Virtualization and hypervisors

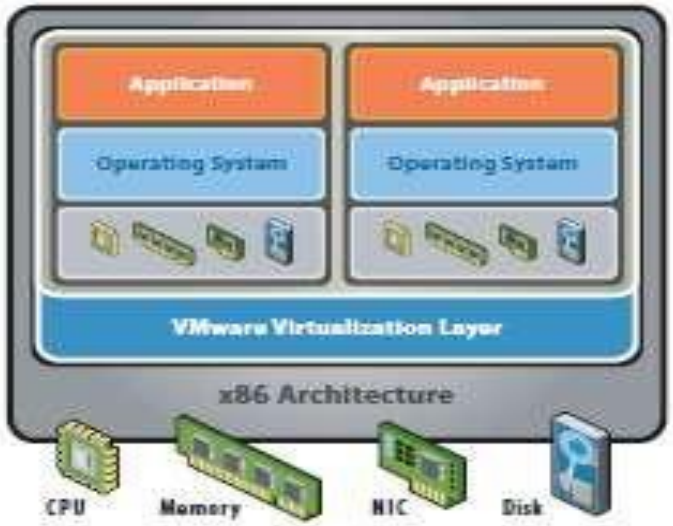
MAJOR PROJECT
MID-EVALUATION

What is a virtualization?

Virtualization allows multiple operating system instances to run concurrently on a single computer; it is a means of separating hardware from a single operating system.

Before Virtualization:

- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure



After Virtualization:

- Hardware-independence of operating system and applications
- Virtual machines can be provisioned to any system
- Can manage OS and application as a single unit by encapsulating them into virtual machines

