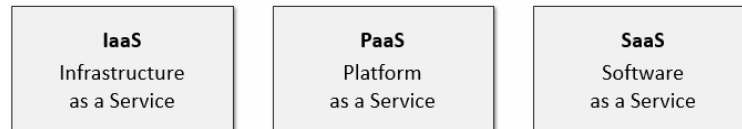


# LES BASES DE AWS

## I. Généralités sur le cloud

**Le cloud computing** c'est le calcul dans le nuage. le cloud computing c'est le fait d'avoir de la ressource à la demande que l'on paie à l'usage. Mécanisme qui permet de consommer des ressources de tout ordre à la demande et que l'on paie à l'usage. C'est le mode pay-as-you-go (Faire l'analogie avec Internet un FAI ou alors avec l'électricité).

On distingue 03 modèles de **cloud computing** :



**IaaS** : Infrastructure as service, qui comme son nom l'indique permet de fournir des infra en tant que service. Ce model contient donc l'ensemble des services de type Infrastructure et à ce moment-là le cloud va gérer toute la partie physique ou infra (les serveurs, le réseau, le stockage...)

**Paas** : model adapté pour les développeurs car en plus de fournir et maintenir l'infra, l'opérateur se charge également de créer des machines virtuelles et s'assure de leur interconnexion afin que les développeurs ou utilisateurs finaux y intègrent juste leur code pour le déployer dans le cloud et rendre disponible

**Saas** : Software as service, idéal pour le business man startuper qui ne sait pas développer mais qui veut un logiciel déjà fonctionnel qu'il pourra consommer. L'opérateur cloud gère tout, l'infra, les Vms ou l'environnement et le software.

On distingue également 03 modes de déploiement vers le cloud

- **All-In Cloud** : Tout déléguer au cloud provider, délocaliser toute son infrastructure ou ses serveurs vers le cloud
- **Hybrid** : dans ce mode, une partie de l'infra est délocalisée chez un cloud provider et une autre en local. (exemple délocaliser la partie calcul vers un cloud operator et stocker les résultats de ces calculs là en local pour des raisons de Sécurité et autre).
- **Private Cloud (On-premises)** : Pour des raisons de souveraineté, une entreprise peut décider de financer et de créer elle-même son propre cloud permettant de consommer des ressources à la demande.

### Comparaison entre le mode All-in Cloud vs On-premises



#### All-In Cloud

- ✚ Pas de dépenses d'investissement
- ✚ Faibles coûts permanents
- ✚ Focus sur l'innovation
- ✚ Capacité flexible
- ✚ Rapidité et agilité
- ✚ Portée mondiale à la demande



#### On-Premises

- ✚ Grande dépense initiale
- ✚ Cycles de travail, de correctifs et de mise à niveau
- ✚ Administration système
- ✚ Ressources fixes
- ✚ Long cycle de mise en oeuvre
- ✚ Zone géographique limitée.

AWS est un opérateur cloud qui propose un ensemble de logiciels qui sont consommables à distance via l'appel d'API. C'est une infrastructure mise à disposition que l'on peut consommer en interrogeant le service qui va bien. AWS dispose de plus de 165 services repartis en catégories dépendant de votre activité et permettant de délocaliser votre SI au fur et à mesure.

Pour accéder à AWS, on peut utiliser l'une des 03 méthodes suivantes :

- AWS Management Console
- AWS Command Line Interface (CLI)
- Software Development Kit (SDK)

## II. Les Services de AWS

### 2.1. Les Core Services

Ils sont regroupés en modules en fonction des fonctionnalités de chaque services, on distingue :

- Le module de calcul : COMPUTE
- Le module de Réseau : Networking
- Le module de Storage : Storage
- Le module de base de données : Database

Chaque catégorie ou module fait appel à un ensemble de services pouvant être consommé fonction de ses besoins.

### 2.2. Les Foundational services (orientés métiers)

On distingue :

- Le module Analytics
- Module Enterprise Apps
- Module Mobile Services
- Module Internet of things

### 2.3. Les Developer and Operations services

On distingue :

- Le Module Developer Tools
- Module Management Tools
- Module Security and identity
- Le module Apps Services

## III. Bonnes pratiques à adopter pour migrer dans le cloud.

Afin de faciliter l'utilisation et d'optimiser le fonctionnement des ressources du Cloud AWS, AWS a mis sur pied un ensemble de bonnes pratiques à utiliser pour migrer sereinement son infrastructure ou ses services vers le Cloud.

Ces bonnes pratiques sont appelées par le sigle CAF ( AWS Cloud Adoption Framework).

Ces bonnes pratiques s'appuient sur 06 grands piliers qui sont :

- 1) **Business perspective** : Il s'agit ici de bien vérifier et de se rassurer que le fait de vouloir aller vers le Cloud s'aligne avec notre politique Business
- 2) **People Perspective** : Vérifier quelles sont les compétences dont auront besoin les employés pour passer vers le Cloud
- 3) **Governance perspective** : Est-ce que le fait de passer vers le Cloud s'aligne en tout point avec nos besoins de gouvernances IT définies par la DSI
- 4) **Platform Perspectives** : Quels seront les outils pour optimiser nos services sur le cloud AWS
- 5) **Security Platform** : Comment va être définie et implémentée le niveau de sécurité, de gouvernance et de risques pour le Cloud
- 6) **Operations Perspectives** : Comment va-t-on maintenir notre infrastructure sur AWS.

## IV. Facturation AWS

La facturation AWS tourne autour de 03 principes :

- **La partie calcul** : Compute (Processeur + RAM)
- **Le volet Stockage** : Ce qui va effectivement être stocké comme données
- **Le Outbound data transfert** : Le trafic sortant de la machine vers internet

Dans la plupart des cas, le trafic entrant n'est pas facturé et le transfert des données entre services de la même région n'est également pas facturé.

Le **TCO** : c'est le cout total incluant dépenses directes et indirectes nécessaires pour la mise en place de notre infrastructure.

AWS propose plusieurs calculateurs de couts permettant d'obtenir ce TCO tels que : **AWS Simple Montly Calculator** ; **AWS TCO Calculator**

### 4.1. Politique de facturation AWS

AWS facture en s'appuyant sur les politiques suivantes :

- 1) **Vous payez ce que vous utilisez** : Pay What you use
- 2) **Pay less when you reserve**: Payer moins si vous réservez
- 3) **Pay less when you use more** : vous payez moins si vous utilisez plus
- 4) **Pay even less as AWS grows** : payez de plus en plus moins quand AWS grandit

## V. AWS INFRASTRUCTURE

### 5.1. AWS Global Infrastructure

Les 03 notions importantes pour l'infrastructure dans AWS sont :

- **Les régions** : qui sont des endroits dans le monde où on trouve des datacenters AWS
- **Availability Zones** : Zones d'une région ayant plusieurs datacenter interconnectés par F.O (une région peut avoir plusieurs AZ)
- **Edge Locations** : Zones virtuelles ou datacenter temporaires qu'on déploie dans une zone n'ayant pas de datacenter AWS pour couvrir un besoin ponctuel.

Une région est composée d'au moins 02 Availability Zone qui contiennent à leur tour plusieurs datacenters. Un datacenter comporte en moyenne entre 50000 et 70000 serveurs physiques. Les datacenter d'un même Availability zone sont reliés entre eux par Fibre Optique et isolés des autres Availability zone ou régions. Les Edge Location quant à eux permettent d'avoir les services AWS au plus prêt de nous lorsqu'il n'y'a pas d'Availability zone proche de nous.

