

Laboratoire sur AWS Storage: Mise en place d'une répllication S3 Bucket interrégionale

Contexte

Nom de l'entreprise: GlobalTech Innovations

Secteur: Technologie et services numériques

Taille: 2 500 employés, avec des bureaux en Amérique du Nord, et en Europe.

Problème: GlobalTech Innovations est une entreprise internationale qui stocke une grande quantité de données critiques dans un bucket S3 situé dans la région **us-east-1**. En raison de la croissance rapide de l'entreprise, elle se développe dans d'autres régions du monde, notamment en Californie (région **us-west-2**).

L'équipe IT de **GlobalTech** a identifié plusieurs défis liés à la distribution de données à l'échelle mondiale:

1. **Performance des applications:** Les utilisateurs situés en Californie rencontrent des temps de latence plus élevés lorsqu'ils accèdent aux données stockées dans le bucket S3 en **us-east-1**.
2. **Continuité des activités:** L'entreprise souhaite s'assurer que ses données critiques sont protégées en cas de sinistre dans une région AWS.
3. **Conformité et réglementation:** GlobalTech doit respecter des réglementations locales qui imposent que certaines données soient stockées dans des centres de données situés dans la région même.

Demande de l'Entreprise

GlobalTech Innovations vous contacte en tant qu'un **ingénieur cloud spécialisé en AWS** pour mettre en place une solution de réplication de bucket S3 entre les régions afin de résoudre les problèmes de performance, de continuité des activités et de conformité.

Objectifs de l'Entreprise

1. **Réduction de la latence:** Répliquer les données vers des buckets S3 situés en Californie pour réduire les temps d'accès pour les utilisateurs locaux.
2. **Sauvegarde et reprise après sinistre:** Mettre en place une stratégie de réplication pour garantir que les données sont disponibles même en cas de sinistre dans la région `us-east-1`.
3. **Conformité régionale:** Répliquer certaines données sensibles dans des régions spécifiques pour répondre aux exigences réglementaires locales.

Description

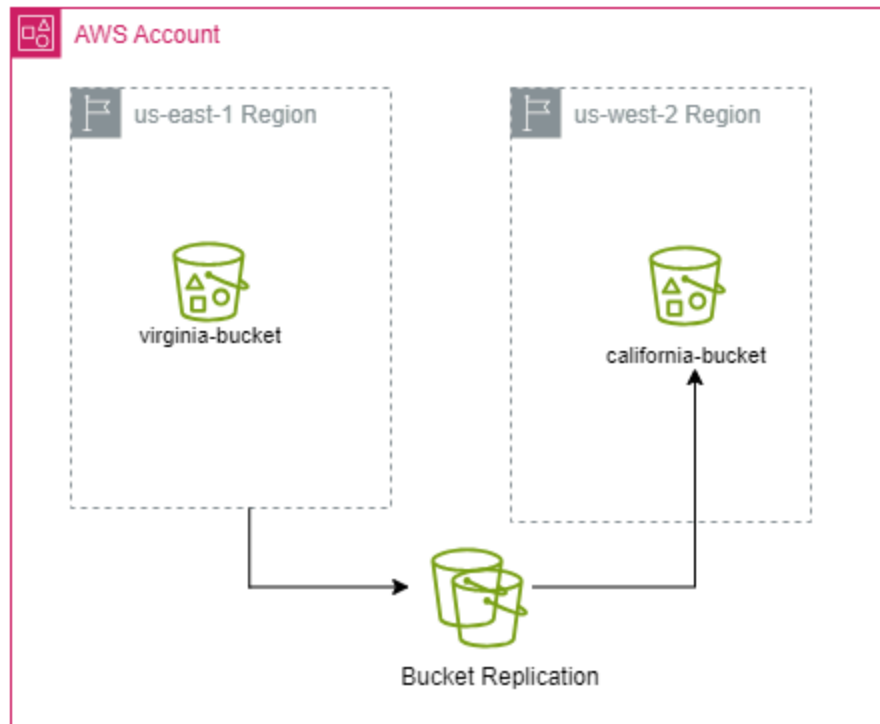
Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de premier ordre. Dans ce laboratoire, nous explorons comment utiliser Amazon S3 pour répliquer automatiquement tout objet stocké dans votre bucket S3 vers une autre région à l'autre bout du pays. Ce processus permet de s'assurer que nos fichiers restent accessibles dans n'importe quel scénario extrême où une perte de données pourrait se produire. À la fin de ce laboratoire, vous saurez comment créer des buckets S3 et activer la réplication automatique pour sauvegarder des fichiers dans un autre emplacement physique.

