



SNS COLLEGE OF TECHNOLOGY



(An Autonomous Institution)

Re-accredited by NAAC with A+ grade, Accredited by NBA(CSE, IT, ECE, EEE & Mechanical)
Approved by AICTE, New Delhi, Recognized by UGC, Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER APPLICATIONS

COURSE

23CAE717
Cloud Computing

UNIT II

Virtualization

TOPIC

**Virtualization for
Data-Center
Automation**

Semester

II Semester /
I MCA



Automation of Data Center



Google data center in Netherlands | Image credit: Google



Automation of Data Center



- ❑ Involves huge volumes of computing resources in these data centers can be **allocated dynamically to millions of Internet users** simultaneously, with guaranteed **QoS and cost-effectiveness**
- ❑ Automation process is triggered by the growth of virtualization
- ❑ Virtualization development highlights
 - High availability (HA)
 - Backup services
 - Workload balancing
 - Increase in client bases



Server Consolidation

- ❑ **Heterogeneous** workloads can run on servers at various times
- ❑ These workloads can be divided into **two categories**:
 - **Chatty workloads** - may burst at some point and return to a silent state at some other point
 - **Non-interactive workloads** - do not require people's efforts to make progress after they are submitted
- ❑ Resource optimization is focused on the CPU, memory, and network interfaces
- ❑ Server consolidation is an **approach to improve the low utility ratio of hardware resources by reducing the number of physical servers**
- ❑ Virtualization-based server consolidation is the most powerful among centralized and physical consolidation



Server Consolidation



- ❑ Server virtualization has the following side effects
 - Enhances hardware utilization
 - Enables more **agile provisioning** and deployment of resources
 - Total cost of ownership is reduced
 - Improves availability and business continuity
- ❑ To automate data-center operations, one must consider
 - Resource scheduling
 - Architectural support
 - Power management
 - Automatic or autonomic resource management
 - Performance of analytical models