## VI. Services de base de AWS



## Créer un compte AWS gratuit

- 1) Rechercher sur google « AWS create account »
- 2) Sélectionner « Amazon Web Services - Sign Up For a Free AWS Account »
- 3) Cliquer sur créer un compte gratuit
- 4) Renseigner les champs et créez votre compte.

NB : vous devez disposer d'une adresse email et une carte de crédit valide ayant un montant minimum de 1€.

## 6.1. Services de type Compute

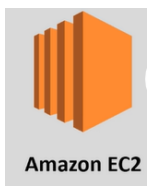
L'utilisation de AWS se manifestant au niveau de la maîtrise de ses différents services, nous commencerons par le service Compute.

Les Compute services appartiennent en effet aux Core Services ou Foundation Services d'AWS et sont presque incontournable pour l'utilisation d'AWS.

Il existe plusieurs services appartenant au module Compute d'AWS tels que :

- **Amazon Elastic Compute Cloud (Amazon EC2)** : Permet la création d'environnement ou de machines virtuelles de calcul dans le cloud
- **AWS Lambda** : permet de gérer tout ce qui est serverless (fait références aux applications dont l'allocation et la gestion des ressources sont entièrement gérées par le fournisseur de services cloud)
- **Automatic Scaling** : permet de gérer la montée en performance si besoin et la haute disponibilité de nos machines EC2
- **Elastic Load Balancer** : qui nous permet de répartir le trafic entrant et permet d'atteindre un niveau élevé de tolérance aux pannes.
- **AWS Elastic Beanstalk** : permet de gérer rapidement nos déploiement, nos besoins de montée en performance et de manager rapidement nos applications
- **AWS Lightsail** : permet de rapidement déployer une machine virtuelle sans toutefois comprendre le fonctionnement intérieur de AWS, permet de manager de simples applications web ou applications servers
- **Amazon Elastic Container Services (ECS)** : qui nous permet de déployer de façon rapide, scalable nos conteneurs et nous permet également d'éliminer les tâches de management de cluster de notre infra.
- **AWS Fargate** : permet de créer des container sans serveur ni cluster de management
- **Amazon Elastic Container Service for Kubernetes (EKS)** : Permet de utiliser kubernetes sans manager les cluster Kubernetes.

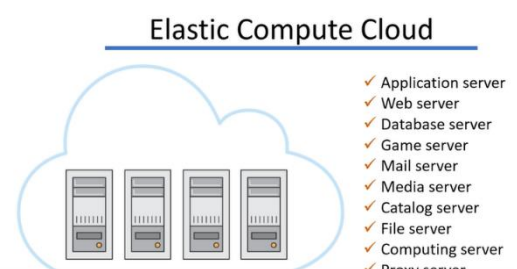
## 6.2. AMAZON ELASTIC COMPUTE CLOUD (AMAZON EC2)



Il s'agit en effet du service AMAZON qui est responsable de l'exécution des machines virtuelles.

Il permet déployer plusieurs types d'application comme vu ci-après sur l'image suivante. Il se rapproche le plus de nos serveurs que nous disposons en On premises

Le service EC2 nous permet donc d'avoir un environnement virtuel de calcul que l'on appelle Instance, il supporte la majorité de système d'exploitation existants. On peut créer, sauvegarder, réutiliser les images comme Amazon Machine Images (AMIs) qui sont en effet des images de machines que Amazon utilise pour créer ses instances EC2. Le service Amazon Ec2 nous permet de définir les ressources CPU, mémoire, carte réseau, carte graphique qu'une instance virtuelle va consommer, il est également possible de décider de l'endroit où notre machine sera hébergée physiquement à l'aide des VPC ; il permet également de définir l'ensemble des sécurité pour protéger l'accès à nos instances.

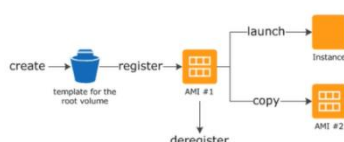


### AMI Lifecycle and Uses

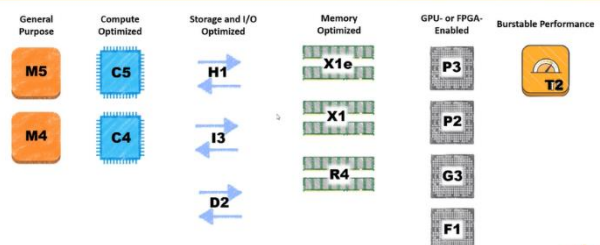
- ❏ Create and register an AMI.

- ❏ Uses:

- ❏ Launch new instance.
- ❏ Copy within the same region or to different regions.
- ❏ De-register the AMI when no longer required.

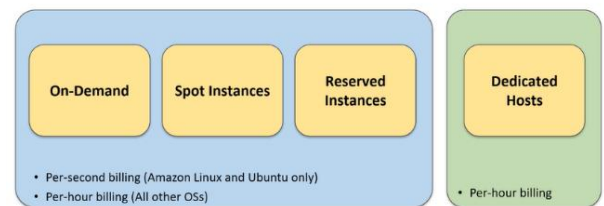


### Broad Set of Compute Instance Types



## Modes de tarification d'instances AWS.

### Amazon EC2 Pricing



### Amazon EC2 Pricing: Costs

On-Demand Instances	Spot Instances	Reserved Instances	Dedicated Hosts
• Pay for what you use • Per-second billing	• Spot price based on supply and demand • Per-second billing	• Pay low or no upfront fee; overall cost is lower • Per-second billing	• Pay the On-Demand rate for every hour the host is active in the account

#### Les modes de tarification d'instances EC2

- **A la demande** : c'est le mode le plus utilisé à ce jour qui est celui qui veut que le client crée ses instances au moment où il en a besoin les utilise et puis quand plus nécessaire els supprime
- **Spot instances** : il s'agit d'un système d'enchère où AWS place ses ressources inutilisées aux enchères, les clients surenchérissent et lorsque votre prix s'aligne avec la ressource que vous demandez, AWS vous fournit ladite instance. Néanmoins dès lors que le prix de cette instance vient à changer, AWS vous la retire sans préavis. Il est fortement conseillé en cas d'utilisation de ce type de toujours sauvegarder ses données.
- **Instances réservées** : Possibilité de réserver les instances à l'avance sur 1 à 3 ans et les payer à l'avance cela permet de réduire les coûts de plus de 75%
- **Instance dédiés** : dans le cas où les options fournies par AWS ne vous satisfont pas alors vous pouvez demander une instance dédiée avec des caractéristiques particulières et AWS la mettra à votre disposition

**NB** : Les types d'instance à la demande, réservées et spot instances sont éligibles à la facturation à la seconde, à la condition que les OS soient du Amazon linux ou du Ubuntu. Les instances dédiés et tous les autres OS quant à eux sont à la facturation à l'heure.

