

AWS - IAM & EC2

AWS IAM (Identity and Access Management) est un service d'Amazon Web Services permettant de gérer les accès aux ressources de manière sécurisée.

Grâce à IAM, vous pouvez contrôler qui peut accéder aux ressources AWS (utilisateurs, rôles, applications) et définir les permissions pour chacune de ces entités.

Job 0 :

Création d'un compte **AWS**

Objectif : créer un compte **AWS**, car c'est la base pour accéder aux services cloud.

Étapes :

sur **aws.amazon.com** et clique sur "Créer un compte **AWS**".

Util: laurent.....io

MDP : @A.....4

ID compte 084828566790

Choisir la formule free après avoir fourni vos coordonnées bancaires

S'inscrire à AWS

Sélectionner un forfait de support

Choisissez un forfait de support pour votre compte professionnel ou personnel. [Comparez les forfaits et les exemples de tarification](#). Vous pouvez modifier votre forfait à tout moment dans AWS Management Console.

Support Basic – Gratuit

- Recommandé pour les développeurs effectuant un essai avec AWS
- Accès en libre-service aux ressources AWS 24 h/24 et 7 j/7
- Uniquement pour les problèmes relatifs au compte et à la facturation
- Accès à Personal Health Dashboard et Trusted Advisor



Support Développeur – À partir de 29 USD/mois

- Recommandé pour les développeurs effectuant un essai avec AWS
- Contact par e-mail avec AWS Support pendant les heures de travail
- Temps de réponse de 12 heures (ouvrées)



Support Business – À partir de 100 USD/mois

- Recommandé pour les développeurs effectuant un essai avec AWS
- Support technique 24 h/24, 7 j/7 par e-mail, téléphone et messagerie instantanée
- Temps de réponse de 1 heure
- Ensemble complet de recommandations de bonnes pratiques Trusted Advisor



Détails des offres gratuites

Filtrer par :

[Effacer tous les filtres](#)

▼ Type d'offre

- En vedette
 - 12 mois gratuits
 - Toujours gratuit
 - Essais

▼ Catégories de produits

- Analytique
 - Intégration d'applications
 - Productivité d'entreprise
 - Calcul
 - Conteneurs
 - Engagement client
 - Base de données
 - Outils pour développeurs
 - Informatique pour l'utilisateur final
 - Web et mobile front-end
 - Game Tech
 - Internet des objets (IdO)
 - Machine learning
 - Gestion et gouvernance
 - Services multimédias
 - Migration et transfert
 - Mise en réseau et diffusion de contenu
 - Robotique
 - Sécurité, identité et conformité
 - Sans serveur
 - Stockage

Q Rechercher des produits de l'offre gratuite

CALCUL	STOCKAGE	BASE DE DONNÉES
Offre gratuite 12 MOIS GRATUITS Amazon EC2 750 heures par mois Capacité de calcul redimensionnable dans le cloud. 750 heures d'utilisation des instances t2.micro	Offre gratuite 12 MOIS GRATUITS Simple Storage Service (Amazon S3) 5 Go de stockage standard Infrastructure de stockage d'objets sécurisée, durable et scalable.	Offre gratuite 12 MOIS GRATUITS Amazon RDS 750 heures par mois d'utilisation de base de données (moteurs de base de données applicables) Service de base de données relationnelle géré pour MySQL, PostgreSQL, MariaDB ou SQL Server.
BASE DE DONNÉES	MACHINE LEARNING	CALCUL
Offre gratuite TOUJOURS GRATUIT Amazon DynamoDB 25 Go de stockage Base de données NoSQL rapide et flexible, avec une scalabilité aisée. 25 Go de stockage	Offre gratuite ESSAI GRATUIT Amazon SageMaker 2 mois essai gratuit Le machine learning pour tous les scientifiques des données et développeurs. 250 heures d'utilisation mensuelle des instances ml.t3.medium sur les blocs-notes Studio OU 250 heures d'utilisation mensuelle des instances ml.t2.medium ou ml.t3.medium sur les instances de blocs-notes à la demande 25 heures par mois sur les instances ml.m5.4xlarge sur SageMaker Data Wrangler 10 millions d'unités d'écriture, 10 millions d'unités de lecture, 25 Go de stockage par mois sur SageMaker Feature Store 50 heures d'utilisation sur les instances m4.xlarge ou m5.xlarge par mois sur l'entraînement	Offre gratuite TOUJOURS GRATUIT AWS Lambda 1 million de requêtes gratuites par mois Service de calcul qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul.
ANALYTIQUE		MOBILE
Offre gratuite ESSAI GRATUIT Amazon Redshift 2 mois d'essai gratuit Entreposage de données rapide, simple et abordable. Essai gratuit de deux mois		Offre gratuite TOUJOURS GRATUIT Amazon SNS 1 million de publications Service de messagerie en mode push entièrement géré, flexible et rapide. 1 000 000 de publications

Remplis les informations demandées (e-mail, carte bancaire, etc.) et choisis un plan **"Free Tier"** pour éviter les frais inutiles.



Félicitations !

Merci de vous être inscrit à AWS.

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

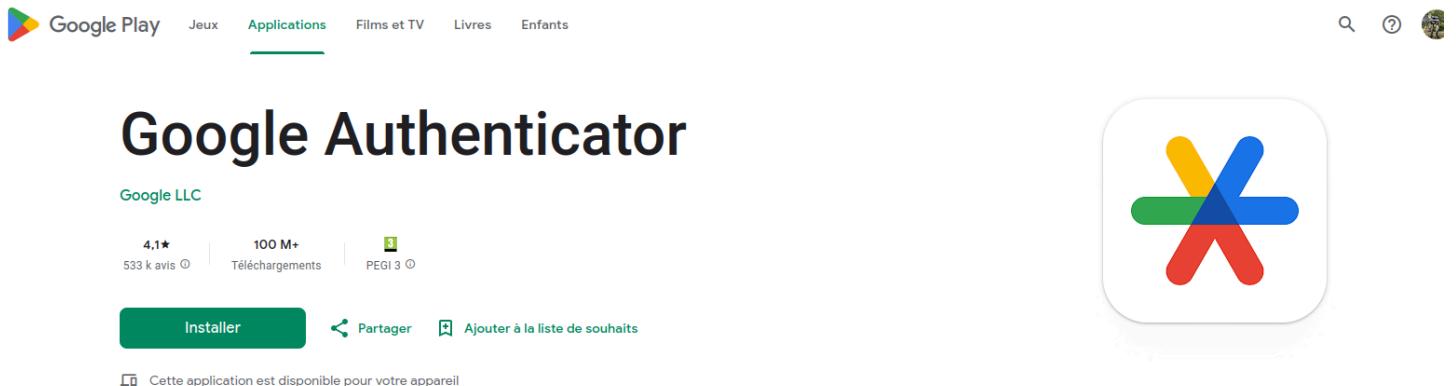
[Accéder à la console de gestion AWS](#)

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

Sécurité du compte

Activer la double Authentification avec **la MFA de l'utilisateur racine.**

Télécharger Google Authenticator sur Play store Android



Puis scanner le QR code d'authentification



Job 1 :

A quoi sert AWS IAM ? : Amazone Web Services / Identity Access Manager

AWS IAM (Identity and Access Management) est un service d'**Amazon Web Services** permettant de gérer les accès aux ressources de manière sécurisée. Grâce à **IAM**, vous pouvez contrôler qui peut accéder aux ressources AWS (utilisateurs, rôles, applications) et définir les permissions pour chacune de ces entités.

Objectifs et intérêt de AWS IAM

1. Gestion des utilisateurs et permissions : IAM permet de créer des utilisateurs et des groupes, d'assigner des rôles spécifiques, et de définir des permissions précises pour chaque entité. Cela permet de s'assurer que seules les personnes ou applications autorisées peuvent accéder aux ressources sensibles.
2. Gestion de la sécurité : IAM améliore la sécurité en limitant l'accès à certains services ou actions. Par exemple, vous pouvez limiter l'accès d'un utilisateur à certaines régions géographiques ou à des actions spécifiques (lecture, écriture).
3. Contrôle granulaire des accès : Avec IAM, vous pouvez créer des stratégies (policies) personnalisées pour gérer finement les accès à chaque ressource. Ces stratégies peuvent être très détaillées et appliquées au niveau des actions, des services ou même des ressources spécifiques.
4. Mise en conformité et audit : IAM inclut des fonctionnalités de journalisation (CloudTrail) qui permettent de suivre les actions des utilisateurs, facilitant ainsi l'audit des accès et la vérification de conformité.
5. Automatisation des accès temporaires : Grâce aux rôles IAM, il est possible de fournir des accès temporaires pour des tâches automatisées, ce qui limite l'exposition des permissions à un temps défini et réduit les risques de sécurité.

IAM est essentiel pour les entreprises utilisant AWS, car il garantit que les accès sont gérés de manière centralisée, sécurisée et conforme aux bonnes pratiques en matière de cybersécurité.

The screenshot shows the AWS Management Console Home page. At the top, there's a navigation bar with links like Applications, Emplacements, Système, and various browser icons. Below that is a toolbar with Eichier, Édition, Affichage, Historique, Marque-pages, Outils, and Aide. The main content area has a header "Console Home" with a "Info" link. On the left, there's a sidebar with "Recently visited" services and a "View all services" button. The main panel displays the "Applications" section, which is currently empty (0 applications). It includes a "Create application" button and a "Find applications" search bar. Below this, there's a table with columns for Name, Description, Region, and Originating account. A note at the bottom says "The data couldn't be retrieved. Try again later." At the bottom of the page, there are sections for "Welcome to AWS", "AWS Health", "Cost and usage", and "Getting started with AWS".

Créer 6 utilisateurs qui seront les suivants :

Creation compte Administrateur:

Connectez-vous à la console de gestion AWS en tant qu'**administrateur**.

1/ Cliquez sur Services.

2/ Dans la liste, sélectionnez IAM.

3/ Cliquez sur Utilisateurs > Ajouter un utilisateur.

The screenshot shows the AWS Management Console search results for the term 'iam'. The top navigation bar has 'Résultats de recherche pour 'iam'' displayed. On the left, there's a sidebar with links like 'Services (18)', 'Fonctionnalités (27)', 'Ressources New', etc. The main content area is titled 'Services' and shows four results: 'IAM' (selected), 'IAM Identity Center', 'Resource Access Manager', and 'AWS App Mesh'. Each result has a small icon, the service name, a star icon, and a brief description. Below this is another section titled 'Fonctionnalités' with 'Groupes' and 'Roles Anywhere' listed. A 'Voir tous les résultats' link is present in both sections.

Résultats de recherche pour 'iam'

Services (18) Fonctionnalités (27) Ressources New Publications de blog (12) Documentation (4 221) Articles de connaissances (155) Marketplace (912)

Services

Voir tous les résultats 18 ►

- IAM** ☆
Gérer l'accès aux ressources AWS
- IAM Identity Center** ☆
Gérer l'accès du personnel à plusieurs comptes et applications cloud AWS
- Resource Access Manager** ☆
Partage de ressources AWS avec d'autres comptes ou avec AWS Organizations
- AWS App Mesh** ☆
Surveillez et contrôlez facilement les microservices.

