Cloud Computing
Fall 2020

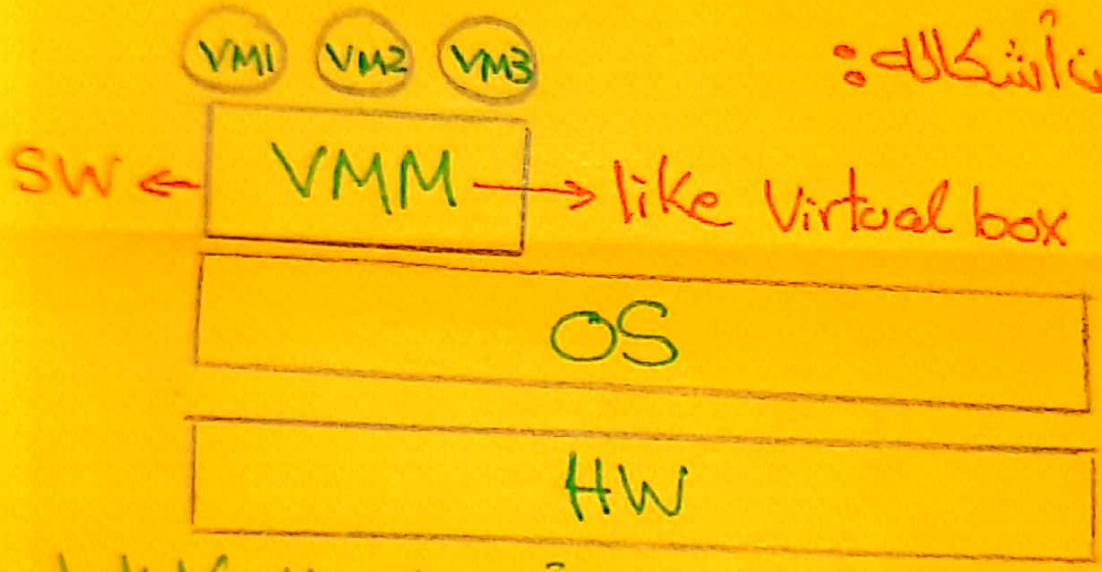
Dr. Samah Rahamneh

Cloud Computing?

- a style of computing where massively scalable and elastic IT capabilities are provided as a service to external customers using internet technology.
- A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (the National Institute for Standards and Technology of the United States). -> NIST

* Virtualization *

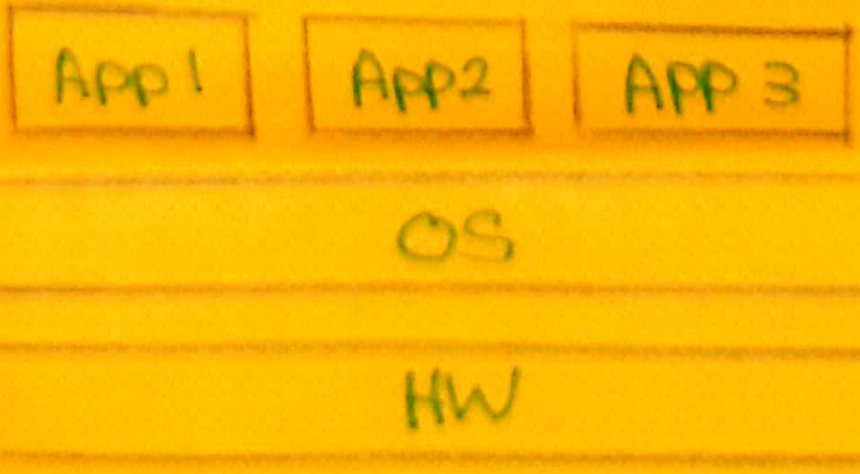
* بشكل من أشكاله:



* لو خربت وحدة الباقي ما بتأثر عكس الشكل التقليدي

* الشكل التقليدي:

* بالعادة الـ VMM بكون فايل عالـ HW كمثل ما بتأثر حالة الـ OS



* لو خرب الـ OS كلهم بيتأثروا

Cloud Computing (Continued)

عملية سريعة

- A type of parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on Service Level Agreements (SLAs) established through negotiation between the service providers and consumers.

حرفيا cloud service provider

الخدمة مايقل كن المتفق عليه هو الـ Consumer

History of Cloud Computing

أجهزة ضخمة جدا

Enabling Technologies of Cloud Computing

Mainframes →

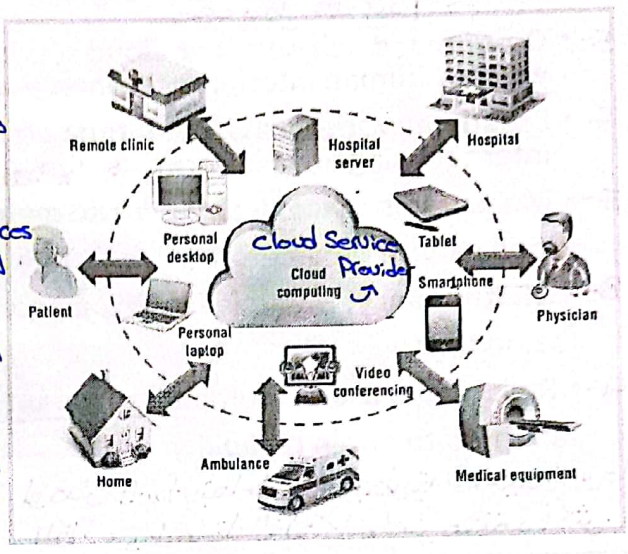
internet →

virtualization →

cloud computing

Cloud Ecosystem → Cloud components

- Cloud service providers → مقدّم الخدمة مثل أمازون
- Cloud users → Cloud الـ users اي بستخدم و بيبنوا موقع أو تطبيق معين وخلوه متاح resources للجميع
- Cloud end users → الـ users اللي بيستخدموا الأشياء المبنية والجلهزة
- Cloud carrier → internet Service Provider الـ → نحتاجه ضروري في الـ Cloud



Cloud Computing Characteristics (1)

1- **Large-scale computing resources:** economies of scales. → data centers الـ بتكون ضخمة فبحصل فائدة اقتصادية
2- **Shared resource pooling:** Pooling of virtual and physical resources into the cloud provides an abstraction of resource location. → VM storage
3- **Dynamic resource scheduling:** cloud resources are provisioned dynamically based on the current demand requirements and ensures that the cloud service capability is being expanded or contracted based on demand.
4- **High scalability:** Cloud computing architecture allows you to add new nodes and servers with no reconfiguration and re-modification requirements to cloud software and infrastructure. → القدرة على التوسع

Cloud Computing Characteristics (2)

↳ Pay as you use

5- • **On-demand self-service :** Cloud services are automatically made available without human interference when required by a potential consumer.

6- • **Broad network access :** Real-time access and use of cloud services via the internet using any platform → بنحتاجها ضروري

7- • **Measured service:** A pay-per-use metering model is being used by the cloud service providers → خدمة مقاسة بالضبط

8- • **Multitenancy:** Multiple users can access the same cloud services at the same time

9- • **Reliability** : use of multiple redundant sites is an approach being adopted to attain reliability → ↳ like Backups

لو صار fault بتعامل معاه بطريقة صحيحة وما يبين للغلط ، وكل ما قل الغلط كل ما صار معتمد أكثر

Cloud Computing Characteristics (3)

← تكاليف بنحتاجها زمان مع وجود الـ cloud صرنا نوفرها

10- • **Cost effectiveness**: No Capital Expenditure (CapEx).

11- • **Efficient resource utilization**: The cloud architecture ensures that resources that are delivered are efficiently utilized and made available only for the period needed

12- • **Green technology:** Cloud computing is an energy-efficient technology that does not require huge power consumption

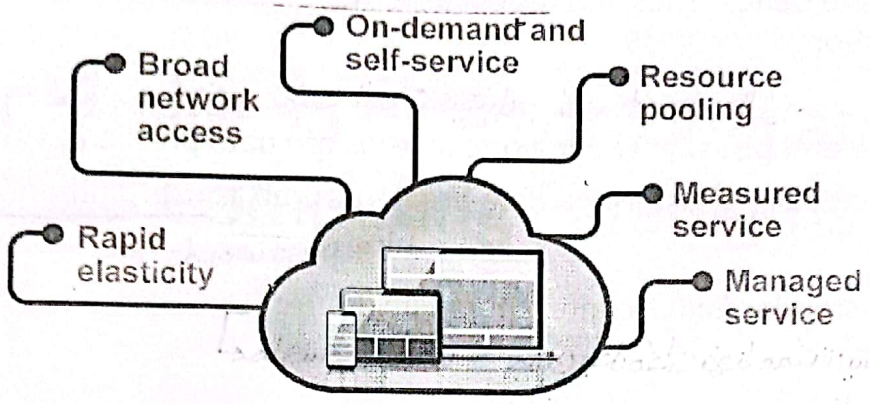
← صديق للبيئة لأنه ما بستهلك طاقة عالية Power .

* DVFS * →

* الهدف منه تقليل البور قدر الإمكان بعمل Scale down .

* العلاقة بين الـ Power consumption والـ Freq طردية .

Cloud Computing Characteristics (4)



Advantages of Cloud Computing

النفقات التجهيزية ← عكسها OPEX → النفقات التشغيلية ← مثل فاتورة الكهرباء
لا برضه بنخف

- **Economical**: No upfront investment (CAPEX)
- **Almost unlimited storage**: Cloud provides access to very large storage space based on users' requirements
- **Backup and recovery**: backup for everything
- **Easy access to information**: anywhere and anytime
- Users need not worry about upgrading the technology stack and software.

Disadvantages of Cloud Computing (1)

1- • **Technical issues**: These issues occur if there is a bad internet connection.

↳ لما أزيد كتير خطوات الأمان حيقابله overhead عالي.

2- • **Security and privacy**: The major concerns are data protection and confidentiality, disaster and data breach as well as user authentication.

like passwords ↵

3- • **Lack of standards:** Pose interoperability issues.

↳ ماكنش Standard يمشي بكل مكان فهنا ممكن يسبب مشاكل لإنه الـ Clouds بتختلف عن بعض ما في اشي يحكموم فالشغل بينهم صعب.

* Security: بعمل حماية لأشياء هتش لمعلومات شخصية.

* Privacy: بعمل حماية للمعلومات الشخصية.

Disadvantages of Cloud Computing (2)

4- • **Continuously evolving**: Hard to catch up!

↳ كل شوي بتطور فصعب تتعلم كل شي.

5- • **Compliance concerns**: Data usage and protection laws differ from one country to another. → حماية البيانات بتختلف من بلد إلى بلد آخر.

6- • **Service migration**: User lock-in to a particular provider is a problem after service migration to the cloud.

↳ الشغل من Cloud Service Provider إلى آخر حيكون صعب لإنه ما في اشي موحد بينهم.

Comparison of Traditional and Cloud Computing Paradigms

الهدف منه تقليل وقت الـ task وتقسيمها لأكثر من جزء.

مثال على الـ Traditional.

Cluster Computing

مجموعة من الأجهزة مشبوكة على وحدة LAN

- set of stand-alone systems inter-connected via a local area network or a group of linked computers, working together as a single integrated system for scaling workloads.

ممكن الأجهزة تكون متجانسة أو مختلفة.

- The main motivation for cluster computing is performance improvement, fault tolerance, scalability, huge cost-savings, throughput, redundancy, high memory, enormous speed, load balancing and high availability. It is a local network that is often characterized by high speed interconnections and centralized job management and scheduling system

لو اشي خرب ما بنحس فيه

تقسيم الشغل

دائمًا متاح، أكيدهو معا ٪ بس أفضل اشي

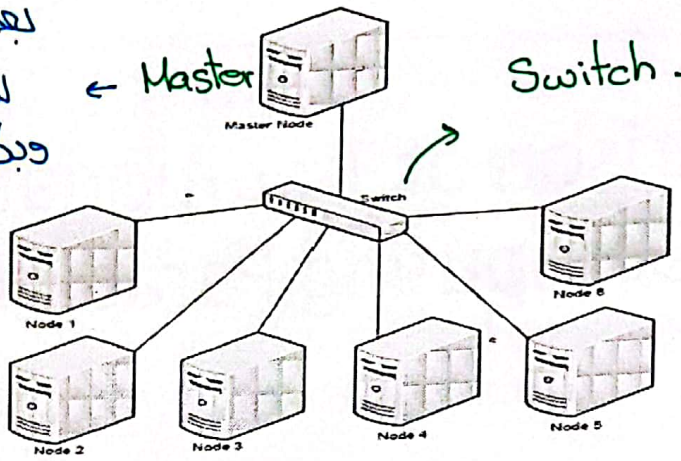
*لو في task بدها ١٠ دقائق لتخلص جبنا ١٠ أجهزة لنقسم عليها هذا الـ task مارح يكون Parallel بنسبة ١٠٠٪ فمارح تكون دقيقة بالزبط.

Cluster Computing (1)

Schedule بعمل
Slaves لل ← Master
وبكون عارف مين بشتغل
ومين خربان
وكل واحد شو بنفذ.

Slaves

Switch → ما بنستبدله
Router بـ
لإنه الـ Router
معناه كل
جهاز مشبوك
Network بـ
مختلفة



Cluster Computing

Grid Computing (1)

الفرق بين الـ grid والـ clusters

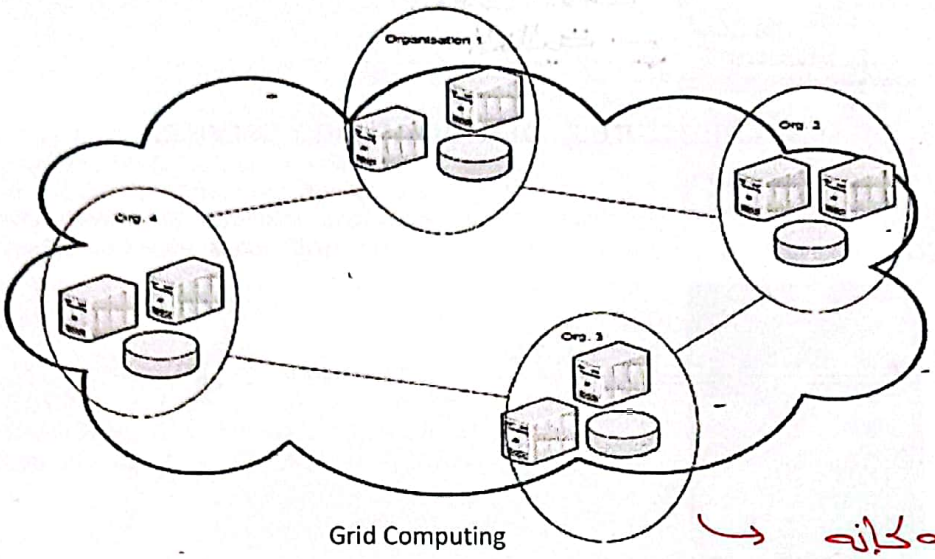
- Consolidation of several computing resources from several supervisory domains into one or more logical entity, coordinated with a high-performance distributed grid and applied to solving large batch processing problems.

- In grid computing, computing resources are located on loosely-coupled but geographically dispersed, distributed and heterogeneous networks unlike in cluster computing.

ما بكونوا موجودين
مختلفة.

بنفس المنطقة مشان الـ cluster لازم نفس الـ LAN

Grid Computing (2)



Grid Computing

↳ بصير أشوفه كإنه one user entity

Business drivers of cloud computing adoption

↳ business ليه بستخدم الـ Cloud

- Help to pursue new business opportunities
- Upfront costs reduction
- Potential improvement in business continuity
- Potential reduction in carbon footprint

Future of Cloud → لازم يحلوا التلاث نقاط التالية

1 • Standardization of architectures, platforms, and services.

2 • Hybrid cloud

3 : Cloud of clouds

Comparison of Cluster, Grid and Cloud

مملوك لـ one Supervisor Domain ولا أكثر

الدفع عبارة عن Resources Sharing

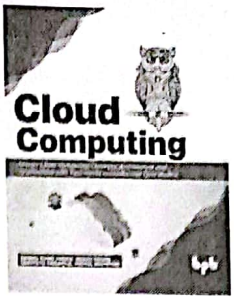
	Cluster Computing	Grid Computing	Cloud Computing
Ownership	? Yes, one	? No, more than one	? Yes, one
Service pricing	? No, ما بندفع فلوس	? No, ما بندفع فلوس	? Yes, بندفع فلوس
Virtualization	? No	? No	? Yes

↳ Virtual Machines

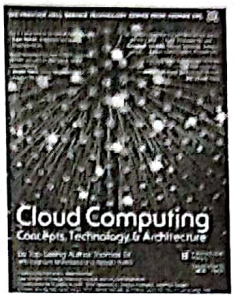
هل الـ user بيدفع فلوس بس يستخدم الخدمة → ممكن الدفع ما يكون فلوس ممكن مشاركة data أو هيك بس هون بنحكي عالفلوس.

Suggested Readings

- Hiran, K. K., Doshi, R., Fagbola, D. T., & Mahrishi, M. (2019). *Cloud Computing: Concepts, Architecture and Applications with Real-world examples and Case studies* . BPB Publications. Chapter1



- Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: concepts, technology, & architecture*. Pearson Education. Sections 3.1 – 3.3



Cloud Services and Deployment Models

Outline

implementation بتوفصلي الـ
Cloud الـ design ولا لينا الـ

- Cloud Deployment Models
- Cloud Service Models

Cloud Deployment Models

- A cloud deployment model can be described as a distinct - parameterized configuration of the cloud computing environment. These parameters include storage size, ownership and accessibility. There are four main cloud deployment models: public, private, hybrid, and community.

① ② ③ ④

3

مفتوحة لأي شخص بده يستخدموها بس بيدفع أكيد

① Public Cloud (1)

Public clouds are owned and operated by a third-party cloud service providers, which deliver their computing resources like servers and storage over the Internet.

- **ownership**: Public cloud platforms are fully owned and maintained by a third-party cloud service provider.
- **Accessibility**: open access.
- **Storage size**: Huge storage size.

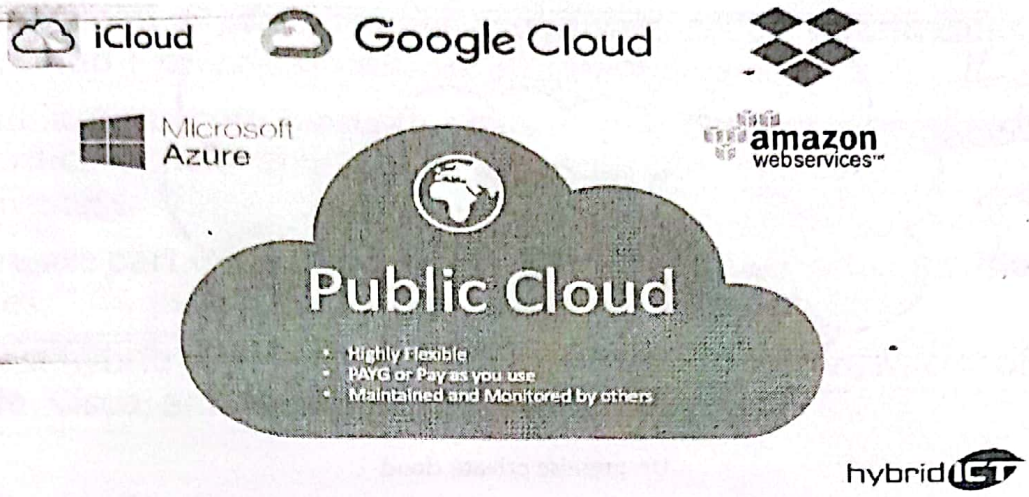
❖ public cloud consumers (customers) are relieved of the cost of application, bandwidth and hardware acquisition and maintenance requirements in their daily business operations. → مش صحيحة بشكل كامل.

4

مثلا: الـ Google Drive محاي ومابطلب تدفعي بس بستفيدوا إنه بياخدوا الـ Data، مثلا علت Search شغلة معينة بحفظوها عشان يبعتوها الشركات عشان تظهرلك.

Public Cloud (2)

أمثلة على الـ Public Cloud ↓



https://www.hybridict.com.au/corporate-cloud-services/cloud-computing/public-cloud/

② Private Cloud → الـ Cloud owners بتبعوا بتبع لـ Single organization

مثل Cloud خاصة فقط بالجامعة الأردنية.

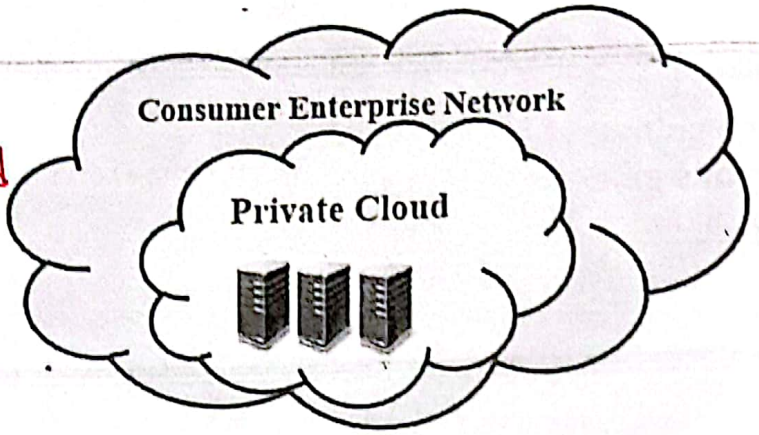
- Known as internal or corporate cloud.
- **Ownership**: owned any managed by single organization.
- **Accessibility**: provided and accessible over a private network (with permission). → متاحة بس لموظفين الشركة بس مثلاً
- **Storage size**: Limited storage

- More security than public cloud at the expense of cost.

* التكلفة أكثر هي الـ Public بالنسبة لـ "Cloud Service Provider"
والأمان أكثر هي الـ Private.

A: On-premise Private Cloud

Private الـ
بتكون Cloud
داخل تحكم
organization الـ

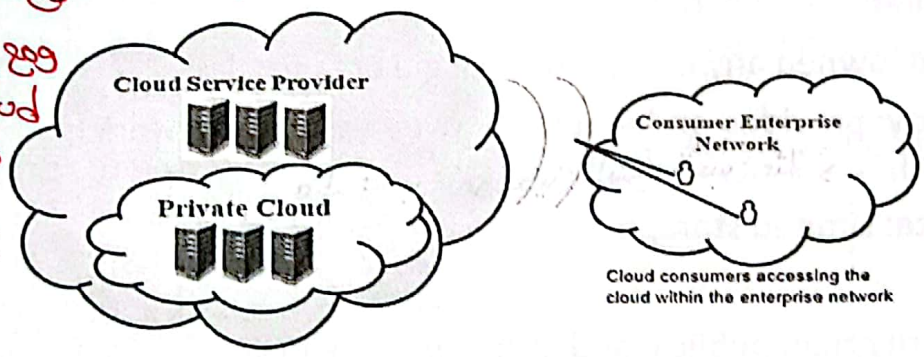


On-premise private cloud

7

B: Externally-hosted Private Cloud

organization خارج Private بعمل
وهو إنها داخل
Public cloud
كبيرة إلا
Private إنها



Out-sourced private cloud

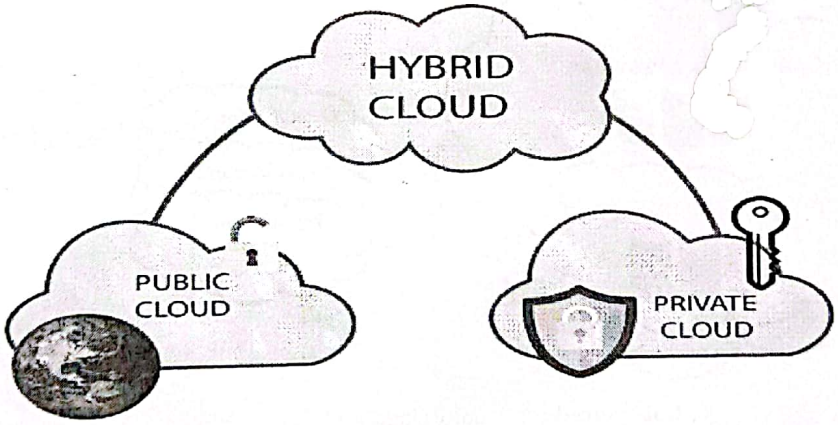
* VPC: Virtual private cloud *

8

③Hybrid Cloud (1)

- A hybrid cloud integrates public and private clouds (**Hybrid cloud = public cloud + private cloud**).
- The public part is often used for backup purpose and to keep records (non-critical activities) due to its high scalability and cost-effectiveness. → بنحط فيه الأقل خصوصية مثل نظام الإجازات.
- The private part is used to process sensitive (critical activities) cloud services. → بنحط فيه الأشيا المهمة مثل الرواتب أو العلامات.
- The best hybrid cloud provider companies are **Amazon, Microsoft, Google, Cisco,** and **NetApp**.

Hybrid Cloud (2)



Hybrid cloud

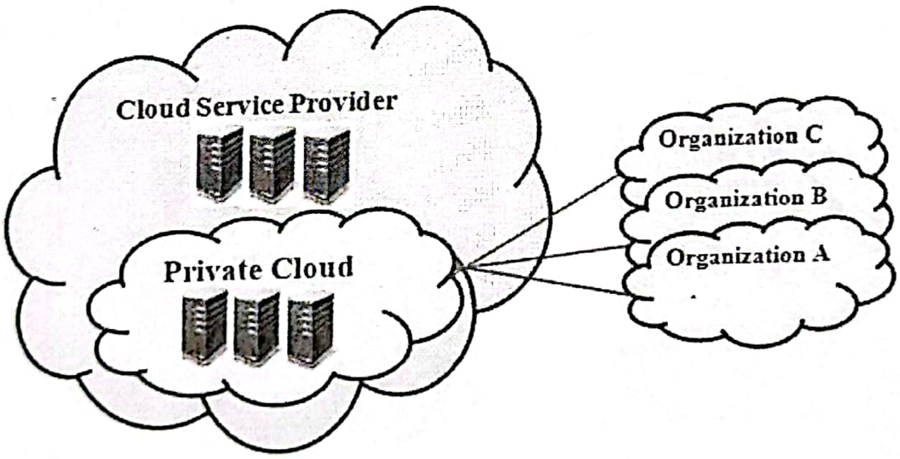
(4) Community Cloud

Private clouds مجموعة كل Private cloud تابعة لـ Single organization

- Community Cloud is a hybrid form of private cloud.
- Multi-tenant platforms that enable different organizations, from the same community, to work on a shared platform. (لازم يكونوا نفس القطاع)
- It offers high cost savings because it is shared among all the cooperating users.
- Examples of community clouds include Google Government Cloud, IGT Cloud, Optum Health Care Cloud.
- Cost and security? → ما إلها جواب مطلق بعتمد عالموقف

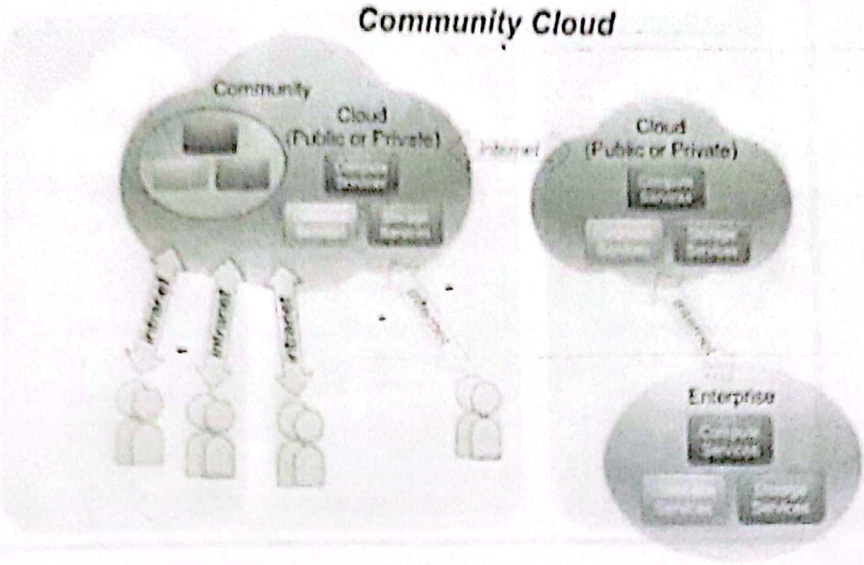
* الفائدة منه أقل cost لإنه صار يشتري huge number of resources.

A: Off-site Community Cloud



Out-sourced community cloud

B: On-site Community Cloud



13

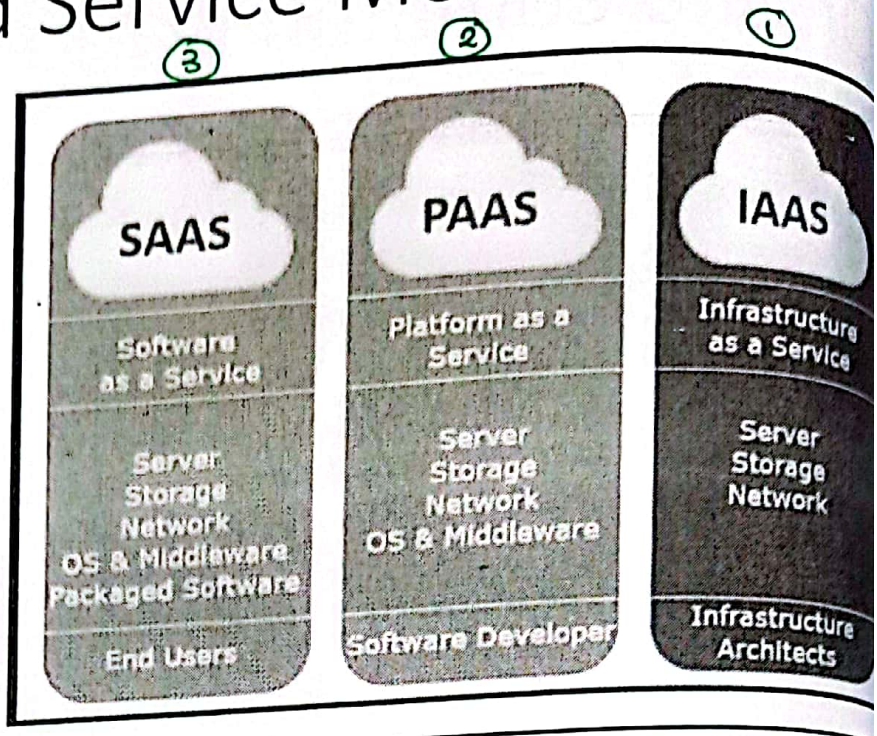
Outline

- Cloud Deployment Models
- Cloud Service Models

14

Cloud Service Models

A *cloud service/delivery model* represents a specific, pre-packaged combination of IT resources offered by a cloud provider.



①-Infrastructure as a Service (1)

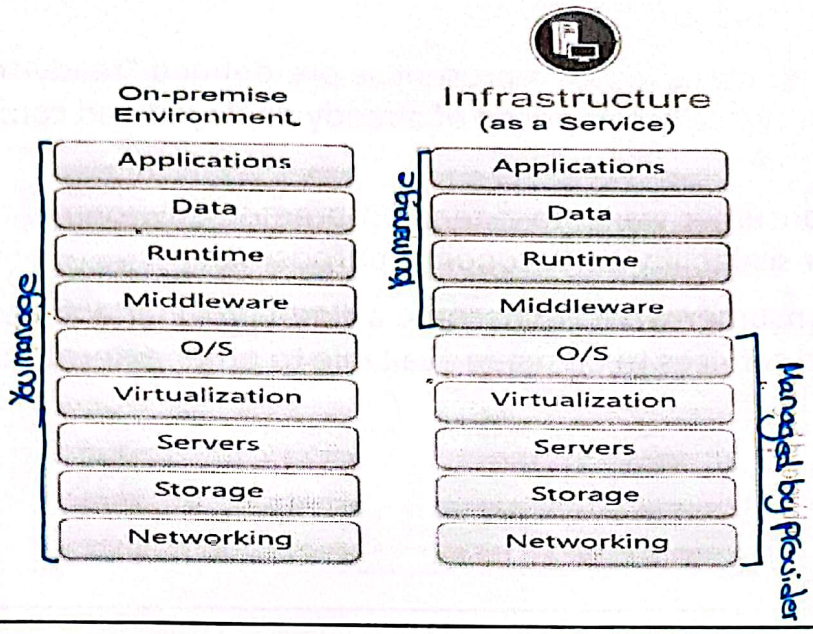
البنية التحتية

بستأجرها وقت احتياجي وبرجعها بعدين و بكون الي control كامل عليها ومسؤول عنها بشكل كامل

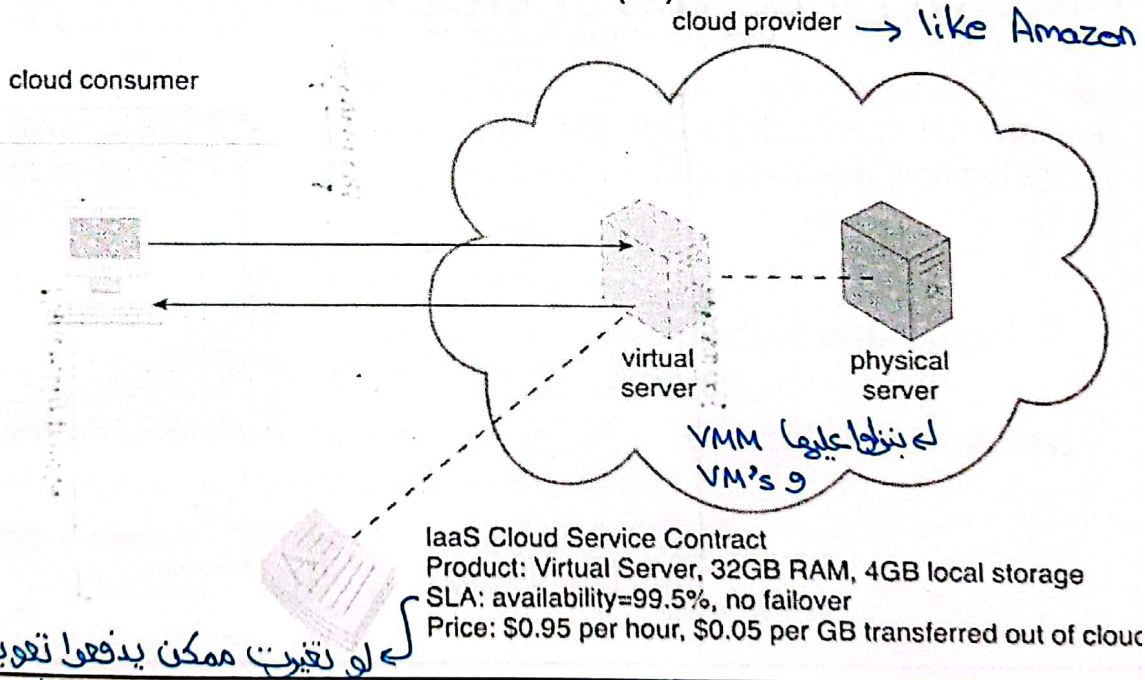
- Infrastructure as a Service (IaaS) Provides you with virtualized computing resources (VMs, storage, and network) that can completely replace on-premise infrastructure.
- No investment in expensive hardware and pay-as-you-go pricing model.
- Pros: complete control over the infrastructure, secure, scalable, cost-effectiveness. (مميزات)
- Cons: maintain the VMs, security issues, software maintenance. (عيوب)
- Examples of such services: Amazon Web Services (AWS), Rackspace, DigitalOcean, Linode, Google Compute Engine (GCE).

بتكون عليك لو شاركت data بالغلط مثلا

Infrastructure as a Service (2)



Infrastructure as a Service (3)



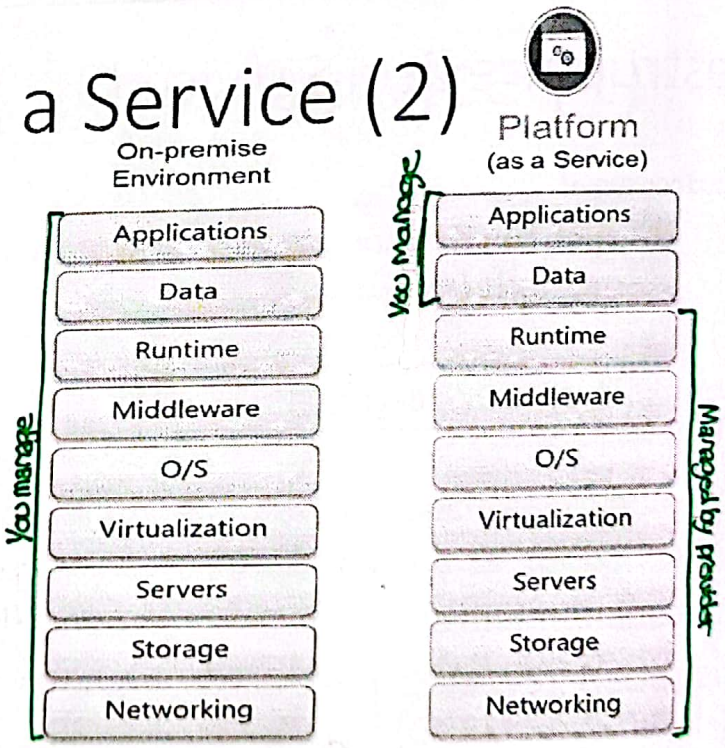
لو تغيرت ممكن يدفعوا تعويض ال Cloud Service providers .
كلما زاد السنة كل ما كان أغلى .

↳ كل اشي يكون جاهز بطلبه ونازل عال VM .

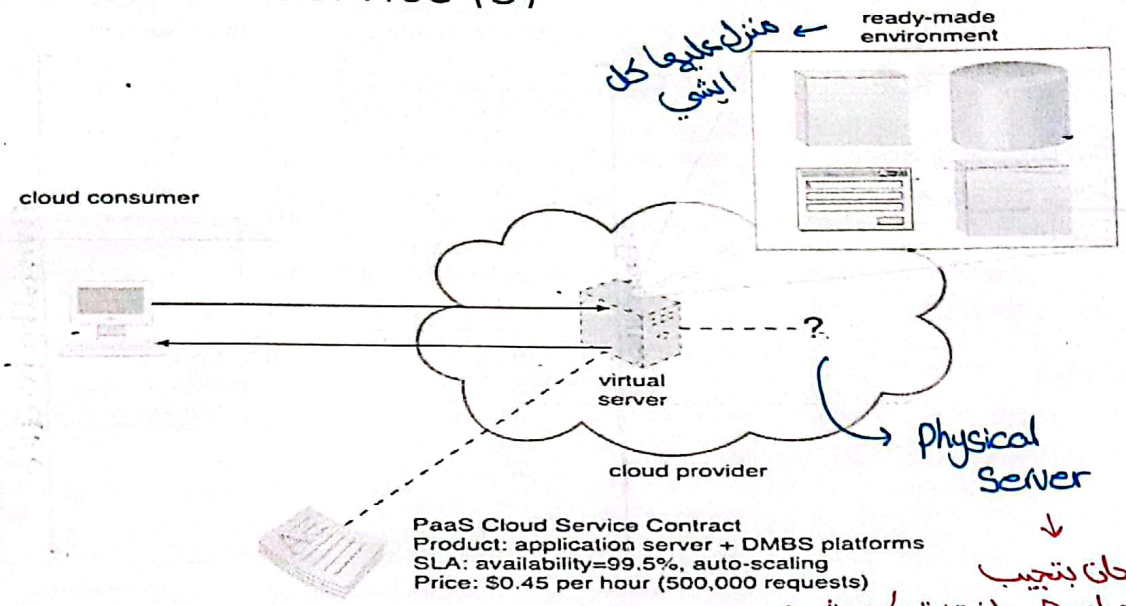
②- Platform as a Service (1)

- Platform as a Service (PaaS) represents a pre-defined "ready-to-use" environment typically comprised of already deployed and configured IT resources.
- The cloud consumer wants to extend on-premise environments into the cloud for scalability and economic purposes.
- The cloud consumer wants to become a cloud provider and deploys its own cloud services to be made available to other external cloud consumers.

Platform as a Service (2)



Platform as a Service (3)



منزل عليها كل اشي ←

Physical Server

بالامتحان بتجيب Part missing وانت تحكي شوهو .

1

③-Software as a Service (1) → like gmail

* أنا كـ user ما بهتم كيف معمولة بستخدم الservice بشكلها النهائي .

- Software as a Service (SaaS): a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.
- free or have a pay-as-you-go model.
- It works on any platform without any downloads or installations. Services are available directly in a web browser.
- Cons: no installation/ integration of software, easy/ quick to access and use, and many are free!
- Pros: ?? Need to Internet → لو ماني بتخدش Internet بتخدش نستخدمها.

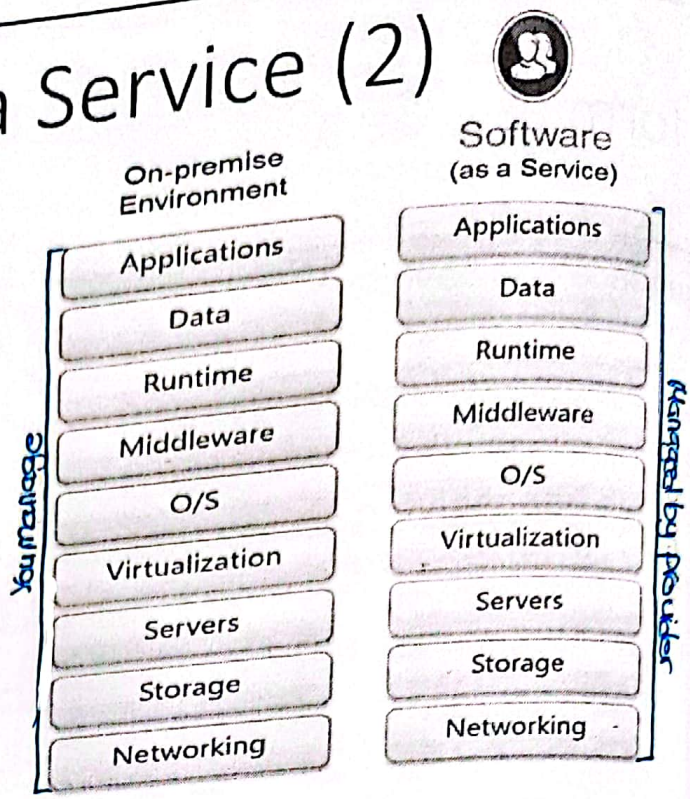
عيوب ↓

مميزات ↓

22

Software as a Service (2)

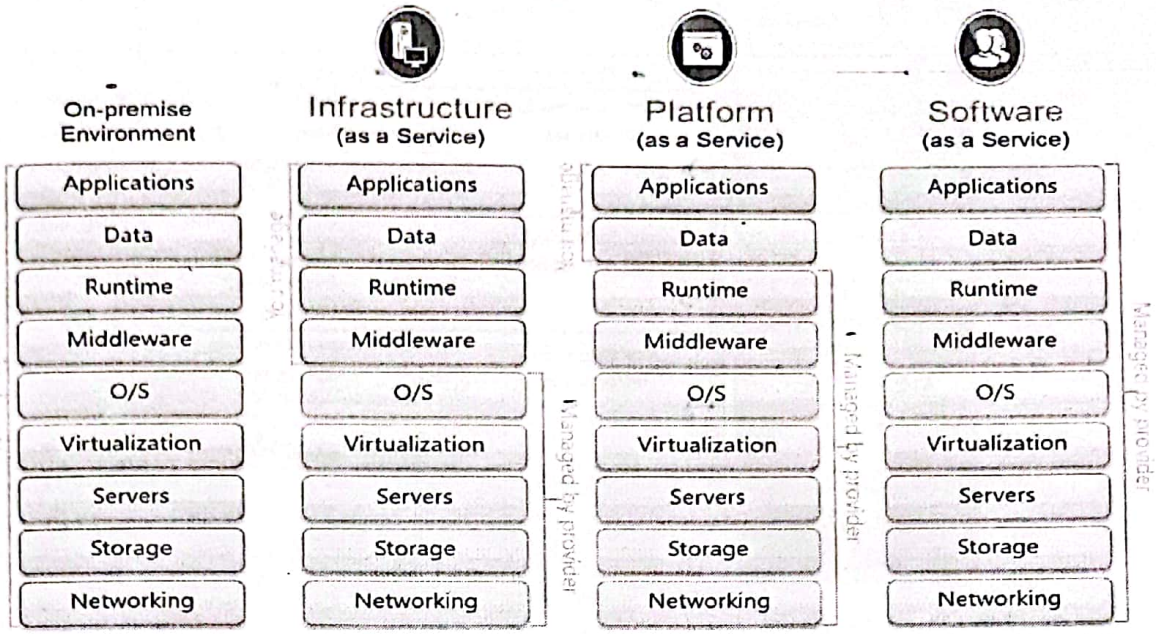
Ex.: Dropbox, Google Docs, Gmail, and GitHub.



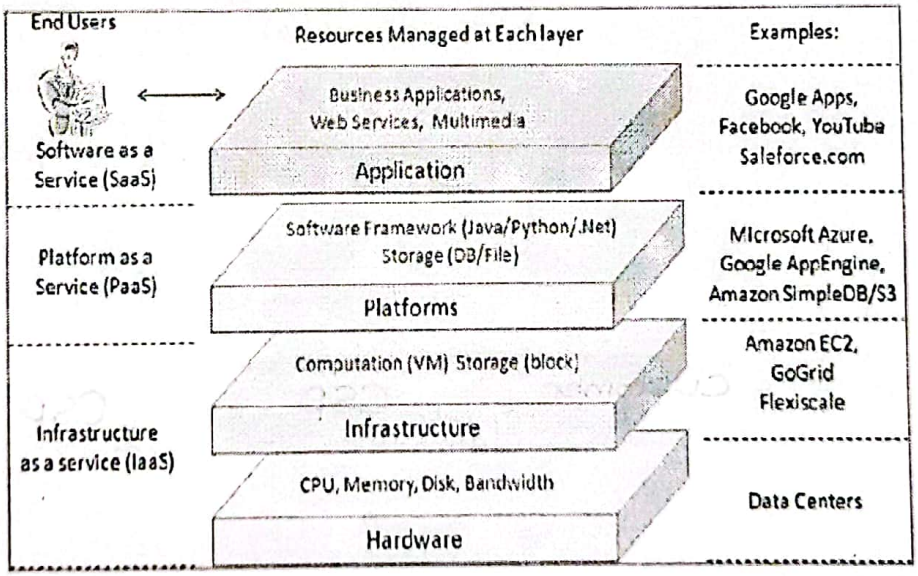
Anything as a Service

- Anything as a Service (XaaS). صار في كثير عنا Services
- Examples of X:
  - Storage-as-a-Service
  - Database-as-a-Service
  - Security-as-a-Service
  - Communication-as-a-Service
  - Integration-as-a-Service
  - Testing-as-a-Service
  - Process-as-a-Service

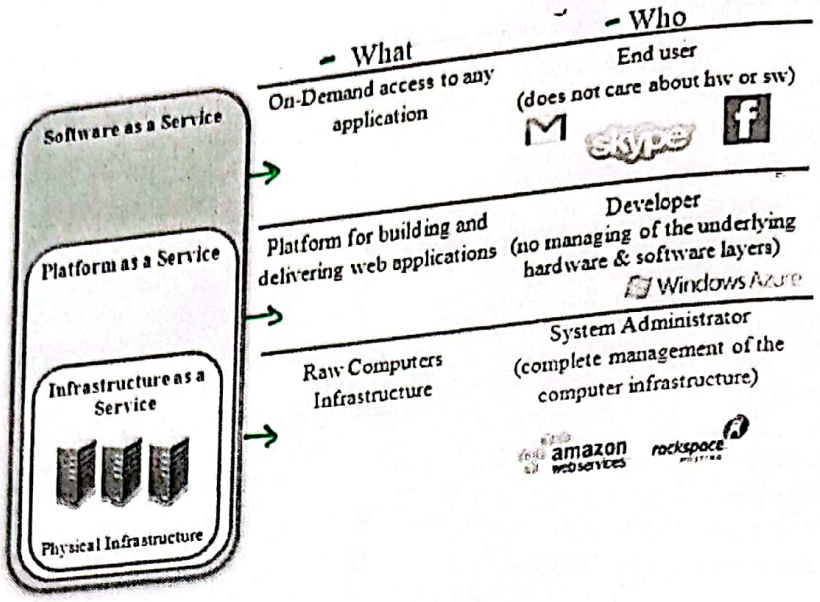
Summary of Cloud Service Models



Layered Model of Cloud Services



The Audience of Cloud Service Mod



Quiz

Customer or CSP?

