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 une entité associée à un compte root AWS qui peut 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 donné pour 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 une gestion sur des services gérés et contrôlés par AWS, ce qui est différent du user managed policy qui est géré et contrôlé par les utilisateurs IAM.

    4. Constituants de base d'une policy IAM :

        - 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 différentes variantes de ressources. Dans le cas où l'on veut stocker nos données en utilisant de grosses data sets, on 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, une 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 accédé, l'utilisateur se verra rejeter à un instant

donné de cette MV avec un temps d'avisement limité (L'utilisateur ici est donné une chambre tout en sachant qu'il pourra être éjecté à n'importe quel moment) 1.

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

   Pour des travaux à longue 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 1.

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 informatiques dans divers réseaux à travers internet.

7. Placement group et son utilité :

   Un placement group est un emplacement de stockage d’une ou plusieurs instances EC2 dans une AZ donnée.
   Utilisation : Il sert à former des groupes d'instances EC2 comme dans des étagères de serveur afin qu'ils puissent communiquer (même étant dans des différentes AZ) facilitant l'attribution des rôles.

Elastic Block Store (EBS) :

1. Questions de cours :
    1. EBS et sa fonction principale :

        EBS est un service AWS de création de volumes de type block avec pour fonction principale d'attacher du stockage à une machine virtuelle créée 1.

    2. Différents types de volumes EBS avec leurs caractéristiques :

        - General Purpose (SSD) volumes : moins coûteux avec un mélange équilibré de performance entre la mémoire et la CPU.
        - Throughput Optimized HDD and Cold HDD volumes: favorisent beaucoup la ressource IOPS. Utilisés dans des lourdes charges de travail comme des datawarehouses.
        - Provisioned IOPS SSD : pour des charges de travail élevées et des entrées-sorties élevées nécessitant une faible latence.

    3. Attacher un volume EBS à une instance EC2 :

        - Tout d'abord, le volume est créé avec une capacité et un type défini dans une AZ donnée, en s'assurant qu'il se trouve dans la même AZ que son instance EC2 en allant à Volume > Create Volume > et en validant avec le create volume.
        - Puis sélectionnez ce volume et allez à: Action > Attach Volume > Select interface et là vous verrez votre instance créée bien sûr s'ils sont dans la même AZ 1.

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

   Les volumes EBS optimisés pour les IOPS sont pour des volumes de grande capacité avec une très faible latence comme des bases de données, tandis que les volumes EBS optimisés pour le débit sont pour des volumes de faible coût de stockage nécessitant une charge de travail séquentielle comme des datawarehouses 1.

5. Création d'un snapshot d'un volume EBS et son utilité :

   - Aller dans la rubrique : Volume (tout en choisissant le volume désiré) > Action > Create Snapshot. Une fois le nom donné, validez-le. Utilisation : Sert à copier des volumes EBS à travers différents AZ pour vouloir ensuite peut-être vouloir attacher à une instance se trouvant dans une autre AZ.

6- Options de redondance disponibles pour les volumes EBS :

- Création d'un snapshot à partir d'un volume donné.
- Création d'un EBS Snapshot Archive.
- Corbeille pour les EBS snapshots.

7- Chiffrer un volume EBS :

- De la console AWS, choisissez le service EC2.
- Sous la section Elastic Block Store, choisissez Volumes.
- Choisissez "Create Volume".
- Entrez les configurations requises pour votre volume.
- Cochez la case "Encrypt this volume".
- Choisissez la clé KMS à utiliser sous la section "Master Key".
- Validez avec "Create Volume".

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

On peut utiliser Amazon Data Life cycle Manager pour la gestion (création, rétention et la suppression des volumes EBS). À l'intérieur, je :

- Utilise des politiques pour définir mes créations de sauvegardes en utilisant les politiques par défaut ou personnalisées.
- Planifie des politiques pour définir quand les volumes EBS sont créés.
- Définit des tags de ressources cibles.
- Crée un Snapshot pour la sauvegarde de mes données du volume EBS.
- Utilise des tags Amazon Data Lifecycle Manager (optionnel).

9- Outils AWS que vous pouvez utiliser pour surveiller les performances et la santé d'un volume EBS :

Amazon Cloud Watch.

10- Un stockage de type block :

C’est un type de stockage utilisé pour stocker des fichiers de données sur des réseaux de stockage (SAN) ou des environnements de stockage en cloud fonctionnant sur le principe de block.

