

# Sécurité avec AWS : gestion des identités et des accès (IAM)

## Objectifs du projet

Dans ce projet, nous allons nous concentrer sur trois objectifs d'apprentissage :

1. Configurer l'accès sécurisé des utilisateurs dans AWS IAM, y compris la création et la gestion de comptes d'utilisateurs, de groupes et de stratégies
2. Configurez l'accès sécurisé des utilisateurs et gérez les autorisations pour créer des rôles pour l'accès entre comptes et mettre en œuvre les meilleures pratiques
3. Gérez les autorisations dans AWS IAM en configurant des politiques, en reconnaissant les structures de politique et en utilisant des clés de condition pour appliquer des contrôles d'accès granulaires.

### Tâche 1 : Mise en place et présentation du projet

#### Description :

La sécurité est une priorité dans tout environnement cloud. Pour ce projet, j'ai configuré **Multi-Factor Authentication (MFA)** sur le compte utilisateur racine et les utilisateurs IAM pour garantir une protection supplémentaire contre les accès non autorisés.

#### Ce que j'ai fait :

- Activé la MFA sur le compte racine et IAM.
- Utilisé une application MFA (comme Google Authenticator) pour lier le compte.
- Vérifié que la connexion nécessite le code MFA en plus du mot de passe.

#### Compétences acquises :

- Gestion des meilleures pratiques de sécurité pour AWS IAM.
- Utilisation de l'interface AWS pour sécuriser les comptes.

Essayer la nouvelle interface utilisateur de connexion

Découvrez notre nouvelle expérience de connexion à Amazon Web Services améliorée avant son lancement officiel.

Activer une nouvelle connexion



### Authentification multifacteur

Votre compte est sécurisé à l'aide d'une authentification multifacteur (MFA). Pour finir de vous connecter, activez ou affichez votre appareil MFA et saisissez le code d'authentification ci-dessous.


Adresse e-mail : [laurent@amazon.com](mailto:laurent@amazon.com)

Code MFA

Soumettre

[Résoudre les problèmes MFA](#)



 **Captures** : Capture de l'écran affichant l'activation MFA réussie.

---

## Tâche 2 : Création d'un utilisateur IAM à partir de la console

### Description :

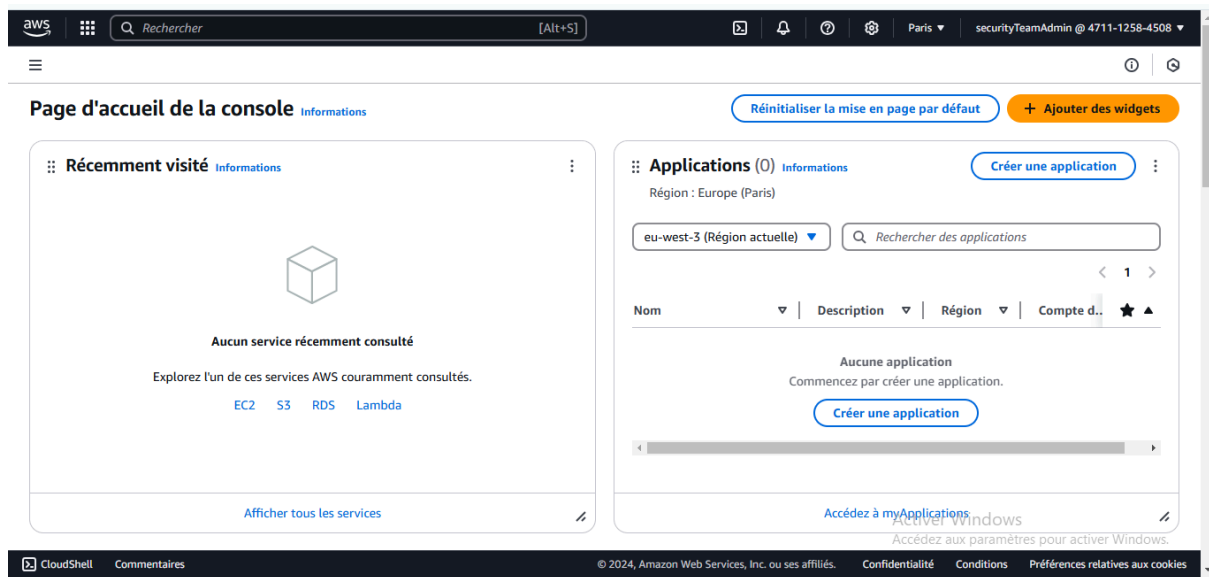
J'ai créé un utilisateur IAM appelé **SecurityTeamAdmin** dans la console AWS avec des autorisations administratives complètes, tout en suivant les bonnes pratiques pour sécuriser les identifiants.

### Ce que j'ai fait :


- Créé un utilisateur IAM avec un accès sécurisé.
- Attribué à la stratégie **AdministratorAccess**.
- Généré un mot de passe sécurisé pour cet utilisateur.

### Compétences acquises :

- Gestion des utilisateurs IAM dans AWS.
- Application des stratégies de sécurité préconçues.



