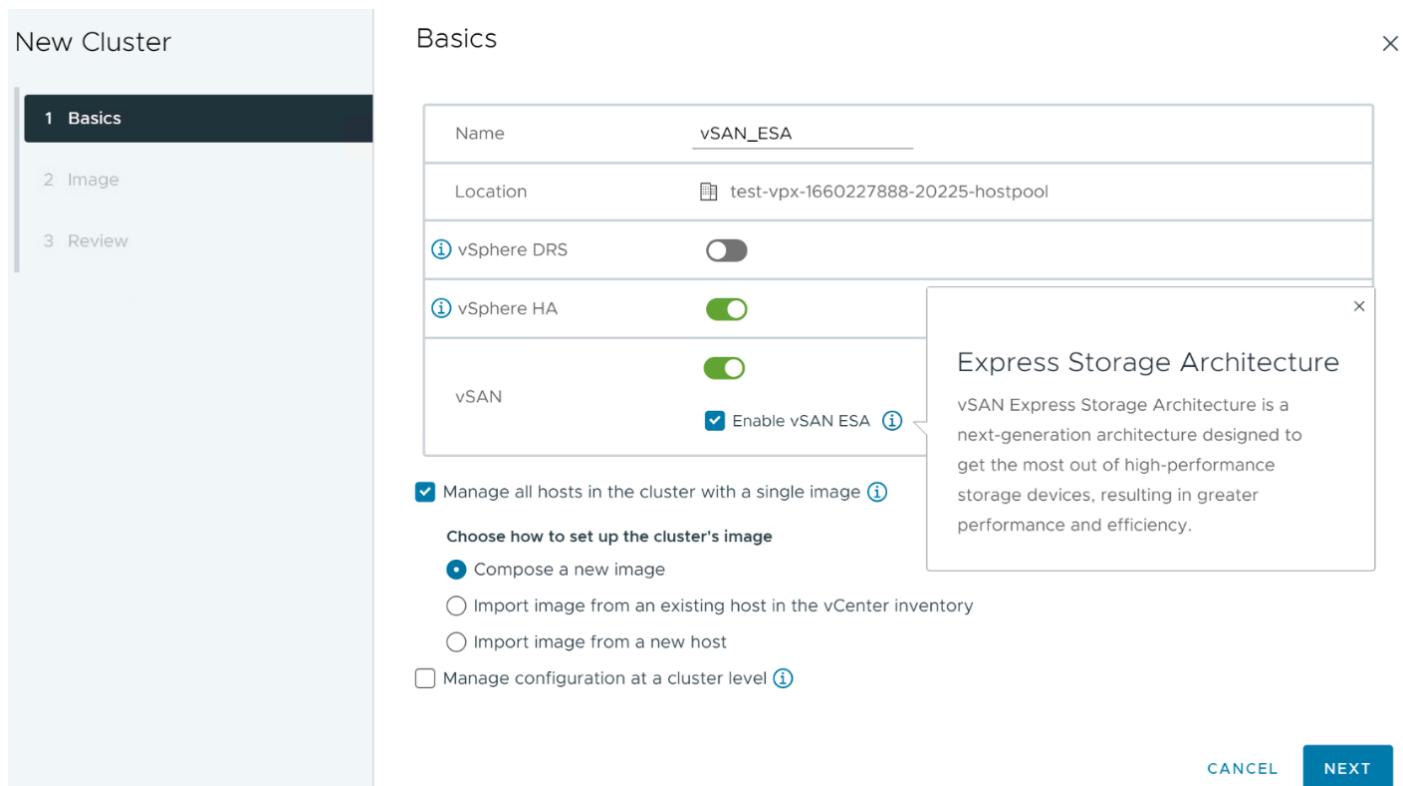
**Finer granularity** of compression rates

**Improved efficiency** with up to 8:1 compression ratios per 4KB data block

With vSAN 8.0 ESA, VMware bring a **completely new native snapshot system** that allows you to proceed with snapshot operations much faster. VMware talks about snapshot operation times going up to 100x faster consolidation times.

Also, the new snapshots are accessible by backup APIs. Imagine now when using Virtual machine backup and replication products. Imagine your backups should proceed much faster for vSAN 8.0 ESA workloads now. Good times ahead it seems. Let's see.

From the configuration perspective, all you'll see is this check box allowing you to enable vSAN ESA. If not, you uncheck and still get the good old vSAN we know.



## VMware vSAN ESA Next-Gen Architecture

### vSAN 8.0 ESA Hardware and software Requirement and Restrictions

Yes, as you can doubt, the new storage architecture needs new devices. While you don't have to use vSAN ESA Ready nodes, it's still recommended as your first step for your vSAN configuration.

- For storage, you can use NVMe devices of class D (3 Drive Writes per day – DWPD) or higher for endurance and Class F or higher for performance.
- NICs with Network speed of 25Gbps is a hard requirement.
- 2 Nodes and higher (Up to 64 Nodes). Note that 2-Node architecture needs a Witness host. (Same as traditional VSAN OSA).
- vSAN ESA only supports SSDs, so no hybrid architecture with mix of SSDs and HDDs.
- vSAN ESA supports a maximum of 24 drives per node

If your cluster already running with NVMe devices, then you might transition to vSAN 8.0 ESA easier. The ESA architecture will be able to exploit the full potential of these storage devices, and will offer what VMware say “near device-level performance” and consistency while improving operational simplicity, and driving down TCO.

If you thinking of purchasing new hardware and thinking that it will cost you more than hardware with traditional SAS/SATA devices. Think of it that ESA delivers more IOPs for more money. At the end, overall, you should end up cheaper.

## **Objective 1.8 – Describe the role of Virtual Machine Encryption in a data center**

VMware Virtual Machine (VM) encryption is an essential feature in a data center that provides an additional layer of security to virtual machines. VM Encryption ensures that virtual disks containing sensitive data are encrypted, protecting the data against unauthorized access, theft, and data breaches.

Regardless of which key provider you use, with vSphere Virtual Machine (VM) Encryption you can create encrypted virtual machines and encrypt existing virtual machines. Because all virtual machine files with sensitive information are encrypted, the virtual machine is protected. Only administrators with encryption privileges can perform encryption and decryption tasks. VM encryption will work by applying a new Storage policy to a VM.

VM Encryption is a **Policy driven feature**. You'll be able to encrypt the VMDK and the VM home files. There is **no modification within the guest OS**. It does not matter which OS you're running (Linux, Windows, DOS, iOS) or on which storage the VMs files are located (NFS, block storage, VSAN....). The **encryption is happening outside of the Guest OS**. The guest does not have an access to the keys.

The encryption works also for vMotion but both the source and the destination hosts must support it. We'll see the settings later in this post. It will get a key from the default key manager. It will be per-VM policy application model. It is easy to manage and also scalable.

If you have some unencrypted VMs, it's fairly simple to encrypt them via a policy. The example within vSphere Web client bellow – apply encryption policy to two sample VMs...Right click on vm and select **VM Policies > Edit Storage Policy**.

Select a storage policy for the virtual machines.

Storage Policy	Description
	SAN datastore.
<input type="radio"/> Management Storage Policy - Regular	Management Storage policy used for VMC regular cluster
<input type="radio"/> Management Storage Policy - Single Node	Management Storage policy used for VMC single node cluster
<input type="radio"/> Management Storage policy - Thin	Management Storage policy used for VMC regular cluster which requires THIN provisioning
<input checked="" type="radio"/> VM Encryption Policy	Sample storage policy for VMware's VM and virtual disk encryption
<input type="radio"/> Management Storage policy - Encryption	Management Storage policy used for encrypting VM
<input type="radio"/> Management Storage Policy - Stretched Lite	Management Storage policy used for smaller VMC Stretched Cluster configuration.

13 items

**i** Changing the VM storage policies for large number of virtual machines might take significant time and system resources.

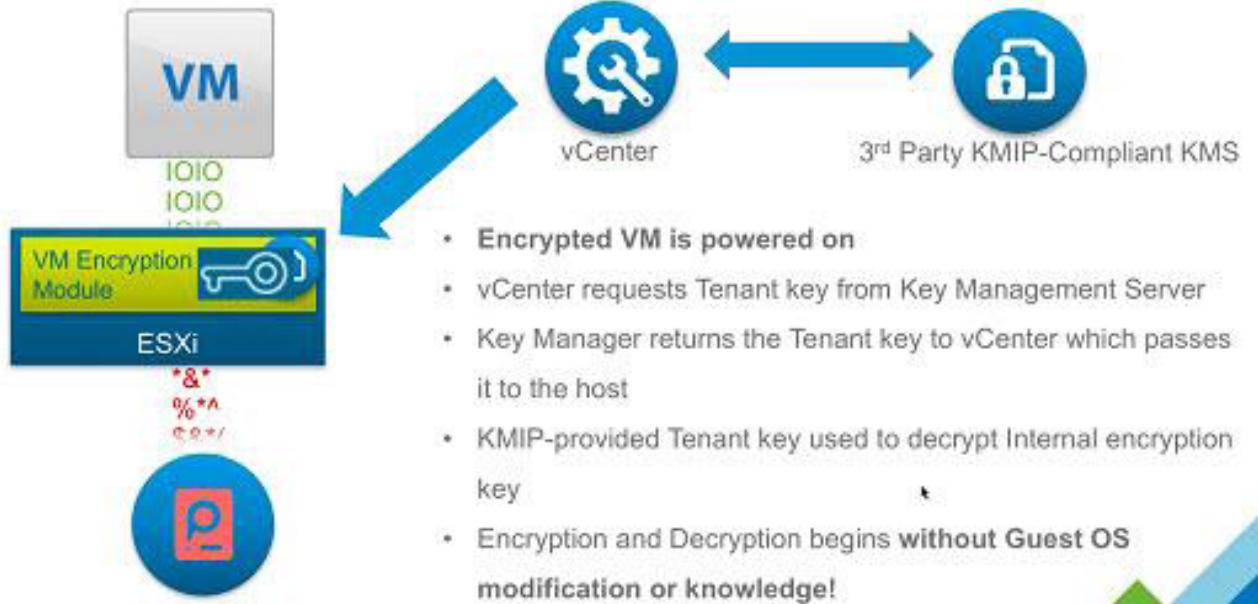
CANCEL    OK

## VM encryption – How it works?

You have an encrypted VM after you have applied an encryption policy too. Then, a randomly generated key is created for each VM, and that key is encrypted with the key from the key manager. When you power On the **VM** which has the Encryption Storage policy applied to, **vCenter** retrieves the key from the Key Manager, sends that down to the **VM encryption Module** and unlocks that key in the ESXi hypervisor.

So all **IO** coming out from the virtual SCSI device goes through the encryption module before it hits the storage module within the ESXi hypervisor. All IO coming directly from a VM is encrypted.

## VM Encryption – How it works



The workflow on activating the VM encryption would look like this:



### To Decrypt a VM?

You may ask: How do I decrypt a VM then? It is very simple. By changing the Storage Policy back to a **Datastore default**. The VM's files, the VMDKs will be decrypted.

What Components Does vSphere Virtual Machine Encryption Not Encrypt?

Some of the files that are associated with a virtual machine are not encrypted or partially encrypted.

- **Log files** – Log files are not encrypted because they do not contain sensitive data.
- **Virtual machine configuration files** – Most of the virtual machine configuration information, stored in the VMX and VMSD files, is not encrypted.
- **Virtual disk descriptor file** – To support disk management without a key, most of the virtual disk descriptor file is not encrypted

Who Manages encryption?

It is not vCenter server, which is only a **client**. The 3rd party **Key management Server (KMS)** is the one responsible for the encryption of the key and the management.

With that you may ask who will be able to manage encryption of your VMs? Does all your vSphere admins needs to have access to encryption? Possibly. But possibly NOT. VMware has created a new default role "

VMware has created a new default role "**No Cryptography Administrator**".

## Who Manages VM Encryption?



- Not all administrators should control encryption operations and have access to keys
- A new default role "No Cryptography Administrator"
- Delegation of encryption privileges to various admins via custom roles
- New vCenter crypto privileges such as Encrypt, Decrypt, Manage Keys, Clone

**ESXvirtualization** www.esxvirtualization.com

You'll find this new role within the Roles, as usually. The new role will have still all the other privileges like a "standard" admin, but less the Encryption rights.

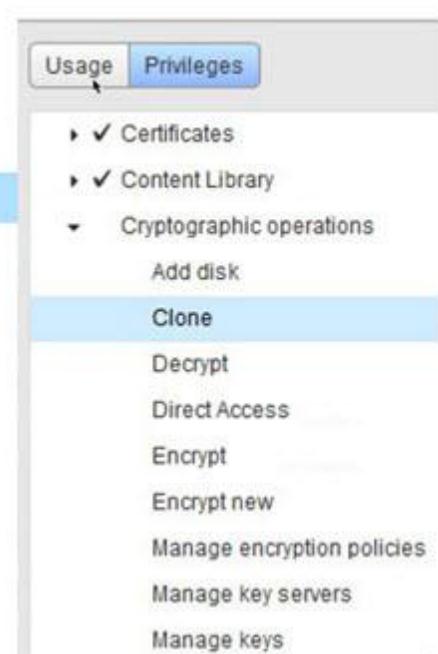
There Power ON, Off, shut down, vMotion etc...

## No operations like:

- Manage key servers
- Manage keys
- Manage encryption policies
- No console access to encrypted VMs
- No upload/download encrypted VMs

## New Role: No Cryptography Administrator

- Most of the same privileges as "Administrator"
  - Power On
  - Power Off
  - Boot
  - Shutdown
  - vMotion
  - Etc...
- Does not include any Cryptographic Operations
  - No Encrypt
  - No Decrypt
- No Console Access to Encrypted virtual machines
- No download/upload of encrypted VM's



All permissions are customizable.

## Objective 1.8.1 – Describe vSphere Trust Authority

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.

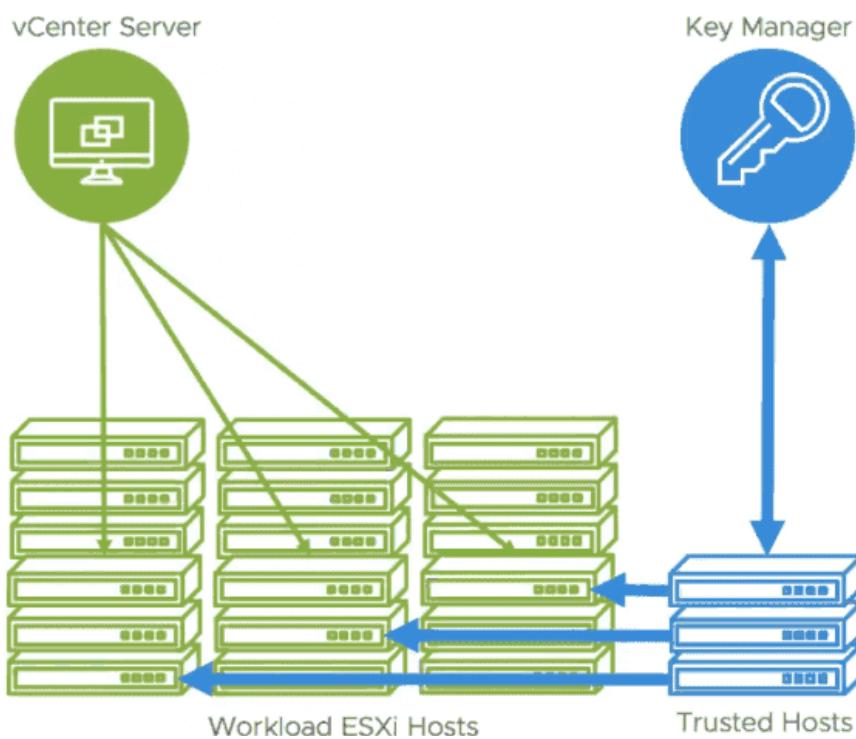
VMware is trying to work toward a better security model, and the introduction of vTA is the first step. vTA represents the foundation to which VMware will add more functions in future releases. In this release, VMware is building the base block of the architecture.

### 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 8 allow the Key Manager to talk to trusted hosts instead of the vCenter Server (which is a VM).



vSphere Trust Authority in vSphere

**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 8.0 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 1.8.2 – Describe the role of a Key Management Services (KMS) server in vSphere

It's not a «full blown» KMS server, as the NKP can only talk to vSphere and you can't point other things at it. It is a vSphere-only feature.

Traditional KMS servers provide other features that NKP does not. For example, they may offer a hardware word of trust in a hardware security module; they also provide certifications and compliance guarantees.

So, if you only want to protect your vSphere environment, you no longer need to pay for this software via external channels, as was the case with vSphere 6.7 or vSphere 6.5. But most likely you won't get all the functions that traditional KMS solutions provide. There is a reason why paid KMS solutions exist.

You can use the NKP feature for vSAN encryption, which offers **data-at-rest** or **data-in-transit** encryptions, as well as vSphere VM encryption, to protect your data. You can also set up a secure boot of ESXi servers and protect the boot environment.

Since vSphere 7 Update 2 offers TPM v2.0, and you can use it to seal sensitive information by using a TPM policy based on PCR values for UEFI Secure Boot.

VMware KMS is a necessary part of the configuration when you want to use vSphere Virtual Machine (VM) encryption to perform encryption operations. What you have to do is connect your vCenter Server to a KMS/Key Provider.

**Note:** *This does not mean that you can't continue to use your KMS if you have previously purchased that software from your vendor.*

You should also get the TPM 2.0 hardware for your servers. This is a hardware component designed to securely store information, such as credentials or measurements. It costs about \$40.



TPM hardware module from Dell

## Setup of Native Key Provider (NKP)

First, create the key provider. You'll need to log in to the vCenter Server with the vSphere Web Client and select the **vCenter Server** in the inventory list.

Click **Configure > Key Management Servers or Key Providers**.

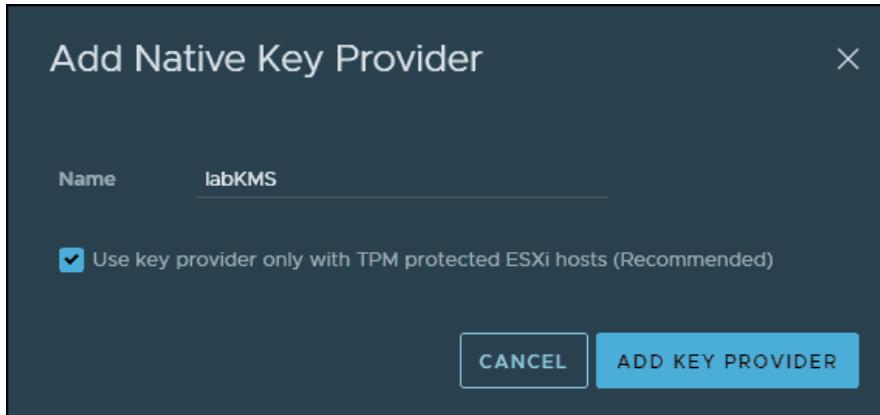
Click **Add Native Key Provider**, complete the required information, and click **Add Key Provider**.

The screenshot shows the vSphere Client interface with the following details:

- Top Bar:** Shows 'vSphere Client' and 'Menu'.
- Search Bar:** 'Search in all environments'.
- Inventory View:** Shows a tree structure with 'vcsaphoton.lab.local' selected. Under it, there are Datacenter, Cluster, and Hosts & Clusters sections.
- Current View:** 'vcsaphoton.lab.local' selected in the top navigation bar.
- Actions Bar:** Buttons for 'Summary', 'Monitor', 'Configure' (selected), 'Permissions', 'Datacenters', 'Hosts & Clusters', 'VMs', and 'Datastores'.
- Configure Tab:** Submenu for 'Key Providers'.
- Action Bar:** Buttons for 'ADD', 'BACK-UP', 'RESTORE', 'SET AS DEFAULT', 'EDIT', and 'DELETE'.
- Submenu Options:** 'Add Native Key Provider' (highlighted with a blue arrow) and 'Add Standard Key Provider'.

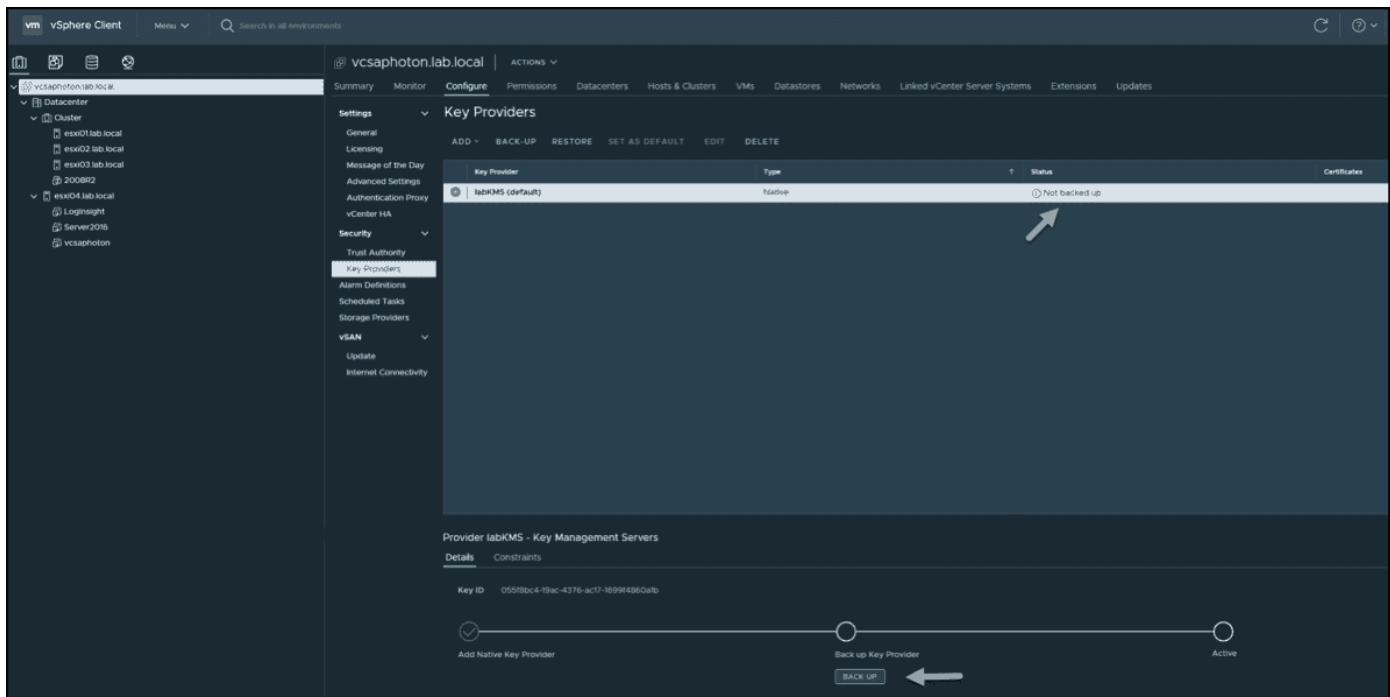
[Add Native Key Provider](#)

After it is clicked, a pop-up window asks you for a name. Enter a meaningful name.



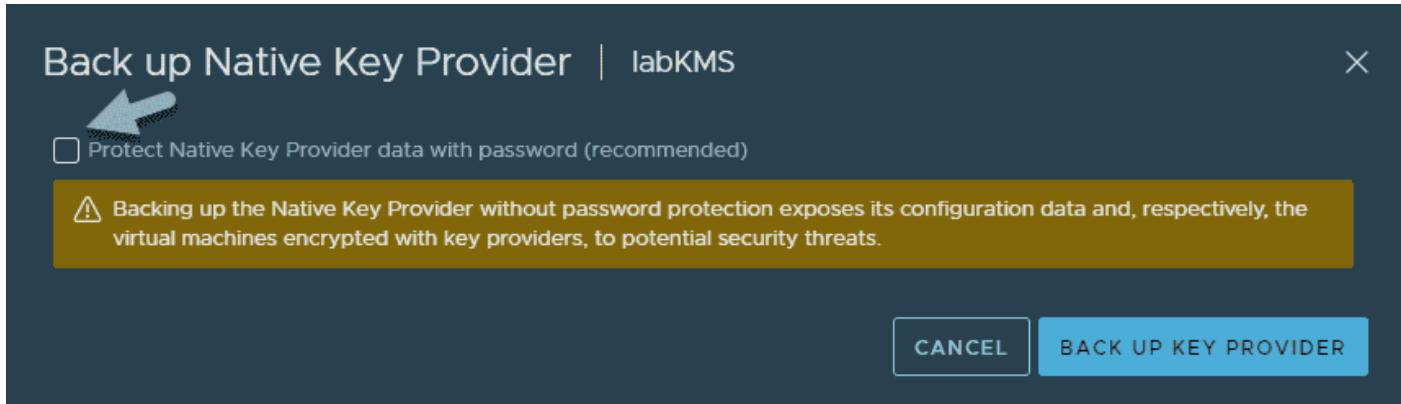
Add Native Key Provider pop up window

Once done, you can select the key provider from the list (in our case, we have only one); you'll see that the status says «not backed up» and that there is a button enabling you to perform a backup. You must back up the vSphere NKP before you can use it.



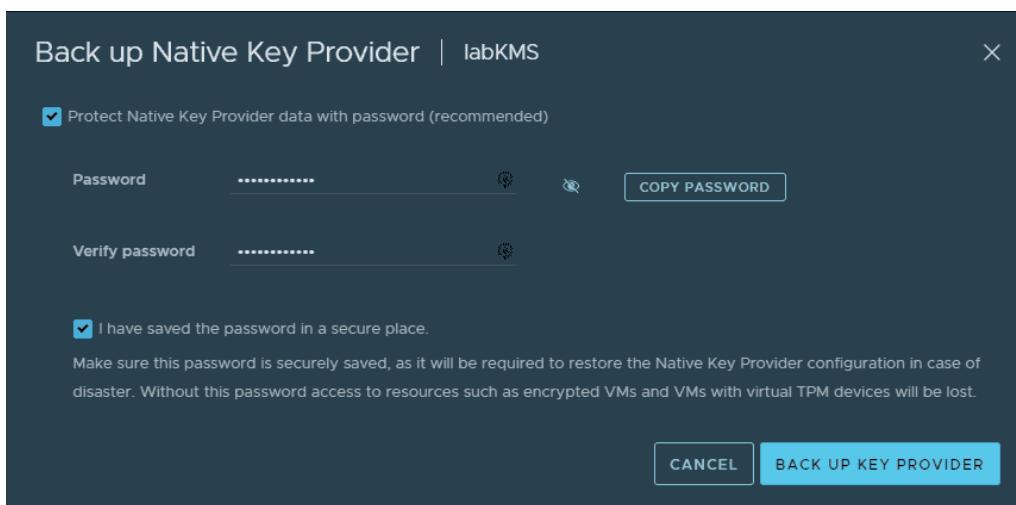
Backup of your key provider

Click the button, and you'll see another pop-up window. You can see that the «Protect Native Key Provider data with password» option is unchecked.



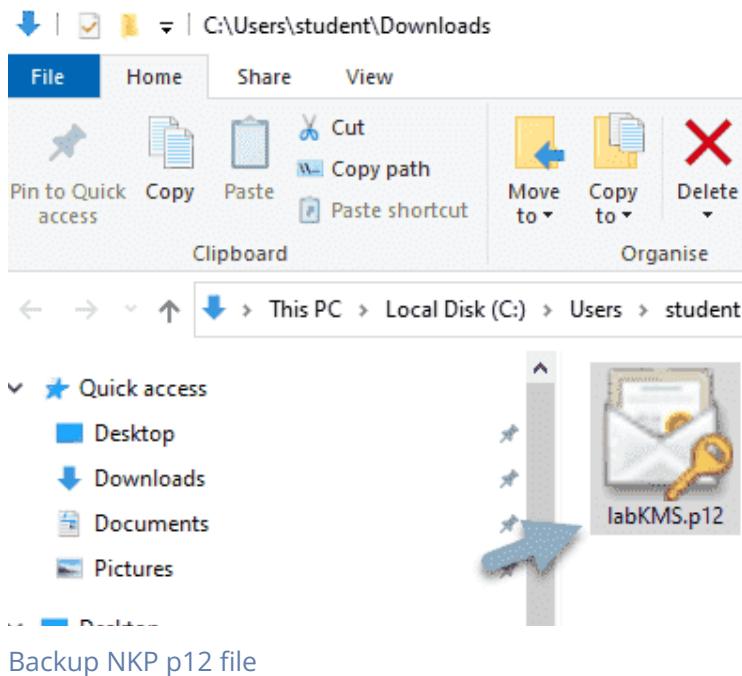
You should protect the key data with a password

Check the box and click the **Backup Key Provider** button to proceed with password creation.



Back up Native Key Provider

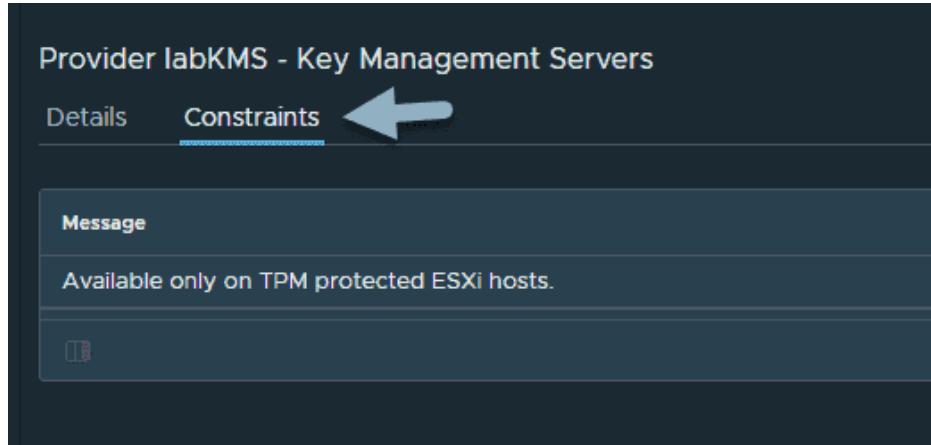
The result is a p12 file, which is automatically saved in your default browser location. In my lab example, it is in the usual Windows Downloads directory. You can then place it on a USB stick or upload it to a secure cloud location.



[Backup NKP p12 file](#)

In the notification area, click **Constraints**. A message is displayed indicating that this KMS is «Available only on TPM protected ESXi hosts». If you remember, at the beginning of our tutorial, we checked the box saying that our hosts have the TPM hardware installed.

The TPM hardware should be configured in each ESXi host's BIOS to use the SHA-256 hashing algorithm and the TIS/FIFO (first-in, first-out) interface, not the command response buffer (CRB).



[Available only on TPM protected ESXi hosts](#)

**Note:** vSphere NKP is backed up as part of the vCenter Server file-based backup (if you set it up). However, you must back up the vSphere NKP at least once before you can use it.

vCenter Server creates an alarm if the NKP has not been backed up. If this happens, it will send you a notification every 24 hours. I think it's good to know when planning your infrastructure deployments or upgrades.

Another very important tip. When creating the backup of the NKP, you **should be logged in**

**to the vCenter Server via fully qualified domain name (FQDN) and not via IP address.** If not, the backup will not finish.

If you're using Enhanced Link Mode configuration with several vCenter Servers linked together, you **must do this backup on the vCenter Server to which the key provider belongs.**

The backup process might take some time as the vCenter Server needs to push the information to all ESXi hosts in the data center. The status changes from **Not Backed** to **Warning** to **Active**. Once done, you're good to go and continue with other tasks before using encryption in your vSphere environment.

### Some tips for using TPM

If you want to protect your data against theft, you should buy TPMs for your servers and store the keys in the TPM instead of on the boot devices. If someone steals a few hard drives from a host, most likely he will not be able to walk away with the heavy server itself.

Make a backup of your keys and set a password; then, be sure to put it in a safe location. You can use a USB key or online storage in a cloud location, but be sure that you and a member of your security team are the only ones that have access.

Be sure you protect your file-level backup of your vCenter Server Appliance (VCSC), as those keys are backed up via this mechanism. If anyone gets their hands on those backups, they pretty much have access to your encrypted environment, as they can recover the keys from those backups.

## Objective 1.9 – Recognize methods of securing virtual machines

Virtualization is one of the most popular technologies in modern IT infrastructure, offering numerous benefits such as improved resource utilization, scalability, and flexibility. One of the most widely used virtualization platforms is VMware vSphere, which enables the creation and management of virtual machines (VMs) on a single physical server. While virtualization provides many advantages, it also introduces new security challenges that need to be addressed.

**Enable Encryption** – Encrypting virtual machines is one of the most effective ways of securing data stored on them. You can use the built-in Key Management Server (KMS) that is free, or you can add your KMS if you already have one. With VMware vSphere 8.0, it is possible to encrypt virtual machines at rest and in motion. Virtual machine encryption is a feature that encrypts virtual machine files and virtual disks, making it harder for attackers to access sensitive data. Additionally, network encryption is another feature that encrypts data in motion between virtual machines and networks, which prevents attackers from intercepting the data.

**Use Virtual Machine Isolation** – You can isolate VMs running by segregating network traffic via VLANS. VMs can run also in a sandboxed environment that isolates them from other virtual machines and the host system and from the internet. By isolating virtual machines, administrators can prevent unauthorized access to sensitive data and reduce the risk of malware spreading from one virtual machine to another.

**Implement Access Controls** – Access control is a fundamental security measure that limits access to resources based on the user's identity and privileges. VMware vSphere 8.0 provides several access control mechanisms, including role-based access control (RBAC) and virtual machine permissions. By implementing access controls, administrators can restrict access to virtual machines, preventing unauthorized users from accessing sensitive data or making changes to virtual machine configurations.

**Activate or Deactivate UEFI Secure Boot for a Virtual Machine** – UEFI Secure Boot is a security standard that helps ensure that your OS boots using only software that is trusted by the PC manufacturer. For certain virtual machine hardware versions and operating systems, you can activate secure boot just as you can for a physical machine.

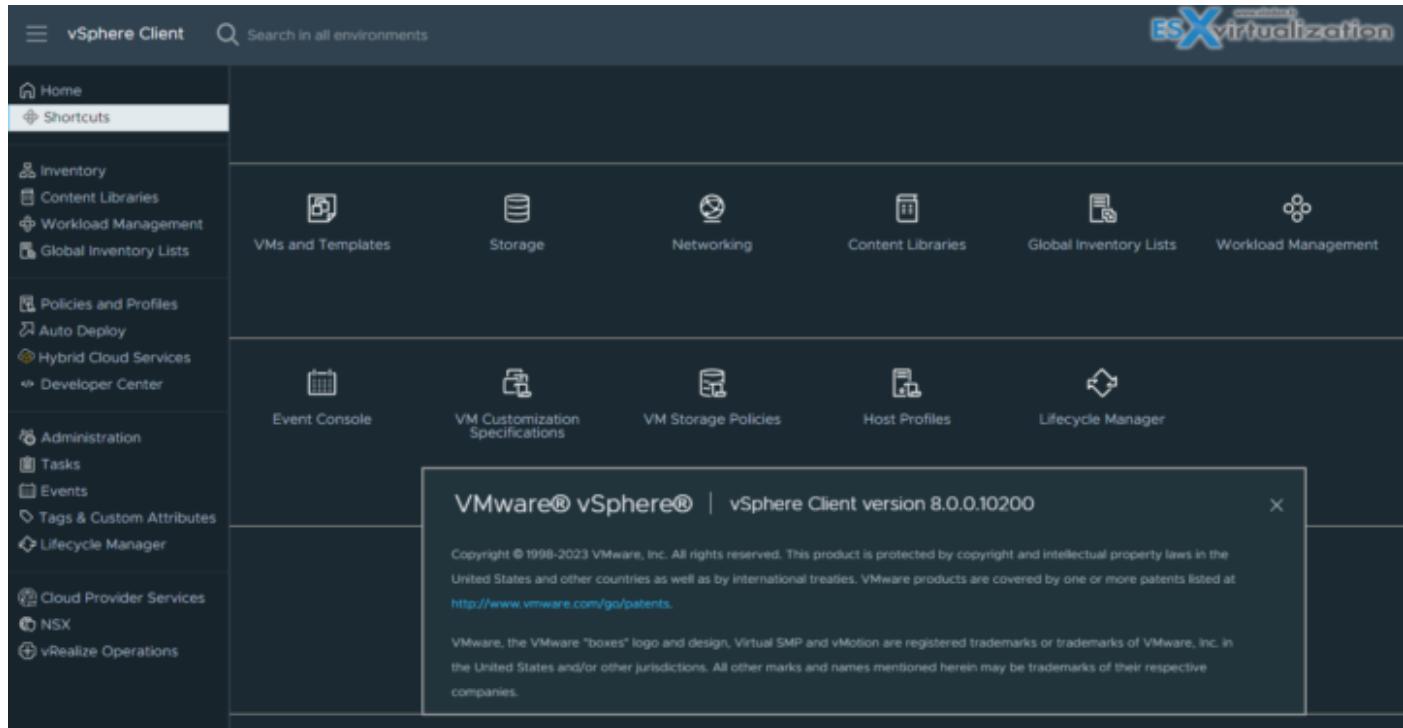
**Apply Security Patches and Updates** – More than ever, this is crucial today, when zero day vulnerabilities and ransomware are spreading very fast. Security patches and updates are crucial in maintaining the security of virtual machines. VMware regularly releases security patches and updates for vSphere, which include bug fixes and vulnerability patches. By applying these patches and updates, administrators can keep virtual machines secure and reduce the risk of attacks.

**Securing Virtual Machines with Intel Software Guard Extensions** – vSphere enables you to configure Virtual Intel® Software Guard Extensions (vSGX) for virtual machines. Using vSGX enables you to provide additional security to your workloads

**Use Antivirus and Anti-Malware Software** – I should not even talk about this one, which is a must. Antivirus and anti-malware software are essential tools in protecting virtual machines from malware and other security threats. VMware vSphere 8.0 supports the use of third-party antivirus and anti-malware software, which can be installed directly on the virtual machines. By using these tools, administrators can detect and remove malware, preventing it from spreading to other virtual machines or the host system.

**Use Templates to Deploy Virtual Machines** – When you manually install guest operating systems and applications on a virtual machine, you introduce a risk of misconfiguration. By using a template to capture a hardened base operating system image with no applications installed, you can ensure that all virtual machines are created with a known baseline level of security.

## vSphere 8



**Deactivate Unnecessary Functions Inside Virtual Machines** – Any service that runs in a virtual machine provides the potential for attack. By deactivating system components that are not necessary to support the application or service that is running on the system, you reduce the attack potential

## Objective 1.9.1 – Recognize use cases for a virtual Trusted Platform Module (vTPM)

A vTPM is a software-based version of a TPM that is used in virtualized environments, such as VMware vSphere 8. Quote VMware documentation here:

*vTPMs provide hardware-based, security-related functions such as random number generation, attestation, key generation, and more. When added to a virtual machine, a vTPM enables the guest operating system to create and store keys that are private. These keys are not exposed to the guest operating system itself. Therefore, the virtual machine attack surface is reduced. Usually, compromising the guest operating system compromises its secrets, but enabling a vTPM greatly reduces this risk. These keys can be used only by the guest operating system for encryption or signing. With an attached vTPM, a client can remotely attest the identity of the virtual machine, and verify the software that it is running.*

There are some concerns that you should be aware of when willing to backup VMs with vTPM enabled.

### Quote:

When you back up a virtual machine enabled with a vTPM, the backup must include all virtual machine data, including the \*.nvram file. If your backup does not include the \*.nvram file, you cannot restore a virtual machine with a vTPM. Also, because the VM home files of a vTPM-enabled virtual machine are encrypted, ensure that the encryption keys are available at the time of a restore.

Other than that, you can configure vTPM even if your ESXi does not have a physical TPM 2.0 chip installed. However, if you want to perform host attestation, an external entity, such as a TPM 2.0 physical chip, is required.

The screenshot shows the 'Customize hardware' step of the 'New Virtual Machine' wizard. The left sidebar lists steps 1 through 8, with '7 Customize hardware' currently selected. The main area displays hardware configuration options for a new VM. A blue arrow points from the 'Security Devices' section to the 'Trusted Platform Module' option in the 'ADD NEW DEVICE' dropdown menu. The compatibility note at the bottom states: 'Compatibility: ESXi 8.0 and later (VM version 20)'.

New Virtual Machine

Customize hardware

Configure the virtual machine hardware

Virtual Hardware    VM Options    Advanced Parameters

ADD NEW DEVICE ▾

Disks, Drives and Storage  
Hard Disk  
Existing Hard Disk  
RDM Disk  
Host USB Device  
NVDIMM  
CD/DVD Drive

Controllers  
NVMe Controller  
SATA Controller  
SCSI Controller  
USB Controller

Other Devices  
PCI Device  
Trusted Platform Module

Watchdog Timer  
Precision Clock  
Serial Port

Network  
Network Adapter

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

CPU: 2

Memory: 4 GB

New Hard disk \*: 30 GB

Maximum Size: 45.75 GB

VM storage policy: Management Storage policy - Thin

Location: Store with the virtual machine

Disk Provisioning: Thin Provision

Sharing: Unspecified

Disk Mode: Dependent

Virtual Device Node: New SCSI controller ▾ SCSI(0:0) New Hard disk ▾

New SCSI controller: LSI Logic SAS

New Network: starwindiscsi ▾ Connected

New CD/DVD Drive: Client Device ▾ Connected

New USB Controller: USB 3.1

Video card: Specify custom settings

New SATA Controller: New SATA Controller

Security Devices: Not Configured

Other: Additional Hardware

Compatibility: ESXi 8.0 and later (VM version 20)

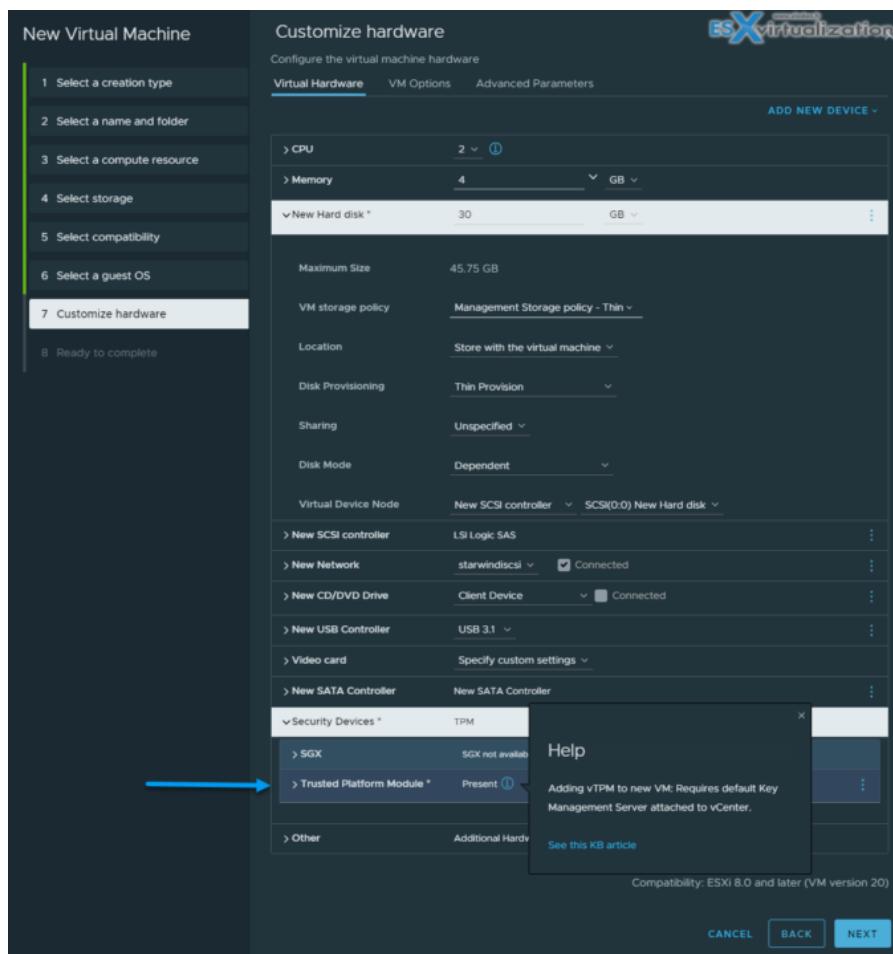
CANCEL    BACK    NEXT

Virtualization has revolutionized the way we think about server infrastructure and the management of data centers. VMware vSphere 8 is one of the most popular virtualization platforms on the market today, and it offers a wide range of features to help businesses optimize their infrastructure. One of the most interesting features of VMware vSphere 8 is the virtual Trusted Platform Module (vTPM). In this blog post, we will explore the use cases for a vTPM within VMware vSphere 8.

Now that we understand what a vTPM is, let's explore some of the use cases for it within VMware vSphere 8:

**Enhanced Security for Virtual Machines** – One of the most obvious use cases for a vTPM is to enhance the security of virtual machines (VMs) running on the VMware vSphere 8 platform. By leveraging the secure storage and cryptographic capabilities of a vTPM, VMs can be better protected against attacks that attempt to compromise their data. This is particularly important for VMs that run critical workloads, such as financial or healthcare applications, that require a high level of security.

**Compliance with Industry Standards** – Many industries, such as finance and healthcare, have specific regulatory requirements that must be met when it comes to data security. The use of a vTPM within VMware vSphere 8 can help businesses comply with these standards by providing a secure platform for storing cryptographic keys and other sensitive data.



**Encryption of Virtual Disks** – Another use case for a vTPM within VMware vSphere 8 is the encryption of virtual disks. By using a vTPM to securely store the encryption keys, VMs can be protected against attacks that might try to access or modify their virtual disks. This can be particularly important for VMs that store sensitive data, such as credit card numbers or patient health records.

**Protection of Cloud Infrastructure** – VMware vSphere 8 is often used in cloud environments where businesses rely on the platform to provide critical services. By using a vTPM, businesses can help protect their cloud infrastructure against attacks that might try to compromise the security of the underlying platform. This can help ensure that business-critical applications and services remain available and secure.

In conclusion, the use of a virtual Trusted Platform Module (vTPM) within VMware vSphere 8 can provide businesses with a wide range of benefits, including enhanced security for virtual machines, compliance with industry standards, encryption of virtual disks, protection of intellectual property, secure multi-tenancy, and protection of cloud infrastructure. As virtualization continues to become more prevalent in modern data centers, the use of vTPMs is more and more necessary for certain workloads.

## **Objective 1.9.2 – Differentiate between Basic Input or Output System (BIOS) and Unified Extensible Firmware Interface (UEFI ) firmware**

**BIOS** – legacy, old

**UEFI** – Unified Extensible Firmware Interface (UEFI) is an interface between the operating system and the platform firmware. UEFI has architectural advantages over Basic Input/Output System (BIOS) firmware.

When installing a new VM, depending on the guest operating system, you might have the option of enabling UEFI Secure Boot. UEFI Secure Boot secures the boot process by preventing the loading of drivers and operating system loaders that are not signed with an acceptable digital signature.

UEFI stores all the information about initialization and startup in a **.efi file**, a file stored on a special partition called **EFI System Partition (ESP)**.

As of vSphere 6.7 Update 3, the default firmware for creating a Windows 10 and Windows Server 2016 guest OS is now EFI. So old BIOS for Windows VMs is going away from the security standpoint, speed etc.

## Example BIOS screen



## In General – Advantages UEFI over BIOS

Firmware is the embedded software that provides low-level control over the hardware components of a computer. It is the interface between the hardware and the operating system. Two of the most commonly used firmware technologies in personal computers are BIOS and UEFI.

BIOS (Basic Input/Output System) has been the standard firmware interface used in personal computers since the 1980s. However, with the introduction of UEFI (Unified Extensible Firmware Interface), many computer manufacturers have started to shift from BIOS to UEFI. This shift has occurred due to the advantages of UEFI over BIOS. In this blog post, we will discuss the advantages of UEFI over BIOS.

**1. Faster boot times** -UEFI has been designed to boot up faster than BIOS. This is because UEFI initializes the hardware components in parallel, whereas BIOS initializes them in a sequential manner. With UEFI, the computer can boot up in a matter of seconds, whereas with BIOS, it may take several seconds or even minutes.

**2. Large disk support** – BIOS was designed for computers with disk drives of 2.1GB or less. With the advent of larger hard drives, BIOS became obsolete. UEFI, on the other hand, was designed to support hard drives larger than 2.1GB. This means that UEFI can support the latest high-capacity hard drives and solid-state drives.

- 3. Secure boot** – UEFI includes a feature called Secure Boot, which helps protect the computer from malware during the boot process. Secure Boot ensures that only trusted software can boot on the computer. This prevents malware from infecting the boot process and compromising the security of the computer.
- 4. Multiple OS support** – Whereas BIOS allows a single boot loader, UEFI lets users install multiple loaders. You can use loaders for Debian-based Ubuntu and other Linux variants, along with Windows OS loaders, in the same EFI system partition.
- 5. Graphics support** – BIOS has limited graphics support and cannot provide a graphical user interface (GUI) during the boot process. UEFI, on the other hand, provides advanced graphics support and can display a GUI during the boot process. This makes it easier to interact with the computer during the boot process and provides a better user experience.
- 6. Remote diagnostics and repair** – UEFI provides remote diagnostics and repair capabilities, which can be very useful for IT administrators. With UEFI, IT administrators can diagnose and repair computers remotely, without the need for physical access to the computer. This saves time and reduces downtime, which can be critical in a business environment.
- 7. More flexible** – UEFI is more flexible than BIOS and allows for more customization. This means that computer manufacturers can customize the UEFI firmware to suit their needs. They can add new features and functionality to the firmware, which can improve the performance and reliability of the computer.

In conclusion, UEFI offers many advantages over BIOS. It provides faster boot times, large disk support, secure boot, advanced graphics support, remote diagnostics and repair capabilities, and more flexibility. As computer hardware continues to evolve, UEFI will become the standard firmware interface used in personal computers.

## Quick FAQ

**What is the difference between UEFI and BIOS?** – BIOS and UEFI are two firmware interfaces for computers to start the operating system. BIOS uses the Master Boot Record (MBR) to save information about the hard drive data while UEFI uses the GUID partition table (GPT). Compared with BIOS, UEFI is more powerful and has more advanced features. It is the latest method of booting a computer, which is designed to replace BIOS. In brief, UEFI is the successor to BIOS.

**Should I use UEFI or BIOS?** – UEFI progressively replaces the old-school BIOS on most modern PCs as it brings more security features than the legacy BIOS mode and also boots faster than Legacy systems. If your computer supports UEFI firmware, you should convert MBR disk to GPT disk to use UEFI boot instead of BIOS.

**What is UEFI boot mode?** – During the POST procedure, the UEFI firmware scans all of the bootable storage devices that are connected to the system for a valid GUID Partition Table

(GPT). UEFI stores all the information about initialization and startup in an .efi file that is saved on a special partition called EFI System Partition (ESP). If the EFI bootable partition is not found, the firmware may revert to the old BIOS Boot method. If both UEFI boot and Legacy boot fail, you may receive the disk boot failure error message.

**What is the advantage of UEFI boot?** – UEFI Supports unlimited number of partitions, and support the disk which is larger than 2 TB. Computers that use UEFI firmware can boot faster than BIOS, as no magic code must execute as part of booting. UEFI also has more advanced security features such as secure startup, which helps to keep your computer more secure.

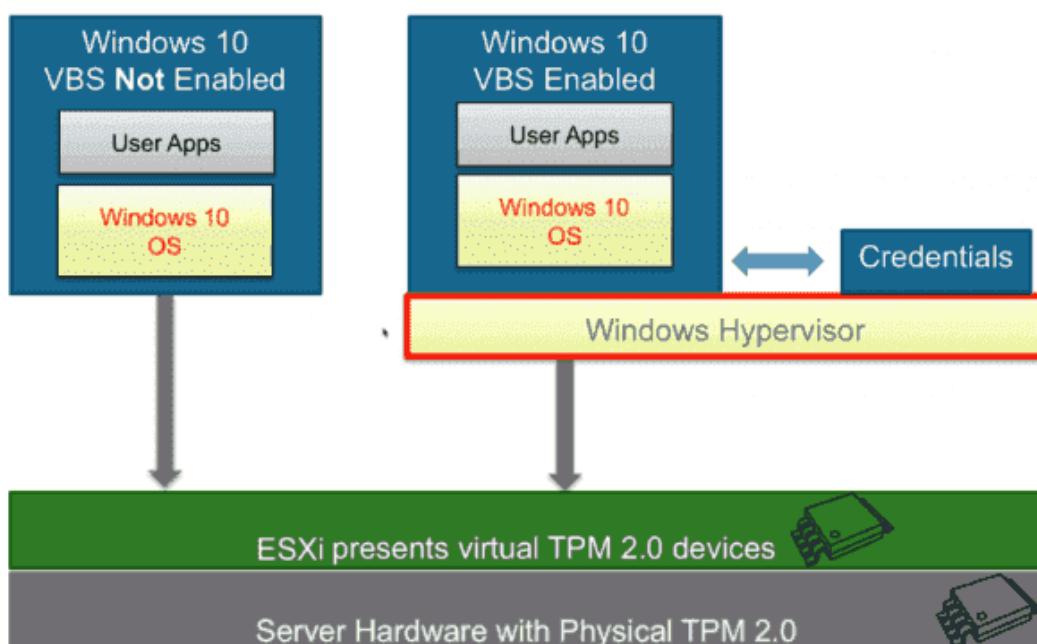
## Objective 1.9.3 – Recognize use cases for Microsoft virtualization-based security (VBS)

### What is Virtualization-based Security (VBS)?

VBS uses hardware and software virtualization features to enhance Windows system security by creating an isolated, hypervisor-restricted, specialized subsystem.

Basically, Microsoft is using a Windows role (or component) called the Hyper-V role, which boots the OS. This hypervisor allows Microsoft to isolate some sensitive information in places that would normally be accessible to the OS. Here we can think of cached credentials and such things.

Most modern systems have a Trusted Platform Module (TPM) 2.0 device built into the hardware. However, someone had to do it in software. And this is the goal. To give you an idea, here is a screenshot from a VMware blog post.



As you can see, the Windows 10 virtual machine (VM) has a hypervisor role active and has the credentials stored elsewhere.

### What are the restrictions on VBS-enabled VMs?

VBS is only usable on Windows 10 and Windows Server 2016, and vSphere features exist that are not compatible with VBS:

- VMware Fault Tolerance (FT)
- vSphere PCI passthrough
- vSphere hot add for CPU or memory

### What are the vSphere requirements for VBS?

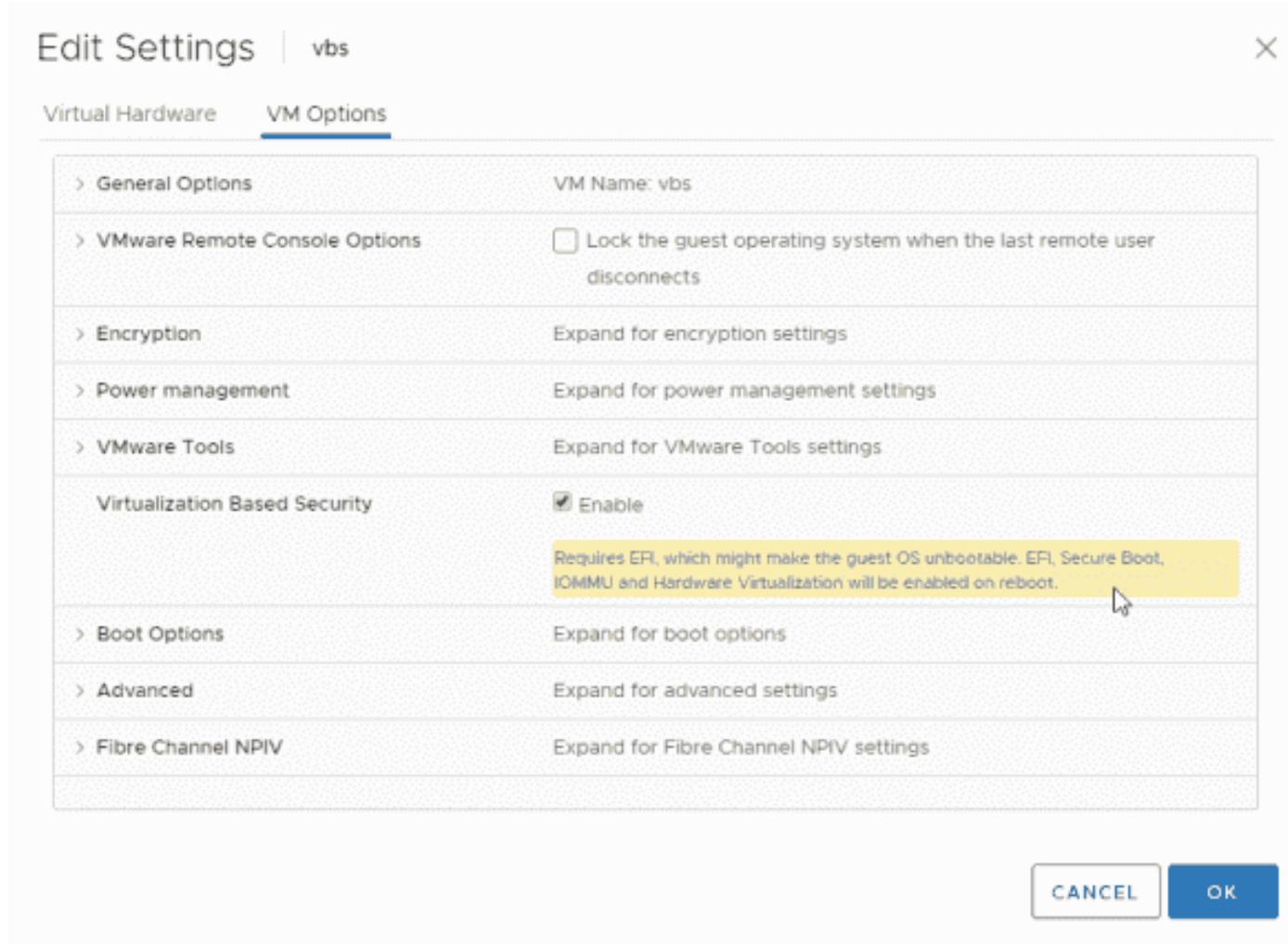
As mentioned above, VBS is only available as of vSphere 6.7. The requirements for working with VBS are:

- A VM with virtual hardware 14
- Hardware virtualization and an input/output memory management unit (IOMMU) exposed to the VM
- Secure boot enabled
- EFI firmware
- 64-bit CPU
- Intel VT-d or AMD-Vi ARM64 system memory management units (SMMUs)
- TPM 2.0

### How do you enable VBS?

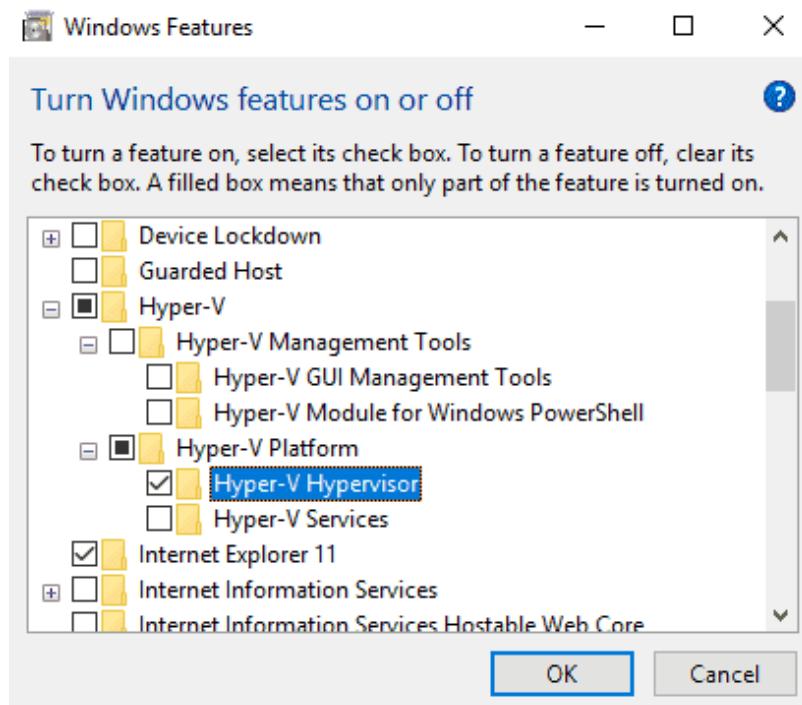
In the VMware vSphere client, first connect to vSphere and select the VM for which you want to enable VBS.

1. Shut down the VM and tick the **Enable** box next to **Virtualization Based Security** under VM Options.



**Note:** The VM has to be booting EFI (not BIOS) to satisfy the requirements. If you are creating new Windows 10 or Windows 2016 VMs, you should make sure you are selecting UEFI firmware before installing. After installing the system, it is pretty difficult to switch.

And once the VM is up and running, we'll need to activate the Hyper-V role. You can do this through a simple command **appwiz.cpl**, which automatically brings up the window where we select Add/Remove **Turn Windows features on and off**. Once there, we can look for the Hyper-V section and check the box **Hyper-V Hypervisor**.



Enabling the Hyper V Hypervisor

If you want to add a Hyper-V role on Windows Server 2016, you'll use the **Add roles and features** wizard within your Server Manager.

Once you're done, it'll ask you to **reboot the system**.

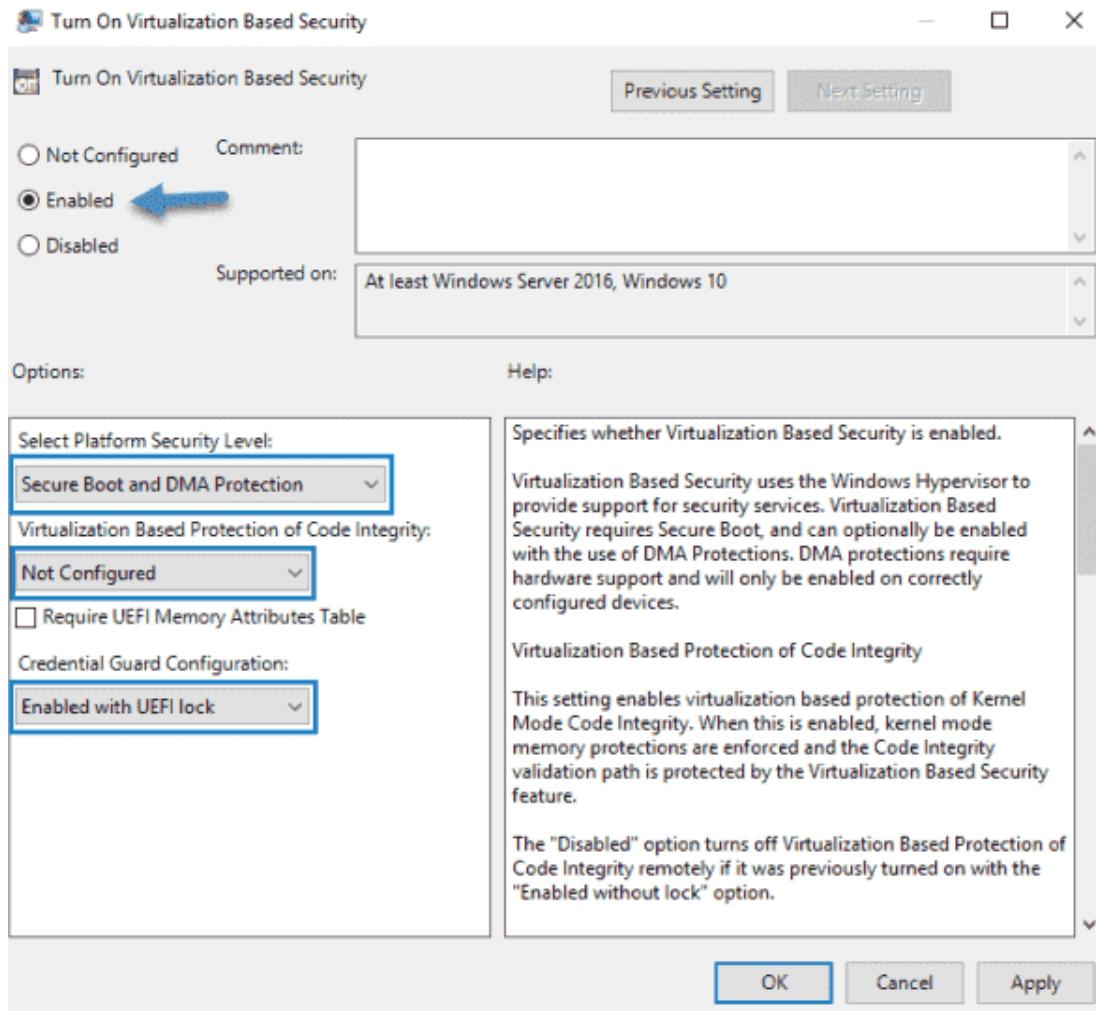
Let's continue after the VM comes up.

1. In the VM, open **gpedit.msc** and browse to:

**Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security**. Set it to **Enable** and configure the options as follows:

- Select Platform Security Level: Secure Boot and DMA Protection
- Virtualization Based Protection of Code Integrity: Enabled with UEFI lock
- Credential Guard Configuration: Enabled with UEFI lock

If you want to be able to turn off Windows Defender Credential Guard remotely, choose **Enabled without lock**.



#### Credential Guard configuration

If you want to activate VBS for multiple systems, you can do this via Group Policy in your domain.

## Objective 1.10 – Describe identity federation

vSphere 7 has brought the Identity Federation feature, so it is not new in vSphere 8. Identity Federation allows you to attach vCenter Server to enterprise identity providers like Active Directory Federation Services (ADFS). Corporate users can use the same methods to log into vCenter Server as they do their desktops or in their cloud workloads. vSphere 7 and 8 versions support MFA & 2FA.

vCenter Server 8, if attached to the identity provider, the vSphere Client will redirect logins to the provider's login page. The user can log-in by using their corporate credentials, with including any MFA that is configured as part of the system.

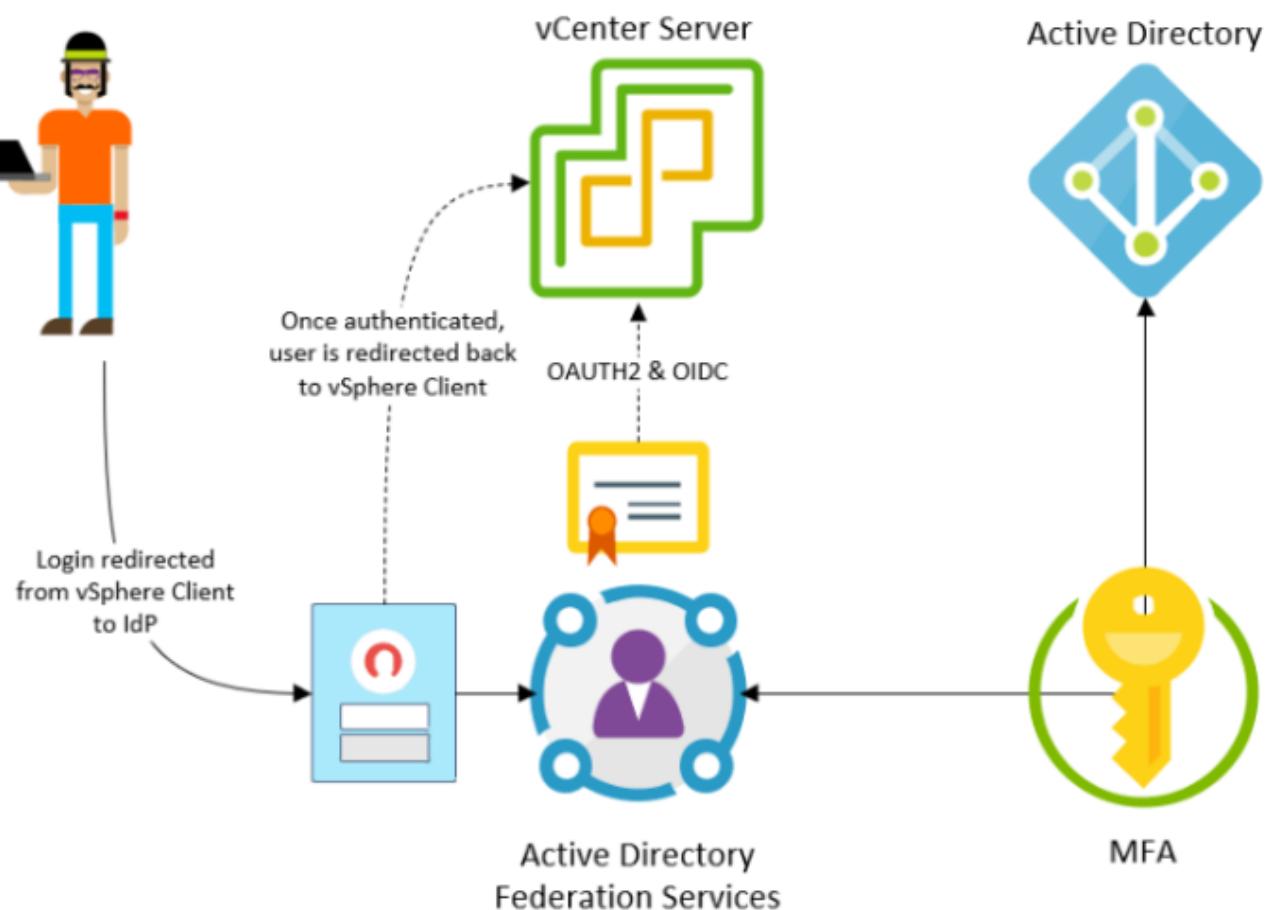
Once authenticated, the identity provider redirects those clients back to the vSphere Client with a cryptographic token that authorizes them. You can see similar technology used when you basically log into your Google, FB or [Twitter](#) accounts....

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. Screenshot from VMware



vSphere Identity Federation will basically allow 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.

In this initial release, vSphere and ADFS will support some additional providers, such as Azure AD, PingID, Okta, vIDM, and others.

## Objective 1.10.1 – Describe identity federation

Already described in 10.1

## Objective 1.10.2 – Recognize use cases for identity federation

Identity federation enables organizations to integrate their existing identity systems with [vSphere 8](#) to provide seamless authentication and authorization across their virtualized environments. You can use Single Sign-On with existing federated infrastructure and applications and improve data center security because vCenter Server never handles the user's credentials. vCenter server allows you to use the authentication mechanisms, such as multi-factor authentication, supported by the external identity provider. In this blog post which is part of our [community study guide towards VCP-DCV certification based on vSphere 8.x](#), we will explore the use cases of VMware vSphere 8 identity federation and how it can benefit organizations.

VMware vSphere 8 supports identity federation through the use of industry-standard protocols, such as Security Assertion Markup Language (SAML) and OpenID Connect (OIDC). These protocols allow vSphere 8 to integrate with existing identity systems, such as Active Directory or LDAP, and enable users to authenticate using their existing credentials.

### Use Cases for VMware vSphere 8 Identity Federation

#### 1. Multi-Cloud Environments

Many organizations use multiple clouds to meet their business needs, and managing identities across different clouds can be a significant challenge. VMware vSphere 8 identity federation enables organizations to provide single sign-on (SSO) access to resources across different clouds, simplifying identity management and enhancing security.

For example, suppose an organization has a private cloud deployed using vSphere 8 and also uses a public cloud service such as AWS or Azure. In that case, identity federation enables users to access resources across both environments using a single set of credentials. This eliminates the need for users to maintain separate sets of credentials for each cloud, simplifying the user experience and reducing the risk of credential theft.

#### 2. Cross-Organizational Collaboration

Identity federation is also useful for organizations that collaborate with external partners or contractors. In such cases, it is essential to ensure that users from different organizations

can access resources securely and efficiently. VMware vSphere 8 identity federation enables organizations to share resources across different domains or vCenter servers securely.

For example, suppose two organizations need to collaborate on a project that requires access to shared resources hosted on a vSphere 8 environment. In that case, identity federation enables users from both organizations to access these resources using their existing credentials, without the need to create new accounts or passwords.

### 3. User Mobility

In today's fast-paced business environment, users need to access resources from anywhere and at any time. VMware vSphere 8 identity federation enables users to access resources securely and efficiently from any device or location.

For example, suppose a user needs to access resources hosted on a vSphere 8 environment from a remote location or using a mobile device. In that case, identity federation enables the user to authenticate using their existing credentials, providing seamless access to the resources they need.

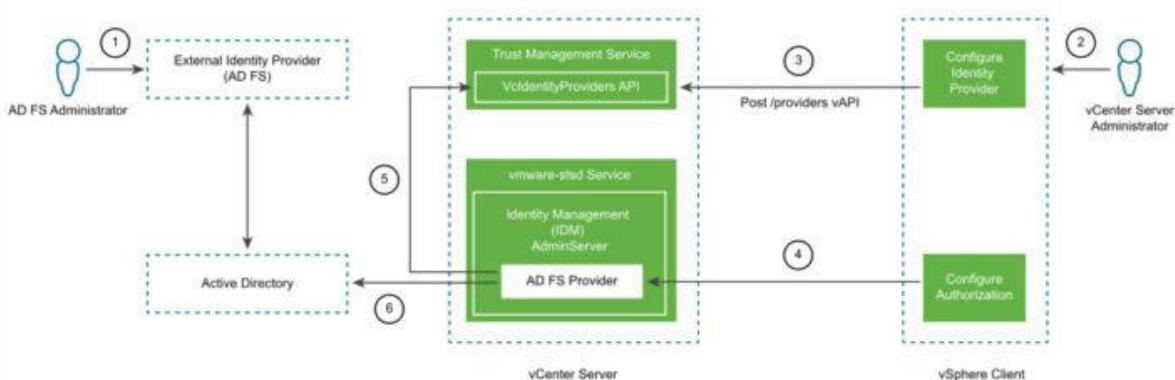
### 4. Compliance and Security

Identity federation is a critical component of security and compliance in today's digital landscape. VMware vSphere 8 identity federation enables organizations to enforce security policies across different domains and vCenter servers, ensuring that users have access to only the resources they are authorized to access.

For example, suppose an organization needs to ensure that only authorized users can access sensitive resources hosted on a vSphere 8 environment. In that case, identity federation enables the organization to enforce policies such as multi-factor authentication (MFA) or role-based access control (RBAC) across different domains and vCenter servers, ensuring that only authorized users can access the resources.

Example of configuration flow from VMware Documentation below

vCenter Server Identity Provider Federation Configuration Process Flow



vCenter server identity provider federation configuration process flow

## Objective 1.11 – Describe VMware vSphere Distributed Services Engine

Formerly project Monterey, the vSphere Distributed Services Engine, allows you to improve infrastructure performance by using the Data Processing Units (DPU) for hardware accelerated data processing to improve the performance of the whole infrastructure. With vSphere 8, the applications will be able to benefit from those features. Admins will be able to simplify DPU lifecycle management and boost infrastructure security with NSX.

Project Monterey:

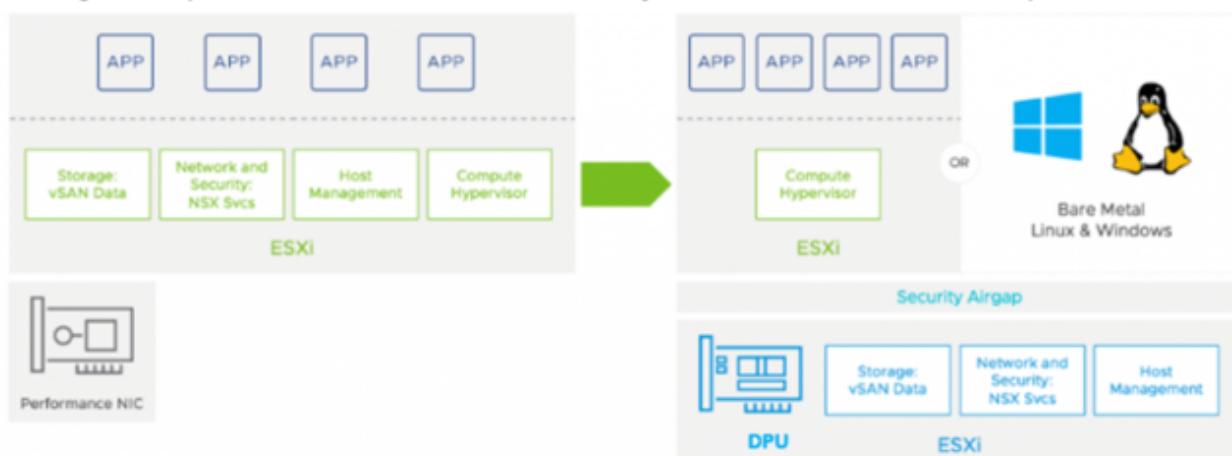
*"Project Monterey reimagines the virtual infrastructure as a distributed control fabric through tight integration with DPUs (Data Processing Unit – also known as SmartNICs). VMware is leading an industry wide initiative to deliver a solution for its customers by bringing together the best of breed DPU silicon (NVIDIA, Pensando Systems, Intel) and server designs (Dell Technologies, HPE, Lenovo)."*

What's DPU?

DPU is sitting at the hardware layer. Any PCIe devices (graphics, nic...). The ESXi, at the top layer, with the DPU and NSX services underneath. A second instance of the ESXi is directly running in the DPU which allows offloading of some of the ESXi services to the DPU for increased performance. This technology can free CPU cycles that then can be used for running workflows.

Screenshot from VMware

Starting with vSphere 8.0, VMware moves functionality that runs on the core CPU complex to the DPU CPU complex:



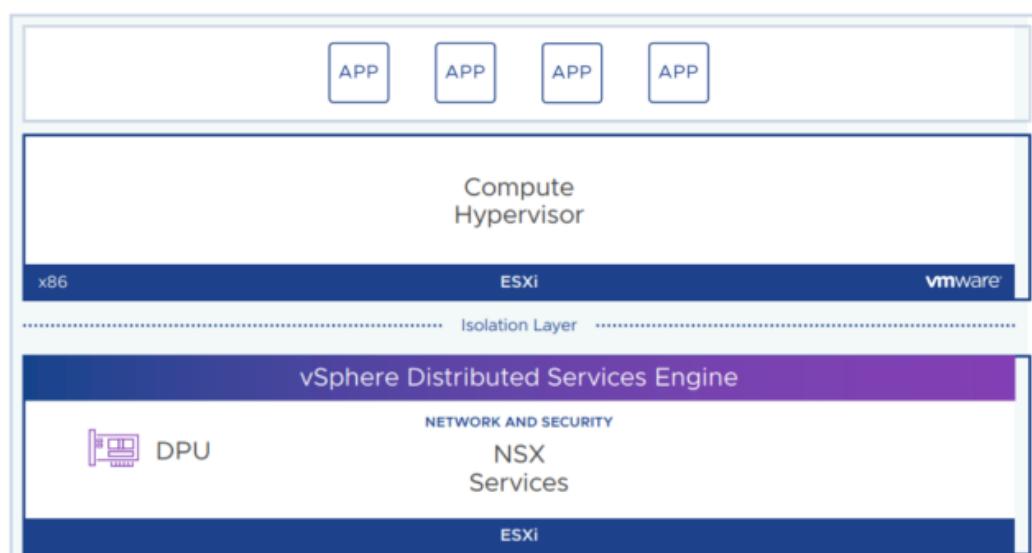
Two ESXi instances per physical server: There are now two ESXi instances running simultaneously, one on the main x86 CPU and one on the SmartNIC. These two ESXi instances can be managed separately or as a single logical instance. CSPs providing VCF-as-a-service will want the former while enterprises using VCF as normal will prefer the latter

SmartNIC is a NIC with a general-purpose CPU, out-of-band management, and virtualized device functionality.

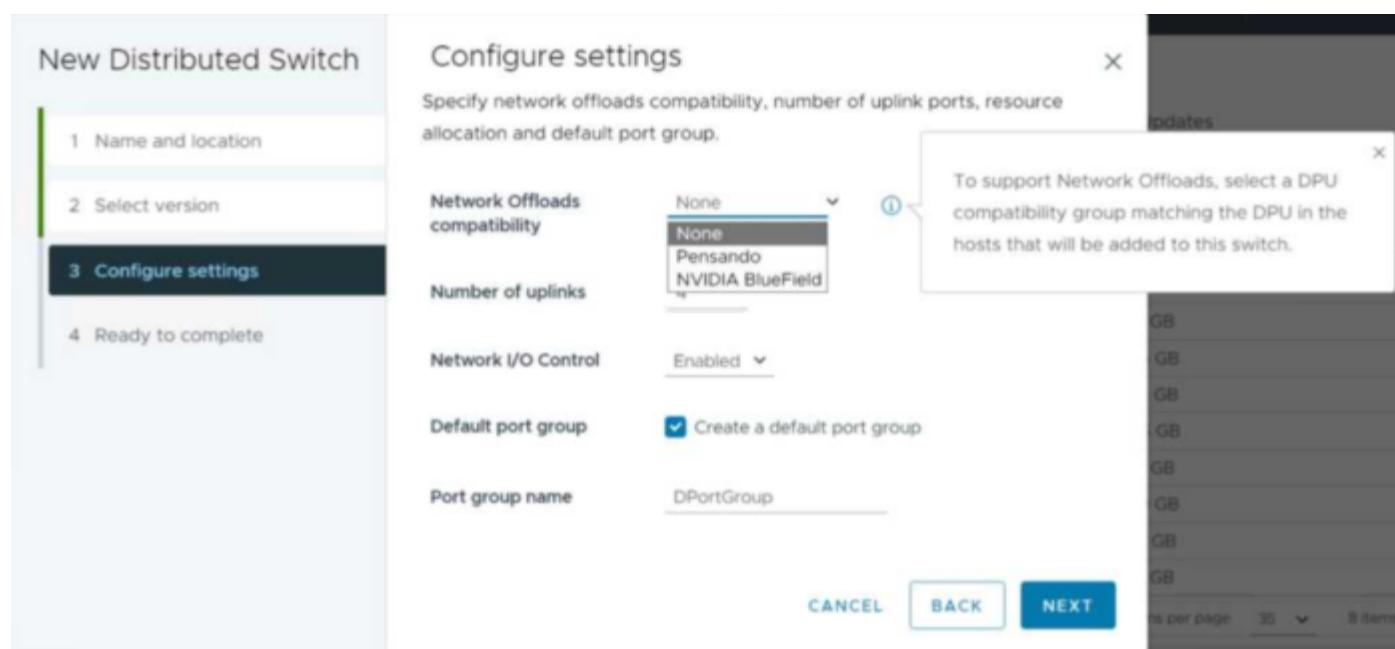
The vSphere distributed services engine is a lifecycle managed via vSphere Lifecycle Manager. There is no difference in versions when ESXi is installed on the DPU. When you remediate the parent host that contains the DPU, the version of ESXi that you remediate with will also get remediated to the DPU itself.

## Meet vSphere Distributed Services Engine

#### Offload network services to DPU



vSphere Distributed Switch version 8.0 will be introduced and it shall increase the network performance, and enhance the visibility and observability of network traffic. Also, provides security encryption, isolation, and protection from NSX.



The supported DPU will appear within the drop-down menu on the Network Offload Compatibility. You should select the DPU compatibility group matching the DPU in the hosts that will be added to this switch. A DRS and vMotion are still supported.

vSphere Distributed Services Engine does not require a separate ESXi license. An internal network that is isolated from other networks, connects the DPUs with ESXi hosts. ESXi 8.0 server builds are unified images, which contain both x86 and DPU content.

