MINES Saint-Étienne | Institut Mines-Télécom

Cloud Architecture

Luis Gustavo Nardin
gnardin@emse.fr

Cloud and Edge Infrastructures

October 22, 2025

Question 1

- What are the advantages of the Public Cloud Computing? (multiple options possible)
  1. Data confidentiality
  2. Outsourcing of the IT department
  3. Cost reduction
  4. Easy access
  5. All the above

Question 1

- What are the advantages of the Public Cloud Computing? (multiple options possible)
  1. Data confidentiality
  2. **Outsourcing of the IT department**
  3. **Cost reduction**
  4. **Easy access**
  5. All the above

Question 2

- Which is NOT a common type of Cloud Computing?
  1. Hardware as a Service
  2. Platform as a Service
  3. Software as a Service
  4. Infrastructure as a Service

Question 2

- Which is NOT a common type of Cloud Computing?
  1. **Hardware as a Service**
  2. Platform as a Service
  3. Software as a Service
  4. Infrastructure as a Service

Question 3

- A Multi-cloud strategy is the same as hybrid cloud.
  1. TRUE
  2. FALSE

Question 3

- A Multi-cloud strategy is the same as hybrid cloud.
  1. TRUE
  2. **FALSE**

Question 4

- What is the main business advantage of Cloud Computing?
  1. Reduce OPEX
  2. Move expenses from OPEX to CAPEX
  3. Reduce management cost
  4. Move expenses from CAPEX to OPEX

Question 4

- What is the main business advantage of Cloud Computing?
  1. Reduce OPEX
  2. Move expenses from OPEX to CAPEX
  3. Reduce management cost
  4. **Move expenses from CAPEX to OPEX**

Question 5

- What is the major concern about the Public Cloud Computing?
  1. High cost
  2. Confidentiality
  3. Too many platforms
  4. Accessibility

Question 5

- What is the major concern about the Public Cloud Computing?
  1. High cost
  2. **Confidentiality**
  3. Too many platforms
  4. Accessibility

Question 6

- What is a disadvantage of the Public Cloud Computing?
  1. Limited offer
  2. Dependence on suppliers
  3. Management cost
  4. The price of subscriptions

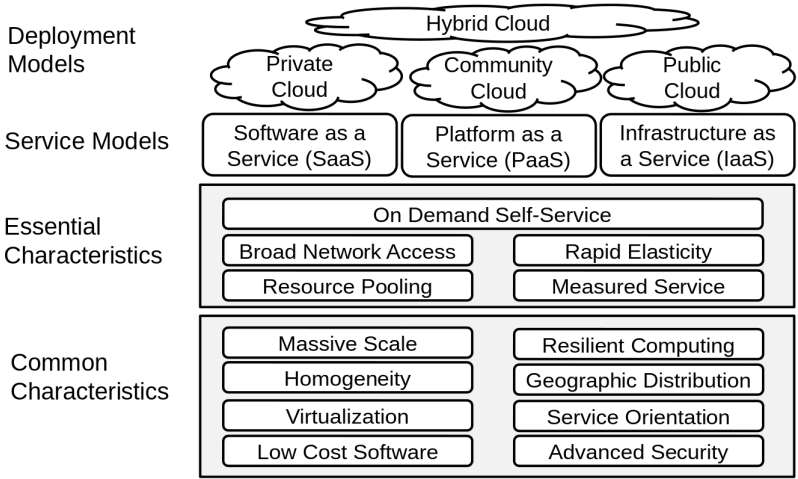
Question 6

- What is a disadvantage of the Public Cloud Computing?
  1. Limited offer
  2. **Dependence on suppliers**
  3. Management cost
  4. The price of subscriptions

Outline

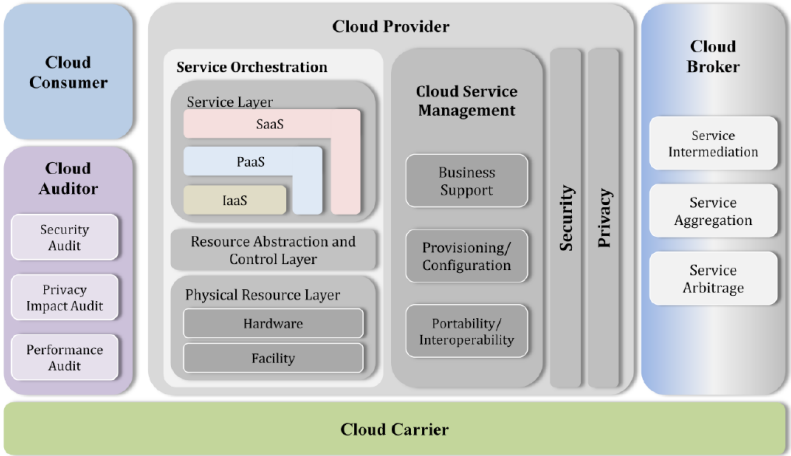
Reference Architecture

NIST Cloud Definition Framework



(National Institute of Standards and Technology [NIST], 2011)

