

# AWS / Azure(AD) Entra ID

## JOUR 1 AWS - IAM & EC2



## Félicitations !

Merci de vous être inscrit à AWS.

Nous procédons actuellement à l'activation de votre compte. Cela devrait prendre quelques minutes. Vous recevrez un e-mail au terme de la procédure.

[Accéder à la console de gestion AWS](#)

[Créer un autre compte ou contacter le service commercial](#)

Billing and Cost Management > Budgets > Overview

**Budgets (1)** [Info](#) [Download CSV](#) [Actions](#) [Create budget](#)

<input type="checkbox"/>	Name	Thresholds	Budget	Amount ...	Forecast...	Current vs. bu...
<input type="checkbox"/>	<a href="#">My Zero-Spend Budget</a>	<input checked="" type="checkbox"/> OK	\$1.00	\$0.00	-	

## AWS IAM

AWS IAM (Identity and Access Management): IAM est un service de gestion des identités et des accès. Il permet de contrôler de manière sécurisée l'accès aux ressources AWS. Avec IAM, vous pouvez créer et gérer des utilisateurs, des groupes et des rôles, ainsi que définir des permissions précises.

# Le Principe du Moindre Privilège

## **Définition du principe du moindre privilège**

Le principe du moindre privilège (PMP), également connu sous le nom de principe du privilège minimum, est un concept fondamental en sécurité informatique. Il stipule qu'un utilisateur, un programme ou un processus ne devrait avoir que les privilèges minimums nécessaires pour accomplir sa tâche.

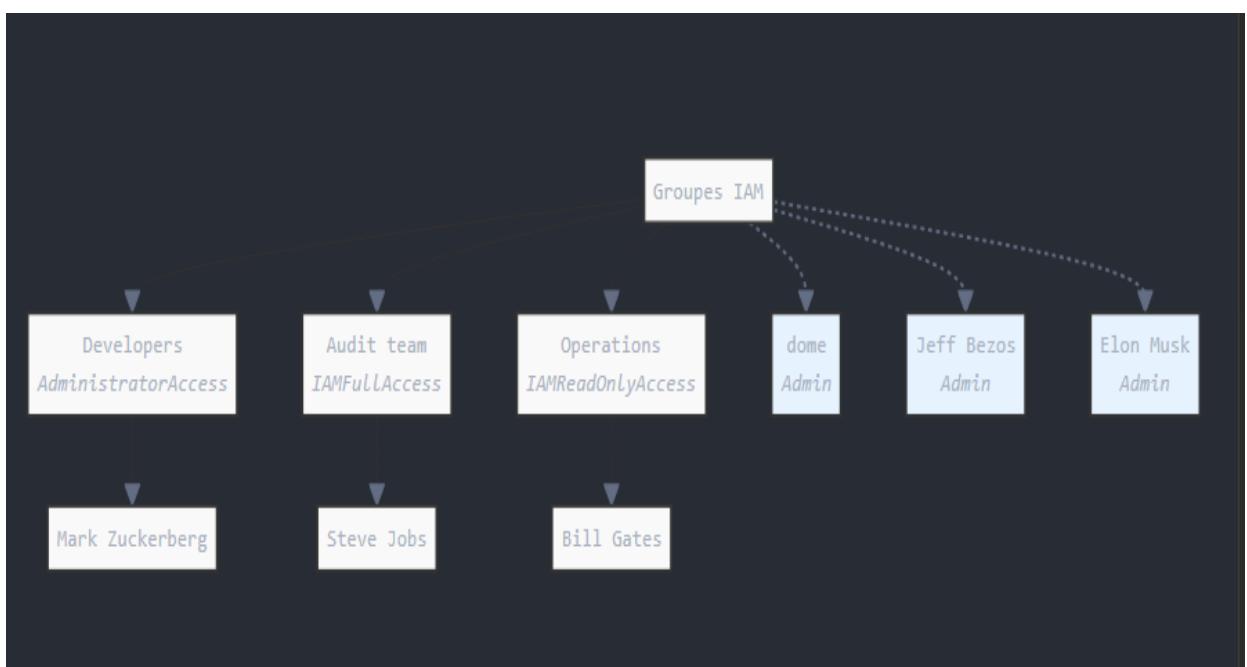
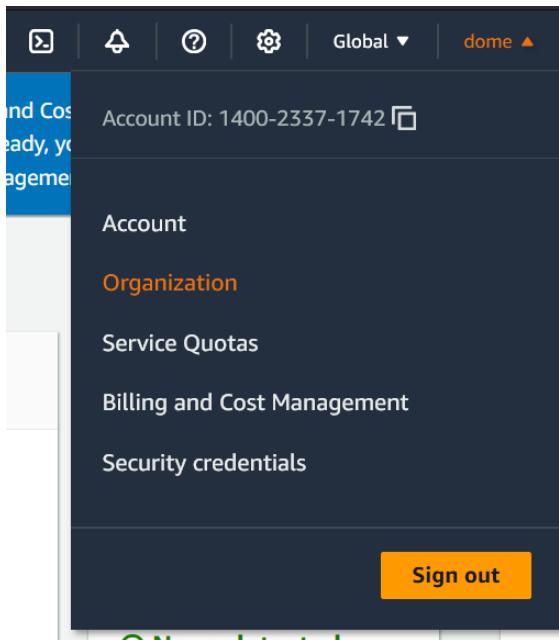
## **Importance dans le contexte AWS**

Dans le cadre d'AWS et plus particulièrement d'IAM (Identity and Access Management), le PMP est crucial pour plusieurs raisons :

1. **\*\*Réduction de la surface d'attaque\*\*** : En limitant les privilèges, on réduit les possibilités d'exploitation en cas de compromission d'un compte.
2. **\*\*Limitation des dommages potentiels\*\*** : Si un compte est compromis, les dégâts seront limités aux ressources auxquelles ce compte a accès.
3. **\*\*Conformité\*\*** : De nombreuses normes de sécurité et réglementations (comme GDPR, PCI DSS) exigent l'application du PMP.
4. **\*\*Audit simplifié\*\*** : Il est plus facile de suivre et d'auditer les actions lorsque les privilèges sont clairement définis et limités.

En appliquant rigoureusement le PMP(principe du moindre privilège), on renforce considérablement la sécurité de l'infrastructure AWS, réduisant ainsi les risques de

violations de données ou d'utilisations non autorisées des ressources.



Groupe	Clé (Key)	Valeur (Value)
Developers	Role	Developer
	AccessLevel	Full
	Department	Engineering
Audit team	Role	Auditor
	AccessLevel	IAMFull
	Department	Compliance
Operations	Role	Operator
	AccessLevel	IAMReadOnly
	Department	IT

### Création des groupes :

- Dans la console AWS, allez dans le service IAM.
- Dans le menu de gauche, cliquez sur "User groups" (Groupes d'utilisateurs).
- Cliquez sur "Create group" (Créer un groupe).
- Créez les trois groupes un par un :
  - Nom : "Developers" - Attachez la politique "AdministratorAccess"
  - Nom : "Audit team" - Attachez la politique "IAMFullAccess"
  - Nom : "Operations" - Attachez la politique "IAMReadOnlyAccess"

The screenshot shows the AWS IAM Groups page. At the top, there is a header with the title "Groupes d'utilisateurs (3) Infos" and buttons for "Supprimer" (Delete) and "Créer un groupe" (Create group). Below the header, a message states: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." There is a search bar labeled "Rechercher". To the right of the search bar are navigation icons for pages 1, 2, and 3, and a refresh icon. A table below the message lists the three user groups:

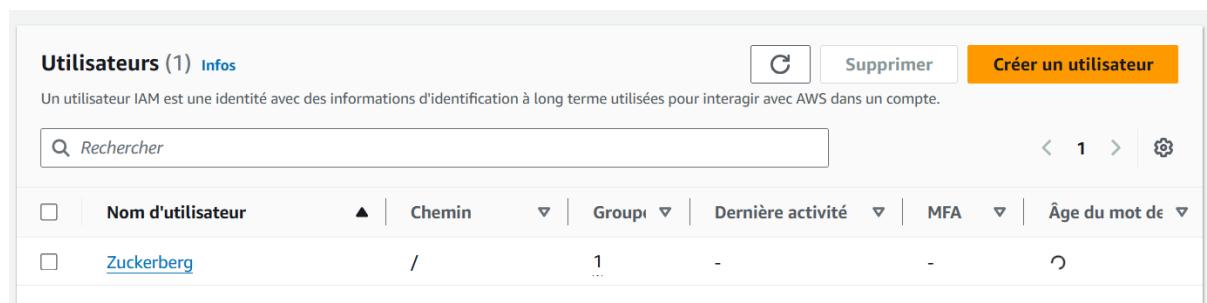
Nom du groupe	Utilisateurs	Autorisations	Heure de création
<a href="#">AuditTeam</a>	⚠ 0	✔ Défini	Il y a 20 minutes
<a href="#">Developers</a>	1	✔ Défini	Il y a 22 minutes
<a href="#">Operations</a>	⚠ 0	✔ Défini	Il y a 20 minutes

## Ajouter les utilisateurs admin

- Jeff Bezos ( admin )
- Elon Musk ( admin )

Dans le panneau de navigation à gauche, cliquez sur "Users" (Utilisateurs).

Cliquez sur "Add users" (Ajouter des utilisateurs).



The screenshot shows the AWS IAM Users interface. At the top, there is a header with the title "Utilisateurs (1) [Infos](#)". To the right of the title are three buttons: "Supprimer" (Delete), "Créer un utilisateur" (Create a user), and a "C" icon. Below the header, a message states: "Un utilisateur IAM est une identité avec des informations d'identification à long terme utilisées pour interagir avec AWS dans un compte." A search bar labeled "Rechercher" is followed by a pagination indicator "[1](#)". The main table lists one user: "Zuckerberg". The columns in the table are: "Nom d'utilisateur" (User name), "Chemin" (Path), "Groupe" (Group), "Dernière activité" (Last activity), "MFA" (MFA), and "Âge du mot de passe" (Age of password). The "Nom d'utilisateur" column shows "Zuckerberg" with a checkbox next to it.

Pour chaque utilisateur (Jeff Bezos et Elon Musk), suivez ces étapes :

- a. Entrez le nom d'utilisateur (par exemple, "jeff.bezos" et "elon.musk").
- b. Cochez "Provide user access to the AWS Management Console" (Fournir un accès utilisateur à la console de gestion AWS).
- c. Choisissez "I want to create an IAM user" (Je veux créer un utilisateur IAM).
- d. Définissez un mot de passe fort et unique pour chaque utilisateur.

e. Cliquez sur "Next: Permissions" (Suivant : Autorisations).

Sur l'écran des permissions :

a. Cliquez sur "Attach existing policies directly" (Attacher directement des politiques existantes).

The screenshot shows the 'Régler les autorisations' (Set permissions) page in AWS IAM. At the top, there are three options: 'Ajouter un utilisateur à un groupe' (Add user to group), 'Copier les autorisations' (Copy permissions), and 'Attacher directement des politiques' (Attach directly). The third option is selected. Below this, a section titled 'Politiques des autorisations (1233)' shows a list of policies. A search bar at the top of the list is set to 'Rechercher' and contains the text 'AdministratorAccess'. The list includes two items:

Nom de la politique	Type	Entités attachées
<a href="#">AccessAnalyzerServiceRoleP...</a>	Gérées par AWS	0
<a href="#">AdministratorAccess</a>	Gérées par AWS – fonction profession...	1

b. Recherchez et cochez la case à côté de "*AdministratorAccess*".

c. Cliquez sur "Next: Tags" (Suivant : Balises).

Ajoutez des balises si nécessaire (par exemple, "Role: Admin"), dans notre cas, pour les administrateurs, utiliser :

- Clé (Key): "Role"
- Valeur (Value): "Admin"

puis cliquez sur "Next: Review" (Suivant : Vérification).

Vérifiez les informations et cliquez sur "Create user" (Créer l'utilisateur).

Répétez ce processus pour le deuxième administrateur.

*Jeff Bezos = jeffadmin*

*Elon Musk = Elon@admin*

## Ajouter les utilisateurs

- Mark Zuckerberg ( utilisateur simple sans droit )

- Steve Jobs ( utilisateur simple sans droit )

- Bill Gates ( utilisateur simple sans droit )

Dans le panneau de navigation à gauche, cliquez sur "Users" (Utilisateurs).

Cliquez sur "Add users" (Ajouter des utilisateurs).

Pour chaque utilisateur, suivez ces étapes :

a. Entrez le nom d'utilisateur

b. Cochez "Provide user access to the AWS Management Console" (Fournir un accès utilisateur à la console de gestion AWS).

c. Choisissez "I want to create an IAM user" (Je veux créer un utilisateur IAM).

d. Définissez un mot de passe personnalisé ou laissez AWS en générer un automatiquement.

e. Cliquez sur "Next: Permissions" (Suivant : Autorisations)

Sur l'écran des permissions :

- Pour votre personnel et les administrateurs, vous pouvez attacher directement la politique "*AdministratorAccess*".
- Pour les utilisateurs simples (Mark Zuckerberg, Steve Jobs, Bill Gates), ne sélectionnez aucune permission pour le moment.

*Mark Zuckerberg -> Groupe Developers -> Attachez la politique "*AdministratorAccess*"*

- *Steve Jobs -> Groupe Audit team -> Attachez la politique "*IAMFullAccess*"*
- *Bill Gates -> Groupe Operations -> Attachez la politique "*IAMReadOnlyAccess*"*

Pour ajouter les utilisateurs aux groupes :

a) Sélectionnez le groupe.

b) Allez dans l'onglet Users" (Utilisateurs).

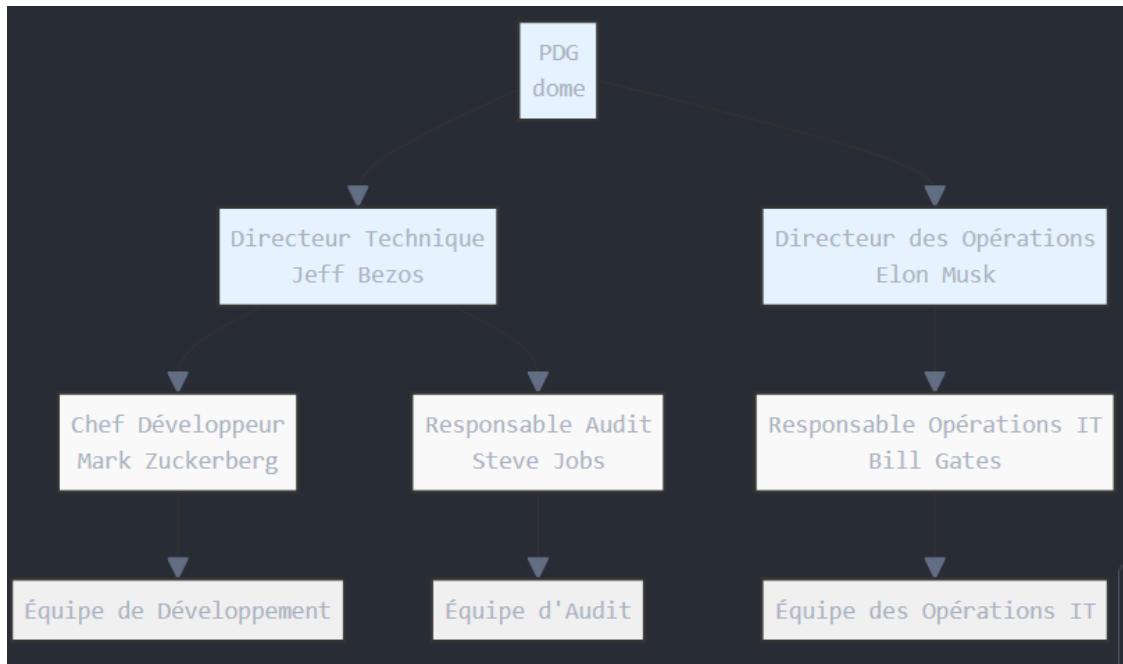
c) Cliquez sur "Add users" (Ajouter des utilisateurs).

d) Sélectionnez l'utilisateur approprié et ajoutez-le au groupe.

*Mark Zuckerberg -> Developers aD19l9(e*

*Steve Jobs -> Audit team |3j+X6Q{*

*Bill Gates -> Operations vBe-#\_5\$*



## Configuration de la politique de mot de passe et activation de la MFA

### Configuration de la politique de mot de passe

#### Étape 1 : Accéder aux paramètres du compte

- Connectez-vous à la console AWS avec votre compte administrateur.
- Cliquez sur le nom de votre compte en haut à droite, puis sélectionnez "Security credentials" (Informations d'identification de sécurité).

IAM > Informations d'identification de sécurité

**Mes autorisations de sécurité** Root user Infos

L'utilisateur root a accès à toutes les ressources AWS de ce compte ; nous recommandons de suivre les [bonnes pratiques](#) suivantes. Pour en savoir plus sur les types d'informations d'identification AWS et la manière dont elles sont utilisées, consultez [Informations d'identification de sécurité AWS](#) dans les références générales AWS

<b>Aucune MFA ne vous a pas été attribuée</b> Comme bonne pratique de sécurité, nous vous recommandons d'activer l'authentification MFA.	<a href="#">Affecter l'authentification MFA</a>
<b>Détails du compte</b>	
Nom du compte dome	Modifier le nom du compte, l'adresse e-mail et le mot de passe
ID de compte AWS <input type="text"/> 140023371742	Adresse e-mail domenico.mandolino@laplateforme.io
ID d'utilisateur canonique : <input type="text"/> 10d9e8bec5b43a6ee1b34b47f203750ee818ea2f97f3f2198df81f1bf484fb9b9	
<b>Authentification multi-factor (MFA) (0)</b>	
Utilisez l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre environnement AWS. La connexion avec la MFA nécessite un code d'authentification provenant d'un dispositif MFA. Chaque utilisateur peut disposer au maximum de huit dispositifs MFA attribués. <a href="#">En savoir plus</a>	
<a href="#">Supprimer</a> <a href="#">Resynchroniser</a> <a href="#">Attribuer un dispositif MFA</a>	

#### Étape 2 : Accéder aux paramètres du compte:

- Dans le panneau de navigation à gauche, faites défiler vers le bas et cliquez sur "Account settings" (Paramètres du compte).

Trouver la section de politique de mot de passe:

- Sur cette page, vous devriez voir une section intitulée "Password policy" (Politique de mot de passe).

Modifier la politique:

- Cliquez sur le bouton "Edit" (Modifier) à côté de "Password policy".

Étape 3 : Configurer la politique: Une fois que vous avez cliqué sur "Edit", vous devriez voir les options pour configurer la politique de mot de passe. Voici comment les configurer selon les exigences du projet:

- Set minimum password length (Définir la longueur minimale du mot de passe) : 12
- Require at least one uppercase letter (Exiger au moins une lettre majuscule) : Coché
- Require at least one lowercase letter (Exiger au moins une lettre minuscule) : Coché
- Require at least one number (Exiger au moins un chiffre) : Coché
- Require at least one non-alphanumeric character (Exiger au moins un caractère non alphanumérique) : Coché

Étape 4 : Enregistrer les modifications

- Après avoir configuré ces options, faites défiler vers le bas et cliquez sur "Save changes" (Enregistrer les modifications).

**Politique de mot de passe**

IAM par défaut  
Appliquez les exigences de mot de passe par défaut.

Personnalisé  
Appliquez les exigences de mot de passe personnalisé.

Longueur minimale du mot de passe.  
Appliquer une longueur minimale de caractères.  
**12** caractères  
Elle doit être comprise entre 6 et 128.

Force du mot de passe

Requiert au moins une lettre majuscule de l'alphabet latin (A-Z)  
 Requiert au moins une lettre minuscule de l'alphabet latin (a-z)  
 Nécessite au moins un chiffre  
 Requière au moins un caractère non alphanumérique (! @ # % ^ & \* () \_ + - = [ ] { } )

Autres exigences

Activer l'expiration des mots de passe  
 L'expiration du mot de passe nécessite la réinitialisation de l'administrateur.  
 Autoriser les utilisateurs à modifier leur propre mot de passe  
 Empêcher la réutilisation d'un mot de passe

Annuler **Enregistrer les modifications**

## Activation de la MFA pour le compte root

### Étape 1 : Accéder aux paramètres de sécurité du compte root

- Déconnectez-vous de votre compte administrateur et connectez-vous avec le compte root.
- Cliquez sur le nom du compte en haut à droite, puis sélectionnez "Security credentials".

### Étape 2 : Activer la MFA

- Dans la section "Multi-factor authentication (MFA)", cliquez sur "Assign MFA device" (Attribuer un dispositif MFA).
- Choisissez "Virtual MFA device" (Dispositif MFA virtuel).

Type	Identificateur	Certifications	Crée le
Aucun périphérique MFA. Attribuez un périphérique MFA pour améliorer la sécurité de votre environnement AWS			
<a href="#">Attribuer un dispositif MFA</a>			

### Étape 3 : Configurer l'application d'authentification

- Installez une application d'authentification sur votre smartphone (comme Google Authenticator ou Authy).

**MFA device name**

Nom du dispositif  
Ce nom sera utilisé dans l'ARN d'identification de cet appareil.

64 caractères au maximum. Utilisez des caractères alphanumériques et les caractères « + , . @ - \_ ».

**MFA device**

Options de l'appareil  
Outre le nom d'utilisateur et le mot de passe, vous utiliserez cet appareil pour vous authentifier sur votre compte.

**Clé d'accès ou clé de sécurité**  
Authentifiez-vous à l'aide de votre empreinte digitale, de votre visage ou du verrouillage d'écran. Créez une clé d'accès sur cet appareil ou utilisez un autre appareil, comme une clé de sécurité FIDO2.

**Application d'authentification**  
S'authentifier à l'aide d'un code généré par une application installée sur votre appareil mobile ou votre ordinateur.

- Scannez le code QR affiché sur l'écran AWS avec votre application d'authentification.

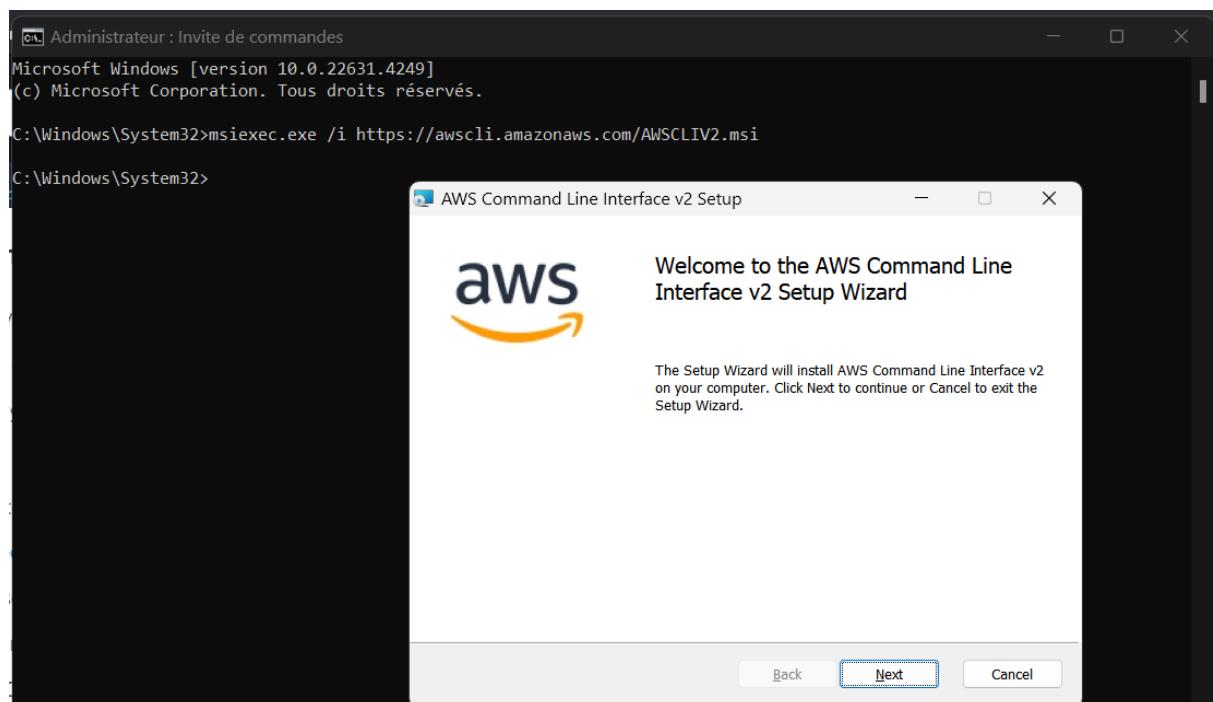
#### Étape 4 : Entrer les codes MFA

- Entrez deux codes MFA consécutifs générés par votre application d'authentification.
- Cliquez sur "Assign MFA" (Attribuer MFA).

### Télécharger la CLI AWS 2

Suivre les étapes sur le site officiel:

<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-version.html>



```
C:\ Administateur : Invite de commandes
Microsoft Windows [version 10.0.22631.4249]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>msiexec.exe /i https://awscli.amazonaws.com/AWSCLIV2.msi

C:\Windows\System32>aws --version
aws-cli/2.18.2 Python/3.12.6 Windows/11 exe/AMD64

C:\Windows\System32>
```

Si le système ne reconnaît pas encore la commande `aws`, fermez l'invite de commande actuelle et ouvrez-en une nouvelle. Parfois, les changements de chemin d'accès ne sont pas pris en compte immédiatement.

## Création d'un IAM Role "DemoForEC2" avec la permission "IAMReadOnlyAccess".

### Comprendre les IAM Roles :

Un IAM Role est une identité AWS à créer pour le compte et qui a des permissions spécifiques. Les rôles sont utilisés pour donner des accès temporaires à des utilisateurs ou des services AWS.

Ce rôle sera utilisé pour permettre à une instance EC2 (une machine virtuelle dans AWS) d'accéder à des informations IAM en lecture seule.

Étapes pour créer le rôle :

- Allez dans le service IAM (utilisez la barre de recherche en haut).
- Dans le menu de gauche, cliquez sur "Roles".

Tableau de bord

▼ Gestion des accès

Groupes d'utilisateurs

Utilisateurs

**Rôles**

Politiques

Fournisseurs d'identité

Paramètres du compte

- Cliquez sur le bouton "Create role".
- Sous "Trusted entity type", choisissez "AWS service".

## Sélectionner une entité de confiance Infos

### Type d'entité approuvée

#### Service AWS

Autorisez les services AWS tels qu'EC2, Lambda ou autre à effectuer des actions dans ce compte.

#### Compte AWS

Autorisez les entités d'autres comptes AWS qui appartiennent à vous à un tiers à effectuer des actions dans ce compte.

#### Identité Web

Permet aux utilisateurs fédérés par le fournisseur d'identité web externe spécifié d'assumer ce rôle pour effectuer des actions dans ce compte.

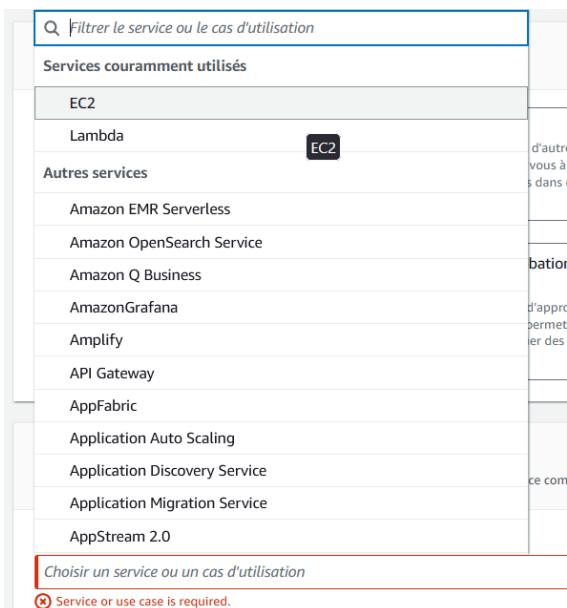
#### Fédération SAML 2.0

Autorisez les utilisateurs fédérés avec SAML 2.0 à partir d'un répertoire d'entreprise à effectuer des actions dans ce compte.

#### Stratégie d'approbation personnalisée

Créez une stratégie d'approbation personnalisée pour permettre à d'autres utilisateurs d'effectuer des actions dans ce compte.

- Sous "Use case", sélectionnez "EC2".



- Cliquez sur "Next".
- Dans la barre de recherche des permissions, tapez "IAMReadOnlyAccess".

Ajouter des autorisations [Infos](#)

**Politiques des autorisations (951) [Infos](#)**

Choisissez une ou plusieurs stratégies à attacher à votre nouveau rôle.

Nom de la politique		Type
<input type="checkbox"/>	IAMReadOnlyAccess	Gérées par AWS

▶ Définir une limite d'autorisations - facultatif

- Cochez la case à côté de "IAMReadOnlyAccess".

Informations du rôle

Nom du rôle  
Saisissez un nom explicite pour identifier ce rôle.

Description  
Ajoutez une brève explication de ce rôle.

Étape 1 : sélectionner des entités de confiance

Politique de confiance

```

1 ~ [object Object]
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [

```

- Cliquez sur "Next".
- Nommez le rôle "DemoForEC2".
- Ajoutez une description si vous le souhaitez.
- Cliquez sur "Create role".

Rôles (5) [Infos](#)

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. Les rôles peuvent être utilisés pour déléguer des autorisations à d'autres services et applications.

Nom du rôle	Entités de confiance
<a href="#">AWSServiceRoleForOrganizations</a>	Service AWS: organizations (Rôle lié à un service)
<a href="#">AWSServiceRoleForSSO</a>	Service AWS: sso (Rôle lié à un service)
<a href="#">AWSServiceRoleForSupport</a>	Service AWS: support (Rôle lié à un service)
<a href="#">AWSServiceRoleForTrustedAdvisor</a>	Service AWS: trustedadvisor (Rôle lié à un service)
<a href="#">DemoForEC2</a>	Service AWS: ec2

Vérification : Après avoir créé le rôle, vous devriez le voir dans la liste des rôles IAM. Cliquez dessus pour vérifier ses détails et ses permissions.

