

# Projet AWS

## Job 01

### Déployer une application web sur un serveur EC2 avec mise à l'échelle automatique

Etapes:

- 1.[Création de l'infrastructure AWS - VPC et sous-réseaux](#)
  - 2.[Configurer les groupes de sécurité](#)
  - 3.[Créer une instance EC2 avec Launch Template](#)
  - 4.[Configuration d'un Application Load Balancer \(ALB\)](#)
  - 5.[Configurer l'Auto Scaling Group \(ASG\)](#)
  - 6.[Tests et validation](#)
- 

#### 1.Création de l'infrastructure AWS - VPC et sous-réseaux

##### 1. Créez un VPC :

- Accédez à VPC > Créez un VPC.
- Nom : `my-vpc-01`.
- CIDR : `10.0.0.0/24` (plage de 256 adresses).

##### 2. Créez deux sous-réseaux publics :

- Sous-réseau 1 :
  - Nom : `my-subnet-01`.
  - CIDR : `10.0.0.0/28` (adresses de `10.0.0.0` à `10.0.0.15`).
  - Zone de disponibilité : `eu-west-3a`.
- Sous-réseau 2 (*nous aurons besoin de ça plus tard dans le cadre de la mise en place de l'Auto Scaling Group et Application Load Balancer*) :
  - Nom : `my-subnet-02`.
  - CIDR : `10.0.0.16/28` (adresses de `10.0.0.16` à `10.0.0.31`).
  - Zone de disponibilité : `eu-west-3b`.

##### 3. Créez une passerelle Internet :

- Nom : `my-internet-gateway`.
- Attachez-la au VPC (`my-vpc-01`).

#### 4. Configurer la table de routage :

- Créez une table de routage publique **my-route-table-01**.
- Ajoutez une route :
  - Destination : **0.0.0.0/0**.
  - Cible : **my-internet-gateway**.
- Associez cette table de routage aux deux sous-réseaux (**my-subnet-01** et **my-subnet-02**).

## 2. Configurer les groupes de sécurité

### Créer un groupe de sécurité pour l'instance EC2 :

- Nom : **web-server-sg**.
- **Règles entrantes** :
  - Port 22 (SSH) : Autorisez uniquement votre IP (**203.0.113.0/32**).
  - Port 80 (HTTP) : Autorisez tout (**0.0.0.0/0**).
- **Règles sortantes** :
  - Autorisez tout (**0.0.0.0/0**).

## 3. Créer une instance EC2 avec Launch Template

### Créer un modèle de lancement (Launch Template) :

- Nom : **web-server-template**.

#### Créer un modèle de lancement

La création d'un modèle de lancement vous permet de créer une configuration d'instance enregistrée qui peut être réutilisée, partagée et lancée ultérieurement. Les modèles peuvent avoir plusieurs versions.

Nom et description du modèle de lancement

Nom du modèle de lancement - **obligatoire**  
  
Doit être propre à ce compte. 128 caractères au maximum. Pas d'espaces ni de caractères spéciaux tels que « & », « \* », « @ ».

Description de la version du modèle  
  
255 caractères maximum

Instructions relatives à Auto Scaling | [Informations](#)  
Sélectionnez cette option si vous avez l'intention d'utiliser ce modèle avec EC2 Auto Scaling.  
 Fournir des instructions pour vous aider à configurer un modèle que vous pouvez utiliser avec EC2 Auto Scaling.

- AMI : Amazon Linux 2.
- Type d'instance : **t2.micro**

[EC2](#) > [Modèles de lancement](#) > [Créer un modèle de lancement](#)

Récentes      Démarrage rapide

Amazon Machine Image (AMI)

AMI Amazon Linux 2023  
ami-0f38b927e6597da05 (64 bits (x86), uefi-preferred) / ami-0d9394d73f29efa99 (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 2023.6.20250115.0 x86\_64 HVM kernel-6.1

Architecture	Mode de démarrage	ID AMI	Nom d'utilisateur	
64 bits (x86)	uefi-preferred	ami-0f38b927e6597da05	ec2-user	Fournisseur vérifié

▼ Type d'instance [Informations](#) | [Obtenez des conseils](#)      Avancé

Type d'instance

t2.micro  
Famille: t2 1 vCPU 1 Go Mémoire Génération actuelle: true À la demande RHEL base tarification: 0.0276 USD per Hour  
À la demande SUSE base tarification: 0.0132 USD per Hour À la demande Linux base tarification: 0.0132 USD per Hour  
À la demande Ubuntu Pro base tarification: 0.015 USD per Hour À la demande Windows base tarification: 0.0178 USD per Hour

Éligible à l'offre gratuite

Toutes les générations

[Comparer les types d'instance](#)

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

- Key Pair : Utilisez une paire de clés existante ou en créez une nouvelle.

▼ 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

WebAppServer.key

[Créer une paire de clés](#)

- Sous-réseau : my-subnet-01.( pas sur que ce soit à faire dans le cadre de Auto Scaling
- Groupe de sécurité : **web-server-sg**.

▼ Paramètres réseau [Informations](#)

Sous-réseau [Informations](#)

Ne pas inclure dans le modèle de lancement

Lorsque vous indiquez un sous-réseau, une interface réseau est automatiquement ajoutée à votre modèle.

[Créer un nouveau sous-réseau](#)

Par-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.

Sélectionner un groupe de sécurité existant       Créez un groupe de sécurité

Groupes de sécurité [Informations](#)

Sélectionnez les groupes de sécurité

web-server-SG sg-09562580fe87ccbc7 X  
VPC: vpc-035a5a3421dfa28d

[Comparer les règles de groupe de sécurité](#)

► Configuration réseau avancée

- Stockage : Volume par défaut (8 Go GP2).

▼ Stockage (volumes) [Informations](#)

**EBS Volumes**

**Masquer les informations**

▶ Volume 1 (Racine AMI) (8 Gio, EBS, SSD à usage général (gp3), 3000 IOPS)  
Les volumes AMI ne sont pas inclus dans le modèle. Ils ne peuvent l'être que si l'on modifie.

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](#)

- Ajouter le script dans le modèle de lancement dans l'onglet **Détails avancées > Données utilisateur**
- Collez le script

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

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

↑ Choisir un fichier

```
#!/bin/bash
# Met à jour les paquets
yum update -y

# Installe Apache
yum install httpd -y

# Démarrer Apache
systemctl start httpd
systemctl enable httpd

# Crée une page HTML personnalisée
cat <<EOF > /var/www/html/index.html
<!DOCTYPE html>
<html lang="fr">
```

Ci-dessus un exemple de script Bash permettent d'installer Apache et configurer une page web de test.

```
#!/bin/bash

# Met à jour les paquets
yum update -y

# Installe Apache
yum install httpd -y

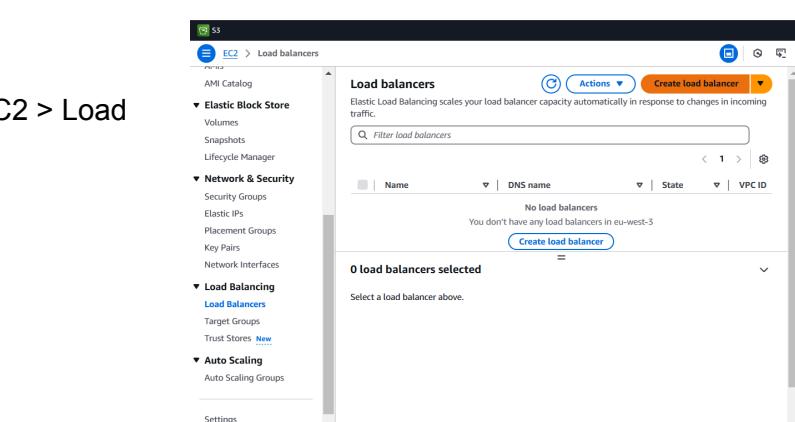
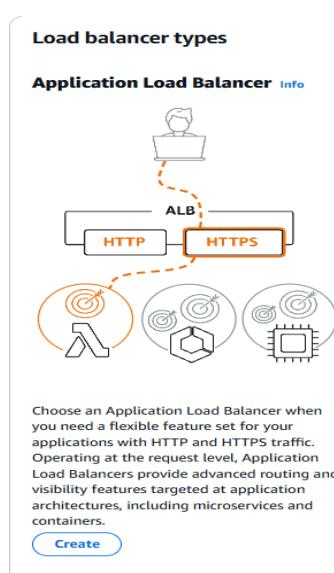
# Démarre Apache
systemctl start httpd
systemctl enable httpd

# Crée une page web par défaut
echo "<html><h1>Bienvenue sur mon serveur Apache</h1></html>" >
/var/www/html/index.html
```

## 4. Configuration d'un Application Load Balancer (ALB)

### Créer un Load Balancer

- Accédez à la console EC2 > Load Balancers.



- Cliquez sur Crée un Load Balancer et choisissez Application Load Balancer.

- Configurez les paramètres :

- Nom : **web-server-alb**.
- Type : Internet-facing.

## Configuration de base

### Nom de l'équilibrEUR de charge

Le nom doit être unique au sein de votre compte AWS et ne peut pas être modifié une fois l'équilibrEUR de charge créé.

**web-server-alb**

32 caractères alphanumériques au maximum, y compris les traits d'union, sont autorisés mais le nom ne doit pas commencer ou se terminer par un trait d'union.

### Méthode | Infos

Le schéma ne peut pas être modifié après la création de l'équilibrEUR de charge.

#### Accessible sur Internet

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

#### Interne

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible avec les types d'adresses IP IPv4 et Dualstack.

- Listener : HTTP sur le port 80.

## Groupes de sécurité Infos

Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic vers votre équilibrEUR de charge. Sélectionnez un groupe de sécurité existant ou vous pouvez [créer un nouveau groupe de sécurité](#).

### Groupes de sécurité

Sélectionner jusqu'à 5 groupes de sécurité



launch-wizard-2

sg-0880f2993de6c4c85 VPC: vpc-086a305ca2d18dfc9

## Écouteurs et routage Infos

Un écouteur est un processus qui vérifie les demandes de connexion à l'aide du port et du protocole que vous configurez. Les règles que vous définissez pour un écouteur déterminent la façon dont l'équilibrEUR de charge achemine les demandes vers ses cibles enregistrées.

### ▼ Écouteur HTTP:80

Supprimer

#### Protocole

#### Port

HTTP

: 80

1-65535

#### Action par défaut | Infos

Réacheminer vers

Sélectionner un groupe cible

▼

Créer un groupe cible

### Balises d'écouteur - facultatif

Envisagez d'ajouter des balises à votre écouteur. Les balises permettent de classer vos ressources AWS afin de les gérer plus facilement.

Ajouter une balise d'écouteur

Vous pouvez ajouter jusqu'à 50 balises de plus.

- Zones de disponibilité : Sélectionnez les sous-réseaux publics (par exemple, **my-subnet-01**).
- Cliquez sur Suivant pour continuer.

**Mappage réseau** [Infos](#)

L'équilibrer de charge achemine le trafic, conformément à vos paramètres d'adresses IP, vers les cibles des sous-réseaux sélectionnés.

**VPC** | [Infos](#)

L'équilibrer de charge existera et évoluera au sein du VPC sélectionné. Le VPC sélectionné est également l'endroit où les cibles de l'équilibrer de charge doivent être hébergées, sauf si elles sont acheminées vers des cibles Lambda ou sur site, ou si vous utilisez le peering VPC. Pour confirmer le VPC de vos cibles, consultez les [groupes cibles](#). Pour un nouveau VPC, [créez-en un](#).

my-vpc-01  
 vpc-086a305ca2d18dfc9  
 CIDR VPC IPv4 : 10.0.0.0/24

**Mappages** | [Infos](#)

Sélectionnez au moins deux zones de disponibilité et un sous-réseau par zone. L'équilibrer de charge achemine le trafic uniquement vers les cibles de ces zones de disponibilité. Les zones de disponibilité non prises en charge par l'équilibrer de charge ou par le VPC ne sont pas disponibles pour la sélection.

**Zones de disponibilité**

eu-west-3a (euw3-az1)

**Sous-réseau**

subnet-0f193dce4d2f1874e      my-subnet-01

**Adresse IPv4**  
Attribuées par AWS

## 2. Configurer les groupes cibles

- Créez un nouveau groupe cible :
  - Type de cible : Instances.

≡ EC2 > [Groupes cibles](#) > Créer un groupe cible

Etape 1 **Spécifier les informations de groupe**

Etape 2 Enregistrer les cibles

**Spécifier les informations de groupe**

Votre équilibrer de charge achemine les demandes vers les cibles d'un groupe cible et effectue des vérifications de l'état sur les cibles.

**Configuration de base**

Les paramètres de cette section ne peuvent pas être modifiés après la création du groupe cible.

**Choisir un type de cible**

Instances
 

- Prend en charge l'équilibrage de charge dans les instances dans un VPC spécifique.
- Facilite l'utilisation d'[Amazon EC2 Auto Scaling](#) pour gérer et mettre à l'échelle votre capacité EC2.

Adresses IP
 

- Prend en charge l'équilibrage de charge sur les ressources VPC et sur site.
- Facilite le routage vers plusieurs adresses IP et interfaces réseau sur la même instance.
- Offre une flexibilité avec les architectures basées sur des microservices, ce qui simplifie la communication entre les applications.
- Prend en charge les cibles IPv6, ce qui permet la communication IPv6 de bout en bout et le protocole NAT IPv4-to-IPv6.

- Nom : **web-server-target-group**.