Fonctionnalités

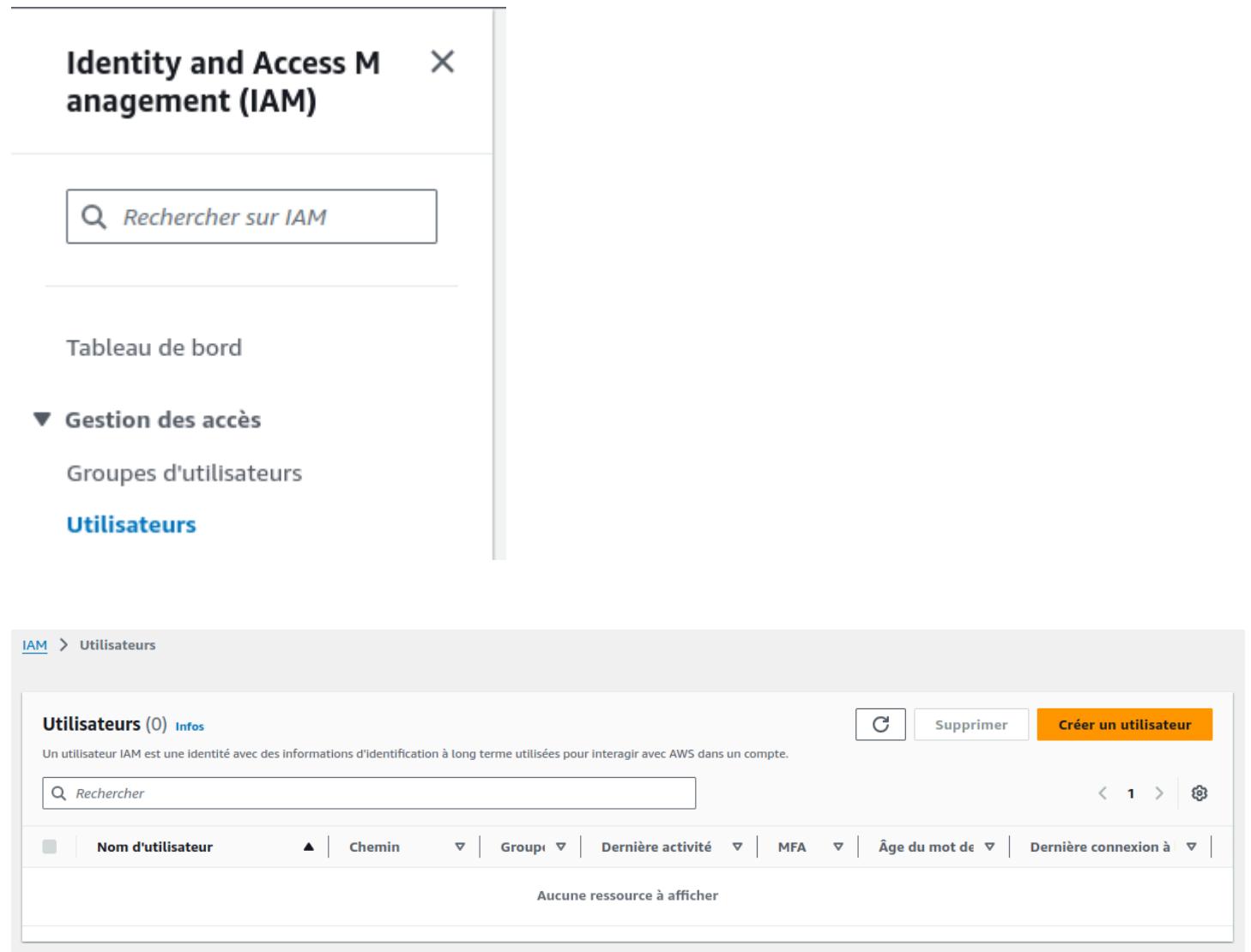
Voir tous les résultats 27 ►

- Groupes**
Fonctionnalité IAM
- Roles Anywhere**

Qu'est-ce que l'IAM ?

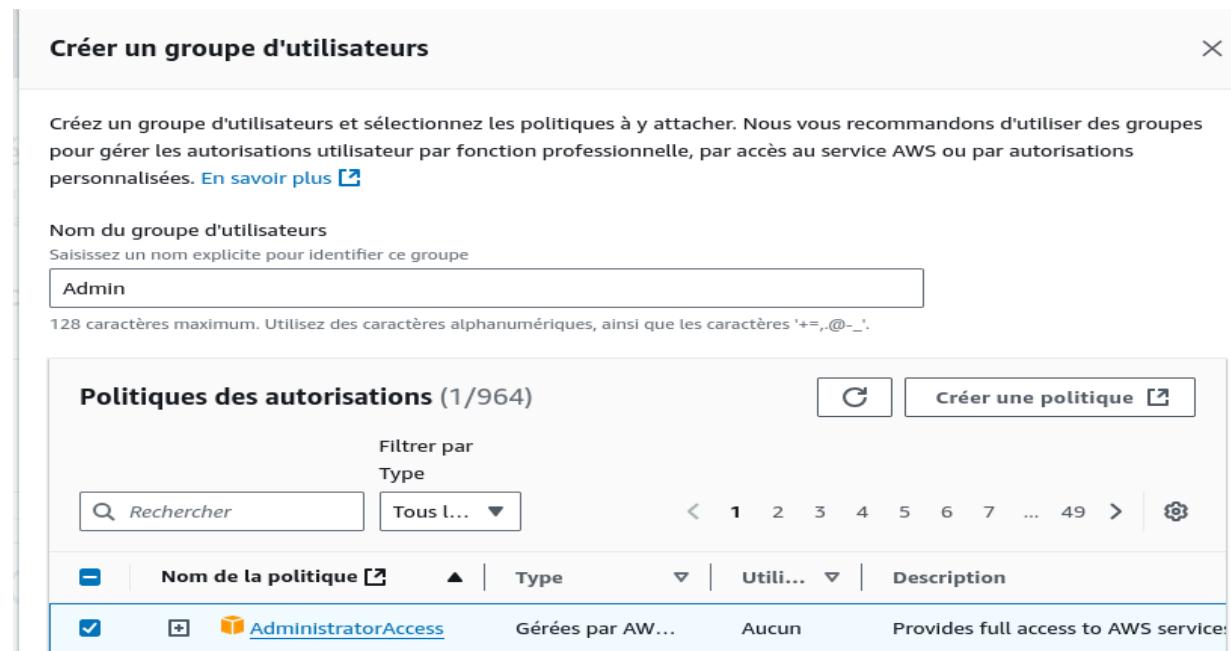
<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

Exemple création Utilisateur avec droits Administrateur :



The screenshot shows the AWS Identity and Access Management (IAM) console. In the left sidebar, under 'Gestion des accès', the 'Utilisateurs' option is selected. At the top right of the main content area, there is a prominent orange button labeled 'Créer un utilisateur'. The main area displays a table titled 'Utilisateurs (0) Infos' with one row: 'Aucune ressource à afficher'.

faudra créer un Groupe pour donner les droits spécifique à chaque utilisateur : (Administrateur)



The screenshot shows the 'Créer un groupe d'utilisateurs' dialog box. In the 'Nom du groupe d'utilisateurs' field, the value 'Admin' is entered. Below the table, the 'AdministratorAccess' policy is selected, indicated by a checked checkbox and highlighted in blue.

⌚ Groupe d'utilisateurs Admin créé.

Étape 2
Régler les autorisations

Étape 3
Vérifier et créer

Étape 4
Récupérer le mot de passe

Options d'autorisations

- Ajouter un utilisateur à un groupe
Ajouter un utilisateur à un groupe existant ou créer un nouveau groupe. Nous vous recommandons d'utiliser des groupes pour gérer les autorisations utilisateur par fonction de tâche.
- Copier les autorisations
Copiez toutes les appartenances à un groupe, les stratégies gérées attachées et les stratégies en ligne à partir d'un utilisateur existant.
- Attacher directement des politiques
Attacher une politique gérée directement à un utilisateur. La bonne pratique consiste à attacher des politiques à un groupe à la place. Ensuite, ajouter l'utilisateur au groupe approprié.

Groupes d'utilisateurs (1/1)

	Nom du groupe	Utilisateurs	Politiques attachées	Création
<input checked="" type="checkbox"/>	Admin	0	AdministratorAccess	2024-11-04 (Il y a 31 minutes)

▶ Définir une limite d'autorisations - facultatif

Annuler Précédent **Suivant**

⌚ Groupe d'utilisateurs Admin créé.

Étape 2
Régler les autorisations

Étape 3
Vérifier et créer

Étape 4
Récupérer le mot de passe

Détails de l'utilisateur

Nom d'utilisateur Jeff_Bezos	Type de mot de passe de la console Custom password	Demander la réinitialisation du mot de passe Non
---------------------------------	---	---

Résumé des autorisations

Nom	Type	Utilisé comme
Admin	Groupe	Groupe d'autorisations

⌚ Utilisateur créé avec succès

Vous pouvez afficher et télécharger le mot de passe de l'utilisateur et les instructions par e-mail pour vous connecter à la Console de gestion AWS.

Afficher l'utilisateur

IAM > Utilisateurs > Créer un utilisateur

Étape 1
Spécifier les détails de l'utilisateur

Étape 2
Régler les autorisations

Étape 3
Vérifier et créer

Étape 4
Récupérer le mot de passe

Récupérer le mot de passe

Vous pouvez consulter et télécharger le mot de passe de l'utilisateur ci-dessous ou envoyer par e-mail les instructions pour se connecter à la console de gestion AWS aux utilisateurs. C'est la seule fois que vous pourrez afficher et télécharger ce mot de passe.

Détails de connexion à la console

URL de connexion à la console <input type="text"/> https://084828566790.signin.aws.amazon.com/console	Envoyer par e-mail les instructions de connexion
Nom d'utilisateur <input type="text"/> Jeff_Bezos	
Mot de passe de la console <input type="text"/> @Jeff_Bezos <input type="button" value="Masquer"/>	

Annuler Télécharger le fichier .csv **Revenir à la liste des utilisateurs**

- Jeff Bezos (admin)Mdp : @Jeff_Bezos
- Elon Musk (admin)Mdp : @Elon_Musk

les deux comptes Droits Administrateur crée :
ils font parti du groupe Admin.

Utilisateurs (2) Infos		Supprimer	Créer un utilisateur
Un utilisateur IAM est une identité avec des informations d'identification à long terme utilisées pour interagir avec AWS dans un compte.			
<input type="checkbox"/>	Nom d'utilisateur	▲ Chemin ▾ Groupes ▾ Dernière activité ▾ MFA ▾ Âge du mot de passe ▾ Dernière connexion à ▾	
<input type="checkbox"/>	Elon_Musk	/ 1 .. - Maintenant -	
<input type="checkbox"/>	Jeff_Bezos	/ 1 .. - 5 minutes -	

Créations des comptes Utilisateurs:

- Mark Zuckerberg (utilisateur simple sans droit)
- Steve Jobs (utilisateur simple sans droit)
- Bill Gates (utilisateur simple sans droit)

Créer un Utilisateur :

Utilisateurs (4) Infos		Supprimer	Créer un utilisateur
Un utilisateur IAM est une identité avec des informations d'identification à long terme utilisées pour interagir avec AWS dans un compte.			
<input type="checkbox"/>	Nom d'utilisateur	▲ Chemin ▾ Groupes ▾ Dernière activité ▾ MFA ▾ Âge du mot de passe ▾ Dernière connexion à ▾	

Spécifier les détails de l'utilisateur

Détails de l'utilisateur

Nom d'utilisateur

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

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

En cas de création d'un accès par programmation à AWS CodeCommit ou Amazon Keyspaces via des clés d'accès ou des informations d'identification spécifiques à un service, vous pourrez les générer après avoir créé cet utilisateur IAM. [En savoir plus](#)

[Annuler](#)
Suivant

régler les autorisations (choisir le groupe)

Régler les autorisations

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

Options d'autorisations

- Ajouter un utilisateur à un groupe
Ajouter un utilisateur à un groupe existant ou créer un nouveau groupe. Nous vous recommandons d'utiliser des groupes pour gérer les autorisations utilisateur par fonction de tâche.
- Copier les autorisations
Copiez toutes les appartenances à un groupe, les stratégies gérées attachées et les stratégies en ligne à partir d'un utilisateur existant.
- Attacher directement des politiques
Attacher une politique gérée directement à un utilisateur. La bonne pratique consiste à attacher des politiques à un groupe à la place. Ensuite, ajouter l'utilisateur au groupe approprié.

Groupes d'utilisateurs (1/2)

Nom du groupe	Utilisateurs	Politiques attachées	Création
Admin	2	AdministratorAccess	2024-11-04 (Il y a 1 heure)
Utilisateurs	0	-	2024-11-04 (Il y a 4 minutes)

Vérifier la création de l 'utilisateur :

Vérifier et créer

Vérifiez vos choix. Après avoir créé l'utilisateur, vous pouvez afficher et télécharger le mot de passe généré automatiquement, si cette option est activée.

Détails de l'utilisateur

Nom d'utilisateur Bill_Gates	Type de mot de passe de la console None	Demander la réinitialisation du mot de passe Non
---	--	---

Résumé des autorisations

Nom	Type	Utilisé comme
Utilisateurs	Groupe	Groupe d'autorisations

.Utilisateur créé avec succès

Vous pouvez afficher et télécharger le mot de passe de l'utilisateur et les instructions par e-mail pour vous connecter à la Console de gestion AWS.

