Crear bucket Información

Los buckets son contenedores de datos almacenados en S3.

Configuración general

Región de AWS

EE.UU. Este (Norte de Virginia) us-east-1

Tipo de bucket | Información

- (•) Uso general
  Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.
- ( ) Directorio
  Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.

Nombre del bucket | Información

upm-next-practicaray-bucket

Los nombres de los buckets deben tener entre 3 y 63 caracteres y ser únicos dentro del espacio de nombres global. Los nombres de los buckets también deben empezar y terminar con una letra o un número. Los caracteres válidos son a-z, 0-9, puntos (.) y guiones (-). Más información

Copiar la configuración del bucket existente: *opcional*

Solo se copia la configuración del bucket en los siguientes ajustes.

Elegir el bucket

Formato: s3://bucket/prefijo

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

- [x] **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

- (•) Cifrado del servidor con claves administradas de Amazon S3 (SSE-S3)
- ( ) Cifrado del servidor con claves de AWS Key Management Service (SSE-KMS)
- ( ) 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

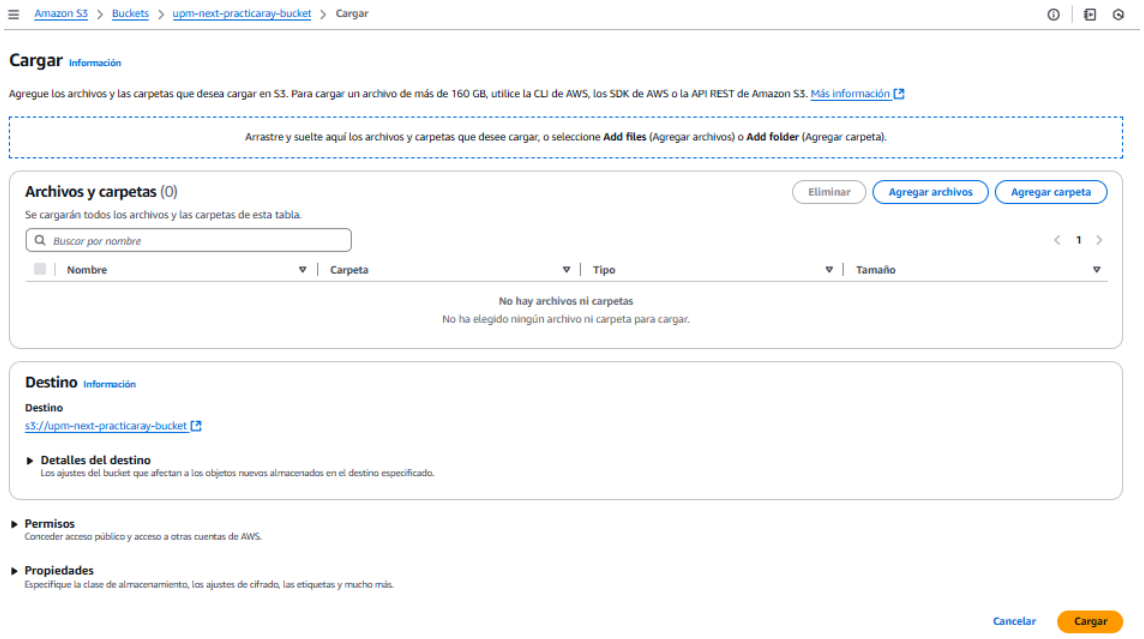
El uso de una clave de bucket de S3 para SSE-KMS reduce los costos de cifrado al reducir las llamadas a AWS KMS. Las claves de bucket de S3 no son compatibles con DSSE-KMS. Más información

