

LAB AWS — Hébergement sécurisé d'un site web statique avec Amazon S3 et CloudFront

Objectif :

L'objectif de ce projet est de déployer un site web statique dans un environnement sécurisé sur AWS, en utilisant Amazon **S3** pour le stockage et Amazon CloudFront pour la distribution en **HTTPS**. L'accès au contenu du bucket **S3** est restreint à la distribution **CloudFront** via un **Origin Access Identity (OAI)**, conformément aux meilleures pratiques de sécurité cloud.

Services AWS Utilisés

- **Amazon S3** : hébergement du site web statique.
- **Amazon CloudFront** : distribution globale sécurisée du contenu.
- **IAM** : gestion des permissions d'accès via OAI.

Étape 1 – Créer le Bucket S3

1. Va dans **Amazon S3** → clique sur **Créer un compartiment**
2. Donne un nom unique, ex : monbucket-profil25
3. Laisse **toutes les options par défaut**
4. Clique sur **Créer un compartiment**

Amazon S3 > Compartiments > 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
monbucket-profil25

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.

Gestion des versions de compartiment

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour conserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Grâce à la gestion des versions, vous pouvez aisément récupérer en cas d'actions involontaires des utilisateurs et de défaillances des applications. [En savoir plus](#)

Gestion des versions de compartiment

☒ Désactiver

☐ Activer

Chiffrement par défaut [Info](#)

Le chiffrement côté serveur est automatiquement appliqué aux nouveaux objets stockés dans ce compartiment.

Type de chiffrement [Info](#)

☒ Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

☐ Chiffrement côté serveur avec des clés AWS Key Management Service (SSE-KMS)

☐ Chiffrement côté serveur double couche avec des clés AWS Key Management Service (DSSE-KMS)

Sécurisez vos objets avec deux couches de chiffrement distinctes. Pour plus d'informations sur la tarification, consultez Tarification DSSE-KMS dans l'onglet Stockage de la [page tarification Amazon S3](#).

Clé de compartiment

L'utilisation d'une clé de compartiment S3 pour SSE-KMS réduit les coûts de chiffrement en réduisant les appels à AWS KMS. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS. [En savoir plus](#)

☐ Désactiver

☒ Activer

► Paramètres avancés

① 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](#)

✓ Compartiment «monbucket-profil25» créé avec succès

Pour charger des fichiers et dossiers ou configurer des paramètres de compartiment supplémentaires, sélectionnez [Afficher les détails](#).

[Afficher les détails](#)

✕

► 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 (1) [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

< 1 > ⚙️

Nom	Région AWS	Analyseur d'accès IAM	Date de création
<input type="radio"/> monbucket-profil25	USA Ouest (Oregon) us-west-2	Afficher l'analyseur pour us-west-2	12 May 2025 10:23:30 AM WAT

Étape 2 – Activer l'hébergement statique et charger le fichier

1. Allez dans **Amazon S3** → cliquez sur **monbucket-profil25** → **propriétés**
2. Dans la section **Hébergement de site Web statique** cliquez sur **Modifier**
3. En bas d'**Hébergement de site Web statique** cliquez sur **Activer**
4. Dans **Document d'index** entrez **index.html**
5. Laissez le reste des options par défaut
6. Cliquez sur **Enregistrer les modifications**
7. Uploader un fichier `index.html` :
 - Cliquez sur **monbucket-profil25** → **Objets** → **Charger** → **Ajouter des fichiers**
 - Charger le fichier **index.html**
 - Laissez le reste des options par défaut et cliquez sur **Charger**

monbucket-profil25

monbucket-profil25 Info

Objets | Métadonnées | **Propriétés** | Autorisations | Métriques | Gestion | Points d'accès

Présentation des compartiments

Région AWS USA Ouest (Oregon) us-west-2	Amazon Resource Name (ARN) arn:aws:s3::monbucket-profil25	Date de création 12 May 2025 10:23:30 AM WAT
---	---	--

Hébergement de site Web statique Modifier

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](#).

Créer une application Amplify

Hébergement de site Web statique S3
Désactivé

monbucket-profil25 > Modifier l'hébergement de site Web statique

Modifier l'hébergement de site Web statique Info

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

☐ Désactiver
☒ **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 lisible. 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

Annuler

Enregistrer les modifications

monbucket-profil25

🔍 📄 🗨

✔ Hébergement de site Web statique modifié avec succès.

