1. Connexion au Lab

Pour réaliser ce TP chaque binome aura accés à un compte AWS.

- **Les régions AWS dans lesquelles vous allez travailler sont fournies par l'encadrant du TP :**
  - 1 binômes par région (1 VPC par région et par binôme)
  Régions disponibles :
  - us-east-1 : USA Est (Virginie du Nord)
  - us-east-2 : USA Est (Ohio)
  - eu-west-1 : Europe (Irlande)
  - eu-west-2 : Europe (Londres)
  - eu-west-3 : Europe (Paris)
  - eu-central-1 : Europe (Francfort)
- **Pour vous connectez à la console AWS utilisez le fichier founis par l'instructeur pour reccuperer les informations d'identifications .**

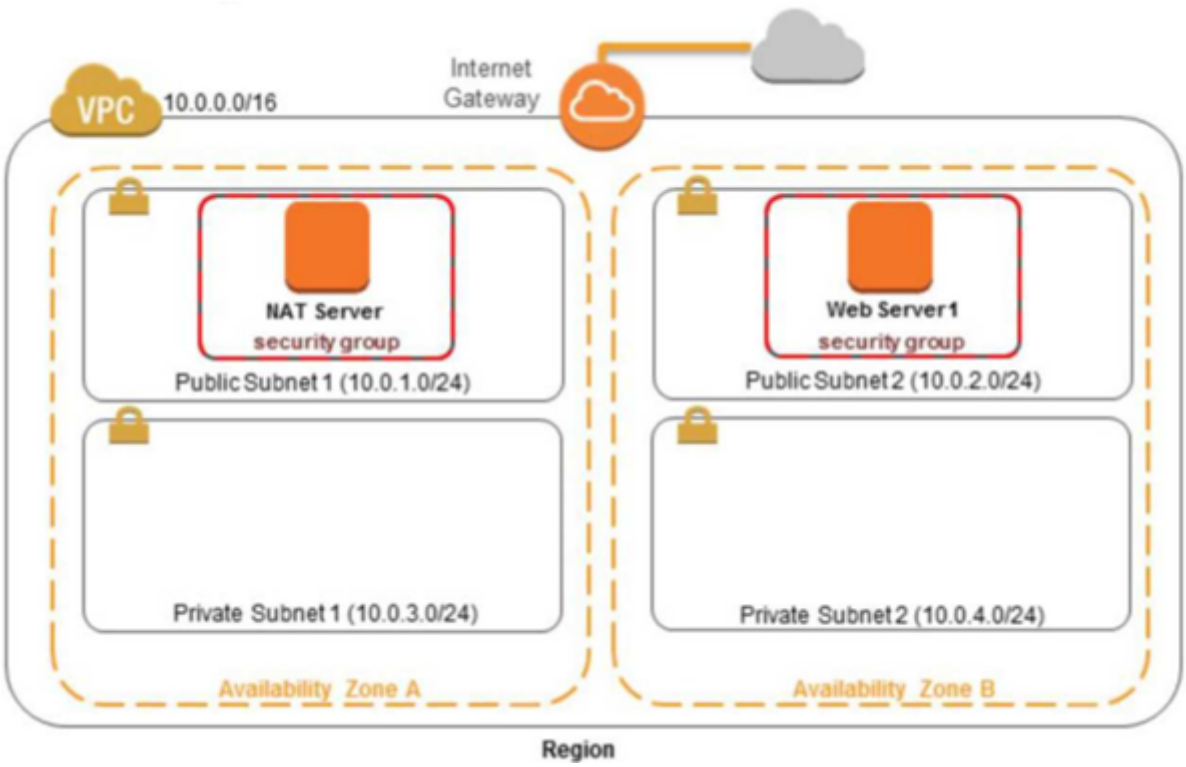
2. 1ère partie - Introduction

Dans ce TP, vous allez créer un VPC complet avec son environnement réseau pour installer un serveur web dans un sous-réseau public puis installer un serveur NAT permettant à un serveur dans un réseau privé d'accéder à internet.

L'architecture finale sera constituée :

- **1 VPC**
- **2 sous-réseaux publics :**
  - **Utilisation de 2 zones de disponibilité différentes**
- **2 sous-réseaux privés**
  - **Utilisation de 2 zones de disponibilité différentes**
- **Configuration de network ACL**
- **Configuration des groupes de sécurité**
- **Création d'un serveur Web**
- **Création d'un serveur NAT**

- Test de fonctionnement du serveur NAT à partir d'un serveur dans le sous réseau privé



2.1. Création du VPC

Sur la console de management, créez un VPC ayant pour *IPv4 CIDR block* 10.0.0.0/16.

