Distributed Systems COMP 212

Lecture 26

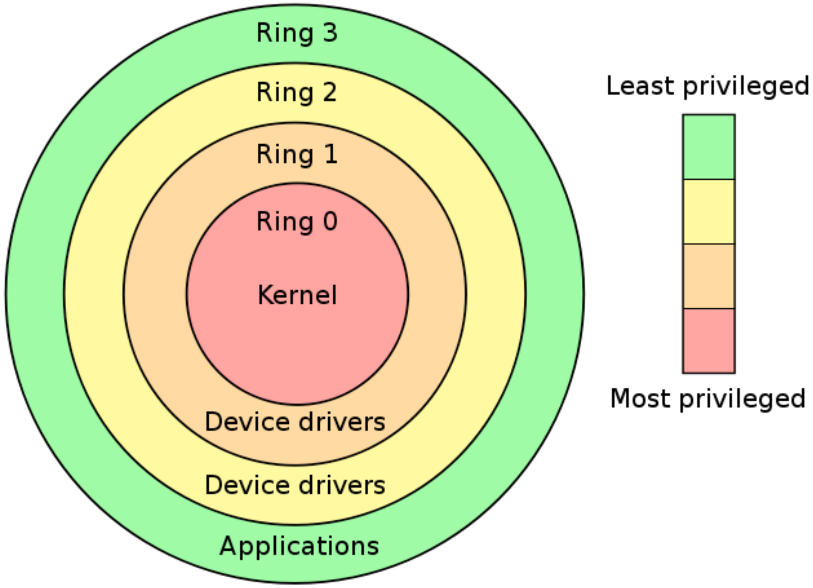
Othon Michail

UNIVERSITY OF LIVERPOOL

Virtualisation & Cloud Computing

Protection rings

- It’s all about protection rings in modern processors
- Hardware mechanism to protect data and functionality from faults and malicious behaviour

