

# AWS – IAM

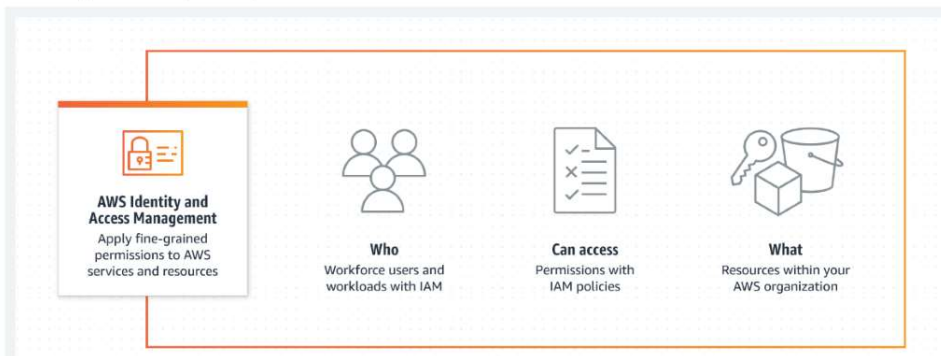
mercredi 15 février 2023 08:33

Formateur : Mohamed AIJJOU

<https://aws.amazon.com/fr/iam/>

## Fonctionnement

AWS Identity and Access Management (IAM) vous permet de contrôler l'accès aux services et aux ressources dans AWS, de gérer de manière centralisée les autorisations précises et d'analyser l'accès pour affiner les autorisations dans AWS.



Exemple d'interface IAM

The screenshot shows the AWS IAM dashboard. On the left is a navigation menu with options like 'Dashboard', 'Access management', 'Access reports', and 'Service control policies (SCPs)'. The main area displays 'IAM dashboard' with 'Security recommendations' (Add MFA for root user, Deactivate or delete access keys for root user, Update your access permissions for AWS Billing, Cost Management, and Account consoles) and 'IAM resources' (User groups: 7, Users: 8, Roles: 69, Policies: 44, Identity providers: 0). A 'What's New' section at the bottom mentions an advanced notice about S3 Block Public Access.

Sécurité : il est important d'utiliser un compte secondaire avec le plus de droit possible plutôt que le compte root, ce compte root ne doit jamais être utilisé

Autre sécurité à mettre en place : MFA

L'authentification multifacteur (MFA) ajoute une couche de protection au processus de connexion. Pour accéder à leurs comptes ou à des applications, les utilisateurs doivent confirmer leur identité, par exemple en scannant leur empreinte ou en entrant un code reçu par téléphone.

Notion d'ARN : [https://docs.aws.amazon.com/fr\\_fr/general/latest/gr/aws-arns-and-namespaces.html](https://docs.aws.amazon.com/fr_fr/general/latest/gr/aws-arns-and-namespaces.html)

## Amazon Resource Names (ARN)

PDF

Les noms ARN identifient de façon unique les ressources AWS. Nous avons besoin d'un ARN lorsque vous devez spécifier une ressource sans ambiguïté dans l'ensemble de ses éléments AWS, par exemple dans les politiques IAM, les balises Amazon Relational Database Service (Amazon RDS) et les appels d'API.

### Format ARN

Voici les formats généraux des ARN. Les formats spécifiques dépendent de la ressource. Pour utiliser un ARN, remplacez le texte en *italique* par les informations spécifiques à la ressource. Sachez que les ARN de certaines ressources omettent la région, l'ID du compte ou la région et l'ID du compte.

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
```

```
arn:aws:ec2:us-east-1:region:account-id:resource-type:resource-id  
arn:partition:service:region:account-id:resource-type:resource-id
```

## Exemples

### Utilisateur IAM