During vSphere 8 launch, vSphere Distributed Services Engine is supported by DPUs from NVIDIA and AMD, and server designs from Dell and HPE. vSphere Distributed Services Engine is available on servers with pre-installed DPUs.

## **Objective 1.11.1 – Describe VMware vSphere Distributed Services Engine**

Described in 1.11

## **Objective 1.12 – Identify use cases for VMware Tools**

*VMware Tools is a set of services and modules that enable several features in VMware products for better management of guests operating systems and seamless user interactions with them.*

*VMware Tools has the ability to:*

- *Pass messages from the host operating system to the guest operating system.*
- *Customize guest operating systems as a part of the vCenter Server and other VMware products.*
- *Run scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.*
- *Synchronize the time in the guest operating system with the time on the host operating system*

VMware tools can run services that helps with VM workloads. Helps with performance, security etc. Here are few examples of services that can be (or are) installed by default when you install your VMware Tools package inside of your Virtual Machine (VM).

**Appdefense** – (not installed by default) VMware Tools installation include the VMware AppDefense, a security management and monitoring solution. AppDefense agent can be installed on the guest virtual machine using the VMware Tools installer.

**SVGA Driver** – This virtual driver enables 32-bit displays, high display resolution, and faster graphics performance. When you install VMware Tools, a virtual SVGA driver replaces the default VGA driver, which allows for only 640 X 480 resolution and 16-color graphics.

**VMCI Driver** – The Virtual Machine Communication Interface driver supports fast and efficient communication between virtual machines and the hosts they run on. Developers can write client-server applications to the VMCI Sock (vsock) interface to make use of the VMCI virtual device.

**VMXNet NIC Driver** – The VMXNET and VMXNET3 networking drivers improve network performance.

**Paravirtual SCSI Driver** – A VMware Paravirtual SCSI driver is included for use with Paravirtual SCSI devices. This driver for VMware Paravirtual SCSI adapters enhances the performance of some virtualized applications. Drivers for other storage adapters are either bundled with the operating system, or they are available from third-party vendors.

The screenshot shows the VMware Customer Connect website for VMware Tools 12.1.5. The top navigation bar includes links for Products and Accounts, Knowledge, Communities, Support, and Learning. The right side features the ESX Virtualization logo. The main content area is titled "Download Product". It displays product details: Select Version (12.1.5), Documentation (Release Notes), Release Date (2022-11-29), and Type (Product Binaries). Below this, a "Product Downloads" section lists several options:

File	Information	Action
VMware Tools packages for Windows	File size: 108.56 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for Windows	File size: 108.56 MB File type: gz	<a href="#">DOWNLOAD NOW</a>
VMware Tools for Windows, 32-bit in-guest installer	File size: 34.85 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools for Windows, 64-bit in-guest installer	File size: 70.36 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for GuestStore	File size: 105.22 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for GuestStore	File size: 105.22 MB File type: gz	<a href="#">DOWNLOAD NOW</a>
VMware Tools Offline VIB Bundle	File size: 321.82 MB File type: zip	<a href="#">DOWNLOAD NOW</a>

**Mouse Driver** – The virtual mouse driver improves mouse performance. This driver is required if you use third-party tools such as Microsoft Terminal Services.

**Modules and drivers that support making automatic backups of virtual machines**

- If the guest operating system is Windows Vista, Windows Server 2003, or other newer Windows operating systems, a Volume Shadow Copy Services (VSS) module is installed. For other, earlier Windows operating systems, the Filesystem Sync driver is installed. These modules allow external third-party back up software that is integrated with vSphere to create application-consistent snapshots.

What are the differences between VMware Tools and Open-VM tools?

Open-VM tools (OVT) is an open source implementation of VMware tools. The same as VMware tools, OVT is suite of virtualization utilities which improves the performance, functionality, administration and management of virtual machines (VMs) running within VMware vSphere environment.

It has kernel modules for enhancing the performance of VMs running Linux or another VMware supported Unix like guest OS.

With OVT you'll be able to perform graceful shutdown, authentication for guest OS operations, generation of heartbeat from guest to host (so VMware High Availability can determine if the guest OS is up and running or not).

OVT are also responsible for clock synchronization between guest and host, as well as quiescing of guest file systems which is needed for filesystem consistent guest snapshots.

The benefits of Open-VM Tools

**Installed out of the box** – The primary benefit of OVT is the fact, that Linux distros have in most cases incorporated those packages within the installation ISO so when you create a new Linux VM within your environment and you're using this installation ISO, most likely the OVT will be installed out-of-the-box.

It is the software and OS vendors, as well as communities, who does bundle the open-VM tools into their product releases.

**Easier patching** – the patching process of the Linux distro using open-VM tools is usually handled by the Linux distro itself and not your vCenter server. It's perhaps easier to let the Linux VM patch itself (including OVT) instead of letting this job done via vCenter update manager (VUM).

**Small footprint** – the OVT package is small package included with the guest OS. It is optimized for each particular distro, not a single Linux package like VMware tools for Linux.

**Compatibility matrix not needed** – The compatibility matrix check is VMware online tool which shall be used to verify that the guest OS release version is sufficient for your version of tools.

In case OVT isn't installed, you have to use the OS package management system to install it. In general, Ubuntu, Debian and other OSes from this family use apt to install Debian (\*.deb) packages.

Redhat, Fedora and CentOS use dnf or yum to install RPM (\*.rpm) packages. And lastly, SuSE Linux Enterprise (SLE) and OpenSuSE use zypper to install RPM (\*.rpm) packages.

## Objective 1.13 – Describe the high-level components of VMware vSphere with Tanzu

VMware vSphere with Tanzu is a powerful platform that enables organizations to run and manage modern, containerized applications on their existing vSphere infrastructure. Tanzu is built on top of Kubernetes, the industry-standard container orchestration platform, and provides a number of features and capabilities that enable organizations to simplify the deployment and management of containerized applications. In this article, we will describe the high-level components of VMware vSphere with Tanzu and how they work together to provide a powerful platform for modern application development.

**Workload Management**

Workload Management enables deploying and managing Kubernetes workloads in vSphere. By using Workload Management, you can leverage both Kubernetes and vSphere functionality. Once you configure a vSphere cluster for Workload Management and it becomes a Supervisor, you can create namespaces that provide compute, networking, and storage resources for running your Kubernetes applications. You can also configure Supervisors with policies for resource consumption.

[Learn more about Workload Management](#)

[GET STARTED](#)

**Prerequisites for setting up a Supervisor**

**Network Support**

You can select between two networking stacks when setting up a vSphere cluster as a Supervisor. vSphere Distributed Switch (vDSC) and NSX are supported.

[VIEW DOCUMENTATION](#)

**HA and DRS Support**

You must enable vSphere HA and DRS in fully-automated mode on the vSphere cluster that you set up as a Supervisor.

[VIEW DRS/HA DOCUMENTATION](#)

**Storage Policy**

You must create storage policies or use existing policies that will determine the datastore placement of the Supervisor control plane VMs, containers, and images. You can create storage policies associated with different storage classes.

[VIEW STORAGE POLICIES](#)

**Load Balancer**

If you use the vSphere Distributed Switch (vDSC) network, you must configure a load balancer to support the network connectivity to workloads from client networks and to load balance traffic between Tanzu Kubernetes clusters. You can configure either NSX Advanced Load Balancer or HAProxy.

**vSphere** – At the heart of VMware vSphere with Tanzu is vSphere, the industry-leading virtualization platform that provides a scalable and secure infrastructure for running enterprise applications. vSphere enables organizations to virtualize their compute, storage, and networking resources, providing a flexible and agile infrastructure for running a wide range of workloads.

**Kubernetes** – Tanzu is built on top of Kubernetes, the popular container orchestration platform that is widely used for managing containerized applications. Kubernetes provides a range of features and capabilities for automating the deployment, scaling, and management of containerized applications, making it an ideal platform for modern application development.

**Tanzu Kubernetes Grid Service** – Tanzu Kubernetes Grid Service (TKGS) is a key component of Tanzu that provides a fully integrated Kubernetes solution for vSphere. TKGS enables organizations to deploy and manage Kubernetes clusters directly from the vSphere interface, providing a seamless experience for developers and operators alike.

**vSphere Networking** – Tanzu leverages the powerful networking capabilities of vSphere to provide a highly scalable and flexible network infrastructure for containerized applications. vSphere networking provides a range of features and capabilities, including virtual networking, load balancing, and security, enabling organizations to build highly available and secure containerized applications.

**Tanzu Kubernetes Grid Integrated Edition** – Tanzu Kubernetes Grid Integrated Edition (TKGI) is a comprehensive Kubernetes platform that provides a range of features and capabilities for deploying and managing containerized applications. TKGI includes a number of advanced features, such as multi-tenancy, role-based access control, and integrated logging and monitoring, making it an ideal platform for organizations that need to manage large-scale Kubernetes environments.

**Harbor Registry** – Harbor is an open-source container registry that is fully integrated with Tanzu Kubernetes Grid Integrated Edition. Harbor provides a highly scalable and secure platform for storing and distributing container images, enabling organizations to easily manage and deploy containerized applications.

**Tanzu Mission Control** – Tanzu Mission Control is a powerful management platform that provides a unified view of all Kubernetes clusters deployed across an organization. Tanzu Mission Control enables organizations to easily manage and monitor their Kubernetes environments, ensuring that they are running securely and efficiently.

## **Objective 1.13.1 – Identify the use case for a Supervisor Cluster and Supervisor Namespace**

Supervisor Cluster and Supervisor Namespace provides a centralized point of control for managing multiple Kubernetes clusters. Here are several use cases for a Supervisor Cluster and Supervisor Namespace that can be leveraged when running a virtual infrastructure based on vSphere and Tanzu.

**Multi-Cluster Management** – With Tanzu, you can deploy multiple Kubernetes clusters across different environments, such as on-premises or in the cloud. Managing multiple clusters can be a challenge, but with a Supervisor Cluster, you can manage all of your clusters from a single control plane. This makes it easier to manage and monitor your clusters, and to roll out updates across all of your clusters.

**Disaster Recovery** – If one of your clusters experiences a failure, you can quickly spin up a new cluster and restore your applications and services. With a Supervisor Cluster, you can

manage and monitor multiple clusters from a single control plane, making it easier to recover from disasters and minimize downtime.

**Compliance and Governance** – A Supervisor Cluster and Supervisor Namespace can also be used to enforce compliance and governance across multiple clusters. With Tanzu, you can define policies and regulations that must be followed across all of your clusters. This ensures that your applications and services are being deployed in a secure and compliant manner, and reduces the risk of security breaches or compliance violations.

**Resource Sharing** – A Supervisor Namespace in VMware Tanzu allows you to manage resources across multiple clusters. This makes it easier to share resources between applications and teams, and to ensure that resources are being used efficiently across all of your clusters. With a Supervisor Namespace, you can create a single source of truth for your resources, reducing the risk of conflicts and ensuring that resources are being used effectively.

**Testing and Development** – Finally, a Supervisor Cluster and Supervisor Namespace can be used to manage testing and development environments. With Tanzu, you can quickly spin up new environments for testing and development purposes, and manage them from a single control plane. This makes it easier to test new features and applications, and to iterate quickly on your development projects.

Supervisor Cluster and Supervisor Namespace in VMware Tanzu provide a powerful set of tools for managing multiple Kubernetes clusters. With Tanzu, you can deploy and manage clusters across different environments, enforce compliance and governance policies, share resources more efficiently, and manage testing and development environments more effectively. As organizations continue to adopt Kubernetes for their modern application development needs, the use cases for a Supervisor Cluster and Supervisor Namespace are likely to continue to grow in importance.

## **Objective 1.13.2 – Identify the use case for vSphere Zones**

**Resource Allocation** – With Tanzu, multiple Kubernetes clusters can be deployed on a vSphere infrastructure, and vSphere Zones can be used to allocate specific resources to each cluster. This ensures that the Kubernetes clusters have the resources they need to run efficiently and effectively. By dedicating resources to a particular zone, administrators can prevent contention for resources such as CPU, memory, and storage, which can lead to performance issues and application downtime.

**Workload Isolation** – Tanzu allows organizations to run multiple workloads, including development, test, and production environments, on the same infrastructure. With vSphere Zones, administrators can create isolated environments for each workload, ensuring that they do not interfere with each other. This prevents issues such as production workloads

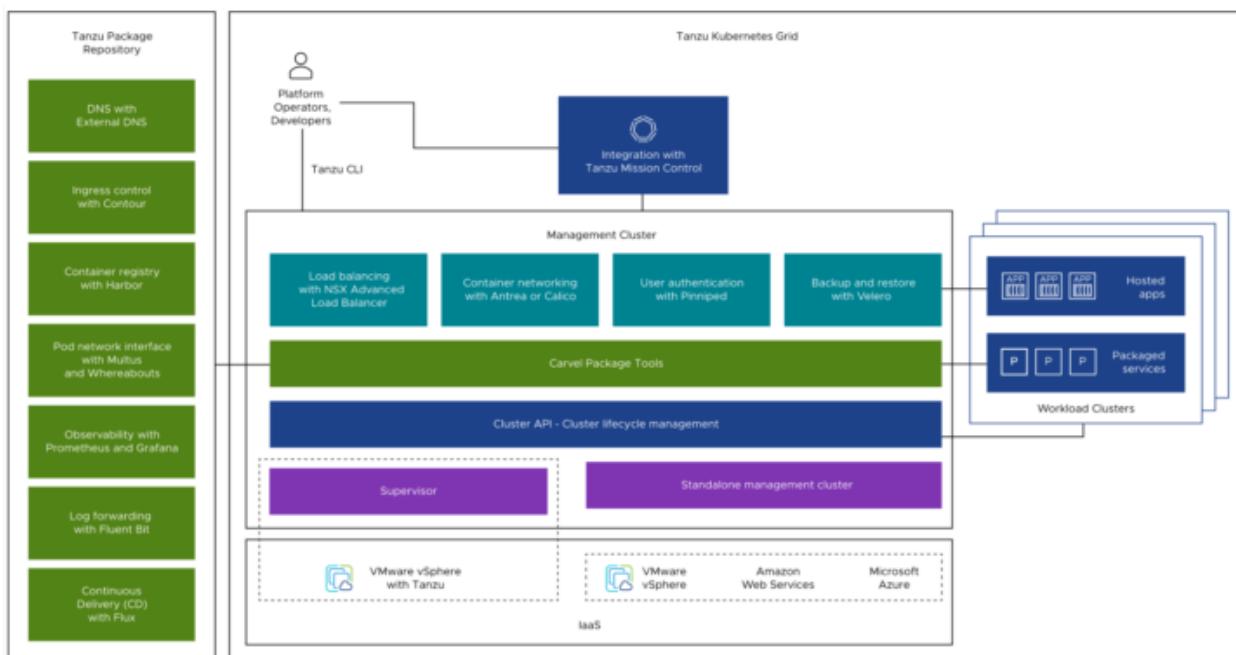
being impacted by development or test workloads, and ensures that each workload has the necessary resources and security policies in place.

**High Availability and Disaster Recovery** – vSphere Zones in Tanzu can also be used to support high availability and disaster recovery. With vSphere, administrators can create vSphere clusters that span multiple physical hosts, and vSphere Zones can be used to group together the hosts that make up each cluster. By creating clusters in this way, administrators can ensure that if a physical host fails, the VMs running on that host can be restarted on another host within the same cluster. This reduces downtime and ensures that critical applications remain available.

**Security and Compliance** – Finally, vSphere Zones in Tanzu can be used to support security and compliance requirements. By grouping together resources that are subject to specific security and compliance policies, administrators can ensure that those policies are consistently enforced across the infrastructure. For example, vSphere Zones can be used to ensure that all VMs that handle sensitive data are running on hosts that are subject to specific security controls, or that all VMs running in a particular zone are subject to specific compliance regulations.

With vSphere Zones, administrators can allocate resources to specific clusters, isolate workloads, support high availability and disaster recovery, and enforce security and compliance policies. As organizations continue to adopt Kubernetes and other modern application development technologies, the use cases for vSphere Zones in Tanzu are likely to continue to grow in importance.

## Objective 1.13.3 – Identify the use case for VMware Tanzu Kubernetes Grid (TKG) cluster



Tanzu Kubernetes Grid deploys clusters using an opinionated configuration of Kubernetes open-source software that is supported by VMware, so that you do not have to build a Kubernetes environment by yourself. In addition to validated Kubernetes component binaries, Tanzu Kubernetes Grid provides packaged services such as networking, authentication, ingress control, and logging that a production Kubernetes environment requires.

**Consistent Kubernetes Experience** – One of the primary use cases for a TKG cluster is to provide a consistent Kubernetes experience across different environments. TKG allows organizations to deploy and manage Kubernetes clusters across different infrastructure, including on-premises data centers and public cloud providers like AWS, Azure, and Google Cloud Platform. This means that organizations can use the same tools and processes to deploy and manage Kubernetes, regardless of the underlying infrastructure. This is particularly useful for organizations that need to manage a large number of Kubernetes clusters across different environments.

**Scalability and Flexibility** – Another important use case for a TKG cluster is scalability and flexibility. TKG allows organizations to scale their Kubernetes clusters up or down based on demand. This means that organizations can increase the number of nodes in a cluster to handle increased traffic, or decrease the number of nodes to save costs when traffic is lower. TKG also allows organizations to deploy Kubernetes clusters with different configurations and settings, depending on the needs of each workload. This flexibility allows organizations to optimize their Kubernetes deployment for different workloads and use cases.

**Security and Compliance** – TKG also supports security and compliance requirements. With TKG, organizations can deploy Kubernetes clusters with specific security and compliance policies in place. This can include network policies, access controls, and auditing and logging requirements. TKG also allows organizations to deploy Kubernetes clusters in a way that is compliant with specific regulations, such as PCI DSS, HIPAA, and GDPR. This ensures that organizations can deploy and manage Kubernetes in a way that meets their security and compliance needs.

**Integration with VMware Infrastructure** – Finally, TKG is tightly integrated with VMware infrastructure, including vSphere and [NSX-T](#). This means that organizations can use their existing VMware infrastructure to deploy and manage Kubernetes clusters. TKG also integrates with other VMware products, such as vRealize Operations, to provide advanced monitoring and management capabilities for Kubernetes clusters.

## **Objective 2.1 – Describe the role of VMware vSphere in the Software-Defined Data Center**

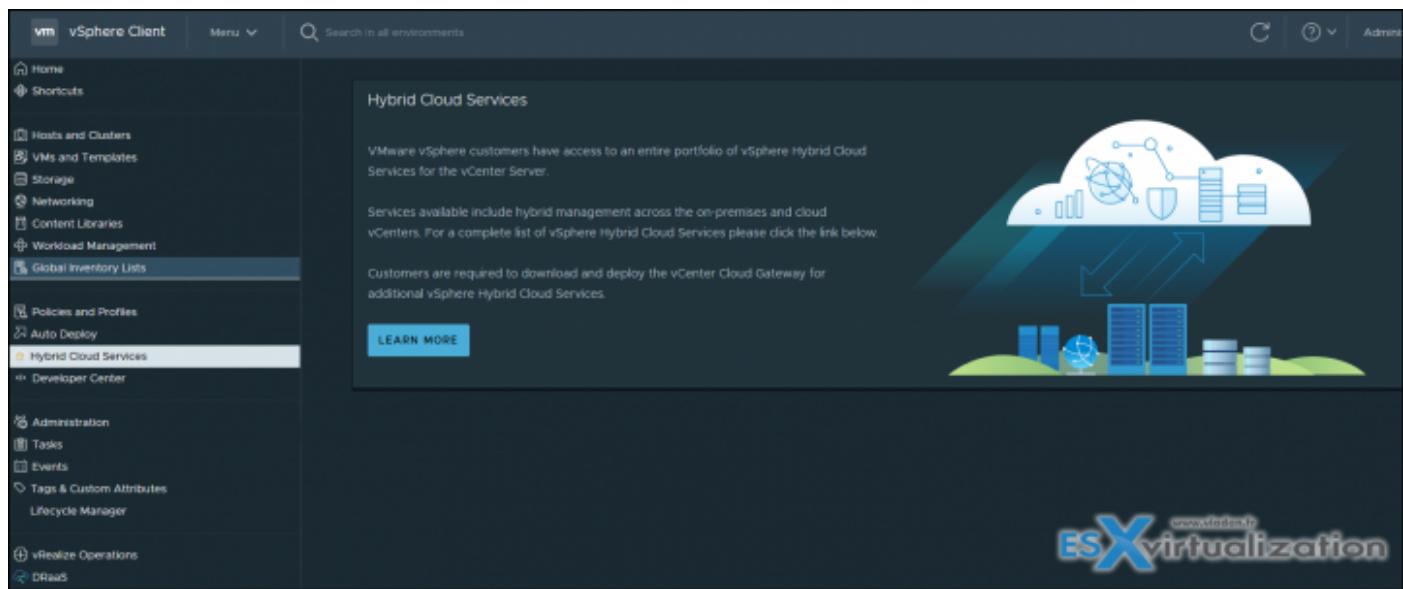
VMware Software-Defined Datacenter (SDDC) is a data center that uses local infrastructure services that are abstracted from the underlying physical infrastructure. It allows any apps

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 case for vSphere+

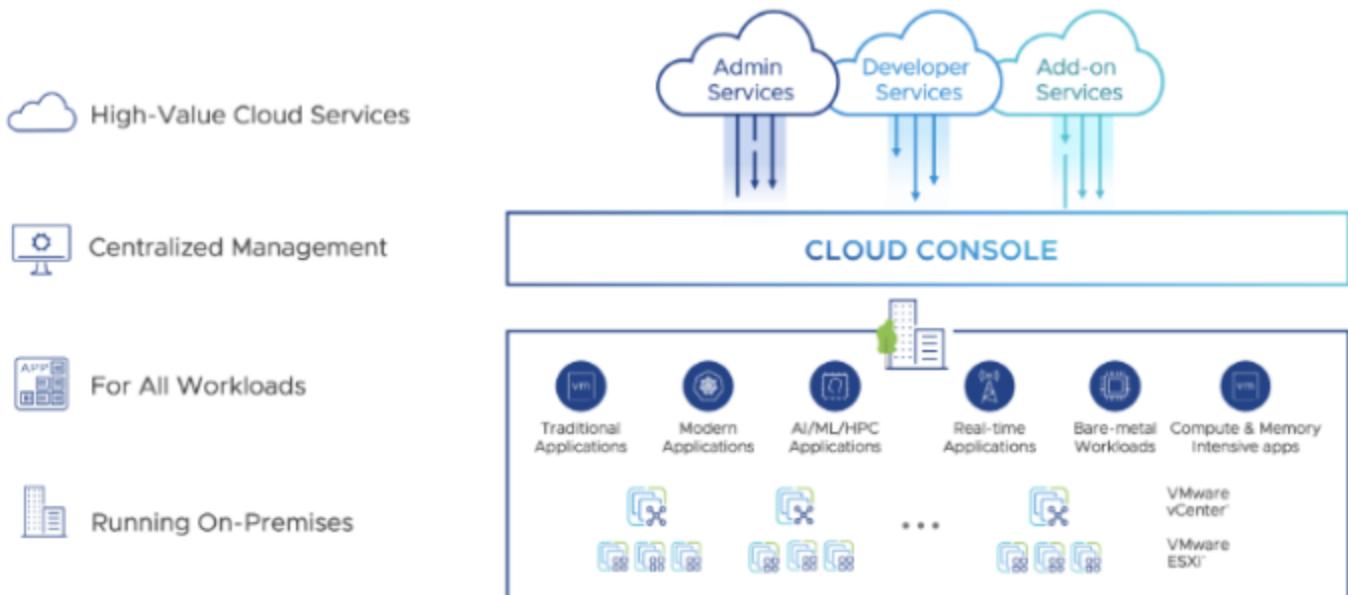
Basically, VMware vSphere Plus is a suite of virtualization features that are built on top of VMware vSphere. It provides businesses with an all-in-one virtualization solution that offers a range of features such as virtualization, networking, storage, and security. vSphere Plus is an ideal solution for businesses that need to optimize their IT infrastructure, improve efficiency, and reduce costs.

What does VMware vSphere Plus offer?

VMware vSphere Plus offers a range of features that are designed to enhance the virtualization experience for businesses. Some of the key features of vSphere Plus include:

- 1. Virtualization** – vSphere Plus provides businesses with the ability to create and manage virtual machines (VMs) on a single physical server. This allows for the consolidation of servers, which reduces costs and improves efficiency.
- 2. Networking** – vSphere Plus includes features such as Distributed Switches, Network I/O Control, and vSphere Network Security that provide businesses with a reliable and secure network infrastructure.
- 3. Storage** – vSphere Plus includes features such as vSphere Storage DRS, vSphere Storage I/O Control, and vSphere Storage APIs that provide businesses with a flexible and scalable storage infrastructure.
- 4. Security** – vSphere Plus includes features such as vSphere AppDefense, vSphere Encrypted vMotion, and vSphere Authentication Proxy that provide businesses with a secure virtual environment.

### vSphere+ Delivers Benefits of Cloud to On-Premises Workloads



## Why is VMware vSphere Plus important for businesses?

It's because it solves a lot of problems and brings solutions. VMware vSphere Plus is an essential tool for businesses that want to optimize their IT infrastructure, improve efficiency, and reduce costs. Here are some reasons why vSphere Plus is important for businesses:

- 1. Simplified Virtualization** – vSphere Plus provides businesses with a simplified virtualization experience by providing an all-in-one solution for virtualization, networking, storage, and security. This simplifies the management of virtual machines and reduces the time and effort required to manage virtualized infrastructure.
- 2. Improved Efficiency** – vSphere Plus improves efficiency by consolidating servers, reducing hardware costs, and improving resource utilization. This allows businesses to get the most out of their existing IT infrastructure, which reduces costs and increases efficiency.
- 3. Scalability** – vSphere Plus provides businesses with a scalable virtualization solution that can easily adapt to changing business needs. This allows businesses to scale up or down their virtual infrastructure as needed, which reduces costs and improves flexibility.
- 4. Security** – vSphere Plus provides businesses with a secure virtual environment by including features such as vSphere AppDefense, vSphere Encrypted vMotion, and vSphere Authentication Proxy. This ensures that virtualized environments are protected from threats and are compliant with industry regulations.

## Admin Services

Admin services are delivered as SaaS through the **Cloud Console**, enhancements will appear without requiring any manual downloads or updates. New services will also be introduced when they are ready. Through the cloud console, several admin services can be utilized to simplify and streamline management of the entire vSphere+ estate. These services are delivered through the cloud, so they are easy to use without having to download or install anything.

**vCenter lifecycle management service** – This service makes on-premises vCenter updates a lot simpler and faster. When an update is available you simply click the 'Update Now' button and the service takes care of the rest. The maintenance window is only a few minutes, and if there's a problem you can roll back to the previous version.

**Global inventory service** – With this service you can visualize available resources across the entire vSphere+ estate. See all your clusters, hosts, VMs at a glance, and quickly assess the CPU, memory, storage and other resources you have at your command.

**Event view service** – View all events and alerts across your entire vSphere+ estate. This makes it easy to quickly triage problems that need immediate attention without having to manually check individual vCenters separately.

**Security health check service** – Monitor your security posture across the entire vSphere+ estate. Highlight security exposures across all vSphere+ infrastructure, such as idle SSH sessions or deprecated SSL protocols and initiate remedial actions.

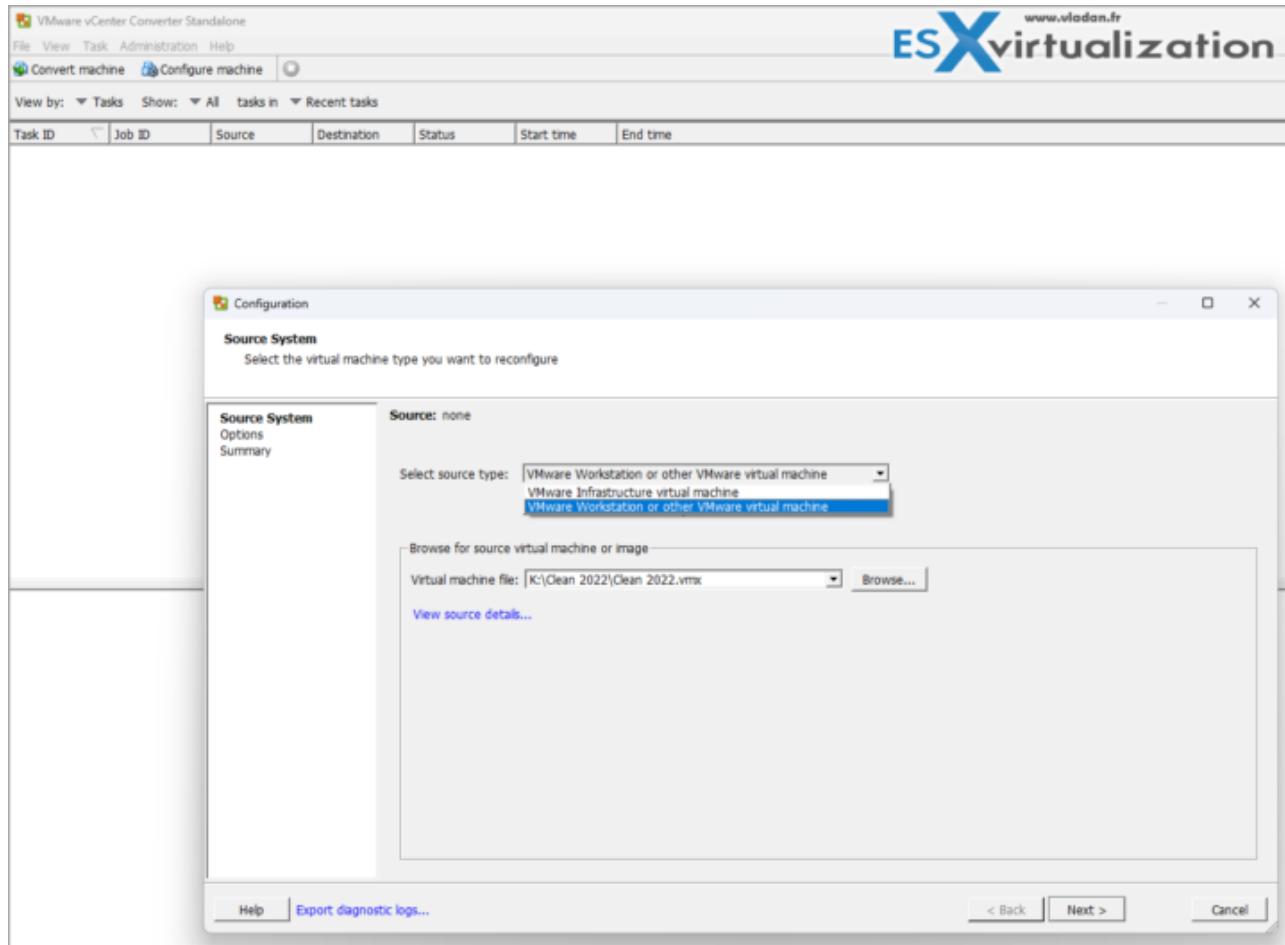
**Provision VM service** – Quickly create VMs from the cloud console without having to first connect to a vCenter instance. If you need to create a lot of VMs in different places, this can be a real time saver.

**Configuration management service** – Sometimes vCenter configurations can diverge from each other. With this service, you'll be able to quickly spot configuration drift so you can keep your vCenter configurations in line with your global standard.

## Objective 2.3 – Identify use cases for VMware vCenter Converter

VMware vCenter Converter should be well known software to any admin. Its use case is to virtualize physical workloads to VMware Virtual Machines (VMs), migrate workloads, export VMs managed by vCenter server to other or re-configure virtual workloads. The software can be used for free.

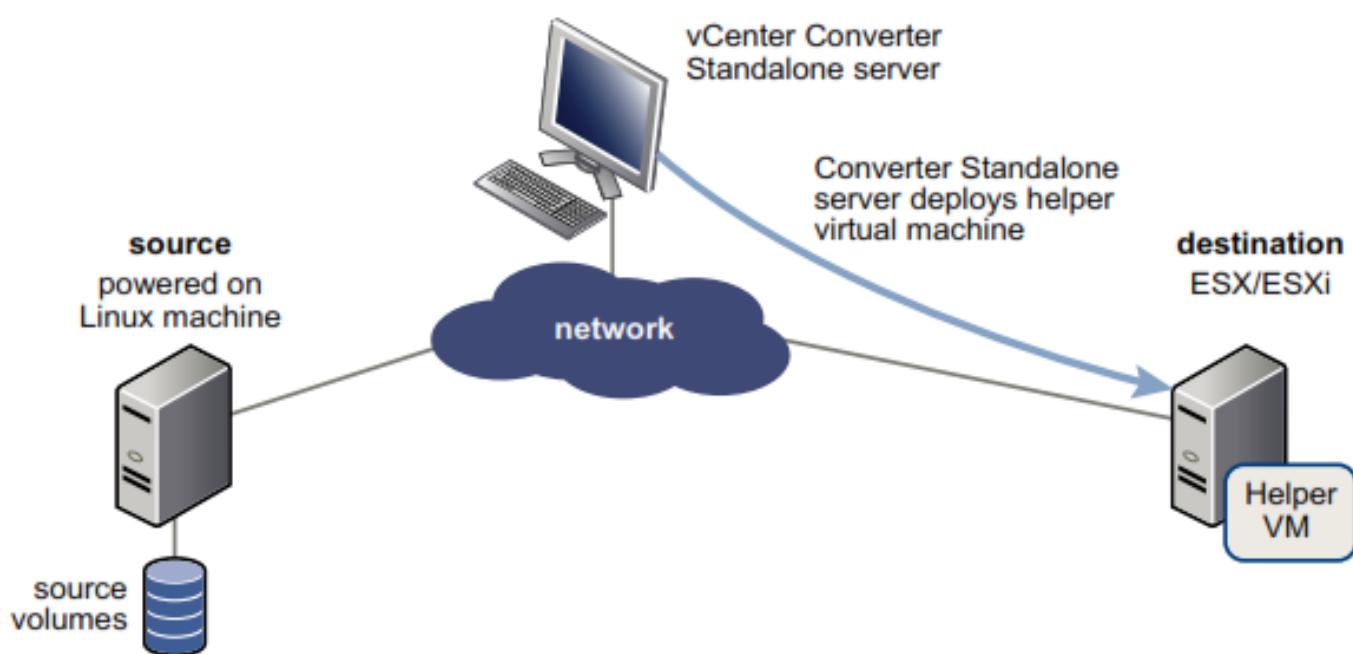
Screenshot shows reconfiguration of virtual machine



VMware vCenter Converter is a powerful tool used for virtual machine (VM) conversion, migration, and creation. It helps organizations efficiently convert physical machines, other virtual machine formats, and even cloud-based VMs into VMware-based VMs. The tool simplifies the process of converting and migrating VMs while ensuring compatibility and minimal disruption to operations.

Some of the most common use cases for VMware vCenter Converter.

**Physical to Virtual (P2V) Migration** – One of the most common use cases for VMware vCenter Converter is P2V migration. It enables organizations to convert their physical servers into virtual machines, enabling greater flexibility and reducing hardware costs. With vCenter Converter, organizations can quickly convert their physical machines into virtual ones, allowing them to run multiple servers on a single physical host. This helps improve resource utilization and reduce the physical footprint of servers.



**Virtual to Virtual (V2V) Migration** – VMware vCenter Converter can also be used to migrate VMs from one virtualization platform to another. For instance, organizations can use it to migrate VMs from VMware ESX to [VMware Workstation](#), or from Hyper-V to VMware. V2V migration ensures that VMs can be easily moved between different platforms, thereby improving flexibility and minimizing downtime.

**Disaster Recovery** – VMware vCenter Converter is a critical tool in disaster recovery planning. It helps organizations create replicas of their VMs, which can be used in the event of a disaster. By creating VM replicas, organizations can quickly and easily recover from outages, thereby minimizing downtime and reducing the impact on business operations.

**Testing and Development** – VMware vCenter Converter is also useful for testing and development purposes. It enables organizations to create VMs from existing production environments, allowing developers to test new applications or changes without impacting production environments. It also helps organizations create sandboxes, allowing IT teams to test patches and updates before applying them to the production environment.

**Cloud Migration** – VMware vCenter Converter can also be used to migrate VMs to cloud-based environments. This is particularly useful for organizations that are looking to move to cloud-based infrastructures. With vCenter Converter, organizations can easily migrate VMs to cloud environments such as AWS or Azure, enabling greater scalability and flexibility.

**Server Consolidation** – Server consolidation is another common use case for VMware vCenter Converter. It enables organizations to consolidate multiple servers onto a single physical host, thereby reducing hardware and maintenance costs. With vCenter Converter, organizations can easily convert their physical servers into virtual ones and consolidate them onto a single host.

**Legacy Application Support** – VMware vCenter Converter is also useful for supporting legacy applications. Many legacy applications run on older hardware platforms that are difficult to maintain. By converting these physical machines into virtual ones, organizations can continue to run legacy applications on newer hardware platforms, thereby extending the life of these applications.

As you can see, VMware vCenter Converter is a versatile tool that offers a range of benefits for organizations. It simplifies the process of converting, migrating, and creating VMs, while ensuring compatibility and minimal disruption to operations.

By leveraging vCenter Converter, organizations can improve their disaster recovery planning, reduce hardware costs, improve resource utilization, and support legacy applications. It is a valuable tool for any organization looking to improve their virtualization and cloud-based infrastructure capabilities.

If you need system requirements, detailed scenarios, ports used or conversion limitations of using VMware converter, I'd recommend getting the VMware vCenter Converter Stanalaon User's Guide PDF from VMware.

## Objective 2.4 – Identify disaster recovery (DR) use cases

Disaster recovery (DR) is a critical aspect of business continuity planning. In the event of a disaster, organizations need to have a plan in place to ensure that their critical systems and data can be recovered as quickly as possible. VMware vSphere is a powerful virtualization platform that offers a range of DR solutions. In this article, we will identify **some of the most common DR use cases for VMware vSphere** and highlight how it can benefit organizations.

**Site Recovery** – Site recovery is one of the most common DR use cases for VMware vSphere. It enables organizations to replicate their virtual machines and data to a secondary site, ensuring that they can quickly recover in the event of a disaster. With vSphere Site Recovery, organizations can automate the recovery process, minimizing downtime and reducing the risk of data loss. This is particularly useful for organizations that have critical systems and applications that need to be available 24/7.

**Backup and Restore** – VMware vSphere also offers a range of backup and restore solutions. Organizations can use vSphere's native backup solutions or third-party backup solutions to create backups of their virtual machines and data. This enables them to quickly recover in the event of a disaster, ensuring that they can resume operations as quickly as possible. Backup and restore solutions are particularly useful for organizations that have limited resources or cannot afford to have a secondary site.

**High Availability** – High availability (HA) is another DR use case for VMware vSphere. It ensures that critical systems and applications are always available, even in the event of a hardware failure. With vSphere HA, virtual machines are automatically restarted on another host in the event of a failure, ensuring that downtime is minimized. This is particularly useful for organizations that cannot afford to have any downtime for critical systems and applications.

The screenshot shows the 'Edit Cluster Settings' dialog box for an HA cluster. The 'Failures and responses' tab is active. The configuration details are as follows:

Action	Setting
Host Failure Response	Restart VMs
Response for Host Isolation	Disabled
Datastore with PDL	Power off and restart VMs
Datastore with APD	Power off and restart VMs - Conservative restart policy
VM Monitoring	Disabled

At the bottom right are 'CANCEL' and 'OK' buttons.

**Disaster Recovery as a Service (DRaaS)** – Disaster Recovery as a Service (DRaaS) is a cloud-based DR solution that leverages VMware vSphere. With DRaaS, organizations can replicate their virtual machines and data to a cloud-based environment, ensuring that they can quickly recover in the event of a disaster. DRaaS is particularly useful for organizations that do not have the resources to build and maintain their own secondary site.

**Testing and Validation** – Testing and validation is an important aspect of DR planning. VMware vSphere offers a range of tools that enable organizations to test and validate their DR plans. For instance, vSphere Replication can be used to replicate virtual machines to a test environment, allowing organizations to test their recovery procedures without impacting production environments.

**Storage Replication** – Storage replication is another DR use case for VMware vSphere. It enables organizations to replicate their virtual machines and data to another storage location, ensuring that they can quickly recover in the event of a disaster. With vSphere storage replication, organizations can replicate data across different types of storage, ensuring that they can meet their recovery objectives. You can use vSphere Replication (VR) product that is part of vSphere [Essentials Plus](#) bundle, and setup a replication to a DR site. A DR site can be a building over the street, next room in your datacenter, or a replication to a cloud based datacenter.

In conclusion, VMware vSphere offers a range of DR solutions that can help organizations quickly recover in the event of a disaster. Whether it's site recovery, backup and restore, high availability, DRaaS, testing and validation, virtual machine snapshots, or storage replication, vSphere has a solution that can meet the needs of any organization. By leveraging these DR solutions, organizations can ensure that their critical systems and data are always available, thereby reducing the impact of a disaster on their operations.

## Objective 2.4.1 – Identify VMware vCenter replication options

VMware vCenter is a powerful virtualization management platform that enables organizations to manage their virtual infrastructure. One of the key features of vCenter is replication, which enables organizations to replicate their virtual machines and data to another site. In this article, we will identify some of the replication options available with VMware vCenter and highlight how they can benefit organizations.

**vSphere Replication (VR)** – vSphere Replication is a built-in replication feature of vCenter (needs to install and configure the component) that enables organizations to replicate their virtual machines and data to another site. With vSphere Replication, organizations can replicate their virtual machines to a secondary site, ensuring that they can quickly recover in the event of a disaster. vSphere Replication offers a range of replication options, including

replication frequency, retention policies, and network bandwidth utilization. This enables organizations to tailor their replication settings to meet their specific needs.

**Configure Replication for 2003srv01**

**Recovery settings**  
Configure recovery settings for the virtual machine.

**Recovery Point Objective (RPO)**  
Lower RPO times reduce potential data loss, but use more bandwidth and system resources.

15 min [Slider] 24 hr

3 hr 0 min

**Point in time instances**  
Retained replication instances are converted to snapshots during recovery. Replication of existing VM snapshots is not supported.

Enable

Keep 2 instances per day for the last 5 days (10 total)

If the RPO period is longer than 12 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.

**Site Recovery Manager** – Site Recovery Manager (SRM) is another replication option available with vCenter. SRM is an add-on that enables organizations to **automate** the recovery process in the event of a disaster. With SRM, organizations can replicate their virtual machines and data to a secondary site, and automate the recovery process. This ensures that organizations can quickly recover in the event of a disaster, minimizing downtime and reducing the risk of data loss.

**Storage Array Replication** – Storage Array Replication is another replication option available. Usually provided by your storage device manufacturer, this option enables organizations to replicate their virtual machines and data at the storage level. Storage Array Replication requires that both the primary and secondary sites use the same storage array. This replication option is particularly useful for organizations that have critical systems and applications that require high levels of availability.

**vSphere Data Protection** – vSphere Data Protection (VDP) is a backup and replication solution that enables organizations to protect their virtual infrastructure. (Yes, it still exists). With VDP, organizations can backup and replicate their virtual machines and data to another site. This enables them to quickly recover in the event of a disaster, ensuring that critical systems and applications are always available. VDP is a robust, simple-to-deploy, disk-based backup and recovery solution. VDP is fully integrated with VMware vCenter Server and the VMware vSphere Web Client. VDP enables centralized and efficient management of backup jobs while storing backups in deduplicated destination storage.

**Third-Party Replication** – In addition to the replication options available with vCenter, organizations can also leverage third-party replication solutions. These solutions are often more advanced than the built-in replication options and can provide additional features such

as cross-site replication and failover. Third-party replication solutions can also be customized to meet the specific needs of organizations. There are many dataprotection software vendors, such as [Veeam](#), Zerto, Nakivo, HornetSecurity, just to name a few.

## Objective 2.4.2 – Identify use cases for VMware Site Recovery Manager (SRM)

VMware Site Recovery Manager (SRM) is a powerful disaster recovery solution that enables organizations to protect their virtual infrastructure in the event of a disaster. With SRM, organizations can automate the recovery process, ensuring that critical systems and data are quickly restored. In this article, we will identify some of the use cases for VMware Site Recovery Manager (SRM) and highlight how it can benefit organizations.

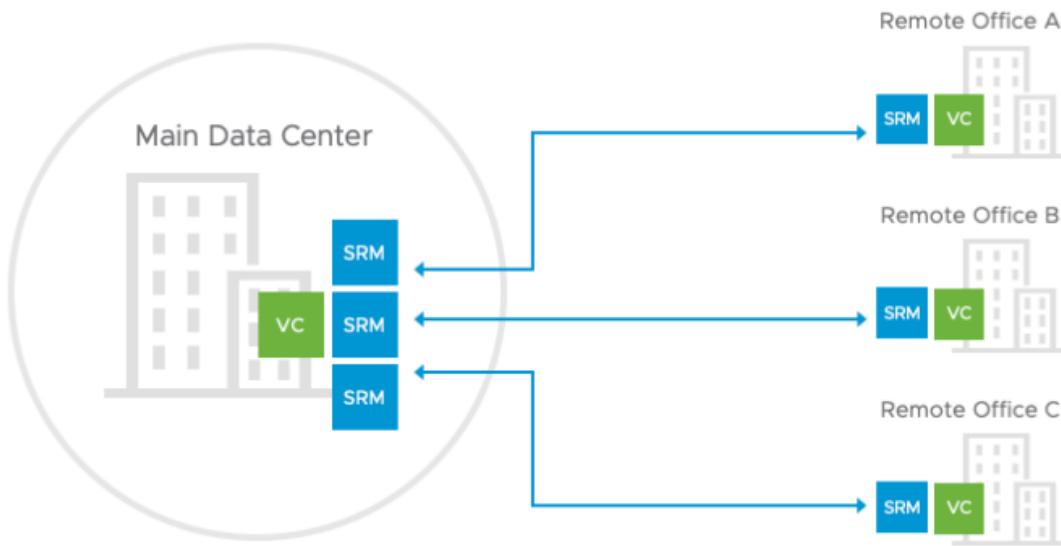
**Business Continuity** – One of the primary use cases for SRM is business continuity. By replicating virtual machines and data to a secondary site, organizations can ensure that critical systems and data are always available, even in the event of a disaster. SRM automates the recovery process, ensuring that virtual machines and data are quickly restored to their original state. This helps organizations minimize downtime and maintain business continuity, even in the face of a disaster.

**Testing** – Another use case for SRM is testing. SRM enables organizations to test their disaster recovery plans without disrupting their production environment. By simulating a disaster and testing the recovery process, organizations can identify any issues and ensure that their recovery plans are effective. This helps organizations build confidence in their disaster recovery plans and ensure that they are prepared for any eventuality.

**Compliance** – Compliance is another use case for SRM. Many organizations are subject to regulatory compliance requirements, which often include disaster recovery provisions. SRM can help organizations meet these compliance requirements by ensuring that critical systems and data are protected and quickly restored in the event of a disaster. This can help organizations avoid costly fines and penalties associated with non-compliance.

**Simplification** – SRM can also be used to simplify disaster recovery. By automating the recovery process, organizations can reduce the complexity of their disaster recovery plans. This can help organizations save time and resources, as they no longer need to manually restore virtual machines and data. This can also help organizations reduce the risk of human error, which can often lead to downtime and data loss.

**Multi-Site Operations** – Finally, SRM can be used to support multi-site operations. Organizations that operate multiple sites can use SRM to replicate virtual machines and data between sites, ensuring that critical systems and data are always available. This can help organizations improve their operational efficiency, as they no longer need to manually manage their disaster recovery processes across multiple sites.



### **SRM can:**

- Application-agnostic protection eliminates the need for app-specific point solutions
- Automated orchestration of site failover and fallback with a single-click reduces recovery times
- Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives
- Centralized management of recovery plans from the HTML5 UI replaces manual runbooks
- Planned migration workflow enables disaster avoidance and data center mobility

## **Objective 4.1 – Describe single sign-on (SSO)**

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 chose 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.

Group Name	Description
ActAsUsers	Act-As Users
Administrators	Users allowed to perform update related operations
AutoUpdate	
CAAdmins	Component Manager Administrators
ComponentManager Administrators	
DCAdmins	
DCClients	
ExternalIDPUsers	Well-known external IDP users' group, which registers external IDP users as guests.
LicenseService Administrators	License Service Administrators
NsxAdministrators	SSO group to view and modify NSX configuration.

Once there you can join the PSC to Microsoft AD and then only to ad 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 into 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 represents 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.*

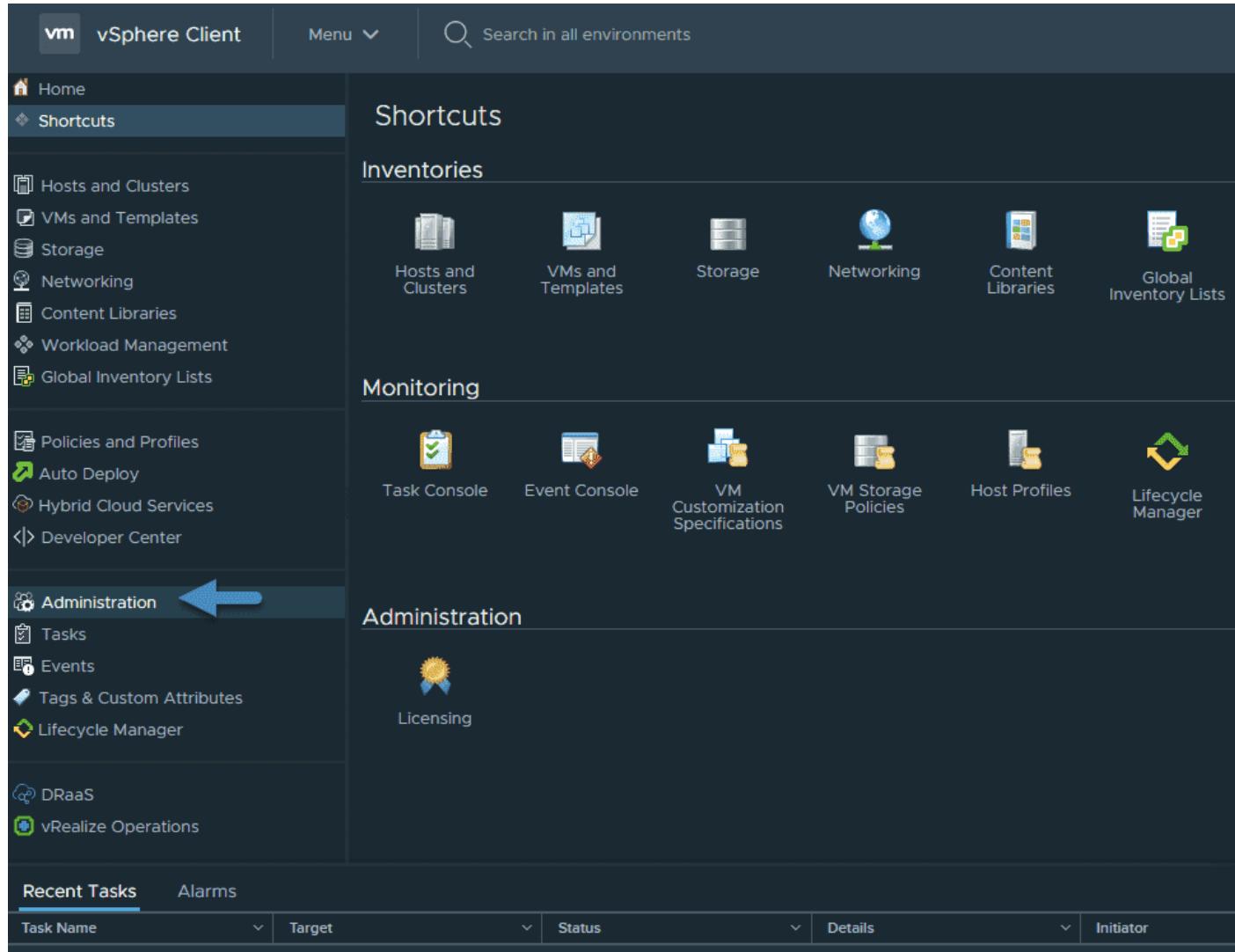
**VMware Directory Service (vmdir)** – the VMware Directory service (vmdir) is associated with the domain you specify during installation and is included in each embedded deployment and on each Platform Services Controller. This service is a multi-tenanted, multi-mastered directory service that makes 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 – Configure single sign-on (SSO) Domain

### 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

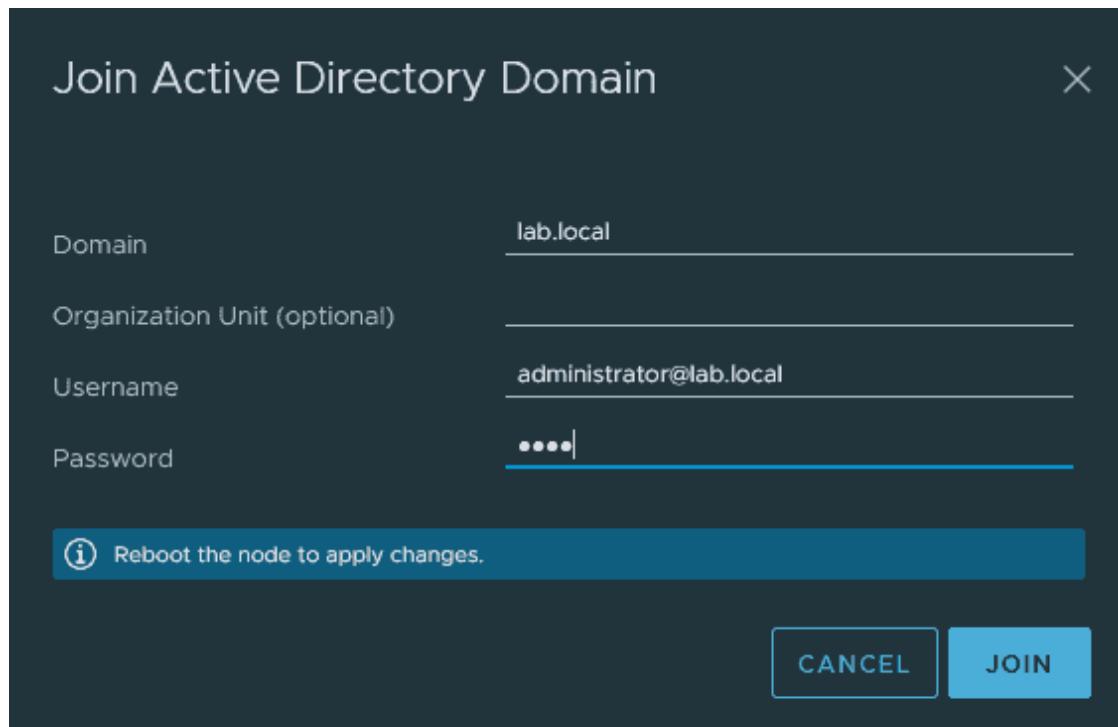
Click the **Single Sign-On** section and **Configuration**. On the **Identity provider tab**, click **Active Directory Domain > Join AD**.

The screenshot shows the 'Configuration' screen in the vSphere Client. At the top, there are tabs for 'Identity Provider' (which is selected), 'Local Accounts', and 'Login Message'. The main content area has two columns: 'Type' and 'Embedded'. Under 'Type', there is a section for 'Identity Sources' with three options: 'Active Directory Domain' (selected), 'Smart Card Authentication', and 'SSO'. Below this is a 'JOIN AD' button with a blue arrow pointing to it. The 'LEAVE AD' button is also visible. The 'Node' section shows a tree view with 'vcsaphoton.lab.local' expanded. A message at the bottom states: '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.

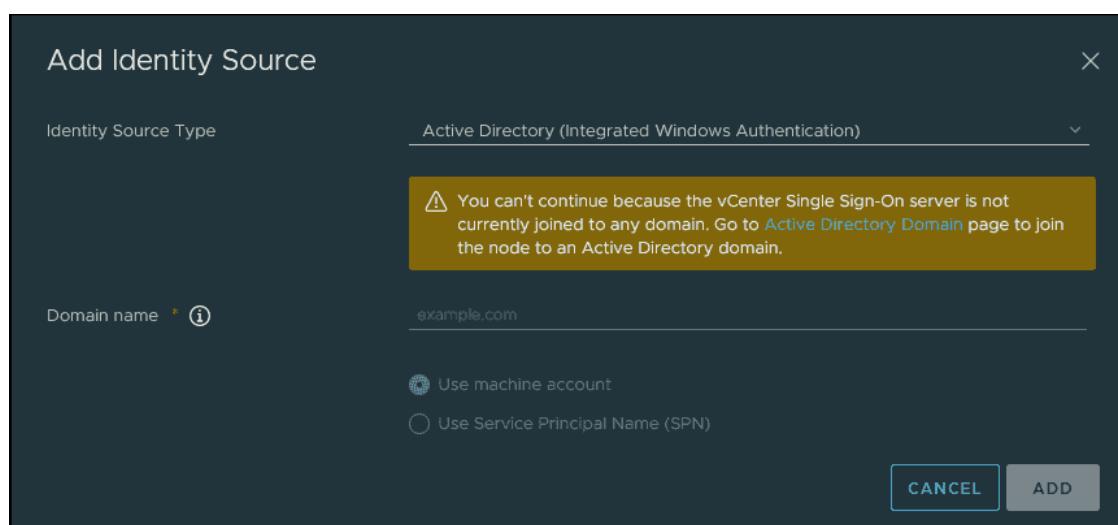
I thought that VMware is better than Microsoft, but both vendors' products need a reboot when changing Microsoft AD specifications, changing domain, going from workgroup to domain, etc.



Join 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.*

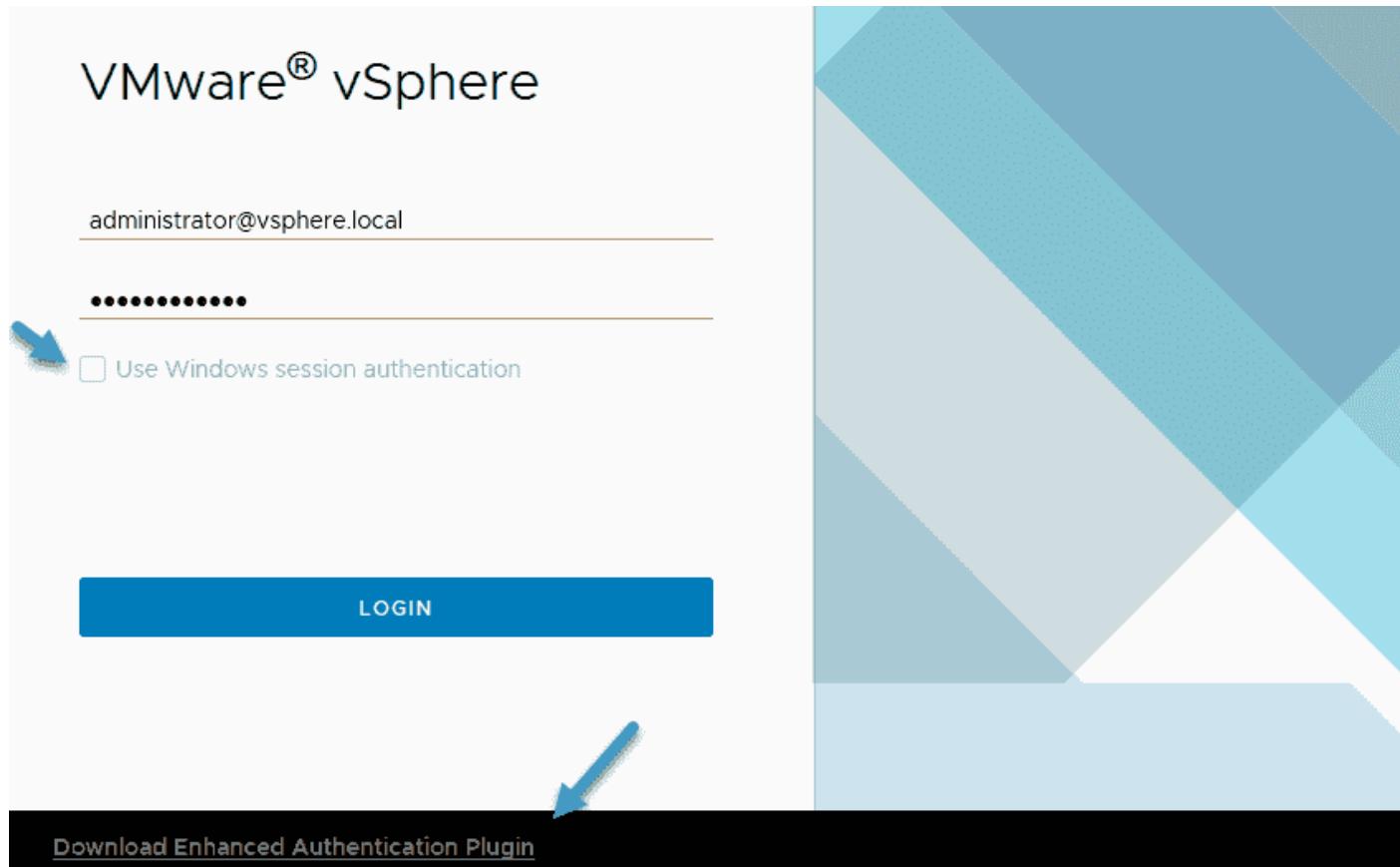


Change identity source type

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 tick the check box «use Windows session authentication» when connecting to vCenter Server.

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



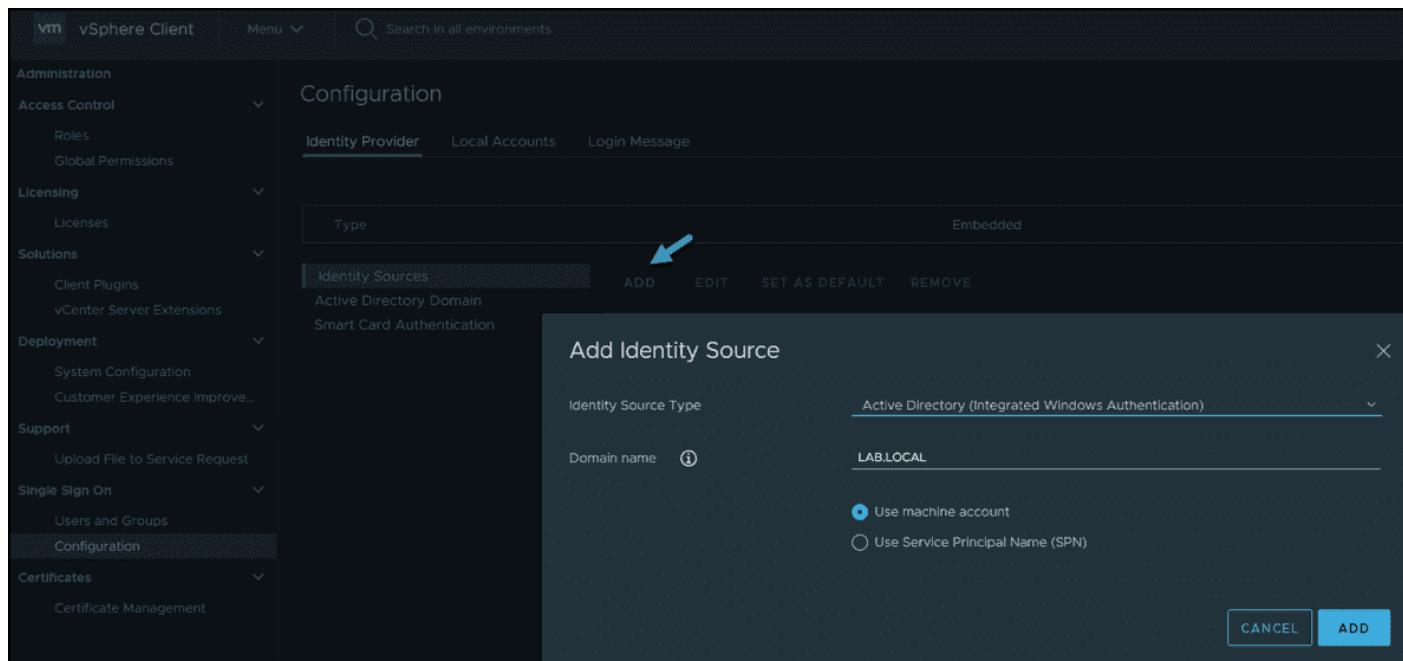
Use Windows session authentication is grayed out

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

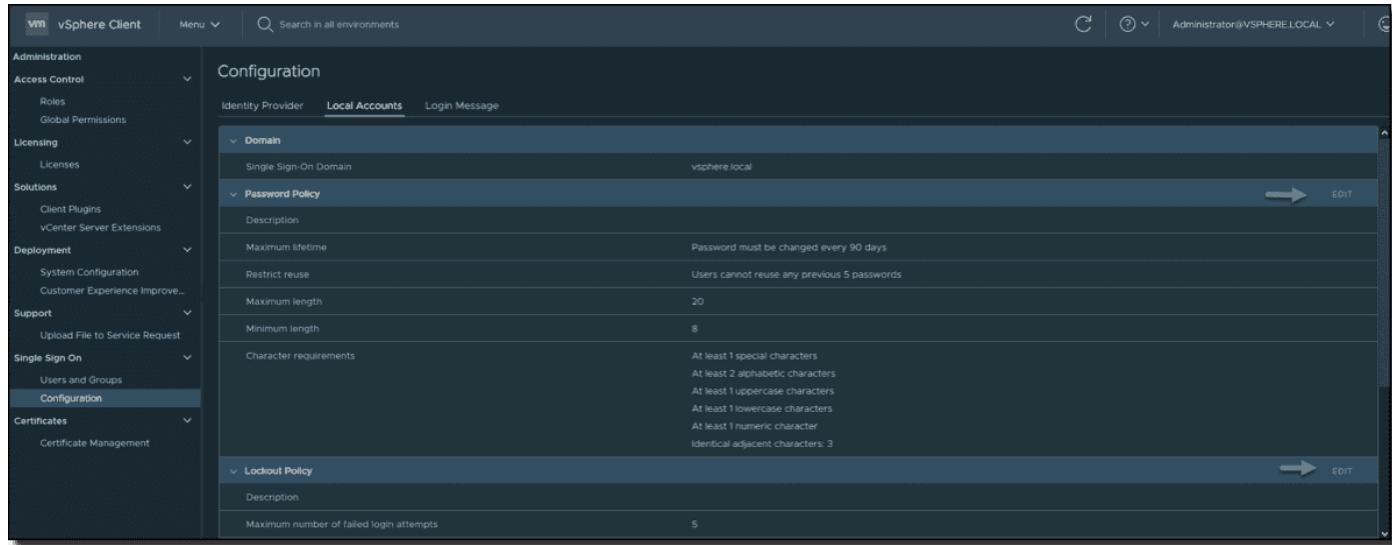
## Users and groups

**Users and groups** is also found in the same section. We can 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.

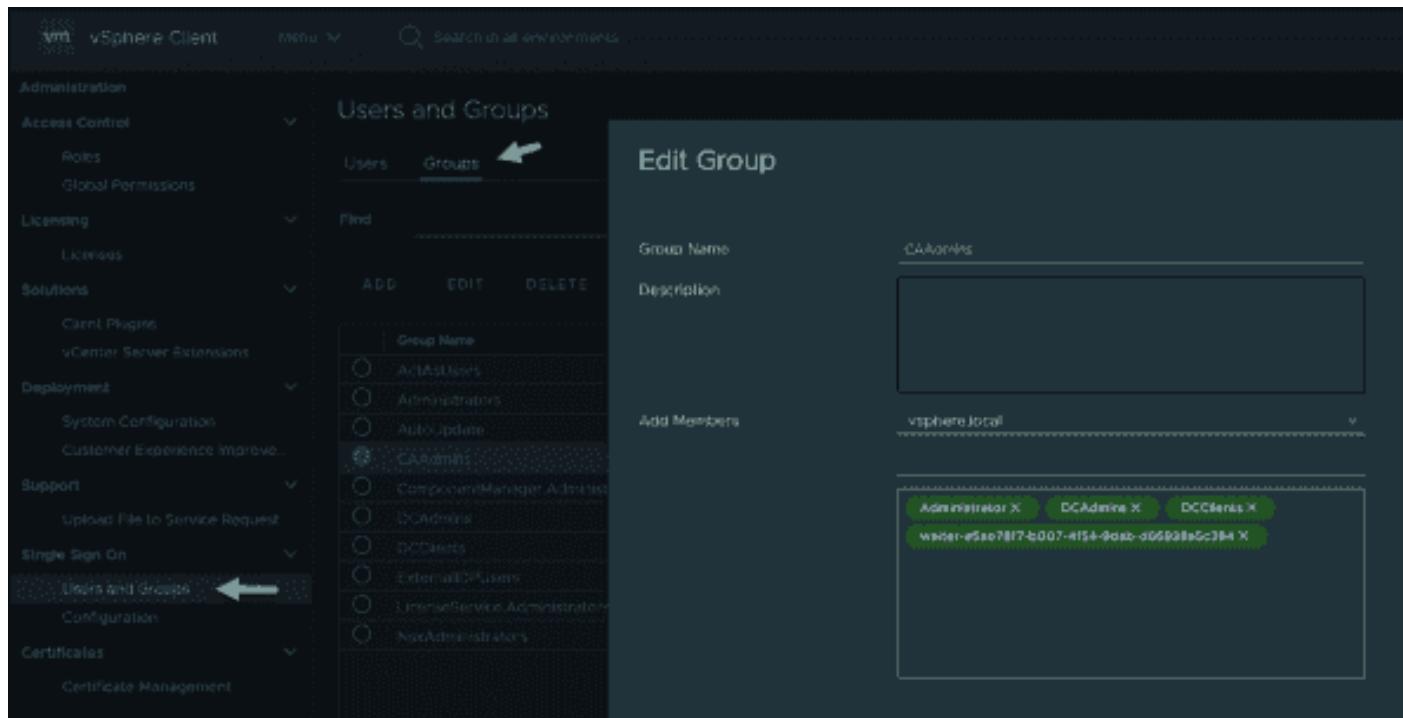


Possibility to change local password policy

## 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.

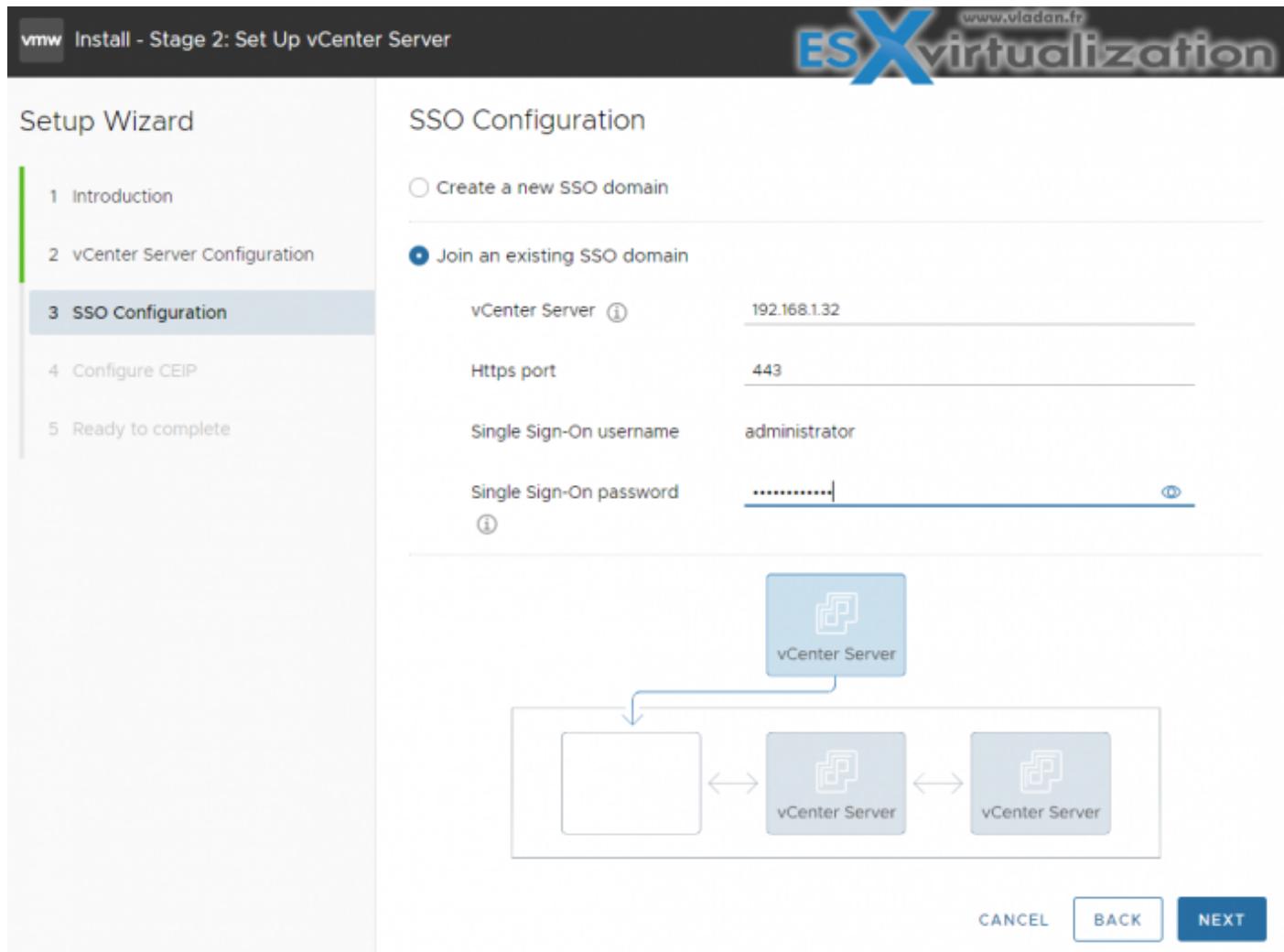
However, for some services that are not managed by vCenter Server directly, you'll need to be a member of certain SSO groups that determine the privilege. For example, a user who is a member of the Administrators group can manage vCenter Single Sign-On. A user who is a member of the CAAdmins group can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



Example of CAAdmins group

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

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



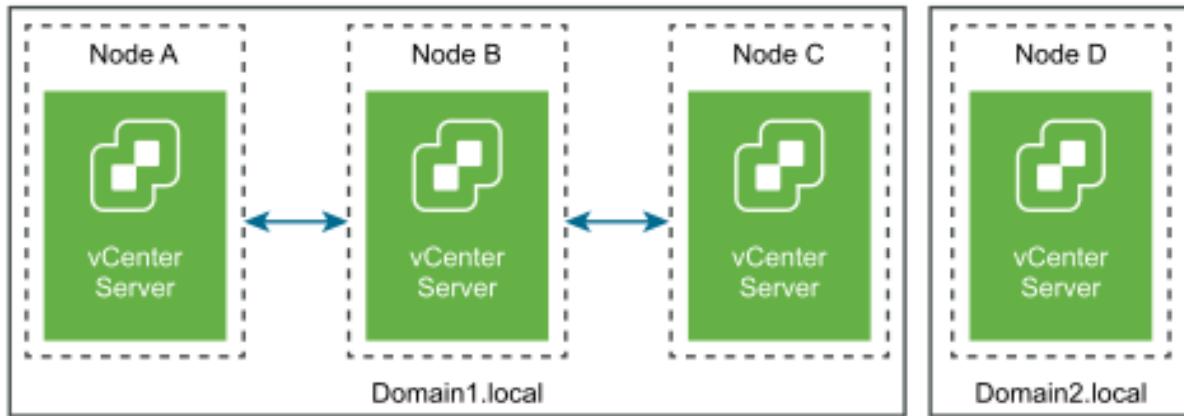
SSO Domain Repointing was introduced in vSphere 6.7 to allow the repointing of a vCenter Server from one SSO Domain to another. Let's say you have an environment with a couple of vCenter Servers, each within one site. One day, your boss tells you that your company just bought another company and that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

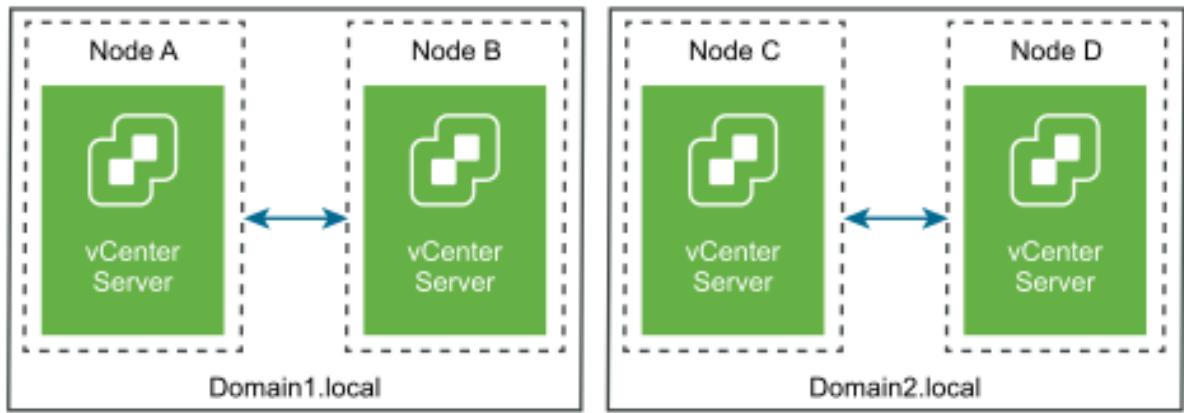
Screenshot from VMware documentation...

## 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 below on the reporting process :

1. Shut down the node (for example, Node C) that is being repointed (moved to a different domain).
2. 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.