- Aperçu du profil du **SecurityTeamAdmin** -

 **Captures** : Résumé de l'utilisateur IAM créé.

## Tâche 3 : Création d'utilisateurs IAM avec AWS CLI

### Description :

Pour automatiser les tâches IAM, j'ai utilisé AWS CLI pour créer plusieurs utilisateurs et générer des clés d'accès de manière efficace.

### Ce que j'ai fait :

- Configurez l'AWS CLI sur les paramètres régionaux de ma machine.
- Créé les utilisateurs **Matt** , **Sarah** , et **Deborah** via des commandes CLI.
- Automatisé la création d'un utilisateur supplémentaire, **Rachel** , directement depuis la ligne de commande.

### Compétences acquises :

- Maîtrise des commandes CLI pour AWS.
- Gestion rapide des utilisateurs dans AWS.

C:\Windows\system32\cmd.exe

```
C:\Users\HP>aws configure
AWS Access Key ID [*****7H05]: AKIAW3MD7RU6ONMKU2OT
AWS Secret Access Key [*****Yyot]: UH2NQAFha5iZ5vWXz9Z2pi4tH8yr3YLq4jXn+kz
Default region name [eu-west-3]:
Default output format [json]:

C:\Users\HP>aws iam create-user --user-name Matt
{
  "User": {
    "Path": "/",
    "UserName": "Matt",
    "UserId": "AIDAW3MD7RU6MIU5UJDY7",
    "Arn": "arn:aws:iam::471112584508:user/Matt",
    "CreateDate": "2024-11-27T12:58:52+00:00"
  }
}

C:\Users\HP>
C:\Users\HP>aws iam create-user --user-name Sarah
{
  "User": {
    "Path": "/",
    "UserName": "Sarah",
    "UserId": "AIDAW3MD7RU6FGVX2MGJG",
    "Arn": "arn:aws:iam::471112584508:user/Sarah",
    "CreateDate": "2024-11-27T13:00:01+00:00"
  }
}

C:\Users\HP>aws iam create-user --user-name Deborah
{
  "User": {
    "Path": "/",
    "UserName": "Deborah",
    "UserId": "AIDAW3MD7RU6BHGKBSN66",
    "Arn": "arn:aws:iam::471112584508:user/Deborah",
    "CreateDate": "2024-11-27T13:04:57+00:00"
  }
}
```

-Création des utilisateurs **Matt** , **Sarah** , et **Deborah** via des commandes CLI-

 **Captures** : Commandes CLI utilisées et résultats.

---

## Tâche 4 : Création de groupes IAM et ajout d'utilisateurs

### Description :

Pour une meilleure organisation et gestion des permissions, j'ai créé des groupes IAM et attribué des utilisateurs à ces groupes avec des stratégies spécifiques.

### Ce que j'ai fait :

- Créé deux groupes : **AdminGroup** et **CloudSecurityTeam** .

- Assigné des utilisateurs à ces groupes.
- Attaché des stratégies comme **AWSAccountManagementFullAccess** pour AdminGroup et **AmazonS3FullAccess** pour CloudSecurityTeam.

### Compétences acquises :

- Organisation hiérarchique des utilisateurs IAM.
- Gestion des stratégies au niveau des groupes.

```
C:\Users\HP>aws iam add-user-to-group --group-name CloudSecurityTeam --user-name Matt
C:\Users\HP>aws iam add-user-to-group --group-name CloudSecurityTeam --user-name Sarah
```

- Attribution des utilisateurs à ces groupes via CLI-

```
C:\Windows\system32\cmd.exe
C:\Users\HP>aws iam attach-group-policy --group-name CloudSecurityTeam --policy-arn "arn:aws:iam::aws:policy/AmazonS3FullAccess"
C:\Users\HP>
```

- stratégie **AmazonS3FullAccess** pour CloudSecurityTeam via cli -

AdminGroup Infos

Supprimer

Récapitulatif

Modifier

Nom du groupe d'utilisateurs AdminGroup	Heure de création November 27, 2024, 13:14 (UTC)	ARN arn:aws:iam::471112584508:group/AdminGroup
--	---	---

Utilisateurs (2)

Autorisations

Access Advisor

Politiques des autorisations (1) Infos

Simuler

Supprimer

Ajouter des autorisations

Vous pouvez attacher jusqu'à 10 politiques gérées.

Rechercher

Filtrer par Type

Tous les types

< 1 >

<input type="checkbox"/> Nom de la politique	Type	Entités attachées
<input type="checkbox"/> <a href="#">AWSAccountManagementFullAccess</a>	Gérées par AWS	2

Autoriser l'administration

- stratégies **AWSAccountManagementFullAccess** pour "AdminGroup " via console -

**Captures** : Groupes et stratégies attachées dans AWS CLI et console.

## Tâche 5 : Mise en œuvre des politiques IAM

### Description :

J'ai conçu une politique personnalisée pour gérer l'accès des utilisateurs à certains services AWS.

Ce que j'ai fait :

- Créé une politique gérée par le client appelé **IAMReadPolicy** , permettant uniquement l'accès en lecture aux ressources IAM.
- Testé cette politique dans le simulateur IAM pour garantir son efficacité.

Compétences acquises :

- Rédaction et mise en œuvre de politiques JSON pour IAM.
- Débogage des politiques avec le simulateur IAM.