[Afficher l'utilisateur](#)

[IAM](#) > Utilisateurs

Utilisateurs (5) [Infos](#)

Nom d'utilisateur	Chemin	Groupes	Dernière activité	MFA	Âge du mot de passe	Dernière connexion à
BILL_GATES	/	0	-	-	-	-
Elon_Musk	/	1	-	-	1 heure	-
Jeff_Bezos	/	1	-	-	1 heure	-
Mark_Zuckerberg	/	0	-	-	-	-
Steve_Jobs	/	0	-	-	-	-

On doit switcher pour vérifier la création de chaque utilisateurs :

Connexion d'utilisateur IAM ⓘ

ID de compte (12 chiffres) ou alias de compte
084828566790

Nom d'utilisateur IAM
Steves_Job

Mot de passe
••••••••••

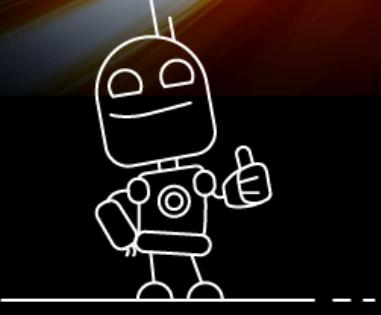
Afficher le mot de passe [Vous rencontrez des problèmes ?](#)

Connexion

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)



aws | Services | Rechercher [Alt+S] | Paris | Steve_Jobs @ 0848-2856-6790 ▾

Console Home [Info](#) | [Reset to default layout](#) | [+ Add widgets](#)

Recently visited [Info](#)

-  [Gestion de la facturation et des coûts](#)
-  [IAM Identity Center](#)
-  [IAM](#)

[View all services](#)

Applications (0) [Info](#)

Region: Europe (Paris)

[Create application](#)

Name	Description	Region	Originating account
✖ Accès refusé			

[Go to myApplications](#)

Job 2

- Developers (AdministratorAccess) = Mark Zuckerberg

Groupe d'utilisateurs Audit_team créé.

Afficher le groupe X

Developers

Supprimer

Récapitulatif

Modifier

Nom du groupe d'utilisateurs Developers	Heure de création November 04, 2024, 15:09 (UTC+01:00)	ARN arn:aws:iam::084828566790:group/Developers
--	---	---

Utilisateurs (1) Autorisations Access Advisor

Utilisateurs de ce groupe (1)

Un utilisateur IAM est une entité que vous créez dans AWS pour représenter la personne ou l'application qui l'utilise pour interagir avec AWS.

C Supprimer Ajouter des utilisateurs

Rechercher	Groupes	Dernière ac...	Heure de cr...
<input type="checkbox"/> Nom d'utilisateur ▾ Mark_Zuckerberg	2	Aucun	Il y a 51 minutes

IAM > Groupes d'utilisateurs

Groupes d'utilisateurs (3)

Infos Supprimer Crérer un groupe

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

Rechercher

Nom du groupe	Utilisateurs	Autorisations	Heure de création
Admin	2	Défini	Il y a 2 heures
Developers	1	Défini	Maintenant
Utilisateurs	3	Non défini	Il y a 47 minutes

- Audit team (IAMFullAccess) = Steve Jobs

Steve_Jobs 1 Il y a 22 minutes Il y a 47 minutes

Attacher des politiques d'autorisations - Facultatif (1/962)

Infos C

Vous pouvez attacher jusqu'à 10 politiques à ce groupe d'utilisateurs. Tous les utilisateurs de ce groupe disposeront des autorisations définies dans les politiques sélectionnées.

Filtrer par Type

Rechercher Tous les types 10 correspondances

Nom de la politique	Type	Utilisé comme	Description
AWSIAMIdentityCenterAll...	Gérées par AWS	Aucun	Provides the list of actions that are all...
AWSQuickSightListIAM	Gérées par AWS	Aucun	Allow QuickSight to list IAM entities
IAMAccessAdvisorReadOnly	Gérées par AWS	Aucun	This policy grants access to read all acc...
IAMAccessAnalyzerFullAcc...	Gérées par AWS	Aucun	Provides full access to IAM Access Anal...
IAMAccessAnalyzerReadO...	Gérées par AWS	Aucun	Provides read only access to IAM Acces...
<input checked="" type="checkbox"/> IAMFullAccess	Gérées par AWS	Aucun	Provides full access to IAM via the AW...

Audit_team Infos[Supprimer](#)

Récapitulatif

[Modifier](#)Nom du groupe d'utilisateurs
Audit_teamHeure de création
November 04, 2024, 15:12 (UTC+01:00)ARN
arn:aws:iam::084828566790:group/Audit_team[Utilisateurs](#)
(1)[Autorisations](#)[Access Advisor](#)

Utilisateurs de ce groupe (1)

[C](#)[Supprimer](#)[Ajouter des utilisateurs](#)

Un utilisateur IAM est une entité que vous créez dans AWS pour représenter la personne ou l'application qui l'utilise pour interagir avec AWS.

<input type="checkbox"/> Nom d'utilisateur ?		▲	Groupes	Dernière ac...	▼	Heure de cr...	▼
<input type="checkbox"/>	Steve_Jobs	2		Il y a 25 minutes		Il y a 50 minutes	

⌚ Groupe d'utilisateurs Audit_team créé.

[Afficher le groupe](#)

X

Groupes d'utilisateurs (4) Infos[Supprimer](#)[Créer un groupe](#)

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

<input type="checkbox"/> Nom du groupe		▲	Utilisateurs	▼	Autorisations	▼	Heure de création	▼
<input type="checkbox"/>	Admin	2		✔ Défini			Il y a 2 heures	
<input type="checkbox"/>	Audit_team	1		✔ Défini			Maintenant	
<input type="checkbox"/>	Developers	1		✔ Défini			Il y a 3 minutes	
<input type="checkbox"/>	Utilisateurs	3		⚠ Non défini			Il y a 50 minutes	

- Operations (IAMReadOnlyAccess) = Bill Gates

Nommer le groupe

Nom du groupe d'utilisateurs

Saisissez un nom explicite pour identifier ce groupe

 Operations

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

Ajouter des utilisateurs au groupe - Facultatif (1/5) Infos

Un utilisateur IAM est une entité que vous créez dans AWS pour représenter la personne ou l'application qui l'utilise pour interagir avec AWS.

[C](#)

<input type="checkbox"/> Nom d'utilisateur ?		▲	Groupes	Dernière ac...	▼	Heure de cr...	▼
<input checked="" type="checkbox"/>	Bill_Gates	1		Aucun		Il y a 35 minutes	
<input type="checkbox"/>	Elon_Musk	1		Aucun		Il y a 1 heure	

Attacher des politiques d'autorisations - Facultatif (1/962) [Infos](#)

Vous pouvez attacher jusqu'à 10 politiques à ce groupe d'utilisateurs. Tous les utilisateurs de ce groupe disposeront des autorisations définies dans les politiques sélectionnées.

Filtrer par Type

<input type="checkbox"/>	Nom de la politique	Type	Utilisé comme	Description
<input type="checkbox"/>	 AWSIAMIdentityCenterAll...	Gérées par AWS	Aucun	Provides the list of actions that are all...
<input type="checkbox"/>	 AWSQuickSightListIAM	Gérées par AWS	Aucun	Allow QuickSight to list IAM entities
<input type="checkbox"/>	 IAMAccessAdvisorReadOnly	Gérées par AWS	Aucun	This policy grants access to read all acc...
<input type="checkbox"/>	 IAMAccessAnalyzerFullAcc...	Gérées par AWS	Aucun	Provides full access to IAM Access Anal...
<input type="checkbox"/>	 IAMAccessAnalyzerReadO...	Gérées par AWS	Aucun	Provides read only access to IAM Acces...
<input type="checkbox"/>	 IAMFullAccess	Gérées par AWS	politique des autorisations (1)	Provides full access to IAM via the AW...
<input checked="" type="checkbox"/>	 IAMReadOnlyAccess	Gérées par AWS	Aucun	Provides read only access to IAM via th...
<input type="checkbox"/>	 IAMSelfManageServiceSpe...	Gérées par AWS	Aucun	Allows an IAM user to manage their o...

Groupes d'utilisateurs (5) [Infos](#)

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

[Supprimer](#)

[Créer un groupe](#)

Rechercher

< 1 >



<input type="checkbox"/>	Nom du groupe	Utilisateurs	Autorisations	Heure de création
<input type="checkbox"/>	Admin	2	Défini	Il y a 2 heures
<input type="checkbox"/>	Audit_team	1	Défini	Il y a 4 minutes
<input type="checkbox"/>	Developers	1	Défini	Il y a 7 minutes
<input type="checkbox"/>	Operations	1	Défini	Maintenant
<input type="checkbox"/>	Utilisateurs	3	Non défini	Il y a 54 minutes

Job 3 sécurité AWS

sécurité et politique de mot de passe, sur AWS,

Politique du Mot de Passe :

- minimum 12 caractères
- le mot de passe doit inclure un caractère en majuscule
- le mot de passe doit inclure un caractère en minuscule
- le mot de passe doit inclure un nombre
- le mot de passe doit inclure un caractère spécial (!?. etc...)

dans Paramètres du compte = Politique de Mot de passe ici on peut modifier les options de la politique des mots de passe

IAM > Paramètres du compte

Paramètres du compte Infos

Politique de mot de passe Infos

Configurez les exigences de mot de passe pour les utilisateurs IAM.

Modifier

Ce compte AWS utilise la politique de mot de passe par défaut suivante :

Longueur minimale du mot de passe
8 caractères

Force du mot de passe

Incluez au moins des différents types de caractères suivants :

- Majuscule
- Minuscule
- Chiffres
- Caractères non alphanumériques

Autres exigences

- Jamais de mot de passe expiré
- Il ne doit pas être identique au nom ou à l'adresse e-mail de votre compte AWS

choisir personnalisé =>

Modifier la politique de mot de passe Infos

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
8 caractères

Force du mot de passe

Incluez au moins des différents types de caractères suivants :

- Majuscule
- Minuscule
- Chiffres
- Caractères non alphanumériques

Autres exigences

- Jamais de mot de passe expiré
- Il ne doit pas être identique au nom ou à l'adresse e-mail de votre compte AWS

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
- Requiert 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

la politique est établie

Les exigences de mot de passe pour les utilisateurs IAM sont mises à jour.

[IAM](#) > Paramètres du compte

Paramètres du compte Infos

Politique de mot de passe Infos

[Modifier](#)

Configurez les exigences de mot de passe pour les utilisateurs IAM.

Ce compte AWS utilise la politique de mot de passe personnalisée suivante :

Longueur minimale du mot de passe

12 caractères

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
- Nécessite au moins un caractère non alphanumérique