3. Power on Node C to begin the repointing process.
4. 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.

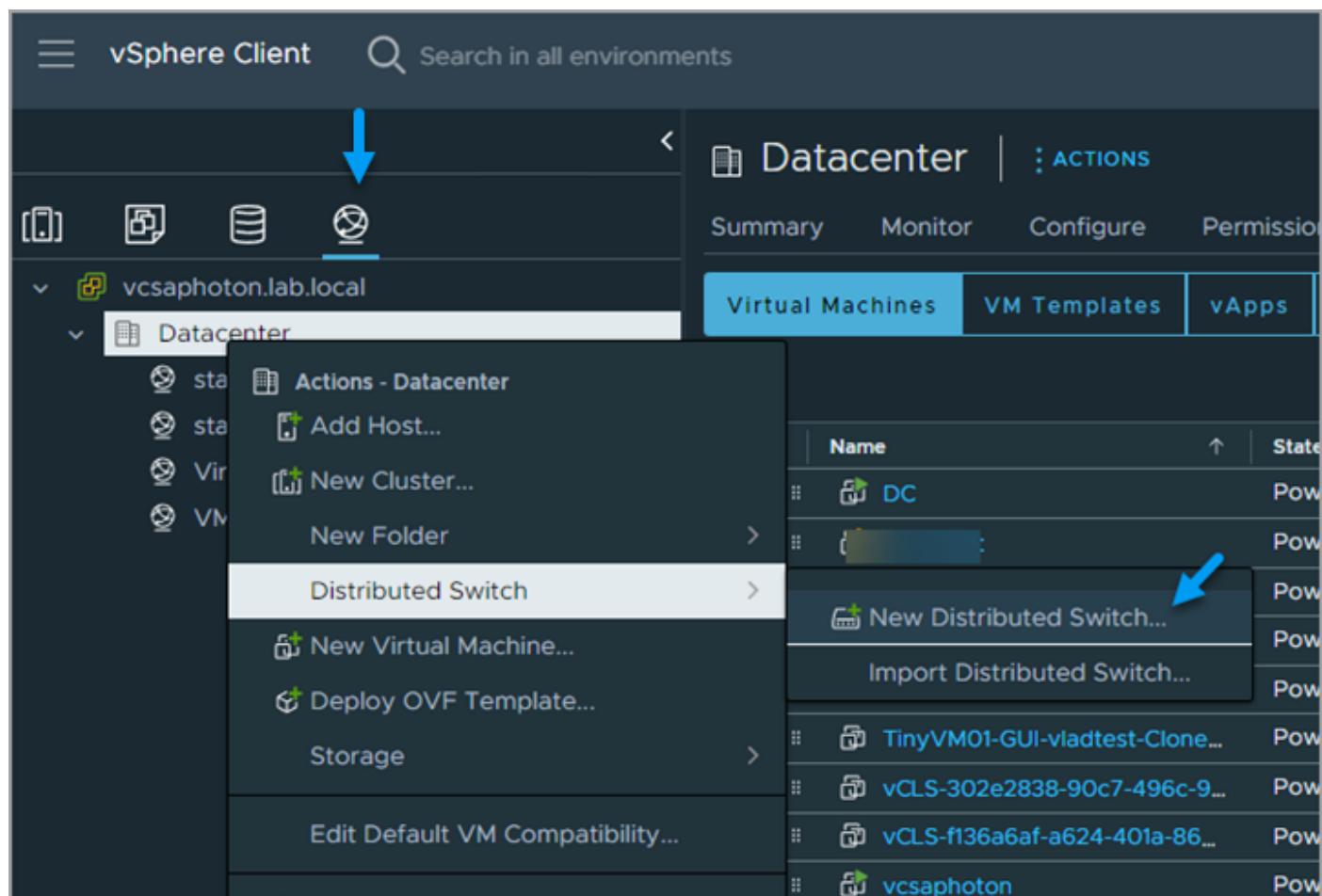
For example, run the execute command with the following:

```
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.

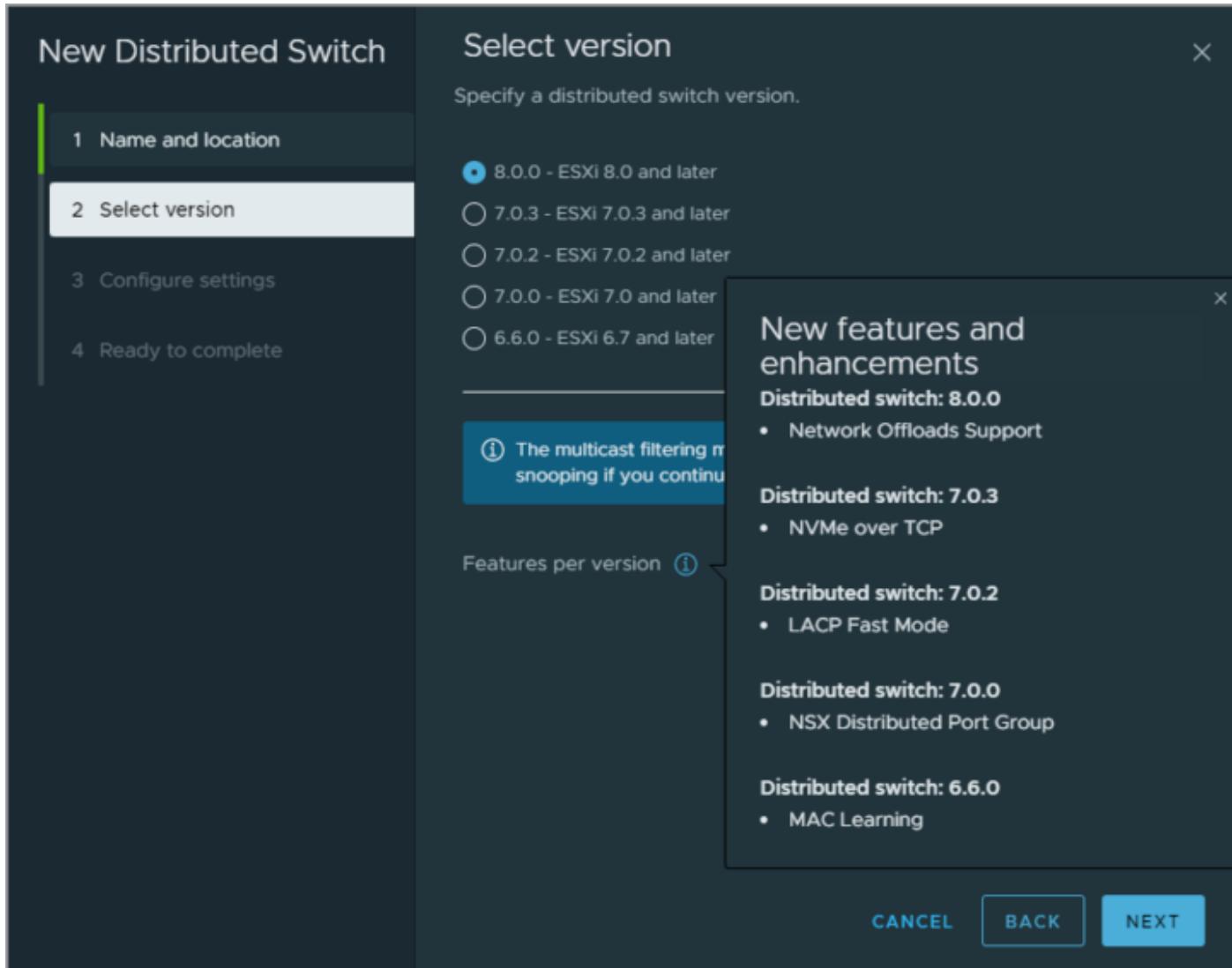
## Objective 4.2 Configure vSphere distributed switches

The configuration of vSphere Distributed Switch (vDS) starts with its creation. By default, vSphere does not contain one. **Select the network icon > Right click Datacenter > Distributed Switch > New Distributed Switch.**

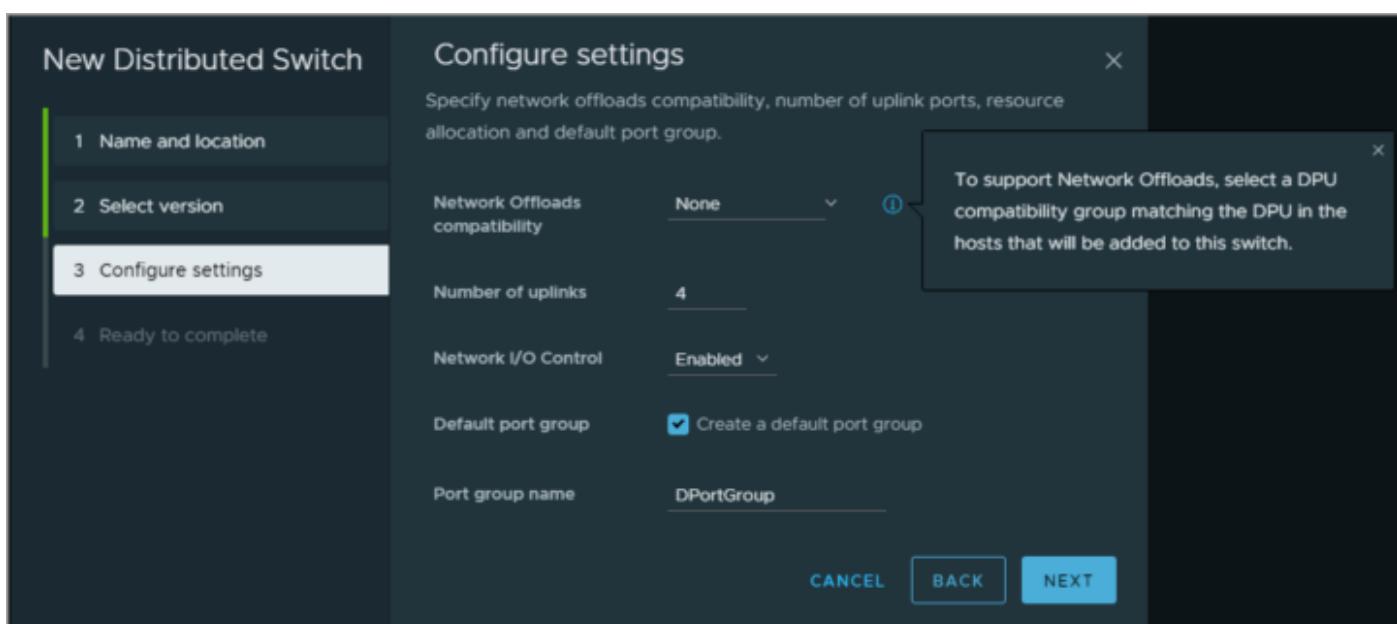


A new wizard will guide you through the process.

Put some meaningful name and then select the version. Within vSphere 8 you can create different versions of vDSs. You can go from version 6.6 up all the way up to version 8.0.



And then on the next screen, you'll have an option to pick Network Offloads compatibility, number of uplinks, Network I/O control (NIOC) and port group name.



## Add host to vDS

Select **vDS > Hosts > Actions > Add and manage hosts**

Host	Host state	Cluster	Compatibility
192.168.1.10	Not responding	HA cluster	Compatible
192.168.1.11	Connected	HA cluster	Compatible
192.168.1.14	Not responding	HA cluster	Compatible
<input checked="" type="checkbox"/> 192.168.1.15	Connected	N/A	Compatible
esxinuc.lab.local	Connected	N/A	Compatible

Host	Adapter assigned to switch
192.168.1.15	vSwitch0

## Examine the distributed switch configuration

vSphere Distributed Switch handles VMkernel adapters for vSphere vMotion and for the management network, and virtual machines grouped. You can use the central topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

You can modify all vDS settings from here. You can change the vDS name, configure uplinks, activate NIOC, LACP, [Private VLANs](#), Port Mirroring, create DVswitch port groups ...

## Objective 4.2.1 - Create a distributed switch

Covered in 4.2

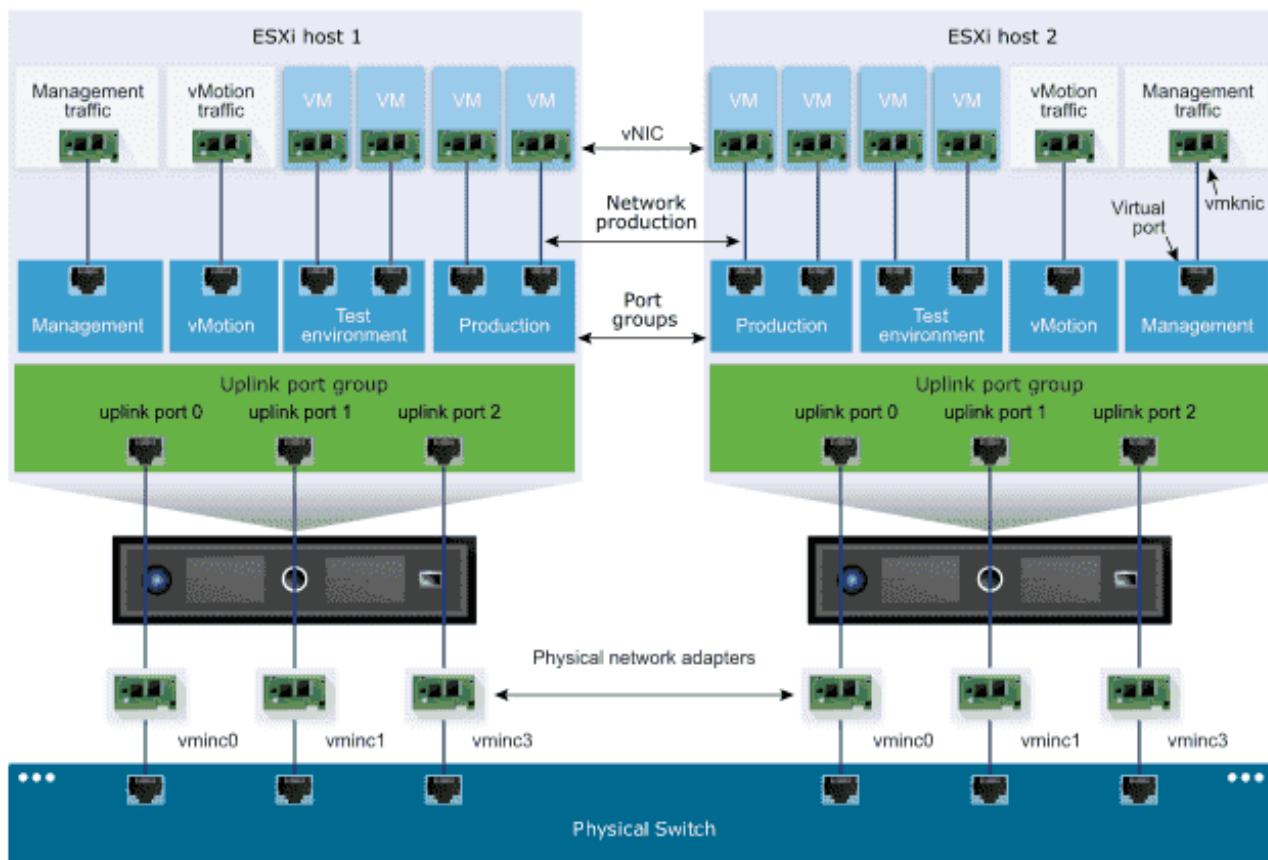
## Objective 4.2.2 - Add ESXi hosts to the distributed switch

Covered in 4.2

## Objective 4.3 - Configure Virtual Standard Switch (VSS) advanced virtual networking options

### 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.

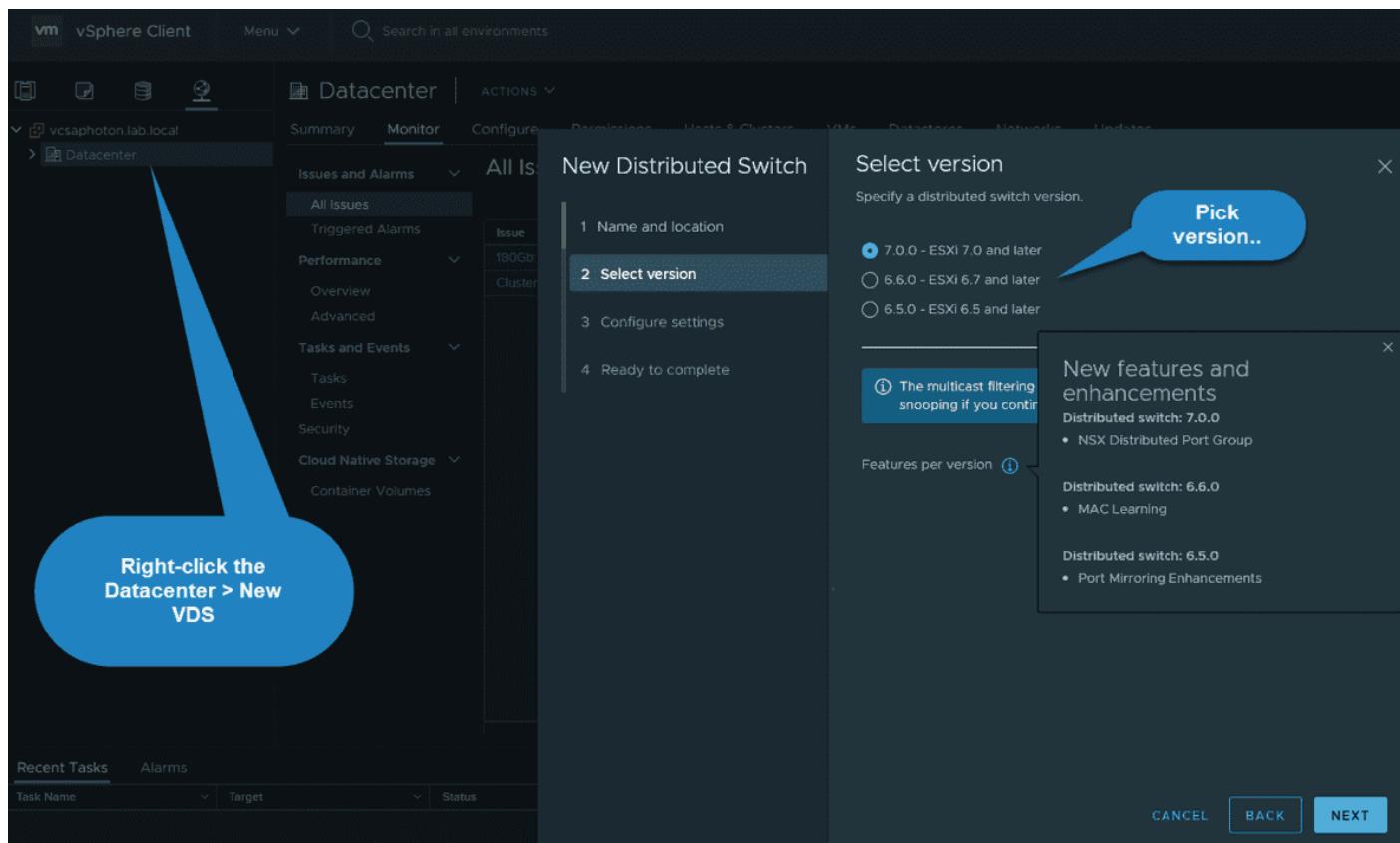


Connectivity with the vSphere Standard Switch

## vSphere Distributed Switch

Imagine VDS as a single switch connected with all associated hosts in a data center. 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 8 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 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.

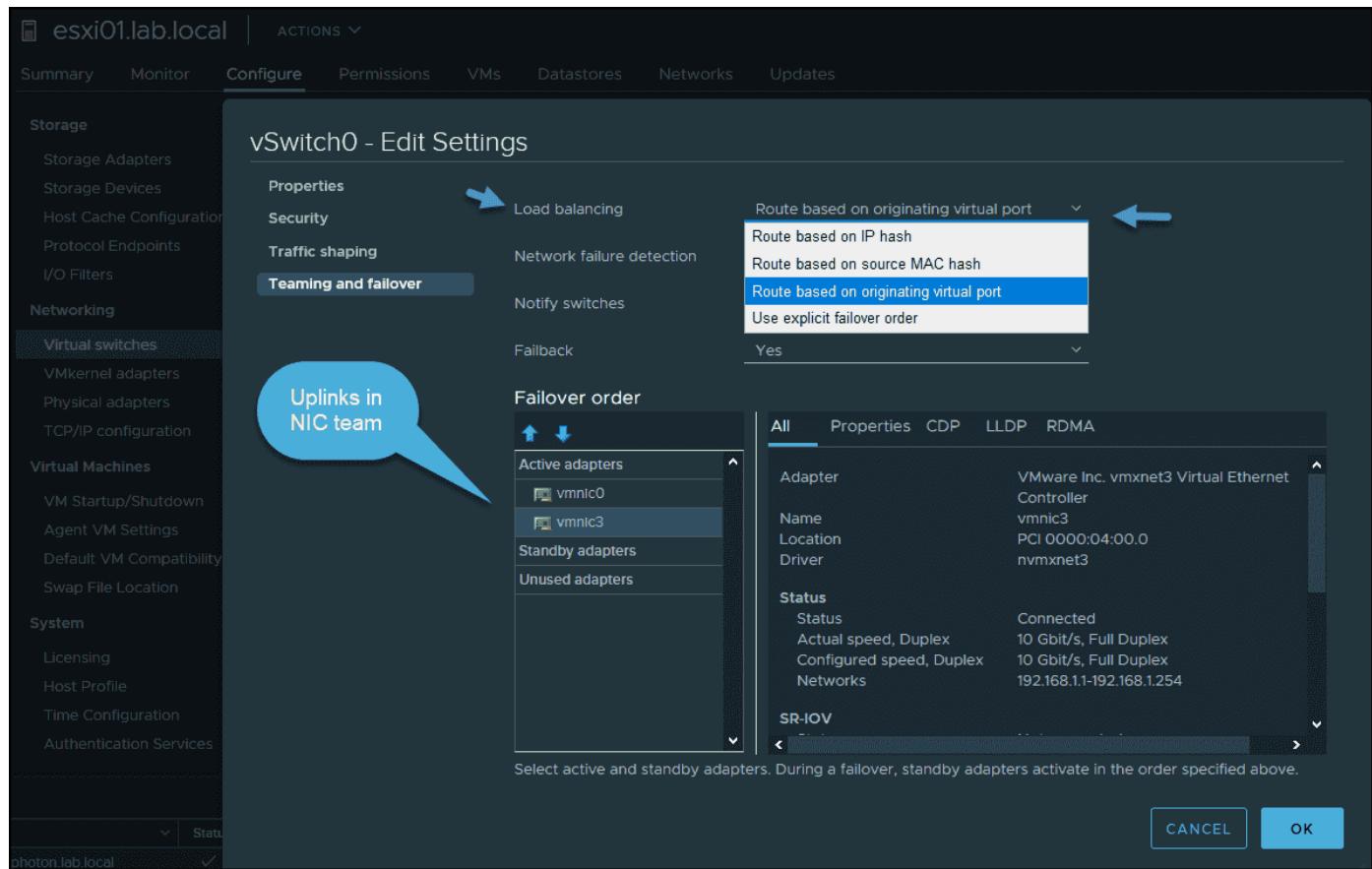
#### Route based on physical (only available for VDS)

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.

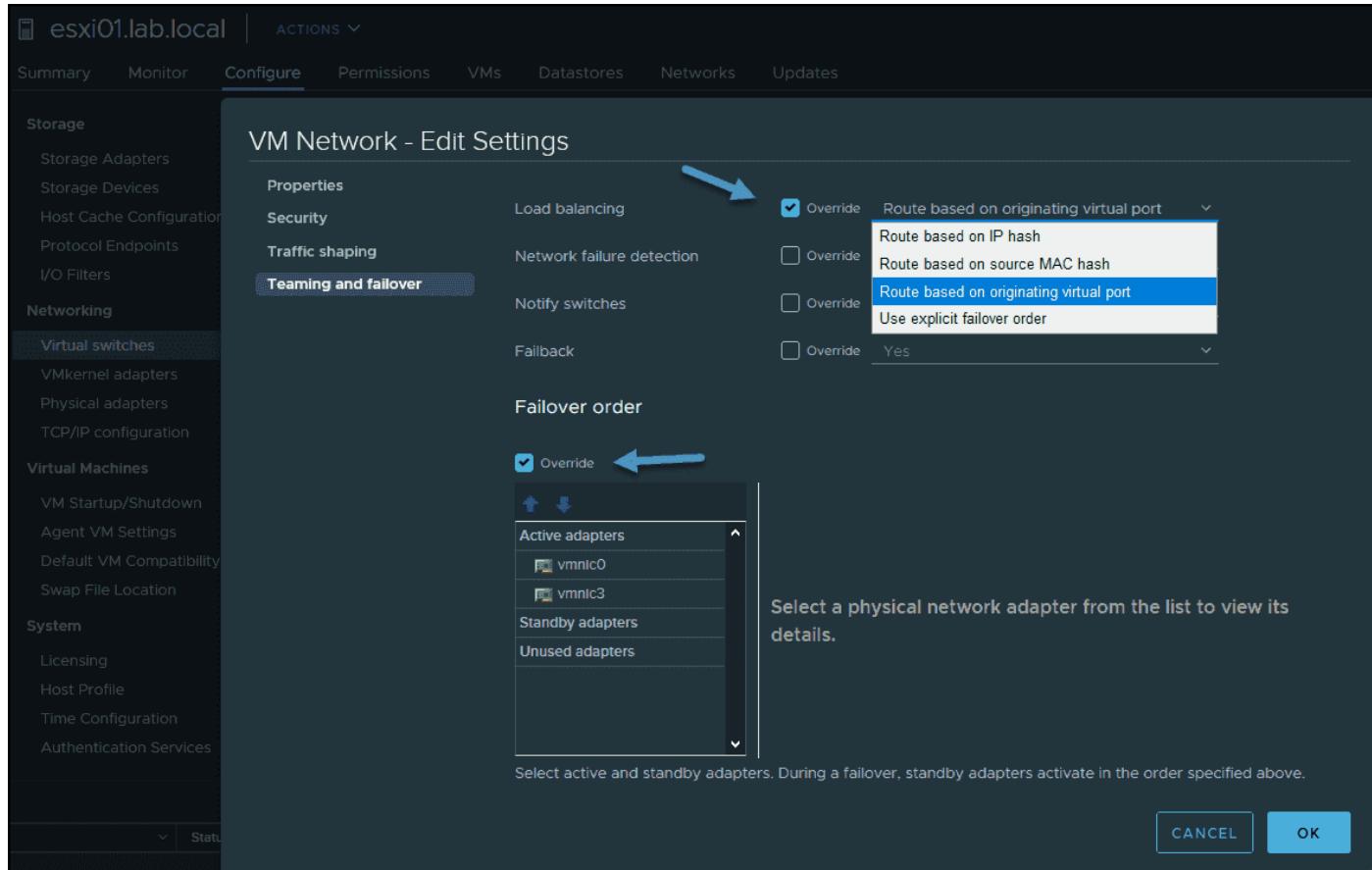
## Use Explicit Failover Order

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.



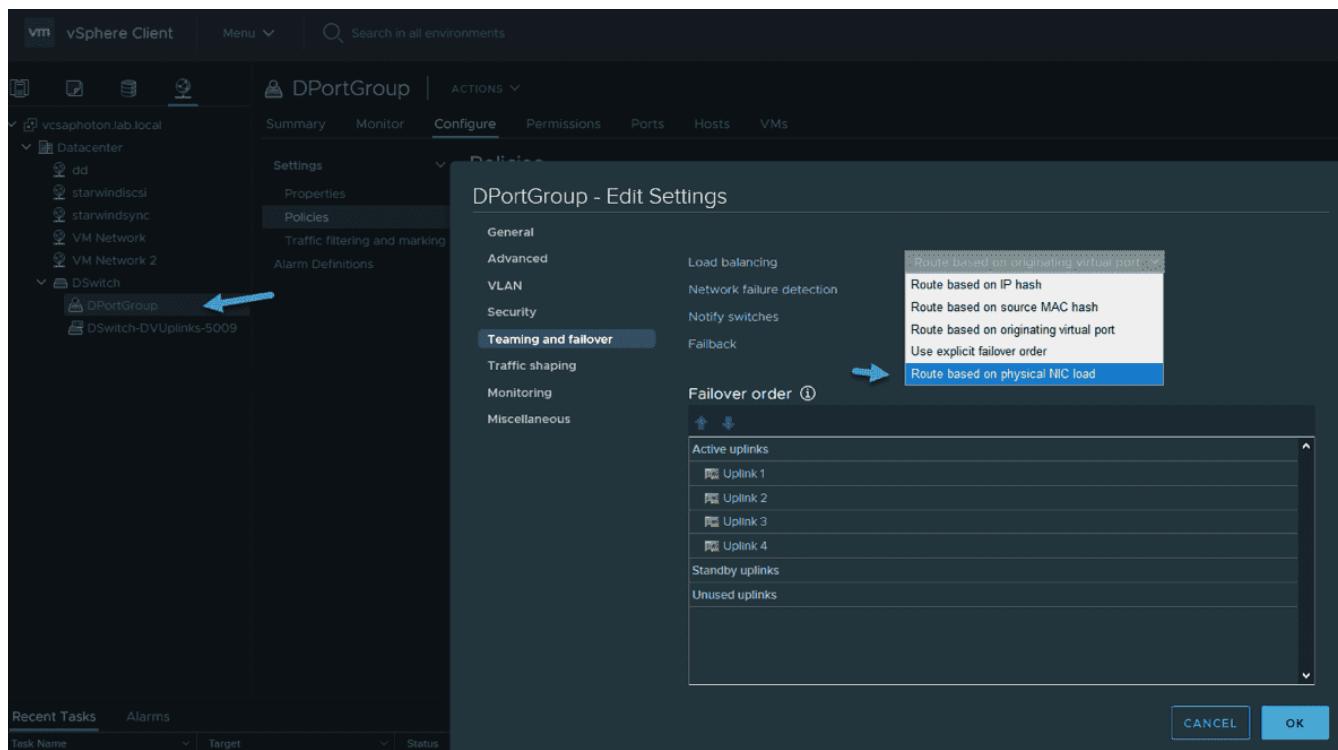
### Changing load balancing policy on vSwitch

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 4.4 – Setup Identity Sources

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 stored either 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 8?

- **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

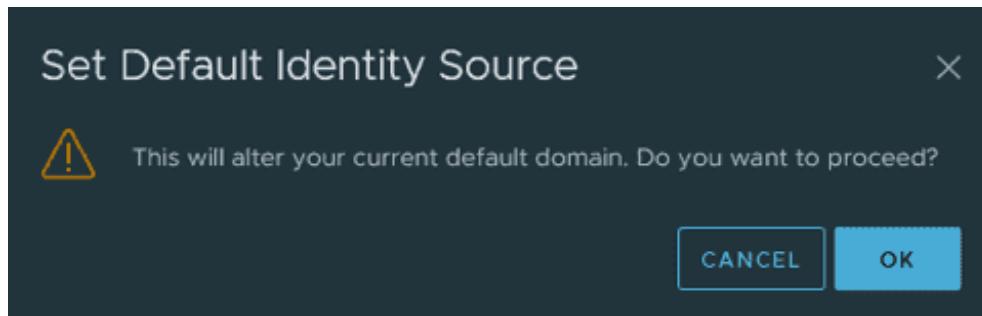
Connect to the vCenter Server with the default [administrator@vsphere.local](mailto:administrator@vsphere.local) login and password. This is the default that you created during the installation process. (Note: if you created a different domain during the installation, connect via administrator@yourdomain.)

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.

### How about the near future with 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 behavior 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 are 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 recommendations 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.

The screenshot shows the vSphere Client interface with the title bar "vSphere Client". The left sidebar has a "Configuration" section selected. Under "Identity Provider", the "Active Directory Domain" tab is selected, showing the "vcsaphoton.lab.local" node joined to the domain. There are "JOIN AD" and "LEAVE AD" buttons above the list of nodes.

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**.

There is another one, **service-control**, that 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 4.4.1 – Configure identity federation

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 trust that a particular user is authenticated and can be granted access to secure documents and corporate emails.

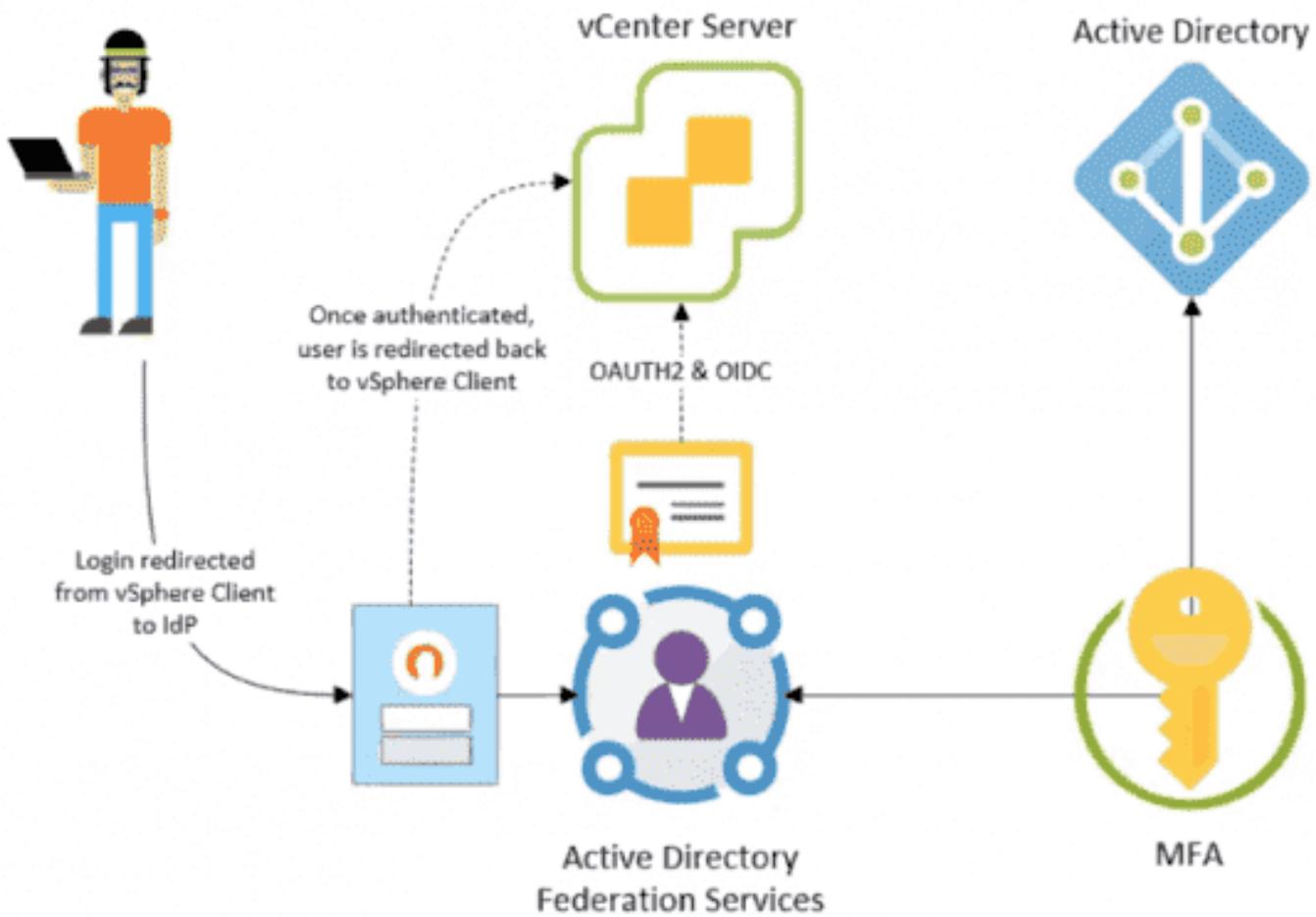
Identity management is one of the key elements needed for each organization to remain secure. Organizations are looking to consolidate their authentication into dedicated identity providers with flexible options, such as Multi-Factor Authentication (MFA). Another consideration is the reduction of risk 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 will 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.

In this initial release, vSphere and ADFS will 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 will be a new wizard that will allow 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.

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

#### 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 post.

Other configurations are also needed, such as users and group configuration, as well as permission configuration within the vCenter SSO Administration section.

## Objective 4.4.2 – Configure 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 use 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 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.*

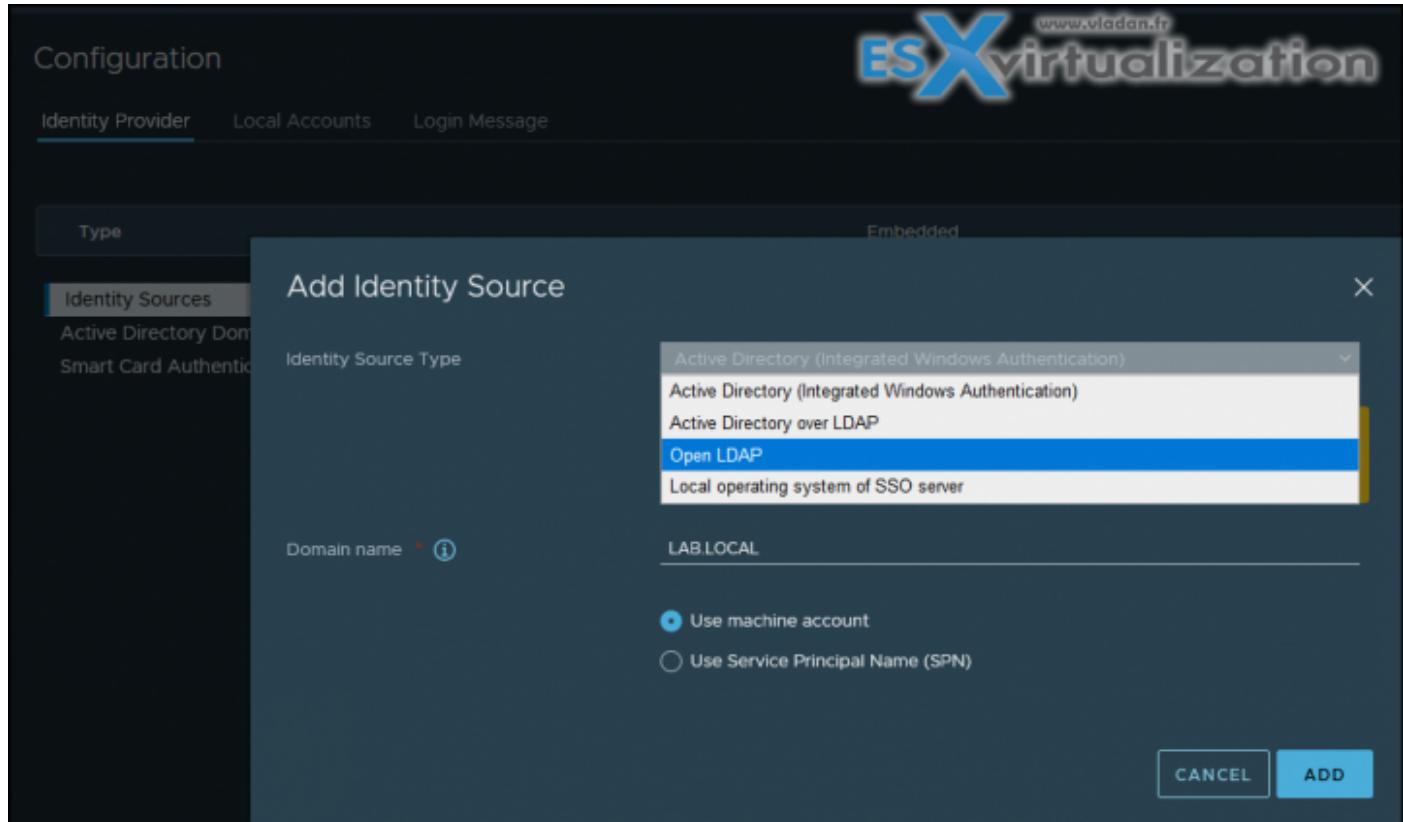
Note that OpenLDAP is also supported, but there are some requirements that need to be met:

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 in 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 4.5 – Deploy and configure VMware vCenter Server Appliance (VCSC)**

### System Requirements for VCSC 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.

This single ISO has everything so you can **Install, Upgrade, Migrate or Restore**.

The installation order is as follow:

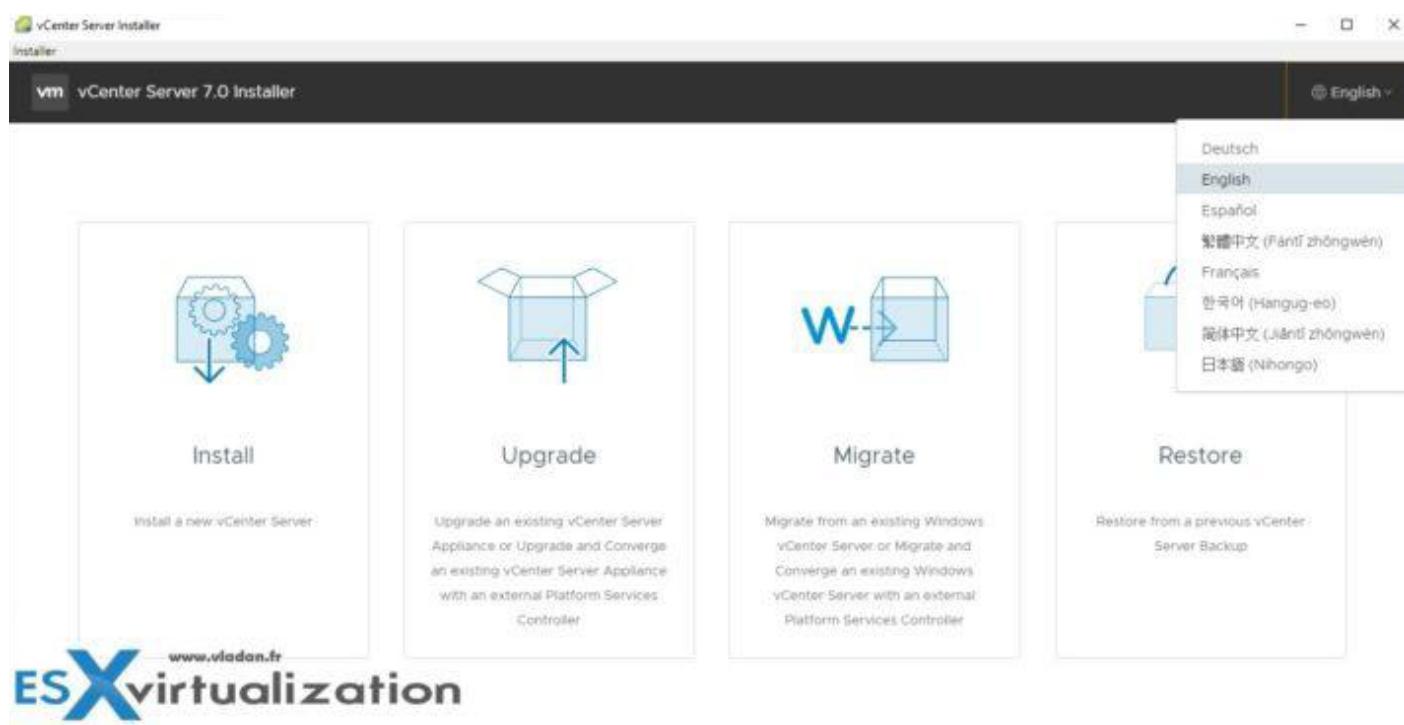
Install ESXi on at least one host, then setup ESXi, deploy vCenter Server Appliance (VCSC). Login to vSphere client to create and organize your vCenter server inventory.

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 and inside we have 3 folders:

1. lin64
2. mac
3. win32

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



As you can see, there are different languages available for installation.

The GUI deployment is a two-stage process. The first stage is a deployment wizard that deploys the OVA file of the appliance on the target ESXi host or vCenter Server instance. After the OVA deployment finishes, 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 a 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.

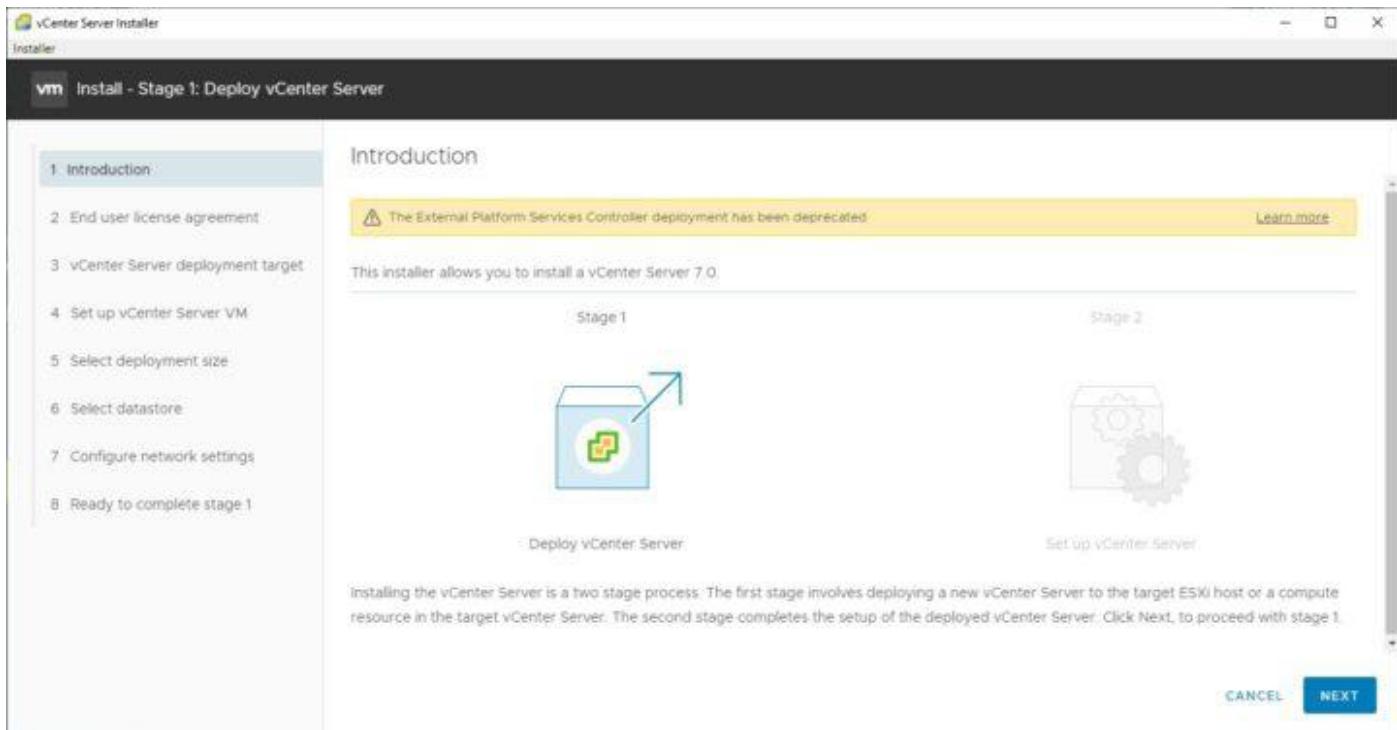
Version 7.0 of vCenter Server is deployed with virtual hardware version 10, which supports 64 virtual CPUs per virtual machine in ESXi.

## Where is Platform Service Controller (PSC)?

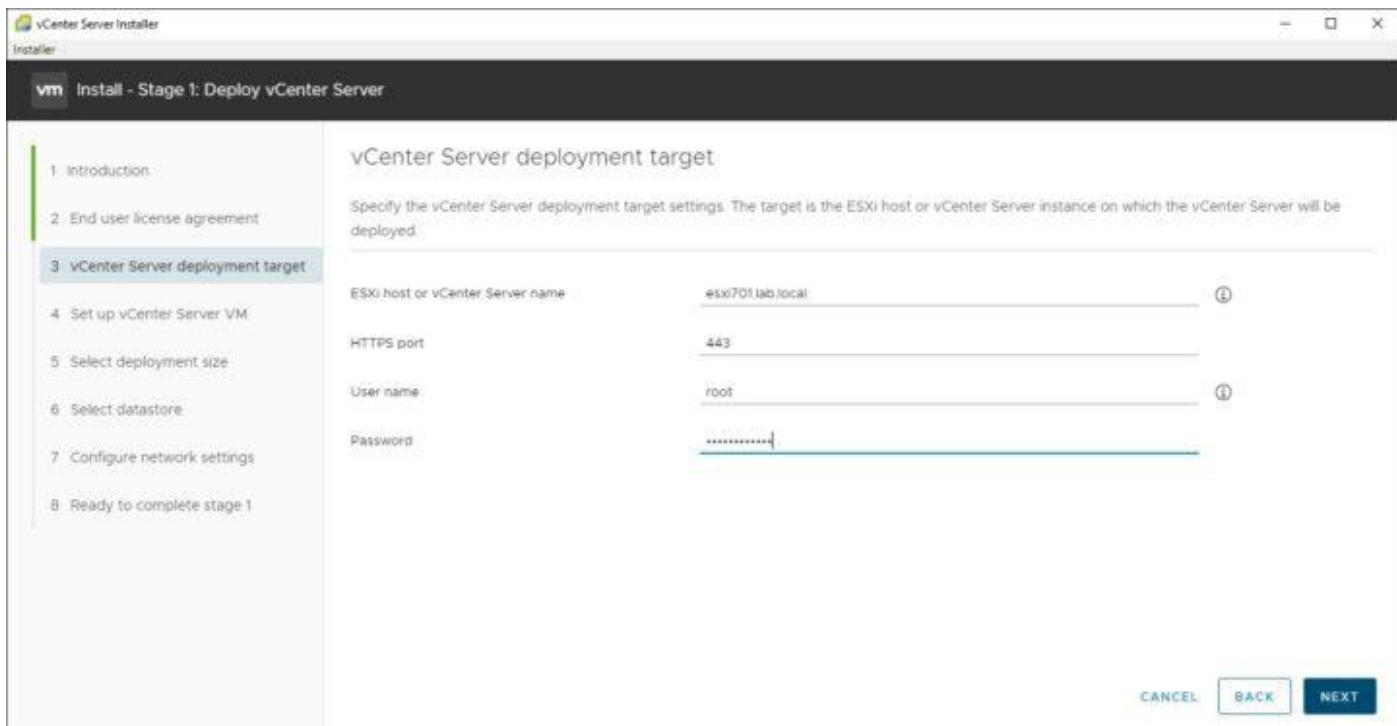
No more external PSC. vCenter Server contains all Platform Services Controller services, preserving the functionality and workflows, including authentication, certificate management, tags, and licensing. It is no longer necessary nor possible to deploy and use an external Platform Services Controller. All Platform Services Controller services are consolidated into vCenter Server.

Which services are installed with vCenter server?

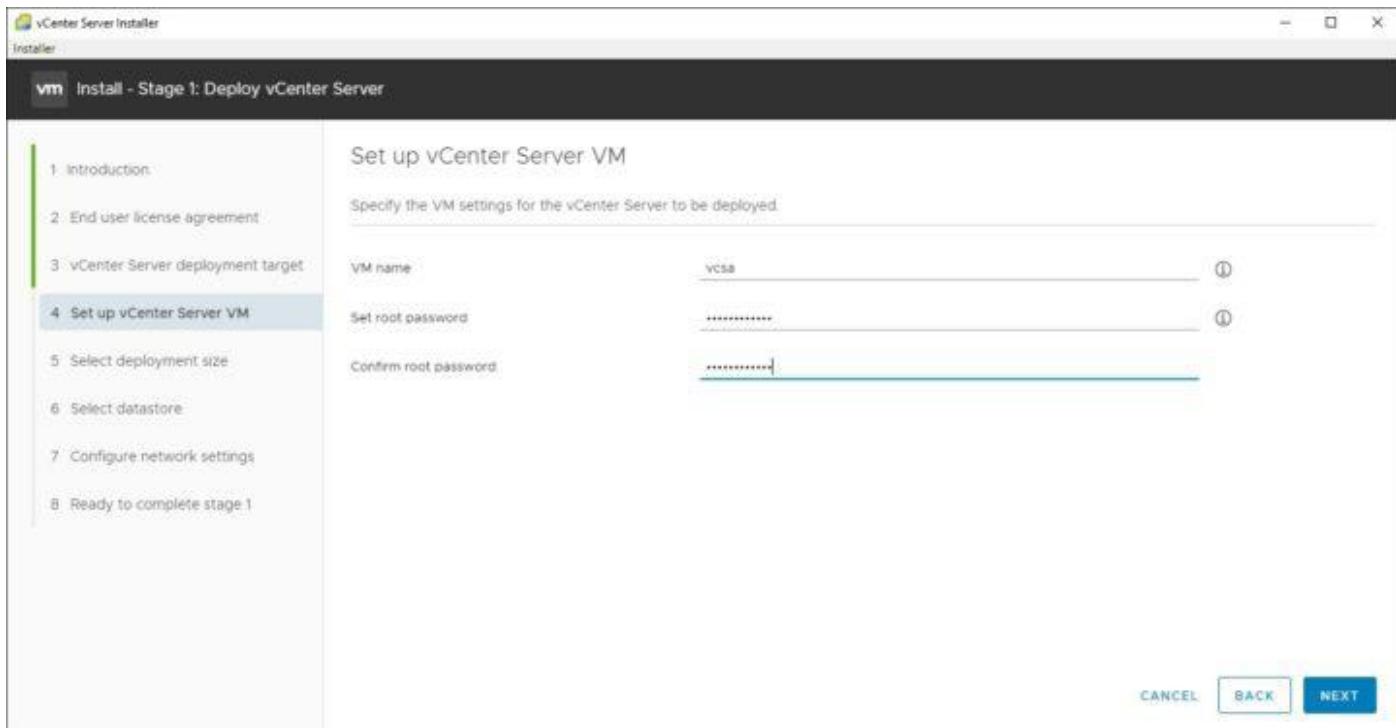
- **PostgreSQL** – a DB bundled and preinstalled. It is a VMware distribution of PostgreSQL database for vSphere and vCloud Hybrid Services.
- **vSphere Client** – HTML 5 UI which can be accessed through web browser. No more Macromedia/Adobe Flash.
- **ESXi Dump Collector** – The vCenter Server support 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** – 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.



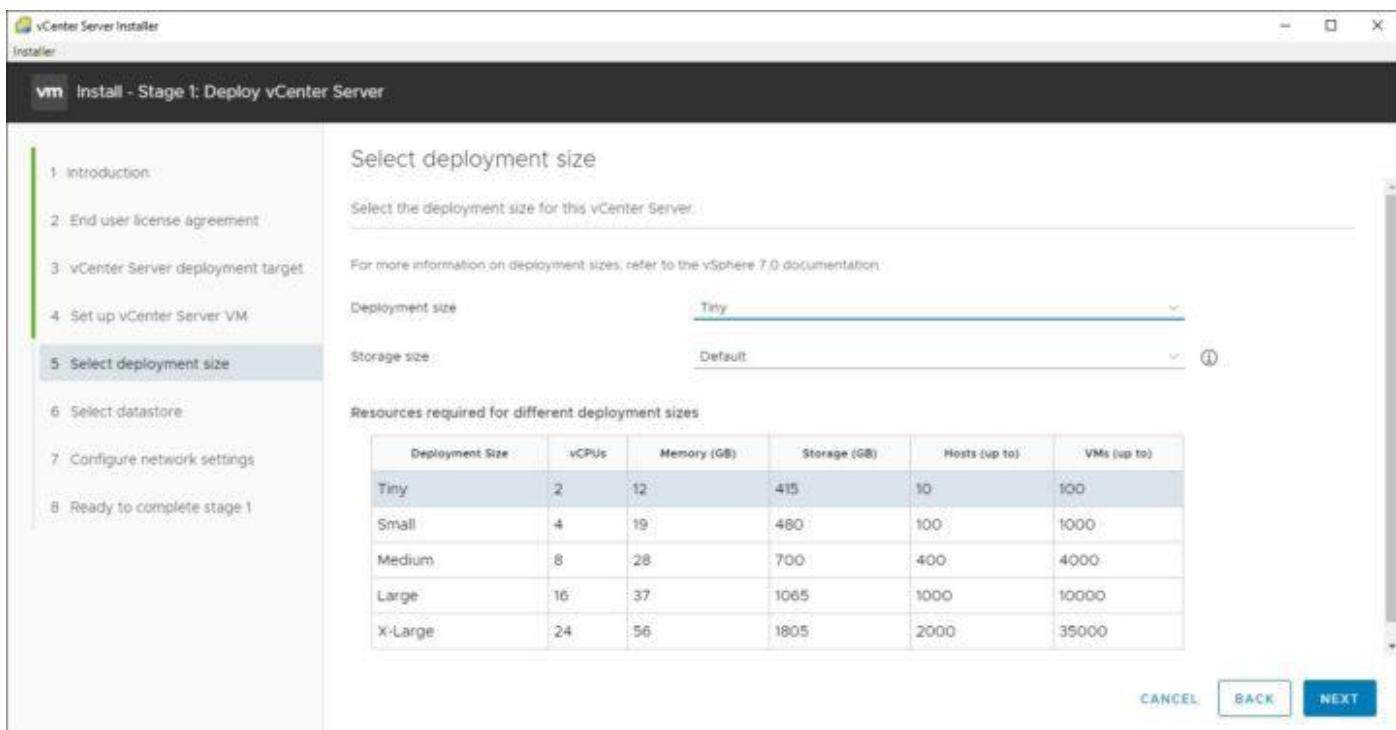
then



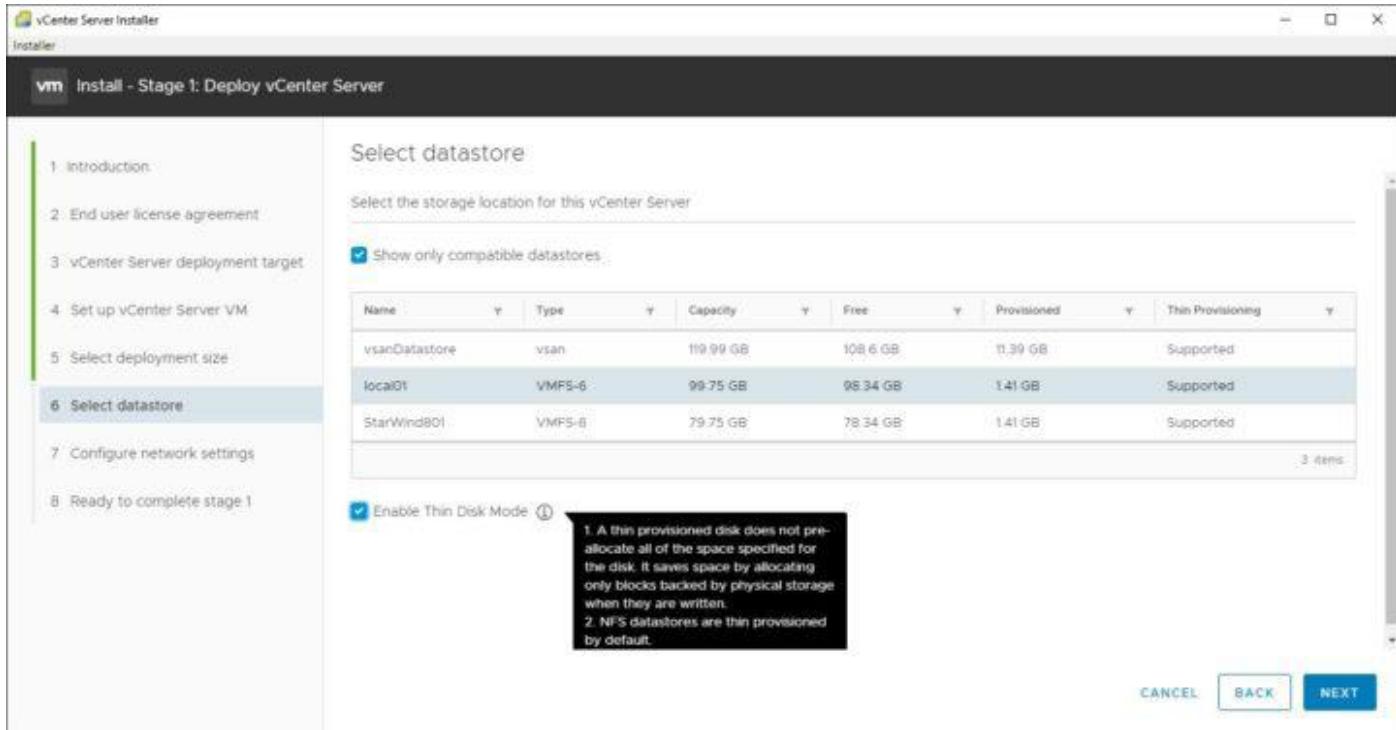
then



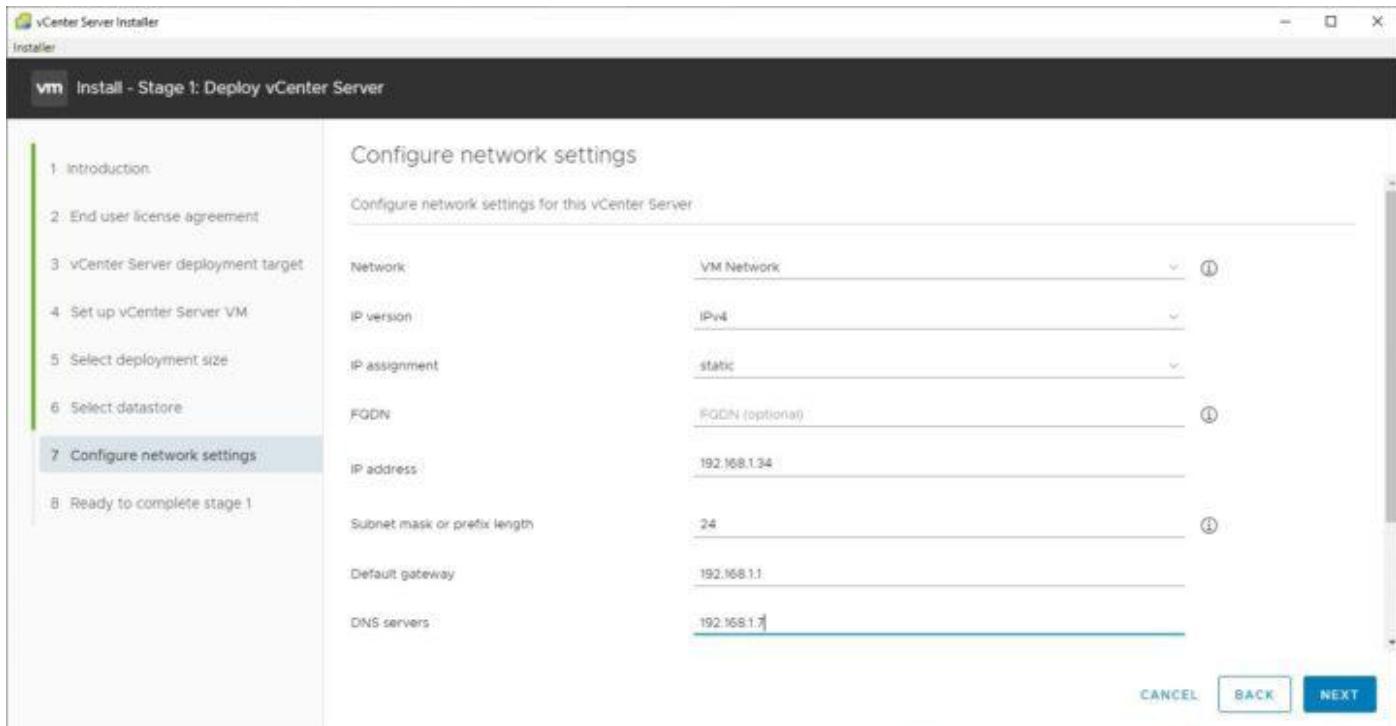
then



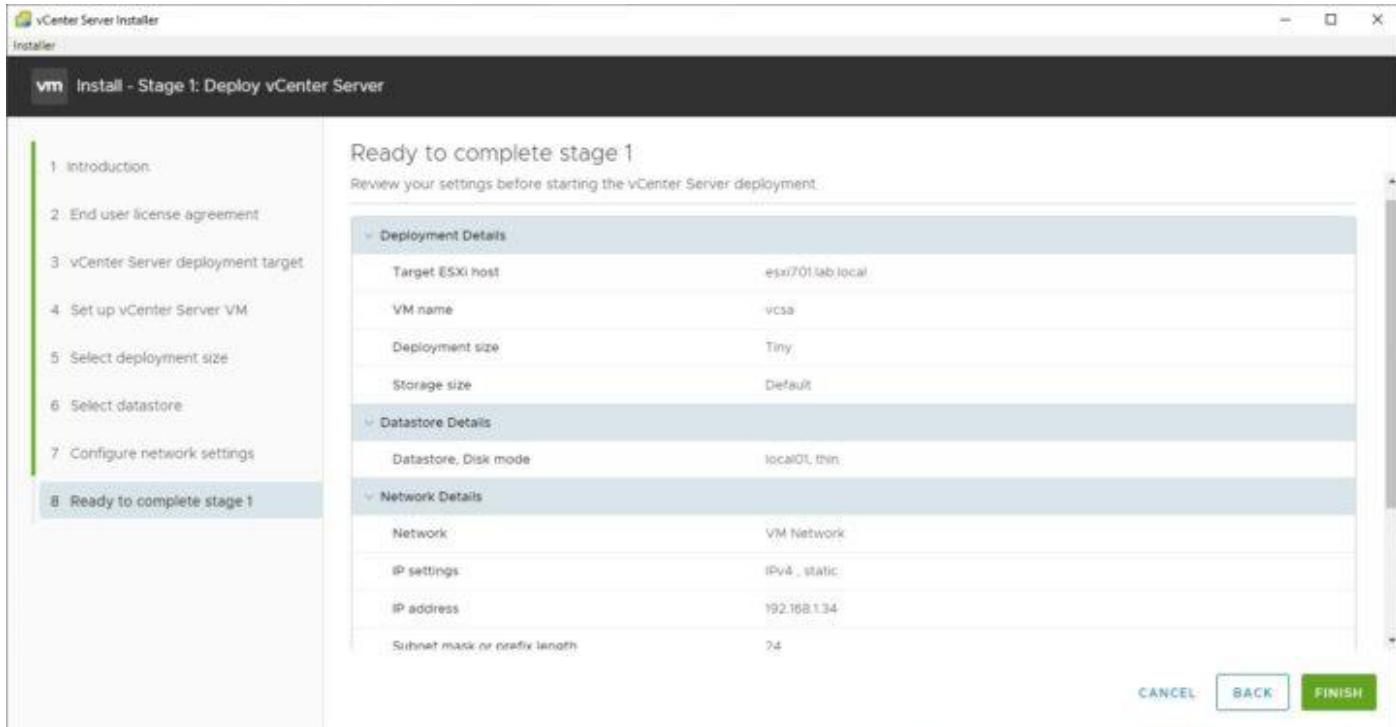
then



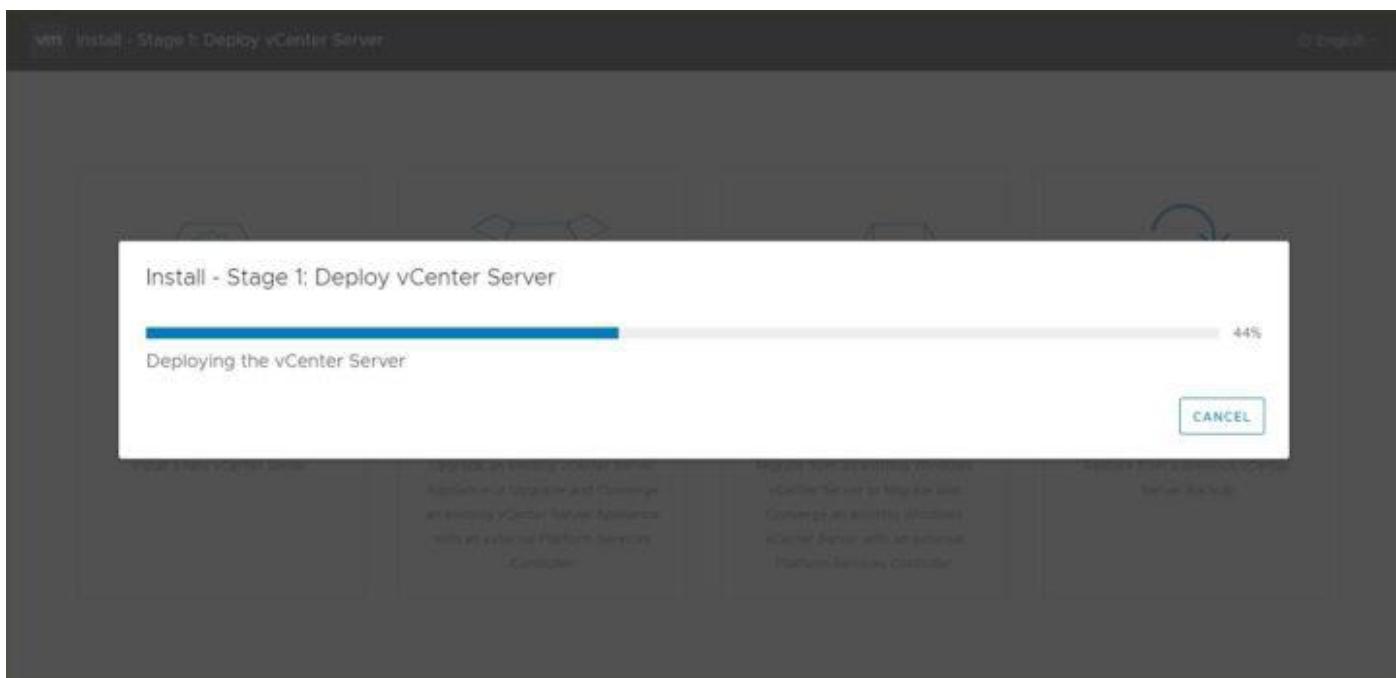
then



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.

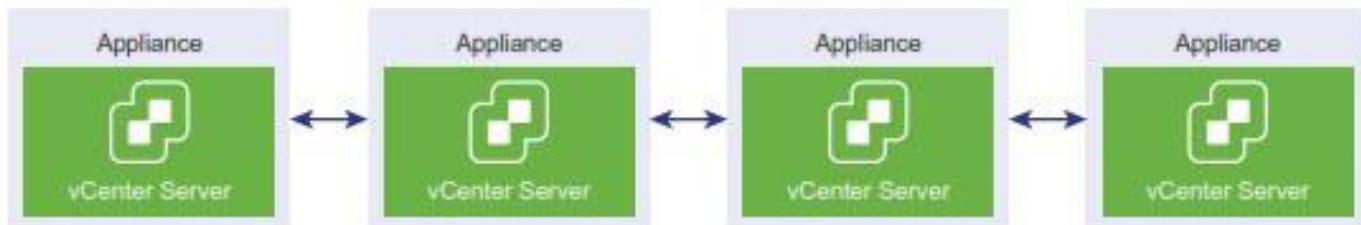
## vCenter Enhanced Linked Mode

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 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 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

ⓘ 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.

**vm Install - Stage 2: Set Up vCenter Server**

1 Introduction

2 vCenter Server configuration

3 SSO configuration

4 Configure CEIP

5 Ready to complete

**Introduction**  
vCenter Server installation overview

Stage 1      Stage 2




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

**vm Install - Stage 2: Set Up vCenter Server**

1 Introduction

2 vCenter Server configuration

3 SSO configuration

4 Configure CEIP

5 Ready to complete

**vCenter Server configuration**

Time synchronization mode	Synchronize time with the ESXi ho ▾
SSH access	Disabled ▾

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

CANCEL      BACK      NEXT

Then

Install - Stage 2: Set Up vCenter Server

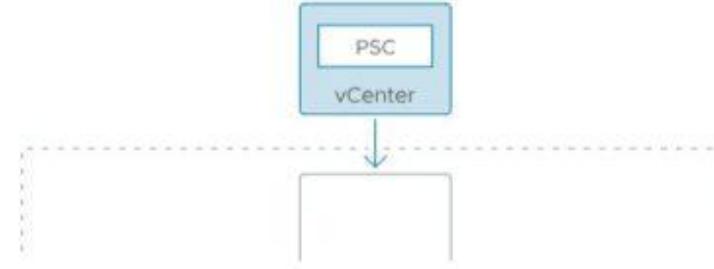
1 Introduction  
2 vCenter Server configuration  
**3 SSO configuration**  
4 Configure CEIP  
5 Ready to complete

**SSO configuration**

Create a new SSO domain

Single Sign-On domain name	vladan.lab	(i)
Single Sign-On user name	administrator	
Single Sign-On password	*****	(i)
Confirm password	*****	

Join an existing SSO domain



CANCEL BACK NEXT

Then 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	vcse.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**

## Objective 4.6 – Create and configure VMware HA and DRS advanced options (Admission Control, Proactive HA, etc.)

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 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 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.

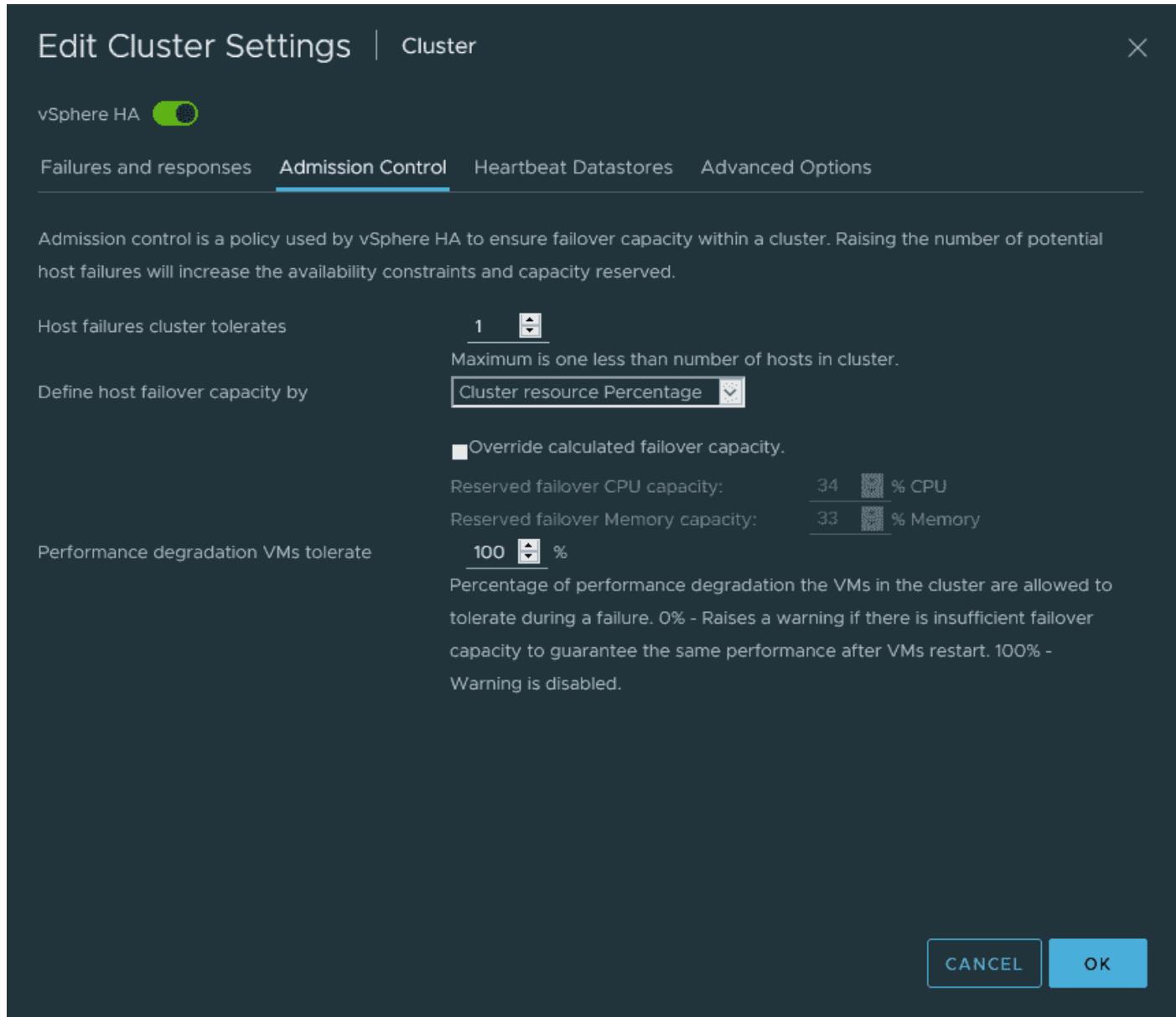
Selecting either quarantine or maintenance mode will apply the same response for both moderate and severe failures. Selecting mixed mode will enforce quarantine mode for moderate failures and maintenance mode for severe failures.

The screenshot shows the 'Edit Proactive HA' dialog box for a 'Cluster'. At the top, there is a 'Status' toggle switch which is turned on (green). Below it, there are two tabs: 'Failures & Responses' (which is selected) and 'Providers'. A descriptive text block explains that Proactive HA responds when a provider notifies health degradation to vCenter. Under the 'Automation Level' section, a dropdown menu is set to 'Automated', with a note below stating that virtual machines will be migrated to healthy hosts and degraded hosts will be entered into quarantine or maintenance mode. In the 'Remediation' section, a dropdown menu is set to 'Maintenance mode', with a note below stating that it ensures VMs do not run on partially failed hosts. At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

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 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 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 at the beginning of the post, 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.

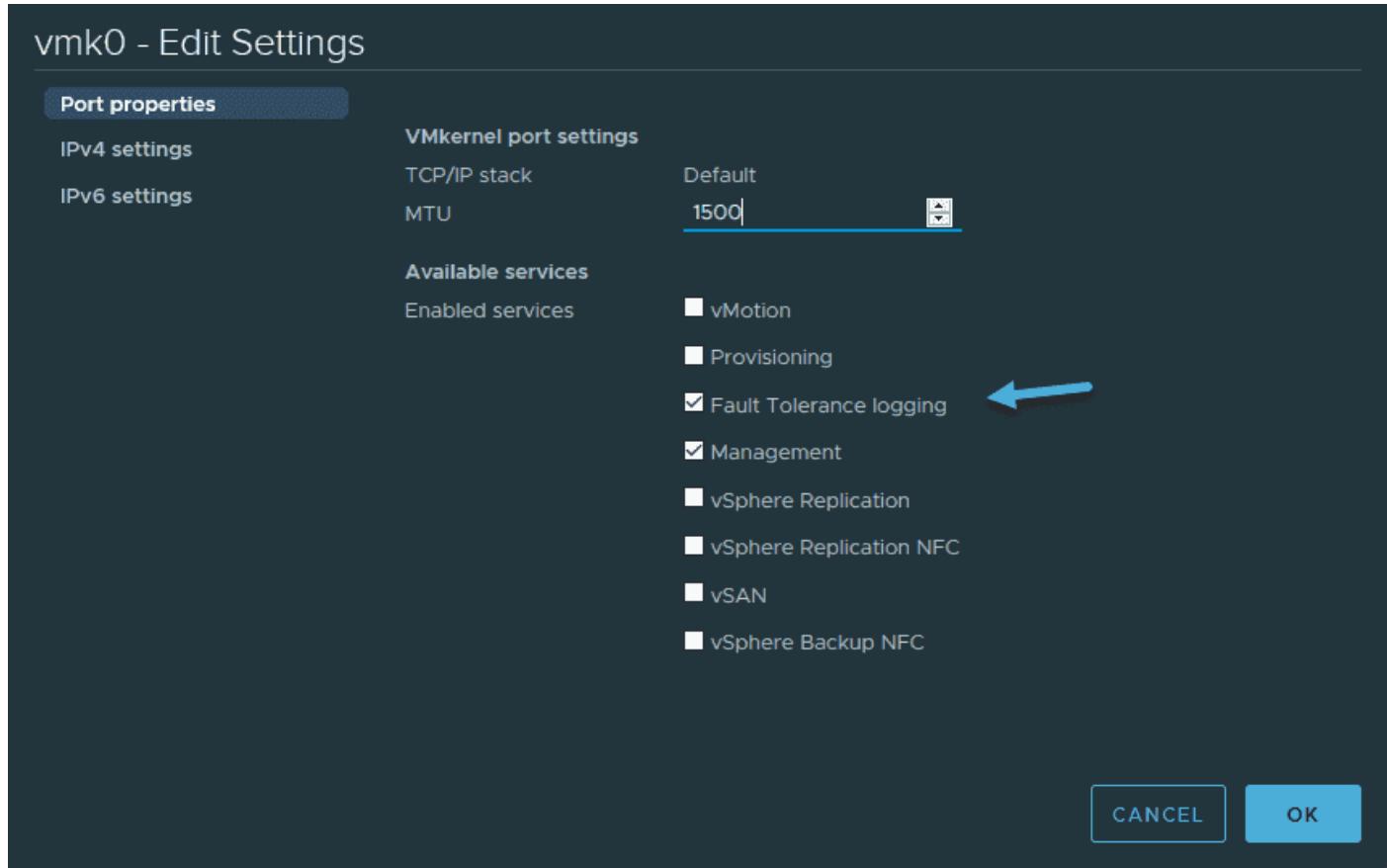
If the primary VM fails, the secondary VM takes over, and vSphere creates a new shadow VM. If the secondary VM fails, vSphere also creates a new shadow VM.

**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

## Objective 4.7 – Deploy and configure VMware vCenter 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, we will see that 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.

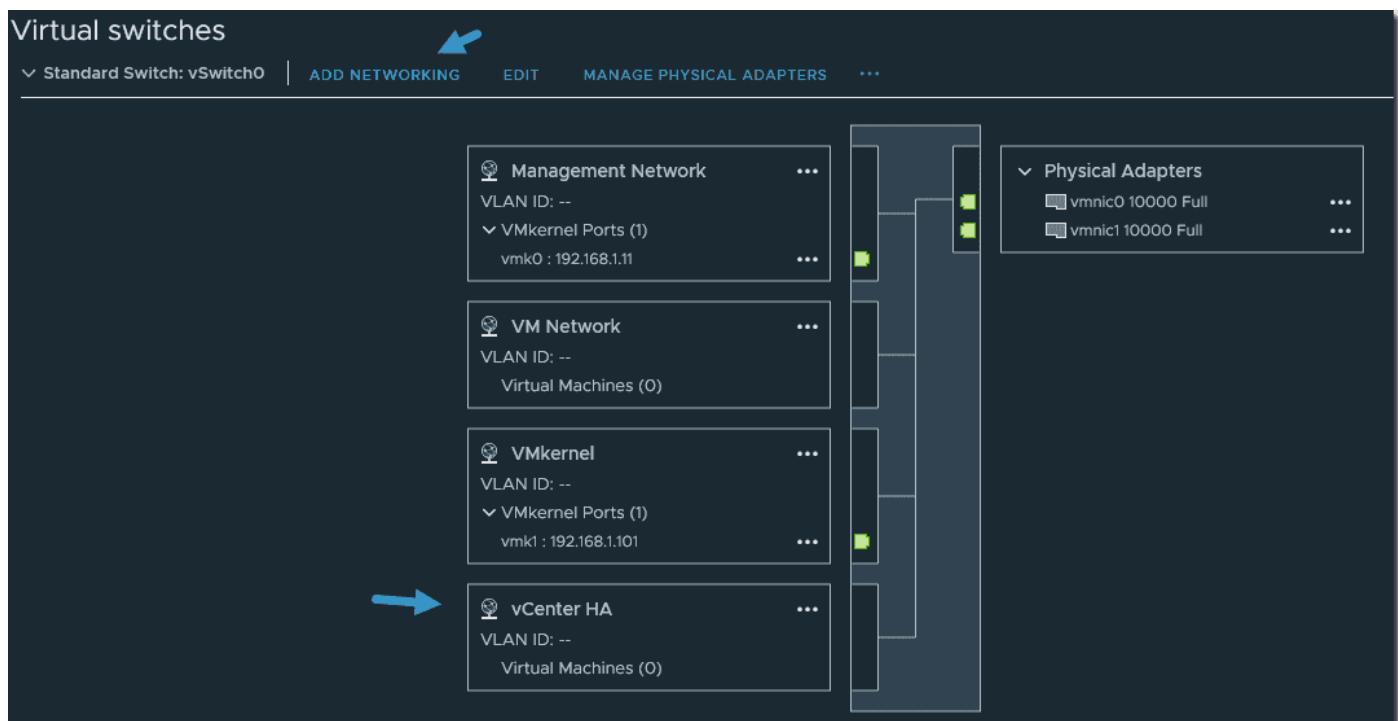
We do not have to deal with external Platform Service Controller (PSC) VMs, as this architecture decision has been phased out in vSphere 7.

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.

vSphere Client | Search in all environments

**vcsaphoton.lab.local** | ACTIONS ▾

- Summary
- Monitor
- Configure**
- Permissions
- Datacenters
- Hosts & Clusters
- VMs
- Datastores
- Networks
- Linked vC

**vCenter HA**

**Prerequisites**

- Create a vCenter HA network. This private network must be separate from the management network. It is used for internal communication between the nodes. The latency between the nodes should be less than or equal to 10ms.
- Reserve static IP addresses for all the nodes. These will be required in vCenter HA IP settings during the set up process.

**SET UP VCENTER HA**

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 Up vCenter HA**

**1. Resource settings**

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

Select vCenter HA network for Active node  **BROWSE ...**

Automatically create clones for Passive and Witness nodes

**Active node (vcsaphoton)**

Location	Networks	Storage
vcsaphoton.lab.local	VM Network Management (NIC 0)	local
Datacenter	vCenter HA vCenter HA (NIC 1)	
esxi04.lab.local		

**Passive node (vcsaphoton-Passive)**

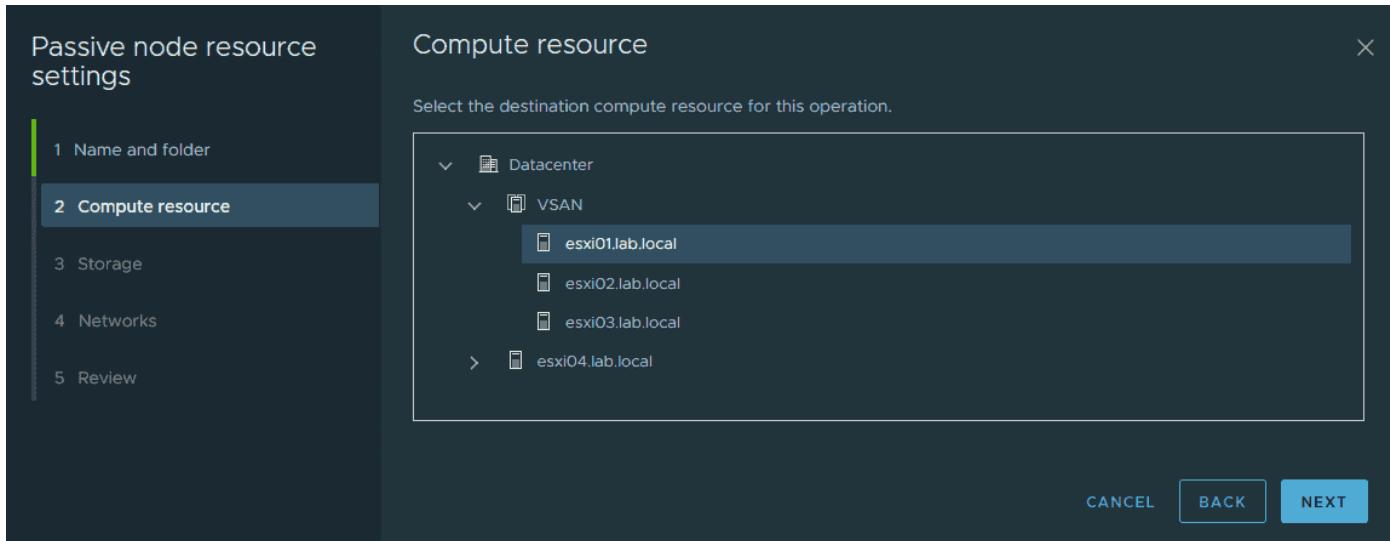
Location	Networks	Storage
vcsaphoton.lab.local	(not selected) Management (NIC 0)	(not selected)
(not selected)	(not selected) vCenter HA (NIC 1)	
(not selected)		

**EDIT**

Set the HA network and the different resources

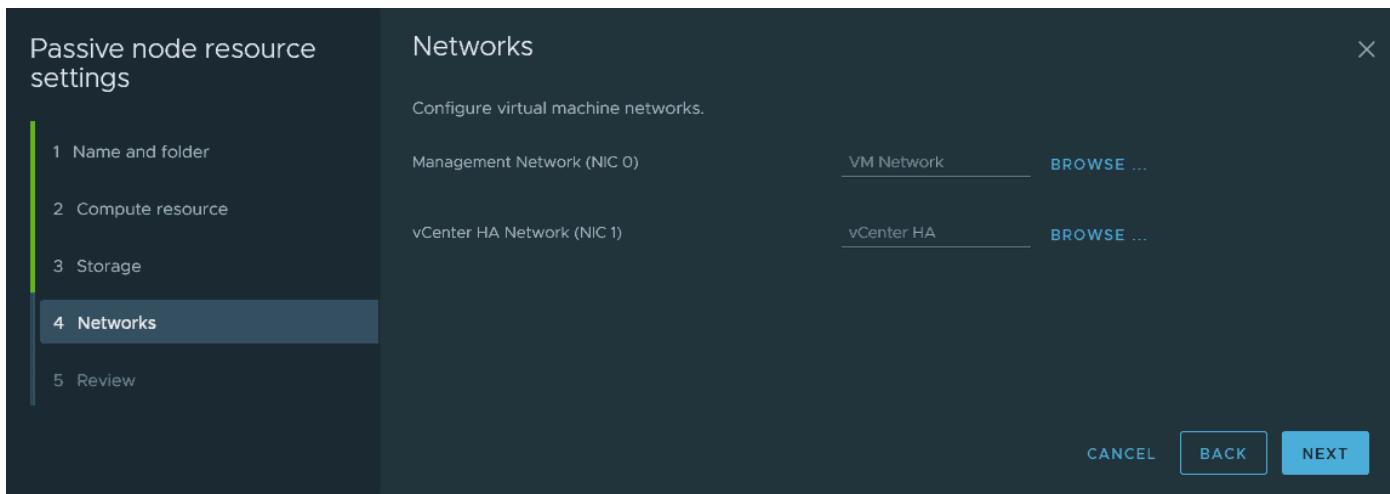
Then we must select the compute resources where the passive node will be running. When we say it's in passive node, it does not mean that the VM is powered off. No, it is a fully running VM, but it only receives a copy of the data from the active node.

Then, in case of a failure, this node is «promoted» as 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 then 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	192.168.1.32

VCSA HA cluster nodes

## Objective 4.8 – Set up 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 version, the Content Library has matured and 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 your organization 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 HTTP NFC protocol.

When you enable 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.

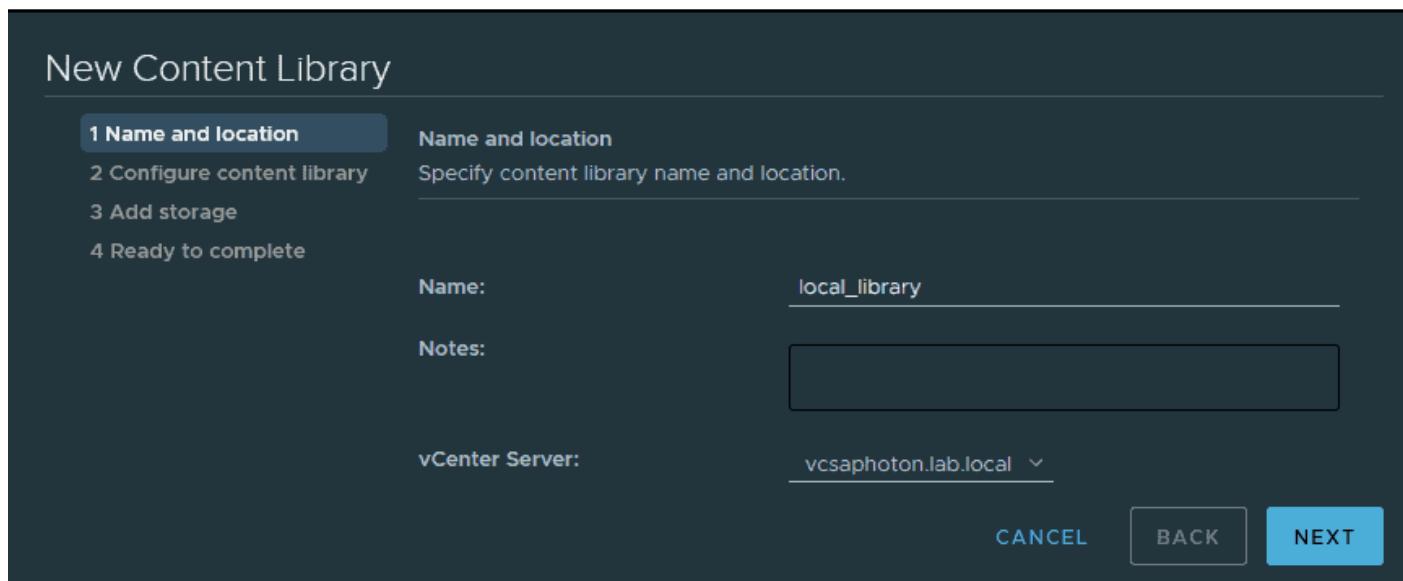
The idea is to have an efficient, centralized method to manage important data required in a vSphere environment. Note that it is possible to edit items only in a local library, no matter whether it is published or not. Library items in subscribed libraries cannot be modified.

The use of subscriptions allows content distribution between a publisher and a subscriber in some scenarios. We can consider the following:

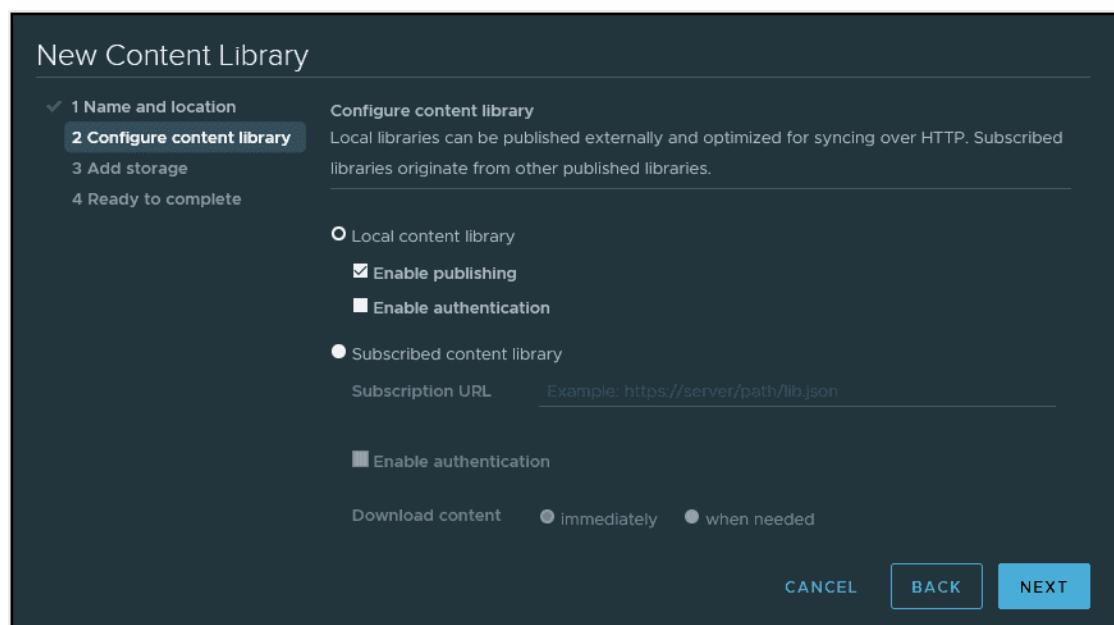
- The publisher and subscriber are in the same vCenter Server instance.
- The publisher and subscriber are in vCenter Server instances that are in Enhanced Linked mode.
- The publisher and subscriber are in vCenter Server instances that are in Hybrid Linked mode.

## Create a local or subscription Content Library in vSphere

Connect to your vSphere web client and select **Home > Shortcuts > Content Libraries**. Click **Create** to start the assistant.



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.



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

Local content library

Enable publishing

Enable authentication

Subscribed content library

Subscription URL <https://download3.vmware.com/software/vmw-tools/lib.json>

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 we can clone/export them.

vSphere Client

Content Libraries

- local\_library
- Subscribed Library**

Subscribed library | ACTIONS

Summary Templates Other Types

VM Templates OVF & OVA Templates

Name	Actions
Nested_ESXi7.0u1_Appliance_Template_v1.0	<input type="checkbox"/> Actions - Nested_ESXi7.0u1_Appliance_Template_v1.0 <input type="checkbox"/> New VM from This Template... <input type="checkbox"/> Export Item... <input type="checkbox"/> Clone Item...
Nested_ESXi6.5u2_Appliance_Template_v1.0	
Nested_ESXi6.5d_Appliance_Template_v1.0	
Nested_ESXi7.0_Appliance_Template_v1.0	
Nested_ESXi6.7u2_Appliance_Template_v1.0	
Nested_ESXi6.7u1_Appliance_Template_v1.0	

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.

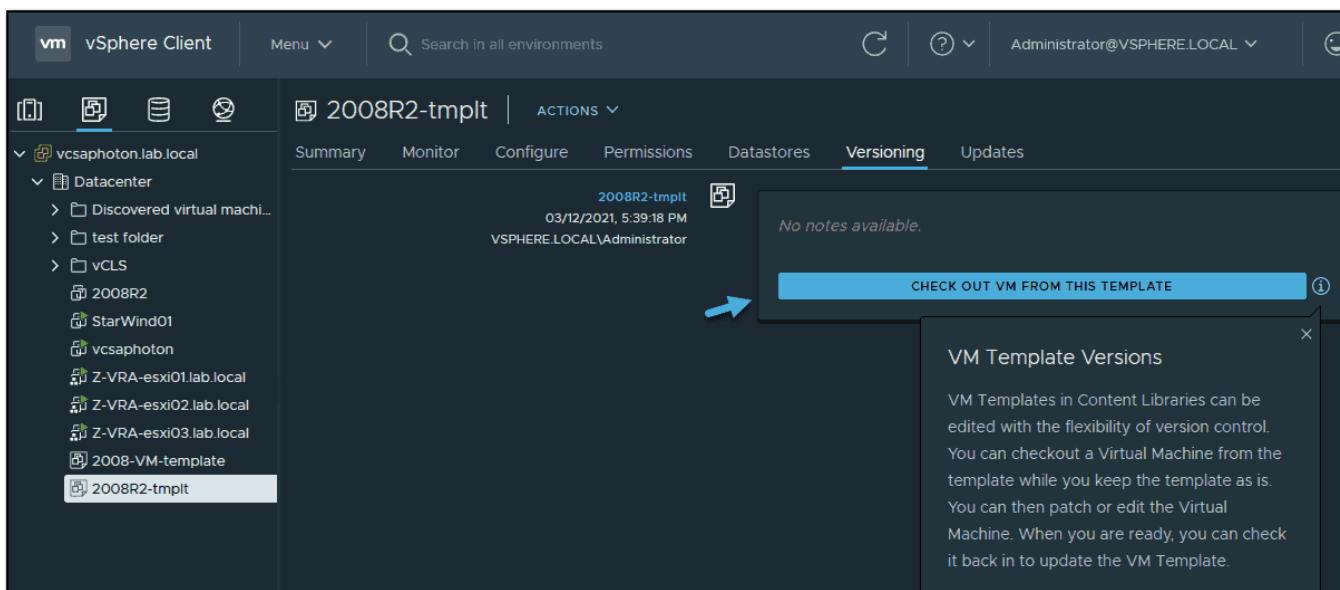
## What is Check-In/Check-Out?

Before vSphere 7, when an administrator needed to perform maintenance on a VM template (.vmtx), the process was quite manual and included multiple steps. 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.

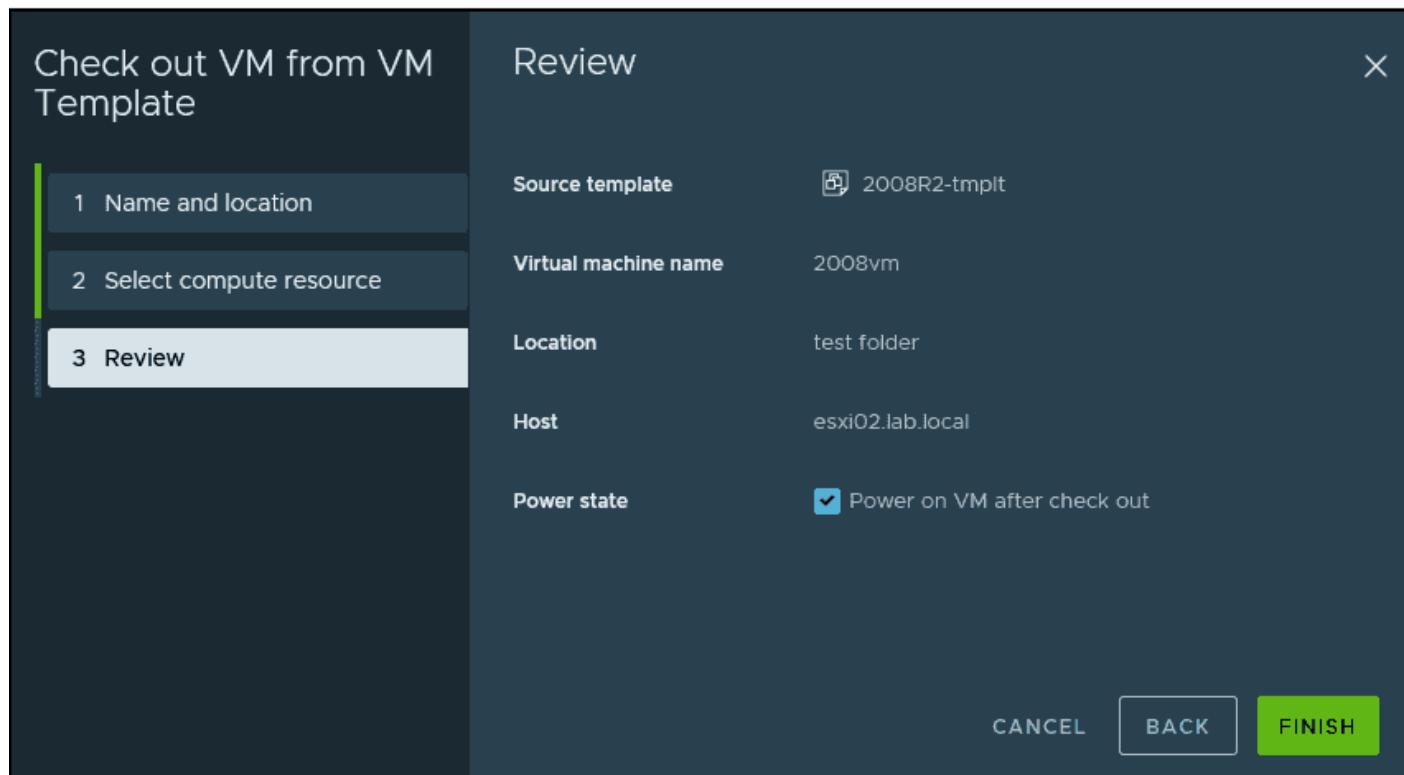
Now with the check-in/check-out function, you have versioning. You'll be able to check out the VM from this template for edits and then check in that template VM back to the Content Library to save the changes you made.

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 privilege 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 set some advanced sync operations, 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.

The screenshot shows the 'Advanced Configuration' dialog box. It has two main sections: 'Auto-sync Frequency' and 'Performance Optimization'. In the 'Auto-sync Frequency' section, there is a tooltip for 'Library Auto Sync Enabled' which says: 'Subscribed library automatic synchronization enabled status'. The value is set to 'true'. Below it, 'Library Auto Sync Refresh Interval' is set to 240 seconds. Under 'Performance Optimization', 'Library Maximum Concurrent Sync Items' is set to 5, 'Max concurrent NFC transfers per ESX host' is set to 8, 'Maximum Bandwidth Consumption' is set to 0, 'Maximum Number of Concurrent Priority Transfers' is set to 5, and 'Maximum Number of Concurrent Transfers' is set to 20. At the bottom are 'CANCEL' and 'SAVE' buttons.

Advanced Configuration

Auto-sync Frequency

Library Auto Sync Enabled i

Subscribed library automatic synchronization enabled status

true

Library Auto Sync Refresh Interval i

240

Library Auto Sync Setting Refresh Interval (seconds) i Service restart required

600

Library Auto Sync Start Hour i

20

Library Auto Sync Stop Hour i

7

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

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 blog post.

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 fiber 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 4.8.1 (4.8.2-4.9.2) – Content library**

Covered in 4.8

## **Objective 4.10 – Manage virtual machine (VM) template versions**

In a content library, you can store and manage virtual machine templates as OVF templates or VM templates. vApps are always converted to OVF templates in the content library. A VM template can be managed by vCenter Server or by a content library.

You can track history of changes over time by using the vertical timeline view. The vertical timeline view provides you with detailed information about the different VM template versions, the updates that privileged users have made, and when the last change was made. By using the vertical timeline, you can revert VM templates back to their previous state or delete the previous version of a VM template.

In addition, you can deploy a virtual machine from the latest version of the VM template without any disruptions while it is checked out for update. You can update the virtual machine and check it back in into the same VM template.

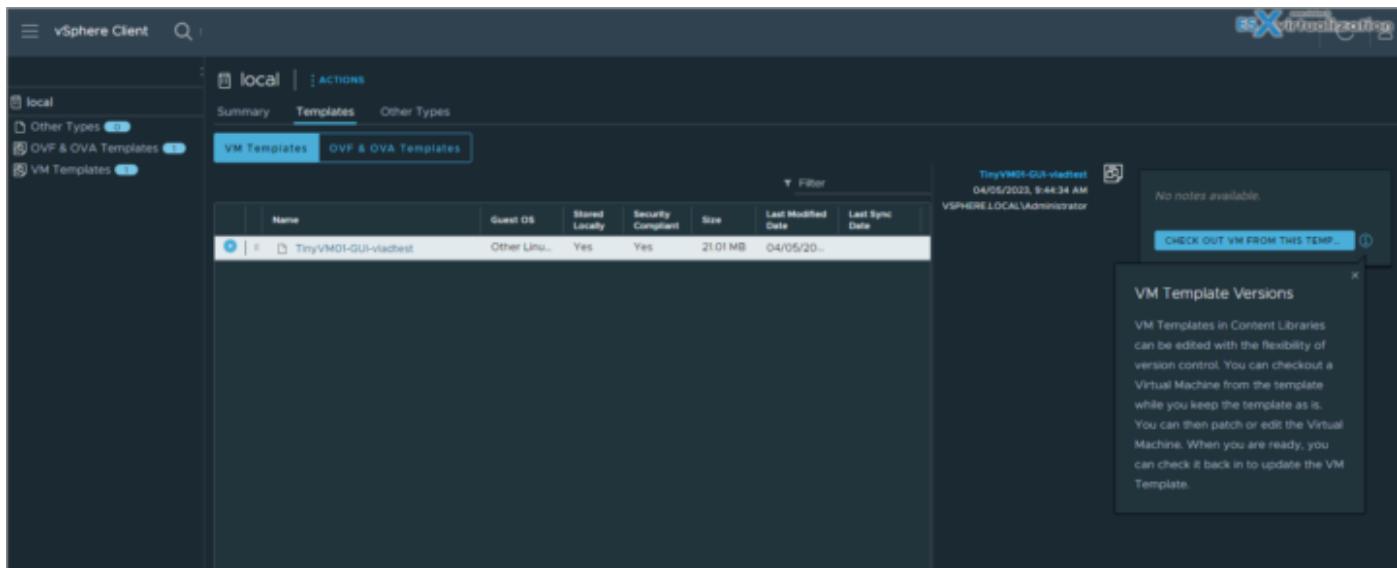
You'll need to have certain privileges and also a content library configured within your vSphere.

### **Check Out a Virtual Machine from a Template**

In the vSphere Client, you can edit the VM templates and monitor the changes that have been made by other privileged users. You can perform the checkout operation to update a virtual machine from the VM template. During this process, the VM template is not available for checkout from other users, but they can deploy a virtual machine from the VM template without any disruptions.

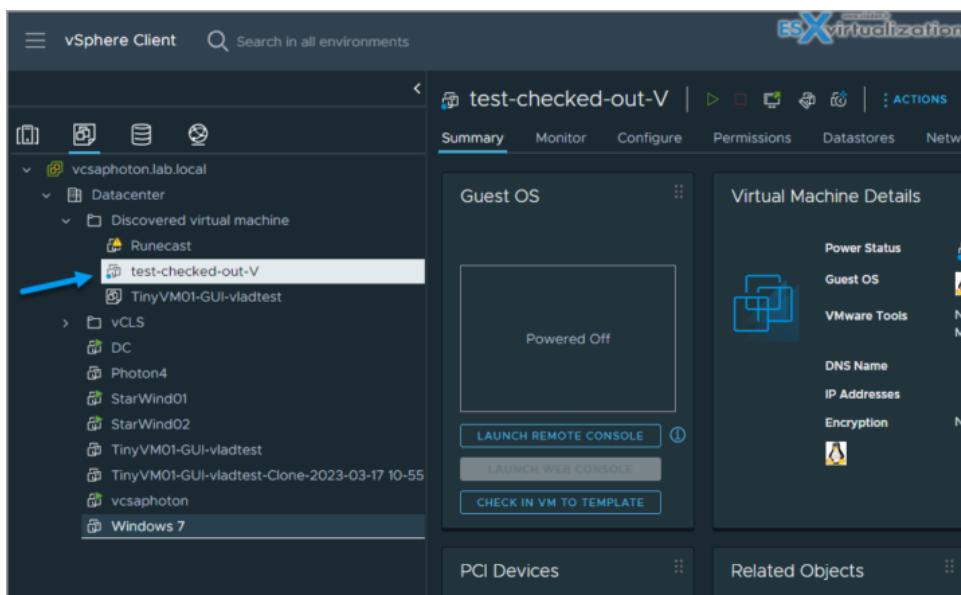
When you check out a VM template, you cannot convert the virtual machine to a template or migrate the virtual machine to a different vCenter Server inventory.

- 1. From content library** - From the vSphere Client inventory > Navigate to Menu > VMs and Templates and click the VM template > Click the Versioning tab and in the vertical timeline view, click Check out VM from this template.
- 2. From vSphere Client Inventory** - Alternatively, you can also navigate to Menu > VMs and Templates and click the VM template. Click the Versioning tab and in the vertical timeline view, click Check out VM from this template.



On the Name and location page, enter a virtual machine name, select the virtual machine location, and click Next. On the Select compute resource page, select the compute resource for the checked out virtual machine and click Next. On the Review page, review the configuration. Choose whether to power on the virtual machine after checkout by selecting the Power on VM after checkout check box. Click Finish.

The checked out virtual machine appears in the selected location marked with a blue circle icon. You can perform the necessary configuration changes.



You can then go back to the VM templates to see the versions...

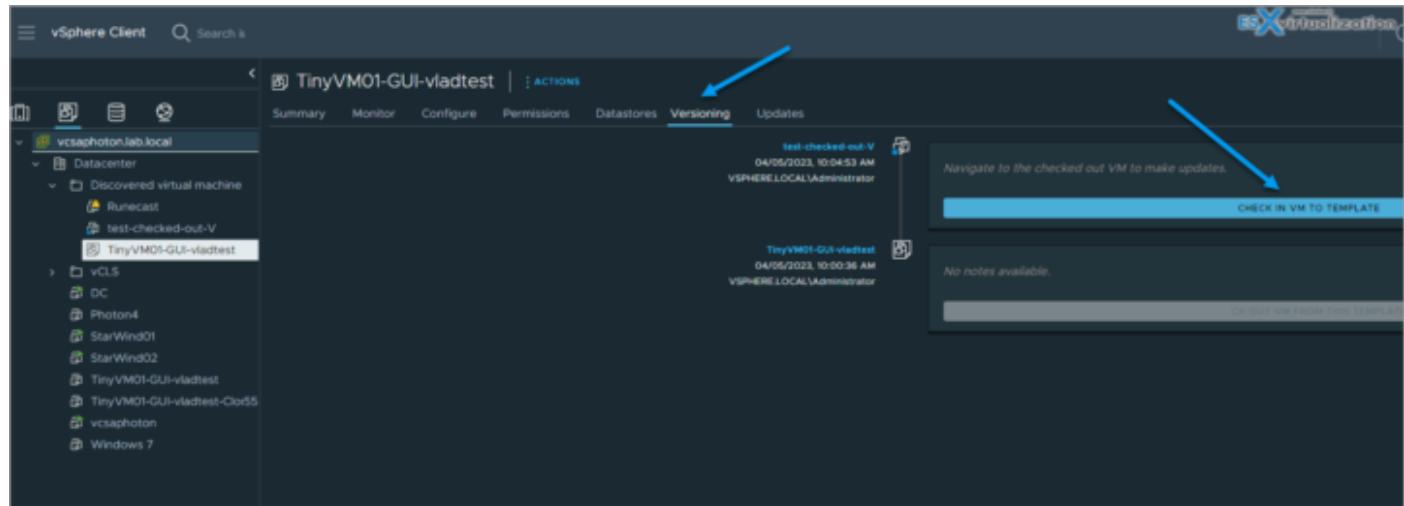
## Check In a Virtual Machine to a Template

After you check out a virtual machine from a template and update the virtual machine, you must check the virtual machine back into the VM template. When you check in the virtual machine to a template, you create a new version of the VM template containing the updated state of the virtual machine.

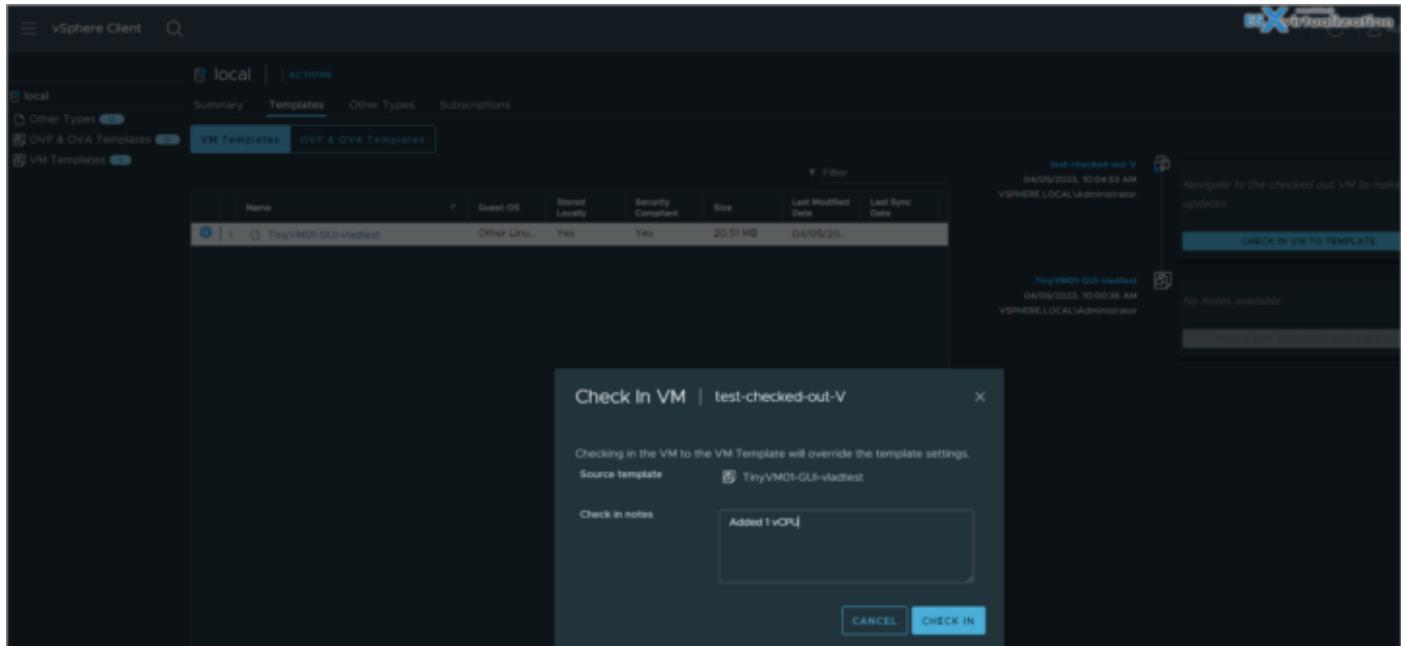
When you check in the virtual machine to the VM template, you allow the deployment of the last changes that you make to the virtual machine.

**1. From a content library** - Navigate to Menu > Content Libraries. To open a content library, click its name. On the Templates tab, select a VM template and click Check in VM to template.

**2. From vSphere Client Inventory** - Navigate to Menu > VMs and Templates and click the VM template. Click the Versioning tab and in the vertical timeline view, click Check in VM to template.



The Check in VM dialog box opens. To describe the change, enter a comment in Check in notes . Click **Check in**.



**Delete a Previous Version of a VM Template** - Delete a previous version of a VM template if you no longer want to allow the use of the template. Deleting a VM template removes the template and its content from the inventory.

From the vSphere Client inventory > Navigate to Menu > VMs and Templates and click the VM template. Click the Versioning tab. From the vertical timeline, navigate to the previous state of the VM template, click the horizontal ellipsis icon (horizontal ellipsis icon), and select Delete Version. The Confirm Delete dialog box opens. To delete permanently the VM template and its contents, click Yes.

## Objective 4.10.1 – Update template in content library

Covered in 4.10

## Objective 4.11 – Configure VMware vCenter file-based backup

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.

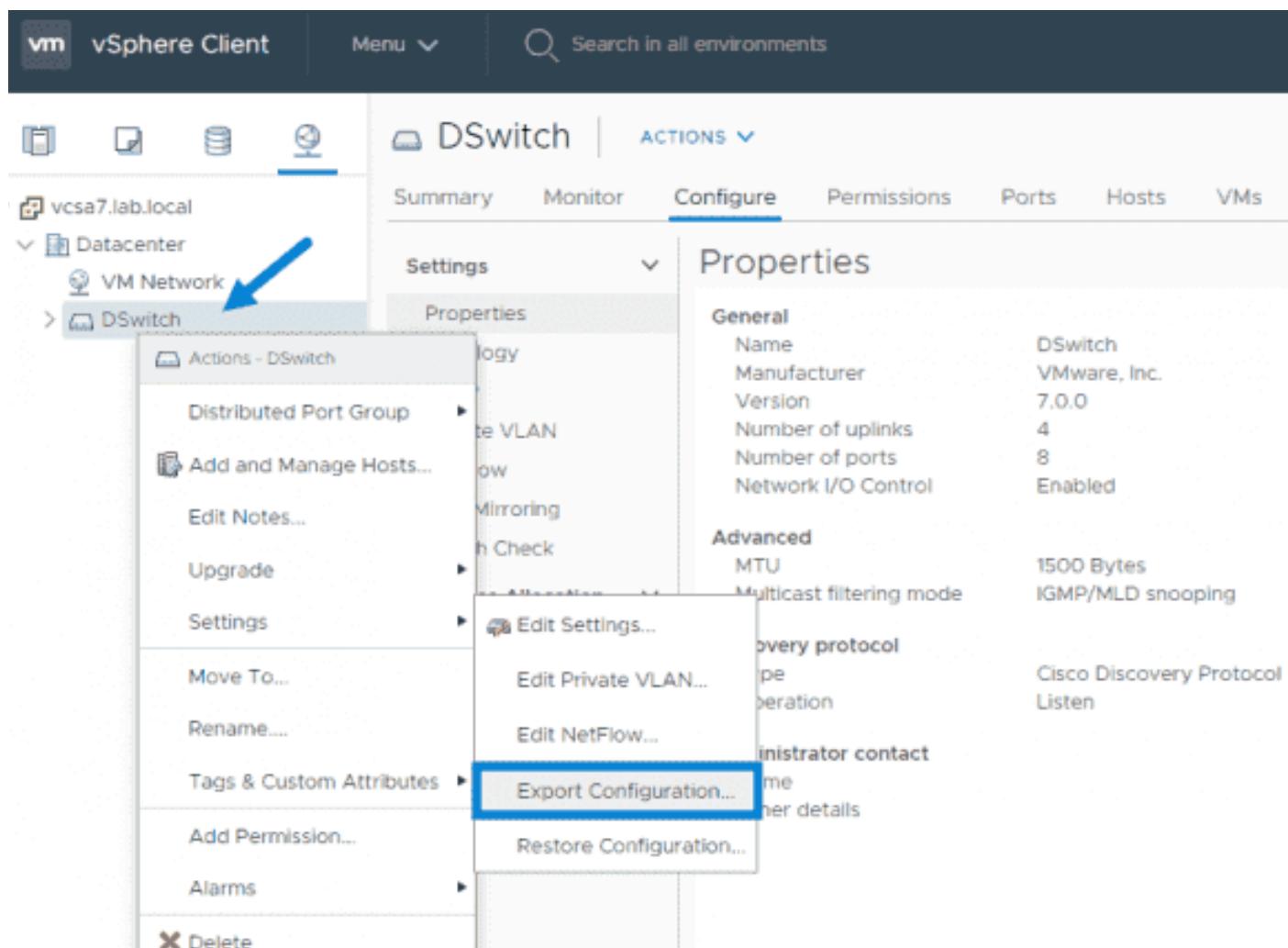
The VMware vSphere Storage APIs – Data Protection framework is used by those backup software products to do a backup of all your virtual machines (VMs), including the VMware vCSA.

So 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 reimport 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 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.

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 vSphere Client interface for managing backups. The top navigation bar has 'Backup Schedule' selected. Below it, the 'Activity' tab is active, showing a list of backup tasks. A specific task is highlighted, showing its details: Backup Location (smb://192.168.1.7/d\$/backup), Type (Manual), Status (In Progress, 2%), Data Transferred (0 B). A tooltip message states: 'The restore process requires that both the installer and backup versions are identical.' At the bottom of the activity list, a message says: 'Db health check in progress. This may take 3 to 10 min based on db size.'

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), 'Backup server credentials' (User name: administrator@lab.local, Password: [redacted]), 'Schedule' (Daily at 03 : 25 P.M. Etc/GMT+4), 'Encrypt backup (optional)' (Encryption Password: [redacted], Confirm Password: [redacted]), 'DB Health Check' (Disable checked, indicated by a blue arrow), 'Number of backups to retain' (Retain last 7 backups selected, indicated by a blue arrow), 'Data' (Stats, Events, and Tasks checked, Inventory and configuration checked), and 'Total size (compressed)'. At the bottom are 'CANCEL' and 'SAVE' buttons.

