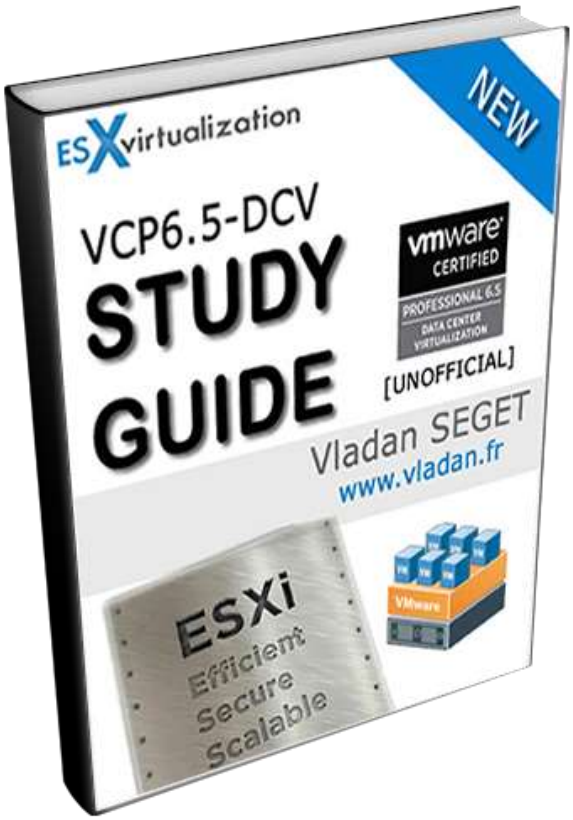
VCP6.5-DCV STUDY GUIDE

[UNOFFICIAL]

By Vladan SEGET
www.vladan.fr



NAKIVO Backup & Replication

Fast, Reliable, and Affordable Data Protection Solution for VMware, Hyper-V, and AWS EC2 Environments

Used by over 10,000 companies worldwide

97.3% customer satisfaction

Priced from $149 per socket

Download Free Trial

Choose NAKIVO Backup & Replication to benefit from:

- ✓ Variety of deployment options (install on Windows, Linux, and a NAS; deploy as a VMware VA, AWS AMI)
- ✓ Up to 2X higher backup speed with incremental backups, CBT/RCT, LAN-free data transfer, and Network Acceleration
- ✓ Up to 90% storage space savings achieved by automated exclusion of swap data, deduplication, and compression
- ✓ Guaranteed recovery with automated Screenshot Verification of VM backups and replicas
- ✓ Near-instant recovery of VMs, files/folders, and application objects (Microsoft Exchange, SQL Server, Active Directory)

Download the full-featured Free Trial

TABLE OF CONTENTS:

The exam has **70 Questions** (single and multiple choices), **passing score 300**, and you have **105 min** to complete the test. Price: **$250.** Wish everyone good luck with the exam.

Please check the vSphere 6.5 documentation (online or PDF) for further study. Our little contribution to learning towards successful pass of the VCP 6.5-DCV certification exam shall be helpful, but **don't rely only on our guide...**

I highly recommend getting all the PDFs when studying for the exam.

The VMware Datacenter exam has become more and more difficult to master because the volume of knowledge is higher. But I'm sure that many of you will succeed. And if you don't pass on your first time, don't get discouraged as you can take this as a learning experience and be successful the second time.

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

The VMware VCP6.5-DCV certification is one of the first bricks for other, more advanced VMware certification exams. Those are the VMware Advanced Professional (VCAP6.5-DCV Design) and the VMware Certified Design Expert (VCDX6-DCV).

There are separate certification paths for cloud management and automation (VCP-CMA), network virtualization (VCP-NV), and desktop and mobility (VCP-DTM). Note that there are also associate-level certifications available which are the easiest exams, and are required to pass VCP6.5-DCV.

VCP6.5-DCV Objective 1.1 Configure and Administer Role-based Access Control

This is the first VCP6.5-DCV Objective 1 from the exam guide for preparation for VMware VCP6.5-DCV Datacenter virtualization exam. Find all exam topics directly on our new VCP6.5-DCV Study Guide Page. Note that it is a work in progress which started just recently so we need to add more content to it.

VMware certification exam is important to have when you start with the IT, data center administration. It's important to have it on your CV, but that's not all.

During your career, you'll certainly need to study further. Stay up to date with the knowledge. It's a continuous process where the next step for some is VCAP, while for others even VCDX as an ultimate VMware certification.

Note that VCP certs expire after 2-3 years, where VCAPs don't. This might also be a reason to continue to study and pass a higher, more difficult exam. VCAP 6.5 - design and (or) VCAP 6.5 deploy exams are the ones you might wish to pass after passing your VCP.

VCP6.5-DCV Objective 1 - Configure and Administer Role-based Access Control.

Compared to the VCP6-DCV Study guide, this chapter is a little bit more demanding, with more topics to cover.

Compare and contrast propagated and explicit permission assignments

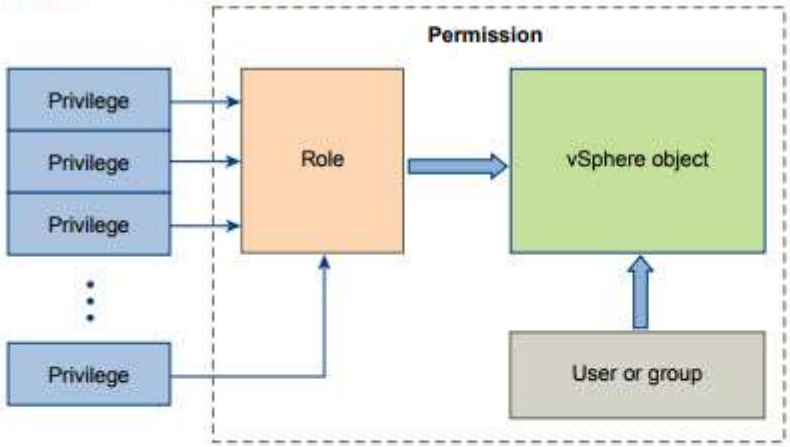
To check the propagated and explicit permission assignments, we have to connect to our vCenter server > Global Administration. But before doing this, it's important to know the difference between Permissions and Users and Groups.

- **Permissions** - each object in the vCenter hierarchy has associated permissions. Each permission
- **Privileges** - access controls to the resource. You group privileges into roles, which are mapped to users or groups.
- **Users and groups** - pretty obvious. Only users authenticated through Single Sign-ON (SSO) can be given some privileges. Users must be defined within the SSO or users from external identity sources such as Microsoft AD.
- **Roles** - what is a role? A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc are predefined roles. You can clone them or change them (except Administrator).

When you assign a permission to an object, you can choose whether the permission propagates down the object hierarchy. You set propagation for each permission. Propagation is not universally applied. Permissions defined for a child object always override the permissions that are propagated from parent objects.

The image below (from vSphere 6.5 Security guide) illustrates the inventory hierarchy and the paths by which permissions can propagate.

Figure 2-1. vSphere Permissions



To assign permissions to an object, you follow these steps:

1 Select the object to which you want to apply the permission in the vCenter object hierarchy.

2 Select the group or user that should have privileges on the object.

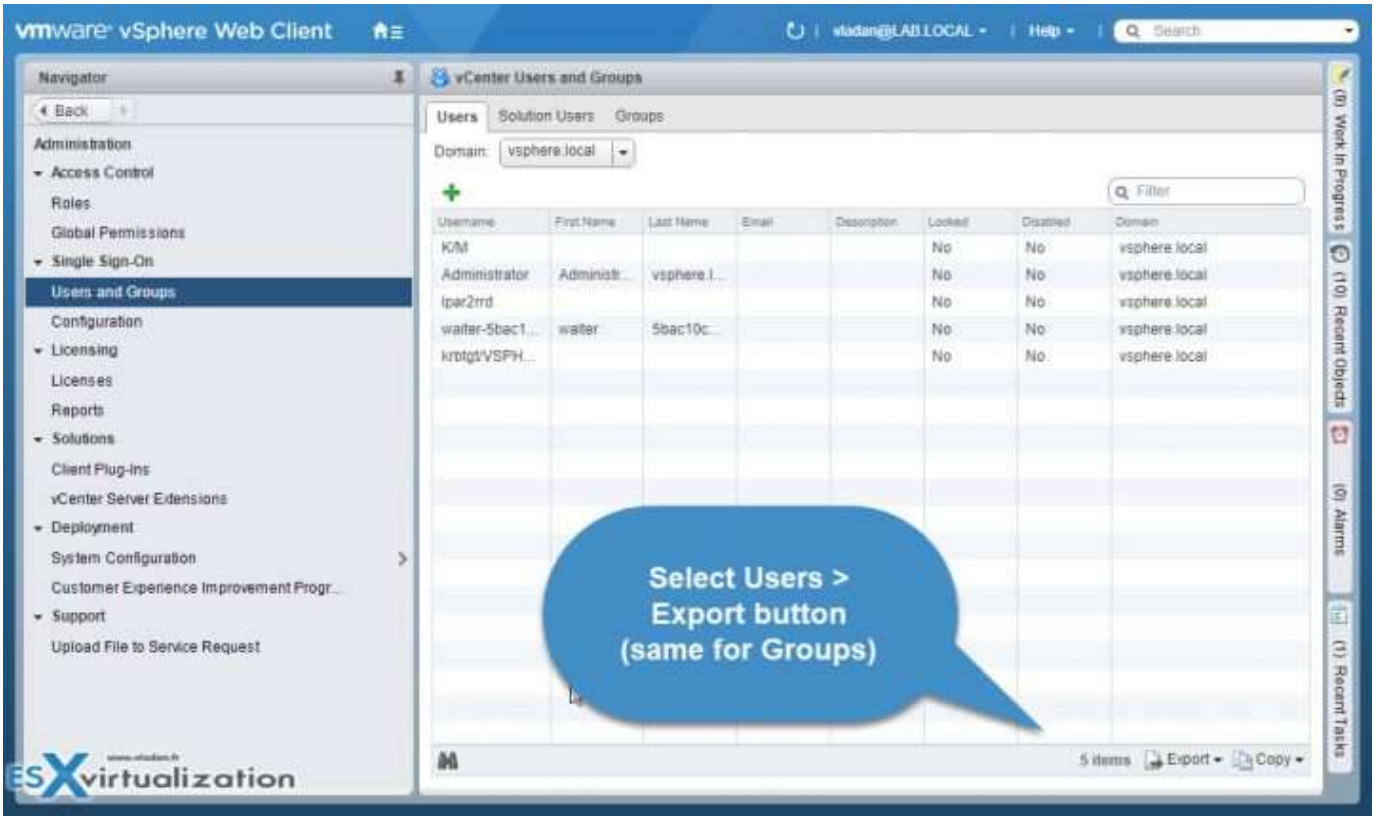
3 Select individual privileges or a role, that is a set of privileges, that the group or user should have on the object.

By default, permissions propagate, that is the group or user has the selected role on the selected object and its child objects.

VIEW/SORT/EXPORT USER AND GROUP LISTS

Home > Administration > SSO > Users and Groups. You can click the top of each column to sort username, view the details or add an additional user (group).

User lists can be exported via the export button in the bottom right of the Users and Groups page, located under Administration > SSO. Select the user(s) by holding shift or CTRL key for multiple, then click the export button.

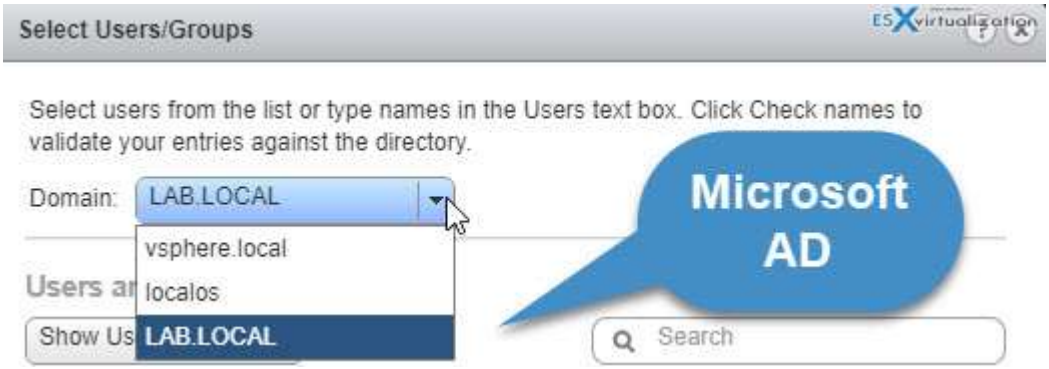


ADD/MODIFY/REMOVE PERMISSIONS FOR USERS AND GROUPS ON VCENTER SERVER INVENTORY OBJECTS

To Add/Modify/Remove permission for a user and group from vCenter inventory you have to **Select an object from the inventory** > click **Permissions TAB >** there you can add, edit, and remove permissions.

Example:

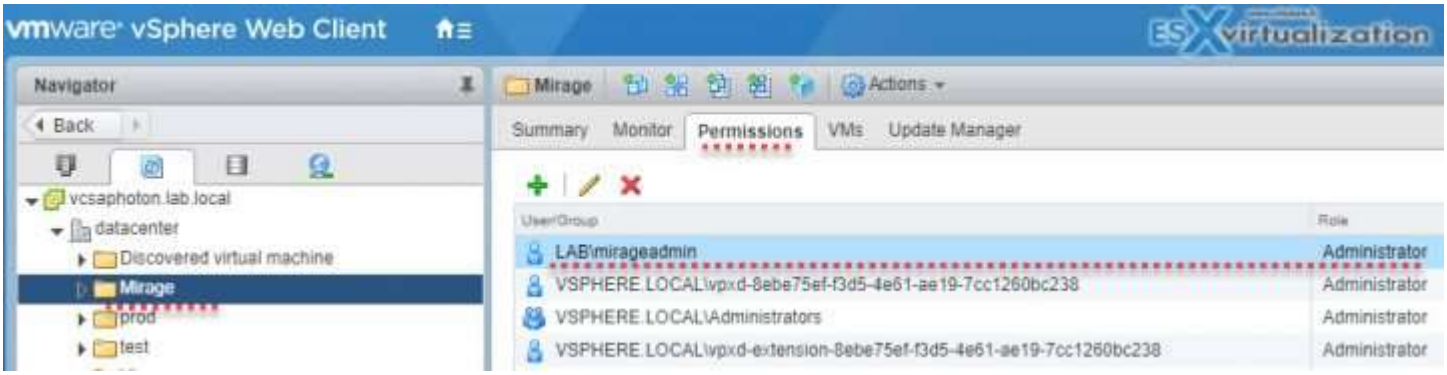
Click **Home** > **Host and clusters** (or VMs and templates view from where you can assign permission to the other node, folder, cluster, datacenter > **Select** vCenter Server (or other nodes...) > **Permissions TAB** > **Add new** permission. From there you can pick a user/group from SSO domain or from other identity sources. Use the drop-down selection to pick an AD user for example.



For example, MirageAdmin user from AD has an Administrator role (with its associated permissions) to the whole Mirage folder within the vCenter hierarchy.... I have worked on the VMware Mirage Guide recently.

- What is VMware Mirage?

It really depends on your needs. You can also create a custom role and then assign a user to this role.



Where possible, assign a role to a group rather than individual users to grant privileges to that group.

Grant permissions only on the objects where they are needed, and assign privileges only to users or groups that must have them.

If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges. If not, the admin won't be happy...

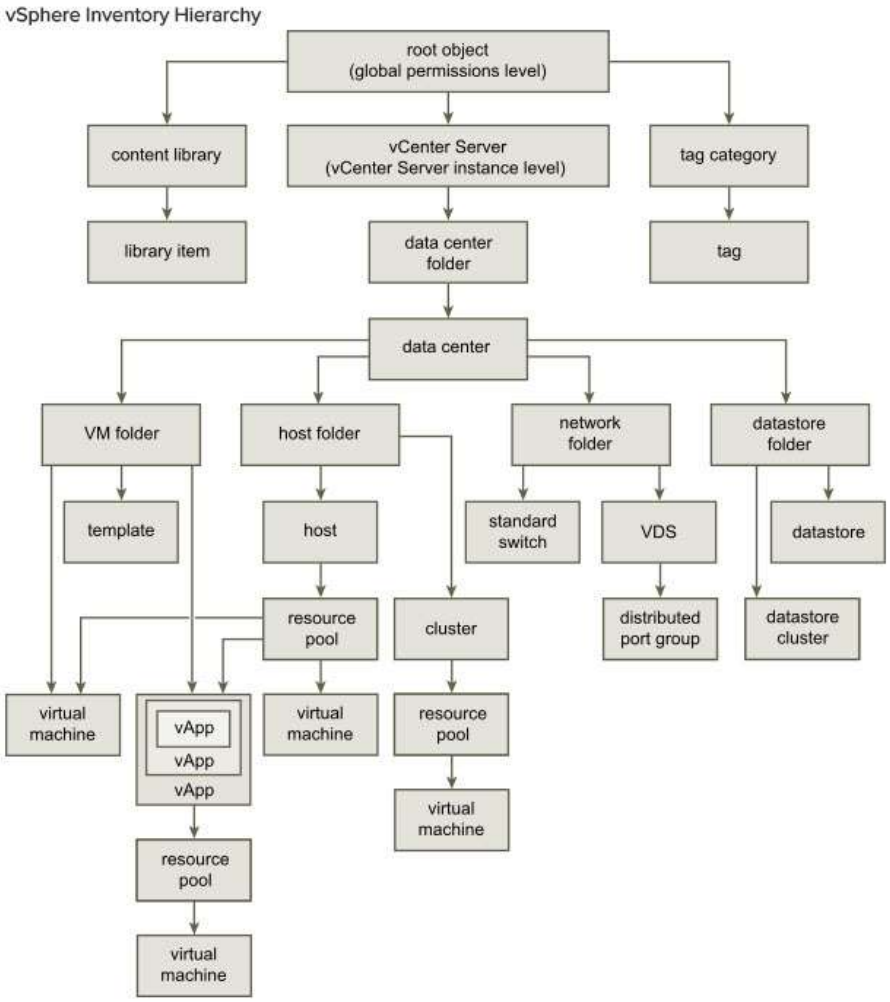
The best is to group objects into folders, (including hosts). Then you can assign permissions to folders containing hosts and other objects.

In most cases, enable propagation when you assign permissions to an object. This ensures that when new objects are inserted into the inventory hierarchy, they inherit permissions.

Mask specific areas of the vCenter hierarchy - Use the **No Access role** to mask specific areas of the hierarchy if you do not want for certain users or groups to have access to the objects in that part of the object hierarchy.

Determine how permissions are applied and inherited in vCenter Server

From vSphere security documentation web page we have found this image showing the vSphere Inventory Hierarchy:



After assigning a permission to an object, on the same page you can check the box to propagate permissions down the object hierarchy. You have to set the propagation for each permission. (or not).

Permissions defined for a child object **always override** the permissions that are propagated from parent objects.

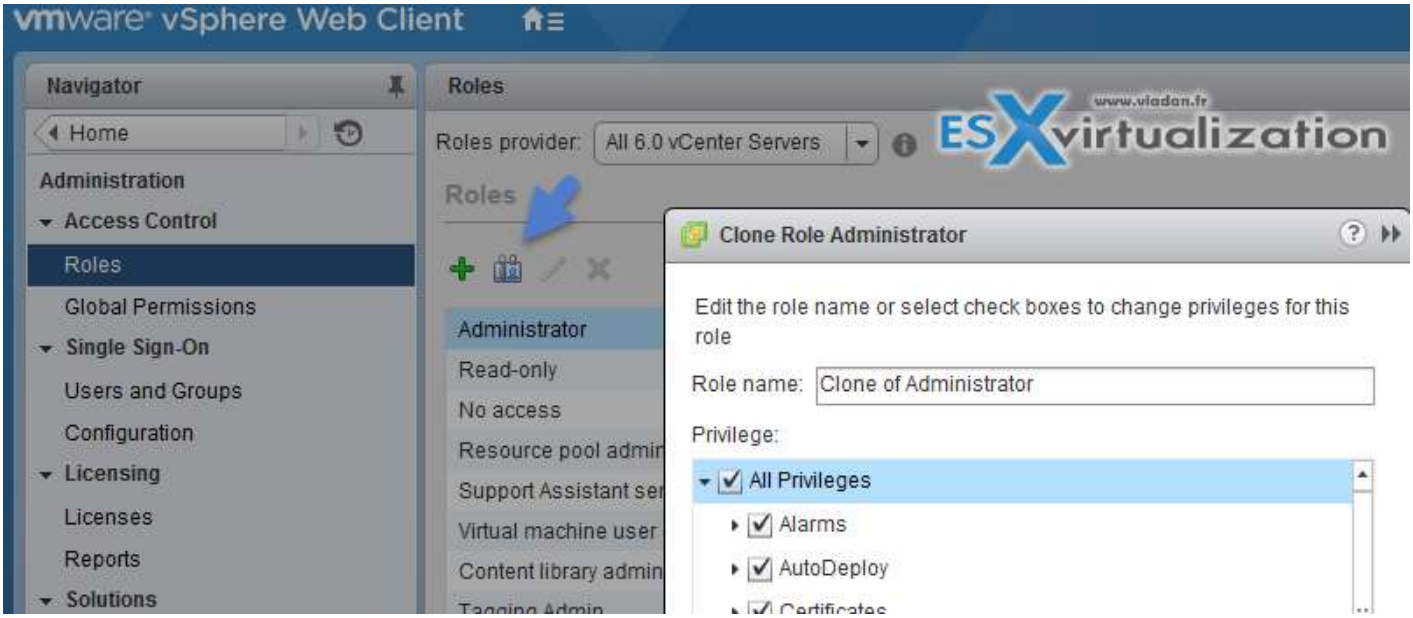
Most inventory objects inherit permissions from a single parent object in the hierarchy. For example, a datastore inherits permissions from either its parent datastore folder or parent data center. Virtual machines inherit permissions from both the parent virtual machine folder and the parent host, cluster, or resource pool simultaneously.

CREATE/CLONE/EDIT VCENTER SERVER ROLES

To edit, create or clone vCenter roles it's necessary to use vSphere Web client > Administration > Roles OR Home > Roles. Default roles are:

- Administrator
- Read-Only
- No Access

To clone role click the icon…



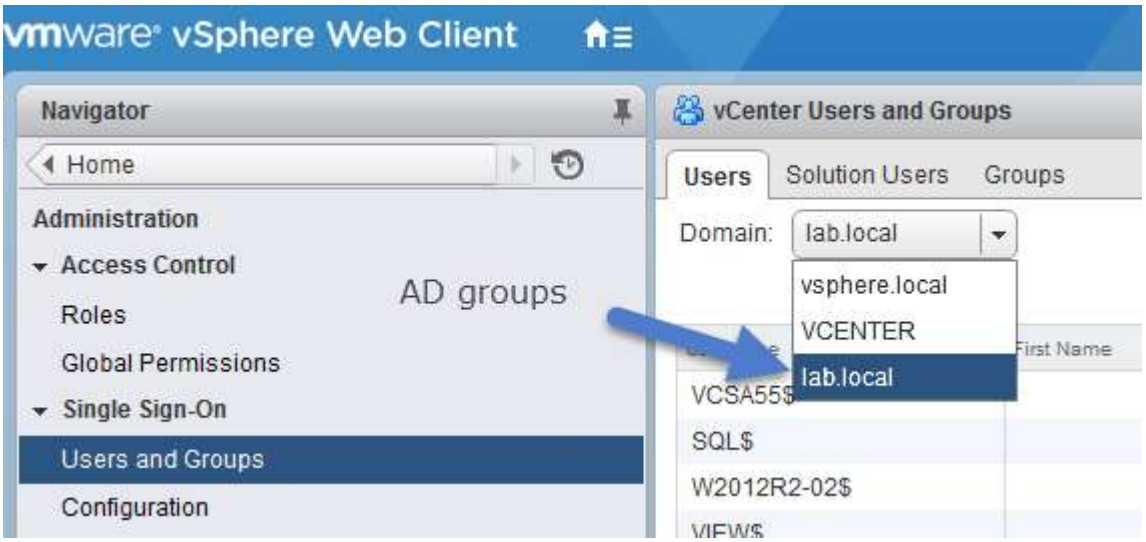
1. Log in to vCenter Server with the vSphere Web Client.
2. Select Home, click **Administration**, and click **Roles**.
3. **Select** a role, and click the **Clone** role action icon.
4. Type a **name** for the cloned role.
5. **Select or deselect privileges** for the role and click **OK**.

When you edit a role, you can change the privileges selected for that role. When completed, these privileges are applied to any user or group that is assigned the edited role.

Configure VMware Identity Sources

During the login process, the user tries to log in to vCenter, and it's vCenter Single Sign-On who does the verification of default identity source whether that user can authenticate. When a user logs in and enters the domain name in the login screen, vCenter SSO checks the domain to see, whether the domain has been added as an identity source. If yes, the user can successfully login.

Home > Administration > Single Sign-ON > Configuration > Identity sources > Add

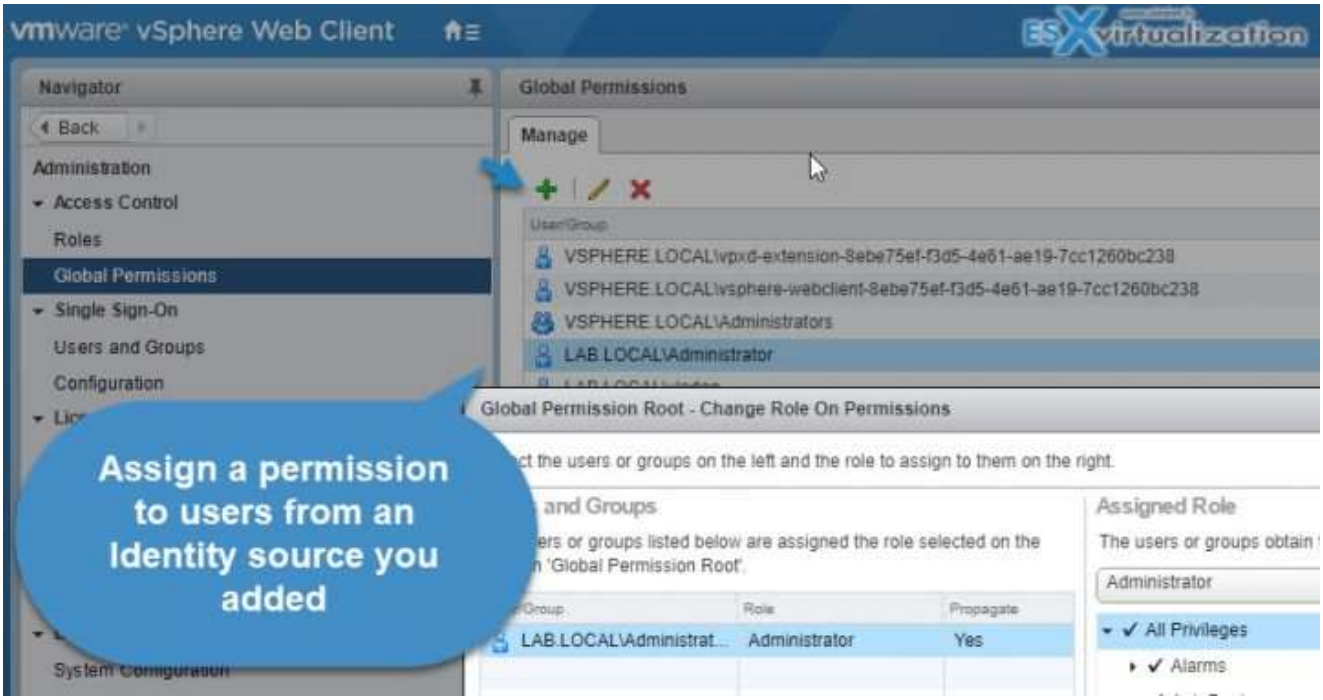


The user administrator@vsphere.local can perform tasks that are associated with services included with the Platform Services Controller.

After installation the only identity sources and users are:

- **Local OS** - All local operating system users. If you are upgrading, those local OS users who can already authenticate can continue to authenticate. Using the local OS identity source does not make sense in environments that use an embedded Platform Services Controller.
- **vsphere.local** - Contains the vCenter Single Sign-On internal users.

After adding the Microsoft AD as an identity source, all users can be authenticated but have the **No access role**. You can, however, change it (login as administrator@vsphere.local) and you can assign to users or groups of users privileges that enable them to log in to vCenter Server and view and manage objects.



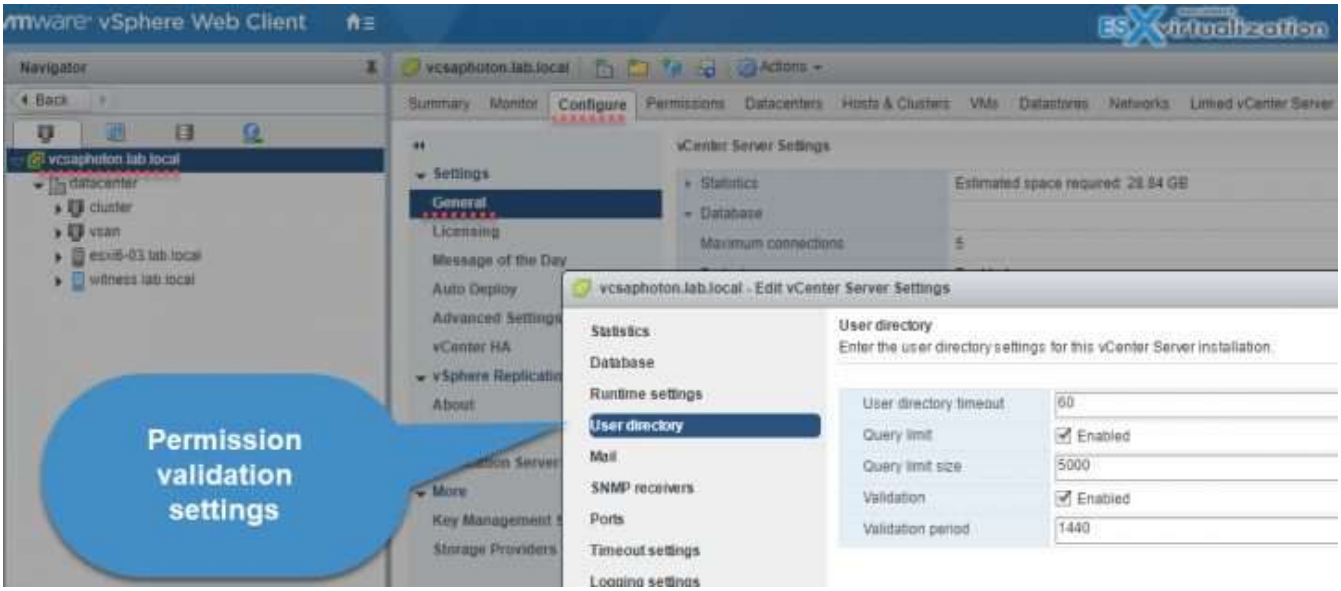
APPLY A ROLE TO A USER/GROUP AND TO AN OBJECT OR GROUP OF OBJECT

A role is a predefined set of privileges. A role allows you to assign permission to an object. Administrator, Resource Pool administrator, etc. are predefined roles. Privileges define rights to perform actions and read properties. For example, the **Virtual Machine Administrator** role allows a user to read and change virtual machine attributes

vCenter Server has some system roles and some sample roles you can play with.

- **System Roles** - System roles are permanent, not editable. You cannot edit the privileges associated with these roles.
- **Sample roles** - Sample roles are useful because they have been created for frequently performed tasks. Those roles are modifiable, so you are allowed to clone, modify, or remove these roles.

CHANGE PERMISSION VALIDATION SETTINGS



vCenter Server systems that use a directory service regularly validate users and groups against the user directory domain. Validation occurs at regular intervals specified in the vCenter Server settings;

Home > **Hosts and clusters** > **Select vCenter server** > **Configure** > **Settings** > **General** > **Edit** and select **User directory** > Change the values as needed.

The Options:

- **User directory timeout -** Timeout interval, in seconds, for connecting to the Active Directory server. This value specifies the maximum amount of time vCenter Server allows a search to run on the selected domain. Searching large domains can take a long time.
- **Query limit** - Select the checkbox to set a maximum number of users and groups that vCenter Server displays.
- **Query limit size** - This is a maximum number of users and groups from the selected domain that vCenter Server displays in the Select Users or Groups dialog box. If you enter 0 (zero), all users and groups appear.
- **Validation** - Deselect the checkbox to disable validation
- **Validation Period** - Specifies how often vCenter Server validates permissions, in minutes.

Determine the appropriate set of privileges for common tasks in vCenter Server

Many tasks require permissions on multiple objects in the inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot finish successfully.

Any operation that consumes storage space requires the Datastore.Allocate Space privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.

Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.

Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the Resource.Assign Virtual Machine to Resource Pool privilege.

Screenshot directly from the [vSphere 6.5 security guide]

Table 2-4. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: • **Virtual machine.Inventory.Create new** • **Virtual machine.Configuration.Add new disk** (if creating a new virtual disk) • **Virtual machine.Configuration.Add existing disk** (if using an existing virtual disk) • **Virtual machine.Configuration.Raw device** (if using an RDM or SCSI pass-through device)	Administrator
	On the destination host, cluster, or resource pool: **Resource.Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or the folder that contains the datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Power on a virtual machine	On the data center in which the virtual machine is deployed: **Virtual machine.Interaction.Power On**	Virtual Machine Power User or Administrator
	On the virtual machine or folder of virtual machines: **Virtual machine.Interaction.Power On**	
Deploy a virtual machine from a template	On the destination folder or data center: • **Virtual machine.Inventory.Create from existing** • **Virtual machine.Configuration.Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine.Provisioning.Deploy template**	Administrator
	On the destination host, cluster or resource pool: **Resource.Assign virtual machine to resource pool**	Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine.Snapshot management.Create snapshot**	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: • **Resource.Assign virtual machine to resource pool** • **Virtual machine.Inventory.Move**	Administrator
	On the destination resource pool: **Resource.Assign virtual machine to resource pool**	Administrator

Table 2-4. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: • **Virtual machine.Interaction.Answer question** • **Virtual machine.Interaction.Console interaction** • **Virtual machine.Interaction.Device connection** • **Virtual machine.Interaction.Power Off** • **Virtual machine.Interaction.Power On** • **Virtual machine.Interaction.Reset** • **Virtual machine.Interaction.Configure CD media** (if installing from a CD) • **Virtual machine.Interaction.Configure floppy media** (if installing from a floppy disk) • **Virtual machine.Interaction.VMware Tools install**	Virtual Machine Power User or Administrator
	On a datastore that contains the installation media ISO image: **Datastore.Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: • **Datastore.Browse datastore** • **Datastore.Low level file operations**	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: • **Resource.Migrate powered on virtual machine** • **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: • **Resource.Migrate powered off virtual machine** • **Resource.Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore.Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource.Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a host into a cluster	On the host: **Host.Inventory.Add host to cluster**	Administrator
	On the destination cluster: **Host.Inventory.Add host to cluster**	Administrator

COMPARE AND CONTRAST DEFAULT SYSTEM/SAMPLE ROLES

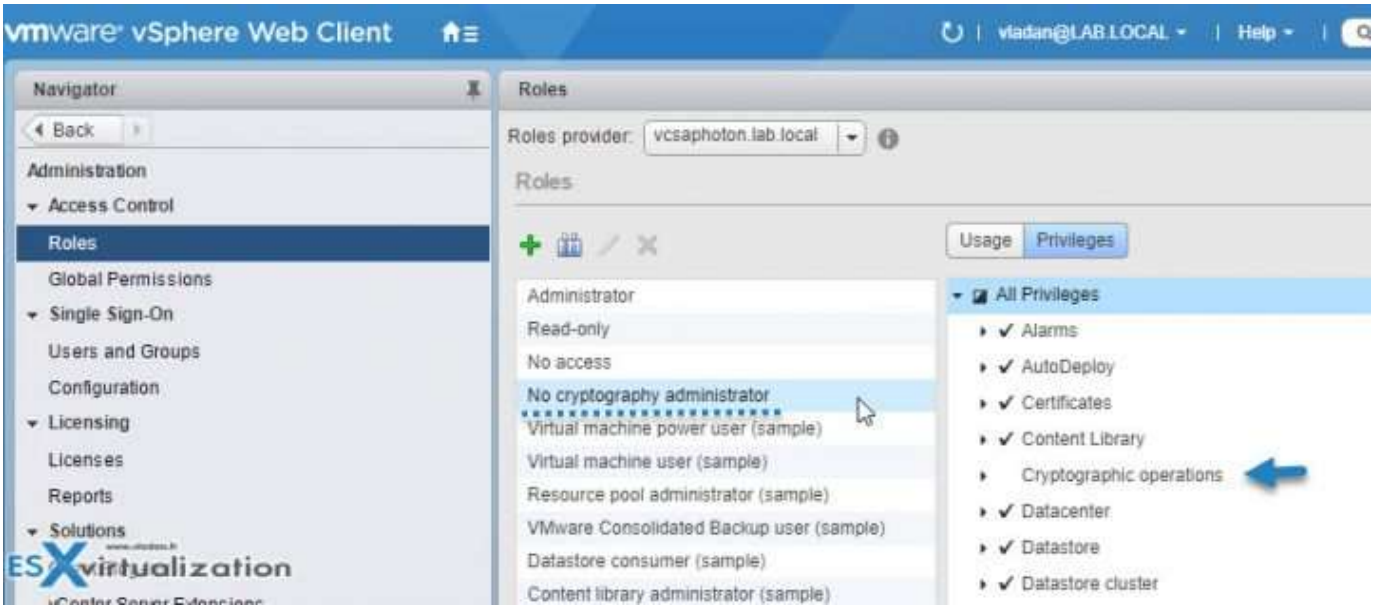
vCenter Server provides a few default roles. You cannot change the privileges associated with the default roles. The default roles are organized as a hierarchy. Each role inherits the privileges of the previous role.

For example, the Administrator role inherits the privileges of the Read Only role. Roles that you create do not inherit privileges from any of the system roles.

Administrator Role - Users with the Administrator role for an object are allowed to view and perform all actions on the object. This role also includes all privileges inherent in the Read Only role. If you are acting in the Administrator role on an object, you can assign privileges to individual users and groups. If you are acting in the Administrator role in vCenter Server, you can assign privileges to users and groups in the default vCenter Single Sign-On identity source. Supported identity services include Windows Active Directory and OpenLDAP 2.4.

By default, the administrator@vsphere.local user has the Administrator role on both vCenter Single Sign-On and vCenter Server after installation. That user can then associate other users with the Administrator role on vCenter Server.

No Cryptography Administrator Role - Users with the No cryptography administrator role for an object have the same privileges as users with the Administrator role, **except for Cryptographic operations privileges**. This role allows administrators to **designate other administrators that cannot encrypt or decrypt virtual machines or access encrypted data**, but that can perform all other administrative tasks.



No Access Role - Users with the No Access role for an object **cannot view or change the object in any way**. New users and groups are assigned this role by default. You can change the role on an object-by-object basis.

The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, the root user, and vpxuser are assigned the Administrator role by default. Other users are assigned the No Access role by default.

Read Only Role - Users with the Read Only role for an object are **allowed to view the state of the object and details about the object**. For example, users with this role can view virtual machine, host, and resource pool attributes but cannot view the remote console for a host. All actions through the menus and toolbars are disallowed.

Determine the correct permissions needed to integrate vCenter Server with other VMware products

The detailed tables can be found in the vSphere 6.5 security document (Chapter 11), there are too many to list them all here. They list the default privileges that, when selected for a role, can be paired with a user and assigned to an object.

vCenter Server extensions might define additional privileges not even listed in the PDF. Check the vSphere 6.5 security guide.

VCP6.5-DCV Objective 2 – Secure ESXi and vCenter Server

vSphere 6.5 is slightly different (from the UI perspective) compared to vSphere 6.0. The TABs are different, the UI has been streamlined in order to facilitate navigation or do fewer clicks for configuration and administration tasks.

Passing a VCP exam has some requirements. Depending if you are current VCP or not you may need to get some training first. In order to pass the VCP6.5-DCV certification exam, you must attend one of the required training courses and pass the vSphere 6 Foundations Exam or vSphere 6.5 Foundations Exam.

Attend one of those required courses:

VMware vSphere: Install, Configure, Manage [V6.5]
VMware vSphere: Install, Configure, Manage [V6.5] - On Demand
VMware vSphere: Optimize and Scale [V6.5]
VMware vSphere: Optimize and Scale [V6.5] - On Demand
VMware vSphere: Install Configure Manage plus Optimize & Scale Fast Track
VMware vSphere: Skills for Public Sector Customers [V6.5]
VMware vSphere: Fast Track [V6.5]
VMware vSphere: Troubleshooting Workshop [V6.5]

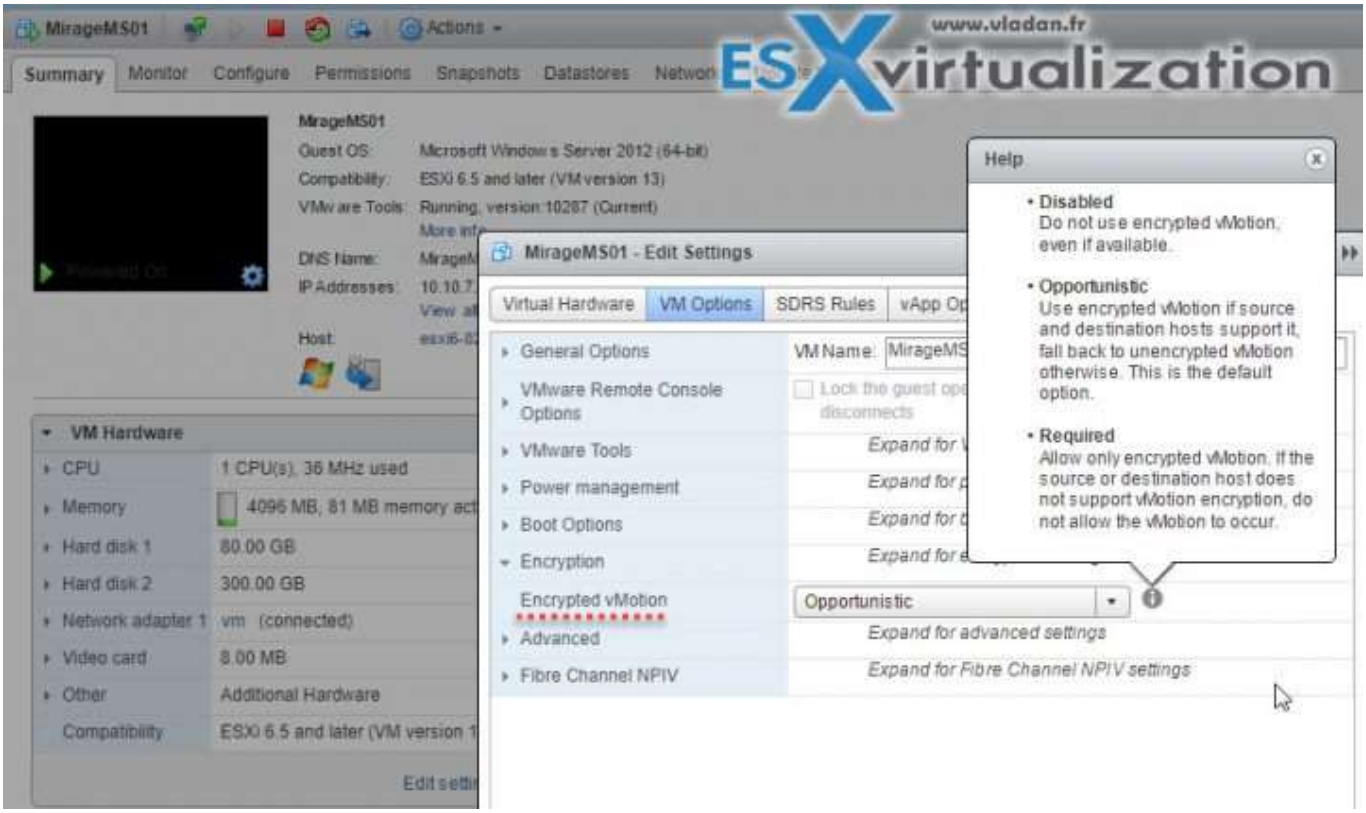
The exam prep guide (previously called "Exam Blueprint") PDF is a good start. Not only it lists all the objectives, but also, at the end of the document, you can find shortcuts to the different PDFs which are necessary for the study. We'll try to get all the information to each blog post, with links to sections presenting too large volume to be handled within a blog post. Already, those blog posts seem to be quite MEGA posts with over 2000 words each ... -:) .

Configure Encrypted vMotion

With vSphere 6.5, vSphere, vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

For virtual machines that are encrypted, migration with vSphere vMotion always uses encrypted vSphere vMotion. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines.

- **Right-click a VM** and select **Edit Settings** > **VM Options** > Click **Encryption**, and select an option from the Encrypted VMotion drop-down menu.



The default is Opportunistic.

- **Disabled** – Do not use encrypted vSphere vMotion.
- **Opportunistic** – Use encrypted vSphere vMotion if the source and destination hosts support it (both sides has to be on ESXi 6.5 version). Only ESXi versions 6.5 and latter uses encrypted vSphere vMotion.
- **Required** – Allow only encrypted vSphere vMotion. If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

For unencrypted VMs - All variants of encrypted vSphere vMotion are supported. Shared storage is required for migration across vCenter Server instances.
For encrypted VMs - migration across vCenter Server instances is not supported.

Describe Secure Boot

With secure boot enabled, a machine refuses to load any UEFI driver or app unless the operating system boot loader is cryptographically signed. Starting with vSphere 6.5, ESXi supports secure boot if it is enabled in the hardware.

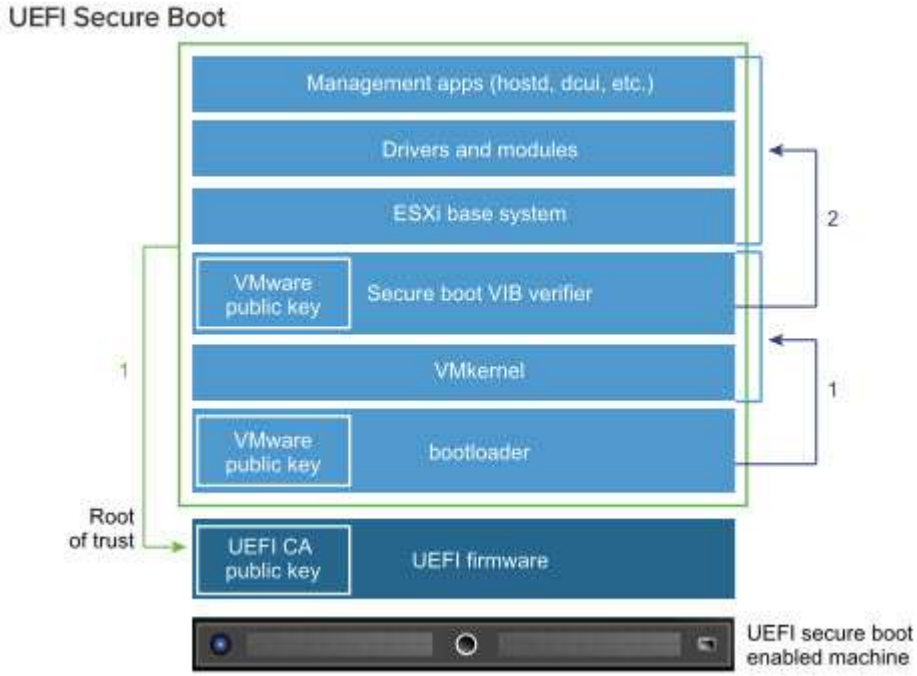


Figure 1: VCP6.5-DCV Study Guide - UEFI Secure Boot

The ESXi secure boot process:

1. ESXi bootloader contains a VMware public key. The bootloader uses this key to verify the signature of the kernel and a small subset of the system that includes a secure boot VIB verifier.
2. The VIB verifier verifies every VIB package that is installed on the system.
3. The system boots with the root of trust in certificates that are part of the UEFI firmware.

HARDEN ESXI HOSTS

Only a limited set of services runs by default on each ESXi host.

- ESXi Shell and SSH are disabled by default.
- You can configure additional features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.
- An ESXi host is also protected with a firewall. You can open ports for incoming and outgoing traffic as needed but should restrict access to services and ports.
- Using the ESXi lockdown mode and limiting access to the ESXi Shell can further contribute to a more secure environment.
- Hosts are provisioned with certificates that are signed by the VMware Certificate Authority (VMCA) by default.
- You might consider using UEFI Secure Boot for your ESXi system.
- Join ESXi hosts to an Active Directory (AD) domain to eliminate the need to create and maintain multiple local user accounts. Using AD for user authentication simplifies the ESXi host configuration, ensures password complexity and reuse policies are enforced and reduces the risk of security breaches and unauthorized access. (Note: if the AD group "ESX Admins" (default) exists then all users and groups that are assigned as members to this group will have full administrative access to all ESXi hosts the domain.)

- **Use ESXi lockdown mode** - Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server. Two modes available (normal and strict). Tip: What is ESXi Lockdown Mode? Users on the Exception Users list can access the host from the ESXi Shell and through SSH if they have the Administrator role on the host and if these services are enabled. This access is possible even in strict lockdown mode. Leaving the ESXi Shell service and the SSH service disabled is the most secure option
- **ESXi.set-shell-timeout** - sets a timeout to limit how long the ESXi shell and SSH services are allowed to run.

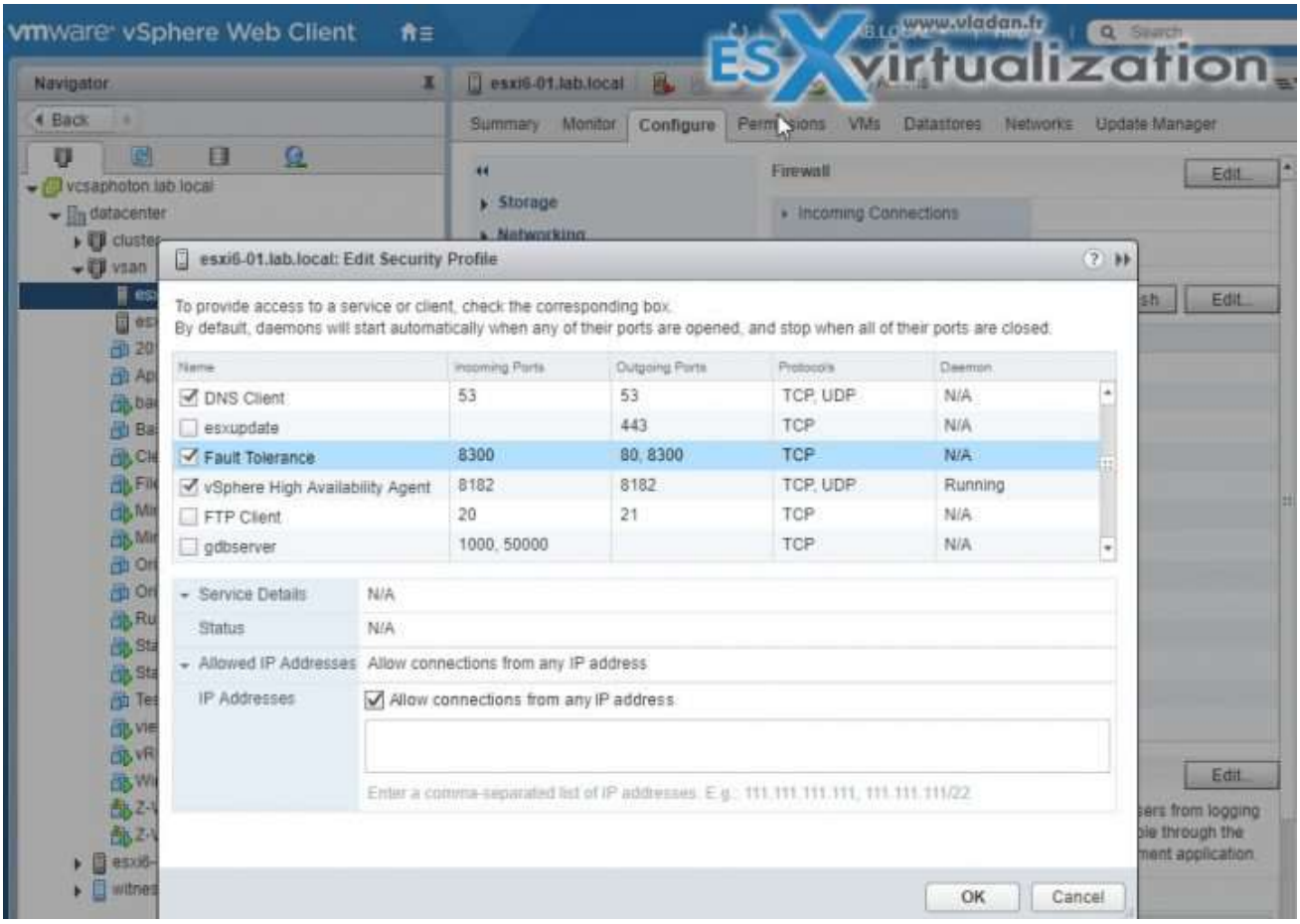
Check the VMware Security Hardening guides at VMware Blog.

ENABLE/CONFIGURE/DISABLE SERVICES IN THE ESXI FIREWALL

For each ESXi host, you can create firewall rules.

Connect via vSphere web client > Configure > System > Security Profile > Firewall section > Edit > Select Rule > Enable/disable.

Select the rule sets to enable, or deselect the rule sets to disable. You can change startup policy to have a particular service started with the host or by port usage. Some services allow configuring IP address from which connections are permitted.



Check which services are active

esxcli network firewall ruleset list

```
[root@esxi6-01:~] esxcli network firewall ruleset list
Name                    Enabled
----------------------  -------
sshServer                  true
sshClient                 false
nfsClient                  true
nfs41Client               false
dhcp                       true
dns                        true
snmp                       true
ntpClient                  true
```

OPEN FIREWALL PORT VIA CLI:

esxcli network firewall ruleset set -e true -r httpsClient

CHANGE DEFAULT ACCOUNT ACCESS

The roles for ESXi are much simpler than roles for vCenter server, which we have covered in the VCP6.5-DCV Objective 1 – Configure and Administer Role-based Access Control. But also, the same as for vCenter server, there are some predefined roles and some other accounts for when the ESXi is managed via vCenter.

Since 6.0 there is a possibility also to use ESXCLI (via putty session for example, or directly via console) for account management. There are some commands for managing ESXi local user accounts.

esxcli system account

```
[root@esxi6-01:~] esxcli system account
Usage: esxcli system account {cmd} [cmd options]

Available Commands:
  add                   Create a new local user account.
  list                  List local user accounts.
  remove                Remove an existing local user account.
  set                   Modify an existing local user account.
[root@esxi6-01:~]
```

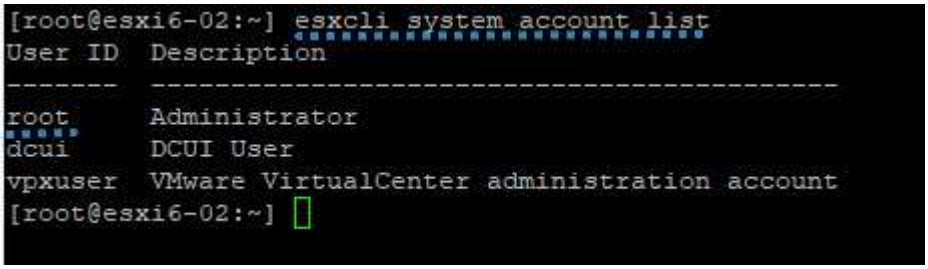
Predefined Roles:

- **Read Only** – Allows a user to view objects associated with the ESXi host but not to make any changes to objects.
- **Administrator** – Administrator role.
- **No Access** – No access role. This role is the default role. You can override the default role.

There is a single root user created by default when you install ESXi.

esxcli system account list

gives us this:



ESXi Privileges:

Best practice is to create at least one named user account, assign it full administrative privileges on the host, and use this account instead of the root account. Set a highly complex password for the root account and limit the use of the root account. Do not remove the root account.

For all versions of ESXi, you can see the list of predefined users in the /etc/passwd file.

root user - root user account has the Administrator role. That root user account can be used for local administration and to connect the host to vCenter Server. It's the account with the highest privilege.

For better auditing, create individual accounts with Administrator privileges. Set a highly complex password for the root account and limit the use of the root account, for example, for use when adding a host to vCenter Server. Do not remove the root account.

Best practice is to ensure that any account with the Administrator role on an ESXi host is assigned to a specific user with a named account. Use ESXi Active Directory capabilities, which allow you to manage Active Directory credentials. You can remove the access privileges for the root user. However, you must first create another permission at the root level that has a different user assigned to the Administrator role.

vpxuser - vCenter Server uses vpxuser privileges when managing activities for the host. vCenter Server has Administrator privileges on the host that it manages. For example, vCenter Server can move virtual machines to and from hosts and change virtual machine configuration.

The vCenter Server administrator can perform most of the same tasks on the host as the root user and also schedule tasks, work with templates, and so forth. However, the vCenter Server administrator cannot directly create, delete, or edit local users and groups for hosts. Only a user with Administrator privileges can perform these tasks directly on a host.

DCUI user - the DCUI user runs on hosts and acts with Administrator rights. This user's primary purpose is to configure hosts for lockdown mode from the Direct Console User Interface (DCUI).

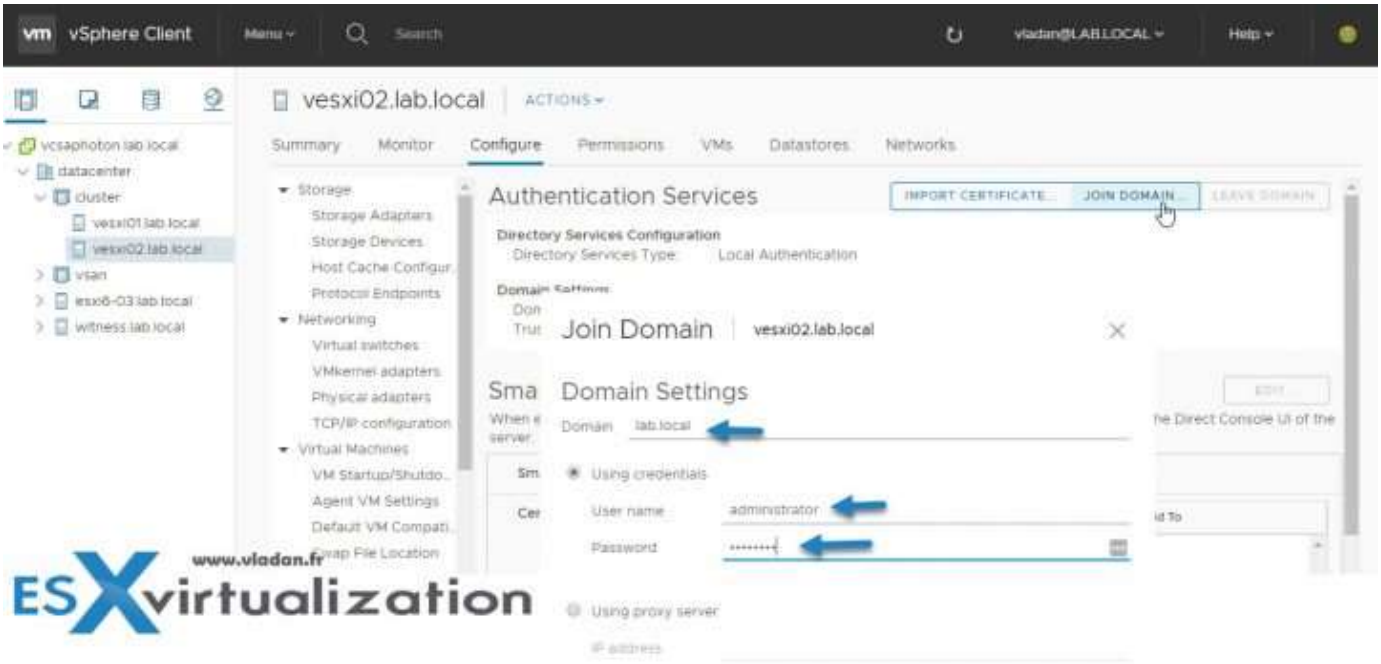
This user acts as an agent for the direct console and cannot be modified or used by interactive users.

Add an ESXi Host to a Directory Service

You can configure a host to use a directory service such as Active Directory to manage users and groups. When you add an ESXi host to Active Directory, the DOMAIN group 'ESX Admins' is assigned full administrative access to the host if it exists.

A special AD group named "**ESX Admins**" shall be manually created before a host is joined to Microsoft AD. Why? Because like this All members of this group (ESX admins) are automatically assigned to the **Administrator role** on the host when this host is joined to an AD. If not the permissions have to be **applied manually.**

Select your host > Configure > System > Authentication Services > Join Domain > Enter your Microsoft domain name > Use a user and password who has **permission** to join the host to the domain > Click OK.



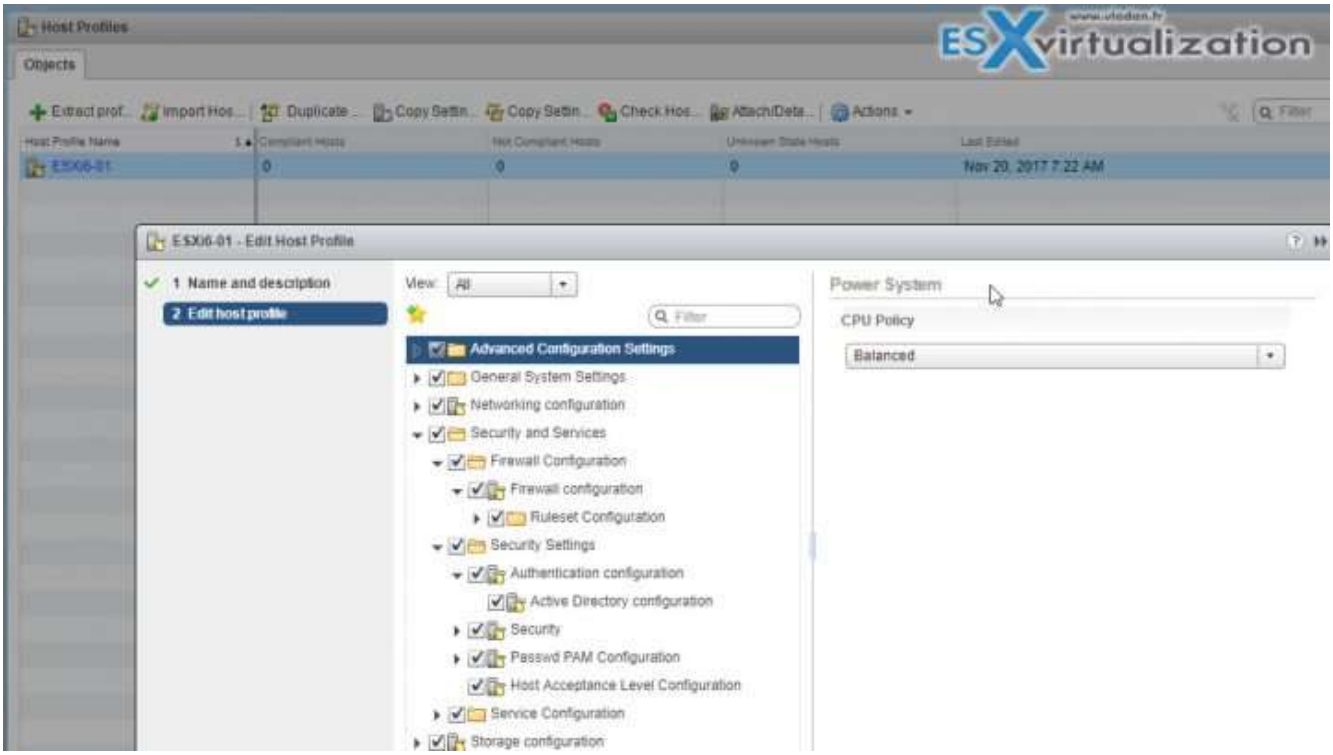
APPLY PERMISSIONS TO ESXI HOSTS USING HOST PROFILES

Host profiles allow you to "standardize" configurations for ESXi hosts and automate compliance for settings you have set on a reference host. Host profiles allow you to control many aspects of host configuration including memory, storage, networking, and so on.In some cases, host profiles can be also useful when for example you need to reset ESXi root password on a host.

1. Set up the reference host to specification and create a host profile.
2. Attach the profile to a host or cluster.
3. Apply the host profile of the reference host to other hosts or clusters.

If you haven't done yet, go to **Home > Host profiles > Extract profile** from a host. Once you have that profile you can apply it to a host…

- **Select** the host profile > Click **Actions** > **Edit Settings** > Expand **Security and Services**
- Select the **Permission Rules** folder > click the **Plus Sign**

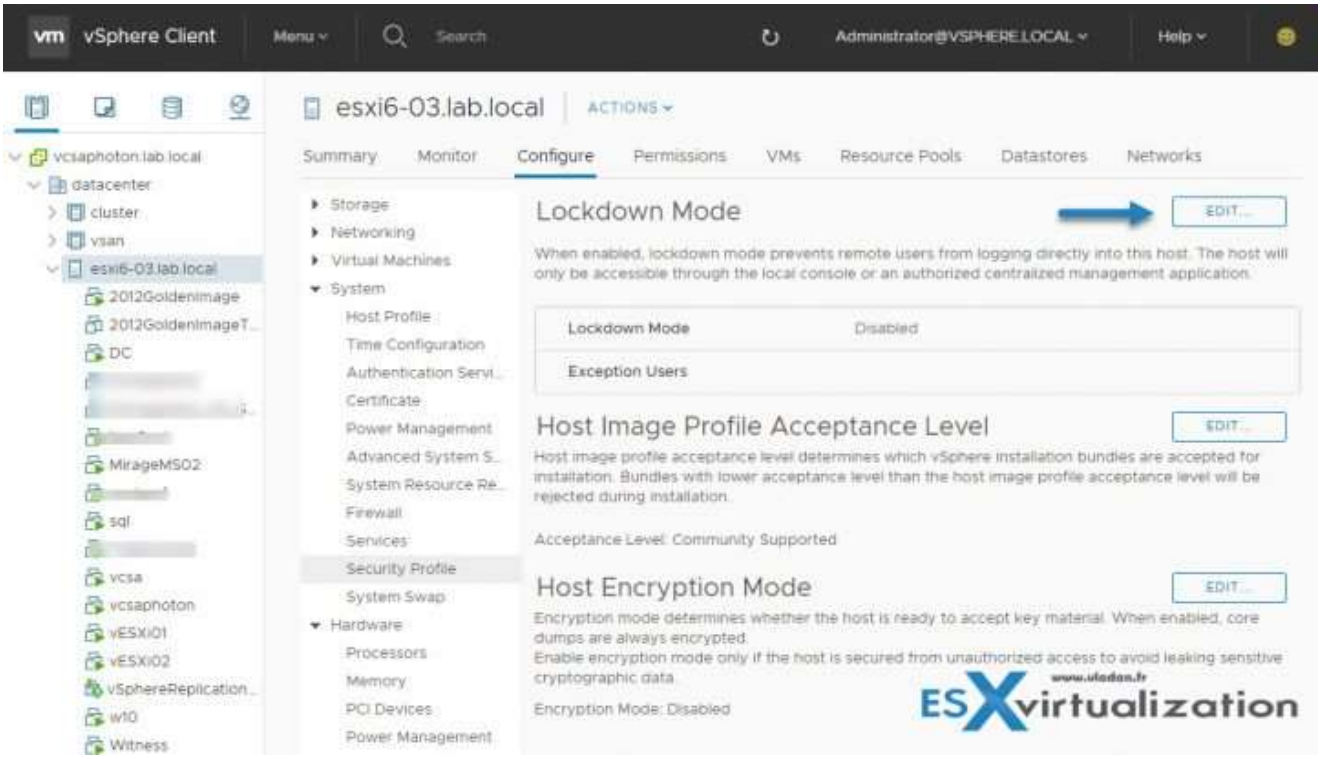


ENABLE LOCKDOWN MODE

Lockdown Modes:

- **Disabled** – Lockdown mode is disabled.
- **Normal** – The host can be accessed through vCenter Server. Only users who are on the **Exception Users list** and have administrator privileges can log in to the Direct Console User Interface. If SSH or the ESXi Shell is enabled, access might be possible.
- **Strict** – The host can only be accessed through vCenter Server. If SSH or the ESXi Shell is enabled, running sessions for accounts in the ***DCUI.Access*** advanced option and for Exception User accounts that have administrator privileges remain enabled. All other sessions are terminated. **DCUI is stopped.**

Select your host > Configure > System > Security Profile > Edit.

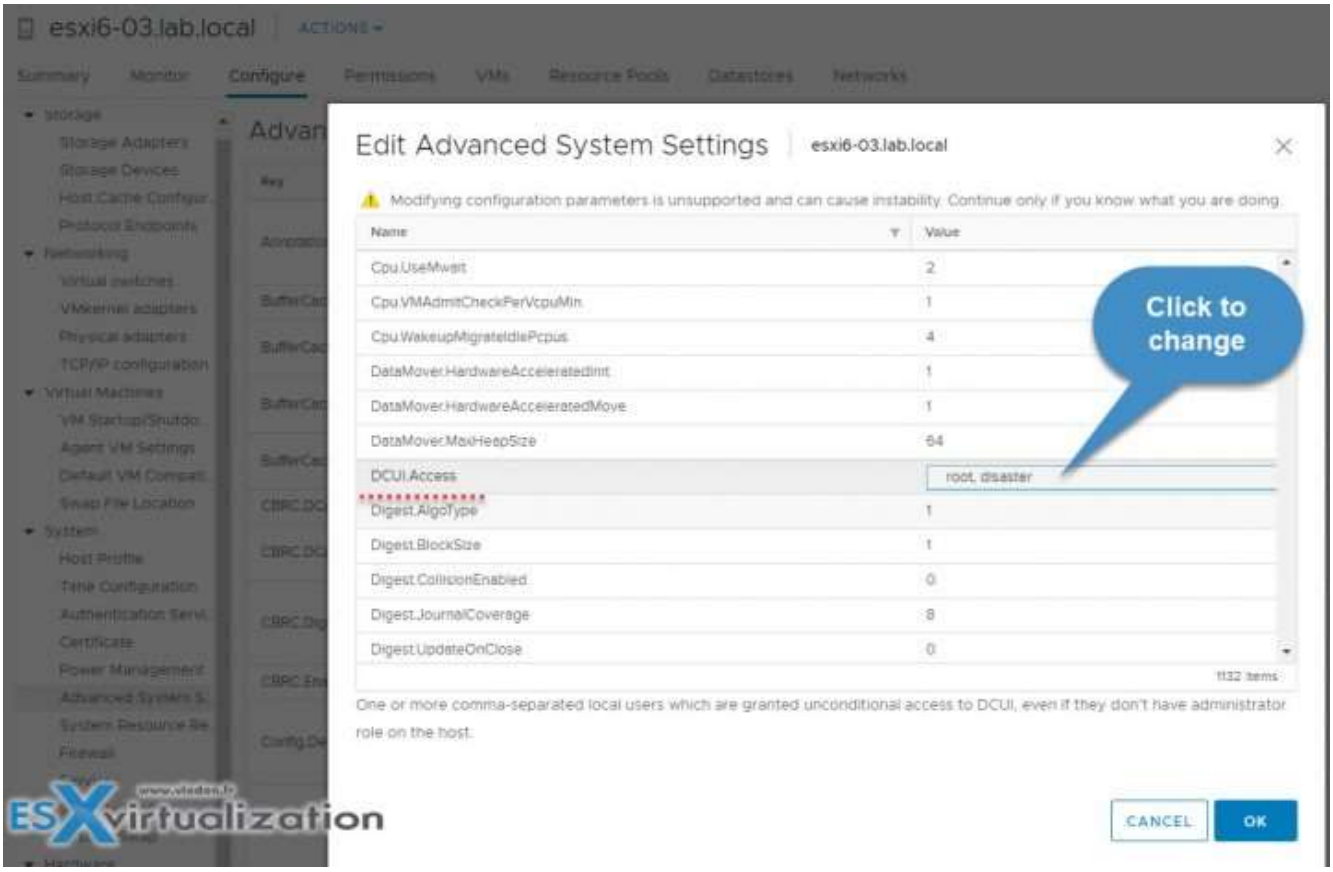


Accounts in the Exception User list for lockdown mode who have administrative privileges on the host. The Exception Users list is meant for service accounts that perform very specific tasks. Adding ESXi administrators to this list defeats the purpose of lockdown mode.

WHERE TO ADD AN ACCOUNT TO THE EXCEPTION USERS LIST?

You'd have to first create a local ESXi user and then specify these advanced settings on a per-host base. So in my case, I created a sample local ESXi user called "disaster" through ESXi host client which is a local ESXi user.

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.



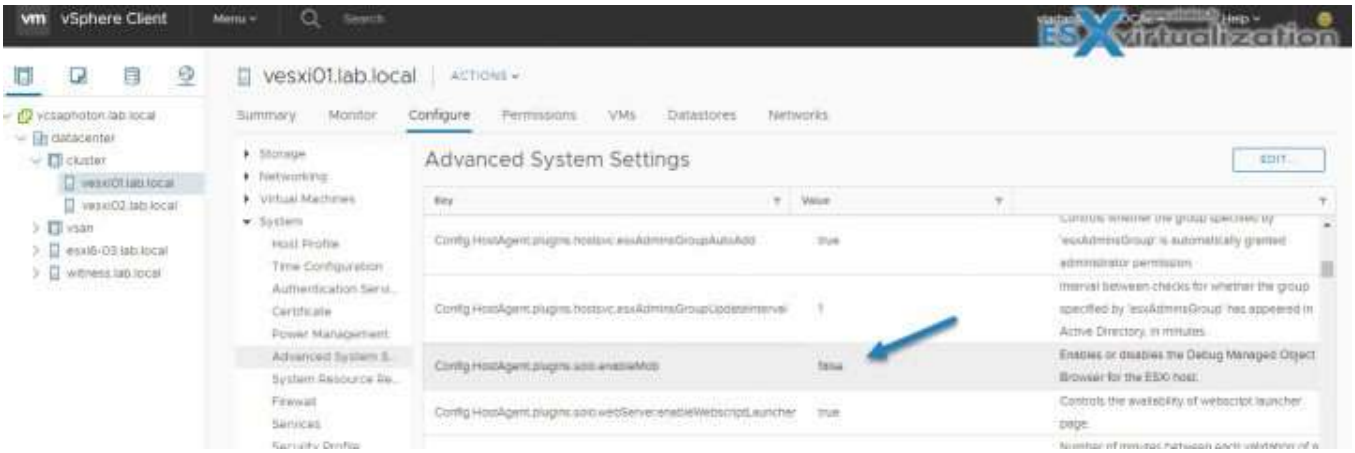
The exception users can only perform tasks for which they have privileges for. So even if you create your local user and put him on the Exceptions list, the user won't be able to connect unless you give him a privilege.

CONTROL ACCESS TO HOSTS (DCUI/SHELL/SSH/MOB)

You can control the access to the DCUI/Shell and SSH. The MOB is the managed object browser (MOB) and provides a way to explore the VMkernel object model. vSphere 6.0 and later has the MOB disabled by default because it could be exploited by hackers.

To Enable MOB:

Select host > Advanced System Settings > Advanced > Config.HostAgent.plugins.solo.enableMob > modify the value.



HARDEN VCENTER SERVER

If the local Windows administrator account currently has the Administrator role for the vCenter server, remove that role and assign the role to one or more named vCenter Server administrator accounts.

You can create custom roles or use the **No cryptography administrator role** for administrators with more limited privileges.

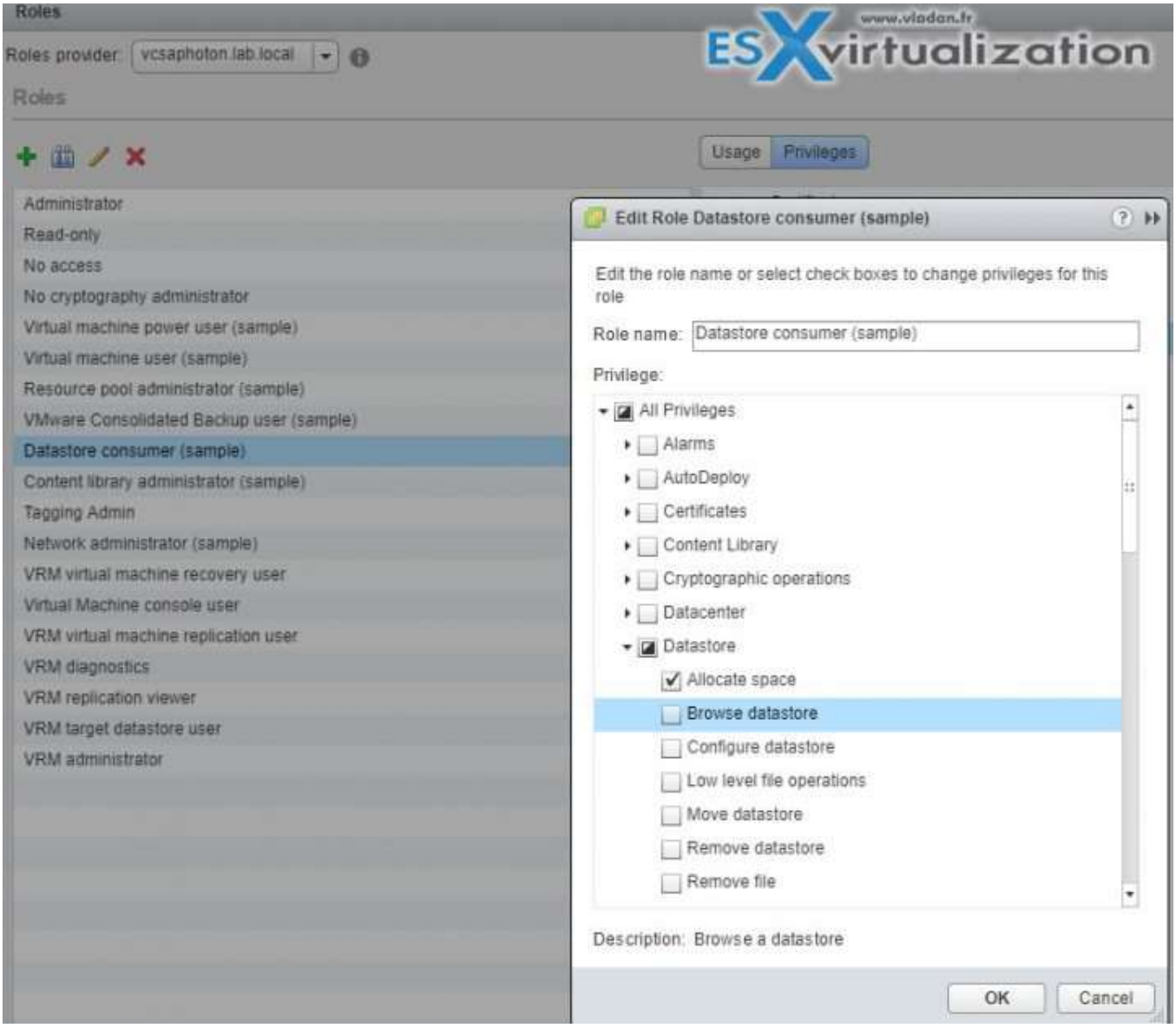
- **Minimize access** - do not let users to login directly to vCenter server host machine.
- **Restrict DB user privileges** - The database user requires only certain privileges specific to database access. Some privileges are required only for installation and upgrade. You can remove these privileges from the database administrator after vCenter Server is installed or upgraded.
- **Restrict Datastore Browser Access** - Assign the Datastore.Browse datastore privilege only to users or groups who really need those privileges
- **Modify password policy for vpxuser** - By default, vCenter Server changes the vpxuser password automatically every 30 days.

Check the vSphere 6.5 security guide for further hardening tips. (Page 98-110) There are also details about default open ports (too large to list it all here), different sections for vCenter on Windows and for vCSA (Linux appliance).

CONTROL DATASTORE BROWSER ACCESS

VMware vSphere allows to grant or refuse access to individual objects of the infrastructure. This can be a host, folder, datastore etc. Datastore access is granted via the **Datastore.Browse datastore privilege**.

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



CREATE/MANAGE VCENTER SERVER SECURITY CERTIFICATES

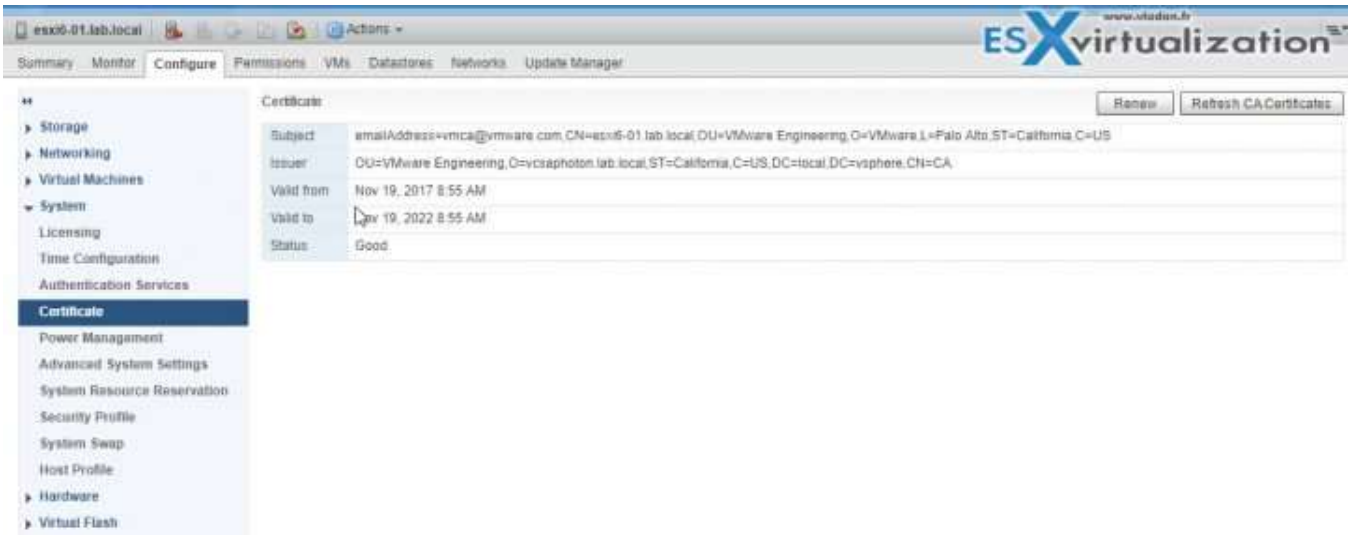
When ESXi and vCenter Server communicate via TLS/SSL for management traffic. In vSphere 6.0 and later, vCenter Server supports the following certificate modes for ESXi hosts:

VMware Certificate Authority (default) - Use this mode if VMCA provisions all ESXi hosts, either as the top-level CA or as an intermediate CA. By default, VMCA provisions ESXi hosts with certificates. In this mode, you can refresh and renew certificates from the vSphere Web Client.

Custom Certificate Authority - Use this mode if you want to use only custom certificates that are signed by a third-party or enterprise CA. In this mode, you are responsible for managing the certificates. You cannot refresh and renew certificates from the vSphere Web Client. Unless you change the certificate mode to Custom Certificate Authority, VMCA might replace custom certificates, for example, when you select Renew in the vSphere Web Client.

Thumbprint Mode - vSphere 5.5 used thumbprint mode and this mode is still available as a fallback option for vSphere 6.x. In this mode, vCenter Server checks that the certificate is formatted correctly, but does not check the validity of the certificate; even expired certificates are accepted. Do not use this mode unless

you encounter problems that you cannot resolve with one of the other two modes. Some vCenter 6.x and later services might not work correctly in thumbprint mode.



Using Custom ESXi Certificates - If your company policy requires that you use a different root CA than VMCA, you can switch the certificate mode in your environment after careful planning. The recommended workflow is as follows:

- Obtain the certificates that you want to use.
- Remove all hosts from vCenter Server.
- Add the custom CA's root certificate to VECS (VMware Endpoint Certificate Store)
- Deploy the custom CA certificates to each host and restart services on that host.
- Switch to Custom CA mode. See "Change the Certificate Mode," on page 56.
- Add the hosts to the vCenter Server system.

Switching from Custom CA Mode to VMCA Mode

If you are using custom CA mode and decide that using VMCA works better in your environment, you can perform the mode switch after careful planning. The recommended workflow is as follows.

- Remove all hosts from the vCenter Server system.
- On the vCenter Server system, remove the third-party CA's root certificate from VECS.
- Switch to VMCA mode. See "Change the Certificate Mode," on page 56. (Link as above).
- Add the hosts to the vCenter Server system.

Control MOB access

See section "Control access to hosts (DCUI/Shell/SSH/MOB)".

Change default account access

With this, we understand that we must change the default roles. Check the Change default account access section above.

Restrict administrative privileges

Not all administrator users must have the Administrator role. You might want to create a **custom role** with the appropriate set of privileges and assign it to other administrators. Users with the vCenter Server Administrator role have privileges on all objects in the hierarchy.

Follow the principle of least privilege. Clone and customize role for nodes you need, and then assign this role to administrators.

Understand the implications of securing a vSphere environment

Being secured but not too "locked", have a good balance between security and manageability. Making any changes to the security of the vSphere environment might have perhaps large impacts on the manageability of the environment for you and your team.

You should always analyze your needs, your risks, and your requirements. Then change the security of your environment.

Check our **VCP6.5-DCV Study Guide Page** for more to study.

VCP6.5-DCV Objective 1.3 – Configure and Enable SSO and Identity Sources

Describe PSC architecture and components

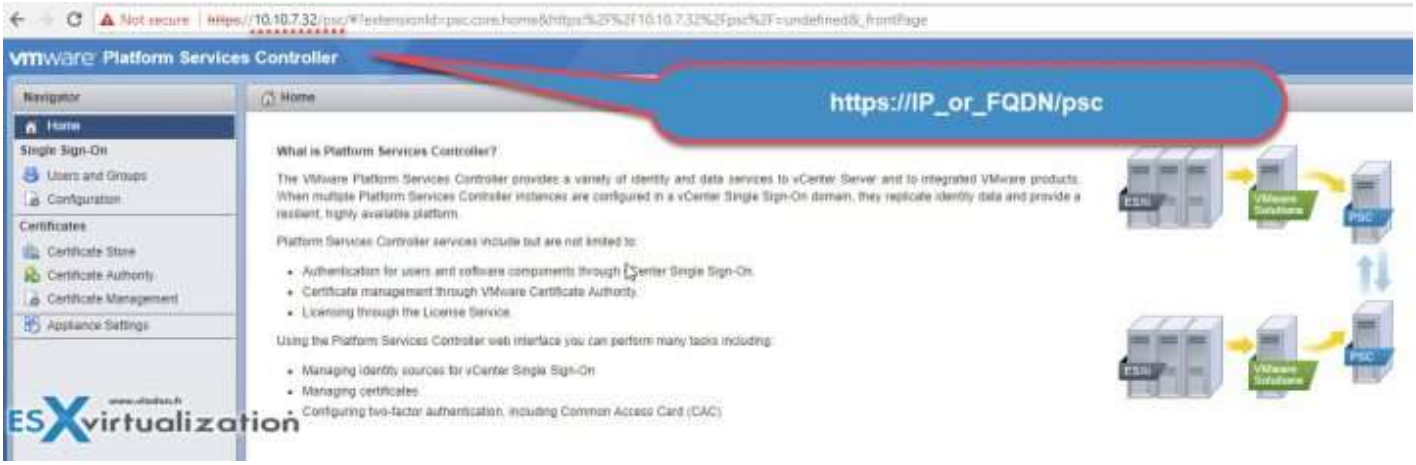
Platform Service Controler (PSC) can be installed along with vCenter (VC)or apart. You can also deploy a Platform Services Controller as an appliance or install it on Windows. If necessary, you can use a mixed operating systems environment.

There are three deployment types:

- VC with External PSC
- VC with Embedded PSC
- PSC only

If you have only a single site, VMware recommends using a single VM (VC+PSC). This is a standalone deployment type that has its own vCenter Single Sign-On domain with a single site. vCenter Server with an embedded Platform Services Controller is suitable for small environments. You cannot join other vCenter Server or Platform Services Controller instances to this vCenter Single Sign-On domain.

Example of PSC login page. Use https://IP_or-FQDN/psc



PSC Domain – when installing PSC, there is a prompt to create vCenter Single Sign-On domain (SSO) or join an existing domain. The domain name is used by VMware directory service for their internal LDAP structuring. You should always use another name than you're using for your Microsoft AD, Open LDAP or other directory services within your organization.

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

PSC Services:

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

PSC Allows you to:

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

USING SINGLE PSC IN SINGLE DOMAIN

The most simple is to deploy VMware PSC and vCenter server on a single VM, together. As such, the PSC component does not need a network connection to the vCenter server (as it communicates already; it is within the same VM).

TIP: How to deploy VMware VCSA 6.5 (VMware vCenter Server Appliance)

Figure 1-1. vCenter Server with an Embedded Platform Services Controller

Further, it has some following advantages:

- Fewer Windows Licenses
- Fewer Virtual machines to manage
- Using fewer resources

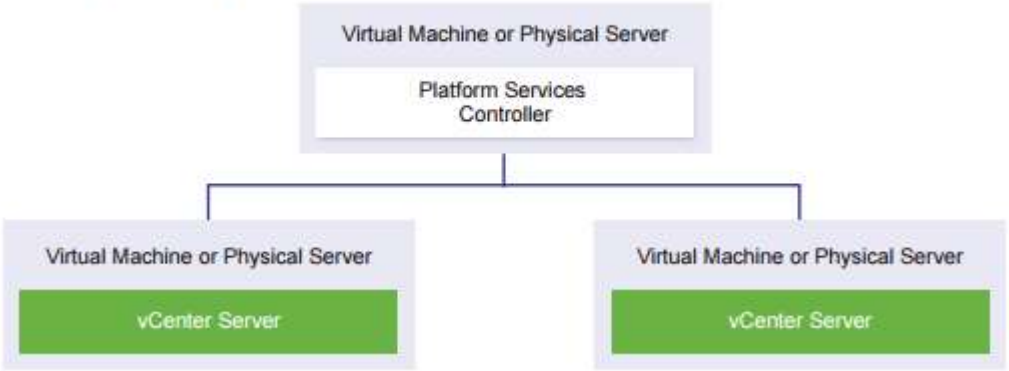
Disadvantages:

- Suitable for smaller-scale environments only
- Single sign-on domain only

USING MULTIPLE PSCS IN SINGLE DOMAIN

Single PSC has several vCenter servers “hooked” into it.

Figure 1-2. Example of Two vCenter Server Instances with a Common External Platform Services Controller



Advantages:

- Can assure HA with an external load balancer

Disadvantages:

- Consumes more resources

DIFFERENTIATE AVAILABLE AUTHENTICATION METHODS WITH VMWARE VCENTER

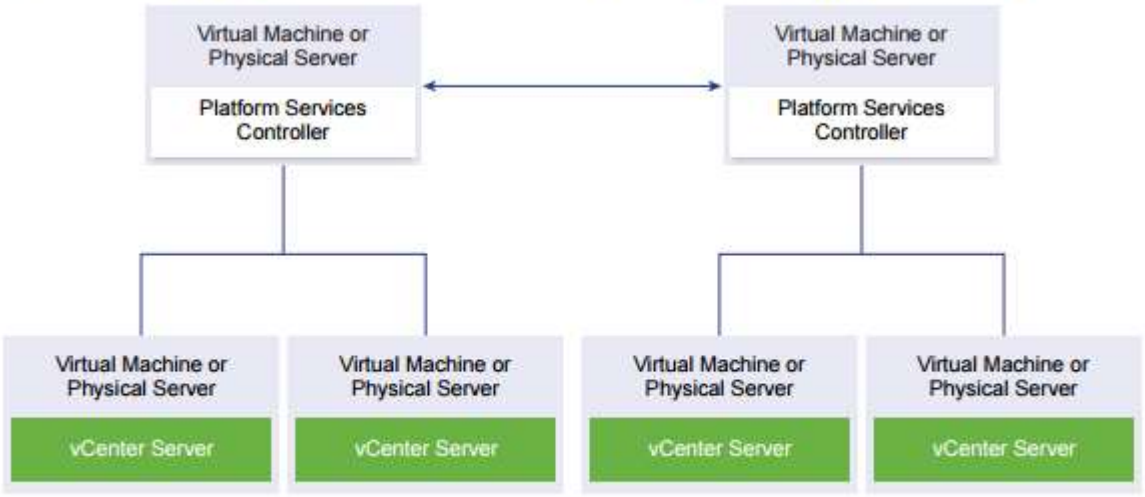
vCenter SSO is an authentication broker and security token exchange infrastructure which uses SAML tokens. When a user or a solution user can authenticate to vCenter Single Sign-On, that user receives a SAML token. Going forward, the user can use the SAML token to authenticate to vCenter services. The user can then perform the actions that user has privileges for. All traffic is encrypted for all communications.

Starting with vSphere 6.0, vCenter SSO is part of the PSC. The PSC contains the shared services that support vCenter Server and vCenter Server components. These services include vCenter Single Sign-On, VMware Certificate Authority, or License Service. For the initial handshake, users authenticate with a username and password, and solution users authenticate with a certificate.

PERFORM A MULTI-SITE PSC INSTALLATION

PSC can also be deployed without a load balancer, but in this case, in a case of failure the PSC, you must manually fail over the vCenter Server instances that are registered to it by repointing them to other functional PSC instances within the same site.

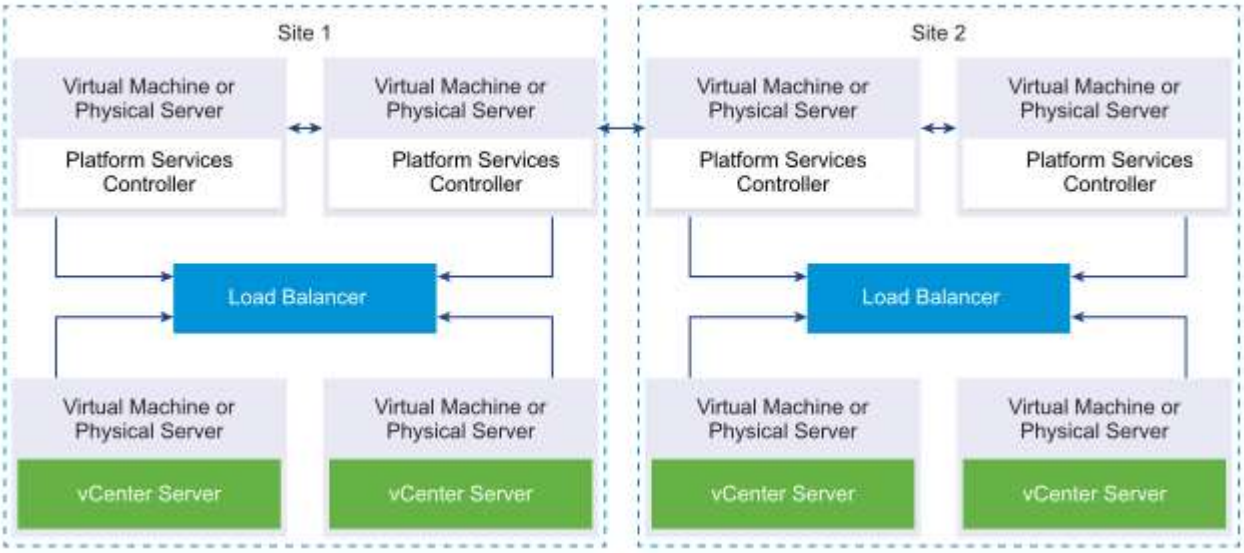
Figure 1-7. Example of Two Joined Platform Services Controller Instances with No a Load Balancer



When you join two or more Platform Services Controller instances in the same site with no load balancer, you configure Platform Services Controller high availability with a manual failover for this site.

- **Mixed Operating system** – Windows VM hosting PSC with two or more VMs running Windows-based vCenters, "hooked" into PSC.
- **External PSC with a load balancer**
- **External PSCs with a Load balancer on multiple sites** – you must install or deploy at least two joined PSC instances in your vCenter SSO domain.

Example of Two Load Balanced Pairs of Platform Services Controller Instances Across Two Sites



CONFIGURE/MANAGE IDENTITY SOURCES

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

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

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

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

CONFIGURE/MANAGE PLATFORM SERVICES CONTROLLER (PSC)

The Platform Services Controller (PSC) provides:

- Single Sign-On (SSO)
- Licensing
- Certificate Authority (VMCA)

You can deploy it on at the same time or apart and you can deploy it as Windows-based or Appliance based (VCSA). It's important to know that PSO is completely transparent working with Windows or VCSA based vCenter!

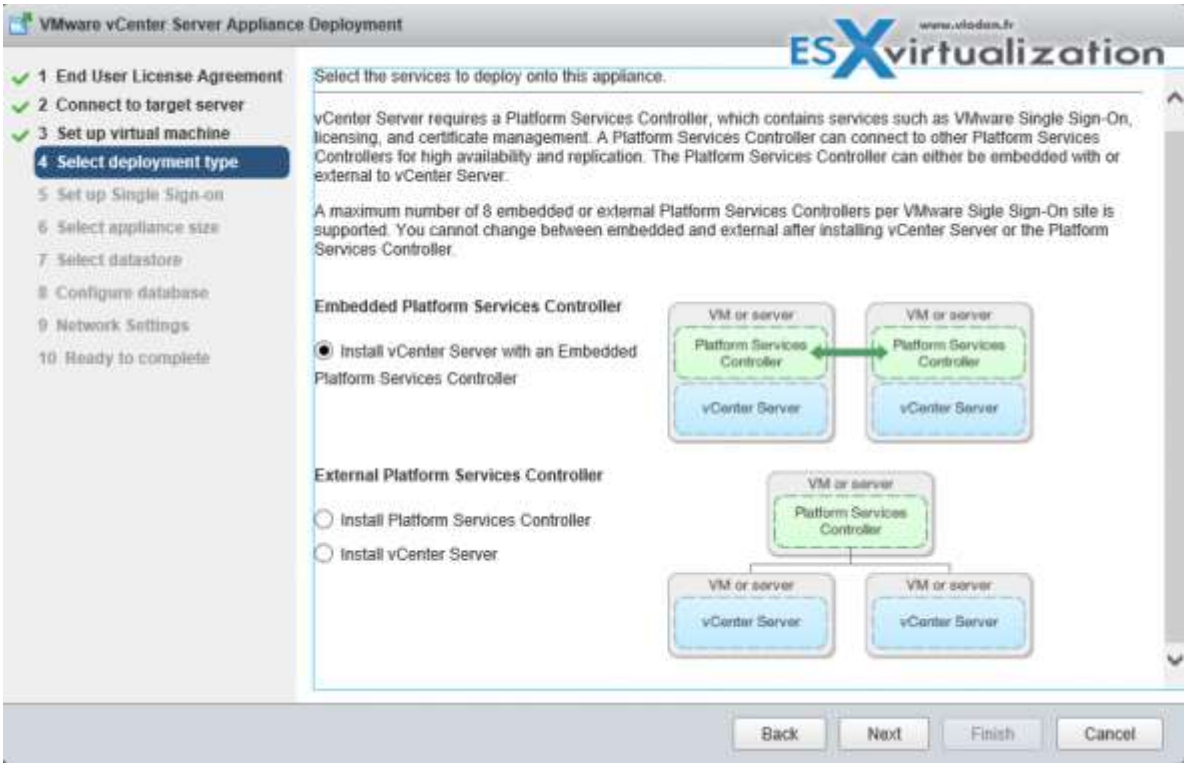
PSC Deployment Options –Two different types of installation are allowed:

- Embedded (in the same VM)
- External

The embedded PSC is meant to be used for standalone sites where a vCenter server will be the only SSO integrated solution. In this case, a replication to another PSC is not necessary.

External PSC shall be deployed in environments where there is more than one SSO enabled solution (vCenter Server, vRealize Automation, etc…) OR where replication to another PSC (another site) is necessary.

Here is the screenshot of the installation process (VCSA) showing the different options and changing the options also changes the different phases of the deployment (on the left).

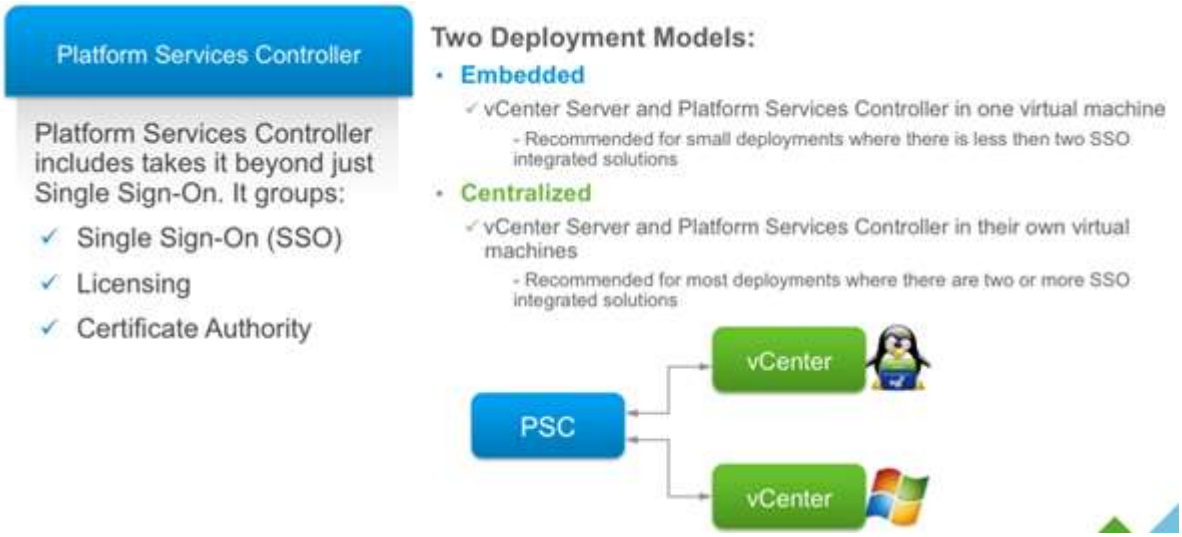


PSC features:

- Manages and generates SSL certificates for your vSphere environment.
- Stores and replicates VMware License Keys
- Stores and replicates permissions via the Global Permissions layer.
- Manages the storage and replication of TAGS and CATEGORIES.
- There is a Built-in automatic replication between different, logical SSO sites. (if any)
- There is only one single default domain for the identity sources.

DEPLOYMENT OPTIONS:

- Embedded Platform Service Controller
  All services bundled with the Platform Services Controller are deployed on the same virtual machine or physical server as vCenter Server.
- External Platform Service Controller
  The services bundled with the Platform Services Controller and vCenter Server are deployed on different virtual machines or physical servers.



CONFIGURE/MANAGE VMWARE CERTIFICATE AUTHORITY (VMCA)

When you first install vSphere, the default certificates are deployed with 10 years of life span. The VMCA generates those self-signed certs during the installation process, and provisions each of the ESXi host with a signed certificate by this root certificate authority. Earlier versions of vSphere with self-signed certificates are automatically replaced by new self-signed certificates by VMCA.

There are different ESXi Certificate replacement modes:

- **Default** – VMCA as cert authority where VMCA issues certs for your hosts. A self-signed root certificate is used. It issues certificates to vCenter, ESXi, etc and manages these certificates. These certificates have a chain of trust that stops at the VMCA root certificate. VMCA is not a general purpose CA and its use is limited to VMware components
- **Custom** – you can override and do issue certs manually via VMCA. You will need to issue a cert for every component, need to be installed into VECS.
- **Enterprise** - VMCA is used as a subordinate CA and is issued subordinate CA signing certificate. It can now issue certificates that trust up to the enterprise CA's root certificate. If you have already issued certs using VMCA Default and replace VMCA's root cert with a CA signing cert then all certificates issued will be regenerated and pushed out to the components.

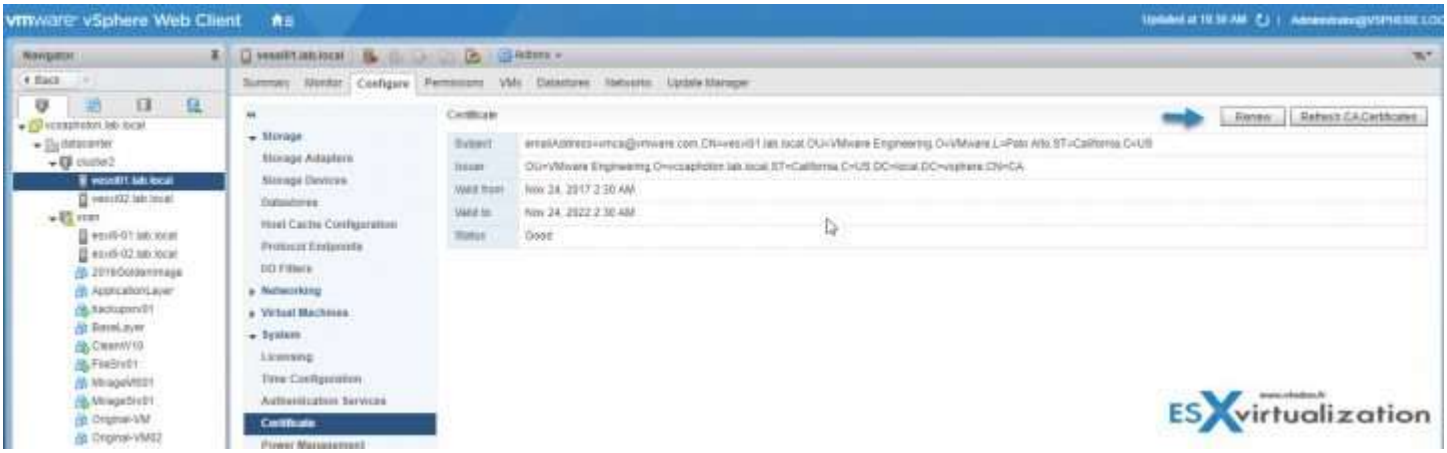
WHERE TO CHECK THE CERTIFICATES IN WEB CLIENT?

Home -> System Configuration -> Nodes -> Node -> Manage -> Certificate Authority

Note: If you're not a member of "SystemConfiguration.Administrators" group than you might want to **add yourself** there.

vSphere web client certificate management

- View access to look at certs and expiration info
- ESXi cert management is performed via web client
- Logon to the web client as a member of the **CAAdmins group**.



VCP6.5-DCV: ENABLE/DISABLE SINGLE SIGN-ON (SSO) USERS

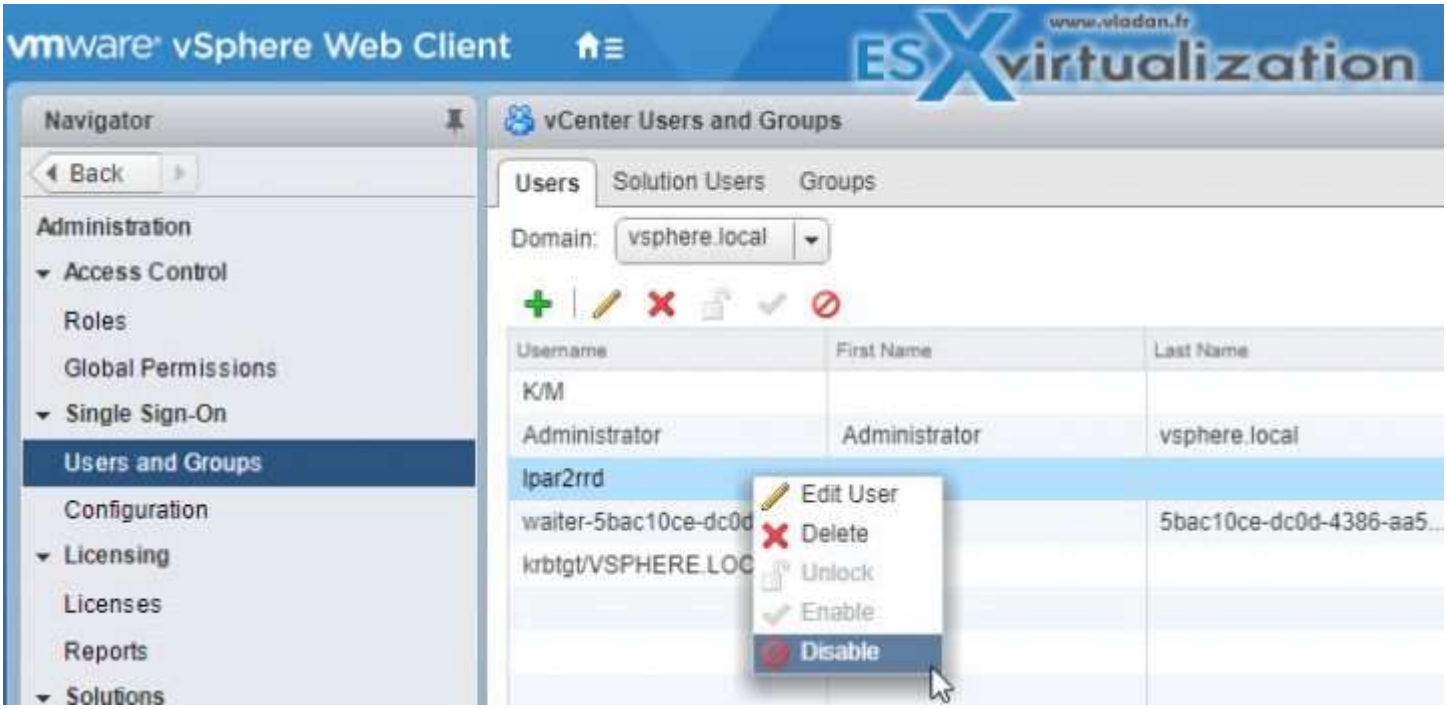
The VMware SSO uses different configuration policy which can be found via vSphere Web client only:

Administration > **Single Sign-On** > **Configuration Policies**

- Password Policy
- Lockout Policy
- Token Policy

TO ENABLE/DISABLE SSO USER:

Connect via **vSphere Web client** > **Administration** > **SSO** > **Users and groups** > **Right-click User** > **Disable** will show in the column “disabled”



Password Policy

You can configure the following parameters:

- **Description** – Password policy description. Required.
- **Maximum lifetime** – Maximum number of days that a password can exist before it has to be changed.
- **Restrict re-use** – Number of the user's previous passwords that cannot be set again.
- **Maximum length** – Maximum number of characters that are allowed in the password.
- **Minimum length** – Minimum number of characters required in the password.
- **Character requirements** – Minimum number of different character types required in the password.
- **Identical adjacent characters** – Maximum number of identical adjacent characters allowed in the password.