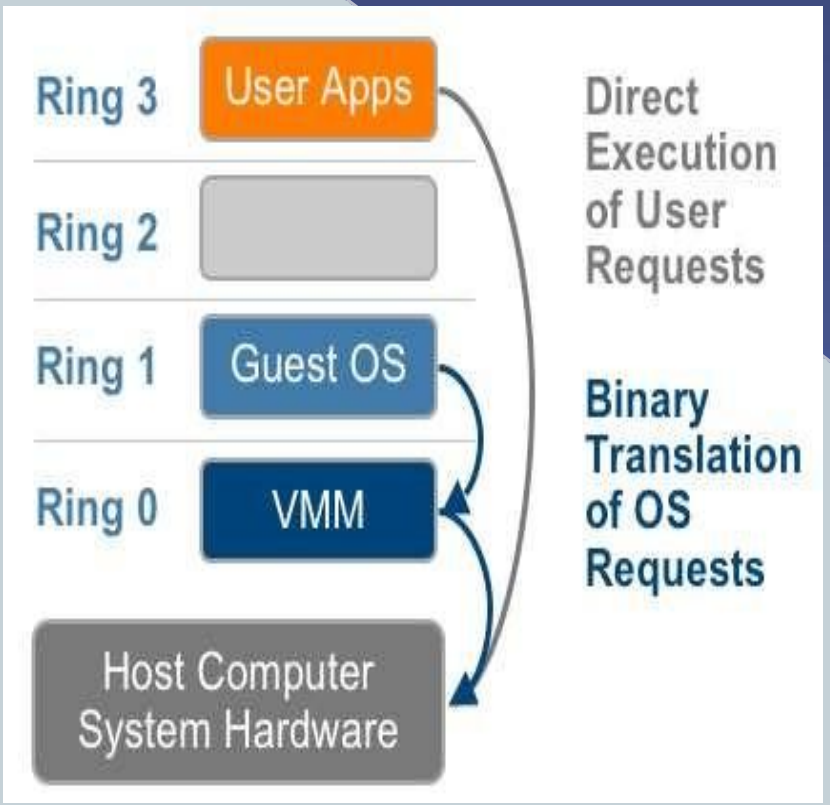
Advantages of virtualization

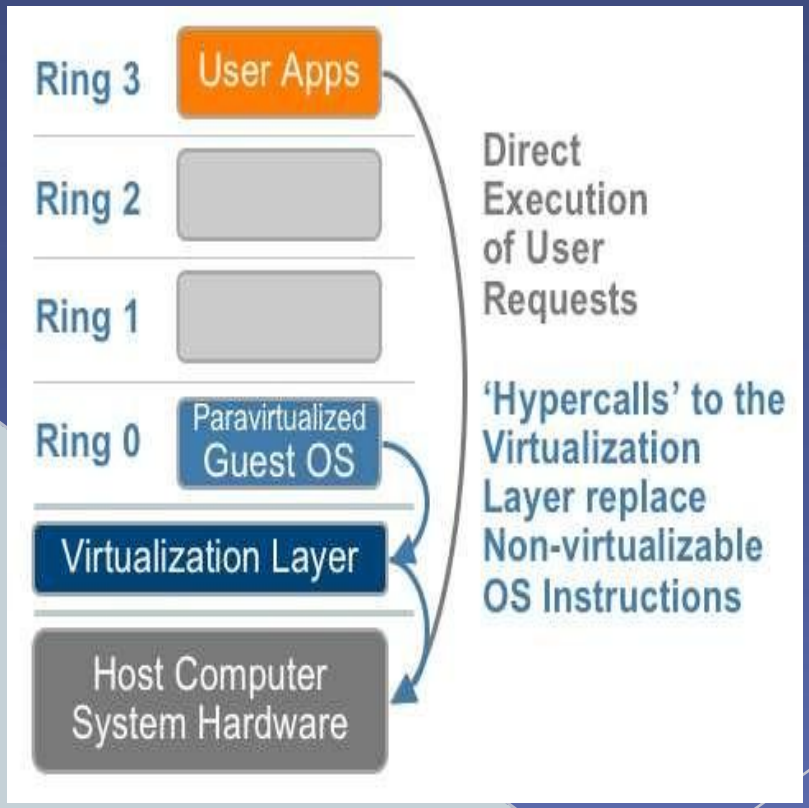
- Coexistence of Operating Systems on the same machine
- Protection
- Operating System research
- Software testing and runtime debugging
- Optimization of hardware utilization
- Job migration
- Virtual storage
- Back Up an Entire Operating System
- AND MANY MORE…..

Types of virtualization

1. CPU virtualization
    1. full virtualization
    2. para-virtualization
    3. hardware assisted virtualization
2. Memory virtualization
3. Device and I/O virtualization

Full vs. paravirtualization

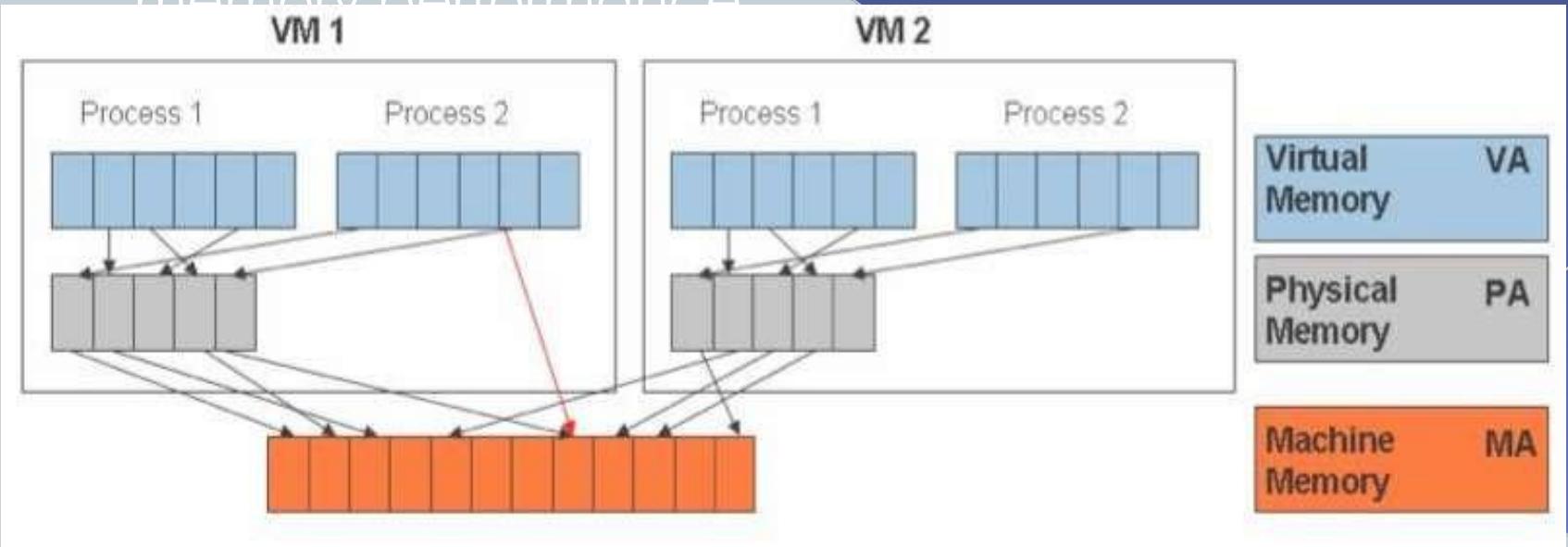




Unlike Full virtualization, Paravirtualization involves modifying the OS kernel to replace nonvirtualizable instructions with hypercalls that communicate directly with the virtualization layer hypervisor.

