

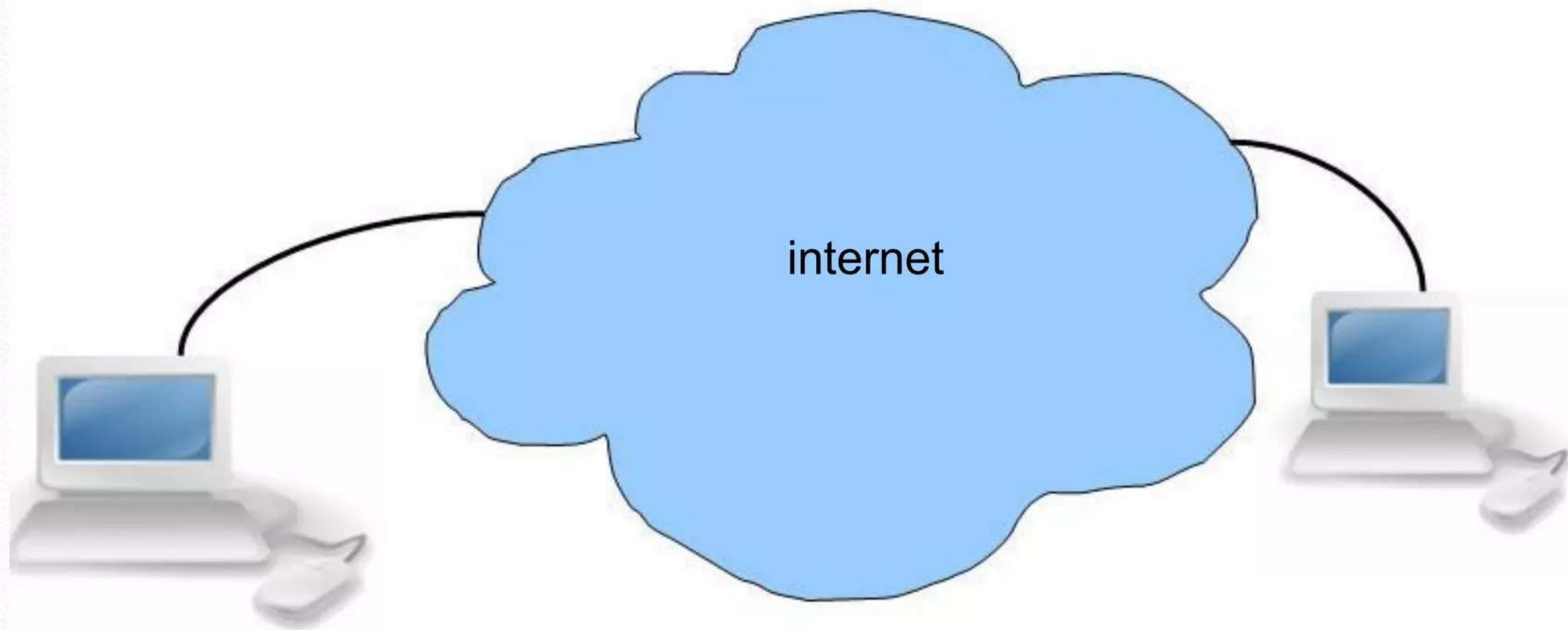
Cloud Computing Openstack

Lê Minh Chí
Nguyễn Sơn Tùng

Nội dung thảo luận

- I. Cloud Computing
 - Giới thiệu về Cloud Computing
 - Virtualization
- II. Amazon Web Services
 - Lịch sử phát triển
 - Các dịch vụ của AWS
- III. Openstack
 - Lịch sử phát triển
 - Các thành phần chính
 - Nội dung thử nghiệm
- IV. Cloud computing security
 - CSA, NIST, ...
 - Security solutions
 - OpenStack security

I. Cloud Computing



Xu hướng IT

Các cuộc cách mạng trong công nghiệp IT

PC đã làm thay đổi hiệu quả và năng suất LĐ của các cá nhân và tổ chức

Internet đã kết nối để tạo nên 1 mạng lưới thông tin không lõi được cho phép chia sẻ và kế thừa

Cloud Computing

Web 2.0

Grid Computing

Điện toán đám mây sẽ làm thay đổi kiến trúc IT trong các tổ chức, cho phép tổ chức có thể tiếp cận với các hạ tầng và hệ thống hiện đại nhưng với chi phí hợp lý



Supercomputers

Mainframe

Centralized Computing



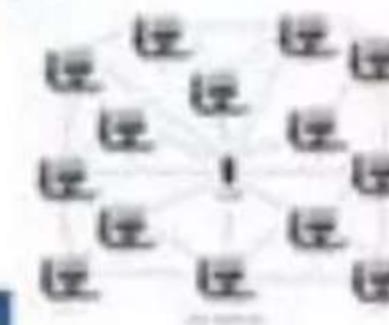
Personal Computer

Unix-based Workstations

Distributed Client-Server



Internet



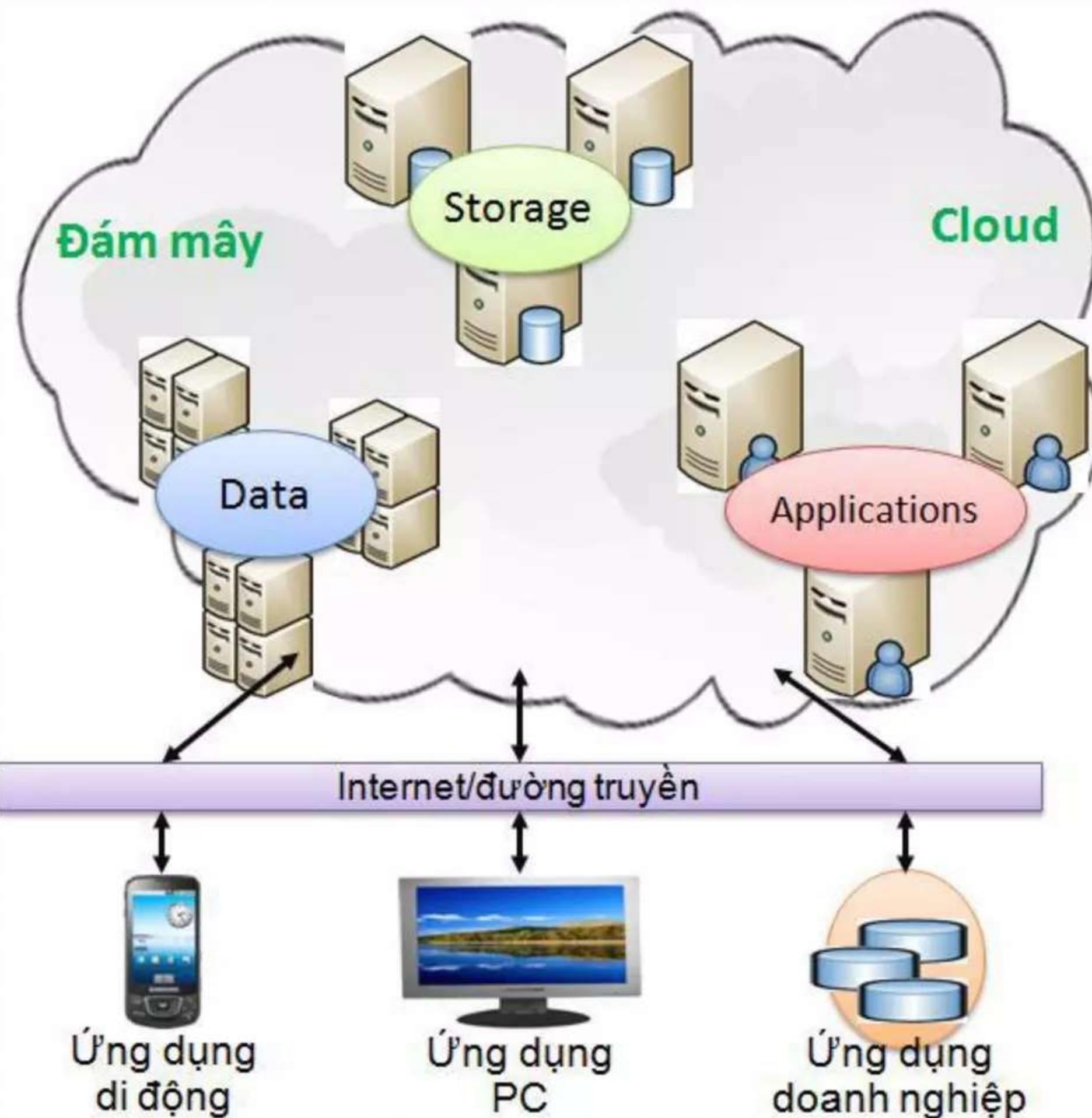
E-commerce
World Wide Web

TCP-IP

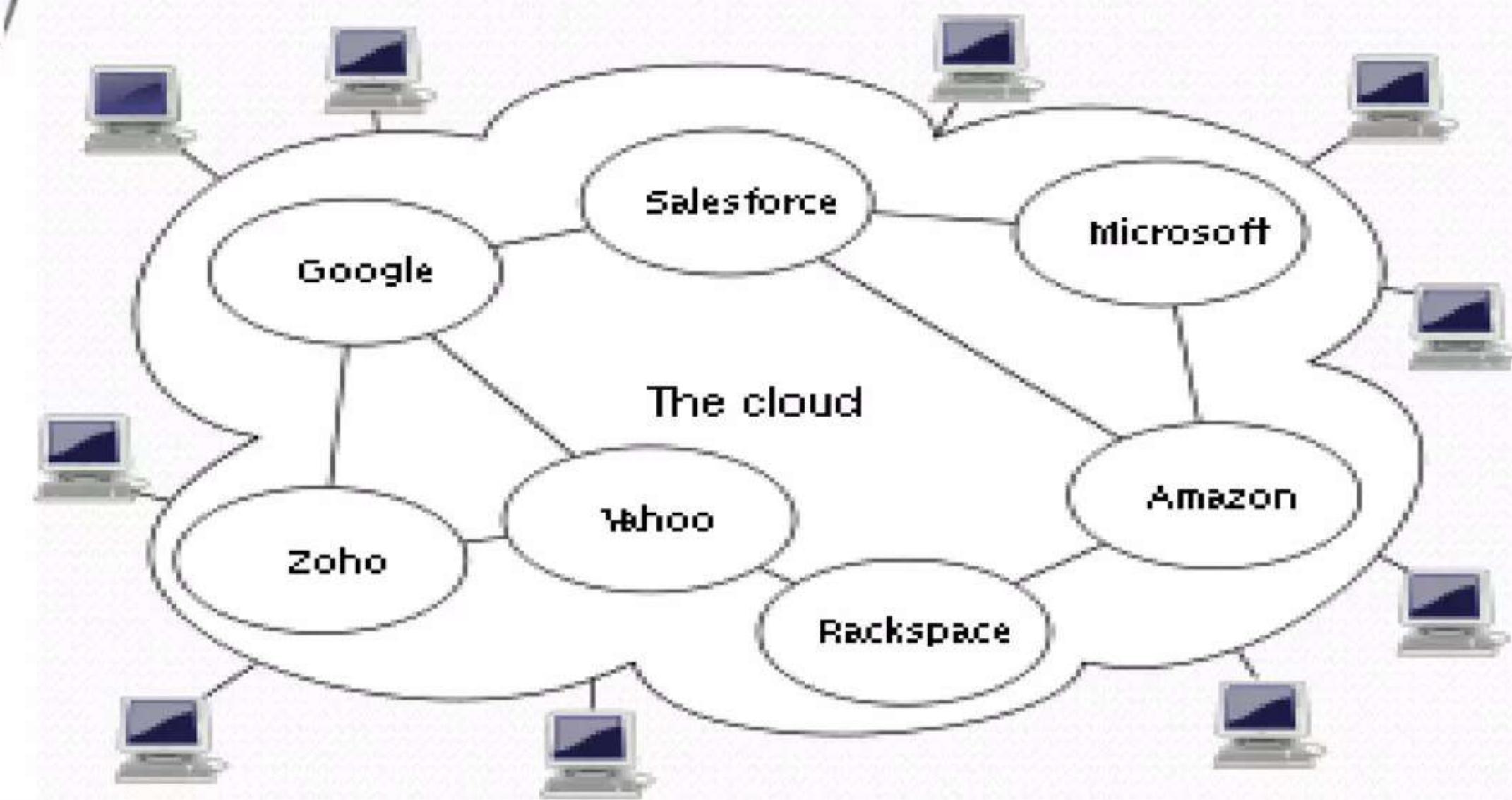
The background of the slide features a large, white, cumulus-like cloud set against a clear blue sky. The cloud is positioned centrally and occupies most of the upper half of the frame.

What is
Cloud Computing?

Cloud computing



- Cloud Computing – tất cả các dịch vụ và lưu trữ trên cloud có thể truy cập ở bất kỳ đâu chỉ cần kết nối internet

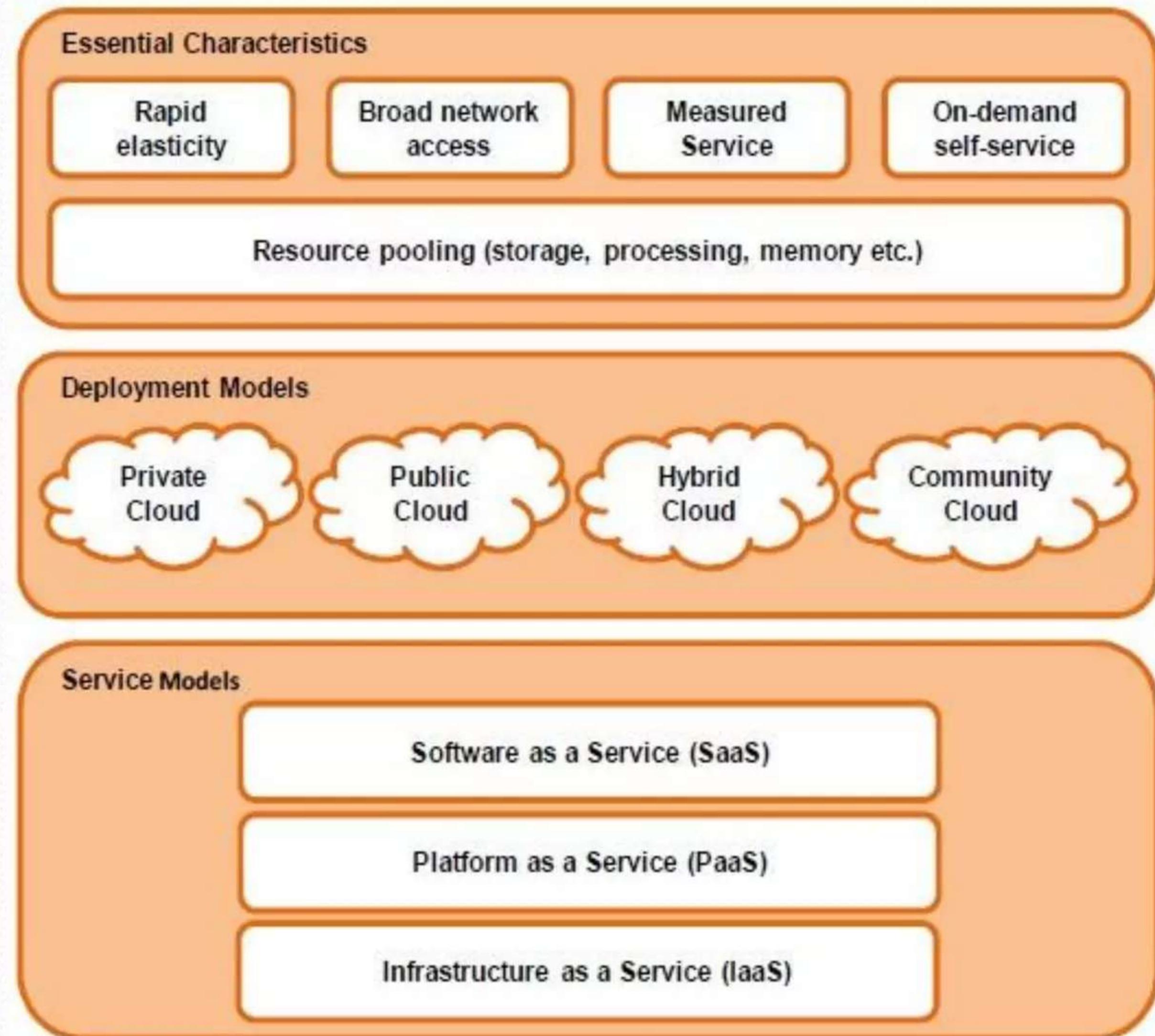


Why Cloud Computing

- Khai thác tối đa hiệu năng, đặc biệt của Data Center
 - Phần lớn các Data Center đều chỉ định tài nguyên vượt nhu cầu
- Chia sẻ tài nguyên
- Tập trung hóa cơ sở hạ tầng
- Tiết kiệm phần cứng
- Tiết kiệm, giảm chi phí đầu tư
- Đa phương tiện
- Khả năng linh hoạt cao
- Trả theo nhu cầu thực tế