IAMReadPolicy

Infos

lecture

Modifier

Supprimer

Détails de la stratégie

Type	Heure de création	Heure de modification	ARN
Gérées par le client	December 03, 2024, 22:09 (UTC)	December 03, 2024, 22:09 (UTC)	arn:aws:iam::471112584508:policy/IAMReadPolicy

Autorisations

Entités attachées

Balises

Versions de politique

Last Accessed

Autorisations définies dans cette politique

Infos

Copier

Modifier

Récapitulatif

JSON

Les autorisations définies dans ce document de politique précisent les actions autorisées ou refusées. Afin de définir les autorisations d'une identité IAM (utilisateur, groupe d'utilisateurs ou rôle), attachez-lui une politique.

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": [
8         "iam:GenerateCredentialReport",
9         "iam:GetPolicyVersion",
10        "iam:GetAccountPasswordPolicy",
11        "iam:GetMFADevice",
12        "iam:GetServiceLastAccessedDetailsWithEntities",
13        "iam:GenerateServiceLastAccessedDetails",
14        "iam:GetServiceLastAccessedDetails",
15        "iam:GetGroup",
16        "iam:GetContextKeysForPrincipalPolicy",
17        "iam:GetOrganizationsAccessReport",
18        "iam:GetServiceLinkedRoleDeletionStatus",
19        "iam:SimulateCustomPolicy",
20        "iam:SimulatePrincipalPolicy",
21        "iam:GenerateOrganizationsAccessReport"
```

```
C:\Users\HP>aws iam attach-user-policy --user-name SecurityTeamAdmin --policy-arn arn:aws:iam::471112584508:policy/IAMReadPolicy
C:\Users\HP>
```

Identity and Access Management (IAM) > Utilisateurs > securityTeamAdmin

Rechercher sur IAM

Tableau de bord

Gestion des accès

- Groupes d'utilisateurs
- Utilisateurs
- Rôles
- Politiques
- Fournisseurs d'identité
- Paramètres du compte
- Root access management
- Nouveau

Rapports d'accès

- Analyseur d'accès
- Accès externe
- Accès non utilisé
- Paramètres de l'analyseur
- Rapport sur les informations d'identification
- Activité de l'organisation
- Politiques de contrôle des services

securityTeamAdmin Infos

Récapitulatif

ARN  
arn:aws:iam::471112584508:user/securityTeamAdmin

Accès par console  
Activé avec l'authentification MFA

Clé d'accès 1  
AKIAW3MD7RU6ONMKU2OT - Utilisé aujourd'hui. 6 jours à

Création  
November 27, 2024, 12:16 (UTC)

Dernière connexion à la console  
Aujourd'hui

Clé d'accès 2  
Créer une clé d'accès

Autorisations

Groupes (1)

Balises (1)

Informations d'identification de sécurité

Last Accessed

Politiques des autorisations (4)

Les autorisations sont définies par des politiques attachées à l'utilisateur directement ou via des groupes.

Filtrer par Type

Rechercher

Tous les types

<input type="checkbox"/>	Nom de la politique	Type	Attaché via
<input type="checkbox"/>	AdministratorAccess	Gérées par AWS – fonction professionnelle	Directement
<input type="checkbox"/>	AWSAccountManagementFullAccess	Gérées par AWS	Directement, Groupe Admin
<input type="checkbox"/>	IAMReadPolicy	Gérées par le client	Directement
<input type="checkbox"/>	IAMUserChangePassword	Gérées par AWS	Directement

 **Captures :** Politique JSON et résultats de simulation.

## Tâche 6 : Création et gestion d'un compartiment S3

### Description :

J'ai créé un compartiment S3 pour le stockage sécurisé et y ai téléchargé des fichiers via AWS CLI.

### Ce que j'ai fait :

- Créé un compartiment nommé **my-security-team-bucket** .
- Téléchargé deux fichiers dans le compartiment S3 à l'aide de commandes CLI.

### Compétences acquises :

- Gestion des services de stockage AWS.
- Automatisation des actions S3 avec CLI.

```
C:\Users\HP>aws s3api create-bucket --bucket my-security-team-bucket --region eu-west-3 --create-bucket-configuration LocationConstraint=eu-west-3
{
  "Location": "http://my-security-team-bucket.s3.amazonaws.com/"
}
```

- Créer un compartiment nommé **my-security-team-bucket** via CLI-

```
C:\Users\HP>aws s3 ls
2024-11-12 12:57:21 cf-templates--axxq0qi73ofm-eu-west-3
2024-11-07 22:56:58 cf-templates-axxq0qi73ofm-eu-west-3
2024-11-07 23:14:18 codepipeline-eu-west-3-724259557326
2024-11-28 17:48:11 financialdatacompletabc
2024-11-08 02:47:33 morseckbucket
2024-12-03 23:00:00 my-security-team-bucket
2024-11-13 18:09:26 samaybucket
```

- affichage des buckets -

```
C:\Users\HP>aws s3 ls s3://my-security-team-bucket/
PRE fichier1.txt/
PRE fichier2.txt/