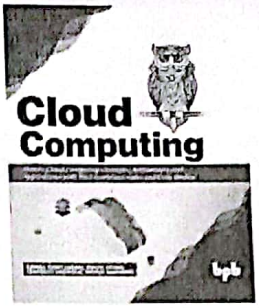
Customer الـ هل مسئولية
Cloud Service الـ و
Provider

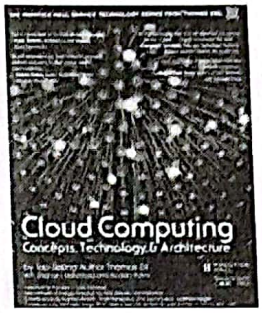
	Application software	Operating system	Hardware and virtualized resources
SaaS	? CSP	? CSP	? CSP
PaaS	? Customer	? CSP	? CSP
IaaS	? Customer	? CSP	? CSP

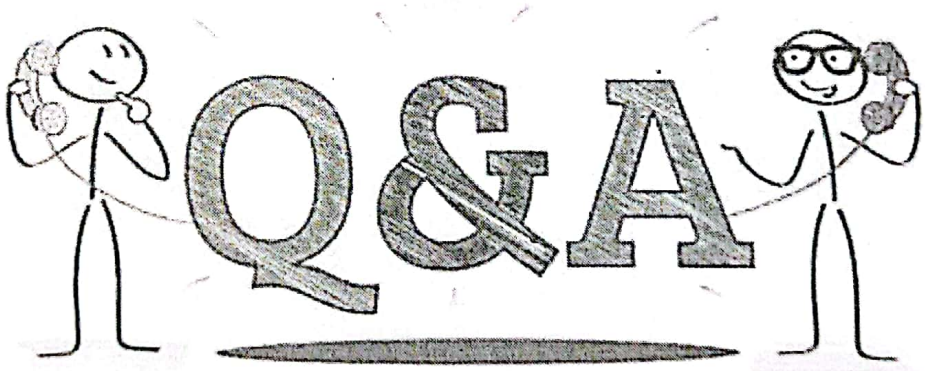
Suggested Readings

- Hiran, K. K., Doshi, R., Fagbola, D. T., & Mahrishi, M. (2019). *Cloud Computing: Concepts, Architecture and Applications with Real-world examples and Case studies* . BPB Publications. Chapter 2

- Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: concepts, technology, & architecture*. Pearson Education.







Part-II: Virtualization

CPE 0907523 Cloud Computing, Spring 2022

Dr. Samah Rahamneh

Slides adapted from Erl, Mahmood, and Puttini

Cloud Computing Enabling Technologies

- Broadband Networks and Internet Architecture
- Data Center Technology
- Virtualization Technology
- Web Technology
- Multitenant Technology
- Service Technology

Virtualization Technology (1)

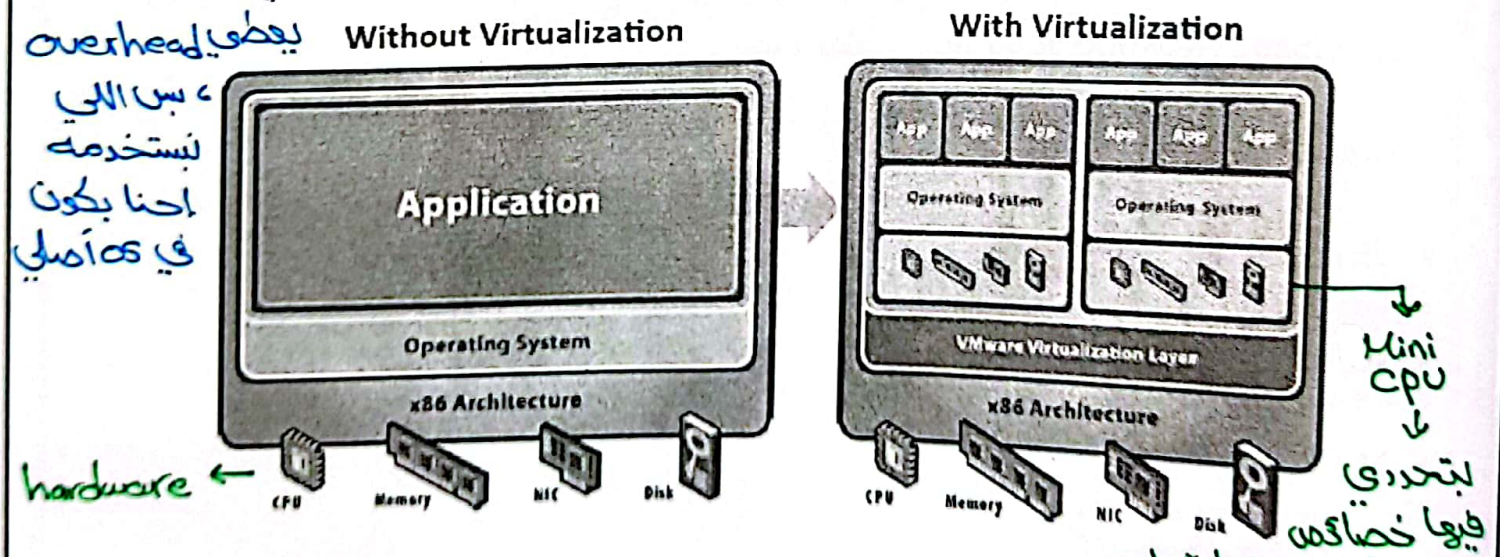
Virtualization is the process of converting a physical IT resource into a virtual IT resource.
Most types of IT resources can be virtualized, including:

1. *Servers* – A physical server can be abstracted into a virtual server.
2. *Storage* – A physical storage device can be abstracted into a virtual storage device or a virtual disk.
3. *Network* – Physical routers and switches can be abstracted into logical network fabrics, such as VLANs.
4. *Power* – A physical UPS and power distribution units can be abstracted into what are commonly referred to as virtual UPSs.

* host os → الأصلي
* guest os → Virtual os الـ

Virtual Machine Architecture

في الـ data center، لإنه شلنا الـ os الأصلي كشان ما يعطي overhead، بس اللي نستخدمه احنا بكون في os أصلي



Mini CPU
بتحدد فيها خصائص الـ guest os لما تنزليه.

* الأسباب اللي بندفعنا أحرك VM من Physical Server إلى آخر:

1- عشان ممكن يكون الـ Physical server عليه كتير VMs فبنقل الـ VM لأحسن الـ Performance.

2- Security ⇐

3- لأغراض Power consumption

3/9/2022

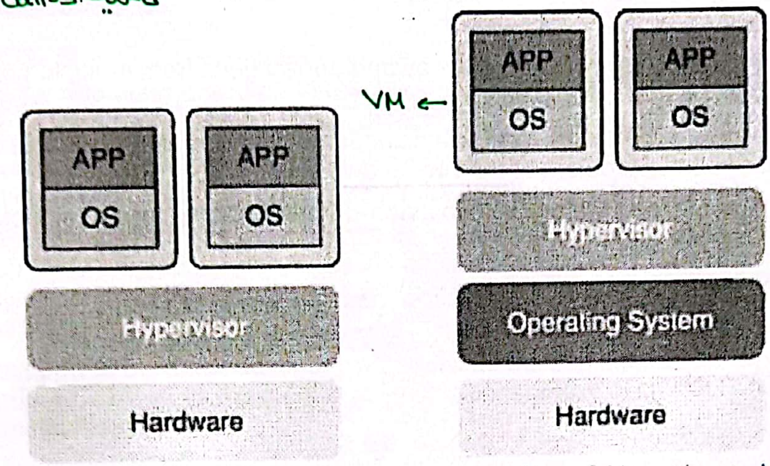
Server1	Server2
VM1	VM1
VM2 →	VM2

عليها critical info بتطلب أمان عالي فبنحرك لـ VM2 لـ server مختلف عشان تخلي VM1 لحاله

Types of Hypervisors

or Virtual Machine Manager

فائدته: أسرع من ناحية الـ System calls



VM ← → VM

* بنستخدم هاي دايما عاجهزتنا لأنه لازم يكون فيه host OS

الـ Hypervisors بنزل على host OS

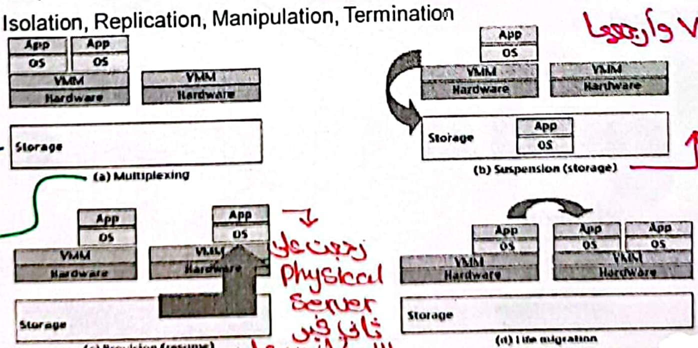
الـ hypervisors لـ بنزل مباشرة على الـ hardware بدون host OS → مستخدم في الـ Cloud data center

5

Primitive Operations in Virtual Machines

- Hypervisor can encapsulate entire state of a VM in a file!
- Allows users to create, copy, save, read, modify, share, migrate and roll back VMs as easily as manipulating a file

  لأنه الـ OS بتتعامل مع الـ VMs كأنها Files نازلة عنده عالـ System.
- States: Multiplex, Suspend, Resume, Migrate
- Actions: Isolation, Replication, Manipulation, Termination



يعني أسكر هاي الـ VM وأرجعها على الـ disk لما أخلص شغل منه من خلال الـ shut down

مقصود فيها الـ hw ككل، فيها الـ Files، Shared بين الـ VMs

رجعت على Physical Server ثاني غير اللي كانت عليه

مجرد ما أعمل turn on لهاي الـ VM بتدخل في الـ Multiplexing State (Sharing)

بدي أرجع أعمل turn on لهاي الـ VM اللي كنت طفيتها من قبل وحطيتها عالـ disk. (موجود عالـ disk كـ File وبدي أحوله لـ Memory)

بتشبه شوي الـ Provision، الفرق بتكون الـ VM هاي شغالة على Physical Server معين وبينما هي شغالة بقدر أحركها لـ different physical Server، وممكن يكون offline يعني نطفي الـ VM بعدين ننقلها أو online ننقلها وهي شغالة.

6

Sever Consolidation (1)

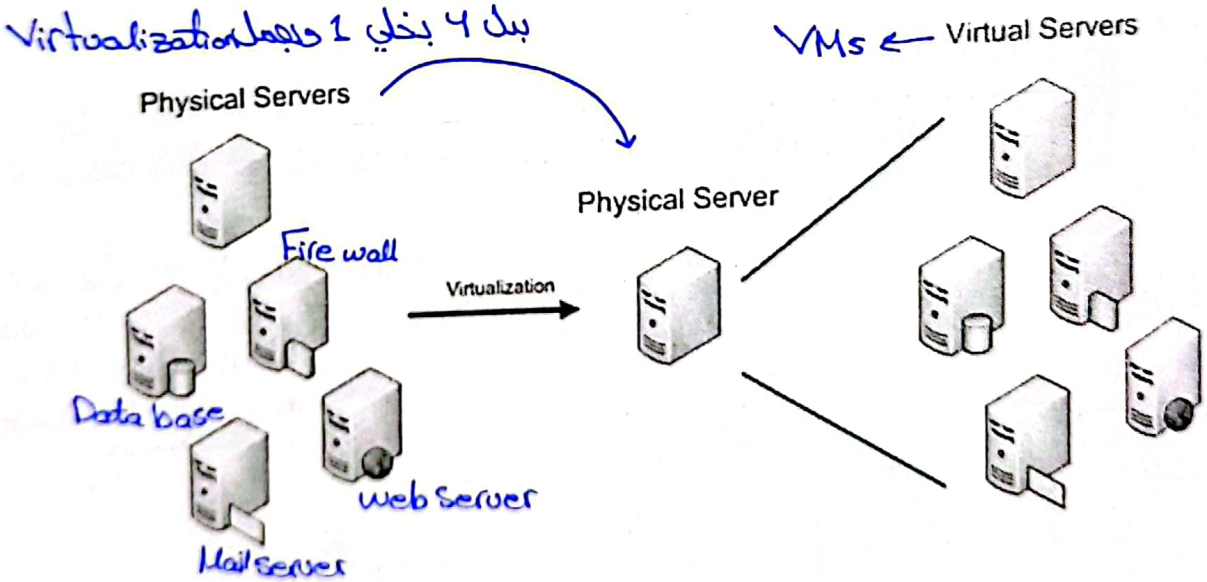
- The process of migrating network services and applications from multiple computers to a singular computer.
- Increases hardware utilization, load balancing, and optimization of available IT resources. Solved the problem of Server Sprawl.
- Supports common cloud features, such as on-demand usage, resource pooling, elasticity, scalability, and resiliency.
- Agile resource replication.
- Drawbacks ?!

هاي المشكلة انحلت بالVirtualization

اشرحوا في السابق

Resource Scale up/down يقصد فيها سرعة

Sever Consolidation (2)



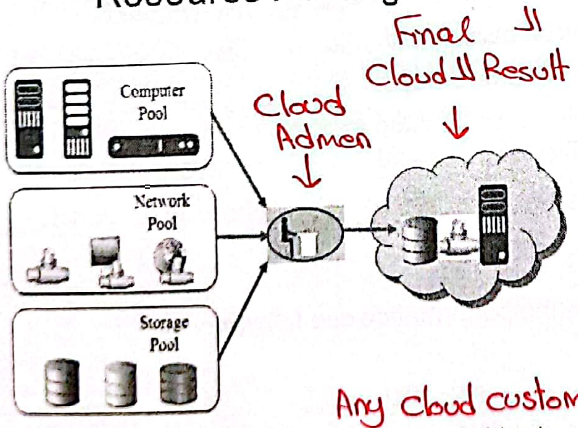
نسخة طبق الأصل يستخدمها لو صار down
load balance الـ sys الأصلي أو لأجل ↑

Resource Replication (1)

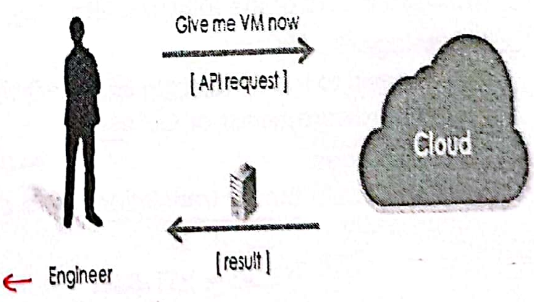
- Virtual servers are created as Virtual Disk Images (VDIs) that contain binary file copies of hard disk content.
- VDIs are accessible to the host's operating system, meaning simple file operations, such as copy, move, and paste, can be used to replicate, migrate, and back up a virtual server.
- The ability to roll back, which is the instantaneous creation of VM snapshots by saving the state of the virtual server's memory and hard disk image to a host-based file. ↱ backup من هاي الـ VM
- The support of business continuity with efficient backup and restoration procedures, as well as the creation of multiple instances of critical IT resources and applications. ↱ like Facebook → إنو الـ Service تظل توصل الـ user بـ quality عالي

Resource Pooling

Resource Pooling



ON-DEMAND SELF-SERVICE



https://www.hitechmv.com/cloud-computing-the-characteris

Virtualization Techniques

- Techniques of virtualization can be categorized into the following three categories:

☑ Full Virtualization

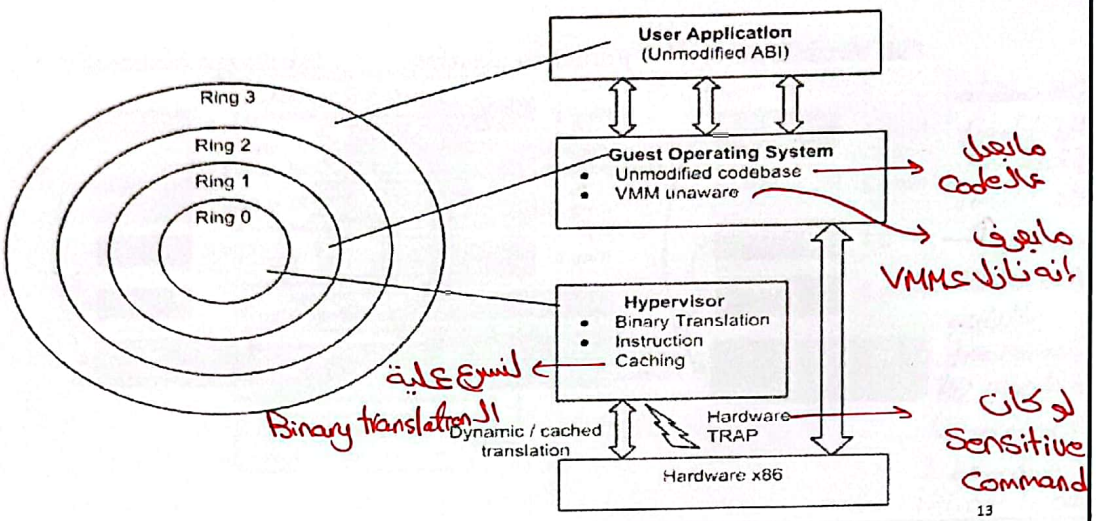
☑ Para virtualization

☑ Hardware-assisted Virtualization

Full Virtualization (1)

- The hardware is made available to the guest operating system, which executes unaware of virtualization.
- Direct execution for non-sensitive instructions on hardware.
- Binary translation for sensitive instructions or hardware traps.
- VMWare is one of the fully virtualized hypervisors for Desktop and server environments.
- Advantages:
  - No need to modify the gust O.S.
  - No hardware assist or OS assist
- Disadvantages:
  - Approach of binary translation slows down the performance due to hypervisor overheads

Full Virtualization (2)



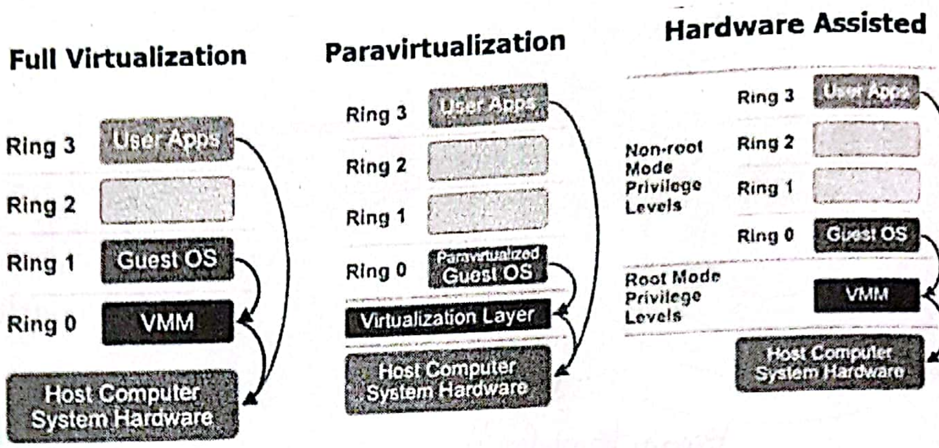
Para Virtualization (1)

- It recompiles the guest OS before installing it inside a VM.
- replacing the non-virtualizable instructions with hyper calls that communicate directly with the virtualization layer hypervisor.
- Its compatibility and portability is poor.
- It is also known as OS assisted virtualization.
- The open source Xen project is an example of paravirtualization.

14

(Type 1 → No host os)

Para Virtualization (2)



ما فيه فكرة إنو نازل عال VM ويعتقد انو نازل عال hardware ← ال VMM بحول ال Command الي بنوصلها من ال guest os لـ Command أقل ضرر أو خطر

(binary translation)

binary code —to→ other binary code

Hardware-assisted Virtualization(1)

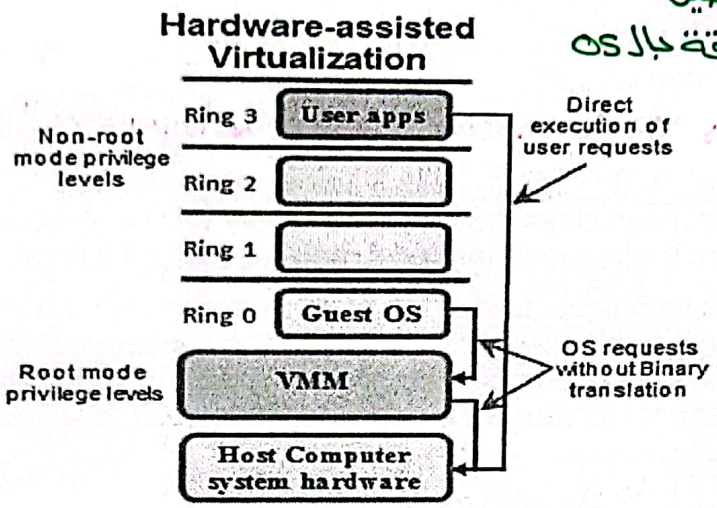
لـ بياخذ من ال Full وال Para

- It provides full virtualization using hardware capabilities (CPU). (لازم تكون Enabled)
- Hardware-assisted virtualization was added to x86 processors (Intel VT-x or AMD-V) in 2005 and 2006. (بتدعم ال Virtualization)
- Advantages:
  - It eliminates the changes needed in the guest operating system. (ما بحتاج أغير ال Code عال os)
  - improves the performance of VMs. → (لأنو ما بحتاج ال Binary translation ال CPU بتصرف من حاله ما برجع لل hypervisors)
- Disadvantages:
  - Hardware-assisted virtualization requires explicit support in the host CPU. (لازم الجهاز يدعم ال Virtualization)
  - Server consolidation:?!

ما بدي أعدل ع ال Code ال os بس في إعدادات معينة بدها تكون معمولة بشكل صحيح

Hardware-assisted Virtualization(2)

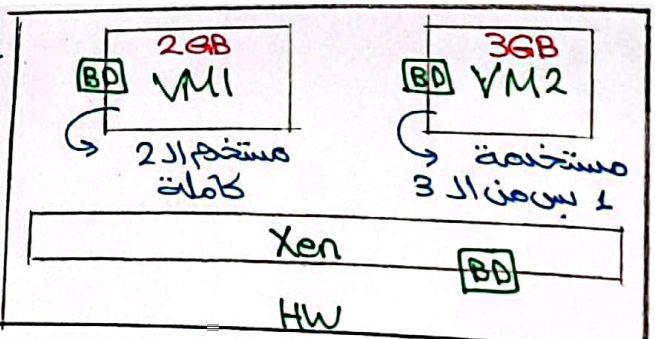
ما حندخل بالتفصيل
لإنه العلاقة بالـ OS



Virtual Machine Managers (VMMs)

"open"

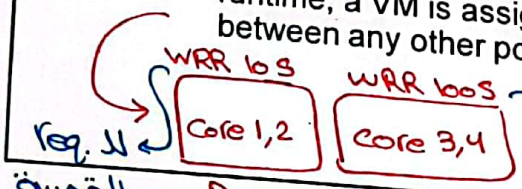
1. Xen → أصولي → Type 1 & HW بدون → Para Virtualization
2. KVM
3. VMWare
4. VirtualBox
5. Citrix (Xen Server)



Physical Server

Xen Hypervisor

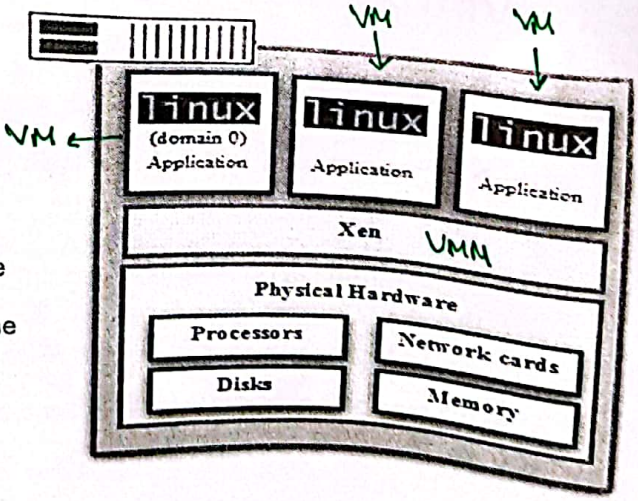
- Type 1, native or bare-metal hypervisor.
- Xen is an open source project which is used in the AWS Cloud, server virtualization, IaaS, desktop virtualization, security virtualization.
- Xen Features:
  - **Memory ballooning**: It is an advance memory management technique in which the hypervisor can claim the unused memory from one guest machine and share it with the other guest machines within a host.
  - **CPU pools**: This technique divides the physical cores on the machine into different pools, each with its own customizable CPU scheduler. At runtime, a VM is assigned to one of the pools, but it can further migrate between any other pools through the course of its execution



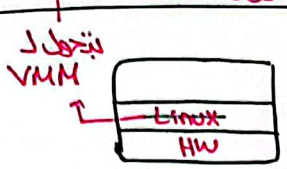
19

Xen Architecture

- *Domain 0 is the management VM:*
  - Designed to have direct access to physical devices and can manage them, and can allocate and map hardware resources for guest domains
  - It is first loaded when Xen boots without any file system drives being available
  - Hacker who compromises Domain 0 controls the entire system, and hence Domain 0 brings a series of security issues that need to be addressed



20

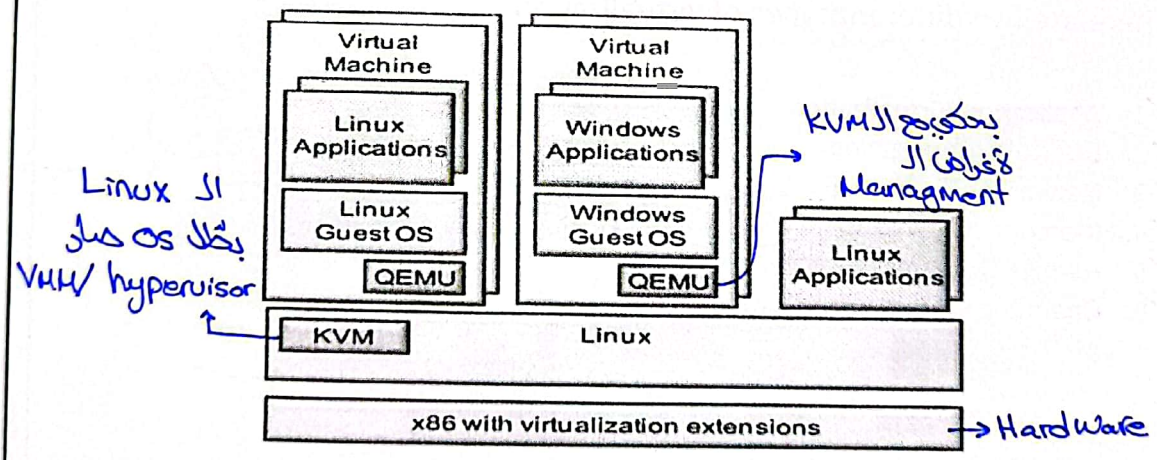


KVM Hypervisor

- Kernel-based Virtual Machine (KVM) turns Linux into a type-1 hypervisor and allows a host machine to run multiple, isolated VMs.
- Every VM is implemented as a regular Linux process, scheduled by the standard Linux scheduler.
- KVM requires a processor with hardware virtualization extensions, such as Intel VT or AMD-V.
- KVM features:
  - Security : KVM uses security-enhanced Linux (Se-Linux) and secure Virtualization (sVirt) to enhance VM security and isolation.
  - Live migration.
  - Memory management.

21

KVM Architecture



22

Major VMM Comparison

Table 6.2 Comparison of Three Virtual Machine Monitors (VMMs)

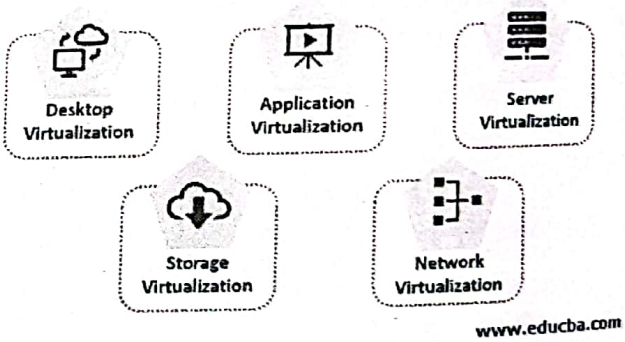
VMM Provider	Host CPU	Guest CPU	Host OS	Guest OS	VM Architecture
VMware Work-station	X86, x86-64	X86, x86-64	Windows, Linux	Windows, Linux, Solaris, FreeBSD, Netware, OS/2, SCO, BeOS, Darwin	Full Virtualization
VMware ESX Server	X86, x86-64	X86, x86-64	No host OS	The same as VMware workstation	Para-Virtualization
XEN	X86, x86-64, IA-64	X86, x86-64, IA-64	NetBSD, Linux, Solaris	FreeBSD, NetBSD, Linux, Solaris, windows XP and 2003 Server	Hypervisor Para-Virtualization
KVM	X86, x86-64, IA64, S390, PowerPC	X86, x86-64, IA64, S390, PowerPC	Linux	Linux, Windows, FreeBSD, Solaris	Para-Virtualization

23

Type of Virtualization

- There are five different types of virtualization:

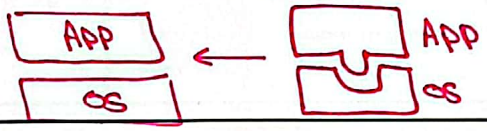
1. Application Virtualization
2. Desktop Virtualization
3. Network Virtualization
4. Memory Virtualization
5. Hardware (server) Virtualization
6. Operating System Virtualization



24

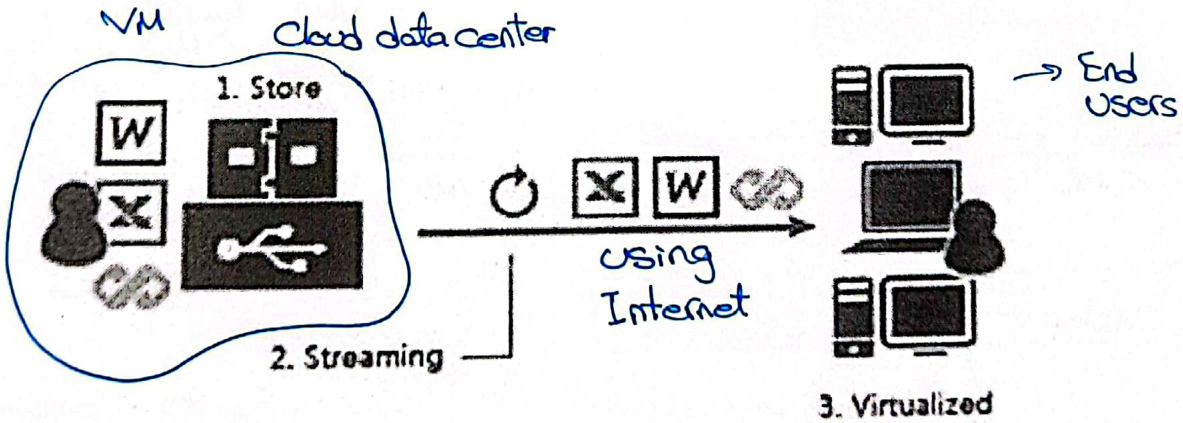
Application Virtualization (1)

- Applications are not installed on the user's machine.
- Applications are streamed to users when they click on the application icon.
- AV decouples the application layer from OS.
- AV centralizes/ simplifies application updating.
- For example, Microsoft APP V.



25

Application Virtualization (2)



26

* remote login ← في OS نازل عالجهاز الأصلي .
* DV ← الجهاز مابكون عليه OS .

3/9/

بدون ما أعمل remote login → بصير ممكن أدخله لـ dc آخر

Desktop Virtualization(1)

desktop ← بختفي الـ desktop الي كان شغال ويطلع الـ desktop الجديد ، remote login الي بيبلك الـ desktop الجديد على الأصلي الي كان

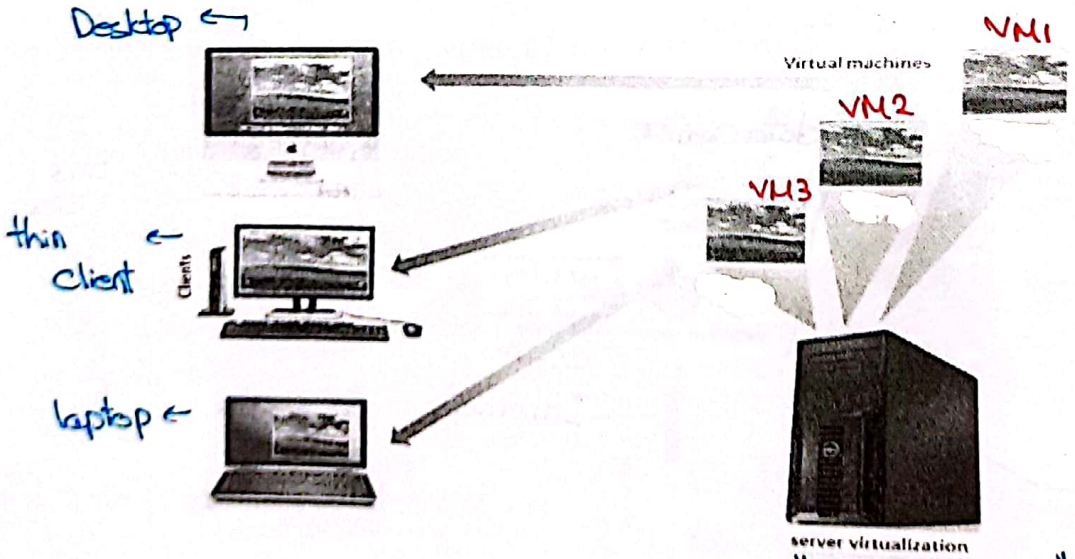
- Decouple user's OS, applications, settings, and data from the end user computing device and client.
- Virtualized desktops are generally hosted on a remote central server, rather than the hard drive of the personal computer.
- Enable end users to securely access corporate resources and work anytime, anywhere, on any device. → « فائدة الـ DV »
- There are three techniques to realize desktop virtualization:
  - * - Virtual Desktop Infrastructure (VDI)
  - * - Remote Desktop Service (RDS)
  - * - Desktop as a Service (DaaS) such as Amazon Workspaces.

" بدون تفاصيل "

27

بكون الجهاز الأصلي مو نازل عليه OS .

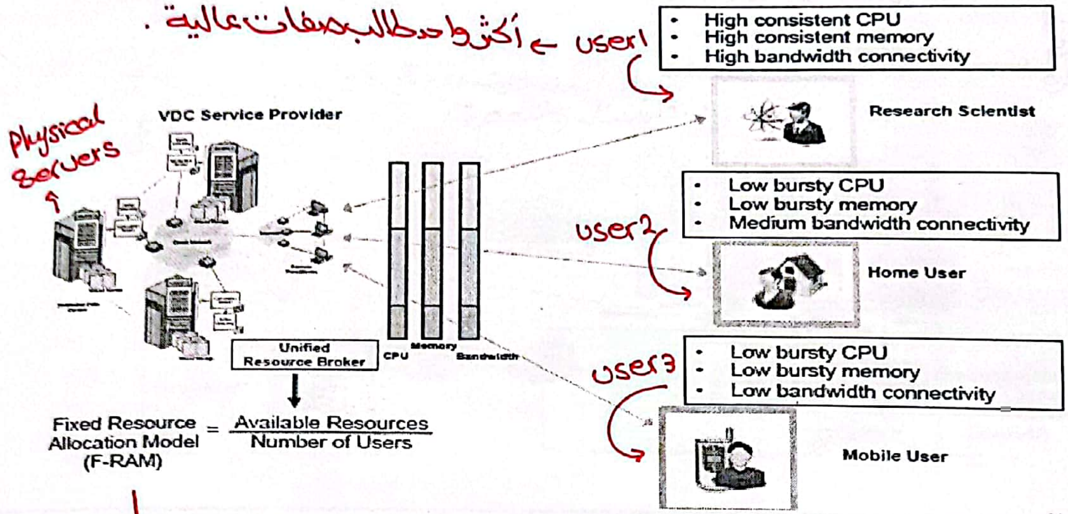
Desktop Virtualization(2)



28

VDCs Today – Overprovisioning and Guesswork…

user1 ← أكثر واحد طالب مواصفات عالية .



Fixed Resource Allocation Model (F-RAM) = $\frac{\text{Available Resources}}{\text{Number of Users}}$

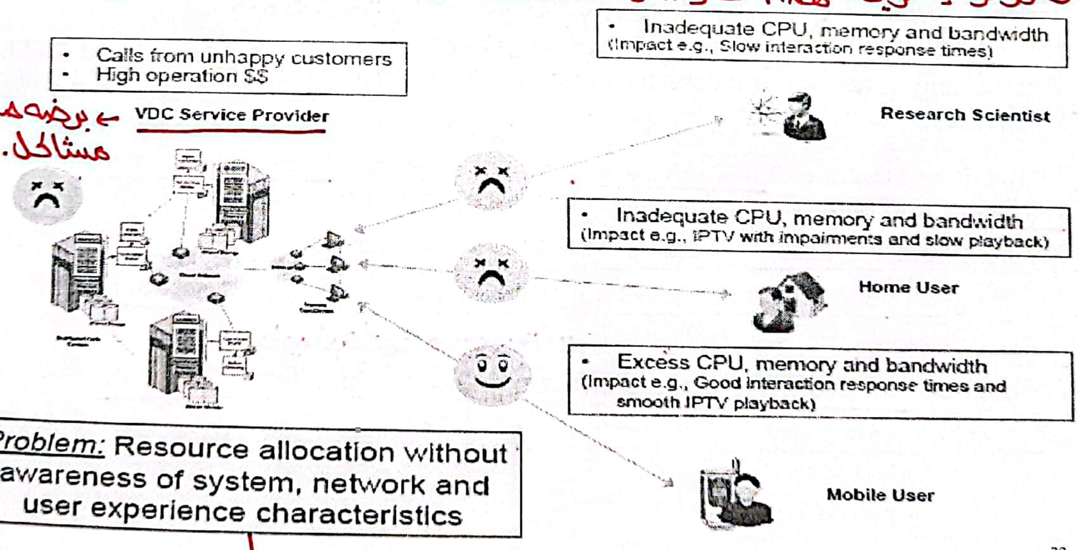
29

بالتالي كل user حياخذ نفس التاني من cpu و Mem و etc. ←

ولكن هنا حل غير ناجح لإنه مو كل user طلباته واحتياجاته نفس التاني .

Overprovisioning and Guesswork Fails!

عشان وزعوا بطريقة Fixed فال Research Sci.. وال Home user ما أخذوا قد ما يحتاجوا.



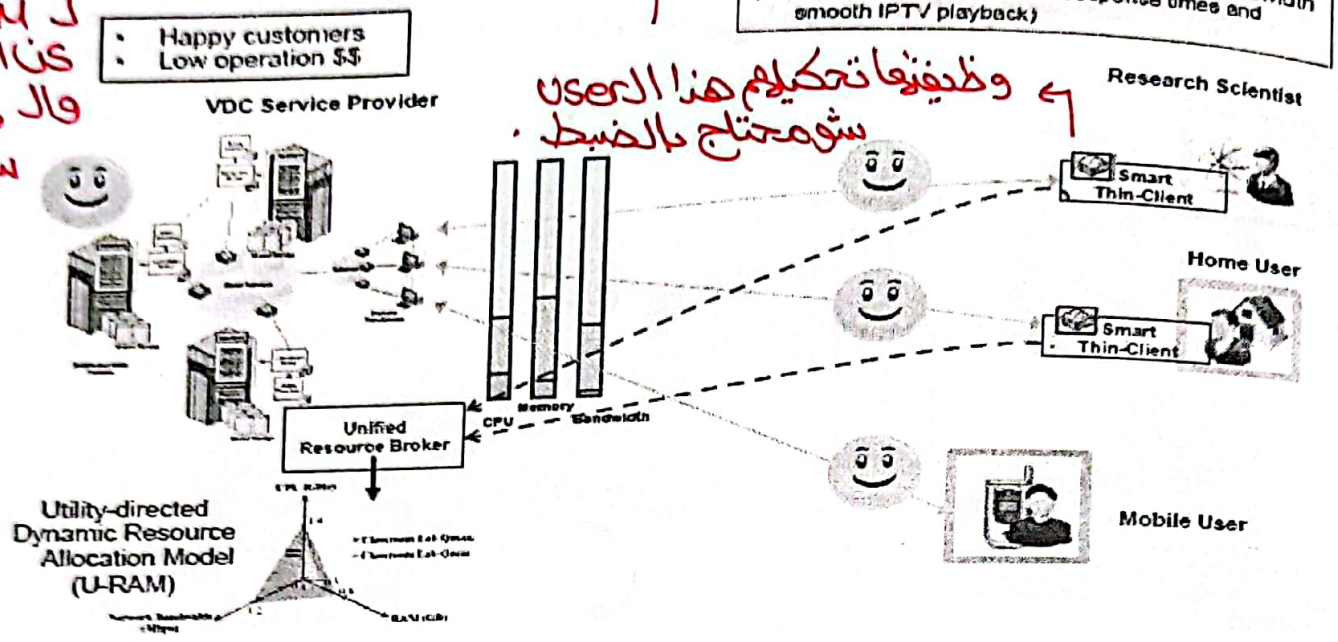
← برضه صار عنده مشاكل.

Problem: Resource allocation without awareness of system, network and user experience characteristics

30

ما كانوا يعرفوا كل user
شو كان يحتاج و يعطوه
حسب حاجته لا أكثر
ولا أقل بنسبة عالية .

VDCs in the Future – Smart set-top boxes at user sites

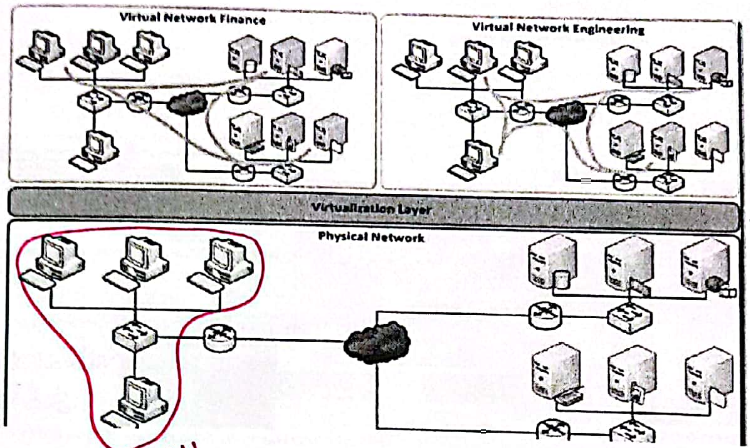


Network Virtualization (1)

- Abstracting network resources traditionally delivered in hardware to software.
- Network virtualization (NV) decouples network services from the underlying hardware and allows virtual provisioning of an entire network.
- NV combines multiple physical networks to one virtual, software-based network, or it can divide one physical network into separate, independent virtual networks.
- NV creates a network overlay that can run separate virtual network layers on top of the same physical network fabric.

Network Virtualization (2)

Virtual Net. 2 ←



→ Virtual Net. 1

→ over lay Net.

Physical Network

LAN → رح يقسموا

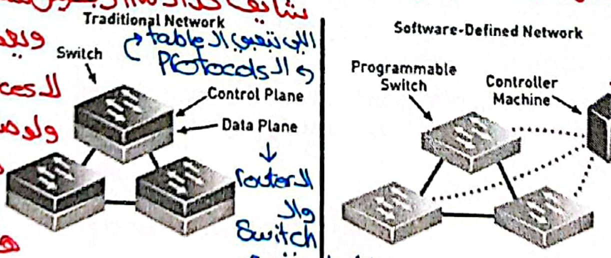
33

Network Function Virtualization (1)

- NFV: Consolidate diverse network equipment types (firewall, switching, routing, ADC, BRAS, EPC, etc.) onto industry-standard servers or commercial off-the-shelf (COTS) using virtualization
- Software Defined Network (SDN): Separate control plane from data plane in network devices (physical/virtual) with intelligence and programmability centralized in a controller

صرنا نستبدل هذول ال HW مثل ال Switch وغيره بـ laptop بنحوله لـ Switch أو router ... بدون ما نحتاج نشتري هذول ال HW.

هاد كل التحكم هون عشان بصير شايف كل ال HW وبصير مسؤول يشيل أو يجيب routing table ويعمل ال devices ويبعتها إله. ولو صار مشكلة بجهاز معين بيشوفها ويخبر الباقي إنه هذا الجهاز خرب.

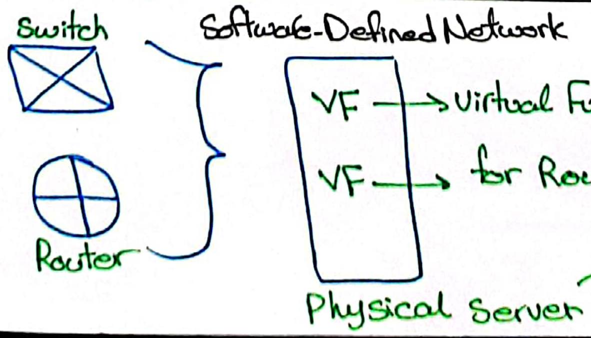


اللي بتعبي ال table ال Protocols ال

ال router وال Switch نفسهم tables.

34

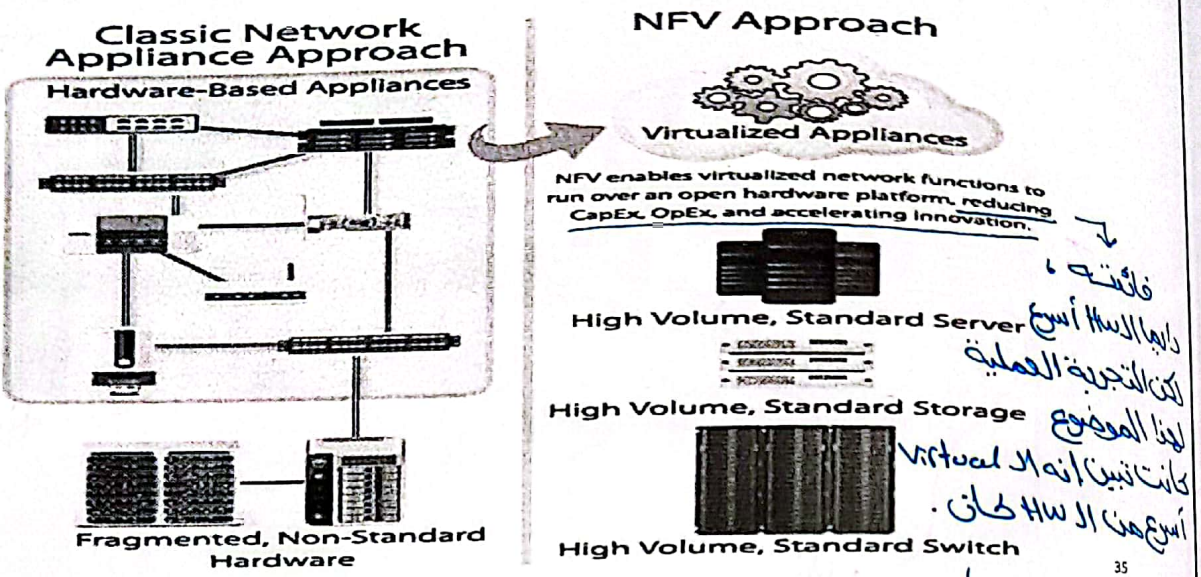
specific hardware



*ممكن تحطهم بداخل ال VM.

→ بشتغل كـ Switch أو router على نفس الوقت.

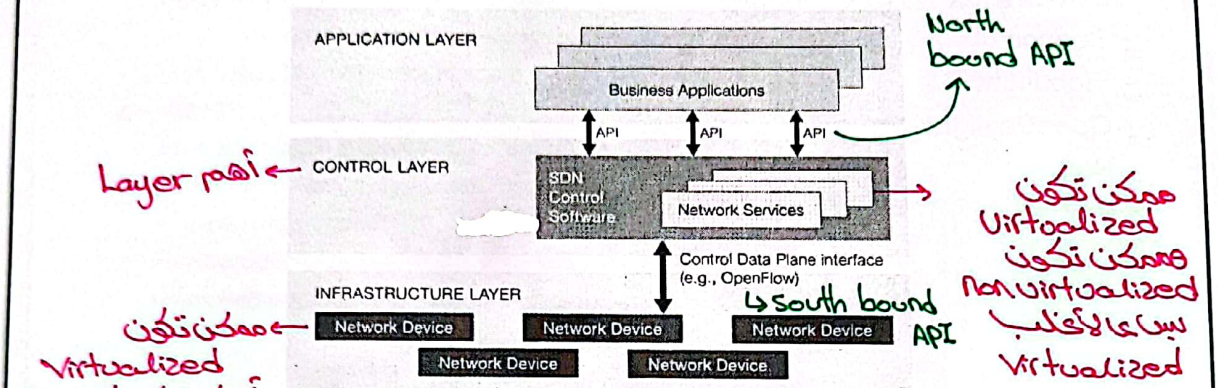
Network Function Virtualization (2)



Software Defined Networking ← SDN Architecture (1)

- An SDN architecture delivers a centralized, programmable network and consists of the following:
  - A controller, the core element of an SDN architecture, that enables centralized management and control, automation, and policy enforcement across physical and virtual network environments
  - Southbound APIs that relay information between the controller and the individual network devices (such as switches, access points, routers, and firewalls)
  - Northbound APIs that relay information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device

SDN Architecture (1)



SDN Adaption

- SDN has seen wide adoption across data centers (64%), WANs (58%), and access networks (40%)
- Advantages:
  - Centralized network provisioning and management
  - Reduced Capital Expenditures
  - Reduced operational cost
  - Security Approach
- Disadvantages:
  - ? Network Infrastructure changes
  - ? Security issues
  - ? Taining and learning curve

الـ Security ممكن تكون نقمة أو نقمة.

