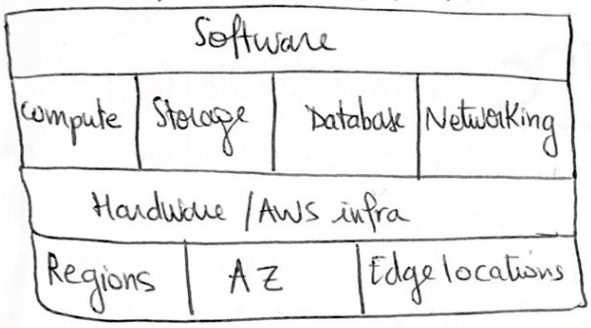
بسم الله الرحمن الرحيم

Cloud

I) AWS security:

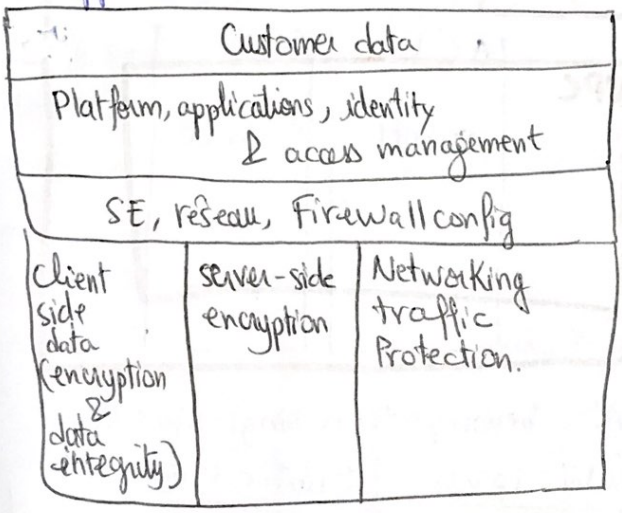
① AWS Shared Responsibility Model:

* AWS est responsable de la sécurité du cloud : tout ce qui est en rapport avec l'implémentation physique.



* Customer est responsable de la sécurité dans le cloud.

Il utilise les tools d'AWS pour sécuriser ses applications et ses données.



AWS

* Sécurité physique des datacenters
* Hardware and software infrastructure
* Network infrastructure
* Virtualization infrastructure
  [isolation des instances

Platform as a service (PAAS)

Infra managed by AWS, it is hidden from view of customer.

Amazon RDS | Amazon Lambda | Amazon Elastic Beanstalk

Customer

Responsable des apps qu'il déploie sur AWS.

* EC2 instance operating system
* Applications
  ↳ passwords, role based access ...
* Security groups config

...

Infrastructure as a service (IAAS)

Amazon EC2 | Amazon EBS | Amazon VPC

↳ Customer maintains control and management of most of the sys.

Software as a service (SAAS)

* Software is centered hosted
* Customers need to manage infra
* services accessed via web, app ...

AWS trusted advisor | AWS Shield | Amazon chime.

② AWS IAM:

(identity and access Management)

↳ définir les utilisateurs et leurs types d'accès [free services]

↳ service global

IAM group: collection of IAM users

↳ grant same permission to multi users.

* IAM role: IAM identity with specific permission.
  * not uniquely associated with one person.
  * provides temporary security credentials.

③ Securing new AWS account:

* At first, you begin with a single identity that has complete access to all AWS services [AWS root account]

④ Securing data on AWS:

AWS KMS (Key manag. secret)

↳ to manage secret keys.

① Encryption of data at rest (data physically stored and not moving)

using open standard advanced encryption

② Encryption of data in transit

↳ use TLS

↳ use AWS certificate manager (to manage the deployment of TLS certificates)

↳ secure http (https)

→ when creating IAM policy: you can grant AWS Manag. consol access / programmatic access to user.

Root user: change AWS support plan

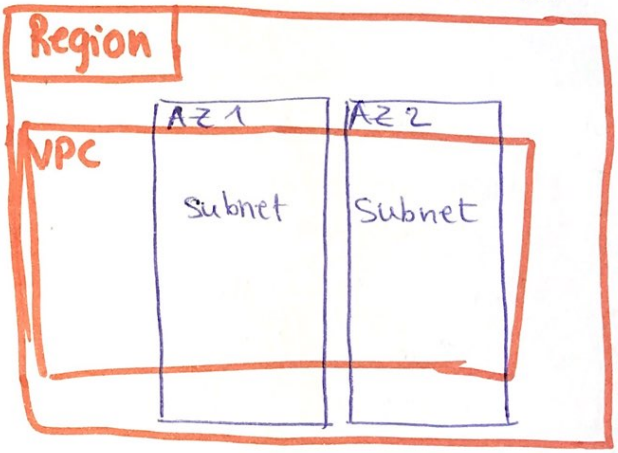
II) Network and content delivery:

Router — subnet

VPC Virtual Private Cloud

↳ provisionner une section logiquement isolée du AWS cloud où on peut launcher AWS ressources dans un réseau qu'on définie.