Backup location	smb://192.168.1.7/d\$/backup
Backup server credentials	User name: administrator@lab.local Password: [redacted]
Schedule	Daily at 03 : 25 P.M. Etc/GMT+4
Encrypt backup (optional)	Encryption Password: [redacted] Confirm Password: [redacted]
DB Health Check	<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)	
<button>CANCEL</button> <button>SAVE</button>	

Backup options and ability to disable DB health check

These are the supported backups of vCSA.

## Objective 4.12 – Configure vSphere Trust Authority

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.

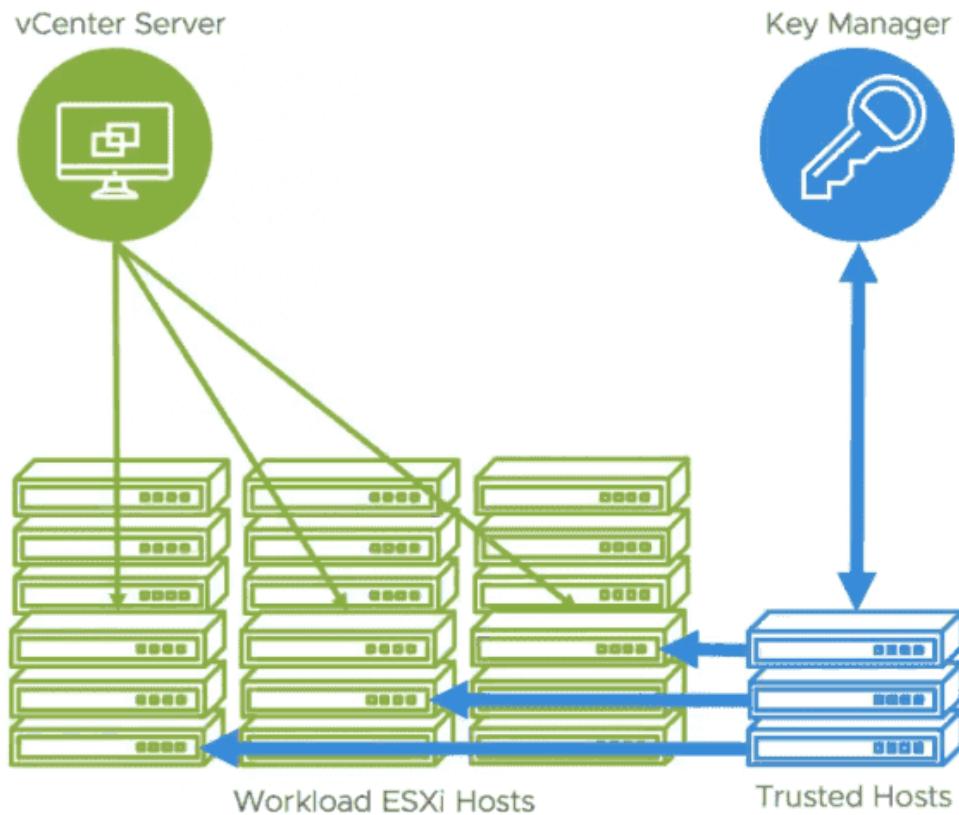
VMware is trying to work toward a better security model, and the introduction of vTA is the first step. vTA represents the foundation to which VMware will add more functions in future releases. In this release, VMware is building the base block of the architecture.

### **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 8 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

**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 4.13 – Configure vSphere certificates

vSphere certificates you can basically stick to the defaults when it comes to provision 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 trusted third-party certificate authorities (CAs), as for example VeriSign or GoDaddy. So quite a lot of options here.

The certificates under vSphere can:

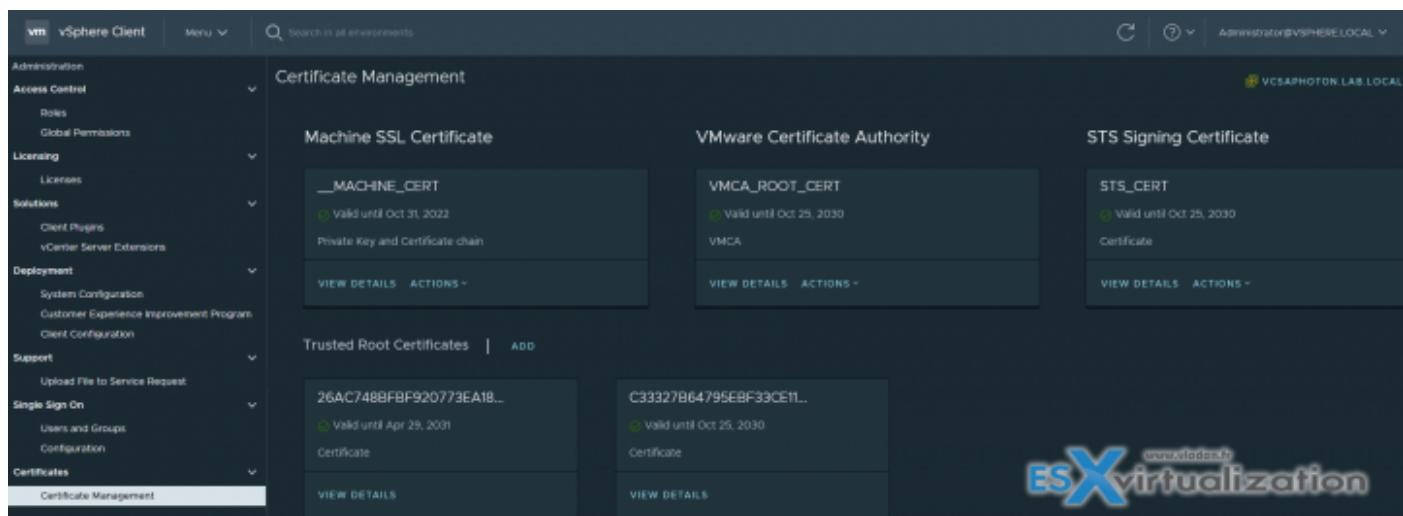
- Authenticate vSphere services
- Signing tokens (SSO for example)
- Encrypt communication between vCenter and ESXi

VMware VMCA runs on VCSA as a service. It provides all the required certificates for vCenter Server and ESXi. They 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 it comes.

VMware recommendations for certificate management are basically the following. If you replace certificates by 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 expiration data 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 autogenerated 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 when re-connected.

**Machine SSL Certificate** – is used to create SSL sockets for secure socket layer (SSL) client connections, for server verification, and for 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).

## Objective 4.13.1 – Describe Enterprise PKI's role for SSL certificates

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 8

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.

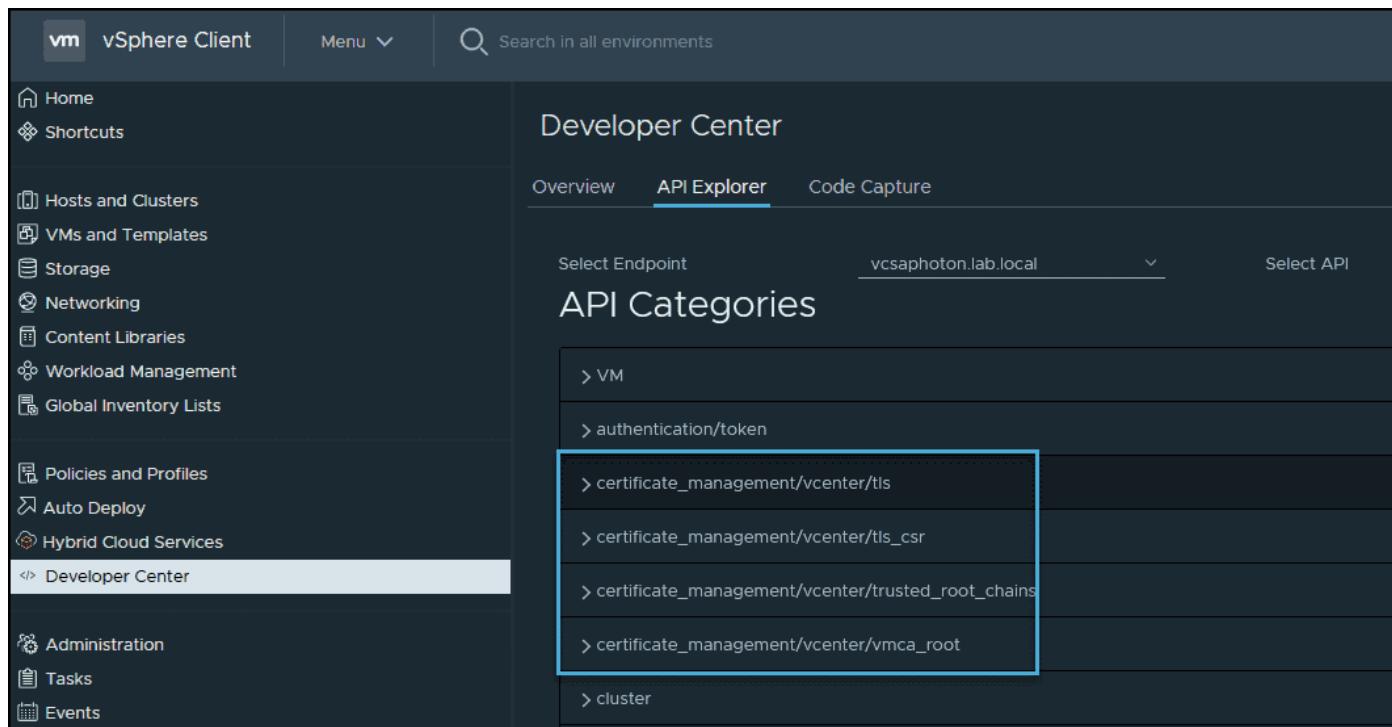
By default, vSphere comes with self-generated certificates so you don't have to lose time during the installation and deployment of the product. If you have to replace the certificates on your own, you'll do it through the certificate management menu, as shown in the above screenshot.

## 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. There are now APIs present for nearly everything in vSphere.

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).

## Objective 4.14 – Configure vSphere Lifecycle Manager

The screenshot shows the 'Welcome to VMware vSphere' page. On the left, there's a 'Getting Started' section with a 'LAUNCH VSPHERE CLIENT (HTML5)' button. Below it is a 'Documentation' section with a 'VMware vSphere Documentation Center' link. On the right, there's a 'For Administrators' sidebar with sections for 'Web-Based Datastore Browser' (describing how to find and download files) and 'vSphere Web Services SDK' (describing tools for managing ESXi and vCenter). At the bottom of the sidebar, there's a 'Download trusted root CA certificates' link. A blue arrow points from this link in the sidebar to the same link in the text below.

[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.

VMware vSphere Update Manager (VUM) product has evolved and now it's called vSphere Lifecycle Manager. There has been new functionality added in vSphere and also there are some new configuration options as well. In this post we'll detail those changes and see how to configure vSphere Lifecycle Manager (vLCM).

In vSphere, vSphere Lifecycle Manager replaces VMware Update Manager from prior versions. Lifecycle Manager adds to 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 are no special extra installation.

If you need to install an optional module 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 an USB disk that you then present to vSphere Lifecycle Manager.

## Fast Upgrades with vLCM

What is it? 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 the downtime as short as possible.

You can configure **Quick Boot** where supported OEM vendors enable skipping the initialization of firmware and many other hardware devices during boot times.

Fast upgrades preserve state of VMs running on a host by suspending them to the **host's memory**. Once the host reboots there are automatically restored from memory.

You save time by not migrating the VMs off the host in first time.

## Image remediation Settings

The image remediation settings allow you also to change and benefit from quick boot. With vSphere web client go to **Shortcuts > Lifecycle Manager > Settings** > under **Host remediation** chose **Images**.

Images Remediation Settings ⓘ	
ⓘ Remediation settings are set to VMware-provided settings. They will change if VMware updates their provided settings.	
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. When regular reboot 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.

We have some different options here, such as changing power state of VM or suspend to disk, **suspend to memory** or power off.

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

Enable Quick Boot ⓘ

VM power state

Do not change power state

Suspend to disk

Suspend to memory ⓘ

Power off

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

Retry entering maintenance mode in case of failure

Retry delay: 5 minutes

Number of retries: 3

Disable HA admission control on the cluster

Disable DPM on the cluster

Prevent remediation if hardware compatibility issues are found

### 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 when the host needs to enter into a maintenance mode as well as the number of retries.

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 preventing applying new updates to a host which might have problems afterwards.

## 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**.

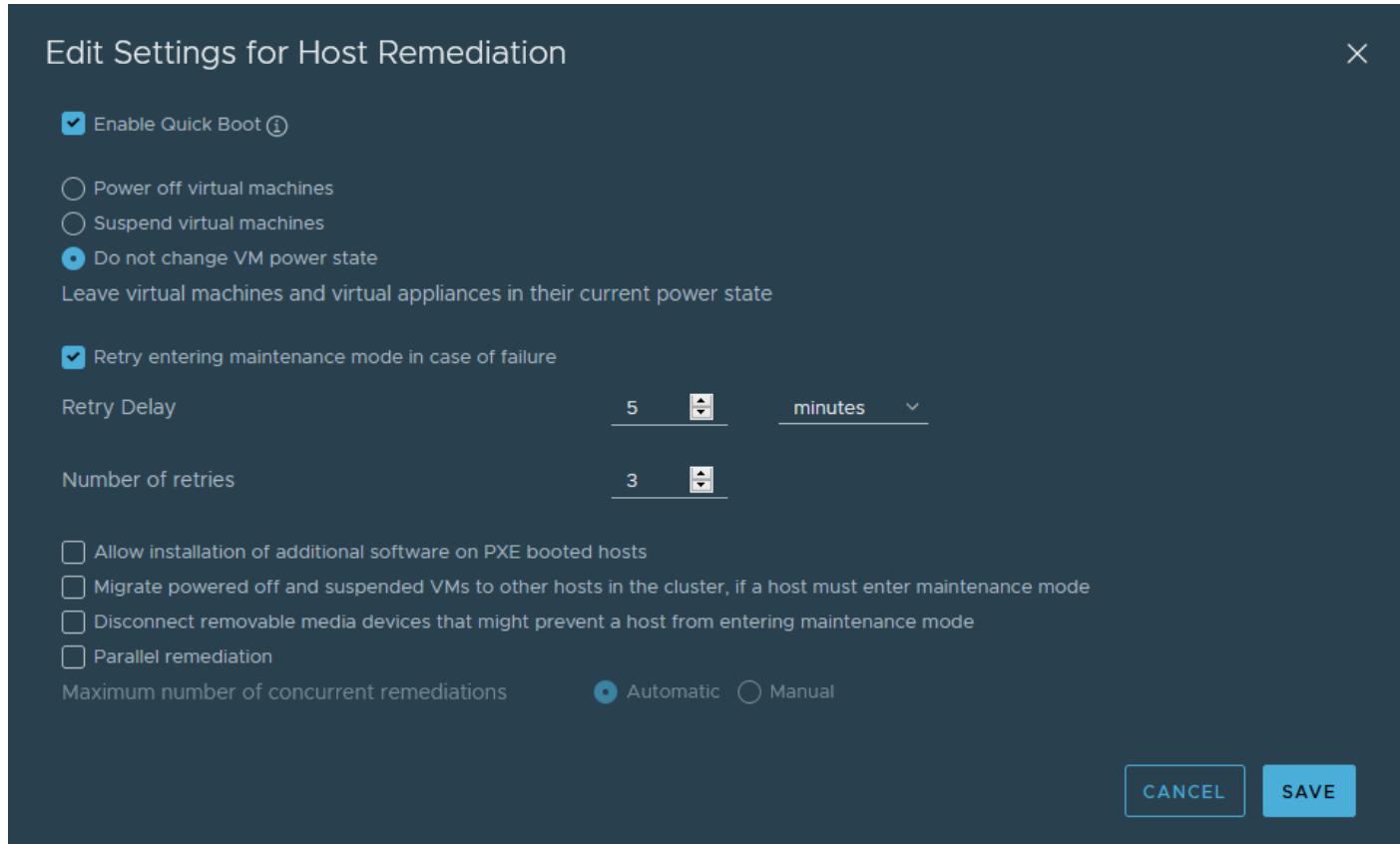
The screenshot shows the vSphere Lifecycle Manager interface. On the left, there's a sidebar with 'Image Depot', 'Updates', 'Imported ISOs', 'Baselines' (which is selected and highlighted in blue), and 'VMs'. The main area has a header 'Lifecycle Manager | ACTIONS ▾' and tabs 'Image Depot', 'Updates', 'Imported ISOs', 'Baselines', and 'Settings' (which is active). Below the tabs, there's a section titled 'Baselines Remediation Settings' with a sub-section 'Host Remediation'. It contains several configuration items:

Setting	Value
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

A large blue arrow points from the 'Host remediation' section in the sidebar to the 'Host Remediation' section in the main content area. A smaller blue button labeled 'EDIT' is located in the top right corner of the main content area.

## vSphere Lifecycle Manager

By clicking the Edit button you'll have a pop-up window which will bring you to the configuration options. And this opens similar page where we can (again) see the Enable quick boot check box.



### vSphere Lifecycle Manager configuration options

Other options below are unchecked, but we can check them. One of the options is called Parallel Remediation. By enabling parallel remediation, it 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 specify for how long we want to keep those snapshots before they are deleted.

Lifecycle Manager | ACTIONS ▾

Image Depot   Updates   Imported ISOs   Baselines   Settings

Administration  
Patch Downloads  
Patch Setup

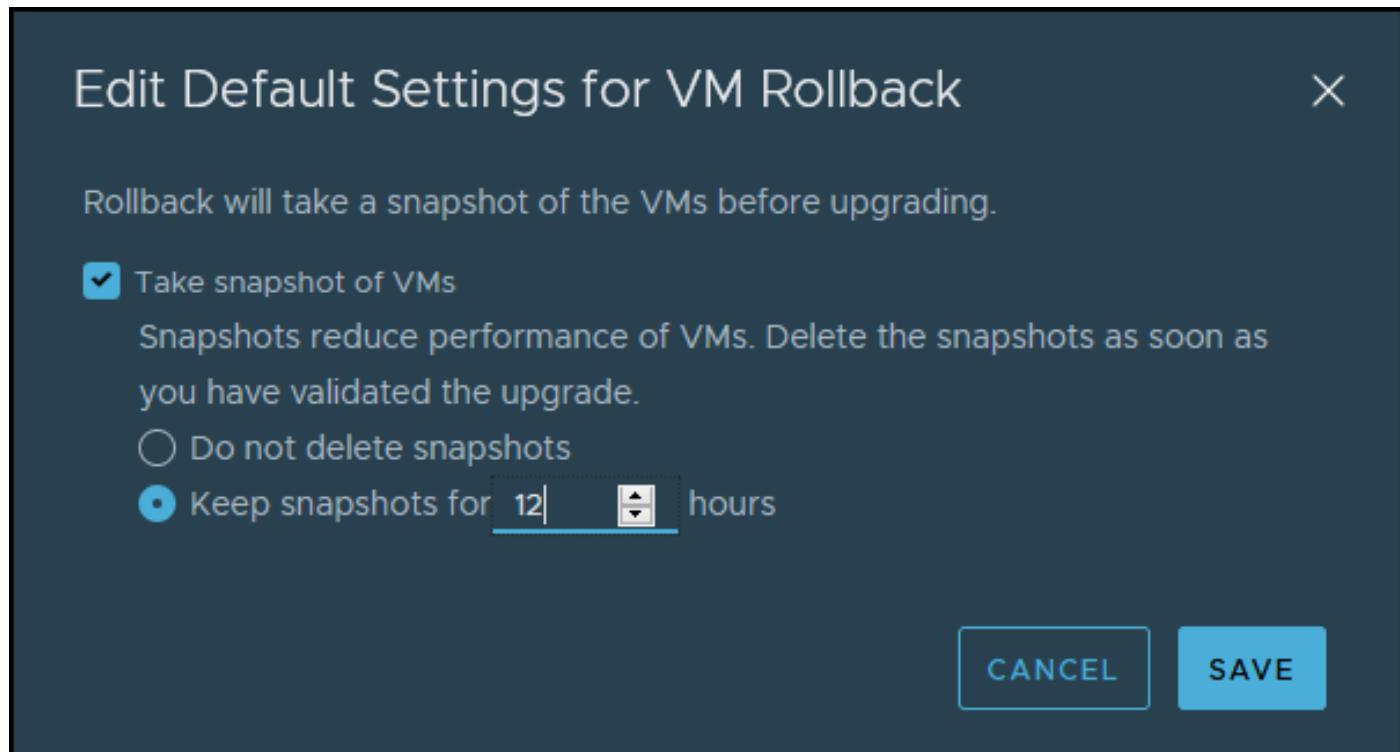
Host Remediation  
Images  
Baselines  
**VMs**

Default Settings for VM Rollback	
Take snapshot of VMs	No
Keep snapshots	--

**EDIT**

### VM Rollback settings

Then this shows up a pop-up window where we can specify for how long and if we want to have our VMs snapshotted before upgrades.



#### 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.

By default, vSphere Lifecycle Manager takes snapshots of virtual machines before upgrading them. It's ON. If the upgrade fails, you can use the snapshot to return a virtual machine to its state before the upgrade.

## Objective 4.15 – Configure different network stacks

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 completes 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, respectively 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** – connect 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 VM 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 4.16 – Configure Host Profiles

Host Profiles allow you to automate and centralize the configuration of your hosts, whether part of a cluster or an individual host. They allow storing parameters that can configure networking, storage, security, and another host's configuration 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 here of having completely uniform clusters with 100 percent identical host configuration. You will never be sure with manual work.

Note that Host Profiles are only part of 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 help your organization or not.

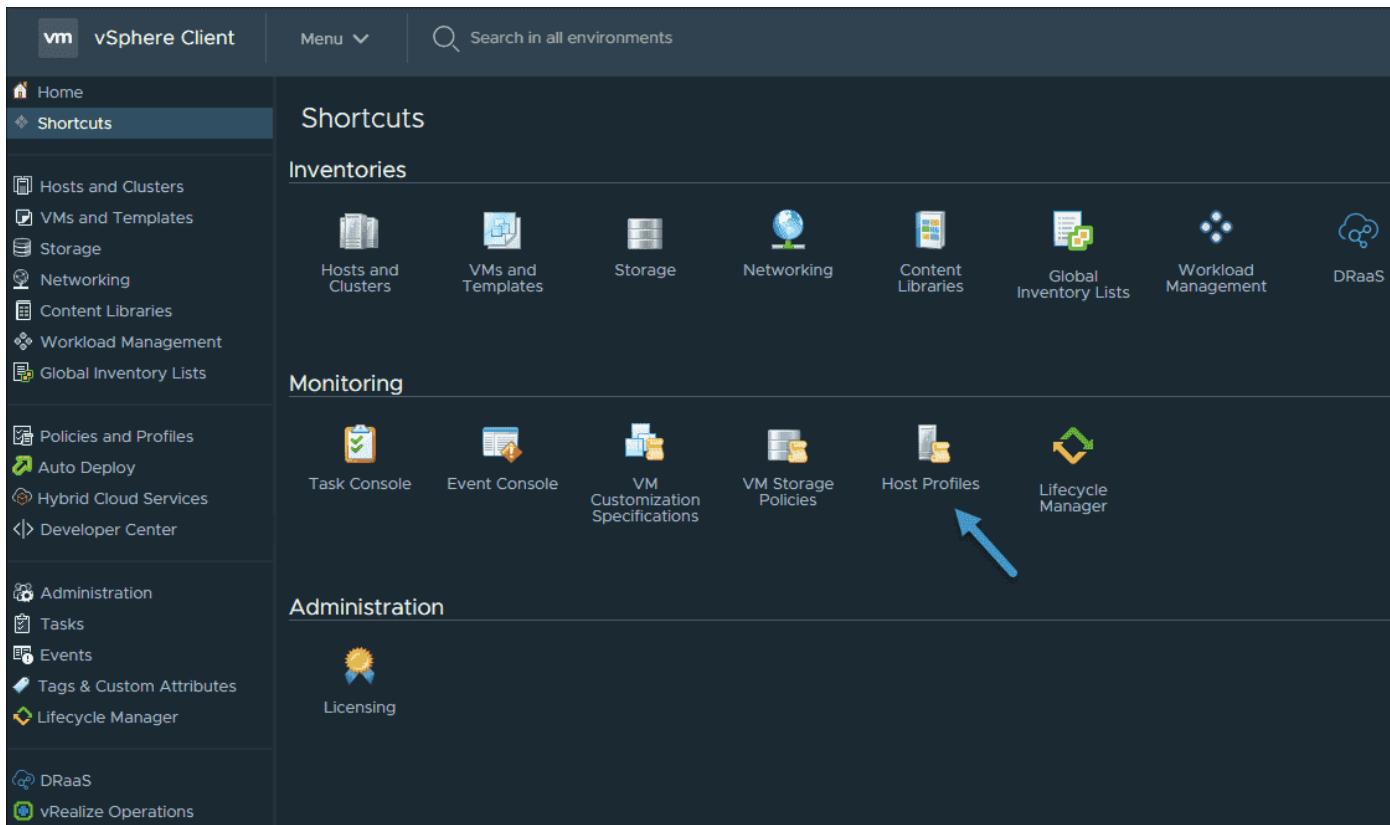
### Set up and configure a reference host

In this step, which we will not detail, you'll basically need to configure a reference host with all the necessary configuration. You'll install a new host and configure networking, storage, and security. We won't go into those details as they are outside the scope of this post.

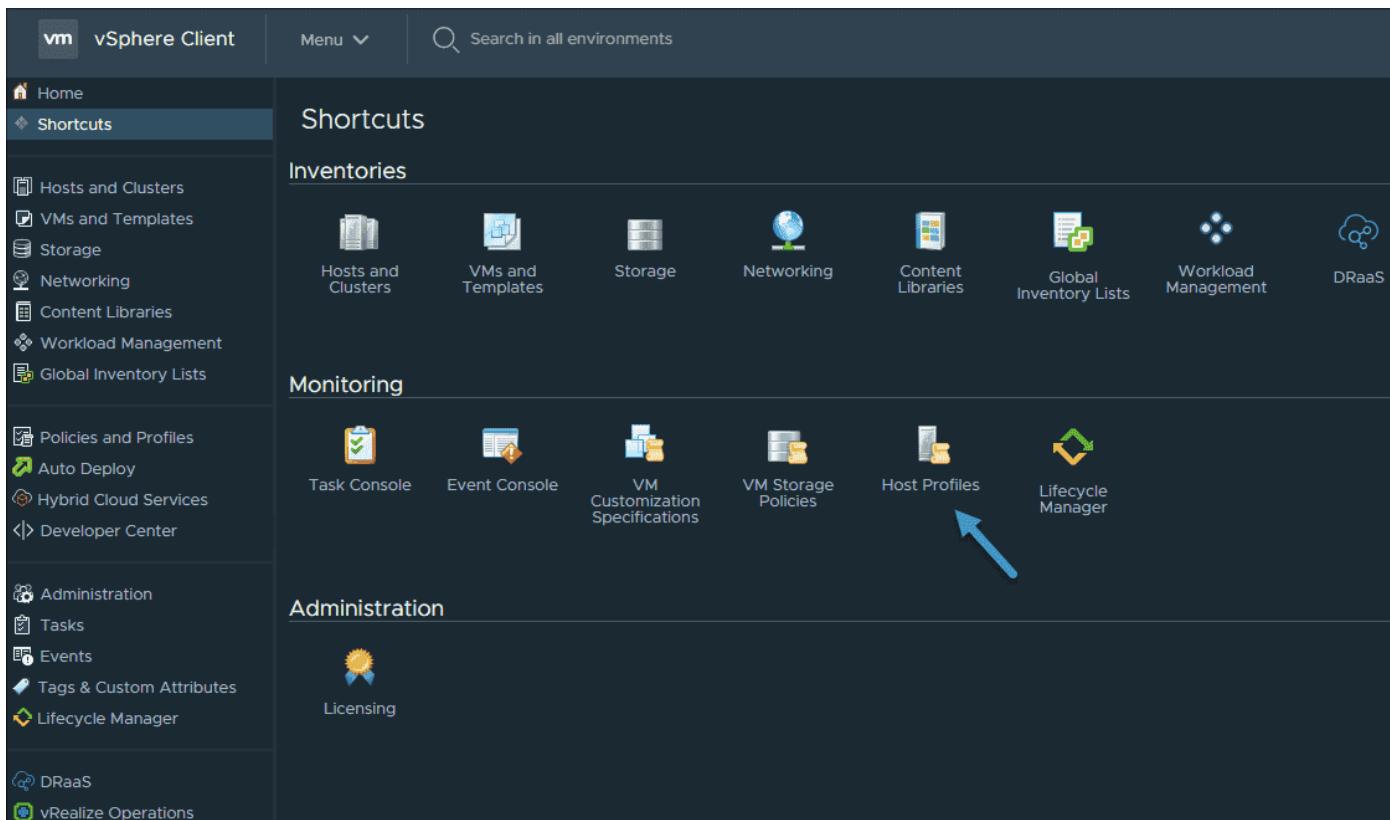
### Create a new vSphere Host Profile

The best way to create a new Host Profile is to extract one **from an already configured host**. In this way, you don't start from scratch. Instead, you're taking an existing config that you'll apply to the rest of the cluster.

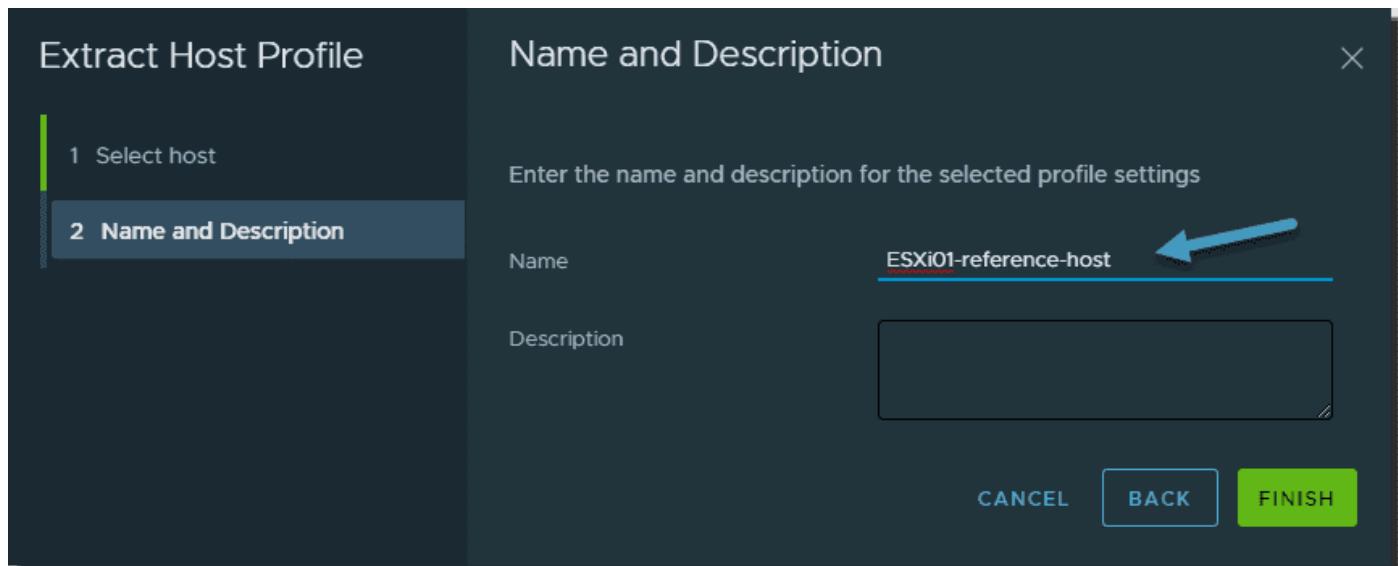
Go to Menu > Shortcuts and click the Host Profiles shortcut.



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).



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 hosts within our cluster via Host Profiles.

Now that we have our Host Profile created, we can do many things. We can:

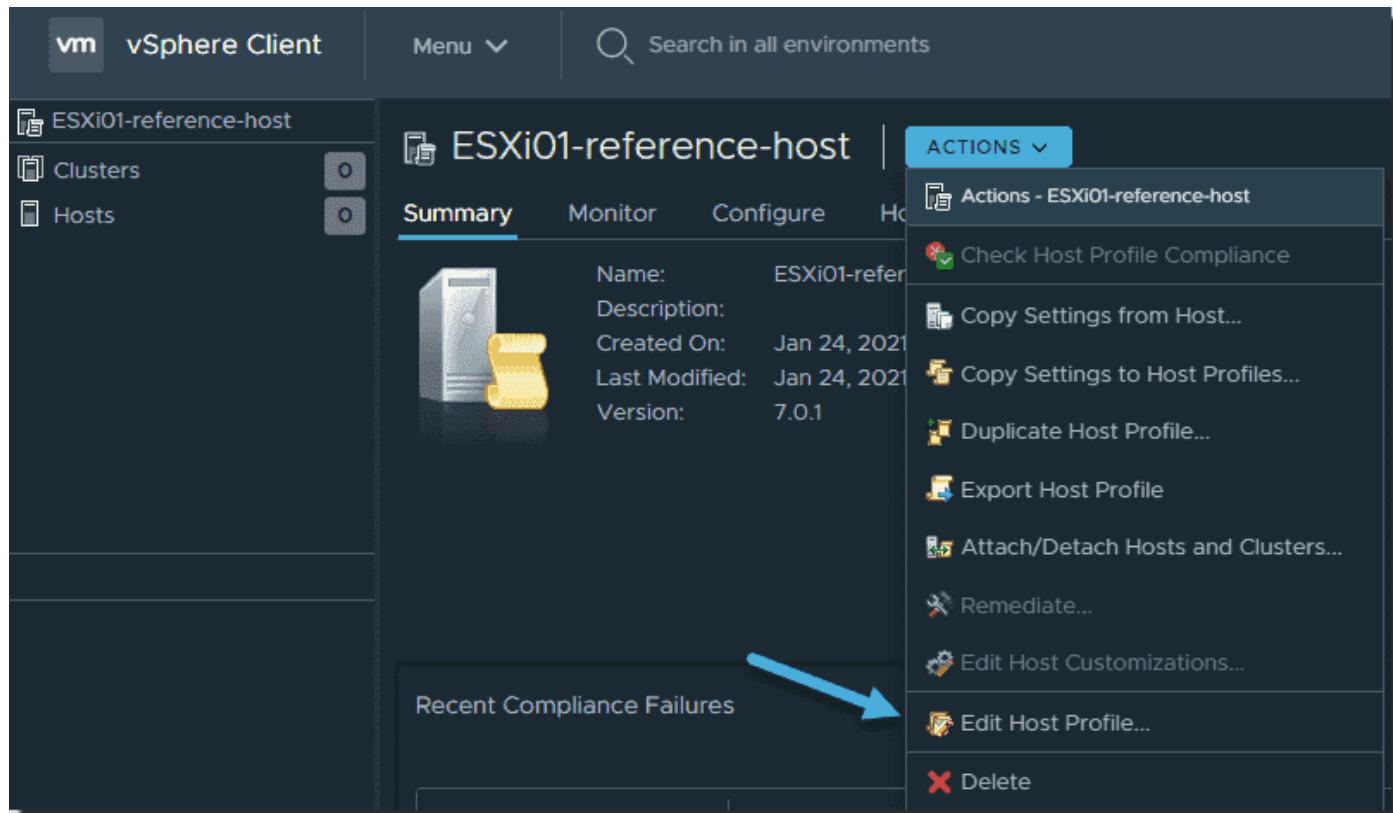
- Duplicate the Host Profile
- Copy settings from a host
- Copy settings to Host Profiles
- Import/export Host Profiles

The screenshot shows the vSphere Client interface under the 'Policies and Profiles' section. The 'Host Profiles' tab is selected. The main pane displays a table with columns: 'Host Profile Name', 'Compliant Hosts', 'Not Compliant Hosts', 'Unknown State Hosts', 'Last Edited', 'Hosts', and 'VC'. One row is visible, showing 'ESXi01-reference-host' in the 'Host Profile Name' column. A blue arrow points to the top of the 'Host Profile Name' column header. The top navigation bar includes 'vm', 'vSphere Client', 'Menu', 'Search in all environments', and 'Administrator@VSPHERE.LOCAL'.

## Edit the vSphere Host Profile

When you want to change the configuration of your hosts, the first thing to do is to edit your Host Profile and then 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**.



### 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.

Edit host profile | ESXi01-reference-host X

Name and description Settings

FAVORITES ALL

Filter

- >  Advanced Configuration Settings
- >  General System Settings
- ✓ Networking configuration
  - ✓ Standard switch
    - >  vSwitch0
    - >  vSwitch1
    - >  vSwitch2

CANCEL SAVE

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.

Edit host profile | ESXi01-reference-host Edit host profile | ESXi01-reference-host

Name and description Settings

FAVORITES ALL

Filter

- >  Advanced Configuration Settings
- >  General System Settings
- ✓ Networking configuration
  - ✓ Standard switch
    - >  vSwitch 5
    - >  vSwitch0
    - >  vSwitch1
    - >  vSwitch2

When you hover a mouse, you can also delete a component

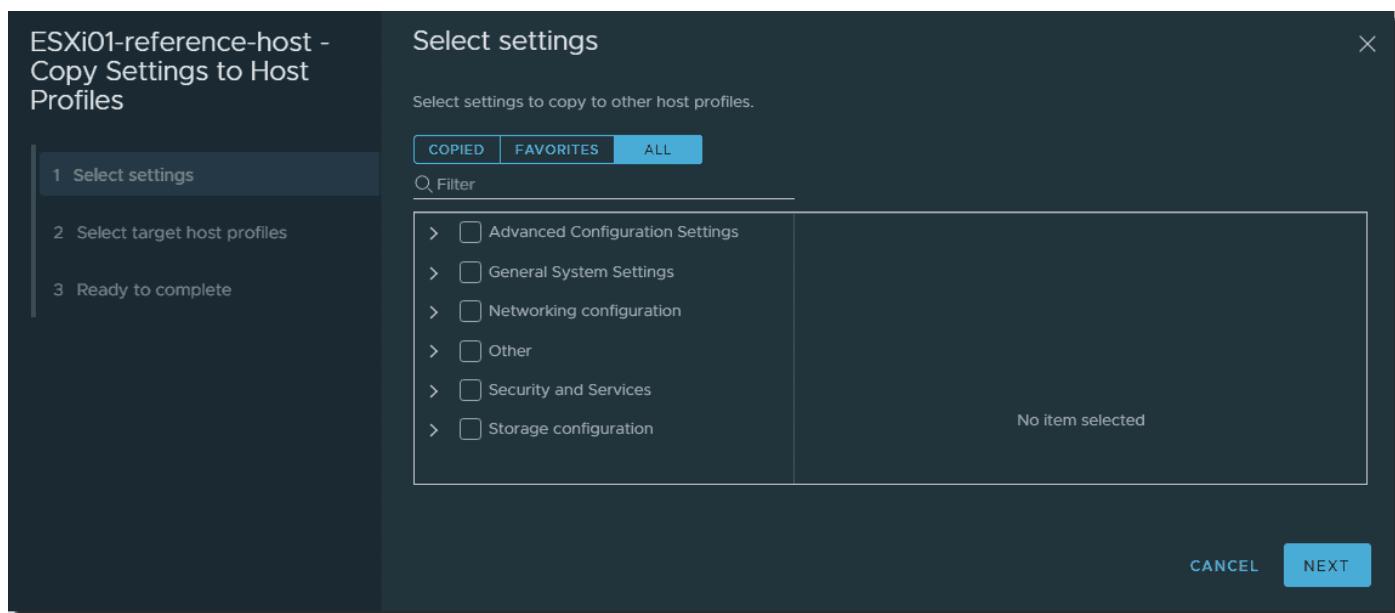
You can also add additional attributes.

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.



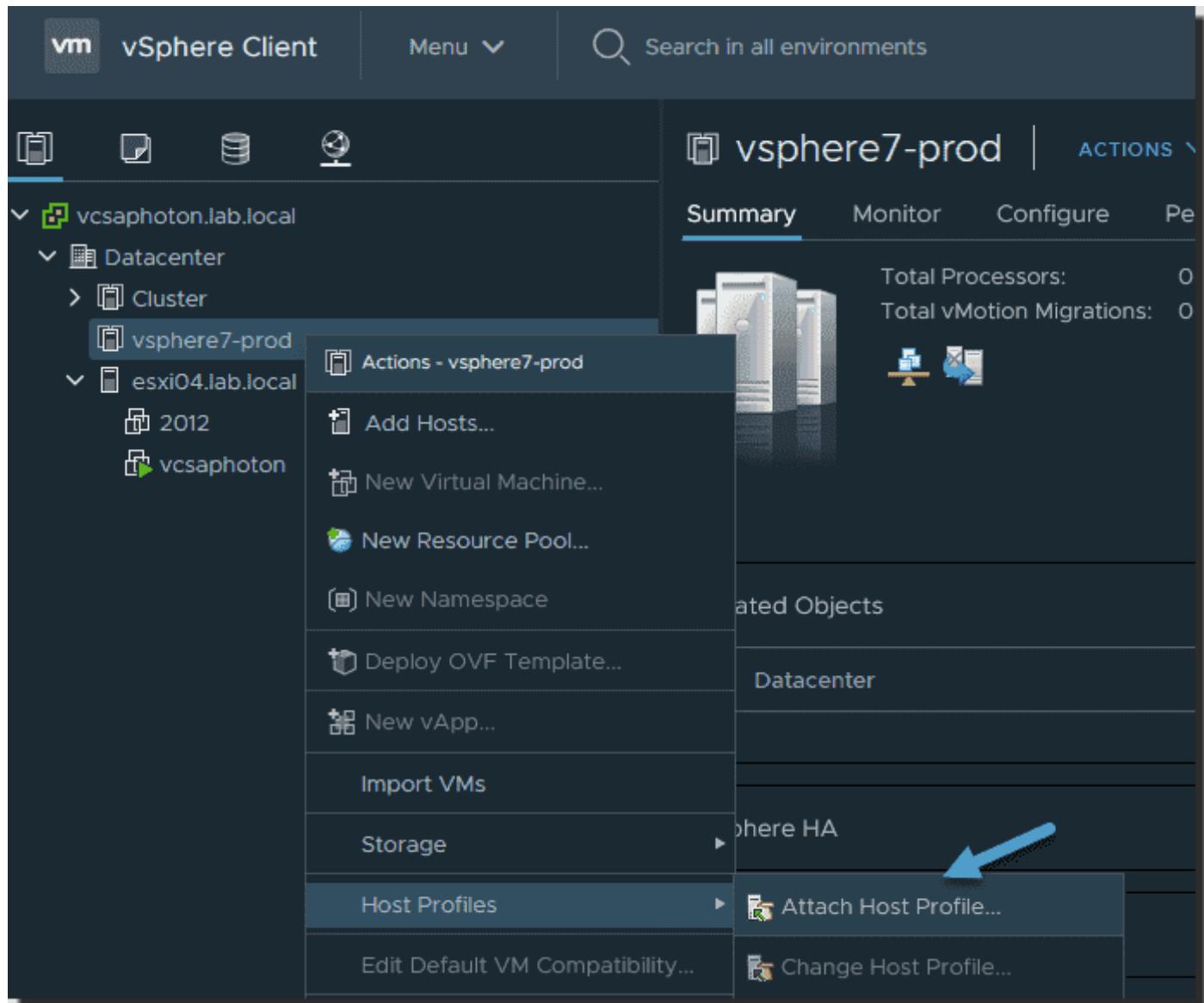
### Copy settings to a Host Profile

Then choose the destination Host Profile to apply.

### Apply a Host Profile to a host or cluster

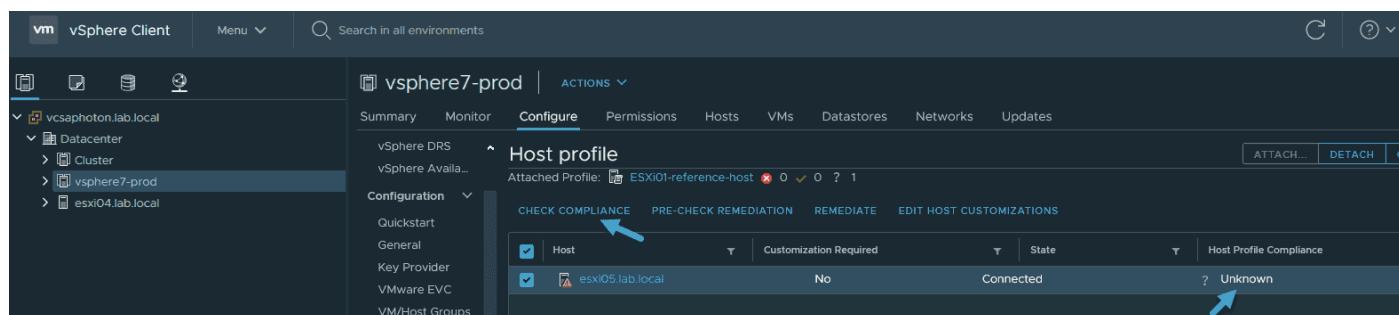
Once you have the Host Profile created and extracted from a reference host, you can apply it to a cluster or host.

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.



### Check compliance of an ESXi host in a cluster

We need to check the compliance via the **Check Compliance** button. But as 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. But it was just a part of our test.

Here is the view. When you select the check box next to the host, the lower pane shows you why it is not compliant.

Category	Profile Path	Setting Name
Virtual Machine Port Group	Networking configuration > Virtual machine portgroup > VM Network > Network policy 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		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

As you can see, the system will tell you exactly what's not the same compared to the profile. Before you execute the remediation, you can click the **Pre-Check Remediation** button and see what will be changed on the host before the remediation.

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 4.17 – Identify ESXi Boot Options

These are the media options for booting the ESXi installer:

1. Boot from a CD or DVD.
2. Boot from a USB device.
3. Boot from a network using the Preboot Execution Environment (PXE).
4. 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

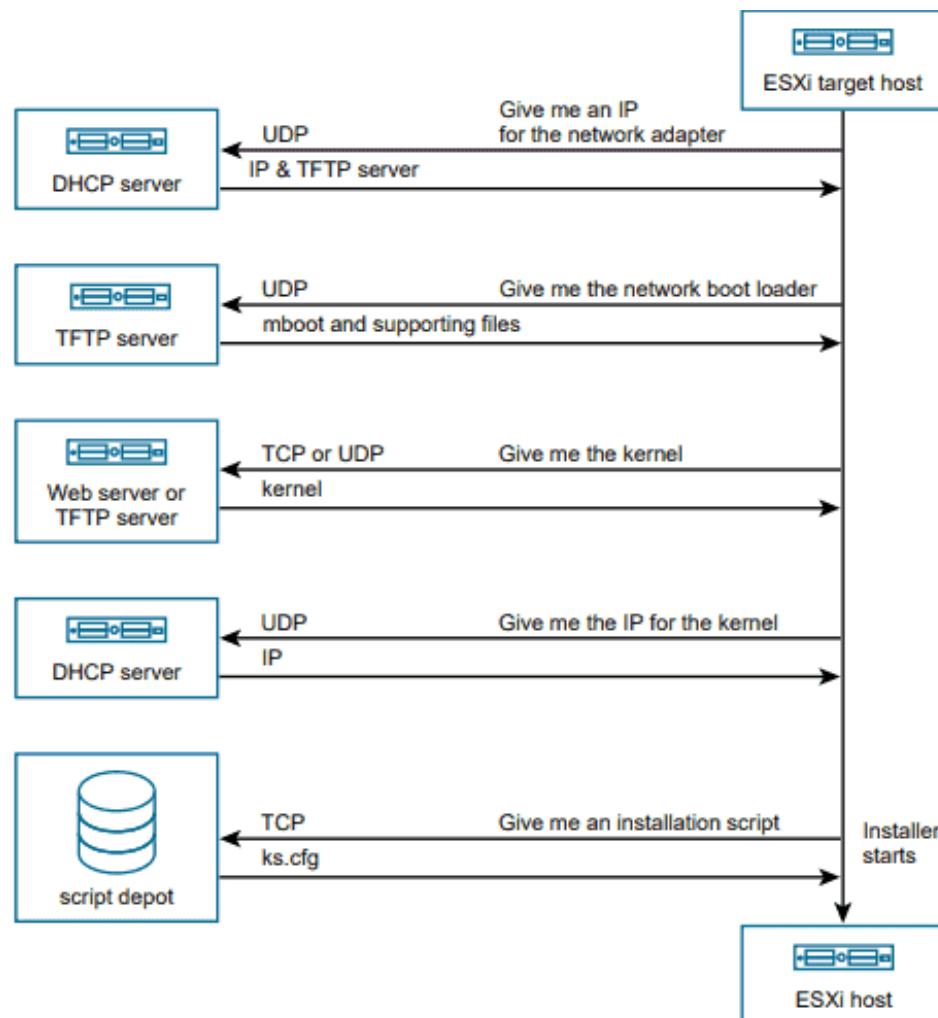
Booting from a CD or DVD is pretty straightforward. It is an interactive process in which you choose the disk or partition where you would like to install the ESXi hypervisor. Other steps, like networking or password configuration, are also easy; so we won't go into much detail here. You can also use 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:

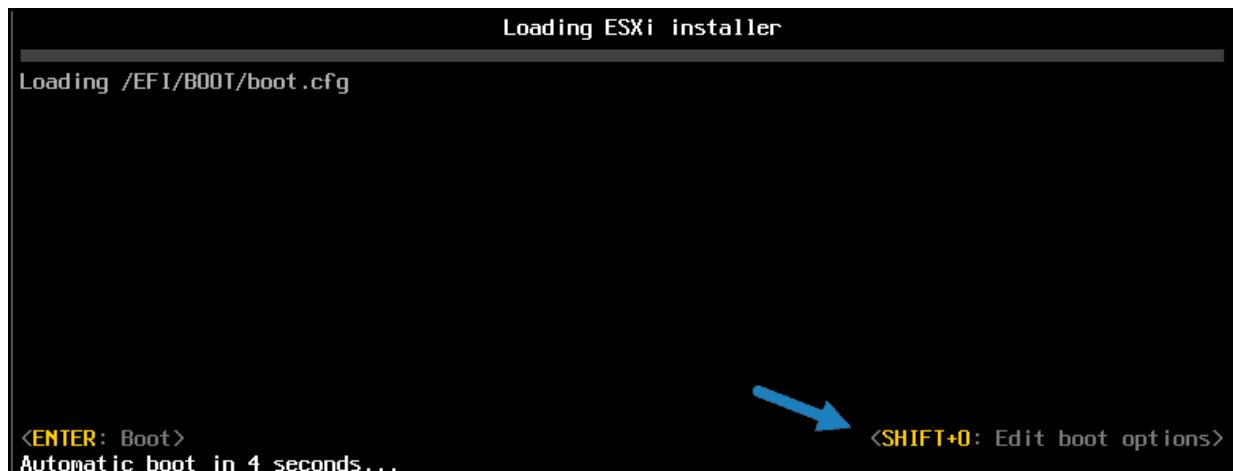
- The user boots the target ESXi host.
- The target ESXi host makes a DHCP request.
- The DHCP server responds with the IP information and the location of the TFTP server.
- The ESXi host contacts the TFTP server and requests the file that the DHCP server has specified.
- The TFTP server sends the network 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 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 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 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.

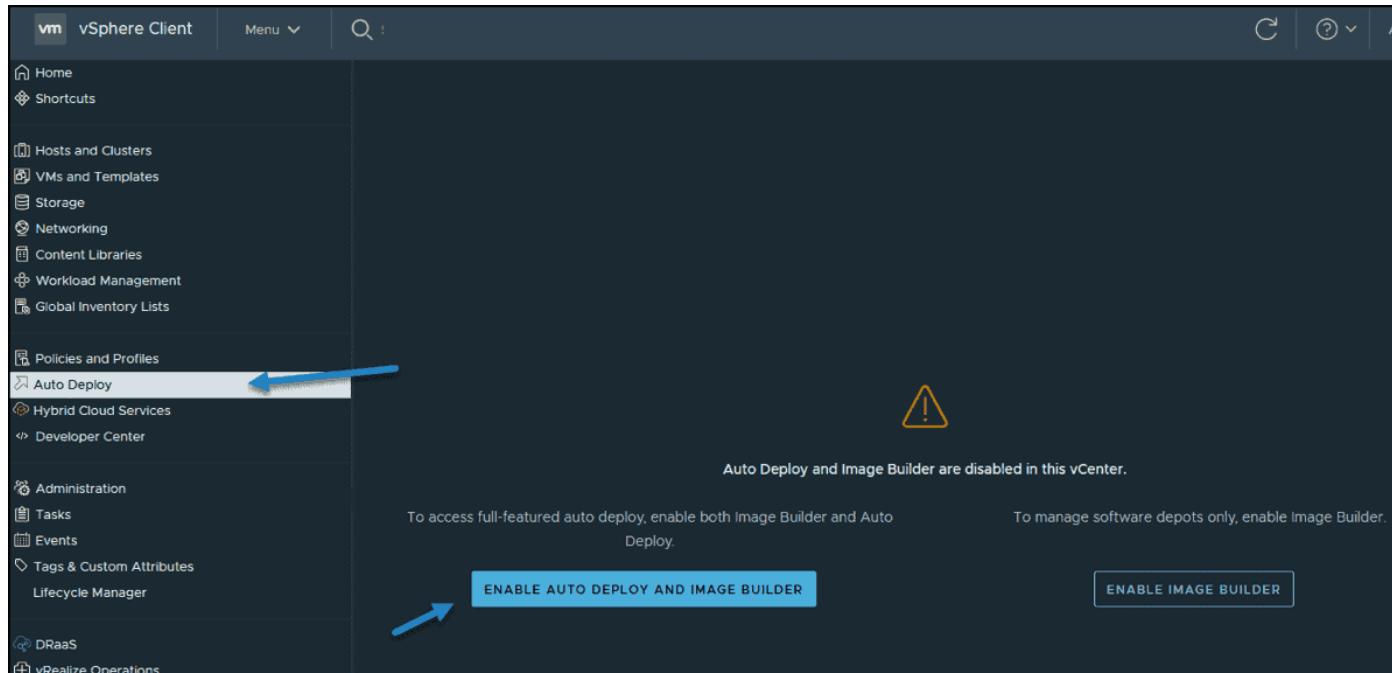
If a network boot fails, the ESXi host can use a local cache to boot from the last known ESXi image.

**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.



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.

Auto Deploy Runtime Summary (Read-only)	
Proxy Servers	none
BIOS DHCP File Name	undionly.kpxe.vmw-hardwired
UEFI DHCP File Name	snponly64.efi.vmw-hardwired
UEFI Secure Boot File Name	snponly64.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

VMware Auto Deploy Service	
cachesize_GB	2
managementport	6502
loglevel	INFO
serviceport	6501

VMware Image Builder Service	
cacheSize_GB	2
loglevel	INFO
httpPort	8099
vmomiPort	8098

Auto Deploy and Image Builder configuration screen

## Objective 4.17.1 – Configure Quick Boot

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 would it be interesting when it is not often when you have to reboot your hosts? 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 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.

**Cluster** | ACTIONS ▾

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

**Hosts** ▾

**Image**

Hardware Compatibility

VMware Tools

VM Hardware

**esxi02.lab.local**

Last checked on 01/22/2021, 4:06:05 PM (0 days ago)

⚠️ 3 of 3 hosts are out of compliance with the cluster's image

**REMEDIEATE ALL** | **RUN PRE-CHECK**

Hosts
: esxi02.lab.local
: esxi03.lab.local
: esxi01.lab.local

3 hosts

**esxi02.lab.local**

⚠️ Host is out of compliance with the image

ⓘ Quick Boot is supported on the host.  
The host will be rebooted during remediation.

**Software compliance**

Show Only drift comparison ▾

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 in the beginning of the post, 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 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 4.17.2 – Securely Boot ESXi hosts

**vSphere ESXi Secure Boot Options** - 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 only the ESXi OS is loaded and you get finally to the UI where you can log in.

When Secure Boot is enabled, the UEFI firmware process the validation of the kernel which is digitally signed. It is verified and compared with a digital certificate which is stored in the UEFI firmware.

VMware has started to support Secure boot with 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 some 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 supports TPM version 2.0.

A TPM 2.0 chip basically guarantees the ESXi host's identity.

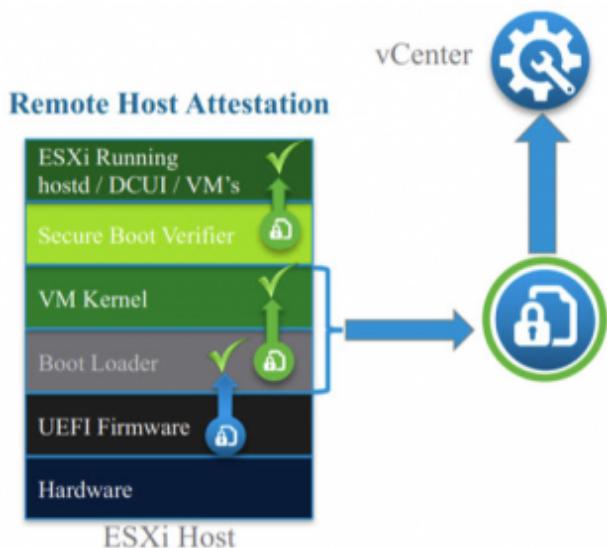
UEFI Secure Boot makes basically sure that only signed software is loaded at boot time. So it is a requirement for successful attestation.

### 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



TPM v2.0



The hardware chip will be used by ESXi host. Within the hardware, there is the UEFI firmware which validates the bootloader and the VM kernel. In the Kernel, a number of measurements are taken, which are stored in the TPM device.

The boot continues and that information is passed to vCenter. It's vCenter which queries the ESXi host and queries the TPM device and compares the hashes which have been reported by ESXi against the hashes reported by TPM.

## Objective 4.18 – Deploy and configure clusters using the vSphere Cluster QuickStart workflow

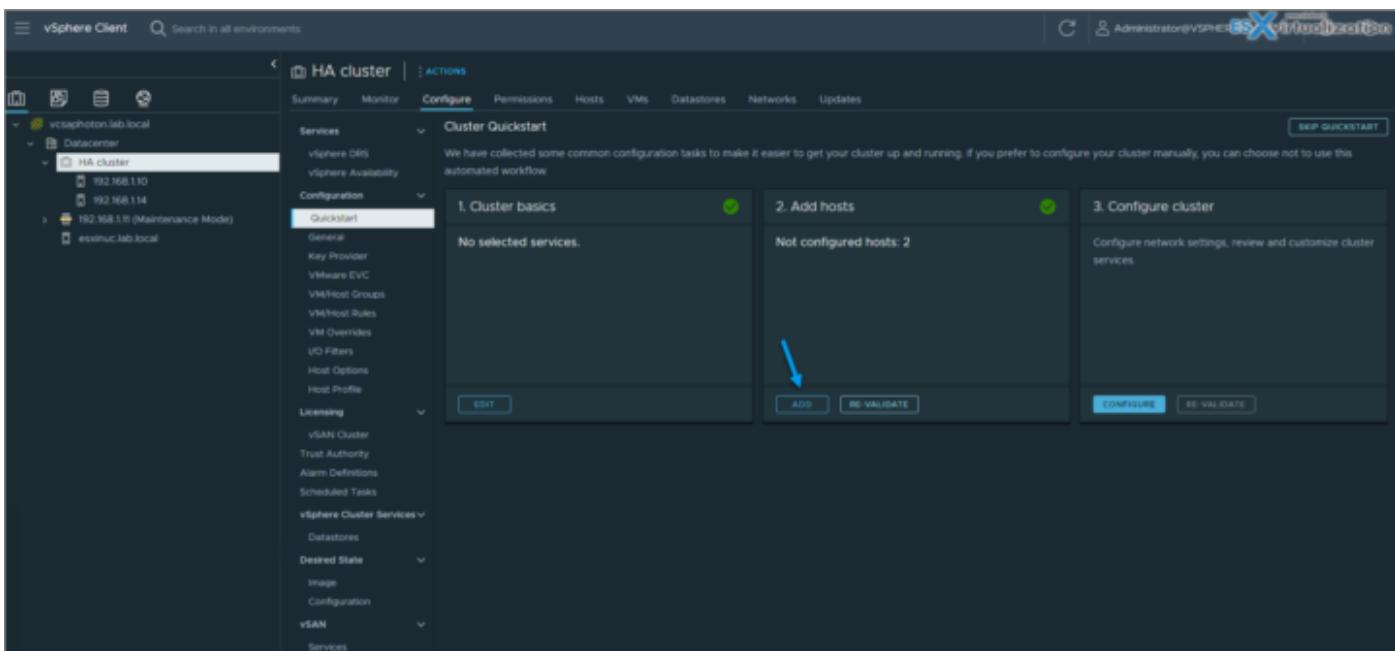
A cluster is a group of hosts. When a host is added to a cluster, the resources of the host become part of the resources of the cluster. The cluster manages the resources of all hosts that it contains. You can create clusters in the vSphere Client and then configure them using the Quickstart workflow or manually.

You can use Quickstart to configure HA/DRS cluster and also for vSAN configuration. Quickstart can also be used to expand existing cluster(s).

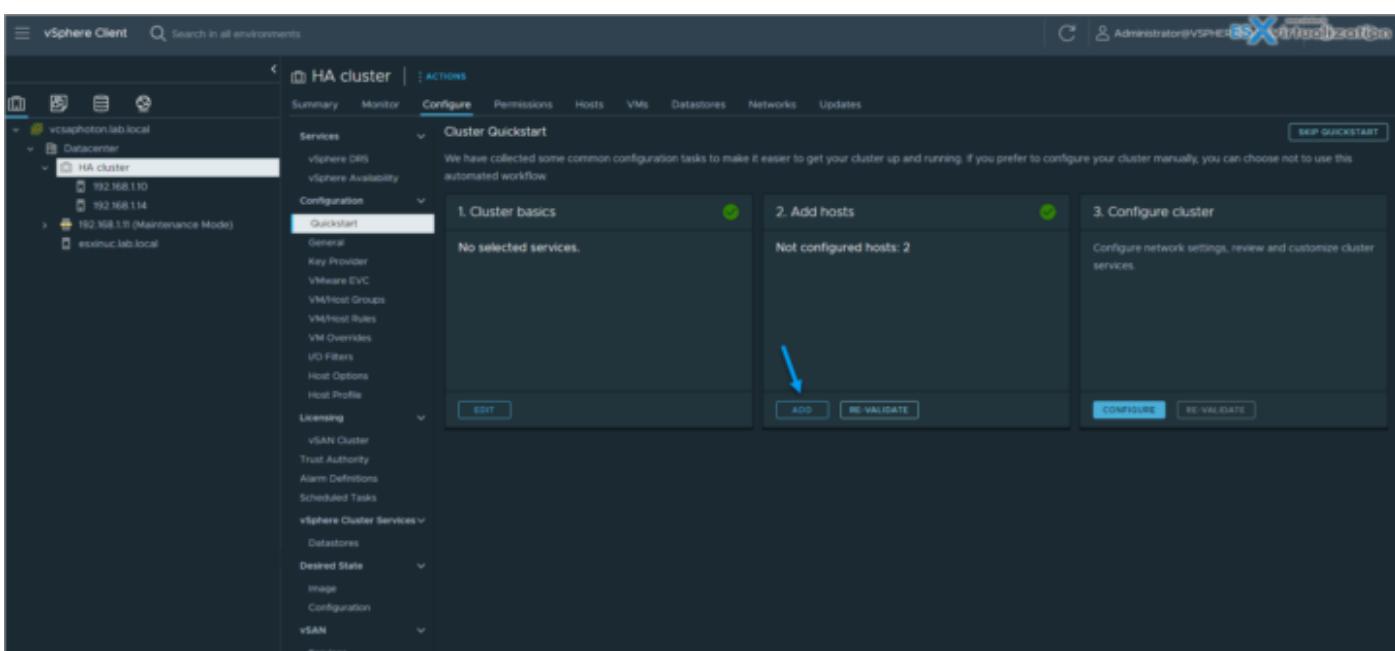
Quickstart groups common tasks and offers configuration wizards that guide you through the process of configuring and extending a cluster. Once you provide the required information on each wizard, your cluster is configured based on your input.

## Objective 4.18.1 – Use Cluster QuickStart workflow to add hosts

You can add new ESXi hosts. After the hosts are added, the card shows the total number of hosts present in the cluster and displays health check validation for those hosts.

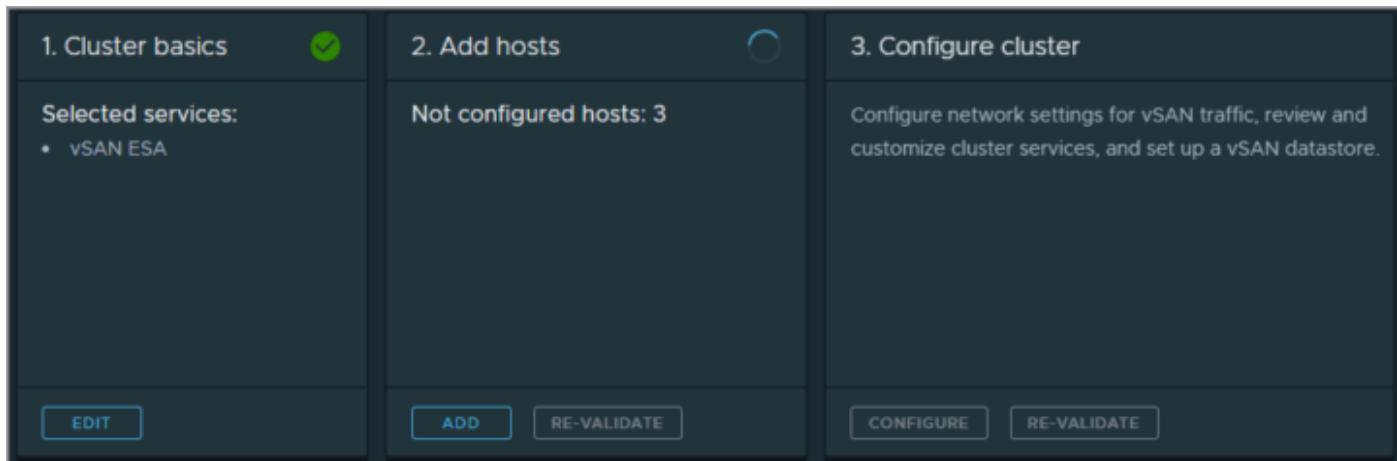


You can add existing host or a new host, via the wizard.



## Objective 4.18.2 – Use Cluster QuickStart workflow to configure a cluster

You can configure network settings for vMotion and vSAN traffic, review and customize cluster services, and set up a vSAN datastore. After the cluster is configured, the card provides details on configuration mismatch and reports cluster health results through the vSAN Health service.

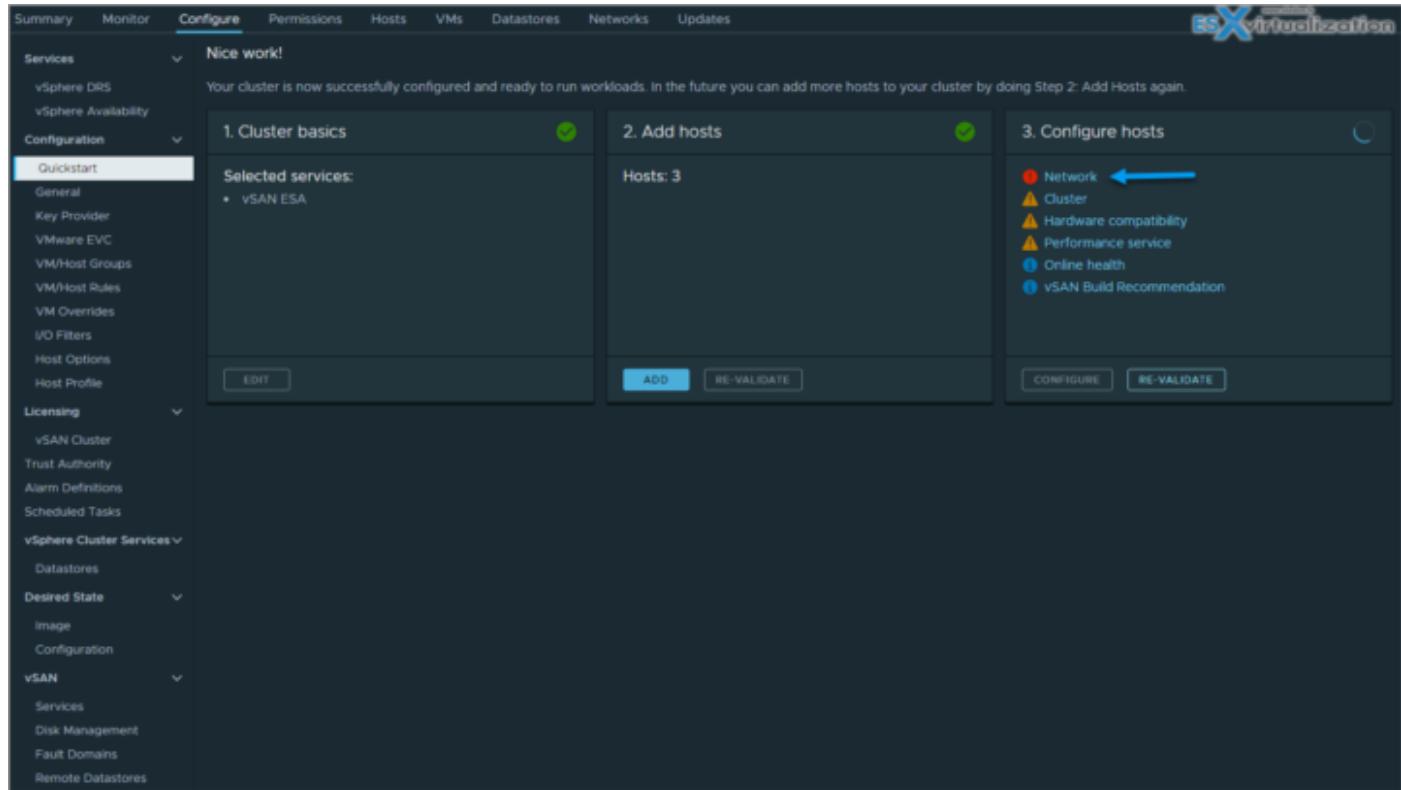


## Objective 4.18.3 – Use QuickStart to expand clusters

In order to expand cluster, you can add more hosts via the wizard. The vSAN cluster can be expanded as well by adding more compatible hosts you'll expand your cluster's resources. Expand your cluster manually or by using the Quickstart workflow and the Add hosts card.

Screenshot from the lab, after activating vSAN ESA, HA and DRS via QuickStart. You appreciate the automation that is going on under cover. The yellow triangles messages is because the lab hardware isn't certified and the vLCM configuration is not set to manage the cluster via single image (yet).

The cluster QuickStart is helpful when troubleshooting cluster services. It pinpoint the problems and shows you where to look at.



## Objective 4.19.1 – Configure Time Configuration

**Note:** screenshots from older ESXi, but principle the same.

If your host is not configured with a correct time source then you might have problems with the time sync within your VMs as those picking time sync from your host. (if not configured on per-VM basis). How? Via **VMware tools periodic time synchronization** which is happening during specific events, such as:

- Snapshot operation (during regular daily backups!)
- Resuming or suspend operation
- vMotion operation
- VMware Tools startup operation (startup/reboot)

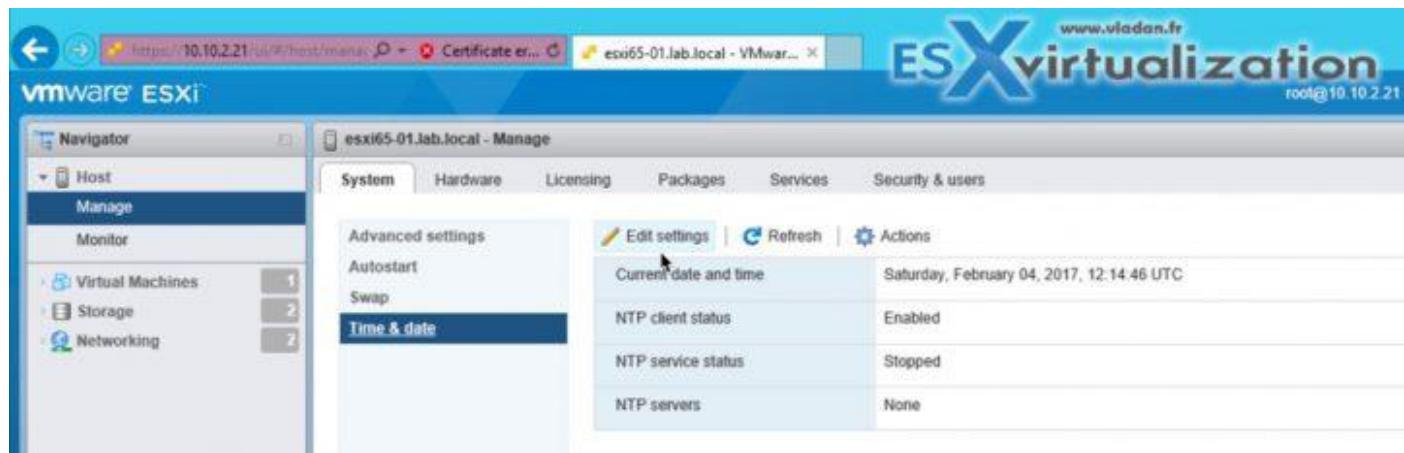
Many admins also use MAC or Linux desktops/laptops so the choice of [ESXi host client](#) is their preferred method. Perhaps they simply don't want to use a Windows machine with vSphere client installed or they don't want to bother to set up a Windows VM through [VMware Workstation](#)/Player or Fusion.

How to configure ESXi 6.5 Network Time Protocol (NTP) via Host Client?

Simple. Connect to your ESXi host via vSphere host client (if it's individual host. If the host is managed via vCenter, use vSphere Web client – we'll join a screenshot too at the end of this post). The url of the connection is:

*https://IP\_of\_ESXi/UI*

Then on the left, just below the host, select the **Manage > System > Time and Date**

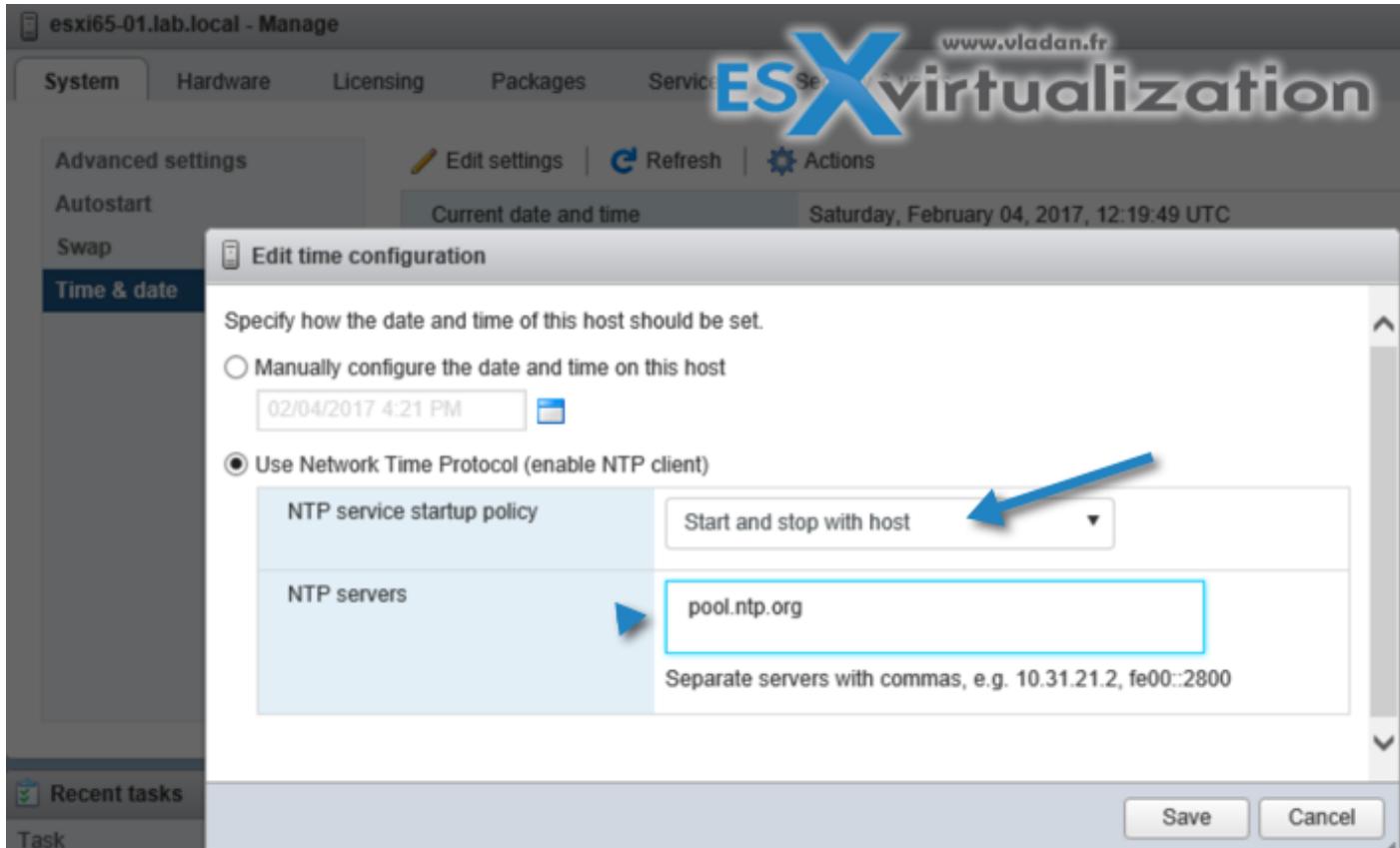


Then click the Edit Settings button to bring up the configuration window. Set the NTP service startup policy as "Start and stop with host". Like this everytime the host will reboot, the NTP service will be started automatically.

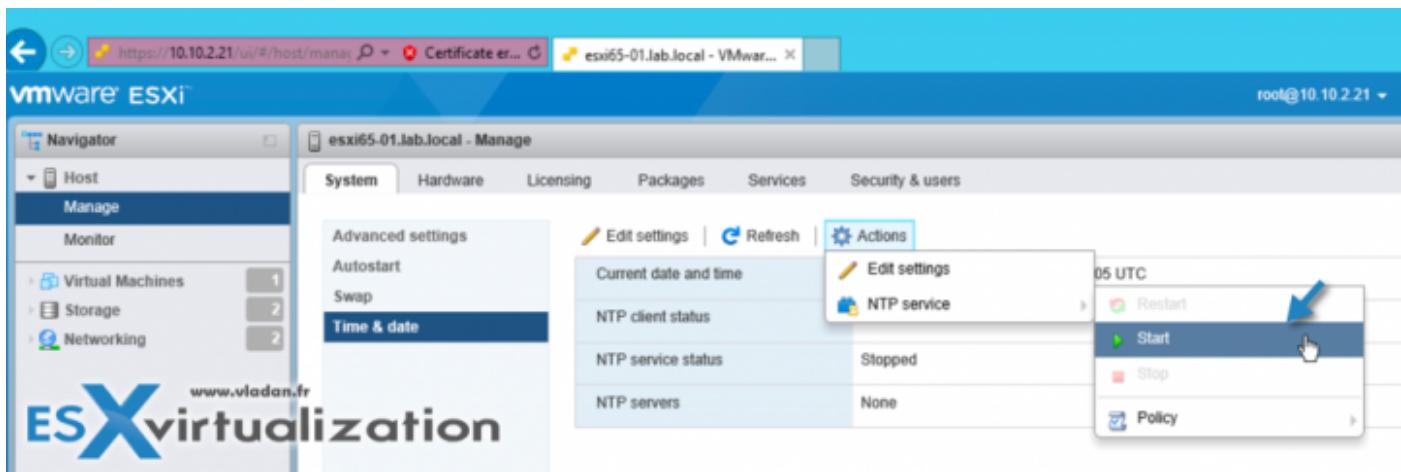
Then enter a local or remote NTP server. For example:

*pool.ntp.org*

Validate your settings with the Save button.



Next you'll have to make sure to actually start the NTP service because configuring the policy and not starting the service is not enough. You can start the service by selecting again the **Time and date > Actions > NTP service > Start**



You're done. The host is now syncing the time with the NTP server you have entered.

**Note:** You'll have to check that your host can communicate successfully with the public server over NTP (UDP Port 123), make sure that your firewall has this port open.

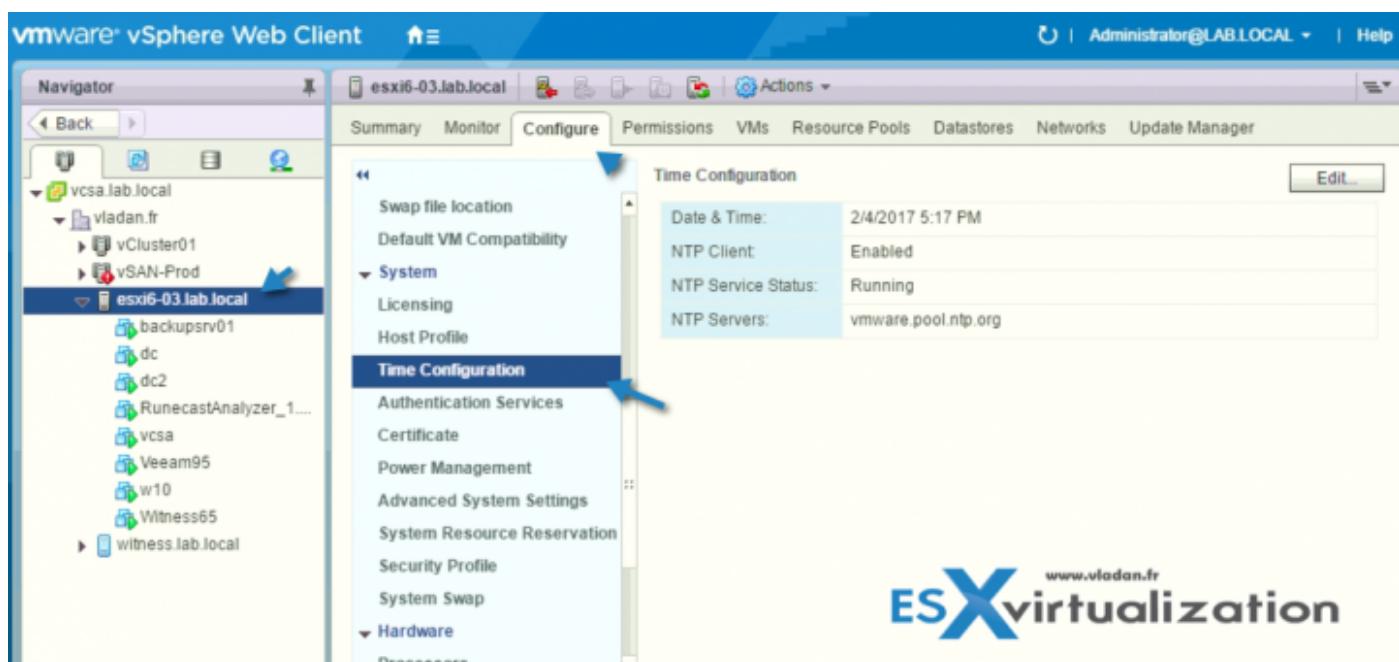
What can happen if your host has incorrect time?

Few min, or even half an hour or more than an hour. Everything is possible. Well, where time sync really matters is certainly for Domain controllers. If your Domain controller is off sync, then you'll have a certain number of problems happening within your domain infrastructure starting with long login times and then refused logins because of expired Kerberos tickets.

If you have vCenter installed and you're managing your hosts via vSphere Web client?

You can find the settings in this location by **Selecting your Host > Configure > System > Time configuration**

Here is a screenshot too...



## Objective 4.19.2 – Configure ESXi Services

Covered in 4.19.1 – you see the principle

## Objective 4.19.3 – Configure Product Locker

VMware *ProductLocker* is a central location for VMware tools. It is a VMware tools repository that all ESXi hosts can reach, which means that it is a shared datastore.

What is a VMware Tools version-mapping file?

This is what's called by VMware a VMware version-mapping file that details the version of VMware Tools released and which release of VMware ESXi is mapped into that version of VMware tools. it looks like this:

<https://packages.vmware.com/tools/versions>

### Quote:

*This file provides a one-to-one mapping between VMware Tools for*

*# ESX/ESXi version-number codes, and paths to OSP repositories suitable*

*# for that Tools version.*

*#*

*# The ESXi server mapping is only to show that the particular version of*

*# Tools ships with that particular ESXi server build number, but the Tools*

*# can work with a greater range of ESXi versions.*