بتلزم أغيرلي وبده تحضيرات طويلة

بإنه اشي جديد وكيف بتعرف عليه

SDN Controllers

There are many SDN controllers that have been developed over the years:

- Beacon
- Floodlight
- OpenDaylight
- Nox
- Pox

Mininet

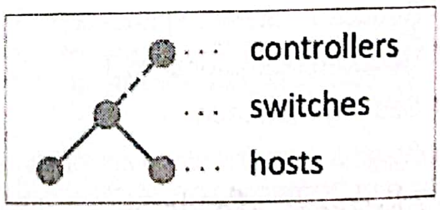
حنشتغلها بالاسايمنت

Simulator ← Mininet

- Mininet creates a realistic virtual network, running real kernel, switch and application code, on a single machine (VM, cloud or native), in seconds, with a single command.

> sudo mn

بـ Command واحد
يبني Network كاملة
وبقدر أعطي الـ Config Command
لأكبر عدد الـ Nodes
وهكذا.



Real Environments الشغل فيها
Simulation مش .

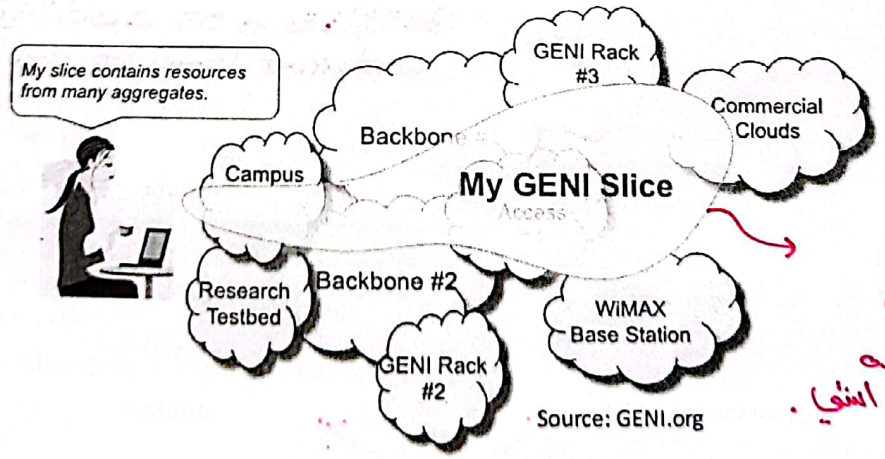
GENI (1)

- GENI (Global Environment for Network Innovations) provides a virtual laboratory for networking and distributed systems research and education.
- It is used to explore networks at scale
- Why GENI?
  - *A large-scale experiment infrastructure.*
  - *Non-IP connectivity across resources*
  - *Deep programmability*
  - *Reproducibility* ← إذا عملت تجربة في الـ GENI بقدر أكررها، وتحت نفس الظروف
  - *Instrumentation and measurement tools*

41

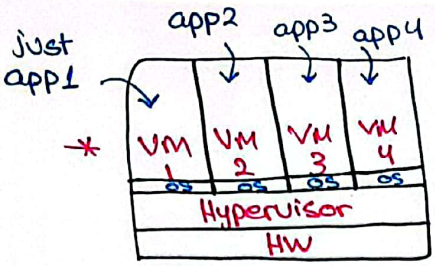
GENI (2) ← مجموعة من الـ Clouds

المفروض إنهم جامعات .



شريحة من الـ GENI بحدد شو بده فيها وكل اشي .

42



بيأوهم كل App إنه الله OS خاص فيه لإنه بدنا السيناريو في بطء كبير (Slide 44)

3/9/2022

Operating System Virtualization (1)

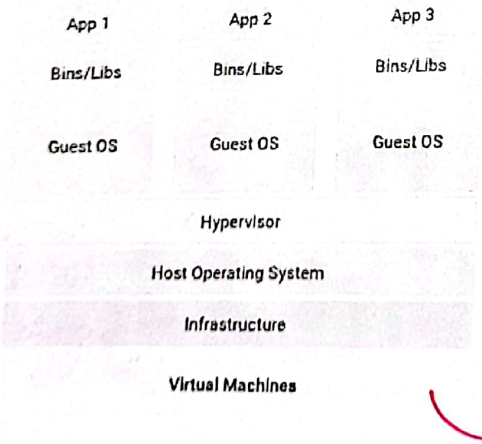
- A logical packaging mechanism in which application and its dependencies/ lib. can be abstracted from the environment in which they run (OS)
- Instead of virtualizing the hardware stack as with the virtual machines approach, containers virtualize at the operating system level, with multiple containers running atop the OS kernel directly.
- There are many container formats available. Docker is a popular, open-source container format that is supported on Google Cloud Platform

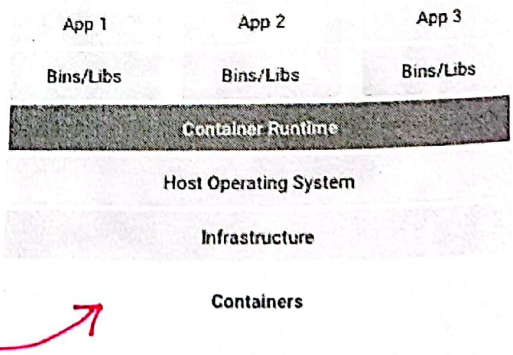
43

Operating System Virtualization (2)

light weight VM ← أسرع .

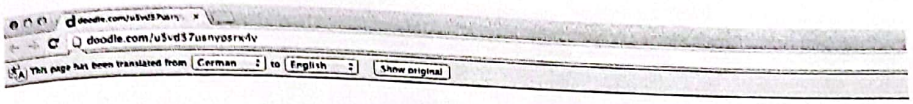
كل App متفكر إنها نازلة OS مختلفة بس بالحقيقة كلهم OS وحدة نازلة على Container عبارة عن isolated Invironment





44

Another Problem…Doodle on 09-30-13_6:28pm CST



Doodle is currently under heavy load and can not serve all requests. Please try again in a few minutes. We're sorry for the inconvenience.

Doodle is just under heavy load and can not answer all inquiries. There is a temporary problem. Please try again in a few minutes. We apologize for any inconvenience.

تصميم الديزاين
هو اللي ممكن يسبب زي هالمشكلة

* "Designing intelligent elastic cloud architectures, so that infrastructure runs only 'when you need it' and 'as you need it', is an art in itself."

61

response ماني
كل request كنه

Reading

Hiran,K.K.,Doshi,R.,Fagbola,D.T., & Mahrishi,M.(2019). *Cloud Computing: Concepts, Architecture and Applications with Real –world examples and Case studies*. BPB Publications.

Chapter 4

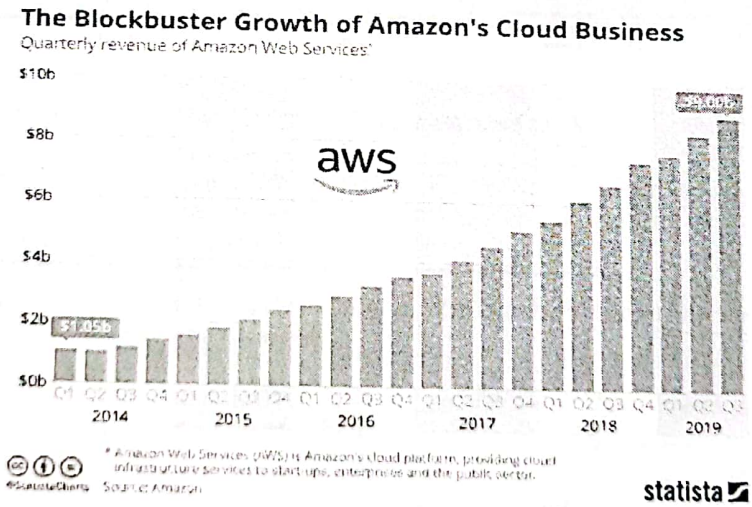
Erl,T., Puttini,R., & Mahmood,Z.(2013). *Cloud computing: concepts, technology, &architecture*.

Pearson Education. Chapter 4, capter 5.3

AWS Concepts

CPE 0907523 Cloud Computing, Spring 2022

AWS Growth



* Amazon كانوا بيشغلوا Virtualization زمان.

3/8/2022

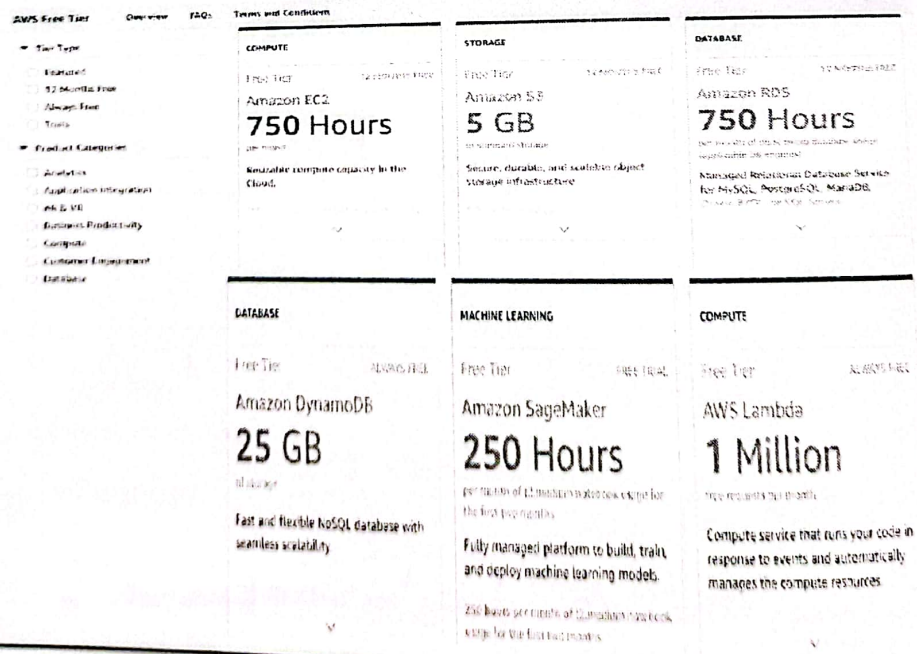
Cloud Service Provider ↩

Top 10 AWS Cloud Computing Services

* Amazon Elastic Compute Cloud (EC2) → Virtual Server (Virtual Machine)
* Amazon Simple Storage Services (S3) → Storage Service
* Elastic Block Storage (EBS) → Storage Service
* Amazon Elastic Load Balancing (ELB)
* Amazon Relational Database Service
* Amazon DynamoDB
* Auto Scaling
* Amazon ElastiCache
* Identity and Access Management (IAM) → User Management يتعامل فيها
* Amazon Elastic Cache

بيعطوك limit معينة ↩

AWS Free Tier . Free tier ال



Free Tier Usage Limits

- All services that offer a AWS Free Tier have limits on what you can use without being charged. Many services have multiple types of limits. For example, Amazon EC2 has limits on both the type of instance you can use and how many hours you can use in one month. Amazon S3 has a limit on how much storage you can use and on how often you can call certain operations each month.
  In some cases, leaving your resources running minimizes your AWS Free Tier benefits.

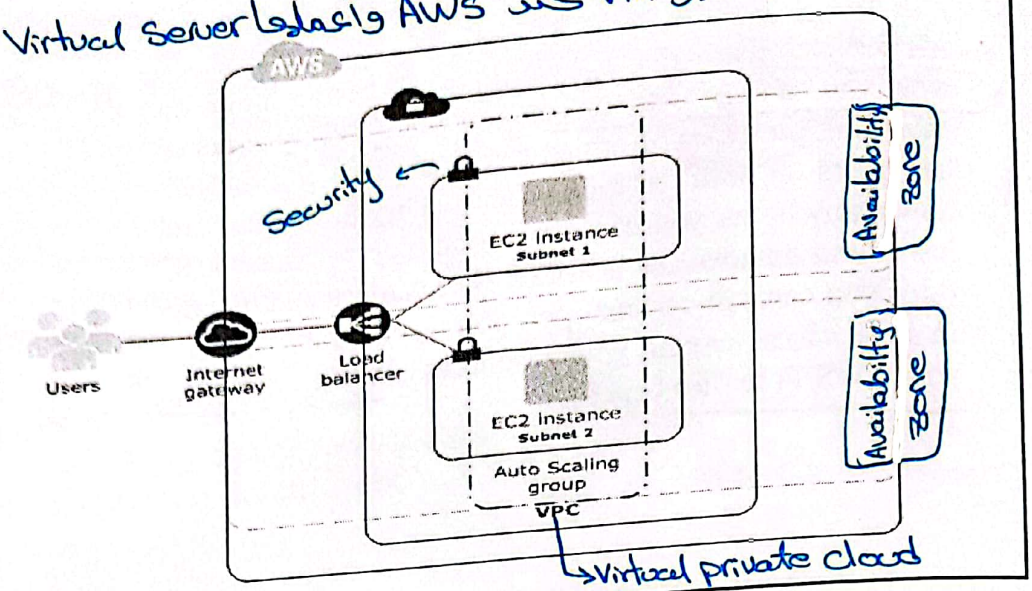
$100 Credit /Student (AWS Educate)

- **Students will receive a $100 AWS usage credit.**
- **Although each assigned lab session will only use free-tier resources**, the credit is helpful if there are accidental charges or if a student would like to experiment with any advanced AWS capabilities.
- **If a student exceeds the $100 usage credit, he/she will be responsible for payment of any overage charges.**
- You will be provided instructions in AWS Lab 1 to setup billing alerts to monitor usage, and **at the end of each AWS lab session, you should turn off your instances**

((EC2))

Elastic Cloud Computing

"Virtual Server لعملاء AWS في VM احجز"



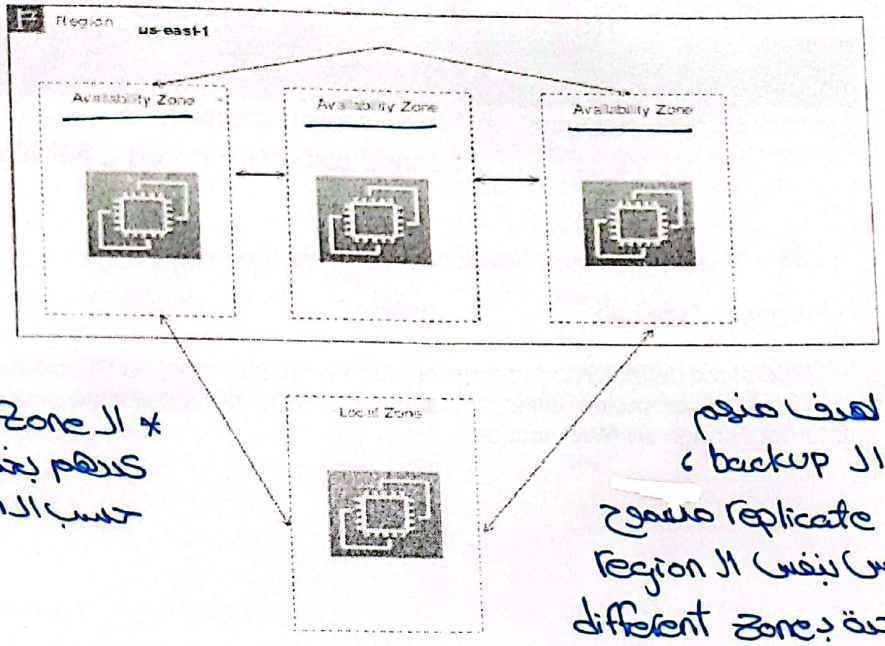
Regions and Availability Zones (1)

AWS مقسمة عشوى العالم (30) data center

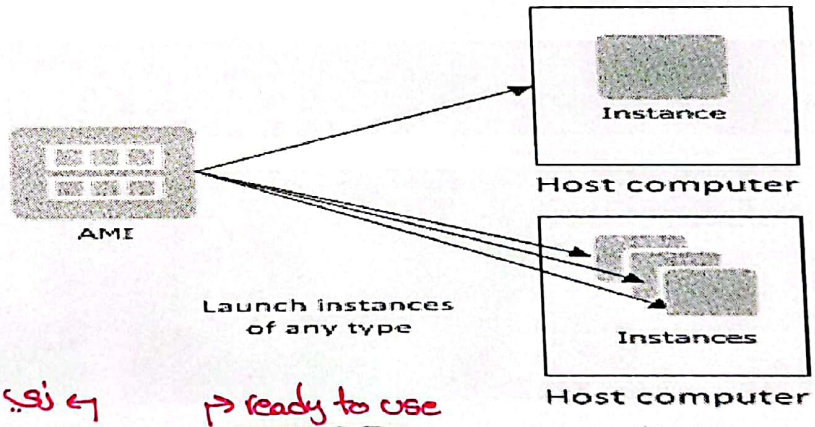
أقرب وحدة إلى البحرين.

Ohio	
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka-Local)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Middle East (Bahrain)	me-south-1
South America (São Paulo)	sa-east-1

Regions and Availability Zones (2)



Instances and AMIs



An *Amazon Machine Image (AMI)* is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, you launch an *instance*, which is a copy of the AMI running as a virtual server in the cloud.

Lab-1 Steps and 'what to turn-in'

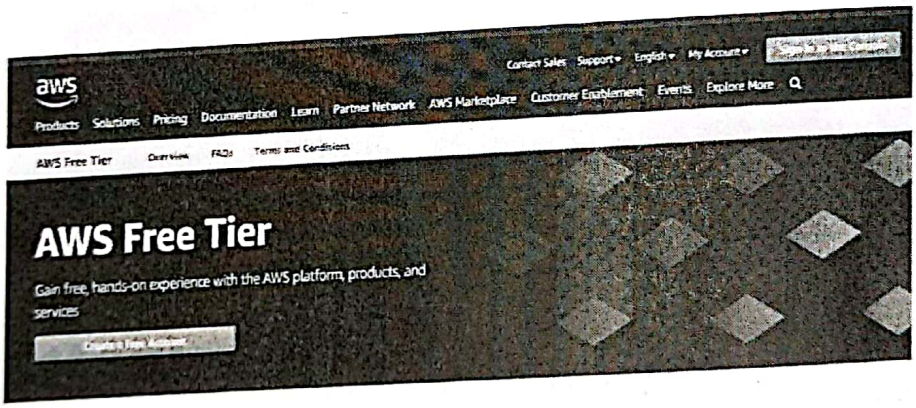
Amazon Web Services → AWS account creation →
Launch instance → Add a bill alarm

- **Lab # 1 – AWS Account Setup and Services Overview**
- **Purpose of the Lab**

– Understand definitions of various Amazon Web Services (AWS) and their use in cloud computing based web applications that are accessible over the Internet through an AWS account.

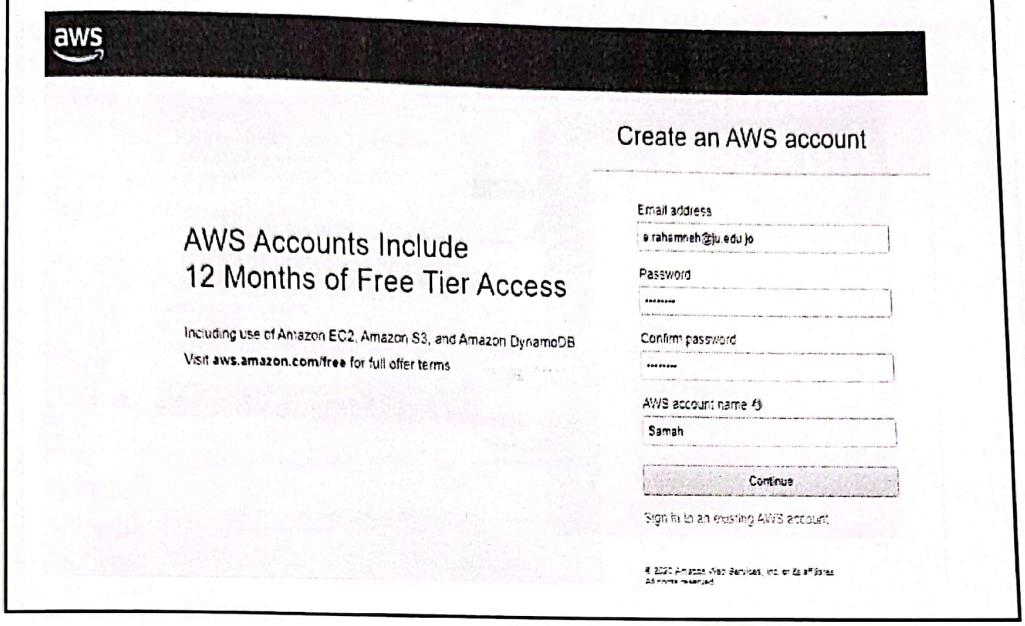
* لما أعمل Sign up بكون أنا الـ« Root user

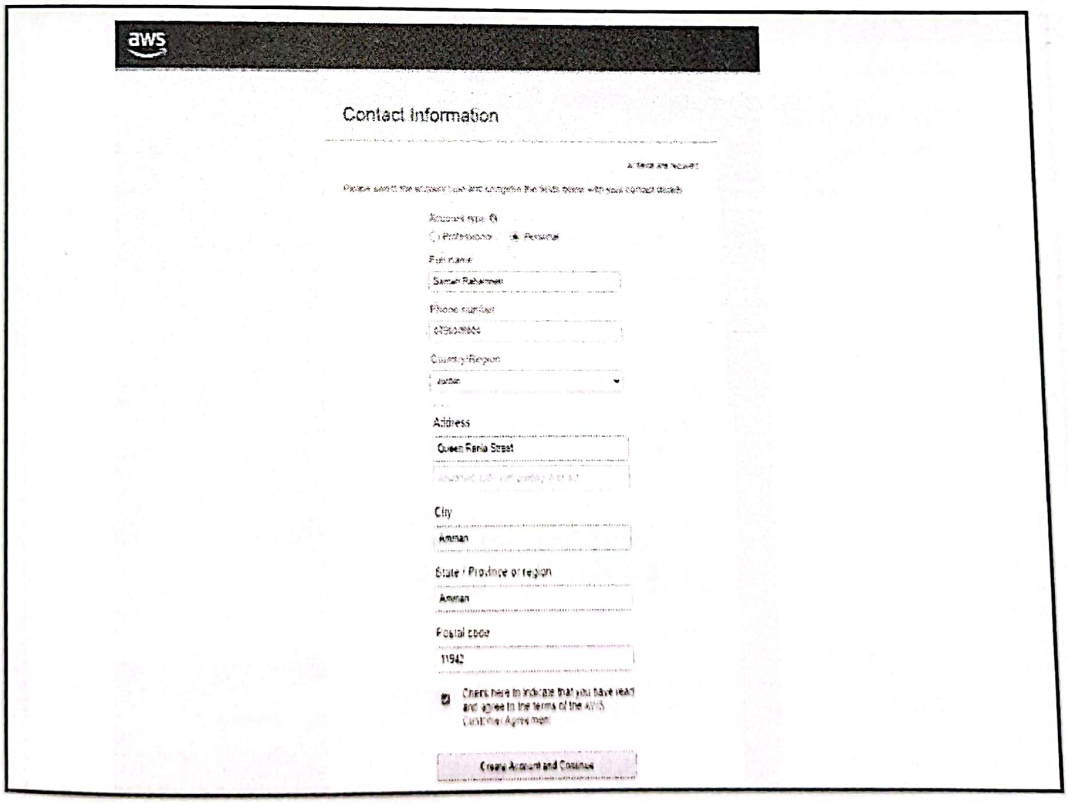
Create a free AWS account (1)

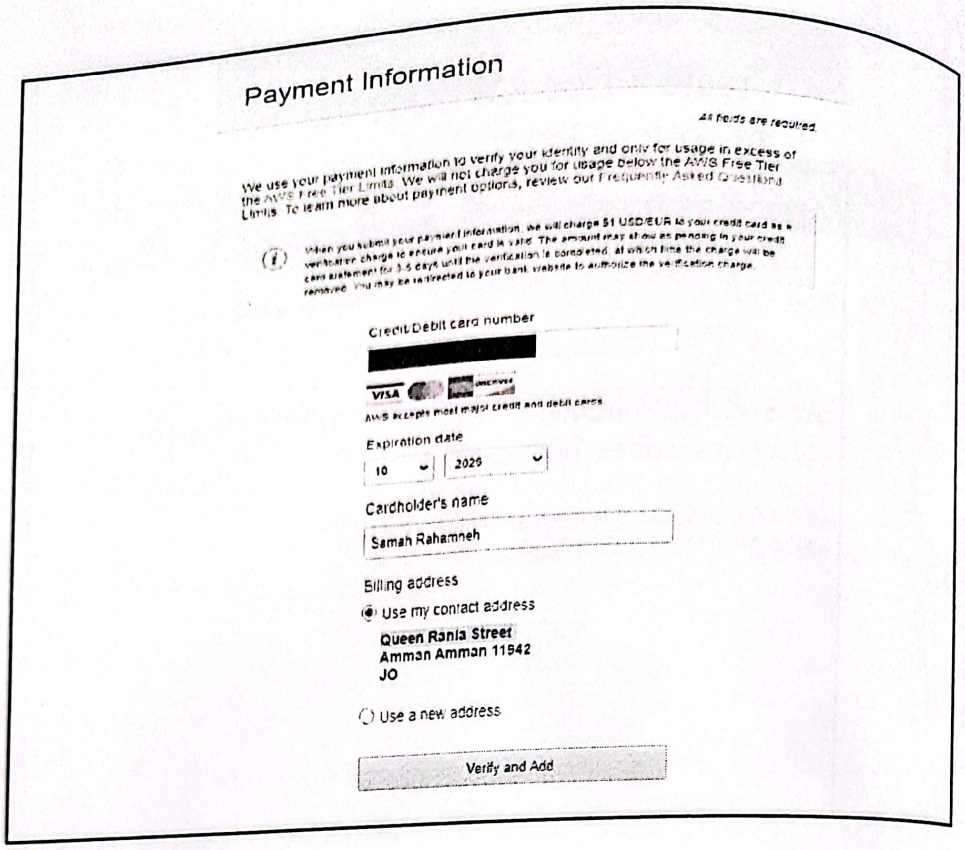


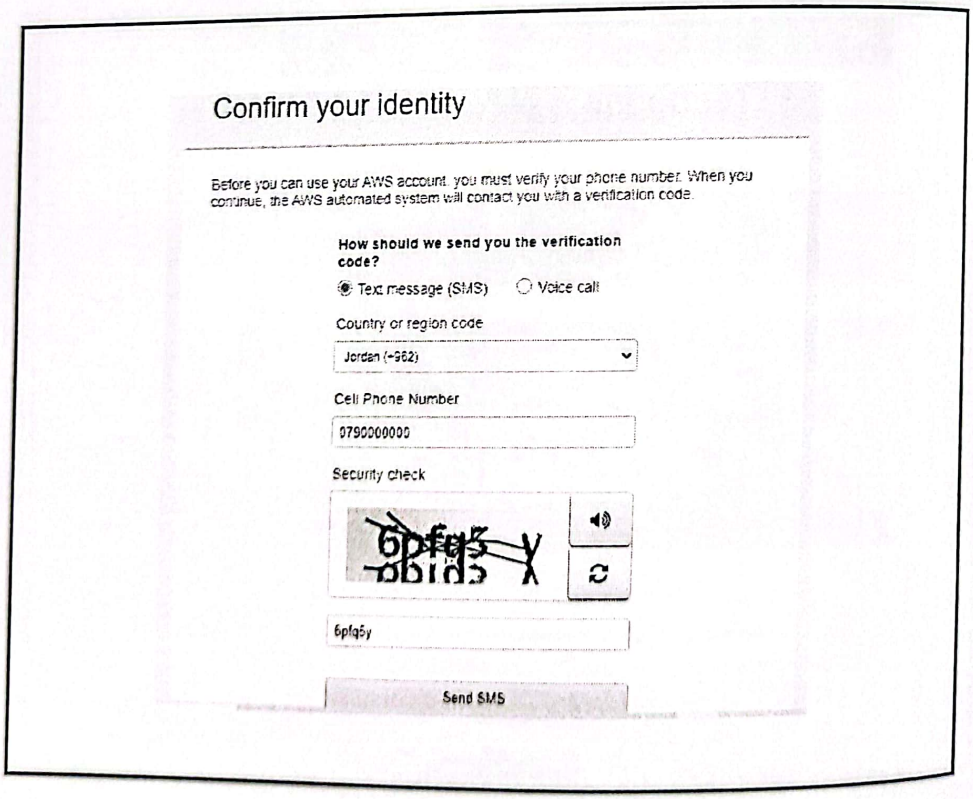
Types of offers

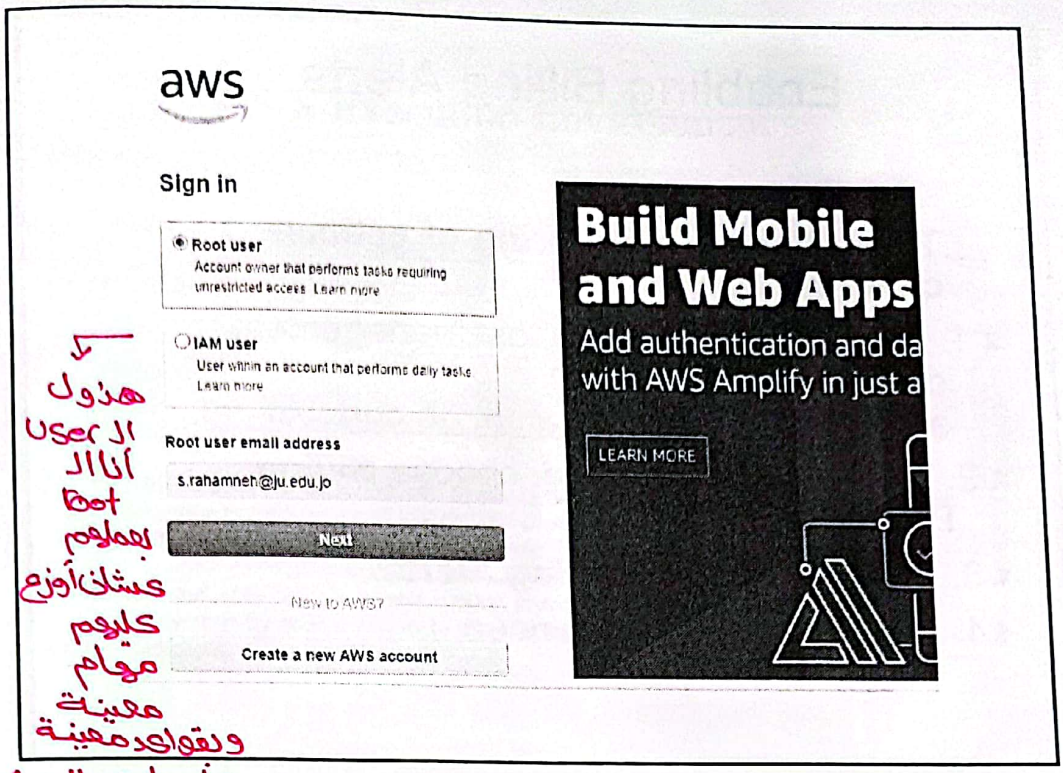
Create a free AWS account (2)



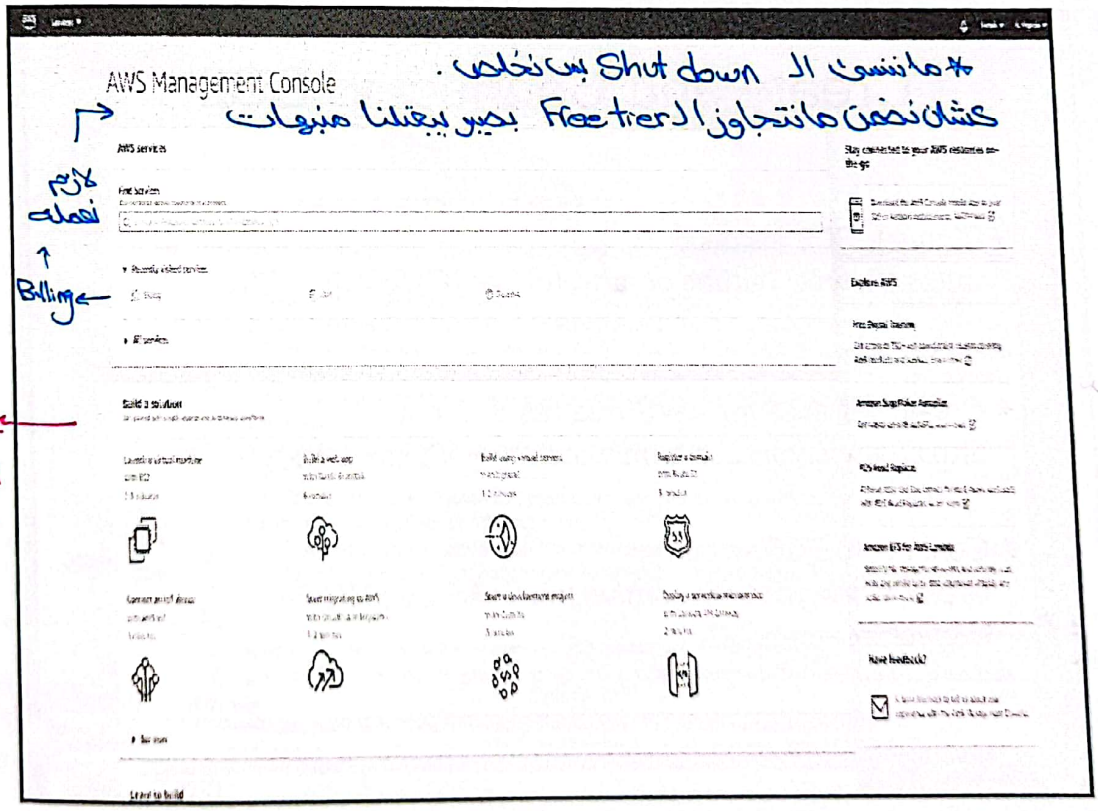



Payment Information
All fields are required.
We use your payment information to verify your identity and only for usage in excess of the AWS Free Tier Limits. We will not charge you for usage below the AWS Free Tier Limits. To learn more about payment options, review our Frequently Asked Questions.
When you submit your payment information, we will charge $1 USD/EUR to your credit card as a verification charge to ensure your card is valid. The amount may show as pending in your credit card statement for 3-5 days until the verification is completed, at which time the charge will be removed. You may be redirected to your bank website to authorize the verification charge.
Credit/Debit card number
[redacted]
VISA
AWS accepts most major credit and debit cards
Expiration date
10
2029
Cardholder's name
Samah Rahamneh
Billing address
Use my contact address
Queen Rania Street
Amman Amman 11942
JO
Use a new address
Verify and Add


Confirm your identity
Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.
How should we send you the verification code?
Text message (SMS)
Voice call
Country or region code
Jordan (+962)
Cell Phone Number
0790000000
Security check
6pfq5y
Send SMS



هذول الـ User اللي الـ Root بعطوهم عشان أوزع كل يوم مهام معينة وبقواعد معينة مانبعطوهم المسؤولية لأشياء كبيرة.



* ماننسى الـ Shut down بس نخلص.

عشان نضمن ماتتجاوز الـ Free tier بحيث يبعتلنا تنبيهات

لازم نعمله

يبين عدد الـ AWS اللي عندهم وتقلي

Enabling Billing Alerts

- **To enable the monitoring of estimated charges**

1. Open the Billing and Cost Management console at https://console.aws.amazon.com/billing/.
2. In the navigation pane, choose **Billing Preferences**.
3. Choose **Receive Billing Alerts**.
4. Choose **Save preferences**.

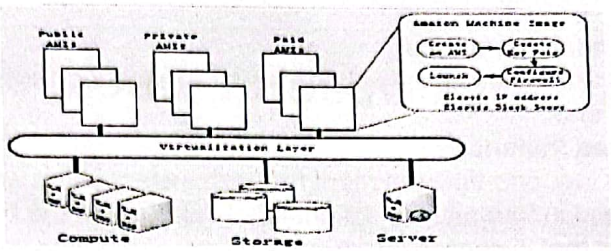
Create and Connect to EC2

* Launch EC2 instance: https://www.youtube.com/watch?v=4GUc6LzW_PM

* Create bill alert for AWS free tier account: https://www.youtube.com/watch?v=pXTxmXhRZV4

* Connect to EC2 w/putty: https://www.youtube.com/watch?v=bi7ow5NGC-U&feature=emb_title

AWS Execution Environment



Private AMI: Images created by you, which are private by default; you can grant access to other users to launch your private images.
- **Private AMI:** Images created by users and released to the community, so anyone can launch instances based on them and use them any way they like.
- **Paid AMI:** You can create images providing specific functions that can be launched by anyone willing to pay you per each hour of usage on top of AWS charges.

AWS Access Credentials

- Credential type you use depends on the type of AWS API

① – **Access Keys**
- To make secure REST or Query protocol requests to any AWS service API
- Parts and Usage
  - *Access Key ID*—Your Access Key ID identifies you as the party responsible for service requests; you include it in each request, so it's not a secret
  - *Secret Access Key*—Each Access Key ID has a Secret Access Key associated with it; This key is used to calculate the digital signature that you include in the request; Your Secret Access Key is a secret, and only you and AWS should have it

② – **X.509 Certificates**
- To make secure SOAP protocol requests to AWS service APIs
- Parts and Usage
  - *X.509 Certificate* – holds the public key and related metadata; You include it in each service request, so it's not a secret
  - *Private Key*—Each certificate has a private key associated with it; Use the private key to calculate the digital signature to include in the request; Your private key is a secret, and only you should have it and AWS doesn't keep a copy

③ – **Key Pairs**
- To launch and then securely access your Amazon EC2 instances
- You can make as many as you like by giving friendly names (can't replace any particular key pair)
- Private key that you keep with you; Public key that AWS keeps to allow access

لنفكر انه رخيصة بس هي من كثرة الاستخدام حتحس بالتكلفة.
خاصة للشركات الكبيرة

Cost Saving Considerations in AWS

* **On-Demand Instances**
  – Pay for compute capacity by the hour with no long-term commitments
* **Reserved Instances** ← للشركات الكبيرة
  – Make a low, one-time payment for each instance you want to reserve and in turn receive a significant discount on the hourly charge for that instance
  بأجروها بشروها بدل ما يدفعوا عالساعة ما بيزمنا
* **Spot Instances**
  – Bid on unused EC2 capacity and run those instances for as long as their bid exceeds the current Spot Price7

* الـ Instance ممكن أحجزها مدى الحياة (هذا اللي بهمك تعرفه)

Other Best Practices…

← بيجي عليها أسئلة لازم نقرأها وبناقشها بالمحاضرة.

* AWS Lab-1 Reading
  https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf
* Design for failure and nothing will fail → من البداية بتعرف نقاط الضعف وبتشتغل عليها وبتجرب نظامي
* Decouple your components ← أحاول ما أخلي في اعتمادية بين الـ Components قدر الإمكان
* Implement elasticity → الـ System لازم يكون مرن
* Think parallel ← حاول قدر الإمكان تحققه
* Keep dynamic data closer to compute and static data closer to user → حاول خلي كل اشي قريب من اللي بحتاجه
* Know security and performance tradeoffs → اشي مقابل اشي
  ← أحسن اشي مقابل اشي، يعني لو زدت Security كثير رح أخسر Performance فلازم أحدد مين الأولى عندي واشتغل عليه.
* Another great link for high scalability, architecture case studies
  – http://highscalability.com/ → اقرأ عنهم.
  - 'Building bigger, faster, more reliable websites
  - YouTube Architecture
  http://highscalability.com/youtube-architecture
  – Good Dashboard Example:
  https://stackexchange.com/performance
  اقرئيه

تقف وبجرب شوائب وبشوف كيف حيتم التصرف
↑ Kios Monkey
↑ like Netflix ← عشان أشوف كيف بتصرف

Critical Services → Security اولا
Non-Critical → Performance اولا

Part-III: Cloud Infrastructure Mechanisms

CPE 0907523 Cloud Computing, Fall 2020

Dr. Samah Rahamneh

Slides adapted from Erl, Mahmood, and Puttini

« مرحلة بناء الـ Cloud Server »

Cloud Infrastructure Mechanisms

ال basic اللي بحتاجهم لبناء ال cloud .

- Cloud infrastructure mechanisms are foundational building blocks of cloud environments that establish primary artifacts to form the basis of fundamental cloud technology architecture.
- Cloud infrastructure mechanisms: → Cloud data center server بحتاجهم لأبني
  - Logical network perimeter
  - Virtual server
  - Cloud storage device
  - Cloud usage monitor
  - Resource replication
  - Ready-made environment

- Not all of these mechanisms are necessarily broad-reaching, nor does each establish an individual architectural layer. Instead, they should be viewed as core components that are common to cloud platforms.

Logical Network Perimeter (1)

Virtual = Logical

- LNP is the isolation of a network environment from the rest of a communications network.
- LNP establishes a virtual network boundary that can encompass and isolate a group of related cloud-based IT resources that may be physically distributed.
- LNP are typically established via:
  1. *Virtual Firewall* – An IT resource that actively filters network traffic to and from the isolated network while controlling its interactions with the Internet.
  2. *Virtual Network* – Usually acquired through VLANs, this IT resource isolates the network environment within the data center infrastructure.

Logical Network Perimeter (2)

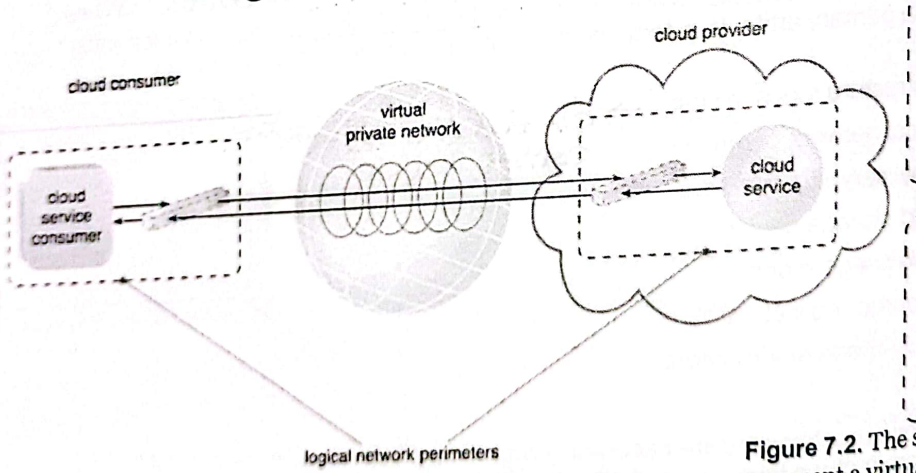


Figure 7.3. Two logical network perimeters surround the cloud consumer and cloud provider environments.

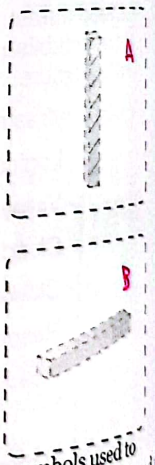


Figure 7.2. The symbols used to represent a virtual firewall (top) and a virtual network (bottom).

Virtual Servers (1)

نفس ما اشتغلنا بأول لاب.

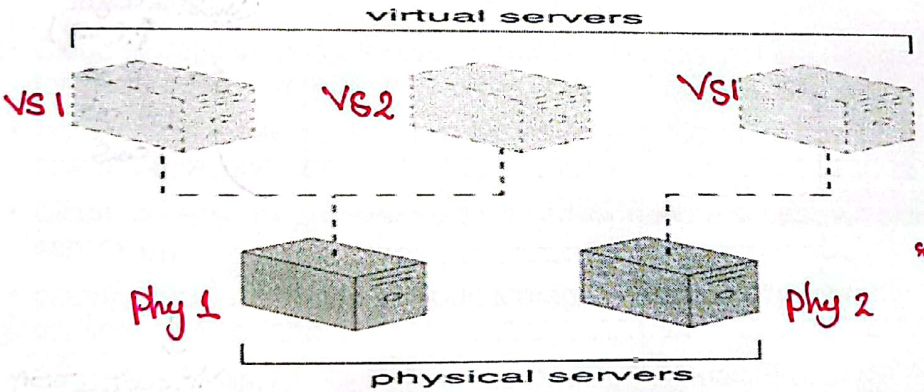
* *A virtual server* is a form of virtualization software that emulates a physical server. Virtual servers are used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances.

* Each virtual server can host numerous IT resources, cloud-based solutions, and various other cloud computing mechanisms. The instantiation of virtual servers from image file is resource allocation process that can be completed rapidly and on-demand.

بيعطوك نسخة اله وبتشغلها لبه ← مكتوبة بلغة 0,1

* (AMI) = Amazon Machine Images.

Virtual Servers (2)



بتغير عدد الـ Virtual servers مع الوقت.
وعددهم بيعتمد على خصائص Phy. server والـ load اللي بتتحمله + على نوعهم لو ثقيل أو لا

Figure 7.5. The first physical server hosts two virtual servers, while the second physical server hosts one virtual server.

Virtual Servers (3)

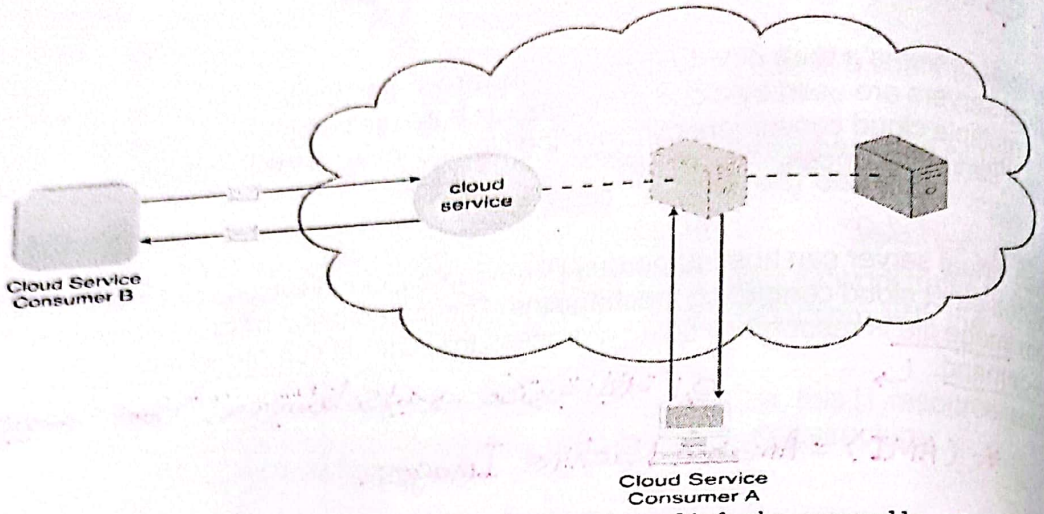


Figure 7.6. A virtual server hosts an active cloud service and is further accessed by a cloud consumer for administrative purposes.

« بتجيب صور ناقصة وبتطلب تكملوها »

Virtual Servers (3)

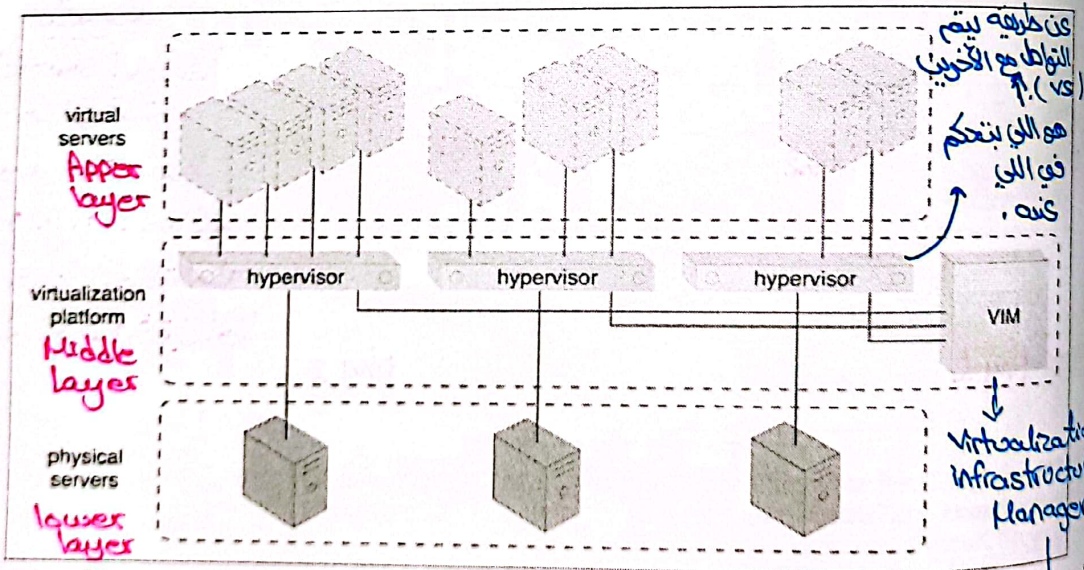


Figure 7.7. Virtual servers are created via the physical servers' hypervisors and a central VIM.