· N'utilisez pas l'IPv6 CIDR Block

· Location : par défaut

Pour votre VPC, vérifiez l'activation :

· de la résolution DNS

· des noms d'hôtes DNS

Notez, dans un document (pour mémoire) les identifiants suivants :

· ID du VPC : vpc-**…

· ID de la table de routage principale : rtb-**…

· ID de l'ACL réseau principal : acl-****…

Ils pourront vous servir ultérieurement…

2.2. Création de la passerelle vers internet

Créer une passerelle vers internet (Internet Gateway) puis la rattacher au VPC précédemment créé.

2.3. Création des différents sous-réseaux

Créez deux sous-réseaux privés dans les zones de disponibilité A et B au sein de votre VPC

- **Ces sous-réseaux privés auront pour IPv4 CIDR block**
  - **10.0.3.0/24**
  - **10.0.4.0/24**
- **Désactiver l'attribution automatique d'une adresse IPv4 publique**

Créez deux sous-réseaux publics dans les zones de disponibilité A et B au sein de votre VPC

- **Ces sous-réseaux publics auront pour IPv4 CIDR block**
  - **10.0.1.0/24**
  - **10.0.2.0/24**
  - **Activer l'attribution automatique d'une adresse IPv4 publique**

Observez que les règles de routage par défaut et les règles ACL (firewall) par défaut de chaque sous-réseau correspondent à ceux du VPC.

2.4. Création puis mise à jour des tables de routage par sous-réseau

Créez une table de routage spécifique pour chaque sous-réseau de votre VPC puis rattachez ces tables de routage à chaque sous-réseau.

Mettez à jour les tables de routage des sous-réseaux publics.

- **Rajouter la route par défaut 0.0.0.0/0 vers internet (cible Internet Gateway précédemment créée)**

2.5. Création puis mise à jour de network ACL par ensemble de sous-réseaux

Créer une règle de contrôle d’accès réseau (ACL réseau) pour chaque ensemble de sous-réseaux suivants :

- **Sous-réseaux publics**
- **Sous-réseaux privés**

Rattachez à chaque sous-réseau sa nouvelle règle ACL.

Rajoutez pour chaque network ACL une règle qui permet à tous les flux entrants et sortants de passer de priorité supérieure à la règle par défaut qui refuse tous les flux.

2.6. Création d'un nouveau groupe de sécurité

Configurez un nouveau groupe de sécurité :

- **Pour les instances dans les sous-réseaux publics**
  - **Entrant : Tous les ICMP IPv4, SSH, HTTP et HTTPS depuis n'importe où**
  - **Sortant : Tout le trafic à destination de n'importe où**

- **Pour les instances dans les sous-réseaux privés**
  - **Entrant : SSH et Tous les ICMP – IPV4 : depuis le VPC (10.0.0.0/16)**
  - **Sortant : Tout le trafic à destination de n'importe où**

2.7. Création du serveur web et test d'accès au serveur web

Créez une instance AMI2 (amzn2-ami-kernel-5.10-hvm-2.0.20220912.1-x86_64-gp2) de type t2.micro avec 8 Go de disque SSD standard (GP2 non crypté) en utilisant les images ci-dessous par région :

Configuration (principales) de l'instance :
· Nombre d'instances : 1
· VPC : « votre VPC »
· Sous-réseau : « votre sous-réseau public 2 »
· Reste des paramètres : inchangés
· Groupe de sécurité : « votre groupe de sécurité pour les instances des sous-réseaux publics »
· Paire de clés : choisir la paire de clé existante indiquée au début de l'énoncé

Se connecter à l'instance créée puis y installer un serveur web apache2.

[ec2-user ~]$ sudo yum update -y
[ec2-user ~]$ sudo yum install -y httpd
[ec2-user ~]$ sudo service httpd start
[ec2-user ~]$ sudo chkconfig httpd on

[ec2-user ~]$ sudo groupadd www
[ec2-user ~]$ sudo usermod -a -G www ec2-user
[ec2-user ~]$ sudo chown -R root:www /var/www
[ec2-user ~]$ sudo chmod 2775 /var/www
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} +
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} +

Rajouter les pages web dans le répertoire /var/www/html :
-test.html

```
<!DOCTYPE html> <html> <head> <title>Coucou</title> </head> <body>Cette page est une page toute simple du serveur</body> </html>
```

-ping.html

```
<!DOCTYPE html> <html> <head> <title>Test de ping</title> </head> <body>Si vous lisez cette ligne, le test est réussi !!!</body> </html>
```

Tester le bon fonctionnement des deux pages web depuis votre navigateur via http...

Faites valider votre montage par l'encadrant du TP.