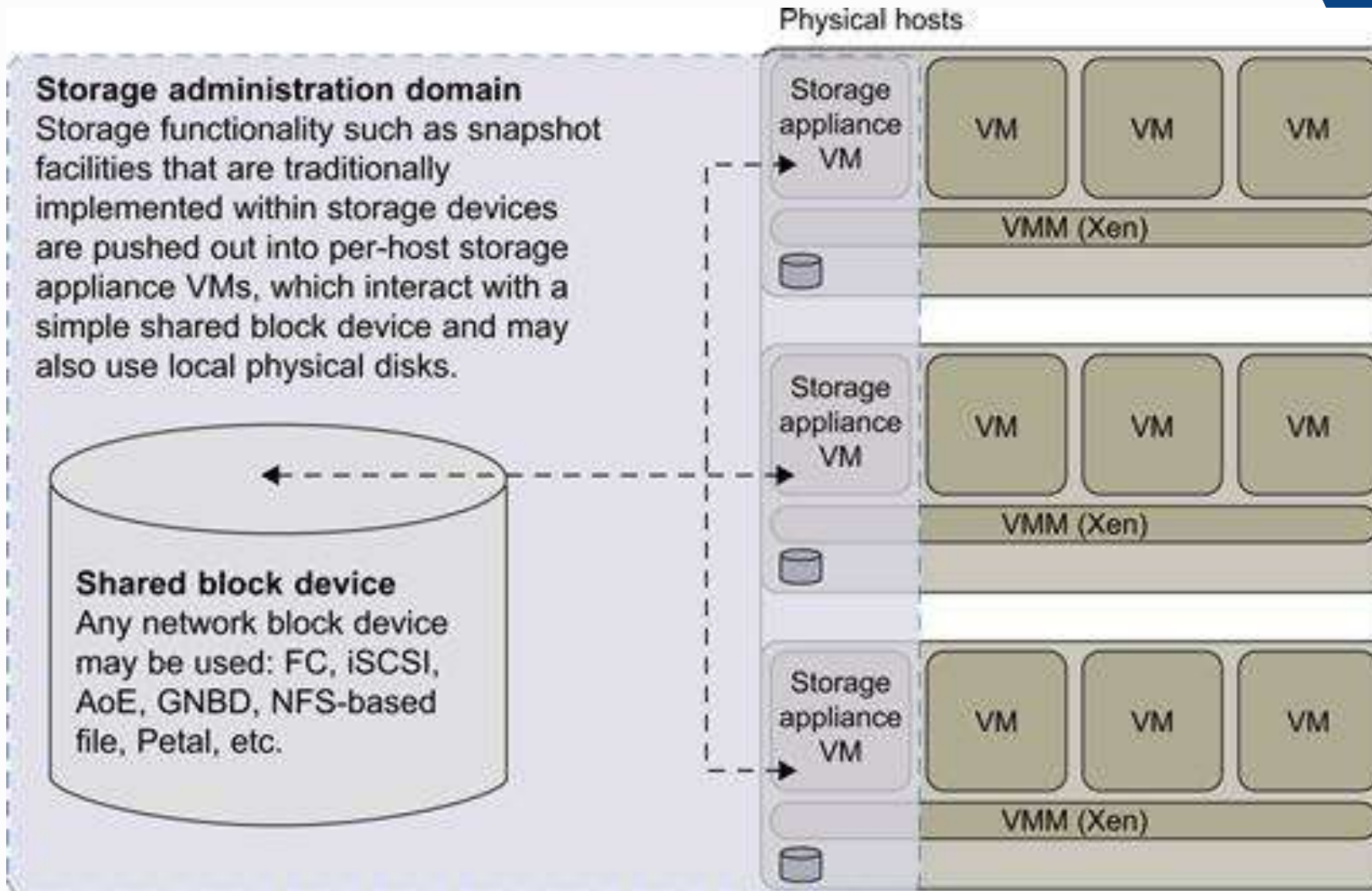


Server Consolidation

- ❑ An efficient, on-demand, fine-grained scheduler is the key for **resource utilization**
- ❑ Scheduling and reallocations can be done in various levels
- ❑ Dynamic CPU allocation is based on VM utilization and application-level QoS metrics
- ❑ **two-level resource management** system to handle the complexity involved. A **local controller** at the **VM level** and a **global controller** at the **server level** are designed
- ❑ storage management of the underlying VMM is much more complex than that of guest OSes
- ❑ **Parallax is a distributed storage system** customized for virtualization environments
- ❑ **Content Addressable Storage (CAS)** is a solution to reduce the total size of VM images, and therefore supports a large set of VM- based systems in data centers



Server Consolidation



Parallax is a distributed storage system customized for virtualization environments