### Nom du groupe cible

32 caractères alphanumériques au maximum, y compris les traits d'union, sont autorisés mais le nom ne doit pas commencer ou se terminer par un trait d'union.

- Vérifications de santé (Health Checks) :
  - Protocole : HTTP.
  - Chemin : **/** (ou **/index.html** si applicable).

**Surveillances de l'état**

L'équilibrer de charge associe envoie régulièrement des demandes, conformément aux paramètres ci-dessous, aux cibles enregistrées afin de tester leur état.

**Protocole de vérification de l'état**

HTTP

**Chemin de vérification de l'état**

Utilisez le chemin par défaut « / » pour effectuer des surveillances de l'état sur la racine ou, si vous le souhaitez, spécifiez un chemin personnalisé.

/var/www/html/index.html

1 024 caractères maximum sont autorisés.

► **Paramètres avancés de vérification de l'état**

- Enregistrez le groupe cible.

### 3. Finaliser le Load Balancer

- Revoyez la configuration et cliquez sur Créer.
- Notez l'URL DNS public du Load Balancer pour tester l'application.

## web-server-target-group

### Détails

arn:aws:elasticloadbalancing:eu-west-3:140023371742:targetgroup/web-server-target-group/c11ad

## 5. Configurer l'Auto Scaling Group (ASG)

### 1. Créer un Auto Scaling Group :

- Nom : **web-server-scaling-group**.
- Modèle de lancement : **web-server-template**.

The screenshot shows the AWS EC2 Auto Scaling 'Create New Auto Scaling Group' wizard, Step 1: Choisir un modèle de lancement. The 'Launch template' section is selected. The 'Nom' field contains 'web-server-scaling-group'. The 'Modèle de lancement' dropdown is set to 'web-server-template'. A note at the bottom states: 'Pour les comptes créés après le 31 mai 2023, la console EC2 prend uniquement en charge la création de groupes Auto Scaling avec des modèles de lancement. La création de groupes Auto Scaling avec des configurations de lancement n'est pas recommandée mais reste disponible via l'interface de ligne de commande et l'API jusqu'au 31 décembre 2023.'

- VPC : **my-vpc-01**.
- Sous-réseaux : Sélectionnez **my-subnet-01** et **my-subnet-02**.

## Réseau Info

Pour la plupart des applications, vous pouvez utiliser plusieurs zones de disponibilité et laisser EC2 Auto Scaling équilibrer vos instances entre les zones. Le VPC par défaut et les sous-réseaux par défaut conviennent pour démarrer rapidement.

### VPC

Choisissez le VPC qui définit le réseau virtuel de votre groupe Auto Scaling.

vpc-035a5a34211dfa28d (my-vpc-01)

10.0.0.0/24



[Créer un VPC](#)

### Zones de disponibilité et sous-réseaux

Définissez les zones de disponibilité et les sous-réseaux que votre groupe Auto Scaling peut utiliser dans le VPC choisi.

Sélectionner les zones de disponibilité et les sous-réseaux



eu-west-3a | subnet-06dc698b63968adfe (my-subnet-01) [X](#)

10.0.0.0/28

eu-west-3b | subnet-08a2453ec65c833f1 (my-subnet-02) [X](#)

10.0.0.16/28

[Créer un sous-réseau](#)

### Distribution des zones de disponibilité - nouveau

Auto Scaling équilibre automatiquement les instances entre les zones de disponibilité. Si des échecs de lancement se produisent dans une zone, sélectionnez une stratégie.

Meilleur effort équilibré

Si les lancements échouent dans une zone de disponibilité, Auto Scaling essaiera de lancer l'instance dans une autre zone de disponibilité saine.

Équilibré uniquement

Si les lancements échouent dans une zone de disponibilité, Auto Scaling continuera d'essayer de lancer les instances dans la zone de disponibilité défaillante afin de préserver l'équilibre de la répartition.

- Load Balancer : Sélectionnez **web-server-alb** et **web-server-target-group**.

## Attacher à un équilibrEUR de charge existant

Sélectionnez les équilibrEURS de charge que vous souhaitez attacher à votre groupe Auto Scaling.

Choisir parmi les groupes cibles de votre équilibrEUR de charge

Cette option vous permet d'attacher des Application Load Balancers, des Network Load Balancers ou des Gateway Load Balancers.

Choisir parmi les Classic Load Balancers

### Groupes cibles d'équilibrEUR de charge existants

Seuls les groupes cibles d'instance qui appartiennent au même VPC que votre groupe Auto Scaling sont disponibles pour la sélection.

Sélectionner des groupes cibles



web-server-target-group | HTTP [X](#)

Application Load Balancer: web-server-alb

## 2. Définir la capacité :

- Capacité minimale : 1.
- Capacité maximale : 5.
- Capacité souhaitée : 1.

## Taille du groupe Info

Définissez la taille initiale du groupe Auto Scaling. Après avoir créé le groupe, vous pouvez modifier sa taille en fonction de la demande, manuellement ou à l'aide de la mise à l'échelle automatique.

### Type de capacité souhaitée

Choisissez l'unité de mesure pour la valeur de capacité souhaitée. Les vCPU et la mémoire (GiB) ne sont pris en charge que pour les groupes d'instances mixtes configurés avec un ensemble d'attributs d'instances.

Unités (nombre d'instances)



### Capacité souhaitée

Spécifiez la taille de votre groupe.

1

## Mise à l'échelle Info

Vous pouvez redimensionner votre groupe Auto Scaling manuellement ou automatiquement en fonction de l'évolution de la demande.

### Limits de mise à l'échelle

Fixez des limites relatives à l'augmentation ou à la diminution de la capacité souhaitée.

#### Capacité minimale souhaitée

1

Inférieure ou égale à la capacité souhaitée

#### Capacité maximale souhaitée

5



Supérieure ou égale à la capacité souhaitée

### Mise à l'échelle automatique - facultatif

#### Choisir d'utiliser ou non une politique de suivi de cible | Info

Vous pouvez configurer d'autres politiques de mise à l'échelle basées sur les métriques et une mise à l'échelle planifiée après avoir créé votre groupe Auto Scaling.

Aucune politique de mise à l'échelle

Votre groupe Auto Scaling conservera sa taille initiale et ne sera pas redimensionné de manière dynamique en fonction de la demande.

Politique de suivi des objectifs et d'échelonnement

Choisissez une valeur cible et de métrique CloudWatch et laissez la politique de mise à l'échelle ajuster la capacité souhaitée proportionnellement à la valeur de la métrique.

### 3. Configurer les stratégies de mise à l'échelle :

- Augmentez les instances si l'utilisation CPU dépasse 70 % pendant 5 minutes.
- Diminuez les instances si l'utilisation CPU descend en dessous de 30 % pendant 5 minutes.

**Mise à l'échelle** [Info](#)  
Vous pouvez redimensionner votre groupe Auto Scaling manuellement ou automatiquement en fonction de l'évolution de la demande.

**Limites de mise à l'échelle**  
Fixez des limites relatives à l'augmentation ou à la diminution de la capacité souhaitée.

Capacité minimale souhaitée	Capacité maximale souhaitée
1	5

Inférieure ou égale à la capacité souhaitée      Supérieure ou égale à la capacité souhaitée

**Mise à l'échelle automatique - facultatif**  
**Choisir d'utiliser ou non une politique de suivi de cible** [Info](#)  
Vous pouvez configurer d'autres politiques de mise à l'échelle basées sur les métriques et une mise à l'échelle planifiée après avoir créé votre groupe Auto Scaling.

**Aucune politique de mise à l'échelle**  
Votre groupe Auto Scaling conservera sa taille initiale et ne sera pas redimensionné de manière dynamique en fonction de la demande.

**Politique de suivi des objectifs et d'échelonnement**  
Choisissez une valeur cible et de métrique CloudWatch et laissez la politique de mise à l'échelle ajuster la capacité souhaitée proportionnellement à la valeur de la métrique.

**Nom de politique de mise à l'échelle**  
Target Tracking Policy

**Type de métrique** [Info](#)  
Métrique surveillée qui permet de déterminer si l'utilisation des ressources est trop faible ou trop élevée. Si vous utilisez des métriques EC2, envisagez d'activer la surveillance détaillée afin d'améliorer les performances de mise à l'échelle.

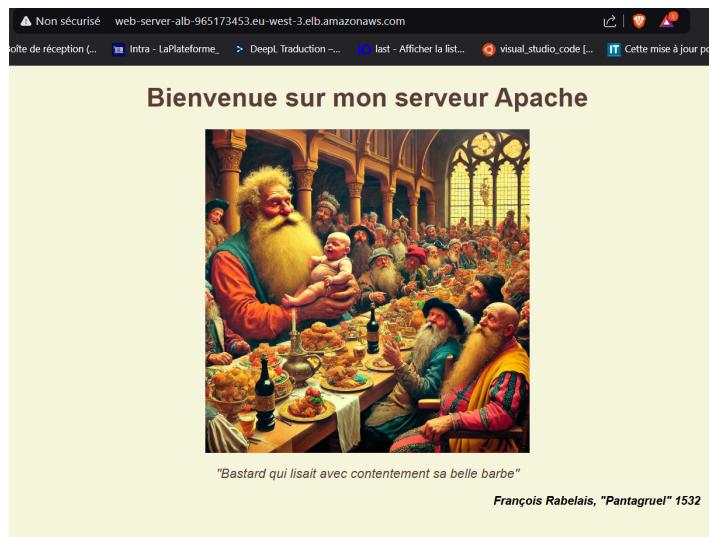
Utilisation moyenne du processeur

**Valeur cible**  
70

## 6. Tests et validation

### • Tester le Load Balancer :

- Accédez à l'URL DNS public du Load Balancer.
- Vous devriez voir votre page web s'afficher.



### • Tester l'Auto Scaling :

- Simulez une charge CPU pour vérifier que de nouvelles instances sont ajoutées automatiquement.
- Diminuez la charge pour vérifier que les instances inutiles sont supprimées.

Statut	Description	Cause	Heure de début	Heure de fin
Réussi	Terminating EC2 instance: i-04b5ef6b4cebe1c94	At 2025-01-20T13:41:11Z a monitor alarm TargetTracking-web-server-scaling-group-AlarmLow-a2ebb43f-fbc7-4262-9859-a0d69d82e923 in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 2 to 1. At 2025-01-20T13:41:19Z an instance was taken out of service in response to a difference between desired and actual capacity, shrinking the capacity from 2 to 1. At 2025-01-20T13:41:19Z instance i-04b5ef6b4cebe1c94 was selected for termination.	2025 January 20, 02:41:19 PM +01:00	2025 January 20, 02:47:24 PM +01:00
Réussi	Launching a new EC2 instance: i-061fc823acd04ff10	At 2025-01-20T13:24:25Z a monitor alarm TargetTracking-web-server-scaling-group-AlarmHigh-bdd6cc90-5026-4d8b-a94b-fdf5a20fe67 in state ALARM triggered policy Target Tracking Policy changing the desired capacity from 1 to 2. At 2025-01-20T13:24:31Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 1 to 2.	2025 January 20, 02:24:33 PM +01:00	2025 January 20, 02:29:39 PM +01:00
Réussi	Launching a new EC2 instance: i-04b5ef6b4cebe1c94	At 2025-01-19T21:10:16Z an instance was launched in response to an unhealthy instance needing to be replaced.	2025 January 19, 10:10:17 PM +01:00	2025 January 19, 10:10:24 PM +01:00
Réussi	Terminating EC2 instance: i-04a8179931ff4c1a9	At 2025-01-19T21:10:15Z an instance was taken out of service in response to an EC2 health check indicating it has been terminated or stopped.	2025 January 19, 10:10:16 PM +01:00	2025 January 19, 10:15:22 PM +01:00
Réussi	Launching a new EC2 instance: i-04a8179931ff4c1a9	At 2025-01-19T21:06:09Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 1. At 2025-01-19T21:06:20Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 1.	2025 January 19, 10:06:22 PM +01:00	2025 January 19, 10:06:29 PM +01:00

## Job 2

# Héberger un site web statique avec une distribution CloudFront pour une meilleure performance et sécurité.

### Ressources AWS utilisées :

- S3 (Simple Storage Service)** : Stockage des fichiers statiques.
- CloudFront** : Distribution mondiale et cache pour améliorer les performances.
- IAM (Identity and Access Management)** : Gestion des permissions.

Voici une documentation détaillée et optimisée pour l'objectif : héberger un site web statique avec S3 et CloudFront.

### Étapes

- 1. [Créer un bucket S3 pour héberger les fichiers statiques](#)
- 2. [Activer l'hébergement de site web sur le bucket S3](#)
- 3. [Configurer une distribution CloudFront](#)
- 4. [Attribuer une Stratégie de compartiment](#)

## 1. Créer un bucket S3 pour héberger les fichiers statiques

### 1. Accéder au service S3 :

- Connectez-vous à votre console AWS.
- Recherchez **S3** dans la barre de recherche et cliquez dessus.

### 2. Créer un bucket :

- Cliquez sur le bouton **Créer un bucket**.

Stockage

## Amazon S3

Stockez et récupérez n'importe quelle quantité de données, n'importe où

Amazon S3 est un service de stockage d'objet offrant une capacité de mise à l'échelle, une disponibilité des données, une sécurité et des performances de pointe.

**Créer un compartiment**

Chaque objet dans S3 est stocké dans un compartiment. Pour charger des fichiers et des dossiers dans S3, vous devez créer un compartiment dans lequel les objets seront stockés.

