



RT CLOUD AWS

JOUR 1

JOB 0

Création du compte AWS.

JOB 1

Service AWS IAM

AWS Identity and Access Management, ou IAM, est très important dans le monde d'AWS. C'est un service qui nous aide à gérer l'accès aux ressources et services AWS de manière sécurisée. Avec IAM, on peut créer et gérer des utilisateurs, des groupes et des rôles, tout en définissant des permissions qui déterminent qui peut accéder à quoi. Une bonne gestion des identités et des accès est essentielle pour protéger nos données dans le cloud et éviter que des personnes non autorisées n'accèdent à nos informations sensibles.

Principes clés

- **Utilisateurs** : Ce sont les personnes ou les services qui vont interagir avec AWS. Chaque utilisateur a son propre nom et ses identifiants, comme un mot de passe ou des clés d'accès.
- **Groupes** : On regroupe les utilisateurs dans des groupes. Quand on attribue des permissions à un groupe, tous les membres héritent de ces permissions. Ça simplifie vraiment la gestion des accès !
- **Rôles** : Un rôle, c'est un ensemble de permissions qu'on peut attribuer à des utilisateurs ou des services AWS. Contrairement aux utilisateurs, les rôles ne sont pas attachés à une seule personne, ce qui les rend parfaits pour les services ou applications AWS.
- **Permissions** : Ce sont les règles qui définissent ce qu'un utilisateur, un groupe ou un rôle peut faire sur les ressources AWS. Elles sont généralement définies dans des politiques IAM, qui peuvent autoriser ou refuser certaines actions.

Principe du Moindre Privilège : Accorder uniquement les permissions nécessaires.

Authentification Multi-Facteurs (MFA) : Ajouter une sécurité supplémentaire.

Auditez Régulièrement les Permissions : Retirer les accès inutiles.

Conclusion

AWS IAM est essentiel pour sécuriser l'accès aux ressources AWS. En comprenant les utilisateurs, groupes, rôles et politiques, nous pouvons configurer un environnement AWS sécurisé.

Principe du Moindre Privilège

Le principe du moindre privilège stipule que chaque utilisateur ou composant d'un système informatique ne devrait avoir accès qu'aux ressources strictement nécessaires pour accomplir ses tâches, et rien de plus.

Importance :

Réduction des Risques de Sécurité : Limite les dommages potentiels en cas de compromission d'un compte ou d'un service.

Meilleure Gestion des Permissions : Facilite l'audit et la révision des accès, permettant de s'assurer que seules les permissions nécessaires sont accordées.

Application dans IAM :

Création de Politiques Précises : Rédigez des politiques qui définissent exactement quelles actions peuvent être effectuées sur quelles ressources.

Revue Régulière des Permissions : Effectuez des audits réguliers pour s'assurer que les permissions accordées sont toujours nécessaires et appropriées.

Utilisation de Rôles Temporaires : Employez des rôles pour accorder des permissions temporaires pour des tâches spécifiques, réduisant ainsi les risques d'accès prolongé non nécessaire.

Dans ce projet, nous allons documenter la création de plusieurs utilisateurs IAM (Identity and Access Management) sur AWS, en suivant le principe du moindre privilège

- Je vais maintenant créer les autres utilisateurs et les assigner aux groupes appropriés.

Jeff Bezos (Administrateur)

Nom d'utilisateur : jeff_bezos

Permissions : J'attache la politique d'administrateur "AdministratorAccess".

Elon Musk (Administrateur)

Nom d'utilisateur : elon_musk

Permissions : J'attache la politique d'administrateur "AdministratorAccess".

Mark Zuckerberg (Utilisateur Simple)

Nom d'utilisateur : mark_zuckerberg

Permissions : Je crée une politique qui limite strictement les permissions nécessaires.

Steve Jobs (Utilisateur Simple)

Nom d'utilisateur : steve_jobs

Permissions : Je crée une politique qui limite strictement les permissions nécessaires.

Bill Gates (Utilisateur Simple)

Nom d'utilisateur : bill_gates

Permissions : Je crée une politique qui limite strictement les permissions nécessaires.

Utilisateurs (6) [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.

Rechercher

< 1 >

<input type="checkbox"/>	Nom d'utilisateur ▲	Chemin ▼	Groupe ▼	Dernière activité ▼	MFA ▼	Âge du mot de ▼	Dernière
<input type="checkbox"/>	bill_gates	/	1	-	-	✓ 22 heures	-
<input type="checkbox"/>	elon_musk	/	0	-	-	✓ 22 heures	-
<input type="checkbox"/>	jeff_bezos	/	0	-	-	✓ 22 heures	-
<input type="checkbox"/>	mark_zuckerberg	/	1	-	-	✓ 21 heures	-
<input type="checkbox"/>	steve_jobs	/	1	-	-	✓ 21 heures	-
<input type="checkbox"/>	tara_derri	/	0	✓ Hier	-	✓ Hier	Novem

Création de la Politique pour les Utilisateurs Simples

Pour les utilisateurs simples (Mark Zuckerberg, Steve Jobs, Bill Gates), je vais créer une politique limitant strictement leurs permissions.

