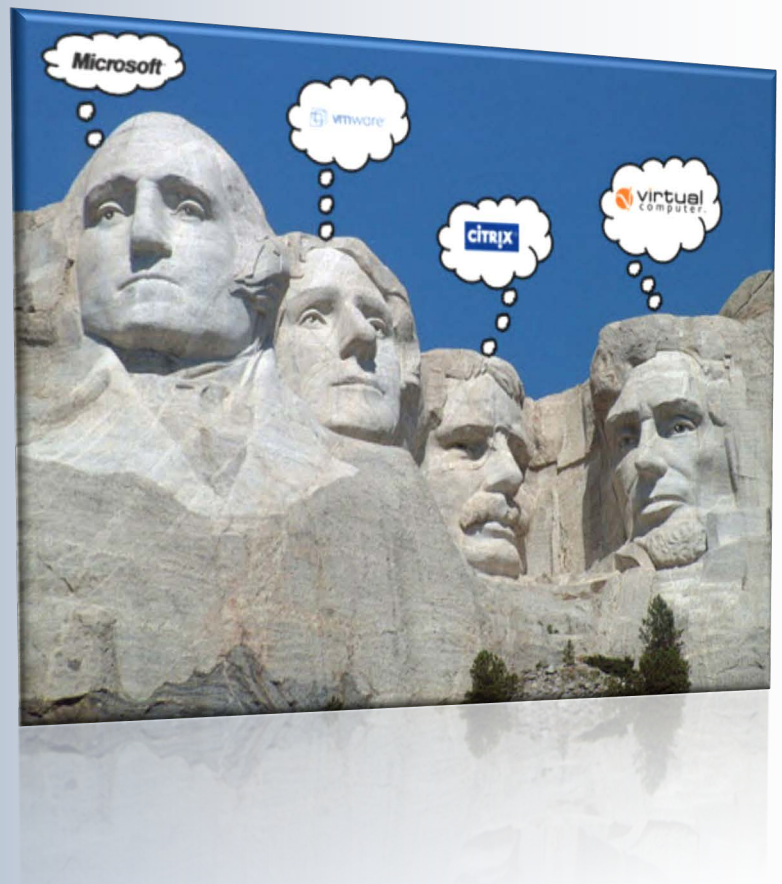
COMP 175

System Administration and Security



VIRTUALIZATION

Installation and Configuration

What we have to learn to do we learn by doing.

-Aristotle, Ethcia Nicomachea II c. 325 BC

Using a Live CD/DVD/USB only goes so far.

At some point you'll need to install an operating system

Physical – easier in a desktop, less so in a laptop

Multiboot - Partitions across one or more drives

Virtual machine - under a host OS

Flexible, inexpensive, experience, real-world

Additional layer of complexity

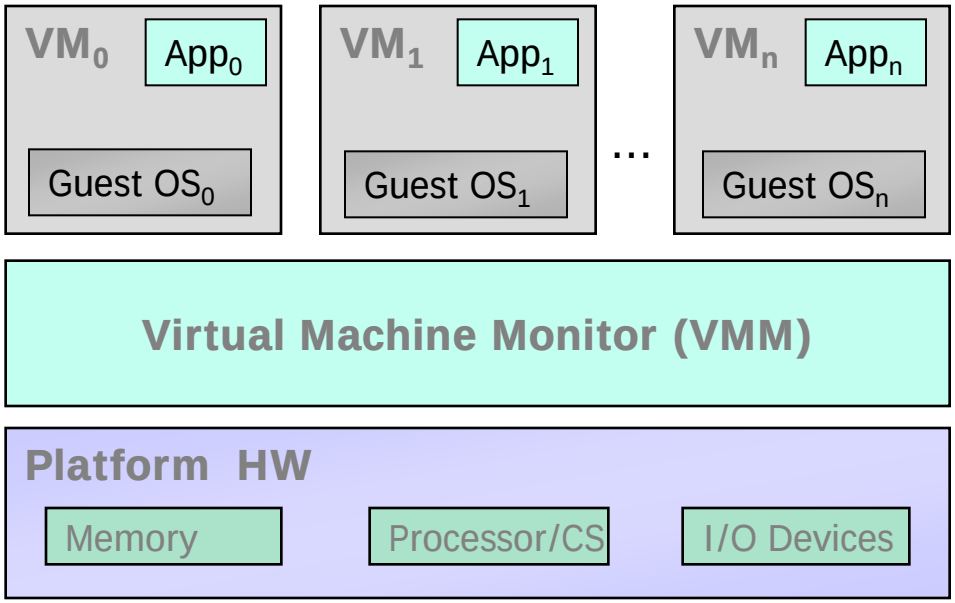
Virtual Machines

- A virtual machine (VM) is a "completely isolated guest operating system installation within your normal host operating system". Modern virtual machines are implemented with either software emulation or hardware virtualization.
- An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the virtual machine—it cannot break out of its virtual world.

Platform Virtualization

- Hide the physical characteristics of computer resources from the applications
- Not a new idea: IBM's CP-40 1967, CP/CMS, VM
- Full Virtualization
  - Simulate enough hardware so that an unmodified guest operating system can be run
  - Provides a full "virtual machine"
- Scenarios:
  - Run Linux in a virtual machine on Windows
  - Run multiple logical servers (each with own VM) on a single physical server

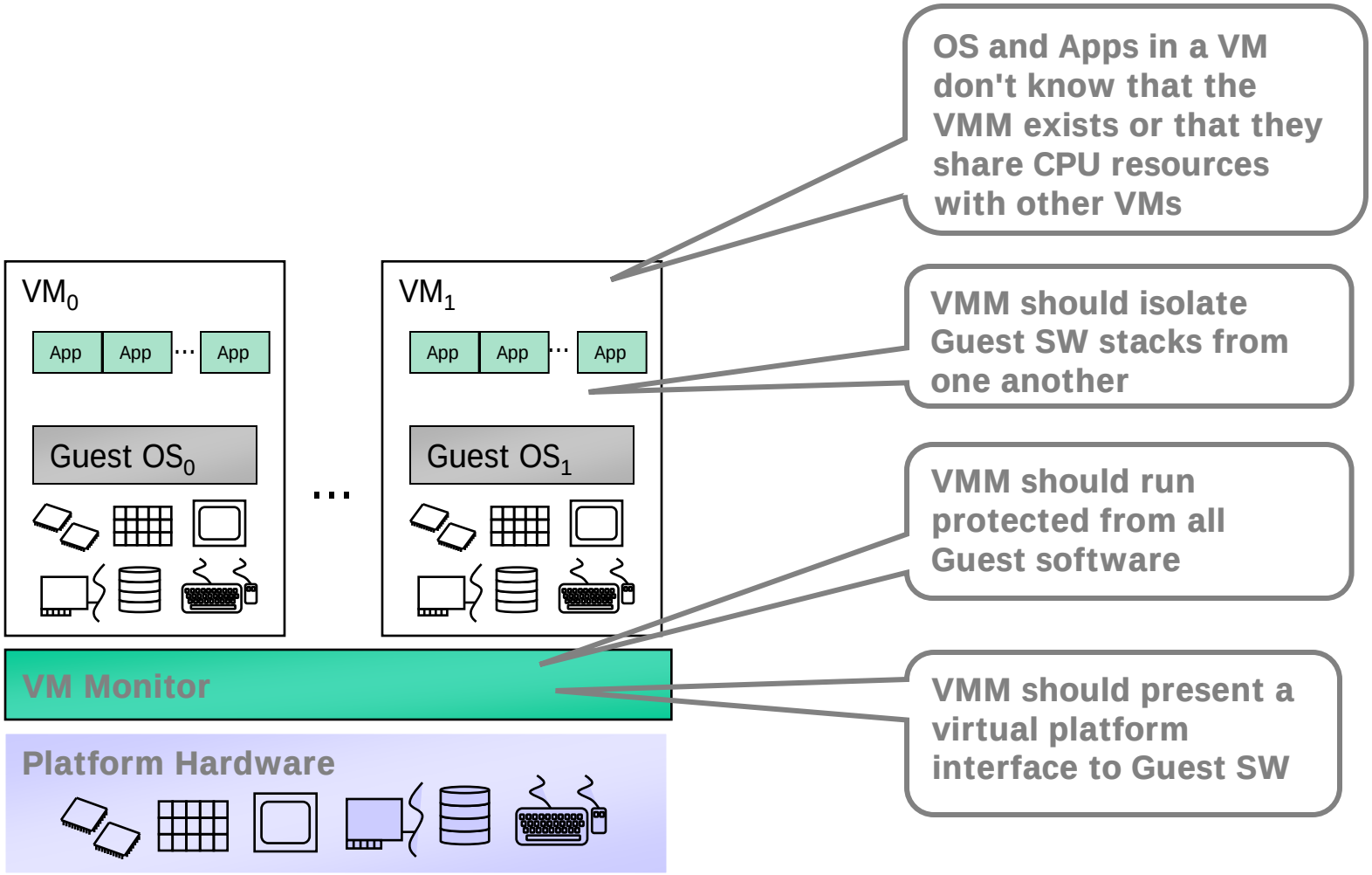
Virtual Machine Monitors (VMMs)



VMM - Hypervisor

Source: *Understanding Intel Virtualization Technology", N. Sahgal, D. Rodgers*

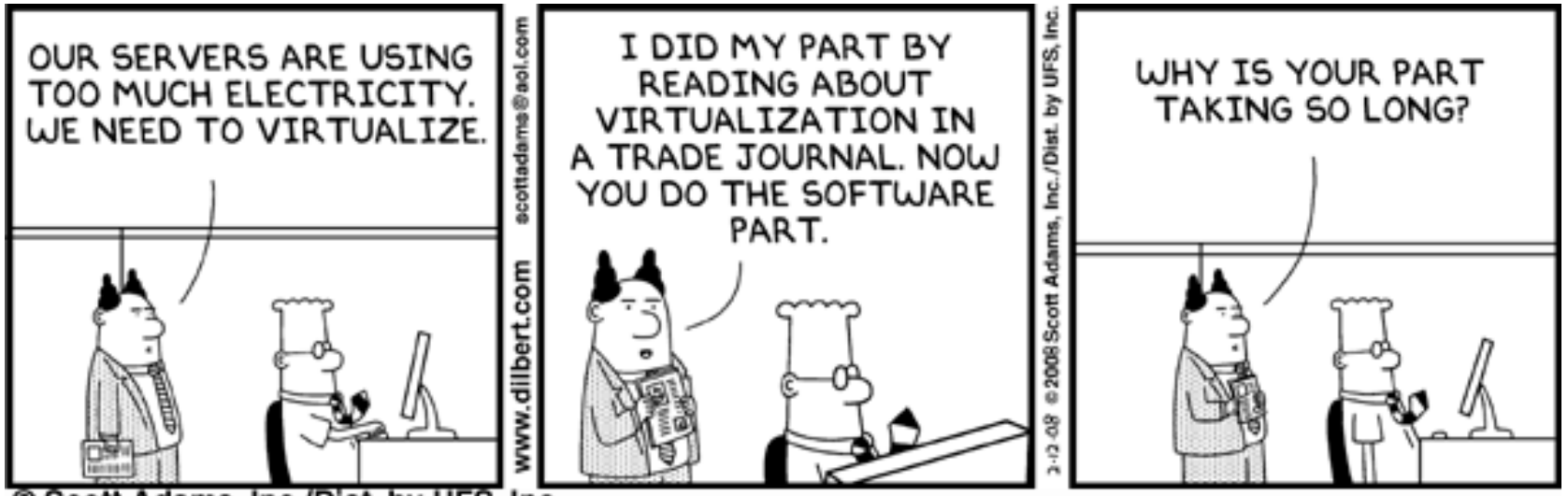
Challenges of Running a VMM



Source: *Understanding Intel Virtualization Technology", N. Sahgal, D. Rodgers*

VM & Hypervisor

- Virtual Machine
  - capable of virtualizing all hardware resources, processors, memory, storage, and peripherals
- Virtual Machine Monitor (VMM)
  - provides virtual machine abstraction
  - Also referred to as hypervisor



Virtualization Properties

- Equivalence
  - Program running under a VMM should exhibit a behavior identical to that of running on the equivalent machine
- Resource Control
  - VMM is in full control of virtualized resources
- Efficiency
  - Many machine instructions may be executed without VMM intervention

Recursive Virtualization

- The VMM can run on a copy of itself
- Possible if:
  - The architecture is virtualizable
  - VMM without timing dependences can be built
  - Virtualized Guest OS can’t see if it’s a guest?

Anyone recall the blue pill?
Blue Pill concept - trap a running instance of the OS by starting a thin hypervisor and virtualizing the rest of the machine under it. The previous OS would still maintain its existing references to all devices and files, but nearly anything, including hardware interrupts, requests for data and even the system time could be intercepted (and a fake response sent) by the hypervisor.