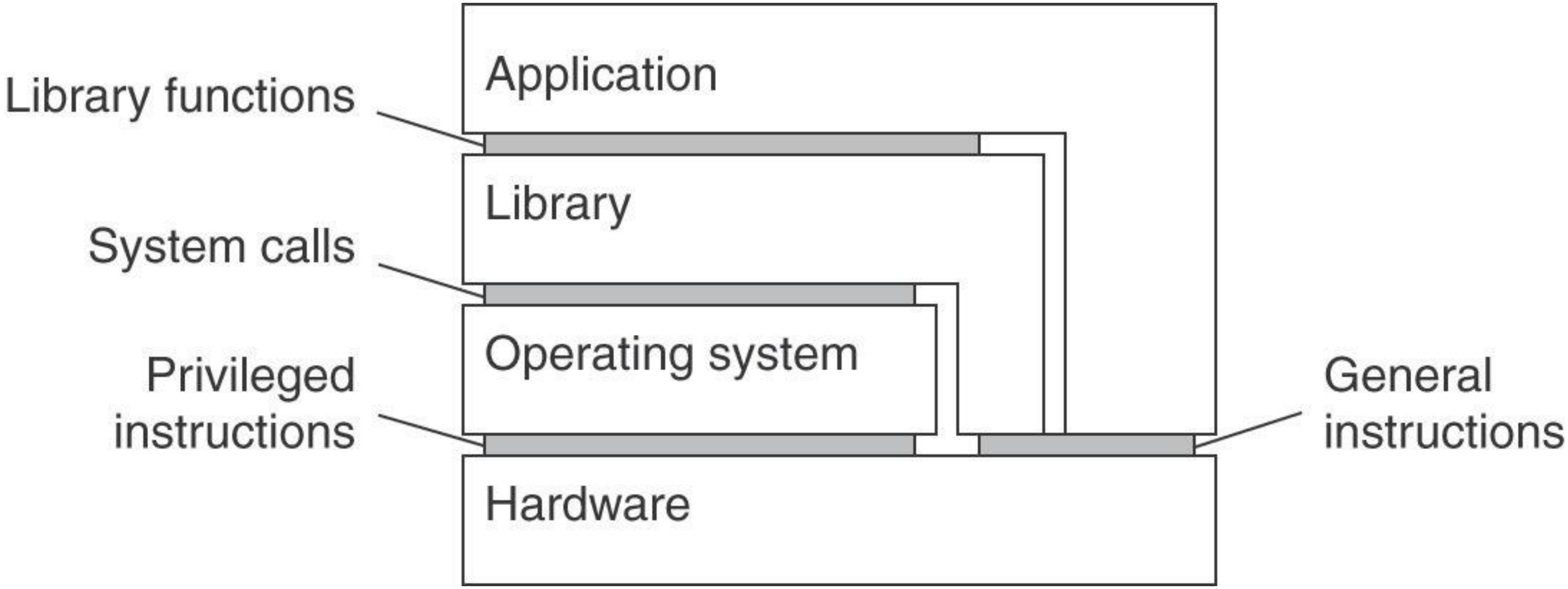


- x86 processor can function in one of 4 modes
- Modern operating systems only use Ring 0 and Ring 3

x86 protection rings
http://upload.wikimedia.org/wikipedia/en/2/2f/Priv_rings.svg

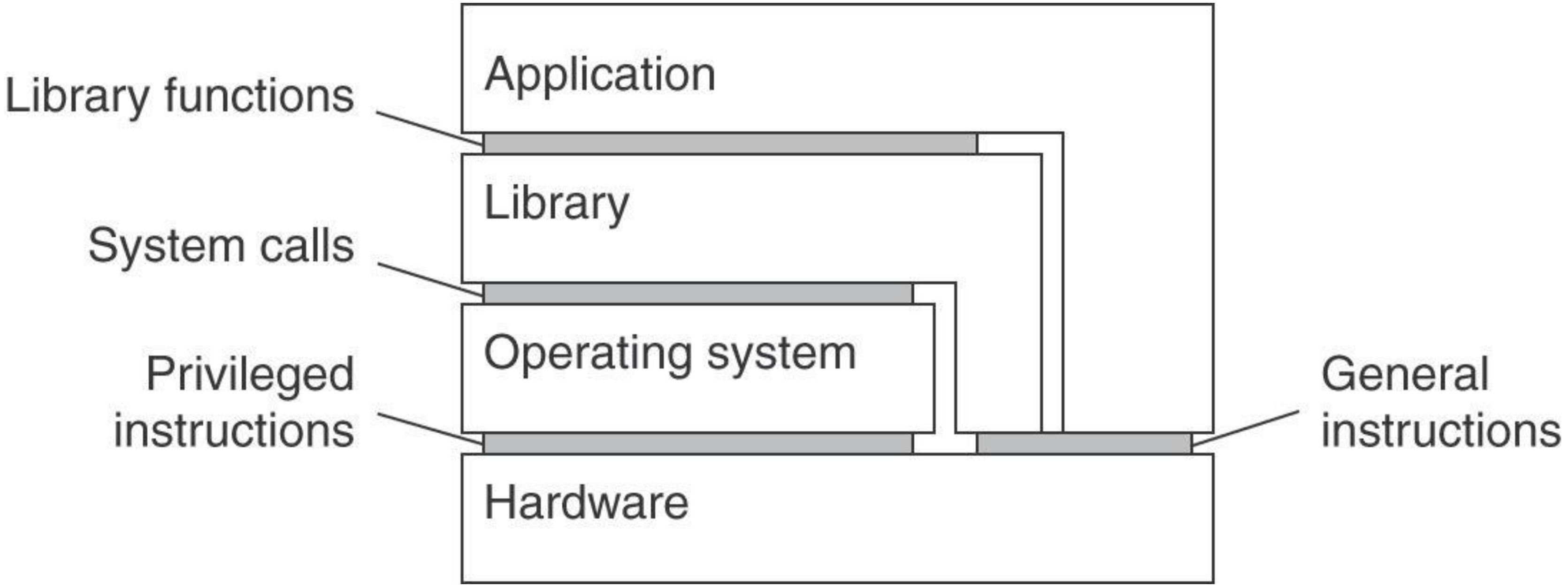
Interfaces at different levels (1)

- Hardware ↔ software general machine instructions
  - that can be invoked by any program.
- Hardware ↔ software privileged machine instructions
  - that can be invoked only by privileged programs, such as an operating system.