Politique Limitées

Autorisations définies dans cette politique Infos

Copier
Modifier
Récapitulatif
JSON

Les autorisations définies dans ce document de politique précisent les actions autorisées ou refusées. Afin de définir les autorisations d'une identité IAM (utilisateur, groupe d'utilisateurs ou rôle), attachez-lui une politique.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Deny",
6       "Action": "*",
7       "Resource": "*"
8     }
9   ]
10 }

```

- Étapes pour Créer et Attacher la Politique :

Dans la console IAM, je clique sur "Politiques" dans le panneau de navigation de gauche.

Je clique sur "Créer une politique".

Je copie et colle la politique JSON ci-dessus.

Je clique sur "Réviser la politique",

Je donne un nom à la politique ("politiquesansdroit").

J'attache cette politique aux utilisateurs Mark Zuckerberg, Steve Jobs et Bill Gates.

Conclusion

En suivant ces étapes, j'ai créé et configuré les utilisateurs IAM sur AWS en respectant le principe du moindre privilège. Cela permet de sécuriser l'accès à mes ressources AWS tout en attribuant des permissions appropriées à chaque utilisateur.

JOB 2

Je vais Créer des Groupes IAM pour la Gestion des Permissions

Administrateurs (AdministratorAccess)

Équipe d’audit (IAMFullAccess)

Opérations (IAMReadOnlyAccess)

Groupes d'utilisateurs (3) Infos

↻

Supprimer

Créer un groupe

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

< 1 > ⚙

<input type="checkbox"/>	Nom du groupe ▲	Utilisateurs ▼	Autorisations ▼	Heure de création ▼
<input type="checkbox"/>	Auditteam	1	✔ Défini	Il y a 21 heures
<input type="checkbox"/>	Developers	1	✔ Défini	Il y a 21 heures
<input type="checkbox"/>	Operations	1	✔ Défini	Il y a 21 heures

Voici comment j’ai procédé :

Étapes de Création des Groupes :1. Accéder à la Console IAM

Je me suis connecté à la console de gestion AWS et j’ai accédé au service IAM.

2. Naviguer vers la Section Groupes

Dans le panneau de navigation de gauche, j'ai cliqué sur "Groupes".

3. Créer le Groupe "Administrateurs"

J'ai cliqué sur "Créer un groupe".

J'ai entré "Administrateurs" comme nom du groupe.

J'ai attaché la politique "AdministratorAccess" au groupe Administrateurs pour leur donner les permissions nécessaires.

4. Créer le Groupe "Équipe d'audit"

J'ai répété les étapes précédentes.

J'ai nommé ce groupe "Équipe d'audit".

J'ai attaché la politique "IAMFullAccess" au groupe Équipe d'audit pour leur donner un accès complet à IAM.

5. Créer le Groupe "Opérations"

J'ai encore une fois répété les mêmes étapes.

J'ai nommé ce groupe "Opérations".

J'ai attaché la politique "IAMReadOnlyAccess" au groupe Opérations pour leur donner un accès en lecture seule à IAM.

En suivant ces étapes, j'ai pu créer et configurer efficacement les groupes IAM, simplifiant ainsi la gestion des permissions pour mes utilisateurs AWS.

JOB 3

Ensuite je cree une politique de mot de passe qui sera celle-ci

- 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...)

The screenshot shows the AWS IAM console interface for modifying a password policy. The breadcrumb navigation indicates the path: IAM > Paramètres du compte > Modifier la politique de mot de passe. The main heading is 'Modifier la politique de mot de passe' with an 'Infos' link. Below this, there are two radio buttons: 'IAM par défaut' (selected) and 'Personnalisé'. The 'Personnalisé' option is highlighted with a blue border. Under 'Personnalisé', the settings are: 'Longueur minimale du mot de passe' set to 12 characters, and 'Force du mot de passe' with four checked requirements: uppercase letters, lowercase letters, numbers, and non-alphanumeric characters. There are also unchecked options for 'Autres exigences' like password expiration and reuse. At the bottom right, there are two buttons: 'Annuler' and 'Enregistrer les modifications'.

J’ai cliqué sur “Appliquer la politique” pour enregistrer les modifications.

Activation de la MFA

Accéder aux Paramètres de Sécurité :

Après m’être connectée a mon compte root , j’ai cliqué sur mon nom de compte en haut à droite.

J’ai sélectionné “Mon compte” dans le menu déroulant.

Section Paramètres de Sécurité :

