VMware vSphere

Partie 9

Université Mohammed V de Rabat / Faculté des Sciences de Rabat

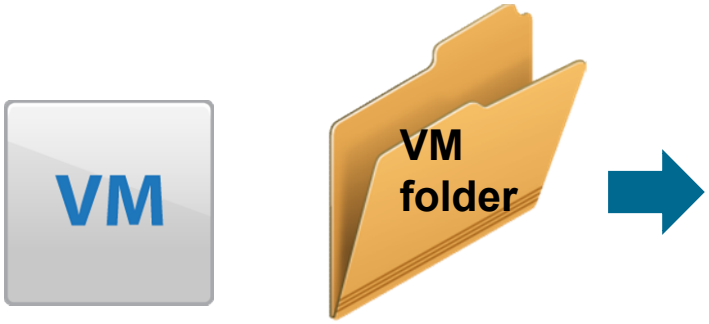
Réalisé par : Pr Hassan ECHOUKAIRI

Lesson 9:
Virtual Machine Concepts

What files does the virtual machine include?

About Virtual Machine Files

- A virtual machine includes a set of related files.
- **Except for the log** files, the name of **each file starts** with the virtual machine's name **VM_name**



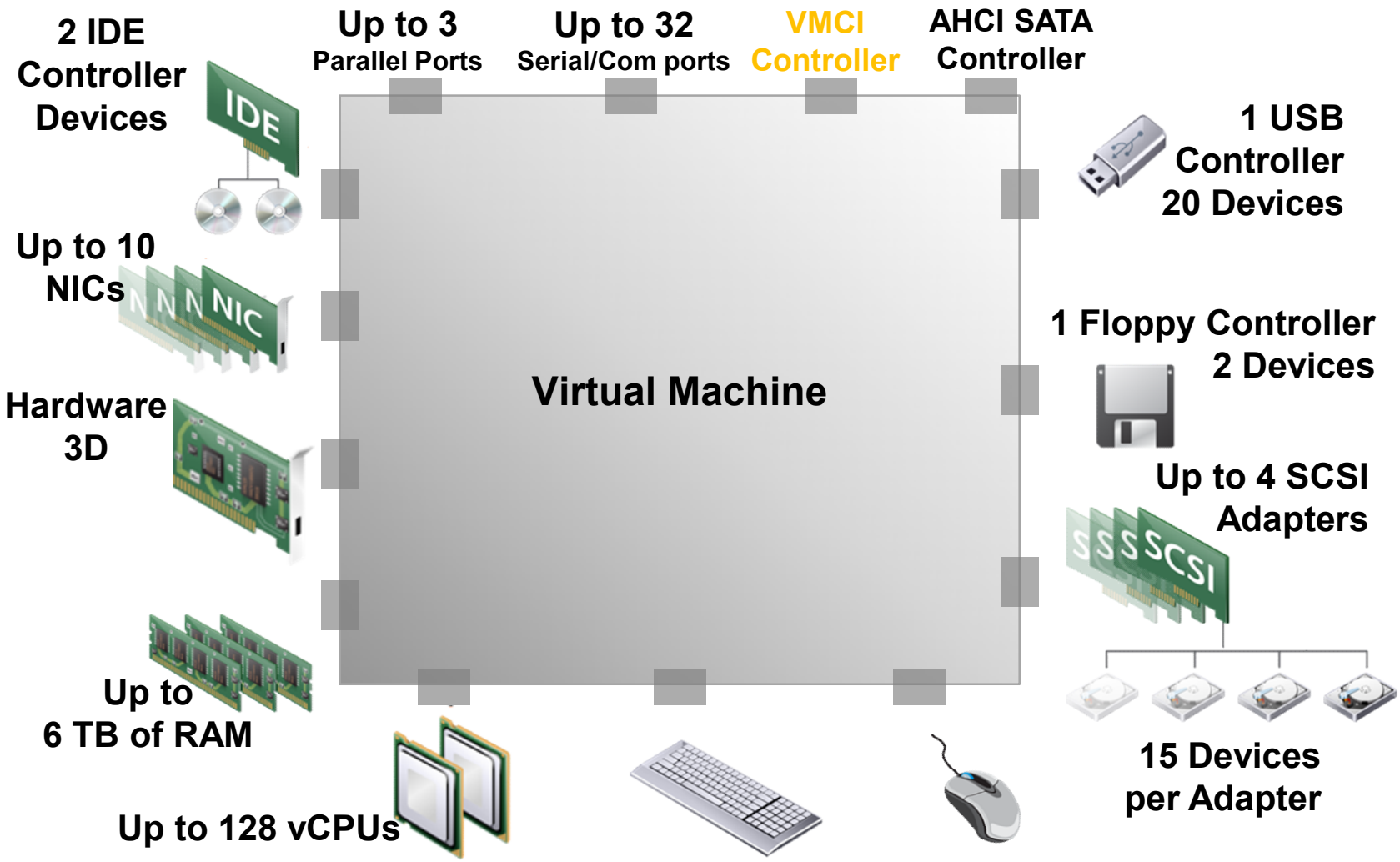
Configuration file	*VM_name*.vmx
Swap files	*VM_name*.vswp
	vmx-*VM_name*.vswp
BIOS file	*VM_name*.nvram
Log files	vmware.log
Template file	*VM_name*.vmtx
Raw device map file	*VM_name*-rdm.vmd*k*
Disk descriptor file	*VM_name*.vmdk
Disk data file	*VM_name*-flat.vmdk
Suspend state file	*VM_name*.vmss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

About Virtual Machine Files

1) A **configuration file** (. vmx): Each VMX file includes a virtual **machine's memory**, **hard disk**, and **processor limit** settings.
2) One or more virtual disk files. The first virtual disk has files **VM_name. vmdk** and **VM_name-flat . vmdk**
3) A file containing the virtual machine's BIOS settings (. nvram).
4) A virtual machine's current log file (. log) and a set of files used to archive old log entries (- # . log).
5) Swap files (. vswp) used to reclaim (récupérer) memory during periods of **contention** (conflits).
6) A snapshot description file (. vmsd). This file is empty if the virtual machine has no snapshots

- If the virtual machine is converted to a template, a v**irtual machine template** configuration file (. vmtx) replaces the virtual machine configuration file (. vmx).
- A virtual machine template is a **master copy of the virtual machine**

About Virtual Machine Virtual Hardware



About Virtual Machine Virtual Hardware

- **Virtual Machine Communication Interface (VMCI**) provides a high-speed communication channel between a **virtual machine** and the **hypervisor**.
- The SATA controller provides **access to virtual disks** and DVD/CD-ROM devices.
- The SATA virtual controller appears to a virtual machine as an **AHCI SATA Controller**.
- The **VMCI** is an infrastructure that provides fast and efficient communication between a **virtual machine and the host operating system**
- **Without VMCI**, virtual machines communicate with the host using the **network layer**. Using the network layer **adds overhead** to the communication
- **With VMCI**, communication **overhead is minimal** and tasks that require that communication can be optimized

Virtual Hardware Versions

- Each release of a VMware product has a corresponding virtual machine hardware version included
- The virtual hardware version determines the operating system functions that a virtual machine supports.

Compatibility	Hardware Version
ESXi 6.5 and later	12
ESXi 6 and later	11
ESXi 5.5 and later	10
ESXi 5.1 and later	9
ESXi/ESX 5.0 and later	8

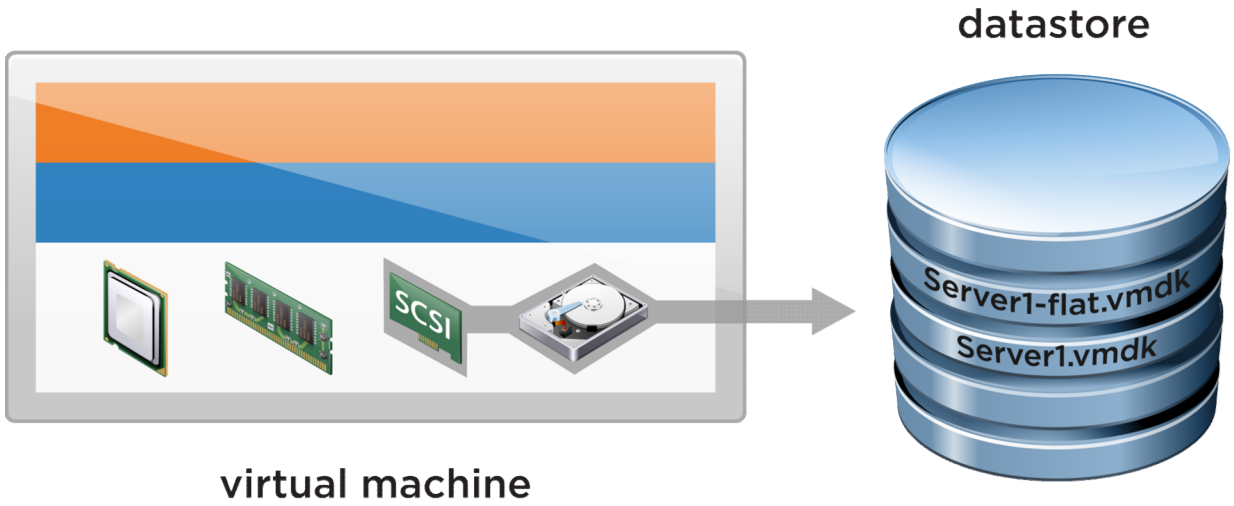
About Virtual Hardware Version 12

Features	Benefits
Increased RAM capacity	Hardware version 12 virtual machines support up to 6 TB of RAM.
NVMe in Guest (vNVMe)	Provides high performance guest block I/O and up to a 50% reduction in software overhead. vNVMe also supports back-end vSAN and vSphere Virtual Volumes storage object-backed disk support.
RDMA in Guest (vRDMA)	vRDMA supports Remote Direct Memory Access providing OS bypass, zero-copy, low latency, and high bandwidth with less power usage and faster data access.