C:\Users\HP>
```

-Fichiers existants affichés via CLI .

 **Captures** : Compartiment S3 et fichiers téléchargés.

---

## Tâche 7 : Création d'un rôle IAM pour un service AWS

### Description :

J'ai créé un rôle IAM permettant à une instance EC2 d'accéder à un compartiment S3.

### Ce que j'ai fait :

- Créé une stratégie S3 personnalisée.
- Configuré un rôle appelé **EC2toS3Role** .
- Attaché le rôle à une instance EC2 pour gérer les ressources S3 en toute sécurité.

### Compétences acquises :

- Gestion des autorisations inter-services AWS.
- Sécurisation des accès entre EC2 et S3.



aws [Rechercher] [Alt+S] S3 IAM

IAM > Rôles > Créer un rôle

Étape 1  
● Sélectionner une entité de confiance  
● Ajouter des autorisations  
● **Nommer, vérifier et créer**

### Nommer, vérifier et créer

**Informations du rôle**

**Nom du rôle**  
Saisissez un nom explicite pour identifier ce rôle.  
ec2tos3roles  
64 caractères au maximum. Utilisez des caractères alphanumériques et les caractères « +, -, @, \_ ».

**Description**  
Ajoutez une brève explication de ce rôle.  
Allows EC2 instances to call AWS services on your behalf.  
Nombre maximum de 1000 caractères. Utilisez des lettres (A-Z et a-z), des chiffres (0-9), des tabulations, des nouvelles lignes ou l'un des caractères suivants : \_ +, -, @, / \ | ] # \$ % ^ & \* ( ) , = ' " : ;

**Étape 1 : sélectionner des entités de confiance**

**Politique de confiance**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [

```

Activer Windows  
Accédez aux paramètres pour activer Windows.

- configuration du rôle “EC2toS3Role” -

aws [Rechercher] [Alt+S] Paris securityTeamAdmin @ 4711-1258-4508

Tableau de bord  
Vue globale EC2  
Événements

▼ **Instances**  
Instances  
Types d'instances  
Modèles de lancement  
Demandes Spot  
Savings Plans  
Instances réservées  
Hôtes dédiés  
Réservations de capacité

▼ **Images**  
AMI  
Catalogue des AMI

▼ **Elastic Block Store**

Les options de métadonnées d'instance ont été modifiées pour i-028b1226feb8f49d9. La propagation de ce processus peut prendre quelques minutes.

**Instances (1/5)** Informations  
Date de la dernière mise à jour : il y a 1 minute

Se connecter État de l'instance Actions Lancer des instances

Rechercher Instance par attribut ou identification (case-sensitive)

Name	ID d'instance	État de l'instance
i-028b1226feb8f49d9 (ec2tos3)		

**Détails** Statuts et alarmes

▼ **Résumé de l'instance** Informations

ID d'instance : i-028b1226feb8f49d9

Adresse IPv4 publique : 15.188.76.109 | [adresse ouverte](#)

Adresses IPv4 privées : 172.31.21.116

Accédez aux paramètres pour activer Windows.

Se connecter  
Afficher les détails  
Gérer l'état de l'instance  
Paramètres de l'instance  
Mise en réseau  
Sécurité  
Image et modèles  
Surveiller et dépanner

Modifier les groupes de sécurité  
Obtenir le mot de passe Windows  
Modifier le rôle IAM

```
ubuntu@ip-172-31-21-116:~$ aws s3 ls
2024-11-12 12:57:21 cf-templates--axxq0qi73ofm-eu-west-3
2024-11-07 22:56:58 cf-templates-axxq0qi73ofm-eu-west-3
2024-11-07 23:14:18 codepipeline-eu-west-3-724259557326
2024-11-28 17:48:11 financialdatacompletabc
2024-11-08 02:47:33 morseckbucket
2024-11-13 18:09:26 samaybucket
ubuntu@ip-172-31-21-116:~$
```

**i-028b1226feb8f49d9 (ec2tos3)**

PublicIPs: 15.188.76.109 PrivateIPs: 172.31.21.116

-Attacher le rôle à une instance EC2 pour gérer les ressources S3 en toute sécurité-