عن طريقه يتم التواصل مع الأخرين (VS).
هو اللي بتحكم في اللي تحته.
المتحكم الأكبر (يعمل control لكل الـ hypervisors) + (فيه كل المعلومات).
والـ hypervisor لما احتاج شي من كيف بطلبه منه.

Virtual Servers (4)

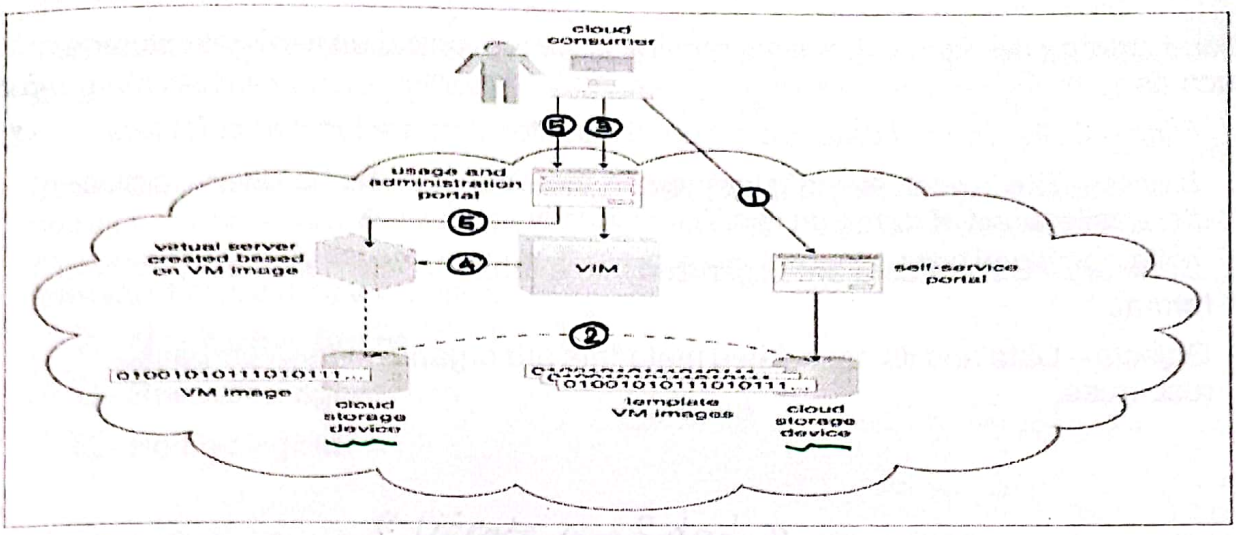


Figure 7.8. Creation and management of virtual servers.

Cloud Storage Device "مهم جدًا"

- Cloud storage device represents storage devices that are designed specifically for cloud-based provisioning. → Phy. Server على الـ VM لهاي الـ resources احجز
- Instances of these devices can be virtualized, similar to how physical servers can spawn virtual server images. (1) (2)
- Cloud storage devices can be exposed for remote access via cloud storage services.
- primary concern related to cloud storage is the security (1), integrity (2), and confidentiality (3) of data.
- Examples: Dropbox, Google drive, OneDrive, MediaFire, and AWS S3.

Cloud Storage Levels (1)

Cloud storage device mechanisms provide common logical units of data storage, such as:

1. *Files* – Collections of data are grouped into files that are located in folders.
2. *Blocks* – The lowest level of storage and the closest to the hardware, a block is the smallest unit of data that is still individually accessible.
3. *Datasets* – Sets of data are organized into a table-based, delimited, or record format.
4. *Objects* – Data and its associated metadata are organized as Web-based resources.

« lab 2 بنفوه بـ »

11

Cloud Storage Levels (2)

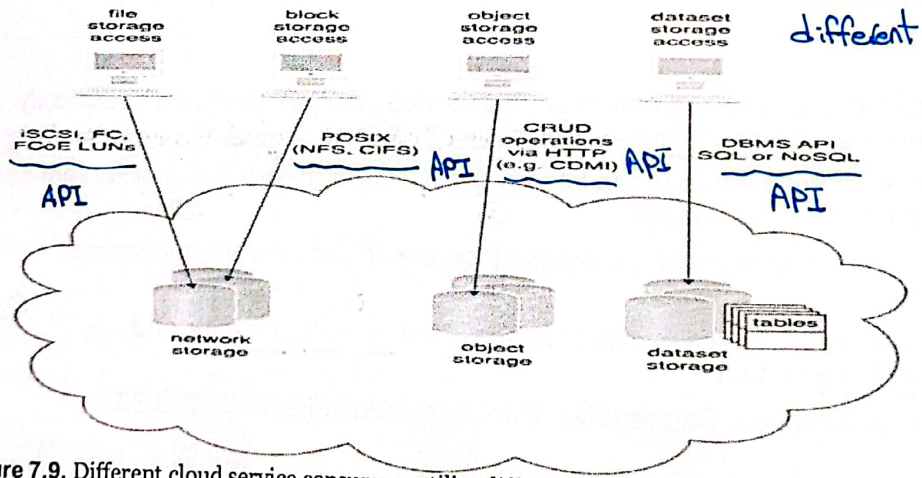


Figure 7.9. Different cloud service consumers utilize different technologies to interface with virtualized cloud storage devices. (Adapted from the CDMI Cloud Storage Reference Model.)

12

Cloud Usage Monitor

Also = pay as use

- The *cloud usage monitor* mechanism is a lightweight and autonomous software program responsible for collecting and processing IT resource usage data.

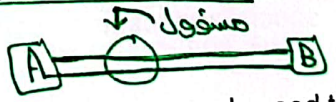
- Depending on the type of usage metrics they are designed to collect and the manner in which usage data needs to be collected, cloud usage monitors can exist in different formats. There are three common agent-based implementation formats of cloud usage monitor:
  - A - **Monitoring Agent**
  - B - **Resource agent**
  - C - **Polling agent**

collect كل واحد منهم بعمل مختلف data

Monitoring Agent (1)

- ***Monitoring agent:*** ما بشتغل إلا لو صار event معينة

  - *It* is an intermediary, event-driven program that exists as a service agent and resides along existing communication paths to transparently monitor and analyze dataflows.



  - This type of cloud usage monitor is commonly used to measure network traffic and message metrics.

Monitoring Agent (2)

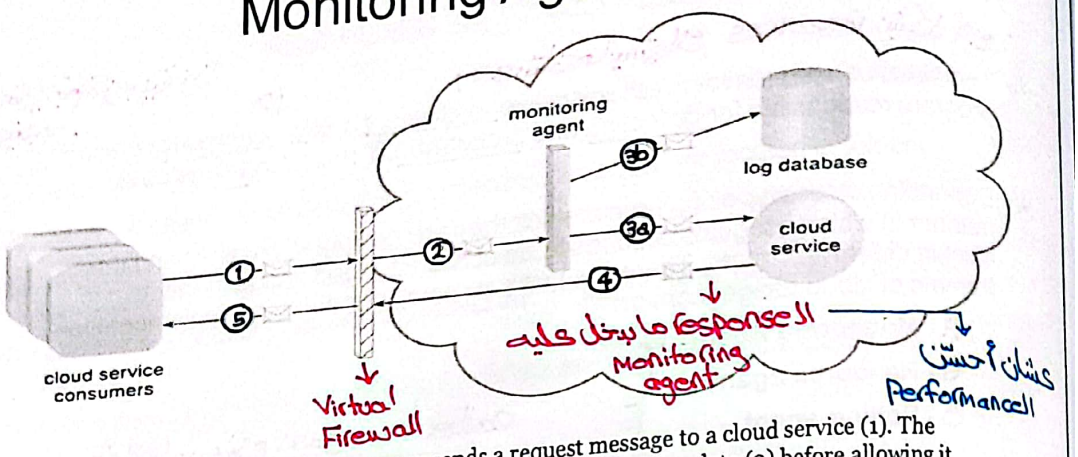


Figure 7.12. A cloud service consumer sends a request message to a cloud service (1). The monitoring agent intercepts the message to collect relevant usage data (2) before allowing it to continue to the cloud service (3a). The monitoring agent stores the collected usage data in a log database (3b). The cloud service replies with a response message (4) that is sent back to the cloud service consumer without being intercepted by the monitoring agent (5).

15

Resource Agent (1)

- **A *resource agent:***

  - It is a processing module that collects usage data by having event-driven interactions with specialized resource software.

  - This module is used to monitor usage metrics based on pre-defined, observable events at the resource software level, such as initiating, suspending, resuming, and vertical scaling.

Create
Shutdown
Restart
مسؤول عن تجميع المعلومات في هاي الحالات

16

* Scaling → أزيد الـ IT resources
  - horizontal → ... مثال تبني بيت، جنب بيت ← new phy. Servers بضيف
  - Vertical → .... مثال تبني بيت بطوابق ← نفس الـ Server بعطيه حجم أكبر وهكذا

* الأفضل بالـ Cloud هو الـ Vertical بحفظ ميزانية.

Resource Agent (2)

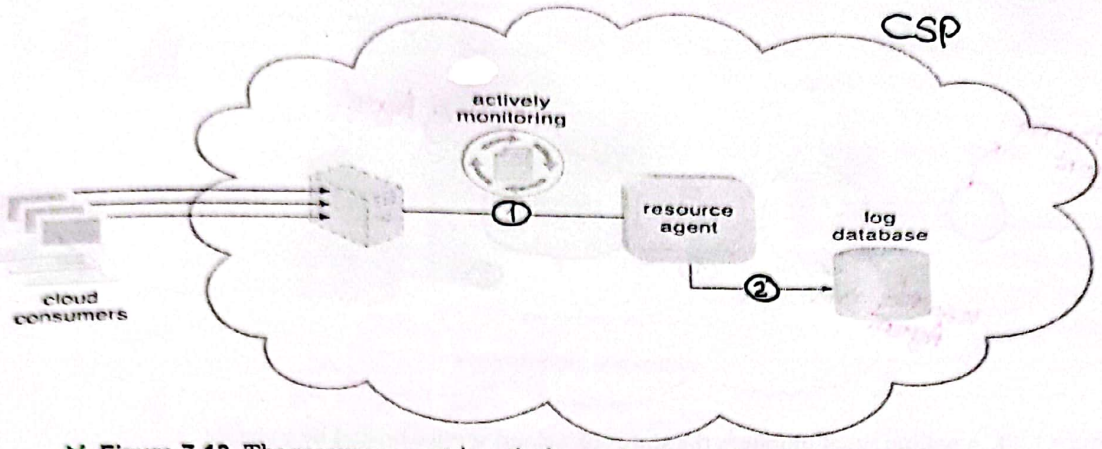


Figure 7.13. The resource agent is actively monitoring a virtual server and detects an increase in usage (1). The resource agent receives a notification from the underlying resource management program that the virtual server is being scaled up and stores the collected usage data in a log database, as per its monitoring metrics (2).

17

Polling agent (1)

- **A *polling agent:***

« اختلفوا فيهم إنه مش event-driven »

is a processing module that collects cloud service usage data by polling IT resources. This type of cloud service monitor is commonly used to periodically monitor IT resource status, such as uptime and downtime.

Read case study page 204-205, textbook 2 → مطلوبة

18

Polling agent

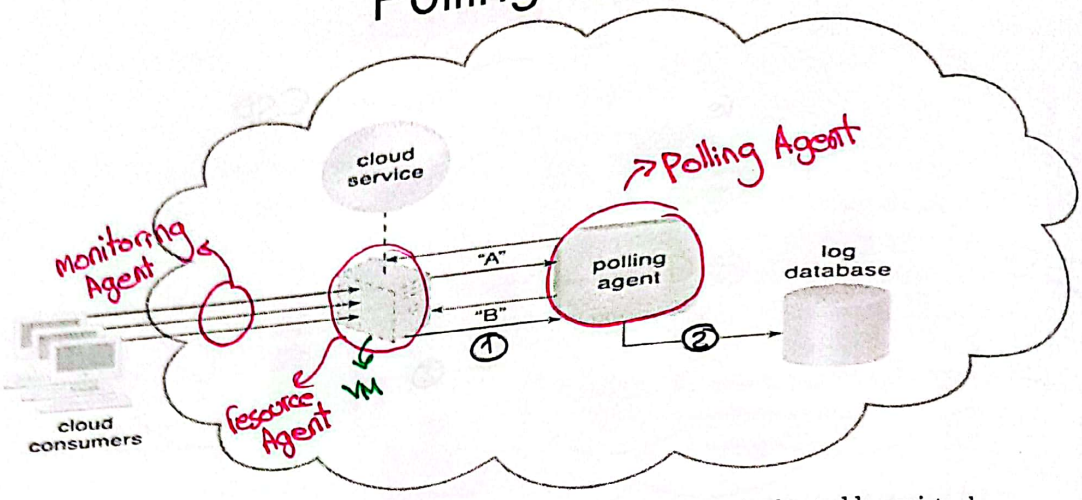


Figure 7.14. A polling agent monitors the status of a cloud service hosted by a virtual server by sending periodic polling request messages and receiving polling response messages that report usage status "A" after a number of polling cycles, until it receives a usage status of "B" (1), upon which the polling agent records the new usage status in the log database (2).

19

*SLA : Service Level Agreement

Resource Replication (1)

- Resource replication is the creation of multiple instances of the same IT resource.
  ← دائما متاحة تكون
- Replication is typically performed when an IT resource's availability and performance need to be enhanced. (related issues)
  تكون أفضل ← هايكون
- Virtualization technology is used to implement the *resource replication* mechanism to replicate cloud-based IT resources. (Traditional IT?)
  . Virtual بس Physical ← إنها تكون
- VIMs from different data centers coordinate to overcome the unavailability by reallocating the virtual server to a different physical server running in another data center. (failover)

20

performance/etc

Resource Replication (2)

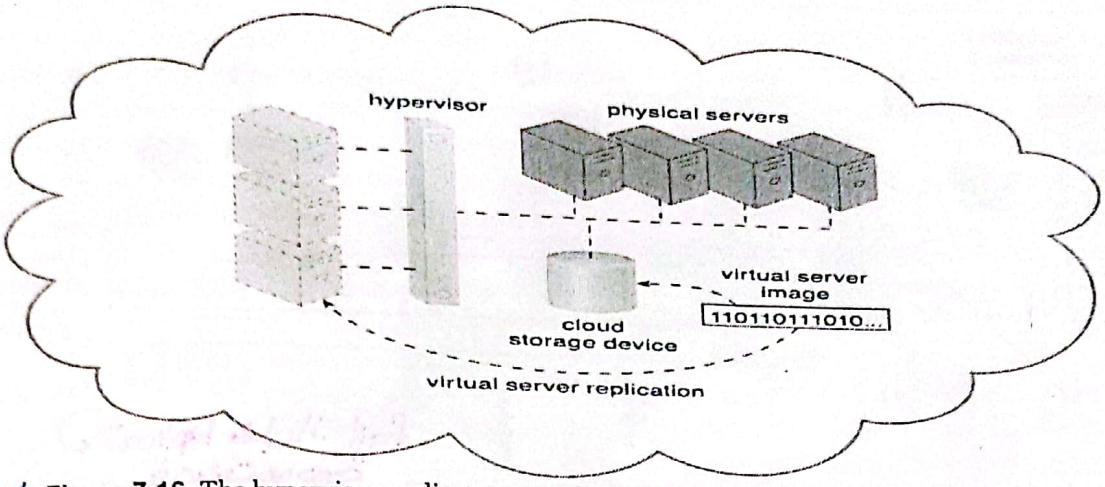


Figure 7.16. The hypervisor replicates several instances of a virtual server, using a stored virtual server image.

الـReplications بكون بنفس المنطقة (البوت)

Resource Replication (3)

بتبعوا نفس البوت

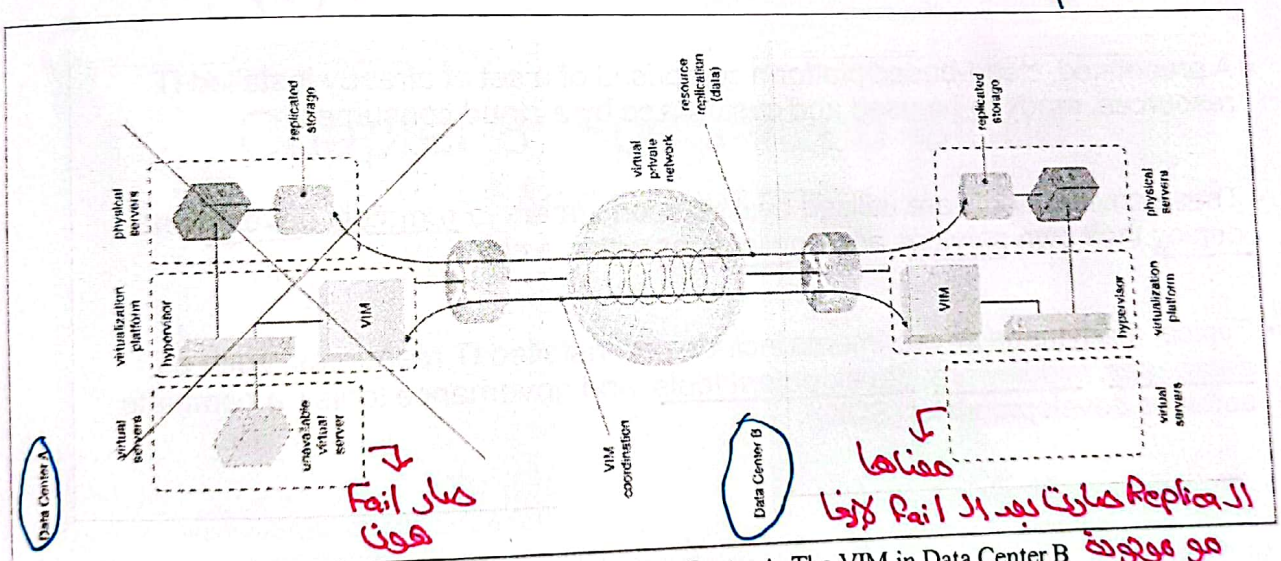


Figure 7.18. The virtual server becomes unavailable in Data Center A. The VIM in Data Center B detects the failure condition and starts to reallocate the high-availability server from Data Center A to Data Center B.

Resource Replication (4)

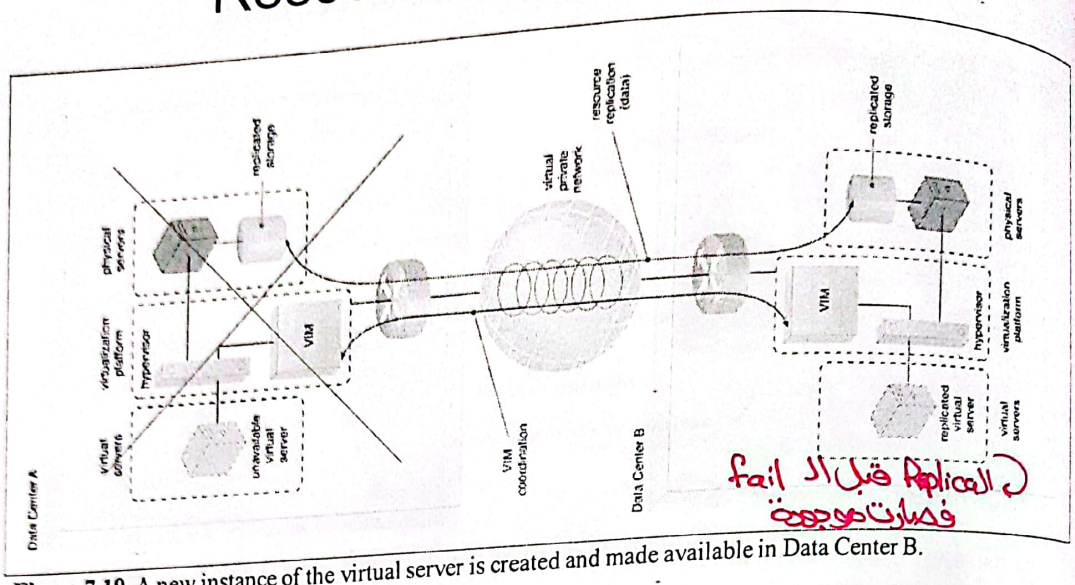


Figure 7.19. A new instance of the virtual server is created and made available in Data Center B.

23

developed جاهزة لاستخدام

Plat form as a Service [PaaS]

Ready-Made Environment (1)

- A predefined, cloud-based platform comprised of a set of already installed IT resources, ready to be used and customized by a cloud consumer.
- These environments are utilized by cloud consumers to remotely develop and deploy their own services and applications within a cloud.
- Typical readymade environments include pre-installed IT resources, such as databases, middleware, development tools, and governance tools (a complete software development kit (SDK)).

24

Ready-Made Environment (2)

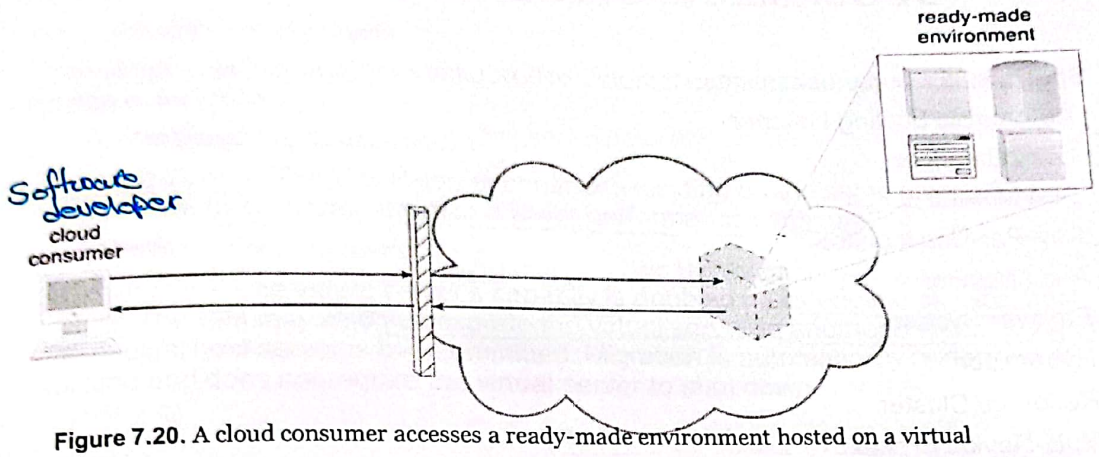


Figure 7.20. A cloud consumer accesses a ready-made environment hosted on a virtual server.

Chapter 8: Specialized Cloud Mechanisms

Specialized Cloud Mechanisms

Specialized cloud mechanisms:

- Automated Scaling Listener
- Load Balancer
- SLA Monitor
- Pay-Per-Use Monitor
- Audit Monitor
- Failover System
- Hypervisor
- Resource Cluster
- Multi-Device Broker
- State Management Database

Automated Scaling Listener (1)

- The *automated scaling listener* mechanism is a service agent that monitors and tracks communications between cloud service consumers and cloud services for dynamic scaling purposes.

يحطوها جنب الـ Firewall.

- Automated scaling listeners are deployed within the cloud, typically near the firewall, from where they automatically track workload status information.

- Workloads can be determined by the volume of cloud consumer-generated requests (1) or via back-end processing demands (2) triggered by certain types of requests.

لـ كم من الوقت بده هذا الـ Server يعمل Processing لـ Request 1

Automated Scaling Listener (2)

hypervisor+VIMs

The virtualization platform is configured to automatically scale a virtual server at runtime, as follows:

vertical or horizental

- *Scaling-Down* – The virtual server continues residing on the same physical host server while being scaled down to a lower performance configuration. → مثلاً يقلل عدد الـ cpus

vertical or horizental

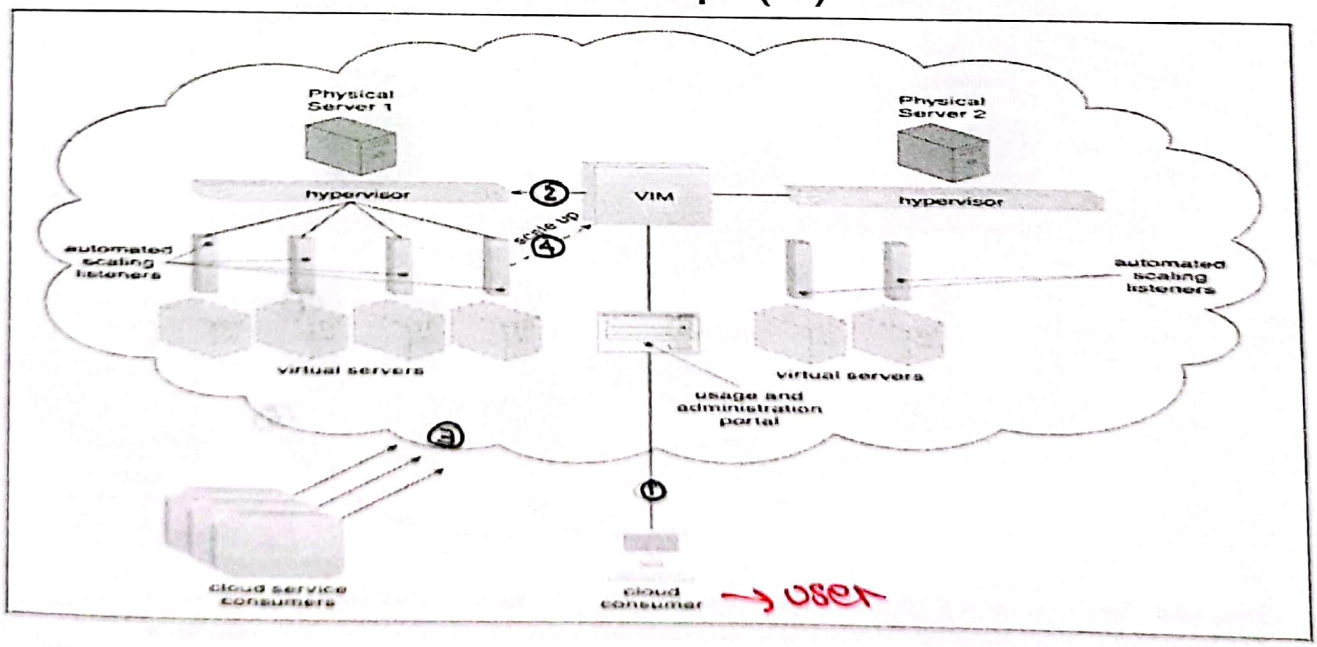
- *Scaling-Up* – The virtual server's capacity is doubled on its original physical host server. The VIM may also live migrate the virtual server to another physical server if the original host server is overcommitted. Migration is automatically performed at runtime and does not require the virtual server to shut down.

increase (1)

(2)

لو كان الأخير موقدر يعمل up Scale

Scale Up (1)



روحي آخر صفحة للتفاصيل.

Scale up

1- a cloud consumer creates and starts a virtual server with 8 virtual processor cores and 16 GB of virtual RAM.
2- The VIM creates the virtual server at the cloud service consumer's request and allocates it to physical server 1 to join 3 other active virtual severs.
3- cloud consumer demand causes the virtual server usage to increase by over 80% of the cpu capacity for 60 consecutive seconds
4- the automated scaling listener running at the hypervisor detects the need to scale up and commands the VIM accordingly.

Cloud customer بستفيد منها
Cloud service provider والـ

Scale Up (2)

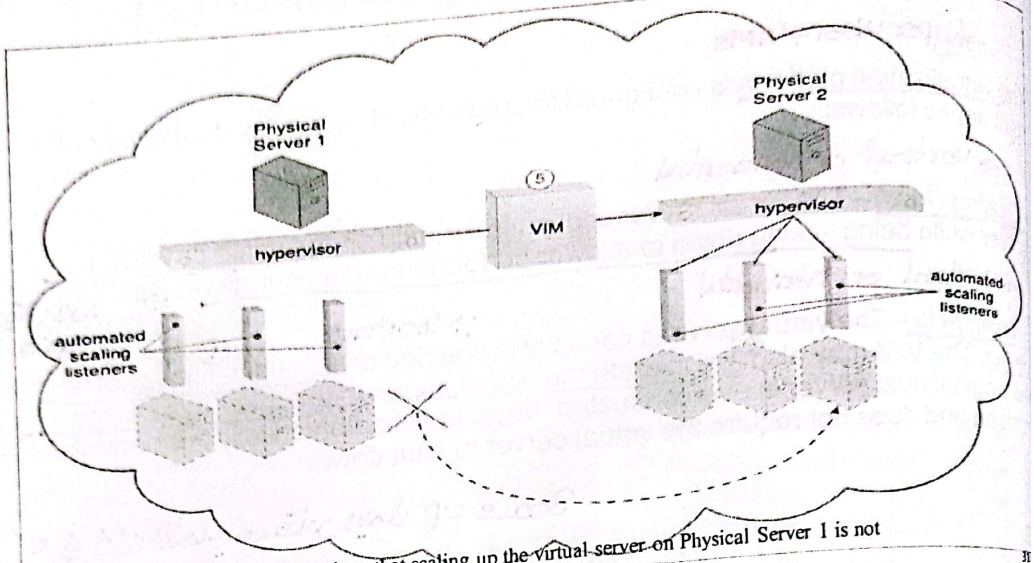


Figure 8.3. The VIM determines that scaling up the virtual server on Physical Server 1 is not possible and proceeds to live migrate it to Physical Server 2.

دائما بتزيد على الـ Physical server
ما بتعمل Migration ولكن ممكن نعملها في ظروف معينة

Scale Down

Cloud Service Provider بستفيد منها الـ

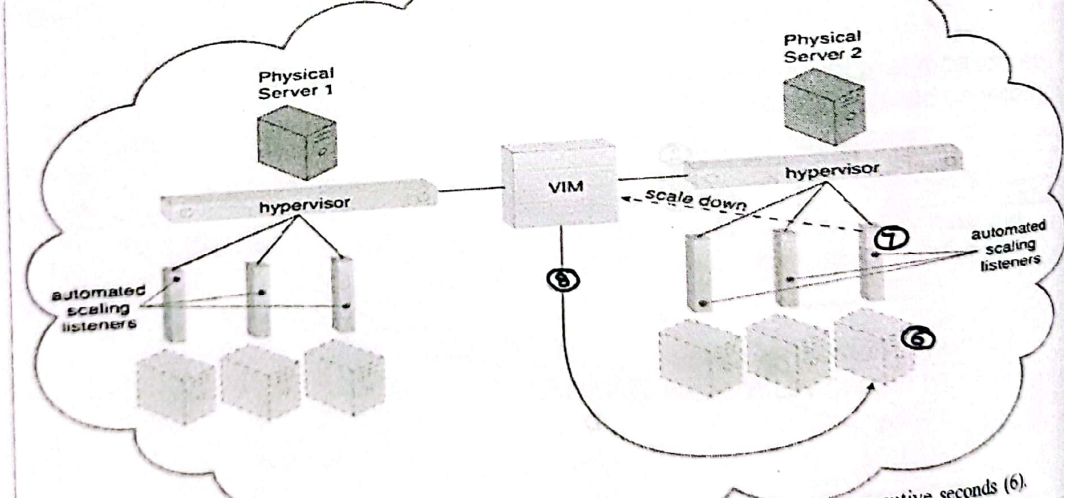


Figure 8.4. The virtual server's CPU/RAM usage remains below 15% capacity for 60 consecutive seconds (6). The automated scaling listener detects the need to scale down and commands the VIM (7), which scales down the virtual server (8) while it remains active on Physical Server 2.

* cpu utilization = $\frac{\text{Used}}{\text{Total}}$ كمية الوقت اللي الـ cpu فيها مشغول بتنفيذ instructions

Load Balancer (1)

أعامل وأوازن بين سنغلتين

- A common approach to horizontal scaling is to balance a workload across two or more IT resources to increase performance and capacity beyond what a single IT resource can provide.
- Load balancers can perform a range of specialized runtime workload distribution functions that include:
  1. - *Asymmetric Distribution* – larger workloads are issued to IT resources with higher processing capacities → higher processing عنده load أكثر للي بعطي
  2. - *Workload Prioritization* – workloads are scheduled, queued, discarded, and distributed workloads according to their priority levels
  3. - *Content-Aware Distribution* – requests are distributed to different IT resources as dictated by the request content

تقريع غير متكافئ

. distributed بناء كليه بعمل

Load Balancer (2)

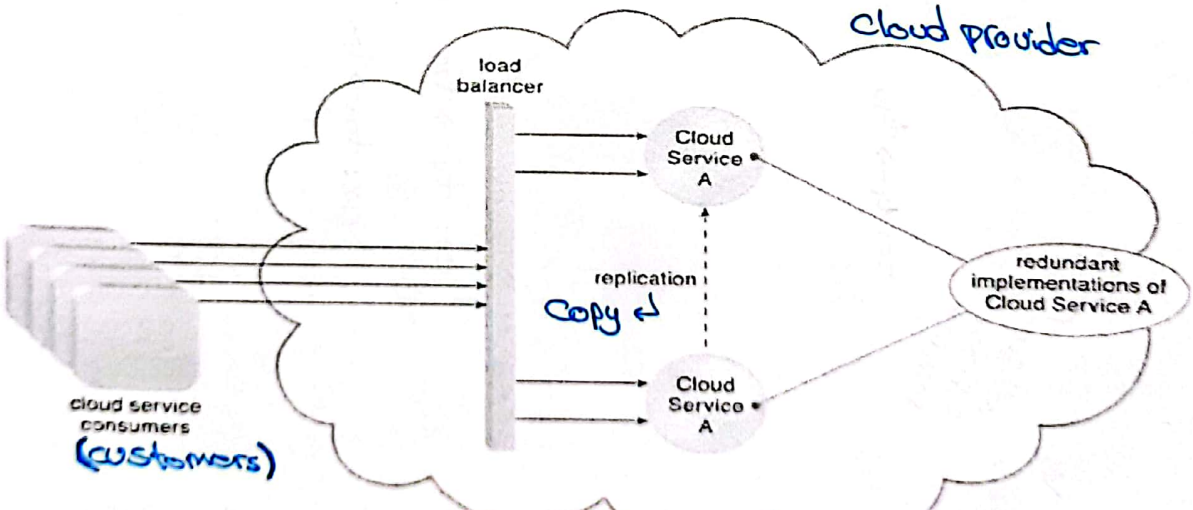
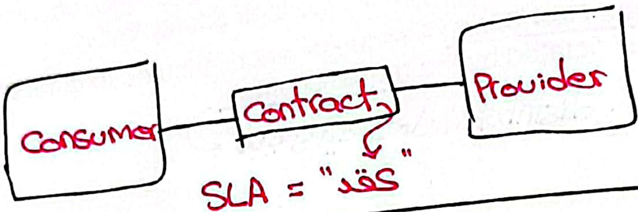


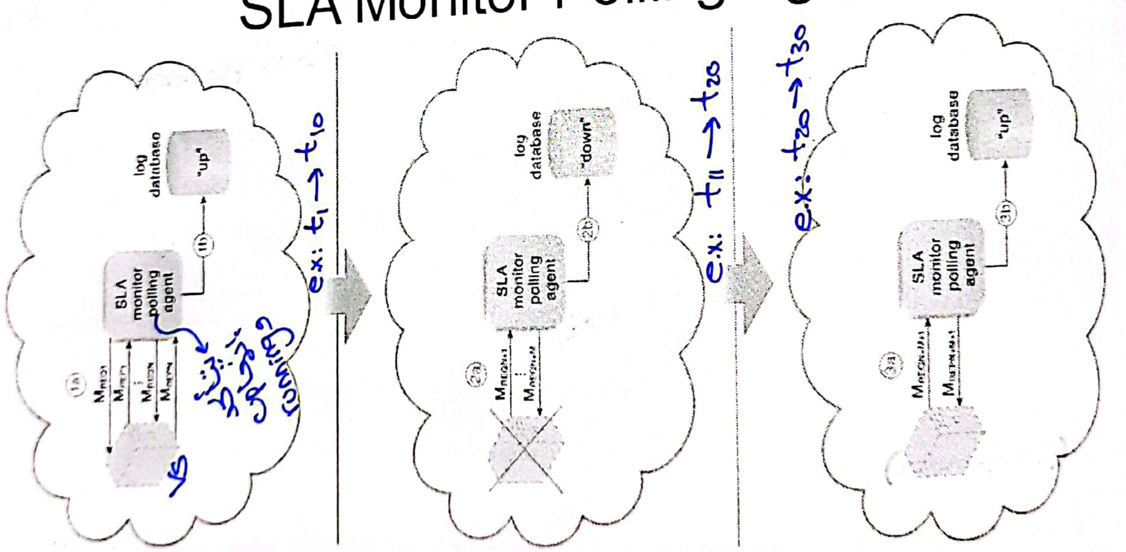
Figure 8.5. A load balancer implemented as a service agent transparently distributes incoming workload request messages across two redundant cloud service implementations, which in turn maximizes performance for the cloud service consumers.

SLA Monitor

- The SLA monitor mechanism is used to specifically observe the runtime performance of cloud services to ensure that they are fulfilling the contractual QoS requirements that are published in SLA.
- The data collected by the SLA monitor is processed by an SLA management system to be aggregated into SLA reporting metrics.



SLA Monitor Polling Agent



Pay-per-use Monitor (1)

- The *pay-per-use monitor* mechanism measures cloud-based IT resource usage in accordance with predefined pricing parameters and generates usage logs for fee calculations and billing purposes.

- Some typical monitoring variables are:
  - ① - Request/response message quantity
  - ② - Transmitted data volume
  - ③ - Bandwidth consumption

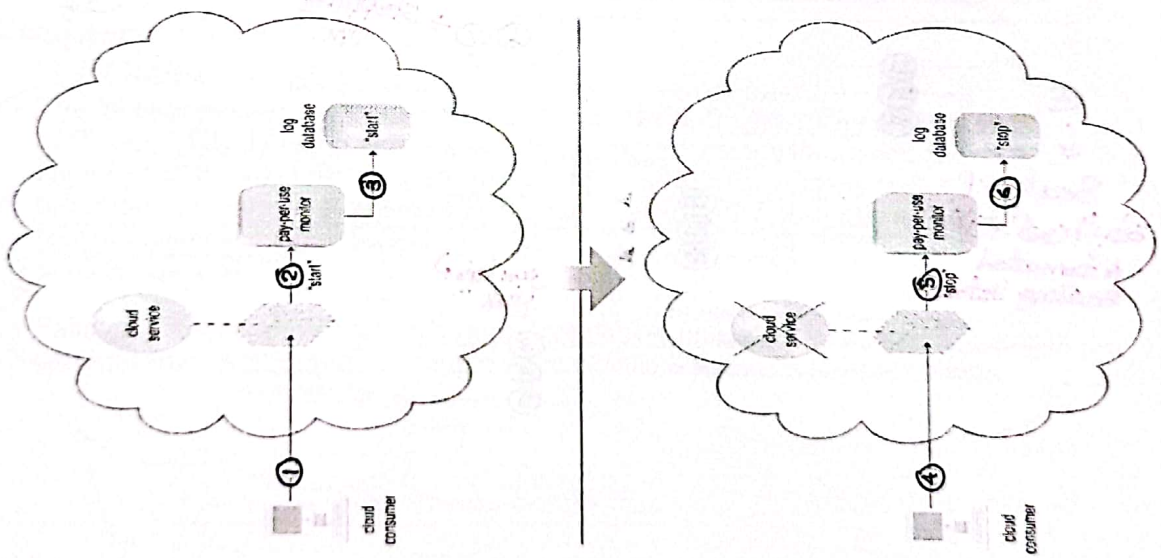
① A cloud consumer requests the creation of a new instance of a cloud service.
② The IT Resources is instantiated and the pay-per-use monitor receives a "start" event notification from the Source Software. The pay-per-use monitor stores the value timestamp in the log database.

37

③ The cloud consumer later requests that the cloud service instance be stopped
④ The pay-per-use monitor receives a "stop" event notification.

event driven

Pay-per-use Monitor (2)



38

Pay-per-use Monitor (3)

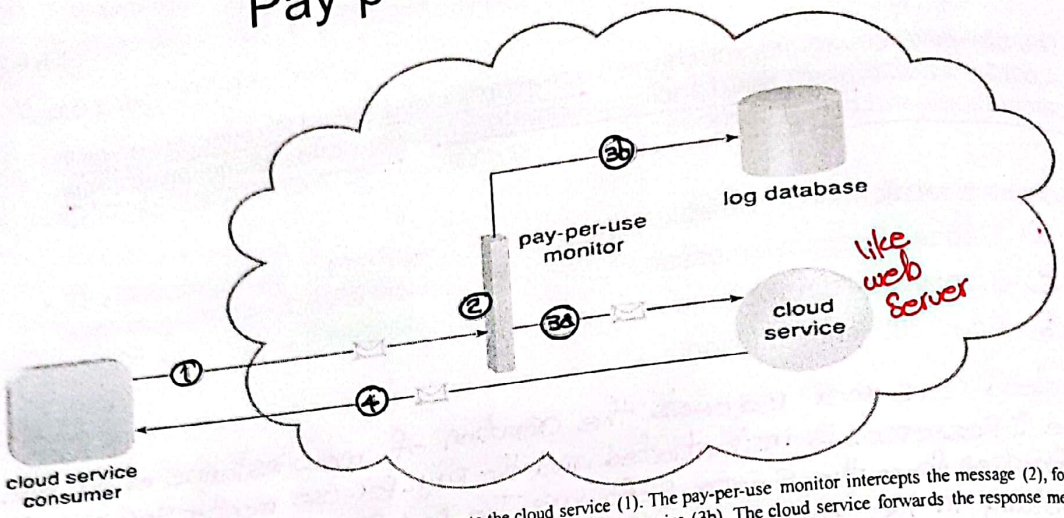
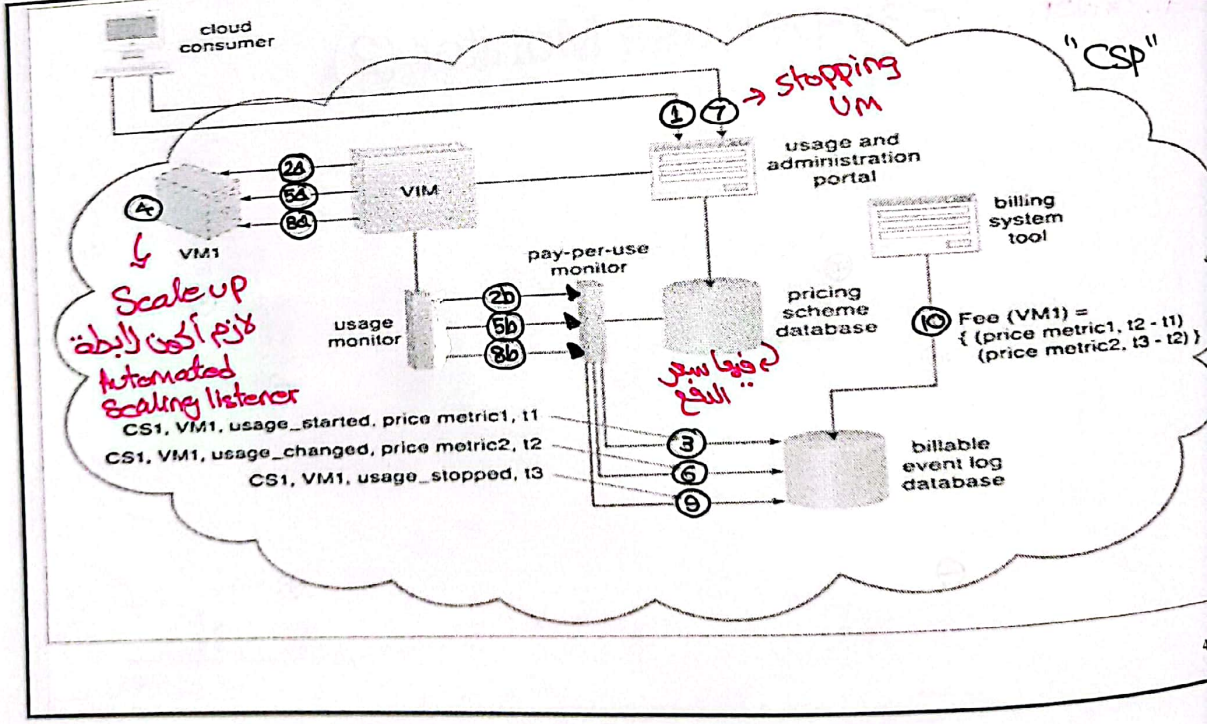
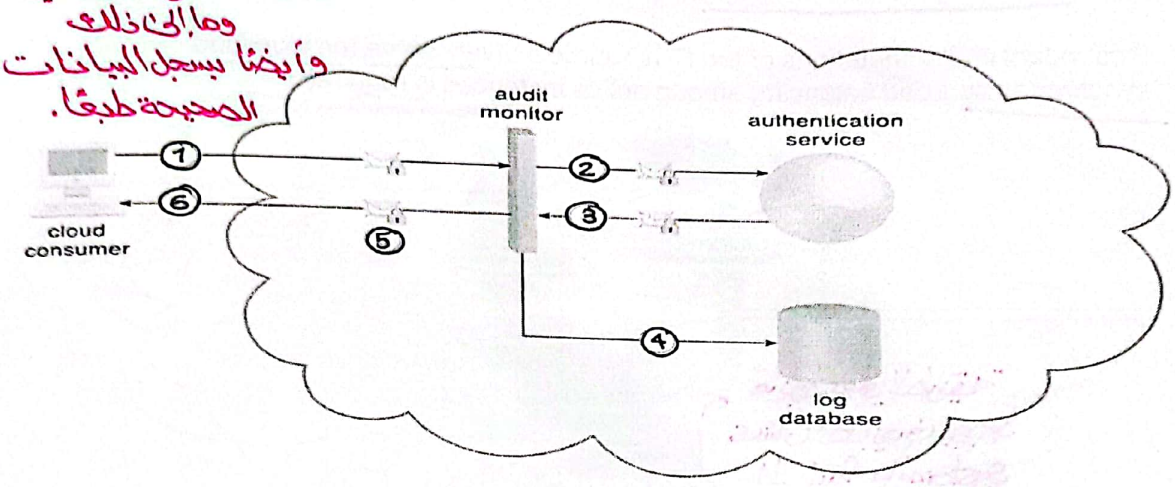


Figure 8.13. A cloud service consumer sends a request message to the cloud service (1). The pay-per-use monitor intercepts the message (2), forwards it to the cloud service (3a), and stores the usage information in accordance with its monitoring metrics (3b). The cloud service forwards the response messages back to the cloud service consumer to provide the requested service (4).



Audit Monitor

يسجل كل الإدخالات الخاطئة لأغراض التحليل وما إلى ذلك وأيضًا يسجل البيانات الصحيحة طبقًا.



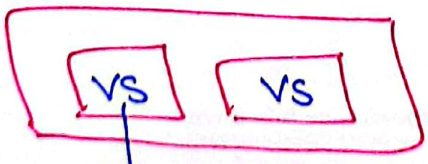
41

Failover System

إذا حصل fail لازم نصلحه بأسرع وقت وهي وظيفة الـ load balancer في تطبيق الـ clusters.

- The *failover system* mechanism is used to increase the reliability and availability of IT resources by using established clustering technology to provide redundant implementations. A failover system is configured to automatically switch over to a redundant or standby IT resource instance whenever the currently active IT resource becomes unavailable.

- Failover systems are commonly used for mission-critical programs and reusable services that can introduce a single point of failure for multiple applications.