Định nghĩa Cloud Computing

- Các tính năng
- Mô hình triển khai
- Mô hình dịch vụ



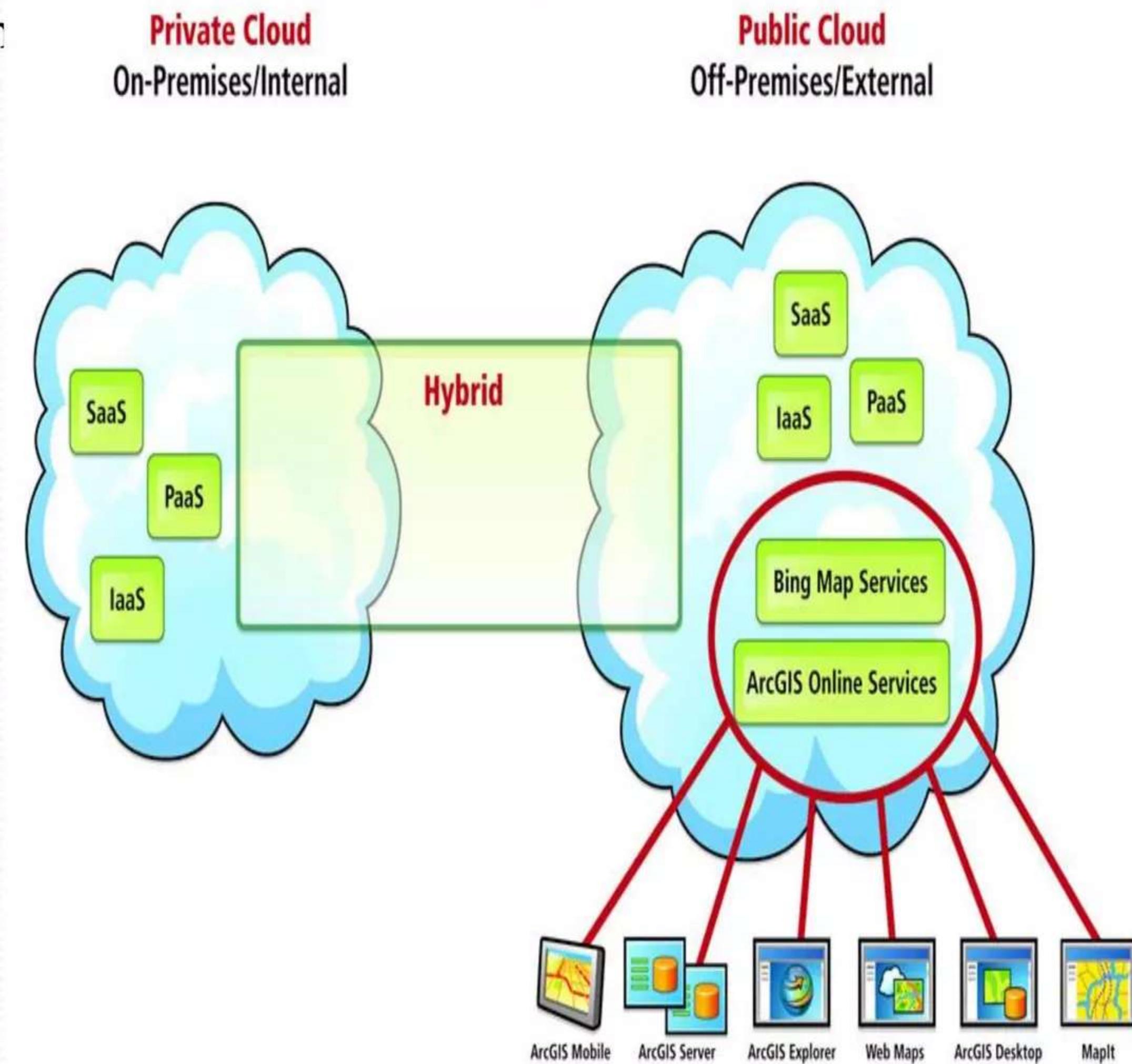
Định nghĩa Cloud Computing (tt)

• Các tính năng

- 1. Thu hồi và cấp phát tài nguyên
- 2. Truy cập thông qua các chuẩn mạng
- 3. Đo lường dịch vụ
- 4. Tự phục vụ theo nhu cầu
- 5. Chia sẻ tài nguyên

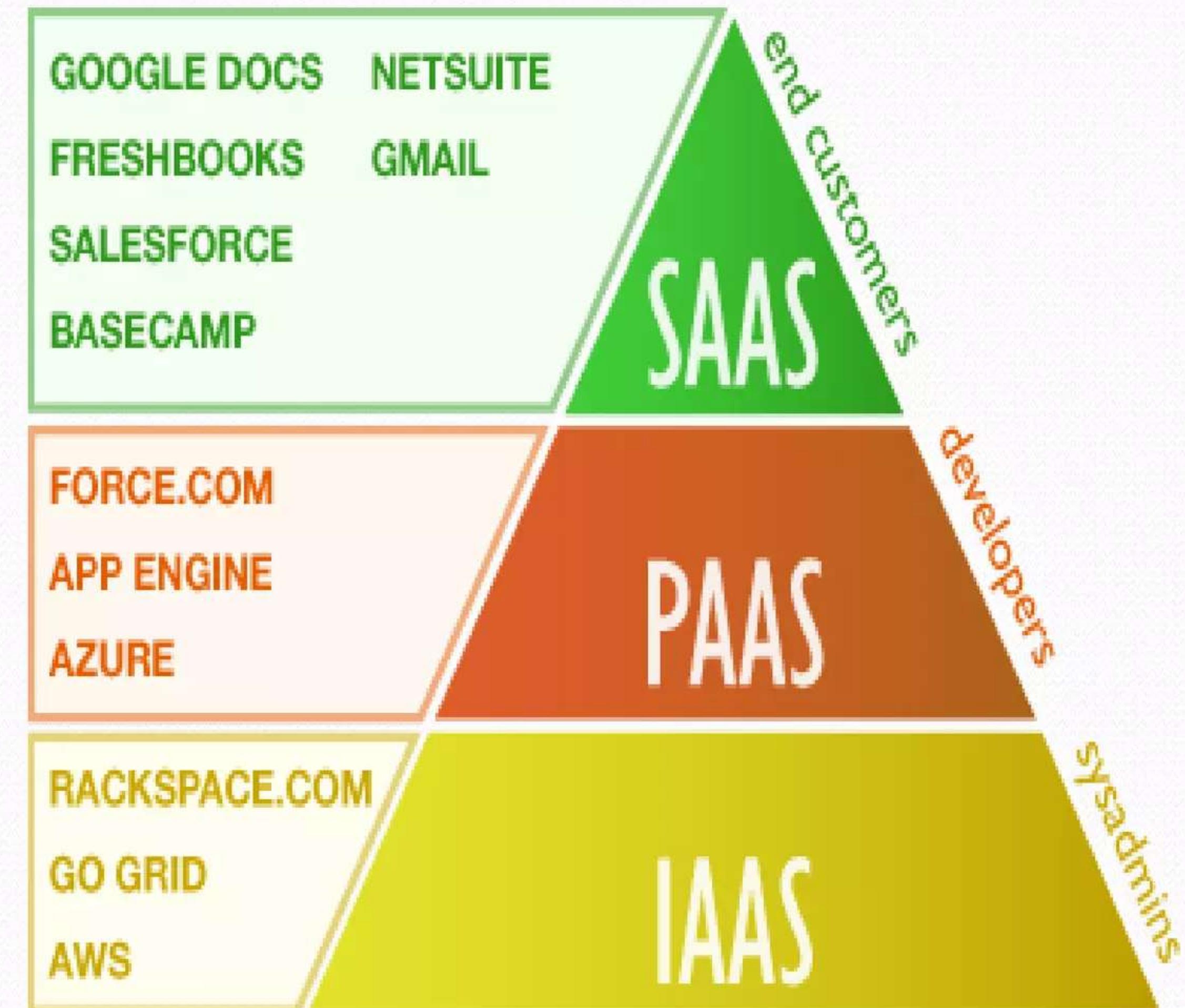
• Mô hình triển khai

- 1. Đám mây riêng
- 2. Đám mây công cộng
- 3. Đám mây “lai”
- 4. Đám mây cộng đồng



Định nghĩa Cloud Computing (tt)

- Mô hình dịch vụ
 - 1. SaaS: Software as a Service
 - 2. PaaS: Platform as a Service
 - 3. IaaS: Infrastructure as a service



Ứng dụng Cloud Computing

SaaS

- Chuyển sang sử dụng dịch vụ CRM package của một SaaS provider như Salesforce.com thay vì phải dựng 1 CRM system
- Chuyển sang sử dụng exchange server thay vì phải xây dựng mail server.

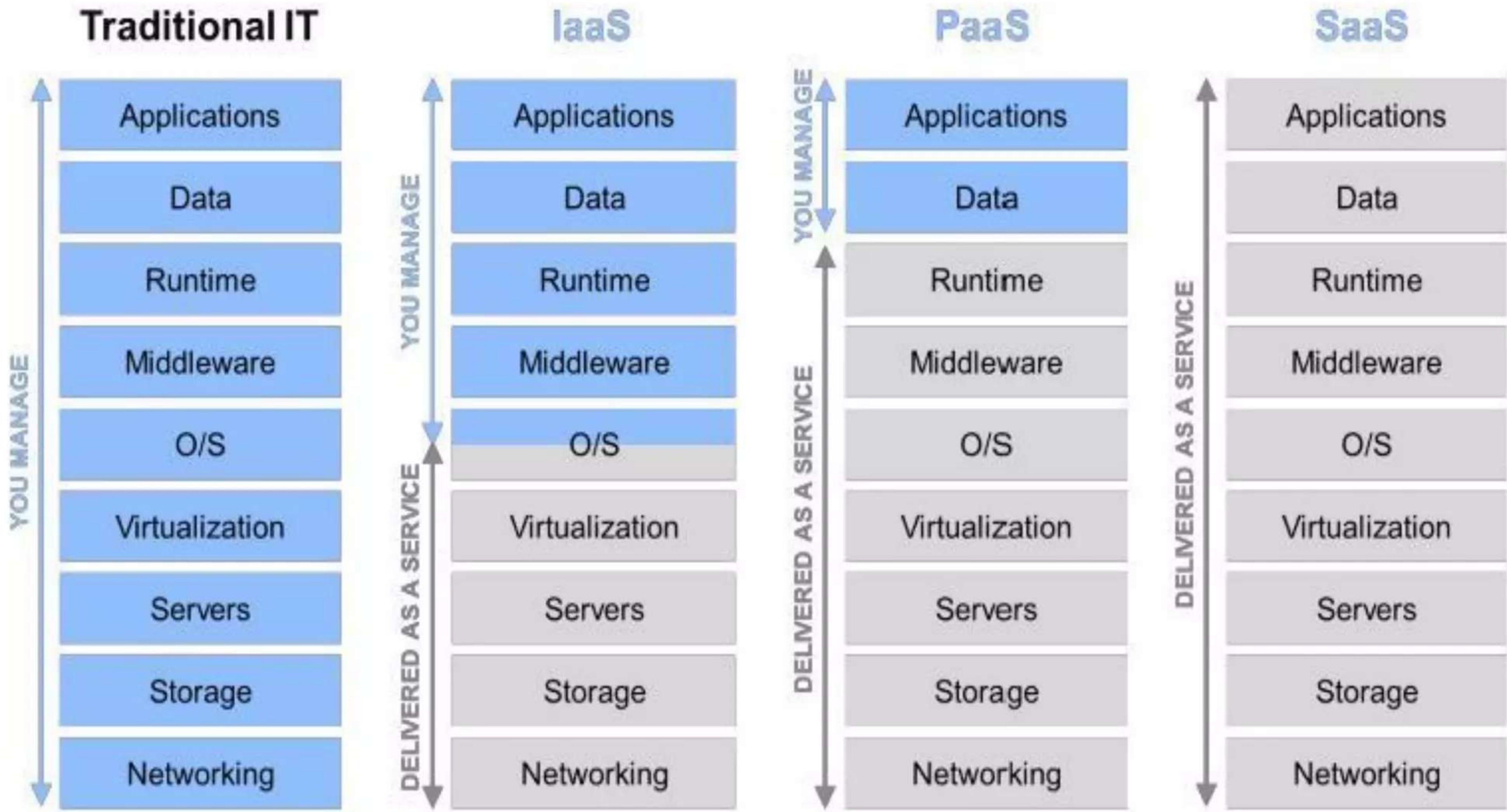
PaaS

- Cần một không gian lưu trữ lớn để lưu trữ số lượng lớn files - sử dụng dịch vụ S3 của amazon.
- Cần một môi trường để phát triển ứng dụng Java

IaaS

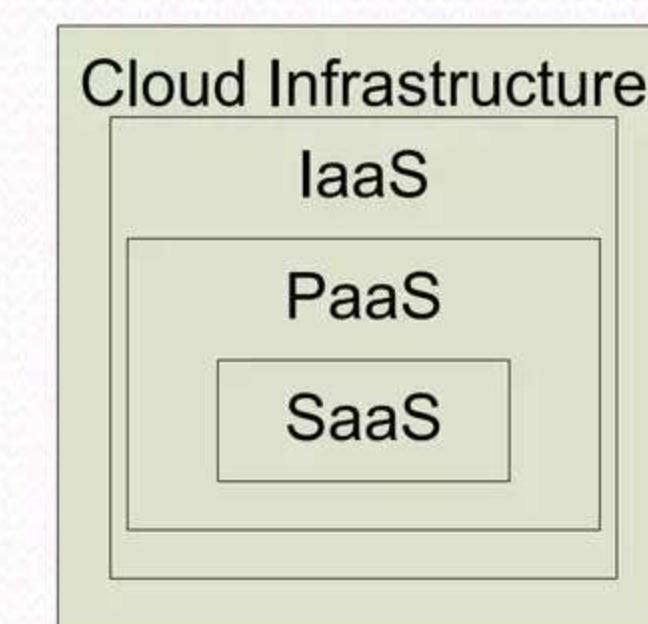
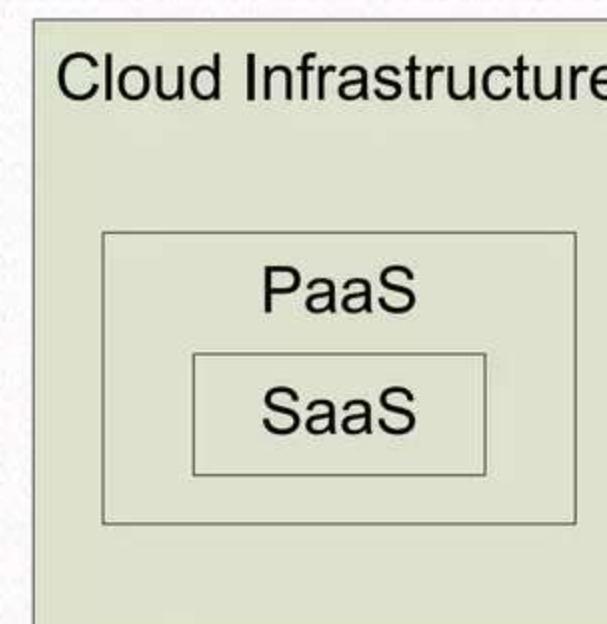
- Chạy một batch job - Sử dụng Amazon EC2.
- Host một website, nhưng trong một thời gian ngắn – thay vì đầu tư chi phí ban đầu, sử dụng Flexiscale.

Customer IT management

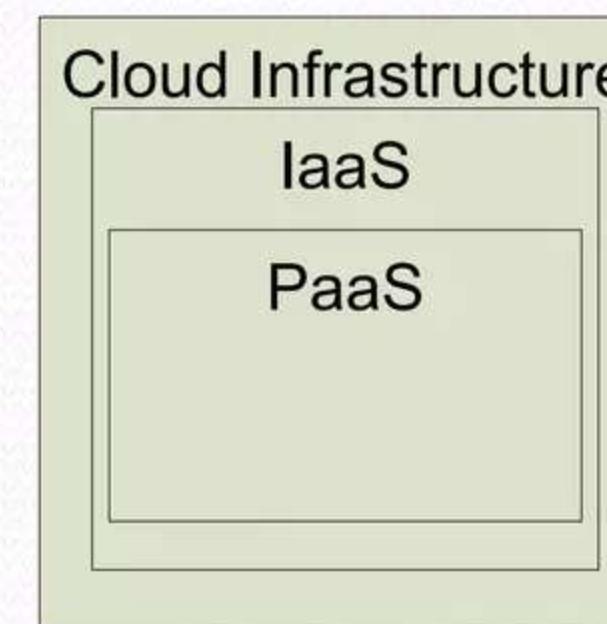
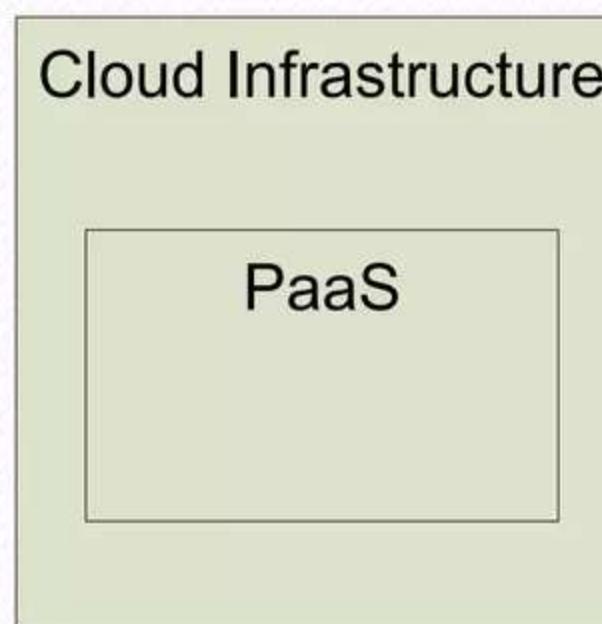


Source: Microsoft.