Interfaces at different levels (2)

- System calls offered by an operating system
  - A programmatic way in which a program requests a service from the kernel of the OS it is executed on (e.g. accessing a disk drive).
- Library calls
  - generally forming what is known as an application programming interface (API)



Virtualization in a Nutshell

- Implementation of a virtual, instead of a physical version of a server, a storage device, an OS, etc.

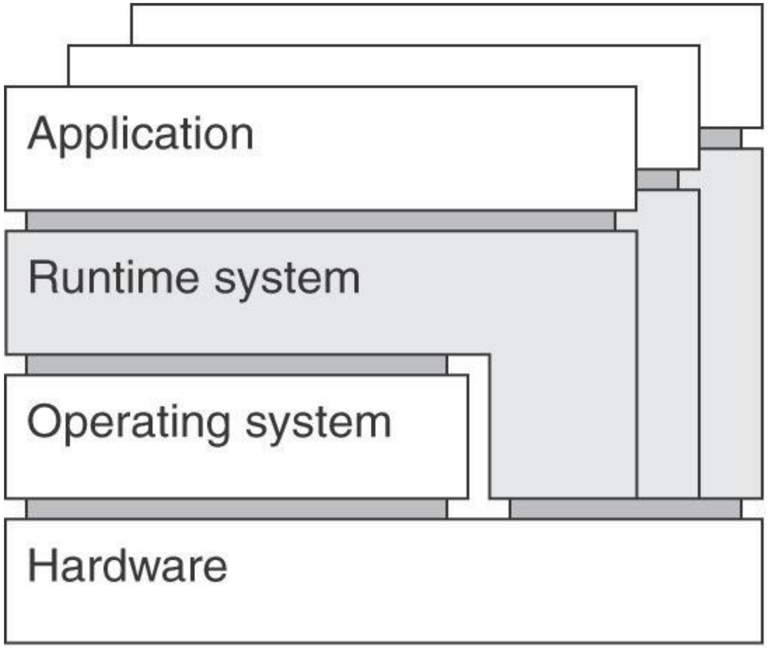
- Threads and (mainly) processes maintain a virtual environment for a task (context)
  - An illusion of parallelism is created
  - Resource virtualization

- Other examples of virtualization:
  - Storage virtualization (your CS network disk)
  - Virtual memory (processes have own address space)
  - Virtual machines (e.g. Java)
  - VM Ware

- Virtualisation deals with extending or replacing an existing interface so as to mimic the behaviour of another system.

Architectures of Virtual Machines (1)

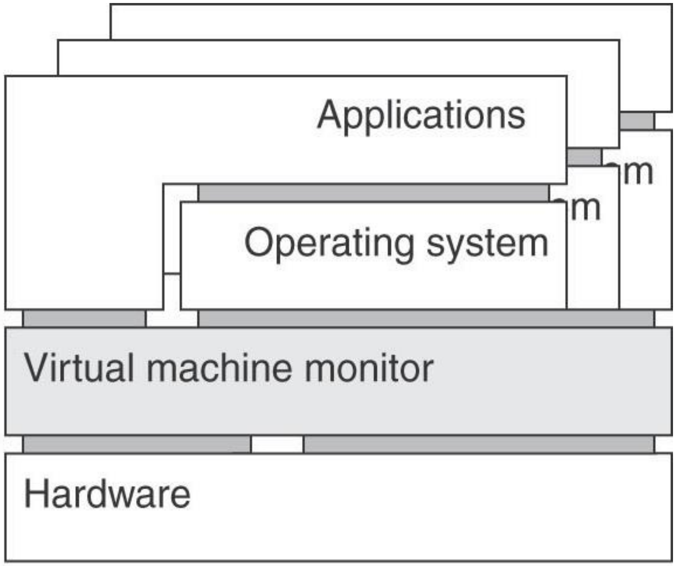
- Process Virtualisation (single process)
  - Build a runtime system that provides an abstract instruction set.