NIST Conceptual Reference Model



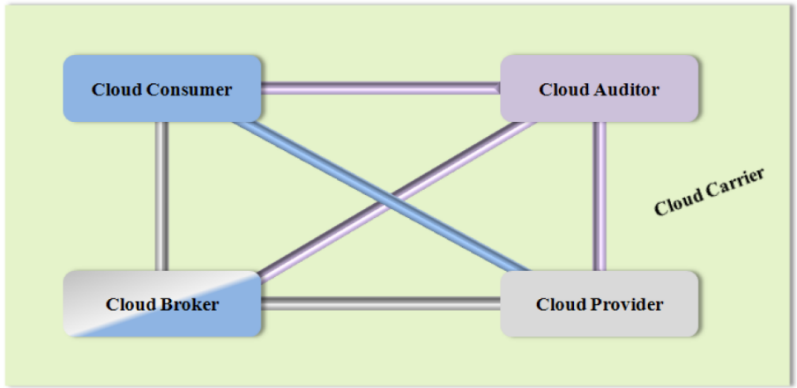
(National Institute of Standards and Technology [NIST], 2011b)

Actors

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*

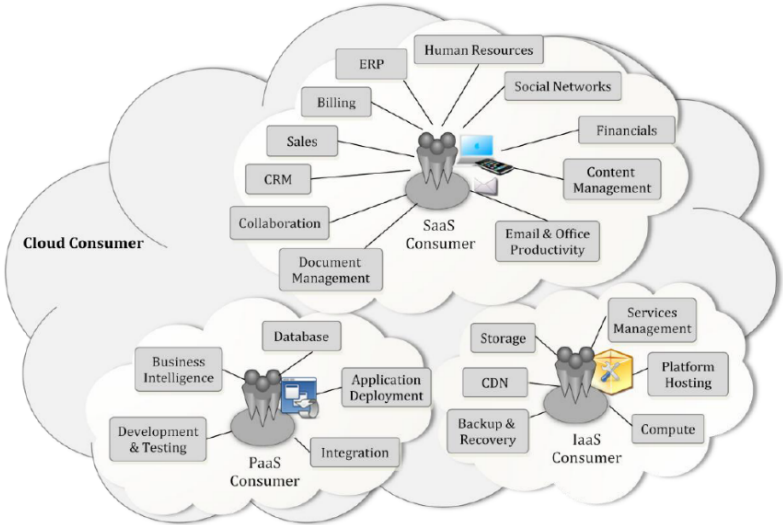
(National Institute of Standards and Technology [NIST], 2011b)

Interaction between Actors



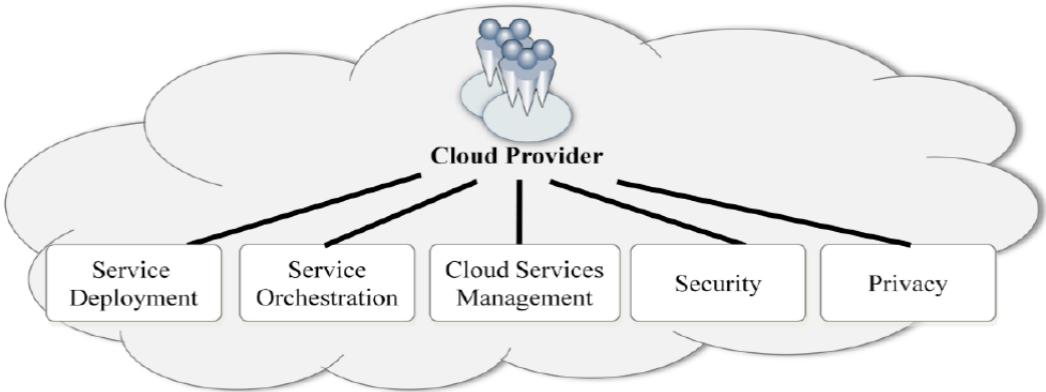
(National Institute of Standards and Technology [NIST], 2011b)

Cloud Consumer



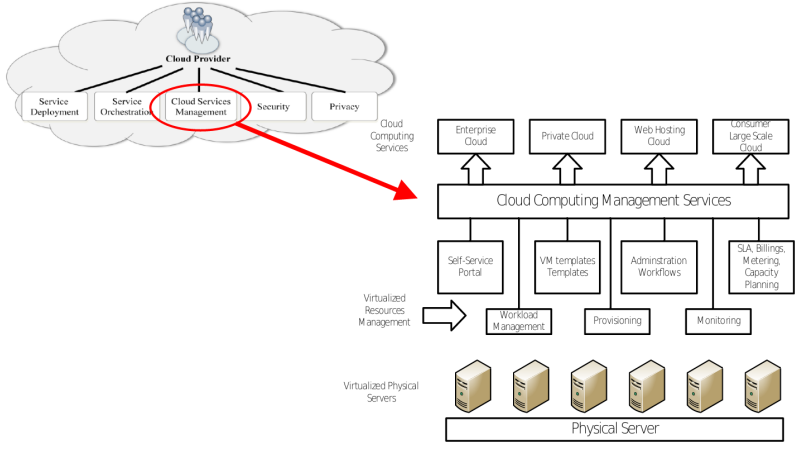
(National Institute of Standards and Technology [NIST], 2011b)