Memory virtualization

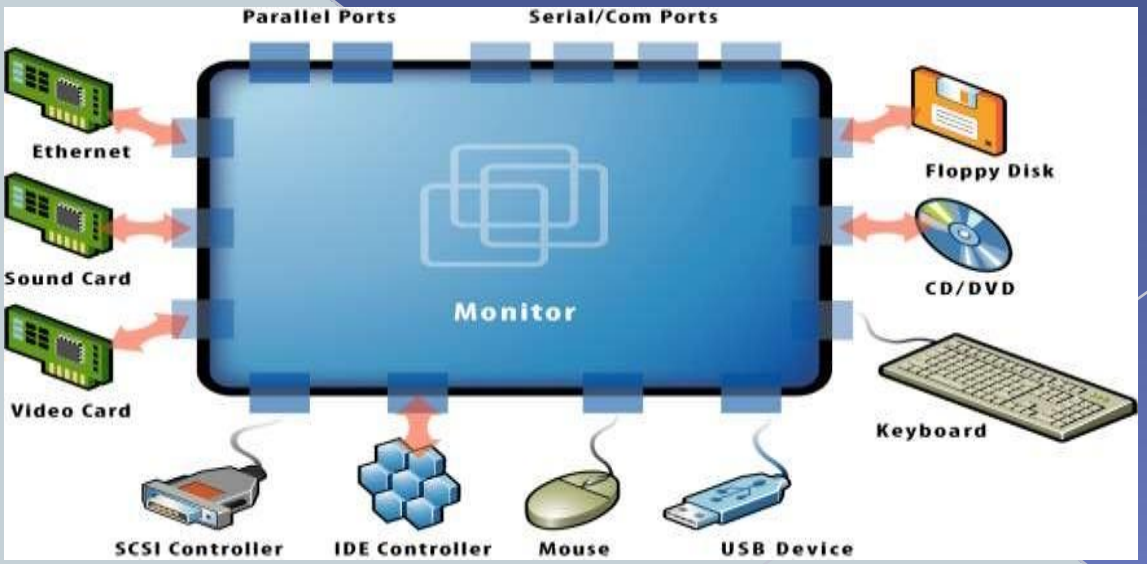
- Beyond CPU virtualization, This involves sharing the physical system memory and dynamically allocating it to virtual machines.
- The operating system keeps mappings of virtual page numbers to physical page numbers stored in page tables. All modern x86 CPUs include a memory management unit (MMU) and a translation lookaside buffer (TLB) to optimize virtual memory performance.



Device and I/O Virtualization

- The final component required beyond CPU and memory virtualization is device and I/O virtualization. This involves managing the routing of I/O requests between virtual devices and the shared physical hardware.

The hypervisor virtualizes the physical hardware and presents each virtual machine with a standardized set of virtual devices as seen in Figure .



What is a hypervisor?

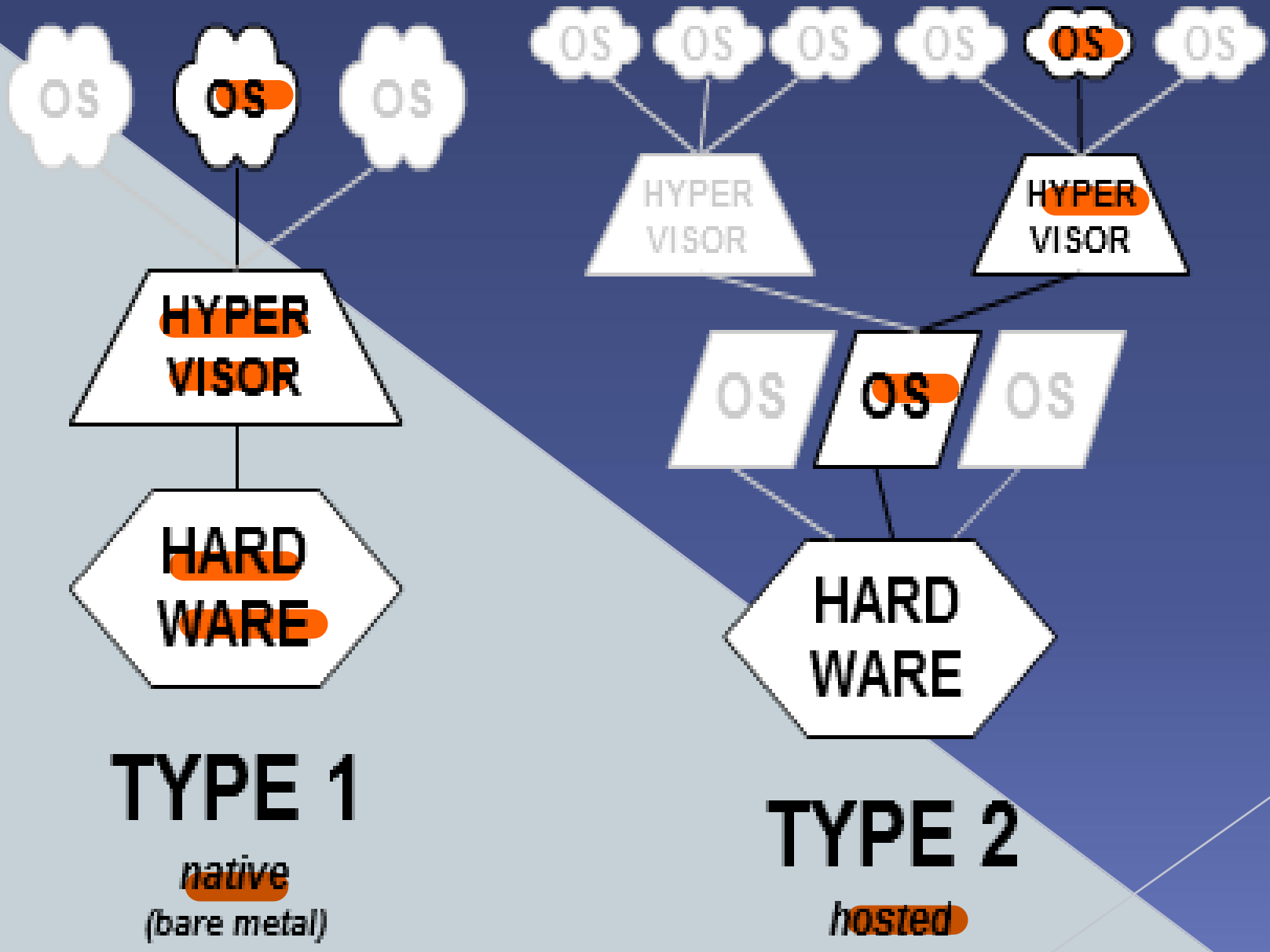
- A **hypervisor** or **virtual machine monitor** (**VMM**) is a piece of computer software, firmware or hardware that creates and runs virtual machines.
- A computer on which a hypervisor is running one or more virtual machines is defined as a *host machine*.
- Each virtual machine is called a *guest machine.*