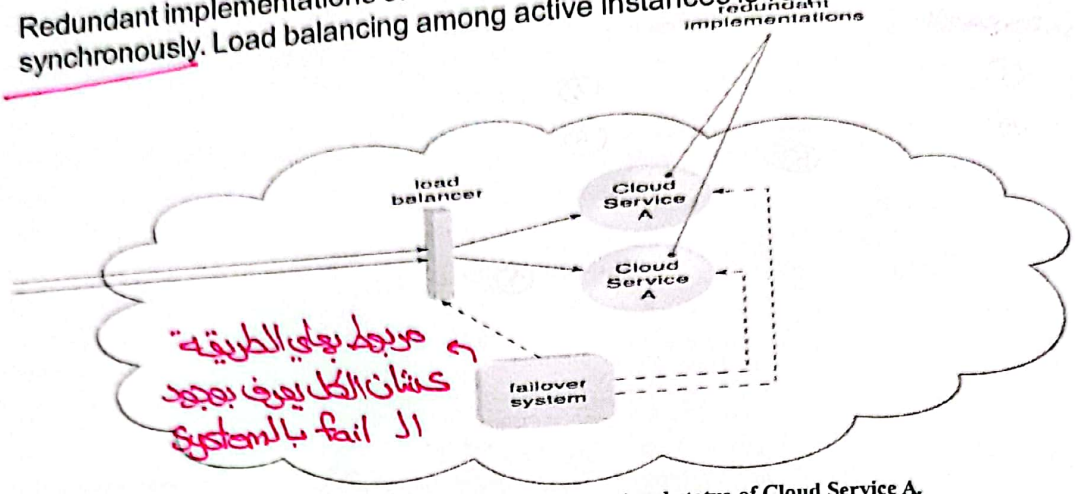
Cluster → لو حصل fail بتنقل للـ VS الـ Replica كل البيانات.

Replica نسخة من الأوبجكت

42

① Active-Active Failover System (1)

Redundant implementations of the IT resource actively serve the workload synchronously. Load balancing among active instances is required.



مربوط بهي الطريقة ← كشان الكل يعرف بوجود ال fail بالسيستم

Figure 8.17. The failover system monitors the operational status of Cloud Service A.

Active-Active Failover System (2)

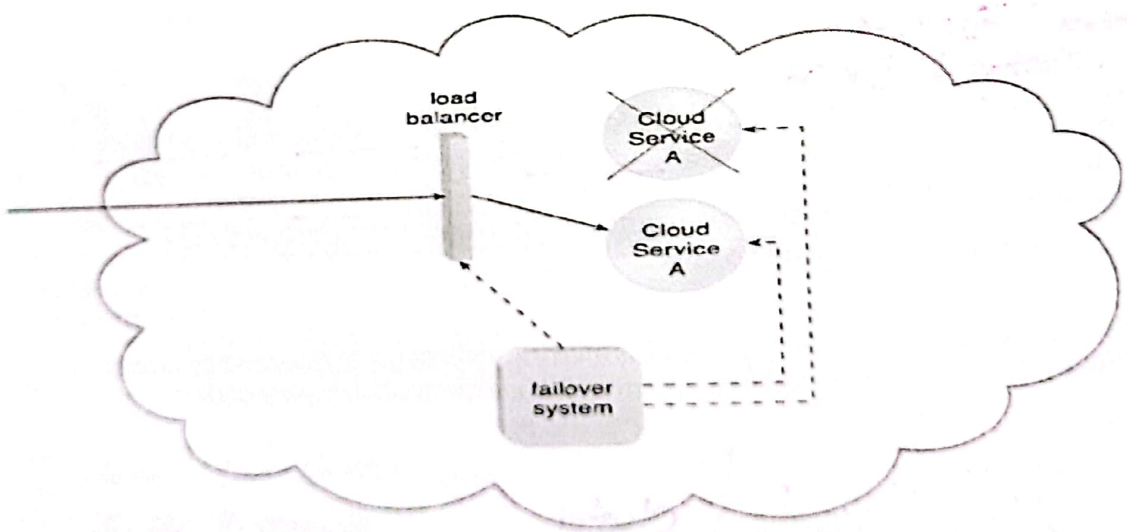


Figure 8.18. When a failure is detected in one Cloud Service A implementation, the failover system commands the load balancer to switch over the workload to the redundant Cloud Service A implementation.

Active-Active Failover System (3)

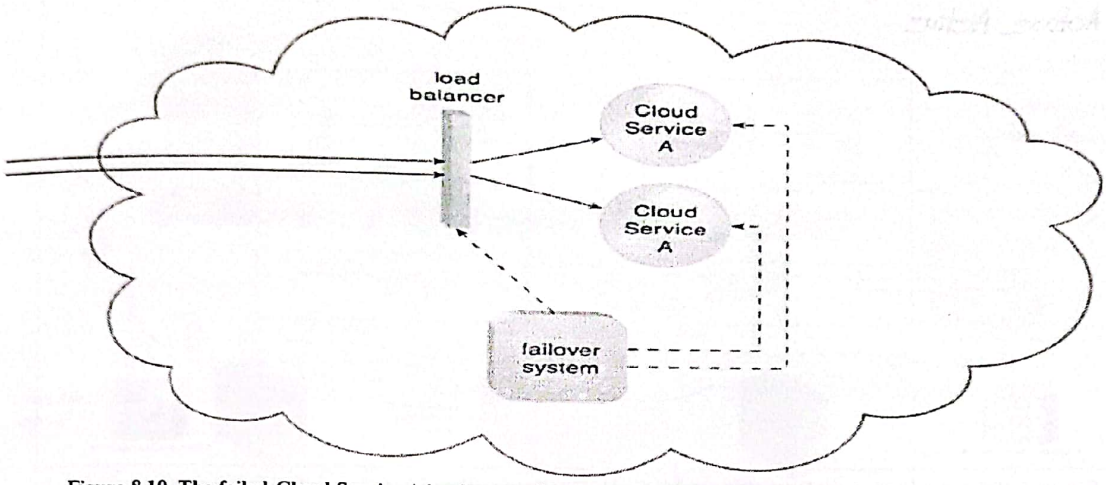
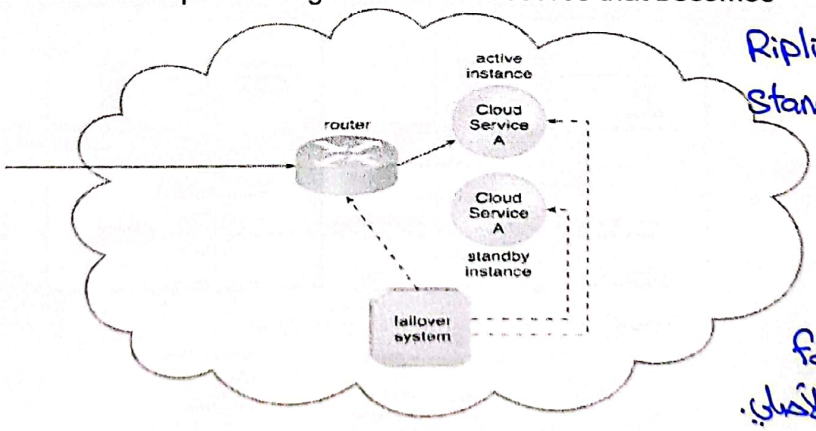


Figure 8.19. The failed Cloud Service A implementation is recovered or replicated into an operational cloud service. The failover system now commands the load balancer to distribute the workload again.

45

② Active-Passive Failover System (1)

- In an active-passive configuration, a standby or inactive implementation is activated to take over the processing from the IT resource that becomes unavailable.



Replica ال
Standby بتكون
ما بتكون
مشغلة و
up but
Not running
بتشتغل بس
لو صار
عال VS الأصلي.

Figure 8.20. The failover system monitors the operational status of Cloud Service A. The Cloud Service A implementation acting as the active instance is receiving cloud service consumer requests.

46

Across-datacenter Failover System (2)

لتكون load-balancer عندي ← active-passive
Active_Active

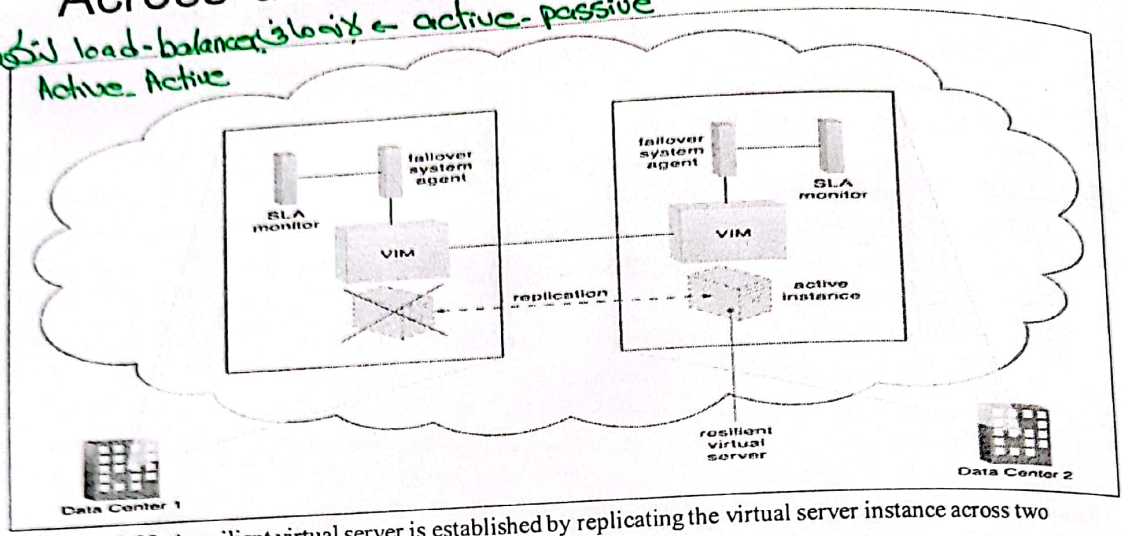


Figure 8.23. A resilient virtual server is established by replicating the virtual server instance across two different data centers.

47

* الأحسن active-active ← across data center بكون شوي متعب عشان شغلة
الـ load balancer .

Across-datacenter Failover System (2)

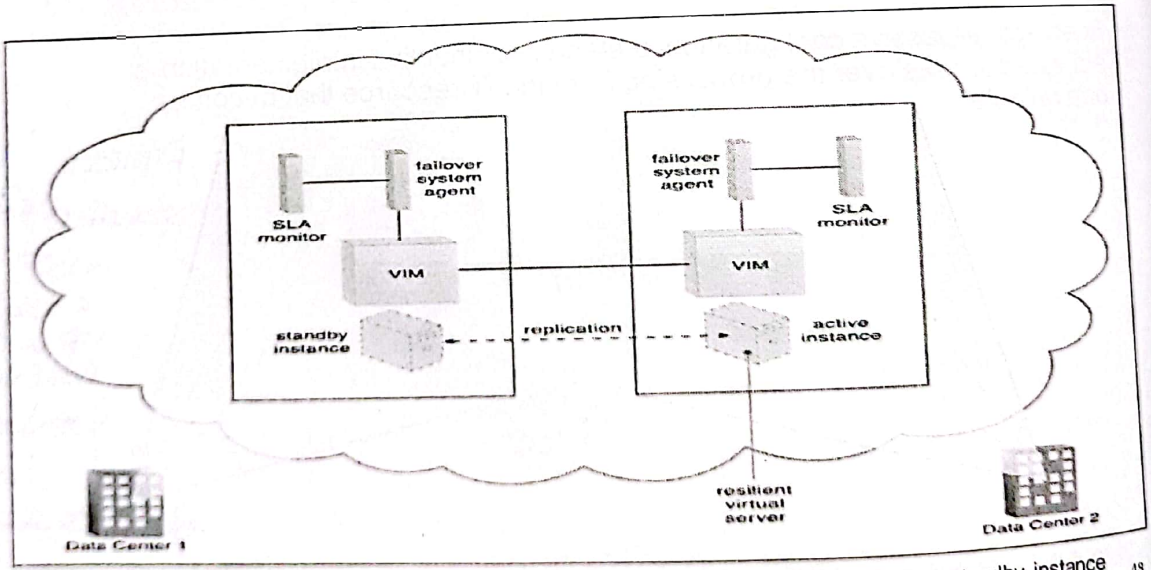


Figure 8.26. The failed virtual server instance is revived and scaled down to the minimum standby instance configuration after it resumes normal operation.

48

Hypervisor (1)

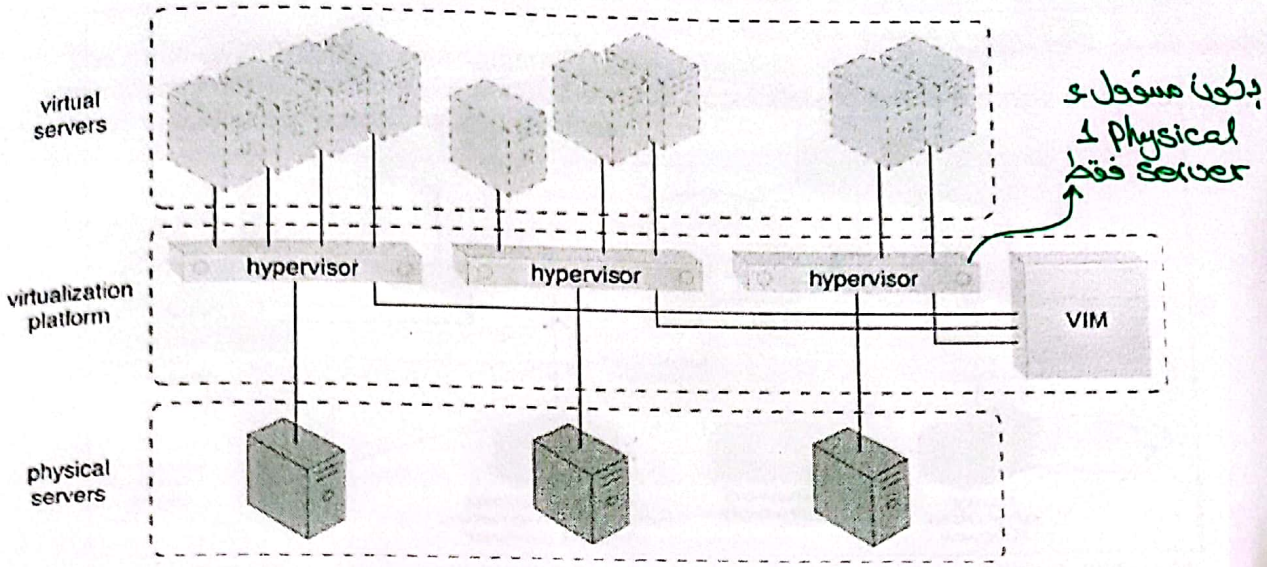


Figure 8.27. Virtual servers are created via individual hypervisor on individual physical servers. All three hypervisors are jointly controlled by the same VIM.

VIM and Hypervisor (1)

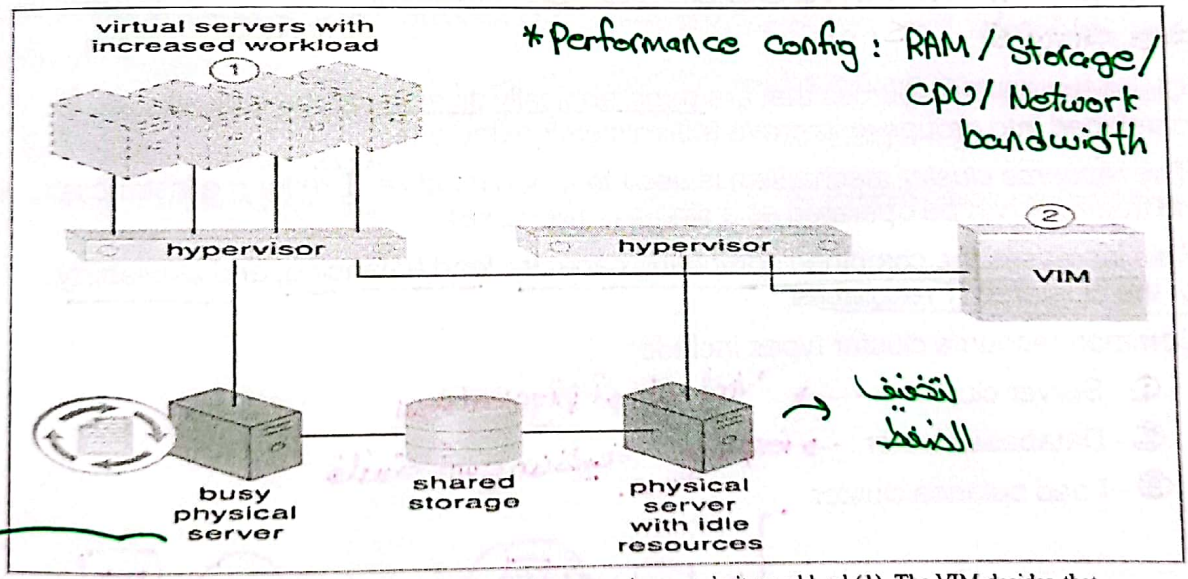


Figure 8.28. A virtual server capable of auto-scaling experiences an increase in its workload (1). The VIM decides that the virtual server cannot scale up because its underlying physical server host is being used by other virtual servers (2).

Automatic listner server بيعمل
بينبه لاجل load عالي.

VIM and Hypervisor (2)

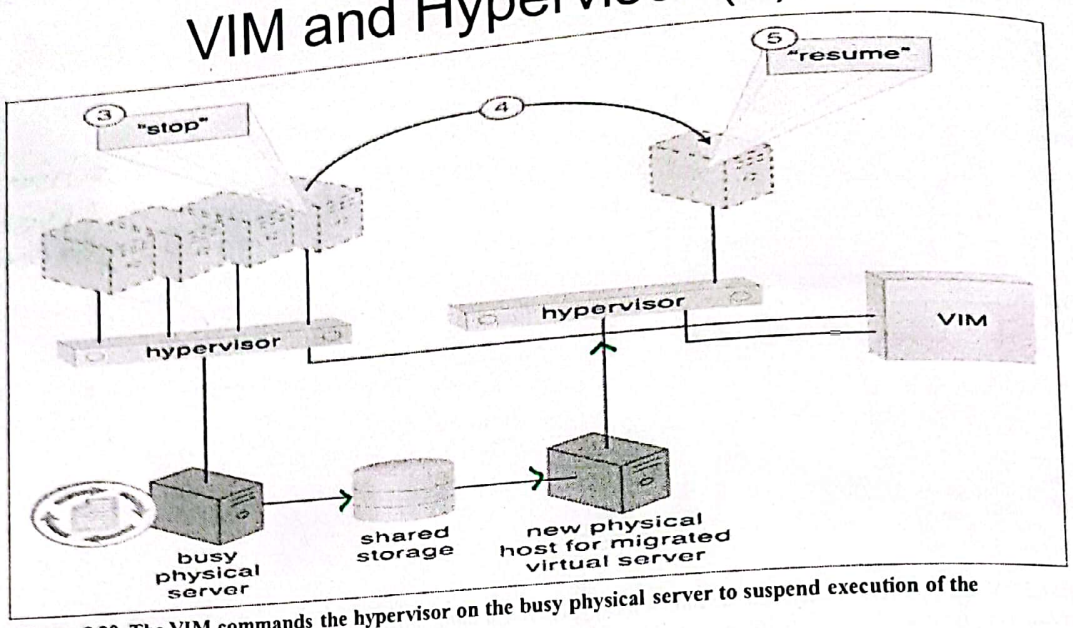
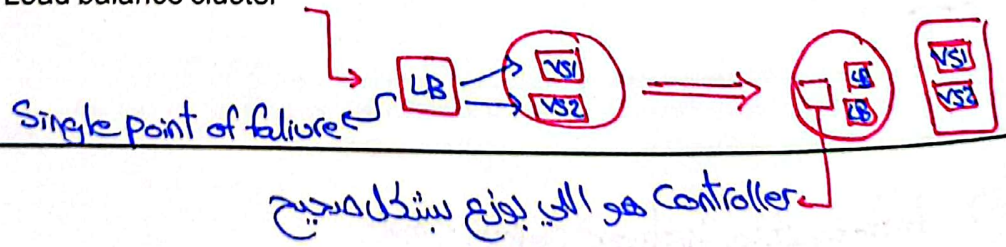


Figure 8.29. The VIM commands the hypervisor on the busy physical server to suspend execution of the virtual server (3).

Resource Cluster

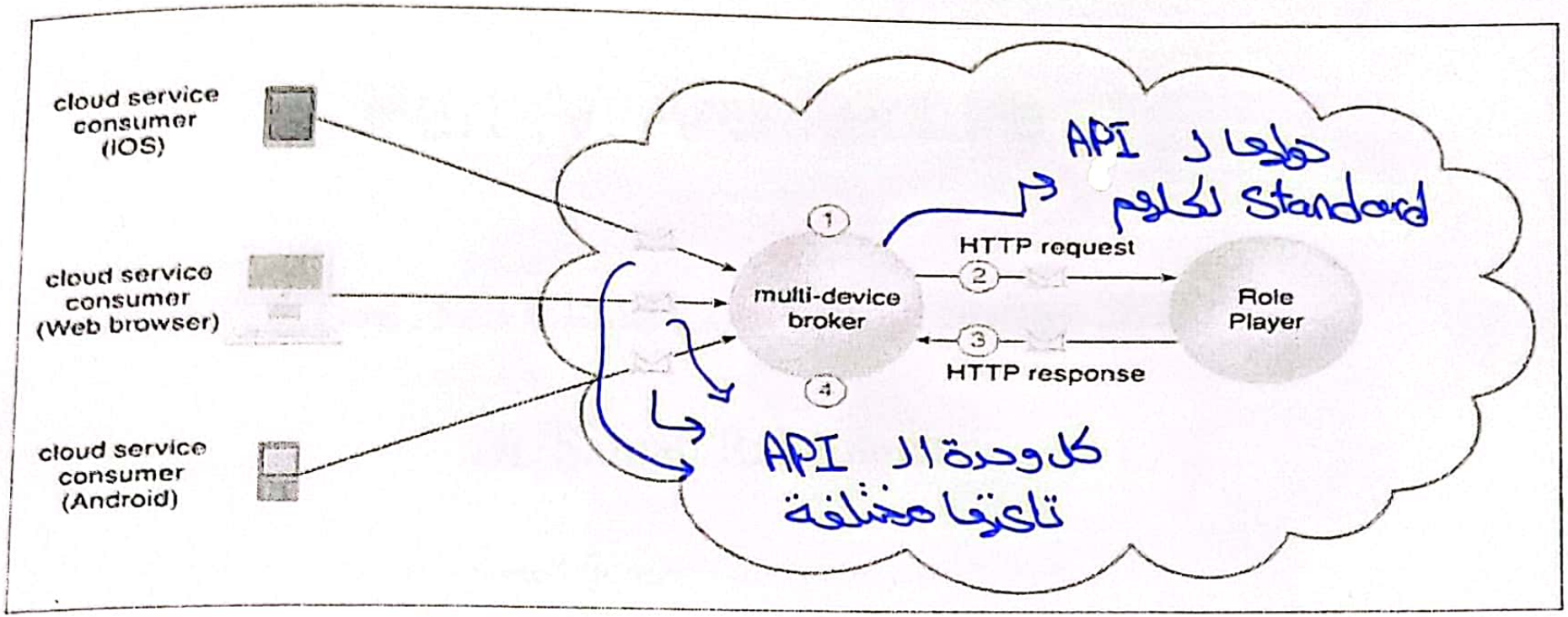
- Cloud-based IT resources that are geographically diverse can be logically combined into groups to improve their allocation and use.
- The *resource cluster* mechanism is used to group multiple IT resource instances so that they can be operated as a single IT resource.
- This increases the combined computing capacity, load balancing, and availability of the clustered IT resources.
- Common resource cluster types include:
  - ① - Server cluster
  - ② - Database cluster
  - ③ - Load balance cluster



Multi-device Broker

لازم الـ Cloud تدعم كل أنواع الـ devices بغض النظر عن اختلاف الأجهزة والـ API's من خلال

- The *multi-device broker* mechanism is used to facilitate runtime data transformation so as to make a cloud service accessible to a wider range of cloud service consumer programs and devices.



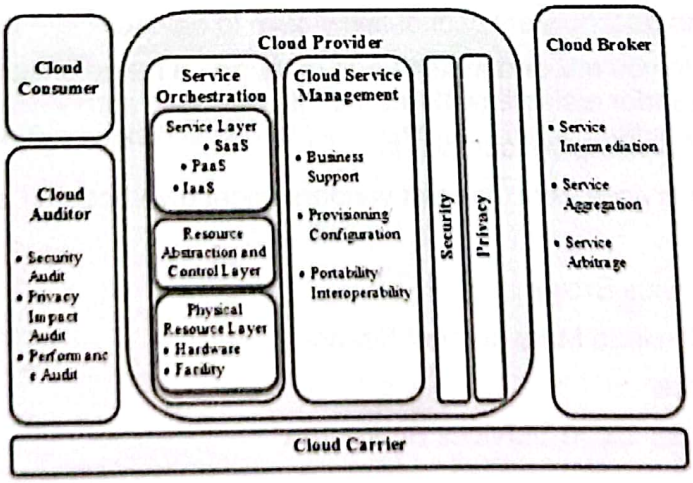
Part-IV: Architecture

CPE 0907523 Cloud Computing, Spring 2022

Dr. Samah Rahamneh

Slides adapted from Erl, Mahmood, and Puttini

NIST Cloud Computing Reference Architecture



Actors in Cloud Computing

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with and uses service from cloud providers.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

Cloud Broker

- **Cloud broker:**
  - - Allows to you mix and match - and manage - a range of cloud services under a single platform.
  - - It helps avoiding vendor lock-in.
  - - Mixing services from different vendors might give better IT solution.
- **Examples:**
  - - AWS Service Broker
  - - IBM Multi-cloud Management Services
  - - Cloudmore
  - - Jamcracker Cloud Services Brokerage

Fundamental Cloud Architectures

بتقسم traffic ال

2. Workload Distribution Architecture
   - Resource Pooling Architecture
   - Dynamic Scalability Architecture
   - Service Load Balancing Architecture
   - Cloud Bursting Architecture
   - Elastic Disk Provisioning Architecture
   - Redundant Storage Architecture

بشوف كذا كبير مزوم مختلفة بنفس الوقت. مش شرط ال Cloud تستخدم بس وحدة مزوم.

الفرق بينهم و ما بعرفش

ال Service في ال even distribution Load Balancing Architecture

ما بيهمه ال workload ككل وانه يقسمه بشكل متساوي بيهمه ال Service اللي موجودة كل واحد المهم ما يتعدى الحد المسموح

5

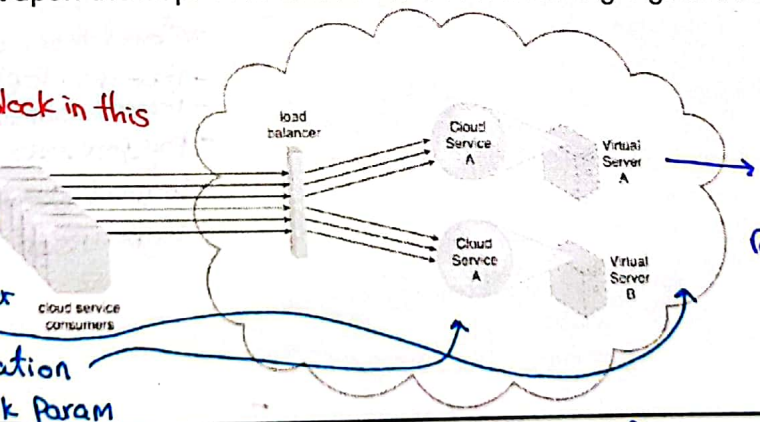
استخدام Load balancer = Workload Distribution Architecture

- provides runtime logic capable of evenly distributing the workload among the available IT resources.
- reduces both IT resource over-utilization and underutilization to an extent dependent upon the sophistication of the load balancing algorithms and runtime logic.

ال load لازم يكون متساوي

basic building block in this figure:

- active-active sys
- failover agent
- Autoscaling listner
- Hypervisor
- resource replication
- logical network Param
- cluster



حالة A horizontal scaling لأن ماكينات resources جديدة.

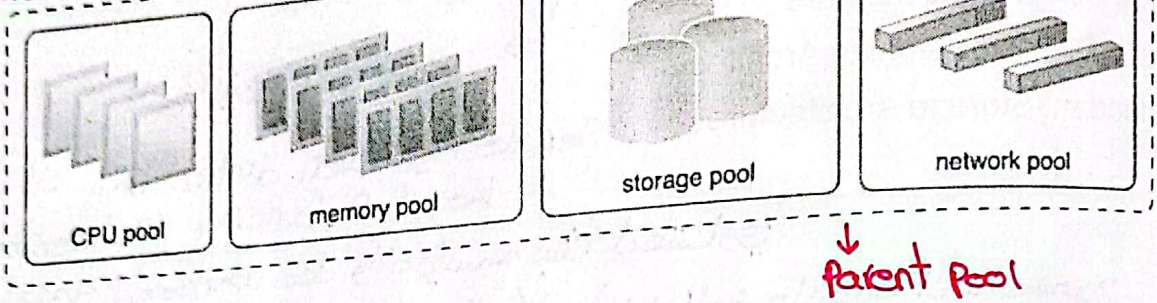
6

* الأولوية هون لل failover.

Resource Pooling Architecture (1)

- A *resource pooling architecture* is based on the use of one or more resource pools, in which identical IT resources are grouped and maintained by a system that automatically ensures that they remain synchronized.

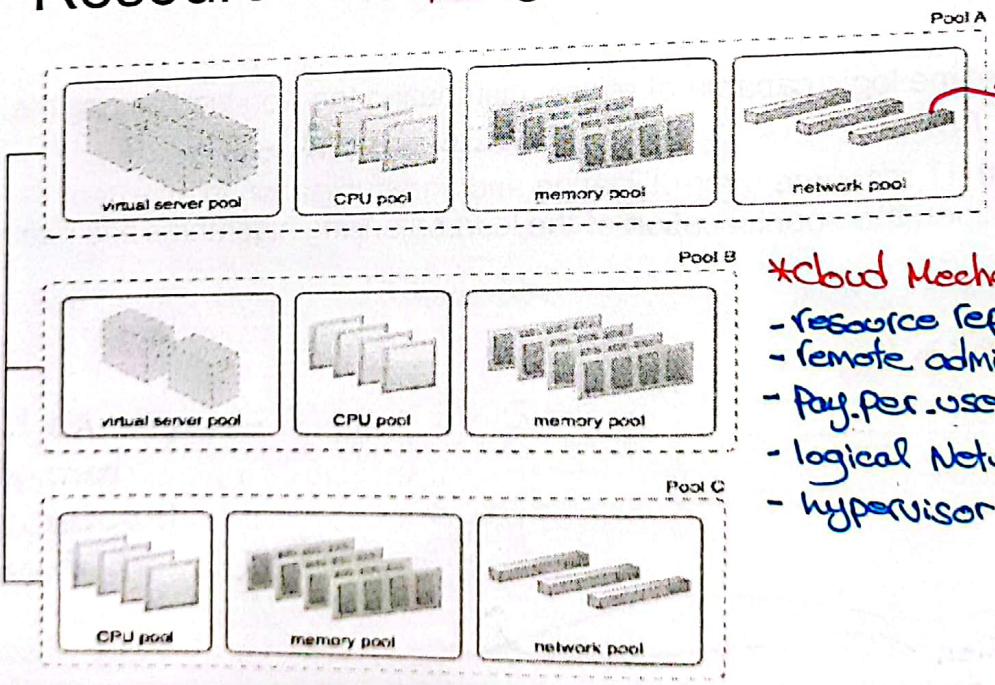
and fast ↵ physical pools بتقسم لـ child pool or siblings



parent pool

لأغراض التنظيم وسرعة الـRun ←

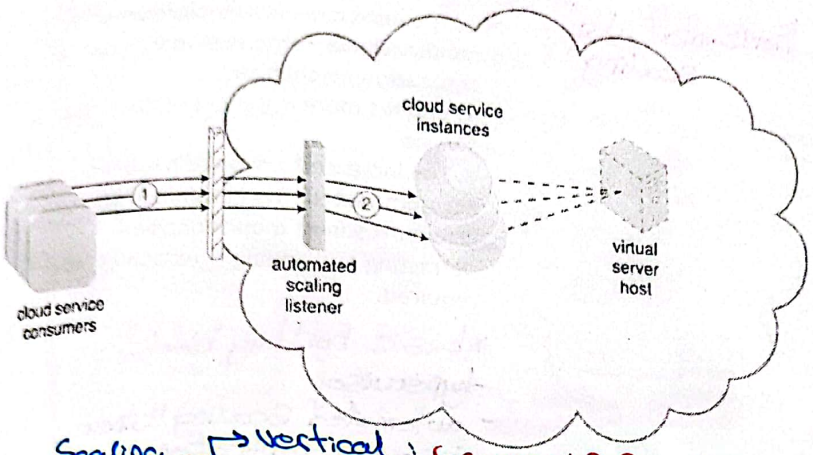
Resource Pooling Architecture (2)



like virtual firewalls, Physical switches

*Cloud Mechanisms :
- resource replication
- remote administrator system
- Pay.per.use
- logical Network Param
- hypervisor

Dynamic Scalability Architecture (1)

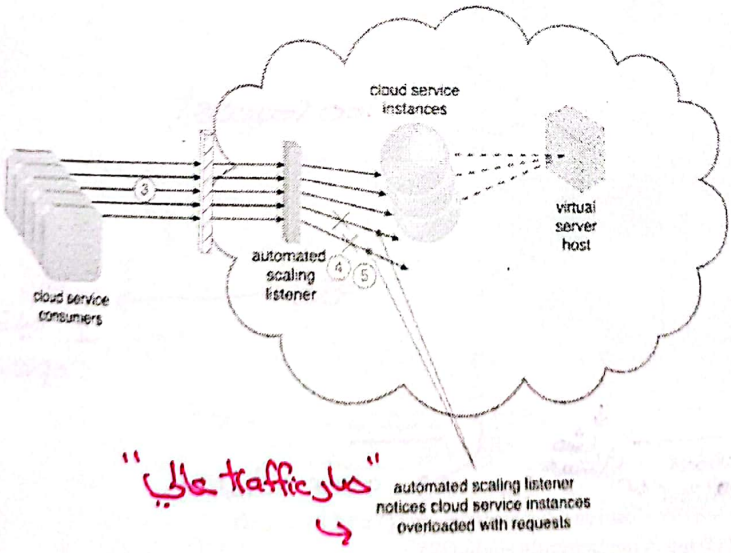


1. Cloud service consumers are sending requests to a cloud service.
2. The automated scaling listener monitors the cloud service to determine if predefined capacity thresholds are being exceeded.

Scaling → vertical : resource ↓↑ Performance/Cost
→ horizontal : replication/cost

9

Dynamic Scalability Architecture (2)

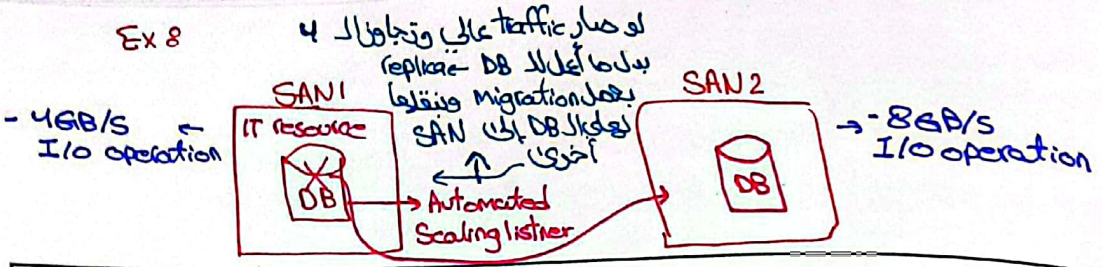


3. The number of requests coming from cloud service consumers increases .
4. The workload exceeds the performance thresholds. The automated scaling listener determines the next course of action based on a predefined scaling policy.
5. If the cloud service implementation is deemed eligible for additional scaling, the automated scaling listener initiates the scaling process.

"الـ traffic زاد"

10

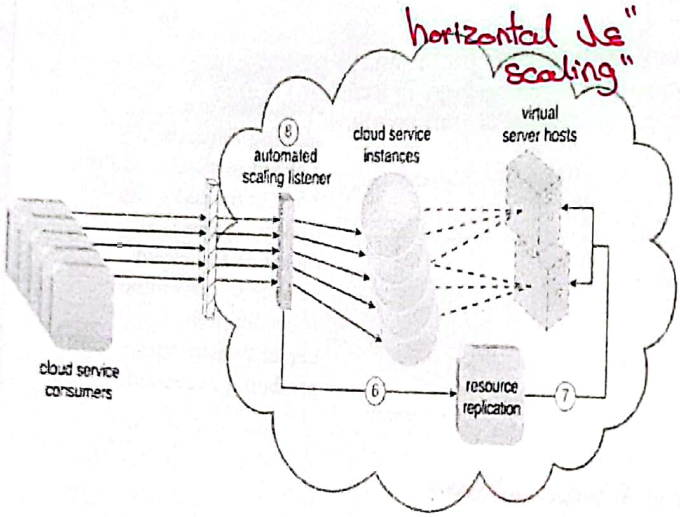
Ex 8



4/13/2022

SAN: Storage Area Network (Storage devices)

Dynamic Scalability Architecture (3)



6. The automated scaling listener sends a signal to the resource replication mechanism.
7. Creates more instances of the cloud service.
8. The increased workload has been accommodated, the automated scaling listener resumes monitoring and detracting and adding IT resources, as required.

*basic building blocks:
- hypervisor
- automated Scaling listner
- resource replication
- logical Network Parameter

Service Load Balancing Architecture

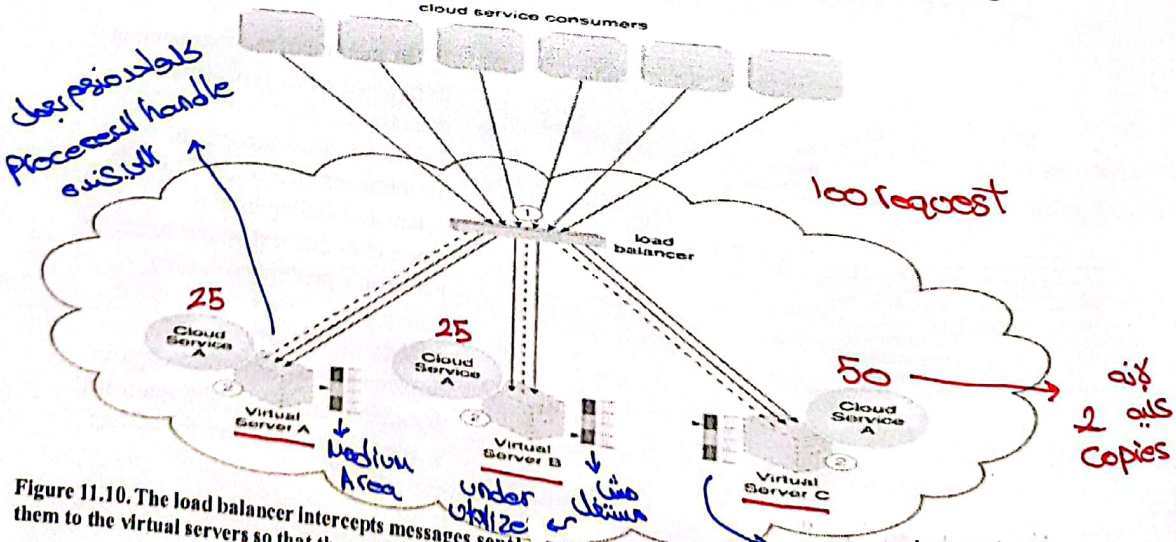
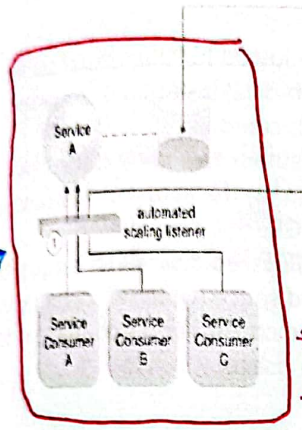


Figure 11.10. The load balancer intercepts messages sent by cloud service consumers (1) and forwards them to the virtual servers so that the workload processing is horizontally scaled (2).

Cloud Bursting Architecture

The *cloud bursting architecture* establishes a form of dynamic scaling that scales or "bursts out" on-premise IT resources into a cloud whenever predefined capacity thresholds have been reached.



cloud based IT-resource

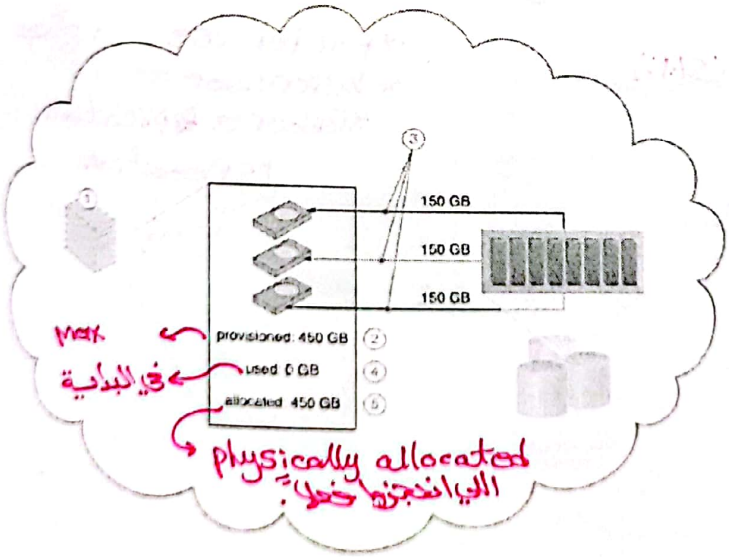
* Automated Scaling : بتتابع listner
* resource replication
onpremise IT-resource * LB ?

1. An automated scaling listener monitors the usage of on premise Service A, and redirects Service Consumer C's request to Service A's redundant implementation in the cloud (Cloud Service A) once Service A's usage threshold has been exceeded.
2. A resource replication system is used to keep state management databases synchronized.

13

بعدما تتفعل بنط Scale ال بتفعل Cloud في ال
من load balancer

Elastic Disk Provisioning Architecture (1)



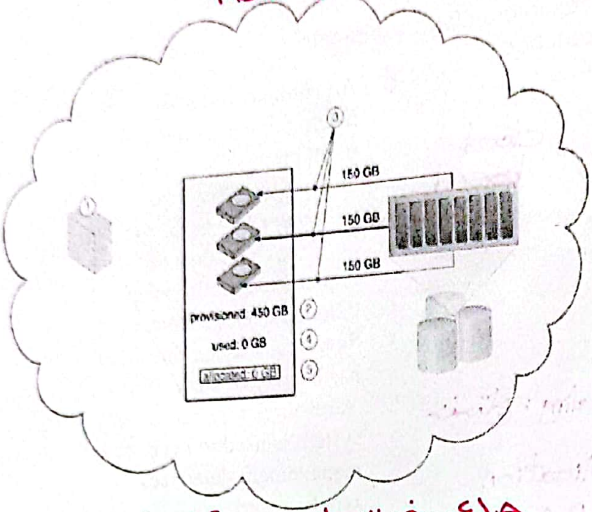
max.
في البداية
physically allocated
الي انحجز خلص

1. The cloud consumer requests a virtual server with three hard disks, each with a capacity of 150 GB.
2. The virtual server is provisioned according to the elastic disk provisioning architecture, with a total of 450 GB of disk space.
3. The 450 GB is allocated to the virtual server by the cloud provider.
4. The cloud consumer has not installed any software yet, meaning the actual used space is currently 0 GB.
5. Because the 450 GB are already allocated and reserved for the cloud consumer, it will be charged for 450 GB of disk usage as of the point of allocation.

14

Elastic Disk Provisioning Architecture (2)

More Elastic



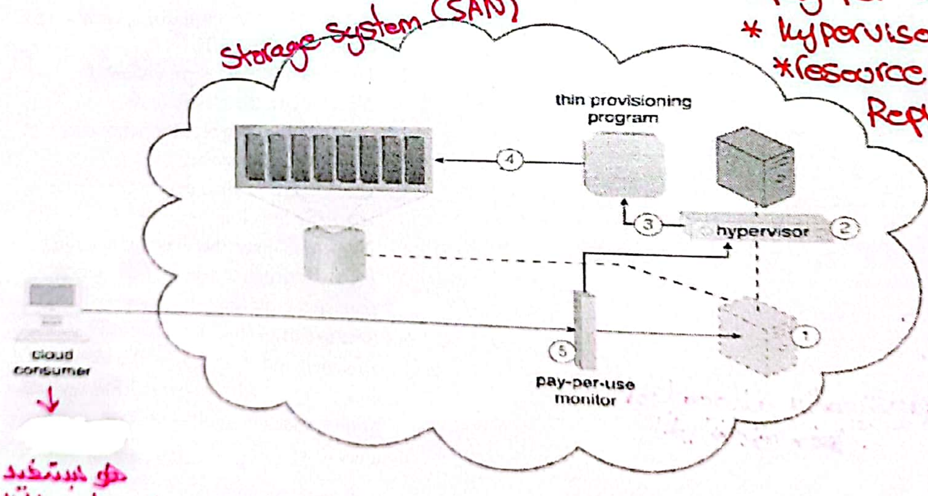
1. The cloud consumer requests a virtual server with three hard disks, each with a capacity of 150 GB.
2. The 450 GB are set as the maximum disk usage that is allowed for this virtual server, although no physical disk space has been reserved or allocated yet.
3. The cloud consumer has not installed any software, meaning the actual used space is currently at 0 GB.
4. Because the allocated disk space is equal to the actual used space (which is currently at zero), the cloud consumer is not charged for any disk space usage.

هيك وقت ماحجزت أول مابلش فما بدفع
عاشي انا هو مشتغله لسا.

Elastic Disk Provisioning Architecture (3)

Storage System (SAN)

بحتاج :
*Pay Per use
* hypervisor
*resource Repleaction
:



هو بستفيد أكثر
لأنه مابدفع إلا اللي
بيستخدم

Elastic Disk Provisioning Architecture (4)

1. A request is received from a cloud consumer, and the provisioning of a new virtual server instance begins.
2. As part of the provisioning process, the hard disks are chosen as dynamic or thin-provisioned disks.
3. The hypervisor calls a dynamic disk allocation component to create thin disks for the virtual server.
4. Virtual server disks are created via the thin-provisioning program and saved in a folder of near-zero size. The size of this folder and its files grow as operating applications are installed and additional files are copied onto the virtual server.
5. The pay-per-use monitor tracks the actual dynamically allocated storage for billing purposes.

Reading

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: concepts, technology, & architecture*. Pearson Education. Chapter 11

Part-V: Applications

لـ اللي استفادت من الـ cloud

CPE 0907523 Cloud Computing, Fall 2020

Dr. Samah Rahamneh

Slides adapted from Erl, Mahmood, and Puttini and

Discussion Topics

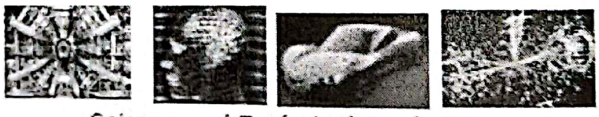
Cloud programming and software environments:

- Cloud application requirements and constraints
- MapReduce, Hadoop library, Pig Latin, Storm, Spark
- Programming support, approaches on real cloud platforms

Big Data and Cloud Storage Relation?

