

# Cloud - AWS et Entra ID

---

Marion BORNE

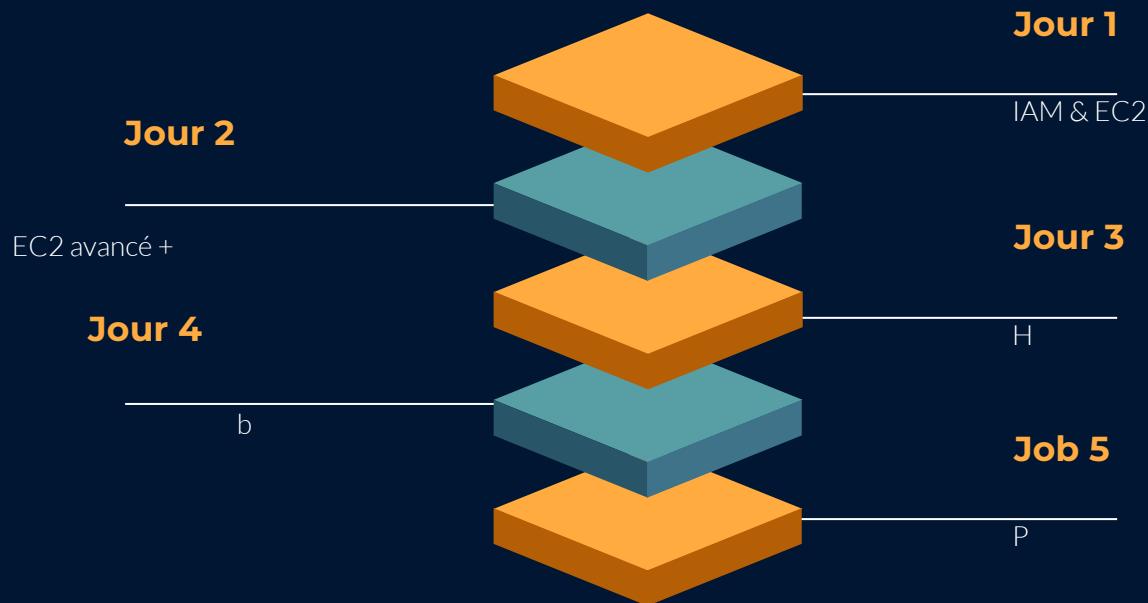
# Qu'est-ce que AWS ?

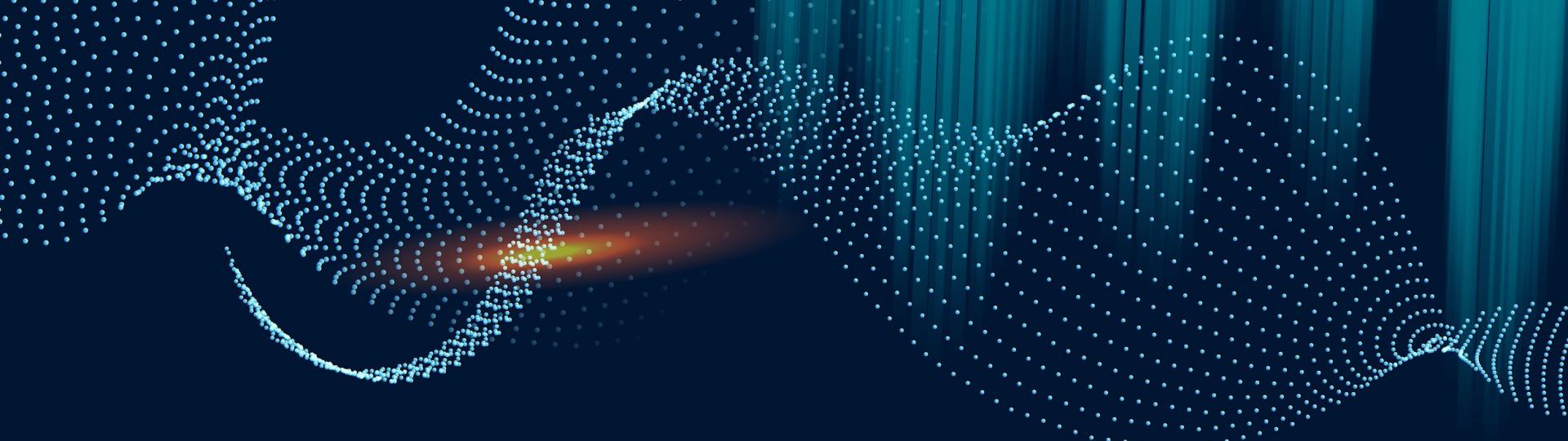
AWS (Amazon Web Services) est une plateforme de services cloud offrant un large éventail de solutions comme :

- Calcul : Services de serveurs virtuels (EC2) ou sans serveur (Lambda).
- Stockage : S3 pour le stockage de fichiers, EBS pour les volumes persistants, Glacier pour l'archivage.
- Bases de données : RDS (relationnelles), DynamoDB (NoSQL), Aurora (performante).
- Réseau : VPC pour les réseaux privés, Route 53 (DNS), CloudFront (distribution de contenu).
- Sécurité : IAM pour la gestion des identités, CloudTrail pour l'audit.
- Analyse : Redshift (data warehouse), EMR (Big Data), Kinesis (flux de données en temps réel).
- IA/ML : SageMaker (machine learning), Rekognition (analyse d'images).
- DevOps : Outils pour automatiser déploiement et gestion (CodePipeline, CloudFormation).

AWS permet aux entreprises de déployer et gérer des applications et ressources de manière flexible et évolutive sans infrastructure physique.

# ETAPES DU PROJET





01

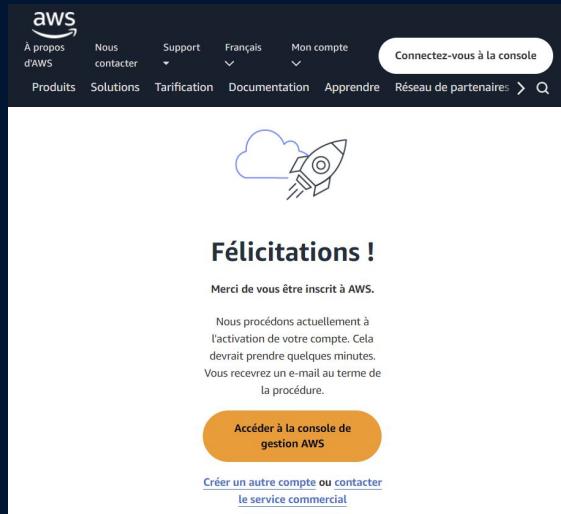
# AWS : IAM et EC2

Xerctvyubino  
extrcyvubin

# Créer un compte AWS

Je commence par créer un compte sur le site AWS (Amazon) en renseignant mes coordonnées bancaires et mes informations personnelles.

Ce compte que je viens de créer est le compte dit RACINE.  
Celui-ci a tous les droits administratifs (root)



# AWS IAM

## (Identify and Access Management)

AWS IAM est un service de gestion des identités et des accès d'Amazon Web Services. Il permet de contrôler qui peut accéder aux ressources AWS et comment ces ressources sont utilisées. Il s'agit d'un composant crucial pour la sécurité de toute infrastructure AWS.

### Principales fonctionnalités d'AWS IAM :

1. **Gestion des utilisateurs :** Créez et gérez des utilisateurs AWS avec des identifiants uniques pour accéder aux services.
2. **Groupes d'utilisateurs :** Organisez les utilisateurs en groupes pour attribuer des permissions de manière collective.
3. **Rôles :** Créez des rôles permettant aux services ou applications d'obtenir des permissions temporaires sans avoir à partager des identifiants.
4. **Politiques IAM :** Documents en format JSON définissant les actions autorisées ou interdites pour chaque utilisateur, groupe ou rôle.
5. **MFA (Authentification Multi-Facteurs) :** Ajoutez une couche supplémentaire de sécurité en demandant un second facteur d'authentification.
6. **Permissions granulaires :** Définissez des permissions spécifiques pour limiter l'accès à certaines actions ou ressources.

**IAM permet une gestion précise des accès, garantissant que les utilisateurs ne disposent que des permissions nécessaires pour accomplir leurs tâches.**

# Principe du moindre privilège

Le principe du moindre privilège stipule que chaque utilisateur, rôle ou service doit disposer du minimum de permissions nécessaires pour accomplir sa tâche, rien de plus. Cela est fondamental pour la sécurité, car cela limite les risques en cas de compromission d'un compte ou d'une mauvaise manipulation.

## Avantages :

- **Réduction des risques :** Limite les dommages en cas d'attaque ou d'erreur humaine.
- **Sécurité renforcée :** Moins de permissions inutiles signifient moins de vecteurs d'attaque.
- **Conformité :** Aide à se conformer aux réglementations de sécurité.

## Bonnes pratiques :

- Utiliser des rôles IAM spécifiques plutôt que des utilisateurs avec des permissions élevées.
- Limiter les permissions en créant des politiques de sécurité très spécifiques.
- Auditer régulièrement les permissions pour s'assurer qu'elles sont toujours nécessaires.
- Activer le MFA pour les comptes ayant des privilèges élevés.

**En respectant le principe du moindre privilège, vous assurez une protection accrue de votre environnement AWS tout en maintenant un accès contrôlé et adapté aux besoins des utilisateurs.**

AWS Services Global marionborne

## Identity and Access Management (IAM)

Rechercher sur IAM

### Tableau de bord

#### Gestion des accès

- Groupes d'utilisateurs
- Utilisateurs
- Rôles
- Politiques
- Fournisseurs d'identité
- Paramètres du compte

## Tableau de bord IAM

### Recommandations de sécurité 1

⚠ Ajouter la MFA pour l'utilisateur racine  
Ajouter la MFA pour l'utilisateur root – Activez l'Authentification multifactorielle (MFA) pour l'utilisateur root afin d'améliorer la sécurité de ce compte.

Ajouter la MFA

# Création utilisateur IAM personnel

1. Je me connecte à AWS avec le compte root.
2. Je vais dans le service IAM depuis la console AWS.
3. Je clique sur Users dans le panneau latéral, puis sur Add user.
4. Je saisis mon nom et prénom sous la forme prénom\_nom.
5. Je sélectionne Programmatic access (si je souhaite accéder via API/CLI) et/ou AWS Management Console access pour un accès via l'interface web.
6. J'assigne le groupe ou les permissions pour votre utilisateur : AdministratorAccess pour avoir les permissions complètes.
7. Je finalise en suivant les instructions pour générer les identifiants d'accès.
8. Je bascule sur le profil de mon utilisateur IAM personnel pour tout le reste des jobs.

**Le service AWS IAM est parfaitement adapté pour cette tâche** car il permet de gérer les utilisateurs, les permissions, et les rôles de manière précise pour un seul compte AWS. L'utilisation de Identity Center (SSO) serait plus appropriée si vous deviez gérer plusieurs comptes AWS ou donner accès à des utilisateurs à des applications différentes avec des identifiants uniques. Mais dans ce cas, pour la gestion des utilisateurs dans un seul compte AWS, IAM est plus simple et direct.

Nom d'utilisateur  
marion\_borne

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

Fournir aux utilisateurs l'accès à la console de gestion AWS - facultatif  
Si vous fournissez à une personne l'accès à la console, c'est une bonne pratique de gérer leur accès dans IAM Identity Center.

**Fournissez-vous à une personne un accès à la console ?**

Type d'utilisateur  
 Spécifier un utilisateur dans Identity Center - recommandé  
Pour accorder à une personne l'accès à la console, nous vous recommandons d'utiliser Identity Center. Grâce à cet outil, vous centralisez la gestion de l'accès des utilisateurs à leurs comptes AWS et à leurs applications cloud.  
 Je souhaite créer un utilisateur IAM  
La création d'utilisateurs IAM est recommandée uniquement en cas de besoin d'accès par programmation à AWS CodeCommit ou Amazon Kinesis via des clés d'accès ou des informations d'identification spécifiques à un service, ou en cas de besoin d'un accès d'urgence à un compte via des informations d'identification de secours.

mari...\_borne [infos](#)

**Récapitulatif**

ARN	arn:aws:iam::043309331246:user/mari..._borne
Création	October 07, 2024, 11:26 (UTC+02:00)
Accès par console	Activé sans l'autentification MFA
Dernière connexion à la console	Jamais

Autorisations   Groups   Balises   Informations d'identification de sécurité   Last Accessed

**Politiques des autorisations (1)**  
Les autorisations sont définies par des politiques attachées à l'utilisateur directement ou via des groupes.