```
arn:aws:iam : 123456789012:user/ johndoe
```

### Rubrique SNS

```
arn:aws:sns : us-east-1 : 123456789012 : example-sns-topic-name
```

### VPC

```
arn:aws:ec2 : us-east-1 : 123456789012:vpc/ VPC-0E9801D129 Exemple
```

Exemple de script des administrateur acces :



Exemple de script global stratégie ec2



Créer un utilisateur :

[IAM](#) > [Utilisateurs](#) > [Créer un utilisateur](#)

Étape 1  
Spécifier les détails de  
l'utilisateur

Spécifier les détails de l'utilisateur

Étape 2  
Régler les autorisations

Étape 3  
Vérifier et créer

### Détails de l'utilisateur

#### Nom d'utilisateur

charles\_b

Le nom d'utilisateur peut comporter jusqu'à 64 caractères. Caractères valides : A-Z, a-z, 0-9 et +, @, \_ - (tiret)

☐ Activer l'accès à la console - *facultatif*

Active un mot de passe qui permet aux utilisateurs de se connecter à la Console de gestion AWS.

📌 Pour un accès par programmation, vous pouvez générer des clés d'accès après avoir créé l'utilisateur. [En savoir plus](#)

### Détails de l'utilisateur

#### Nom d'utilisateur

charles\_b

Le nom d'utilisateur peut comporter jusqu'à 64 caractères. Caractères valides : A-Z, a-z, 0-9 et +, @, \_ - (tiret)

☒ Activer l'accès à la console - *facultatif*

Active un mot de passe qui permet aux utilisateurs de se connecter à la Console de gestion AWS.

#### Mot de passe de la console

☒ Mot de passe généré automatiquement

Vous pouvez afficher le mot de passe après avoir créé l'utilisateur.

☐ Mot de passe personnalisé

Saisissez un mot de passe personnalisé pour l'utilisateur.

• Doit comporter au moins 8 caractères

• Doit inclure au moins trois des types de caractères suivants : lettres majuscules (A-Z), lettres minuscules (a-z), chiffres (0-9) et symboles ! @ # \$ % ^ & \* ( ) \_ + - (trait d'union) = [ ] { } ' "

☐ Afficher le mot de passe

☒ Les utilisateurs doivent créer un nouveau mot de passe lors de la prochaine connexion (recommandé).

Les utilisateurs obtiennent automatiquement la politique [IAMUserChangePassword](#) les autorisant à modifier leur propre mot de passe.

📌 Pour un accès par programmation, vous pouvez générer des clés d'accès après avoir créé l'utilisateur. [En savoir plus](#)

## Régler les autorisations

Ajouter un utilisateur à un groupe existant ou en créer un nouveau. L'utilisation de groupes est une bonne pratique pour gérer les autorisations des utilisateurs par fonctions de tâche. [En savoir plus](#)

### Options d'autorisations

☐ Ajouter un utilisateur à un groupe

Ajouter un utilisateur à un groupe existant ou créer un nouveau groupe. Nous vous recommandons d'utiliser des groupes pour gérer les autorisations utilisateur par fonction de tâche.

☒ Copier les autorisations

Copiez toutes les appartenances à un groupe, les stratégies gérées attachées et les stratégies en ligne à partir d'un utilisateur existant.

☐ Attacher directement des politiques

Attachez une politique gérée directement à un utilisateur. La bonne pratique consiste à attacher des politiques à un groupe à la place. Ensuite, ajouter l'utilisateur au groupe approprié.

Ici on ajoutera notre utilisateur à un groupe : **m2iDevops**