 **Captures** : Rôle IAM attaché à l'instance EC2 et commandes exécutées.

---

## Tâche 8-9 : Accès intercomptes AWS avec et sans ID externe

### Description :

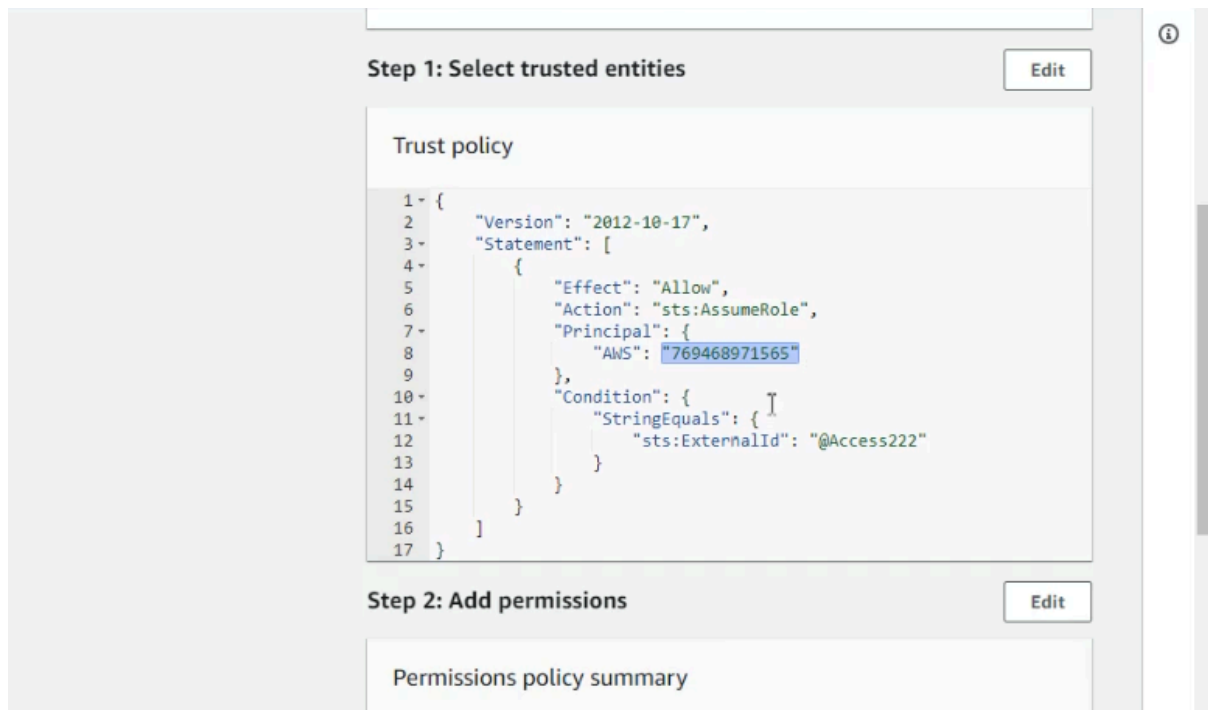
J'ai configuré des rôles pour accorder un accès entre comptes AWS, avec et sans ID externe pour plus de sécurité.

### Ce que j'ai fait :

- Créé un rôle **AuditFinData** pour permettre l'accès intercomptes avec **AmazonS3ReadOnlyAccess**.
- Configurez un rôle avec un **ID externe** pour restreindre l'accès au compte tiers.
- Utilisé **sts:AssumeRole** pour simuler l'accès sécurisé.

### Compétences acquises :

- Configuration des accès intercomptes AWS.
- Utilisation des conditions d'ID externe dans les politiques IAM.



-Utilisation des conditions d'ID externe dans les politiques IAM-

```

C:\Users\Administrator>aws configure
AWS Access Key ID [*****SHGN]: AKIA3GJ7MXIW7JTNHKN6
AWS Secret Access Key [*****Lhlr]: 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
Default region name [us-east-1]: us-east-1
Default output format [text]: text

C:\Users\Administrator>aws sts get-caller-identity
769468971565    arn:aws:iam::769468971565:user/AuditTeamAdmin    AIDA3GJ7MXIW5FXVP4E4P

C:\Users\Administrator>aws s3 ls

C:\Users\Administrator>aws sts assume-role --role-arn arn:aws:iam::962846340211:role/AuditFinDataExtID --role-session-na
me auditdemo

An error occurred (AccessDenied) when calling the AssumeRole operation: User: arn:aws:iam::769468971565:user/AuditTeamAd
min is not authorized to perform: sts:AssumeRole on resource: arn:aws:iam::962846340211:role/AuditFinDataExtID

C:\Users\Administrator>aws sts assume-role --role-arn arn:aws:iam::962846340211:role/AuditFinDataExtID --role-session-na
me auditdemo --external-id @Access222

```

-tentatives d'accès avec un id externe -

```

bIwWSoR8AE42BvPwfyf3AiB5YI76CFge0j44hbGOYFmp8P7rtZKbMpdvsvx89osdJCqfAgik/////////8BEAAaDDk2Mjg0NjM0MDIxMSIM1/OjTEFeW03
gzC/uKvMBs1/eLu0YURNoVbPzhDbbaBadDE8M+j7YQjl9Pu7gM2Vd0hDXyp6NVAp8XikEQULIOgsPDU3BVZEWu1jULEz7hV2w2+kqjz0/zr2Kaw7lcDnhMEE
KE1N4y5n8BMx8xP/PLQVodg5vfMFULCOEZkiZwu00D1xIp1jRiD4xmTCLHU1tbG1PDLnZ8vYo04h+XYLHUMKJUB+PnQIEe2/0ia/MrE10HA6LQyhC+1Lt5nn
P4Jsktk4xGYqCoBMjws1mpuR24QJ2u/CYspT7nLdiurJ9D7jz1KTspoqoT6sJTGvVXdgsq+M3402Qu4QpScLS6YSrR6WAMO3566cGOp4B1N+XONNwn6JdH8k
pbtAxAh19V3UfDU/H1vr2/QHk81I70BgbZwZBvU3QcoV8t1h4fKov4QAv6graBKuUn4XAf5Zv56h13oYsg9077qlj6PQYQG6s75cPEiiW3s3RsGT1GSYZroAG
FRiHxmWJixR5EbQmAAuwKyscW09U5zNT5fYajNoK+kr6hK0i8boZIQ7Knshg9SKfjMGpjsXcNMDc=

C:\Users\Administrator>aws sts get-caller-identity
962846340211    arn:aws:sts::962846340211:assumed-role/AuditFinDataExtID/auditdemo    AROA6ALQSGRZSSYRMOVQ2:auditdemo

C:\Users\Administrator>aws s3 ls
2023-09-08 09:29:52 financialdatacompanyabc

C:\Users\Administrator>

```

- Accès du “ Auditeamadmin “ à la liste des buckets s3 -

 **Captures** : Résultats des bascules de rôle et tentatives d'accès.

## Tâche 10 : Révocation d'un rôle IAM

### Description :

Pour gérer les situations de sécurité critiques, j'ai appris à révoquer un rôle IAM compromis.

