TD3 – Sécurisation réseau AWS avec ALB (architecture 3 tiers)

Objectifs

- Comprendre le rôle d'un Load Balancer dans la sécurité
- Mettre en place une architecture 3 tiers (ALB / backend / DB)
- Contrôler les flux réseau avec les Security Groups
- Éviter l'exposition directe des services internes
- Corriger une infrastructure existante non sécurisée

Contexte

Vous intervenez toujours dans la startup.

L'équipe a amélioré le réseau (VPC, subnets), mais l'application reste mal sécurisée.

Architecture actuelle :

- une instance backend accessible publiquement
- une base de données mal isolée
- aucun point d'entrée centralisé

Un audit impose :

- suppression des accès directs au backend
- mise en place d'un point d'entrée unique
- isolation stricte de la base de données

Objectif technique

Mettre en place une architecture sécurisée :

- Internet → ALB (public)
- ALB → Backend (privé)
- Backend → DB (privé)

Contraintes

- Le backend ne doit plus être accessible depuis Internet
- La base de données ne doit jamais être exposée
- Utiliser uniquement Terraform
- Ne pas casser l'accès à l'application

Infrastructure existante

Fichier : `network/main.tf`

```
provider "aws" {
  region = "eu-west-3"
}

resource "aws_security_group" "backend_sg" {
  name   = "backend-sg"

  ingress {
    from_port   = 80
    to_port     = 80
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

resource "aws_security_group" "db_sg" {
  name = "db-sg"

  ingress {
    from_port   = 5432
    to_port     = 5432
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}
```

Ressources

Fichier : `commandes/terraform.txt`

```
terraform init
terraform plan
terraform apply
terraform destroy
```

1. Compréhension de l’existant

Quels composants sont exposés sur Internet ?

Quels flux sont actuellement autorisés ?

Pourquoi cette architecture fonctionne-t-elle malgré tout ?

Quels sont les risques immédiats ?

2. Analyse des problèmes

Identifier les problèmes de sécurité :

- backend
- base de données

Quelle est la règle la plus critique dans cette configuration ?

Pourquoi ?

3. Mise en pratique – ajout d'un ALB

Objectif :

- introduire un point d'entrée unique

Créer :

- un Security Group pour l'ALB
- autoriser HTTP (80) depuis Internet

Fichier : `network/alb.tf`

```
resource "aws_security_group" "alb_sg" {
  name = "alb-sg"

  ingress {
    from_port   = 80
    to_port     = 80
    protocol    = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }
}
```

Pourquoi l'ALB peut-il être exposé publiquement ?

4. Erreur volontaire – faux sentiment de sécurité

L'ALB est en place.

Mais le backend est toujours accessible directement.

Tester :

- accès via ALB
- accès direct au backend

Peut-on contourner l'ALB ?

Pourquoi est-ce un problème de sécurité ?

5. Correction – sécurisation du backend

Objectif :

- autoriser uniquement le trafic provenant de l'ALB

Modifier le Security Group du backend

Fichier : `network/backend_sg.tf`

```
resource "aws_security_group" "backend_sg" {
  name = "backend-sg"

  ingress {
    from_port       = 80
    to_port         = 80
    protocol        = "tcp"
    security_groups = [aws_security_group.alb_sg.id]
  }
}
```

Pourquoi utilise-t-on un Security Group comme source plutôt qu'une IP ?

6. Correction – sécurisation de la base de données

Objectif :

- autoriser uniquement le backend

Modifier le Security Group de la base de données

Fichier : `network/db_sg.tf`

```
resource "aws_security_group" "db_sg" {
  name = "db-sg"

  ingress {
    from_port       = 5432
    to_port         = 5432
    protocol        = "tcp"
    security_groups = [aws_security_group.backend_sg.id]
  }
}
```

Que se passe-t-il si un attaquant accède au backend ?

Peut-il accéder à la base de données ?

7. Apparition d’un problème

Après sécurisation :

- l’application ne répond plus correctement

Quelles sont les causes possibles ?

Quels éléments faut-il vérifier ?

8. Analyse

Vérifier :

- ports autorisés
- association des Security Groups
- configuration de l’ALB
- health checks

Quel élément est souvent oublié ?

9. Correction

Corriger :

- les règles nécessaires
- la connectivité ALB → backend

10. Extension

Ajouter :

- HTTPS (port 443) sur l’ALB
- redirection HTTP → HTTPS

Pourquoi HTTPS est-il indispensable en production ?

Bonnes pratiques

Pourquoi faut-il :

- un point d'entrée unique ?
- ne jamais exposer le backend ?
- isoler la base de données ?

Challenge final

Objectif :

- seul l'ALB est exposé à Internet
- le backend est accessible uniquement depuis l'ALB
- la base de données est accessible uniquement depuis le backend

Implémenter :

- 3 Security Groups
- règles strictes entre chaque couche

Dessiner les flux réseau autorisés dans votre architecture

Bonus

Ajouter :

- une deuxième instance backend
- configuration du load balancing

Quel est l'intérêt du load balancing en plus de la sécurité ?