Types of hypervisor

- **Type 1** hypervisor is installed directly on bare-metal hardware, it doesn't require an additional OS, it is the OS, even it it is a light or minimal OS.
- **EX.** Kvm and Xen
- **Advantages:** System is thin, the hypervisor has direct access to the HW, higher density hardware.
- **Disadvantages:** Really, Really large VMs are not supported, HW should support virtualization technology, costlier and Really bad console interface.

Types of hypervisor

- **Type 2** is more of an application installed on an operating system and not directly on the bare-metal.
- **EX.** VirtualBox and Vmware Workstation
- **Advantages:** Run on a greater array of HW because the underlying Host OS is controlling HW access, Easy user interface, Data can be secured on the desktop .
- **Disadvantages:** Decreased security, Loss of Centralized Management, Lower VM Density, Cannot support as many VMs are the first type.


OS
OS
OS
HYPER VISOR
HARD WARE
TYPE 1
native
(bare metal)
OS
OS
OS
OS
OS
OS
HYPER VISOR
HYPER VISOR
OS
OS
OS
HARD WARE
TYPE 2
hosted

Top hypervisors

Table 1: Hypervisor Usage

Metrics	Primary	Also Use	Plan To Stop	Evaluating
VMware	52%	21%	1%	8%
Xen (Citrix & Oracle)	18%	32%	7%	31%
KVM (Fedora, Ubuntu, SUSE)	9%	30%	5%	19%
Microsoft Hyper-V	9%	16%	6%	18%
Red Hat (RHEL, RHEV)	6%	29%	5%	11%
Other	6%	14%	8%	12%

- **Primary** — The single main hypervisor used as the standard for virtualizing their servers. The survey allowed only one response in this category.
- **Also Use** — Respondents were asked to report other hypervisors deployed in their datacenter. There was no limit to the number of these responses and many organizations had more than one secondary hypervisor.
- **Plan to Stop** —This was to capture which hypervisors organizations have currently deployed but planned to cease using in the near future.
- **Evaluating** — Aberdeen asked if there were hypervisors that are being evaluated or considered for future datacenter deployment.