### Adhésion à des groupes d'utilisateurs (1)

Un groupe d'utilisateurs est un ensemble d'utilisateurs IAM. Utilisez des groupes pour spécifier des autorisation

🔄 Supprimer Ajouter un utilisateur aux groupes

☐ Nom du groupe [🔗](#)

☐ m2iDevops

### Détails de l'utilisateur

Nom d'utilisateur

charles\_b

Type de mot de passe de la console

Autogenerated

Demander la réinitialisation du mot de passe

Oui

### Résumé des autorisations

Nom [🔗](#)

▼

Type

▼

Utilisé comme

▼

m2iDevops

Groupe

Groupe d'autorisations

IAMUserChangePassword

Gérées par AWS

Stratégie des autorisations

TP : créer deux utilisateurs et donner à l'un des utilisateur uniquement les droit S3

1ère étape : créer le groupe S3 :

IAM > Groupes d'utilisateurs > project\_bc\_s3

# project\_bc\_s3

## Récapitulatif

Nom du groupe d'utilisateurs	Heure de création
project_bc_s3	February 15, 2023, 10:51

Utilisateurs    **Autorisations**    Access Advisor

**Politiques des autorisations (1)** [Infos](#)  
Vous pouvez attacher jusqu'à 10 politiques gérées.

☐ **Nom de la politique** [↗](#)

☐ **AmazonS3FullAccess**

### Résumé des autorisations

Nom <a href="#">↗</a>	Type	Utilisé comme
project_bc_s3	Groupe	Groupe d'autorisations
<a href="#">IAMUserChangePassword</a>	Gérées par AWS	Stratégie des autorisations

Se connecter avec l'utilisateur et accès à S3 -> OK

Tenter d'accès à IAM -> Accès refusé

Comment créer une stratégie :

## Créer une stratégie

1 2 3

Une stratégie définit les autorisations AWS que vous pouvez attribuer à un utilisateur, un groupe ou un rôle. Vous pouvez créer et modifier une stratégie dans l'éditeur visuel et à l'aide de JSON. [En savoir plus](#)

**Éditeur visuel**    JSON    [Importer une stratégie gérée](#)

[Développer tout](#)    [Réduire tout](#)

Sélectionner un service

Service

Choisir un service

Actions

Choisir un service avant de définir des actions

Ressources

Choisir des actions avant d'appliquer des ressources

Conditions de demande

Choisir des actions avant de spécifier des conditions

[Ajouter des autorisations supplémentaires](#)

Création d'un groupe RDS avec comme contrainte le MFA

IAM > Politiques

**Politiques (1088)** [Infos](#)  
Une politique est un objet dans AWS qui définit les autorisations.

[Effacer les filtres](#)

Nom de la politique

Type

Utilisé comme

Description

☐ **demon2**

Gérées par le client

Aucun

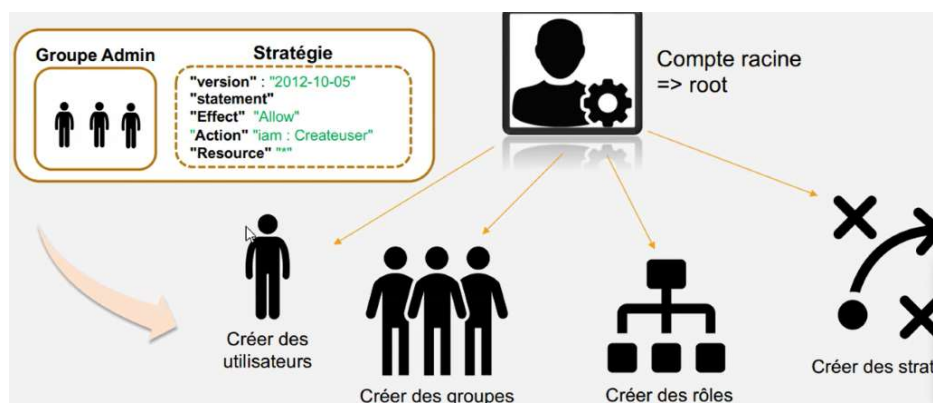
Elle sert à limiter l'accès

## 4 – SERVICE I : Identity and Access Management (IAM)

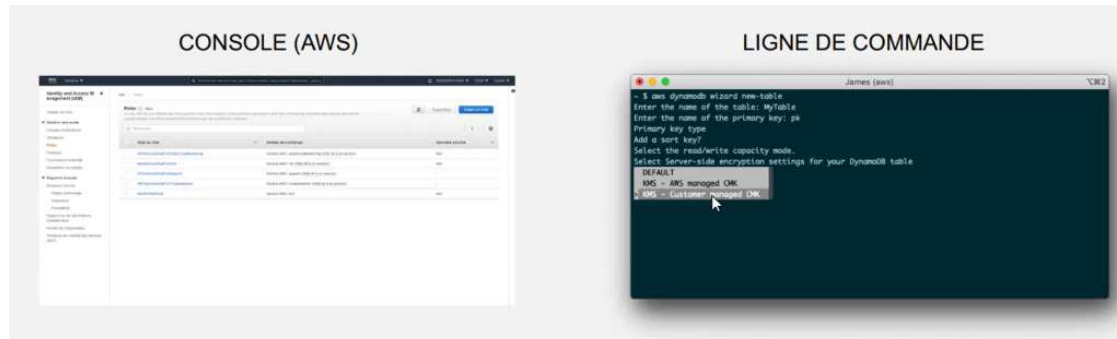


Fonctionnalité IAM :

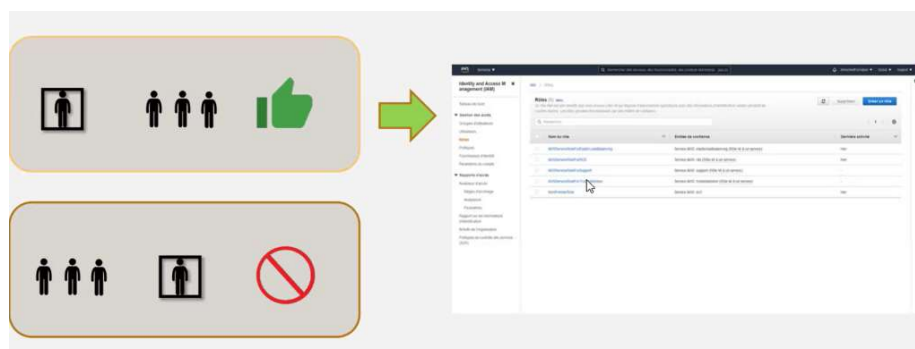
- Centralisation de la gestion des utilisateurs individuelles ou en groupe.
- Sécuriser les utilisateurs grâce au MFA ( Multi-facteurs Authentication).
- Partage de certains accès du compte
- La gestion des permissions de manière très fine.
- La gestion des mots de passe ( rotation, complexité, réinitialisations, etc. )



Interfaces d'opération



Utilisateur et groupe :



Authentification utilisateur :

3 possibilités d'authentification :

- Nom d'utilisateur + mot de passe ( console).
- Clés d'accès (ssh / API) :