Cloud Provider



(National Institute of Standards and Technology [NIST], 2011b)

Cloud Provider



(National Institute of Standards and Technology [NIST], 2011b)

Cloud Auditor

- Perform an independent examination of Cloud service controls to verify conformance to standards, laws, and regulations

Aspect	Description
Security Controls	Assess the extent to which controls are **implemented correctly**, **operating as intended**, and **producing the desired outcome** with respect to the security requirements
Privacy Impacts	Assess the compliance with applicable privacy laws and regulations governing an individual's privacy, and ensure **confidentiality**, **integrity**, and **availability** of an individual's personal data
Performance	Assess the fulfillment of Service Level Agreements (SLAs) that specify performance requirements like quality of service and remedies for performance failures

(National Institute of Standards and Technology [NIST], 2011b)

Cloud Broker

- Entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers

Aspect	Description
Service Intermediation	A cloud broker enhances a given service by **improving** some specific **capability** and **providing value-added** services to cloud consumers
Service Aggregation	A cloud broker **combines and integrates multiple services** into one or more new services
Service Arbitrage	Similar to service aggregation except that the services being aggregated are not fixed, the broker has the **flexibility to choose services from multiple agencies**

(National Institute of Standards and Technology [NIST], 2011b)

Cloud Carrier

- Provide connectivity and transport of cloud services between Cloud Consumers and Cloud Providers

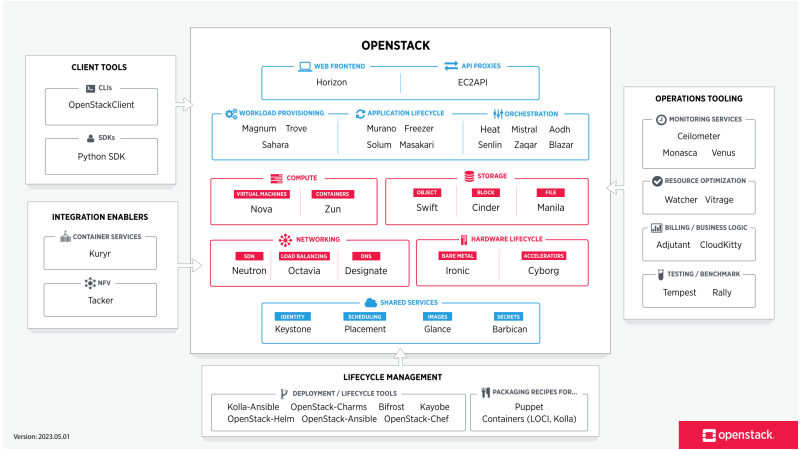
(National Institute of Standards and Technology [NIST], 2011b)

OpenStack Architecture

OpenStack

- **Cloud operating system** that controls large pools of compute, storage, and networking resources throughout a data center, all managed and provisioned through APIs with common authentication mechanisms
- Originated from a joint program between Rackspace & NASA in 2010
  - Written in Python
  - Open Source (Apache License 2.0)
  - Cross-platform
- OpenStack has a **modular architecture**

OpenStack Services



Source: https://www.openstack.org/software

Horizon – Dashboard Service

https://docs.openstack.org/horizon/

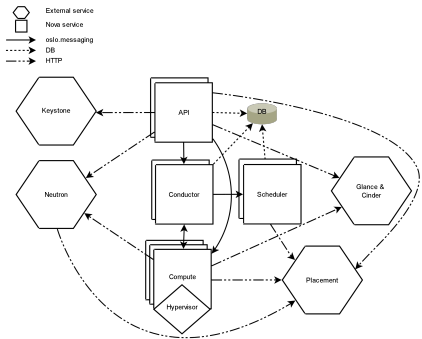
- Web-based user interface to OpenStack service

Characteristics	Description
Core Support	Support for all core OpenStack projects
Extensible	Anyone can add a new component
Manageable	The core codebase is simple and easy-to-navigate
Consistent	Visual and interaction paradigms are maintained throughout
Stable	A reliable API with an emphasis on backwards-compatibility
Usable	Providing an attractive and visual appealing interface that people want to use

Nova – Compute Service

https://docs.openstack.org/nova/

- Manage and automate the provisioning of a pools of computer instances (e.g., KVM, VMware, Xen, Hyper-V)
- Designed to scale horizontally



