

Héberger un Site Web avec AWS

Simplifiez votre Déploiement dans le Cloud



Encadré par : Dr.Routaib Hayat

Réalisé par : Afkir Nada && Kalach Siham

**Gestion d' une
quantité pratiquement
illimitée de données et
des millions de
requêtes par seconde**

**La disponibilité de 99,99 % et la
durabilité de 99,999999999 % (11
nines)**

Pourquoi, On a ? choisit AWS s3

**Coût adapté à l'utilisation,
Dans notre cas on a rien payé**

Sécurité avancée:

1. Cryptage
2. bucket policies, ACLs
3. Public Access Block
4. IAM

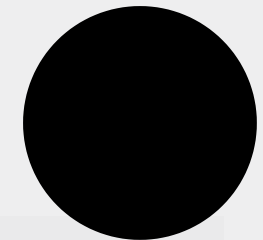
Création et Organisation du Site Web

La création de ce site pour le restaurant Salpicon qui reflète l'identité du restaurant tout en offrant une expérience utilisateur optimale.

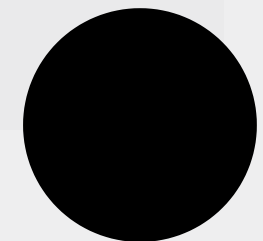


Sections du Site Web

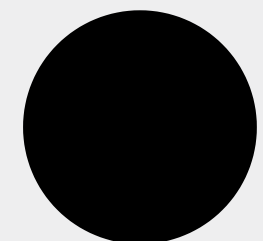
Ce site statique comporte plusieurs sections principales :



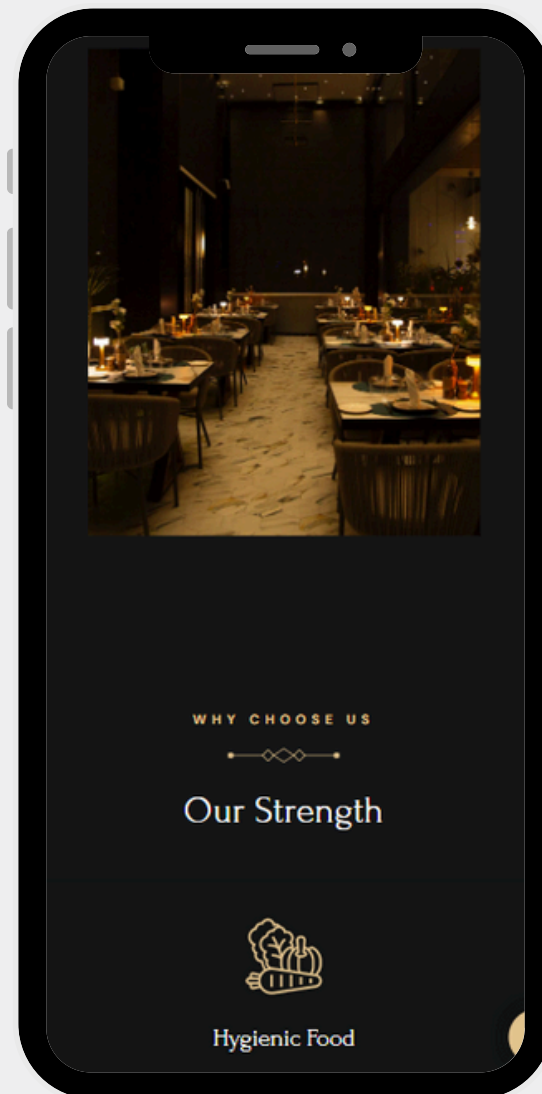
Home



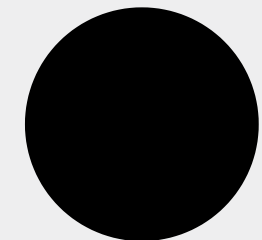
Menus



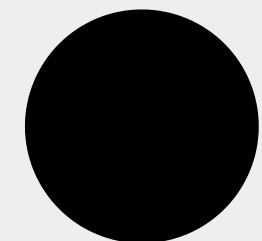
About Us



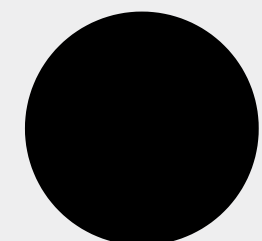
Gallery



Services



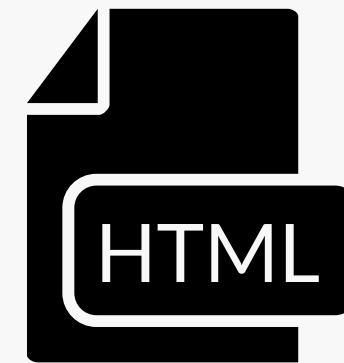
Contact



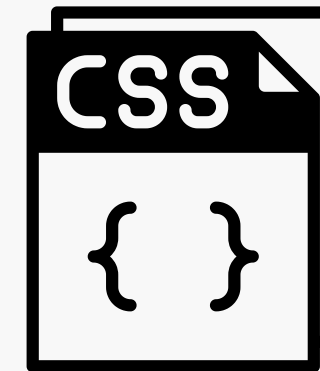
Technologies Utilisées

Pour la création du site web du restaurant Salpicon, les technologies suivantes ont été utilisées :

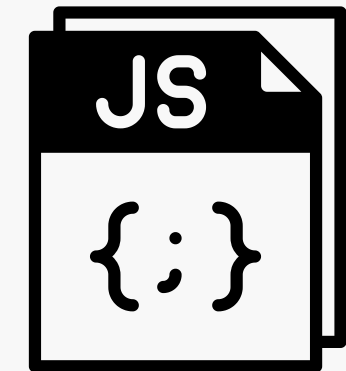
HTML



CSS

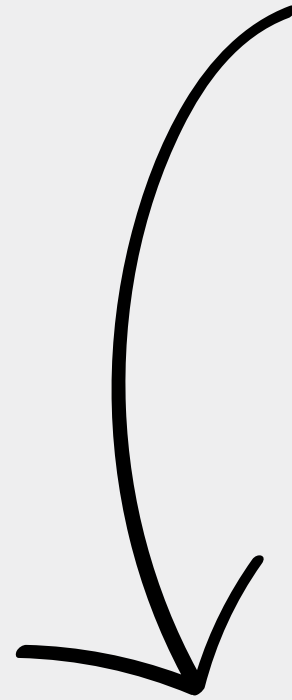








JS







Arborescence du Projet

Le projet est organisé selon
l'arborescence suivante :