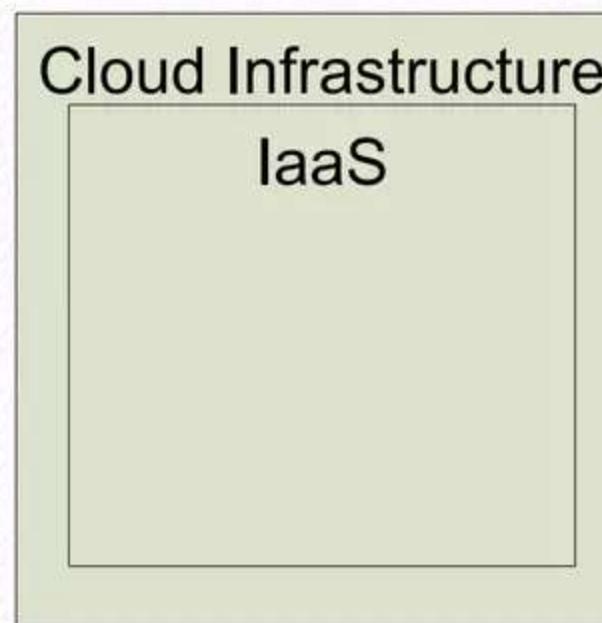
IaaS – PaaS - SaaS



**Software as a Service
(SaaS)
Architectures**



**Platform as a Service (PaaS)
Architectures**



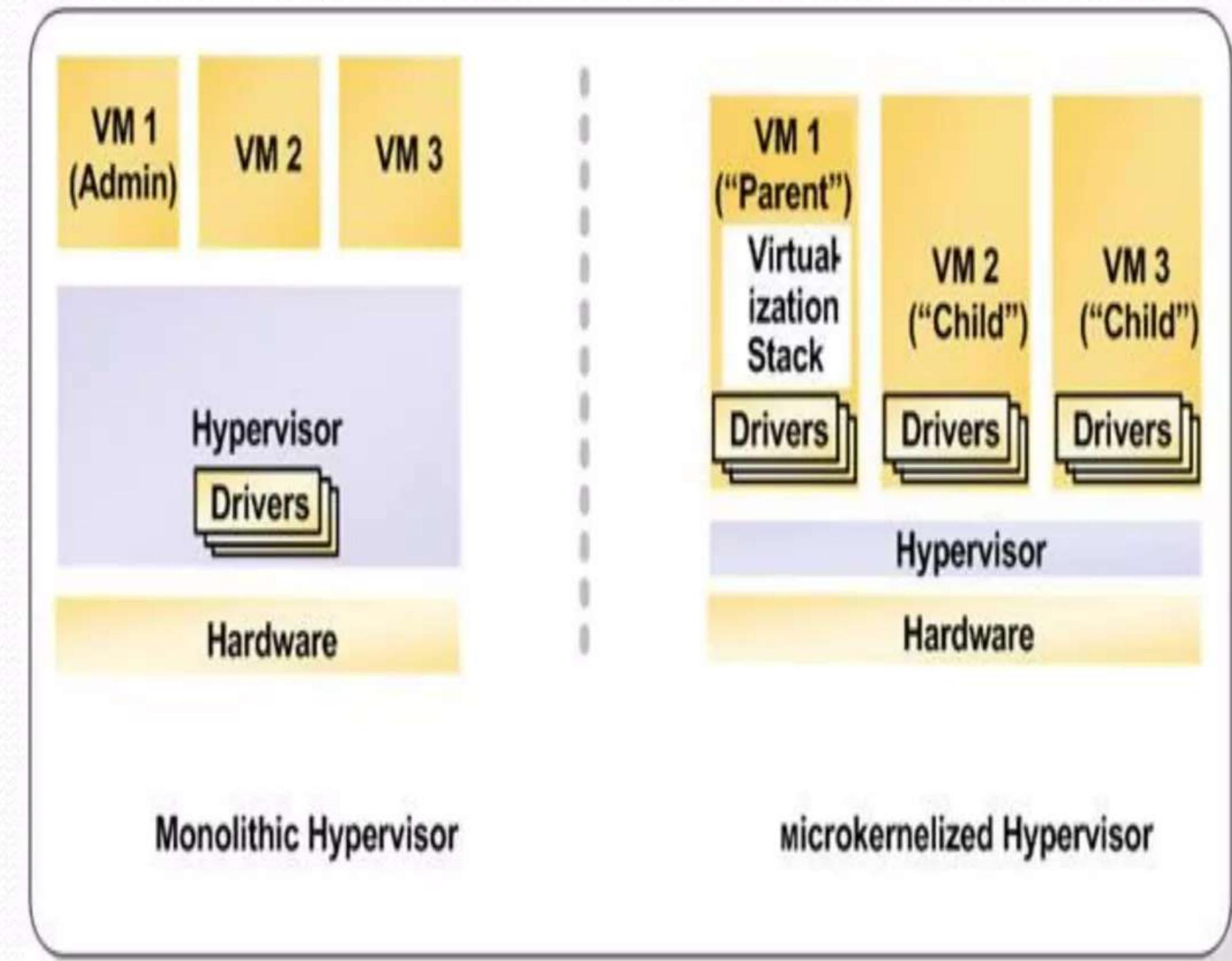
**Infrastructure as a Service (IaaS)
Architectures**

Virtualization Technologies - Background

- Mode Switching
 - Kernel mode
 - User mode
- VMM (Virtual Machine Monitor)
 - *VMM đóng vai trò như một phần mềm trung gian chạy trên HDH để chia sẻ tài nguyên với HDH. Ví dụ: VMware workstation, Virtual PC, KVM.*
 - *VMM đóng vai trò là một hypervisor chạy trên phần cứng. Ví dụ: VMware ESXi, Hyper-V, Xen.*
- Hypervisor
 - Monolithic: ESXi
 - Micro hypervisor: Hyper-V

Monolithic vs Micro-kernelized

- **Monolithic hypervisor**
- Driver riêng biệt để truy cập tài nguyên phần cứng bên dưới.
- Các VMs truy cập tài nguyên hệ thống thông qua drivers của hypervisor.
- *Ưu điểm: hiệu suất cao*
- *Nhược điểm: khi driver trên hypervisor bị sự cố thì cả hệ thống ngưng hoạt động, hoặc phải đổi mặt với vấn đề an ninh khi drivers có thể bị giả dạng bởi malware, một rủi ro trong môi trường ảo hóa.*

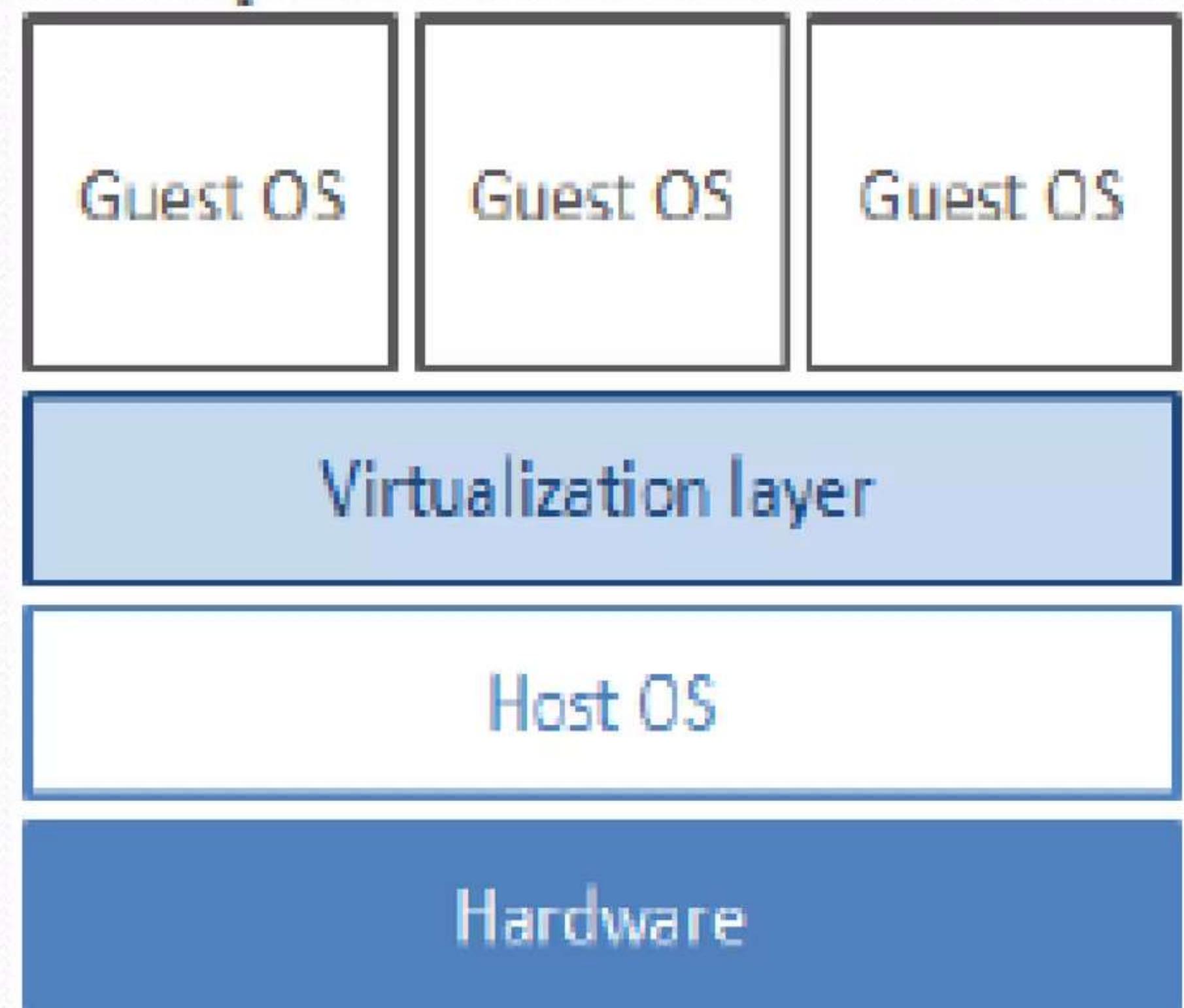


Microkernelized hypervisor: không có driver bên trong hypervisor mà chạy trực tiếp trên mỗi partition. Một VM là partition cha quản lý memory, lưu trữ drivers, và khởi tạo các partition con.

- *Ưu điểm: sự an toàn và tin cậy.*
- *Nhược điểm: độ sẵn sàng (availability) khi partition cha gặp sự cố.*

Các loại ảo hóa

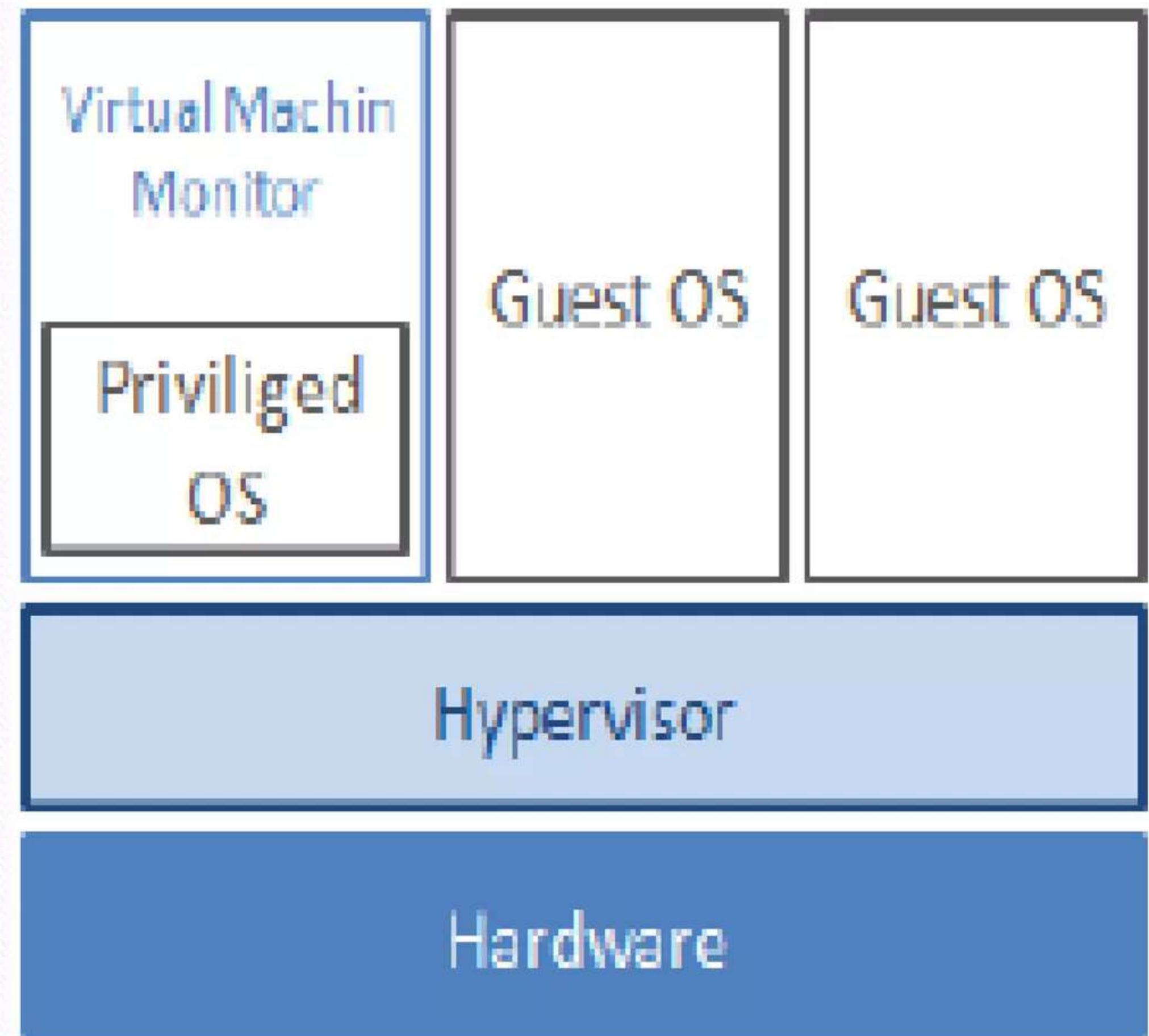
- Full-virtualization
- Cung cấp máy ảo mô phỏng của 1 máy chủ thật với đầy đủ tất cả các tính năng bao gồm input/output operations, interrupts, memory access, ...
- Nhược điểm: Hiệu năng thấp (mode switching).
- Xen, VMWare workstation, Virtual Box, Qemu/KVM, và Microsoft Virtual Server hỗ trợ loại ảo hóa này



Các loại ảo hóa

Para-virtualization

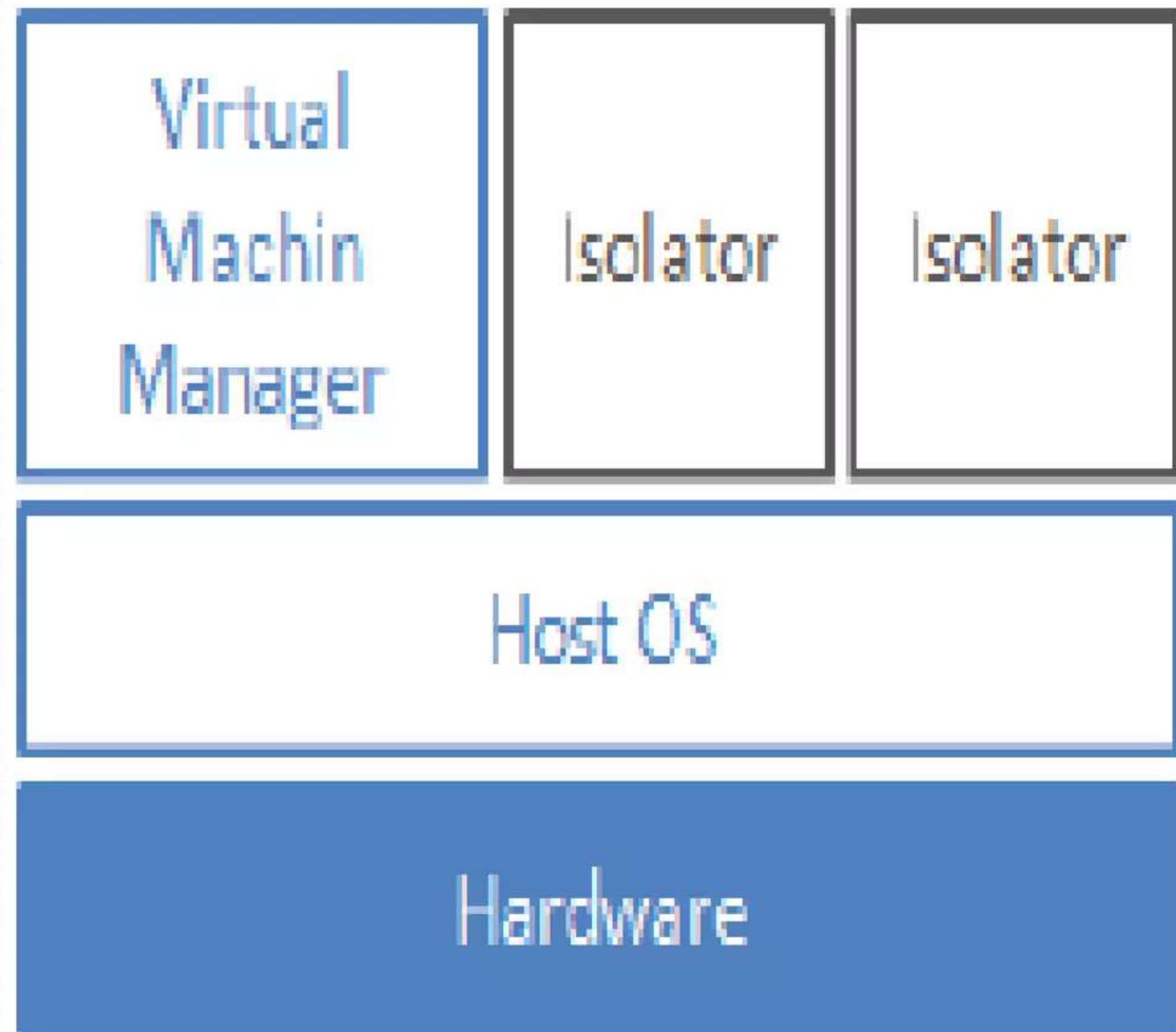
- Kỹ thuật ảo hóa được hỗ trợ và điều khiển bởi 1 hypervisor nhưng các Oss của guest thực thi các lệnh không phải thông qua Hypervisor (hay bất kỳ 1 trình quản lý máy ảo nào) nên không bị hạn chế về quyền hạn.
- Ưu điểm: hiệu suất cao
- Nhược điểm: các OS biết đang chạy trên 1 nền tảng phần cứng ảo và khó cấu hình cài đặt.
- Xen, VMware, Hyper-V, và UML