```
# VMware version-mapping file.
#
# This file provides a one-to-one mapping between VMware Tools for
# ESX/ESXi version-number codes, and paths to OSP repositories suitable
# for that Tools version.
#
# The ESXi server mapping is only to show that the particular version of
# Tools ships with that particular ESXi server build number, but the Tools
# can work with a greater range of ESXi versions.
#
# Column 1: Tools version on NGC/VI Client
# Column 2: ESXi server version.'esx/0.0' indicates that the tools version
# is not yet bundled with ESXi.
# Column 3: ESXi server build number
# Column 4: Tools version on guest Setup/About page
# Column 5: Tools build number
#
12325    esx/8.0p01      21203435      12.1.5      20735119
12320    esx/7.0p06      20842708      12.1.0      20219665
12325    esx/0.0          12.1.5      20735119
12294    esx/8.0          20513097      12.0.6      20104755
12294    esx/6.7p08      20497097      12.0.6      20104755
12294    esx/6.5p09      20502893      12.0.6      20104755
12320    esx/0.0          12.1.0      20219665
10361    esx/0.0          10.3.25      20206839
12294    esx/0.0          12.0.6      20104755
12288    esx/7.0p05      20036589      12.0.0      19345655
12288    esx/6.7p07      19898906      12.0.0      19345655
12293    esx/0.0          12.0.5      19716617
12288    esx/6.5p08      19588618      12.0.0      19345655
11365    esx/7.0p04      19482537      11.3.5      18557794
11365    esx/6.7p06      18828794      11.3.5      18557794
10360    esx/0.0          10.3.24      18733423
11360    esx/6.5p07      18678235      11.3.0      18090558
11360    esx/7.0u3      18644231      11.3.0      18090558
11334    esx/7.0p03      18426014      11.2.6      17901274
11333    esx/7.0u2      17630552      11.2.5      17337674
11333    esx/6.7p05      17700523      11.2.5      17337674
11329    esx/6.5p06      17477841      11.2.1      17243207
10359    esx/6.5p06      17477841      10.3.23      17030940
11328    esx/0.0          11.2.0      16938113
11301    esx/7.0p02      17325551      11.1.5      16724464
11297    esx/7.0u1      16850804      11.1.1      16303738
11297    esx/6.7p04      17167734      11.1.1      16303738
11297    esx/6.7p03      16713306      11.1.1      16303738
11297    esx/6.5p05      16576891      11.1.1      16303738
11296    esx/7.0p01      16324942      11.1.0      16036546
10358    esx/0.0          10.3.22      15902021
11270    esx/0.0          11.0.6      15940789
11269    esx/6.7p02      16075168      11.0.5      15389592
11269    esx/7.0          15843807      11.0.5      15389592
```

Get the latest version of VMware Tools and put it into a shared location (ProductLocker)

Go to this location to get the latest version of VMware tools and login with your VMware account (if you don't have one, you can create one for free).

<https://www.vmware.com/go/tools>

The screenshot shows the VMware Customer Connect website. At the top, there are navigation links: Products and Accounts, Knowledge, Communities, Support, and Learning. On the right, there is a logo for 'ESX virtualization'.

The main content area is titled 'Download Product'. It shows the selected version is '12.1.5'. Below this, there are sections for Documentation (Release Notes), Release Date (2022-11-29), and Type (Product Binaries). To the right, there are links for Product Resources, View My Download History, and Documentation.

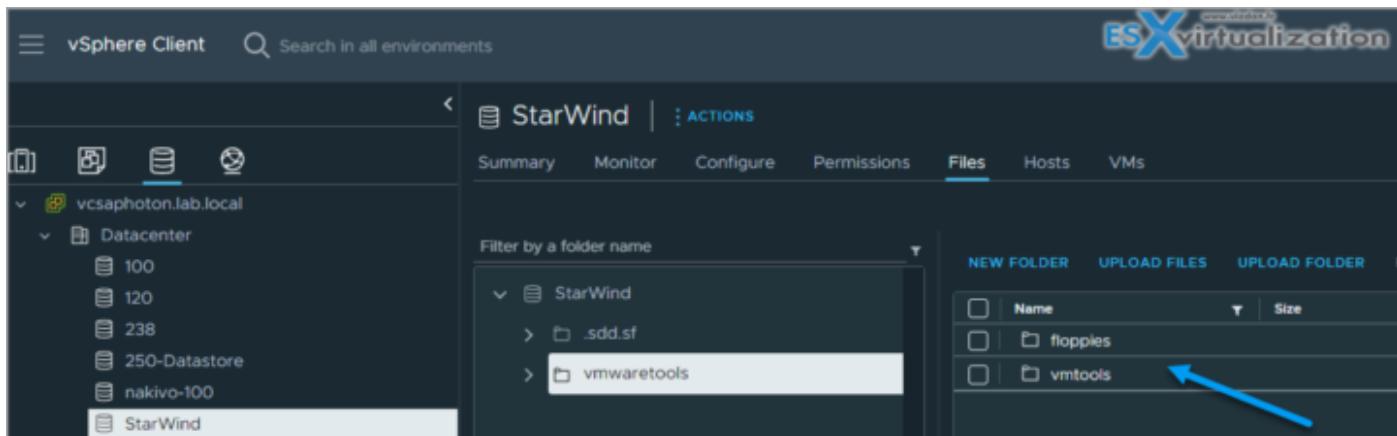
The 'Product Downloads' tab is selected. Below it, there are several download options:

File	Information	Action
VMware Tools packages for Windows	File size: 108.56 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for Windows	File size: 108.56 MB File type: gz	<a href="#">DOWNLOAD NOW</a>
VMware Tools for Windows, 32-bit in-guest installer	File size: 34.85 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools for Windows, 64-bit in-guest installer	File size: 70.36 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for GuestStore	File size: 105.22 MB File type: zip	<a href="#">DOWNLOAD NOW</a>
VMware Tools packages for GuestStore	File size: 105.22 MB File type: gz	<a href="#">DOWNLOAD NOW</a>
VMware Tools Offline VIB Bundle	File size: 321.82 MB File type: zip	<a href="#">DOWNLOAD NOW</a>

Now create a central repository on your shared datastore. This datastore is accessible from all the hosts within your cluster. The process is fairly simple. Here are the steps:

Create a folder, we name it "vmwaretools" and we create it on a shared datastore provided by StarWind. What we need to do next is to extract the latest VMware Tools into the directory we have just created. Simple, right?

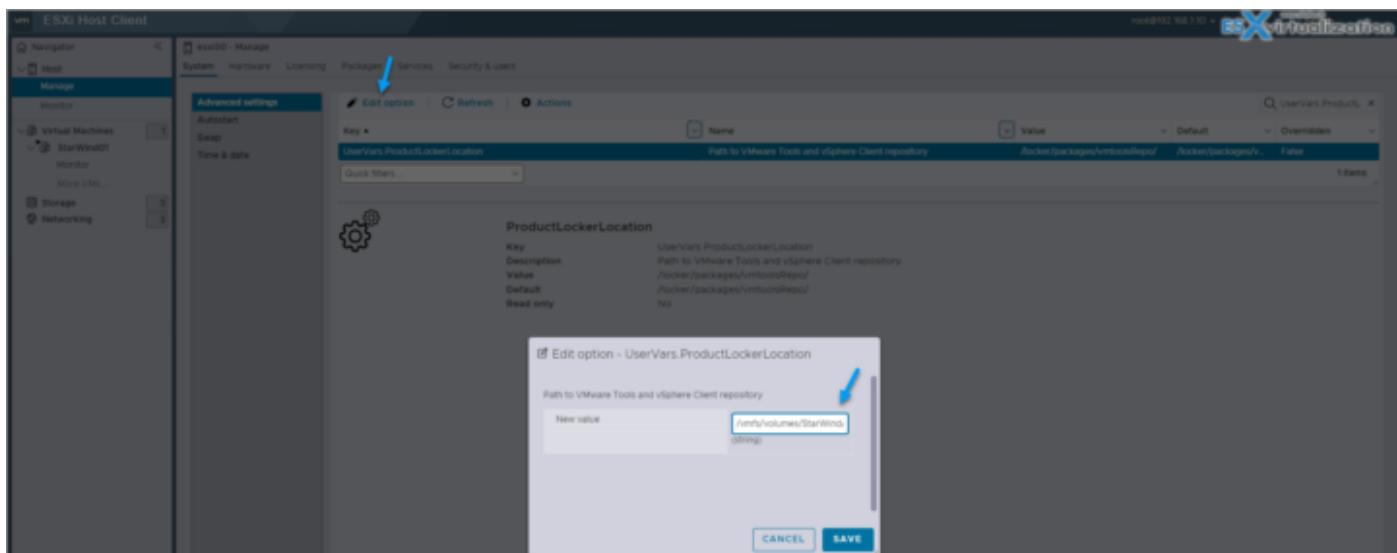
FYI, We have downloaded the latest VMware Tools packages for Windows version 12.1.5.



Next, we need to change the location for ESXi VMware Tools Update. We can do that via ESXi host client for example (note that there are other ways to do it as well, ex. via CLI, via MOB (managed object browser) or others).

Fire up your ESXi host client and go to the **Advanced System Settings**. The user variable that you want to update is the **UserVars.ProductLockerLocation** variable. Just change it to your shared datastore path....

## UserVars.ProductLockerLocation



The defaults are:

/locker/packages/vmtoolsRepo

## Find the current ProductLocker location:

From ESXi shell:

```
ls -l /productLocker
```

*readlink /productLocker*

Next, we need to delete the Symlink location for ProductLocker. We need to change the ProductLocker location to the centralized repo by updating SymLink (in fact, we need to delete the SymLink and recreate it).

You could simply just reboot your ESXi hosts instead, but we can avoid you to do so via this:

*rm productLocker*

*ln -s /vmfs/volumes/StarWind/vmwaretools /productLocker*

Well, this is it my friends.

Check the [VMware KB2129825](#) for further details.

## Objective 4.19.4 – Configure Lockdown Mode

In order to make your ESXi hosts more secure, you can put them what's called Lockdown mode. This post will explain What is VMware ESXi Lockdown Mode, what's the main benefits and the configuration steps. The config is a simple radio button via vSphere web client, but there is also a possibility to activate it through the Direct Console User Interface (DCUI). This is another post for our [Tips](#) category.

This is the first time we treat this topic and It's important to know what services and restrictions apply in each mode. VMware ESXi Lockdown Mode applies not only to users but also to CIM providers or applications using which needs to keep running (ex. backups).

ESXi lockdown mode has been introduced in ESXi 5.0 in its simpler version, which has been expanded with ESXi 6.0 and ESXi 6.5. If you put the host into a lockdown mode, you can only connect and manage your hosts and your VMs through vCenter Server. Your connection is denied if you want to connect directly to the host via host client.

In lockdown mode, operations must be performed through vCenter Server by default. It was in vSphere 6.0 first where you can choose either between a **normal lockdown mode** or **strict lockdown mode**.

ESXi user accounts which are on a special list called Exception Users, which has administrator's privileges and those users can also log in to the ESXi shell through DCUI, or Host client.

Where to Activate VMware ESXi Lockdown Mode?

In order to activate lockdown mode, you can use vSphere Web client or vSphere HTML5 Client.

**Select your host > Configure > System > Security Profile > Edit.**

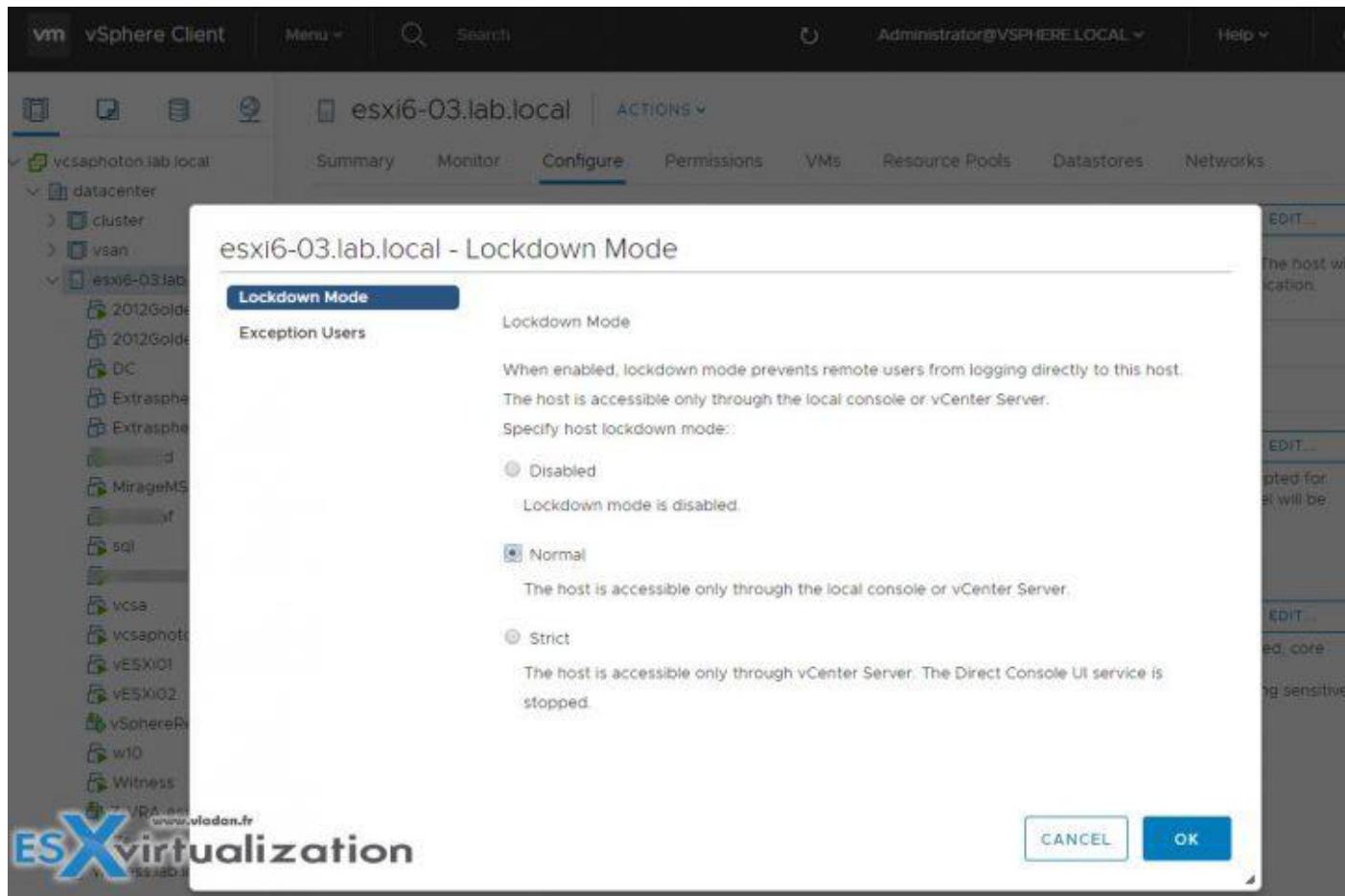
The screenshot shows the vSphere Client interface with the title bar "vSphere Client". The left sidebar lists datacenters, clusters, and hosts under "vcsaphoton.lab.local". The host "esxi6-03.lab.local" is selected. The main pane shows the "Configure" tab selected. Under the "System" section, the "Security Profile" is highlighted. A blue arrow points to the "Lockdown Mode" section, which is currently set to "Disabled". Other sections shown include "Host Image Profile Acceptance Level" (set to "Community Supported") and "Host Encryption Mode" (set to "Disabled"). The right side of the interface features the NAKIVO logo.

VMware ESXi Lockdown Mode – two different modes.

Let's have a look what's the difference between Normal and Strict Lockdown Mode:

**Normal Lockdown Mode** – The host can be accessed through vCenter Server. Only users who are on the **Exception Users** list and have administrator privileges can log in to the Direct Console User Interface. If SSH or the ESXi Shell is enabled, access might be possible.

**Strict Lockdown Mode** – The host can only be accessed through vCenter Server. If SSH or the ESXi Shell is enabled, running sessions for accounts in the DCUI.Access advanced option and for Exception User accounts that have administrator privileges remain enabled. All other sessions are terminated.



In addition, when selecting the Strict Lockdown mode, the DCUI service is completely stopped.

What are the Exception Users?

VMware says that those are users that...

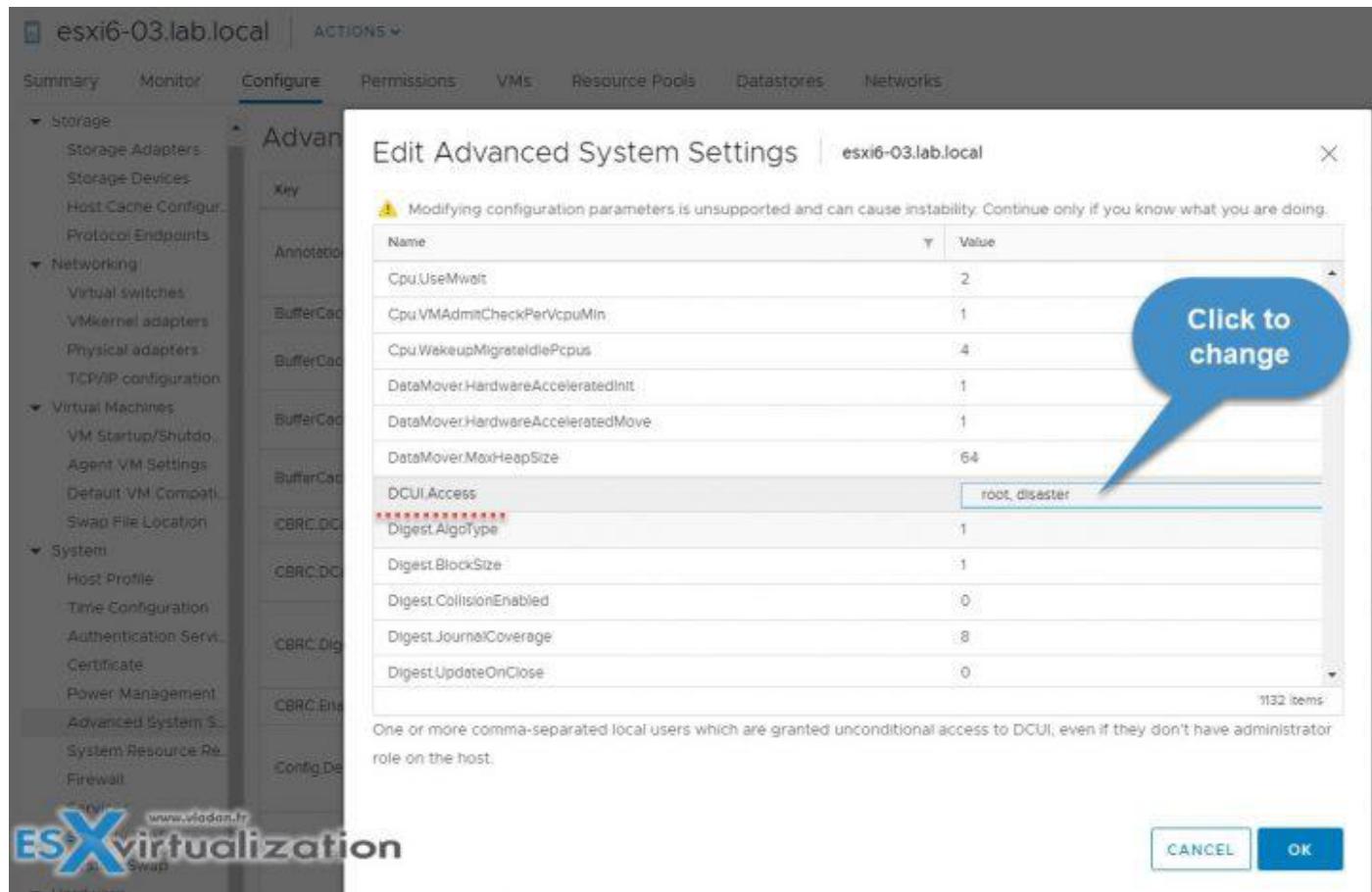
Quote:

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

Where to add an account to the Exception Users list?

You'd have to first create a local ESXi user and then specify this advanced settings on per-host base. So in my case, I created a sample local ESXi user called "disaster" through ESXi host client which is a local ESXi user.

So in order to modify the Exception users list, you'll have to use the vSphere HTML5 client of vSphere Web Client. To access this setting you **Select your host > System > Advanced System Settings >** within the list find the **DCUI.Access** > click to add another local ESXi user there. The root user is already present there by default.



The exception users can only perform tasks for which they have privileges for. So even if you create your local user and put him on the Exceptions list, the user won't be able to connect unless you give him a privilege.

Connect to the ESXi host via **ESXi Host Client > Actions > Permissions**.

This host is being managed by vCenter Server. Actions may be performed automatically by vCenter Server.

Hardware	
Manufacturer	Supermicro
Model	X10SRH
CPU	8 CPUs x Intel(R) Xeon(R) CPU E5-2630L v3 @ 1.80GHz
Memory	127.9 GB

Then Click **Add User**

User	Role
dcui	Administrator
LAB\esx^admins	Administrator
root	Administrator
vpxuser	Administrator

The UI will change and here you have the possibility to **pick the user you have previously created** and then **assign a privilege** to this user.

VMware has a nice table showing exactly which services or which behaviors are different for Normal and for a Strict Locked mode. This behavior has an influence on the vSphere Web services API, CIM providers, DCUI, ESXi Shell and SSH.....

The table can be found at VMware Documentation Center – [Link](#).

Lockdown Mode Behavior			
Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser)	vCenter (vpxuser)
		Exception users, based on permissions	Exception users, based on permissions
		vCloud Director (vslauser, if available)	vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser)	vCenter (vpxuser)
		Exception users, based on permissions	Exception users, based on permissions
		vCloud Director (vslauser, if available)	vCloud Director (vslauser, if available)
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the DCUIAccess advanced option	Users defined in the DCUIAccess advanced option	DCUI service is stopped
		Exception users with administrator privileges on the host	
ESXi Shell (if enabled)	Users with administrator privileges on the host	Users defined in the DCUIAccess advanced option	Users defined in the DCUIAccess advanced option
		Exception users with administrator privileges on the host	Exception users with administrator privileges on the host
SSH (if enabled)	Users with administrator privileges on the host	Users defined in the DCUIAccess advanced option	Users defined in the DCUIAccess advanced option
		Exception users with administrator privileges on the host	Exception users with administrator privileges on the host

So, In which mode I'll be able to log in through the DCUI?

Only if the Standard lockdown mode is activated. **Not** in the Strict mode.

What if vCenter server is unavailable?

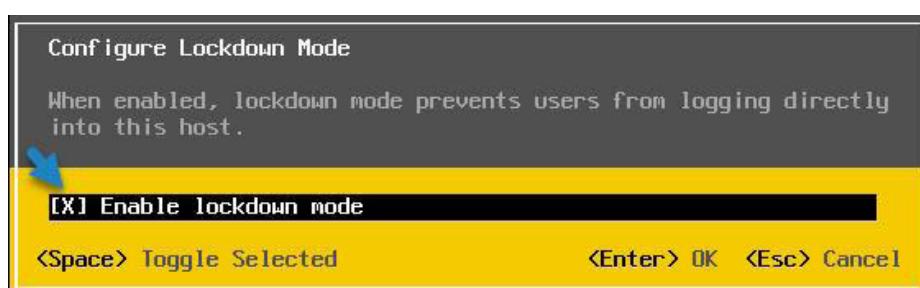
Configure Lockdown Mode will be grayed out if vCenter is down or the host is disconnected from vCenter.

Enable/Disable ESXi lockdown mode from DCUI

*Note: This applies if a host is in **Normal lockdown** mode only. Otherwise you would be able to lock yourself out from within the DCUI.*

In the server room:

**Open server console > Press F2 to Customize System/View Logs > Open Configure Lockdown Mode > Press SPACE to enable or disable lockdown mode**

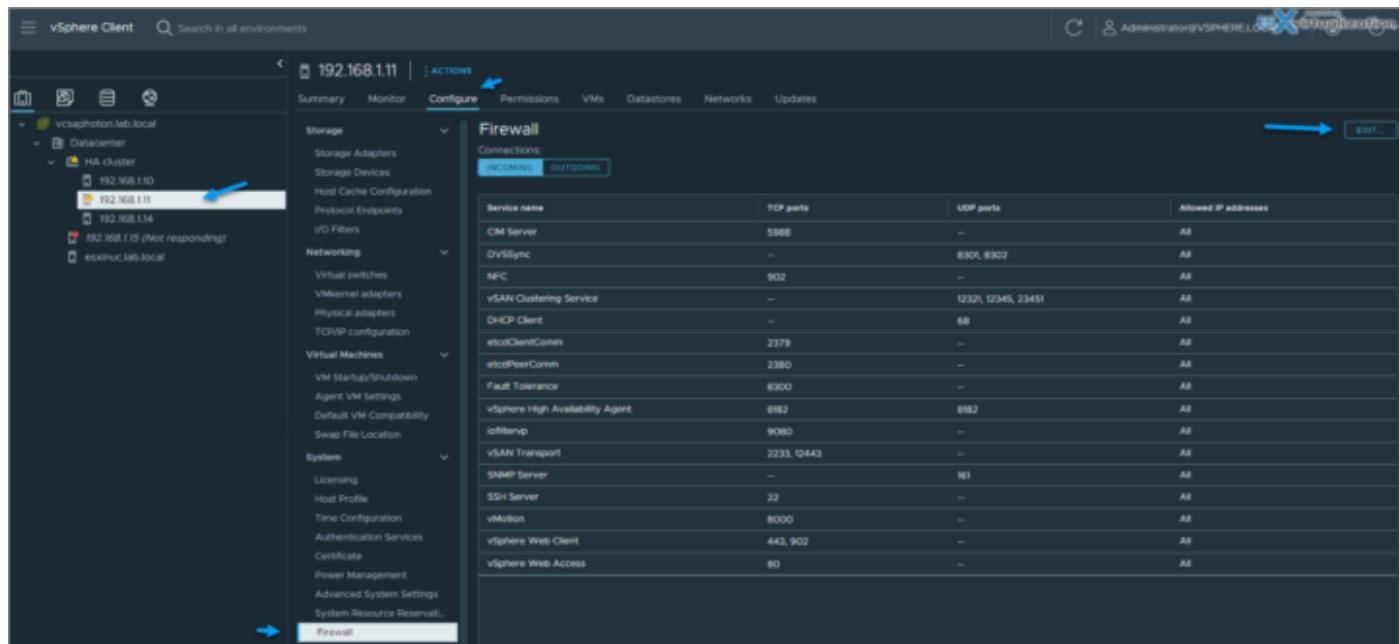


Press ENTER to save the changes. This is it.

## Objective 4.19.5 – Configure ESXi Firewall

You can configure incoming and outgoing firewall connections for a service or a management agent from the vSphere Client or at the command line.

You can use the ESXi Shell or ESXCLI commands to configure ESXi at the command line to automate the firewall configuration.



Log in to the vCenter Server by using the vSphere Client and browse to the host in the inventory > Click Configure, then click Firewall under System. You can toggle between incoming and outgoing connections by clicking Incoming and Outgoing.

In the Firewall section, click Edit. Select from one of the three service groups, Ungrouped, Secure Shell, and Simple Network Management Protocol. Select the rule sets to be activated, or deselect the rule sets to be deactivated.

For some services, you can also manage service details by navigating to Configure > Services under System. For some services, you can explicitly specify IP addresses from which connections are allowed.

via host client:

Name	Key	Incoming Ports	Outgoing Ports	Protocols	Service	Daemon
Active Directory All	activedirectoryAll	2000	123, 127, 138, 3268, 388, 443, 464, 7	UDP, TCP	N/A	None
CM Secure Server	CMHttpServer	5985		TCP	stcbio-watching	Stopped
CM Server	CMHttpServer	5988		TCP	stcbio-watchdog	Stopped
CM SLP	CMSLP	427	427	UDP, TCP	tcpd	Stopped
DHCP Client	dhcps	68	68	UDP	N/A	None
DNS Client	DHCPSv6	545	547	TCP, UDP	N/A	None
DNS Client	dns		53	UDP, TCP	N/A	None
DNS Client	DNSFilter	2222		TCP	N/A	None
DVSsync	DVSsync	8301, 8302	8301, 8302	UDP	N/A	None
esxi-orchestrator	esxi-orchestrator	8384		TCP	N/A	None
esxiComm	esxiComm	162, 2480, 5000, 8814, 8848, 9107	162, 2480, 5000, 8814, 8848, 9107	TCP, UDP	N/A	None
esxiUpdate	esxiUpdate		443	TCP	N/A	None
etcdClientComm	etcdClientComm	2379	2379	TCP	N/A	None
etcdPeerComm	etcdPeerComm	2380	2380	TCP	N/A	None
Fault Tolerance	faultTolerance	8300	80, 8300	TCP	N/A	None
FTT Client	fttClient	20	20	TCP	N/A	None
govcenter	govcenter	1000, 30000		TCP	N/A	None
govcenter	govcenter		443	TCP	N/A	None
HTTP	HTTP		31031, 44046	TCP	N/A	None
httpClient	httpClient		443, 80	TCP	N/A	None
isrltemp	isrltemp	9080		TCP	N/A	None
isrltemp	isrltemp	3005	3005	UDP	N/A	None
NPC	NPC	902	902	TCP	N/A	None

## Add allowed IP

To restrict traffic, change each service to allow traffic only from your management subnet. You can also deselect some services if your environment does not use them. To update the Allowed IP list for a service you can use the vSphere Client, ESXCLI, or PowerCLI.

Browse to the ESXi host. Click **Configure**, then click **Firewall** under System. You can toggle between incoming and outgoing connections by clicking **Incoming** and **Outgoing**.

In the Firewall section, click **Edit**. Select from one of the three service groups, **Ungrouped**, **Secure Shell**, and **Simple Network Management Protocol**.

To display the Allowed IP Addresses section, expand a service.

In the Allowed IP Addresses section, deselect Allow connections from any IP address and enter the IP addresses of networks that are allowed to connect to the host.

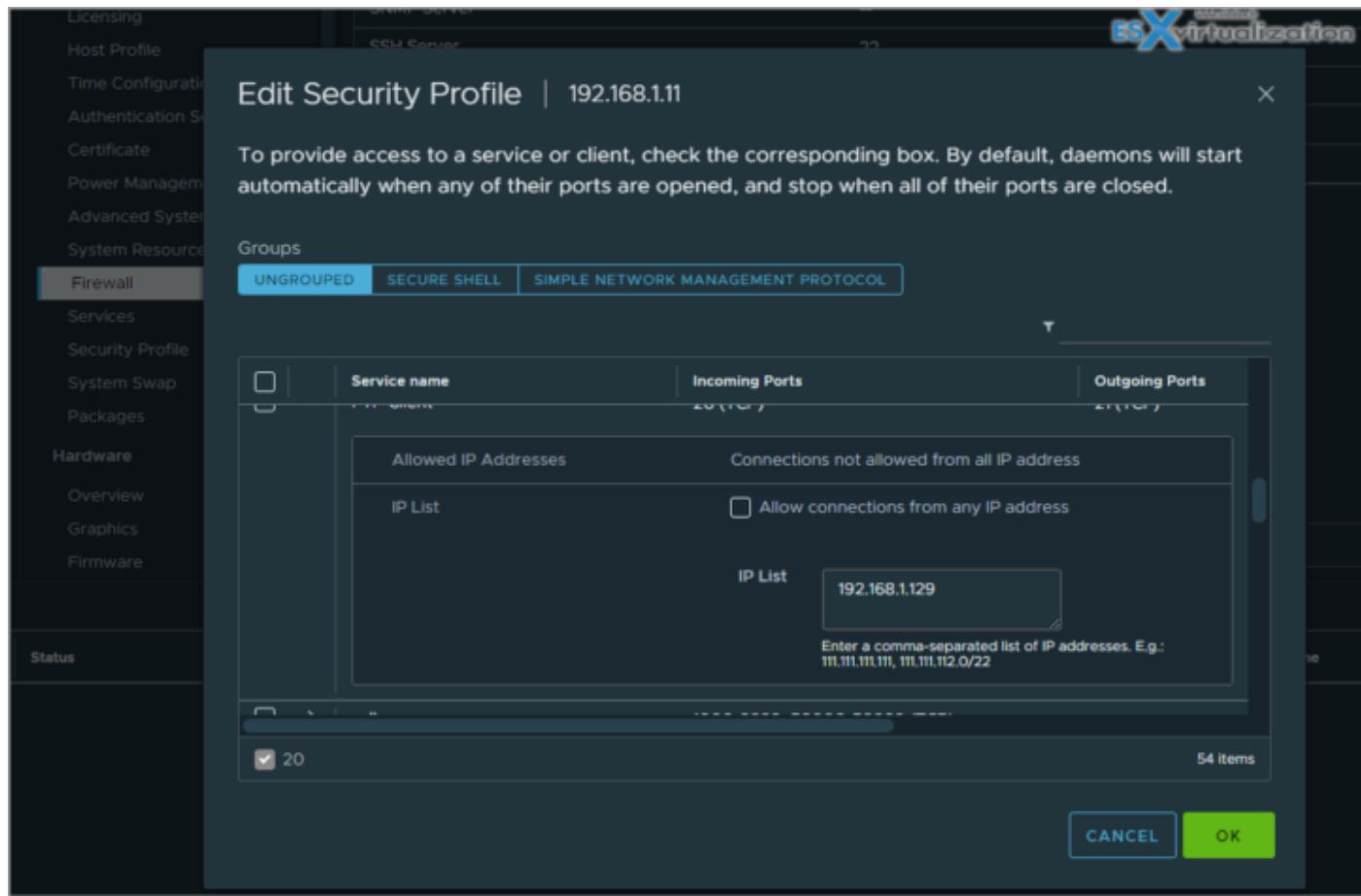
Separate IP addresses with commas. You can use the following address formats:

192.168.0.0/24

192.168.1.2, 2001::1/64

fd3e:29a6:0a81:e478::/64

Example from the lab.....



For the list of supported ports and protocols in the ESXi firewall, see the VMware Ports and Protocols Tool™ at <https://ports.vmware.com/>.

Some of the Firewall commands you can use via ESXi Shell:

***esxcli network firewall get*** - Return the status of the firewall and list the default actions.

***esxcli network firewall set --default-action*** - Set to true to set the default action to pass. Set to false to set the default action to drop.

***esxcli network firewall set --enabled*** - Activate or deactivate the ESXi firewall.

***esxcli network firewall load*** - Load the firewall module and the rule set configuration files.

***esxcli network firewall refresh*** - Refresh the firewall configuration by reading the rule set files if the firewall module is loaded.

***esxcli network firewall unload*** - Destroy filters and unload the firewall module.

***esxcli network firewall ruleset list*** - List rule sets information.

***esxcli network firewall ruleset set --allowed-all*** - Set to true to allow all access to all IPs. Set to false to use a list of allowed IP addresses.

***esxcli network firewall ruleset set --enabled --ruleset-id=<string>*** - Set enabled to true to activate the specified ruleset. Set enabled to false to deactivate the specified ruleset.

***esxcli network firewall ruleset allowedip list*** - List the allowed IP addresses of the specified rule set.

***esxcli network firewall ruleset allowedip*** - add Allow access to the rule set from the specified IP address or range of IP addresses.

***esxcli network firewall ruleset allowedip remove*** - Remove access to the rule set from the specified IP address or range of IP addresses.

***esxcli network firewall ruleset rule*** - list List the rules of each ruleset in the firewall.

The screenshot shows a terminal session on an ESXi host (192.168.1.11) using the esxcli command to list the status of various network services. The output is as follows:

Name	Enabled
sshServer	true
sshClient	false
nfsClient	false
ntfs4Client	false
dhcp	true
dns	true
smp	true
ntpClient	false
CIMHttpServer	true
CIMHttpsServer	false
CIMSLP	false
iSCSI	false
vpxHeartbeats	true
updateManager	true
faultTolerance	true
webAccess	true
vMotion	true
vsphereClient	true
activeDirectoryAll	false
NFC	true
HDHR	true
ftpClient	false
httpClient	false
gdbserver	false
DVFilter	false
DHCPv6	false
DVSync	true
syslog	false
WOL	true
vSPC	false
remoteSerialPort	false
rdt	true
cmmds	true
ipfam	false
vvold	false
iofiltervp	true
esxupdate	false
vsanEncryption	false
pvrdma	false
vic-engine	false
stcdClientComm	true
stcdPeerComm	true
settingasd	false
vdafs	false
gstored	false
trusted-infrastructure-kmxsd	false
iwarp-pm	false
ptpd	false
trusted-infrastructure-kmxsa	true
nvmetcp	false
vsphereCCP	false
esxio-orchestrator	false
esxioComm	false
nvmemdns	false
vltd	false
fdm	true
vsanhealth-unicasttest	false

You can see that both the ESXi Host Client and vSphere Web Client allow you to open and close firewall ports. But you can only manage predefined ports. Can we create custom firewall ports? Yes, however, you'll need to use the VMware command-line interface (CLI) for the job, and I'm not sure that's a supported scenario.

## Objective 4.20 – Configure vSphere with Tanzu

Verify prerequisites for enabling vSphere with Tanzu in your vSphere environment. To run container-based workloads natively on vSphere, as a vSphere administrator you enable vSphere clusters as Supervisors. A Supervisor has a Kubernetes layer that allows you to run Kubernetes workloads on vSphere by deploying vSphere Pods, provision Tanzu Kubernetes clusters, and VMs.

A Supervisor can run on either one or three vSphere clusters associated with vSphere Zones. Each vSphere Zone maps to one vSphere cluster, and you can deploy a Supervisor on either one or three zones. A three-zone Supervisor provides greater amount of resources for running your Kubernetes workloads and has high-availability at a vSphere cluster level that protects your workloads against cluster failure. A one-zone Supervisor has host-level high availability provided by vSphere HA and utilizes the resources of only one cluster for running your Kubernetes workloads.

### Tanzu Prerequisites

- **Create and Configure vSphere Clusters** – A Supervisor can run on either one or three vSphere clusters associated with vSphere Zones. Each vSphere Zone maps to one vSphere cluster, and you can deploy a Supervisor on either one or three zones
- **Create Storage Policies** – you must create storage policies that determine the datastore placement of the Supervisor control plane VMs. More here.
- **Choose and Configure the networking stack** – NSX or vSphere Distributed Switch (vDS) networking with a load balancer
- **Create a content library**

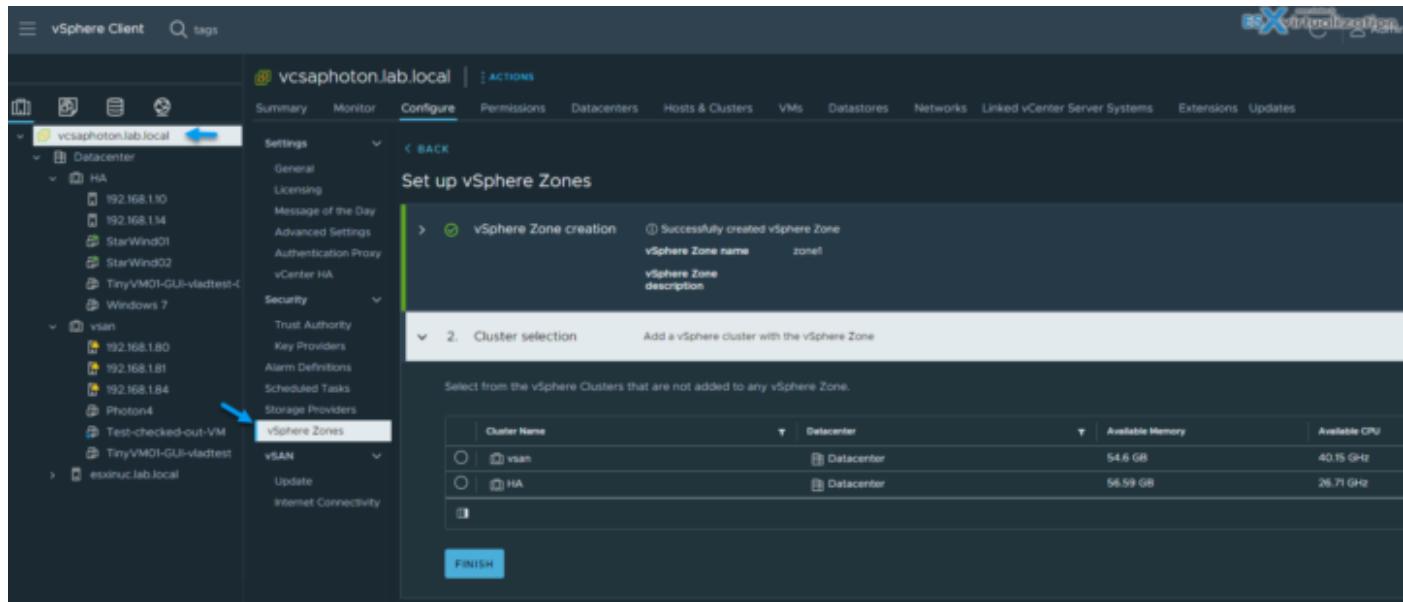
The high-end workflow looks like this:

- ESXi Installation
- VCSA Installation
- Configuring vCenter
- VDS Configuration
- Storage Configuration
- HAProxy Installation

- Enabling workload management
- Create vSphere Namespace, add storage to the namespace ...

Create Zones for Multi-zone Supervisor deployment

Read more [here...](#)



Configure a Supervisor Cluster & Supervisor Namespace

Deploy a workload on the TKC Cluster: <https://github.com/vsphere-tmm/vsphere-with-tanzu-quick-start>

### Configure a vSphere Namespace for Tanzu Kubernetes releases

**Load Balancer** – If you use the vSphere Distributed Switch (VDS) network, you must configure a load balancer to support the network connectivity to workloads from client networks and to load balance traffic between Tanzu Kubernetes clusters. You can configure either NSX Advanced Load Balancer or HAProxy.

- Download the latest version of the VMware HAProxy OVA file from the [VMware-HAProxy site](#).

There is an excellent [quick start guide](#) from VMware which helps to lab this.

## Objective 4.20.1 – Configure a Supervisor Cluster & Supervisor Namespace

Covered within quick start guide.

## Objective 4.20.2 – Configure a Tanzu Kubernetes Grid Cluster

Covered within quick start guide.

## Objective 4.20.3 – Configure vSphere Zones

Covered within quick start guide.

## Objective 4.20.3 – Configure Namespace permissions

Covered within quick start guide.

## Objective 5.1 - Identify resource pools use cases

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. I'm not surprised that the VCP exam has several sections on resource pools and resource management.

VMware vSphere 8 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 8 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 with scalable shares activated recalculates the entitlement for all the workloads running inside the resource pool. Scalable shares are dynamic.

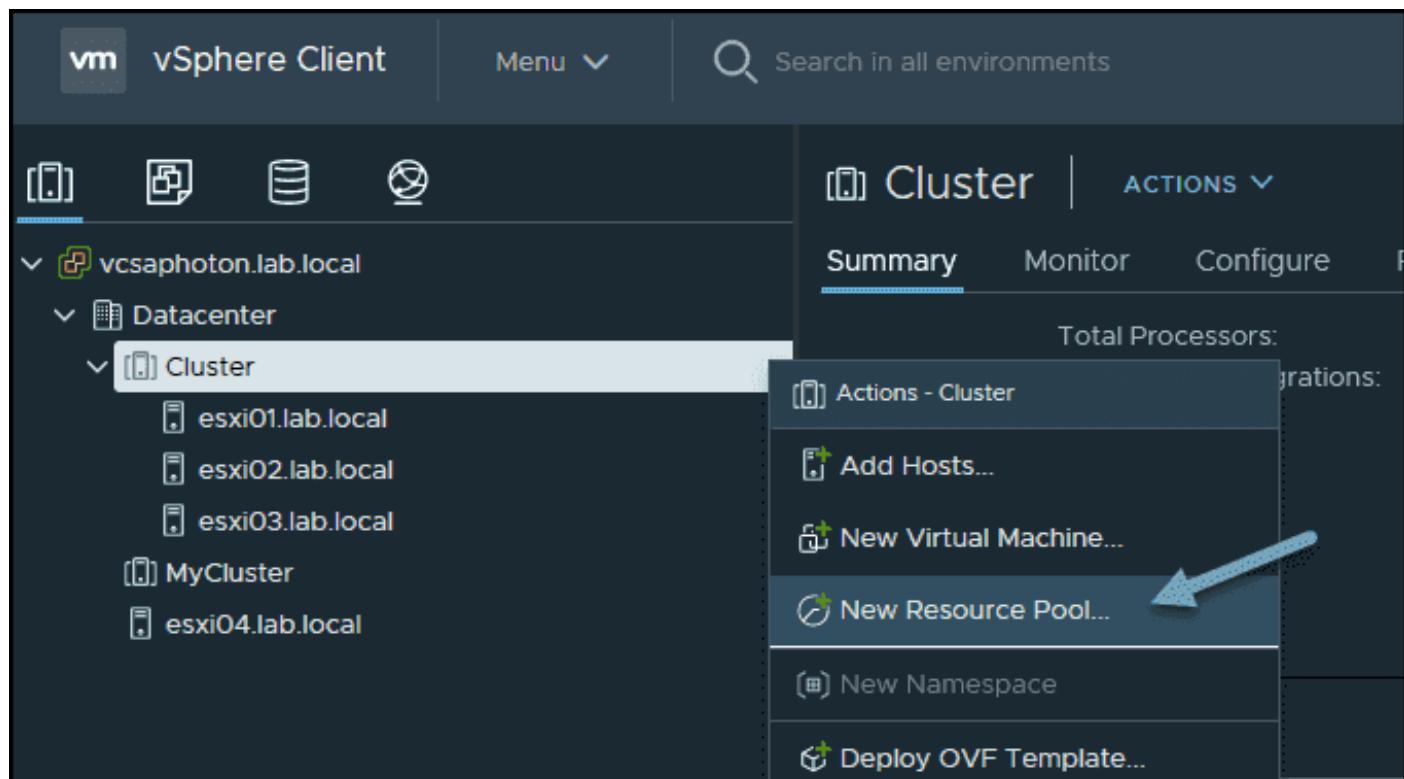
Today's article will be more general and will teach you the basics of resource pools, their usage, examples, and configuration.

vSphere 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 resource pools be created?

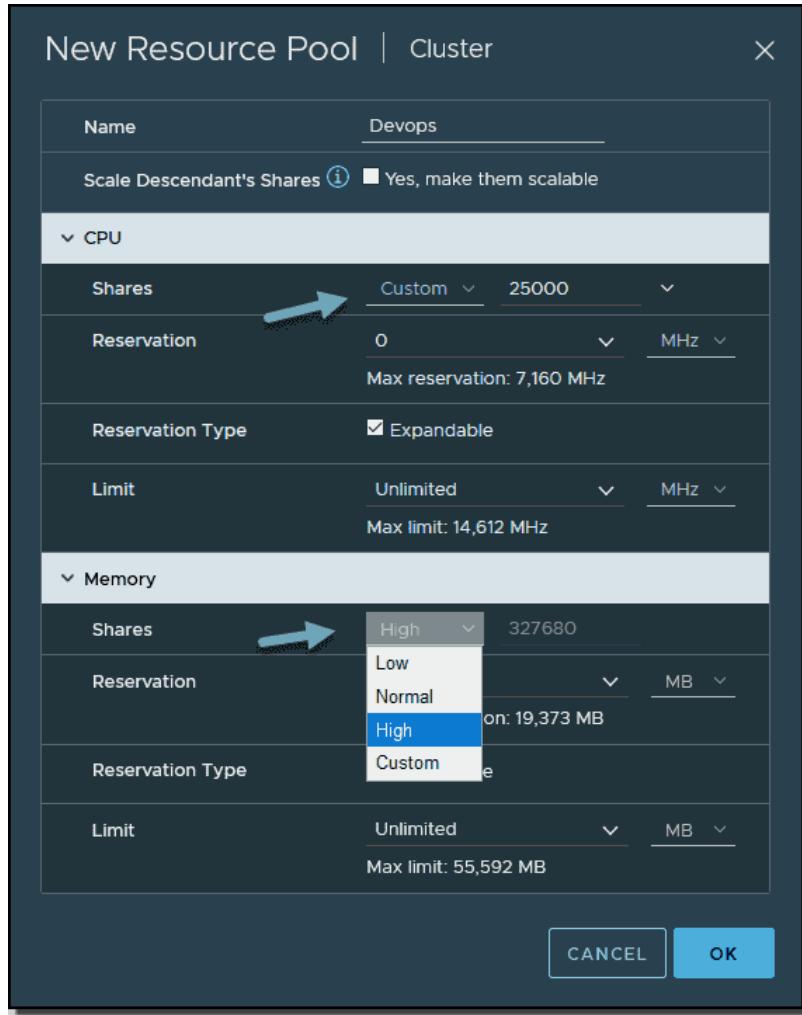
Simply right-click your cluster, and from the menu, choose **New Resource Pool**. Note that resource pools are part of vSphere Enterprise or Enterprise Plus licensing.

Before you try, 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 see this screen. You'll need to give your resource pool a meaningful name first and then 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 environments. For example, if the virtual machine has 2 GHz usage, if you limit it 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.

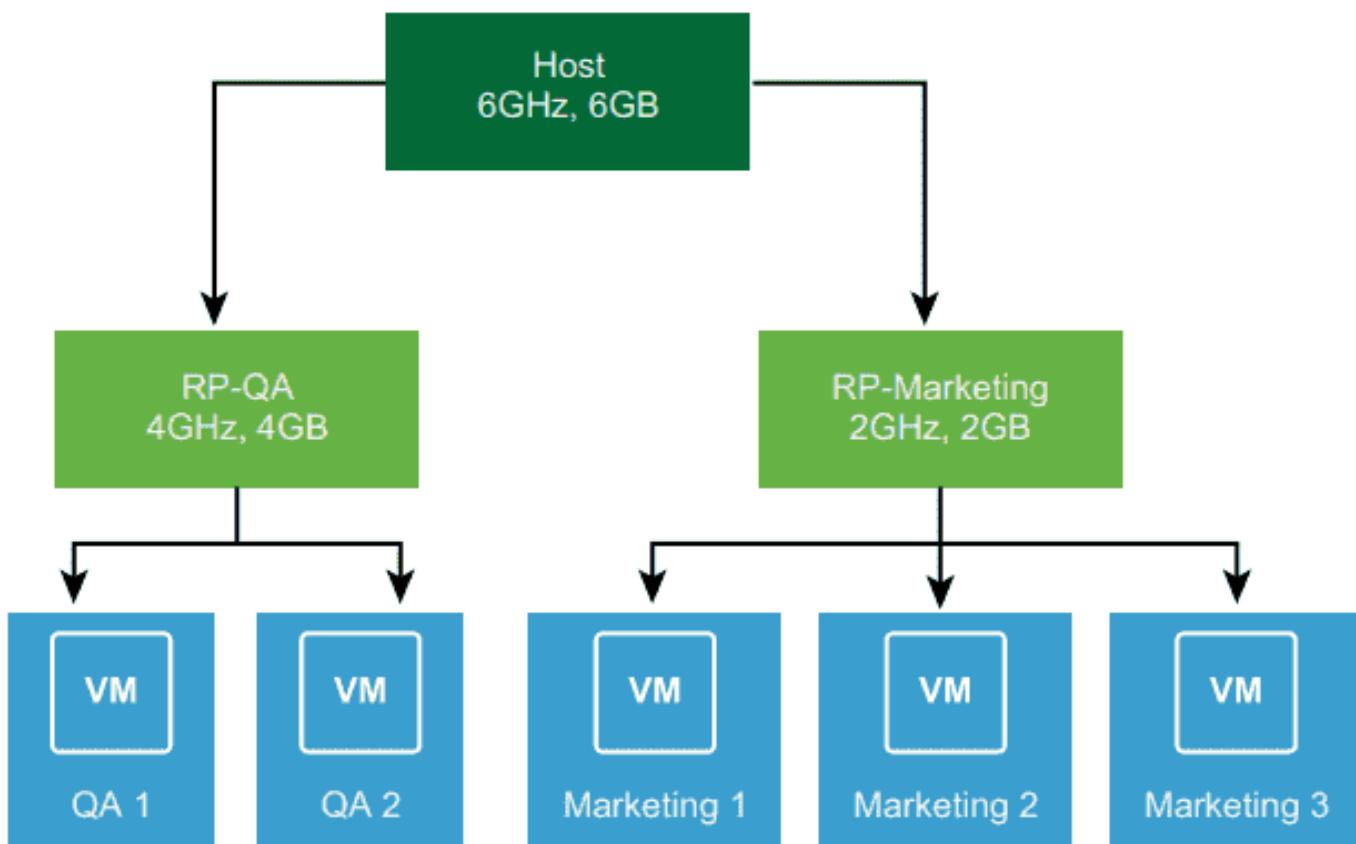
### What are some use cases for using a resource pool?

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. In 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 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.

We looked at VMware documentation, 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.

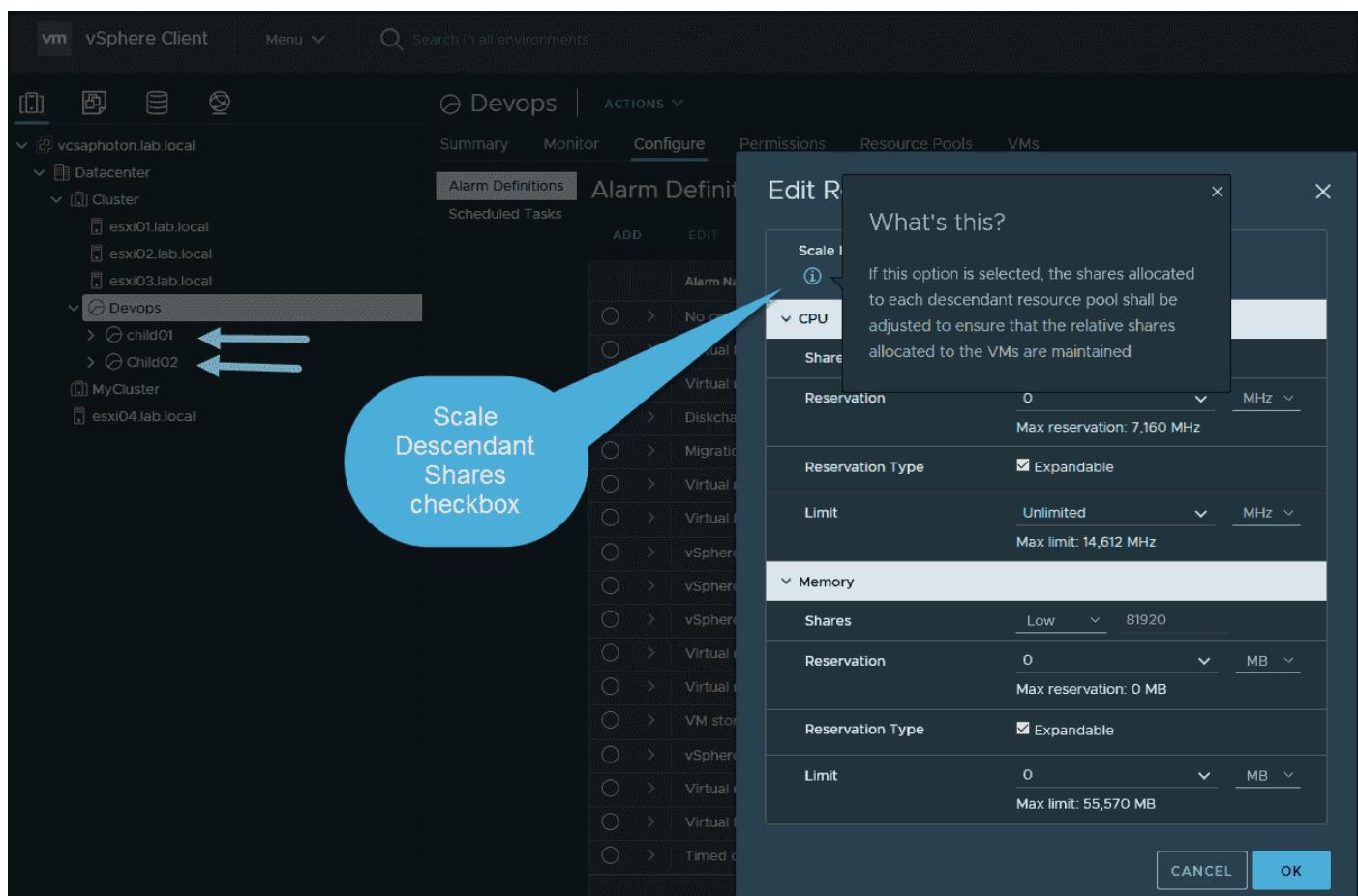
Resource pools are container objects in the vSphere inventory, and they help to create compartments. Each compartment has its own CPU and memory settings set as a percentage of the overall cluster resources. A delegation can be created within vSphere, as resource pools are objects.



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 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 understand better the mechanism behind which vSphere uses to run your VMs and you'll learn with this topic to pass your VCP certification exam.

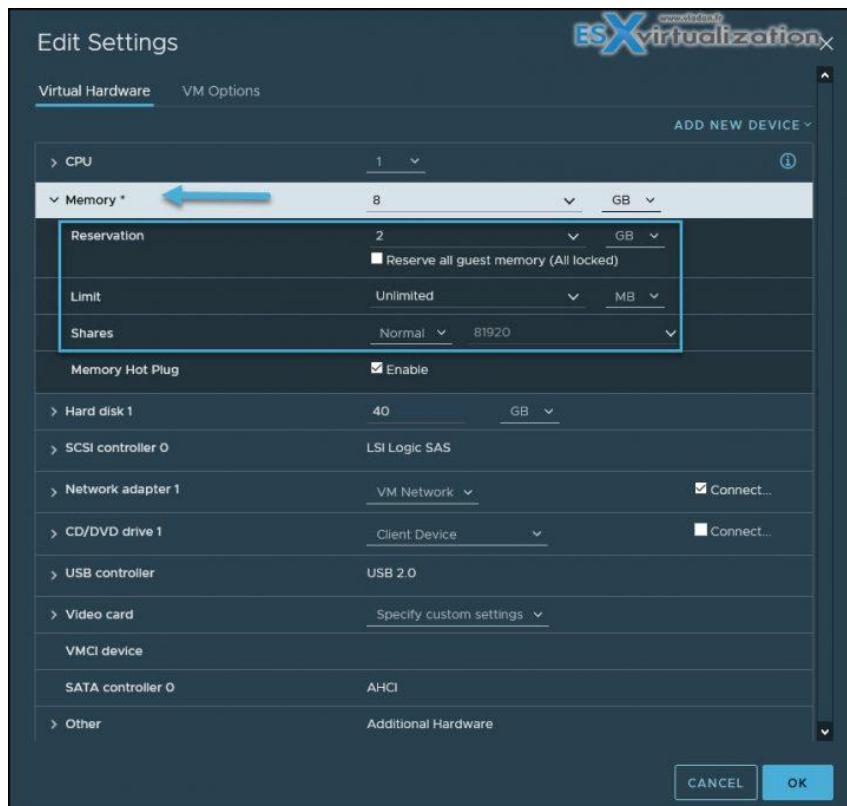
Our VCP-DCV Certification page has all the objectives needed from the VMware Blueprint. Find other chapters on the main page of the guide – [VCP7-DCV Study Guide – VCP-DCV 2021 Certification](#).

## Reservations

**Reservations** is a resource guarantee on CPU or Memory, for a VM. When you set a reservation you basically guarantee that 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 was 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 number 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. What is happening that 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.

The screenshot shows the 'Edit Settings' dialog for a VM named '2008R2'. The 'Virtual Hardware' tab is selected. In the 'CPU' section, there is a dropdown menu for 'Cores per Socket' set to 1, and a dropdown for 'Shares' set to 'Normal' with a value of 1000. A blue arrow points to the 'Shares' field. The 'Reservation' field is set to 1000 MHz. The 'Limit' field is set to 'Unlimited'. The 'CPU Hot Plug' section has a checked checkbox for 'Enable CPU Hot Add'. Below the CPU section, there are sections for 'Hardware virtualization', 'Performance Counters', and 'I/O MMU'. Under 'Memory', the size is set to 8 GB. Under 'Hard disk 1', the size is set to 40 GB. Under 'SCSI controller 0', the controller type is LSI Logic SAS. Under 'Network adapter 1', the network connection is set to 'VM Network' and 'Connect...' is checked. Under 'CD/DVD drive 1', the device type is 'Client Device' and 'Connect...' is checked. Under 'USB controller', the type is USB 2.0. Under 'Video card', the setting is 'Specify custom settings...'. At the bottom right are 'CANCEL' and 'OK' buttons.

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 occurs.

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. It's a shame for this VM....

## Shares

Shares define how much access you get to a resource compared to something else. Every virtual machine has 1000 shares configured pr. vCPU as a default. So you are already using them! All VMs are equal from a hypervisor perspective unless you change the shares and tell it which machines are really more important. What is important to know about shares is that they only are considered in case of contention! If you have available capacity for all machines, it does not help performance to increase the shares on some machines.

Let's have a look at some examples.

Let's say that we have a VM (call this VM a VM01) that has 1000 shares and VM02 has 1000 shares and they are both **competing** for the same physical CPU core. So 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 what we have changed the config so now VM01 has 3000 shares and VM02 has 1000 shares and they are both **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.

When we again, change the config and our VM01 has now 3000 shares and VM02 has 1000 shares and 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 a VMware vCenter Server Appliance (VCSA) and vSphere 8. x environment

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



VCSA is composed of Photon OS, PostgreSQL database, and vCenter server application. Feature parity was a goal for VMware since several vSphere releases. Now it is. 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 login to the management interface of VCSA through port 5480 you get the overview of the health status. You can see if any of the components (CPU, memory, database, storage swap) are in good condition. If any of the mentioned isn't, then you'll see a yellow icon.

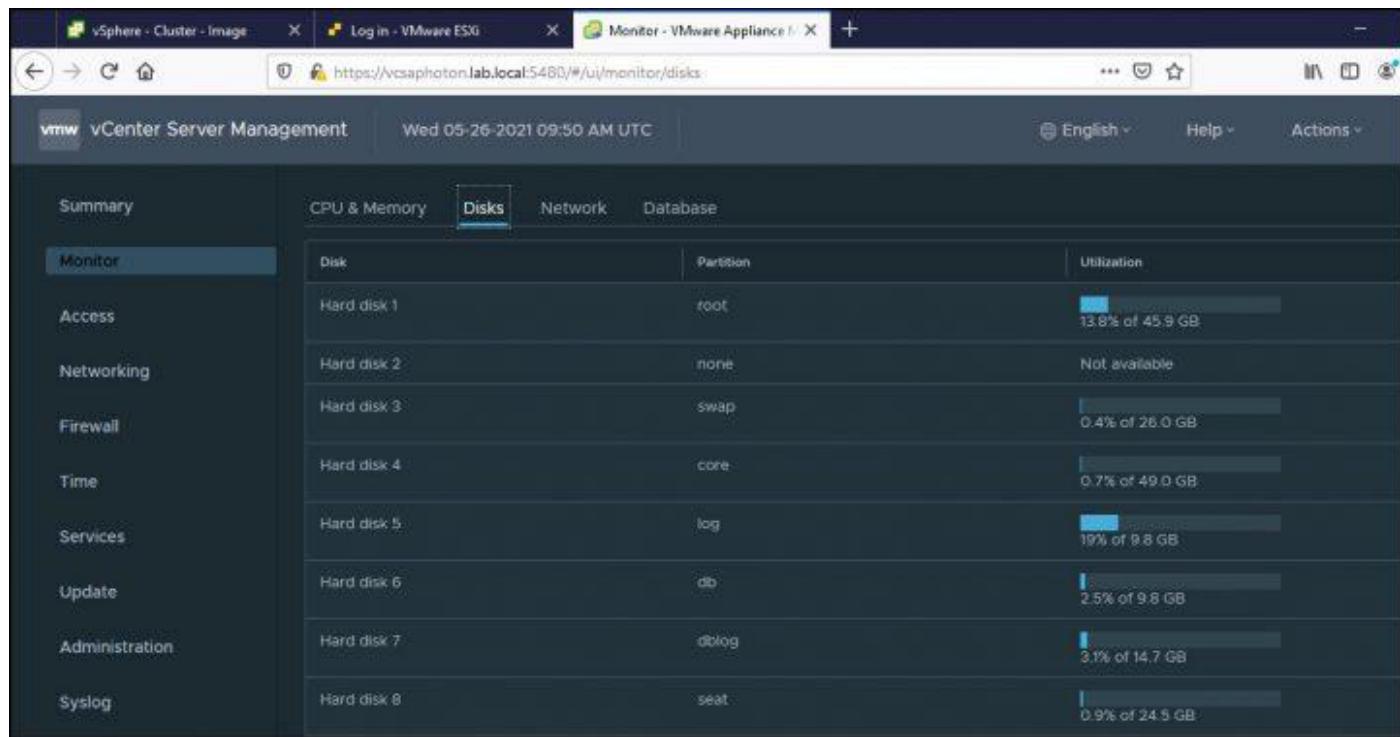
The connection to VCSA management:

[https://ip\\_or\\_fqdn:5480](https://ip_or_fqdn:5480)

The screenshot shows the vCenter Server Management interface at <https://vcsaphoton.lab.local:5480/#/ui/summary>. The left sidebar lists various management categories: Summary (selected), Monitor, Access, Networking, Firewall, Time, Services, Update, Administration, Syslog, and Backup. The main content area displays the 'Health Status' section, which includes a summary table and detailed status for CPU, Memory, Database, Storage, and Swap. The 'Single Sign-On' section shows the domain as 'vsphere.local' and the status as 'Running'. The top right corner features the 'ESX virtualization' logo.

Component	Status
Overall Health	Good (Last checked May 26, 2021, 1:47:58 PM)
CPU	Good
Memory	Good
Database	Good
Storage	Good
Swap	Good

Then when clicking the **Monitor** menu, you'll get full details of each. This single menu item has all the monitoring you need. CPU and Memory, Disks, Network and Database. With the 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.



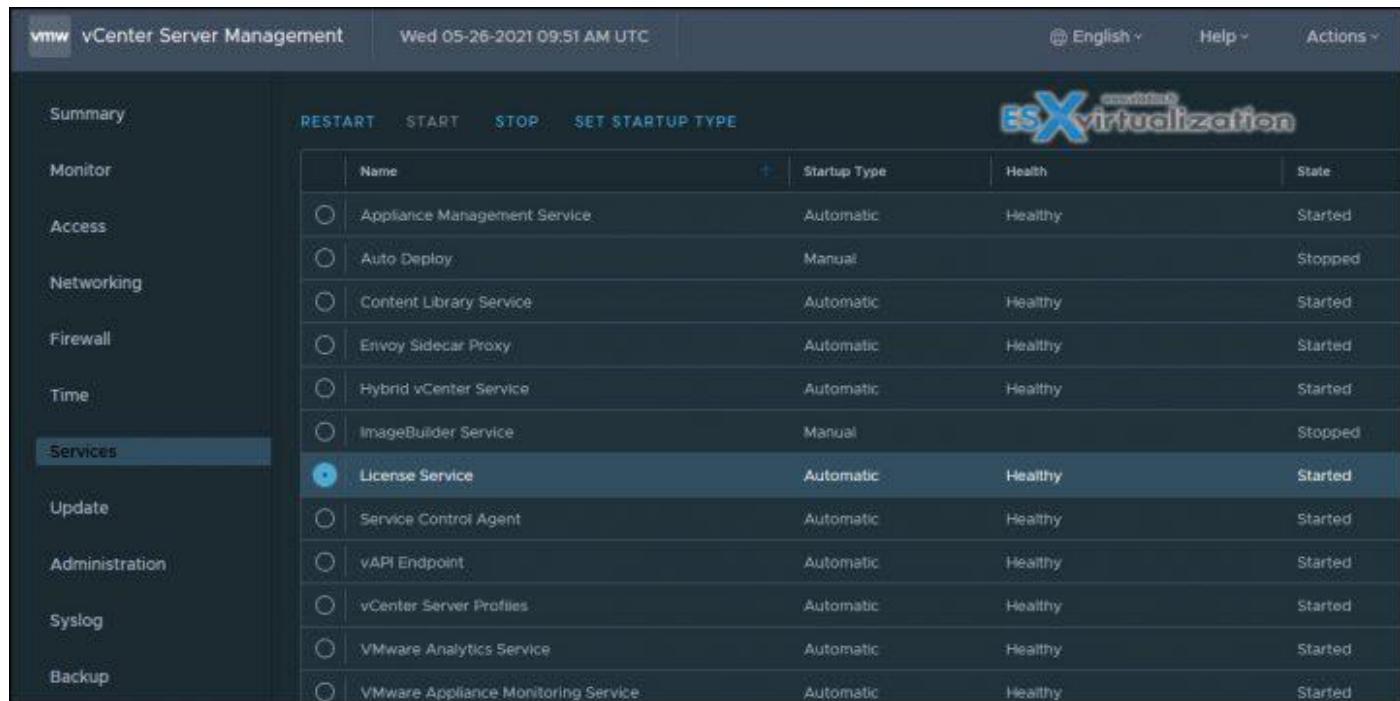
The screenshot shows the vCenter Server Management interface with the 'Monitor' menu selected. The 'Disks' tab is active, displaying a table of disk utilization. The table includes columns for Disk, Partition, and Utilization. A progress bar indicates the utilization percentage for each disk. The utilization values are as follows:

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. You can sort individual columns.

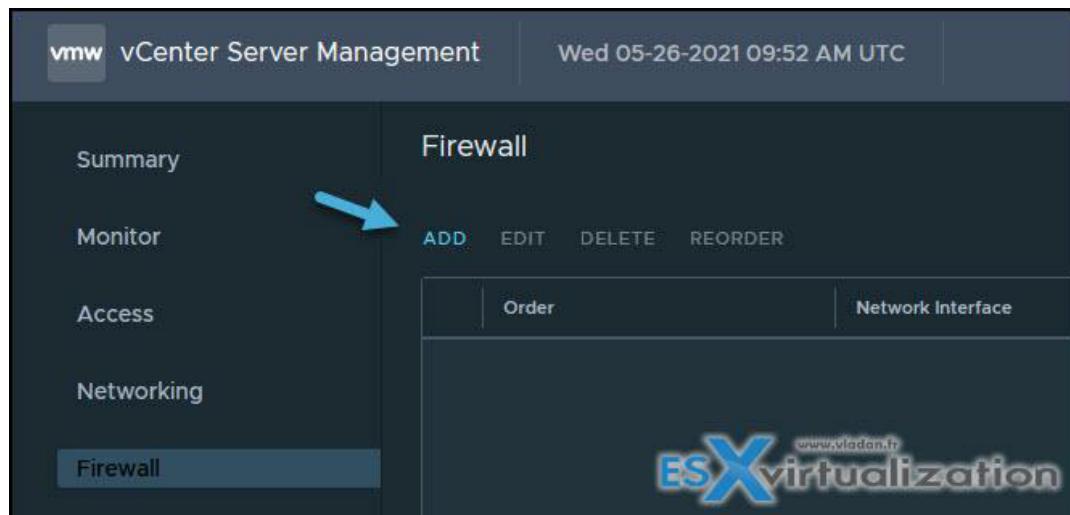


The screenshot shows the vCenter Server Management interface. On the left, there's a sidebar with links like Summary, Monitor, Access, Networking, Firewall, Time, Services (which is selected), Update, Administration, Syslog, and Backup. The main area has tabs for RESTART, START, STOP, and SET STARTUP TYPE. Below these tabs is a table listing various services. The 'License Service' is highlighted with a blue selection bar at the bottom of its row.

	Name	Startup Type	Health	State
<input type="radio"/>	Appliance Management Service	Automatic	Healthy	Started
<input type="radio"/>	Auto Deploy	Manual		Stopped
<input type="radio"/>	Content Library Service	Automatic	Healthy	Started
<input type="radio"/>	Envoy Sidecar Proxy	Automatic	Healthy	Started
<input type="radio"/>	Hybrid vCenter Service	Automatic	Healthy	Started
<input type="radio"/>	ImageBuilder Service	Manual		Stopped
<input checked="" type="radio"/>	License Service	Automatic	Healthy	Started
<input type="radio"/>	Service Control Agent	Automatic	Healthy	Started
<input type="radio"/>	vAPI Endpoint	Automatic	Healthy	Started
<input type="radio"/>	vCenter Server Profiles	Automatic	Healthy	Started
<input type="radio"/>	VMware Analytics Service	Automatic	Healthy	Started
<input type="radio"/>	VMware Appliance Monitoring Service	Automatic	Healthy	Started

## Firewall Management

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



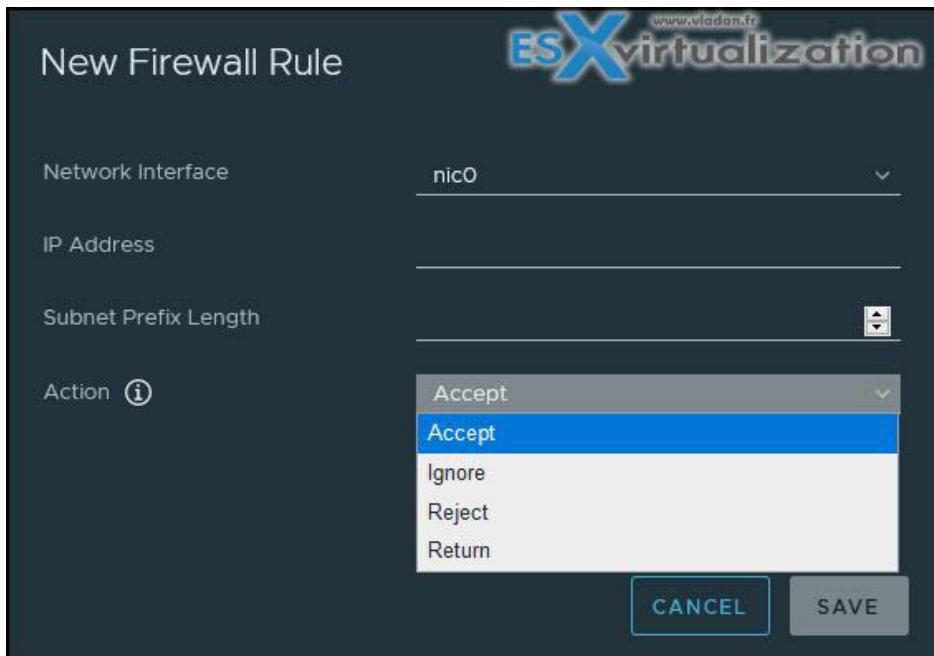
The screenshot shows the vCenter Server Management interface with the Firewall tab selected. On the left, there's a sidebar with links like Summary, Monitor, Access, Networking, and Firewall (which is selected). The main area has tabs for ADD, EDIT, DELETE, and REORDER. Below these tabs is a table with columns for Order and Network Interface. An arrow points to the 'ADD' button.

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

Here are the details. You have the choice of:

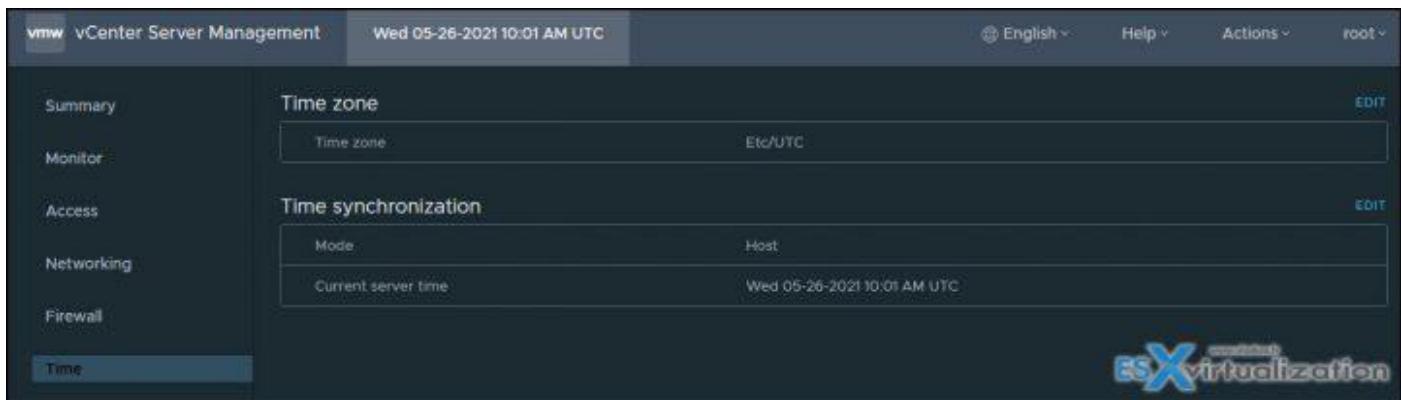
- **Network Interface** – a drop-down menu allowing you to choose the vNIC you want to add the rule for.
- **IP address** – address from which you want to allow/block traffic
- **Subnet Prefix Length** – subnet details
- **Action** – accept or refuse traffic

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 resource monitoring tools

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 periodic, or you can intelligently automate workload management based on current conditions.

### vSphere client performance charts

The built-in charts in the vSphere 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.

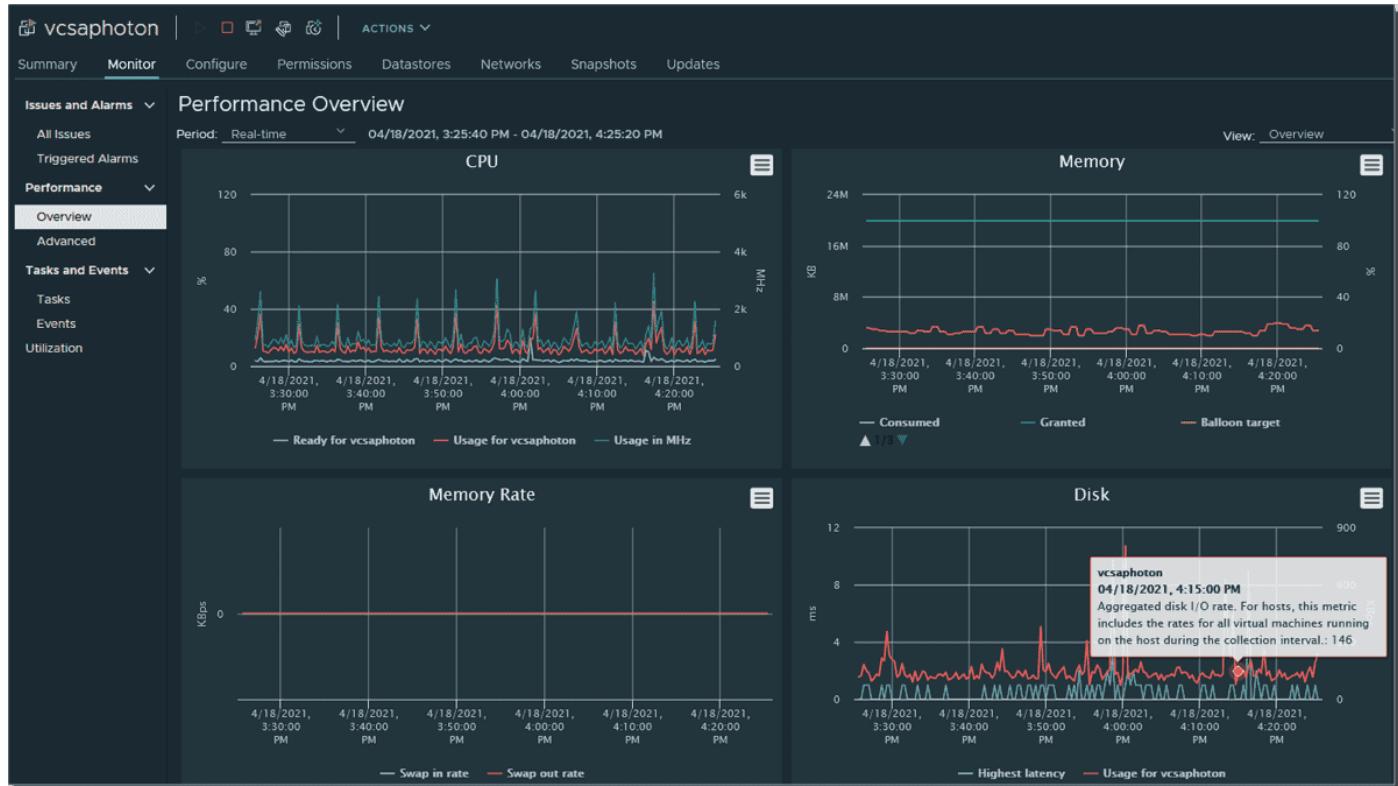
**Pie chart**—Shows metrics for a single object, such that each slice represents a category or child object. An example here would be a pie chart that shows the amount of storage space occupied by each virtual machine or by each file type.

**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 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 performance charts

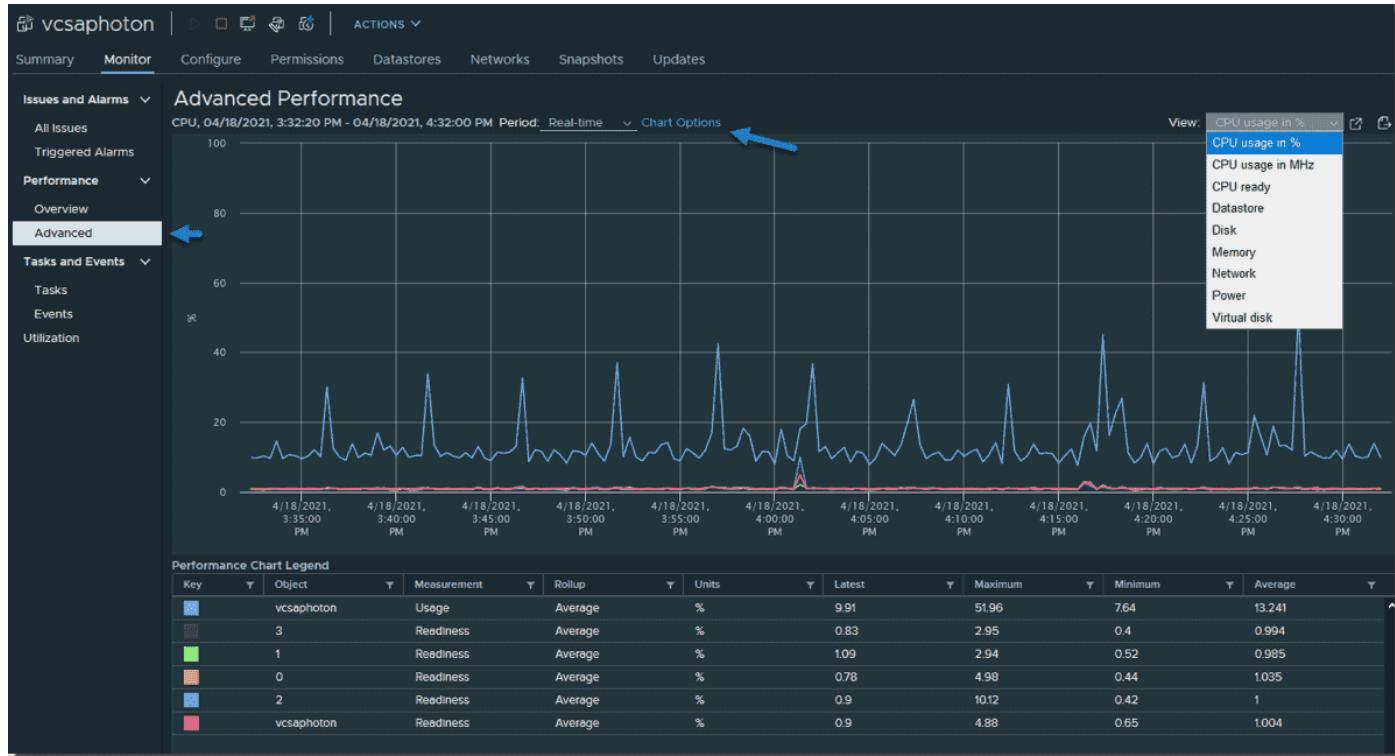
## Advanced performance charts

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.



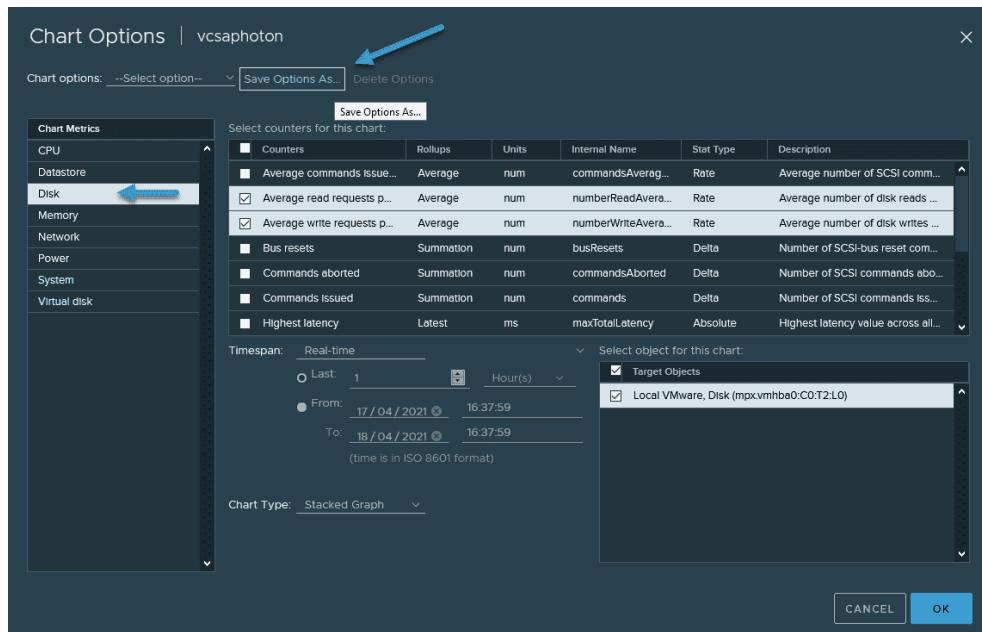
### vSphere advanced performance charts

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.

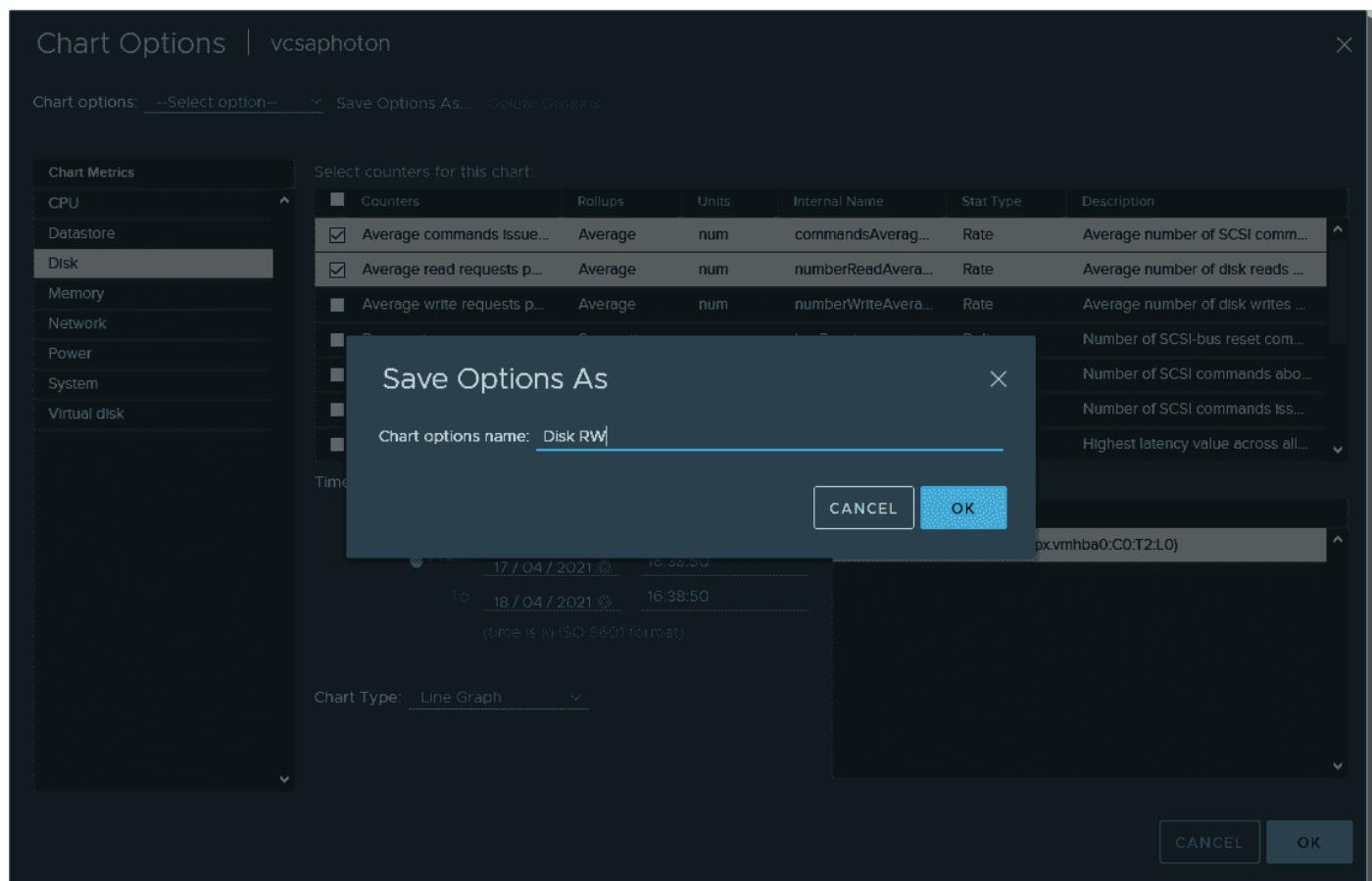


Select chart metrics and click the Save Options As button

vSphere 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.

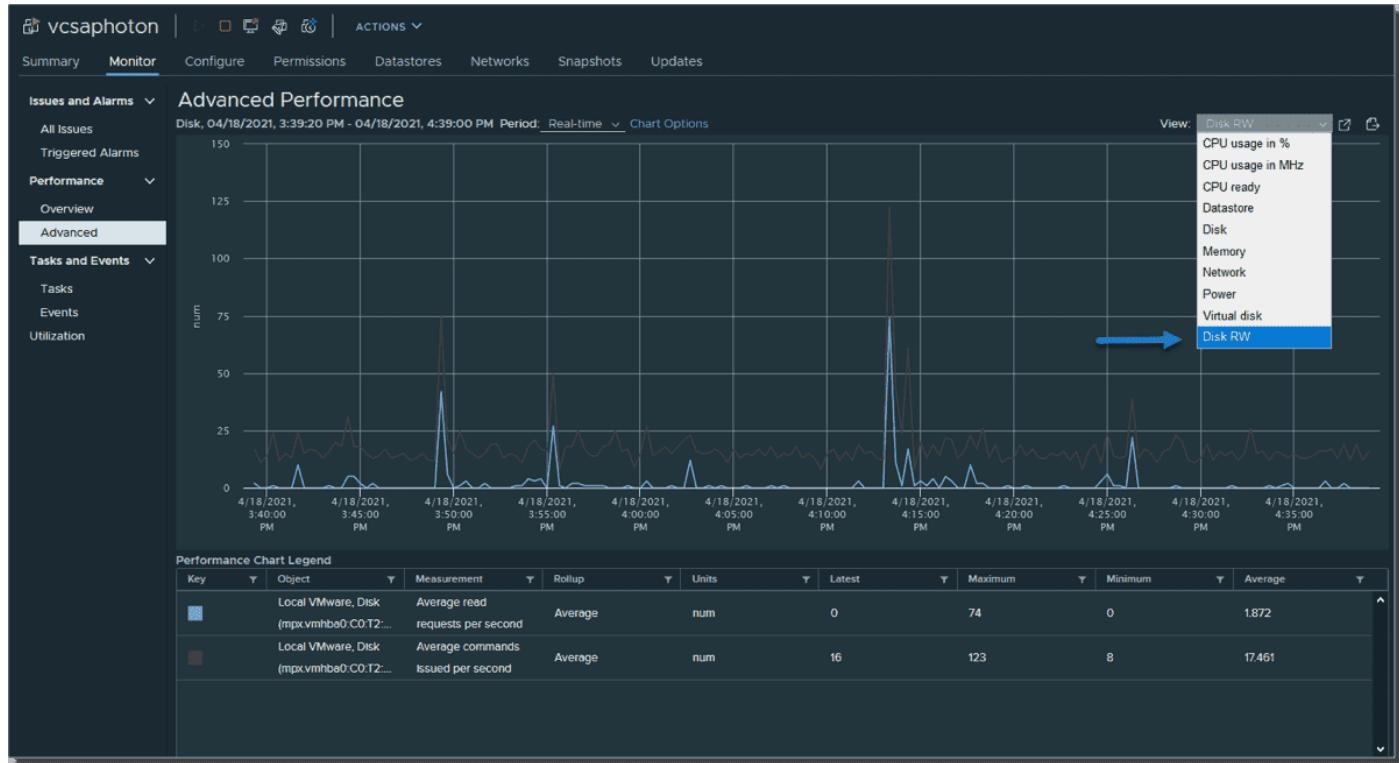
Concerning memory utilization, one of the following applies. Either memory is considered as a guest physical memory, which is the virtual memory of the hypervisor presented to the guest as physical memory.

Put 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-hand side.



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 manipulating the vSphere 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 (NIOC)

With Network I/O control (NIOC), you can adjust the bandwidth of your vSphere 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 Distributed vSwitch (vDS) is version 8 of vDS. Version 8 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.

The screenshot shows the vSphere Client interface with the following details:

- Left sidebar:** Shows the vCenter server "vcsaphoton.lab.local" and its Datacenter, which contains several network profiles: dd, starwindiscsi, starwindsync, VM Network, VM Network 2, and the selected DSwitch.
- Top navigation:** Includes "vSphere Client", "Menu", and a search bar.
- Main content area:** Title "DSwitch" with "ACTIONS" dropdown. Below it are tabs: Summary, Monitor, Configure (selected), Permissions, Ports, Hosts, VMs, Networks.
- Configure Tab Content:**
  - Properties Sub-tab:** Contains sections for General, Advanced, Resource Allocation, Discovery protocol, and Administrator contact.
  - General Section:** Displays Name (DSwitch), Manufacturer (VMware, Inc.), Version (7.0.0), Number of uplinks (4), Number of ports (20), and Network I/O Control (Enabled).
  - A blue arrow points to the "Version" field in the General section.

## 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**.

Dswitch2 - Upgrade Distributed Switch

**1 Configure upgrade**

**2 Check compatibility**

**3 Ready to complete**

**Configure upgrade**  
Specify distributed switch version for upgrade.

7.0.0 - ESXi 7.0 and later  
 6.6.0 - ESXi 6.7 and later

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

Features per version **ⓘ**

CANCEL BACK NEXT

## 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.

### Where should you enable NIOC?

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

vSphere Client

DSwitch

ACTIONS ▾

- Distributed Port Group
- Add and Manage Hosts...
- Edit Notes...
- Upgrade
- Settings
- Move To...
- Rename....
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Delete

DSwitch  
VMware, Inc.  
7.0.0

Ports Hosts VMs Networks

Summary Monitor

Properties

Topology

LACP

Private VLAN

NetFlow

Port Mirroring

Health Check

Resource Allocation

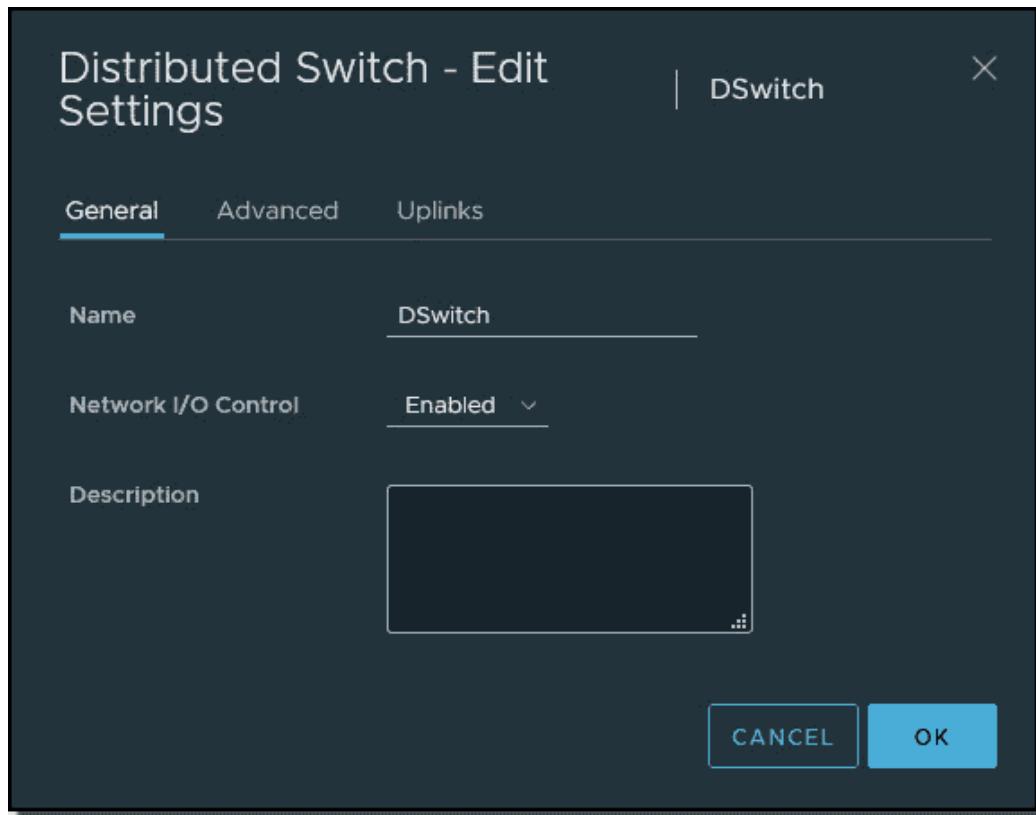
System traffic

Network resource p

Alarm Definitions

## 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

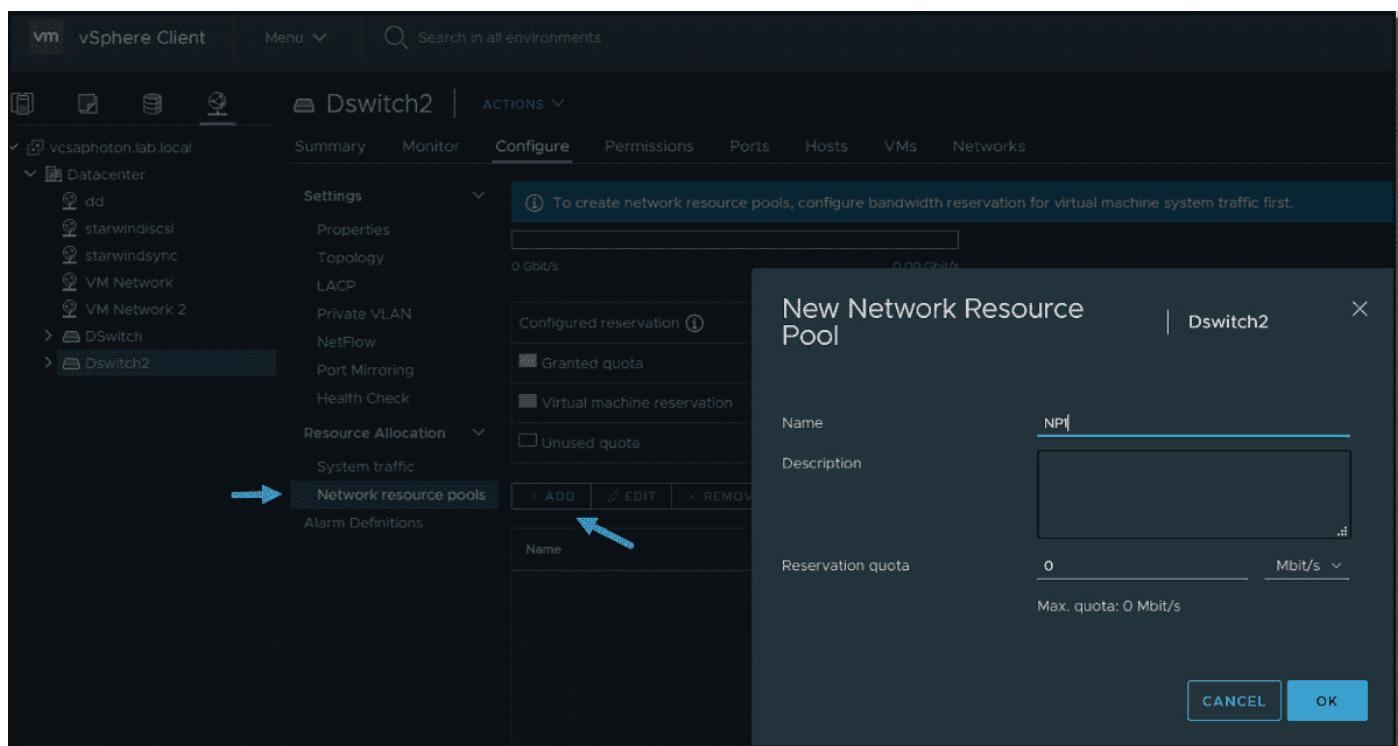
The allocation parameters for the different traffic types are:

- **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 5.5 - Configure Storage I/O Control (SIOC)

With VMware vSphere, 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.

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 too.

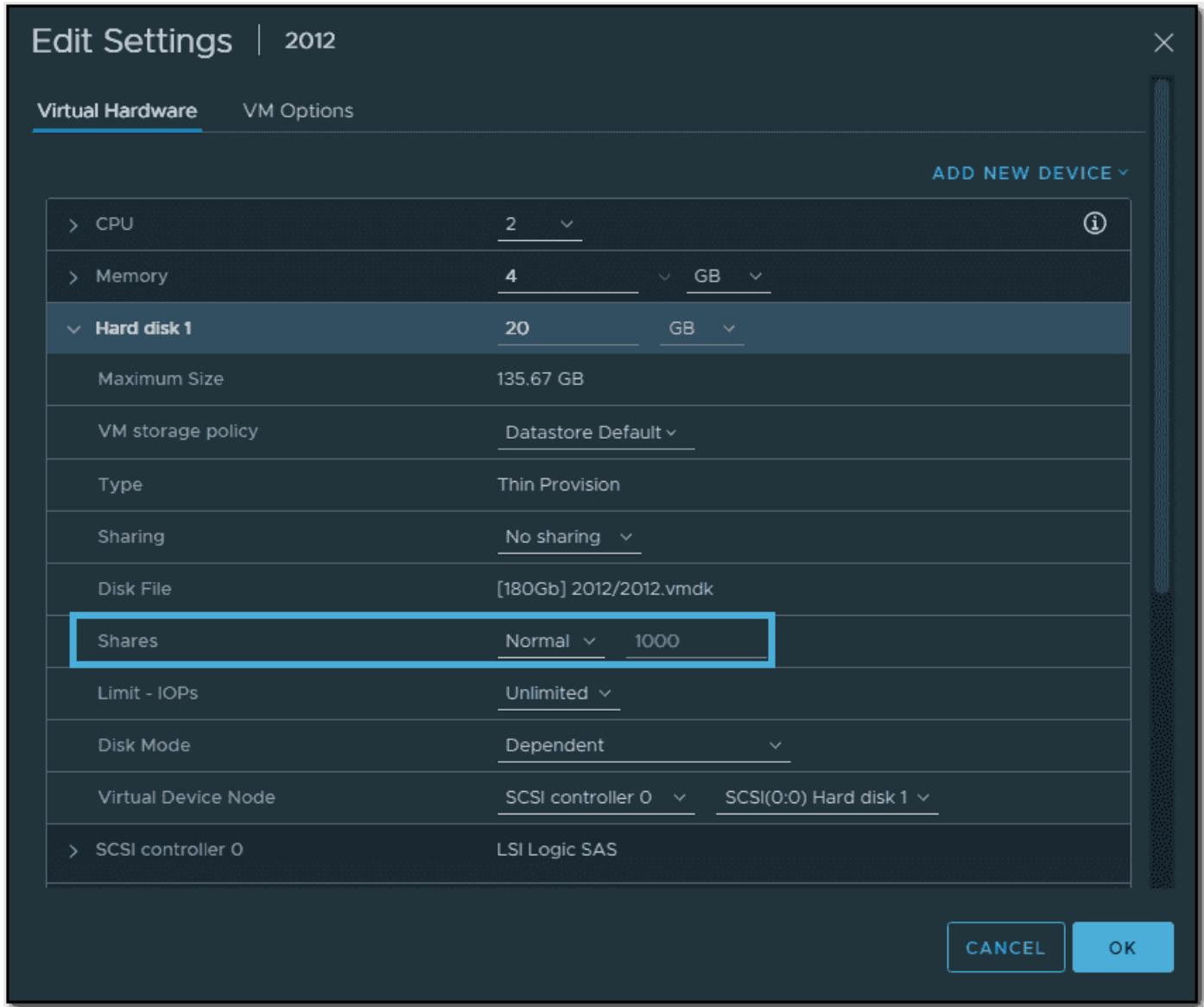
IOC allows you to prevent a single virtual machine from monopolizing I/O consumption on your datastore. SIOC is able to ensure an equal (or fair) distribution of I/Os between VMs when contention occurs. SIOC is not triggered during normal operations. There is a threshold that acts as a trigger for the 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 any 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.**

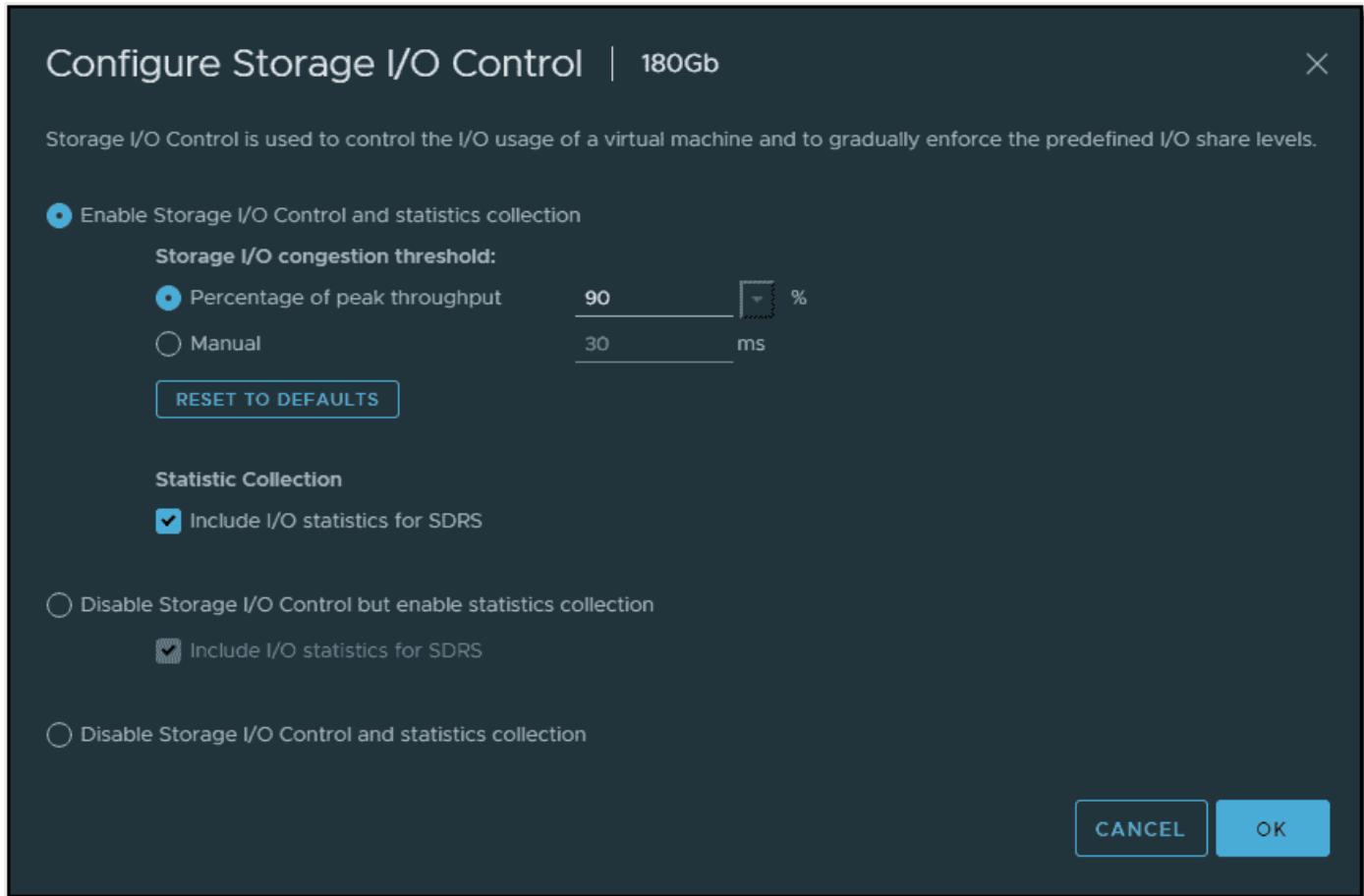
The screenshot shows the vSphere Client interface for managing a datastore. The left sidebar lists various management options like Alarm Definitions, Scheduled Tasks, General, Device Backing, Connectivity and Multipathing, Hardware Acceleration, and Capability sets. The main panel is titled '180Gb' and has tabs for Summary, Monitor, Configure (which is selected), Permissions, Files, Hosts, and VMs. The 'Configure' tab is further divided into sections: Properties, Capacity, Datastore Capabilities, and Space Reclamation. The 'Space Reclamation' section contains a note: 'Enabled at Low priority: Deleted or unmapped blocks are reclaimed on the LUN at low priority'. There are 'REFRESH' and 'INCREASE...' buttons at the top right of the main panel.

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.

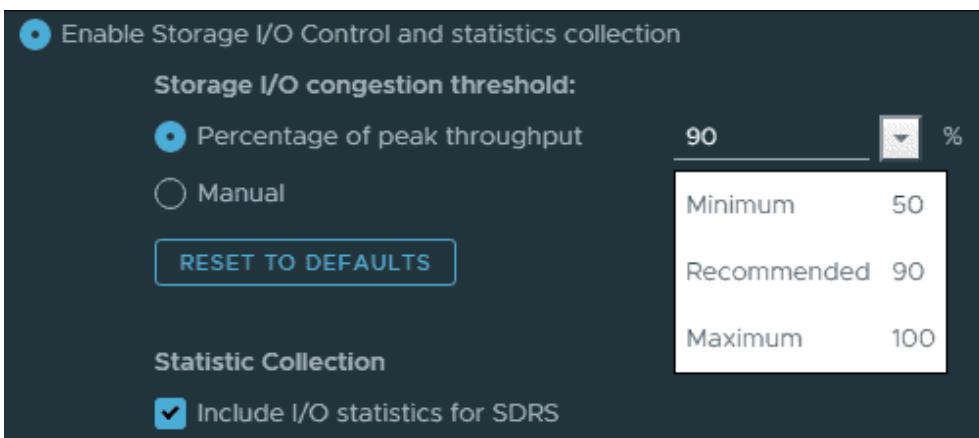
By default, the **Disable Storage I/O Control and statistics collection** option is active and selected. So you can go ahead and select the **Enable Storage I/O Control and statistics collection** radio button.



### 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.

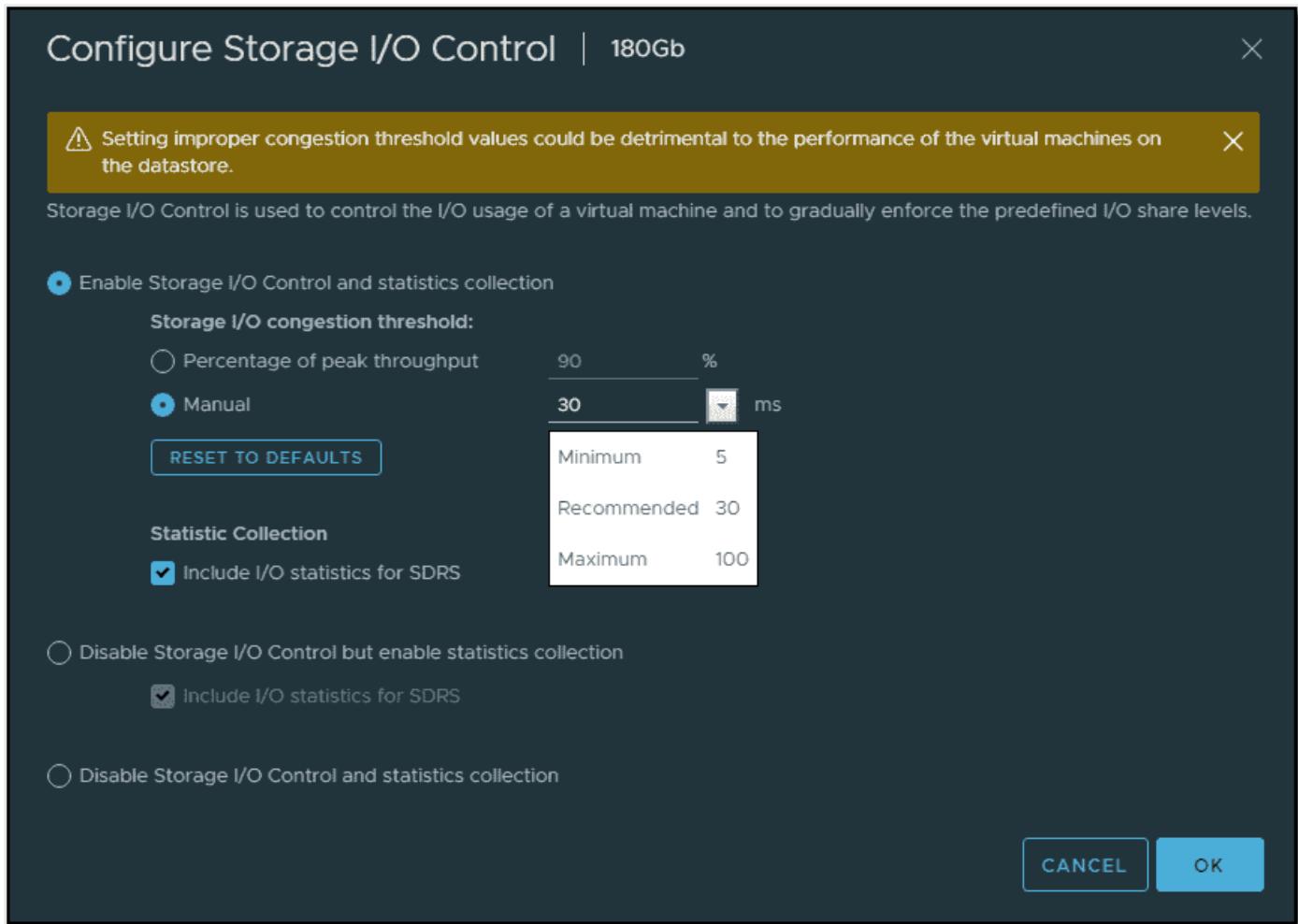
Here is the view.



### SIOC recommended values

There is also the option to enter another number, but you'll get a nice warning message saying that «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.

Name	Disk	Datastore	Limit - IOPS	Shares	Shares Value
vCLS (2)	Hard disk 1	vSEN Datastore	Unlimited	Normal	1000
vCLS (3)	Hard disk 1	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 1	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 2	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 3	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi02.lab.l...	Hard disk 4	vSEN Datastore	Unlimited	Normal	1000
vCLS (4)	Hard disk 1	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi03.lab.l...	Hard disk 1	vSEN Datastore	Unlimited	Normal	1000
Z-VRA-esxi03.lab.l...	Hard disk 2	vSEN Datastore	Unlimited	Normal	1000

Check VMs and their shares value at the cluster level

## Objective 5.6 - Configure a virtual machine port group to be offloaded to a data processing unit (DPU)

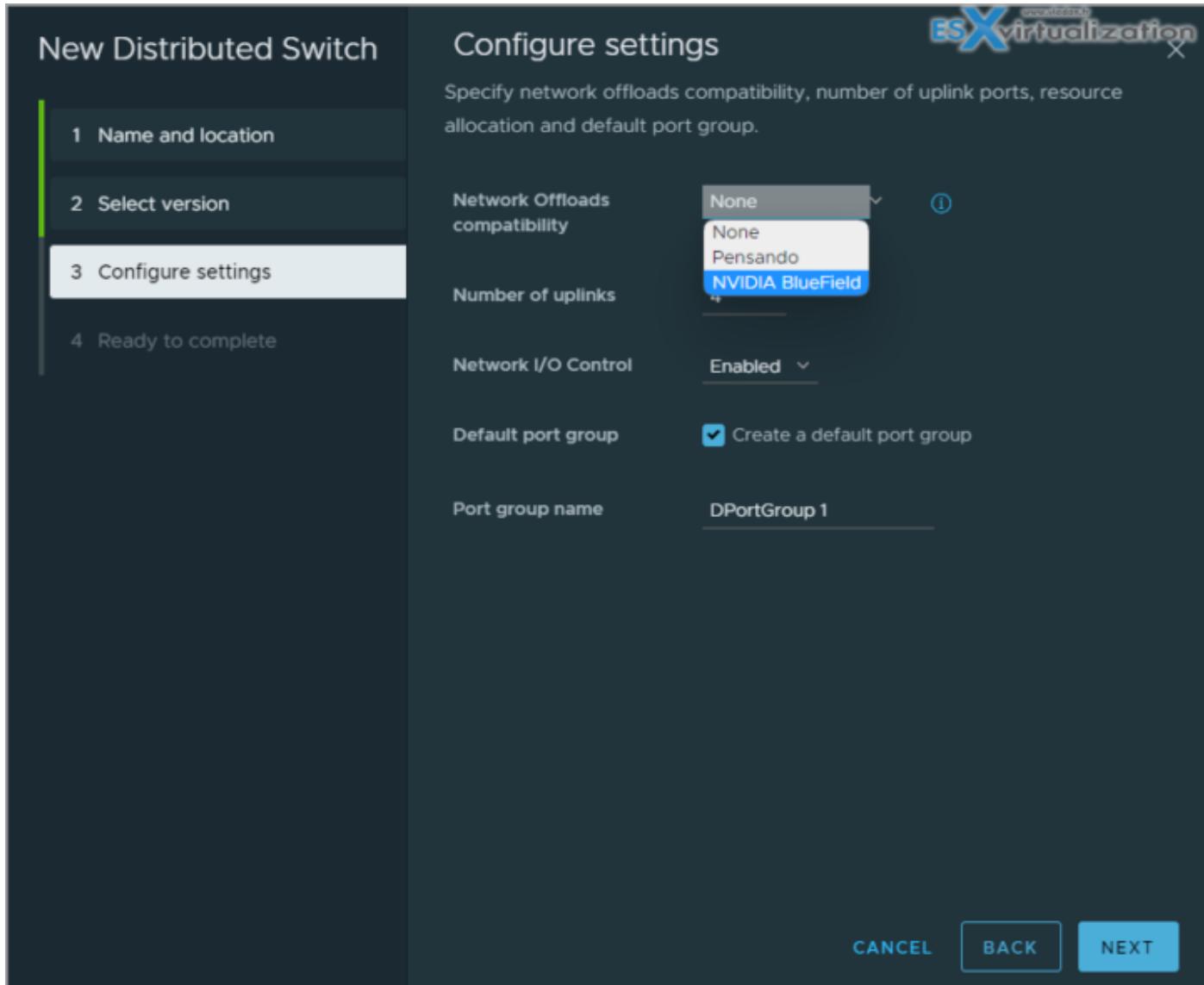
In vSphere 8, the vSphere Distributed Services Engine(vDSE) introduces virtual infrastructure as a distributed architecture with the addition of data processing units (DPUs) also known as SmartNic that enable offloading infrastructure functions from the host or server CPUs to data processing units (DPUs). Starting with vSphere 8.0, VMware moves functionality that runs on the core CPU complex to the DPU CPU complex.

vSphere Distributed Services Engine offloads and accelerates infrastructure functions on the DPU by introducing a VMware vSphere Distributed Switch on the DPU and VMware NSX Networking and Observability, which allows to proactively monitor, identify, and mitigate network infrastructure bottlenecks without complex network taps. The DPU becomes a new control point to scale infrastructure functions and enables security controls that are agentless and decoupled from the workload domain.

vSphere Distributed Services Engine **does not** require a separate ESXi license.

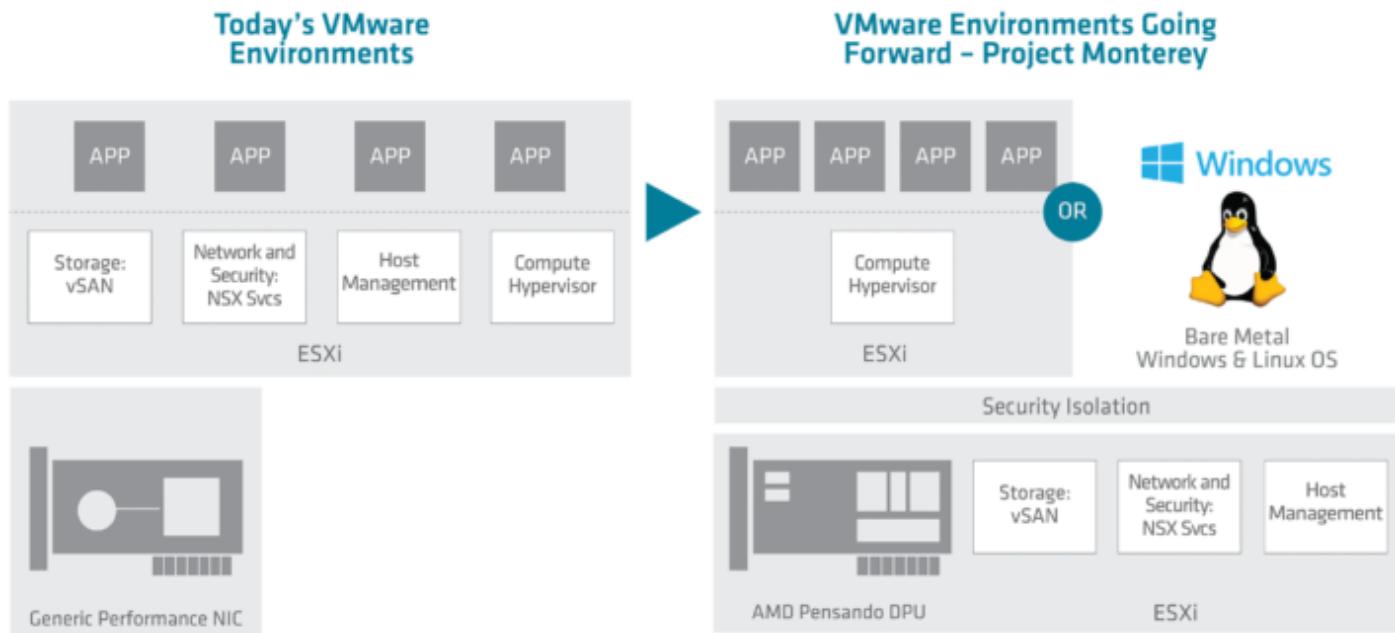
You can offload the networking functionality from the ESXi host to DPU for better performance. vSphere Distributed Switch backed by ESXi on DPU supports the following modes:

- Non-offloading mode before NSX is enabled: The DPU is used as a traditional NIC.
- Offloading mode after NSX is enabled: Traffic forwarding logic is offloaded from the ESXi host to the vSphere Distributed Switch backed by the DPU.



The Pensando Distributed Services Card, powered by the industry's most advanced data processing unit (DPU)<sup>1</sup> will be one of the first DPU solutions to support VMware vSphere® 8. The VMware vSphere Distributed Services Engine (formerly known as Project Monterey) and AMD Pensando DPUs can help customers reduce operational costs by unifying workload management, improving performance by freeing up CPU resources, and providing an added layer of security by isolating infrastructure services from server tenant workloads.

Screenshot from AMD



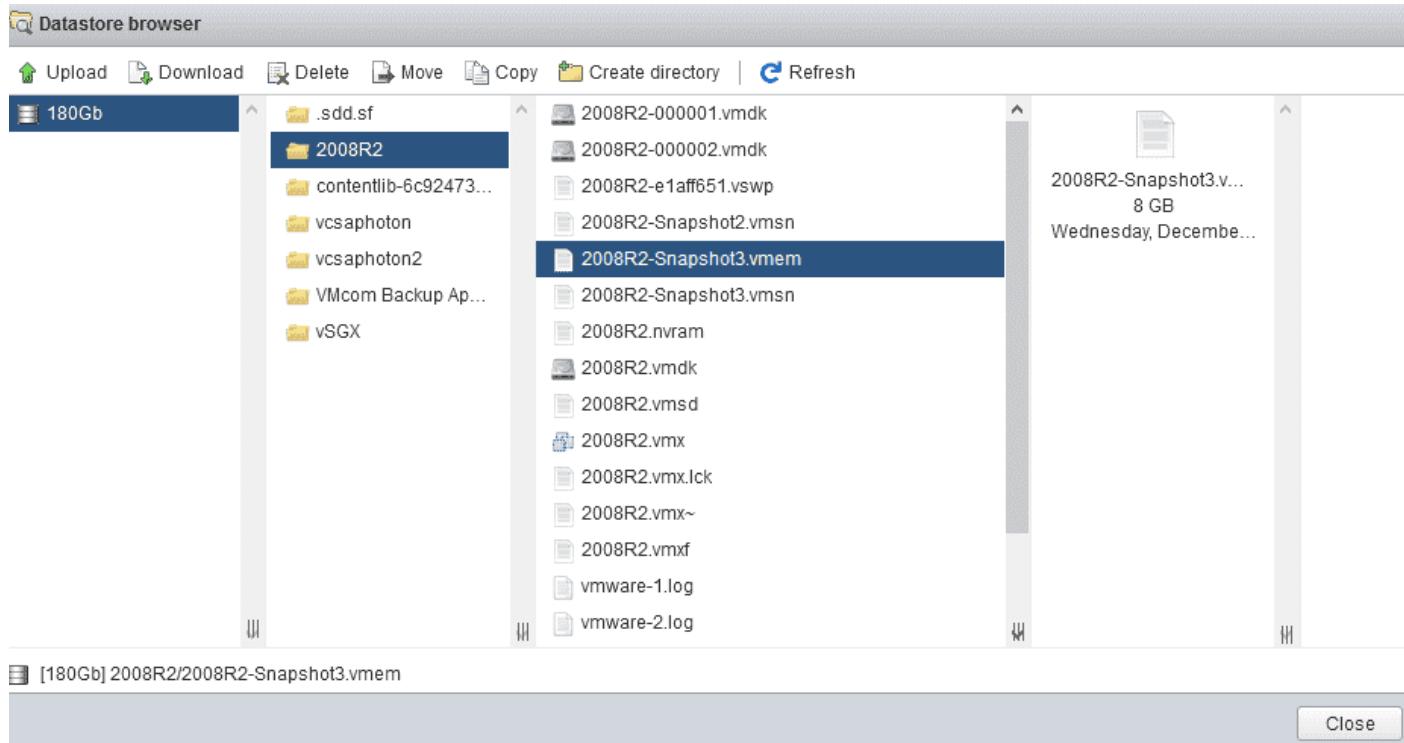
## Objective 5.7 - Explain the performance impact of maintaining virtual machine snapshots

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.

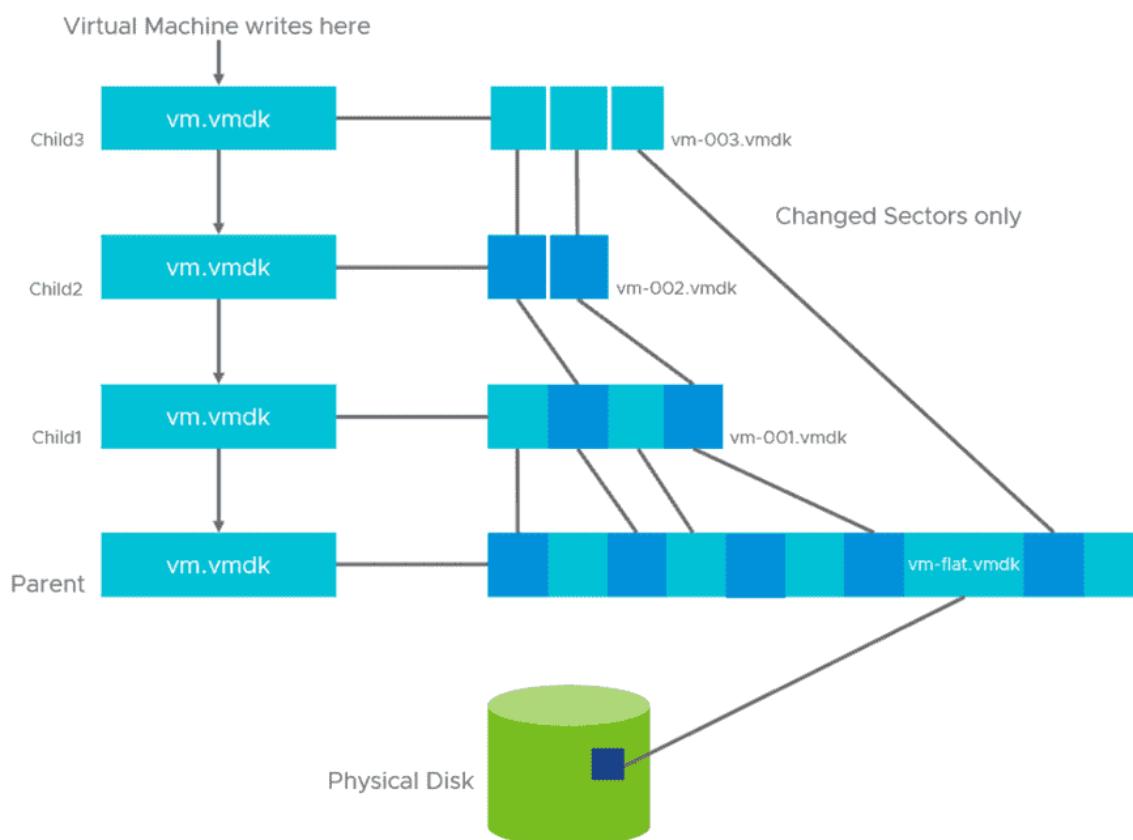
### What files are generated by a snapshot?

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.

Backup VMware, Hyper-V - Easy to use - Restore VMs, files or apps - Free forever

[Download FREE Nakivo Backup & Replication now!](#) Ad

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. On the left, there's a sidebar with icons for Home, Hosts & Clusters, VMs, Datastores, Networks, and Updates. The 'Datacenter' icon is highlighted with a blue arrow. At the top, there's a search bar and a 'Menu' dropdown. The main area is titled 'Datacenter' and has tabs for Summary, Monitor, Configure, Permissions, Hosts & Clusters, VMs, Datastores, Networks, and Updates. The 'VMs' tab is selected and highlighted with a blue arrow. Below this, there are tabs for Virtual Machines, VM Templates, vApps, and VM Folders. The main content area displays a table of VMs with columns for Name, State, Status, Provisioned Space, Used Space, Host CPU, Host Mem, and Needs Consolidation. The 'Needs Consolidation' column is currently empty. On the far right, there's a vertical sidebar with various filter options like Host Mem, Guest Mem - %, Guest OS, Compatibility, Memory Size, and Reservation, each with a checkbox. A blue arrow points to the 'Needs Consolidation' checkbox in this sidebar.

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.

This screenshot is similar to the one above, showing the vSphere Client interface. The 'Datacenters' icon in the sidebar is highlighted with a blue arrow. The 'VMs' tab is selected and highlighted with a blue arrow. The main content area displays a table of VMs with columns for Name, State, Status, Provisioned Space, Used Space, Host CPU, Host Mem, and Needs Consolidation. The 'Needs Consolidation' column is now populated with values like 'Not Required' for most VMs. A blue arrow points to the 'Needs Consolidation' column header.

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.

As a second case, we could say that with native snapshot support (fast file cloning), where you can create VM-linked clones (only for VMs with virtual hardware 9 and higher), the VMs use native snapshot disks instead of VMware redo logs.

## **Objective 5.8 - Use Update Planner to identify opportunities to update VMware vCenter**

At first, within the vSphere web client, you'll see if there are new updates for vCenter servers and get the notifications. Previously you had to go to the VAMI UI to check for updates and

do the update/upgrade of vCSA there, manually. And also check whether, if you upgrade, you won't break the compatibility with other VMware products.

Now with vCenter Server 8, you'll be able to run **What IF scenario with pre-checks** to show you whether your current environment would be affected by the upgrade and show you the individual applications which need to be upgraded first, and to which version! You'll be able to do pre-upgrade checks against a target vCenter server before the actual upgrade process starts, and see whether Yes or No you have an interoperability issue.

Let's say you have an environment with vRA, vRO, Log Insight and you do a pre-upgrade check which will show you that you must first upgrade your vRA to the x.xx version to ensure that the interoperability between the different VMware products within this environment will be assured. That all the products will continue to talk to each other after you upgrade your vCenter.

This is quite a revolutionary, as previously for each upgrade you must go to [VMware Product Interoperability Matrices](#) page and make sure about that .... manually. This is a lengthy process where you can also make errors.

To give you an idea, here is a screenshot from the lab, when selecting **vCenter server > Updates > Update Planner**.

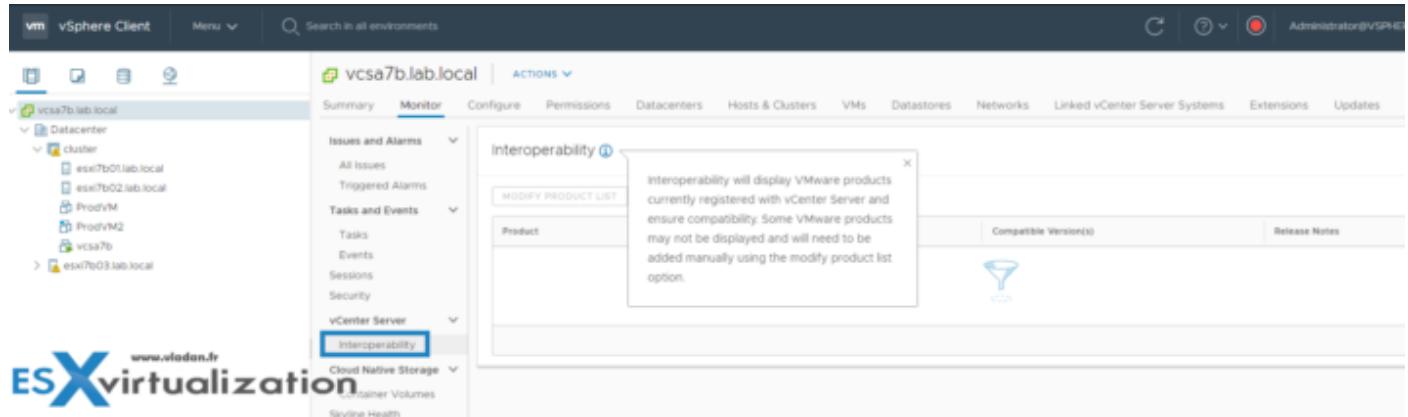
The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and "Search in all environments". The left sidebar shows "vCenter Servers" with "vcsa7b.lab.local" selected. The main content area has a header "vCenter Server" with "Update Planner" highlighted. Below it is a table titled "Update Planner" with columns: Release Date, Version, Build, Type, Severity, and Reboot Required. A blue arrow points to the "Monitor Current Interoperability" link at the top of the table. The status message at the bottom says "Your system is upto date and running the latest version of vCenter Server. Last Checked at : 03/08/2020, 12:28:13 PM". The footer features the "ESX virtualization" logo and "www.vladan.fr".

And when you click the Monitor Current Interoperability link, you'll get to this screen. However, in my case, there is nothing to see obviously as I don't currently have populated other products except a single vCenter server in my nested only lab....

Quote from the UI:

*Interoperability will display VMware products currently registered with vCenter Server and ensure compatibility before the upgrade. Some VMware products may not be displayed and will need to be added manually using the modify product list option.*

Screenshot from the lab.



However, we also have some screenshots with datas... Let's see.

Here is a screenshot from VMware....

## vCenter Update Planner Pre-Upgrade Checks

The screenshot shows the 'vCenter Update Planner' interface. The 'Pre-Upgrade Checks' section is highlighted. A blue arrow points to the 'Pre-Update Checks' link, which is underlined and located at the bottom of the section.

Release Date	Version	Build	Type	Severity	Reboot Required	Release Notes
11/18/2019	6.7.0.42000	15132721	Update	Moderate	No	<a href="#">Link</a>
09/27/2019	6.7.0.41000	14836122	Update	Moderate	No	<a href="#">Link</a>
07/08/2019	6.7.0.40000	14367737	Update	Moderate	No	<a href="#">Link</a>
07/02/2019	6.7.0.32000	14070457	Update	Moderate	No	<a href="#">Link</a>

So if there is something wrong with the environment, you'll get the error or warning message before you actually start the upgrade process. Here again, screenshot from VMware blogger's briefing we had before the announce....

The screenshot shows the vCenter Server Update Planner interface. On the left, there's a sidebar with options like 'vCenter Server', 'Update Planner', 'Hosts' (selected), 'Images', 'Baselines', 'VMware Tools', and 'VM Hardware'. The main area is titled 'Pre-Update Checks' and contains a table with three rows. The first row has an 'Error' status with the message 'Cannot collect component requirements. For more details check out the server logs'. The second row has a 'Warning' status with the message 'The component "VMware vCenter Server High-Availability" precheck will be skipped.'. The third row has a 'Warning' status with the message 'vCenter External Extensions'. There are 'EXPORT' and 'REFRESH' buttons at the top right of the table.

Result	Description	Resolution
<span style="color: red;">⚠ Error</span>	Cannot collect component requirements. For more details check out the server logs	For more information check the VMware logs. Please search for these symptoms in the VMware Knowledge Base for any known issues and possible resolutions. If none can be found, collect a support bundle and open a support request.
<span style="color: yellow;">⚠ Warning</span>	The component "VMware vCenter Server High-Availability" precheck will be skipped.	For more information check the VMware logs. Please search for these symptoms in the VMware Knowledge Base for any known issues and possible resolutions. If none can be found, collect a support bundle and open a support request.
<span style="color: yellow;">⚠ Warning</span>	vCenter External Extensions	Please ensure extensions are compatible with the new vCenter Server and re-register extensions with the new vCenter Server after upgrade. Please refer to the vSphere documentation on extensions, and the upgrade and interoperability guides.

You might also have 3rd party products which are installed. Again, compared to my empty environment, VMware has actually some data on their screenshots, so again, here is the screenshot from the pre-briefing where you can see that an environment has had some vROPs, Log Insight, vRA, but also an incompatible version of ESXi 5 and vCloud Director 9.7.

And as you can see, **you'll be also a given a compatible version** so you must first upgrade the let's say vRealize Log insight from 4.8.0 to 8.0.0 before you will upgrade your vCenter server otherwise the interoperability will not be possible!

This is pretty cool as you will no longer need to check the VMware website for the interoperability page manually :-).

Note that the "Modify product list" allows you to add a product that wasn't detected by the system automatically. But it will allow you to add a product which wasn't detected right away. You can add your product in there and you can still compare it against your environment to see what is ready to be upgraded.

## Interoperability ⓘ

The screenshot shows a table titled 'Product Compatibility' with the following columns: Product, Current Version, Compatible Version(s), and Release Notes. A yellow banner at the top right of the table area says 'Before upgrading, check the compatibility of 3rd party products that are registered with vCenter Server.' There are two buttons at the top left: 'MODIFY PRODUCT LIST' and 'EXPORT'. A blue arrow icon is in the top right corner.

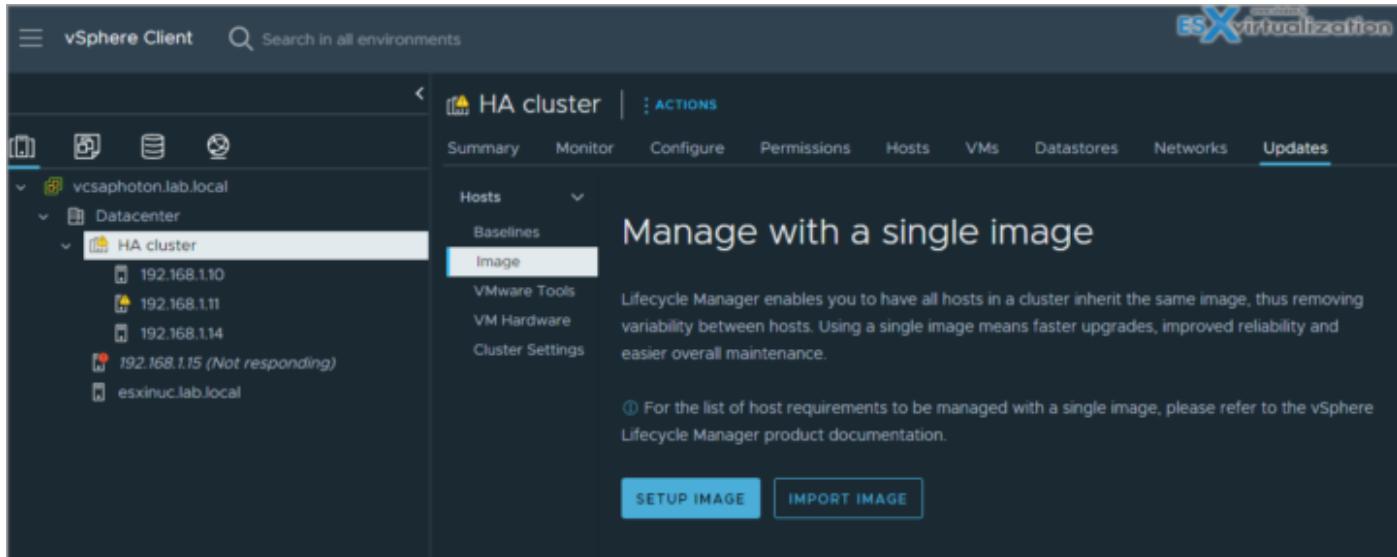
Product	Current Version	Compatible Version(s)	Release Notes
① VMware vCloud Director	9.7	No compatible version	Not Available
① VMware vSphere Hypervisor (ESXi) (5)	7.0.0	No compatible version	Not Available
✓ VMware vRealize Automation	7.5.0	<u>8.0.0</u> ▾	Not Available
✓ VMware vRealize Log Insight	4.8.0	<u>8.0.0</u> ▾	<a href="#">Link</a>
✓ VMware vRealize Operations Manager	6.7.0.000000	<u>7.0.0</u> ▾	<a href="#">Link</a>
✓ Hybrid Cloud Extension (HCX)	3.5.1	3.5.1	Not Available

You'll see what's compatible for upgrades and what's not.

## Objective 5.9 - Use vSphere Lifecycle Manager to determine the need for upgrades and updates

Starting with vSphere 7.0, vSphere Lifecycle Manager introduces the option of using vSphere Lifecycle Manager images as an alternative way to manage the lifecycle of the hosts and clusters in your environment. You can also use vSphere Lifecycle Manager to upgrade the virtual machine hardware and VMware Tools versions of the virtual machines in your environment.

VMware has become a transition from baseline-based updates to Image based updates. VMware Lifecycle Manager (VLM) enables you to have all hosts in a cluster inherit the same image, thus removing variability between hosts. Using a single image means faster upgrades, improved reliability and easier overall maintenance.



You can use vSphere client and vLCM to update your environment, your hosts, your cluster etc. There are a couple of operations you need to be aware of:

**Compliance Check** - An operation of scanning ESXi hosts to determine their level of compliance with a baseline attached to the cluster or with the image that the cluster uses. The compliance check does not alter the object.

**Remediation Pre-Check** - An operation that you perform before remediation to ensure that the health of a cluster is good and that no issues occur during the remediation process.

**Remediation** - This is an operation that does the actual software updates to the ESXi hosts in a cluster. During remediation, you install software on the hosts. Remediation makes a non-compliant host compliant with the baselines attached to the cluster or with the image for cluster.

**Staging** - An operation that reduces the time ESXi hosts spend in maintenance mode. When you stage an image or baseline to an ESXi host, vSphere Lifecycle Manager downloads the respective bulletins or components from the vSphere Lifecycle Manager depot to the host without applying them immediately. Staging makes the components, patches, and extensions available locally on the hosts. You can choose to remediate the hosts at a later time, not immediately after staging.

## Objective 5.9.1 - Update (Upgrade) Virtual Machines

Whether you perform an upgrade of the virtual machine hardware version or the VMware Tools version, the upgrade is a multi-stage process.

- **You check the status of individual virtual machines or a container object** - vSphere Lifecycle Manager checks the status of a virtual machine against the latest virtual machine hardware version supported by the host on which the virtual machine runs. Similarly,

vSphere Lifecycle Manager checks the status of the virtual machine against the latest VMware Tools version supported by the host on which the virtual machine runs.

- You review the status of the scanned virtual machines.
- You upgrade the virtual machine to match the host where it resides.

With vSphere Lifecycle Manager, you can upgrade the virtual machine hardware version and the VMware Tools version that a virtual machine has. You can use vSphere Lifecycle Manager to upgrade the virtual machine hardware version to the latest hardware version, vmx-19, and to the latest VMware Tools version on the hosts.

## Objective 5.9.2 - Update ESXi hosts

Screenshot from the lab shows that I need to update my cluster.....

The screenshot shows the vSphere Client interface with the 'Updates' tab selected for the 'HA cluster'. The left sidebar shows a hierarchy of vCenter servers and datacenters. The main pane displays '3 Host(s)' with '3 of 3 Hosts are non-compliant'. A table at the bottom lists attached baselines and baseline groups, with one entry for 'esxi80' marked as 'Non-compliant'.

Attached Baselines and Baseline Groups	Status	Type	ESXi version	Last Modified
Attached Baselines and Baseline Groups	Non-compliant	Patch	8.0, 7.0, 6.7.0	1 day ago
Host Security Patches (Predefined)	Non-compliant	Patch	8.0, 7.0, 6.7.0	1 day ago
Critical Host Patches (Predefined)	Non-compliant	Patch	8.0, 7.0, 6.7.0	1 day ago
Non-Critical Host Patches (Predefined)	Non-compliant	Patch	8.0, 7.0*, 8.0*, 7.0, 6.7.0, 8.0.0	1 day ago
esxi80	Compliant	Upgrade	8.0.0	2 months ago
vSAN Cluster 'HA cluster'	Non-compliant	Group	Recommendation	8.0

Check for more within VMware Documentation and [vSphere Lifecycle Manager](#) section.

## Objective 5.9.1 - Update virtual machines

Use Update Manager to upgrade the hardware version of one or multiple virtual machines to the latest hardware version that the host supports.

You might not think of it as such, but it allows you to have additional security as VUM can roll back virtual machines and appliances to their previous state. You can manually upgrade the hardware of virtual machines immediately, or you can schedule.

The screenshot shows the vSphere Client interface with the navigation bar at the top. The left sidebar shows a tree view of the environment, including Datacenter, Hosts, Images, Baselines, VMware Tools (which is selected), vCenter Server, and Update. The main content area displays the 'VM Hardware Compatibility Status' for the 'vsan' cluster. It includes a table with columns for Cluster, VMs, and 'VMs - Compatibility Upgrade Available'. Below this is a table titled 'VMs in Cluster vsan' with columns for VM, Host, Host Compatibility, VM Compatibility, and Status. Several VMs are listed, including 'Test-checked-out-VM', 'vcsaphoton', 'HA-Proxy', 'StarWind02', 'Photon4', 'DC', 'Windows 7', 'StarWind01', and 'TinyVM01-GUI-vladtest (template)'. A blue arrow points to the 'CHECK STATUS' button in the top right corner of the compatibility status table.

You can use Lifecycle Manager **to upgrade VMware Tools** to the latest version that the host supports. Navigate to Menu > Hosts and Clusters > Select a host or a cluster from the inventory and click the Updates tab > The Update Overview page appears > Select VMware Tools.

The screenshot shows the vSphere Client interface with the navigation bar at the top. The left sidebar shows a tree view of the environment, including Datacenter, Hosts, Images, Baselines, VMware Tools (selected), vCenter Server, and Update. The main content area displays the 'VMware Tools Status' for the 'HA' cluster. It includes a table with columns for Cluster, VMs, and 'VMs - Upgrade Available' and 'VMs - Version Unsupported'. Below this is a table titled 'VMs in Cluster HA' with columns for VM, Host, Tools Status, and Auto Update. Several VMs are listed, including 'StarWind02', 'Windows 7', 'StarWind01', and 'TinyVM01-GUI-vladtest-Clone-2023-03-17 10-55'. A blue arrow points to the 'CHECK STATUS' button in the top right corner of the tools status table.

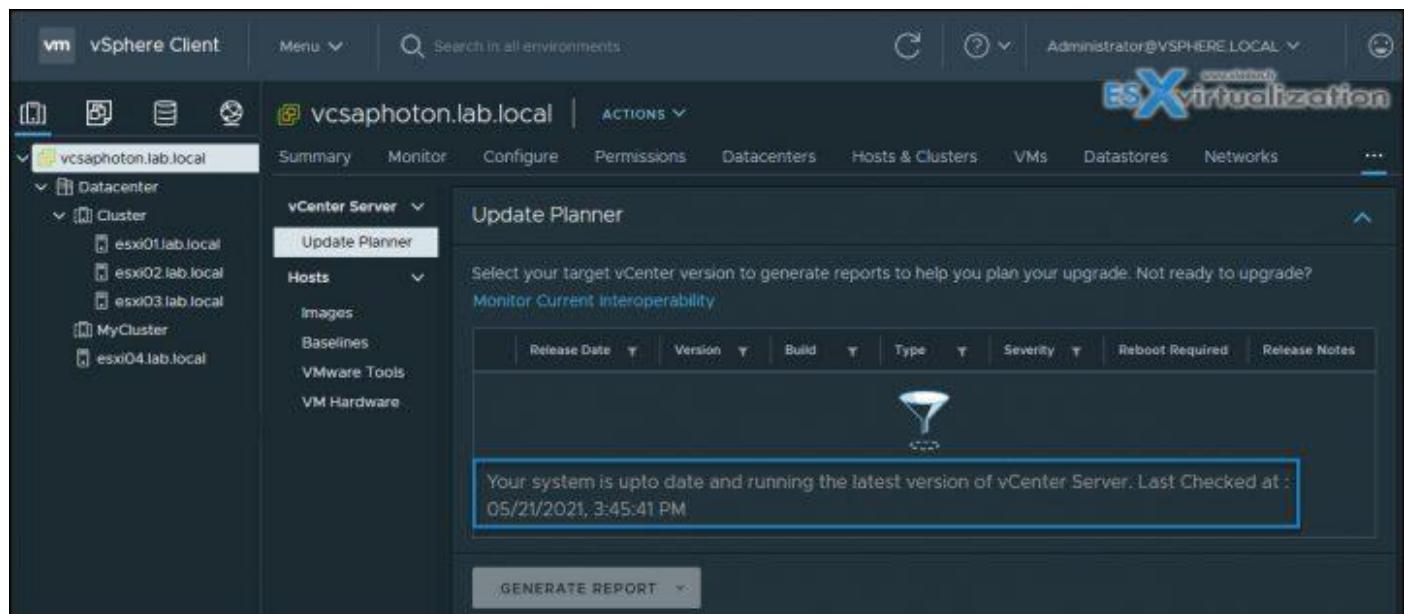
## Objective 5.9.2 - Update VMware ESXi

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).



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 or ESXi 8.x 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 5.10 - Use performance charts to monitor performance

Covered in 5.3

## Objective 5.11 - Perform proactive management with VMware Skyline

VMware Skyline is a proactive and predictive analytics service that enables administrators to proactively manage their VMware environment. It helps identify potential issues and provides recommendations to avoid them, reducing the risk of downtime and ensuring business continuity.

**Identify potential issues before they occur** – VMware Skyline uses machine learning algorithms and analytics to identify potential issues in the VMware environment. It analyzes the environment for known issues and recommends solutions to avoid them. It also looks for patterns of behavior that may indicate an issue is likely to occur in the future. By identifying potential issues before they occur, Skyline can help avoid downtime and ensure business continuity.

**Provide recommendations for best practices** – VMware Skyline provides recommendations for best practices based on industry standards and VMware's own

experience. It looks for areas where the environment can be improved to ensure optimal performance, security, and compliance.

For example, Skyline may recommend that virtual machines be moved to a different datastore to improve performance, or that security patches be applied to avoid potential security vulnerabilities. By following these recommendations, administrators can ensure that their VMware environment is running optimally and in compliance with industry standards.

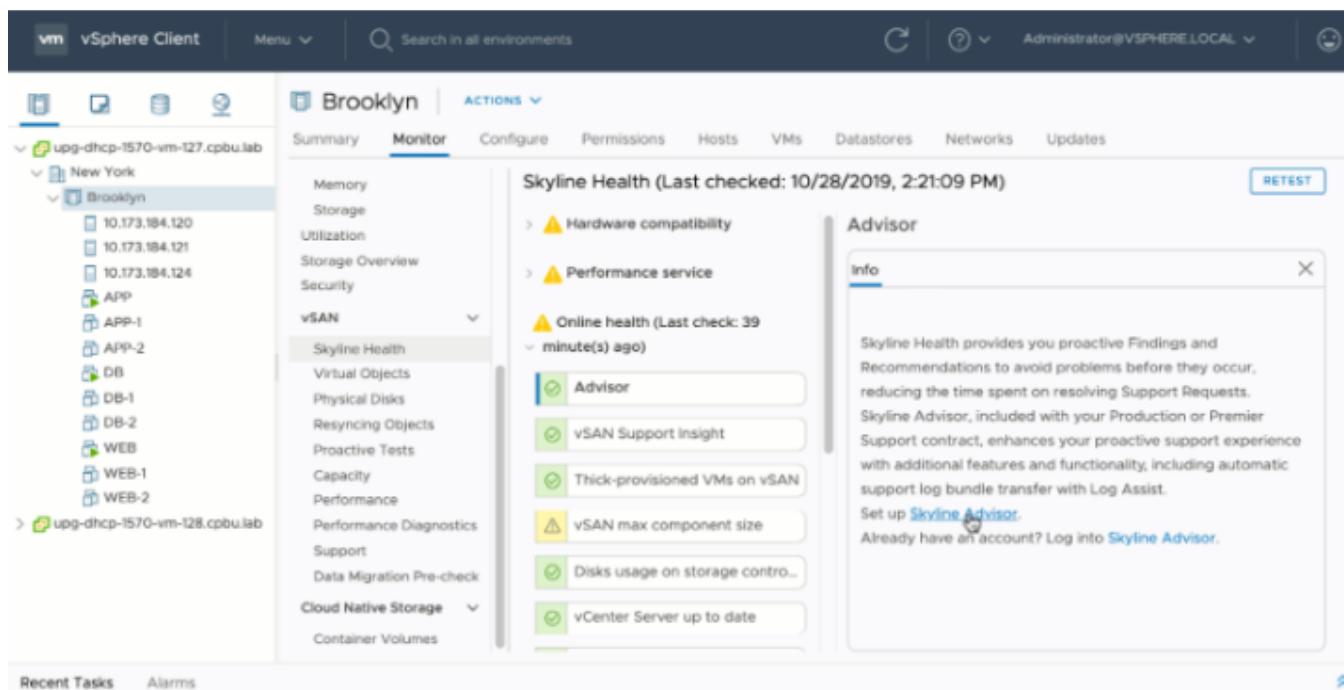
**Improve efficiency and reduce operational costs** – VMware Skyline can help improve efficiency and reduce operational costs by automating routine tasks. It can perform tasks such as collecting logs and configuration data, and analyzing them for potential issues. This can save administrators time and resources, allowing them to focus on more strategic tasks.

**Increase visibility and control** – VMware Skyline provides administrators with increased visibility and control over their VMware environment. It provides a single pane of glass view of the environment, allowing administrators to easily identify potential issues and take action to address them.

**Provide proactive support** – VMware Skyline provides proactive support to customers. It can automatically create support requests for potential issues and provide recommendations for resolution. This can help ensure that issues are addressed quickly and efficiently, reducing the impact on business operations.

In addition, Skyline provides access to VMware technical support experts who can provide additional guidance and assistance if needed. This can help administrators feel confident that they have the support they need to keep their environment running smoothly.

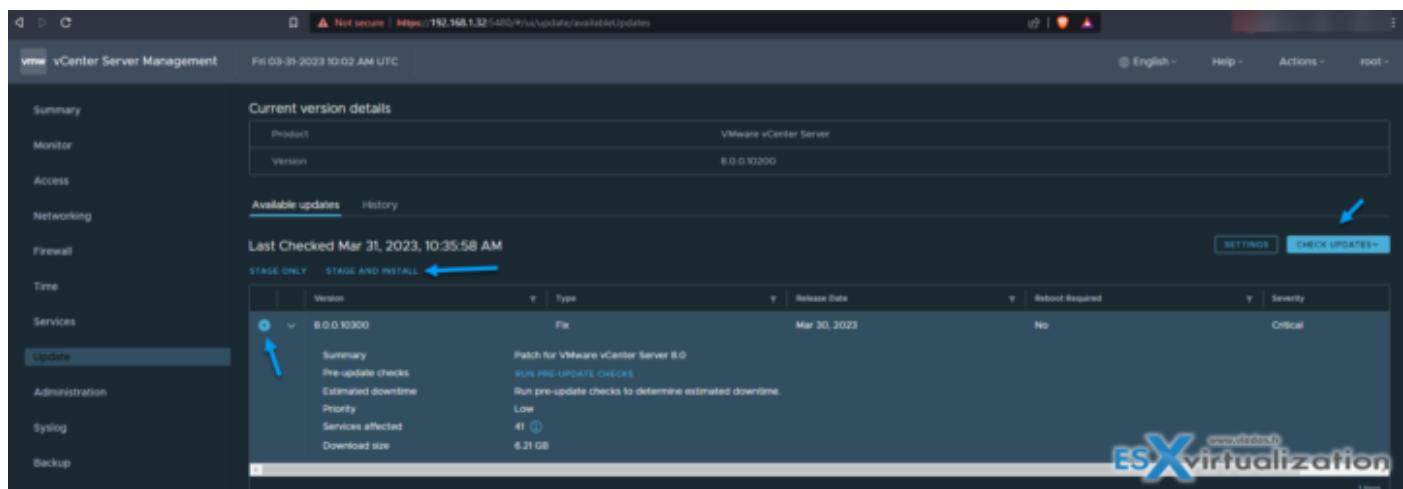
Screenshot from VMware



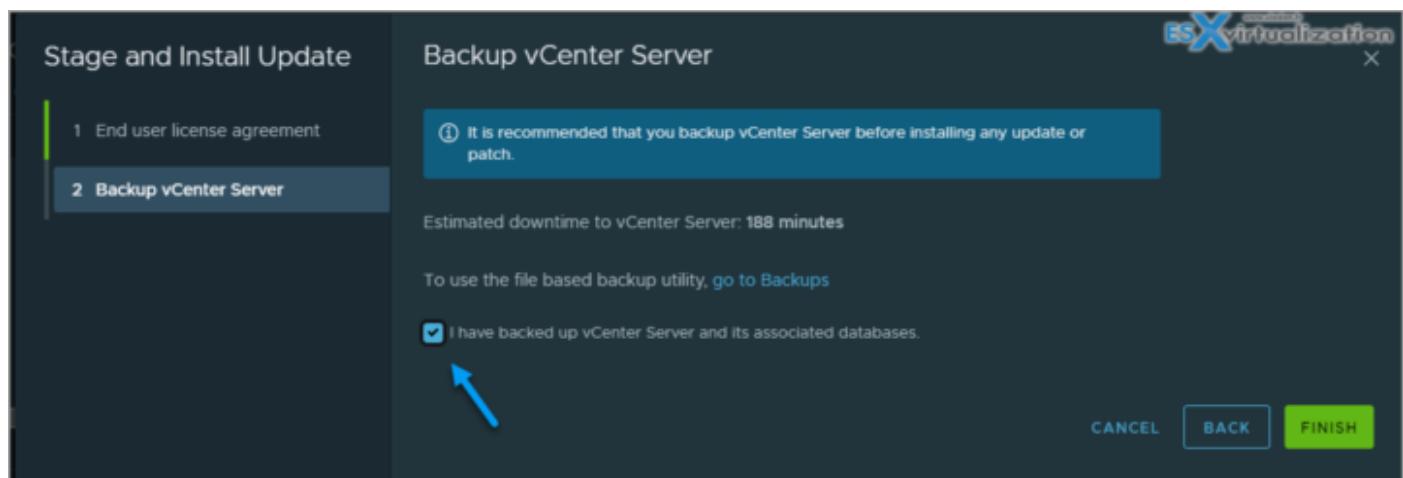
VMware Skyline is a powerful tool for performing proactive management of VMware environments. It can help identify potential issues before they occur, provide recommendations for best practices, improve efficiency and reduce operational costs, increase visibility and control, and provide proactive support. By leveraging the power of Skyline, organizations can ensure that their VMware environment is running optimally and in compliance with industry standards, while minimizing the risk of downtime and ensuring business continuity.

## Objective 5.12 - Use VMware vCenter management interface to update VMware vCenter

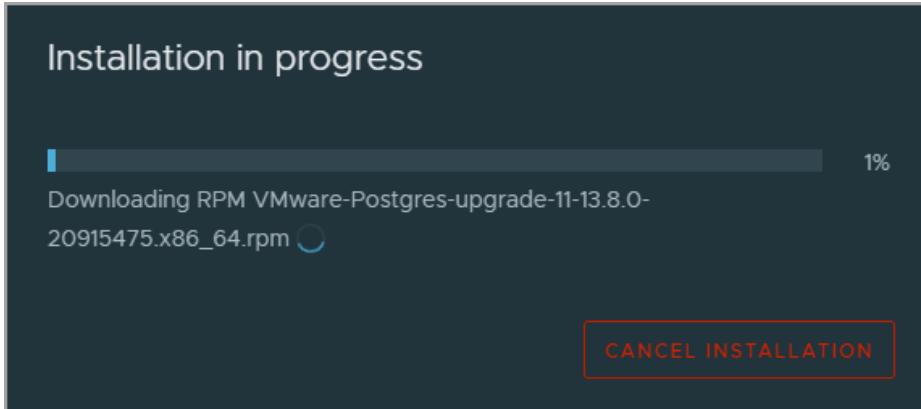
vCenter server management UI (VAMI) is accessible via IP\_of\_VCSA:5480 where after connecting with login/password combination, you'll click on **Updates > Check Updates > Select the update from the list** (if any) and then click **Stage and Install** button.



The next screen asks you to agree to the EULA and the one after reminds you about backing up your vCenter server and its database. You can configure file-level-backup via the VAMI as well. Make sure you have the backup configured and done before you upgrade.



The progress of the download and installation window below....



Hopefully this chapter will help you to study towards VMware VCP-DCV Certification based on vSphere 8.x. Find other chapters on the main page of the guide – [VCP8-DCV Study Guide Page](#).

## Objective 5.13 - Complete lifecycle activities for VMware vSphere with Tanzu

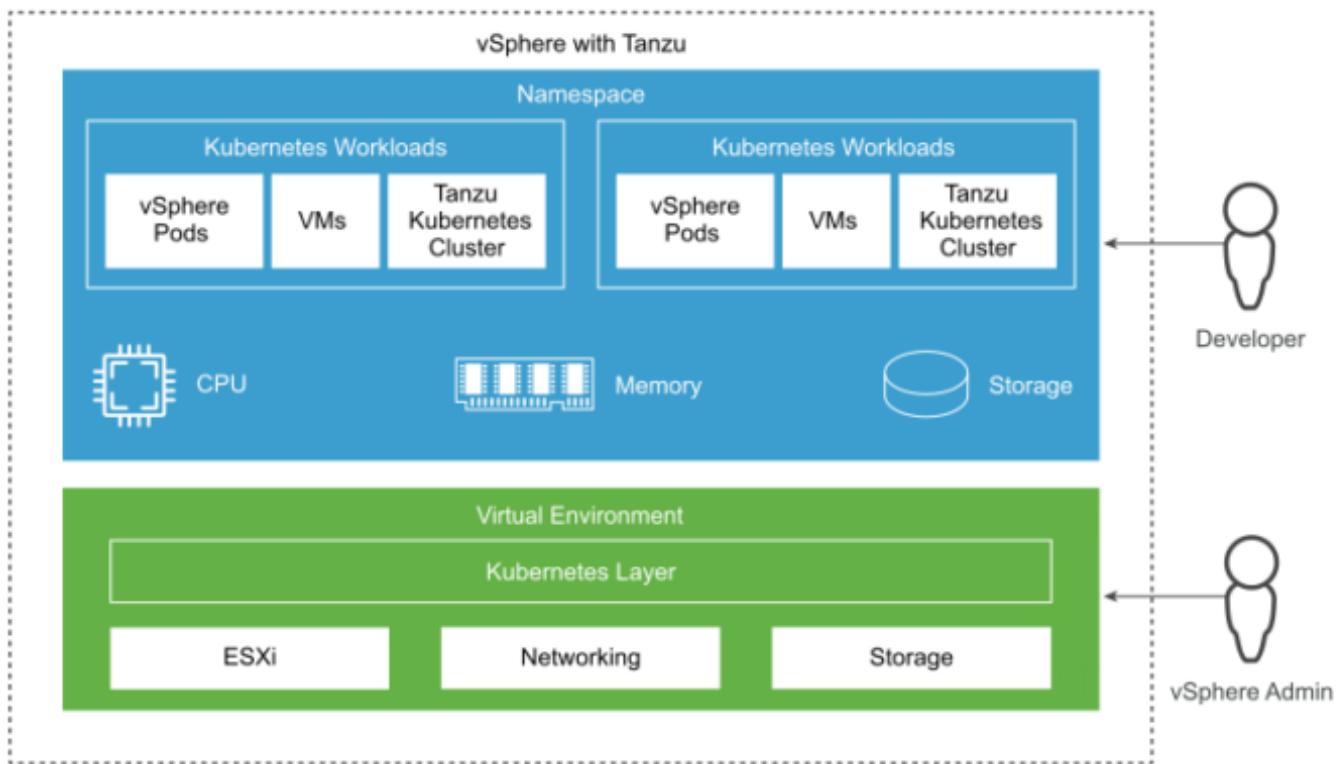
You can backup and restore the workloads running on vSphere Pods and Tanzu Kubernetes clusters, as well as the vCenter Server and [NSX-T](#) infrastructure supporting your vSphere with Tanzu installation. There is a Velero plugin that will help you with that.

The solution requires the installation and configuration of several components. Once you have the Velero Plugin for vSphere installed and configured on the Supervisor Cluster, you can backup and restore vSphere Pods. For persistent workloads, the Velero Plugin for vSphere lets you take snapshots of the persistent volumes. Read more [here](#).

You're able to backup and restore:

- vSphere Pods – note that the plugin is not backing up Supervisor Cluster state. See more.
- Backup stateless and stateful workloads on a Tanzu Kubernetes cluster and restore to a cluster provisioned by the Tanzu Kubernetes Grid Service – Both Kubernetes metadata and persistent volumes can be backed up and restored. Velero snapshotting (not Restic) is used for persistent volumes. See [more](#).
- Backup stateless and stateful workloads on a Tanzu Kubernetes cluster and restore to a conformant Kubernetes cluster not provisioned by the Tanzu Kubernetes Grid Service
- After a Supervisor Cluster upgrade, you must do a new backup. Restoring a vCenter Server to a backup where it expects an older version of Supervisor Cluster is not supported.
- vCenter Configuration – use tools for vCenter backup and restore.
- NSX-T Data Center – Load balancer and ingress services depend on NSX-T backup. Use NSX-T Manager to backup and restore the NSX-T database.

More reading in VMware documentation [here](#).



## Objective 5.13.1 - Update Supervisor cluster

Covered in 5.13

## Objective 5.13.2 - Backup and restore VMware vSphere with Tanzu

Covered in 5.13

## Objective 6.1 - Identify use cases for enabling vSphere Cluster Services (vCLS) retreat mode

VMware introduced vSphere Cluster Services (vCLS) in vSphere 7.0 Update 1, and we reported on that in detail [here](#). These vCLS mini-VMs, also called agent VMs, must be run on the cluster. However, there is a way to disable them, and we'll show you how and why you might need to do this.

VMware says that vCLS uses agent virtual machines (vCLS VMs) to maintain the health of cluster services, even if the vCenter Server is not available. The vCLS VMs are created when you add hosts to clusters.

There is a maximum of three such VMs, even if your cluster has more than three hosts. During normal operation, there is no way to disable vCLS agent VMs and the vCLS service. It is

a mandatory service that is required for DRS to function normally. vSphere DRS depends on the health of the vSphere Cluster Services starting with vSphere 7.0 Update 1.

If the agent VMs are missing or not running, the cluster shows a warning message.

vSphere DRS functionality was impacted due to unhealthy state vSphere Cluster Services caused by the unavailability of vSphere Cluster Service VMs. vSphere Cluster Service VMs are required to maintain the health of vSphere DRS.

It is possible to manually disable vCLS on a vSphere cluster via Retreat Mode, but some of the cluster's services, such as DRS, will be affected. The VMs running inside your cluster are not load-balanced and will not be migrated to different hosts if your host running a particular VM is running out of resources.

### What is retreat mode?

Retreat mode should only be used when you need to put your datastore into maintenance mode. If your datastore has a vCLS VM running, you must manually evacuate this VM via storage vMotion to a new location **or put the cluster in retreat mode**.

When first activating DRS on your cluster and the vCLS agent VMs are created and deployed, the datastores that will host the VMs are automatically selected. The selection of the datastores connected to the hosts inside your cluster is based on ranking.

A datastore is usually selected to host a vCLS VM if the host connected to the datastore has free reserved DRS slots. A **datastore with more free space is preferred**, and the algorithm tries not to place more than one vCLS VM on the same datastore.

Starting with vSphere 7.0 Update 2, a new [anti-affinity](#) rule is created and applied automatically. This rule makes sure that every 3 minutes, a check is performed if there are multiple vCLS VMs on the same datastore. If that's the case, the rule **triggers a storage vMotion operation and redistributes those VMs to different datastores**.

When a datastore hosting vCLS VMs is placed in maintenance mode, you must manually apply storage vMotion to the vCLS VMs to move them to a new location or put the cluster in retreat mode. A warning message is displayed.

Note: To enter maintenance mode, the task will start but cannot finish because there is a virtual machine residing in the datastore. To move forward, you can cancel the task in your Recent Tasks if you want to continue to evacuate the VM.

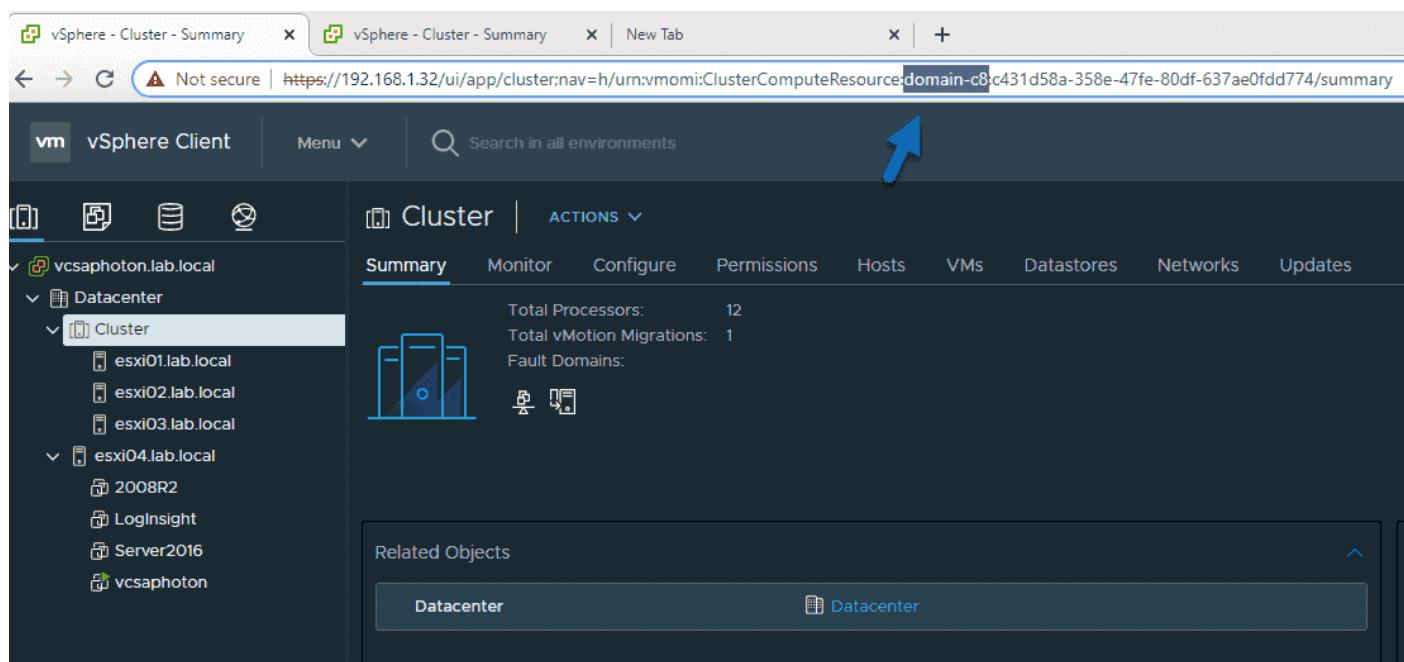
## vCLS Retreat Mode advanced configuration

1. Log in to the vSphere client and navigate to the cluster on which you want to disable vCLS.
2. Copy the cluster domain ID from the URL of the browser. It should be similar to **domain-c(number)**.

The URL will be something like this:

<https://<fqdn-of-vCenter-server>/ui/app/cluster;nav=h/urn:vmomi:ClusterComputeResource:domainc10001:eef257af-fa50-455a-af7a-6899324fabe6/summary>

Copy the **part in bold**—in this case, **domain-c8**.



Copy the cluster domain ID from the URL

1. Then select your vCenter Server and navigate to the vCenter Server **Configure** tab.

**vSphere Client** | Menu ▾ | Search in all environments

**vcsaphoton.lab.local** | ACTIONS ▾

**Summary** | **Monitor** | **Configure** | Permissions | Datacenters | Hosts & Clusters | VMs | Datastores | Networks | Linked vCenter Server Systems | Extensions | Updates

**Advanced vCenter Server Settings**

Name	Value	Summary
alarms.version	-1	Default alarm upgrade version
alarms.versionEx	111.0.24	Default alarm extended version
config.alarms.vim.version	vim.version.v7_0_2_0	--
config.drs.kvstore.local	False	--
config.license.client.lsNotificationsSyncSeconds	30	--
config.license.client.oldServerLsNotificationsSyncSeconds	600	--
config.log.compressOnRoll	true	--
config.log.level	info	--
config.log.maxFileNum	30	--
config.log.maxFileSize	52428800	--
config.log.outputToConsole	false	--
config.log.outputToFiles	true	--
config.registry.DB.key_2	vc	--
config.registry.DB.key_3	'8KIGylGJWUhs0YhdDPe/YwXbU2oSF2g/92KMVuSOL8zCs8EWPOQoJaeSUlk6	--
config.registry.key_EvaluationExpiryDate	AQD+yyggAAADWcTYkcgB0gAAAABSBF7cx0x3c9E27gtar3WnUJU650zg;INGLf6IVDp+gMmoDfpzdwXfElp4oly59/vmuisfnEHtHGYWt8voIqg==	--
config.registry.key__VCVmId	vm-26	--
config.task.minCompletedLifetime	60	--
config.vtI.severity	none	Defines the verbosity level on which distributed tracing collects data
config.vmacore.cacheProperties	true	--
config.vmacore.ssl.tlps	false	--
config.vmacore.threadPool.TaskMax	90	--
config.vmacore.threadPool.threadNamePref	vpd	--
config.vmomi.validation	--	--
config.vpd.cert.prefix.solutionUser	vcsoluser	--
config.vpd.cert.prefix.ssl	rui	--

## vCenter Server 7 U2 Advanced Settings

- Under **Advanced Settings**, click the **Edit Settings** button.
- Add a new entry, **config.vcls.clusters.domain-c(number).enabled**. Use the domain ID copied in Step 3.

**Edit Advanced vCenter Server Settings**

⚠️ 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
alarms.version	-1	Default alarm upgrade version
alarms.versionEx	111.0.24	Default alarm extended version
config.alarms.vim.version	vim.version.v7_0_2_0	--
config.drs.kvstore.local	False	--
config.license.client.lsNotificationsSyncSeconds	30	--
config.license.client.oldServerLsNotificationsSyncSeconds	600	--
config.log.compressOnRoll	true	--
config.log.level	info	--
config.log.maxFileNum	30	--
config.log.maxFileSize	52428800	--

1 - 10 of 756 settings | < 1 / 76 > |

Name: config.vcls.clusters.domain-c8 Value: False

**ADD** **CANCEL** **SAVE**

Name must start with 'config.' For example: config.log

Add a new line in the Advanced Settings parameters

- Set the **Value** to **False**.

- Click **Save**.

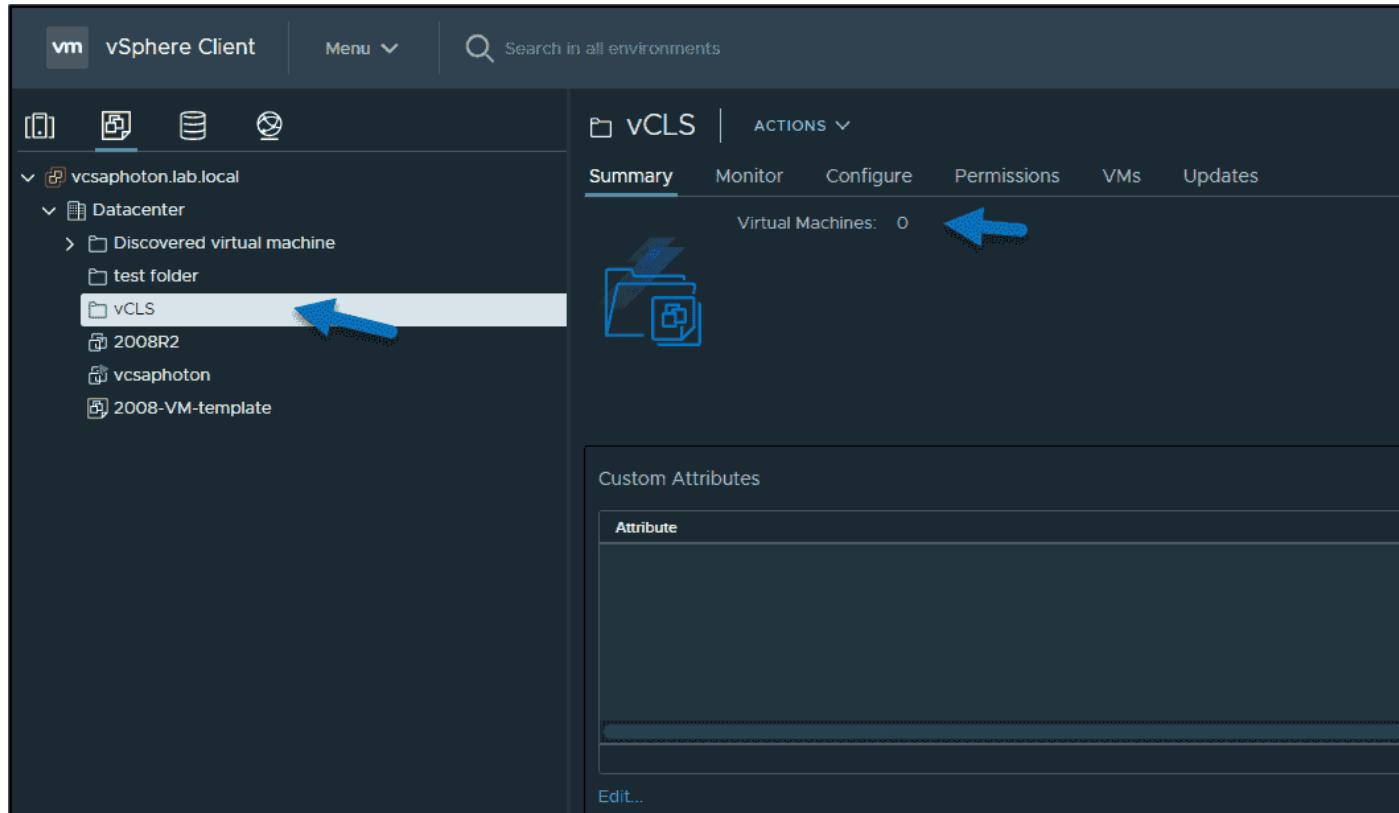
You should see a screen similar to the one below.

Name	Value	Summary
alarms.version	-1	Default alarm upgrade version
alarms.versionEx	111.0.24	Default alarm extended version
config.alarms.vim.version	vim.version.v7_0_2_0	--
config.drs.kvstore.local	False	--
config.license.client.lsNotificationsSyncSeconds	30	--
config.license.client.oldServer.lsNotificationsSyncSeconds	600	--
config.log.compressOnRoll	true	--
config.log.level	info	--
config.log.maxFileNum	30	--
config.log.maxFileSize	52428800	--
config.log.outputToConsole	false	--
config.log.outputToFiles	true	--
config.registry.DB.key_2	vc	--
config.registry.DB.key_3	*BKTGylGIW7hks0YklIDPe/YwXbU2o5F2g/9 2kMViuSOLbzCsEWPOQuJaevSUK6	--
config.registry.key_EvaluationExpiryDate	AQD+yygAAAADWcTY6KogBl0QAAABSBF7 cbXBc39E27gar3WnU0Jb50zgclNGLsF61V Dp+GmnoDf6pIzdwXfIEtip4oyS9/wmiusfn ethII/Gyv1YBvoiqg==	--
config.registry.key_VCVmid	vm-26	--
config.task.minCompletedLifetime	60	--
<b>config.vcls.clusters.domain-c8</b>	<b>False</b>	--
config.vd.t.severity	none	Defines the verbosity level on which distributed tracing collects data
config.vmacore.cacheProperties	true	--
config.vmacore.ssl.flps	false	--
config.vmacore.threadPool.TaskMax	90	--
config.vmacore.threadPool.threadNamePrefix	vpxd	--
config.vmomi.validation	--	--
config.vpxd.cert.prefix.solutionUser	vcsoluser	--

Retreat advanced settings for vCLS

VMware has a detailed KB on this [here](#).

The vCLS monitoring service runs every 30 seconds, so after about 1 minute, you'll see that all the vCLS VMs in the cluster are cleaned up and the Cluster Services health will be set to **Degraded**.



There are no more vCLS VMs

If the cluster has DRS enabled, **it stops functioning**. You'll see some additional warnings displayed in the Cluster Summary.

**Note:** *DRS is not functional, even if you enable it within the UI. It stays this way until vCLS is reconfigured by removing it from Retreat Mode.*

Besides vSphere DRS, High Availability (HA) will not perform optimal placement during a host failure. vSphere HA depends on DRS for placement recommendations; as such, it needs the Retreat Mode deactivated.

However, vSphere HA will be able to power the VMs if there is a host failure. These VMs will be powered on a host, but it might not be the best host with the best resources (not an optimal host).

To remove Retreat Mode from the cluster, change the value in Step 7 to **True**.

## How to log in to the VMware vCLS virtual machine

Do you want to log in to the vCLS VM? You can. In fact, I have found a small procedure in the VMware documentation that enables you to do so.

1. Use SSH to log in to the vCenter Server Appliance.
2. Run the following python script, which you can find at the following location:**/usr/lib/vmware-wcp/decrypt\_clustervm\_pw.py**
3. Read the output for the password.

Pwd-script-output

*Read key from file*

*Connected to PSQL*

*PWD: (password displayed here)*

You might need it if you want to perform an additional check for the cluster's health. However, it is meant to be used only for detailed diagnostics of the vCLS agent VMs. You won't need it for normal operations.

## **Objective 6.2 - Differentiate between the main management services in VMware ESXi and vCenter and their corresponding log files**

VMware log files are important because they allow you to find the root cause of a problem or point out that something is about to break. If something strange is happening within your infrastructure, the first thing to do is gather and check the logs.

You can then send these log files to VMware support after opening a support request to investigate what's going on and resolve problems you might have.

But different VMware products have different log locations and different ways to get these logs. How do you keep track of it all? When working in an enterprise environment, you'll perhaps want to get software that will not only be able to centralize and gather all of these logs but also «ingest» the logs and tell you if there are more errors than usual.

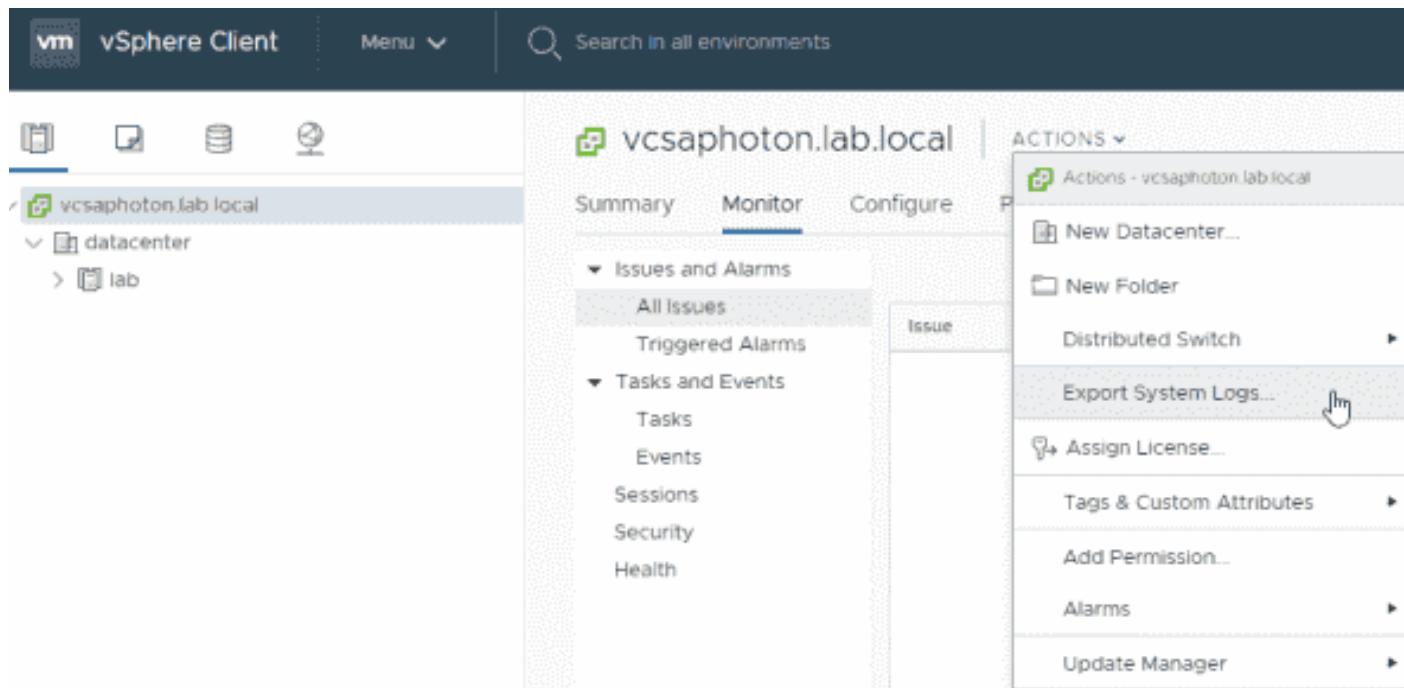
A proactive option is monitoring software that can store logs in one location and analyze them to provide you with patterns identified as warnings or failures.

One such application is VMware Log Insight, but in this post, we will not install and configure this software. Today we only want to know which logs are the most important, how to get them, and how to send them to VMware.

### **vCenter Server log files**

For environments using VMware vCenter Server, this operation of gathering support logs is now greatly simplified. To generate a support bundle, connect to your vCenter Server via the

vSphere HTML 5 Web Client and then go to **Home > Hosts and Clusters**. Select the vCenter Server you want to generate support logs from and go to **Actions > Export System Logs**.



### Exporting system logs from VMware vCenter Server

You can choose to export ESXi host log bundles and vSphere web client log files within the same bundle. With this information, VMware has everything they need to identify the problem. Within these subdirectories, vCenter Server logs are grouped by component and purpose. However, most of the time, you won't need to know all of this.

vCenter Server	vCenter Server Appliance	Description
vmware-vpx\vpd.log	vpd/vpd.log	The main vCenter Server log
vmware-vpx\vpd-profiler.log	vpd/vpd-profiler.log	Profile metrics for operations performed in vCenter Server
vmware-vpx\vpd-alert.log	vpd/vpd-alert.log	Non-fatal information logged about the vpxd process
perfcharts\stats.log	perfcharts/stats.log	VMware Performance Charts
eam\eam.log	eam/eam.log	VMware ESX Agent Manager
invavo	invavo	VMware Inventory Service
netdump	netdumper	VMware vSphere ESXi Dump Collector
vapi	vapi	VMware vAPI Endpoint
vmkdir	vmkdir	VMware Directory Service daemon
vmwsyslogcollector	syslog	vSphere Syslog Collector
vmware-sps\spc.log	vmware-sps/spc.log	VMware vSphere Profile-Driven Storage Service
vpctpostgres	vpctpostgres	vFabric Postgres database service
vsphere-client	vsphere-client	VMware vSphere Web Client
vws	vws	VMware System and Hardware Health Manager
workflow	workflow	VMware vCenter Workflow Manager
ss0	ss0	VMware Single Sign-On

All vCenter Server log files (from the VMware knowledge base article)

If you're using a vCenter Server Appliance (VCSA) as VMware recommends, you can also get the logs from a Secure Shell (SSH) session or a direct console session in case you have problems and using the vSphere Web Client isn't a possibility. You'll find the main vCenter Server log at vpxd/vpxd.log

## VMware ESXi host log files

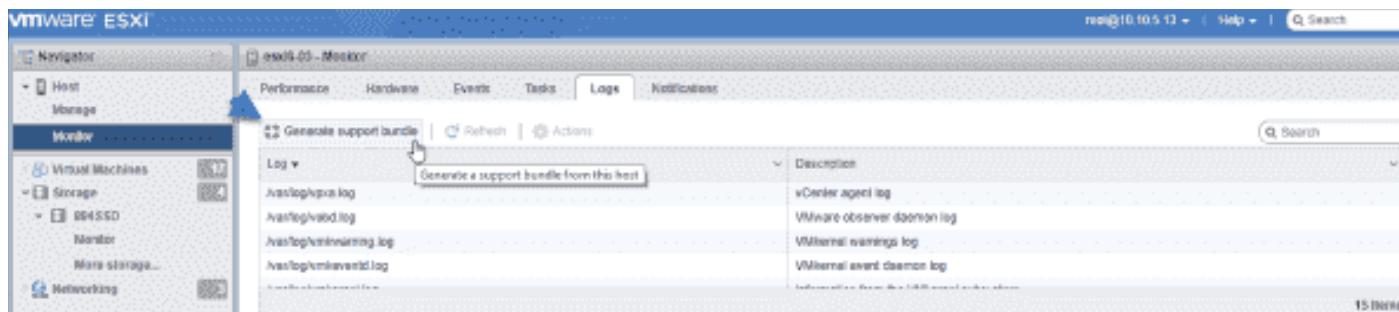
What if you don't have vCenter and want to check the logs for a VMware ESXi host? For individual ESXi hosts vCenter Server doesn't manage, you can get support logs via this procedure:

In your web browser, go to <https://ESXI-IP-ADDRESS/UI>.

Then go to **Monitor > Logs > Generate log bundle**.

You can do two things here:

1. You can check different logs by selecting a log file and verifying the content in the lower pane.
2. You can generate a log bundle.



Creating logs takes a few minutes, maybe five. Afterward, a small pop-up window appears telling you this:



Creation of a support bundle has completed. You can download the support bundle from [here](#).

You can find the download URL for this support bundle from the [Generate support bundle](#) task

The bundle will be automatically removed from the host after 15 minutes.

[Download](#)

[Dismiss](#)

The logs are quite voluminous; in my case they were like 155 MB in size. It's pretty convenient and simple to have these logs on your C: drive, but then you'll have to «ship» them to VMware. But again, it's simple.

You simply have to connect to your space at the myVMware portal and go to the **Get Support** section. There you will have to **Select an issue** and upload a log file.

The screenshot shows the 'Get Support' page on the myVMware portal. At the top, there are three dropdown menus: 'Technical' (set to 'Fault/Crash'), 'Product Licensing or Account' (set to 'Select one'), and 'General Inquiry' (set to 'Select one'). Below these is a section titled 'Select the Product Associated with the Issue'. It includes a link 'Don't see your product listed? Read KB article 2009213' and a dropdown menu labeled 'Supported Products | FOR ACCOUNT'. At the bottom of this section are buttons for 'Rows: Expand All' and 'Collapse All'.

Getting support at VMware and uploading log files

## ESXi logs and locations

You can find different ESXi log locations and the meaning of each log in this table from a VMware knowledge base article.

Component	Location	Purpose
VMkernel	/var/log/vmkernel.log	Records activities related to virtual machines and ESXi.
VMkernel warnings	/var/log/vmkwarning.log	Records activities related to virtual machines.
VMkernel summary	/var/log/vmksummary.log	Used to determine uptime and availability statistics for ESXi (comma separated).
ESXi host agent log	/var/log/hostd.log	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
vCenter agent log	/var/log/vpxa.log	Contains information about the agent that communicates with vCenter Server (if the host is managed by vCenter Server).
Shell log	/var/log/shell.log	Contains a record of all commands typed into the ESXi Shell as well as shell events (for example, when the shell was enabled).
Authentication	/var/log/auth.log	Contains all events related to authentication for the local system.
System messages	/var/log/syslog.log	Contains all general log messages and can be used for troubleshooting. This information was formerly located in the messages log file.
Virtual machines	The same directory as the affected virtual machine's configuration files, named vmware.log and vmware*.log. For example, /vmfs/volumes/datastore/virtual_machine/vmware.log	Contains virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, and so on.

### VMware ESXi logs and their locations

As you can see, quite a few logs are stored on ESXi hosts. ESXi records host activity in log files by using syslog, a standard for message logging. It is not proprietary to VMware and ESXi.

Within your environment, you can configure a syslog server. Instead of jumping from one ESXi host to another to check the logs, it's way better to install and configure a syslog server to pull the data from many ESXi hosts. Without a syslog server, you'd have to check through each ESXi host individually.

The syslog protocol supports a wide range of devices, and you can use it to log different types of events. For example, a router might send messages about users logging on to console sessions, while a web server might log access-denied events.

Syslog is a great way to consolidate logs from multiple sources into a single location, so you can configure each ESXi host to send its logs to a syslog server—to a single, central location.

You can download and test many free syslog servers. One of them for example is [Kiwi Syslog Server](#) from SolarWinds, but it is outside the scope of this post.

Whether you administer a small company's network or an enterprise-grade network infrastructure, in the long term, you should definitely consider employing a syslog monitoring tool.

## Objective 6.3 – Generate Log Bundle

Covered in 6.3

## 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.

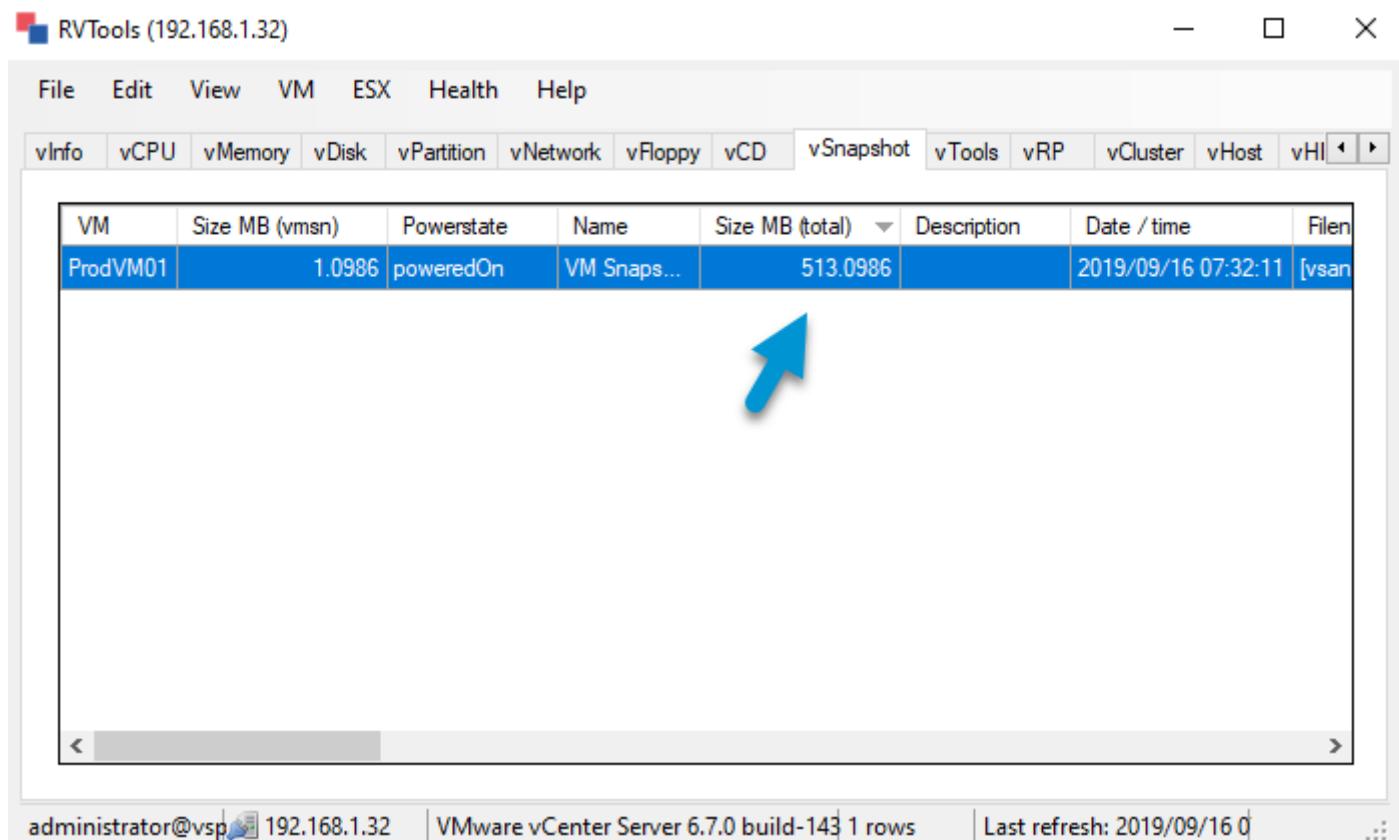
Do not use a snapshot for more than 72 hours. The snapshot files continue to grow as you keep using the VM. This can cause the snapshot storage location to run out of space and impact the system performance.

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 interface for managing VMware snapshots. The main window has a menu bar with File, Edit, View, VM, ESX, Health, Help. Below the menu is a toolbar with tabs: vInfo, vCPU, vMemory, vDisk, vPartition, vNetwork, vFloppy, vCD, vSnapshot, vTools, vRP, vCluster, vHost, vH. The vSnapshot tab is selected. A table lists a single VM entry: ProdVM01. The columns are: VM, Size MB (vmsn), Powerstate, Name, Size MB (total), Description, Date / time, and File. The 'Size MB (vmsn)' column contains the value 1.0986. The 'Powerstate' column shows poweredOn. The 'Name' column shows VM Snaps... The 'Size MB (total)' column shows 513.0986. The 'Date / time' column shows 2019/09/16 07:32:11. The 'File' column shows [vsan]. At the bottom of the interface, there is a status bar with administrator@vsp| 192.168.1.32 | VMware vCenter Server 6.7.0 build-143 1 rows | Last refresh: 2019/09/16 0 | ...

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]

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.

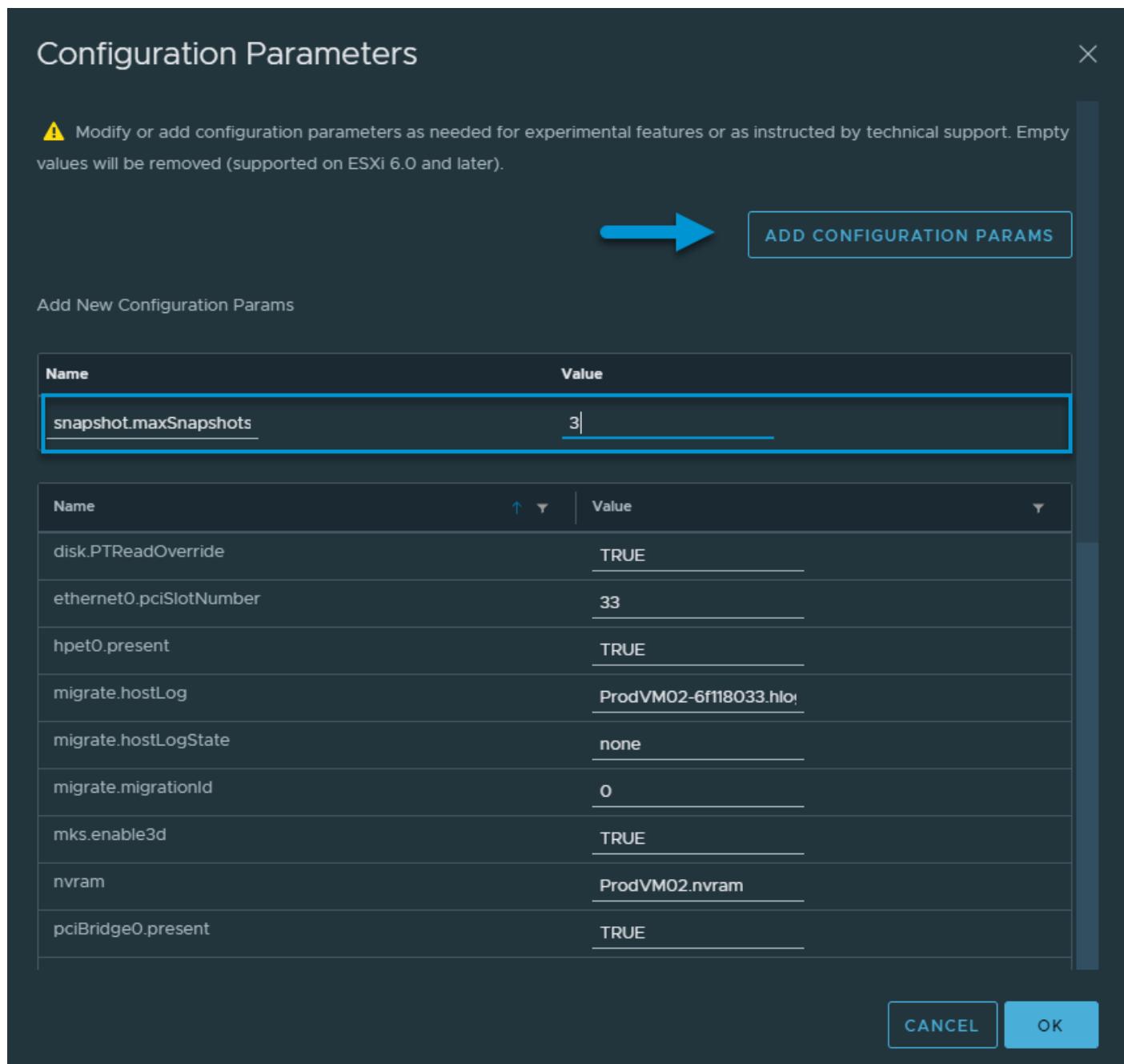
### How many snapshots to keep per VM?

When working with a team where many users has 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.



The screenshot shows the "Configuration Parameters" dialog box. At the top, a warning message reads: "⚠️ Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Empty values will be removed (supported on ESXi 6.0 and later)." A large blue arrow points from this message to the "ADD CONFIGURATION PARAMS" button. Below the message, there is a section titled "Add New Configuration Params" with a table. The table has two columns: "Name" and "Value". The first row shows "snapshot.maxSnapshots" with the value "3" entered. Below this table is another table listing various configuration parameters and their values. The parameters listed are: disk.PTReadOverride (Value: TRUE), ethernet0.pciSlotNumber (Value: 33), hpet0.present (Value: TRUE), migrate.hostLog (Value: ProdVM02-6f118033.hlog), migrate.hostLogState (Value: none), migrate.migrationId (Value: 0), mks.enable3d (Value: TRUE), nvram (Value: ProdVM02.nvram), and pciBridge0.present (Value: TRUE). At the bottom right of the dialog box are "CANCEL" and "OK" buttons.

Name	Value
snapshot.maxSnapshots	3

Name	Value
disk.PTReadOverride	TRUE
ethernet0.pciSlotNumber	33
hpet0.present	TRUE
migrate.hostLog	ProdVM02-6f118033.hlog
migrate.hostLogState	none
migrate.migrationId	0
mks.enable3d	TRUE
nvram	ProdVM02.nvram
pciBridge0.present	TRUE

Limit the Maximum snapshots number to three via advanced VM configuration

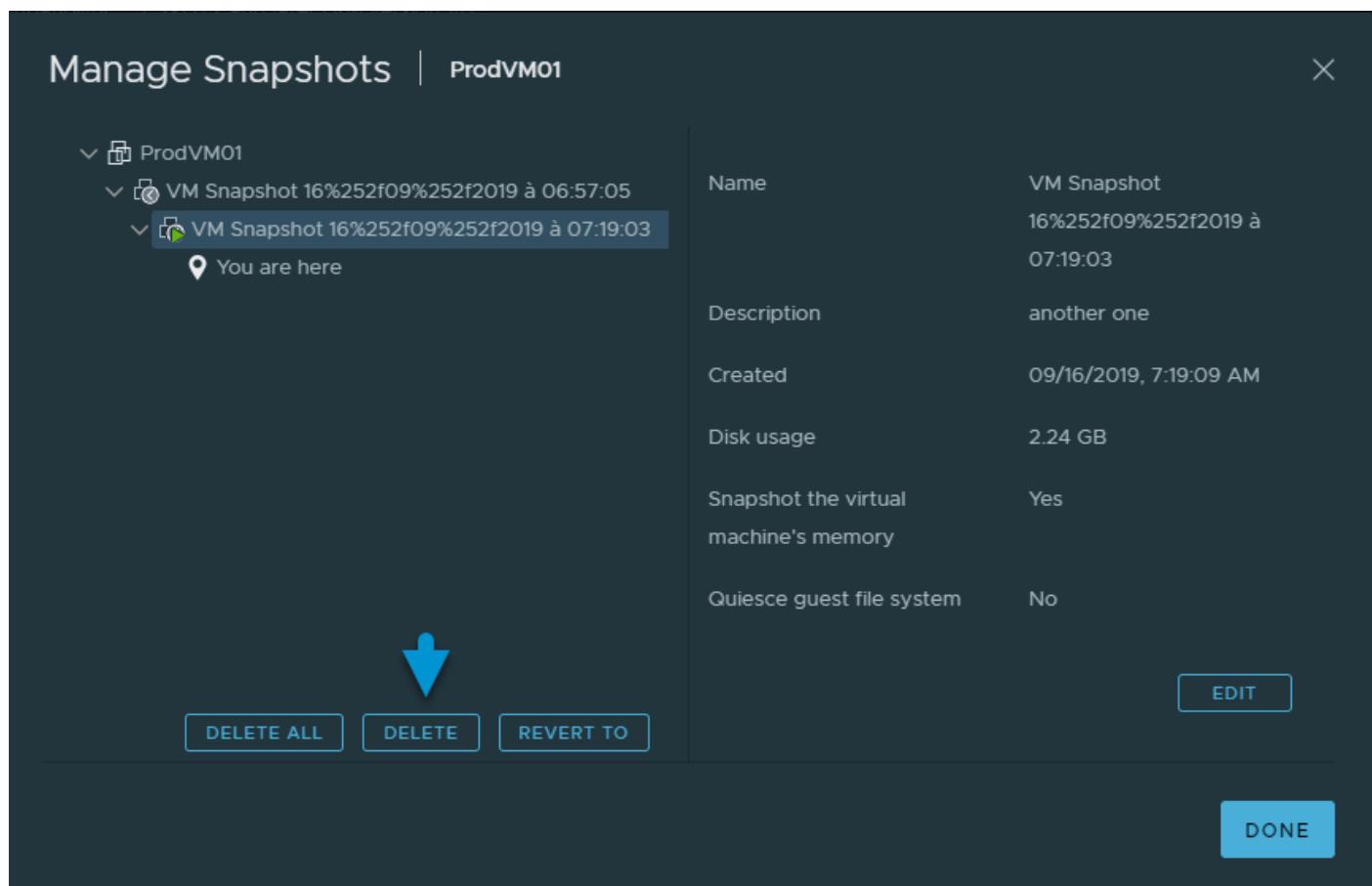
This way you can also disable snapshots completely. Just enter "0" to the field and nobody will be able to snapshot the VM. (including your backup software). So actually, to stay safe and

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.**



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 – Create virtual machines using different methods (Open Virtualization Format (OVF) templates, content library, etc.)

**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 7.3 – Manage virtual machines (modifying virtual machine settings, VMware per-VM EVC, latency sensitivity, CPU affinity, etc.)**

Covered in 7.2

## Objective 7.4 – Manage Storage

Identify storage adapters and devices

We will be heavily using one document – vSphere Storage Guide PDF.

VMware vSphere supports different classes of adapters: SCSI, iSCSI, RAID, Fibre Channel, Fibre Channel over Ethernet (FCoE), and Ethernet. ESXi accesses adapters directly through device drivers in the VMkernel.

Note that you must enable certain adapters (like the software iSCSI), but this isn't new as it's been the case already in previous release.

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:esxi-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.02000000000500a0751095c5844437275636961
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. The name indicates that the vmware.com domain name was registered in January of 1998, and iscsi is a subdomain, maintained by vmware.com.
- 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.

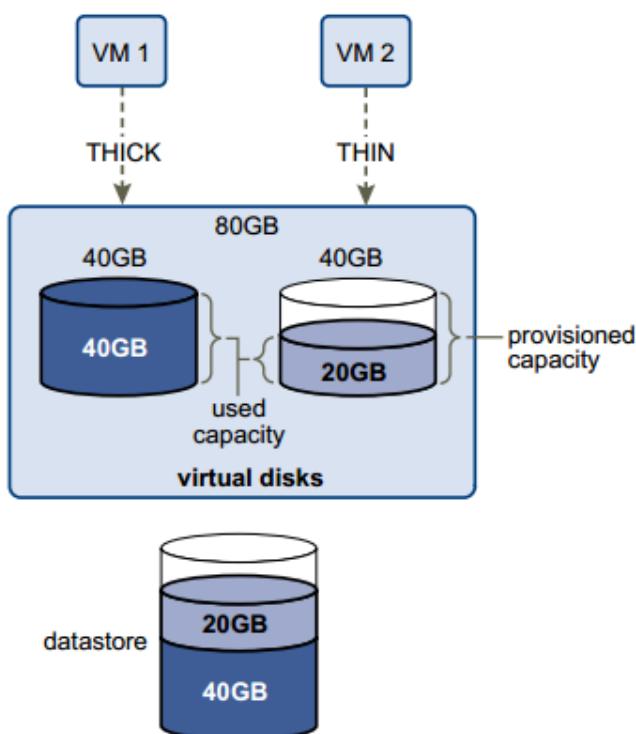
Dependent adapters can use CHAP, which is not the case of Independent adapters.

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.

Image says thousands words... p.254 of vSphere Storage Guide

**Figure 23-1. Thick and thin virtual disks**



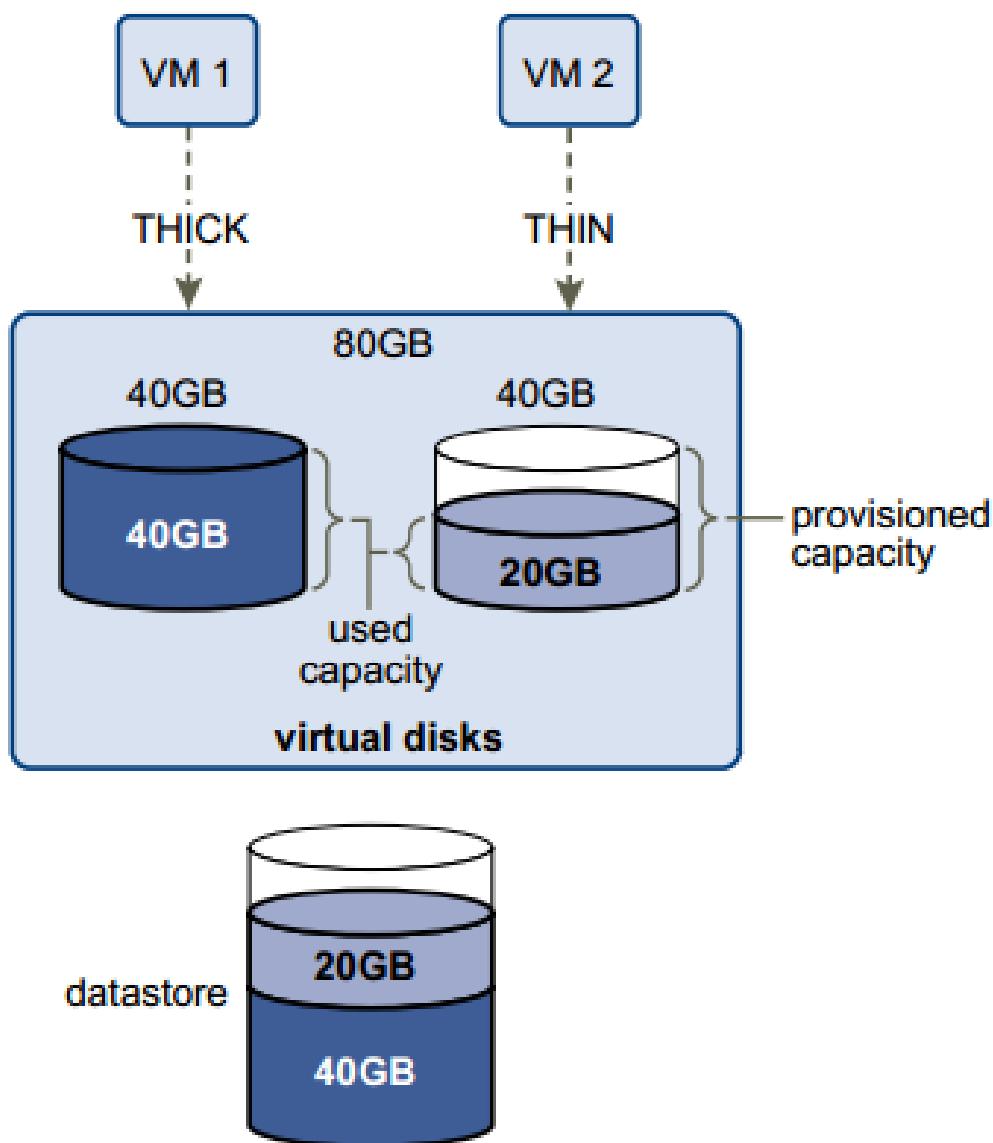
**Thick Lazy Zeroed** – default thick format. Space is allocated at creation, but the physical device is not erased during the creation process, but **zeroed-on-demand** instead.

**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

**Figure 23-1. Thick and thin virtual disks**



## 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 vmlxxxxxxxxxxxxxxx
```

```
[root@esxi6-01:~] esxcli storage core device list -d vml.02000000005e83a971000520d64f435a2d5341
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
```

