

# LAB AWS — Système de Notification d'Événements

## Objectif :

Recevoir un **email automatique** chaque fois qu'un **fichier est chargé dans un bucket S3**.

## Services AWS Utilisés

Dans le cadre de ce projet, plusieurs services managés d'AWS ont été mis en œuvre pour automatiser la chaîne de notification à partir d'un événement S3. En effet, chaque service a été configuré pour interagir de manière sécurisée et automatisée, respectant les bonnes pratiques AWS en matière de permissions, de découplage et d'architecture événementielle. Voici une description des services utilisés :

### 1. Amazon S3 (Simple Storage Service)

Amazon S3 est un service de stockage d'objets hautement disponible et scalable.

**Rôle dans le projet** : Déclencheur de l'événement. Lorsqu'un fichier est téléversé dans le bucket S3, il génère un événement qui active la fonction Lambda.

### 2. AWS Lambda

Lambda permet d'exécuter du code sans provisionner ou gérer de serveurs (serverless).

**Rôle dans le projet** : Fonction qui reçoit l'événement de S3, traite les métadonnées du fichier (nom, type, etc.), et publie un message dans le sujet SNS.

### 3. Amazon SNS (Simple Notification Service)

SNS est un service de messagerie pub/sub entièrement managé qui permet l'envoi de notifications aux abonnés.

**Rôle dans le projet** : Transmet l'information reçue de Lambda par **email** aux abonnés du sujet SNS.

### 4. AWS IAM (Identity and Access Management)

IAM permet de gérer les autorisations et les rôles pour sécuriser l'accès aux services AWS.

**Rôle dans le projet** : Attribution des **autorisations minimales nécessaires** à Lambda pour accéder à S3 et publier sur SNS.

## Étape 1 – Créer le Bucket S3

1. Va dans **Amazon S3** → clique sur **Créer un compartiment**
2. Donne un nom unique, ex : sns-bucket-lab25
3. Laisse **toutes les options par défaut**, sauf :
  - Décoche **"Bloquer tout l'accès public"** si tu veux tester les accès publics
4. Clique sur **Créer un compartiment**

**Amazon S3** > Compartiments

**Aperçu du compte : mis à jour toutes les 24 heures** Toutes les régions AWS [Afficher le tableau de bord de Storage Lens](#)

Storage Lens offre une visibilité sur l'utilisation du stockage et les tendances d'activité. Les métriques ne comprennent pas les compartiments de répertoire. [En savoir plus](#)

**Compartiments à usage général** Compartiments de répertoires

**Compartiments à usage général (0)** info Toutes les régions AWS [Copier l'ARN](#) [Vider](#) [Supprimer](#) **Créer un compartiment**

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

Rechercher des compartiments par nom

Nom	Région AWS	Analyseur d'accès IAM	Date de création
Aucun compartiment			

Aucun compartiment  
Vous n'avez aucun compartiment.

[Créer un compartiment](#)

**Créer un compartiment** info

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

**Configuration générale**

**Région AWS**  
USA Ouest (Oregon) us-west-2

**Type de compartiment** info

☒ **Usage général**  
Recommandé pour la plupart des cas d'utilisation et des modèles d'accès. Les compartiments à usage général sont du type de compartiment S3 d'origine. Ils permettent une combinaison de classes de stockage qui stockent de manière redondante des objets dans plusieurs zones de disponibilité.

☐ **Annuaire**  
Recommandé pour les cas d'utilisation à faible latence. Ces compartiments utilisent uniquement la classe de stockage S3 Express One Zone, qui permet un traitement plus rapide des données au sein d'une seule zone de disponibilité.

**Nom du compartiment** info

sns-bucket-lat25

Les noms de compartiment doivent comporter de 3 à 63 caractères et être uniques dans l'espace de noms global. Les noms des compartiments doivent également commencer et se terminer par une lettre ou un chiffre. Les caractères valides sont les suivants : a-z, 0-9, points (.) et tirets (-). [En savoir plus](#)

**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

**Propriété d'objets** info

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

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

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

**Propriété d'objets**  
Propriétaire du compartiment appliqué

**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 fonctionneront correctement sans accès public. Si vous souhaitez autoriser un certain niveau d'accès public pour votre compartiment ou ses objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos besoins en stockage. [En savoir plus](#)

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

☐ **Bloquer l'accès public aux compartiments et aux objets, accordé via de nouvelles listes de contrôle d'accès (ACL)**  
S3 bloque les autorisations d'accès public appliquées aux compartiments ou objets récemment ajoutés et empêche la création de listes ACL d'accès public pour les compartiments et objets existants. Ce paramètre ne modifie pas les autorisations existantes qui permettent l'accès public aux ressources S3 qui utilisent les listes ACL.

☐ **Bloquer l'accès public aux compartiments et aux objets, accordé via n'importe quelles listes de contrôle d'accès (ACL)**  
S3 ignore toutes les listes ACL qui accordent l'accès public aux compartiments et aux objets.

