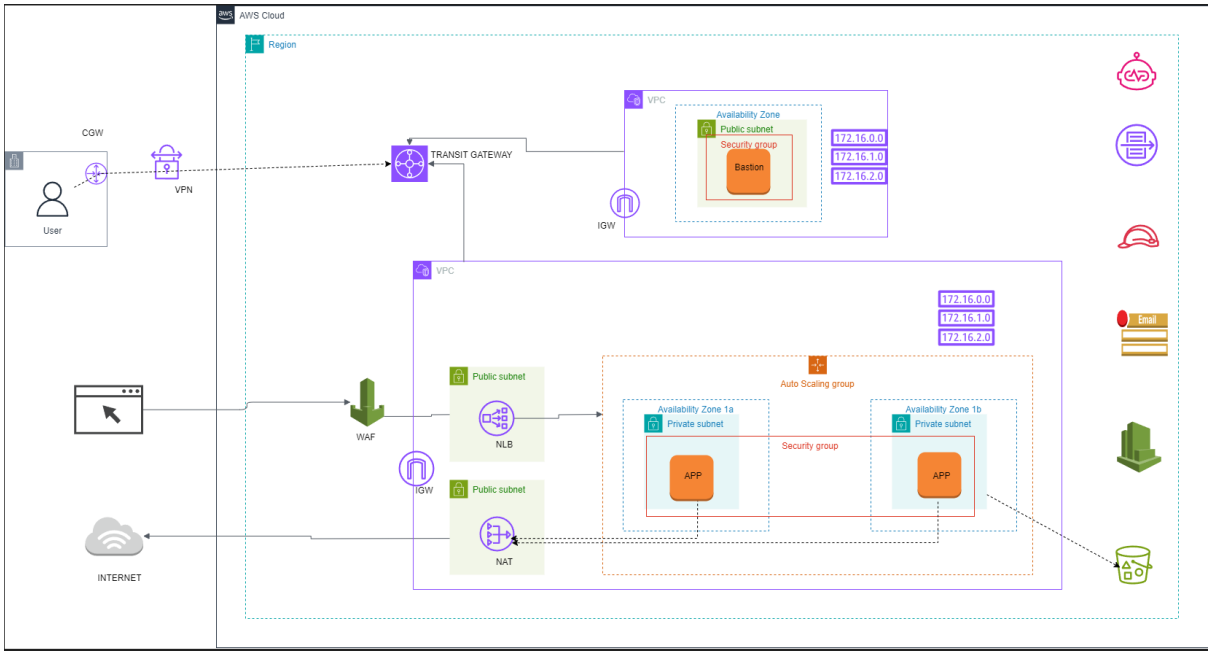
PROJET BOOTCAMP CLOUD ENGINEER AWS

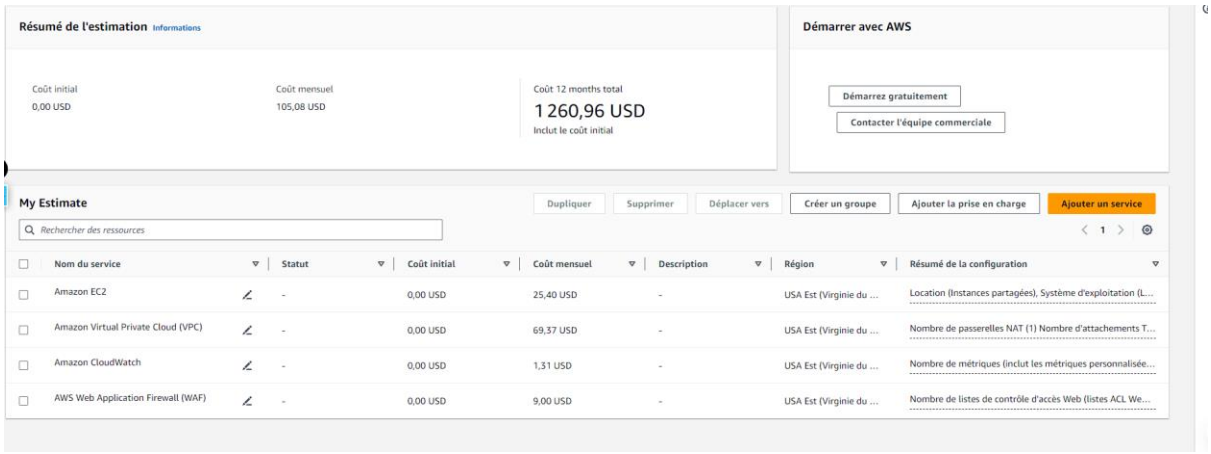
Gestion des réseaux

Objectifs: L’objectifs de ce projet est de mettre en place une architecture réseau cloud robuste et sécurisé au sein de aws