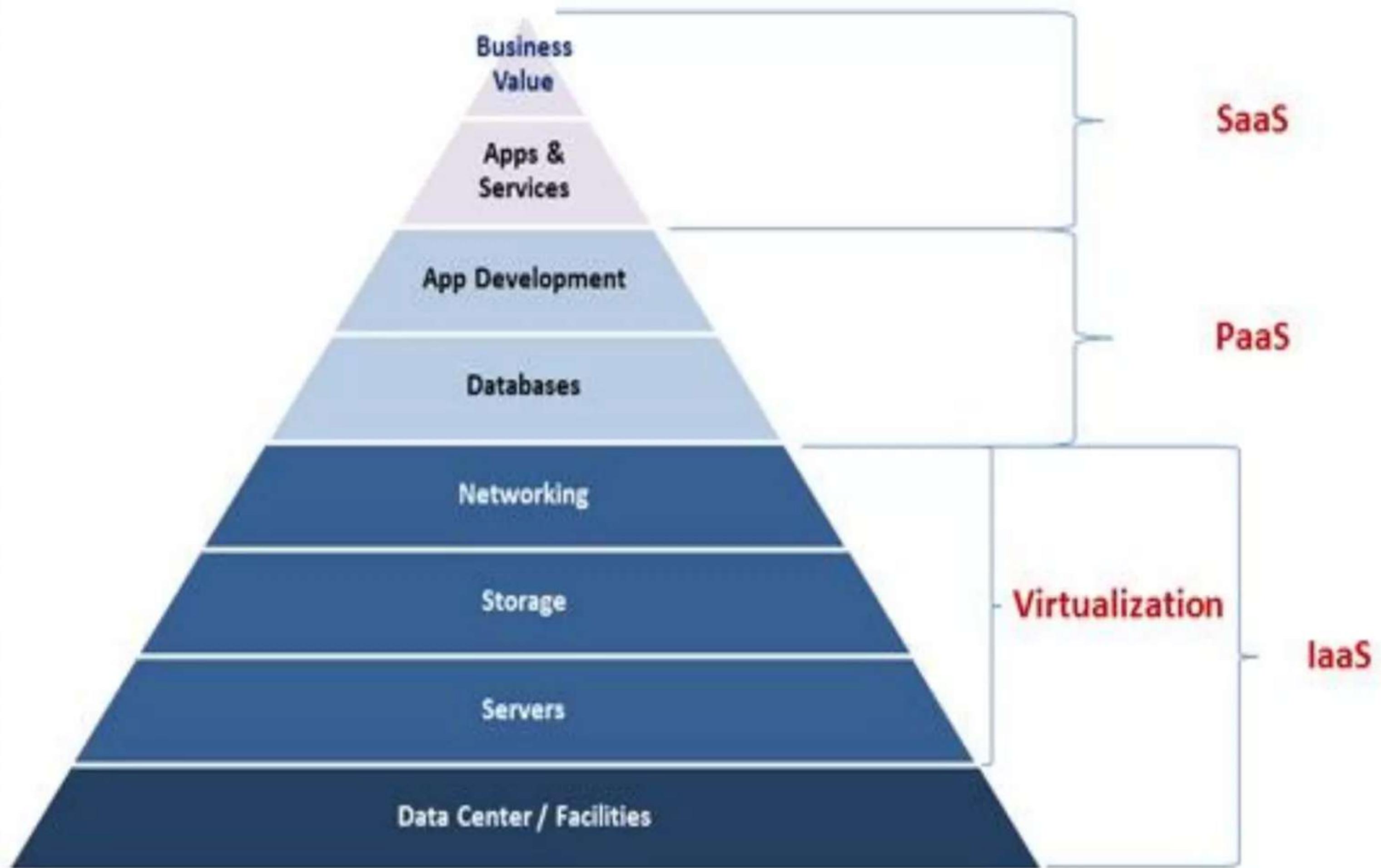
Các loại ảo hóa

OS-level virtualization (Isolation)

- Tạo và chạy được nhiều máy ảo cách ly và an toàn (secure) dùng chung 1 HĐH.
- Ưu điểm: bảo trì nhanh chóng nên được ứng dụng rộng rãi trong các lĩnh vực hosting.
- Chỉ có trên HĐH Linux.
- OpenVZ, Virtuozzo, Linux-VServer, Solaris Zones, và FreeBSD Jails.



Cloud vs Virtualization



Cloud vs Virtualization

Virtualization

- Infrastructure
- Hypervisor & related tools.
- Computer OS.
- Compute, network, and storage.
- IT manager, IT administrator
- Provision resource

Cloud

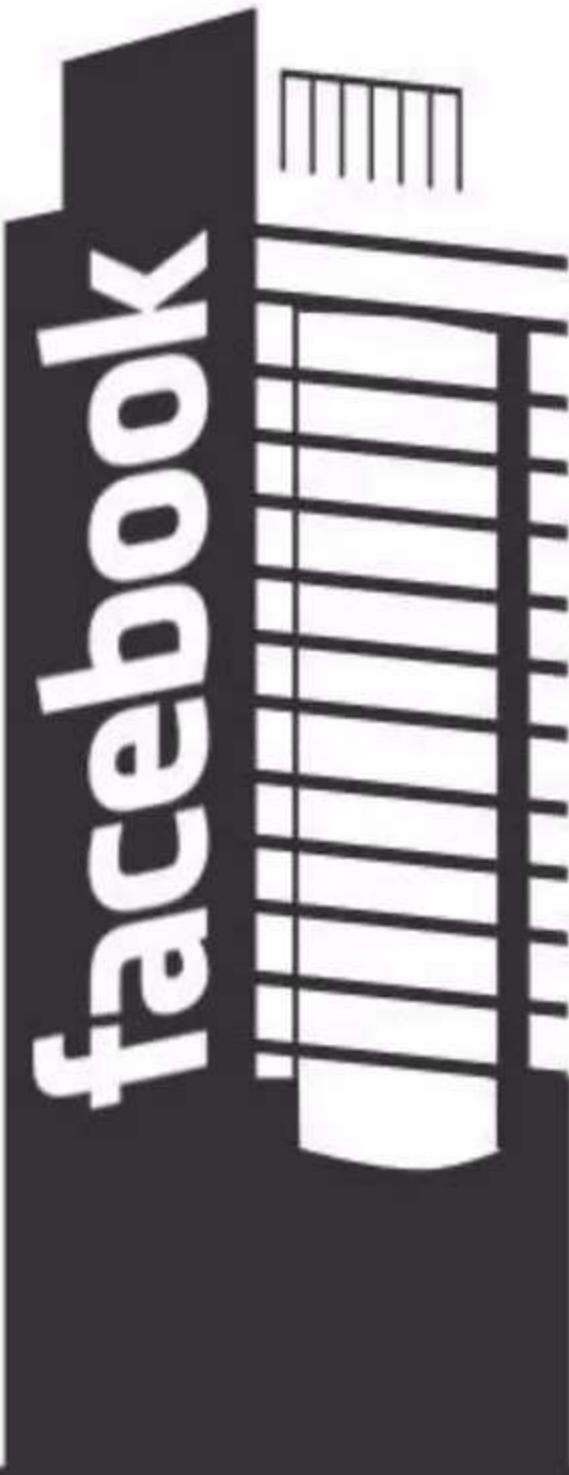
- Application
- Services.
- Service catalog.
- IaaS, PaaS, SaaS.
- Business app owner, developer, end users.
- Pay as you go

II. Amazon Web Services



<http://aws.amazon.com>

Amazon.com: a digital shop around the corner...



... and a digital colossus.



amazon.com

amazon kindle

amazon instant video

Amazon Prime™

amazon cloud drive

amazon MP3

amazon appstore

amazon web services™



amazon cloud player

amazon fresh

Customers in 190 Countries

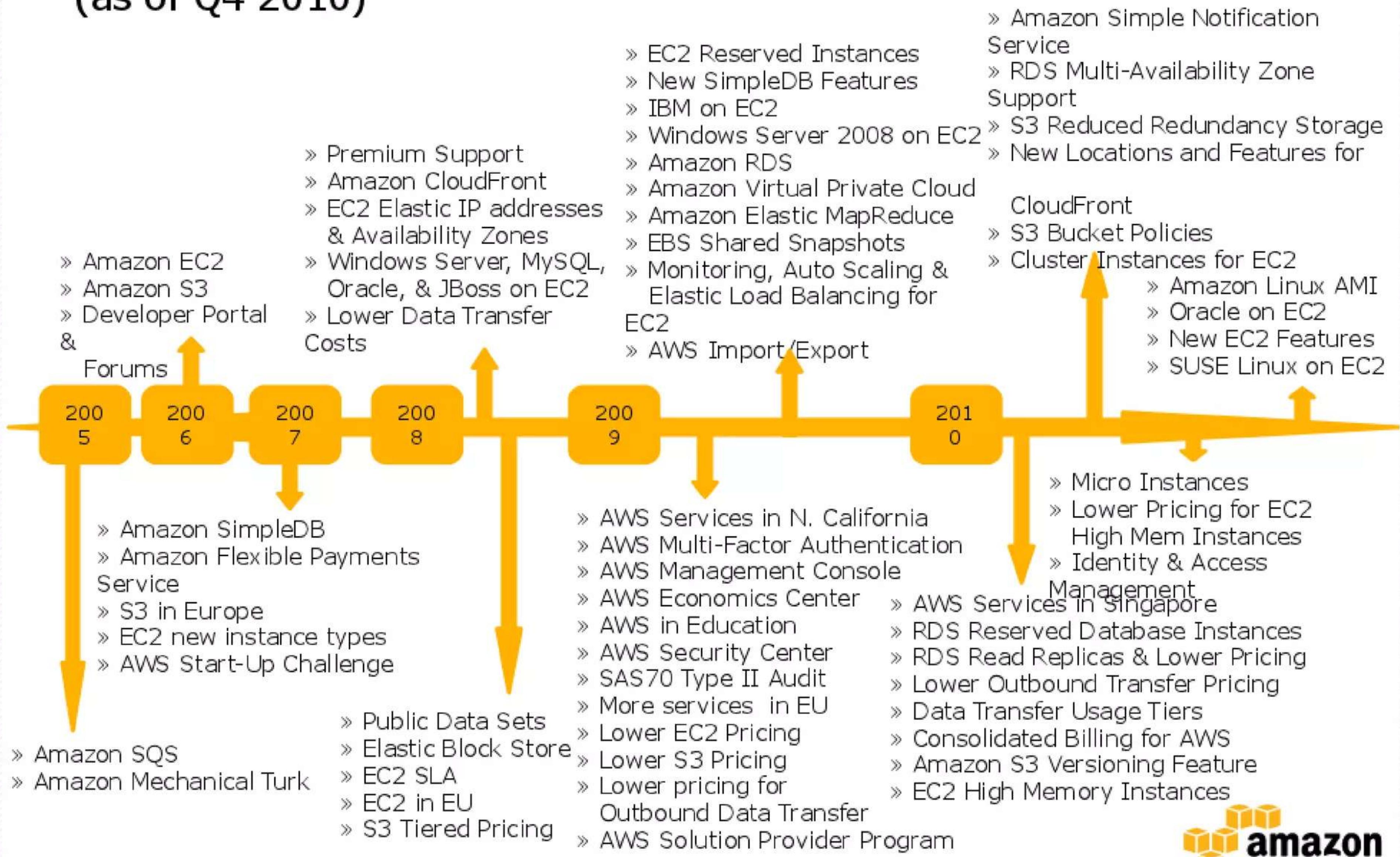


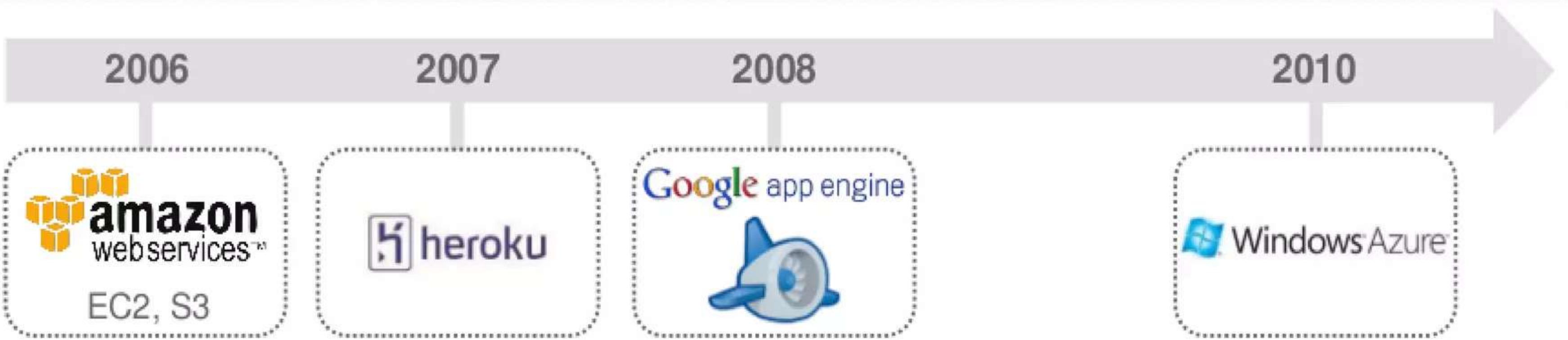
- Zynga.com
 - Farmville, Mafia Wars, Treasure Isle...
 - 12,000 servers on AWS
 - More than 230 million monthly users
 - 100% on AWS
-
- Netflix
 - 9 Billion USD market cap
 - Migrating 100% on Amazon Web Services
 - 10 M subscribers, 100k DVD titles



AWS Pace of Innovation

(as of Q4 2010)

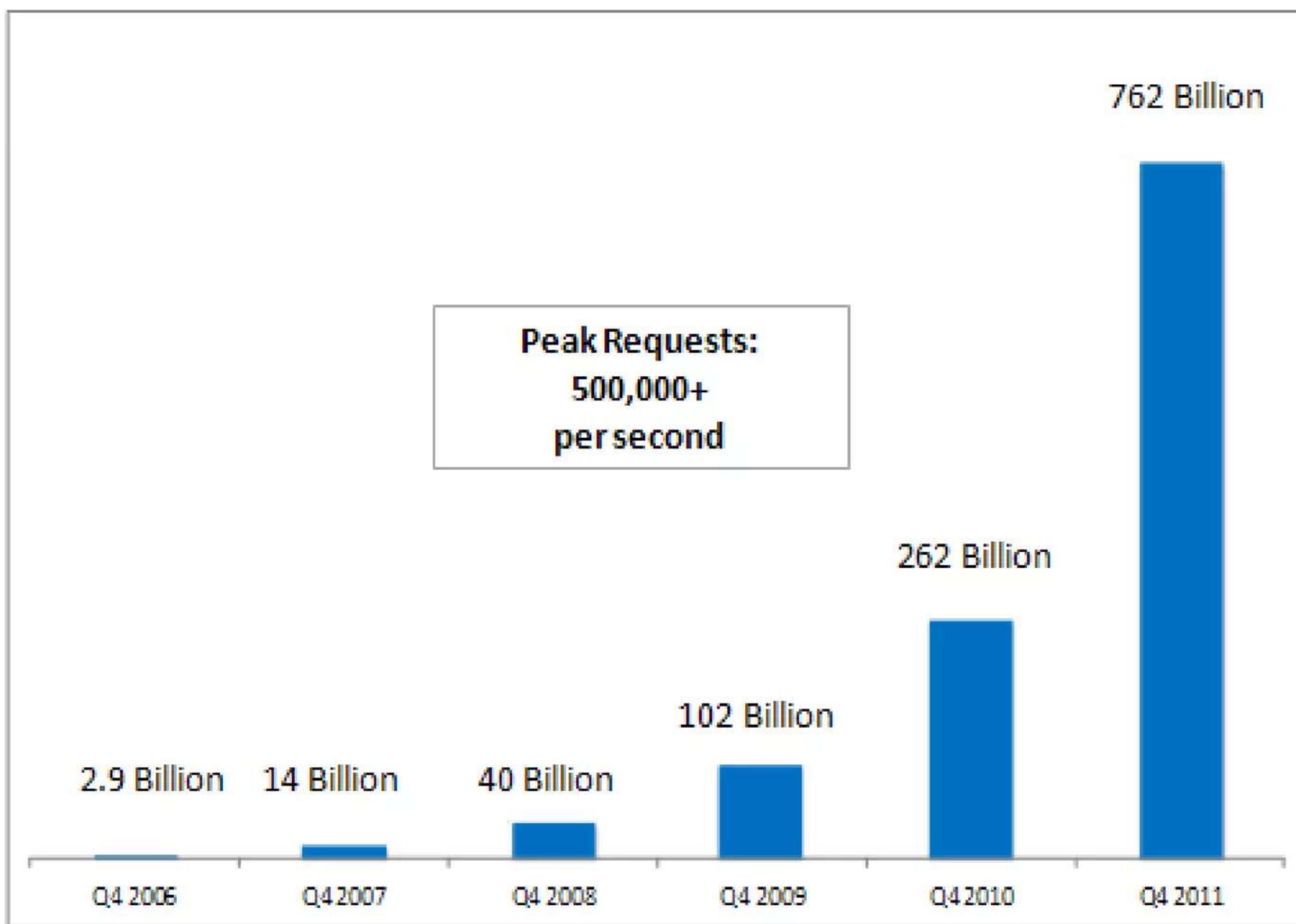




Slide about EC2 what it is?