- (vRDMA) also helps accelerate the VMkernel network performance by allowing multiple guests simultaneous access to virtual devices providing low latency and high bandwidth

About Virtual Disks

- A virtual machine usually has at least (au moins) one virtual disk.



Sample virtual disk definition:

Virtual disk size:	8 GB
Datastore:	MyVMFS
Virtual disk node:	0:0
Virtual storage adapter:	LSI Logic SAS
Virtual disk files:	`Server1.vmdk` and `Server1-flat.vmdk`
Default disk mode:	Snapshots allowed
Optional disk mode:	Independent: Persistent or nonpersistent
Disk provisioning policy:	Thick provision lazy zeroed, thick provision eager zeroed, or thin provision

- **For example**:

  If the virtual machine named Test01 has **two virtual disks**, this virtual machine has the:

  Test01.vmdk and Test01-flat.vmdk,
  Test01_1.vmdk, and Test01_1-flat.vmdk files

- **Persistent** : Changes are immediately and permanently written to the disk.

- **Non Persistent** : Changes to this disk are discarded (écarté) when you **power off** or **restore a snapshot**

About Thick-Provisioned Virtual Disks

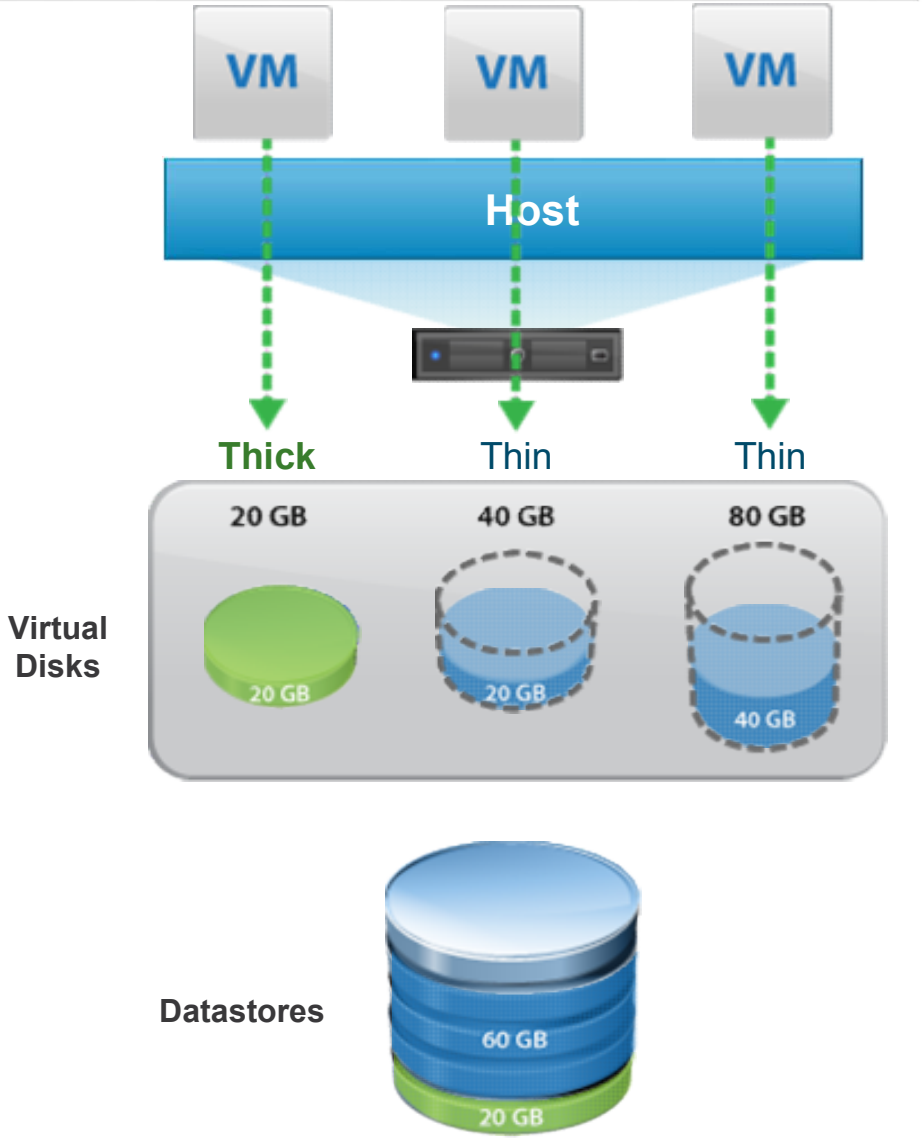
Thick provisioning uses all the defined disk space at the creation of the virtual disk:

- Virtual machine disks consume all the capacity, as defined at creation, regardless of (qq soit) the amount of data in the guest operating system file system.

Eager-zeroed or lazy-zeroed:

- Every block in an **eager-zeroed** thick-provisioned disk is prefilled (rempli) with a zero.
- Every block in a **lazy-zeroed** thick-provisioned disk is filled (remplie) with a zero **when data is written to the block**

(lorsque les données sont écrites dans le bloc)



About Thick-Provisioned Virtual Disks

❑ Thin Provision:

A thin-provisioned disk uses only as much datastore space as the disk initially needs.

If the thin disk needs more space later, it can expand to the maximum capacity allocated to it.

❑ **Thick Provision Eager Zeroed** (mise à zéro rapide)

Space required for the virtual disk is **allocated during creation**.

Data remaining on the physical device is **zeroed out (**mis à zero) **when the disk is created**

❑ **Thick Provision Lazy Zeroed** (mise à zéro lente)

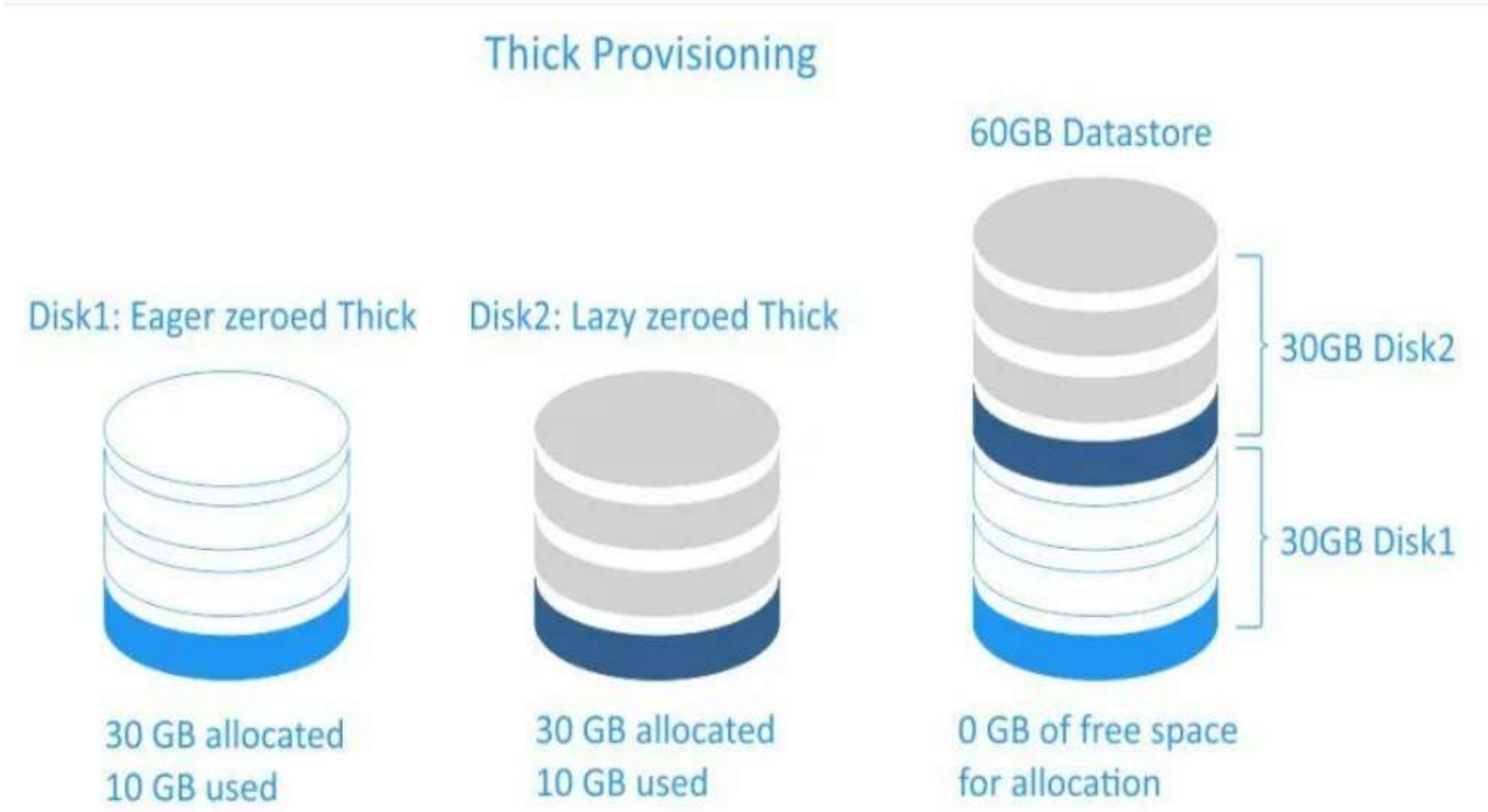
Space required for the virtual disk is **allocated during creation**.