Lorsque cette option est activée, le demandeur paie le coût des demandes et des transferts de données et l'accès anonyme à ce compartiment est désactivé. [En savoir plus](#)

Paie par le demandeur
Désactivé

Hébergement de site Web statique Modifier

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

📘 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 [ici](#)

Créer une application Amplify

Hébergement de site Web statique S3
Activé

Type d'hébergement
Hébergement du compartiment

Point de terminaison de site Web de compartiment
Lorsque vous configurez votre compartiment en tant que site Web statique, le site Web est disponible au point de terminaison de site Web spécifique à la région AWS du compartiment. [En savoir plus](#)
<http://monbucket-profil25.s3-website-us-west-2.amazonaws.com>

monbucket-profil25

🔍 📄 🗨

monbucket-profil25 [Info](#)

Objets

Métadonnées

Propriétés

Autorisations

Métriques

Gestion

Points d'accès

Objets (0)

🔄 Copier l'URI S3

📄 Copier l'URL

⬇ Télécharger

🔗 Ouvrir

🗑 Supprimer

Actions ▼

📁 Créer un dossier

⬆ Charger

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

< 1 > ⚙

Nom

Type

Dernière modification

Taille

Classe de stockage

Aucun objet

Vous n'avez aucun objet dans ce compartiment.

⬆ Charger

monbucket-profil25 > Charger

🔍 📄 🗨

Charger [Info](#)

Ajoutez les fichiers et dossiers que vous souhaitez charger dans S3. Pour charger un fichier d'une taille supérieure à 160 Go, utilisez la CLI AWS, le kit SDK AWS ou l'API REST Amazon S3. [En savoir plus](#)

Faites glisser et déposez les fichiers et dossiers que vous souhaitez charger ici, ou sélectionnez **Ajouter des fichiers** ou **Ajouter un dossier**.

Fichiers et dossiers (0)

Supprimer

Ajouter des fichiers

Ajouter un dossier

Tous les fichiers et dossiers de cette table seront chargés.

🔍 Rechercher par nom

< 1 >

Nom

Dossier

Type

Taille

Aucun fichier ou dossier

Vous n'avez sélectionné aucun fichier ou dossier à charger.

Charger Info

Ajoutez les fichiers et dossiers que vous souhaitez charger dans S3. Pour charger un fichier d'une taille supérieure à 160 Go, utilisez la CLI AWS, le kit SDK AWS ou l'API REST Amazon S3. [En savoir plus](#)

Faites glisser et déposez les fichiers et dossiers que vous souhaitez charger ici, ou sélectionnez **Ajouter des fichiers** ou **Ajouter un dossier**.

Fichiers et dossiers (1 total, 1.1 Ko)

Supprimer

Ajouter des fichiers

Ajouter un dossier

Tous les fichiers et dossiers de cette table seront chargés.

Rechercher par nom

< 1 >

<input type="checkbox"/>	Nom	Dossier	Type	Taille
<input type="checkbox"/>	index.html	-	text/html	1.1 Ko

Destination Info

Destination

s3://monbucket-profil25

► Détails de la destination

Paramètres de compartiment ayant un impact sur les nouveaux objets stockés dans la destination spécifiée.

► 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

Chargement réussi

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

Charger : statut

Fermer

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

Résumé

Destination

s3://monbucket-profil25

Opération réussie

✓ 1 fichier, 1.1 Ko (100.00%)

Échec

✗ 0 fichiers, 0 o (0%)

Fichiers et dossiers

Configuration

Fichiers et dossiers (1 total, 1.1 Ko)

Rechercher par nom

< 1 >

Nom	Dossier	Type	Taille	Statut	Erreur
index.html	-	text/html	1.1 Ko	✓ Opération réussie	-

Étape 3 –Créer une distribution CloudFront

1. Va dans le **service CloudFront**.
2. Clique sur **Créer une distribution CloudFront**.
3. Dans la section **Distribution option** clique sur **Single website or app**
4. Dans la section **Origine** :
 - **Origin domain** : choisis **monbucket-profil25.s3.us-west-2.amazonaws.com**.