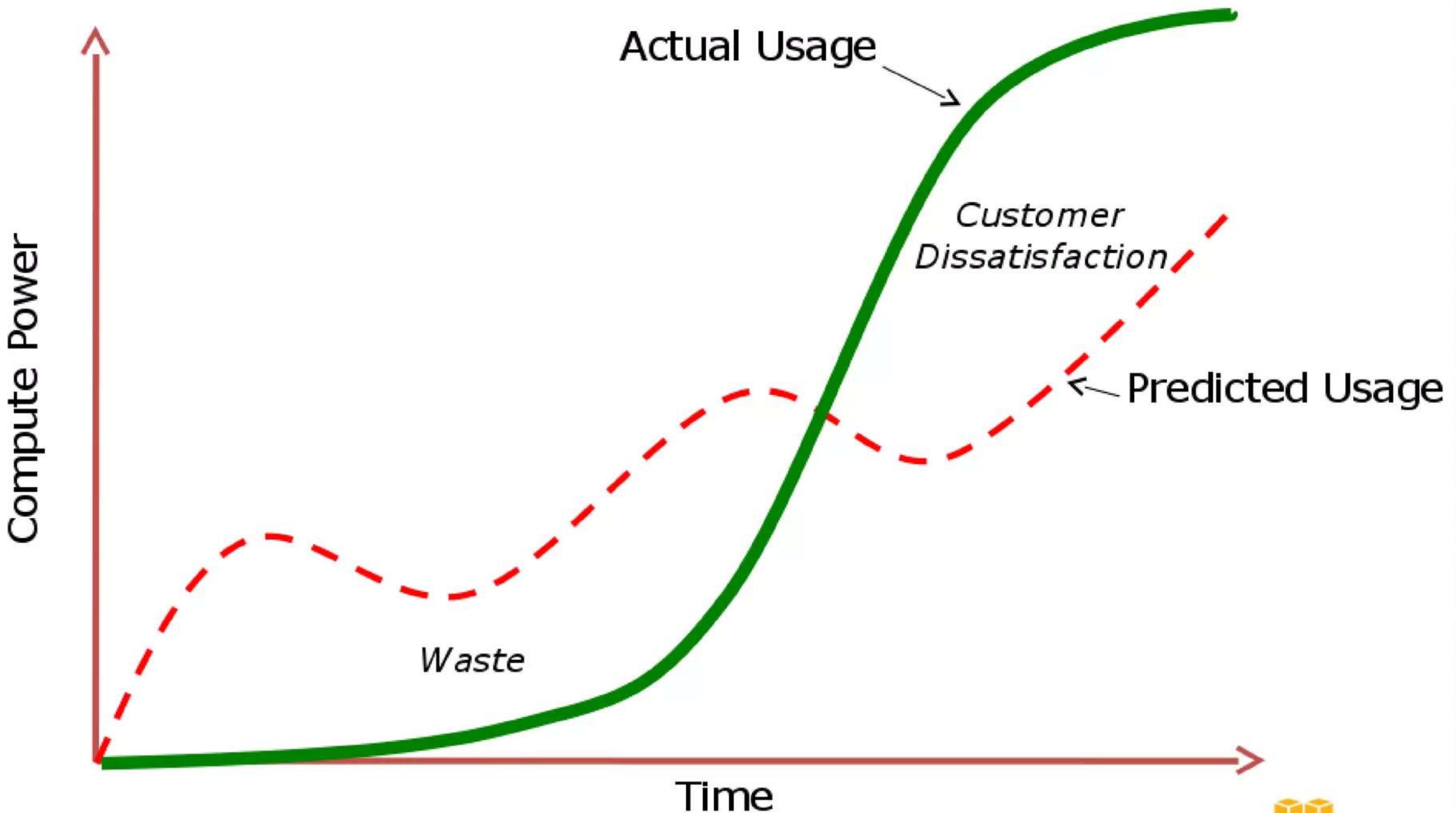
Amazon S3

Total Number of Objects Stored in Amazon S3

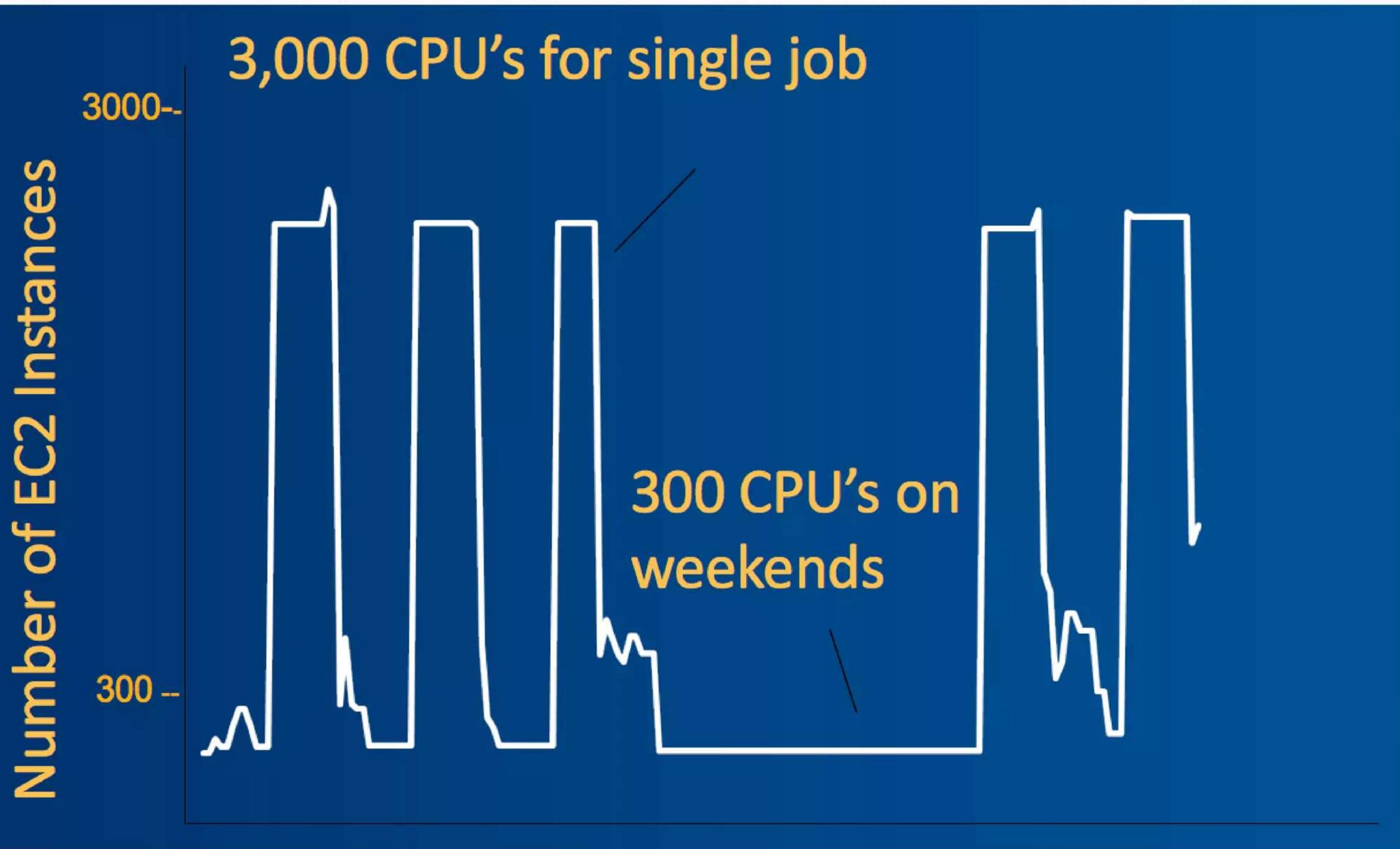




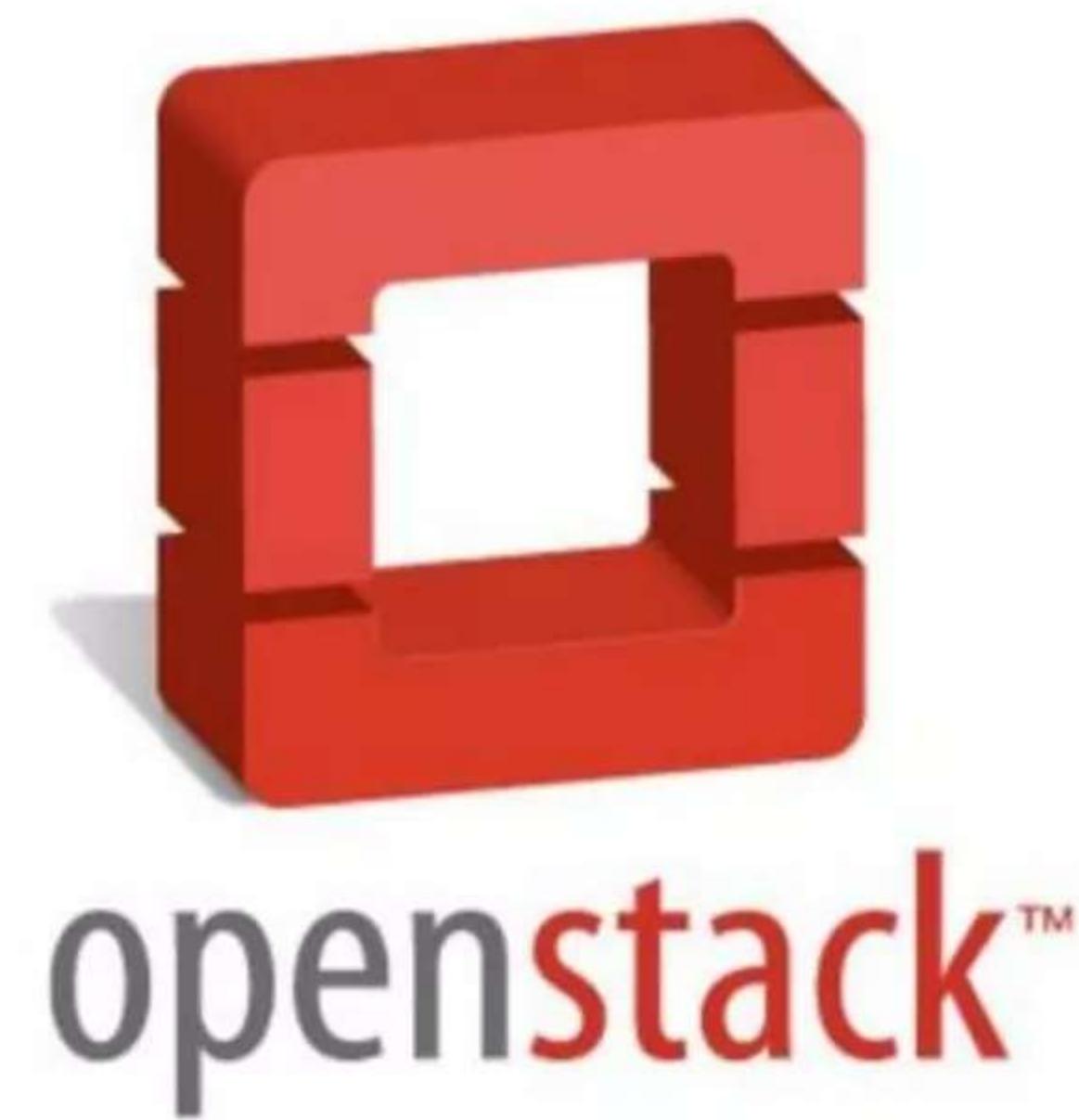
Predicting Infrastructure Needs



Scenario



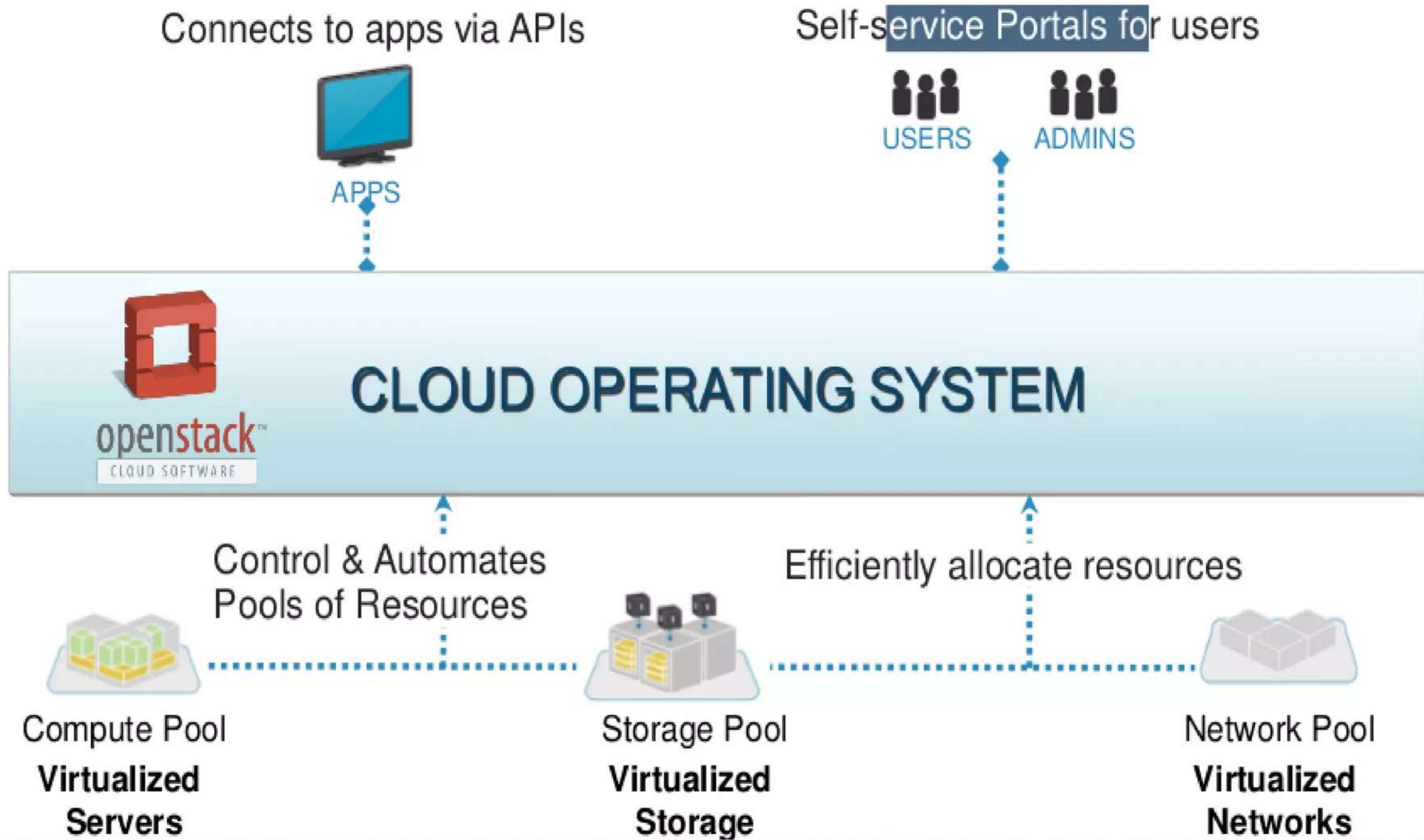
III. Openstack



OpenStack?

“Open source software for building private and
public clouds”

OpenStack, A Kernel of the Cloud OS



Open Source

Apache 2.0 license, NO ‘enterprise’ version

Open Design

Open Design Summit

Open Development

Anyone can involve development process

Open development management via Launchpad &
Github

Open Community

OpenStack Foundation in 2012

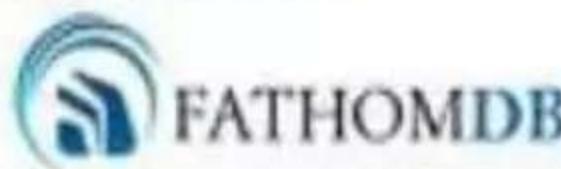
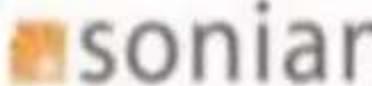
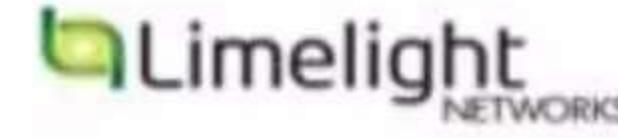
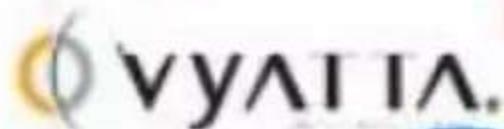
Openstack History

- July 2010 - Initial announcement
- October 2010 - Austin Release
- April 2011 - Cactus Release
- October 2011 - Diablo Release
- April 2012 - Essex Release
- October 2012 - Folsom Release

Hơn 160 đối tác



openstack™



Một số công ty đang sử dụng Openstack



e-commerce / 8th Largest in the World
6000 VMs in Production



Sony Entertainment America
OpenStack Private Cloud



at&t

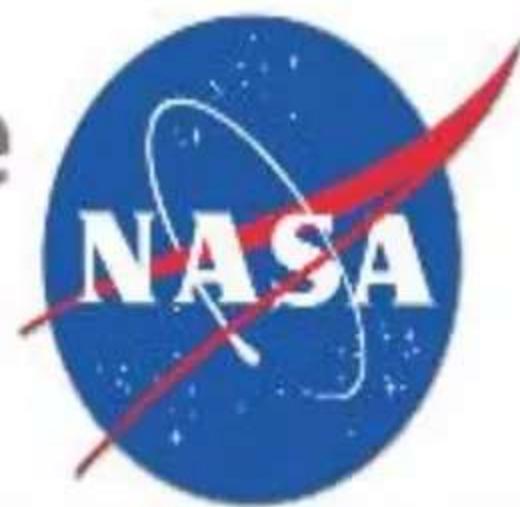
OpenStack-based Cloud Service
Currently, Private Beta