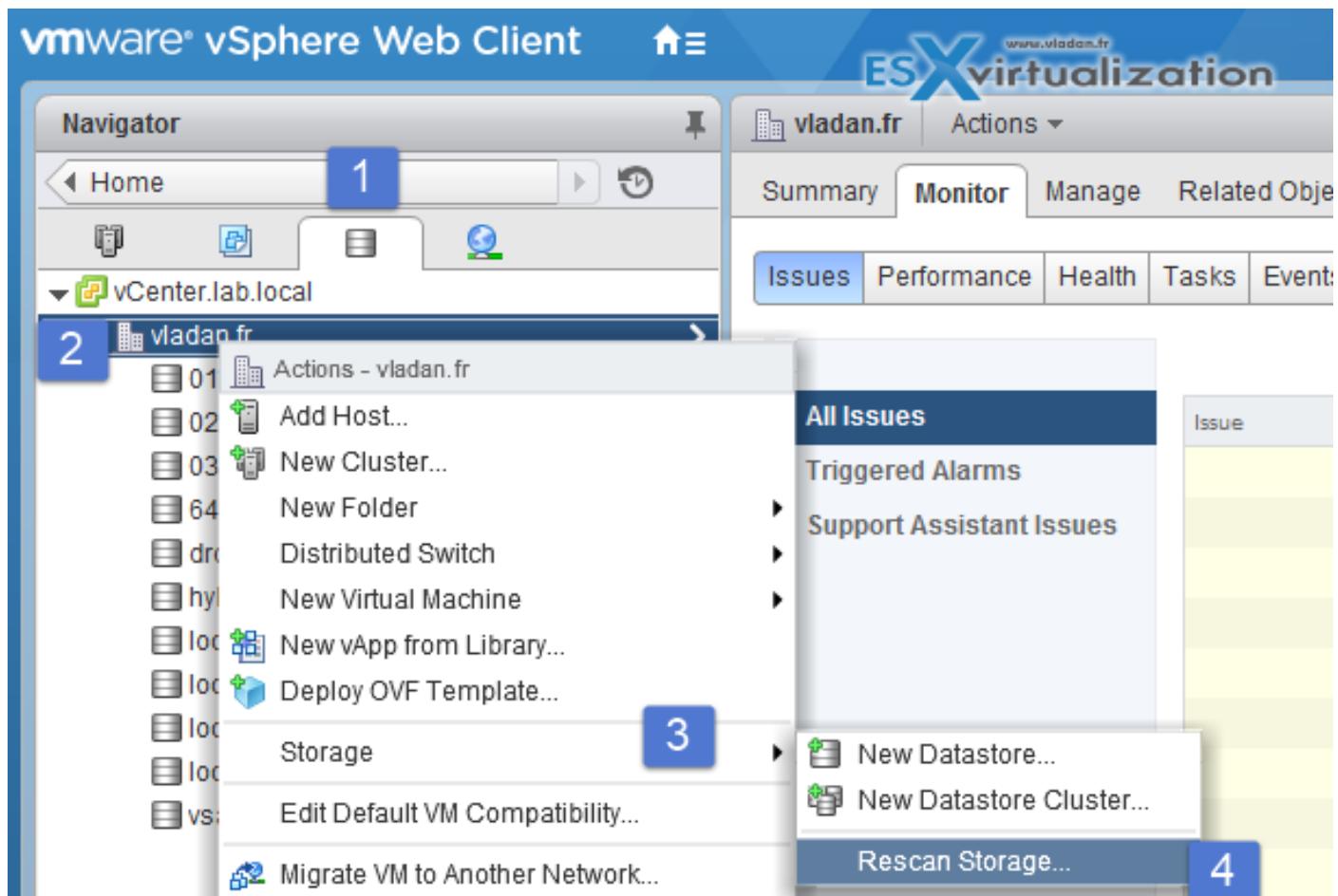
Scan/Rescan storage

Perform the manual rescan each time you make one of the following changes.