Temps de réalisation estimé: 45 minutes

Coûts: free tier

Architecture:

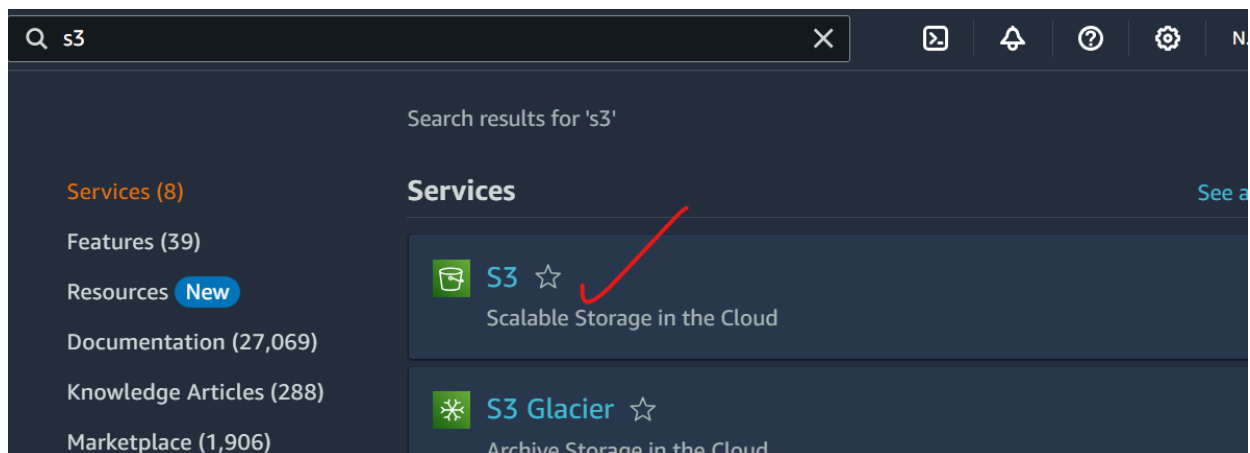
Mise en place de S3 Cross-Region Replication



Réalisation



Etape 1: Créer d'un bucket S3 dans la région de Virginia

- Dans la console AWS, naviguez vers S3.




- Copiez le nom du bucket **bucket-virginia-bootcamp** fourni par le laboratoire.

General purpose buckets (1) [Info](#) **All AWS Regions**

  **Copy ARN** **Empty** **Delete** **Create bucket**

Buckets are containers for data stored in S3.

 *Find buckets by name*

US East (N. Virginia) us-east-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 - New**
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](#)

bucket-virginia-bootcamp

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

- Décocher le Public Access Settings, cochez le acknowledgement, et activez le versioning

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

- Laissez le choix par défaut concernant le bucket key et cliquez sur create bucket pour créer votre compartiment S3.


Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

► Advanced settings

 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

- Une fois que votre compartiment est créé, vous pouvez uploader vos fichiers ou document, pour ce lab, nous allons uploader un fichier texte nommé version 1. Pour cela, nous allons cliquer sur upload comme sur l'image.

bucket-virginia-bootcamp [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#)

Objects (0) [Info](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

☐ Show versions < 1 > [Settings](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
--------------------------	------	------	---------------	------	---------------

No objects

- La nouvelle fenêtre suivante s'affiche à nous. Et de la, nous pouvons ajouter des fichiers en cliquant sur add files ou add folder pour ajouter un document entier. Enfin, pour effectivement valider l'ajout, nous allons cliquer sur upload

[Amazon S3](#) > [Buckets](#) > [bucket-virginia-bootcamp](#) > Upload

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (0)

All files and folders in this table will be uploaded.

[Remove](#)

[Add files](#)

[Add folder](#)

< 1 >

<input type="checkbox"/>	Name	Folder	Type
--------------------------	------	--------	------

Files and folders (1 Total, 125.0 B) Remove Add files Add folder

All files and folders in this table will be uploaded.

< 1 >

<input type="checkbox"/>	Name	Folder	Type
<input type="checkbox"/>	Version1.txt	-	text/plain

Metadata - optional

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

No metadata associated with this resource.

Add metadata

Cancel Upload

- Dans l'image ci-dessous, nous avons uploadé une nouvelle le fichier txt nommé **version 1** mis a jour, mais portant les mêmes noms avec des contenus différents, étant donné que nous avons activé le versioning, nous avons désormais la possibilité de voir les différentes versions de notre fichier **version 1**.
- **NB:** l'activation du versioning permet de protéger contre la suppression et la réplication ne se fait qu'en activant le versioning.

Objects (2) [Info](#)

Refresh Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Show versions < 1 > Settings

<input type="checkbox"/>	Name	Type	Version ID	Last modified	Size	Storage class
<input type="checkbox"/>	Version1.txt	txt	UOjL2ebHg45bgcgf3 OT13ze_Mxeszd_9	August 25, 2024, 20:42:01 (UTC+02:00)	192.0 B	Standard
<input type="checkbox"/>	Version1.txt	txt	vFIRh3yYTSJ2Jbo3OJ Y2cZiAzesbFi90	August 25, 2024, 20:39:08 (UTC+02:00)	125.0 B	Standard

Etape 2: Création d'un bucket de réplication dans la région de la californie

De la même façon que dans l'étape précédente, nous allons cliquer sur create bucket, entrez le nom de notre bucket nommé **my-replica-bucket-california**

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region
US West (N. California) us-west-1

Bucket name [Info](#)

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.

Format: s3://bucket/prefix

- Décocher le Public Access Settings, cochez le acknowledgement, et activez le versioning et valider les configurations en cliquant sur create bucket.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☐ **Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Etape 3: création de la règle de réplication

Dans cette étape, nous allons configurer une règle de réplication, ce qui va permettre à notre bucket de la virginie d'avoir une réplique dans une autre région qui est la californie.

- Pour cela, sélectionnez¹ notre compartiment **bucket-virginia-bootcamp**.

General purpose buckets (2) Info All AWS Regions

Buckets are containers for data stored in S3.