Private Cloud based on OpenStack



Running Commercial Service
based on OpenStack Swift



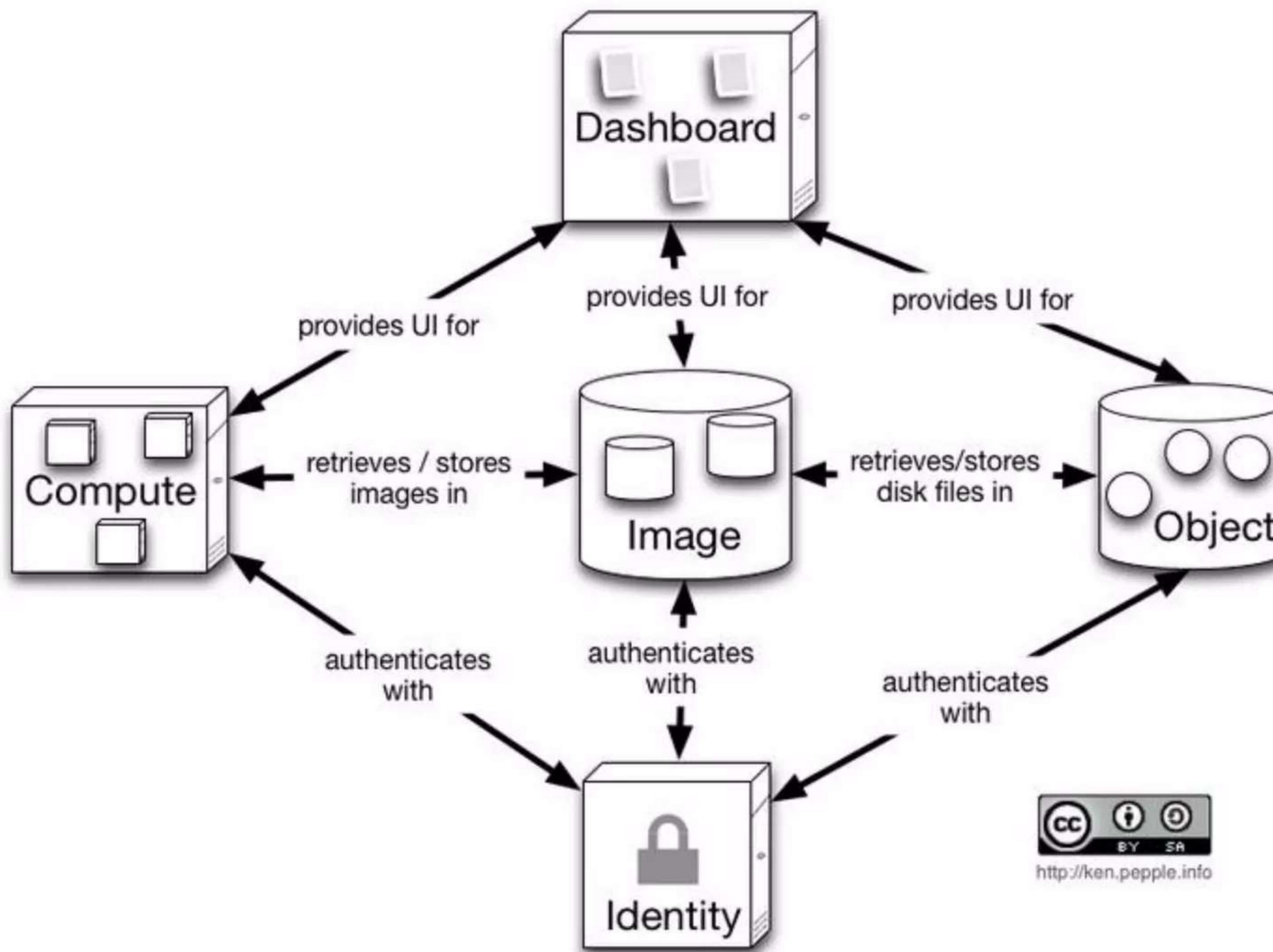
Public Cloud Service based
on OpenStack



Public Cloud Service based
on OpenStack



Các thành phần chính

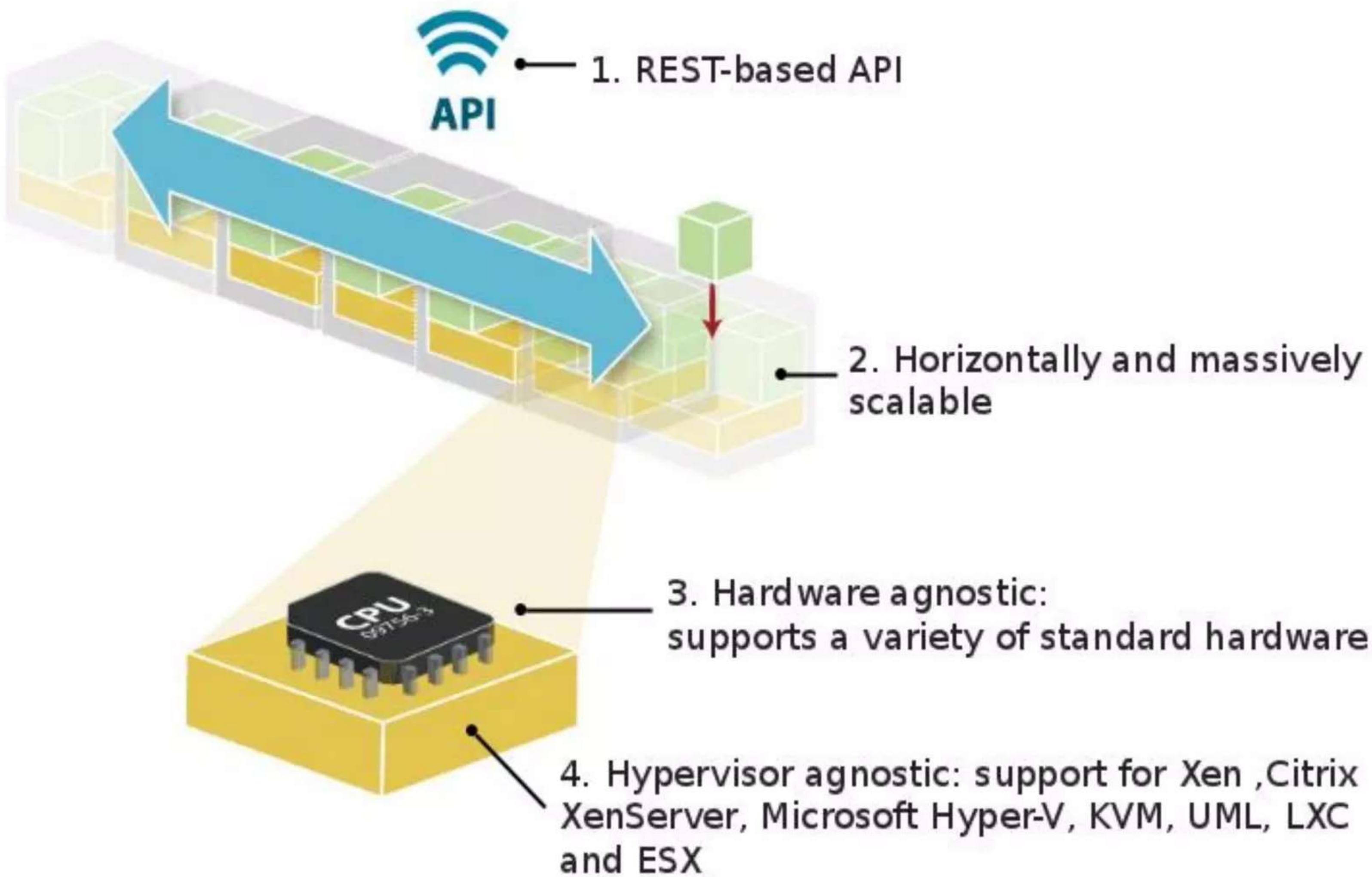


Openstack Compute - Nova

Thành phần quản lý hạ tầng tài nguyên.

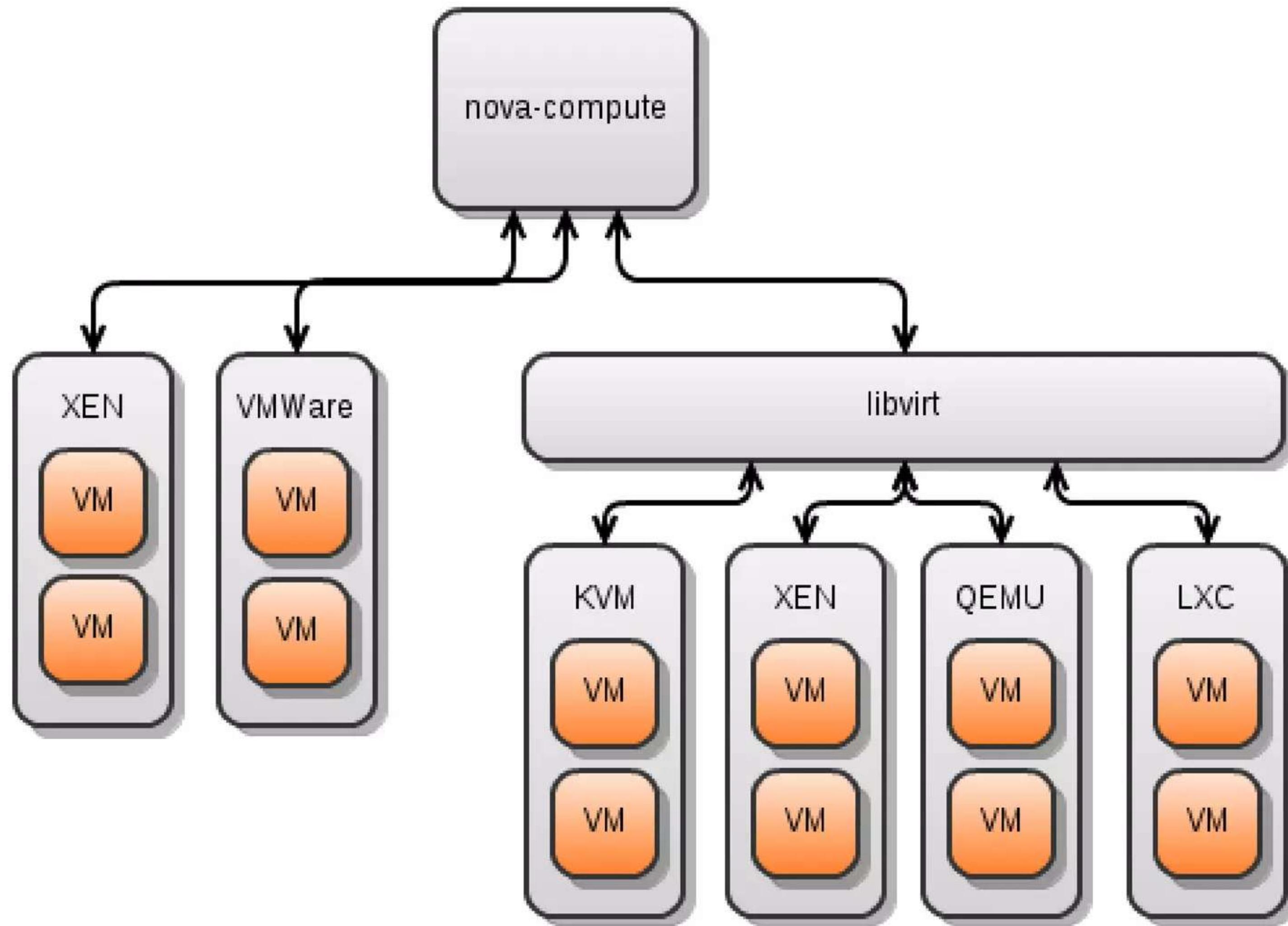
Sử dụng các phần mềm ảo hóa để cung cấp các máy ảo (instance)

Đặc điểm chính



Hỗ trợ các Hypervisor

- ✓ KVM - Kernel-based Virtual Machine
- ✓ LXC - Linux Containers (through libvirt)
- ✓ QEMU - Quick EMULATOR
- ✓ UML - User Mode Linux
- ✓ VMWare ESX/ESXi 4.1 update 1
- ✓ Xen - XenServer 5.5, Xen Cloud Platform (XCP)



Nova Networking

Có 2 kiểu IP trong Nova:

Fixed IPs: được gán cho instance khi khởi tạo, không thay đổi được (private IP)

Floating IPs: được gán thêm cho instance sau khi khởi tạo bởi admin, có thể thay đổi (public IP)

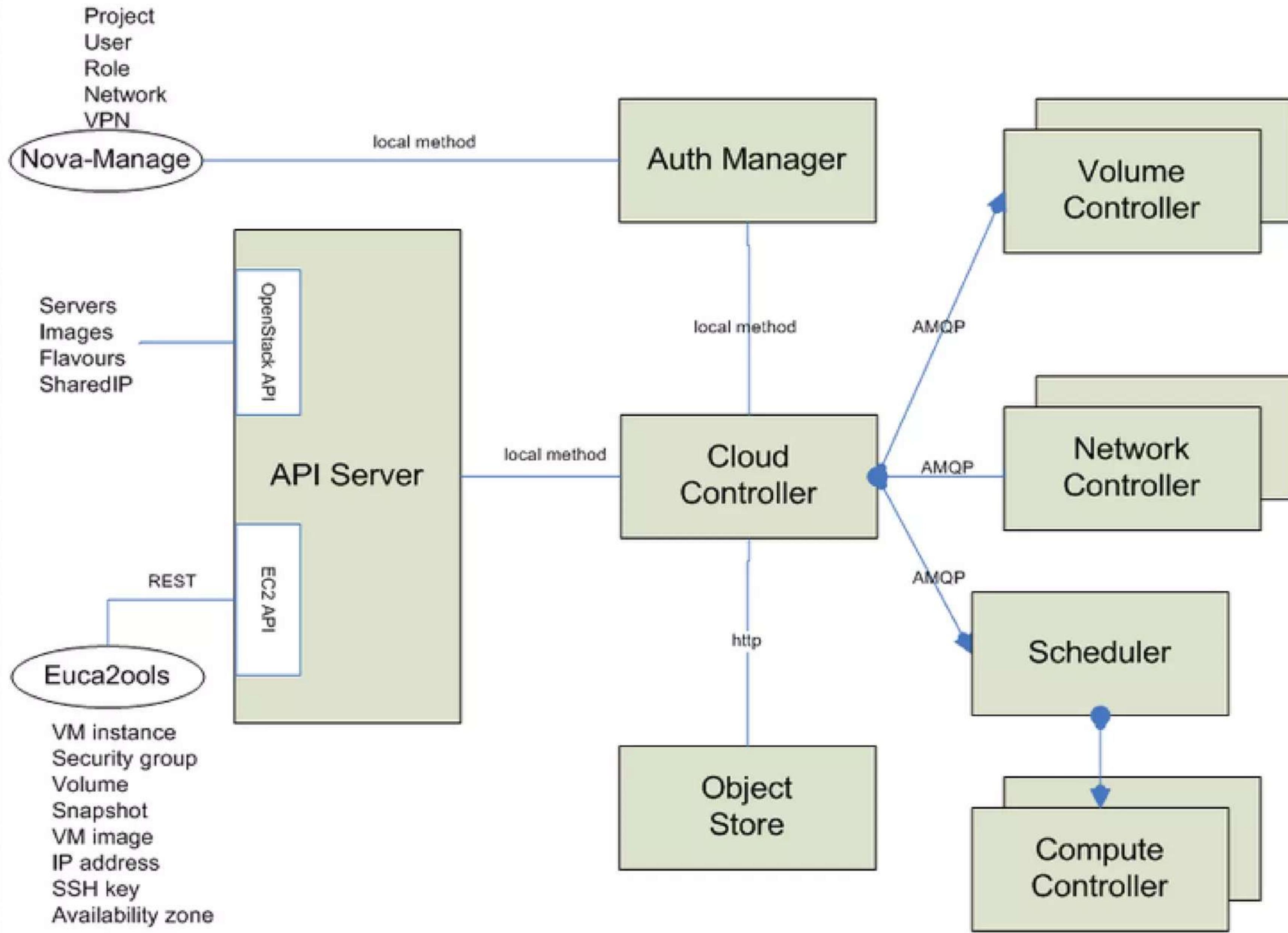
Có 3 kiểu cấu hình cho Fixed IPs:

Flat mode: các instance được gán địa chỉ theo một bridge interface br100.

Flat DHCP mode: tương tự như Flat mode nhưng br100 được cấu hình như một DHCP server sẽ gán IP cho các instance

Vlan DHCP mode: mỗi project sẽ được gán cho một VLAN riêng.

Thành phần chính



Thành phần chính

- Cloud Controller - quản lý và tương tác với tất cả các thành phần của Nova
- API Server - giống như một Web service đầu cuối của Cloud Controller
- Compute Controller - cung cấp, quản lý tài nguyên từ các instance
 - Object Store - cung cấp khả năng lưu trữ, thành phần này đi cùng với Compute Controller
- Auth Manager - dịch vụ xác thực cho user.
- Volume Controller - lưu trữ theo block-level - giống như Amazon EBS
- Network Controller - tạo quản lý các kết nối trong virtual network để các server có thể tương tác với nhau và với public network
- Scheduler - chọn ra compute controller thích hợp nhất để lưu instance.

Users & Projects (Tenants)

- Cloud Administrator (admin): Global role. Toàn quyền trong hệ thống.
- IT Security (itsec): Global role. IT security. Cách ly bất cứ instance nào trong bất kì project nào.
- Project Manager (projectmanager): Projecrole. Mặc định cho người sở hữu project. Thêm bớt user vào proj, tương tác với các img, chạy instance.
- Network Administrator (netadmin): Project role. Cấu hình tường lửa, và các rule cho network, gán public IP cho instance.
- Developer (developer): Project role. Mặc định cho user.

Openstack Storage – Swift

Lưu trữ dữ liệu (object) linh hoạt đến hàng Petabytes trên các cụm server.

Giảm thiểu sự dư thừa.

Nâng cao hiệu suất, khả năng tương tác với người dùng.

<http://swift.openstack.org/>

Thành phần chính

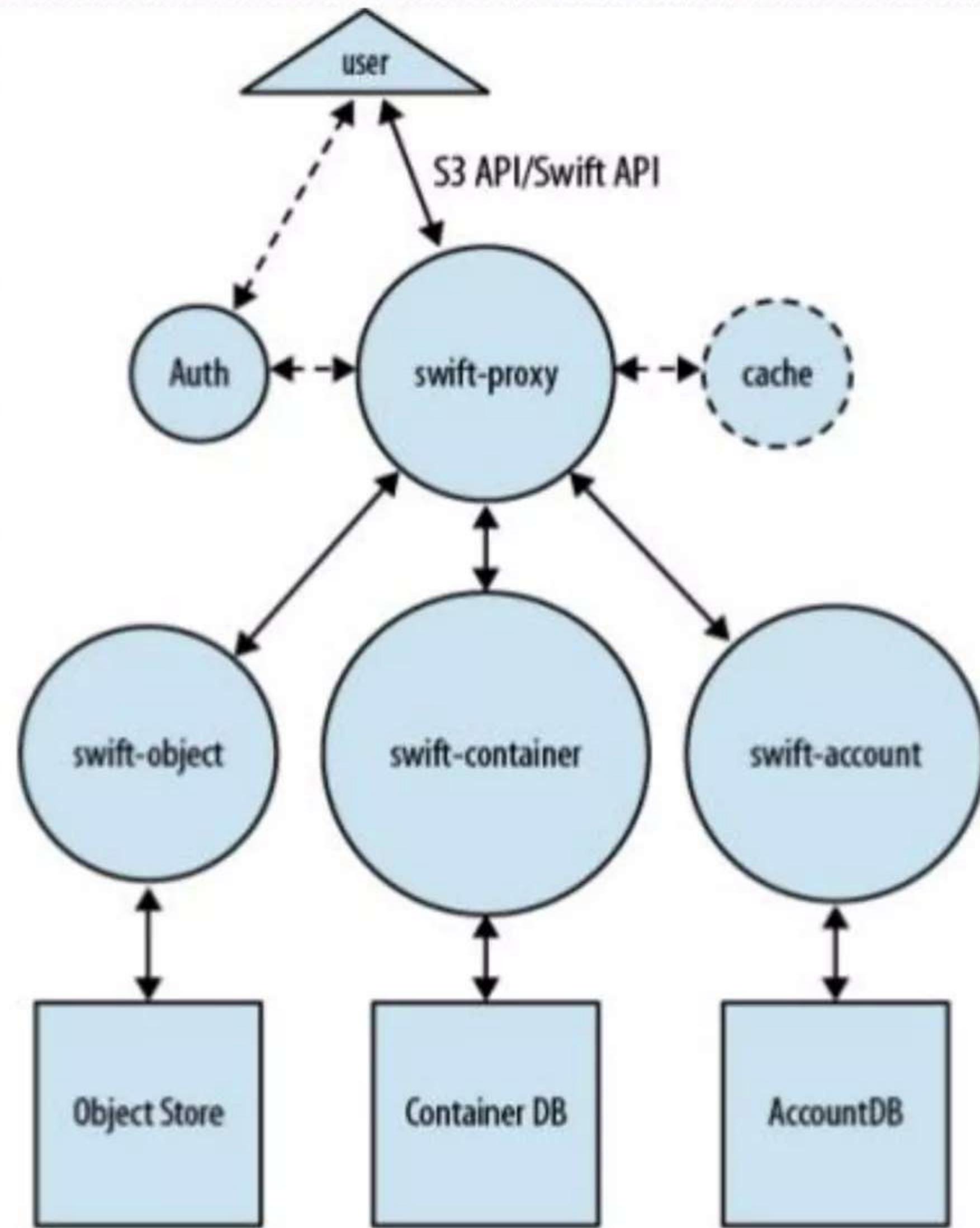
Proxy Server - nhận các request và chứng thực user.