Dans la section “Paramètres de sécurité“, j’ai cliqué sur “Activer MFA“.

Configurer la MFA :

J’ai suivi les instructions pour configurer la MFA avec Google Authenticator.

J’ai scanné le code QR avec l’application d’authentification.

Entrer les Codes de Vérification :

J’ai entré les deux codes générés par l’application d’authentification.

Confirmation de l’Activation de la MFA :

Une fois les codes vérifiés, la MFA a été activée pour le compte root.

Étape 2
Configurer le dispositif

Authenticator app

Un dispositif MFA virtuel est une application s'exécutant sur votre appareil que vous pouvez configurer en scannant un code QR.

1

Installez une application compatible telle que Google Authenticator, Duo Mobile ou Authy sur votre appareil mobile ou votre ordinateur.

[Consultez la liste des applications compatibles](#)

2

Afficher le code QR

Ouvrez votre application d'authentification, choisissez **Show QR code** (Afficher le code QR) sur cette page, puis utilisez l'application pour scanner le code. Vous pouvez également saisir une clé secrète. [Afficher la clé secrète](#)

3

Saisir deux codes MFA consécutifs ci-dessous

Saisir un code depuis votre application virtuelle ci-dessous

Code MFA 1

Code MFA 2

Patiencez 30 secondes, puis saisissez un second code.

Annuler

Précédent

Ajouter la MFA

Authentification multi-facteur (MFA) (1)				
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				
<div><div>Supprimer</div><div>Resynchroniser</div><div>Attribuer un dispositif MFA</div></div>				
	Type	Identificateur	Certifications	Créé le
<input type="radio"/>	Virtuel	arn:aws:iam::484907501012:mfa/Auth	Ne s'applique pas	Tue Nov 05 2024

En documentant chaque étape avec des captures d'écran et des explications détaillées, j'ai assuré une compréhension claire et complète de la procédure l'activation de la MFA sur le compte root, et de la configuration de la politique de mot de passe.

JOB 4

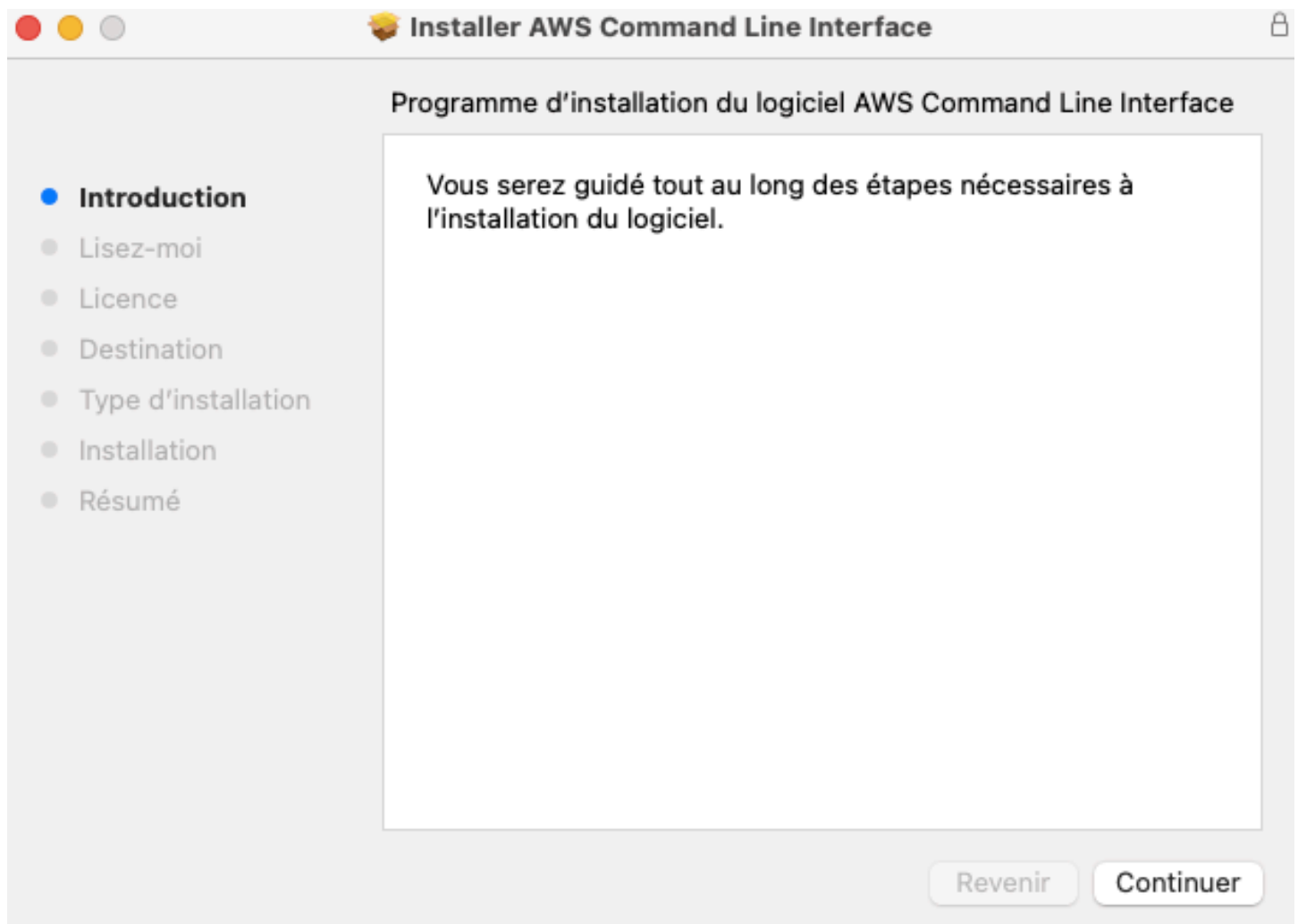
Maintenant je vais apprendre a administrer AWS autrement qu'en utilisant l'interface utilisateur web. Pour cela, je vais utiliser les clés d'accès AWS (AWS Access Keys) et l'interface en ligne de commande AWS (AWS CLI).

Voici les étapes détaillées pour installer et configurer la CLI AWS afin d'interagir avec les services AWS de manière sécurisée.

- Étape 1 : Télécharger et Installer la CLI AWS

Téléchargement de la CLI AWS :

Je vais sur la [page de téléchargement de la CLI AWS](#) pour obtenir la version 2 de l'outil. Selon mon système d'exploitation , ici macOS je choisis le package d'installation approprié.



- Étape 2 : Configuration des Clés d'Accès AWS

- **Générer des Clés d'Accès IAM :**

- Dans la console AWS, je vais sur "IAM".

- Je clique sur "Utilisateurs" dans le panneau de navigation de gauche.

- Je sélectionne mon utilisateur IAM personnel.

- Sous l'onglet "Identifiants de sécurité", je clique sur "Créer une clé d'accès".

- Je note l'ID de clé d'accès et la clé d'accès secrète fournies (je télécharge aussi le fichier CSV contenant ces informations)

Récupérer les clés 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



AKIAXBZV5IXKNB7YYE77



[Afficher](#)

Bonnes pratiques concernant les clés d'accès

- Ne stockez jamais votre clé d'accès en texte brut dans un référentiel de code ou dans le code.
- Désactivez ou supprimez la clé d'accès lorsque vous n'en avez plus besoin.
- Activez les autorisations à moindre privilège.
- Effectuez régulièrement une rotation des clés d'accès.

Pour plus d'informations sur la gestion des clés d'accès, consultez les [bonnes pratiques de gestion des clés d'accès AWS](#).

Télécharger le fichier .csv

Terminé

Je Configure la CLI AWS

J'ouvre un terminal et je tape la commande suivante pour configurer la CLI

Je saisis les informations suivantes :

AWS Access Key ID: (l'ID de clé d'accès généré)

AWS Secret Access Key: (la clé d'accès secrète générée)

Default region name: (la région AWS par défaut, par exemple, us-east-1)

Default output format: (le format de sortie par défaut, par exemple, json)

Je teste la configuration en exécutant une commande simple pour lister les buckets S3