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

☐ **Bloquer l'accès public et entre comptes aux compartiments et objets via n'importe quelles stratégies de compartiment ou de point d'accès public**  
S3 ignore l'accès public et entre comptes pour les compartiments ou points d'accès avec des stratégies qui accordent l'accès public aux compartiments et aux objets.

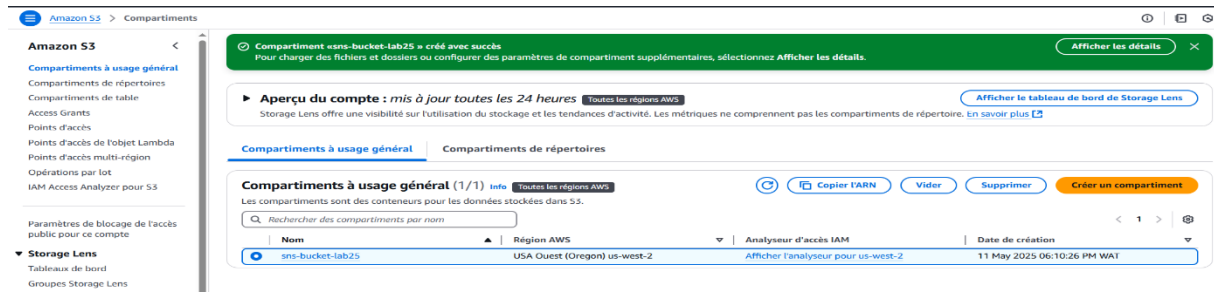
**Si le paramètre « Bloquer l'accès public » est désactivé, ce compartiment et les objets qu'il contient peuvent devenir publics.**  
AWS vous recommande de bloquer tout accès public, sauf si celui-ci est requis dans des cas d'utilisation spécifiques et vérifiés, tels que l'hébergement de site Web statique.

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

**Paramètres avancés**

Après avoir créé le compartiment, vous pouvez y charger des fichiers et des dossiers et configurer des paramètres de compartiment supplémentaires.

[Annuler](#) **Créer un compartiment**



## Étape 2 – Créer la fonction Lambda

1. Va dans **AWS Lambda** → **Créer une fonction**
2. Choisis **Créer à partir de zéro**
  - **Nom** : notifierFunction
  - **Runtime** : Python 3.12
  - **Rôle d'exécution** : créer un **nouveau rôle avec autorisations Lambda de base**
3. Clique sur **Créer la fonction**
4. Dans la section **Code source**, copie ce code :

```
import json
import boto3
import os

sns_client = boto3.client('sns')

TOPIC_ARN = os.environ['TOPIC_ARN']

def lambda_handler(event, context):

    bucket = event['Records'][0]['s3']['bucket']['name']

    key = event['Records'][0]['s3']['object']['key']

    message = f"Nouveau fichier ajouté : {key} dans le bucket {bucket}"

    sns_client.publish(

        TopicArn=TOPIC_ARN,

        Subject="Nouvel Upload S3",

        Message=message

    )

    return {

        'statusCode': 200,

        'body': json.dumps('Notification envoyée avec succès')

    }
```

5. Cliquez sur **Déployer**.

Calcul

# AWS Lambda

permet d'exécuter du code sans vous soucier des serveurs.

Vous payez uniquement le temps de calcul utilisé et vous n'êtes pas facturé lorsque votre code ne s'exécute pas. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou service dorsal, sans aucune tâche d'administration.

**Démarrer**

Créez une fonction Lambda de bout en bout ou choisissez l'un des nombreux exemples préconfigurés.

**Créer une fonction**

**Créer une fonction**

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

- ☒ **Créer à partir de zéro**  
Commencez avec un exemple Hello World simple.
- ☐ **Utiliser un plan**  
Créez une application Lambda à partir d'un exemple de code et de préconfigurations de configuration pour les cas d'utilisation courants.
- ☐ **Image de conteneur**  
Sélectionnez une image de conteneur à déployer pour votre fonction.

**Informations de base**

**Nom de la fonction**  
Entrez un nom qui décrit l'objectif de votre fonction.  
  
Le nom de la fonction doit comprendre de 1 à 64 caractères, doit être propre à la région et ne doit pas inclure d'espaces. Les caractères valides sont a-z, A-Z, 0-9, les traits d'union(-) et les traits de soulignement (\_).

**Exécution** [Info](#)  
Choisissez le langage à utiliser pour écrire votre fonction. Notez que l'éditeur de code console prend en charge uniquement Node.js, Python, et Ruby.

**Architecture** [Info](#)  
Choisissez l'architecture de jeu d'instructions (ISA) désirée pour le code de votre fonction.  
☒ **x86\_64**  
☐ arm64

**▼ Modifier le rôle d'exécution par défaut**

**Rôle d'exécution**  
Choisissez un rôle qui définit les autorisations de votre fonction. Pour créer un rôle personnalisé, accédez à la [console IAM](#).