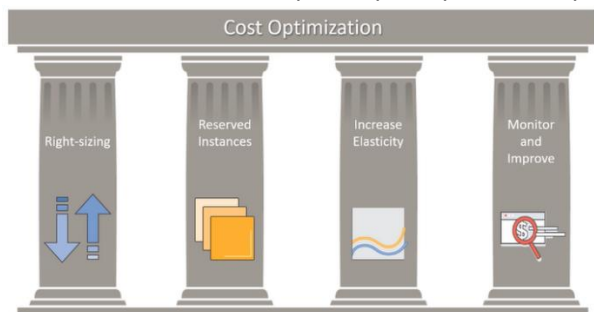
## Critères à prendre en compte lors de l'estimation des coûts des instances EC2

Ils sont au nombre de 9

- **Le temps d'exécution des instances** : les ressources AWS ne sont facturées que lorsqu'elles sont en exécution
- **La configuration de l'instance** : le coût de l'instance dépend de ses paramètres tels que sa région, son nombre de cœurs, sa mémoire, taille de disque, capacité réseau et autre
- **La méthode d'achat des instances** : le prix varie fonction du mode d'achat des instances (à la demande, réservées, spot instances, instances dédiées).
- **Le nombre d'instance** : votre facturation mensuelle prendra en compte la totalité de vos instances
- **Le load balancing** : prendre en compte le coût de la fonctionnalité load balancing si jamais elle est activée sur votre compte.
- **Cloudwatch** : prendre en compte le coût de cette fonctionnalité si jamais elle est activée sur votre compte.
- **Auto-scaling** : fonctionnalité gratuite, mais prendre en compte le coût des ressources ajoutées à vos instances en cas de montée de charge grâce à l'auto-scaling.
- **Elastic Ip address** : les adresses IP publiques sont gratuites sur AWS

### 6.2.1. Optimisation des coûts avec EC2

EC2 nous permet d'aligner notre infrastructure aux besoins du marché et de ce fait de ne payer que pour ce dont j'ai réellement besoin. On a 4 piliers principaux de l'optimisation de la consommation des ressources



- **Bien dimensionner ses ressources** : mettre la bonne taille au niveau de ses ressources fonction de l'OS et de l'application
- **Utiliser si possible les instances réservées** : réserver des instances sur 1 à 3 ans afin d'avoir des réductions de prix
- **Améliorer l'élasticité** : utiliser tout ce qui est Load balancing ou Auto Scaling pour augmenter la flexibilité de l'infrastructure
- **Monitorer et améliorer** : il faut monitorer afin d'anticiper sur ce qui sera nécessaire pour l'amélioration de votre infra

## 6.3. AWS Lambda

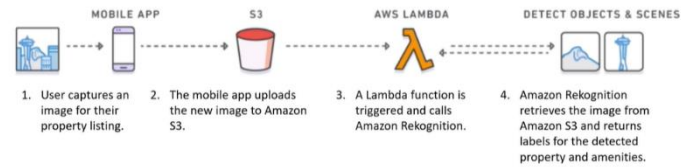
AWS Lambda est l'un des services phares d'AWS qui permet de mettre en place du Serverless. AWS LAMBDA permet de lancer à certaines dates ou alors appeler par certains événements des opérations qui vont durer maximum 5 minutes, il supporte plusieurs langages (le Bash, python...) . de façon générale, AWS Lambda nous permettra de lancer des opérations particulières écrites dans un langage spécifique pour lancer des actions qui peuvent être :

- Suite à une demande d'un de vos clients sur votre site, Amazon Lambda pourra récupérer le contenu de sa commande et l'envoyer sur un autre serveur




- Suite à un bug d'une application, Amazon lambda peut être configuré pour déclencher automatiquement la sauvegarde de la BDD vers un autre serveur
- A une date précise, faire un backup de votre machine

## Lambda Example



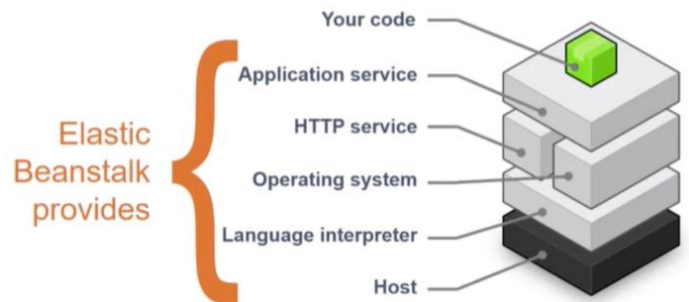
## 6.4. AWS Elastic Beanstalk

Elastic Beanstalk est un service du type Paas (Platform as Service) qui permet de faciliter la tâche aux développeurs voulant déployer leurs applications sur Amazon sans toute fois maîtriser le fonctionnement des ressources AMAZON. Pour ce faire, le Dev devra juste uploader son code sur AWS Elastic Beanstalk et Amazon se chargera de déployer l'ensemble des ressources Amazon permettant le bon fonctionnement de l'application. Amazon sera comme un guide permettant au Dev de déployer son application fonction du langage. Il supporte une large plage de langage



**AWS Elastic Beanstalk**

- Supports a large range of platforms:
  - Packer Builder
  - Single Container, Multi-container, or Pre-configured Docker
  - Go
  - Java SE
  - Java with Tomcat
  - .NET on Windows Server with IIS
  - Node.js
  - PHP
  - Python
  - Ruby
- No charge for Elastic Beanstalk; pay only for the underlying services used.



## VII. SERVICES AWS POUR LE STOKAGE

Le stockage dans le cloud est un composant essentiel du cloud computing, contenant les informations utilisées par les applications. Afin de choisir le stockage approprié fonction de son besoin, il est important de différencier les types de stockage et de chercher à savoir s'ils offrent un stockage "au niveau bloc" ou un stockage "au niveau objet".

En effet cette différence a un impact majeur sur le débit, la latence et le coût de votre solution de stockage, car avec un stockage Objet, la modification des données dans ce stockage exige la modification et le rechargement entier du fichier ainsi modifié dans le stockage. Par contre avec un stockage bloc la modification d'un fichier se fait juste sur le bloc contenant le paramètre à modifier dans le fichier (pas besoin de recharger le fichier entier dans le stockage). Les solutions de stockage par blocs sont généralement plus rapides et utilisent moins de bande passante, mais coûtent plus cher que le stockage au niveau objet.

Amazon propose 03 grandes variétés de stockage : Amazon EBS, Amazon S3, et Amazon EFS.

### 7.1. Stockage AMAZON EBS

Amazon EBS fournit des volumes de stockage de blocs persistants à utiliser avec les instances Amazon EC2 dans le cloud. Chaque volume Amazon EBS est automatiquement répliqué dans sa zone de disponibilité pour vous protéger des pannes de composants, offrant une haute disponibilité et durabilité. Les volumes Amazon EBS offrent les performances cohérentes et à faible latence nécessaires pour exécuter vos charges de travail. Il existe 02 type de volume AMAZON EBS ; le type SSD et le type HDD.



	Solid-State Drives (SSD)		Hard Disk Drives (HDD)	
	General Purpose	Provisioned IOPS	Throughput-Optimized	Cold
Max volume size	16 TiB	16 TiB	16 TiB	16 TiB
Max IOPS/volume	16,000	64,000	500	250
Max throughput/volume	250 MiB/s	1,000 MiB/s	500 MiB/s	250 MiB/s

Pour fournir un niveau encore plus élevé de durabilité des données, Amazon EBS vous donne la possibilité de créer des instantanés ponctuels (snapshots) de vos volumes, et AWS vous permet de recréer un nouveau volume à partir d'un instantané à tout moment

L'estimation du cout des volumes AMAZON EBS s'appuie sur les paramètres suivants :

- **Le type et la taille (capacité) de volume provisionnée**
- **Le nombres d'opérations entrées/sorties par secondes (IOPS)** : la facturation prend en compte le nombre de demandes que vous adressez à votre EBS
- **Les snapshots existants** : le couts supplémentaire est par Go/mois de données stockées.
- **Data transférées** : Prend en compte la quantité de données transférées hors de votre EBS.