```

region json config-file ~/.aws/config
[Air-de-User:~ user$ aws configure
AWS Access Key ID [*****YE77]: 
AWS Secret Access Key [*****hua6]: 
Default region name [json]: eu-west-3
Default output format [json]: json
[Air-de-User:~ user$ aws configure
AWS Access Key ID [*****YE77]: ^X^C
[Air-de-User:~ user$ aws s3 ls
[Air-de-User:~ user$ aws ec2 describe-instances
{
  "Reservations": []
}

```

JOB 5

Qu'est-ce qu'un IAM Role ?

Un IAM Role est une identité IAM que je peux créer dans mon compte AWS. Un rôle IAM a des permissions spécifiques qu'il autorise. Contrairement à un utilisateur IAM, un rôle n'a pas de clés d'identification de longue durée. Au lieu de cela, lorsqu'un rôle est assumé, il fournit des clés d'identification temporaires pour accéder aux ressources AWS.

Pourquoi utiliser les IAM Roles ?

Sécurité améliorée : Les rôles peuvent être utilisés pour accorder des permissions temporaires à des entités de confiance.

Flexibilité : Les rôles peuvent être assumés par n'importe quelle entité de confiance, y compris les services AWS, les utilisateurs IAM, les applications ou les comptes AWS.

Meilleure gestion des permissions : Ils permettent une gestion fine des accès et des permissions, minimisant ainsi les risques liés à l'utilisation des identifiants permanents.

Création d'un IAM Role "DemoForEC2" avec la Permission "IAMReadOnlyAccess"

Pour créer un rôle IAM, je vais suivre ces étapes

Je me connecte à AWS Management Console.

Je vais dans le service IAM.

Créer un rôle :

Je clique sur "Rôles" dans le panneau de navigation de gauche.

Je clique sur "Créer un rôle".

Sélectionner le type de rôle :

Je sélectionne le type de rôle en fonction de l'entité qui assumera ce rôle. Pour ce scénario, je choisis "AWS service" puis "EC2" car je crée un rôle pour une instance EC2.

☒ **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.

☐ EC2 Role for AWS Systems Manager

Attacher les permissions :

Je recherche la politique "IAMReadOnlyAccess".

Je coche la case à côté de cette politique pour l'attacher au rôle.

Je clique sur "Suivant : Balises". Je peux ajouter des balises si nécessaire pour la gestion des ressources

Ajouter des autorisations Infos

Politiques des autorisations (1/963) Infos

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

Filtrer par Type

Tous les types

10 correspondances

< 1 >

<input type="checkbox"/>	Nom de la politique	Type	Description
<input type="checkbox"/>	AWSIAMIdentityCenterAllowList...	Gérées par AWS	Provides the list of actions that are all...
<input type="checkbox"/>	AWSQuickSightListIAM	Gérées par AWS	Allow QuickSight to list IAM entities
<input type="checkbox"/>	IAMAccessAdvisorReadOnly	Gérées par AWS	This policy grants access to read all ac...
<input type="checkbox"/>	IAMAccessAnalyzerFullAccess	Gérées par AWS	Provides full access to IAM Access Anal...
<input type="checkbox"/>	IAMAccessAnalyzerReadOnlyAccess	Gérées par AWS	Provides read only access to IAM Acces...
<input type="checkbox"/>	IAMFullAccess	Gérées par AWS	Provides full access to IAM via the AW...
<input checked="" type="checkbox"/>	IAMReadOnlyAccess	Gérées par AWS	Provides read only access to IAM via th...
<input type="checkbox"/>	IAMSelfManageServiceSpecificCr...	Gérées par AWS	Allows an IAM user to manage their o...
<input type="checkbox"/>	IAMUserChangePassword	Gérées par AWS	Provides the ability for an IAM user to ...
<input type="checkbox"/>	IAMUserSSHKeys	Gérées par AWS	Provides the ability for an IAM user to ...

Une fois le rôle créé, je m’assure qu’il apparaît dans la liste des rôles avec les permissions correctes attachées.

[IAM](#) > Rôles

Rôles (3) 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.

< 1 >

<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	-
<input type="checkbox"/>	DemoForEC2	Service AWS: ec2	-

JOB 6

Générer le Rapport des Identifiants Dans le panneau de navigation de gauche, je clique sur “Rapports sur les informations d’identification”.

Je clique sur le bouton “Générer un rapport” pour créer un nouveau rapport. AWS peut prendre quelques instants pour générer le rapport.

Rapport sur les informations d'identification des utilisateurs IAM associés à ce compte [Infos](#)

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. Une fois qu'un rapport est créé, il est stocké pendant une durée maximale de quatre heures.

Rapport sur les informations d'identification


[Télécharger le rapport sur les informations d'identification](#)

Aucun rapport créé au cours des 4 dernières heures. Un nouveau rapport sera créé.

• Télécharger le Rapport :

Une fois le rapport prêt, un lien “Télécharger” apparaît à côté du bouton “Générer un rapport”.

Je clique sur “Télécharger” pour obtenir le fichier CSV contenant le rapport des identifiants.

● ● ●  status_reports_Sat Nov 09 2024 16_05_13 GMT+0100 (heure normale d'Europe centrale)...

