

#### Propiedad de objetos Información

Controle la propiedad de los objetos escritos en este bucket desde otras cuentas de AWS y el uso de listas de control de acceso (ACL). La propiedad de los objetos determina quién puede especificar el acceso a los objetos.

## ACL deshabilitadas (recomendado)

Todos los objetos de este bucket son propiedad de esta cuenta. El acceso a este bucket y sus objetos se especifica solo mediante políticas.

#### ACL habilitadas

Los objetos de este bucket pueden ser propiedad de otras cuentas de AWS. El acceso a este bucket y sus objetos se puede especificar mediante ACL.

Propiedad del objeto

Aplicada al propietario del bucket

## Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. Más información

#### Bloquear todo el acceso público

Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

- Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)
  S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.
- Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)
  - S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.
- Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas
  - S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.
- Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública
  - S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.

## Control de versiones de buckets

El control de versiones es una forma de mantener múltiples variantes de un objeto dentro del mismo bucket. Puede utilizar el control de versiones para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Amazon S3. Con el control de versiones, puede recuperarse con facilidad de las acciones involuntarias de los usuarios y de los errores en las aplicaciones. Más información

Control de versiones de buckets

- Desactivar
- Habilitar

## Etiquetas - opcional (0)

Puede utilizar etiquetas de bucket para realizar un seguimiento de los costos de almacenamiento y organizar buckets. Más información 🔀

No hay etiquetas asociadas a este bucket.

Agregar etiqueta

## Cifrado predeterminado Información

El cifrado del lado del servidor se aplica automáticamente a los nuevos objetos almacenados en este bucket.

Tipo de cifrado Información

- O Cifrado del servidor con claves administradas de Amazon S3 (SSE-S3)
- O Cifrado del servidor con claves de AWS Key Management Service (SSE-KMS)
- O Cifrado de doble capa del servidor con claves de AWS Key Management Service (DSSE-KMS)

Proteja sus objetos con dos capas de cifrado independientes. Para obtener más información sobre los precios, consulte DSSE-KMS pricing (Precios de DSSE-KMS) en la pestaña Storage (Almacenamiento) de la página de precios de Amazon S3.

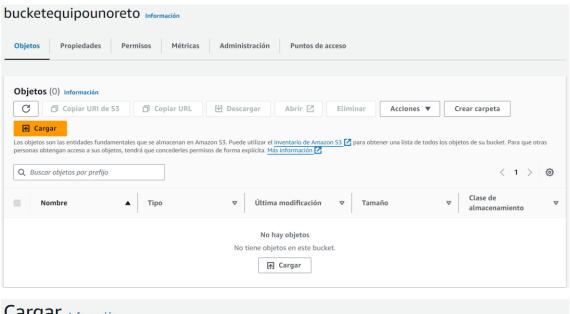
#### Clave de bucket

El uso de una clave de bucket de S3 para SSE-KMS reduce los costos de cifrado al reducir las llamadas a AWS KMS. Las claves de bucket de S3 no son compatibles con DSSE-KMS. Más información 🔀

