

Ameth fall

## Cloudfront + S3

### Diffusions de contenu avec Amazon CloudFront

Dans ce mini projet, nous allons diffuser du contenu et à réduire la latence de l'utilisateur final de votre application Web à l'aide d'Amazon CloudFront .

Nous allons utiliser S3 comme point origine.

#### 1. Création d'un bucket S3 :

- Sélectionnons le service au niveau de la console aws :



- Création du compartiment :



Nous allons choisir un nom, une région, une zone et un type pour le 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.
- ☐ **Répertoire - Nouveau**  
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  
projet-cloudfront

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

- Gestion des ACLS :

Nous devons activer les acls pour mettre en place des règles afin d'autoriser la diffusion du contenu de notre bucket.

M.

## 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.

**⚠ Nous vous recommandons de désactiver les listes de contrôle d'accès (ACL), sauf si vous avez besoin de contrôler l'accès à chaque objet individuellement ou de faire en sorte que l'auteur de l'objet soit propriétaire des données qu'il télécharge. L'utilisation d'une politique de compartiment au lieu d'une ACL pour partager des données avec des utilisateurs en dehors de votre compte simplifie la gestion des autorisations et l'audit.**

**Propriété d'objets**

- ☒ **Propriétaire du compartiment préféré**  
Si de nouveaux objets écrits dans ce compartiment spécifient la liste ACL prédéfinie « bucket-owner-full-control », ils appartiennent au propriétaire du compartiment ou encore au créateur de l'objet.
- ☐ **Créateur d'objets**  
Le créateur d'un objet en reste le propriétaire.

**ℹ Si vous souhaitez appliquer la propriété des objets uniquement pour les nouveaux objets, votre politique de compartiment doit spécifier que la liste ACL prédéfinie « bucket-owner-full-control » pour le contrôle complet du compartiment est obligatoire pour les chargements d'objets. [En savoir plus](#)**


Il faut décocher l'option bloquer tous les accès publics pour permettre au contenu d'être accessible.

### 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.

- Lancement de la création du compartiment :