* Pour limiter l'accès:
  - Security groups
  - Network access control List.



VPC : belongs to a single AWS Region

Public ipv4	Elastic ip@
- Assignée manually through Elastic ip@	- associée avec compte AWS
- assignée auto through auto assign public ip at subnet	- can be allocated ~~at~~ anytime $

Route table

contient un ensemble de règles ou routes pour configurer pour diriger le traffic réseau des subnets.

* Un subnet ne peut être associé qu'à une seule route table.
* On peut associer plusieurs subnets à une seule route table.

↳ one to one mapping

VPC networking options:

* Internet gateway:

VPC component: scalable, hautement disponible qui permet la comm. entre instances dans le VPC et l'internet publique.

1) provides a target in your VPC route tables for internet traffic.
2) Perform network @ translation for instances.

* To make a subnet public: you attach an Internet gateway to your VPC and add a route entry to the route table associated with the subnet.

* NAT Gateway:

enables instances in private subnets to connect to the internet or other AWS services.

↳ It prevents the public internet from initiating a conn with those instances.

VPC endpoint:

a virtual device that enables you to privately connect your VPC to these supported AWS services.

Sécurité du VPC:

- Security groups
- Network access control lists

1) Security groups act at the instance level
2) Network ACLs act at the subnet level.

Network ACL ⟷ subnet
one to one relationship

NACL: stateless: no info about a request is maintained after a request is processed.

SG	Network ACLs
Instance level	subnet level
Allow rules only	Allow + deny rules
stateful	stateless
All rules are evaluated before decision to allow traffic	Rules are evaluated in number order before decision.

DNS: the process of translating an internal name to the corresponding ip @.

D N S
domain name system

Amazon Route 53

Gives you the ability to register to register a domain name and have the service handle the names & and hosts related to that domain.

Amazon Route 53 DNS failover
↳ configures a backup and failover scenarios for your app.

Cloud Front

A fast content delivery service that securely delivers data to customers at high transfer speeds.
↳ Relies on Route 53's geolocation Routing
(A customer makes a request
⇓
Route 53 finds out where the customer is located and responds with the IP @ of the edge location closest to that customer)

Amazon EC2

Elastic Compute Cloud

↳ provides virtual machines where you can host the same apps.

① Amazon Image (AMI)
Machine
a template that is used to create EC2 instance. [linux, windows]

② Attaches an IAM Role to EC2 instance

③ Storage

* Amazon EBS: durable, block level storage volumes.
* Amazon EC2 Instance Storage: located on hard disks physically attached to the host computer
↳ Instance stops ⇒ data stored deleted.

④ Tags: a label that you assign to an AWS resource.
(Key, value) by ~~not~~ purpose, owner or environment.

Container services

Containers = a method of operating system virtualization.

Your container

your app
dependencies
configs
Hooks into Os

A large EC2 instance can run hundreds of containers

Amazon elastic container Service
Scalable, fast container manage. service. (ECS)

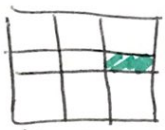
Serverless : AWS Lambda deployment

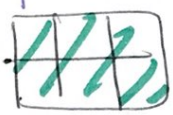
* enables devs to easily deploy and manage app in cloud : Elastic Beanstalk

Storage

① EBS : Elastic Block Store

Provides persistent block storage volumes for use with EC2 instances.
↳ Retains data after power off.
(Non volatile storage)
* Automatically replicated within its AZ.
Hautement dispo et durable.


block storage


object storage

If I want to change small thing
↑ change one block that contains the character
↑ Entire file updated

Snapshot: backup of an EBS volume.
* the first snapshot: Baseline snapshot
Any other snapshot only capture what's different from the previous one.

Uses:
- boot volume
- Storage for EC2 instance
- DB hosts
- Data that require frequent updates (system drive for instance)
- requires encryption solution

② EFS : Elastic file system

Implement storage for EC2 instances that multiple VMs can access at the same time.
↳ A shared file system that uses the Network file system.

Use:
- build file system for big data and analytics
- Petabyte-scale
- Shared storage

③ S3 : Simple storage Service

Object level storage
↳ stores data as objects in resources that are called buckets.

* Virtually unlimited storage [single object 5TB]
* Designed for 11 9s of durability.
* bucket names need to be unique around the world.
* Data not associated with one server.
* Access Control : AWS identity, Access Management policies, Amazon S3 bucket policies, per object access control lists
* encrypt data in transit / rest by enabling server side encryption.
* Bucket associated with Region.