Cloud OS for Data Center



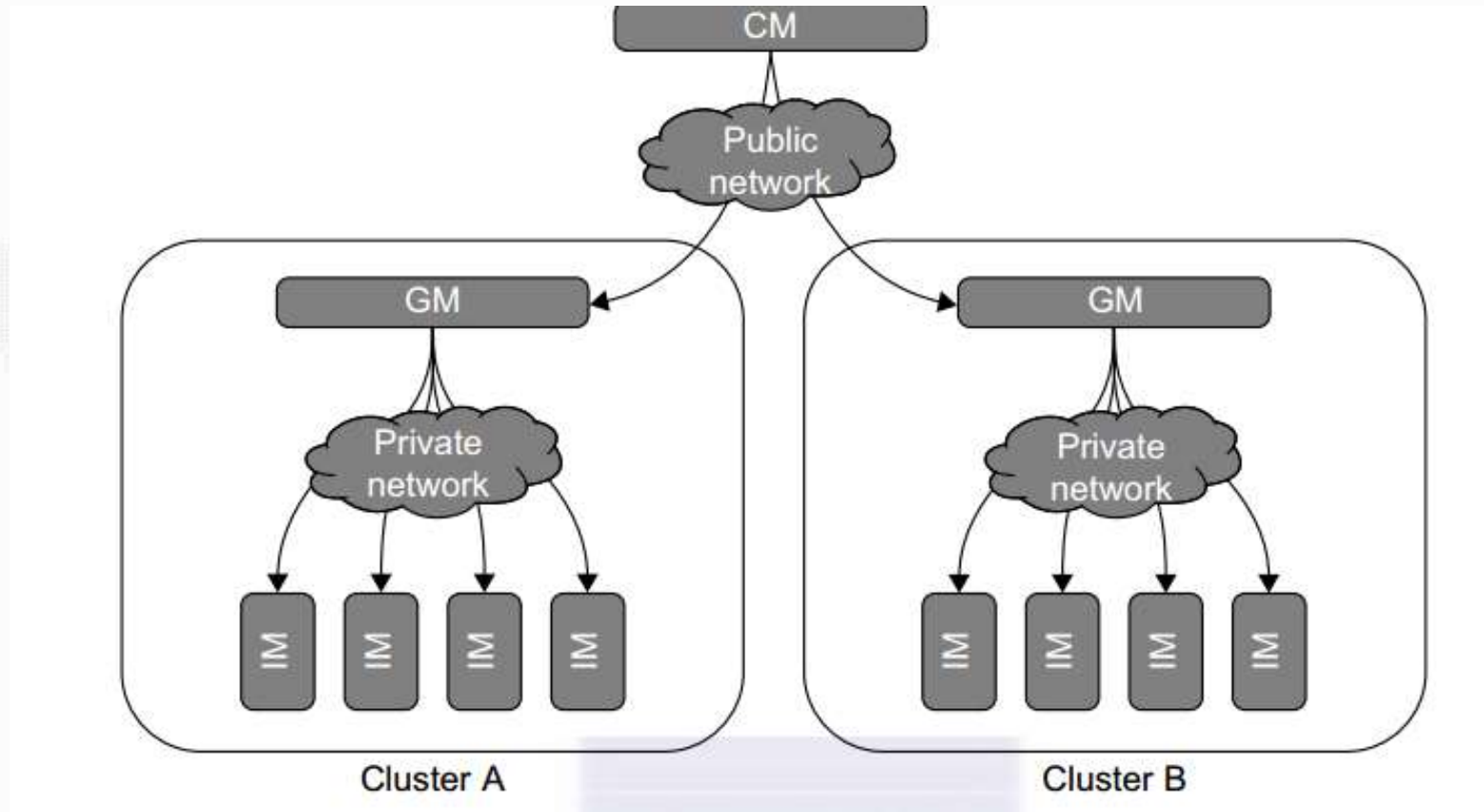
Manager/ OS, Platforms, License	Resources Being Virtualized, Web Link	Client API, Language	Hypervisors Used	Public Cloud Interface	Special Features
Nimbus Linux, Apache v2	VM creation, virtual cluster, www.nimbusproject.org/	EC2 WS, WSRF, CLI	Xen, KVM	EC2	Virtual networks
Eucalyptus Linux, BSD	Virtual networking (Example 3.12 and [41]), www.eucalyptus.com/	EC2 WS, CLI	Xen, KVM	EC2	Virtual networks
OpenNebula Linux, Apache v2	Management of VM, host, virtual network, and scheduling tools, www.opennebula.org/	XML-RPC, CLI, Java	Xen, KVM	EC2, Elastic Host	Virtual networks, dynamic provisioning
vSphere 4 Linux, Windows, proprietary	Virtualizing OS for data centers (Example 3.13), www.vmware.com/products/vsphere/ [66]	CLI, GUI, Portal, WS	VMware ESX, ESXi	VMware vCloud partners	Data protection, vStorage, VMFS, DRM, HA



Eucalyptus

- ❑ Developed @ CSE Dept, University of California
- ❑ Open source software **supporting Infrastructure as a Service (IaaS) clouds**
- ❑ To build **private clouds interact** with end users through Ethernet or the Internet
- ❑ Primarily **supports virtual networking** & VM management, but **virtual storage is not supported**
- ❑ Each high-level system component is implemented as a stand-alone web service.
- ❑ It is installed on Linux-based platforms, is compatible with EC2 with SOAP and Query.