```
user,arn,user_creation_time,password_enabled,password_last_used,password_last_changed,password_next_rotation,mfa_active,access_key_1_active,access_key_1_last_rotated,access_key_1_last_used_date,access_key_1_last_used_region,access_key_1_last_used_service,access_key_2_active,access_key_2_last_rotated,access_key_2_last_used_date,access_key_2_last_used_region,access_key_2_last_used_service,cert_1_active,cert_1_last_rotated,cert_2_active,cert_2_last_rotated
<root_account>,arn:aws:iam::484907501012:root,2024-11-02T12:44:56Z,true,2024-11-06T11:05:19Z,2024-11-02T12:44:56Z,not_supported,true,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,false,N/A
bill_gates,arn:aws:iam::484907501012:user/
bill_gates,2024-11-04T13:32:01Z,true,no_information,2024-11-04T15:55:28Z,N/A,false,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
elon_musk,arn:aws:iam::484907501012:user/
elon_musk,2024-11-04T13:04:40Z,true,no_information,2024-11-04T15:56:56Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
jeff_bezos,arn:aws:iam::484907501012:user/
jeff_bezos,2024-11-04T13:01:30Z,true,no_information,2024-11-04T15:59:39Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
mark_zuckerberg,arn:aws:iam::484907501012:user/
mark_zuckerberg,2024-11-04T13:29:39Z,true,no_information,2024-11-04T16:01:22Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
steve_jobs,arn:aws:iam::484907501012:user/
steve_jobs,2024-11-04T13:31:28Z,true,no_information,2024-11-04T16:02:40Z,N/A,false,false,N/A,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
tara_derri,arn:aws:iam::484907501012:user/
tara_derri,2024-11-04T12:29:26Z,true,2024-11-09T13:57:16Z,2024-11-04T12:29:26Z,N/A,false,true,2024-11-06T11:44:26Z,2024-11-09T13:39:00Z,eu-west-3,s3,false,N/A,N/A,N/A,N/A,N/A,false,N/A,N/A,N/A
```

JOB 7

Pour ce job j'ai créé une politique de budget .

Budgets (1)

Infos

Télécharger le rapport CSV

Actions ▾

Créer un budget

Rechercher un budget

Type – Afficher tous les budgets ▾

< 1 >

<input type="checkbox"/>	Nom	▲	Seuils	▼	Budget	Montant u...	Montant p...	Actuels contre bud...
<input type="checkbox"/>	My Zero-Spend Budget		<div><div>OK</div></div>		1,00 \$US	0,00 \$US	-	<div><div></div></div> 0.0

JOB 8

Qu'est ce que EC2 ?

EC2 est un service web qui permet de créer et de gérer des instances de machines virtuelles (VM) dans le cloud AWS. EC2 offre une capacité de calcul redimensionnable, ce qui permet aux utilisateurs de faire évoluer leurs ressources en fonction de leurs besoins.

Quelles sont ses options de configuration et les tailles disponibles ?

Options de Configuration et Tailles Disponibles pour Amazon EC2 Type d'instance

Les instances EC2 sont classées en différentes familles en fonction de l'usage prévu. Chaque famille est optimisée pour des types de charges de travail spécifiques :

- Généraliste (General Purpose) :**
Usage : Équilibre entre CPU, mémoire et réseau.
 t3, m5.
- Optimisé pour le calcul (Compute Optimized) :**
Usage : Idéal pour des charges de travail nécessitant des performances élevées du processeur.
 c5, c6g.
- Optimisé pour la mémoire (Memory Optimized) :**
Usage : Pour les applications nécessitant un accès rapide et important à la mémoire.
 r5, x1e.
- Optimisé pour le stockage (Storage Optimized) :**
Usage : Conçu pour des opérations d'entrée/sortie (I/O) intensives sur des bases de données ou des systèmes de fichiers.

i3, d2.

- **Accélération matérielle (Accelerated Computing) :**

Usage : Utilise des GPU et FPGA pour des charges de travail comme le machine learning et le calcul scientifique.

p3, f1.

Tailles d'instance : Chaque type d'instance propose différentes tailles allant de micro (très petite) à des tailles très grandes, offrant des combinaisons spécifiques de CPU, de mémoire et de capacité réseau. Par exemple, la famille t3 inclut des tailles telles que t3.micro, t3.small, t3.medium, etc.

Pourquoi ces différentes configurations ?

General Purpose (Usage général) : Ces instances offrent un équilibre entre les ressources de calcul, de mémoire et de réseau, ce qui les rend polyvalentes pour une variété de charges de travail, comme les serveurs web, les environnements de développement et de test.

Compute Optimized (Optimisé pour le calcul) : Ces instances sont conçues pour des applications nécessitant une puissance de traitement élevée, comme les serveurs de jeux, le calcul scientifique et le traitement batch.

Memory Optimized (Optimisé pour la mémoire) : Ces instances sont idéales pour des applications qui nécessitent un accès rapide et important à la mémoire, comme les bases de données haute performance, le traitement en mémoire et les charges de travail d'analyse en temps réel.

Storage Optimized (Optimisé pour le stockage) : Ces instances sont parfaites pour les applications nécessitant des IOPS élevés (opérations d'entrée/sortie par seconde), comme les bases de données NoSQL, les systèmes de fichiers distribués et les entrepôts de données.

Accelerated Computing (Calcul accéléré) : Ces instances utilisent des GPU ou des FPGA pour des charges de travail spécialisées nécessitant des performances de calcul parallèles massives, comme le machine learning, les simulations scientifiques et le rendu 3D.

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

- **EC2 User Data** est un moyen de passer des informations ou des scripts à une instance EC2 lors de son lancement. Ces données peuvent être utilisées pour effectuer des configurations automatisées ou exécuter des commandes spécifiques au démarrage de l'instance.

Utilisation de EC2 User Data :

Initialisation de l'instance : Automatiser des configurations initiales telles que la mise à jour de logiciels, l'installation de paquets, la configuration de services, etc.

Script de démarrage : Exécuter des scripts bash ou des commandes PowerShell au démarrage de l'instance.

Provisioning : Déployer des applications ou des configurations spécifiques à partir du moment où l'instance devient opérationnelle.

Quelles sont les types d'instances qui existent ?

- Les types d'instances EC2 sont classifiés en plusieurs familles en fonction de leur usage spécifique :

General Purpose (Usage général) :

Exemples : t3, t4g, m5, m6g

Utilisation : Applications nécessitant un équilibre entre CPU, mémoire et réseau.

Compute Optimized (Optimisé pour le calcul) :

Exemples : c5, c6g

Utilisation : Charges de travail nécessitant des performances élevées du processeur comme le traitement de batch, les serveurs web haute performance.

Memory Optimized (Optimisé pour la mémoire) :

Exemples : r5, r6g, x1e

Utilisation : Applications nécessitant un accès rapide et important à la mémoire, comme les bases de données en mémoire.

Storage Optimized (Optimisé pour le stockage) :

Exemples : i3, d2

Utilisation : Charges de travail nécessitant des IOPS élevés et un accès rapide au stockage, comme les bases de données NoSQL.

Accelerated Computing (Calcul accéléré) :

Exemples : p3, p4, g4, f1

Utilisation : Applications nécessitant des GPU pour le machine learning, le rendu graphique, ou des FPGA pour les calculs personnalisés.

JOB 9

- Étape 1 : Accéder à la Console AWS EC2
Je me suis connecté à la console AWS et j'ai navigué vers le service EC2.
- Étape 2 : Lancer une Nouvelle Instance
J'ai cliqué sur le bouton "**Lancer des instances**" pour créer une nouvelle instance.
- Étape 3 : Configurer les Détails de l'Instance

Nom de l'Instance :

J'ai donné le nom "Serveur Web Dev" à mon instance.

▼ Nom et balises Informations

Clé Informations

Valeur Informations

Types de ressources Informations

Q Name X

Q Serveur Web De' X

Sélectionner les ty... ▼

Instances X

Supprimer

Ajouter une balise

Vous pouvez ajouter jusqu'à 49 balises supplémentaires.

Image d'Exécution :

J'ai sélectionné l'image "Amazon Linux 2 AMI (HVM), SSD Volume Type".

Démarrage rapide

Launch an instance

Amazon Linux

aws

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Explorer plus d'AMI

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

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

Description

Amazon Linux 2023 est un système d'exploitation moderne basé sur Linux, à usage général et offrant cinq ans de support garanti. Optimisé pour AWS, il est conçu afin de fournir un environnement d'exécution sécurisé, stable et à hautes performances pour le développement et l'exécution de vos applications cloud.

Amazon Linux 2023 AMI 2023.6.20241031.0 x86_64 HVM kernel-6.1

Architecture

Mode de démarrage

ID AMI

Nom d'utilisateur

64 bits (x86)

uefi-preferred

ami-0db5e28c1b3823bb7

ec2-user

Fournisseur vérifié

Type d'Instance :

J'ai choisi l'instance de type **t2.micro**, qui est la plus petite et gratuite dans le cadre du niveau

de gratuité d’AWS.

Launch an instance

Infos

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 Gio

Annulez

Lancer l'instance

 Code de prévisualisation

Key Pair :

J’ai généré une nouvelle paire de clés en cliquant sur “**crée une pair de clé**”, puis j’ai téléchargé le fichier .pem correspondant. Cette clé sera utilisée pour se connecter à l’instance via SSH.

un trafic spécifique à atteindre votre instance.

☒ Créer un groupe de sécurité

☐ Sélectionner un groupe de sécurité existant

Nom du groupe de sécurité - obligatoire

ServeurWebDevSG

Ce groupe de sécurité sera ajouté à toutes les interfaces réseau. Le nom ne peut pas être modifié après la création du groupe de sécurité. La longueur maximale est de 255 caractères. Caractères valides : a-z, A-Z, 0-9, espaces et _ - : / () # , @ [] + = & ; { } ! \$ *

Description - obligatoire Informations

Groupe de securite pour le serveur web de developpement.

Règles entrantes des groupes de sécurité

Launch an instance

▼ Règle de groupe de sécurité 1 (TCP, 22, 0.0.0.0/0)

Supprimer

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

0.0.0.0/0 ✕

Description - facultatif

Informations

par exemple, SSH pour le bureau de

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

Supprimer

Type Informations

HTTP

Protocole Informations

TCP

Plage de ports Informations

80

Type de source Informations

N'importe où

Source Informations

🔍 Ajouter une adresse CIDR, une

0.0.0.0/0 ✕

Description - facultatif

Informations

par exemple, SSH pour le bureau de

▼ Règle de groupe de sécurité 3 (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

Stockage :

J'ai configuré le stockage avec un volume gp2 de 8 Go.

- Étape 4 : Configurer les Scripts User Data

J'ai ajouté un script bash dans la section “**User Data**” pour déployer un serveur web automatiquement à la création de l'instance. Voici le script que j'ai utilisé

Données utilisateur **Launch an instance** **Informations**

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

📁 Choisir un fichier

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<html><h1>Bienvenue sur le Serveur Web Dev</h1></html>" >
/var/www/html/index.html
```