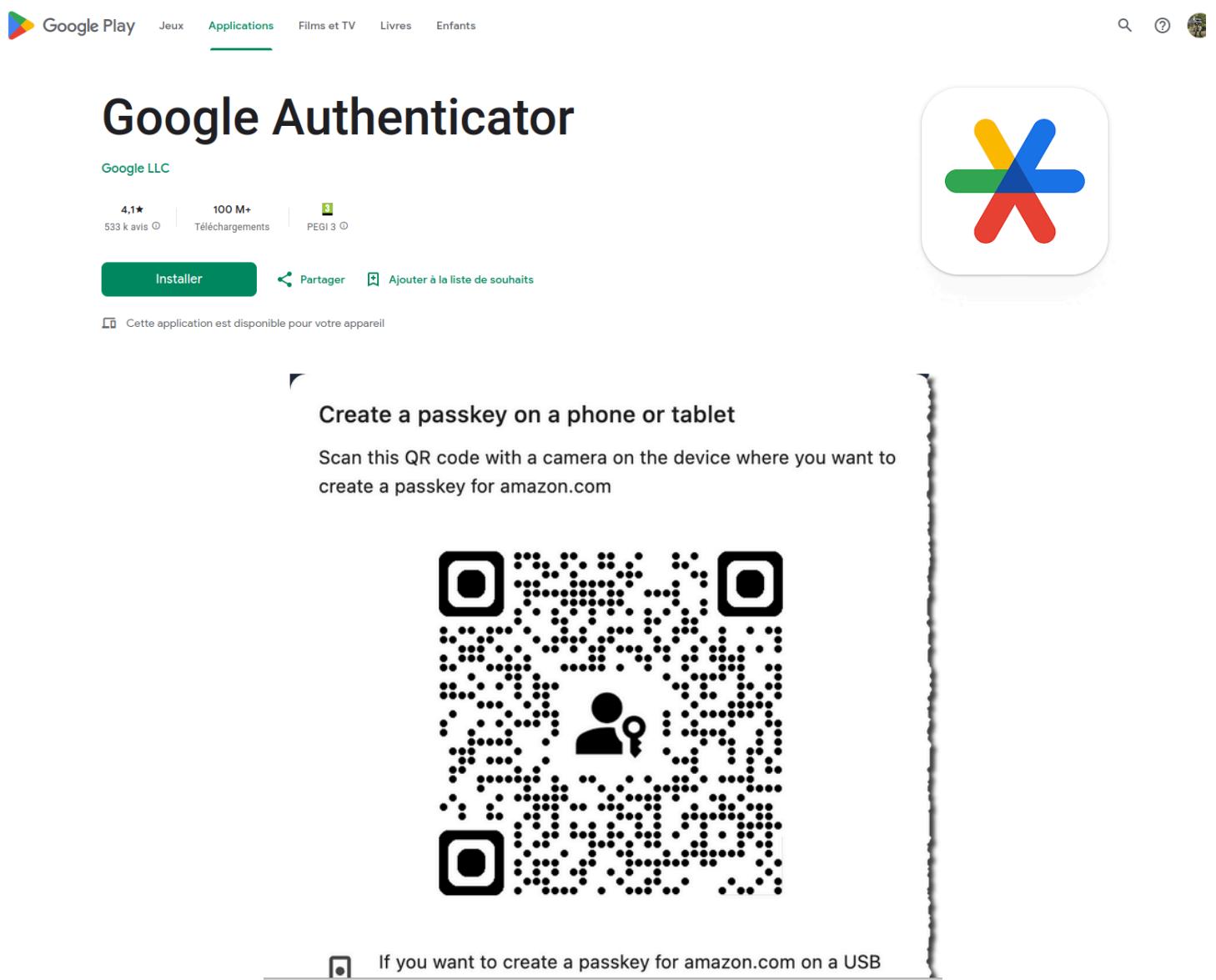
Autres exigences

- Jamais de mot de passe expiré

Sécurité du compte ROOT

Activer la double Authentification avec **la MFA de l'utilisateur racine.**

Télécharger Google Authenticator sur Play store Android



The image shows the Google Play Store page for the "Google Authenticator" app. At the top, there's a navigation bar with categories: Google Play, Jeux, Applications (which is underlined), Films et TV, Livres, and Enfants. To the right are search, refresh, and account icons. Below the navigation is the app's title, "Google Authenticator", in large bold letters. Underneath the title is the developer information, "Google LLC". The app has a rating of 4.1 stars from 533k reviews, over 100 million downloads, and is PEGI 3 rated. There are buttons for "Installer" (Install), "Partager" (Share), and "Ajouter à la liste de souhaits" (Add to wishlist). A note below the buttons says, "Cette application est disponible pour votre appareil". On the right side of the page is a large icon of the Google Authenticator logo, which consists of four colored bars (yellow, green, blue, red) forming an 'X' shape. Below the icon is a QR code with a small user icon in the center. Text next to the QR code reads, "Create a passkey on a phone or tablet" and "Scan this QR code with a camera on the device where you want to create a passkey for amazon.com". At the bottom, there's another note: "If you want to create a passkey for amazon.com on a USB".

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with 'Recommandations de sécurité' (Security Recommendations) containing two items: 'L'utilisateur racine dispose de la MFA' (Root user has MFA enabled) and 'L'utilisateur racine n'a aucune clé d'accès active' (Root user has no active access key). Below this is a section for 'Ressources IAM' (IAM Resources) with counts for Groups, Users, Roles, Policies, and Providers. On the right, there's a 'Compte AWS' (AWS Account) summary with the account ID '084828566790', alias 'Créer', and URL 'https://084828566790signin.aws.amazon.com/console'. There's also a 'Quick Links' section with a 'Mes autorisations de sécurité' (My security permissions) link.

Groupes d'utilisateurs	Utilisateurs	Rôles	Politiques	Fournisseurs d'identité
5	5	2	0	0

Job 4 AWS CLI

L'administration AWS

Utilisez vos AWS Access Keys pour accéder de manière sécurisée aux services AWS via la CLI

La CLI (Command Line Interface) est une interface en ligne de commande qui permet d'interagir avec des systèmes ou des logiciels en tapant des commandes textuelles, plutôt qu'en utilisant une interface graphique.

Dans le contexte d'AWS CLI (Amazon Web Services Command Line Interface), il s'agit d'un outil qui permet de gérer et de configurer les services AWS directement depuis votre terminal. En utilisant l'AWS CLI, vous pouvez :

- Créer, configurer et gérer des ressources AWS comme des instances EC2, des buckets S3, des bases de données RDS, etc.
- Automatiser des tâches courantes en exécutant des commandes au lieu de passer par la console web AWS.
- Intégrer des commandes dans des scripts pour des tâches d'administration ou d'automatisation.
- **Après analyse il est pas recommandé de se connecter au compte racine (Root) avec les clés CLI**

L'Access Key ID et la Secret Access Key pour le compte racine (root) d'AWS ne sont pas générés par défaut pour des raisons de sécurité.

AWS recommande vivement de ne pas utiliser le compte racine pour des opérations quotidiennes et de plutôt utiliser des utilisateurs IAM avec des priviléges appropriés.

installer AWS CLI version 2

1. Télécharger le package d'installation AWS CLI V2

```
laurent@debian:~$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

2. Installer les dépendances requises

```
laurent@debian:~$ sudo apt install unzip
```

3. Décompresser le fichier ZIP

```
laurent@debian:~$ unzip awscliv2.zip
```

4. Installer AWS CLI V2

```
laurent@debian:~$ sudo ./aws/install
```

5. Vérifier l'installation

```
laurent@debian:~$ aws --version
aws-cli/2.9.19 Python/3.11.2 Linux/6.1.0-26-amd64 source/x86_64.debian.12 prompt/off
```

Avant de configurer AWS CLI faut générer les cle :

Obtenir la clé d'accès pour le compte racine, voici les étapes :

1. Connectez-vous à la console AWS en tant qu'utilisateur racine

Allez sur AWS Management Console et connectez-vous avec les identifiants du compte racine.

2. Accédez à IAM (Identity and Access Management)

Une fois connecté, allez dans le service IAM.

Dans le panneau de navigation de gauche, cliquez sur My Security Credentials (Mes autorisations de sécurité).

IAM

Identity and Access Management (IAM)

Rechercher sur IAM

Tableau de bord

Gestion des accès

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

Rapports d'accès

- Analyseur d'accès
- Accès externe
- Accès non utilisé
- Paramètres de l'analyseur

Rapport sur les informations

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

Détails du compte		Modifier le nom du compte, l'adresse e-mail et le mot de passe	
Nom du compte	laurent.fauveau@laplateforme.io	Adresse e-mail	laurent.fauveau@laplateforme.io
ID de compte AWS	084828566790	ID d'utilisateur canonique :	68c1ee09d0e2b2ee5c5a1db123fb19a70f6b3bd9d703baa194806b85f3b8b1a1

Authentification multi-facteur (MFA) (1)				
Supprimer Resynchroniser Attribuer un dispositif MFA				
Type	Identificateur	Certifications	Créé le	
Virtuel	arn:aws:iam::084828566790:mfa/xiaomi	Ne s'applique pas	Mon Nov 04 2024	

3. Générez une clé d'accès pour le compte racine

Clés d'accès (0)

Créer une clé d'accès

Utilisez les clés d'accès pour effectuer des appels par programmation vers AWS à partir d'AWS CLI, des outils AWS pour PowerShell, des kits SDK AWS ou des appels d'API AWS directs. Vous pouvez disposer d'un maximum de deux clés d'accès (actives ou inactives) à la fois. [En savoir plus](#)

Identifiant de la clé d'accès	Créé le	Dernière utilisation de la clé d'accès	Dernière région utilisée	Dernier service utilisé	Statut
Aucune clé d'accès					

Il est déconseillé d'utiliser des informations d'identification à long terme, comme des clés d'accès. Utilisez plutôt des outils qui fournissent des informations d'identification à court terme. [En savoir plus](#)

Créer une clé d'accès

Dans la section Access keys (access key ID and secret access key), créer une clé d'accès pour le compte racine.

Cliquez sur Create New Access Key (Créer une nouvelle clé d'accès).

AWS générera une Access Key ID et une Secret Access Key pour le compte racine.

Alternatives aux clés d'accès d'utilisateur racine Infos

⚠️ Les clés d'accès d'utilisateur racine ne sont pas recommandées.

Nous vous déconseillons de créer des clés d'accès d'utilisateur racine. Comme vous ne pouvez pas spécifier l'utilisateur racine dans une politique d'autorisations, vous ne pouvez pas limiter ses autorisations, ce qui est recommandé.

Utilisez plutôt des alternatives, comme un rôle IAM ou un utilisateur dans IAM Identity Center, qui fournissent des informations d'identification temporaires plutôt qu'à long terme. [Learn More](#)

Si votre cas d'utilisation nécessite une clé d'accès, créez un utilisateur IAM avec une clé d'accès et appliquez-lui les autorisations de moindre privilège. [Learn More](#)

Continuer pour créer une clé d'accès?

Je comprends que la création d'une clé d'accès racine n'est pas une bonne pratique, mais je souhaite quand même en créer une.

Annuler **Créer une clé d'accès**

Récupérer la clé d'accès Infos

Clé d'accès

Si vous perdez ou oubliez votre clé d'accès secrète, vous ne pouvez pas la récupérer. Au lieu de cela, créez une clé d'accès et rendez l'ancienne clé inactive.

Clé d'accès

Clé d'accès secrète



AKIARHQBNGUDB7BK4WGJ



***** [Afficher](#)

4. Téléchargez et sauvegardez les clés

Authentification multi-facteur (MFA) (1)

[Supprimer](#)

[Resynchroniser](#)

[Attribuer un dispositif MFA](#)

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. [En savoir plus](#)

Type

Identificateur

Certifications

Créé le

Virtuel

arn:aws:iam::084828566790:mfa/xiaomi

Ne s'applique pas

Mon Nov 04 2024

Clés d'accès (1)

[Actions ▾](#)

[Créer une clé d'accès](#)

Utilisez les clés d'accès pour effectuer des appels par programmation vers AWS à partir d'AWS CLI, des outils AWS pour PowerShell, des kits SDK AWS ou des appels d'API AWS directs. Vous pouvez disposer d'un maximum de deux clés d'accès (actives ou inactives) à la fois. [En savoir plus](#)

Identifiant de la clé d'accès

Créé le

Dernière utilisation de la clé d'accès

Dernière région utilisée

Dernier service utilisé

Statut

AKIARHQBNGUDB7BK4WGJ

Il y a 16 minutes

Aucun

N/A

N/A

Active

```
laurent@debian:~$ aws configure
```

```
AWS Access Key ID [None]: KhRPX4ZLKQYvh5+gIMgYPv4kpBaUqbrgBXH+S2jl
```

```
laurent@debian:~$ aws configure list
```

Name	Value	Type	Location
profile	<not set>	None	None
access_key	*****4WGJ	shared-credentials-file	
secret_key	*****S2jl	shared-credentials-file	
region	eu-west-1	config-file	~/.aws/config

Une fois la clé générée, AWS vous permettra de télécharger un fichier .csv contenant l'Access Key ID et la Secret Access Key. Sauvegardez-le dans un endroit sécurisé car vous ne pourrez pas récupérer la Secret Access Key plus tard.

Important :Ne jamais utiliser le compte racine pour des opérations régulières. Créez un utilisateur IAM avec les permissions nécessaires et utilisez ce compte pour interagir avec AWS.

Révoquez la clé d'accès du compte racine si vous ne l'utilisez plus. La gestion des clés d'accès racine doit être évitée autant que possible pour des raisons de sécurité.

6. Configurer AWS CLI

```
laurent@debian:~$ aws configure
```

AWS Access Key ID : Votre **Access Key ID** générée depuis la console AWS.

AWS Secret Access Key : Votre **Secret Access Key** générée depuis la console AWS.

Default region name : La région AWS à utiliser (ex. **us-east-1**, **eu-west-1**, etc.).

Default output format : Le format de sortie que vous souhaitez (généralement **json**, mais vous pouvez choisir **text** ou **table** si vous préférez).