**Créer un compartiment**

- Donnez un nom unique à votre bucket (ex. **mon-site-web-statique**).

### Créer un compartiment Info

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

#### Configuration générale

##### Région AWS

Europe (Paris) eu-west-3

##### Nom du compartiment Info

mon-site-web-statique

Le nom du compartiment doit être unique dans l'espace de nommage global et respecter les règles de dénomination du compartiment. [Voir les règles relatives à la dénomination des compartiments](#)

##### Copier les paramètres depuis un compartiment existant - facultatif

Seuls les paramètres de compartiment dans la configuration suivante sont copiés.

##### Sélectionner un compartiment

Format : s3://bucket/prefix

- **Désactivez** le blocage de l'accès public (nécessaire pour un site web public) :
  - Décochez **Bloquer l'accès public à tous les paramètres**.
  - Confirmez en cochant la case **Je comprends**.

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

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

##### Bloquer tous les accès publics

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

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

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

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

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

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

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

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

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

⚠ Si le paramètre « Bloquer l'accès public » est désactivé, ce compartiment et les objets qu'il contient peuvent devenir publics.

AWS vous recommande de bloquer tout accès public, sauf si celui-ci est requis dans des cas d'utilisation spécifiques et vérifiés, tels que l'hébergement de site Web statique.

Je suis conscient, qu'avec les paramètres actuels, ce compartiment et les objets qu'il contient peuvent devenir publics.

- Cliquez sur **Créer le bucket**.
- 3. Téléverser les fichiers :**
- Entrez dans le bucket créé.
  - Cliquez sur **Télécharger** et ajoutez tous vos fichiers statiques (HTML, CSS, images, etc.).

Objets (4) <small>Info</small>		Copier l'URI S3	Copier l'URL	Télécharger	Ouvrir	Supprimer	Actions	Créer un dossier	Chargez
Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l' <a href="#">inventaire Amazon S3</a> pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. <a href="#">En savoir plus</a>									
<input type="text" value="Rechercher des objets en fonction du préfixe"/> <span style="float: right;">1</span>									
Nom	Type	Dernière modification	Taille	Classe de stockage					
<a href="#">f1_car2.png</a>	png	21 Jan 2025 04:59:14 PM CET	501.5 Ko	Standard					
<a href="#">f1_car3.png</a>	png	21 Jan 2025 04:59:15 PM CET	378.6 Ko	Standard					
<a href="#">f1_car6.png</a>	png	21 Jan 2025 04:59:18 PM CET	283.4 Ko	Standard					
<a href="#">index.html</a>	html	21 Jan 2025 04:59:18 PM CET	1.8 Ko	Standard					

## 2. Activer l'hébergement de site web sur le bucket S3

- 1. Configurer l'hébergement statique :**
- Dans les paramètres du bucket, allez à **Propriétés**.
  - Recherchez **Hébergement de site web statique** et cliquez sur **Modifier**.

**Hébergement de site Web statique**

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

**(i)** Nous vous recommandons d'utiliser AWS Amplify Hosting pour l'hébergement de sites Web statiques  
Déployez rapidement un site Web rapide, sécurisé et fiable avec AWS Amplify Hosting. Apprenez-en plus sur [Amplify Hosting](#) ou consultez vos applications Amplify existantes.

**Hébergement de site Web statique S3**  
Désactivé

- Cochez **Activer**.
- Spécifiez le fichier **index** (ex. `index.html`) comme document d'index.

**Hébergement de site Web statique**

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

**Hébergement de site Web statique**

Activer

**Type d'hébergement**

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

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

**(i)** Pour que vos clients puissent accéder au contenu au point de terminaison du site Web, vous devez rendre tout votre contenu publiquement visible. Pour ce faire, vous pouvez modifier les paramètres S3 Block Public Access pour le compartiment. Pour plus d'informations, consultez [Utilisation d'Amazon S3 Block Public Access](#).

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

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

Règles de redirection - facultatif

- Si un fichier d'erreur est nécessaire, ajoutez son nom (ex. `error.html`).
- 2. Obtenir l'URL du site web :**
- Une fois l'hébergement activé, une URL est générée (ex. `http://<nom-du-bucket>.s3-website-<région>.amazonaws.com`).
  - Copiez cette URL. Elle sera utilisée pour la configuration de CloudFront.
- 

### 3. Configurer une distribution CloudFront

- 1. Accéder au service CloudFront :**
  - Dans la console AWS, recherchez **CloudFront** et cliquez dessus.
- 2. Créer une nouvelle distribution :**
  - Cliquez sur **Créer une distribution**.



- Dans la section **Origine**, configurez :
  - **Origine Domain Name** : Entrez l'URL de votre bucket S3 obtenue précédemment.

#### Créer une distribution

**Origine**

**Origin domain**  
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

X

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

Pour répondre à la consigne et offrir une meilleure expérience utilisateur avec un site web statique, utilisez le **point de terminaison du site Web S3** en suivant les recommandations AWS. Cliquez sur le bouton correspondant pour l'activer.

**⚠️** Ce compartiment S3 est configuré avec un site Web S3. Si vous envisagez d'utiliser cette distribution en tant que site Web, il est recommandé d'utiliser le point de terminaison du site Web S3 plutôt que le point de terminaison du compartiment.

**Utiliser le point de terminaison du site Web**

- **Origine Access Control** : Configurez pour permettre l'accès public ou utilisez une stratégie IAM si nécessaire.

## Créer une distribution

### Origine

#### Origin domain

Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

 mon-site-web-statique.s3-website.eu-west-3.amazonaws.com 

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

### 3. Paramétriser les options de cache :

- Activez la **compression automatique** pour réduire la taille des fichiers envoyés.

### Comportement du cache par défaut

Modèle de chemin | [Informations](#)

Par défaut (\*)

Compresser automatiquement les objets | [Informations](#)

- No  
 Yes

- Configurez le **TTL par défaut** pour définir la durée de mise en cache des fichiers.

#### Demandes de clé de cache et d'origine

Nous recommandons d'utiliser une politique de cache et une politique de demande à l'origine pour contrôler la clé de cache et les demandes à l'origine.

- Cache policy and origin request policy (recommended)  
 Legacy cache settings

En-têtes

Choisissez les en-têtes à inclure dans la clé de cache.

Aucun

Châînes de requête

Choisissez les chaînes de requête à inclure dans la clé de cache.

Aucun

Cookies

Choisissez les cookies à inclure dans la clé de cache.

Aucun

Mise en cache d'un objet

- Use origin cache headers  
 Customize

Durée de vie minimale

Durée de vie minimale en secondes.

0

Durée de vie maximale

Durée de vie maximale en secondes.

31536000

Durée de vie par défaut

Durée de vie par défaut en secondes.

86400

### 4. Configurer les paramètres de distribution :

- **Nom de domaine personnalisé** : Si vous avez un domaine (ex. [www.mon-site.com](http://www.mon-site.com)), configurez un CNAME. Sinon, utilisez l'URL générée par CloudFront.
- **Certificat SSL** : Si vous utilisez un domaine personnalisé, ajoutez un certificat via ACM pour sécuriser la connexion HTTPS.

### 5. Créer la distribution :

- Cliquez sur **Créer**. La distribution peut prendre plusieurs minutes pour être déployée.

## 6.Trouver l'URL de la distribution

- Dans la liste des distributions, repérez la colonne intitulée Domain Name (Nom de domaine). L'URL affichée dans cette colonne correspond à votre distribution CloudFront, par exemple :

dxxxxxxxxxx.cloudfront.net

The screenshot shows the AWS CloudFront console with the distribution details for E2IX1ET15SIFQ. The top navigation bar includes the AWS logo, a search bar, and various global settings. The main page displays the distribution's ARN, last modified date, and other basic information. Below this, there are sections for parameters like description, alternative domain names, and logging settings.

- Copiez cette URL. C'est l'URL que vous utiliserez pour accéder au contenu distribué par CloudFront.
- Tester l'URL
  - Ouvrez un navigateur web et collez l'URL (par exemple : <https://dxxxxxxxxxx.cloudfront.net>).

## 403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 5CRD2XZ41BBP0G9H
- HostId: cHrtyyJKEGPYm5DFRCEUPn2+HD9iXE+DmFpX85jh7NQF8PzeGeEJDpU3U/MnoeAZTWRxzL6QnOX8oAW/tC/U9Lcv2qPUdfZU

**Le message d'erreur 403 Forbidden - AccessDenied signifie que CloudFront n'a pas les permissions nécessaires pour accéder à votre bucket S3 ou à l'origine configurée. Voici les étapes pour corriger ce problème :**

## 4. Attribuer une Stratégie de compartiment

CloudFront doit pouvoir lire les fichiers dans le bucket S3. Pour cela :

- Accédez à votre bucket S3 et ouvrez la console S3 et sélectionnez le bucket utilisé comme origine.

2. Modifier l'onglet Stratégie de compartiment dans l'onglet Autorisations.

3. Copie l'**ARN du compartiment** puis cliquez Générateur de stratégie

The screenshot shows the AWS S3 console. In the top navigation bar, 'Amazon S3' is selected. Below it, 'Compartiments à usage général' (General purpose compartments) is shown. Under 'Compartiments de répertoires', 'mon-site-web-statique' is selected. The main content area displays the compartment details for 'mon-site-web-statique'. At the top of this section is the title 'mon-site-web-statique' with an 'Info' link. Below the title are tabs: 'Objets', 'Propriétés', 'Autorisations' (which is highlighted in blue), 'Métriques', 'Gestion', and 'Points d'accès'. A secondary navigation bar at the top of the 'Autorisations' tab shows 'Amazon S3 > Compartiments > mon-site-web-statique > Modifier la stratégie de compartiment'. The main content area is titled 'Modifier la stratégie de compartiment' with an 'Info' link. It contains two sections: 'Stratégie de compartiment' and 'Stratégie'. The 'Stratégie de compartiment' section includes a note about JSON format and links to 'Exemples de stratégies' and 'Générateur de stratégies'. The 'ARN du compartiment' field contains 'arn:aws:s3:::mon-site-web-statique'. The 'Stratégie' section shows a single rule: '1' with a 'Modifier l'instruction' button. On the left sidebar, there are other compartments like 'Compartiments de table', 'Access Grants', and 'Points d'accès'.

**Vous serez redirigé vers une page outil qui vous permet de créer des stratégies qui contrôlent l'accès à [Amazon Web Services \(AWS\)](#) produits et des ressources.**

The screenshot shows the AWS Policy Generator tool at the URL 'awspolicygen.s3.amazonaws.com/policygen.html'. The page has a header with browser tabs and icons. The main content area starts with the 'Amazon web services' logo. Below it is the 'AWS Policy Generator' title and a brief description. The first step is 'Step 1: Select Policy Type', which is set to 'S3 Bucket Policy'. The second step is 'Step 2: Add Statement(s)'. It asks for a statement description and provides fields for 'Effect' (Allow or Deny), 'Principal' (with a placeholder 'arn:aws:s3:::'), 'AWS Service' (set to 'Amazon S3'), 'Actions' (set to '1 Action(s) Selected'), and 'Amazon Resource Name (ARN)' (set to 'arn:aws:s3:::mon-site-web-'). There are also 'Add Conditions (Optional)' and a 'Add Statement' button.

Cliquez sur le bouton Générer une politique pour générer une stratégie.

Vous avez ajouté les déclarations suivantes. Cliquez sur le bouton ci-dessous pour générer une stratégie.

Principal(s)	Effet	Action	Ressource	Conditions
• *	Autoriser	• s3:ObjetObjet	arn:aws:s3:::mon-site-web-statique	Aucun

### Étape 3: Générer une politique

A *politique* est un document (écrit dans le [Accès Politique Langue](#)) qui agit comme un conteneur pour un ou plusieurs déclarations.

[Générer une Politique](#)    [Commencer](#)

Copiez le Json dans la stratégie et enfin “Enregistrer les modifications”

**json**

```
{  
  "Version": "2012-10-17",  
  
  "Statement": [  
  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::mon-site-web-statique/*"  
    }  
  ]  
}
```

## Modifier la stratégie de compartiment Info

Stratégie de compartiment

ARN du compartiment [arnaws:s3::mon-site-web-statique](#)

Stratégie

```
1 Version: "2012-10-17",
2 Statement: [
3     {
4         Sid: "PublicReadGetObject",
5         Effect: "Allow",
6         Principal: "*",
7         Action: "s3:GetObject",
8         Resource: "arn:aws:s3:::mon-site-web-statique/*"
9     }
10 ]
11 ]
12 ]
```

Exemples de stratégies [Génératrice de stratégies](#)

Modifier l'instruction

Sélectionner une instruction

Sélectionnez une instruction existante dans la politique ou ajoutez une nouvelle instruction.