☐ Les données utilisateur ont déjà été codées en base64

- Étape 5 : Lancer l'Instance

Après avoir vérifié toutes les configurations, j'ai cliqué sur “**démarrer l'instance**”

- Étape 7 : Accès via un Navigateur Web

J'ai ouvert un navigateur web et saisi l'adresse IP publique de l'instance. La page affichait "Bienvenue sur le Serveur Web Dev", confirmant que le déploiement avait réussi.

The image shows two screenshots. The top screenshot is from the AWS Management Console, displaying a list of instances. The instance 'i-002b1ad3e82d59745' (Serveur Web Dev) is highlighted, showing its state as 'En cours d'exécution' (Running) and its public IP address as 35.180.100.228. The bottom screenshot is a browser window showing the URL 'https://35.180.100.228' and the page content 'Bienvenue sur le Serveur Web Dev'.

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

Name	ID d'instance	État de l'instance	Type d'instance	Contrôle des statuts	Statut d'alarme	Zone de disponibilité
Serveur Web ...	i-002b1ad3e82d59745	En cours d'exécution	t2.micro	2/2 vérifications réussies	Afficher les alarmes	eu-west-3c

i-002b1ad3e82d59745 (Serveur Web Dev)

[Détails](#) [Statuts et alarmes](#) [Surveillance](#) [Sécurité](#) [Mise en réseau](#) [Stockage](#) [Balises](#)

▼ Résumé de l'instance Informations

ID d'instance i-002b1ad3e82d59745	Adresse IPv4 publique 35.180.100.228 adresse ouverte	Adresses IPv4 privées 172.31.32.85
Adresse IPv6 -	État de l'instance En cours d'exécution	DNS IPv4 public ec2-35-180-100-228.eu-west-3.compute.amazonaws.com adresse ouverte
Type de nom d'hôte Nom de l'adresse IP: ip-172-31-32-85.eu-west-3.compute.internal	Nom DNS de l'IP privé (IPv4 uniquement) ip-172-31-32-85.eu-west-3.compute.internal	Adresses IP élastiques -
Réponse à un nom DNS de ressource privée IPv4 (A)	Type d'instance t2.micro	Backups d'AMI Compute Optimized
Adresse IP attribuée automatiquement	ID de VPC	

Non sécurisé — 51.44.15.35

[Intra - L...](#) [RTS](#) [book 9...](#) [Instanc...](#) [https://...](#)

Bienvenue sur le Serveur Web Dev

JOB 10

Je vais me connecter à mon instance EC2 via SSH pour permettre aux développeurs d'y accéder. Voici comment je procède

Je récupère l'adresse publique de mon instance EC2 dans la console AWS, sous **Public IPv4 Address**

Ensuite, je lance cette commande dans mon terminal :

```
ssh -i ~/Documents/DevServerKeyPair.pem ec2-user@35.180.100.228
```

Une fois connecté, je vois une invite comme celle-ci dans mon terminal

```
-----
Air-de-User:Documents user$ ssh -i ~/Documents/DevServerKeyPair.pem ec2-user@35.180.100.228

A newer release of "Amazon Linux" is available.
Version 2023.6.20241111:
Run "/usr/bin/dnf check-release-update" for full release and version update info

#_
~\_##### Amazon Linux 2023
~\_#####\
~\_###|
~\_#/_---- https://aws.amazon.com/linux/amazon-linux-2023
~\_V~' ' ->
~\_/
~\_/
~\_/
~\_/

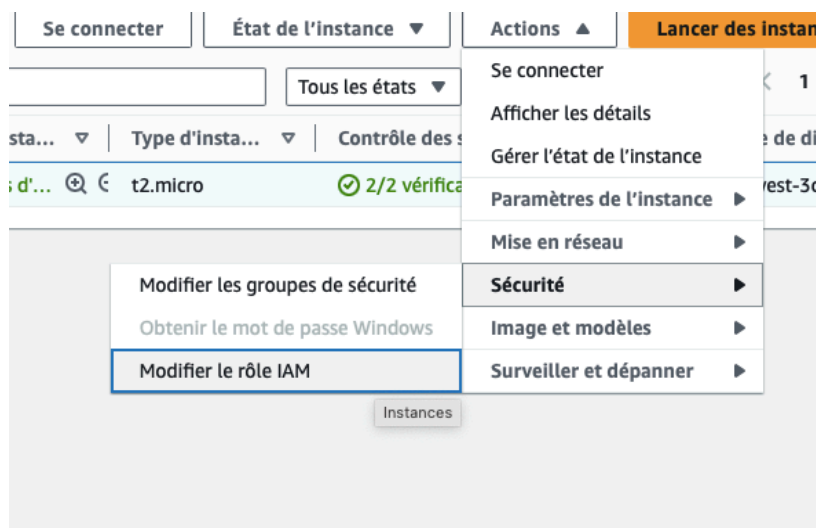
[[ec2-user@ip-172-31-32-85 ~]$ sudo systemctl ststus httpd
Unknown command verb ststus.
[[ec2-user@ip-172-31-32-85 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Tue 2024-11-12 10:48:30 UTC; 6 days ago
     Docs: man:httpd.service(8)
  Process: 345600 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 1997 (httpd)
    Status: "Total requests: 17421; Idle/Busy workers 100/0;Requests/sec: 0.0327; Bytes served/s"
      Tasks: 230 (limit: 1113)
    Memory: 30.7M
       CPU: 5min 54.215s
    CGroup: /system.slice/httpd.service
            └─ 1997 /usr/sbin/httpd -DFOREGROUND
              └─ 345603 /usr/sbin/httpd -DFOREGROUND
                └─ 345604 /usr/sbin/httpd -DFOREGROUND
                  └─ 345605 /usr/sbin/httpd -DFOREGROUND
                    └─ 345606 /usr/sbin/httpd -DFOREGROUND
                      └─ 355708 /usr/sbin/httpd -DFOREGROUND

Nov 12 10:48:30 ip-172-31-32-85.eu-west-3.compute.internal systemd[1]: Starting httpd.service - T>
Nov 12 10:48:30 ip-172-31-32-85.eu-west-3.compute.internal systemd[1]: Started httpd.service - Th>
Nov 12 10:48:30 ip-172-31-32-85.eu-west-3.compute.internal httpd[1997]: Server configured, listen>
Nov 17 00:00:04 ip-172-31-32-85.eu-west-3.compute.internal systemd[1]: Reloading httpd.service - >
```