## 7.2. AMAZON SIMPLE STORAGE SERVICE (S3)



Il s'agit d'un système de stockage de type objet fonctionnant comme Dropbox. Amazon S3 est une solution de stockage cloud entièrement gérée conçue pour évoluer de manière transparente et offrir une durabilité supérieure à 99,9 %. Vous pouvez stocker autant d'objets que vous le souhaitez dans un compartiment et écrire, lire et supprimer des objets dans votre compartiment.

Un stockage S3 est un compartiment dans lequel on peut stocker des objets identifié par un nom unique ou encore Bucket name. Il peut stocker des objets mesurant jusqu'à 5To. Chaque fois qu'un Compartiment S3 ou Bucket S3 est créé, ses données sont répliquées dans au moins 3 autres zones de disponibilité de sa région afin de garantir la sécurité et la résilience des données.

Il existe plusieurs classes de stockage de type S3 :

- **S3 standard** : Cette classe offre une durabilité, une disponibilité et des performances élevées (faible latence et débit élevé) de stockage d'objets correspondant au stockage d'objets fréquemment utilisés.
- **S3 Intelligent-Tiering** : idéal lorsque vous ne connaissez pas à l'avance la fréquence d'utilisation de vos objets qui y seront stockés. En effet cette classe dispose d'un trieurs intelligents qui trie les objets fonction de leur fréquence d'utilisation et classe les objets non utilisés depuis plus de 30jours vers un niveau d'accès peu fréquent (niveau à prix réduit et performances optimisées pour les accès peu fréquents) et quant aux autres objets fréquemment utilisés, il les classe dans un niveau d'accès correspondant au S3 Standard.
- **S3 Standard-Infrequent Access** : Classe correspondante aux données ou objets auxquels on accède peu fréquemment. S3 Standard-IA offre la durabilité élevée, le débit élevé et la faible latence de S3 Standard, avec un faible prix de stockage par Go
- **S3 One-Zone-Infrequent Access (S3 One Zone-IA)** : identique au mode S3 Standard-IA, seulement que dans ce cas, les données ne sont répliquées que dans une seule autre zone de disponibilité au lieu d'un minimum de 03 comme c'est le cas pour les autres classes de stockage.
- **Amazon S3 Glacier** : S3 Glacier est une classe de stockage sécurisée, durable et économique pour l'archivage des données. Vous pouvez stocker de manière fiable n'importe quelle quantité de données à des coûts compétitifs ou moins chers que les solutions sur site
- **Amazon S3 Glacier Deep Archive** : S3 Glacier Deep Archive est la classe de stockage la moins chère d'Amazon S3 et prend en charge la conservation à long terme et la préservation numérique des données accessibles une ou deux fois par an

L'estimation du cout du stocke de type AMAZON S3 prend en compte les paramètres suivants :

- **Le type de classe de stockage** : le prix varie fonction de la classe choisie (standard, intelligent, Glacier...).
- **La taille du stockage** : varie en fonction du nombre d'objets qui y sont stockés.
- **Le nombre et le type de requêtes faites sur le S3** : requête (GET, PUT et COPY), tarifs pour les requêtes GET par rapport aux autres.
- **Data Transfert** : Tarification basée sur la quantité de données transférées hors de la région AWS du stockage S3

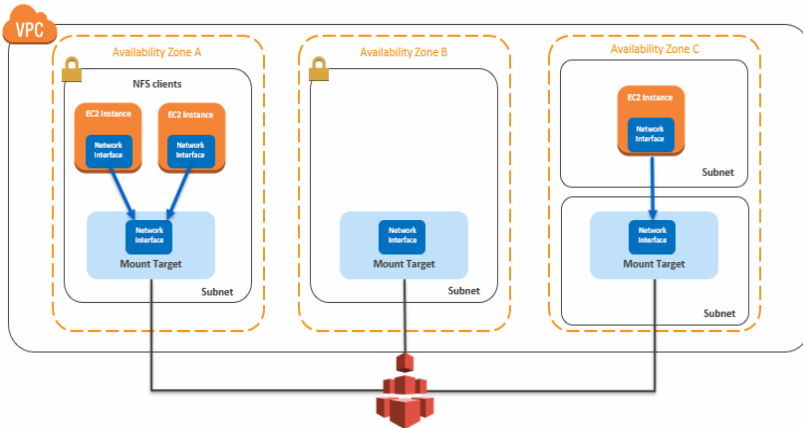
## 7.3. AMAZON ELASTIC FILE SYSTEM (EFS)



Amazon Elastic File System (Amazon EFS)

Cette solution de stockage d'Amazon permet de partager un même stockage avec plusieurs machines virtuelles EC2. Ce service de stockage d'Amazon permet de créer des file system storage permettant de partager la même donnée à des serveurs devant y avoir accès. exemple de base de données partageant les même fichiers ou alors site web partageant les même fichiers.

Lorsqu'on créer notre stockage EFS et que l'on veut le rendre disponible pour nos EC2, il faudra créer un point de montage ou (mount target) pour chaque zone de disponibilité à l'intérieur de laquelle on aimerait le



### Procédure de mise en place d'un stockage EFS

- 1) Créer et lancer une instance Amazon EC2
- 2) Créer le stockage Amazon EFS
- 3) Créer les points de montages dans le bon réseau et AZ
- 4) Connecter ses instances EC2 au point de montage
- 5) Sécurisez et consommez vos ressources.

## File system

### Mount target

- Subnet ID
- Security groups
- One or more per file system
- Create in a VPC subnet
- One per Availability Zone
- Must be in the same VPC

### Tags

- Key-value pairs

Dans Amazon EFS, un système de fichiers est la ressource principale. Donc lors de la création de votre stockage EFS, vous devez spécifier les paramètres de votre système de fichiers.

Chaque système de fichiers a des propriétés telles que :

- L'ID
- le jeton de création
- l'heure de création
- la taille du système de fichiers en octets
- le nombre de cibles de montage créées pour le système de fichiers et
- l'état du système de fichiers.

Ensuite pour accéder à votre système de fichiers, vous devez créer des cibles de montage dans votre VPC (réseau privé). Chaque cible de montage a les propriétés suivantes :

- L'ID de la cible de montage
- L'ID de sous-réseau dans lequel il est créé
- L'ID du système de fichiers pour lequel il est créé
- Une adresse IP à laquelle le système de fichiers peut être monté
- L'état de la cible de montage.

rendre visible. Et une fois le point de montage créer dans la bonne zone de disponibilité, les instances EC2 de cette zone pourront utiliser le point de montage pour se connecter à notre stockage EFS.

## 7.4. AMAZON GLACIER



Amazon Glacier

Amazon Glacier est un service managé d'Amazon qui va permettre en fait d'archiver l'ensemble, il supporte l'encryption des données qui vont y transiter. L'accès aux données stockées dans Amazon glacier sont conditionnées par la suite à un certain temps d'attente pouvant aller de quelques minutes à plusieurs heures.

Il existe trois termes clés d'Amazon Glacier que vous devez connaître :

- **Archive** : tout objet tel qu'une photo, une vidéo, un fichier ou un document que vous stockez dans Amazon Glacier. C'est l'unité de base de stockage dans Amazon Glacier. Chaque archive a son propre identifiant unique et peut également avoir une description.
- **Vault** : Un conteneur pour stocker des archives. Lorsque vous créez un coffre-fort, vous spécifiez le nom du coffre-fort et la région dans laquelle vous souhaitez que le coffre-fort se trouve.
- **Politique d'accès au coffre-fort (Vault Access policies)** : déterminez qui peut et ne peut pas accéder aux données stockées dans le coffre-fort ainsi que les opérations que les utilisateurs peuvent et ne peuvent pas effectuer.