- ☒ **Créer un nouveau rôle avec les autorisations Lambda de base**
- ☐ Utiliser un rôle existant
- ☐ Créer un nouveau rôle à partir de la stratégie AWS templates

La création du rôle peut prendre quelques minutes. Ne supprimez pas le rôle et ne modifiez pas les stratégies d'approbation ou d'autorisation de ce rôle.

Lambda va créer le rôle d'exécution `notifierFunction-role-hy84npc4` avec l'autorisation de charger des journaux vers Amazon CloudWatch Logs.

**► Configurations supplémentaires**  
Utilisez des configurations supplémentaires pour configurer la signature de code, l'URL de la fonction, les balises et l'accès Amazon VPC pour votre fonction.

[Annuler](#) **Créer une fonction**

The top screenshot shows the AWS Lambda console for the function 'notifierFunction'. A green banner at the top states: 'Fonction notifierFunction créée avec succès. Vous pouvez désormais modifier son code et sa configuration. Pour appeler votre fonction avec un événement de test, choisissez « Test ».' The left sidebar shows the navigation menu with 'notifierFunction' selected. The main area displays the function overview, including a diagram, layers, and a description. The bottom tab bar shows 'Code', 'Tester', 'Surveiller', 'Configuration', 'Alias', and 'Versions'.

The bottom screenshot shows the 'Source du code' page for 'notifierFunction'. The 'EXPLORER' pane on the left shows the file structure. The main editor displays the code for 'lambda\_function.py'. A red circle highlights the 'Deploy (Ctrl+Shift+I)' button in the 'DEPLOY (UNDEPLOYED CHANGES)' section. The code in the editor is as follows:

```

1 import json
2 import boto3
3 import os
4
5 sns_client = boto3.client('sns')
6 TOPIC_ARN = os.environ['TOPIC_ARN']
7
8 def lambda_handler(event, context):
9     bucket = event['Records'][0]['s3']['bucket']['name']
10    key = event['Records'][0]['s3']['object']['key']
11
12    message = f"Nouveau fichier ajouté : {key} dans le bucket {bucket}"
13
14    sns_client.publish(
15        TopicArn=TOPIC_ARN,
16        Subject="Nouvel Upload S3",
17        Message=message
18    )
19
20    return {
21        'statusCode': 200,
22        'body': json.dumps('Notification envoyée avec succès')
23    }
24

```

## Étape 3 – Créer un Topic SNS et s'abonner

1. Va dans **Amazon SNS** → **Créer un sujet**
  - Type : **Standard**
  - Nom : **S3UploadTopic**
2. Clique sur **Créer un sujet**
3. Clique ensuite sur **Créer un abonnement**
  - Protocole : **Email**
  - Point de terminaison : ton adresse email (ex: test@gmail.com)
4. Tu vas recevoir un email → clique sur **Confirmer l'abonnement**

6

The screenshot displays the AWS SNS console and a Gmail inbox. In the AWS SNS console, a subscription for topic '97a70d1b-e4f0-4d75-bb6c-356cbd51b6f8' is shown, with status 'Confirmation en attente'. The email in the Gmail inbox is titled 'AWS Notification - Subscription Confirmation' and contains the following text:

You have chosen to subscribe to the topic:  
**arn:aws:sns:us-west-2: [redacted]:S3UploadTopic**

To confirm this subscription, click or visit the link below (if this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](mailto:sns-opt-out)

The browser address bar shows the confirmation URL: `sns.us-west-2.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-west-2:[redacted]:S3UploadTopic&Token=2336412f37fb687f5d...`



Service de notification simple

**Abonnement confirmé !**

Vous êtes inscrit avec succès.

L'identifiant de votre abonnement est :

arn:aws:sns:us-west-2:[redacted]:S3UploadTopic:97a70d1b-e4f0-4d75-bb6c-356cbd51b6f8

Si ce n'était pas votre intention de vous abonner, [cliquez ici pour vous désabonner](#).



Amazon SNS > Rubriques > S3UploadTopic

**Détails**

Nom S3UploadTopic	Nom complet -
ARN arn:aws:sns:west-2- <span style="background-color: red; color: black;">XXXXXXXXXX</span> :S3UploadTopic	Propriétaire de la rubrique <span style="background-color: red; color: black;">XXXXXXXXXX</span>
Type Standard	

**Abonnements (1)**

ID	Point de terminaison	Statut	Protocole
Supprimé	stanbant94@gmail.com	Confirmé	EMAIL

## Étape 4 – Ajouter les variables d'environnement et permissions

- Va dans ta fonction Lambda → onglet **Configuration > Variables d'environnement**
  - Ajoute : TOPIC\_ARN = colle l'ARN de ton Topic SNS
- Va dans **Configuration > Autorisations**  
Clique sur le nom du rôle IAM attaché à la fonction
  - Ajoute cette **stratégie en ligne** :

```
{
  "Effect": "Allow",
  "Action": "sns:Publish",
  "Resource": "arn:aws:sns:REGION:ACCOUNT_ID:S3UploadTopic"
}
```

Remplace REGION, ACCOUNT\_ID par les valeurs de ton compte

Lambda > Fonctions > notifierFunction

**Variables d'environnement (0)**

Aucune variable d'environnement n'est associée à cette fonction.