Rechercher	Filtrer par Type	Tous les types
<input type="checkbox"/> Nom de la politique <a href="#">?</a>	<a href="#">▲</a>	Type
<input type="checkbox"/> AdministratorAccess		Généré par AWS - Fonction professionnelle
		Directement

**Connexion d'utilisateur IAM** [?](#)

ID de compte (12 chiffres) ou alias de compte  
043309331246

Nom d'utilisateur IAM  
marion\_borne

Mot de passe  
\*\*\*\*\*

Afficher le mot de passe   Vous rencontrez des problèmes ?

**Connexion**

# Création des autres utilisateurs

Je retourne dans la section Utilisateurs et je clique sur Ajouter un utilisateur : Je créer les utilisateurs suivants avec leurs permissions spécifiques :

- Jeff Bezos : Admin (attribuez la stratégie AdministratorAccess).
- Elon Musk : Admin (attribuez la stratégie AdministratorAccess).
- Mark Zuckerberg : Utilisateur simple (n'attribuez aucune stratégie pour le moment).
- Steve Jobs : Utilisateur simple (n'attribuez aucune stratégie pour le moment).
- Bill Gates : Utilisateur simple (n'attribuez aucune stratégie pour le moment).

Utilisateurs (6) <small>Infos</small>				
<input type="checkbox"/>	Nom d'utilisateur	Chemin	Groupes	
<input type="checkbox"/>	bill_gates	/	0	
<input type="checkbox"/>	elon_musk	/	0	
<input type="checkbox"/>	jeff_bezos	/	0	
<input type="checkbox"/>	marion_borne	/	0	
<input type="checkbox"/>	mark_zuckerberg	/	0	
<input type="checkbox"/>	steve_jobs	/	0	

Politiques des autorisations (1) <small>Infos</small>				
<input type="checkbox"/>	Nom de la politique	Type	Entités attachées	
<input type="checkbox"/>	AdministratorAccess	Gérées par AWS – fonction prof...	4	

# Création des groupes et attribution des utilisateurs

## Création des groupes et attributions :

1. Je vais dans la section Groupes dans IAM.
2. Je clique sur Créer un groupe et suis ces étapes pour chaque groupe :
  - o Nom du groupe : Developers > Permissions : Attachez la stratégie AdministratorAccess.
  - o Nom du groupe : Audit team > Permissions : Attachez la stratégie IAMFullAccess.
  - o Nom du groupe : Operations > Permissions : Attachez la stratégie IAMReadOnlyAccess.
3. J'attribue chaque Utilisateur à son groupe.

**Developers** Infos

**Récapitulatif**

Nom du groupe d'utilisateurs Developers	Heure de création October 07, 2024, 12:12 (UTC+02:00)	ARN arn:aws:iam::043309331246:group/Developers
--	---	---

**Utilisateurs** (1) Autorisations Access Advisor

**Utilisateurs de ce groupe (1)**

Utilisateur	Groupes	Dernière ac...	Heure de cr...
mark_zuckerberg	1	Aucun	Il y a 18 minutes

**Groups d'utilisateurs (3)** Infos

**Groupes d'utilisateurs (3)** Infos

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Groupes d'utilisateurs	Utilisateurs	Autorisations	Heure de création
Audit_team	1	Défini	Maintenant
Developers	1	Défini	Il y a 2 minutes
Operations	1	Défini	Maintenant

# Mise en place MFA

## Créer une politique de mot de passe :

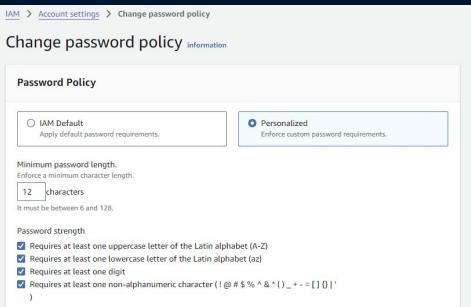
1. Dans la console IAM, accédez à Paramètres du compte dans le panneau de gauche.
2. Cliquez sur Modifier dans la section Politique de mot de passe.
3. Configurez la politique de mot de passe avec les paramètres choisis.
4. Sauvegardez les paramètres de la politique de mot de passe.

## Activer la MFA (Multiple Factor Authentication) sur le compte root :

1. Connectez-vous au compte root (si vous n'y êtes pas déjà connecté).
2. Allez dans IAM, puis dans la section Utilisateurs.
3. Sélectionnez l'utilisateur root (visible dans la section root du panneau IAM).
4. Cliquez sur Sécurité des informations dans le panneau root et activez la MFA.
5. Suivez les instructions pour configurer un appareil MFA :

Dans votre cas, à moins que vous disposiez d'une clé physique de sécurité (FIDO2) ou d'un dispositif TOTP matériel, je vous recommande de choisir l'option "Application d'authentification". Cela vous permet d'utiliser une application mobile telle que Google Authenticator ou Authy, qui est largement utilisée, facile à configurer et suffisamment sécurisée pour la plupart des scénarios. Vous aurez juste besoin de votre smartphone pour générer les codes lors de chaque connexion.

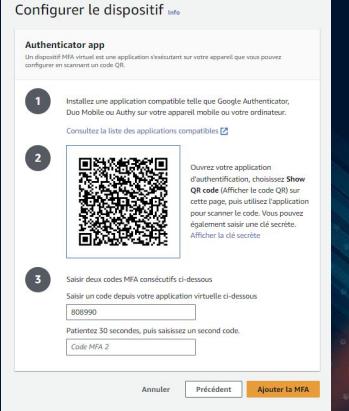
1. Sélectionnez l'option Application d'authentification.
2. AWS vous fournira un code QR à scanner avec l'application.
3. Ouvrez Google Authenticator ou Authy sur votre téléphone et ajoutez un nouveau compte en scannant le code QR.
4. Entrez les deux premiers codes générés pour vérifier la configuration et finaliser l'activation de la MFA.



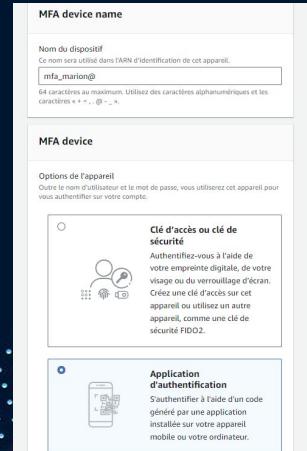
A screenshot of the AWS IAM 'Change password policy' page. It shows two options: 'IAM Default' (radio button not selected) and 'Personalized' (radio button selected). Under 'Personalized', it says 'Enforce custom password requirements.' Below that, there's a 'Minimum password length' section with a dropdown set to '12 characters'. A note says 'It must be between 6 and 128.' Under 'Password strength', there are four checked checkboxes: 'Requires at least one uppercase letter of the Latin alphabet (A-Z)', 'Requires at least one lowercase letter of the Latin alphabet (a-z)', 'Requires at least one digit', and 'Requires at least one non-alphanumeric character (! @ # \$ % ^ & \* ( ) \_ + - = { } | \ )'.



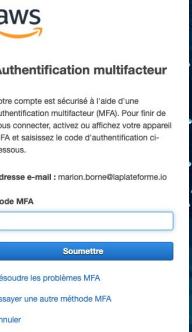
A screenshot of the Google Authenticator app interface. It shows a large colorful 'X' icon made of colored segments (yellow, blue, green, red). Below it, the text 'Google Authenticator' and 'Google' is displayed. Underneath, it says 'N°17 en Utilitaires' with a rating of 4.8 stars and 54.9k reviews. The word 'Gratuit' (Free) is also visible.



A screenshot of the 'Authenticator app' configuration step in the AWS IAM process. Step 1: 'Installlez une application compatible telle que Google Authenticator, Duo Mobile ou Authy sur votre appareil mobile ou votre ordinateur.' Step 2: 'Ouvrez votre application d'authentification, choisissez Show QR code (Afficher le code QR) sur cette page, puis utilisez l'application pour scanner le code. Vous pouvez également saisir une clé secrète. Afficher la clé secrète' with a QR code shown. Step 3: 'Saisir deux codes MFA consécutifs ci-dessous' with fields for 'Saisir le code depuis votre application virtuelle ci-dessous' (containing '808990') and 'Patientez 30 secondes, puis saisissez un second code.' (containing 'Code MFA 2').



A screenshot of the 'MFA device' configuration steps. Step 1: 'Nom du dispositif' (Device name) with input field 'mfa\_marijon@'. Note: 'Ce nom sera utilisé dans l'ARN d'identification de cet appareil.' Step 2: 'Options de l'appareil' (Device options) with note: 'Dès le nom d'utilisateur et le mot de passe, vous utiliserez cet appareil pour vous authentifier sur votre compte.' It shows two options: 'Gé d'accès ou clé de sécurité' (with a note about using biometric authentication or a physical key) and 'Application d'authentification' (with a note about using a mobile app like Google Authenticator).



A screenshot of the 'Authentification multifactor' summary page. It shows the AWS logo and the heading 'Authentification multifactor'. It says 'Votre compte est sécurisé à l'aide d'une authentification multifactor (MFA). Pour finir de vous connecter, activez ou affichez votre appareil MFA et saisissez le code d'authentification ci-dessous.' It has an 'Adresse e-mail' field with 'marion.borne@laplateforme.io', a 'Code MFA' input field, and a 'Soumettre' (Submit) button. Below it are links for 'Résoudre les problèmes MFA', 'Essayer une autre méthode MFA', and 'Annuler'.

**L'AWS CLI (Command Line Interface) est un outil en ligne de commande qui vous permet d'interagir avec les services d'Amazon Web Services directement depuis un terminal ou une invite de commande, sans passer par l'interface graphique (la console web AWS).**

Utiliser WSL sur l'ordinateur Windows : ici un sus system Debian LINUX

### Étapes pour installer AWS CLI v2 sur Linux :

1. Ouvrir un terminal : Sur votre machine Linux, ouvrez un terminal pour exécuter les commandes suivantes.

2. Télécharger le fichier d'installation de AWS CLI v2 : Exécutez la commande suivante pour télécharger le programme d'installation directement depuis AWS :

```
marion@WIN-P895AFVTD8F:~$ sudo curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
[sudo] password for marion:
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload Total   Spent    Left Speed
100 62.9M  100 62.9M    0     0  32.6M      0  0:00:01  0:00:01 --:--:-- 32.6M
```

Décompressez le fichier ZIP téléchargé :

```
marion@WIN-P895AFVTD8F:~$ sudo apt install unzip
Reading package lists... Done
```

```
marion@WIN-P895AFVTD8F:~$ sudo unzip awscliv2.zip
Archive: awscliv2.zip
  creating: aws/
  creating: aws/dist/
  inflating: aws/README.md
```

Exécutez la commande suivante pour installer AWS CLI v2

```
marion@WIN-P895AFVTD8F:~$ sudo ./aws/install
You can now run: /usr/local/bin/aws --version
marion@WIN-P895AFVTD8F:~$ |
marion@WIN-P895AFVTD8F:~$ aws --version
aws-cli/2.18.0 Python/3.12.6 Linux/5.15.153.1-microsoft-standard-WSL2 exe/x86_64/ubuntu.24
```

Après l'installation, vous devrez configurer AWS CLI avec vos identifiants AWS (Access Key ID, Secret Access Key, région par défaut) :

### Étapes pour obtenir une Access Key ID et une Secret Access Key pour un utilisateur IAM :

Lorsque vous exécutez la commande aws configure, vous devez fournir une Access Key ID et une Secret Access Key spécifiques à l'utilisateur IAM que vous avez créé sur AWS. Ces clés permettent à AWS CLI d'authentifier votre utilisateur et d'autoriser les commandes que vous exécutez via la ligne de commande.