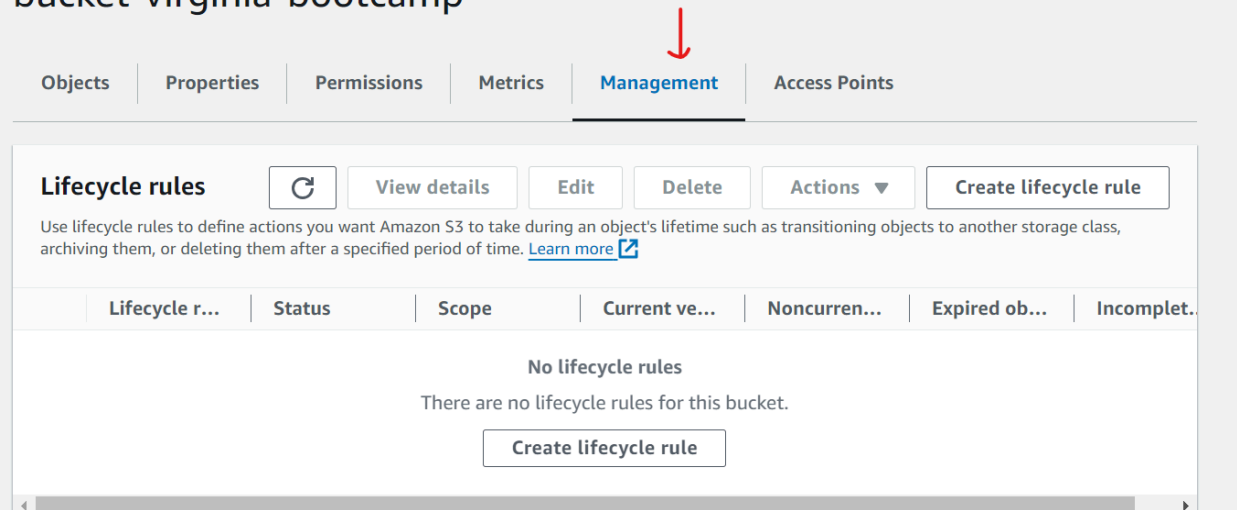
Find buckets by name

Name	AWS Region	IAM Access Analyzer	Creation date
bucket-virginia-bootcamp	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 25, 2024, 20:31:11 (UTC+02:00)

- Dans notre compartiment, naviguons sur management, comme sur l'image, scroller jusqu'à **create replication rule** et cliquer.

¹ Lab proposed by Lahda Biassou Alphonsine.

bucket-virginia-bootcamp

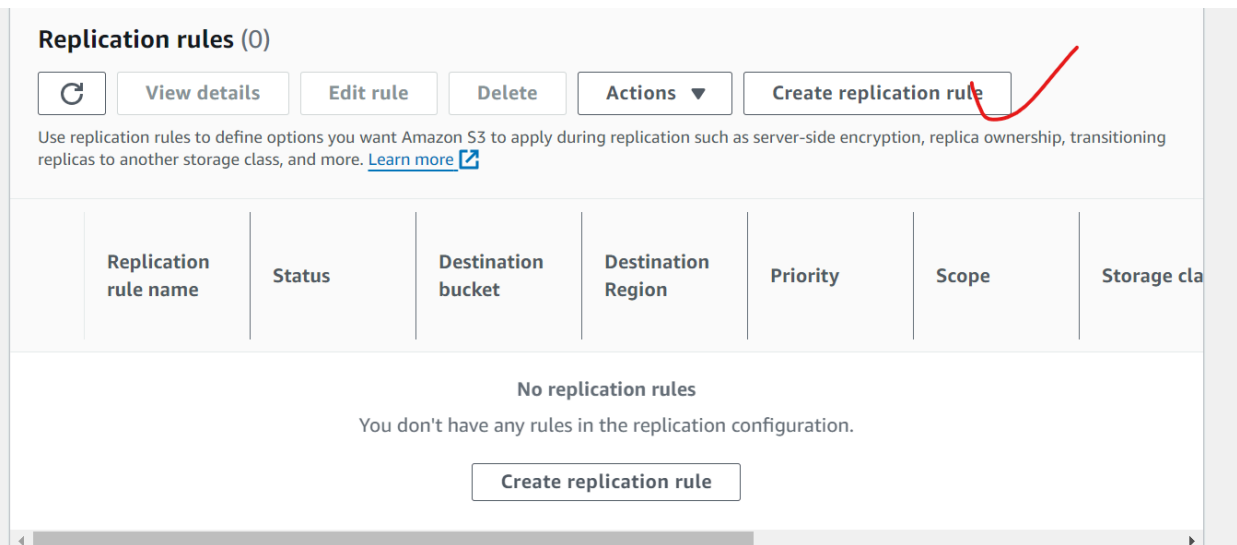


Objects | Properties | Permissions | Metrics | **Management** | Access Points

Lifecycle rules

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Lifecycle r...	Status	Scope	Current ve...	Noncurren...	Expired ob...	Incomplet...
No lifecycle rules						
There are no lifecycle rules for this bucket.						
Create lifecycle rule						