* Includes event notifs

Amazon S3 storage classes

① Amazon S3 standard (3AZ)
highly available, durable, performant [frequently accessed data]
↳ content distribution / big data analytics

② Amazon S3 standard infrequent Access storage : (IA) (3AZ)
- data accessed less frequently
- Requires rapid access when needed
- low per GB storage price and per GB retrieval fee.
↳ long term storage and backups

③ Amazon S3 One zone-Infrequent Access (IA)
- Stores data in 1 AZ
- less cost
- data less freq., require rapid access when needed.
↳ secondary backup copies, easy to recreate data.

④ Amazon S3 Intelligent-Tiering Storage:
- optimize costs by automatically moving data to the most cost-effective access tier.
* Moves objets not accessed for 30 consecutive days To the infrequent access tier
If an objet in IA is accessed, it is moved back to the standard access tier.
↳ long lived data with access patterns that are unknown or unpredictable.

⑤ S3 Glacier
- Secure, durable, low cost
- For data archiving
↳ 3 Retrieval options:
* upload objects directly to S3 glacier
* Use Amazon S3 life cycle policies to transfer data between S3 storage.

⑥ S3 Glacier Deep Archive:
- lowest cost class storage
- Support long term retention, digital preservation for data that might be accessed once or twice a year.
↳ backup, disaster recovery use cases
Financial services, healthcare.
- 11 9's durability
- All data is replicated and stored in at least 3 A
- Can be restored within 12 hours.

* S3 URL styles

① Bucket path style URL

https://s3.ap-north.azom/bucket-name

ap-north: region; bucket-name: BK name

↳ to access objects

② Bucket virtual-hosted-style URL

https://bucket-name.s3-ap-nort.....

bucket-name: BK name; ap-nort.....: Region.

↳ bucket as a website for static data.

☆ Standard storage:
- 11 9s of durability
- 4 9s of availability

☆ Standard-infrequent Access
- 11 9s of durability
- 3 9s of availability.

Amazon S3 glacier

Archive: any object you store in

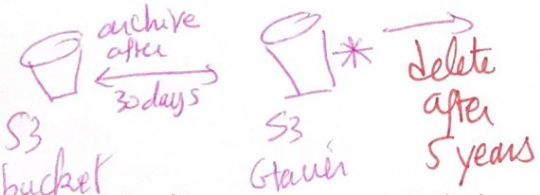
Vault: container for storing archives.

Retrieval options:

① Expedited: 1-5 minutes (highest cost)

② Standard: 3-5 hours

③ Bulk: 5-12 hours



☆ Default encryption for data.

Databases

RDS: Relational database Service

EC2: unmanaged solution

* Sets up, operates and scale relational databases without any on going administration.

Database instance: an isolated DB environment that contains databases.

☆ the basic functionality of RDS is the same with or without VPC.

* Multi AZ deployment:

RDS auto generates a standby copy of the DB instance in another AZ in the same VPC.

☆ If main DB instance fails

⇒ RDS auto makes the standby DB the main instance.

* Read Replicas. | * complex transactions

Dynamo DB: non relational databases

* items can have ≠ attributes
* Unlimited storage
* data stored in solid state drives

☆ to find an item using an attribute other than the item's PK: Scan

* very fast and performing

Amazon Redshift

Analysing data: SQL + BI

Aurora: Postgre / MySQL

AWS well-architected framework

Operational excellence | Security | Reliability

Performance efficiency | cost optimization

Elastic Load Balancing

↳ A service that distributes incoming application or network traffic across multiple targets.

① Application Load balancer
- HTTP and HTTPS traffic
- Routes traffic to targets based on content of request.
- OSI Layer 7.
- Modern app. architectures [micro services / container based apps]

② Network load Balancer:
- TCP, UDP, TLS
- Routes traffic based on IP protocol data.
- optimized to handle sudden and volatile traffic patterns.
- OSI Layer 4

③ Classic Load Balancer
- HTTP, HTTPS, TC, SSL
- Load Balancing across multiple EC2s.
- Layer 4 and 7
- Register targets to the LB directly.

Load Balancer Monitoring
① Amazon Cloudwatch metrics
② Access logs
③ AWS Cloudtrail logs
: captures the who, what, when and where of API interactions.

Cloudwatch events
become aware of operational changes as they occur & responds to take corrective actions.

AWS EC2 auto Scaling

Enables you to maintain availability.

Auto scaling group: a collection of EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management.

Amazon EC2 auto scaling
+ AWS auto scaling
= Predictive scaling