Data remaining on the physical device **is not erased during creation**, but is **zeroed out on demand at a later time** on first write from the virtual machine. (mais les zéro sont écris au moment où la VM a besoin de l'espace disque)

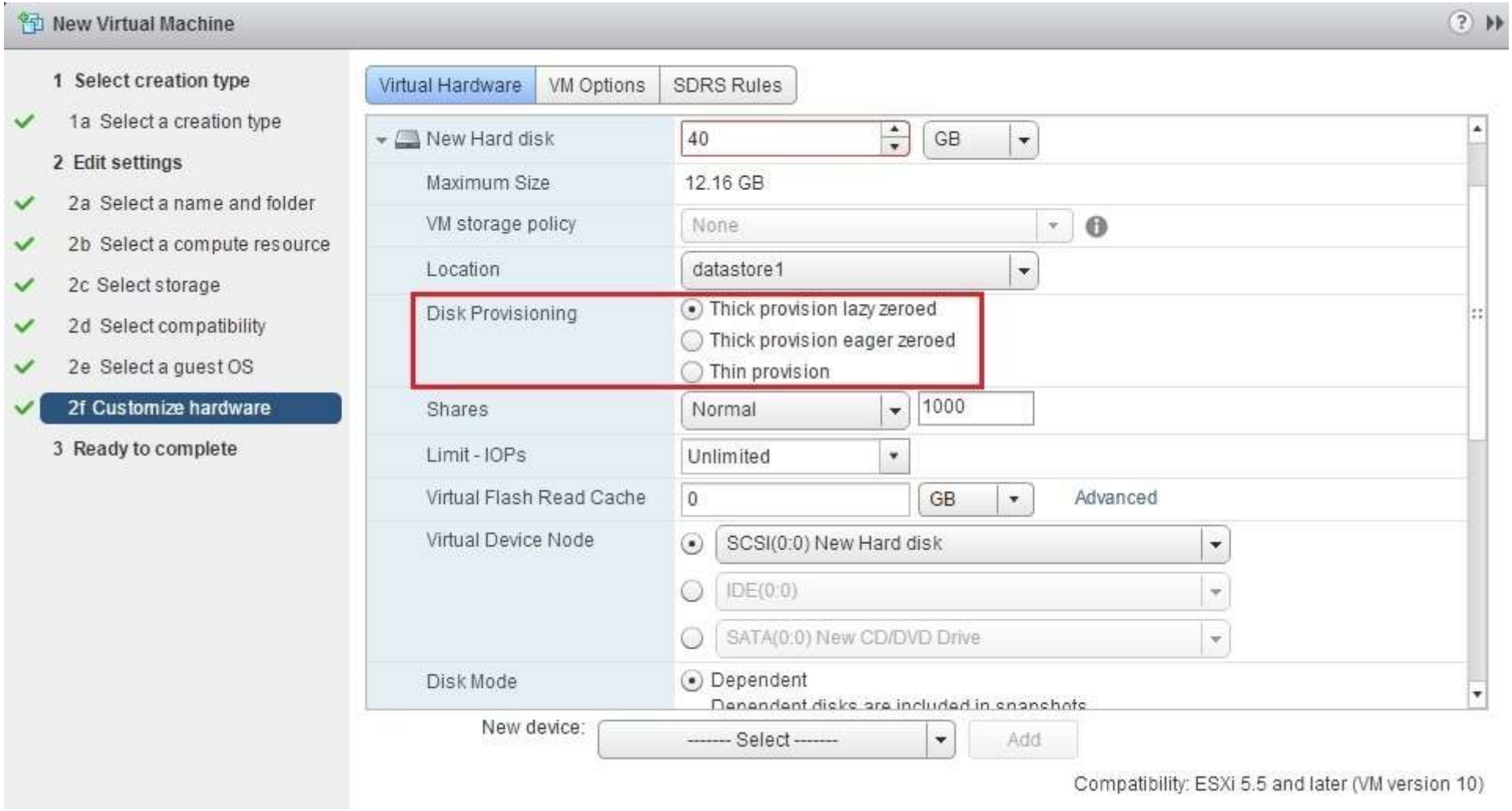
This type is the default disk type

Thin Provisioning : Example

Thick Provisioning : Example

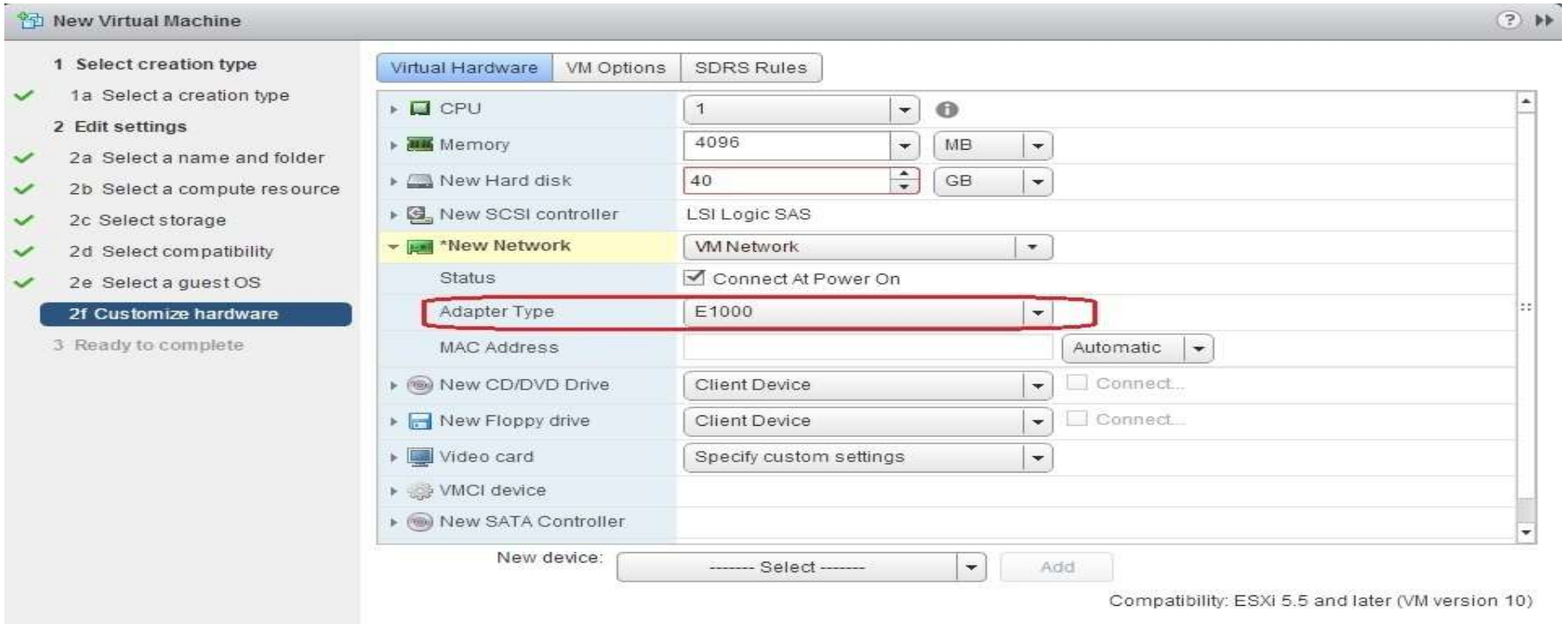


About Disk Provisioned Virtual Disks



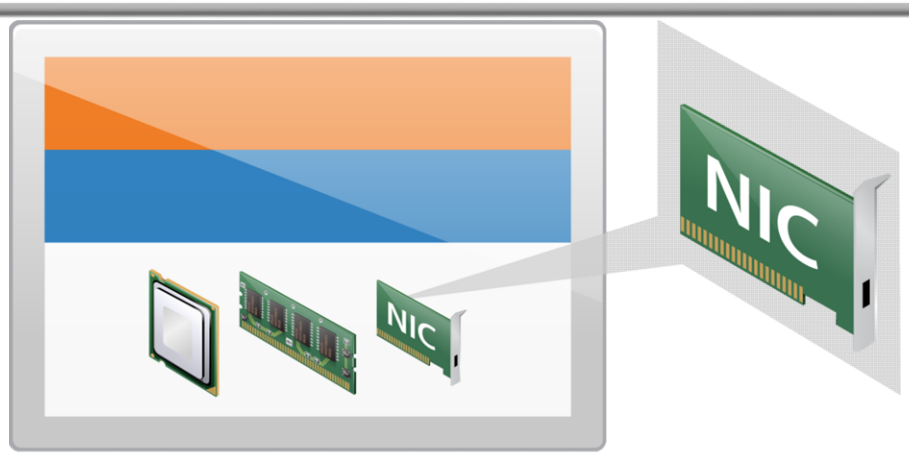
About Virtual Network Adapters (1)

- A virtual network enables communication between virtual machines and physical machines
- When you configure networking for a virtual machine, you select or change the following items:
  - The network adapter type
  - The network connection
  - Whether to connect to the network when the virtual machine powers on



About Virtual Network Adapters (1)

- When you configure a virtual machine, **you can add network adapters (NICs) and specify the adapter type**. Whenever possible, select VMXNET3.



- Supported network adapter types:

- **Flexible**: Can function as either a **Vlanc**e or **VMXNET** adapter.
- **E1000-E1000E**: High-performance adapter available for **only some guest operating systems.**
- **VMXNET, VMXNET2, and VMXNET3** are VMware drivers that are available only with VMware Tools.

About Virtual Network Adapters (1)

- **flexible** – a virtual NIC identifies itself as a **Vlance adapter**, an **emulated form of the AMD 79C970 PCnet32 LANCE 10 Mbps NIC** with drivers available in most **32-bit guest operating system**.

If VMware Tools is installed, this virtual NIC functions as the higher-performance vmxnet adapter, a virtual network adapter optimized for performance in a virtual machine