[Ajouter des variables d'environnement](#)

Lambda > Fonctions > notifierFunction > Modifier les variables d'environnement

**Modifier les variables d'environnement**

**Variables d'environnement**

Vous pouvez définir des variables d'environnement comme paires clé-valeur accessibles depuis le code de votre fonction. Ces variables sont pratiques pour stocker les paramètres de configuration sans avoir à modifier le code de la fonction. [En savoir plus](#)

Il n'existe pas de variable d'environnement pour cette fonction.

[Ajouter des variables d'environnement](#)

► Configuration du chiffrement

[Annuler](#) [Enregistrer](#)



[notifierFunction](#) > Modifier les variables d'environnement

## Modifier les variables d'environnement

**Variables d'environnement**  
Vous pouvez définir des variables d'environnement comme paires clé-valeur accessibles depuis le code de votre fonction. Ces variables sont pratiques pour stocker les paramètres de configuration sans avoir à modifier le code de la fonction. [En savoir plus](#)

Clé	Valeur	
TOPIC_ARN	arn:aws:sns:us-west-2:██████████:██████████S3UploadTopic	<a href="#">Supprimer</a>

[Ajouter des variables d'environnement](#)

► Configuration du chiffrement

[Annuler](#) [Enregistrer](#)

Mise à jour de la fonction **notifierFunction** effectuée avec succès.

Code | Tester | Surveiller | **Configuration** | Alias | Versions

Configuration générale | Déclencheurs | Autorisations | Destinations | URL de fonction | **Variables d'environnement**

### Variables d'environnement (1)

Les variables d'environnement ci-dessous sont chiffrées au repos avec la clé de service Lambda par défaut.

Rechercher des variables d'environnement

Clé	Valeur
TOPIC_ARN	arn:aws:sns:us-west-2:██████████:██████████S3UploadTopic

[Modifier](#)

Lambda > Fonctions > notifierFunction

**Lambda**

- Tableau de bord
- Applications
- Fonctions
  - notifierFunction**
- ▼ Ressources supplémentaires
  - Configurations de signature de code
  - Mappages des sources d'événements
  - Couches
  - Réplicas
- ▼ Ressources AWS connexes
  - Machines d'état Step Functions

Configuration générale | Déclencheurs | **Autorisations** | Destinations | URL de fonction | Variables d'environnement

### Rôle d'exécution

Nom du rôle  
[notifierFunction-role-hy84npc4](#)

Récapitulatif des ressources  
Pour afficher les ressources et les actions auxquelles votre fonction est autorisée à accéder, choisissez un service.

Amazon CloudWatch Logs  
9 actions, 2 ressources

Par action | **Par ressource**

Ressource	Actions
arn:aws:logs:us-west-2:██████████:log-group:/aws/lambda/notifierFunction:*	Allow: logs:CreateLogGroup
arn:aws:logs:us-west-2:██████████:log-group:/aws/lambda/notifierFunction:*	Allow: logs:CreateLogStream Allow: logs:PutLogEvents

[Modifier](#) [Afficher le document de rôle](#)

May 11, 2025, 18:15 (UTC+01:00)

**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
- ▼ Rapports d'accès
  - Analysateur d'accès
  - Accès externe
  - Accès non utilisé

**Autorisations** | Relations d'approbation | Balises | Dernier accès | Révoquer les séances

### Politiques des autorisations (1/1) Infos

Vous pouvez attacher jusqu'à 10 politiques gérées.

Rechercher

Filtrer par Type  
Tous les types

1 2 3 4 5 6

1 - Nom de la politique

2 - Type

3 - Entités attachées

4 - ☒ ☐ AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434 Gérées par le client 1

**AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434**

[Copier JSON](#) [Modifier](#)

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "logs:CreateLogGroup",
7       "Resource": "arn:aws:logs:us-west-2:██████████:log-group:/aws/lambda/notifierFunction:*"
8     }
9   ]
10 }
```

Étape 1 **Modifier les autorisations dans AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434** [Infos](#)

Étape 2 Vérifier et enregistrer

### Modifier les autorisations dans AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434 [Infos](#)

Ajouter des autorisations en sélectionnant des services, des actions, des ressources et des conditions. Créer des instructions d'autorisation à l'aide de l'éditeur JSON.

**Éditeur de politique**

Visuel **JSON**

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "logs:CreateLogGroup",
7       "Resource": "arn:aws:logs:us-west-2:123456789012:log-group:/*",
8     },
9     {
10      "Effect": "Allow",
11      "Action": "sns:Publish",
12      "Resource": "arn:aws:sns:us-west-2:123456789012:S3UploadTopic",
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "logs:CreateLogStream",
18        "logs:PutLogEvents"
19      ],
20      "Resource": [
21        "arn:aws:logs:us-west-2:123456789012:log-group:/aws/lambda/notifierFunction:*"
22      ]
23    }
24  ]
25 }
```

Modifier l'inst

Ajouter des a

Choisir un sen

Q Filtrer le

Inclus

SNS

Disponible

AI Operations

AMP

API Gateway

API Gateway

ARC Zonal Shi

ASC

Ajouter une r

5736 de 6144 caractères restants

vertissements: 0 Suggestions: 0

Vérification de nouvel accès

Annuler **Suivant**

Étape 1 **Modifier les autorisations dans AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434** [Infos](#)

Étape 2 **Vérifier et enregistrer**

### Vérifier et enregistrer [Infos](#)

Vérifier les autorisations, spécifiez les détails et les identifications.