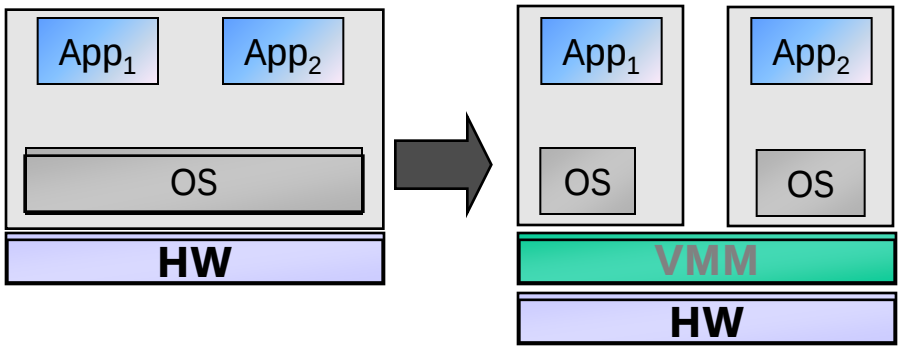
Non-Virtualizable Machines

- VMMs can't be built on non-virtualizable machines
- Workarounds:
  - patching – critical instructions removed and replaced with trap to VMM
  - paravirtualization – guest OS is modified (e.g., IBM VM)

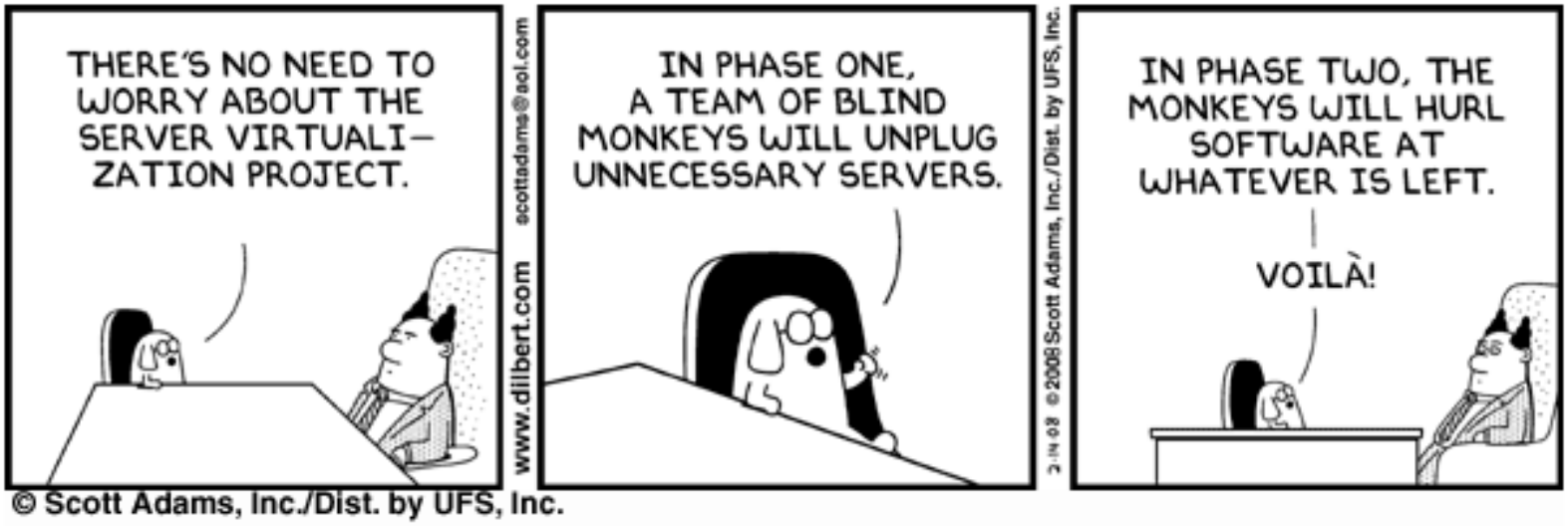
X86 Virtualization

- Before 2005 the x86 processor architecture did not meet virtualization requirements
- Change happened
- x86-64 Extension of the x86 instruction set
  - Intel VT-i (Virtualization Technology)
    - IA-32e, EM64T, Intel 64
    - IA-64 Itanium (not compatible)
  - AMD-V (Pacifica)
    - Athlon 64, Turion 64, Opteron

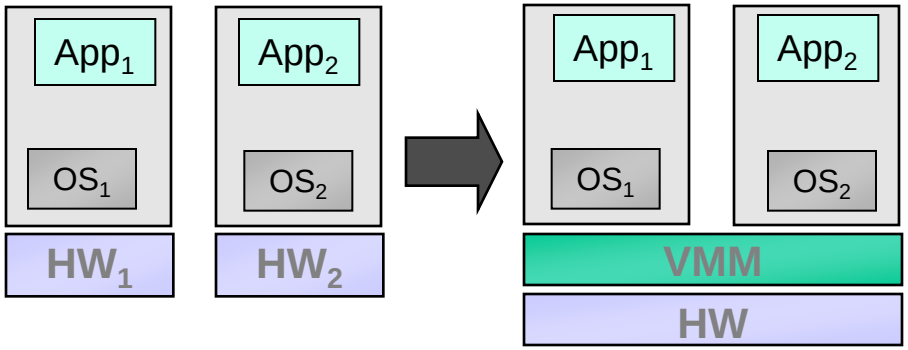
Virtualization: Isolation



- Provides multiple isolated user-space instances, instead of just one. Such instances (aka containers) may look and feel like a real server, from the point of view of its owner.
- Sandbox prevents interference between VM's



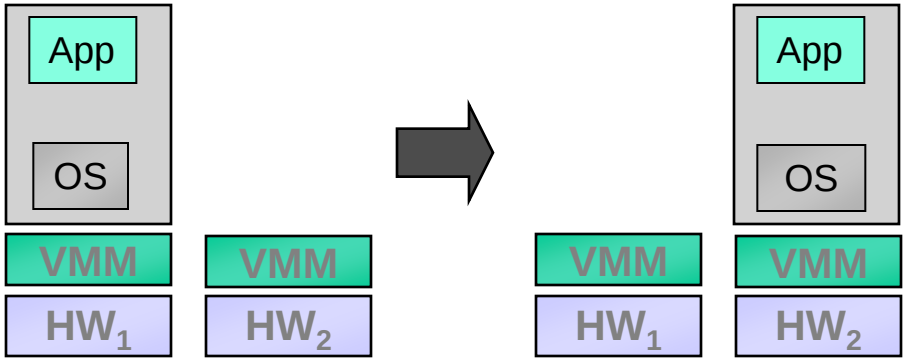
Virtualization: Consolidation



- Virtualize many single-purpose servers
- Less power, heat
- More efficient resource utilization

- Problem: Keeping C-level executives away from in-flight magazines laced with vendor articles?

Virtualization: Migration



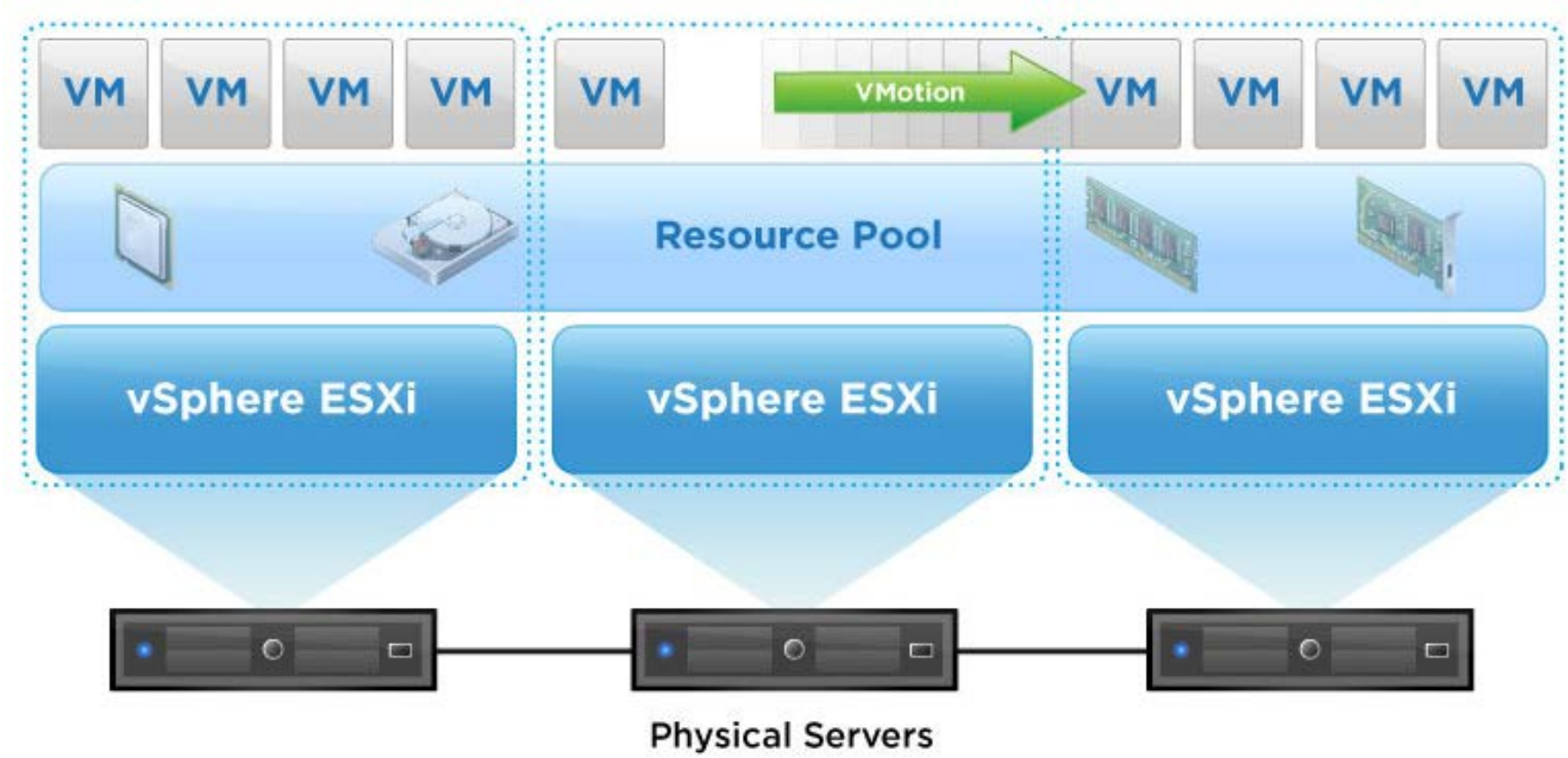
- Perform live migrations with zero downtime
- Undetectable to the user
- Continuously automatically optimize virtual machines within resource pools
- Perform hardware maintenance without scheduling downtime and disrupting business operations
- Proactively move virtual machines away from failing or underperforming servers

Virtualization Usages

- Legacy software support – Consolidation
- Training/QualityAssurance – Consolidation
- Activity Partioning – Isolation
- Administration – Consolidation, Isolation, Migration
- Failover Infrastructure – Migration

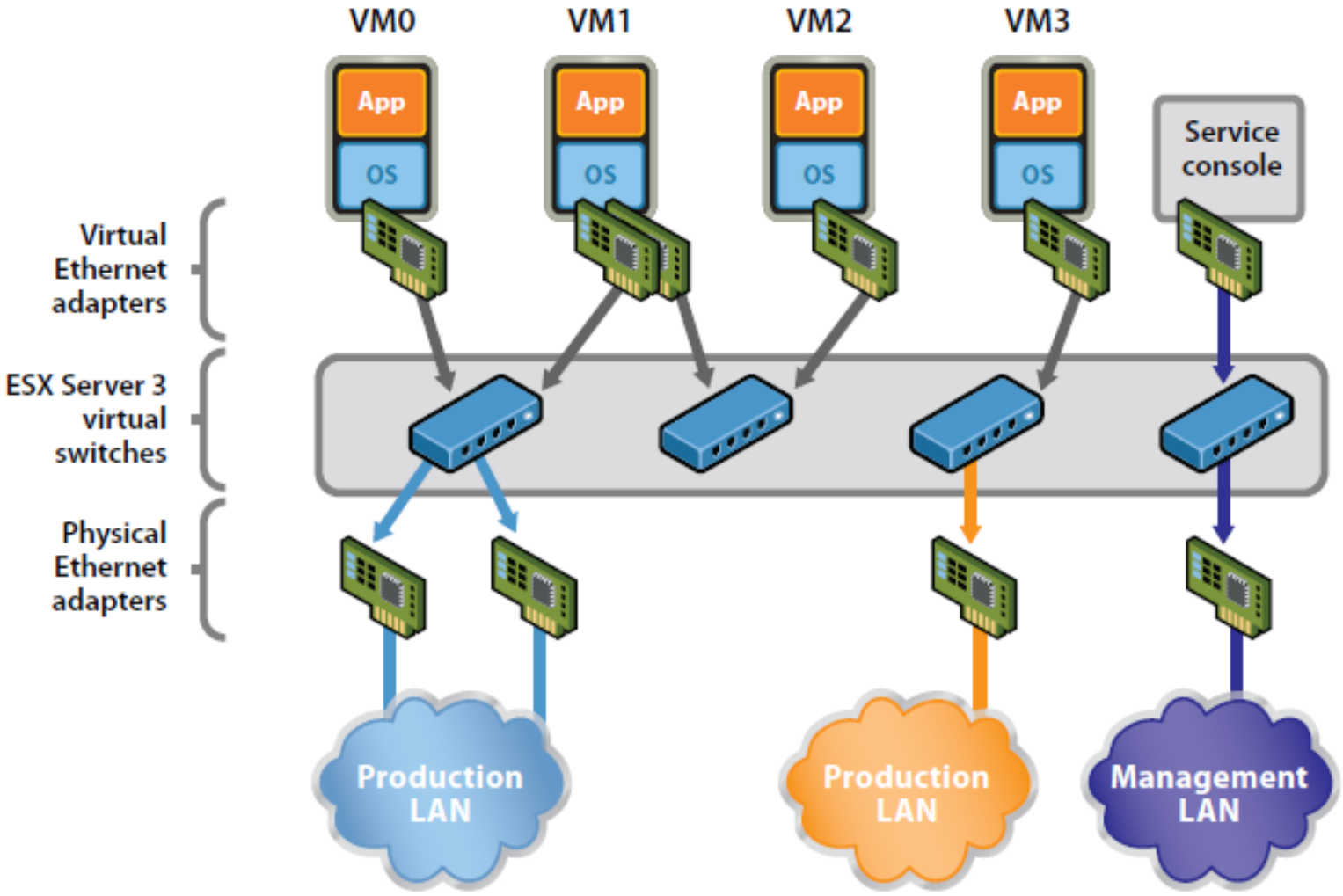
- Standardization
- Virtual sprawl – lack of controls
- Need additional management tools
- Specialized expertise