+ Ajouter une nouvelle instruction

Ajouter une nouvelle instruction

JSON Ln 12, Col. 1

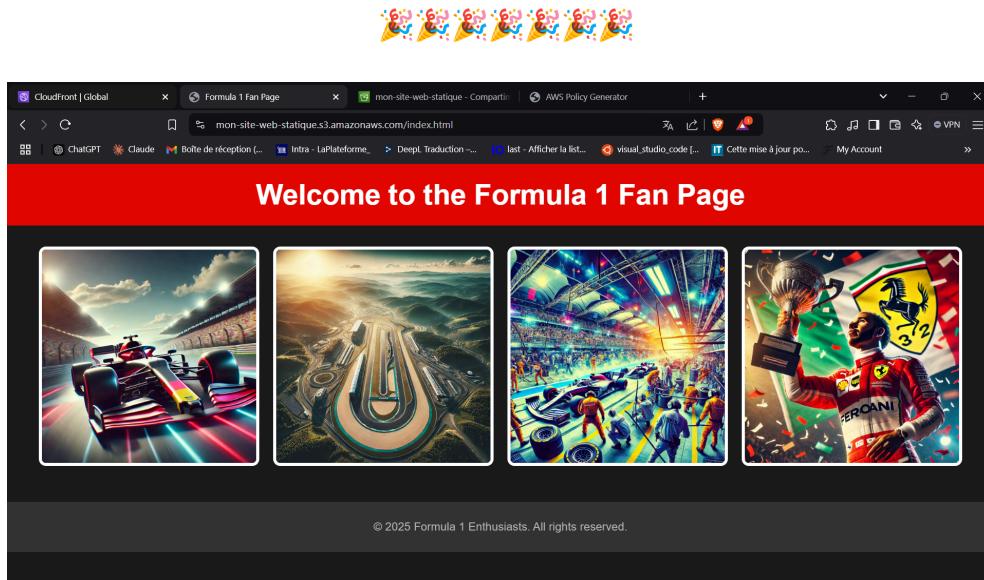
Sécurité: 0 Erreurs: 0 Avertissements: 0 Suggestions: 0

Aperçu de l'accès externe

Annuler Enregistrer les modifications

## Tester l'accès :

- Une fois les permissions mises à jour, accédez à l'URL de CloudFront.
- Accédez à l'URL de CloudFront pour tester la distribution du contenu
- Vérifiez que tous les fichiers se chargent correctement.



Si cela fonctionne, votre bucket est bien configuré pour un accès public.

## Job 3

# Déployer une base de données relationnelle sécurisée sur Amazon RDS

---

## Étapes

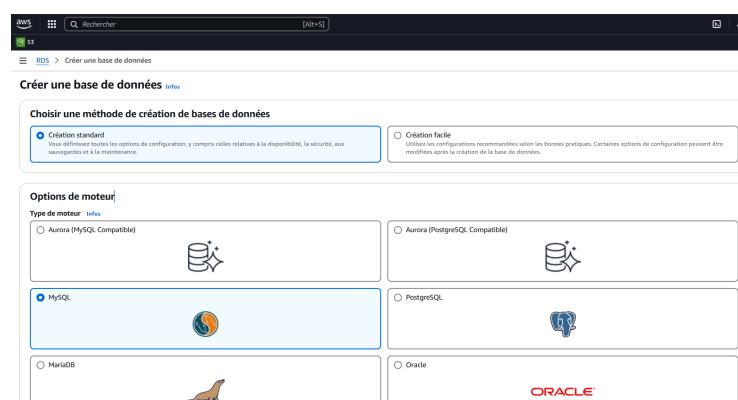
- 1. [Création de l'instance RDS](#)
  - 2. [Configuration des sauvegardes automatiques et snapshots](#)
  - 3. [Tester l'accès à la base de données](#)
  - 4. [Optimiser la sécurité](#)
  - 5. [Nettoyage après test](#)
- 

Avant de commencer :

- Connecte-toi à la **console AWS**.
  - Assure-toi que tu as les droits nécessaires pour créer des ressources RDS.
  - Vérifie que tu es dans la bonne **région AWS** pour tes besoins.
- 

## 1. Création de l'instance RDS

1. **Accéder au service RDS :**
  - Depuis la console AWS, recherche **RDS** dans la barre de recherche.
  - Cliquez sur **Créer une base de données**.
2. **Choisir un moteur de base de données :**
  - Sélectionne le moteur : **MySQL** ou **PostgreSQL**.



### 3. Configurer les détails de l'instance :

- **Modèle de déploiement** : Choisis **Offre Gratuite**

#### Modèles

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

**Production**

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

**Dev/Test**

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

**Offre gratuite**

Utilisez l'offre gratuite RDS afin de développer de nouvelles applications, de tester des applications existantes ou d'acquérir de l'expérience pratique avec Amazon RDS. [Infos](#)

- **Identifiant de la base de données** : Donne un nom à ta base (exemple : **MaBaseRDS**).
- **Utilisateur principal** : Indique un nom d'utilisateur (exemple : **admin**).
- **Mot de passe principal** : Saisis un mot de passe sécurisé.

#### Paramètres

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

Saisissez un nom pour votre instance de base de données. Le nom doit être unique parmi toutes les instances de base de données appartenant à votre compte AWS dans la région AWS actuelle.

MaBaseRDS

L'identifiant d'instance de base de données est sensible à la casse mais stocké intégralement en minuscules (comme dans « mydbinstance »). Contraintes : doit contenir entre 1 et 63 caractères alphanumériques ou traits d'union. Le premier caractère doit être une lettre. L'identifiant ne peut pas contenir deux traits d'union consécutifs ou se terminer par un trait d'union.

▼ Configuration des informations d'identification

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

Saisissez un ID de connexion pour l'utilisateur principal de votre instance de base de données.

admin

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

**Gestion des informations d'identification**

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

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

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

**Autogéré**

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

**Générer automatiquement un mot de passe**

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

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

\*\*\*\*\*



**Password strength** [Neutral](#)

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

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

\*\*\*\*\*



- **Type d'instance** : Sélectionne **db.t3.micro** (c'est inclus dans le niveau gratuit AWS).

#### Configuration d'instance

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

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

▼ Masquer les filtres

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

**Infos**

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

- Inclure les classes de la génération précédente**

- Classes standard (inclus les classes m)**
- Classes à mémoire optimisée (inclus les classes r et x)**
- Classe à capacité extensible (inclus les classes t)**

db.t3.micro

2 vCPUs 1 GiB RAM Réseau : jusqu'à 2 085 Mbps

#### 4. Paramètres de connectivité :

- **Réseau** : Assure-toi de choisir un **VPC** approprié ou celui par défaut.

##### Virtual Private Cloud (VPC) [Infos](#)

Choisissez le VPC. Le VPC définit l'environnement de mise en réseau virtuel pour cette instance de base de données.

my-vpc-01 (vpc-035a5a34211dfa28d)

2 Sous-réseaux, 2 Zones de disponibilité



Seuls les VPC avec un groupe de sous-réseaux de base de données correspondant sont répertoriés.

- **Accès public** : Mets sur **Non** si tu veux sécuriser l'accès.
- **Groupes de sécurité** : Crée ou utilise un groupe de sécurité existant pour autoriser l'accès à des IP spécifiques.

##### Accès public [Infos](#)

Oui

RDS attribue une adresse IP publique à la base de données. Les instances Amazon EC2 et les autres ressources en dehors du VPC peuvent se connecter à votre base de données connecter à la base de données. Choisissez un ou plusieurs groupes de sécurité VPC qui spécifient quelles ressources peuvent se connecter à la base de données.

Non

RDS n'attribue pas d'adresse IP publique à la base de données. Seules les instances Amazon EC2 et les autres ressources à l'intérieur du VPC peuvent se connecter à votre base qui spécifient quelles ressources peuvent se connecter à la base de données.

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

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

Choisir existants

Choisir les groupes de sécurité VPC existants

Créer

Créer un groupe de sécurité VPC

##### Groupes de sécurité VPC existants

Sélectionner une ou plusieurs options

web-server-SG

##### Zone de disponibilité [Infos](#)

Aucune préférence

##### Proxy RDS

Le proxy RDS est un proxy de base de données hautement disponible et entièrement géré qui améliore la capacité de mise à l'échelle, la résilience et la sécurité des applications.

Créer un proxy RDS [Infos](#)

RDS crée automatiquement un rôle IAM et un secret Secrets Manager pour le proxy. Le proxy RDS entraîne des coûts supplémentaires. Pour plus d'informations, consultez [la t](#);

#### 5. Activer les options de sauvegarde :

- **Période de rétention des sauvegardes automatiques** : Configure un délai (par exemple, 7 jours).
- Active les **snapshots automatiques**.

RDS > Créer une base de données

▼ Configuration supplémentaire

Options de base de données

Nom de la base de données initiale [Infos](#)

MaBaseRDS

Si vous ne spécifiez pas de nom de base de données, Amazon RDS ne crée pas de base de données.

Groupe de paramètres de base de données [Infos](#)

default.mysql8.0

Groupe d'options [Infos](#)

default.mysql8-0

Sauvegarde

Activer les sauvegardes automatiques

Crée un instantané de votre base de données à un moment donné

Veuillez noter que les sauvegardes automatiques sont actuellement prises en charge pour le moteur de stockage InnoDB uniquement. Si vous utilisez MyISAM, reportez-vous à la documentation.

Période de rétention des sauvegardes [Infos](#)

Nombre de jours (entre 1 et 35) pendant lesquels les sauvegardes automatiques sont conservées.

7 jours

Fenêtre de sauvegarde [Infos](#)

Plage de temps quotidienne (en UTC) au cours de laquelle RDS effectue des sauvegardes automatiques.

Choisir une fenêtre

Aucune préférence

Heure de début

23 : 59 UTC

Durée

0.5 heures

## 6. Lancer l'instance :

- Vérifie les configurations dans la récapitulation.
- Cliquez sur **Créer une base de données**.

The screenshot shows the 'Bases de données' (Data Sources) section of the AWS RDS console. A green banner at the top indicates a successful creation of the 'mabaserds' database. Below the banner, there's a table with one row for 'mabaserds'. The table columns include 'Identifiant de base de données' (Database identifier), 'Statut' (Status), 'Rôle' (Role), 'Moteur' (Engine), 'Région ...' (Region), 'Taille' (Size), and 'Recommandations' (Recommendations). The 'mabaserds' row is highlighted with a blue border. At the bottom of the table, there are navigation arrows and a gear icon.

## 2. Configuration des sauvegardes automatiques et snapshots

### 1. Sauvegardes automatiques :

- Une fois l'instance créée, navigue vers la section **Sauvegardes** dans RDS.
- Vérifie que la planification des sauvegardes automatiques est activée.

### 2. Créer un snapshot manuel :

- Dans l'interface RDS, sélectionne ton instance.
- Clique sur **Actions > Prendre un snapshot**.
- Donne un nom au snapshot et confirme.

## 3. Tester l'accès à la base de données

### 1. Obtenir les détails de connexion :

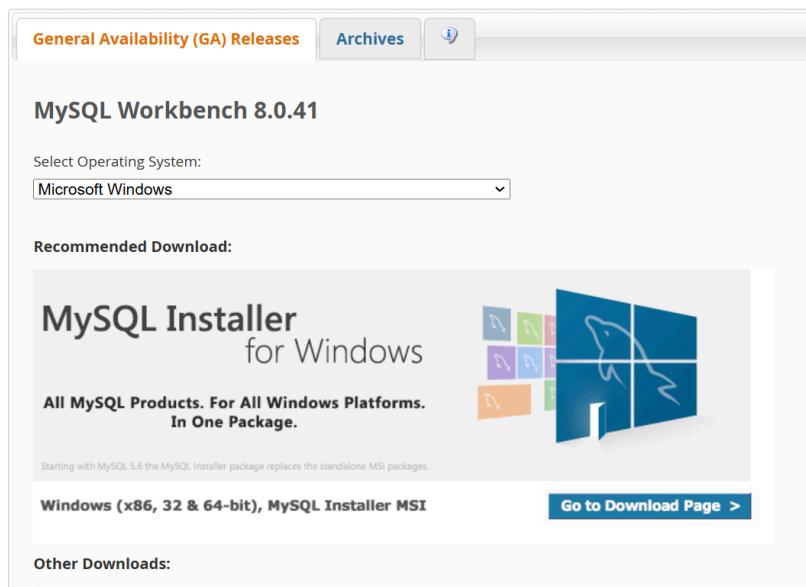
- Dans RDS, sélectionnez l'instance et récupérez l'**endpoint** (adresse de connexion).

The screenshot shows the 'mabaserds' instance details page in the AWS RDS console. On the left, there's a sidebar with various RDS-related options like Tableau de bord, Bases de données, etc. The main content area has a 'Récapitulatif' (Summary) section with details such as Identifiant de base de données (mabaserds), Statut (Sauvegarde en cours), Rôle (Instance), Moteur (MySQL Community), and Région et AZ (eu-west-3b). Below this, there are tabs for Connectivité et sécurité, Surveillance, Journaux et événements, Configuration, and Intégrations. Under the 'Connectivité et sécurité' tab, it shows the Point de terminaison et port (Endpoint and port) as 'mabaserds.cricyouc8gc.eu-west-3.rds.amazonaws.com' and the Mise en réseau (Network settings) as 'Zone de disponibilité: eu-west-3b, VPC'. There's also a 'Sécurité' (Security) section with a note about security groups.

- Note également le **port** par défaut (3306 pour MySQL ou 5432 pour PostgreSQL).

## 2. Utiliser un outil client :

- Télécharge un outil comme **MySQL Workbench** ou **pgAdmin** selon le moteur choisi.



- Configure une nouvelle connexion en entrant l'endpoint, le port, le nom d'utilisateur et le mot de passe.

## 3. Configurer la connexion dans MySQL Workbench (pour MySQL) :

### 1. Créer une nouvelle connexion :

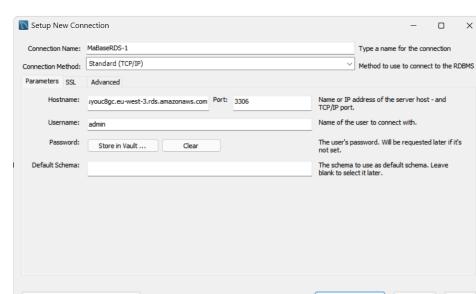
- Ouvre MySQL Workbench.
- Cliquez sur l'icône à côté de "MySQL Connections".