Name	Type
 assets	File folder
 favicon	Microsoft Edge HTML Docum...
 index	Chrome HTML Document
 index	Fichier source Text
 script	Fichier source JavaScript
 style-guide	Fichier source Markdown

Name	Type
 css	File folder
 images	File folder
 js	File folder
 menu	File folder

Utilisation de **S3** pour Héberger un Site Web

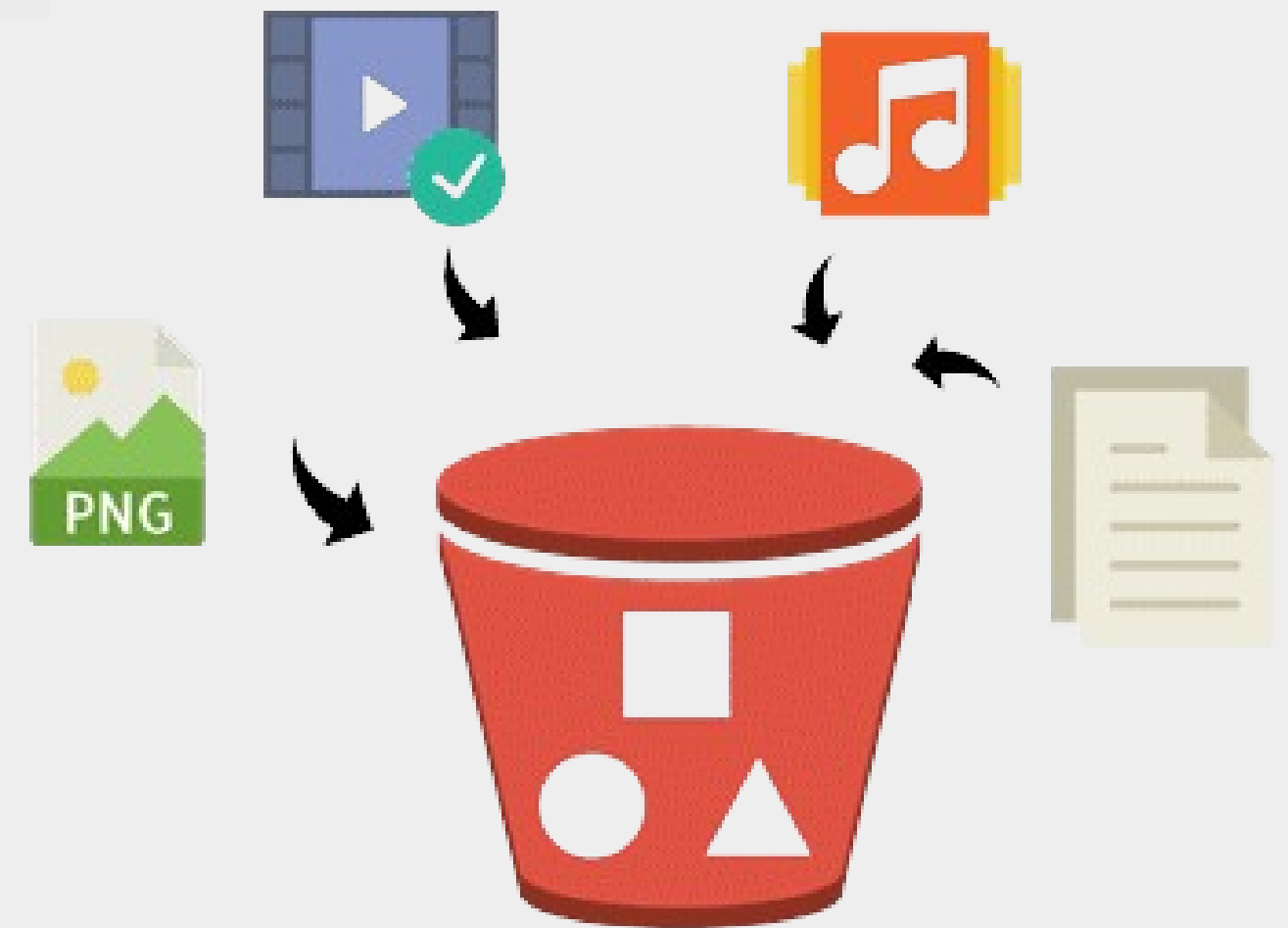


Qu'est-ce que S3 ?

Amazon S3 (Simple Storage Service) est un service de stockage en ligne proposé par Amazon Web Services (AWS).

Il permet de stocker et de récupérer n'importe quelle quantité de données, à tout moment, à partir de n'importe où sur le web. S3 est largement utilisé pour héberger des fichiers statiques tels que des images, des vidéos, des documents, et des sites web statiques, grâce à sa fiabilité, sa sécurité, et son évolutivité.

Avec S3, vous pouvez créer un "bucket" (seau) où vous pouvez stocker tous les fichiers de votre site web. Ces fichiers peuvent ensuite être accessibles via une URL publique, ce qui en fait un moyen idéal pour héberger un site web statique.