```
laurent@debian:~$ aws configure
AWS Access Key ID [None]: AKIARHQBNUGUDB7BK4WGJ
AWS Secret Access Key [None]: KhRPX4ZLKQYvh5+gIMgYPv4kpBaUqbrgBXH+S2j1
Default region name [None]: Europe
Default output format [None]: json
laurent@debian:~$ aws configure list
```

Name	Value	Type	Location
profile	<not set>	None	None
access_key	*****4WGJ	shared-credentials-file	
secret_key	*****S2j1	shared-credentials-file	
region	eu-west-1	config-file	~/.aws/config

Une fois la clé générée, AWS vous permettra de télécharger un fichier .csv contenant l'Access Key ID et la Secret Access Key. Sauvegardez-le dans un endroit sécurisé car vous ne pourrez pas récupérer la Secret Access Key plus tard.

Important :Ne jamais utiliser le compte racine pour des opérations régulières. Créez un utilisateur IAM avec les permissions nécessaires et utilisez ce compte pour interagir avec AWS.

Révoquez la clé d'accès du compte racine si vous ne l'utilisez plus. La gestion des clés d'accès racine doit être évitée autant que possible pour des raisons de sécurité.

Job 5 IAM Roles

Créer un IAM Role :

1. Introduction à IAM et aux IAM Roles

- **IAM (Identity and Access Management)** : AWS IAM est le service qui permet de gérer les accès aux ressources AWS en contrôlant qui est authentifié et autorisé à utiliser les services.
- **IAM Role** : Un rôle IAM est une identité AWS dotée d'autorisations spécifiques, mais il n'est pas lié à un utilisateur ni à un groupe.

Les IAM Roles sont conçus pour permettre l'accès aux services ou applications qui ont besoin d'agir avec des autorisations particulières, sans nécessiter d'identifiants permanents comme un nom d'utilisateur ou un mot de passe.

2. Pourquoi utiliser un IAM Role ?

- Un rôle IAM est utile pour les tâches qui nécessitent des permissions temporaires. Par exemple, si un développeur dans le groupe "Developers" a besoin d'accéder à certaines informations de l'infrastructure, un rôle IAM permet de limiter l'accès en fonction du besoin sans accorder les permissions globales d'un administrateur.
- Le rôle **DemoForEC2** avec la permission **IAMReadOnlyAccess** permet aux développeurs d'accéder aux informations de l'IAM sans pouvoir modifier les configurations.

Permissions IAMReadOnlyAccess

Cette permission donne un accès en lecture seule à l'ensemble des ressources IAM. Cela signifie que les utilisateurs disposant de ce rôle peuvent afficher les configurations IAM (utilisateurs, rôles, politiques), mais ne peuvent rien modifier. C'est idéal pour les développeurs qui ont besoin de consulter les configurations sans risque de les altérer.

3. Création du rôle IAM "DemoForEC2" avec AWS Management Console

étapes pour créer le rôle avec la permission **IAMReadOnlyAccess** :

1. Accédez à AWS Management Console :

- Connectez-vous à AWS avec un compte ayant des droits administratifs.

Connexion

Accédez à votre compte AWS par type d'utilisateur.

Type d'utilisateur ([vous n'êtes pas sûr ?](#))

Utilisateur racine
Propriétaire du compte qui effectue des tâches nécessitant un accès illimité.

Utilisateur IAM
Utilisateur au sein d'un compte qui effectue des tâches quotidiennes.

Adresse e-mail

laurent.fauveau@laplateforme.io

Suivant

OU

Nouveau sur AWS ? Inscrivez-vous

Garantir votre sécurité

Votre compte est protégé par l'**authentification multifactorielle (MFA)**.

Pour terminer la connexion, saisissez le code de votre dispositif MFA ci-dessous.

Code MFA

Saisir le code

Connexion

Se connecter à un autre compte

[Vous rencontrez des difficultés pour vous connecter ?](#)

Avec Google Authenticator inserez le code

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.

Tableau de bord
▼ Gestion des accès
Groupes d'utilisateurs
Utilisateurs
Rôles
Politiques
Fournisseurs d'identité
Paramètres du compte
▼ Rapports d'accès
Analyseur d'accès
Accès externe
Accès non utilisé
Paramètres de l'analyseur

Détails du compte

[Modifier le nom du compte, l'adresse e-mail et le mot de passe](#)

Nom du compte
laurent.fauveau@laplateforme.io

Adresse e-mail
laurent.fauveau@laplateforme.io

ID de compte AWS
084828566790

ID d'utilisateur canonique :
68c1ee09d0e2b2ee5c5a1db123fb19a70f6b3bd9d703baa194806b85f3b8b1a1

Authentification multi-facteur (MFA) (1)

[Supprimer](#)[Resynchroniser](#)[Attribuer un dispositif MFA](#)

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. [En savoir plus](#)

Type	Identificateur	Certifications	Créé le
Virtuel	arn:aws:iam::084828566790:mfa/xiaomi	Ne s'applique pas	Mon Nov 04 2024

2. Ouvrez le service IAM :

- accédez au service IAM.

IAM

▼ Gestion des accès

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

▼ Rapports d'accès

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

Consoles connexes

[IAM Identity Center](#)

IAM > Tableau de bord

Tableau de bord IAM Infos

Recommandations de sécurité 1

✓ L'utilisateur racine dispose de la MFA

L'utilisation de l'authentification multi-facteur (MFA) pour l'utilisateur racine renforce la sécurité de ce compte.

⚠ Désactiver ou supprimer les clés d'accès pour l'utilisateur racine

Désactivez ou supprimez les clés d'accès de l'utilisateur racine et utilisez plutôt les clés d'accès attachées à un utilisateur IAM pour renforcer la sécurité.

Ressources IAM

Ressources de ce compte AWS

Groupes d'utilisateurs	Utilisateurs	Rôles	Politiques	Fournisseurs d'identité
5	5	2	0	0

Compte AWS

ID de compte
084828566790

Alias de compte
[Créer](#)

URL de connexion pour les utilisateurs IAM de ce compte
<https://084828566790.siginn.aws.amazon.com/> console

Quick Links

[Mes autorisations de sécurité](#)

Gérez vos clés d'accès, l'authentification multi-facteur (MFA) et autres informations d'identification.

3. Créez un nouveau rôle :

- Cliquez sur Roles dans le panneau de gauche, puis sur Create role.

IAM

Identity and Access Management (IAM)

Tableau de bord

▼ Gestion des accès

- Groupes d'utilisateurs
- Utilisateurs
- Rôles**

IAM > Rôles

Rôles (2) 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 endossés par des entités de confiance.

<input type="checkbox"/>	Nom du rôle	Entités de confiance	Dernière activité
<input type="checkbox"/>	AWSServiceRoleForSupport	Service AWS: support (Rôle lié à un s -)	
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	Service AWS: trustedadvisor (Rôle lié -)	

[Supprimer](#)[Créer un rôle](#)

rites durées. Les rôles peuvent être endossés par des entités

4. Sélectionnez le type de rôle (EC2) :

choisissez le type **AWS Service** et sélectionnez **EC2**

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

Autoriser 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.

Cas d'utilisation

Autorisez un service AWS comme EC2, Lambda ou autres à effectuer des actions dans ce compte.

Service ou cas d'utilisation

EC2



Choisissez un cas d'utilisation pour le service spécifié.

Cas d'utilisation

EC2

Allows EC2 instances to call AWS services on your behalf.

5. Attachez la politique de permission :

- Dans la liste des permissions, recherchez **IAMReadOnlyAccess**.

Politiques des autorisations (962) [Infos](#)

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

Filtrer par Type



Tous les types



10 correspondances

Cochez la case à côté de **IAMReadOnlyAccess** pour attacher cette politique de lecture seule au rôle.

The screenshot shows the AWS IAM Role creation interface. At the top, there are three checkboxes: one checked, one partially checked, and one unchecked. Next to them is the text "IAMReadOnlyAccess". To the right, it says "Gérées par AWS" and "Provides read only access to IAM via th...".

6. Nommez le rôle et ajoutez une description :

le nom au rôle, par **DemoForEC2**.

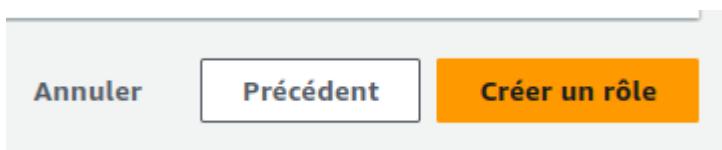
- Ajoutez une description si souhaité pour clarifier l'objectif du rôle, comme : "*Rôle de lecture seule pour les développeurs permettant d'accéder aux configurations IAM sans possibilité de modification.*"

Nommer, vérifier et créer

This screenshot shows the final review step of creating a role. It includes fields for the role name ("Nom du rôle") containing "DemoForEC2", a description field ("Description") containing "role de lecture seul pour les developpeurs pouvant accéder au configurations IAM sans possibilites de modifier celle ci", and a note about character limits. A large orange "Créer un rôle" button is at the bottom.

7. Créez le rôle :

- Passez en revue les détails, puis cliquez sur **Create role** pour finaliser la création.



The screenshot shows the "Rôles (3)" page in the IAM console. It lists three roles: "AWSServiceRoleForTrustedAdvisor", "DemoForEC2", and "DemoForEC2" (the one we just created). The newly created role is highlighted with a green bar at the top stating "Rôle DemoForEC2 créé." Below the list is a search bar and a table with columns for "Nom du rôle" and "Entités de confiance".

Job 6 AWS Credentials Report

Utilisez **AWS Credentials Report**, (rapport d'informations d'identification AWS), générez le et enregistrez-le.

Prérequis!!

- Vous avez besoin des permissions IAM appropriées pour générer et accéder au rapport. Les permissions suivantes sont nécessaires :

iam:**GenerateCredentialReport**

et

iam:**GetCredentialReport**.

Étapes pour générer et télécharger le rapport

1. **Connectez-vous à AWS CLI** depuis un terminal (assurez-vous que vos informations d'identification AWS CLI sont correctement configurées) :

```
laurent@debian:~$ aws configure list
  Name          Value        Type    Location
  ----          ----        ----    -----
  profile       <not set>    None    None
access_key     ****4WGJ**** shared-credentials-file
secret_key     ****S2j1**** shared-credentials-file
region         eu-west-1    config-file  ~/.aws/config
```

2. **Générez le rapport** :

Utilisez la commande suivante pour générer le rapport d'informations d'identification IAM :

```
laurent@debian:~$ aws iam generate-credential-report
```

3. Vérifiez le statut :

Pour vérifier que le rapport est bien généré

```
laurent@debian:~$ aws iam get-credential-report
```

réponse une multitude de caractères et a la fin :

```
"ReportFormat": "text/csv",
"GeneratedTime": "2024-11-08T08:51:06+00:00"
```

4. Téléchargez le rapport :

Pour enregistrer le rapport localement sous forme de fichier CSV:

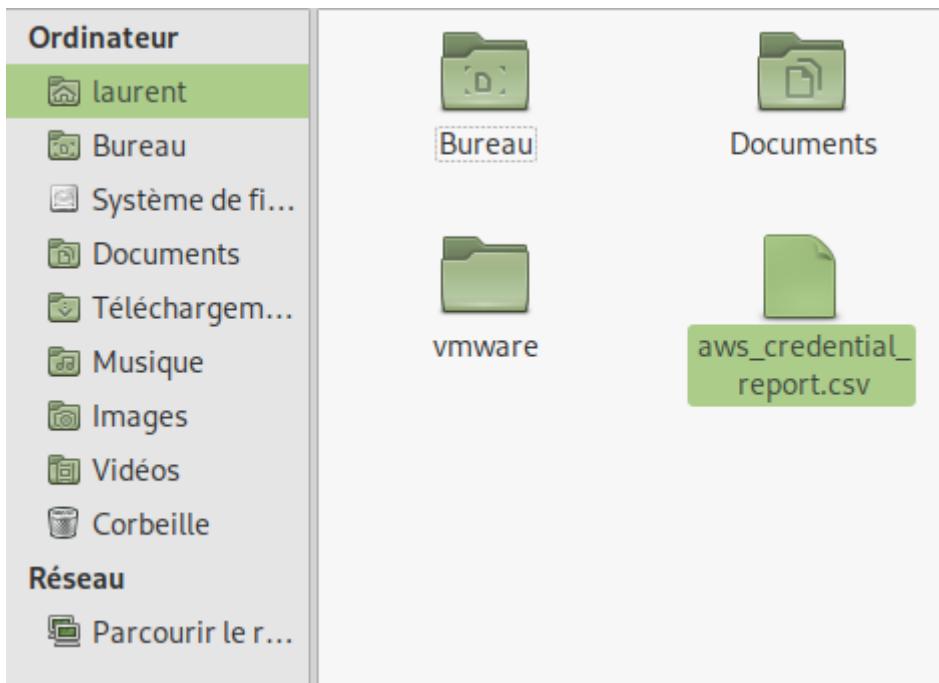
```
laurent@debian:~$ aws iam get-credential-report --query 'Content' --output text | base64 -d > aws_credential_report.csv
```

commande exploitable:

```
aws iam get-credential-report --query 'Content' --output text | base64 -d >
aws_credential_report.csv
```

Le fichier **aws_credential_report.csv** contiendra le rapport, et le rapport se situera à l'endroit où vous l'avez demandé avec la commande ci dessus:

“home/laurent le fichier .csv sera sauvegardé sur bureau de laurent



Nota !!

la commande **PWD** permet de situer où est enregistré le rapport .CSV

```
laurent@debian:~$ pwd  
/home/laurent
```

La commande **pwd** (print working directory) ne trouve pas un fichier spécifique; elle indique simplement le répertoire de travail actuel dans le terminal. En d'autres termes, elle montre **où vous êtes situé** dans l'arborescence de votre système de fichiers à un moment donné. Cela vous permet de savoir dans quel répertoire vos commandes et fichiers sont exécutés ou créés par défaut.

lister le fichier en ligne de commande

- Sur **Linux/MacOS**, vous pouvez lister le fichier pour confirmer sa présence avec :

```
laurent@debian:~$ ls -l aws_credential_report.csv
```

Sur **Windows**, le fichier sera également dans le répertoire courant de l'invite de commande PowerShell. Vous pouvez l'ouvrir directement avec un tableur comme Excel.