**Autorisations définies dans cette politique** [Infos](#)

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

Rechercher

Autoriser (2 des 439 services) Afficher les services 437 restants

Service	Niveau d'accès	Ressource	Demande de condition
CloudWatch Logs	Limité: Écriture	Multiple	None
SNS	Limité: Écriture	TopicName  chaîne similaire [S3UploadTopic, region] chaîne similaire [us-west-2	None

☒ Définissez cette nouvelle version comme version par défaut.  
Les autorisations définies dans cette version seront appliquées à toutes les entités auxquelles cette politique est attachée.

Annuler Précédent **Enregistrer les modifications**

The first screenshot shows the 'AWSLambdaBasicExecutionRole-85b000f0-196d-4b63-b9f8-231e1e952434' policy page. The 'Autorisations définies dans cette politique' tab is active, showing a table of authorized services:

Service	Niveau d'accès	Ressource	Demande de condition
CloudWatch Logs	Limité: Écriture	Multiple	None
SNS	Limité: Écriture	TopicName] chaîne similaire [SNSUploadTopic, region] chaîne similaire [us-west-2	None

The second screenshot shows the 'Entités attachées' tab, which is currently empty, indicating that no entities are attached to this policy.

## Étape 5 – Connecter S3 à Lambda

1. Va dans **S3** > ouvre ton bucket
2. Onglet **Propriétés** → **Événements**
  - Clique sur **Créer un événement**
    - Nom : uploadTrigger
    - Type d'événement : PUT
    - Cible : **fonction Lambda**
    - Sélectionne ta fonction notifierFunction
3. Clique sur **Enregistrer les modifications**

Amazon S3 > Compartiments > sns-bucket-lab25

Notifications d'événements (0)

Envoyez une notification lorsque des événements spécifiques se produisent dans votre compartiment. [En savoir plus](#)

[Modifier](#) [Supprimer](#) [Créer une notification d'événement](#)

Nom	Types d'événements	Filtres	Type de destination	Destination
Aucune notification d'événement. Sélectionnez Créer une notification d'événement pour être informé lorsqu'un événement spécifique se produit.				

[Créer une notification d'événement](#)

**Amazon EventBridge** [Modifier](#)

Pour d'autres fonctionnalités, utilisez Amazon EventBridge pour créer des applications axées sur les événements à grande échelle à l'aide de notifications d'événements S3. [En savoir plus](#) ou [consultez la tarification d'EventBridge](#)

Envoyer des notifications à Amazon EventBridge pour tous les événements de ce compartiment

Désactivé

Amazon S3 > Compartiments > sns-bucket-lab25 > Créer une notification d'événement

Créer une notification d'événement [Info](#)

Pour activer les notifications, vous devez commencer par ajouter une configuration des notifications qui identifie les événements que vous voulez qu'Amazon S3 publie et les destinations vers lesquelles vous voulez qu'Amazon S3 envoie les notifications.

**Configuration générale**

Nom de l'événement

uploadTrigger

Le nom de l'événement peut contenir jusqu'à 255 caractères.

Préfixe - facultatif

Limitez les notifications aux objets dont la clé commence par des caractères spécifiés.

images/

Suffixe - facultatif

Limitez les notifications aux objets dont la clé se termine par des caractères spécifiés.

.jpg

**Types d'événements**

Spécifiez au moins un événement pour lequel vous souhaitez recevoir des notifications. Pour chaque groupe, vous pouvez choisir un type d'événement pour tous les événements ou choisir un ou plusieurs événements individuels.

**Création d'objet**

☐ Tous les événements de création d'objets s3:ObjectCreated:\*

☒ PUT s3:ObjectCreated:Put

☐ Publier s3:ObjectCreated:Post

☐ Copier s3:ObjectCreated:Copy

☐ Chargement partitionné terminé s3:ObjectCreated:CompleteMultipartUpload

Destination

① Pour qu'Amazon S3 puisse publier des messages vers une destination, vous devez accorder au mandataire Amazon S3 les autorisations nécessaires pour appeler l'API appropriée afin de publier des messages dans une rubrique SNS, une file d'attente SQS ou une fonction Lambda. [En savoir plus](#)

**Destination**

Sélectionnez une destination pour publier l'événement. [En savoir plus](#)

☒ Fonction Lambda

Exécutez un script de fonction Lambda basé sur les événements S3.

☐ Rubrique SNS

Distribuez les messages aux systèmes pour un traitement parallèle ou directement aux personnes.