- **e1000** – an emulated version of the **Intel 82545EM Gigabit Ethernet NIC**.

The driver for this NIC is found in many modern guest operating sytems, including Windows XP and Linux version 2.4.19 and later.
The default adapter type for virtual machines running **64-bit guest operating systems**

- **e1000e** – an emulated version of the **Intel 82574L Gigabit Ethernet NIC**.

This adapter type can be chosen on Windows 8 guest operating systems and newer

- **vmxnet2 (Enhanced vmxnet)** – based on the vmxnet adapter but offers **some high-performance features** such as **jumbo frames** and **hardware offload support**

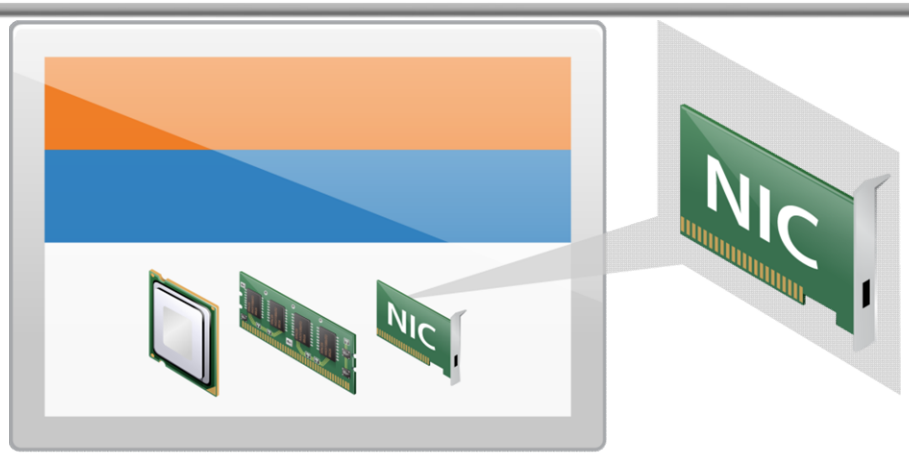
- **vmxnet3** – the latest version of a **paravirtualized** driver designed for performance and offers such high-performance features such as jumbo frames, hardware offloads, support for multiqueue, IPv6 offloads, etc

About Virtual Network Adapters (2) !!!!!

Supported network adapter types:

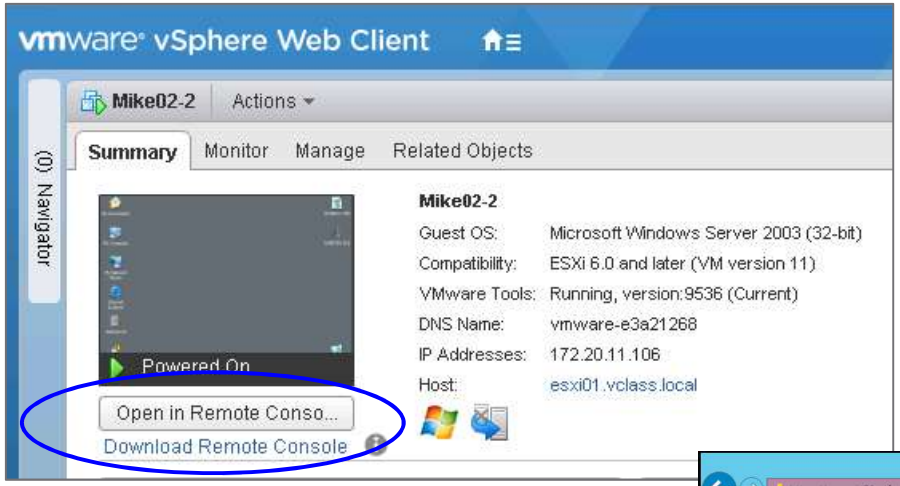
- **SR-IOV passthrough**: The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary:
  - Limited guest operating system support
- VMware vSphere® DirectPath I/O™: vSphere DirectPath I/O allows virtual machine access to physical PCI network functions on platforms with an I/O memory management unit.
- vRDMA: Virtual RDMA is a paravirtualized device that provides improved virtual device performance. It provides an RDMA-like interface for vSphere guests.

RDMA has been exploited for accelerating ESXi hypervisor services like vSphere vMotion

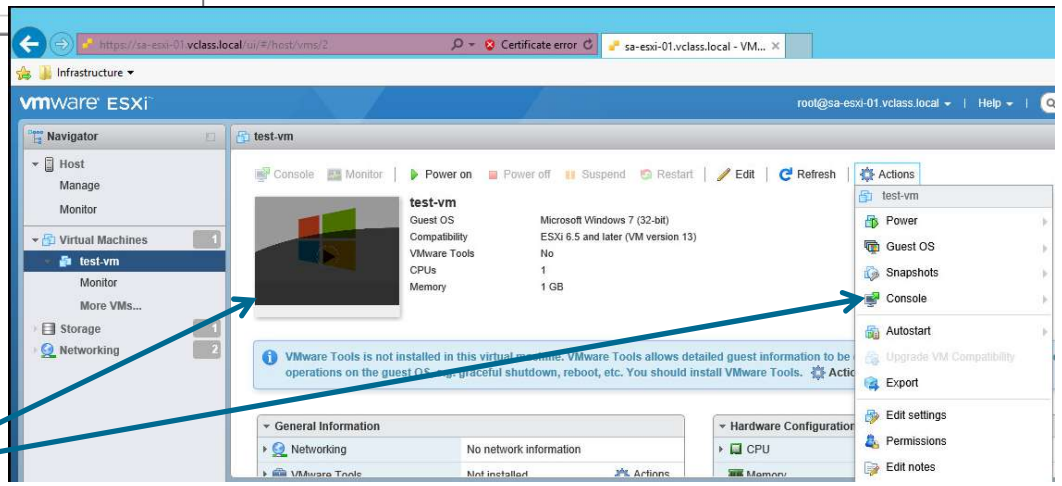


About the Virtual Machine Console

The virtual machine console provides the mouse, keyboard, and screen features to control the virtual machine.