Object Server - lưu trữ, quản lý các đối tượng được lưu.

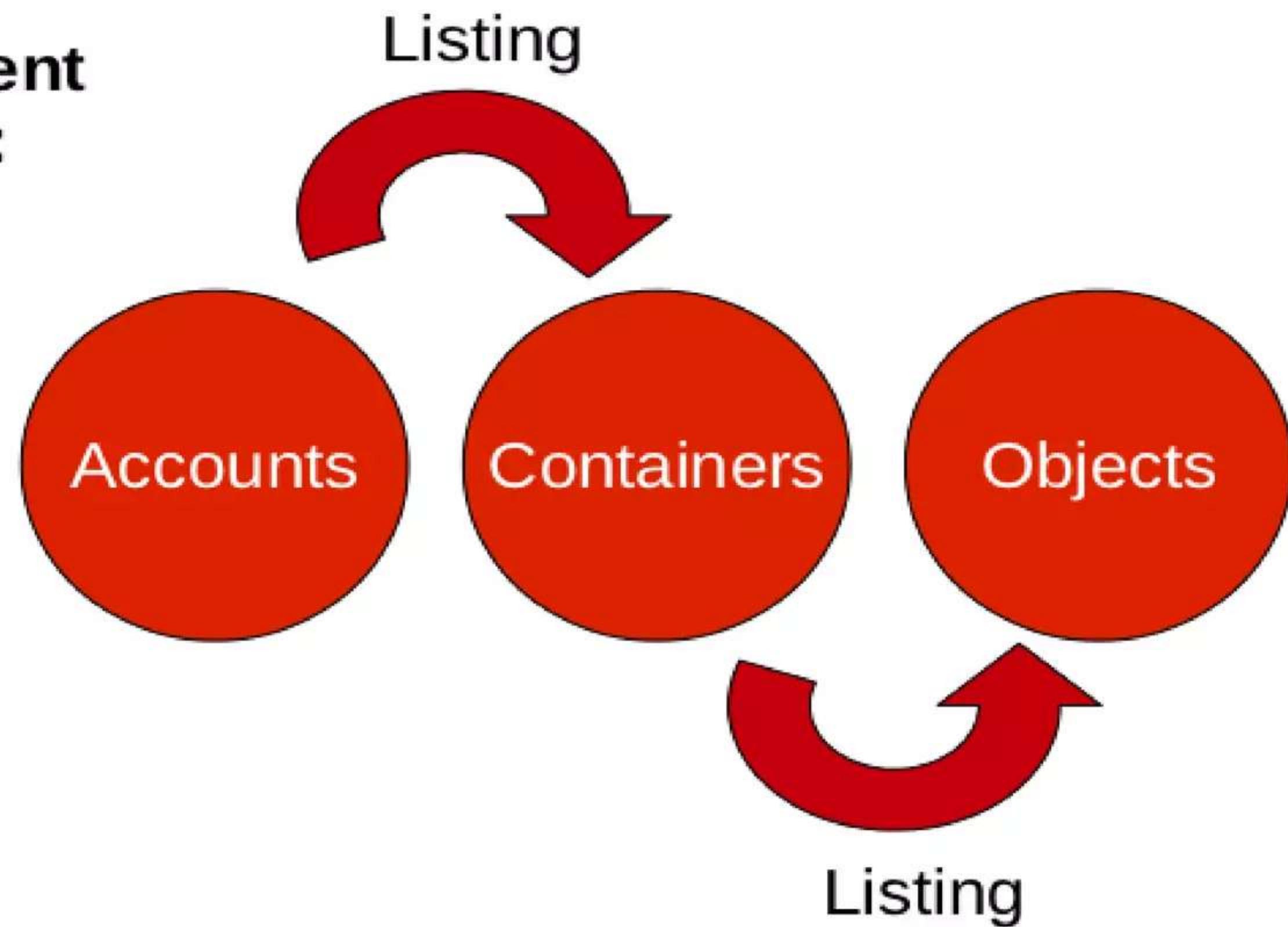
Container Server - lưu trữ thông tin và trả về danh sách các object đang được lưu bên Object Store.

Account Server - cũng giống như Container Server nhưng nhiệm vụ của nó là quản lý danh sách các Container

The Ring - Thành phần này sẽ tạo một ánh xạ giữa tên của các thực thể được lưu trên đĩa cứng và địa chỉ vật lý của nó.



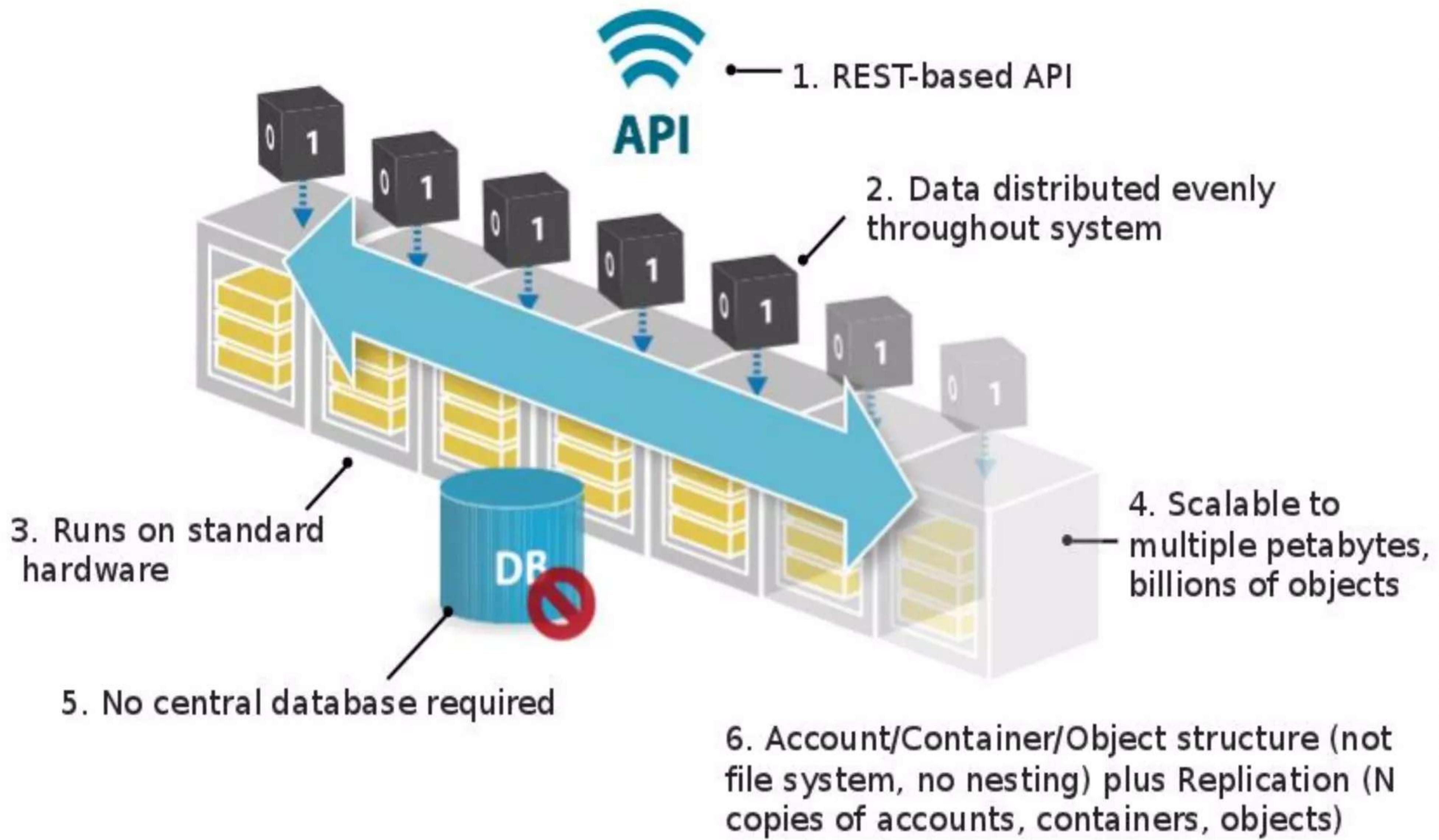
3 Different entities:



The Ring: location of an entity in the cluster

- Three rings (were intended for the Elves)
- Weights can be used to balance the distribution
- Three different logical levels

Đặc điểm chính



Swift Operations

- Managing the rings (adding/removing devices, zones, search for devices, rebalance the ring)
- Upgrading services (one zone at a time)
- Handling driver failure (unmount; optionally remove it from the ring, mount a new EMPTY drive)
- Zone failure (temporal: nothing!)
- Detecting failing disks (device audit)
- Object auditor (manually after a system crash)

Openstack Image Service - Glance

Glance cung cấp các dịch vụ khai báo, lưu trữ, quản lý các virtual machine images.