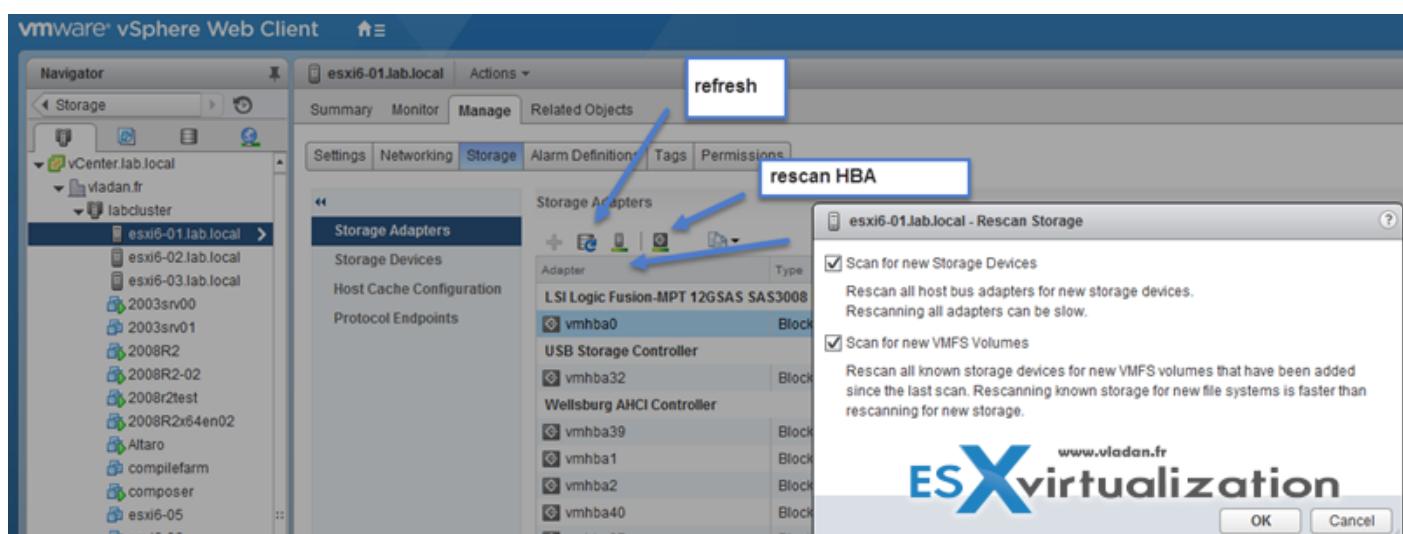
- Zone a new disk array on a SAN.
- Create new LUNs on a SAN.
- Change the path masking on a host.
- Reconnect a cable.
- Change CHAP settings (iSCSI only).
- Add or remove discovery or static addresses (iSCSI only).

- 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.

#### Docs:

- Boot from FC SAN – vSphere Storage Guide on p. 49
- Boot from iSCSI SAN – p.107.
- Boot from Software FCoE – P.55

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:

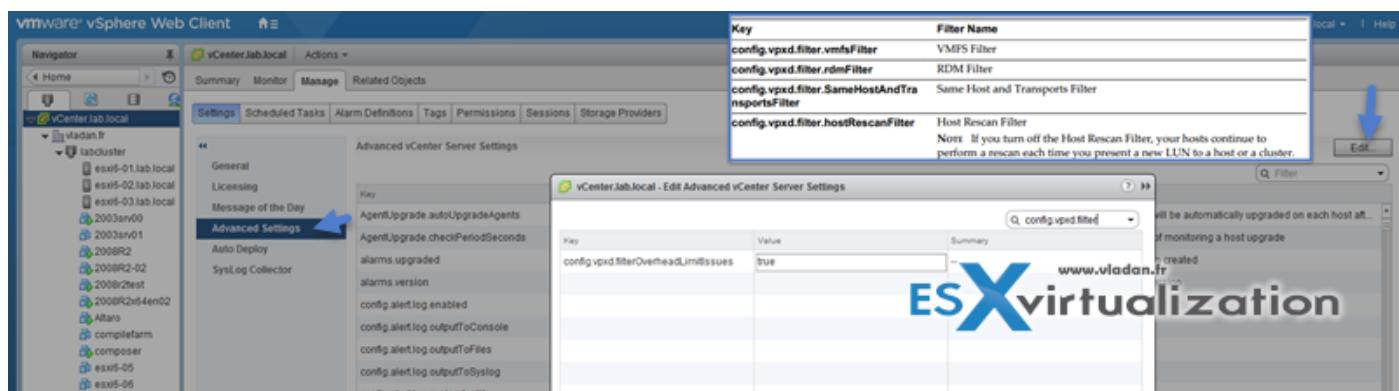
## NFS Protocols and vSphere Solutions

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:

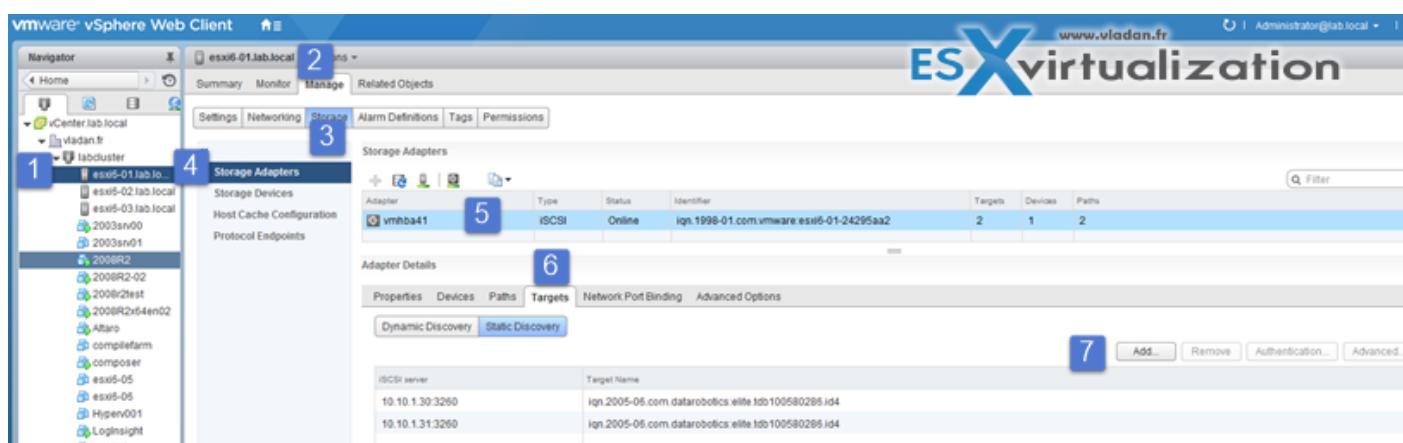
Key	Filter Name
<code>config.vpxd.filter.vmfsFilter</code>	VMFS Filter
<code>config.vpxd.filter.rdmFilter</code>	RDM Filter
<code>config.vpxd.filter.SameHostAndTransportFilter</code>	Same Host and Transports Filter
<code>config.vpxd.filter.hostRescanFilter</code>	Host Rescan Filter
	<b>NOTE</b> If you 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?

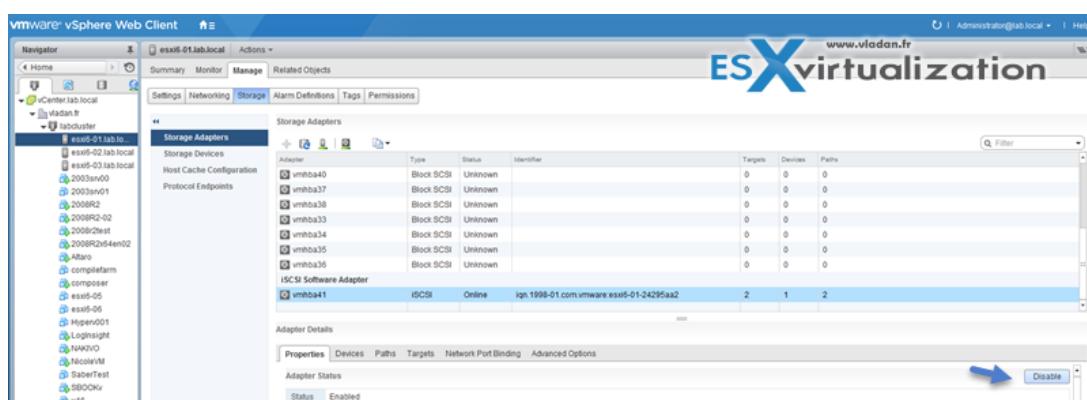
**Host and Clusters > Host > Manage > Storage > Storage Adapters.**

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



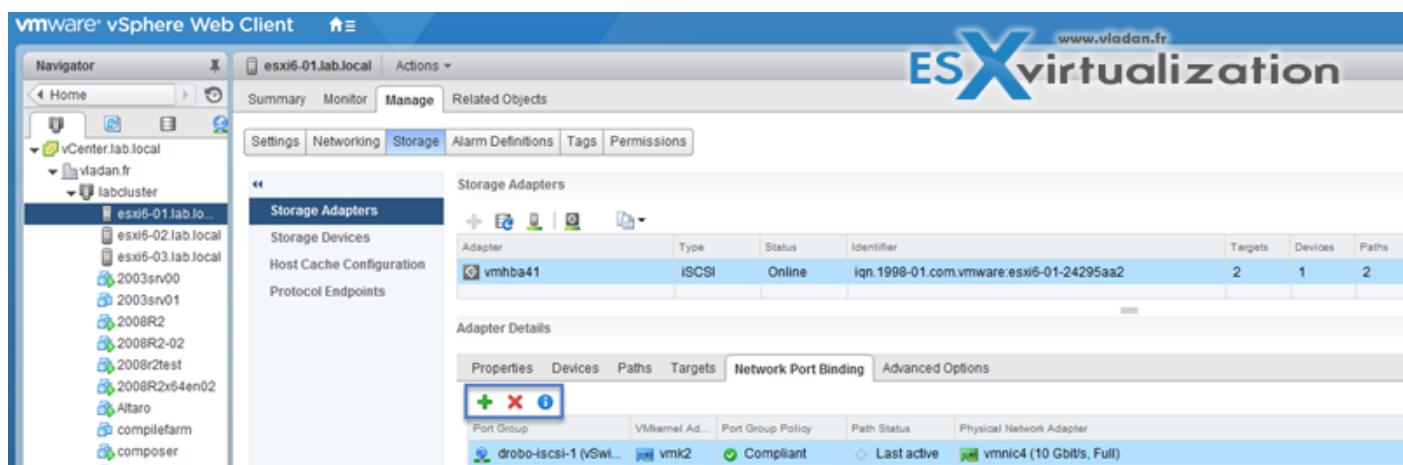
## Configure/Edit software iSCSI initiator settings

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:

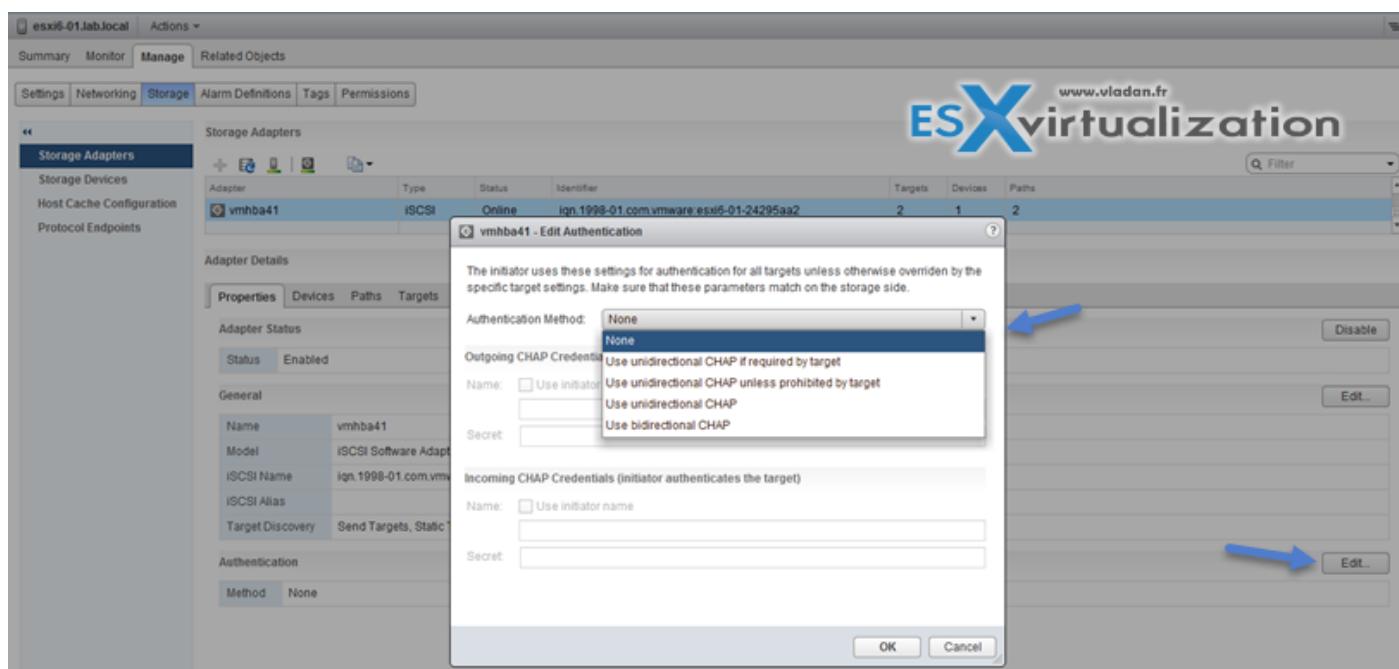
- Array target iSCSI ports are in a different broadcast domain and IP subnet.
- VMkernel adapters used for iSCSI connectivity exist in different broadcast domains, IP subnets, or use different virtual switches.
- Routing is required to reach the iSCSI array.

**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 dependent 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.

## **Objective 7.5 – Create DRS affinity and anti-affinity rules for common use cases**

VMware vSphere has a really good system for configuring different workloads and their requirements. You might have VMs that are meant to stay together on the same host, or you might have VMs that should not be executed on the same host. VMware calls this VM-to-VM affinity and anti-affinity rules.

VMware Distributed Resource Scheduler (DRS) balances and optimizes the VM's performance and DRS score (the DRS score is a measure of the resources available for consumption by the VM). The higher the DRS score for a VM, the better the resource availability for that VM. VMware DRS moves a VM from one host to another to improve this VM DRS score; however, it respects VM-to-VM affinity and anti-affinity rules.

Affinity rules are also respected by VMware High Availability (HA), which does the 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 misposition some VMs that you would not like to have placed there, as you might have a special requirement (separation or keeping together).

For example, if you have an application comprising multiple VMs (web frontend, application server, and database backend), there is likely strong network traffic among these three VMs. So the backend traffic would be quite significant if you allow those VMs to run on different hosts.

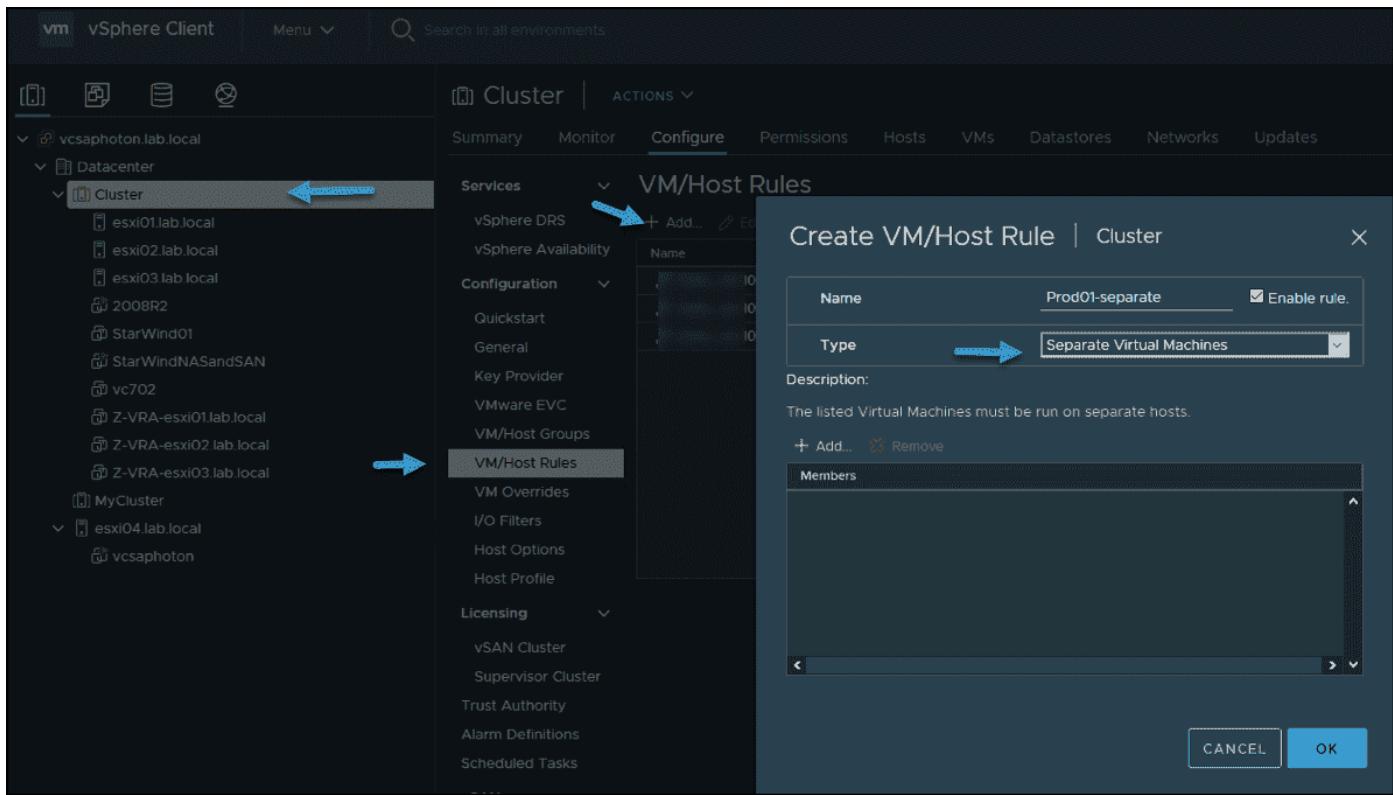
### Common use cases for VM-to-VM affinity and anti-affinity rules

- **Multi-node VMs**—You need to improve the 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 stay on the same host and that 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 each execute on a different host. You can have a database server on one host and a 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. Then select **Configure > VM/Host Rules > Add**.

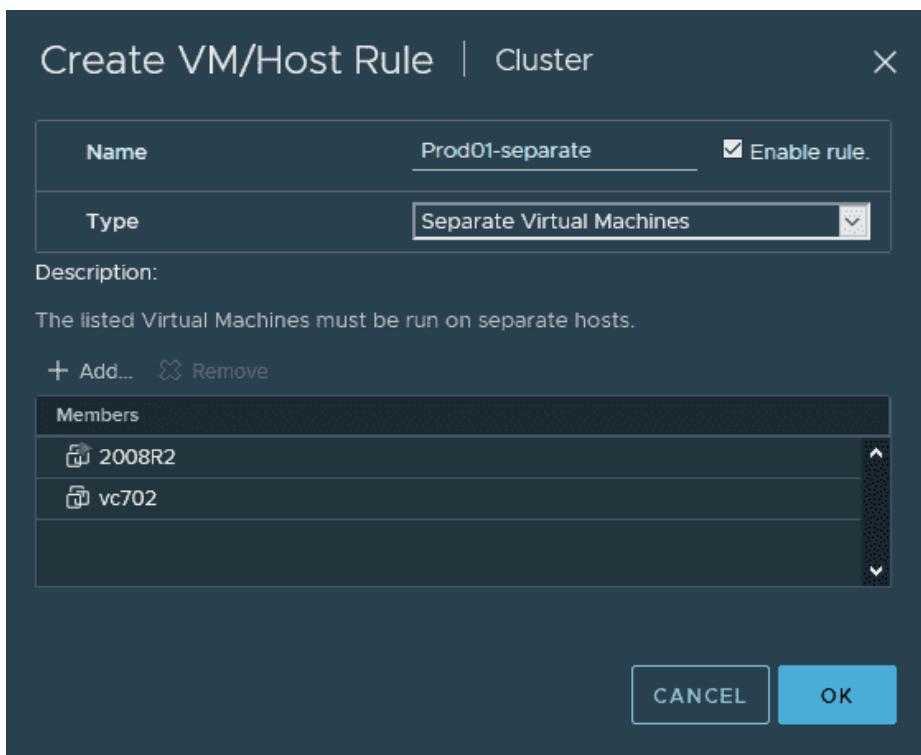
There, you'll see the **Create VM/Host Rule** dialog box. Type a name for the rule.



### Create a 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 the 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.

There are 'required' rules (must) and 'preferential' rules (should).

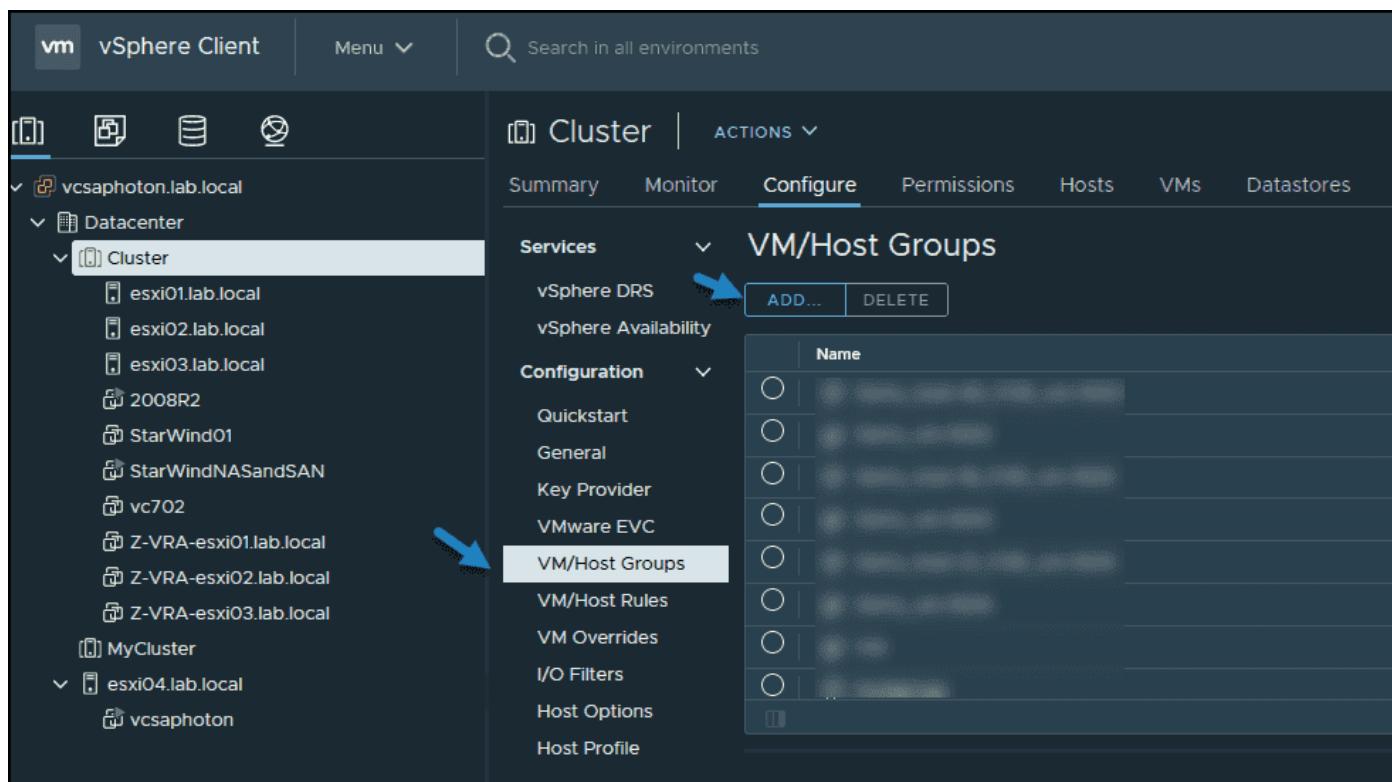
A VM-Host affinity rule basically has three different parts:

- One VM DRS group
- One host DRS group
- A specification if the rule is a requirement (must) or a preference (should), and if it creates an affinity (run on this host) or an anti-affinity (do not run on this host).

These types of rules are usually used when setting up storage appliances, where each one must be attached to a single host. These types of Virtual Storage Appliances (VSAs) are not meant to be migrated or started on other hosts within a cluster.

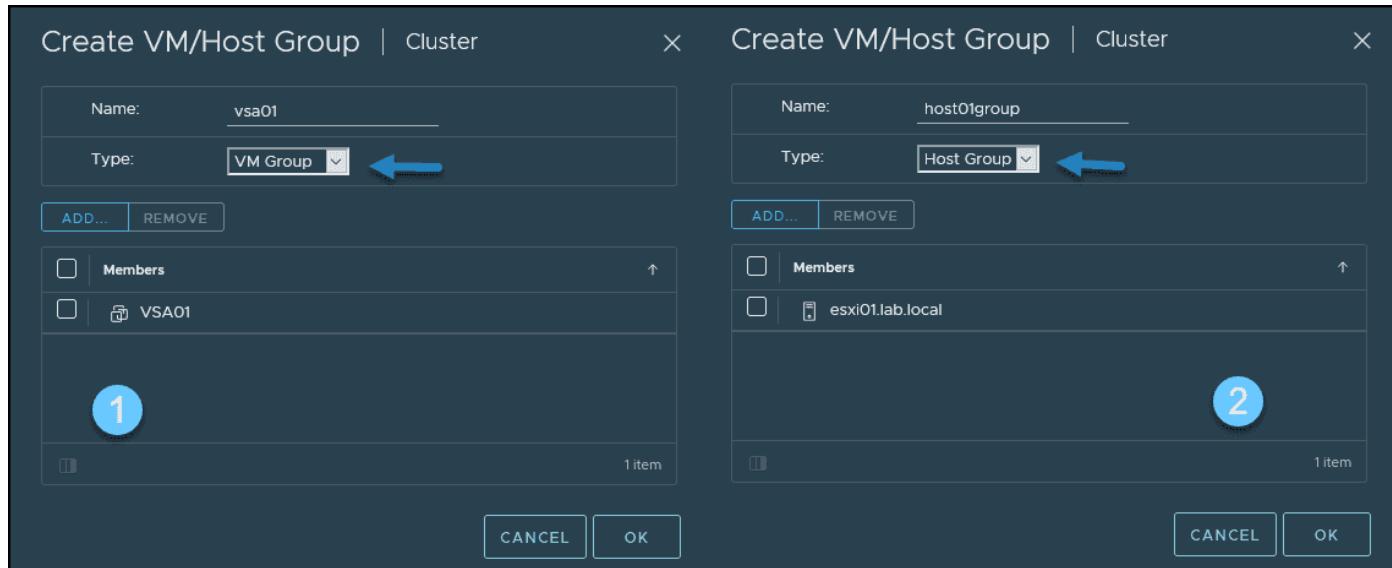
In the example below, we have three VSA VMs (VSA01, VSA02, and VSA03) that run on three different hosts (ESXi01, ESXi02, and ESXi03). We will make sure that each VM always starts and executes on particular hosts.

Select your Cluster. Then select **VM/Host Groups > Add**.



Create two groups

Create two groups in separate steps: a **VM group** and a **host group**.



Create a VM group and a host group

Then go back to the UI VM/Host rules and add a new rule.

For our case, where we need VSA01 to run on ESXi01, we simply pick the **VSA01** group and the **Host01** group that we previously created from the drop-down menu.

Click **Validate** and repeat these steps for the two other VSAs. You should end up with three different rules, like this:

The screenshot shows the 'VM/Host Rules' section of the vSphere Web Client. On the left, there's a sidebar with 'Services' (vSphere DRS, vSphere Availability), 'Configuration' (Quickstart, General, Key Provider, VMware EVC, VM/Host Groups), and 'Licensing' (vSAN Cluster, Supervisor Cluster, Trust Authority, Alarm Definitions). The 'VM/Host Groups' section is currently selected. In the main area, the 'VM/Host Rules' tab is active. It lists several rules: 'Zero\_vm-1002\_TO\_Zero\_host-40\_F...' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User), 'Zero\_vm-1003\_TO\_Zero\_host-19\_F...' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User), 'Zero\_vm-1004\_TO\_Zero\_host-21\_F...' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User), 'Prod01-separate' (Separate Virtual Machines, Enabled Yes, Conflicts 0, Defined By User), 'vsa01-rule' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User), 'vsa02-rule' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User), and 'vsa03-rule' (Run VMs on Hosts, Enabled Yes, Conflicts 0, Defined By User). Below this, the 'VM/Host Rule Details' section shows 'Virtual Machines that are members of the VM Group must run on hosts that are members of the Host Group.' It lists 'vsa01 Group Members' (VSA01) and 'host01group Group Members' (esxi01.lab.local). Blue arrows point from the text descriptions to the respective entries in the lists.

Rules showing the group and the VM

The specification for the rule is as follows:

- **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 hosts 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 is able to handle conflicts between rules. There are two different cases or scenarios.

**There is no possibility of enabling 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 that 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 must 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 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 – Migrate virtual machines

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 definitions. 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.

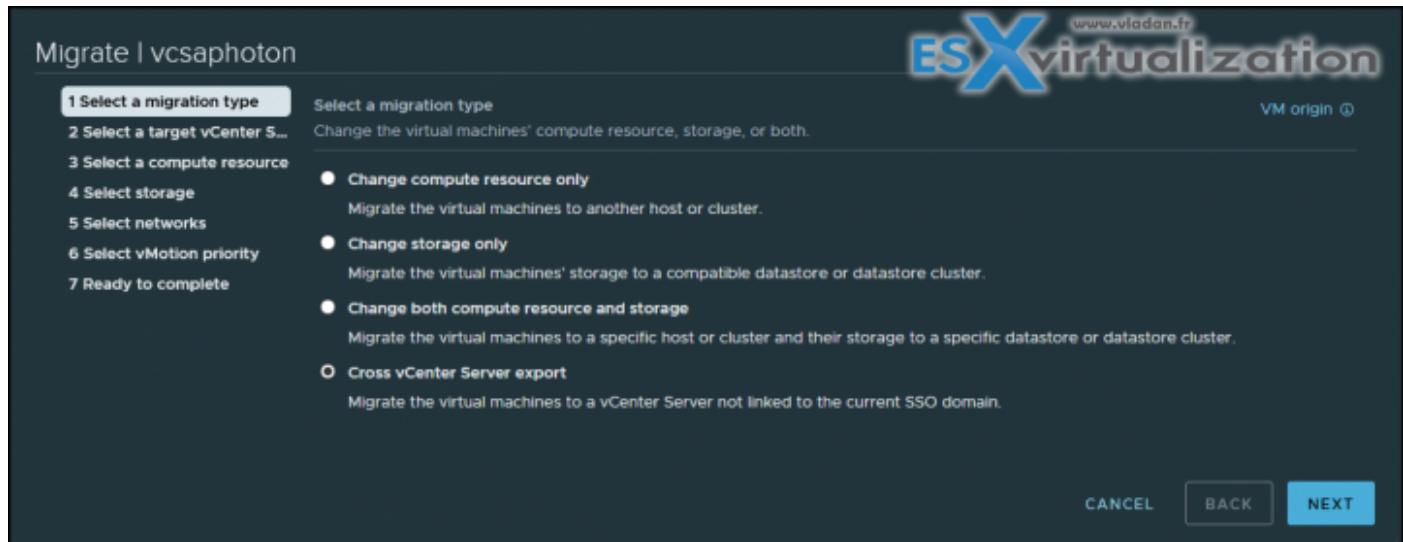
**Cold Migration** – when moving powered-off or suspended VMs to another host, another datastore.

**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 Center 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 bellow 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 GigE 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 Center 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 when VM is 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 7.6.1 – Identify requirements for Storage vMotion, Cold Migration, vMotion, and Cross vCenter Export**

Covered in 7.6

## **Objective 7.7 – Configure role-based access control**

While vCenter Server 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.

vm 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...

Roles

Roles provider: VS SPHERE.LOCAL ▾

+ X

- Content Library administrator (sample)
- Content Library Registry administrator (sample)
- Datastore consumer (sample)
- Network administrator (sample)
- No cryptography administrator
- No Trusted Infrastructure administrator
- NSX Administrator

### 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.

Roles provider: VS SPHERE.LOCAL

No access

AppdApplianceUser

AutoUpdateUser

Clone of No cryptography administrator (sample)

Content library administrator (sample)

Content Library Registry administrator (sample)

Datastore consumer (sample)

Network administrator (sample)

No cryptography administrator

No Trusted Infrastructure administrator

NSX Administrator

NSX Auditor

NSX VI Administrator

Resource pool administrator (sample)

SupervisorService Cluster Operator

SupervisorService Operator

SupervisorService RootFolder Operator

SyncUsers

Tagging Admin

Edit Role

DESCRIPTION USAGE PRIVILEGES

Cryptographic operations

All Cryptographic operations Privileges

Add disk

Clone

Decrypt

Direct Access

Encrypt

Encrypt new

Manage KMS

Manage encryption policies

CANCEL BACK NEXT

### 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:

- 1. System Roles**—These are permanent roles. You are not allowed to edit the privileges associated with these roles.
- 2. 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?

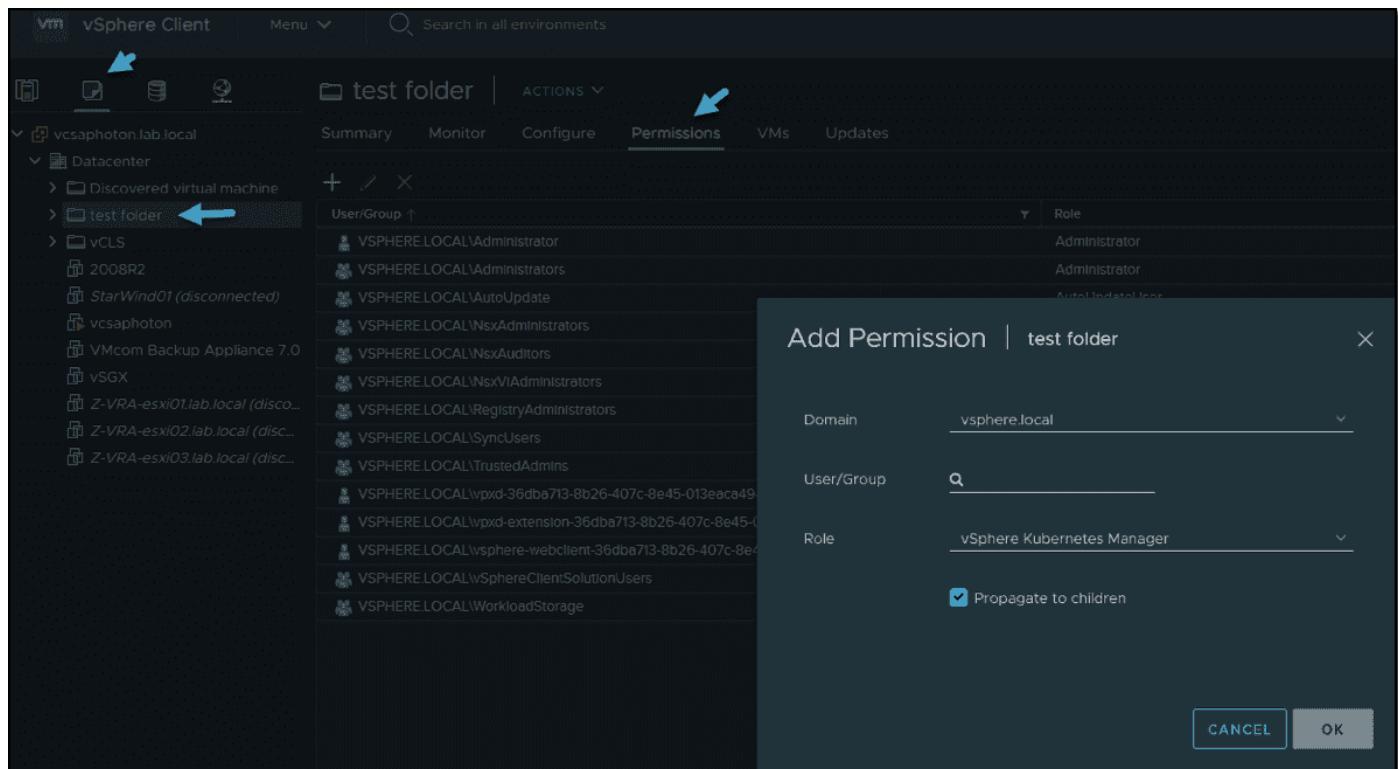
Let's quickly recap the different objects we can find within vCenter Server.

- **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
- Configuration

**Users and Groups**

Users Groups

Domain: vsphere.local

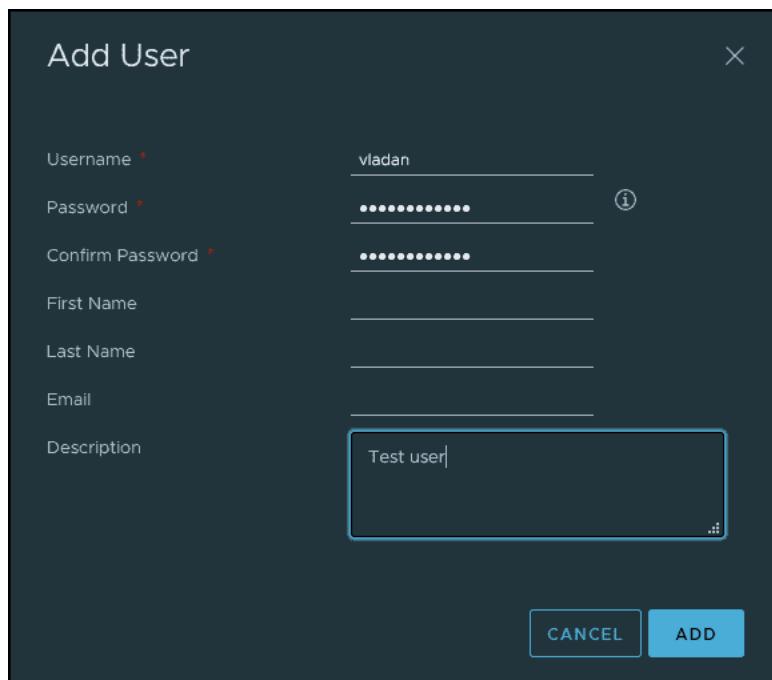
Find:

**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 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 grayed 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 – Manage Host Profiles

Covered in Objective 4.16

## Objective 7.9 – Utilize VMware Lifecycle Manager

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.

### 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. You can see a screenshot from a VMware presentation before the product announce.

The screenshot shows the vSphere Lifecycle Manager (vLCM) interface. On the left, there are two sections: "Add/Remove host" and "Drift management".

- Add/Remove host:**
  - ADD Host:** NSX Manager will update the TNP (Transport node profile). vLCM will automatically start the remediation and install NSX-T bits to newly added ESXi host.
  - Remove Host:** NSX manager will remove the TNP (Transport node profile). vLCM will un-install NSX-T bits.
- Drift management:** NSX manager now gets the feedback from vLCM if there is any drift with respect to NSX components. NSX manager also has the capability to **Resolve** the same. Resolve will trigger vLCM remediation tasks and will ensure that NSX-T bits are in desired state.

In the center, there is a table titled "NSX Configuration" showing the status of host remediation:

Host	Status	Progress	Details
Applying Profile: nsx-basic...	U	48%	Waiting for connection
48% vLCM remediation i...	U	23%	vLCM remediation initiated

To the right, a "Installation Progress" window is open, showing the following steps:

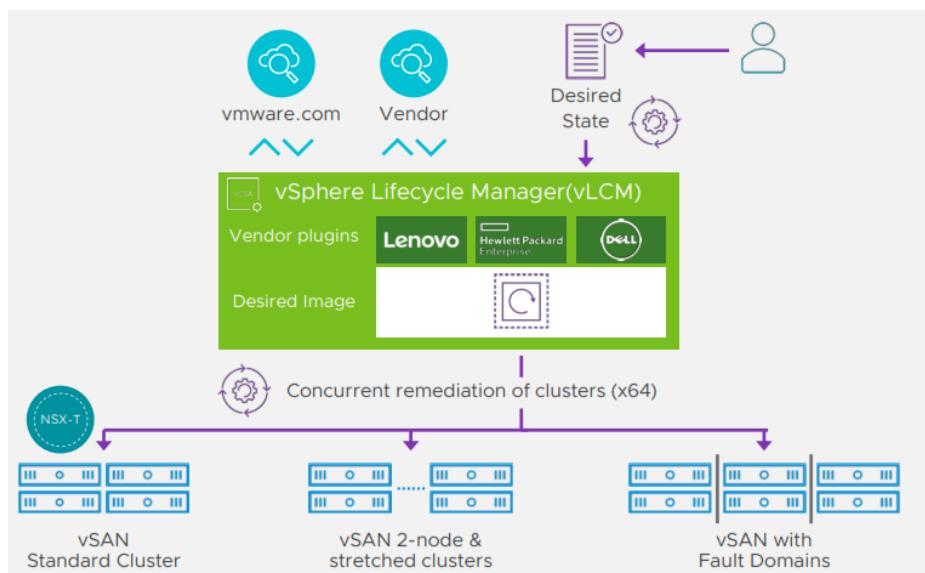
- ✓ Preparing Installation
- ⌚ vLCM remediation initiated
- vLCM remediation successful
- Registering Host
- Waiting for connection to Managers
- Applying NSX switch configuration
- Enabling host status in controller
- Updating host status
- Configuration complete

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 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. Those 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 7.9.1 – Describe firmware upgrades for VMware ESXi

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 7.9.2 – Describe VMware ESXi Updates

Covered in Objective 5.9.2

## Objective 7.9.3 – Describe component and driver updates for VMware ESXi

Covered in Objective 7.9.1

## Objective 7.9.4 – Describe hardware compatibility check

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).

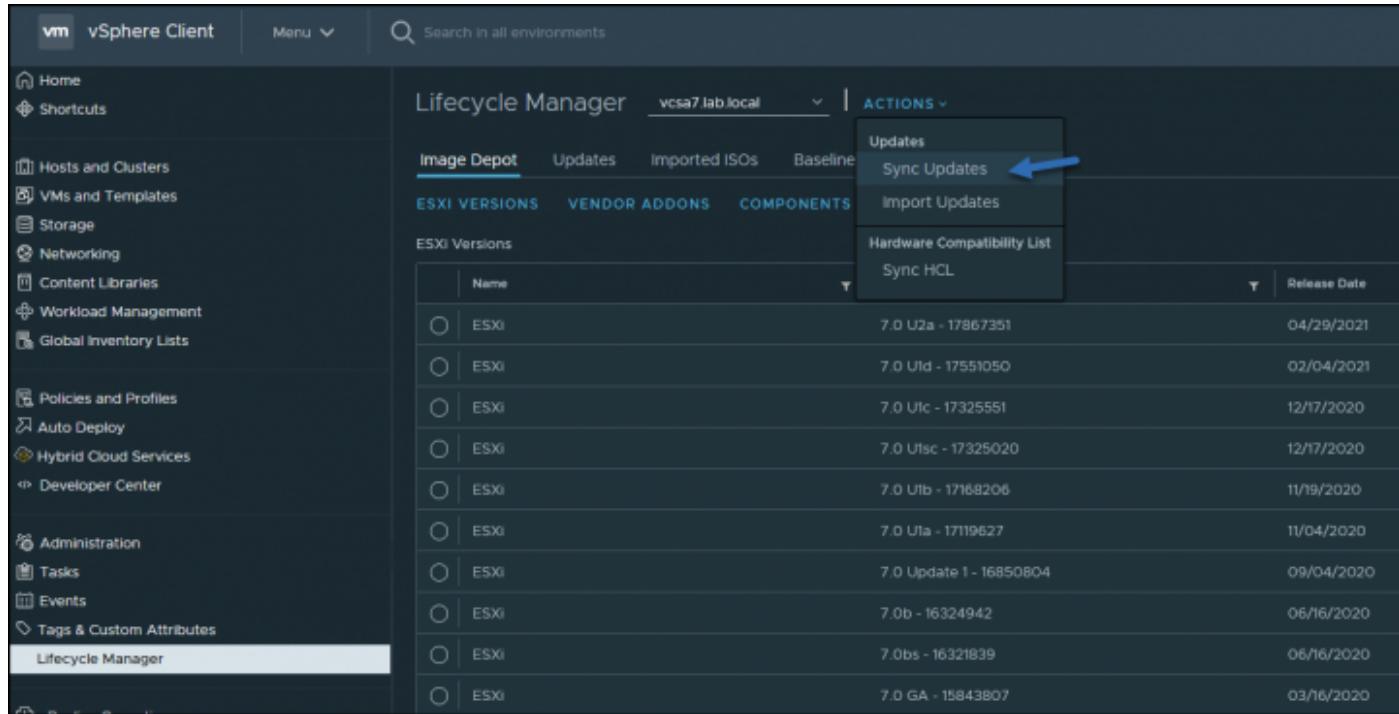
The hardware compatibility check that you initiate for a single host check whether the server and the physical devices on the host are Certified for use with a selected ESXi version. The check is performed against the VCG.

**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

1. In the vSphere Client, navigate to a standalone host or a host in a cluster.
2. On the Updates tab, select Hosts > Hardware Compatibility.
3. 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.



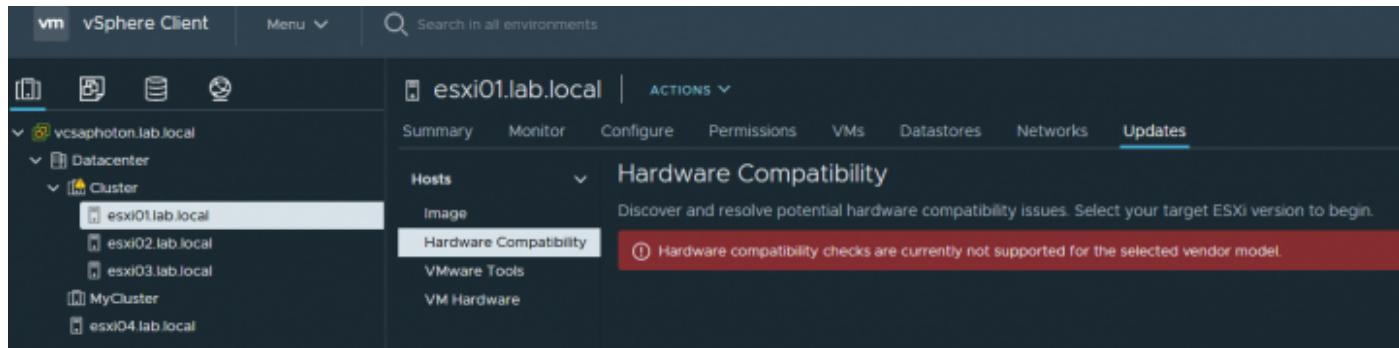
The screenshot shows the vSphere Client interface with the 'Lifecycle Manager' tab selected in the sidebar. The main pane displays a table of ESXi versions with columns for Name, Version, and Release Date. A context menu is open over the first row, with 'Sync Updates' highlighted and a blue arrow pointing to it. The table data is as follows:

Name	Version	Release Date
ESXi	7.0 U2a - 17867351	04/29/2021
ESXi	7.0 Ufd - 17551050	02/04/2021
ESXi	7.0 Ufc - 17325551	12/17/2020
ESXi	7.0 Usfc - 17325020	12/17/2020
ESXi	7.0 Ulb - 17168206	11/19/2020
ESXi	7.0 Ula - 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 ....



The screenshot shows the vSphere Client interface with the 'esxi01.lab.local' host selected. The 'Updates' tab is active in the top navigation bar. The 'Hardware Compatibility' section is displayed, showing a message: 'Discover and resolve potential hardware compatibility issues. Select your target ESXi version to begin.' Below this, a red banner states: 'Hardware compatibility checks are currently not supported for the selected vendor model.' The left sidebar shows the host structure under 'vcsaphoton.lab.local'.

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 7.9.5 – 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.

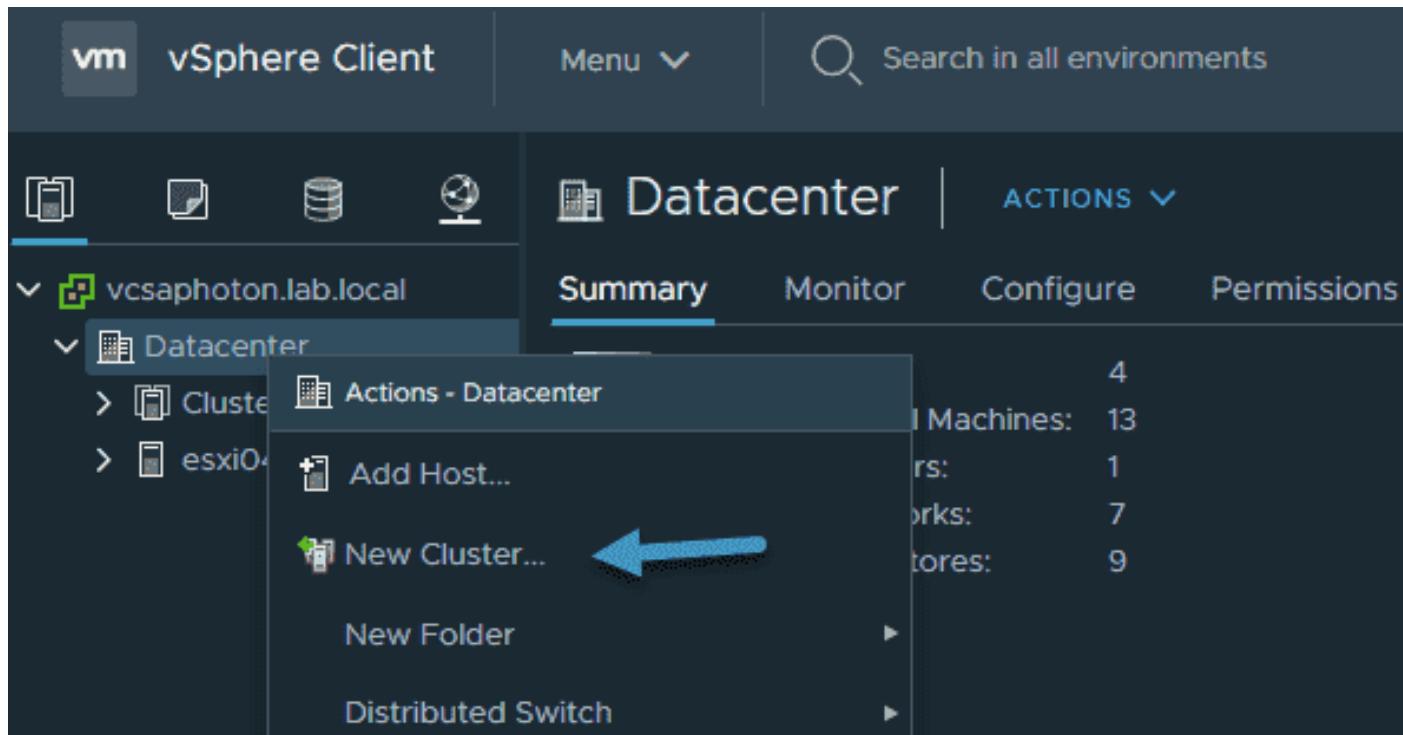
ESXi with cluster imaging allows you to maintain a consistent configuration across infrastructure by bundling an ESXi base image with firmware, vendor, and driver add-ons.

### The requirements

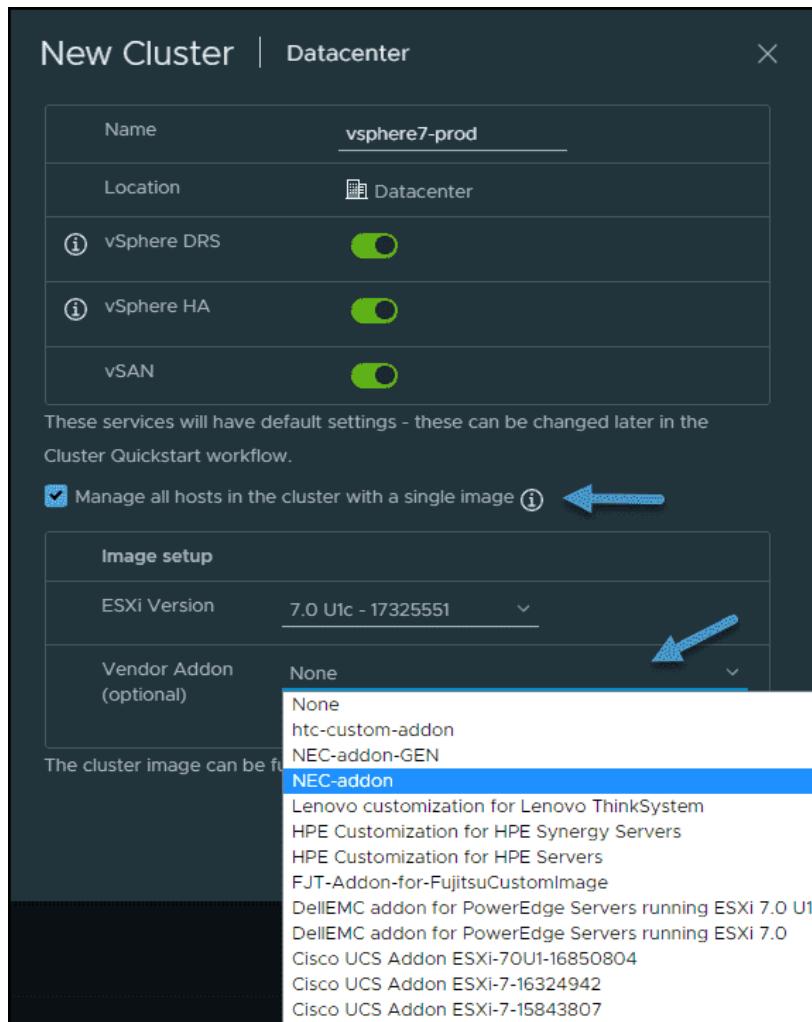
- ESXi and vSphere.
- Within your inventory, you'll have to have a datacenter cluster. Normally it's obvious, but make sure they have been created.
- All ESXi hosts must be on the same version.
- You must know the ESXi root account password.

### 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.



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**.



**Note:** The vendor add-on is optional. You may use this perfectly well without the server on the list too.

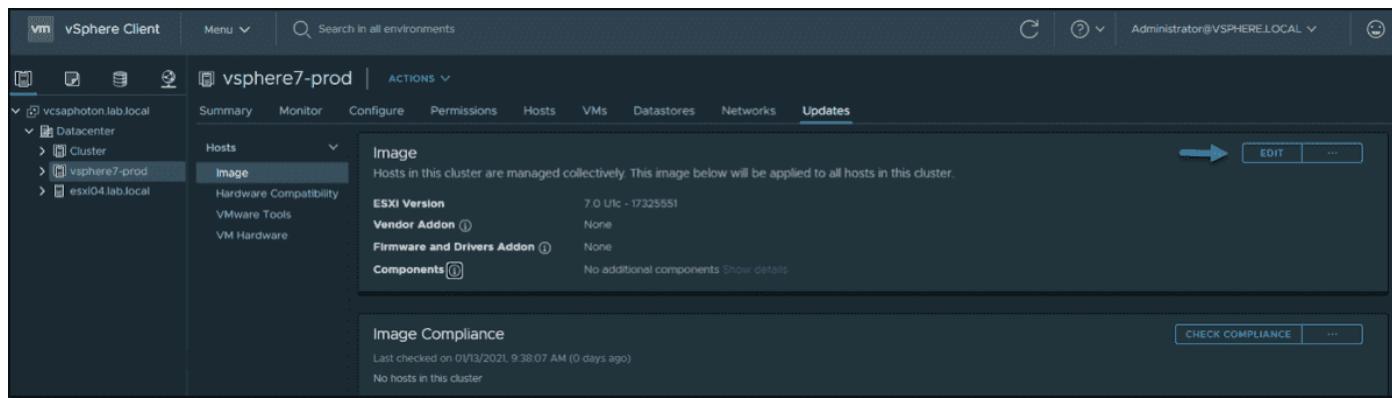
## The ESXi images have four elements

**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.

The screenshot shows the vSphere7-prod cluster management interface. The 'Updates' tab is active. On the left, there's a sidebar with 'Hosts' expanded, showing 'Image' selected. The main content area has two sections: 'Image' and 'Image Compliance'. The 'Image' section displays ESXi version 7.0 Utc - 17325551, Vendor Addon (None), Firmware and Drivers Addon (None), and Components (None). The 'Image Compliance' section shows it was last checked on 01/13/2021 at 9:54:24 AM (0 days ago) and no hosts in this cluster. A context menu is open over the 'Image' section, with an arrow pointing to the 'Export' option in the list.

You can export the ESXi 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.

The screenshot shows the 'Export Image' dialog box. It contains three radio button options: 'JSON' (selected), 'ISO', and 'ZIP (offline bundle)'. Each option has a description below it. At the bottom are 'CANCEL' and 'EXPORT' buttons.

Format	Description
<input checked="" type="radio"/> JSON	Download the image as a JSON file that can be imported into other clusters managed by images. Note that this only contains metadata about the image, not the actual software packages.
<input type="radio"/> ISO	Download an installable ISO from the image to reuse this in other clusters managed using Baselines, or to image new hosts.
<input type="radio"/> ZIP (offline bundle)	Download a ZIP offline bundle that contains all components (software packages) included in this image that can be imported into Lifecycle Manager's depot.

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 7.9.6 – Create VMware ESXi cluster image

Covered in 7.9.5

## Objective 7.10 – Use predefined alarms in VMware vCenter

The vSphere 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.

Sphere 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 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. On the left, the navigation tree is expanded to show the datacenter 'vcsaphoton.lab.local' and its clusters: 'esxi01.lab.local', 'esxi02.lab.local', 'esxi03.lab.local', 'MyCluster', and 'esxi04.lab.local'. The main pane is titled 'Alarm Definitions' under the 'Configure' tab. A dropdown menu on the left lists various configuration options like General, Licensing, and Security. The 'Security' section is currently selected. The main area displays a table of existing alarms, each with an icon, alarm name, object type, and a status indicator. At the top of the table area, there are four buttons: 'ADD', 'EDIT', 'ENABLE/DISABLE', and 'DELETE'. A blue arrow points to the 'ADD' button.

	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	

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.

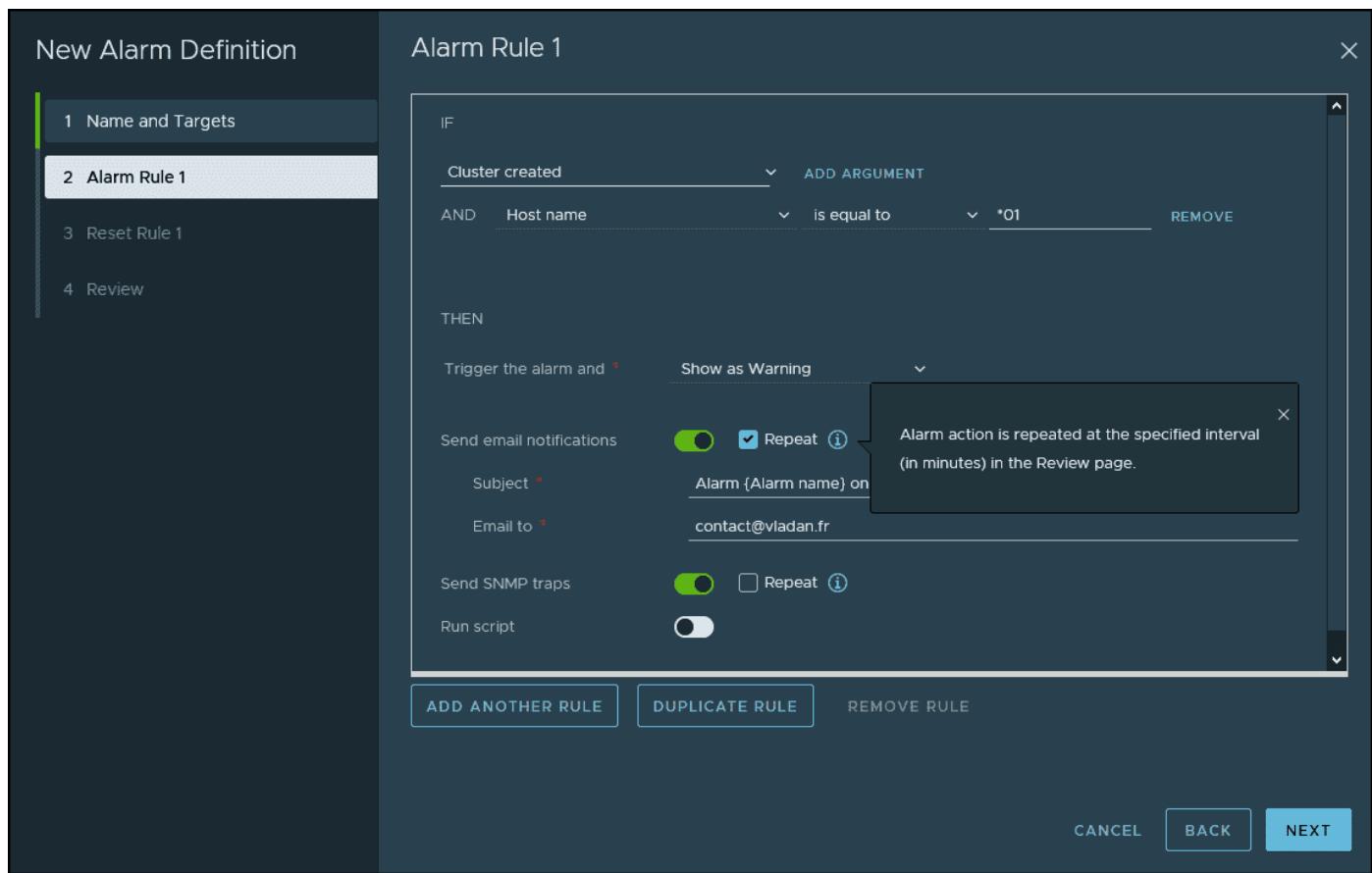
The screenshot shows the 'New Alarm Definition' wizard. The left sidebar lists steps: 1. Name and Targets, 2. Alarm Rule 1, 3. Reset Rule 1, and 4. Review. The main panel is titled 'Name and Targets'. It has fields for 'Alarm Name' (set to 'myNewAlarm') and 'Description'. Below these is a 'Targets' section with a 'Target type' dropdown. The dropdown menu is open, showing a list of target types: vCenter Server, Virtual Machines, Hosts, Clusters, Datacenters, Datastores, Distributed Switches, Distributed Port Groups, Datastore Clusters, and vCenter Server. The 'vCenter Server' option is highlighted with a blue background. At the bottom right are 'CANCEL' and 'NEXT' buttons.

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**.

New Alarm Definition

1 Name and Targets

2 Alarm Rule 1

3 Reset Rule 1

4 Review

Alarm Rule 1

IF

VM VCPUs Usage is above 90 % for 25 min

ADD ADDITIONAL TRIGGER

THEN

Show as Critical

Send email notifications (OFF)

Send SNMP traps (OFF)

Run script (OFF)

Select an advanced action (SELECT)

Migrate VM

Power off VM

Power on VM

Reboot guest on VM

Reset VM

Shutdown guest on VM

Suspend VM

CREATE RULE REMOVE RULE

CANCEL BACK NEXT

### 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.

New Alarm Definition

1 Name and Targets

2 Alarm Rule 1

3 Reset Rule 1

4 Review

Reset Rule 1

Reset the alarm to green (ON)

CANCEL BACK NEXT

### 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.

New Alarm Definition

Review

Alarm Name: myNewAlarm

Description:

Targets: All Clusters on vcsaphoton.lab.local (2)

Alarm Rules:

```

IF Cluster created
THEN Trigger the alarm as Critical
Send emails to contact@vladan.fr
with subject Alarm {Alarm name} on Cluster : {Target Name} is {New status}
Send SNMP traps

```

Enable this alarm

CANCEL BACK CREATE

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.

vcsaphoton.lab.local | ACTIONS ▾

Summary Monitor Configure Permissions Datacenters Hosts & Clusters VMs Datastores Networks

**Settings** ▾ **Alarm Definitions**

**ADD** **EDIT** **DISABLE** **DELETE**

	Alarm Name	Object type	Defined In
● >	myNewAlarm	Cluster	This Object
○ >	Skyline Health has detected issues...	vCenter Server	This Object
○ >	vSAN cluster alarm 'vSAN Direct h...	Cluster	This Object
○ >	Identity Source LDAP Certificate is ...	Host	This Object
○ >	Trusted Host Attestation Failed AI...	Host	This Object
○ >	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.

## **Objective 7.11 – Create custom alarms**

Covered in 7.10

## **Objective 7.12 – Deploy an encrypted virtual machine**

- 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

### **Objective 7.12.1 – Convert a non-encrypted virtual machine to an encrypted virtual machine**

#### **Prerequisites**

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Ensure that the virtual machine is powered off.
- Make sure your host has TPM v2 installed and it supports encryption

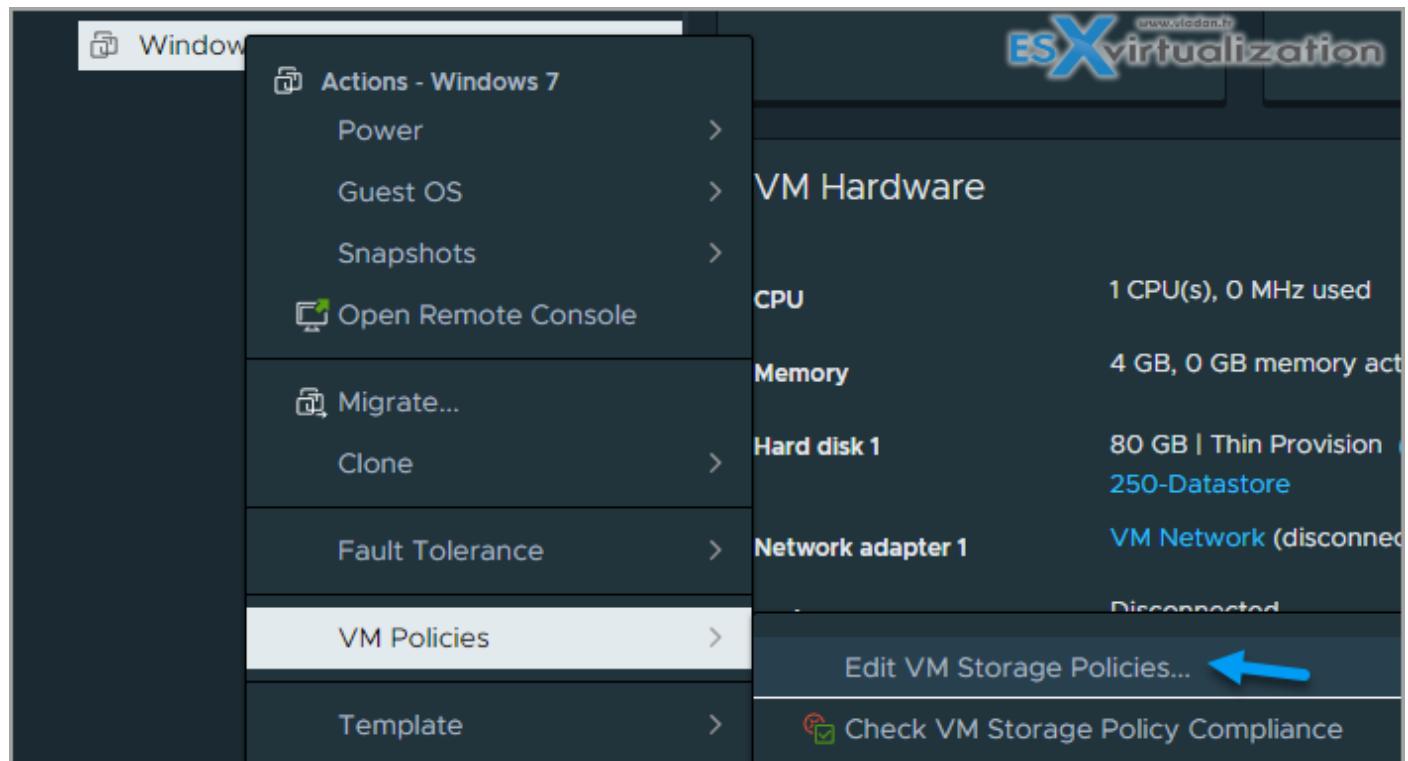
Host encryption mode must be set if you want to perform encryption tasks, such as creating an encrypted virtual machine, on an ESXi host. In most cases, host encryption mode is activated automatically when you perform an encryption task

Check that you have the required privileges:

- *Cryptographic operations.* Encrypt new
- If the host encryption mode is not Enabled, you also need Cryptographic operations. Register host.

Log in vSphere Client, and connect to vCenter Sever.

Right-click the virtual machine you want to encrypt, and select VM Policies > Edit VM Storage Policies.



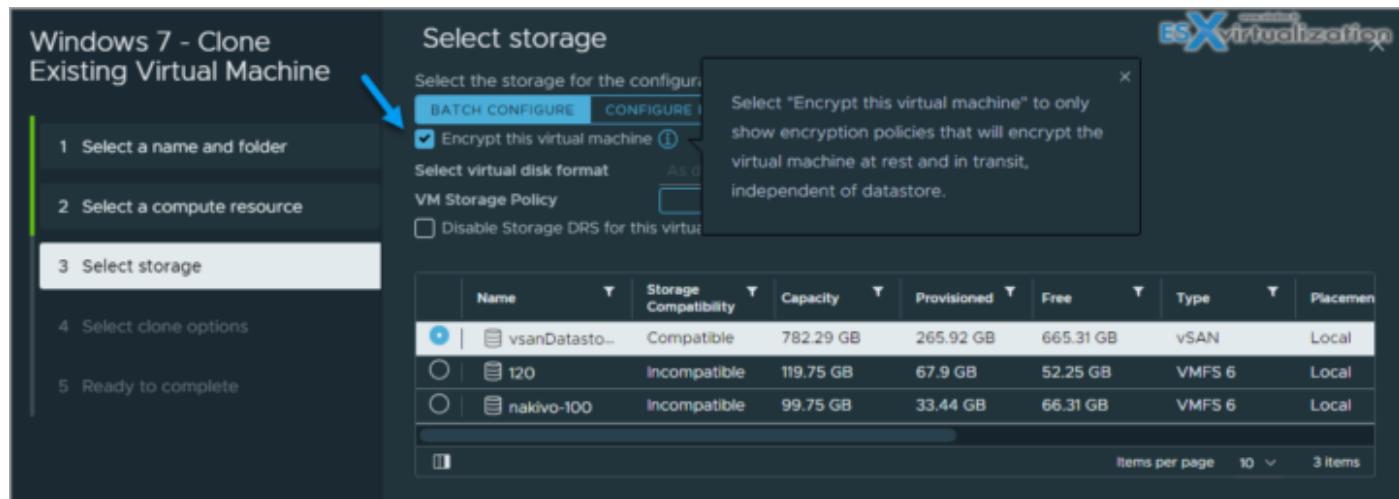
In VM storage policy, select VM Encryption Policy. Click OK.

You can use per-disk configuration too...



Click OK.

You can also make a clone of your VM and during the process you can check the box «Encrypt this virtual machine».



## Objective 7.12.2 – Migrate an encrypted virtual machine

Many admins might think that encrypted vMotion is something that they don't really need in their datacenter. However, when you're using vMotion across hybrid or across public clouds, you leave your door open to threats. IT admins can protect critical VM data traveling across long distance and public clouds via a simple way in vSphere 7.

It is important to secure sensitive vMotion traffic at the network endpoints. This protects critical VM data when the vMotion traffic leaves the traditional IT environment and goes over the public networks.

Encrypted vMotion can make the process more secure with small effort from the admin in vSphere 7. No need for KMS if that's your main concern. You'll only need a vCenter server without any other software component installed.

The encryption keys that are used for the vMotion are ephemeral and not stored anywhere. They are present only temporarily in the memory of vCenter Server and the two ESXi hosts that are selected for the vMotion operation.

### What is encrypted vMotion?

This feature has been introduced in vSphere 6.5 and uses end-to-end encryption for vMotion network traffic. You don't need any additional hardware devices or hardware reconfiguration to configure and use encrypted vMotion in vSphere 7.

Encrypted vMotion encrypts all the data travelling across your VMkernel adapter and uses AES-GCM encryption. vSphere supports encrypted vMotion of unencrypted and encrypted virtual machines across vCenter Server instances.

When using encryption on a VM level and your VMDKs are encrypted, you can use storage vMotion. However, to set up a VM encryption, you'll need to use a Key Management Server (KMS) as your VMDKs must be encrypted for storage vMotion.

### Different encrypted vSphere 7 vMotion States

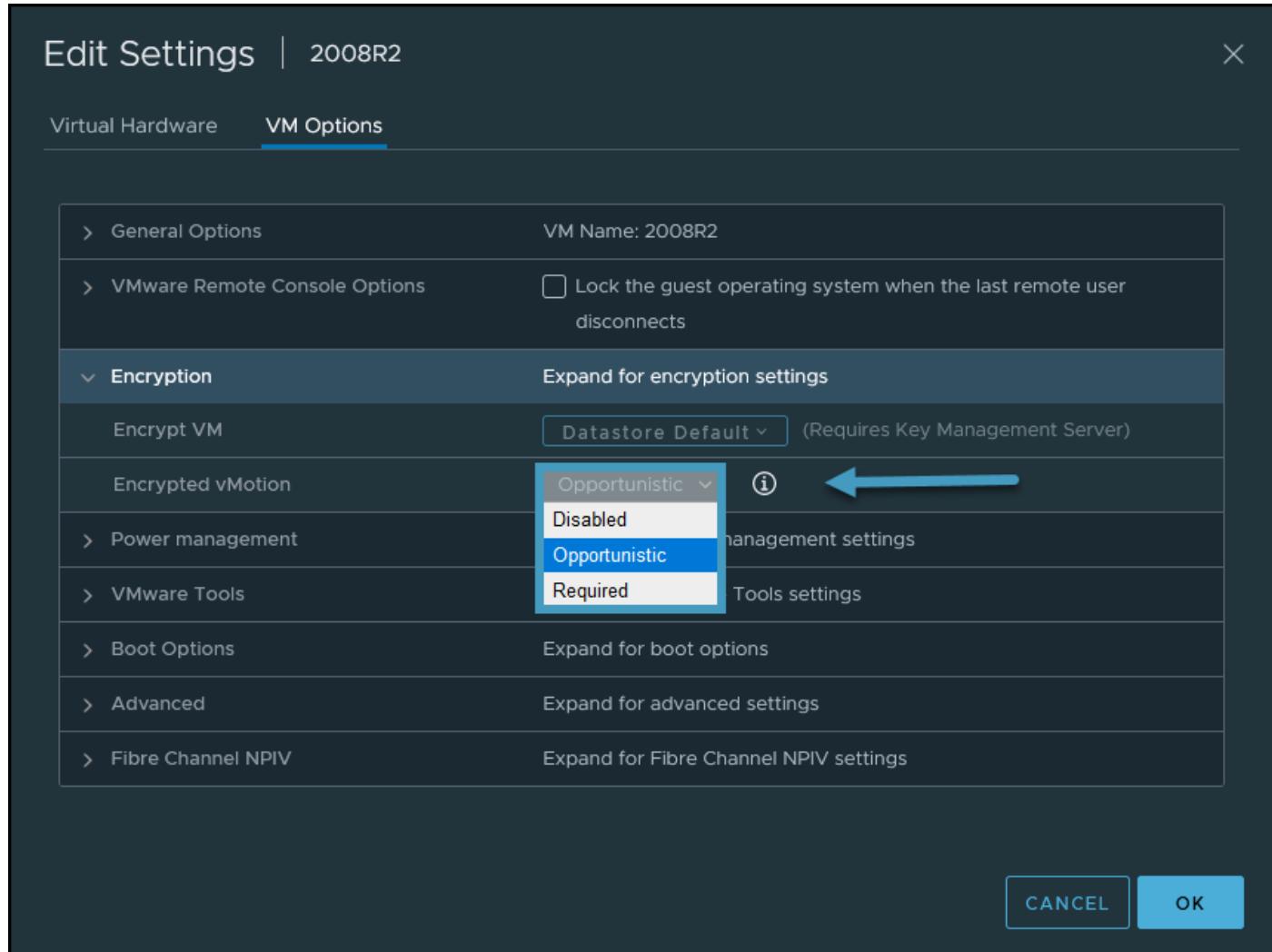
You should know that when setting up a vMotion, there can be 3 different encrypted vMotion states:

- **Disabled** – Do not use encrypted vSphere vMotion.
- **Opportunistic** – Use encrypted vSphere vMotion if source and destination hosts support it. Only ESXi versions 6.5 and later use encrypted vSphere vMotion, so if you have still some vSphere 6.0 hosts, they won't be able to be used as a destination.
- **Required** – Allow only encrypted vSphere vMotion. In this case, if the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

**Note:** If you're using VM encryption on some of your VMs, those VMs are automatically vMotioned with encrypted vMotion.

### Where to enable or disable encrypted vMotion in vSphere 7?

This is done at the VM level and your VM has to be turned OFF. Go and select your **VM > Edit Settings > VM Options > Encryption**. Here, select Encrypted vMotion from the drop-down menu.



## Objective 7.12.3 – Configure virtual machine vMotion encryption properties

Covered in 7.12.2