SSO groups:

Administrator - can manage SSO users added to this group have global permissions to SSO & all of inventory that is managed by that SSO domain

CAAdmins - can manage VMCA

LicenseService.Administrators - can manage licenses

Upgrade a single/complex PSC installation

Upgrade VCSA 5.5 or 6.0 and the PSC appliance 6.0 to version 6.5. The upgrade of the VCSA or PSC appliance is a migration of the old version to the new version (including deployment of the new appliance of version 6.5). You can deploy the new appliance on an ESXi host 5.5 or later, or on the inventory of a vCenter Server instance 5.5 or later. Wizard driven. You assign a temporary IP address to the new appliance to facilitate the configuration and services data migration from the old appliance to the newly deployed appliance.

After the migration, the IP address and hostname of the old appliance are applied to the new upgraded appliance of version 6.5. At the end of the upgrade, the temporary IP address is released and the old appliance is powered off.

Version 6.5 of the VCSA uses the embedded PostgreSQL DB. If you are upgrading a vCenter Server Appliance that is using an external database, the external database will be migrated to the embedded PostgreSQL database of the new upgraded appliance. During the upgrade, you must select a storage size for the new appliance that is suitable for the database size.

Version 6.5 of the VCSA uses the embedded VMware vSphere Update Manager Extension (VUM) service. If you are upgrading a VCSA that is using an external VUM instance, the external VUM instance will be migrated to the embedded VUM Extension of the new upgraded appliance. The embedded VUM Extension uses the embedded PostgreSQL DB. Before the upgrade, you must run the Migration Assistant on the source VMware Update Manager instance.

For topologies with external PSC instances, you must upgrade the replicating PSC instances in a sequence. After the successful upgrade of all PSC instances in the domain, you can perform concurrent upgrades of multiple VCSA appliances that point to a common external PSC instance.

The VCSA installer contains executable files GUI and CLI upgrades which you can use alternatively.

The GUI upgrade is a two-stage process:

- **The first stage** - is a deployment wizard that deploys the OVA file of the new appliance on the target ESXi host or vCenter Server instance.
- **The Second stage** - after deployment phase you are redirected to the second stage of the process that sets up and transfers the services and configuration data from the old appliance to the newly deployed appliance.

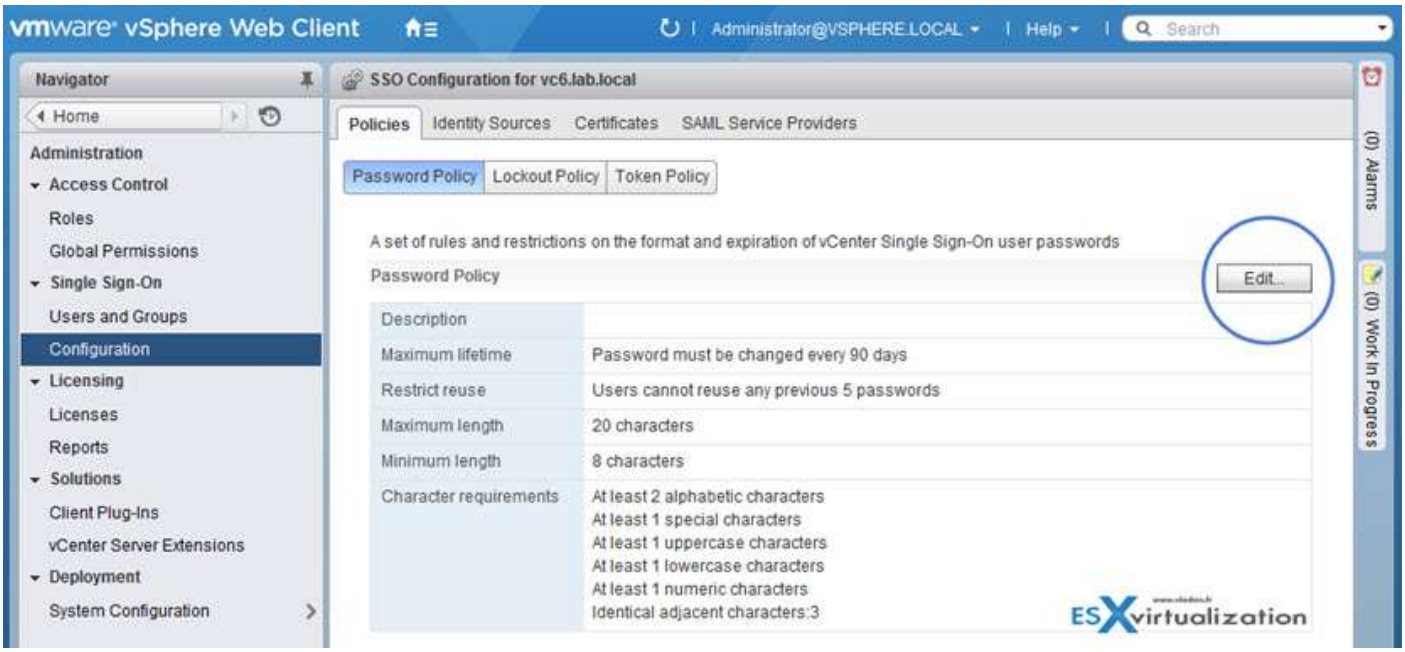
The CLI upgrade method involves running a CLI command against a JSON file that you previously prepared. The CLI installer parses the configuration parameters and their values from the JSON file and generates an OVF Tool command that automatically deploys the new appliance and transfers the services and configuration data from the old appliance.

If the appliance that you are upgrading is configured in a mixed IPv4 and IPv6 environment, only the IPv4 settings are preserved.

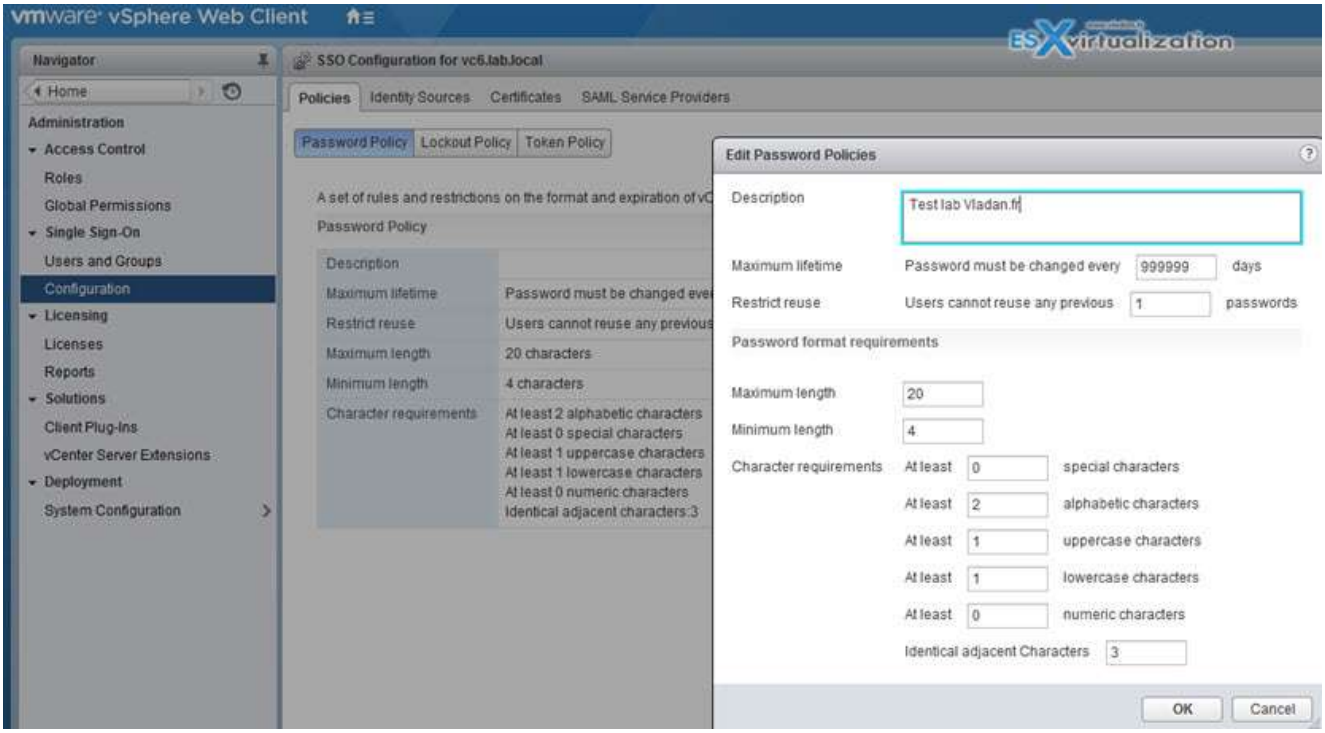
If the appliance that you are upgrading uses a non-ephemeral distributed virtual port group, the port group is not preserved. After the upgrade, you can manually connect the new appliance to the original non-ephemeral distributed virtual port group of the old appliance

CONFIGURE SSO POLICIES

VMware SSO policies are accessible through **Home > Administration > SSO > Configuration**.



By clicking the Edit button, you are able to change values there…



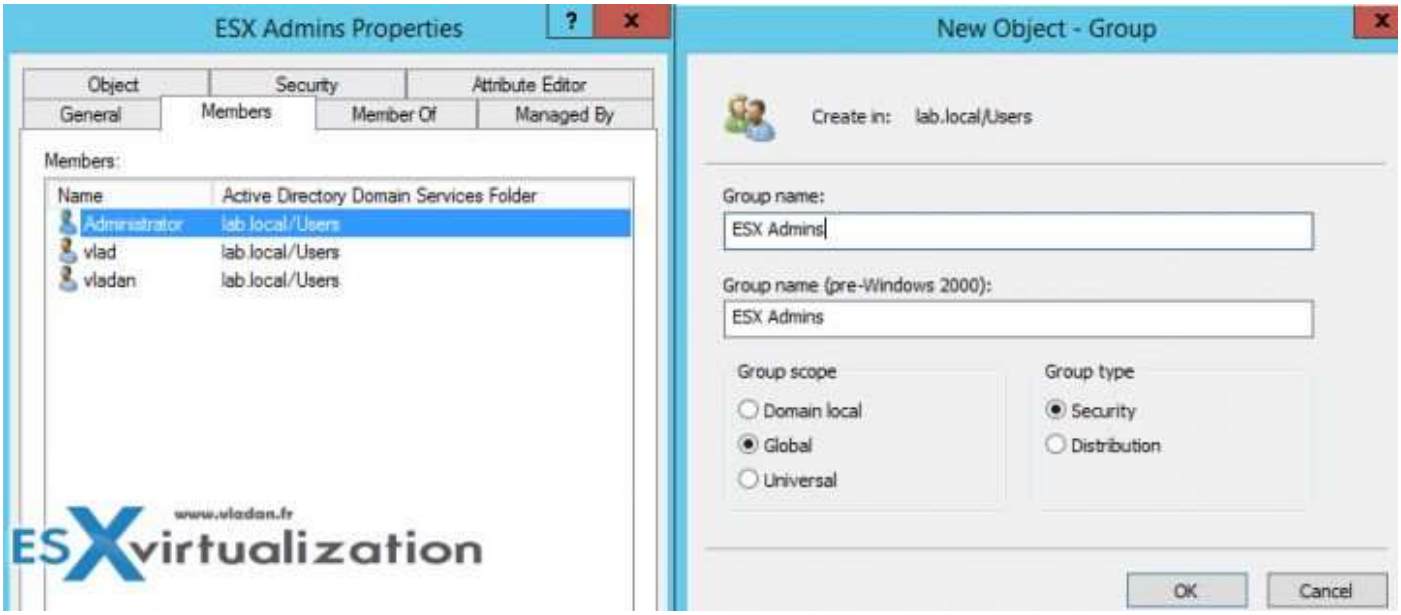
If you leave the default values and after 90 days you want to log-in, you might end up with messages saying that:

- User Account is locked.
- User Account is disabled.

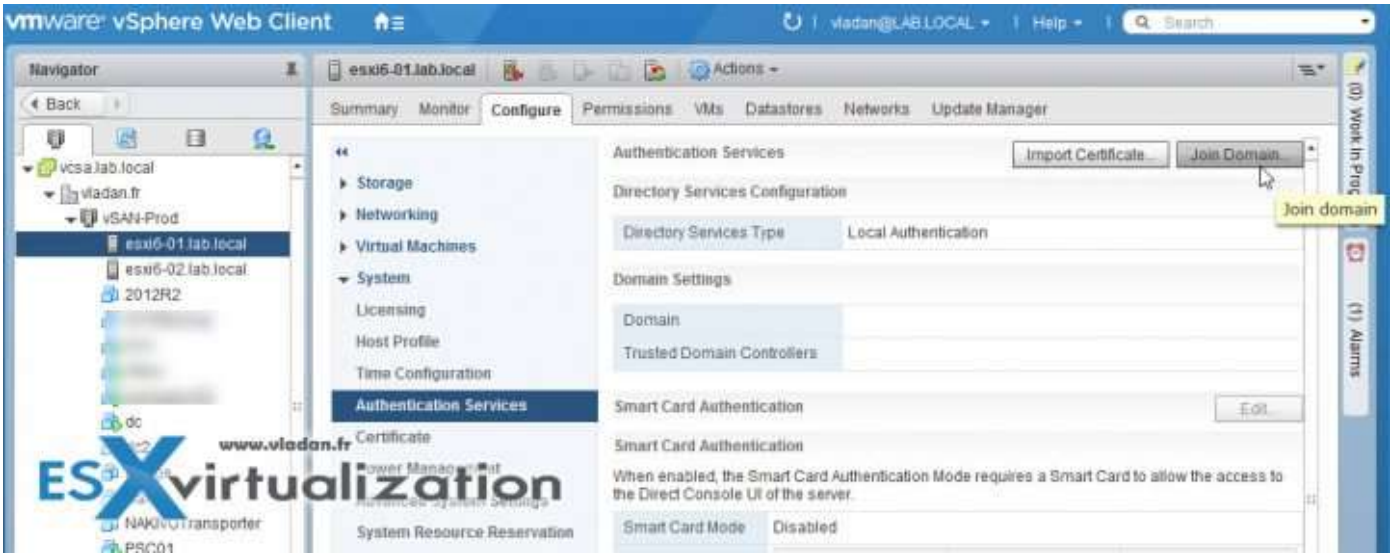
Those SSO policies are pretty much the same as in vSphere 5.5, but with a difference that in [vSphere 5.5 we also had an administrator password expiry](#) on the vCenter server appliance (VCSA). The VCSA 6.0 is pretty much locked out and the GUI we use to manage VCSA accessible via the port 5480 is no longer available.

ADD AN ESXI HOST TO AN AD DOMAIN

Create the ESX Admins group in the AD domain and populate it with user accounts or groups to which administrative access to the hosts should be granted. Also, additional AD user accounts and groups can be granted with appropriate access to hosts. Go to your Domain controller and create a Global Security group called “ESX Admins” > Make a domain administrator part of this group.



Log in to your vCenter with the vSphere Web Client and **Select your ESXi host > Configure > System > Authentication Services > Join Domain.**



Enter the domain name and user credentials for your environment > **click OK**.

Use the form name.tld or name.tld/container/path.

Check this: [Using the ESX Admins AD group with ESX/ESXi 4.1 and ESXi 5.x/6.x domain membership and user .]

You should also make sure that on your DNS server you have created static forward AND reverse DNS records for your host. DNS can be a pain if configured wrong. A good DNS resolution is a good start on healthy vSphere setup.

NTP is also an important configuration step. ESXi should use, when possible, an external source of time. Synchronize the time between ESXi and the directory service system using NTP.

TIP: [How to configure ESXi 6.5 Network Time Protocol (NTP) via Host Client?]

First, you must set up the key management server (KMS) cluster. You add the KMS and establish trust with the KMS. When you add a cluster, you are prompted to make it the default. You can explicitly change the default cluster. vCenter Server provisions keys from the default cluster.

You add a KMS to your vCenter Server system from the vSphere Web Client or by using the public API. vCenter Server creates a KMS cluster when you add the first KMS instance. When you add the KMS, you are prompted to set this cluster as a default. You can later change the default cluster explicitly.

After vCenter Server creates the first cluster, you can add KMS instances from the same vendor to the cluster. You can set up the cluster with only one KMS instance. If your environment supports KMS solutions from different vendors, you can add multiple KMS clusters.

WHO MANAGES ENCRYPTION?

It is not a 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? Do all your vSphere admins need to have access to encryption? Possibly. But possibly NOT. VMware has created a new default role, "**No Cryptography Administrator**", but we won't go into details as it is not the purpose of this lesson.

Detailed steps are for setting up KMS cluster can be found on pages 137 and 152 within the latest Security Guide PDF.

VCP6.5-DCV OBJECTIVE 1.4 – SECURE VSPHERE VIRTUAL MACHINES

Enable/Disable Virtual Machine Encryption

VM encryption will work by applying a new Storage policy to a VM. It is Policy driven. It will be per-VM policy application model.

There is **no modification within the guest OS**. It does not matter which OS you're running (Linux, Windows, DOS, iOS). The encryption is happening **outside of the Guest OS**. So the guest does not have an access to the keys.

VM encryption allows protection against data theft. VMware VM encryption encrypts VMDKs, virtual machine files, and core dump files. It does not encrypt log files, VM config files. You might ask why? It's because there are no sensitive data within those files.

If someone who is not authorized tries to extract some data, they get only meaningless data. The VM owns the VMDK, has the necessary key to decrypt the data whenever read and then fed to the guest operating system. It's done by using industry-standard encryption algorithms to secure this traffic with minimal overhead. But yes, there is a slight overhead.

VMware **does not** recommend to encrypt vCenter server appliance VMs.

The components:

- **Key Management Server (KMS)** - not provided by VMware, but rather by VMware partners.
- **vCenter Server** - keeps credentials for logging into the KMS. It "pushes" keys to the ESXi host when the host needs a key.
- **ESXi Hosts** - The host must have encryption mode enabled. The keys that the ESXi host generates are called internal keys. These keys typically act as data encryption keys (DEKs). ESXi host makes sure that the guest data for encrypted VMs is encrypted when stored on disk. Also, the ESXi make sure that the guest data for encrypted VMs are not sent over the network without encryption.

The workflow:

vSphere Web client > Right Click VM > VM Policies > Edit VM storage policies > Drop down select policy > Apply to All

To decrypt > select storage policy > Apply to all.

Key Management Server - vCenter Server requests keys from an external KMS. The KMS generates and stores the keys, and passes them to vCenter Server for distribution. You can use the vSphere Web Client or the vSphere API to add a cluster of KMS instances to the vCenter Server system. If you use multiple KMS instances in a cluster, all instances must be from the same vendor and must replicate keys.

vCenter server - required privilege is "*Cryptographic operations.Decrypt*".

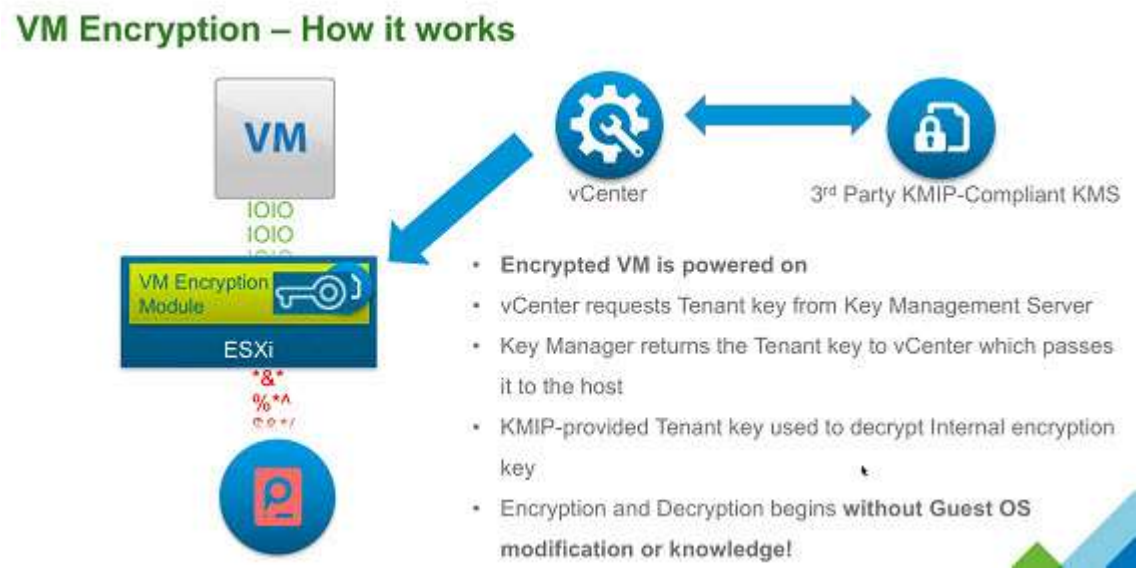
ESXi Hosts - ESXi hosts are responsible for several aspects of the encryption workflow. vCenter Server pushes keys to an ESXi host when the host needs a key. The host must have encryption mode enabled. The current user's role must include cryptographic operation privileges.

The keys that the ESXi host generates are called internal keys in this document. These keys typically act as data encryption keys (DEKs).

How does it work?

When you power On the **VM** which has the Encryption Storage policy applied to, **vCenter** retrieves the key from the Key Manager and sends the key down to the **VM encryption Module** and unlocks that key in the ESXi hypervisor.

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.



Describe Secure Boot

Secure boot, also called UEFI Secure Boot, is a security standard that makes sure that your PC boots using only software that is trusted by the PC manufacturer. For certain VMs hardware versions and operating systems, you can enable secure boot just as you can for a physical machine.

If an OS supports UEFI secure boot it means that all the bits and pieces participating in the boot process, use software which is signed, including the bootloader, the operating system kernel, and operating system drivers. The VM's default configuration includes several code signing certificates:

- Microsoft cert that is used **only for booting Windows**.
- Microsoft cert that is used for **third-party code that is signed by Microsoft**, such as Linux bootloaders.
- VMware certificate that is used only for **booting ESXi inside a VM**.

The VM's default config has a cert for authenticating requests to modify the secure boot configuration including the secure boot revocation list, from inside the virtual machine, which is a Microsoft KEK (Key Exchange Key) certificate.

UEFI Secure Boot Requirements:

- VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot. You can upgrade those virtual machines to a later version of VMware Tools when it becomes available.
- For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode. Remove VMware Host-Guest Filesystem from VMware Tools before you enable secure boot.
- Check the VM's OS and Firmware supports UEFI boot.
- EFI firmware

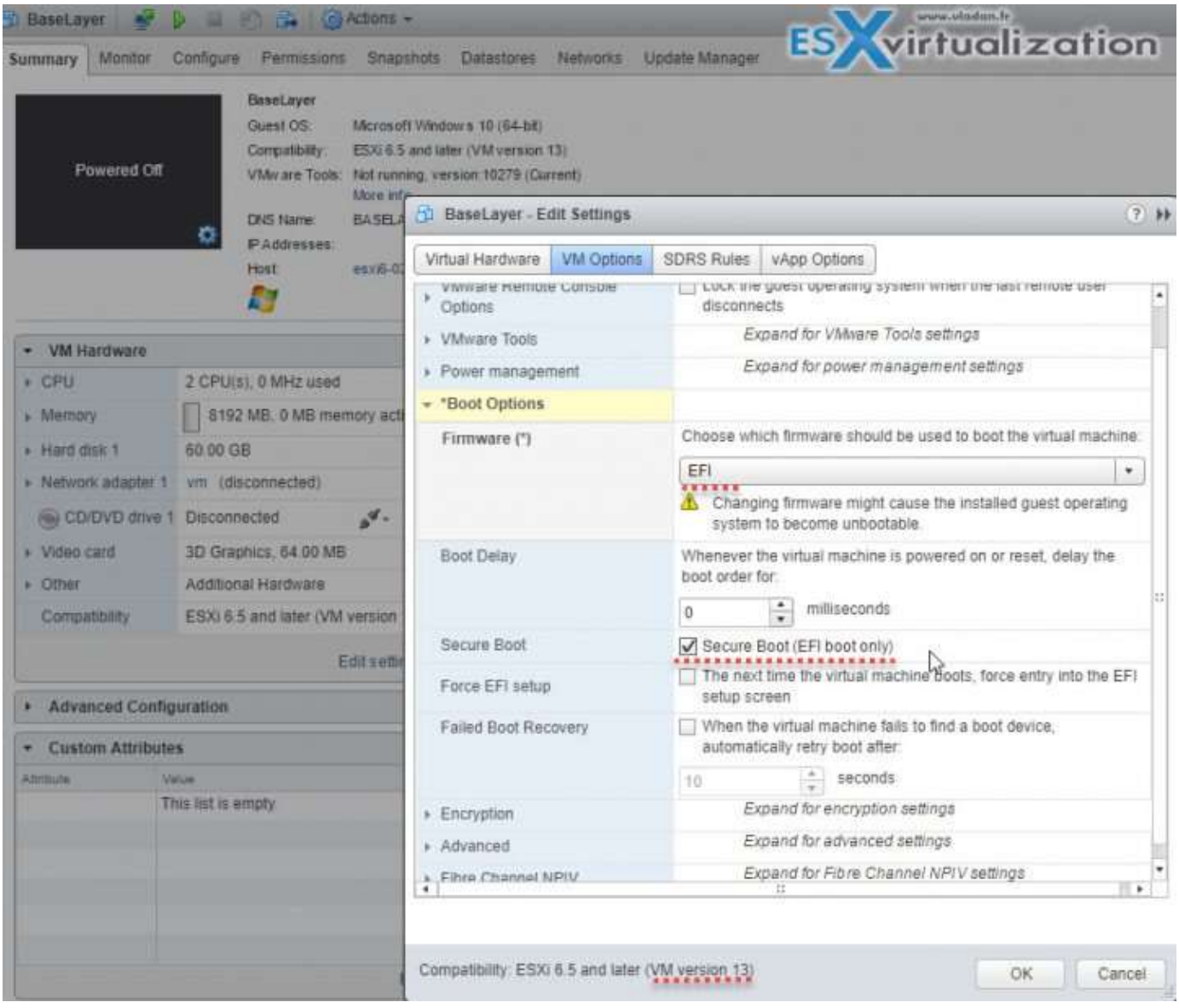
- Virtual hardware version 13 or later. (VMX-13)

If requirements are not met, the **checkbox is grayed out:**

The workflow:

- Gracefully shut down your VM. If the VM is running, the **checkbox is grayed out.**
- Privileges - "*VirtualMachine.Config.Settings*" privileges to enable or disable UEFI secure boot for the virtual machine.

vSphere Web Client > select VM > Edit Settings > Boot Options > firmware is set to EFI > Enable secure boot check box > click OK.



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

Harden virtual machine access

Use templates as much as you can. A template allows you to save your security settings to have uniformized configuration for all future deployments for your VMs. For further configuration, you should consider using scripting, PowerCLI, allowing you to perform mass modification on VMs, grouped by folder structure within your datacenter.

The guest OS should be protected with anti-spyware and anti-malware software. You should patch the template VM on regular basis in order to keep the patches up-to-date.

Disable unnecessary functions within the VM. You can optimize further by disabling unnecessary services

- Disable unused services in the OS. For example, if the system runs a file server, turn off any Web services.
- Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adapters.
- Disable unused functionality, such as unused display features or HGFS (Host Guest File System)
- Turn off screen savers.
- Do not run the X Window system on top of Linux, BSD, or Solaris guest operating systems unless it is necessary.
- Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls. Console access might, therefore, allow a malicious attack on a virtual machine.

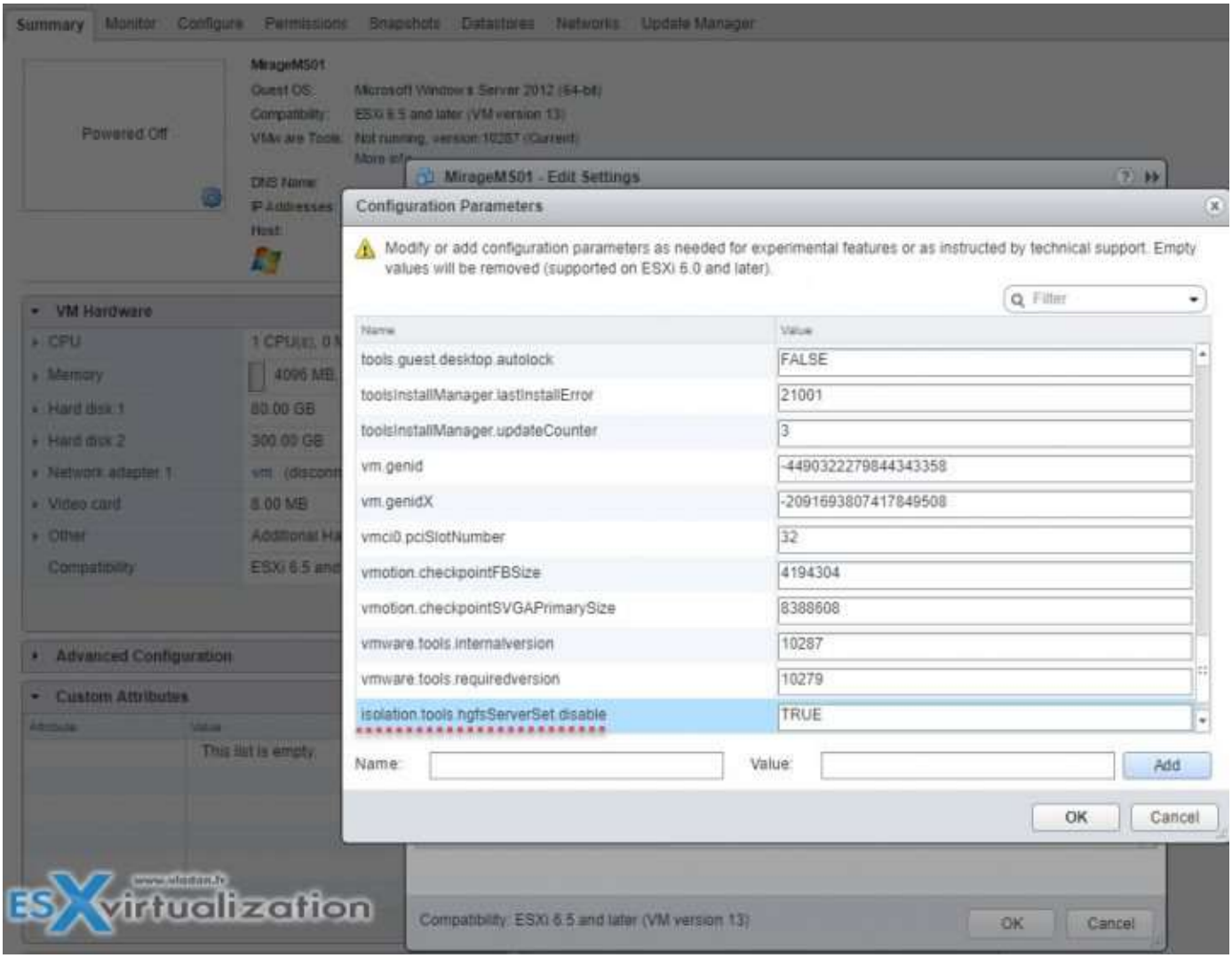
Control VMware Tools installation

Required privilege: Interaction .VMware Tools install (allows to mount or unmount VMware tools ISO)

Control VM data access

HGFS stands for Host guest file system. Certain operations such as automated VMware Tools upgrades use a component in the hypervisor called host guest file system (HGFS). In high-security environments, you can disable this component to minimize the risk that an a hacker can use HGFS to transfer files inside the guest operating system.

vSphere Web Client > Select VM > Right-click > Edit Settings > VM Options > Click Advanced > Edit configuration > Check the ***isolation.tools.hgfsServerSet.disable*** is set to **TRUE**.



After that change, the VMX process no longer responds to commands from the tools process. APIs that use HGFS to transfer files to and from the guest operating system, such as some VIX commands or the VMware Tools auto-upgrade utility, no longer work.

Disable Copy and Paste Operations Between Guest Operating System and Remote Console - by default, this setting is disabled.

There are 3 advanced values to check within the same section as on the image above:

isolation.tools.copy.disable true
isolation.tools.paste.disable true
isolation.tools.setGUIOptions.enable false

If those settings are enabled then the following could happen:

As soon as the console window gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard for the virtual machine console. If a user copies sensitive information to the clipboard before using the console, the user— perhaps unknowingly—exposes sensitive data to the virtual machine.

Configure virtual machine security policies

Check the Security policy information on pages 113 and 121 of the vSphere ESXi and vCenter Server 6.5 Security Guide PDF.

Harden virtual machine against Denial-of-Service attacks

VMware recommends disabling virtual disk shrinking, which can be used by non-administrative users which have access to the guest OS. Shrinking of virtual disk allows reclaiming unused space. If you shrink repeatedly, you can cause a disk unavailability and cause a denial of service.

Select VM > Edit Settings > Click Advanced > VM Options > Edit Configuration.

isolation.tools.diskWiper.disable TRUE
isolation.tools.diskShrink.disable TRUE

When you disable this feature, you cannot shrink virtual machine disks when a datastore runs out of space.

Control VM-VM communications

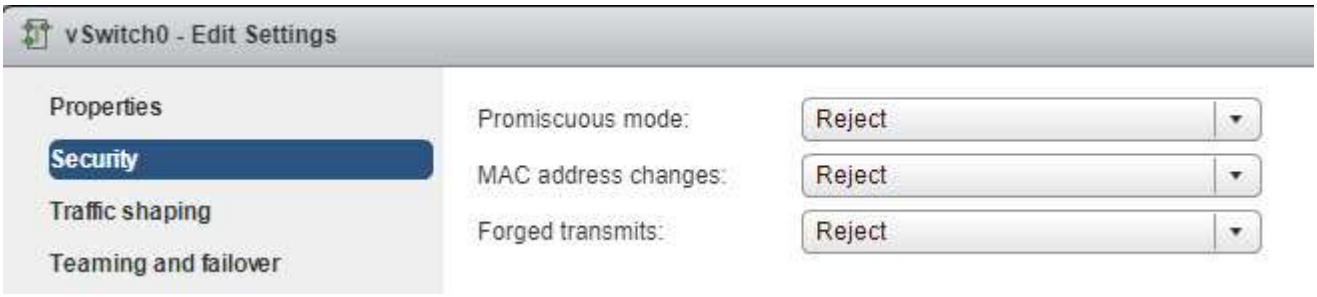
This was previously done via VMCI. (Since vSphere 6.5 this is disabled).

The Virtual Machine Communication Interface (VMCI) is an infrastructure that provides fast and efficient communication between a virtual machine and the host operating system and between two or more virtual machines on the same host.

Control VM device connections

Check Remove Unnecessary Hardware Devices section, but basically, any enabled or connected device represents a potential attack channel. Users and processes with privileges
on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Configure network security policies



Securing Standard Switch Ports With Security Policies - VM NIC can send frames that appear to be from a different machine or impersonate another machine so that it can receive network frames that are intended for that machine. Also, like physical network adapters, a VM NIC can be configured so that it receives frames targeted for other machines. Both scenarios present a security risk.

When you create a standard switch for your network, you add port groups in the vSphere Web Client to impose a policy for the virtual machines and VMkernel adapters for system traffic attached to the switch.

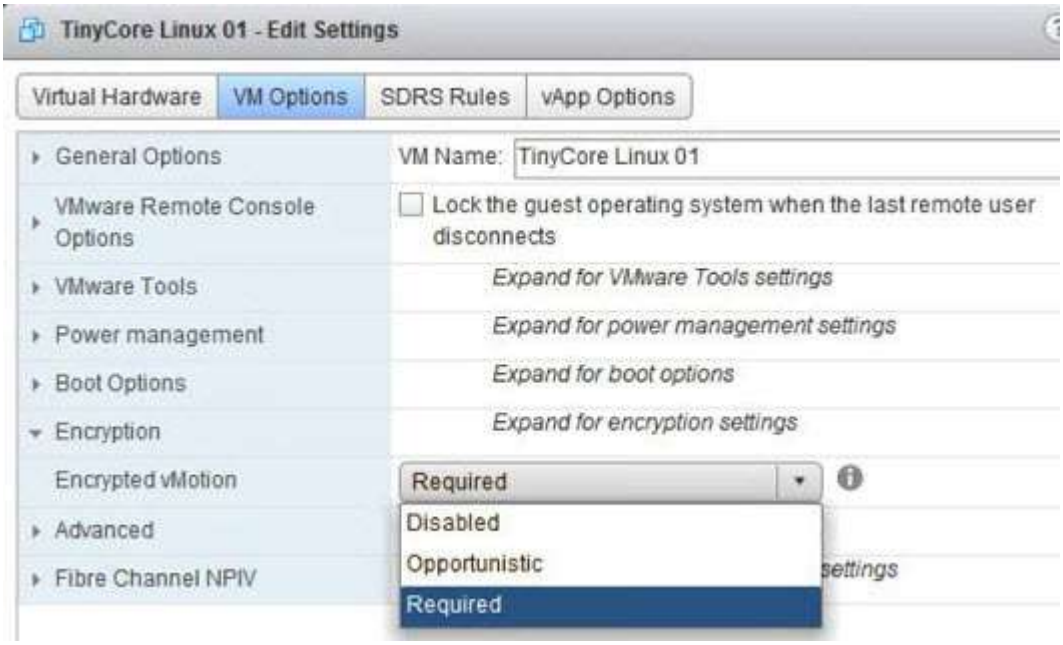
As part of adding a VMkernel port group or virtual machine port group to a standard switch, ESXi configures a security policy for the ports in the group. You can use this security policy to ensure that the host prevents the guest operating systems of its virtual machines from impersonating other machines on the network. This security feature is implemented so that the guest operating system responsible for the impersonation does not detect that the impersonation was prevented.

The security policy determines how strongly you enforce protection against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profiles you must understand how virtual machine network adapters control transmissions and how attacks are staged at this level.

Configure encrypted vMotion

There are 3 settings which are possible on the **per-VM** basis:

- **Disabled** – do not use encrypted vMotion
- **Opportunistic** – use encrypted vMotion if the source and destination hosts support it. If not it will do a normal vMotion.
- **Required** – allow only encrypted vMotion. If the source or destination does not support encrypted vMotion, then the vMotion fails.



It is **one-time generated random key, which is generated by vCenter** (not the KMS).

Starting with vSphere 6.5, vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

Encrypted vSphere vMotion secures confidentiality integrity and authenticity of data that is transferred with vSphere vMotion. Encrypted vSphere vMotion supports all variants of vSphere vMotion for

unencrypted virtual machines, including migration across vCenter Server systems. Migration across vCenter Server systems is not supported for encrypted virtual machines.

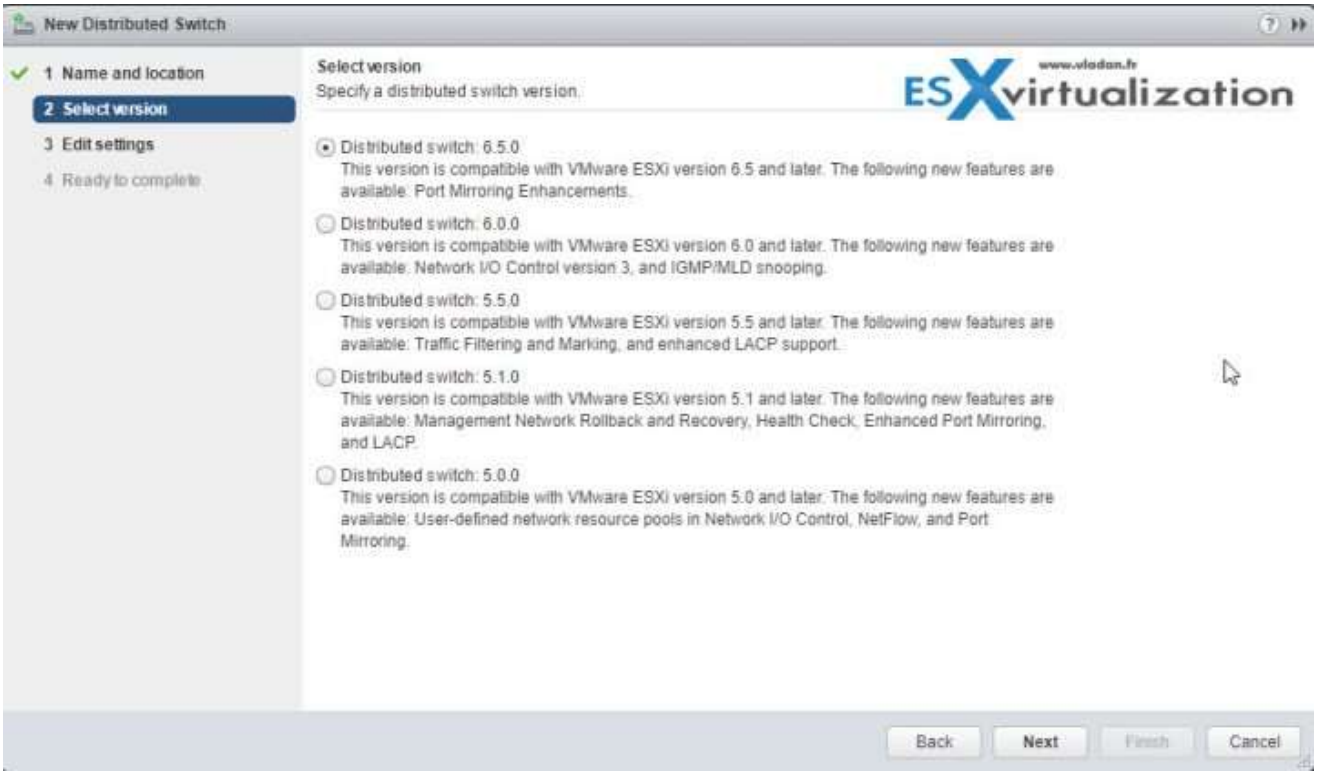
When you encrypt a virtual machine, the virtual machine keeps a record of the current encrypted vSphere vMotion setting If you later disable encryption for the virtual machine, the encrypted vMotion setting remains at Required until you change the setting explicitly. You can change the settings using Edit Settings.

VCP6.5-DCV Objective 2.1 – Configure policies/features and verify vSphere networking

Create/Delete a vSphere Distributed Switch

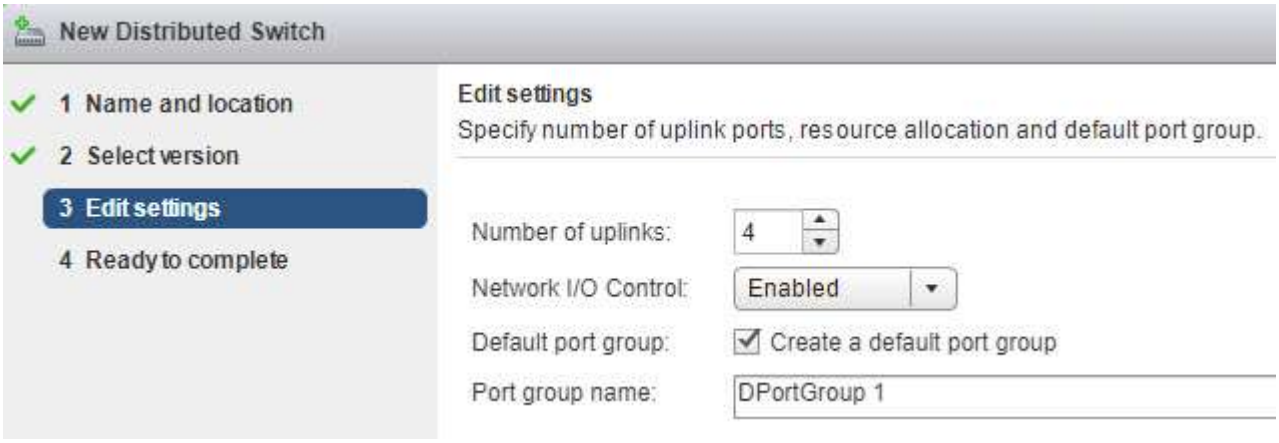
VMware vDS allows managing networking of multiple ESXi hosts, from a single location.

vSphere Web Client > **Right-Click Datacenter object** > **New distributed switch** > **Enter some meaningful name** > **Next** > **Select Version** > **Next** > **Enter the number of uplinks.**



Uplink ports connect the distributed switch to physical NICs on associated hosts. The number of uplink ports is the maximum number of allowed physical connections to the distributed switch per host. Select the Create a default port group check box to create a new distributed port group with default settings for this switch.

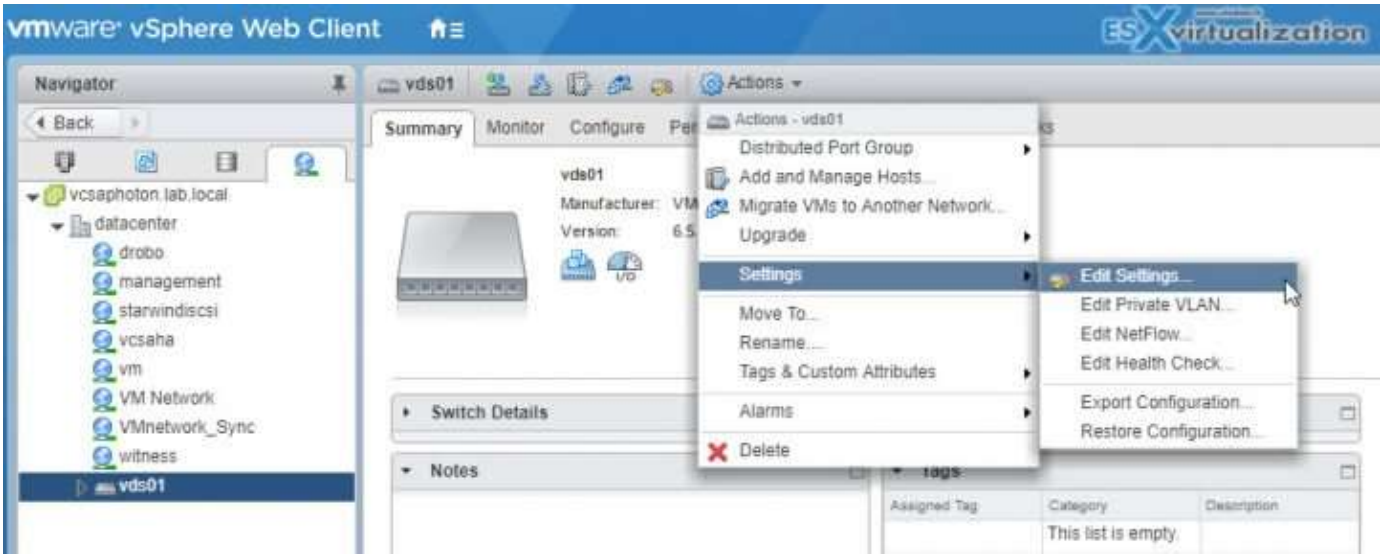
Enable or disable Network I/O control via the drop-down menu.



To change the settings of the distributed switch select **networking** > select your **Distributed switch** > **Actions** > **Settings** > **Edit Settings**.

There you can:

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



ADD/REMOVE ESXI HOSTS FROM A VSPHERE DISTRIBUTED SWITCH

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

- Create distributed port groups for VM networking
- Create distributed port groups for VMkernel services, such as vMotion, VSAN, FT etc...

- Configure a number of uplinks on the distributed switch for all physical NICs that you want to connect to the switch

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

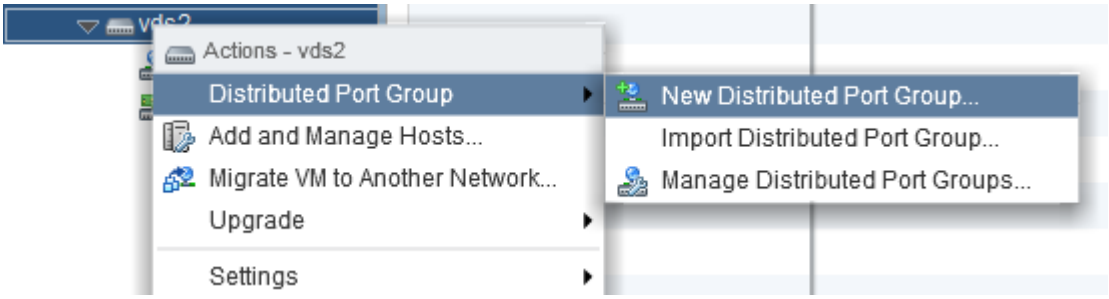
Removing Hosts from a vSphere Distributed Switch - Before you remove hosts from a distributed switch, you must migrate the network adapters that are in use to a different switch.

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

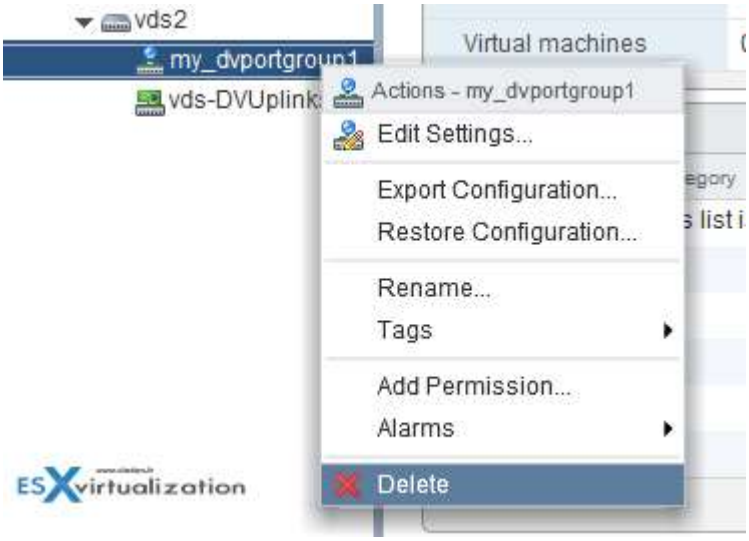
To migrate host networking to standard switches, you must migrate the network adapters in stages. For example, remove physical NICs on the hosts from the distributed switch by leaving one physical NIC on every host connected to the switch to keep the network connectivity up. Next, attach the physical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

ADD/CONFIGURE/REMOVE DVPORT GROUPS

Right-click on the vDS > New Distributed Port Group.



To remove a port group. Simple. Right-click **on the** port group **>** delete…

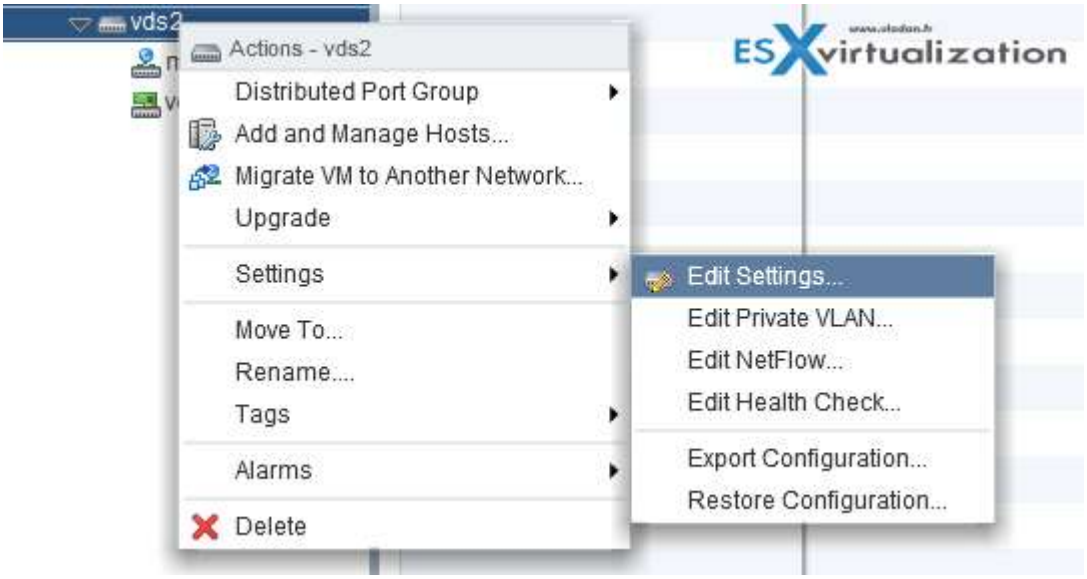


A distributed port group specifies port configuration options for each member port on a vSphere distributed switch. Distributed port groups define how a connection is made to a network.

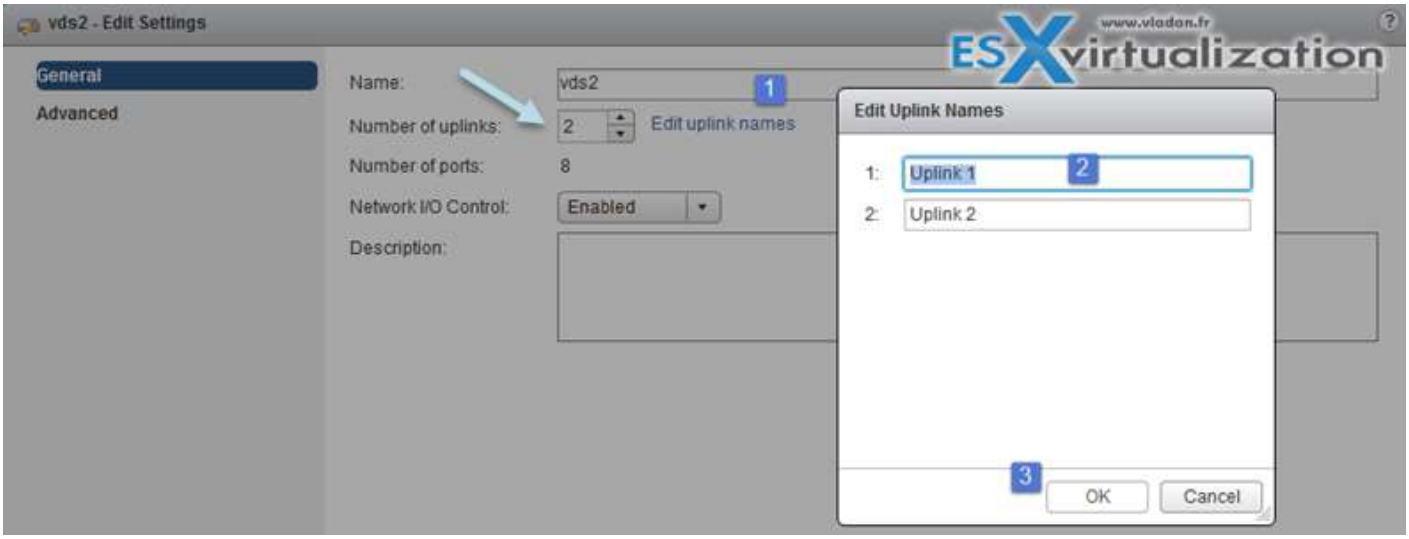
ADD/REMOVE UPLINK ADAPTERS TO DVUPLINK GROUPS

If you want to add/remove (increase or decrease) a number of uplinks you can do so by going to the properties of the vDS. For consistent networking configuration throughout all hosts, you can assign the same physical NIC on every host to the same uplink on the distributed switch.

Right-click on the **vDS** > **Edit settings**

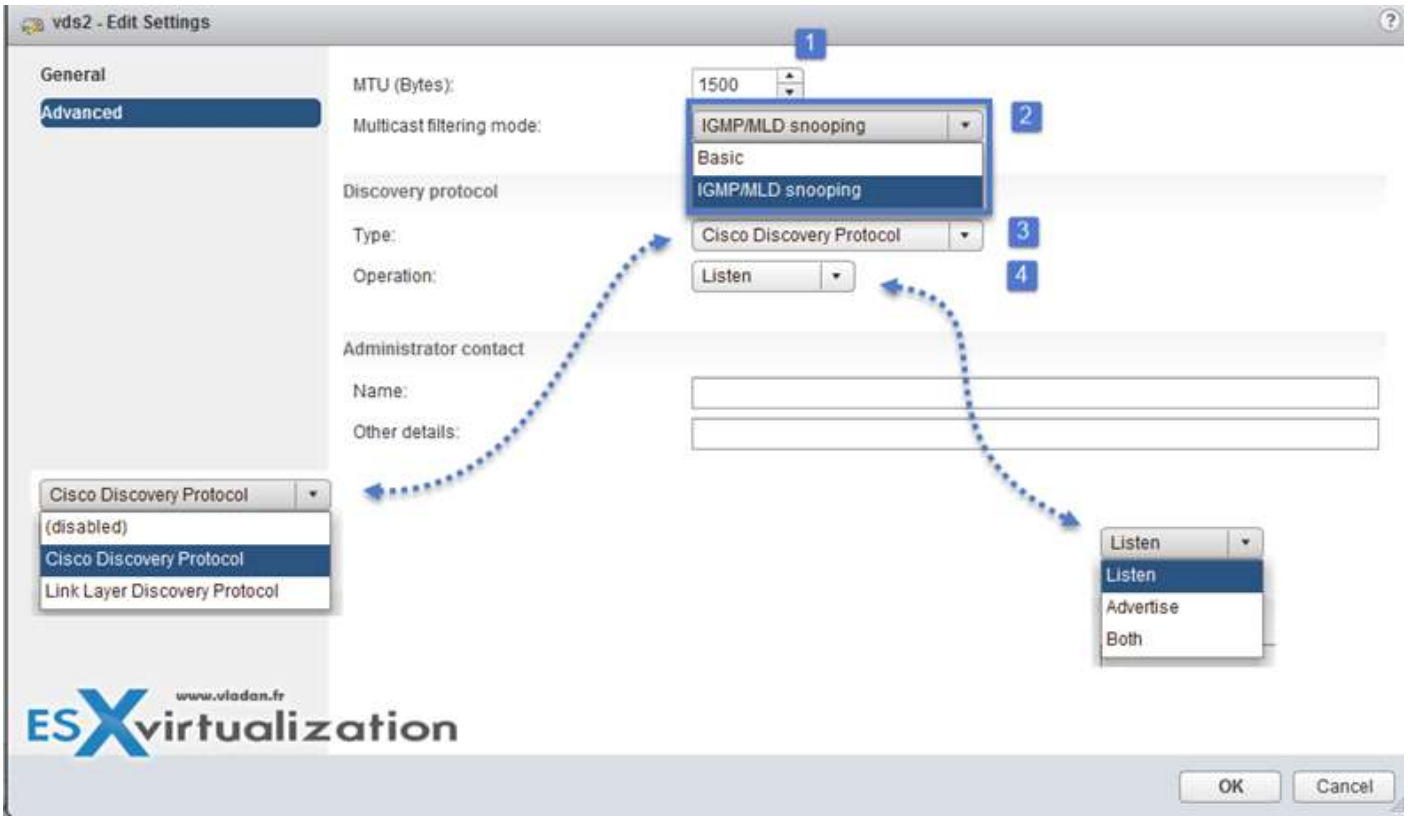


And on the next screen, you can do that… Note that at the same time you can give different names to your uplinks…



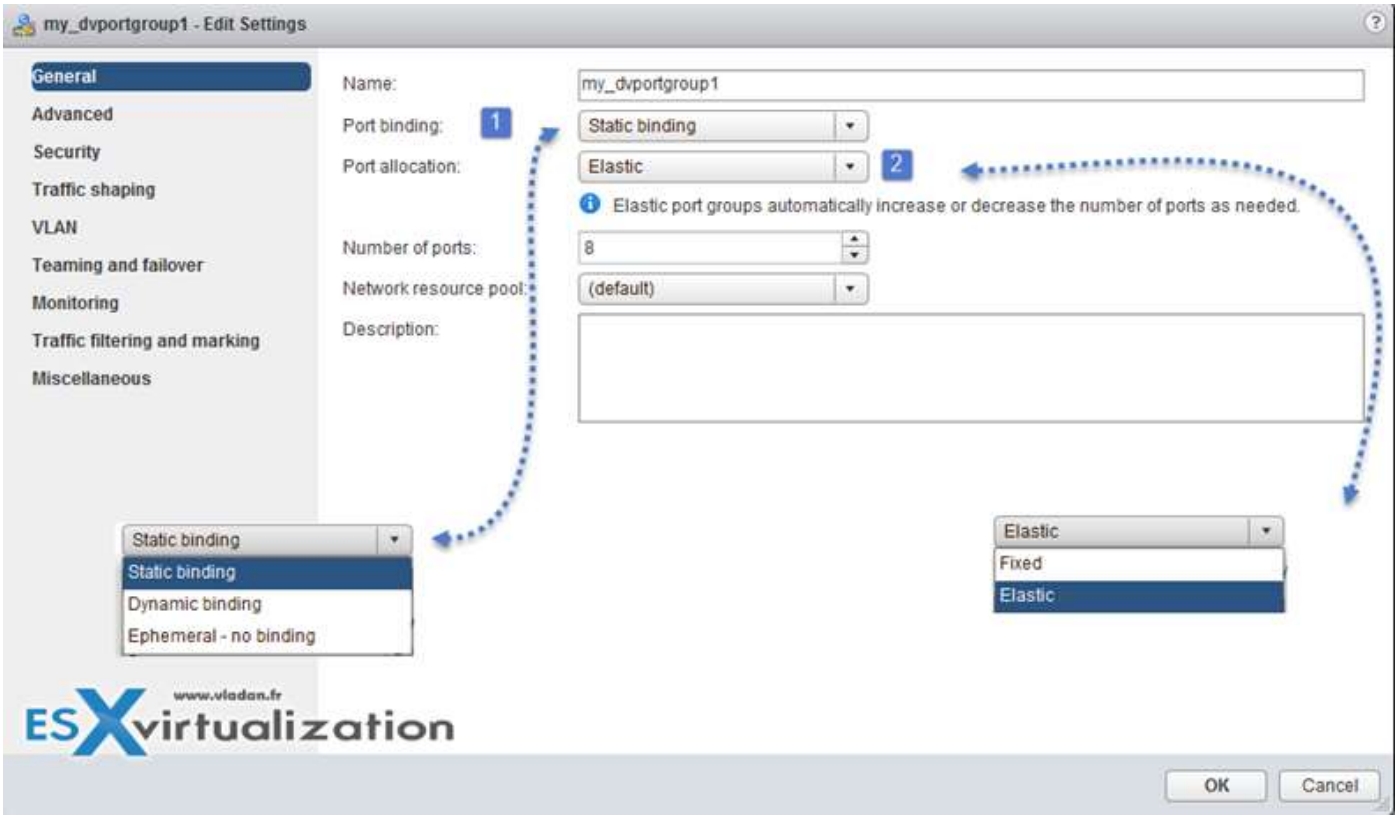
CONFIGURE VSPHERE DISTRIBUTED SWITCH GENERAL AND DVPORT GROUP SETTINGS

General properties of vDS can be reached via **Right-click on the vDS** > **Settings** > **Edit settings**



Port binding properties (at the dvPortGroup level – **Right click port group** > **Edit Settings**)

- **Static binding** – Assigns a port to a VM when the virtual machine is connected to the PortGroup.
- **Dynamic binding** – It's kind of deprecated. For best performance use static binding.
- **Ephemeral** – No binding.



PORT BINDING

- **Static binding -** Allows assigning a port to a VM when the VM connects to the distributed port group.
- **Dynamic binding** - Assign a port to a virtual machine the first time the virtual machine powers on after it is connected to the distributed port group. Dynamic binding has been deprecated since ESXi 5.0.
- **Ephemeral – no binding -** No port binding. You can assign a virtual machine to a distributed port group with ephemeral port binding also when connected to the host.

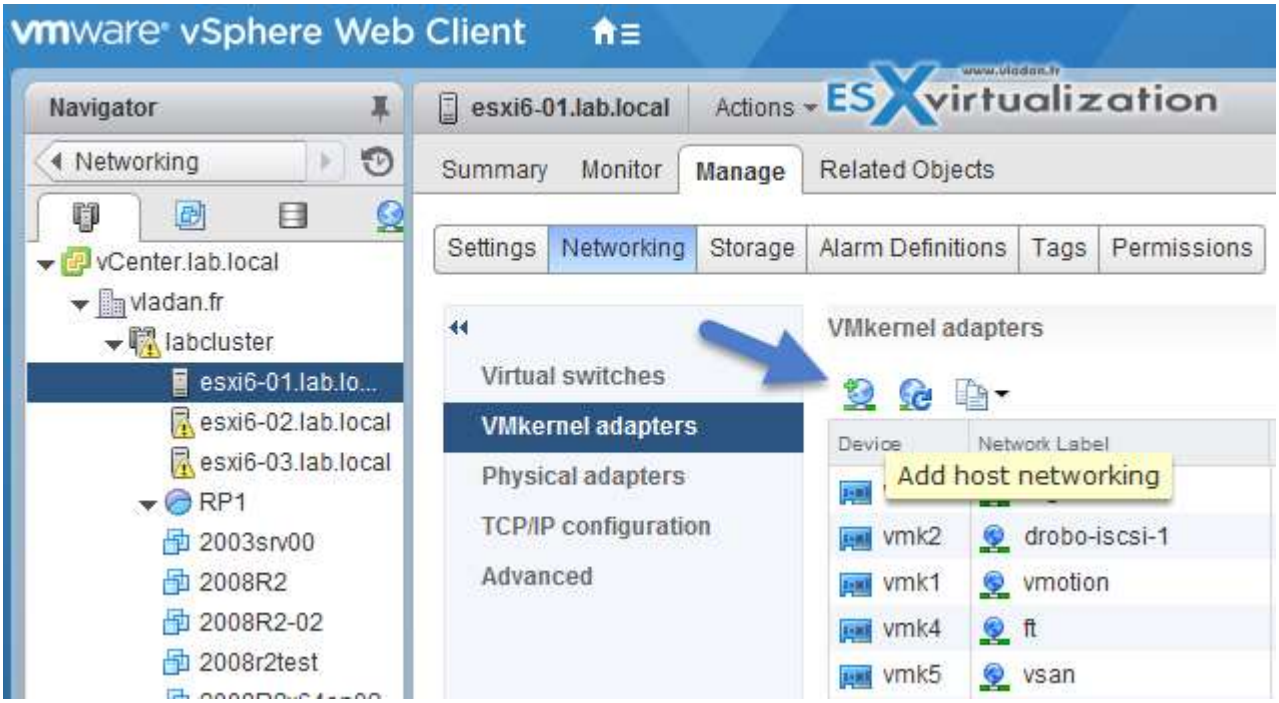
PORT ALLOCATION

- **Elastic -** The default number of ports is eight. When all ports are assigned, a new set of eight ports is created. This is the default.
- **Fixed -** The default number of ports is set to eight. No additional ports are created when all ports are assigned.

CREATE/CONFIGURE/REMOVE VIRTUAL ADAPTERS

VMkernel adapters can be added/removed at the Networking level

vSphere **Web Client** > **Host and Clusters** > Select **Host** > **Manage** > **Networking** > **VMkernel adapters**

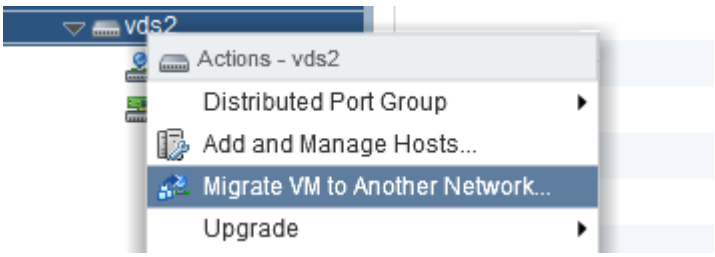


Different VMkernel Services, like:

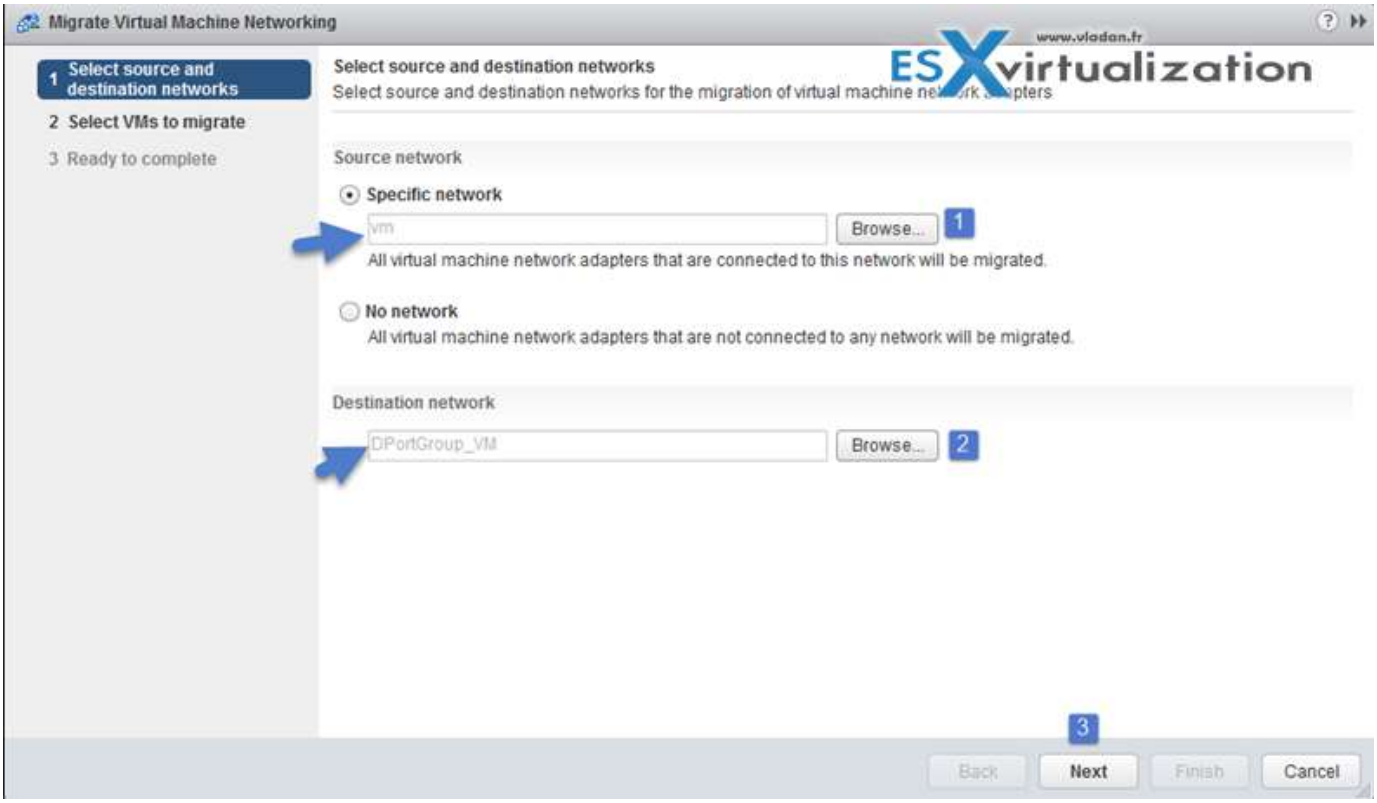
- vMotion traffic
- Provisioning traffic
- Fault Tolerance (FT) traffic
- Management traffic
- vSphere Replication traffic
- vSphere Replication NFC traffic
- VSAN traffic

Migrate virtual machines to/from a vSphere Distributed Switch

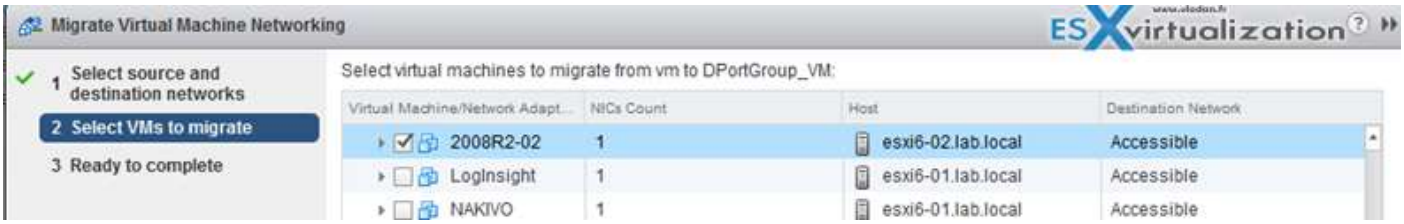
Migrate VMs to vDS. **Right-click vDS > Migrate VM to another network**



Make sure that you previously created a distributed port group with the same VLAN that the current VM is running… (in my case the VMs run at VLAN 7)



Pick a VM…

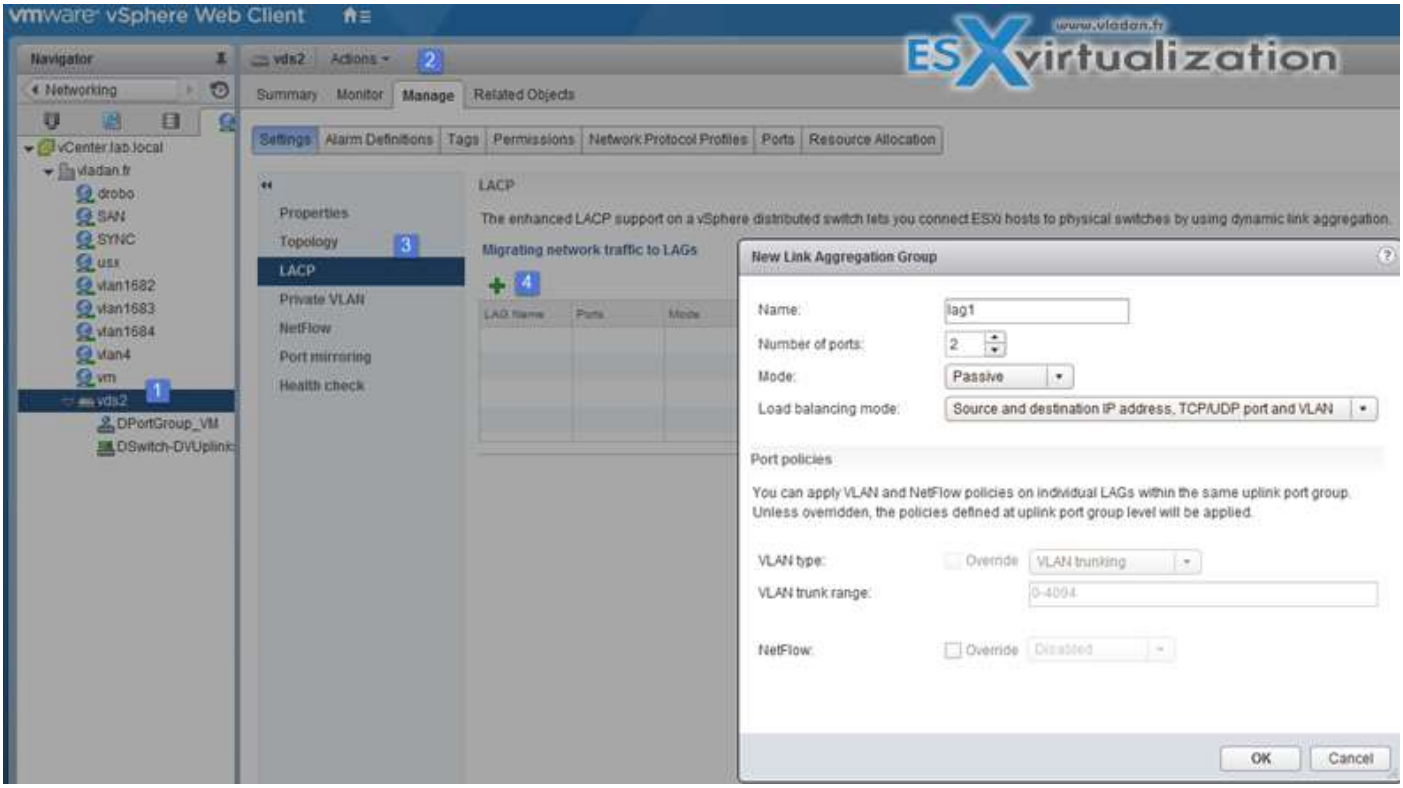


Done!

CONFIGURE LACP ON VDS GIVEN DESIGN PARAMETERS

vSphere **Web Client** > **Networking** > **vDS** > **Manage** > **Settings** > **LACP**

Create Link Aggregation Groups (LAG)



LAG Mode can be:

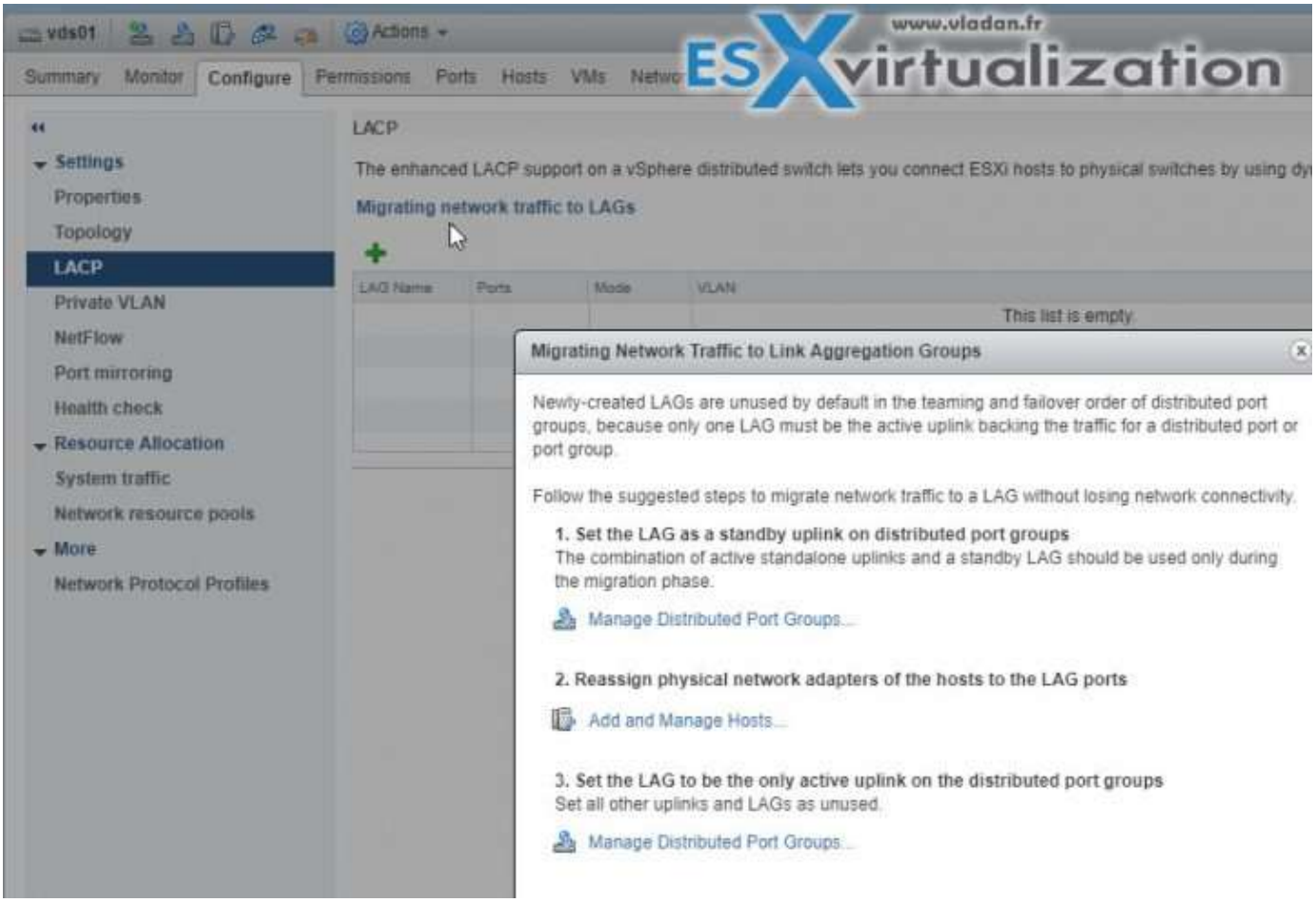
- **Passive** – where the LAG ports respond to LACP packets they receive but do not initiate LACP negotiations.
- **Active** – where LAG ports are in active mode and they initiate negotiations with LACP Port Channel.

LAG load balancing mode (LNB mode):

- Source and destination IP address, TCP/UDP port and VLAN
- Source and destination IP address and VLAN
- Source and destination MAC address
- Source and destination TCP/UDP port
- Source port ID
- VLAN

Note that you must configure the LNB hashing same way on both virtual and physical switch, at the LACP port channel level.

Migrate Network Traffic to Link Aggregation Groups (LAG)



DESCRIBE VDS SECURITY POLICIES/SETTINGS

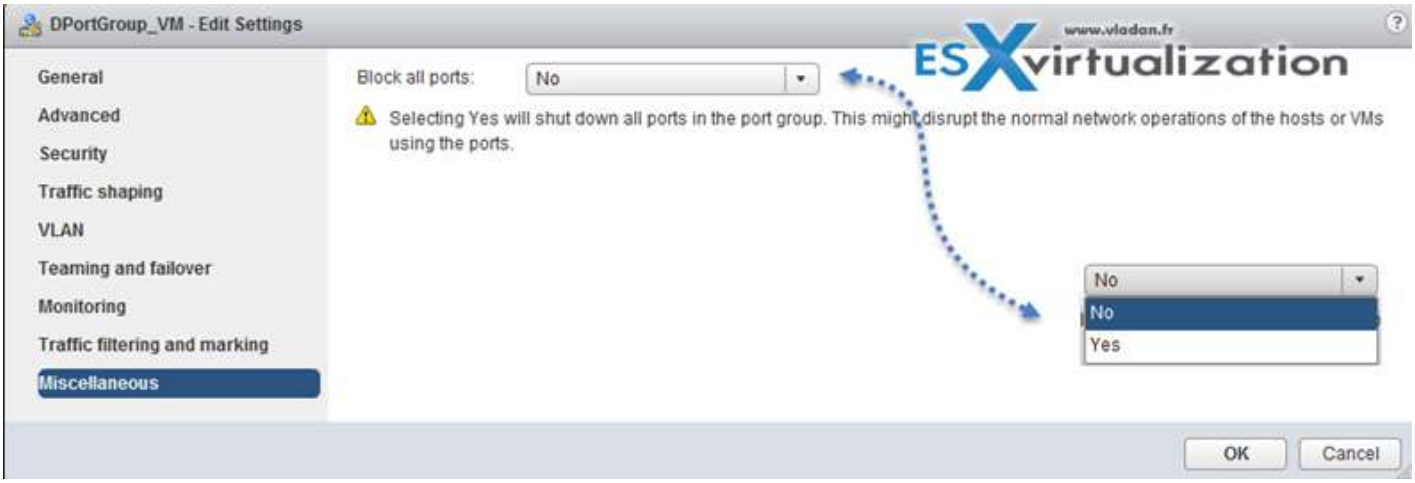
Note that those security policies exist also on standard switches. There are 3 different network security policies:

- **Promiscuous mode** – Reject is by default. In case you set to **Accept** > the guest OS will receive all traffic observed on the connected vSwitch or PortGroup.
- **MAC address changes** – Reject is by default. In case you set to **Accept** > then the host will accept requests to change the effective MAC address to a different address than the initial MAC address.
- **Forged transmits** – Reject is by default. In case you set to **Accept** > then the host does not compare source and effective MAC addresses transmitted from a virtual machine.

Network security policies can be set on each vDS PortGroup.

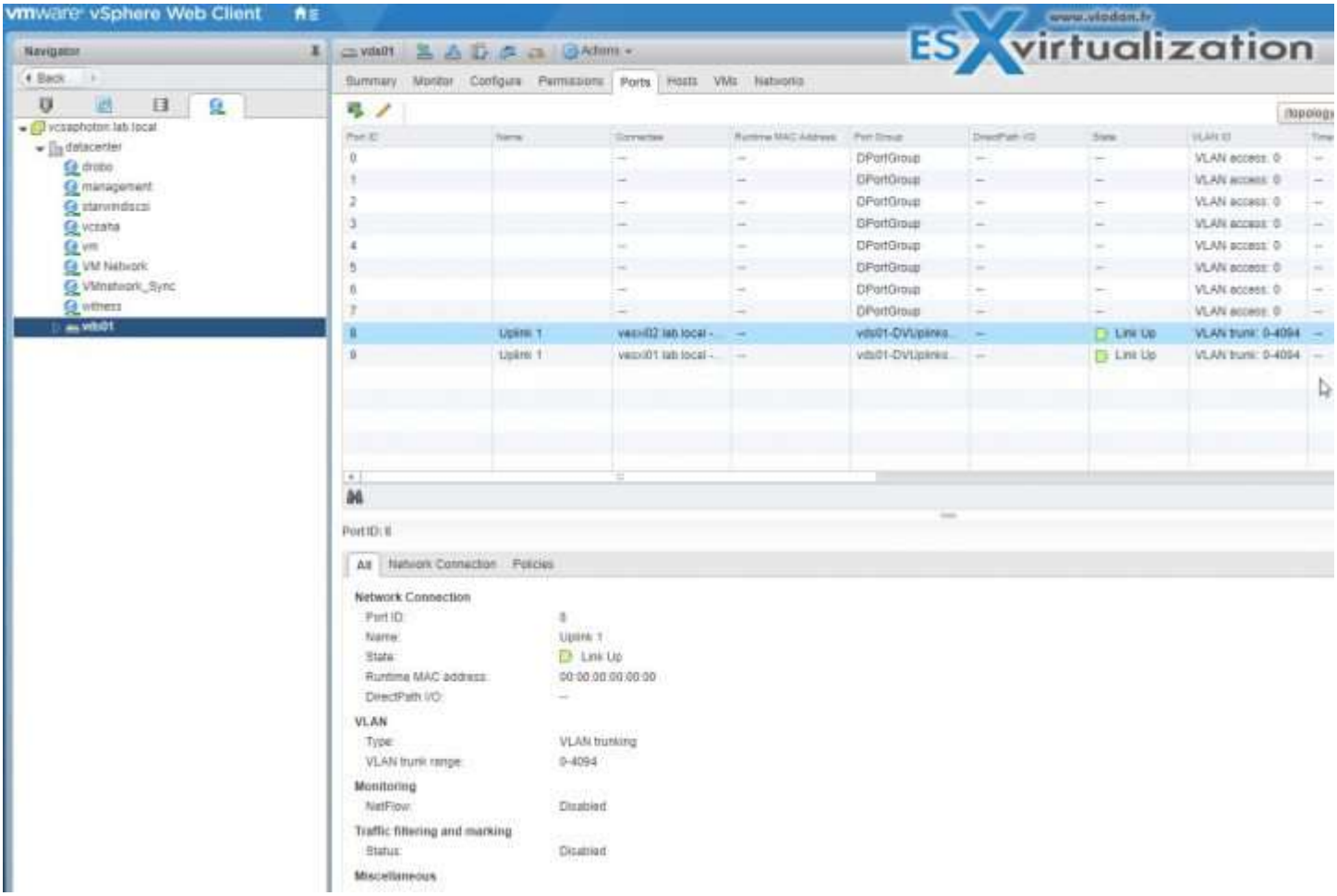
CONFIGURE DVPORT GROUP BLOCKING POLICIES

Port blocking can be enabled on a port group to block all ports on the port group



or you can configure the vDS or uplink to be blocked at the vDS level…

vSphere **Web Client** > **Networking** > **vDS** > **Manage** > **Ports**

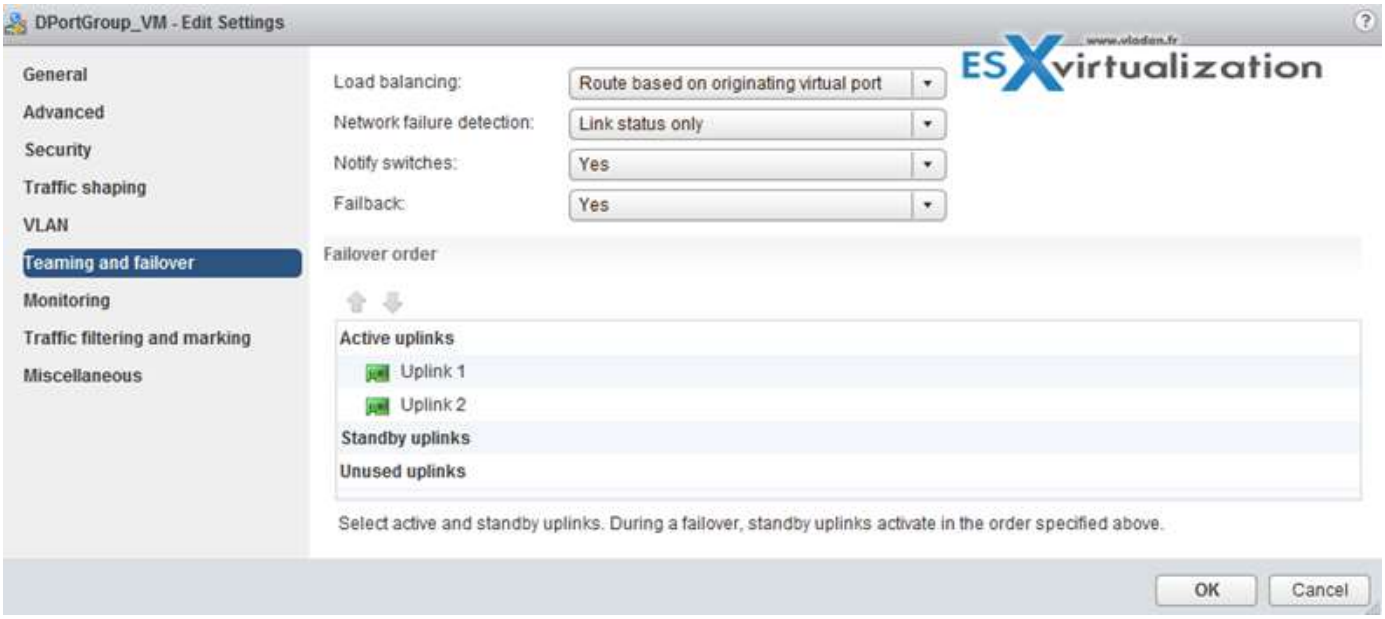


And then **select** the port > **edit** settings > **Miscellaneous** > **Override** check box > set **Block port** to **yes**.

CONFIGURE LOAD BALANCING AND FAILOVER POLICIES

vDS load balancing (LNB):

- **Route based on IP hash** – The virtual switch selects uplinks for virtual machines based on the source and destination IP address of each packet.
- **Route based on source MAC hash** – The virtual switch selects an uplink for a virtual machine based on the virtual machine MAC address. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine MAC address and the number of uplinks in the NIC team.
- **Route based on originating virtual port** – Each virtual machine running on an ESXi host has an associated virtual port ID on the virtual switch. To calculate an uplink for a virtual machine, the virtual switch uses the virtual machine port ID and the number of uplinks in the NIC team. After the virtual switch selects an uplink for a virtual machine, it always forwards traffic through the same uplink for this virtual machine as long as the machine runs on the same port. The virtual switch calculates uplinks for virtual machines only once, unless uplinks are added or removed from the NIC team.
- **Use explicit failover order** – No actual load balancing is available with this policy. The virtual switch always uses the uplink that stands first in the list of Active adapters from the failover order and that passes failover detection criteria. If no uplinks in the Active list are available, the virtual switch uses the uplinks from the Standby list.
- **Route based on physical NIC load (Only available on vDS)** – based on Route Based on Originating Virtual Port, where the virtual switch checks the actual load of the uplinks and takes steps to reduce it on overloaded uplinks. Available only for vSphere Distributed Switch. The distributed switch calculates uplinks for virtual machines by taking their port ID and the number of uplinks in the NIC team. The distributed switch tests the uplinks every 30 seconds, and if their load exceeds 75 percent of usage, the port ID of the virtual machine with the highest I/O is moved to a different uplink.



Virtual switch failover order:

- Active uplinks
- Standby uplinks
- Unused uplinks

CONFIGURE VLAN/PVLAN SETTINGS FOR VMS GIVEN COMMUNICATION REQUIREMENTS

Private VLANs allows further segmentation and creation of private groups inside each of the VLAN. By using private VLANs (PVLANs) you splitting the broadcast domain into multiple isolated broadcast "subdomains".

Private VLANs needs to be configured at the physical switch level (the switch must support PVLANs) and also on the VMware vSphere distributed switch. (Enterprise Plus is required). It's more expensive and takes a bit more work to set up.

THERE ARE DIFFERENT TYPES OF PVLANS:

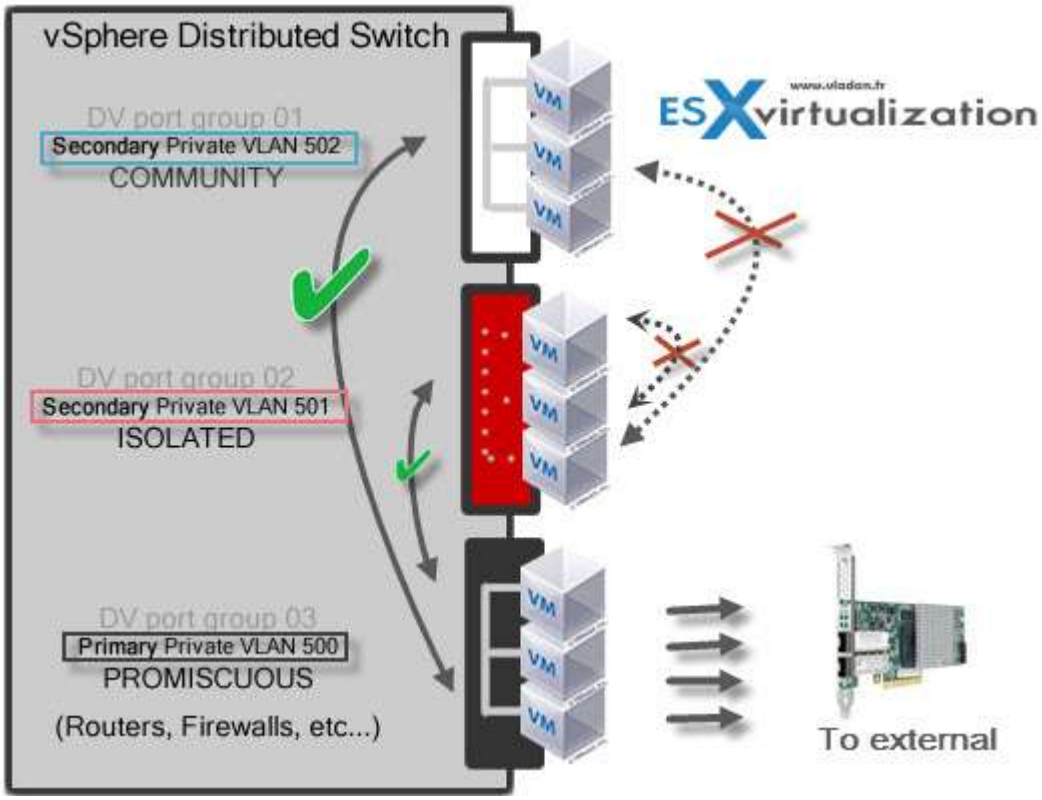
PRIMARY

- **Promiscuous Primary VLAN –** Imagine this VLAN as a kind of a router. All packets from the secondary VLANS go through this VLAN. Packets which also goes downstream and so this type of VLAN is used to forward packets downstream to all Secondary VLANs.

SECONDARY

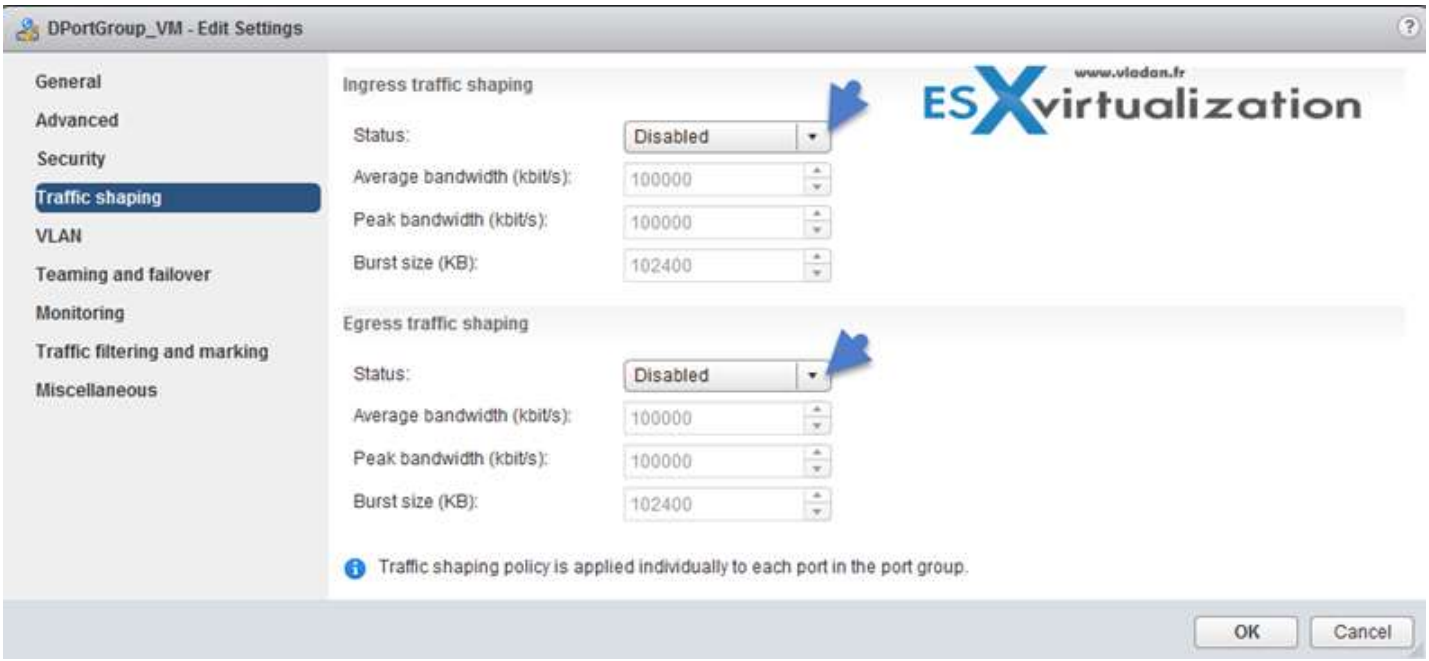
- **Isolated (Secondary)** – VMs can communicate with other devices on the Promiscuous VLAN but not with other VMs on the Isolated VLAN.
- **Community (Secondary)** – VMs can communicate with other VMs on Promiscuous and also with those on the same community VLAN.

The graphics show it all…



CONFIGURE TRAFFIC SHAPING POLICIES

vDS supports both ingress and egress traffic shaping.



Traffic shaping policy is applied to each port in the port group. You can Enable or Disable the Ingress or egress traffic

- **Average bandwidth in kbits (Kb) per second** – Establishes the number of bits per second to allow across a port, averaged over time. This number is the allowed average load.

- **Peak bandwidth in kbits (Kb) per second** – Maximum number of bits per second to allow across a port when it is sending or receiving a burst of traffic. This number limits the bandwidth that a port uses when it is using its burst bonus.
- **Burst size in kbytes (KB) per second** – Maximum number of bytes to allow in a burst. If set, a port might gain a burst bonus if it does not use all its allocated bandwidth. When the port needs more bandwidth than specified by the average bandwidth, it might be allowed to temporarily transmit data at a higher speed if a burst bonus is available

Enable TCP Segmentation Offload support for a virtual machine

Use TCP Segmentation Offload (TSO) in VMkernel network adapters and virtual machines to improve the network performance in workloads that have severe latency requirements.

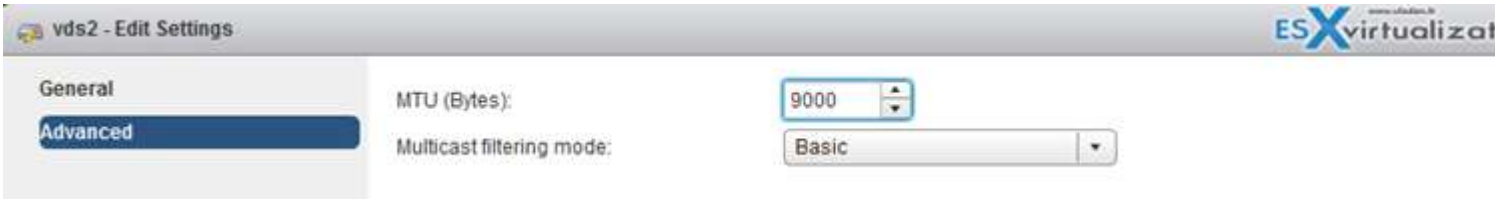
When TSO is enabled, the network adapter divides larger data chunks into TCP segments instead of the CPU. The VMkernel and the guest operating system can use more CPU cycles to run applications.

By default, TSO is enabled in the VMkernel of the ESXi host, and in the VMXNET 2 and VMXNET 3 virtual machine adapters

Enable Jumbo Frames support on appropriate components

There are many places where you can enable Jumbo frames and you should enable jumbo frames end-to-end. If not the performance will not increase, but rather the opposite. Jumbo Frames can be enabled on a vSwitch, vDS, and VMkernel Adapter.

Jumbo frames maximum value = 9000.



Recognize behavior of vDS Auto-Rollback

By rolling configuration changes back, vSphere protects hosts from losing connection to vCenter Server as a result of misconfiguration of the management network.

VMware recognizes Host networking rollback and vDS rollback.

Host networking rollback - Host networking rollbacks can happen when an invalid change is made to the networking configuration for the connection with vCenter Server. Every network change that disconnects a host **also triggers a rollback**. The following examples of changes to the host networking configuration might trigger a rollback:

- Updating the speed or duplex of a physical NIC.
- Updating DNS and routing settings
- Updating teaming and failover policies or traffic shaping policies of a standard port group that contains the management VMkernel network adapter.

- Updating the VLAN of a standard port group that contains the management VMkernel network adapter.
- Increasing the MTU of management VMkernel network adapter and its switch to values not supported by the physical infrastructure.
- Changing the IP settings of management VMkernel network adapters.
- Removing the management VMkernel network adapter from a standard or distributed switch.
- Removing a physical NIC of a standard or distributed switch containing the management VMkernel network adapter.
- Migrating the management VMkernel adapter from vSphere standard to distributed switch.

vSphere Distributed Switch (vDS) Rollback - vDS rollbacks happens when invalid updates are made to distributed switches, distributed port groups, or distributed ports. The following changes to the distributed switch configuration trigger a rollback:

- Changing the MTU of a distributed switch.
- Changing the following settings in the distributed port group of the management VMkernel network adapter:
    - Teaming and failover
    - VLAN
    - Traffic shaping
- Blocking all ports in the distributed port group containing the management VMkernel network adapter.
- Overriding the policies on at the level of the distributed port for the management VMkernel network adapter.

Configure vDS across multiple vCenters to support [Long Distance vMotion]

Starting vSphere 6.0 you have a possibility to migrate VMs between vCenter Server instances. You'll want to do that in some cases, like:

- Balance workloads across clusters and vCenter Server instances.
- Expand or shrink capacity across resources in different vCenter Server instances in the same site or in another geographical area.
- Move virtual machines to meet different Service Level Agreements (SLAs) regarding storage space, performance, and so on.

Requirements:

- The source and destination vCenter Server instances and ESXi hosts must be 6.0 or later.
- The cross vCenter Server and long-distance vMotion features require an Enterprise Plus license.
- Both vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification.
- For migration of computing resources only, both vCenter Server instances must be connected to the shared virtual machine storage.
- When using the vSphere Web Client, **both vCenter Server instances must be in Enhanced Linked Mode** and must be in the **same vCenter Single Sign-On domain**. This lets the source vCenter Server to authenticate to the destination vCenter Server.
- If the vCenter Server instances exist in separate vCenter Single Sign-On domains, you can use vSphere APIs/SDK to migrate virtual machines.

The migration process performs checks to verify that the source and destination networks are similar.

vCenter Server performs network compatibility checks to prevent the following configuration problems:

- MAC address compatibility on the destination host
- vMotion from a distributed switch to a standard switch
- vMotion between distributed switches of different versions
- vMotion to an internal network, for example, a network without a physical NIC
- vMotion to a distributed switch that is not working properly
- vCenter Server does not perform checks for and notifies you of the following problems:

If the source and destination distributed switches are not in the same broadcast domain, virtual machines lose network connectivity after migration.

COMPARE AND CONTRAST VSPHERE DISTRIBUTED SWITCH (VDS) CAPABILITIES

When you configure vDS on a vCenter server, the settings are pushed to all ESXi hosts which are connected to the switch.

vSphere Distributed Switch separates data plane and the management plane. The data plane implements the package switching, filtering, tagging, etc. The management plane is the control structure that you use to configure the data plane functionality.

The management functionality of the distributed switch resides on the vCenter Server system that lets you administer the networking configuration of your environment on a data center level. The data plane remains locally on every host that is associated with the distributed switch. The data plane section of the distributed switch is called a host proxy switch. The networking configuration that you create on vCenter Server (the management plane) is automatically pushed down to all host proxy switches (the data plane).

The vSphere Distributed Switch introduces two abstractions that you use to create consistent networking configuration for physical NICs, virtual machines, and VMkernel services.

Uplink port group - An uplink port group or dvuplink port group is defined during the creation of the distributed switch and can have one or more uplinks. An uplink is a template that you use to configure physical connections of hosts as well as failover and load balancing policies. You map physical NICs of hosts to uplinks on the distributed switch. At the host level, each physical NIC is connected to an uplink port with a particular ID. You set failover and load balancing policies over uplinks and the policies are automatically propagated to the host proxy switches, or the data plane. In this way, you can apply consistent failover and load balancing configuration for the physical NICs of all hosts that are associated with the distributed switch.

Distributed port group - Distributed port groups provide network connectivity to virtual machines and accommodate VMkernel traffic. You identify each distributed port group by using a network label, which must be unique to the current data center. You configure NIC teaming, failover, load balancing, VLAN, security, traffic shaping, and other policies on distributed port groups. The virtual ports that are connected to a distributed port group share the same properties that are configured to the distributed port group. As with uplink port groups, the configuration that you set on distributed port groups on vCenter Server (the management plane) is automatically propagated to all hosts on the distributed switch through their host proxy switches (the data plane). In this way, you can configure a group of virtual machines to share the same networking configuration by associating the virtual machines to the same distributed port group.

Configure multiple VMkernel Default Gateways

In order to override the default gateway for a VMkernel adapter to provide a different gateway for services such as vMotion and Fault Tolerance logging, you'll need to assign another gateway. Each TCP/IP stack on a host can have only one default gateway. This default gateway is part of the routing table and all services that operate on the TCP/IP stack use it.

For example, the VMkernel adapters vmk0 and vmk1 can be configured on a host.

vmk0 is used for management traffic on the 10.162.10.0/24 subnet, with default gateway 10.162.10.1

vmk1 is used for vMotion traffic on the 172.16.1.0/24 subnet

If you set 172.16.1.1 as the default gateway for vmk1, vMotion uses vmk1 as its egress interface with the gateway 172.16.1.1. The 172.16.1.1 gateway is a part of the vmk1 configuration and is not in the routing table. Only the services that specify vmk1 as an egress interface use this gateway. This provides additional Layer 3 connectivity options for services that need multiple gateways.

You can use the vSphere Web Client or an ESXCLI command to configure the default gateway of a VMkernel adapter

Configure ERSPAN

Port Mirroring. ERSPAN and RSPAN allow vDS to mirror traffic across the datacenter to perform remote traffic collection for central monitoring. IPFIX or NetFlow version v10 is the advanced and flexible protocol that allows defining the NetFlow records that can be collected at the VDS and sent across to a collector tool.