Architecture:



Estimation des couts:



Solution: Mise en place de notre stack sur AWS

Etape 1 : Création du template de l'image

- Allez sur services > ec2 > lancer une instance
- Lancer la création d'une instance avec les paramètres par défauts
- Connectez vous a l'instance et lancer la configuration du serveur
- Utiliser le fichier script.sh fourni

Créer un rôle IAM pour l'accès à Cloudwatch et SSM

Étape 2 : Création des VPC et des sous-réseaux

1. Créer les VPC :
    - Connectez-vous à la console AWS.
    - Allez dans "VPC" et cliquez sur "Create VPC".
    - Créez deux VPC (Virtual Private Cloud) distincts, chacun avec son propre CIDR block (par exemple, 10.0.0.0/16 et 10.1.0.0/16).
2. Créer les sous-réseaux :
    - Dans chaque VPC, créez les sous-réseaux publics et privés nécessaires.
    - Par exemple, pour le premier VPC (10.0.0.0/16) :
        - Sous-réseau public (10.0.1.0/24)
        - Sous-réseau privé (10.0.2.0/24)
    - Répétez l'opération pour le deuxième VPC (10.1.0.0/16) :
        - Sous-réseau public (10.1.1.0/24)
        - Sous-réseau privé (10.1.2.0/24)

    - Allez dans Services > VPC > Your VPCs > Create VPC.
    - Remplissez les informations pour créer le premier VPC :
        - Name tag: VPC1
        - IPv4 CIDR block: 10.0.0.0/16
        - Cliquez sur Create.
    - Répétez l'opération pour le deuxième VPC :
        - Name tag: VPC2
        - IPv4 CIDR block: 10.1.0.0/16
        - Cliquez sur Create.
2. Créer les sous-réseaux :
    - Allez dans Services > VPC > Subnets > Create subnet.
    - Créez les sous-réseaux pour le premier VPC (VPC1) :
        - Name tag: PublicSubnet1
        - VPC: VPC1
        - Availability Zone: Choisissez une zone (ex. us-east-1a)
        - IPv4 CIDR block: 10.0.1.0/24
        - Cliquez sur Create subnet.
        - Name tag: PrivateSubnet1
        - VPC: VPC1
        - Availability Zone: Choisissez une zone (ex. us-east-1a)
        - IPv4 CIDR block: 10.0.2.0/24
        - Cliquez sur Create subnet.
    - Répétez l'opération pour le deuxième VPC (VPC2) :

        - Name tag: PublicSubnet2
        - VPC: VPC2
        - Availability Zone: Choisissez une zone (ex. us-east-1b)
        - IPv4 CIDR block: 10.1.1.0/24
        - Cliquez sur Create subnet.
        - Name tag: PrivateSubnet2
        - VPC: VPC2
        - Availability Zone: Choisissez une zone (ex. us-east-1b)
        - IPv4 CIDR block: 10.1.2.0/24
        - Cliquez sur Create subnet.