#### 1. Accéder à la console IAM :

- Connectez-vous à votre console AWS avec votre utilisateur IAM personnel (ou un utilisateur ayant des droits administratifs).
- Dans le menu de navigation de la console AWS, recherchez IAM et cliquez sur le service Identity and Access Management (IAM).

#### 2. Sélectionner l'utilisateur IAM :

- Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur pour lequel vous souhaitez créer une clé d'accès (par exemple, votre utilisateur personnel IAM ou un des autres utilisateurs que vous avez créés, comme Jeff Bezos, Elon Musk, etc.).

#### 3. Créer une clé d'accès :

- Dans l'onglet Informations de sécurité de l'utilisateur sélectionné, recherchez la section Clés d'accès.
- Cliquez sur le bouton Créer une clé d'accès.

#### 4. Télécharger la clé d'accès :

- Une nouvelle clé d'accès sera générée, comprenant une Access Key ID et une Secret Access Key.
- Téléchargez le fichier CSV contenant ces informations ou copiez-les immédiatement. Important : la Secret Access Key ne sera plus affichée après cette étape, donc assurez-vous de la sauvegarder dans un endroit sécurisé.

The screenshot shows the first step of the 'Create New Access Key' wizard. It includes sections for 'Best practices and alternatives in the matter of access keys' (with a note to avoid long-term key reuse), 'Case usage' (with a selected option for 'Command-line interface (CLI)' and a note about using it for AWS CLI access), and 'Next Step' (with a link to 'Get the access key').

The screenshot shows the second step of the 'Get the access key' wizard. It displays the generated Access Key ID (AKIAQUFLP6MXKRCGB2UO) and Secret Access Key (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). A 'Hide' button is also present. Below this, a summary table titled 'marion\_borne\_accessKeys' lists the Access key ID and Secret access key.

Access key ID	Secret access key
AKIAQUFLP6MXKRCGB2UO	ml+6AB/WSU0PLCnUhP7aFOhEmS+iEF7rTkwPL7de

```
marion@WIN-P895AFVTD8F:~/aws$ aws configure
AWS Access Key ID [None]: AKIAQUFLP6MXKRCGB2UO
AWS Secret Access Key [None]: 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
Default region name [Bouches du Rhônes]: Bouches-du-Rhônes
Default output format [json]: json
marion@WIN-P895AFVTD8F:~/aws$
```

# Les IAM roles

Un IAM Role (Rôle IAM) est une entité AWS qui permet à des services ou applications AWS d'assumer des permissions spécifiques pour effectuer des actions dans votre compte AWS. Contrairement à un utilisateur IAM qui a des identifiants permanents, un rôle IAM est temporaire et souvent utilisé par des services AWS comme EC2 ou Lambda pour accéder à d'autres ressources AWS sans avoir à fournir des identifiants.

## Naviguer vers la section "Rôles" dans IAM

1. Dans le panneau de navigation IAM à gauche, cliquez sur Rôles.
2. Cliquez sur le bouton Créer un rôle.

## Selectionner le type d'entité de confiance

1. AWS vous demandera pour quel service ou entité vous souhaitez créer le rôle.
2. Sélectionnez AWS Service, car ce rôle sera utilisé par EC2.
3. Sous Service qui va utiliser ce rôle, sélectionnez EC2.
4. Cliquez sur Suivant : Autorisations.

Sélectionner une entité de confiance Info

Type d'entité approuvée

- Service AWS Autorise les services AWS tels que EC2, Lambda ou autres à effectuer des actions dans ce compte.
- Compte AWS Autorise les entités d'autres comptes AWS qui appartiennent à nous à nous à effectuer des actions dans ce compte.
- Fédération SAML 2.0 Autorise les utilisateurs fédérés avec SAML 2.0 à nous à effectuer des actions différentes à effectuer des actions dans ce compte.
- Stratégie d'apporstation personnalisée Crée une stratégie d'apporstation personnalisée pour permettre à d'autres utilisateurs d'effectuer des actions dans ce compte.
- Identité Web Permet aux utilisateurs fédérés par le fournisseur d'identité web externe également à nous à effectuer des actions dans ce compte.

Cas d'utilisation Autorise un service AWS comme EC2, Lambda ou autres à effectuer des actions dans ce compte.

Service ou cas d'utilisation EC2

Choisissez un cas d'utilisation pour le service spécifié.

Cas d'utilisation EC2

- EC2 Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling Allows EC2 Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging Allows EC2 Spot Fleet to launch and manage spot instances on your behalf.
- EC2 - Spot Instances Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances Allows EC2 Scheduled Instances to manage instances on your behalf.

Anuler Suivant

Rôles (2) Info

Un rôle IAM est une identité que vous pouvez créer et qui dispose d'autorisations spécifiques avec des informations d'identification valides pendant de courtes durées peuvent être endossées par des entités de confiance.

Entités de confiance	Dernier
Service AWS: support (Rôle lié à un s...)	-
Service AWS: trustedadvisor (Rôle lié à ...)	-

Rechercher

Nom du rôle

- AWSServiceRoleForSupport
- AWSServiceRoleForTrustedAdvisor

## Attacher les permissions au rôle

1. Dans la page Ajouter des autorisations, vous verrez une liste des politiques AWS.
2. Dans la barre de recherche des politiques, tapez IAMReadOnlyAccess.
3. Cochez la case à côté de IAMReadOnlyAccess pour accorder la permission de lecture seule sur les ressources IAM.
4. Cliquez sur Suivant : Balises (facultatif).

## Ajouter des balises (optionnel)

1. Les balises sont des paires clé-valeur que vous pouvez ajouter pour identifier ou organiser vos rôles.
2. Si vous n'avez pas besoin de balises, vous pouvez ignorer cette étape en cliquant sur Suivant : Vérification.

## Vérifier et nommer le rôle

1. Dans la page de Vérification, assurez-vous que toutes les informations sont correctes:
  - o Type de rôle : EC2.
  - o Politique : IAMReadOnlyAccess.
2. Nom du rôle : Entrez DemoForEC2.
3. Cliquez sur Créer un rôle pour finaliser le processus.

### Pourquoi créer un rôle IAM "DemoForEC2" ?

Ce rôle permet à des instances EC2 d'accéder aux services IAM en lecture seule via la stratégie IAMReadOnlyAccess, sans avoir besoin de stocker des clés d'accès ou des identifiants permanents sur l'instance.

### Cas d'usage typique pour EC2 :

Un rôle comme DemoForEC2 pourrait être utilisé pour permettre à une instance EC2 de lire les informations IAM (par exemple, pour une application qui doit auditer les utilisateurs ou rôles dans AWS) sans avoir besoin de permissions supplémentaires.

DemoForEC2 Infos  
Allows EC2 instances to call AWS services on your behalf.  
Supprimer | Modifier

Récapitulatif

Date de création October 07, 2024, 15:53 (UTC+02:00)	ARN arn:aws:iam::043309331246:role/DemoForEC2	ARN de profil d'instance arn:aws:iam::043309331246:instance-profile/DemoForEC2
Dernière activité -	Durée maximale de la session 1 heure	

Autorisations | Relations d'approbation | Balises | Last Accessed | Révoquer les séances

Politiques des autorisations (1) Infos  
Vous pouvez attacher jusqu'à 10 politiques gérées.  
Filtrer par Type

Rechercher	Tous les types
<input type="checkbox"/> Nom de la politique	Type
<input checked="" type="checkbox"/> IAMReadOnlyAccess	Gérées par AWS

Ajouter des autorisations Infos

Politiques des autorisations (1/951) Infos  
Choisissez une ou plusieurs stratégies à attacher à votre nouveau rôle.  
Filtrer par Type

Rechercher	Tous les types
<input checked="" type="checkbox"/> Nom de la politique	Type
<input checked="" type="checkbox"/> IAMReadOnlyAccess	Gérées par AWS Provides read only access to IAM via the IAM API.

▶ Définir une limite d'autorisations - facultatif

Annuler | Précédent | Suivant

Pour générer un AWS Credentials Report (rapport des identifiants AWS), qui permet de surveiller les activités de connexion et les permissions des utilisateurs dans votre infrastructure AWS.

#### Étapes pour générer un AWS Credentials Report :

1. Accédez à IAM.
2. Allez dans la section Rapport d'identifiants.
3. Générez et téléchargez le rapport sous format CSV.
4. Enregistrez le rapport pour analyse.

#### Le rapport contient les informations suivantes :

- Nom de l'utilisateur IAM.
- Date de création de l'utilisateur.
- Statut des mots de passe (s'ils ont été activés et la dernière modification).
- Statut de la MFA (si la MFA est activée ou non pour chaque utilisateur).
- Dernier accès à AWS (la date à laquelle l'utilisateur a accédé aux services AWS pour la dernière fois).
- Clés d'accès (Access Key ID et statut des clés — actives ou inactives).

#### Utilité du rapport AWS Credentials Report :

- Il vous permet de surveiller les va-et-vient des utilisateurs dans votre infrastructure cloud.
- Vous pouvez vérifier si les utilisateurs ont activé la MFA.
- Vous pouvez auditer l'utilisation des Access Keys et détecter des accès anormaux ou des risques de sécurité (par exemple, des utilisateurs ayant des clés d'accès inactives ou n'ayant jamais activé leur MFA).

user	arn	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_active	access_key_1_last_rotated	access_key_1_last_used_date
<root_account>	arn:aws:iam::043309331246:root	2024-10-07T08:24:47Z	true	2024-10-07T12:03:36Z	2024-10-07T08:24:47Z	not_supported	true	false	2024-10-07T11:48:32Z	N/A
bill_gates	arn:aws:iam::043309331246:user/bill_gates	2024-10-07T09:55:53Z	true	no_information	2024-10-07T09:55:53Z	N/A	false	false	N/A	N/A
elon_musk	arn:aws:iam::043309331246:user/elon_musk	2024-10-07T09:52:42Z	true	no_information	2024-10-07T09:52:42Z	N/A	false	false	N/A	N/A
jeff_bezos	arn:aws:iam::043309331246:user/jeff_bezos	2024-10-07T09:46:32Z	true	no_information	2024-10-07T09:46:32Z	N/A	false	false	N/A	N/A
marian_borne	arn:aws:iam::043309331246:user/marian borne	2024-10-07T09:26:19Z	true	2024-10-07T10:08:33Z	2024-10-07T09:26:19Z	N/A	false	true	2024-10-07T11:31:29Z	N/A
mark_zuckerberg	arn:aws:iam::043309331246:user/mark_zuckerberg	2024-10-07T09:54:23Z	true	no_information	2024-10-07T09:54:23Z	N/A	false	false	N/A	N/A
steve_jobs	arn:aws:iam::043309331246:user/steve_jobs	2024-10-07T09:55:01Z	true	no_information	2024-10-07T09:55:01Z	N/A	false	false	N/A	N/A

Gestion de la facturation et des coûts

Accueil

Démarrer

**Facturation et paiements**

Factures

Paiements

Credits

Bons de commande

**Analyse des coûts**

Explorateur de coûts

Rapports enregistrés de l'explorateur de coûts

Détection des anomalies de coûts

Offre gratuite

Exportations de données

**Organisation des coûts**

Categories de coûts

Balises de répartition des coûts

Chef de facturation

**Budgets et planification**

**Budgets**

Facturation AWS

## AWS Budgets

Définir des budgets personnalisés qui vous alertent lorsque vous dépassez vos seuils budgétés

AWS Budgets est votre hub pour la création, le suivi et l'inspection de vos budgets.

**Fonctionnement**

Créer un budget

Commencer à suivre vos coûts et votre utilisation d'AWS

Une fois que vous avez un budget créé, AWS Budgets vous permet de créer des budgets, de prévoir les dépenses et de prendre des mesures sur vos coûts et votre utilisation depuis un seul et même emplacement.

Créer un budget

Tarification (US)

Autres frais supplémentaires ne s'appliquent à l'utilisation d'AWS Budgets. Vous ne payez que les actions configurées qui vont au-delà de l'offre gratuite de 62 jours de budget actives par actions.

Afficher les informations de tarification

Mise en route

Pour éviter des frais inattendus et définir une politique de budget afin de rester dans la limite du niveau gratuit ("free tier") d'AWS, voici les étapes à suivre pour configurer un budget et recevoir des alertes si vous dépassez les seuils définis.