### Ce que j'ai fait :

- Détaché toutes les stratégies d'un rôle.
- Supprimé le rôle et vérifié que l'accès au S3 était refusé.

### Compétences acquises :

- Gestion des crises de sécurité dans AWS.
- Révocation efficace des accès compromis.

 **Captures** : Tentative d'accès refusée après révocation.

## Tâche 11 : Définition des limites d'autorisation

### Description :

Pour éviter les abus de privilèges, j'ai défini des limites d'autorisation correspondant aux utilisateurs de modifier leurs propres permissions.

### Ce que j'ai fait :

- Créé une politique appelée **IAMPermissionBoundary** .
- Attribué cette limite à l'utilisateur **James** et testé ses restrictions.

### Compétences acquises :

- Mise en œuvre des limites de permissions dans IAM.
- Prévention des escalades de privilèges.

IAM > Politiques > Créer une politique

① | ②

Étape 1

● Spécifier les autorisations

Étape 2

● **Vérifier et créer**

**Vérifier et créer** [Infos](#)

Vérifier les autorisations, spécifiez les détails et les identifications.

**Détails de la stratégie**

**Nom de la politique**

Saisissez un nom explicite pour identifier cette politique.

128 caractères maximum. Utilisez des caractères alphanumériques, ainsi que les caractères '+', '=', '@', '-', '.'.

**Description – facultatif**

Ajoutez une brève explication de cette stratégie.

1 000 caractères maximum. Utilisez des caractères alphanumériques, ainsi que les caractères '+', '=', '@', '-', '.'.

ⓘ Cette politique définit certaines actions, ressources ou conditions qui ne fournissent pas d'autorisations. Pour accorder l'accès, les politiques doivent avoir une action qui comporte une ressource ou une condition applicable. Pour plus d'informations, choisissez **Afficher les éléments restants**. [En savoir plus](#)

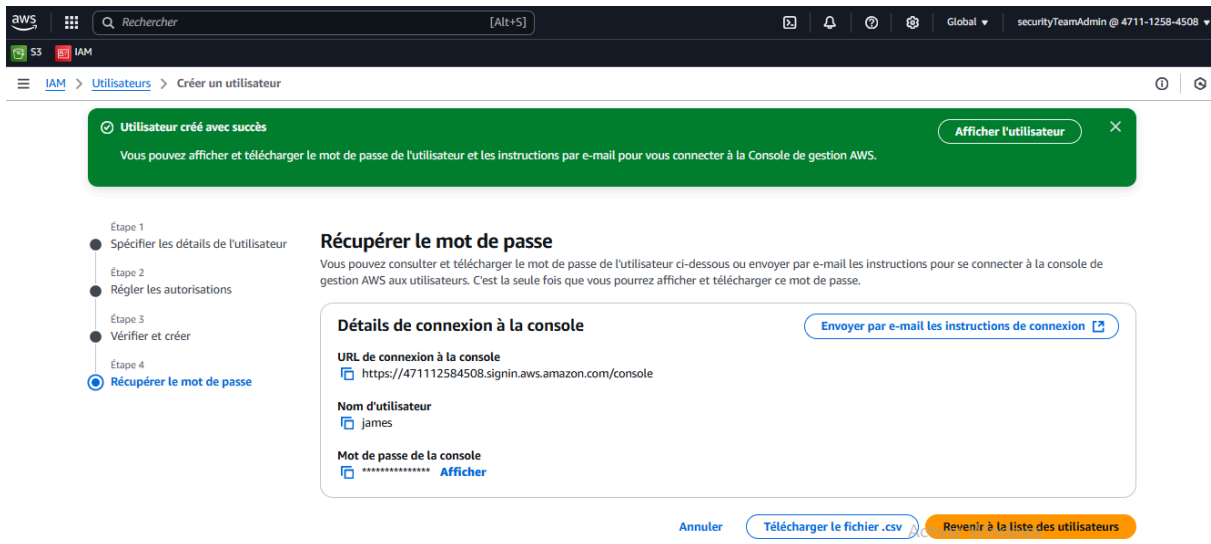
**Autorisations définies dans cette politique** [Infos](#)