JOB 11

Attribuer le rôle IAM à mon instance

Je vais dans la console AWS, dans la section EC2. Je sélectionne mon instance et je clique sur **“Modify IAM Role”**. Là, je choisis le rôle IAM que j’avais créé lors de l’étape précédente. Une fois sélectionné, je mets à jour.



Modifier le rôle IAM [Informations](#)

Attachez un rôle IAM à votre instance.

ID d'instance

 i-002b1ad3e1... (Serveur Web Dev)

[Modifier le rôle IAM](#)

Rôle IAM

Sélectionner un rôle IAM à attacher à votre instance ou créer un rôle si vous n'en avez pas encore créé. Le rôle que vous sélectionnez remplace tous les rôles actuellement attachés à votre instance.

DemoForEC2



[Créer un nouveau rôle IAM](#) 

Annulez

Mettre à jour le rôle IAM

Une fois dans l'instance , je tape cette commande pour vérifier que le rôle IAM fonctionne :

```
lines 1-24/24 (END)
[ec2-user@ip-172-31-32-85 ~]$ aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "bill_gates",
      "UserId": "AIDAXBZV5IXKJZL2AI2RI",
      "Arn": "arn:aws:iam::484907501012:user/bill_gates",
      "CreateDate": "2024-11-04T13:32:01+00:00"
    },
    {
      "Path": "/",
      "UserName": "elon_musk",
      "UserId": "AIDAXBZV5IXKC7PKR5PGM",
      "Arn": "arn:aws:iam::484907501012:user/elon_musk",
      "CreateDate": "2024-11-04T13:04:40+00:00"
    },
    {
      "Path": "/",
      "UserName": "jeff_bezos",
      "UserId": "AIDAXBZV5IXKJZ4GX7P7J",
      "Arn": "arn:aws:iam::484907501012:user/jeff_bezos",
      "CreateDate": "2024-11-04T13:01:30+00:00"
    },
    {
      "Path": "/",
      "UserName": "mark_zuckerberg",
      "UserId": "AIDAXBZV5IXKCN56Z3JUN",
      "Arn": "arn:aws:iam::484907501012:user/mark_zuckerberg",
      "CreateDate": "2024-11-04T13:29:39+00:00"
    },
    {
      "Path": "/",
      "UserName": "steve_jobs",
      "UserId": "AIDAXBZV5IXKD63JE3R72",
      "Arn": "arn:aws:iam::484907501012:user/steve_jobs",
      "CreateDate": "2024-11-04T13:31:28+00:00"
    },
    {
      "Path": "/",
      "UserName": "tara_derri",
      "UserId": "AIDAXBZV5IXKBKLSFXJCY",
      "Arn": "arn:aws:iam::484907501012:user/tara_derri",
      "CreateDate": "2024-11-04T13:31:28+00:00"
    }
  ],
  "IsTruncated": false
}
: ... skipping ...
{
  "Users": [
    {
      "Path": "/",
      "UserName": "bill_gates",
      "UserId": "AIDAXBZV5IXKJZL2AI2RI",
      "Arn": "arn:aws:iam::484907501012:user/bill_gates",
      "CreateDate": "2024-11-04T13:32:01+00:00"
    },
    {
      "Path": "/",
      "UserName": "elon_musk",
      "UserId": "AIDAXBZV5IXKC7PKR5PGM",
      "Arn": "arn:aws:iam::484907501012:user/elon_musk",
      "CreateDate": "2024-11-04T13:04:40+00:00"
    },
    {
      "Path": "/",
      "UserName": "jeff_bezos",
      "UserId": "AIDAXBZV5IXKJZ4GX7P7J",
      "Arn": "arn:aws:iam::484907501012:user/jeff_bezos",
      "CreateDate": "2024-11-04T13:01:30+00:00"
    },
    {
      "Path": "/",
      "UserName": "mark_zuckerberg",
      "UserId": "AIDAXBZV5IXKCN56Z3JUN",
      "Arn": "arn:aws:iam::484907501012:user/mark_zuckerberg",
      "CreateDate": "2024-11-04T13:29:39+00:00"
    },
    {
      "Path": "/",
      "UserName": "steve_jobs",
      "UserId": "AIDAXBZV5IXKD63JE3R72",
      "Arn": "arn:aws:iam::484907501012:user/steve_jobs",
      "CreateDate": "2024-11-04T13:31:28+00:00"
    },
    {
      "Path": "/",
      "UserName": "tara_derri",
      "UserId": "AIDAXBZV5IXKBKLSFXJCY",
      "Arn": "arn:aws:iam::484907501012:user/tara_derri",
      "CreateDate": "2024-11-04T13:31:28+00:00"
    }
  ],
  "IsTruncated": false
}
```


JOB 12

Rapport sur les Options d'Achat d'Instances EC2 pour Optimiser les Coûts

Dans ce rapport, je vais détailler les différentes options d'achat d'instances EC2 sur AWS. Ces options me permettront de mieux comprendre comment optimiser les coûts en fonction des besoins de performance, de flexibilité et du budget.

- **Instances à la Demande (On-Demand Instances)**

Les **instances à la demande** sont idéales pour les utilisateurs qui n'ont pas de prévision sur la durée ou la quantité d'utilisation des ressources. Elles sont facturées à l'heure ou à la seconde en fonction de l'instance choisie.

