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

Objectif:

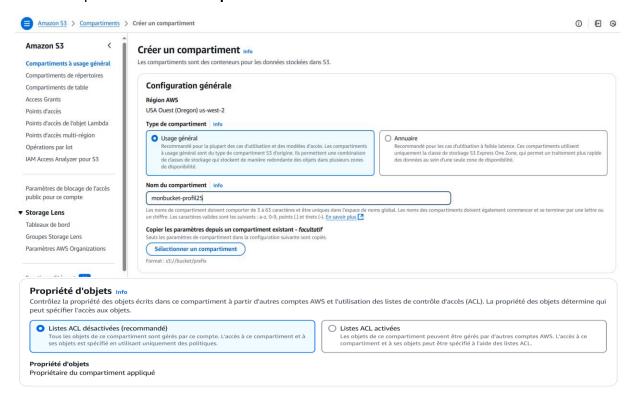
L'objectif de ce projet est de déployer un site web statique dans un environnement sécurisé sur AWS, en utilisant Amazon S3 pour le stockage et Amazon CloudFront pour la distribution en HTTPS. L'accès au contenu du bucket S3 est restreint à la distribution CloudFront via un Origin Access Identity (OAI),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



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 [2] ✓ 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 obiets, accordé via de nouvelles listes de contrôle d'accès (ACL) s ACL d'accès public pour les compartiments et objets e Bloquer l'accès public aux compartiments et aux objets, accordé via n'importe quelles listes de contrôle d'accès (ACL) Bloquer l'accès public aux compartiments et aux objets, accordé via de nouvelles stratégies de compartiment ou de point d'accès public Bloquer l'accès public et entre comptes aux compartiments et objets via n'importe quelles stratégies de compartiment ou de point d'accès public 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 [2] 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. O Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) Chiffrement côté serveur avec des clés AWS Key Management Service (SSE-KMS) O Chiffrement côté serveur double couche avec des clés AWS Key Management Service (DSSE-KMS) Securisez vos objets av ations sur la tarification, consultez **Tarification DSSE-KMS** dans l'onglet **Stockage** de la <u>page tarification Amazon</u> Clé de compartiment L'utilisation d'u savoir plus ine 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 Désactive 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. Créer un compartiment Afficher les détails **⊘** Compartiment «monbucket-profil25 » créé avec succès Pour charger des fichiers et dossiers ou configurer des paramètres de compartiment supplémentaires, sélectionnez Afficher les détails ▶ Apercu 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 C (C) (Copier l'ARN) Vider Supprimer Créer un compartiment Les compartiments sont des conteneurs pour les données stockées dans S3. Q Rechercher des compartiments par nom 〈 1 〉 戀 Nom ▲ Région AWS ▼ Analyseur d'accès IAM Date de création