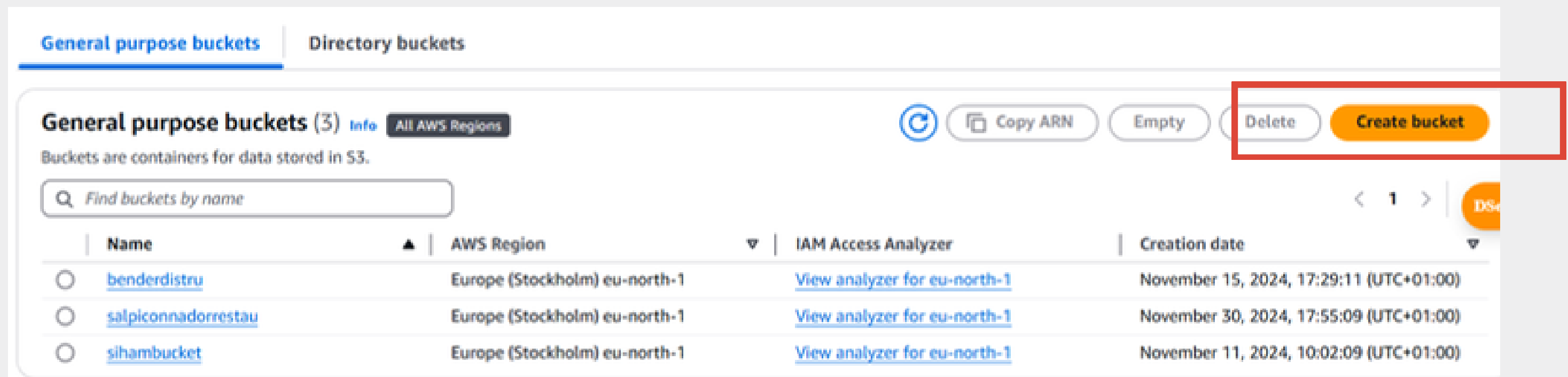
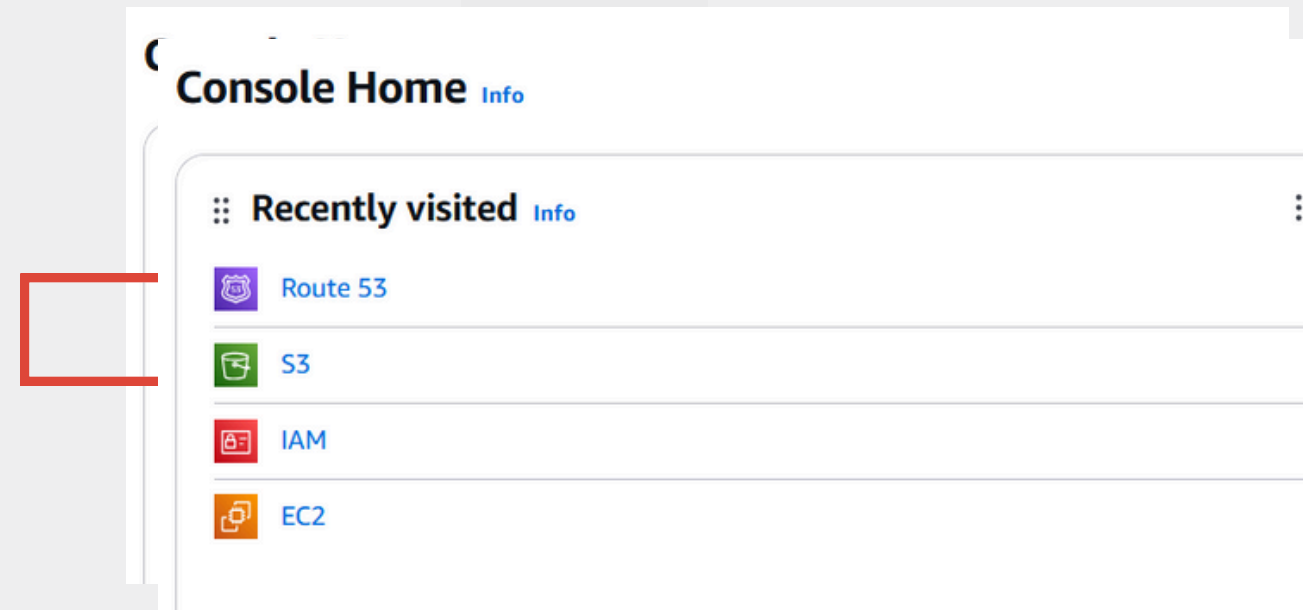


Comment Héberger un Site Web avec Amazon S3 ?!



Créer un Bucket S3

- Connectez-vous à la console AWS
- Allez dans Services > S3
- Cliquez sur Créer Compartiment pour créer un nouveau compartiment.



Créer un Bucket S3

Configuration de Base (General Configuration)

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type [Info](#)

☒ **General purpose**
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

☐ **Directory**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

myawsbucket

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

Q1



Nom du Bucket

- Doit être unique à l'échelle mondiale.
- Utiliser uniquement des lettres minuscules, chiffres, et des tirets (-). Pas d'espaces ni de majuscules.

Q2



Choisir le Type de Bucket

- Usage général : Convient à la plupart des cas d'utilisation, avec un stockage redondant sur plusieurs zones de disponibilité.
- Répertoire : Utilisé pour les cas nécessitant une faible latence. Ce type utilise la classe de stockage S3 Express One Zone.

Q3



Copier les Paramètres d'un Bucket Existant (Optionnel)

- Cliquez sur Choisir un bucket pour sélectionner un bucket existant si vous souhaitez copier ses paramètres.
- Cela peut inclure des configurations telles que les permissions, le chiffrement, etc.

Créer un Bucket S3

Configurer les Paramètres d'Accessibilité

Propriété des Objets

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced



ACLs désactivées (recommandé)

- Tous les objets dans le bucket sont considérés comme appartenant au propriétaire du bucket.
- Les permissions d'accès au bucket et à ses objets sont uniquement définies par des politiques (policies).

ACLs activées

- Permet d'utiliser des ACLs pour définir les permissions directement sur des objets individuels.
- Les objets peuvent être possédés par d'autres comptes AWS en utilisant des ACLs personnalisées.