☐ File d'attente SQS

Envoyez des notifications à une file d'attente SQS pour qu'elle soit lue par un serveur.

**Spécifier Fonction Lambda**

☒ Choisissez parmi votre Fonctions Lambda

☐ Saisir l'ARN Fonction Lambda

**Fonction Lambda**

notifierFunction

Annuler [Enregistrer les modifications](#)

Amazon S3 > Compartiments > sns-bucket-lab25

Notification d'événement « uploadTrigger » créée avec succès. L'opération s'est terminée avec succès.

Notifications d'événements (1/1)

Envoyez une notification lorsque des événements spécifiques se produisent dans votre compartiment. [En savoir plus](#)

[Modifier](#) [Supprimer](#) [Créer une notification d'événement](#)

Nom	Types d'événements	Filtres	Type de destination	Destination
<input checked="" type="checkbox"/> uploadTrigger	PUT	-	Fonction Lambda	<a href="#">notifierFunction</a>

**Amazon EventBridge** [Modifier](#)

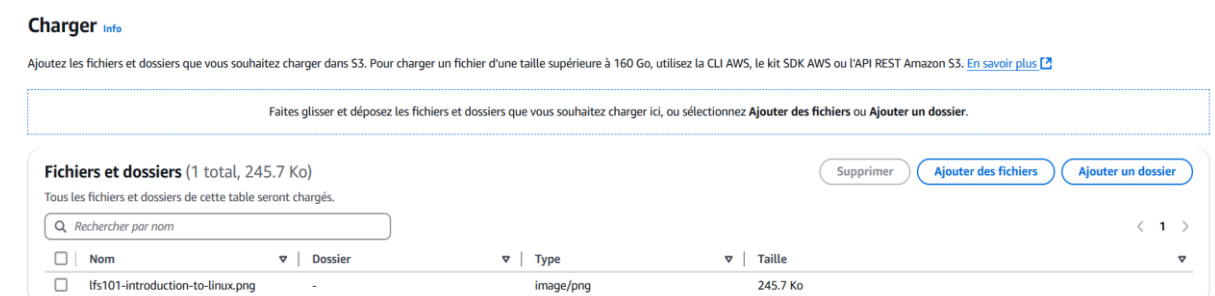
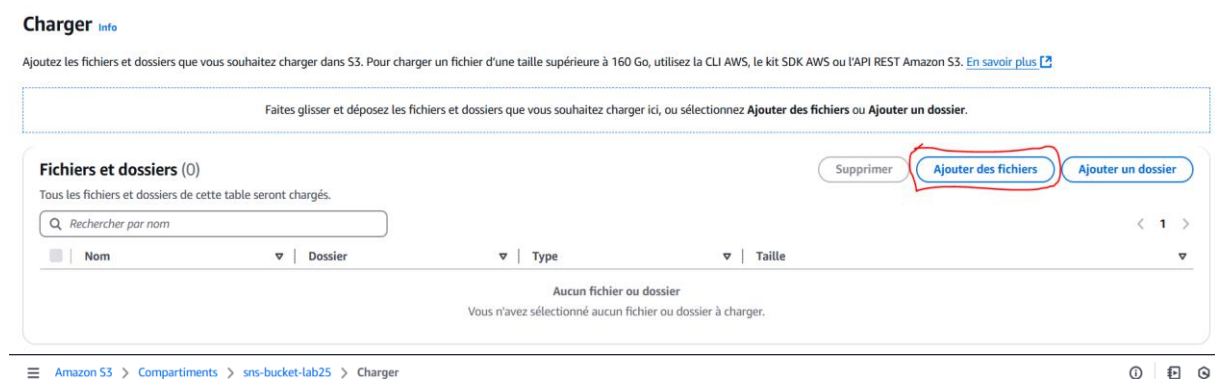
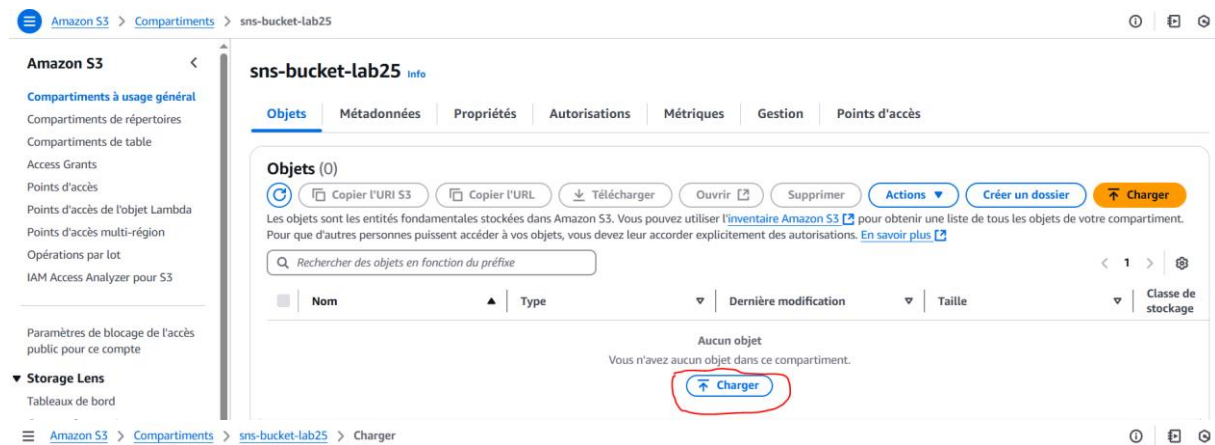
Pour d'autres fonctionnalités, utilisez Amazon EventBridge pour créer des applications axées sur les événements à grande échelle à l'aide de notifications d'événements S3. [En savoir plus](#) ou [consultez la tarification d'EventBridge](#)

