

# Travaux pratiques

## AWS Infra as a service

### Identity and Access Management (IAM)

#### 1. Questions de cours

1. différence entre utilisateur IAM et rôle IAM :

un utilisateur IAM est toute entité associée à un compte root AWS pouvant avoir des permissions sur l'utilisation des services tandis qu'un rôle IAM est une permission créée qui facilite l'interaction entre 2 ou plusieurs services AWS sur le cloud.

2. différence entre trust policy et permission policy:

Une trust policy est une permission donnant à un rôle l'accès à un service pour donner d'accéder à un autre tandis qu'une permission policy est une permission autorisant le droit d'accéder à un rôle (et donc les droits d'exécution d'un service pour un autre).

3. une "aws managed policy" et différence avec un "user managed" policy:

une aws managed policy est une permission offrant des fonctionnalités et des gestion sur des services gérés et contrôlés par AWS qui est différent du user managed policy qui sont par contre gérés et contrôlés par les utilisateurs IAM.

4. constituants de base d'une policy IAM

On a :

- \* Version
- \* Principal
- \* Action
- \* Resource

### Elastic Cloud Compute (EC2)

1. Questions de cours :

1. Le service EC2 sert à émuler des machines virtuelles sur le cloud contenant différents variants de ressources: Dans le cas où on veut stocker nos données utilisant des gros datasets on n'aura besoin de la grosse quantité de ressources de stockage qui n'est pas toujours facile à avoir sur des machines physiques.

## 2. Types d'instances :

- Spot instance
- on-demand instance
- Reserved instance
- Dedicated instances
- Dedicated host instances

## 3. Différence entre "on demand" les "spot instance type" avec quelques cas d'usages

Dans les on-demand instances, la machine virtuelle est sollicitée à un moment donné et pour un temps précis par l'utilisateur et se porte garant pour payer le prix fort de cette MV (Dans le cas d'un hôtel de la place ou pour une soirée, un client vient payer pour la nuit qu'il passera après avoir donné les caractéristiques de la chambre voulue) tandis que les spot-demand c'est l'offre des machines virtuelles à un plus faible coût mais la disponibilité de la MV devra être assurée d'abord et une fois accéder l'utilisateur se verra rejeter à un instant donné de cette MV avec un temps d'avertissement limité. (L'utilisateur ici est donné une chambre tout en sachant qu'il pourra être éjecté à n'importe quel moment).

## 4. L'utilité des instances de type "compute optimized"

\* Pour des travaux à long utilisation de la CPU comme dans le domaine du machine learning.

## 5. Les security group sont encore appelés stateless firewall ?

Raison : Car les security group traitent chaque paquet indépendamment des autres et décident en fonction des règles (inbound et outbound) stipulées de bloquer ou de laisser passer le paquet ce qui les rend donc incapables de détecter plusieurs attaques potentielles car ils n'appliquent pas un mode de filtrage dynamique.

## 6. Différence entre Adresse IP privée et IP publique ?

Les adresses IP privées sont utilisées pour la communication et l'identification des équipements informatiques dans un même réseau tandis que les adresses IP publiques sont utilisées pour la communication entre 2 équipements info dans divers réseaux à travers Internet.

## 7. Placement group et son utilité :

Un placement group est un emplacement de stockage d'un ou plusieurs instances EC2 dans une AZ donnée.

Utilisation : Il sert a former des group d'instance EC2 comme dans des etagere de serveur afin qu'ils puisse communiquer (meme etant des differents AZ) facilitant l'atribution des roles.

Elastic Block Store (EBS) :

1. Questions de cours :

1.EBS et sa fonction principale :

EBS est un service AWS de creation de volumes de type block avec pour fonction principale d'attacher du stockage a une machine virtuelle creer.