```
laurent@debian:~$ ls -l aws_credential_report.csv  
-rw-r--r-- 1 laurent laurent 1575 8 nov. 10:00 aws_credential_report.csv
```

Astuce pour spécifier un chemin différent :

Si vous souhaitez enregistrer le rapport dans un répertoire spécifique, vous pouvez inclure le chemin directement dans la commande, comme suit :

```
laurent@debian:~$ aws iam get-credential-report --query 'Content' --output text | base64 -d > /chemin/vers/dossier/aws_credential_report.csv
```

commande exploitable:

```
aws iam get-credential-report --query 'Content' --output text | base64 -d > /chemin/vers/dossier/aws_credential_report.csv
```

Remplacez **/chemin/vers/dossier/** par le chemin d'accès voulu.

5. Ouvrir et examinez le rapport :

Le fichier CSV contient des informations sur les utilisateurs IAM, telles que les dates d'expiration des clés d'accès, les dates de dernier accès, les statuts MFA, etc. Vous pouvez l'ouvrir avec un éditeur de texte ou un tableau.

Standard	Standard	Standard	Standard	Standard	Standard	Standard	Standard
1 user	arn	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	
2 <root_account>	arn:aws:iam::084828566790:root	2024-11-04T10:31:25Z	true	2024-11-08T08:24:08Z	2024-11-04T10:31:25Z	not_supported	
3 Bill_Gates	arn:aws:iam::084828566790:user/Bill_Gates	2024-11-04T13:40:48Z	false	N/A	N/A	N/A	
4 Elon_Musk	arn:aws:iam::084828566790:user/Elon_Musk	2024-11-04T12:17:35Z	true	no_information	2024-11-04T12:17:35Z	N/A	
5 Jeff_Bezos	arn:aws:iam::084828566790:user/Jeff_Bezos	2024-11-04T12:13:08Z	true	no_information	2024-11-04T12:13:08Z	N/A	
6 Mark_Zuckerberg	arn:aws:iam::084828566790:user/Mark_Zuckerberg	2024-11-04T13:23:14Z	false	N/A	N/A	N/A	
7 Steve_Jobs	arn:aws:iam::084828566790:user/Steve_Jobs	2024-11-04T13:24:51Z	true	2024-11-04T13:49:57Z	2024-11-04T13:24:52Z	N/A	

Explication des colonnes du rapport

Le rapport contient généralement des colonnes avec des informations telles que :

- **user** : nom de l'utilisateur IAM.
- **arn** : Amazon Resource Name de l'utilisateur.
- **user_creation_time** : date de création de l'utilisateur.
- **password_last_used** : dernière utilisation du mot de passe.
- **access_key_1_last_used_date, access_key_2_last_used_date** : date de dernière utilisation des clés d'accès.

En suivant ces étapes, vous aurez généré et sauvegardé un rapport d'informations d'identification AWS pour audit ou revue de sécurité.

Job 7

Création d'un budget à Zéro Euro !!

The screenshot shows the AWS Budgets interface. At the top, a green banner displays a success message: "Votre budget My Zero-Spend Budget a bien été créé. Après la création d'un budget, le remplissage de toutes vos données de dépenses peut prendre jusqu'à 24 heures." Below the banner, there are buttons for "Soumettre un commentaire" and a close button (X). The main area shows a breadcrumb navigation: Facturation et gestion des coûts > Budgets > Présentation. A table titled "Budgets (1)" lists one item: "My Zero-Spend Budget". The table columns include Nom, Seuils, Budget, Montant utilisé, Montant prév..., Actuels contre bud..., and Prévu. The "Budget" column shows "1,00 \$US", "0,00 \$US", and "0.00%". The "Seuils" column shows "OK". There are also "Actions" and "Créer un budget" buttons.

Job 8

EC2 (Elastic Compute Cloud) :

Qu'est-ce que EC2 ?

- Amazon **EC2 (Elastic Compute Cloud)** est un service d'Amazon Web Services (AWS) qui permet de créer et gérer des serveurs virtuels dans le cloud.

Quelles sont ses options de configuration et les tailles disponibles ?

- EC2** propose des configurations personnalisables selon les besoins de performance, avec des tailles d'instances (types) variées : t2.micro (basique), m5.large (intermédiaire), jusqu'à p4d.24xlarge (haute performance pour le calcul intensif).

C'est quoi EC2 User Data et à quoi ça sert ?

- EC2 User Data** est un script ou des commandes spécifiées lors du lancement d'une instance pour automatiser des tâches comme l'installation de logiciels ou la configuration initiale.

Quels sont les types d'instances qui existent ?

- Il existe plusieurs types, chacun optimisé pour un usage spécifique :
 - Généraliste (ex. : t3, m5),
 - Optimisé pour le calcul (ex. : c5),
 - Optimisé pour la mémoire (ex. : r5),
 - Optimisé pour le stockage (ex. : i3),
 - Accéléré par GPU (ex. : p4).

Job 9 création d'une instance EC2

c 'est quoi une instance EC2 ?

Une instance EC2 est une machine virtuelle qui fonctionne dans l'infrastructure AWS. Elle fonctionne comme un serveur physique, mais elle est virtualisée et vous pouvez en créer, démarrer et arrêter autant que nécessaire. Vous payez seulement pour les ressources utilisées, en fonction de la durée d'exécution de l'instance et des ressources qu'elle consomme (processeur, mémoire, stockage, etc.).

Étapes pour créer une instance EC2 :

1. Accédez au portail AWS :

Connectez-vous à la [console de gestion AWS](#).

2. Ouvrez le service EC2 :

- Dans le menu "Services", => **Calcul** => cliquez sur "**EC2**"



The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar menu includes 'Tableau de bord', 'Instances' (selected), 'Images', and 'AMI'. The main area displays 'Ressources' (Resources) with a summary of usage in the Europe (Paris) region. It lists 0 instances, 0 addresses, 0 capacity reservations, 0 load balancers, 0 auto scaling groups, 0 placement groups, 1 security group, 0 dedicated hosts, 0 instances, 0 snapshots, 0 key pairs, and 0 volumes. Below this is a 'Lancer une instance' (Launch instance) button. To the right, a 'Santé du service' (Service Health) section shows the 'Tableau de bord d'AWS Health'.

3. Lancez une instance :

- Cliquez sur Launch Instances.

This screenshot shows the 'Lancer une instance' (Launch instance) page. It features a large orange 'Lancer une instance' button at the top left. Below it is a 'Migrer un serveur' (Migrate a server) button. A note at the bottom states: 'Remarque : vos instances seront lancées dans la région Europe (Paris)' (Note: your instances will be launched in the Europe (Paris) region).

4. Configurez les paramètres de l'instance :

- Le nom de l'instance sera "Serveur Web Dev"
- L'image d'exécution sera "Amazon Linux"
- le type d'instance sera la plus petite (renseignez vous bien) t2.Micro

- comme les développeurs devront y avoir accès depuis ssh, il faudra générer une key pair

- il faut que le trafic soit ouvert pour tout le monde sur les port 80 et 443
- comme storage, un disque gp2 de 8Go

-
- o Nom et balises : "Serveur Web Dev"

Nom et balises [Informations](#)

Nom

Serveur Web Dev

[Ajouter des balises supplémentaires](#)

- o AMI (Amazon Machine Image) : Sélectionnez une image d'AMI qui définit le système d'exploitation et les applications pré-installées (par exemple, Amazon Linux 2, Ubuntu, Windows Server). "Amazon Linux"

Démarrage rapide

Amazon Machine Image (AMI)

AMI Amazon Linux 2023

ami-0db5e28c1b3823bb7 (64 bits (x86), uefi-preferred) / ami-0849a4d04c8822ce6 (64 bits (Arm), uefi)

Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs

Éligible à l'offre gratuite

Y compris les AMI d'AWS, de Marketplace et de la communauté

- o Type d'instance : Choisissez le type d'instance (par exemple, t2.micro pour une petite instance éligible à l'offre gratuite d'AWS). **t2.Micro**

Type de serveur virtuel (type d'instance)
t2.micro

- **Clé SSH (Key Pair)** : Sélectionnez ou créez une clé SSH pour se connecter de manière sécurisée à l'instance. Si vous n'en avez pas, vous pouvez en générer une :

▼ Paire de clés (connexion) Informations

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - *obligatoire*

Sélectionnez

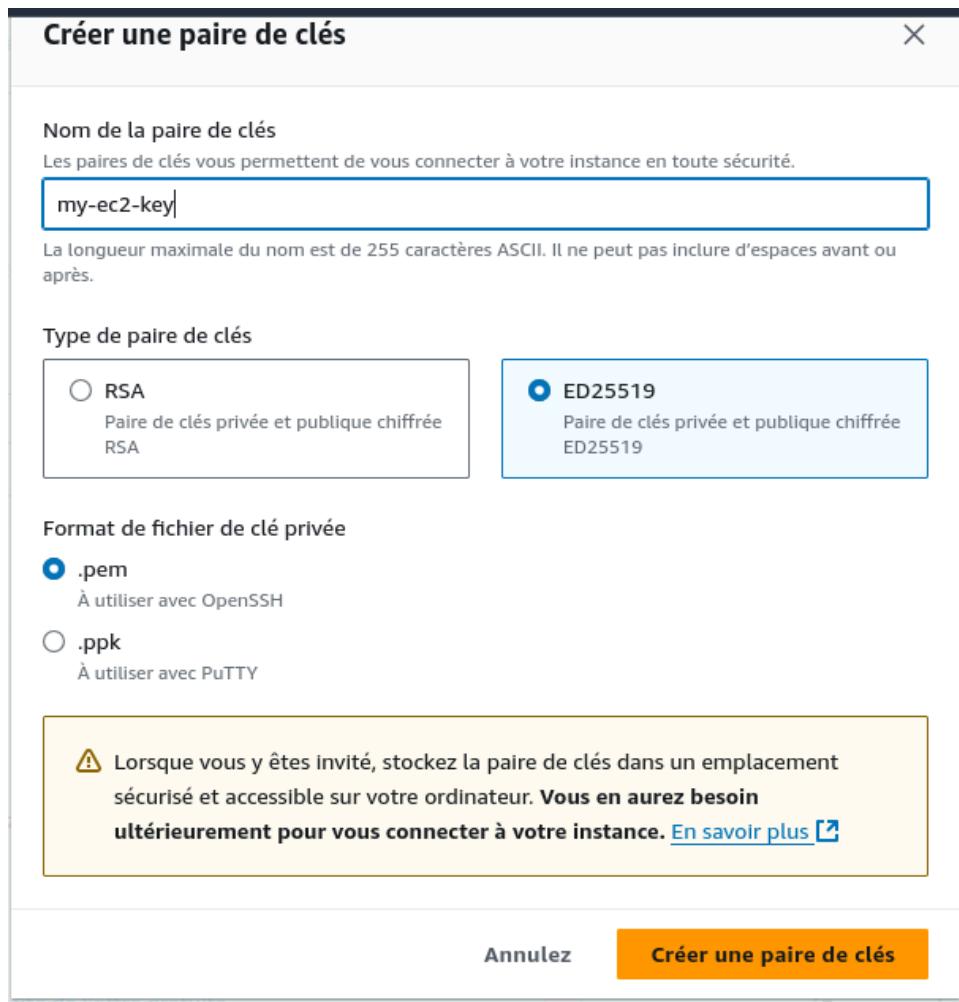


[Créer une paire de clés](#)

Étapes pour générer et utiliser une clé RSA dans AWS EC2

1. Génération de la clé RSA via la Console AWS :

- Allez dans le **service EC2** de la console AWS.
- Dans le panneau de gauche, cliquez sur **Key Pairs** (Paires de clés) sous "Network & Security".
- Cliquez sur **Create Key Pair** (Créer une paire de clés).
- Dans la fenêtre qui s'affiche :
 - Donnez un nom à votre clé (ex. : **my-ec2-key**).
 - **Type de clé** : Sélectionnez **clé ED25519 compatible et sécurisée pour Debian 12**.
 - **Format de fichier** : Choisissez **PEM** pour utiliser la clé facilement avec SSH sur **Debian 12**.
- Cliquez sur **Create key pair**. Le fichier **.pem** sera téléchargé sur votre machine locale.



2. Déplacez et configurez la clé sur Debian :

- Déplacez le fichier **.pem** téléchargé vers le répertoire **~/.ssh/** pour des raisons de sécurité.

Déplacez le fichier vers le répertoire **.ssh :**

```
laurent@debian:~/ssh$ mv ~/Téléchargements/my-ec2-key.pem ~/.ssh/
```

Modifiez les autorisations de la clé pour la sécuriser :