Une stratégie d'autorisations d'accès au coffre peut être créée pour chaque coffre afin de gérer les autorisations d'accès pour ce coffre. Vous pouvez également utiliser une stratégie de verrouillage de coffre pour vous assurer qu'un coffre ne peut pas être modifié. Chaque coffre peut être associé à une stratégie d'accès au coffre et à une stratégie de verrouillage de coffre.

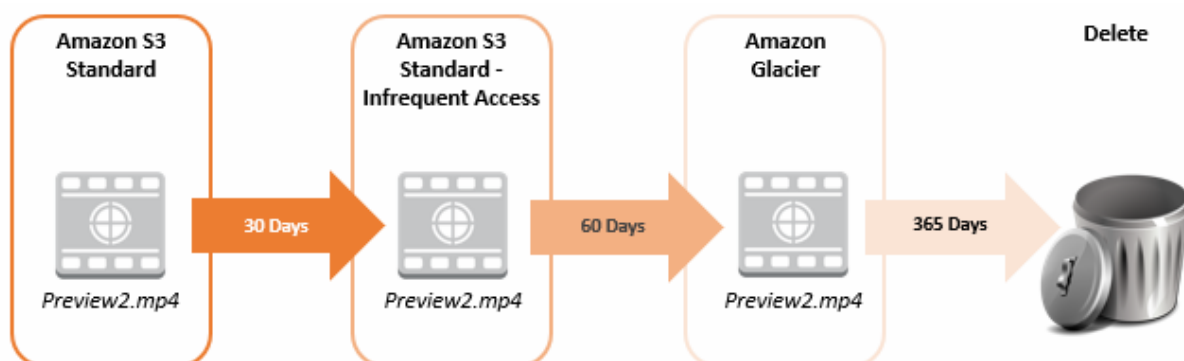
Il existe trois options pour récupérer des données avec des temps d'accès et des coûts variables : récupérations accélérées, standard et en bloc, comme suit :

- **Les récupérations accélérées (Expedited)** sont généralement disponibles en 1 à 5 minutes (coût le plus élevé).
- **Les récupérations standard (Standard)** se terminent généralement en 3 à 5 heures (moins que accéléré, plus qu'en vrac).
- **Les récupérations en masse (bulk)** se terminent généralement dans les 5 à 12 heures (coût le plus bas).

Pour stocker et accéder aux données dans Amazon Glacier, vous pouvez utiliser AWS Management Console ; cependant, seules quelques opérations, telles que la création et la suppression de coffres et la création et la gestion de stratégies d'archivage, sont disponibles dans la console.

Presque toutes les autres opérations nécessitent que vous utilisiez l'API REST Amazon Glacier ou les kits SDK AWS Java ou .NET pour interagir avec Amazon Glacier via l'interface de ligne de commande (CLI).

Vous pouvez également archiver des données dans Amazon Glacier à l'aide de stratégies de cycle de vie.



En plus de pouvoir définir des règles de cycle de vie par objet, vous pouvez également définir des règles de cycle de vie par compartiment.

## VIII. NETWORK

### 8.1. AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)



**Amazon Virtual Private Cloud (or Amazon VPC)** est un réseau personnalisé au sein du cloud AWS. Il vous permet de concevoir et de mettre en œuvre un réseau indépendant qui fonctionne dans le cloud. C'est le service qui permet de mettre en place des réseaux privés, sous réseaux ou Vlan dans le cloud. Amazon VPC est votre environnement réseau dans le cloud. Il vous permet de créer un réseau privé dans le cloud AWS qui utilise bon nombre des mêmes concepts et constructions qu'un réseau sur site.

Au sein d'une région, vous pouvez créer plusieurs Amazon VPC, et chaque Amazon VPC est logiquement isolé même s'il partage son espace d'adressage IP (Internet Protocol). Un VPC est lié à une région donc il ne peut pas couvrir plusieurs régions à la fois. Par contre un VPC d'une région est visible dans toutes les zones de disponibilité de ladite région.

**NB :** Amazon VPC permet de créer des réseaux virtuels afin d'isoler les ressources. Toutes les ressources de AMAZON (EC2...) doivent être créées dans un VPC.

Les éléments pour la configuration de AMAZON VPC sont :

- **La plage d'adresse principale du VPC :** LA plage d'adresse du VPC doit être au maximum dans une plage /16 exemple 10.0.0.0/16. Cette plage d'adresse ne plus être changée après la création du VPC. Une plage d'adresses Amazon VPC peut être aussi grande que /16 (65 536 adresses disponibles) ou aussi petite que /28 (16 adresses disponibles) et ne doit pas chevaucher les adresses des autres réseaux auxquels elles sont connectées.
- **Création de sous-réseau dans le VPC :** Il faut créer des sous réseaux dans des zone de disponibilité définies et les lier à un VPC ; ensuite préciser une plage d'adresse pour ce sous-réseau : les plages d'adresses de sous réseau

pour le réseau le plus petit c'est en /28 (10.0.0.0/28). AWS réserve les quatre premières adresses IP et la dernière adresse IP de chaque sous-réseau à des fins de mise en réseau interne.

- **Création des tables de routages** : les tables de routage sont utilisées pour spécifier les chemins ou les routes que devront utiliser les Sous-réseaux dans le VPC
- **Créer les Internet Gateway (IGW)** : qui permettent d'interconnecter les VPC à internet, ils jouent le rôle de passerelles entre Internet et les VPC. Un VPC qui n'est pas lié à une Internet Gateway est considéré comme un réseau privé et celui lié à un Internet Gateway comme un réseau public.

Les composants additionnels d'un AMAZON VPC sont :

- **Dynamic Host Configuration Protocol (DHCP) option sets** : AWS crée et associe automatiquement un ensemble d'options DHCP (Dynamic Host Configuration Protocol) pour votre Amazon VPC lors de la création et définit deux options : Domain-name-servers et Domain-name.
- **Groupes de sécurité ou Security groups** : est un pare-feu virtuel avec état qui contrôle le trafic réseau entrant et sortant vers les ressources AWS et les instances Amazon EC2.
- **Network Access Control List (ACLs)** : est une couche de sécurité facultative pour votre Amazon VPC qui agit comme un pare-feu pour contrôler le trafic entrant et sortant d'un ou plusieurs sous-réseaux. C'est l'équivalent des security groups mais qui se place au niveau du sous-réseau au lieu de l'instance EC2.
- **Elastic IP (EIP) Adresses**: Adresse IP publique statique pouvant être extraite d'un pool pour une utilisation temporaire.
- **Elastic Network Interface (ENI)**: Interface réseau virtuelle.
- **Endpoint**: Connexion directe à un autre service AWS.
- **Peering**: Permet à deux Amazon VPC de communiquer.
- **NAT Address Translation (NATs) instances and NAT Gateways**: Accepte, traduit et transfère le trafic au sein d'un sous-réseau privé.