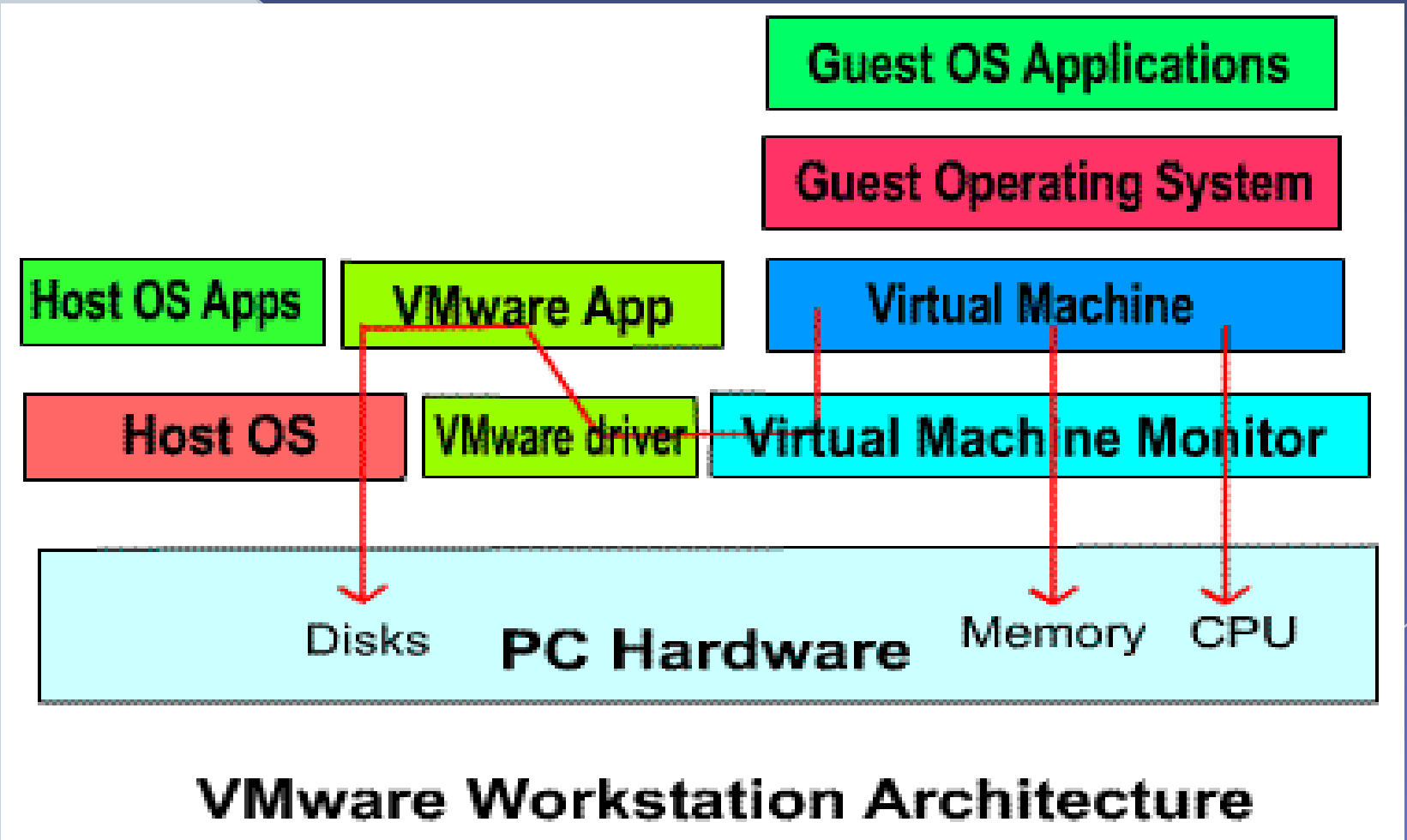
Vmware workstation– features

- Supports bridging existing host network adapters and share physical disk drives and USB devices with a virtual machine.
- It can simulate disk drives. It can mount an existing ISO image file into a virtual optical disc drive so that the virtual machine sees it as a real one. Likewise, virtual hard disk drives are made via .vmdk files
- VMware Workstation can save the state of a virtual machine (a "snapshot") at any instant. These snapshots can later be restored, effectively returning the virtual machine to the saved state.

architecture

- **Infrastructure** : Vmware Virtual machine file system(VMFS), Vmware Virtual Symmetric Multi processing(SMP), Virtual Infrestucture web access, Vmware Vmotion, Vmware Distributed Resource Scheduler
- **Storage And Arrays**:Fiber Channel SAN arrays, iSCSI SAN arrays and NAS arrays are widely-used storage technologies supported by Vmware Infrastructure to meet different data center storage needs
- **Ip Networks**: Each computing server can have multiple gigabit Ethernet network interface cards(NICs) to provide high bandwidth and reliable networking to the entire data center

Vmware Workstation-architecture



Vmware

pros

- Encrypts a virtual machine as a way to keep it from being used by unauthorized personnel
- Each VM can now support up to 16 virtual CPUs and 16 cores per virtual CPU, up to 64GB of RAM
- Can configure up to 20 virtual networks within a single instance of Workstation.
- Availability of hardware-specific features to guests is constrained by the actual machine

cons

- VMware is overpriced.
- Availability, reliability, Complexity issue.
- Reduced application performance
- Hyper-V and XenServer are better alternatives
- Hardware compatibility
- Application compatibility

Virtualbox – features

- **Portability.** VirtualBox runs on a large number of 32-bit and 64-bit **host** operating systems.
- **No hardware virtualization required.**
- **Guest Additions.** After installing the Guest Additions, a virtual machine will support automatic adjustment of video resolutions, seamless windows, accelerated 3D graphics and more. Hence, improving the performance of the guest OS and providing additional integration and communication with the host system.
- **Great hardware support.**
- **Guest multiprocessing-** VirtualBox can present up to 32 virtual CPUs to each virtual machine, irrespective of how many CPU cores are physically present on your host.
- USB device support, Hardware compatibility, Full ACPI support, PXE Network boot, Built-in iSCSI support.
- **Multigeneration branched snapshots.**
- **Clean architecture; unprecedented modularity.**
- **Remote machine display.**
- **Extensible RDP authentication, USB over RDP**