Créer un Bucket S3

Configurer les Paramètres d'Accessibilité

Propriété des Objets

Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Cas d'utilisation



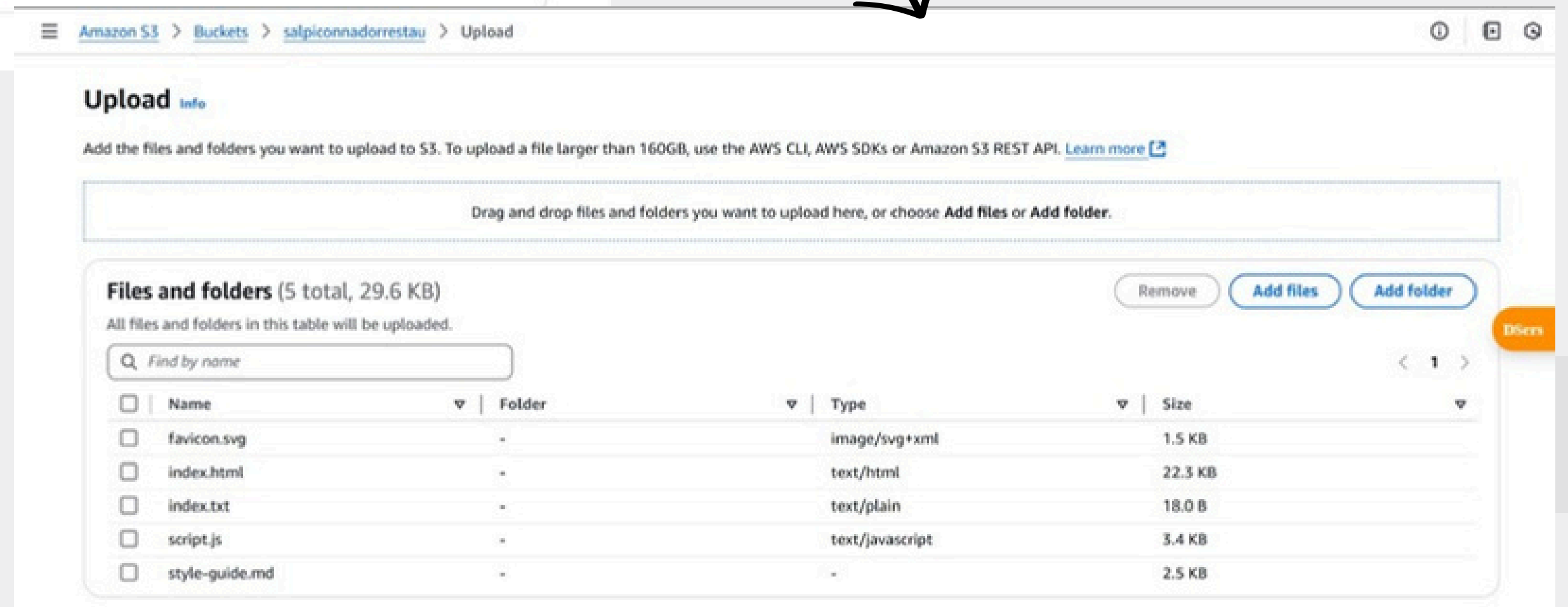
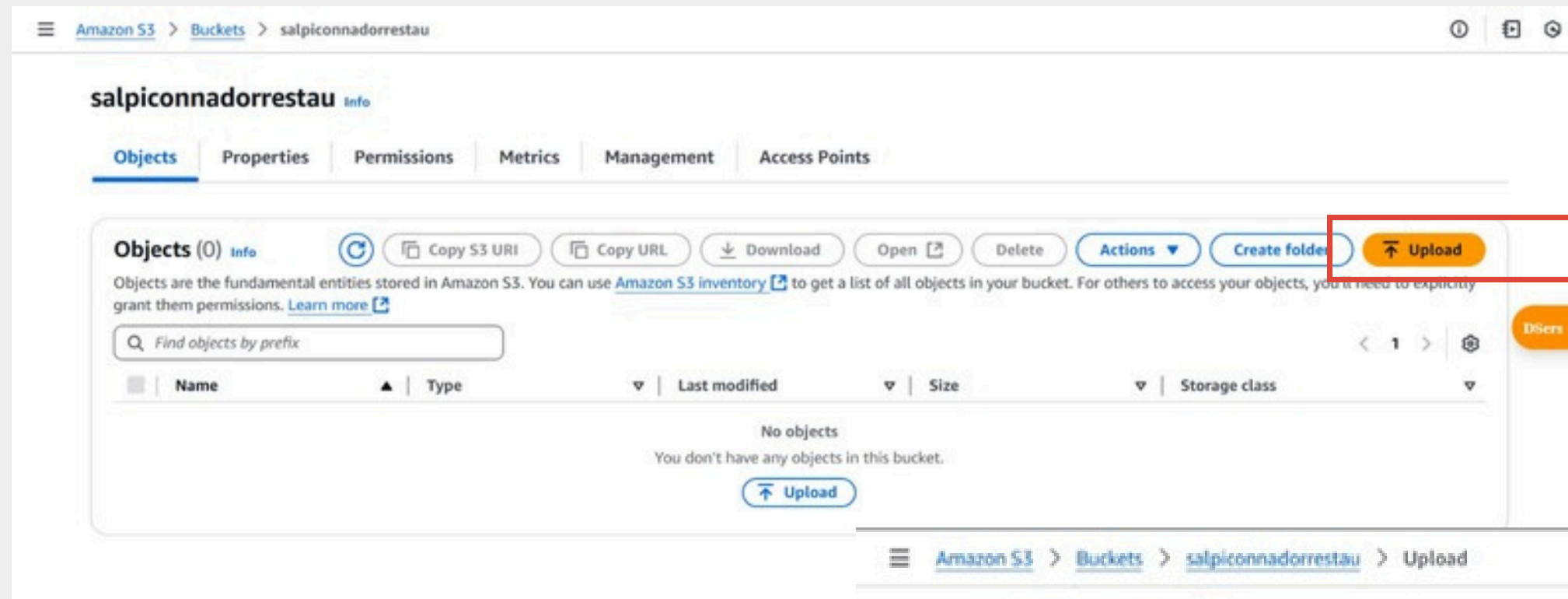
ACLs désactivées (recommandé)

Idéal pour la plupart des scénarios, sauf si vous avez des exigences spécifiques pour attribuer différentes permissions à différents objets ou utilisateurs.