### Points importants à noter :

- Ce rôle ne donne que des accès en lecture aux ressources IAM.
- Il est spécifiquement conçu pour être utilisé par des instances EC2.
- C'est une bonne pratique de sécurité d'utiliser des rôles plutôt que des clés d'accès codées en dur dans les applications.

## Génération d'un rapport de credentials AWS.

Comprendre le AWS Credentials Report c'est un rapport qui liste tous les utilisateurs de votre compte AWS et l'état de leurs crédits (mots de passe, clés d'accès, MFA, etc.).

Étapes pour générer le rapport :

- a. Connectez-vous à la console AWS avec un compte administrateur.
- b. Allez dans le service IAM (utilisez la barre de recherche en haut).
- c. Dans le panneau de navigation à gauche, cliquez sur "Credential report".
- d. Cliquez sur le bouton "Download report" ou "Generate report" s'il n'a jamais été généré.

The screenshot shows the AWS IAM service interface. On the left, there's a sidebar with a search bar labeled 'Rechercher sur IAM'. Below it, under 'Gestion des accès', are links for Groupes d'utilisateurs, Utilisateurs, Rôles, Politiques, Fournisseurs d'identité, and Paramètres du compte. Under 'Rapports d'accès', there are links for Analyseur d'accès, Accès externe, Accès non utilisé, and Paramètres de l'analyseur. A blue link 'Rapport sur les informations d'identification' is highlighted. The main content area has a breadcrumb trail 'IAM > Rapport sur les informations d'identification'. It displays a section titled 'Rapport sur les informations d'identification des utilisateurs IAM associés à ce compte' with a 'Infos' link. Below it, a message says 'Le rapport sur les informations d'identification répertorie tous vos utilisateurs IAM associés à ce compte et le statut de leurs différentes informations d'identification'. There's a button 'Télécharger le rapport sur les informations d'identification' and a note 'Dernier rapport créé : Maintenant.'

Analyser le rapport :

- Le rapport est téléchargé au format CSV (Comma-Separated Values).

- Ouvrez-le avec un tableur comme Excel ou Google Sheets.

```
C:\> Users\Asus-Tuf-Laptop\Downloads> status_reports_Wed Oct 09 2024 12_55_56 GMT+0200 (heure d'été d'Europe centrale).csv x
1 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
2 <root_account>,arn:aws:iam::140023371742:root,2024-10-07T04:40:41Z,true,2024-10-09T10:55:08Z,2024-10-09T10:54:12Z,not_supported,true,false,N/A,N/A,N/A,N/A,N
3 BillGates,arn:aws:iam::140023371742:user/BillGates,2024-10-07T14:13:41Z,true,no_information,2024-10-07T14:13:41Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,fas
4 ElonMusk,arn:aws:iam::140023371742:user/ElonMusk,2024-10-08T19:14:51Z,true,no_information,2024-10-08T19:14:51Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,fals
5 JeffBezos,arn:aws:iam::140023371742:user/JeffBezos,2024-10-08T19:11:31Z,true,no_information,2024-10-08T19:11:31Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,N/A,fals
6 MarkZuckerberg,arn:aws:iam::140023371742:user/MarkZuckerberg,2024-10-07T14:12:24Z,true,no_information,2024-10-07T14:12:24Z,N/A,false,false,N/A,N/A,N/A,N/A,N
7 SteveJobs,arn:aws:iam::140023371742:user/SteveJobs,2024-10-07T14:09:37Z,true,no_information,2024-10-07T14:09:37Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,fals
```

Contenu du rapport : Le rapport inclut des informations comme :

- Nom d'utilisateur
  - Date de création du compte
  - Mot de passe activé/désactivé
  - Date du dernier changement de mot de passe
  - MFA activé/désactivé
  - Clés d'accès actives
  - Dernière utilisation des clés d'accès
  - Et bien d'autres informations...

## Importance du rapport :

- Il permet de surveiller l'état de sécurité des comptes utilisateurs.
  - Aide à identifier les comptes inactifs ou les credentials qui n'ont pas été rotés récemment.
  - Utile pour les audits de sécurité et la conformité.

## Bonnes pratiques :

- Générez et analysez ce rapport régulièrement (par exemple, mensuellement).
  - Utilisez les informations pour identifier et corriger les problèmes de sécurité potentiels.
  - Ne partagez jamais ce rapport en dehors de votre organisation, car il contient des informations sensibles.

Documentation AWS EC2 (Elastic Compute Cloud)

## 1. Qu'est-ce que EC2 ?

Amazon Elastic Compute Cloud (EC2) est un service web qui fournit une capacité de calcul redimensionnable dans le cloud. Il est conçu pour faciliter le cloud computing à l'échelle du web pour les développeurs.

#### **Caractéristiques principales :**

- Instances virtuelles dans le cloud
- Contrôle complet sur vos ressources de calcul
- Flexibilité pour s'adapter aux besoins changeants
- Paiement à l'utilisation

## 2. Options de configuration et tailles disponibles

EC2 offre une large gamme d'options de configuration, appelées "types d'instances", optimisées pour différents cas d'utilisation.

### Familles d'instances principales :

- Usage général (ex: t3, m5)
- Calcul optimisé (ex: c5)
- Mémoire optimisée (ex: r5)
- Stockage optimisé (ex: i3, d2)
- Accélérées par GPU (ex: p3, g4)

### Tailles disponibles :

Les tailles varient de nano (t3.nano avec 0.5 GiB de RAM) à metal (comme i3.metal avec jusqu'à 512 GiB de RAM), offrant une grande flexibilité pour différents besoins en ressources.

## 3. EC2 User Data

EC2 User Data est un script qui s'exécute automatiquement lors du lancement d'une instance EC2.

### Utilité :

- Automatiser les tâches de configuration
- Installer des logiciels
- Télécharger des données
- Exécuter des mises à jour

### Fonctionnement :

- Le script est passé à l'instance au moment du lancement
- Il s'exécute avec les priviléges root
- Peut être en bash, PowerShell, ou autres langages de script

## 4. Types d'instances EC2

Les types d'instances varient en combinaisons de CPU, mémoire, stockage et capacité réseau. Voici quelques catégories principales :

1. **Instances à usage général** (série T, M)
  - Équilibre entre ressources
  - Adaptées à diverses charges de travail
2. **Instances optimisées pour le calcul** (série C)
  - Hautes performances CPU
  - Idéales pour les charges de travail intensives en calcul
3. **Instances optimisées pour la mémoire** (série R, X)
  - Grande capacité de mémoire
  - Parfaites pour les bases de données en mémoire
4. **Instances de stockage optimisé** (série I, D)
  - E/S élevées
  - Bonnes pour les bases de données, l'analyse big data
5. **Instances accélérées** (série P, G)
  - Équipées de GPU
  - Idéales pour le machine learning, le rendu graphique

Chaque type d'instance est conçu pour offrir des performances optimales pour des charges de travail spécifiques, permettant aux utilisateurs de choisir la configuration la plus adaptée à leurs besoins.

## Création d'une instance EC2 "Serveur Web Dev"

### Objectif

Créer une instance EC2 pour héberger un serveur web de développement selon des spécifications précises.

Connexion à AWS :

- Allez sur [aws.amazon.com](https://aws.amazon.com) et connectez-vous à votre compte AWS.

Accéder au service EC2 :

- Dans la barre de recherche en haut, tapez "EC2" et sélectionnez le service.

Lancer une nouvelle instance :

The screenshot shows the AWS EC2 console with the 'Launch instance' button highlighted in orange. The interface includes sections for Ressources, Niveau EC2 gratuit, Santé du service, Attributs du compte, and Zones.

- Cliquez sur le bouton orange "Launch instance" (Lancer une instance).

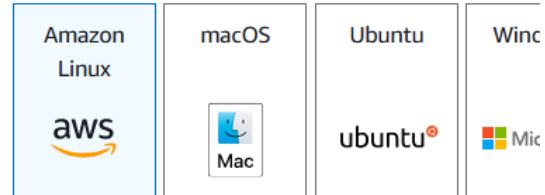
Nommer l'instance :

- Dans le champ "Name", entrez "Serveur Web Dev".

Choisir l'AMI :

- Sous "Application and OS Images", cherchez "Amazon Linux 2023".
- Sélectionnez la version Amazon Linux 2023 AMI.

### Démarrage rapide



### Amazon Machine Image (AMI)

#### AMI Amazon Linux 2023

ami-0fff1b9a61dec8a5f (64 bits (x86), uefi-preferred) / ami-0  
Virtualisation: hvm ENA activé: true Type de périphérique

Sélectionner le type d'instance :

Sous "Instance type", choisissez "t2.micro" (ou la plus petite instance disponible).

### Créer une paire de clés

The dialog box for creating a key pair has the following fields:

- Nom de la paire de clés:** serveur-web-dev-key
- Type de paire de clés:** RSA (selected)
- Format de fichier de clé privée:** .pem (selected)
- Warning:** Lorsque vous y êtes invité, stockez la paire de clés dans un emplacement sécurisé et accessible sur votre ordinateur. Vous en aurez besoin ultérieurement pour vous connecter à votre instance. [En savoir plus](#)

Annulez

Créer une paire de clés

## Créer une paire de clés :

- Sous "Key pair", cliquez sur "Create new key pair".
- Nommez-la "serveur-web-dev-key".
- Téléchargez le fichier .pem et conservez-le en sécurité.

## Configurer le réseau :

- Sous "Network settings", cliquez sur "Edit".
- Assurez-vous que "Auto-assign public IP" est sur "Enable".
- Dans "Firewall (security groups)", sélectionnez "Create security group".
- Ajoutez des règles pour autoriser le trafic HTTP (port 80) et HTTPS (port 443) depuis n'importe où.

▼ Règle de groupe de sécurité 2 (TCP, 80, 0.0.0.0/0)

**Supprimer**

Type   <a href="#">Informations</a>	Protocole   <a href="#">Informations</a>	Plage de ports   <a href="#">Informations</a>
HTTP	TCP	80
Type de source   <a href="#">Informations</a>	Source   <a href="#">Informations</a>	Description - facultatif
Personnalisé	Ajouter une adresse CIDR, une... 0.0.0.0/0	Informations par exemple, SSH pour le bureau de

► Règle de groupe de sécurité 3 (TCP, 443, 0.0.0.0/0)

**Supprimer**

▼ Règle de groupe de sécurité 4 (TCP, 443, 0.0.0.0/0)

**Supprimer**

Type   <a href="#">Informations</a>	Protocole   <a href="#">Informations</a>	Plage de ports   <a href="#">Informations</a>
HTTPS	TCP	443
Type de source   <a href="#">Informations</a>	Source   <a href="#">Informations</a>	Description - facultatif
Personnalisé	Ajouter une adresse CIDR, une... 0.0.0.0/0	Informations par exemple, SSH pour le bureau de

## Configurer le stockage :

⚠️ Les règles avec la  Nous vous recommandons de Sélectionnez à votre instance. autoriser l'accès à

Ajouter une règle de... SSD à usage général (gp3) ✓

Configurer le sto... SSD à usage général (gp2)

SSD IOPS provisionnés (io1)

IOPS provisionnés SSD (io2)

HDD à froid (sc1)

HDD à débit optimisé (st1)

1x 8 Gio gp3 Volume racine (Non chiffré)

Avancé

💡 Les clients éligibles à l'offre gratuite peuvent obtenir jusqu'à 30 Go de stockage EBS à usage général (SSD) ou magnétique.

Ajouter un volume

- Sous "Configure storage", réglez la taille à 8 GB et le type à gp2.

## Configurer le User Data :

- Faites défiler jusqu'à la section "Advanced Details" (Détails avancés).
- Trouvez le champ "User data" (Données utilisateur).
- Assurez-vous que l'option "Text" est sélectionnée (pas "File").
- Copiez-collez le script ci-dessus dans la zone de texte

```
#!/bin/bash
```

```
yum update -y
```

```
yum install -y httpd
```

```
systemctl start httpd
```

```
systemctl enable httpd
```

```
echo "<h1>Hello from Serveur Web Dev</h1>" >  
/var/www/html/index.html
```

Points importants à comprendre :

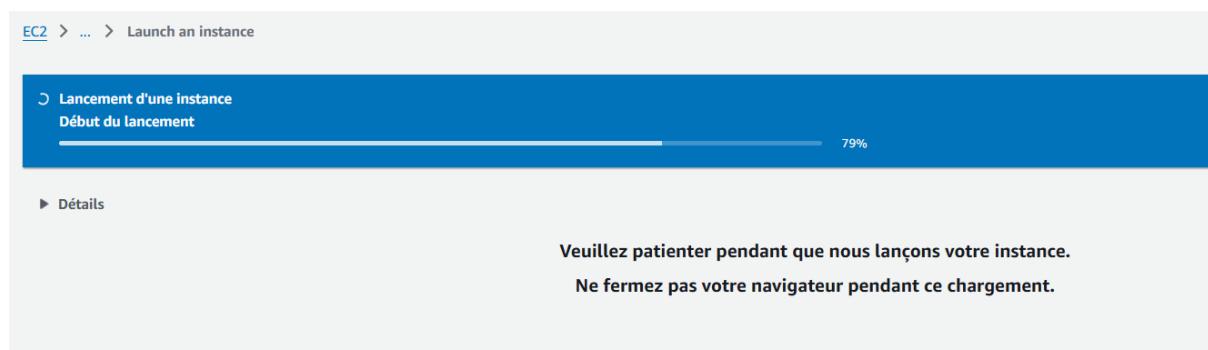
- Ce script s'exécute avec les privilèges root (administrateur) sur l'instance.
- Il ne s'exécute qu'au premier démarrage de l'instance. Si vous redémarrez l'instance, le script ne s'exécutera pas à nouveau.
- Les commandes yum sont spécifiques aux systèmes basés sur Red Hat, comme Amazon Linux.
- httpd est le nom du paquet Apache sur ces systèmes.
- systemctl est utilisé pour gérer les services sur les systèmes modernes utilisant systemd.

Utilité de ce script :

1. Il met à jour le système pour s'assurer que vous avez les dernières versions des logiciels.
2. Il installe un serveur web (Apache) automatiquement.
3. Il configure le serveur web pour qu'il démarre automatiquement à chaque démarrage de l'instance.
4. Il crée une page web simple pour vérifier que tout fonctionne correctement

Lancer l'instance :

- Vérifiez tous les paramètres.
- Cliquez sur "Launch instance".



Attendre le démarrage :

- Retournez à la page des instances EC2.

- Attendez que l'état de votre instance passe à "Running".

**Succès**  
Lancement de l'instance réussi (i-0506ce99225f71a7f)

Journal de lancement

Étapes suivantes

Créer des alertes de facturation et d'utilisation de l'offre gratuite  
Pour gérer les coûts et éviter les factures surprises, configurez des notifications par e-mail pour la facturation et les seuils d'utilisation de l'offre gratuite.  
[Créer des alertes de facturation](#)

Connectez-vous à votre instance  
Une fois que votre instance est en cours d'exécution, connectez-vous à celle-ci à partir de votre ordinateur local.  
[Connectez-vous à l'instance](#)  
[En savoir plus](#)

Connecter une base de données RDS  
Configurez la connexion entre une instance EC2 et une base de données pour autoriser le flux de trafic entre elles.  
[Connecter une base de données RDS](#)  
[Créer une nouvelle base de données RDS](#)  
[En savoir plus](#)

Afficher toutes les instances

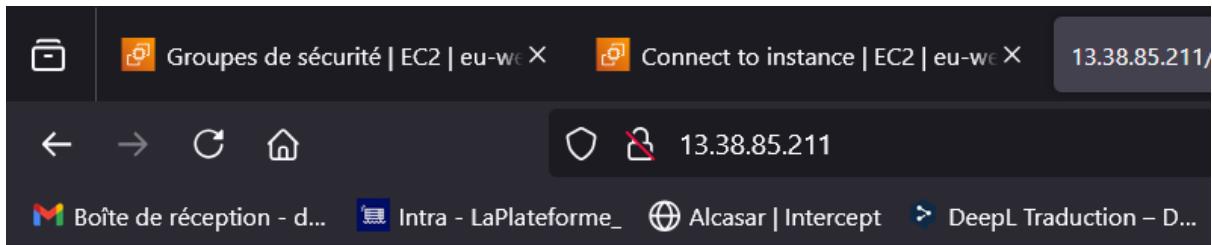
Accéder à votre serveur web :

- Sélectionnez votre instance.
- Copiez l'adresse "Public IPv4 address".
- Ouvrez un nouvel onglet dans votre navigateur et collez cette adresse.

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-33-105 ~]$
```

Vérification :

- Vous devriez voir le message "Hello from Serveur Web Dev".



# Hello from Serveur Web Dev

## Points clés

- L'utilisation d'Amazon Linux 2023 assure un système d'exploitation à jour et optimisé pour AWS.
- Le type d'instance t2.micro est idéal pour le développement et les tests, tout en restant dans la free tier d'AWS.
- Le script User Data permet d'automatiser le déploiement du serveur web, économisant du temps et réduisant les erreurs manuelles.
- L'ouverture des ports 80 et 443 est essentielle pour un serveur web, mais il faut rester vigilant sur la sécurité.

## Améliorations possibles

- Mettre en place un nom de domaine personnalisé
- Configurer HTTPS avec un certificat SSL
- Implémenter des règles de sécurité plus strictes dans le groupe de sécurité
- Utiliser Elastic IP pour une adresse IP statique

## Conclusion

Cette configuration fournit un environnement de base solide pour le développement web, facilement accessible et modifiable selon les besoins futurs du projet.

## Connexion à EC2 via SSH (Secure Shell)

Localiser votre fichier de clé privée (.pem) :

- C'est le fichier que vous avez téléchargé lors de la création de l'instance EC2.

Sécuriser votre fichier de clé (sur Windows) :

- Ouvrez les propriétés du fichier .pem.
- Allez dans l'onglet Sécurité > Avancé.
- Désactivez l'héritage et supprimez toutes les autorisations sauf la vôtre.

Trouver l'adresse IP publique de votre instance :

- Dans la console AWS EC2, sélectionnez votre instance.
- Trouvez et copiez l'adresse "IPv4 publique".

Ouvrir un terminal (PowerShell sur Windows, Terminal sur Mac/Linux).

Naviguer vers le dossier contenant votre fichier .pem :

*cd chemin/vers/votre/dossier*

- Sur Windows (PowerShell) :

*ssh -i "votre-cle.pem" ec2-user@adresse-ip-publique*

Si c'est votre première connexion, vous verrez un avertissement de fingerprint. Tapez "yes" pour continuer. Vous devriez maintenant être connecté à votre instance EC2.

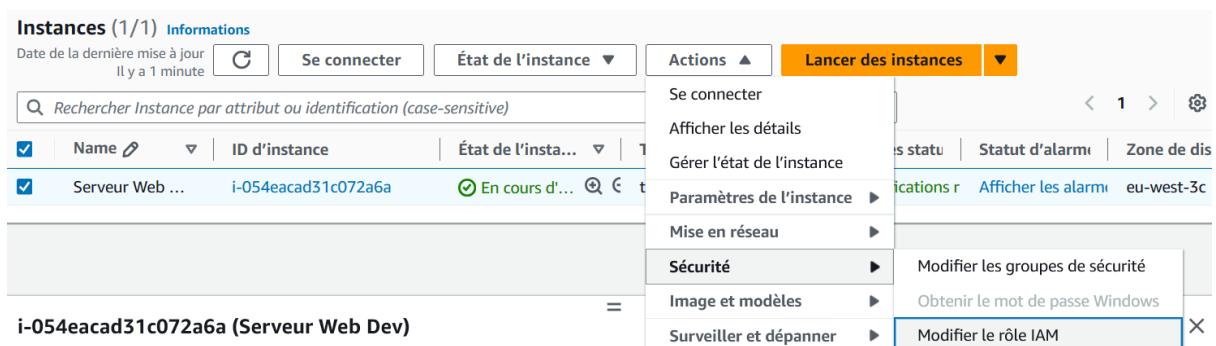
```
Répertoire de C:\Users\Asus-Tuf-Laptop\Desktop\EC2
18/10/2024 12:49 <DIR> .
18/10/2024 10:49 <DIR> ..
18/10/2024 12:48 1 674 serveur-web-dev-key.pem
18/10/2024 12:48 1 597 statut-reports.Thu Oct 10 2024 12_41_52 GMT+0200 (heure d'été d'Europe centrale).csv
2 Fichier(s) 3 271 octets
2 Rép(s) 748 041 027 584 octets libres

C:\Users\Asus-Tuf-Laptop\Desktop\EC2>ssh -i "serveur-web-dev-key.pem" ec2-user@13.38.85.211
The authenticity of host '13.38.85.211 (13.38.85.211)' can't be established.
ED25519 key fingerprint is SHA256:Uh5Eg4BZz9jNHxe2/SrlwnGyjIPyDLNhqNNJYqm1MWo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.38.85.211' (ED25519) to the list of known hosts.

# 
~\_\_ ##### Amazon Linux 2023
~~ \_\#\#\#
~~ \#\#\#
~~ \#/ 
~~ \_\_\_> https://aws.amazon.com/linux/amazon-linux-2023
~~ \_\_\_
~~ \_\_\_/
~~ \_\_\_/
Last login: Thu Oct 10 10:55:55 2024 from 35.180.112.84
[ec2-user@ip-172-31-33-105 ~]$
```

## Attribution du rôle IAM "DemoForEC2" à l'instance EC2

- Allez dans la console AWS et accédez au service EC2.
- Sélectionnez votre instance "Serveur Web Dev".
- Cliquez sur "Actions" > "Sécurité" > "Modifier le rôle IAM".



- Dans la liste déroulante, sélectionnez le rôle "DemoForEC2".

e. Cliquez sur "Enregistrer".

Se connecter à l'instance via SSH : Utilisez la commande SSH

[ssh -i "votre-cle.pem" ec2-user@adresse-ip-publique](#)

```
C:\Users\Asus-Tuf-Laptop\Desktop\EC2>ssh -i "serveur-web-dev-key.pem" ec2-user@13.38.85.21
'_
~\_ ####_          Amazon Linux 2023
~~ \_\#####\
~~ \###]
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~' '-->
~~ . .
~~ /_/
~~ /_/
~/m/'

Last login: Thu Oct 10 10:58:14 2024 from 37.26.187.6
[ec2-user@ip-172-31-33-105 ~]$
```

Vérifier que le rôle fonctionne : Une fois connecté, exécutez la commande suivante :

[aws iam list-users](#)

Interprétation des résultats :

- Si la commande retourne une liste des utilisateurs IAM, cela signifie que le rôle fonctionne correctement.
- Si vous obtenez une erreur, cela peut indiquer un problème avec l'attribution du rôle ou les permissions.

```
~~  \###|
~~  \#/ --- https://aws.amazon.com/linux/amazon-linux-2023
~~  V~' '-->
~~~ /
~~. ./
~/_/
~/m/'  
Last login: Thu Oct 10 10:58:14 2024 from 37.26.187.6
[ec2-user@ip-172-31-33-105 ~]$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "BillGates",
      "UserId": "AIDASBGQLC7PJPU6YOW4R",
      "Arn": "arn:aws:iam::140023371742:user/BillGates",
      "CreateDate": "2024-10-07T14:13:41+00:00"
    },
    {
      "Path": "/",
      "UserName": "ElonMusk",
      "UserId": "AIDASBGQLC7PL57MJ6BZI",
      "Arn": "arn:aws:iam::140023371742:user/ElonMusk",
      "CreateDate": "2024-10-08T19:14:51+00:00"
    },
    {
      "Path": "/",
      "UserName": "JeffBezos",
      "UserId": "AIDASBGQLC7PLY4HTZ20B",
      "Arn": "arn:aws:iam::140023371742:user/JeffBezos",
      "CreateDate": "2024-10-08T19:11:31+00:00"
    },
    {
      "Path": "/",
      "UserName": "MarkZuckerberg",
      "UserId": "AIDASBGQLC7P06GAZUWRL",
      "Arn": "arn:aws:iam::140023371742:user/MarkZuckerberg",
      "CreateDate": "2024-10-07T14:12:24+00:00"
    }
  ]
}
.... skipping...
```

```
"Users": [
    {
        "Path": "/",
        "UserName": "BillGates",
        "UserId": "AIDASBGQLC7PJPU6YOW4R",
        "Arn": "arn:aws:iam::140023371742:user/BillGates",
        "CreateDate": "2024-10-07T14:13:41+00:00"
    },
    {
        "Path": "/",
        "UserName": "ElonMusk",
        "UserId": "AIDASBGQLC7PL57MJ6BZI",
        "Arn": "arn:aws:iam::140023371742:user/ElonMusk",
        "CreateDate": "2024-10-08T19:14:51+00:00"
    },
    {
        "Path": "/",
        "UserName": "JeffBezos",
        "UserId": "AIDASBGQLC7PLY4HTZ20B",
        "Arn": "arn:aws:iam::140023371742:user/JeffBezos",
        "CreateDate": "2024-10-08T19:11:31+00:00"
    },
    {
        "Path": "/",
        "UserName": "MarkZuckerberg",
        "UserId": "AIDASBGQLC7P06GAZUWRL",
        "Arn": "arn:aws:iam::140023371742:user/MarkZuckerberg",
        "CreateDate": "2024-10-07T14:12:24+00:00"
    },
    {
        "Path": "/",
        "UserName": "SteveJobs",
        "UserId": "AIDASBGQLC7PBPGNTSYGB",
        "Arn": "arn:aws:iam::140023371742:user/SteveJobs",
        "CreateDate": "2024-10-07T14:09:37+00:00"
    }
]
...skipping...
{
```

```
"Users": [
    {
        "Path": "/",
        "UserName": "BillGates",
        "UserId": "AIDASBGQLC7PJPU6YOW4R",
        "Arn": "arn:aws:iam::140023371742:user/BillGates",
        "CreateDate": "2024-10-07T14:13:41+00:00"
    },
    {
        "Path": "/",
        "UserName": "ElonMusk",
        "UserId": "AIDASBGQLC7PL57MJ6BZI",
        "Arn": "arn:aws:iam::140023371742:user/ElonMusk",
        "CreateDate": "2024-10-08T19:14:51+00:00"
    },
    {
        "Path": "/",
        "UserName": "JeffBezos",
        "UserId": "AIDASBGQLC7PLY4HTZ20B",
        "Arn": "arn:aws:iam::140023371742:user/JeffBezos",
        "CreateDate": "2024-10-08T19:11:31+00:00"
    },
    {
        "Path": "/",
        "UserName": "MarkZuckerberg",
        "UserId": "AIDASBGQLC7PO6GAZUWRL",
        "Arn": "arn:aws:iam::140023371742:user/MarkZuckerberg",
        "CreateDate": "2024-10-07T14:12:24+00:00"
    },
    {
        "Path": "/",
        "UserName": "SteveJobs",
        "UserId": "AIDASBGQLC7PBPGNTSYGB",
        "Arn": "arn:aws:iam::140023371742:user/SteveJobs",
        "CreateDate": "2024-10-07T14:09:37+00:00"
    }
]
}
~
```

(END)

# Rapport sur les différentes options d'achat EC2 pour optimiser les coûts

## 1. Introduction aux options d'achat EC2

Option	Flexibilité	Coût	Engagement	Cas d'utilisation
<b>On-Demand Instances</b>	Élevée	Le plus élevé	Aucun	Charges de travail imprévisibles, développement/test
<b>Reserved Instances</b>	Faible	Réduction jusqu'à 72%	1 ou 3 ans	Applications stables avec utilisation prévisible
<b>Spot Instances</b>	Très élevée	Le plus bas (jusqu'à 90% de réduction)	Aucun, mais peut être interrompu	Tâches tolérantes aux interruptions, traitement par lots
<b>Savings Plans</b>	Moyenne	Réduction jusqu'à 72%	1 ou 3 ans	Utilisation flexible entre régions et familles d'instances
<b>Dedicated Hosts</b>	Faible	Le plus élevé	Peut être à la demande ou réservé	Conformité, licences logicielles par socket/cœur

## Options d'achat EC2 pour l'optimisation des coûts

### 1. On-Demand Instances

- Paiement à l'utilisation, sans engagement
- Idéal pour : charges de travail à court terme et imprévisibles
- Coût : le plus élevé, mais flexible

### 2. Reserved Instances (RI)

- Engagement sur 1 ou 3 ans
- Types : Standard, Convertible, Scheduled

- Économies : jusqu'à 72% par rapport à On-Demand
- Idéal pour : applications stables avec utilisation prévisible

### **3. Spot Instances**

- Utilise la capacité EC2 inutilisée
- Économies : jusqu'à 90% par rapport à On-Demand
- Risque : peut être interrompu avec un préavis de 2 minutes
- Idéal pour : tâches tolérantes aux interruptions (traitement par lots, analyse de données)

### **4. Savings Plans**

- Engagement sur un montant d'utilisation horaire (1 ou 3 ans)
- Flexible entre types d'instances et régions
- Économies : similaires aux RI
- Idéal pour : utilisation variée d'EC2 et autres services de calcul AWS

### **5. Dedicated Hosts**

- Serveurs physiques dédiés
- Utile pour : exigences de conformité, licences logicielles spécifiques
- Coût : le plus élevé, mais offre un contrôle total

### **Stratégies d'optimisation**

1. Combinez différentes options pour équilibrer coûts et flexibilité
2. Utilisez AWS Cost Explorer pour analyser l'utilisation et les dépenses
3. Profitez d'AWS Trusted Advisor pour des recommandations d'optimisation

## 4. Surveillez et ajustez régulièrement votre stratégie d'achat

### Conclusion

Le choix de la bonne option d'achat EC2 peut considérablement réduire les coûts. La clé est de comprendre vos besoins en charge de travail et d'aligner votre stratégie d'achat en conséquence.

### Création d'un snapshot du volume attaché à l'instance "Serveur Web Dev"

- a. Allez dans la console AWS EC2.
- b. Dans le panneau de navigation, cliquez sur "Volumes" sous "Elastic Block Store".
- c. Trouvez le volume attaché à votre instance "Serveur Web Dev".
- d. Sélectionnez ce volume.
- e. Dans le menu "Actions", choisissez "Create snapshot".