```

awscli --help
Last login: Fri Dec 11 10:42:06 on ttys000
b0c856392176:~$ awscli --help
awscli --help

```



- Access Key Id
- Secret Access Key.
- Authentification à multiple facteur :
  - Token matériel.
  - Google Authenticator.

```
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key [None]: 20170601000000000000000000000000
Default region name [None]: us-east-1
Default output format [None]: json
b0e856392176:- adanglics
```



Rôles :

- Un rôle est une stratégie ou un ensemble de stratégie.
- Pour chaque rôle, il faut définir :
  - Une stratégie d'approbation (Trust policy) qui est autorisée à assumer ce rôle par authentification.
  - Une stratégie d'autorisation (Access policy) qui associe les droits au rôle affecté.

### Quand créer un rôle IAM (au lieu d'un utilisateur) :

- Vous créez une application qui s'exécute sur une instance EC2 et cette application fait des requêtes à AWS.
- Vous créez une application qui fonctionne sur un téléphone mobile et qui fait des requêtes à AWS.
- Les utilisateurs de votre entreprise sont authentifiés dans votre réseau d'entreprise et veulent pouvoir utiliser AWS sans avoir à se reconnecter, c'est-à-dire, vous voulez permettre aux utilisateurs de se fédérer dans AWS.

Les stratégies :

### **Détails stratégie sous format JSON**

```
{
  "Statement": [{
    "Effect": "effect",
    "Principal": "principal",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  }]
}
```

## Le Principal :

```
<!-- Tout le monde (utilisateurs anonymes) -->
"Principal": "AWS:*.*"

<!-- Compte ou comptes spécifiques -->
"Principal": { "AWS": "arn:aws:iam::123456789012:root" }
"Principal": { "AWS": "123456789012" }

<!-- Utilisateur IAM individuel -->
"Principal": "AWS:arn:aws:iam:123456789012:user/username"

<!-- Utilisateur fédéré (avec la fédération d'identité web) -->
"Principal": { "Federated": "www.amazon.com" }
"Principal": { "Federated": "graph.facebook.com" }
"Principal": { "Federated": "accounts.google.com" }

<!-- Rôle spécifique -->
"Principal": { "AWS": "arn:aws:iam:123456789012:role/rolename" }

<!-- Service spécifique -->
"Principal": { "Service": "ec2.amazonaws.com" }
```

Stratégie IAM :

## Détails stratégie sous format JSON

```
{
  "Statement": [{
    "Effect": "effect",
    "Principal": "principal",
    "Action": "action",
    "Resource": "arn",
    "Condition": {
      "condition": {
        "key": "value"
      }
    }
  }]
}
```

Les conditions :

**Conditionner l'accès pour une période et à une plage IP**

```
ET {
  "Condition": {
    "DateGreaterThan": { "aws:CurrentTime": "2015-10-08T12:00:00Z" },
    "DateLessThan": { "aws:CurrentTime": "2015-10-08T15:00:00Z" },
    "IpAddress": { "aws:SourceIp": ["192.0.2.0/24", "203.0.113.0/24"] }
  }
}
```

Les bonnes pratiques IAM :

- Protéger vos clés d'accès Utilisateur racine d'un compte AWS
- Créer des utilisateurs IAM individuels
- Utiliser des groupes pour attribuer des autorisations à des utilisateurs IAM
- Appliquer le principe du moindre privilège

- **Accorder le privilège le plus faible**
- **Mise en route avec les autorisations à l'aide des stratégies gérées AWS**
- **Utiliser les stratégies gérées par le client au lieu des stratégies en ligne**
- **Utiliser des niveaux d'accès pour examiner les autorisations IAM**
- **Configurer une stratégie de mot de passe fiable pour vos utilisateurs**
- **Activer MFA**
- **Utiliser des rôles pour les applications qui s'exécutent sur des instances Amazon EC2**
- **Utiliser des rôles pour déléguer des autorisations**
- **Ne pas partager des clés d'accès**
- **Effectuer une rotation régulière des informations d'identification**
- **Supprimer les informations d'identification inutiles**
- **Utiliser les conditions des stratégies pour une plus grande sécurité**
- **Surveillance de l'activité de votre compte AWS**