Available since vSphere 5.1, allows creating a port mirroring session by using vSphere web client to mirror vDS traffic to ports, uplinks, and remote IP addresses.

Requirements:

- vDS 5.0 and later.

Then

- Select Port Mirroring Session Type, to begin a port mirroring session, you must specify the type of port mirroring session.
- Specify Port Mirroring Name and Session Details, to continue creating a port mirroring session, specify the name, description, and session details for the new port mirroring session.
- Select Port Mirroring Sources, to continue creating a port mirroring session, select sources and traffic direction for the new port mirroring session.
- Select Port Mirroring Destinations and Verify Settings, to complete the creation of a port mirroring session, select ports or uplinks as destinations for the port mirroring session.

Create and configure custom TCP/IP Stacks

You can create a custom TCP/IP stack on a host to forward networking traffic through a custom application.

- Open an SSH connection to the host.
- Log in as the root user.
- Run the vSphere CLI command.
- esxcli network ip netstack add -N="stack_name"

The custom TCP/IP stack is created on the host. You can assign VMkernel adapters to the stack.

Configure Netflow

You can analyzeVMs IP traffic that flows through a vDS by sending reports to a NetFlow collector. It is vDS 5.1 and later which supports IPFIX - Netflow version 10.

vSphere Web client > vDS > Actions > Settings > Edit Netflow Settings

There you can set collector port, Observation Domain ID that identifies the information related to the switch, and also some advanced settings such as Active (or idle) flow export timeout, sampling rate or to process internal flows only.

Tip: Check our How-to, tutorials, videos on a dedicated vSphere 6.5 Page.

VCP6.5-DCV Objective 2.2 – Configure Network I/O control (NIOC)

Explain NIOC capabilities

Version 3 of the Network I/O Control (NIOC) feature offers improved network resource reservation and allocation across the entire switch. vSphere NIOC v3 introduces a mechanism to reserve bandwidth for system traffic based on the capacity of the physical adapters on a host. It enables fine-grained resource control at the VM network adapter level similar to the model that you use for allocating CPU and memory resources.

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

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

The two traffic categories have different nature. System traffic is strictly associated with an ESXi host. The network traffic routes change when you migrate a virtual machine across the environment. To provide network resources to a virtual machine regardless of its host, in Network I/O Control you can configure resource allocation for virtual machines that is valid in the scope of the entire distributed switch.

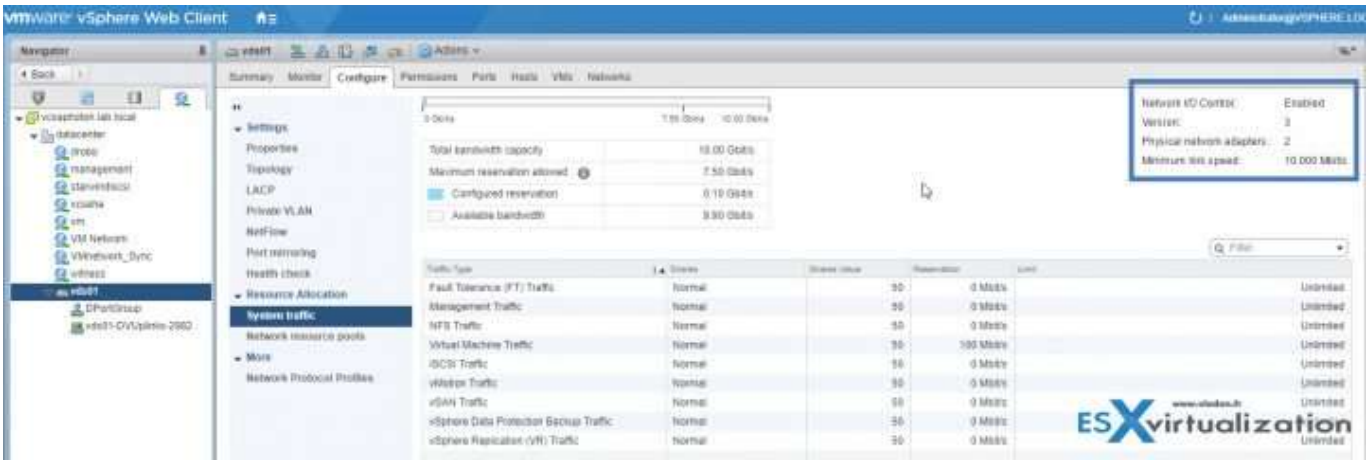
Bandwidth Guarantee to Virtual Machines - Network I/O Control version 3 provisions bandwidth to the network adapters of virtual machines by using constructs of shares, reservation and limit. Based on these constructs, to receive sufficient bandwidth, virtualized workloads can rely on admission control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

Configure NIOC shares/limits based on VM requirements

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

Requirements:

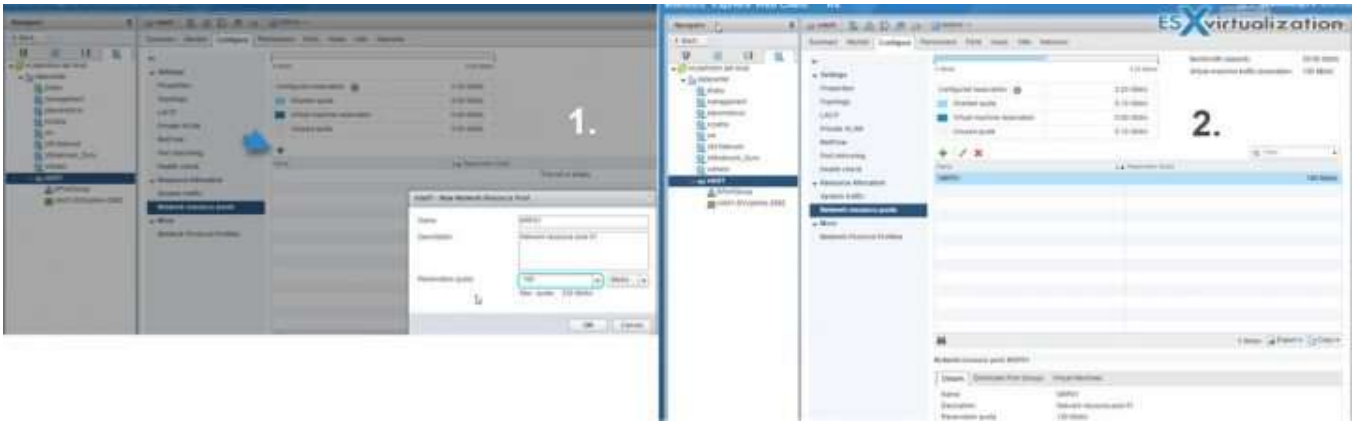
- Verify that vSphere Distributed Switch is version 6.0.0 and later.
- Verify that Network I/O Control on the switch is version 3.
- Verify that Network I/O Control is enabled.



- Verify that the virtual machine system traffic has a configured bandwidth reservation.

vSphere Web Client > vDS > Configure TAB > Expand Resource Allocation > Click Network resource pools > Click the Add icon > Type a **name and a description** for the network resource pool.

Enter a value for Reservation quota, in Mbps, from the free bandwidth that is reserved for the virtual machine system traffic.



The maximum quota that you can assign to the pool is determined according to the following formula:

max reservation quota = aggregated reservation for vm system traffic – quotas of the other resource pools

where: aggregated reservation for vm system traffic = configured bandwidth reservation for the virtual machine system traffic on each pNIC * number of pNICs connected to the distributed switch quotas of the other pools = the sum of the reservation quotas of the other network resource pools

Explain the behavior of a given NIOC setting

By using several configuration parameters Network I/O Control allocates bandwidth to traffic from basic vSphere system features.

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

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

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

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

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

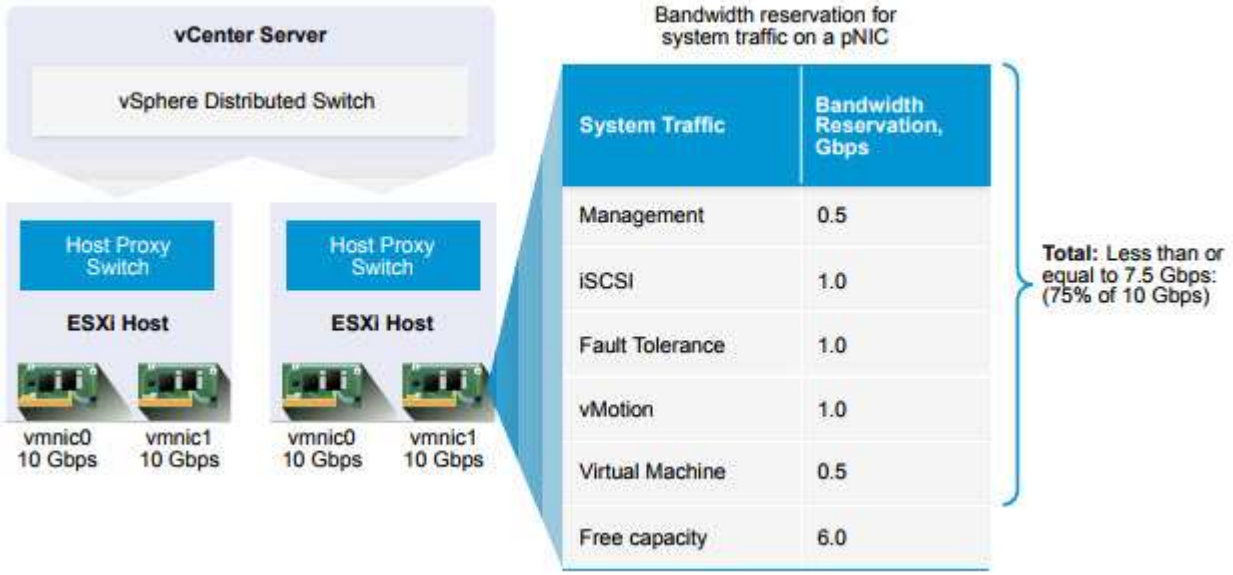
Determine Network I/O Control requirements

Example Bandwidth Reservation for System Traffic.

The capacity of the physical adapters determines the bandwidth that you guarantee. According to this capacity, you can guarantee a minimum bandwidth to a system feature for its optimal operation. For example, on a distributed switch that is connected to ESXi hosts with 10 GbE network adapters, you might configure reservation to guarantee 1 Gbps for management through vCenter Server, 1 Gbps for iSCSI storage, 1 Gbps for vSphere Fault Tolerance, 1 Gbps for vSphere vMotion traffic, and 0.5 Gbps for virtual machine traffic. Network I/O Control allocates the requested bandwidth on each physical network adapter. You can reserve no more than 75 percent of the bandwidth of a physical network adapter, that is, no more than 7.5 Gbps.

You might leave more capacity unreserved to let the host allocate bandwidth dynamically according to shares, limits, and use, and to reserve only bandwidth that is enough for the operation of a system feature.

Figure 11-1. Example Bandwidth Reservation for System Traffic on a 10 GbE Physical Network Adapter

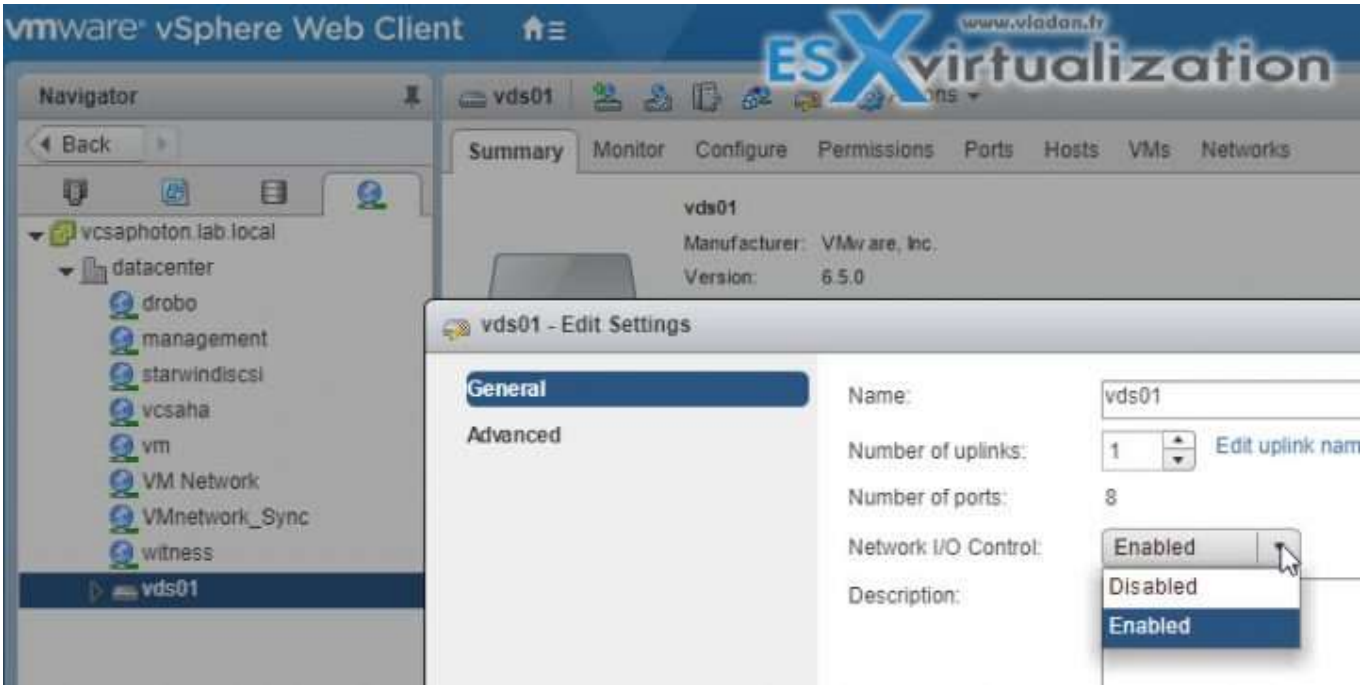


DIFFERENTIATE NETWORK I/O CONTROL CAPABILITIES

Check above.

ENABLE/DISABLE NETWORK I/O CONTROL

vSphere **Web** Client > **Networking** > **vDS** right click > **Edit Settings**> **NIOC (disable/enable drop-down)**



MONITOR NETWORK I/O CONTROL

Tip: Check our How-to, tutorials, videos on a dedicated vSphere 6.5 Page.

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

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

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

In order to monitor the NIOC setting, manage resource allocation under system traffic.

VCP6.5-DCV Objective 3.1 – Manage vSphere Integration with Physical Storage

Perform NFS v3 and v4.1 configurations

NFS – Network file system, can be mounted by ESXi host (which uses NFS client). NFS datastores supports vMotion or SvMotion, HA, DRS, FT or host profiles.

- At first, you must go over to the NFS server where you'll need to set up an NFS volume and export it, so it can then be mounted on the ESXi hosts.
- You'll need: IP or the DNS (FQDN) of the NFS server, and also the **full path**, or **folder name**, for the NFS share.
- Each ESXi has to have configured VMkernel network port for NFS traffic
- For NFS 4.1, you can collect multiple IP addresses or DNS names to use the multipathing support that the NFS 4.1 datastore provides.
- In case you'll want to secure the communication between the NFS server and ESXi hosts, you might want to use Kerberos authentication with the NFS 4.1 datastore. You'll have to configure the ESXi hosts for Kerberos authentication.

Discover new storage LUNs

When doing changes to SAN config, you might need to rescan your storage to see the changes.

You can disable the automatic rescan feature by turning off the Host Rescan Filter. But by default, when you perform VMFS datastore management operations, such as creating a VMFS datastore or RDM, adding an extent, and increasing or deleting a VMFS datastore, your host or the vCenter Server automatically rescans and updates your storage.

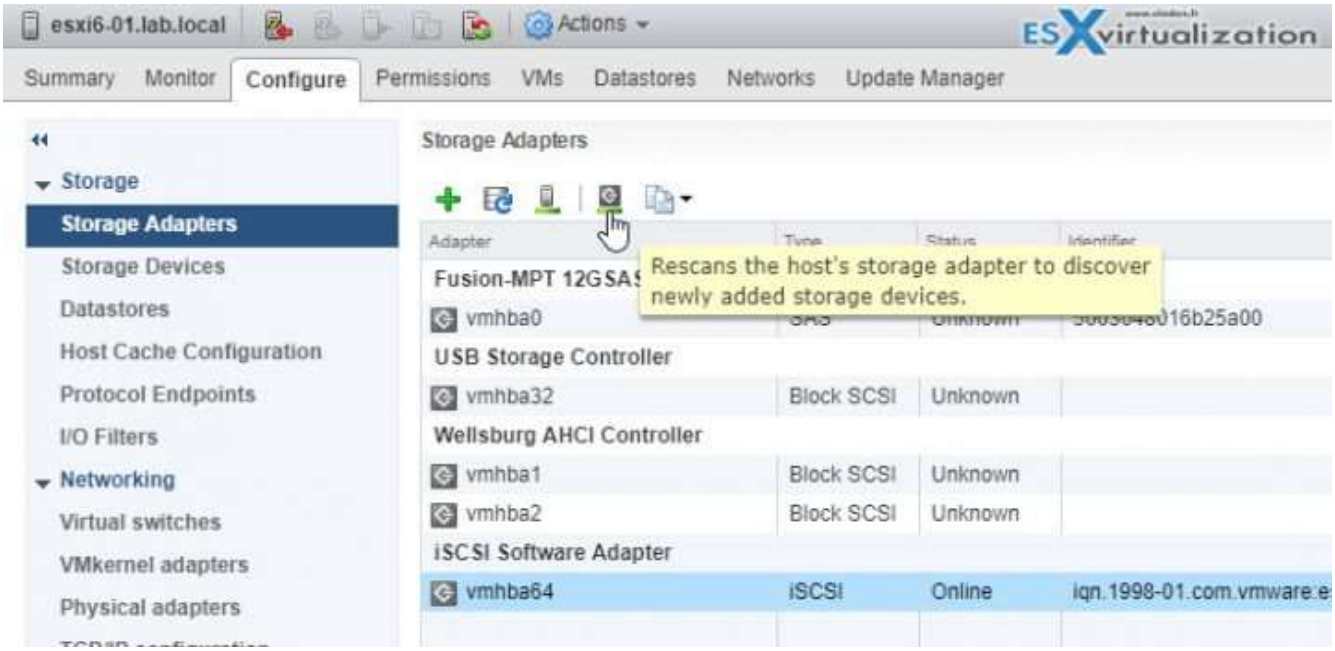
Manual Adapter Rescan - If the changes you make are isolated to storage connected through a specific adapter, perform a rescan for this adapter. In certain cases, you need to perform a manual rescan. You can rescan all storage available to your host or to all hosts in a folder, cluster, and data center.

Perform the manual rescan if you need:

- 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.

WHERE?

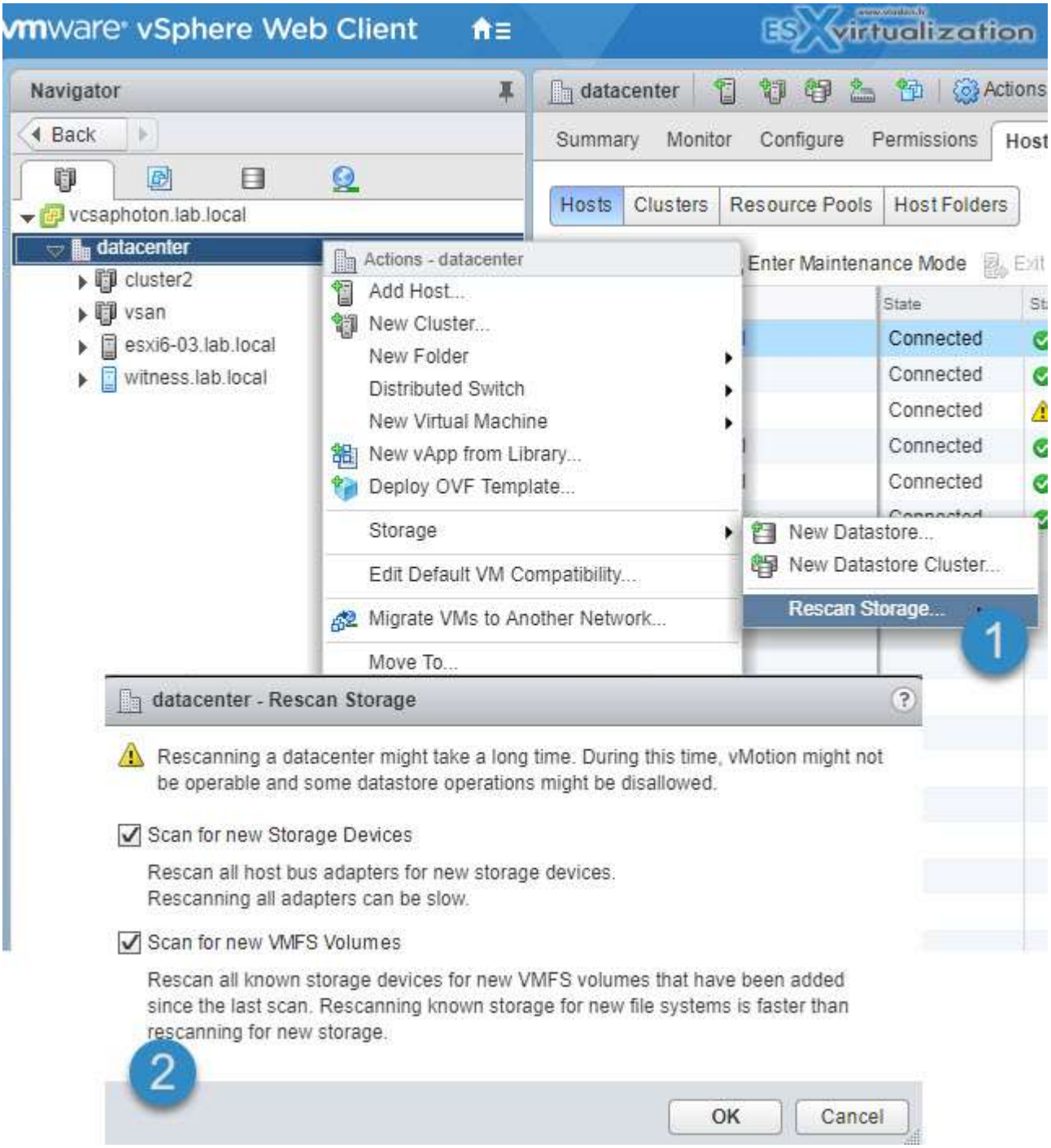
vShpere Web Client > **Host** > **Configure** > **Storage** > **Storage Adapters** > select **adapter** to rescan.



Storage Rescan - When you make changes in your SAN configuration you might need to rescan your storage. You can rescan all storage available to your host, cluster, or data center. If the changes you make are isolated to storage accessed through a specific host, perform the rescan for only this host.

WHERE?

vSphere Web Client > Browse to a **host, a cluster, a data center, or a folder that contains hosts > Right-click > Storage > Rescan Storage**.



CONFIGURE FC/ISCSI/FCOE LUNS AS ESXI BOOT DEVICES

Boot from SAN allows not using local storage of each server as a boot device. The host boots from shared storage LUN (one per host). ESXi support boot from FC HBAs, FCoE converged network adapters.

Benefits - It's easier to replace server because you can "point" the new server to the old boot location.

- Diskless servers are by design taking less space. You can avoid SPOF (single point of failure) because the boot disk is accessible through multiple paths.
- Improved management. Creating and managing the operating system image is easier and more efficient.

- Easier backup processes. You can back up the system boot images in the SAN as part of the overall SAN backup procedures. Also, you can use advanced array features such as snapshots on the boot image.
- Servers can be denser and run cooler without internal storage. (Cheaper).

(check page 50-57 from the vSphere 6.5 storage PDF).

The process basically starts with the storage device where you have to configure SAN LUN, the SAN components, and storage system.

BIOS configuration where you have to configure the Host bios to show the BIOS from the hardware card. After, point the boot adapter to the target boot LUN.

At first, you'll make the first boot from VMware installation media, then only you can configure the boot from SAN. Follow the steps on pages 50-52 of the vSphere 6.5 storage PDF.

MOUNT AN NFS SHARE FOR USE WITH VSPHERE

- The IP address or the DNS name (IP or FQDN) of the NFS server and the full path, or folder name, for the NFS share.
- For NFS 4.1, you can collect multiple IP addresses or DNS names to use the multipathing support that the NFS 4.1 datastore provides.
- On each ESXi host, configure a VMkernel Network port for NFS traffic.
- If you plan to use Kerberos authentication with the NFS 4.1 datastore, configure the ESXi hosts for Kerberos authentication.

Create NFS mount. **Right click datacenter** > **Storage** > **Add Storage**.

You can use NFS 3 or NFS 4.1.

ENABLE/CONFIGURE/DISABLE VCENTER SERVER STORAGE FILTERS

Storage Filtering - vCenter Server provides storage filters to help you avoid storage device corruption or performance degradation that might be caused by an unsupported use of storage devices. These filters are available by default.

Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices. (but **VMware support has to be contacted before**).

WHERE?

vSphere Web Client > Select vCenter Server Object > Configure > Settings > Advanced Settings> Edit > In the value text box enter "**False**" for the specified key.

Config.vpxd.filter.vmfsFilter (VMFS Filter) - Filters out storage devices, or LUNs, that are already used by a VMFS datastore on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with another VMFS datastore or to be used as an RDM.

Config.vpxd.filter.rdmFilter (RDM Filter) - Filters out LUNs that are already referenced by an RDM on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with VMFS or to be used by a different RDM. For your virtual machines to access the same LUN, the virtual machines must share the same RDM mapping files.

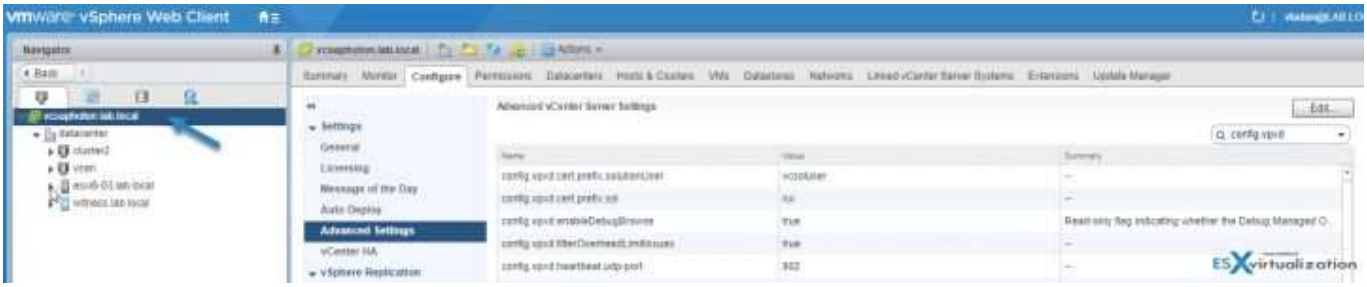
Config.vpxd.filter.SameHostsAndTransportsFilter (Same Hosts and Transports Filter)

Filters out LUNs ineligible for use as VMFS datastore extents because of host or storage type incompatibility. Prevents you from adding the following LUNs as extents:

- LUNs not exposed to all hosts that share the original VMFS datastore.
- LUNs that use a storage type different from the one the original VMFS datastore uses.
- For example, you cannot add a Fibre Channel extent to a VMFS datastore on a local storage device.

Config.vpxd.filter.hostRescanFilter (Host Rescan Filter) - Automatically rescans and updates VMFS datastores after you perform datastore management operations. The filter helps provide a consistent view of all VMFS datastores on all hosts managed by vCenter Server.

You **do not need** to restart the vCenter Server to apply changes. (Check page 172 of the Storage PDF).



CONFIGURE/EDIT HARDWARE/DEPENDENT HARDWARE INITIATORS

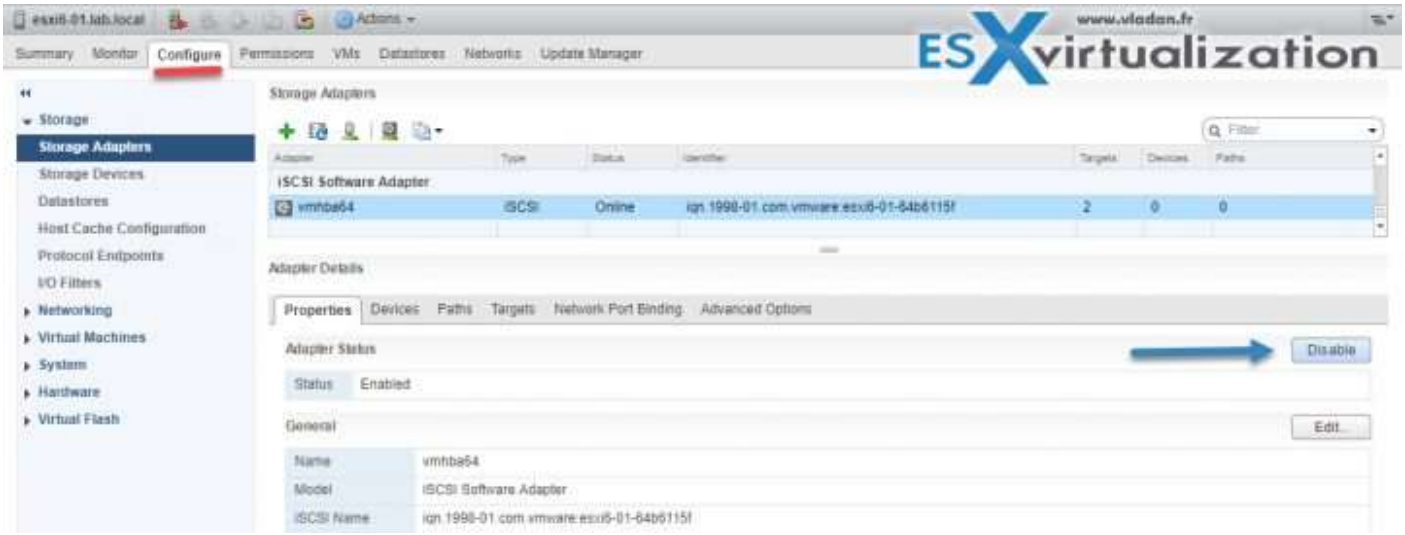
Hardware iSCSI initiators can be used for boot from SAN, for presenting remote storage as local disk, or using it as dedicated iSCSI SAN hardware card providing lower CPU usage and better throughput.

- **Hardware iSCSI** - Host connects to storage through a HBA capable of offloading the iSCSI and network processing. Hardware adapters can be dependent or independent.
- **Software iSCSI** - Host uses a software-based iSCSI initiator in the VMkernel to connect to storage.

The iSCSI adapter (hardware) is enabled by default. But to make it functional, you must first connect it, through a virtual VMkernel adapter (vmk), to a physical network adapter (vmnic) associated with it. You can then configure the iSCSI adapter.

After configuration of the hardware iSCSI adapter, the discovery and authentication data are passed through the network connection, while the iSCSI traffic goes through the iSCSI engine, bypassing the network.

ENABLE/DISABLE SOFTWARE ISCSI INITIATOR



CONFIGURE/EDIT SOFTWARE ISCSI INITIATOR SETTINGS

As on the image above, stay where you are. 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:

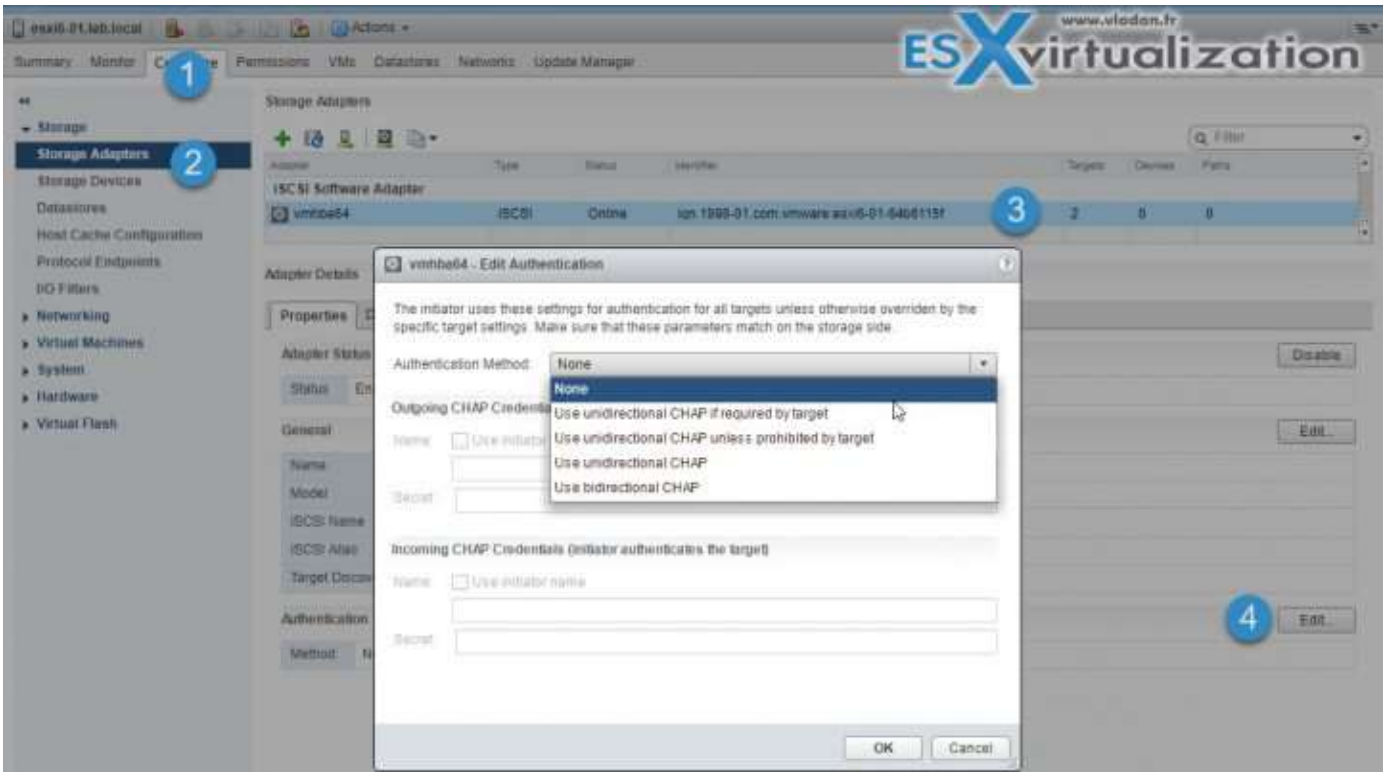
- Array target iSCSI ports are in a different broadcast domain and IP subnet.

- 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 the single **Active uplink**. All the others as **unused** only (not Active/standby). If not they are not listed…

ENABLE/CONFIGURE/DISABLE ISCSI CHAP

Web Client > **Host and Clusters** > **Host** > **Configure** > **Storage** > **Storage Adapters** > **Properties** > **Authentication** section > **Edit**.



Page 95 of the vSphere 6.5 storage PDF guide.

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 cases for Fiber Channel zoning

SAN Zoning - allows you to restrict server access to storage arrays which are not allocated to that server. Usually one create zones for a group of hosts that access a shared group of storage devices and LUNs. Zones basically define which HBAs can connect to which Storage Processors (SPs). Devices living outside a zone are not visible to the devices inside the zone.

Zoning is similar to LUN masking, which is commonly used for permission management. LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

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.

It Allows:

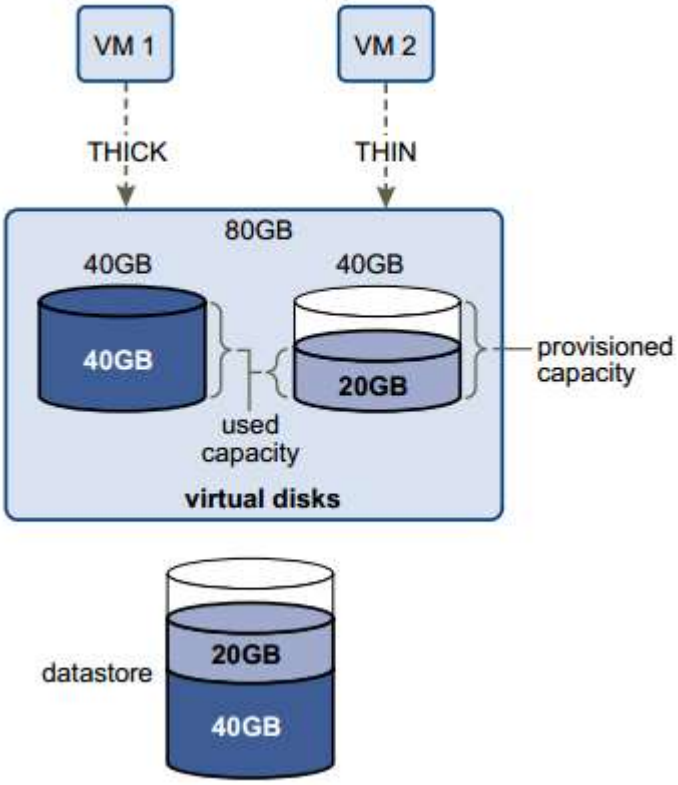
- Protecting from access non desired devices the LUN and possibly corrupt data.
- Can be used for separation different environments (clusters).
- Reduces the number of targets and LUN presented to host.
- Controls and isolates paths in a fabric.

Best practice? Single-initiator-single target.

Compare and contrast array thin provisioning and virtual disk thin provisioning

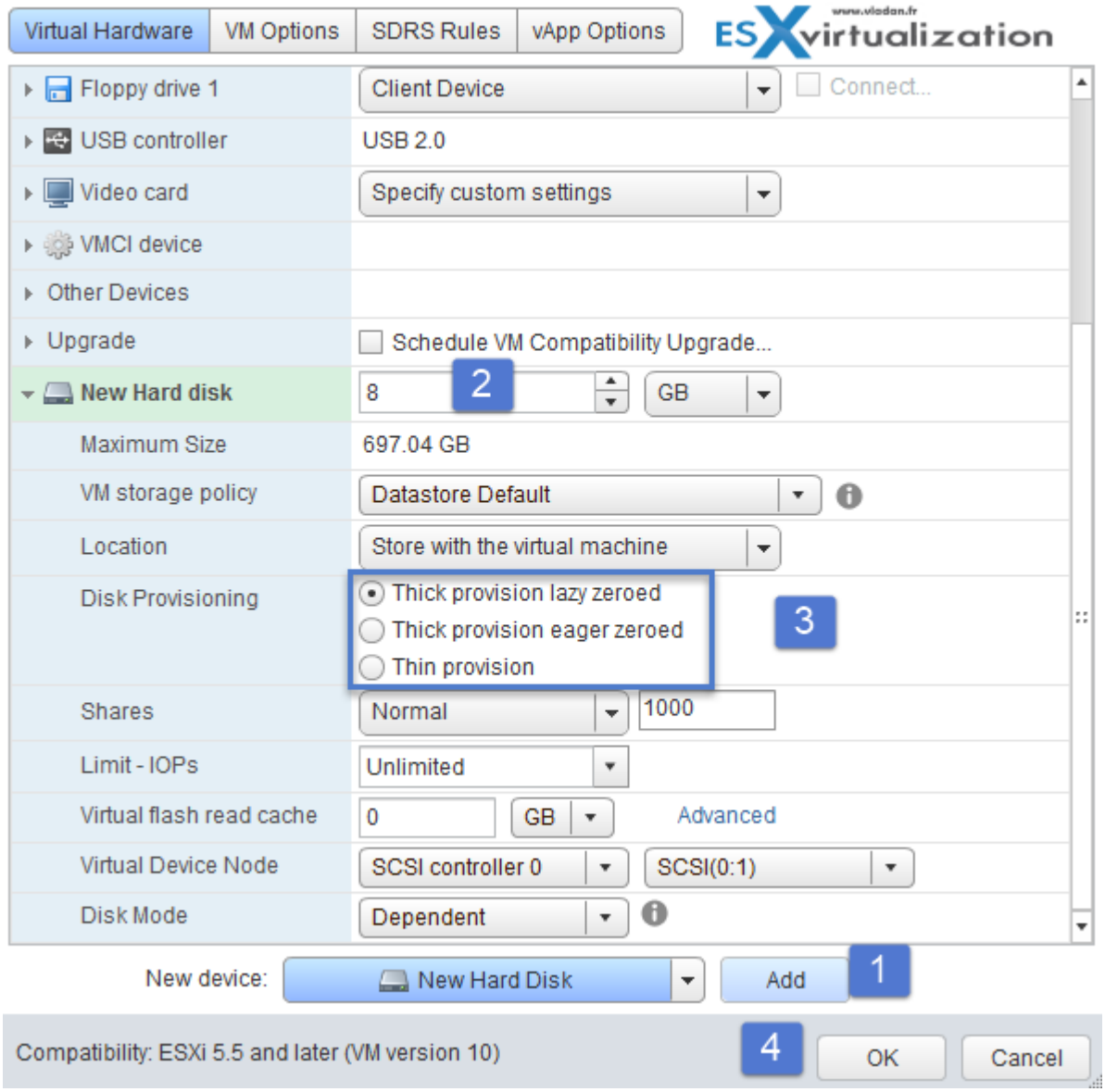
Virtual disk thin provisioning allows to allocate only a small amount of disk space at the storage level, but the guest OS sees as it had the whole space. The thin disk grows in size when adding more data, installing applications at the VM level. So it's possible to over-allocate the datastore space, but it brings a risk so it's **important to monitor** actual storage usage to avoid conditions when you run out of physical storage space.
An image says thousands of words…

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. A thin disk can be **inflated** (thin > thick) via datastore browser (right click vmdk > inflate).

Check the different VMDK disk provisioning options when creating new VM or adding an additional disk to existing VM.



Thin-provisioned LUN

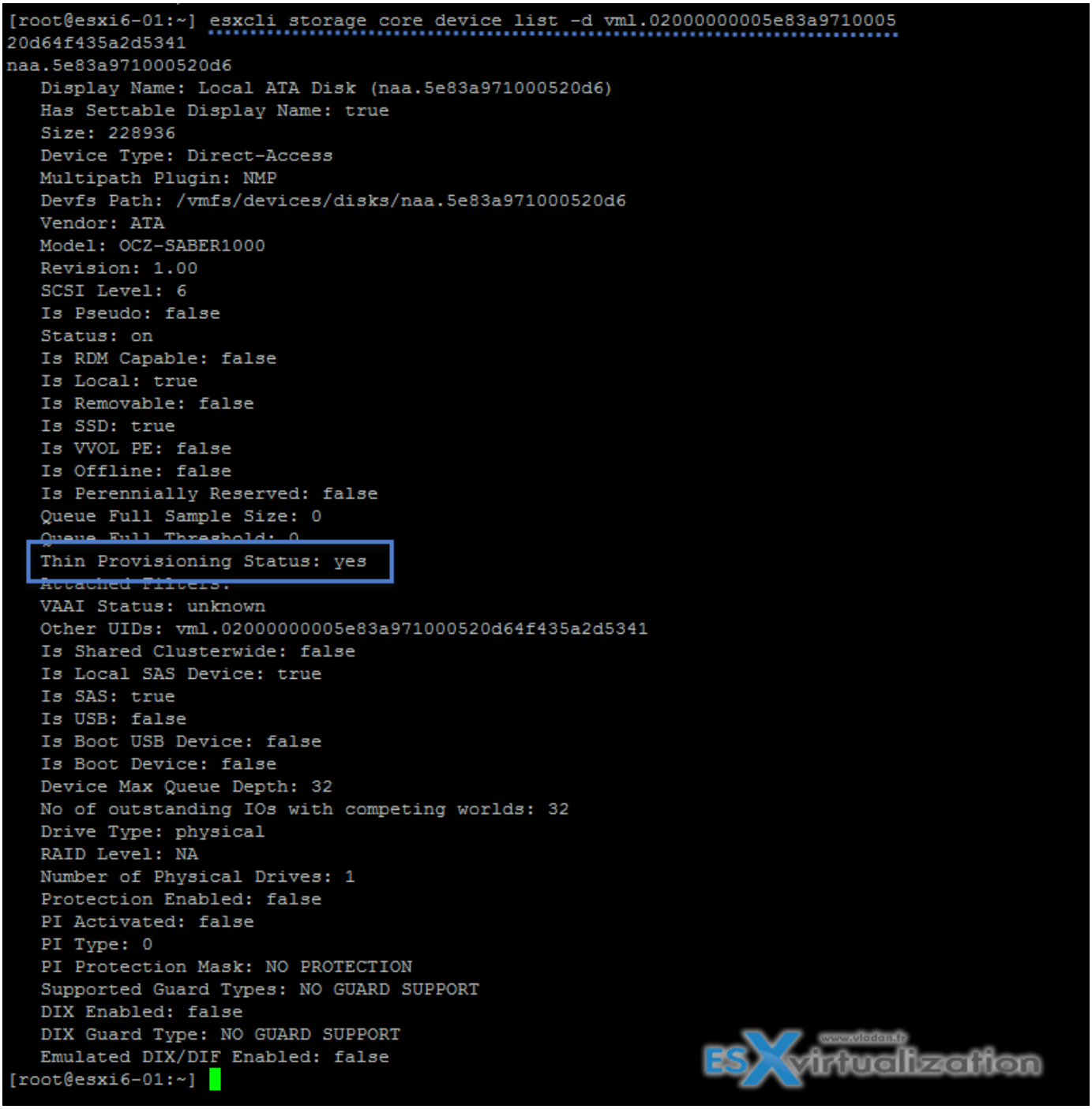
ESXi also supports thin-provisioned LUNs. When a LUN is thin-provisioned, the storage array reports the LUN's logical size, which might be larger than the real physical capacity backing that LUN. A VMFS datastore that you deploy on the thin-provisioned LUN can detect only the logical size of the LUN.

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 thing-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 vml.xxxxxxxxxxxxxxx

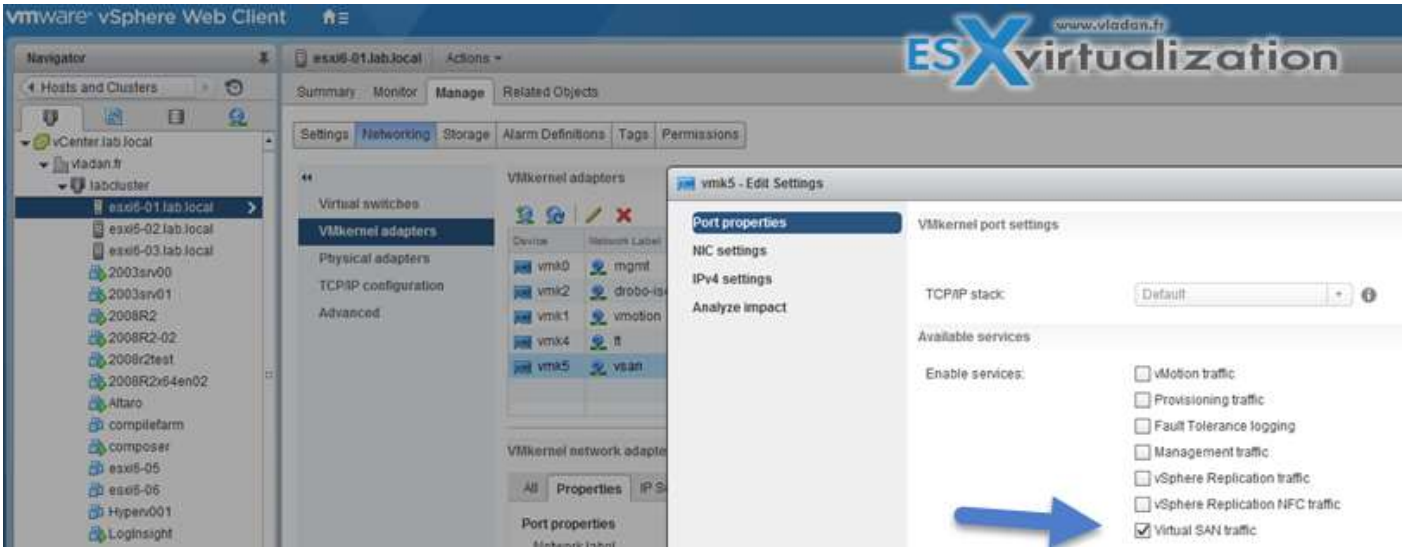


VCP6.5-DCV Objective 3.1 - Manage vSphere Integration with Physical Storage is certainly a very large topic. Make sure that you download the vSphere 6.5 storage PDF (the link which is direct to the PDF might change over time, but do a quick search on Google and you'll find it).

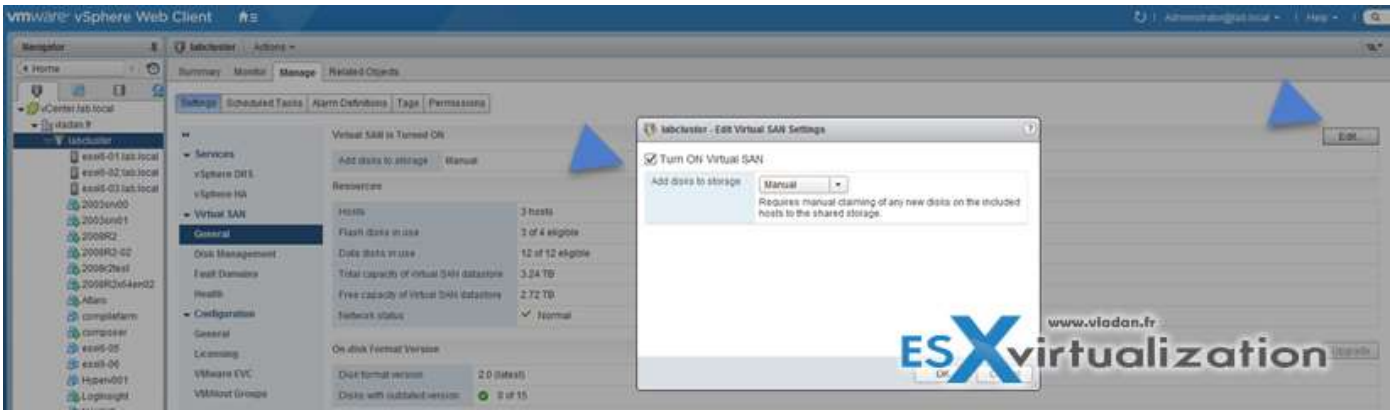
VCP6.5-DCV Objective 3.2 – Configure Software-Defined Storage

Configure Virtual SAN Cluster

Create VMkernel interface with VSAN traffic on **Host** > **Manage** > **Networking** > **VMkernel Adapters** > **Add**



Enable VSAN at the cluster level: **Hosts and Clusters** > **Cluster** > **Manage** > **Settings** > **Virtual SAN** > **General**



Add disk to storage:

- **Manual** – Requires manual claiming of any new disks.
- **Automatic** – All empty disks on cluster hosts will be automatically claimed by VSAN

Claim disks for VSAN

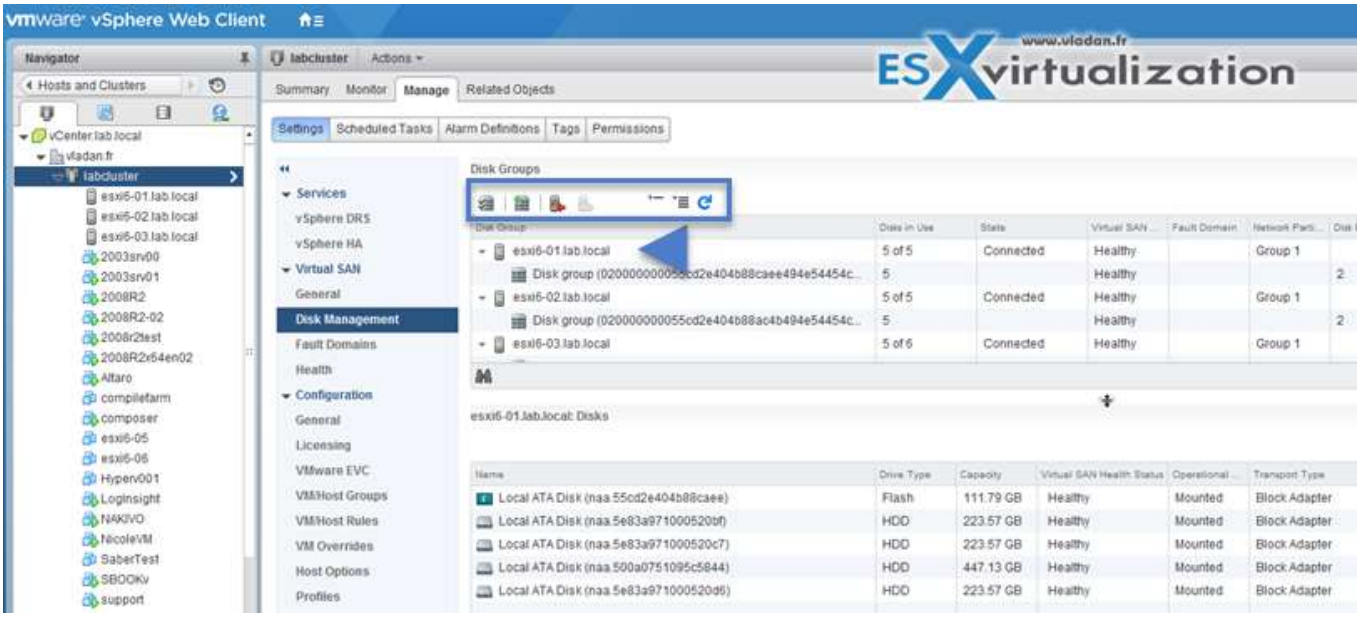
You can do several tasks when managing disk in VSAN cluster.

- Claim Disks for VSAN
- Create a new disk group (when adding more capacity).
- Remove the disk group
- Add a disk to the selected disk group
- Place a host in maintenance mode

Create disk groups

Hosts and Clusters > **Cluster** > **Manage** > **Settings** > **Virtual SAN** > **Disk Management**

Each disk group has to have 1 SSD for caching and at least one disk (or SSD) for capacity.

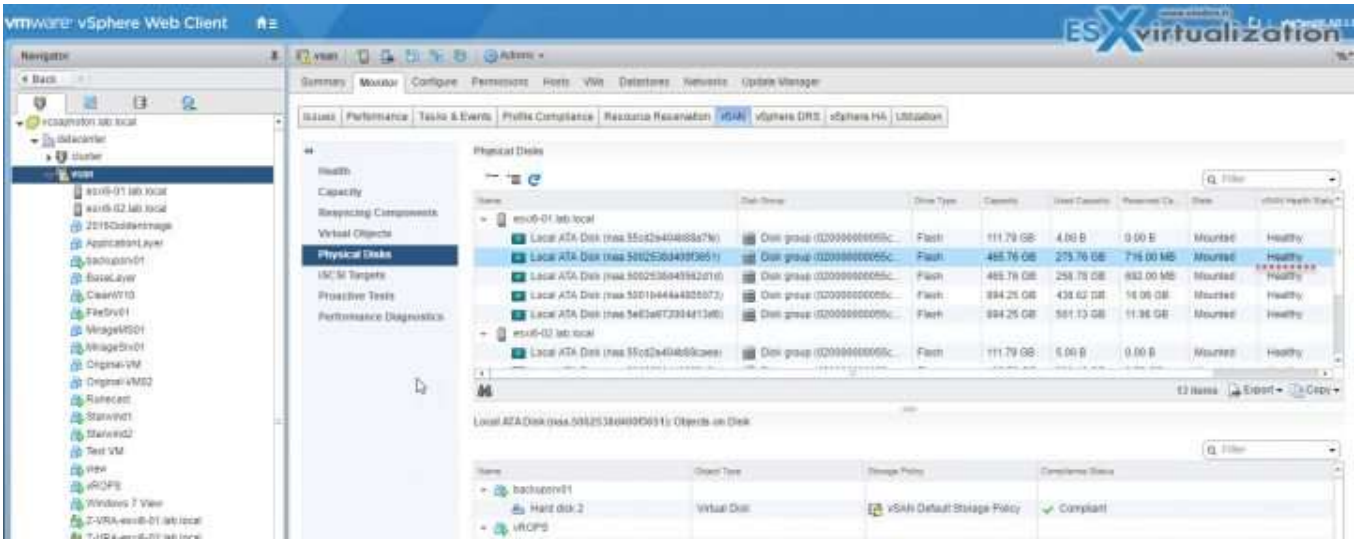


MONITOR VSAN

You can monitor vSAN several ways, including CLI or vSAN observer utility.

Monitor vSAN from vSphere Web client:

- Navigate to the **vSAN cluster** in the vSphere Web Client > **Monitor tab** and click **vSAN** > Select **Physical Disks** to review all hosts, c**ache devices**, and **capacity devices** in the cluster.



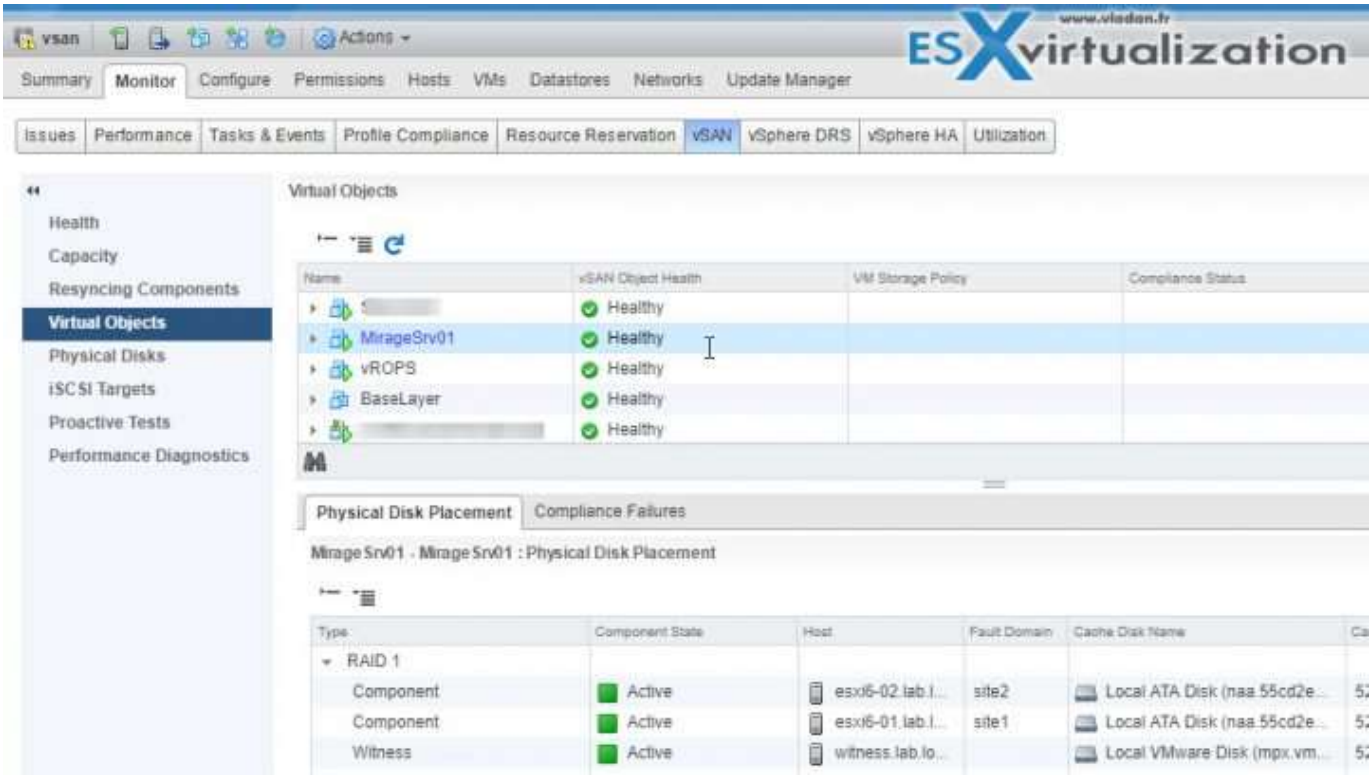
You can select capacity device, to see in the lower pane the storage policy associated with the disk.

If you select Capacity then you have a view showing:

- Capacity provisioned and used within the cluster, free space
- Breakdown of the used capacity by object type or data type.
- See if deduplication or compression is enabled, and if yes, the savings.

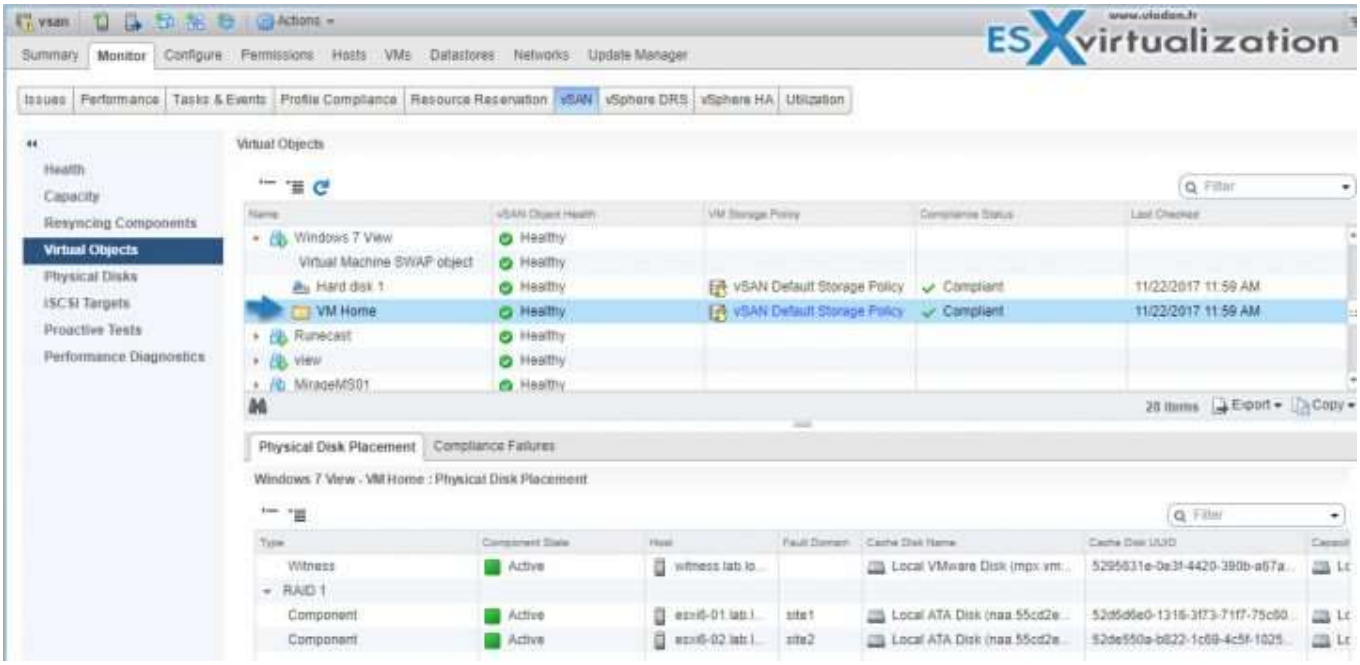
You can also select **virtual objects** to see:

Select vSAN cluster in the vSphere Web Client > **Monitor tab** and click vSAN > **Select Virtual objects** to view all hosts and the corresponding virtual disks in the vSAN cluster, including which hosts, cache and capacity devices their components are currently consuming.



You can see also the Physical Disk Placement to view device information, cache disk name, capacity disk name identifier or UUID, and so on.

The Compliance Failures can show you the compliance status of your VM. If you **select hard disk** on one of the VMs and click the **Physical Disk Placement** tab to view the device information, such as name, identifier or UUID, number of devices used for each virtual machine. You can also see where the components are stored, on which hosts.



The Compliance Failures allows you to check the compliance status of the individual VMDK.

VCP6.5-DCV Objective 3.2 Describe vVOLs

Virtual volumes are object exported by a compliant storage system. vVOLs correspond one-to-one with a VMs disk and other VM - related files. The virtual volume is created and manipulated out-of-band, not in the data path, by a VASA provider.

With Virtual Volumes (VVols), VMware offers a new paradigm in which an individual virtual machine and its disks, rather than a LUN, becomes a unit of storage management for a storage system. Virtual volumes encapsulate virtual disks and other virtual machine files, and natively store the files on the storage system.

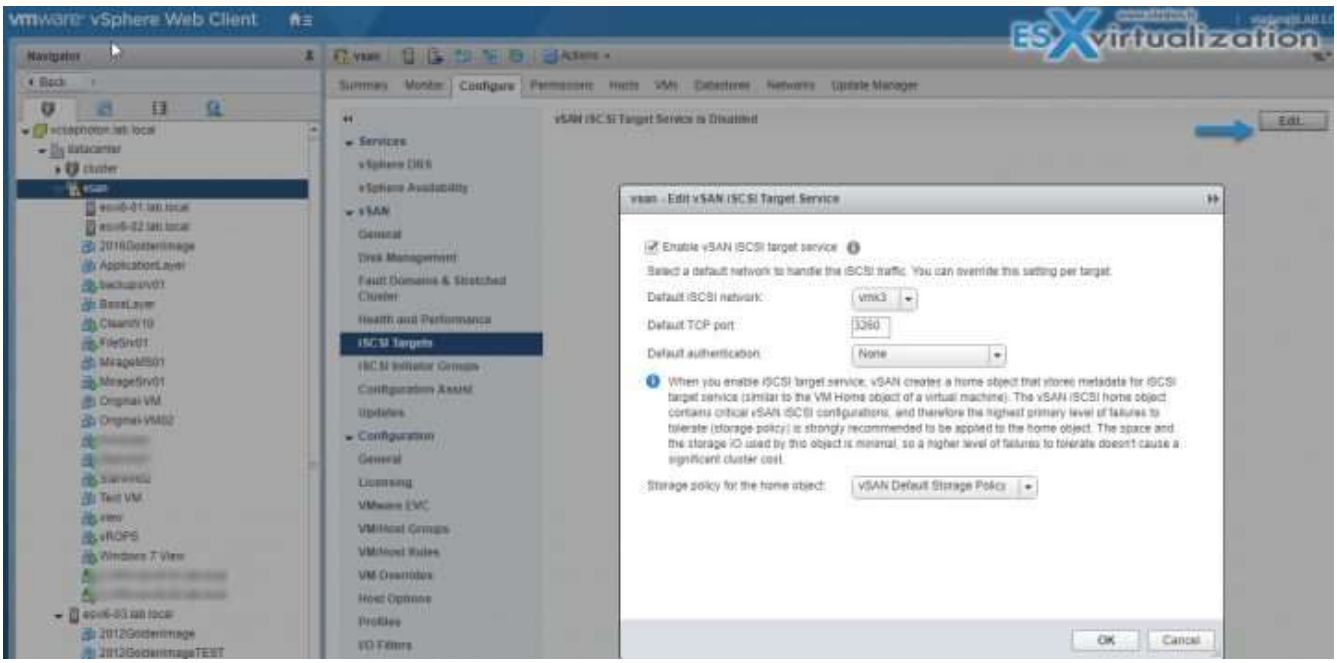
The vVOL functionality is helping for better granularity. Instead of manipulating and arranging storage around features of a storage system, it's vVOLs which arranges storage around the needs of individual VMs. Now it is storage which is VM centric.

vVOLs are mapping virtual disk, snapshots, and replicas, directly to objects, which we call virtual volumes, on a storage system. This mapping allows vSphere to offload intensive storage operations (snapshots, cloning, replication) to the storage system. When creating a volume for each individual virtual disk, it is possible to set policies more granularly, more optimal.

Understand a vSAN iSCSI target

VMware vSAN can export an iSCSI and provide storage services to hosts which are **outside of the vSAN cluster**. iSCSI can also be consumed by dedicated hosts which needs more storage. vSAN provides iSCSI target service.

External hosts can activate an iSCSI initiator which can transport block-level data to the iSCSI target exported by a vSAN cluster. The iSCSI target discovery is similar as used with dedicated storage arrays supporting block-level storage. You can configure multipath support for the iSCSI.



Explain vSAN and vVOL architectural components

VMware vSAN - VMware vSAN creates shared datastore by pooling local disk drives and SSDs from each individual host participating in vSAN cluster. It virtualizes the local physical storage resources of ESXi hosts and turns them into pools of storage that can be divided and assigned to virtual machines and applications according to their quality-of-service requirements. vSAN is implemented directly in the ESXi hypervisor.

vSAN can be activated on existing cluster if storage controller, disks, SSD for caching are part of the HCL. You need at least one HDD and one SSD to create a disk group in each host of the vSAN cluster.

Host from a vSAN cluster can have up to 5 disk groups. Each group has a maximum of 7 capacity disks and 1 SSD for caching.

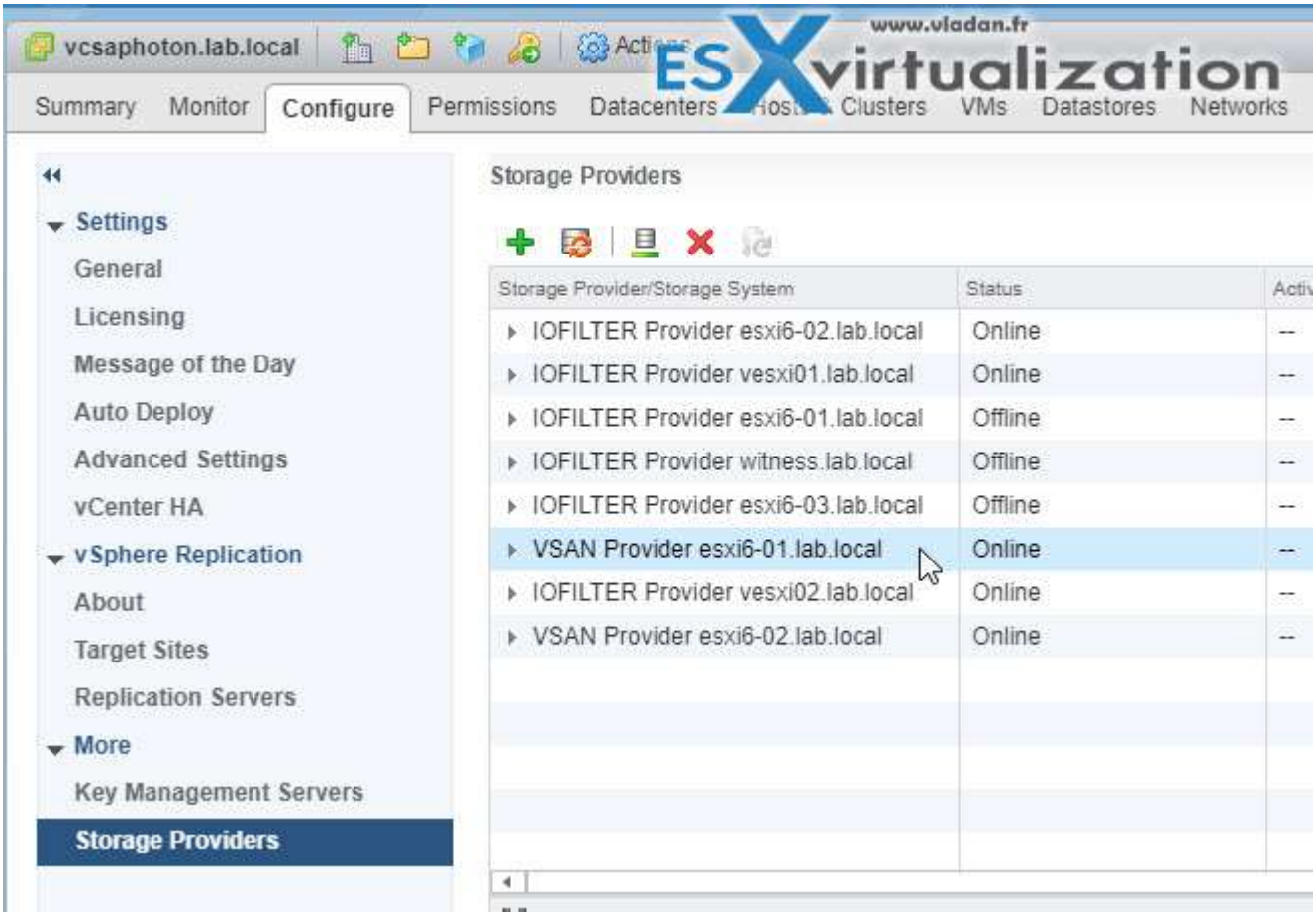
vVOL architecture - The ESXi hosts have no direct access to the virtual volume's storage. Instead, the hosts access the virtual volumes through an intermediate point in the data path, called the protocol endpoint. The protocol endpoints establish a data path on demand from the virtual machines to their respective virtual volumes. The protocol endpoints serve as a gateway for direct in-band I/O between ESXi hosts and the storage system. ESXi can use Fibre Channel, FCoE, iSCSI, and NFS protocols for in-band communication.

The virtual volumes reside inside storage containers that logically represent a pool of physical disks on the storage system. On the vCenter Server and ESXi side, storage containers are presented as Virtual Volumes datastores. A single storage container can export multiple storage capability sets and provide different levels of service to different virtual volumes.

DETERMINE THE ROLE OF STORAGE PROVIDERS IN VSAN

When you enable VMware vSAN in your cluster, it automatically configures and registers a storage provider for each host in the vSAN cluster. The vSAN storage providers report a set of underlying storage capabilities to vCenter Server. They also communicate with the vSAN layer to report the storage requirements of the virtual machines.

You can check whether storage providers are registered. Connect to vSphere client > **Home** > **Select vCenter Server** > Click the **Configure** tab, and click **Storage Providers.**



The storage providers for vSAN should appear on the list. Each host has a storage provider, but only one storage provider is active.

Determine the role of storage providers in vVOLs

vCenter Server and ESXi use the storage providers to obtain information about storage configuration status, and storage data services offered in your environment. This information appears in the vSphere Web Client.

Built-in storage providers typically do not require registration. For example, the storage providers that support I/O filters become registered automatically.

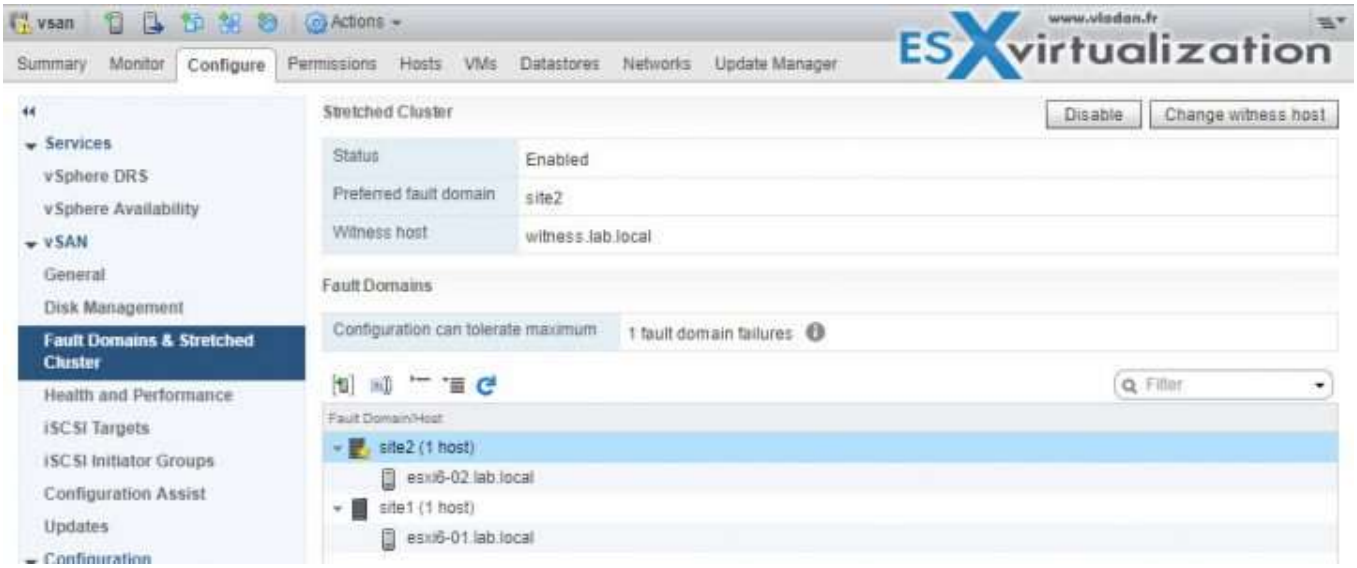
When a third party offers a storage provider, you typically must register the provider. An example of such a provider is the Virtual Volumes provider. You use the vSphere Web Client to register and manage each storage provider component.

Explain vSAN failure domains functionality

Think of virtual infrastructure in few racks. If one rack fails, all the host within this rack fail too. vSAN intelligently spreads vSAN components through several racks or rather several "fault domains".

vSAN requires at least two fault domains, each of which consists of one or more hosts. Fault domain definitions must acknowledge physical hardware constructs that might represent a potential zone of failure, for example, an individual computing rack enclosure.

On the image below you can see a vSAN installation having two fault domains. Each fault domain has one ESXi host and there is also a witness host which runs as a virtual appliance on a third ESXi host (outside of vSAN cluster).



VMware recommends using at least four fault domains (FD) as some evacuation modes (full data evacuation) aren't supported with three FD only. vSAN cannot rebalance the components if there is not the capacity left in another fault domain while doing a maintenance.

You can provide local fault protection for virtual machine objects within a single site in a stretched cluster. You can define a **Primary level of failures to tolerate** for the cluster, and a **Secondary level of failures to tolerate** for objects within a single site. In the case that one site is down, vSAN maintains availability with local redundancy in the available site.

number of fault domains = 2 * PFTT + 1

CONFIGURE/MANAGE VMWARE VSAN

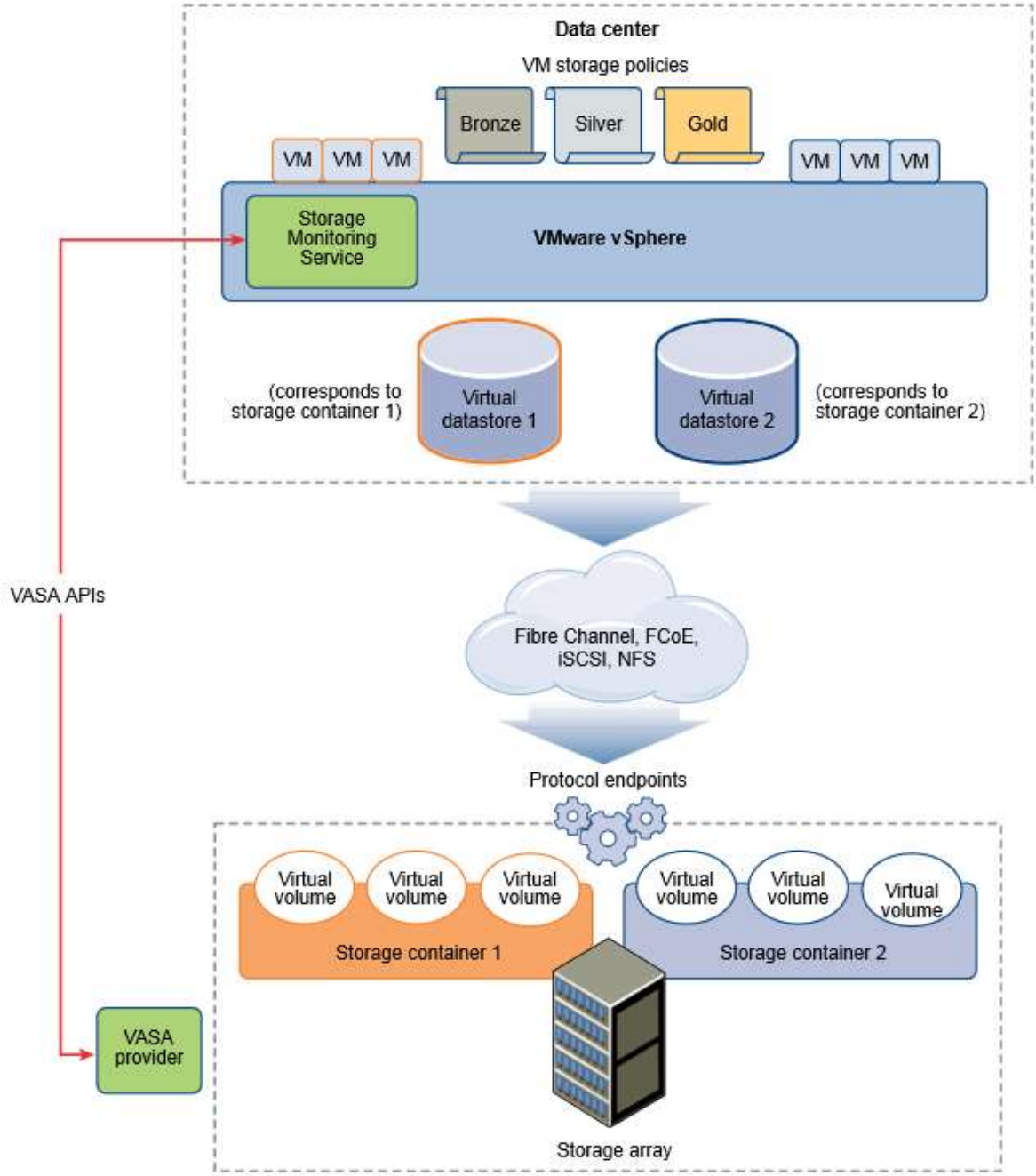
- VMware VSAN (hybrid) needs some spinning media (SAS or SATA) and 1 SSD per host (SATA, SAS or PCIe).
- VMware VSAN (All-Flash) needs some SATA/SAS for a capacity tier and 1 SSD high performance and endurance for caching.
- HBA which is on the VMware HCL (queue depth > 600).
- All hardware must be part of HCL (or if you want easy way -> via VSAN ready nodes!)
- HBA with RAID0 jor direct pass-through so ESXi can see the individual disks, not a raid volume.
- SSD sizing - 10% of consumed capacity.
- 1Gb Network (10GbE recommended).
- 1 VMkernel interface configured (dedicated) for VSAN traffic.
- Multicast activated on the switch (Note that vSAN 6.6 and higher does not use multicast any more. It uses unicast).
- IGMP Snooping and an IGMP Querier can be used to filter multicast traffic to a limited to a specific port group. Useful if other non-Virtual SAN network devices exist on the same layer 2 network segment (VLAN).
- IPv4 only on the switch.
- Minimum 3 hosts in the cluster (4 recommended) - maxi. 64 hosts (since vSphere 6).

CREATE/MODIFY VMWARE VIRTUAL VOLUMES (VVOLS)

VVOls are here since vSphere 6. By using a special set of APIs called vSphere APIs for Storage Awareness (VASA), the storage system becomes aware of the virtual volumes and their associations with the relevant virtual machines. Through VASA, vSphere and the underlying storage system establish a two-way out-of-band communication to perform data services and offload certain virtual machine operations to the storage system. For example, such operations as snapshots, storage DRS and clones can be offloaded.

- VVOLs are supported on SANs compatible with VAAI (vSphere APIs for Array Integration).
- VVOLs supports vMotion, sVMotion, Snapshots, Linked-clones, vFRC, DRS
- VVOLs supports backup products which use VADP (vSphere APIs for Data Protection)
- VVOLs supports FC, FCoE, iSCSI and NFS

Image courtesy VMware



Virtual volumes are objects exported by a compliant storage system and typically correspond one-to-one with a virtual machine disk and other VM-related files. A virtual volume is created and manipulated out-of-band, not in the data path, by a VASA provider.

VVOLs Limitations

- VVOLs Does not work with standalone ESXi hosts (needs vCenter).
- VVOLs do not support RDMs.
- VVOLs with the virtual datastores are tightened to vCenter or if used with Host profiles, then only within this particular vCenter as the extracted host profile can be attached only to the hosts within the same vCenter as the reference host is located.
- No IPv6 support.
- NFS v3 only (v4.1 isn't supported).
- Multipathing only on SCSI-based endpoints, not on NFS-based protocol endpoint.

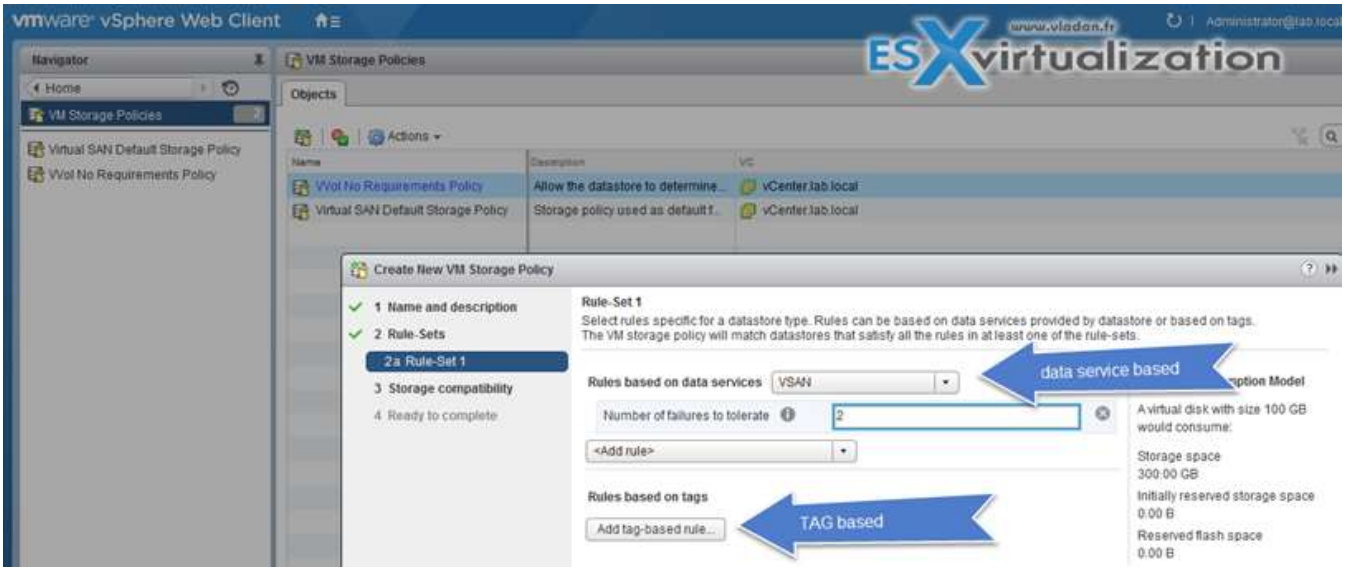
CONFIGURE STORAGE POLICIES

Virtual Machine Storage policies are covered vSphere Storage Guide on p. 225. Virtual machine storage policies are essential to virtual machine provisioning. These policies help you define storage requirements for the virtual machine and control which type of storage is provided for the virtual machine, how the virtual machine is placed within the storage, and which data services are offered for the virtual machine. SP contains storage rule or collection of storage rules.

To define a storage policy, you specify storage requirements for applications that run on virtual machines. After you apply this storage policy to a virtual machine, the virtual machine is placed in a specific datastore that can satisfy the storage requirements.

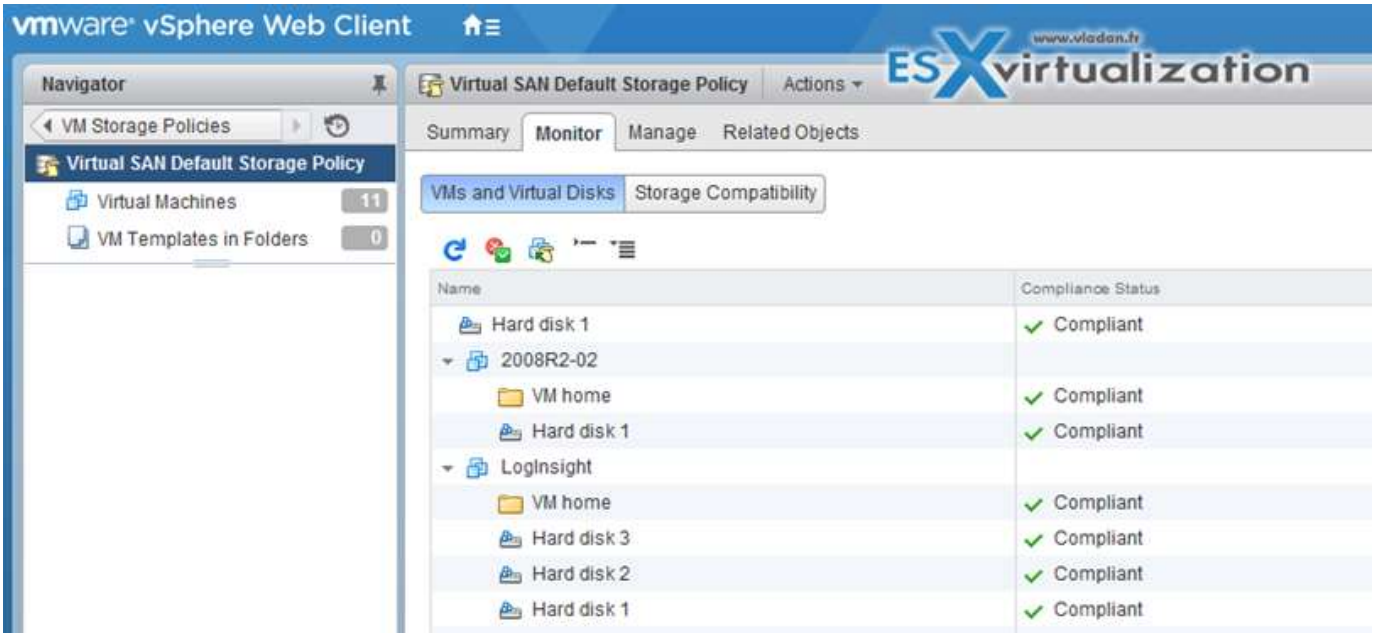
In case of VSAN and VVOLs, the SP determines how the VM storage objects are handled and allocated within the datastore to guarantee the SLA.

- **Rules based on storage-specific data service** - VSAN and VVOLs uses VASA to surface the storage capability to VMstorage policies' interface.
- **Rules based on TAGs** - by tagging a specific datastore. More than One tag can be applied per datastore.



VIEW VMS AND DISKS IF THEY COMPLY WITH VM STORAGE POLICIES

VM Storage Policies > Click a particular Storage Policy > Monitor



ENABLE/DISABLE VSAN FAULT DOMAINS

VSAN fault domains allow creating an environment where the in case of failure 2 hosts for example, which are in the same rack. Failure of all hosts within a **single fault domain is treated as one failure**. VSAN will not store more than one replica in this group (domain).

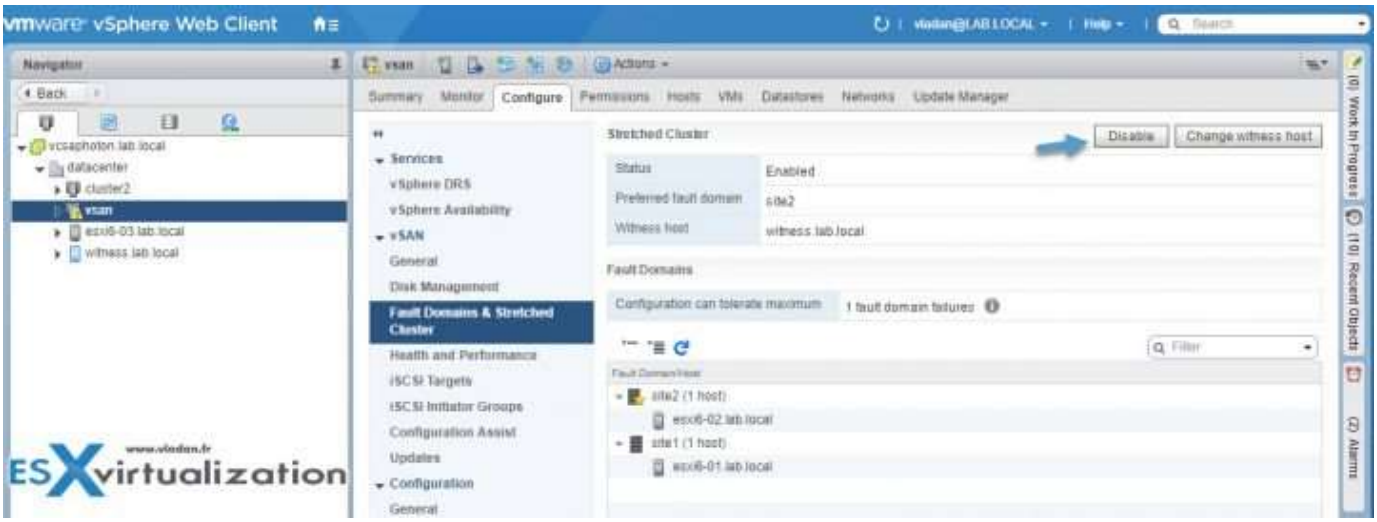
Requirements: 2*n+1 fault domains in a cluster. In order to leverage fault domain, you need at least 6 hosts (3 fault domains). Using three domains does not allow the use of certain evacuation modes, nor is Virtual SAN able to reprotect data after a failure.

VMware recommends **4 Fault domains**. (the same for vSAN clusters - 4 hosts in a VSAN cluster).

Hosts and Clusters > **Cluster** > **Manage** > **Settings** > **Virtual SAN** > **Fault Domains**

You can only include hosts that are 6.0 or later in fault domains.

If a host is not a member of a fault domain, Virtual SAN interprets it as a separate domain.



CREATE VIRTUAL VOLUMES GIVEN THE WORKLOAD AND AVAILABILITY REQUIREMENTS

- Virtual Volumes supports such vSphere features as vSphere vMotion, Storage vMotion, snapshots, linked clones, Flash Read Cache, and DRS.

You use the VM Storage Policies interface to create a storage policy. When you define the policy, you specify various storage requirements for applications that run on the virtual machines. You can also use storage policies to request specific data services, such as caching or replication, for virtual disks.

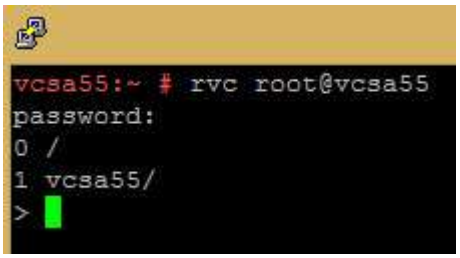
You apply the storage policy when you create, clone, or migrate the virtual machine. After you apply the storage policy, the SPBM mechanism assists you with placing the virtual machine in a matching datastore. In certain storage environments, SPBM determines how the virtual machine storage objects are provisioned and allocated within the storage resource to guarantee the required level of service. The SPBM also enables requested data services for the virtual machine and helps you to monitor policy compliance.

COLLECT VSAN OBSERVER OUTPUT

01. Connect via SSH and run this single command: (note my vCenter server's name is **vcsa55**

rvc root@vcsa55

02. You can navigate in the rvc as on Linux. By typing "cd .." you go up one level and "ls" lists you available objects. Pretty simple. So as you can see in the pic below, I went to the ***/vcsa55/home/computers/vsan*** level and then, to enable live monitoring for a cluster, run the command (Note: The cluster in my lab is named VSAN. -:)



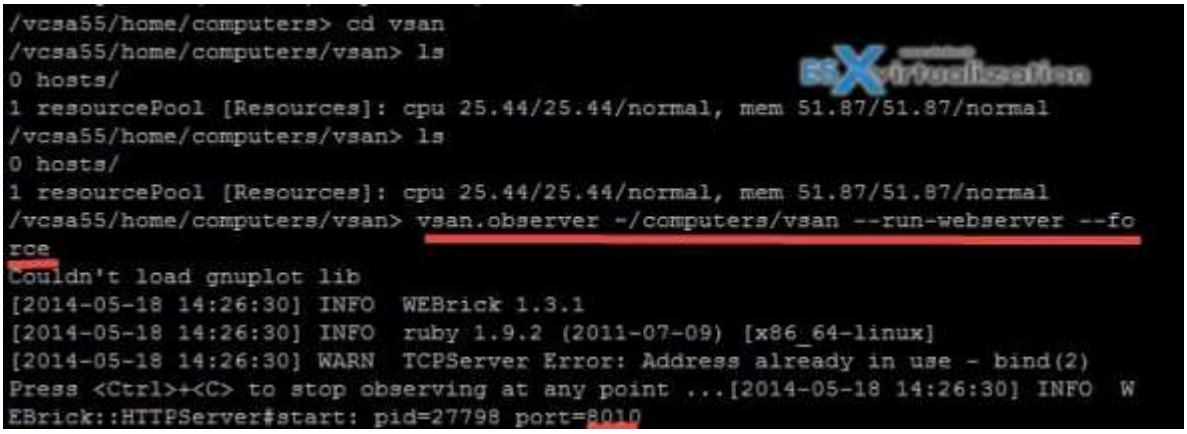
You can start web server and generate bundle with this command:

vsan.observer –run-webserver –force –generate-html-bundle /tmp — interval 30 –max-runtime 1

If you want just to view the graphs and check the real-time performance you can use this command:

vsan.observer ~/computers/VSAN --run-webserver --force

(Note there is double dash before "**run**" and before "**force**", but WordPress sometimes cut this off).



Once done, you'll need to navigate to the web UI which is accessible at this address:

https://vCenterServer_hostname_or_IP_Address:8010

So this simple command activates the webserver and the port is shown at the bottom. So in my particular situation I'll connect via web browser to the web server via: **vcsa55.lab.local:8081**

CREATE STORAGE POLICIES APPROPRIATE FOR GIVEN WORKLOADS AND AVAILABILITY REQUIREMENTS

VM Storage policy control which type of storage is provided for the virtual machine and to which storage the virtual machine is placed. They also determine data services that the virtual machine can use.

You use the VM Storage Policies interface to create a storage policy. When you define the policy, you specify various storage requirements for applications that run on the virtual machines. You can also use storage policies to request specific data services, such as caching or replication, for virtual disks.

You apply the storage policy when you create, clone, or migrate the virtual machine. After you apply the storage policy, the SPBM mechanism assists you with placing the virtual machine in a matching datastore. In certain storage environments, SPBM determines how the virtual machine storage objects are provisioned and allocated within the storage resource to guarantee the required level of service. The SPBM also enables requested data services for the virtual machine and helps you to monitor policy compliance.

CONFIGURE VVOLS PROTOCOL ENDPOINTS

Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives. Virtual volumes are not pre-provisioned but created automatically when you perform virtual machine management operations. These operations include a VM creation, cloning, and snapshotting. ESXi and vCenter Server associate one or more virtual volumes to a virtual machine.

- **Storage Provider** - A Virtual Volumes storage provider, also called a VASA provider, is a software component that acts as a storage awareness service for vSphere.

- **Storage Container** - A storage container is a part of the logical storage fabric and is a logical unit of the underlying hardware. The storage container logically groups virtual volumes based on management and administrative needs.
- **Protocol Endpoints** -ESXi hosts use a logical I/O proxy, called the protocol endpoint, to communicate with virtual volumes and virtual disk files that virtual volumes encapsulate. ESXi uses

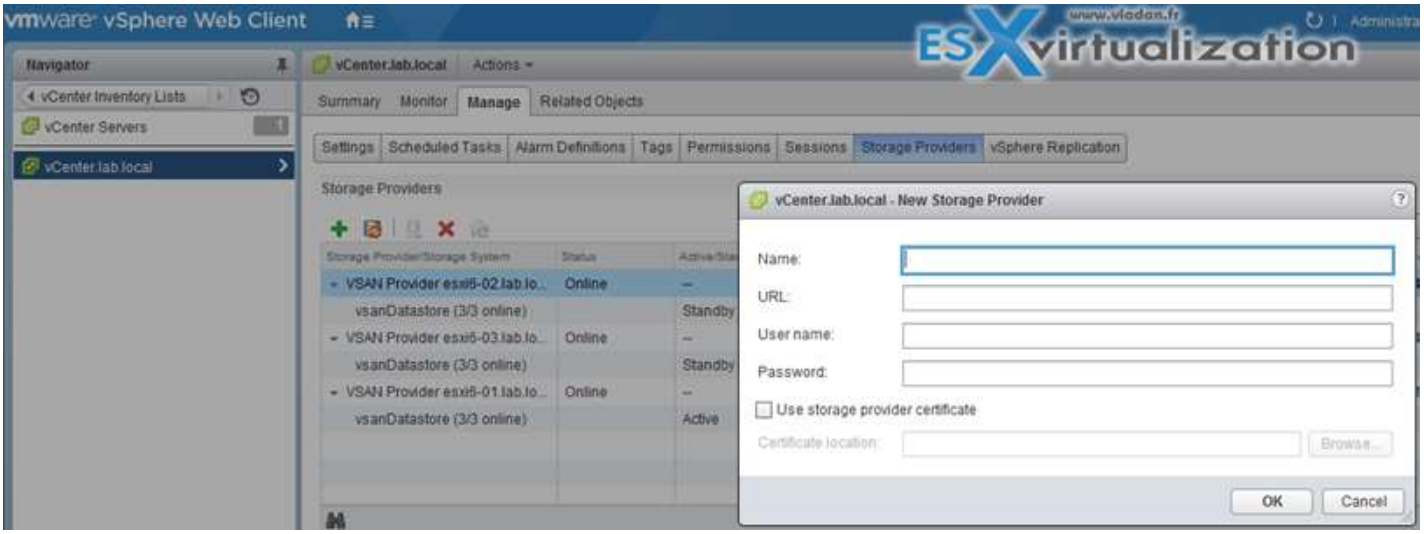
protocol endpoints to establish a data path on demand from virtual machines to their respective virtual volumes.

- **Virtual Datastores** - A virtual datastore represents a storage container in vCenter Server and the vSphere Web Client.

Steps to Enable VVOLs

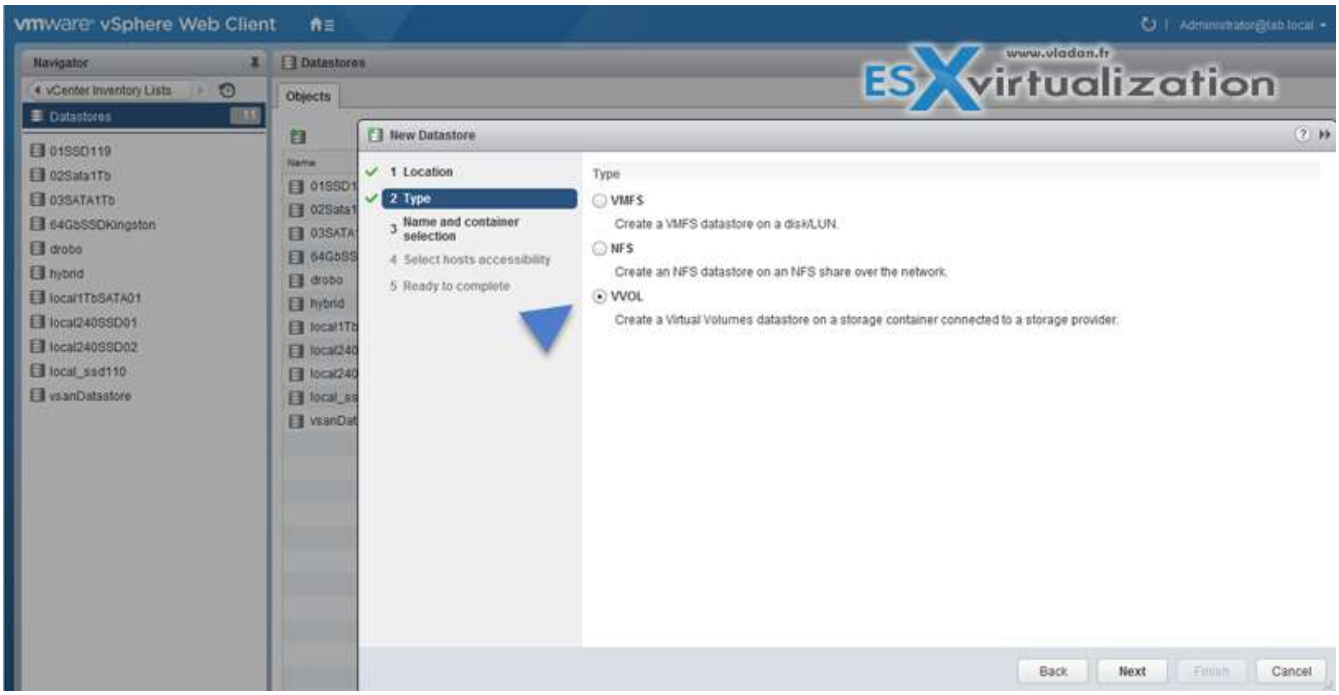
- **Step 1:** Register Storage Providers for VVOLs

vCenter Inventory Lists > **vCenter Servers** > **vCenter Server** > **Manage** > **Storage Providers**



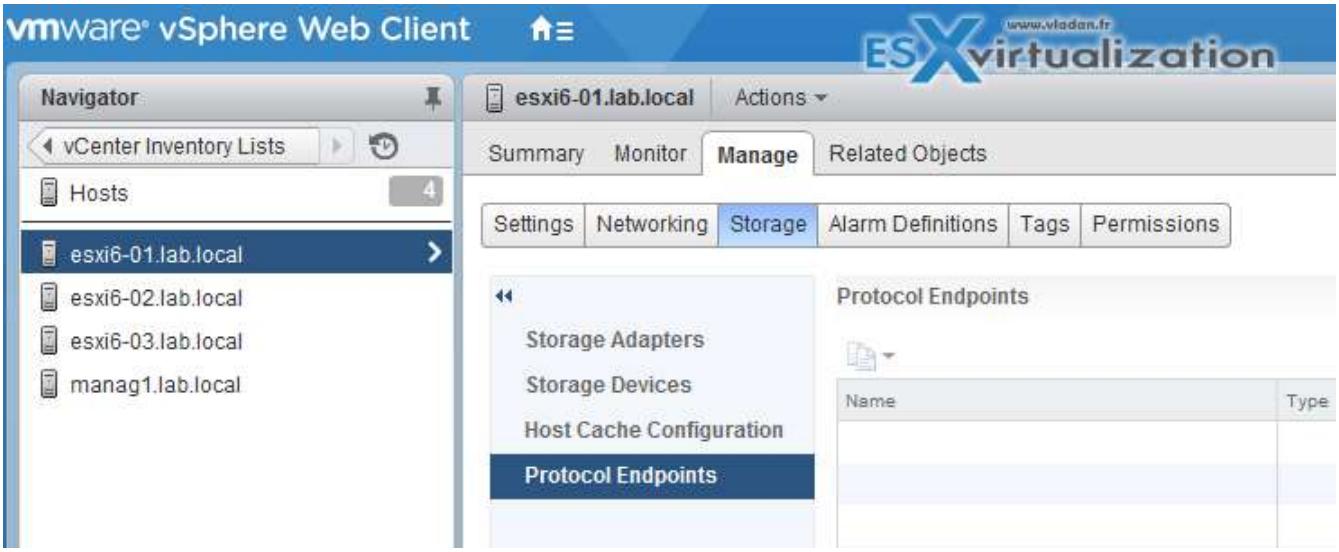
- **Step 2**: Create a Virtual Datastore

vCenter Inventory Lists > **Datastores**



- **Step 3:** Review and manage protocol endpoints

vCenter Inventory Lists > **Hosts** > **Host** > **Manage** > **Storage** > **Protocol Endpoints**



- (optional) Change the path selection policy (psp) for protocol endpoint.

Manage > **Storage** > **Protocol Endpoints** > **select** the protocol endpoint you want to change and click Properties > under Multipathing Policies click **Edit Multipathing**

VCP6.5-DCV Objective 3.3 - Configure vSphere Storage Multipathing and Failover

Explain common multipathing components

VMware ESXi, in order to keep its connection to a storage, it supports multipathing, which is basically a technology allowing to use more than one physical path that transfers data between ESXi host and storage device.

This is particularly helpful when you have a failure on your storage network (NIC, storage processor, switch, cable). VMware ESXi can switch to another physical path, which does not use the failed component. The path switching to avoid failed components is called path failover.

In addition to path failover, multipathing provides load balancing. Load balancing is the process of distributing I/O loads across multiple physical paths. Load balancing reduces or removes a potential bottleneck.

For iSCSI, there can be two different cases whether you use software iSCSI or hardware iSCSI.

Failover with Software iSCSI - With software iSCSI, as shown on Host 2 of the Host-Based Path Failover illustration, you can use multiple NICs that provide failover and load balancing capabilities for iSCSI connections between your host and storage systems.

For this setup, because multipathing plug-ins do not have direct access to physical NICs on your host, you first need to connect each physical NIC to a separate VMkernel port. You then associate all VMkernel ports with the software iSCSI initiator using a port binding technique. As a result, each VMkernel port connected to a separate NIC becomes a different path that the iSCSI storage stack and its storage-aware multipathing plug-ins can use.

Failover with Hardware iSCSI - ESXi host has at least two (or more) hardware iSCSI adapters connected. The storage system can be reached using one or more switches (at least two preferably). Also, the storage array should have two storage processors (SP) so that the adapter can use a different path to reach the storage system.

Differentiate APD and PDL states

VMware High Availability (HA) was further enhanced with a function related to shared storage and it's called **VM Component Protection (VMCP).**

When VMCP is enabled, vSphere can detect datastore accessibility failures, APD (All paths down) or PDL (Permanent device lost), and then recover affected virtual machines by restarting them on other hosts in the cluster which is not affected by this datastore failure. VMCP allows the admin to determine the response that vSphere HA will make. It can be simple alarm only or it can be the VM restart on other hosts. The latter one is perhaps what we're looking for.