- **Accès d'origine** : coche "**Origin access control settings (recommended)**".
5. Dans la section **Origin access control** clique sur **Create new OAI**.
 6. Dans **Create new OAC** :
 - Nom : **monbucket-profil25.s3.us-west-2.amazonaws.com**
 - Comportement de signature : clique sur **Demandes de signature**
 - Laisse les autres paramètres par défaut et clique sur **create**

NB : Un message s'affichera en demandant de mettre à jour la politique du compartiment S3.

7. Dans la section **Comportement du cache par défaut** → **politique de protocole d'utilisateur** sélectionne « **Redirect HTTP to HTTPS** ».
8. Dans la section **Pare-feu d'application Web (WAF)** sélectionne « **Ne pas activer les protections de sécurité** ».
9. Laisse les autres paramètres par défaut et clique sur **Créer une distribution**.

NB : **CloudFront** vous fournira la déclaration de politique après la création de la distribution.

Mise en réseau et diffusion de contenu

Amazon CloudFront

Diffusez du contenu en toute sécurité avec une faible latence et des vitesses de transfert élevées

Amazon CloudFront est un service de réseaux de diffusion de contenu (CDN) rapide qui fournit en toute sécurité des données, des vidéos, des applications et des API aux clients du monde entier avec une faible latence et des vitesses de transfert élevées.

Démarrer avec CloudFront

Activez, en 5 minutes ou moins, la diffusion de contenu accélérée, fiable et sécurisée pour les compartiments Amazon S3, les Application Load Balancers, les API d'Amazon API Gateway et plus encore.

Créer une distribution CloudFront

CloudFront > Distributions > Créer

Créer une distribution

Distribution options Informations
Choose the type of distribution that best fits your needs

☒ **Single website or app**
Choose if you have a single app or website

☐ **Multi-tenant architecture - New**
Choose when you have multiple domains that need to share configurations. This is a common architecture for SaaS providers.

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

monbucket-profil25.s3.us-west-2.amazonaws.com

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

⚠ 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

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

Enter the origin path

Nom

Saisissez un nom pour cette origine.

monbucket-profil25.s3.us-west-2.amazonaws.com

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.

Origin access control

Select an existing origin access control (recommended) or create a new control.

Select an origin access control

Create new OAC

Nom

Saisissez un nom pour cette origine.

monbucket-profil25.s3.us-west-2

Accès d'origine Informations

Public

Bucket must allow public access.

Origin access control settings (r

Bucket can restrict access to only Cl

Legacy access identities

Use a CloudFront origin access ident

Origin access control

Select an existing origin access control (r

Select an origin access control

Ajouter un en-tête personnalisé

CloudFront inclut cet en-tête à toutes les

Ajouter un en-tête

Enable Origin Shield

Origin shield is an additional caching lay

Non

Oui

Nom

Saisissez un nom pour cette origine.

monbucket-profil25.s3.us-west-2.amazonaws.com

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.

Origin access control

Select an existing origin access control (recommended) or create a new control.

monbucket-profil25.s3.us-west-2.amazonaws.com

Create new OAC

Vous devez mettre à jour la politique du compartiment S3

CloudFront vous fournira la déclaration de politique après la création de la distribution.

Comportement du cache par défaut

Modèle de chemin Informations

Par défaut (*)

Compresser automatiquement les objets Informations

No

Yes

Utilisateur

Politique de protocole d'utilisateur

HTTP and HTTPS

Redirect HTTP to HTTPS

HTTPS only

Méthodes HTTP autorisées

GET, HEAD

GET, HEAD, OPTIONS

GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Limiter l'accès aux utilisateurs

Si vous restreignez l'accès des utilisateurs, les utilisateurs doivent utiliser des URL signées CloudFront ou des cookies signés pour accéder à votre contenu.

No

Yes

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

Politique de cache

Choisissez une politique de cache existante ou créez-en une.

CachingOptimized
Recommended for S3

Policy with caching enabled. Supports Gzip and Brotli compression.

[Create cache policy](#)
[Afficher la politique](#)

Politique de demande à l'origine – facultatif

Choisissez une politique de demande d'origine existante ou créez-en une.

Sélectionner la politique d'origine

[Create origin request policy](#)

Pare-feu d'application Web (WAF) Informations

☐ Activer les protections de sécurité

Protégez votre application contre les menaces Web et les vulnérabilités de sécurité les plus courantes à l'aide d'AWS WAF. Les demandes bloquées sont bloquées avant qu'elles n'atteignent vos serveurs Web.