### 2. Remplir les champs de la connexion :

- **Connection Name** : Donne un nom à la connexion (exemple : **MaBaseRDS**).
- **Hostname** : Copiez et collez l'**endpoint** (adresse) de l'instance RDS.
- **Port** : Saisis **3306** (ou le port que tu as configuré pour MySQL).
- **Username** : Entre le nom d'utilisateur configuré (par exemple : **admin**).
- **Password** :
  - Cliquez sur **Store in Vault...** pour sauvegarder votre mot de passe dans MySQL Workbench.
  - Saisis le mot de passe défini lors de la création de l'instance.

### 3. Tester la connexion :

- Cliquez sur **Test Connection** pour vérifier que tout est bien configuré.
- Si tout est correct, un message de confirmation s'affiche.



### 4. Enregistrer la connexion :

- Clique sur **OK** pour enregistrer cette connexion dans MySQL Workbench.

#### 4. Tester les commandes SQL :

- Effectuer des opérations de base comme créer une table ou insérer des données pour valider le fonctionnement.
- 

## 4. Optimiser la sécurité

### 1. Configurer IAM pour l'accès :

- Créer un rôle IAM avec des permissions spécifiques pour gérer l'instance RDS.
- Attache ce rôle aux utilisateurs ou applications.

### 2. Limiter l'accès réseau :

- Ajuste les règles du groupe de sécurité pour autoriser uniquement des IP spécifiques.

### 3. Activer la journalisation :

- Active la journalisation des requêtes pour surveiller les activités sur la base.
- 

## Job 4

# Création d'une API RESTful sans serveur avec AWS Lambda et API Gateway

Dans ce projet, nous allons :

1. Créer une API RESTful avec **API Gateway** pour gérer les requêtes HTTP.
  2. Connecter cette API à une **fonction Lambda** qui traite les données ou renvoie des réponses.
  3. Activer **CloudWatch** pour surveiller et enregistrer les interactions avec l'API.
- 

## Objectifs

Créer une API qui répond à des requêtes HTTP avec un message simple : "**Hello from Lambda!**"

1. [AWS Lambda : Exécution du code backend.](#)
2. [API Gateway : Interface HTTP pour exposer la fonction Lambda.](#)
3. [CloudWatch Logs : Suivi des journaux d'exécution.](#)

---

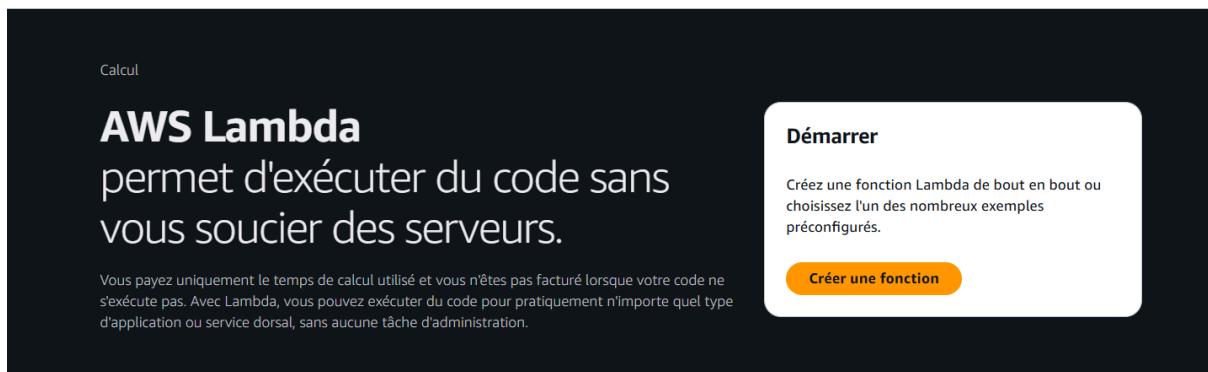
## 1. Créer une fonction Lambda

### 1. Accéder à AWS Lambda :

- Connectez-vous à la console AWS.
- Recherchez le service **Lambda**.

### 2. Créer une nouvelle fonction :

- Cliquez sur "**Créer une fonction**".



- Sélectionnez "**Créer à partir de zéro**".

#### Créer une fonction Info

Choisissez l'une des options suivantes pour créer votre fonction.

- Créer à partir de zéro**

Commencez avec un exemple Hello World simple.

- Donnez un nom à votre fonction (par exemple : `HelloWorldFunction`).
- Choisissez un runtime (Python 3.9 ou Node.js).
- Cliquez sur "**Créer une fonction**".

### 3. Ajouter du code :

- Une fois la fonction créée, éditez le code directement dans la console.

Remplacez le contenu par ce code Python :

```
import json

def lambda_handler(event, context):
    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

The screenshot shows the AWS Lambda function editor interface. At the top, there are tabs: Code (which is selected), Tester, Surveiller, Configuration, Alias, and Versions. Below the tabs, there's a header bar with a search field containing 'HelloWorldFunction' and several icons. On the left, there's an Explorer sidebar with sections for EXPLORER, HELLOWORLDFUNCTION (containing 'lambda\_function.py'), and DEPLOY. A 'Deploy (Ctrl+Shift+U)' button is at the bottom of this sidebar. The main area is titled 'Source du code' with an 'Info' link. It shows the Python code for the lambda function. A tooltip at the bottom right says 'Amazon Q Tip 1/3: Start typing to get suggestions ([ESC] to exit)'. There are also 'Charger depuis' and '...' buttons in the top right.

#### 4. Tester la fonction :

This screenshot shows the 'Tester' section of the AWS Lambda function configuration page. At the top, there's a header with 'Événement de test' and an 'Info' link, along with buttons for 'CloudWatch Logs Live Tail', 'Enregistrer', and 'Tester'. Below this, there's a note: 'Pour appeler la fonction sans enregistrer un événement, configurez l'événement JSON, puis choisissez Test.' Under 'Action d'événement de test', there are two options: 'Créer un événement' (selected) and 'Modifier l'événement enregistré'. The 'Nom de l'événement' field contains 'my-test-event'. A note says '25 caractères maximum composés de lettres, de chiffres, de points, de tirets et de traits de soulignement.'. Under 'Paramètres de partage d'événements', there are two options: 'Privé' (selected) and 'Partageable'. A note for 'Privé' says 'Cet événement est uniquement disponible dans la console Lambda et pour le créateur de l'événement. Vous pouvez configurer un total de 10.' and a 'En savoir plus' link. A note for 'Partageable' says 'Cet événement est disponible pour les utilisateurs IAM du même compte qui sont autorisés à accéder aux événements partageables et à les utiliser.' and a 'En savoir plus' link. Under 'Modèle - facultatif', there's a dropdown menu with 'hello-world' selected.

Cliquez sur "Tester".

Créez un nouvel événement de test (utilisez un JSON vide : {}).

Exécutez le test pour vérifier que la réponse est :

```
{  
  "statusCode": 200,  
  "body": "Hello from Lambda!"  
}
```

Exécution de la fonction : réussite ([journals \[2\]](#))

Détails

La zone ci-dessous montre les 4 derniers KB du journal d'exécution.

```
{ "statusCode": 200, "body": "\\\"Hello from Lambda!\\\""}  
/
```

Récapitulatif

Code SHA-256	Délai d'exécution
HAPq9EReJVEC5gLavtc/gyd5vZtd9eiUGF932t0jBxY=	Il y a 31 secondes
ID de demande	Version de la fonction
09820fcc-3e33-4404-b440-6d09c6b1c74f	\$LATEST
Durée initiale	Durée
80.14 ms	1.54 ms
Durée facturée	Ressources configurées
2 ms	128 MB
Mémoire max utilisée	
30 MB	

Sortie de journal

La section ci-dessous montre les appels de journalisation dans votre code. [Cliquez ici](#) pour afficher le groupe de journaux CloudWatch correspondant.

```
START RequestId: 09820fcc-3e33-4404-b440-6d09c6b1c74f Version: $LATEST
END RequestId: 09820fcc-3e33-4404-b440-6d09c6b1c74f
REPORT RequestId: 09820fcc-3e33-4404-b440-6d09c6b1c74f Duration: 1.54 ms Billed Duration: 2 ms Memory Size: 128 MB Max Memory Used: 30 MB Init Duration: 80.14 ms
/
```

## 2. Configurer une API Gateway

### 1. Accéder à API Gateway :

- Recherchez le service **API Gateway** dans la console AWS.
- Cliquez sur "**Créer une API**".

### 2. Choisir le type d'API :

- Sélectionnez "**HTTP API**" (option plus simple).
- Cliquez sur "**Créer**".

### 3. Configurer une intégration :

- Cliquez sur **Ajouter une intégration** et choisissez **Fonction Lambda**.
- Sélectionnez votre fonction Lambda (par exemple : [HelloWorldFunction](#)).
- Donnez un nom à votre API (par exemple : [HelloWorldAPI](#)).
- Cliquez sur **Suivant**.

## 4. Configurer des routes :

- Ajoutez une route avec la méthode HTTP **GET**.
- Définissez le chemin de ressource (par exemple, `/` ou `/HelloWorldFunction`).
- Associez cette route à votre fonction Lambda configurée précédemment.
- Cliquez sur **Suivant**.

## 5. Définir les étapes :

- Laissez le nom de l'étape par défaut (`$default`).
- Assurez-vous que l'option de déploiement automatique est activée.
- Cliquez sur **Suivant**.

### 3. Activer CloudWatch Logs

#### Pour AWS Lambda

##### 1. Vérifier l'activation des journaux Lambda :

- Par défaut, les journaux d'exécution sont activés pour Lambda et envoyés à **CloudWatch Logs**.
- Accédez à **CloudWatch > Logs** dans la console AWS.

The screenshot shows the AWS CloudWatch Logs Groups interface. On the left, there's a sidebar with navigation links like CloudWatch, Favoris et récents, Tableaux de bord, Alarms, Journaux (Groups de journaux, Nouveau), Anomalies dans les journaux, Queue en direct, Logs Insights (Nouveau), Contributor Insights, and Métriques. The main area is titled "Groupes de journaux (3)" and contains a table with three entries:

Groupe de journaux	Classe de j...	Détection ...	Protection
/aws/lambda/HelloWorldFunction	Standard	<a href="#">Configurer</a>	-
/aws/rds/instance/mabaserds/error	Standard	<a href="#">Configurer</a>	-
RDSONMetrics	Standard	<a href="#">Configurer</a>	-

- Recherchez un groupe de journaux avec le nom correspondant à votre fonction Lambda (par exemple, `/aws/lambda/HelloWorldFunction`).

##### 2. Personnaliser les journaux (facultatif) :

- Dans la configuration de la fonction Lambda, accédez à l'onglet **Monitoring**.
- Configurez un rôle IAM si nécessaire pour permettre l'accès à CloudWatch.

#### Pour API Gateway

##### 1. Accéder aux paramètres de journalisation :

- Dans API Gateway, ouvrez votre API.
- Cliquez sur **Paramètres** dans le menu de l'API.

##### 2. Activer la journalisation :

- Sous la section **CloudWatch Logs**, cochez les options pour activer la journalisation des requêtes et des erreurs.

The screenshot shows the "Modifier les paramètres de journalisation" (Edit logging parameters) dialog. It includes fields for the CloudWatch Log role (ARN: arn:aws:logs:eu-west-3:140023371742:log-group:/aws/lambda/HelloWorldFunction) and buttons for Annuler (Cancel) and Enregistrer les modifications (Save changes).

- Configurez un rôle IAM avec les autorisations appropriées pour écrire dans CloudWatch Logs.

**IAM > Rôles > Créer un rôle**

Étape 3 : Nommer, vérifier et créer

**Ajouter des autorisations**

- Ajouter des autorisations
- Service AWS
- Compte AWS
- Identité Web
- Fédération SAML 2.0
- Stratégie d'approbation personnalisée

**Service ou cas d'utilisation**

API Gateway

**Cas d'utilisation**

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

**Service ou cas d'utilisation**

API Gateway

Choisissez un cas d'utilisation pour le service spécifié.

**Cas d'utilisation**

API Gateway

Allows API Gateway to push logs to CloudWatch Logs

**IAM > Rôles > Créer un rôle**

Étape 1 : Sélectionner une entité de confiance

Étape 2 : Ajouter des autorisations

Étape 3 : Nommer, vérifier et créer

**Ajouter des autorisations**

**Politiques des autorisations (1) Infos**

Le type de rôle que vous avez sélectionné nécessite la stratégie suivante.

Nom de la politique	Type
AmazonAPIGatewayPushToCloudWatchLogs	Générée par AWS

**Définir une limite d'autorisations - facultatif**

Annuler Précédent Suivant

**API Gateway > API > Paramètres > Modifier les paramètres de journalisation**

**Modifier les paramètres de journalisation**

**Rôle du journal CloudWatch**

ARN de rôle du journal CloudWatch

arn:aws:iam::140023371742:role/APIGatewayCloudWatchRole

Annuler Enregistrer les modifications

**IAM > Rôles > APIGatewayCloudWatchRole**

**Identity and Access Management (IAM)**

Rechercher sur IAM

Tableau de bord

Gestion des accès

Groupes de personnes

Personnes

**Rôles**

Politiques

Fournisseurs d'identité

Paramètres du compte

Gestion de l'accès racine

Nouveau

**APIGatewayCloudWatchRole Infos**

Allows API Gateway to push logs to CloudWatch Logs.

**Récapitulatif**

Date de création : January 24, 2025, 15:41 (UTC+01:00)

Dernière activité : Il y a 45 minutes

ARN : arn:aws:iam::140023371742:role/APIGatewayCloudWatchRole

Durée maximale de la session : 1 heure

**Autorisations**

**Politiques des autorisations Infos**

Vous pouvez attacher jusqu'à 10 politiques gérées.

Simuler Supprimer Ajouter des autorisations

## 4. Tester l'API

### 1. Tester via un navigateur ou Postman :

- Ouvrez l'URL de l'API dans un navigateur ou utilisez un outil comme Postman.
- Vous devriez voir le message : "**Hello from Lambda!**".