Hỗ trợ nhiều định dạng: raw, vhd, vmdk, vdi, iso, qcows2, aki, ari, ami

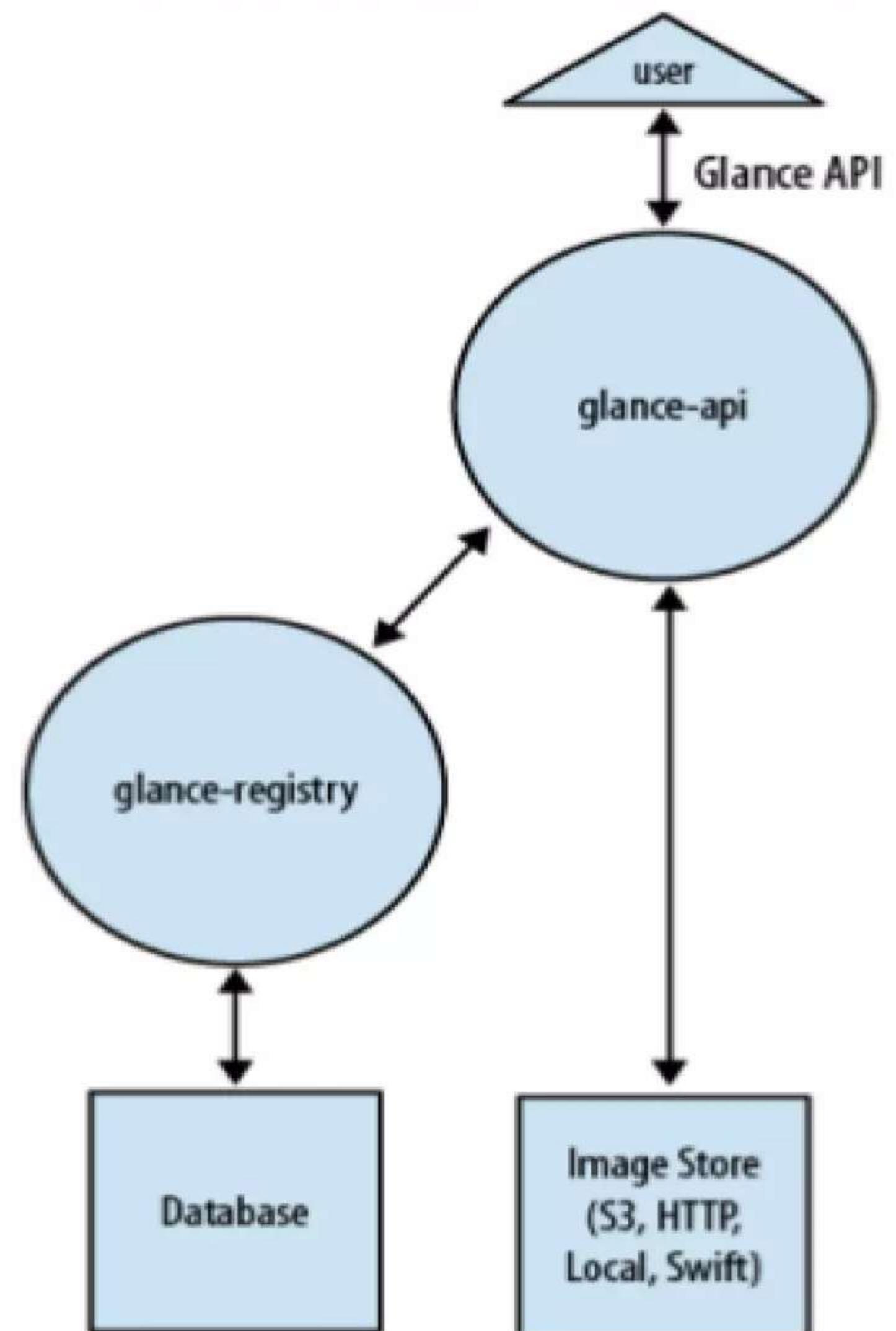
<http://glance.openstack.org/>

Thành phần chính

Glance API server - nhận các hàm gọi API

Glance Registry server - lưu và cung cấp các thông tin (metadata) về image

Image Storage - lưu trữ các file image

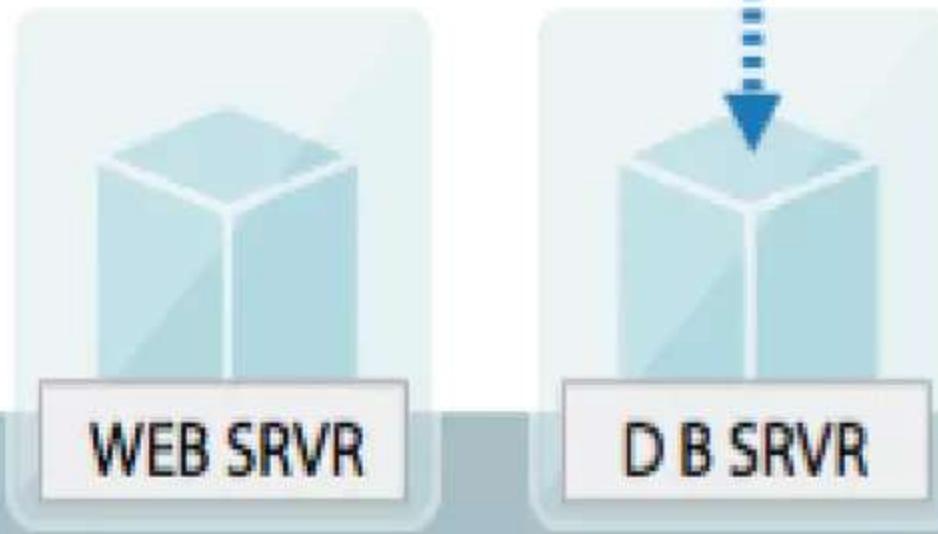


Đặc điểm chính

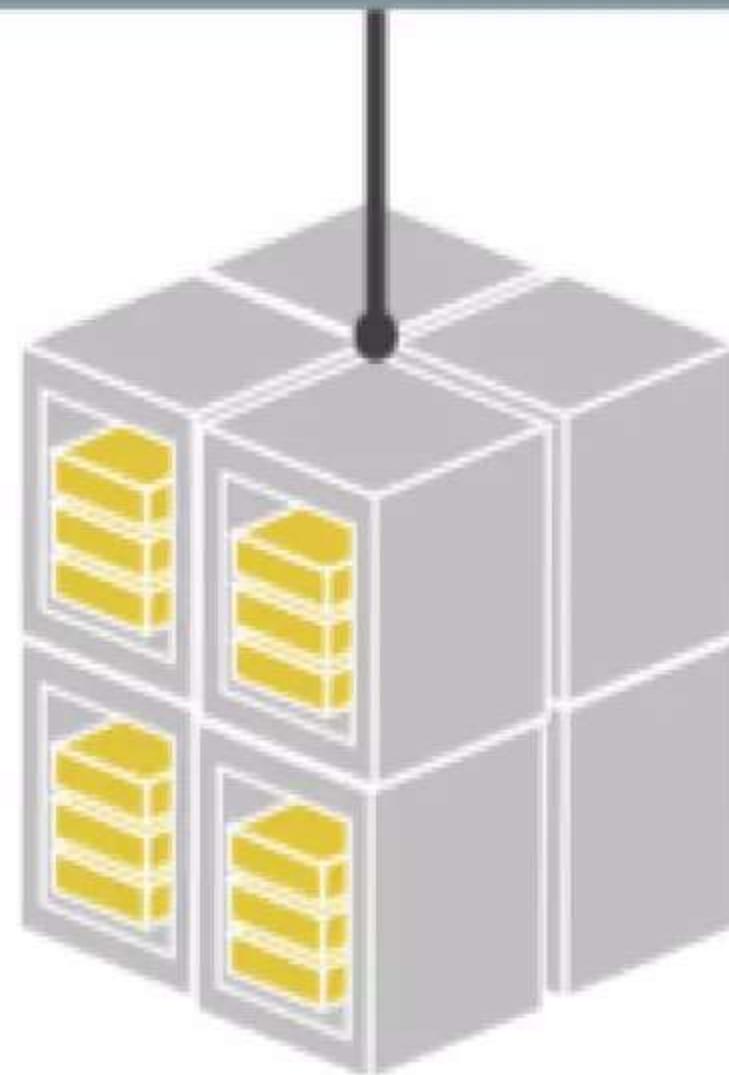
1. Store & retrieve VM images



2. REST-based API



3. Compatible with all common image formats



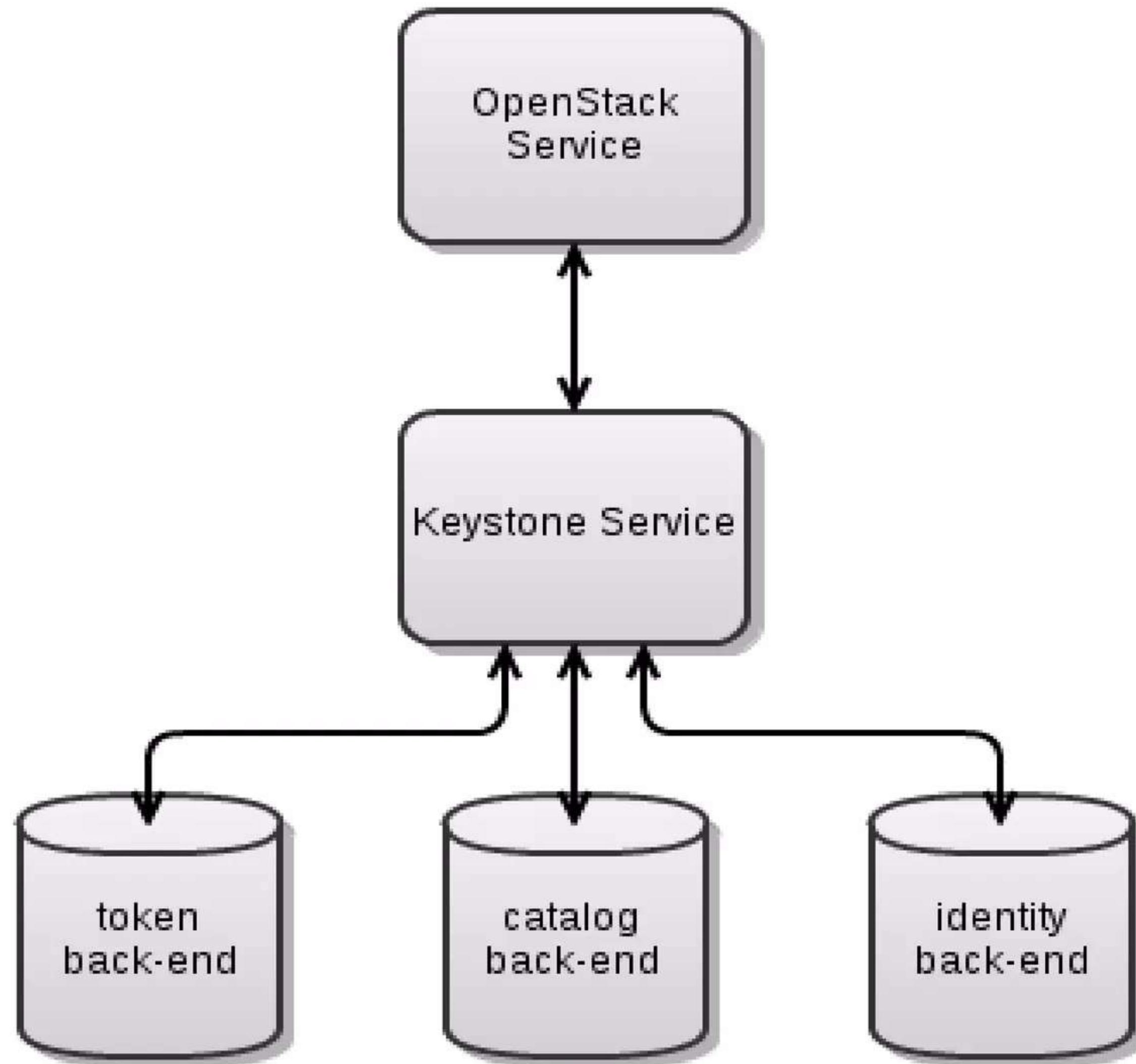
4. Storage agnostic: Store images locally, or use OpenStack Object Storage, HTTP, or S3

Hỗ trợ các định dạng

Disk Format	Description
raw	This is an unstructured disk image format
vhd	This is the VHD disk format, a common disk format used by virtual machine monitors from VMWare, Xen, Microsoft, VirtualBox, and others
vmdk	Another common disk format supported by many common virtual machine monitors
vdi	A disk format supported by VirtualBox virtual machine monitor and the QEMU emulator
iso	An archive format for the data contents of an optical disc (e.g. CDROM).
qcow2	A disk format supported by the QEMU emulator that can expand dynamically and supports Copy on Write
aki	This indicates what is stored in Glance is an Amazon kernel image
ari	This indicates what is stored in Glance is an Amazon ramdisk image
ami	This indicates what is stored in Glance is an Amazon machine image

Openstack Identity - Keystone

Cung cấp khả năng chứng thực, đặt các chính sách phân quyền cho các project trong Openstack.



Các kiểu dữ liệu trong Keystone

User: có các credential liên kết với các 'tenant' tương ứng.

Tenant (project) chứa một hoặc nhiều user.

Role: Xác định các quyền trong tenant tương ứng cho các user.

Token: xác định các credential liên kết giữa user và tenant.

Các thao tác cài đặt

Add tenants

Add users

Add roles

Grant roles to users

Add endpoint templates

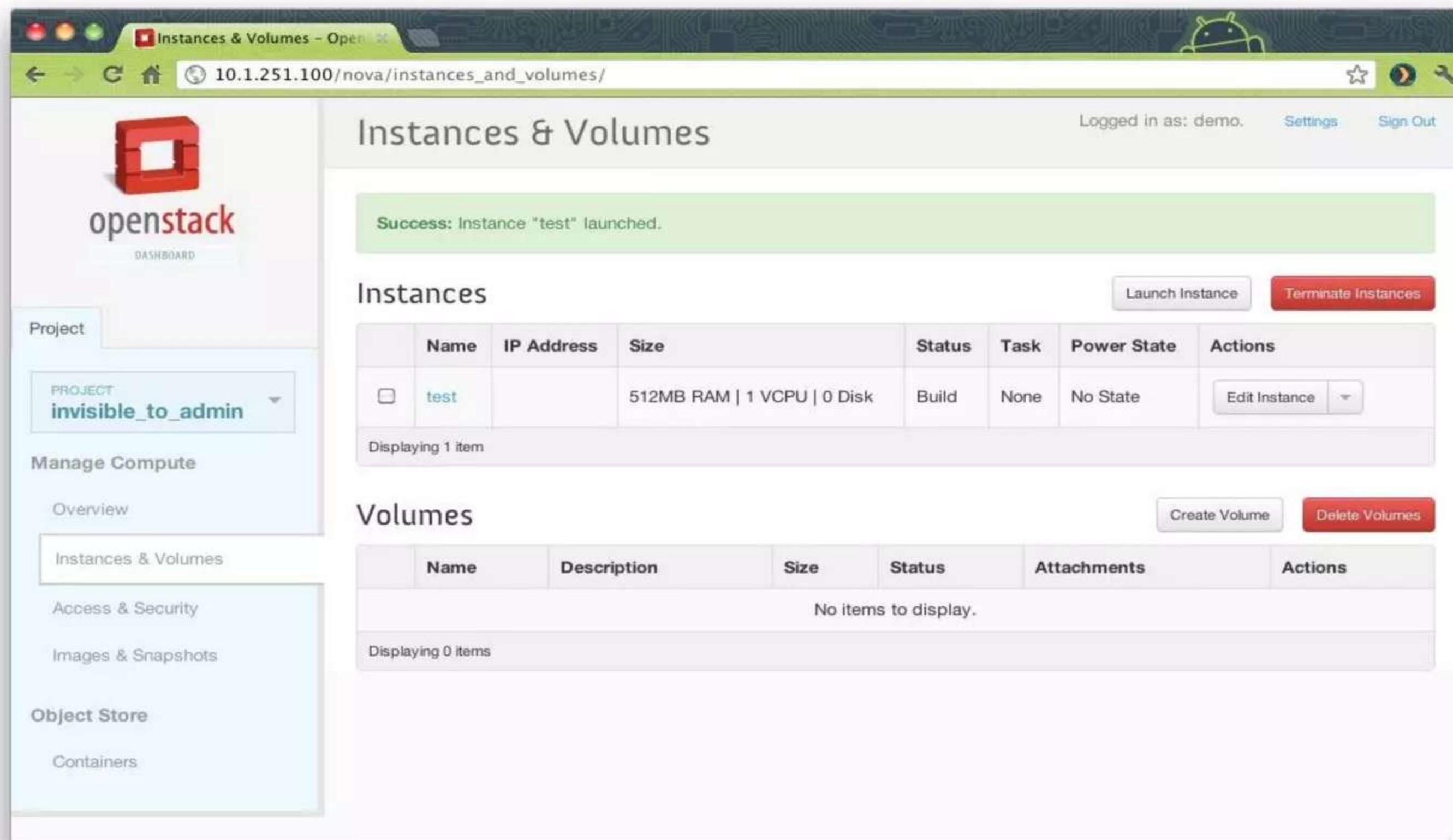
Map endpoint templates to zones

Openstack Dashboard – Horizon

Dashboard cung cấp một giao diện web nhằm tương tác quản lý các thành phần còn lại của Openstack.

Kết hợp với Keystone để chứng thực user.

<http://horizon.openstack.org/>



Horizon

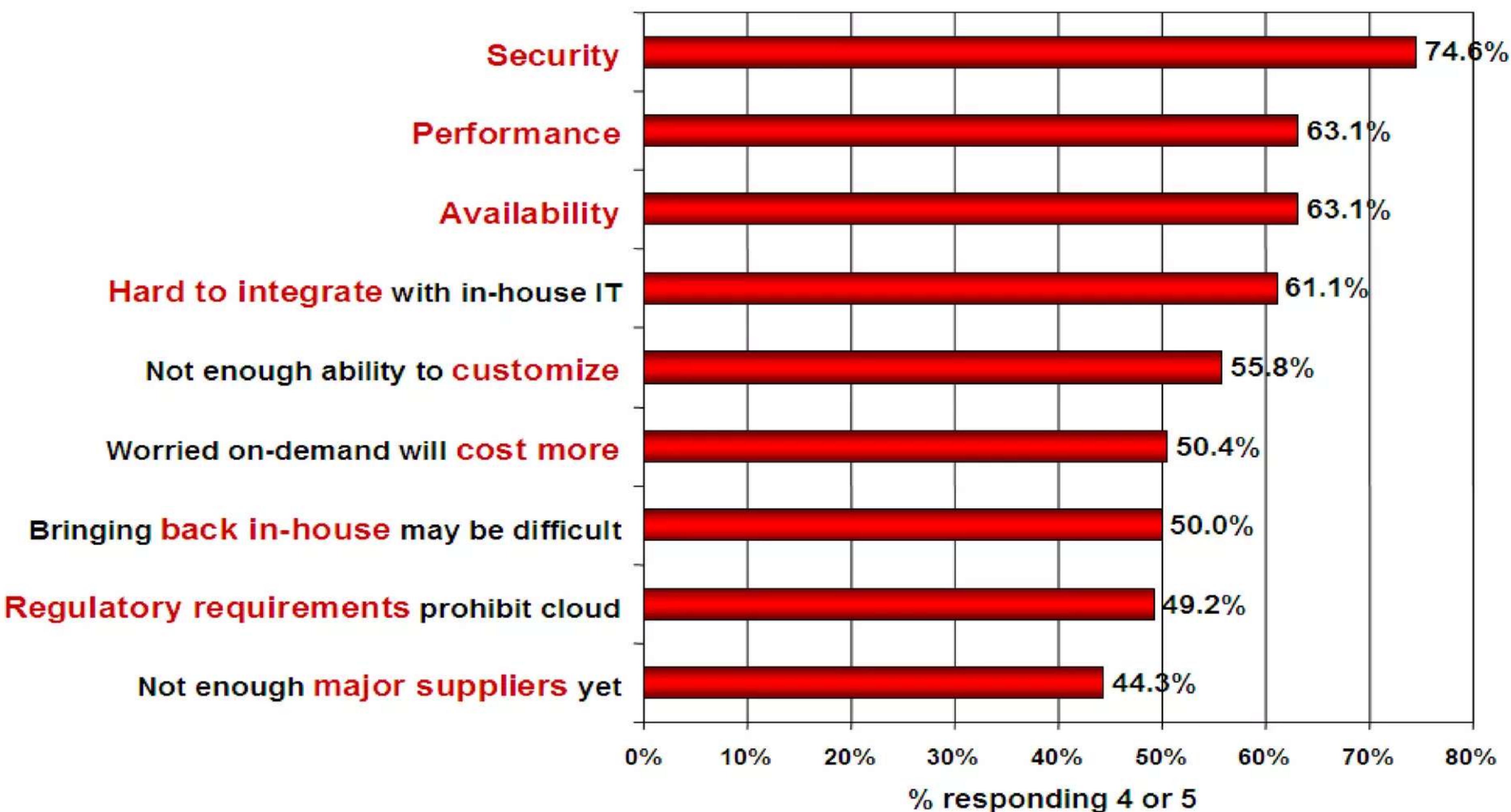
- "Stateless"
- Chưa hỗ trợ một số thao tác: đẩy img lên glance, di chuyển instance...
- Chưa hỗ trợ tốt (tất cả) các API
-

IV. Cloud Computing Security



Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

CSA - Cloud Security Alliance

Cloud management và Operation

- **Cloud management**
 - Quản lý và phát hiện các mối nguy hiểm
 - Quản lý và bảo mật thông tin, dữ liệu
 - Di chuyển data giữa các nhà cung cấp, hoặc sang mô hình truyền thống
- **Cloud operation**
 - Các nguy cơ security truyền thống, vấn đề recovery khi có thiên tai Data Center Operations
 - Khả năng phản ứng với các sự cố xảy ra
 - Bảo mật ứng dụng
 - Mã hóa và quản lý khóa (Key Management)
 - Quản lý việc nhận dạng, quyền hạn, và truy cập vào hệ thống
 - Ảo hóa
 - Security as a Service

NIST (National Institute of Standard and Technology)

- Quản lý và kiểm soát
- Sở hữu dữ liệu, *insider threats* và *risk management*
- Kiến trúc cloud
 - *Cloud computing software* - OpenStack, OpenNebula, ...
 - *Hypervisor (VMM)*
 - *Virtual traffic* và *VM images*
 - *Client-side* và *Server-side protection*
- Quản lý việc truy cập và chứng thực
- *Software Isolation*
- *Data Protection*
- *Availability (DDoS)*
- *Khả năng phản ứng* với các sự cố xảy ra

Security requirements

- **Availability management:** độ sẵn sàng của hệ thống trong mọi trường hợp
- **Access control management:** quản lý việc truy cập
- **Vulnerability and problem management:** khả năng ngăn cản các lỗ hổng và thâm nhập
- **Patch and configuration management:** update hệ thống thường xuyên ngay khi có bản vá và cấu hình
- **Countermeasure:** các biện pháp đối phó khi gặp sự cố về security
- **Cloud system using and access monitoring:** quản lý việc sử dụng và truy cập của user với cloud.

Security solutions

- **Điều khiển việc truy cập vào thông tin, dữ liệu**
- **Quản lý quyền truy cập của users**
- **Quản lý và giám sát truy cập và các dịch vụ mạng, các Oss, và các ứng dụng.**
- **SaaS:**
 - tập trung vào quản trị người dùng, các cơ chế chứng thực mạnh và sử dụng one-time password, Single Sign On, quản lý quyền hạn, ...
- **PaaS:**
 - trọng tâm vào tầng network, servers, và các platform hạ tầng ứng dụng. Người dùng chịu trách nhiệm quản lý các ứng dụng đặt trên platform PaaS.
- **IaaS:**
 - truy cập vào các server ảo, network ảo, hệ thống lưu trữ ảo, và ứng dụng trên một IaaS platform được thiết kế và quản lý bởi khách hàng. Việc quản lý truy cập ở mô hình IaaS bao gồm 2 phần chính: quản lý host, network, và ứng dụng thuộc sở hữu của cloud provider trong khi người dùng phải quản lý việc truy cập đến các server ảo, lưu trữ ảo, networks ảo, và các ứng dụng chạy trên các virtual servers

Security solutions

- **Partitioning:** nâng cao hiệu suất tính toán của các ứng dụng.
- **Migration:** Sự linh hoạt và khả năng dịch chuyển các hệ thống CSDL nhưng vẫn đảm bảo trong suốt.
- **Workload analysis and allocation**
- **DDoS**

OpenStack Security

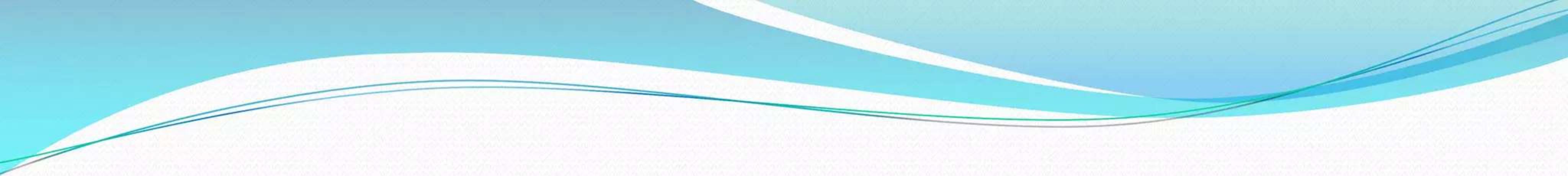
- **Keystone** (hay OpenStack Identity) chính là thành phần chính cho security với các chức năng chứng thực, chính sách, ...
- **User và Project**: việc tạo các user và project cũng đảm bảo việc truy cập chứng thực khi user không thể truy cập vào các project không thuộc chủ quản của mình – chức năng User và Project trong Nova.
- **Keypairs**: Tạo các khóa để gán cho instance khi khởi tạo cũng là 1 công cụ đảm bảo security khi chỉ có user được cấp khóa mới đủ thẩm quyền truy cập instance.

Keystone

- Các thành phần của Keystone
 - Endpoints - Nova, Swift, Glance chạy trên 1 port và URL xác định gọi là endpoint
 - Regions – vùng server vật lý chạy các dịch vụ OpenStack
 - User - A keystone authenticated user.
 - Services – các dịch vụ quản lý bởi keystone.
 - Role - gán quyền cho users.
 - Tenant – cũng chính là project, bao gồm các dịch vụ endpoint, role gán cho user thuộc project.

Keystone

- Keystone cung cấp 2 phương thức chứng thực:
 - username/password
 - token based
- Keystone cung cấp các dịch vụ bảo mật sau
 - Token Service (thông tin chứng thực 1 user)
 - Catalog Service (các dịch vụ dành cho 1 user)
 - Policy Service (quản lý và hạn chế việc truy cập đến các dịch vụ đối với từng user hay group).



Demonstration
Thank you !