☒ Ne pas activer les protections de sécurité

Sélectionnez cette option si votre application n'a pas besoin de protections de sécurité à partir d'AWS WAF.

Paramètres

Anycast static IP list - optional Informations

Deliver traffic from a small set of IP addresses

There are no Anycast static IP lists available

[Create an Anycast static IP list](#)

There are no Anycast static IP lists available

Catégorie de tarifs Informations

Choisissez la catégorie de tarifs associée au prix maximum que vous souhaitez payer.

☒ Utiliser tous les emplacements périphériques (meilleures performances)
 ☐ Utiliser uniquement l'Amérique du Nord et l'Europe
 ☐ Utiliser l'Amérique du Nord, l'Europe, l'Asie, le Moyen-Orient et l'Afrique

Nom de domaine alternatif (CNAME) – facultatif

Ajoutez les noms de domaine personnalisés que vous utilisez dans les URL pour les fichiers servis par cette distribution.

[Ajouter un élément](#)

☐ Pour ajouter une liste de noms de domaine alternatifs, utilisez le [éditeur en vrac](#).

Standard logging Informations

Additional charges may apply. See info for more details.

Livraison de journaux

Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose

☒ Désactivé
 ☐ Activé

[Annuler](#)
[Créer une distribution](#)

Distributions > E2XSV9DY17YIIZ

Nouvelle distribution créée: To get in-depth monitoring information for your distribution's internet traffic, create an Internet Monitor

E2XSV9DY17YIIZ Standard

[Afficher les métriques](#)

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

Détails

Nom de domaine de distribution
du87058b4wcd.cloudfront.net

ARN
arn:aws:cloudfront::distribution/E2XSV9DY17YIIZ

Dernière modification
Déploiement

Paramètres

Description
Autres noms de domaine

Catégorie de tarifs
Utiliser tous les emplacements périphériques (meilleures performances)

Versions HTTP prises en charge
HTTP/2, HTTP/1.1, HTTP/1.0

Journalisation standard
Off

Cookie logging
Désactivé

Objet racine par défaut
index.html

Continuous deployment Informations

[Create staging distribution](#)

Distributions > E2XSV9DY17YIIZ

La politique du compartiment S3 doit être mise à jour. Complétez la configuration de la distribution en autorisant l'accès en lecture au contrôle d'accès à l'origine CloudFront dans votre déclaration de politique. Accédez aux autorisations du compartiment S3 pour mettre à jour la politique

E2XSV9DY17YIIZ Standard

[Afficher les métriques](#)

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

Détails

Nom de domaine de distribution
du87058b4wcd.cloudfront.net

ARN
arn:aws:cloudfront::distribution/E2XSV9DY17YIIZ

Dernière modification
Déploiement

Paramètres

Description
Autres noms de domaine

Catégorie de tarifs
Utiliser tous les emplacements périphériques (meilleures performances)

Versions HTTP prises en charge
HTTP/2, HTTP/1.1, HTTP/1.0

Journalisation standard
Off

Cookie logging
Désactivé

Objet racine par défaut
index.html

NB : Copier la déclaration de politique du compartiment S3 fournit par CloudFront après la création de la distribution en cliquant sur « **Politique de copie** ». La politique ressemblera à ceci :