The screenshot shows the AWS EC2 Volumes page. A context menu is open over a selected volume named 'vol-0f26fa32f3bd1ad8e'. The menu options include: Modifier le volume, Créer un instantané (highlighted), Créer une stratégie de cycle de vie d'instantané, Supprimer le volume, Attacher un volume, Détacher un volume, Forcer le détachement de volume, Gérer les E/S activées automatiquement, Gérer les balises, and Injection de perturbations. The main table displays one volume entry:

Name	ID du volume	Type	Taille
-	vol-0f26fa32f3bd1ad8e	gp2	8 GiB

Detailed view for the selected volume:

ID du volume	Contrôles des statuts	Surveillance	Balises	Statut du volume
vol-0f26fa32f3bd1ad8e	Taille 8 GiB	Type gp2	OK	

- f. Donnez un nom descriptif au snapshot, par exemple "Snapshot-Serveur-Web-Dev".

- g. Ajoutez une description si nécessaire.

- h. Cliquez sur "Create snapshot".

The screenshot shows the 'Create snapshot' dialog box. It has three tabs: Description, Chiffrement, and Balises.

**Description** tab:

Ajouter une description pour votre instantané  
Snapshot-Serveur-Web-Dev  
255 caractères maximum.

**Chiffrement** tab:

Non chiffré

**Balises** tab:

Une balise est une étiquette que vous attribuez à une ressource AWS. Chaque balise se compose d'une clé et d'une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources ou suivre vos coûts AWS.  
Aucune balise n'est associée à cette ressource.  
Ajouter une balise  
Vous pouvez ajouter 50 balises supplémentaires.

Buttons at the bottom: Annuler and Crée un instantané.

## Arrêt de l'instance :

- Retournez à la liste des instances EC2.
- Sélectionnez votre instance "Serveur Web Dev".
- Dans le menu "Instance state", choisissez "Stop instance".

The screenshot shows the AWS EC2 Instances page. A success message at the top says "DemoForEC2 attaché à l'instance i-054eacad31c072a6a avec succès". The main area displays "Instances (1/1) Informations" for the instance "i-054eacad31c072a6a (Serveur Web Dev)". On the right, there's a "Actions" dropdown menu with options: "Arrêter l'instance" (which is highlighted), "Démarrer l'instance", "Redémarrer une instance", "Mettre l'instance en veille prolongée", and "Résilier (éliminer) l'instance". Below the instance list, the instance details are shown again with the name "Serveur Web ..." and ID "i-054eacad31c072a6a".

- Confirmez l'action.

The screenshot shows the "Arrêter l'instance" (Stop instance) dialog. It contains the following fields:

- ID d'instance: i-054eacad31c072a6a (Serveur Web Dev)
- Protection contre l'arrêt: Désactivé (Possible d'arrêter l'instance) (checkbox checked)

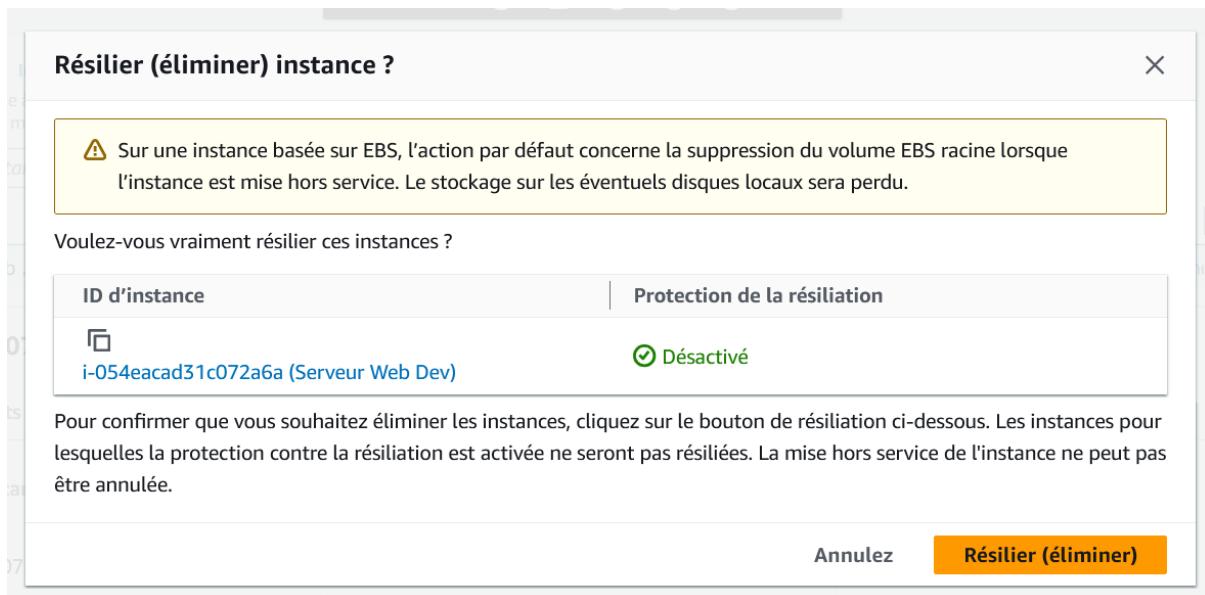
A warning message in a yellow box states: "Les ressources associées vous seront facturées. Une fois l'instance arrêtée, les frais d'utilisation ou de transfert de données ne vous sont plus facturés. Toutefois, les volumes EBS attachés et les adresses IP Elastic associées vous seront toujours facturés." Below this, a section titled "Ressources associées" notes that associated resources will continue to incur costs during the stop instance process. At the bottom are "Annulez" and "Stop (Arrêter)" buttons.

## Résiliation de l'instance :

- Une fois l'instance arrêtée, sélectionnez-la à nouveau.

The screenshot shows the AWS EC2 Instances page again. The instance "i-054eacad31c072a6a (Serveur Web Dev)" is selected. The "Actions" dropdown menu is open, and the "Lancer des instances" (Launch instances) button is highlighted with a yellow border. Other options in the menu include "Forcer l'arrêt de l'instance", "Démarrer l'instance", "Redémarrer une instance", "Mettre l'instance en veille prolongée", and "Résilier (éliminer) l'instance".

b. Dans le menu "Instance state", choisissez "Terminate instance".



c. Lisez attentivement l'avertissement et confirmez la résiliation.

#### Important :

- Les snapshots permettent de sauvegarder les données
- La résiliation est irréversible et supprime les données
- Les snapshots sont facturés (stockage S3)
- Vérifiez toujours les dépendances avant la résiliation

### JOUR 2 AWS - EC2 avancé +

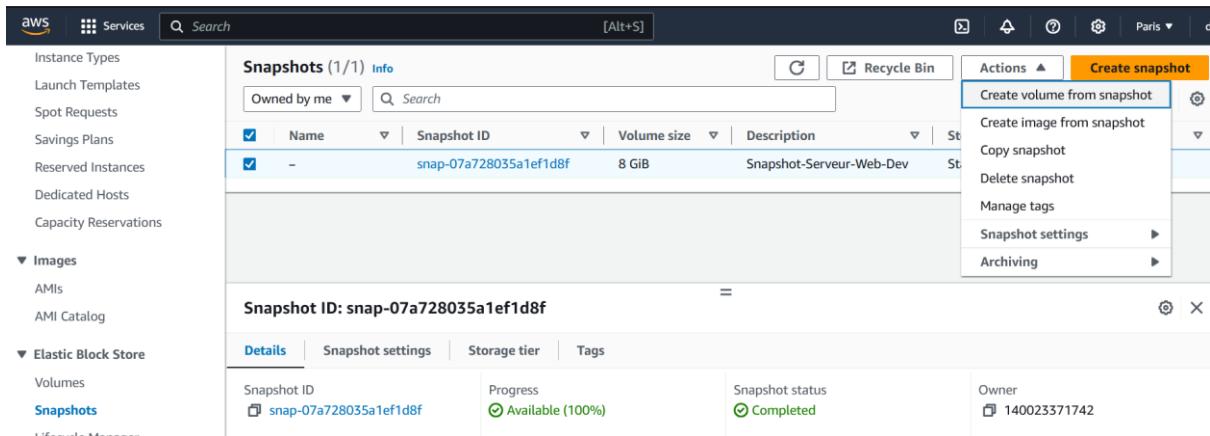
#### Lancer une instance EC2 à partir du snapshot

Accéder à la console AWS

- Connectez-vous à votre compte AWS et accédez à la console EC2.

Localiser le snapshot

- Dans le menu de gauche, cliquez sur "Snapshots" sous la section "Elastic Block Store".
- Trouvez le snapshot que vous avez créé lors du Job 13 du jour 1. Il devrait avoir le nom que vous lui avez donné, par exemple "Snapshot-Serveur-Web-Dev".



## Créer un volume à partir du snapshot

- Sélectionnez le snapshot.
- Cliquez sur "Actions" puis "Create volume from snapshot".
- Choisissez le type de volume (généralement gp2 pour un usage général).
- Sélectionnez la zone de disponibilité où vous voulez créer l'instance.
- Cliquez sur "Create volume".

## Lancer une nouvelle instance

- Allez dans "Instances" dans le menu de gauche.
- Cliquez sur "Launch instances".
- Choisissez une AMI Amazon Linux 2023 (comme dans le jour 1).
- Sélectionnez le type d'instance (t2.micro si vous êtes toujours dans la free tier).

## Configurer l'instance

- Dans la section "Configure Instance", gardez les paramètres par défaut.
- Dans "Add Storage", supprimez le volume root par défaut.
- Cliquez sur "Add New Volume" et sélectionnez le volume que vous venez de créer à partir du snapshot.

## Configurer les groupes de sécurité

- Choisissez une paire de clés existante ou créez-en une nouvelle
- Vous pouvez soit créer un nouveau groupe de sécurité, soit utiliser celui que vous aviez configuré dans le jour 1.
- Assurez-vous que les ports 80 (HTTP) et 443 (HTTPS) sont ouverts.

## Lancer l'instance

- Vérifiez tous les détails sur la page de revue.
- Cliquez sur "Launch".

The screenshot shows a green success banner at the top with the text "Succès" and "Lancement de l'instance réussi (i-0a8ba75741616cf1a)". Below the banner, there is a link "▶ Journal de lancement". Underneath, a section titled "Étapes suivantes" is visible.

## Vérifier l'instance

- Retournez à la liste des instances et attendez que votre nouvelle instance soit dans l'état "running".
- Vérifiez que le volume créé à partir du snapshot est bien attaché à l'instance.

## Tester l'instance

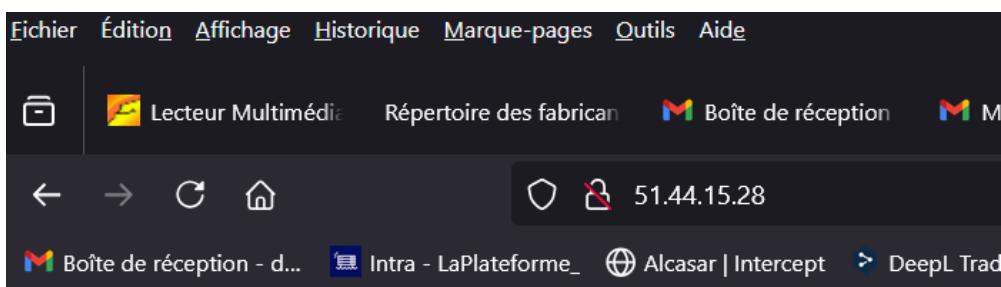
- Une fois l'instance en état "running", copiez son adresse IP publique.

The screenshot shows the "Résumé de l'instance pour i-0a8ba75741616cf1a" page. It includes tabs for "Informations", "Se connecter", "État de l'instance", and "Actions". The "État de l'instance" tab is selected, showing the instance is "En cours d'exécution". The "Actions" tab is also visible.

ID d'instance	Adresse IPv4 publique	Adresses IPv4 privées
<a href="#">i-0a8ba75741616cf1a</a>	<a href="#">51.44.15.28   adresse ouverte</a>	<a href="#">172.31.38.137</a>
Adresse IPv6	État de l'instance	DNS IPv4 public
-	<a href="#">En cours d'exécution</a>	<a href="#">ec2-51-44-15-28.eu-west-3.compute.amazonaws.com</a>
Type de nom d'hôte	Nom DNS de l'IP privé (IPv4 uniquement)	<a href="#">adresse ouverte</a>
Nom de l'adresse IP: ip-172-31-38-137.eu-west-3.compute.internal	<a href="#">ip-172-31-38-137.eu-west-3.compute.internal</a>	

- Ouvrez un navigateur et entrez cette adresse IP pour vérifier si le serveur web est opérationnel.

Si vous n'arrivez pas à accéder à la page d'accueil du serveur web après avoir lancé votre instance à partir du snapshot, voici quelques étapes de dépannage à suivre :



## It works!

Vérifiez l'état de l'instance :

- Assurez-vous que l'instance est en état "running" dans la console EC2.

Vérifiez le groupe de sécurité :

- Confirmez que les ports 80 (HTTP) et 443 (HTTPS) sont ouverts pour le trafic entrant.
- Vérifiez que la source est configurée sur 0.0.0.0/0 pour permettre l'accès depuis n'importe où.

Vérifiez l'adresse IP publique :

- Assurez-vous d'utiliser l'adresse IP publique correcte de l'instance.
- L'adresse IP peut changer si vous arrêtez et redémarrez l'instance.

Testez la connectivité :

- Essayez de ping l'adresse IP de l'instance pour vérifier la connectivité réseau.

Vérifiez le service web :

- Connectez-vous à l'instance via SSH.
- Vérifiez si le service Apache est en cours d'exécution :

`sudo systemctl status httpd`

- Si le service n'est pas en cours d'exécution, démarrez-le :

`sudo systemctl start httpd`

Si le serveur web Apache (httpd) n'est pas installé

Tout d'abord, mettez à jour votre système :

`sudo yum update -y`

Installez Apache :

`sudo yum install httpd -y`

Démarrez le service Apache :

`sudo systemctl start httpd`

Activez Apache pour qu'il démarre automatiquement au redémarrage :

`sudo systemctl enable httpd`

Vérifiez l'état du service :

`sudo systemctl status httpd`

Créez une page web simple (si besoin) :

`echo "<html><body><h1>Mon serveur web fonctionne!</h1></body></html>" | sudo tee /var/www/html/index.html`

Vérifiez que le pare-feu autorise le trafic HTTP :

`sudo yum install -y iptables-services`

`sudo iptables -L`

Si nécessaire, ajoutez une règle pour autoriser le trafic HTTP :

`sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

`sudo service iptables save`

Vérifiez que vous pouvez accéder au serveur web localement :

`curl http://localhost`

Après avoir suivi ces étapes, essayez à nouveau d'accéder à la page web en utilisant l'adresse IP publique de votre instance dans un navigateur.

## Types d'adresses IP pour instances EC2

### 1. Adresse IP privée

- Attribuée automatiquement à chaque instance dans un VPC

- Non accessible depuis Internet
- Utilisée pour la communication interne au sein du VPC
- Format : généralement dans la plage 10.0.0.0/8, 172.16.0.0/12, ou 192.168.0.0/16

## **2. Adresse IP publique**

- Attribuée dynamiquement lors du lancement de l'instance (si configuré)
- Change si l'instance est arrêtée puis redémarrée
- Accessible depuis Internet
- Gratuite, mais non persistante

## **3. Elastic IP**

- Adresse IPv4 publique statique
- Peut être associée et dissociée des instances à volonté
- Reste attribuée à votre compte AWS jusqu'à ce que vous la libérerez
- Payante si non utilisée ou associée à une instance arrêtée

## **4. Adresse IP du VPC secondaire**

- Adresse IP privée supplémentaire dans le même sous-réseau
- Utile pour héberger plusieurs sites web sur une seule instance
- Peut être ajoutée ou supprimée dynamiquement

## **5. IPv6**

- Peut être attribuée à une instance si le VPC est configuré pour IPv6
- Toujours publiquement routable
- Ne remplace pas l'adresse IPv4, fonctionne en dual-stack

## 6. NAT Gateway IP

- Pas directement attachée à l'instance, mais utilisée pour accéder à Internet depuis des instances privées
- Gérée par AWS, hautement disponible dans la zone de disponibilité

Note : Les instances EC2 dans un VPC ont toujours une adresse IP privée primaire. Les autres types sont optionnels ou dépendent de la configuration.

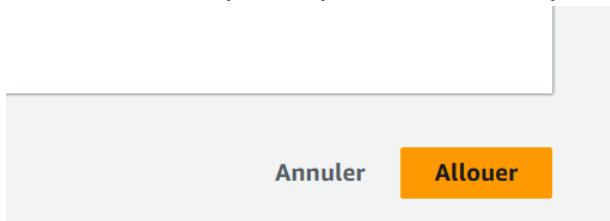
## Génération d'une Elastic IP

**Générer une Elastic IP et son attachement à votre instance EC2** (gratuit quand asso à une instance en cours d'exécution, payant si non utilisé):

- Dans la console AWS EC2, allez dans le menu de gauche et cliquez sur "Elastic IPs" sous la section "Network & Security".
- Cliquez sur "Allocate Elastic IP address".

The screenshot shows the AWS EC2 management console. The left sidebar has a tree structure with 'Services' selected at the top. Under 'Network & Security', 'Adresses IP élastiques' is selected. The main content area is titled 'Adresses IP Elastic'. At the top right, there is a large orange button labeled 'Allouer l'adresse IP Elastic'. Below the button, there is a search bar and some filter options. A message at the bottom of the table area says 'Aucune adresse IP Elastic trouvée dans cette région' (No Elastic IP addresses found in this region). A tooltip at the bottom left of the table area provides information about releasing unused IP addresses.

c. Laissez les options par défaut et cliquez sur "Allocate".



d. Notez l'Elastic IP qui vient d'être créée.

Name	Adresse IPv4 allouée	Type	ID d'allocation
-	<a href="#">15.237.97.40</a>	Adresse IP publique	eipalloc-07897958f021be2cc

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

a. Sélectionnez l'Elastic IP que vous venez de créer.

b. Cliquez sur "Actions" puis "Associate Elastic IP address".

Adresse IP Elastic allouée avec succès.  
Adresse IP Elastic 15.237.97.40

Adresses IP Elastic (1/1)

Actions ▲ Allouer l'adres

Afficher les détails  
Libérer les adresses IP Elastic  
**Associer l'adresse IP Elastic**  
Dissocier l'adresse IP Elastic  
Mettre à jour le DNS inverse  
Activer les transferts  
Désactiver les transferts  
Accepter les transferts

c. Dans "Resource type", sélectionnez "Instance".

d. Choisissez votre instance "Serveur Web Dev" dans la liste déroulante.

e. Cliquez sur "Associate".

**Associer l'adresse IP Elastic**

Choisissez l'instance ou l'interface réseau à associer à cette adresse IP Elastic (15.237.97.40)

**Adresse IP Elastic: 15.237.97.40**

Type de ressource  
Choisissez le type de ressource auquel l'adresse IP Elastic doit être associée.

instance  
 Interface réseau

**⚠ Si vous associez une adresse IP Elastic à une instance qui possède déjà une adresse IP Elastic associée, l'adresse IP Elastic associée précédemment sera dissociée, mais l'adresse sera toujours allouée à votre compte.**  
[En savoir plus](#)

Si aucune adresse IP privée n'est spécifiée, l'adresse IP Elastic sera associée à l'adresse IP privée principale.

instance

Adresse IP privée  
L'adresse IP privée à laquelle associer l'adresse IP Elastic.

Réassocation  
Spécifiez si l'adresse IP Elastic peut être réassociée à une autre ressource si elle est déjà associée à une ressource.  
 Autoriser la réassociation de cette adresse IP Elastic

Annuler **Associer**

## Vérifier l'association :

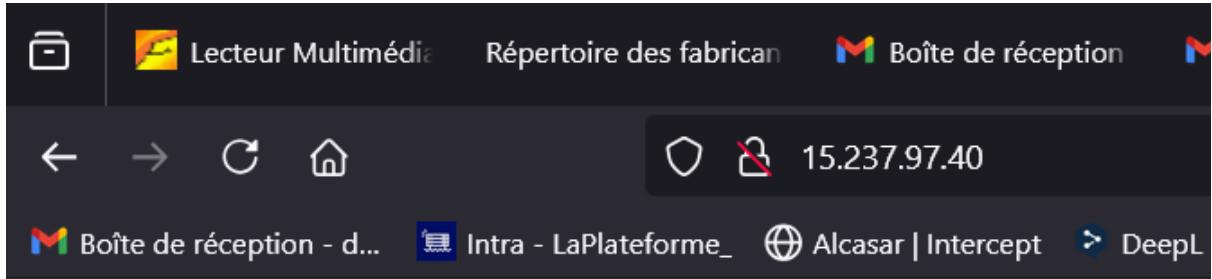
a. Retournez à la liste des instances EC2.

b. Vérifiez que l'adresse IP publique de votre instance a changé pour correspondre à l'Elastic IP.

Instances (1/1) Informations										
Instances (1/1) Informations										
Instances (1/1) Informations										
Date de la dernière mise à jour	Il y a less than a minute	<input type="button" value="Cependant"/>	<input type="button" value="Se connecter"/>	<input type="button" value="État de l'instance"/>	<input type="button" value="Actions"/>	<input type="button" value="Lancer des instances"/>				
Rechercher Instance par attribut ou identification (case-sensitive)	Tous les états									
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> ID d'instance	<input type="checkbox"/> État de l'instance	<input type="checkbox"/> Type d'insta...	<input type="checkbox"/> Contrôle des statu...	<input type="checkbox"/> Statut d'alarme	<input type="checkbox"/> Zone de dispon...	<input type="checkbox"/> DNS IPv4 public	<input type="checkbox"/> Adresse IPv4...	<input type="checkbox"/> IP élastique	
<input checked="" type="checkbox"/> i-0a8ba75741616cf1a	<input type="checkbox"/> En cours d'exécution	<input type="checkbox"/> t2.micro	<input type="checkbox"/> 2/2 vérifications	<input type="checkbox"/> Afficher les alarmes	<input type="checkbox"/> eu-west-3c	<input type="checkbox"/> ec2-15-237-97-40.eu-w...	<input type="checkbox"/> 15.237.97.40			

## Tester l'accès :

- a. Essayez d'accéder à votre serveur web en utilisant la nouvelle Elastic IP dans votre navigateur.



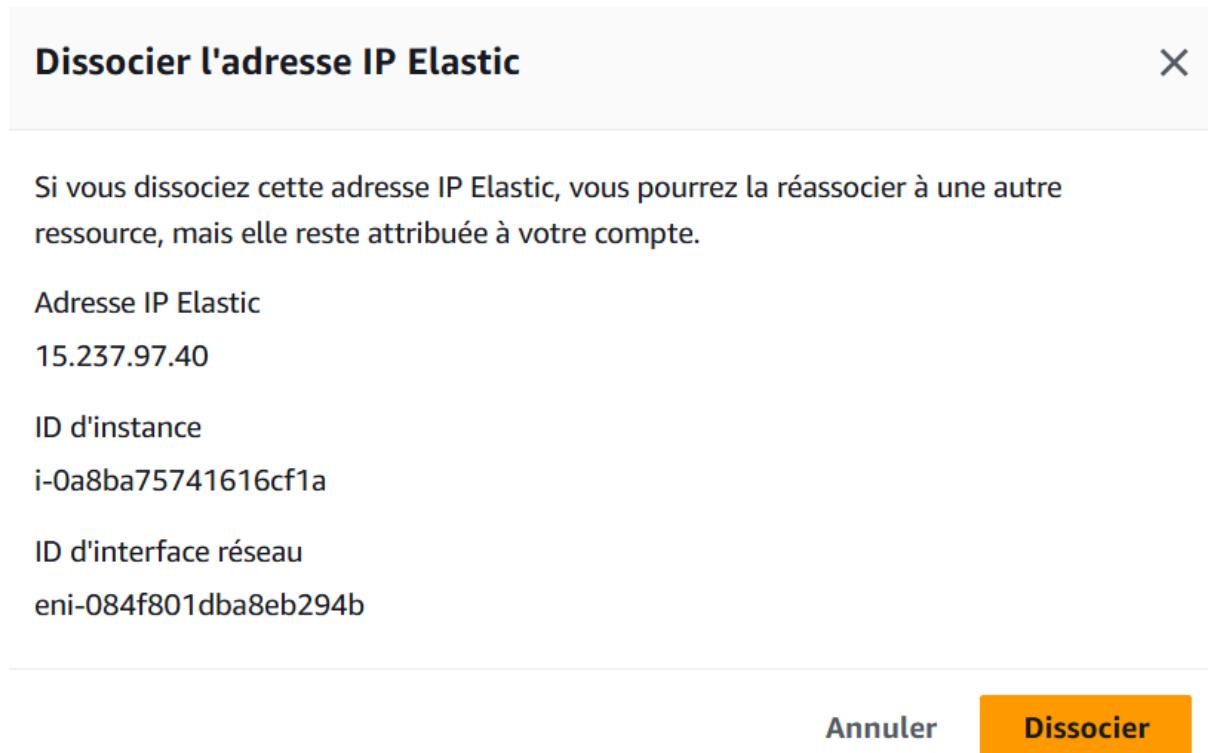
# It works!

## Résilier l'Elastic IP (une fois les tests terminés) :

- Retournez à la section "Elastic IPs".
- Sélectionnez votre Elastic IP.
- Cliquez sur "Actions" puis "Disassociate Elastic IP address".

A screenshot of the AWS Management Console, specifically the Elastic IP section. A green banner at the top indicates that an association was successful: "Adress IP Elastic associée avec succès. Adress IP Elastic 15.237.97.40 associée à instance i-0a8ba75741616cf1a". Below this, a table lists the assigned IP address. The table has columns for 'Name' (with a checked checkbox), 'Adresse IPv4 allouée' (containing '15.237.97.40'), and 'Type' (containing 'Adresse IP publique'). On the right side of the table, there is an 'Actions' dropdown menu. The 'Dissocier l'adresse IP Elastic' option is highlighted with a blue border. Other options in the menu include 'Afficher les détails', 'Libérer les adresses IP Elastic', 'Associer l'adresse IP Elastic', 'Mettre à jour le DNS inverse', 'Activer les transferts', and 'Désactiver les transferts'.

d. Confirmez la dissociation.



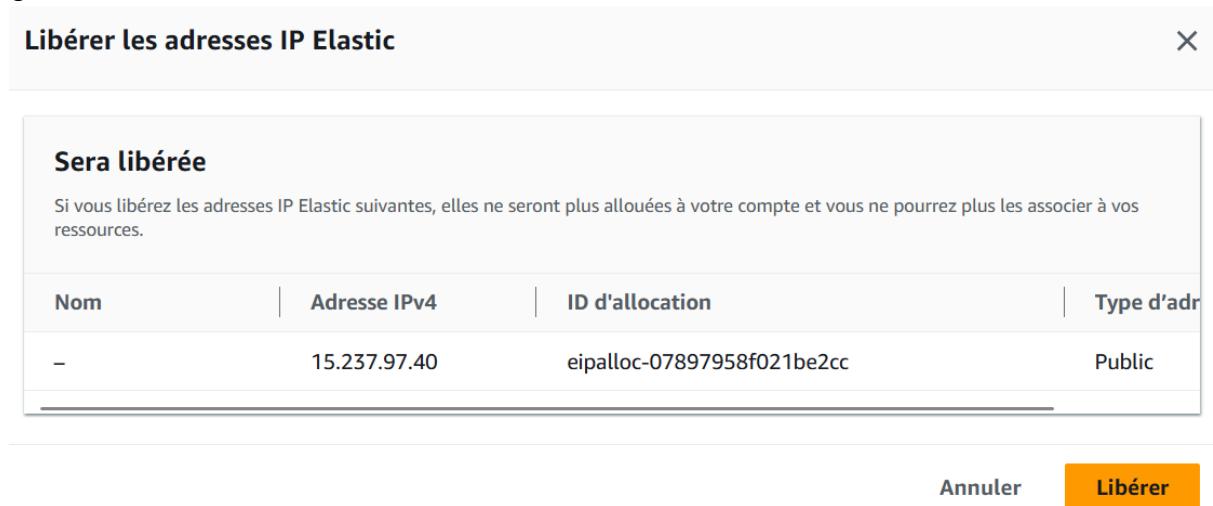
e. Une fois dissociée, sélectionnez à nouveau l'Elastic IP.

f. Cliquez sur "Actions" puis "Release Elastic IP address".

The screenshot shows the AWS Elastic IP Addresses page with the following details:

- Success message: "✓ Adresse IP Elastic dissociée avec succès.  
Adresse IP Elastic 15.237.97.40"
- Table header: "Adresses IP Elastic (1/1)"
- Table columns: "Name", "Adresse IPv4 allouée", and "Type".
- Table data: A single row with Name checked, Address "15.237.97.40", and Type "Adresse IP publique".
- Actions menu (dropdown):
  - Afficher les détails
  - Libérer les adresses IP Elastic
  - Associer l'adresse IP Elastic
  - Dissocier l'adresse IP Elastic
  - Mettre à jour le DNS inverse

g. Confirmez la libération



## Elastic Network Interfaces (ENI).

### Partie 1 : Recherche sur les ENI

Une Elastic Network Interface (ENI) est un composant réseau virtuel dans Amazon VPC qui représente une carte réseau virtuelle.

#### 1. Définition :

- Une ENI est une interface réseau virtuelle que vous pouvez attacher à une instance dans un VPC.

#### 2. Caractéristiques principales :

- Peut avoir une ou plusieurs adresses IP privées
- Peut avoir une adresse IP publique
- Peut avoir une ou plusieurs adresses IP Elastic
- Peut avoir une ou plusieurs adresses IPv6
- Peut avoir des groupes de sécurité associés
- Peut avoir une adresse MAC

#### 3. Utilisations courantes :

- Créer un réseau de gestion
- Utiliser des appliances réseau et de sécurité dans votre VPC

- Créer des instances à double hébergement avec des charges de travail/rôles sur des sous-réseaux distincts
- Créer une configuration réseau à faible budget et haute disponibilité

## Partie 2 : Crédation et attachement d'une ENI

Suivez ces étapes pour créer une ENI et l'attacher à votre instance :

### 1. Crédier une ENI :

- Dans la console EC2, allez dans "Network Interfaces" sous "Network & Security".
- Cliquez sur "Create Network Interface".