### Résumé des étapes :

1. Accédez à Billing and Cost Management via votre compte AWS.
2. Allez dans la section Budgets et cliquez sur Create a budget.
3. Sélectionnez le type de budget Zero spend budget pour éviter toute dépense.
4. Configurez votre budget et vos alertes e-mail pour surveiller vos dépenses.
5. Créez et sauvegardez le budget.

**Ce processus garantit que vous serez averti en cas de dépassement de la limite du niveau gratuit d'AWS, vous évitant ainsi des coûts inattendus pour les tests ou l'utilisation non planifiée des services AWS.**

Budgets (1) [Infos](#)

Télécharger le rapport CSV Actions [Créer un budget](#)

Rechercher un budget Type - Afficher tous les budgets

Nom	Seuils	Budget	Montant utilisé	Montant prévu	Actuels contre budget	Pré
My_Zero-Spend_Budget	OK	1,00 \$US	0,00 \$US	-	0,00%	-

Facturation et gestion des coûts > Budgets > Créer un budget

## Choisir le type de budget [Infos](#)

**Configuration du budget**

Utiliser un modèle (simplifié)  
Utilisez les configurations recommandées. Vous pouvez modifier certaines options de configuration une fois le budget créé.

Personnaliser (avancé)  
Personnalisez un budget pour définir des paramètres spécifiques à votre cas d'utilisation. Vous pouvez personnaliser la période, le mois de début et des comptes spécifiques.

**Modèles – nouveau**

Choisissez le modèle qui correspond le mieux à votre cas d'utilisation.

Budget de dépense nul  
Créez un budget qui vous informe dès que vos dépenses dépassent 0,01 USD, ce qui dépasse les limites de l'Offre gratuite d'AWS.

Budget de coûts mensuel  
Créez un budget mensuel qui vous informe si vous dépassez ou êtes en passe de dépasser le montant du budget.

Budget quotidien d'utilisation des réservations  
Créez un budget d'utilisation pour vos réservations qui vous avertit lorsque vous passez en dessous de l'objectif établi.

**Budget de dépense nul – Modèle**

**Nom du budget**  
Indiquez un nom descriptif pour ce budget.

Les noms doivent comporter entre 1 et 100 caractères.

**Destinataires d'e-mail**  
Indiquez les destinataires d'e-mail que vous souhaitez avertir lorsque le seuil est dépassé.

Le nombre maximal de destinataires d'e-mail est de 10.

**Portée**  
Tous les services AWS sont concernés par ce budget.

Vous serez averti par e-mail lorsque des dépenses supérieures à 0,01 USD sont encourees.

# EC2

**Amazon EC2 (Elastic Compute Cloud) est un service fourni par AWS qui permet de louer des serveurs virtuels dans le cloud pour exécuter des applications. Ces serveurs, appelés instances EC2, offrent une capacité de calcul flexible et évolutive. EC2 permet de déployer et gérer des machines virtuelles en ajustant les ressources nécessaires (CPU, mémoire, stockage) en fonction des besoins.**

L'un des principaux avantages d'EC2 est sa scalabilité : vous pouvez facilement ajuster la taille et le nombre de vos instances en fonction de la demande, tout en ne payant que pour les ressources utilisées.

## Options de configuration et tailles disponibles pour EC2 :

1. **Tailles d'instances :** Différentes tailles adaptées aux besoins en CPU, mémoire et stockage :
  - o t2.micro : 1 vCPU, 1 Go RAM (petites applications, tests).
  - o m5.large : 2 vCPU, 8 Go RAM (serveurs web, petites bases de données).
  - o r5.4xlarge : 16 vCPU, 128 Go RAM (applications mémoire intensives).
2. **Types d'instances :**
  - o Générales (t2, m5) : Équilibre CPU/mémoire, adapté aux applications web et serveurs généraux.
  - o Optimisées pour le calcul (c5) : Puissance CPU élevée, pour calculs intensifs et traitement scientifique.
  - o Optimisées pour la mémoire (r5) : Grande mémoire, parfait pour les bases de données en mémoire ou analyses.
  - o Optimisées pour le stockage (i3) : E/S intensives, pour bases de données NoSQL et big data.
  - o GPU (p3, g4) : Conçu pour le machine learning, l'IA et le rendu graphique.
3. **Autres options :**
  - o AMI (Amazon Machine Image) : Choisissez un système d'exploitation (Amazon Linux, Ubuntu, Windows).
  - o Stockage : Volumes persistants EBS ou stockage temporaire lié à l'instance.
  - o Mise en réseau : Déploiement dans un VPC, configuration de sécurité via des groupes de sécurité.

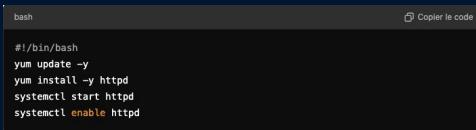
Cela vous permet de choisir la configuration adaptée à vos besoins spécifiques en termes de performance et d'usage.

## EC2 User Data et à quoi ça sert ?

EC2 User Data est un script ou des commandes que vous pouvez spécifier lorsque vous lancez une instance EC2. Ce script est automatiquement exécuté au démarrage de l'instance. Il est souvent utilisé pour automatiser certaines tâches initiales, comme :

- Installer des logiciels (Apache, Nginx, etc.).
- Configurer des paramètres de votre système d'exploitation.
- Télécharger et exécuter des scripts personnalisés lors du premier démarrage.
- Configurer des services ou déployer des applications au lancement sans intervention manuelle.

Par exemple, dans le champ User Data, vous pouvez entrer un script bash pour installer Apache :



```
bash
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
```

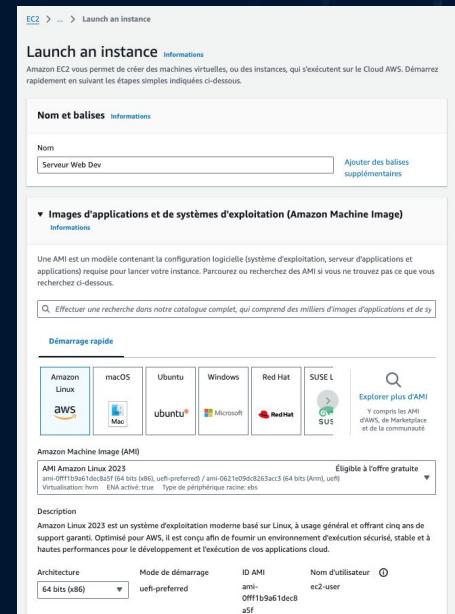
Cela permet à l'instance EC2 de démarrer, de se mettre à jour et d'installer et démarrer un serveur Web Apache automatiquement.

pour créer une instance EC2 qui respecte le cahier des charges : Toujours se mettre sur le bon fuseau horaires en haut de page à droite (localisation Paris)

**Accéder à la console EC2 :** Tapez EC2 dans la barre de recherche et cliquez sur EC2 pour accéder à la section de gestion des instances.

## Lancer une nouvelle instance EC2

1. Cliquez sur Lancer une instance.
2. Nom de l'instance :
  - o Dans la section Nom de l'instance, entrez Serveur Web Dev.
3. Choisir une AMI (Amazon Machine Image) :
  - o Sélectionnez Amazon Linux 2 comme image d'exécution.
4. Choisir le type d'instance :
  - o Choisissez la plus petite instance, c'est-à-dire t2.micro (1 vCPU, 1 Go RAM). C'est la taille minimale et elle fait partie du niveau gratuit d'AWS.



Launch an instance

Nom et balises

Images d'applications et de systèmes d'exploitation (Amazon Machine Image)

Démarage rapide

Amazon Machine Image (AMI)

AMI Amazon Linux 2023

Description

Architecture

Mode de démarrage

ID AMI

Nom d'utilisateur

Type de périphérique racine

## Configurer une paire de clés pour SSH

- Dans la section Pair de clés (login SSH), choisissez Créer une nouvelle paire de clés.
  - Nommez la paire de clés (par exemple dev-keypair).
  - Choisissez le format (PEM pour Linux, PPK pour PuTTY sur Windows).
  - Téléchargez la clé privée générée et conservez-la en lieu sûr. Vous en aurez besoin pour accéder à l'instance via SSH.

## Configurer le pare-feu (Groupes de sécurité)

- Ajouter des règles de sécurité pour permettre l'accès au serveur :
  - Cliquez sur Modifier les groupes de sécurité.
  - Créez un nouveau groupe de sécurité (par exemple Dev-SecurityGroup).
  - Ajouter les règles suivantes :
    - SSH (port 22) : Autoriser l'accès depuis My IP pour sécuriser la connexion SSH.
    - HTTP (port 80) : Autoriser le trafic depuis n'importe où (0.0.0.0/0).
    - HTTPS (port 443) : Autoriser le trafic depuis n'importe où (0.0.0.0/0).

The screenshot shows the AWS VPC configuration interface. On the left, under 'Paramètres réseau', it lists an IP address (vpc-09c02d0ed4d59480) and a security group (Dev-SecurityGroup). It also shows options for creating a new subnet or route table. On the right, three security groups are listed: 'Règles entrantes des groupes de sécurité', 'Règle de groupe de sécurité 2 (TCP, 80, 0.0.0.0/0)', and 'Règle de groupe de sécurité 5 (TCP, 443, 0.0.0.0/0)'. Each rule specifies the source (My IP, Anywhere, Anywhere), protocol (TCP), port range (22, 80, 443), and description ('SSH pour le bureau', 'HTTP pour le bureau', 'HTTPS pour le bureau').

## Configurer le stockage

- Sous la section Stockage, sélectionnez un disque EBS gp2 de 8 Go :
  - Type de volume : gp2 (SSD général).
  - Taille : 8 Go (conformément au cahier des charges).

The dialog box for creating a key pair. It asks for the key name ('dev-keypair') and specifies the type as RSA. It also provides options for file formats (.pem or .ppk) and notes that the private key should be stored securely. A large button at the bottom right says 'Créer une paire de clés'.

The storage configuration dialog box. It shows a selection for a 1x 8 GiB gp2 volume labeled 'Volume racine (Non chiffré)'. An 'Avancé' button is visible in the top right corner.

## Ajouter un script User Data pour installer un serveur web

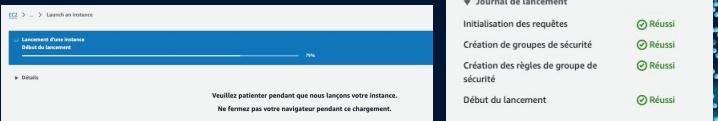
1. Dans la section Advanced Details (Détails avancés), trouvez le champ User Data.
2. Entrer un script bash pour déployer un serveur web (Apache) au démarrage de l'instance
3. Met à jour les paquets de l'instance.
4. Installe et démarre le serveur web Apache.
5. Crée une page HTML simple indiquant que le serveur fonctionne.