2.8. Création du groupe de sécurité pour la passerelle NAT

Ports entrants et sortants à définir suivant besoins de la passerelle NAT.
o Entrant :
§ Tous les ICMP IPv4 et SSH depuis n'importe où
§ Tout le trafic depuis le groupe de sécurité des sous-réseaux privés
o Sortant :
§ Tout le trafic à destination de n'importe où

2.9. Création d'une instance NAT

Dans le sous-réseau public 1 de la zone de disponibilité A, créez une instance avec une image ami proposant le service NAT (amzn-ami-vpc-nat-2018.03.0.20220419.0-x86_64-ebs) sur une instance de type t2.micro avec 8 Go

de disque SSD standard (GP2 non crypté) en utilisant les images ci-dessous par région :

Configuration (principales) de l'instance :
· Nombre d'instances : 1
· VPC : « votre VPC »
· Sous-réseau : « votre sous-réseau public 1 »
· Reste des paramètres : inchangés
· Groupe de sécurité : « votre groupe de sécurité pour les instances NAT »
· Paire de clés : choisir la paire de clé existante indiquée au début de l'énoncé

Pensez à désactiver les contrôles source/destination pour l'instance NAT.

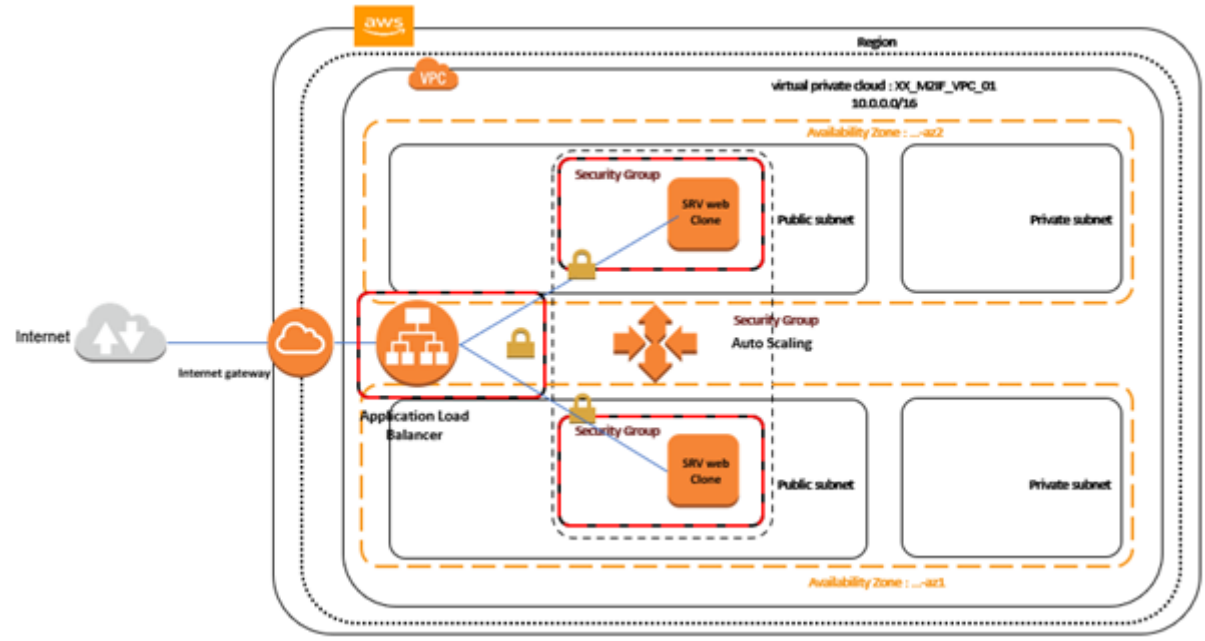
Testez l'instance NAT avec une instance linux de base dans le sous-réseau privé 1 (attention – comment y accéder sans IP publique ???

- Pensez au rebond SSH depuis un serveur accessible dans un sous-réseau public (i.e. : serveur WEB ou serveur NAT à attention mauvaise pratique… il faudrait passer par un serveur BASTION…) – il faudra y uploader la clé SSH privée…
- Pensez à rajouter la route vers internet passant par l'instance NAT à la table de routage du sous-réseau privé

3. 2ème partie - Introduction

Dans cette seconde partie du TP vous allez créer une architecture résiliente et hautement disponible du serveur web précédemment installé.

Le schéma ci-dessous décrit l'architecture globale que vous allez mettre en œuvre.



3.1. Création d'une image du serveur web

Arrêter l'instance du serveur web pour pouvoir en effectuer une image puis créer une image depuis l'instance arrêtée du serveur web. Une fois créée, elle sera disponible dans la rubrique « Images à AMI »

3.2. Création d'une configuration de lancement

A partir de votre image précédente (rubrique « Images à AMI »), créer une configuration de lancement dans la rubrique « Autoscaling à Configurations de lancement » pour une instance de type t2.micro avec 8 Go de disque SSD standard (GP2 non chiffré).