(a)

Architectures of Virtual Machines (2)

- System Virtualisation (multiple processes)
  - Provide a system that is implemented as a layer, completely shielding the original hardware.
  - Offering the complete instruction set of the same (or another) hardware as an interface.
  - Simultaneous use of this interface by different programs (multiple OS run independently on the same platform)



(b)

Desktop Virtualisation Benefits

- Desktop virtualisation, typically, allows one to run an entire (guest) operating system as a process within the (host) operating system controlling the hardware

- E.g. Ubuntu Linux in VirtualBox running under Windows
- Access to new and experimental technology
- Easy network programming
- Portability checks
  - E.g. checking that your JavaScript works in IE6, IE7,.. Mozilla, Firefox,…

Server Virtualisation Benefits

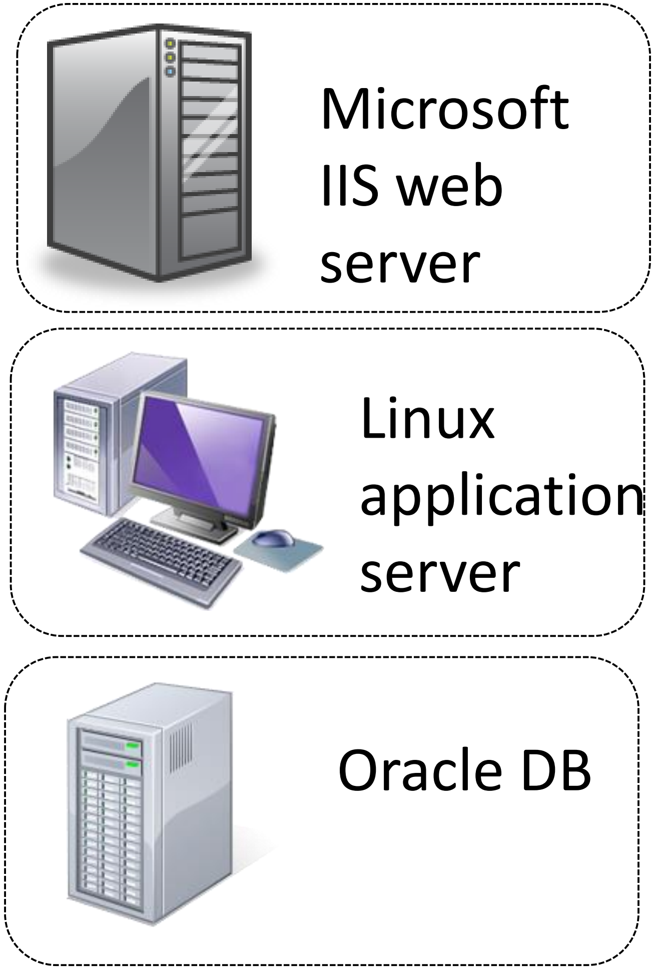
- Multiple servers live on a single physical machine.