The screenshot shows the 'User Data' configuration step in the AWS Lambda console. It includes a file input field labeled 'Choisir un fichier' and a code editor containing the following bash script:

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "Hello, Serveur Web Dev is running!" > /var/www/html/index.html
```

## Lancer l'instance

1. Après avoir vérifié les configurations, cliquez sur Lancer.
2. L'instance Serveur Web Dev sera maintenant en cours de démarrage.



## Accéder à l'instance depuis un navigateur

1. Obtenez l'adresse IP publique de votre instance :
  - o Allez dans Instances dans la console EC2, sélectionnez Serveur Web Dev et copiez son IP publique.
2. Accéder au serveur web :
  - o Ouvrez un navigateur et entrez l'IP publique de votre instance dans la barre d'adresse.
  - o Vous devriez voir le message : "Hello, Serveur Web Dev is running!".

This screenshot shows the 'Résumé de l'instance pour i-03c2b2ed4f178dcc (Serveur Web Dev)' page. It lists the instance ID (i-03c2b2ed4f178dcc), its name (Serveur Web Dev), and its public IP address (13.39.109.20). Other details include the type of host name, DNS resolution, and automatically assigned IP address.



Pour que les développeurs puissent accéder à l'instance EC2 via SSH, voici les étapes détaillées que vous devez suivre pour permettre cette connexion :

#### Prérequis pour la connexion SSH

1. **Clé privée (Key Pair) :** Vous avez besoin du fichier de clé privée (.pem) téléchargé lors de la création de l'instance EC2.
2. **Adresse IP publique de l'instance EC2 :**
  - Allez dans la console EC2 > Instances.
  - Repérez votre instance et notez son adresse IP publique.

#### Ouvrir les ports nécessaires pour SSH

Configurer le groupe de sécurité pour permettre l'accès SSH : Vérifiez que vous avez une règle SSH (port 22) autorisant les connexions depuis l'adresse IP des développeurs (ou 0.0.0.0/0 pour tout le monde si vous voulez permettre à tout le monde d'accéder temporairement).

#### Se connecter à l'instance via SSH

Dans un terminal:

1. Remplacer **/chemin/vers/votre/clé.pem** par le chemin vers votre fichier de clé privée téléchargé sur votre ordinateur.
2. Remplacer **<IP\_publique\_de\_l\_instance>** par l'adresse IP publique de votre instance EC2. (ici c'est la adresse IP d'une ancienne instance, c'est normal que ce ne soit pas la même pour la suite du job)

```
mariom@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ ssh -i /mnt/c/Users/mario/Downloads/dev-keypair.pem ec2-user@3.87.97.248
The authenticity of host '3.87.97.248 (3.87.97.248)' can't be established.
ED25519 key fingerprint is SHA256:F4s9AUl3jzw0hVyKCmwbTh98VF0Mbhw0xwffRuhYUM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.87.97.248' (ED25519) to the list of known hosts.
oooooooooooooooooooooooooooooooooooooooooooooooooooo
          WARNING: UNPROTECTED PRIVATE KEY FILE!
oooooooooooooooooooooooooooooooooooooooooooo
Permissions 0777 for '/mnt/c/Users/mario/Downloads/dev-keypair.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "/mnt/c/Users/mario/Downloads/dev-keypair.pem": bad permissions
ec2-user@3.87.97.248: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
mariom@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$
```

Le problème ici vient des permissions du fichier **dev-keypair.pem**. Pour que SSH fonctionne correctement, la clé privée doit avoir des permissions très restreintes (seulement l'utilisateur qui exécute la commande doit pouvoir lire le fichier).

Actuellement, le fichier a des permissions incorrectes (-r-xr-xr-x ou 0777, ce qui permet à tous les utilisateurs de lire/écrire/voir le fichier). Cela doit être changé pour que seul **vous** puissiez lire la clé.

#### Corriger les permissions du fichier de clé privée :

Dans votre terminal, exécutez cette commande pour ajuster les permissions du fichier à un niveau sécurisé : chmod 400 /mnt/c/Users/mario/Downloads/dev-keypair.pem

Cette commande fait en sorte que **seul votre utilisateur** peut lire le fichier, ce qui est nécessaire pour éviter que SSH refuse de l'utiliser : vous pouvez vérifier que les permissions sont bien en -r-----

```
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ sudo chmod 400 /mnt/c/Users/mario/Downloads/dev-keypair.pem
[sudo] password for marion:
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ ls -l /mnt/c/Users/mario/Downloads/dev-keypair.pem
-r--r--r-- 1 marion marion 1678 Oct  7 16:53 /mnt/c/Users/mario/Downloads/dev-keypair.pem
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ |
```

Le problème vient du fait que, même après avoir exécuté la commande chmod 400, les permissions du fichier dev-keypair.pem n'ont pas été correctement appliquées. Comme on peut le voir sur la capture, les permissions sont toujours en r-xr-xr-x au lieu de r-----.

Cela est dû au fait que WSL (Windows Subsystem for Linux) utilise le système de fichiers Windows, qui ne gère pas les permissions de la même manière que Linux.

Étape 1 : Copier le fichier vers un dossier Linux natif

Sur WSL, les permissions du système de fichiers Windows (comme les fichiers situés dans /mnt/c/) ne sont pas totalement respectées. Pour contourner cela, copions la clé privée dans un répertoire propre à WSL (par exemple, dans le répertoire ~/ssh de votre utilisateur WSL) : Copier le fichier vers le répertoire WSL : Dans votre terminal, exécutez la commande suivante pour copier votre fichier de clé dans un répertoire où les permissions peuvent être correctement gérées :

```
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ cp /mnt/c/Users/mario/Downloads/dev-keypair.pem ~/.ssh/
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ ls -l ~/.ssh/
total 8
-r--r--r-- 1 marion marion 1678 Oct  8 12:42 dev-keypair.pem
-rw-r--r-- 1 marion marion 142 Oct  8 12:32 known_hosts
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ chmod 400 ~/.ssh/dev-keypair.pem
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ ls -l ~/.ssh/dev-keypair.pem
-r----- 1 marion marion 1678 Oct  8 12:42 /home/marion/.ssh/dev-keypair.pem
marion@WIN-P895AFVTD8F:/mnt/c/Users/mario/Downloads$ |
```

## **Reessayer de se connecter à l'instance EC2 avec la clé corrigée**

Vous pouvez désormais : Exécuter des commandes sur votre instance, Installer des logiciels, Configurer des services, comme un serveur web, si nécessaire.

```
marion@WIN-P895AFVTD8F:/mnt$ ssh -i ~/.ssh/dev-keypair.pem ec2-user@13.39.109.20
The authenticity of host '13.39.109.20 (13.39.109.20)' can't be established.
ED25519 key fingerprint is SHA256:Lx3p9wMTOQ2+dG47nL1JF2Kz5fu0JEMAGH2whKHMJLE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.39.109.20' (ED25519) to the list of known hosts.

#_
  _###_      Amazon Linux 2023
  _\####\_
  _\#\#\#
  _\#/  ___   https://aws.amazon.com/linux/amazon-linux-2023
  _\`~`_>
  _\`_/
  _\`/_`_/
  _\`/m`_/
[ec2-user@ip-172-31-41-33 ~]$
```

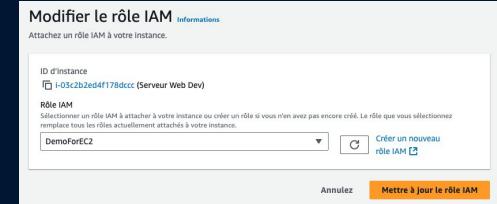
## Étape 1 : Attribuer le rôle IAM à l'instance EC2

1. **Accédez à la console AWS** : Connectez-vous à AWS et allez dans la section EC2.
  2. **Sélectionner l'instance EC2** :
    - o Cliquez sur Instances dans le panneau de navigation à gauche.
    - o Sélectionnez votre instance EC2 pour laquelle vous souhaitez attribuer le rôle.
  3. **Modifier le rôle IAM de l'instance** :
    - o Avec l'instance sélectionnée, cliquez sur Actions > Sécurité > Modifier le rôle IAM (Modify IAM Role).
    - o Dans la section Rôle IAM, choisissez le rôle que vous avez créé dans le Job 5 (par exemple DemoForEC2).
    - o Cliquez sur Mettre à jour (Update). Cela attribuera le rôle IAM à l'instance EC2. Ce rôle doit inclure les permissions IAMReadOnlyAccess comme spécifié dans le Job 5.

Tester la commande **aws iam list-users**

**Installer l'AWS CLI** (si ce n'est pas encore fait) : Si AWS CLI n'est pas encore installé sur l'instance EC2, vous pouvez l'installer avec cette commande :

Exécuter la commande pour tester le rôle IAM : Tapez la commande suivante dans votre session SSH pour lister les utilisateurs IAM. Cela vérifiera si le rôle IAM avec les permissions IAMReadOnlyAccess fonctionne correctement : Si le rôle est bien appliqué, vous verrez une liste des utilisateurs IAM associés à votre compte.



```
[ec2-user@ip-172-31-41-33 ~]$ sudo yum install -y aws-cli
Last metadata expiration check: 0:27:08 ago on Tue Oct  8 12:03:28 2024.
Package awscli-2.2.15.30-1.amzn2023.0.1.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-41-33 ~]$ |
```