VirtualBox - pros

- Offers built-in GUI-based wizard for cloning a VM.
- Offers built-in VM snapshot, and supports multiple snapshots.
- Supports multiple types of disk image (e.g., vdi, vmdk, vhd, hdd, qed, qcow).
- Supports multiple virtual monitors for a guest VM. Multiple virtual monitors belonging to a VM can be displayed in multiple windows of host machine, or via multiple physical monitors.
- Can be installed on OS X, Windows 7, Windows 2008 Server, Solaris, OpenSolaris, FreeBSD host operating systems.
- More frequent minor version upgrades.
- Comprehensive built-in command-line interface for creating and running VMs (e.g., VBoxManage).

VirtualBox cons

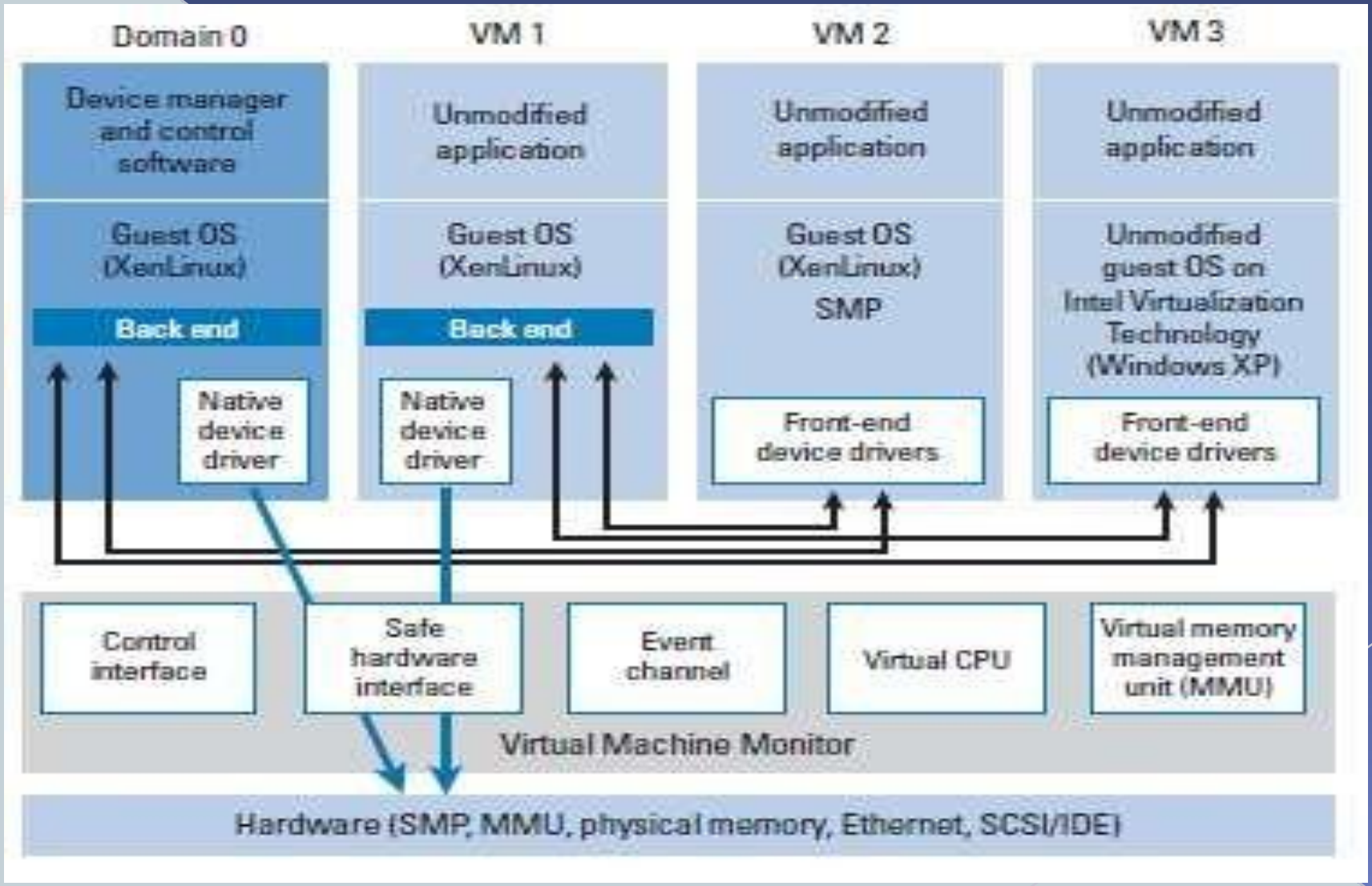
- OVF localization (multiple languages in one OVF file) is not yet supported.
- Cannot access NATed guest VMs from host machine without enabling port forwarding on host machine.
- NATed guest VMs are isolated from one other, and cannot communicate with one another.
- Bridged networking or host-only networking is required if guest VMs need to communicate with one another on the same Layer-2 network.
- Can add up to eight vNICs to a guest VM, while VMware Player can create up to ten vNICs per guest VM. You can configure only four vNICs via VirtualBox GUI. To add more than four vNICs, you need to use VirtualBox CLI.
- Does not support nested hardware-assisted virtualization.
- No support for USB 3.0.