- Abstraction
  - Hide physical characteristics of hardware
- Isolation
  - Run several “logical” servers on a single physical server
  - Easily create heterogeneous environment
- Replication

- Reliability and scalability

Server Virtualisation Scenario (1)

- Consider a multi-tier heterogeneous system
- Requires three different machines to run
  - Prone to failure
  - Poor maintainability



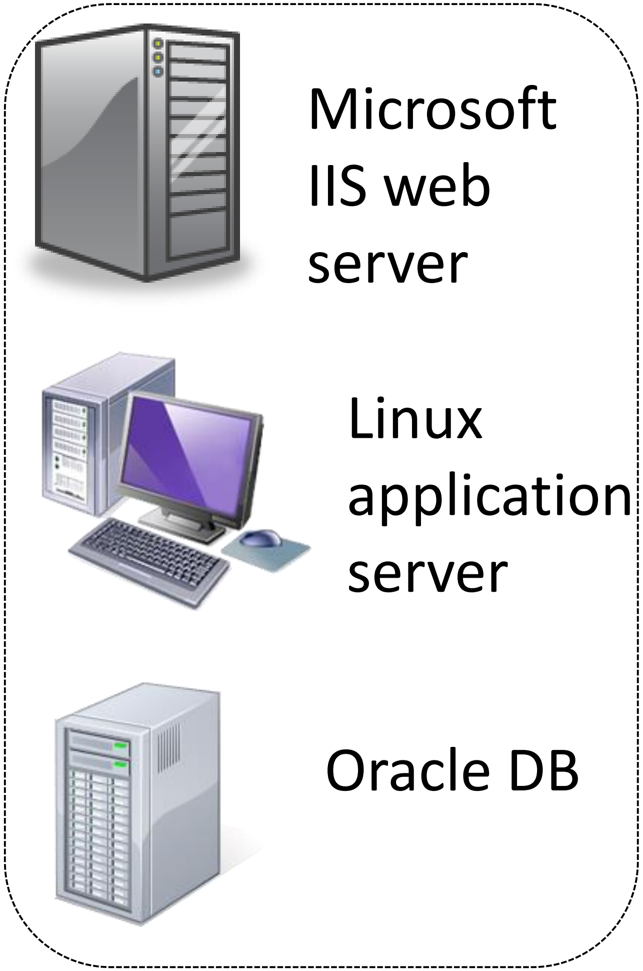
Microsoft IIS web server

Linux application server

Oracle DB

Server Virtualisation Scenario (2)

- Consider a virtualised multi-tier heterogeneous system
- Can run on one computer
  - Prone to failure
- Can spread over a computer cluster
  - Fault tolerant
  - Scalable
  - More stable



Microsoft IIS web server

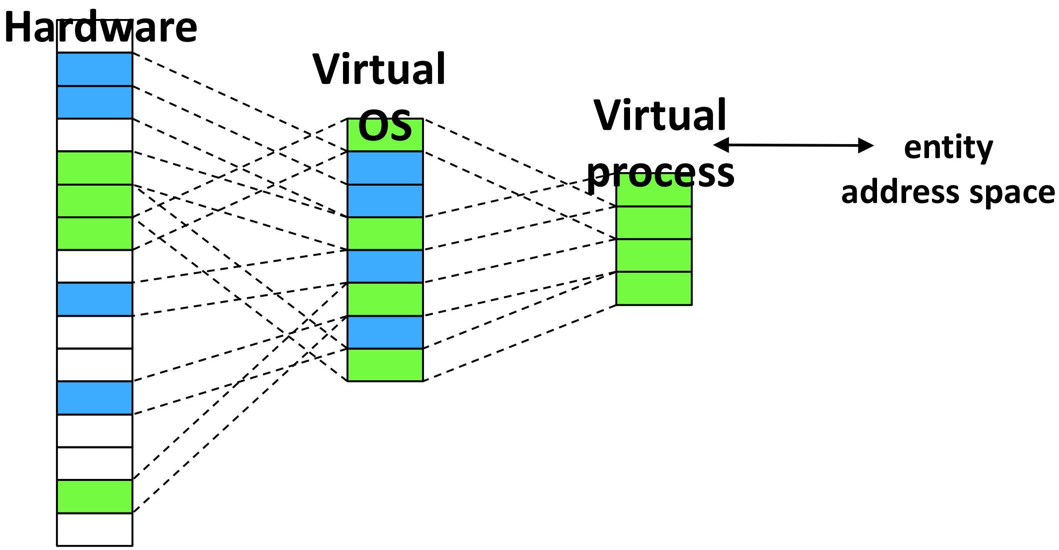
Linux application server

Oracle DB

Hardware-Assisted VMM

Hardware-assisted virtualisation benefits from

- Running general instructions directly on the hardware
- Trapping privileged instructions