Envoyer des notifications à Amazon EventBridge pour tous les événements de ce compartiment

Désactivé

## Étape 6 – Tester

1. Va dans le compartiment S3 (**sns-bucket-lab25**) → Objets → clique sur **Charger**
2. Ajouter des fichiers
3. Sélectionne le fichier et clique sur **Ouvrir**
4. Va dans ta messagerie et consulte le mail reçu en provenance de **Amazon Notifications**
5. Résultats :
  - La fonction Lambda est déclenchée
  - Tu reçois un **email SNS** avec le nom du fichier
  - Tu peux consulter les logs dans **CloudWatch Logs > notifierFunction**



► **Autorisations**

Accordez l'accès public et l'accès à d'autres comptes AWS.

► **Propriétés**

Spécifiez la classe de stockage, les paramètres de chiffrement, les balises, etc.

Annuler

**Charger**

**Amazon S3**

**Compartiments à usage général**

- Compartiments de répertoires
- Compartiments de table
- Access Grants
- Points d'accès
- Points d'accès de l'objet Lambda
- Points d'accès multi-région
- Opérations par lot
- IAM Access Analyzer pour S3

Paramètres de blocage de l'accès public pour ce compte

**Storage Lens**

- Tableaux de bord
- Groupes Storage Lens
- Paramètres AWS Organizations

Compartiments > sns-bucket-lab25

**Chargement réussi**

Pour plus d'informations, consultez le tableau Fichiers et dossiers.

Une fois que vous quittez cette page, les informations suivantes ne sont plus disponibles.

**Résumé**

<b>Destination</b> s3://sns-bucket-lab25	<b>Opération réussie</b> 1 fichier, 245.7 Ko (100.00%)	<b>Échec</b> 0 fichiers, 0 o (0%)
---	---	--------------------------------------

**Fichiers et dossiers** Configuration

**Fichiers et dossiers** (1 total, 245.7 Ko)

Rechercher par nom

Nom	Dossier	Type	Taille	Statut	Erreur
ifs101-introduction-to-li...	-	image/png	245.7 Ko	Opération réussie	-

**sns-bucket-lab25** info

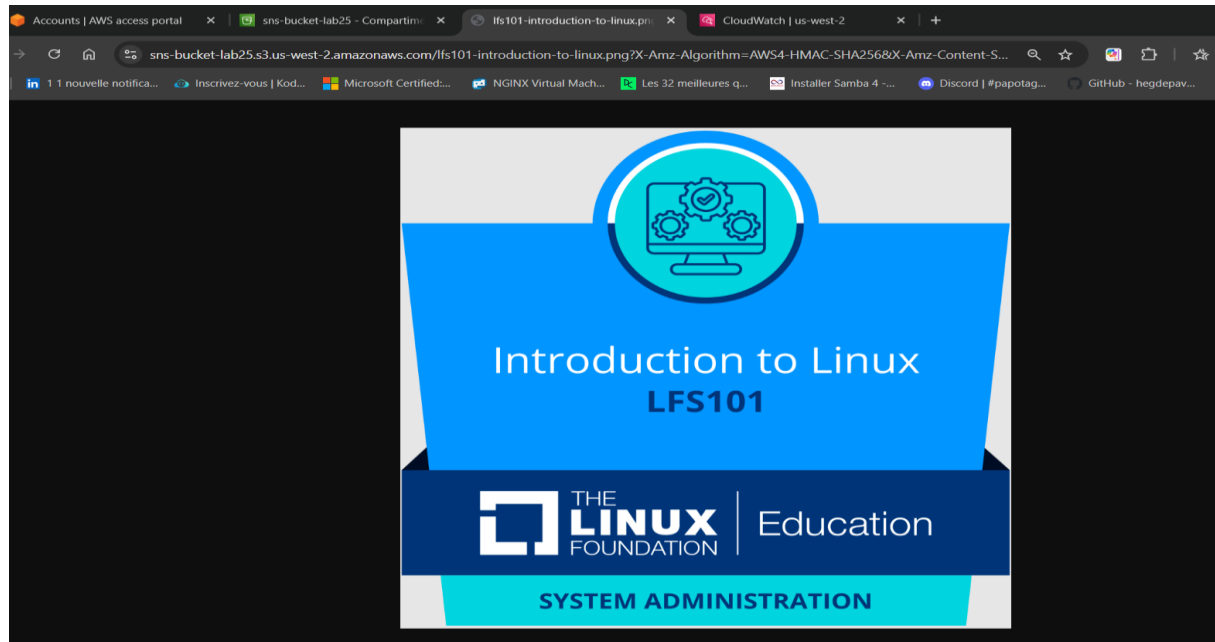
Objets Métaadonnées Propriétés Autorisations Métriques Gestion Points d'accès