Activer Windows

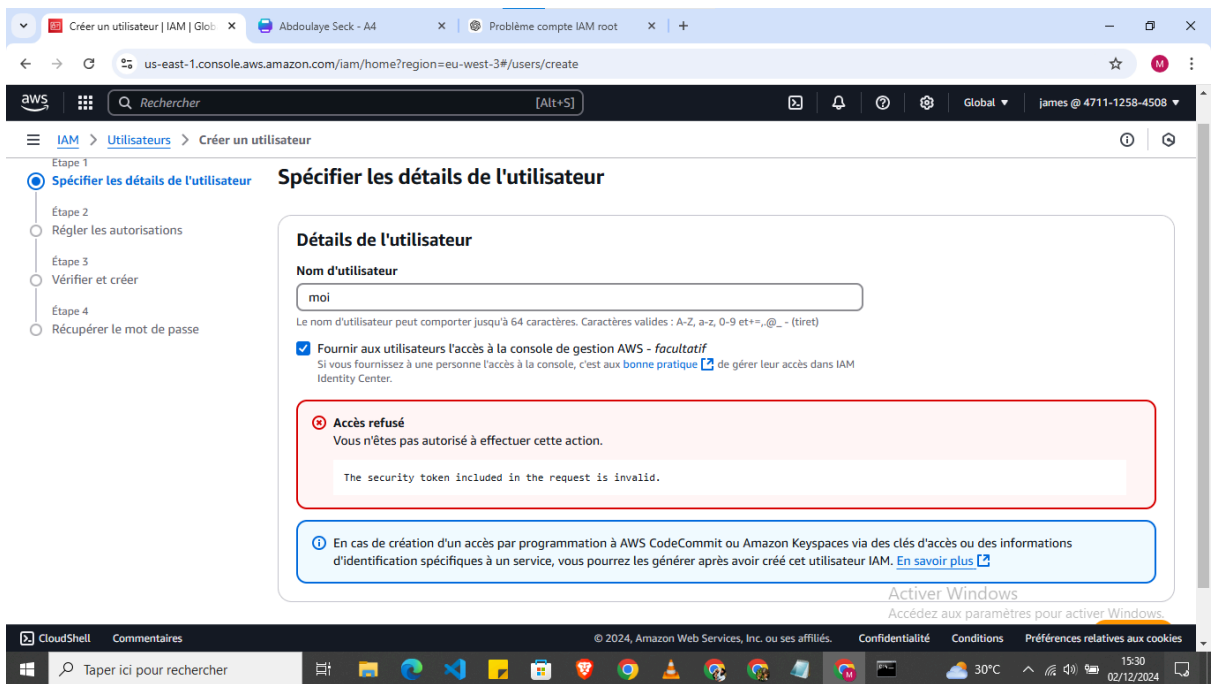
Accédez aux paramètres pour activer Windows.

**Modifier**

-Création de la politique appelée **IAMPermissionBoundary** .-



-Création du profil du user James-



-La limite a été bien appliquée car james ne peut pas créer d'autres users -

📸 **Captures** : Limitée appliquée et testée avec l'utilisateur James.

## Tâche 12 : Débogage avec le simulateur IAM

### Description :

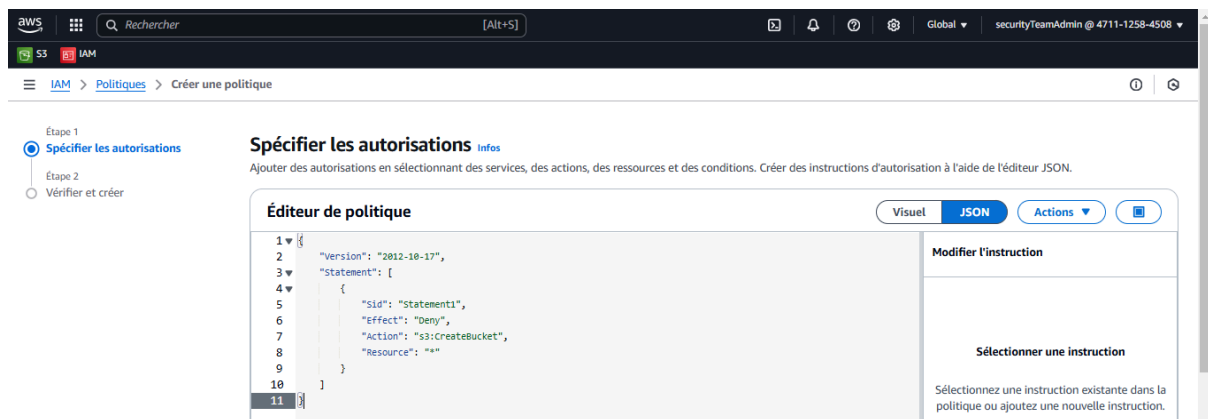
J'ai utilisé le simulateur IAM pour tester et valider mes politiques avant leur mise en production.