```
[ec2-user@ip-172-31-41-33 ~]$ aws iam list-users
{
    "Users": [
        {
            "Path": "/",
            "UserName": "bill_gates",
            "UserId": "AIDAQULFLPGMXFGCRET3P",
            "Arn": "arn:aws:iam:043309331246:user/bill_gates",
            "CreateDate": "2024-10-07T09:55:53+00:00"
        },
        {
            "Path": "/",
            "UserName": "elon_musk",
            "UserId": "AIDAQULFLPGMXZ3GL3R7E",
            "Arn": "arn:aws:iam:043309331246:user/elon_musk",
            "CreateDate": "2024-10-07T09:52:42+00:00"
        },
        {
            "Path": "/",
            "UserName": "jeff_bezos",
            "UserId": "AIDAQULFLPGMXFJWNGKQ3",
            "Arn": "arn:aws:iam:043309331246:user/jeff_bezos",
            "CreateDate": "2024-10-07T09:46:32+00:00"
        },
        {
            "Path": "/",
            "UserName": "marion_borne",
            "UserId": "AIDAQULFLPG6XMLGBTRVGVX",
            "Arn": "arn:aws:iam:043309331246:user/marion_borne",
            "CreateDate": "2024-10-07T09:26:19+00:00",
            "CreateDate": "2024-10-07T09:46:32+00:00"
        }
    ],
    "UserNames": [
        "skipping...
```

Attribuer le rôle IAM DemoForEC2 à votre instance EC2 permet à l'instance d'assumer certaines permissions spécifiques sans avoir besoin d'identifiants permanents (comme des clés d'accès ou des secrets). Voici quelques raisons pour lesquelles cela est important :

#### Raisons d'attribuer un rôle IAM à une instance EC2 :

- Sécuriser les accès :** Permet d'accéder aux services AWS sans avoir à utiliser des identifiants permanents.
- Limiter les permissions :** Vous pouvez spécifier exactement quelles actions l'instance peut effectuer.
- Bonne pratique de sécurité :** Respecter le principe du moindre privilège et réduire les risques liés à la gestion des clés d'accès.
- Accès à des services spécifiques :** Par exemple, avec IAMReadOnlyAccess, vous pouvez lister les utilisateurs IAM depuis l'instance.

## Options d'achat EC2

Option d'achat EC2	Utilisation	Coût	Flexibilité	Avantages	Inconvénients
On-Demand (À la demande)	Charges de travail imprévisibles ou temporaires (tests, développement).	Plus cher sur le long terme, facturation à la seconde/heure.	Très flexible, instances peuvent être lancées et arrêtées à tout moment.	Pas d'engagement, flexibilité maximale.	Coût plus élevé sur le long terme.
Reserved Instances	Charges de travail constantes et prévisibles (serveurs web, bases de données).	Jusqu'à 75% de réduction avec engagement 1 ou 3 ans.	Moins flexible, engagement sur 1 ou 3 ans, possibilité de modifier le type d'instance.	Optimise les coûts à long terme.	Engagement à long terme, moins flexible.
Spot Instances	Charges tolérantes aux interruptions (calcul batch, big data).	Très économique, jusqu'à 90% de réduction.	Faible flexibilité, instance peut être interrompue si AWS a besoin de capacité.	Coût extrêmement réduit.	Risque d'interruption, pas pour des charges critiques.
Dedicated Instances	Applications nécessitant un matériel isolé (compliance, sécurité accrue).	Plus élevé que les autres options.	Moins flexible, isolation physique pour des raisons de conformité.	Isolation physique des ressources.	Coût plus élevé, moins flexible.
Dedicated Hosts	Nécessité de gérer les licences logicielles et de contrôler l'infrastructure.	Plus cher, facturation par hôte.	Très limité en flexibilité, contrôle total du matériel.	Gestion des licences et conformité stricte.	Coût très élevé, complexe à gérer.

# Snapshot volume attaché

1. **Accéder à la console AWS :**
  - o Connectez-vous à la console AWS et allez dans le service EC2.
2. **Trouver l'instance "Serveur Web Dev" :**
  - o Allez dans la section Instances dans le panneau de gauche.
  - o Sélectionnez l'instance "Serveur Web Dev".
3. **Identifier le volume attaché :**
  - o Avec l'instance sélectionnée, cliquez sur l'onglet Storage (Stockage) ou dans la section Volumes du menu de gauche.
  - o Vous verrez le volume EBS attaché à votre instance, souvent marqué comme /dev/xvda (le volume racine).
4. **Créer un snapshot :**
  - o Dans la liste des volumes EBS, sélectionnez le volume que vous voulez sauvegarder (probablement le volume racine /dev/xvda).
  - o Cliquez sur Actions > Create Snapshot (Créer un snapshot).
  - o Donnez un nom et une description à votre snapshot, par exemple "Snapshot Serveur Web Dev".
  - o Cliquez sur Create Snapshot.
5. **Vérification :**
  - o Une fois le snapshot créé, vous pouvez vérifier son état en allant dans la section Snapshots du menu de gauche.
  - o Attendez que le statut du snapshot devienne complété.

The screenshot shows two main parts of the AWS EC2 interface. On the left, a modal window titled 'Créer un instantané' (Create a snapshot) is open. It displays the selected volume source (ID: vol-05b0cc4d26a84f5e9, Zone: eu-west-3c) and allows setting a snapshot description ('Snapshot Serveur Web Dev'). On the right, the 'Volumes (1/1) Information' table shows one volume entry:

Name	Volume ID	Kind	Size	IOPS
-	vol-05b0cc4d26a84f5e9	gp2	8 GiB	100

A context menu is open over the first volume row, listing actions: Change volume, Create a snapshot (which is highlighted), Create a Snapshot Lifecycle Strategy, Delete volume, Attach a volume, Detach a volume, Force volume detach, Manage automatically activated I/O, Manage Tags, and Disturbance Injection.

## Arrêter et résilier l'instance

1. Arrêter l'instance EC2 :
  - o Revenez à la section Instances.
  - o Sélectionnez votre instance "Serveur Web Dev".
  - o Cliquez sur Actions > Instance State > Stop (Arrêter).
  - o Confirmez l'arrêt.
2. Résilier l'instance EC2 :
  - o Une fois que l'instance est arrêtée, sélectionnez-la à nouveau.
  - o Cliquez sur Actions > Instance State > Terminate (Résilier).
  - o Confirmez la résiliation de l'instance.

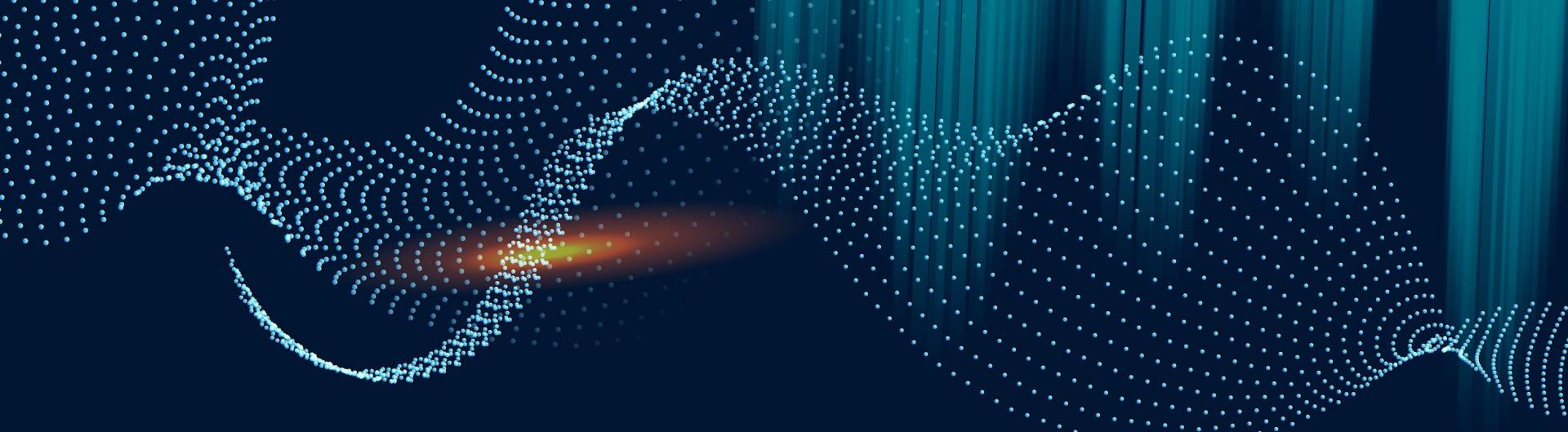
**Vous avez effectué un snapshot et résilié l'instance EC2 pour deux raisons principales :**

1. **Sauvegarde des données :** Le snapshot permet de sauvegarder les données du volume EBS de l'instance avant sa suppression. Cela vous donne la possibilité de restaurer les données à tout moment en recréant un volume à partir du snapshot.
2. **Réduction des coûts :** Résilier l'instance permet de stopper les frais liés à son utilisation. Conserver un snapshot coûte moins cher que de maintenir une instance active ou arrêtée.

**En résumé, le snapshot sauvegarde les données et la résiliation de l'instance optimise les coûts.**



The screenshot shows two side-by-side AWS management console pages. The left page is titled 'Gérer l'état de l'instance' and displays the 'Instances details' section for an instance named 'Serveur Web ...'. It shows the instance is currently 'running'. Below this is the 'Paramètres d'état de l'instance' section, which contains several options for stopping or terminating the instance. The right page is titled 'Instances (1/1) Informations' and shows a single instance row for the same 'Serveur Web ...' instance. The status is listed as 'En cours d...' and 't2.micro'. A dropdown menu is open over the 'Actions' button, with the option 'Gérer l'état de l'instance' highlighted. The rest of the page includes tabs for 'Informations', 'Actions', and 'Lancer des instances', along with various status and configuration details.



02

## AWS : EC2 Avancé +

Dans ce projet, vous allez voir comment utiliser EC2 à un niveau plus poussé,  
et également apprendre à gérer les différents volumes et paramétrages annexes.

Il sera impératif de documenter chacune des étapes qui vous ramèneront à la réalisation des Jobs.

Pour lancer une nouvelle instance EC2 à partir d'un snapshot, voici les étapes à suivre. Vous allez maintenant l'utiliser pour créer une nouvelle instance.

## Créer un volume EBS à partir du snapshot

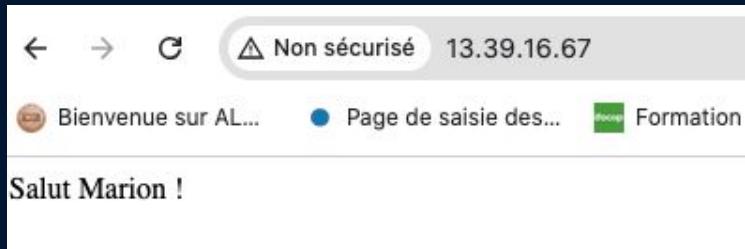
- Accédez à la console AWS.
- Allez dans la section EC2.
- Dans le menu de gauche, sous la section Elastic Block Store, cliquez sur Snapshots.
- Trouvez le snapshot que vous avez créé lors du Jour 1 - Job 13.
- Selectionnez le snapshot, puis cliquez sur Actions > Create Volume.
- Dans la fenêtre de création du volume :
  - Selectionnez la zone de disponibilité où vous souhaitez lancer l'instance (elle doit correspondre à la zone où vous voulez déployer l'instance EC2).
  - Laissez les autres options par défaut (comme la taille et le type de volume).
- Cliquez sur Create Volume.

## Lancer une nouvelle instance EC2 et attacher le volume

- Dans la console EC2, allez dans Instances et cliquez sur Launch Instance.
- Choisissez une Amazon Machine Image (AMI) qui correspond à votre système d'exploitation préféré ou utilisé précédemment.
- Choisissez le type d'instance en fonction des besoins (la plus petite instance, par exemple, t2.micro si vous voulez rester dans la couche gratuite).
- À l'étape Add Storage :
  - Cliquez sur Add New Volume et choisissez Attach an Existing Volume.
  - Selectionnez le volume que vous avez créé à partir du snapshot à l'étape précédente.
- Continuez les étapes pour configurer le réseau, les tags, la configuration de la sécurité (ouvrez les ports nécessaires), et lancez l'instance.
- Selectionnez ou créez une Key Pair pour vous connecter à l'instance via SSH.

## Vérifier l'instance et le volume attaché

1. Après le lancement de l'instance, allez dans la section Instances pour vérifier que l'instance est bien en running.
2. Dans les détails de l'instance, vérifiez que le volume EBS que vous avez créé à partir du snapshot est bien attaché à votre instance EC2.
3. Vous pouvez maintenant vous connecter à votre instance EC2 via SSH en utilisant la clé privée spécifiée.



```
marion@WIN-P895AFVTD8F:/mnt$ cp /mnt/c/Users/mario/Downloads/marion-keypair.pem ~/.ssh/
marion@WIN-P895AFVTD8F:/mnt$ ls -l ~/.ssh/
total 16
-r----- 1 marion marion 1678 Oct  8 14:16 dev-keypair.pem
-rw----- 1 marion marion  728 Oct  8 14:17 known_hosts
-rw----- 1 marion marion  504 Oct  8 14:17 known_hosts.old
-rwxr-xr-x 1 marion marion 1674 Oct  8 16:16 marion-keypair.pem
marion@WIN-P895AFVTD8F:/mnt$ chmod #00 ~./ssh/marion-keypair.pem
marion@WIN-P895AFVTD8F:/mnt$ ssh -i ~/.ssh/marion-keypair.pem ec2-user@13.39.16.67
The authenticity of host '13.39.16.67 (13.39.16.67)' can't be established.
ED25519 key fingerprint is SHA256:u/u24znz0h5biF07mA5Ve+R2Vs2FNHbaBPxEcITrlis.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.39.16.67' (ED25519) to the list of known hosts.