11- Conditions de création d’un volume EBS multi-Attach:

- Le type de volume choisi doit être : Provisioned IOPS SSD (io1) ou Provisioned IOPS SSD (io2).
- L'option "Enable Multi-Attach" doit être cochée lors de la création du volume.

12 - Type de volume EBS à choisir pour une utilisation de 3000 IOPS et pourquoi :

Je vous conseille un volume SSD de type gp2 car si vous avez besoin de 3000 IOPS, cela sous-entend que vous connaissez déjà votre quantité d'IOPS et le volume gp3 offre donc une constance de 3000 IOPS (souvent par défaut) avec des performances de base associées à un débit de 125 MiB/s, qui sera indépendant de la taille de stockage, contrairement au gp2 que je pourrais choisir mais qui fonctionne sur les performances burst (évolue avec la taille de stockage).

Elastic File System (EFS) :

1. Question de cours

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

   EFS est un service Amazon sans serveur qui fournit un stockage de fichiers totalement élastique pour partager des données en fichiers sans avoir à gérer les capacités de stockage ou les performances.

   Avantages : Entièrement élastique et hautement évolutif.

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 système de fichiers EFS ?

- En utilisant les points d'accès Amazon EFS, qui sont des points d'entrée spécifiques pour accéder aux fichiers dans un système de fichiers EFS. Cela permet d'utiliser un répertoire racine différent pour les systèmes de fichiers pour accéder aux fichiers dans des répertoires/sous-répertoires spécifiques.

3. Gestion de contrôle d'accès d'EFS :

En créant un rôle IAM qui contient les permissions requises, EFS peut gérer et contrôler l'utilisation d'une application spécifique sur un contrôle d'accès spécifique. Les différents mécanismes disponibles sont :

- 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. Classe de stockage sur EFS :

- EFS standard
- EFS Infrequent Access

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

- Étape 1 : Configurer les paramètres du système de fichiers.
- Étape 2 : Configurer l'accès au réseau.
- Étape 3 : Création d'un système de fichiers (optionnelle).
- Étape 4 : Réexamen et création.

6. Modes de performance pour les systèmes de fichiers EFS :

- General performance mode
- Max I/O performance mode Ils affectent les performances et les coûts en se basant sur les dimensions de latence, de débit et

d'entrée/sortie, ainsi que sur le type de système de fichiers (région ou OneZone).

7. L'adaptation d'EFS automatiquement :

EFS s'adapte automatiquement avec la capacité de stockage définie par l'utilisateur sans aucune interruption ni temps d'arrêt, tout en garantissant l'accès à l'espace de stockage requis à un moment donné.

Facteurs influant sur son évolutivité :

- Capacité de stockage
- Débit
- IOPS
- Compatibilité avec des systèmes d'exploitation

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

En utilisant AWS Transfer Family et AWS DataSync, qui sont des services de sauvegarde entre les systèmes de fichiers réseau (NFS), en passant par un protocole tel que SFTP, dans le but 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 chiffrées.
- Les personnes autorisées à utiliser les ressources EFS.
- Le contrôle d'accès NFS à l'utilisation du système de fichiers EFS. Pour atténuer les risques potentiels :
- Chiffrer les données au repos lors de la création d'un système de fichiers Amazon EFS.

- Définir des autorisations IAM sur l'utilisation des ressources EFS.
- Utiliser des mécanismes de sécurité de la couche réseau disponibles avec Amazon EC2, tels que les règles de groupe de sécurité VPC et les listes de contrôle d'accès réseau (ACL).

10. Comparaison entre EFS et EBS :

- Similitudes :

- Les deux offrent une grande durabilité.
- Des mécanismes de sauvegarde et de chiffrement sont disponibles pour les deux systèmes.
- Le coût augmente dans les deux cas avec une augmentation des performances provisionnées.

- Différences :

- Les volumes EFS peuvent être mis à l'échelle plus rapidement et automatiquement, ce qui n'est pas le cas des volumes EBS qui ont une taille définie.
- EBS est un service de zone de disponibilité, tandis qu'EFS est un service de portée régionale.
- Les volumes EBS sont configurables (en choisissant un SSD, HDD, Provisioned IOPS), tandis que les volumes EFS se basent sur les performances de base.