**Objets** (1/1)

Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l'inventaire Amazon S3 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. [En savoir plus](#)

Rechercher des objets en fonction du préfixe

<input checked="" type="checkbox"/>	Nom	Type	Dernière modification	Taille	Classe de stockage
<input checked="" type="checkbox"/>	ifs101-introduction-to-linux.png	png	11 May 2025 07:22:02 PM WAT	245.7 Ko	Standard



**Gmail**

Rechercher dans les messages

Nouveau message

Boîte de réception 1

Messagerie suivie

En attente

Principale Promotions Réseaux sociaux Notifications

**AWS Notifications** Nouvel Upload S3 - Nouveau fichier ajouté : ifs101-introduction-to-linux.png dans le bucket sns-bucket-lab25 -- If you wish to stop receiving notifications from L... 19:22

**AWS Notifications 2** AWS Notification - Unsubscribe Confirmation - Your subscription to the topic below has been deactivated: arn:aws:sns:us-west-2:056264389880:S3UploadTopic L... 19:14

The image displays two screenshots from a web browser. The top screenshot shows a Gmail inbox with a message from 'AWS Notifications' titled 'Nouvel Upload S3 (Nouvel Upload S3)'. The message content states: 'Nouveau fichier ajouté : ifs101-introduction-to-linux.png dans le bucket sns-bucket-lab25'. It includes a link to unsubscribe and a support link. The bottom screenshot shows the AWS CloudWatch console for the Lambda function '/aws/lambda/notifierFunction'. It displays the 'Flux de journaux' (Log Streams) section with two log events. The first event is dated 2025-05-11 at 18:22:03 (UTC) and the second is dated 2025-05-11 at 18:11:56 (UTC). The console also shows the 'Événements de journaux' (Log Events) section with a table of log events.

**Gmail Message:**

**From:** AWS Notifications <no-reply@sns.amazonaws.com>  
**To:** À moi  
**Subject:** Nouvel Upload S3 (Nouvel Upload S3)

Nouveau fichier ajouté : ifs101-introduction-to-linux.png dans le bucket sns-bucket-lab25

Si vous souhaitez ne plus recevoir de notifications de ce sujet, veuillez cliquer ou visiter le lien ci-dessous pour vous désabonner :  
<https://sns.us-west-2.amazonaws.com/subscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:74464081bc20ef933c2b521f88902b0287c36c73d31d47774c5e8b8428b5d:S3UploadTopic:97a70d1b-e4f0-4d75-bb6c-356cxd51b698&Endpoint=stanbant94@gmail.com>

Veuillez ne pas répondre directement à cet e-mail. Pour toute question ou commentaire concernant cet e-mail, veuillez nous contacter à <https://aws.amazon.com/support>

**AWS CloudWatch Console:**

**/aws/lambda/notifierFunction**

**Informations de groupe de journaux**

**Flux de journaux (2)**

Flux de journaux	Heure du dernier événement
<a href="#">2025/05/11/[\$LATEST]7f6546757d9e4f5fae56e439c951b4ed</a>	2025-05-11 18:22:03 (UTC)
<a href="#">2025/05/11/[\$LATEST]65d4150793d24bed8da3f0b35521f78c</a>	2025-05-11 18:11:56 (UTC)

**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](#)

Filter les événements : appuyez sur Entrée pour rechercher.

Effacer 1m 30m 1h 12h Personnalisées Fuseau horaire UTC Affichage

Horodatage	Message
2025-05-11T18:22:02.995Z	Aucun ancien événement pour le moment <a href="#">Réessayer</a> INIT_START Runtime Version: python:3.12.v65 Runtime Version ARN: arn:aws:lambda:us-west-2::runtime:74b4a081bc20ef933c2b521f88902b0287c36c73d31d47774c5e8b8428b5d
2025-05-11T18:22:03.444Z	START RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776 Version: \$LATEST START RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776 Version: \$LATEST
2025-05-11T18:22:03.726Z	END RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776 END RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776
2025-05-11T18:22:03.727Z	REPORT RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776 Duration: 282.47 ms Billed Duration: 283 ms Memory Size: 128 MB Max Memory Used: 82 MB Init Duration: 444.81 ms REPORT RequestId: 2a37e968-fc7b-46ea-abed-fbd25a5c4776 Duration: 282.47 ms Billed Duration: 283 ms Memory Size: 128 MB Max Memory Used: 82 MB Init Duration: 444.81 ms

Aucun nouvel événement pour le moment Nouvelle tentative automatique suspendue. [Reprendre](#)