- Big Data applications use data sets that cannot be stored and processed using local resources
- Storage and processing on the cloud are intimately tied to one another
  - – Most cloud applications process very large amounts of data; effective data replication and storage management strategies are critical to the computations performed on the cloud
  - – Strategies to reduce the access time and to support *real-time* multimedia access are necessary to satisfy the requirements of content delivery
- Sensors feed a continuous stream of data to cloud applications
  - – An ever increasing number of cloud-based services collect detailed data about their services and information about the users of these services
  - – The service providers use cloud infrastructures to analyze the data

Cloud Applications

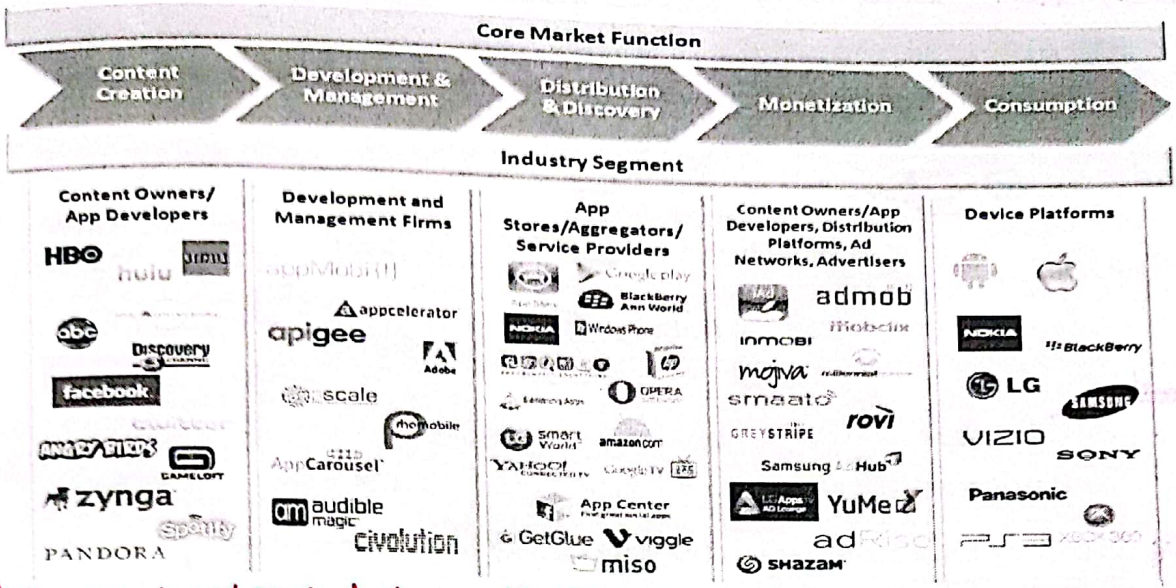


Science and Technical Applications

Business Applications

Consumer/Social Applications

App Marketplaces



نفس الـ Apps موجودة بمختلف الـ Market places لإنه فيه OS مختلفة

5

. Market place لكل

5

Evolution of Big Data

$$\left(\frac{\dot{a}}{a}\right)^2 = \frac{4\pi G\rho}{3} - K\frac{c^2}{a^2}$$

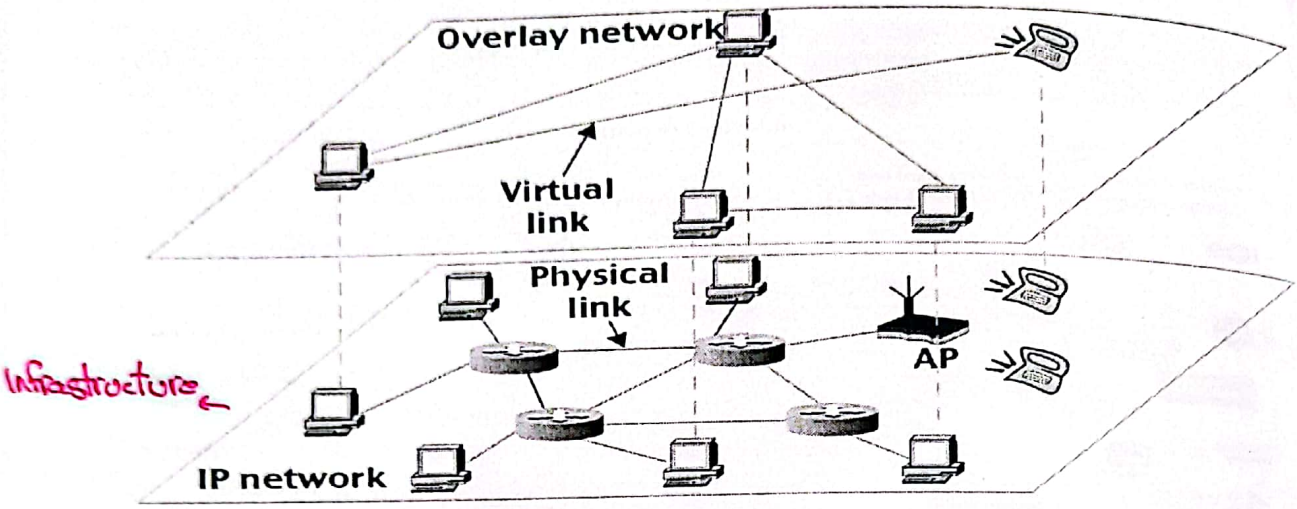
Experimental	Theoretical	Computational	Analytical
Thousand years ago	Last few hundred years	Last few decades	Today and the Future
Description of natural phenomena	*Newton's laws, Maxwell's equations…*	*Simulation of complex phenomena*	*Unify theory, experiment and computation with largemultidisciplinary Big Data Using data exploration and data mining (from instruments, sensors, humans…)*

Simulators

6

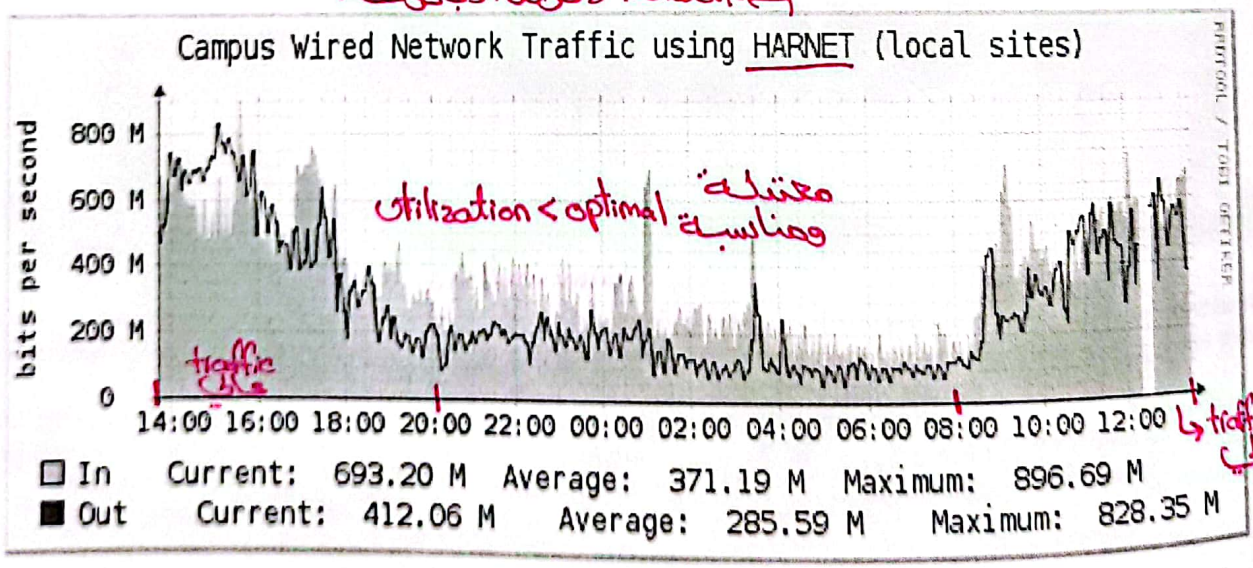
6

End-to-End Overlay Networks



* Big Data handling requires overlay networking, especially for satisfying real-time application requirements!

Typical Campus Traffic



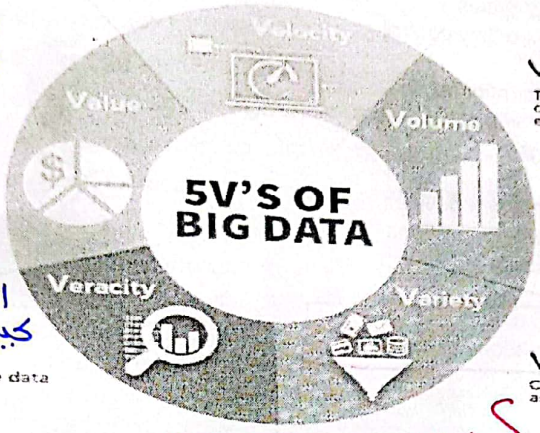
5V's of Big Data

متى أحكي إنه الـ App يعتبر big data

② **Velocity** · تغير الـ data بسرعة
Speed at which data is emanating and changes are occurring between the diverse data sets

Analysis هل العلاقات الـ data ستكون مفيدة؟

⑤ **Value**
Having access to big data is all well and good but that's only useful if we can turn it into a value



Volume ①
This refers to the sheer volume of data being generated every second
الـ data كبيرة جدًا بتكون.

الـ data ما فيها noise بكمية كبيرة.

④ **Veracity**
Data reliability and trust. Verifying and validating the data

Variety ③ . الـ data متنوعة
Can use structured as well as unstructured data
like tables
like Videos/audio

CSV في اشي بينهم مثل
↳ comma Separated Values

"بتركز على الـ Apps العلمية"

Campus firewall

هيك بنحسن الـ security بس بنخرب الـ performance

بسببهم انطرينا نقوي الأمان

- Cyber-attacks pose a formidable threat to enterprise network
  - .....Conservative Campus Firewall to thwart attacks
- Campus Firewall setting:
  - – Optimized for enterprise 'security'
  - – Partially sacrifices 'performance' → Software
  - – Blocking of ports for data-intensive collaboration tools
- Not trivial for science researchers to override campus security policies

↳ Slide العدد 12+13

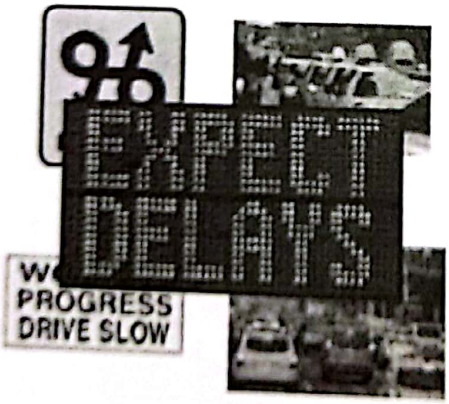
Hardware limitations

- Traditional traffic engineering methods
  - Long provisioning cycles
  - Lack of fine-grained flow control
- Network or device misconfiguration
  - NIC incapability
  - Buffer size settings
- Data rate mismatch between devices
  - Devices of different generations
  - Device incompatibility

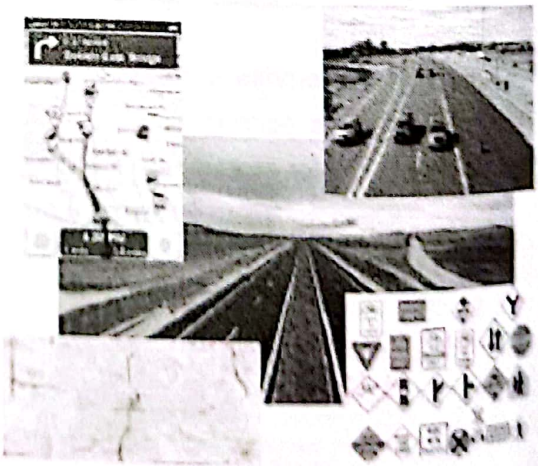
.....all these factors lead to underwhelming Performance and expectation mismatch!!

Towards a parallel infrastructure

Campus Network **Frictions**



Big Data Highway



Science DMZ….definition

According to Dart et al., the functionalities of a Science DMZ are:

1 * – *A scalable, extensible network infrastructure free from packet loss that causes poor TCP performance;* (Highway ✓)

2 * – *Appropriate usage policies so that high-performance applications are not hampered by unnecessary constraints;* (Rules ✓)

3 * – *An effective "on-ramp" for local resources to access wide area network services;* (Ramp ✓)

4 * – *Mechanisms for testing and measuring, thereby ensuring consistent performance.* (Live Traffic ✓)

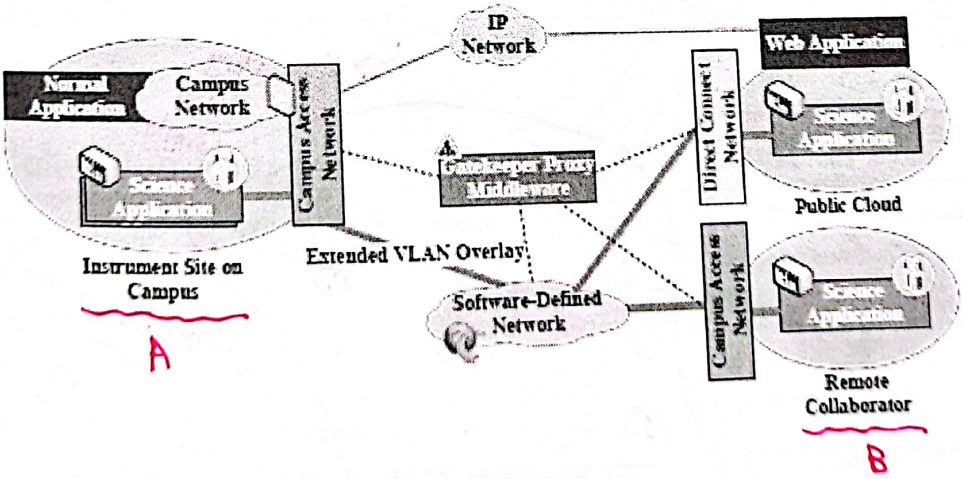
منطقة منزوعة السلاح لسرعة الحركة

* TCP → بتتشفل لحد ما تعرف إنه المسج وصلت
* UDP → بتبعت ومابهمها وصلت ولا لأ

مشكلة لو كان اكتر من جهاز على بحيس بطيء.

13

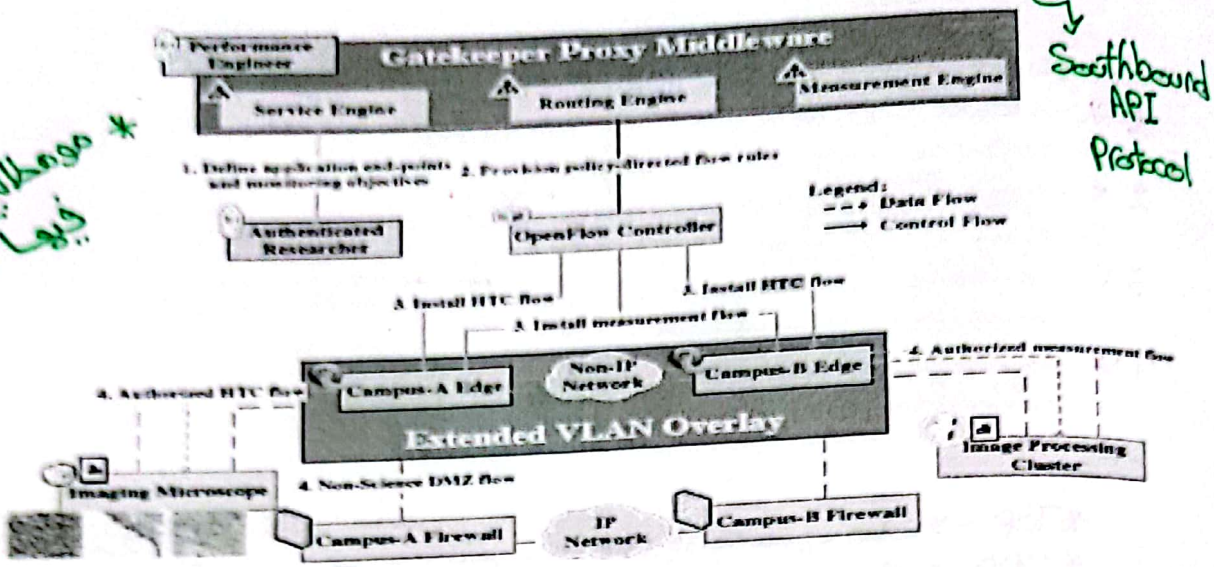
Science DMZ Use Case with OpenFlow



« A و B حيحكوا مع بعض »

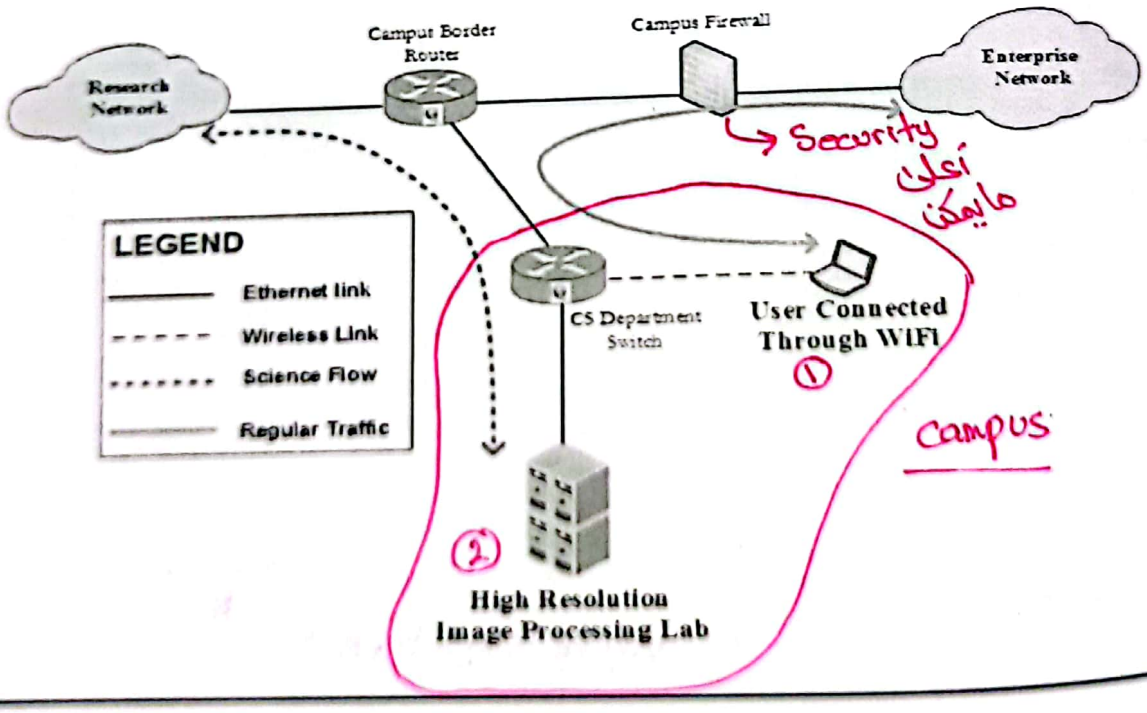
14

Science DMZ Flow Orchestration with OpenFlow



15

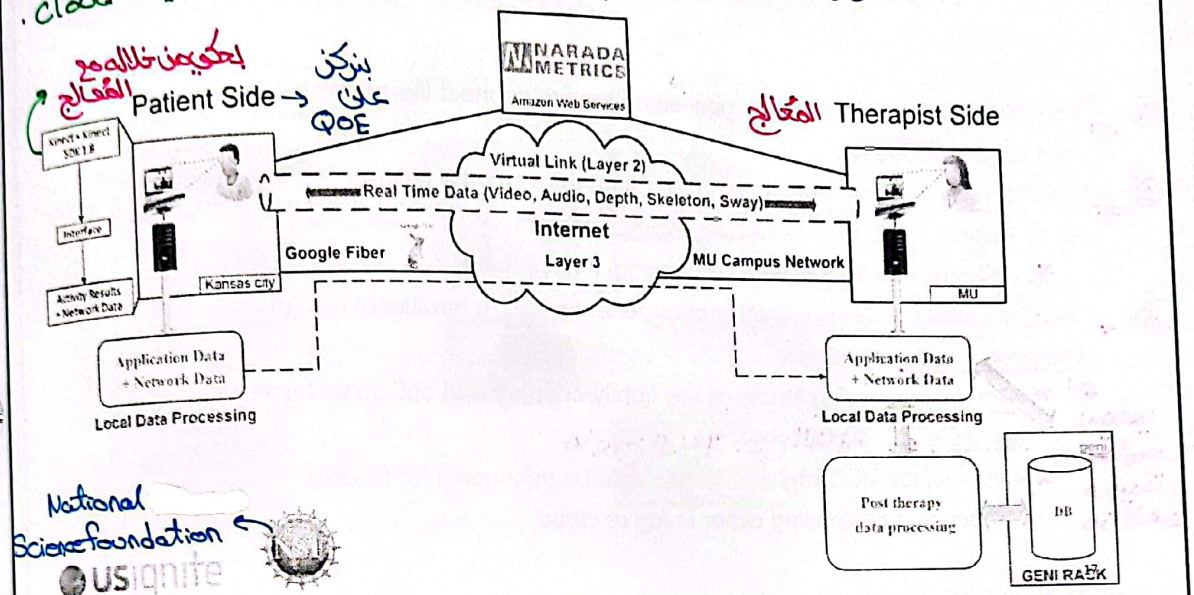
Transit selection



16

العلاج الطبيعي للمريض بدون ما يغادر بيته عن طريق الـ cloud.

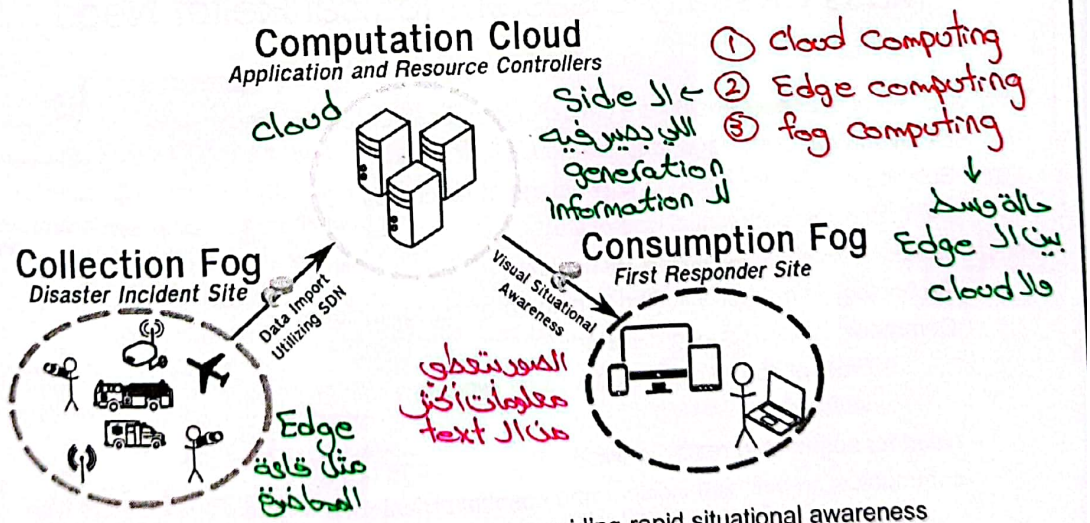
Physical Therapy-as-a-Service



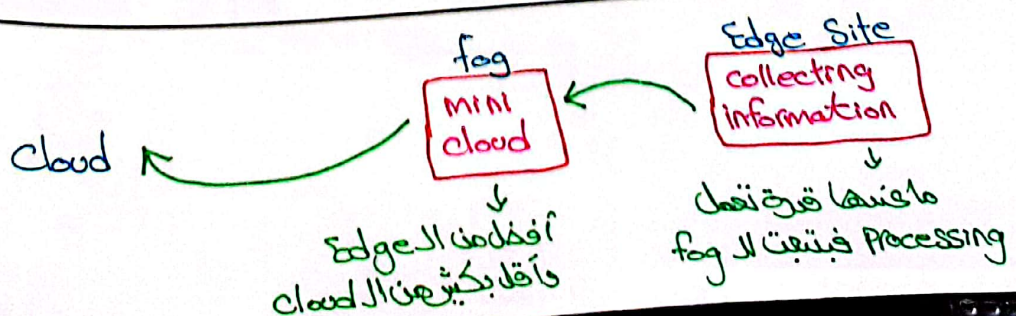
17 Provider لـ ← * quality of service (QoS): Network performance Parameter قياس

User لـ ← * quality of Experience (QoE) & بتركز على تقييم الـ Service User اللي حققوا

Network Edge Computing Vision



18



Challenges for Incident-supporting VCC

① • Fog-Cloud Networking requires new algorithms to connect the network-edge and the core cloud

② • Need for *resilient* computation and networking to overcome failures due to limited/unstable infrastructure during disasters

* – Should handle real-time processing, if necessary

③ • Reduced Quality of Service/Quality of Experience due to traditional design of computer vision algorithms

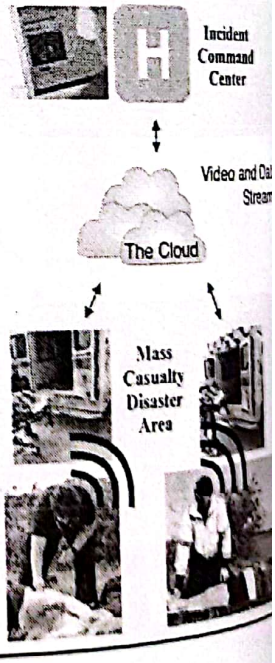
* – Image processing functions are tightly-coupled and optimized for hardware

* – Versus, the VCC requires functions to be decoupled for flexible computation processing either in fog or cloud

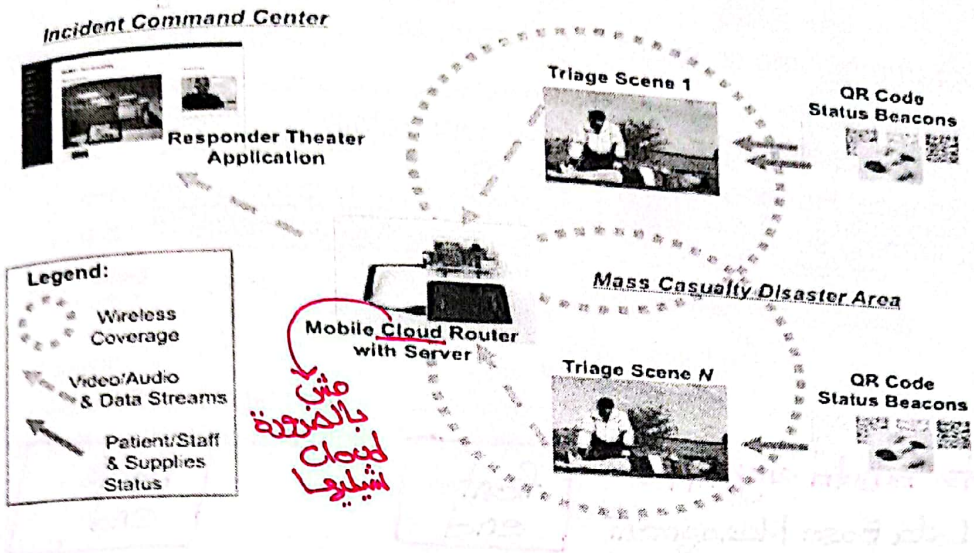
19

Mass Casualty Disaster Medical Relief Need

- Time" and "situational awareness" are critical during disaster relief
  - ***Delayed / missed triage may cause loss of lives!***
  - Balance needed for over-triage (wastage of resources $$) and under-triage (potential loss of life)
- Disaster Medical Relief Infrastructure Technology
  - Technology in market is limited to help co-ordinate "Incident Command System" during disasters
    - *Present co-ordination of triage by two-way radio is inefficient*
  - Need for augmented reality to avoid "Blackout" zone of communication between incident and hospital arrival



Mass Casualty Disaster



In-class Exercise

What emerging technologies can you think that Cloud Computing will enable in the next "Hype Cycle(s)"?

- Location-aware Apps like gps
- Virtual Assistants; Virtual Worlds
- Social Analytics based Mobile Services
- Augmented Reality
- Desktop-as-a-Service
- Simulation-as-a-Service
- Remote Elder-care → زي مثال العلاج الطبيعي
- ....others

1/3/2021

Discussion Topics

Cloud programming and software environments:

- Cloud application requirements and constraints
- MapReduce, Hadoop library, Storm, Spark
- Programming support, approaches on real cloud platforms

2 Parts to build any App:
* Relational Data Base Managment System:
front end
back end
include Data base
23

Primary key, foreign key, Pk T1 Fk T2 T3 T4
الأهم علاقة بينهن بتربطهن ببعضهن عشان ما أخذنا data بال data base
سبب إنه بطيء إنه ما يقسم الجدول الواحد لعدة أجزاء.

Database Requirements of Cloud Apps

- Most cloud applications are data-intensive and test the limitations of the existing infrastructure, and have requirements such as:
  1. – Rapid application development and short-time to the market
  2. – Low latency
  3. – Scalability
  4. – High availability
  5. – Consistent view of the data

صعب تحققهم جميع → NoSQL لاشي أفضل.

- These requirements cannot be satisfied ***simultaneously*** by existing database models
  - E.g., relational databases are easy to use for application development but do not scale well for Big Data
- The NoSQL model is useful when the structure of the data does not require a relational model and the amount of data is very large
- Does not support SQL as a query language
- May not guarantee the ACID (Atomicity, Consistency, Isolation, Durability)

Not only SQL
لو صار مشكلة بـ Partitions الباقي ما بتأثر
لـ لازم يتوفى الـ transaction كامل بدونها يصير انقطاع.
الداتا لازم مكررة بنفس المكان لازم الاثنين العينة
Leaveilability
24

* Transaction : Data base أي عملية بعملها على الـ (read, write, update, delete)

Partition
* NoSQL: P1 P2 P3 DB DB DB
→ availability ليس Replication & Partitions
horizontal Scaling

NoSQL Databases

- The name NoSQL is misleading
  - A soft-state approach allows data to be inconsistent and transfers the task of implementing only the subset of the ACID properties required by a specific application to the application developer
- NoSQL systems ensure that data will be eventually consistent at some future point in time
  - i.e., they do not enforce consistency at the time when a transaction is *committed*
- Attributes:
  - Scale well
  - Do not exhibit a single point of failure
  - Support partitioning and replication as basic primitives

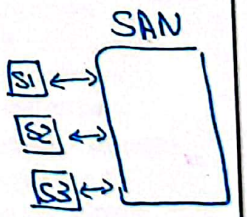
25

File Systems

- File system is a collection of directories; each directory provides information about a set of files
  - Traditional – Unix File System

① Network File Systems (NFS)
- Very popular and based on client/server interaction through RPC
- Have been used for some time, but do not scale well and have reliability problems
- An NFS server could be a single point of failure

② Storage Area Networks (SAN)
- Allow cloud servers to deal with non-disruptive changes in the storage configuration
- Storage in a SAN can be pooled and then allocated based on needs of servers
- SAN-based implementation of a file system can be expensive, as each node must have a Fiber Channel adapter to connect to the network



③ Parallel File Systems (PFS)
- Scalable, capable of distributing files across a large number of nodes, with a global naming space
- Many I/O nodes serve data to all computational nodes

26

1/3/2021

Google File System (GFS)

- Developed in the late 1990s; uses thousands of storage systems built from *inexpensive commodity components* to provide petabytes of storage to a large user community with diverse needs
- Design considerations:
  - Scalability and reliability are critical features of the system; they must be considered from the beginning, rather than at some stage of the design
  - Vast majority of files range in size from a few GB to hundreds of TB
  - Most common operation is to append to an existing file
    - Random write operations to a file are extremely infrequent
    - Sequential read operations are the norm
  - Users process data in bulk and are less concerned with response time
  - Consistency model relaxed to simplify the system implementation but without placing an additional burden on the application developers

27

27

Google Bigtable

- Distributed storage system developed by Google to:
  - store massive amounts of data
  - scale up to thousands of storage servers
  - Used in Google Maps, YouTube, Gmail, etc.
- The system uses:
  - Google File System → to store user data and system information
  - Chubby distributed lock service → to guarantee atomic read and write operations; the directories and the files in the namespace of Chubby are used as locks
- Simple & flexible data model with a multi-dimensional array of cells
  - A row key → an arbitrary string of up to 64 KB and a row range is partitioned into tablets serving as units for load balancing
  - A column key → consists of a string, a set of printable characters, and an arbitrary string as qualifier

28

28

Parallel and Distributed Programming

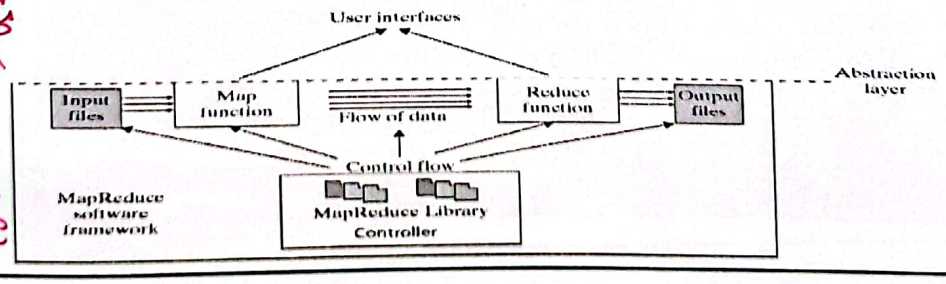
Table 1.7 Parallel and Distributed Programming Models and Tool Sets

Model	Description	Features
MPI	A library of subprograms that can be called from C or FORTRAN to write parallel programs running on distributed computer systems [6,28,42]	Specify synchronous or asynchronous point-to-point and collective communication commands and I/O operations in user programs for message-passing execution
MapReduce	A Web programming model for scalable data processing on large clusters over large data sets, or in Web search operations [16]	*Map* function generates a set of intermediate key/value pairs; *Reduce* function merges all intermediate values with the same key
Hadoop	A software library to write and run large user applications on vast data sets in business applications (http://hadoop.apache.org/core)	A scalable, economical, efficient, and reliable tool for providing users with easy access of commercial clusters

29

MapReduce: Scalable Data Processing on Large Clusters

- A web programming model for fast processing of large datasets
  - Applied in web-scale search and cloud computing applications
  - Users specify a Map function to generate intermediate key/value pairs
    - Runs on thousands of computers to each logical input record
  - Reduce function used to merge intermediate values with the same key
    - Collapses values using another user-supplied function

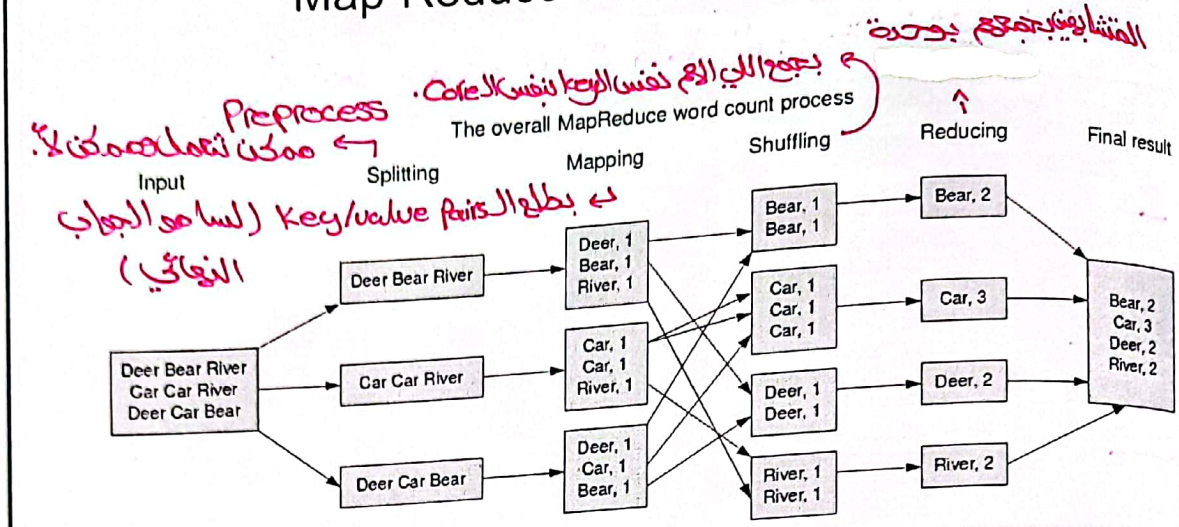


30

30

معطيك عدد من الفايلات وبده
تحكيله كم عدد تكرار كل كلمة من هاي
الفايلات

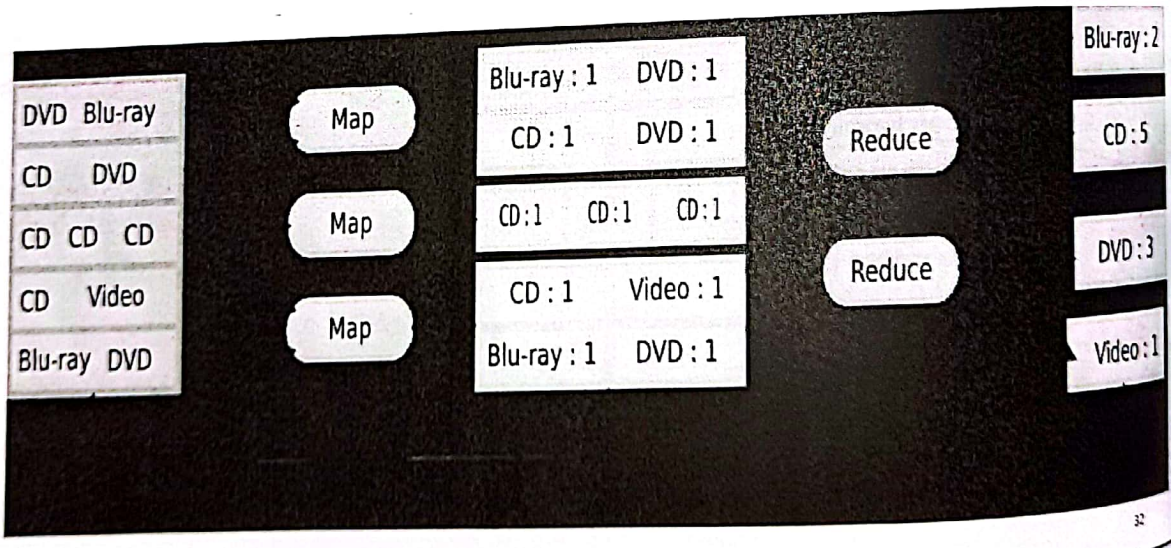
Map-Reduce Word Count Example



31

31

Map-Reduce Word Count Example (2)



32

32

Map Code Example

- Counting the number of occurrences of each word in a large collection of documents
- The Map function emits each word w plus an associated count of occurrences (just a "1" is recorded in this pseudo-code)

```
map(String key, String value):
  // key: document name
  // value: document contents
  for each word w in value:
    EmitIntermediate(w, "1");
```

33

Reduce Code Example

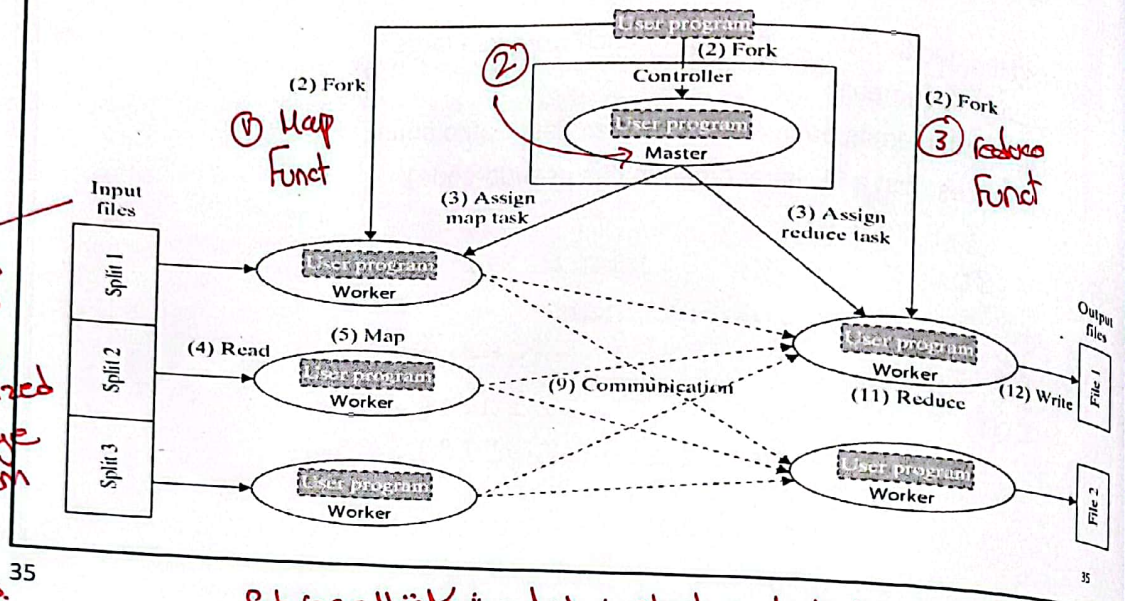
- Counting the number of occurrences of each word in a large collection of documents
- The Reduce function sums together all counts emitted for a particular word

```
reduce(String key, Iterator values):
  // key: a word
  // values: a list of counts
  int result = 0;
  for each v in values:
    result += ParseInt(v);
  Emit(AsString(result));
```

يعد كد records اللي الهم نفس الkey

34

Control Flow Implementation of MapReduce



35

Hadoop Platform

Open-source (Java-based) software platform developed by Yahoo to enable users write and run applications over vast distributed data • Used by:

- Major IT companies e.g., Apple, IBM, HP, Microsoft, Yahoo, and Amazon
- Media companies e.g., New York Times and Fox, social networks including, Twitter, Facebook, and LinkedIn

• Hadoop system has two components: (i) MapReduce Engine, and (ii) Database
- Database could be the Hadoop File System (HDFS), Amazon's S3, or CloudStore, an implementation of GFS

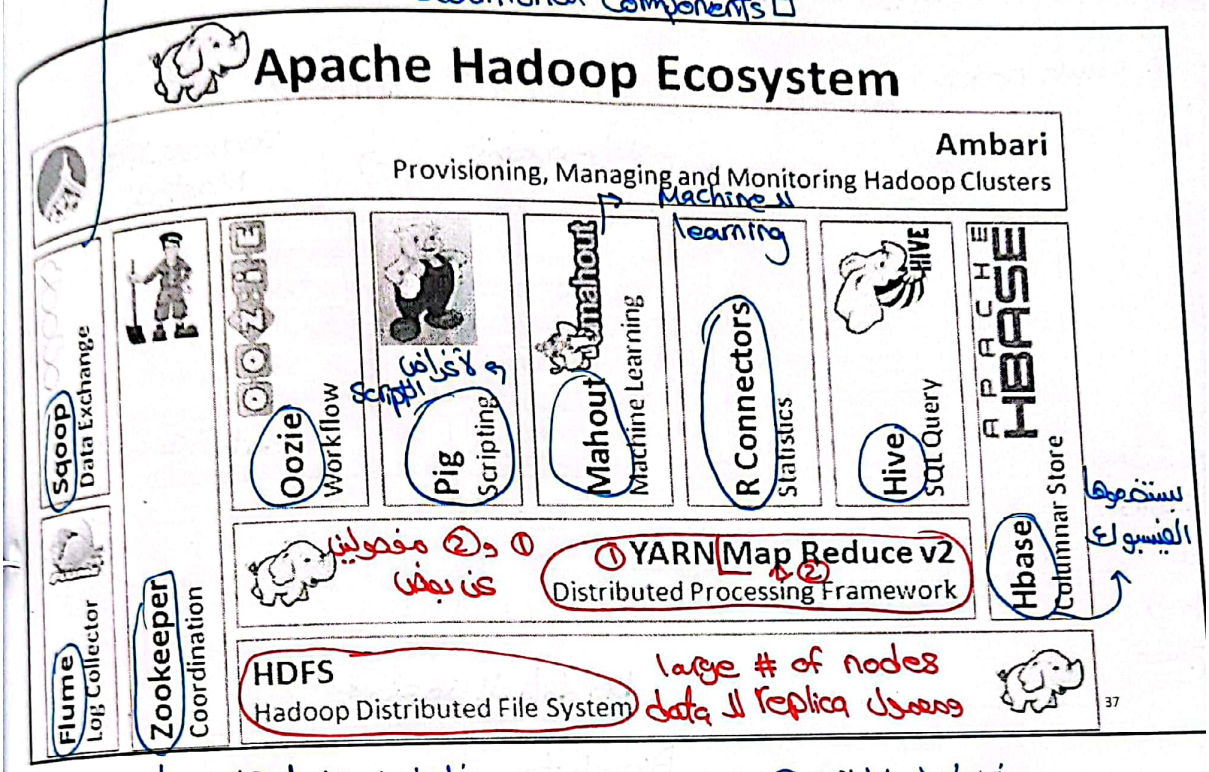
• Attractive Features in Hadoop:
* – Scalable: Can easily scale to store and process petabytes of data in the Web space
* – Economical: An open-source MapReduce minimizes the overheads in task spawning and massive data communication
* – Efficient: Processing data with high-degree of parallelism across a large number of commodity nodes – Reliable: Automatically maintains multiple copies of data

36

Export و Import لو كنت database وبدك تنقلها مع الـ HDFS

1/3/202

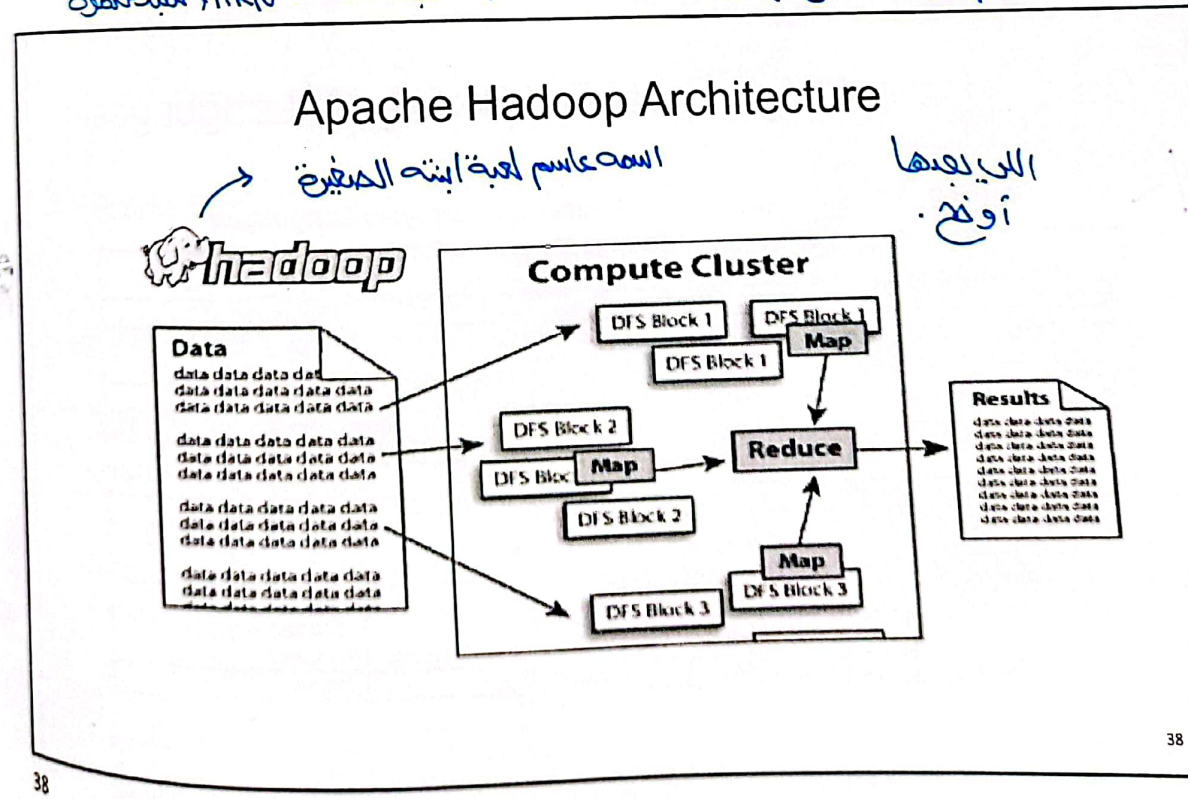
Main components
additional components



37

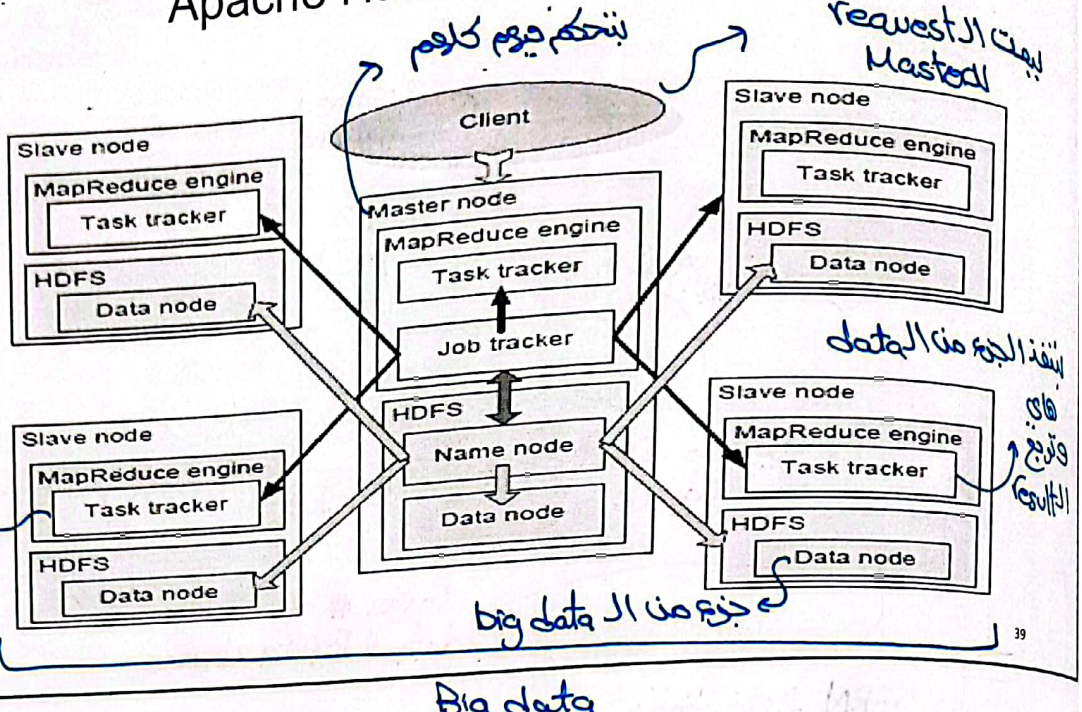
YARN وظيفته زي الـ
اللي ما بستخدما الـ YARN بستخدموا

وفي كمان نزلت Spark مع الـ Hadoop أكتر بس هاد ملخص.



