AWS – IAM

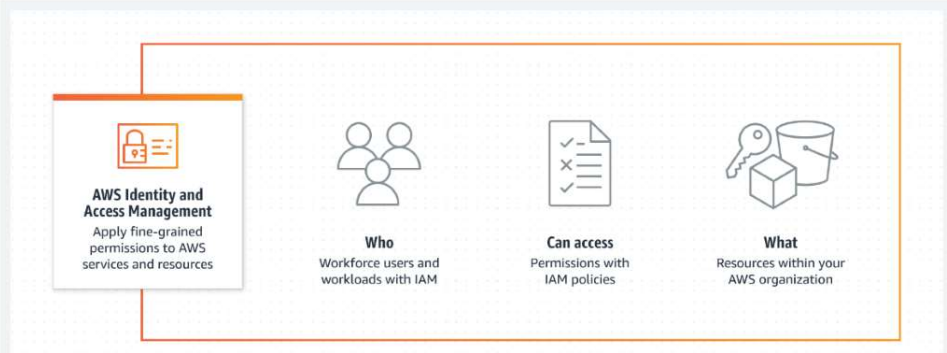
mercredi 15 février 2023 08:33

Formateur : Mohamed AIJJOU

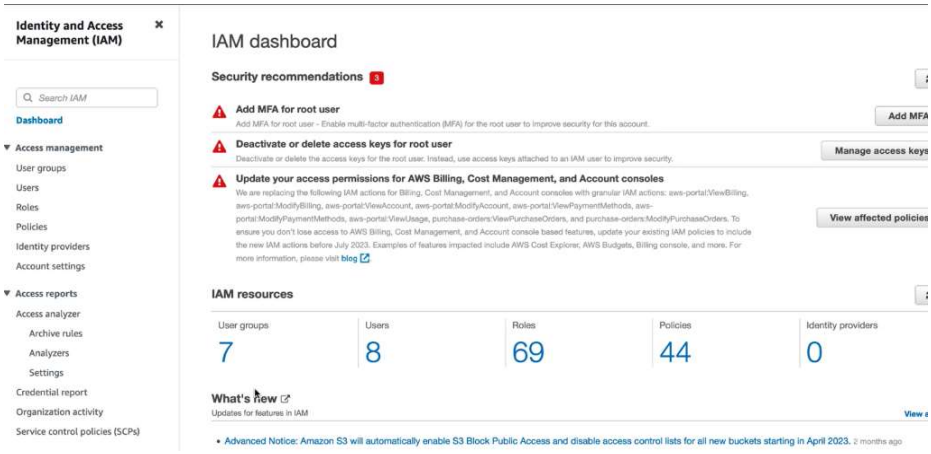
https://aws.amazon.com/fr/iam/

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



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

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 élémentsAWS, 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:partition:service:region:account-id:resource-type:resource-id
```

Exemples

Utilisateur IAM

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

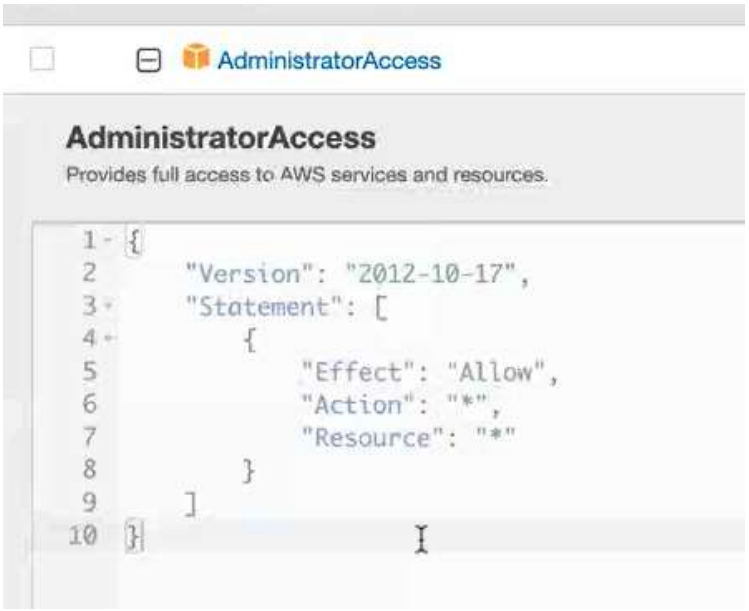
Rubrique SNS

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

VPC