- **DB**: SQL database for data storage
- **API**: component that receives and converts HTTP requests to communicate with other components
- **Scheduler**: decides which host gets each instance
- **Compute**: manages communication with hypervisor and virtual machines
- **Conductor**: handles requests that need coordination (build/resize), acts as a database proxy, or handles object conversions
- **Placement**: tracks resource provider inventories and usages

Glance – Image Service

https://docs.openstack.org/glance/

- Provide discovery, registration, and delivery services of virtual machine (VM) images
- Host a *metadef* catalog allowing to programmatically determine various metadata key names and valid values applied to resources
- Provide a standard REST interface for querying information about images letting clients to stream images to new servers

Swift – Object Store Service

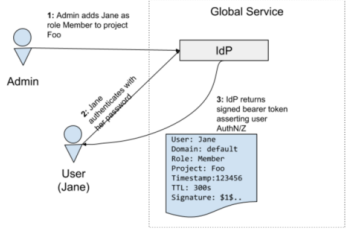
https://docs.openstack.org/swift/

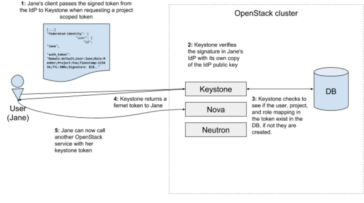
- Highly available, distributed, eventually consistent object/blob store
- Scalable and optimized for durability, availability, and concurrency
- Ideal for storing unstructured data
- Responsible for ensuring data replication and integrity
- Scale horizontally simply by adding new servers

Keystone – Identity Service

https://docs.openstack.org/keystone/

- Common authentication system across services
- Provide API client authentication, service directory, and distributed multi-tenant authorization
- Specifies the service access by each user
- Integrate with existing directory services like LDAP





Source: https://wiki.openstack.org/wiki/Keystone_edge_architectures

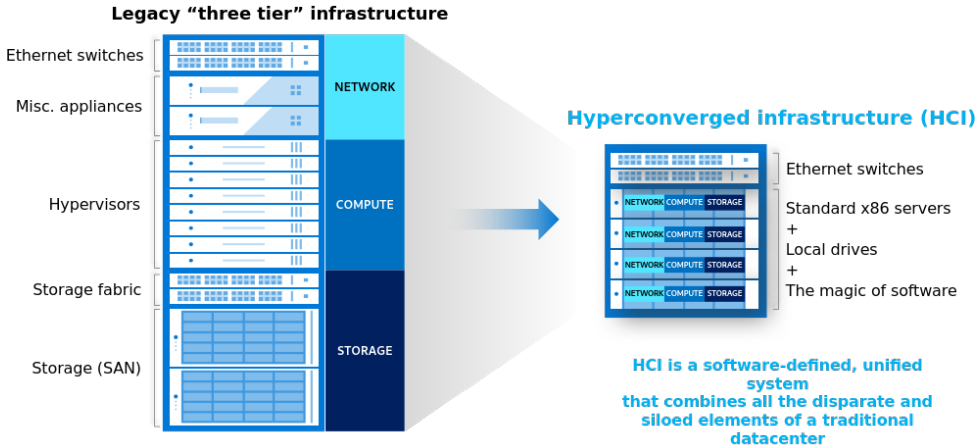
Neutron – Networking Service

https://docs.openstack.org/neutron/

- Manage all networking facets for the Virtual Networking
- Infrastructure (VNI) and the access layer aspects of the Physical Networking Infrastructure (PNI) in the OpenStack environment
- Provide networks, subnets, and routers as object abstractions
- Allow Static IP, DHCP or Floating IP addresses
- Gives users self-service ability over network configurations (i.e., users can create their own networks, control traffic, and connect servers and devices to one or more networks)
- Can deploy additional services like Intrusion Detection Systems (IDS), Load Balancing, Firewalls, and Virtual Private Networks (VPN)

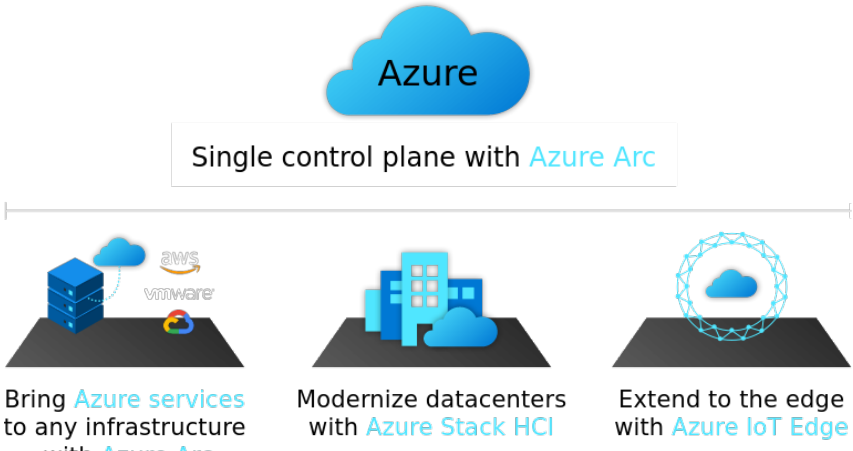
Azure Stack HCI

What is Hyper Converged Infrastructure (HCI)