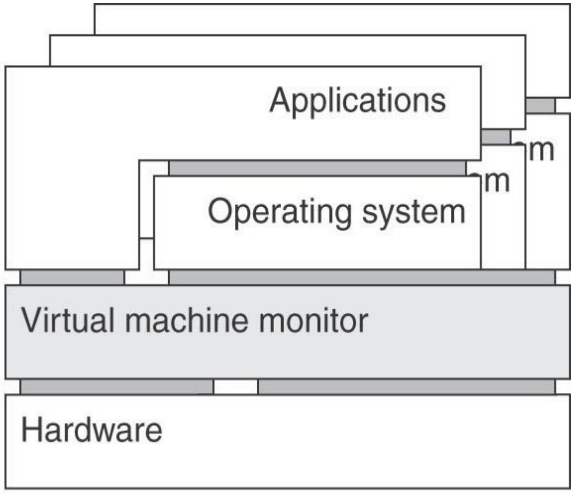
VMM Principles

Popek and Goldberg (1974):

- Equivalence
  - Guest system should run in the same way as if the environment was not virtualised
- Resource control
  - VMM takes full control over the virtualised resources
- Efficiency
  - Majority of machine instructions should be executed without VMM interventions

Virtual Machine Monitor

- VMM intercepts operations that interfere with the host hardware
- Higher level of control than the operating system
  - Hardware support (Ring -1)
    - Intel VT-x, AMD-V
- Software virtualisation
  - Modify guest OS
    - Xen hypervisor
  - Software emulation (slow)
  - Modifying (parts of) guest code on the fly



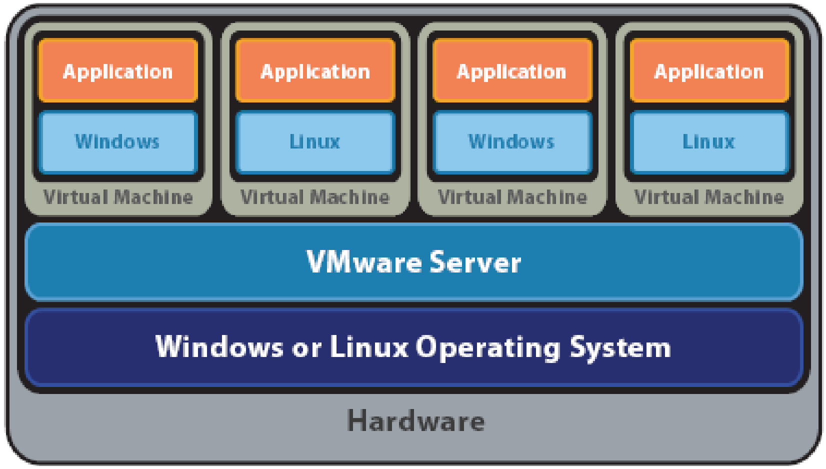
(b)