Étape 3 : Configurer les tables de routage et les passerelles

1. Ajouter une passerelle Internet (IGW) :
    - Allez dans Services > VPC > Internet Gateways > Create Internet Gateway.
    - Name tag: IGW1
    - Cliquez sur Create Internet Gateway.
    - Sélectionnez IGW1, cliquez sur Actions > Attach to VPC, et choisissez VPC1.
    - Répétez l'opération pour le deuxième VPC :
        - Name tag: IGW2
        - Cliquez sur Create Internet Gateway.
        - Sélectionnez IGW2, cliquez sur Actions > Attach to VPC, et choisissez VPC2.
2. Configurer les tables de routage :
    - Allez dans Services > VPC > Route Tables > Create Route Table.
    - Name tag: PublicRouteTable1
    - VPC: VPC1
    - Cliquez sur Create.
    - Sélectionnez PublicRouteTable1, cliquez sur Routes > Edit routes > Add route :
        - Destination: 0.0.0.0/0
        - Target: Sélectionnez IGW1
        - Cliquez sur Save routes.
    - Sélectionnez PublicRouteTable1, cliquez sur Subnet Associations > Edit subnet associations :
        - Sélectionnez PublicSubnet1
        - Cliquez sur Save.
    - Répétez l'opération pour le deuxième VPC :
        - Name tag: PublicRouteTable2
        - VPC: VPC2
        - Cliquez sur Create.
        - Sélectionnez PublicRouteTable2, cliquez sur Routes > Edit routes > Add route :
            - Destination: 0.0.0.0/0
            - Target: Sélectionnez IGW2
            - Cliquez sur Save routes.
        - Sélectionnez PublicRouteTable2, cliquez sur Subnet Associations > Edit subnet associations :
            - Sélectionnez PublicSubnet2
            - Cliquez sur Save.

3. Créer des NAT Gateways :
    - Allez dans Services > VPC > NAT Gateways > Create NAT Gateway.
    - Subnet: PublicSubnet1
    - Allocation ID: Choisissez une nouvelle adresse IP élastique (Elastic IP).
    - Cliquez sur Create NAT Gateway.
    - Répétez l'opération pour le deuxième VPC :
        - Subnet: PublicSubnet2
        - Allocation ID: Choisissez une nouvelle adresse IP élastique (Elastic IP).
        - Cliquez sur Create NAT Gateway.
    - Allez dans Route Tables et créez des tables de routage pour les sous-réseaux privés :
        - Name tag: PrivateRouteTable1
        - VPC: VPC1
        - Cliquez sur Create.
        - Sélectionnez PrivateRouteTable1, cliquez sur Routes > Edit routes > Add route :
            - Destination: 0.0.0.0/0
            - Target: Sélectionnez le NAT Gateway associé à PublicSubnet1
            - Cliquez sur Save routes.
        - Sélectionnez PrivateRouteTable1, cliquez sur Subnet Associations > Edit subnet associations :
            - Sélectionnez PrivateSubnet1
            - Cliquez sur Save.
        - Répétez l'opération pour le deuxième VPC :
            - Name tag: PrivateRouteTable2
            - VPC: VPC2
            - Cliquez sur Create.
            - Sélectionnez PrivateRouteTable2, cliquez sur Routes > Edit routes > Add route :
                - Destination: 0.0.0.0/0
                - Target: Sélectionnez le NAT Gateway associé à PublicSubnet2
                - Cliquez sur Save routes.
            - Sélectionnez PrivateRouteTable2, cliquez sur Subnet Associations > Edit subnet associations :
                - Sélectionnez PrivateSubnet2
                - Cliquez sur Save.

Étape 4 : Configuration du Transit Gateway

1. Créer un Transit Gateway :
    - Allez dans Services > Transit Gateway > Create Transit Gateway.
    - Name tag: TGW
    - Cliquez sur Create Transit Gateway.
2. Attacher les VPC au Transit Gateway :
    - Allez dans Services > Transit Gateway Attachments > Create Transit Gateway Attachment.
    - Transit Gateway ID: Sélectionnez TGW
    - Attachment type: VPC

- VPC ID: Sélectionnez VPC1
- Subnet IDs: Sélectionnez les sous-réseaux dans VPC1
- Cliquez sur Create attachment.
- Répétez l'opération pour le deuxième VPC :
  - Transit Gateway ID: Sélectionnez TGW
  - Attachment type: VPC
  - VPC ID: Sélectionnez VPC2
  - Subnet IDs: Sélectionnez les sous-réseaux dans VPC2
  - Cliquez sur Create attachment.