vSphere Web Client



vSphere Client

About the Virtual Machine Console

- You use the virtual machine console to **access the BIOS of the virtual machine**, **install an operating system** on a virtual machine, **power the virtual machine on and off, and reset the virtual machine**

- The virtual machine console is normally **not used to connect** to the virtual machine for daily tasks (tâches quotidiennes)

- Remote Desktop Connection, Virtual Network Connection, or other options are normally used to connect to the virtual desktop

- **The virtual machine console is used for tasks such as power cycling (calcul de puissance), configuring hardware, and troubleshooting network issue (dépannage des problèmes de réseau)**

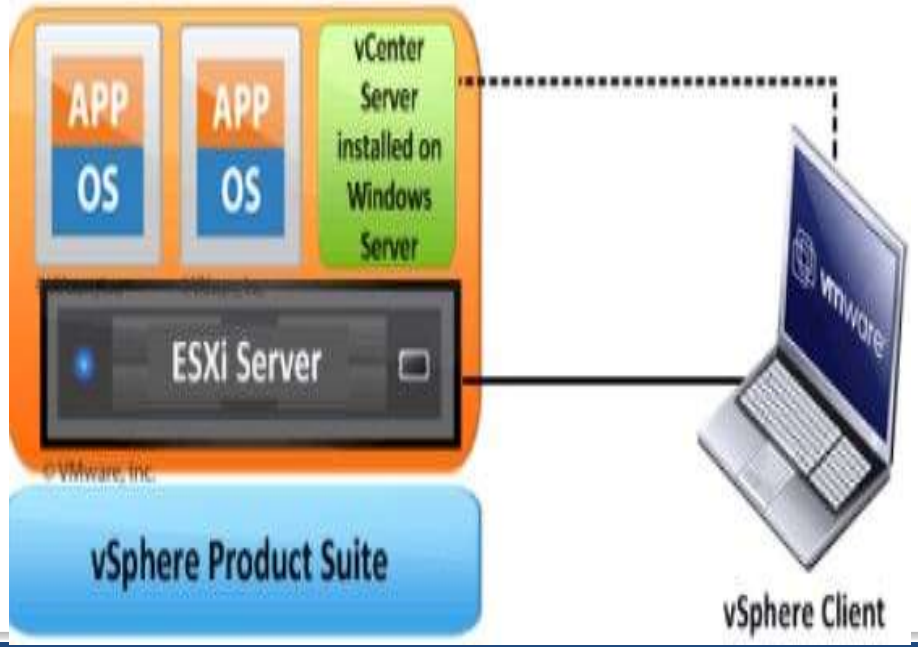
What’s vSphere ?

What's vSphere ?

- VMware vSphere is a **server virtualization platform** from the publisher VMware that transforms DataCenters into simplified cloud computing infrastructures and **enables IT organizations to deliver flexible and reliable IT services.**

- VMware vSphere collects several **distinct products and technologies** that work together under the brand of the **VMware virtualization family** of products which acts as a **suite of software products** (like the **Microsoft Office suite**).

  - **Hyperviseur ESX / ESXi,**
  - **VMware vCenter Server,**
  - **VMware vSphere Client,**
  - **VMware VMFS.**



Composants of VMware vSphere

- vSphere is a suite of products that exists in several versions: Standard, Enterprise and Enterprise Plus
- **ESX**i is a Type 1 hypervisor installed on a physical machine on which you can create and run virtual machines and **virtual appliances**.
  It is the main foundation for all VMware functionality
- **vCenter Server** is a service that acts as a central administrator for ESXi hosts connected in a network. It also allows you to manage the resources of several hosts. vCenter Server can be installed on **Server** or on **a virtual appliance**
- **vSphere Client HTML5** is used to access ESXi Server to create and manage virtual machines on an ESXi server.

Shared Resources: Overview of ESXi

Learner Objectives

1) Describe the ESXi host architecture
2) Navigate the Direct Console User Interface (**DCUI)** to configure an ESXi host
3) Use the new VMware Host Client to administer an ESXi host
4) Configure ESXi host settings

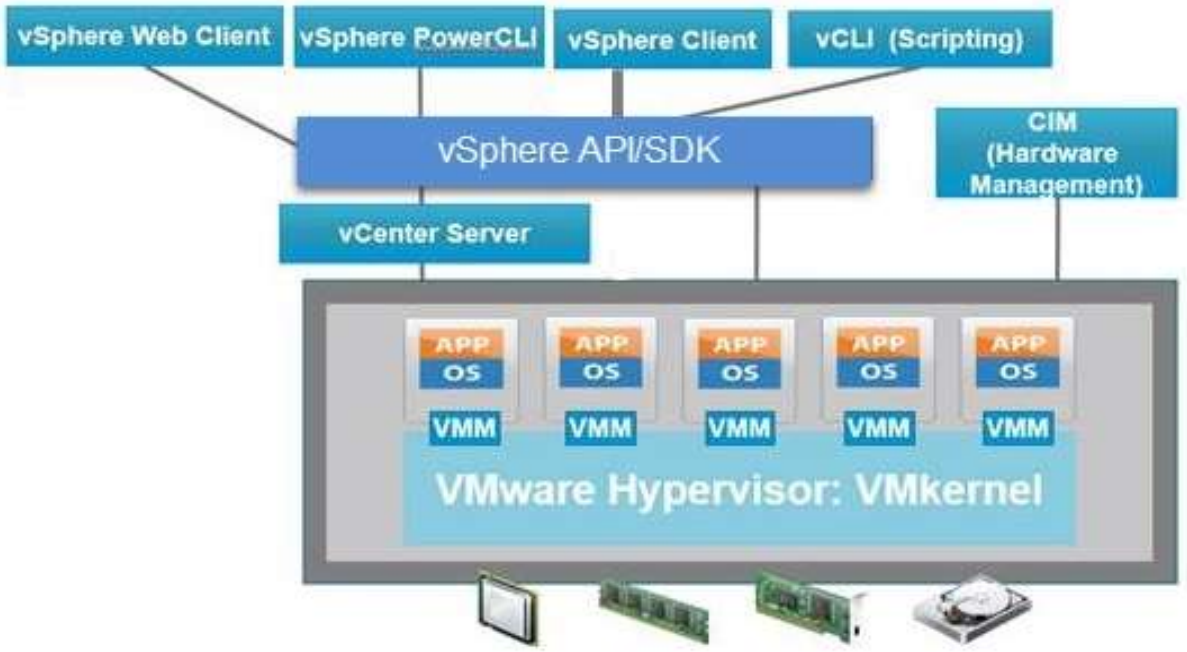
About ESXi Hosts

An ESXi host has the following availability and features:

- Available for **purchase (**acheter) **with vSp**here or as a **free version** that can be downloaded.
- High security:
  - **Host-based firewall**: ESXi includes a firewall between the management interface and the network
  - **Kernel module integrity** :Digital signing ensures the integrity and authenticity of modules, drivers,…
  - **Lockdown modes** (**confinement mode**) :Lockdown mode is a vSphere feature that **disables login and API functions** from being executed directly on an ESXi host
  - Trusted platform module
  - UEFI secure boot
- Small disk footprint (Faible encombrement disque)
- Installable on **hard disks**, **SAN LU**Ns, **USB** devices, **SD cards**, and diskless hosts (Hotes sans disque)

Physical and Virtual Architecture

The ESXi hypervisor provides a virtualization layer that abstracts the processor, memory, storage, and networking resources of the physical host and allocates them to multiple virtual machines.