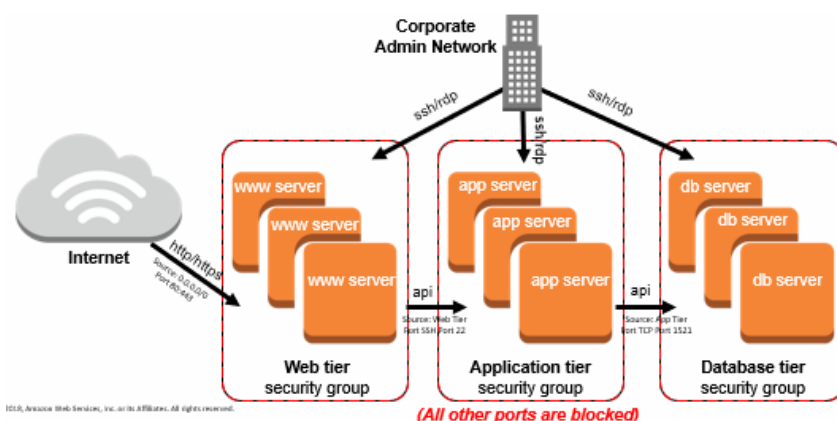
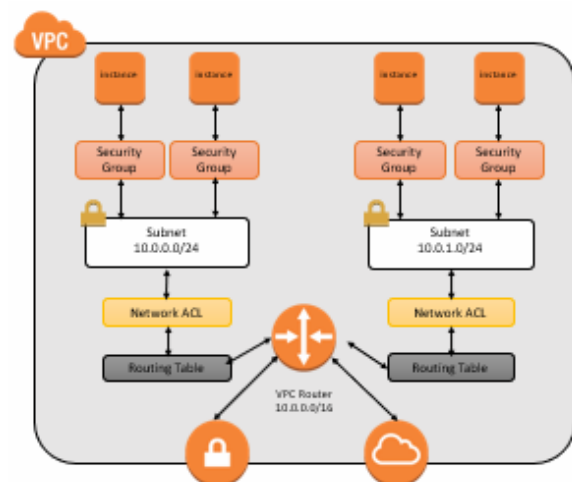
Il existe plusieurs options de connectivité VPN pour Amazon VPC. Vous pouvez connecter votre Amazon VPC à des réseaux distants à l'aide d'un AWS Hardware VPN, AWS Direct Connect, AWS VPN CloudHub ou d'un Software VPN.

Options de connectivité VPN	Description
AWS Hardware VPN	Vous pouvez créer une connexion VPN matérielle IPsec entre votre Amazon VPC et votre réseau distant.
AWS Direct Connect	AWS Direct Connect fournit une connexion privée dédiée d'un réseau distant à votre Amazon VPC.
AWS VPN CloudHub	Vous pouvez créer plusieurs connexions VPN matérielles AWS via votre VPC pour permettre les communications entre divers réseaux distants.
Software VPN	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your Amazon VPC that's running a software VPN appliance.

## 8.2. AMAZON SECURITY GROUPS

Chez AWS, les groupes de sécurité agiront comme un pare-feu intégré pour vos serveurs virtuels. Avec ces groupes de sécurité, vous avez un contrôle total sur l'accessibilité de vos instances.

Au niveau le plus basique, il s'agit simplement d'une autre méthode pour filtrer le trafic vers vos instances. Il vous permet de contrôler le trafic à autoriser ou à refuser



Vous pouvez utiliser plusieurs couches de sécurité, y compris des groupes de sécurité et des NACL, pour aider à contrôler l'accès aux instances Amazon EC2 dans chaque sous-réseau.

## 8.3. AMAZON CLOUDFRONT

Pour diffuser du contenu à vos utilisateurs, Amazon CloudFront utilise le réseau mondial d'emplacements périphériques pour la diffusion de contenu. En utilisant CloudFront, vous pouvez tirer parti de plusieurs emplacements dans le monde pour diffuser votre contenu, permettant à vos utilisateurs d'interagir avec votre application avec une latence plus faible. Amazon CloudFront est un service Web pour la diffusion de contenu ou Content Delivery Network (CDN).

Lorsque vous commencez à estimer le coût d'Amazon CloudFront, vous devez prendre en compte la distribution du trafic, les demandes et le transfert de données.

- **Distribution du trafic** – Les prix du transfert de données et des demandes varient selon les régions géographiques, et les prix sont basés sur l'emplacement périphérique à travers lequel votre contenu est diffusé.
- **Demandes** – Le nombre et le type de demandes (HTTP ou HTTPS) effectuées et la région géographique dans laquelle les demandes sont effectuées.
- **Transfert de données sortant** – La quantité de données transférées hors de vos emplacements périphériques Amazon CloudFront.

## IX. DATABASE

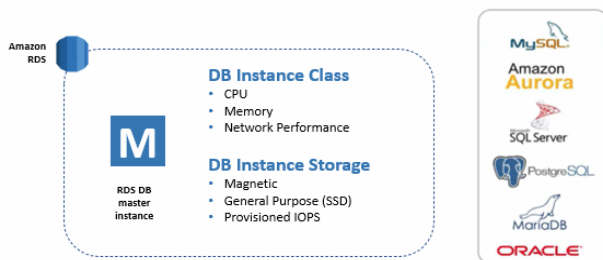
### 9.1. Amazon RDS (Amazon Relational Database Service)



Amazon Relational Database Service (RDS)

Etant donné la difficulté les difficultés d'administration d'une base de données relationnelles qui demande non seulement une expertise dans l'administration des systèmes (administration et maintenance des serveurs), expertise dans la gestion des base de données (configuration, maintenance et gestion des sauvegarde et de la haute disponibilité), Amazon a mis sur pied un service entièrement géré permettant la gestion de base de données relationnelle. AMAZON RDS est un service géré qui configure et exploite une base de données relationnelle dans le cloud. En effet, pour relever les défis liés à l'exécution d'une base de données relationnelle autonome et non gérée, AWS fournit un service qui configure, exploite et fait évoluer la base de données relationnelle sans aucune administration continue. Amazon RDS fournit une capacité économique et redimensionnable, tout en automatisant les tâches administratives fastidieuses.

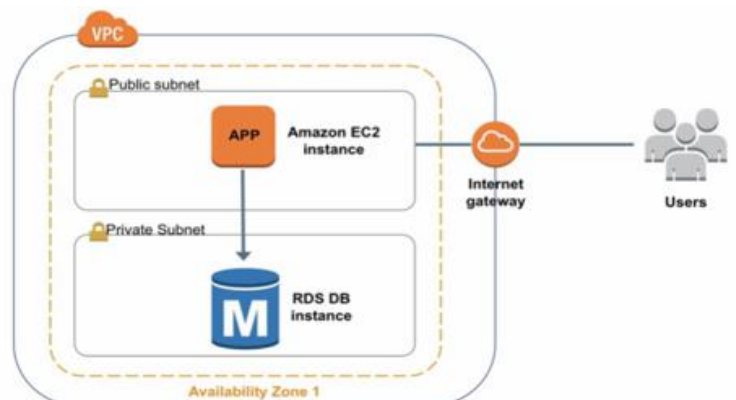
Amazon RDS permet de créer des blocs de bases appelées Instance de base de données. Une instance de base de données est un environnement de base de données isolé qui peut contenir plusieurs bases de données.



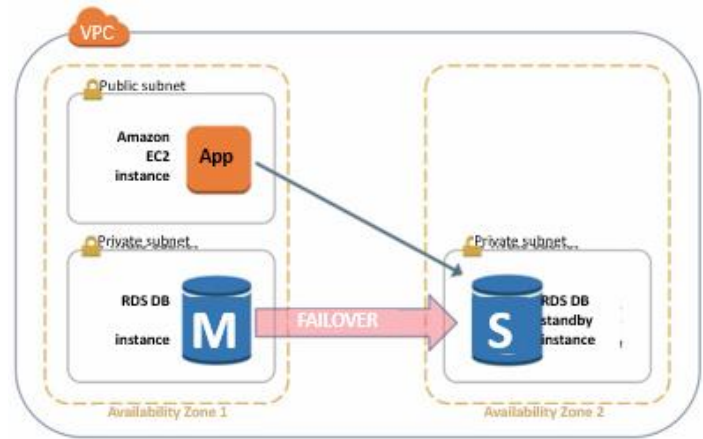
Pour la création d'une instance de base de données RDS, on doit spécifier la classe d'instance qui sera liée à cette BDD ; cette classe d'instance correspond en effet aux caractéristique matérielles de l'instance devant abriter la BDD.