USA Ouest (Oregon) us-west-2

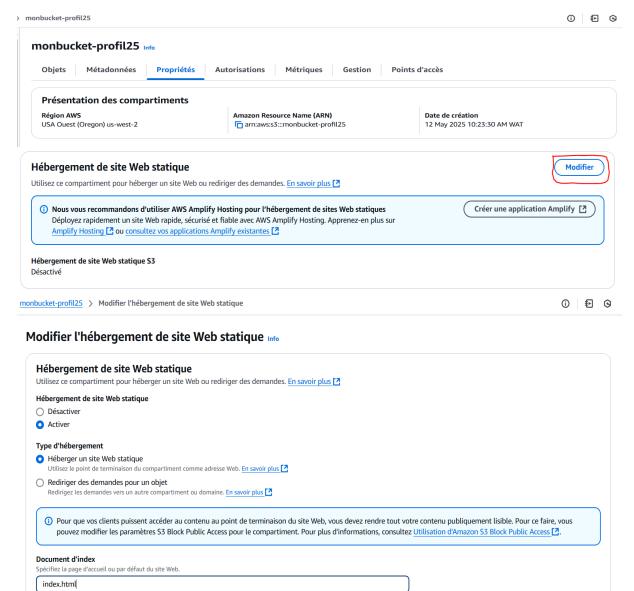
Afficher l'analyseur pour us-west-2

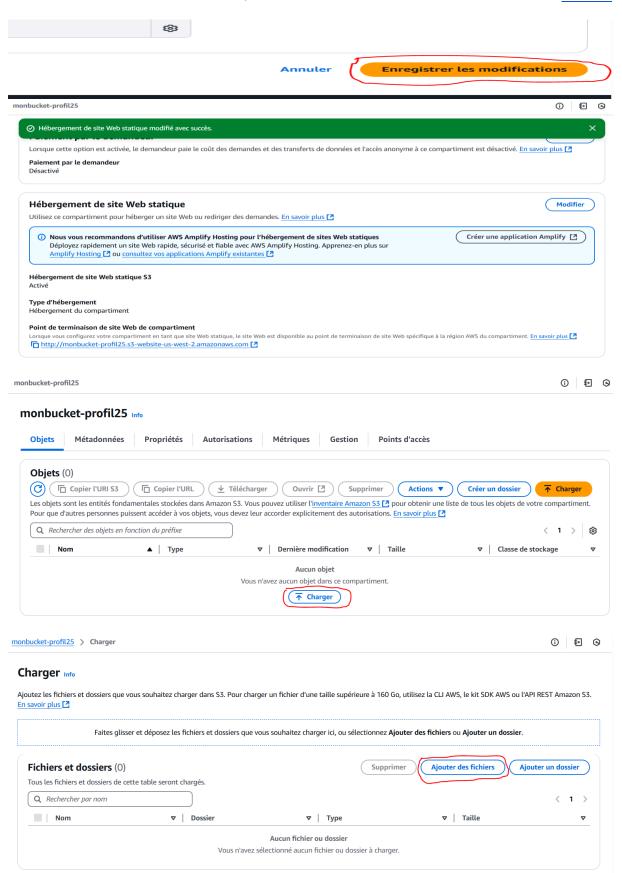
monbucket-profil25

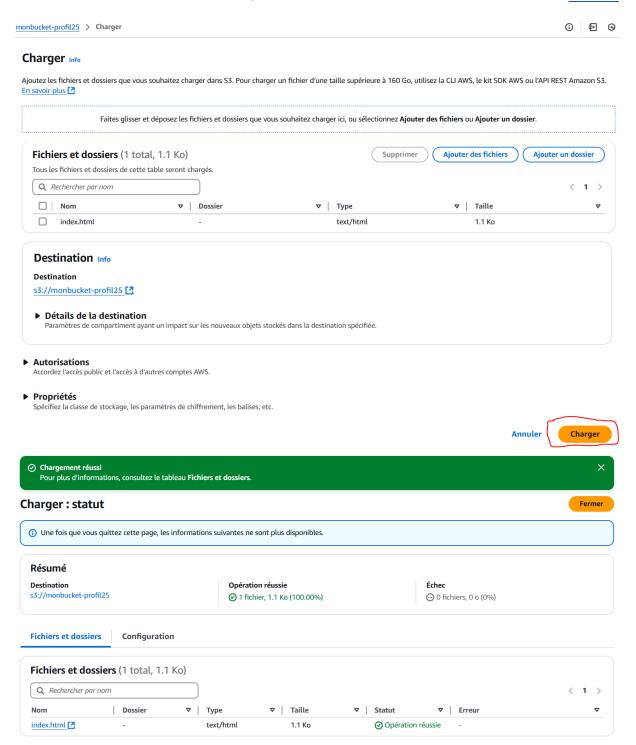
12 May 2025 10:23:30 AM WAT

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

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







Étape 3 - Créer une distribution CloudFront

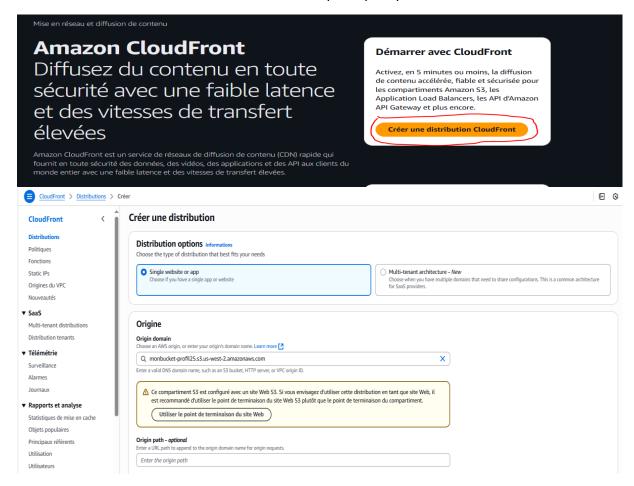
- 1. Va dans le service CloudFront.
- 2. Clique sur Créer une distribution CloudFront.