38

Apache Hadoop Architecture (2)



39

39

Comparison of High-Level Data Analysis Languages

Table 6.7: Comparison of High Level Data Analysis Languages

	Sawzall	Pig Latin	DryadLINQ
Origin	Google	Yahoo	Microsoft
Data Model	Google Protocol Buffer or basic	Atom, Tuple, Bag,Map	Partition File
Typing	Static	Dynamic	Static
Category	Interpreted	Compiled	Compiled
Programming Style	Imperative	Procedural: sequence of declarative steps	Imperative and Declarative
Similarity to SQL	Least	Moderate	A lot!
Extensibility (User defined functions)	No	Yes	Yes
Control Structures	Yes	No	Yes
Execution Model	Record Operations + fixed aggregations	Sequence of MapReduce operations	Directed Acyclic Graphs
Target Runtime	Google MapReduce	Hadoop (Pig)	Dryad

40

40

* الـ Hadoop هو Batch processing يعني الـ Algo اللي بدي اشتغلها عالـ data بتطلب كل الـ data تكون موجودة من البداية بس ممكن مايكون كل الـ data موجودة هلأ طلع

* كمان عنا الـ Stream بشتغل عالـ data أول بأول مثل تويتر

1/3/2021

② Apache Storm

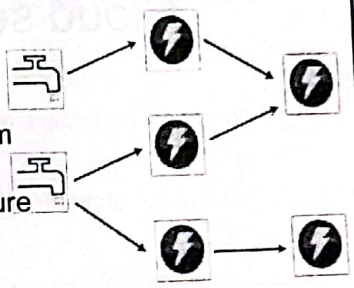
وفيسبوك

Software → data ll Analysis بعمل

أول ما توصل أول بأول

- Used for Real-time 'Stream Processing' and 'Streaming Analytics' of Big Data with Hadoop and a data warehouse
  - Analyze and act on streaming data, using "continuous queries" (i.e. SQL-type queries that operate over time and buffer windows)
  - Fraud detection, Live trend analysis, network monitoring, etc.
  - Continuous statistical analytics on the fly within the stream
  - Design handles high volume 'data in motion' in real time with a scalable, highly available and fault tolerant architecture
- Storm was created by Twitter
  - Used by Groupon, Spotify, etc.
  - Concept of Bolts and Spouts; instances process in parallel

→ Social Media لشركات



advantages: Free open source + Free software

41

41

Other Stream Processing Technologies

أما الـ Storm بحتاج أكتر الـ HDFS

بقدر أنن لعمال hadoop بس هو هو بحاجته

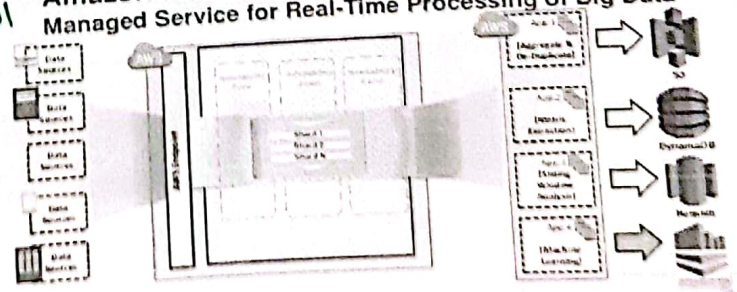
② • Apache Spark →

  - General framework for large-scale data processing
  - Supports MapReduce, in-memory processing, stream processing, graph processing or machine learning → hadoop ملبي أقل من الـ distributed file system
  - Can be used on top of Hadoop ll Processing بعمل data في

Examples

- IBM InfoSphere Streams
- AWS Kinesis

Amazon Kinesis
Managed Service for Real-Time Processing of Big Data



Memory الـ

فبزيد performance

بإنه بقلل الـ execution time

42

الخصائص المشتركين بين Spark و Storm و hadoop

- large dataset بتعاملوا
- Scalability بقدروا يعملوا
- fault tolerant (replication كن طريق)

Cloud security and trust management

* Asset & أي شيء بدك تحميه, any resource do you want to protect.
* Vulnerabilities & weak point in the system (نقطة ضعف).
* threat & التهديد, vulnerability سببه وجود الـ
* Attack & التخريب, physical attack.

attacker هو اللي بيشكل تهديد (threat) بيؤشر لـ Attack ويؤدي إليه.

43

43

بسبب 1- huge resources
2- Shared Inviroment

vulnerability amplifire

Cloud Computing System Design

	①	②	
في البداية هيك كنا نعمل	Design System	Design Security	In the good old days of High Performance Computing... (traditional)
حاليا هيك صرنا نعمل Security أول الـ	① Design Security	② Design System	In the Cloud era of High Throughput Computing...

44

44

high Performance → وقت إنجاز المهمة

high throughput → عدد المهام المنجزة في وحدة زمن

* CIA & NIST triad
- C : Confidentiality → السرية → access للي لازم يعملله access فقط
- I : Integrity → data التعديل على
- A : Availability → الإتاحة
(Authorized Person)

1/3/2021

للأشخاص المسموح لهم فقط .

Cloud Security Risks

- Traditional threats are amplified
  - * – Impact amplified due to the vast amount of cloud resources and the large user population that can be affected
  - * – Fuzzy bounds of responsibility between the providers of cloud services and users and the difficulties to accurately identify the cause
- Issue greater for Virtual Private Cloud (VPC) types of services
  - * – Identifying the path followed by an attacker more difficult in a cloud environment
- New threats arise given the nature of cloud infrastructures
  - * – Cloud servers host multiple VMs; multiple applications may run under each VM
  - * – One server failure can have larger impact!
  - * – Multi-tenancy and VMM vulnerabilities open new attack channels for malicious users
  - * – Third-party control → generates a spectrum of concerns caused by the lack of transparency and limited user control

45

45

لازم الـ user يقوم بمسؤولياته من ناحية System secured

صعب الـ track تاعوا بإنهن برا الـ cloud بيجي الـ traffic

ما لها standard

أحيانا الـ attack بكون جاية من جوا و هذا خطر جدا

Cloud Systems are Vulnerability Amplifiers!

- Main Concerns Cause/Effect

1 – **Information Leakage** → بيجي شخص بتنشف معلومات غير مخولة له
- Cause: Eavesdropping, Traffic interception
- Effect: Loss of Confidentiality

2 – **Integration Violation** → شخص غير مخول يعدل data
- Cause: Intercept/alter, Repudiation
- Effect: Loss of Integrity

3 – **Denial of Service**
- Cause: Trojan Horse, Resource exhaustion
- Effect: Loss of Availability

4 – **Illegitimate Use**
- Cause: Spoofing, Theft
- Effect: Improper Authentication

حجم الـ attack أقل بكتير من الـ cloud

Traditional Paradigm

Cloud Paradigm

logs ما أعمل بالـ system

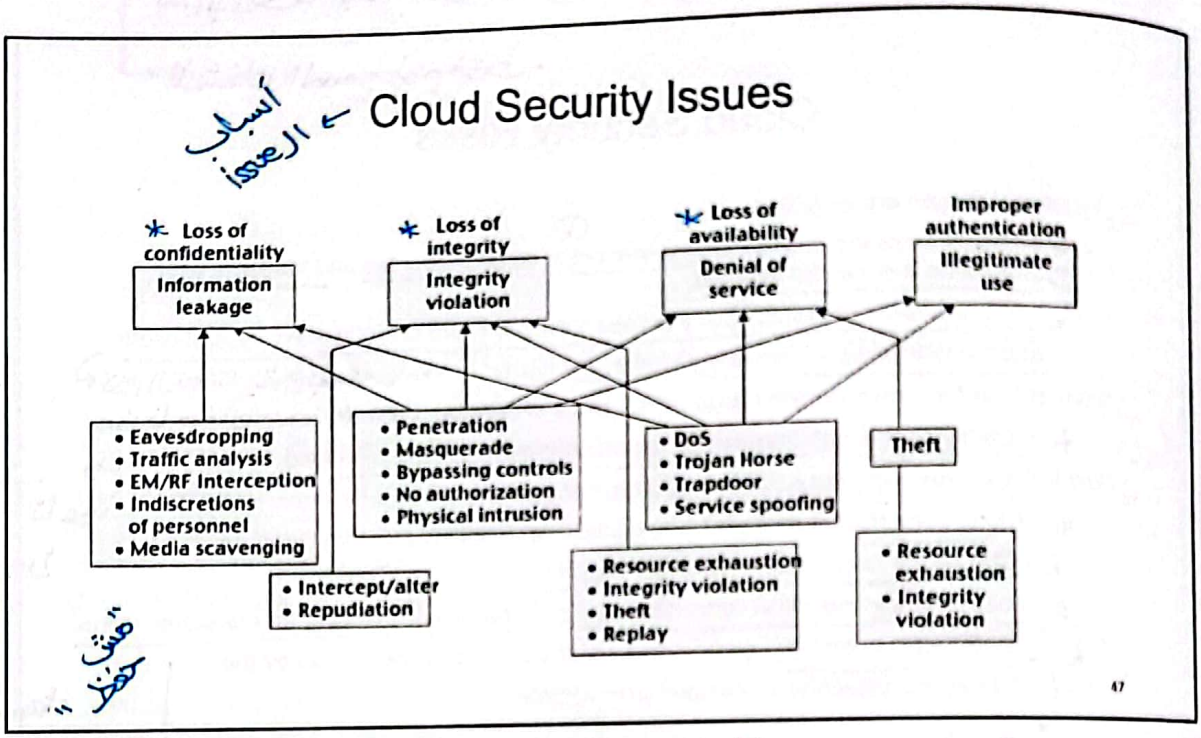
Service access يعمل denied وهي

46

46

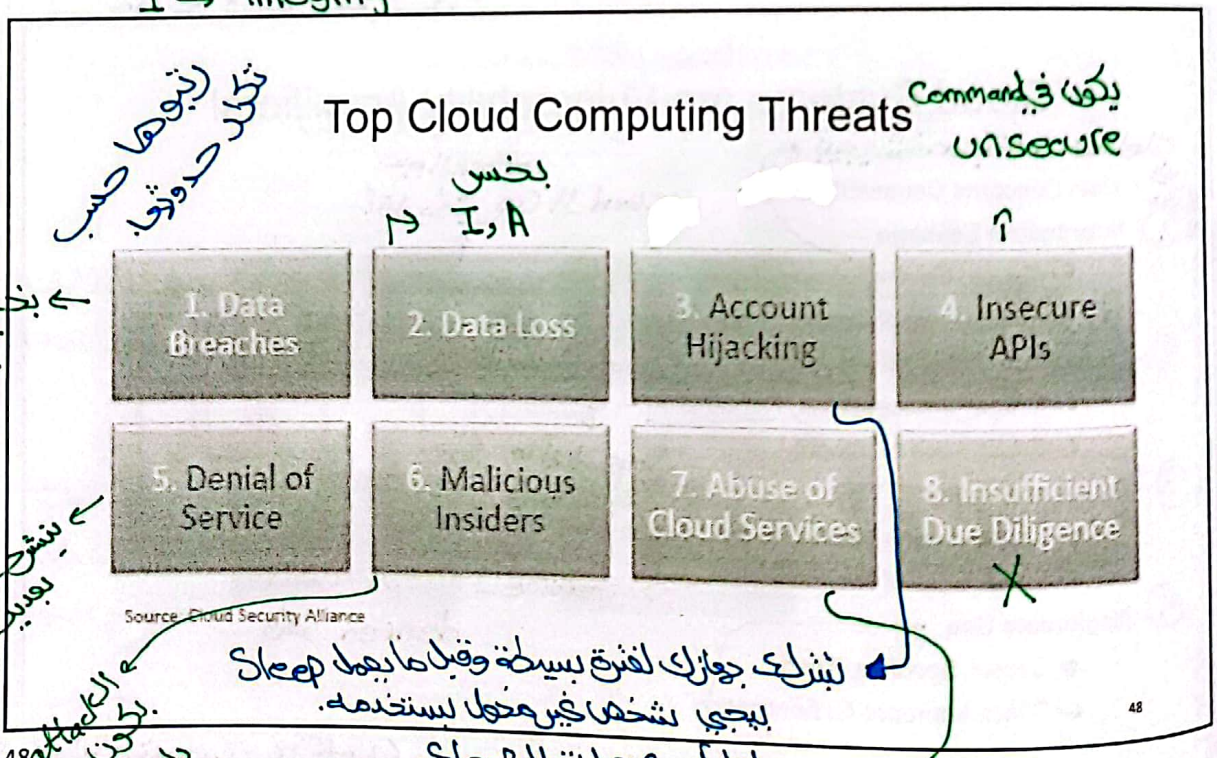
illegal use (Netflix أكثر من واحد يفتح حساب واحد)

2
- * Authorization : انا بعد ما كنت عملت login بعد data of Permissions بعمل
- 1 * Authentication : login بعمل بطريقة معينة .



47

C → Confidentiality A → Availability
I → Integrity

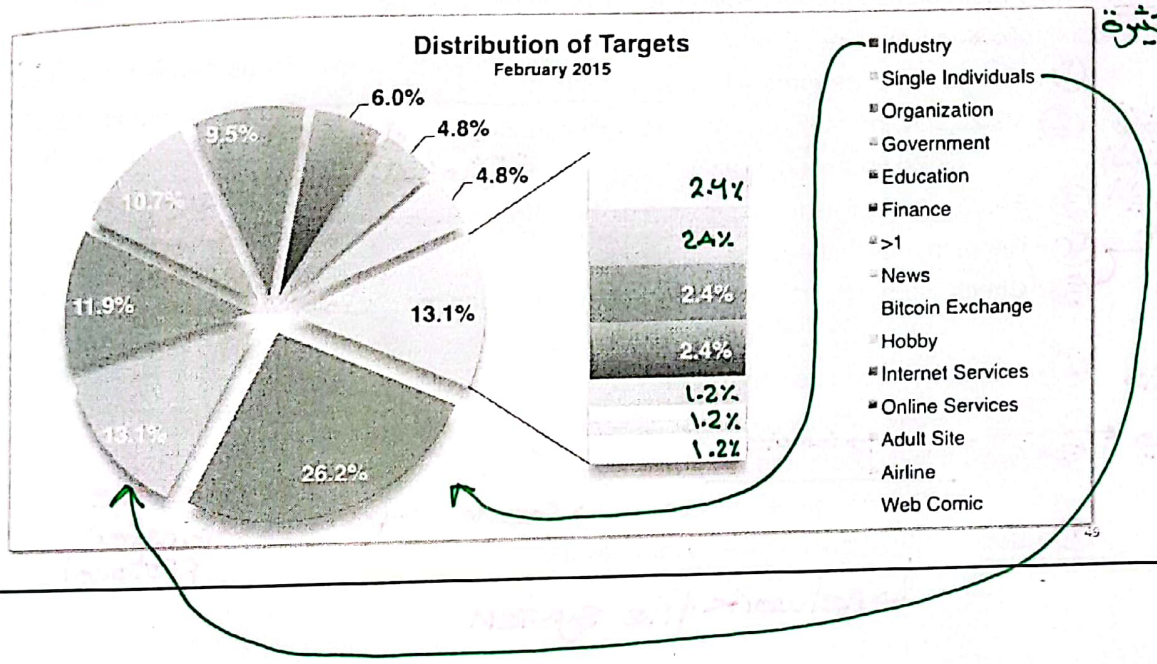


48

Slide 51 & Security الى كتبي linux كيف أحسن لها *

فممكن ← cyber space صار موضوع مهم لإنه الناس صارت تعيش فيه كمان Everyone is being cyber-attacked!

بحيث له attacks كثيرة



49

← الأسباب اللي بتدفع شخص يعمل attack

Why Cyber-attacks are launched by hackers?

- Entertainment → للتسلية
  - Disruptive mentality to write virus/worms/trojans
- Social acceptance → (للشهرة) أسماء وهمية /
  - Website defacement, "Hacker's God"
- Fraud → السرقة
  - Hacking for SSN, Credit Card #s and other sensitive information
- Earning ransoms
  - Threats to sabotage services using DDoS attacks

50

50

. سؤال امتحان : الـ recommendation لتحقيق الـ Security

* على الـ attack الـ VM أصعب من الـ VM نفسه .

← بنركز عليه لأنه Free و open و widly use

1/3/2021

In-Class Exercise: How to Secure Linux OS?

- To avoid malicious compromise of system resources for DDoS attacks, following issues need to be addressed:
  1. Use strong passwords – lock account if multiple login failures
  2. Install only the required software packages → نزل أشياء كاتبينها ناس موثوقة
     - Do you need Apache?
  3. Setup access lists for services (i.e., host firewall) → كل Service يكون معروف شو مسموحلها تعمل
  4. Regularly patch the OS
  5. Check listening ports and verify if those are required (نفتح الـ Port الي بنحتاجه فقط)
     - Use "netstat" or even an Intrusion Detection System (IDS) for monitoring
  6. Run only required system services
     - Use "chkconfig" to list all services started at bootup
  7. Avoid telnet, rlogin (→ remote) and rsh – use scp/sftp instead (Protocols فيها نقاط ضعف)
     - Secure remote access (scp ↳ secure copy; sftp → Secure file transfer protocol)
  8. Secure NFS if sharing files over network ↳ network file system

51

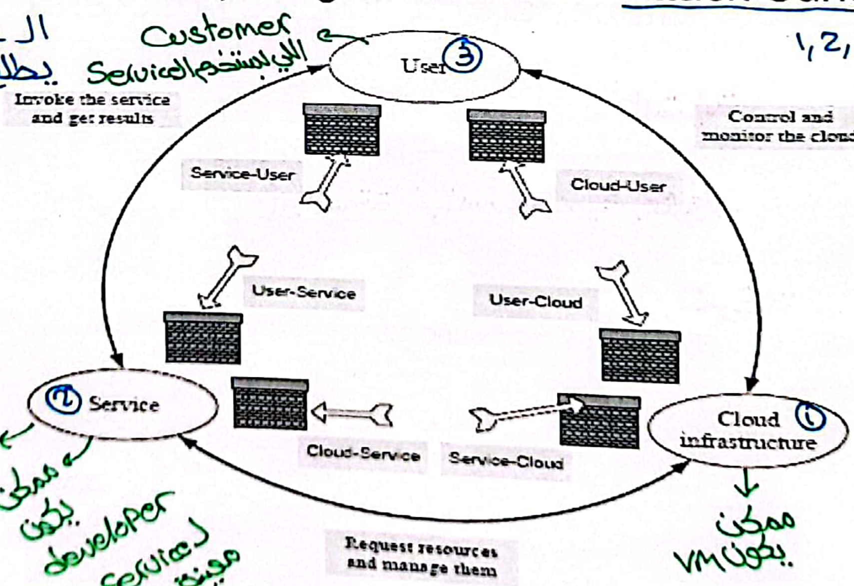
51

← بتحدد فيه شو هم الـ actors الي موجودين في الـ System الي ممكن

Cloud Computing Environment Attack Surfaces

الـ attack يطلع منهم أو يحصل عليهم .

1,2,3 Main actors



Customer ← الي بيستخدم الـ Service

web server ← ممكن يكون developer ← Service معينة على الـ VM

↓ ممكن يكون VM.

52

52

*صارت الشركات عشان تلاقي نقاط الضعف تنزل الـ System وتحكي للكل معكم شهر اللي بيوجد أكبر نقاط ضعف الها مكافئة مادية فبحيس كل الناس يشتغلوا ليكتشفوا الأخطاء وفيك ما بدفعها كتير ليكتشفوا الأخطاء.

Attacks in a Cloud Computing Environment (1)

Three actors involved; six types of attacks possible

1- The user can be attacked by:
   - (a) • Service → SSL certificate spoofing, attacks on browser caches, or phishing attacks
   - (b) • The cloud infrastructure → attacks that either originates at the cloud or spoofs originate from the cloud infrastructure →

مثلاً جوجل ممكن تطلع معلومات كتير ما بدكم تطلع.

attack الـ ممكن

2- The service can be attacked by:
   - (a) • A user → buffer overflow, SQL injection, and privilege escalation are the common types of attacks

لـ ← حناخدهم بالتفصيل

53

Attacks in a Cloud Computing Environment (2)

   - (b) • The cloud infrastructure → the most serious line of attack; Limiting access to resources, privilege-related attacks, data distortion, injecting additional operations → Service الـ attack الـ VM بتحاول تعمل

3- The cloud infrastructure can be attacked by: طبقًا بعد ما الـ VM حارفيها attack.
   - (a) • A user → targets the cloud control system
   - (b) • A service → requesting an excessive amount of resources and causing the exhaustion of the resources →

Setting بتخرب الـ VM تاعت الـ

بتشل Service تعمل الـ VM down وفيك بخرب كل الـ Services

54

سؤال امتحان ؟ بتعطيك مثال وبتقلك شو اللي حيخرب (C or I or A)

* Certificate ← مثلاً لو بدك تتقدم لطلب رسمي لازم ترفق هويتك ليتأكدوا منك وهاي هي الـ Certificate.

* Certificate Authority: منظمة (جهة) بتعطيك الـ Certificate مثل الأحوال المدنية.

* لو اثنين بدهم يتواصلوا لازم كل واحد يظهر الـ Certificate تاعته + key لنفس

المسج عشان ماحد غريب يفهموا. (شيفرة وفك شيفرة)

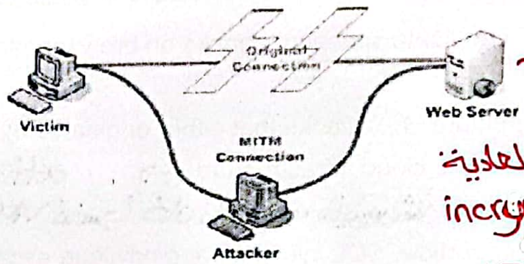
← Attak من الـ User باتجاه الـ Service

SSL-Authentication Attack = HTTPS downgrade

فيه نقاط ضعف ← Service Socket Layer ـها

- "Man-in-the-Middle" Attack – attack on mutual authentication (or lack thereof); occurs if there is no trusted Certificate Authority — الـ Certificate مش صالحة.

شخص بالنص بصير يبعت للأول والثاني وأساساً هو الأول والثاني وبيوهمهم إنه هو الشخص الصح



→ HTTP (80) ↓ بيبعت بالصيغة العادية مابعمل incryption

فعملوا HTTPS = HTTP + Secure Socket layer Protocol

hyper text transfer Protocol

- Hacker hijacks user data
- Bypasses nearly all site security

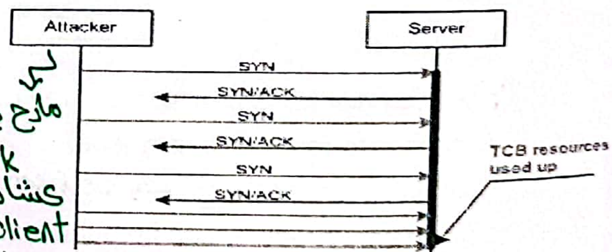
بعمل شيفرة.

③ DNS: بعملك translation من Names لـ IP Addresses

Client → DNS (fake IP) ← attacker → Attacker الخطأ

Denial of Service ← الأشهر.

ـه حيضرب الـ availability



ـه مارح يبعت Ack عشانه مو أصلاً Client فحيظل يهلك الـ Server لحد ما يوقعه

① • Attacks on end hosts
   – SYN attack

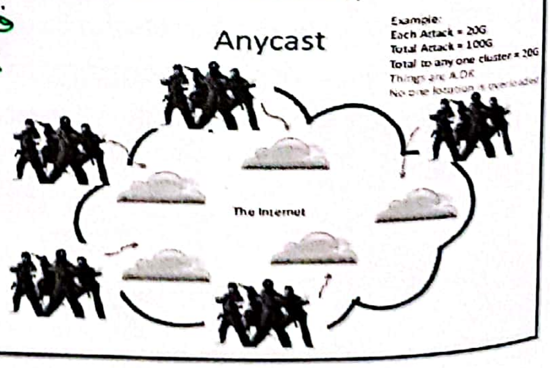
② • Attacks on routers
   – Pollute route cache ← بخلي الـ entry الموجودة بالـ router غير صحيحة فبوديني على أماكن غلط

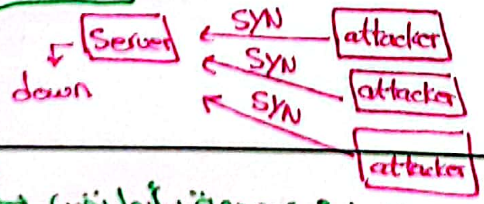
• DNS Poisoning ③

• Authentication attacks
   – False requests block legitimate access attempts → Denial of Service

④ • Distributed DoS attacks can be defended by Anycast → (DDoS)

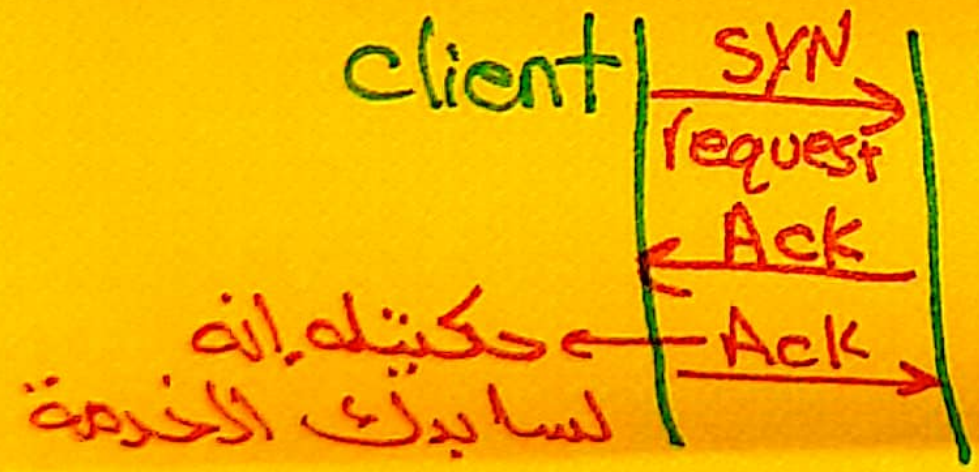
خطير وأوسع من DoS وعلى الـ التقارير الإعلامية.





← الحل: مجموعة بيأدوا نفس الوظيفة (أي request بيجيني بقدر أبعته لأي حد من الـ Servers)

① Tcp connection ؟ I need 3 way hand shake



Internet Control Message Protocol (ICMP)

الـ Protocol اللي بنستخدمه بالـ Ping لبعت الـ Packet

Ping Flood

زي اللي بنعملها Command على الـ Prompt مثلاً:

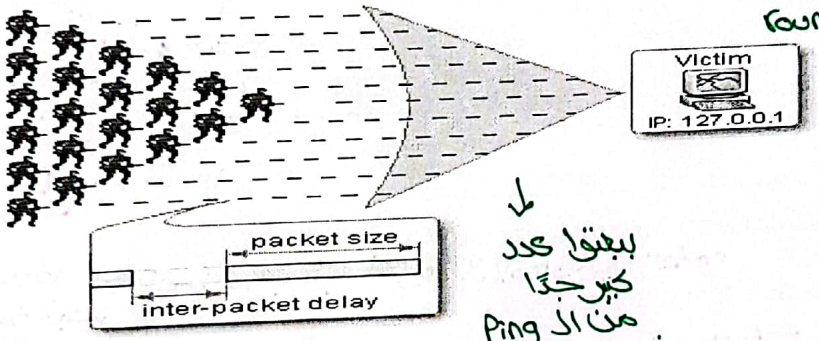
Ping www.google.com

الغاية منه

1- نتأكد من السيرفر running و up إذا

2- نعرف الـ roundtrip time (وقت) الرحلة والرجعة للـ Packets

- Often from many computers, Ping used for testing latency
- Huge amounts of pinging can slow a server and make it unusable



بيبعتوا عدد كبير جدًا من الـ Ping فبخلي الـ System بطيء أو down

57

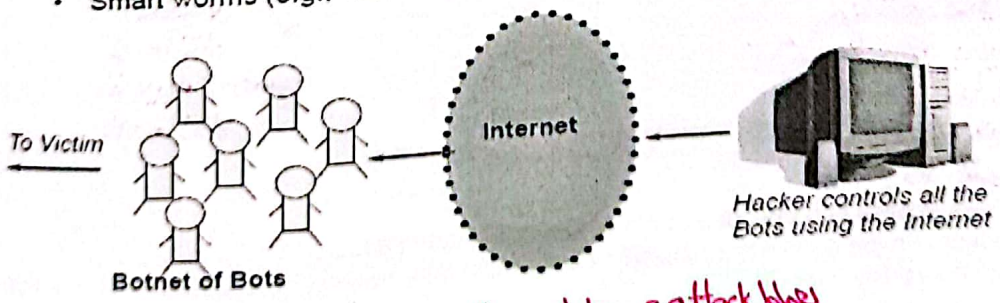
57

Hackers use "Botnets"

برنامج بسيط بحطه على الـ Computer بتعمله access عن طريق الانترنت

- "Bot" – a simple program planted on a computer that accesses a "Command Center" (E.g. IRC Channel)
- A huge group of bots on the Internet is called a "Botnet"
- Botnets are rented out for launching cyber attacks and spam services
- Smart worms (e.g., C-Worm)

* Attack هذا الـ * مدسوس بتعمل



↳ Bot zombie → other entity attack بعمل بالـ Net حسب نوع الـ Bot اللي انزرع فيهم.

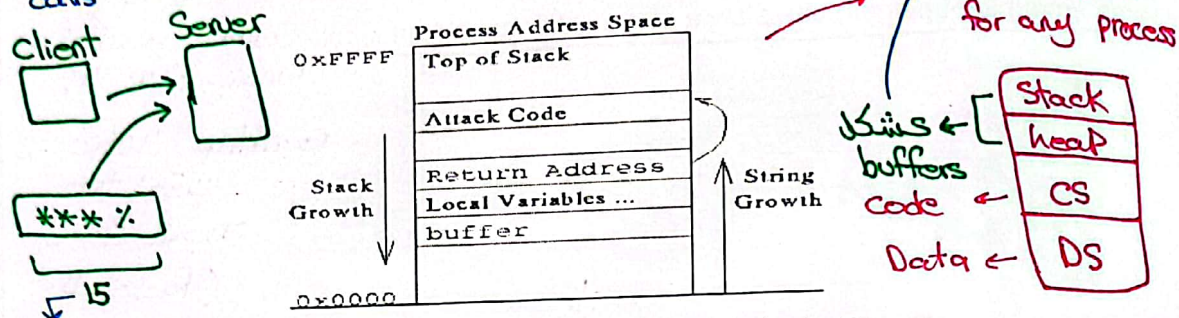
58

58

Buffer Overflow

Stack ↓ (Static / Function calls) heap ↓ (Dynamic / Variables) local variables مسموح نكتب فيها الـ

- Buffer is the window of space allotted for use in a computer



مطلوب مثال user يدخل، max الـ 15

- Hackers use viruses to use more memory than the buffer can handle → – Often causes computer or server to crash

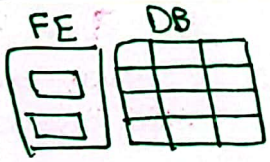
→ الـ hackers بكتب أكثر من الـ max وبزيد الـ code فبتخلص كل الـ task فبصير يكتب عالي بعده

* الحل إني ما أسمحله يعمل Buffer overflow بطريق إني أعمل Filtering

فوقيك بتتضرر الـ Server لإنه انزرع فيه أشياء غلط (crashed).

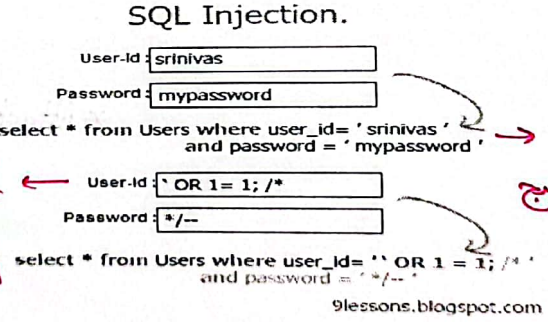
59

* الـ frontend فيه GUI والـ backend بكون فيها الـ database.



SQL-Injection

- Attacker executes malicious code with purposeful errors on a website



المفروض لو ما لقاه إنه يبعت مسج إنه ما لقاه

هذا الكود اللي كتبه الـ attacker بخير بروحك الـ table كامل تاع الـ users فوقيك خيروق كل اشي، وما يروح مسج إنه ما لقى username الـ

- Allows access into the computer's or server's databases
- Attacker can get database dump with confidential information from the website if user input is not rigorously filtered

الحل انه نعمل Filtering

60

60

هيك بكون وصل لـ database وهذا خطر.

* HTML ← language لكتابة المواقع.

* ماتفتح أي link بيوصلك عشان ممكن يكون خطير.

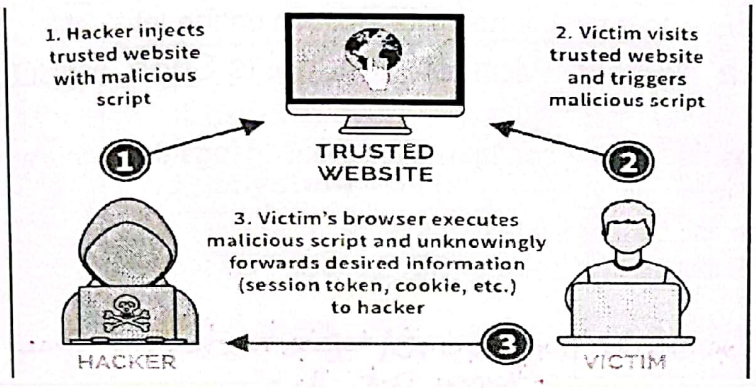
1/3/2021

لو في أشياء بها تطلع عالـ webpage متغيرة بشكل مستمر مثل فيديو.

Cross Side Scripting

attack → بستغل الـ DHTML به خبرة عالية مو أي حد بقدر يعمله.

- Hacker takes advantage of dynamic HTML pages
  - Embeds malicious Javascript, ActiveX, Flash into a vulnerable dynamic page to fool users, executes them and steals data
  - Webpage that passes parameters to a database is vulnerable



* بحيروا يحطوا فيروس داخل هاي البيانات المتغيرة فبحير لو كبست الـ link أو فتحته بخربلك الـ Server أو بنزل فيروسات.

61

61

بدنا نحاول نكتشف الـ attacks قبل ماتحير ؟

Network Security Tools

Packets بشوف كل الـ اللي بتفوت وبتطلع ولو كان كتير Packet ؛ high traffic volume معينة

① • Wireshark - monitors all information entering and leaving the computer

http://www.wireshark.org/

بلاحظ إنها ممكن تكون DoS attack ضروري نتطلع عليها باستمرار.

② • Snort - detects intrusions into the system and logs them for further examination on servers AND networks

http://www.snort.org/

براقب وبعمل detect لو اجاني high volume (traffic

IDS → Introgin Detection System

62

لنعرف نوع الـ attack قبل ما يخطر في الـ System.

Robot Network كلمة اجت من ← Botnet *

Honey Pot

بالعامية بحطوها أصلهم ال Real Service الي بهم يحموها.

- Honey Pot is a network of computers that need to be protected
  - It appears to a hacker as a real-system while in fact, it carefully monitors the hacker attacks
  - Collects clues to trace the hacker's location on the Internet
- It includes a "Network Monitor" that hosts Snort, MySQL, etc.
  - Snort rules need to be configured for creating logs that contain:
    - Alert Timestamp
    - Source and Destination IPs
    - Alert Signature (E.g. could be DDoS attack, Port-scanning)

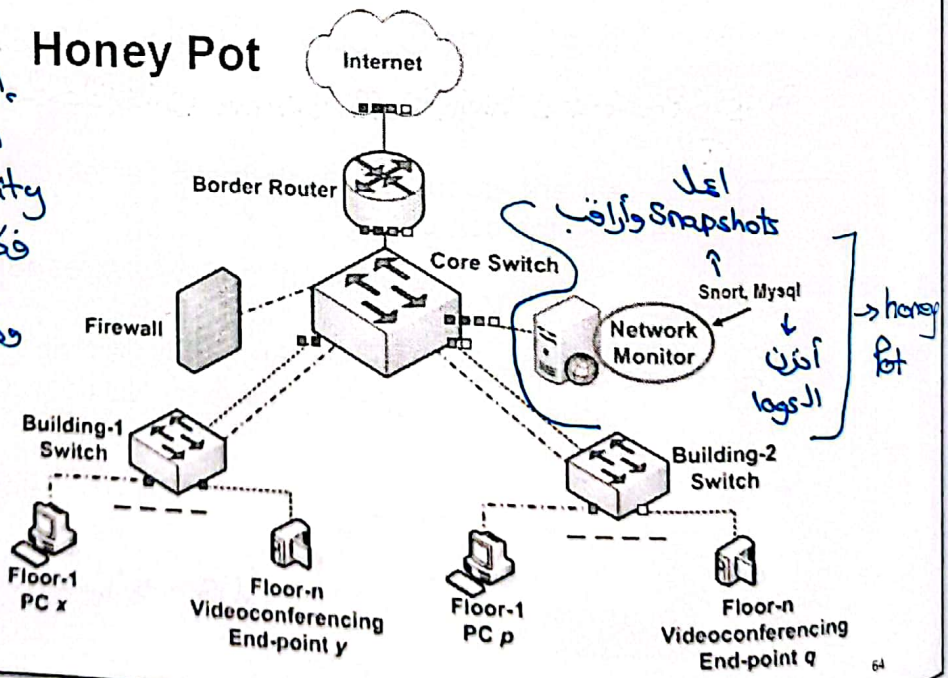
مساحة لل hackers بيفكروا إنهم خربوا فيروال Server بس هم بكفوا بال Honey Pot

63

63

بتدخل على Real service فقط الأشياء الموثوقة غير ذلك بتخليهم بال honey pot بلعبوا و يخربوا فيروا كيفهم.

Honey Pot



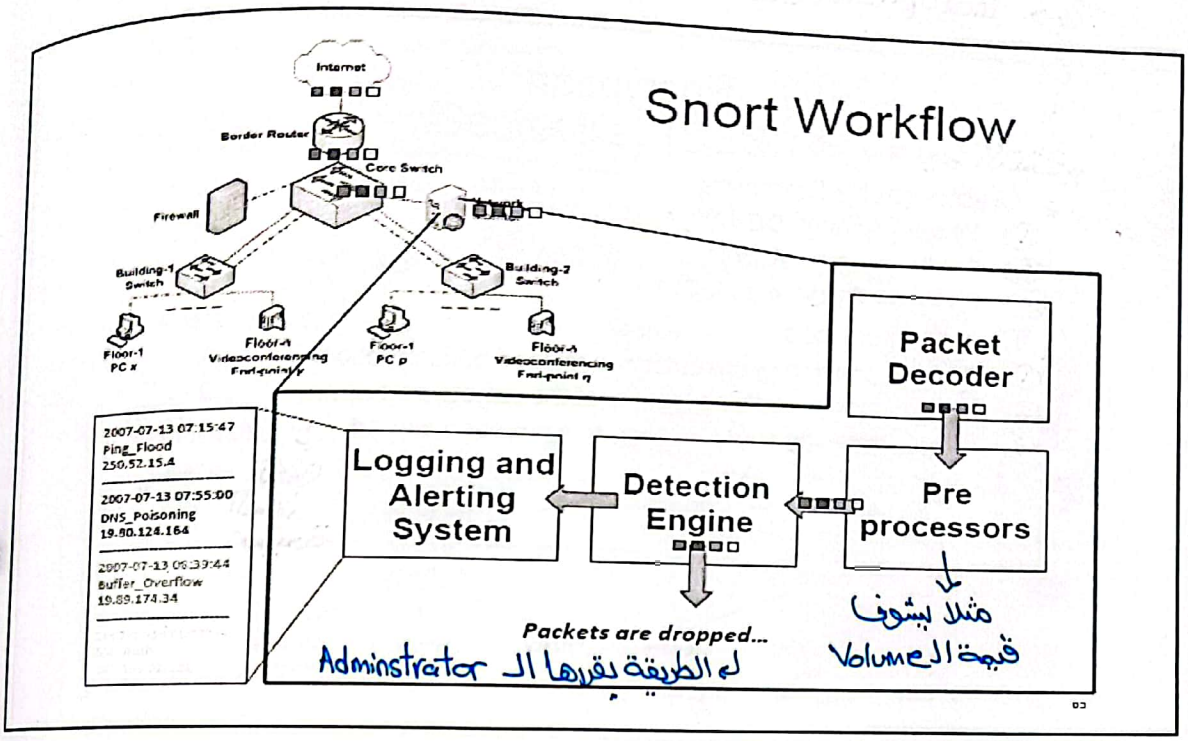
بتبين للأشخاص (attacker) إنها network عادية بس هي بالأصل honey pot حاطط عالية Security فكإنها محببة لل attacker. وهي بتكون monitoring فقط ولكن بتبين لل attacker إنها Real Service.

اعمل وأراقب Snapshots

أخزن الدوما

64

64



65

Auditability of Cloud Environments

resources sharing سببها الـ

- The lack of transparency makes auditability a very difficult proposition for cloud computing والـ Virtualization لأنه تسجيل كل اشي بفيرنا .
  - Standardization of cloud computing is in evolution, and hence is also a major concern
- There is the need for international regulations adopted by countries where data centers of cloud computing providers are located * المشكلة هنا Standard .
  - SLAs do not provide adequate legal protection for cloud computer users, often left to deal with events beyond their control * لحالها ما بتخوف
  - International Safe Harbor Privacy: enables some US companies to comply with privacy laws protecting EU and Swiss citizens ✗ → بعض الدول الأوروبية طلعت Standards
- Auditing guidelines elaborated by the National Institute of Standards (NIST) are mandatory for US Government agencies:
  - Federal Information Processing Standard (FIPS)
  - Federal Information Security Management Act (FISMA)

→ داخل US

لا في اشي هما الـ Standard بحطوله.

66

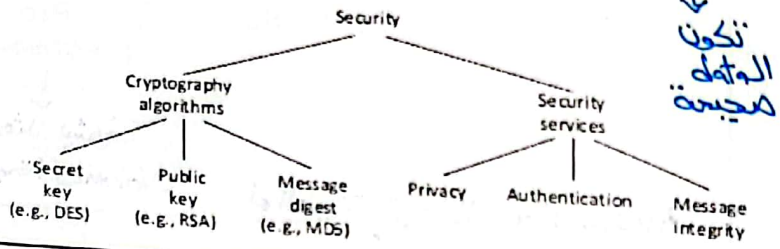
لـ مش مطالبين فيه ، بس لازم نعرف إنه في بلدان مطالبة بتحقيق الـ Security والأمان عن طريق أهم طلعوا Standard زي سويسرا

Incryption and decryption

Encryption

التشفير

- Cryptography functions
  1. Secret key (e.g., DES)
  2. Public key (e.g., RSA)
  3. Message digest (e.g., MD5)
- Security services
  1. Privacy: preventing unauthorized release of information
  2. Authentication: verifying identity of the remote participant
  3. Integrity: making sure message has not been altered

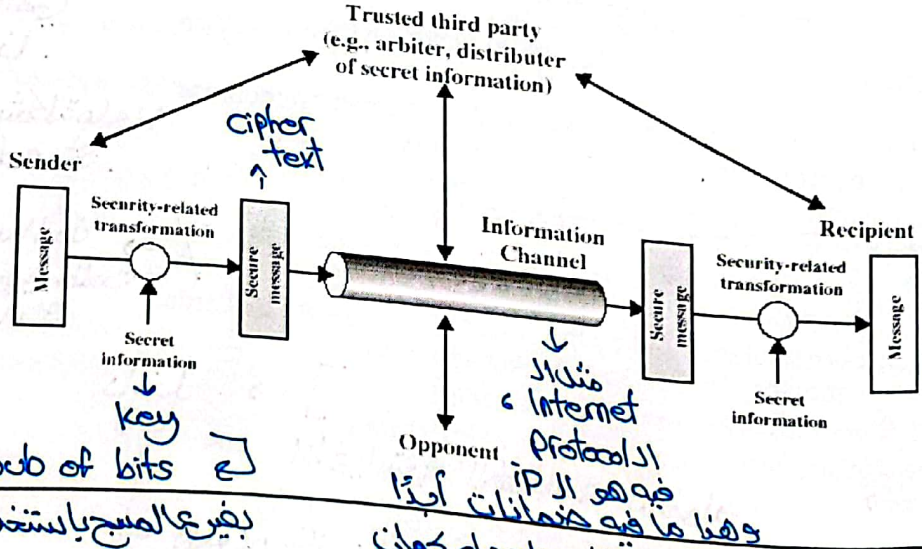


نكون الداتا صحيحة

67

67

Model for Cyber Security



key → group of bits

بفيرغ الصح باستخدموم

مثلاً Internet Protocol هو الـ IP وهنا ما فيه ضمانات أبدًا فبالعادة بستخدموا معه كمان Protocols للتحسين.

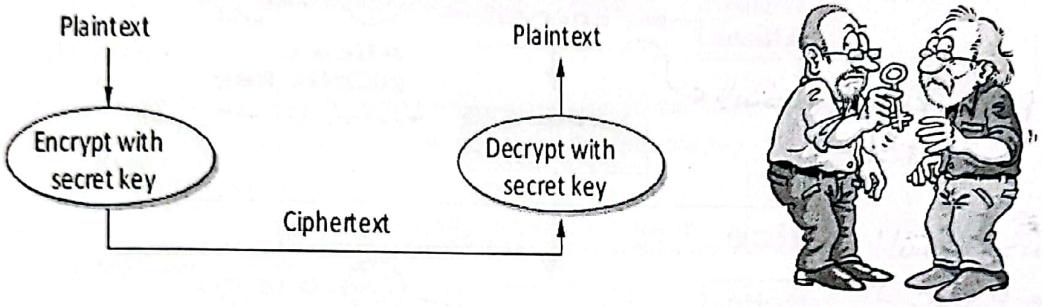
68

68

①

Secret Key (DES) = Symmetric key.

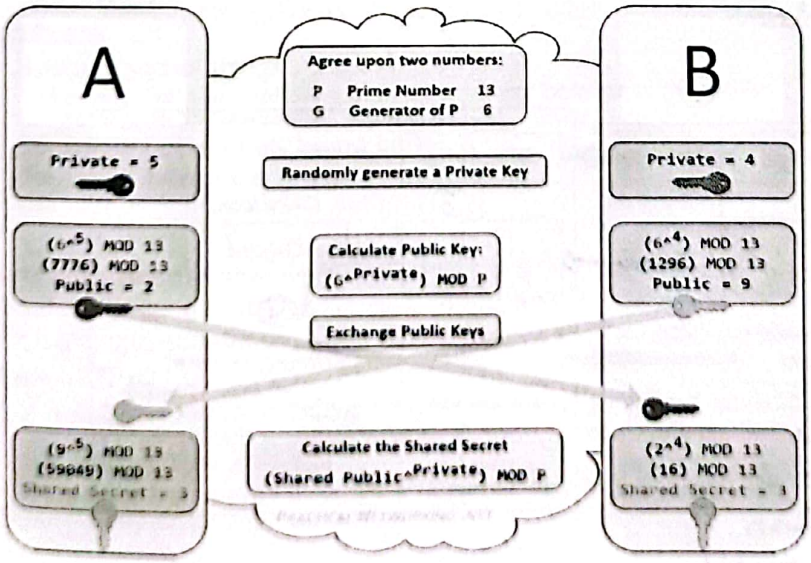
نفس الـ key للطرفين وهما
معروف بين الطرفين والجهة اللي أصدرته .



69

9

Authentication Protocols



X

غير مطالبين فيها بالمادة.