Étape 5 : Lancer les instances et configurer le Bastion

1. Lancer une instance Bastion :
   - Allez dans Services > EC2 > Instances > Launch Instance.
   - Name tag: Bastion
   - AMI: Sélectionnez une AMI (par exemple, Amazon Linux 2)
   - Instance type: t2.micro
   - Key pair: Sélectionnez ou créez une clé SSH
   - Network: Sélectionnez VPC1
   - Subnet: Sélectionnez PublicSubnet1
   - Auto-assign Public IP: Enable
   - Cliquez sur Launch.
2. Lancer les instances d'application :
   - Allez dans Services > EC2 > Instances > Launch Instance.
   - Name tag: AppInstance
   - AMI: Sélectionnez une AMI (par exemple, Amazon Linux 2)
   - Instance type: t2.micro
   - Key pair: Sélectionnez ou créez une clé SSH
   - Network: Sélectionnez VPC1
   - Subnet: Sélectionnez PrivateSubnet1
   - Cliquez sur Launch.
   - Répétez l'opération pour PrivateSubnet2 dans VPC2.

Étape 6 : Configurer le Load Balancer et l'Auto Scaling

1. Créer un Network Load Balancer (NLB) :
   - Allez dans Services > EC2 > Load Balancers > Create Load Balancer > Create Network Load Balancer.
   - Name: NLB
   - Scheme: Internet-facing
   - VPC: Sélectionnez VPC1
   - Subnets: Sélectionnez PublicSubnet1 et PublicSubnet2
   - Cliquez sur Next: Configure Routing.
   - Target group: New target group
   - Name: AppTargetGroup
   - Target type: Instance
   - Protocol: TCP
   - Port: 80
   - Cliquez sur Next: Register Targets.

- Sélectionnez les instances d'application et cliquez sur Include as pending below.
- Cliquez sur Create.

2. Configurer les Auto Scaling Groups :
   - Allez dans Services > EC2 > Auto Scaling > Auto Scaling Groups > Create Auto Scaling group.
   - Name: AppAutoScalingGroup
   - Launch configuration: Créez une nouvelle configuration de lancement ou utilisez une existante.
   - Name: AppLaunchConfig
   - AMI: Sélectionnez une AMI (par exemple, Amazon Linux 2)
   - Instance type: t2.micro
   - Cliquez sur Next: Configure details.
   - Auto Scaling group name: AppAutoScalingGroup
   - Group size: Desired: 2, Minimum: 1, Maximum: 3
   - Network: Sélectionnez VPC1
   - Subnet: Sélectionnez PrivateSubnet1 et PrivateSubnet2
   - Cliquez sur Next: Configure scaling policies.
   - Configurez les politiques de mise à l'échelle en fonction des besoins.
   - Cliquez sur Next: Configure notifications et configurez les notifications si nécessaire.
   - Cliquez sur Next: Configure tags et ajoutez les tags si nécessaire.
   - Cliquez sur Review et ensuite sur Create Auto Scaling group.

Étape 7 : Configurer les connexions VPN et le CloudWatch

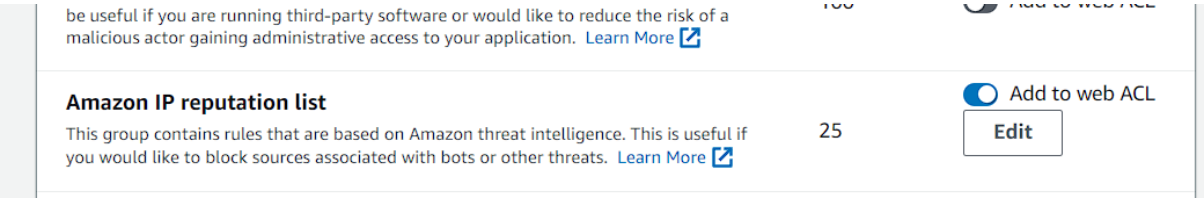
1. Configurer le VPN : (configuration falcultative car necessite une infrstructure on premise)
   - Allez dans Services > VPC > VPN Connections > Create VPN Connection.
   - Name tag: VPNConnection
   - Virtual Private Gateway: Sélectionnez le Virtual Private Gateway créé précédemment.
   - Customer Gateway: Sélectionnez ou créez un nouveau Customer Gateway avec les informations de votre réseau local.
   - Cliquez sur Create VPN Connection.
2. Configurer les alarmes CloudWatch :
   - Allez dans Services > CloudWatch > Alarms > Create Alarm.
   - Sélectionnez les métriques que vous souhaitez surveiller (par exemple, CPU Utilization).
   - Configurez les seuils et les actions en fonction de vos besoins.
   - Cliquez sur Create Alarm.