          _#
         /###
        /###\
       /##|   Amazon Linux 2023
      /#| \
     /#|  https://aws.amazon.com/linux/amazon-linux-2023
    /#| /
   /#| /
  /#| /
 /#| /
/_m'/ |
```

[ec2-user@ip-172-31-40-239 ~]\$ |

Pour les instances EC2, voici les types d'adresses IP qui peuvent être attachées à une instance :

Type d'adresse IP	Description	Portée	Utilisation
Adresse IP privée	Attribuée automatiquement pour la communication interne dans un VPC.	Accessible uniquement dans le réseau privé AWS.	Pour des communications internes entre instances dans le VPC.
Adresse IP publique	Assignnée dynamiquement pour permettre un accès à Internet.	Accessible via Internet.	Pour permettre l'accès à l'instance depuis Internet.
Elastic IP	IP publique statique associée à une instance, même après redémarrage.	Accessible via Internet.	Pour des applications nécessitant une IP publique persistante.
Adresse IP secondaire	Adresse IP privée supplémentaire pour des instances ayant plusieurs interfaces réseau.	Utilisable pour des communications internes au VPC.	Pour gérer plusieurs services ou interfaces réseau avec une instance unique.

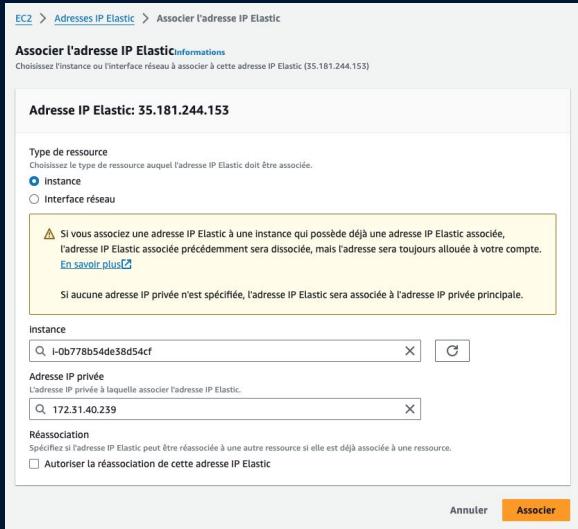
Pour générer une Elastic IP, l'attacher à votre instance EC2, et ensuite la résilier une fois l'opération terminée.

#### Générer une Elastic IP

- Accédez à la console AWS > EC2 > Elastic IP > Allouer Elastic IP address :
  - Laissez les paramètres par défaut pour allouer une IP à partir de la plage d'adresses IP d'Amazon.
  - Cliquez sur Allocate (Allouer).
- Vous verrez une nouvelle Elastic IP générée et disponible dans la liste.

#### Attacher l'Elastic IP à votre instance EC2

- Sélectionnez l'Elastic IP :
  - Dans la liste des Elastic IPs, sélectionnez celle que vous venez de générer.
- Associer l'Elastic IP à votre instance EC2 :
  - Cliquez sur Actions > Associate Elastic IP address (Associer une adresse Elastic IP),
  - Dans la section Instance, sélectionnez l'instance EC2 à laquelle vous voulez attacher l'Elastic IP (votre "Serveur Web Dev", par exemple).
  - Laissez le champ Private IP par défaut pour associer l'Elastic IP à l'IP privée de l'instance, Une liste des adresses IP privées associées à vos instances EC2 s'affichera.
  - Cliquez sur Associate (Associer).
- L'instance EC2 sera désormais accessible via l'Elastic IP que vous venez de générer.



## Résilier (libérer) l'Elastic IP

Une fois que vous avez fini de tester ou que l'Elastic IP n'est plus nécessaire, vous pouvez la libérer pour éviter tout frais supplémentaire.

1. Dissocier l'Elastic IP :
  - o Revenez dans la section Elastic IPs de la console EC2.
  - o Sélectionnez l'Elastic IP que vous avez attachée.
  - o Cliquez sur Actions > Disassociate Elastic IP address (Dissocier l'adresse Elastic IP).
  - o Confirmez la dissociation.
2. Libérer l'Elastic IP :
  - o Sélectionnez à nouveau l'Elastic IP dissociée.
  - o Cliquez sur Actions > Release Elastic IP address (Libérer l'adresse Elastic IP).
  - o Confirmez que vous souhaitez libérer l'adresse IP.
3. L'Elastic IP sera désormais libérée et ne sera plus facturée.

The image contains two screenshots of the AWS Elastic IP management interface. Both screenshots show a table with one row of data:

Name	Adresse IPv4 allouée	Type	ID d'allocation
-	35.181.244.153	Adresse IP publique	eipalloc-0fa60588755ce818

In the top screenshot, the 'Actions' dropdown menu is open, and the 'Associate l'adresse IP Elastic' option is highlighted. In the bottom screenshot, the 'Actions' dropdown menu is open again, but the 'Release' option is highlighted, indicating the process of releasing the IP address.

## Elastic Network Interface (ENI) :

Une ENI (Elastic Network Interface) est une carte réseau virtuelle dans AWS, qui représente une interface réseau avec une ou plusieurs adresses IP associées. Chaque instance EC2 a par défaut une ENI primaire, mais vous pouvez en créer plusieurs pour ajouter des interfaces réseau supplémentaires à une instance.

Une ENI inclut :

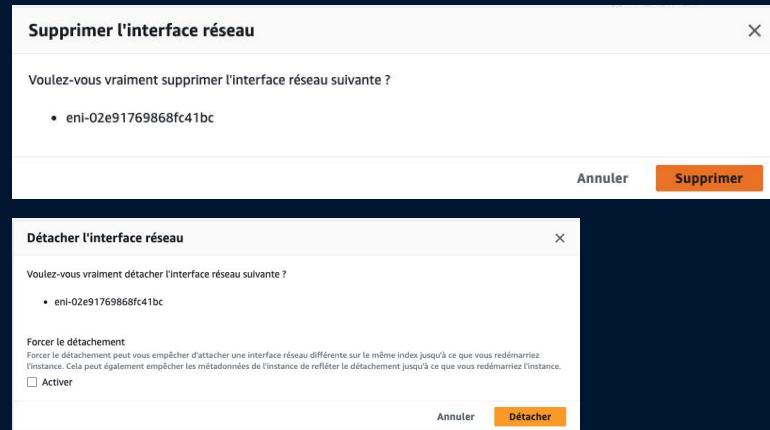
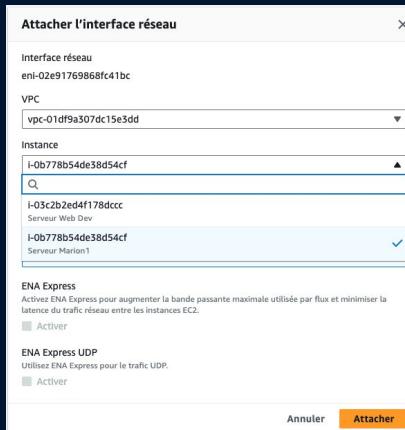
- Une ou plusieurs adresses IP privées.
- Une adresse IP publique (si nécessaire).
- Un ou plusieurs groupes de sécurité.
- Un Mac address.

Utilisation d'une ENI :

- Haute disponibilité : En cas de défaillance d'instance, vous pouvez détacher l'ENI et la réattacher à une autre instance pour maintenir la connectivité réseau.
- Segmentation réseau : Permet d'attribuer différentes interfaces pour séparer le trafic réseau (par exemple, front-end et back-end).
- Gestion de plusieurs adresses IP : Permet d'attribuer plusieurs IP à une seule instance pour des besoins spécifiques.

## Étapes pour créer et attacher une ENI :

1. Créer une ENI :
  - o Accédez à la console AWS, dans la section EC2.
  - o Sous Network & Security, cliquez sur Network Interfaces (Interfaces réseau).
  - o Cliquez sur Create Network Interface (Créer une interface réseau).
  - o Donnez un nom à l'ENI, sélectionnez un sous-réseau, et attachez un groupe de sécurité.
  - o Cliquez sur Create pour créer l'ENI.
2. Attacher l'ENI à une instance EC2 :
  - o Sélectionnez l'ENI que vous venez de créer.
  - o Cliquez sur Actions > Attach. (il faut que la zone de disponibilité de mon instance et de mon eni soit la même : par exemple eu-west-3a)
  - o Sélectionnez votre instance EC2 à laquelle vous voulez attacher l'ENI.
  - o Cliquez sur Attach.
3. Résilier l'ENI :
  - o Après avoir testé, retournez dans la section Network Interfaces.
  - o Sélectionnez l'ENI, cliquez sur Actions > Detach pour la dissocier de l'instance.
  - o Puis, sélectionnez Delete pour la résilier.



ID du groupe	Nom du groupe	Description
sg-0018f2e217e4275cb	Dev-SecurityGroup	Pare-feu du groupe dev

## Groupes de placement dans AWS EC2 :

**Les groupes de placement dans AWS EC2 permettent de contrôler la manière dont les instances EC2 sont déployées au sein du réseau AWS. Ils optimisent la latence réseau et la résilience des instances selon les besoins spécifiques de l'application (faible latence ou haute disponibilité). Il existe trois types de groupes de placement.**

## En quoi consiste l'hibernation d'une instance EC2 ?

L'hibernation d'une instance EC2 permet de suspendre une instance tout en préservant son état complet (mémoire RAM et stockage) afin de la restaurer exactement comme elle était au moment de l'hibernation. Contrairement à l'arrêt classique, l'hibernation sauvegarde le contenu de la mémoire vive (RAM) sur le volume de stockage, permettant à l'instance de reprendre son exécution avec ses applications et ses données inchangées.

## Fonctionnement de l'hibernation :

1. Sauvegarde de la mémoire RAM : Le contenu de la RAM est enregistré sur le volume racine EBS.
2. Arrêt de l'instance : Une fois que la mémoire est sauvegardée, l'instance est arrêtée.
3. Reprise : Lors du redémarrage, l'instance récupère le contenu de la RAM et reprend exactement là où elle s'était arrêtée.

## Avantages de l'hibernation :

- Conserve l'état des applications : Tous les processus en cours d'exécution (applications, sessions utilisateur) sont préservés.
- Reprise rapide : L'instance reprend immédiatement son état précédent sans avoir à redémarrer et réinitialiser tous les services.
- Économie d'énergie : Pendant l'hibernation, l'instance est arrêtée et vous ne payez pas pour les ressources CPU ou RAM, mais uniquement pour le stockage (EBS).

## Conditions pour utiliser l'hibernation :

- L'instance doit utiliser un volume racine EBS chiffré.
- Certaines tailles d'instance prennent en charge l'hibernation, généralement les types T2, T3, M3, M4, M5, C3, C4, C5, et R3.
- La taille de la RAM ne doit pas dépasser 150 Go.
- Les instances doivent utiliser une AMI compatible avec l'hibernation.

Type de groupe de placement	Utilisation	Caractéristique clé
Cluster	Applications nécessitant une faible latence et une bande passante élevée (calculs haute performance, big data).	Instances regroupées dans un même rack physique, faible tolérance aux pannes.
Partition	Applications nécessitant une tolérance aux pannes (bases de données distribuées).	Instances séparées en partitions isolées les unes des autres pour éviter les pannes matérielles.
Spread	Charges de travail critiques nécessitant une fiabilité élevée et une tolérance aux pannes.	Instances réparties sur des racks distincts, haute tolérance aux pannes (7 instances maximum par AZ).

## Étapes pour activer l'hibernation sur votre instance EC2 :

### 1. Vérifier la compatibilité :

- Assurez-vous que votre instance est de type compatible (par exemple, T2, T3, M4, M5, etc.).
- Le volume racine de votre instance doit être chiffré.

### 2. Configurer l'hibernation lors du lancement de l'instance :

- Lors de la configuration de l'instance EC2, dans la section Advanced Details (Détails avancés), vous devez cocher l'option Enable hibernation (Activer l'hibernation). Il n'est pas possible d'activer l'hibernation sur une instance EC2 déjà en cours d'exécution ou déjà créée si cette option n'a pas été activée lors de son lancement. L'hibernation doit être configurée au moment du lancement de l'instance. Je vais donc recréer une instance. Avec ces caractéristiques suivantes : Volume chiffré et Comportement d'arrêt (hibernation) activé

Stockage (volumes) Informations Simple

EBS Volumes Masquer les informations

Volume 1 (Racine AMI) (Personnalisé)

Type de stockage Informations Nom du périphérique - obligatoire Instantané Informations EBS snap-0df95e947ed77781a /dev/xvda

Taille (Gi) Informations Type de volume Informations IOPS Informations 8 gp2 100 / 3000

Supprimer à la résiliation Informations Chiffré Informations Clé KMS Informations Oui Chiffré Sélectionnez Non chiffré

Ajouter un volume

Clicker sur Actualiser pour afficher les informations de sauvegarde Les balises que vous attribuez déterminent si l'instance sera sauvegardée conformément aux stratégies de Data Lifecycle Manager.

Systèmes de fichiers Afficher les informations

Comportement d'arrêt – de veille prolongée Informations

Activer

Pour activer la mise en veille prolongée, de l'espace est alloué sur le volume racine pour stocker la mémoire (RAM) de l'instance. Veillez à ce que le volume racine soit suffisamment grand pour stocker le contenu de la RAM sans nuire à vos prévisions d'utilisation, par exemple le système d'exploitation ou les applications. Pour utiliser la mise en veille prolongée, le volume racine doit être un volume EBS chiffré. En savoir plus

### 3. Lançer l'instance avec l'option d'hibernation activée.

#### 4. Hiberner l'instance :

- Une fois l'instance lancée, vous pouvez l'hiberner à partir de la console AWS.
- Allez dans Actions > Instance State > Hibernate (Hiberner).

#### 5. Reprise de l'instance :

- Pour relancer l'instance, cliquez sur Instance State > Start.
- L'instance récupérera son état tel qu'il était au moment de l'hibernation.

EC2 > Instances > i-0d6d20283c335ae67 > Manage instance state

Manage instance state

Instance details

i-0d6d20283c335ae67 (MarionZ) running

Instance State Settings

Beginning Available when instance is stopped

Stop

Hibernate

Restart

Terminate

Cancel Change status

## Comportement d'une instance EC2 en hibernation :

1. Sauvegarde de la RAM : L'état de la mémoire (RAM) est sauvegardé sur le volume racine EBS, incluant toutes les applications et sessions en cours.
2. Arrêt : L'instance passe en arrêt hiberné, libérant les ressources (CPU, mémoire, réseau). Vous ne payez que pour le stockage EBS.
3. Reprise : Lors de la relance, l'instance récupère son état exact (applications et services restaurés comme avant l'hibernation) sans redémarrage complet.