The Vision



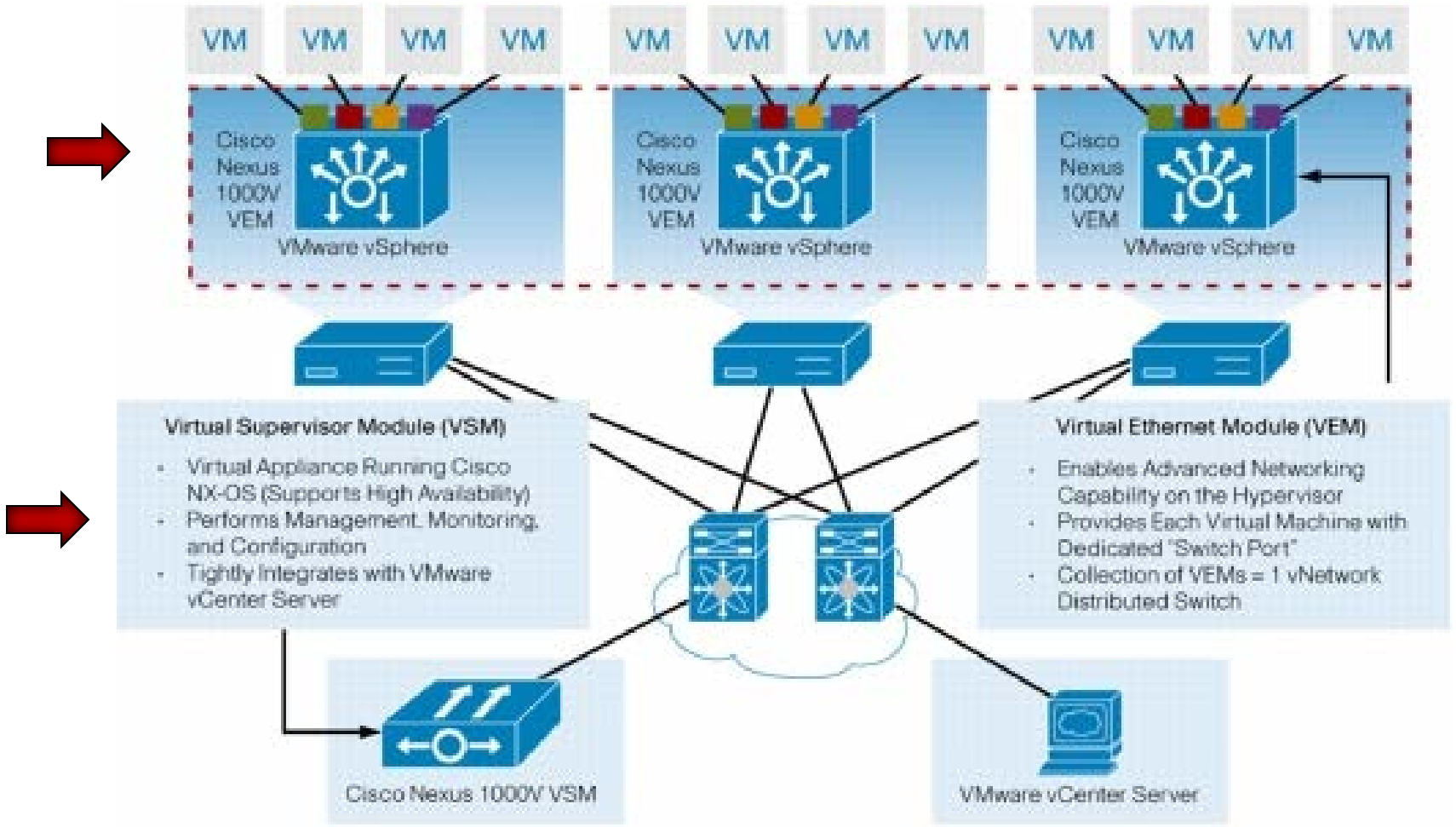
- Storage pool – SAN or NAS
  - SAN is Storage Area Network (virtualization)
  - NAS is Network Attached Storage

Virtualized Networking



Virtualized switching infrastructure

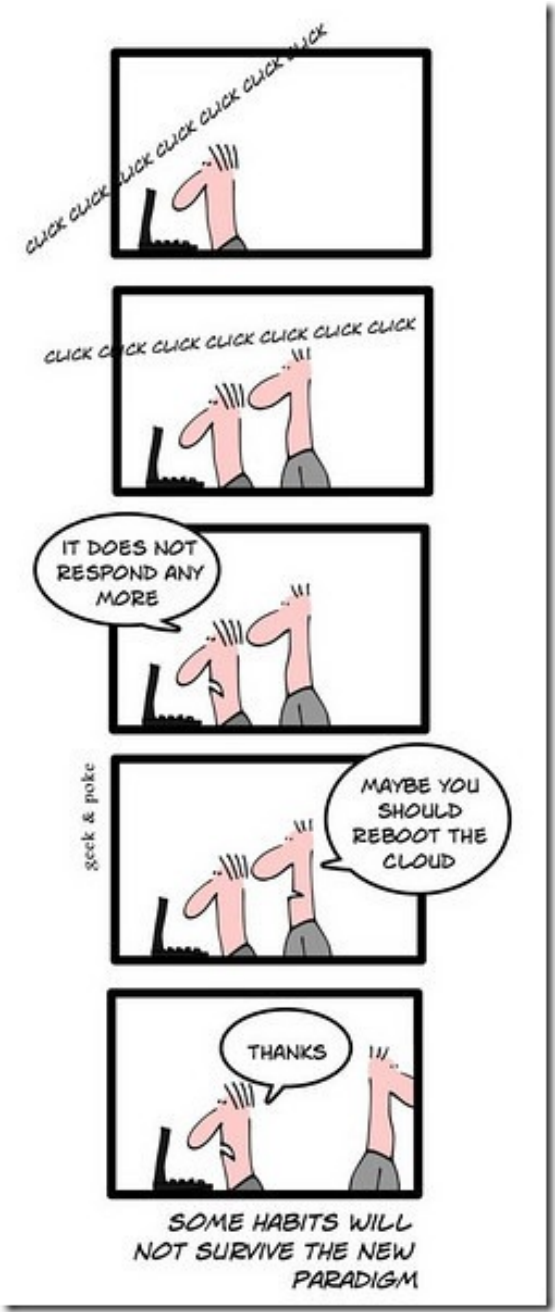
Virtual Data Center



New product opportunity: Cisco Nexus Switches

Virtualization

- Optimal for:
  - Datacenters
  - Clouds
- Issues
  - Increased abstraction
  - Complexity
  - Risk
    - Can’t reboot the cloud



Virtual Ethernet

- PortChannels
- Quality of service (QoS)
- Security
  - Private VLAN
  - Access Control Lists (ACLs)
  - Port Security
- Monitoring
  - NetFlow
  - Switch Port Analyzer (SPAN)
  - Encapsulated Remote SPAN (ERSPAN)

This is just asking for problems.
It is another skill set.
Easy to get things wrong.

Virtual Headaches

- VM's in different security domains – same VMM
- Virtual problems – hard to troubleshoot
  - Where is the VM at?
- Virtual spanning tree loops
- Patching problem still present
- Multiple vendors
- Virtual sprawl
- Problems can have large impacts

"The application is slow"

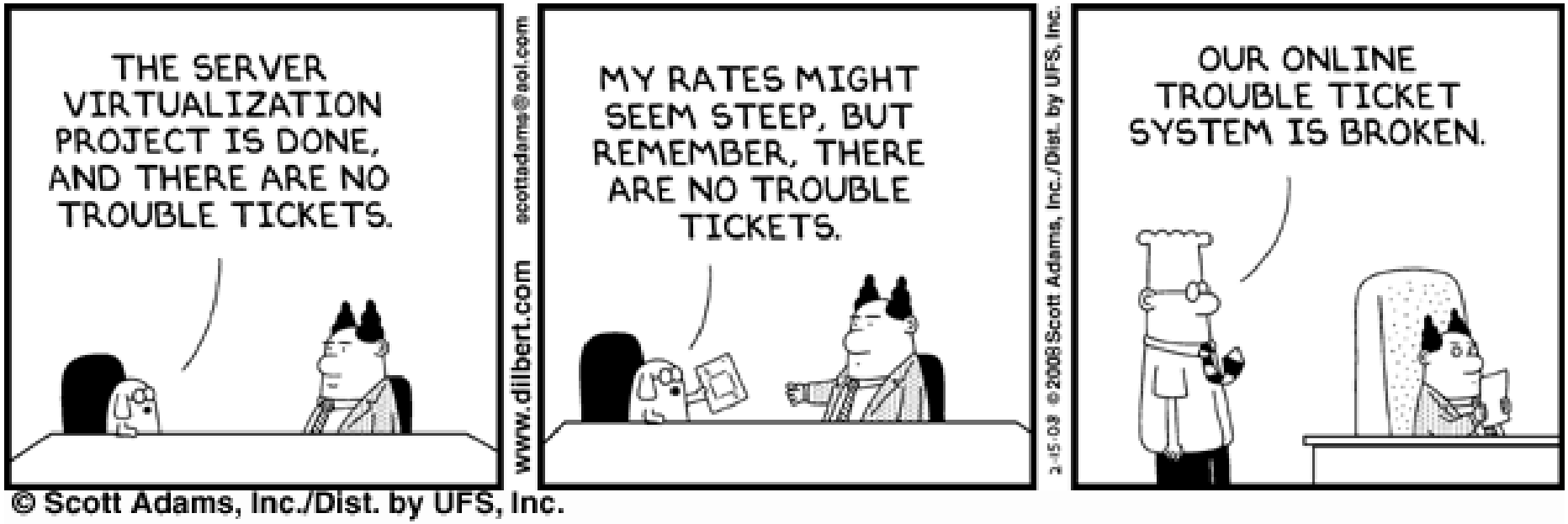
"The network is slow"

- What is the root-cause of the problem:
  - Is it the application? The virtualization layer?
  - Is it the network? Database? Storage …?
- Traditional tools have limited visibility
- Multiple administrators and tools
- Problem diagnosis becomes a very manual, time consuming and expert-based process

"The network is slow"

- One Egg – One basket
- August 9-13+ outage

It Was Virtualized 1st



Gaining Interest

- Desktop Virtualizition – why – what does it offer?
- Virtual desktop infrastructure (VDI)
- Store "virtualized" desktop on a remote server
- ~~ECPE's Virtual Lab?~~

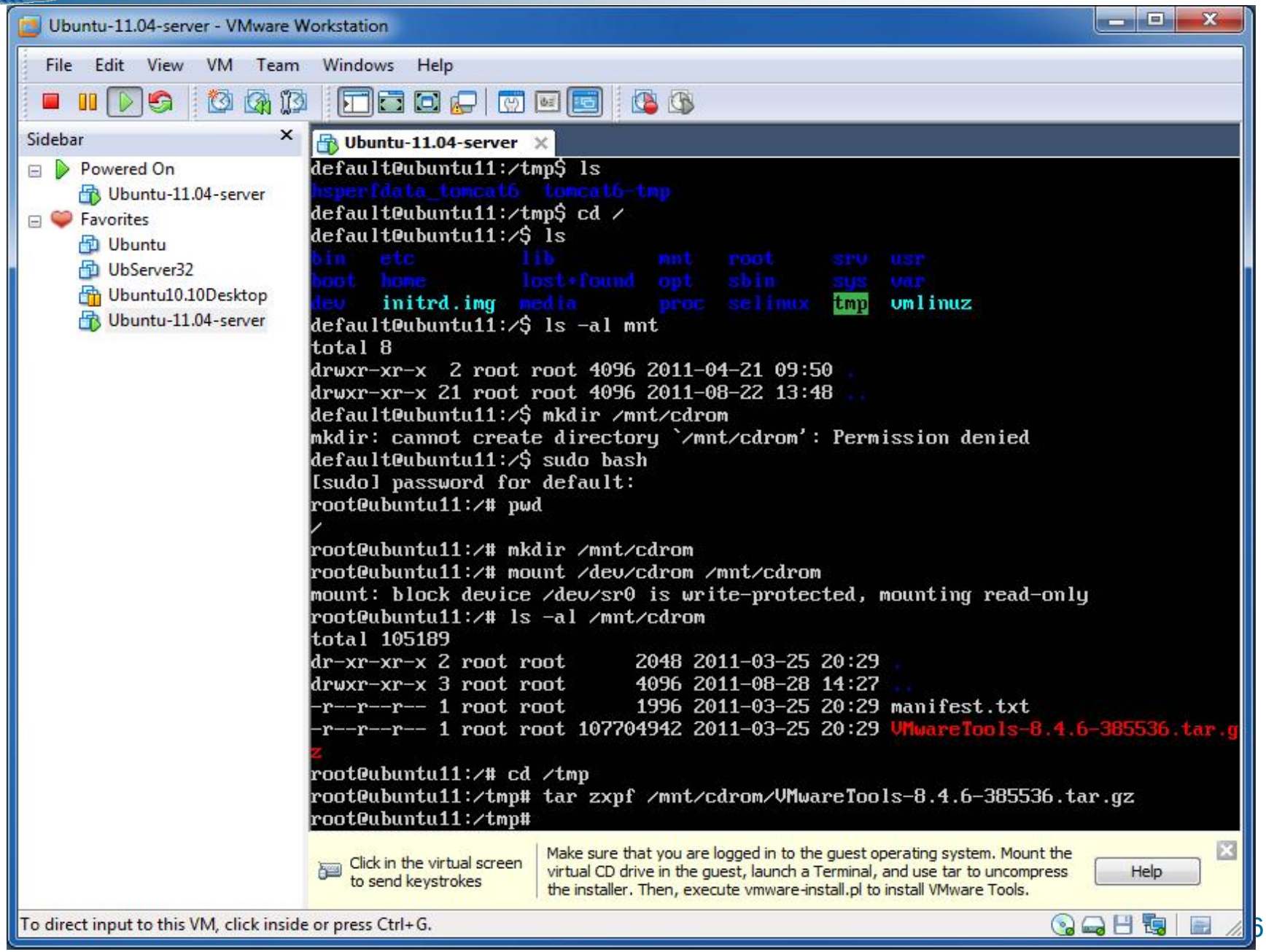
VMM Questions

- What OS does virtual Host run on? Is OS needed?
- What OS does it support as guests?
- Can it support a VM even if instructions are not on physical CPU, e.g., IA-64 VM on IA-32 machine?
- How are resources shared between guest OS's?
  - Oversubscribe CPU, Memory, Storage?
- What tools does it provide for managing VMs?
- Understand pricing models
- Documentation level and quality

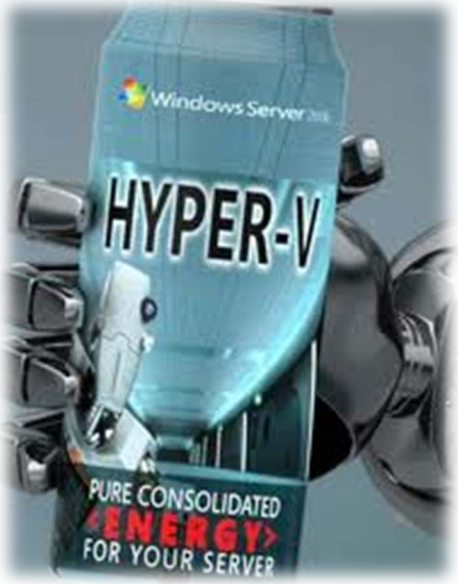
VMWare (EMC)