Physical and Virtual Architecture

- ESXi is a **bare-metal hypervisor** that creates the foundation for a dynamic and automated data center
- In the ESXi architecture, applications running in virtual machines access CPU, memory, disk, and network interfaces without direct access to the underlying hardware

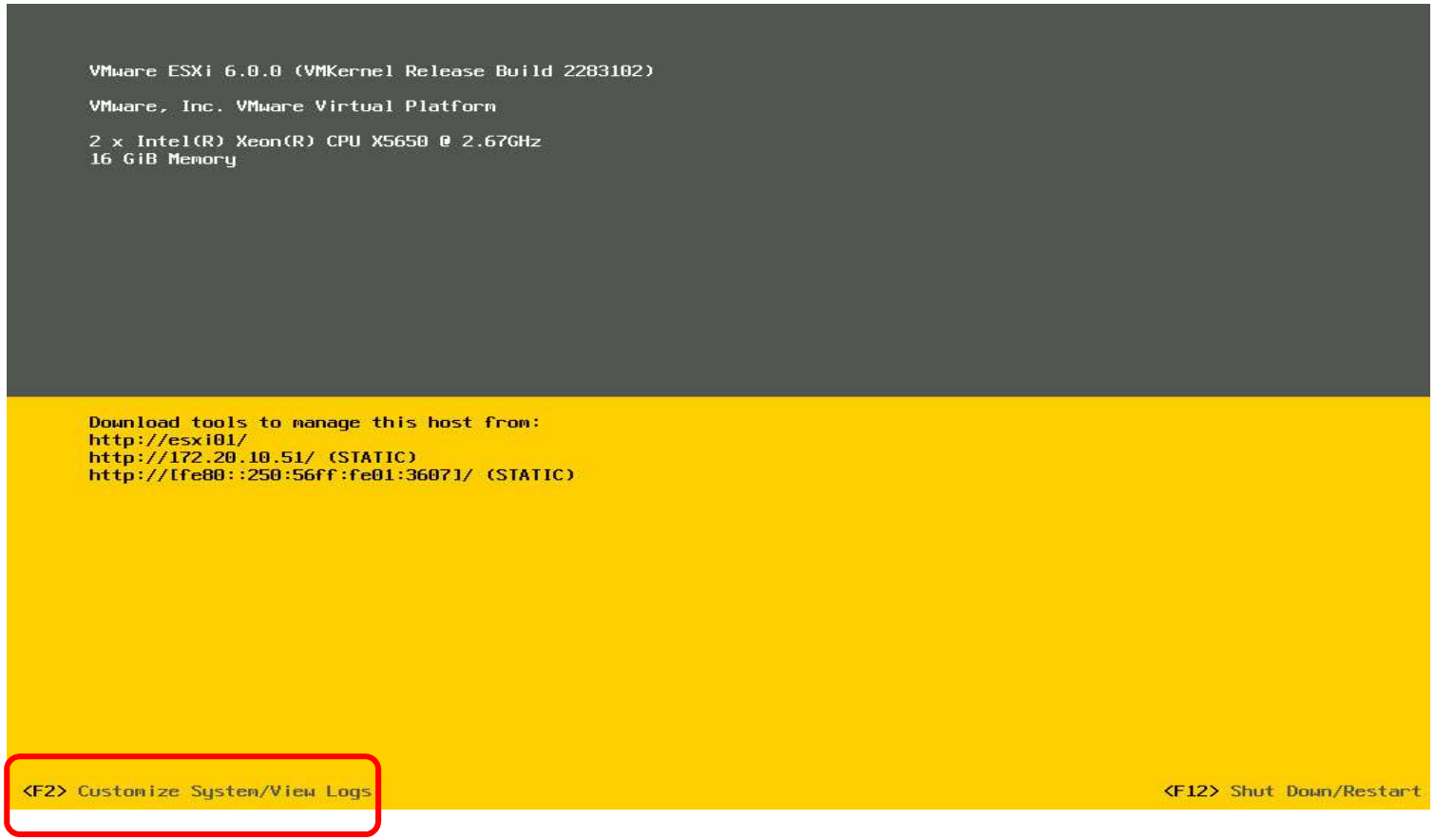
- The ESXi Hypervisor receives requests from virtual machines for resources from t**he virtual machine monitor (VMM**) and presents the requests to the physical hardware

- Each **powered-on virtual machine** has its **own dedicated VMM** that is responsible for presenting virtual hardware to the virtual machine and receiving request

- An ESXi host can be accessed through several interfaces:
  - vSphere Web Client (connected to vCenter Server)
  - vSphere HTML5-based clients (connected directly to the host or to vCenter Server)
  - VMware vSphere® Command-Line Interface
  - VMware vSphere® API and VMware vSphere® Management SDK

Configuring an ESXi Host

The DCUI is similar to the BIOS of a computer, with a keyboard-only UI.

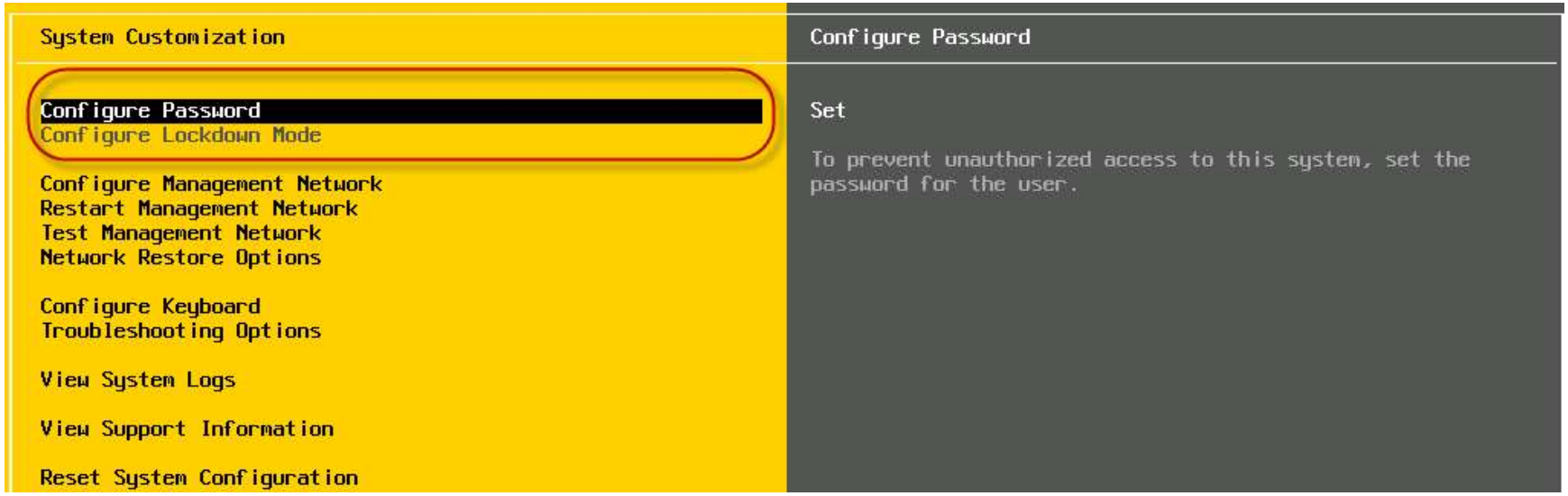


You use the Direct Console User Interface (DCUT) to configure certain settings for ESXi hosts. The DCUT is a low-level configuration and management interface, accessible through the console of the server, used primarily for initial basic configuration. You press F2 to start customizing system settings

Configuring an ESXi Host: Root Access

DCUI enables an administrator to configure **root access** settings:

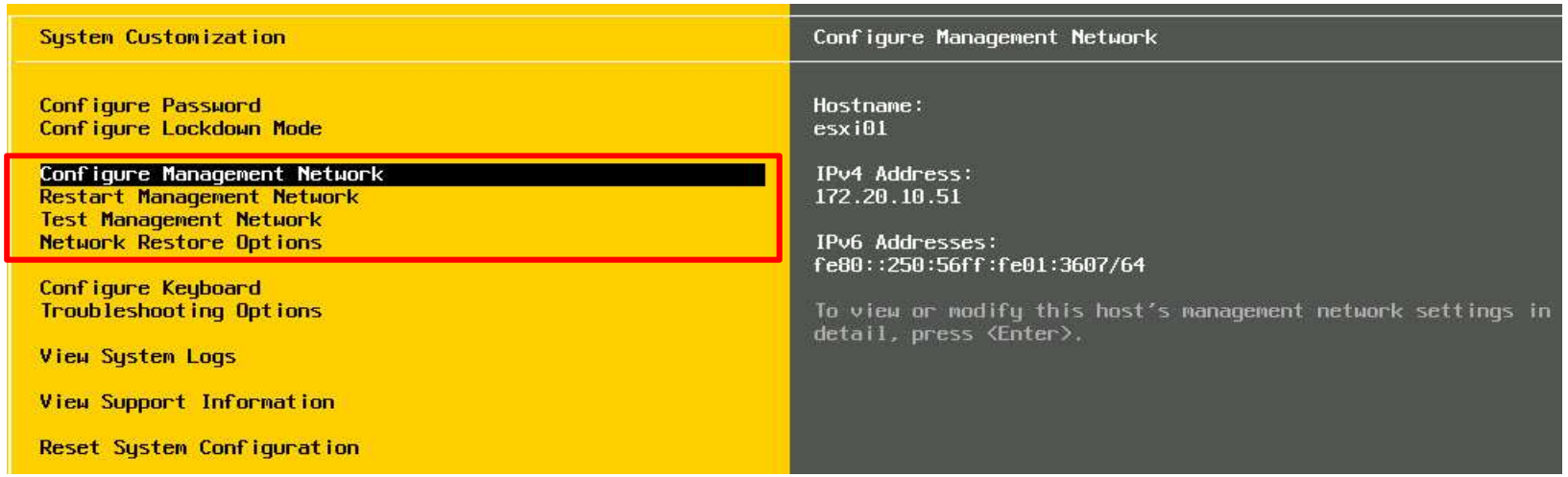
- Set a root password (complex passwords only).
- Enable or disable **lockdown mode**:
  - Limits management of the host to vCenter Server.
  - Enabled only for hosts managed by vCenter Server.