2. différents types de volumes EBS avec leur caracteristiques :

\*.General Purpose(SSD) volumes : moins couteau avec un melange equilibre de performance entre la memoire et la CPU

\*Throughput Optimized HDD and Cold HDD volumes: Favorise beacoup la resource iops

Utiliser dans des lourds charge de travaux comme des datawarehouses

\* provision IOPS SSD: pour des charges de travaux eleve et des entres-sorties eleve neccessitant une faible latence

3. Attacher un volume EBS a une instance EC2 :

- Tout d'abord le volume est creer avec une capacite et type definie dans un AZ donne assurant qu'il se trouve dans le meme AZ que son instance EC2 en allant a Volume > Create Volume > et validant avec le create volume

-Puis selectionnez ce volume et aller a : Action > Attach Volume > Select interface et la vous verrez votre instance creer biensur si ils sont dans le meme AZ.

4.Différence entre les volumes EBS optimisés pour les IOPS et ceux optimisés pour le débit.

Les volumes EBS optimises poule IOPs sont pour des volumes de grande stockage avec une tres faible latence comme des base de donnees tandis que les volumes EBS debit sont pour des volumes de faible cout de stockage nessistant une charge de travail sequentiel comme des Datawarehouses.

5. Creation d'un snapshot d'un volume EBS et son utilite:

-Aller dans la rubrique : Volume (tout en choisissant le volume desire) > Action > Create Snapshot. Une fois le nom donner valider le.  
Utilisation : Sert a copier des volumes EBS a travers differents AZ pour vouloir ensuite peut-etre vouloir attacher a une instance se trouvant dans une autre AZ.

6- options de redondance disponibles pour les volumes EBS.

Creant un snapshot a partir d'un volume donner

.Creation d'un EBS Snapshot Archive

-Recycle bin pour les EBS snapshots

7- chiffrer un volume EBS pour

-De la console AWS, choisissez le service EC2.

- Sous la section Elastic Block Store choisissez Volumes

-Choisissez "Create Volume"

- Entrez les configuration requise pour votre volume

- Cochez la case de " Encrypt this volume"

- Choisissez la cle KMS a utiliser sous la section " Master Key"

- Et puis valider avec " Create Volume "

8- gérer le cycle de vie d'un volume EBS, de sa création à sa suppression.

On peut utiliser la Amazon Data Lifecycle Manager pour la gestion(creation,retention et la suppression des volumes EBS) et a l'interieure je :

\* Politiques pour definir mes creation de backups en utilisant les default ou custom policy.

\* Policy schedule : definir quand les volumes EBS sont creer par la police

\* Definir un Target resource tags

\* Creer un Snapshot: Pour le back up de mes donnees du volume EBS

\* Amazon Data Lifecycle Manager tags(optionnel)

9- outils AWS pouvez-vous utiliser pour surveiller les performances et la santé d'un volume EBS ?

Amazon CloudWatch

10- Un stockage de type block

C'est un type de stockage utiliser pour stocker des fichiers de donnees sur des reseaux de stockage(SAN) ou des environnement de stockage en cloud fonctionnant sur le principe de block.

11- conditions de creation d'un volume ebs multi – Attach

-le type de volume choisir doit etre : Provisioned IOPS SSD (io1) ou Provisioned IOPS SSD(io2)

- L'option "Enable Multi-Attach " doit etre cocher l'or de la creation du colume

12 - Type de volume EBS a choisir pour une utilisation de 3000 iops et pourquoi ?

Je vous conseille un General Purpose SSD volume de type gp2 car si vous avez besoin de 3000iops ca sous attend que vous connaissez deja votre quantite iops et le volume gp3 offrira donc une consistance de 3000 iops(souvent par default) baseline performance associer a un throughput de 125MiB/s qui sera independant du storage size contrairement au gp2 que je pourrais choisir mais fonctionne sur le burst performance(scale avec le storage size).

Elastic File System (EFS) :

1. Question de cours

1. Qu'est-ce qu'EFS ses principaux avantages par rapport aux options de stockage de fichiers traditionnels :

EFS est un serveless service Amazon donant des fully elastic file storage en vue de partager les donnees en fichier sans avoir a gerer les capacites de stockage ou performance.