- Desktop – runs in a host OS
- Workstation (1999) – runs on PC Free
- Fusion – runs on Intel Mac OS X
- Player – run VM's Free
- Server (bare metal hypervisors)
- ESX – service console
- ESXi – busybox - free stripped-down Unix tools in single executable
- vCenter Converter
- ACE distribute virtual desktops to networked client PCs
- vMotion – move running VM's
- vSphere – cloud manager Free
- vTools – integration, cut & paste Free

VMWare Workstation



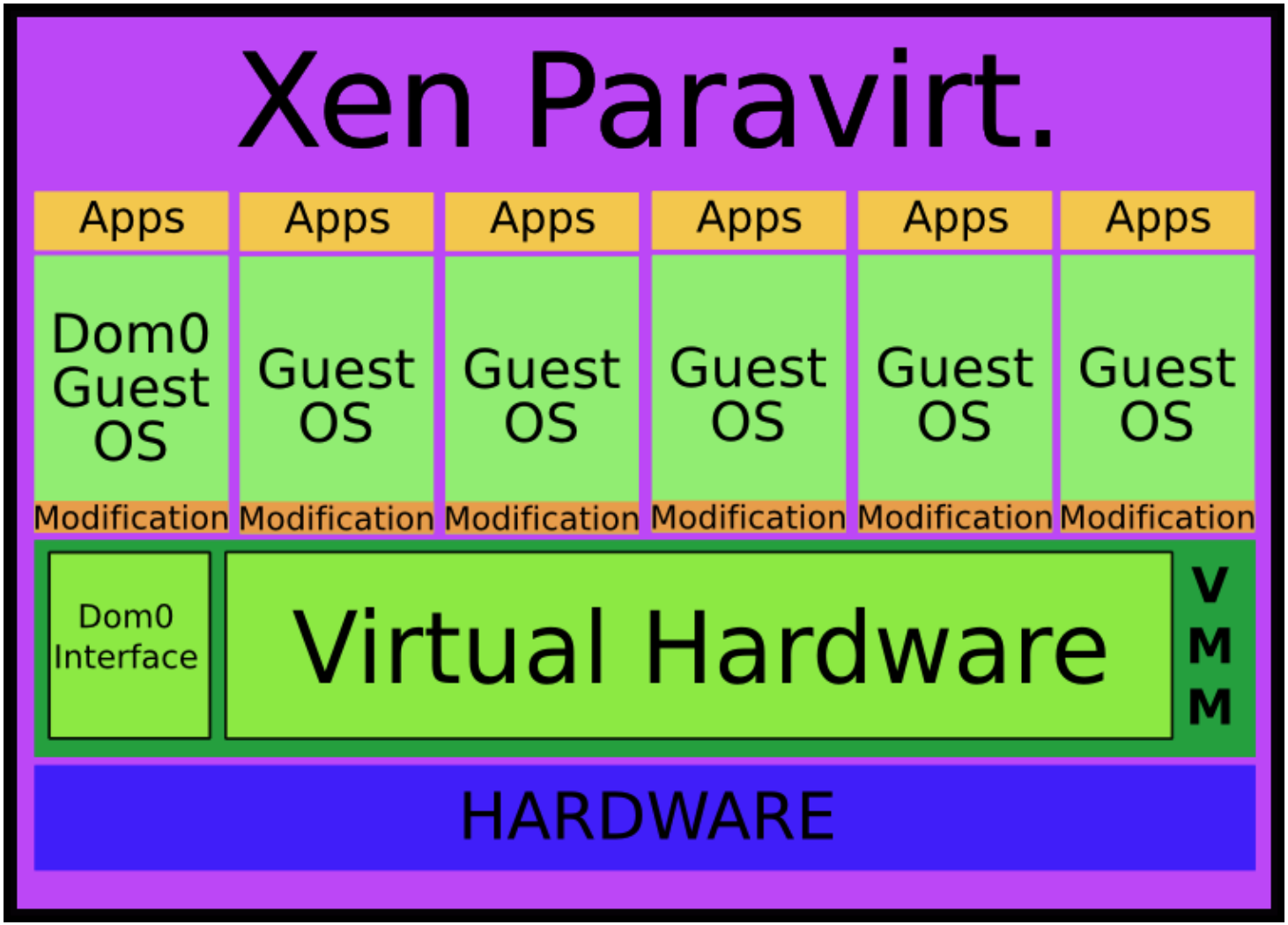
Microsoft Hyper-V



- Windows Server Virtualization
- VMM runs directly on hardware
- Host CPU: x64 + IVT or AMD-V
- Guest OS: Windows, SUSE, Linux (?)
- Two varients
  - Stand alone Hyper-V Server 2012
    - Limited Windows services, CLI only
  - Installable role in Server 2012
    - Parent partition manages child VMs
    - Another Server 2012 can manage it

XEN

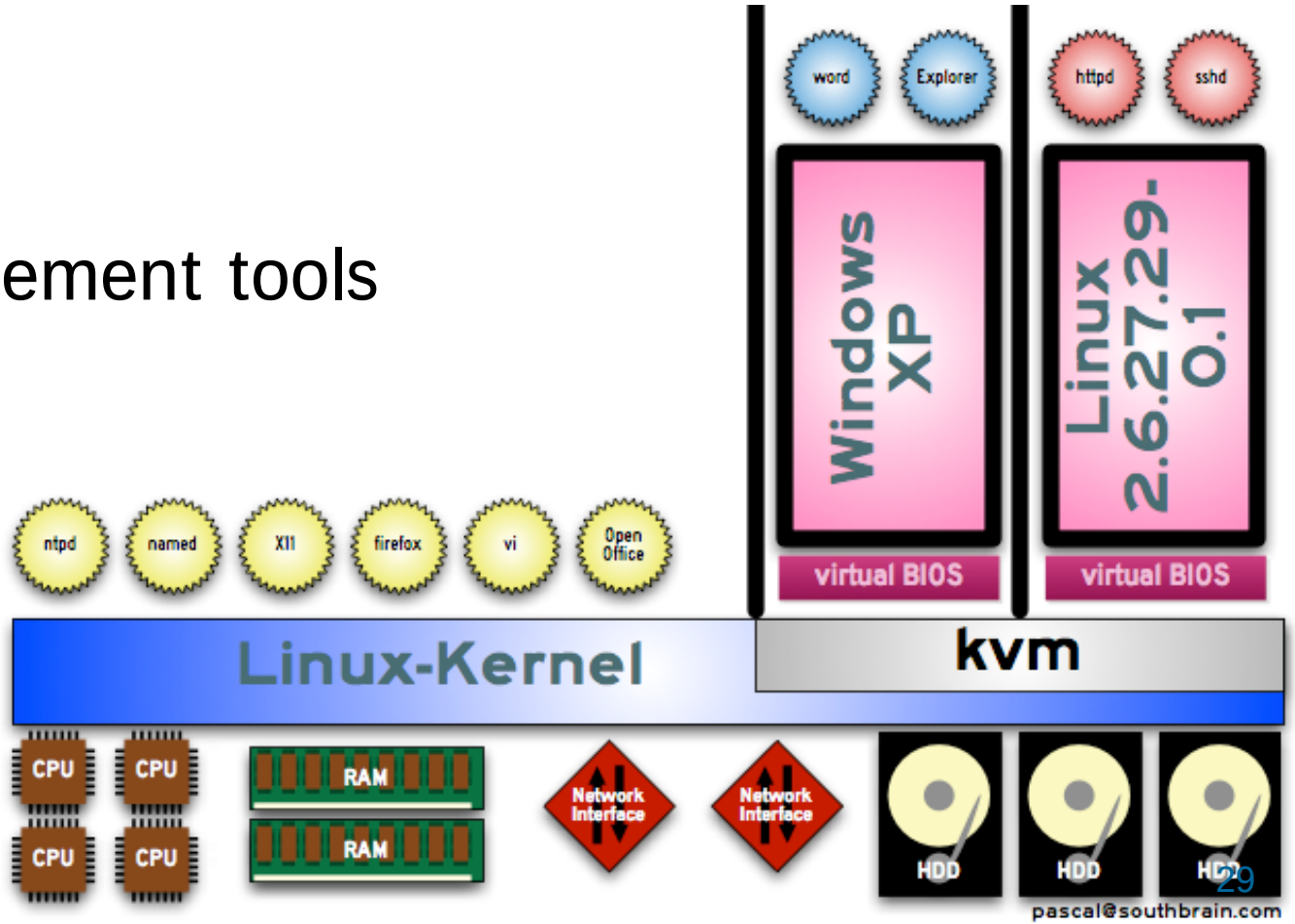
- Open Source - Free
- Dom0 OS (Linux, NetBSD, Solaris) starts other VMs



Ring Zero

KernelVirtualMachine

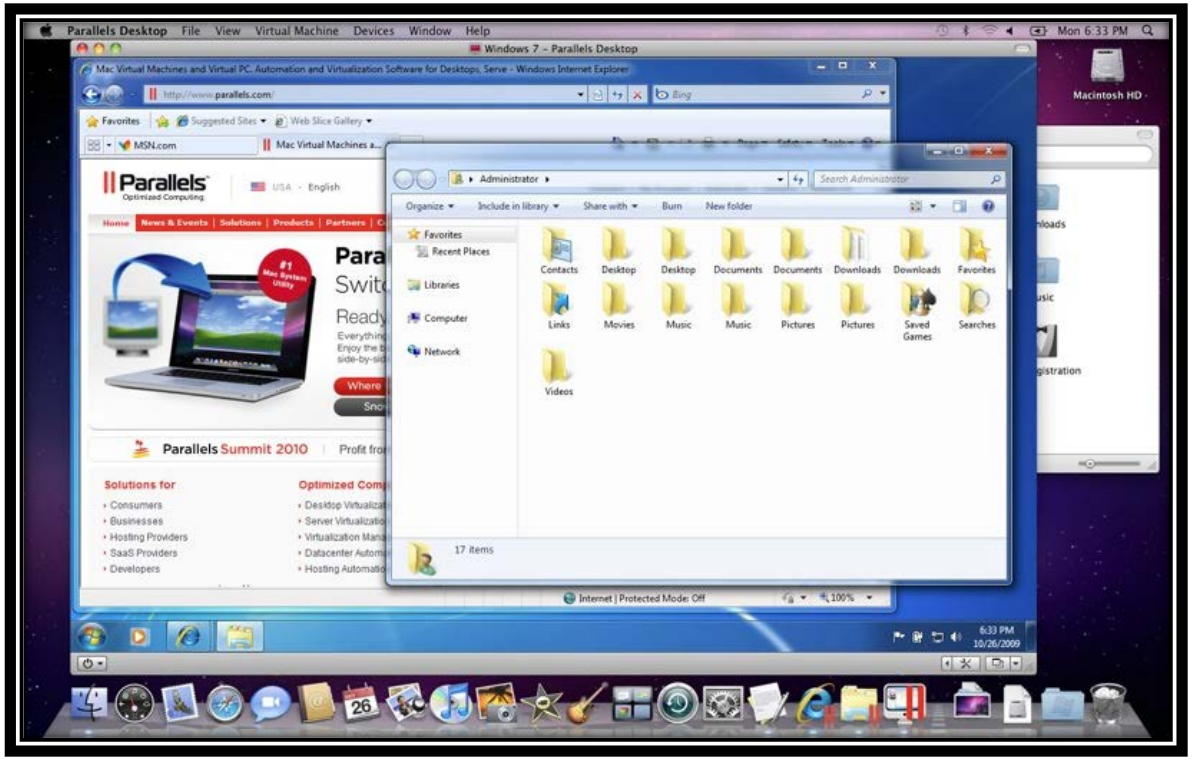
- Linux kernel virtualization infrastructure
- Guests – Windows, Linux, Solaris, DOS, Plan 9
- Native virtualization on x86 CPU's w/
  - Intel VT
  - AMD-V
- GUI management tools



pascal@southbrain.com

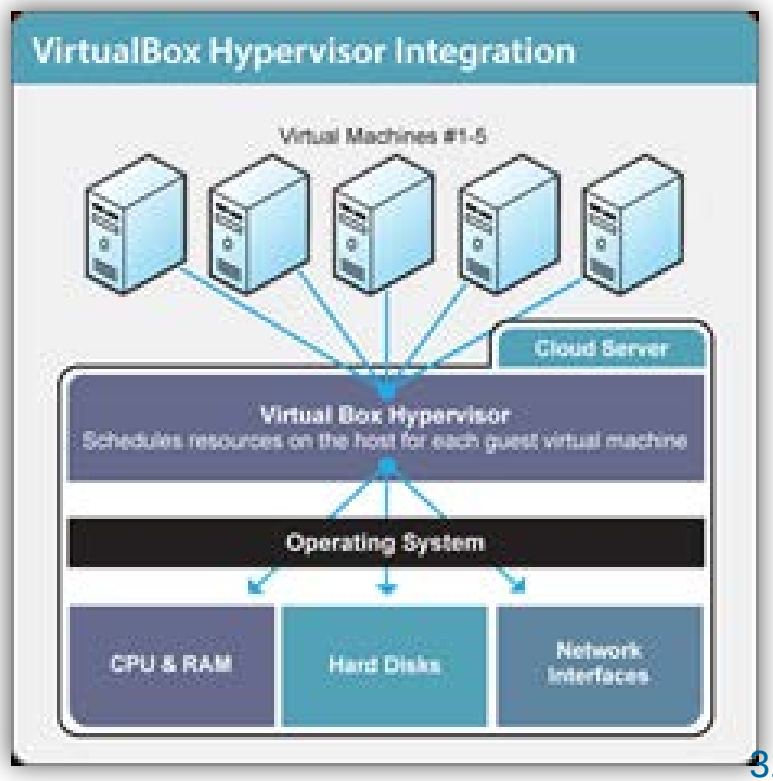
Parallels

- Hardware virtualization for Intel-based OS X
- Supports Windows, Linux, OS X guests
- 32/64-bit support
- Commercial license ~$100



~~Sun~~ Oracle VirtualBox

- Supports - x86 and AMD64/Intel64
- Hosts - Windows, Linux, Macintosh, and Solaris
- Guests – Windows, Linux, Solaris, BSD, OS X Limited
- Software emulation supports 32-bit guests
- Hardware-assisted emulation supports Intel's VT-x and AMD's AMD-V



Mac OS X EULA does not permit the OS to run on non-Apple hardware, enforced within the operating system by calls to the Apple System Management Controller (SMC) in all Apple machines, which verifies the authenticity of the hardware

Virtual Machines *

Product	Host OS	Guest OS
KVM	Linux	Linux Solaris Windows
Parallels	OS X	Linux Solaris Windows
VirtualBox	Linux, Solaris Windows	Linux Solaris Windows
Windows VirtualPC	Windows 7	XP Vista 7
VMWare •Workstation •Player •ESXi	Windows Linux	Windows Linux
XEN	Linux Solaris NetBSD	Linux Solaris XP 2003 Server

* Standard disclaimer applies, not an endorsement, your mileage may vary.