ACLs activées

Utile lorsque plusieurs entités ou comptes AWS doivent gérer des permissions spécifiques pour des objets.

Téléverser les fichiers



Activer 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](#)

❗ Pour que vos clients puissent accéder au contenu au point de terminaison du site Web, vous devez renvoyer les demandes vers le point de terminaison du site Web. Vous pouvez modifier les paramètres S3 Block Public Access pour le compartiment. Pour plus d'informations, consultez [la documentation](#).

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

Hébergement de site Web statique

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](#).

[Créer une application](#)

Hébergement de site Web statique S3

Activé

Type d'hébergement

Hébergement du compartiment

Point de terminaison de site Web de compartiment

Quand 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.

<http://salpiconnadorrestau.s3-website.eu-north-1.amazonaws.com>

Comment Gérer les Politiques d'un static website sur AWS ?

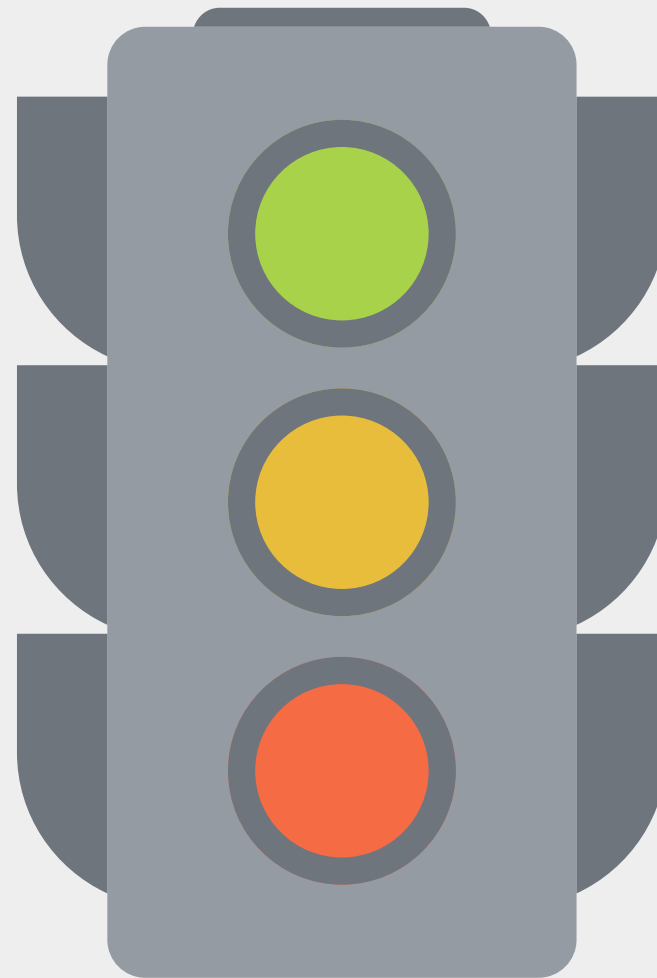


Quels sont ces politiques sur AWS ?

Public Access

ACL Control Lists

Bucket Policy



Public Access, Comment faire ?



Public Access

Bloquer l'accès public (paramètres de compartiment)

Modifier

L'accès public aux compartiments et objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, des stratégies de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à tous vos compartiments et objets S3, activez « Bloquer tous les accès publics ». Ces paramètres s'appliquent uniquement à ce compartiment et ses points d'accès. AWS recommande d'activer « Bloquer tous les accès publics ». Toutefois, avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos cas d'utilisation de stockage spécifiques. [En savoir plus](#)

Bloquer tous les accès publics

⚠ Désactivé

► Paramètres de blocage individuel de l'accès public pour ce compartiment

Normalement On trouve l'option Bloquer tous les accès publics est coché par défaut . Puisque ce n'est pas notre but on le modifie en désactivant cette option comme remarquez

Bloquer l'accès public (paramètres de compartiment)

L'accès public aux compartiments et objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, des stratégies de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à tous vos compartiments et objets S3, activez « Bloquer tous les accès publics ». Ces paramètres s'appliquent uniquement à ce compartiment et ses points d'accès. AWS recommande d'activer « Bloquer tous les accès publics ». Toutefois, avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos cas d'utilisation de stockage spécifiques. [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. 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 accordent 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.

Comment Gérer les ACLs sur un bucket ou un objet ?



Comment Gérer les ACLs sur un bucket?

Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

This bucket has the bucket owner enforced setting applied for Object Ownership
When [bucket owner enforced](#) is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) <small>Canonical ID:</small> 7400bc9b70c598949e3e17415c4fa4de95db8a601ef10c5d6390520be7965557	List, Write	Read, Write
Everyone (public access) <small>Group:</small> http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) <small>Group:</small> http://acs.amazonaws.com/groups/global/AuthenticatedUsers		
S3 log delivery group <small>Group:</small> http://acs.amazonaws.com/groups/s3/LogDelivery		

- Accédez à l'onglet Permissions du bucket.
- Trouvez la section Access Control List.

- Configurez les autorisations pour :
 - a. **Bucket owner** : Le propriétaire du bucket.
 - b. **Other AWS accounts** : Comptes AWS spécifiques.
 - c. **Public access** : Pour rendre le bucket public.