Limitations:

- VMCP does not support vSphere Fault Tolerance. If VMCP is enabled for a cluster using Fault Tolerance, the affected FT virtual machines will automatically receive overrides that disable VMCP.
- No VSAN support (if VMDKs are located on VSAN then they're not protected by VMCP).
- No VVOLs support (same here).
- No RDM support (same here).

Compare and contrast Active Optimized vs. Active non-Optimized port group states

The active unoptimized is the path to the LUN which is not owned by the storage processor. This situation occurs on Arrays which are Asymmetric Active-Active.

- Optimized paths: are the paths to the Storage Processor which owns the LUN.
- Unoptimized paths: are the paths to the Storage Processor which does not own the LUN. And has a connection to the LUN via interconnect between the processors.

The default PSP for devices claimed by VMW_SATP_ALUA is VMW_PSP_MRU, which selects an "active/optimized" path reported by VMW_SATP_ALUA, or an "active/unoptimized" path if there's no "active/optimized" path. The system will revert to active/optimized when available.

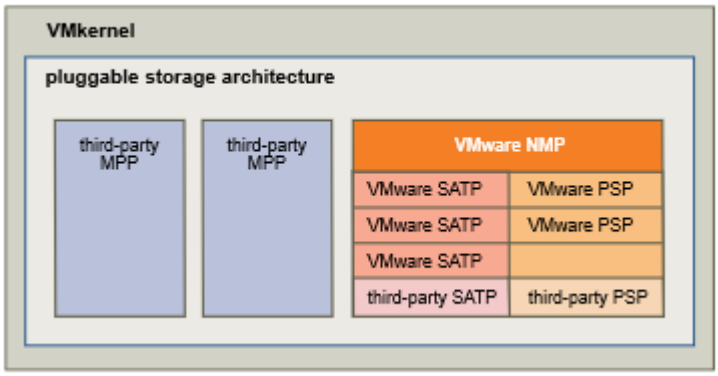
Explain features of Pluggable Storage Architecture (PSA)

To manage storage multipathing, ESXi uses a collection of Storage APIs, also called the Pluggable Storage Architecture (PSA). The PSA is an open, modular framework that coordinates the simultaneous operation of multiple multipathing plug-ins (MPPs). The PSA allows 3rd party software developers to design their own load balancing techniques and failover mechanisms for a particular storage array, and insert their code directly into the ESXi storage I/O path.

The VMkernel multipathing plug-in that ESXi provides by default is the VMware Native Multipathing Plugin (NMP). The NMP is an extensible module that manages sub plug-ins. 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.

- **VMware NMP** – default multipathing module (**N**ative **M**ultipathing **P**lugin). Nmp plays a role when associating the set of physical paths with particular storage device or LUN, but delegates the details to SATP plugin. On the other hand, the choice of path used when IO comes is is handled by PSP (**P**ath **S**election **P**lugin)
- **VMware SATP** – Storage Array Type Plugins runs hand in hand with NMP and are responsible for array based operations. ESXi has SATP for every supported SAN. It also provides default SATPs that support non-specific active-active and ALUA storage arrays, and the local SATP for direct-attached devices.
- **VMware PSP**s – Path Selection Plugins are sub-plugins of VMware NMP and they choose a physical path for IO requests.

Figure 17-5. Pluggable Storage Architecture



The multipathing modules perform the following operations:

- Manage physical path claiming and unclaiming.
- Manage creation, registration, and deregistration of logical devices.
- Associate physical paths with logical devices.
- Support path failure detection and remediation.
- Process I/O requests to logical devices:
    - Select an optimal physical path for the request.
    - Depending on a storage device, perform specific actions necessary to handle path failures and I/O
      command retries.
- Support management tasks, such as reset of logical devices.

UNDERSTAND THE EFFECTS OF A GIVEN CLAIM RULE ON MULTIPATHING AND FAILOVER

ESXi does rescan your storage adapter. You can rescan manually as well. When ESXi host discovers all physical paths to storage devices available to the host, it uses a **storage multipathing plugin** (MPP) to claim the path to a particular storage device.

By default, the ESXi host scans its paths every 5 minutes to find out which unclaimed paths should be claimed by the appropriate MPP.

The claim rules are numbered. For each physical path, the host runs through the claim rules starting with the lowest number first. The attributes of the physical path are compared to the path specification in the claim rule. If there is a match, the host assigns the MPP specified in the claim rule to manage the physical path. This continues until all physical paths are claimed by corresponding MPPs, either third-party multipathing plug-ins or the **native multipathing plug-in** (NMP).

For the paths managed by the NMP module, the second set of claim rules is applied. These rules determine which **Storage Array Type Plug-In** (SATP) should be used to manage the paths for a specific array type, and which Path Selection Plug-In (PSP) is to be used for each storage device.

Use the vSphere Web Client to view which SATP and PSP the host is using for a specific storage device and the status of all available paths for this storage device. If needed, you can change the default VMware PSP using the client. To change the default SATP, you need to modify claim rules using the vSphere CLI.

The objective **VCP6.5-DCV Objective 3.3 - Configure vSphere Storage Multipathing and Failover** is quite important so you really understand how multipathing works under the hood. Claim rules is a must.

Explain the function of claim rule elements

Claim rules indicate whether the NMP multipathing plug-in or a third-party MPP manages a given physical path.

List the multipathing claim rules by running the esxcli command:

--server=server_name storage core claimrule list --claimrule-class=MP

- Vendor - Indicate the vendor of the paths to user in this operation (-V)
- Model - Indicate the model of the paths to use in this operation. (-M)
- Device ID - Indicate the device Uid to use for this operation. (-d)
- SATP - The SATP for which a new rule will be added -s)
- PSP - Indicate which PSA plugin to use for this operation. (-P) (A required element)

Change the Path Selection Policy using the UI

See "Differentiate available Storage multipathing policies" chapter, for visuals.

Determine required claim rule elements to change the default PSP

Use the esxcli command to list available multipathing claim rules.

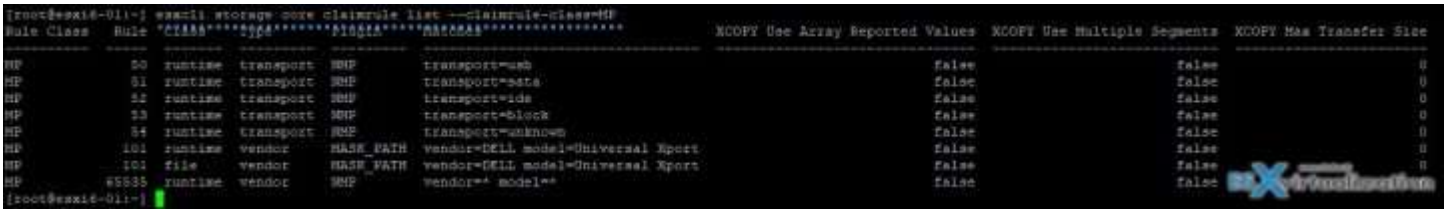
Claim rules indicate which multipathing plug-in, the NMP or any third-party MPP, manages a given physical path. Each claim rule identifies a set of paths, the parameters for which are earlier on this page.

Run this command:

esxcli storage core claimrule list --claimrule-class=MP

(there is a double dash in front of "claimrule").

in my case



DETERMINE THE EFFECT OF CHANGING PSP ON MULTIPATHING AND FAILOVER

The NMP SATP claim rules specify which SATP should manage a particular storage device. Usually, you do not need to modify the NMP SATP rules. If you need to do so, use the esxcli commands to add a rule to the list of claim rules for the specified SATP.

VMware SATP monitors the health of each physical path and can respond to error messages from the storage array to handle path failover. If you change the SATP for an array, it may change the PSP which might create unexpected failover results.

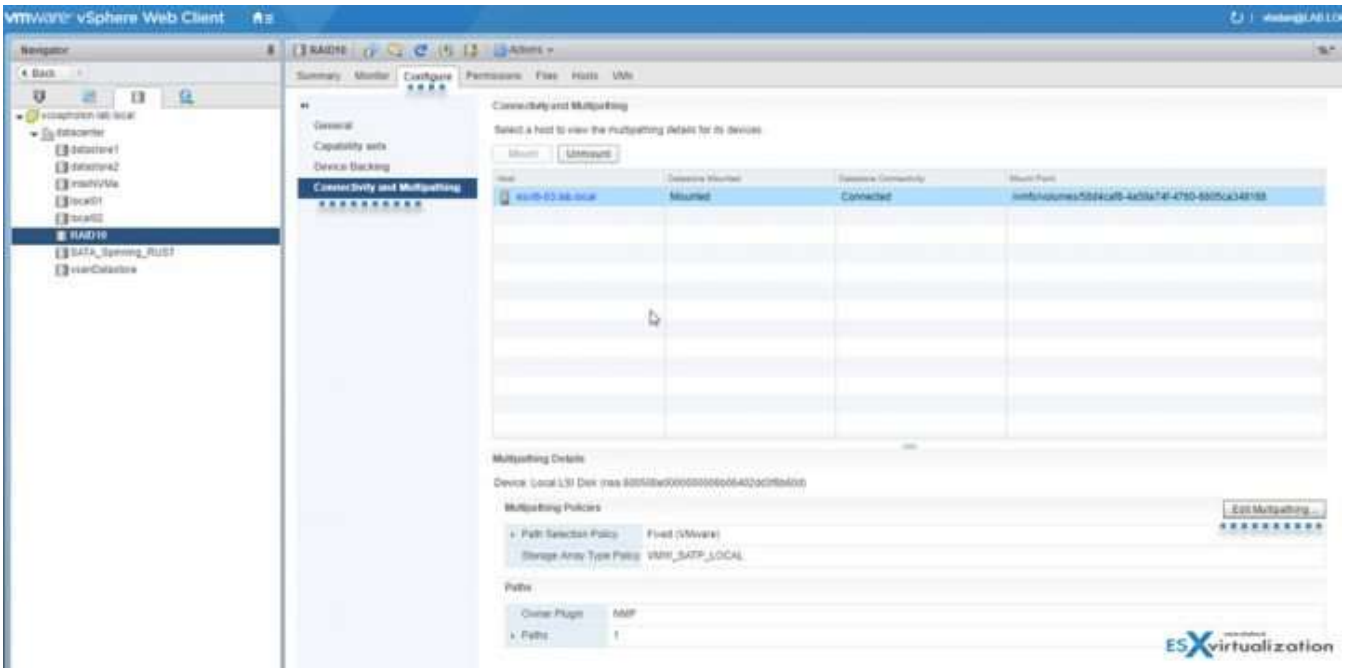
DETERMINE THE EFFECTS OF CHANGING SATP ON RELEVANT DEVICE BEHAVIOR

VMware provides a SATP for every type of array on the HCL. The SATP monitors the health of each physical path and can respond to error messages from the storage array to handle path failover. If you change the SATP for an array, it may change the PSP which might create unexpected failover results.

CONFIGURE/MANAGE STORAGE LOAD BALANCING

The goal of load balancing policy is to give equal “chance” to each storage processors and the host server paths by distributing the IO requests equally. Using the load balancing methods allows optimizing Response time, IOPs or MBPs for VMs performance.

To get started, if you’re using block storage – check the **Storage** > **Datastore** > **Configure** > **Connectivity and Multipathing > Edit Settings.**



Load balancing is the process of spreading server I/O requests across all available SPs and their associated host server paths. The goal is to optimize performance in terms of throughput (I/O per second, megabytes per second, or response times).

DIFFERENTIATE AVAILABLE STORAGE LOAD BALANCING OPTIONS

Make sure read/write caching is enabled.

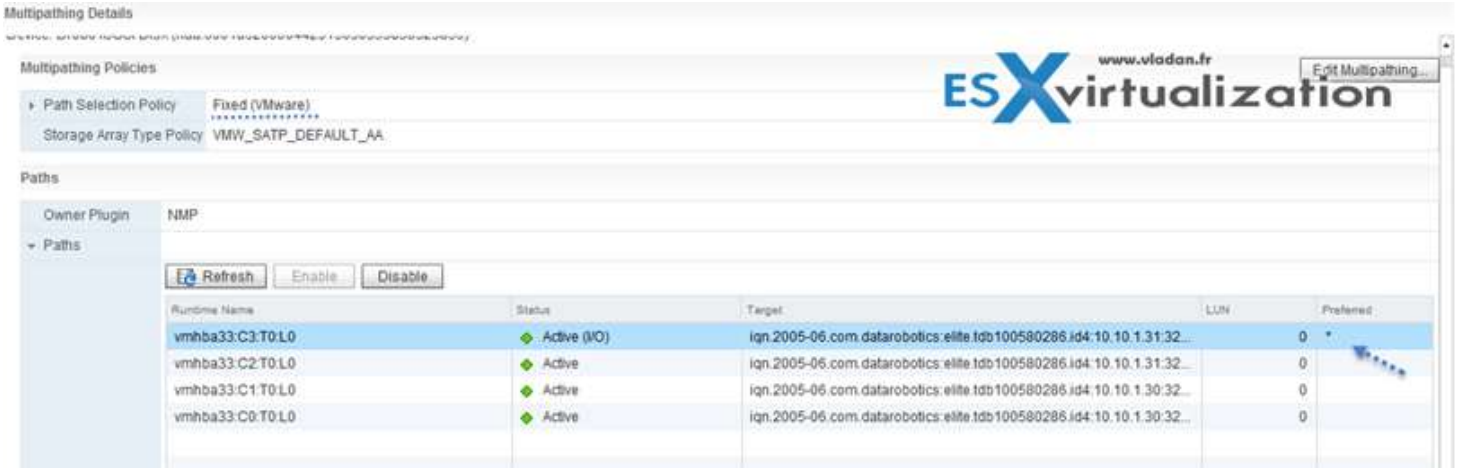
SAN storage arrays require continual redesign and tuning to ensure that I/O is load balanced across all storage array paths. To meet this requirement, distribute the paths to the LUNs among all the SPs to provide optimal load balancing. Close monitoring indicates when it is necessary to rebalance the LUN distribution.

Tuning statically balanced storage arrays is a matter of monitoring the specific performance statistics (such as I/O operations per second, blocks per second, and response time) and distributing the LUN workload to spread the workload across all the SPs

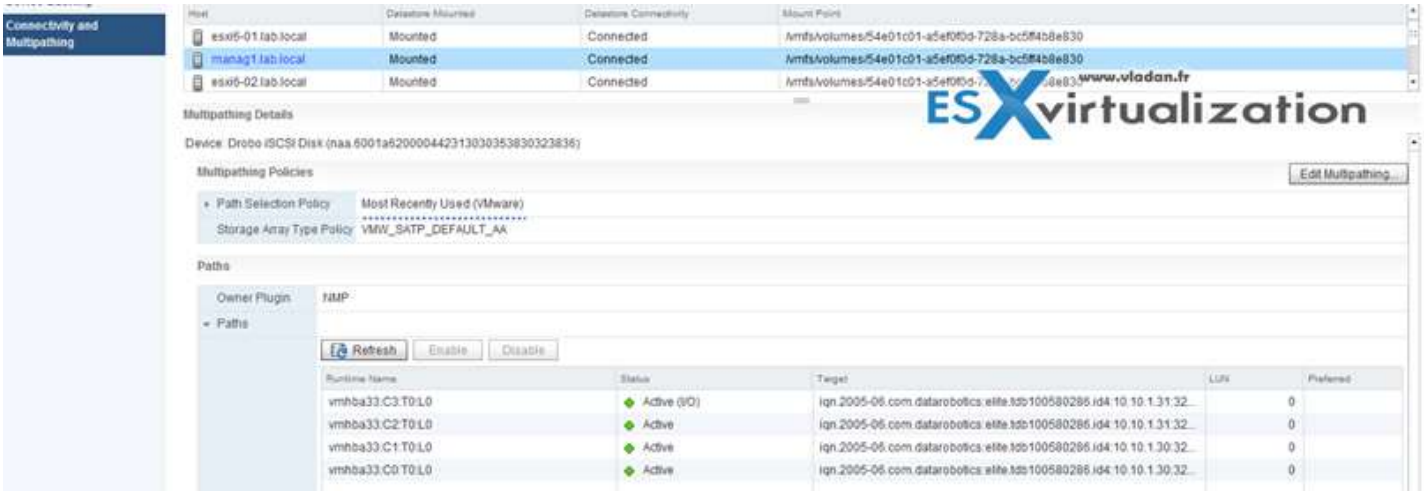
DIFFERENTIATE AVAILABLE STORAGE MULTIPATHING POLICIES

You can select different path selection policy from the default ones, or if you have installed a third-party product which has added its own PSP:

- **Fixed** – (VMW_PSP_FIXED) the host uses designated preferred path if configured. If not it uses first working path discovered. **The prefered path needs to be configured manually.**



- **Most Recently Used** – (VMW_PSP_MRU) The host selects the path that it used most recently. When the path becomes unavailable, the host selects an alternative path. The host does not revert back to the original path when that path becomes available again. There is **no preferred path** setting with the MRU policy. MRU is the default policy for most active-passive arrays.



- **Round Robin** (RR) – VMW_PSP_RR – The host uses an automatic path selection algorithm rotating through all active paths when connecting to active-passive arrays, or through all available paths when connecting to active-active arrays. RR is the default for a number of arrays and can be used with both active-active and active-passive arrays to implement load balancing across paths for different LUNs.

CONFIGURE STORAGE POLICIES INCLUDING VSPHERE STORAGE APIS FOR STORAGE AWARENESS

For entities represented by storage (VASA) providers, verify that an appropriate provider is registered. After the storage providers are registered, the VM Storage Policies interface becomes populated with information about datastores and data services that the providers represent.

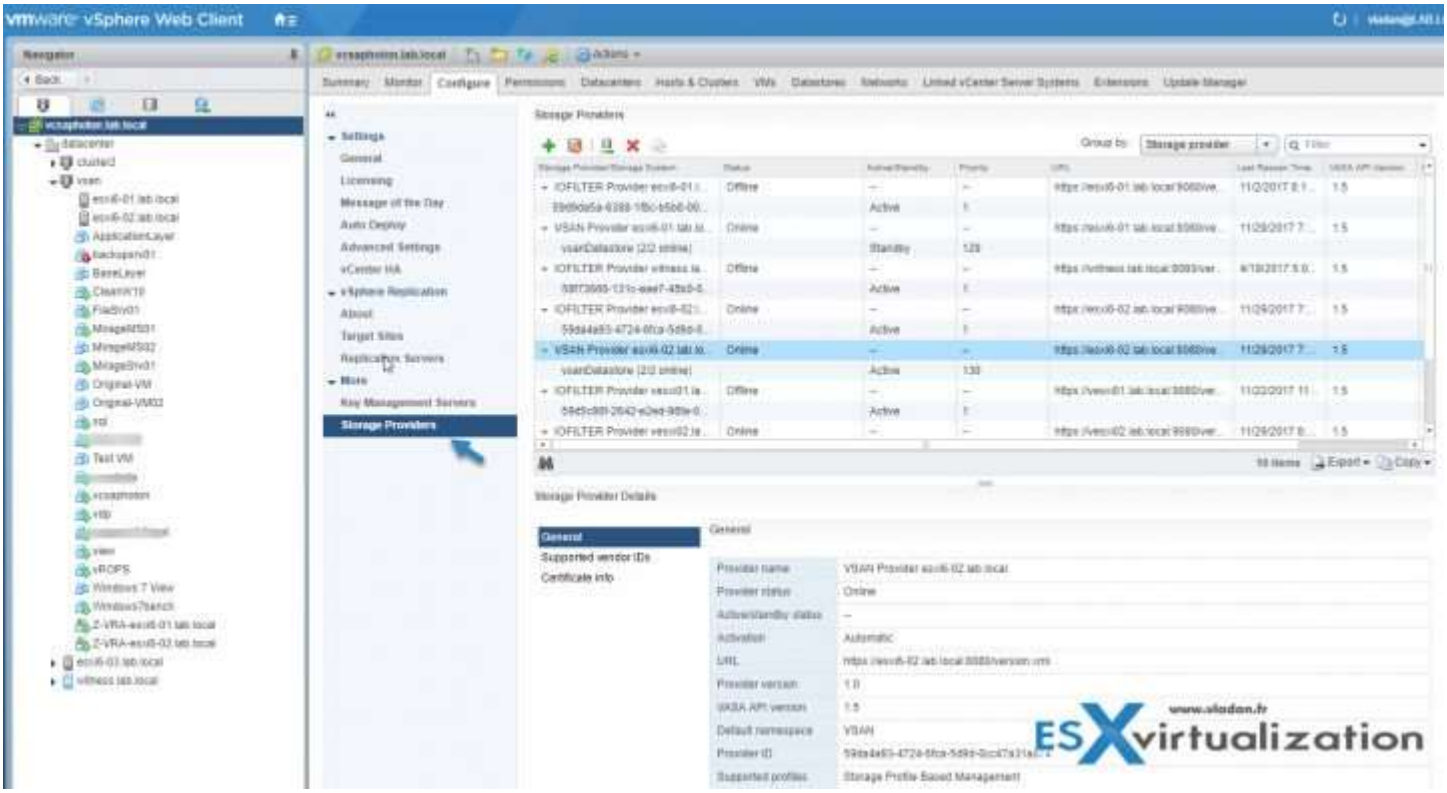
Entities that use the storage provider include Virtual SAN, Virtual Volumes, and I/O filters. Depending on the type of the entity, some providers are self-registered. Other providers, for example, the Virtual Volumes storage provider, must be manually registered. After the storage providers are registered, they deliver the following data to the VM Storage Policies interface:

- Storage capabilities and characteristics for such datastores as Virtual Volumes and Virtual SAN
- I/O filter characteristics

WHERE?

vSphere Web Client > Select **vCenter Server** object > **Configure TAB** > **Storage Providers**

There you can check the storage providers which are registered with vCenter.



The list shows general information including the name of the storage provider, its URL and status, storage entities that the provider represents, and so on. To display more details, select a specific storage provider or its component from the list.

Locate failover events in the UI

You can check failover events in the Events TAB of the monitor window from vCenter server.

VCP6.5-DCV Objective 3.4 - Perform VMFS and NFS configurations and upgrades

Perform VMFS v5 and v6 configurations

It's possible to create VMFS datastore on any SCSI based storage available to your ESX host. Basically, you need to configure any adapters (iSCSI, FC..) then discover the new storage by rescaning the adapter.

VMFS6 - This option is a default for 512e storage devices. The ESXi hosts of version 6.0 or earlier cannot recognize the VMFS6 datastore. If your cluster includes ESXi 6.0 and ESXi 6.5 hosts that share the datastore, this version might not be appropriate.

VMFS5 - This option is a default for 512n storage devices. VMFS5 datastore supports access by the ESXi hosts of version 6.5 or earlier.

Define configuration details for the datastore. Specify partition configuration.

Check "Create/Rename/Delete/Unmount VMFS datastores" chapter for visuals.

Describe VAAI primitives for block devices and NAS

VAAI is a method for offloading specific storage operations from the ESXi Host to the storage array, so it lowers CPU load and accelerates the operations.

VAAI has three built-in capabilities:

- Full Copy
- Block Zeroing
- Hardware-assisted locking

For NAS, an additional plugin needs to be installed to help perform the offloading. VAAI defines a set of storage primitives, which replace select SCSI operations with VAAI operations that are performed on the storage array instead of the ESXi Host.

Part of the today's topic which is VCP6.5-DCV Objective 3.4 - Perform VMFS and NFS configurations and upgrades, is also a recap of all those VMware File system technologies such as VMFS, NFS, VSAN or VVOLs.

Differentiate VMware file system technologies

- **VMFS (version 3, 5, and 6)** - Datastores that you deploy on block storage devices use the vSphere Virtual Machine File System format, a special high-performance file system format that is optimized for storing virtual machines.
- **NFS (version 3 and 4.1)** - 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 mounts the volume as an NFS datastore, and uses it for storage needs. ESXi supports versions 3 and 4.1 of the NFS protocol.
- **Virtual SAN** - Virtual SAN aggregates all local capacity devices available on the hosts into a single datastore shared by all hosts in the Virtual SAN cluster.
- **Virtual Volumes (VVOLs)** - Virtual Volumes datastore represents a storage container in vCenter Server and vSphere Web Client.

Migrate from VMFS5 to VMFS6

Online upgrade process allows VMFS datastores to be upgraded without disrupting hosts or virtual machines. New VMFS datastores are created with the GPT format.

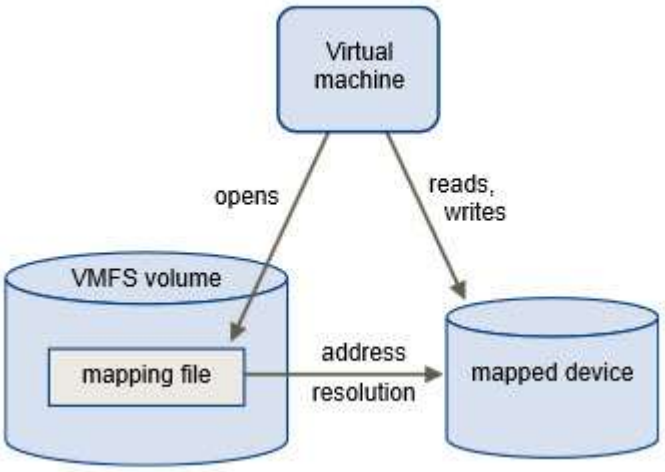
An upgraded VMFS datastore will continue to use the MBR format until it is expanded beyond 2TB. Once expanded beyond 2TB the MGS format is converted to GPT. Supports up to 256 VMFS datastores per host.

VMFS5 upgrade is a one-way process. Once upgraded to VMFS5 the datastore cannot be reverted back to the previous VMFS format. VMFS3 to VMFS5 datastore upgrade can be performed while the data store is in use.

Differentiate Physical Mode RDMs and Virtual Mode RDMs

RDM allows a VM directly access a LUN. Think of an RDM as a symbolic link from a VMFS volume to a raw LUN.

Figure 18-1. Raw Device Mapping



An RDM is a mapping file in a separate VMFS volume that acts as a proxy for a raw physical storage device. The RDM allows a virtual machine to directly access and use the storage device. The RDM contains metadata for managing and redirecting disk access to the physical device.

When to use RDM?

- When SAN snapshot or other layered applications run in the virtual machine. The RDM better enables scalable backup offloading systems by using features inherent to the SAN.
- In any MSCS clustering scenario that spans physical hosts — virtual-to-virtual clusters as well as physical-to-virtual clusters. In this case, cluster data and quorum disks should be configured as RDMs rather than as virtual disks on a shared VMFS.

If RDM is used in **physical compatibility mode** – no snapshots of VMs… Virtual machine snapshots are available for RDMs with **virtual compatibility mode**.

Physical Compatibility Mode – VMkernel passes all SCSI commands to the device, with one exception: the REPORT LUNs command is virtualized so that the VMkernel can isolate the LUN to the owning virtual machine. If not, all physical characteristics of the underlying hardware are exposed. It does allow the guest operating system to access the hardware directly. VM with physical compatibility RDM has limits like that you cannot clone such a VM or turn it into a template. Also, sVMotion or cold migration is not possible.

Virtual Compatibility Mode – VMkernel sends only READ and WRITE to the mapped device. The mapped device appears to the guest operating system exactly the same as a virtual disk file in a VMFS volume. The real hardware characteristics are hidden. If you are using a raw disk in virtual mode, you can realize the benefits of VMFS such as advanced file locking for data protection and snapshots for streamlining development processes. Virtual mode is also more portable across storage hardware than the physical mode, presenting the same behavior as a virtual disk file. (VMDK). You can use snapshots, clones template. When an RDM disk in virtual compatibility mode is cloned or a template is created out of it, the contents of the LUN are copied into a .vmdk virtual disk file.

Other limitations:

- You cannot map to a disk partition. RDMs require the mapped device to be a whole LUN.
- VFRC – Flash Read Cache does not support RDMs in physical compatibility (virtual compatibility is compatible).

- If you use vMotion to migrate virtual machines with RDMs, make sure to maintain consistent LUN IDs for RDMs across all participating ESXi hosts

Create a Virtual/Physical Mode RDM

After giving your VM direct access to a raw SAN LUN, you create an RDM disk that resides on a VMFS datastore and points to the LUN. You can create the RDM as an initial disk for a new virtual machine or add it to an existing virtual machine. When creating the RDM, you specify the LUN to be mapped and the datastore on which to put the RDM.

Although the RDM disk file has the same.vmdk extension as a regular virtual disk file. the RDM contains only mapping information. The actual virtual disk data is stored directly on the LUN.

The process:

- **Create a new VM** > proceed with the steps required to create a virtual machine > **Customize Hardware** page, click the **Virtual Hardware tab**.
- To delete the default virtual hard disk that the system created for your virtual machine, move your cursor over the disk and click the Remove icon > From the New drop-down menu at the bottom of the page, select RDM Disk and click Add > From the list of SAN devices or LUNs, select a raw LUN for your virtual machine to access directly and click OK.

The system creates an RDM disk that maps your virtual machine to the target LUN. The RDM disk is shown on the list of virtual devices as a new hard disk.

- Click the New Hard Disk triangle to expand the properties for the RDM disk > Select a location for the RDM disk. You can place the RDM on the same datastore where your virtual machine configuration files reside or select a different datastore. Select a compatibility mode.

Check above chapter "Differentiate Physical Mode RDMs and Virtual Mode RDMs" for Physical Compatibility or Virtual compatibility modes.

Differentiate NFS 3.x and 4.1 capabilities

NFS v3:

- ESXi managed multipathing
- AUTH_SYS (root) authentication
- VMware proprietary file locking
- Client-side error tracking

NFS v4.1:

- Native multipathing and session trunking
- Optional Kerberos authentication
- Built-in file locking
- Server-side error tracking

Compare and contrast VMFS and NFS datastore properties

The maximum size of a VMFS datastore is 64 TB. The maximum size of an NFS datastore is 100TB.

Another difference:

- VMFS uses SCSI queuing and has a default queue length of 32 outstanding I/Os at a time.
- NFS gives to each VM its own I/O data path.

You can run as twice as more VMs on NFS based datastores compared to VMFS ones.

Configure Bus Sharing

SCSI bus sharing for a VM means if the SCSI bus is shared. VMs can access the same VMDK simultaneously. The VM can be on the same ESXi or on different ESXi.

Where?

Right-click a VM > **Edit Settings** > On the **Virtual Hardware tab**, expand **SCSI controller** > Type of sharing in the SCSI Bus Sharing drop-down menu > 3 choices:

- **None:** Virtual disks cannot be shared by other virtual machines.
- **Virtual**: Virtual disks can be shared by virtual machines on the same ESXi host.
- **Physical**: Virtual disks can be shared by virtual machines on any ESXi host.

Configure Multi-writer locking

Useful for VMware FT, third-party cluster-aware applications or Oracle RAC VMs.

The multi-writer option allows VMFS-backed disks to be shared by multiple virtual machines. This option is used to support VMware fault tolerance, which allows a primary virtual machine and a standby virtual machine to simultaneously access a .vmdk file.

You can use this option to disable the protection for certain cluster-aware applications where the applications ensure that writes originating from two or more different virtual machines does not cause data loss. This document describes methods to set the multi-writer flag for a virtual disk.

In vSphere 6.0 and later, the GUI has the capability of setting Multi Writer flag without any need to edit .vmx file.

In the vSphere Client, power off the VM.

Select VM > Edit Settings > Options > Advanced > General > Configuration Parameters. Add rows for each of the shared disks and set their values to multi-writer

Add the Settings for each virtual disk that you want to share as below.
scsi1:0.sharing = ""multi-writer""
scsi1:1.sharing = ""multi-writer""
scsi1:2.sharing = ""multi-writer""
scsi1:3.sharing = ""multi-writer""

scsi1:0.sharing	multi-writer
scsi1:1.sharing	multi-writer
scsi1:2.sharing	multi-writer
scsi1:3.sharing	multi-writer

Connect an NFS 4.1 datastore using Kerberos

Prepare your NFS storage first.

vSphere client > Add datastore > NFS > type IP or FQDN, NFS mount and folder name > enable Kerberos and select an appropriate Kerberos model.

Two options:

1. **Use Kerberos for authentication only (krb5)** - Supports identity verification
2. **Use Kerberos for authentication and data integrity (krb5i)** - In addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

Create/Rename/Delete/Unmount VMFS datastores

Create Datastore – **vSphere Web Client** > **Hosts and Clusters** > Select **Host**> **Actions** > **Storage** > **New Datastore**

And you have a nice assistant which you follow…

The datastore can be created also via vSphere C# client.

To **rename datastore** > **Home** > **Storage** > **Right click** datastore > **Rename**

As you can see you can also **unmount** or **delete** datastore via the same right click.

Make sure that:

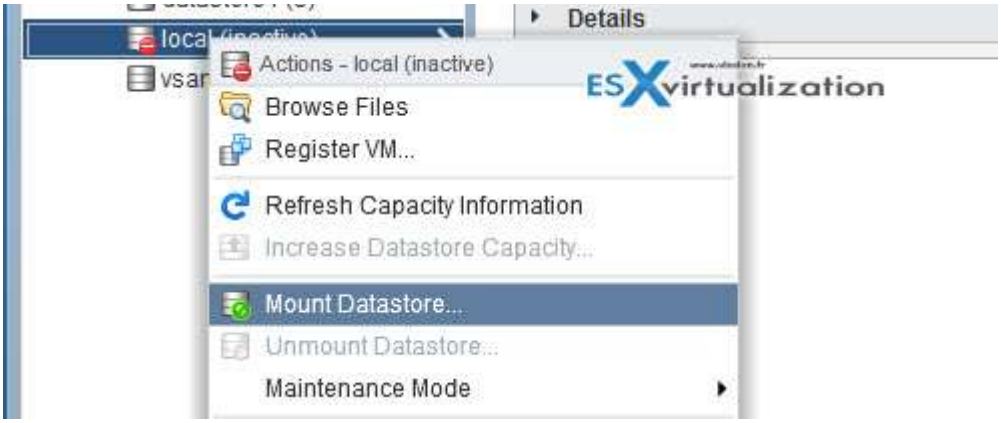
- There are **NO VMs** on that datastore you want to unmount.
- If HA configured, make sure that the datastore is **not** used for HA heartbeats
- Check that the datastore is **not** managed by Storage DRS
- Verify also that **Storage IO control** (SIOC) **is disabled** on the datastore

MOUNT/UNMOUNT AN NFS DATASTORE

Create NFS mount. Similar way as above **Right click datacenter** > **Storage** > **Add Storage**.

You can use NFS 3 or NFS 4.1 (note the limitations of NFS 4.1 for FT or SIOC). Enter the Name, Folder, and Server (IP or FQDN)

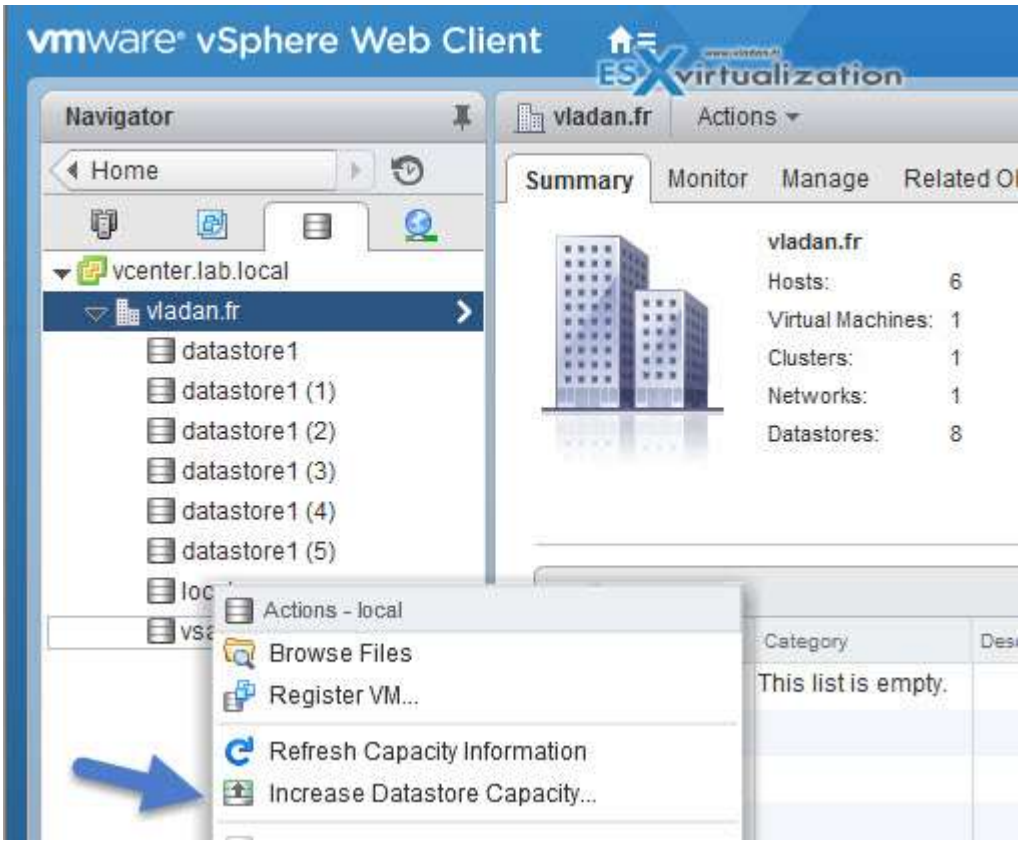
To Mount/unmount NFS datastore…



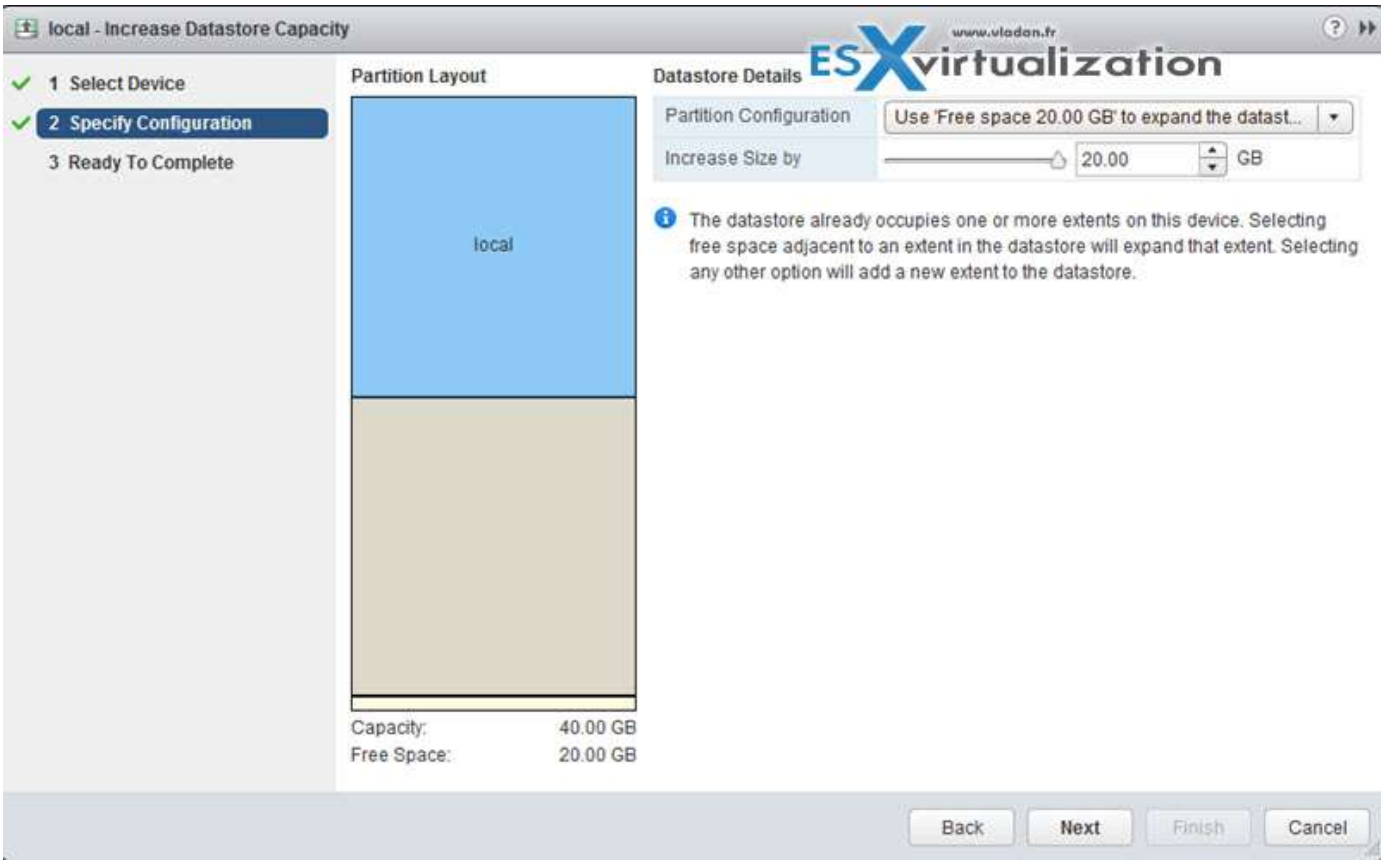
And then choose the host(s) to which you want this datastore to mount…

EXTEND/EXPAND VMFS DATASTORES

It’s possible to expand existing datastore by using extent OR by growing an expandable datastore to fill the available capacity.



and then you just select the device.

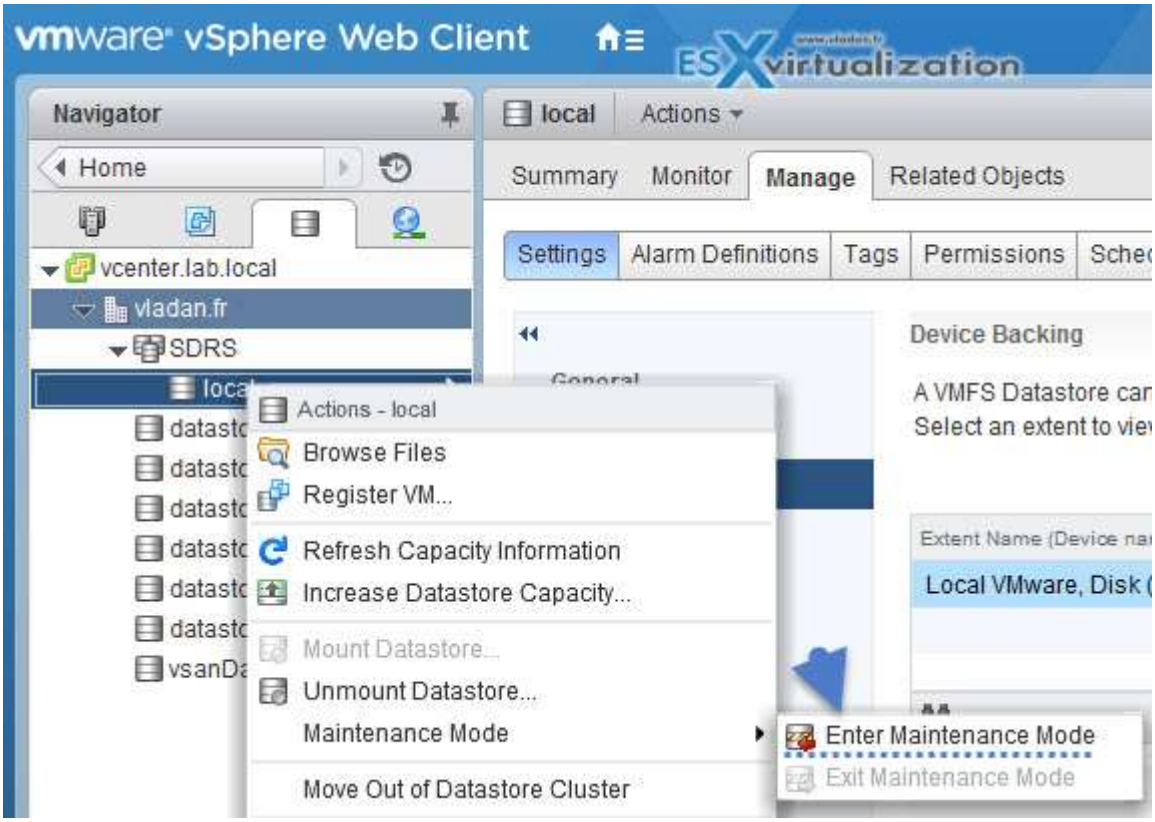


You can also **Add a new extent**. Which means that datastore can span over up to 32 extents and appear as a single volume…. But in reality, not many VMware admins likes to use extents….

Place a VMFS datastore in Maintenance Mode

Maintenance mode for datastore is available if the datastore takes part in Storage DRS cluster (SDRS). Regular datastore cannot be placed in maintenance mode. So if you want to activate SDRS you must first create SDRS cluster by right clicking **Datacenter** > **Storage** > **New Datastore Cluster**.

Then only you can put the datastore in maintenance mode…



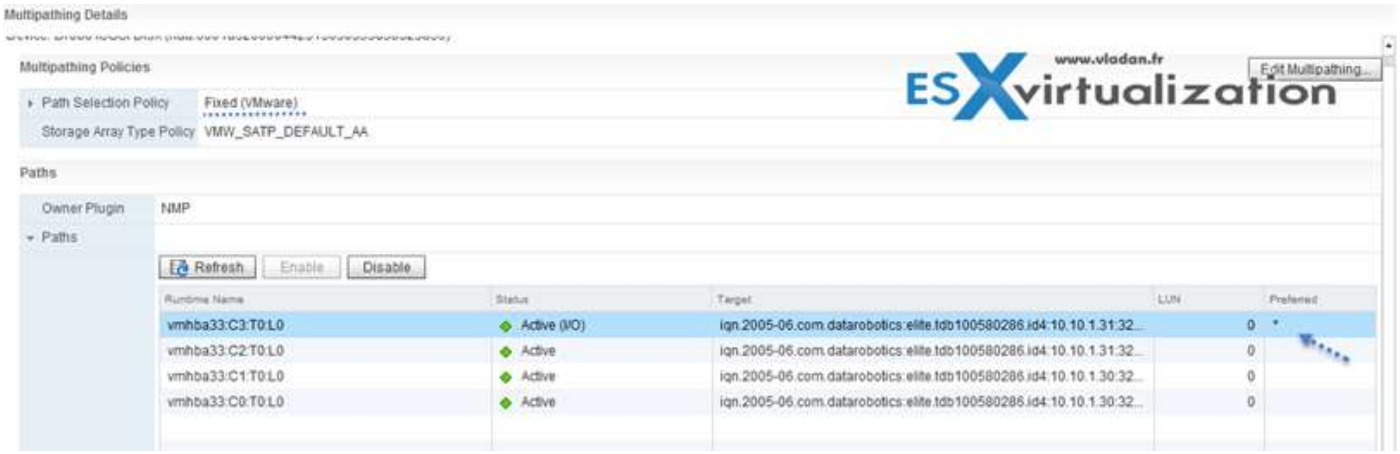
Select the Preferred Path/Disable a Path to a VMFS datastore

For each storage device, the ESXi host sets the path selection policy based on the claim rules. The different path policies we treated in our earlier chapter here – Configure vSphere Storage Multi-pathing and Failover.

Now if you want just to select a preferred path, you can do so. If you want the host to use a particular preferred path, specify it manually.

Fixed is the default policy for most active-active storage devices

Fixed – (VMW_PSP_FIXED) the host uses designated preferred path if configured. If not, it uses the first working path discovered. **The preferred path needs to be configured manually.**



ENABLE/DISABLE VSTORAGE API FOR ARRAY INTEGRATION (VAAI)

Tip: Check our How-to, tutorials, videos on a [dedicated vSphere 6.5 Page].

You need to have hardware that supports the offloading storage operations like:

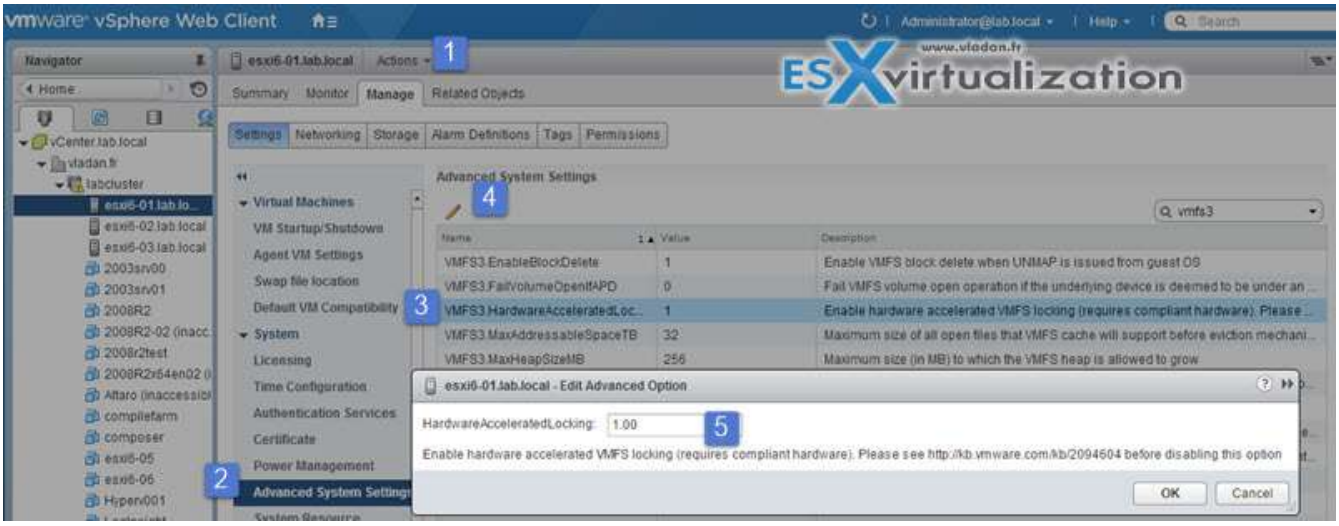
- Cloning VMs
- Storage vMotion migrations
- Deploying VMs from templates
- VMFS locking and metadata operations
- Provisioning thick disks
- Enabling FT protected VMs

HOW TO DISABLE? OR ENABLE?

Enable = 1
Disable = 0

vSphere **Web Client** > **Manage** tab > **Settings** > System, click **Advanced System Settings** > Change the value for any of the options to **0** (disabled):

- VMFS3.HardwareAcceleratedLocking
- DataMover.HardwareAcceleratedMove
- DataMover.HardwareAcceleratedInit



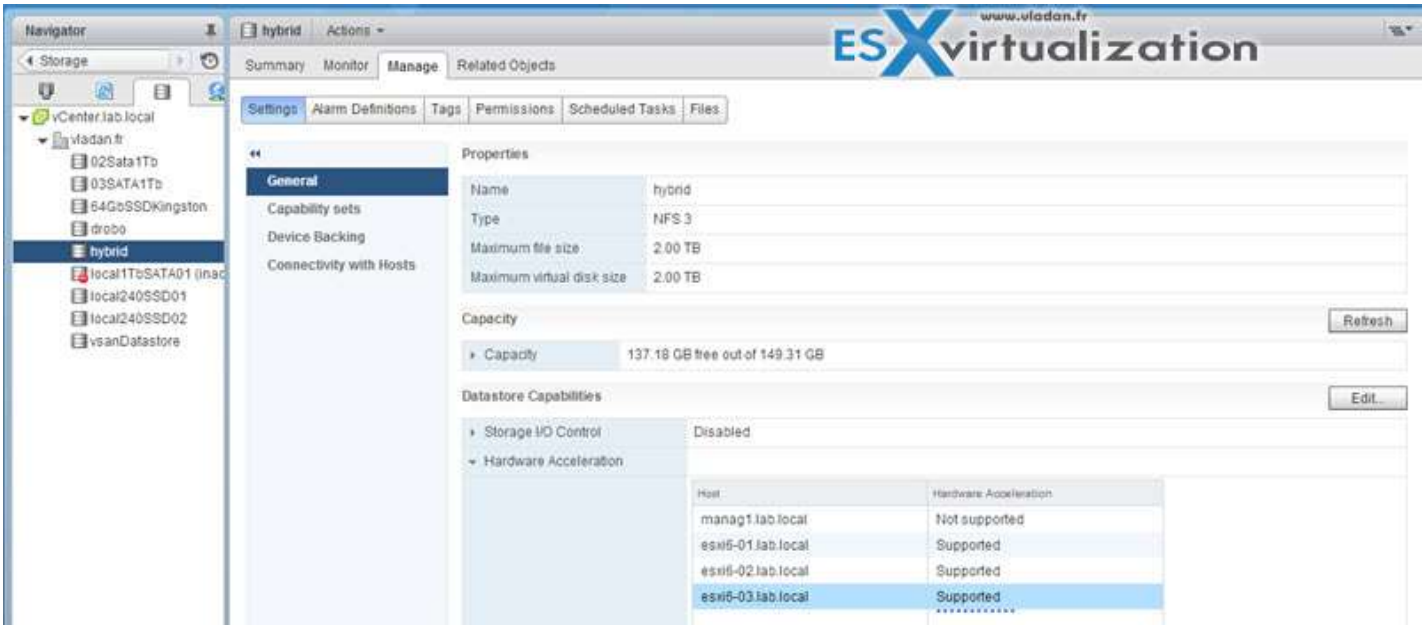
You can check the status of the hardware via CLI (via esxcli storage core device vaai status get)

```
[root@esxi6-02:~] esxcli storage core device vaai status get
t10.ATA_____KINGSTON_SNVP325S264GB_____________________________10BS1049T72Z
   VAAI Plugin Name:
   ATS Status: unsupported
   Clone Status: unsupported
   Zero Status: supported
   Delete Status: unsupported

naa.55cd2e404b88ac4b
   VAAI Plugin Name:
   ATS Status: unsupported
   Clone Status: unsupported
   Zero Status: supported
   Delete Status: supported
```

or on the NAS devices with (esxcli storage nfs list).

Via vSphere web client you can also see if a datastore has hardware acceleration support…



Determine a proper use case for multiple VMFS/NFS datastores

Usually, the choice for multiple VMFS/NFS datastores is based on performance, capacity and data protection.

Separate spindles – having different RAID groups to help provide better performance. Then you can have multiple VMs, executing applications which are I/O intensive. If you make a choice with single big datastore, then you might have performance issues…
Separate RAID groups – for certain applications, such as SQL server you may want to configure a different RAID configuration of the disks that the logs sit on and that the actual databases sit on.
Redundancy – You might want to replicate VMs to another host/cluster. You may want the replicated VMs to be stored on different disks than the production VMs. In case you have a failure on production disk system, you most likely still be running the secondary disk system just fine.

Load balancing – you can balance performance/capacity across multiple datastores.

Tiered Storage – Arrays comes often with Tier 1, Tier 2, Tier 3 and so you can place your VMs according to performance levels…

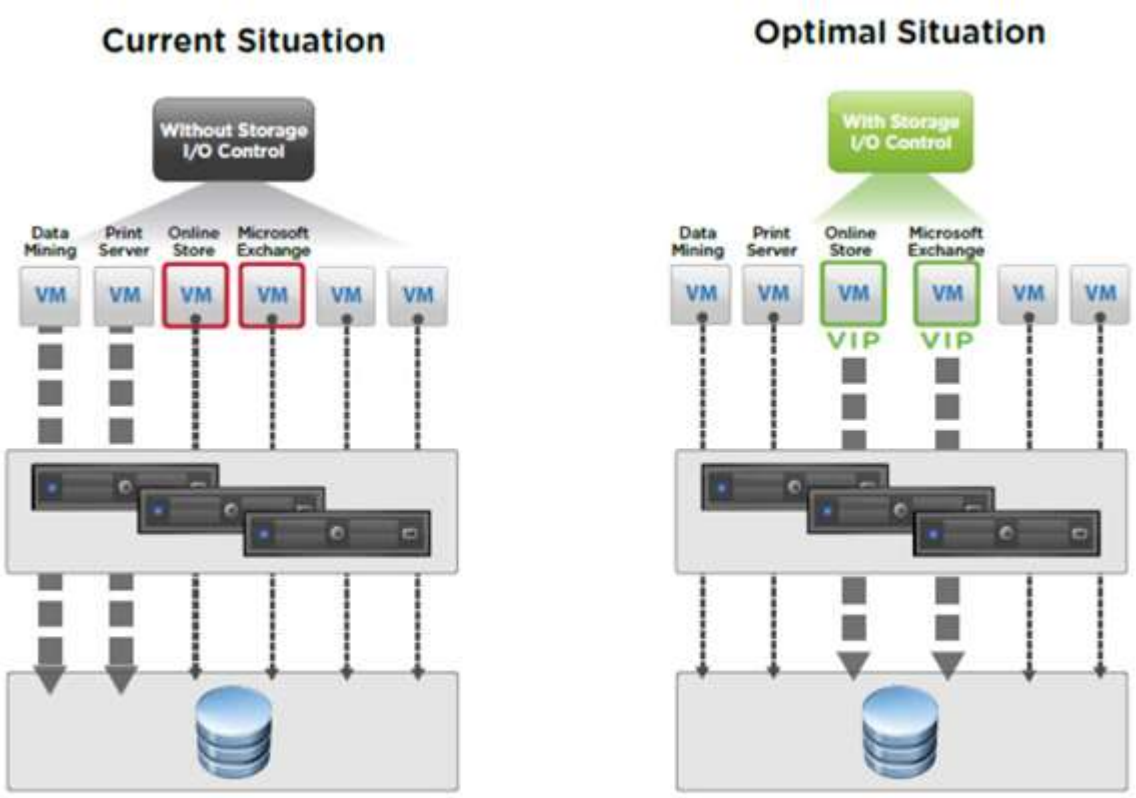
VCP6.5-DCV Objective 3.5 – Set up and Configure Storage I/O Control (SIOC)

Describe the benefits of SIOC

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

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

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



Quote from VMware:

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

Few limitations and requirements:

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

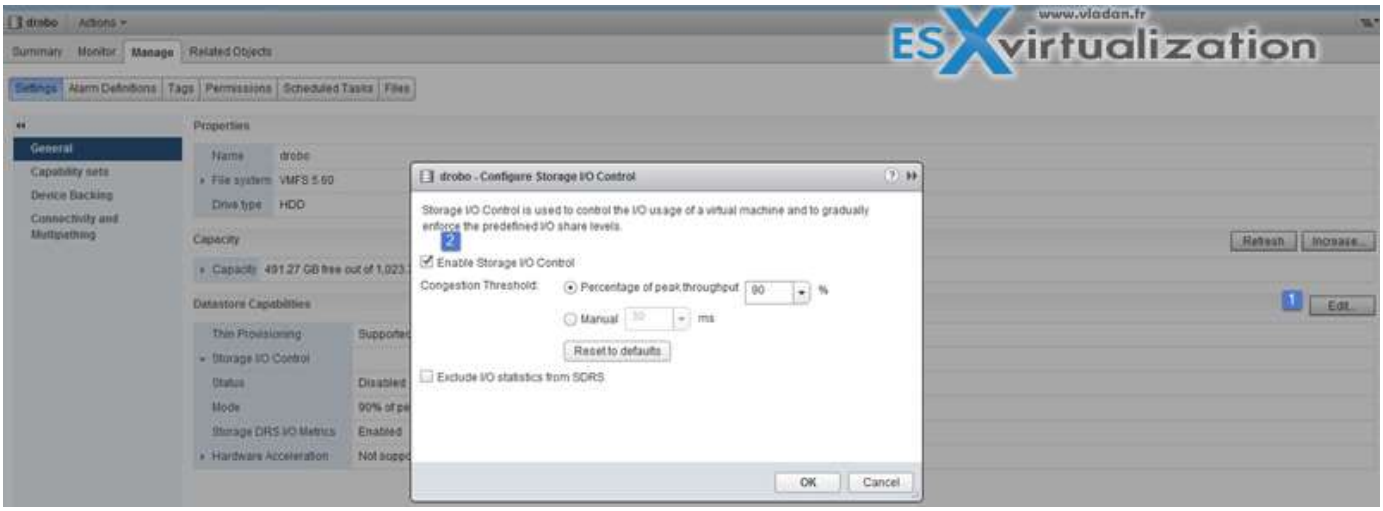
Activate at the datastore level via vSphere Client or vSphere Web client.

ENABLE AND CONFIGURE SIOC

Configuring Storage I/O Control is a two-step process.

1. Enable Storage I/O Control for the datastore.

In the **vSphere Client** > **select a datastore** > **Configuration** tab > **Properties** > Storage I/O Control, select the **Enabled check box**.



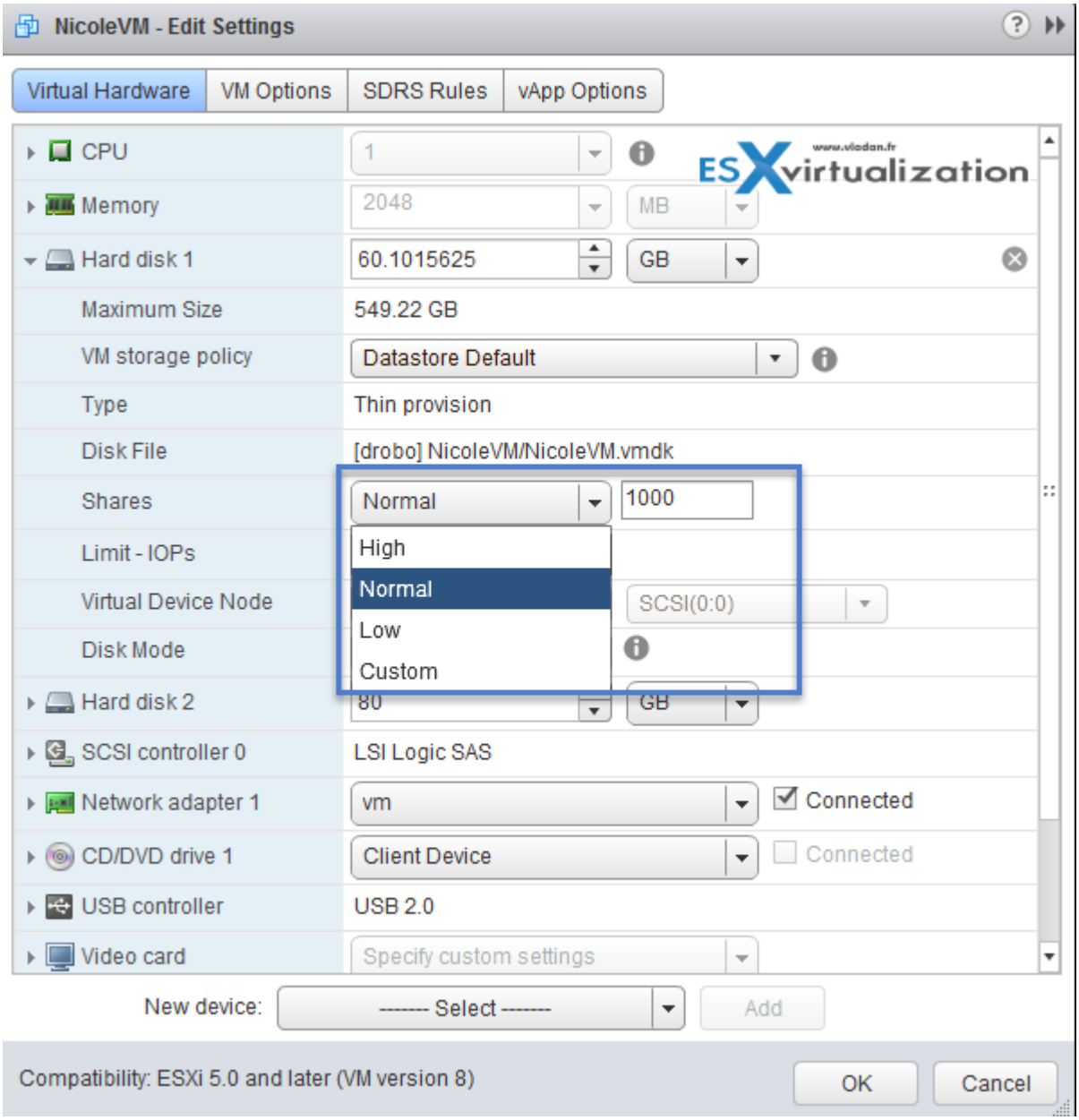
The advanced settings - Threshold - default value there. Check if the value is 30ms.

2. Set the **number of storage I/O shares** and an **upper limit of I/O operations** per second (IOPS) allowed for each virtual machine. Those settings are **per-VMDK** so you could possibly prioritize (or limit) the virtual disk where your important production DB sits!

Set the threshold. The more the VM is important, the greater the number... You can use the drop-down or the **custom** and enter your value...

- **Shares** - select relative amount of shares (low, normal, high or custom)
- **Limits** - enter the upper limit of storage resources to allocate to your VM (to your VMDK).

IOPS are the number of I/O operations per second. By default, IOPS are unlimited. You select Low (500), Normal (1000), or High (2000), or you can select Custom to enter a user-defined number of shares.



In case you're getting an error on activating SIOC this can be due to 2 reasons:

- Not having proper licensing - VMware vSphere **Enterprise Plus is required**. Yes, Storage I/O Control (SIOC) requires Enterprise Plus licensing. Without this license, the option to enable **SIOC is grayed out.**
- Check that the host is installed with ESXi 4.1 or higher.

TIP: What's the difference between vSphere Standard and Enterprise Plus.

If you select a storage policy, do not manually configure Shares and Limit – IOPS.

CONFIGURE/MANAGE SIOC

Covered above.

VCP6.5-DCV OBJECTIVE 3.5: MONITOR SIOC

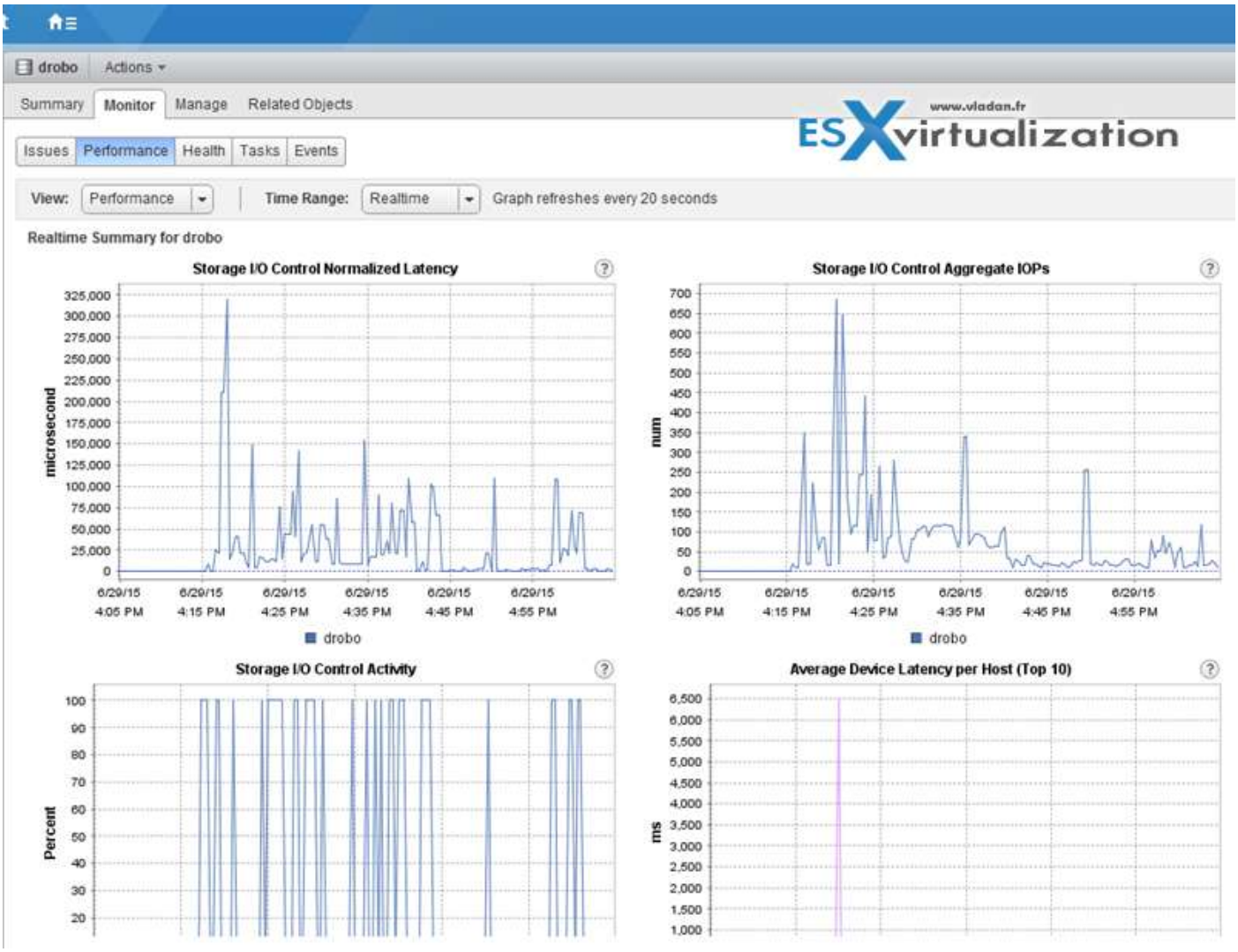
There is a Performance TAB to monitor Storage I/O.

Datastore performance charts allow monitoring:

- Average latency and aggregated IOPS on the datastore.
- Latency among hosts n Queue depth among hosts.
- Read/write IOPS among hosts.
- Read/write latency among virtual machine disks n Read/write IOPS among virtual machine disks.

WHERE?

vSphere Web client > **Datastore** > **Monitor** tab > **Performance** tab > **View** drop-down menu > select **Performance**.



The datastore Performance tab is used to monitor how Storage I/O Control handles the I/O workloads of the virtual machines accessing a datastore based on their shares.

DATASTORE PERFORMANCE CHARTS ALLOW YOU TO MONITOR:

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

Differentiate between SIOC and Dynamic Queue Depth Throttling features

Dynamic Queue depth throttling aka "Adaptive Queue Depth", is able to adjust the LUN queue depth. The algorithm which is used kicks in when storage I/O congestion returns **QUEUE FULL** or **BUSY** status codes. When these codes are received, the queue depth is **cut in half**.

Storage I/O Control uses proportional shares when there is congestion to allow for a proportional amount of I/Os. Much in the same way share values can be assigned to CPU or RAM within DRS resource groups.

Determine a proper use case for SIOC

First, as I already invoked, make sure that you have Enterprise Plus license. The SIOC can be configured making sure that all VMs get a correct allocation of storage resources. With SIOC enabled on a datastore, you prevent the other VMs from "noisy neighbor" situation where a single VM takes all the resources.

The device's latency is monitored. If latency is higher than configured values, SIOC kicks in and reduces the latency by throttling back VMs that are exceeding their consumption of IOPS.

VCP6.5-DCV Objective 3.5: Compare and contrast the effects of I/O contention in environments with and without SIOC

With SIOC enabled, no VM can take over the datastore's resources by exhausting them. With SIOC, reservations, shares and limits, you can control the storage IO on the datastore. Without SIOC you can use shares, limits, but you can't control the over-all datastore performance because you don't have a hand on the threshold value (30ms by default).

Understand SIOC metrics for Datastore Clusters and Storage DRS

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

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

Important to know as well, that SIOC isn't available for VMware vSAN datastores (as of vSAN 6.6.1). This is an important fact as the only way to limit the VM's consumption on vSAN datastore is through VM storage policy. (there is an option to enter IOPS limit per object).

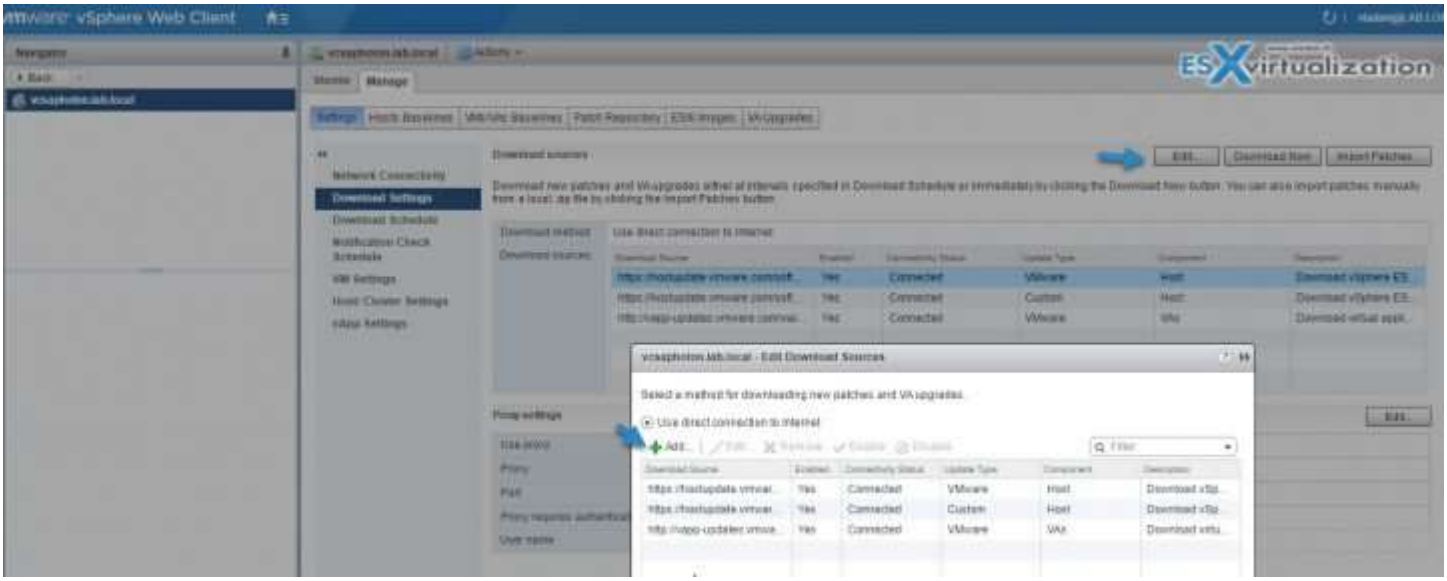
VM storage policy within vSAN cluster is able to define IOPS limit for a disk. IOPS is calculated as the number of I/Os using weighted size. By default, the system is using a base size of 32KB, then a 64KB I/O will represent 2 I/O.

VCP6.5-DCV Objective 4.1 - Perform ESXi Host and Virtual Machine Upgrades

Configure download source(s)

You can configure the Update Manager server to download patches and extensions for ESXi hosts or upgrades for virtual appliances from:

- Internet.
- Shared repository of UMDS data.
- Manual import of ZIP file for ESXi upgrade too.



With VMware Update Manager (VUM) it's possible to import VMware patches, but also third-party patches. You can do so by importing those manually from a ZIP file (offline bundle). Import of offline bundles is supported only for hosts that are running ESXi 5.0 and later.

You download the offline bundle ZIP files from the Internet or copy them from a media drive, and save them on a local or a shared network drive. You can import the patches or extensions to the VUM patch repository later. You can download offline bundles from the VMware Web site or from the Web sites of third-party vendors.

Offline bundles contain one metadata.zip file, one or more VIB files, and optionally two .xml files, index.xml and vendor-index.xml. When you import an offline bundle to the VUM patch repository, VUM extracts it and checks whether the metadata.zip file has already been imported.

If the metadata.zip file has never been imported, VUM performs sanity testing and imports the files successfully. After you confirm the import, VUM saves the files into the Update Manager database and copies the metadata.zip file, the VIBs, and the .xml files, if available, into the VUM patch repository.

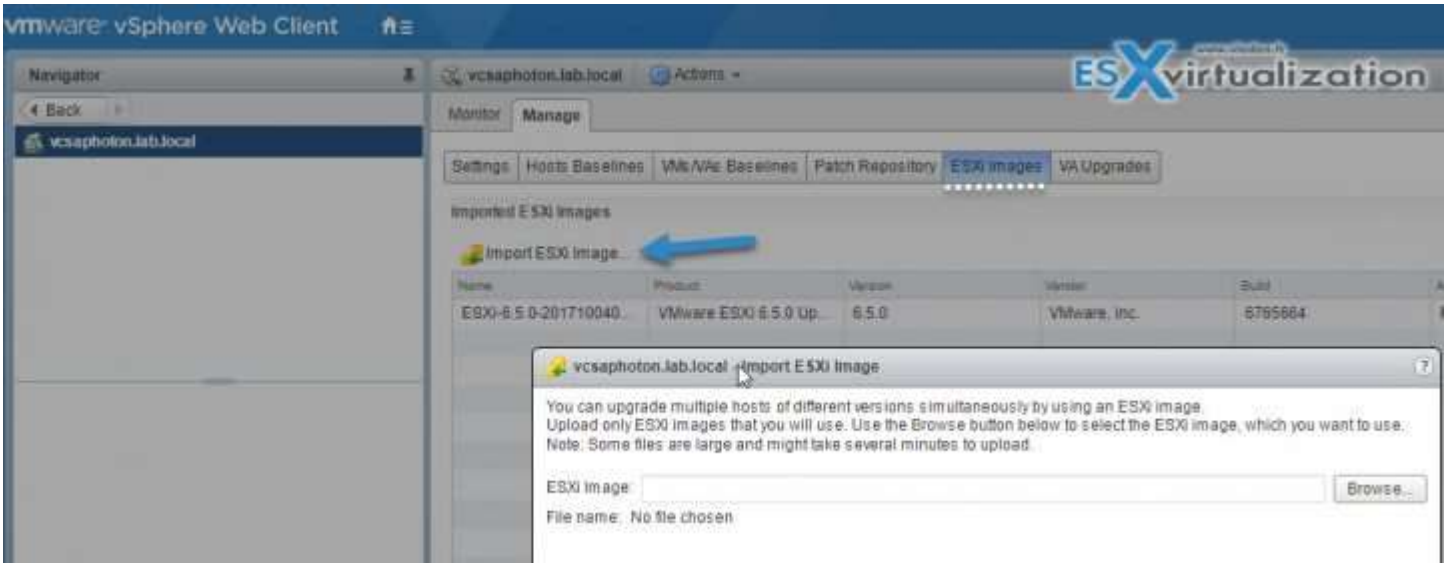
Set up UMDS to set up download repository

VMware VUM supports both HTTP and HTTPS URL addresses. Use HTTPS URL addresses, so that the data is downloaded securely. The URL addresses that you add must be complete and contain the index.xml file, which lists the vendor and the vendor index.

Import ESXi images

It's possible to upgrade the hosts in your environment to ESXi 6.5 by using **host upgrade baselines**. To create a host upgrade baseline, you must first upload at least one ESXi 6.5 .iso image to the Update Manager repository.

With VUM version 6.5 you can upgrade hosts that are running ESXi 5.5 or ESXi 6.0 to ESXi 6.5. Host upgrades to ESXi 5.0, ESXi 5.1, ESXi 5.5, or ESXi 6.0 are not supported.



You can create custom ESXi images that contain third-party VIBs by using vSphere ESXi Image Builder.

- Tip: How to create a custom ESXi 6.5 ISO with VMware Image Builder GUI
- Tip: How To Create VMware ESXi ISO With Latest Patches
- Tip: How to upgrade an ESXi 6.0 to ESXi 6.5 via VMware Update Manager

Create Baselines and/or Baseline groups

First we'll talk about what are baselines and baseline groups. Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades, and can be classified as patch, extension, or upgrade baselines. Baseline groups are assembled from existing baselines.

TIP: There are differences between host baselines and VM baselines.

- Host baseline groups can contain a single upgrade baseline, and various patch and extension baselines.
- Virtual machine and virtual appliance baseline groups can contain up to three upgrade baselines: one VMware Tools upgrade baseline, one virtual machine hardware upgrade baseline, and one virtual appliance upgrade baseline.

When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines and baseline groups to determine their level of compliance.

VMware VUM has two predefined patch baselines and three predefined upgrade baselines. **You cannot edit or delete the predefined virtual machine and virtual appliance upgrade baselines**.

You can use the predefined baselines, or create patch, extension, and upgrade baselines that meet your criteria. Baselines you create, and predefined baselines, can be combined in baseline groups. For more information about creating and managing baselines and baseline groups.

Baseline Types - VUM supports different types of baselines that you can use when scanning and remediating objects in your inventory.

Update Manager Default Baselines - Update Manager includes default baselines that you can use to scan any virtual machine, virtual appliance, or host to determine whether the hosts in your environment are updated with the latest patches, or whether the virtual appliances and virtual machines are upgraded to the latest version.

Baseline Groups - Baseline groups can contain patch, extension, and upgrade baselines. The baselines that you add to a baseline group must be non-conflicting.

ATTACH BASELINES TO VSPHERE OBJECTS

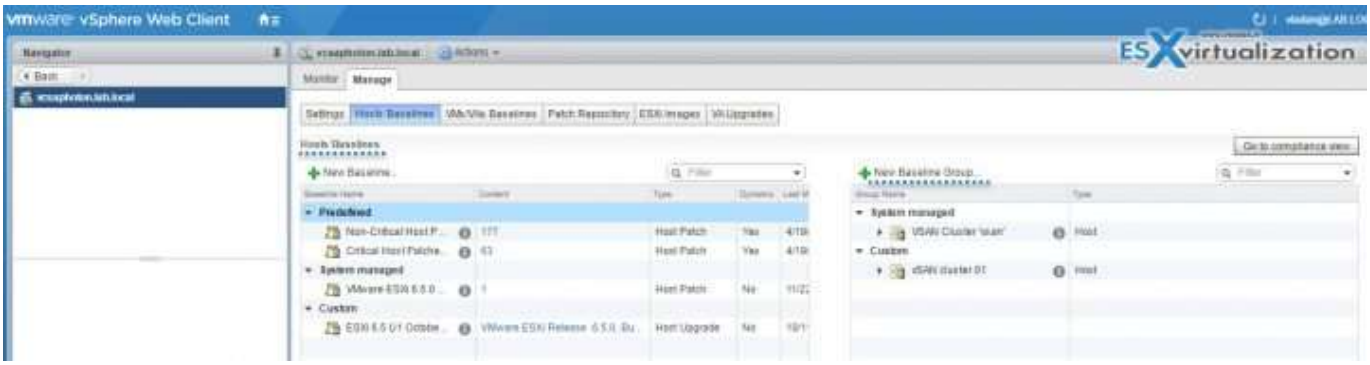


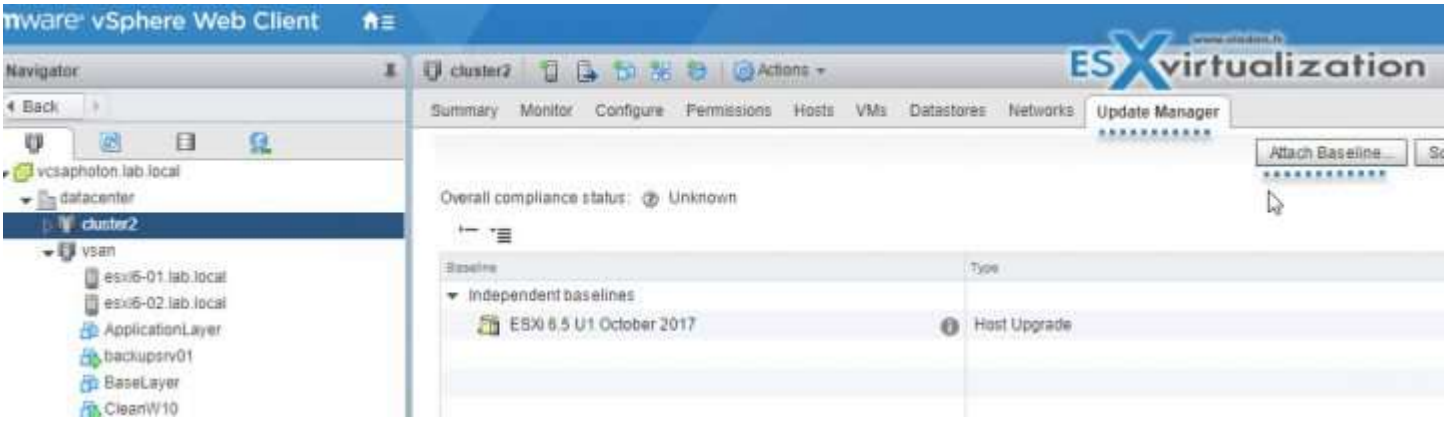
Figure 1: Host Baselines and baseline groups

In order to see a compliance information (whether the host needs to be patched or not), you need to first attach existing baselines and baseline groups to the objects within your inventory, which needs to be scanned.

You'll need certain privilege for this: **VMware vSphere Update Manager > Manage Baselines > Attach Baseline**.

How?

Select the type of object in the vSphere Web Client object navigator. (ex Cluster) > go to the **Update manager TAB** > **Attach baseline or baseline group** > **select baseline to attach** to the selected object.



Scan vSphere objects

When you're scanning objects (VMs, hosts, clusters), those are compared to patches, extensions, and upgrades included in the attached baselines and baseline groups.

You can configure VUM to scan virtual machines, virtual appliances, and ESXi hosts by manually initiating or scheduling scans to generate compliance information. To generate compliance information and view scan results, you must attach baselines and baseline groups to the objects you scan.

You can scan vSphere objects from the Update Manager Client Compliance view

Stage Patches and Extensions

Staging is a process where you "push" patches and extensions from VUM to the ESXi host. The patches are stored at the ESXi host and wait there to be deployed. It "prepares" the patches at their destination so the remediation process is then faster. It's clever as the maintenance window can be shortened.

To stage patches or extensions to hosts, first, attach a patch or extension baseline or a baseline group containing patches and extensions to the host.

Requirements: Stage Patches and Extensions privilege.

Obsolete patches - VMware VUM can stage only patches that it can install in a "**subsequent remediation process**", after a scan of ESXi host. If a patch is obsoleted by patches in the same selected patch set, the obsoleted patch is not staged.

Conflicts - If a patch is in conflict with the patches in VUM patch repository and is not in conflict with the host, after a scan, VUM will report this patch as a **conflicting one**. You can stage the patch to the host and after the stage operation, Update Manager reports this patch as staged.

Prescan and Postscan - VUM executes prescan and postscan operations to be able to update the compliance state of the baseline.

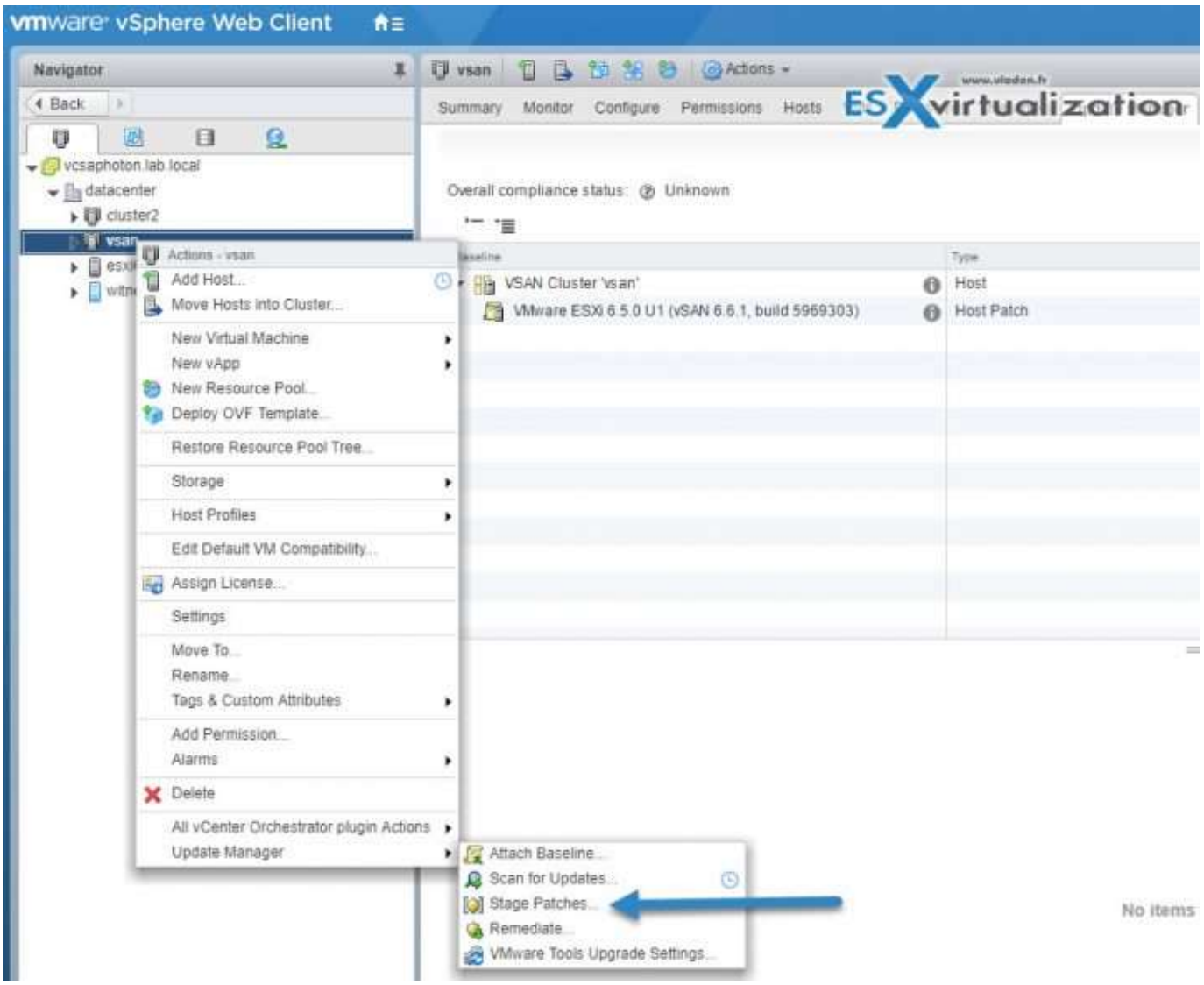
After Staging - Remediation

When patches or extensions are staged to your hosts, you can remediate the hosts against all staged patches or extensions.

After Remediation, all staged patches or extensions **are deleted by the hosts** from its cache.

WHERE?

vSphere Web Client > Select **Home** > **Hosts and Clusters** > **Right-click a datacenter**, a cluster, or a host, and select **Update Manager** > **Stage Patches**.



The Stage Patches wizard opens.

Select the patch and extension baselines to stage on the **Baseline Selection page of the Stage wizard > select hosts > Next. > Review > Finish.**

You can also deselect patches and(or) extensions to exclude from the stage operation. It's also possible to search within the list of patches and extensions, enter text in the text box on the right hand side.

REMEDIATE AN OBJECT

Remediation can be manual or scheduled. You can remediate VMs, or virtual appliances together if they are inside a container (folder, datacenter or vApp). If you attach a baseline group, it can contain both a virtual machine and virtual appliance baselines. The virtual machine baselines apply to virtual machines only, and the virtual appliance baselines apply to virtual appliances only.

During remediation, virtual appliances must be able to connect to the Update Manager server. You can also remediate templates by using VUM.

VMware tools can be upgraded (updated) as a part of the process, but a restart is necessary.

VUM present in vSphere 6.0 is able to remediate hosts of version ESXi 5.x against offline bundles that has been manually imported.

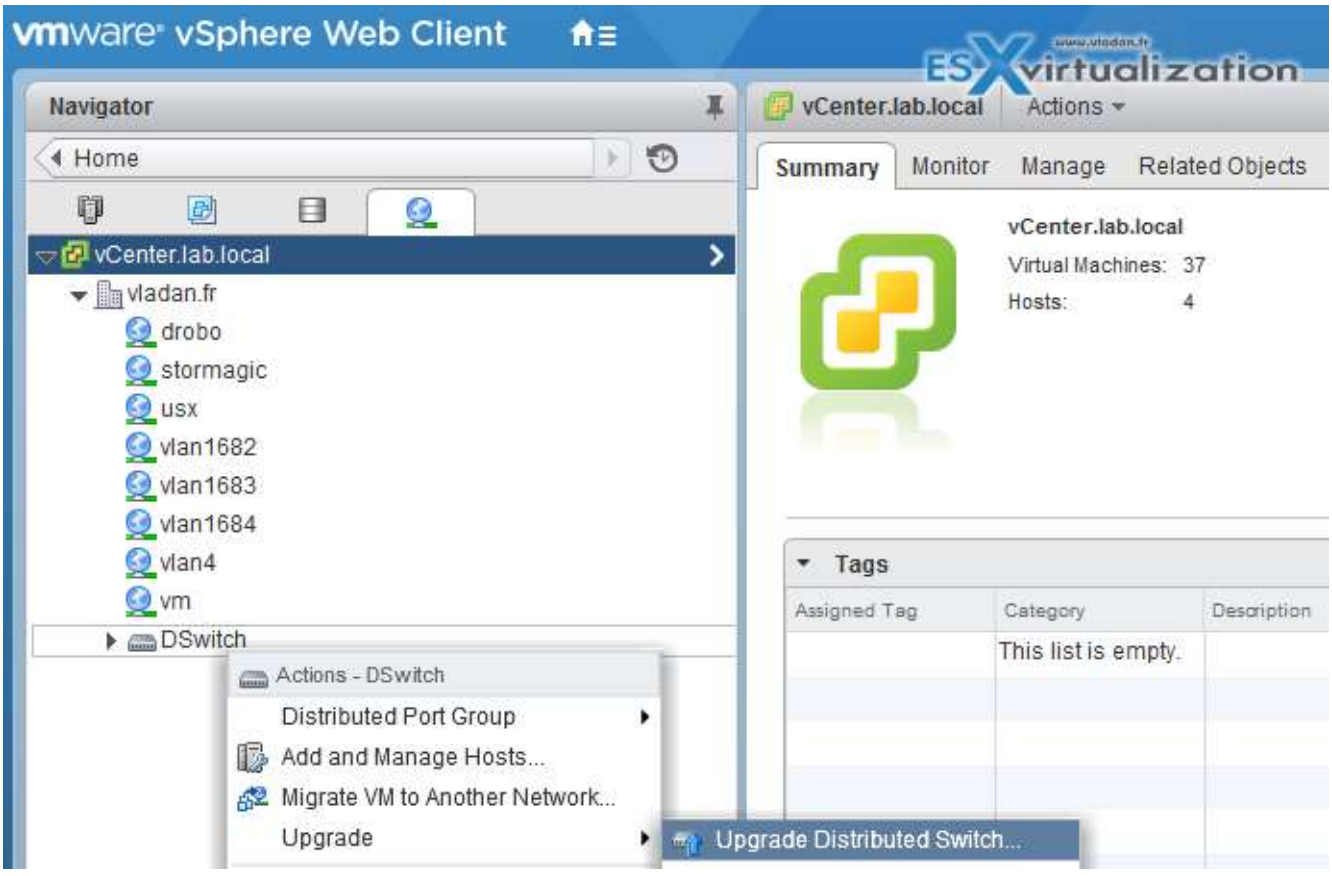
UPGRADE A VSPHERE DISTRIBUTED SWITCH

The upgrade from 5.x to 6.0 or 6.5 is not reversible.

WHERE?

vSphere Web client > Networking > Right-click the distributed switch and select > Upgrade > Upgrade Distributed Switch

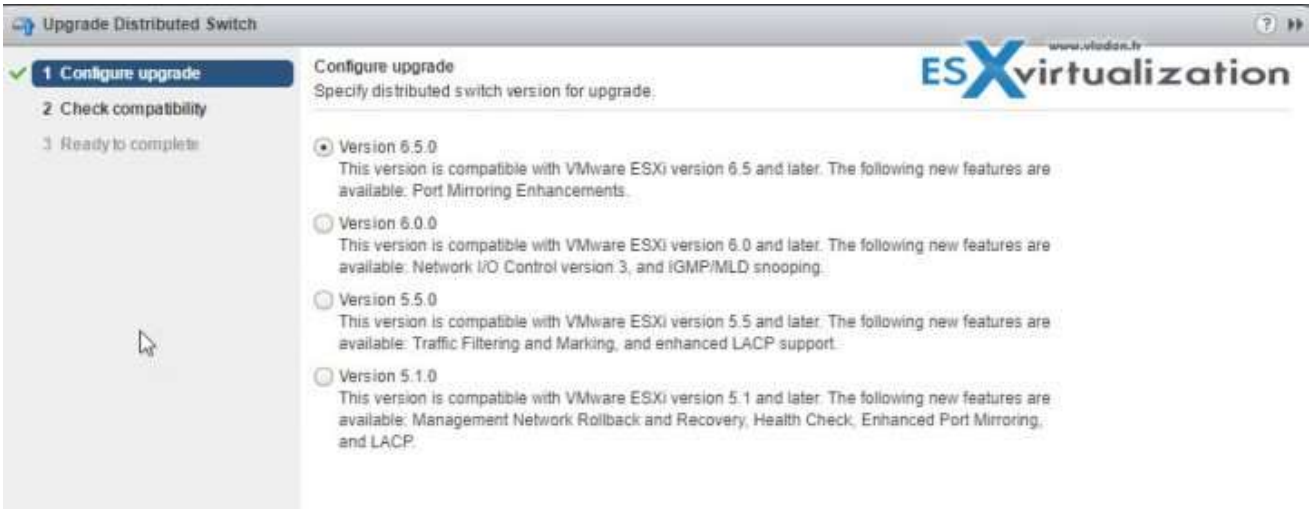
It's non-disruptive operation, so no downtime.



Version 6.0.0 - Compatible with ESXi version 6.0 and later.

Version 5.5.0 - Compatible with ESXi version 5.5 and later. Features released with later vSphere Distributed Switch versions are not supported.

Version 5.1.0 - Compatible with ESXi version 5.1 and later. Features released with later vSphere Distributed Switch versions are not supported.



UPGRADE VMWARE TOOLS

VMware tools can be upgraded automatically or manually. It's possible to configure VMs to check latest versions of VMware Tools too at power ON.

Within the Guest OS, there is a status bar (Windows) which shows you whether a new version is available. The yellow (caution) icon shows up when a VMware Tools upgrade is available.

To install a VMware Tools upgrade: Same as clean install.

Automatic configuration of VM tools installation/upgrade - The automatic upgrade will trigger when you power off or restart the virtual machine. The status bar displays the message "Installing VMware Tools".

The steps:

Virtual Machines TAB > Select VM(s) Update Manager TAB >

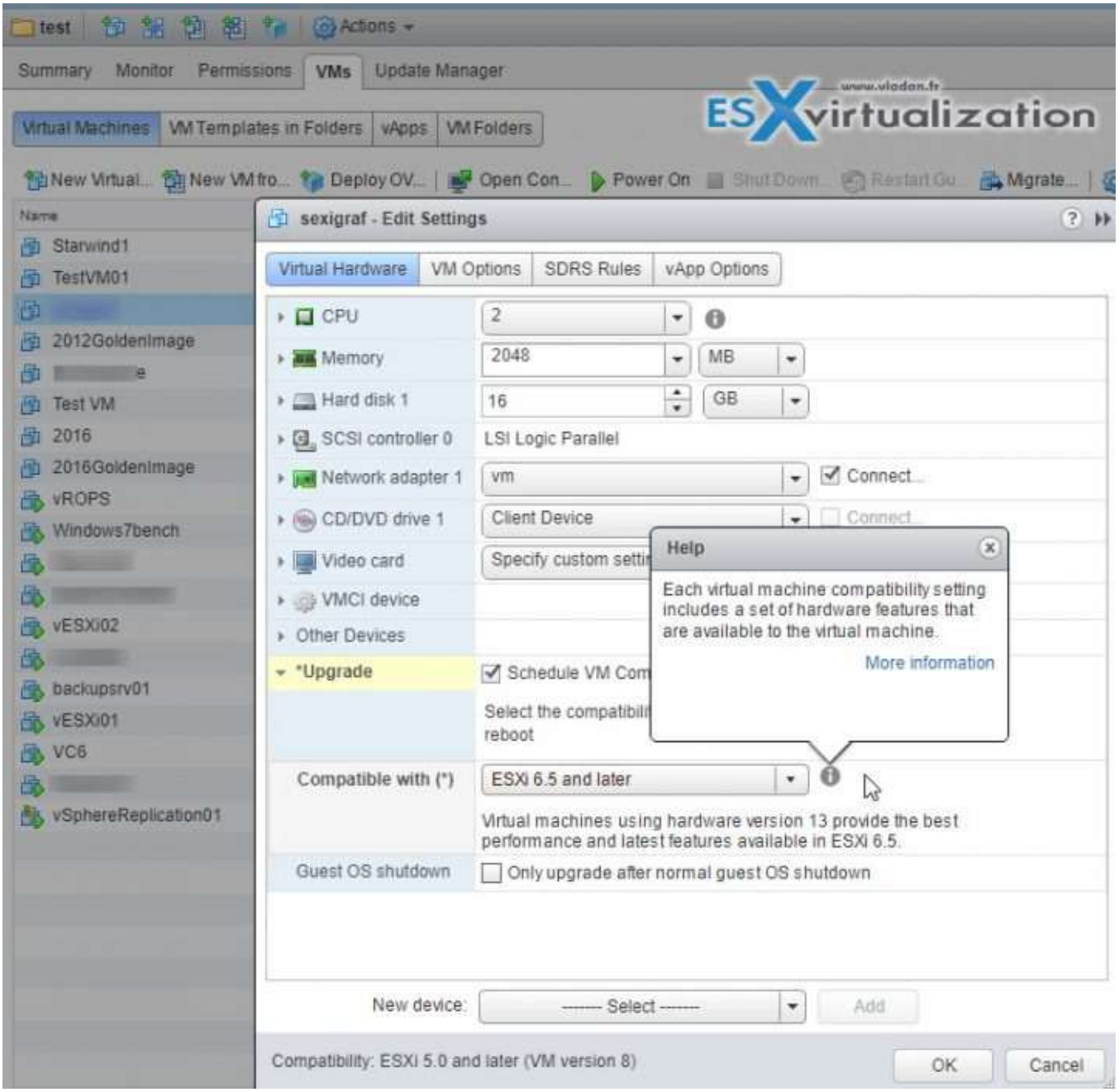
VMware highly recommends that you upgrade to the most updated version of the VMware Tools.

Some features in a particular release of a VMware product might depend on installing or upgrading to the version of VMware Tools included in that release. Upgrading to the latest version of VM tools will assure the particular feature to work.

UPGRADE VIRTUAL MACHINE HARDWARE

You can upgrade the Virtual machine hardware (VMX) to the latest version of ESXi in use.

vSphere Web client > Power Off VM > Right click VM > Options > Upgrade Virtual Hardware.



Or,

In the **vSphere Web Client** > **right click VM** > **Compatibility** > **Upgrade VM Compatibility**.

Then, the VM's virtual hardware is upgraded to the **latest supported version**. (You have no choice between version, like in the previous example.)

UPGRADE AN ESXI HOST USING VCENTER UPDATE MANAGER

During host scan, the host is compared to the VIBs from the upgrade image. The host scanned against an upgrade baseline compares the ISO image referenced in the baseline. If the ISO is the same version as the target host, VUM shows "Compliant" (or Non-compliant if it's not).

You can also use an ISO 6.5 image in an upgrade operation of an ESXi 6.5 host. The remediation process of ESXi 6.5 host by using ESXi 6.5 image with additional VIBs is equivalent to a patching process. Because the upgrade image of the same version as the target host, with completing the upgrade operation the additional VIBs are added to the target host.

Stage multiple ESXi Host upgrade

Within clustered VMware environments, the patching process used by VUM does the remediation one-by-one. Sequentially. Each host goes to maintenance mode > remediation > exit maintenance mode > next host. Etc.

If a host in a DRS enabled cluster runs a virtual machine on which Update Manager or vCenter Server are installed, DRS first attempts to migrate the virtual machine running vCenter Server or Update Manager to another host so that the remediation succeeds. In case the virtual machine cannot be migrated to another host, the remediation fails for the host, but the process does not stop.

Requirements: Disable DPM and HA admission control. Also FT disable, you should.

You can remediate in parallel too:

When you remediate a cluster of hosts in parallel, VUM does the remediate actions on multiple hosts at the same time. During parallel remediation, if VUM finds an error when remediating a host, **it ignores the host** and the remediation process continues for the other hosts in the cluster. VUM continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.

VUM remediates hosts that are part of a vSAN cluster sequentially even if you select the option to remediate them in parallel. The reason is that by design only one host from a vSAN cluster can be in a maintenance mode at any time.

For multiple clusters under a datacenter, the remediation processes run in parallel. If the remediation process fails for one of the clusters within a datacenter, the remaining clusters are still remediated.

Align appropriate Baselines with target inventory objects

VUM baselines are hosts baselines, virtual machine baselines, and virtual appliance baselines. In order to upgrade objects within your environment, it's possible to use:

- Predefines baselines.
- System-managed baselines.
- Custom baselines that you create.

Depending on the purpose for which you want to use them, host baselines can contain a collection of one or more patches, extensions, or upgrades. Therefore host baselines are upgrade, extension, or patch baselines. To update or upgrade your hosts you can use the Update Manager default baselines, or custom baselines that you create.

The VMs/VAs baselines are predefined. You cannot create custom VMs/VAs baselines.

The default baselines are the predefined and system managed baselines - VUM displays system managed baselines that are generated by vSAN. These baselines appear by default when you use vSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. If your vSphere environment does not contain any vSAN clusters, no system managed baselines are created.

The system managed baselines automatically update their content periodically, which requires Update Manager to have constant access to the Internet. The vSAN system baselines are typically refreshed every 24 hours.

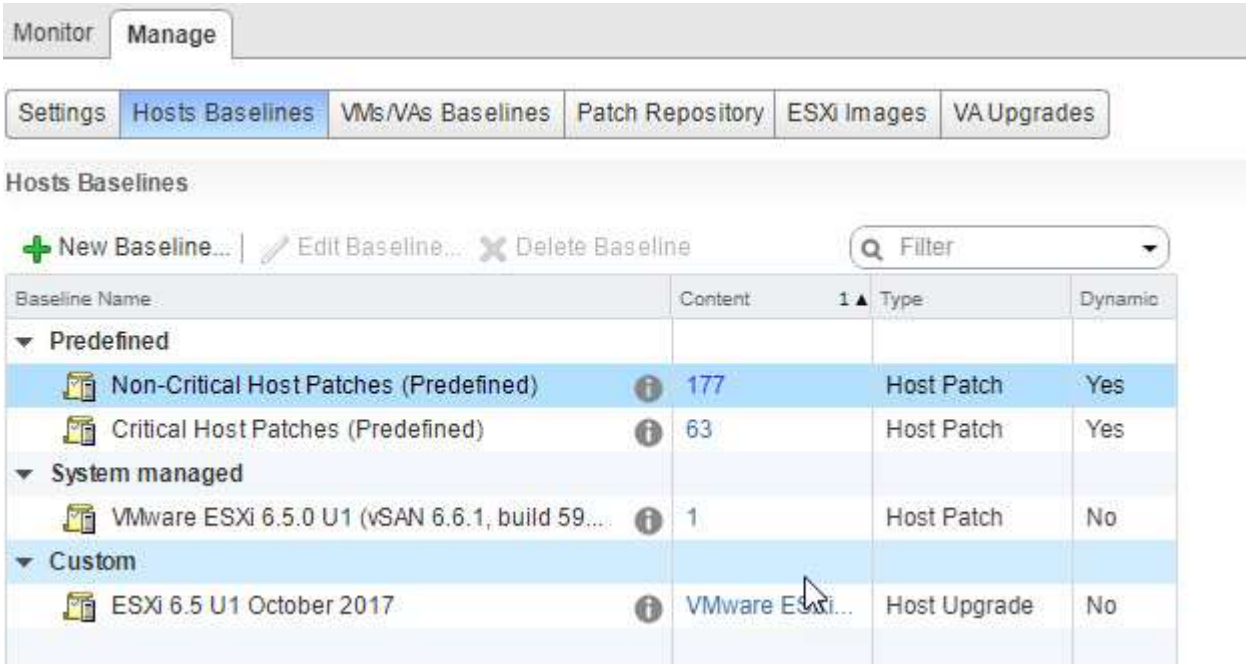
You can use the system managed baselines to upgrade your vSAN clusters to recommended critical patches, drivers, updates or latest supported ESXi host version for vSAN.

Predefined Baselines - Predefined baselines cannot be edited or deleted. The only actions are:

- Attach
- Detach

them to(from) the respective inventory objects. Host Baselines tab in **VUM Admin view** > **predefined baselines**:

- **Critical Host Patches** (Predefined) - Checks ESXi hosts for compliance with all critical patches.
- **Non-Critical Host Patches** (Predefined) - Checks ESXi hosts for compliance with all optional patches.