Name	ID d'interface réseau	ID de sous-réseau	ID de VPC	Zone de disponibilité
eni-084f801dba8eb294b	subnet-0c2fe928f2cdcb8dc	vpc-005ebf27fb2bad676	eu-west-3c	

- Choisissez un sous-réseau (le même que votre instance).

- Attribuez une adresse IP privée ou laissez AWS en attribuer une automatiquement.

### Créer une interface réseau

Une interface réseau Elastic est un composant de mise en réseau logique dans un VPC qui représente une carte réseau virtuelle.

**Détails** [Informations](#)

Description - facultatif  
Nom descriptif de l'interface réseau.

**Sous-réseau**  
Sous-réseau dans lequel créer l'interface réseau.  
 [X](#) [C](#)

**Adresse IPv4 privée**  
Adresse IPv4 privée à attribuer à l'interface réseau.  
 Attribution automatique  
 Personnalisé

**Elastic Fabric Adapter**  
 Activer

[▶ Paramètres avancés](#)

- e. Sélectionnez le groupe de sécurité approprié.
- f. Ajoutez une description (par exemple, "ENI-Test").
- g. Cliquez sur "Create".

**Groupes de sécurité (1/3) Informations**

ID du groupe	Nom d...	Description
<input checked="" type="checkbox"/> sg-051410c9abecbe7f0	launch-wi...	launch-wizard-1 created 2024-10-10T10:52:14.834Z
<input type="checkbox"/> sg-01b444e67ab7dc4f3	default	default VPC security group
<input type="checkbox"/> sg-02346679a8308ef8	launch-wi...	launch-wizard-2 created 2024-10-10T13:21:57.812Z

**Tags - facultatif**  
Une identification est un label que vous attribuez à une ressource AWS. Chaque identification est constituée d'une clé et d'une valeur facultative. Vous pouvez utiliser des identifications pour rechercher et filtrer vos ressources ou suivre vos coûts AWS.

Aucune balise n'est associée à cette ressource.

**Ajouter une balise**  
Vous pouvez ajouter d'autres balises 50.

**Annuler** **Créer une interface réseau**

## 2. Attacher l'ENI à votre instance :

- a. Sélectionnez la nouvelle ENI.
- b. Cliquez sur "Actions" puis "Attach".

**Interface réseau créée avec succès eni-0df8be7a3bd31b39d**

**Interfaces réseau (1/2) Informations**

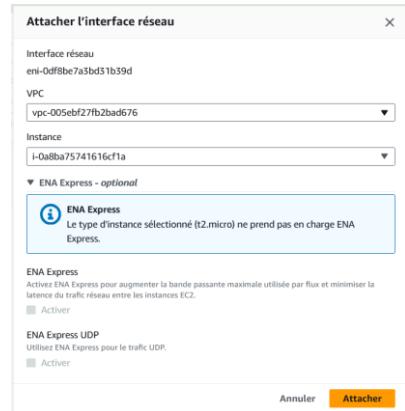
Name	ID d'interface réseau	ID de sous-réseau	ID de VPC
<input type="checkbox"/> eni-084f801dba8eb294b	subnet-0c2fe928f2cdcb8dc	vpc-005ebf27f	
<input checked="" type="checkbox"/> eni-0df8be7a3bd31b39d	subnet-0c2fe928f2cdcb8dc	vpc-005ebf27f	

**Actions**

- Attacher
- Détacher
- Supprimer
- Gérer les adresses IP
- Associer l'adresse
- Dissocier l'adresse
- Modifier le comportement de résiliation

c. Choisissez votre instance EC2.

d. Cliquez sur "Attach".



### 3. Vérification :

a. Allez dans les détails de votre instance EC2.

b. Vérifiez sous "Network interfaces" que la nouvelle ENI est bien attachée.

The screenshot shows the AWS EC2 Instances details page for instance i-0a8ba75741616cf1a. The 'Résumé de l'instance' section displays basic information such as the instance ID (i-0a8ba75741616cf1a), public IP (52.47.184.94), private IP (172.31.38.137), instance type (t2.micro), and state (En cours d'exécution). The 'Network interfaces' section is partially visible at the bottom of the page.

## Les groupes de placement dans AWS EC2.

### Qu'est-ce qu'un groupe de placement ?

Un groupe de placement est une stratégie de placement des instances EC2 dans l'infrastructure sous-jacente d'AWS. Il influence la façon dont les instances sont placées sur le matériel physique, affectant ainsi les performances et la résilience.

### À quoi servent les groupes de placement ?

Les groupes de placement sont utilisés pour :

- Optimiser les performances réseau entre les instances
- Améliorer la tolérance aux pannes

- Exploiter les capacités matérielles spécifiques

## Types de groupes de placement

Il existe trois types de groupes de placement :

Type	Caractéristiques	Cas d'utilisation
Cluster	<ul style="list-style-type: none"> <li>- Instances groupées étroitement dans une seule zone de disponibilité</li> <li>- Latence inter-instance très faible</li> <li>- Débit réseau élevé</li> </ul>	<ul style="list-style-type: none"> <li>- Applications HPC</li> <li>- Big Data avec besoin de performances élevées</li> </ul>
Spread	<ul style="list-style-type: none"> <li>- Instances placées sur du matériel distinct</li> <li>- Répartition sur plusieurs zones de disponibilité possible</li> <li>- Nombre limité d'instances par groupe</li> </ul>	<ul style="list-style-type: none"> <li>- Applications nécessitant une haute disponibilité</li> <li>- Réduction des risques de défaillances simultanées</li> </ul>
Partition	<ul style="list-style-type: none"> <li>- Instances réparties en partitions logiques</li> <li>- Chaque partition sur du matériel distinct</li> <li>- Permet un plus grand nombre d'instances que Spread</li> </ul>	<ul style="list-style-type: none"> <li>- Applications distribuées à grande échelle</li> <li>- Systèmes de fichiers distribués</li> </ul>

## Caractéristiques supplémentaires :

a. Groupe de placement Cluster :

- Offre la latence la plus faible et le débit réseau le plus élevé
- Toutes les instances partagent le même rack
- Risque de panne simultanée plus élevé

b. Groupe de placement Spread :

- Maximum de 7 instances en cours d'exécution par groupe de placement par zone de disponibilité
- Chaque instance s'exécute sur du matériel distinct
- Idéal pour les applications qui ont besoin de maximiser la haute disponibilité

c. Groupe de placement Partition :

- Peut s'étendre sur plusieurs zones de disponibilité dans une région

- Jusqu'à 7 partitions par zone de disponibilité
- Les instances d'une partition ne partagent pas le matériel avec les instances d'autres partitions

## **Considérations importantes :**

- Certains types d'instances peuvent ne pas être pris en charge dans tous les types de groupes de placement
- Il est préférable de lancer toutes les instances d'un groupe de placement en une seule fois
- Vous ne pouvez pas fusionner des groupes de placement
- Une instance ne peut être lancée dans un groupe de placement que lors de sa création

## **Hibernation d'une instance EC2**

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

L'hibernation d'une instance EC2 est un état dans lequel :

- Le système d'exploitation de l'instance est mis en pause.
- Le contenu de la mémoire RAM est persisté sur le volume EBS root.
- L'instance est arrêtée, mais pas terminée.
- Lors du redémarrage, l'état de la RAM est restauré, permettant à l'instance de reprendre là où elle s'était arrêtée.

### **Mise en place de l'hibernation :**

Voici les étapes pour configurer et tester l'hibernation :

#### a. Vérifiez que votre instance est éligible à l'hibernation :

- Elle doit utiliser une AMI compatible (Amazon Linux 2, Ubuntu, Windows, etc.)
- Le type d'instance doit supporter l'hibernation
- Le volume root doit être un volume EBS chiffré et suffisamment grand pour stocker la RAM

#### b. Activez l'hibernation pour votre instance :

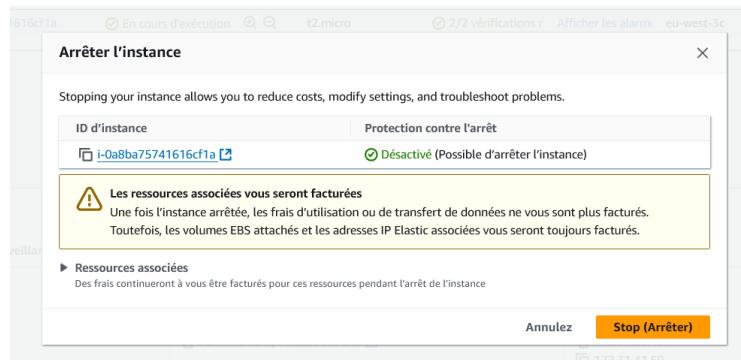
- Arrêtez l'instance si elle est en cours d'exécution

Instances (1/1) Informations Date de la dernière mise à jour Il y a 2 minutes Se connecter État de l'instance Actions Lancer des instances

Rechercher Instance par attribut ou identification (case-sensitive) Tous les états

Name ID d'instance État de l'instance Type d'insta... Contrôle des stat...  
i-0a8ba75741616cf1a En cours d'exécution t2.micro 2/2 vérifications

Arrêter l'instance Démarrer l'instance Redémarrer une instance Mettre l'instance en veille prolongée Résilier (éliminer) l'instance ec2-52-47-184-94.eu-w...



- Sélectionnez l'instance, cliquez sur "Actions" > "Instance Settings" > "Enable hibernation"
- Redémarrez l'instance

c. Testez l'hibernation :

- Connectez-vous à l'instance et créez un fichier test ou modifiez un fichier existant
- Dans la console EC2, sélectionnez l'instance
- Cliquez sur "Actions" > "Instance State" > "Hibernate"

d. Vérifiez l'état de l'instance :

- L'état devrait passer à "Stopping" puis "Stopped"

e. Redémarrez l'instance :

- Sélectionnez l'instance et choisissez "Start"

f. Vérifiez le comportement après le redémarrage :

- Reconnectez-vous à l'instance
- Vérifiez si vos modifications sont toujours présentes
- Vérifiez les logs système pour voir les messages liés à l'hibernation et au réveil

## **Les types de stockage EBS (Elastic Block Store) et EFS (Elastic File System) dans AWS.**

### **Présentation d'EBS (Elastic Block Store) :**

EBS fournit des volumes de stockage en bloc persistants pour une utilisation avec les instances EC2.

Caractéristiques d'EBS :

- Stockage persistant au niveau du bloc
- Peut être attaché à une seule instance EC2 à la fois (dans la plupart des cas)
- Hautement disponible et durable dans une seule zone de disponibilité
- Différents types de volumes optimisés pour différentes charges de travail

### **Présentation d'EFS (Elastic File System) :**

EFS est un système de fichiers entièrement géré qui peut être monté sur plusieurs instances EC2 simultanément.

Caractéristiques d'EFS :

- Système de fichiers partagé (NFS)
- Peut être monté sur plusieurs instances EC2 simultanément
- Accessible à travers plusieurs zones de disponibilité
- Croissance et décroissance automatiques selon les besoins

Comparaison détaillée :

Caractéristique	EBS	EFS
Type de stockage	Stockage en bloc	Système de fichiers
Accès	Une seule instance à la fois (généralement)	Multiples instances simultanément
Disponibilité	Une seule zone de disponibilité	Plusieurs zones de disponibilité
Capacité	Fixe (peut être modifiée)	Élastique (croissance automatique)
Performance	Optimisée pour faible latence	Optimisée pour le partage de fichiers
Cas d'utilisation	Bases de données, boot volumes	Partage de fichiers, applications Web

## Utilisations courantes :

### EBS :

- Volumes de démarrage pour instances EC2
- Stockage pour bases de données
- Applications nécessitant des E/S élevées
- Applications nécessitant un contrôle granulaire sur le stockage

### EFS :

- Systèmes de gestion de contenu
- Big data et analyses
- Serveurs web et stockage de médias
- Applications nécessitant un accès partagé aux fichiers

## Contraintes techniques :

### EBS :

- Limité à une seule zone de disponibilité
- Capacité fixe (bien que modifiable)
- Performances liées au type de volume choisi
- Snapshots et chiffrement disponibles

### EFS :

- Latence légèrement plus élevée que EBS
- Coût potentiellement plus élevé pour les petits volumes de données

- Performances pouvant varier en fonction de la taille du système de fichiers

Points supplémentaires à considérer :

- Sauvegarde : EBS utilise des snapshots, EFS a son propre service de sauvegarde.
- Chiffrement : Disponible pour les deux, mais mis en œuvre différemment.
- Coût : Généralement, EBS est moins cher pour les petits volumes, EFS pour les grands volumes partagés.
- Gestion : EBS nécessite plus de gestion manuelle, EFS est plus automatisé.
- Définition d'une AMI :

## Définir ce qu'est une AMI

Une Amazon Machine Image (AMI) est un modèle préconfiguré d'une instance EC2. Elle contient les informations nécessaires pour lancer une instance, incluant :

- Un modèle pour le volume racine de l'instance (système d'exploitation, applications, etc.)
  - Des autorisations de lancement qui contrôlent quels comptes AWS peuvent utiliser l'AMI
  - Un mappage de périphériques en mode bloc spécifiant les volumes à attacher à l'instance au lancement
2. Types d'AMI :

Type d'AMI	Description	Utilisation courante
<b>AMI AWS</b>	Fournies et maintenues par AWS	Démarrage rapide, OS standard
<b>AMI de la communauté</b>	Crées et partagées par des utilisateurs AWS	Configurations spécifiques, logiciels préinstallés
<b>AMI personnalisées</b>	Crées à partir de vos propres instances EC2	Environnements spécifiques à l'entreprise, conformité
<b>AMI Marketplace</b>	AMI commerciales de fournisseurs tiers	Logiciels spécialisés, solutions clé en main

## **Création d'une AMI à partir de votre instance**

Une AMI (Amazon Machine Image) est un modèle qui contient une configuration logicielle (système d'exploitation, serveur d'applications et applications) requise pour lancer une instance. C'est comme une "photo" d'une instance EC2 qui peut être utilisée pour créer de nouvelles instances avec la même configuration.

### **Types d'AMI existants**

#### **1. AMI Amazon publiques**

- **Description:** Crées et maintenues par AWS
- **Caractéristiques:**
  - Gratuites
  - Pré-configurées avec des systèmes d'exploitation courants
  - Mises à jour régulières par AWS
- **Utilisations:**
  - Déploiement rapide d'instances standards
  - Environnements de test
  - Projets de développement

#### **2. AMI Marketplace**

- **Description:** Crées par des vendeurs tiers
- **Caractéristiques:**
  - Payantes (licence incluse)
  - Solutions pré-configurées
  - Support commercial disponible
- **Utilisations:**
  - Déploiement de solutions d'entreprise
  - Applications spécialisées
  - Solutions sécurisées

#### **3. AMI personnalisées**

- **Description:** Crées par l'utilisateur
- **Caractéristiques:**
  - Personnalisables selon les besoins
  - Privées à votre compte
  - Peuvent être partagées
- **Utilisations:**
  - Standardisation des déploiements

- Sauvegarde de configurations spécifiques
- Conformité et sécurité

## Utilisations courantes

### Scénarios d'utilisation

#### 1. Déploiement rapide

- Création rapide d'environnements identiques
- Scaling horizontal d'applications

#### 2. Sauvegarde et récupération

- Backup de configurations serveur
- Plan de reprise d'activité

#### 3. Migration

- Transfert entre régions
- Migration vers de nouveaux types d'instances

#### 4. Standardisation

- Conformité d'entreprise
- Configuration standard des serveurs

## Création d'une AMI à partir de votre instance

Voici les étapes pour créer une AMI à partir de votre instance existante :

a. Allez dans la console EC2 et sélectionnez votre instance.

b. Cliquez sur "Actions" > "Image and templates" > "Create image".

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like 'Tableau de bord EC2', 'Vue globale EC2', 'Événements', and a expanded 'Instances' section containing 'Instances', 'Types d'instances', 'Modèles de lancement', 'Demandes Spot', 'Savings Plans', and 'Instances réservées'. The main area displays a table titled 'Instances (1/1) Informations' with one row. The row shows an instance with ID 'i-0a8ba75741616cf1a', status 'Arrêté(e)', type 't2.micro', and zone 'eu'. At the bottom of the table, there are three buttons: 'Créer une image' (highlighted in blue), 'Créer un modèle à partir de l'instance', and 'En lancer plus comme ceci'. On the far right, an 'Actions' menu is open, showing options like 'Lancer des instances', 'Se connecter', 'Afficher les détails', 'Gérer l'état de l'instance', 'Paramètres de l'instance', 'Mise en réseau', 'Sécurité', 'Image et modèles' (which has 'Créer une image' listed under it), and 'Surveiller et dépanner'.

c. Donnez un nom et une description à votre AMI.

d. Ajustez les paramètres de volume si nécessaire.

[EC2](#) > [Instances](#) > [i-0a8ba75741616cf1a](#) > [Créer une image](#)

## Créer une image Informations

Une image (également appelée AMI) définit les programmes et les paramètres appliqués lorsque vous lancez une instance EC2. Vous pouvez créer une configuration d'une instance existante.

ID d'instance  
 i-0a8ba75741616cf1a

Nom de l'image  
AMI\_Test  
127 caractères maximum. Ne peut pas être modifié après la création.

Description de l'image — facultatif  
Description de l'image  
255 caractères maximum

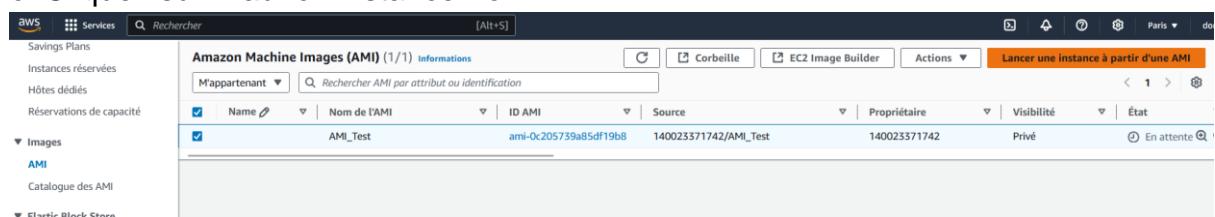
Redémarrer une instance  
Lorsque cette option est sélectionnée, Amazon EC2 redémarre l'instance afin que les données soient au repos lorsque des captures instantanées des volumes attachés sont effectuées pour assurer la cohérence des données.

Volumes d'instance

e. Cliquez sur "Create image".

**Lancer une nouvelle instance à partir de l'AMI :**

- a. Une fois l'AMI créée, allez dans "AMIs" dans le menu de gauche.
- b. Sélectionnez votre nouvelle AMI.
- c. Cliquez sur "Launch instance from AMI".



d. Suivez le processus de lancement d'instance standard.

The screenshot shows the AWS EC2 instance launch wizard. The first part is a modal titled "Sélectionner une paire de clés existante ou créer une paire de clés". It contains three options: "Paire de clés existante" (selected), "Créer une paire de clés", and "Continuer sans paire de clés". Below this is a dropdown for "Nom de la paire de clés" set to "serveur-web-dev-key". At the bottom are "Annulez" and "Lancer l'instance" buttons. The second part is the main EC2 dashboard under "Launch an instance". It shows a progress bar at 79% for "Lancement d'une instance" (Launch instance). Below it, a message says "Veuillez patienter pendant que nous lançons votre instance". The third part is a table titled "Instances (2) Informations" showing two instances: "i-0a8ba75741616cf1a" (Stopped, t2.micro) and "i-01d6758767178d061" (Running, t2.micro).

ici on peut constater que est bien démarré

Instances (2) Informations		Date de la dernière mise à jour Il y a less than a minute	Se connecter	État de l'inst...
<input type="checkbox"/>	Name	ID d'instance	État de l'instance	Type d'insta...
<input type="checkbox"/>		i-0a8ba75741616cf1a	Arrêté(e)	t2.micro
<input type="checkbox"/>		i-01d6758767178d061	En cours d'exécution	t2.micro

ici la confirmation qu'il s'agit du bien de la nouvelle AMI

▼ Détails de l'instance Informations	
Plateforme	ID AMI
Linux/UNIX (déduit)	ami-0c205739a85df19b8
Informations sur la plateforme	Nom de l'AMI
Linux/UNIX	AMI_Test
Protection contre l'arrêt	Heure de lancement
Désactivé	Fri Oct 11 2024 11:03:53 GMT+0200 (heure d'été d'Europe) (2 minutes)

## Effacement de l'AMI :

### 1. Déesenregistrement de l'AMI :

- Allez dans la console EC2 d'AWS.
- Dans le menu de gauche, cliquez sur "AMIs" sous "Images".
- Sélectionnez votre AMI.

The screenshot shows the AWS EC2 Machine Images (AMI) page. On the left, there's a sidebar with 'Tableau de bord EC2', 'Vue globale EC2', 'Événements', 'Instances' (selected), 'Images' (selected), and 'AMI' (selected). The main area displays a table titled 'Amazon Machine Images (AMI) (1/1) Informations'. It shows one item: 'Name' (AMI\_Test), 'ID AMI' (ami-0c205739a85df19b8), 'Source' (140023371742/AMI\_Test), and 'Propriétaire' (14002...). A context menu is open over the first row, with 'Désenregistrer une AMI' highlighted. Other options in the menu include 'Copier l'AMI', 'Modifier les autorisations AMI', 'Demander des instances Spot', 'Gérer les balises', 'Gérer la protection contre le déesenregistrement d'AMI', 'Modifier la description', 'Configurer le lancement rapide', 'Gérer l'obsolescence de l'AMI', 'Enregister une AMI basée sur le stockage d'instance', and 'Désactiver l'AMI'.

### d. Cliquez sur "Actions" puis "Déesenregistrer l'AMI".

The screenshot shows a confirmation dialog titled 'Désenregister une AMI'. It contains the message: 'Une fois que vous avez déesenregistré une AMI, vous ne pouvez pas l'utiliser pour lancer de nouvelles instances.' Below this is the question: 'Voulez-vous vraiment déesenregistrer ces AMI ?' followed by a checkbox with the value 'ami-0c205739a85df19b8'. A warning box contains the text: 'Des frais continueront à vous être facturés pour les instantanés associés' and 'Les instantanés ne sont pas automatiquement supprimés lorsque vous déesenregistrez une AMI. Une fois que vous aurez déesenregistré l'AMI, vous pouvez supprimer les instantanés sur l'écran d'instantanés.' At the bottom are two buttons: 'Annulez' and 'Désenregister une AMI'.

### e. Confirmez l'action.

## Suppression du snapshot associé :

- Après avoir déesenregistrer l'AMI, allez dans "Snapshots" dans le menu de gauche.

- b. Trouvez le snapshot associé à votre AMI (il aura généralement une description liée à l'AMI).
- c. Sélectionnez le snapshot.
- d. Cliquez sur "Actions" puis "Supprimer le snapshot".
- e. Confirmez la suppression.

#### Vérification :

- Retournez dans la section AMIs et assurez-vous que votre AMI n'est plus listée.
- Vérifiez également dans la section Snapshots que le snapshot associé a bien été supprimé.

## Chiffrement des volumes EC2

### Définition

Le chiffrement EBS (Elastic Block Store) est une solution de chiffrement transparent pour les volumes EBS qui ne nécessite pas de configuration supplémentaire de la part de l'utilisateur. Il utilise les clés AWS KMS (Key Management Service) pour le chiffrement.

### Méthodes de chiffrement

#### 1. Chiffrement d'un nouveau volume

- Création directe d'un volume chiffré
- Utilisation des clés KMS par défaut ou personnalisées
- Configuration au moment de la création

#### 2. Chiffrement d'un volume existant

Processus en plusieurs étapes :

1. Création d'un snapshot du volume

2. Création d'une copie chiffrée du snapshot
3. Création d'un nouveau volume à partir du snapshot chiffré
4. Remplacement du volume original

## **Guide pratique de chiffrement**

### **Méthode 1 : Pour un volume existant**

1. Création du snapshot

Actions > Créer un snapshot

2. Copie du snapshot avec chiffrement

Actions > Copier le snapshot

Activer le chiffrement

3. Création du nouveau volume

Actions > Créer un volume

Sélectionner le snapshot chiffré

4. Attachement du nouveau volume

Actions > Attacher le volume

### **Méthode 2 : Pour une nouvelle instance**

1. Lors du lancement

- Activer le chiffrement par défaut

- Sélectionner la clé KMS

- Configurer les volumes additionnels

## **Configuration de KMS**

### Clés de chiffrement

1. Clé par défaut

- aws/ebs
- Gérée par AWS
- Gratuite

## 2. Clé personnalisée

- Création dans KMS
- Gestion des permissions
- Coût supplémentaire

## **Bonnes pratiques**

### Sécurité

#### 1. Gestion des clés

- Rotation régulière
- Audit des accès
- Sauvegarde des clés

#### 2. Documentation

- Inventaire des volumes chiffrés
- Procédures de récupération
- Historique des modifications

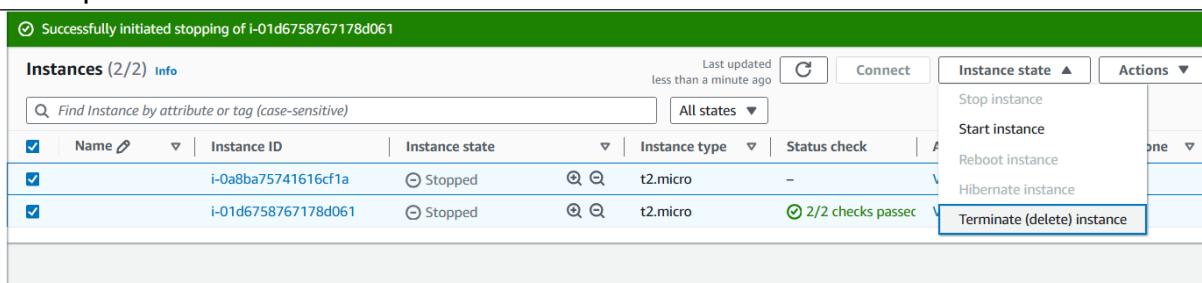
## **Performance**

- Impact minimal sur les performances
- Latence légèrement augmentée
- Compatibilité avec tous les types de volumes

## Résiliation de toutes les instances et volumes

### Résiliation des instances EC2 :

- Allez dans la console EC2 d'AWS.
- Sélectionnez "Instances" dans le menu de gauche.
- Sélectionnez toutes les instances que vous avez créées.
- Cliquez sur "Instance state" > "Terminate instance".

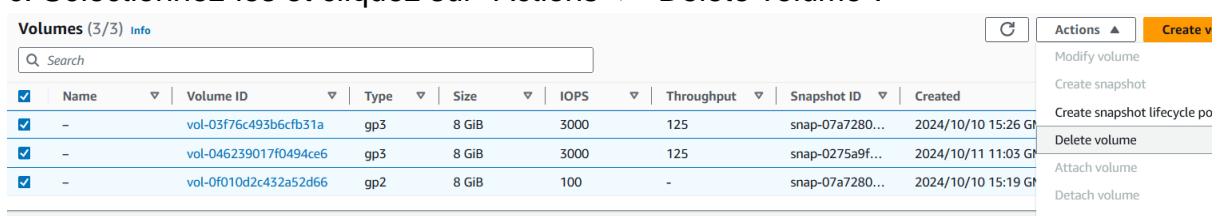


The screenshot shows the AWS EC2 Instances page. At the top, a green banner indicates "Successfully initiated stopping of i-01d6758767178d061". Below this, the "Instances (2/2) info" section displays two instances: "i-0a8ba75741616cf1a" and "i-01d6758767178d061", both of which are currently stopped. On the right side of the table, there is a "Actions" column with a dropdown menu open. The "Terminate (delete) instance" option is highlighted with a blue border.

- Confirmez la résiliation.

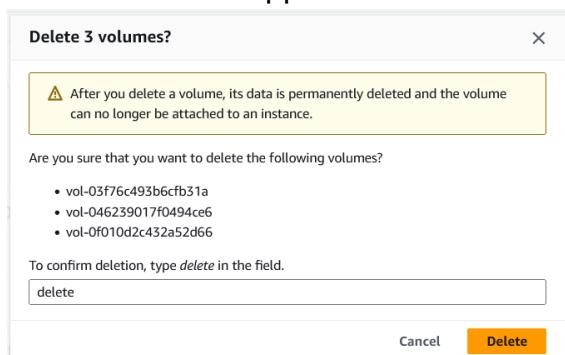
### Suppression des volumes EBS :

- Dans la console EC2, allez dans "Volumes" sous "Elastic Block Store".
- Identifiez les volumes que vous avez créés.
- Sélectionnez-les et cliquez sur "Actions" > "Delete volume".



The screenshot shows the AWS EBS Volumes page. It lists three volumes: "vol-03f76c493b6cfb31a", "vol-046239017f0494ce6", and "vol-0f010d2c432a52d66", all of which are selected. On the right side, the "Actions" menu is open, and the "Delete volume" option is highlighted with a blue border.

- Confirmez la suppression.



The screenshot shows a confirmation dialog titled "Delete 3 volumes?". It contains a warning message: "⚠ After you delete a volume, its data is permanently deleted and the volume can no longer be attached to an instance." Below this, it asks "Are you sure that you want to delete the following volumes?" followed by a list of three volume IDs: "vol-03f76c493b6cfb31a", "vol-046239017f0494ce6", and "vol-0f010d2c432a52d66". A text input field at the bottom is labeled "To confirm deletion, type *delete* in the field." with the word "delete" already typed in. At the bottom right are "Cancel" and "Delete" buttons, with "Delete" being highlighted in orange.

## Vérification des ressources associées :

- a. Vérifiez les snapshots (Snapshots sous Elastic Block Store).
- b. Vérifiez les AMIs (AMIs sous Images).
- c. Vérifiez les Elastic IPs (Elastic IPs sous Network & Security).
- d. Supprimez ces ressources si elles ne sont plus nécessaires.