Full VMM vs. Thin Hypervisor

- Create full system abstraction and isolation for guest
- Emulation of I/O devices
  - Disks, NIC's, BIOS
- Easily detected
- Usage:
  - Development systems
  - Malware analysis
  - Virtual botnet

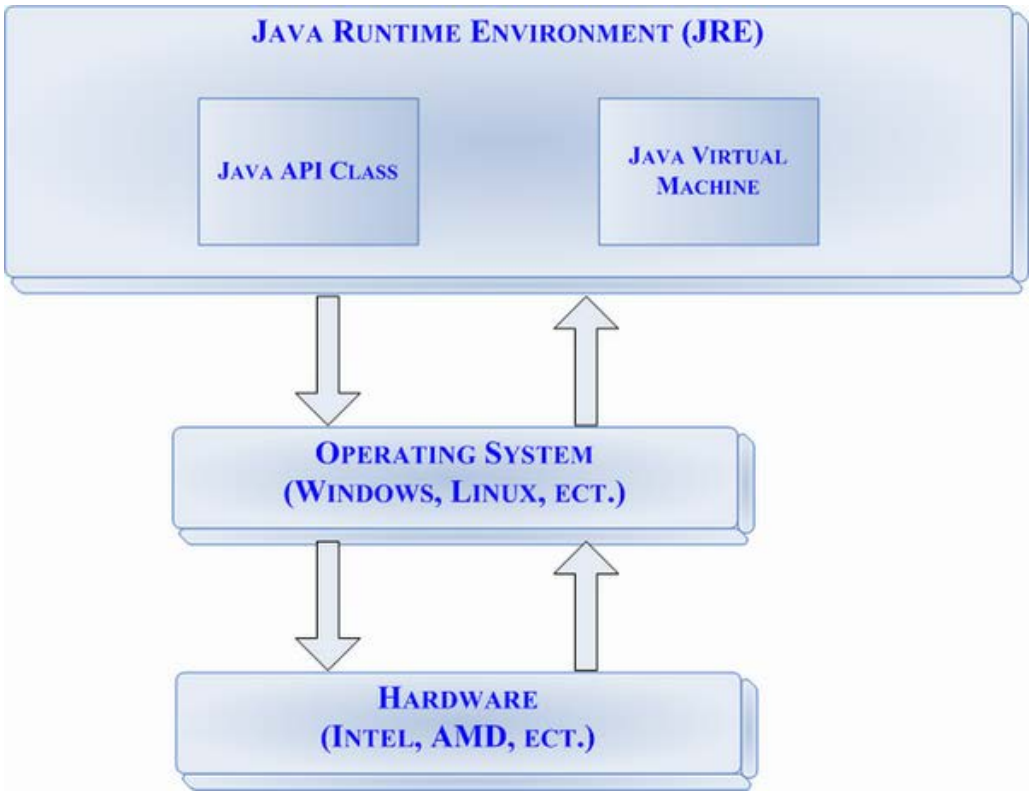
- Transparently control target machine
- Hardware based (VT-x)
- Native I/O

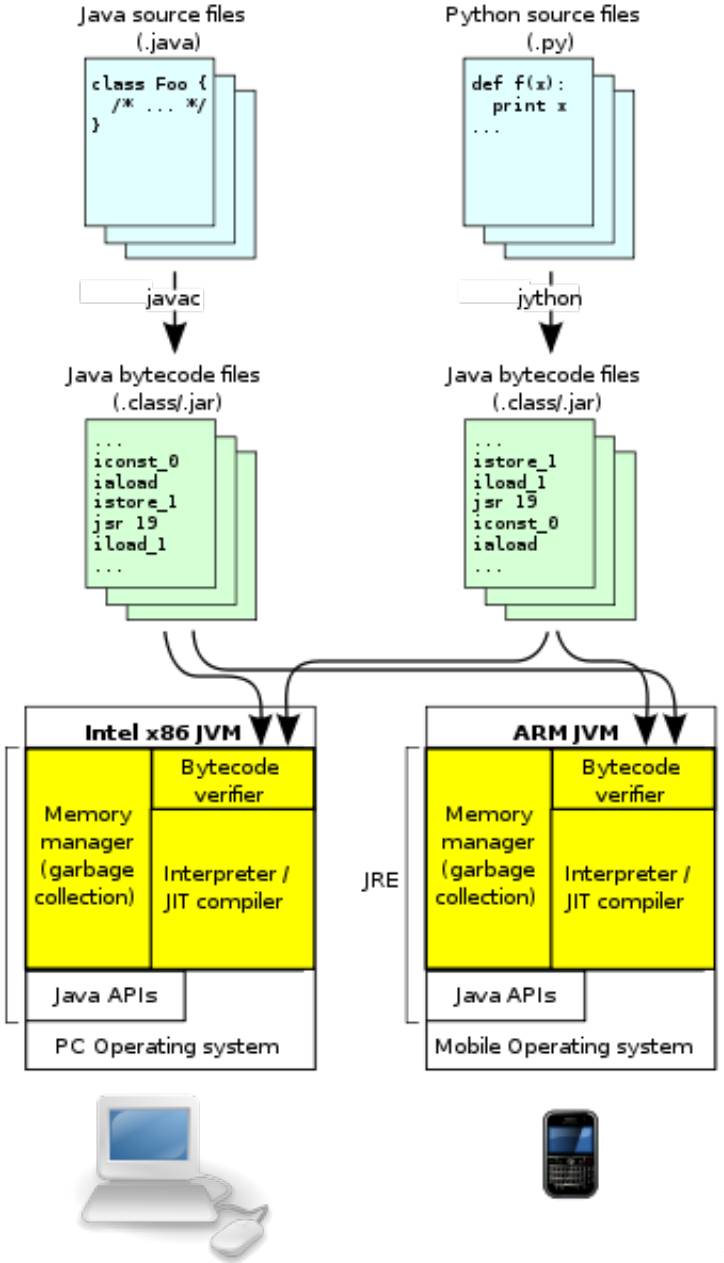
- Very hard to detect
- Usage:
  - Anti-DRM
  - Steath malware

Question

What Virtual Machine is claimed to be on 4.5 billion devices?

Java VM


JAVA RUNTIME ENVIRONMENT (JRE)
JAVA API CLASS
JAVA VIRTUAL MACHINE
OPERATING SYSTEM (WINDOWS, LINUX, ECT.)
HARDWARE (INTEL, AMD, ECT.)


Java source files (.java)
class Foo { /* ... */ }
javac
Python source files (.py)
def f(x): print x
...
jython
Java bytecode files (.class/.jar)
... iconst_0 iaload istore_1 jsr 19 iload_1 ...
Java bytecode files (.class/.jar)
... istore_1 iload_1 jsr 19 iconst_0 iaload ...
Intel x86 JVM
Memory manager (garbage collection)
Bytecode verifier
Interpreter / JIT compiler
Java APIs
PC Operating system
JRE
ARM JVM
Memory manager (garbage collection)
Bytecode verifier
Interpreter / JIT compiler
Java APIs
Mobile Operating system

JRE Alerts

- These vulnerabilities may be remotely exploitable without authentication, i.e., they may be exploited over a network without the need for a username and password.
- To be successfully exploited, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that leverages this vulnerability.
- Successful exploits can impact the availability, integrity, and confidentiality of the user's system.

Application Virtual Machines

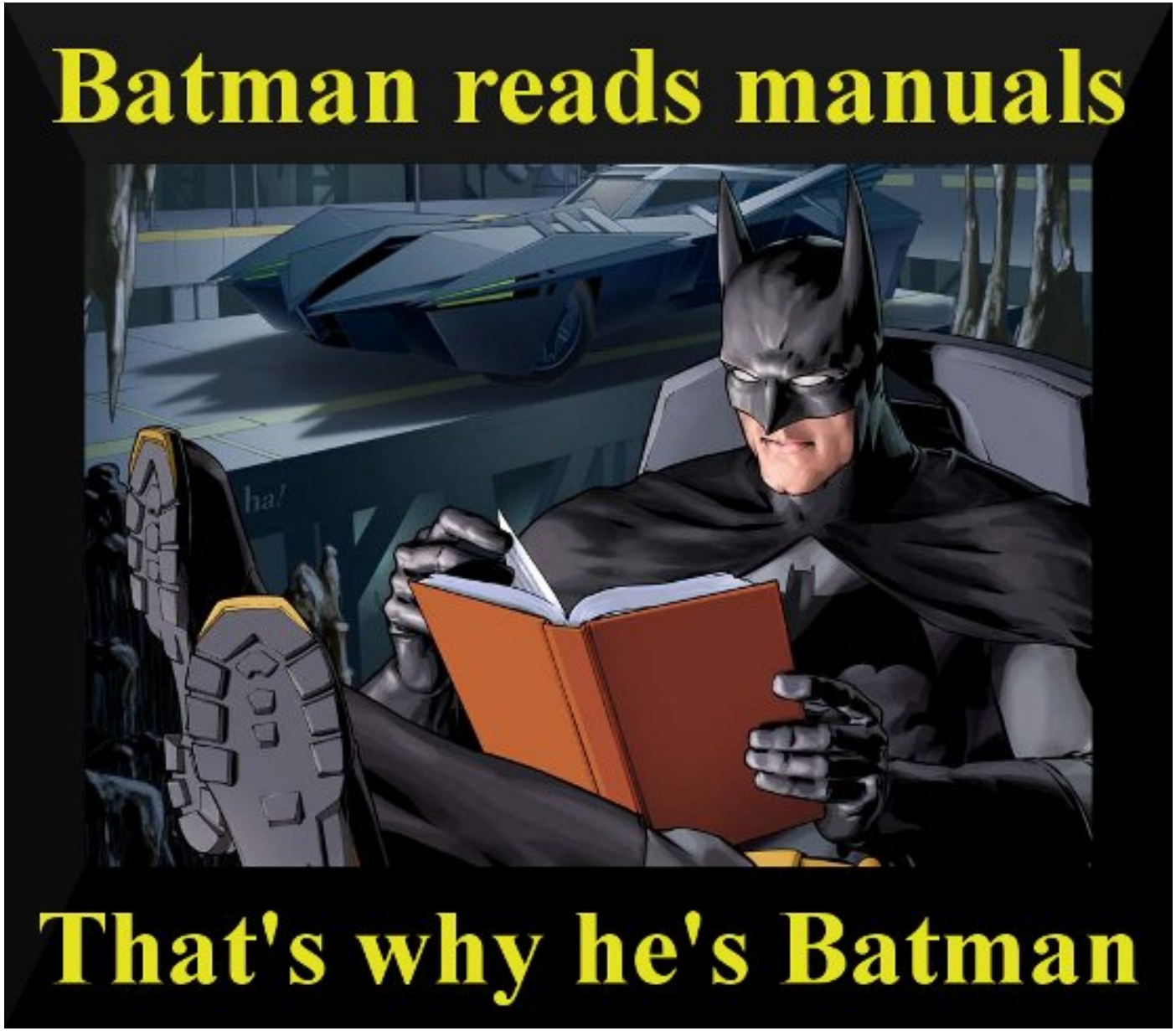
- Microsoft's .NET Framework
- Programs written for it execute in a software environment (contrasted to a hardware environment)
- Called the Common Language Runtime (CLR), it is an **application virtual machine** that provides services such as:
  - security,
  - memory management
  - exception handling.
- The class library + CLR = .NET Framework.

Virtualization

We've covered the virtual landscape

- For Windows users VMware Player easiest
- 1-2GB memory
- 1-2GHz CPU
- 150MB disk space
- www.vmware.com - support & downloads
- Read VMware Player Release Notes
- Read Getting Started Guide
- Read Guest Operating System Installation Guide
- Check VMware Compatibility Guide (Maybe)