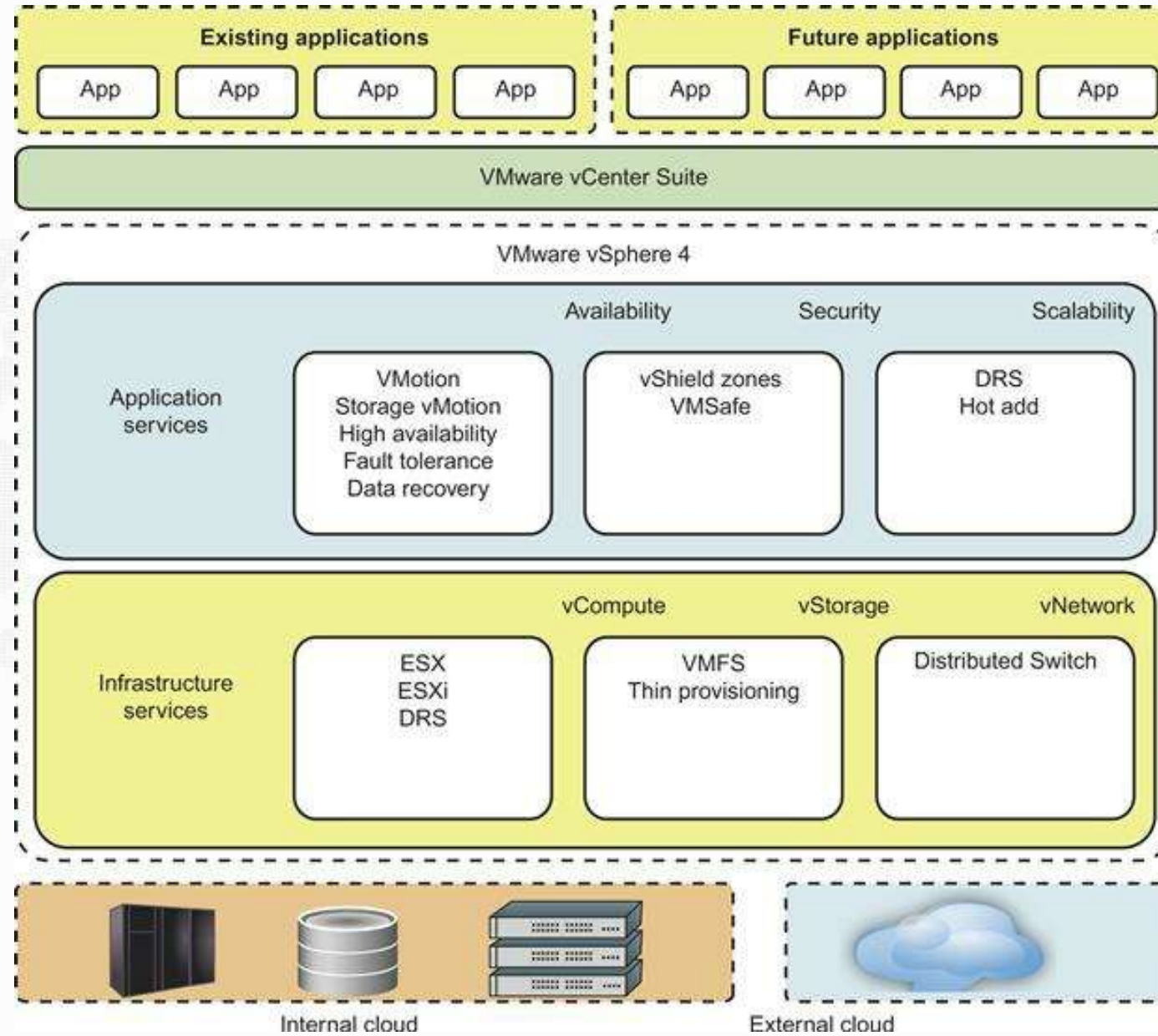
Eucalyptus



- ❑ **Instance Manager** controls the execution, inspection, and terminating of VM instances on the host where it runs.
- ❑ **Group Manager** gathers information about and schedules VM execution on specific instance managers, as well as manages virtual instance network.
- ❑ **Cloud Manager** is the entry-point into the cloud for users and administrators. It queries node managers for information about resources, makes scheduling decisions, and implements them by making requests to group manager



vSphere





vSphere



- ❑ offer virtualization support and **resource management of data-center resources in building private clouds**
- ❑ VMware claims the system is the first cloud OS that supports **availability, security, and scalability** in providing cloud computing services
- ❑ Two functional software suites: **infrastructure services and application services.**
- ❑ It also has three component packages intended mainly for virtualization purposes:
 - ❑ **vCompute**
 - ❑ **vStorage**
 - ❑ **vNetwork**