System Snapshot

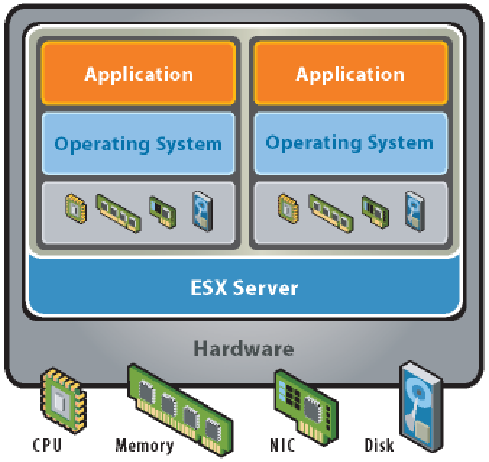
- A VMM can Stop/Freeze/Resume a VM
- Take a snapshot, archive and rollback
- Move/replicate a VM
  - Downloadable “appliances”
- Live Migration
  - Until moved
    - Stop the source machine
    - Copy some information
    - Resume the machine
- Increased availability & load balancing

Example: VMWare

- Workstation / Fusion / Player
- VMWare Server (GSX server) runs over a Linux/Windows host
- VMWare Server (ESX server) runs natively

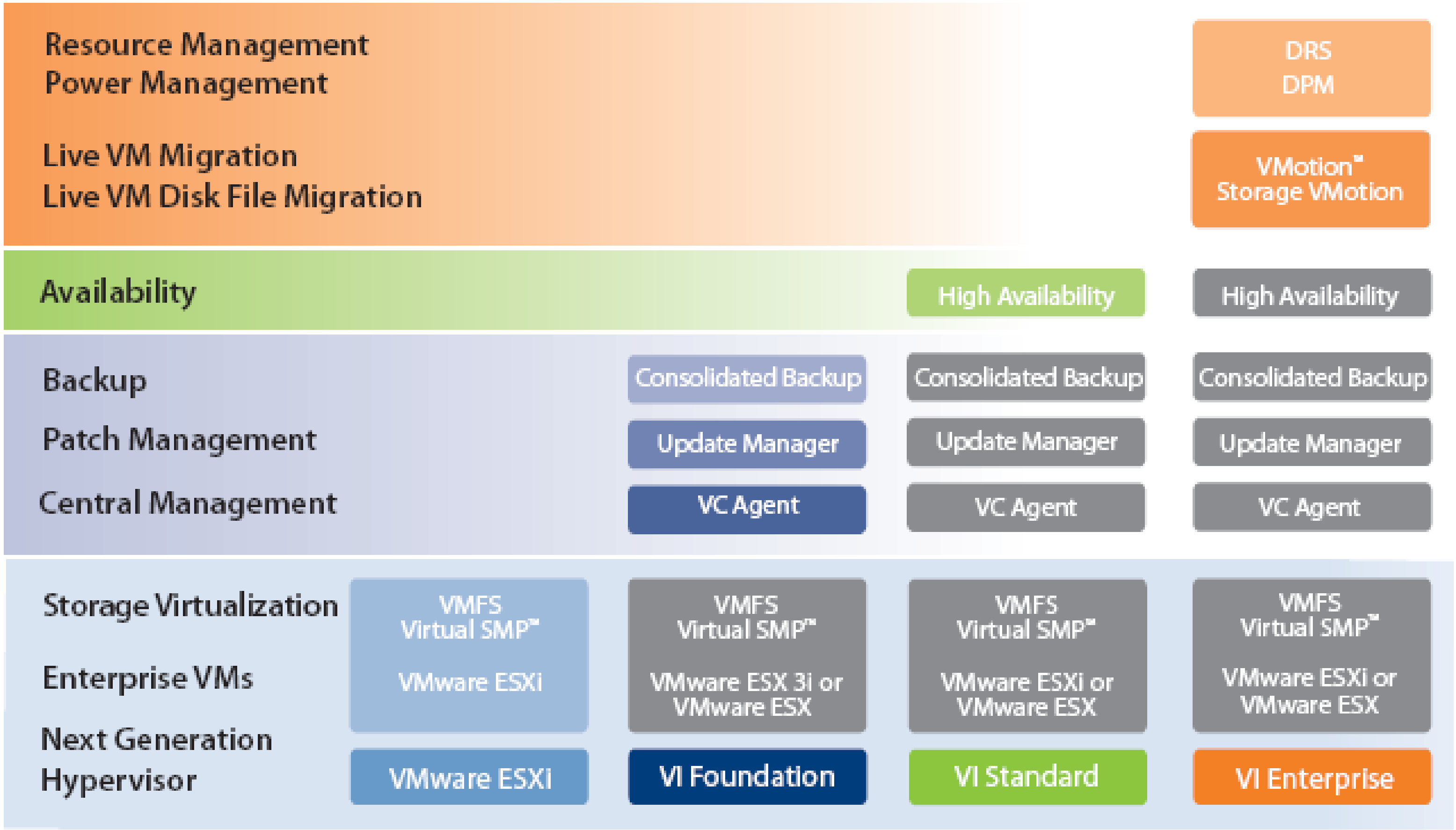


Hosted virtualisation



Bare-metal virtualisation

VMWare Infrastructure



Resource Management Power Management				DRS DPM
Live VM Migration Live VM Disk File Migration				VMotion™ Storage VMotion
Availability			High Availability	High Availability
Backup		Consolidated Backup	Consolidated Backup	Consolidated Backup
Patch Management		Update Manager	Update Manager	Update Manager
Central Management		VC Agent	VC Agent	VC Agent
Storage Virtualization Enterprise VMs Next Generation Hypervisor	VMFS Virtual SMP™ VMware ESXi	VMFS Virtual SMP™ VMware ESX 3i or VMware ESX	VMFS Virtual SMP™ VMware ESXi or VMware ESX	VMFS Virtual SMP™ VMware ESXi or VMware ESX
	VMware ESXi	VI Foundation	VI Standard	VI Enterprise

Example: Microsoft Hyper-V

- Bare-metal solution
- Requires a copy of Windows Server in one of partitions
- Supports Windows and Linux guests
  - Microsoft produced a Linux driver to improve performance

Example: VirtualBox

- Mainly desktop virtualization solution
- The bulk of it is free software
  - Contains proprietary parts
- Software virtualization
  - Runs the guest OS in Ring 1 (not used otherwise by many systems)
  - Requires fiddling on the fly
- Hardware-assisted virtualization
  - Runs a Ring -1 VMM
  - Guest OS runs in Ring 0 (no modification needed)