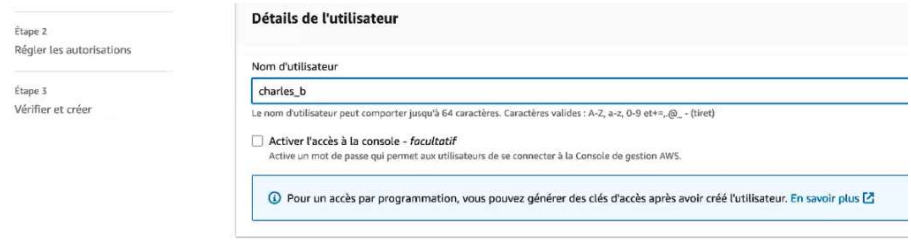
`arn:aws:ec2 : us-east-1 : 123456789012:vpc/ VPC-0E9801D129 Exemple`

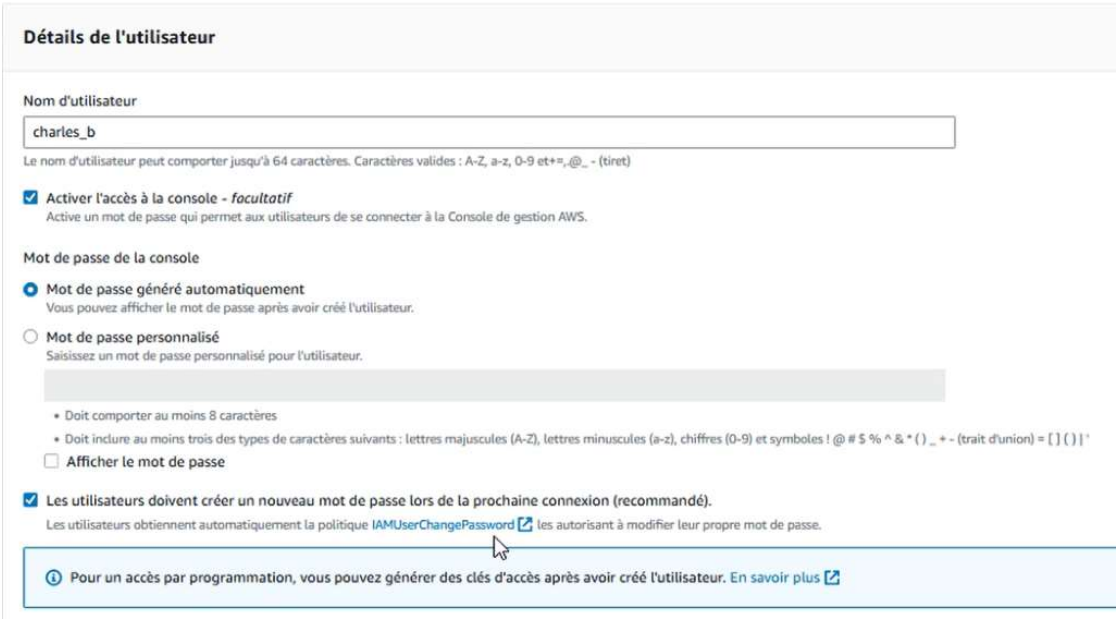
Exemple de script des administrateur acces :



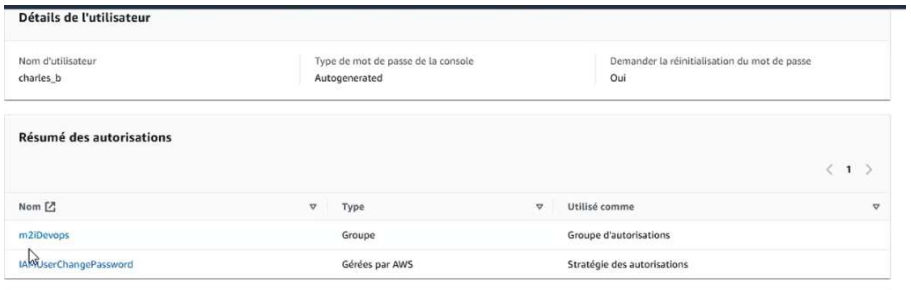
Exemple de script global stratégie ec2

Créer un utilisateur :



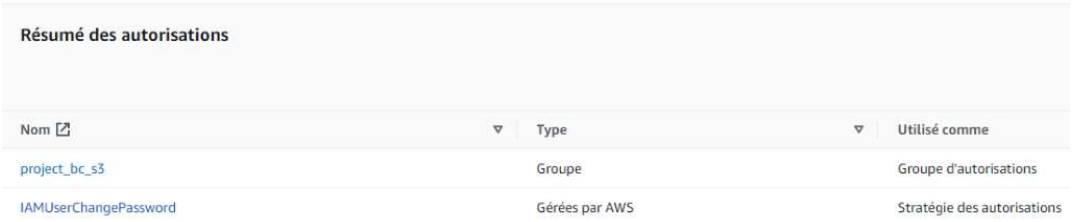


Ici on ajoutera notre utilisateur à un groupe : **m2iDevops**



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

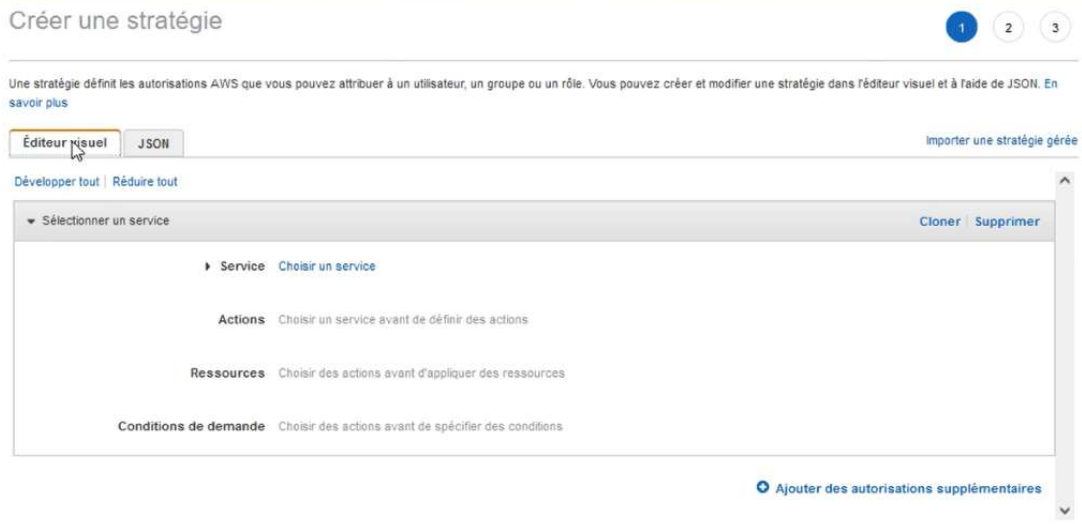
1ère étape : créer le groupe S3 :



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

Tenter d'accès à IAM -> Accès refusé

Comment créer une stratégie :