On doit également spécifier le type de stockage qui sera utilisé (DB Instance Storage).

Afin d'augmenter la sécurité au niveau de votre instance de base de données, vous pouvez la mettre dans un AMAZON VPC contenant un sous-réseau privé devant contenir la BDD et un sous réseau public devant contenir l'application qui sera exposée à internet et devant consommer votre instance de Base données.



Etant donné qu'il s'agit d'un service entièrement gérés d'Amazon, afin de gérer la haute disponibilité et la tolérance aux pannes, Amazon RDS donne la possibilité de configurer votre instance de base de données pour une haute disponibilité avec un déploiement multi-AZ. Une fois configuré, Amazon RDS génère automatiquement une copie de secours de l'instance de base de données dans une autre zone de disponibilité au sein du même Amazon VPC. Après l'amorçage de la copie de la base de données, les transactions sont répliquées de manière synchrone sur la copie de secours. Si l'instance de base de données maître échoue, Amazon RDS met automatiquement l'instance de base de données de secours en ligne en tant que nouveau maître. En raison de la réplication synchrone, il ne devrait y avoir aucune perte de données. Étant donné que vos applications référencent la base de données par nom à l'aide du point de terminaison DNS RDS, vous n'avez pas besoin de modifier quoi que ce soit dans votre code d'application pour utiliser la copie de secours pour le basculement.



Lorsque vous commencez à estimer le coût d'Amazon RDS, vous devez tenir compte :

- 1) **Temps d'exécution** : les ressources n'entraînent des frais que lors de leur exécution. Par exemple, à partir du moment où vous lancez une instance de base de données jusqu'à ce que vous résilie l'instance.
- 2) **La capacité physique de la base de données** : la capacité que vous choisissez affectera le montant qui vous sera facturé. Les caractéristiques de la base de données varient en fonction du moteur de base de données, de la taille et de la classe de mémoire de la base de données.
- 3) **Le type de facturation de l'instance** : à la demande, réservées...
- 4) **Le nombre d'instances de BDD** : le nombre d'instance est à prendre en compte lors de l'estimation des coûts.
- 5) **Taille de stockage provisionnée pour la BDD** : les backups de BDD inférieure ou égale à 100% de la taille de stockage provisionnée se sont pas facturés, mais lorsque la BDD est supprimée, donc plus de capacité de stockage provisionnée, alors les backups sont facturés en fonction de leur taille (Go/mois)
- 6) **Stockage additionnels** : stockage liés au backups, en fait lorsque la taille des backups dépassent la capacité initiale provisionnée, alors le stockage additionnels nécessaires pour ces backups vous ait facturé également en Go/mois.
- 7) **Requêtes** : la facturation dépend également du nombre de requêtes d'entrée et de sortie faites à la base de données.
- 8) **Type de déploiement** : déploiement zone de disponibilité unique ou multiple zone de disponibilité
- 9) **Data transfert** : Aucun frais pour le transfert de données entrantes, Frais échelonnés pour le transfert de données sortantes

## 9.2. Amazon DynamoDB



Amazon DynamoDB

DynamoDB est un service de base de données NoSQL entièrement géré. Amazon gère toute l'infrastructure de données sous-jacente de ce service et stocke de manière redondante les données sur plusieurs installations au sein d'une région. Une base de données NoSQL est en fait une base de données de type clé/valeurs. L'un des avantages d'une base de données NoSQL est que les éléments d'une même table peuvent avoir des attributs différents, Cela vous donne la possibilité d'ajouter des attributs au fur et à mesure de l'évolution de votre application.

Les tableaux, les éléments et les attributs sont les composants principaux de DynamoDB. Un tableau est un ensemble de données. Les éléments sont un groupe d'attributs identifiables de manière unique parmi tous les autres éléments. DynamoDB prend en charge deux types de clés primaires. La clé de partition est une clé primaire simple, composée d'un attribut appelé clé de partition. La clé de partition et la clé de tri sont également appelées clé primaire composite composée de deux attributs.

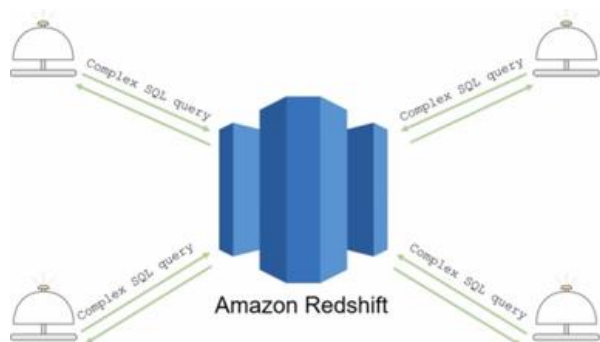
DynamoDB s'exécute exclusivement sur des disques SSD et prend en charge les modèles de stockage de documents et de valeurs-clés. La fonctionnalité Tables globales réplique automatiquement vos tables DynamoDB dans les régions AWS de votre choix.

Dynamo DB est idéal pour les applications mobiles, Web, de jeux, de technologie publicitaire et d'Internet des objets. Il est accessible via la console, la CLI et de simples appels d'API.

### 9.3. Amazon Redshift



Amazon Redshift est un entrepôt de données rapide et entièrement géré qui permet d'analyser toutes vos données de manière simple et économique à l'aide de SQL standard et de vos outils de Business Intelligence (BI) existants.



Amazon Redshift est un entrepôt de données rapide et puissant, entièrement géré, qui le rend simple et rentable à configurer, à utiliser et à faire évoluer. Il vous permet d'exécuter des requêtes analytiques complexes sur des pétaoctets de données structurées à l'aide d'une optimisation de requête sophistiquée, d'un stockage en colonnes sur des disques locaux hautes performances et d'une exécution de requête massivement parallèle. La plupart des résultats reviennent en quelques secondes.

La fonctionnalité Amazon Redshift Spectrum vous permet d'exécuter des requêtes sur des exaoctets de données directement dans Amazon S3. Amazon Redshift prend en charge le standard SQL et fournit des connecteurs JDBC et ODBC hautes performances, ce qui vous permet d'utiliser les clients SQL et les outils de BI de votre choix.

### 9.4. AMAZON AURORA



Amazon Aurora est une base de données relationnelle compatible MySQL et PostgreSQL conçue pour le cloud. Il combine les performances et la disponibilité des bases de données commerciales haut de gamme avec la simplicité et la rentabilité des bases de données open source. Amazon Aurora est hautement disponible et offre environ 5 fois les performances de MySQL. Il est simple à configurer et utilise des requêtes SQL. Il a une compatibilité directe avec MySQL 5.6 en utilisant le

moteur de stockage InnoDB. Amazon Aurora est un service de paiement à l'utilisation, qui garantit que vous ne payez que pour les services et les fonctionnalités que vous utilisez. Amazon Aurora est hautement disponible, stockant six copies de vos données dans trois zones de disponibilité avec des sauvegardes continues vers Amazon S3. Jusqu'à 15 réplicas en lecture peuvent être utilisés pour vous aider à vous assurer que vos données ne sont pas perdues. De plus, Amazon Aurora est conçu pour une récupération instantanée sur incident au cas où votre base de données principale deviendrait défectueuse.