```
Asus-Tuf-Laptop@AsusTUFGaming MINGW64 ~
$ curl -X GET https://bv11anz869.execute-api.eu-west-3.amazonaws.com/HelloWorldFunction
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload   Total   Spent    Left  Speed
100       20  100      20      0       0  109      0 --:--:-- --:--:-- --:--:--  111"Hello from Lambda!"
```

```
Asus-Tuf-Laptop@AsusTUFGaming MINGW64 ~
$ |
```

### 2. Vérifier les journaux :

- Consultez les journaux dans CloudWatch pour analyser les requêtes et réponses.

Événements de journaux

Vous pouvez utiliser la barre de filtre ci-dessous pour rechercher et faire correspondre des termes, des expressions ou des valeurs dans vos événements de journal. [En savoir plus sur les modèles de filtre](#)

Horodatage	Message
2025-01-24T15:21:15.061Z	{ "requestId": "E5hsyjaOCGYEPVah", "ip": "37.26.187.6", "requestTime": "24/Jan/2025:15:21:15 +0000", "httpMethod": "GET", "routeKey": "GET /", "status": "200", "protocol": "HTTP/1.1", "responseLength": "20" }

## Job 5

### Mettre en place une surveillance et des alertes pour une application ou un service AWS

Dans ce projet, nous allons :

- Configurer un système de surveillance pour les ressources ou services AWS en utilisant **CloudWatch**.
- Définir des seuils critiques pour des métriques spécifiques (comme l'utilisation CPU ou la mémoire).
- Créer des notifications automatiques via **SNS** (Simple Notification Service) pour alerter en cas de dépassement des seuils définis.

## Objectifs :

1. [Configurer des métriques CloudWatch pour Surveiller les performances](#)
2. [Créer des alarmes pour les métriques](#)
3. [Configurer SNS pour les notifications](#)

### 1. Configurer des métriques CloudWatch pour Surveiller les performances

#### 1. Accéder à la console CloudWatch

- Connectez-vous à votre compte AWS.
- Dans la barre de recherche, tapez **CloudWatch** et ouvrez le service.

#### 2. Vérifiez les métriques par défaut

Lorsque vous déployez une ressource AWS (comme une instance EC2), AWS collecte automatiquement certaines métriques de base, telles que :

- **CPUUtilization** (Utilisation CPU).
- **NetworkIn** et **NetworkOut** (trafic réseau entrant/sortant).
- **DiskReadOps** et **DiskWriteOps** (opérations de lecture/écriture sur disque).

Pour visualiser ces métriques :

1. Dans CloudWatch, cliquez sur **Metrics** dans le menu de gauche.
2. Sélectionnez le type de ressource que vous voulez surveiller (par exemple, EC2).
3. Choisissez une instance ou une autre ressource AWS pour afficher ses métriques.

#### 3. Configurer des métriques supplémentaires avec l'Agent CloudWatch

Certaines métriques, comme la mémoire et l'utilisation du disque, ne sont pas collectées par défaut. Vous devez installer l'**Agent CloudWatch** pour les activer.

##### **Étape 3.1 : Installer l'Agent CloudWatch**

1. Connectez-vous à une instance EC2 via SSH.
2. Installez l'agent CloudWatch :

Pour Amazon Linux ou RHEL :

bash

## CopierModifier

```
sudo yum install amazon-cloudwatch-agent -y
```

## Pour Ubuntu :

bash

## CopierModifier

```
sudo apt-get install amazon-cloudwatch-agent -y
```

### **Étape 3.2 : Configurer l'Agent CloudWatch**

1. Créez un fichier de configuration pour définir les métriques à collecter.

Exemple de configuration JSON (fichier `amazon-cloudwatch-agent.json`) :

{

```
"metrics": {
```

```
"append_dimensions": {
```

```
"InstanceId": "${aws:InstanceId}"
```

1

```

"metrics_collected": {

    "cpu": {

        "measurement": [ "cpu_usage_idle", "cpu_usage_iowait"] ,

        "metrics_collection_interval": 60
    } ,


    "mem": {

        "measurement": [ "mem_used_percent"] ,

        "metrics_collection_interval": 60
    } ,


    "disk": {

        "measurement": [ "disk_used_percent"] ,

        "metrics_collection_interval": 60
    }
}
}
}

```

## 2. Enregistrez ce fichier dans

/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json.

```

GNU nano 5.8                               /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

{
    "metrics": {
        "append_dimensions": {
            "InstanceId": "${aws:i-00e17d34d1a18ee31}"
        },
        "metrics_collected": {
            "cpu": {
                "measurement": [ "cpu_usage_idle", "cpu_usage_iowait"] ,
                "metrics_collection_interval": 60
            } ,
            "mem": {
                "measurement": [ "mem_used_percent"] ,
                "metrics_collection_interval": 60
            } ,
            "disk": {
                "measurement": [ "disk_used_percent"] ,
                "metrics_collection_interval": 60
            }
        }
    }
}

```

## *Étape 3.3 : Démarrer l'Agent*

Démarrez l'agent pour activer la collecte des métriques configurées :

```
bash

sudo
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
-a start \
-m ec2 \
-c
file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
```

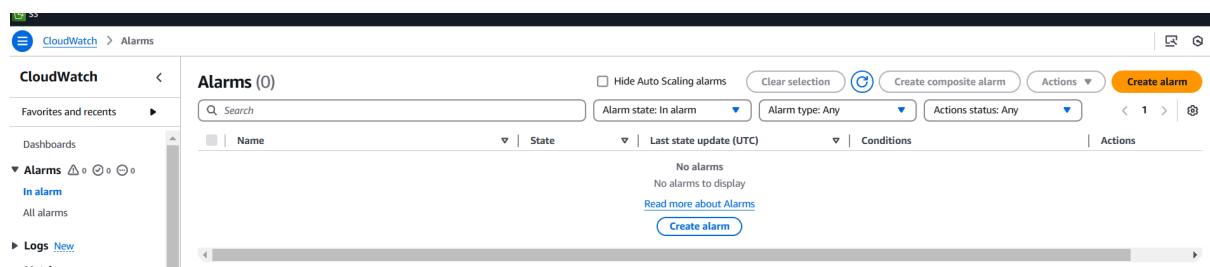
```
[ec2-user@ip-10-0-0-5 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
-a start \
-m ec2 \
-c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
*****
processing amazon-cloudwatch-agent *****
amazon-cloudwatch-agent has already been started
[ec2-user@ip-10-0-0-5 ~]$ █
```

## 2. Créer des alarmes pour les métriques

Les alarmes permettent d'agir lorsque des métriques dépassent des seuils prédéfinis.

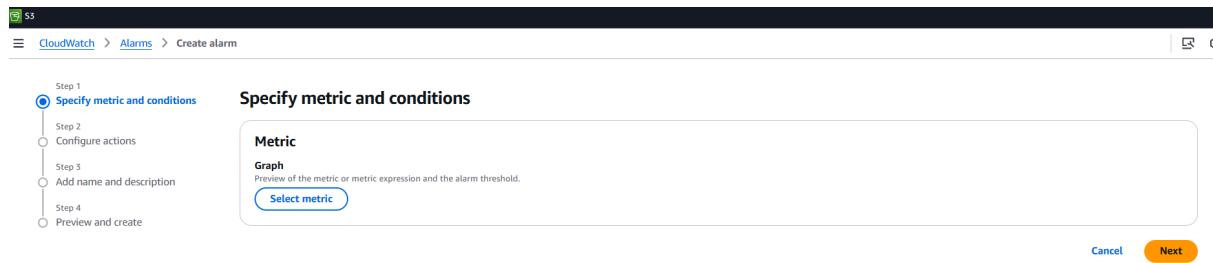
### 1. Accéder à l'onglet des alarmes :

- Dans la console CloudWatch, sélectionnez **Alarms > Create alarm**.

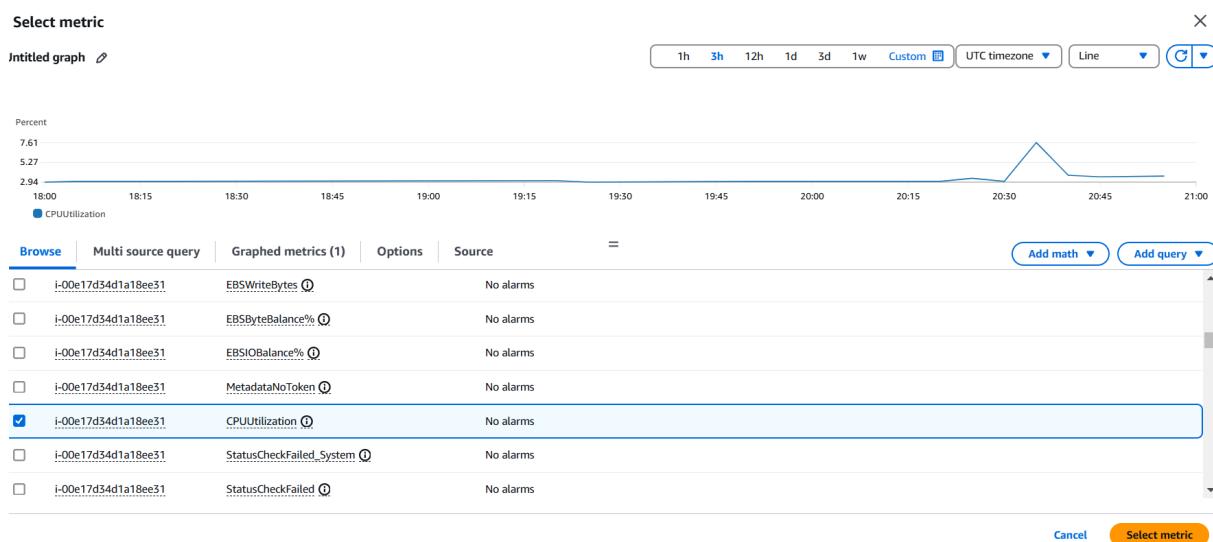


## 2. Choisir une métrique :

- Cliquez sur **Select metric**.



- Naviguez dans les métriques collectées pour choisir celle à surveiller (par exemple, CPUUtilization pour une instance EC2).



## 3. Configurer l'alarme :

- Définissez un seuil d'alerte. Exemple :
  - Si l'utilisation CPU dépasse 80 %, déclencher une alarme.
- Sélectionnez la période d'évaluation (par exemple, 5 minutes).

**Specify metric and conditions**

Graph
Alarm recommendations 
View details

**Metric**

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

80

41.5

2.94

18:00 18:30 19:00 19:30 20:00 20:30 21:00

CPUUtilization

Namespace
Edit

AWS/EC2

**Metric name**

**InstanceId**

**Instance name**

No name specified

**Statistic**

**Period**

5 minutes

**Conditions**

**Threshold type**

Static      Use a value as a threshold

Anomaly detection      Use a band as a threshold

**Whenever CPUUtilization is...**

Define the alarm condition.

Greater      > threshold

Greater/Equal      >= threshold

Lower/Equal      <= threshold

Lower      < threshold

**than...**

Define the threshold value.

80

Must be a number

**▼ Additional configuration**

**Datapoints to alarm**

Define the number of datapoints within the evaluation period that must be breached to cause the alarm to go to ALARM state.

1      out of      1

**Missing data treatment**

How to treat missing data when evaluating the alarm.

Treat missing data as missing

**Add name and description**

**Name and description**

**Alarm name**

**Alarm description - optional** [View formatting guidelines](#)

[Edit](#) [Preview](#)

# This is an H1  
\*\*double asterisks will produce strong characters\*\*  
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

[Cancel](#) [Previous](#) [Next](#)

- 4. Configurer les actions d'alarme :**
- Cliquez sur **Add notification**.
  - Choisissez l'option **Send a notification to an Amazon SNS topic**.

## Configure actions

**Notification**

**Alarm state trigger**  
Define the alarm state that will trigger this action.

In alarm  
The metric or expression is outside of the defined threshold.

OK  
The metric or expression is within the defined threshold.

Insufficient data  
The alarm has just started or not enough data is available.

[Remove](#)

**Send a notification to the following SNS topic**  
Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN to notify other accounts

**Send a notification to...**

[X](#)

Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Email (endpoints)  
Topic has no endpoints - [View in SNS Console](#)

[Add notification](#)

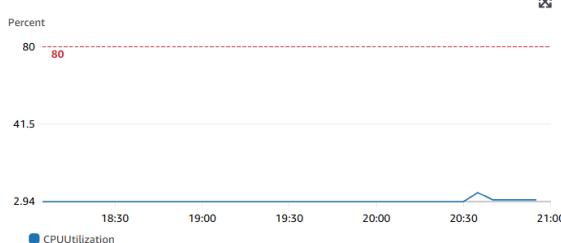
## Preview and create

### Step 1: Specify metric and conditions

#### Metric

##### Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.



Successfully created alarm CPU dépasse 80 %.

### Alarms (0)

Hide Auto Scaling alarms

Search

Alarm state: In alarm

Name

State

Last state update (UTC)

No alarms



CloudWatch > Alarms

CloudWatch

Alarms (1)

Hide Auto Scaling alarm

Alarm state: Any

Search

Name

State

Last state update (UTC)

CPU dépasse 80 %

Insufficient data

2025-01-26 21:07:28

## 3. Configurer SNS pour les notifications

Amazon SNS (Simple Notification Service) envoie des notifications par email ou SMS.

## Étapes :

### 1. Créez un sujet SNS :

- Allez dans la console SNS.
- Cliquez sur **Topics > Create topic**.
- Donnez un nom au sujet (par exemple, `alertes_cloudwatch`).
- Cliquez sur **Create topic**.

The screenshot shows the 'Create topic' wizard. The 'Topic name' field is filled with 'alertes\_cloudwatch'. Below it are two buttons: 'Next step' (in yellow) and 'Start with an overview'.

### 2. Abonnez une adresse email :

- Dans la liste des sujets, sélectionnez celui que vous venez de créer.

The screenshot shows the 'Topics' page with one topic listed: 'alertes\_cloudwatch'. The ARN is shown as 'arn:aws:sns:eu-west-3:140023371742:alertes\_cloudwatch'.

- Cliquez sur **Create subscription**.

The screenshot shows the 'alertes\_cloudwatch' topic details page. The 'Subscriptions' tab is selected. It shows a table with one row for a new subscription. The 'Protocol' column is empty, and the 'Endpoint' column is also empty. There are buttons for 'Edit', 'Delete', 'Request confirmation', 'Confirm subscription', and 'Create subscription'.

- Configurez :
  - **Protocol** : Email.
  - **Endpoint** : Adresse email pour recevoir les notifications.
- Confirmez l'abonnement via le lien envoyé à l'email.

## Create subscription

### Details

#### Topic ARN

arn:aws:sns:eu-west-3:140023371742:alertes\_cloudwatch X

#### Protocol

The type of endpoint to subscribe

Email ▼

#### Endpoint

An email address that can receive notifications from Amazon SNS.

domenico.mandolino@laplateforme.io

i After your subscription is created, you must confirm it. [Info](#)

### 3. Associer le sujet SNS à l'alarme :

- Retournez à l'alarme dans CloudWatch.
- Sous la section **Actions >Edit**, modifieez le sujet SNS créé précédemment.

- Step 1 - optional  
Specify metric and conditions
- Step 2 - optional  
**Configure actions**
- Step 3 - optional  
Add name and description
- Step 4 - optional  
Preview and create

### Configure actions - optional

#### Notification

##### Alarm state trigger

Define the alarm state that will trigger this action.

In alarm

The metric or expression is outside of the defined threshold.

OK

The metric or expression is within the defined threshold.

Insufficient data

The alarm has just started or not enou

#### Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN to notify other accounts

#### Send a notification to...

alertes\_cloudwatch X

Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

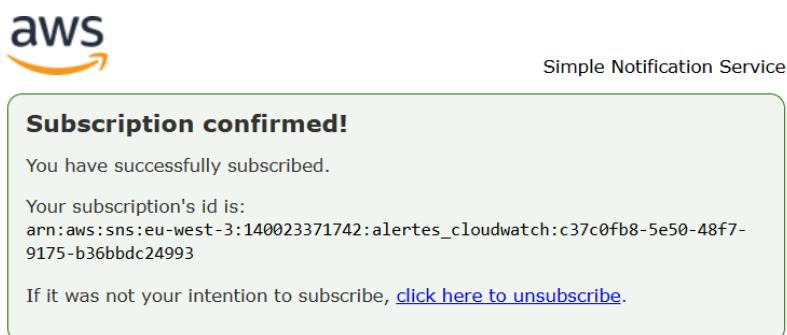
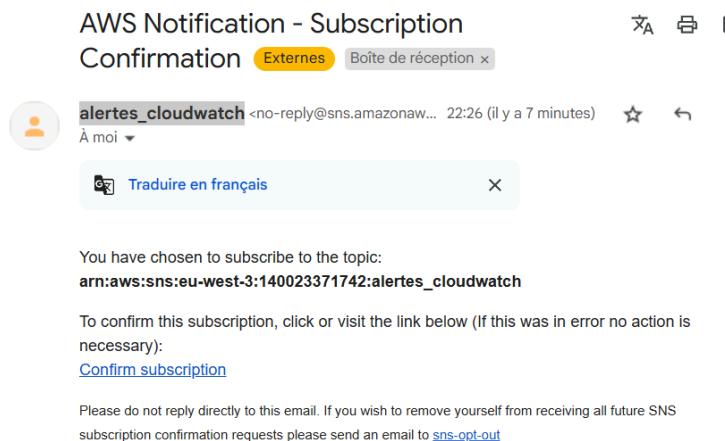
#### Email (endpoints)

[domenico.mandolino@laplateforme.io](#) - View in SNS Console i

[Add notification](#)

### 4. Confirmez inscription alertes\_cloudwatch :

- Confirmation requise dans votre boite mail



## Vérification

- Une fois configurée, déclenchez un test en dépassant le seuil (par exemple, générez une charge CPU élevée sur une instance EC2).

### Simulez une charge sur l'instance

- Connectez-vous à une instance EC2 créée par l'ASG :

Utilisez SSH pour accéder à l'instance principale.

bash