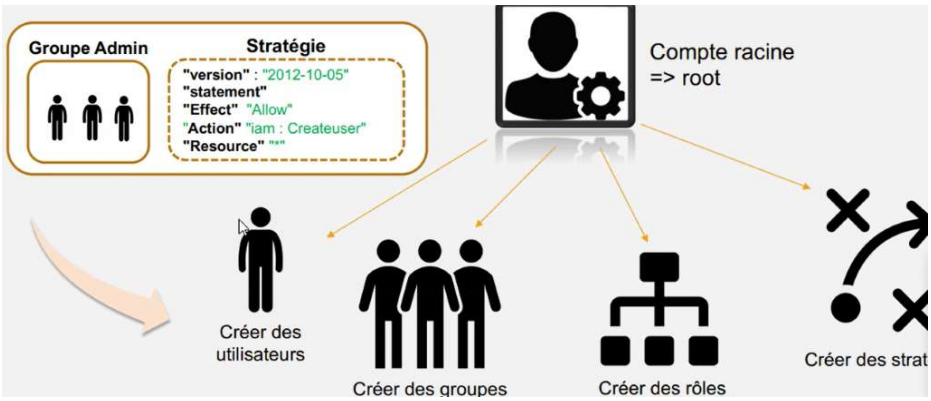
Création d'un groupe RDS avec comme contrainte le MFA

Cours :

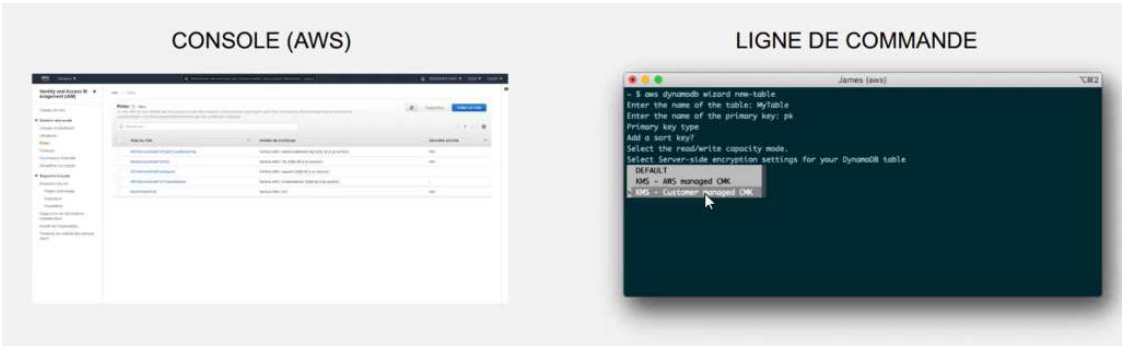
4 – SERVICE 1 : Identity and Access Management (IAM)

Fonctionnalité IAM :

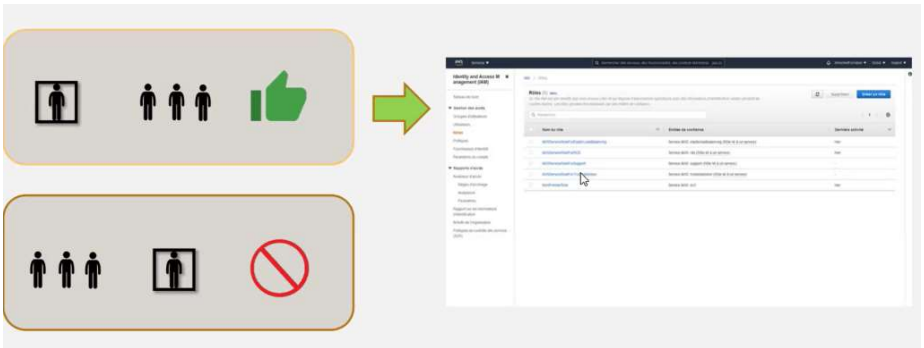
- Centralisation de la gestion des utilisateurs individuelles ou en groupe.
- Sécuriser les utilisateurs grâce au MFA (Multi-facteurs Authentification).
- Partage de certains accès du compte
- La gestion des permissions de manière très fine.
- La gestion des mots de passe (rotation, complexité, réinitialisations,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

- Access Key Id
- Secret Access Key.

- Authentification à multiple facteur :
  - Token matériel.
  - Google Authentificator.

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.
  - Un stratégie d'autorisation (Access policy) qui associe les droits au rôle affecté.

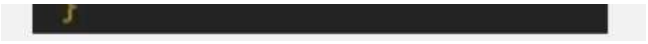
Quand créer un rôle IAM (au lieu d'un utilisateur) :

- *Vous créez une application qui s'exécute sur une instance EC2 et cette application fait des requêtes a 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

```
"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"]}
}
```

ET

OU

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***
- ***Accorder le privilège le plus faible***

- 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