XEN – features

- EFI (extensible Firmware Interface) support for hypervisor. Allows Xen to boot on machines which use EFI rather than a traditional BIOS
- Support up to 4095 Host CPUs for 64 bit h/v (from 256)
- Support for dom0 kernels compressed with xz
- Per-device interrupt remapping (increases scalability)
- Support for PVHVM guest direct physical IRQ injection (improves performance for PCI passthrough to Linux Guests)
- Multiple PCI segment support
- Lots of XSM / Flask fixes (security)
- AMD SVM "DecodeAssist" support (AMD CPU feature that avoids emulation and increases performance)
- Credit Scheduler tuning parameters:
  - sched_ratelimit_us
  - tslice_ms

- AMD OSVW (OS Visible Workarounds): Disables OS workarounds for hardware errata which are not necessary to workaround in guests because it is handled at the host level.
- Early boot time CPU microcode patching. Xen can supplied with the microcode image by the bootloader and load it early rather than relying on the domain 0 kernel to supply it later.
- Improvements to paging and sharing, enabling higher VM density for VDI use-cases
  - Heavily reworked page sharing. This remains a tech preview though due to limited tools support.
- Enhanced memaccess interfaces allowing increased introspection of guest memory by tools.
- Initial support for nested virtualisation. This allows HVM guests access to hardware virtualisation features such that they can run their own hypervisor.

XEN - architecture



XEN

pros

- It is more modernized than KVM, user friendly and can run without hardware support
- Support for multiple hardware platforms
- High security isolation features, independent of operating systems
- Offers paravirtualization and hardware assisted virtualization
- A different, user-friendly interface

cons

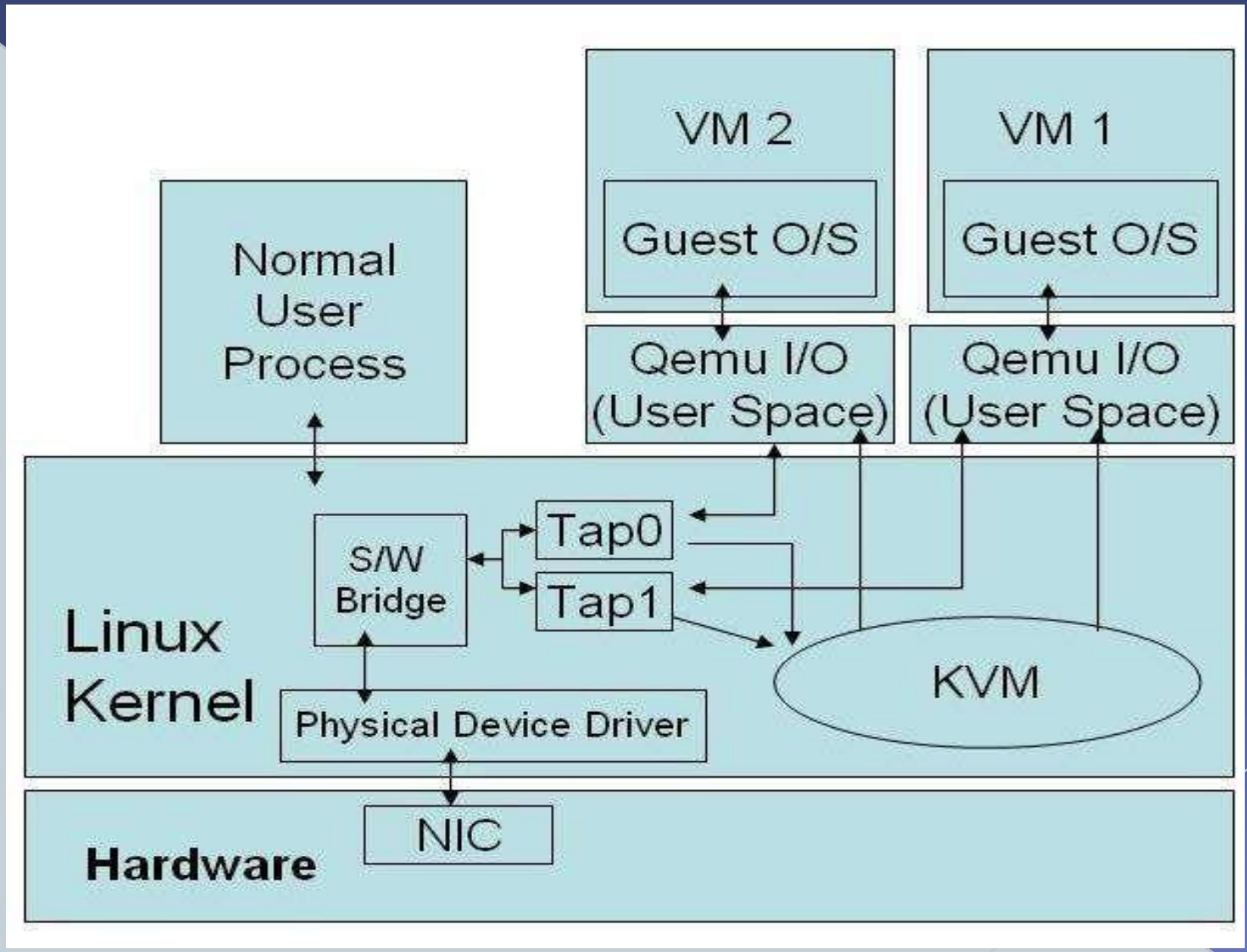
- It is not included in Linux except in recent versions
- It has minimal power management features
- It has a different dom0 structure increasing overload on CPU.
- More complex than other hypervisors