```
ssh -i "chemin/vers/votre-cle.pem" ec2-user@[IP-PUBLIQUE]
```

○

- Installez un utilitaire pour simuler la charge :

Installez stress pour générer une charge CPU :

bash

```
sudo yum install epel-release -y
```

```
sudo yum install stress -y
```

- Générez une charge CPU élevée :

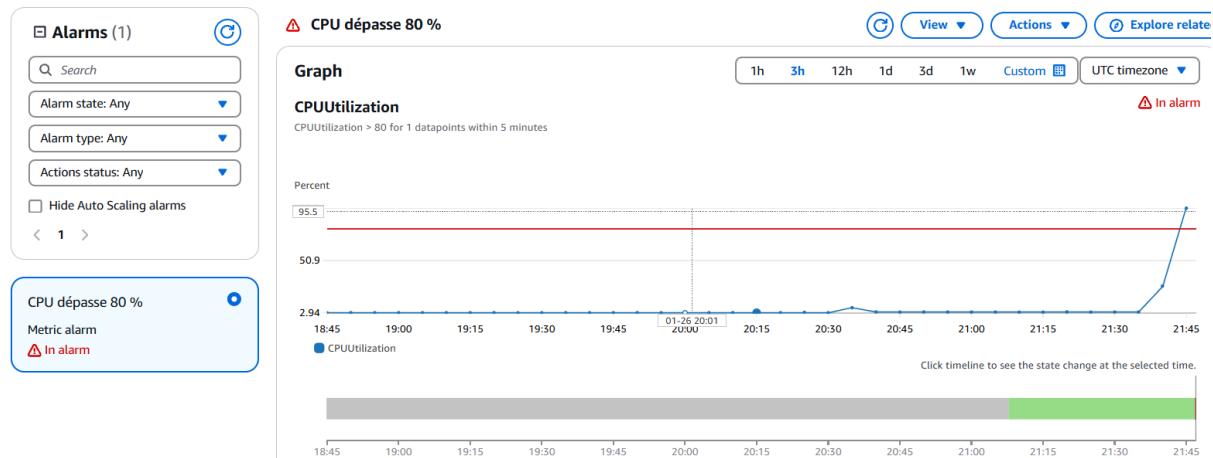
Exécutez cette commande pour simuler une charge de 2 minutes :

bash