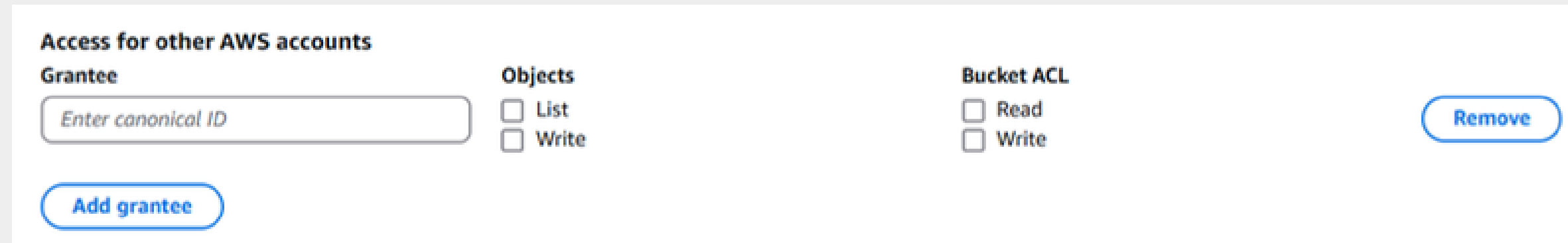
Access control list (ACL)
Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) <small>Canonical ID:</small> 7400bc9b70c598949e3e17415c4fa4de95db8a601ef10c5d6390520be7965557	<input checked="" type="checkbox"/> List <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) <small>Group:</small> http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account) <small>Group:</small> http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> List <input type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input type="checkbox"/> Write
S3 log delivery group <small>Group:</small> http://acs.amazonaws.com/groups/s3/LogDelivery	<input type="checkbox"/> List <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access the objects in this bucket.
[Learn more](#)

☒ I understand the effects of these changes on my objects and buckets.

Gérer les ACLs sur un bucket



Access for other AWS accounts

Grantee

Objects

☐ List

☐ Write

Bucket ACL

☐ Read

☐ Write

ETAPE : 1



Identifier les grantees

Identifiez un utilisateur ou un compte AWS via son Canonical User ID ou son AWS account ID.

ETAPE : 2



Attribuer des autorisations :

1. **Lecture (Read)** : Autorise l'utilisateur à lire les objets ou la liste des objets dans un bucket.
2. **Écriture (Write)** : Autorise l'utilisateur à ajouter, remplacer ou supprimer des objets dans un bucket.
3. **Lire les permissions ACL (Read ACL)** : Autorise l'utilisateur à lire les permissions existantes.
4. **Écrire les permissions ACL (Write ACL)** : Autorise l'utilisateur à modifier les ACLs.

Comment Gérer **Bucket policy** ?



Type: Fichier JSON

Définir les permissions appliquées à un bucket Amazon S3 et à ses objets

Bucket Policies

Gérer et contrôler l'accès à un bucket et aux fichiers qu'il contient

Bucket Policies

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies

Bucket ARN

 arn:aws:s3::salpiconnadorrestau

Policy

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

1. **Version** : La version de la syntaxe utilisée (souvent "2012-10-17").
2. **Statement** : Liste des règles ou déclarations.
3. **Effect** : "Allow" (autoriser) ou "Deny" (refuser).
4. **Principal** : Qui est concerné (utilisateurs, rôles, ou "*", qui signifie tout le monde).
5. **Action** : Actions AWS permises (par exemple, s3:GetObject pour lire un fichier).
6. **Resource** : Ressource affectée (par exemple, le bucket spécifique ou des fichiers spécifiques).
7. **Condition** : **(+)** **(Optionnel)** Règles conditionnelles supplémentaires.

Utilisation de **Route 53** pour Créer un Nom de Domaine



Amazon Route 53

Qu'est-ce que Route 53 ?

Amazon Route 53 est un service de gestion des noms de domaine (DNS) proposé par AWS.

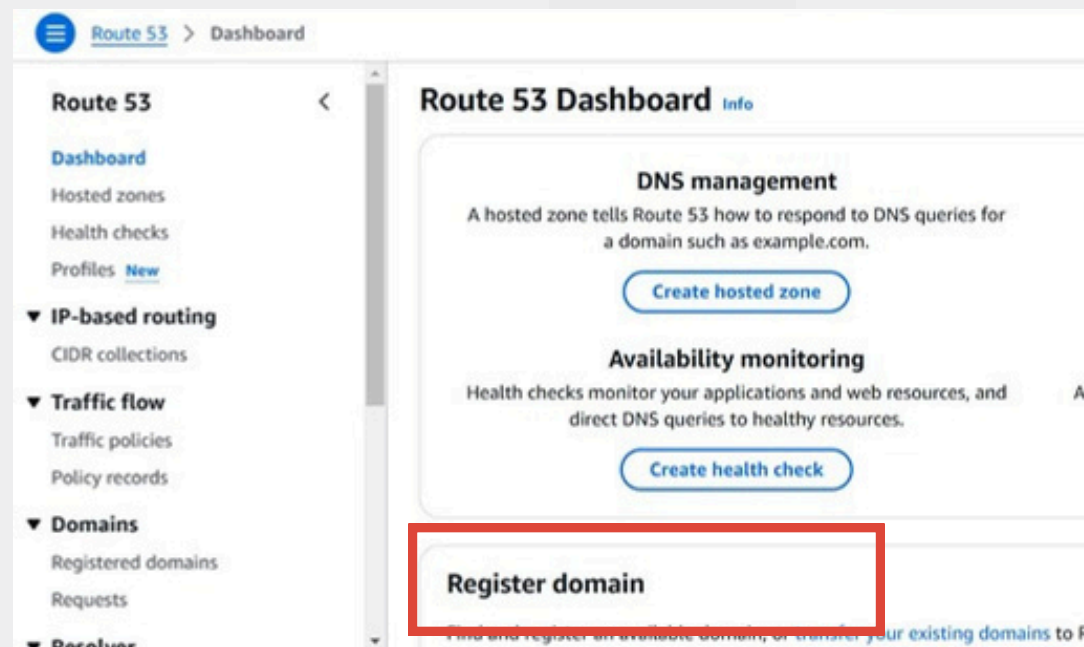
Il permet de gérer les noms de domaine et de diriger le trafic Internet vers vos ressources, comme des serveurs Web, des serveurs d'applications, ou des sites Web hébergés sur Amazon S3. Si vous souhaitez utiliser un nom de domaine personnalisé pour votre site Web hébergé sur S3, Route 53 est l'outil idéal pour configurer les enregistrements DNS.