70

70

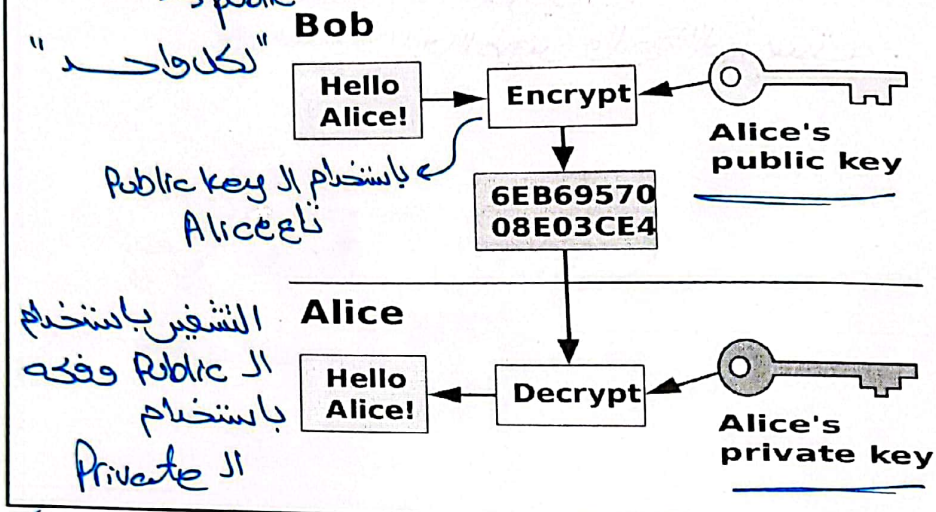
* بالبداية كان الـ key حجمه 64 bit الآن أصبح يزداد
كشان نصعب عملية الـ attack
يجربوا كل احتمالات الـ key لحد ما يفكوا التشفير ← (exhaustive search)

1/3/2021

② Public Key Authentication = Assymetric

2 keys → Private
→ public

"لكل واحد"



باستخدام الـ Public key تاع Alice

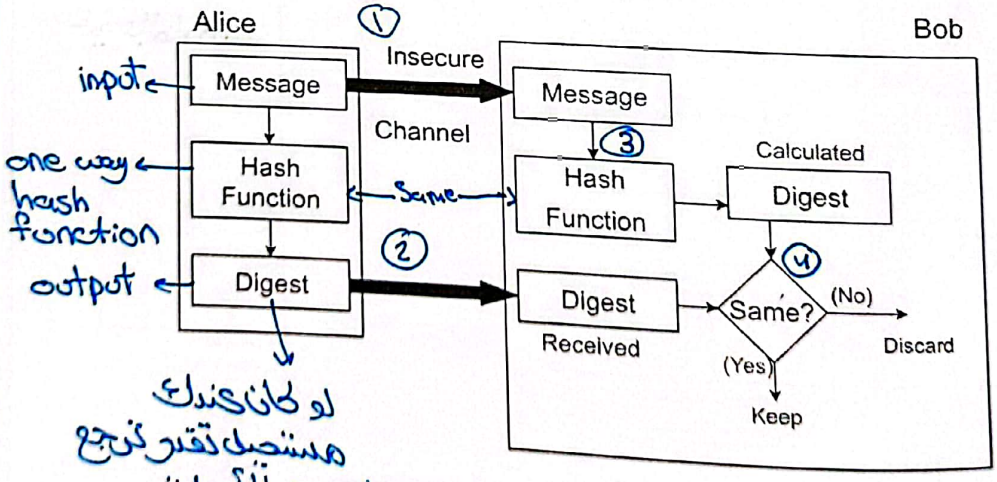
التشفير باستخدام الـ Public وفكه باستخدام الـ Private

71

بالنهاية بترجع نفس المسج.

Confidentiality أكتر من الـ Integrity يعني؟
(هاي اللي بتشتاق المسج المهم ما يغيرها المسج)

Message Digest

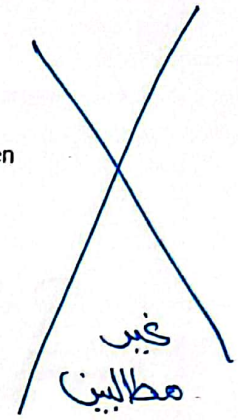


لو كان عندك مستحيل تقدر ترجع المسج الأصلية.

72

Message Integrity Protocols → في كذا حد كبير هنوعا

- Cryptographic checksum in Message Digest
  - Just as a regular checksum protects the receiver from **accidental** changes to the message, a cryptographic checksum protects the receiver from **malicious** changes to the message
- Protocols
  - Digital signature using RSA
    - special case of a message integrity where the code can only have been generated by one participant
    - compute signature with private key and verify with public key
  - Keyed MD5
    - sender: $m + MD5(m + k) + E(k, private)$
    - receiver
      - recovers random key using the sender's public key
      - applies MD5 to the concatenation of this random key message
  - MD5 with RSA signature
    - sender: $m + E(MD5(m), private)$
    - receiver
      - decrypts signature with sender's public key
      - compares result with MD5 checksum sent with message



73

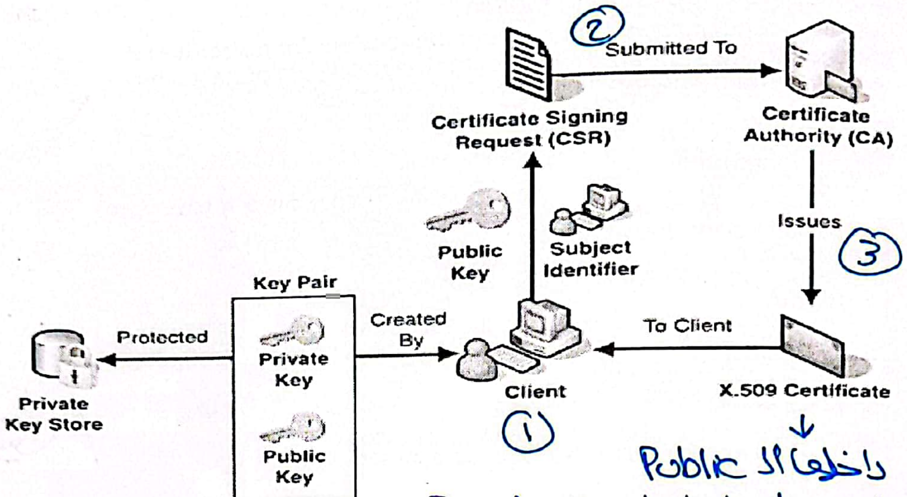
Key Distribution (X.509) (1) "مناوين بنجيب الـ key" *keytools

key distribution لـ إحدى طرق الـ · key بنعمل generate

- Certificate
  - Special type of digitally signed document:
    "I certify that the public key in this document belongs to the entity named in this document, signed X."
  - the name of the entity being certified
  - the public key of the entity
  - the name of the certified authority
  - a digital signature
- Certified Authority (CA) → بجيب منه الـ Public key
  - Administrative entity that issues certificates
  - Useful only to someone that already holds the CA's public key
- Chain of Trust
  - If *X* certifies that a certain public key belongs to *Y*, and *Y* certifies that another public key belongs to *Z*, then there exists a chain of certificates from *X* to *Z*
  - Someone that wants to verify *Z*'s public key has to know *X*'s public key and follow the chain

74

Key Distribution (X.509) (2)



Public داخلها ال

بعمله distribution وال Private بحفظه جوه وما بشاركه مع أي شخص.

75

Trust

لو ما في threat كان ما بنحتاج الثقة ← Trust → بحتاجه لما يكون عندي Risk معين وبنفس الوقت في عندي Interdependence (أشخاص عندي ثقة فيهم)

- "Trust is the assured reliance on the character, ability, strength, or truth of someone or something..."
  - Needed for dealing with complex phenomena: enable cooperative behavior, promote adaptive organizational forms, reduce harmful conflict, decrease transaction costs, promote effective responses to crisis
- Two conditions must exist for trust to develop:
  - *Risk* → the perceived probability of loss; trust not necessary if there is no risk involved, if there is a certainty that an action can succeed
  - *Interdependence* → the interests of one entity cannot be achieved without reliance on other entities
- A trust relationship goes though three phases: → بحتاجها بال VM migration
  1. *Building phase*, when trust is formed → بنبني الثقة بال entity
  2. *Stability phase*, when trust exists → عندك ثقة كاملة بال ,,
  3. *Dissolution phase*, when trust declines
- An entity must work hard to build trust, but may lose the trust very easily!
  - Internet obscures or lacks entirely the dimensions of character and personality, nature of relationship, and institutional character of the traditional trust

76

* سمعة ال VM مهمة: من الصعب بناؤها وبسهولة يمكن خسارتها.

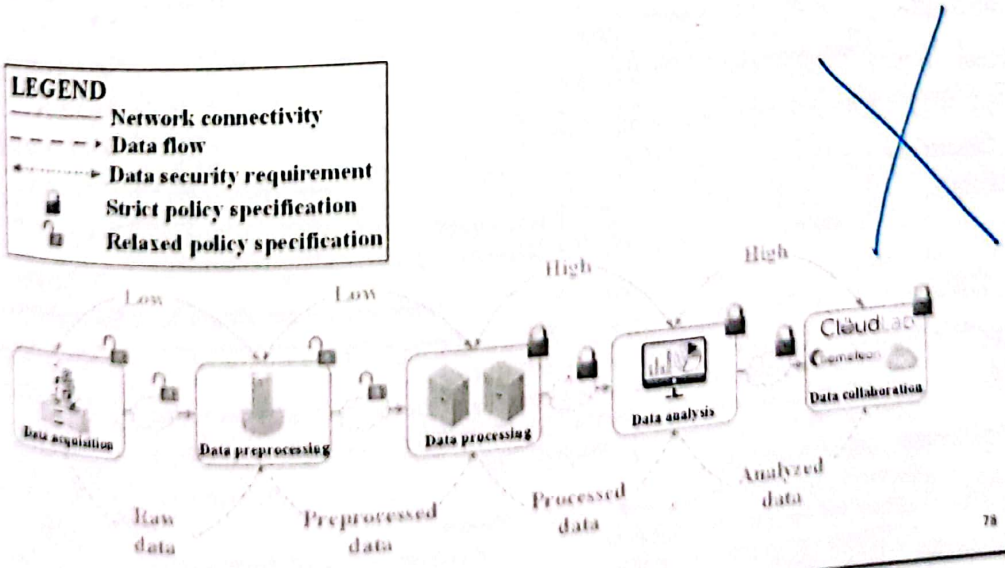
Trust Determination

- Policies and reputation are two ways of determining trust:
  - *Policies* reveal the conditions to obtain trust, and the actions when some of the conditions are met
    - Policies require the verification of credentials
    - Credentials are issued by a trusted authority and describe the qualities of the entity using the credential
  - *Reputation* is a quality attributed to an entity based on a relatively long history of interactions or possibly observations of the entity
    - Recommendations are based on trust decisions made by others and filtered through the perspective of the entity assessing the trust

- In a computer science context:
  - Trust of a party *A* to a party *B* for a service *X* is the measurable belief of *A* in that *B* behaves *dependably* for a specified period within a specified context (in relation to service *X*)

77

Federation Trust for Application Workflow



78

In-Class Exercise

- What are the cybersecurity challenges for the cyberinfrastructure supporting data-intensive science applications?
- How can a secure middleware benefit a user for such applications?

* سؤال امتحان؟ بتعطيك مثال وبتقلك شو في Trusted Base Computing فيه.

↳ trusted base computing

* Dom0 هي الـ Xen في الـ Security المسؤولة عن الـ entity الـ *

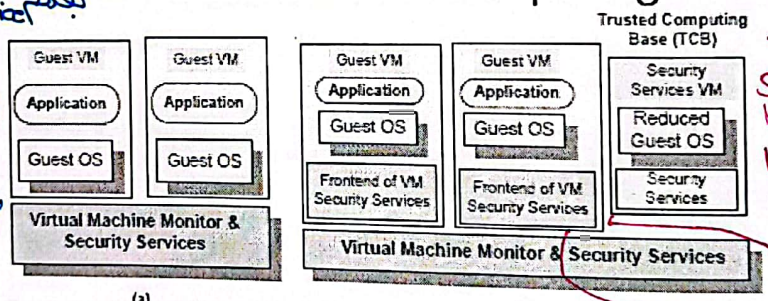
79

Cloud Invironment ← شي مهم كتير في الـ

Trusted Base Computing

أي شي في الـ System بقدم Security Service

Firewall إذا Physical أو الـ HW بقدم Security Service.



مسؤولة فقط Security بنط كليا light weight OS

أفضل الـ Security Services

Virtual security services provided by the VMM

Dedicated security VM

- A secure TCB (Trusted Computing Base) is a necessary condition for security in a virtual machine environment
  - If the TCB is compromised then the security of the entire system is affected
    - URB or Gatekeeper-Proxy are the TCB elements!
  - Can you recall the Domain 0 case with Xen?
- Trusted paths mechanisms
  - Support user interactions with trusted software
  - Critical for system security: if such mechanisms do not exist, then malicious software can impersonate trusted software

جزء من الـ VM

للتعريف انه في اشي خاص Security منفصل عن الـ VM

80

أنضمن الـ os وأنقى من ناحية الـ Security لأنه التركيز عليه هون أكثر من الـ OS

Virtual Machine Security

- In a traditional VM, the Virtual Machine Monitor (VMM) controls the access to the hardware and provides a stricter isolation of VMs from one another than the isolation of processes in a traditional OS
  - A VMM controls the execution of privileged operations and can enforce memory isolation as well as disk and network access
  - The VMMs are considerably less complex and better structured than traditional operating systems thus, are in a better position to respond to security attacks
  - A major challenge → a VMM sees only raw data regarding the state of a guest operating system, while security services typically operate at a higher logical level, e.g., at the level of a file rather than a disk block

① VMM ناخذ الـ VM ناخذ مباشرة (hypervisor) عال HW

② host os يكون الـ VMM ناخذ الـ

advanced

ما عنده تفاصيل كثيرة عن الـ guest OS

Machine Image Security

→ بتوصلني لل Infrastructure as a service.

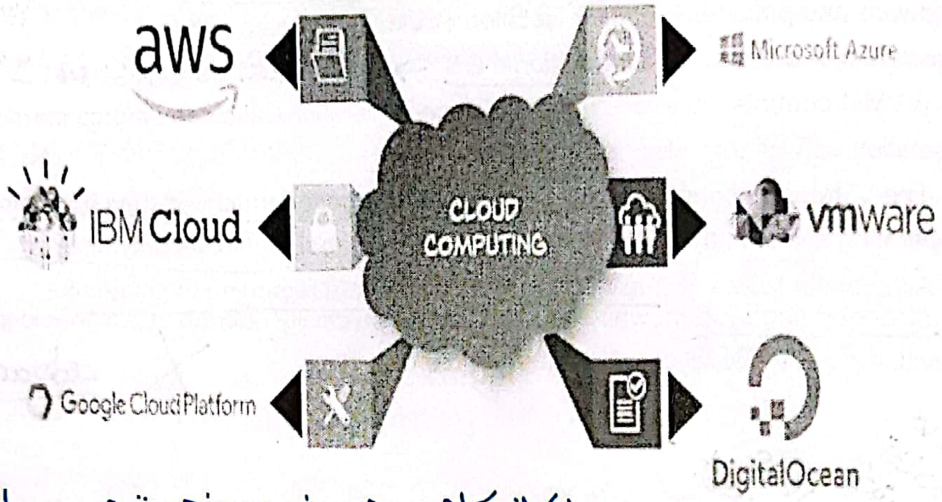
- Image sharing is critical for the IaaS cloud delivery model
  - Amazon Machine Images (AMIs) accessible through AWS Quick Start
    - Access: Community AMIs of the EC2 service; VM Appliance Marketplaces
- Many of the images analyzed recently show concern → تعتبر نقاط ضعف
  - Allow a user to undelete files, recover credentials, private keys, or other types of sensitive information with little effort and using standard tools
  - A software vulnerability audit revealed that 98% of the Windows AMIs and 58% of Linux AMIs audited had critical vulnerabilities
- Security risks:
  - Backdoors and leftover credentials
  - Unsolicited connections
  - Malware

فيها VMs كثير منهم محسنين من VM آخرين وحتى لو انت عدلت بتقدر تنزل الـ VM وبيجيبك اللي بيستخدموا بيدفعلك فلوس.

* الـ SLA لوحده موكافي يحل مشكلة الـ Security بين الـ customer والـ Provider.
لأنه مابيحكي فيه عالـ Security.

1/3/2021

Cloud Platforms



Free teer مشكلتهم كلهم بدهم دفع ، بعضهم بقدم

 ولكن لفترة زمنية معينة فقط

فطلع عندي open source :

① Eucalyptus → بستخدمه

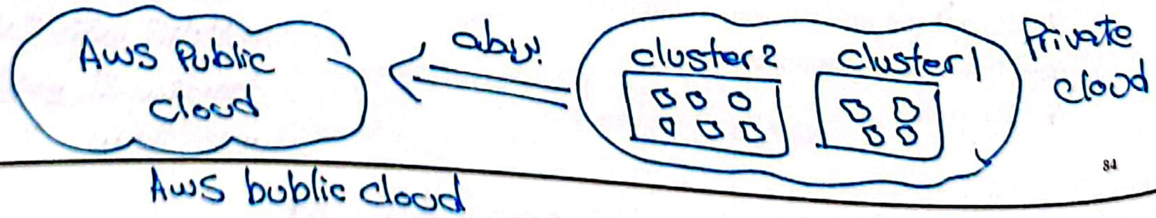
Private يعني ممكن نبني
AWS Public وترتبطها cloud
بتحط فيها data cloud مش حساسة

* Private cloud لـ build لعمل + hybrid

- Eucalyptus is an open source, Amazon Web Services-compatible, private and hybrid cloud computing environment

باختصار

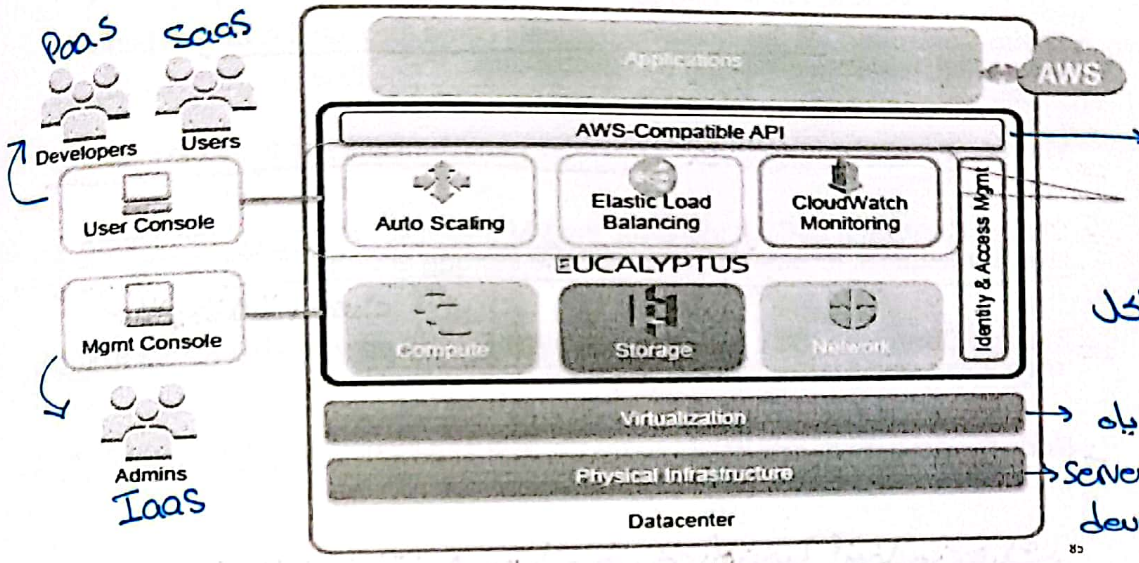
- It is an acronym for **Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems**
- The goal of Eucalyptus is to allow sites with existing clusters and server infrastructure to host a cloud that is interface-compatible with Amazon's AWS and the Sun Cloud open API.



Aws bublic cloud

(general View)

Eucalyptus cloud platform → فيها تشابه مع الـ AWS

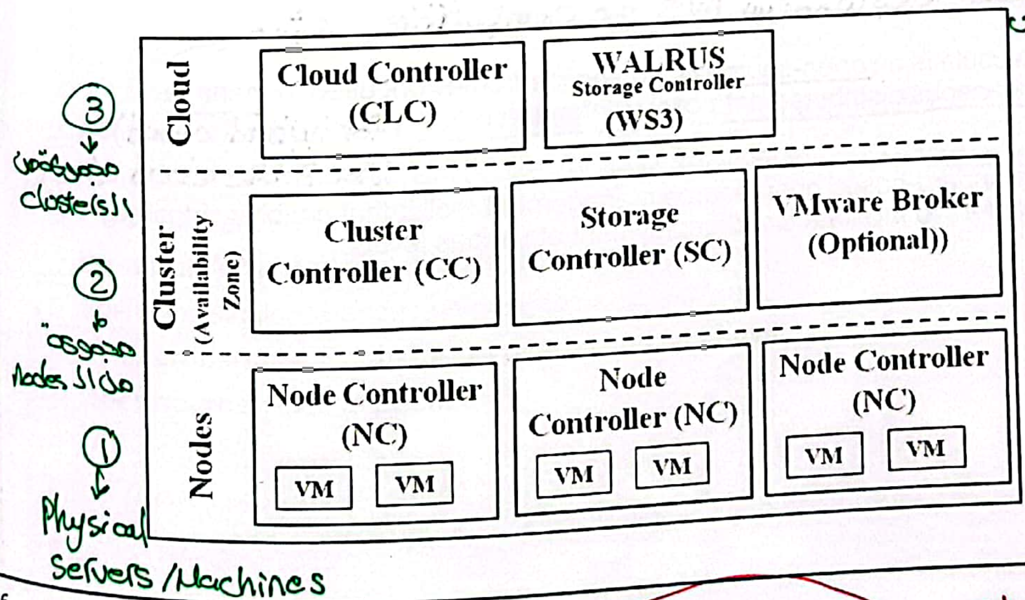


85

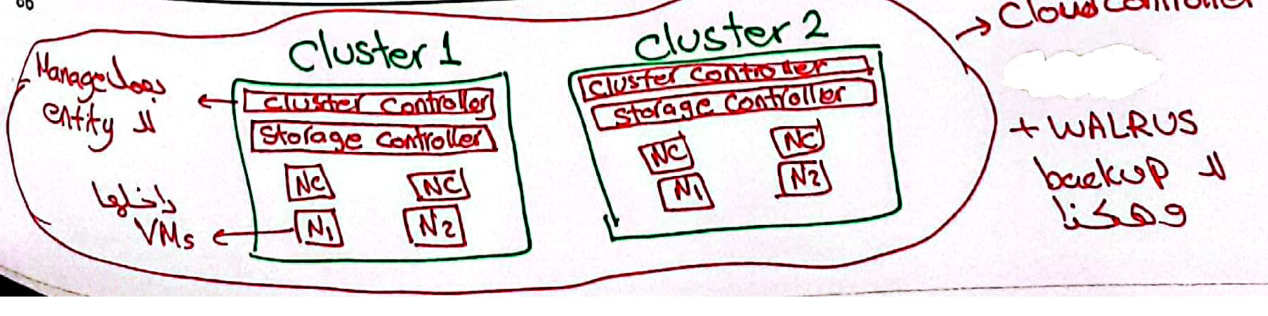
ماهي الـ basic Services اللي أي open source cloud platforms لازم يقدمها؟
1- Pooling الـ resources 2- Identity and access Managment 3- VM Images (لازم تخزنها Storage)

Components of Eucalyptus (1)

* عدد الـ clusters والـ Nodes بعتمد على الـ use case



86



Components of Eucalyptus (2)

- **Cloud Controller**: All the incoming requests come through the CLC. It performs scheduling, resource allocation and accounting.
- **Walrus**: It is similar to **AWS S3**. It provides persistent storage to all the instances.
- **Cluster Controller (CC)**: It manages the VM (instance) execution and service level agreements. It communicates with the storage and network controller.
  ← الي جوا الـ cluster
- **Storage Controller (SC)**: It is similar to **AWS EBS**. It provides block level storage to instances and snapshots within a cluster.
- **Node Controller**: It hosts all the instances and manages their end points.

طبعا كلما بنتقدم بتطور فممكن يكون حل أفضل من هيك.

87

87

② OpenNebula Cloud Platform

. بس ممكن يكونوا اشتغلوا عالنقطة AWS EC2 compatible مش ←

- OpenNebula is an open-source cloud service framework used to manage heterogeneous distributed data center infrastructures. (for hybrid cloud) (for public cloud also)
- It is a standard-based open-source management toolkit that enables virtualized data centers to facilitate cloud deployment at various levels.

88

88

Why should we use OpenNebula?

- Easy to download, install and update through packages
- Fully open-sourced and distributed under an Apache license
- Enables easier running of virtualized data centers for both private and hybrid clouds
- Supports any platform, storage and networking resource
- Open and extensible architecture with the possibility to build customized cloud services

89

89

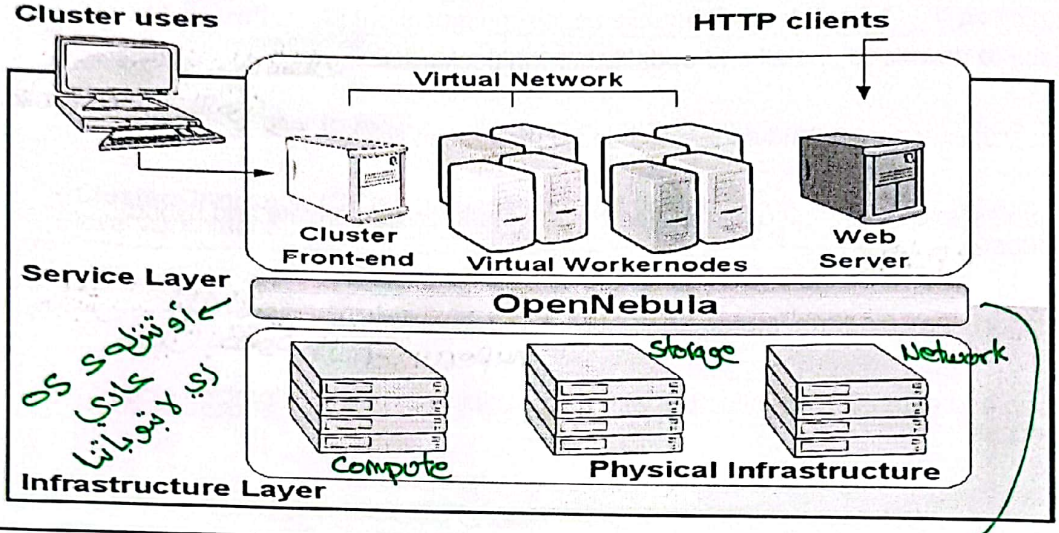
OpenNebula Features

- **Adaptable**: Assimilation abilities to integrate into any infrastructure
- **No lock-in**: Expansive infrastructure and platform independent
- **Light**: Efficient and intuitive
- **Powerful**: Advanced features for virtualization
- **Scalable**: Single instance and multi-tier architectures
- **Be interoperable**: Extensive set of APIs and interfaces
- **Open source**: Apache License v2

90

90

Layers of OpenNebula (1)



91

91

Layers of OpenNebula (2)

- **Data center virtualization management**: This layer is used to manage data center virtualization, consolidate servers, and integrate existing IT assets for computing, storing and networking. In this deployment model, OpenNebula directly integrates with hypervisors (like KVM) and has complete control over virtual and physical resources.

- **Cloud management**: This layer is used to provide a multi-tenant, cloudlike provisioning layer on top of an existing infrastructure management solution.

92

92

أكثرهم انتشارًا

③ OpenStack Cloud Platform

- OpenStack is a free and open-source software platform for IaaS cloud. It provides a modular cloud infrastructure that allows you to deploy the tools of your choice, when you need them, using a single dashboard based on the OpenStack API.
- Basically, it acts like a cloud operating system of a private or public cloud that controls a large pool of computing, storing and networking resources.

or hybrid

93

93

OpenStack Components (1)

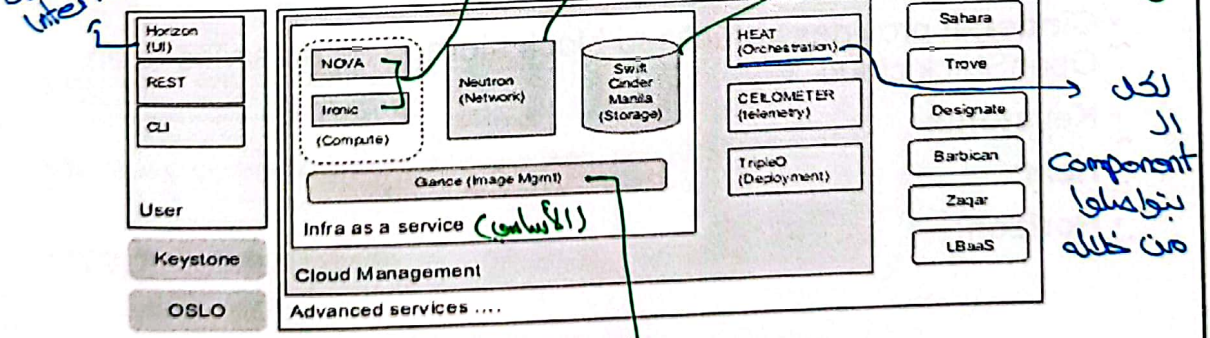
Cloud بالـ Compute Resources Management مسؤولين عن الـ

Network مسؤولة عالـ

مسؤول عالـ Storage

مسؤول عالـ user interface

Cloud management platform (CMP)



لكل الـ Component بتواصلوا من خلاله

Images الـ Manage بتصل وبيفتوا = Glance

94

94

Slides بالـ component المذكورين فقط خركز عالـ

اللي مميزين بالصورة بدون توضيح بالـ Slides

مش مطلوبين.

OpenStack Components (2)

- **Nova**: It is responsible to implement services and associated libraries to provide massively scalable, on-demand, self-service access to compute resources
- **Glance**: It is a service that discovers, registers and retrieves VM images.
- **Zun**: It provides an API to launch and manage containers.
- **Keystone**: It is the authentication and authorization component built into each OpenStack cloud.

95

OpenStack Components (3)

- **Neutron**: It is responsible for creating the virtual networks within an OpenStack cloud
- **Cinder**: It provides virtualized block storage as a service to an OpenStack cloud
- **Keystone**:
- **Heat**:
- **Horizon**:

96

Benefits of OpenStack

- Private clouds
- Public clouds
- Network virtualization
- Network Function Virtualization
- Containers

الفوائد الجديدة

→ OS Virtualization

* ال disadvantages : بتظل متطورة باستمرار ما بتقدر تواكبها + تعلمها صعب
للـ open source platform (continuous development) complex للبعض

④ Nimbus Cloud Computing Platform

- Nimbus is a toolkit that, once installed on a cluster, provides an IaaS cloud to its client
- AWS EC2 and S3 compatible
- Nimbus supports both the hypervisor Xen and KVM
- https://www.nimbus.cloud/

12/2/2020

Protocol هي مو ←
Architecture هي ●
Style

Part-V: Service Oriented Architecture

CPE 0907523 Cloud Computing, Fall 2020

Dr. Samah Rahamneh

Slides adapted from Erl, Mahmood, and Puttini.

كل وحدة ممكن تكون مكتوبة بلغة غير عن غيرها.

Service → sub service, sub " "

زمان كانوا يكتبوا الـ Code الـ Services بـ block واحد وهذا صعب،
هلا صرنا نقسم لـ Modules عشان نسهل على حالنا الـ debug وهكذا.
كل module خاص بنفسه و hidden حتى لو يستفيدوا من بعض.
حتى التعديل بتعدل بس عال module اللي بدك إياه.
*عشان أقدر أقسم لـ Modules لازم يكون عنا Application Programming Interface (API) وسيط بينهم

Service Oriented Architecture

نتائجها: بعمل reuse لـ Service مكتوبة من الأساس عشان ما أرجع اكتبها مرة ثانية فصارت كأنها ليجو بستخدمها لأبني الـ Code.

- A service Oriented architecture (SOA):
  - is a design methodology used to develop software based on interoperable services.

* بنبني Service باستخدام Sub services *

Characteristics of SOA

① • **Refurbished and reusable:** → Applications/Services
  - Services can be reused multiple times for multiple processes.

② • **Loosely coupled:**
  - Services are designed to be independent with minimum dependency on implementation.

③ • **Platform independent:**
  - The base of services in the XML format. → ما بتعتمد ع format معين بس الـ base الها الـ XML

④ • **Based on standards:**
  - The service design is based on WSDL and SOAP standards.

كنا Standard وهذا اشي ممتاز.

* الـ best practice دائمًا إني أقسم الـ Code لـ Modules.

Web Services and SOA

language بستخدموها لعمل Description لأي Service موجودة على الانترنت

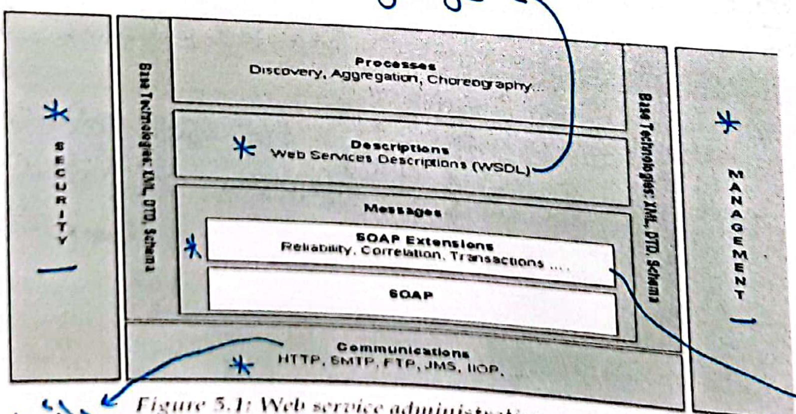
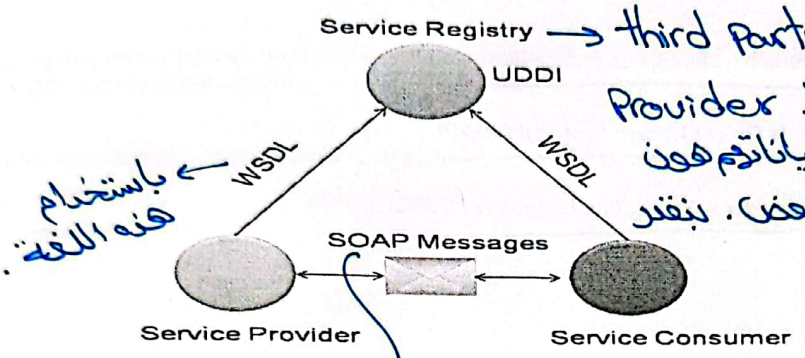


Figure 5.1: Web service administration architecture

دائمًا لازم نستخدمهم

للـ exchange

SOA communication (1)



Service Registry → third Party → لازم الـ Provider والـ Consumer يكونوا مسجلين بياناتهم هون. قبل ما يحكوا مع بعض. بنفتر بعدها بفضل بينهم exchange الـ msg.

باستخدام هذه اللغة.

بستخدم HTTP لوحدها Protocol غير قادرة .Transmition بعمل

5

5

SOA communication (2)

- **Service Provider**: It provides all kinds of service-related operations like service registration, service discovery, exception handling, platform independence, interoperability, and so on.
- **Service Consumer**: It is a human or a system that uses service(s) supported by SOA and which has a valid entry in the service registry.
- **Service Registry**: It is the connection between service providers and service customers. Both the service provider and service consumer needs to register themselves to service registry before starting communication. It is just like an information catalog that allows service providers to discover services.

6

6

SOA components

1. **Extensible Markup Language (XML)**
2. **Simple Object Access Protocol (SOAP)**
3. **Web Services Description Language (WSDL)**

7

SOA مستخدم فيه Protocol

Extensible Markup Language (XML)

- XML features:

1. Device independent and structured way to represent the content.
2. Compatible with different data formats in different applications across multiple platforms.
3. Text-based which makes it natural, easily representable and flexible. → سهل تتعلموا
4. Generic language that underlies a web service. XML namespaces and XML schemas are widely used while creating a web service.

مش مطالبين فيها بس اعرف
- Simple و ايها
- Independent

8

Simple Object Access Protocol (SOAP)

بين msg ال exchange بيعمل Protocol
client ال و remote server

- It is a universally accepted XML based messaging protocol through which a client calls a service remotely.
- SOAP relies on **Hypertext Transfer Protocol (HTTP)** and **Simple Mail Transfer Protocol (SMTP)** for message negotiation and transmission.
- A SOAP message consists of three parts: مميزاتها كتابتي
  - **An envelope**
  - **A Header**
  - **Body**

9

Simple: مميزاتها SOAP message

XML بإستخدم

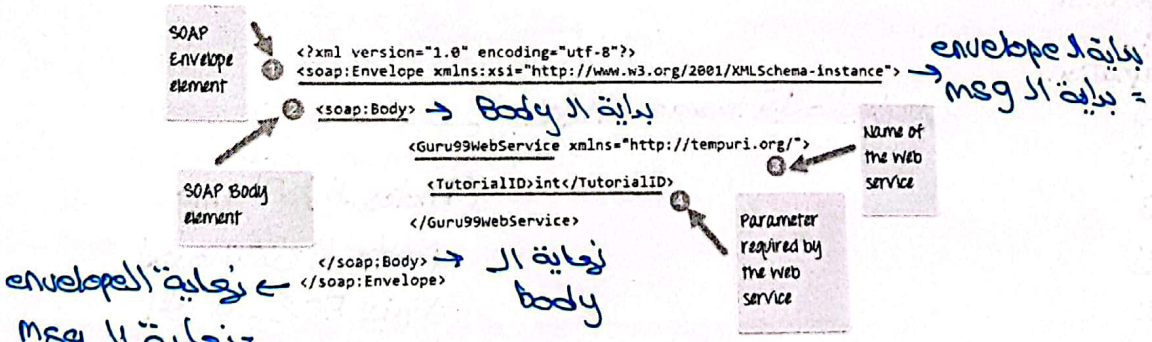


Figure 5.3: SOAP message

10

Web Services are great for Processing Pipelines!

Stages] Processing ال يقسم عملية ال ← .Pipelined ويعملها

Indexing large datasets created by web crawler engines

- **Data mining** - searching large collections of records to locate items of interests → مجموعة كبيرة من ال data نعملها Processing لتاخذ منها المفيد فقط.
- **Image processing**
  - Image conversion, e.g., enlarge an image or create thumbnails
  - Compress or encrypt images
- **Video transcoding** from one video format to another
  - e.g., from AVI to MPEG
- **Document processing.**
  - Convert large collections of documents from one format to another, e.g., from Word to PDF
  - **Encrypt documents**

See examples at – www.highscalability.com

بس افهمي المكتوب.

11

Active-passive → ما يكون فيه load balancer لإنه واحد اللي يكون شغال.

web server بخليك تعمل upload لصورتك وتعملها تحسينات.

Recall: S3 and EC2 Use Case (1)

بتعطيك System وبتقلك اعلى

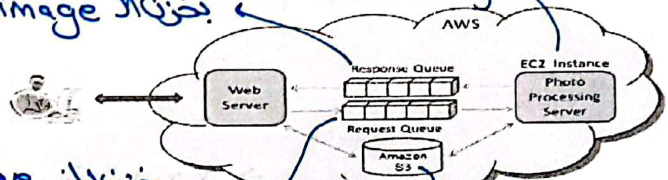
Failure isolation ↑

and • Failure isolation and adaptation

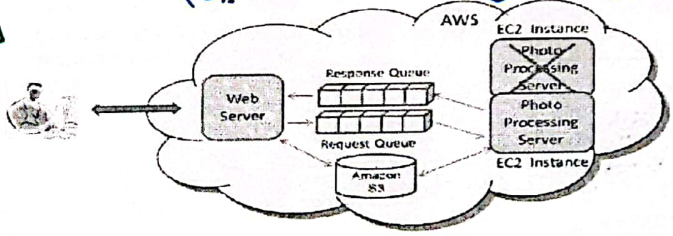
adaptation ↓ بتصيري تحمي نقاط الضعف لتحليلها

Processing ←

بخزن ال image بعد ما يعدل عليها



بخزن ال image قبل ما يعدل عليها



(Photos ال) Storing لحد ما تكمل ال photo اللي بال EC2 بنرجل عليها اللي بعدها.

- Scalability with new EC2 instances to meet heavy load demands

12

1- EC2 → بعملها replica لإنه ممكن يصيرلها fail.

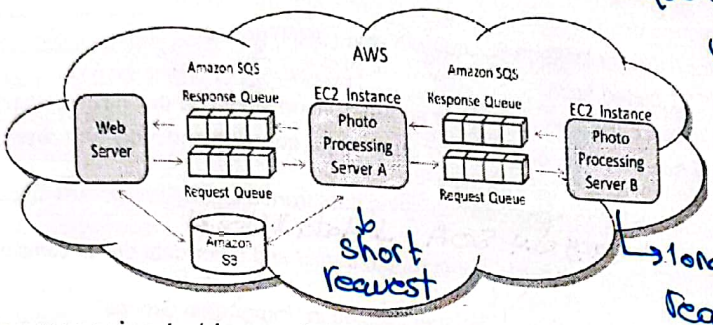
2- queue → ممكن تكون مشكلة لو حجمها صغير

3- S3 → transaction ممكن تكون مشكلة من ناحية الأمان و الحجم و ال

Recall: S3 and EC2 Use Case (2)

Can you think of another use case extension?

requests الـ تقسموا القصيرة يمكان ويمشيوا أول لبعدين الطويلة



Pipeline processing to 'decouple' longer-running operations in a separate, dedicated server

13

13

* بتحبك System وبتقلك كيف أعمل Pipeline .

Representational State Transfer

ولكن أنا أساسا ماكان مطلوب مني اتذكر اشي فلذلك هو أفضل .

+ بأثر هون لإنه ما بيكون مخزنينا اشي. ← الـ fail

الـ Code والـ debug أسهل وأسع

not protocol, it is style to build the Architecture

- * Representational State Transfer (**REST**) ← مستخدم بال web services
- * – Used between clients and "Stateless" servers
  - View a client request as an independent transaction and respond
  - Loose coupling of components: – Used in web app "Mash-ups"
  - E.g., Library locations on a Google Map

client ↔ WS

Stateless ← ما بيخزن أثناء التواصل أي معلومات

- * – Software architecture for distributed hypermedia systems
- * – Platform independent message formats such as JSON; language independent – uses HTTP/HTTPS
- * – Supports data caching, and can be used in the presence of firewalls
- * – Operations are defined in messages

عكسها Stateful

14

14

* ما بيربط باشي معين كنوع flexibility .

* فيها data caching صفية لما يكون في Firewall .

Key Web Service Protocols

1. Universal Description, Discovery, and Integration (**UDDI**)
   - Defines the publication and discovery of web service implementations
   - Suitable for SOAP-based Apps
2. Uniform Resource Identifier (**URI**)
   - String of characters used to identify a web resource; can be Uniform Resource Locator (URL) or Uniform Resource Name (URN) or both
   - Suitable for REST-based Apps
3. The Web Services Description Language (**WSDL**) is an XML-based language that defines Web Services
4. The Lightweight Directory Access Protocol (**LDAP**) is protocol for querying and modifying directory services
5. Extract, Transform, and Load (**ETL**) is a process of moving data from a legacy system and loading it into a SOA application
   - E.g., Informatica ETL tool is popular in insurance, banks and other data driven companies with legacy systems
   - ETL, REST and SOAP technology developers reside in "Integration Groups"

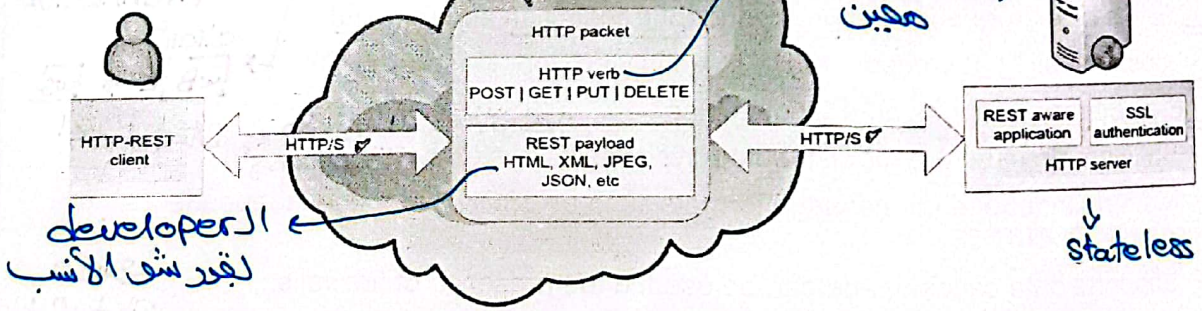
Others: Resource Data Format (**RDF**), Web Ontology Language (**OWL**)

15

15

RESTful Web Services

(Publish-Subscribe Model)



- **REST**: *Representational State Transfer* – minimal information in header, and message body that carries all the needed information (a.k.a. payload)

16

16

Sample REST Request-Response for Creating an S3 Bucket

طبقًا احنا كنا نستخدم API's بسهاد كمثال توضيحي المخطط بالأزرق اللي بتقوليه

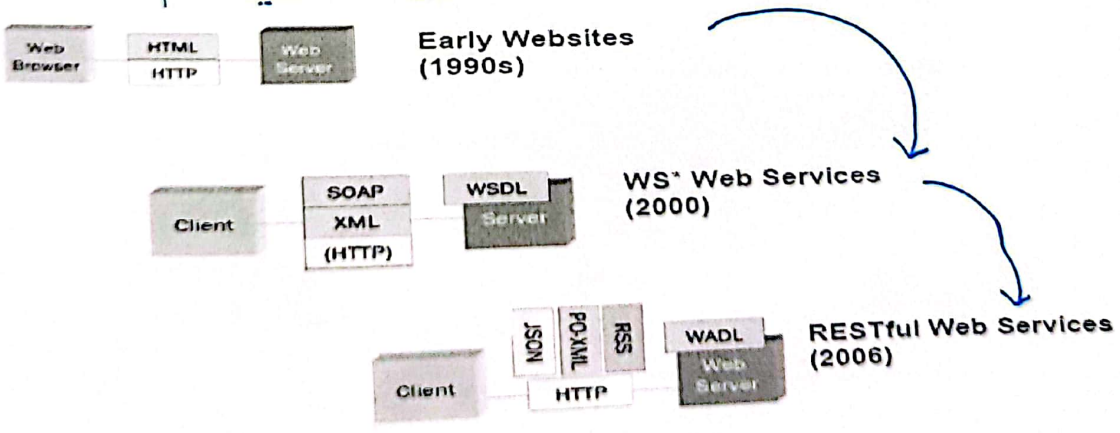
REST Request	REST Response
PUT /[bucket-name] HTTP/1.0	HTTP/1.1 200 OK ← status
Date: Wed, 15 Mar 201- 14:45:15 GMT	x-amz-id-2: VjzdTviQorQtSjcgLshzCZSzN
Authorization:	+7CnewvHA
AWS [aws-access-key-id]:	+6sNxR3VRcUPyO5fmSmo8bWnIS52qa
[header-signature]	x-amz-request-id: 91A8CC60F9FC49E7
Host: s3.amazonaws.com	Date: Wed, 15 Mar 2010 14:45:20 GMT
	Location: /[bucket-name]
	Content-Length: 0
	Connection: keep-alive

17

7

Evolution of Web Services

كان عدد ال Protocols قليلة

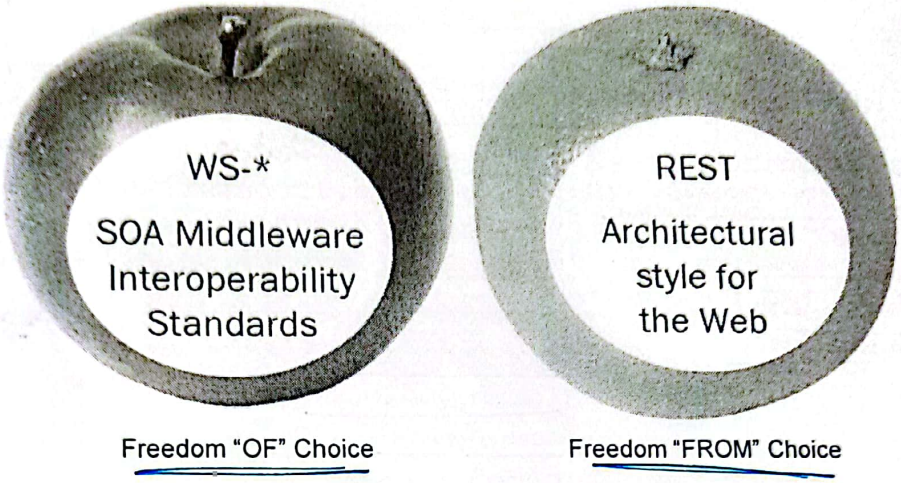


« ومازلنا بتطور مستمر »

18

18

Can we really compare WS-* and REST?



Freedom "OF" Choice

Freedom "FROM" Choice

Reading

- https://aws.amazon.com/blogs/aws/rest_and_soap/
- https://www.nicklitten.com/ibm-i-webservices-rest-vs-soap/