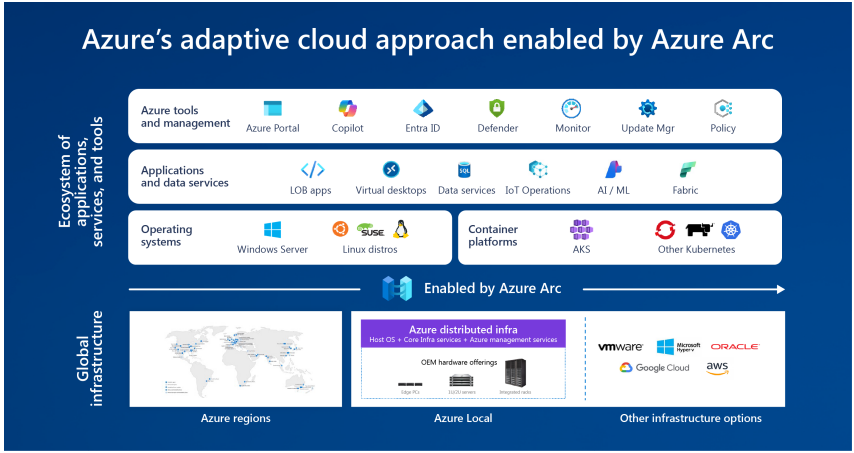
Source: https://github.com/abekifle/STACK-HCI/

Overview



Source: https://github.com/abekifle/STACK-HCI/

Ecosystem



Source: https://go.microsoft.com/fwlink/?linkid=2296064&clcid=0x409

Features

Azure Stack HCI (or Azure Local) designed to enhance operational efficiency, security, and scalability for diverse IT environments. Key functionalities include:

Cloud-based operations Use Azure tools and APIs for consistent infrastructure provisioning and lifecycle operations across distributed locations.

Multi-node clustering Increase resilience and uptime with high availability and robust software-defined storage.

Central management and visibility Monitor, update, and secure Azure Local infrastructure directly from the Azure portal using familiar Azure services.

Cloud-based virtual machine (VM) management Extend cloud practices with VM extensions, Azure Marketplace images, templates, and RBAC.

Disconnected operations Meet the strictest data residency regulations with a locally hosted control plane that works fully disconnected.

Components

Azure Arc **cloud governance and management** by delivering a consistent multicloud and on-premises management platform.

Azure machines enable the **management** of Windows and Linux **physical servers and virtual machines hosted outside** of Azure.

Azure Arc VM enable **provisioning and management** of Windows and Linux **VMs hosted in an on-premises** Azure Local environment.

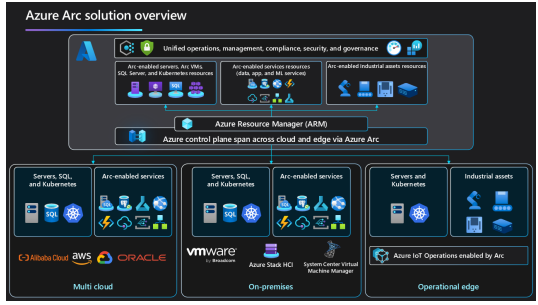
Azure AKS enable the **creation and management** of Kubernetes clusters

Source: https://learn.microsoft.com/en-us/azure/azure-local/hybrid-capabilities-with-azure-services-23h2

Azure Arc

Azure Arc provides a centralized, unified way to:

- Manage the entire cloud environment (non-Azure and on-premises)
- Manage virtual machines, Kubernetes clusters, and databases
- Use Azure services and management capabilities
- Configure custom locations as an abstraction layer on top of Kubernetes clusters and cluster extensions



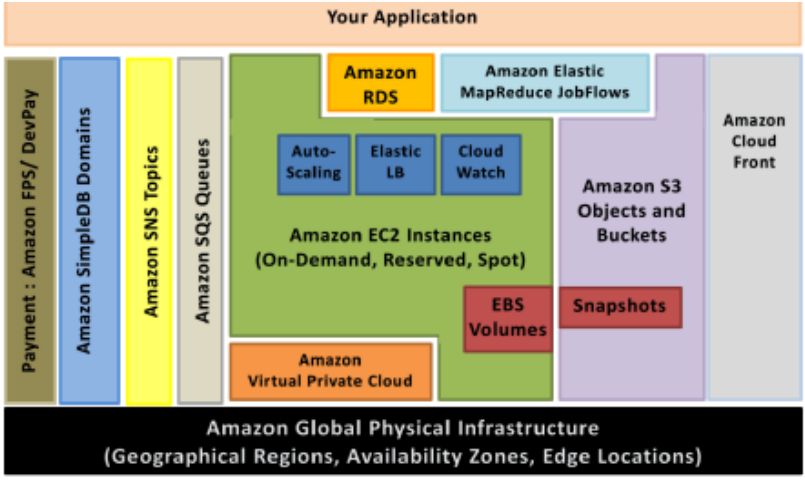
Source: https://learn.microsoft.com/en-us/azure/azure-arc/overview