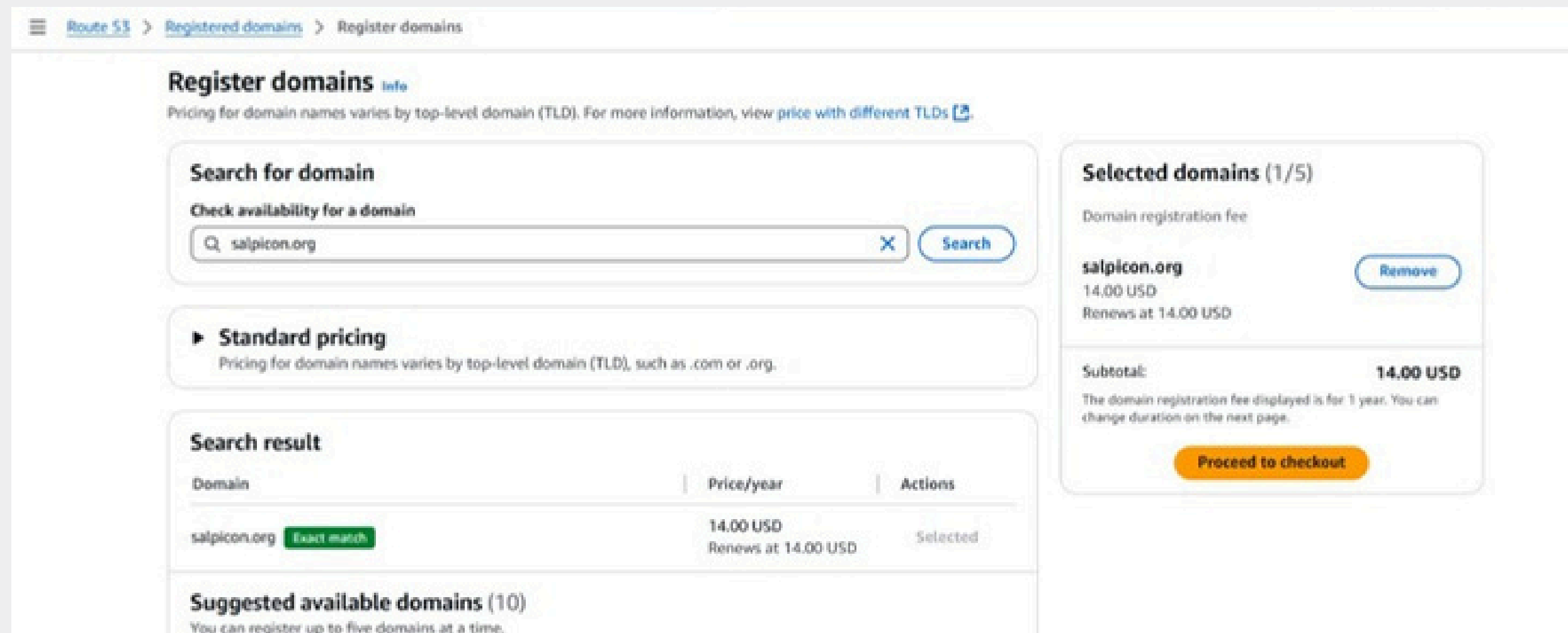
Étapes pour Créer un Nom de Domaine avec Route 53 et le Connecter à un Bucket S3

1. **Créer un Nom de Domaine avec Route 53**
2. **Créer une Zone Hébergée dans Route 53**
3. **Ajouter des Enregistrements DNS dans Route 53**
4. **Redirection vers Domaine Principal**

Créer un Nom de Domaine avec Route 53



- Cliquez sur Enregistrer un domaine.
- Vérifiez si votre domaine est disponible, puis ajoutez-le à votre panier.
- Entrez vos informations personnelles et acceptez les termes et conditions.



Créer une Zone Hébergée dans Route 53

Create hosted zone [Info](#)

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name [Info](#)

This is the name of the domain that you want to route traffic for.

Valid characters: a-z, 0-9, ! * # \$ % & ' () * + , - / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)

This value lets you distinguish hosted zones that have the same name.

The description can have up to 256 characters. 0/256

Type [Info](#)

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☒ **Public hosted zone**

A public hosted zone determines how traffic is routed on the internet.