- 3. Dans la section Distribution option clique sur Single website or app
- 4. Dans la section Origine :
 - Origin domain: choisis monbucket-profil25.s3.us-west-2.amazonaws.com.

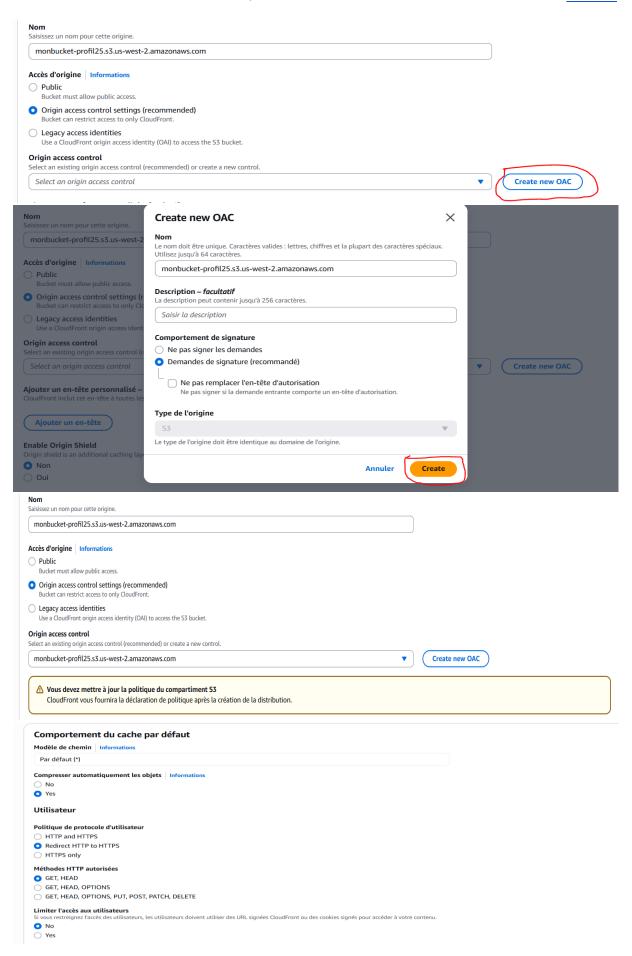
- o Accès d'origine : coche "Origin access control settings (recommended)".
- 5. Dans la section Origin access control clique sur Create new OAI.
- 6. Dans Create new OAC:
 - o Nom: monbucket-profil25.s3.us-west-2.amazonaws.com
 - o Comportement de signature : clique sur Demandes de signature
 - Laisse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