## Nettoyage des groupes de sécurité :

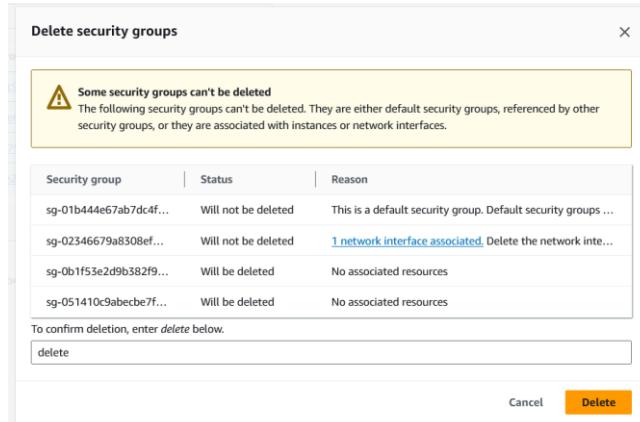
- a. Allez dans "Security Groups" sous Network & Security.

Security Groups (4/4) <a href="#">Info</a>					<a href="#">Actions ▲</a>	<a href="#">Export security</a>
<input type="text"/> Find resources by attribute or tag						
✓	Name	▼	Security group ID	▼	Security group name	▼
✓	-		<a href="#">sg-051410c9abecbe7f0</a>		launch-wizard-1	
✓	-		<a href="#">sg-01b444e67ab7dc4f3</a>		default	
✓	-		<a href="#">sg-02346679a8308efd8</a>		launch-wizard-2	
✓	-		<a href="#">sg-0b1f53e2d9b382f98</a>		launch-wizard-3	

[View details](#)  
[Edit inbound rules](#)  
[Edit outbound rules](#)  
[Manage tags](#)  
[Manage stale rules](#)  
[Copy to new security group](#)  
[Delete security groups](#)

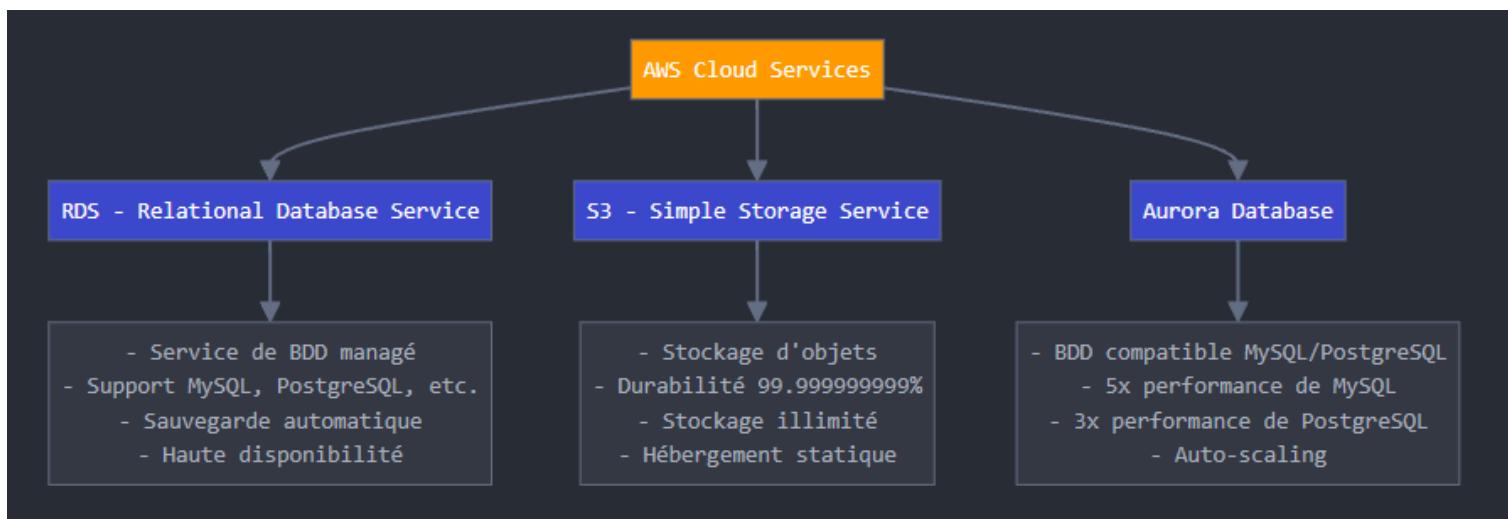
vpc-005ebf27fb2bad676 [x]

- b. Supprimez les groupes de sécurité personnalisés que vous avez créés.



## JOUR 3 AWS -RDS & S3

Résumé détaillé des trois services AWS demandés :



### 1. Amazon RDS (Relational Database Service)

C'est un service de base de données relationnelle managé. Permet de déployer et gérer facilement des bases de données. Prend en charge plusieurs moteurs de base de données (MySQL, PostgreSQL, MariaDB, etc.)

- Gère automatiquement :
  - Les sauvegardes
  - Les mises à jour
  - La haute disponibilité
  - La scalabilité

Choisir RDS quand :

- Vous avez besoin d'une base de données relationnelle classique
- Vous voulez une solution simple à gérer
- Votre budget est limité
- Les performances standard sont suffisantes
- Exemples :
  - Site web avec trafic modéré
  - Applications d'entreprise classiques
  - Systèmes de gestion de contenu

## 2. Amazon Aurora

C'est un moteur de base de données relationnelle compatible MySQL et PostgreSQL

- Performances :
  - 5x les performances de MySQL standard
  - 3x les performances de PostgreSQL standard
- Caractéristiques principales :
  - Auto-scaling automatique
  - Réplication multi-région
  - Sauvegarde continue
  - Reprise après sinistre automatisée

**Choisir Aurora quand :**

- Vous avez besoin de performances élevées
- Votre application nécessite une haute disponibilité
- Vous avez un budget plus important
- Vous anticipiez une forte croissance
- Exemples :
  - Applications à fort trafic
  - Applications financières
  - Jeux en ligne
  - E-commerce à grande échelle

## 3. Amazon S3 (Simple Storage Service)

Service de stockage d'objets hautement évolutif

- Caractéristiques principales :
  - Durabilité de 99,99999999%
  - Stockage illimité
  - Différentes classes de stockage selon les besoins

- Cas d'utilisation :
  - Stockage de fichiers
  - Hébergement de sites web statiques
  - Sauvegarde et archivage
  - Stockage d'applications

### **Choisir S3 quand :**

- Vous devez stocker des fichiers
- Vous n'avez pas besoin de structure relationnelle
- Vous voulez une solution très économique
- Vous avez besoin d'un accès depuis le web
- Exemples :
  - Stockage de médias (images, vidéos)
  - Hébergement de sites statiques
  - Backups
  - Archivage de données

### **Critères de décision clés en terme de budget :**

- S3 : Le moins cher pour le stockage simple
- RDS : Coût modéré
- Aurora : Le plus cher mais plus performant

## **Read Replica - Définition et utilisation**

Un Read Replica, c'est comme une photocopie en lecture seule de votre base de données principale. Imaginez :

- **Base principale** : C'est là où se font toutes les écritures (ajouts, modifications)
- **Read Replica** : C'est une copie qui sert uniquement à lire les données

L'avantage principal ?

Quand beaucoup d'utilisateurs veulent lire des données en même temps, au lieu que tout le monde sollicite la base principale, certains peuvent lire depuis les copies

C'est comme avoir plusieurs exemplaires d'un livre populaire dans une bibliothèque au lieu d'un seul

### **1. Définition :**

- Copie en lecture seule de la base de données principale

- Synchronisée de manière asynchrone avec la base principale
- Peut être créée dans la même région ou dans une autre région AWS

## 2. Utilité :

- Améliore les performances en distribuant la charge de lecture
- Permet de répartir les requêtes de lecture sur plusieurs bases
- Soulage la base de données principale

## 3. Contexte d'utilisation :

- Applications avec beaucoup plus de lectures que d'écritures
- Rapports et analyses qui nécessitent beaucoup de lectures
- Applications nécessitant une scalabilité des lectures

## Étapes de déploiement RDS

### Accès à RDS

- Connectez-vous à la console AWS
- Dans la barre de recherche en haut, tapez "RDS"
- Cliquez sur le service "RDS"

### Création de la base

- Cliquez sur le bouton orange "Create database"

**Créer une base de données**

Amazon Relational Database Service (RDS) facilite l'installatio  
l'utilisation et la mise à l'échelle d'une base de données relativ  
dans le cloud.

**Créer une base de données**

Remarque : vos instances de base de données seront lancées i

## Méthode de création

- Choisissez "Standard create"
- Cette option vous donne plus de contrôle sur les paramètres

## Créer une base de données Infos

### Choisir une méthode de création de bases de donn

#### Crédation standard

Vous définissez toutes les options de configuration, y compris celles relatives à la disponibilité, la sécurité, aux sauvegardes et à la maintenance.



## Options du moteur, Templates

### Version du moteur

MySQL 8.0.39

#### Activer le support étendu RDS Infos

Le support étendu Amazon RDS est un [offre payante](#). En sélectionnant cette option, vous utilisez la version majeure de votre base de données au-delà de la date de fin de support standard pour votre version majeure dans le [Documentation RDS](#)

## Modèles

Choisissez un exemple de modèle en fonction de votre scénario d'utilisation.

#### Production

Utilisez les valeurs par défaut pour la haute disponibilité et pour des performances rapides, uniformes.

#### Dev/Test

Cette instance est destinée au développement en dehors d'un environnement de production.

## Important!!

**Disponibilité et durabilité**

**Options de déploiement** [Infos](#)  
Les options de déploiement ci-dessous sont limitées à celles prises en charge par le moteur que vous avez sélectionné ci-dessus.

- Cluster de bases de données multi-AZ**  
Crée un cluster de base de données avec une instance de base de données primaire et deux instances de base de données de secours accessibles en lecture, chaque instance de base de données se trouvant dans une zone de disponibilité différente. Fournit la haute disponibilité et la redondance des données, et augmente la capacité de traitement des applications en lecture.
- Instance de base de données Multi-AZ**  
Crée une instance de base de données primaire et une instance de base de données de secours dans une autre zone de disponibilité. Fournit la haute disponibilité et la redondance des données, mais l'instance de base de données de secours ne prend pas en charge les connexions pour les applications en lecture.
- Instance de base de données unique**  
Crée une instance de base de données unique sans instance de base de données de secours.

## Paramètres

**DB instance identifier:**  
**laplateforme**

**Identifiant de cluster de base de données** [Infos](#)

Saisissez un nom pour votre cluster de base de données. Le nom doit être unique parmi tous les clusters de bases de données appartenant à votre compte AWS dans la région AWS actuelle.

**laplateforme**

L'identifiant d'instance DB est sensible à la casse, mais il stocké intégralement en minuscules, comme dans « mydbcluster ». Limites : 1 à 60 caractères alphanumériques ou traits d'union. Le premier caractère doit être une lettre. Il ne peut contenir deux traits d'union consécutifs et ne peut se terminer par un trait d'union.

▼ Configuration des informations d'identification

**Identifiant principal** [Infos](#)

Saisissez un ID de connexion pour l'utilisateur principal de votre cluster de bases de données.

**laplateforme**

Entre 1 et 16 caractères alphanumériques. Le premier caractère doit être une lettre.

**Gestion des informations d'identification**

Vous pouvez utiliser AWS Secrets Manager ou gérer les informations d'identification de votre utilisateur principal.

**Géré dans AWS Secrets Manager - le plus sûr**

RDS génère un mot de passe pour vous et le gère tout au long de son cycle de vie à l'aide d'AWS Secrets Manager.

**Autogéré**

Créez votre propre mot de passe ou demandez à RDS de créer un mot de passe que vous gérez.

**Générer automatiquement un mot de passe**

Amazon RDS peut générer un mot de passe pour vous. Vous pouvez aussi spécifier votre propre mot de passe.

**Mot de passe principal** [Infos](#)

.....

**Password strength** Weak

Contraintes minimales : au moins 8 caractères ASCII imprimables. Ne peut contenir aucun des symboles suivants : / " @

**Confirmer le mot de passe principal** [Infos](#)

.....

## Configuration de l'instance

**db.t3.micro**

**Configuration d'instance**

Les options de configuration d'instance de base de données ci-dessous sont limitées à celles prises en charge par le moteur choisi ci-dessus.

**Classe d'instance de base de données** [Infos](#)

▼ Masquer les filtres

**Afficher les classes d'instance qui prennent en charge les écritures optimisées pour Amazon RDS**

**Infos**

Les écritures optimisées pour Amazon RDS améliorent le débit d'écriture jusqu'à 2 fois plus rapide, sans frais supplémentaires.

**Inclure les classes de la génération précédente**

**Classes standard (inclus les classes m)**

**Classes à mémoire optimisée (inclus les classes r et x)**

**Classe à capacité extensible (inclus les classes t)**

**db.t3.micro**  
2 vCPUs 1 GiB RAM Réseau : Jusqu'à 2.085 Mbps

## Stockage

Storage type: General Purpose SSD (gp2)

Allocated storage: 20 GiB

Maximum storage threshold: 1024 GiB

### Stockage

#### Type de stockage [Infos](#)

Les volumes de stockage SSD à IOPS provisionnés (IoZ) sont désormais disponibles.

**SSD polyvalent (gp3)**

Les performances évoluent indépendamment du stockage.

#### Stockage alloué [Infos](#)

200

GiB

Minimum : 20 GiB. Maximum : 6 144 GiB

Après avoir modifié le stockage d'une instance de base de données, l'instance de base sera en statut d'optimisation du stockage. Votre instance restera disponible jusqu'à la fin de l'opération d'optimisation du stockage. [En savoir plus](#)

#### Paramètres avancés

Pour un stockage alloué inférieur à 400 GiB, une base de 3 000 IOPS et un débit de stockage de 125 MiB/s sont inclus.

Pour allouer des IOPS et un débit supplémentaires, augmentez le stockage alloué à 400 GiB ou plus.

#### IOPS provisionnés [Infos](#)

3000

IOPS

#### Débit de stockage [Infos](#)

125

MiBps

#### Mise à l'échelle automatique du stockage

#### Mise à l'échelle automatique du stockage [Infos](#)

Fournit un support de mise à l'échelle de votre stockage de base de données en fonction des besoins de votre application.

##### Activer la mise à l'échelle automatique du stockage

L'activation de cette fonction autorisera l'augmentation du stockage une fois que le seuil défini sera dépassé.

#### Seuil de stockage maximal [Infos](#)

Des frais seront appliqués lorsque votre base de données sera automatiquement mise à l'échelle au seuil défini.

1024

GiB

La valeur de stockage allouée doit être comprise entre 220 GiB et 6 144 GiB

## Points importants à savoir

- Le stockage ne s'étendra jamais au-delà de 1 To
- L'extension est automatique
- Le stockage ne se réduit jamais automatiquement
- AWS vous facture uniquement l'espace réellement utilisé

## Connectivité

### Connectivité [Infos](#)

#### Ressource de calcul

Choisissez si vous souhaitez configurer une connexion à une ressource de calcul. La connexion modifiera automatiquement les paramètres de connectivité de données.

##### Ne pas se connecter à une ressource de calcul EC2

Ne configurez pas de connexion à une ressource de calcul pour cette base de données. Vous pouvez configurer manuellement une connexion à une ressource de calcul ultérieurement.

Public access: Yes

Accès public [Infos](#)

Oui

RDS attribue une adresse IP publique pour connecter à votre cluster. Les groupes de sécurité VPC spécifiques

VPC security group: Create new

New VPC security group name: rds-laplateforme-sg

Groupe de sécurité VPC (pare-feu) [Infos](#)

Choisissez un ou plusieurs groupes de sécurité VPC pour autoriser l'accès à votre base de données. Assurez-vous que les règles du groupe de sécurité autorisent le trafic entrant approprié.

Choisir existants

Choisir les groupes de sécurité VPC existants

Créer

Créer un groupe de sécurité VPC

Nom du nouveau groupe de sécurité VPC

rds-mysql-public

## Base de données authentification

[x] Password authentication

### Authentification de base de données

Options d'authentification de base de données [Infos](#)

Authentification par mot de passe

L'authentification s'effectue en utilisant les mots de passe de la base de données.

Authentification de base de données par mot de passe et IAM

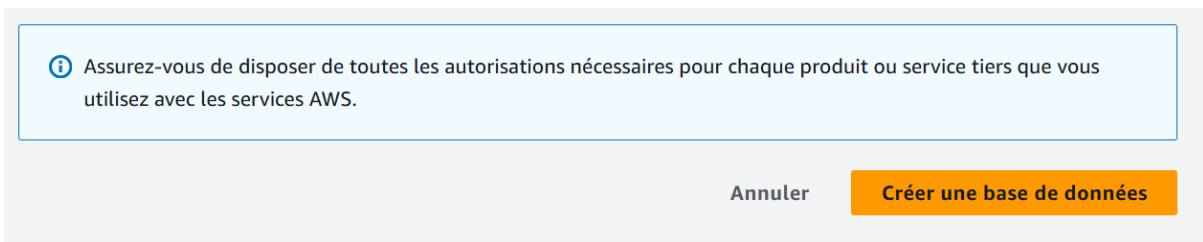
L'authentification s'effectue en utilisant le mot de passe et les informations d'identification utilisateur de la base de données via les utilisateurs et les rôles AWS IAM.

Authentification par mot de passe et Kerberos (non disponible pour le cluster de bases de données Multi-AZ)

Choisissez un répertoire dans lequel vous voulez permettre aux utilisateurs autorisés de s'authentifier auprès de cette instance de base de données à l'aide de l'authentification Kerberos.

## Création finale

- Vérifiez tous les paramètres
- Cliquez sur "Create database"



**Après la création :**

- **Vous pouvez suivre le progrès dans la section "Databases"**
- **Le statut passera à "Available" une fois terminé**

Identifiant de base de données	Statut	Rôle	Moteur	Région ...	Taille
laplateforme	Disponible	Instance	MySQL Co...	eu-west-3c	db.t3.micro

## -Installation de SQLSelectron et connection à la BD

### Trouver l'endpoint dans la console AWS

1. Allez dans le service RDS
2. Cliquez sur "Bases de données" dans le menu de gauche
3. Cliquez sur le nom de votre base "laplateforme"
4. Dans la page de détails, regardez la section "Connectivity & security"

### Connectivité et sécurité

Point de terminaison et port

Point de terminaison  
laplateforme.cricuyouc8gc.eu-west-3.rds.amazonaws.com

Port  
3306

### Dans SQLSelectron :

### Configuration:

1. Add - Create New Connection
2. Type : MySQL
3. Name : Laplateforme RDS

4. Server Address : [votre endpoint]

5. User : laplateforme

6. Password : tropcool

7. Port : 3306

**Pour créer la base aws\_db :**

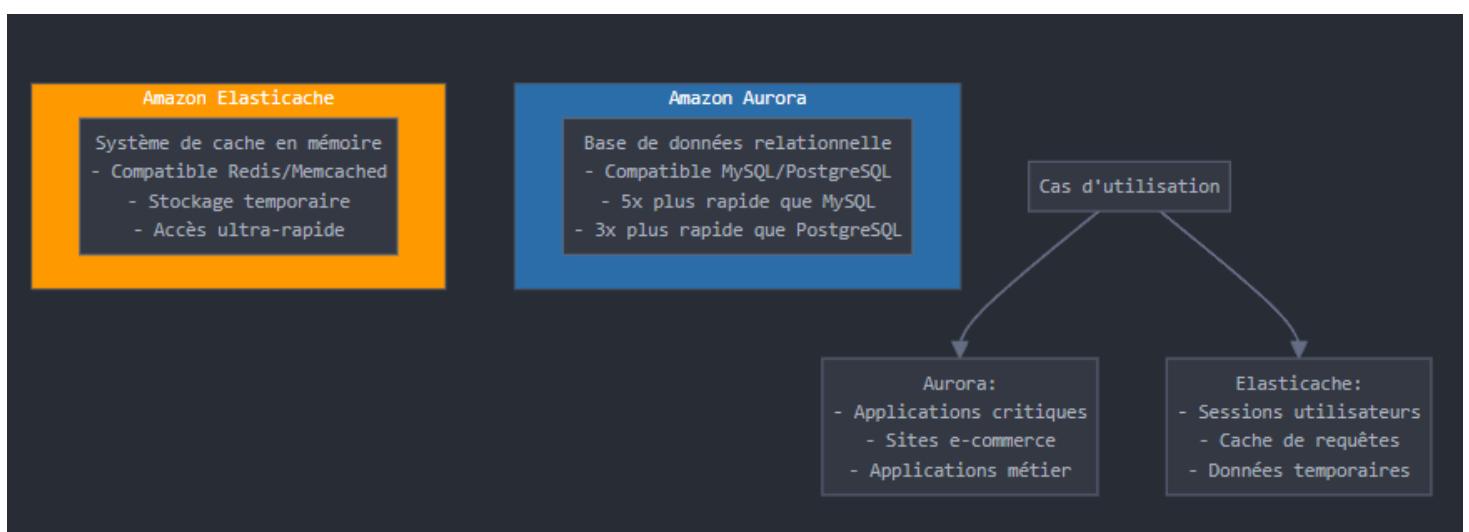
sql

Copy

**CREATE DATABASE aws\_db;**

The screenshot shows the SQL Electron interface. On the left, there's a sidebar titled 'Laplateforme RDS MySQL' with a search bar and a list of databases: aws\_db, information\_schema, mysql, performance\_schema, and sys. On the right, a main panel titled 'undefined #1' contains the SQL command 'CREATE DATABASE aws\_db;'. The command is numbered 1 and 2, with the second line being the semicolon.

## Amazon Aurora, Amazon ElastiCache - Définition et utilisation



### 1. Amazon Aurora :

#### A. Fonctionnement

- Moteur de base de données cloud-native
- Architecture distribuée
- Stockage automatiquement réparti sur 3 zones
- Réplication continue des données

## B. Spécifications techniques

- Performance :
  - 5x les performances de MySQL
  - 3x les performances de PostgreSQL
- Stockage auto-extensible jusqu'à 128 To
- Jusqu'à 15 répliques en lecture
- Recovery Point Objective (RPO) quasi nul

## C. Différences avec RDS standard

Aurora	RDS Standard
----- -----	
Cloud-native	DB traditionnelle
Plus performant	Performance standard
Plus cher	Moins cher
Auto-healing	Backup manuel possible

## D. Cas d'utilisation

- Applications SaaS
- Jeux en ligne
- E-commerce à grande échelle
- Applications critiques

## 2. Amazon ElastiCache :

### A. Fonctionnement

- Service de cache en mémoire
- Supporte Redis et Memcached
- Stockage des données fréquemment accédées
- Réduit la charge sur la base de données principale

## B. Spécifications techniques

- Latence < 1 milliseconde
- Scalabilité horizontale et verticale
- Encryption au repos et en transit
- Backup et restauration automatiques

## C. Différences entre Redis et Memcached

Redis		Memcached
-----	-----	
Structures complexes		Structures simples
Persistence		Pas de persistance
Multi-AZ		Single-AZ
Réplication		Pas de réplication

## D. Exemples d'utilisation

### 1. Redis

- Leaderboards de jeux
- Sessions utilisateurs
- Files d'attente
- Cache géospatial

### 2. Memcached

- Cache de page web
- Cache d'objets simples
- Cache de résultats DB

### Exemple concret d'architecture :

Client → ElastiCache (cache rapide)

    ↳ Aurora (si données pas en cache)

Cette architecture permet :

- Des performances optimales
- Une réduction des coûts
- Une meilleure expérience utilisateur

**Amazon Aurora en bref :** C'est une base de données relationnelle compatible avec MySQL et PostgreSQL, créée par AWS. Son principal avantage est la performance : elle est jusqu'à 5 fois plus performante que MySQL standard et 3 fois plus que PostgreSQL. Elle est idéale pour les applications nécessitant haute disponibilité et performance, comme les sites e-commerce ou les applications critiques d'entreprise.

**Amazon ElastiCache en bref :** C'est un service de mise en cache en mémoire qui supporte deux types de moteurs : Redis et Memcached. Son but principal est d'améliorer les performances des applications en stockant temporairement des données fréquemment consultées en mémoire. Typiquement utilisé pour le cache de session utilisateur, les classements en temps réel (leaderboards) et pour réduire la charge sur les bases de données principales.

La différence principale :

- Aurora = Base de données permanente haute performance
- ElastiCache = Système de cache temporaire ultra-rapide

## Présentation de S3

C'est un service de stockage d'objets (fichiers) en ligne d'AWS. Imaginez un immense disque dur sur internet avec une capacité illimitée.

**Caractéristiques principales :**

- Stockage illimité
- Haute disponibilité (99.99%)
- Sécurisé (chiffrement disponible)
- Accessible via internet

**Utilisations courantes :**

- Stockage de fichiers (images, vidéos, documents)
- Hébergement de sites web statiques
- Sauvegardes
- Stockage d'applications

**Tarification simple :**

- Vous payez uniquement ce que vous utilisez
- Basé sur :

- Volume stocké
- Transfert de données
- Nombre de requêtes

## Création pratique d'un bucket S3

Dans la console AWS:

Services > S3 > Create bucket



Configuration de base :

- Nom du bucket : choisissez un nom unique
- Région : gardez votre région actuelle

**Configuration générale**

Région AWS  
Europe (Paris) eu-west-3

Nom du compartiment [Info](#)

Le nom du compartiment doit être unique dans l'espace de nommage global et respecter les règles de dénomination des compartiments [\[?\] Copier les paramètres depuis un compartiment existant - facultatif](#)  
Seuls les paramètres de compartiment dans la configuration suivante sont copiés.

[Sélectionner un compartiment](#)

Format : s3://bucket/prefix

**Important :**

- **Le nom doit être unique au niveau mondial**
- **Si un nom est déjà pris, AWS vous le dira immédiatement**
- **Évitez les caractères spéciaux**

## Les paramètres spécifiques demandés:

Object Ownership : ACLs disabled

### Propriété d'objets Info

Contrôlez la propriété des objets écrits dans ce compartiment à partir d'autres comptes AWS et l'utilisation des listes de contrôle (ACL). La propriété des objets détermine qui peut spécifier l'accès aux objets.

- Listes ACL désactivées (recommandé)**  
Tous les objets de ce compartiment sont gérés par ce compte. L'accès à ce compartiment et à ses objets est spécifié en utilisant uniquement des politiques.

- Listes ACL activées**  
Les objets de ce compartiment peuvent être gérés par d'autres comptes AWS. L'accès à ce compartiment et à ses objets peut être spécifié à l'aide des listes ACL.

Propriété d'objets

Propriétaire du compartiment appliquée

Block Public Access : cocher tout

### Gestion des versions de compartiment

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour conserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Grâce à la gestion des versions, vous pouvez aisément récupérer en cas d'actions involontaires des utilisateurs et de défaillances des applications. [En savoir plus](#)

Versioning : désactivé

### Gestion des versions de compartiment

- Désactiver  
 Activer

#### Paramètres de blocage de l'accès public pour ce compartiment

L'accès public aux compartiments et aux objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, de point d'accès et de tous ces éléments à la fois. Pour bloquer l'accès public à votre compartiment et aux objets qui contiennent, activez le paramètre Bloquer tous les accès publics. Si l'application fonctionne correctement à ce compartiment et à ses points d'accès, AWS recommande de bloquer tous les accès publics, mais avant d'appliquer ces paramètres, vérifiez que vos applications fonctionnent correctement sans accès public. Si vous souhaitez autoriser un certain niveau d'accès public pour votre compartiment ou ses objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos besoins en stockage. [En savoir plus](#)

##### Bloquer tous les accès publics

L'activation de ce paramètre revient à activer les quatre paramètres ci-dessous. Chacun des paramètres suivants est indépendant l'un de l'autre.

- Bloquer l'accès public aux compartiments et aux objets, accordé via de nouvelles listes de contrôle d'accès (ACL)  
S3 bloque les autorisations d'accès publiques appliquées aux compartiments ou objets récemment ajoutés et empêche la création de listes ACL d'accès public pour les compartiments et objets existants. Ce paramètre ne modifie pas les autorisations existantes qui permettent l'accès public aux ressources S3 qui utilisent les listes ACL.
- Bloquer l'accès public aux compartiments et aux objets, accordé via n'importe quelles listes de contrôle d'accès (ACL)  
S3 ignore toutes les listes ACL qui accordent l'accès public aux compartiments et aux objets.
- Bloquer l'accès public aux compartiments et aux objets, accordé via de nouvelles stratégies de compartiment ou de point d'accès public  
S3 bloque les nouvelles stratégies de compartiment et de point d'accès qui accordent un accès public aux compartiments et objets. Ce paramètre ne modifie pas les stratégies existantes qui autorisent l'accès public aux ressources S3.
- Bloquer l'accès public et entre comptes aux compartiments et objets via n'importe quelles stratégies de compartiment ou de point d'accès public  
S3 ignore l'accès public et entre comptes pour les compartiments ou points d'accès avec des stratégies qui accordent l'accès public aux compartiments et aux objets.

Encryption : SSE-S3

Bucket Key : activé

### Chiffrement par défaut Info

Le chiffrement côté serveur est automatiquement appliqué aux nouveaux objets stockés dans ce compartiment.

#### Type de chiffrement Info

- Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)  
 Chiffrement côté serveur avec des clés AWS Key Management Service (SSE-KMS)  
 Chiffrement côté serveur double couche avec des clés AWS Key Management Service (DSSE-KMS)  
Sécurisez vos objets avec deux couches de chiffrement distinctes. Pour plus d'informations sur la tarification, consultez [Tarification DSSE-KMS](#) dans l'onglet Stockage de la page [tarification Amazon S3](#).

#### Clé de compartiment

L'utilisation d'une clé de compartiment S3 pour SSE-KMS réduit les coûts de chiffrement en réduisant les appels à AWS KMS. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS. [En savoir plus](#)

- Désactiver  
 Activer

Une fois créé, uploadez les fichiers :

### Compartiments à usage général (1) Info Toutes les régions AWS

Les compartiments sont des conteneurs pour les données stockées dans S3.

Copier l'ARN Vider Supprimer Crée un compartiment

Rechercher des compartiments par nom

< 1 >

Nom	Région AWS	Analyseur d'accès IAM	Date de création
<a href="#">laplateforme-dome-bucket-2024</a>	Europe (Paris) eu-west-3	<a href="#">Afficher l'analyseur pour eu-west-3</a>	13 Nov 2024 04:34:17 PM CET

Aucun objet

Vous n'avez aucun objet dans ce compartiment.