RTFM

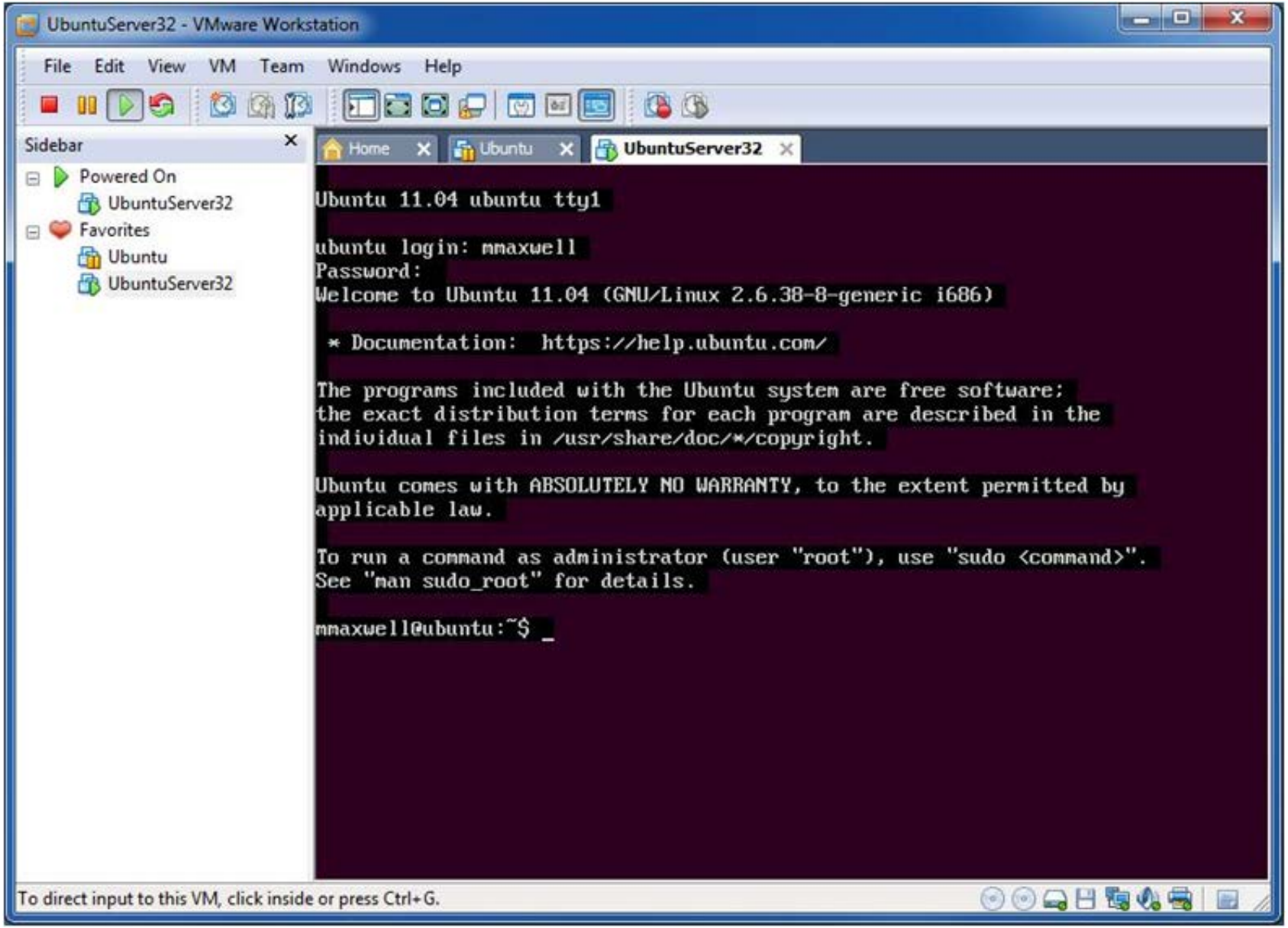


Alternative

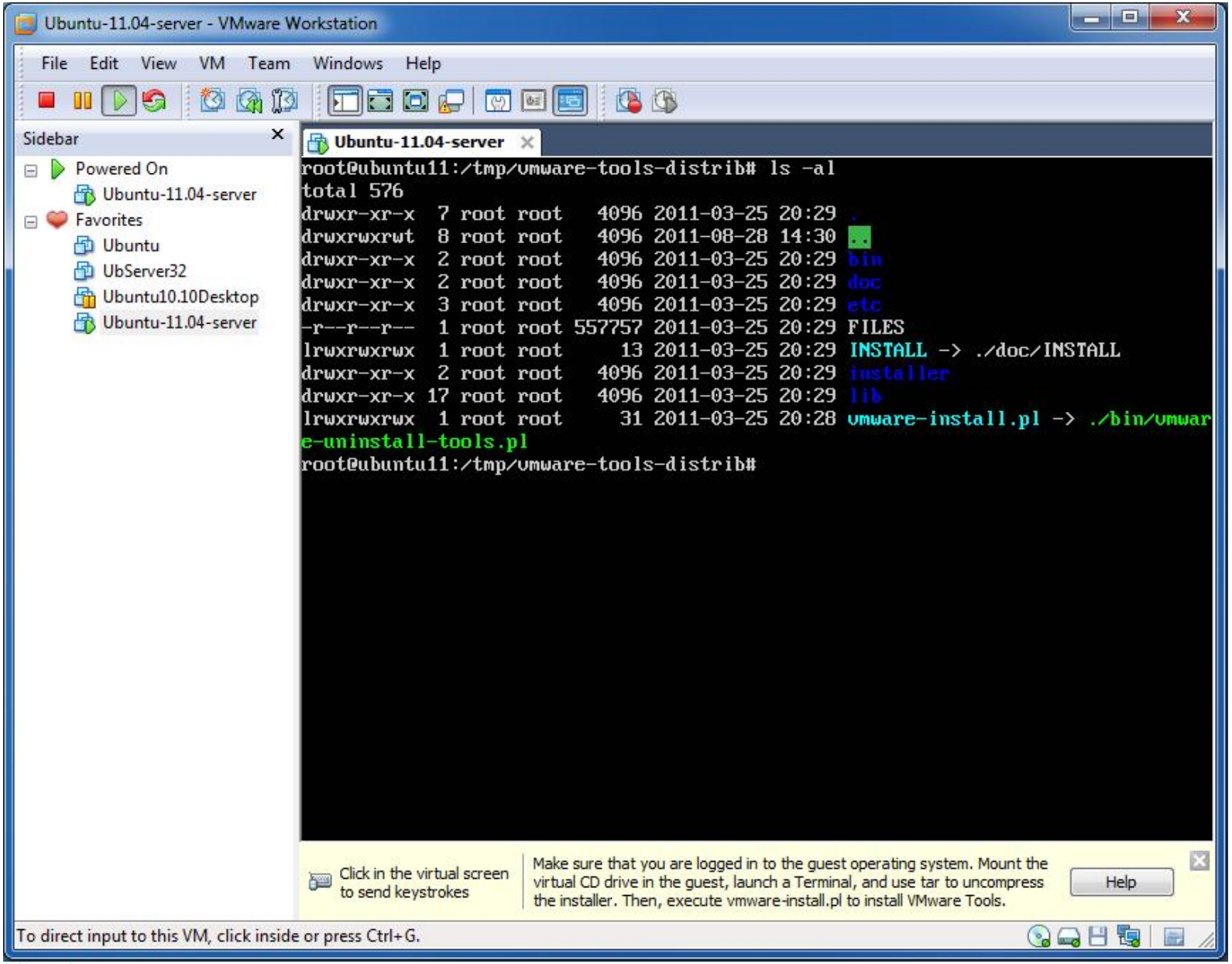
- Install VMware Workstation
- Registration needed to obtain key (Free)
- Browse the OS Appliances (many)(**why??**)

- Instructor's Development System
  - VMware Workstation 7.1.4
  - ASUS P7P55D-E PRO
  - i7 870 @ 2.93 GHz
  - 8 GB DDR3
  - USB 3 & SATA 6Gb/s
  - Host OS – Windows 7 Professional 64-bit
  - 1TB + .5TB SATA

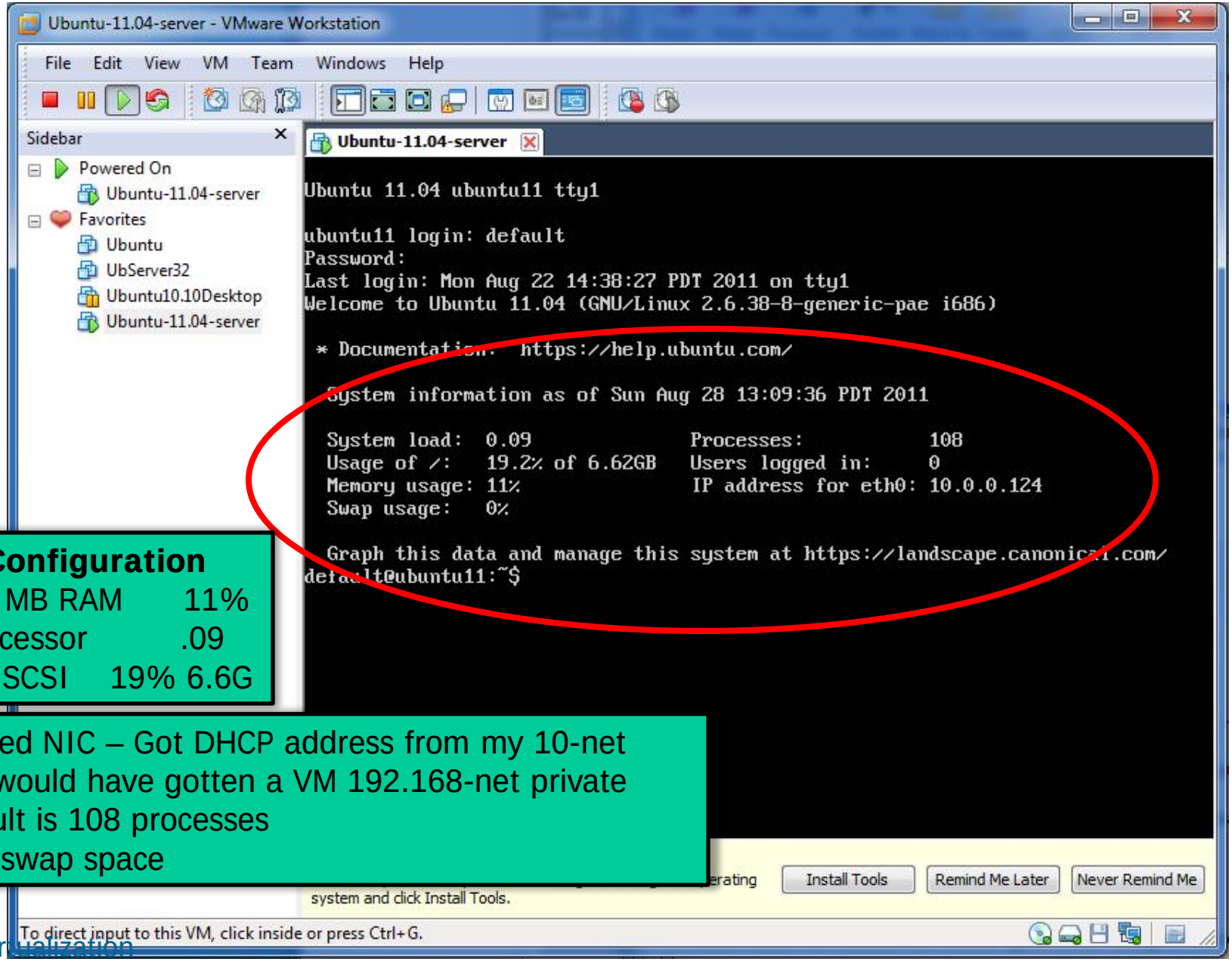
Ubuntu Server 11.04 32-bit



Ubuntu Server 11.04 64-bit



Ubuntu Server 11.04 64-bit



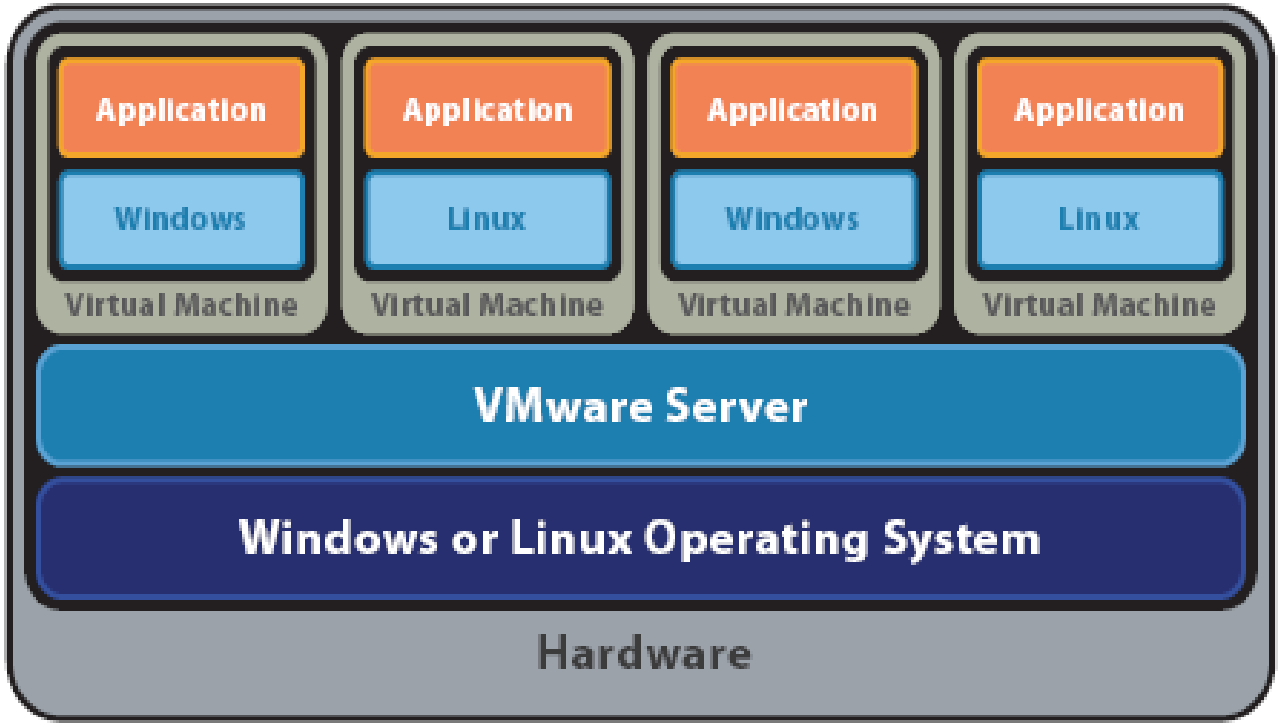
VM Configuration

1024 MB RAM	11%	
1 Processor	.09	
8 GB SCSI	19%	6.6G

Bridged NIC – Got DHCP address from my 10-net
NAT would have gotten a VM 192.168-net private
Default is 108 processes
1.4G swap space

Performance Cost

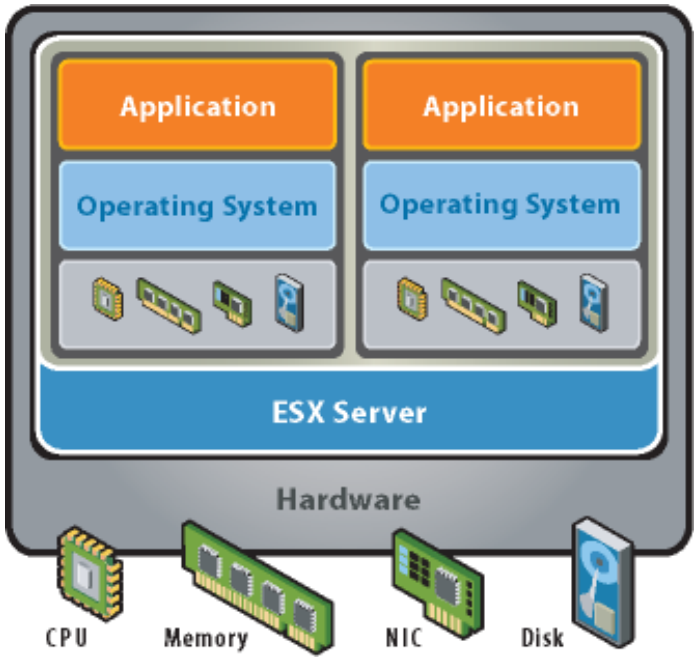
- Overhead of a full general-purpose operating system (host OS) between the virtual machines and the physical hardware results in performance typically 70-90-% of native OS