AWS Architecture

AWS

- Amazon Web Services (AWS) provides on-demand cloud computing platforms and APIs on a metered pay-as-you-go basis
- AWS was launched in the early 2000's to provide services to Amazon's third-party retailers in the Merchant.com
- AWS has a worldwide presence that spans over 120 Availability Zones within 38 geographical regions (https://aws.amazon.com/about-aws/global-infrastructure/regions_az/)

AWS Architecture



(Hwang, 2017)

AWS Cloud Services

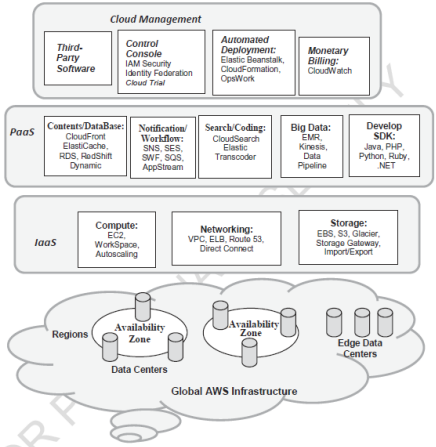


Figure 4.14
The AWS public cloud consisting of the top management layer, PaaS, and IaaS platforms, and the global infrastructure built over data centers in availability zones located in various regions.

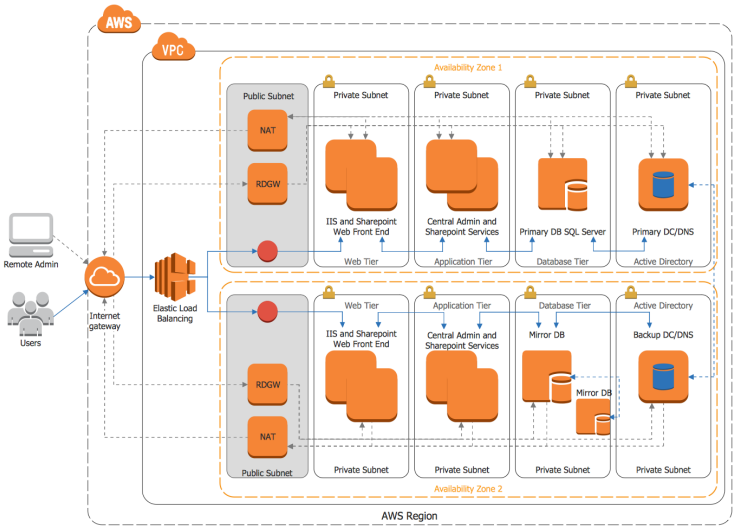
(Hwang, 2017)

AWS Cloud Services

Category	Offering	Service Modules or Short Description
Compute	EC2	Virtual Servers in the AWS Cloud
	Lambda	Run Code in Response to Events
	EC2 Container Service	Run and Manage Docker Containers
Storage & Content Delivery	S3	Scalable Storage in the AWS Cloud
	Elastic File System	Fully Management File System for EC2 (Preview)
	Storage Gateway	Integrate On-Premises IT Facilities with Cloud Storage
	Glacier	Archive Storage in the Cloud
	CloudFront	Global Content Delivery Network
Database	RDS	MySQL, Postgres, Oracle, SQL Server, and Amazon
	DynamicDB	Predictable and Scalable NoSQL Data Store
	ElastiCache	In-Memory Cache
	Redshift	Managed Petabyte-Scale Warehouse Service
Networking	VPC	Virtual Private Cloud as Isolated Cloud Resources
	Direct Connect	Dedicated Network Connection to AWS
	Route S3	Scalable DNS and Domain Name Registration

(Hwang, 2017)

AWS Architecture Example



Source: https://www.conceptdraw.com/examples/sharepoint-application-architecture-diagram1

Elastic Cloud Computing (EC2)

- Core component of Amazon Web Services
- Allow to rent virtual computers to run applications
  - very similar in functionality to dedicated physical servers
  - more cost efficient
  - can be created in minutes
- Complete administrative control over the virtual server
- Allow choosing the operating system (multiple Linux distributions, macOS, or Microsoft Windows Server)
- Multiple built-in security features
  - Instances run in virtual private cloud (VPC), a logically isolated network
  - EC2 has security groups acting like virtual firewalls to control traffic