Etape 8 : configuration de waf

- Allez dans services > WAF > IP Sets > create IP Set
- Donnez un nom
- Choisir la region
- Entrée une adresse ip valide en /32
- Enregistrer

Configuration de la règles

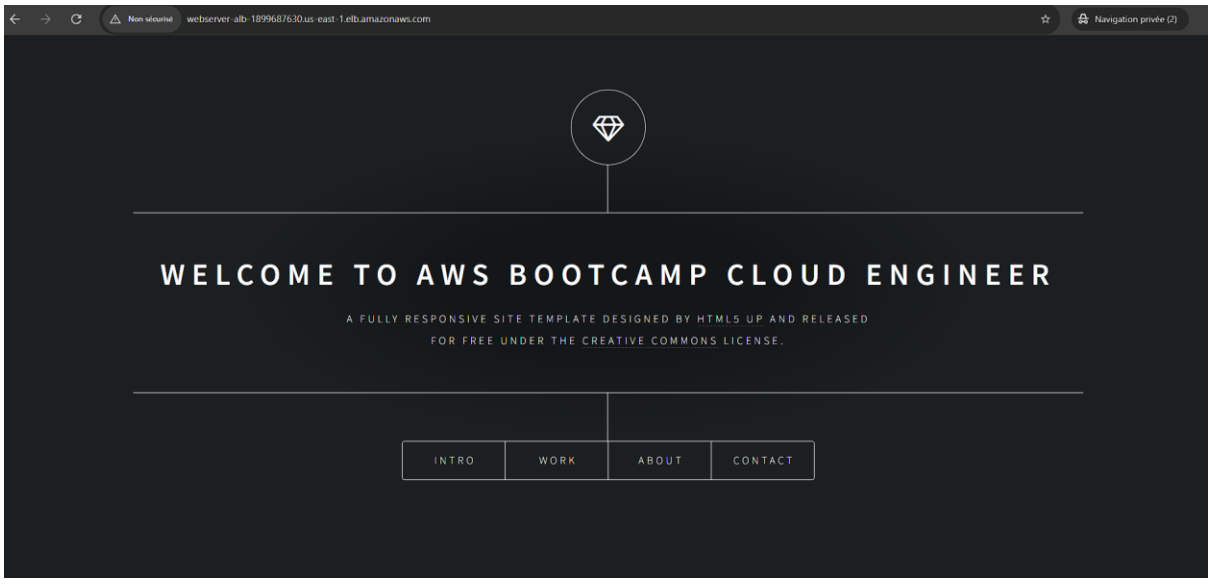
- Revenir sur Web ACLs > Create Web ACLs
- Choisir la region
- Entrez un nom
- Cliquez sur Next
- Cliquez sur Add rules > Managed rule groups > AWSmanaged rule groups
- Choisir Amazon IP reputation list



- Ajouter la regle
- Cliquez sur Add rules > Add my own rules and rule groups > IP Set
- Choisir un nom
- Choisir IP Set deja créer
- Choisir si vous le bloquer ou pas
- Ajouter la règles

Etape 9 : Configuration de la route 53

- Allez sur service > route53 > zones heberges > créer une zone
- Rajouter votre nom de domaine
- Créer un enregistrement
- Laisser les paramètres par défauts
- Utiliser la configuration en Alias afin de cibler votre alb
- Enregistrer
- Puis aller sur votre hébergeur de nom de domaine et rajouter les configurations NS et ainsi le nom de domaine sera rattacher a votre alb



Conclusion

En suivant ces étapes, vous devriez pouvoir configurer l'architecture décrite dans le diagramme en utilisant uniquement l'interface console AWS. Cette configuration comprend la création de VPC, de sous-réseaux, de tables de routage, de passerelles, de NAT Gateways, d'un Transit Gateway, de connexions VPN, de groupes de mise à l'échelle automatique, et de load balancers.