```
laurent@debian:~/ssh$ ls
cle_open_ai.pem  known_hosts  known_hosts.old  my-ec2-key.pem
laurent@debian:~/ssh$ chmod 400 ~/.ssh/my-ec2-key.pem
```

ID d'instance

[I-0620deaa63931ba0d \(Serveur Web Dev\)](#)

1. Ouvrez un client SSH.
2. Recherchez votre fichier de clé privée. La clé utilisée pour lancer cette instance est `my-ec2-key.pem`
3. Exécutez, si nécessaire, cette commande pour vous assurer que votre clé n'est pas visible publiquement.
 `chmod 400 "my-ec2-key.pem"`
4. Connectez-vous à votre instance à l'aide de son DNS public :
 `ec2-15-237-128-40.eu-west-3.compute.amazonaws.com`

Exemple :

`ssh -i "my-ec2-key.pem" ec2-user@ec2-15-237-128-40.eu-west-3.compute.amazonaws.com`

Remarque : Dans la plupart des cas, le nom d'utilisateur deviné est correct. Cependant, lisez les instructions d'utilisation de l'AMI pour vérifier si le propriétaire de l'AMI a modifié le nom d'utilisateur par défaut.

- **Paramètres réseau :** Configurez les paramètres de réseau et de sécurité :
 - Sélectionnez ou créez un VPC et un sous-réseau pour l'instance.
 - Configurez le groupe de sécurité (firewall) pour définir les règles d'accès réseau (autorisez par exemple le SSH sur le port 22 pour les instances Linux) **.port 80 et 443**

Activer

Des frais supplémentaires s'appliquent en cas de dépassement de la [limite de l'offre gratuite](#)

Pare-feu (groupes de sécurité) | [Informations](#)

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.

[Créer un groupe de sécurité](#)

[Sélectionner un groupe de sécurité existant](#)

Nous allons créer un nouveau groupe de sécurité appelé « **launch-wizard-1** » avec les règles suivantes :

[Autoriser le trafic SSH depuis](#)
Vous permet de vous connecter à votre instance.

N'importe où
0.0.0.0/0

[Autoriser le trafic HTTPS depuis l'Internet](#)
Pour configurer un point de terminaison, par exemple lors de la création d'un serveur web

[Autoriser le trafic HTTP depuis l'Internet](#)
Pour configurer un point de terminaison, par exemple lors de la création d'un serveur web

- **Stockage :** Configurez le volume de stockage de l'instance (taille et type de disque). **disque gp2 de 8Go**

▼ Configurer le stockage Informations

Avancé

1x 8 ▾ Glo gp2 ▾ Volume racine (Non chiffré)

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

Ajouter un volume

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



0 systèmes de fichiers

Modifier

5. Vérifiez les configurations et lancez l'instance :

- Vérifiez les paramètres de l'instance.
- Cliquez sur Launch Instance.

▼ Récapitulatif

Nombre d'instances Informations

1

Image logicielle (AMI)

Amazon Linux 2023 AMI 2023.6.2...[en savoir plus](#)
ami-0db5e28c1b3823bb7

Type de serveur virtuel (type d'instance)

t2.micro

Pare-feu (groupe de sécurité)

Nouveau groupe de sécurité

Stockage (volumes)

1 volume(s) - 8 Glo

i **Offre gratuite :** La première année inclut 750 heures d'utilisation mensuelle des instances t2.micro (ou

Annulez

Lancer l'instance

Code de prévisualisation

Succès

Lancement de l'instance réussi ([i-0620deaa63931ba0d](#))

Instances (1/1) Informations		Date de la dernière mise à jour Il y a less than a minute	C	Se connecter	État de l'instance ▾	Actions ▾	Lancer des instances	▼
<input type="text"/> Rechercher Instance par attribut ou identification (case-sensitive)					Tous les états ▾			
État de l'instance = running X				Effacer les filtres				
<input checked="" type="checkbox"/> Name D	ID d'instance	État de l'insta... ▾	Type d'insta... ▾	Contrôle des statu	Statut d'alarme	Zone de disponib	DNS IPv4 public	▼
<input checked="" type="checkbox"/> Serveur Web ...	i-0620deaa63931ba0d	En cours d'... 	t2.micro	2/2 vérifications r	Afficher les alarm	eu-west-3c	ec2-15-237-128-40.eu-...	

Il faut que le 80 et 443 soit ouvert :

Type [Informations](#)

ssh

Protocole [Informations](#)

TCP

Plage de ports [Informations](#)

22

Type de source [Informations](#)

N'importe où

Source [Informations](#)

Ajouter une adresse CIDR, une

Description - facultatif [Informations](#)

par exemple, SSH pour le bureau de

▼ Règle de groupe de sécurité 2 (TCP, 443, 0.0.0.0/0)

[Supprimer](#)

Type [Informations](#)

HTTPS

Protocole [Informations](#)

TCP

Plage de ports [Informations](#)

443

Type de source [Informations](#)

N'importe où

Source [Informations](#)

Ajouter une adresse CIDR, une

Description - facultatif [Informations](#)

par exemple, SSH pour le bureau de

Dans la partie Data inserez le script:

Données utilisateur - *facultatif* | [Informations](#)

Chargez un fichier contenant vos données utilisateur ou saisissez-les dans le champ.

```
# Installation de firewall (si nécessaire)
sudo yum install -y firewalld

# Ouverture des ports 80 et 443 dans le firewall
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --reload

# Création de la page index.html
echo "<html><body><h1>Server is running!</h1></body></html>" | sudo tee /
var/www/html/index.html

# Redémarrage d'Apache pour appliquer la configuration
sudo systemctl restart httpd
```



It works!

6. Connexion à l'instance : Une fois l'instance en cours d'exécution, vous pouvez vous y connecter :

- Dans la liste des instances, sélectionnez l'instance et cliquez sur Connect.
- Suivez les instructions pour vous connecter via SSH :

Job 10 se connecter via SSH

```
ssh -i ~/.ssh/my_ec2_key.pem ec2-user@<EC2-PUBLIC-IP>
ssh -i ~/.ssh/my_ec2_key.pem ec2-user@13.37.46.241
```

```
laurent@debian:~$ ssh -i ~/.ssh/my_ec2_key.pem ec2-user@13.37.46.241
,      #
~\_ ####_      Amazon Linux 2023
~~ \#####\
~~   \###|
~~     \#/ __ https://aws.amazon.com/linux/amazon-linux-2023
~~       \~' '->
~~~      /
~~.~.  _/
~/_/
/_m/'
```

Last login: Fri Nov 8 12:07:04 2024 from 2.15.57.93
[ec2-user@ip-172-31-42-145 ~]\$ ^C
[ec2-user@ip-172-31-42-145 ~]\$

Job 11 Attribuer à l'instance EC2 le IAM Role que vous avez créé (cf. Job 5):

Role à attribuer => **IAMReadOnlyAccess**

Attacher le rôle IAM à l'instance EC2 :

Allez dans le tableau de bord **EC2**.

1. Sélectionnez l'instance à laquelle vous souhaitez attribuer le rôle.

Instances (1/1) Informations		Date de la dernière mise à jour Il y a 14 minutes	Se connecter	État de l'instance	Actions	Lancer des instances
		<input type="text"/> Rechercher Instance par attribut ou identification (case-sensible)	Tous les états			
		État de l'instance = running	Effacer les filtres			
Name	ID d'instance	État de l'instance	Type d'instance	Contrôle des statut	Statut d'alarme	Zone de disponibilité
Serveur Web ...	I-0620deaa63931ba0d	Arrêté(e)	t2.micro	2/2 vérifications r	Afficher les alarmes	eu-west-3c

2. Cliquez sur Actions > Security (Sécurité) > Modify IAM role.

The screenshot shows the AWS EC2 Instances page. At the top, there are filters for 'Name' and 'ID d'instance'. A search bar contains the text 'Rechercher Instance par attribut ou identification (case-sensitive)'. Below the filters, a table lists an instance: 'Serveur Web ...' with ID 'i-0620deaa63931ba0d'. The instance status is 'Arrêté(e)' (Stopped). The 'Type d'insta...' column shows 't2.micro'. To the right of the instance details, there is a 'Actions' menu with several options: 'Se connecter', 'Afficher les détails', 'Gérer l'état de l'Instance', 'Paramètres de l'instance', 'Mise en réseau', 'Sécurité' (which is selected and highlighted in blue), 'Image et modèles', and 'Surveiller et dépanner'. A sub-menu for 'Sécurité' is open, showing 'Modifier les groupes de sécurité', 'Obtenir le mot de passe Windows', and 'Modifier le rôle IAM', with 'Modifier le rôle IAM' also highlighted in blue.

3. Sous IAM role, sélectionnez le rôle créer au Job5: DemoForEC2

The screenshot shows the 'Modify IAM role' configuration dialog. It has two main sections: 'ID d'instance' and 'Rôle IAM'. In the 'ID d'instance' section, an input field contains the value 'i-0620deaa63931ba0d (Serveur Web Dev)'. In the 'Rôle IAM' section, a dropdown menu is set to 'DemoForEC2'. To the right of the dropdown is a button labeled 'Créer un nouveau rôle IAM'. At the bottom of the dialog are two buttons: 'Annulez' and 'Mettre à jour le rôle IAM', with 'Mettre à jour le rôle IAM' being the primary action button.

4. Cliquez sur Update IAM role pour appliquer le rôle à l'instance EC2.

Après cela, l'instance EC2 aura des autorisations en lecture seule sur IAM, ce qui permet à cette instance d'interroger les ressources IAM sans pouvoir effectuer des modifications.

test pour vérifier la liste des utilisateurs

tapez sous la console AWS la ligne commande suivante :

```
aws iam list-users
```

last login: ttt nov 6 12:09 2024 from 2.13.57.93

[ec2-user@ip-172-31-42-145 ~]\$ aws iam list-users

```
[{"Users": [ {"Path": "/", "UserName": "Bill_Gates", "UserId": "AIDARHQBNNGUDNFLGX242G", "Arn": "arn:aws:iam::084828566790:user/Bill_Gates", "CreateDate": "2024-11-04T13:40:48+00:00"}, {"Path": "/", "UserName": "Elon_Musk", "UserId": "AIDARHQBNNGUDGVQUX0R5", "Arn": "arn:aws:iam::084828566790:user/Elon_Musk", "CreateDate": "2024-11-04T12:17:35+00:00"}, {"Path": "/", "UserName": "Jeff_Bezos", "UserId": "AIDARHQBNNGUDK3BFEPLUA", "Arn": "arn:aws:iam::084828566790:user/Jeff_Bezos", "CreateDate": "2024-11-04T12:13:08+00:00"}], ...skipping...]
```

Job 12

Détails des offres gratuites

Filtrer par :

Effacer tous les filtres

Type d'offre

- En vedette
- 12 mois gratuits
- Toujours gratuit
- Essais

Catégories de produits

- Analytique
- Intégration d'applications
- Productivité d'entreprise
- Calcul
- Conteneurs
- Engagement client
- Base de données
- Outils pour développeurs
- Informatique pour l'utilisateur final
- Web et mobile front-end
- Game Tech
- Internet des objets (IoT)
- Machine learning
- Gestion et gouvernance
- Services multimédias
- Migration et transfert
- Mise en réseau et diffusion de contenu
- Robotique
- Sécurité, identité et conformité
- Sans serveur
- Stockage

CALCUL			
Offre gratuite	12 MOIS GRATUITS	STOCKAGE	BASE DE DONNÉES
Amazon EC2		Simple Storage Service (Amazon S3)	
750 heures		5 Go	
par mois		de stockage standard	par mois d'utilisation de base de données (moteurs de base de données applicables)
Capacité de calcul redimensionnable dans le cloud.		Infrastructure de stockage d'objets sécurisée, durable et scalable.	
750 heures d'utilisation des instances t2.micro		750 heures	
▼		▼	

BASE DE DONNÉES			
Offre gratuite	12 MOIS GRATUITS	MACHINE LEARNING	CALCUL
Amazon RDS		AWS Lambda	
750 heures		1 million	
par mois d'utilisation de base de données (moteurs de base de données applicables)		de requêtes gratuites par mois	de requêtes gratuites par mois
Service de base de données relationnelle géré pour MySQL, PostgreSQL, MariaDB ou SQL Server.		Service de calcul qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul.	
▼		▼	

ANALYTIQUE			
Offre gratuite	ESSAI GRATUIT	MOBILE	
Amazon Redshift		Amazon SNS	
2 mois		1 million	
d'essai gratuit		de publications	de publications
Entreposage de données rapide, simple et abordable.		Service de messagerie en mode push entièrement géré, flexible et rapide.	
▼		▼	

STOCKAGE			
Offre gratuite	12 MOIS GRATUITS	ANALYSTIQUE	
Amazon DynamoDB		Amazon CloudWatch Metrics	
25 Go		1 million	
de stockage		de publications	de publications
Base de données NoSQL rapide et flexible, avec une scalabilité aisée.		Service de messagerie en mode push entièrement géré, flexible et rapide.	
25 Go de stockage		▼	