The administrative user name for the ESXi host is root. By default, the administrative password is not set .

Configuring an ESXi Host: Management Network

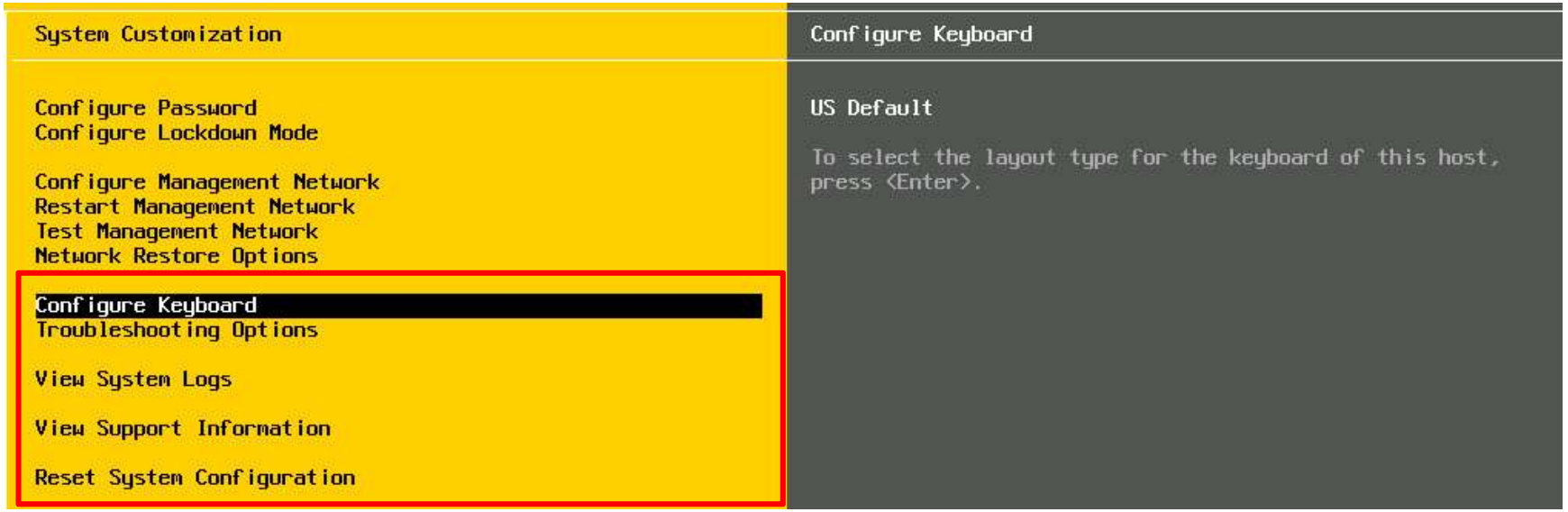
- The DCUI enables you to modify network settings:
  - Host name
  - IP configuration (IP address, subnet mask, default gateway)
  - DNS servers



- By default, a DHCP-assigned address is configured for the ESXi host.
- You can also modify the network adapter used for the management network, configure VLAN setting, configure IPv6 addressing, and set custom DNS suffixes
- You can restart the management network (without rebooting the system), test the management network (using ping and DNS requests), and disable a management network.

Configuring an ESXi Host: Other Settings

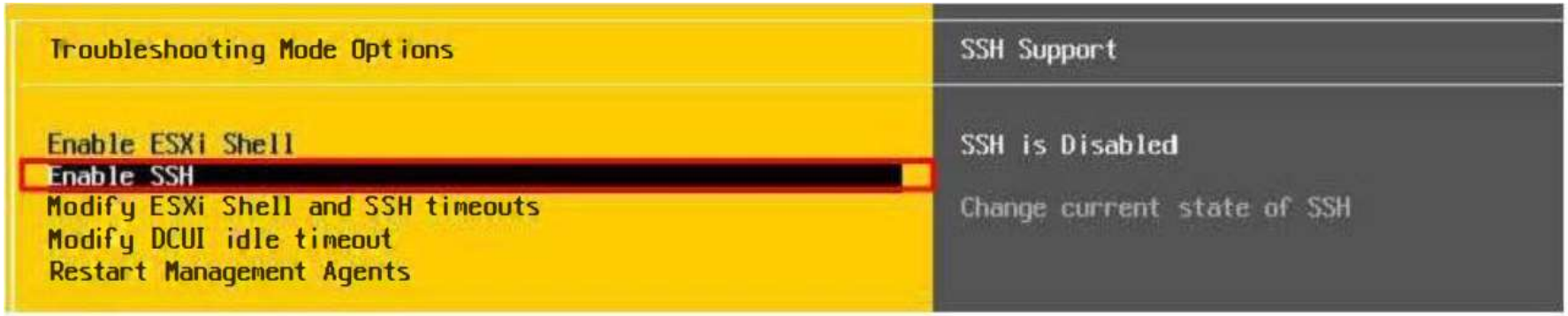
The DCUI enables an administrator to configure the keyboard layout, enable troubleshooting services, view support information, and view system logs.



The DCUI enables you to change the keyboard layout, view support information, such as the host's license serial number, and view system logs.
The default keyboard layout is U.S. English

Configuring an ESXi Host: Other Settings

- The troubleshooting options allow you to enable or disable troubleshooting services. By default, they are disabled:
  - VMware vSphere® ESXi™ Shell: For troubleshooting issues locally
  - SSH: For troubleshooting issues remotely by using an SSH client, for example, **PuTTY**



- The best practice is to keep troubleshooting services disabled until they are necessary, for example, when you are working with VMware technical support to resolve a problem

Remote Access Settings: Security Profile

❑ The security profile controls **remote access to an ESXi host**:

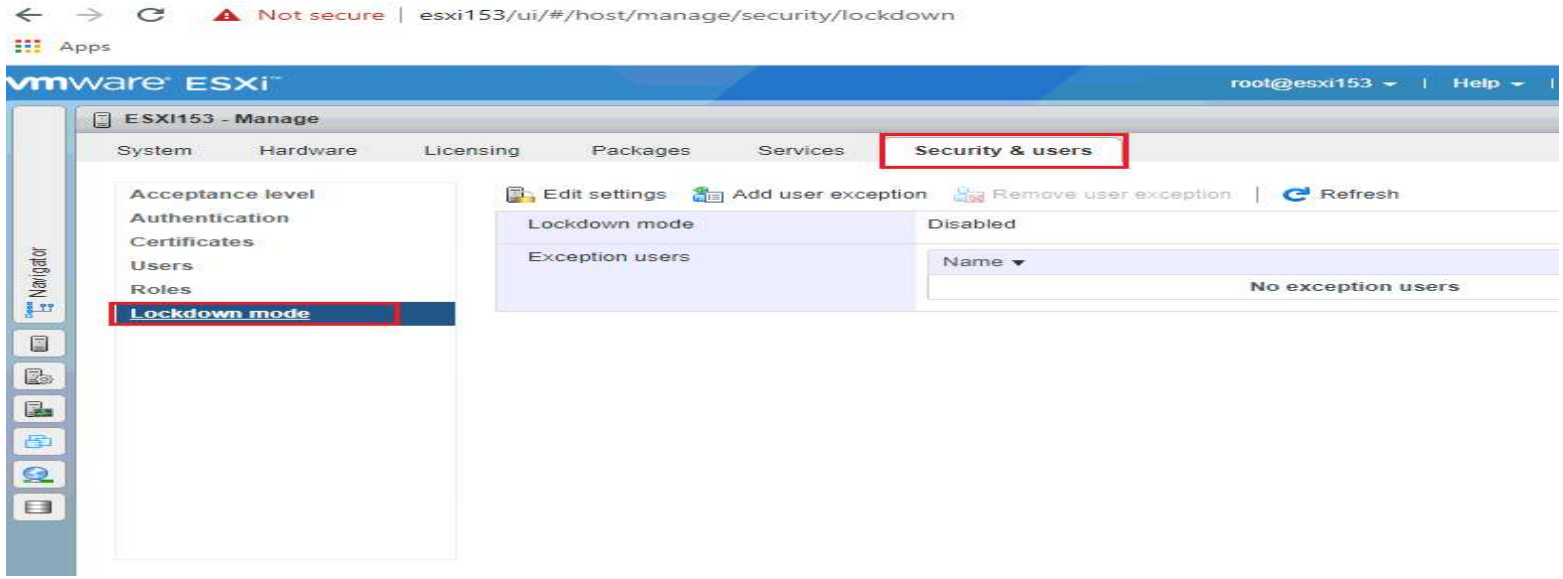
- ESXi includes a **firewall** that is enabled by default.
- The ESXi firewall **blocks incoming and outgoing traffic**, except for the traffic that is enabled in the host's security profile.(excepté traffic activé dans le profil de sécurité de l'hôte)
- You can customize many essential security settings for an ESXi host through the Security Profile panel in vSphere Web Client.
- Some services can be managed by the administrator. Some daemons, such as DCUI and NTP server processes, can start and stop automatically with the ESXi host.