Avantages

Ils ont l'avantage d'etre fully elastic et highly scalable

2. Concepts de point de montage dans EFS :

\* Pendant l'opération de montage, vous spécifiez un point de montage [il s'agit du répertoire local sur le client où le système de fichiers EFS est monté et accessible sur le client]. Essentiellement, vous présentez le niveau supérieur/racine du système de fichiers au client ainsi que toutes les données qui s'y trouvent.

\*\* Comment les mount points permettent-ils d'accéder aux fichiers d'un Systeme de fichiers EFS

En utilisant les Amazon EFS access points qui sont des point d'entree specific d'accès au donnee dans un systemes de fichier EFS. Ceci en pouvant utiliser un repertoire racine different pour les systemes de fichiers pour acceder aux fichiers dans des repertoires/sous-repertoies specifiques.

3. EFS gestion de control d'accès

En creant un role IAM qui contiendra les permission requise, EFS pourra gerer et controler l'utilisation d'une application specifique sur un control d'accès specifique.

\*\* Les differents mecanisme disponible

Appliquer une identité utilisateur en utilisant un point d'accès

Appliquer un répertoire racine avec un point d'accès

Modèle de sécurité pour les répertoires racine des points d'accès.

4. class de stockage sur EFS:

\* EFS standard

\* EFS Infrequent Access

5. processus de création et de configuration d'un système de fichiers EFS.

Etape 1 : Configurer les parametre de systeme de fichiers

Etape 2 : Configurer l'accès au reseau

Etape 3 : Creation d'un system de fichier(optionnelle)

Etape 4 : Reconsultation et creation

6. modes de performance pour les systemes de fichiers EFS

\* General performance mode

\* Max I/O performance mode

Ils affectent les performance et les couts en se basant sur les dimension de latence,throughput, and Inpu/Output et sur le type de system de fichier(region ou OneZone)

7. L'adaptation d'EFS automatiquement

EFS s'adapte automatiquement avec le storage capacity de depart poser par l'utilisateur sans aucune interruption et downtime tout en garantissant l'accès a l'espace stockage requise a un moment donnee

Facteur influent son évolutivité

Storage capacity

Throughput

IOPS

compatibilisation avec des systèmes d'exploitation

#### 8. Sauvegarde des données dans un système de fichiers EFS pour récupération

En utilisant AWS Transfer Family and AWS DataSync qui sont des services de sauvegarde entre les Systèmes de fichiers réseau (NFS) en passant par un protocole tel que SFTP à des fins de reprise après sinistre.

#### 9. aspects à prendre en compte pour la sécurité lors de l'utilisation d'EFS ?

- Si les données dans le système de fichiers EFS sont cryptées
- Les personnes ayant été autorisées à utiliser les ressources EFS.
- le contrôle d'accès NFS à l'utilisation du Amazon EFS file system.

\* Atténuer les risques potentiels

L'encryption des données est restée l'ordre de la création d'un Amazon EFS système de fichiers et l'encryption des données en transit l'ordre du montage du système de fichiers

En définissant des permissions IAM sur l'utilisation des ressources EFS.

En utilisant des mécanismes de sécurité de la couche réseau disponibles avec Amazon EC2, tels que les règles de sécurité group VPC et les listes de contrôle d'accès réseau (ACL).

#### 10. Comparaison entre EFS et EBS

Similitudes :

Les deux offrent une grande durabilité

Les mécanismes de Back-ups et d'encryption sont disponibles pour les 2 systèmes

Le coût augmente dans les deux avec une augmentation de provisioned performance

Différences :

les volumes EFS peuvent scaler plus rapidement et automatiquement ce qui n'est pas le cas de EBS qui a une taille définie

EBS est un availability Zone service tandis que EFS est un region service scope

Les volumes EBS sont configurables (en choisissant un SSD, HDD, provision IOPS) tandis que les volumes EFS se basent sur les performances de base.