Avantages :

Flexibilité totale sans engagement de durée.

Idéales pour les applications qui sont imprévisibles ou temporaires.

Inconvénients :

Les coûts peuvent rapidement augmenter si l'utilisation est élevée sur le long terme.

Cas d'utilisation :

Développement ou tests à court terme.

Applications avec des pics de demande imprévisibles.

- **Instances Réservées (Reserved Instances)**

Les **instances réservées** me permettent de m'engager à utiliser une instance pendant 1 à 3 ans en échange de réductions sur les tarifs. Cette option est idéale pour les environnements de production stables où l'on connaît à l'avance la demande en ressources.

Avantages :

Réductions significatives sur les tarifs (jusqu'à 75 % par rapport aux instances à la demande).

Engagement à long terme avec une planification de la capacité.

Inconvénients :

Nécessitent un engagement à long terme, ce qui n'est pas idéal si les besoins changent fréquemment.

Moins flexibles si les exigences de la charge de travail évoluent.

Cas d'utilisation typiques :

Applications critiques en production.

Serveurs de bases de données ou autres applications avec une demande stable.

- **Instances Spot (Spot Instances)**

Les **instances spot** offrent une capacité de calcul excédentaire à prix réduit, en utilisant des ressources non utilisées d’AWS. Cependant, AWS peut récupérer ces instances à tout moment si la demande pour des ressources augmente, ce qui peut interrompre vos applications.

Avantages :

Coût très bas, pouvant atteindre jusqu’à 90 % de réduction par rapport aux instances à la demande.

Idéales pour des tâches qui sont tolérantes aux interruptions.

Inconvénients :

Risque d’interruption à tout moment.

Pas adaptées aux applications critiques.

Cas d’utilisation typiques :

Traitement de données en batch.

Calculs scientifiques ou simulations.

Conclusion : AWS offre une large gamme d’options tarifaires pour EC2, chacune ayant des avantages spécifiques en fonction des besoins de performance, de coût et de flexibilité. Si vous avez des besoins flexibles et variables, les **instances à la demande** et les **Spot Instances** sont de bonnes options. Si vous avez des besoins à long terme et stables, les **Instances réservées** ou les **Savings Plans** offrent des économies significatives.

Les **Hôtes dédiés** et les **On-Demand Capacity Reservations** peuvent être intéressants dans des situations très spécifiques où la conformité ou la capacité réservée sont cruciales.

JOB 13

Voici comment je procède pour effectuer un **snapshot** de mon volume attaché à l’instance “Serveur Web Dev” et ensuite arrêter et résilier l’instance sur Amazon EC2 :

1. Effectuer un Snapshot du Volume Attaché à l’Instance “Serveur Web Dev”

Accéder aux Volumes :

Dans le menu de gauche, sous la section “Elastic Block Store”, je sélectionne **Volumes**.

Sélectionner le Volume Attache à l’Instance :

Je trouve le volume attaché à mon instance “Serveur Web Dev” dans la liste des volumes.

Je coche la case à côté de ce volume

Créer un Snapshot :

Je clique sur **Actions** en haut de la page, puis je sélectionne **Create Snapshot** dans le menu déroulant.

Dans la fenêtre qui apparaît, je donne un **nom** et une **description** à mon snapshot (par exemple : “Snapshot Serveur Web Dev”).

Je clique ensuite sur **Create Snapshot**.

Actions ▲

Modifier le volume

Créer un instantané

Créer une stratégie de cycle de Volumes instantané

Supprimer le volume

Attacher un volume

Détacher un volume

Forcer le détachement de volume

Gérer les E/S activées automatiquement

Gérer les balises

Injection de perturbations ▶


pe ▼	Taille ▼	ID	Créé
2	8 GiB	1	2024/

Créer un instantané [Informations](#)

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

Volume source

ID du volume

 vol-0ccb66db2c64c0686

Zone de disponibilité

eu-west-3c

Détails de l'instantané

Description

Ajouter une description pour votre instantané

Snapshot Serveur Web Dev

255 caractères maximum.

Chiffrement [Informations](#)

Non chiffré

Annuler

Créer un instantané

Créer un instantané

2. Arrêter et Résilier l'Instance "Serveur Web Dev"

Arrêter l'Instance :

Je sélectionne l'instance "Serveur Web Dev" et clique sur **Actions**.

Ensuite, je vais dans **Instance State** et je choisis **Stop** pour arrêter l'instance. Cela met l'instance en état d'arrêt sans la supprimer, ce qui permet de la redémarrer plus tard si nécessaire.

Gérer l'état de l'instance

Instance details

i-002b1ad3e82d59745 (Serveur Web Dev)

running

Paramètres d'état de l'instance

- ☐ Début
Disponible lorsque l'instance est arrêtée
- ☒ Stop (Arrêter)
- ☐ Mettre en veille prolongée
Arrêt était absent pour cette instance – La mise en veille prolongée était activée lors du lancement.
- ☐ Redémarrer
- ☐ Terminate (Résilier)



Notez que lorsque vos instances sont arrêtées :

Toute donnée relative au magasin éphémère de vos instances sera perdue.



Gérer l'état de l'instance

Annulez

Modifier l'état

Résilier l'Instance :

Si je souhaite complètement supprimer l'instance et éviter toute facturation future, je dois **terminer l'instance**.

Je sélectionne à nouveau **Actions**, puis **Instance State**, et je choisis **Terminate**.

Une fenêtre de confirmation apparaît, je confirme que je veux terminer l'instance. Attention, une fois l'instance terminée, toutes les données sur l'instance seront supprimées (à moins d'avoir sauvegardé les données ailleurs, comme dans un snapshot).

Gérer l'état de l'instance

Instance details

i-002b1ad3e82d59745 (Serveur Web Dev)

stopped

Paramètres d'état de l'instance

- ☐ Début
- ☐ Stop (Arrêter)
Disponibile lorsque l'instance est en cours d'exécution
- ☐ Mettre en veille prolongée
Disponibile lorsque l'instance est en cours d'exécution
- ☐ Redémarrer
Disponibile lorsque l'instance est en cours d'exécution
- ☒ Terminate (Résilier)




Notez que lorsque vos instances sont résiliées :

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.



Annulez

Modifier l'état

 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-002b1ad3e82d59745 (Serveur Web Dev)	 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)**

Je viens de créer un **snapshot** de mon volume, ce qui me permet de le sauvegarder pour plus tard, puis j'ai arrêté et résilié l'instance "Serveur Web Dev". Cela m'évite de continuer à être facturé pour l'instance qui n'est plus en service .