Configuring Lockdown Mode

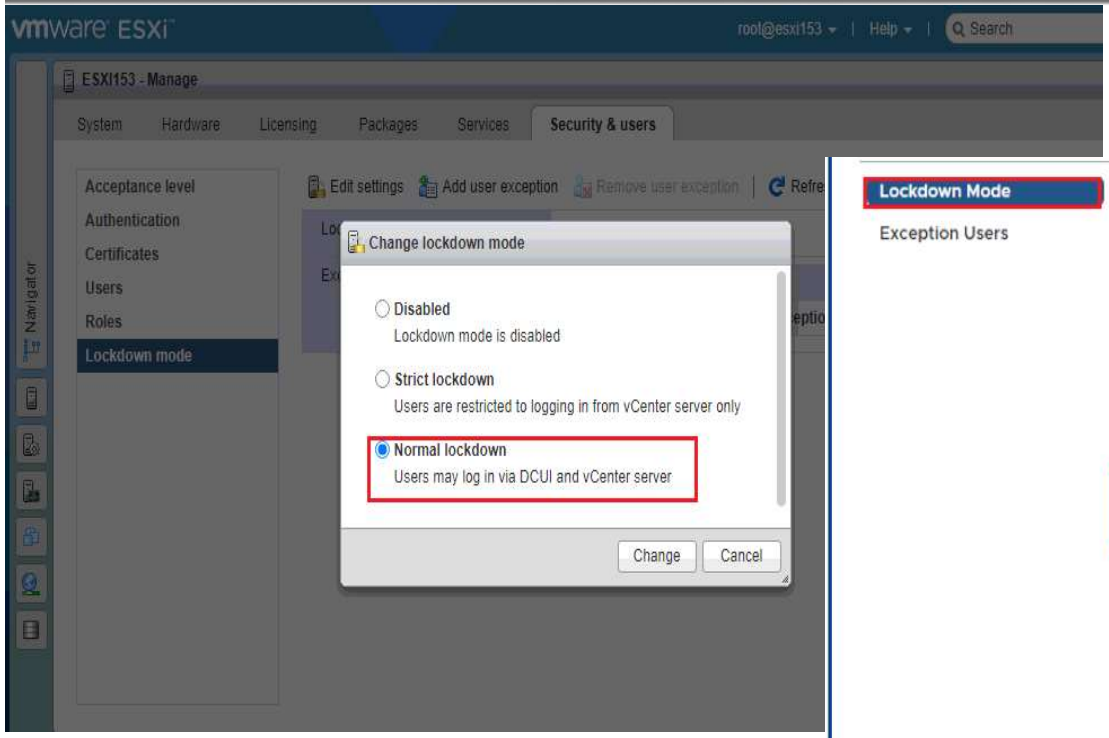
- To increase the security of your ESXi hosts, you can put your hosts in lockdown mode: Two lockdown modes are available: **Normal and strict**.

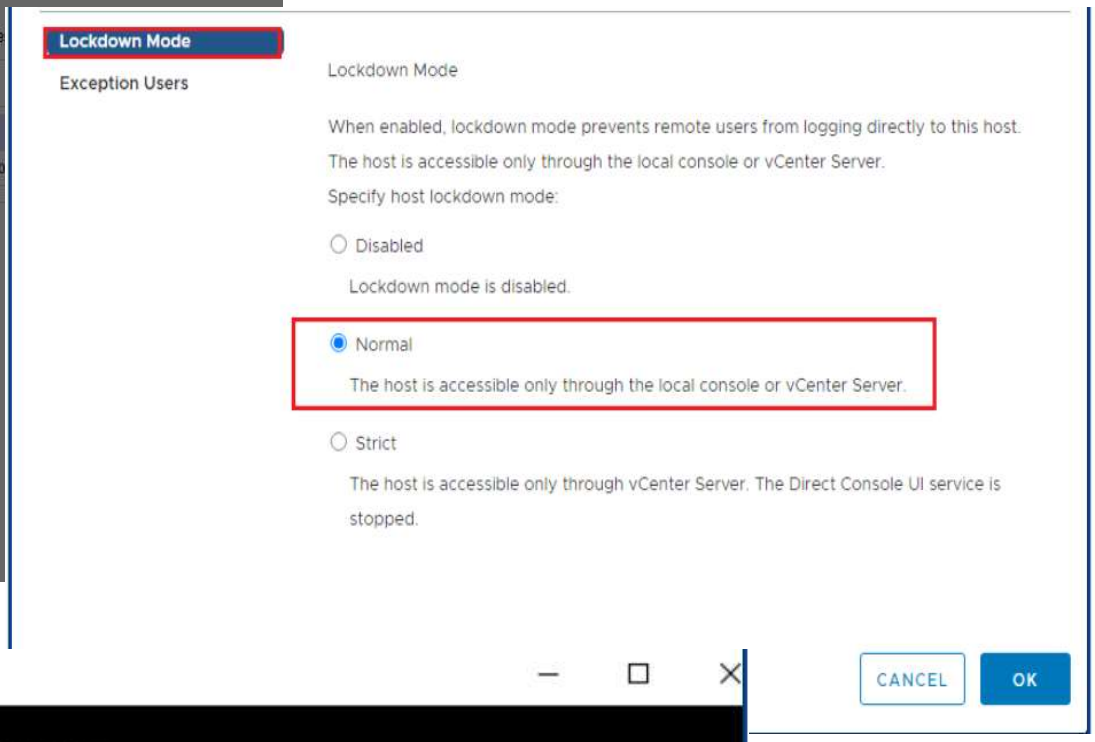
By default lockdown mode is disabled

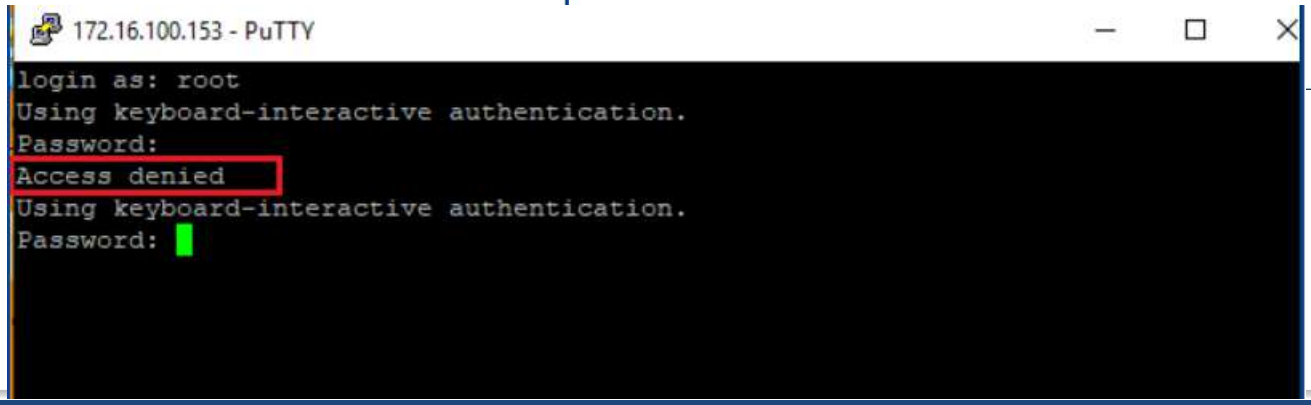
- **enable Lockdown mode from the vSphere Web Client:**
  - •Browse to the host in the vSphere Web Client inventory.
  - •Click the **Manage** tab and click **Settings.** (Click the Configure tab)
  - •Under System, select **Security Profile**.
  - •In the **Lockdown Mode** panel, click **Edit.**
  - •Click Lockdown Mode and select one of the **lockdown mode option**



Configuring Lockdown Mode







Lab 1 : Installing ESXi

Install ESXi on a VM using your student desktop

1. Access Your Student Desktop
2. Install ESXi
3. Assign VMware Licenses From ESXi

Lab 2 : Configuring ESXi Hosts

Configure an ESXi host

1. Examine the Options in the DCUI
2. Configure the root Password
3. Enable SSH
4. Configure Esxi Networking
5. View the System Logs
6. Add ISO Files to Datastore in VMware ESXi