KVM – features

- NPT/EPT support (server boost)
- KSM (share memory with COW)
- Disk image cloning, sharing, snapshot
- Ballooning
- Live migration (nfs as shared storage)
- Save and restore VM
- Virtio paravirtualization
- PCI-passthrough VT-D/IOMMU support

KVM - architecture

- Each virtual CPU appears as a regular Linux process
- Emulation is handle by a modified version of QEMU
- Linux as a VMM
- Resource management
- The KVM control interface
- Emulation of hardware


VM 2
Guest O/S
VM 1
Guest O/S
Normal
User
Process
Qemu I/O
(User Space)
Qemu I/O
(User Space)
Tap0
S/W
Bridge
Tap1
Linux
Kernel
KVM
Physical Device Driver
NIC
Hardware

KVM

pros

- It is free.
- It is a part of Linux
- Powerful CPU virtualization on Intel and AMD platforms, leverages hardware virtualization and Linux kernel, memory management, I/O capabilities
- Real time scheduling
- Powerful GUI
- Powerful command line scripting tools for better productivity
- Leverages security, kernel capabilities and memory managemnt of Linux

cons

- A bit dated
- Difficult to master for novices and those used to GUI based usage
- Very slow when CPU does not support virtualization and when it works in QEMU mode
- Heavy I/O overhead
- Lack of flexibility in device assignment
- Issues in memory and power management

Comparison

1. TECHNICAL COMPARISON
2. BENCHMARKS
3. REAL-WORLD SCENARIOS

TECHNICAL COMPARISON in vmware and virtualbox

Host operating system support(virtualbox is better)

Ease of editing virtual machine's configuration (virtualbox is better)

Usb support (vmware is better)

Range of virtual hard disks (virtualbox is better)

Remote connections (virtualbox is better)

VM cloning (virtualbox)

7. Ease of boot (vmware is better)
8. USB over RDP (virtualbox is better)
9. "Teleportation" migration functionality.(virtualbox is better)
10. Command-line options.(virtualbox is better)
11. Graphics(VMware is better)
12. Ovf support(vmware is better)

TECHNICAL COMPARISON in XEN and KVM

HOST OS - KVM isn't an option on older CPUs made before the virtualization extensions were developed, and it rules out newer CPUs (like Intel's Atom CPUs) that don't include virtualization extensions.

Red Hat drops XEN and anoints KVM

Market of KVM and XEN - If you're going with RHEL over the long haul, bank on KVM. If you're running on Amazon's EC2, you're already using Xen, and so on

Operating system overhead - Xen is not burdened with any operating system overhead that is unrelated to processing a series of guests on a given machine

Security - Xen ensures a high level of security via a variety of methods/features: guest isolation,priviliged access, small code base and operating system seperation

6. **Maturity -** The Xen hypervisor has been available for enterprise deployment since 2004 and is the first open source hypervisor to successfully be deployed by industry leading Linux vendors
7. **Scheduling -**Xen uses its own kernel for thread scheduling and dispatching virtual machines, while KVM, accepted into mainline Linux kernel sources, uses that kernel for these operations
8. **Ease of use -** KVM is generally considered easier to configure and operate given it is just a single module that you load in the Linux kernel.
9. **Memory page sharing -**XEN doesn't implement memory page sharing and KVM does it very efficiently.
10. **Lack of Dom0 in kvm -**KVM introduces many performance benefits, such as less I/O latency due to lack of Dom0
11. **I/O and network operations –**

Kvm- VM -> Virtio -> CentOS with KVM

XEN- VM -> PV-OPS Driver -> Dom0 -> Xen