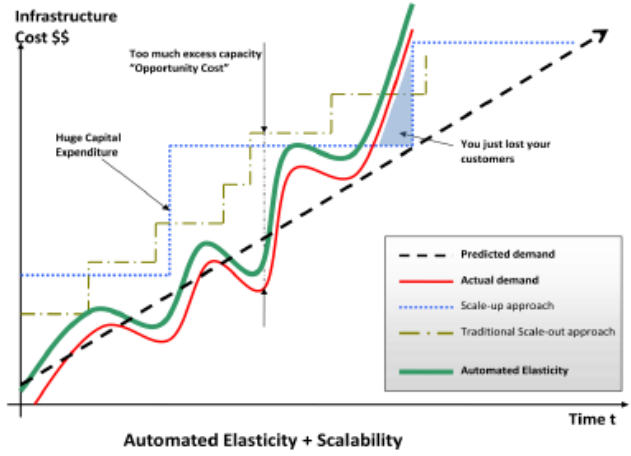
Based on slides of Charlotte Laclau – Télécom Saint-Étienne

EC2 Auto Scaling

- Allow the **scaling** of Amazon EC2 **capacity up or down** automatically according to conditions predefined
- Ensure that the number of Amazon EC2 instances used **increases seamlessly during demand spikes** to maintain performance and **decreases automatically** during demand lulls to **minimize costs**
- Particularly well suited for applications that experience hourly, daily, or weekly **variability in usage**
- Enabled by Amazon CloudWatch and available at no additional charge beyond Amazon CloudWatch fees

(Hwang, 2017)

EC2 Auto Scale



(Hwang, 2017)

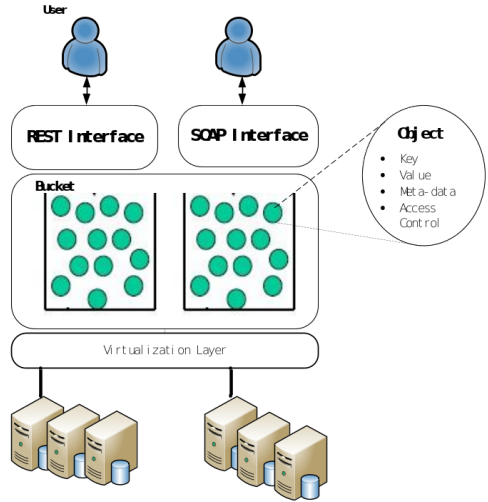
Amazon Simple Storage Service (S3)

- Provides developers and IT teams with secure **object storage**
- Easy to use with its simple web service interface
- Store and retrieve **any amount of data** at any time from Amazon EC2 or from anywhere on the web
- **Automatically making copies** of your object on multiple devices across multiple facilities
- Only pay for the storage actually used. **No minimum fee and no setup cost**
- Securely upload and download data with SSL encrypted points and provide multiple options for encrypting stored data

Based on slides of Charlotte Laclau – Télécom Saint-Étienne

Amazon Simple Storage Service (S3)

- Object is the basic unit of data
- Bucket for storing objects
- Key for data object retrieval
- Object is attributed to value, metadata and access control



Amazon Simple Storage Service (S3)

- Write, read, and delete objects containing from 1 byte to 5TB of data each. The number of objects you can store is unlimited
- Each object is stored in a bucket and retrieved via a unique, developer-assigned key
- A bucket can be stored in one of several Regions. You can choose a Region to optimize for latency, minimize costs, or address regulatory requirements
- Objects stored in a Region never leave the Region unless you transfer them out. For example, objects stored in the EU (France) Region never leave the EU

Identity and Access Management (IAM)

- Control access to AWS resources
  - **Authentication**: control who can use the AWS resources
  - **Authorization**: control what resources they can use and in which ways
- Each IAM user has a unique identity recognized by AWS services and applications
- Each IAM user has a unique name and can identify itself using familiar security credentials such as a password or access key
- Possible to permit a user to access any or all of the AWS services that have been integrated with IAM

Based on slides of Charlotte Laclau – Télécom Saint-Étienne

Amazon Simple Queue Services (SQS)

- Fast, reliable, scalable, fully managed queueing service
- Enable a simple and cost-effective form to decouple the components of cloud applications
- Used to transmit any volume of data, at any level of throughput, without losing messages
- Can be used with other AWS Services to make distributed applications more scalable and reliable

Amazon Simple Queue Services (SQS)

- **Work queues**: Decouple components of a distributed application that may not process all the same amount of work simultaneously
- **Buffer and batch operations**: Add scalability and reliability to the system architecture, and smooth out temporary volume spikes without losing messages or increasing latency
- **Request offloading**: Move slow operations off of interactive request paths by enqueuing the request

Amazon Simple Notification Service (SNS)