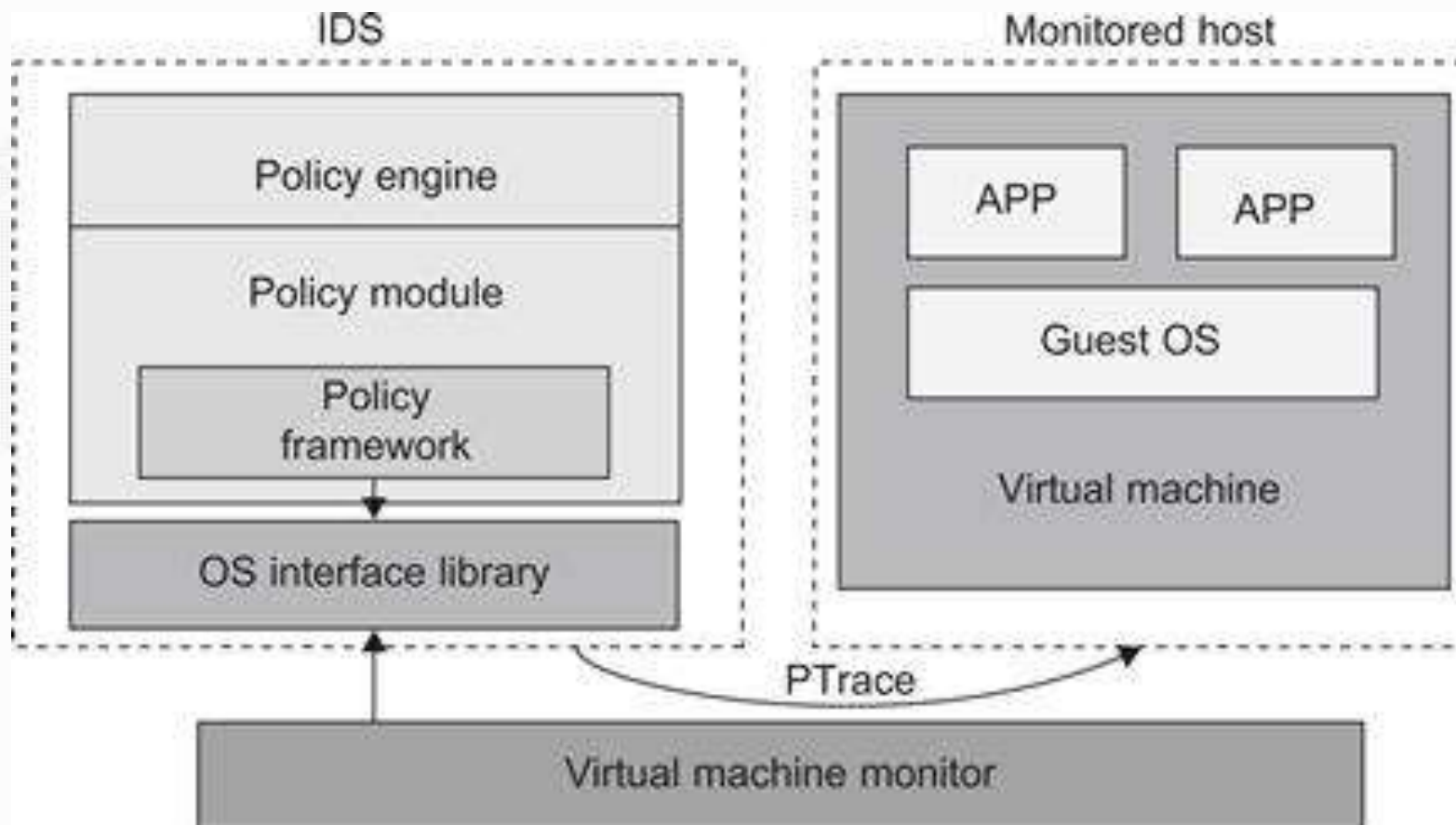


- VMM can provide secure isolation and a VM accesses hardware resources through the control of the VMM
- VMM is the base of the security of a virtual system and one VM is taken as a management VM to have some **privileges such as creating, suspending, resuming, or deleting a VM**

- Intrusions are unauthorized** access to a certain computer from local or network users
- intrusion detection** is used to recognize the unauthorized access.
- An intrusion detection system (IDS) is built on operating systems, and is based on the characteristics of intrusion actions. It can be classified as a **host-based IDS (HIDS) or a network-based IDS (NIDS)**, depending on the data source



VM Based Intrusion Detection





VM Based Intrusion Detection



- Honeypots and honeynets** are also prevalent in intrusion detection
- They attract and provide a fake system view to attackers in order to protect the real system
- A honeypot is a purposely defective system that simulates an operating system to cheat and monitor the actions of an attacker
- A honeypot can be divided into physical and virtual forms.
- A guest OS and the applications running on it constitute a VM.
- The host OS and VMM must be guaranteed to prevent attacks from the VM in a virtual honeypot



References



- ❑ Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012
- ❑ James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
- ❑ Kumar Saurabh, “Cloud Computing – insights into New-Era Infrastructure”, Wiley India, 2011.
- ❑ Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, TMH, 2009.
- ❑ John W. Rittinghouse and James F. Ransome, “Cloud Computing: Implementation, Management, and Security”, CRC Press, 2011