- LogoPlateforme.png
- s3.txt

Nom	Dossier
s3.txt	-
Logo_Plateforme_Blc_fond-bleu.png	-

## Générer une "bucket policy" pour permettre l'accès public à l'image

Dans votre bucket S3 :

- Sélectionnez votre bucket
- Allez dans l'onglet "Autorisations"

Pour la Bucket Policy ajouter :

{

"Version": "2012-10-17",

```
"Statement": [  
    {  
        "Sid": "PublicReadForGetObject",  
        "Effect": "Allow",  
        "Principal": "*",  
        "Action": "s3:GetObject",  
        "Resource": "arn:aws:s3:::NOM-DE-VOTRE-BUCKET/*"
```

**Stratégie de compartiment**

La stratégie de compartiment, écrite au format JSON, permet d'accéder aux objets stockés dans le compartiment. Les stratégies de compartiment ne s'appliquent pas aux objets appartenant à d'autres comptes. [En savoir plus](#)

**Modifier** **Supprimer** **Copier**

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "PublicReadForGetObject",  
            "Effect": "Allow",  
            "Principal": "*",  
            "Action": "s3:GetObject",  
            "Resource": "arn:aws:s3:::laplateforme-dome-bucket-2024/*"  
        }  
    ]  
}
```

}

]

}

## Pour l'appliquer

1. Dans "Bucket Policy", cliquez "Modifier"
4. Cliquez "Save"

### Bloquer l'accès public (paramètres de compartiment)

Modifier

L'accès public aux compartiments et objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, des stratégies de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à tous vos compartiments et objets S3, activez « Bloquer tous les accès publics ». Ces paramètres s'appliquent uniquement à ce compartiment et ses points d'accès. AWS recommande d'activer « Bloquer tous les accès publics ». Toutefois, avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos cas d'utilisation de stockage spécifiques. [En savoir plus](#)

#### Bloquer tous les accès publics

⚠ Désactivé

#### ▼ Paramètres de blocage individuel de l'accès public pour ce compartiment

##### Bloquer l'accès public aux compartiments et aux objets, accordé via de **nouvelles listes de contrôle d'accès (ACL)**

S3 bloque les autorisations d'accès public appliquées aux compartiments ou objets récemment ajoutés et empêche la création de listes ACL d'accès public pour les compartiments et objets existants. Ce paramètre ne modifie pas les autorisations existantes qui permettent l'accès public aux ressources S3 qui utilisent les listes ACL.

##### Bloquer l'accès public aux compartiments et aux objets, accordé via **n'importe quelles listes de contrôle d'accès (ACL)**

S3 ignore toutes les listes ACL qui accordent l'accès public aux compartiments et aux objets.

##### Bloquer l'accès public aux compartiments et aux objets, accordé via de **nouvelles stratégies de compartiment ou de point d'accès public**

S3 bloque les nouvelles stratégies de compartiment et de point d'accès qui accordent un accès public aux compartiments et objets. Ce paramètre ne modifie pas les stratégies existantes qui autorisent l'accès public aux ressources S3.

##### Bloquer l'accès public et entre comptes aux compartiments et objets via **n'importe quelles stratégies de compartiment ou de point d'accès public**

S3 ignore l'accès public et entre comptes pour les compartiments ou points d'accès avec des stratégies qui accordent l'accès public aux compartiments et aux objets.

**Une fois fait, on peut accéder à votre image via l'URL du type :**

<https://NOM-BUCKET.s3.REGION.amazonaws.com/LogoPlateforme.png>

**Le JSON (la bucket policy) est crucial pour plusieurs raisons :**

1. Désactiver le blocage public = "Ouvrir la porte"
2. La bucket policy = "Donner la permission d'entrer"

Sans la policy, même avec le blocage public désactivé, les fichiers restent inaccessibles car par défaut, S3 refuse tout accès externe.

Le JSON que nous avons ajouté dit essentiellement :

"Autoriser (\*) tout le monde à

voir (GetObject) les fichiers

dans ce bucket"

C'est comme avoir :

- Une porte déverrouillée (blocage public désactivé)
- Une autorisation écrite (bucket policy) pour entrer

Les deux sont nécessaires pour un accès public complet !

## Héberger ce site statique sur S3

**D'abord, activez l'hébergement de site web statique sur le bucket :**

1. Allez dans les propriétés du bucket

## 2. Descendez jusqu'à "Static website hosting"

**Hébergement de site Web statique**

Utilisez ce compartiment pour héberger un site Web ou rediriger des demandes. [En savoir plus](#)

**Modifier**

**Nous vous recommandons d'utiliser AWS Amplify Hosting pour l'hébergement de sites Web statiques**

Déployez rapidement un site Web rapide, sécurisé et fiable avec AWS Amplify Hosting. Apprenez-en plus sur [Amplify Hosting](#) ou [consultez vos applications Amplify existantes](#)

**Créer une application Amplify**

Hébergement de site Web statique S3  
Désactivé

### 3. Cliquez sur "Edit"

### 4. Activez l'hébergement statique

### 5. Définissez :

- Index document: index.html
- Error document: index.html

**Hébergement de site Web statique**

Utilisez ce compartiment pour héberger un site Web ou rediriger des demandes. [En savoir plus](#)

**Hébergement de site Web statique**

Désactiver  
 Activer

**Type d'hébergement**

Héberger un site Web statique  
Utilisez le point de terminaison du compartiment comme adresse Web. [En savoir plus](#)

Rediriger des demandes pour un objet  
Redirige les demandes vers un autre compartiment ou domaine. [En savoir plus](#)

**Document d'index**  
Spécifiez la page d'accueil ou par défaut du site Web.  
index.html

**Document d'erreur - facultatif**  
Cette valeur est renvoyée en cas d'erreur.  
index.html

**Règles de redirection - facultatif**  
Les règles de redirection, écrites au format JSON, redirigent automatiquement les demandes de pages Web pour du contenu spécifique. [En savoir plus](#)

1

JSON   Ln 1, Col 1   0 Erreurs   0 Avertissements

Annuler   Enregistrer les modifications

### Uploadez les fichiers dans le bon ordre :

Buckets -> Objects->Upload:

index.html (page principale)

index-with-fetch.html

extra-page.html

CORS\_CONFIG.json

coffee.jpg

beach.jpg

.DS\_Store (optionnel, c'est un fichier système Mac)

The screenshot shows the AWS S3 console with a progress bar at the top indicating 'Chargement en cours' (Uploading) at 99%. Below it, a table lists seven files:

Nom	Dossier	Type	Taille	Statut	Erreur
DS_Store	-	-	6.0 Ko	Opération réussie	-
beach.jpg	-	image/jpeg	85.8 Ko	Opération réussie	-
coffee.jpg	-	image/jpeg	108.4 Ko	Opération réussie	-
CORS_CONFIG...	-	application/json	313.0 o	Opération réussie	-
extra-page.h...	-	text/html	69.0 o	En attente	-
index-with-f...	-	text/html	545.0 o	En attente	-
index.html	-	text/html	597.0 o	En attente	-

## Configurez les permissions :

- Dans votre bucket S3, cliquez sur l'onglet "Permissions"
- Trouvez la section "Bucket Policy"
- Cliquez sur "Edit"
- C'est là que vous collez le JSON des permissions

{

    "Version": "2012-10-17",

    "Statement": [

        {

            "Sid": "PublicReadGetObject",

            "Effect": "Allow",

            "Principal": "\*",

        "Action": [

```
    "s3:GetObject"  
],  
  "Resource": [  
    "arn:aws:s3:::NOM-DE-VOTRE-BUCKET/*"  
  ]  
}  
]  
}
```

### **Configurez CORS (nécessaire à cause de index-with-fetch.html) :**

Toujours dans l'onglet "Permissions"

Descendez jusqu'à trouver "Cross-origin resource sharing (CORS)"

Cliquez sur "Edit"

C'est là que vous collez le JSON de configuration CORS

```
[  
  {  
    "AllowedHeaders": ["*"],  
    "AllowedMethods": ["GET"],  
    "AllowedOrigins": ["*"],  
    "ExposeHeaders": []  
  }  
]
```

Qu'est-ce que CORS ?

### **CORS expliqué simplement :**

1. C'est une mesure de sécurité du navigateur

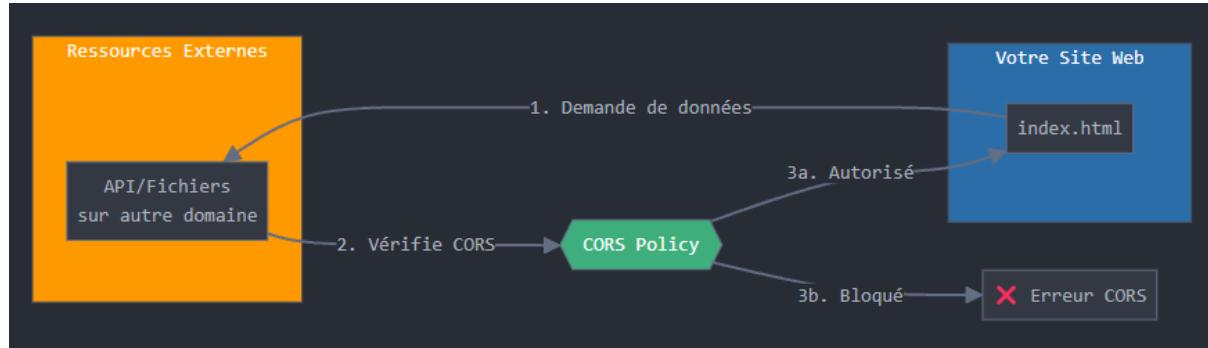
2. Elle contrôle quels sites web peuvent accéder à vos ressources
3. Sans CORS, un site malveillant ne peut pas utiliser vos ressources

### Exemple concret :

- Imaginez votre site comme une maison
- CORS est comme une liste d'invités
- La configuration CORS dit "qui peut entrer"
- Sans bonne configuration = la porte reste fermée

### Pourquoi en avez-vous besoin ?

- Votre fichier `index-with-fetch.html` fait probablement des requêtes
- Ces requêtes doivent être autorisées par CORS
- Sans CORS, ces requêtes seront bloquées par le navigateur



**Une fois configuré, vous aurez une URL du type :**

<http://nom-de-votre-bucket.s3-website.REGION.amazonaws.com>

mon exercice :

<https://laplateforme-dome-bucket-2024.s3.eu-west-3.amazonaws.com/index.html>

**Mise en place du versioning pour le bucket S3 et remplacement du fichier S3.txt**

**Activer le versioning:**

1. Allez dans votre bucket
2. Onglet "Properties"

### 3. Trouvez "Bucket Versioning"

### 4. Cliquez "Edit"

The screenshot shows the 'Bucket Versioning' configuration page. At the top right is an 'Edit' button. Below it, the status is set to 'Disabled'. A note about Multi-factor authentication (MFA) delete is present, stating that it requires MFA for changing settings and deleting versions. The status is also labeled as 'Disabled'.

### 5. Sélectionnez "Enable"

The screenshot shows the 'Edit Bucket Versioning' dialog. The 'Bucket Versioning' section has the 'Enable' radio button selected. A note says: 'After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.' Below this, another note about MFA delete is shown. At the bottom right are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted.

**Edit Bucket Versioning**

**Bucket Versioning**

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

**Bucket Versioning**

**Suspend**  
This suspends the creation of object versions for all operations but preserves any existing object versions.

**Enable**

After enabling Bucket Versioning, you might need to update your lifecycle rules to manage previous versions of objects.

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

**Upload succeeded**

View details below.

The information below will no longer be available after you navigate away from this page

**Summary**

Destination	Status
s3://laplateforme-dome-bucket-2024	Succeeded 1 file, 38.0 B (100.00%)

**Files and folders**

Name	Folder	Type	Size	Status
s3.txt	-	text/plain	38.0 B	Succeeded

### Pour remplacer le fichier S3.txt :

- Uploadez simplement la nouvelle version
- L'ancienne version sera conservée automatiquement
- Vous pouvez voir les versions en :
  - Cliquant sur le fichier
  - Onglet "Versions"

Version ID	Type	Last modified	Size	Storage class
mmrU1wAAhwMuqU61GZuyj...	txt	November 14, 2024, 11:17:57 (UT...)	38.0 B	Standard

## Les différentes classes de stockage S3

Les classes de stockage S3 sont différentes options de stockage proposées par AWS, chacune avec ses propres caractéristiques de prix et de performance

Le choix dépend de trois facteurs principaux :

1. La fréquence d'accès aux données
2. Le temps d'accès acceptable
3. Le budget disponible

## Classes de Stockage Amazon S3

Classe de Stockage	Disponibilité	Temps d'accès	Coût/Go/Mois	Durée minimale	Cas d'usage typique
S3 Standard	99.99%	Instantané	\$0.023	Aucune	Sites web, Applications actives
S3 Intelligent-Tiering	99.9%	Instantané	\$0.0125-0.023	Aucune	Données à accès imprévisible
S3 Standard-IA	99.9%	Millisecondes	\$0.0125	30 jours	Sauvegardes, Données peu consultées
S3 One Zone-IA	99.5%	Millisecondes	\$0.01	30 jours	Données secondaires reproductibles
Glacier Instant	99.9%	Millisecondes	\$0.004	90 jours	Archives à accès rapide
Glacier Flexible	99.99%	Minutes-Heures	\$0.0036	90 jours	Archives à long terme
Glacier Deep	99.99%	12-48 heures	\$0.00099	180 jours	Archives rarement consultées

## JOUR 4 Entra ID ( ex Azure AD )

Après avoir réussi à me connecté avec le compte GitHub, m'enregistrer a Entra ID, l'activation requièrent un carte de crédit, l'inscription met à disposition un crédit de 200€, on peut consulter la facturation à tout moment dans l'onglet suivant :

[Gestion des coûts + facturation | Compte de facturation](#)

### Job 01

#### Création des Groupes :

- Accédez au portail Azure ([portal.azure.com](https://portal.azure.com))
- Dans le menu, cliquez sur "Microsoft Entra ID"
- Sélectionnez "Groupes" dans le menu de gauche
- Cliquez sur "Nouveau groupe" et pour chaque groupe (Amiral, Capitaine, Équipage) :
  - Type de groupe : "Sécurité"
  - Nom du groupe : [Nom]
  - Description : [Description du rôle]
  - Cliquez sur "Créer"

Tous les groupes ...

The screenshot shows the Microsoft Entra ID Groups management interface. At the top, there are navigation links: "Nouveau groupe", "Télécharger des groupes", "Actualiser", "Gérer la vue", "Supprimer", and "Des commentaires ?". Below this is a search bar with "Rechercher" and a filter button "Ajouter un filtre". A note at the top says: "Microsoft Entra offre une expérience plus simple et intégrée pour gérer tous vos besoins de gestion des identités et des accès. Essayez le nouveau Centre d'administration !". The main area displays a table of groups:

<input type="checkbox"/>	Nom ↑	ID d'objet	Type de groupe	Type d'appartenance
<input type="checkbox"/>	A Amiral	1286b72f-9547-429c-b934-abbfc973ca70	Sécurité	Affecté
<input type="checkbox"/>	C Capitaine	57b3ce1c-a1b8-4003-a739-8aaad6ce6cf8	Sécurité	Affecté
<input type="checkbox"/>	É Équipage	b228fb4-ee4e-4b5e-bd59-4b510182b134	Sécurité	Affecté

Plus en détail groupes sécurité les groupes de sécurité sont le meilleur choix car nous nous concentrions uniquement sur la gestion des accès et des rôles, sans besoin de fonctionnalités collaboratives Microsoft 365.

## Job 02

### Configuration préalable Azure pour Entra ID Premium

#### Création du groupe de ressources

Le groupe de ressources est comme un dossier qui contiendra toutes nos ressources pour le projet Star Trek.

*Un groupe de ressources dans Azure est un concept fondamental qu'on peut expliquer avec une analogie simple :*

*Imaginez que vous avez une grande maison (votre abonnement Azure) avec plusieurs pièces (groupes de ressources). Dans chaque pièce, vous rangez des objets spécifiques (ressources Azure) qui sont liés entre eux.*

*Concrètement, un groupe de ressources c'est :*

1. *Un conteneur logique qui permet de :*
  - *Regrouper des ressources liées à un même projet*
  - *Organiser vos services Azure*
  - *Gérer les accès et les permissions*
  - *Suivre les coûts par projet*
2. *Exemples de ressources qu'on peut mettre dans un groupe :*
  - *Machines virtuelles*
  - *Bases de données*
  - *Applications web*
  - *Services de stockage*
  - *etc.*
3. *Avantages principaux :*
  - *Organisation : Tout ce qui concerne un projet est au même endroit*
  - *Gestion des coûts : Vous voyez facilement combien coûte chaque projet*
  - *Sécurité : Vous pouvez donner des accès par groupe*
  - *Nettoyage facile : Supprimer un groupe supprime toutes les ressources qu'il contient*

Étapes de création :

1. Aller sur portal.azure.com
2. Rechercher "Groupes de ressources"
3. Cliquer sur "+ Créer"
4. Remplir :
  - o Abonnement : Votre abonnement étudiant
  - o Nom : "StarTrekProject-rg"
  - o Région : France Central
5. Cliquer sur "Vérifier + créer" puis "Créer"

## Créer un groupe de ressources

[De base](#)   [Étiquettes](#)   [Vérifier + créer](#)

**Groupe de ressources**- Un conteneur qui contient les ressources associées à une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous voulez gérer en tant que groupe. Vous choisissez la façon dont vous voulez allouer des ressources aux groupes de ressources en fonction de ce qui est le plus adapté à votre organisation. [En savoir plus](#)

### Détails du projet

Abonnement *	<input type="text" value="Azure subscription 1"/>
Groupe de ressources *	<input type="text" value="StarTrekProject-rg"/> <span style="color: green;">✓</span>

### Détails de la ressource

Région *	<input type="text" value="(Europe) France Central"/> <span style="color: purple;">▼</span>
----------	--

[Vérifier + créer](#)   [< Précédent](#)   [Suivant : Étiquettes >](#)

## Activation d'Entra ID

Pour pouvoir utiliser les fonctionnalités de gestion d'identités, il faut activer le service :

1. Dans le portail Azure :
  - o Rechercher "Fournisseurs de ressources"
  - o Trouver "Microsoft.AzureActiveDirectory"
  - o Si "Non enregistré", cliquer et sélectionner "S'inscrire"
  - o Attendre quelques minutes

Imaginez Azure comme un grand centre commercial (votre abonnement), et les différents services Azure comme des magasins. Certains magasins sont ouverts par défaut, d'autres doivent être "activés" avant qu'on puisse les utiliser.

L'enregistrement du fournisseur de ressources "Microsoft.AzureActiveDirectory", c'est comme activer votre carte d'accès pour entrer dans une zone spéciale du centre commercial (la zone de gestion des identités).

Pourquoi c'est nécessaire ?

1. Sécurité : Pas tous les abonnements n'ont besoin d'accéder aux services de gestion d'identité
2. Contrôle des coûts : Ça évite d'activer des services qu'on n'utilisera pas
3. Organisation : On active uniquement ce dont on a besoin

Dans notre cas pratique :

- On veut gérer des utilisateurs et des groupes (comme Jean-Luc Picard, etc.)
- Pour ça, on a besoin d'Entra ID (ex Azure AD)
- Donc on doit "activer" cette fonctionnalité dans notre abonnement

C'est comme dire à Azure : "Oui, je veux utiliser le service de gestion des identités dans mon abonnement, merci de l'activer"

2. Lier l'abonnement :

- Retourner dans Entra ID|External Identities
- Sélectionner Abonnement|Abonnements liés
- Dans le menu déroulant "Abonnement", sélectionnez "Azure subscription 1"
- Dans le menu déroulant "Groupe de ressources", sélectionnez le groupe que vous venez de créer "StarTrekProject-rg"
- L'unité de facturation sera automatiquement définie sur MAU (Monthly Active Users)
- Cliquer sur "Appliquer"

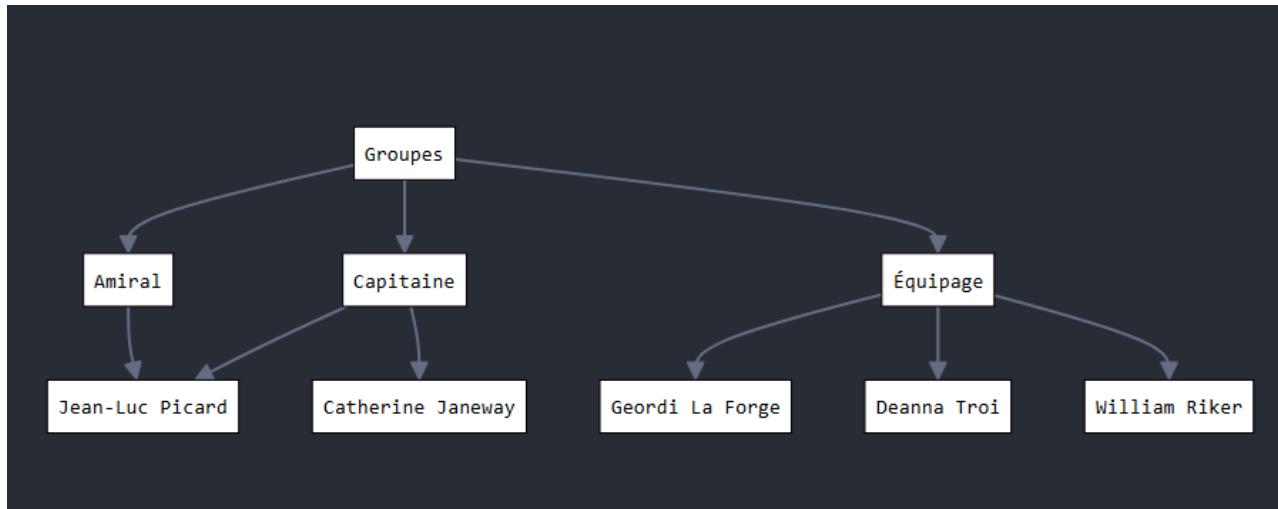
The screenshot shows the 'External Identities | Abonnements liés' (Link subscription) section of the Microsoft Entra ID interface. A warning message states: 'En passant aux tarifs en fonction des utilisateurs actifs mensuels (MAU), vous ne serez plus limité à un ratio de 1:5 pour la licence d'invité Microsoft Entra ID. Enregistrez vos 50 000 premiers MAU gratuitement et payez uniquement pour ce que vous utilisez.' Below this, there's a form to link a subscription to a specific locataire and resource group.

## Important !

Cette configuration est nécessaire pour :

- Créer et gérer les utilisateurs Star Trek (Picard, Janeway, etc.)
- Attribuer les rôles d'administrateur
- Utiliser les fonctionnalités premium d'Entra ID

Une fois ces étapes complétées, nous pourrons passer à la création des utilisateurs et l'attribution des rôles.



## Création des Utilisateurs :

- Dans Entra ID, sélectionnez "Utilisateurs"
- Cliquez sur "Nouvel utilisateur"
- Pour chaque utilisateur :
  - Nom d'utilisateur : [prénom.nom]@[votredomaine].onmicrosoft.com
  - Nom : [Prénom Nom]
  - Mot de passe : Azerty\_\_666!
  - Décochez "L'utilisateur doit changer son mot de passe"

Accueil > la plateforme | Utilisateurs >

## Utilisateurs

Tous les utilisateurs

- Rechercher
- Nouvel utilisateur
- Supprimer
- Téléc...

Créer un utilisateur

Créer un utilisateur interne dans votre organisation

Inviter un utilisateur externe

Inviter un utilisateur externe à collaborer avec votre organisation

Avatar	Nom	Adresse e-mail
CJ	Catherine Janeway	s.janeway@laplatef...
DM	Domenico Mandolino	d.mandolino@lapla...
GL	Geordi La forge	g.laforge@laplatef...
JP	Jean-Luc Picard	j.picard@laplatefor...

## Créer un utilisateur

Créer un utilisateur interne dans votre organisation

### Identité

Nom d'utilisateur principal \*

w.riker

@ laplateforme1302.onmi...



Domaine non répertorié ? [En savoir plus](#)

Pseudonyme de messagerie \*

w.riker

Dériver du nom d'utilisateur principal

Nom d'affichage \*

William Riker

Mot de passe \*

\*\*\*\*\*



Générer automatiquement le mot de passe

Compte activé ⓘ



**Vérifier + créer**

< Précédent

Suivant : Propriétés >

## Créer un utilisateur

Créer un utilisateur interne dans votre organ

Informations de base Propriétés

Faites jusqu'à 20 attributions de groupe

[+ Ajouter une unité administrative](#)

Aucune affectation à afficher

## Sélectionner le groupe

ⓘ Essayez de modifier ou d'ajouter des filtres si vous ne trouvez pas ce que vous cherchez.

Rechercher



3 résultats trouvés

[Tout](#) Groupes

	Nom	Type	Détails
<input type="checkbox"/>	Amiral	Groupe	Amiral@laplatefo
<input type="checkbox"/>	Capitaine	Groupe	Capitaine@laplat
<input checked="" type="checkbox"/>	Équipage	Groupe	equipage@laplat

[Vérifier + créer](#)[Sélectionner](#)

## Créer un utilisateur

...

Créer un utilisateur interne dans votre organisation

### Identité

Nom d'utilisateur principal \*

jl.picard

@ platefor.onmicrosoft.com

Domaine non répertorié ? [En savoir plus](#)

Pseudonyme de messagerie \*

jl.picard

 Dériver du nom d'utilisateur principal

Nom d'affichage \*

Jean-Luc Picard

Mot de passe \*

\*\*\*\*\*

 Générer automatiquement le mot de passeCompte activé ⓘ[Vérifier + créer](#)[Précédent](#)[Suivant : Propriétés >](#)

## Attribution des rôles administratifs dans Entra ID

Structure des rôles par groupe

### Groupe Amiral

Rôles à attribuer :

- Administrateur d'authentification privilégié
- Administrateur de groupes
- Administrateur de mots de passe

The screenshot shows the 'Rôles affectés' (Assigned roles) page for the user 'Jean-Luc Picard'. The left sidebar lists various administrative roles: Vue d'ensemble, Journaux d'audit, Journaux de connexion, Diagnostiquer et résoudre les problèmes, Attributs de sécurité personnalisés, Rôles affectés (which is selected), Unités administratives, Groupes, Applications, Licences, and Appareils. The main content area displays a table of assigned roles:

Rôle	Description	Nom de la ressource	Type de ressource	Chemin d'attribution	Type
<input type="checkbox"/> Administrateur d'authentification	Peut afficher, définir et réinitialiser les informations de méthode d'authentification pour tout utilisateur (administrateur ou non administrateur).	Directory	Organization	Direct	Intégré
<input type="checkbox"/> Administrateur de groupes	Les membres de ce rôle peuvent créer/gérer des groupes, créer/gérer des paramètres de groupes tels que des stratégies de nommage et d'expiration, et afficher l'activité des groupes et les rapports d'audit.	Directory	Organization	Direct	Intégré
<input type="checkbox"/> Administrateur de mots de passe	Peut réinitialiser les mots de passe pour les non-administrateurs et les administrateurs de mot de passe.	Directory	Organization	Direct	Intégré

### Groupe Capitaine

Rôles à attribuer :

- Administrateur d'authentification
- Administrateur de mots de passe

The screenshot shows the Microsoft Entra ID interface for managing assigned roles. The left sidebar includes options like 'Vue d'ensemble', 'Journaux d'audit', 'Journaux de connexion', 'Diagnostiquer et résoudre les problèmes', 'Attributs de sécurité personnalisés', and 'Rôles affectés'. The 'Rôles affectés' option is selected. The main area displays a table of roles:

Rôle	Description	Nom de la ressource	Type de ressource
<input type="checkbox"/> Administrateur d'extensibilité d'authentification	Personnalisez les expériences de connexion et d'inscription pour les utilisateurs en créant et en gérant des extensions d'authentification personnalisées.	Directory	Organization
<input type="checkbox"/> Administrateur de mots de passe	Peut réinitialiser les mots de passe pour les non-administrateurs et les administrateurs de mot de passe.	Directory	Organization

## Étapes d'attribution des rôles

### 1. Accéder aux rôles :

- Dans Entra ID
- Aller dans "Rôles et administrateurs"
- Rechercher le rôle souhaité

### 2. Pour chaque rôle du groupe Amiral :

- Cliquer sur le rôle
- Sélectionner "Ajouter des attributions"
- Rechercher le groupe "Amiral"
- Confirmer l'attribution

### 3. Pour chaque rôle du groupe Capitaine :

- Même procédure que pour Amiral
- Sélectionner le groupe "Capitaine"

## Vérification

Pour vérifier les attributions :

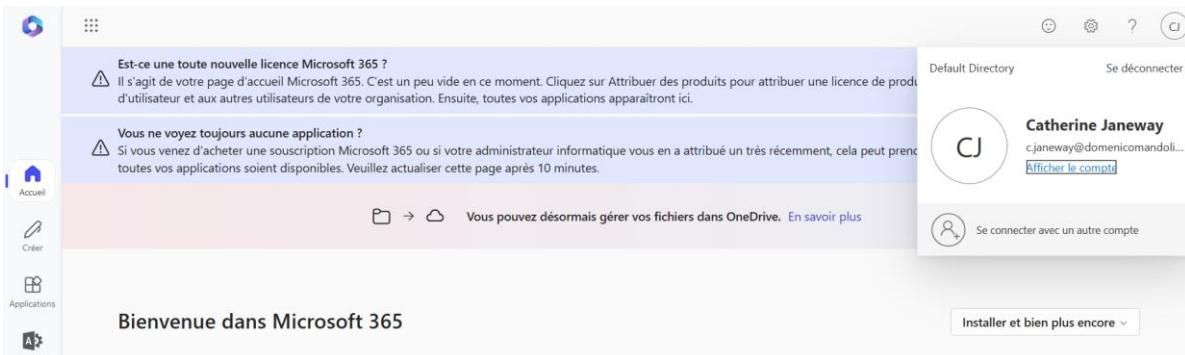
1. Aller dans "Groupes"
2. Sélectionner un groupe
3. Vérifier les "Rôles attribués"

#### Important

- Les rôles sont cumulatifs (Picard aura les rôles Amiral + Capitaine)
- Les permissions sont héritées par tous les membres du groupe
- Les modifications de rôles peuvent prendre quelques minutes pour s'appliquer

## JOB 3

### Essai de connexion aux différents comptes créés



This screenshot is identical to the one above, showing the Microsoft 365 home page with three accounts: Catherine Janeway, Jean-Luc Picard, and Deanna Troi. The layout, messages, and account details are the same.

## JOB 4

### Création de clés SSH dans Azure

#### Création depuis Azure

##### 1. Dans le portail Azure :

- Recherchez "Clés SSH" dans la barre de recherche
- Ou aller dans "Tous les services" > "Clés SSH"

- Cliquez sur "+ Ajouter"

Aucun Clés SSH à afficher  
SSH est un protocole de connexion chiffrée qui permet des connexions sécurisées sur des connexions non sécurisées.  
Les clés SSH permettent une connexion sécurisée aux machines virtuelles, sans utiliser de mots de passe.

[Créer Clé SSH](#) [Envoyer des commentaires](#)

Remplir les informations :

- Nom de la clé "StarTrekProject-Key"
- Groupe de ressources : "StarTrekProject-rg"
- Algorithme : RSA
- Taille : 2048 bits ou 4096 bits
- Cliquez sur "Vérifier + créer"

Nom	Type	Groupe de ressources	Emplacement	Abonnement
StarTrekProject-Key	Clé SSH	StarTrekProject-rg	France Central	Abonnement Azure 1

## Créer une clé SSH

### Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * ⓘ	Abonnement Azure 1
Groupe de ressources * ⓘ	StarTrekProject-rg
	<a href="#">Créer nouveau</a>

### Détails de l'instance

Région ⓘ	(Europe) France Central
Nom de la paire de clés *	StarTrekProject-Key
Source de la clé publique SSH	Générer une nouvelle paire de clés
Type de clé SSH	<input checked="" type="radio"/> Format SSH RSA <input type="radio"/> Format SSH Ed25519

**Ed25519 offre un meilleur niveau de performance et une meilleure sécurité avec une taille de clé plus petite, tandis que RSA est toujours largement utilisé, en particulier pour les systèmes et applications hérités.**

[Vérifier + créer](#)

[< Précédent](#)

[Suivant : Étiquettes >](#)

## Création depuis votre PC

### 1. Pour Windows (avec PowerShell) :