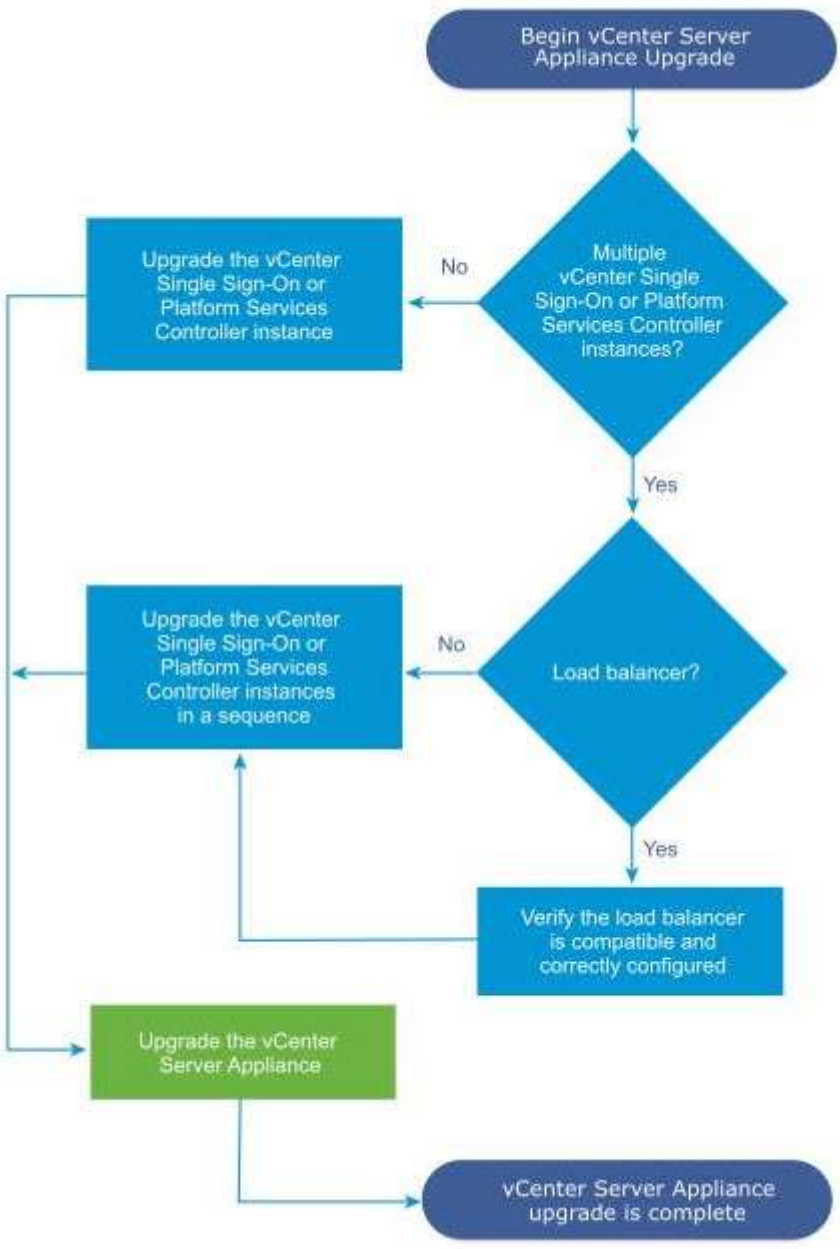
Under the VMs/VAs Baselines tab Update Manager Admin view, you can see the following predefined baselines:

- **VMware Tools Upgrade to Match Host** (Predefined) - Checks virtual machines for compliance with the latest VM Tools version on the host. VUM supports upgrading of VMware Tools for virtual machines on hosts that are running ESXi5.5.x and later.
- **VM Hardware Upgrade to Match Host** (Predefined) - Checks the virtual hardware of a virtual machine for compliance with the latest version supported by the host. VUM supports upgrading to virtual hardware version vmx-13 on hosts that are running ESXi 6.5 .

- **VA Upgrade to Latest** (Predefined) - Checks virtual appliance compliance with the latest released virtual appliance version.

VCP6.5-DCV Objective 4.2 - Perform vCenter Server Upgrades (Windows)

Compare the methods of upgrading vCenter Server



The upgrade process for CLI or GUI installations:

- Deploying a new appliance of version 6.5 with temporary network configuration
- If you are upgrading VCSA, you must select a deployment size for the new appliance. You must also select a storage size for the new appliance that is suitable for the vCenter Server Appliance database.
- You'll need also specify the type of data which you want to transfer to the new appliance.

- If you are upgrading a vCSA that uses an external Update Manager instance, you must ensure that the **Migration Assistant is running on the Update Manager machine**, which facilitates the export of the Update Manager configuration and database.
- You'll need to transfer the exported data to the appliance. Be aware that **non-ephemeral distributed virtual port groups are not migrated.**
- After the upgrade, you can manually connect the new appliance to a non-ephemeral distributed virtual port group.
- If the source vCSA uses an external database, the database is migrated to the embedded PostgreSQL database of the new appliance.
- If you are upgrading a vCSA that uses an Update Manager instance (on Windows machine), the Update Manager instance is migrated to the embedded VMware vSphere Update Manager Extension of the new upgraded appliance.
- Powering off the source appliance. The new upgraded appliance assumes the network configuration of the source appliance.
- If your current appliance version is earlier than 5.5, you must upgrade to 5.5 or 6.0 before upgrading to version 6.5.

You can upgrade vCenter server (VC) on Windows and there are supported and unsupported scenarios. According to VMware vSphere 6.5 documentation, you can perform an upgrade from:

- VC 5.5 with an embedded vCenter Single Sign-On on Windows
- VC 6.0 with an embedded Platform Services Controller instance on Windows
- VC Single Sign-On (SSO) 5.5 on Windows
- PSC 6.0 on Windows
- VC 5.5 on Windows
- VC 6.0 on Windows

The vCenter Server 5.5 example upgrade paths demonstrate some common starting configurations before vCenter Server upgrade and their expected configuration outcomes after vCenter Server upgrade.

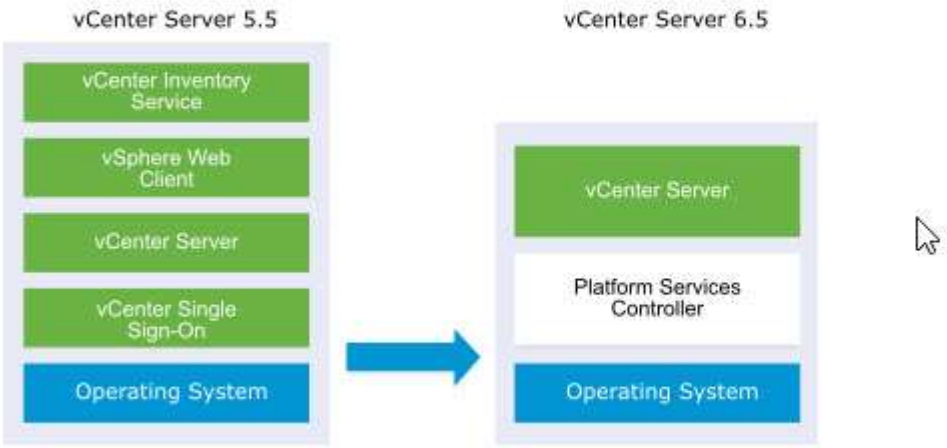
Tip: What is VMware Platform Service Controller (PSC)?

If you have a simple installation with all vCenter Server 5.5 components on the same system, the vCenter Server 6.5 software upgrades your system to vCenter Server with an embedded Platform Services Controller instance.

The software upgrades your vCenter Server common services such as vCenter Single Single-On in the Platform Services Controller instance. The rest of the vCenter Server components, such as vSphere Web Client Inventory Service, are upgraded to 6.5 as part of the vCenter Server group of services.

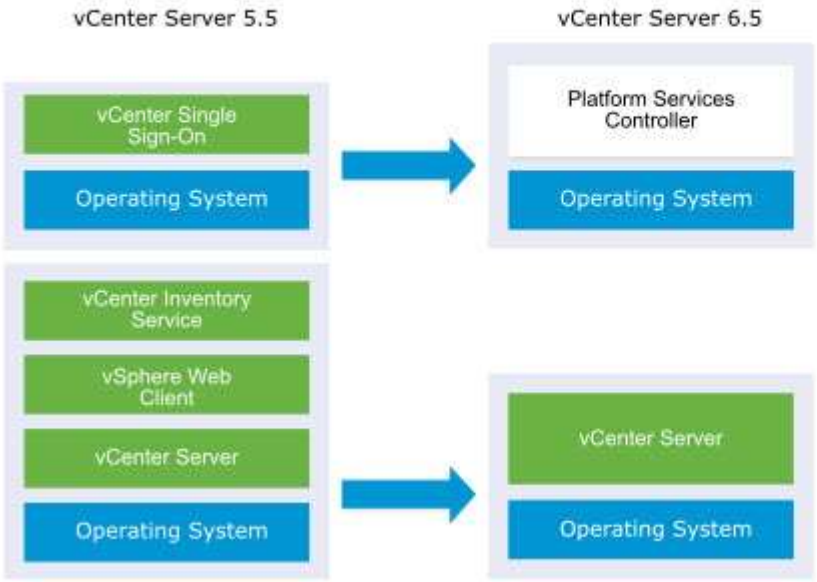
The software upgrades vCenter Server and all its services in the correct order to the same version.

vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Upgrade



Note that you cannot change your deployment type during the upgrade process.

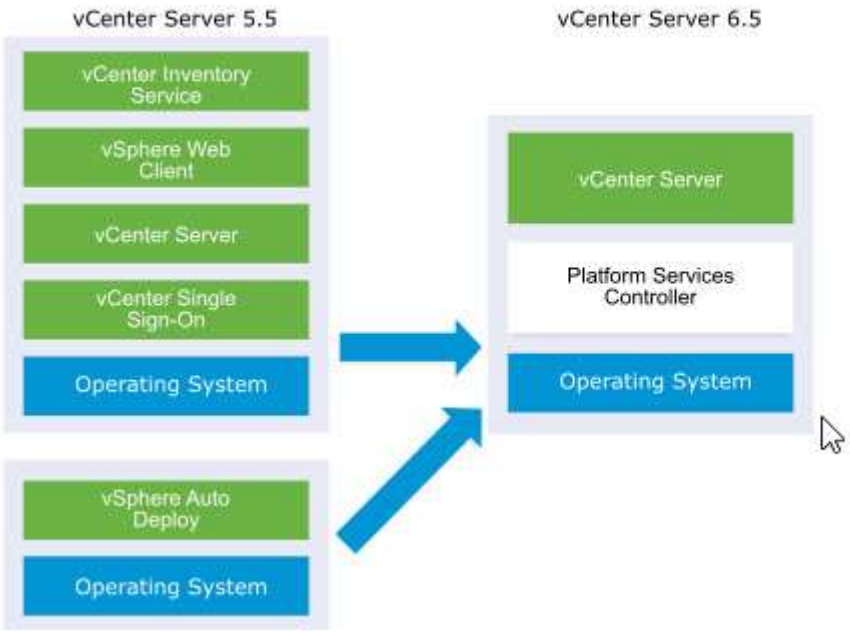
vCenter Server 5.5 with External vCenter Single Sign-On Before and After Upgrade



You should:

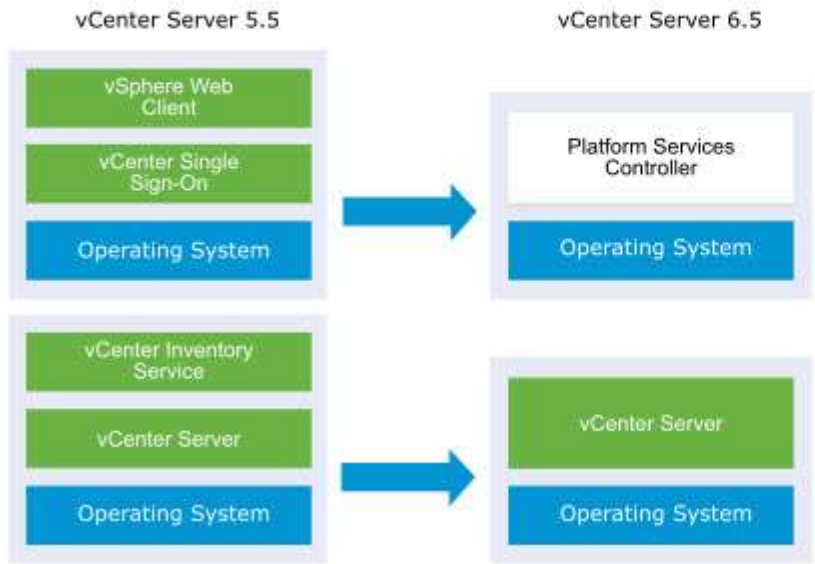
- Download and Mount the vCenter Server Appliance Installer
- Assemble the Required Information for Upgrading vCenter Server on Windows.
- Upgrade a vCenter Server 5.5 Installation with an Embedded vCenter Single Sign-On or Upgrade vCenter Single Sign-On 5.5 on Windows.

vCenter Server 5.5 with Remote vSphere Auto Deploy Server Before and After Upgrade



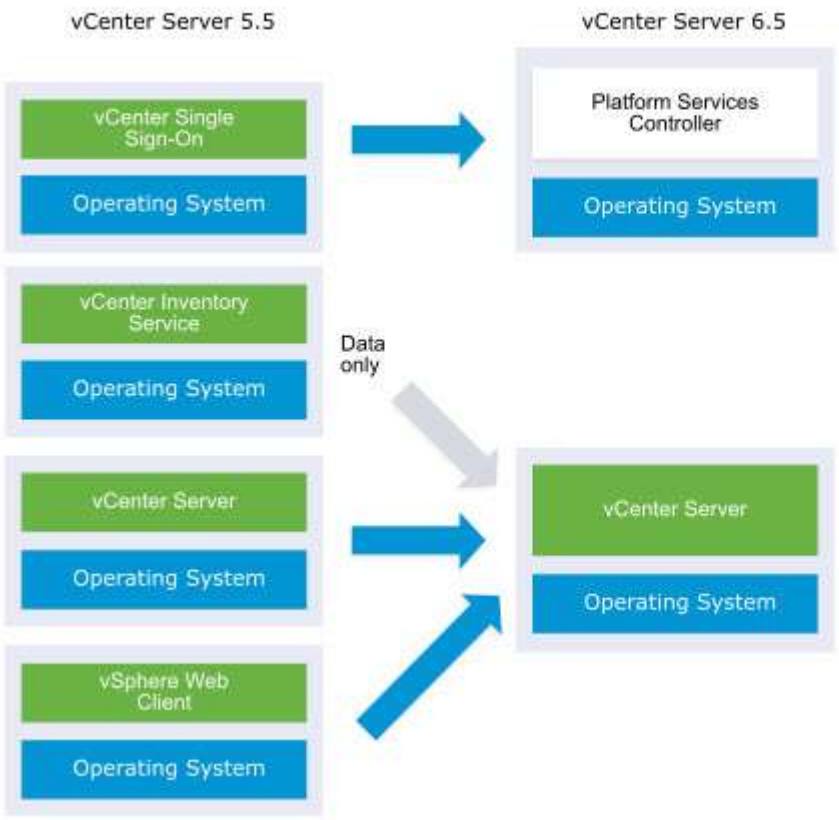
or

vCenter Server 5.5 with Remote vSphere Web Client and vCenter Signle Sign-On Before and After Upgrade



Upgrade order - you have to upgrade all PSC instances **before** upgrading vCenter Server instances.

vCenter Server 5.5 with All Remote Components Before and After Upgrade



Upgrading vCenter Server 6.0 on Windows - You upgrade a vCenter Server instance with an embedded Platform Services Controller in one step. When you upgrade a vCenter Server with an external Platform Services Controller on Windows, you upgrade the instance in two steps.

Phase1 - Upgrade the PSC instance to version 6.5.
Phase 2 - Upgrade the vCenter Server instance to version 6.5.

WHAT IS THE ORDER TO UPGRADE AND WHAT?

Upgrade all PSC instances before upgrading vCenter Server instances.

Concurrent upgrades of PSC instances are **not supported**. When upgrading multiple instances of vCenter Server that share the same vCenter Single Sign-On or PSC, you can upgrade the vCenter Server instances concurrently after first upgrading the vCenter Single Sign-On or PSC.

Mixed Platform Upgrades - When upgrading vCenter Server instances on Windows in a mixed platform environment with a Platform Services Controller 6.0 appliance, you upgrade the Platform Services Controller appliance to version 6.5 before upgrading the vCenter Server instances.

When upgrading vCenter Server Appliance instances in a mixed platform environment with a Platform Services Controller instance on Windows, you upgrade the Platform Services Controller instance before upgrading the vCenter Server Appliance instances to version 6.5.

Backup vCenter Server database, configuration, and certificate datastore

Before starting ANY upgrade, do a backup of your vCenter server.

You'll have a point-in-time to which you can restore in case something goes wrong. Whether you have "All-in-one" installation or a vCenter server with a separate PSC, you should:

- Perform Backup of vCenter Database (SQL, Oracle..., there are tools for that).
- Perform a backup of every external PSC and (or) servers in case you don't have "all-in-one" on single VM
- Do a backup of the whole VCSA appliance (via an external backup program, VDP, Veeam, Nakivo.....)

Note: You should always follow the vendor documentation on how to backup vCenter server with your backup product. It depends on your backup product.

vSphere 6.5 supports file server backup (backup configuration) of VCSA.

It's done within VCSA's Management Interface where you create a file-based backup of the vCenter Server Appliance and Platform Services Controller appliance.

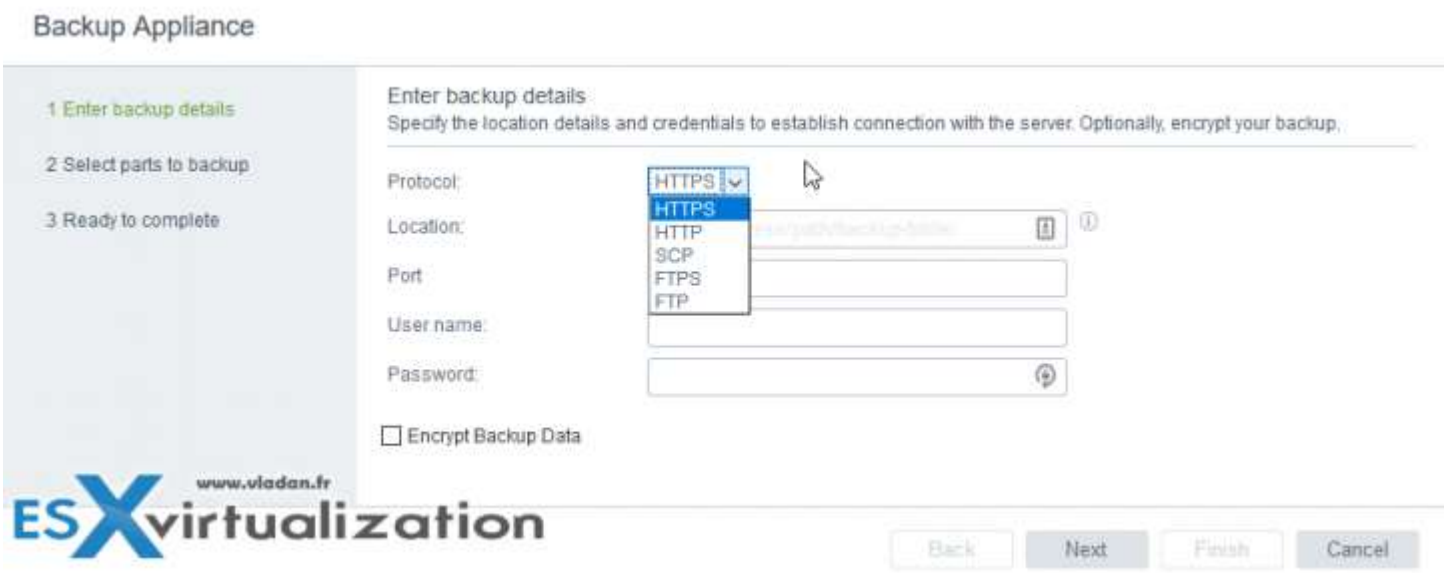
Note it's the config backup, with a historical data (or not).

After you create the backup, you can restore it by using the GUI installer of the appliance.

Tip: VMware VCSA 6.5 Backup and Restore How-To

The target can be different. You have a choice between FTP, FTPS, HTTP, HTTPS, or SCP to a remote system. The backup is not stored on the vCenter Server Appliance.

Note the option to encrypt your backup data, a simple checkbox…



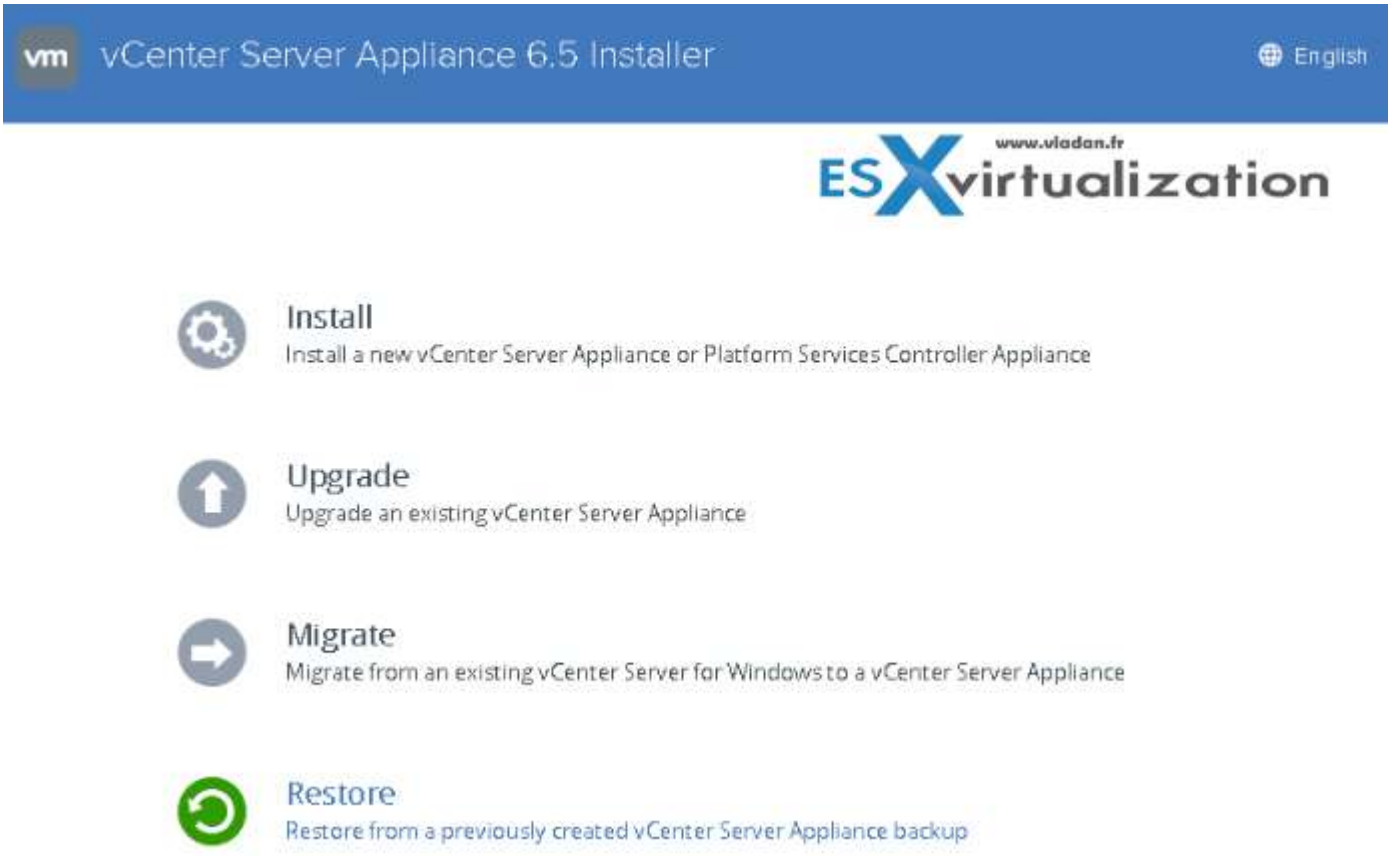
So during the restore operation, you deploy a clean VCSA (phase 1) and you restore from backup (phase 2). The vCenter Server UUID and all configuration settings are restored. The backup file is stored elsewhere, not on the VCSA itself.

If you're using vSphere Distributed switch, it is recommended to export vDS config separately. After restore of VCSA you can restore the vDS config separately.

RESTORE OPERATION

Well, from then it is very straightforward.

Launch the setup application of the VCSA 6.5 (from the ISO) and hit the Restore button > Deploy a new appliance > Accept EULA > Enter Backup details > Review backup information > Enter appliance deployment target (ESXi host). From this moment it is pretty similar to a clean deployment…



After a restore, the following configurations revert to the state when the backup was taken.

- Virtual machine resource settings
- Resource pool hierarchy and setting
- Cluster-host membership
- DRS configuration and rules

Perform update as prescribed

Check above sections.

Upgrade vCenter Server

The same. Check above sections.

Determine the upgrade compatibility of an environment

A specific software and hardware requirements must be followed before you can proceed with an upgrade.

Hardware Requirements for the vCenter Server Appliance and Platform Services Controller Appliance
- When you deploy the vCenter Server Appliance, you can select to deploy an appliance that is suitable for the size of your vSphere environment. The option that you select determines the number of CPUs and the amount of memory for the appliance. The size of the PSC appliance is the same for all environment sizes.

Storage Requirements for the vCenter Server Appliance and Platform Services Controller Appliance
- When you deploy the vCSA or PSC appliance, the ESXi host or DRS cluster on which you deploy the

appliance must meet minimum storage requirements. The required storage depends not only on the size of the vSphere environment and the storage size but also on the disk provisioning mode.

Software Requirements for the vCenter Server Appliance and Platform Services Controller Appliance - The VMware vCenter Server Appliance and Platform Services Controller appliance can be deployed on ESXi hosts 5.5 or later, or on vCenter Server instances 5.5 or later.

Determine correct order of steps to upgrade a vSphere implementation

In general, you always update external PSCs, if any, within the environment, first. We can give some guidance on what to upgrade first. Detailed VMware KB 2147289 shall be followed in order to get ALL the details:

- Any external(s) vCenter SSO(s)
- vCenter Server(s)
- vSphere Replication / VUM/vROP/ vDP
- vCloud Connector (vCC)
- ESXi hosts
- VMware tools for all the VMs within the environment

You should check the following:

- Synchronize the clocks of the virtual machines on which you plan to install vCenter server and the PSC.
- Check that the DNS name of the VM or physical server matches the actual full computer name (FQDN=fully qualified domain name).
- Check that the hostname of the VM or physical server on which you are installing or upgrading vCenter Server complies with RFC 1123 guidelines.
- Check that the system on which you are installing vCenter Server **is not** an Active Directory domain controller.
- If you plan to use a user account other than the Local System account in which to run your vCenter Server service, verify that the user account has the following permissions:
    - Member of the Administrators group
    - Log on as a service
    - Act as part of the operating system (if the user is a domain user)
- If the system that you use for your vCenter Server installation belongs to a workgroup rather than a domain, not all functionality is available to vCenter Server. If assigned to a workgroup, the vCenter Server system is not able to discover all domains and systems available on the network when using some features. Your host machine must be connected to a domain if you want to add Active Directory identity sources after the installation.
- Check that the LOCAL SERVICE account has read permission on the folder in which vCenter Server is installed and on the HKLM registry.
- Check that the connection between the virtual machine or physical server and the domain controller is working.

VCP6.5-DCV Objective 4.3 - Perform vCenter Server migration to VCSA

VCP6.5-DCV OBJECTIVE - PERFORM VCENTER SERVER MIGRATION TO VCSA

- Migrate to VCSA
- Understand the migration paths to the vCSA

VMware has a built-in tool which supports certain scenarios when you want to migrate to vCSA. You must plan ahead because, for example, it does not support migration from vCenter 6.5 on Windows to vCSA 6.5. But we'll cover all supported scenarios, with or without embedded Platform Service Controller (PSC).

Tip: What is VMware Platform Service Controller?

VCENTER SERVER MIGRATION PATHS:

(Note: Images are taken from VMware Online Documentation - link. There are more examples as well)

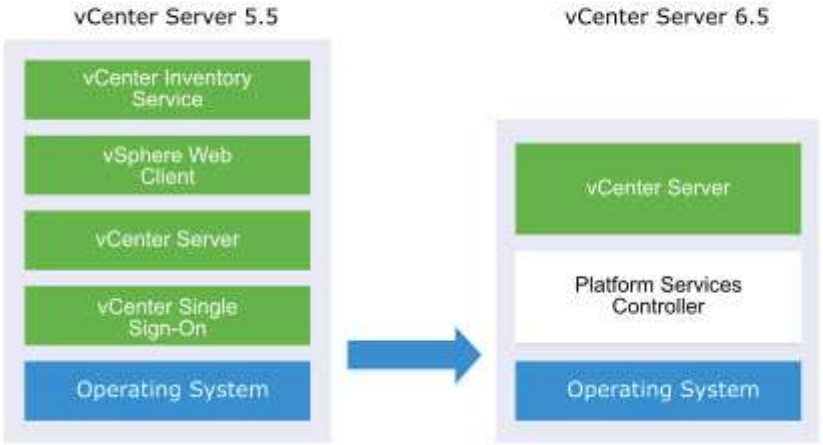
You might want to check Moving from Deprecated to a Supported vCenter topology before migration - link.

5.5 > 6.5 - You can migrate a vCenter Server version 5.5 or version 6.0 instance on Windows to a vCenter Server Appliance 6.5 deployment on a Linux-based OS.

You can migrate a vCenter Server instance with an embedded vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.5 instance with an embedded Platform Services Controller appliance.

In this case, the software migrates the vCenter Server instance and the embedded vCenter Single Sign-On instance or Platform Services Controller instance at the same time.

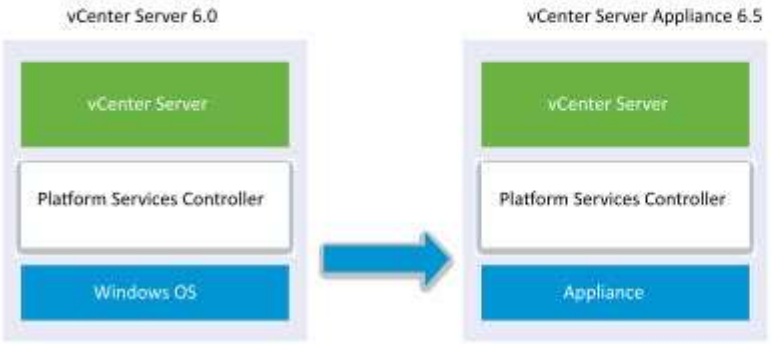
vCenter Server 5.5 with Embedded vCenter Single Sign-On Before and After Upgrade



6.0 > 6.5 - You can migrate a vCenter Server instance with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.5 instance with an external Platform Services Controller appliance.

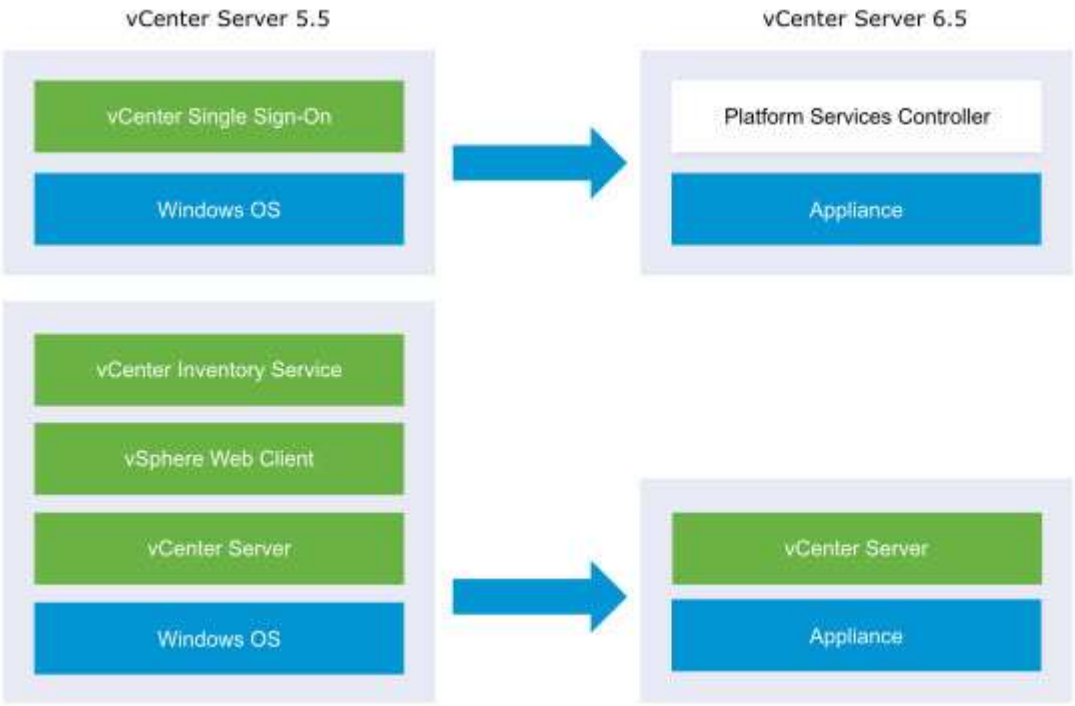
In this case, you must first migrate the external vCenter Single Sign-On instance or Platform Services Controller instance and then the vCenter Server instance.

vCenter Server 6.0.x with Embedded Platform Services Controller Installation Before and After Migration



5.5 With External PSC > vCSA with External PSC - You can migrate a vCenter Server instance with an external vCenter Single Sign-On (version 5.5) or Platform Services Controller (version 6.0) to a vCenter Server Appliance 6.5 instance with an external Platform Services Controller appliance.

In this case, you must first migrate the external vCenter Single Sign-On instance or Platform Services Controller instance and then the vCenter Server instance.



If you have multiple systems configured for high availability, vCenter Server enables you to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process.

If you have a multi-site setup configured with replication, you can use vCenter Server to incorporate your common services into an external Platform Services Controller configuration as part of your upgrade process.

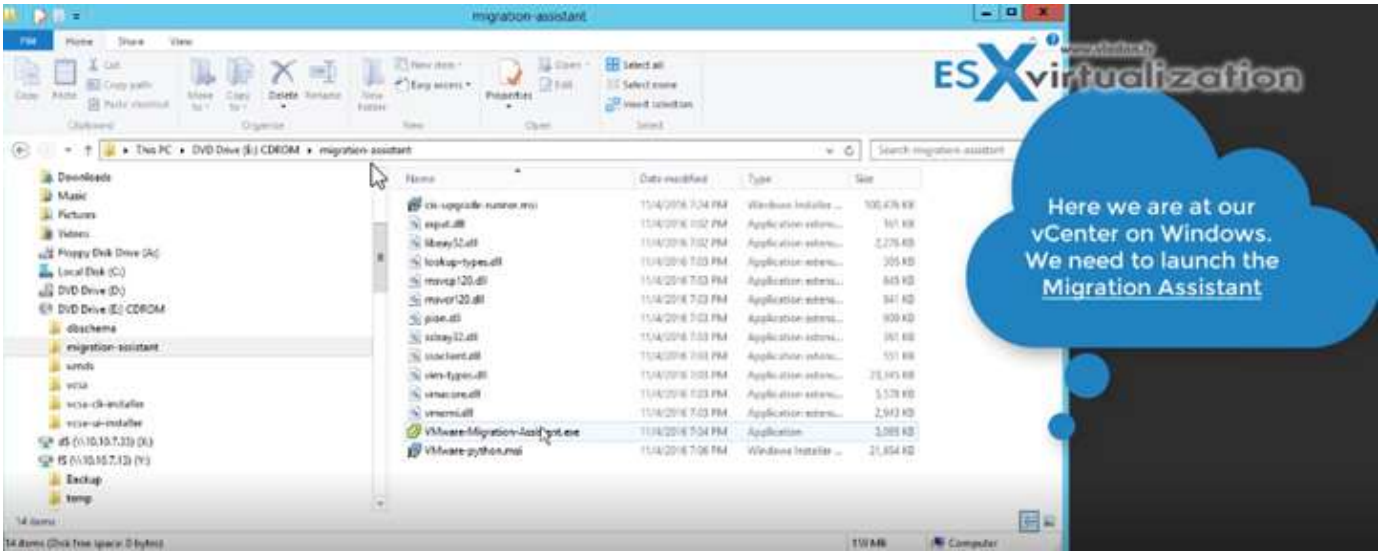
THE ACTUAL PROCESS OF MIGRATION: VCP6.5-DCV OBJECTIVE - PERFORM VCENTER SERVER MIGRATION TO VCSA

You'll need to run the migration assistant. The Migration Assistant serves two purposes:

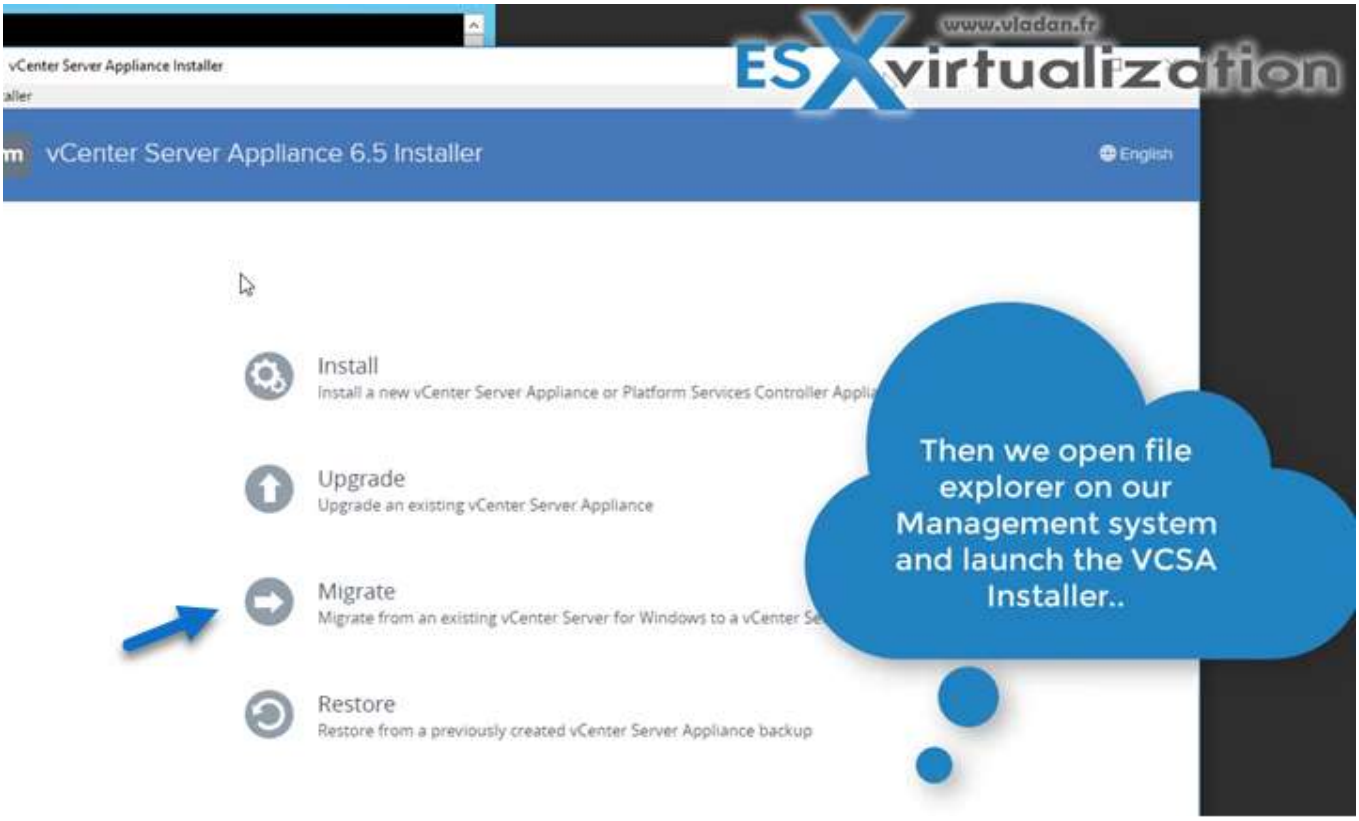
1. The first is running pre-checks on the source Windows vCenter Server. The Migration Assistant displays warnings of installed extensions and provides a resolution for each. It will also show the source and the destination deployment types.
2. The actual wizard-driven Migration Tool (GUI). This requires the vCenter Server Appliance 6.5 Installer.

WHAT DO WE NEED TO MIGRATE?

Step 1: connect to your vCenter server on Windows and mount the VCSA 6.5 iso file. Then open the folder called migration-assistant and execute the VMware-Migration-Assistant.exe to start the CLI helper. Next, you'll be asked for an SSO password (it's a CLI window). Hit enter and leave like this... The product will initialize itself, executes its scripts. You should **NOT** close this window...

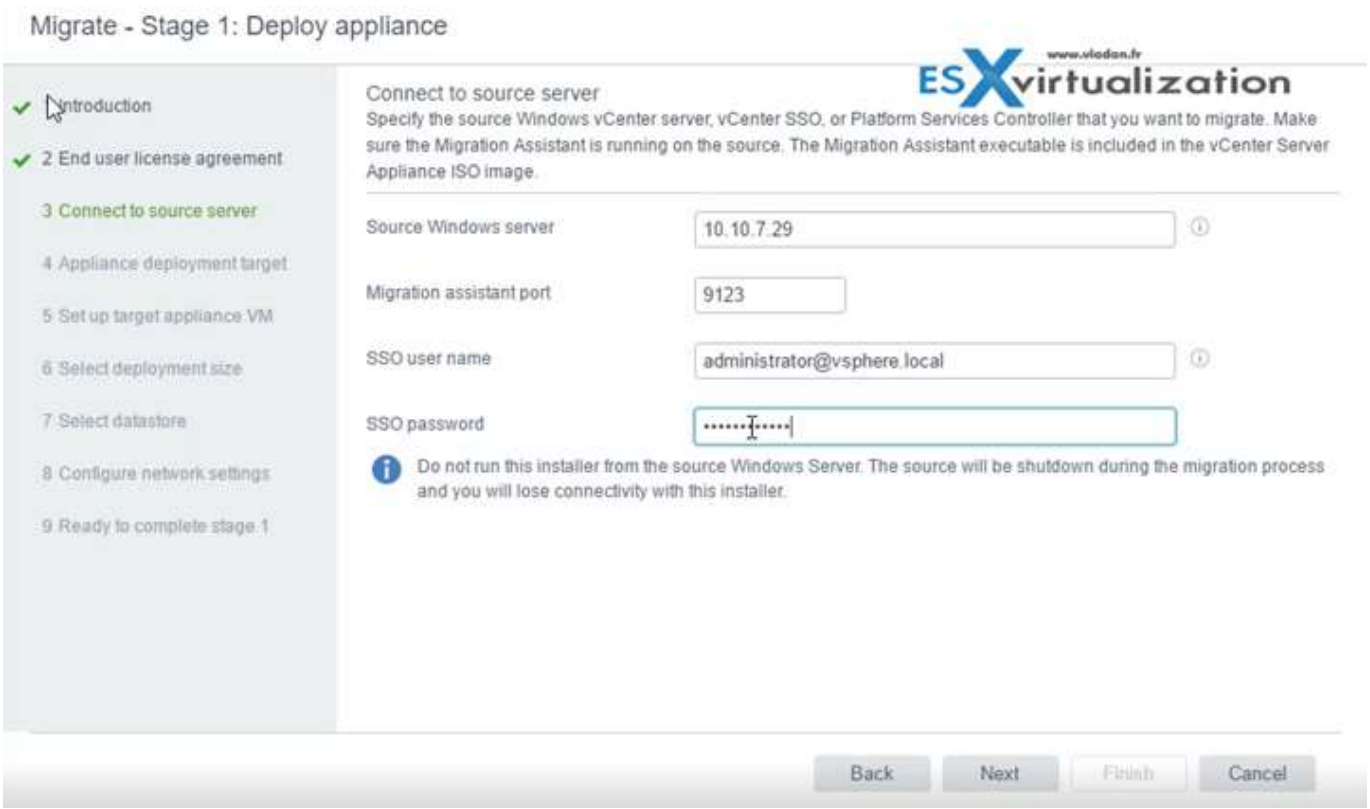


Step 2: Go to your management workstation/laptop and mount again the VCSA 6.5 file > open the **vcsa-ui-installer** folder and pick the version you need. You can have Windows, MAC or Linux based management workstation... plenty of choices!!! Launch the **installer.exe**



Then follow the assistant. You'll be asked questions about what's your source vCenter server, where you want to register the VCSA 6.5 VM, the temporary IP configuration of the VCSA etc...

An example below showing the connection to my "legacy" Windows vCenter...



The VCSA will have a temporary IP address during the copy of the data. The second stage of the assistant will configure the VCSA 6.5 and will also import the source Windows vCenter Server data:

- FQDN
- IP address
- UUID
- Certificates
- MoRef IDs

During the migration, there are no changes to the source Windows vCenter Server. So if anything goes sideways, the source vCenter is still there.

WRAP UP:

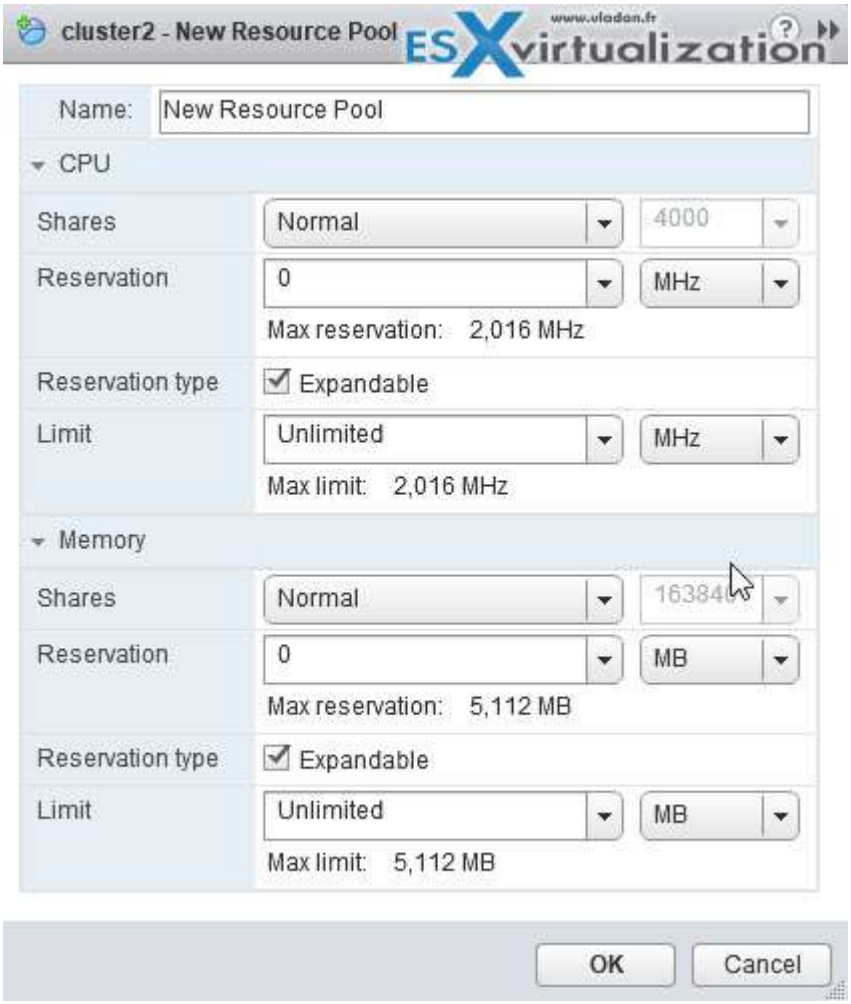
VMware does a very good job with this tool. For smaller IT shops, it provides a way to save 1 Windows server license. VCSA has more features than a Windows-based vCenter server. By "locking" the vCSA appliance, the admin does not have much choice and just use it, no "tweaking". No additional software install like it may be the case for some shops.

VCP6.5-DCV OBJECTIVE 5.1 - CONFIGURE MULTILEVEL RESOURCE POOLS

DETERMINE THE EFFECT OF THE EXPANDABLE RESERVATION PARAMETER ON RESOURCE ALLOCATION

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

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



CREATE A RESOURCE POOL HIERARCHICAL STRUCTURE

Resource pools always start at the root level. Each standalone host and DRS cluster has (invisible) root resource pool. You have to **enable DRS first** in order to create a resource pool.

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

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

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

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

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

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

CONFIGURE CUSTOM RESOURCE POOL ATTRIBUTES

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

CPU RESOURCES

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

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

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

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

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

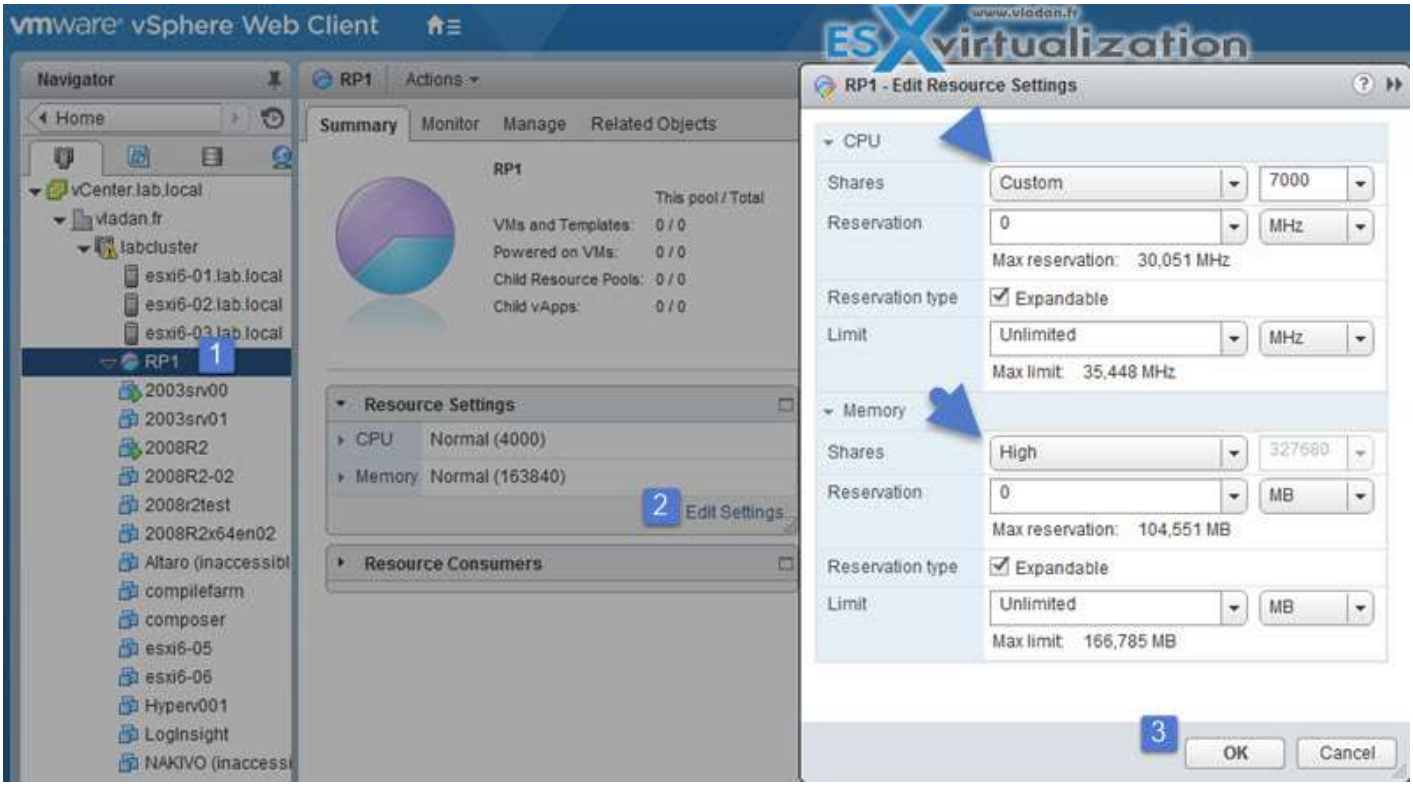
MEMORY RESOURCES

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

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

Reservation – Guaranteed memory allocation for this resource pool.

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



Expandable Reservation - When the checkbox is selected (default), expandable reservations are considered during admission control.

If you power on a virtual machine in this resource pool, and the combined reservations of the virtual machines are larger than the reservation of the resource pool, the resource pool can use resources from its parent or ancestors.

Determine how Resource Pools apply to vApps

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

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

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

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

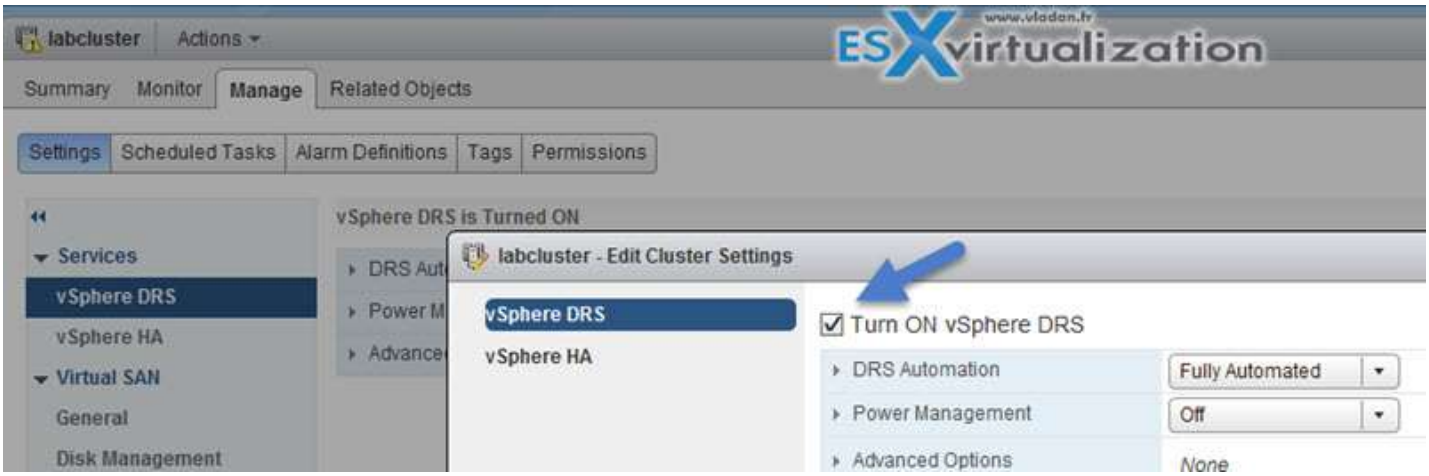
Shares - CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select Low, Normal, or High, which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific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

Reservation - Guaranteed CPU allocation for this vApp.

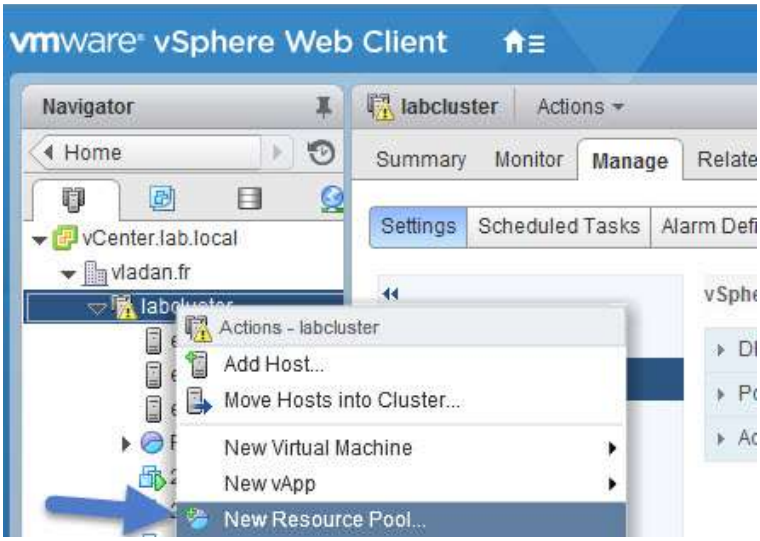
- **Reservation Type** - Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
- **Limit** - the upper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

CREATE/REMOVE A RESOURCE POOL

To be able to create Resource pool you must enable DRS. You can use both vSphere C# client or vSphere Web Client. (Web client) Select **Hosts and clusters** > **Manage** > **vSphere DRS** > **Edit** > **Check the Turn ON**.



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



ADD/REMOVE VIRTUAL MACHINES FROM A RESOURCE POOL

It’s possible to use both clients. Drag and drop… -:)

Or when creating new VM, during the wizard creation you’re asked whether you want to place the VM into specific resource pool…

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

Determine appropriate shares, reservations, and limits for hierarchical Resource Pools

You can find some examples in the vSphere 6.5 documentation set.

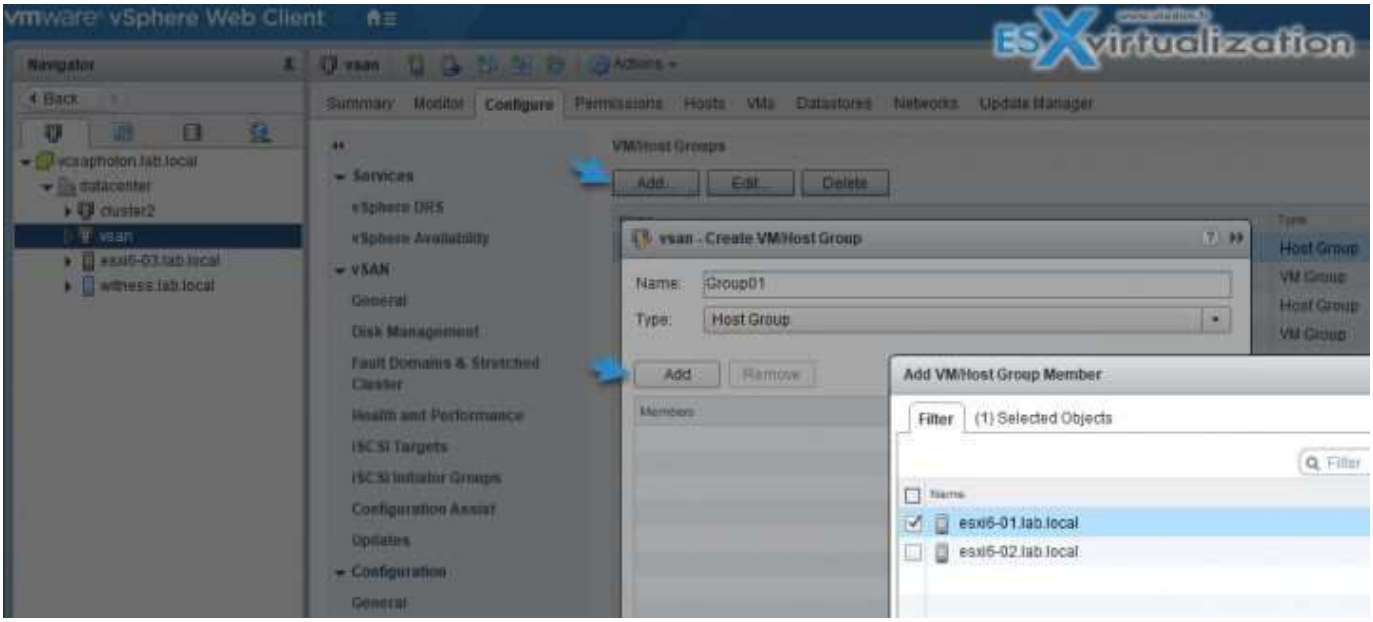
VCP6.5-DCV Objective 5.2 - Configure vSphere DRS and Storage DRS Cluster

Add/remove Host DRS Group

In order to **Create a Host DRS group** you'll need to:

vSphere Client > Select **Hosts and Clusters** > **Configure** > Select **VM/Host Groups** and click **Add**.

In the **Create VM/Host Group** dialog box, type a name for the group > Select **Host Group** from the Type drop-down box and click **Add** > **Click the checkbox next to a host** to add it. Continue this process until all desired hosts have been added > **Click OK**.

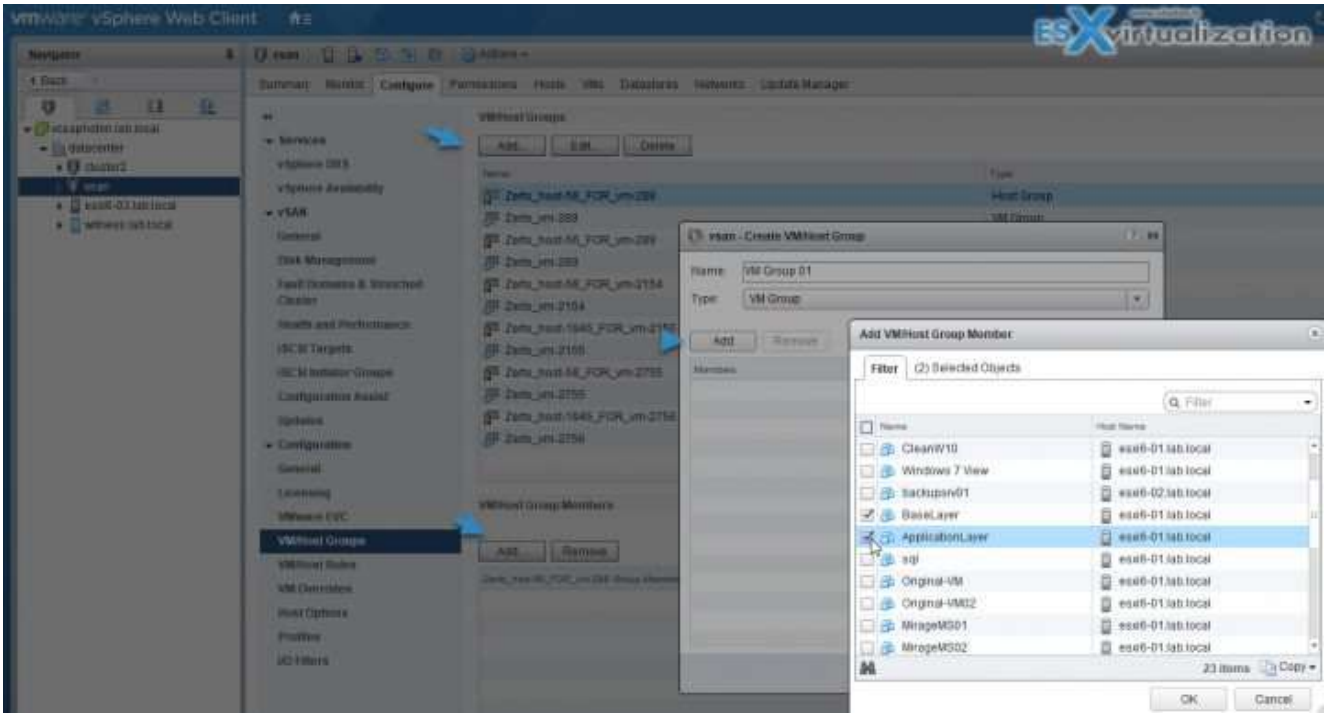


ADD/REMOVE VIRTUAL MACHINE DRS GROUP

Let's create a VM DRS Group:

vSphere Client > Select **Hosts and Clusters** > **Configure** > select **VM/Host Groups** and click **Add**.

In the Create VM/Host Group dialog box, **type a name** for the group > Select **VM Group** from the Type drop-down box and click **Add** > Click the checkbox next to a virtual machine to add it > **Click OK**.



MANAGE DRS AFFINITY/ANTI-AFFINITY RULES

vSphere Client > Select Hosts And Clusters > Configure > VM/Host Rule > Add. > Type a **name** for the rule > From the Type drop-down menu, select either **Keep Virtual Machines Together** or **Separate Virtual Machines. > Add > Select at least two VMs** to which the rule will apply and **click OK**.

Automation levels are described as follows.

- **Manual -** Placement and migration recommendations are displayed but do not run until you manually apply the recommendation.
- **Fully Automated -** Placement and migration recommendations run automatically.
- **Partially Automated -** Initial placement is performed automatically. Migration recommendations are displayed but do not run.
- **Disabled**

TIP: When DRS is disabled, the cluster's resource pool hierarchy and affinity rules are not reestablished when DRS is turned back on. So if you **disable DRS**, the resource pools are **removed** from the cluster.

To avoid losing the resource pools, instead of disabling DRS, you should **suspend it** by changing the DRS automation level **to manual** (and disabling any virtual machine overrides). This prevents automatic DRS actions but preserves the resource pool hierarchy.

There you can check the drop-down menu and try to check:

vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

To change the automation level on a per VM basis

vSphere Client > Select Hosts and Clusters > Configure > Services > under Services, select vSphere DRS and click Edit. Expand DRS Automation.

- Select the Enable individual virtual machine automation levels check box.
- To temporarily disable any individual virtual machine overrides, deselect the Enable individual virtual machine automation levels check box.

Virtual machine settings are restored when the checkbox is selected again.

- To temporarily suspend all vMotion activity in a cluster, put the cluster in manual mode and deselect the Enable individual virtual machine automation levels check box.
- Select one or more virtual machines.
- Click the Automation Level column and select an automation level from the drop-down menu > Click OK.

EXPLAIN HOW DRS AFFINITY RULES EFFECT VIRTUAL MACHINE PLACEMENT

You can control the placement of virtual machines on hosts within a cluster by using affinity rules. Certainly useful if you want (or not) that two or more VMs runs on the same host(s).

You can create two types of rules.

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

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

A VM-Host affinity rule includes the following components:

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

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

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

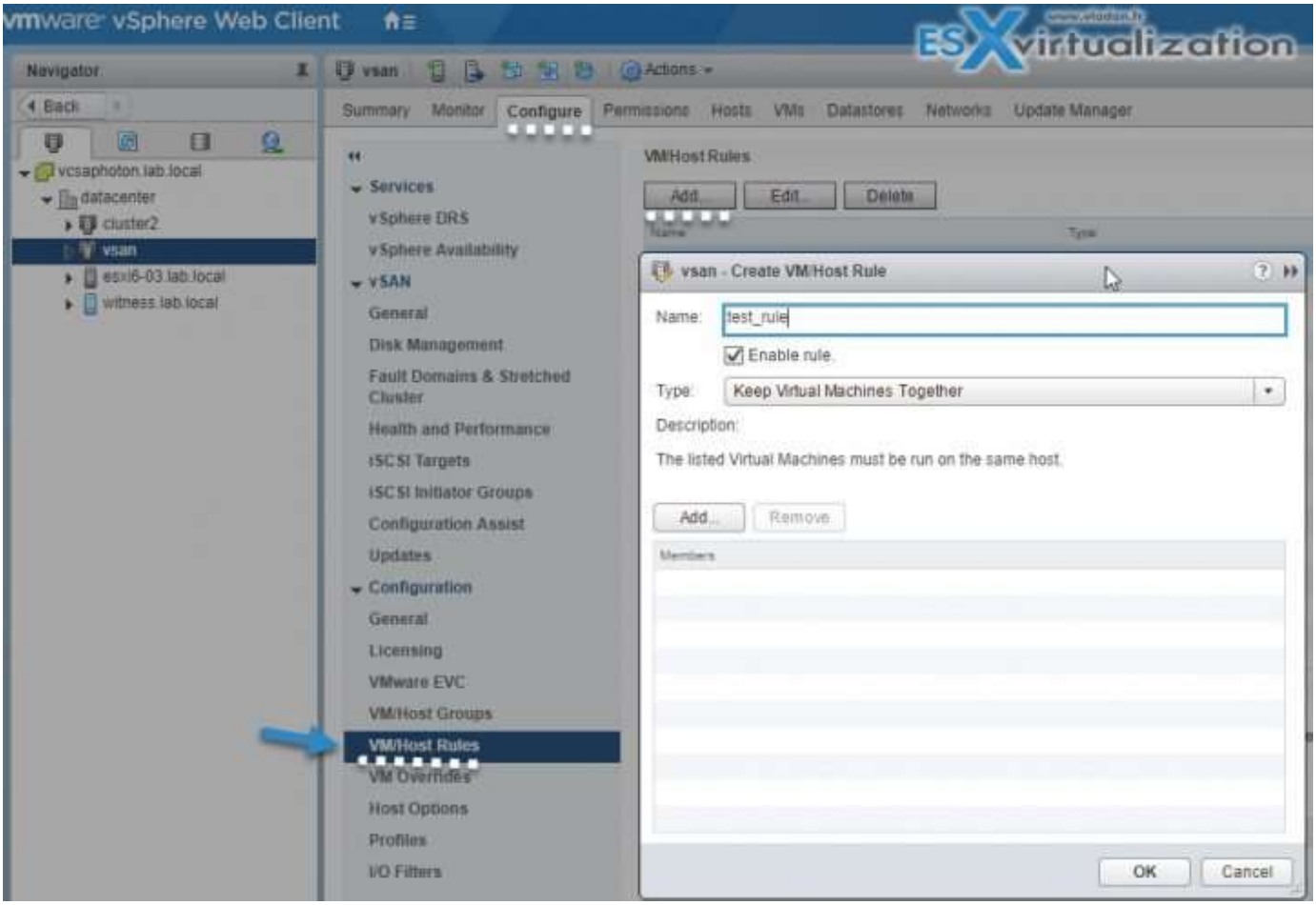
A rule specifying affinity causes DRS to try to keep the specified virtual machines together on the same host, for example, for performance reasons. With an anti-affinity rule, DRS tries to keep the specified virtual machines apart, for example, so that when a problem occurs with one host, you do not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

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

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

WHERE?

In the **vSphere Web Client** > **Host and clusters** > **Configuration** > **VM/Host Rules**> **Add** > Give your rule a **name**. From the Type menu, select Virtual Machines to Hosts. Select the virtual machine DRS group and the host DRS group to which the rule applies.



UNDERSTAND NETWORK DRS

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

This wasn't always the case as usually, DRS considered only the compute resource (CPU and memory) utilization of hosts and VMs for balancing load cross hosts and placing VMs during Power-on operations. While CPU and memory resources are the most important in most cases, the network utilization is another aspect. We could end up in a situation where the network is already saturated on a host, but DRS still makes the decision to place the VM on that particular host.

The network-aware DRS in vSphere 6.5 is only to make sure the host has sufficient network resources available, as well as all compute resources required by the VM.

However, compared to a regular DRS, which balances the CPU and memory load, the network-aware DRS **does not balance** the network load in the cluster, which means it **will not trigger** a vMotion when there is network load imbalance.

DRS does the initial placement in two steps:

- It compiles the list of possible hosts based on cluster constraints and compute resource availability and ranks them.

- Then, from the list of hosts, it picks the host with the best rank and best network resource availability

Differentiate load balancing policies

During DRS operation:

- DRS generates a list of possible migration proposals.
- Eliminates the proposals whose destination hosts are network saturated.
- From the remaining list of proposals, recommends the one with the maximum balance improvement in terms of compute resources and that also contributes to network resource availability on the source host, in case the source host is network saturated.

Host Network Saturation Threshold - DRS will not place a VM to a host which network is overloaded. Only if its network utilization is beyond a certain threshold. This threshold is set to 80% by default. So, unless the host network utilization is above 80%, DRS considers the host to be a good candidate in terms of network resource availability.

If a host's network utilization is at or above the saturation threshold, DRS considers it to be **network saturated**. If all the hosts in the cluster are network saturated, DRS will prefer not to migrate VMs with network load, since migrating network loaded VMs to an already network saturated host would result in further degradation of VM performance. When DRS cannot migrate VMs due to this behavior, this can sometimes result in an imbalanced cluster.

Monitoring Host Network Utilization - Introduced in vSphere 6.5 you have a possibility to monitor the host network load distribution under the DRS monitoring tab in the vSphere Web Client.

The network utilization percentage of a host is the average capacity that is being utilized across all the physical NICs (pNICs) on that host. For example, if a host has three pNICs, one of them is 90% utilized and the other two are 0% utilized, then the network utilization of the host is considered to be 30%.

Describe Predictive DRS

Predictive DRS happens when vCenter server proactively rebalances the VMs based on predictive patterns in the cluster workload. Predictive DRS bases its data provide by vRealize Operations Manager. vROPS monitor VMs running within a vCenter server and analyzes the historical data. Based on this, it can forecast data, predictable patterns of resources usage. Those data are used by predictive DRS, which moves VMs around based on the patters.

VCP6.5-DCV Objective 6.1 - Configure and Administer vCenter Appliance Backup/Restore

Configure vCSA File-based Backup and Restore

The vCenter Server Appliance supports a file-based backup and restore. In case your VCSA becomes corrupt or non-recoverable from traditional backup via your favorite backup software, you can still restore from file-level backup.

In vSphere 6.5, you can use the vCSA's Management Interface (VAMI) accessible via the port 5480, to create a file-based backup of the vCSA and Platform Services Controller (PSC) appliance. After you create the backup, you are able to restore its configuration by using the GUI installer of the appliance. (executing the phase 2).

You use the vCenter Server Appliance Management Interface to perform a file-based backup of the vCenter Server core configuration, inventory, and historical data of your choice. The backed-up data is streamed over FTP, FTPS, HTTP, HTTPS, or SCP to a remote system. The backup is not stored on the vCenter Server Appliance.

The steps:

- Deploy a new vCSA.
- Copy the data from the file-based backup to the new appliance.

Simple, right?

What is backed up?

The minimum set of data needed is backed up by default. Those are for example the OS, vCenter services and Inventory. You can additionally backup also Inventory, configuration, and historical data (Statistics, events, and tasks) in a vCenter server database.

You can select whether to include historical data, such as stats, events, and tasks, during the assistant.

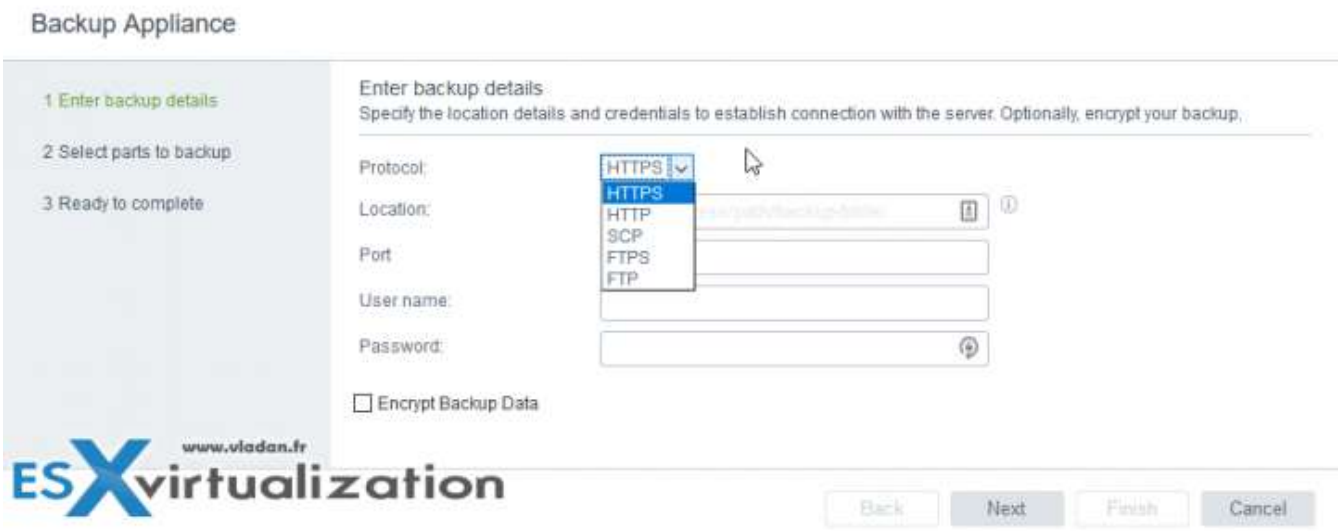
Login via:

https://IP_or_FQDN:5480

After you log in, then you can hit the big **Backup** button. A wizard will start… (click to enlarge)

There you'll be presented with a nice wizard which will allow you to specify where you want to send this backup. The location must be an empty folder. Note the option to encrypt your backup data, a simple checkbox.

Note the option to encrypt your backup data, a simple checkbox… Select Encrypt Backup Data to encrypt your backup file and enter a password for the encryption. If you select to encrypt the backup data, you must use the encryption password for the restore procedure.



You must have an FTP, FTPS, HTTP, HTTPS, or SCP server up and run with sufficient disk space to store the backup.

You should dedicate a separate folder on your server for each file-based backup. Review the data that is backed up by default and select Stats, Events, and Tasks to back up additional historical data from the database.

Within the Description text box, enter a description of the backup and proceed with the wizard. You'll have a Ready to complete page, review the summary information for the backup and click Finish. The Backup Progress window will open and shows you the progress of the backup operation.

Define supported backup targets

As being mentioned above there are quite a few backup target possibilities. The most important to note is the fact that the backup data are not stored on the appliance so in case something goes wrong and you need to restore, you have the data stored elsewhere.

Supported protocols: FTP, FTPS, HTTP, HTTPS or SCP.

If you want to use FTP, FTPS, HTTP, or HTTPS you should know that the path is relative to the home directory configured for the service. But for SCP protocol, the path is absolute to the remote systems root directory.

VMware is really working hard on the VCSA in order to bring feature parity. That's now the case and even more as we have a built-in backup configuration, and (or) vCSA High Availability, which is really useful. With the fact that you can save one Windows license, the VMware environment costs you a little bit cheaper now...

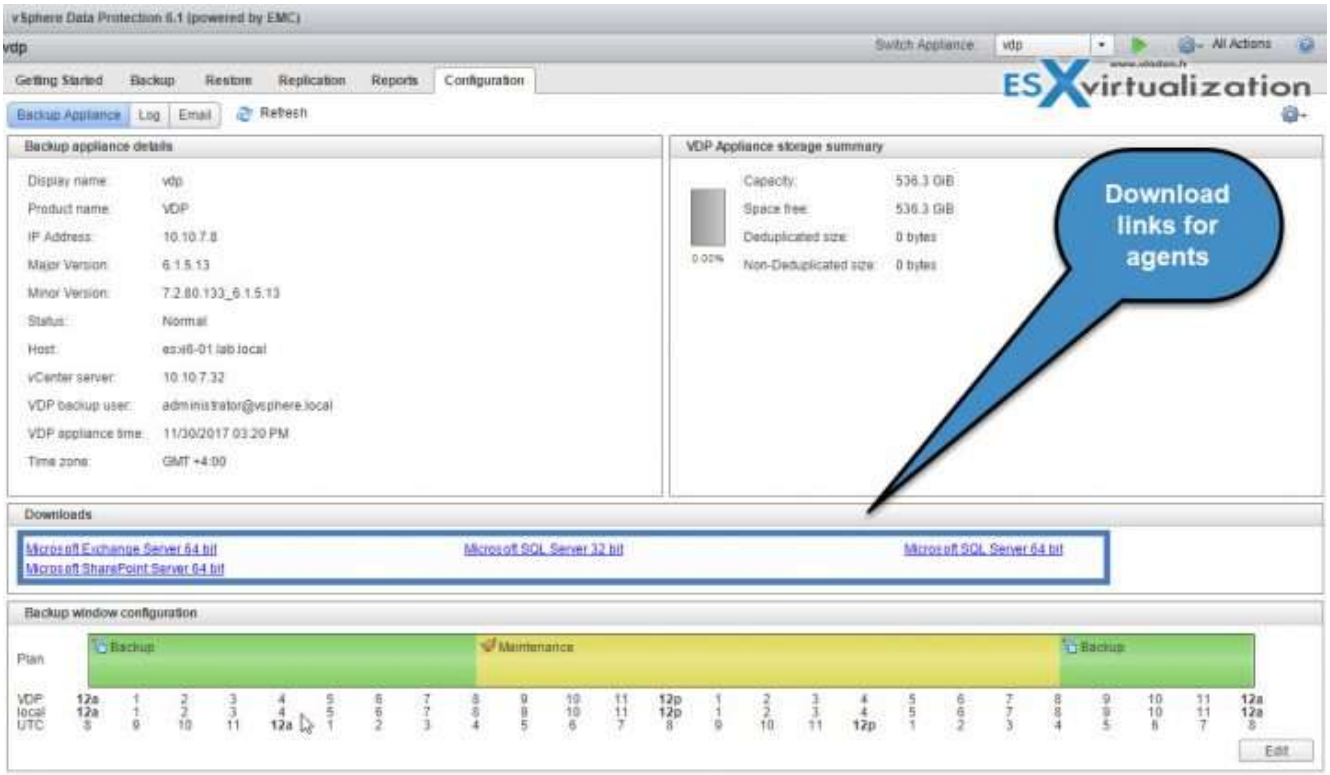
VCP6.5-DCV Objective 6.2 – Configure and Administer vCenter Data Protection

Deploy VDP Application Agents

VDP supports granular guest-level backup and recovery support for:

- Microsoft Exchange Servers
- SQL Servers
- SharePoint Servers.

To support guest-level backups, a VDP client is installed on the Exchange Servers, SharePoint Servers, and SQL Servers. It is a process of downloading the agent from within the VDP UI and installing it on the guest OS. It's an MSI package so if you have many systems, you might consider deploying those agents via Microsoft AD and using GPO.



DIFFERENTIATE VMWARE DATA PROTECTION (VDP) CAPABILITIES

VDP uses Image Level Backup and Restore. VDP creates image-level backups, which are integrated with the vStorage API for Data Protection. The VDP appliance communicates with the vCenter server to make a snapshot of a virtual machine's .vmdk files. Deduplication takes place within the appliance by using a patented variable-length deduplication technology.

vSphere Data Protection's algorithm analyzes the binary structure of a data set (all the 0s and 1s that make up a dataset) in order to determine segment boundaries that are context-dependent. Variable-length segments average 24 KB in size and are compressed to an average of 12 KB. By analyzing the binary structure within the VMDK files, vSphere Data Protection works for all file types and sizes and intelligently deduplicates the data.

In fact, VDP product is based on EMC's Avamar code.

Each VDP appliance can simultaneously back up up to 8 virtual machines if the internal proxy is used, or back up to 24 virtual machines if the maximum number of 8 external proxies are deployed with the VDP appliance.

VDP utilizes Changed Block Tracking (CBT) to back up only changes, after the successful first full backup. It's also used for restores of VMs to their original location and reduces data transfer within the vSphere environment during a recovery operation and more importantly reduces the recovery time.

VDP automatically evaluates the workload between both restore methods (full image restore or a recovery leveraging CBT) and performs the method resulting in the fastest restore time. This is useful in scenarios where the change rate since the last backup in a virtual machine being restored is very high and the overhead of a CBT analysis operation would be more costly than a direct full-image recovery. VDP determines which method results in the fastest image recovery times for virtual machines in the environment.

vCenter Server Backup and Restore support - VDP supports backups of a vCenter Server by using an embedded Platform Service Controller (PSC) and an external PSC. VDP can perform file system quiescing during backups.

You must create a separate backup job that contains only vCenter Server. Schedule this backup job in the VDP backup window during off-peak times to ensure that you can generate a file system-consistent snapshot during the backup. If the vCenter Server's workload is heavy, the backup can fail because of failure to quiesce the VM. vCenter Server is also reasonably resilient to crash-consistent restore. However, VMware supports backup and restore of vCenter Server by using VDP on the best-effort basis, and **does not guarantee a successful restore**.

Single VMDK Backup and Restore - You can select individual disk backup job, which allows you to select only the disks you need.

When you restore a VM, the VDP appliance restores the VM configuration file (.vmx), which results in the creation of all VMDKs from the original VM. If any of the original VMDKs were not backed up, the restore process creates them as provisional VMDKs. The VM may not be fully functional in this case. The protected VMDKs, however, can be accessed from the restore.

Guest-level Backup and Restore - You'll have to install (and maintain) agents inside the VMs. VDP supports guest-level backups for Microsoft SQL Servers, Exchange Servers, and Share Point Servers. With guest-level backups, client agents (VMware VDP for SQL Server Client, VMware VDP for Exchange Server Client, or VMware VDP for SharePoint Server Client) are installed on the SQL Server, Exchange Server, or SharePoint Server in the same manner that backup agents are typically installed on physical servers.

The advantages of VMware guest-level backups are:

- Provides additional application support for Microsoft SQL Server, Microsoft Exchange Server, or SharePoint Server inside the VMs
- Support for backing up and restoring entire Microsoft SQL Server, Microsoft Exchange Server, or SharePoint Servers or selected databases
- Identical backup methods for physical and virtual machines

Replication - Think of it as a Backup copy job, if you're using Veeam... VDP replication enables you to avoid data loss if the source VDP appliance fails because copies of the backups are available on the destination target.

Replication jobs determine which backups are replicated, and when and to where the backups are replicated. With scheduled or ad hoc replication jobs for clients that have no restore points, only the client

is replicated on the destination server. Backups created with VDP 6.0 or later can be replicated to another VDP appliance, to an EMC Avamar server, or to a Data Domain system. If the target VDP appliance is 5.8 or earlier, then the target must be VDP Advanced or Replication Target Identity.

File Level Recovery - File Level Recovery (FLR) allows local administrators of protected virtual machines to browse and mount backups for the local machine. From these mounted backups, the administrator can then restore individual files. FLR is accomplished by using the VDP Restore Client.

EXPLAIN VMWARE DATA PROTECTION SIZING GUIDELINES

You must do some math before deploying VDP because you must know which size of appliance and number of appliances are necessary for your environment:

- Number of and type of VMs
- Amount of data
- Retention periods (daily, weekly, monthly, yearly)
- Typical change rate

You must think before on what size you'll need at the destination deduplication datastore since the VDP appliance size **cannot be changed later.**

vSphere Data Protection Administration Guide

The following table shows examples for vSphere Data Protection sizing recommendations:

Table 2-3. Sample recommendations for vSphere Data Protection sizing

# of VMs	Data storage per client	Retention: daily	Retention: weekly	Retention: monthly	Retention: yearly	Recommendation
25	20	30	0	0	0	1-0.5 TB
25	20	30	4	12	7	1 -2 TB
25	40	30	4	12	7	2 - 2 TB
50	20	30	0	0	0	1 - 1 TB
50	20	30	4	12	7	2 - 2 TB
50	40	30	4	12	7	3 -2 TB
100	20	30	0	0	0	1 - 2 TB
100	20	30	4	12	7	3 - 2 TB
100	40	30	4	12	7	6 - 2 TB

CREATE/DELETE/CONSOLIDATE VIRTUAL MACHINE SNAPSHOTS

VM's snapshots should not be used in production. Everyone knows that.

Memory Snapshots - The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.

Quiesced Snapshots - When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

If the virtual machine is powered off or VMware Tools is not available, the Quiesce parameter is **not available**. You cannot quiesce virtual machines that have large capacity disks.

Delete - Use the Delete option to remove a single parent or child snapshot from the snapshot tree. Delete writes disk changes that occur between the state of the snapshot and the previous disk state to the parent snapshot. You can also use the Delete option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.

Delete All - Use the Delete All option to delete all snapshots from the Snapshot Manager. Deleting a snapshot removes the snapshot from the Snapshot Manager. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk.

When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

To delete a snapshot, a large amount of information needs to be read and written to a disk. This process can reduce virtual machine performance until consolidation is complete. Consolidating snapshots removes redundant disks, which improves virtual machine performance and saves storage space. The time it takes to delete snapshots and consolidate the snapshot files depends on the amount of data that the guest operating system writes to the virtual disks after you take the last snapshot. The required time is proportional to the amount of data the virtual machine is writing during consolidation if the virtual machine is powered on.

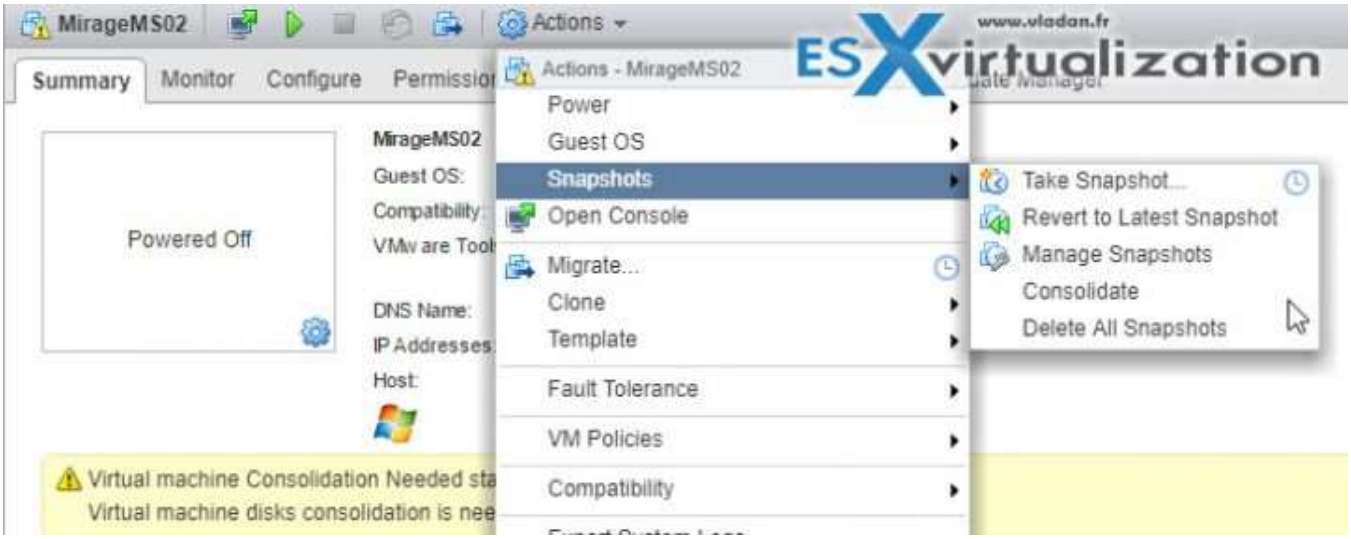
The presence of redundant delta disks can adversely affect virtual machine performance. You can combine such disks without violating a data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

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

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

Show consolidation column: **Right-click the menu bar** for any virtual machine column and select **Show/Hide Columns** > **Needs Consolidation.**

To consolidate the files, **right-click the virtual machine** and select **Snapshots > Consolidate.** Check the Needs Consolidation column to verify that the task succeeded.



INSTALL AND CONFIGURE VMWARE DATA PROTECTION

VDP is VSA based (Linux). The deployment as an OVF is fast and convenient.

VDP System Requirements VDP is available in the following configurations:

- 5 TB
- 1 TB
- 2 TB
- 4 TB
- 6 TB
- 8 TB

After VDP is deployed the size can be increased.

Screenshot from VMware User Guide.

	0.5 TB	1 TB	2 TB	4 TB	6 TB	8 TB
Processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors	Minimum four 2 GHz processors
Memory	4 GB	4 GB	4 GB	8 GB	10 GB	12 GB
Disk space	873 GB	1,600 GB	3 TB	6 TB	9 TB	12 TB

Requirements:

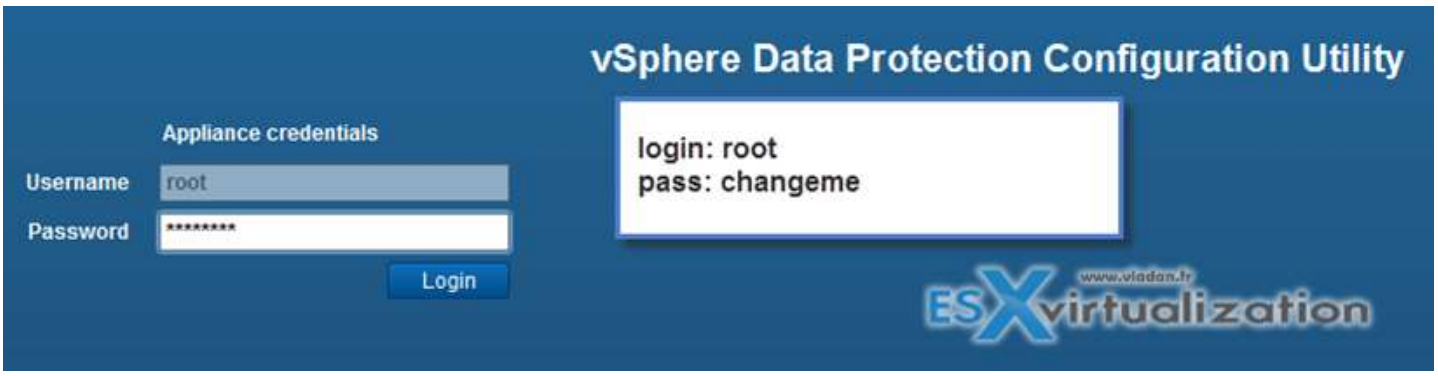
- NTP – All vSphere hosts and the vCenter Server must have NTP configured properly. The VDP Appliance gets the correct time through vSphere and must not be configured with NTP.
- DNS – create DNS forward and reverse record and check that you have vCenter server responding via nslookup.

Deploy the OVF file via vSphere Web client to a VMFS5 datastore (to avoid block size limitations).

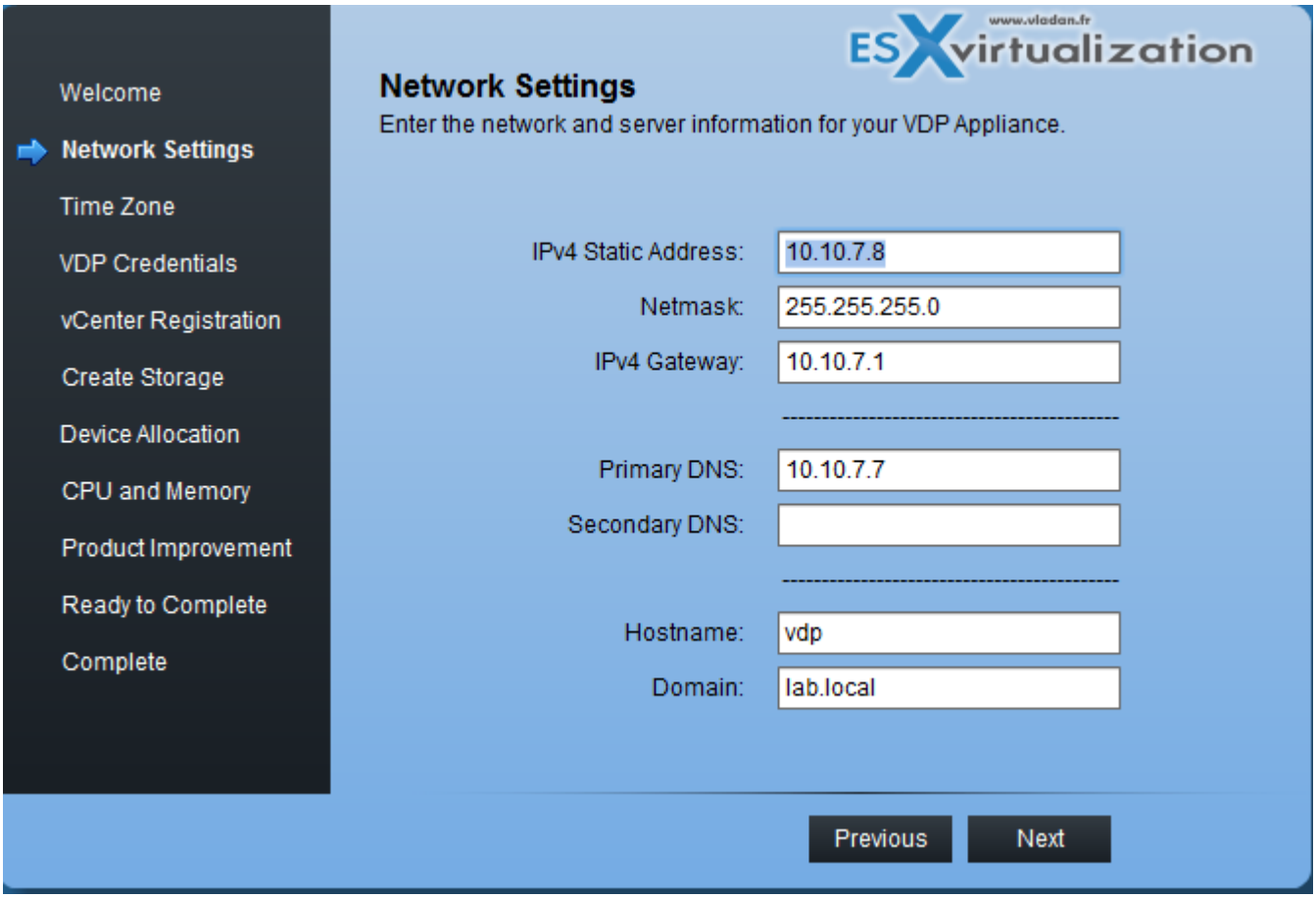
After the deployment and startup of the VM go to the IP address specified on the console.

https://ip_of_vdp:8543/vdp-configure

Login: root
pass: changeme

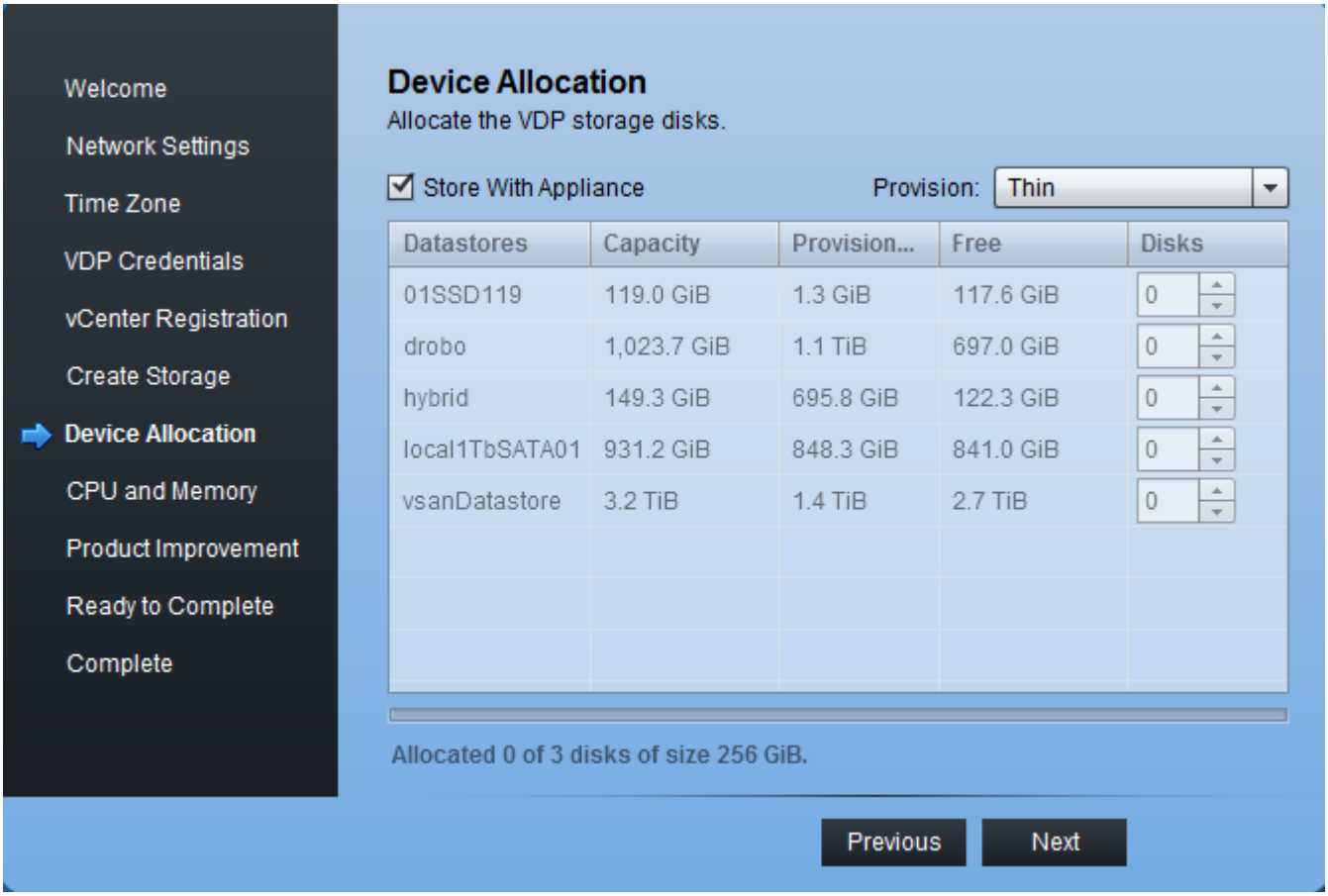


Follow the assistant, you should have the info pre-filled when you click the next button…

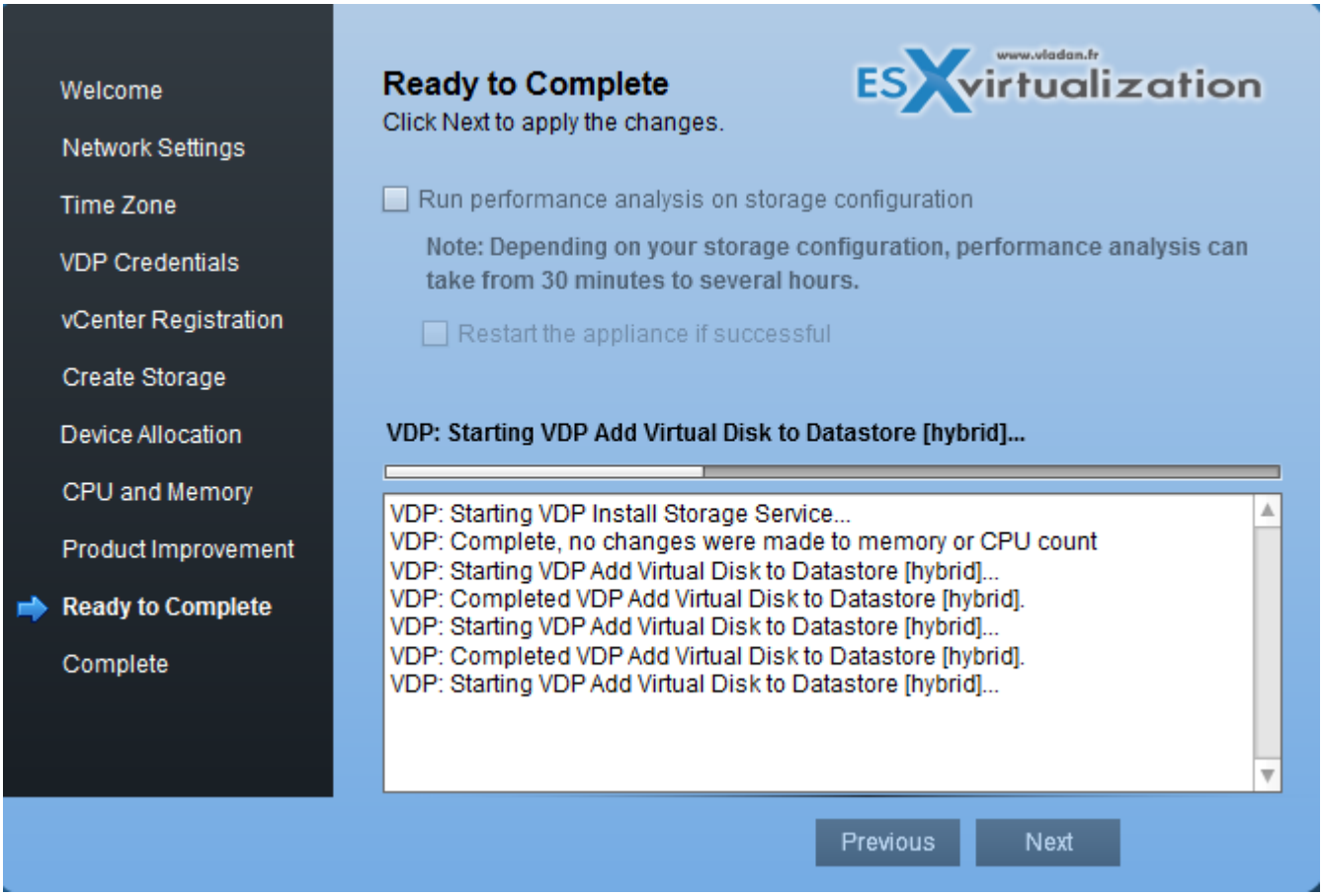


Continue with the wizard. Test your connection to vCenter to avoid issues…

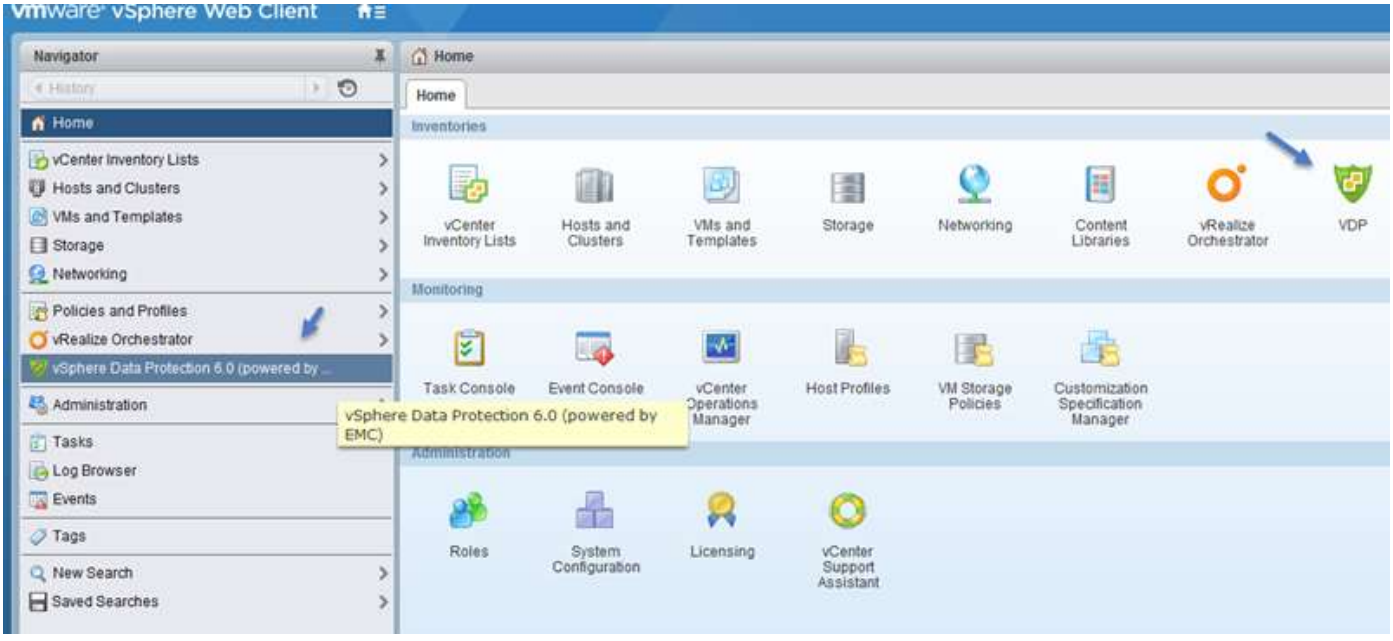
Create storage. Here you can (but don't have to) check the box "store with appliance" in case you have enough space on the shared storage datastore you have chosen.



Continue with the assistant until the end. After the setup is finished the appliance will reboot…



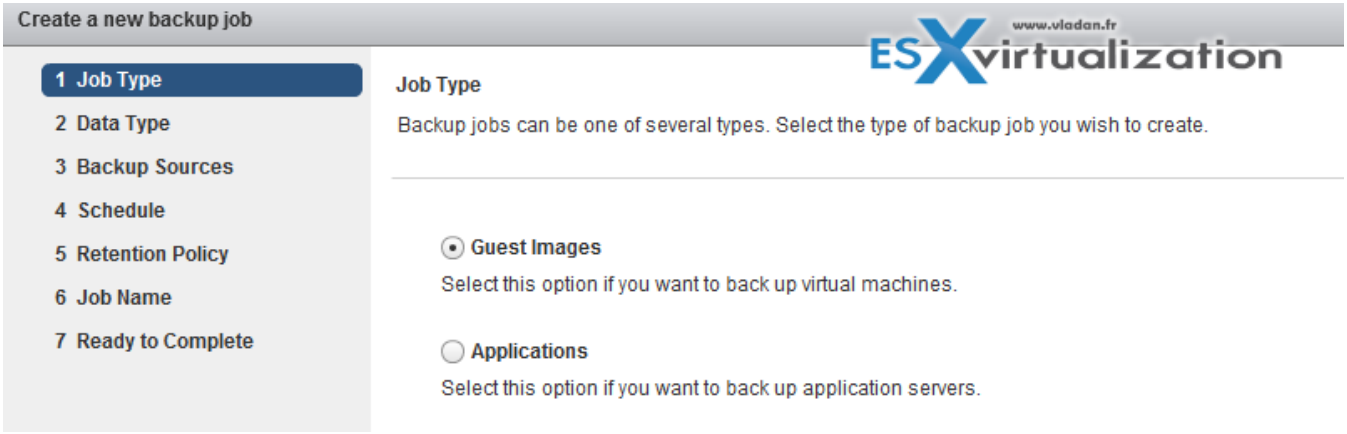
It takes up to 15 min to fully setup after the reboot…You'll have to log off and log in back again through vSphere web client to see this new plugin to appear.