- Amazon Simple Notification Service (Amazon SNS) is a managed service that provides **message delivery from publishers to subscribers**
- Publishers communicate asynchronously with subscribers by sending messages to a **topic**, which is a logical access point and communication channel

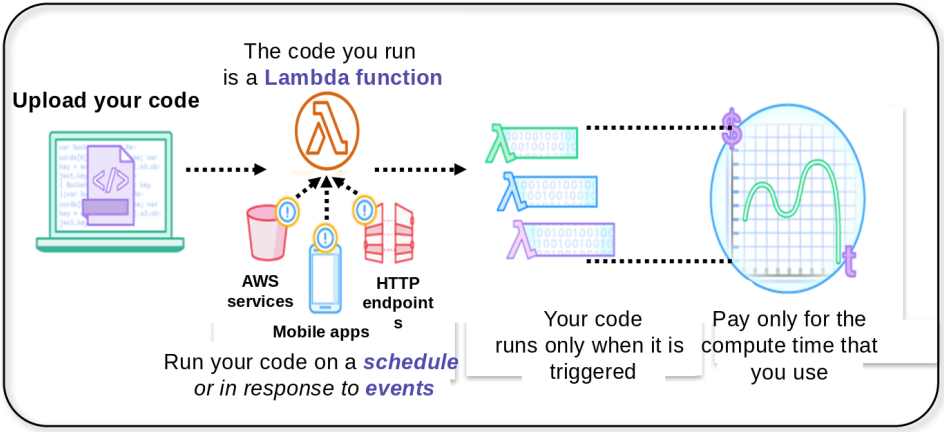
Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (SNS)

- Application-to-application messaging (interact other services)
- Application-to-person notifications (email, mobile)
- Standard and FIFO topics (different ordering)
- Message durability (separate locations)
- Message archiving and analytics (archive service)
- Message attributes (metadata)
- Message filtering (filtering policy)
- Message security (encryption)

AWS Lambda

- AWS Lambda is a serverless compute service



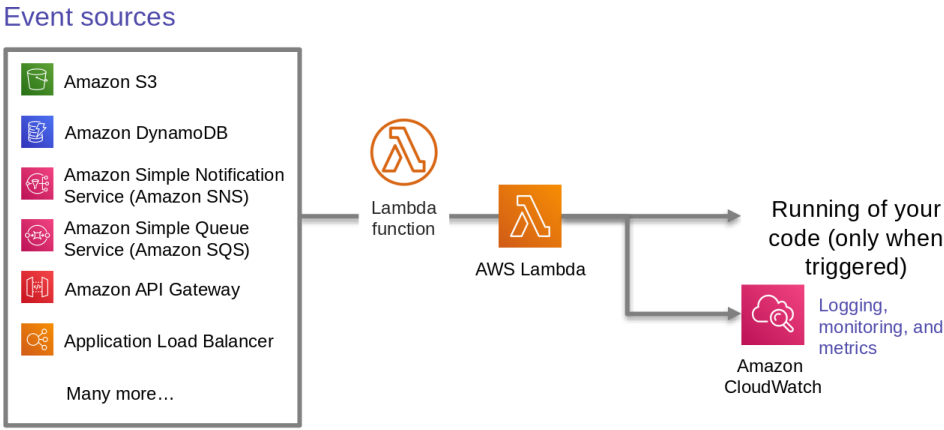
AWS Lambda

AWS Lambda

- It supports multiple programming languages
- Completely automated administration
- Built-in fault tolerance
- It supports the orchestration of multiple functions
- Pay-per-use pricing

Based on slides of AWS Academy Cloud Foundations

AWS Lambda



Based on slides of AWS Academy Cloud Foundations

Magic Quadrant for Distributed Hybrid Infrastructure

Magic Quadrant for Distributed Hybrid Infrastructure

Source: https://www.gartner.com/doc/reprints?id=1-2J0K7ZG4&ct=241007&st=sb

European Industrial Alliances

European Industrial Alliances

- **European Alliance for Industrial Data, Edge and Cloud** aims to foster the development and deployment of next generation edge and cloud technologies (https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance)
  - European Industrial Technology Roadmap for the Next-Generation Cloud-Edge (2023) identify areas of investment for the joint development and deployment of the next generation of European cloud and edge technologies (https://ec.europa.eu/newsroom/dae/redirection/document/102590)
- **European Cloud Industrial Alliance (EUCLIDIA)** is an industry alliance made up of SMEs active in the cloud industry (https://www.euclidia.eu)

References

- Hwang, K. (2017). Cloud Computing for Machine Learning and Cognitive Applications. Cambridge, MA: The MIT Press.
- National Institute of Standards and Technology (2011a). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-145). [https://csrc.nist.gov/publications/sp#800-145]
- National Institute of Standards and Technology (2011b). NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology (NIST Special Publication 500-292). [https://www.nist.gov/publications/nist-cloud-computing-reference-architecture]