```
```powershell
```

```
ssh-keygen -t rsa -b 4096
```

```
```
```

### Pour Linux/MacOS (Terminal) :

```
```bash
```

```
ssh-keygen -t rsa -b 4096
```

```
```
```

Importation dans Azure :

- Copiez le contenu de la clé publique (.pub)
- Dans Azure, créez une nouvelle clé SSH
- Collez le contenu de votre clé publique

Points importants

- Conservez votre clé privée en sécurité
- La clé publique sera utilisée dans le Job 5 pour la VM
- Ne partagez jamais votre clé privée

## **JOB 5**

### **Création d'une VM Debian dans Azure**

#### **1. Création de la VM**

1. Dans le portail Azure :

- Recherchez "Machines virtuelles"
- Cliquez sur "+ Créer"
- Choisissez "Machine virtuelle Azure"

2. Configuration de base :

- Groupe de ressources : StarTrekProject-rg
- Nom de la machine : Debian-StarTrek
- Région : France Central

## Créer une machine virtuelle

M'aider à créer une machine virtuelle à faible coût    M'aider à créer une machine virtuelle optimisée pour la haute disponibilité    M'aider à créer une machine virtuelle avec une sécurité renforcée

**Détails du projet**

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement \* ⓘ    Abonnement Azure 1

Groupe de ressources \* ⓘ    StarTrekProject-rg    Créez nouveau

**Détails de l'instance**

Nom de la machine virtuelle \* ⓘ    Debian-StarTrek

Région \* ⓘ    (Europe) France Central

Options de disponibilité ⓘ    Zone de disponibilité

Options de zone ⓘ

Zone autosélectionnée  
Choisissez jusqu'à 3 zones de disponibilité, une machine virtuelle par zone

Zone sélectionnée par Azure (préversion)

< Précédent    Suivant : Disques >    Vérifier + créer

- Image : Debian (dernière version)
- Taille : Standard\_B1s (suffisant pour les tests)

Type de sécurité ⓘ    Lancer des machines virtuelles approuvées    Configurer les fonctionnalités de sécurité

Image \* ⓘ    Debian 12 "Bookworm" - x64 de 2e génération    Voir toutes les images | Configurer la génération de machine virtuelle

Architecture de machine virtuelle ⓘ     x64     Arm64

Exécuter avec la remise Azure Spot ⓘ   

Taille \* ⓘ    Standard\_B1s - 1 processeur virtuel, 1 Gio de mémoire (8,61 \$US/mois) (acc...    Voir toutes les tailles

Activer la mise en veille prolongée ⓘ      
Actuellement, la mise en veille prolongée ne prend pas en charge le lancement fiable et les machines virtuelles confidentielles pour les images Linux.  
[En savoir plus](#)

< Précédent    Suivant : Disques >    Vérifier + créer

### 3. Compte administrateur :

- Nom d'utilisateur : azureuser
- Type d'authentification : Clé publique SSH

## - Utiliser la clé SSH créée au Job 4

### Compte d'administrateur

Type d'authentification (1)

Clé publique SSH

Mot de passe

i Désormais, Azure génère automatiquement une paire de clés SSH et vous permet de la stocker pour pouvoir l'utiliser par la suite. Il s'agit d'un moyen rapide, simple et sécurisé de vous connecter à votre machine virtuelle.

Nom d'utilisateur \* (1)

azureuser ✓

Source de la clé publique SSH

Utiliser la clé existante stockée dans Azure ✓

i Les formats Ed25519 et RSA SSH sont pris en charge pour l'image de machine virtuelle sélectionnée. Ed25519 offre un meilleur niveau de performance et une meilleure sécurité avec une taille de clé plus petite, tandis que RSA est toujours largement utilisé, en particulier pour les systèmes et applications hérités.

Clés stockées

StarTrekProject-Key ✓

## 4. Ports d'entrée :

### - Autoriser SSH (port 22)

#### Règles des ports d'entrée

Sélectionnez les ports réseau de machine virtuelle accessibles publiquement à partir d'Internet. Vous pouvez spécifier un accès réseau plus limité ou granulaire sous l'onglet Mise en réseau.

Ports d'entrée publics \* (1)

Aucun

Autoriser les ports sélectionnés

Sélectionner des ports d'entrée \*

SSH (22) ✓

i Tout le trafic en provenance d'Internet sera bloqué par défaut. Vous pouvez changer les règles de port d'entrée dans la page Machine virtuelle > Mise en réseau.

## 5. Création du réseau virtuel

### 1. Pendant la création de la VM, dans l'onglet "Réseau" :

- Dans "Réseau virtuel", cliquez sur "Créer nouveau"
- Nom : StarTrek-vnet
- Plage d'adresses : 10.0.0.0/16 (par défaut)
- Sous-réseau :
  - Nom : default
  - Plage d'adresses : 10.0.0.0/24

# Créer un réseau virtuel

Le service Réseau virtuel Microsoft Azure permet aux ressources Azure de communiquer entre elles, qui est une isolation logique du cloud Azure dédiée à votre abonnement. Vous pouvez connecter vos réseaux virtuels ou à votre réseau local. [En savoir plus](#)

Nom \* StarTrek-vnet

## Espace d'adressage

Espace d'adressage du réseau virtuel, spécifié sous la forme d'un ou plusieurs préfixes d'adresse (par exemple 192.168.1.0/24).

| Plage d'adresses *                              | Adresses                                 | Chevauchement |
|---|--|---------------|
| <input checked="" type="checkbox"/> 10.0.0.0/16 | 10.0.0.0 - 10.0.255.255 (65536 adresses) | Aucun         |
|   | (0 adresses)                             | Aucun         |

## 2. Configuration des ports :

- Groupe de sécurité réseau : "Basic"
- Ports d'entrée publics : Autoriser SSH (22)
- Ne pas ajouter d'autres ports pour l'instant

## Interface réseau

Quand vous créez une machine virtuelle, une interface réseau est créée pour vous.

|  |   |
|--|---|
| Réseau virtuel *                             | <input type="text" value="(nouveau) StarTrek-vnet"/>  |
|  | <a href="#">Créer</a>   |
| Sous-réseau *                                | <input type="text" value="(nouveau) default (10.0.0.0/24)"/>  |
| Adresse IP publique                          | <input type="text" value="(nouveau) Debian-StarTrek-ip"/>   |
| Groupe de sécurité réseau de la carte réseau | <input type="radio"/> Aucun<br><input checked="" type="radio"/> De base<br><input type="radio"/> Paramètres avancés |
| Ports d'entrée publics *                     | <input type="radio"/> Aucun<br><input checked="" type="radio"/> Autoriser les ports sélectionnés                    |
| Sélectionner des ports d'entrée *            | <input type="text" value="SSH (22)"/>   |

**⚠ Cela permet à toutes les adresses IP d'accéder à votre machine virtuelle.**  
Ceci est recommandé uniquement pour les tests. Utilisez les contrôles avancés de l'onglet **Avancé** en réseau pour créer des règles afin de limiter le trafic entrant

Vue d'ensemble

Le déploiement est en cours

Nom du déploiement : CreateVm-debian.debian-12-12-gen2-20241219213312 | Heure de début : 19/12/2024 21:43:02  
Abonnement : Abonnement Azure 1 | ID de corrélation : 9d1546d3-b015-4f62-bb7e-977694dac9d5

| Ressource             | Type                                    | Statut  | Détails de l'opération                 |
|-----------------------|---|---------|--|
| Debian-StarTrek       | Microsoft.Compute/virtualMachines       | Created | <a href="#">Détails de l'opération</a> |
| debian-startrek504_z1 | Microsoft.Network/networkInterfaces     | Created | <a href="#">Détails de l'opération</a> |
| Debian-StarTrek-nsg   | Microsoft.Network/networkSecurityGroups | OK      | <a href="#">Détails de l'opération</a> |
| Debian-StarTrek-ip    | Microsoft.Network/publicIPAddresses     | OK      | <a href="#">Détails de l'opération</a> |
| StarTrek-vnet         | Microsoft.Network/virtualNetworks       | OK      | <a href="#">Détails de l'opération</a> |

Envoyer des commentaires

Partagez votre expérience avec le déploiement

## 2. Connexion à la VM

### 1. Depuis Windows (PowerShell) :

```
```bash
```

```
ssh -i chemin/vers/votre/cle_privee azureuser@IP_DE_LA_VM
```

```
```
```

### 3. Depuis Linux/MacOS :

```
```bash
```

```
ssh -i ~/.ssh/id_rsa azureuser@IP_DE_LA_VM
```

```
```
```

## Points importants

- Notez l'adresse IP publique de votre VM
- Vérifiez que le port 22 (SSH) est ouvert dans le groupe de sécurité réseau
- La première connexion demandera de confirmer l'authenticité du serveur

Accueil > Debian-StarTrek

## Debian-StarTrek | Connexion

Machine virtuelle

Rechercher

Connexion via  
Adresse IP publique | 4.233.144.221

Nom d'utilisateur de l'administrateur  
azureuser

Port (modifier)  
22 [Vérifier l'accès](#)

Stratégie juste-à-temps  
Non pris en charge par le plan

Recommandé

Ordinateur local Portail Azure

SSH utilisant Azure CLI

Connectez-vous rapidement dans le navigateur. Prend en charge l'authentification Microsoft Entra ID. La clé privée n'est pas obligatoire.

Adresse IP publique (4.233.144.221)

Sélectionner

**1 Configurer les prérequis pour SSH utilisant Azure CLI**

Azure doit configurer quelques fonctionnalités pour se connecter à la machine virtuelle.

**Configuration des prérequis**

- Identité managée affectée par le système Configuration de l'identité managée affectée par le système. [En savoir plus](#)
- Extension de connexion SSH Microsoft Entra ID Installation de l'extension de connexion SSH basée sur Microsoft Entra ID. [En savoir plus](#)
- Connexion de l'administrateur ou de l'utilisateur de la machine virtuelle Un rôle de connexion administrateur de machine virtuelle sur le groupe de ressources autorise la connexion à la machine virtuelle via CloudShell. [En savoir plus](#)
- Accès au port 22 Le port 22 est accessible sur cette machine virtuelle pour toutes les adresses IP configurées. [En savoir plus](#)
  - Modifiez le port de connexion à cet ordinateur virtuel sur la page Connexion de la machine virtuelle.
- Adresse IP publique : 4.233.144.221 Une adresse IP publique est nécessaire pour se connecter via cette méthode de connexion.

Je comprends que la stratégie juste-à-temps sur la machine virtuelle peut être reconfigurée pour permettre à n'importe quelle adresse IP source de demander un accès juste-à-temps au port 22.

Configuration en cours...

Fermer Résolution des problèmes Envoyer des commentaires

### Prise en main

Selectionnez un abonnement pour démarrer. Vous pouvez éventuellement monter un compte de stockage pour conserver les fichiers entre les sessions. [En savoir plus](#)

Aucun compte de stockage requis

Monter le compte de stockage

Abonnement \*

Abonnement Azure 1

Utiliser un réseau virtuel privé existant [En savoir plus](#)

Appliquer Précédent

```

-6fb76e73a3ce
MOTD: SqlServer has been updated to Version 22!
VERBOSE: Authenticating to Azure ...
OpenSSH_8.9p1, OpenSSL 1.1.1k FIPS 25 Mar 2021
The authenticity of host '4.233.144.221 (4.233.144.221)' can't be established.
ED25519 key fingerprint is SHA256:Qvoaadpq9+TrJ0O50bfJ8cYOMvhZFYQ7xsTykfeDs2M.
This key is not known by any other naaz ssh vm --resource-group StarTrekProject-rg --vm-name Debian-StarTrek --subscription b012ecb6-f95
3-4052-bbc4-6fb76e73a3ce continue connecting (yes/no/[fingerprint])? VERBOSE: Building your Azure drive ...
^[[13;10ROpenSSH_8.9p1, OpenSSL 1.1.1k FIPS 25 Mar 2021e-group StarTrekProject-rg --vm-name Debian-StarTrek --subscription b012ecb6-f95
The authenticity of host '4.233.144.221 (4.233.144.221)' can't be established.
ED25519 key fingerprint is SHA256:Qvoaadpq9+TrJ0O50bfJ8cYOMvhZFYQ7xsTykfeDs2M.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?■

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Last login: Thu Dec 19 21:26:15 2024 from 57.153.252.19
$ ipconfig
$ sh: 1: ipconfig: not found
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 60:45:bd:6d:4f:25 brd ff:ff:ff:ff:ff:ff
        inet 10.0.0.4/24 metric 100 brd 10.0.0.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::6245:bdff:fe6d:4f25/64 scope link
            valid_lft forever preferred_lft forever

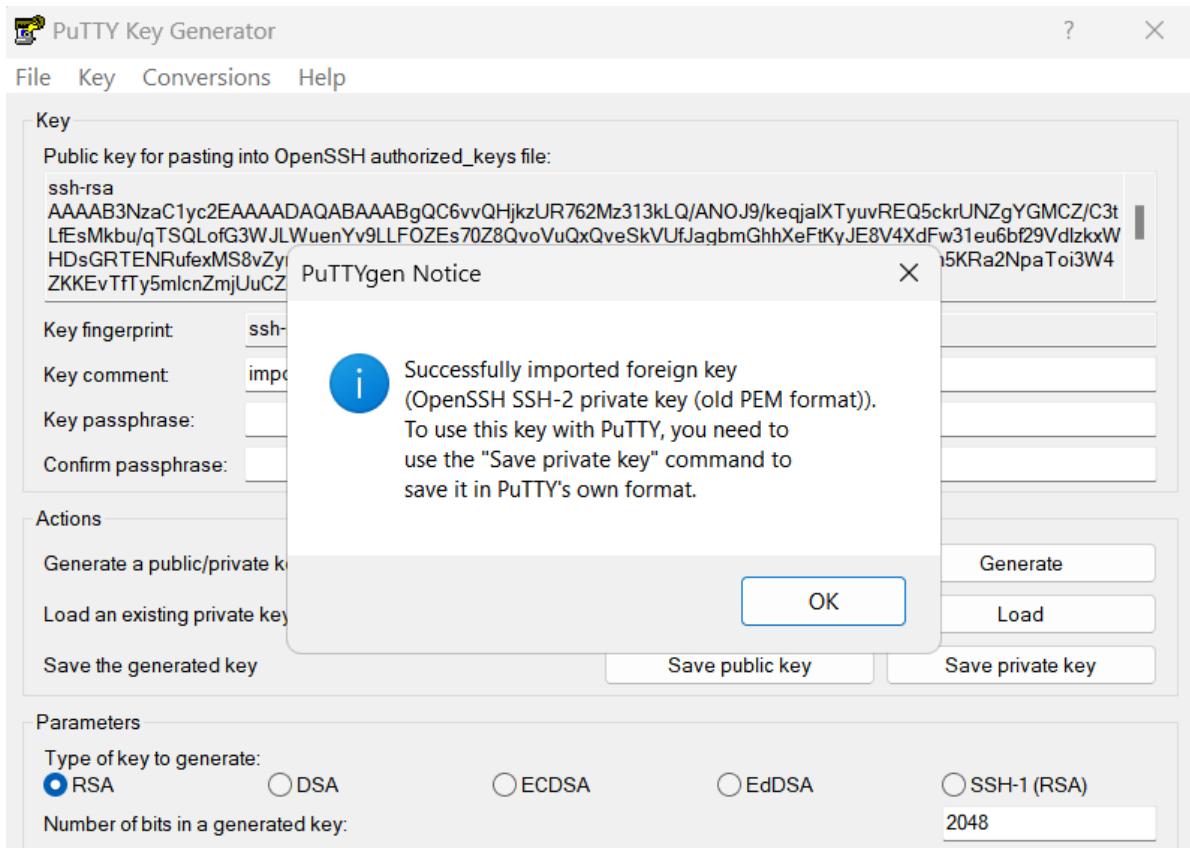
```

## Guide de connexion à la VM Azure avec PuTTY

### 1. Préparer la clé pour PuTTY

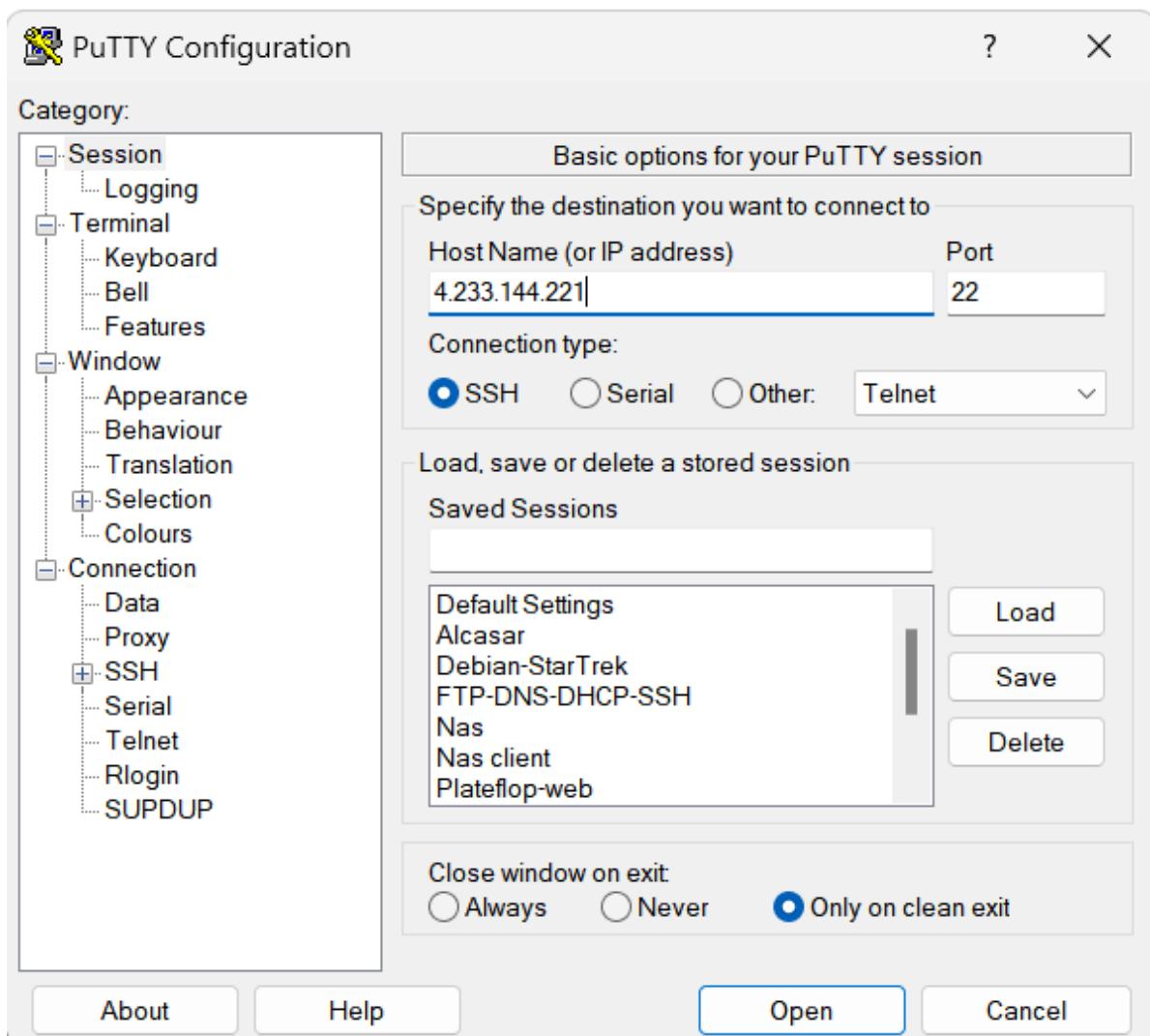
Si vous avez une clé SSH au format .pem ou OpenSSH :

1. Ouvrez PuTTYgen (installé avec PuTTY)
2. Cliquez sur "Load"
3. Sélectionnez votre clé privée
4. Cliquez sur "Save private key"
5. Sauvegardez au format .ppk (format PuTTY)



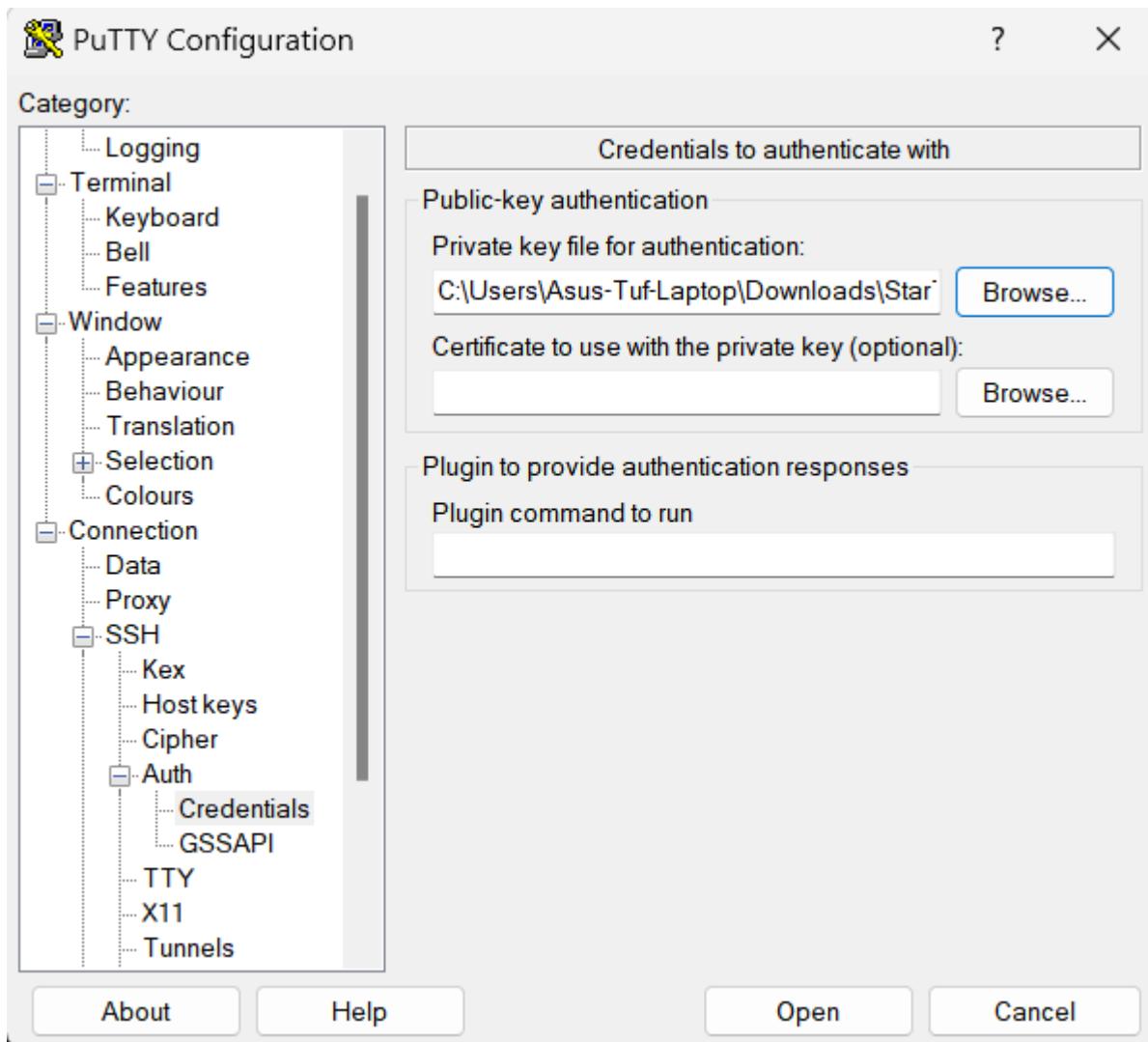
## 2. Configuration de PuTTY

1. Ouvrez PuTTY
2. Configuration de base :
  - o Dans "Host Name" : azureuser@VOTRE\_IP\_VM
  - o Port : 22
  - o Connection type : SSH



### 3. Configuration de la clé SSH :

- Dans le menu de gauche, allez à :
  - Connection > SSH > Auth > Credentials
- Cliquez sur "Browse"
- Sélectionnez votre fichier .ppk



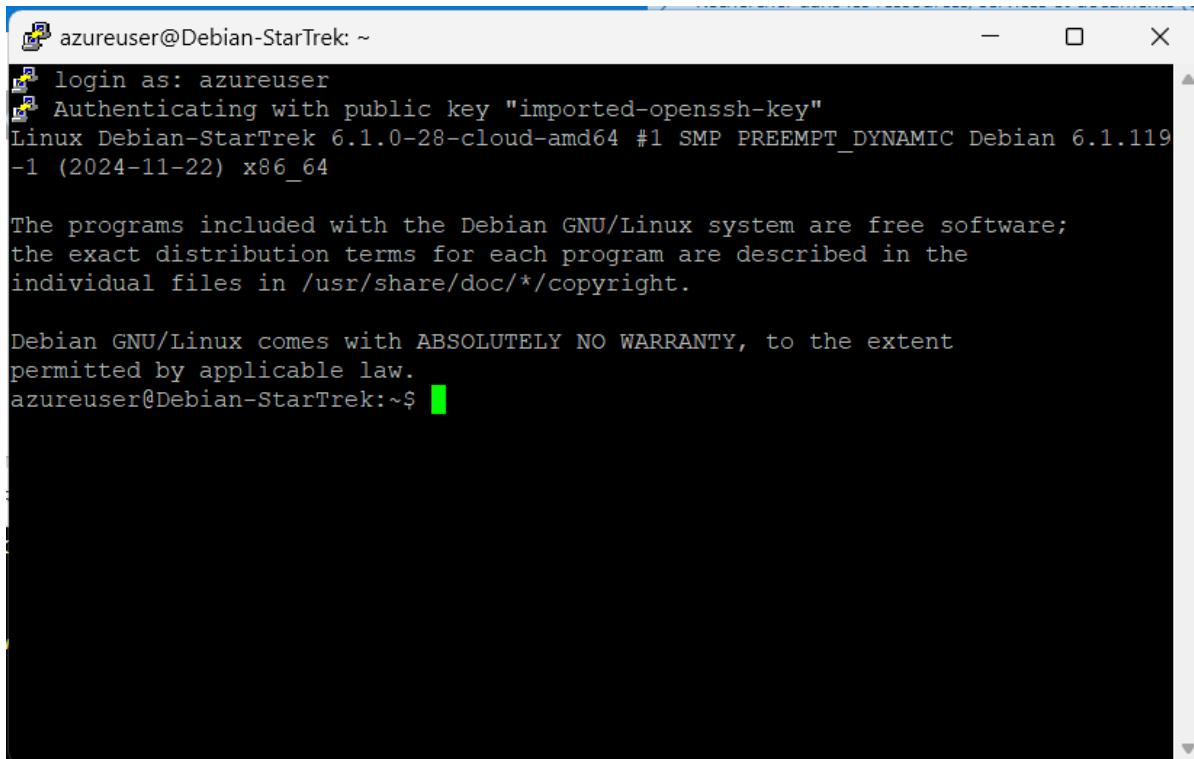
4. Sauvegarder la session (optionnel) :
  - Retournez à "Session" dans le menu
  - Entrez un nom dans "Saved Sessions"
  - Cliquez "Save"

### 3. Se connecter

1. Cliquez sur "Open"
2. Acceptez l'alerte de sécurité lors de la première connexion
3. Vous devriez maintenant être connecté à votre VM

### Résolution des problèmes courants

- Si "Access Denied" : Vérifiez que vous utilisez le bon nom d'utilisateur
- Si "Connection Refused" : Vérifiez que le port 22 est ouvert dans Azure
- Si "Network Error" : Vérifiez l'adresse IP et votre connexion internet



A screenshot of a terminal window titled "azureuser@Debian-StarTrek: ~". The window shows a standard Linux login sequence:

```
azureuser@Debian-StarTrek: ~
login as: azureuser
Authenticating with public key "imported-openssh-key"
Linux Debian-StarTrek 6.1.0-28-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
azureuser@Debian-StarTrek:~$
```

## JOB 6

### Nettoyage des ressources Azure

Ressources à supprimer

#### 1. Machine Virtuelle :

- Dans le portail Azure, allez à "Machines virtuelles"
- Sélectionnez Debian-StarTrek
- Cliquez sur "Supprimer"
- Cette action supprimera aussi :
  - \* Le disque OS
  - \* L'interface réseau
  - \* L'IP publique

Machines virtuelles

Default Directory (domaine.com\domaine\platefor.onmicrosoft.com)

+ Créer ✎ Passer au mode classique Réservations Gérer la vue Actualiser Exporter au format CSV Ouvrir une requête Attribuer des étiquettes Démarrer Redémarrer Arrêter Supprimer Services ...

Filtrer un champ... Abonnement égal à tout Type égal à tout Groupe de ressources égal à tout Emplacement égal à tout Ajouter un filtre

Aucun regroupement Vue liste

Affichage de 1 à 1 sur 1 enregistrements.

| Nom             | Abonnement         | Groupe de ressources | Emplacement    | État                 | Système d'exploitation | Taille       | Adresse IP publique | Disques |
|-----------------|--------------------|----------------------|----------------|----------------------|------------------------|--------------|---------------------|---------|
| Debian-StarTrek | Abonnement Azure 1 | StarTrekProject-rg   | France Central | En cours d'exécution | Linux                  | Standard_B1s | 4.233.144.221       |         |

Épingler au tableau de bord Ajouter aux favorisModifier les étiquettesOuvrir sur l'appareil mobileDémarrerRedémarrerArrêterSupprimer

## 2. Réseau Virtuel :

- Allez à "Réseaux virtuels"
- Sélectionnez StarTrek-vnet
- Supprimez-le

## 3. Clés SSH :

- Supprimez les clés SSH créées dans Azure
- Gardez vos clés locales si besoin futur

## Éléments à conserver

- Les utilisateurs créés (Picard, Janeway, etc.)
- Les groupes (Amiral, Capitaine, Équipage)
- Les attributions de rôles

## Vérification des coûts

### 1. Dans le portail Azure :

- Allez dans "Cost Management + Billing"
- Vérifiez "Cost analysis"
- Examinez les coûts par ressource

## Important

- Vérifiez que toutes les ressources sont bien supprimées
- Gardez une trace des coûts pour votre documentation
- Conservez les configurations des utilisateurs/groupes pour une utilisation future

## JOUR 5 Enterprise Azure

### JOB 1 Crédit d'infrastructure

Pour exécuter ces commandes :

- 1. Ouvrez Cloud Shell dans le portail Azure (icône > en haut)**
- 2. Assurez-vous d'être en mode Bash (pas PowerShell)**
- 3. Créez un fichier script :**

```
nano create_vms.sh
```

- 4. Copiez ce contenu dans le fichier :**

```
#!/bin/bash
```

```
# Définition des variables
```

```
RESOURCE_GROUP="StarTrekVMs-rg"
```

```
LOCATION="francecentral"

VNET_NAME="StarTrek-vnet"

VM1_NAME="Enterprise-VM1"

VM2_NAME="Enterprise-VM2"

echo "Création du groupe de ressources..."

az group create --name $RESOURCE_GROUP --location $LOCATION

echo "Création du réseau virtuel..."

az network vnet create \
    --resource-group $RESOURCE_GROUP \
    --name $VNET_NAME \
    --address-prefix 10.0.0.0/16 \
    --subnet-name default \
    --subnet-prefix 10.0.0.0/24

echo "Création de la première VM..."

az vm create \
    --resource-group $RESOURCE_GROUP \
    --name $VM1_NAME \
    --image Debian:debian-12:12:latest \
    --admin-username azureuser \
    --generate-ssh-keys \
    --public-ip-sku Standard \
    --size Standard_B1s \
    --vnet-name $VNET_NAME \
    --subnet default
```

```
echo "Création de la deuxième VM..."  
  
az vm create \  
    --resource-group $RESOURCE_GROUP \  
    --name $VM2_NAME \  
    --image Debian:debian-12:12:latest \  
    --admin-username azureuser \  
    --generate-ssh-keys \  
    --public-ip-sku Standard \  
    --size Standard_B1s \  
    --vnet-name $VNET_NAME \  
    --subnet default  
  
echo "Affichage des IPs publiques..."  
  
az vm list-ip-addresses --resource-group $RESOURCE_GROUP --output table
```

#### 4. Rendez le script exécutable :

```
chmod +x create_vms.sh
```

#### 5. Exédez le script :

```
./create_vms.sh
```

```

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
domenico_mandolino [ ~ ]$ nano create_vms.sh
domenico_mandolino [ ~ ]$ chmod +x create_vms.sh
domenico_mandolino [ ~ ]$ ./create_vms.sh
Création du groupe de ressources...
{
  "id": "/subscriptions/b012ecb6-f953-4052-bbc4-6fb76e73a3ce/resourceGroups/StarTrekVMs-rg",
  "location": "francecentral",
  "managedBy": null,
  "name": "StarTrekVMs-rg",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": "Microsoft.Resources/resourceGroups"
}
Création du réseau virtuel...
{
  "newVNet": {
    "addressSpace": {
      "addressPrefixes": [
        "10.0.0.0/16"
      ]
    },
    "enableDdosProtection": false,
    "etag": "W/"5ea47162-dcc6-4159-bd52-f76c2a25d71a\""
  }
}
Création de la première VM...
Selecting "northeurope" may reduce your costs. The region you've selected may cost more for the same services. You can disable this message in the future with the command "az config set core.display_region_identified=false". Learn more at https://go.microsoft.com/fwlink/?linkid=222571
/usr/lib64/az/lib/python3.9/site-packages/paramiko/pkey.py:100: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in 48.0.0.
  "cipher": algorithms.TripleDES,
/usr/lib64/az/lib/python3.9/site-packages/paramiko/transport.py:259: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from this module in 48.0.0.
  "class": algorithms.TripleDES,
SSH key files '/home/domenico_mandolino/.ssh/id_rsa' and '/home/domenico_mandolino/.ssh/id_rsa.pub' have been generated under ~/.ssh to allow SSH access to the VM. If using machines without permanent storage, back up your keys to a safe location.
Consider upgrading security for your workloads using Azure Trusted Launch VMs. To know more about Trusted Launch, please visit https://aka.ms/TrustedLaunch.
[]/ Running ...

```

```

Consider upgrading security for your workloads using Azure Trusted Launch VMs. To know more about Trusted Launch, please visit https://aka.ms/TrustedLaunch.
{
  "fqdns": "",
  "id": "/subscriptions/b012ecb6-f953-4052-bbc4-6fb76e73a3ce/resourceGroups/StarTrekVMs-rg/providers/Microsoft.Compute/virtualMachines/Enterprise-VM2",
  "location": "francecentral",
  "macAddress": "00-0D-3A-89-AA-78",
  "powerstate": "VM running",
  "privateIpAddress": "10.0.0.5",
  "publicIpAddress": "4.211.129.248",
  "resourceGroup": "StarTrekVMs-rg",
  "zones": ""
}
Affichage des IPs publiques...
VirtualMachine   PublicIPAddresses   PrivateIPAddresses
-----
Enterprise-VM1  4.211.129.11          10.0.0.4
Enterprise-VM2  4.211.129.248         10.0.0.5
domenico_mandolino [ ~ ]$ []

```

## Points importants :

- Les VMs seront créées avec une IP publique par défaut
- Les clés SSH seront générées automatiquement
- Nous utilisons la taille Standard\_B1s qui est économique
- Le nom d'utilisateur par défaut est 'azureuser'

## JOB 2 Nettoyage des anciens utilisateurs

### Créez le fichier :

*nano delete\_users.sh*

### Copiez le contenu du script:

```
#!/bin/bash
```

```
# Liste des utilisateurs à supprimer

USERS_TO_DELETE=(

    "jean-luc.picard"
    "catherine.janeway"
    "geordi.laforge"
    "deanna.troi"
    "william.riker"

)

# Boucle pour supprimer chaque utilisateur

for user in "${USERS_TO_DELETE[@]}"

do

    echo "Suppression de l'utilisateur : $user"

    # Récupérer l'ID de l'utilisateur

    USER_ID=$(az ad user list --filter "userPrincipalName eq '$user@votredomaine.onmicrosoft.com'" --query [].id -o tsv)

    if [ ! -z "$USER_ID" ]

        then

            # Supprimer l'utilisateur

            az ad user delete --id $USER_ID

            echo "Utilisateur $user supprimé avec succès"

        else

            echo "Utilisateur $user non trouvé"

    fi

done
```

```
fi
```

```
done
```

```
echo "Vérification des utilisateurs restants..."
```

```
az ad user list --output table
```

Modifiez les noms d'utilisateurs selon vos besoins

**Rendez le script exécutable :**

```
chmod +x delete_users.sh
```

**Exécutez le script :**

```
./delete_users.sh
```

```
domenico_mandolino [ ~ ]$ nano delete_users.sh
domenico_mandolino [ ~ ]$ chmod +x delete_users.sh
domenico_mandolino [ ~ ]$ ./delete_users.sh
Suppression de l'utilisateur : jean-luc.picard
utilisateur jean-luc.picard non trouvé
Suppression de l'utilisateur : catherine.janeway
utilisateur catherine.janeway non trouvé
Suppression de l'utilisateur : geordi.laforge
utilisateur geordi.laforge non trouvé
Suppression de l'utilisateur : deanna.troi
utilisateur deanna.troi non trouvé
Suppression de l'utilisateur : william.riker
utilisateur william.riker non trouvé
Vérification des utilisateurs restants...
+-----+-----+-----+
| DisplayName | UserPrincipalName | GivenName | PreferredLanguage | Surname |
+-----+-----+-----+
Catherine Janeway	c.janeway@domenicomandolinolaplatefor.onmicrosoft.com		en	mandolino
Deanna Troi	d.troi@domenicomandolinolaplatefor.onmicrosoft.com			
d.mandolino	d.mandolino@domenicomandolinolaplatefor.onmicrosoft.com	domenico	en	mandolino
Geordi La forge	g.laforge@domenicomandolinolaplatefor.onmicrosoft.com			
Jean-Luc Picard	jl.picard@domenicomandolinolaplatefor.onmicrosoft.com			
William Riker	w.riker@domenicomandolinolaplatefor.onmicrosoft.com			
+-----+-----+-----+
```

## JOB 3 Nouvelle configuration des groupes

**Créez le fichier :**

```
nano create_star trek_users.sh
```

**Copiez le contenu du script:**

```
#!/bin/bash

# Définition du domaine

DOMAIN=$(az rest --method get --url 'https://graph.microsoft.com/v1.0/domains' --
query 'value[?isDefault].id' -o tsv)

echo "Création des groupes..."

# Création du groupe Amiral

az ad group create --display-name "Amiral" \
    --mail-nickname "amiral" \
    --description "Groupe des Amiraux de Starfleet"

# Création du groupe Capitaine

az ad group create --display-name "Capitaine" \
    --mail-nickname "capitaine" \
    --description "Groupe des Capitaines de Starfleet"

echo "Création des utilisateurs..."

# Création de Jean-Luc Picard

az ad user create --display-name "Jean-Luc Picard" \
    --user-principal-name "jean-luc.picard@$DOMAIN" \
    --password "Azerty__666!" \
    --force-change-password-next-login false

# Création de William Riker
```

```
az ad user create --display-name "William Riker" \  
    --user-principal-name "william.riker@$DOMAIN" \  
    --password "Azerty__666!" \  
    --force-change-password-next-login false
```

# Création de Catherine Janeway

```
az ad user create --display-name "Catherine Janeway" \  
    --user-principal-name "catherine.janeway@$DOMAIN" \  
    --password "Azerty__666!" \  
    --force-change-password-next-login false
```

echo "Attribution des utilisateurs aux groupes..."

# Ajout de Picard au groupe Amiral

```
PICARD_ID=$(az ad user list --filter "displayName eq 'Jean-Luc Picard" --query  
[].id -o tsv)
```

```
AMIRAL_ID=$(az ad group list --filter "displayName eq 'Amiral'" --query [].id -o tsv)
```

```
az ad group member add --group $AMIRAL_ID --member-id $PICARD_ID
```

# Ajout de Riker et Janeway au groupe Capitaine

```
CAPITAINE_ID=$(az ad group list --filter "displayName eq 'Capitaine'" --query [].id -  
o tsv)
```

```
RIKER_ID=$(az ad user list --filter "displayName eq 'William Riker'" --query [].id -o  
tsv)
```

```
JANEWAY_ID=$(az ad user list --filter "displayName eq 'Catherine Janeway'" --  
query [].id -o tsv)
```

```
az ad group member add --group $CAPITAINE_ID --member-id $RIKER_ID
```

```
az ad group member add --group $CAPITaine_ID --member-id $JANEWAY_ID
```

```
echo "Vérification des groupes et leurs membres..."
```

```
echo "Membres du groupe Amiral:"
```

```
az ad group member list --group $AMIRAL_ID --query "[].displayName" -o table
```

```
echo "Membres du groupe Capitaine:"
```

```
az ad group member list --group $CAPITaine_ID --query "[].displayName" -o table
```

**Rendez le script exécutable :**

```
chmod +x create_startrek_users.sh
```

**Exécutez le script :**

```
./create_startrek_users.sh
```

**Points importants :**

- Le script récupère automatiquement votre domaine
- Crée les deux groupes demandés
- Crée les utilisateurs avec le mot de passe spécifié
- Attribue les utilisateurs aux groupes appropriés
- Vérifie les attributions à la fin

```
domenico_mandolino [ ~ ]$ nano create_startrek_users.sh
domenico_mandolino [ ~ ]$ chmod +x create_startrek_users.sh
domenico_mandolino [ ~ ]$ ^[[200~/create_startrek_users.sh~
bash: ./create_startrek_users.sh: No such file or directory
domenico_mandolino [ ~ ]$ ./create_startrek_users.sh
Création des groupes...
{
    "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#groups/$entity",
    "classification": null,
    "createdDateTime": "2024-12-19T23:45:05Z",
    "creationOptions": [],
    "deletedDateTime": null,
    "description": "Groupe des Amiraux de Starfleet",
    "displayName": "Amiral",
    "expirationDateTime": null,
    "groupTypes": [],
    "id": "a425dc60-e2a3-443f-aa70-22265bed3a41",
    "isAssignableToRole": null,
    "mail": null,
    "mailEnabled": false,
    "mailNickname": "amiral",
    "membershipRule": null,
    "membershipRuleProcessingState": null,
    "onPremisesDomainName": null,
    "onPremisesLastSyncDateTime": null,
    "onPremisesNetBiosName": null,
    "onPremisesProvisioningErrors": [],
    "onPremisesSamAccountName": null,
    "onPremisesSecurityIdentifier": null,
```

```
Création des utilisateurs...
unrecognized arguments: --force-change-password-next-login false

Examples from AI knowledge base:
az ad user create --display-name mydisplay --password {password} --user-principal-name myuserprincipal
Create an Azure Active Directory user. (autogenerated)

az ad user create --display-name mydisplay --force-change-password-next-login true --password {password} --user-principal-name myuserprincipal
Create an Azure Active Directory user. (autogenerated)

https://docs.microsoft.com/en-US/cli/azure/ad/user#az\_ad\_user\_create
Read more about the command in reference docs
unrecognized arguments: --force-change-password-next-login false

Examples from AI knowledge base:
az ad user create --display-name mydisplay --password {password} --user-principal-name myuserprincipal
Create an Azure Active Directory user. (autogenerated)

az ad user create --display-name mydisplay --force-change-password-next-login true --password {password} --user-principal-name myuserprincipal
Create an Azure Active Directory user. (autogenerated)

https://docs.microsoft.com/en-US/cli/azure/ad/user#az\_ad\_user\_create
Read more about the command in reference docs
unrecognized arguments: --force-change-password-next-login false
```

```
https://docs.microsoft.com/en-US/cli/azure/ad/user#az_ad_user_create
Read more about the command in reference docs
Attribution des utilisateurs aux groupes...
Vérification des groupes et leurs membres...
Membres du groupe Amiral:
Result
-----
Jean-Luc Picard
Membres du groupe Capitaine:
Result
-----
Catherine Janeway
William Riker
domenico_mandolino [ ~ ]$ []
```

## JOB 4 Gestion des droits

**Créez le fichier :**

*nano assign\_roles.sh*

**Copiez le contenu du script:**

*#!/bin/bash*

```
echo "Récupération de l'ID du rôle Global Administrator..."
# Obtenir l'ID du rôle Global Administrator
GLOBAL_ADMIN_ROLE_ID=$(az rest --method get \
--url 'https://graph.microsoft.com/v1.0/directoryRoles' \
--query "value[?displayName=='Global Administrator'].id" -o tsv)
```

```
echo "Attribution des rôles aux membres du groupe Amiral..."
# Pour chaque membre du groupe Amiral
for member in $(az ad group member list --group "Amiral" --query [].id -o tsv); do
    echo "Attribution du rôle Global Administrator au membre $member..."
    az rest --method post \
```

```
--url  
"https://graph.microsoft.com/v1.0/directoryRoles/$GLOBAL_ADMIN_ROLE_ID/me  
mbers/$ref" \  
--headers "Content-Type=application/json" \  
--body  
"{\"@odata.id\":\"https://graph.microsoft.com/v1.0/directoryObjects/$member\"}"  
done
```

```
echo "Attribution des rôles aux membres du groupe Capitaine..."  
# Pour les membres du groupe Capitaine  
for member in $(az ad group member list --group "Capitaine" --query  
[].userPrincipalName -o tsv); do  
    echo "Conversion en Guest User pour $member..."  
    az rest --method patch \  
    --url "https://graph.microsoft.com/beta/users/$member" \  
    --headers "Content-Type=application/json" \  
    --body '{"userType": "Guest"}'
```

done

```
echo "Vérification finale..."  
echo "Membres Guest User:"  
az ad user list --filter "userType eq 'Guest'" --query "[].displayName" -o table
```

```
echo "Membres Global Administrator:"  
az rest --method get \  
--url  
"https://graph.microsoft.com/v1.0/directoryRoles/$GLOBAL_ADMIN_ROLE_ID/me  
mbers" \  
--headers "Content-Type=application/json" \  
--body  
"{"@odata.id": \"$member\"}"
```

```
--query "value[].displayName" -o table
```

### Rendez le script exécutable :

```
chmod +x assign_roles.sh
```

### Exécutez le script :

```
./assign_roles.sh
```

### Remarques importantes :

- Le script utilise l'API Microsoft Graph pour certaines opérations
- Il vérifie les attributions à la fin
- La propagation des droits peut prendre quelques minutes
- Il faut avoir les permissions suffisantes pour exécuter ces commandes

```
domenico_mandolino [ ~ ]$ ./assign_roles.sh
Récupération de l'ID du rôle Global Administrator...
Attribution des rôles aux membres du groupe Amiral...
Attribution du rôle Global Administrator au membre 37e2697b-6fff-4cae-acb4-739981824255...
Bad Request(["error":{"code":"Request_BadRequest","message":"One or more added object references already exist for the following modified properties: 'members'."}])
Attribution des rôles aux membres du groupe Capitaine...
Conversion en Guest User pour c.janeway@domenicomandolinolaplatefor.onmicrosoft.com...
Conversion en Guest User pour w.riker@domenicomandolinolaplatefor.onmicrosoft.com...
Vérification finale...
Membres Guest User:
Result
-----
Catherine Janeway
William Riker
Membres Global Administrator:
Result
-----
d.mandolino
Jean-Luc Picard
domenico_mandolino [ ~ ]$
```

Cette erreur n'est pas critique car elle indique simplement que l'attribution du rôle était déjà faite( suite aux multiples essais )

## JOB 5 Monitoring

### Créez le fichier :

```
nano setup_monitor.sh
```

Copiez le contenu du script:

```
#!/bin/bash
```

```
# Variables
```

```
RESOURCE_GROUP="StarTrekVMs-rg"
WORKSPACE_NAME="StarTrekMonitor"
VM1="Enterprise-VM1"
VM2="Enterprise-VM2"

# Création de l'espace de travail Log Analytics
echo "Création de l'espace de travail Log Analytics..."
az monitor log-analytics workspace create \
    --resource-group $RESOURCE_GROUP \
    --workspace-name $WORKSPACE_NAME \
    --location francecentral

# Récupérer l'ID de l'espace de travail
WORKSPACE_ID=$(az monitor log-analytics workspace show \
    --resource-group $RESOURCE_GROUP \
    --workspace-name $WORKSPACE_NAME \
    --query id -o tsv)

# Activer les insights pour VM1
echo "Activation de Azure Monitor pour $VM1..."
az vm insights enable \
    --resource-group $RESOURCE_GROUP \
    --vm $VM1 \
    --workspace $WORKSPACE_ID
```

```
# Activer les insights pour VM2
echo "Activation de Azure Monitor pour $VM2..."
az vm insights enable \
    --resource-group $RESOURCE_GROUP \
    --vm $VM2 \
    --workspace $WORKSPACE_ID

# Configurer la collecte de données pour les métriques de base
echo "Configuration de la collecte de données..."
az monitor diagnostic-settings create \
    --resource-group $RESOURCE_GROUP \
    --name "VM-Monitoring" \
    --resource $VM1 \
    --workspace $WORKSPACE_ID \
    --metrics '[{"category": "AllMetrics", "enabled": true}]'

az monitor diagnostic-settings create \
    --resource-group $RESOURCE_GROUP \
    --name "VM-Monitoring" \
    --resource $VM2 \
    --workspace $WORKSPACE_ID \
    --metrics '[{"category": "AllMetrics", "enabled": true}]'

echo "Configuration terminée. Vérifiez le portail Azure Monitor pour voir les
métriques."
```

## Rendez le script exécutable :

```
chmod +x setup_monitor.sh
```

## Exécutez le script :

```
./setup_monitor.sh
```

```
domenico_mandolino [ ~ ]$ nano setup_monitor.sh
domenico_mandolino [ ~ ]$ ./setup_monitor.sh
Enregistrement des fournisseurs nécessaires...
Registering is still on-going. You can monitor using 'az provider show -n Microsoft.Insights'
Registering is still on-going. You can monitor using 'az provider show -n Microsoft.OperationsManagement'
Attente de l'enregistrement des fournisseurs (cela peut prendre quelques minutes)...
"Registering"
"Registered"
"Registering"
Création de l'espace de travail Log Analytics...
{
    "createdDate": "2024-12-20T00:04:37.9562867Z",
    "customerId": "b7c18023-8ba0-4f6d-b35b-af2162eb5a0b",
    "etag": "'1102f73d-0000-0000-0000-6764b5a60000\\''",
    "features": {
        "enableLogAccessUsingOnlyResourcePermissions": true
    },
    "id": "/subscriptions/b012ecb6-f953-4052-bbc4-6fb76e73a3ce/resourceGroups/StarTrekVMs-rg/providers/Microsoft.OperationalInsights/workspaces/StarTrekMonitor",
    "location": "francecentral",
    "modifiedDate": "2024-12-20T00:09:10.1909133Z",
    "name": "StarTrekMonitor",
    "provisioningState": "Succeeded",
    "publicNetworkAccessForIngestion": "Enabled",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": null,
    "forcedUpdateTag": null,
    "instanceView": null,
    "location": "francecentral",
    "name": "AzureMonitorLinuxAgent",
    "protectedSettings": null,
    "protectedSettingsFromKeyVault": null,
    "provisionAfterExtensions": null,
    "provisioningState": "Succeeded",
    "publisher": "Microsoft.Azure.Monitor",
    "resourceGroup": "StarTrekVMs-rg",
    "settings": null,
    "suppressFailures": null,
    "tags": null,
    "type": "Microsoft.Compute/virtualMachines/extensions",
    "typeHandlerVersion": "1.9",
    "typePropertiesType": "AzureMonitorLinuxAgent"
}
onfiguration terminée. Attendez quelques minutes pour voir les données dans Azure Monitor.
domenico_mandolino [ ~ ]$
```

Ce script va :

1. Créer un espace de travail Log Analytics
2. Activer Azure Monitor pour les deux VMs
3. Configurer la collecte des métriques de base

Une fois configuré, vous pourrez voir dans le portail Azure :

- L'utilisation CPU
- L'utilisation mémoire
- L'utilisation disque
- Les performances réseau

## JOB 6 Automatisation

### Créez le fichier :

```
nano setup_alerts.sh
```

**Copiez le contenu du script:**

```
#!/bin/bash
```

```
# Variables
```

```
RESOURCE_GROUP="StarTrekVMs-rg"
```

```
VM1="Enterprise-VM1"
```

```
VM2="Enterprise-VM2"
```

```
ACTION_GROUP_NAME="StarTrekAlerts"
```

```
EMAIL="domenico.mandolino@laplateforme.io" # Remplacez par votre email
```

```
# Création du groupe d'action (pour l'envoi d'emails)
```

```
echo "Création du groupe d'action pour les alertes..."
```

```
az monitor action-group create \
```

```
--resource-group $RESOURCE_GROUP \
```

```
--name $ACTION_GROUP_NAME \
```

```
--short-name "STAlerts" \
```

```
--action email $EMAIL \
```

```
--action-name "SendEmail"
```

```
# Récupérer l'ID du groupe d'action
```

```
ACTION_GROUP_ID=$(az monitor action-group show \
```

```
--resource-group $RESOURCE_GROUP \
```

```
--name $ACTION_GROUP_NAME \
```

```
--query id -o tsv)
```

```

# Fonction pour créer une alerte pour une VM

create_alerts_for_vm() {

    local VM_NAME=$1

    local VM_ID=$(az vm show -g $RESOURCE_GROUP -n $VM_NAME --
query id -o tsv)

    # Alerta CPU

    echo "Création de l'alerte CPU pour $VM_NAME..."

    az monitor metrics alert create \
        --resource-group $RESOURCE_GROUP \
        --name "${VM_NAME}-CPU-Alert" \
        --scopes $VM_ID \
        --condition "avg Percentage CPU > 50" \
        --window-size 5m \
        --evaluation-frequency 1m \
        --action $ACTION_GROUP_ID

    # Alerta Mémoire

    echo "Création de l'alerte Mémoire pour $VM_NAME..."

    az monitor metrics alert create \
        --resource-group $RESOURCE_GROUP \
        --name "${VM_NAME}-Memory-Alert" \
        --scopes $VM_ID \
        --condition "avg Available Memory Bytes < 50" \
        --window-size 5m \

```

```

--evaluation-frequency 1m \
--action $ACTION_GROUP_ID

# Alerte Disque

echo "Création de l'alerte Disque pour $VM_NAME..."

az monitor metrics alert create \
--resource-group $RESOURCE_GROUP \
--name "${VM_NAME}-Disk-Alert" \
--scopes $VM_ID \
--condition "avg Used Disk Space Percentage > 50" \
--window-size 5m \
--evaluation-frequency 1m \
--action $ACTION_GROUP_ID

}


```

```

# Créer les alertes pour les deux VMs

echo "Configuration des alertes pour VM1..."

create_alerts_for_vm $VM1

echo "Configuration des alertes pour VM2..."

create_alerts_for_vm $VM2


```

*echo "Configuration des alertes terminée. Vous recevrez des emails quand les seuils seront dépassés."*

**Rendez le script exécutable :**

*chmod +x setup\_alerts.sh*

**Exécutez le script :**

./setup\_alerts.sh

Ce script va :

1. Créer un groupe d'action pour l'envoi d'emails
2. Configurer 3 alertes pour chaque VM :
  - CPU > 50%
  - RAM utilisée > 50%
  - Espace disque > 50%
3. Envoyer des emails quand les seuils sont dépassés

## JOB 7

### Vérification des coûts & Nettoyage des ressources

Pour utiliser ce script :

Sauvegardez-le comme cleanup.sh

```
#!/bin/bash
```

```
# Variables
```

```
RESOURCE_GROUP="StarTrekVMs-rg"
```

```
# Vérification des coûts (utilisant une commande différente)
```

```
echo "Vérification des coûts..."
```

```
az billing usage list --query "[].{Cost:pretaxCost,  
Resource:instanceName}" -o table
```

```
# Suppression des ressources

echo "Suppression des ressources..."

# 1. Suppression des alertes et groupes d'action

echo "Suppression des alertes et monitoring..."

az monitor action-group delete \
    --name "STAlerts" \
    --resource-group $RESOURCE_GROUP


# 2. Suppression des VMs

echo "Suppression des VMs..."

az vm delete \
    --resource-group $RESOURCE_GROUP \
    --name "Enterprise-VM1" \
    --yes

az vm delete \
    --resource-group $RESOURCE_GROUP \
    --name "Enterprise-VM2" \
    --yes


# 3. Suppression de l'espace de travail Log Analytics

echo "Suppression de l'espace de travail Log Analytics..."
```

```
az monitor log-analytics workspace delete \
    --resource-group $RESOURCE_GROUP \
    --workspace-name "StarTrekMonitor"

# 4. Suppression finale du groupe de ressources
echo "Suppression du groupe de ressources..."
az group delete \
    --name $RESOURCE_GROUP \
    --yes

echo "Nettoyage terminé."
```

Rendez-le exécutable avec chmod +x cleanup.sh

Exécutez-le avec ./cleanup.sh

Points importants :

- Le script vérifie d'abord les coûts
- Supprime les ressources dans un ordre logique
- L'option --yes évite les demandes de confirmation
- --no-wait permet de lancer la suppression en arrière-plan

```
domenico_mandolino [ ~ ]$ ./cleanup.sh
Vérification des coûts...
'usage' is misspelled or not recognized by the system.

Examples from AI knowledge base:
https://aka.ms/cli\_ref
Read more about the command in reference docs
Suppression des ressources...
Suppression des alertes et monitoring...
Suppression des VMs...
Suppression de l'espace de travail Log Analytics...
Are you sure you want to perform this operation? (y/n): y
Suppression du groupe de ressources...
Nettoyage terminé.
domenico_mandolino [ ~ ]$ []
```