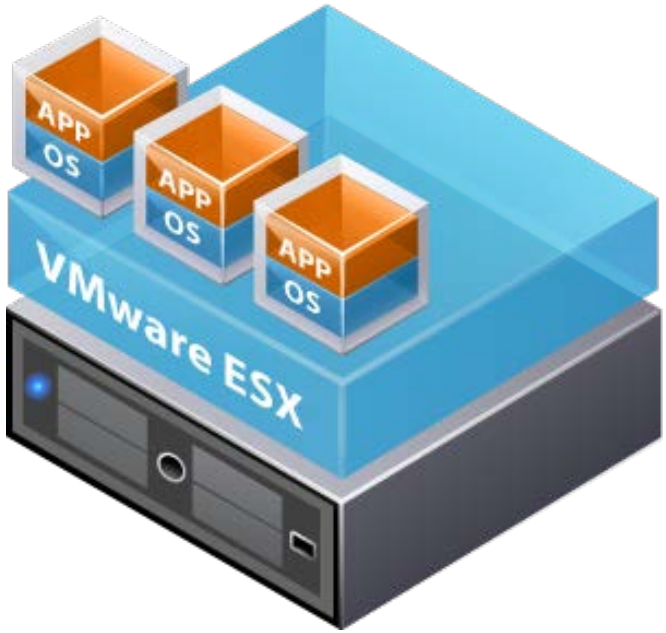


Performance Cost

ESXi & ESX Bare metal hypervisor

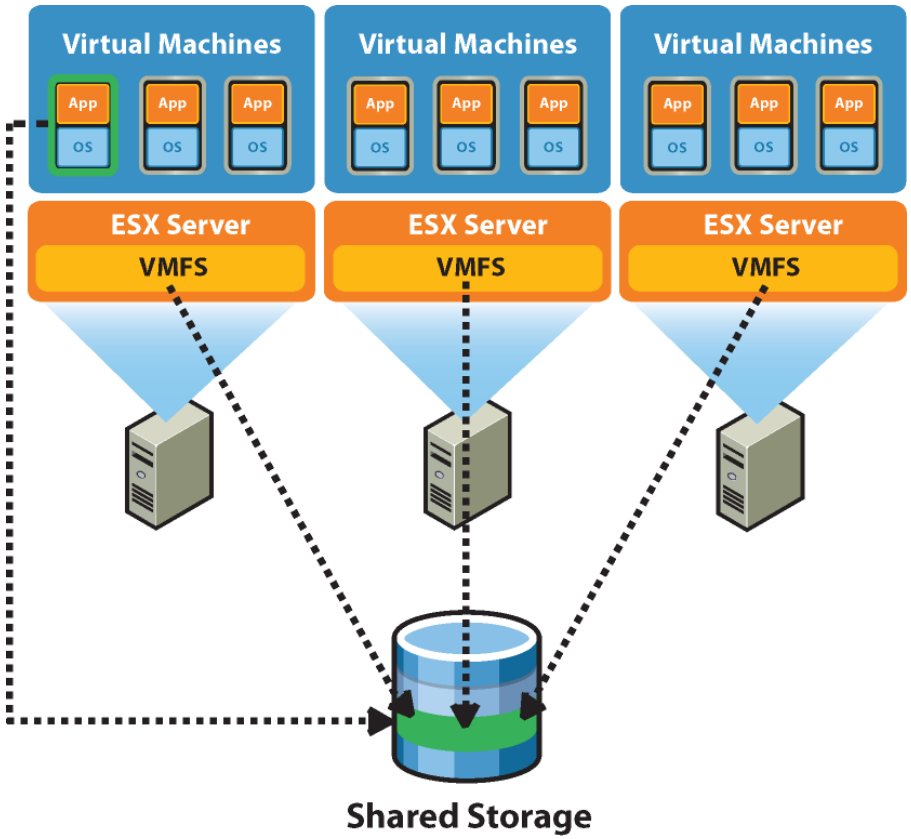
- No overhead from a full host operating system
- Performance is 83-98% of native
- Small overhead from VMKernel virtualization layer





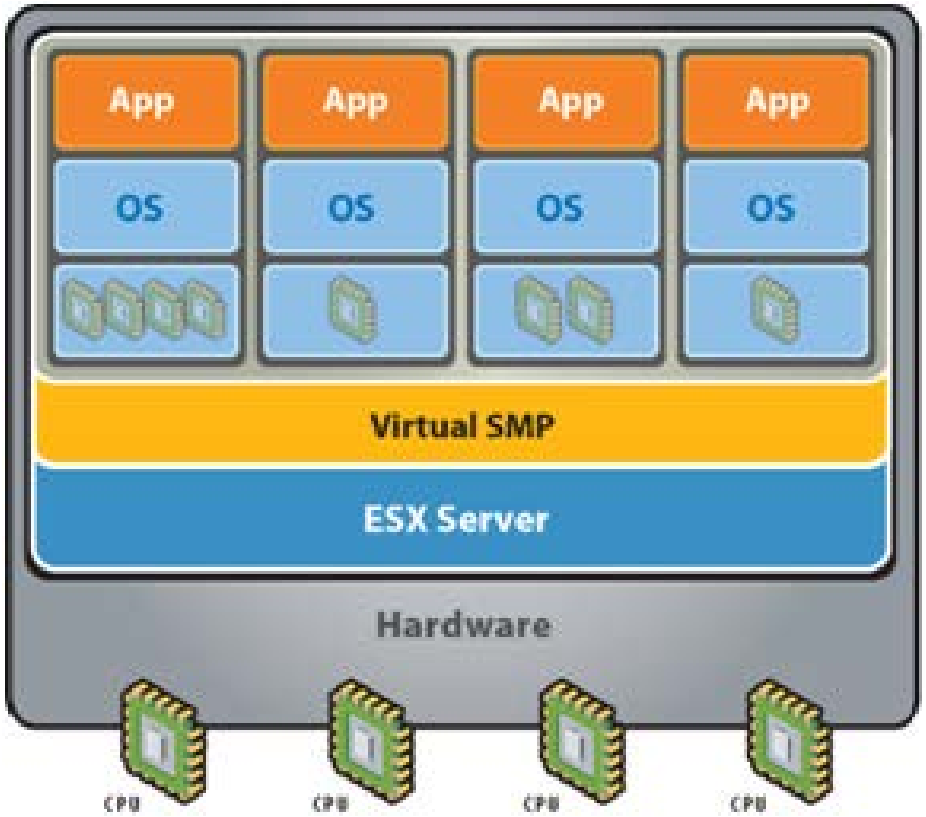
VMFS

- VMFS: VMware's clustering file system allows multiple hosts to read and write from the same storage location concurrently.
- Has adaptive block sizing Uses large block sizes favored by virtual disk I/O and uses sub-block allocation for small files and directories.
- On-disk disk file locking ensures that same VM is not powered on by multiple servers at the same time.



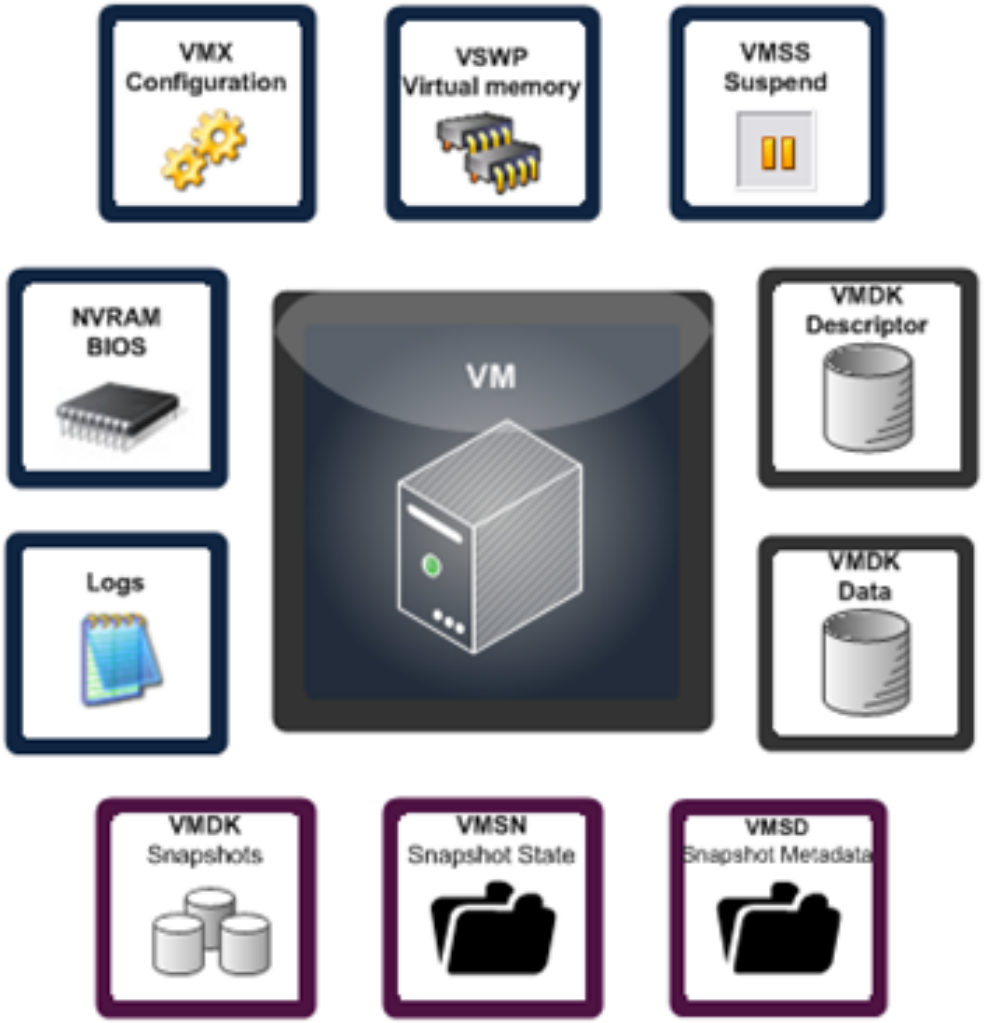
vSMP

- vSMP - you can assign more than one virtual CPU to a virtual machine.
- Up to 4 virtual CPUs can be assigned to any virtual machines.
- Caveat: hypervisor's CPU scheduler must find simultaneous cores available equal to the number assigned to the VM.



Virtual Machine Files

- A virtual machine is comprised of a number of files that are located in it's home directory.
- You may not see all of the possible file types until the VM is in a certain state; for example the .vswp file is only present when the VM is powered on and the .vmss file is only present when a VM is suspended.



From Development System

Name	Date modified	Type	Size
Ubuntu-11.04-server.nvram	8/29/2011 12:08 AM	VMware virtual m...	9 KB
Ubuntu-11.04-server.vmdk	8/28/2011 1:12 PM	VMware virtual dis...	1,553,472 KB
Ubuntu-11.04-server.vmsd	8/29/2011 12:08 AM	VMware snapshot ...	1 KB
Ubuntu-11.04-server.vmx	8/29/2011 12:08 AM	VMware virtual m...	3 KB
Ubuntu-11.04-server.vmxf	8/22/2011 2:41 PM	VMware team me...	1 KB
Ubuntu-11.04-server-000001.vmdk	8/28/2011 8:45 PM	VMware virtual dis...	1,036,096 KB
Ubuntu-11.04-server-000002.vmdk	8/29/2011 12:08 AM	VMware virtual dis...	35,328 KB
Ubuntu-11.04-server-Snapshot1.vmem	8/28/2011 1:14 PM	VMEM File	1,048,576 KB
Ubuntu-11.04-server-Snapshot1.vmsn	8/28/2011 1:14 PM	VMware virtual m...	26,358 KB
Ubuntu-11.04-server-Snapshot2.vmem	8/28/2011 8:46 PM	VMEM File	1,048,576 KB
Ubuntu-11.04-server-Snapshot2.vmsn	8/28/2011 8:46 PM	VMware virtual m...	26,362 KB
vmware.log	8/29/2011 12:08 AM	Text Document	129 KB
vmware-0.log	8/28/2011 8:49 PM	Text Document	147 KB
vmware-1.log	8/28/2011 1:23 AM	Text Document	130 KB
vmware-2.log	8/22/2011 2:43 PM	Text Document	95 KB

- Note that snapshots of the VM can rapidly consume disk space.

Virtual Machine Files

- **.nvram file** – contains Phoenix BIOS used as part of VM boot process. Similar to a physical server that has a BIOS chip that let's you set hardware configuration options; a VM also has a virtual BIOS that is contained in the NVRAM file.
- The BIOS can be accessed when a VM first starts up by pressing the F2 key, whatever changes are made to the hardware configuration of the VM are then saved in the NVRAM file.
- File is in binary format and if deleted will be automatically re-created when VM is powered on.

Virtual Machine Files

- **.vmx file** – contains the VM configuration information and hardware settings. Text file contains information regarding specific hardware configuration (i.e. RAM size, NIC info, hard drive info and serial/parallel port info) advanced power and resource settings, VMware tools options and power management options.
- You can edit this file directly to make changes to a VM's configuration
  - But it is not recommended

Virtual Machine Files

- **.vswp file** - When VM is powered on a memory swap file is created to swap physical host memory if ESX host exhausts all of its physical memory due to overcommitment
- Always created, used only if needed (slowish)
- Size = memory allocated to VM
  - less any memory reservations (default is 0)
- VM will not power on if not enough space to create file (monitor disk space free/used)
- Deleted when VM is powered off or suspended

Virtual Machine Files

- **.vmss file** – Preserves memory contents of VM when it is suspended for restarting.
- Same size as assigned VM RAM
- File contents written back to physical memory of host server when VM is brought out of suspended
- File automatically deleted only when VM is powered off (an OS reboot won't work).
- Reused if a previous suspend file exists and VM is suspended
- Deleting file while VM is suspended will cause VM to start normally and not from a suspended state.