☐ **Private hosted zone**

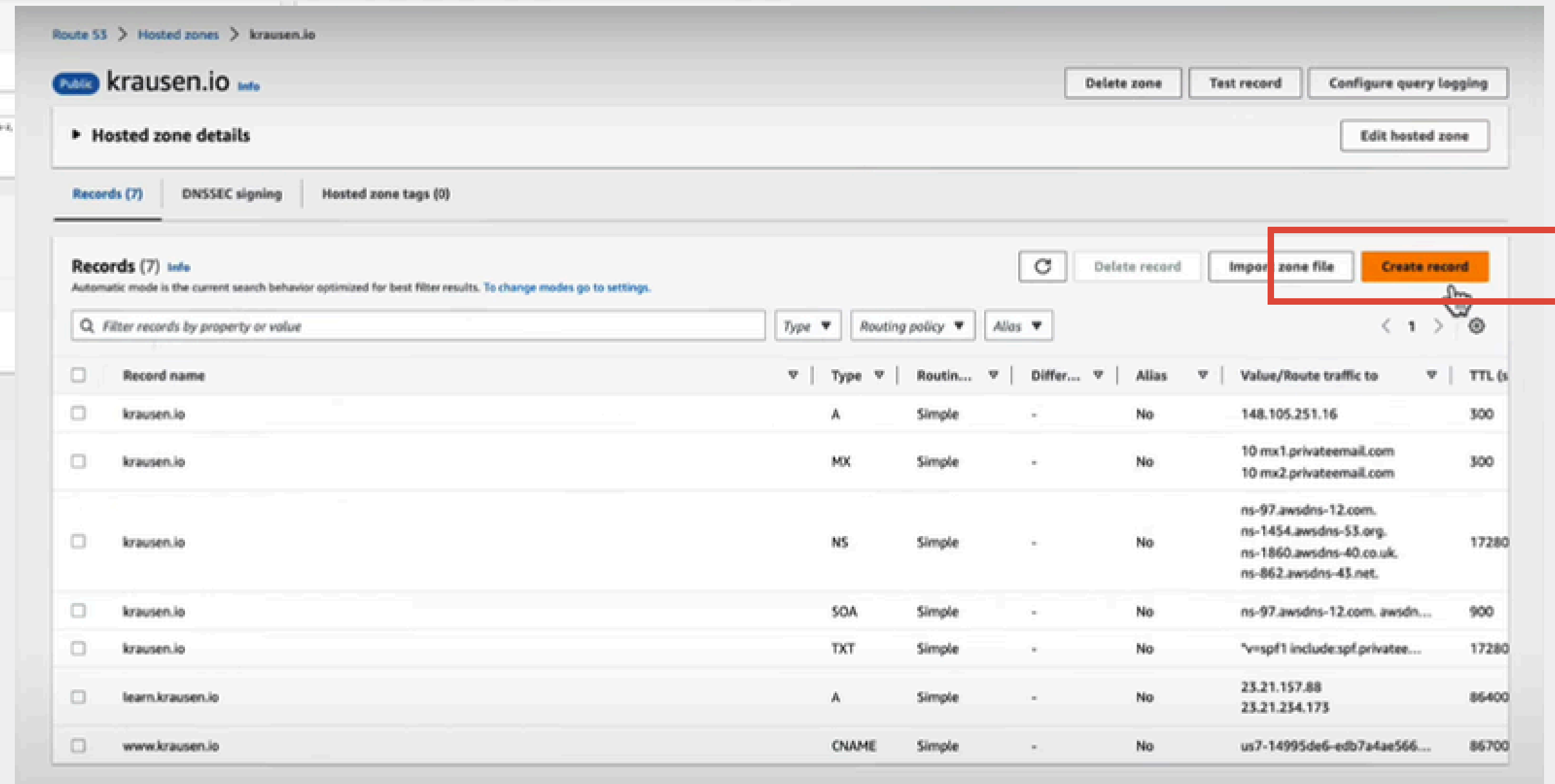
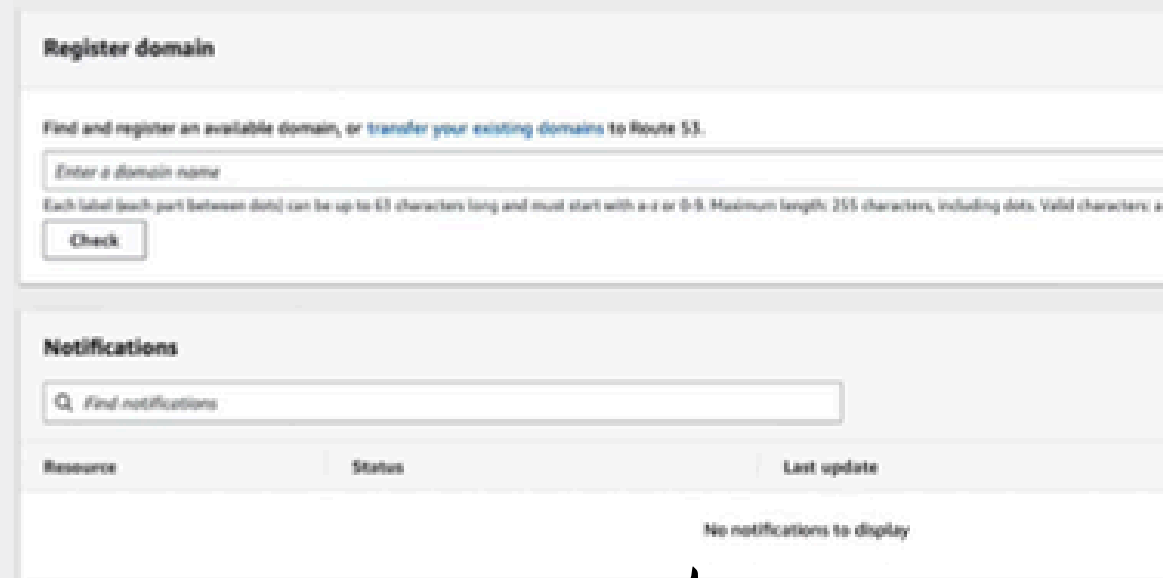
A private hosted zone determines how traffic is routed within an Amazon VPC.

- Dans la console AWS, allez dans Route 53 > Zones hébergées.
- Cliquez sur Créer une zone hébergée.
- Entrez votre domaine.
- Sélectionnez Zone hébergée publique et cliquez sur Créer une zone hébergée.

Ajouter des Enregistrements DNS dans R53



- Sélectionner la zone hébergée de votre domaine, cliquez sur Create Record.



Redirection vers Domaine Principal

Route 53 > Hosted zones > krausen.io > Create record

Create record [Info](#)

Quick create record [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#) .krausen.io

Keep blank to create a record for the root domain.

☐ Alias

Record type [Info](#)

Value [Info](#)

Enter multiple values on separate lines.

TTL (seconds) [Info](#)

Recommended values: 60 to 172800 (two days)

Routing policy [Info](#)

[Add another record](#)

[Cancel](#) [Create records](#)

► View existing records

The following table lists the existing records in krausen.io.

- Cliquez sur Créer un enregistrement
- Choisir le type d'enregistrement
- Dans le champ Nom, entrez le sous-domaine que vous souhaitez rediriger (par exemple, www pour rediriger www.mondomaine.com)
- Dans le champ Valeur, entrez l'URL générée par S3

- A (Adresse) : Pour associer un nom de domaine à une adresse IP (IPv4).
- AAAA : Pour associer un nom de domaine à une adresse IPv6.
- CNAME : Pour associer un alias à un autre nom de domaine.
- MX : Pour les enregistrements de messagerie (mail exchange).

Bonnes Pratiques

Utilisez HTTPS :

Configurez AWS Certificate Manager (ACM) et un **CloudFront Distribution** pour ajouter un certificat SSL.





**Merci pour votre
attention et votre
temps précieux**