```
stress --cpu 2 --timeout 300
```

Cela utilisera 2 cœurs CPU à 100 % pendant 5 minutes.

- Vérifiez que l'alarme se déclenche et que l'email de notification est reçu.



AI ARM: "CPI d' passe 80 %" in EU (Paris) Externes Boîte de réception x

The screenshot shows an email from 'alertes\_cloudwatch <no-reply@sns.amazonaws.com>' to 'A moi'. The subject is 'Your Amazon CloudWatch Alarm "CPU dépasse 80 %" has entered the ALARM state'. The email body contains the following information:

You are receiving this email because your Amazon CloudWatch Alarm "CPU dépasse 80 %" in the EU (Paris) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [98.76426197836167 (26/01/25 21:41:00)] was greater than the threshold (80.0) (minimum 1 datapoint for OK -> ALARM transition)" at "Sunday, 26 January, 2025 21:46:55 UTC".

View this alarm in the AWS Management Console:  
<https://eu-west-3.console.aws.amazon.com/cloudwatch/deeplink/is?region=eu-west-3#alarmsV2:alarm/CPU%20d%C3%A9passe%2080%20%25>

**Alarm Details:**

- Name: CPU dépasse 80 %
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [98.76426197836167 (26/01/25 21:41:00)] was greater than the threshold (80.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Sunday, 26 January, 2025 21:46:55 UTC
- AWS Account: 140023371742
- Alarm Arn: arn:aws:cloudwatch:eu-west-3:140023371742:alarm:CPU dépasse 80 %

**Threshold:**

- The alarm is in the ALARM state when the metric is GreaterThanThreshold 80.0 for at least 1 of the last 1 period(s) of 300 seconds.

**Monitored Metric:**

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-00e17d34d1a18ee31]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified
- TreatMissingData: missing

**State Change Actions:**

- OK
- ALARM: I am using sns.eu-west-3.140023371742.alertes\_cloudwatch
- ALARM: I am using sns.eu-west-3.140023371742.alertes\_cloudwatch

## Job 6

# Automatiser l'ingestion et la transformation de données en utilisant un pipeline de données.

## Objectifs :

1. [Préparer les fichiers bruts et les charger dans Amazon S3](#)
  2. [Utiliser AWS Glue pour :](#)
    - Créer un *crawler* qui détecte automatiquement les schémas des données.
    - Effectuer des transformations de données.
    - Sauvegarder les données transformées dans Amazon S3.
- 

## Étapes :

### 1. Préparer les fichiers bruts et les charger dans Amazon S3

- **Créer un Bucket S3 :**
  1. Accédez à la console Amazon S3.
  2. Cliquez sur **Créer un bucket**.
  3. Donnez un nom unique au bucket et sélectionnez une région.
  4. Configurez les options de stockage (activités par défaut pour le niveau gratuit).
  5. Finalisez la création.

### Créer un compartiment Info

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

#### Configuration générale

##### Région AWS

Europe (Paris) eu-west-3

##### Nom du compartiment Info

mon-bucket-donnees-glue

Le nom du compartiment doit être unique dans l'espace de nommage global et respecter les règles de dénomination du compartiment.

##### Copier les paramètres depuis un compartiment existant - *facultatif*

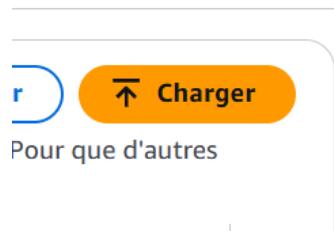
Seuls les paramètres de compartiment dans la configuration suivante sont copiés.

[Sélectionner un compartiment](#)

Format : s3://bucket/prefix

- Charger les fichiers de données :

1. Accédez au bucket créé.
2. Cliquez sur Télécharger.



3. Sélectionnez vos fichiers bruts et cliquez sur Charger.

Fichiers et dossiers (1 total, 5.2 Ko)			
Tous les fichiers et dossiers de cette table seront chargés.			
<input type="button" value="Supprimer"/> <input type="button" value="Ajouter des fichiers"/> <input style="border: none; background-color: #f0f0f0; padding: 2px 5px; border-radius: 5px;" type="button" value="..."/>			
<input type="checkbox"/> Nom	<input type="checkbox"/> Dossier	<input type="checkbox"/> Type	<input type="checkbox"/> Taille
<input type="checkbox"/> utilisateurs_transformes.csv	-	text/csv	5.2 Ko

## 2. Configurer AWS Glue pour détecter les schémas des données

- Créer un rôle IAM pour Glue :

1. Accédez à la console IAM.
2. Créez un rôle avec la politique « Glue Service ».

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.

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**

Glue

Choisissez un cas d'utilisation pour le service spécifié.

**Cas d'utilisation**

Glue  
Allows Glue to call AWS services on your behalf.

[Annuler](#)

- Ajoutez des permissions pour accéder à S3 (politique gérée comme **AmazonS3FullAccess**).

## 1. Créer un rôle IAM

- Dans le menu de gauche, clique sur **Rôles > Créer un rôle**.
- Sélectionne **AWS Service > Glue**.
- Clique sur **Suivant**.

## 2. Ajouter des permissions

- Cherche **AmazonS3FullAccess** et coche la case.

### Ajouter des autorisations Infos

**Politiques des autorisations (1/1035) Infos**

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

Filtrer par Type: Tous les types | 1 correspondance

Nom de la politique	Type	Description
<input checked="" type="checkbox"/> <b>AmazonS3FullAccess</b>	Gérées par AWS	Provides full access to all buckets via the ...

▶ Définir une limite d'autorisations - *facultatif*

Annuler Précédent Suivant

- Cherche **AWSGlueServiceRole** et coche la case.

### Politiques des autorisations (2/1035) Infos

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

Filtrer par Type: Tous les types | 1 correspondance

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

- Clique sur **Suivant**.

## 3. Nommer le rôle

Donne un nom à ton rôle, par exemple :

## GlueS3Role

### Nommer, vérifier et créer

#### Informations du rôle

##### Nom du rôle

Saisissez un nom explicite pour identifier ce rôle.

GlueS3Role

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

##### Description

Ajoutez une brève explication de ce rôle.

Allows Glue to call AWS services on your behalf.

Nombre maximum de 1000 caractères. Utilisez des lettres (A-Z et a-z), des chiffres (0-9), des tabulations, des nouvelles lignes ou l'un des caractères

- Clique sur **Créer un rôle**.
- **Créer un Crawler dans AWS Glue (Un crawler analyse les fichiers dans S3 et détecte leur schéma) :**
  1. Accédez à la console AWS Glue.
  2. Cliquez sur **Crawlers > Ajouter un crawler**.

The screenshot shows the AWS Glue console interface. On the left, there is a navigation sidebar with options like Getting started, ETL jobs, Visual ETL, Notebooks, Job run monitoring, Data Catalog tables, Data connections, Workflows (orchestration), Data Catalog (Databases, Tables, Stream schema registries, Schemas, Connections, Crawlers, Classifiers), and a search bar. The main content area is titled "Crawlers" and contains a sub-header "Crawlers (0) Info". It says "View and manage all available crawlers." and "Last updated (UTC) February 22, 2025 at 20:42:57". There is a "Create crawler" button. Below this, there is a table header with columns: Name, State, Schedule, Last run, Last run ti..., Log, and Table change... A search bar labeled "Filter crawlers" is above the table. The table body displays the message "No resources" and "No resources to display.".

3. Configurez la source des données (le bucket S3 contenant vos fichiers).

**Add data source**

**Data source**  
Choose the source of data to be crawled.

S3

**Network connection - optional**  
Optional include a Network connection to use with this S3 target. Note that each crawler is limited to one Network connection so any other S3 targets will also use the same connection (or none, if left blank).

Clear selection  

**Location of S3 data**

In this account  
 In a different account

**S3 path**  
Browse for or enter an existing S3 path.

All folders and files contained in the S3 path are crawled. For example, type s3://MyBucket/MyFolder/ to crawl all objects in MyFolder within MyBucket.

**Subsequent crawler runs**  
This field is a global field that affects all S3 data sources.

Crawl all sub-folders

4. Associez un rôle IAM au crawler.

Step 1 Set crawler properties

Step 2 Choose data sources and classifiers

**Step 3 Configure security settings**

Step 4 Set output and scheduling

Step 5 Review and create

**Configure security settings**

**IAM role** Info  
Existing IAM role  
GlueS3Role

Create new IAM role   Update chosen IAM role

Only IAM roles created by the AWS Glue console and have the prefix "AWSGlueServiceRole-" can be updated.

**Lake Formation configuration - optional**  
Allow the crawler to use Lake Formation credentials for crawling the data source. [Learn more](#)

- Créer une base de données Glue
- Sélectionne Créer une base de données.

The screenshot shows the AWS Glue Crawler creation wizard. The left sidebar lists various AWS services like ETL jobs, Notebooks, and Data Catalog tables. The main area shows a five-step process: Step 1 (Set crawler properties), Step 2 (Choose data sources and classifiers), Step 3 (Configure security settings), Step 4 (Set output and scheduling), and Step 5 (Review and create). Step 4 is currently active. On the right, under 'Set output and scheduling', there's an 'Output configuration' section. It includes a dropdown for 'Target database' which has 'base\_donnees\_glue' selected. There are also fields for 'Table name prefix - optional' and 'Maximum table threshold - optional'.

Nom de la base de données :  
**base\_donnees\_glue**

The screenshot shows the AWS Glue Databases creation wizard. The left sidebar lists various AWS services. The main area shows a 'Create a database' form. Under 'Database details', the 'Name' field contains 'base\_donnees\_glue'. There are also sections for 'Description - optional' and 'Database settings' with a 'Location - optional' field. At the bottom right, there are 'Cancel' and 'Create database' buttons.

- Clique sur **Suivant > Crée le crawler.**

The screenshot shows the AWS Glue Crawler creation wizard again. The left sidebar and steps are identical to the previous screenshot. The main area shows Step 4: Set output and scheduling. The 'Output configuration' section is visible, showing 'base\_donnees\_glue' selected as the target database. The 'Table name prefix - optional' field is empty. A note at the bottom states: 'This field sets the maximum number of tables the crawler is allowed to generate. In the event that this n'.

## ○ Lancer le Crawler

**Review and create**

**Step 1: Set crawler properties**

Name mon-crawler-donnees	Description	Tags	Edit
-----------------------------	-------------	------	------

**Step 2: Choose data sources and classifiers**

Data sources (1) <small>Info</small> The list of data sources to be scanned by the crawler.			Edit
Type S3	Data source s3://mon-bucket-donnees-glue/	Parameters Recrawl all	

**Step 3: Configure security settings**

IAM role GlueS3Role	Security configuration	Lake Formation configuration	Edit
------------------------	------------------------	------------------------------	------

**Step 4: Set output and scheduling**

Database base_donnees_glue	Table prefix - optional	Maximum table threshold - optional	Schedule On demand
-------------------------------	-------------------------	------------------------------------	-----------------------

Cancel Previous Create crawler

- Sélectionne ton crawler.
- Clique sur **Exécuter le crawler**.
- Attends qu'il termine.

**Le crawler a détecté le schéma de tes données et l'a stocké dans Glue !**

## Set output and scheduling

**Output configuration Info**

**Target database**

Choose a database ▾ C

Clear selection Add database

✖ Target database is required

**Table name prefix - optional**

**Create a database**  
Create a database in the AWS Glue Data Catalog.

<b>Database details</b>	
Name base_donnees_glue	
Database name is required, in lowercase characters, and no longer than 255 characters.	
<b>Description - optional</b>	
Enter text	
Descriptions can be up to 2048 characters long.	

**Database settings**

**Location - optional**  
Set the URI location for use by clients of the Data Catalog.

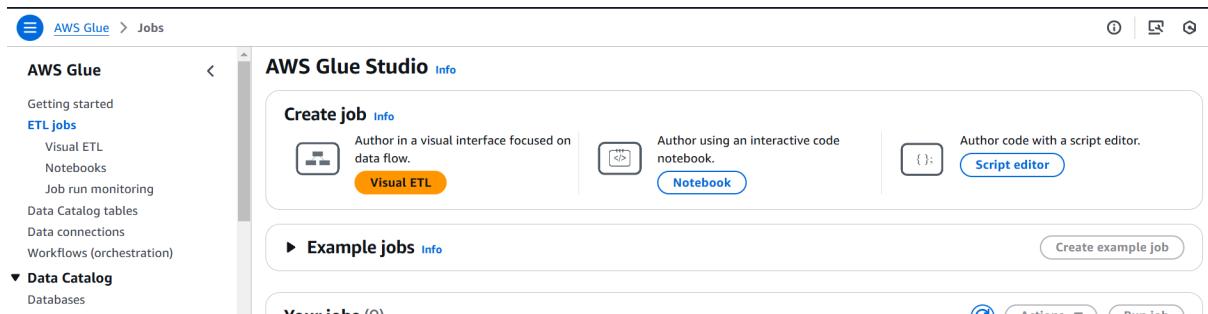
Cancel Create database

5. Planifiez le *crawler* pour qu'il s'exécute immédiatement ou à des intervalles définis.
- 

### 3. Transformer les données avec AWS Glue

- **Créer un script Glue ETL (Extract-Transform-Load) :**

1. Accédez à la console Glue.
2. Cliquez sur **Jobs > Ajouter un job**.



3. Choisissez un rôle IAM et configurez l'emplacement S3 de sortie.
4. Écrivez ou générez un script ETL en Python pour transformer les données

```
import sys

from awsglue.transforms import *

from awsglue.utils import getResolvedOptions

from pyspark.context import SparkContext

from awsglue.context import GlueContext

from awsglue.job import Job

from pyspark.sql.functions import col

# Initialisation de Glue

args = getResolvedOptions(sys.argv, ['JOB_NAME'])
```

```
sc = SparkContext()

glueContext = GlueContext(sc)

spark = glueContext.spark_session

job = Job(glueContext)

job.init(args['JOB_NAME'], args)

# Charger les données depuis Glue Data Catalog

datasource =
glueContext.create_dynamic_frame.from_catalog(database="base_donnees_glue",
table_name="mon_bucket_donnees_")

# Conversion en DataFrame Spark

df = datasource.toDF()

# Transformation 1: Mettre tous les noms de colonnes en majuscules

df = df.toDF(*[c.upper() for c in df.columns])

# Vérifier que les colonnes EMAIL et PASSWORD existent

if "EMAIL" in df.columns and "PASSWORD" in df.columns:

    # Transformation 2: Déplacer la colonne PASSWORD après EMAIL

    colonnes = df.columns

    colonnes.remove("PASSWORD") # Supprimer PASSWORD de sa position actuelle

    index_email = colonnes.index("EMAIL") # Trouver l'index d'EMAIL

    colonnes.insert(index_email + 1, "PASSWORD") # Insérer PASSWORD juste après EMAIL

    df = df.select(*colonnes) # Réorganiser les colonnes

# Correction : Assurer l'écriture en CSV dans S3 avec un dossier unique
```

```

output_path =
"s3://mon-bucket-donnees-glue/donnees-transformees/utilisateurs_transformes"

# Enregistrer sous forme de DataFrame Pandas pour garantir un seul fichier CSV
df.coalesce(1).write.mode("overwrite").option("header", "true").csv(output_path)

# Finalisation du job

job.commit()

```

- **Exécuter le job :**

1. Lancez le job.
2. Vérifiez les journaux pour surveiller l'exécution.

**mon-bucket-donnees-glue** Info

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (2)** [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">donnees-transformees/</a>	Folder	-	-	-
<input type="checkbox"/>	<a href="#">utilisateurs_transformes.csv</a>	csv	February 22, 2025, 18:51:26 (UTC+01:00)	5.2 KB	Standard

## Job 7

**Effectuer des requêtes SQL sur des données stockées dans S3 et visualiser les résultats avec QuickSight.**

### 1. Importer des fichiers de données dans S3

#### Pourquoi S3 ?

Amazon S3 est un service de stockage scalable qui permet de stocker des fichiers (données brutes, fichiers CSV, JSON, etc.). Athena peut interroger directement les fichiers stockés sans qu'il soit nécessaire d'utiliser une base de données traditionnelle.

#### Procédure :

##### 1. Créer un Bucket S3

- Accédez à la console AWS et allez dans **S3**.
- Cliquez sur **Créer un bucket**.
- Donnez un nom unique au bucket et choisissez une région.
- Désactivez **Bloquer l'accès public** si nécessaire (dans un environnement contrôlé).
- Cliquez sur **Créer un bucket**.

##### 2. Importer des fichiers dans le bucket

- Ouvrez le bucket et cliquez sur **Téléverser**.
- Ajoutez vos fichiers (CSV, JSON, etc.).
- Cliquez sur **Téléverser**.

---

### 2. Utiliser Athena pour interroger les données directement dans S3

#### Pourquoi Athena ?

AWS Athena est un service sans serveur qui permet d'exécuter des requêtes SQL sur des données stockées dans S3.

#### Configuration et utilisation d'Athena

##### 1. Configurer un emplacement de requêtes

- Allez dans **Athena** depuis la console AWS.
- Cliquez sur **Configurer un emplacement de requête**.

- Choisissez votre bucket S3 et créez un dossier (ex: `s3://mon-bucket/athena-results/`).
- Sauvegardez les modifications.

## 2. Créer une base de données et une table

- Ouvrez l'éditeur de requêtes d'Athena.

Exécutez cette requête SQL pour créer une base de données :

sql

CopierModifier

```
CREATE DATABASE mon_base_de_donnees;
```

- 

Passez sur cette base de données en exécutant :

sql

CopierModifier

```
USE mon_base_de_donnees;
```

- 

Créez une table en définissant son schéma (ex: pour un fichier CSV avec des colonnes `id`, `nom`, `age`) :

sql

CopierModifier

```
CREATE EXTERNAL TABLE mon_table (
    id INT,
    nom STRING,
    age INT
)
ROW FORMAT DELIMITED
FIELDS TERMINATED BY ','
STORED AS TEXTFILE
LOCATION 's3://mon-bucket/donnees/' ;
```

- 

## 3. Exécuter des requêtes SQL sur les données

Exemple de requête pour récupérer tous les enregistrements :

sql

CopierModifier

```
SELECT * FROM mon_table;
```

- 

Filtrer les données :

sql

CopierModifier

```
SELECT * FROM mon_table WHERE age > 30;
```

o

---

### 3. Créer des tableaux de bord dans QuickSight

#### Pourquoi QuickSight ?

AWS QuickSight est un outil de visualisation permettant de créer des tableaux de bord dynamiques à partir de sources de données comme Athena.

#### Configuration et création de visualisations

##### 1. Activer QuickSight

- o Accédez à la console AWS QuickSight.
- o Inscrivez-vous et activez un abonnement.
- o Connectez QuickSight à S3 et Athena.

##### 2. Créer une source de données à partir d'Athena

- o Dans QuickSight, cliquez sur **Gérer les données** → **Ajouter une source de données**.
- o Sélectionnez **Athena**, donnez un nom à la source et connectez-vous à votre base de données.

##### 3. Créer un jeu de données

- o Sélectionnez la table créée avec Athena (`mon_table`).
- o Configurez le jeu de données et chargez les données.

##### 4. Créer des visualisations

- o Ajoutez des graphiques, des tableaux et des filtres selon vos besoins.
- o Exemple : un histogramme montrant le nombre de personnes par tranche d'âge.