Virtual Machine Files

- **vmsd file** – Stores snapshot metadata about each snapshot active on a VM
- Initial size is 0 bytes until a snapshot is created
- Updated when snapshots are created or deleted
- One file used for all snapshots
- Name of each snapshots vmdk & vmsn file
- Display name, description, and snapshot UID
- Retains deleted snapshot information but increments the snapshot uid for new snapshots

Virtual Machine Files

- **.vmsn file** - Stores the state of a VM when a snapshot is taken.
- Each snapshot taken creates a .vmsn file
- Automatically deleted when snapshot is deleted
- File size larger if option selected to include VM's memory state with snapshot
- **vmxf** file - used by Workstation for VM teaming
- Multiple VMs can be assigned to a team
- Team can be powered on/off or suspended and resumed as a single object

Virtual Machine Files

- **.log file** – current log file always vmware.log
- Up to 6 older log files retained
- Incrementing number added to name
- New log file created either
  - when a VM is powered off and back on or
  - if log file reaches the max. defined size limit
- VM advanced configuration parameters
  - Number of of log files (retained log.keepOld)
  - maximum size limits (log.rotateSize)
- Useful for troubleshooting purposes

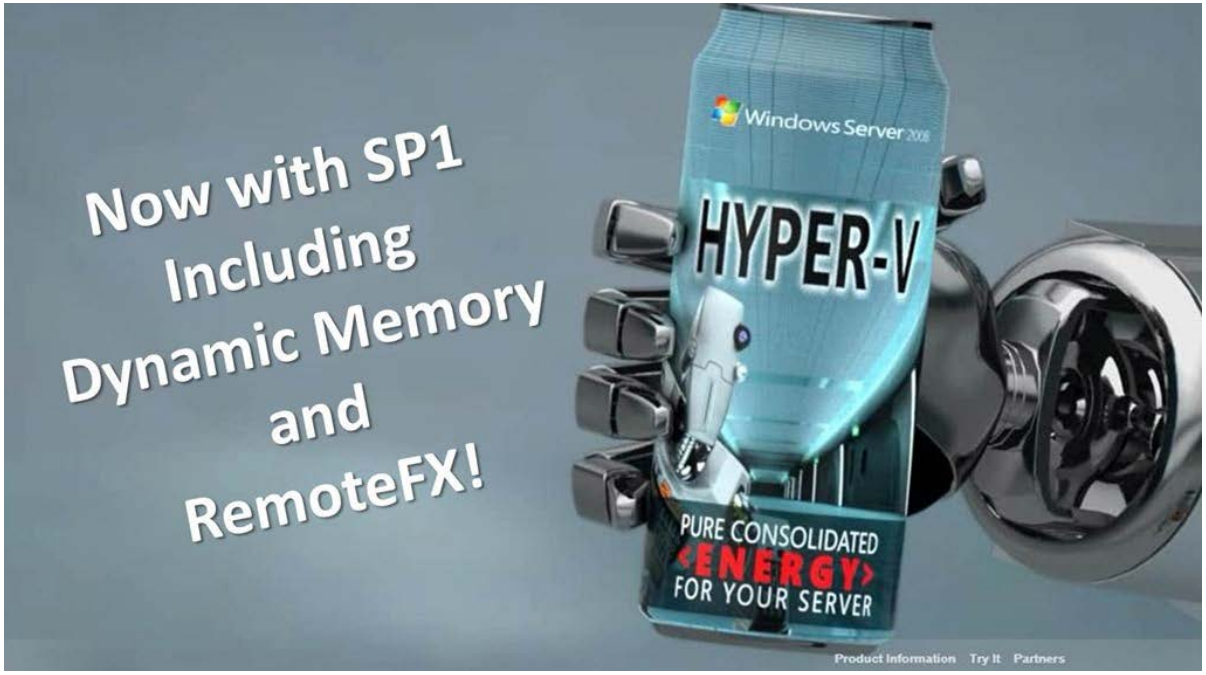
Risks for Virtualized Environments

- Vulnerabilities in Physical Environment Apply in Virtual Environment
- Hypervisor Creates New Attack Surface
- Increased Complexity of Virtualized Systems and Networks
- More Than One Function per Physical System
- Mixing VMs of Different Trust Levels
- Lack of Separation of Duties
- Dormant Virtual Machines
- VM Images and Snapshots
- Immaturity of Monitoring Solutions
- Information Leakage between Virtual Network Segments
- Information Leakage between Virtual Components

Reading

- Payment Card Industry Data Security Standards PCI DSS Virtualization Guidelines

- Guide to Security for Full Virtualization Technologies



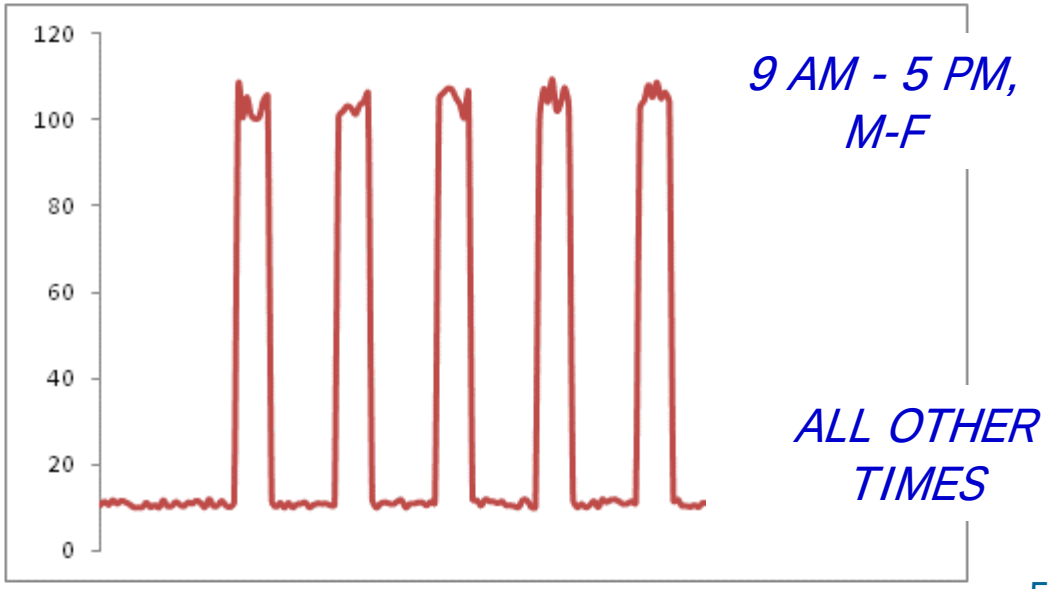
Utilization

- Virtualization is one approach……

- You offer on-line real time stock market data

- Why pay for capacity weekends, overnight?

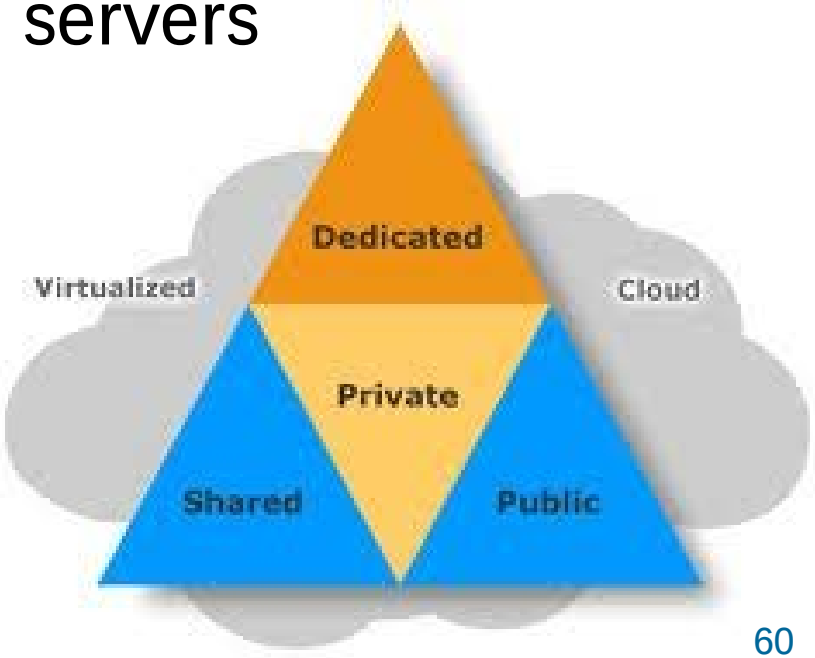
Server Access



Cloud Services

- Host in Amazon's EC2 Elastic Compute Cloud
- Let Amazon worry about the hardware!
- Provision new servers every day
- Deprovision them every night
- Pay just $0.10* per server per hour

  * more for higher capacity servers



Cloud Computing

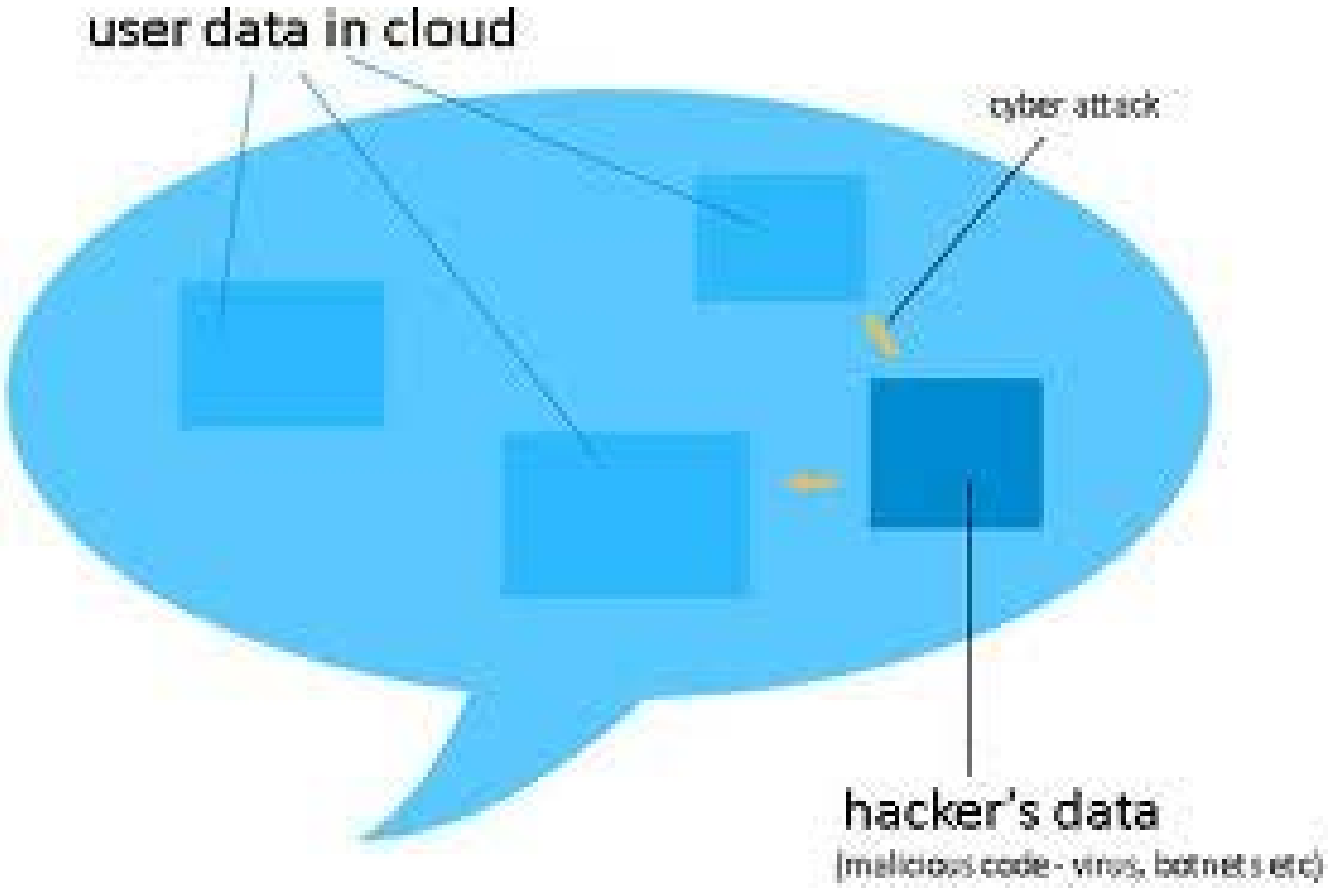
- **Cloud computing takes virtualization to the next step**
- You don't have to own the hardware
- You "rent" it as needed from a cloud
- There are public clouds
  - e.g. Amazon EC2, and now many others (Microsoft, IBM, Sun, and others …)
- A company can create a private one
  - With more control over security, etc.

Cloud Computing

- Cost control over variable demands
  - Especially for startups
- More flexibility
- Fast provisioning
  - Scale up and down as needed
- Stick to core competency
  - Still takes system administrators

Cloud Security

- Cloud Attack Surfaces

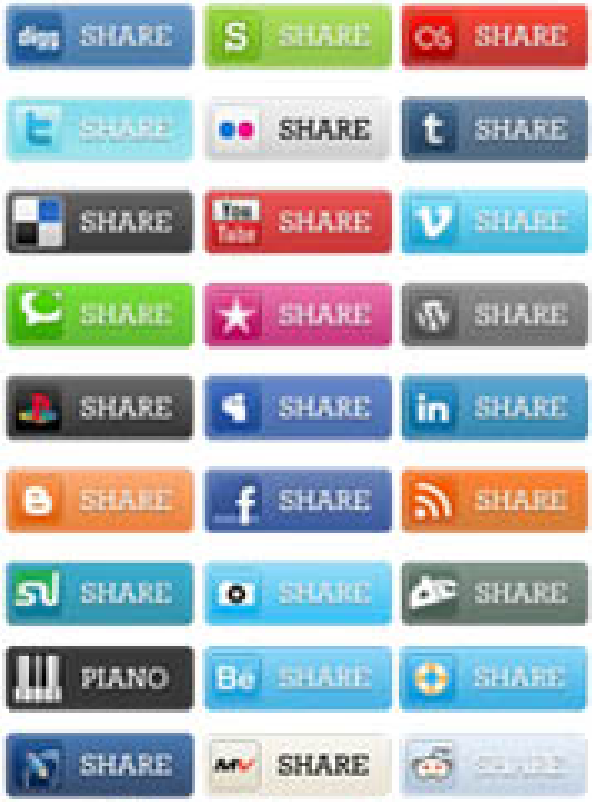


Dropbox

Review

- Network virtualization distinguishes logical from physical networking
- Network devices operate across these logical planes:
  - Data
  - Control
  - Management
- SAN Storage Area Network (e.g. virtualized)
- A virtual machine is a Guest of the hypervisor
- Cloud environments may be deployed over infrastructures
  - Private
  - Public
  - Hybrid

-eot-



AIM
BallHype
Faves
Diigo
Fark
Google
LinkedIn
Mixx
Netvouz
Segnalo

myAOL
Bebo
Yahoo Buzz
Email
FeedMeLinks
Kaboodle
Live
Multiply
Newsvine
Simpy

Ask
BlinkList
Delicious
Facebook
FriendFeed
kIRTSY
Magnolia
MyWeb
Propeller
Sk*rt

Backflip
Blogmar
Digg
Favorite
Furl
Link-a-G
Mister W
MySpac
Reddit
Slashdo