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::monbucket-profil25/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::ton-id-compte:distribution/id-distribution"
        }
      }
    }
  ]
}
```

Étape 4 – Configurer la bucket policy pour permettre l'accès uniquement via CloudFront (en liant l'OAI)

1. Va dans compartiment S3
2. Clique sur ton compartiment **monbucket-profil25**
3. Dans la section **Autorisations** → **Stratégie de compartiment** clique sur **Modifier**
4. Coller la **stratégie** et clique sur **Enregistrer les modifications**

[Compartiments](#) > monbucket-profil25

monbucket-profil25 Info

Objets | Métadonnées | Propriétés | **Autorisations** | Métriques | Gestion | Points d'accès

Présentation des autorisations

Résultats d'accès
Les résultats d'accès sont fournis par des analyseurs d'accès externes IAM. En savoir plus sur le [fonctionnement des résultats de l'analyseur IAM](#)

[Afficher l'analyseur pour us-west-2](#)

Stratégie de compartiment

La stratégie de compartiment, écrite au format JSON, permet d'accéder aux objets stockés dans le compartiment. Les stratégies de compartiment ne s'appliquent pas aux objets appartenant à d'autres comptes. [En savoir plus](#)

L'accès public est bloqué, car les paramètres bloquer l'accès public sont activés pour ce compartiment
Pour déterminer les paramètres activés, vérifiez vos paramètres de blocage de l'accès public pour ce compartiment. En savoir plus sur [l'utilisation d'Amazon S3 Block Public Access](#)

Aucune stratégie à afficher.

[Copier](#)

[monbucket-profil25](#) > Modifier la stratégie de compartiment

Modifier la stratégie de compartiment Info

Stratégie de compartiment

Exemples de stratégies [Exemples de stratégies](#) [Générateur de stratégies](#)

La stratégie de compartiment, écrite au format JSON, permet d'accéder aux objets stockés dans le compartiment. Les stratégies de compartiment ne s'appliquent pas aux objets appartenant à d'autres comptes. [En savoir plus](#)

ARN du compartiment
[arn:aws:s3::monbucket-profil25](#)

Stratégie

```
1 {
2   "Version": "2008-10-17",
3   "Id": "PolicyForCloudFrontPrivateContent",
4   "Statement": [
5     {
6       "Sid": "AllowCloudFrontServicePrincipal",
7       "Effect": "Allow",
8       "Principal": {
9         "Service": "cloudfront.amazonaws.com"
10      },
11      "Action": "s3:GetObject",
12      "Resource": "arn:aws:s3::monbucket-profil25/*",
13      "Condition": {
14        "StringEquals": {
15          "AWS:SourceArn": "arn:aws:cloudfront::[redacted]:distribution/E2XSV9DY17YIIZ"
16        }
17      }
18    }
19  ]
20 }
```

Modifier l'instruction

Sélectionner une instruction

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

[+ Ajouter une nouvelle instruction](#)

[Suggestions: 0](#)

[Aperçu de l'accès externe](#)

[Annuler](#) [Enregistrer les modifications](#)

monbucket-profil25

Stratégie de compartiment modifiée avec succès.

Stratégie de compartiment

La stratégie de compartiment, écrite au format JSON, permet d'accéder aux objets stockés dans le compartiment. Les stratégies de compartiment ne s'appliquent pas aux objets appartenant à d'autres comptes. [En savoir plus](#)

L'accès public est bloqué, car les paramètres bloquer l'accès public sont activés pour ce compartiment
Pour déterminer les paramètres activés, vérifiez vos paramètres de blocage de l'accès public pour ce compartiment. En savoir plus sur [l'utilisation d'Amazon S3 Block Public Access](#)

```
{
  "Version": "2008-10-17",
  "Id": "PolicyForCloudFrontPrivateContent",
  "Statement": [
    {
      "Sid": "AllowCloudFrontServicePrincipal",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudfront.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::monbucket-profil25/*",
      "Condition": {
        "StringEquals": {
          "AWS:SourceArn": "arn:aws:cloudfront::[redacted]:distribution/E2XSV9DY17YIIZ"
        }
      }
    }
  ]
}
```

[Copier](#)

Étape 5 – Tester

1. Va dans la console **CloudFront**.
2. Copie le **domaine CloudFront** généré, ex : du87058bs4wcd.cloudfront.net
3. Ouvre ce lien dans un navigateur :
4. Tu devrais voir le contenu de ton **index.html** et l'URL sera automatiquement en **HTTPS**.

The screenshot displays the AWS CloudFront console interface. The top navigation bar shows the distribution name 'E2XSV9DY17YIIZ' and a 'Standard' cache profile. The 'Origines' tab is active, showing a table with one origin: 'monbucket-profil25.s3.us-west-2.amazonaws.com'. Below this, the 'Groupes d'origines' section is empty. The 'Détails' tab is also shown, with the 'Nom de domaine de distribution' field circled in red, displaying 'du87058bs4wcd.cloudfront.net'. The 'Paramètres' section shows various settings like 'Description', 'Catégorie de tarifs', and 'Journalisation standard'. At the bottom, a browser window shows the URL 'https://du87058bs4wcd.cloudfront.net/' and a profile card for France Stanislas Bantantoula, an AWS & OCI Certified IT Support & System | Cloud & DevOps Enthusiast.