## Ce que j'ai fait :

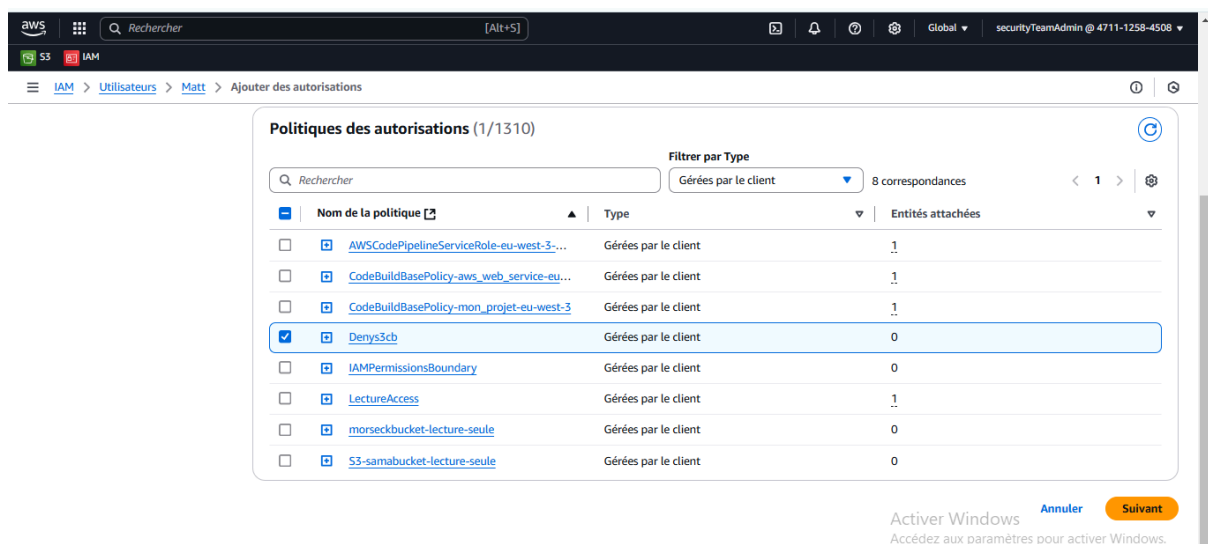
- Créé une politique **DenyS3CreateBucket** pour bloquer la création de nouveaux compartiments S3.
- Simulé les résultats dans le simulateur IAM.

## Compétences acquises :

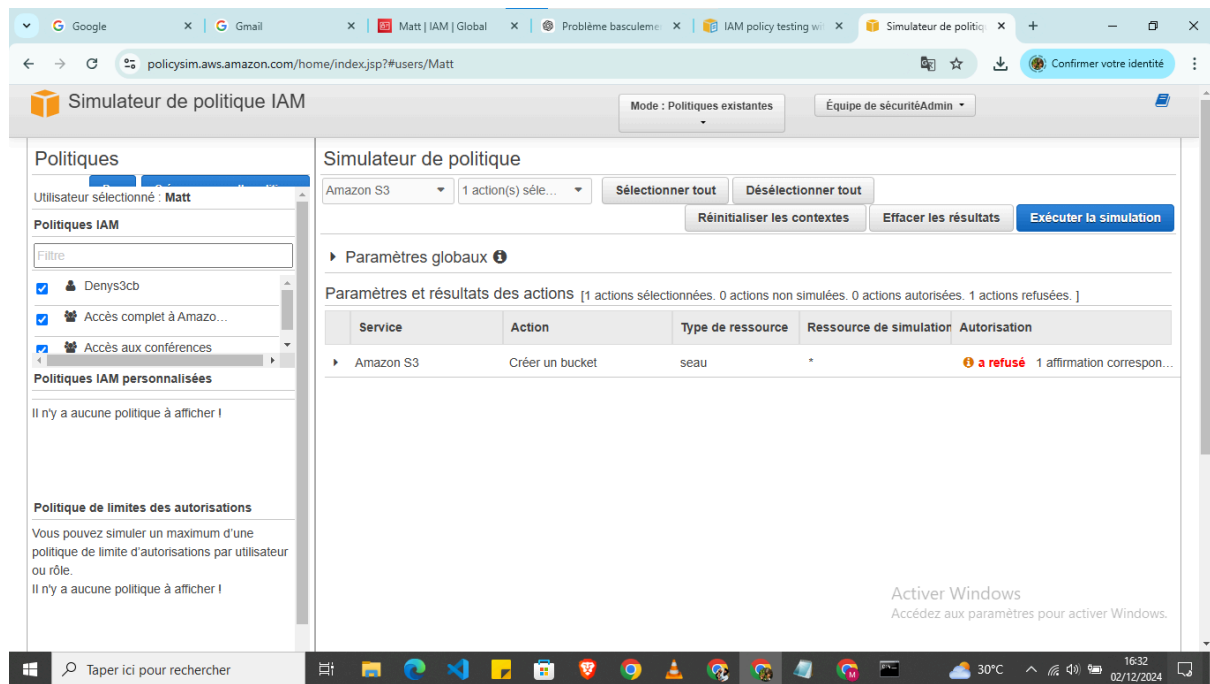
- Débogage avancé des politiques IAM.
- Validation des autorisations avant déploiement.




-Création de la politique **DenyS3CreateBucket** pour bloquer la création de nouveaux compartiments S3.-



-Application de la Politique sur Matt -



-Résultats de la simulation dans le simulateur IAM.-

 **Captures** : Résultats du simulateur pour la stratégie.

## Conclusion

Ces tâches démontrent ma capacité à gérer, sécuriser et automatiser les environnements AWS, tout en appliquant les meilleures pratiques en matière de sécurité cloud. Mon expertise dans IAM et les rôles inter-services/compte font de moi un atout pour toute organisation cherchant à sécuriser ses opérations dans AWS.