

# TD1 - Conception d'une stratégie IAM sécurisée

## Objectifs

- Concevoir une stratégie IAM cohérente
- Appliquer le principe du moindre privilège
- Comprendre les différences entre users, groupes et rôles
- Industrialiser IAM avec Terraform

## Contexte

Vous intervenez comme ingénieur Cloud dans une startup.

L'infrastructure AWS existe déjà, mais aucun cadre de sécurité IAM n'a été défini.

Chaque développeur dispose actuellement de droits administrateur.

Un audit de sécurité impose :

- une refonte complète des accès
- une gestion par rôles
- une limitation stricte des permissions

## Objectif technique

Mettre en place une architecture IAM sécurisée pour :

- les administrateurs
- les développeurs
- les analystes

Le tout doit être :

- reproductible
- versionné
- automatisé avec Terraform

## Contraintes

Vous devez respecter les règles suivantes :

- Aucun utilisateur ne doit avoir de droits administrateur globaux
- Le principe du moindre privilège est obligatoire
- Les permissions doivent être mutualisées (pas de duplication inutile)
- Les accès doivent être compréhensibles et maintenables
- Toute la configuration doit être réalisée avec Terraform

## Ressources

Documentation officielle :

- AWS IAM : concepts (users, groups, roles)
- AWS IAM Policy JSON
- Bonnes pratiques AWS IAM (least privilege)

Commandes utiles :

Fichier : `commandes/terraform.txt`

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

## Travail à réaliser

Vous devez produire une configuration Terraform permettant de :

1. Créer les entités suivantes :
  - 1 groupe Admin
  - 1 groupe Dev
  - 1 groupe Analyst
1. Définir des politiques adaptées :
  - Admin : gestion complète de l'infrastructure
  - Dev : gestion EC2 uniquement
  - Analyst : lecture S3 uniquement
1. Associer correctement :
  - users → groupes
  - groupes → politiques
1. Mettre en place au moins un rôle IAM pour un service AWS

Livrables attendus :

- code Terraform fonctionnel
- structure claire des fichiers
- justification des choix

## Point d'attention (volontaire)

Une mauvaise pratique courante consiste à utiliser :

- Action: "\*"
- Resource: "\*"

Cette pratique est interdite dans ce TD.



Dans quels cas pourrait-on être tenté de l'utiliser ? Pourquoi est-ce dangereux ?

## Phase d'analyse



Quelle est la différence entre :

- un utilisateur IAM
- un groupe IAM
- un rôle IAM

Dans quel cas utiliser chaque élément ?

## Phase de correction

Vous devez revoir votre architecture si :

- un utilisateur a trop de droits
- une policy est trop large
- des permissions sont dupliquées

## Extension

Ajouter :

- une séparation environnement DEV / PROD
- une restriction par ressource (ex : un seul bucket S3)

## Challenge final

Un développeur doit pouvoir :

- lancer une instance EC2
- mais ne pas pouvoir supprimer une instance existante

Implémenter cette contrainte.



Quelle difficulté cela pose-t-il en IAM ?

## Restitution

Vous devez être capable d'expliquer :

- votre architecture IAM
- vos choix de politiques
- les compromis réalisés

From:  
<http://slamwiki2.kobject.net/> - **SlamWiki 2.1**

Permanent link:  
<http://slamwiki2.kobject.net/eadl/bloc4/fm4/td1?rev=1780934413>

Last update: **2026/06/08 18:00**