Example: Xen

Runs on bare metal

- Must have a “master” copy of OS (Linux o FreeBSD)
- Guest OS’s are aware of being run in the virtualised environment – paravirtualisation
- Offers both native and simulated hardware interfaces
- Now support hardware-assisted virtualisation

Unknown Resource Demands

- Scenario: a start-up company requires computing facilities
- Number of users — ??
- Load on servers — ??
- IT budget — ??

Answer: On-demand resource provisioning

Cloud Computing

Virtual machines in the cloud

- Resizable computing capabilities
- Resizable storage
- You get a virtual machine to use it as you like
  - (subject to terms and conditions)
- Service provider maintains the infrastructure
- You pay for what you consume

There are other forms of cloud computing

- Google apps, …

Example: Amazon EC2

Amazon Elastic Compute Cloud:

- Started as Amazon’s own effort to service its customers
- Amazon maintains and supports the infrastructure
  - Uses Xen virtualization
- Coupled with Amazon Simple Storage Service (Amazon S3)

- There are other cloud solutions

Note

Remember that

- Moving your service into the cloud alone will not achieve scalability.
- The cloud provides means for
  - Size scalability
  - Geographical scalability
- You still need to manage scalability

Virtualisation & CC: Advantages

- Abstraction, isolation, distributed transparency
- Reliability, scalability (elasticity)
- Easy to create new “clean” machines
- Run legacy software
- Test new setups, configurations, updates,…
- Lower computer costs

Virtualisation & CC: Disadvantages

- System can work differently in virtual environment
- Might not reach peak performance
- Security and privacy
- Loss of control
- Requires constant high-speed Internet
- Hard to move back (+loss of expertise)