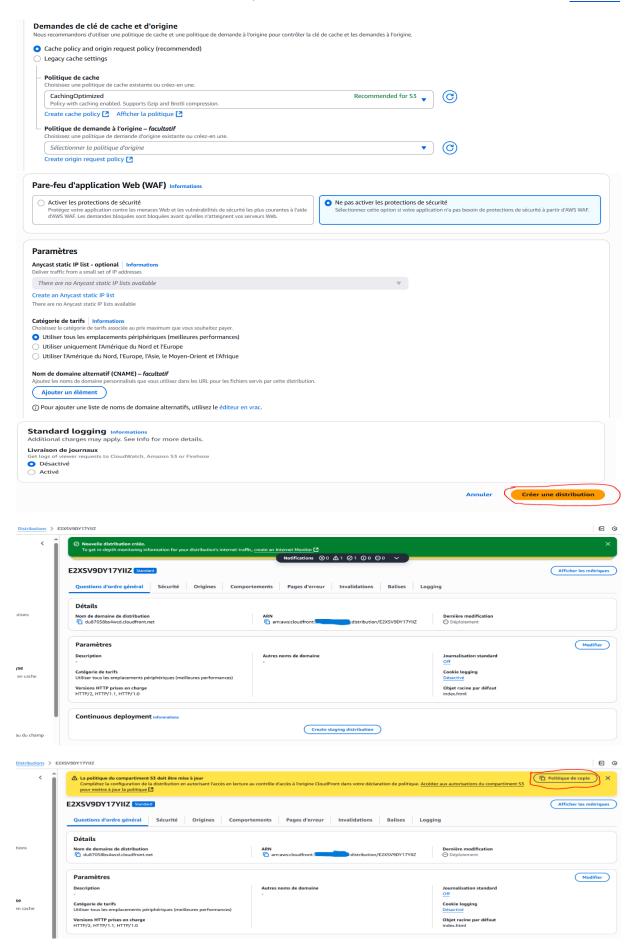
NB: Un message s'affichera en demandant de mettre à jour la politique du compartiment S3.

- 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.





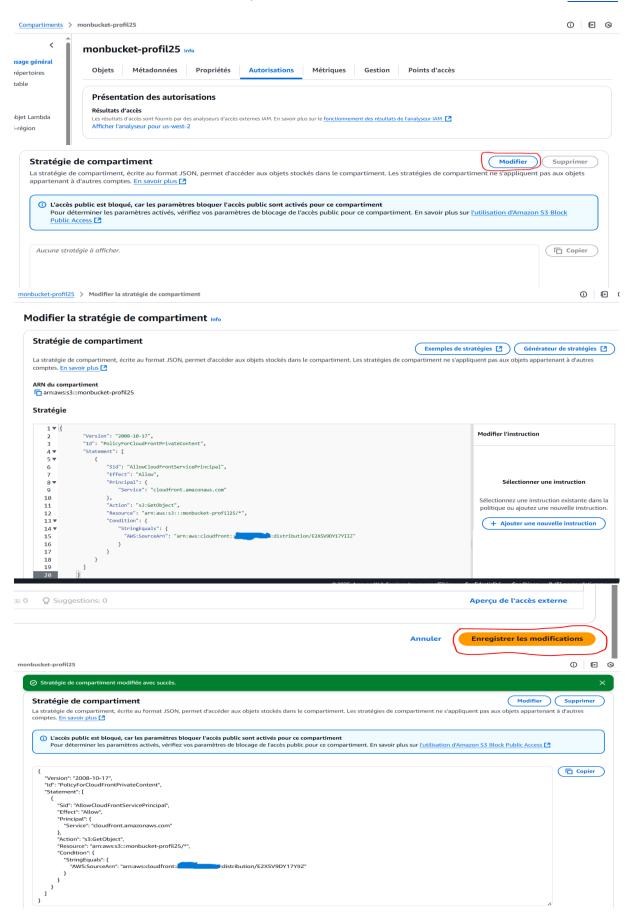


NB: Copier la déclaration de politique du compartiment S3 fournit par CloudFront après la création de la distribution en cliquant sur « **Politique de copie** ». La politique ressemblera à ceci :

```
"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



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.