Replication rules (0)

[View details](#) [Edit rule](#) [Delete](#) [Actions](#) [Create replication rule](#)

Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class
No replication rules						
You don't have any rules in the replication configuration.						
Create replication rule						

- Spécifions le noms de notre règle, pour ce lab, nous mettons **replication-rule-for-california-bootcamp**.

Create replication rule [Info](#)

Replication rule configuration

Replication rule name

replication-rule-for-california-bootcamp

Up to 255 characters. In order to be able to use CloudWatch metrics to monitor the progress of your replication rule, the replication rule name must only contain English characters.

Status

Choose whether the rule will be enabled or disabled when created.

☒ Enabled

☐ Disabled

Priority

The priority value resolves conflicts that occur when an object is eligible for replication under multiple rules to the same destination. The rule is added to the configuration at the highest priority and the priority can be changed on the replication rules table.

- Au niveau de choose rule scope, choisir **apply to all objects in the bucket**

Source bucket

Source bucket name

bucket-virginia-bootcamp

Source Region

US East (N. Virginia) us-east-1

Choose a rule scope

☐ Limit the scope of this rule using one or more filters

☒ Apply to all objects in the bucket

- Choisir l'option a bucket in this account, c'est à dire notre compte actuel.

Destination

Destination

You can replicate objects across buckets in different AWS Regions (Cross-Region Replication) or you can replicate objects across buckets in the same AWS Region (Same-Region Replication). You can also specify a different bucket for each rule in the configuration. [Learn more](#) or see [Amazon S3 pricing](#)

- ☒ Choose a bucket in this account ← 1
- ☐ Specify a bucket in another account

Bucket name

Choose the bucket that will receive replicated objects.

my-replica-bucket-california ← 3

↓ 2
[Browse S3](#)

Destination Region

US West (N. California) us-west-1

- Choisir l'option create new IAM Role, AWS va créer un role pour votre règle de réplication

IAM role

- ☒ Create new role ←
- ☐ Choose from existing IAM roles
- ☐ Enter IAM role ARN

- Pour le reste des paramètres, laissons par défaut, ensuite validons sur **save**.

Additional replication options

☐

Replication Time Control (RTC)

Replication Time Control replicates 99.99% of new objects within 15 minutes and includes replication metrics. Additional fees will apply. [Learn more](#)

☐

Replication metrics

With replication metrics, you can monitor the total number and size of objects that are pending replication, and the maximum replication time to the destination Region. You can also view and diagnose replication failures. CloudWatch metrics fees apply. [Learn more](#) or see [Amazon CloudWatch pricing](#)

☐

Delete marker replication

Delete markers created by S3 delete operations will be replicated. Delete markers created by lifecycle rules are not replicated. [Learn more](#)

☐

Replica modification sync

Replicate metadata changes made to replicas from the destination bucket to the source bucket. [Learn more](#)

Cancel

Save

Etape 4: test de notre réplication

D'abord modifier encore notre fichier version 1 et l'uploader dans le bucket situé en virginie, ensuite aller dans le bucket situé en californie pour vérifier si effectivement le réplication se passe.

- Notre image ci-dessous nous montre que la réplication est efficace.

my-replica-bucket-california [Info](#)

- Objects
- Properties
- Permissions
- Metrics
- Management
- Access Points

Objects (1) [Info](#)

Copy S3 URI

Copy URL

Download

Open [↗](#)

Delete

Actions ▼

Create folder

Upload

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) [↗](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#) [↗](#)

Find objects by prefix

Show versions

< 1 >