## X. Auto Scaling et High Availability

### 10.1. ELASTIC LOAD BALANCER (ELB)

L'Elastic Load balancer de AWS est un service qui permet de distribuer automatiquement le trafic applicatif entrant sur plusieurs cibles, telles que les instances Amazon EC2, les conteneurs et les adresses IP. ELB propose trois types d'équilibreurs de charge : Application Load Balancer, Network Load Balancer et Classic Load Balancer.

- **Application Load Balancer (ALB)** : Il prend en charge le routage basé sur le contenu et les applications qui s'exécutent dans des conteneurs. Il prend en charge une paire de protocoles standard de l'industrie (websocket et http/2) et peut fournir une visibilité supplémentaire sur la santé des instances et des conteneurs cibles
- **Network Load Balancer (NLB)** : NLB est idéal pour équilibrer la charge du trafic TCP (Transmission Control Protocol) et est capable de gérer des millions de requêtes par seconde tout en maintenant des latences ultra-faibles. Ils équilibrent la charge en se basant sur la couche réseau (couche 4 OSI).
- **Classic Load Balancer (CLB)** : fournit l'équilibrage de charge de base sur plusieurs instances Amazon EC2 et fonctionne à la fois au niveau de la demande et de la connexion. C'est idéal pour les applications qui ont été construites au sein du réseau Amazon EC2-Classic.



## 10.2. AMAZON CLOUDWATCH



### Amazon CloudWatch

C'est le service Amazon nous permettant d'avoir les informations liées à la consommation de notre Infrastructure et ensuite si possible de pouvoir l'optimiser.

Il nous permettra de répondre aux questions :

- Qu'est ce qui est fait effectivement sur nos instances ? (en termes de consommation)
- Quelle est la performance de notre application ?
- Combien va nous couter effectivement nos ressources que nous sommes entrain d'utiliser sur AWS.

Ce service va monitorer l'ensemble de nos ressources et le trafic lié à notre infrastructure, il va :




- Scruter chacune des nos ressources afin de savoir ce qui ne va pas
- Il va également collecter ses infos et les stocker dans les fichiers de logs qui seront monitorés à leur tour
- Il sera également capable de nous notifier en cas de problèmes et engager un certain nombre d'action.

Les termes à retenir lors de l'utilisation de Cloudwatch sont :

- **Les métriques** : qui sont tout simplement les données liées à la consommation d'une ressource particulière par exemple (les métriques de la RAM, du CPU, du disque).
- **Les alarmes** : qui permettent de déterminer quel est le seuil de criticité acceptable ; donc il est possible de définir des alarmes sur AWS grâce à CloudWatch
- **Les évènements** : ce service donne en effet la possibilité de configurer des évènements pouvant se déclencher en cas d'alarme.

Les alarmes peuvent par exemple être définies sur les services EC2, RDS ou LoadBalancer... et ces services peuvent bien entendu être piloté par des évènements liés à ces alarmes-là.

Exemple d'alarme : si le CPU de mon instance EC2 est consommé à plus de 60% pendant 5 minutes, alors déclenche l'alarme. Et en termes d'évènement en cas d'alarme, on peut démarrer, arrêter une instance, scaler une instance ou envoyer des notifications via le service SNS (Service de notification de AMAZON).

Amazon EC2		If CPU utilization is <b>&gt; 60%</b> for <b>5</b> minutes...
Amazon RDS		If the number of simultaneous connections is <b>&gt; 10</b> for <b>1</b> minute...
Elastic Load Balancing		If number of healthy hosts is <b>&lt; 5</b> for <b>10</b> minutes...

CloudWatch conserve les métriques gratuitement pendant 15 mois. CloudWatch Metrics prend en charge les trois calendriers de conservation suivants :

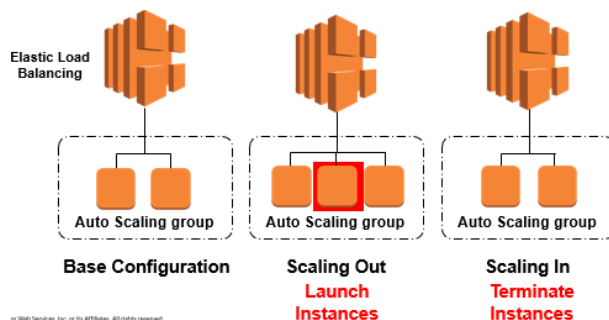
- Les points de données de 1 minute sont disponibles pendant 15 jours
- Les points de données de 5 minutes sont disponibles pendant 63 jours
- Les points de données d'une heure sont disponibles pendant 455 jours

## 10.3. AMAZON AUTO SCALING

L'**amazon Automatic Scaling** fournit une interface utilisateur simple et puissante qui vous permet de créer des plans de mise à l'échelle pour les ressources, notamment : Instances Amazon EC2 et flottes Spot, Tableaux Amazon DynamoDB, Tables et index Amazon DynamoDB, Répliques Amazon Aurora. L'utilisation d'Auto Scaling supprime les approximations quant au nombre de ressources dont vous avez besoin à un moment donné pour répondre aux exigences de votre charge de travail. On distingue 02 type de mise à l'échelle : le Scaling Out et le Scaling In. Le Scaling Out concerne les mises à l'échelle pour lesquelles on ajoute des instances pour supporter la charge tandis que le Scaling In concerne les mises à l'échelle pour lesquelles on met fin à des instances.

Si vous spécifiez des stratégies de mise à l'échelle, la mise à l'échelle peut lancer ou arrêter des instances à mesure que la demande sur votre application augmente ou diminue. L'Automatic Scaling s'intègre à ELB pour vous permettre d'attacher un ou plusieurs équilibres de charge à un groupe Automatic Scaling existant.

Une fois que vous avez attaché l'équilibreur de charge, il enregistre automatiquement les instances dans le groupe et distribue le trafic entrant entre les instances. Lorsqu'une zone de disponibilité devient défectueuse ou indisponible,



une nouvelle instance est lancée dans une zone de disponibilité non affectée. Lorsque la zone de disponibilité défectueuse revient à un état sain, la mise à l'échelle automatique redistribue automatiquement les instances d'application de manière uniforme dans toutes les zones de disponibilité de votre groupe.

x

03 Composants sont requis pour la mise à l'échelle automatique :

- **Tout d'abord, créez une configuration de lancement**, il s'agit ici de définir ce qui devra être lancé par l'automatic scaling (AMI, Instance EC2, Security groups, Rôles)
- **Ensuite, créez un groupe de mise à l'échelle automatique ( Auto Scaling group )** : ici il s'agit de définir où le déploiement a lieu et dans quelles conditions ( définir le VPC et sous réseaux, spécifier ELB si besoin, vous spécifiez le nombre d'instances minimum ou maximum ainsi que la capacité désirée).
- **Définissez ensuite au moins une stratégie d'Auto Scaling (Auto Scaling Policies)** : ici on spécifie quand lancer ou arreter les instances. Vous pouvez planifier un scaling automatique tous les jeudis à 15h00, par exemple, ou créer des conditions qui définissent des seuils pour déclencher l'ajout ou la suppression d'instances. Les stratégies basées sur des conditions rendent votre évolutivité dynamique et capable de répondre aux exigences fluctuantes

Il est également possible de relier Automatic Scaling à CloudWatch de telle sorte qu'une alarme CloudWatch puisse déclencher des opérations d'Automatic scaling. Ce mécanisme s'appelle l'auto scaling dynamique.