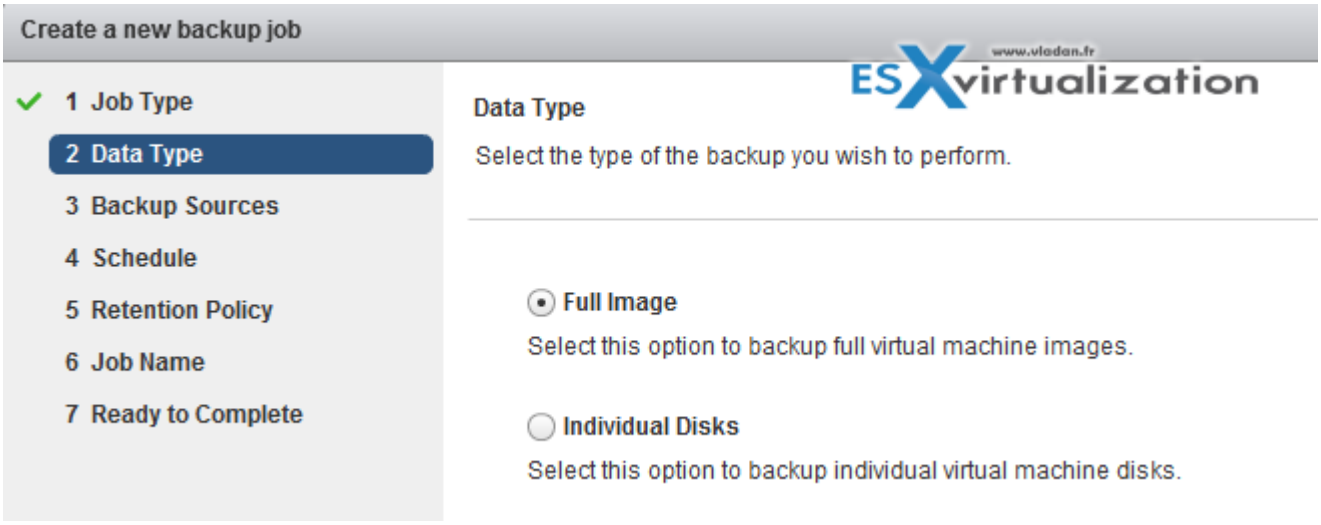
CREATE A BACKUP JOB WITH VMWARE DATA PROTECTION

To create a first backup job, just click through the new icon on the dashboard in vSphere web client.

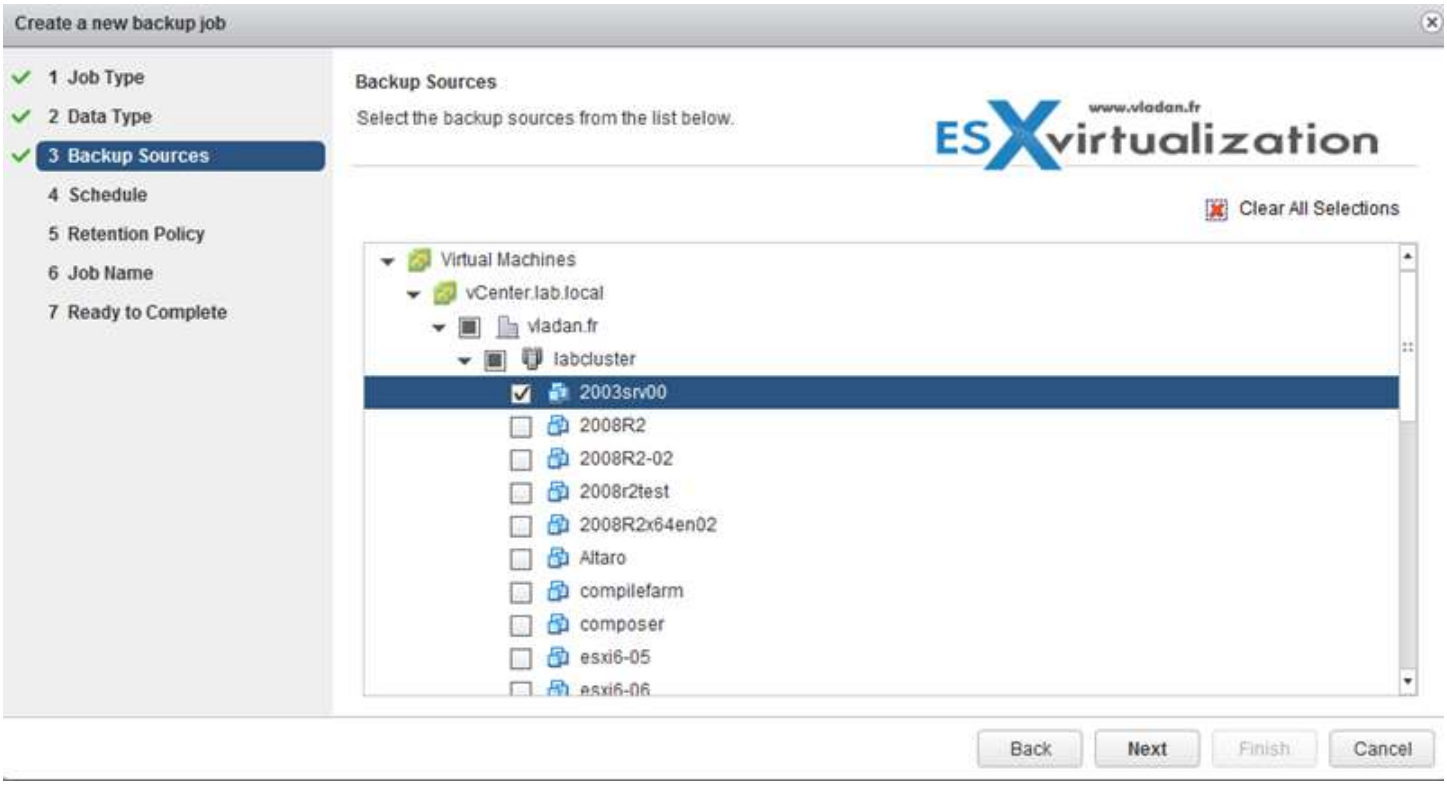
Then start the assistant…



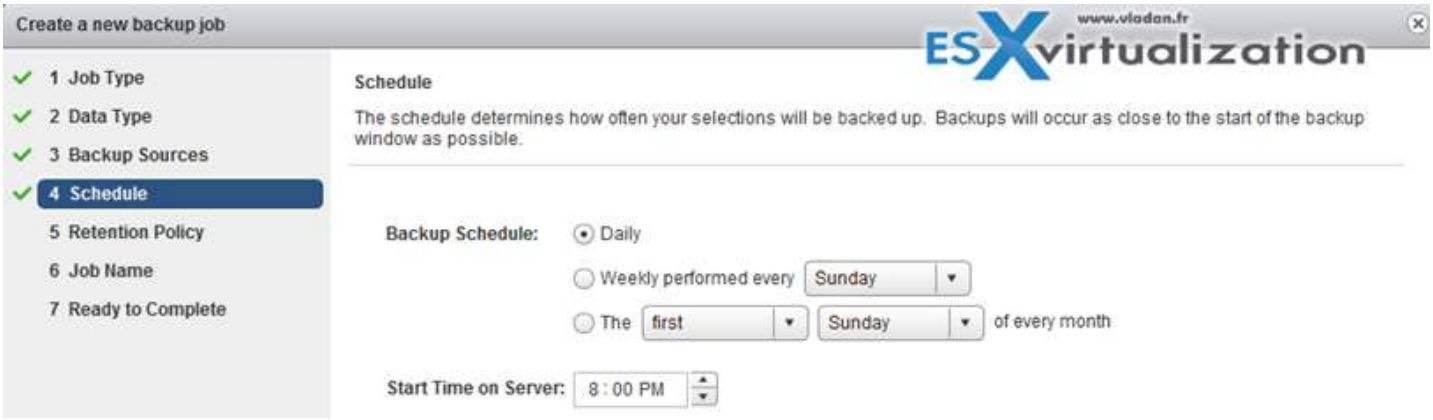
Continue…



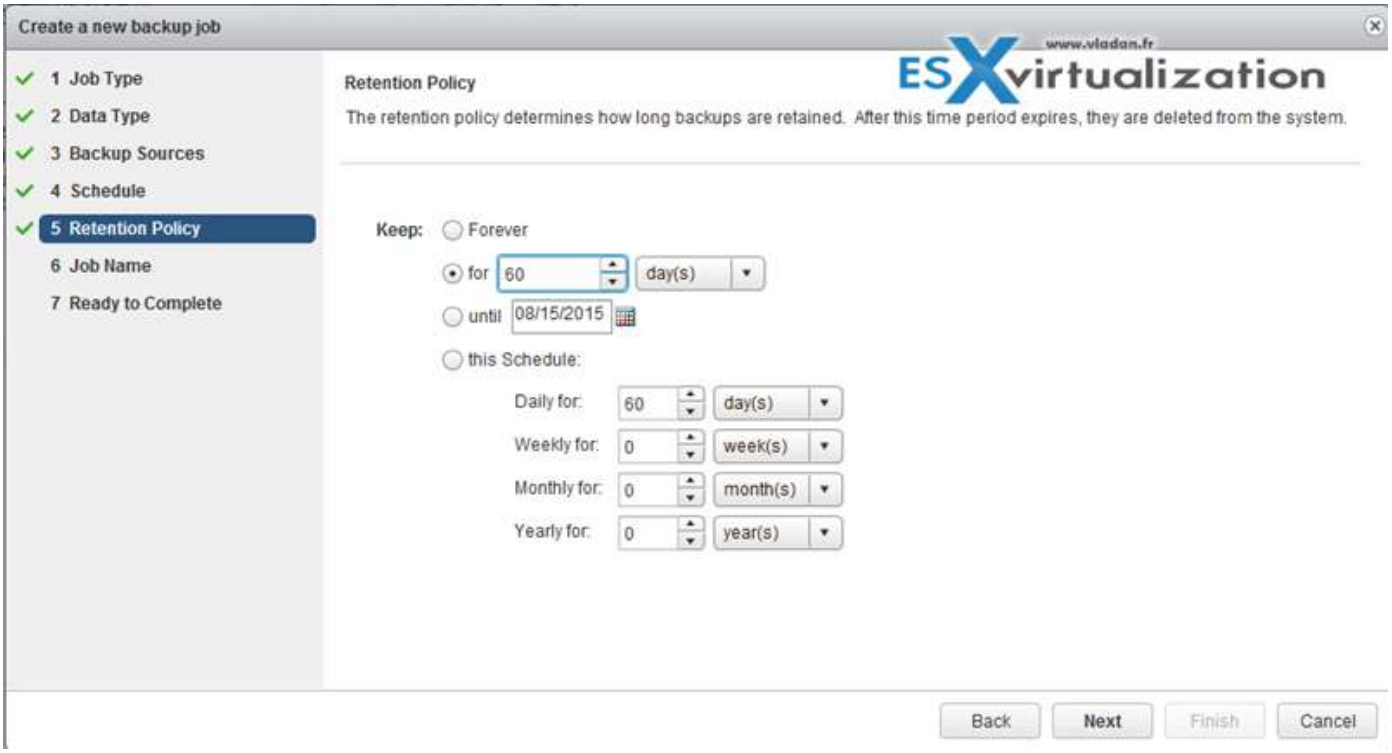
Choose VM(s)…



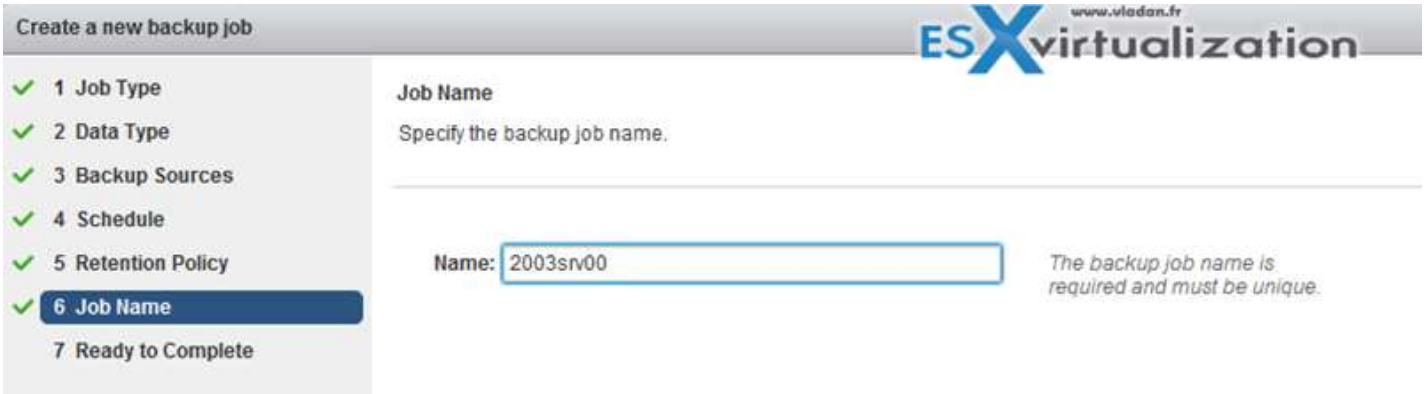
Backup schedule…



Specify retention policy…. Note that this can be changed later. (Think of sizing.)

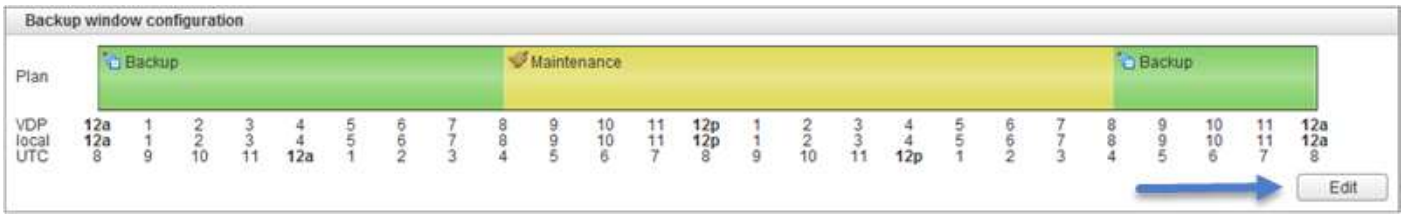


Give the job some meaningful name…



And off you go.

Just created a first backup job. If you go and click the Configuration TAB, then down there you can configure the Backup window configuration… If not, the default backup starts at 8PM…



Backup/Restore a virtual machine with VMware Data Protection

You can run backup jobs immediately by:

- Choosing to backup up a protected virtual machine
- Choosing to run an existing backup job

Select the VM you want to immediately back up:

Right-click the VM > All VDP Actions > Backup Now.

Immediately Running a Backup Job

Click the job you want to run immediately > (use **Ctrl- or Shift-click** for multiple selections) > **Hold down the Ctrl key and click multiple, specific backup jobs.** Hold down the Shift key and click a range of backup jobs > Click Backup Now > **Drop-down selection > Backup all Sources** (or Backup only out of date sources) > **Click the sources you want to back up immediately > OK**.
Backup Now **Immediately** initiates backup jobs if VDP is in the backup window or the maintenance window

Restore Operations

You can restore the backups to either the original location or an alternate location. Restore operations are performed on the **Restore tab**. The Restore tab displays a list of virtual machines that have been backed up by the VDP appliance. By navigating through the list of backups, you can select and restore specific backups. The list shows specific icons for crash-consistent and application-consistent backups.

Note: There are also icons for crash-consistent backups and the expiration date of the backup.

Detection of the application-consistent backups applies only to the Windows clients. The application-consistent backups on the Linux clients appear with the Consistency level, not applicable icon.

You can hit **refresh** to actualize.

VCP6.5-DCV Objective 6.3 - Configure vSphere Replication

Compare and contrast vSphere Replication compression methods

You can configure vSphere Replication (VR) to compress the data that it transfers through the network. Compressing the replication data that is transferred through the network saves network bandwidth and might help reduce the amount of buffer memory used on the vSphere Replication server.

However, compressing and decompressing data requires more CPU resources on both the source site and the server that manages the target datastore

vSphere Replication 6.0 utilizes the FastLZ compression library. This provides a balance of speed, minimal CPU overhead, and compression efficiency.

If you are using vSphere 6.0 and VR 6.0 at both the source and target locations, updates are compressed at the source and stay compressed until they are written to storage at the target. In cases where there is a mixed configuration, packets may be decompressed at some point in the replication path.

Performing this decompression in the VR virtual appliance (VA) will cause higher vCPU utilization in the appliance. Best is, vSphere 6.0 and VR 6.0 at both the **source and target locations**.

For most replication workloads, you will likely see compression ratios of approximately 1.6:1 to 1.8:1. This will result in faster sync times and lower bandwidth utilization.

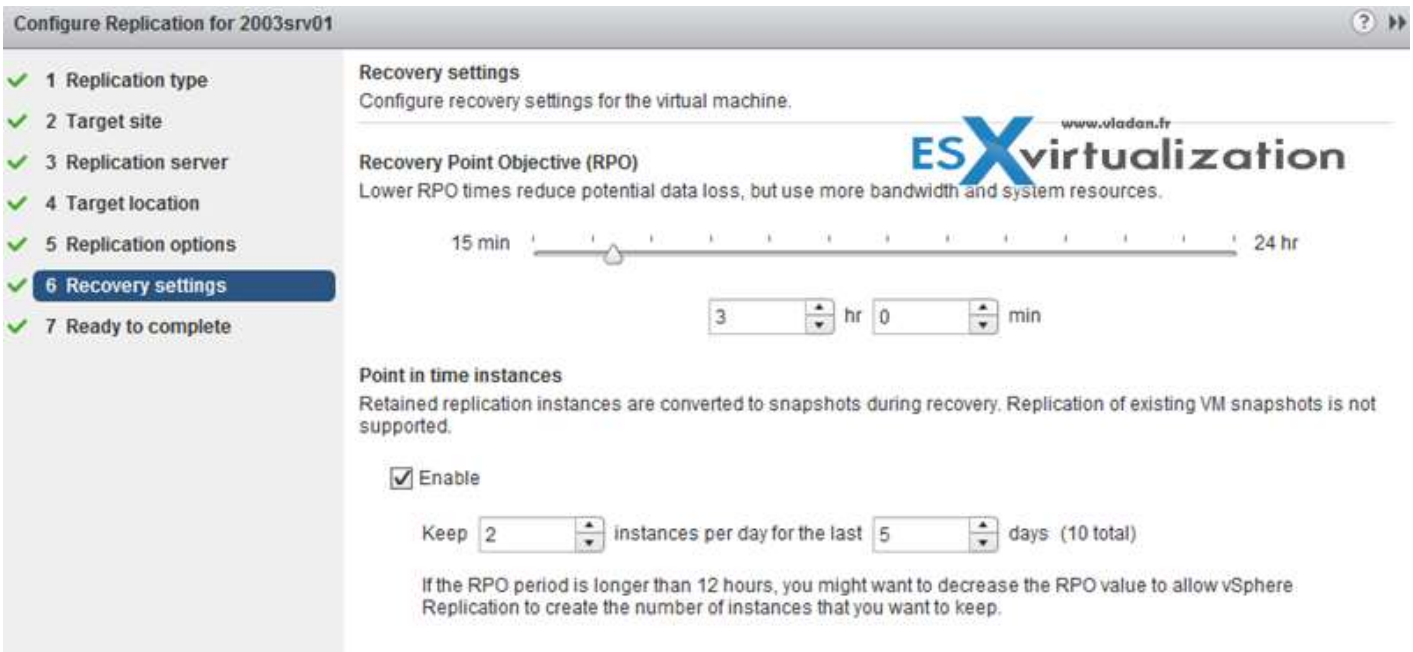
But what's interesting is the fact that if compression is enabled.

Quick quote:

However, if the target ESXi host is earlier than 6.0,vSphere Replication prevents vMotion from moving replication source VMs to that host because it does not support data compression. This prevents DRS from performing automated vMotion operations to hosts that do not support compression. Therefore, if you need to move a replication source VM to an ESXi host earlier than 6.0, before you perform the vMotion operation, you must reconfigure the replication to disable data compression.

CONFIGURE RECOVERY POINT OBJECTIVE (RPO) FOR A PROTECTED VIRTUAL MACHINE

You can change the **RPO settings** and enable the **Point in time instances** on this screen. (follow the "***Configure vSphere Replication for Single/Multiple VMs***" below)



VMware VR allows RPO from 5 min up to 24 hours.

MANAGE SNAPSHOTS ON RECOVERED VIRTUAL MACHINES

vSphere Replication does not maintain virtual machine snapshot hierarchy at the secondary site.

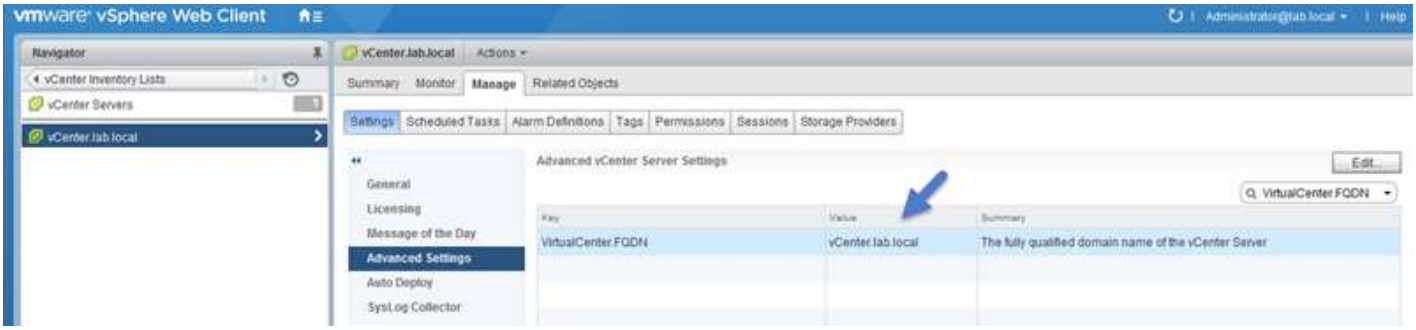
Writes are replicated, so vSphere Replication does not know what snapshots are. As such, snapshots are not replicated. When the VM is accessed at the recovery side, it is like the snapshots have been collapsed.

INSTALL/CONFIGURE/UPGRADE VSPHERE REPLICATION

vSphere Replication is distributed as ISO. Mount the ISO to access the OVF file to be deployed.

Requirements:

- Source and target site must have vSphere web client and the client integration plugin is installed as well.
- **Select the vCenter Server instance** on which you are deploying vSphere Replication, click **Manage** > **Settings > Advanced Settings**, and verify that the **VirtualCenter.FQDN** value is set to a **fully-qualified domain name** or a literal address.

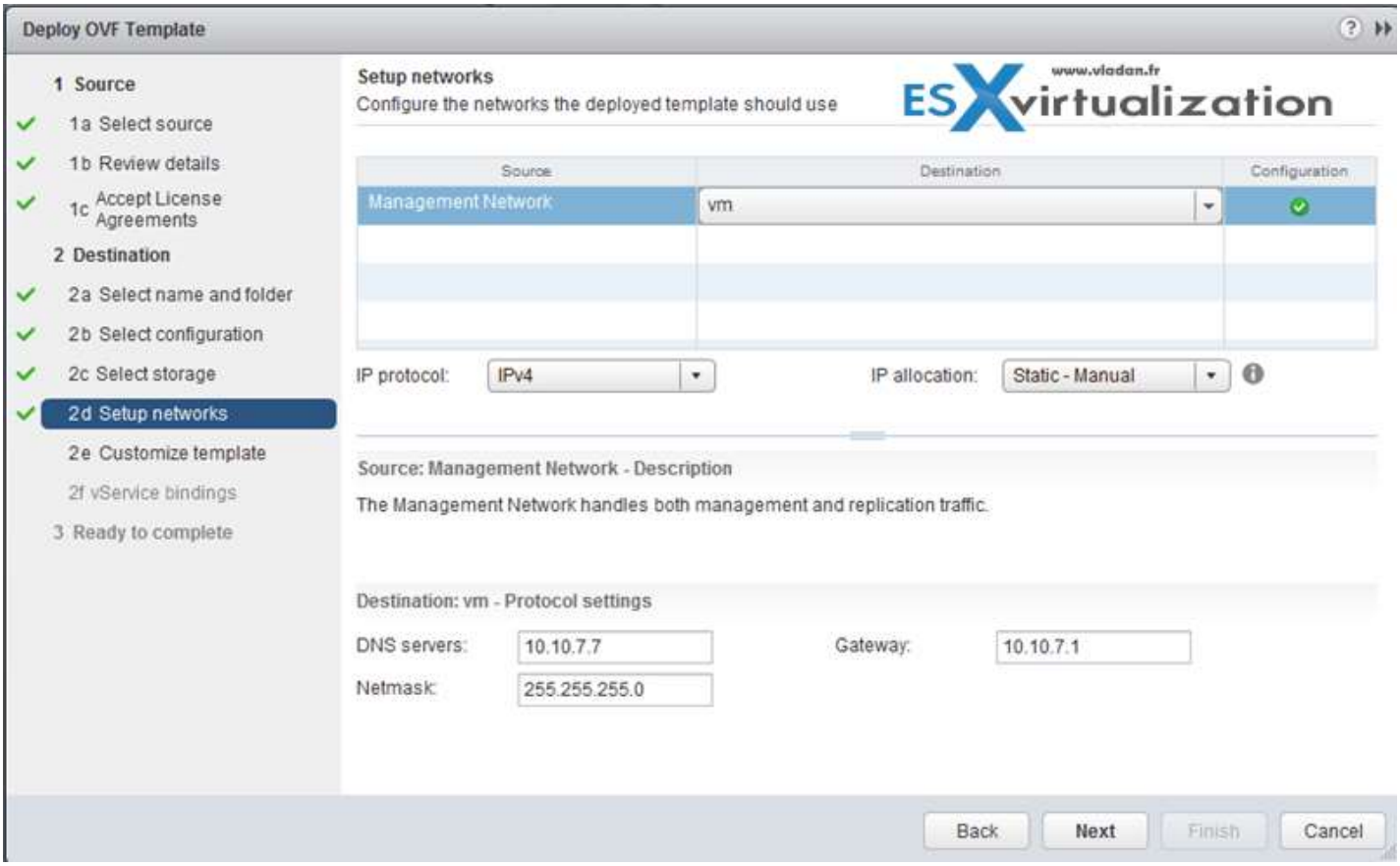


- **Network ports** – For a list of all the ports that must be open for vSphere Replication, see https://kb.vmware.com/kb/2087769.
- **Bandwidth** – vSphere Replication transfers blocks based on the RPO schedule. If you set an RPO of one hour, vSphere Replication transfers any block that has changed in that hour to meet that RPO. vSphere Replication only transfers the block once in its current state at the moment that vSphere Replication creates the bundle of blocks for transfer. vSphere Replication only registers that the block has changed within the RPO period, not how many times it changed.

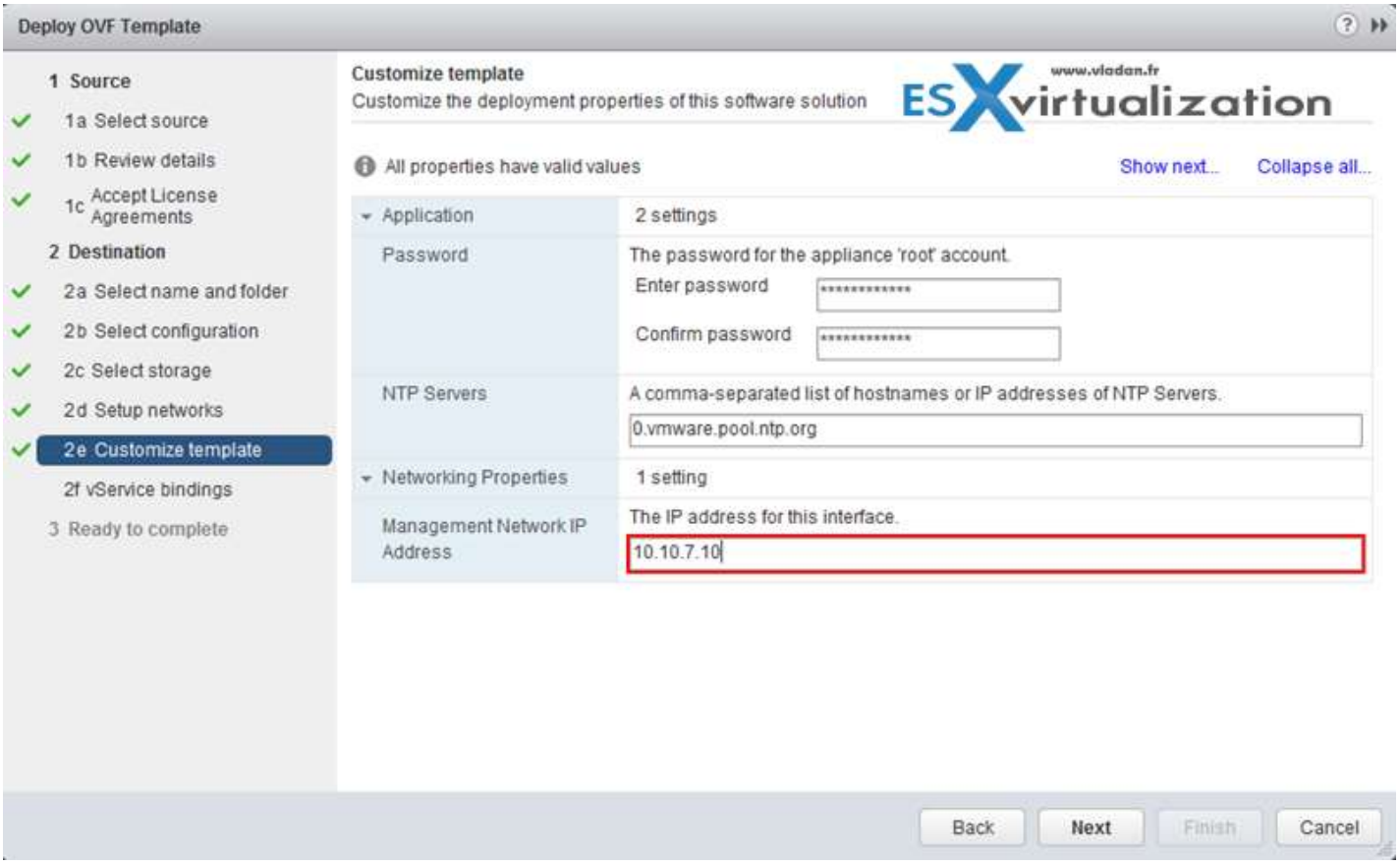
VSPHERE REPLICATION DEPLOYMENT

Select cluster and then **Actions > Deploy OVF template > local file > browse**… and so on…

If you don't want to rely on the DHCP you can use fixed IP…. Select a network from the list of available networks, set the IP protocol and IP allocation, and click Next. vSphere Replication supports both DHCP and static IP addresses. You can also change network settings by using the virtual appliance management interface (VAMI) after installation.



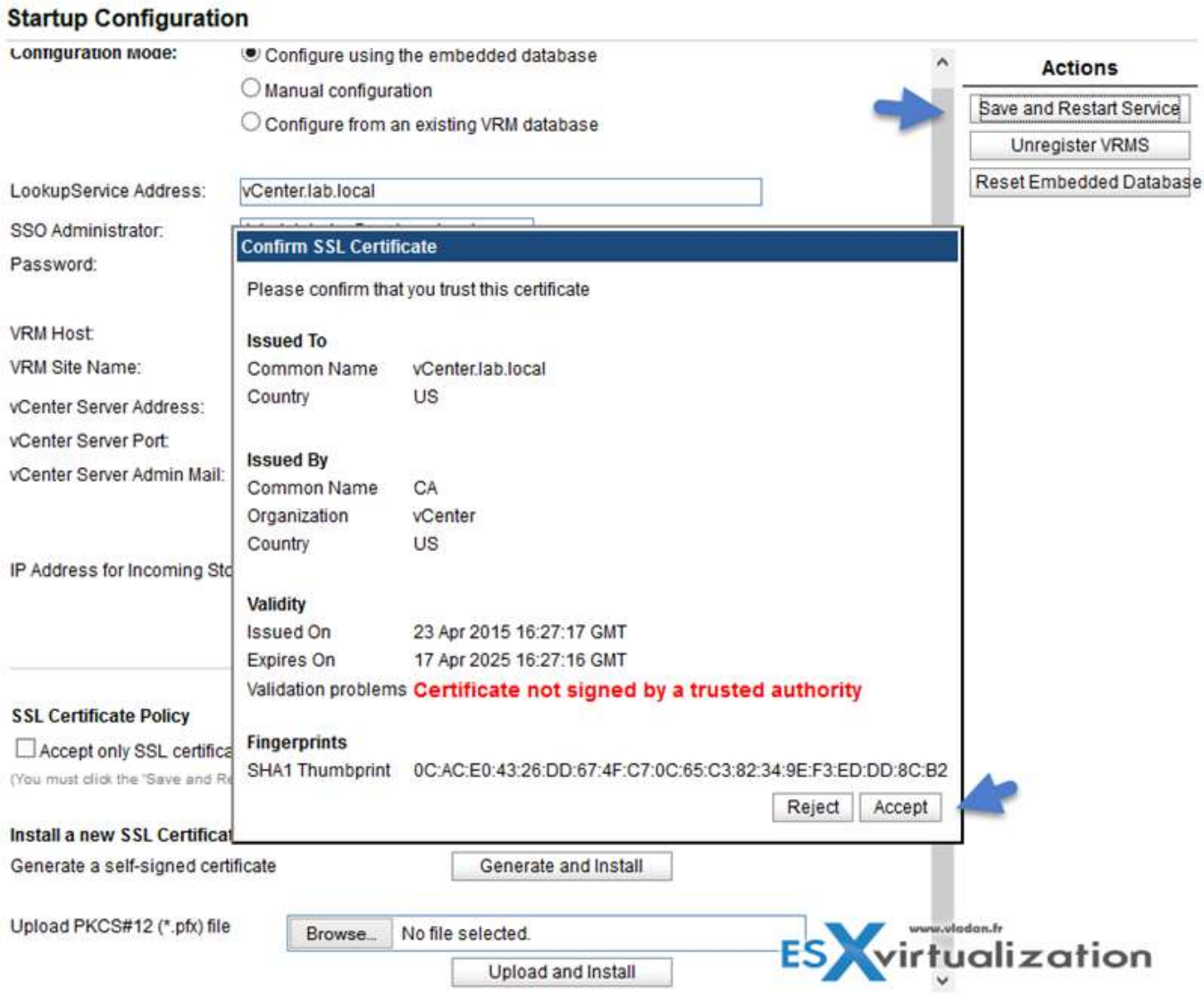
And then



Once done, log off and log back again to see the VR plugin

CONFIGURE VMWARE CERTIFICATE AUTHORITY (VMCA) INTEGRATION WITH VSPHERE REPLICATION

You can change the SSL certificate, for example, if your company's security policy requires that you use trust by validity and thumbprint or a certificate signed by a certification authority. You change the certificate **by using the virtual appliance management interface (VAMI) of the vSphere Replication appliance**.

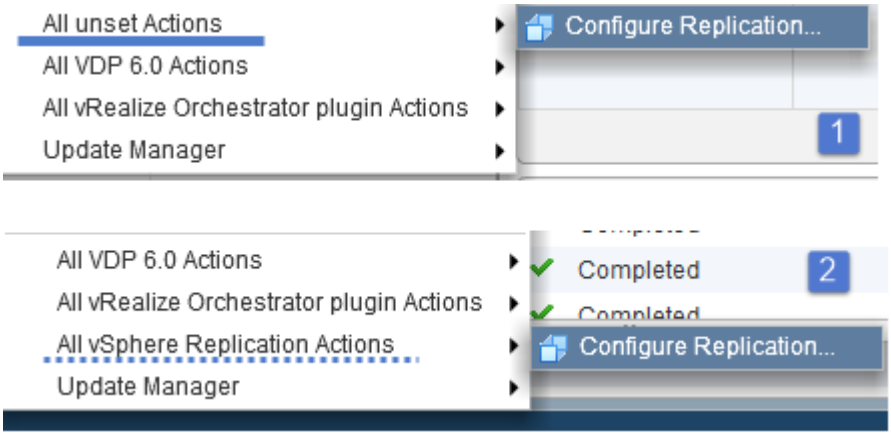


CONFIGURE VSPHERE REPLICATION FOR SINGLE/MULTIPLE VMS

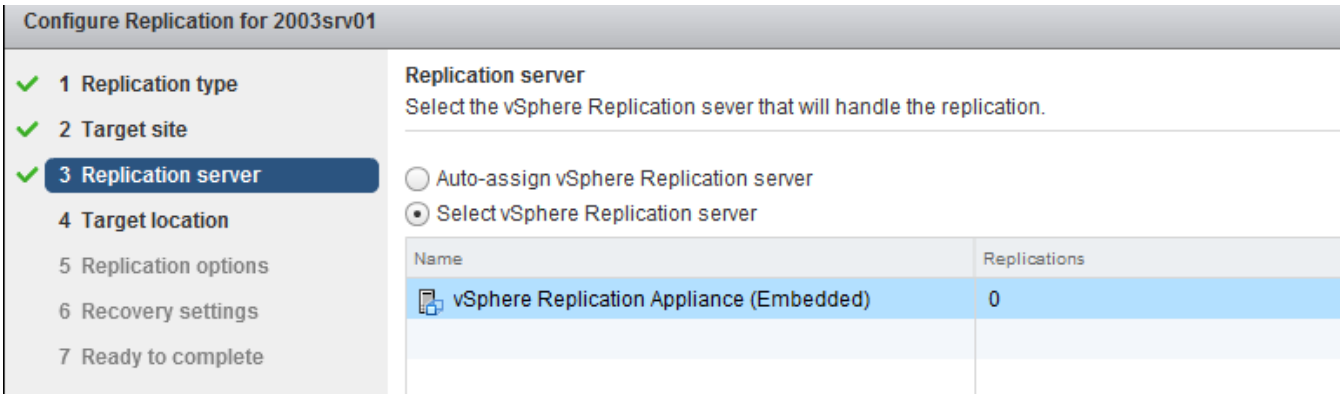
Before this, make sure that you have the permissions.

Step 1: Select VM(s) > Right click > All vSphere Replication Actions > configure Replication

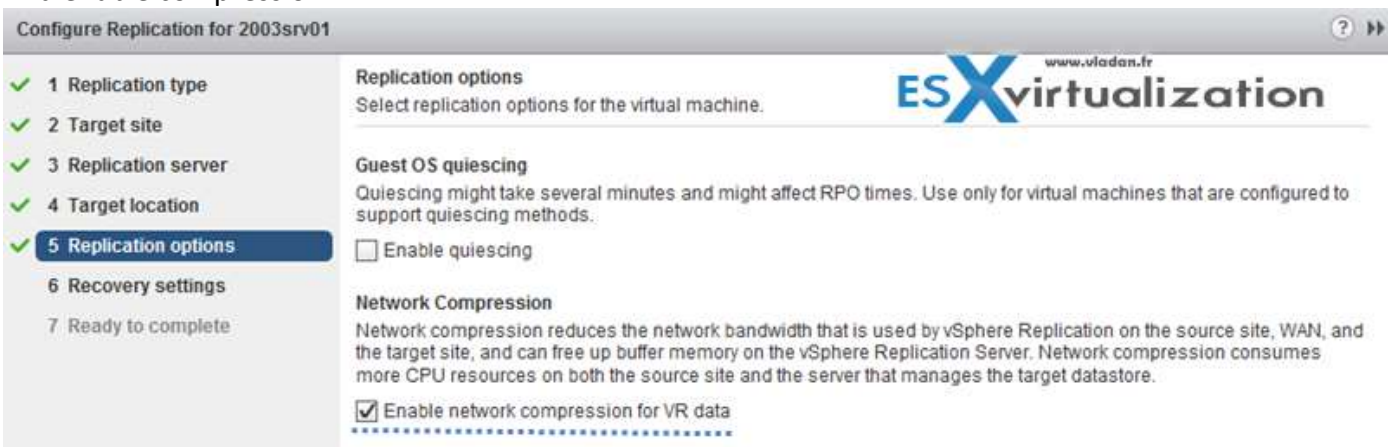
Now if you **haven't restarted the vCenter service**, you see this (1) because after restart you should see this (2). Also, you'll get some error on the permissions if you don't restart, and so you won't be able to configure the replication for your VMs. That "from the field" experience …



Step 2: Replicate to a **vCenter server** (or service provider) > **select target site** > target location…



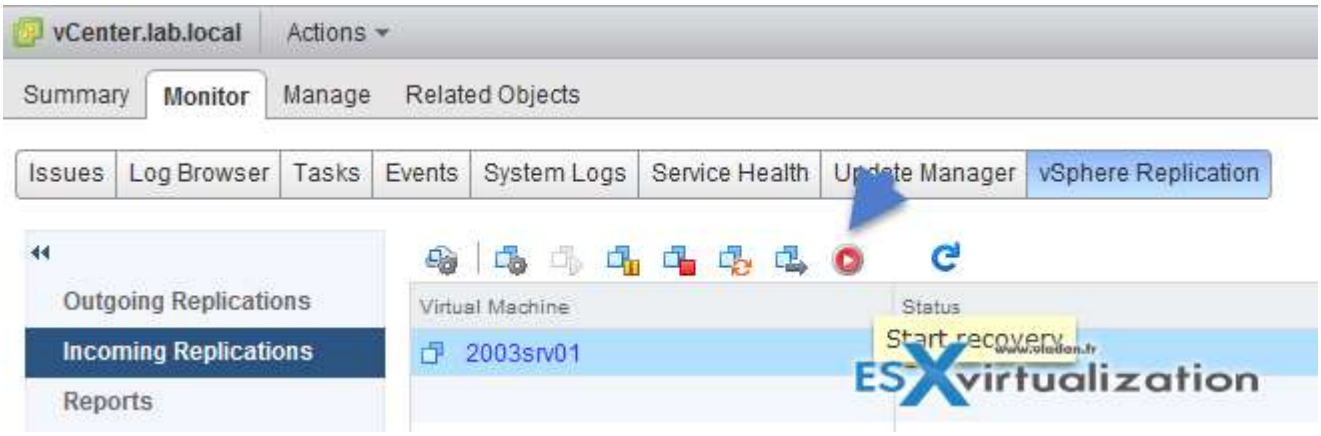
And enable compression…



Recover a VM using vSphere Replication

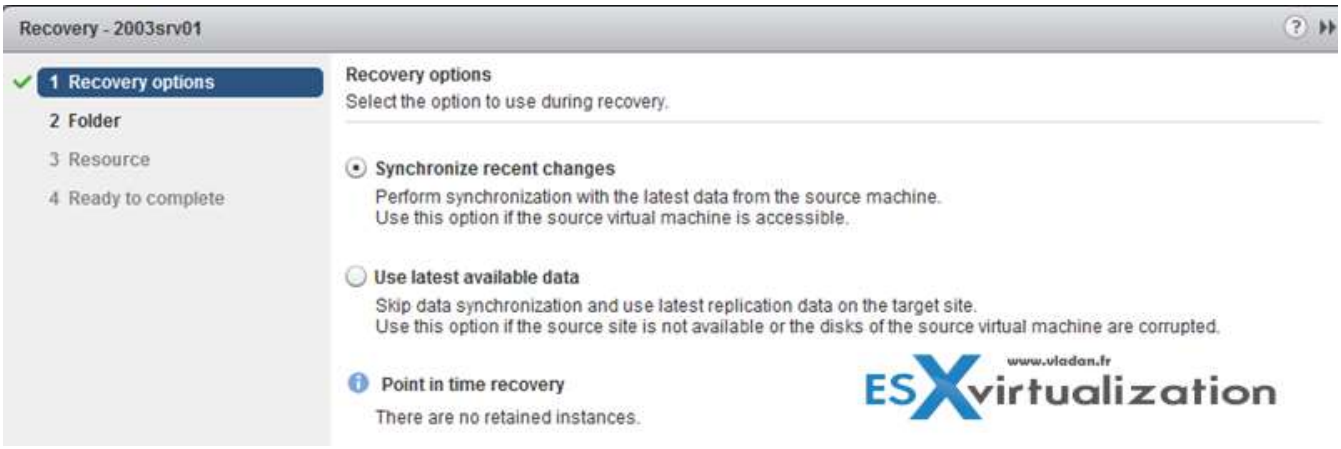
With VR, you can recover virtual machines that were successfully replicated at the target site. You can recover one virtual machine at a time.

Web client > **vSphere replication** > **Home tab** > **Monitor > Incoming replication**



From there you have two options:

1. **Recover with recent changes** – Performs a full synchronization of the virtual machine from the source site to the target site before recovering the virtual machine. Selecting this option avoids data loss, but it is only available if the data of the source virtual machine is accessible. You can only select this option if the virtual machine is powered off.
2. **Recover with latest available data** – Recovers the virtual machine by using the data from the most recent replication on the target site, without performing synchronization. Selecting this option results in the loss of any data that has changed since the most recent replication. Select this option if the source virtual machine is inaccessible or if its disks are corrupted.



You continue and select folder where you want to recover the VM…

Perform a failback operation using vSphere Replication

Failback is manual, it means that after performing a successful recovery on the target vCenter Server site, you can perform failback.

You log in to the target site and **manually configure a new replication in the reverse direction, from the target site to the source site.**

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

Deploy a pair of vSphere Replication virtual appliances

Same as above.

VCP6.5-DCV Objective 7.1 - Troubleshoot vCenter Server and ESXi Hosts

Understand VCSA monitoring tool

You can monitor VCSA through the VAMI user interface which is accessible through the well-known port 5480. So in order to connect there, use this format:

https://IP_or_FQDN:5480

You'll need to provide a root password for the connection. This UI is different and uses different credentials from the vSphere web client login. In some cases you are having problems accessing the web client UI, but the VAMI user interface works as usually.

That's where you can have a look in case you have problems as the UI gives you access to the services status, and you can monitor CPU, network and disk space usage there.

After logging in you can:

- Reboot and (or) shut down the VCSA appliance
- Upgrade/patch the appliance
- Create a vCenter Support Bundle
- Initiate file-level VCSA backup which saves configuration data.
- There is also a Health Status widget

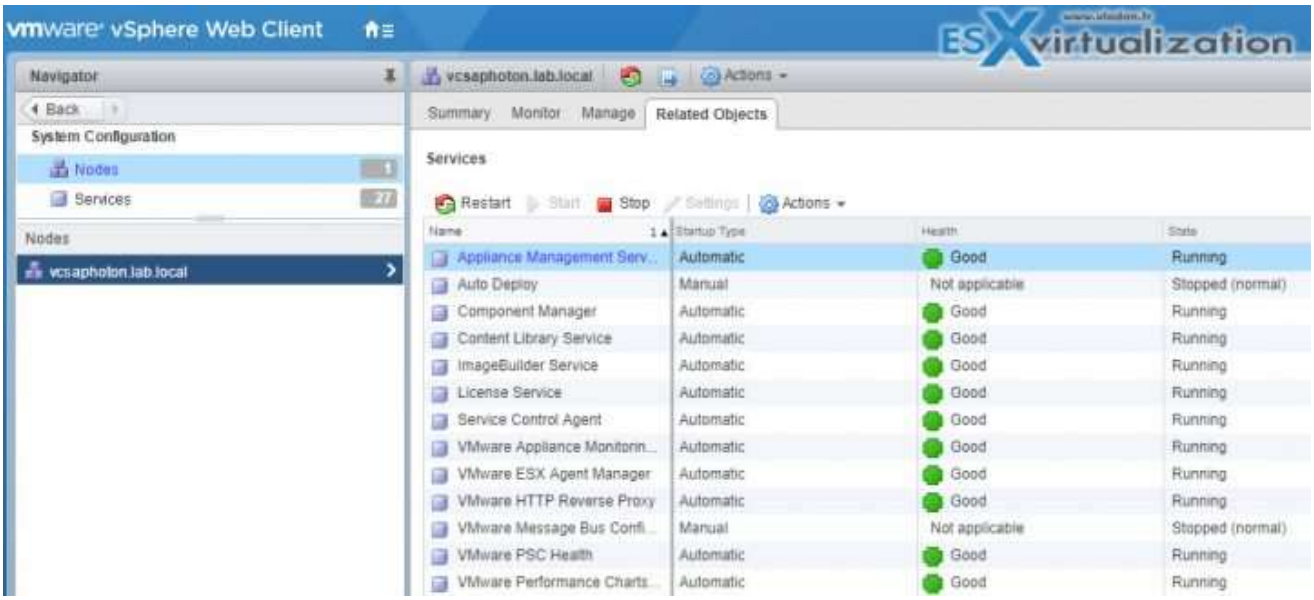
Monitor status of the vCenter Server services

It's possible to visualize the badge showing the status of the most important vCenter server services. For checking the status of vCenter services you must be a member of the SystemConfiguration.Administrators group in the vCenter Single Sign-On domain.

Home > System Configuration Icon

You get to a view where you can further click on the Nodes and Services.

Then you can **click** on **Nodes** > select and **Click the node** > On the right side click the **Related Objects TAB**.



You can see different status such as warnings (yellow) or critical (red). You have a possibility to start or restart a service manually and configure service startup to start with the system. By clicking the individual service, you can see the details about each service.

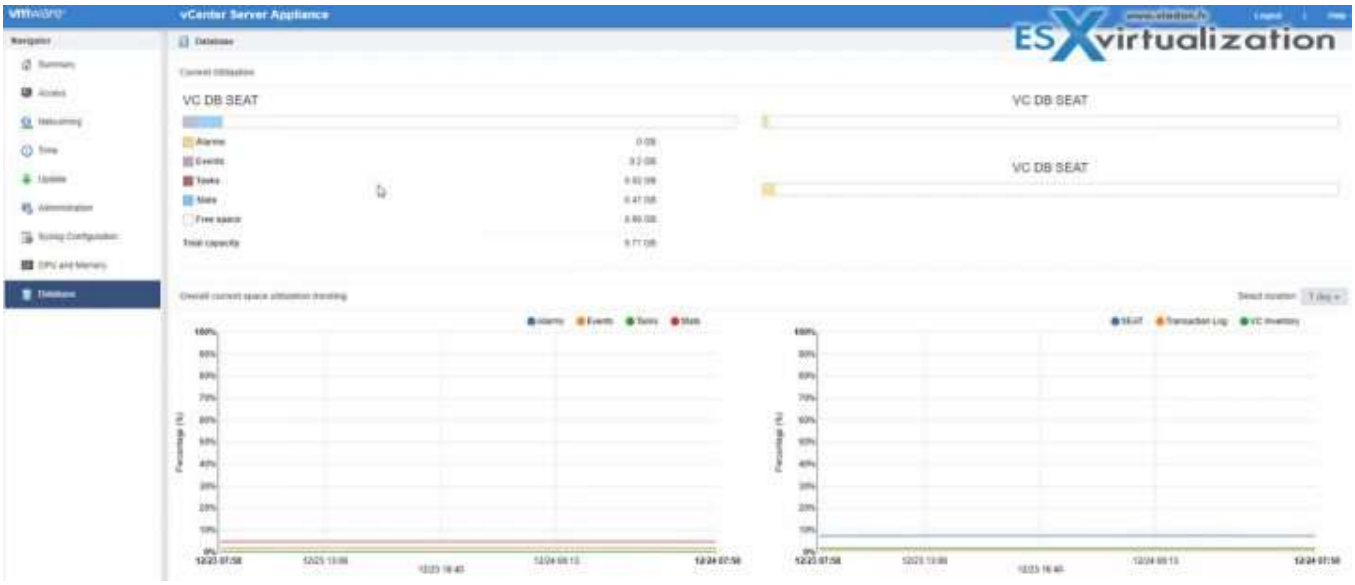
PERFORM BASIC MAINTENANCE OF A VCENTER SERVER DATABASE

vCenter Server database instance and vCenter Server needs some attention when backing up, but it's a necessary step to back up your vCenter server DB before doing any upgrade processes.

One of the usual database maintenance tasks might be one of those below:

- Performing a backup on regular basis (check your vendor's DB docs on that).
- Check the growth of the log file and compact the database log file, if necessary.
- You should be backing up the database before any vCenter Server upgrade.

For VCSA, there is not much to do as Postgre SQL is auto-managed by VCSA and no specific DB tasks are necessary. You can monitor Postgre SQL DB via VAMI UI.



Monitor status of ESXi management agents

From vSphere documentation:

The vCenter Solutions Manager displays the vSphere ESX Agent Manager agents that you use to deploy and manage related agents on ESX hosts.

An administrator uses the solutions manager to keep track of whether a solution's agents are working as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and a list of issues.

When a solution's state changes, the solutions manager update the ESX Agent Manager's summary status and state. Administrators use this status to track whether the goal state is reached.

The agency's health status is indicated by a specific color:

Red - The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution. The solution alerts the administrator to power on the agent.

Yellow - The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.

Green - A solution and all its agents reached the goal state.

Determine ESXi host stability issues and gather diagnostics information

In this section, we'll have a look at **Troubleshooting vSphere HA Host States**.

vCenter Server shows some error messages for vSphere HA host states. Each error message means something different error messages. If there is an error, vSphere HA cannot engage and protect VMs on the host. Those VMs cannot be restarted on other hosts in the cluster.

TIP: Fix 3 Warning Messages when deploying ESXi hosts in a lab

Those errors might occur when activating or deactivating HA on the cluster. When this happens, you should determine how to resolve the error, so that vSphere HA is fully operational.

Troubleshooting vSphere Auto Deploy - The vSphere Auto Deploy troubleshooting topics offer solutions for situations when provisioning hosts with vSphere Auto Deploy does not work as expected.

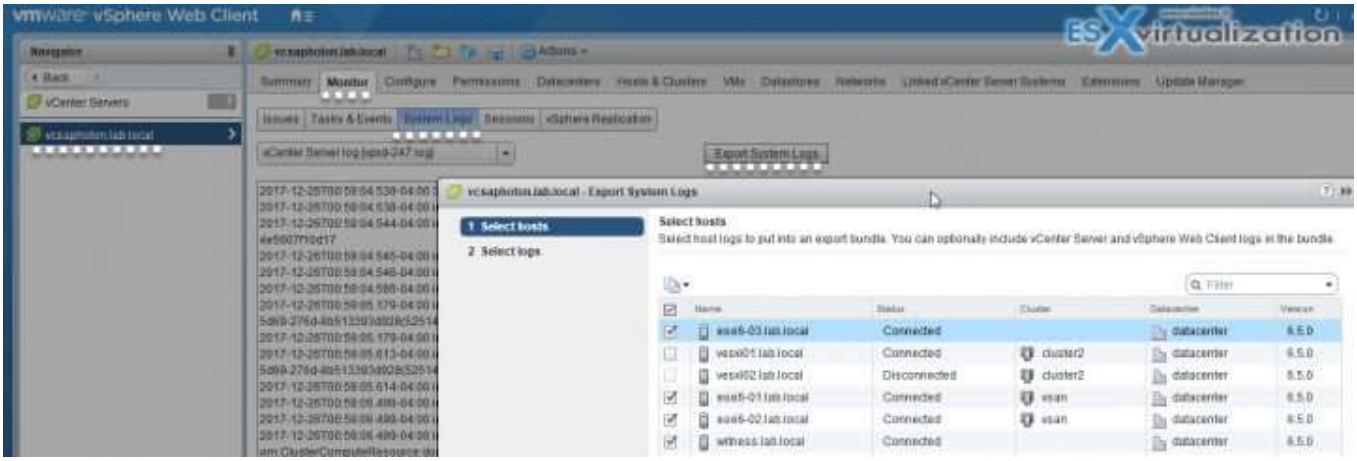
- **Authentication Token Manipulation Error** - Creating a password that does not meet the authentication requirements of the host causes an error.
- **Active Directory Rule Set Error Causes Host Profile Compliance Failure** - Applying a host profile that specifies an Active Directory domain to join causes a compliance failure.
- **Unable to Download VIBs When Using vCenter Server Reverse Proxy** - You are unable to download VIBs if vCenter Server is using a custom port for the reverse proxy.

VMware support bundles.

VMware Technical Support routinely requests diagnostic information from you when a support request is handled. This diagnostic information contains product specific logs, configuration files, and data appropriate to the situation. The information is gathered using a specific script or tool for each product and can include a host support bundle from the ESXi host and vCenter Server support bundle. Data collected in a host support bundle may be considered sensitive. Additionally, as of vSphere 6.5, support bundles can include encrypted information from an ESXi host. For more information on support bundles.

How To collect ESX/ESXi and vCenter Server diagnostic data?

vSphere Web Client > Inventory Lists, select vCenter Servers > Click the vCenter Server that manages the ESX/ESXi hosts from which you want to export logs > **Monitor** tab > **System Logs** > Click **Export System Logs** > **Select the ESX/ESXi hosts** > Select the **Include vCenter Server** and **vSphere Web Client logs** option (optional) > Click **Next.**



Select **Gather performance data** to include performance data information in the log files. You can update the duration and interval time between which you want to collect the data > **Next** >
Click Generate Log Bundle.

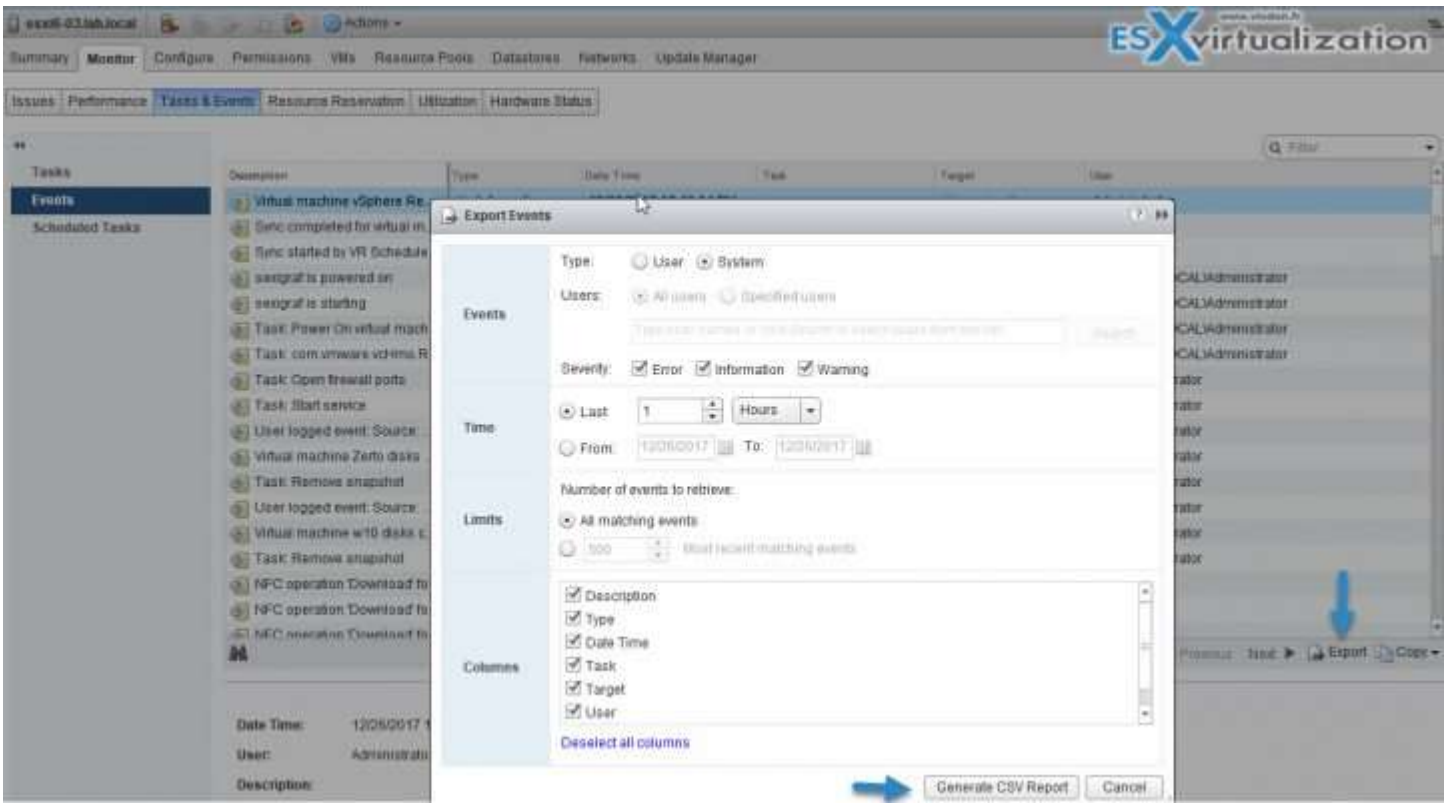
The Download Log Bundles dialog appears when the Generating Diagnostic Bundle task completes.

Click Download Log Bundle to save it to your local computer. The host or vCenter Server generates .zip bundles containing the log files. The Recent Tasks panel shows the Generate diagnostic bundles task in progress.

After the download completes, click Finish or generate another log bundle.

To export the events log:

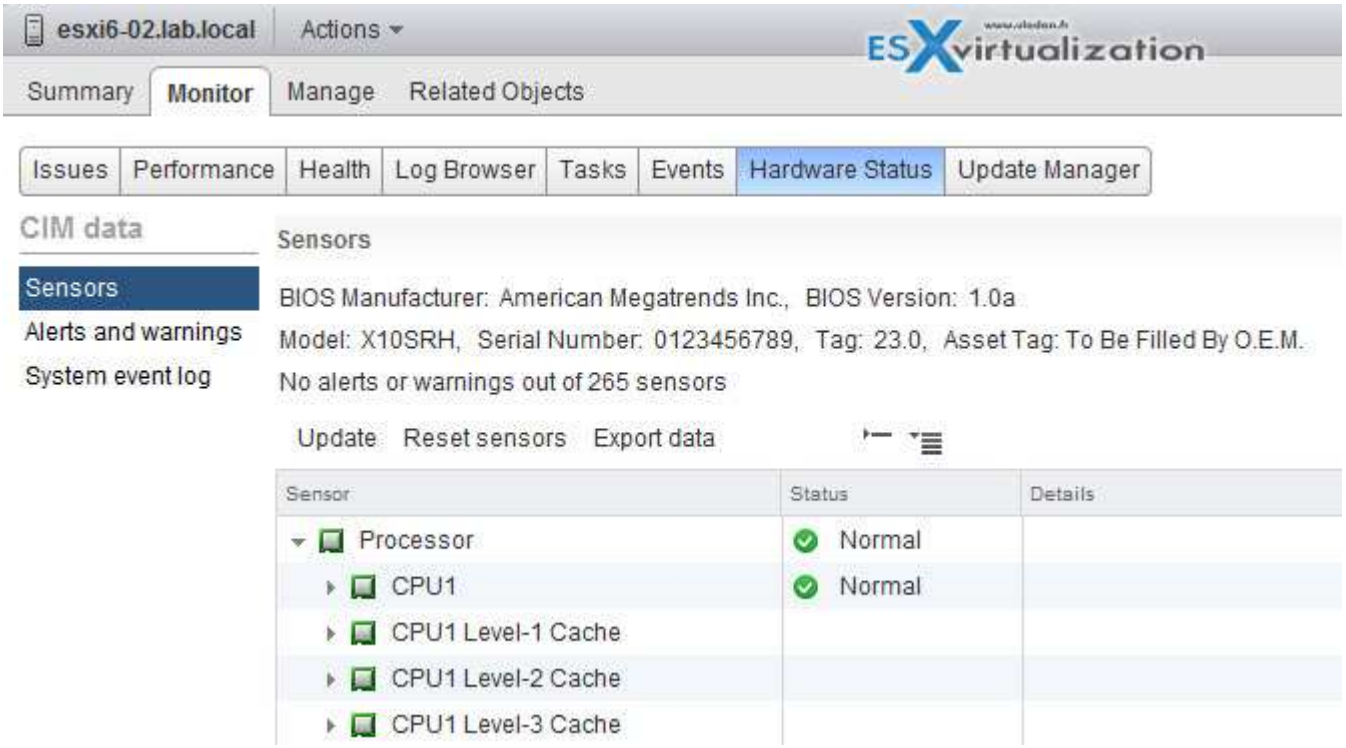
Select an inventory object > Click the Monitor tab, and click Tasks and Events > Events > Click the Export icon > In the **Export Events** window, specify what types of event information you want to export. Click Generate CSV Report, and click Save. Specify a file name and location and save the file.



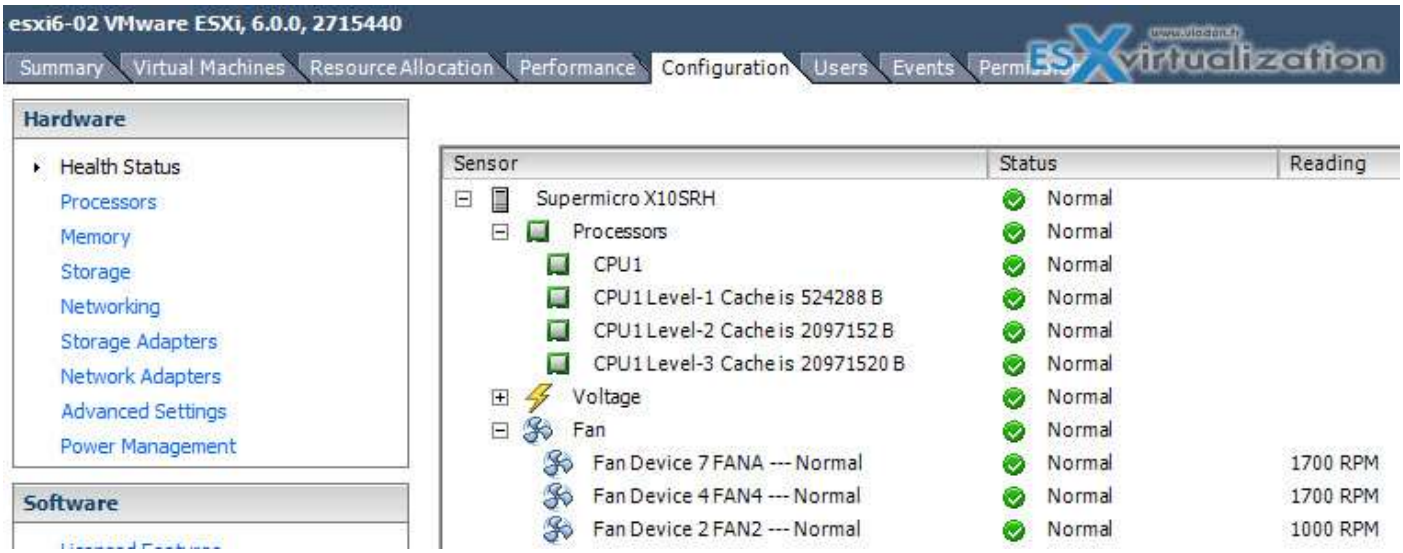
MONITOR ESXI SYSTEM HEALTH

vSphere uses Common Information Model (CIM) on ESXi instead of installing the hardware agents in the Service Console (well there is no Linux console since ages now). The different CIM providers are available for different hardware installed in the server (HBA, Network cards, Raid Controllers etc).

If connected through vCenter:



OR, If connected directly to the ESXi host:



LOCATE AND ANALYZE VCENTER SERVER AND ESXI LOGS

There are many ways to view ESXi system logs. To **view System Logs on an ESXi Host** you can:

- Use the direct console interface to view the system logs on an ESXi host. These logs provide information about system operational events. From the console, select View System Logs. Press a corresponding number key to view a log.

vCenter Server agent (vpxa) logs appear if the host is managed by vCenter Server.

Press Enter or the spacebar to scroll through the messages. You can also (optionally) do a regular expression search by pressing the slash key (/) and type the text to find. Then hit Enter to find the highlighted text on the screen.

To exit the search, just press **q** to return to the direct console.

View vCenter System Log Entries

In the vSphere Web Client, navigate to a vCenter Server > From the Monitor tab, click System Logs > From the drop-down menu, select the log and entry you want to view > Common Logs.

Determine appropriate commands for troubleshooting

The CLI commands is a vast chapter.

Depending what you want to do, which part of the infrastructure you are targeting:

- **vmkping** – simple ping via a vmkernel interface (ex. How-to troubleshoot iSCSI connection to your SAN)
- **vmkfstools** – works with VMFS volumes, VMDKs … (ex Recreate a missing VMDK header file)
- **esxcli network** <namespace> – (ex. How to create custom ESXi Firewall rule)
- **esxcli storage** <namespace>- (ex. How to tag disk as SSD VMware esxi 5.x and 6.0)
- **esxtop** – performance monitoring – (ex. How-to check Queue Depth Of Storage Adapter or Storage Device)

The list of ESXi CLI commands is really vast. For reference, check our previous posts:

- ESXi Commands List – Getting started
- ESXi Commands List – networking commands
- ESXi Commands List – networking commands [Part 2]
- ESXi Commands List – Storage

Troubleshoot common issues, including:

- vCenter Server services
- Identity Sources
- vCenter Server connectivity
- Virtual machine resource contention, configuration and operation
- Platform Services Controller (PSC)
- Problems with installation
- VMware Tools installation
- Fault-Tolerant network latency
- KMS connectivity
- vCenter Certification Authority

You might work with an excellent PDF from VMware called "vSphere Troubleshooting". Do a search on Google to get the latest release. Section below is partly from this document.

There are many scenarios, in general, when it comes to troubleshooting. It would be really time-consuming (and impossible) to identify and invoke even small part of those scenarios. That's why I'll try to give a general guidance on vSphere troubleshooting.

At first, you need to Identify the symptoms. Know what's happen. If something is failing, then there must be an exact cause on that.

Some questions you ask when troubleshooting:

- What is the task or expected behavior that is not occurring?
- Can the affected task be divided into subtasks that you can evaluate separately?
- Is the task ending in an error? Is an error message associated with it?
- Is the task completing but in an unacceptably long time?
- Is the failure consistent or sporadic?
- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space - After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings
- Failure of physical hardware
- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions - After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.
- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.
- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.
- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.

- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.
- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Today's topic VCP6.5-DCV Objective 7.1 - Troubleshoot vCenter Server and ESXi Hosts is a very large, sometimes "painful" topic to learn. Try to install few ESXi hosts in a nested environment and do some "hands-on" UI testing. Also, there are VMware Hands-on Labs or Ravello, if you don't have spare hardware at home.

VCP6.5-DCV Objective 7.2 - Troubleshoot vSphere Storage and Networking

Identify and isolate network and storage resource contention and latency issues

We'll heavily use VMware PDF called "vSphere Troubleshooting". You'll find it on Google. There are several places which can slow performance of your storage:

SAN Performance Problems - A number of factors can negatively affect storage performance in the ESXi SAN environment. Among these factors are excessive SCSI reservations, path thrashing, and inadequate LUN queue depth.

To monitor storage performance in real time, use the resxtop and esxtop command-line utilities. For more information, see the vSphere Monitoring and Performance documentation.

Excessive SCSI Reservations Cause Slow Host Performance - When storage devices do not support the hardware acceleration, ESXi hosts use the SCSI reservations mechanism when performing operations that require a file lock or a metadata lock in VMFS. SCSI reservations lock the entire LUN. Excessive SCSI reservations by a host can cause performance degradation on other servers accessing the same VMFS.

Excessive SCSI reservations cause performance degradation and SCSI reservation conflicts - Several operations require VMFS to use SCSI reservations:

- Creating, resignaturing, or expanding a VMFS datastore.
- Powering on a virtual machine.
- Creating or deleting a file.
- Creating a template.
- Deploying a virtual machine from a template.
- Creating a new virtual machine.
- Migrating a virtual machine with VMotion.
- Growing a file, such as a thin provisioned virtual disk.

To eliminate potential sources of SCSI reservation conflicts, follow these guidelines:

- Serialize the operations of the shared LUNs, if possible, limit the number of operations on different hosts that require SCSI reservation at the same time.
- Increase the number of LUNs and limit the number of hosts accessing the same LUN.
- Reduce the number snapshots. Snapshots cause numerous SCSI reservations.
- Reduce the number of virtual machines per LUN. Follow recommendations in Configuration Maximums.

- Make sure that you have the latest HBA firmware across all hosts.
- Make sure that the host has the latest BIOS.
- Ensure a correct Host Mode setting on the SAN array.

Path Thrashing Causes Slow LUN Access - If your ESXi host is unable to access a LUN, or access is very slow, you might have a problem with path thrashing, also called LUN thrashing.

Your host is unable to access a LUN, or access is very slow. The problem might be caused by path thrashing. Path thrashing might occur when two hosts access the same LUN through different storage processors (SPs) and, as a result, the LUN is never available.

Path thrashing typically occurs on active-passive arrays. Path thrashing can also occur on a directly connected array with HBA failover on one or more nodes. Active-active arrays or arrays that provide transparent failover do not cause path thrashing.

- Ensure that all hosts that share the same set of LUNs on the active-passive arrays use the same storage processor.
- Correct any cabling or masking inconsistencies between different hosts and SAN targets so that all HBAs see the same targets.
- Ensure that the claim rules defined on all hosts that share the LUNs are exactly the same.
- Configure the path to use the Most Recently Used PSP, which is the default.
- Increased Latency for I/O Requests Slows Virtual Machine Performance

If the ESXi host generates more commands to a LUN than the LUN queue depth permits, the excess commands are queued in VMkernel. This increases the latency, or the time taken to complete I/O requests.

The host takes longer to complete I/O requests and virtual machines display unsatisfactory performance.

The problem might be caused by an inadequate LUN queue depth. SCSI device drivers have a configurable parameter called the **LUN queue depth** that determines how many commands to a given LUN can be active at one time. If the host generates more commands to a LUN, the excess commands are queued in the VMkernel.

If the sum of active commands from all virtual machines consistently exceeds the LUN depth, increase the queue depth.
The procedure that you use to increase the queue depth depends on the type of storage adapter the host uses.

When multiple virtual machines are active on a LUN, change the "Disk.SchedNumReqOutstanding" (DSNRO) parameter, so that it matches the queue depth value.

Resolving Network Latency Issues - Networking latency issues could potentially be caused by the following infrastructure elements:

- External Switch
- NIC configuration and bandwidth (1G/10G/40G)
- CPU contention

VERIFY NETWORK AND STORAGE CONFIGURATION

Today's topic VCP6.5-DCV Objective 7.2 - Troubleshoot vSphere Storage and Networking, is really hard topic. You must have some experience with working with VMware vSphere environment and from labs. I highly encourage our readers who want to pass this exam, to get a home lab or do as much as Online Labs as you can in order to get to know vSphere environment.

For troubleshooting, you should Start from one end. Either from the host level > physical switch > uplinks > switches > port groups > VMs. Or from the other side.

- **Check the vNIC status** – connected/disconnected
- **Check the networking config inside Guest OS** – yes it might also be one of the issues. Bad network config of the networking inside of a VM.
- Verify physical switch config.
- Check the vSwitch or vDS config.
- ESXi host network (uplinks).
- Check Guest OS config.

In Windows VM do this:

Click on **Start** > **Run** > **"devmgmt.msc"** > click **+** next to **network adapters** > check if it's not disabled or not present.

You can also check the network config like IP address, Netmask, default gateway and DNS servers. Make sure that that information are correct.

- **If a VM was P2V** – check if there are no "ghosted adapters". To check that:

On your VM go to Start > RUN > CMD > Enter > Type:

set devmgr_show_nonpresent_devices=1

While still in the command prompt window type:

devmgmt.msc

and then **open Device Manager** and click **on the Menu** go to **View > Show Hidden Devices** (like on the pic).

Then you should see which devices are marked like ghosted devices. **They are grayed out**. Those devices you can safely remove from the device manager.

- **Check IP stack** – It happened to me several times that the IP stack of a VM was corrupted. The VM has had intermittent networking connectivity, everything seems to be ok but isn't. You can clear the local cache by entering this:

ipconfig /renew

For Linux:

dhclient -r
dhclient eth0

VERIFY STORAGE CONFIGURATION

VERIFY THE CONNECTION STATUS OF A STORAGE DEVICE

Use the esxcli command to verify the connection status of a particular storage device. Install vCLI or deploy the vSphere Management Assistant (vMA) virtual machine. See ***Getting Started with vSphere Command-Line Interfaces***. For troubleshooting, run esxcli commands in the ESXi Shell.

Run the command:

esxcli –server=***server_name*** storage core device list -d=***device_ID***

Review the connection status in the Status: area.

- **on** – Device is connected.
- **dead** – Device has entered the APD state. The APD timer starts.
- **dead timeout** – The APD timeout has expired.
- **not connected** – Device is in the PDL state.

VERIFY THAT A GIVEN VIRTUAL MACHINE IS CONFIGURED WITH THE CORRECT NETWORK RESOURCES

Same as above section (for Windows and/or Linux VM).

MONITOR/TROUBLESHOOT STORAGE DISTRIBUTED RESOURCE SCHEDULER (SDRS) ISSUES

Storage Issues – Check that the virtual machine has no underlying issues with storage or it is not experiencing resource contention, as this might result in networking issues with the virtual machine. You can do this by logging into ESX/ESXi or Virtual Center/vCenter Server using the VI/vSphere Client and logging into the virtual machine console.

Storage DRS is Disabled on a Virtual Disk - Even when Storage DRS is enabled for a datastore cluster, **it might be disabled** on some virtual disks in the datastore cluster. You have enabled Storage DRS for a datastore cluster, but Storage DRS is disabled on one or more virtual machine disks in the datastore cluster.

There can be some scenarios which can cause Storage DRS to be disabled on a virtual disk.

(Sections below from VMware documentation.)

- A virtual machine's swap file is host-local (the swap file is stored in a specified datastore that is on the host). The swap file cannot be relocated and Storage DRS is disabled for the swap file disk.
- A certain location is specified for a virtual machine's .vmx swap file. The swap file cannot be relocated and Storage DRS is disabled on the .vmx swap file disk.

- The relocate or Storage vMotion operation is currently disabled for the virtual machine in vCenter Server (for example, because other vCenter Server operations are in progress on the virtual machine). Storage DRS is disabled until the relocate or Storage vMotion operation is re-enabled in vCenter Server.
- The home disk of a virtual machine is protected by vSphere HA and relocating it will cause loss of vSphere HA protection.
- The disk is a CD-ROM/ISO file.
- If the disk is an independent disk, Storage DRS is disabled, except in the case of relocation or clone placement.
- If the virtual machine has system files on a separate datastore from the home datastore (legacy), Storage DRS is disabled on the home disk. If you use Storage vMotion to manually migrate the home disk, the system files on different datastores will be all be located on the target datastore and Storage DRS will be enabled on the home disk.
- If the virtual machine has a disk whose base/redo files are spread across separate datastores (legacy), Storage DRS for the disk is disabled. If you use Storage vMotion to manually migrate the disk, the files on different datastores will be all be located on the target datastore and Storage DRS will be enabled on the disk.
- The virtual machine has hidden disks (such as disks in previous snapshots, not in the current snapshot). This situation causes Storage DRS to be disabled on the virtual machine.
- The virtual machine is a template.
- The virtual machine is vSphere Fault Tolerance-enabled.
- The virtual machine is sharing files between its disks.
- The virtual machine is being Storage DRS-placed with manually specified datastores.

Storage DRS Cannot Operate on a Datastore - Storage DRS generates an alarm to indicate that it cannot operate on the datastore. Storage DRS generates an event and an alarm and Storage DRS cannot operate.

vCenter Server can disable Storage DRS for a datastore, in case:

- The datastore is shared across multiple data centers.

Storage DRS is not supported on datastores that are shared across multiple data centers. This configuration can occur when a host in one data center mounts a datastore in another data center, or when a host using the datastore is moved to a different data center. When a datastore is shared across multiple data centers, Storage DRS I/O load balancing is disabled for the entire datastore cluster. However, Storage DRS space balancing remains active for all datastores in the datastore cluster that are not shared across data centers.

- The datastore is connected to an unsupported host.

Storage DRS is not supported on **ESX/ESXi 4.1 and earlier** hosts.

- The datastore is connected to a host that is not running Storage I/O Control.
- The datastore must be visible in only one data center. Move the hosts to the same data center or unmount the datastore from hosts that reside in other data centers.
- Ensure that all hosts associated with the datastore cluster are ESXi 5.0 or later.
- Ensure that all hosts associated with the datastore cluster have Storage I/O Control enabled.

Datastore Cannot Enter Maintenance Mode - You place a datastore in maintenance mode when you must take it out of usage to service it. A datastore enters or leaves maintenance mode only as a result of a user request. A data store in a datastore cluster cannot enter maintenance mode. The Entering Maintenance Mode status remains at 1%.

One or more disks on the datastore cannot be migrated with Storage vMotion. This condition can occur in the following instances.

- Storage DRS is disabled on the disk.
- Storage DRS rules prevent Storage DRS from making migration recommendations for the disk.
- If Storage DRS is disabled, enable it or determine why it is disabled.
- If Storage DRS rules are preventing Storage DRS from making migration recommendations, you can remove or disable particular rules.

How?

vSphere **Web Client object navigator > Click the Manage tab > Settings > Configuration > select Rules and click the rule > Click Remove.**

- Alternatively, if Storage DRS rules are preventing Storage DRS from making migration recommendations, you can set the Storage DRS advanced option IgnoreAffinityRulesForMaintenance to 1.
- Browse to the datastore cluster in the vSphere Web Client object navigator.
- Click the Manage tab and click Settings.
- Select SDRS and click Edit.
- In Advanced Options > Configuration Parameters, click Add.
- In the Option column, enterIgnoreAffinityRulesForMaintenance.
- In the Value column, enter 1 to enable the option.
- Click OK.

RECOGNIZE THE IMPACT OF NETWORK AND STORAGE I/O CONTROL CONFIGURATIONS

What's vSphere Storage I/O - vSphere Storage I/O Control allows cluster-wide storage I/O prioritization, which allows better workload consolidation and helps reduce extra costs associated with over-provisioning.

Storage I/O Control extends the constructs of shares and limits to handle storage I/O resources. You can control the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion, which ensures that more important virtual machines get preference over less important virtual machines for I/O resource allocation.

When you enable Storage I/O Control on a datastore, ESXi begins to monitor the device latency that hosts observe when communicating with that datastore. When device latency exceeds a threshold, the datastore is considered to be congested and each virtual machine that accesses that datastore is allocated I/O resources in proportion to their shares. You set shares per virtual machine. You can adjust the number for each based on need.

The I/O filter framework (VAIO) allows VMware and its partners to develop filters that intercept I/O for each VMDK and provides the desired functionality at the VMDK granularity. VAIO works along Storage Policy-Based Management (SPBM) which allows you to set the filter preferences through a storage policy that is attached to VMDKs.

By default, all virtual machine shares are set to Normal (1000) with unlimited IOPS. Storage I/O Control is enabled by default on Storage DRS-enabled datastore clusters.

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

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

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

The two traffic categories have different nature. System traffic is strictly associated with an ESXi host. The network traffic routes change when you migrate a virtual machine across the environment. To provide network resources to a virtual machine regardless of its host, in Network I/O Control you can configure resource allocation for virtual machines that is valid in the scope of the entire distributed switch.

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

Recognize a connectivity issue caused by a VLAN/PVLAN

If you're not familiar with VLANS/PVLANS, I can recommend reading Objective 2.1 – Configure policies/features and verify vSphere networking.

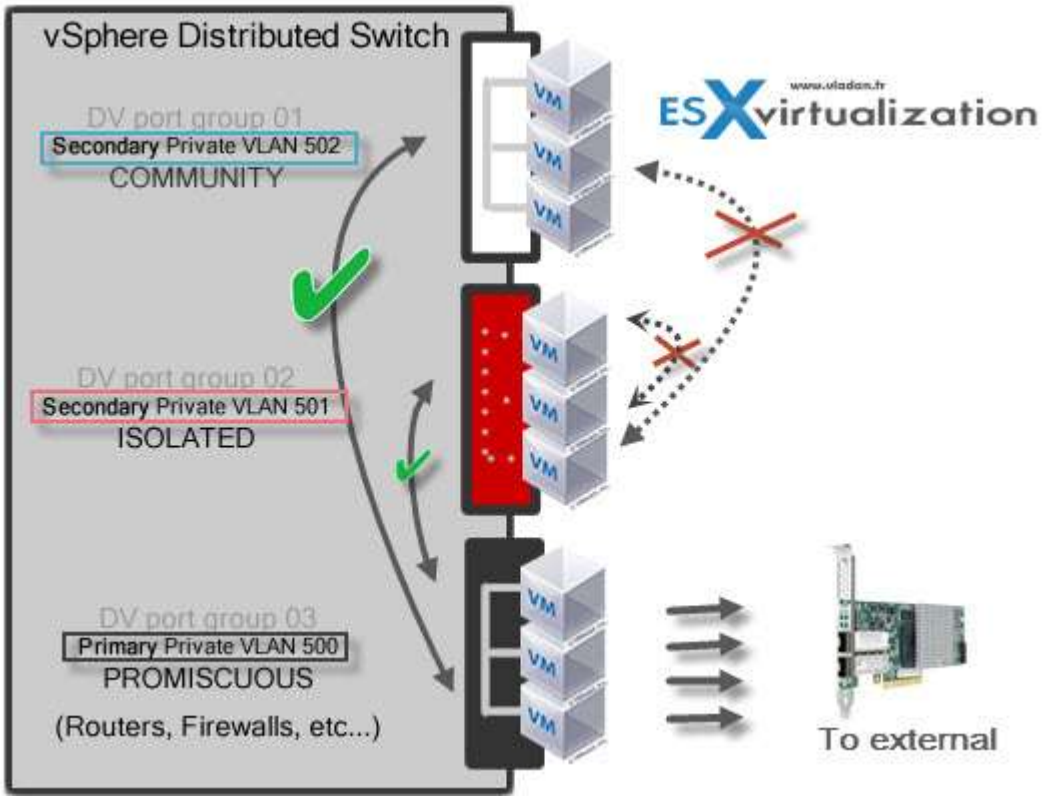
VLANs let you segment a network into multiple logical broadcast domains at Layer 2 of the network protocol stack. Virtual LANs (VLANs) enable a single physical LAN segment to be further isolated so that groups of ports are isolated from one another as if they were on physically different segments. Private VLANs are used to solve VLAN ID limitations by adding a further segmentation of the logical broadcast domain into multiple smaller broadcast subdomains.

The VLAN configuration in a vSphere environment allows you to:

- Integrates ESXi hosts into a pre-existing VLAN topology.
- Isolates and secures network traffic.
- Reduces congestion of network traffic.
- Private VLANs are used to solve VLAN ID limitations by adding a further segmentation of the logical broadcast domain into multiple smaller broadcast subdomains.

A private VLAN (PVLAN) is identified by its primary VLAN ID. A primary VLAN ID can have multiple secondary VLAN IDs associated with it. Primary VLANs are Promiscuous, so that ports on a private VLAN can communicate with ports configured as the primary VLAN. Ports on a secondary VLAN can be either Isolated, communicating only with promiscuous ports, or Community, communicating with both promiscuous ports and other ports on the same secondary VLAN.

The graphics show it all…



To use private VLANs between a host and the rest of the physical network, the physical switch connected to the host needs to be a private VLAN-capable and configured with the VLAN IDs being used by ESXi for the private VLAN functionality. For physical switches using dynamic MAC+VLAN ID based learning, all corresponding private VLAN IDs must be first entered into the switch's VLAN database.

Troubleshoot common issues with

- Storage and network - please refer to earlier sections.
- Virtual switch and port group configuration - same.
- Physical network adapter configuration - same.
- VMFS metadata consistency - Use vSphere On-disk Metadata Analyzer (VOMA) to identify incidents of metadata corruption that affect file systems or underlying logical volumes. You can check metadata consistency when you experience problems with a VMFS datastore or a virtual flash resource. (VMware KB article on using vSphere On-disk Metadata Analyzer.

A difficult chapter again, but necessary to know for the exam. Again, use the "vSphere Troubleshooting PDF" to go through.

VCP6.5-DCV Objective 7.3 - Troubleshoot vSphere Upgrades and Migrations

Collect upgrade diagnostic information

You can collect upgrade diagnostic information through logs being made during the installation/upgrade process. For VMware vCenter server appliance (VCSA) access the appliance shell. You can do so by pressing the Alt + F1 if you have access directly to the appliance.

If you want to connect remotely, you can use SSH and start a remote session. Once connected, run the pi shell command to access the Bash shell. In the Bash shell run the vc-support.sh script to generate a support bundle.

It generates a support bundle as .tgz in /var/tmp.

Export the generated support bundle to the user@x.x.x.x:/tmp folder.

scp /var/tmp/vc-etco-vm-vlan11-dhcp-63-151.eng.vmware.com-2014-02-28--21.11.tgz user@x.x.x.x:/tmp

Determine which firstboot script failed.

cat /var/log/firstboot/firstbootStatus.json

Collect Installation Logs by Using the Installation Wizard - You can use the Setup Interrupted page of the installation wizard to browse to the generated .zip file of the vCenter Server for Windows installation log files.

If the installation fails, the Setup Interrupted page appears with the log collection checkboxes selected by default.

Leave the check boxes selected and click Finish.

The installation files are collected in a .zip file on your desktop, for example, VMware-VCS-logs-time-of-installation-attempt.zip, where time-of-installation-attempt displays the year, month, date, hour, minutes, and seconds of the installation attempt. Get the log files from the .zip file on your desktop.

Manually get the logs - the installation directories

%PROGRAMDATA%\VMware\vCenterServer\logs directory, usually C:\ProgramData\VMware\vCenterServer\logs

%TEMP% directory, usually C:\Users\username\AppData\Local\Temp

The files in the %TEMP% directory include vc-install.txt, vminst.log, pkgmgr.log, pkgmgr-comp-msi.log, and vim-vcs-msi.log.

Open the installation log files in a text editor for examination.

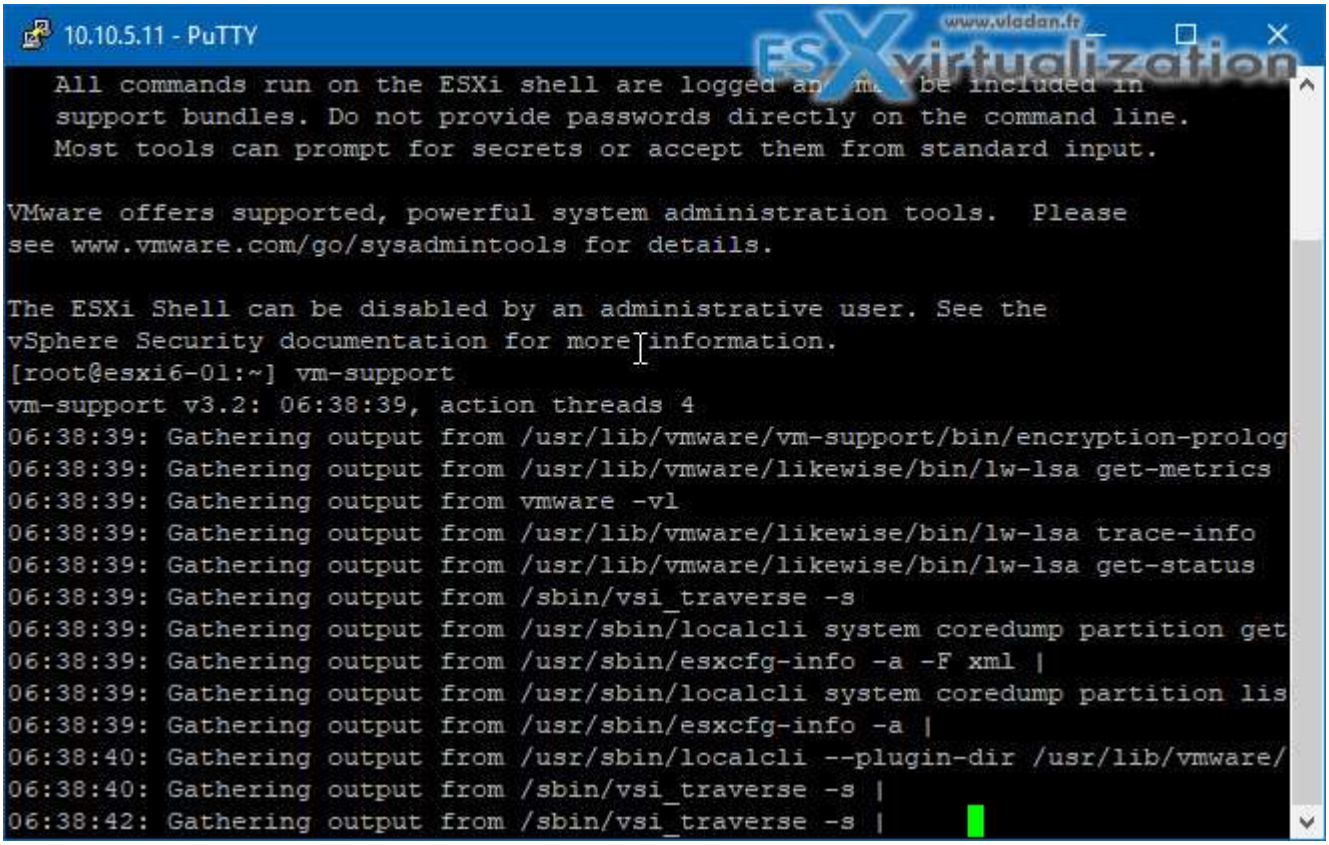
Collect Database Upgrade Logs - You can retrieve the database upgrade logs after you complete the vCenter Server upgrade process.

Navigate to the database upgrade log locations. Open the database upgrade logs in a text editor for examination.

Database Upgrade Locations:

- **For pre-upgrade checks**, review the %TEMP%\..\vcsUpgrade\vcdb_req.out file. The vcdb_req.err file tracks any errors that were identified during the pre-upgrade phase.
- **For export details**, review the %TEMP%\..\vcsUpgrade\vcdb_export.out file. The vcdb_export.err file contains errors that were identified during the export phase of the upgrade.
- **For import details**, review the ProgramData\Vmware\CIS\logs\vmware\vpx\vcdb_import.out file. The vcdb_import.err file contains errors that were identified during the import phase of the upgrade process.
- **For in-place upgrade log details**, review the ProgramData\Vmware\CIS\logs\vmware\vpx\vcdb_inplace.out file. The vcdb_inplace.err file contains in-place upgrade errors.

Collect Logs to Troubleshoot ESXi Hosts - Enter the "vm-support" command in the ESXi Shell or through SSH.



Navigate to the /var/tmp/ directory.

Retrieve the log files from the .tgz file.

RECOGNIZE COMMON UPGRADE AND MIGRATION ISSUES WITH VCENTER SERVER AND VCENTER SERVER APPLIANCE

The installation and upgrade precheck script runs tests to identify problems on the host machine that can cause an installation, upgrade, or migration to fail.

For interactive installations, upgrades, and migrations, the errors or warnings are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log file.

vSphere Update Manager provides custom messages for these errors or warnings. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan, you should review the Update Manager log file vmware-vum-server-log4cpp.log.

Error and Warning Codes That Are Returned by the Installation and Upgrade Precheck Script

64BIT_LONGMODESTATUS - The host processor must be 64-bit.

COS_NETWORKING - Warning. An IPv4 address was found on an enabled service console virtual NIC that has no corresponding address in the same subnet in the vmkernel. A separate warning appears for each such occurrence.

CPU_CORES - The host must have at least two cores.

DISTRIBUTED_VIRTUAL_SWITCH - If the Cisco Virtual Ethernet Module (VEM) software is found on the host, the test checks that the upgrade also contains the VEM software. The test also determines whether the upgrade supports the same version of the Cisco Virtual Supervisor Module (VSM) as the existing version on the host. If the software is

missing or is compatible with a different version of the VSM, the test returns a warning. The result indicates which version of the VEM software was expected on the upgrade ISO and which versions, if any, were found. You can use ESXi Image Builder CLI to create a custom installation ISO that includes the appropriate version of the VEM software.

HARDWARE_VIRTUALIZATION - Warning. If the host processor doesn't have hardware virtualization or if hardware virtualization is not turned on in the host BIOS, host performance suffers. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation.

MD5_ROOT_PASSWORD - This test checks that the root password is encoded in MD5 format. If a password is not encoded in MD5 format, it might be significant only to eight characters. In this case, any characters after the first eight are no longer authenticated after the upgrade, which can create a security issue.

MEMORY_SIZE - The host requires the specified amount of memory to upgrade.

PACKAGE_COMPLIANCE - vSphere Update Manager only. This test checks the existing software on the host against the software contained on the upgrade ISO to determine whether the host has been successfully upgraded. If any of the packages are missing or are an older version than the package on the upgrade ISO, the test returns an error and indicates which software was found on the host and which software was found on the upgrade ISO.

PARTITION_LAYOUT - You can upgrade or migrate software only if at most one VMFS partition on the disk is being upgraded and the VMFS partition must start after sector 1843200.

POWERPATH - This test checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the test checks that matching components, such as CIM, vmkernel and module, also exist in the upgrade. If they do not exist, the test returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found.

PRECHECK_INITIALIZE - This test checks that the precheck script can be run.

SANE_ESX_CONF - The /etc/vmware/esx.conf file must exist on the host.

SPACE_AVAIL_ISO - vSphere Update Manager only. The host disk must have enough free space to store the contents of the installer CD or DVD.

SPACE_AVAIL_CONFIG - vSphere Update Manager only. The host disk must have enough free space to store the legacy configuration between reboots.

SUPPORTED_ESX_VERSION - You can upgrade or migrate to ESXi 6.5 only from version 5.5 or 6.0 ESXi hosts.

TBOOT_REQUIRED - This message applies only to vSphere Update Manager upgrades. The upgrade fails with this error when the host system is running in trusted boot mode (tboot), but the ESXi upgrade ISO does not contain any tboot VIBs. This test prevents an upgrade that can make the host less secure.

UNSUPPORTED_DEVICES - Warning. This test checks for unsupported devices. Some PCI devices are not supported in ESXi 6.5.

UPDATE_PENDING - This test checks the host for VIB installations that require a reboot. This test fails if one or more such VIBs is installed, but the host has not yet been rebooted. In these conditions, the precheck script is unable to reliably determine which packages are currently installed on the host, so it might not be safe to rely on the rest of the precheck tests to determine whether an upgrade is safe.

If you encounter this error, restart the host and retry the upgrade.

Microsoft SQL Database Set to Unsupported Compatibility Mode Causes vCenter Server Installation or Upgrade to Fail - vCenter Server installation with a Microsoft SQL database fails when the database is set to compatibility mode with an unsupported version.

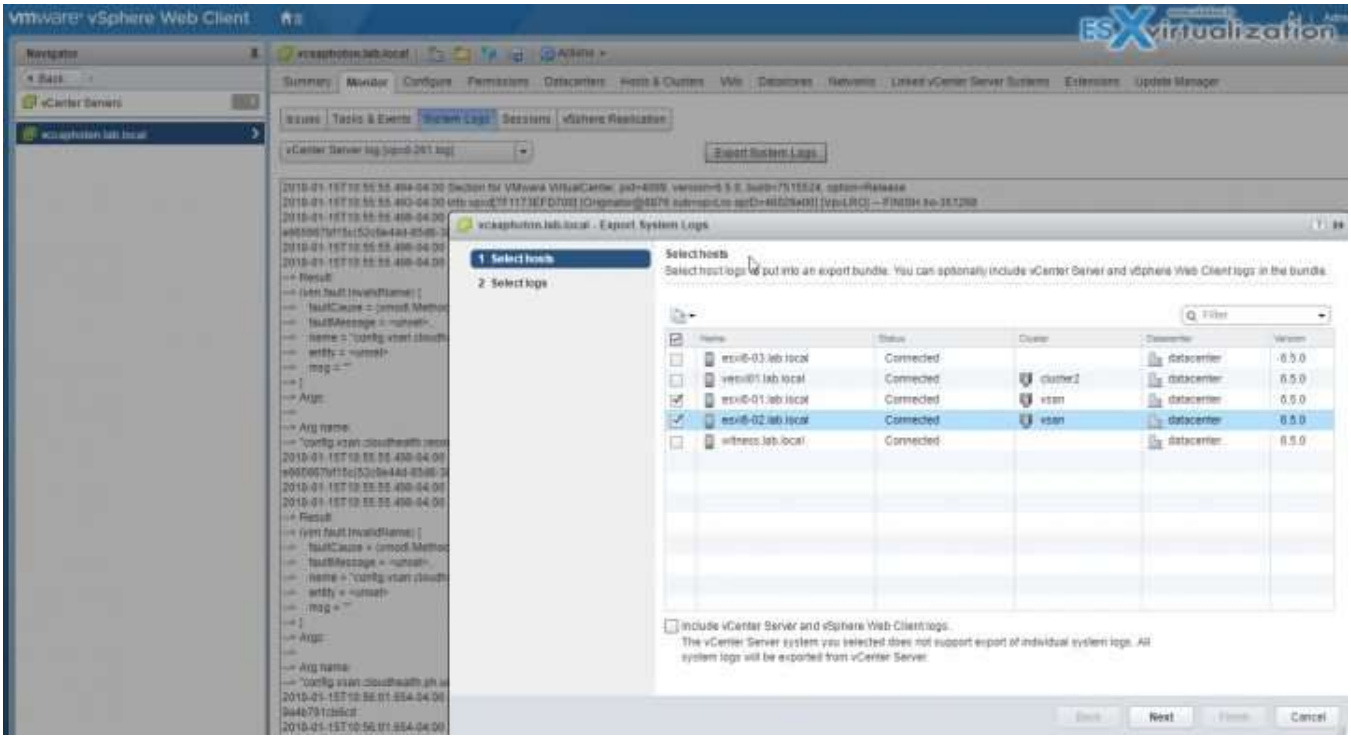
The following error message appears: The DB User entered does not have the required permissions needed to install and configure vCenter Server with the selected DB. Please correct the following error(s): %s

The database version must be supported for vCenter Server. For SQL, even if the database is a supported version, if it is set to run in compatibility mode with an unsupported version, this error occurs. For example, if SQL 2008 is set to run in SQL 2000 compatibility mode, this error occurs.

Make sure the vCenter Server database is a supported version and is not set to compatibility mode with an unsupported version.

CREATE/LOCATE VMWARE LOG BUNDLES

Web Client and log in to the **vCenter Server system** > **Global Inventory** Lists, **select vCenter Servers** > Click the vCenter Server that contains the ESX/ESXi hosts from which you want to export logs > Click the **Monitor tab** > **System Logs >** Click **Export System Logs > Select the ESX/ESXi** hosts > Select the **Include vCenter Server and vSphere Web Client logs** (optional).



Select the system logs that are to be exported > Select Gather performance data to include performance data information in the log files > Next > Click Generate Log Bundle. The Download Log Bundles dialog appears when the Generating Diagnostic Bundle task completes. Click Download Log Bundle to save it to your local computer.

DETERMINE ALTERNATIVE METHODS TO UPGRADE ESXI HOSTS IN EVENT OF FAILURE

Upgrade Hosts Interactively - To upgrade ESXi 5.5 hosts or ESXi 6.0 hosts to ESXi 6.5, you can boot the ESXi installer from a CD, DVD, or USB flash drive.

Installing or Upgrading Hosts by Using a Script - You can quickly deploy ESXi hosts by using scripted, unattended installations or upgrades. Scripted installations or upgrades provide an efficient way to deploy multiple hosts.

PXE Booting the ESXi Installer - You can use the preboot execution environment (PXE) to boot a host. Starting with vSphere 6.0, you can PXE boot the ESXi installer from a network interface on hosts with legacy BIOS or using UEFI.

Upgrading Hosts by Using esxcli Commands - By using vSphere CLI, you can upgrade a ESXi 5.5 host or ESXi 6.0 host to version 6.5 and update or patch ESXi 5.5, ESXi 6.0, and ESXi 6.5 hosts.

Here are some posts (step-by-steps) which was a lab work:

- How to Upgrade ESXi 6.0 to 6.5 via CLI [On Line]
- How to Upgrade ESXi 6.0 to 6.5 via ISO
- How to upgrade ESXi 6.0 to ESXi 6.5 via Offline Bundle
- How to upgrade an ESXi 6.0 to ESXi 6.5 via VMware Update Manager

Configure vCenter Server logging options

vSphere Web Client > Resources, select vCenter Servers > Click the vCenter Server to update the level of logging > **Settings** tab > **General** > **Edit** > **Logging Settings** > Select the **level of logging** from the Logging Options dropdown > **Click OK** when finished

The available options are:

- **None** (Disable Logging)
- **Turns off** logging
- **Error** (Errors Only) - Displays only error log entries
- **Warning** (Errors and Warnings) - Displays warning and error log entries
- **Info** (Normal Logging – Default) - Displays information, error, and warning log entries
- **Verbose** (Verbose) - Displays information, error, warning, and verbose log entries
- **Trivia** (Extended Verbose) - Displays information, error, warning, verbose, and trivia log entries

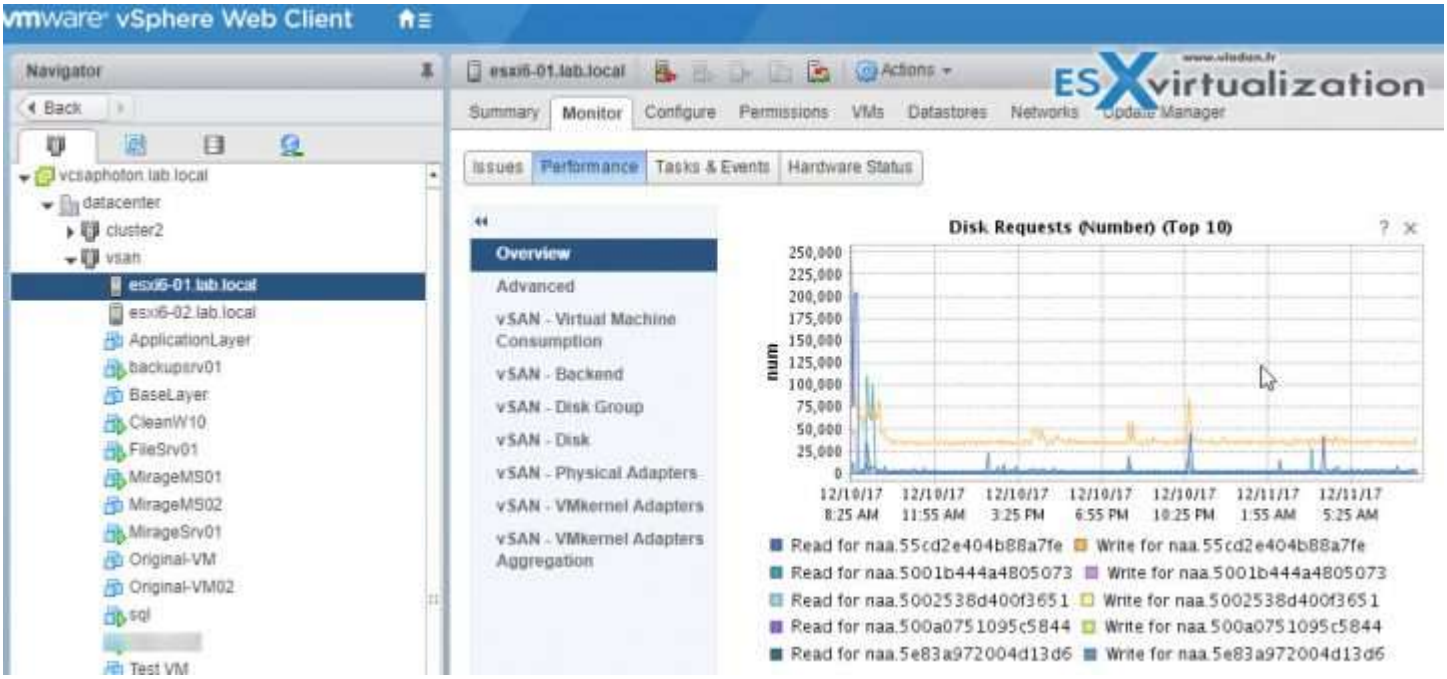
VCP6.5-DCV Objective 7.4 - Troubleshoot Virtual Machines

Monitor CPU and memory usage

vSphere 6.5 has charts and graphs which allows you to monitor different parts of the infrastructure such as hosts, VMs etc.

Hosts - you'll find information about CPU, disk, memory, network, and storage usage for hosts. The counters available depends on the collection level for vCenter Server.

- **CPU (%)** - The CPU (%) chart displays CPU usage for the host.
- **CPU (MHz)** - CPU usage for the host.
- **CPU Usage** - shows CPU usage of the 10 virtual machines on the host with the most CPU usage.
- **Memory (%)** - host memory usage.
- **Memory (Balloon)** - shows balloon memory on a host.
- **Memory (MBps)** - swap in and swap out rates for a host.
- **Memory (MB)** - memory data counters for hosts.
- **Memory Usage** - shows memory usage for the 10 virtual machines on the host with the most memory usage.



Virtual Machines - VM charts show information about CPU, disk, memory, network, storage, and fault tolerance for virtual machines. The counters available are determined by the collection level set for vCenter Server.

You do the same way. Select a **VM** > **Monitor TAB** > **Performance**.

- **CPU (%)** - shows VMs CPU usage and ready values.
- **CPU Usage (MHz)** - virtual machine CPU usage.
- **Memory (%)** - virtual machine memory usage.
- **Memory (MB)** - shows virtual machine balloon memory.
- **Memory (MBps)** - shows virtual machine memory swap rates.
- **Memory (MB)** - shows memory data counters for virtual machines.

Identify and isolate CPU and memory contention issues

CPU ready values are the ones you should be interested in. It is the time that the VM was trying to process threads but was unable to be scheduled by the hypervisor.

When rising above 5 percent, you should start to be interested.