4. Temps de reprise : Plus rapide qu'un démarrage normal, mais dépend de la taille de la RAM.

## Avantages :

- État préservé : Les applications reprennent là où elles se sont arrêtées.
- Coût réduit : Seul le stockage EBS est facturé pendant l'hibernation.

L'hibernation est idéale pour les environnements où les sessions doivent être rapidement restaurées sans redémarrer complètement.

## Présentation des volumes EBS et EFS :

- EBS (Elastic Block Store) : EBS fournit un stockage de blocs persistant pour les instances EC2. Chaque volume EBS est lié à une instance EC2 et fonctionne comme un disque dur externe. Il est conçu pour des performances élevées et un stockage persistant même après l'arrêt de l'instance EC2.
- EFS (Elastic File System) : EFS est un système de fichiers partagé basé sur NFS (Network File System). Il permet à plusieurs instances EC2 d'accéder simultanément à un même système de fichiers partagé, de manière élastique et sans gestion manuelle de la capacité.

	Caractéristiques	Utilisations courantes	Contraintes techniques
EBS (Elastic Block Store)	Stockage en blocs (comme un disque dur traditionnel). Peut être attaché à une seule instance EC2 à la fois. Types de volumes variés (gp2, io1) pour adapter les performances (latence faible, IOPS élevés). Taille configurable, jusqu'à 16 To par volume.	Bases de données, applications nécessitant un accès rapide à des données persistantes. Environnements où chaque instance EC2 a besoin de son propre espace de stockage. Snapshots pour sauvegarder et restaurer les volumes.	Attaché à une seule instance à la fois (sauf en mode multi-attach pour certaines configurations). Pas de partage natif entre instances EC2. La taille des volumes est fixe et nécessite une redimension si besoin.
EFS (Elastic File System)	Système de fichiers partagé accessible par plusieurs instances EC2 simultanément. Évolué automatiquement selon les besoins (jusqu'à plusieurs pétabytes). Basé sur NFSv4, avec gestion automatique de la capacité. Facturé en fonction de la taille des données stockées.	Applications distribuées ou clustering où plusieurs instances EC2 doivent partager des fichiers. Stockage de fichiers nécessitant une échelle automatique. Idéal pour les environnements multizone avec haute disponibilité.	Plus coûteux que l'EBS pour les petits volumes de données. Performances dépendantes du mode de performance (standard ou provisionné) et de la quantité de données stockées. Utilisation limitée à des environnements où les performances réseau sont acceptables (latence réseau).

## L'hibernation est particulièrement utile pour :

- Environnements de test ou de développement où les sessions doivent être préservées sur une longue période.
- Chargements temporaires de services que vous souhaitez interrompre et reprendre rapidement plus tard.

Si vous avez mis en place une instance avec l'hibernation et que vous l'avez testée, vous devriez avoir observé que le retour à l'état initial est plus rapide qu'un redémarrage complet. Le coût est également réduit pendant la période d'hibernation, car seules les ressources de stockage (EBS) sont facturées.

**Une Amazon Machine Image (AMI)** est une image préconfigurée qui contient toutes les informations nécessaires pour démarrer une instance EC2, y compris :

- Le système d'exploitation (Linux, Windows, etc.).
- Les paramètres de configuration.
- Les applications installées.
- Les données d'application si nécessaire.

**Les AMIs permettent de déployer rapidement de nouvelles instances avec des configurations spécifiques et récurrentes, et sont également utilisées pour sauvegarder l'état d'une instance existante.**

Type d'AMI	Utilisation	Differences
AMI AWS officielles	Démarrage rapide d'instances avec un système d'exploitation propre, environnements de développement ou de production standards	Images fournies par AWS avec configurations par défaut
AMI personnalisées	Sauvegarde d'instances avec des applications spécifiques pour un déploiement rapide, automatisation de déploiements spécifiques	Crées par les utilisateurs à partir d'instances EC2 existantes avec des configurations spécifiques
AMI du Marketplace	Déploiement de solutions logicielles prêtes à l'emploi, utilisation de logiciels commerciaux ou solutions spécifiques	Images fournies par des éditeurs tiers avec des logiciels ou solutions préinstallés

Instances (1/1) Informations

Date de la dernière mise à jour : Il y a 1 minute

Lancer des instances

ID d'instance = i-063df2ba4bf9c447b

Effacer les filtres

marion3 i-063df2ba4bf9c447b En cours d'...

Créer une image

Créer un modèle à partir de l'instance

En lancer plus comme ceci

### Étapes pour créer une AMI et la réutiliser :

1. Créer une AMI à partir d'une instance existante :
  - o Dans la console EC2, sélectionnez l'instance de Job 1.
  - o Cliquez sur Actions > Image et modèles > Créer une image (Create Image).
  - o Remplissez les informations demandées, comme le nom de l'image, et cliquez sur Create.
2. Lancer une nouvelle instance à partir de l'AMI créée :
  - o Dans la console EC2, allez dans la section Images > AMI.
  - o Sélectionnez l'AMI que vous avez créée, puis cliquez sur Lancer une instance à partir de l'AMI.
  - o Suivez les étapes de configuration habituelles pour créer la nouvelle instance.
3. Captures d'écran :
  - o Prenez des captures à chaque étape pour documenter la création de l'AMI et le lancement d'une instance à partir de celle-ci.
4. Suppression de l'AMI :
  - o Une fois que vous avez fini d'utiliser l'AMI, revenez dans la section AMI, sélectionnez l'AMI, puis cliquez sur Actions > Deregister (Désinscrire).

Amazon Machine Images (AMI) (1/1) Informations

M'appartenant

Rechercher AMI par attribut ou id

Name : Image1

Lancer une instance à partir d'une AMI

Copier l'AMI

Modifier les autorisations AMI

Demander des instances Spot

Gérer les balises

Désenregister une AMI

Gérer la protection contre le désenregistrement d'AMI

**Pour chiffrer le volume d'une instance EC2 existante, il faut généralement suivre ces étapes. AWS ne permet pas de chiffrer directement un volume EBS non chiffré déjà en cours d'utilisation. Vous devrez donc créer un snapshot, le chiffrer, puis créer un nouveau volume à partir de ce snapshot chiffré.**

Étapes pour chiffrer un volume EBS existant :

#### Créer un Snapshot du volume non chiffré :

- Accédez à la console AWS EC2.
- Dans la section Volumes (sous la rubrique Elastic Block Store), sélectionnez le volume que vous voulez chiffrer.
- Cliquez sur Actions > Create Snapshot (Créer un instantané).
- Donnez un nom et une description à votre snapshot, puis cliquez sur Create Snapshot.

Créer un nouveau volume chiffré à partir du Snapshot :

- Une fois le snapshot créé, allez dans Snapshots dans le menu de gauche.
- Sélectionnez le snapshot que vous venez de créer, puis cliquez sur Actions > Copy (Copier).
- Lors de la copie, sélectionnez l'option Encrypt this snapshot (Chiffrer cet instantané).
- Choisissez la clé KMS par défaut ou une clé personnalisée pour chiffrer le volume.

#### 3. Créer un volume à partir du Snapshot chiffré :

- Une fois le snapshot copié et chiffré, allez dans la section Snapshots.
- Sélectionnez le snapshot chiffré, puis cliquez sur Actions > Create Volume (Créer un volume).
- Configurez les options du volume (taille, type, zone de disponibilité), puis cliquez sur Create Volume.

#### 4. Détacher l'ancien volume et attacher le nouveau volume chiffré :

- Allez dans la section Volumes, sélectionnez le volume non chiffré actuellement attaché à votre instance EC2.
- Cliquez sur Actions > Detach Volume (Détacher le volume).
- Ensuite, sélectionnez le nouveau volume chiffré que vous avez créé, puis cliquez sur Actions > Volume (Attacher le volume).
- Attachez-le à votre instance EC2 en spécifiant le périphérique (généralement /dev/sda1 pour la racine).

The screenshot displays the AWS Management Console interface for managing volumes and snapshots. It shows three main windows:

- Volumes (1/3) Informations:** Shows a list of volumes. One volume is selected (gp3) with the status "Chiffré".
- Volumes (1/3) Informations:** Shows a list of snapshots. One snapshot is selected (snap-0e146ee850c142f) with the status "Chiffré".
- Attacher un volume:** A modal window for attaching a volume to an instance. It shows the selected volume (vol-0f67500c50213352f) and the target instance (i-0a146ee850c142f). The "Encrypt this volume" checkbox is checked. The "Attach" button is visible at the bottom right.

Suite des étapes :

**Instantanés (1/2) Informations**

M'appartenant | Rechercher

Name	ID d'instantané	Taille du volume	Description	Niveau de protection	Statut
<input checked="" type="checkbox"/> snap-0e146ee850c14e896	8 GiB	Volume_chiffre1	Standard	<input checked="" type="radio"/>	Terminé
<input type="checkbox"/> snap-058ba1f5aec127c9b	8 GiB	Created by CreateImage(i-O...)	Standard	<input type="radio"/>	En cours

Actions ▾

- 
- 
- 
- 
- 
- 
- 

**Instantané source**  
L'instantané original à copier.

ID d'instantané : snap-0e146ee850c14e896      Région : us-east-1

**Détails de la copie de l'instantané**

Description : Une description pour la copie de l'instantané.  
[Copied snap-0e146ee850c14e896 from us-east-1] Volume\_chiffre1  
255 caractères maximum.

Région de destination : us-east-1

Chiffrement | Informations : Utilisez le chiffrement Amazon EBS comme solution de chiffrement pour vos ressources EBS.  
 Chiffrez cet instantané

**Instantanés (1/2) Informations**

M'appartenant | Rechercher

Name	ID d'instantané	Taille du volume	Description	Niveau de protection	Statut
<input checked="" type="checkbox"/> snap-0e146ee850c14e896	8 GiB	Volume_chiffre1	Standard	<input checked="" type="radio"/>	Terminé
<input type="checkbox"/> snap-058ba1f5aec127c9b	8 GiB	Created by CreateImage(i-O...)	Standard	<input type="radio"/>	En cours

Actions ▾

- 
- 
- 
- 
- 
- 
- 

**Instantanés (1/3) Informations**

M'appartenant | Rechercher

Name	ID d'instantané	Taille du volume	Description	Niveau de protection	Statut
<input type="checkbox"/> snap-0e146ee850c14e896	8 GiB	Volume_chiffre1	Standard	<input type="radio"/>	En cours
<input type="checkbox"/> snap-058ba1f5aec127c9b	8 GiB	Created by CreateImage(i-O...)	Standard	<input checked="" type="radio"/>	Terminé
<input checked="" type="checkbox"/> snap-0b1384c93a06da685	8 GiB	[Copied snap-0e146...	Standard	<input checked="" type="radio"/>	Terminé

Actions ▾

- 
- 
- 
- 
- 
- 
-



03

## Entra ID (ex Azur AD)

Vous allez voir comment utiliser les potentialités d'Entra ID (ex Azure AD) pour apprendre à administrer une infrastructure cloud. Il sera impératif de documenter chacune des étapes qui vous ramèneront à la réalisation des Jobs. On utilisera le terme 'Entra ID' ou 'Azure' dans le sujet.

## Qu'est-ce que Entra ID ?

Entra ID, anciennement Azure AD, est un service de gestion des identités et des accès dans le cloud de Microsoft. Il permet aux organisations de contrôler qui peut accéder aux ressources et aux applications, tout en renforçant la sécurité. Voici ses principales fonctionnalités :

1. Authentification et SSO : Permet aux utilisateurs de se connecter une seule fois pour accéder à plusieurs applications (Single Sign-On) et supporte l'authentification multifacteur (MFA).
2. Gestion des utilisateurs et rôles : Gère centralement les identités des utilisateurs et leurs autorisations via des rôles spécifiques.
3. Accès conditionnel : Définition de politiques pour contrôler les accès en fonction du contexte (appareil, emplacement, etc.).
4. Sécurité Zero Trust : Stratégie de sécurité qui vérifie systématiquement chaque demande d'accès.
5. Intégration avec des applications SaaS : Prise en charge des applications cloud comme Office 365, Salesforce, etc.