► 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**

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

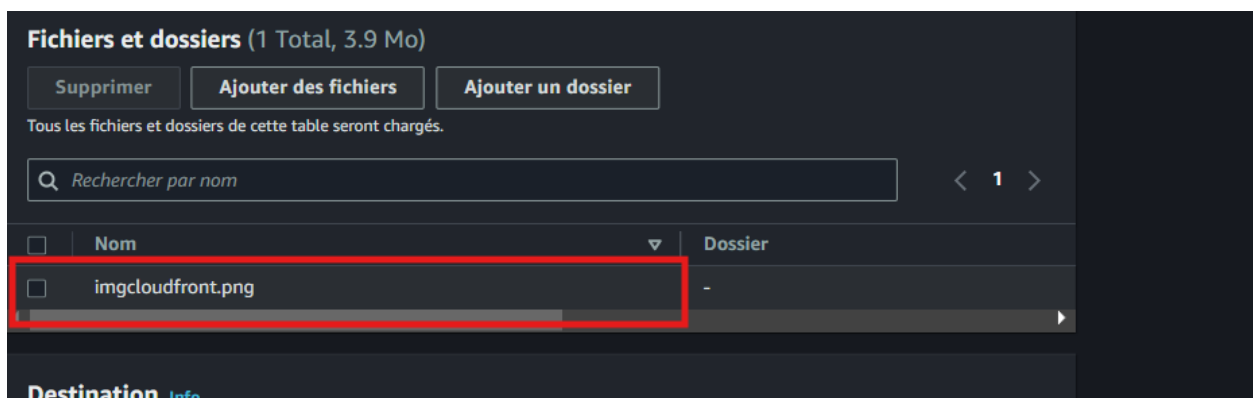
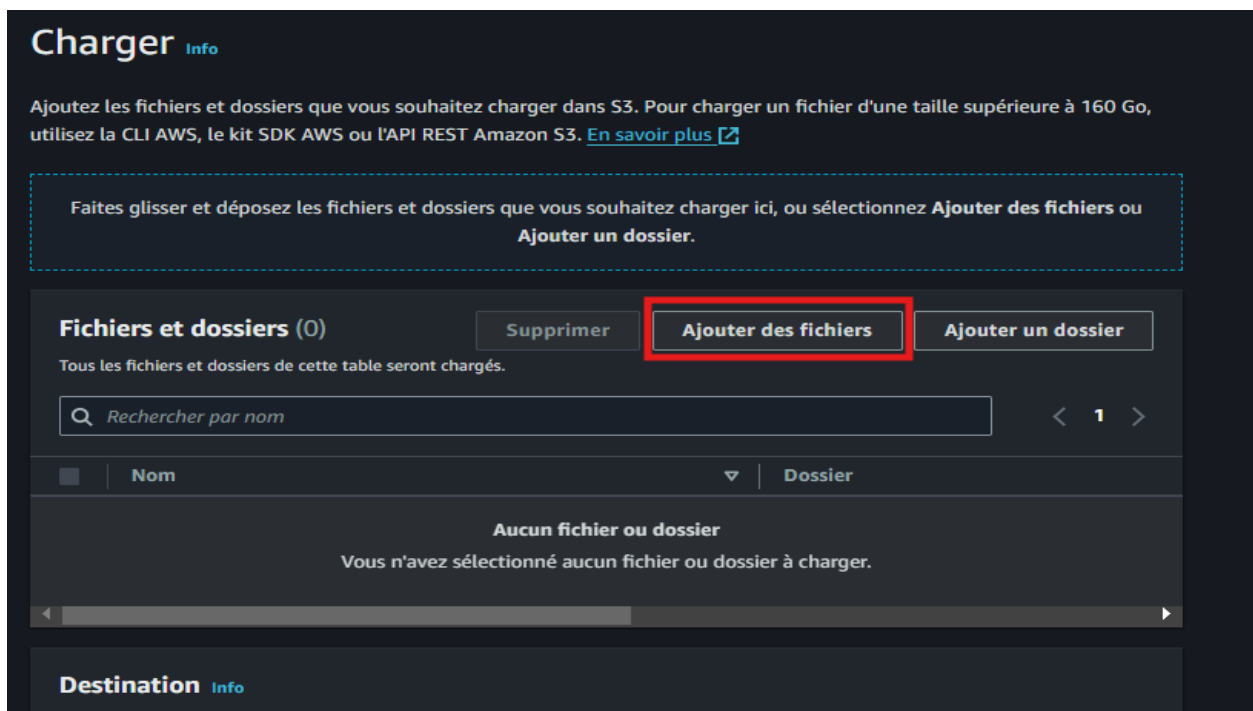
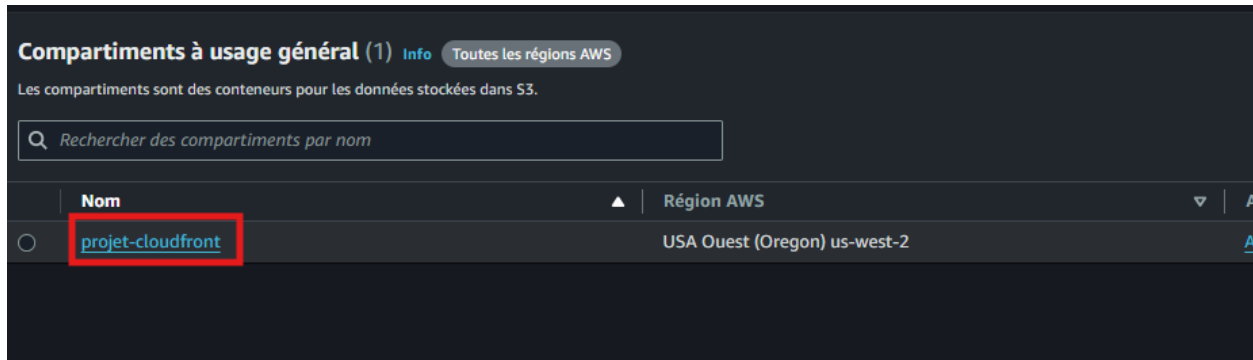
Les compartiments sont des conteneurs pour les données stockées dans S3.