Memory contention at the VM level you should look into a swap in and swap out rates. Also ballooning. When VM starts having some ballooning, and then even swapping, you should verify if your host's memory isn't too much overcommitted.

Recognize impact of using CPU/memory limits, reservations and Describe and differentiate critical performance metrics

You can use resource allocation settings to allocate the amount of CPU, memory, and storage resources provided for a virtual machine. You have a choice to use:

- **Shares** - If a VM, or resource pool, has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources.
- **Reservation** - guaranteed minimum allocation for a virtual machine
- **Limits** - upper bound for CPU, memory, or storage I/O resources that can be allocated to a virtual machine

Resource Allocation Settings Suggestions

Select resource allocation settings (reservation, limit, and shares) that are appropriate for your ESXi environment.

Admission Control - When you power on a VM, the system checks the amount of CPU and memory resources that have not yet been reserved. Based on the available unreserved resources, the system determines whether it can guarantee the reservation for which the virtual machine is configured (if any). This process is called admission control.

DESCRIBE AND DIFFERENTIATE COMMON METRICS, INCLUDING:

- Memory

CPU

- **%USED** – Percentage of physical CPU core cycles used by the resource pool, virtual machine, or world. %USED might depend on the frequency with which the CPU core is running. When running with lower CPU core frequency, %USED can be smaller than %RUN. On CPUs which support turbo mode, CPU frequency can also be higher than the nominal (rated) frequency, and %USED can be larger than %RUN. %USED = %RUN + %SYS – %OVRLP
- **%RDY** – Percentage of time the resource pool, virtual machine, or world was ready to run, but was not provided CPU resources on which to execute. 100% = %RUN + %RDY + %CSTP + %WAIT
- **%CSTP** – Percentage of time a resource pool spends in a ready, co-deschedule state. NOTE You might see this statistic displayed, but it is intended for VMware use only.

  100% = %RUN + %RDY + %CSTP + %WAIT

- **%SYS** – Percentage of time spent in the ESXi VMkernel on behalf of the resource pool, virtual machine, or world to process interrupts and to perform other system activities. This time is part of the time used to calculate %USED. %USED = %RUN + %SYS – %OVRLP
- **%WAIT** – Percentage of time the resource pool, virtual machine, or world spent in the blocked or busy wait state. This percentage includes the percentage of time the resource pool, virtual machine, or world was idle. 100% = %RUN + %RDY + %CSTP + %WAIT

Network, Storage

MONITOR PERFORMANCE THROUGH ESXTOP

connect via SSH client and run "esxtop" command.

options :

esxtop [-h] [-v] [-b] [-s] [-a] [-c config file] [-R vm-support_dir_path] [-d delay] [-n iterations]

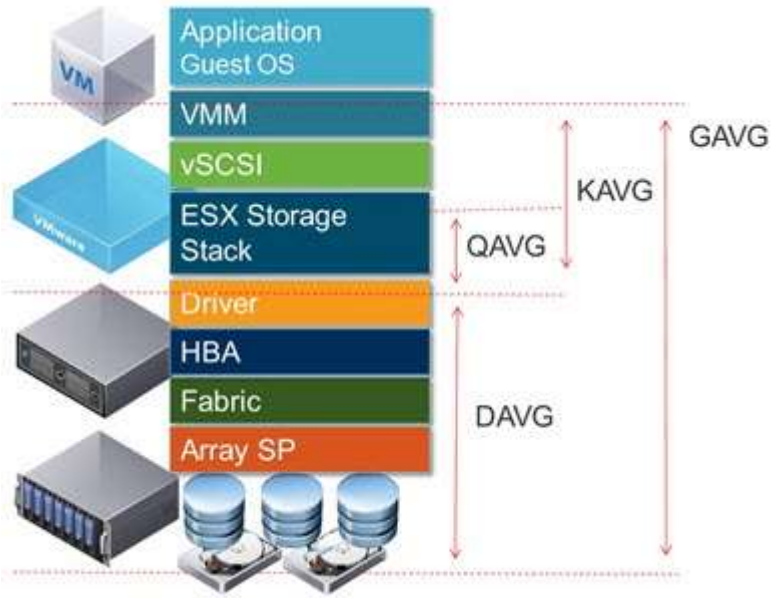
Then if you typ c, m, d, u, v, n, I, or p shows the window with CPU, memory, etc...

m - Memory
c - CPU
n - Network
i - Interrupts
d - Disk Adapter
u - Disk Device
v - Disk VM

p - Power states
x - vsan

Storage:

- **GAVG** (Guest Average Latency) total latency as seen from vSphere
- **KAVG** (Kernel Average Latency) time an I/O request spent waiting inside the vSphere storage stack.
- **QAVG** (Queue Average latency) time spent waiting in a queue inside the vSphere Storage Stack.
- **DAVG** (Device Average Latency) latency coming from the physical hardware, HBA, and Storage device.



TROUBLESHOOT ENHANCED VMOTION COMPATIBILITY (EVC) ISSUES

VMware vCenter server EVC verifies before it migrates running VMs to make sure that the VM is compatible with a target host.

vMotion transfers the running state of a virtual machine from one ESXi host to another. vMotion process has a requirement that the processors of the target host provide the same instructions to the virtual machine after migration that the processors of the source host provided before migration. Clock speed, cache size, and a number of cores can differ between source and target processors. The processors **must come from the same vendor** class (AMD or Intel) to be vMotion compatible.

Migrations of suspended VMs also require that the virtual machine be able to resume execution on the target host using equivalent instructions. When you initiate a migration with vMotion or a migration of a suspended VM, the Migrate VM wizard checks the destination host for compatibility and throws in an error if compatibility problems will prevent migration.

The CPU instruction set available to the operating system and to applications running in a virtual machine is determined at the time that a virtual machine is powered on. This CPU feature set is:

- Host CPU family and model

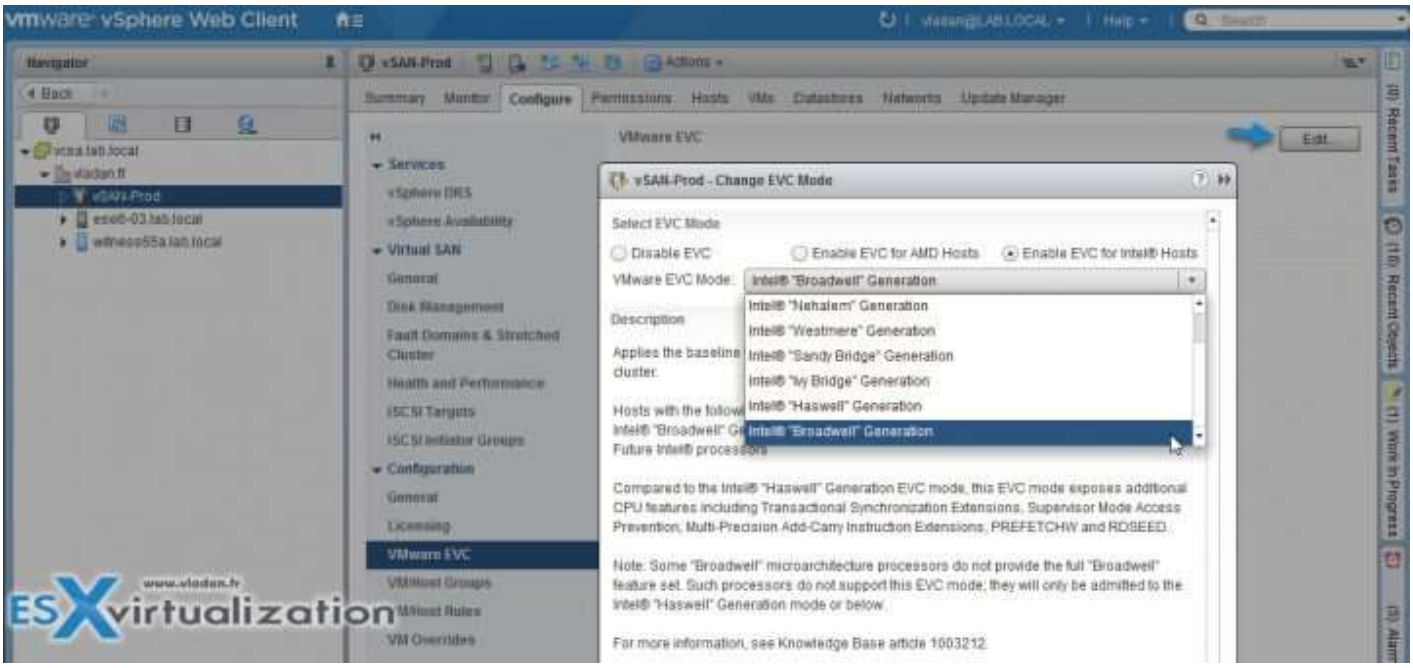
- Settings in the BIOS that might disable CPU features
- ESX/ESXi version running on the host
- The virtual machine's compatibility setting
- The virtual machine's guest operating system

In order to improve CPU compatibility between hosts of varying CPU feature sets, some host CPU features can be hidden from the virtual machine by placing the host in an **Enhanced vMotion Compatibility (EVC) cluster.**

WHERE TO CONFIGURE VMWARE ENHANCED VMOTION COMPATIBILITY (EVC)?

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

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



COMPARE AND CONTRAST OVERVIEW AND ADVANCED CHARTS

Advanced charts do provide:

- Customizable charts - Change chart settings. To create your own charts, save custom settings.
- More info - Hover over a data point in a chart and details about that specific data point are displayed.
- Allows you to do an export, to an XLS.
- Save to image file or spreadsheet.

You can use advanced charts to create your own charts, with the data you want.

Datacenter - provides info about CPU, disk, memory or storage usage for a datacenter. You can use help topics provided there.

Cluster - CPU, Disk, memory and network usage for clusters.

Datastore and Datastore clusters - disk usage

Host - CPU, disk, memory, network usage for hosts.

Resource pool - this chart has CPU and memory usage for resource pool.

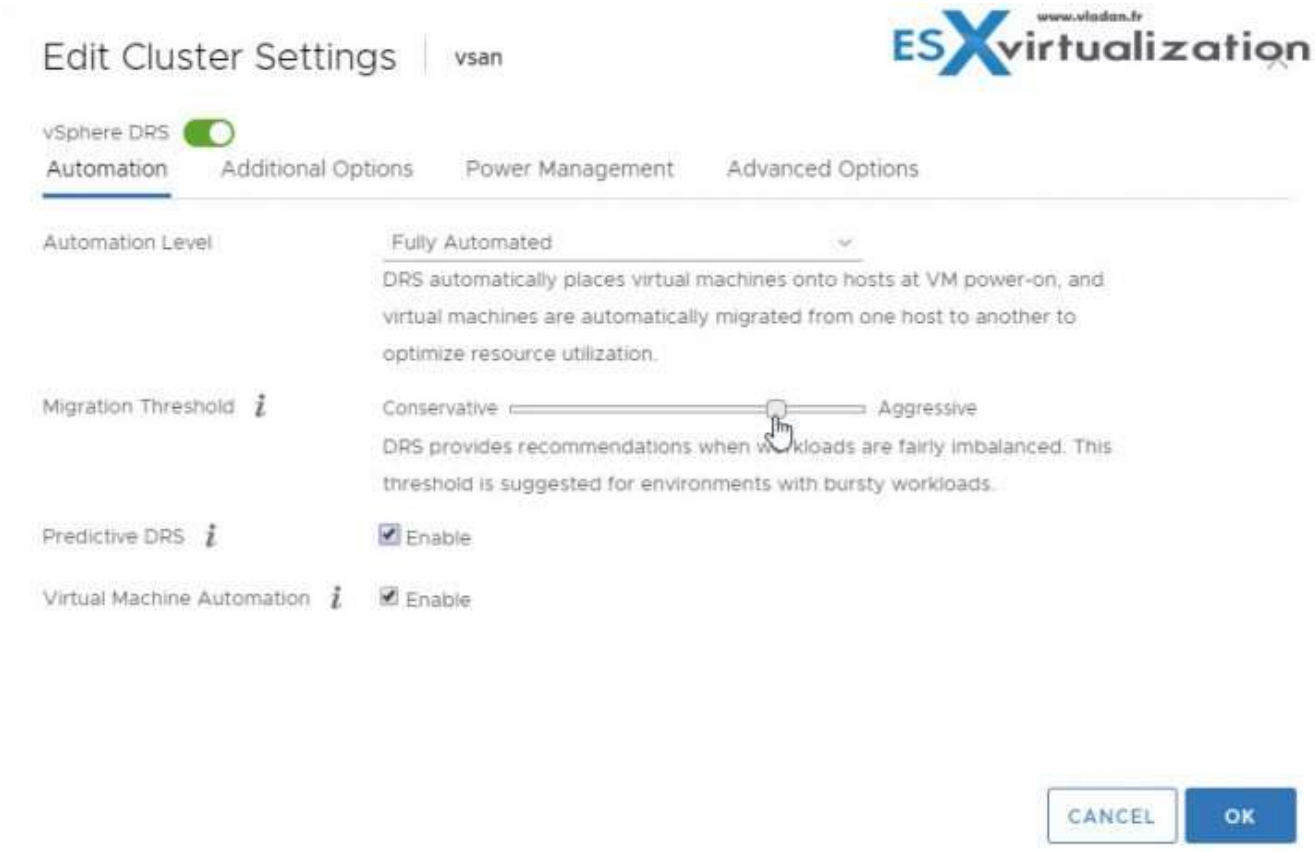
vApps - CPU and memory usage for vApps.

VMs - CPU, disk, memory, network, storage and Fault tolerance or VMs.

VCP6.5-DCV Objective 7.5 - Troubleshoot HA and DRS Configurations and Fault Tolerance

Troubleshoot issues with: DRS workload balancing

There can be a load imbalance on cluster. We say that cluster has a load imbalance of resources. Why is that? It's because VMs running different workloads have spikes in CPU and memory demands, so because of uneven resource demands from virtual machines and unequal capacities of hosts, the cluster goes out of balance.



Possible reasons why the cluster has a load imbalance:

- The migration threshold is too high - A higher threshold makes the cluster a more likely candidate for load imbalance.
- VM/VM or VM/Host DRS rules prevent virtual machines from being moved.
- DRS is disabled for one or more virtual machines.

- VM has CD ROM mounted. A device is mounted to one or more virtual machines preventing DRS from moving the virtual machine in order to balance the load.
- VMs are not compatible with the hosts to which DRS would move them. When least one of the hosts in the cluster is incompatible for the virtual machines that would be migrated, DRS won't move that VM. For example, if host A's CPU is not vMotion-compatible with host B's CPU, then host A becomes incompatible for powered-on virtual machines running on host B.
- It would be more detrimental to the virtual machine's performance to move it than for it to run where it is currently located. This may occur when loads are unstable or the migration cost is high compared to the benefit gained from moving the virtual machine.
- vMotion is not enabled or set up for the hosts in the cluster.
- DRS seldom or never performs vMotion Migrations.

DRS does not perform vMotion migrations.

DRS never performs vMotion migrations when there are issues in the cluster. Issues like:

- DRS is disabled on the cluster.
- The hosts do not have shared storage.
- The hosts in the cluster do not contain a vMotion network.
- DRS is manual and no one has approved the migration.

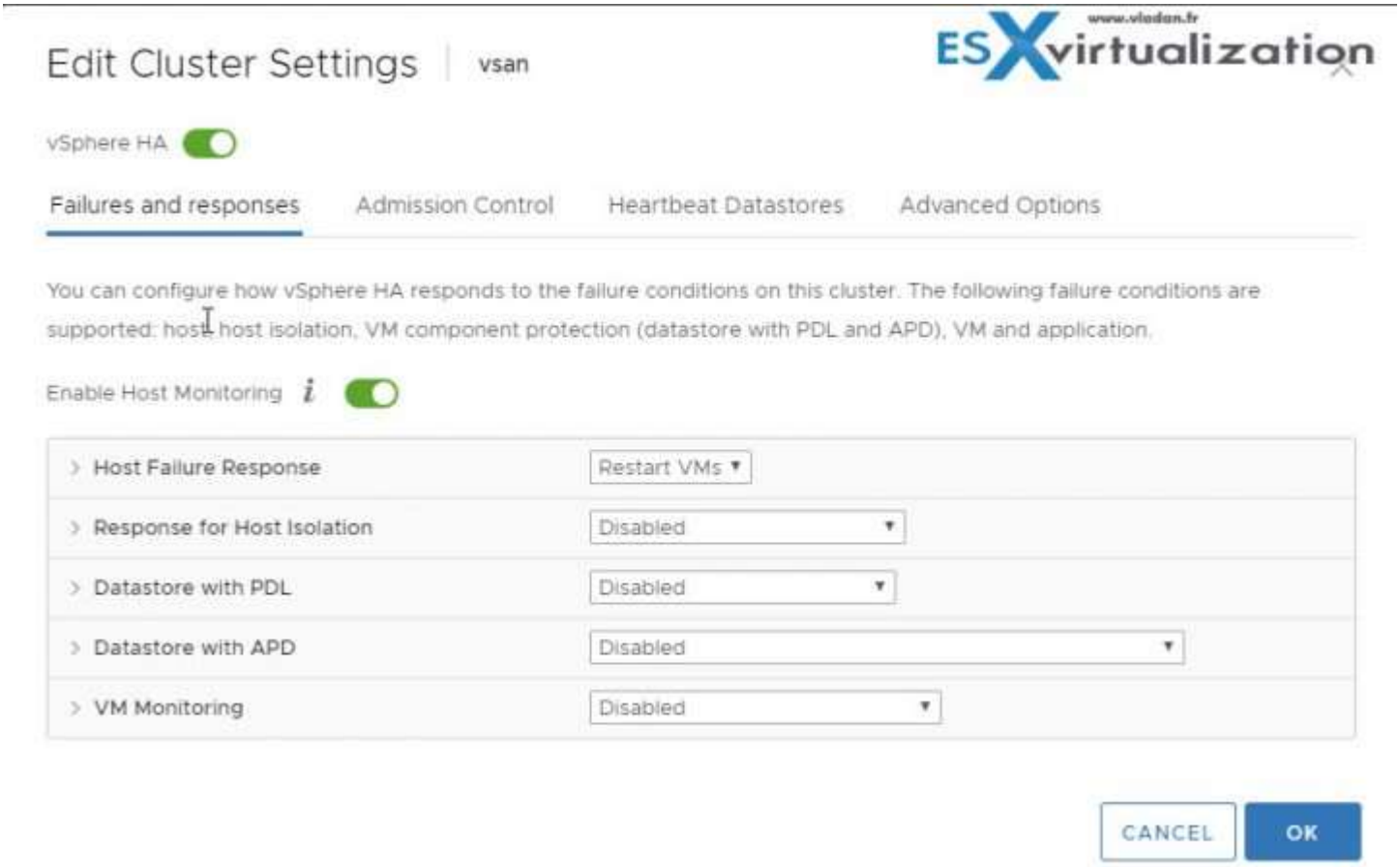
DRS seldom performs vMotion when one or more of the following issues is present on the cluster:

- Loads are unstable, or vMotion takes a long time or both. A move is not appropriate.
- DRS seldom or never migrates virtual machines.
- DRS migration threshold is set too high.

DRS moves virtual machines for the following reasons:

- Evacuation of a host that a user requested enter maintenance or standby mode.
- VM/Host DRS rules or VM/VM DRS rules.
- Reservation violations.
- Load imbalance.
- Power management.

HA FAILOVER/REDUNDANCY, CAPACITY, AND NETWORK CONFIGURATION
HA/DRS CLUSTER CONFIGURATION



Network Configuration and Maintenance - network maintenance suggestions can help you avoid the accidental detection of failed hosts and network isolation because of dropped vSphere HA heartbeats. Check this:

- When changing the networks that your clustered ESXi hosts are on, suspend the Host Monitoring feature. Changing your network hardware or networking settings can interrupt the heartbeats that vSphere HA uses to detect host failures, which might result in unwanted attempts to fail over virtual machines.
- When you change the networking configuration on the ESXi hosts themselves, for example, adding port groups, or removing vSwitches, suspend Host Monitoring. After you have made the networking configuration changes, you must reconfigure vSphere HA on all hosts in the cluster, which causes the network information to be reinspected. Then re-enable Host Monitoring.

Networks Used for vSphere HA Communications - To identify which network operations might disrupt the functioning of vSphere HA, you must know which management networks are being used for heart beating and other vSphere HA communications.

- On legacy ESX hosts in the cluster, vSphere HA communications travel over all networks that are designated as service console networks. VMkernel networks are not used by these hosts for vSphere HA communications. To contain vSphere HA traffic to a subset of the ESX console networks, use the *allowedNetworks* advanced option.
- On ESXi hosts in the cluster, vSphere HA communications, by default, travel over VMkernel networks. With an ESXi host, if you want to use a network other than the one vCenter Server uses to communicate with the host for vSphere HA, you must explicitly enable the Management traffic checkbox.

To keep vSphere HA agent traffic on the networks you have specified, configure hosts so vmkNICs used by vSphere HA do not share subnets with vmkNICs used for other purposes. vSphere HA agents send packets using any pNIC that is associated with a given subnet when there is also at least one vmkNIC configured for vSphere HA management

traffic. Therefore, to ensure network flow separation, the vmkNICs used by vSphere HA and by other features must be on different subnets.

Network Isolation Addresses - A network isolation address is an IP address that is pinged to determine whether a host is isolated from the network. This address is pinged only when a host has stopped receiving heartbeats from all other hosts in the cluster. If a host can ping its network isolation address, the host is not network isolated, and the other hosts in the cluster have either failed or are network partitioned. However, if the host cannot ping its isolation address, it is likely that the host has become isolated from the network and no failover action is taken.

By default, the network isolation address is the default gateway for the host. Only one default gateway is specified, regardless of how many management networks have been defined. Use the das.isolationaddress[…]advanced option to add isolation addresses for additional networks.

Network Path Redundancy - Use at least two management networks. Single management network ends up being a single point of failure and can result in failovers although only the network has failed. If you have only one management network, any failure between the host and the cluster can cause an unnecessary (or false) failover activity if heartbeat datastore connectivity is not retained during the networking failure. Possible failures include NIC failures, network cable failures, network cable removal, and switch resets. Consider these possible sources of failure between hosts and try to minimize them, typically by providing network redundancy.

NIC Teaming - Using a team of two NICs connected to separate physical switches improves the reliability of a management network. Because servers connected through two NICs (and through separate switches) have two independent paths for sending and receiving heartbeats, the cluster is more resilient. To configure a NIC team for the management network, configure the vNICs in vSwitch configuration for Active or Standby configuration.

The recommended parameter settings for the vNICs are:

- Default load balancing = route based on originating port ID
- Failback = No

After you have added a NIC to a host in your vSphere HA cluster, you must reconfigure vSphere HA on that host.

NIC teaming provides sufficient heartbeat redundancy, but as an alternative, you can create a second management network connection attached to a separate virtual switch. Redundant management networking allows the reliable detection of failures and prevents isolation or partition conditions from occurring because heartbeats can be sent over multiple networks.

When the second management network connection is created, vSphere HA sends heartbeats over both management network connections. If one path fails, vSphere HA still sends and receives heartbeats over the other path.

Using IPv6 Network Configurations - Only one IPv6 address can be assigned to a given network interface used by your vSphere HA cluster. Assigning multiple IP addresses increases the number of heartbeat messages sent by the cluster's master host with no corresponding benefit.

Best Practices for Interoperability - Observe the following best practices for allowing interoperability between vSphere HA and other features.

vSphere HA and Storage vMotion Interoperability in a Mixed Cluster

In clusters where ESXi 5.x hosts and ESX/ESXi 4.1 or earlier hosts are present and where Storage vMotion is used extensively or Storage DRS is enabled, do not deploy vSphere HA. vSphere HA might respond to a host failure by restarting a virtual machine on a host with an ESXi version different from the one on which the virtual machine was running before the failure. A problem can occur if, at the time of failure, the virtual machine was involved in a

Storage vMotion action on an ESXi 5.x host, and vSphere HA restarts the virtual machine on a host with a version earlier than ESXi 5.0. While the virtual machine might power-on, any subsequent attempts at snapshot operations might corrupt the vdisk state and leave the virtual machine unusable.

Best Practices for Cluster Monitoring - Observe the following best practices for monitoring the status and validity of your vSphere HA cluster.

Setting Alarms to Monitor Cluster Changes - When vSphere HA or Fault Tolerance take action to maintain availability, for example, a virtual machine failover, you can be notified about such changes. Configure alarms in vCenter Server to be triggered when these actions occur and have alerts, such as emails, sent to a specified set of administrators.

Some vSphere HA alarms which are available:

- Insufficient failover resources (a cluster alarm)
- Cannot find master (a cluster alarm)
- Failover in progress (a cluster alarm)
- Host HA status (a host alarm)
- VM monitoring error (a virtual machine alarm)
- VM monitoring action (a virtual machine alarm)
- Failover failed (a virtual machine alarm)

VMOTION/STORAGE VMOTION CONFIGURATION AND/OR MIGRATION

When vMotion request is sent to the vCenter Server, a call is sent to vCenter Server requesting the live migration of a virtual machine to another host. This call may be issued through the VMware vSphere Web Client, VMware vSphere Client or through an API call.

vCenter Server sends the vMotion request to the destination ESXi host - a request is sent to the destination ESXi host by vCenter Server to notify the host for an incoming vMotion. This step also validates if the host can receive a vMotion. If a vMotion is allowed on the host, the host replies to the request allowing the vMotion to continue. If the host is not configured for vMotion, the host replies to the request disallowing the vMotion, resulting in a vMotion failure.

Possible issues:

- Ensure that vMotion is enabled on all ESX/ESXi hosts.
- Determine if resetting the Migrate.Enabled setting on both the source and destination ESX or ESXi hosts addresses the vMotion failure.
- Verify that VMkernel network connectivity exists using vmkping.
- Verify that VMkernel networking configuration is valid.
- Verify that Name Resolution is valid on the host.
- Verify if the ESXi/ESX host can be reconnected or if reconnecting the ESX/ESXi host resolves the issue.
- Verify that you do not have two or more virtual machine swap files in the virtual machine directory.
- If you are migrating a virtual machine to or from a host running VMware ESXi below version 5.5 Update 2.

vCenter Server sends the vMotion request to the source ESXi host to prepare the virtual machine for migration - Here, request is made to the source ESXi host by vCenter Server to notify the host for an incoming vMotion. This step validates if the host can send a vMotion. If a vMotion is allowed on the host, the host replies to the request allowing the vMotion to continue. If the host is not configured for vMotion, the host will reply to the request disallowing the vMotion, resulting in a vMotion failure.

Once the vMotion task has been validated, the configuration file for the virtual machine is placed into read-only mode and closed with a 90 second protection timer. This prevents changes to the virtual machine while the vMotion task is in progress.

Possible issues:

- Ensure that vMotion is enabled on all ESX/ESXi hosts.
- Determine if resetting the Migrate.Enabled setting on both the source and destination ESX or ESXi hosts addresses the vMotion failure.
- Verify that VMkernel network connectivity exists using vmkping.
- Verify that VMkernel networking configuration is valid.
- Verify that Name Resolution is valid on the host.
- Verify if the ESXi/ESX host can be reconnected or if reconnecting the ESX/ESXi host resolves the issue.

vCenter Server initiates the destination host virtual machine - the destination host creates, registers and powers on a new virtual machine. The virtual machine is powered on to a state that allows the virtual machine to consume resources and prepares it to receive the virtual machine state from the source host. During this time a world ID is generated that is sent to the source host as the target virtual machine for the vMotion.

Possible issues:

- Verify that the required disk space is available.
- Verify that time is synchronized across environment.
- Verify that hostd is not spiking the console.
- Verify that valid limits are set for the virtual machine being vMotioned.
- Verify if the ESXi/ESX host can be reconnected or if reconnecting the ESX/ESXi host resolves the issue.

vCenter Server initiates the source host virtual machine - The source host begins to migrate the memory and running state of the source virtual machine to the destination virtual machine. This information is transferred using VMkernel ports configured for vMotion. Additional resources are allocated for the destination virtual machine and additional helper worlds are created. The memory of the source virtual machine is transferred using checkpoints.

After the memory and virtual machine state is completed, a stun of the source virtual machine occurs to copy any remaining changes that occurred during the last checkpoint copy. Once this is complete the destination virtual machine resume as the primary machine for the virtual machine that is being migrated.

Possible issues:

If Jumbo Frames are enabled (MTU of 9000) (9000 -8 bytes (ICMP header) -20 bytes (IP header) for a total of 8972), ensure that vmkping is using the command:

vmkping -d -s 8972 *destinationIPaddress*

You may experience problems with the trunk between two physical switches that have been misconfigured to an MTU of 1500.

- Verify that valid limits are set for the virtual machine being vMotioned.
- Verify the virtual hardware is not out of date.
- This issue may be caused by SAN configuration. Specifically, this issue may occur if zoning is set up differently on different servers in the same cluster.
  Verify and ensure that the *log.rotateSize* parameter in the virtual machine's configuration file is not set to a very low value.

- If you are migrating a 64-bit virtual machine, verify that the VT option is enabled on both the source and destination host. For more information.
  Verify that there are no issues with the shared storage or networking.
- If you are using NFS storage, verify if the VMFS volume containing the VMDK file of a virtual machine being migrated is on an NFS datastore and the datastore is not mounted differently on both the source and destination.
- If you are using VMware vShield Endpoint, verify the vShield Endpoint LKM is installed on the ESX/ESXi hosts to which you are trying to vMotion the virtual machine.

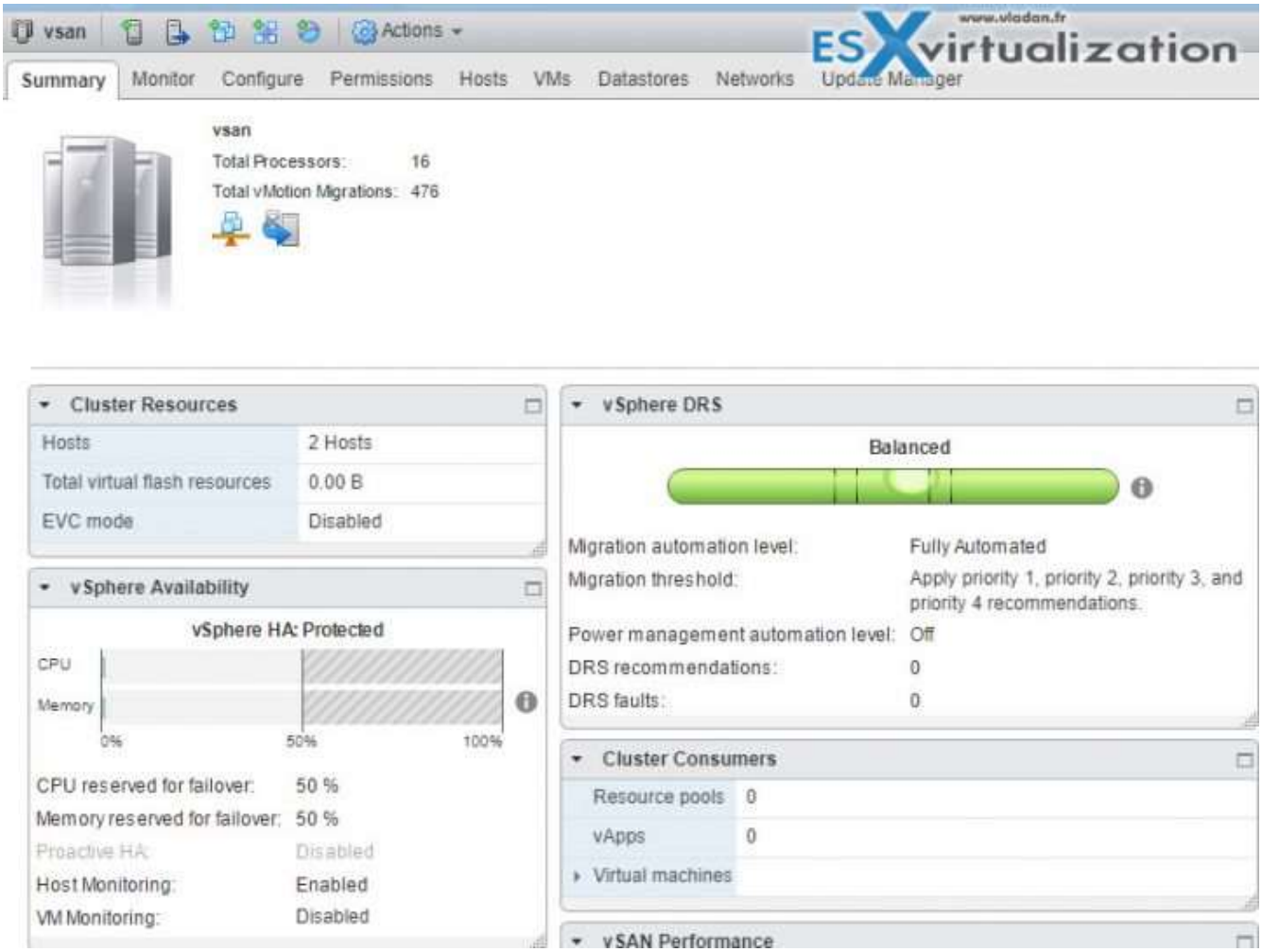
Fault Tolerance configuration and failover issues

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.

Explain the DRS Resource Distribution Graph and Target/Current Host Load Deviation

VMware vSphere has DRS resource distribution graph which shows CPU or Memory metric for each of the hosts in the cluster. The DRS cluster is load balanced when each of the hosts' level of consumed resources is equivalent to all the other nodes in the cluster.



The objective for DRS is not to balance the load perfectly across every host. Rather, DRS monitors the resource demand and works to ensure that every VM is getting the resources entitled. When DRS determines that a better host exists for the VM, it makes a recommendation to move that VM.

Explain vMotion Resource Maps

vMotion resource maps give us a visual representation of hosts, datastores, and networks associated with the selected virtual machine. It indicates which hosts in the cluster or datacenter are compatible with the VM and shows potential migration targets.

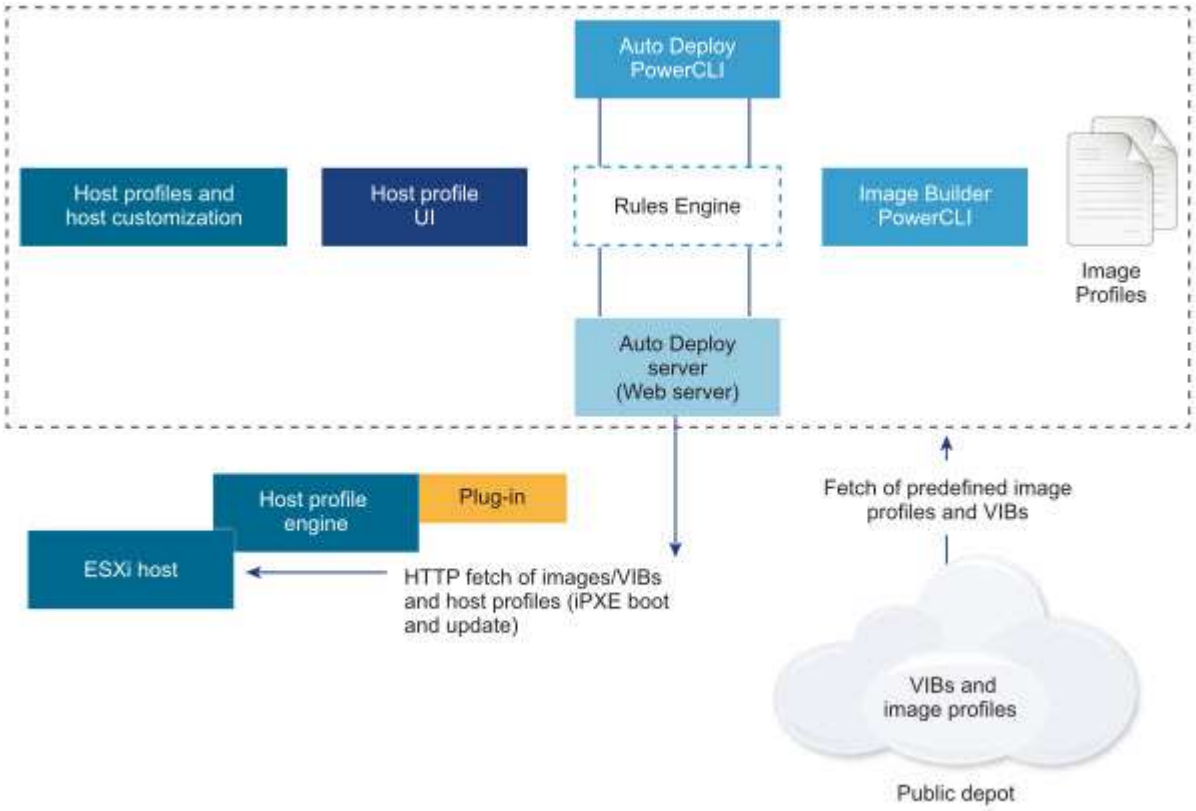
The host must:

- Connect to all the same datastores as the virtual machine.
- Connect to all the same networks as the virtual machine.
- Have compatible software with the virtual machine.
- Have a compatible CPU with the virtual machine.

VCP6.5-DCV Objective 8.1 - Configure Auto Deploy for ESXi Hosts

Describe the components and architecture of an Auto Deploy environment

Auto Deploy uses a PXE boot infrastructure in conjunction with vSphere host profiles to provision and customize that host. No state is stored on the host itself, instead, the Auto Deploy server manages state information for each host.



Auto Deploy Server - Provides images and host profiles.

vSphere Auto Deploy rules engine - Sends information to the vSphere Auto Deploy server which image profile and which host profile to serve to which host. Administrators use vSphere Auto Deploy to define the rules that assign image profiles and host profiles to hosts.

Image profiles - Define the set of VIBs to boot ESXi hosts with.

- VMware and VMware partners make image profiles and VIBs available in public depots. Use vSphere ESXi Image Builder to examine the depot and use the vSphere Auto Deploy rules engine to specify which image profile to assign to which host.
- VMware customers can create a custom image profile based on the public image profiles and VIBs in the depot and apply that image profile to the host.

Host profiles - Define machine-specific configuration such as networking or storage setup. Use the host profile UI to create host profiles. You can create a host profile for a reference host and apply that host profile to other hosts in your environment for a consistent configuration.

Host customization - Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host.

Auto Deploy provides an intuitive way for setting up ESXi hosts easily and consistently. It's very useful for large environment deployment and also for web scaling infrastructure provided by solutions like hyper-converged infrastructure (HCI).

IMPLEMENT HOST PROFILES WITH AN AUTO DEPLOY OF AN ESXI HOST

You can also use vSphere Auto Deploy to install an ESXi host, and set up a host profile that causes the host to store the ESXi image and configuration on the local disk, a remote disk, or a USB drive. Subsequently, the ESXi host boots from this local image and vSphere Auto Deploy no longer provisions the host. This process is similar to performing a scripted installation.

Rules and Rule Sets - You specify the behavior of the vSphere Auto Deploy server by using a set of rules. The vSphere Auto Deploy rules engine checks the rule set for matching host patterns to decide which items (image profile, host profile, vCenter Server location, or script object) to provision each host with.

For hosts that have not yet been added to a vCenter Server system, the vSphere Auto Deploy server checks with the rules engine before serving image profile, host profile, and inventory location information to hosts. For hosts that are managed by a vCenter Server system, the image profile, host profile, and inventory location that vCenter Server has stored in the host object is used.

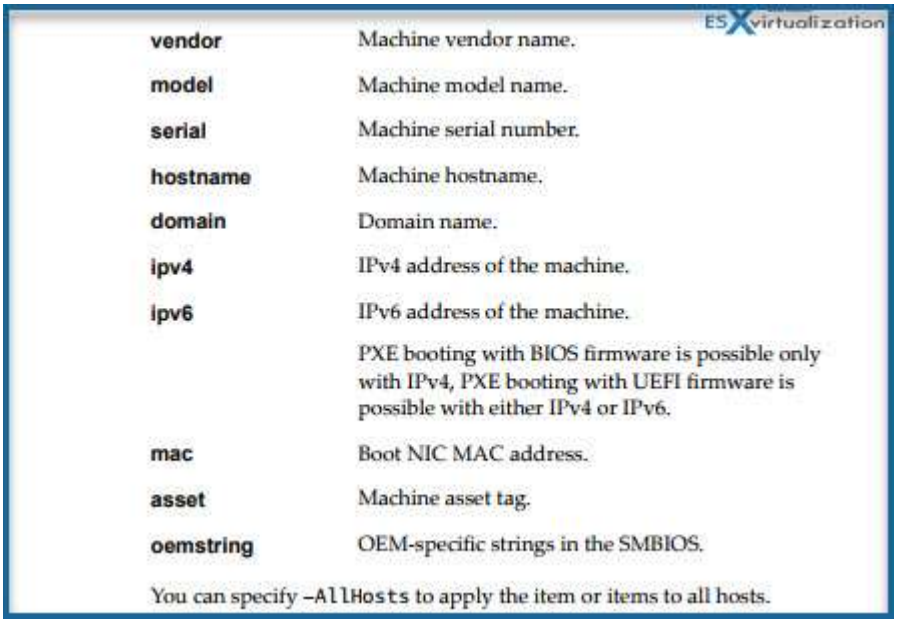
The rules engine includes rules and rule sets.

Rules - can assign image profiles and host profiles to a set of hosts, or specify the location (folder or cluster) of a host on the target vCenter Server system. A rule can identify target hosts by boot MAC address, SMBIOS information, BIOS UUID, Vendor, Model, or fixed DHCP IP address.

You can specify the following parameters in a rule:

- **Name** of the rule, specified with the *-Name* parameter
- **Item** One or more items, specified with the *-Item* parameter. An item can be an image profile, a host profile, a vCenter Server inventory location (datacenter, folder, cluster) for the target host, or a custom script.
- **Pattern** - The pattern specifies the host or group of hosts to which the rule applies.

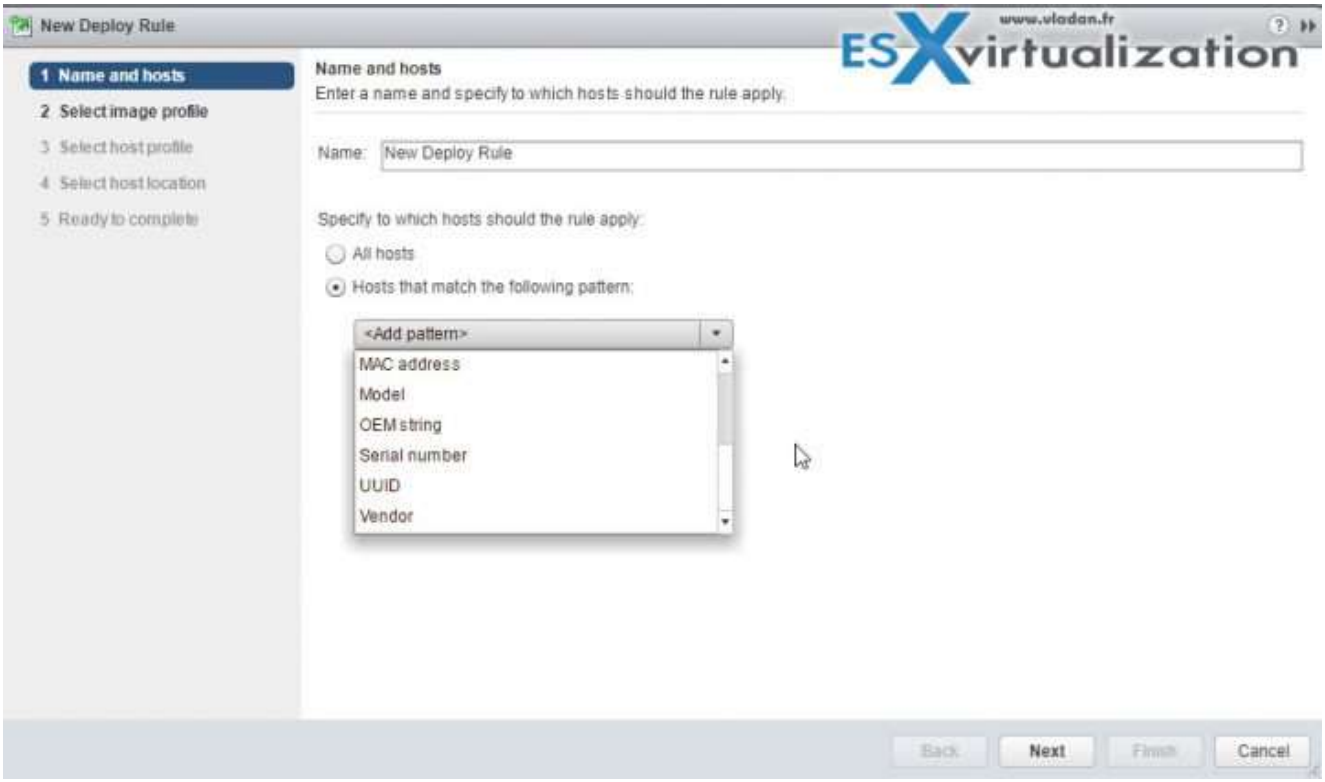
Img from "vSphere Installation and Setup" PDF.



- **Active Rule Set** - When a newly started host contacts the vSphere Auto Deploy server with a request for an image profile, the vSphere Auto Deploy server checks the active rule set for matching rules. The image profile, host profile, vCenter Server inventory location, and script object that are mapped by matching rules are then used to boot the host. If more than one item of the same type is mapped by the rules, the vSphere Auto Deploy server uses the item that is first in the rule set.

- **Working Rule Set** - The working rule set allows you to test changes to rules before making the changes active. For example, you can use vSphere Auto Deploy cmdlets for testing compliance with the working rule set. The test verifies that hosts managed by a vCenter Server system are following the rules in the working rule set. By default, cmdlets add the rule to the working rule set and activate the rules. Use the NoActivate parameter to add a rule only to the working rule set.

You can find the auto-deploy rules within the AutoDeploy UI. Previous releases of vSphere had to use PowerCLI. Before you can manage vSphere Auto Deploy with rules that you create with PowerCLI cmdlets, you must install PowerCLI.



INSTALL AND CONFIGURE AUTO DEPLOY

Autodeploy is preinstalled with vCenter server management node (VCSA or Windows).

Requirements:

- Hardware requirements for ESXi - See ESXi Hardware Requirements.
- Network connectivity to vCenter server and check ports requirements. - Required Ports for vCenter Server and Platform Services Controller.
- You must install prerequisite software and set up the DHCP and TFTP servers that vSphere Auto Deploy interacts with.
- Allocate 2 GB to have enough room for four image profiles and some extra space. Each image profile requires approximately 350 MB. Determine how much space to reserve for the vSphere Auto Deploy repository by considering how many image profiles you expect to use.
- You can use a DHCP server already in your environment, or install a DHCP server. For your vSphere Auto Deploy setup, replace the gpxelinux.0 file name with snponly64.efi.vmw-hardwired for UEFI or undionly.kpxe.vmw-hardwired for BIOS.
- Set up a remote Syslog server.
- Install ESXi Dump Collector, set up your first host so that all core dumps are directed to ESXi Dump Collector, and apply the host profile from that host to all other hosts.

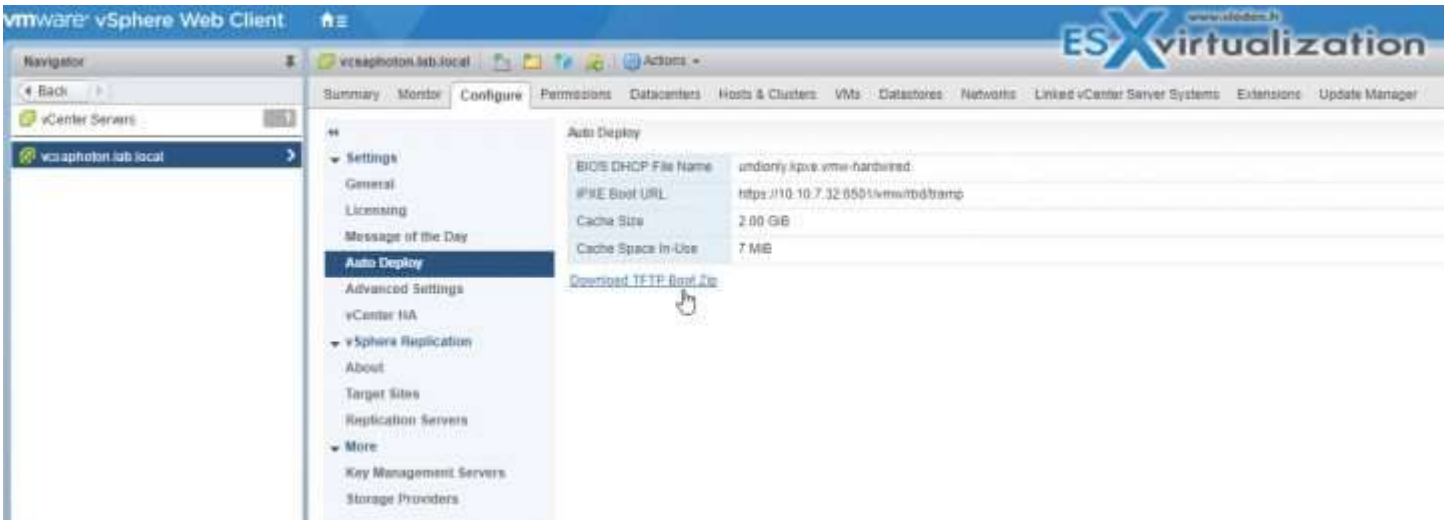
- If the hosts that you plan to provision with vSphere Auto Deploy are with legacy BIOS, verify that the vSphere Auto Deploy server has an IPv4 address. PXE booting with legacy BIOS firmware is possible only over IPv4. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.
- If you want to use VLANs in your vSphere Auto Deploy environment, you must set up the end to end networking properly. When the host is PXE booting, the firmware driver must be set up to tag the frames with proper VLAN IDs. You must do this set up manually by making the correct changes in the UEFI/BIOS interface. You must also correctly configure the ESXi port groups with the correct VLAN IDs.

The Steps:

Install vCenter Server or deploy the vCenter Server Appliance. The vSphere Auto Deploy server is included with the management node.

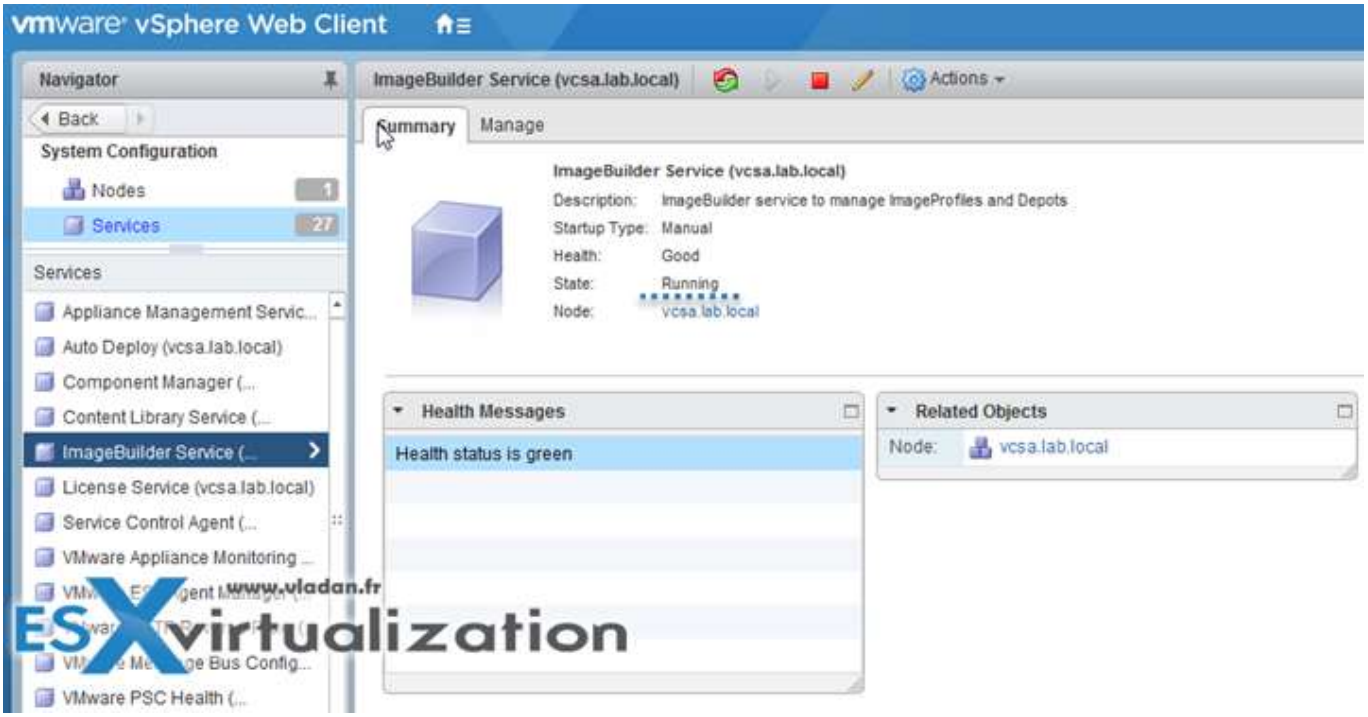
vSphere Web client > Administration > System Configuration > Services > AutoDeploy > Actions > Edit Startup type.

- On Windows, the vSphere Auto Deploy service is disabled. In the Edit Startup Type window, select Manual or Automatic to enable vSphere Auto Deploy.
- On the vCenter Server Appliance, the vSphere Auto Deploy service by default is set to Manual. If you want the vSphere Auto Deploy service to start automatically upon OS startup, select Automatic.
- Configure the TFTP server. In a vSphere Web Client connected to the vCenter Server system, go to the inventory list and select the vCenter Server system. Click the Manage tab, select Settings, and click Auto Deploy.
- Click Download TFTP Boot Zip to download the TFTP configuration file and unzip the file to the directory in which your TFTP server stores files.

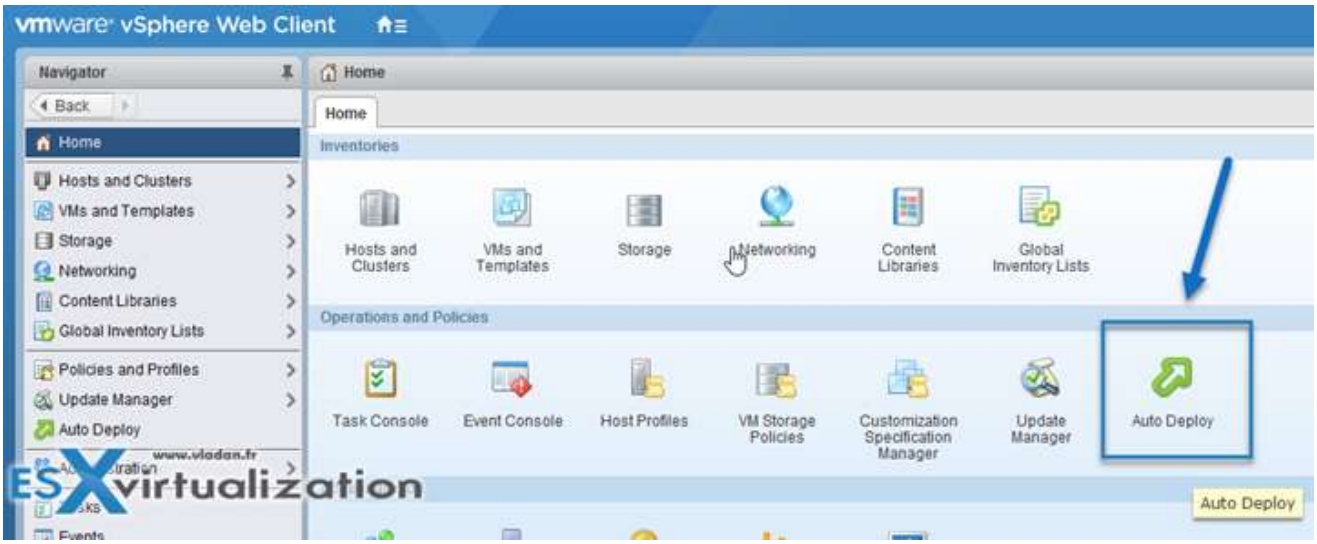


- Set up your DHCP server to point to the TFTP server on which the TFTP ZIP file is located. Specify the TFTP Server's IP address in DHCP option 66, frequently called next-server.
- Specify the boot file name, which is snponly64.efi.vmw-hardwired for UEFI or undionly.kpxe.vmw-hardwired for BIOS in the DHCP option 67, frequently called boot-filename.
- Set each host you want to provision with vSphere Auto Deploy to network boot or PXE boot, following the manufacturer's instructions.

For the Auto Deploy GUI to be visible in vSphere Web Client, both the Image Builder and Auto Deploy services must be running. You should have the ImageBuilder Service up and ruuning…

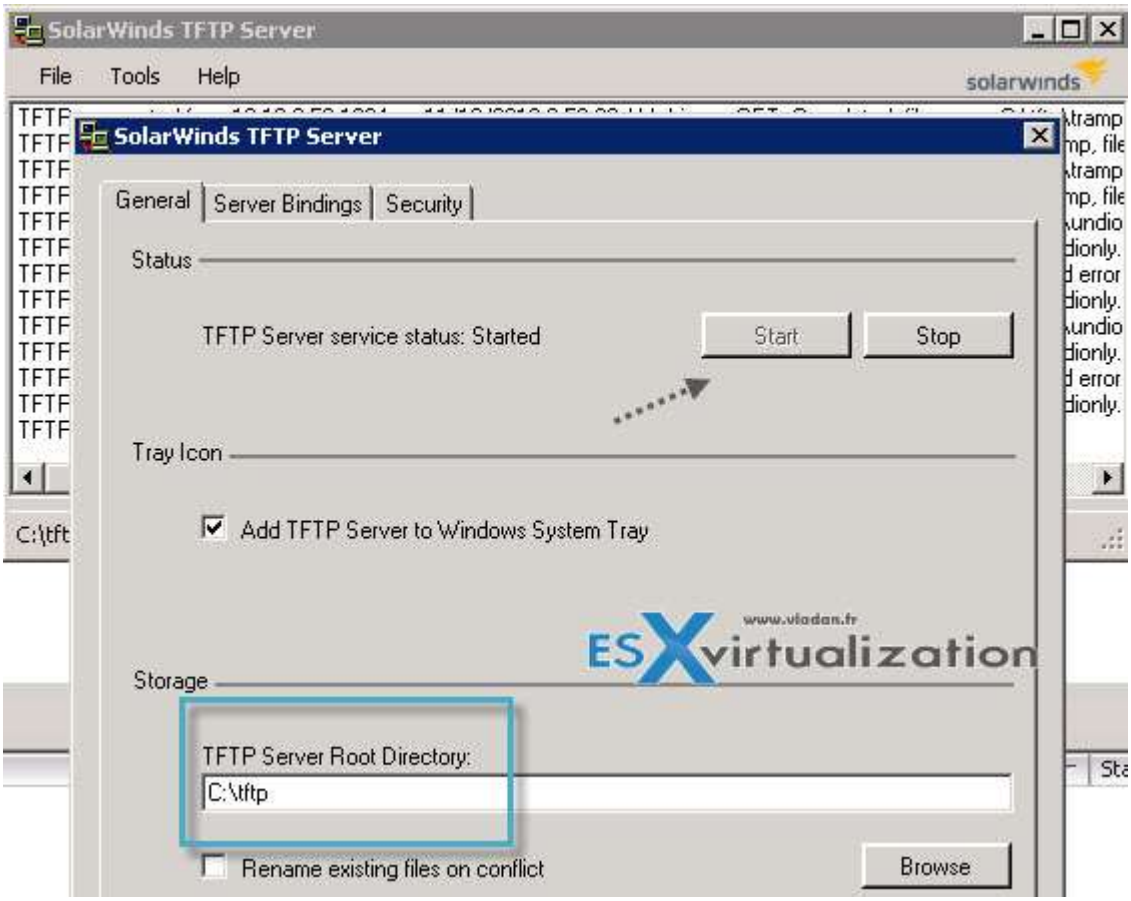


If you want to use vSphere ESXi Image Builder with thevSphere Web Client, log out of the vSphere Web Client and log in again. The Auto Deploy icon is then visible on the home page of the vSphere Web Client (by default it isn't).



Install TFTP server next. We'll need a windows machine. (usually, we can use DHCP server, if it's Windows DC, which has also a role of DHCP). I usually use the Free TFTP server from Solarwinds.

The installer creates a default directory which can be changed. I changed mine to ***c:tftp*** to keep it simple. You can configure the option by going to **File** > **Configure** menu. While there, make sure that you start the service. (Note: you can also go to Windows services to make the TFTP service start automatically during the boot as by default it has manual start only).



That's it for TFTP server. There is nothing else to play with and we can move on.

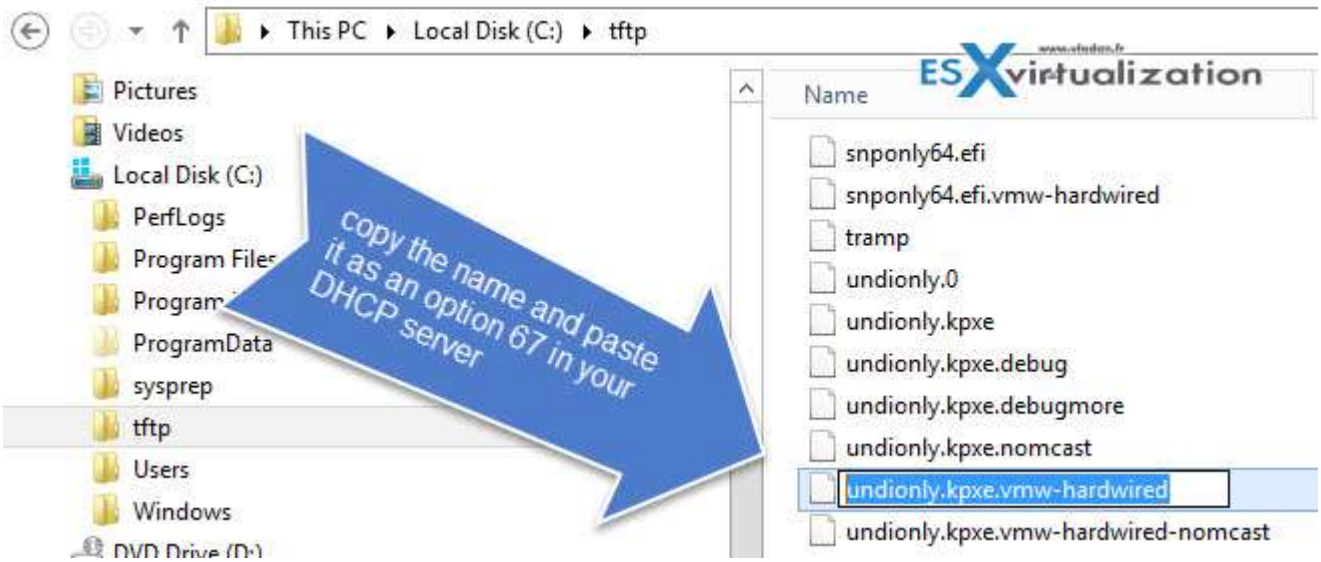
DHCP SERVER OPTIONS

Next, I'll show you the options you need to configure on your DHCP server. There are just two options which need to be configured at the scope level of the DHCP server. When you click on the Autodeploy icon in vSphere client, you'll end up on this page where you can see some strange name of file.

But this exact name will be needed for setting up options in our DHCP server! It's the *undionly.kpxe.vmw-hardwired*.

Note that vSphere 6.5 supports UEFI for TFTP as well. PXE booting with UEFI firmware is possible with either IPv4 or IPv6.

So next step is to click and download the TFTP boot zip files to the c:tftp directory that we created and set up on our TFTP server. Unzip the file into the same directory You should have a view like this:



Once done, we can copy this name of the file (*undionly.kpxe.vmw-hardwired**)*** as an option 67 in our DHCP server. In my case I have Windows DHCP server which sits on my domain controller.

Now you should configure each of your ESXi host's BIOS to **boot from network**.

Deploy multiple ESXi hosts using Auto Deploy

See above topics.

Explain the Auto Deploy deployment model needed to meet a business requirement

Please use PDF called "vSphere ESXi vCenter Server 6.5 installation and setup" for the study of this topic. The PDF is really good and detailed.

You'll be able to learn also to set up a vSphere Auto Deploy reference host which is used in cases where no state is stored on the host. In this case, the reference host helps you set up multiple hosts with the same config. You simply configure the reference host with the logging, coredump, and other settings you want to have, save the host profile and write a rule that applies the host profile to other hosts as needed.

Last but not least, one must think "availability" as Autodeploy server is also a single point of failure (SPOF). It's important to make autodeploy highly available within management cluster (yes, it's recommended to have a separate management cluster).

VCP6.5-DCV Objective 8.2 – Create and Deploy Host Profiles

Host profiles feature creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host or cluster in vCenter Server.

The general steps to manage host profiles are:

1. Set up and configure the reference host.
2. Create a Host Profile from the reference host.
3. Attach other hosts or clusters to the Host Profile.
4. Check the compliance to the Host Profile. If all hosts are compliant with the reference host, they are correctly configured.
5. Apply (remediate).

EDIT ANSWER FILE TO CUSTOMIZE ESXI HOST SETTINGS

Host profile can be attached directly to a single host in vCenter Server, but usually, host profile is attached to a vSphere cluster as usually, all the hosts have the same hardware, storage, and networking configurations. You can extract a host profile from a reference host. To customize individual hosts, you can set up some fields in the host profile to prompt the user for input for each host. After the user has specified the information, the system generates a host-specific answer file and stores it with the Auto Deploy cache and the vCenter Server host object.

Host profiles allow you to prespecify information, for example, the storage setup or Syslog setup in a reference host and apply the host profile to a set of target hosts that share the same settings. You can also use host profiles to specify that certain settings are host-dependent. If you do so, the host comes up in maintenance mode when you provision it with Auto Deploy. Apply the host profile or update the answer file to be prompted for input. The system stores your input and uses it the next time the host boots.

Note: The answer file is not stored in a location or format that administrators can access. Use the Host Profiles UI in the vSphere Client to manage answer files.

Host customization was called "answer file" in earlier releases of vSphere Auto Deploy.

Stores information that the user provides when host profiles are applied to the host. Host customization might contain an IP address or other information that the user supplied for that host. For more information about host customizations, see the *vSphere Host Profiles* documentation.

You can edit the host customizations for specific hosts attached to a host profile or cluster attached to a host profile.

Navigate to a **host profile** > **Right-click the host profile** and select **Edit Host Customizations > Select the host or hosts** for which to edit the customizations, and click **Next > Edit the host configuration** values.

Optionally you can click Browse to import a .csv file from your desktop. After importing the .csv file, the fields are updated with the information from the file.

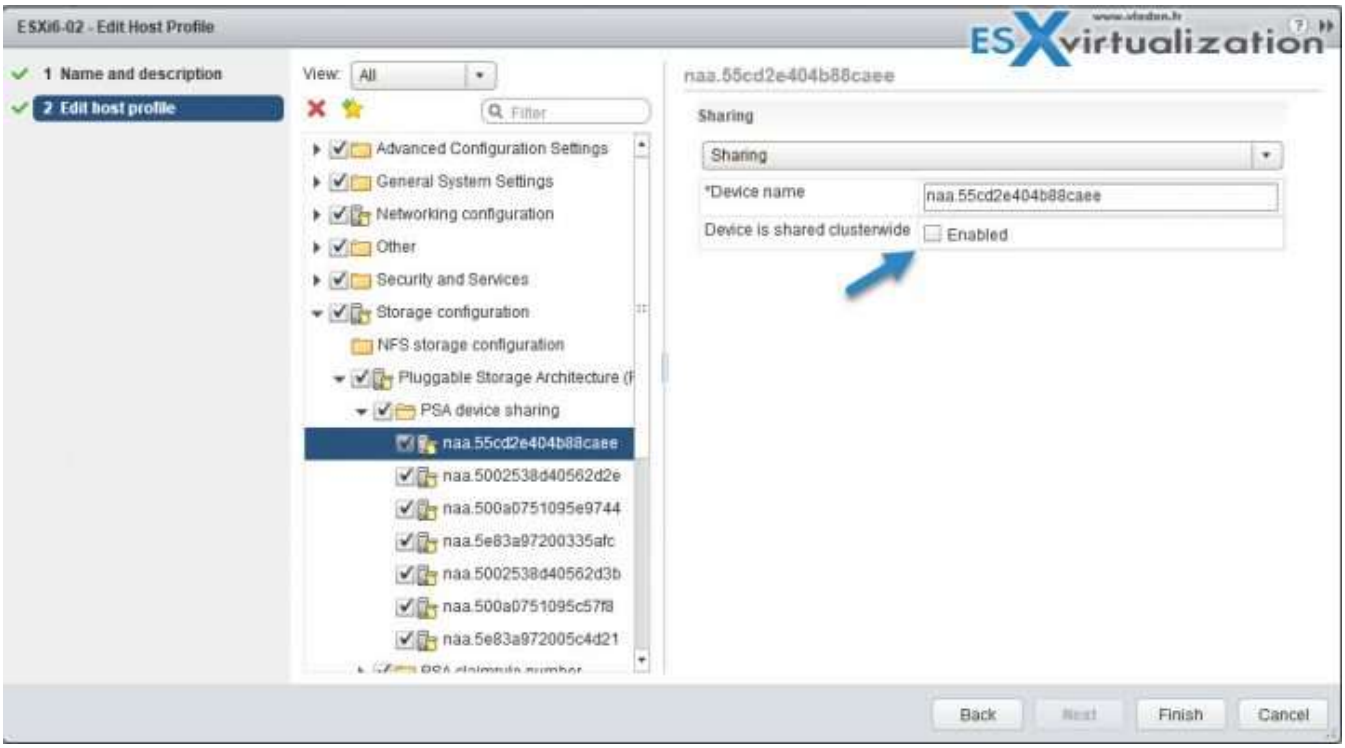
MODIFY AND APPLY A STORAGE PATH SELECTION PLUGIN (PSP) TO A DEVICE USING HOST PROFILES

From the docs:

Extract a host profile from a reference host. For SAS devices that are not detected as local, select **Storage configuration** > **Pluggable Storage Architecture** configuration > **PSA device sharing** > name of a device. For each device not shared across the cluster, disable **Device is shared clusterwide.**

The **Is Shared Clusterwide** value for PSA devices helps you determine which devices in the cluster should be configured by a host profile. Correctly setting this value for devices in the cluster eliminates compliance errors due to non-shared devices.

By default, this value is populated to reflect the Is Local setting for the device. For example, a device with Is Local set to True, this setting is disabled by default. This setting allows storage host profiles to ignore these devices during compliance checks.



You can find the Is Local setting for the device by running the command esxcli storage core device list in the ESXi Shell. For more information on this command and identifying disks or LUNs, see http://kb.vmware.com/kb/1014953.

For SAN boot LUN devices shared across the cluster but logically local to the host, disable the Is Shared Clusterwide on the reference host. You must set the value to False before extracting the host profile from the reference host. When applying the host profile to the target host, the boot device settings for the remote boot LUN device are copied from the reference host into the target host.

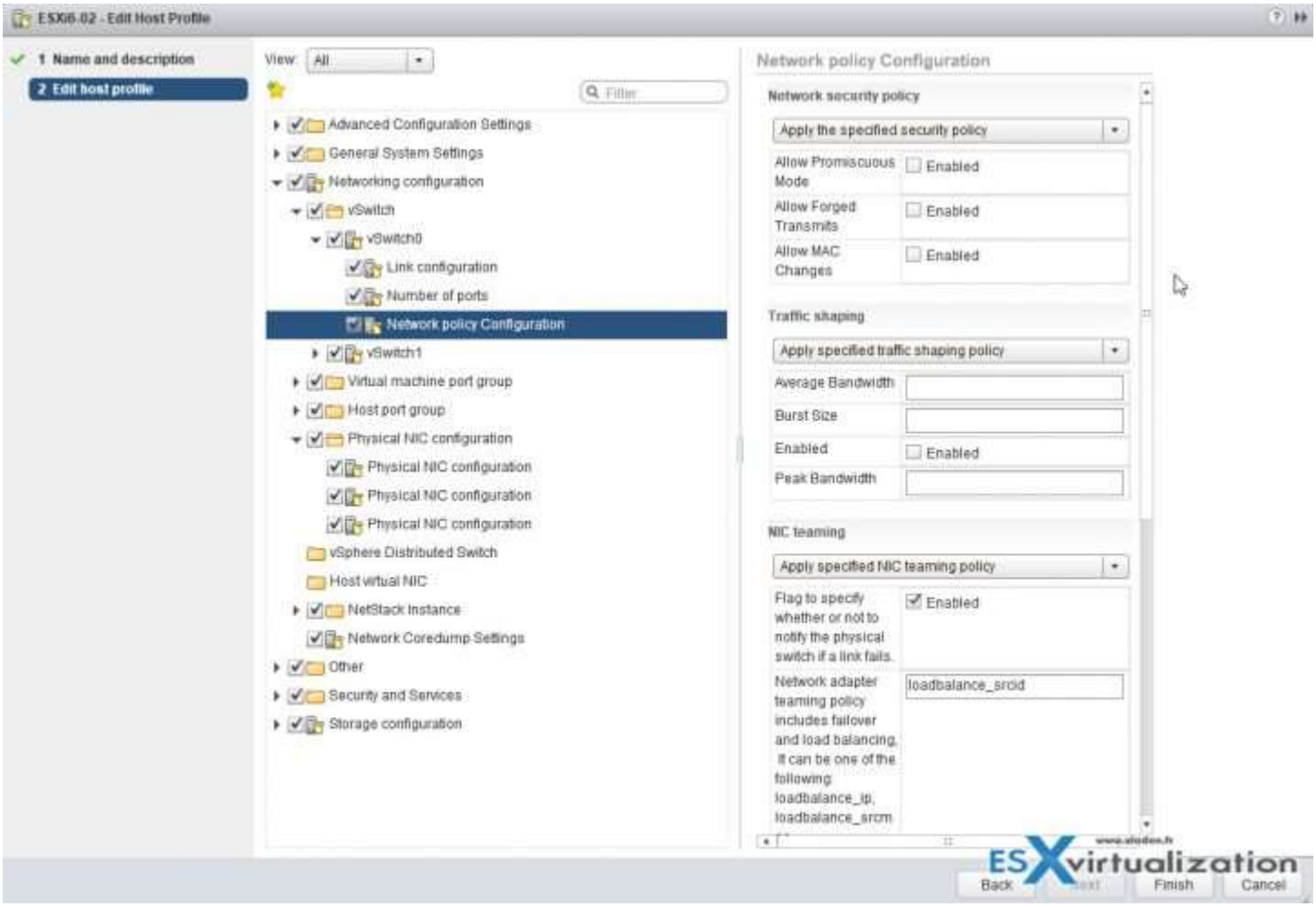
Select **Storage configuration** > **Pluggable Storage Architecture configuration** > **Host boot device configuration** and verify that this LUN is correctly captured.

Remediate the profile to the reference host for the changes in the sharing state to take effect on the reference host. If you must re-extract the profile (for example, if you attach more shared SAN boot LUNs to your cluster), you do not need to reconfigure sharing for devices that you previously configured.

Modify and apply switch configurations across multiple hosts using a Host Profile

After creating and extracting a host profile from a host, you can apply specific settings for network switch configs, such as network policy configuration, number of ports, link configuration etc. It is a per-switch setting so if your environment has multiple vSwitches you must go through all of those.

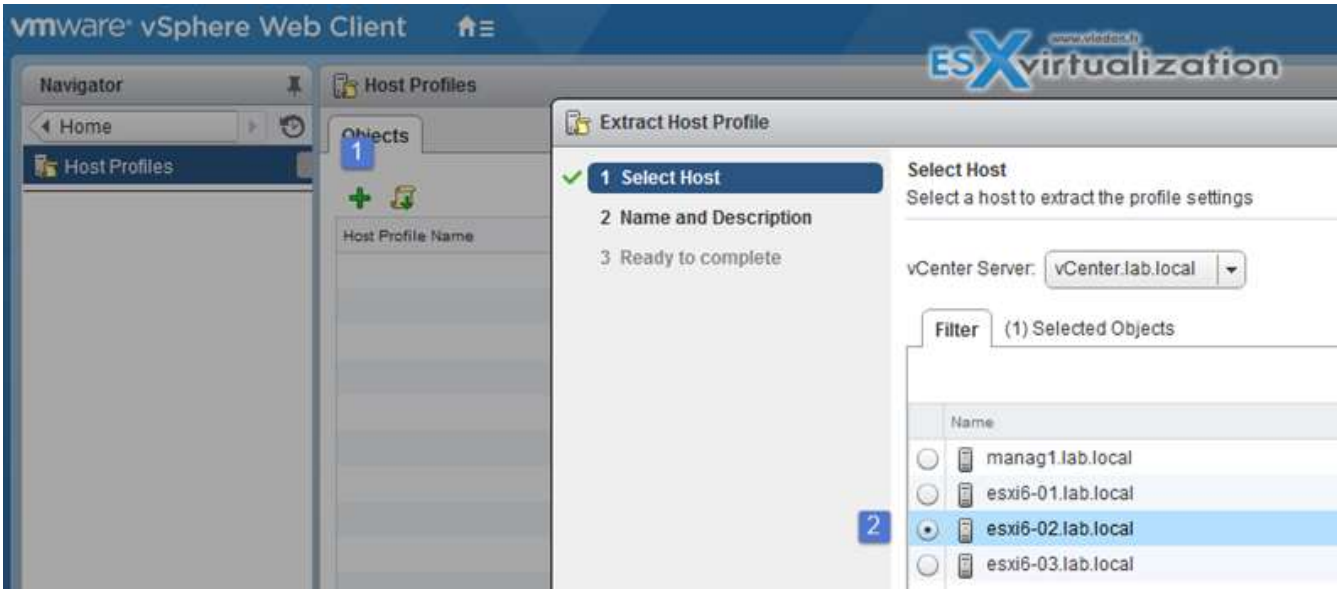
Below is an example.



CREATE/EDIT/REMOVE A HOST PROFILE FROM AN ESXI HOST

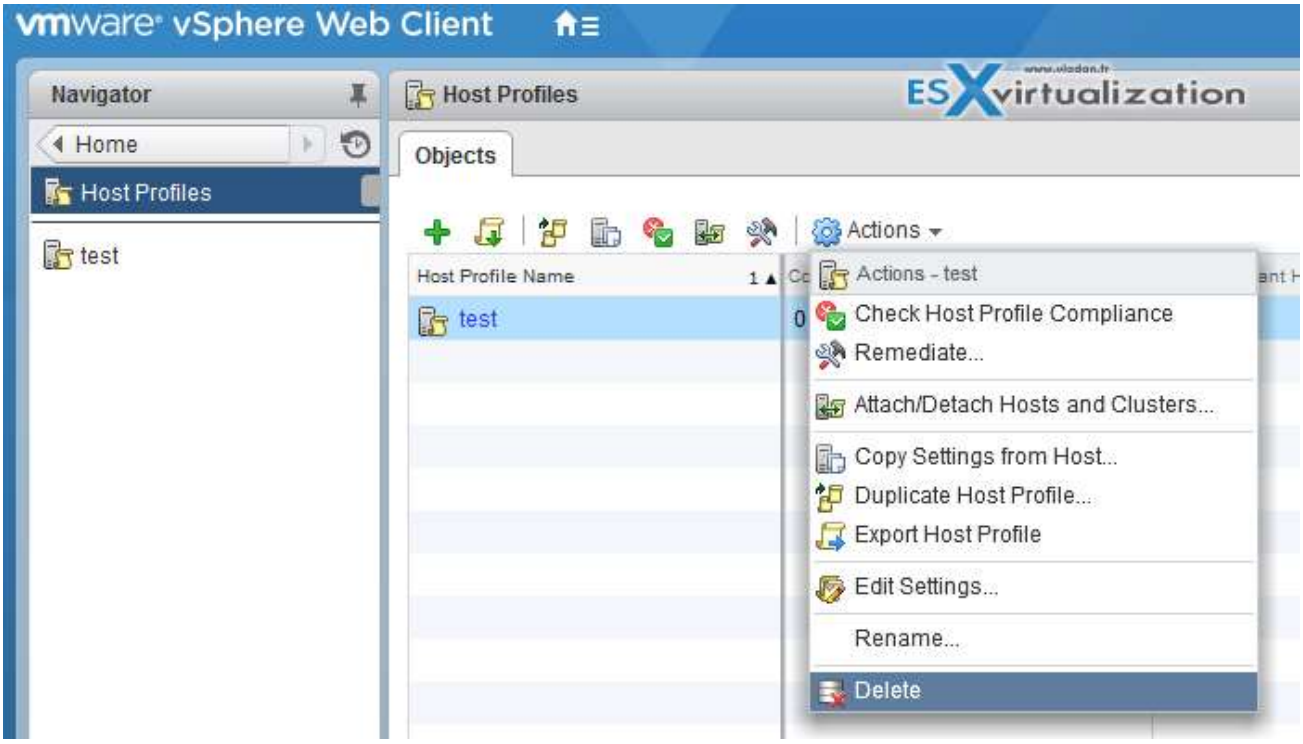
You create a Host Profile by extracting a configuration from a reference host.

vSphere **web client** > **Host profiles** > **Click the Plus sign** > Select **Host** > Enter **Name** for the host profile > **Next** > **Finish**



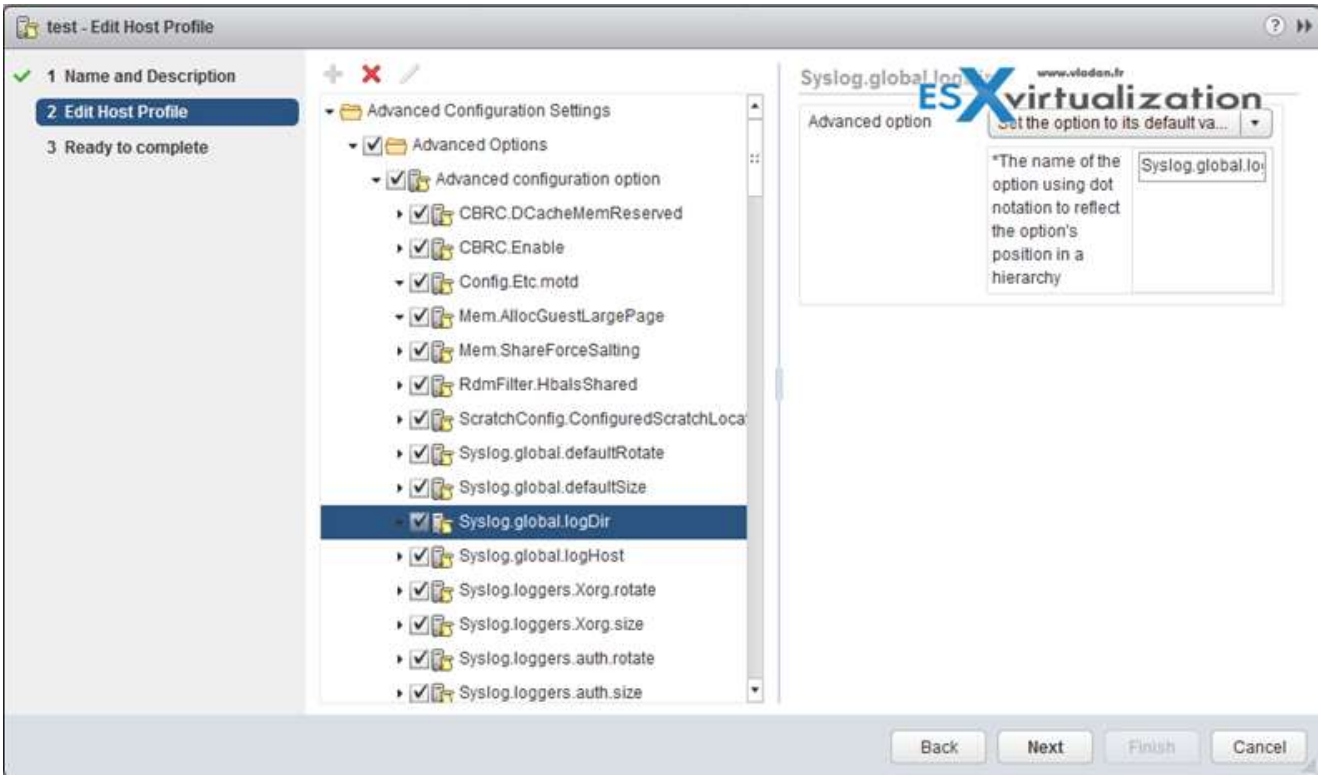
TO DELETE HOST PROFILE:

Select the host profile to delete > **Actions** > **delete**



TO EDIT HOST PROFILE:

Select the Host profile > **Actions** > **Edit** settings > **Next** > **Edit Host profile** > When done, click **Finish**.



Host Profiles can be also used to validate the configuration of a host by checking compliance of a host or cluster against the Host Profile that is associated with that host or cluster.

Import/Export a Host Profile

You can import a profile from a file in the VMware profile format (.vpf).

When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported. You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

How it's done:

- Navigate to the **Host Profiles view** > Click the **Import Host Profile icon** > Click **Browse** > Enter the **Name and Description** for the imported Host Profile, and click **OK**.

Export a Host Profile - You can export a profile to a file that is in the VMware profile format (.vpf). When a host profile is exported, administrator and user profile passwords are not exported. This is a security measure and stops passwords from being exported in plain text when the profile is exported.

You will be prompted to re-enter the values for the password after the profile is imported and the password is applied to a host.

How it's done:

- **Navigate to the Host Profile** you want to export > **Right-click the profile** and select Export Host Profile > **Select the location** and **type the name** > **Save**.

Attach and apply a Host Profile to ESXi hosts in a cluster

Right-click the host > **Host Profiles** > **Attach** > Select **Host** > **Next > follow** assistant **Finish.**

Perform compliance scanning and remediation of an ESXi host and clusters using Host Profiles

In order to check compliance of a host or cluster, you can use host profile.

Navigate to a Host Profile > Click the Check Host Profile Compliance icon > In the Objects tab, the compliance status is updated as Compliant, Unknown, or Non-compliant.

A non-compliant status indicates a discovered and specific inconsistency between the profile and the host. To resolve this, you should remediate the host. Any unknown status indicates that the compliance of the host could not be verified; to resolve the issue, remediate the host through the Host Profile.

Host profiles do not capture offline or unpresented devices. Any changes made to offline devices after extracting a host profile will not make a difference to the compliance check results.

Enable or disable Host Profile components

You can decide whether a Host Profile component is applied or considered during compliance check. This allows administrators to eliminate non-critical attributes from consideration or ignore values that, while part of the Host Profile, are likely to vary between hosts.

Edit a Host Profile > Expand the Host Profile Component hierarchy until you reach the desired component or component element > Disable the checkbox next to a component (enabled by default) to remove it from being applied during remediation or considered during a profile compliance check.

This topic heavily used "vSphere Host Profiles" PDF and vSphere 6.5 documentation set, available from VMware documentation. Check for the latest versions online.

VCP6.5-DCV Objective 9.1 - Configure vSphere HA Cluster Features

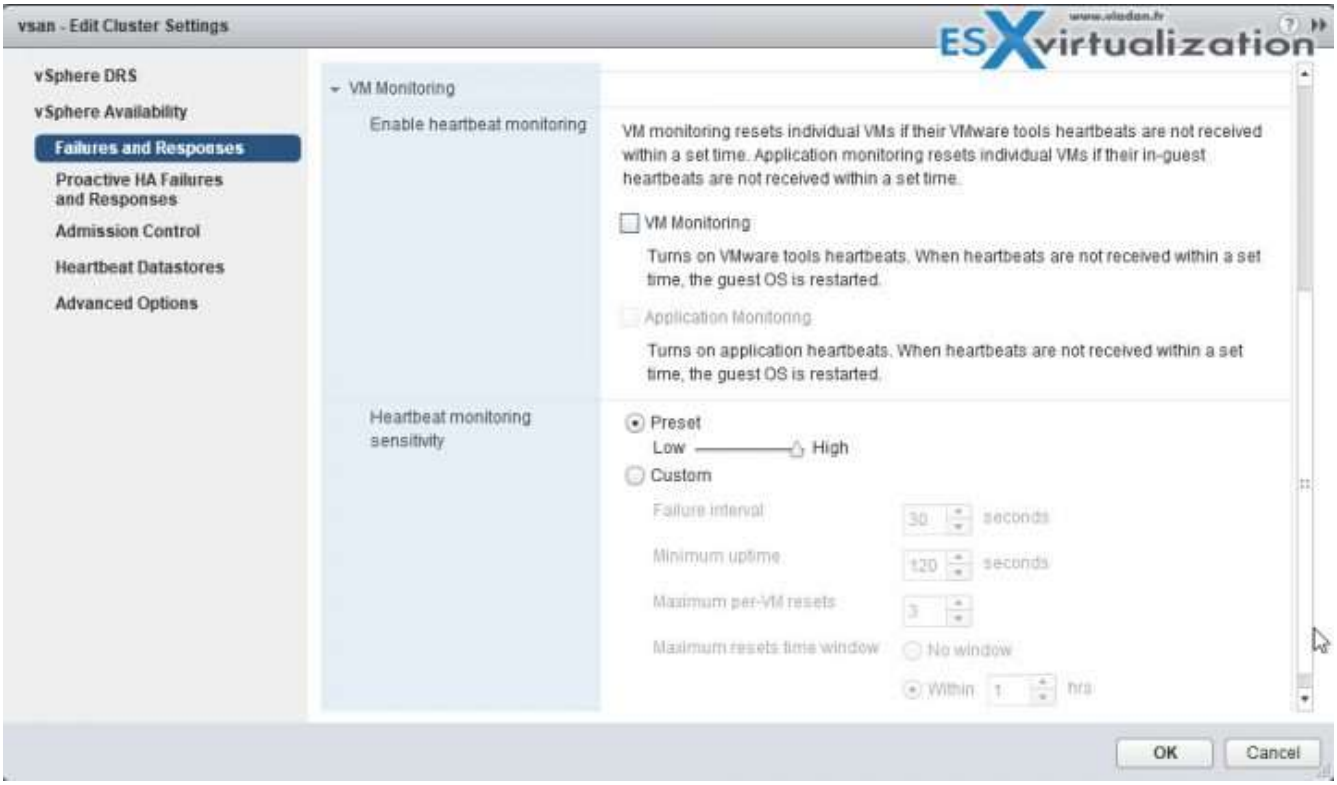
Modify vSphere HA cluster settings

As you know, vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts. There is a small service interruption, the time to restart the VMs.

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 of individual VMs if their VM tools heartbeats are not received within a certain time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.



CONFIGURE A NETWORK FOR USE WITH HA HEARTBEATS

VMware recommends redundant management network connections for vSphere HA.

On legacy ESX hosts in the cluster, vSphere HA communications travel over all networks that are designated as service console networks. VMkernel networks are not used by these hosts for vSphere HA communications. To contain vSphere HA traffic to a subset of the ESX console networks, use the ***allowedNetworks*** advanced option.

On ESXi hosts in the cluster, vSphere HA communications, by default, travel over VMkernel networks. With an ESXi host, if you want to use a network other than the one vCenter Server uses to communicate with the host for vSphere HA, **you must explicitly enable the Management traffic checkbox**.

To keep vSphere HA agent traffic on the networks you have specified, configure hosts so vmkNICs used by vSphere HA do not share subnets with vmkNICs used for other purposes. vSphere HA agents send packets using any pNIC that is associated with a given subnet when there is also at least one vmkNIC configured for vSphere HA management traffic. Therefore, to ensure network flow separation, the vmkNICs used by vSphere HA and by other features **must be on different subnets**.

Network Isolation Addresses - A network isolation address is an IP address that is pinged to determine whether a host is isolated from the network. This address is pinged only when a host has stopped receiving heartbeats from all other hosts in the cluster. If a host can ping its network isolation address, the host is not network isolated, and the other hosts in the cluster have either failed or are network partitioned. However, if the host cannot ping its isolation address, it is likely that the host has become isolated from the network and no failover action is taken.

By default, the network isolation address is the default gateway for the host. Only one default gateway is specified, regardless of how many management networks have been defined. Use the das.isolationaddress[...] advanced option to add isolation addresses for additional networks.

Network Path Redundancy - Network path redundancy between cluster nodes is important for vSphere HA reliability. A single management network ends up being a single point of failure and can result in failovers although only the network has failed. If you have only one management network, any failure between the host and the cluster can cause an unnecessary (or false) failover activity if heartbeat datastore connectivity is not retained during the networking failure. Possible failures include NIC failures, network cable failures, network cable removal, and switch resets. Consider these possible sources of failure between hosts and try to minimize them, typically by providing network redundancy.

The first way you can implement network redundancy is at the NIC level with **NIC teaming**. Using a team of two NICs connected to separate physical switches improves the reliability of a management network. Because servers connected through two NICs (and through separate switches) have two independent paths for sending and receiving heartbeats, the cluster is more resilient. To configure a NIC team for the management network, configure the vNICs in vSwitch configuration for Active or Standby configuration. The recommended parameter settings for the vNICs are:

Default load balancing = route based on originating port ID
Failback = No

After you have added a NIC to a host in your vSphere HA cluster, you must reconfigure vSphere HA on that host.

In most implementations, NIC teaming provides sufficient heartbeat redundancy, but as an alternative, you can create a second management network connection attached to a separate virtual switch.

Redundant management networking allows the reliable detection of failures and prevents isolation or partition conditions from occurring because heartbeats can be sent over multiple networks. The original management network connection is used for network and management purposes.

When the second management network connection is created, vSphere HA sends heartbeats over both management network connections. If one path fails, vSphere HA still sends and receives heartbeats over the other path.

APPLY AN ADMISSION CONTROL POLICY FOR HA

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

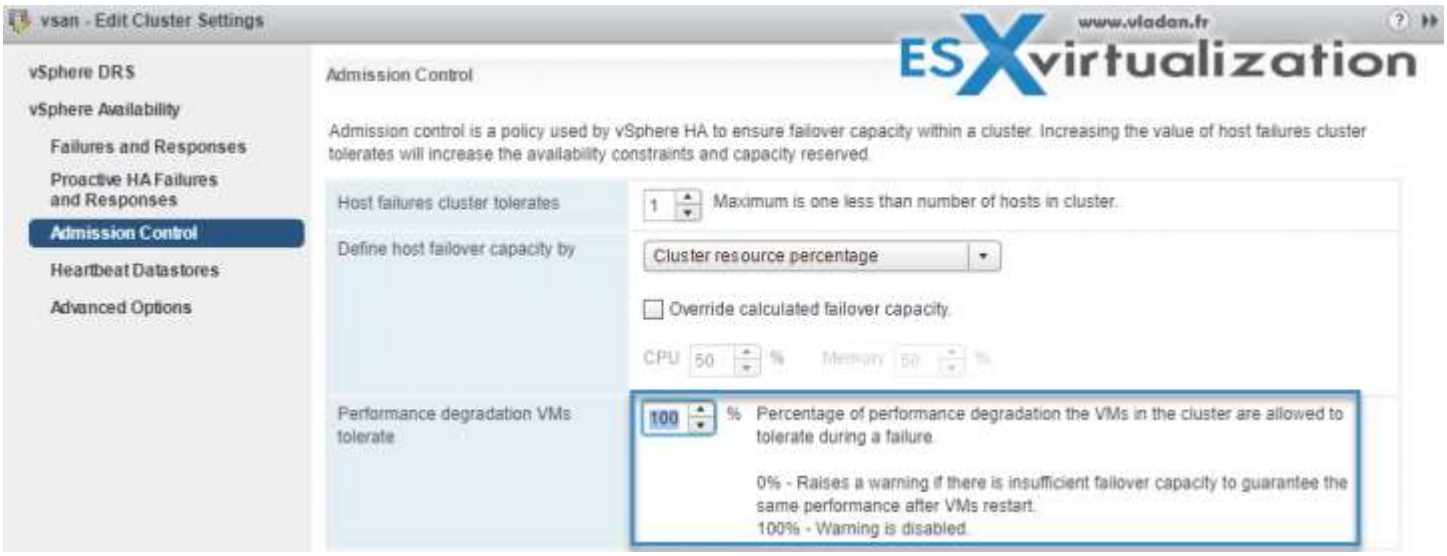
- **The new default is Cluster resource Percentage** – The configuring workflow for admission control is a little bit simpler. You first define a parameter how many failed hosts you want to tolerate within your cluster, and

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 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.

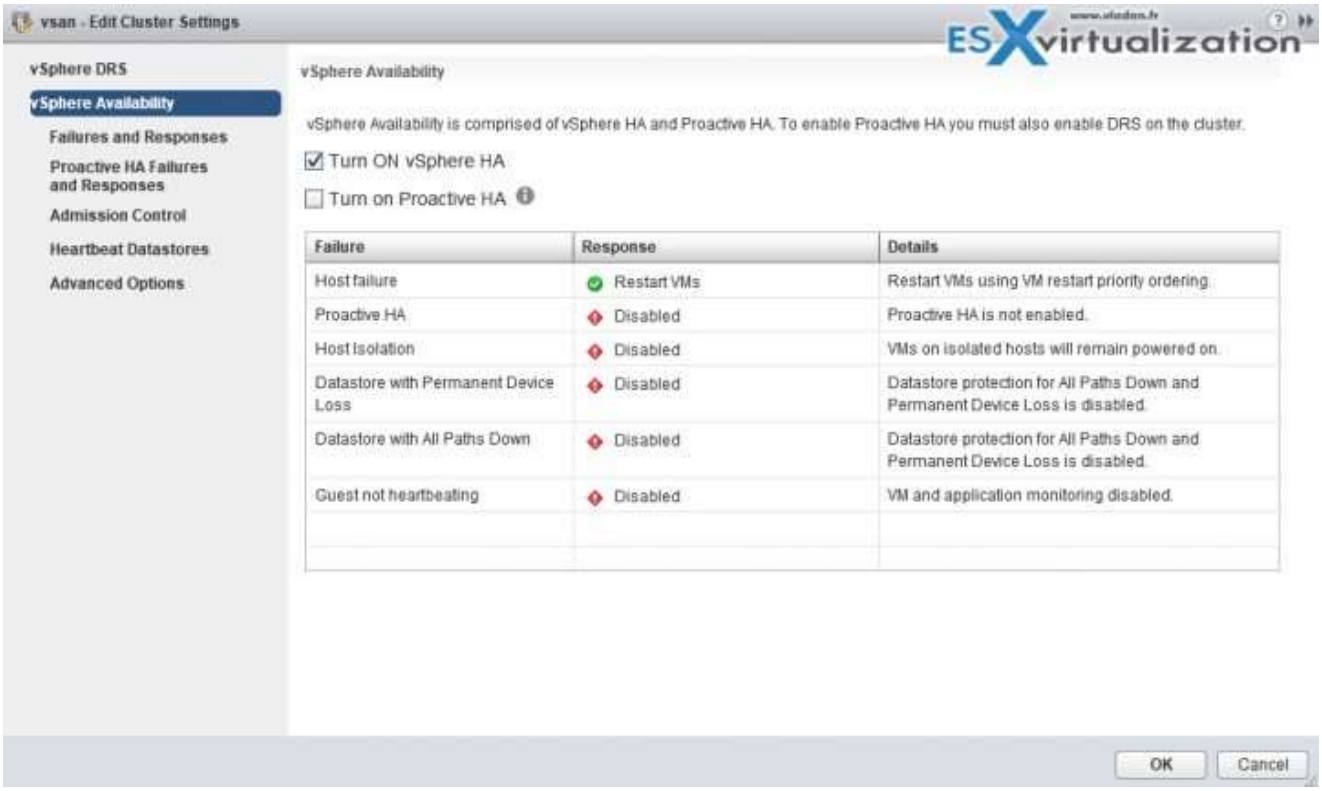
Dedicated Failover Host - You pick a dedicated host which comes into a play when there is a host failure. This host is a "spare" so it does not have running VMs during normal operations. Waste of resources.

ENABLE/DISABLE VSPHERE HA SETTINGS

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

To enable/disable individual settings, select the setting on the left, to activate/deactivate on the right.

Check above for "failure and responses" section.



CONFIGURE DIFFERENT HEARTBEAT DATASTORES FOR AN HA CLUSTER

In case the Master cannot communicate with a slave (doesn't receive the heartbeats), but the heartbeat datastore answers, the server is still working. So if that's the case, the **host** **is partitioned from the network** or isolated. The Datastore heartbeat function helps greatly to determine the difference between host which failed and host that has just been isolated from others.

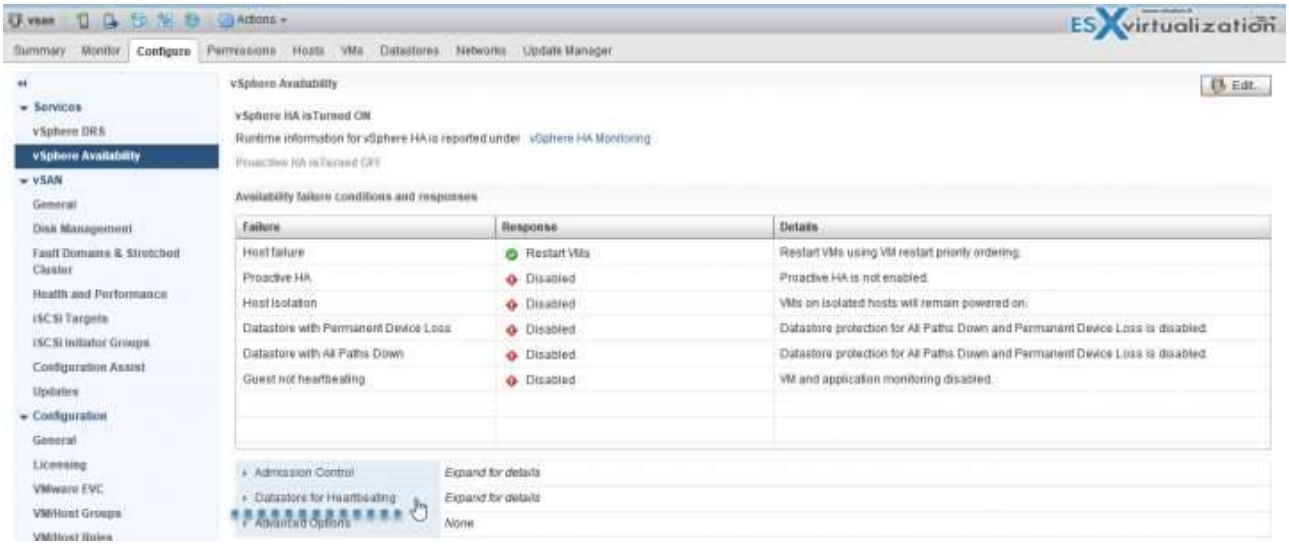
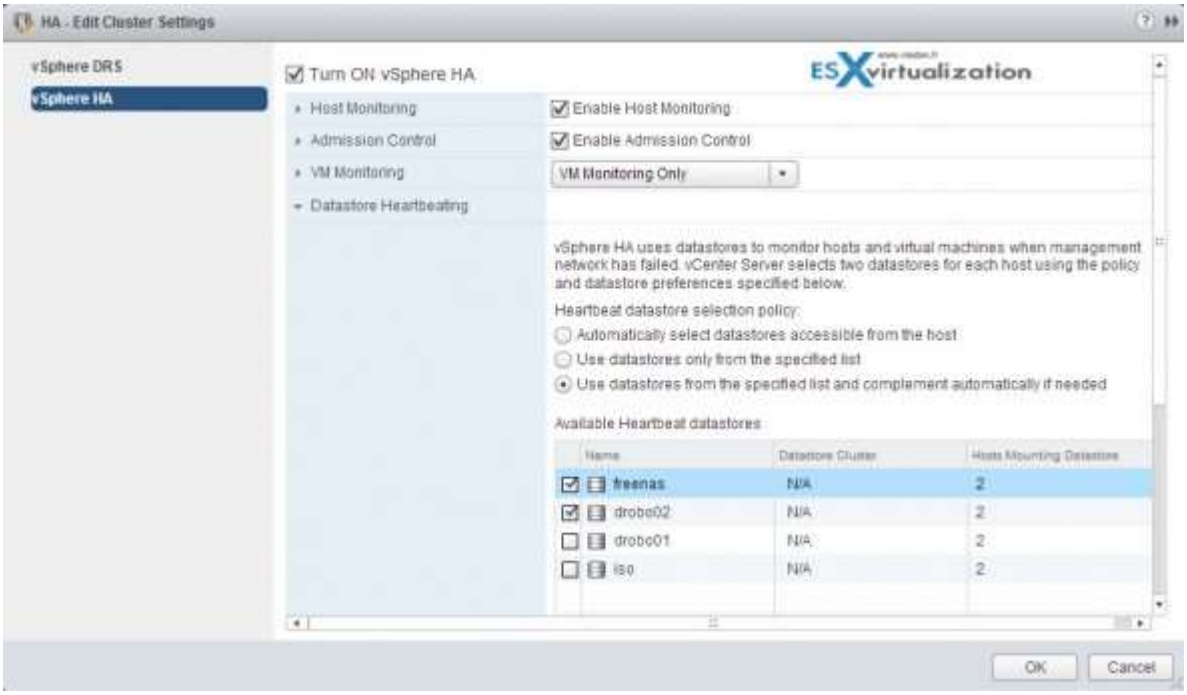


Figure 1: **Select cluster > Configure > vSphere Availability > Datastore for hearbeating.**



vCenter automatically selects **at least two datastores** from the shared datastores. It's preferable to have VMware Datastore heartbeating selected on every NAS/SAN device you have. In my example above I have two shared datastores checked, each on a different storage device.

Apply virtual machine monitoring for a cluster

Same as above, section "Modify vSphere HA cluster settings".

Configure Virtual Machine Component Protection (VMCP) settings

VMCP can be found also at the "Modify vSphere HA cluster settings" section.

VMCP settings are settings for datastores with Permanent Device Lost (PDL) and All paths down (APD).

Implement vSphere HA on a vSAN cluster

To use vSphere HA with Virtual SAN, you must be aware of certain considerations and limitations for the interoperability of these two features.

ESXi Requirements:

- All the cluster's ESXi hosts must be version 5.5 or later.
- The cluster must have a minimum of three ESXi hosts.

Virtual SAN has its own network. If Virtual SAN and vSphere HA are enabled for the same cluster, the HA interagent traffic flows over this storage network rather than the management network. vSphere HA uses the management network only if Virtual SAN is disabled. vCenter Server chooses the appropriate network if vSphere HA is configured on a host.

You can enable Virtual SAN only if vSphere HA is disabled. If you change the Virtual SAN network configuration, the vSphere HA agents do not automatically pick up the new network settings. So you must:

Disable host monitoring for HA cluster > Make vSAN network changes > Right-click all hosts in the vSAN cluster > Reconfigure for vSphere HA. > Re-enable Host Monitoring for HA cluster.

Capacity Reservation Settings - When you reserve capacity for your vSphere HA cluster with an admission control policy, you must coordinate this setting with the corresponding Virtual SAN seeing that ensures data accessibility on failures. Specifically, the Number of Failures Tolerated settng in the Virtual SAN rule set must not be lower than the capacity that the vSphere HA admission control settng reserved.

For example, if the Virtual SAN rule set allows for only two failures, the vSphere HA admission control policy must reserve capacity that is equivalent to only one or two host failures. If you are using the Percentage of Cluster Resources Reserved policy for a cluster that has eight hosts, you must not reserve more than 25% of the cluster resources. In the same cluster, with the Host Failures Cluster Tolerates policy, the setting must not be higher than two hosts.

If vSphere HA reserves less capacity, failover activity might be unpredictable. Reserving too much capacity overly constrains the powering on of virtual machines and intercluster vSphere vMotion migrations.

Explain how vSphere HA communicates with Distributed Resource Scheduler and Distributed Power Management

Using vSphere HA with Distributed Resource Scheduler (DRS) combines automatic failover with load balancing. This combination can result in a more balanced cluster after vSphere HA has moved virtual machines to different hosts. When vSphere HA performs failover and restarts virtual machines on different hosts, its first priority is the immediate availability of all virtual machines. After the virtual machines have been restarted, those hosts on which they were powered on might be heavily loaded, while other hosts are comparatively lightly loaded. vSphere HA uses the virtual machine's CPU and memory reservation and overhead memory to determine if a host has enough spare capacity to accommodate the virtual machine.

In a cluster using DRS and vSphere HA with admission control turned on, virtual machines might not be evacuated from hosts entering maintenance mode. This behavior occurs because of the resources reserved for restarting virtual machines in the event of a failure. You must manually migrate the virtual machines off of the hosts using vMotion.

Note: This topic used partly the "vSphere ESXi vCenter server 6.5 availability" PDF.