- Desactiva
- Habilitar

Crear bucket

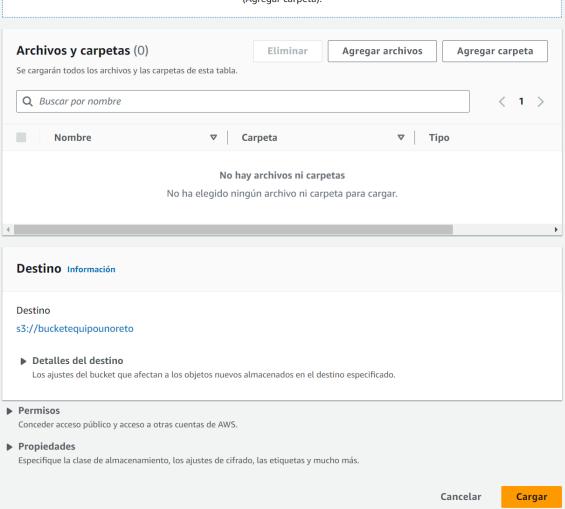


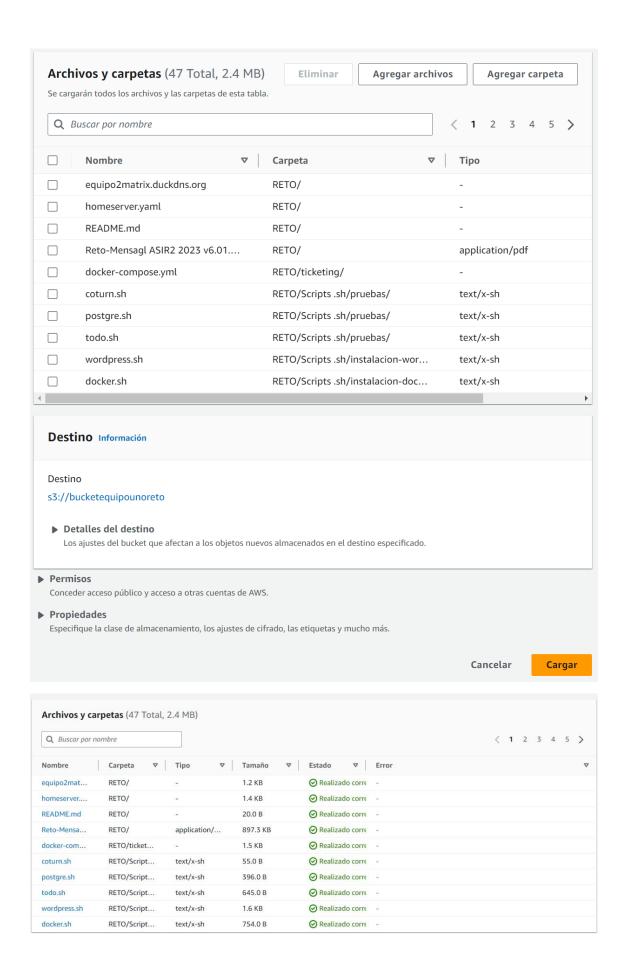


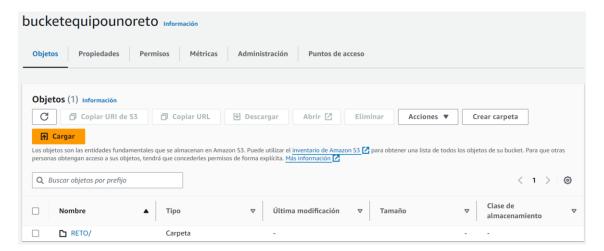
# Cargar Información

Agregue los archivos y las carpetas que desea cargar en S3. Para cargar un archivo de más de 160 GB, utilice la CLI de AWS, el SDK de AWS o la API REST de Amazon S3. Más información 🔀

Arrastre y suelte aquí los archivos y carpetas que desee cargar, o seleccione Add files (Agregar archivos) o Add folder (Agregar carpeta).





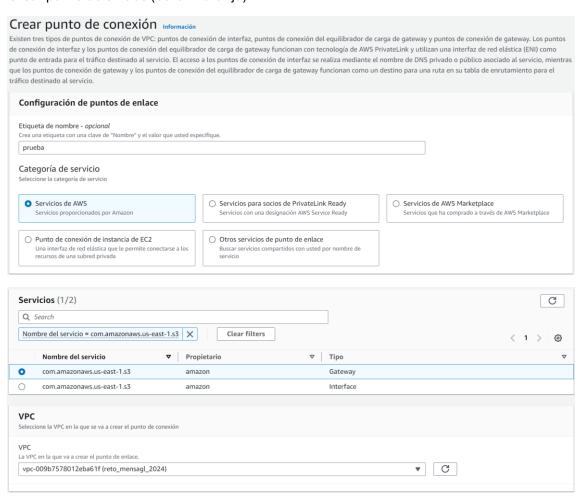


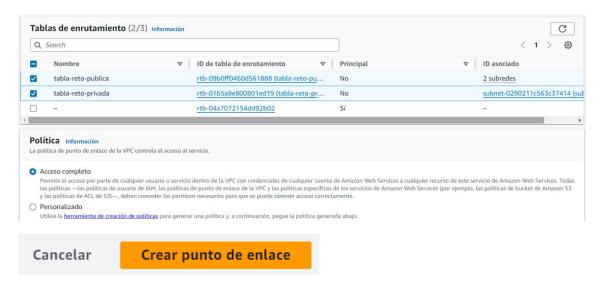
#### Conectarlo a las instancias

#### Ir a VPC

Puntos de conexión (a la izquierda)

Crear punto de enlace (botón naranja)





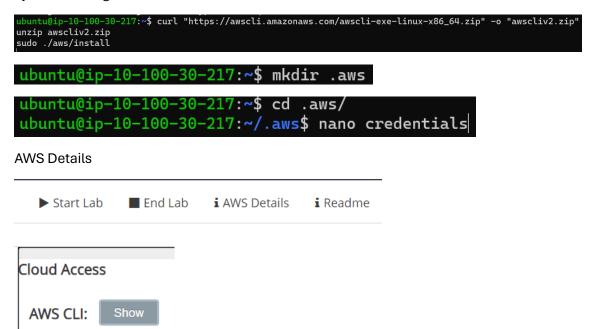
Ir a la instancia que se quiere utilizar el cubo s3.

Se hará en la instancia de nginx.

Instalar unzip.

```
ubuntu@ip-10-100-30-217:~$ sudo apt install unzip -y
```

Ejecutar los siguientes comandos.



Se copia y se pega en el archivo credentials.

## AWS CLI:

Copy and paste the following into ~/.aws/credentials

```
[default]
aws_access_key_id=ASIA4KRX6LMRKZSNVW4S
aws_secret_access_key=aZfXpYV5W9L3XlpxrVD2A5pv3Rp
0BELXMaiQyeXV
aws_session_token=FwoGZXIvYXdzEPr///////wEaDIv
7H11LmgZPjkcTJCK9Af3yXWobExZh1sG++icD9pc6Y7J37mz8
bf46yMMkIli5MqvW0bGCwX22lGAt4b6Yr9rUNudjpcPIIxxos
bGfzeqj5mt0GjyTe9rKJ4+Ek6mUwEsorifey/B94bTllu5oVm
XE6ITSt+7lMxMeUJXwkFjBMjMa0NCUGpW4RoViKlMrfZEIf3T
wOhaDd3zwYIDjq06TGDvdd4X3H+2kVLWwfz4fh+MWiwbVG1aI
6FRIvTHxGkQQcbdGJIIHWmP31yiP5M2tBjIt4J5Iz78681hxI
kkVRsRKSOq2Gh7rF1v7XXmfxTBSjzbAJMPipwg5ZJdhuLNy
```

Se crea un archivo prueba.txt

Con el siguiente comando se sube al cubo s3

ubuntu@ip-10-100-30-217:~\$ aws s3 cp prueba.txt s3://bucketequipounoreto/RETO/prueba.txt upload: ./prueba.txt to s3://bucketequipounoreto/RETO/prueba.txt