Configuration (principales) de l'instance dans la configuration de lancement :

- Type d'instance : t2.micro
- Configuration supplémentaire : par défaut
- Stockage : par défaut (vérifier 8 Go et SSD à usage général)
- Groupe de sécurité : « votre groupe de sécurité pour les sous-réseaux publics »
- Paire de clés : choisir la paire de clé existante indiquée au début de l'énoncé
- Reste des paramètres : inchangés

3.3. Création d'un groupe d'autoscaling avec l'objectif de maintenir 2 instances du serveur web

En vous appuyant sur la configuration de lancement que vous venez de créer précédemment, créez un groupe d'auto scaling en utilisant les paramètres suivants :

- **Réseau : « votre VPC »**
- **Sous-réseaux : « vos deux sous-réseaux publics »**
- **Aucun équilibreur de charge (pour le moment)**
- **Paramètres par défaut (vérifications de l'état et paramètres supplémentaires)**
- **Taille du groupe :**
  - **Souhaitée : 2**
  - **Capacité minimale : 2**
  - **Capacité maximale : 2**
- **Stratégie de mise à l'échelle :**
  - **Aucune**
- **Protection d'instance contre la mise à l'échelle**
  - **Non activée**
- **Pas de notification**
- **Reste des paramètres : inchangés**

Après la création du groupe d'autoscaling, vérifiez que les 2 instances se sont bien lancées automatiquement.

Testez également le bon fonctionnement du groupe d'autoscaling en :

- **Vérifiant le bon fonctionnement des serveurs web des deux instances**
- **Résiliant une des deux instances et en vérifiant qu'une nouvelle instance est automatiquement créée pour la remplacer.**

3.4. Création d'un équilibreur de charge d'application

Il reste maintenant à créer et configurer l'équilibreur de charge permettant de répartir automatiquement les requêtes à destination du serveur web entre les deux instances dans les deux zones de disponibilité. Pour ce faire, créez un équilibreur de charge :

- **Type d'équilibreur de charge : Application Load Balancer**

- Méthode : accessible sur Internet
- Type d'adressage : IPv4
- Ecouteurs : HTTP ; port 80
- VPC : « votre VPC »
- Sélectionner les deux zones de disponibilité : « les deux AZ de vos sous-réseaux publics »
- Utilisation du groupe de sécurité : celui utilisé pour l'instance WEB ayant permis de créer l'image AMI
- Le reste des paramètres : par défaut

La configuration du groupe cible est la suivante :

- Nouveau groupe cible
- Type de cible : instance
- Protocole HTTP et port 80
- Vérification d'état : HTTP
- Chemin : /ping.html
- Paramètres de vérification des états : garder les valeurs par défaut
- NE PAS ENREGISTRER DE CIBLE A CE NIVEAU

Créez l'équilibreur de charge…

3.5. Rajout du groupe cible dans le groupe d'autoscaling

Pour indiquer à l'autoscaling qu'il correspond à un groupe cible de l'équilibreur de charge, il vous faut modifier le groupe d'autoscaling pour rajouter le groupe cible créé précédemment.

Une fois effectué, vérifiez que les deux instances apparaissent bien comme cibles dans votre groupe cible de l'équilibreur de charge avec un statut : healthy

3.6. Test de l'ensemble du montage

Récupérer le « nom du DNS » de l'équilibreur de charge :

- Ouvrez un navigateur et tester le bon fonctionnement à l'adresse : http://Nom_du_DNS/test.html

Connectez-vous à chacune des deux instances et modifier la page web test.html en y rajoutant un numéro différent pour chaque serveur.

- Testez ensuite le bon fonctionnement de l'équilibreur de charge.

Testez l'auto scaling en résiliant une de vos instances présente dans le groupe d'auto scaling :

- **Testez le bon fonctionnement de l'autoscaling, de l'inscription de la nouvelle instance recréée dans le groupe cible de l'équilibreur de charge.**

Faites valider le fonctionnement du montage global par l'encadrant du TP en réalisant ces manipulations en sa présence.

3.7. Suppression de la configuration (autoscaling et équilibreur de charge)

Cette dernière partie du TP consiste à supprimer les composants de l'architecture que vous venez de créer et de tester.

- **Supprimez du groupe d'autoscaling : vérifiez la suppression automatique des instances associées**
- **Supprimez la configuration de lancement**
- **Supprimer l'image AMI : annuler l'inscription**
- **Supprimez l'équilibreur de charge**
- **Supprimez le groupe cible du load-balancer**
- **Supprimez le serveur web initial**
- **Supprimez le serveur NAT initial**
- **Supprimez vos groupes de sécurité**
- **Supprimez votre VPC global**

Faites valider la suppression de tous les composants par l'encadrant du TP.