VCP6.5-DCV Objective 9.2 - Configure vCenter Server Appliance (VCSA) HA

Enable and Configure vCSA HA

To set the foundation for the vCenter HA network, you'll need to add a port group to each ESXi host and add a virtual NIC to the vCenter Server Appliance that later becomes the Active node. You have the option to set up the VCSA HA in two ways:

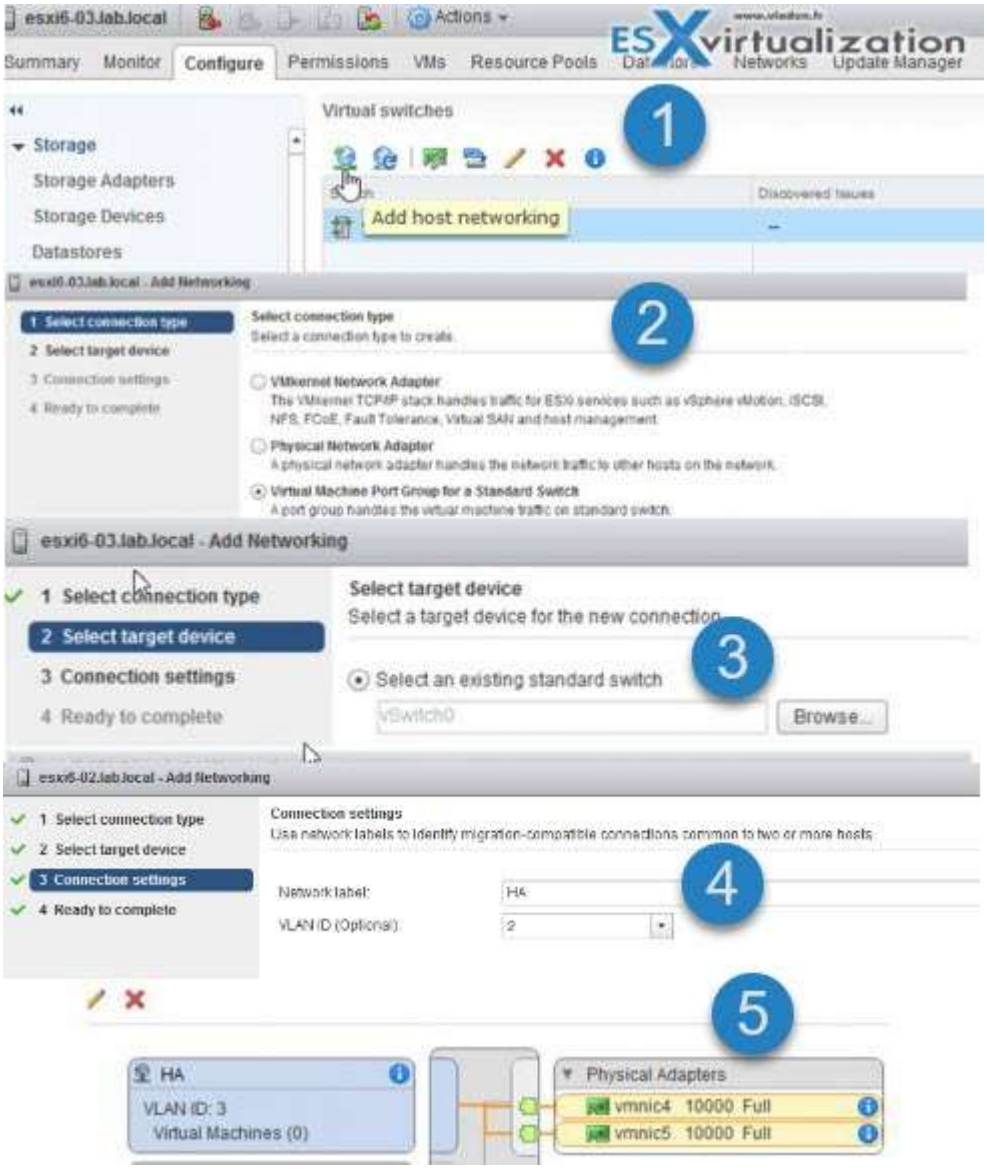
- Simple
- Advanced

The simple way first. After some network configuration, you will create a three-node cluster that contains Active, Passive and Witness nodes.

Here is the network part config:

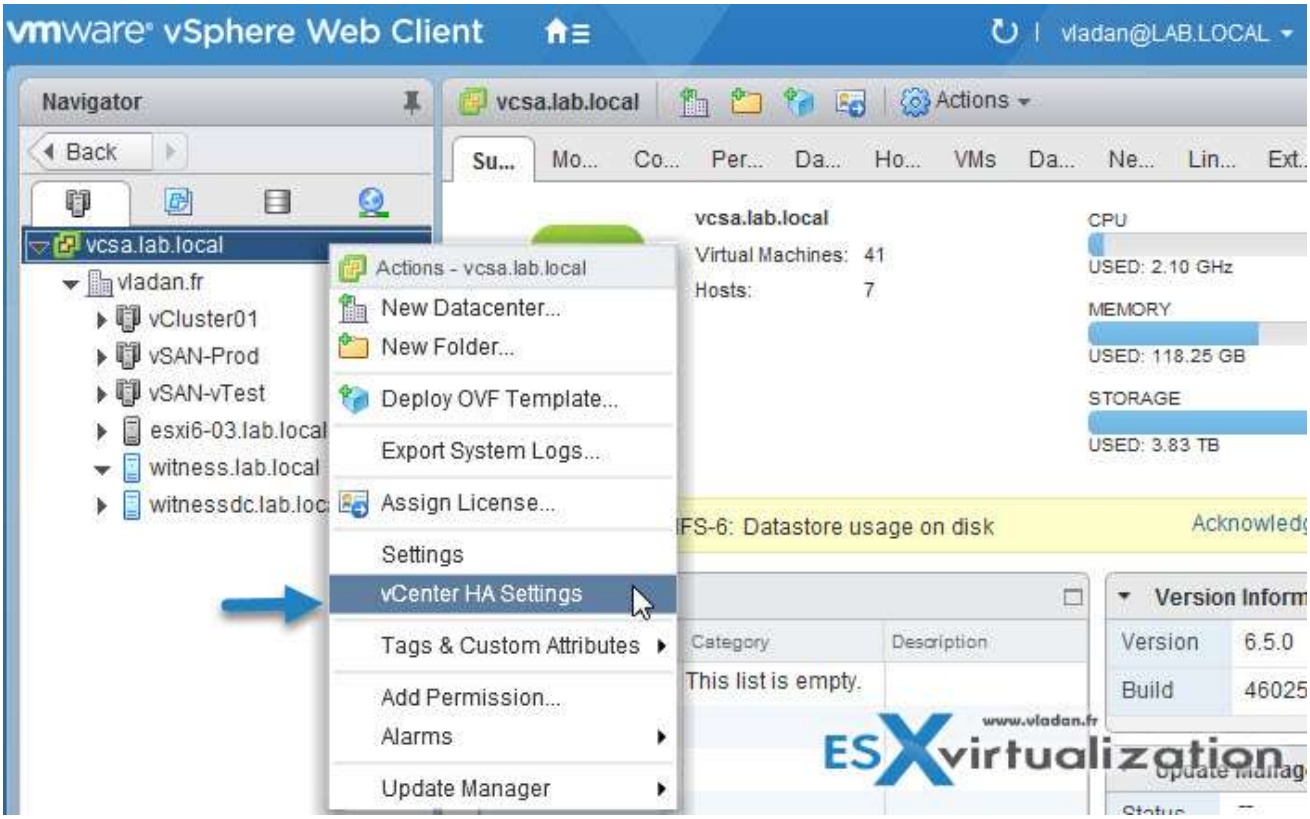
Create a vSphere HA network. Open **vSphere web client and select host. > configure > Networking > virtual switches.**

Here is the workflow…

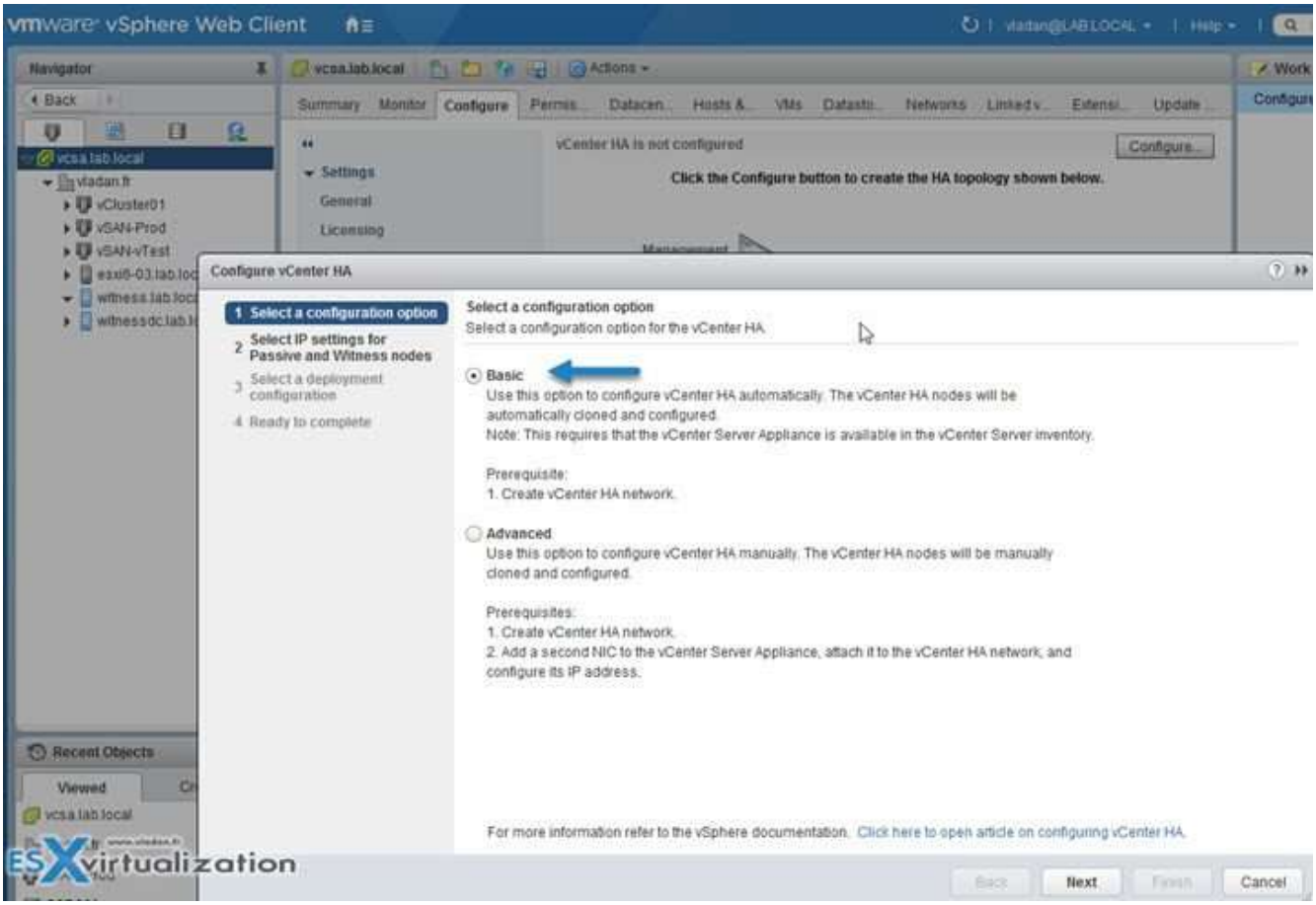


If you're on Standard switches, you'll have to do that for all the hosts in the management cluster.

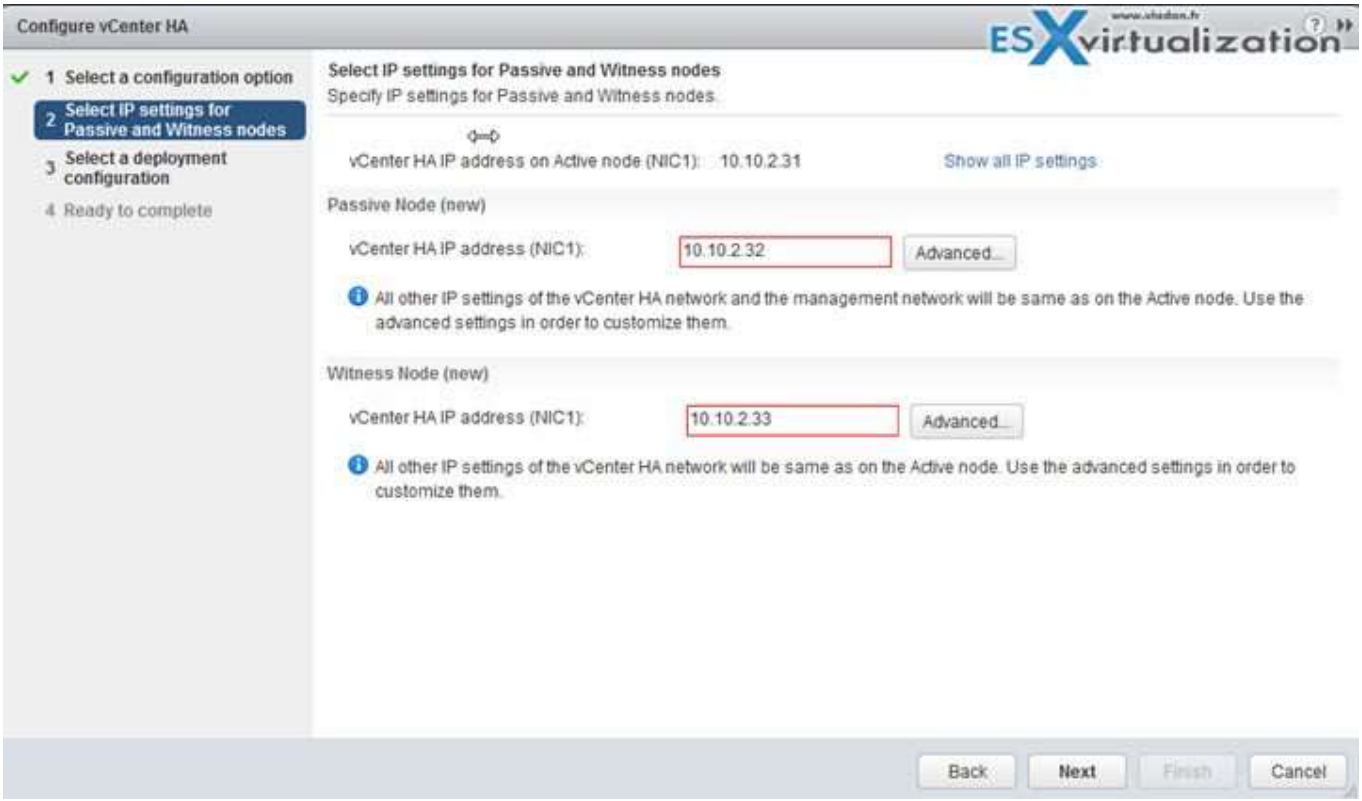
Next, Start the main assistant which will configure the vCenter HA. After you log in to the vSphere Web client, **select the vCenter Server** > do a **right click** > **vCenter HA settings**



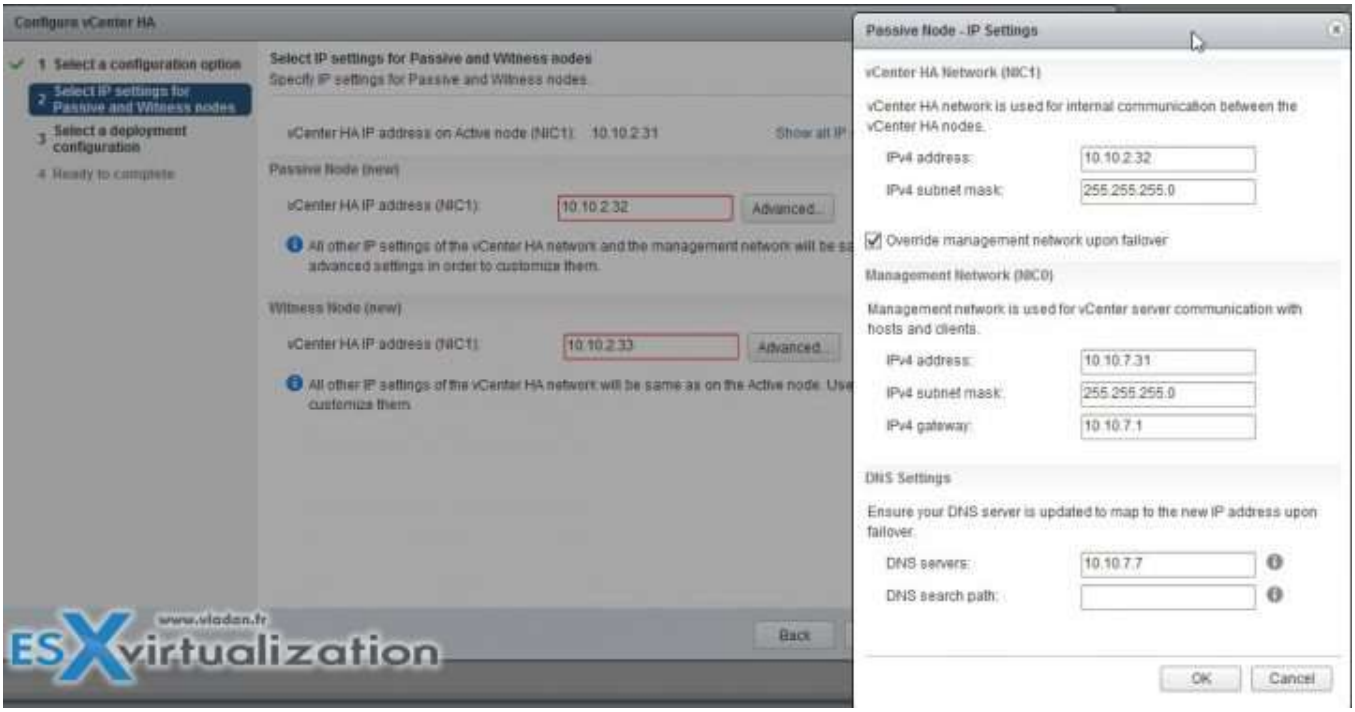
You'll have a nice screen telling you that vCenter HA is not configured. Hit the Configure button to start the assistant which has the first radio button preselected. It is the Basic option. Click the next button. (Note that you'll need to be a member of the SSO Admin group).



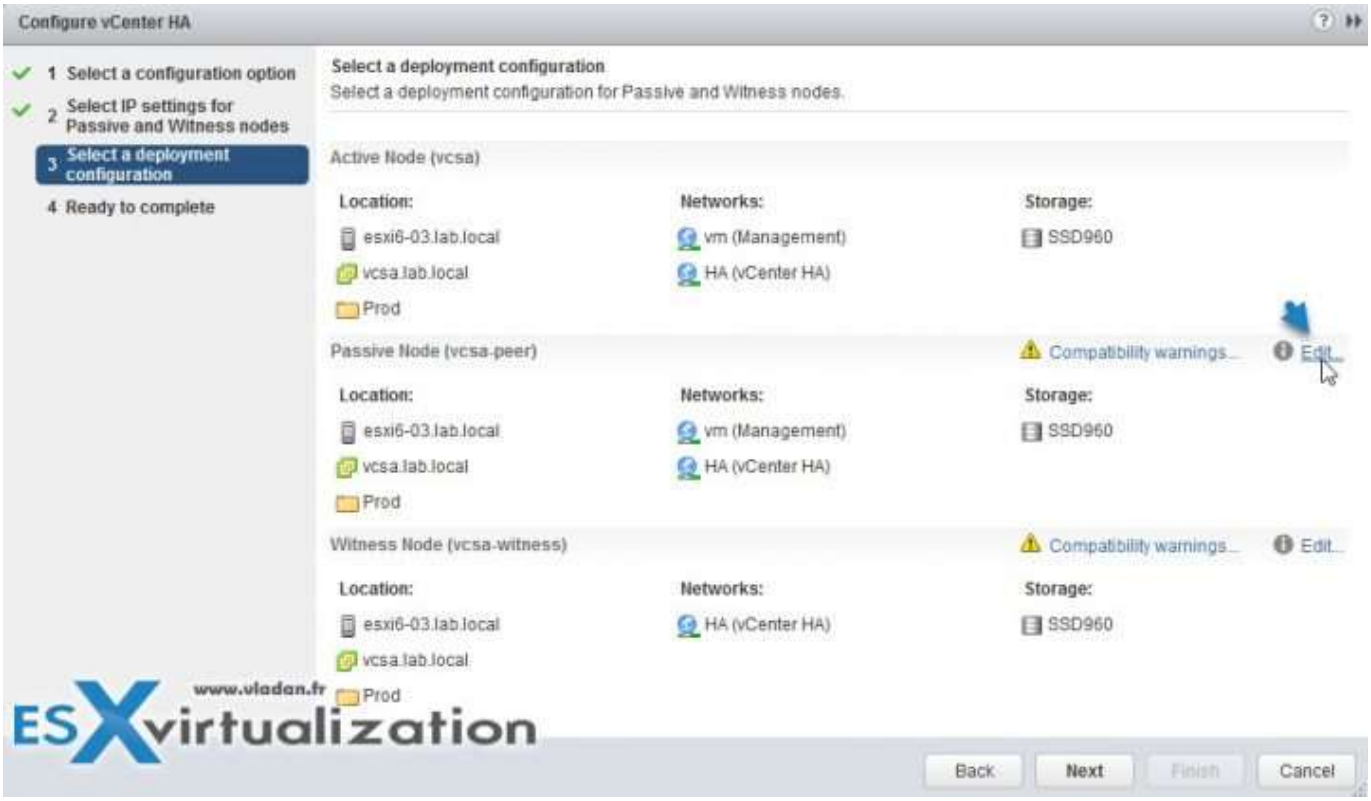
Next page will show up :



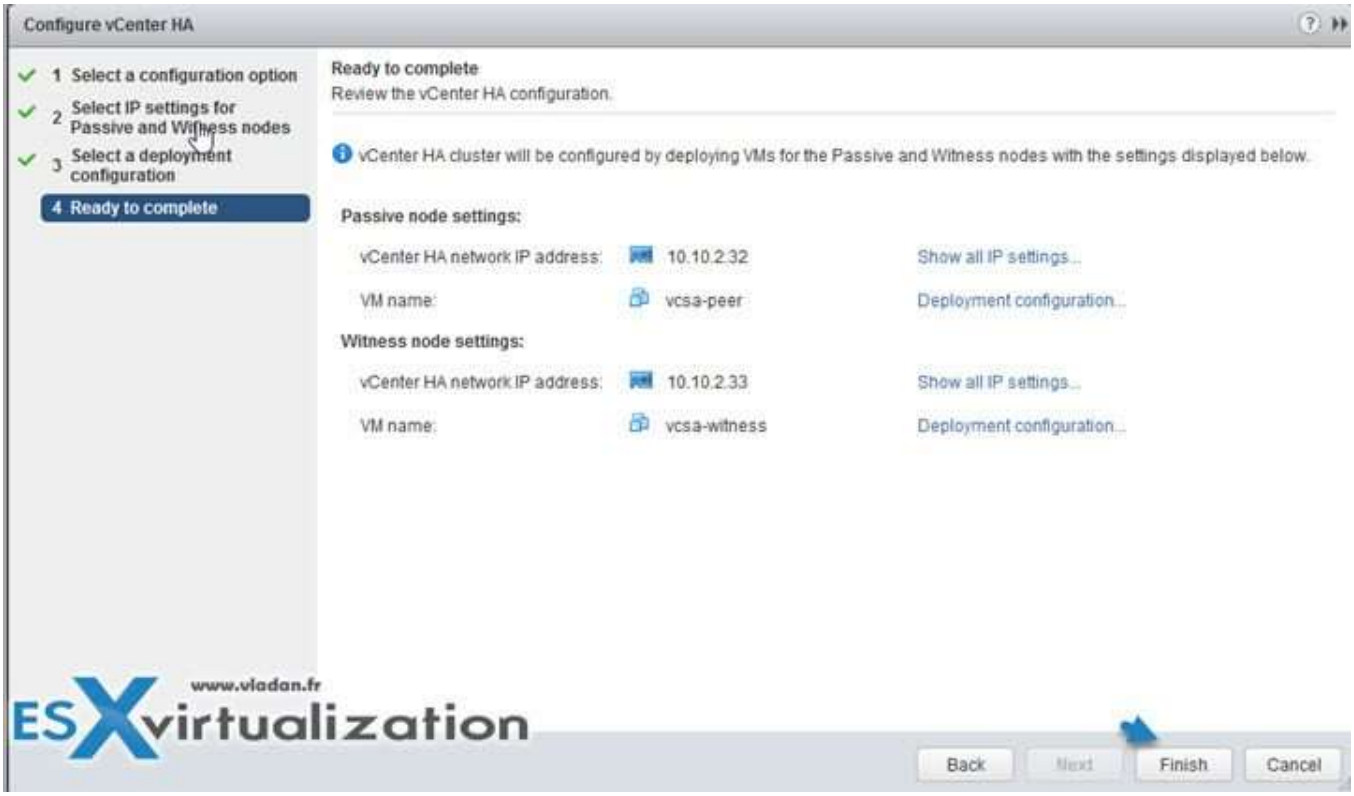
And when you click the **Advanced button** on the Passive node you can see that you can override management network upon failover. (There is a checkbox.)



Next, we move the passive node and the Witness node elsewhere.



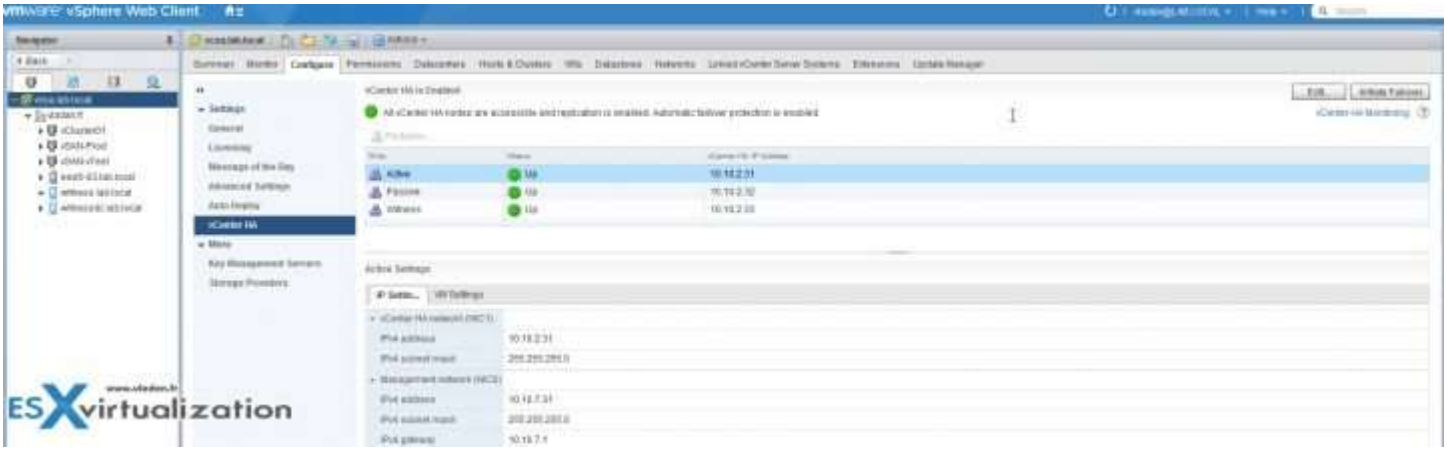
And then finally we can hit the Finish button.



This concludes the workflow. You should have 3 components running:

- VCSA (your primary active VCSA 6.5)
- VCSA-secondary (the passive node)
- VCSA-Witness (appliance running the tiebreaker code)

Here is the final screenshot…. You can see all 3 nodes up and running.



The Advanced option needs more manual steps, but at final, you might be able to adjust things that you would not be able to if you would have gone through the “Simple” config (example set a different SSO domain). The manual steps needed:

- Add manually a second vNIC to our main VCSA 6.5 – (the same as in “Simple” config)
- We need also to add an HA network – (the same as in “Simple” config)
- Clone Active Node manually, to have a Passive Node (and also assign an IP information through the OS customization wizard… yes, it takes longer)
- Clone Active Node manually, to have a Witness Node (and also assign an IP information through the OS customization wizard… yes, more and more manual steps)
- Create affinity and anti-affinity rules so DRS won’t place all 3 nodes on the same host.

Check the advanced config here:

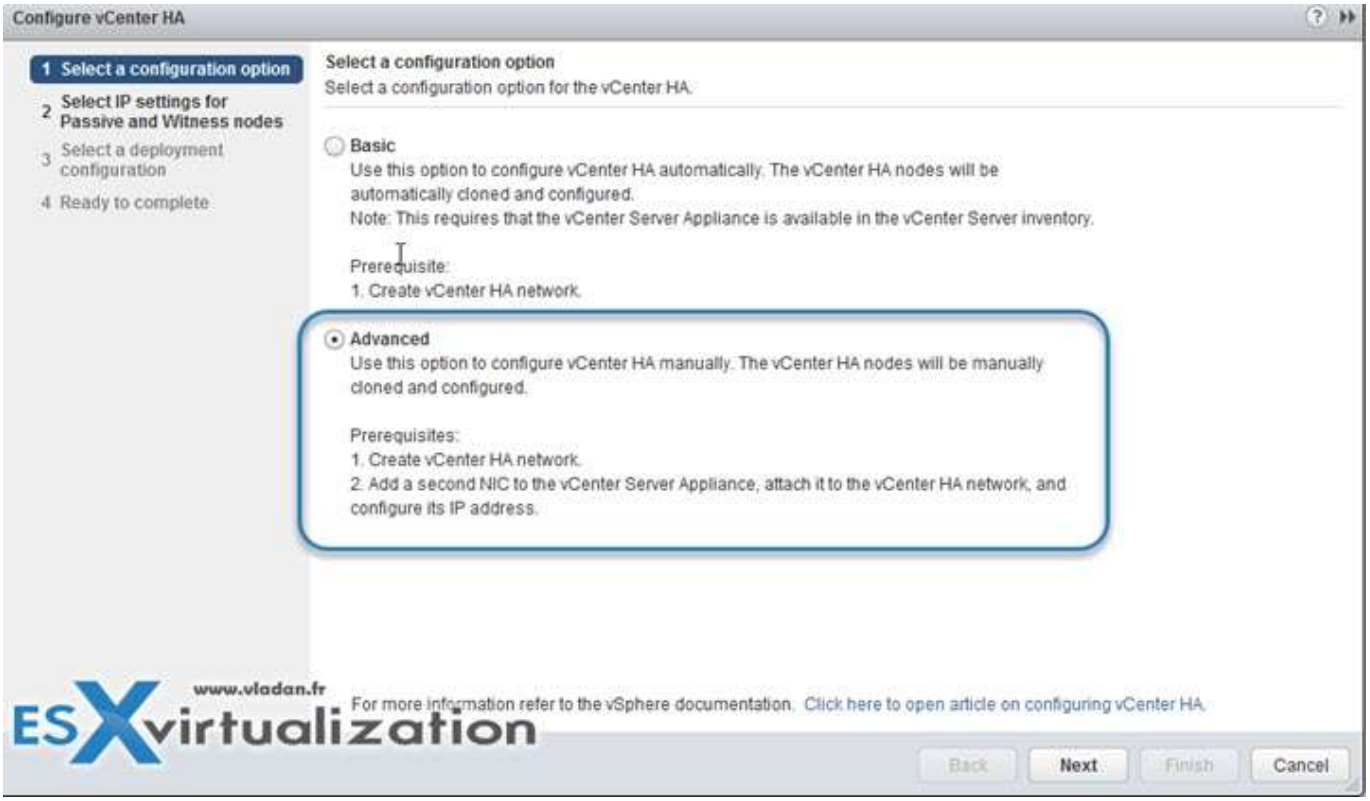
- VMware VCSA 6.5 Active-Passive Setup – Advanced Configuration

At one point you'll have to clone the active node (without exiting the HA wizard).

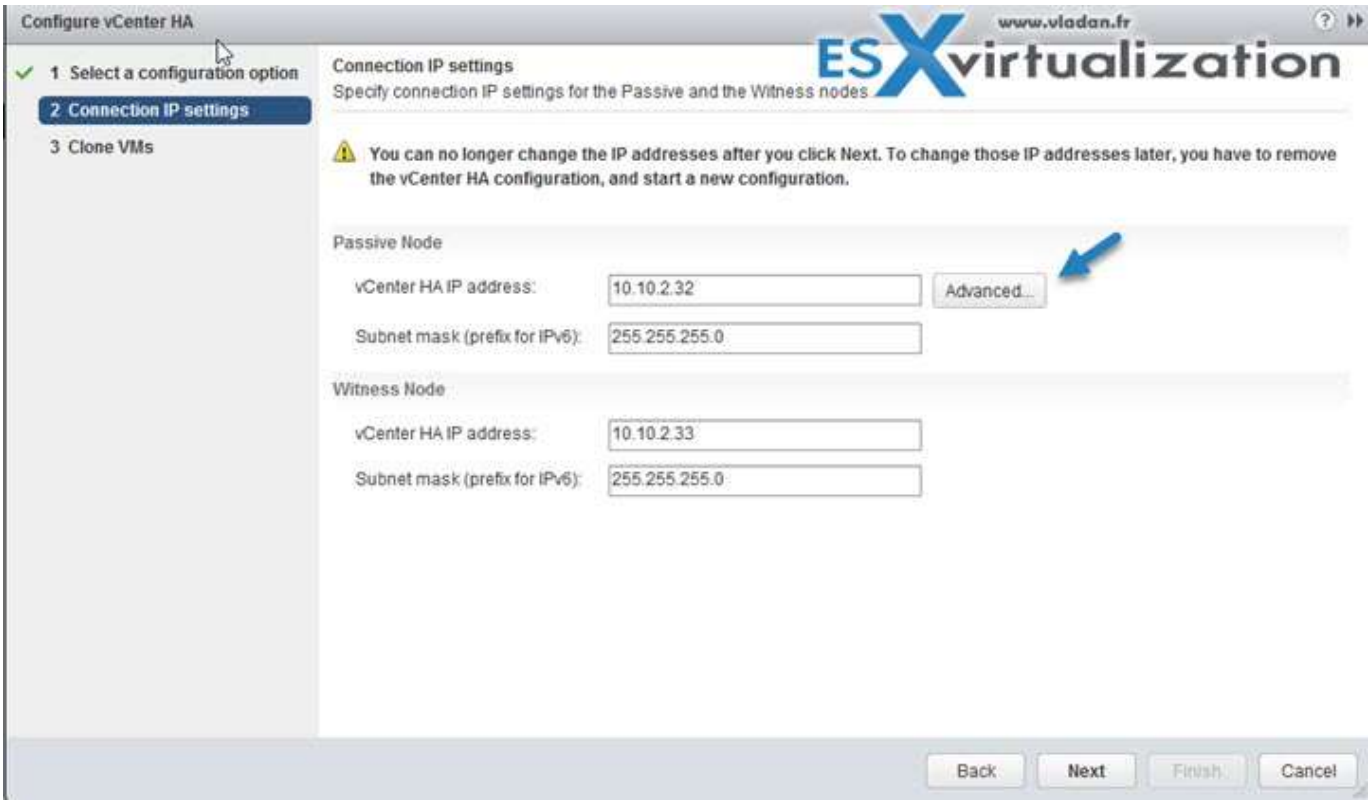
You'll have these options:

- New Virtual Machine Name - Name of the Passive node. For example, use vcsa-peer.
- Select Compute Resource - Select Storage - Use a different target host and datastore than for the Active node if possible.
- Clone Options - Select the Customize the operating system and Power on virtual machine after creation check boxes and click the New Customization Spec icon on the next page. In the New Customization Spec wizard that appears specify the following.
- Use the same host name as the Active node - Ensure the timezone is consistent with the Active node. Keep the same AreaCode/Location with UTC as the Active node. If you have not specified AreaCode/Location with UTC while configuring the Active node, keep London in AreaCode/Location during cloning. London has 0.00 offset, so it keeps the clock to UTC without any offset.
- On the Configure Network page, specify the IP settings for NIC1 and NIC2, which map to the management interface and the vCenter HA interface. Leave the NIC2 Default Gateway blank.

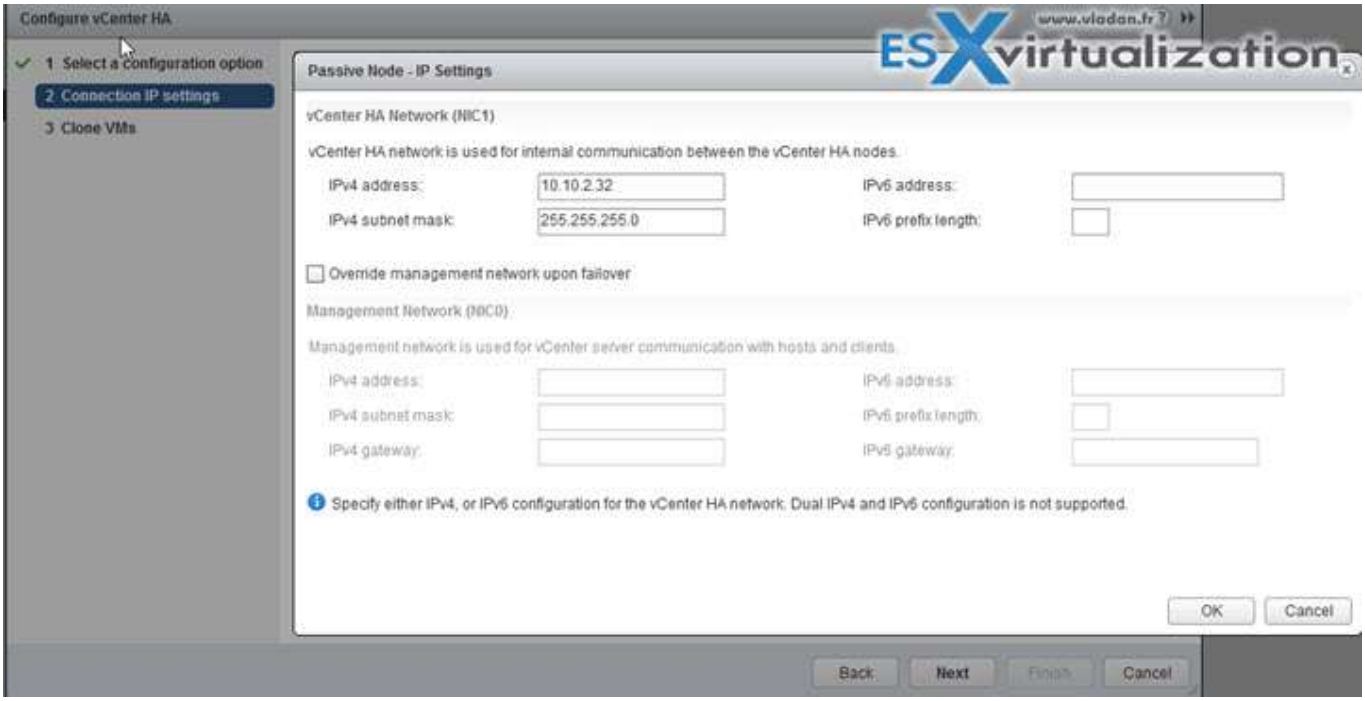
Choose the **Advanced** option.



Then enter the IP information concerning the **Passive** node and a **Witness** node.



The advanced section allows you to specify advanced override options for the management NIC (NIC0).

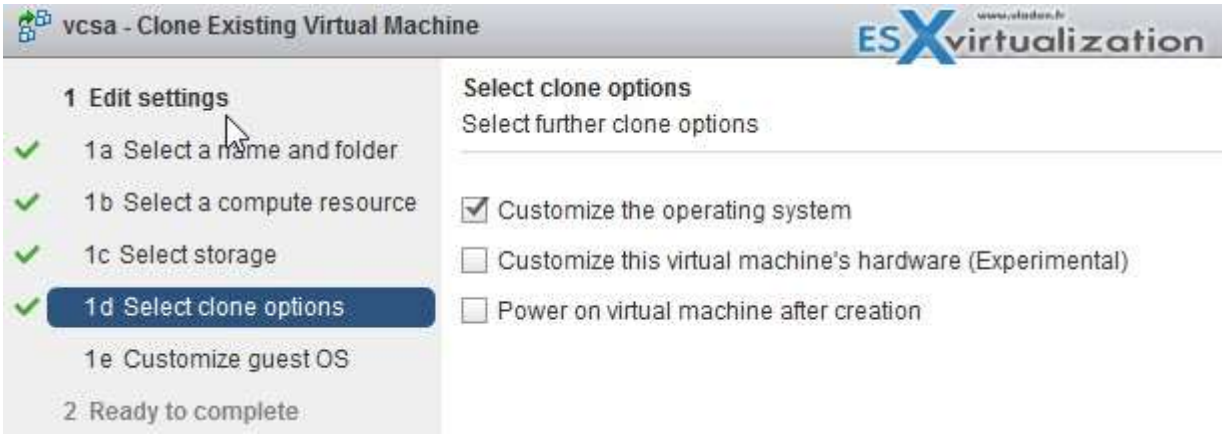


The system "watches" what you're entering and trying to correct the errors. Here is an example if you forgot to add a second NIC…. the system detects it.

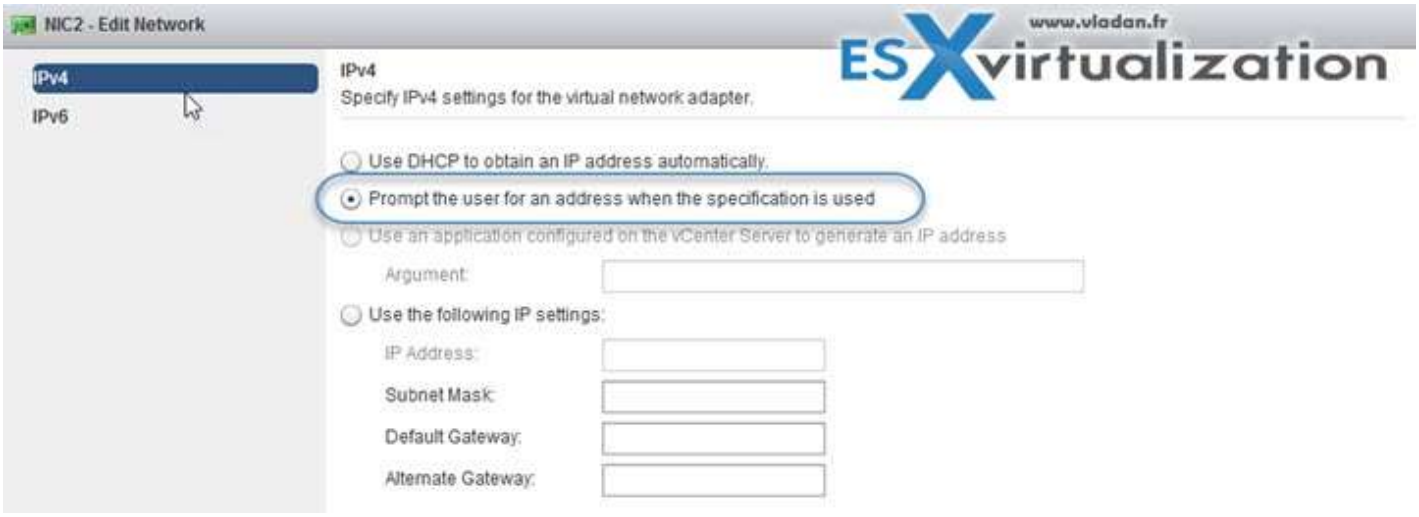
Next, you'll need manually clone the VM, otherwise, the assistant won't let you continue. So you'll have to open another browser window just for the cloning operation and:

- Put a name
- Select Compute
- Select Storage
- Select clone options

Etc, etc…



Basically, you have to prepare a customized template which will be used during the clone operation:



Then, when during the cloning, you'll have the wizard like this…

then the recap screen….

Then rinse and repeat for the Witness. Also needed are the affinity and anti-affinity rules. I assume that you know your way. And at the end, you should end up again with the screen like this one, where you'll have one appliance with the **Active** role, one with **Passive** role and one with **Witness** role.

The same as with Simple config. At this screen you can manually initiate failover with the **Initiate Failover** button.

UNDERSTAND AND DESCRIBE THE ARCHITECTURE OF VCSA HA

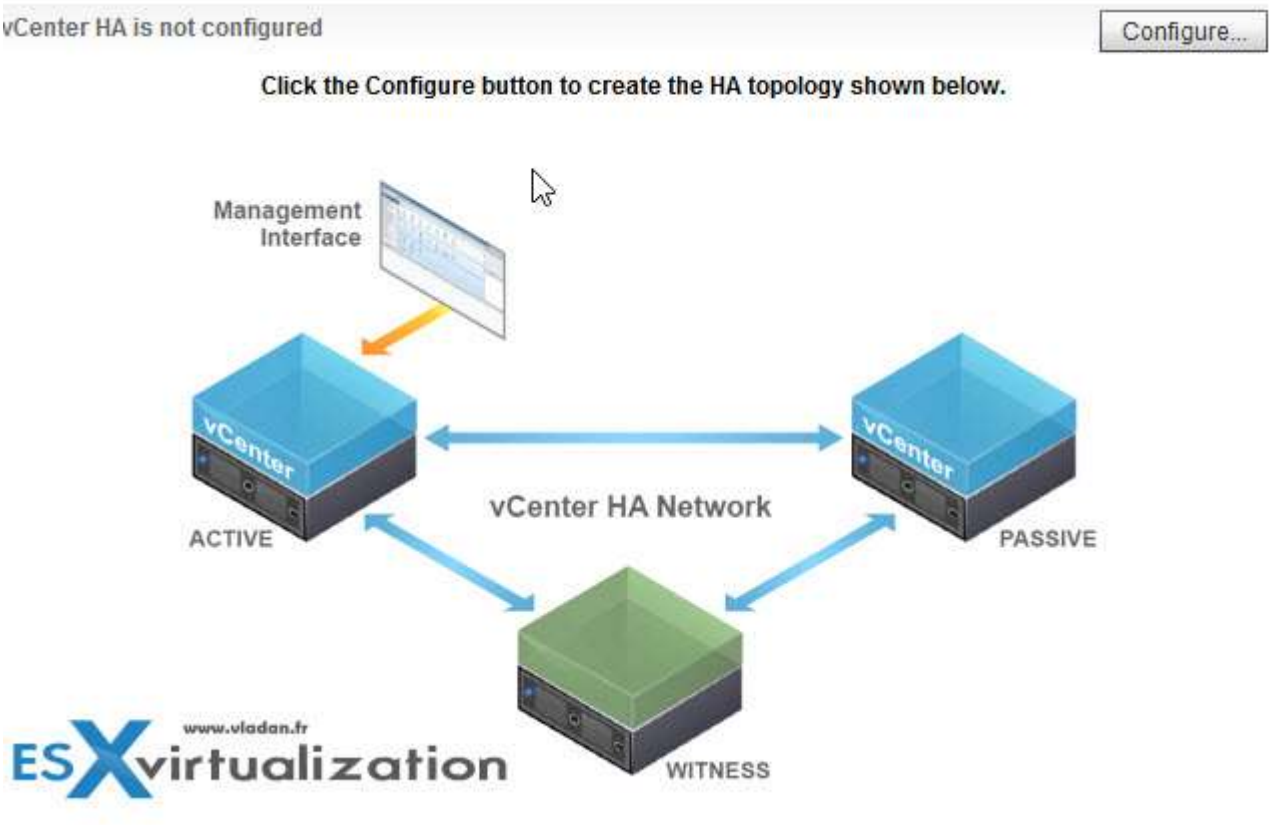
VCSA HA Nodes are 3 in total:

Active - Runs the active vCenter Server Appliance instance. Uses a public IP address for the management interface. and uses the vCenter HA network for replication of data to the Passive node. Also, it uses the vCenter HA network to communicate with the Witness node.

Passive - Is initially a clone of the Active node. It constantly receives updates from and synchronizes state with the Active node over the vCenter HA network. And it automatically takes over the role of the Active node if a failure occurs.

Witness - Is a lightweight clone of the Active node. Provides a quorum to protect against split-brain situations.

The active node is your usual VCSA 6.5 which manages your infrastructure, and the passive node is a node which sits there doing nothing, just receiving files from the active node.



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

Deploying each of the nodes on a different ESXi instance protects against hardware failure. Adding the three ESXi hosts to a DRS cluster can further protect your environment.

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

Check also:

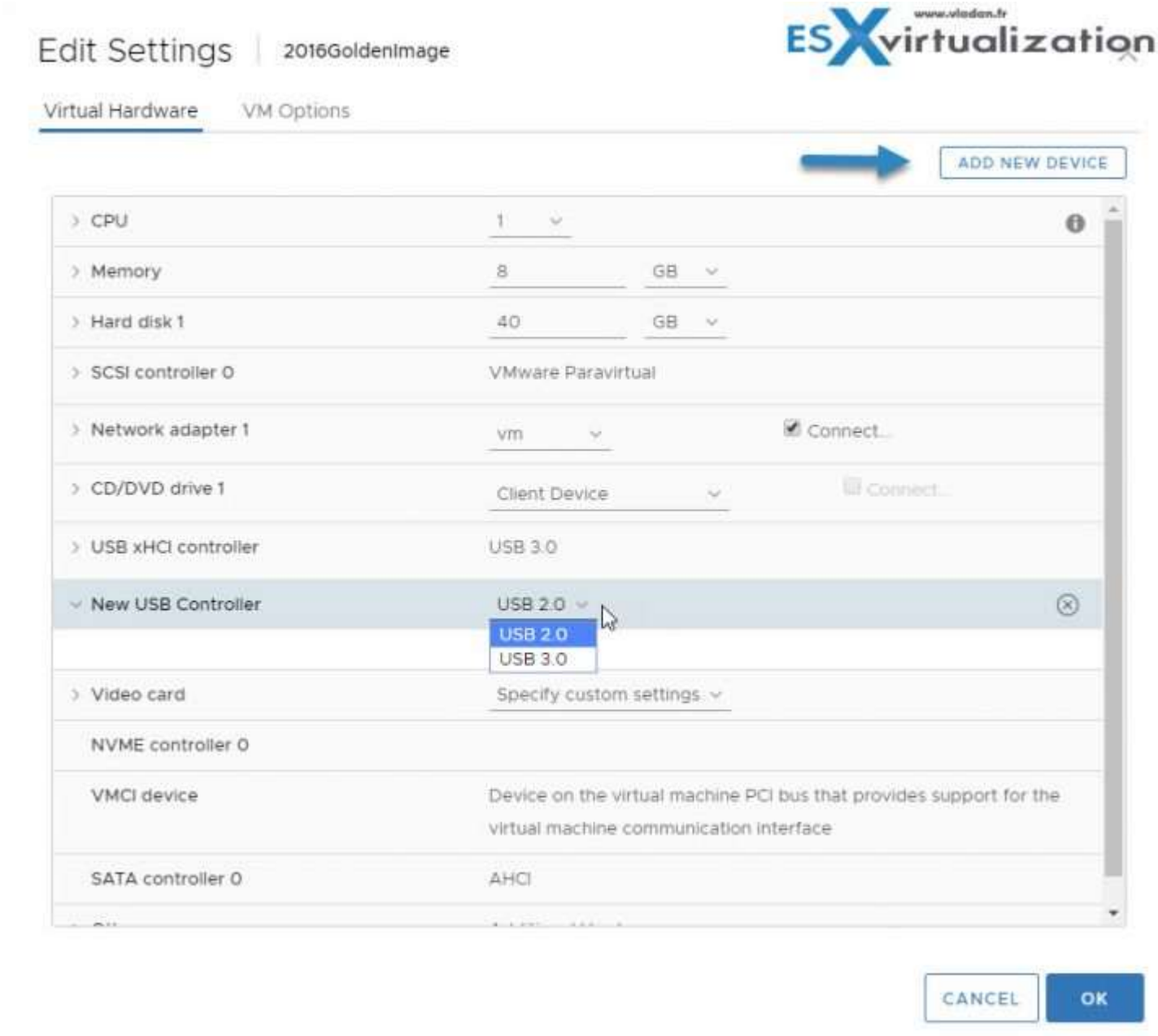
- VMware vCSA 6.5 HA Failover Test – Video

VCP6.5-DCV Objective 10.1 - Create and Manage vSphere Virtual Machines and Templates

Determine how using a shared USB device impacts the environment

You can add multiple USB devices to a virtual machine when the physical devices are connected to an ESXi host. USB passthrough technology supports adding USB devices, such as security dongles and mass storage devices to virtual machines that reside on the host to which the devices are connected.

First you need to add USB controller to the VM. After that you can select the version of the protocol.



When you attach a USB device to a physical host, the device is available only to virtual machines that reside on that host. The device cannot connect to virtual machines that reside on another host in the datacenter.

A USB device is available to only one virtual machine at a time. When a device is connected to a powered-on virtual machine, it is not available to connect to other virtual machines that run on the host. When you remove the active

connection of a USB device from a virtual machine, it becomes available to connect to other virtual machines that run on the host.

CONFIGURE VIRTUAL MACHINES FOR VGPUS, DIRECTPATH I/O AND SR-IOV

If an ESXi host has an NVIDIA GRID GPU graphics device (or other compatible devices), you can configure a virtual machine to use the NVIDIA GRID virtual GPU (vGPU) technology.

It's necessary that VM is compatible with ESXi 6.0 and later.

Select VM > Edit Settings > Virtual Hardware TAB > Shared PCI Device drop down menu > Add > New PCI device > Select Nvidia GRID vGPU passthrough device > Select GPU profile > Click Reserve All memory > OK.

SR-IOV - For low latency network characteristics you can leverage SR-IOV. To use the capabilities of SR-IOV, you must enable the SR-IOV virtual functions on the host and connect a virtual machine to the functions. SR-IOV is a specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear as multiple separate physical devices to the hypervisor or the guest operating system.

Direct Path I/O - allows a guest OS on a VM to directly access physical components on the host such as PCI and PCIe devices. Use cases for this could be high-performance graphics cards or sound cards.

There is a maximum of 6 devices a VM can be connected to.

Note: Snapshots are not supported with PCI vSphere Direct Path I/O devices.

The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary. This adapter type is suitable for virtual machines where latency might cause failure or that require more CPU resources.

Note: When using DirectPath I/O on a virtual machine you CANNOT suspend, vMotion or perform snapshots on that virtual machine.

SR-IOV enabled PCIe devices does require an appropriate BIOS and hardware support, as well as SR-IOV support in the guest operating system driver or hypervisor instance.

SR-IOV is beneficial in workloads with very high packet rates or very low latency requirements. Like DirectPath I/O, SR-IOV is not compatible with certain core virtualization features, such as vMotion. SR-IOV does, however, allow for a single physical device to be shared amongst multiple guests. With DirectPath I/O you can map only one physical function to one virtual machine. SR-IOV lets you share a single physical device, allowing multiple virtual machines to connect directly to the physical function.

CONFIGURE VIRTUAL MACHINES FOR MULTICORE VCPUS

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

Note: You can also enable Hot-Add.

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

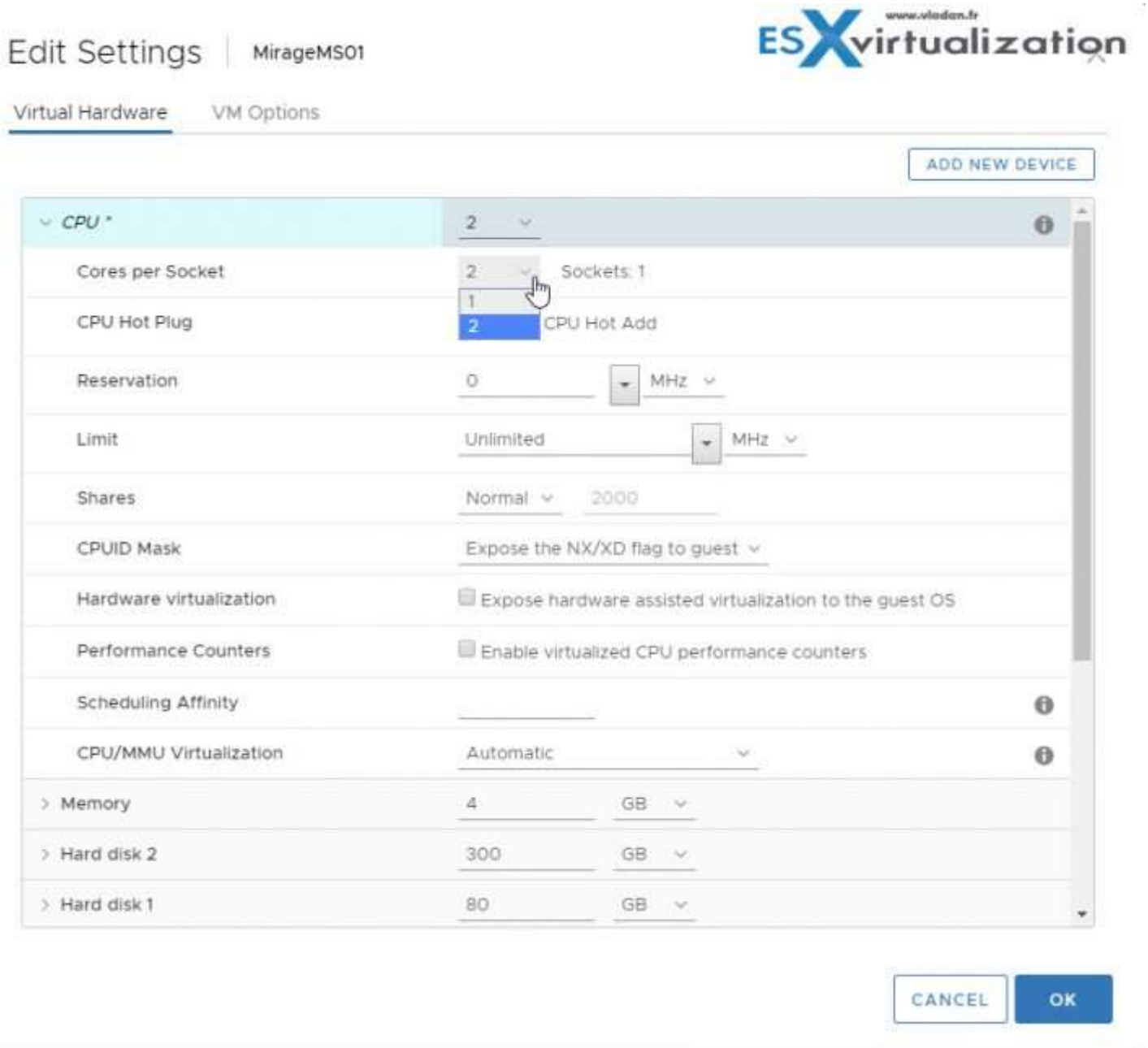
You can configure a virtual machine that runs on an ESXi host 6.0 and later to have up to 128 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical

CPUs means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

C**lick VM > Edit settings > Virtual Hardware tab > expand CPU > select the number of cores from the CPU drop-down menu > Select the number of cores per socket from the Cores Per Socket drop-down menu > Click Save**.

Check the image.



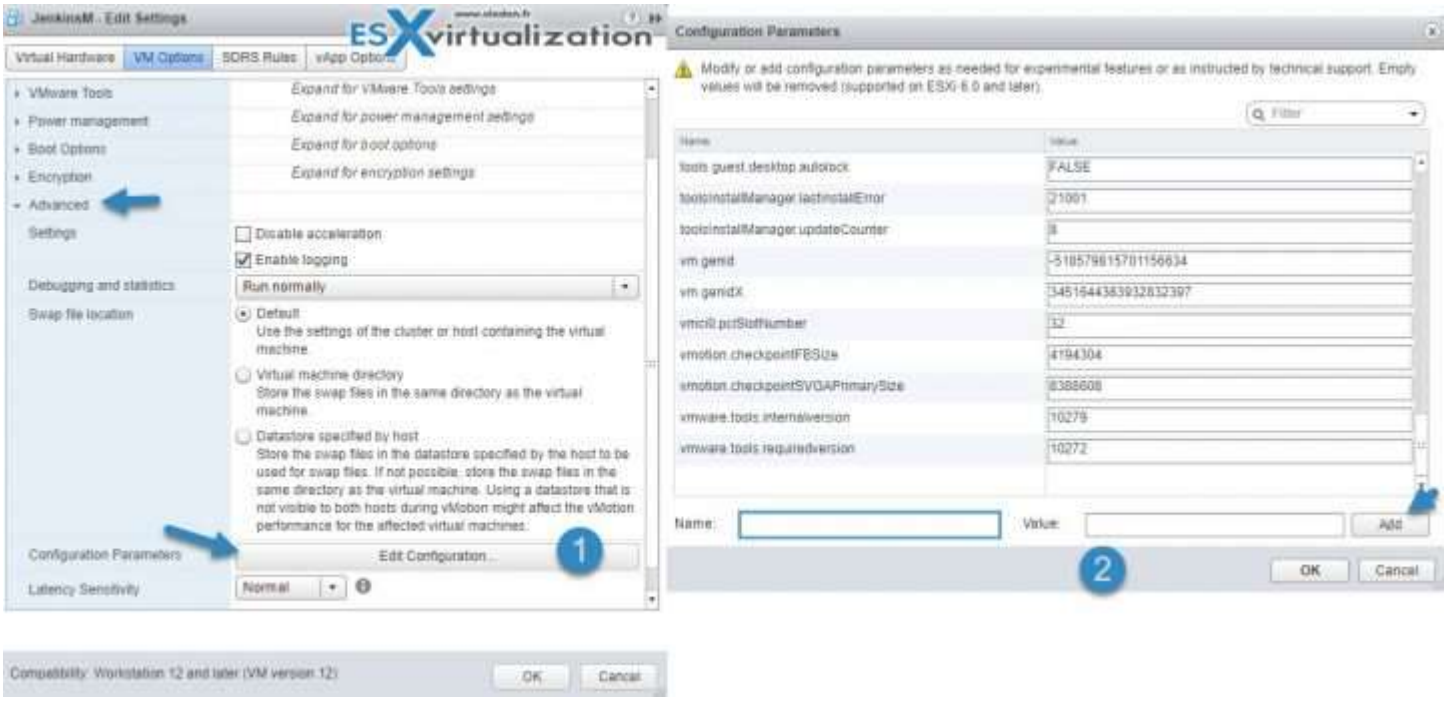
When using *cpuid.coresPerSocket* advanced setting, you should always ensure that you are in compliance with the requirements of your operating system EULA (that is, regarding the number of physical CPUs on which the operating system is actually running).

Also, check [VMware KB 2020993.]

DIFFERENTIATE VIRTUAL MACHINE CONFIGURATION SETTINGS

You can edit VM config by going to its configuration page. Simply **select and right-click a VM > Edit Settings**.

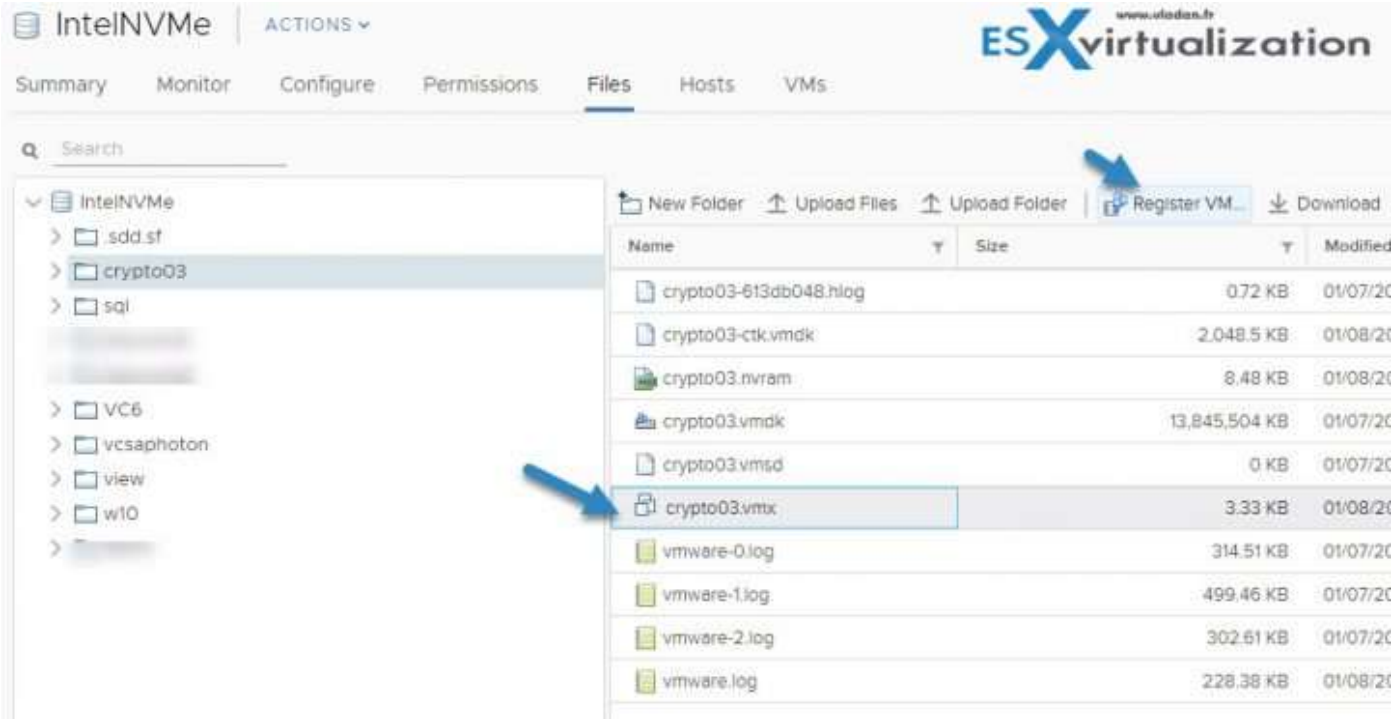
You can edit VM's advanced settings (including adding new advanced options) there.



INTERPRET VIRTUAL MACHINE CONFIGURATION FILES (.VMX) SETTINGS

In order to modify the virtual machine's .vmx file:

- Remove the virtual machine from vCenter Server inventory. Do a right-click the virtual machine and click Remove from Inventory.
- Edit the .vmx file.
- Re-register the virtual machine by browsing the datastore where the VM's files are located.



Before you edit the .vmx file:

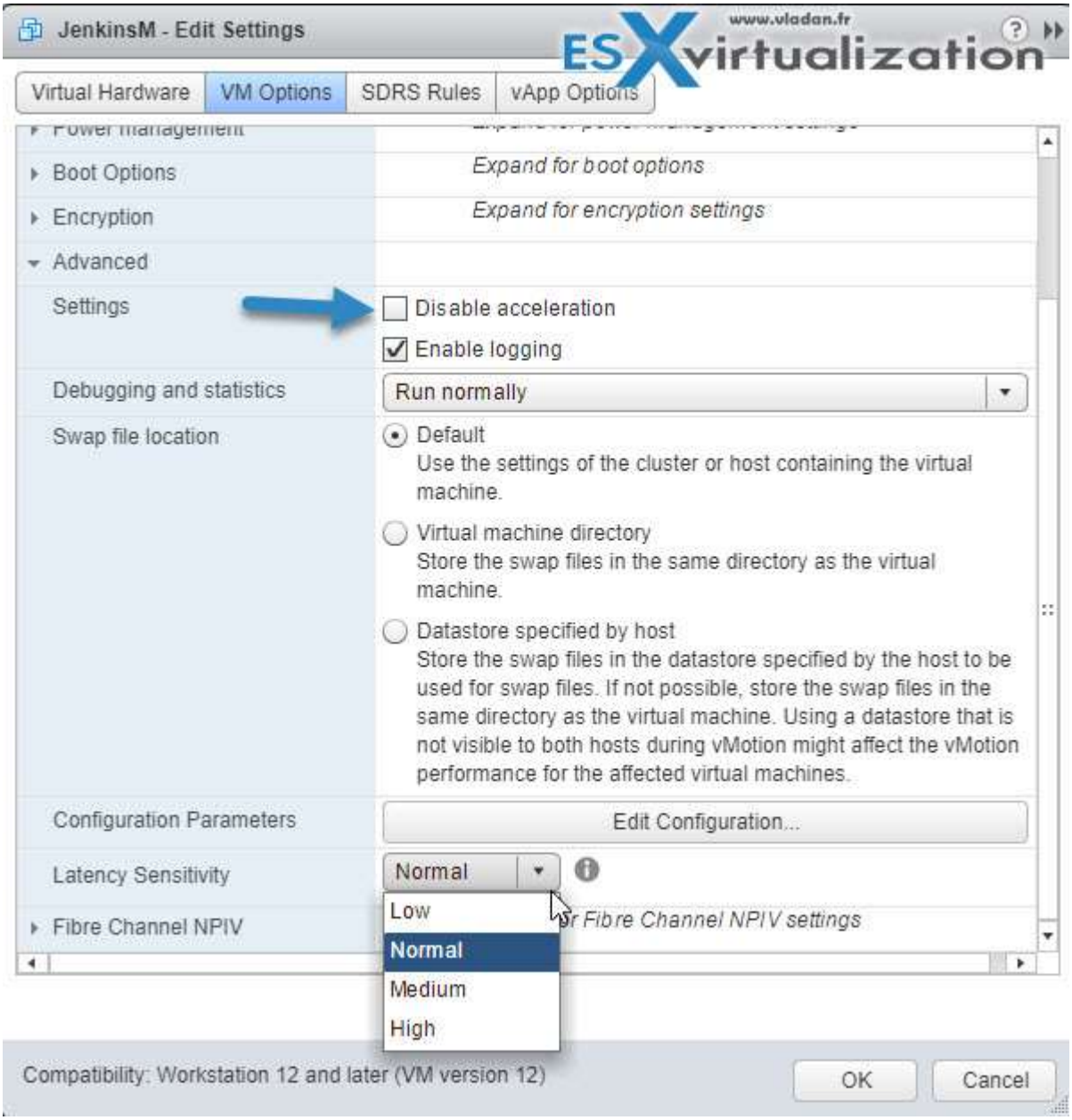
- Always power off the virtual machine.
- Make sure you are logged on as a user with the correct permission level to edit the file.
- Make a backup copy of the .vmx file. If your edits break the virtual machine, you can roll back to the original version of the file

ENABLE/DISABLE ADVANCED VIRTUAL MACHINE SETTINGS

Sometimes you need to enable or disable advanced settings of a VM. It can be in a situation when you need to install an old software which to complete successfully, we have to disable acceleration. More options:

- **Enable Logging** – Collect log files for the VM for debugging or troubleshooting
- **Debugging & Statistics** – Allows for collection/recording for further log analysis.
- **Swap File Location** – You can modify where the swap file resides.
- **Latency Sensitivity** – Configure sensitivity between VM and physical host resource.

And the option we have talked about - Disable Acceleration.



VCP6.5-DCV Objective 10.2 - Create and Manage a Content Library

Publish a content catalog

VCP6.5-DCV Objective 10.2 - Create and Manage a Content Library. This topic isn't very long, so let's get us through.

You can publish the local library so that users from other vCenter Server systems can subscribe to it. When you publish a content library externally, you can configure a password for authentication.

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

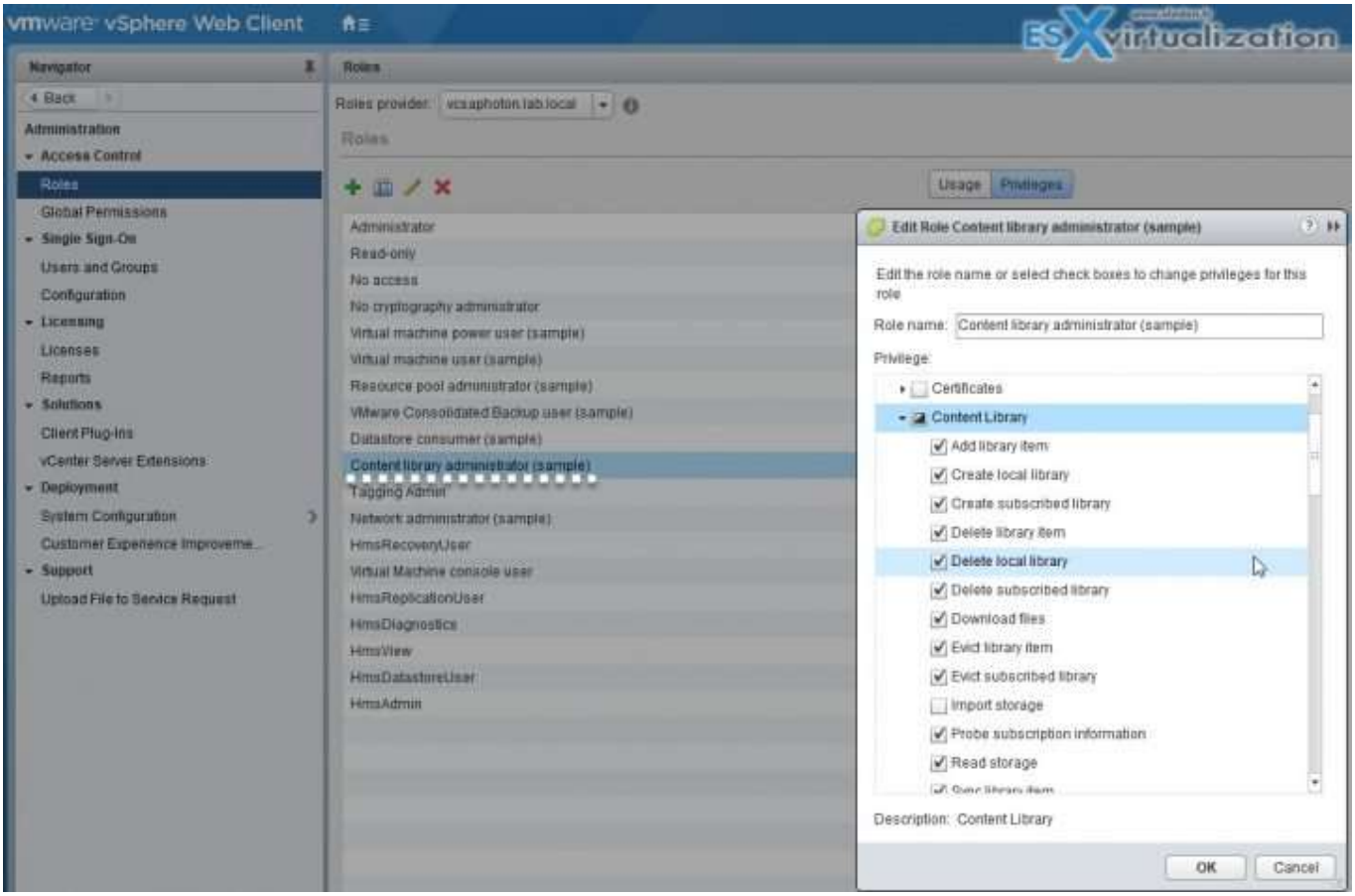
SUBSCRIBE TO A PUBLISHED CATALOG

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

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

DETERMINE WHICH PRIVILEGES ARE REQUIRED TO GLOBALLY MANAGE A CONTENT CATALOG

You'll need to add a new role to manage our content library. You can easily clone the existing 'Content Library Administration (Sample)' role for example. After, you may want to limit further the role privileges.



vSphere objects inherit permissions from a parent object in the hierarchy. Content libraries work in the context of a single vCenter Server instance. However, content libraries are not direct children of a vCenter Server system from an inventory perspective.

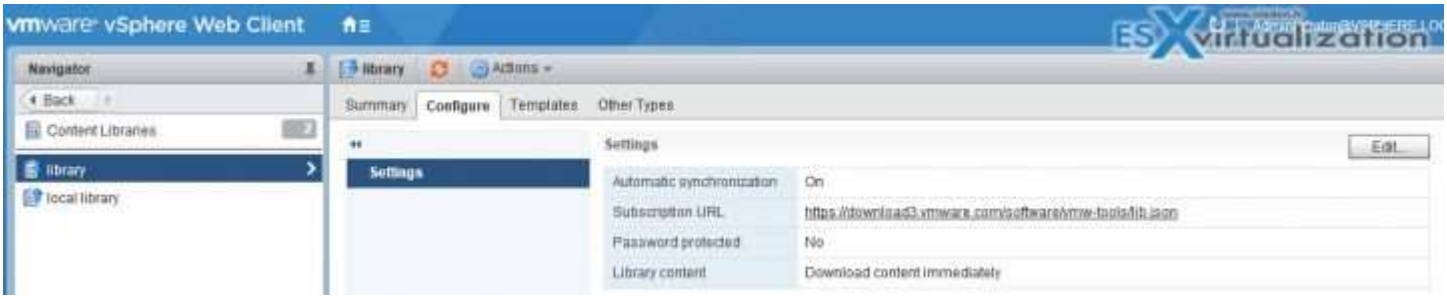
The direct parent for content libraries is the global root. This means that if you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and so on, but does not apply to the content libraries that you see and operate within this vCenter Server instance.

In order to assign a permission on a content library, an Administrator must grant the permission to the user as a **global permission**. Global permissions support assigning privileges across solutions from a global root object.

COMPARE THE FUNCTIONALITY OF AUTOMATIC SYNC AND ON-DEMAND SYNC

You can also have subscribed libraries automatically synchronize with the content of the published library. To enable **automatic synchronization** of the subscribed library, select the option to Enable automatic synchronization with the external library in the subscribed library settings.

Synchronization of a subscribed library that is set with the option to download all the contents of the published library **immediately**, synchronizes both the item metadata and the item contents. During the synchronization, the library items that are new for the subscribed library are fully downloaded to the storage location of the subscribed library.



Take into account that the automatic synchronization requires a lot of storage space because you download full copies of all the items in the published library.

Required privilege: Content library > Sync subscribed library on the library.

vSphere **Web Client** navigator > **vCenter Inventory Lists** > **Content Libraries** > **Right-click a subscribed library** from the list and select **Synchronize**.

On the **Other Types tab**, right-click an item, and select **Synchronize** Item.

Synchronization of a subscribed library that is set with the option to download contents only when needed synchronizes only the metadata for the library items from the published library, and does not download the contents of the items. This saves storage space. If you need to use a library item you need to synchronize that item.

After you are done using the item, you can delete the item contents to free space on the storage.

For subscribed libraries that are set with the option to download contents only when needed, synchronizing the subscribed library downloads only the metadata of all the items in the source published library while synchronizing a library item downloads the full content of that item to your storage.

Configure Content Library to work across sites

Content library can be shared across multiple vCenter server systems.

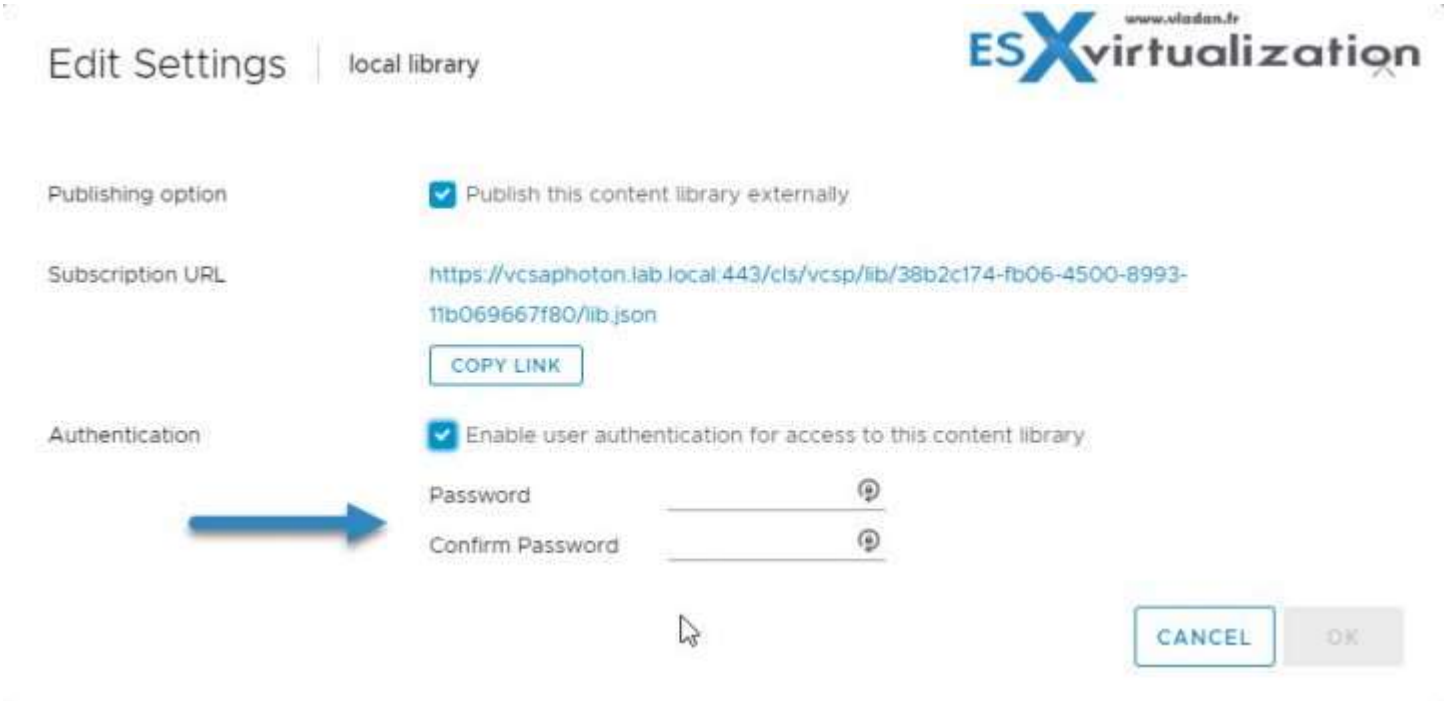
A VM template, vApp template or another type file is considered as a **library item**. Each item can contain several files (ex. OVF has several files .ovf, .vmdk, .mf, …) however vSphere client shows only the .ovf through the content library.

You can publish a local library from your vCenter Server instance to share its contents across multiple vCenter Server systems. From the Edit Setting dialog box, you can obtain the URL of your library and send it to other users to subscribe.

If the library is already published, you can change its password for authentication. Users who are subscribed to your library must update the password to keep access to the published library.

Configure Content Library authentication

You have a possibility to restrict access to a content library. See figure 1 for details, then check the box "Enable user authentication for access to this content library". The window expands, allowing you to set up a password.



SET/CONFIGURE CONTENT LIBRARY ROLES

Same as above.

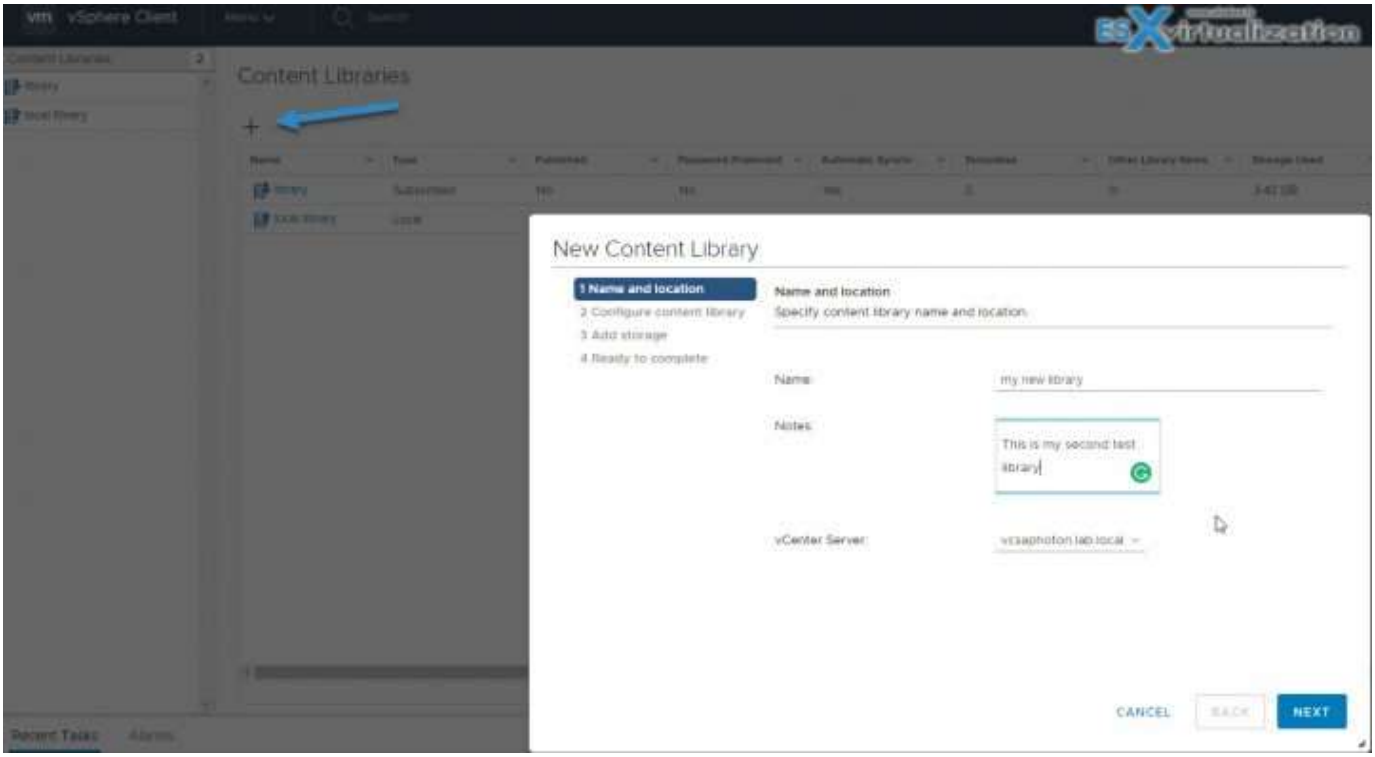
Content Library Administrator role is a predefined role that gives a user privileges to monitor and manage a library and its contents.

A user who has this role can:

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

ADD/REMOVE CONTENT LIBRARIES

vSphere web client > Home > Content Libraries > Click PLUS sign > follow the assistant.



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

- Local content library
- Subscribed content library
- Select datastore

Then click finish to complete the assistant. Note that the content library now works in the HTML5 web client as well. The HTML 5 web client, however does not provide access to all vSphere 6.5 features just yet. For example all stuff concerning vSAN isn't implemented just yet, but the work with this client is much smoother and faster compared to Adobe Flash. But as for the exam, the vSphere 6.5 does not provide features parity through both clients.

VCP6.5-DCV Objective 10.3 – This objective is no longer covered in the exam content

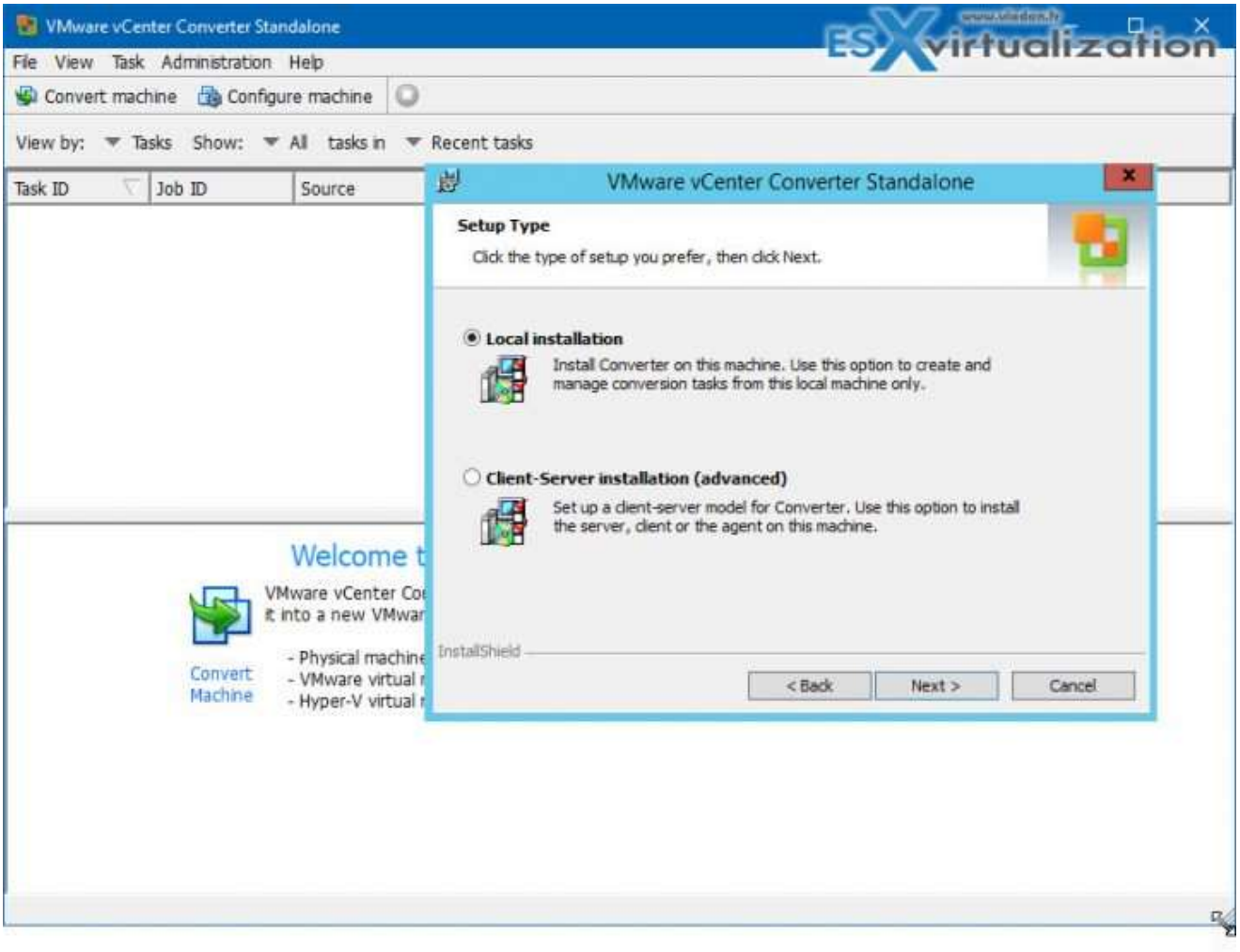
...

VCP6.5-DCV Objective 10.4 – Consolidate Physical Workloads using VMware vCenter Converter

Install vCenter Converter standalone instance

VMware converter can be installed on Linux or Windows. You can choose from two installation type:

- **Local Installation** - installs converter on this local computer. You'll be managing conversion tasks from this management machine.
- **Client-Server Installation** - it installs as client-server environment. You'll have 3 components to install on different systems (server, client and agent).



SYSTEM REQUIREMENTS:

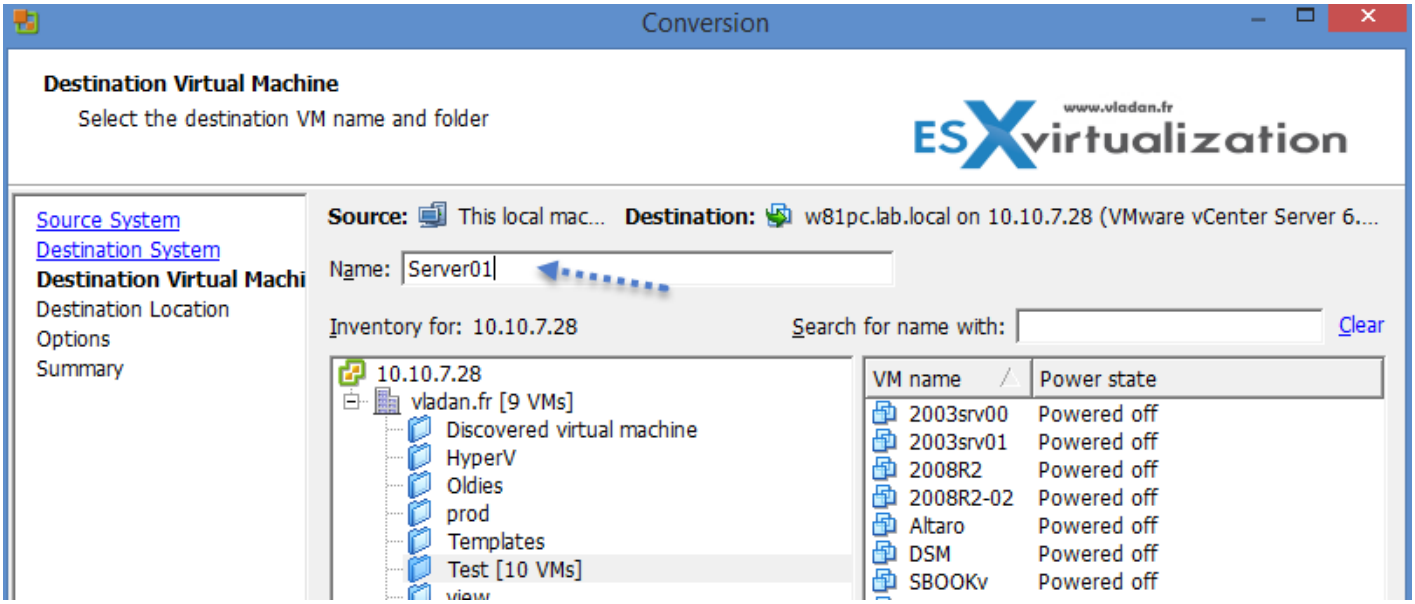
- **Windows** – Windows XP Professional (32-bit and 64-bit) SP3 and higher, 2003 srv (x32 and x64) and up to 2012R2
- **Linux** – RHEL 3.x – 6.x, SUSE 9.x – 11.x, Ubuntu 10.04 LTS – 13.04 …. both x32 and 64-bit versions.

CONVERT PHYSICAL WORKLOADS USING VCENTER CONVERTER

The steps to convert a physical system can be summarized as follows (but this is only one of the ways that's possible; other ways client-server are possible as well):

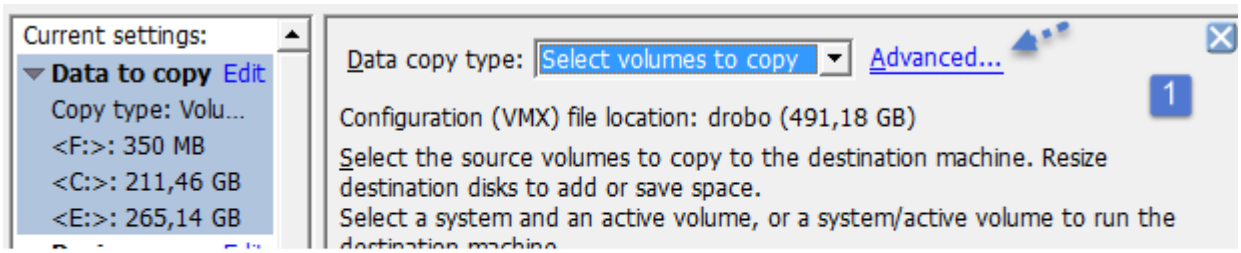
1. Install VMware converter on the Window/Linux server and click **Convert Machine > Powered On machine > This local machine**

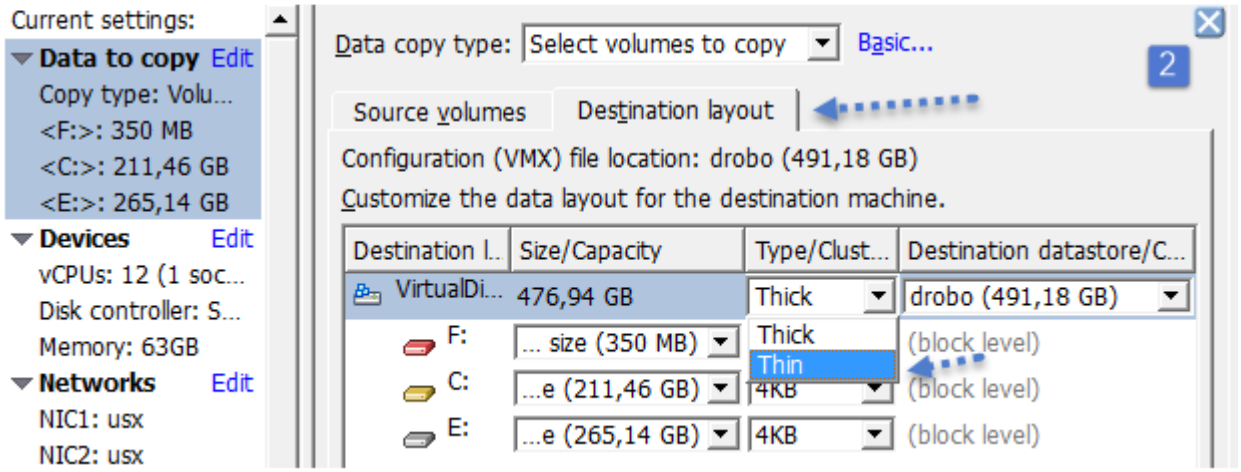
2. Select **Destination type** > choose **VMware infrastructure VM** > enter **vCenter credentials** > Put some meaningful **name** for your VM



3. Choose **Cluster or host** > **Datastore** > **Virtual Machine Version >** Click **Next**

4. Click the **Advanced** Link > chose the **disk type** of your choice (thick or thin). If you do not copy all disks and maintain layout the volume-based cloning is used (at the block level).





You can also modify other resources which the VM does not need, like delete some unwanted NICs, Windows services, or adjust the number of vCPUs and Memory.

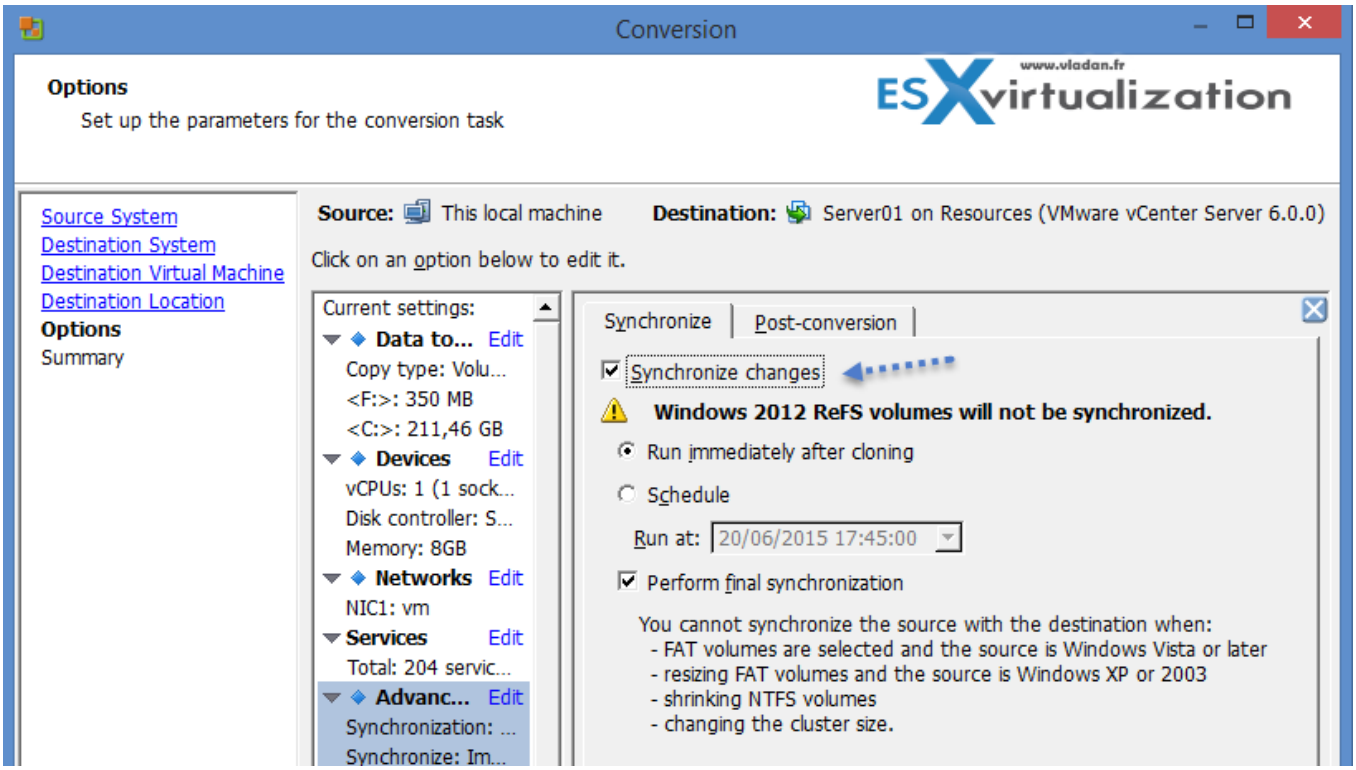
By default, Converter Standalone optimizes the disk partitions alignment. Optimizing the partition alignment improves the performance of the destination virtual machine. (It basically says that the process will align the VM to the LUN). So leave the box checked…

MODIFY SERVER RESOURCES DURING CONVERSION

It's possible to adjust the converter server resources during conversion. For example:

- **Number of concurrent tasks** – It's possible to modify the number of concurrent tasks by going to **Administration > Maximum concurrent tasks**. 1 to 12 concurrent tasks, but the 12 is by default and if your Converter server lacks resources you might want to lower down a bit of number of tasks taking place at the same time.
- **Number of data connections per task** – If you are converting systems with multiple disks and volumes, it's possible to decrease the conversion time by cloning multiple disks and volumes simultaneously. Each data transfer uses a separate TCP connection. Check **Administration > Data connections per Task**.

It's possible to synchronize changes after the first conversion has finished. It's because the source machine continues to generate data. So the delta changes can be synced and the source VM powered down…



INTERPRET AND CORRECT ERRORS DURING CONVERSION

You might encounter errors during conversion. Make sure that you have the necessary firewall ports open.

There are quite a few useful VMware KB articles:

- Troubleshooting when vCenter Converter fails to complete a conversion of a physical or virtual machine.
- Testing port connectivity with Telnet (1003487)
- Best practices for using and troubleshooting VMware Converter (1004588)
- Troubleshooting a virtual machine converted with VMware Converter that fails to boot with the error: STOP 0x0000007B INACCESSIBLE_BOOT_DEVICE (1006295)
- Required VMware vCenter Converter 4.x/5.x ports (1010056)
- Collecting diagnostic information for VMware Converter (1010633)
- TCP and UDP Ports required to access VMware vCenter Server, VMware ESXi and ESX hosts, and other network components (1012382)
- VMware vCenter Converter is unable to see the disks when converting Windows operating systems (1016992)

- vCenter Standalone Converter errors when an ESXi 5.x host is selected as a destination: The access to the host resource settings is restricted. Use the management server as a destination (2012310)

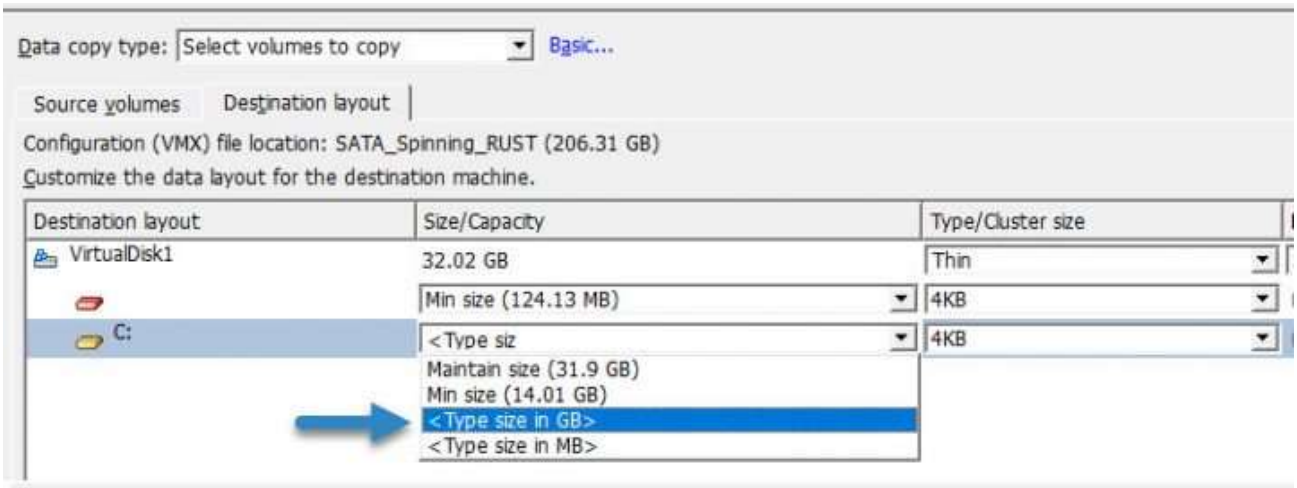
Deploy a physical host as a virtual machine using vCenter Converter. Collect diagnostic information during conversion operation

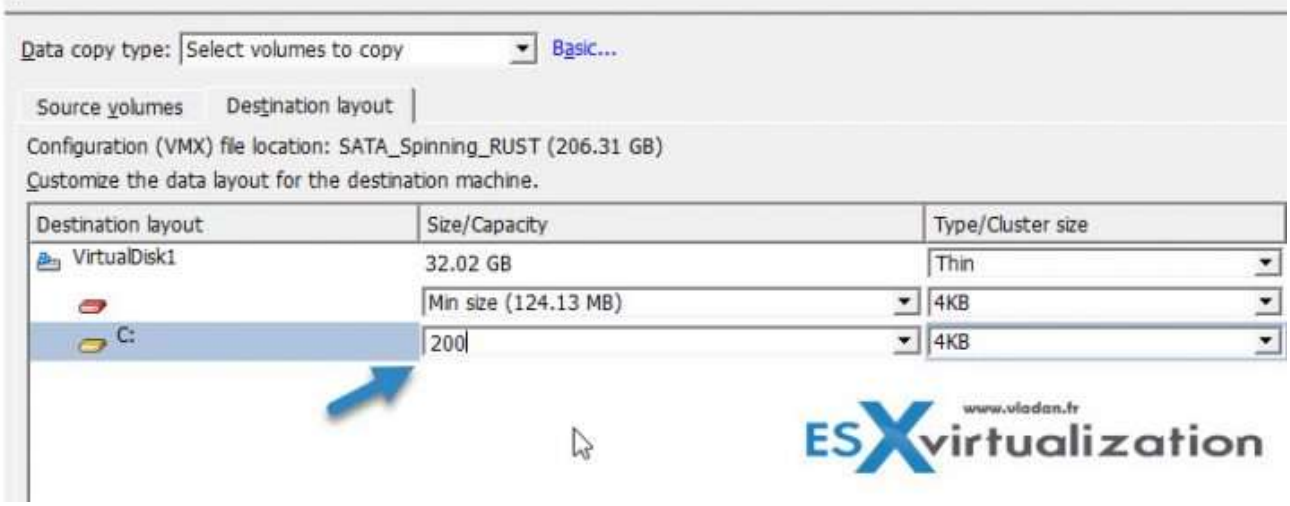
Well, this basically asks us to do a conversion of a physical machine into a VM. I believe the above and below topics give you quite enough information. Keep in mind to uninstall hardware oriented software (monitoring agents etc.) before starting the conversion process and do the usual post-conversion tasks such as finding and deleting ghosted devices etc.

Resize partitions during the conversion process

You can resize partitions during the conversion process. For this, you must choose **Select volumes to copy** and go to the **Advanced view**.

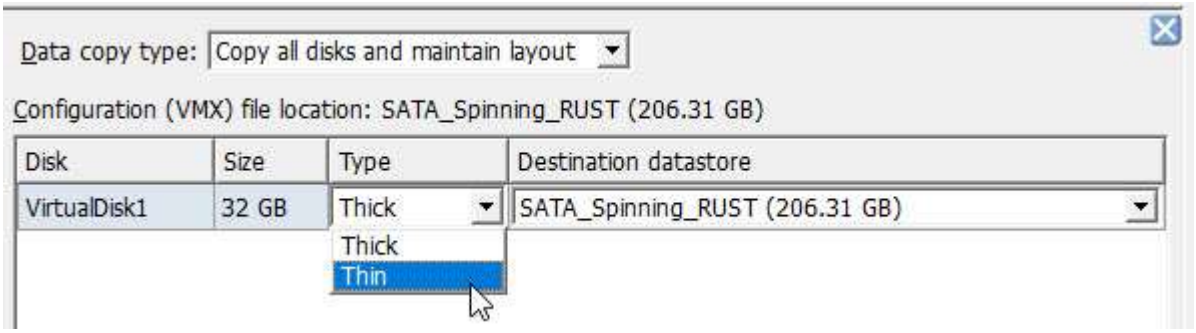
Then you have an option to type the new size in order to resize the disk size.





Determine which virtual disk format to use

You have Thick or Thin as an option, when it comes for a choice for the destination VM.



DOCUMENTATION SETS:

vSphere 6.5 documentation library (PDF):

- Configuration Maximums
- vSphere Installation and Setup
- vSphere Upgrade
- vCenter Server and Host Management
- vCenter Server Appliance Configuration
- Platform Services Controller Administration
- vSphere Virtual Machine Administration
- vSphere Host Profiles
- vSphere Networking
- vSphere Storage
- vSphere Security
- vSphere Resource Management
- vSphere Availability
- vSphere Monitoring and Performance
- vSphere Single Host Management - VMware Host Client
- vSphere Troubleshooting
- Setup for Failover Clustering and Microsoft Cluster Service

Wrap Up: This guide is an unofficial study guide to help you out when studying for your VCP exam. I highly recommend downloading the full documentation set in PDF and not to rely only on our guide. However, our guide is free.

Good luck with the exam -😊.
Vladan
https://www.vladan.fr