🔍 Rechercher des compartiments par nom

	Nom	▲	Région AWS	▼	A
○	<a href="#">projet-cloudfront</a>		USA Ouest (Oregon)	us-west-2	A

- Téléchargement du contenu :

On se positionne sur le bucket ensuite on clique sur charger pour choisir notre image dans son emplacement.



- Activation de l'accès pour le public :

Nous activons l'accès en lecture pour le public.

Accordez des autorisations en lecture/écriture de base à d'autres comptes AWS. [En savoir plus](#)

**ℹ** AWS recommande d'utiliser des stratégies de compartiment S3 ou des stratégies IAM pour le contrôle d'accès. [En savoir plus](#)

Liste de contrôle d'accès (ACL)

☒ Choisir parmi les listes ACL prédéfinies

☐ Spécifier les autorisations de liste ACL individuelles

Liste des ACL prédéfinies

☐ Privé (recommandé)  
Seul le propriétaire de l'objet aura un accès en lecture et en écriture.

☒ **Accorder l'accès en lecture publique**  
N'importe qui dans le monde pourra accéder aux objets spécifiés. Le propriétaire de l'objet aura un accès en lecture et en écriture. [En savoir plus](#)

**⚠** L'octroi d'un accès en lecture publique n'est pas recommandé  
N'importe qui dans le monde pourra accéder aux objets spécifiés. [En savoir plus](#)

☒ Je comprends le risque d'accorder un accès en lecture publique aux objets spécifiés.

- Lancement du chargement :

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

Annuler **Charger**

ⓘ Les informations ci-dessous ne seront plus disponibles une fois que vous aurez quitté cette page.

### Résumé

Destination s3://projet-cloudfront	Opération réussie 🟢 1 fichier, 3.9 Mo (100.00%)	Échec 🔴 0 fichiers, 0 o (0%)
---------------------------------------	--	---------------------------------

Fichiers et dossiers Configuration

### Fichiers et dossiers (1 Total, 3.9 Mo)

🔍 Rechercher par nom


Nom	Dossier ▾	Type ▾	Taille ▾	Statut ▾	Erreur
imgcloudfro...	-	image/png	3.9 Mo	🟢 Opération réussie	-


## 2. Configuration de cloudfront :


- Sélectionnons le service cloudfront dans la console :


### Services

Voir tous les résultats 59 ▶

 **CloudFront** ☆  
Réseau de diffusion de contenu mondial

 **CloudFormation** ☆  
Création et gestion des ressources à l'aide de modèles

 **Application Composer** ☆  
Concevoir visuellement et créer rapidement des applications modernes

 **AWS End User Messaging** ☆  
Impliquez vos clients sur plusieurs canaux de communication

- Nous allons choisir le point d'origine pour cloudfront.

## Créer une distribution

### Origine

Origin domain

Choose an AWS origin, or enter your origin's domain name.

Origin path - *optional*

Enter a URL path to append to the origin domain name for origin requests.

Nom

Saisissez un nom pour cette origine.

Accès d'origine

**Informations**

☒ **Public**

Bucket must allow public access.

☐ **Origin access control settings (recommended)**

Bucket can restrict access to only CloudFront.

☐ **Legacy access identities**

Use a CloudFront origin access identity (OAI) to access the S3 bucket.

Ajouter un en-tête personnalisé – *facultatif*

- Annuler

Créer une distribution

EH0MS3V9KWICP Afficher les métriques

Questions d'ordre général
Sécurité
Origines
Comportements
Pages d'erreur
Invalidations
Balises

Détails

Nom de domaine de distribution d3lhhffc7zxfoc.cloudfront.net	ARN arn:aws:cloudfront:211125426402:distribution/EH0MS3V9KWICP	Dernière modification 30 août 2024 à 13:08:30 UTC
---	---	--

Paramètres Modifier

### 3. Test :

- Création d'un fichier html :

Nous allons créer un fichier html avec un lien img qui pointe vers le nom de domaine de ma distribution web. Nous allons vérifier est ce que cloudfront délivre l'objet a partir depuis l'origine.

```
<html>
<head>My CloudFront Test</head>
<body>
<p>My text content goes here.</p>
<p>
</body>
</html>
```

Nous enregistrons le fichier sous le nom de mycloudfronttest.html

- Vérification dans un navigateur :