INFORMATIQUE			
Offre gratuite	TOUJOURS GRATUIT	DATA VIZUALISATION	
Amazon SageMaker		Amazon CloudWatch Metrics	
2 mois		1 million	
essai gratuit		de publications	de publications
Le machine learning pour tous les scientifiques des données et développeurs.		Service de messagerie en mode push entièrement géré, flexible et rapide.	
250 heures d'utilisation mensuelle des instances ml.t3.medium sur les blocs-notes Studio OU 250 heures d'utilisation mensuelle des instances ml.t2.medium ou ml.t3.medium sur les Instances de blocs-notes à la demande		▼	

DATA VIZUALISATION			
Offre gratuite	ESSAI GRATUIT	SECURISATION	
Amazon Kinesis Data Firehose		Amazon CloudWatch Metrics	
25 Go		1 million	
d'essai gratuit		de publications	de publications
Transfert de données à grande vitesse entre les services AWS et les applications externes.		Service de messagerie en mode push entièrement géré, flexible et rapide.	
▼		▼	

SECURISATION			
Offre gratuite	TOUJOURS GRATUIT	ANALYSTIQUE	
Amazon CloudWatch Metrics		Amazon CloudWatch Metrics	
1 million		1 million	
de publications	de publications	de publications	de publications
Service de messagerie en mode push entièrement géré, flexible et rapide.		Service de messagerie en mode push entièrement géré, flexible et rapide.	
▼		▼	

Job 13

effectuez un
snapshot du volume attaché à votre instance “Serveur web Dev”:

creation Snapshot

The screenshot shows the AWS EBS console with the following details:

- Left sidebar:** Shows navigation links for Tableau de bord, Vue globale EC2, Événements, Instances (selected), Instances, Types d'Instances, Modèles de lancement, Demandes Spot, Savings Plans, Instances réservées, Hôtes dédiés, Réservations de capacité, and Nouveau.
- Main Content:**
 - Volumes (1) Informations:** A table with one row: Name: -, ID du volume: vol-05710b69ebc5eb1be, Type: gp2, Taille: 8 GiB, IOPS: 100, Débit: -, ID de l'instance: snap-0a7f573..., Crée: 2024/11/12 11:36 GMT+1, Zone de disque: eu-west-3.
 - Tolérance aux pannes de tous les volumes de cette région:** Summary of snapshots taken.
 - Résumé de l'instantané:** Shows 0 / 1 volumes recently saved / total volumes.
 - Actions:** Buttons for Create volume, Create snapshot, Create lifecycle policy, Delete volume, Attach volume, Detach volume, Detach volume forcefully, Automatically enable E/S, Manage tags, and Inject perturbations (highlighted).

selectionner l instance et cliquez su Actions

The screenshot shows the AWS EBS console with the following details:

- Left sidebar:** Shows navigation links for Volumes (1/1) Informations, Images (AMI, Catalogue des AMI), and Elastic Block Store.
- Main Content:**
 - Volumes (1/1) Informations:** A table with one row selected: Name: -, ID du volume: vol-05710b69ebc5eb1be, Type: gp2, Taille: 8 GiB, IOPS: 100, Débit: -.
 - ID du volume:** vol-05710b69ebc5eb1be
 - Actions:** Buttons for Modify volume, Create snapshot, Create lifecycle policy, Delete volume, Attach volume, Detach volume, Detach volume forcefully, Automatically enable E/S, Manage tags, and Inject perturbations (highlighted).

Créer un instantané Informations

Créez un instantané ponctuel pour sauvegarder les données d'un volume Amazon EBS sur Amazon S3.

The screenshot shows the 'Create snapshot' wizard with the following steps:

- Volume source:** Shows the selected volume ID: vol-05710b69ebc5eb1be and its availability zone: eu-west-3c.
- Détails de l'instantané:**
 - Description:** A text input field containing "snapshot Serveur Web Dev".
 - Chiffrement:** A dropdown menu showing "Non chiffré".

Instantanés (1) Informations	
M'appartenant	Rechercher
<input type="checkbox"/> Name	ID d'instantané
<input type="checkbox"/> -	snap-0766a0bf235f9c999
	8 GiB
	snapshot Serveur Web Dev
	Standard
	En attente
	2024/11/12 11:41 GMT+1

AWS Services Rechercher [Alt+S] Paris laurent.fauveau@laplateforme.io

DemoForEC2 attaché à l'Instance i-037436301df4257cc avec succès

Instances (1/1) Informations Date de la dernière mise à jour Il y a 5 minutes Se connecter État de l'instance Actions Lancer des instances

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

État de l'instance = running Effacer les filtres

Name	ID d'instance	État de l'insta...	Type d'insta...	Contrôle des statu...	Statut d'alarme	Zone de disp...	DNS IPv4 public	Adresse IPv4...	IP
serveur web dev	i-037436301df4257cc	En cours d'...	t2.micro	2/2 vérifications r	Afficher les alarmes	eu-west-3c	ec2-13-37-46-241.eu-w...	13.37.46.241	-

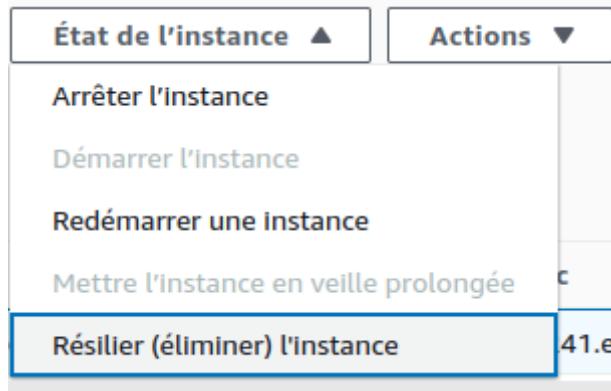
i-037436301df4257cc (serveur web dev)

Détails Statuts et alertes Surveillance Sécurité Mise en réseau Stockage Balises

Résumé de l'instance Informations

ID d'instance I-037436301df4257cc	Adresse IPv4 publique 13.37.46.241 adresse ouverte	Adresses IPv4 privées 172.31.42.145
Adresse IPv6 -	État de l'instance En cours d'exécution	DNS IPv4 public ec2-13-37-46-241.eu-west-3.compute.amazonaws.com adresse ouverte
Type de nom d'hôte Nom de l'adresse IP: ip-172-31-42-145.eu-west-3.compute.internal	Norm DNS de l'IP privée (IPv4 uniquement) ip-172-31-42-145.eu-west-3.compute.internal	Adresses IP élastiques
Réponse à un nom DNS de ressource privée	Type d'instance	

suppression de l 'instance



Résilier (éliminer) instance ?

⚠️ Sur une instance basée sur EBS, l'action par défaut concerne la suppression du volume EBS racine lorsque l'instance est mise hors service. Le stockage sur les éventuels disques locaux sera perdu.

Voulez-vous vraiment résilier ces instances ?

ID d'instance	Protection de la résiliation
I-037436301df4257cc (serveur web dev)	<input checked="" type="checkbox"/> Désactivé

Pour confirmer que vous souhaitez éliminer les instances, cliquez sur le bouton de résiliation ci-dessous. Les instances pour lesquelles la protection contre la résiliation est activée ne seront pas résiliées. La mise hors service de l'instance ne peut pas être annulée.

Annulez Résilier (éliminer)

The screenshot shows the AWS EC2 Instances page. At the top, there's a search bar and a 'Lancer des instances' button. Below the search bar, there's a filter section with 'État de l'Instance = running'. The main table header includes columns for Name, ID d'instance, État de l'instance, Type d'insta..., Contrôle des statu..., Statut d'alarme, Zone de disp..., and DNS IPv4 public. A message at the bottom of the table says 'Aucune Instance correspondante trouvée'.

plus d'instance Job Fini !!!!

JOUR 2

AWS - EC2 avancé +

Job 1

Commencez par lancer une instance **EC2** à partir du snapshot (instantanées) que vous avez effectué dans le **Jour 1 - job 13**

The screenshot shows the AWS Snapshots page. It lists a single snapshot named 'snap-0e0a3ecd8d6171bc5' with a size of 8 GiB, a description 'new serveur web dev', a status 'Standard', and a completion status 'Terminé' (Completed). The date of creation is 2024/11/12 15:38 GMT+1.

Étape 1 : Créer un volume EBS à partir du snapshot

1. Connectez-vous à votre console AWS.
2. Allez dans le service Snapshots sous Elastic Block Store (EBS).
3. Recherchez le snapshot que vous souhaitez utiliser.
4. Sélectionnez le snapshot, puis cliquez sur Actions > Create Volume.
5. Dans la fenêtre qui s'ouvre, configurez les paramètres du volume (comme le type, la taille et la zone de disponibilité).
6. Cliquez sur Create Volume.

Créer un volume Informations

Créez un volume Amazon EBS à attacher à n'importe quelle instance EC2 dans la même zone de disponibilité.

Paramètres du volume

ID d'Instantané
snap-0766a0bf235f9c999

Type de volume | [Informations](#)
SSD à usage général (gp2)

Taille (GiB) | [Informations](#)
8

Min : 1 GiB, Max : 16384 GiB. La valeur doit être un nombre entier.

IOPS | [Informations](#)
100 / 3000

Référence de 3 IOPS par GiB avec un minimum de 100 IOPS, pouvant être exécutées en rafales jusqu'à un maximum de 3000 IOPS.

Débit (Mio/s) | [Informations](#)
Sans objet

Zone de disponibilité | [Informations](#)
eu-west-3a

Étape 2 : Attacher le volume à une instance EC2

- Allez dans la section Volumes sous Elastic Block Store (EBS).

▼ Elastic Block Store

Volumes

- Sélectionnez le volume que vous venez de créer, puis cliquez sur Actions > Attach Volume.

Volumes (1/1) Informations										Actions	Créer un volume
<input type="text"/> Rechercher											
<input checked="" type="checkbox"/>	Name	ID du volume	Type	Taille	IOPS	Débit	ID de l'instantané	Créé			
<input checked="" type="checkbox"/>	-	vol-03af792f30e3d9b20	gp2	8 GiB	100	-	snap-0766a0bf235f9c...	2024/11/12 14:0			

- Choisissez l'instance EC2 à laquelle vous souhaitez attacher ce volume, puis cliquez sur Attach.

Attacher un volume Informations

Attachez un volume à une instance pour l'utiliser comme vous le feriez avec un disque dur physique normal.

Détails de base

ID du volume

[vol-06d4fe31bc87b041c](#)

Zone de disponibilité

eu-west-3c

Instance | [Informations](#)

i-0cc6fc1eb54b177bd



Seules les instances de la même zone de disponibilité que celle du volume sélectionné sont affichées.

Lancer une Nouvelle Instance EC2 :

- Retournez à la section Instances dans le panneau de gauche et cliquez sur Launch Instance.

Launch an instance Informations

Amazon EC2 vous permet de créer des machines virtuelles, ou des instances, qui s'exécutent sur le Cloud AWS. Démarrez rapidement en suivant les étapes simples indiquées ci-dessous.

Nom et balises Informations

Nom

par exemple, Mon serveur web

Ajouter des balises supplémentaires

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

Une AMI est un modèle contenant la configuration logicielle (système d'exploitation, serveur d'applications et applications) requise pour lancer votre instance. Parcourez ou recherchez des AMI si vous ne trouvez pas ce que vous recherchez ci-dessous.

Q Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de sy

- Choisissez une Amazon Machine Image (AMI) de base qui correspond au type de votre snapshot d'origine (par exemple, une AMI Ubuntu si votre snapshot est basé sur Ubuntu).

Récentes

Mes AMI

Démarrage rapide

M'appartenant

Partagé avec moi



Explorer plus d'AMI

Y compris les AMI d'AWS, de Marketplace et de la communauté

Amazon Machine Image (AMI)

ami_new_serveur_web

ami-0547f46f3025e6467

2024-11-12T14:51:04.000Z Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs

Description

- Sélectionnez le type d'instance souhaité (comme t2.micro pour une instance gratuite, si applicable).

▼ Récapitulatif

Nombre d'instances | [Informations](#)

1

Image logicielle (AMI)
ami_new_serveur_web
ami-0547f46f3025e6467

Type de serveur virtuel (type d'instance)
t2.micro

Pare-feu (groupe de sécurité)
Nouveau groupe de sécurité

Stockage (volumes)
1 volume(s) - 8 Gio

Attacher le Volume du Snapshot à l'Instance :

- Dans la section **Configure Instance Details**, sélectionnez la zone de disponibilité où vous avez créé le volume.
- Lancez l'instance en cliquant sur **Launch**.
- Une fois l'instance en cours d'exécution, allez dans **Volumes** dans le panneau de gauche.
- Sélectionnez le volume créé à partir du snapshot, puis cliquez sur **Actions > Attach Volume**.
- Attachez ce volume à votre instance en cours d'exécution.