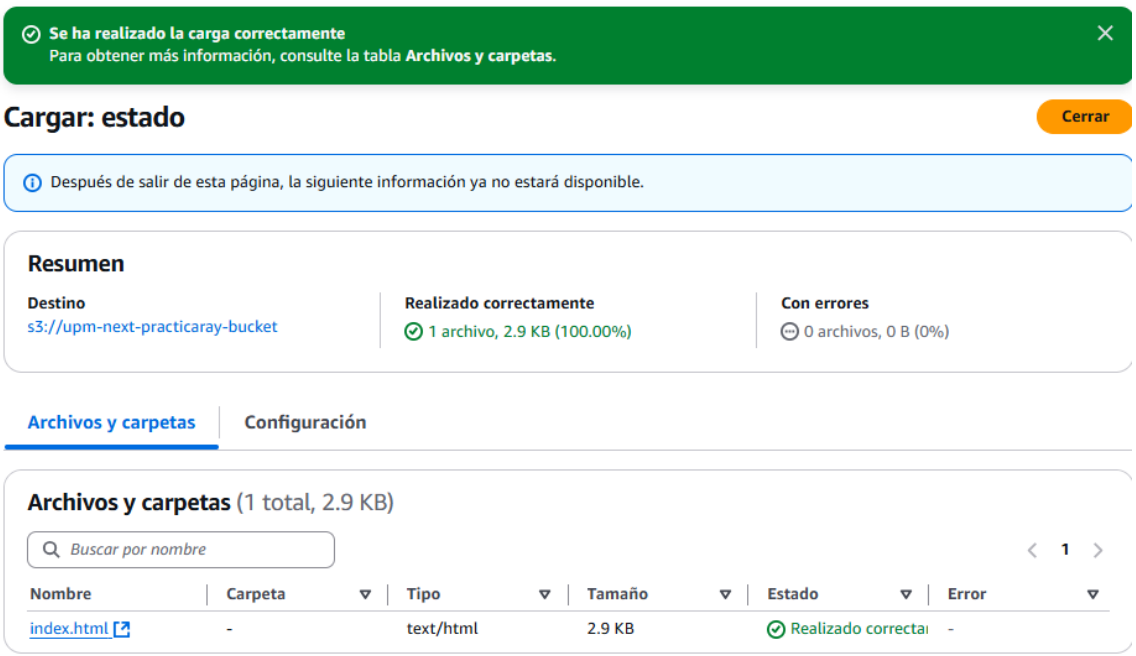
- ( ) Desactivar
- (•) Habilitar

▸ **Configuración avanzada**

ⓘ Después de crear el bucket, puede cargar archivos y carpetas, y configurar ajustes adicionales en él.

Cancelar | Crear bucket


Amazon S3 > Buckets > upm-next-practicaray-bucket > Cargar
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, los 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).
Archivos y carpetas (0)
Se cargarán todos los archivos y las carpetas de esta tabla.
Eliminar
Agregar archivos
Agregar carpeta
Buscar por nombre
Nombre
Carpeta
Tipo
Tamaño
No hay archivos ni carpetas
No ha elegido ningún archivo ni carpeta para cargar.
Destino Información
Destino
s3://upm-next-practicaray-bucket
Detalles del destino
Los ajustes del bucket que afectan a los objetos nuevos almacenados en el destino especificado.
Permisos
Conceder acceso público y acceso a otras cuentas de AWS.
Propiedades
Especifique la clase de almacenamiento, los ajustes de cifrado, las etiquetas y mucho más.
Cancelar
Cargar


Se ha realizado la carga correctamente
Para obtener más información, consulte la tabla Archivos y carpetas.
Cargar: estado
Cerrar
Después de salir de esta página, la siguiente información ya no estará disponible.
Resumen
Destino
s3://upm-next-practicaray-bucket
Realizado correctamente
1 archivo, 2.9 KB (100.00%)
Con errores
0 archivos, 0 B (0%)
Archivos y carpetas
Configuración
Archivos y carpetas (1 total, 2.9 KB)
Buscar por nombre
Nombre
Carpeta
Tipo
Tamaño
Estado
Error
index.html
-
text/html
2.9 KB
Realizado correctar
-

upm-next-practicaray-bucket Información

Objetos | Metadatos | Propiedades | Permisos | Métricas | Administración | Puntos de acceso

Objetos (1/1)

Copiar URI de S3 | Copiar URL | Descargar | Abrir | Eliminar | Acciones | Crear carpeta | Cargar

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el inventario de Amazon S3 para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. Más información

Buscar objetos por prefijo

1

Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
index.html	html	22 Apr 2025 9:36:37 PM CEST	2.9 KB	Estándar

Amazon S3 > Buckets > upm-next-practicaray-bucket > Editar el bloqueo de acceso público (configur...

Editar el bloqueo de acceso público (configuración del bucket) Información

Bloquear acceso público (configuración del bucket)

Se concede acceso público a 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 de S3, active Bloquear todo acceso público. Esta configuración se aplica en exclusiva a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo acceso público pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que sus aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a sus buckets u objetos, puede personalizar los valores de configuración individuales a continuación para que se ajusten mejor a sus necesidades específicas de almacenamiento. 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.

Cancelar | Guardar cambios

ARN del bucket

arn:aws:s3:::upm-next-practicaray-bucket

Política

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6              "Principal": "*",
7              "Effect" : "Allow",
8              "Action": [
9                  "s3:GetObject"
10
11                 ],
12                 "Resource": "arn:aws:s3:::upm-next-practicaray-bucket/*"
13
14         }
15         ]
16
17 }
```

+ Agregar nueva instrucción

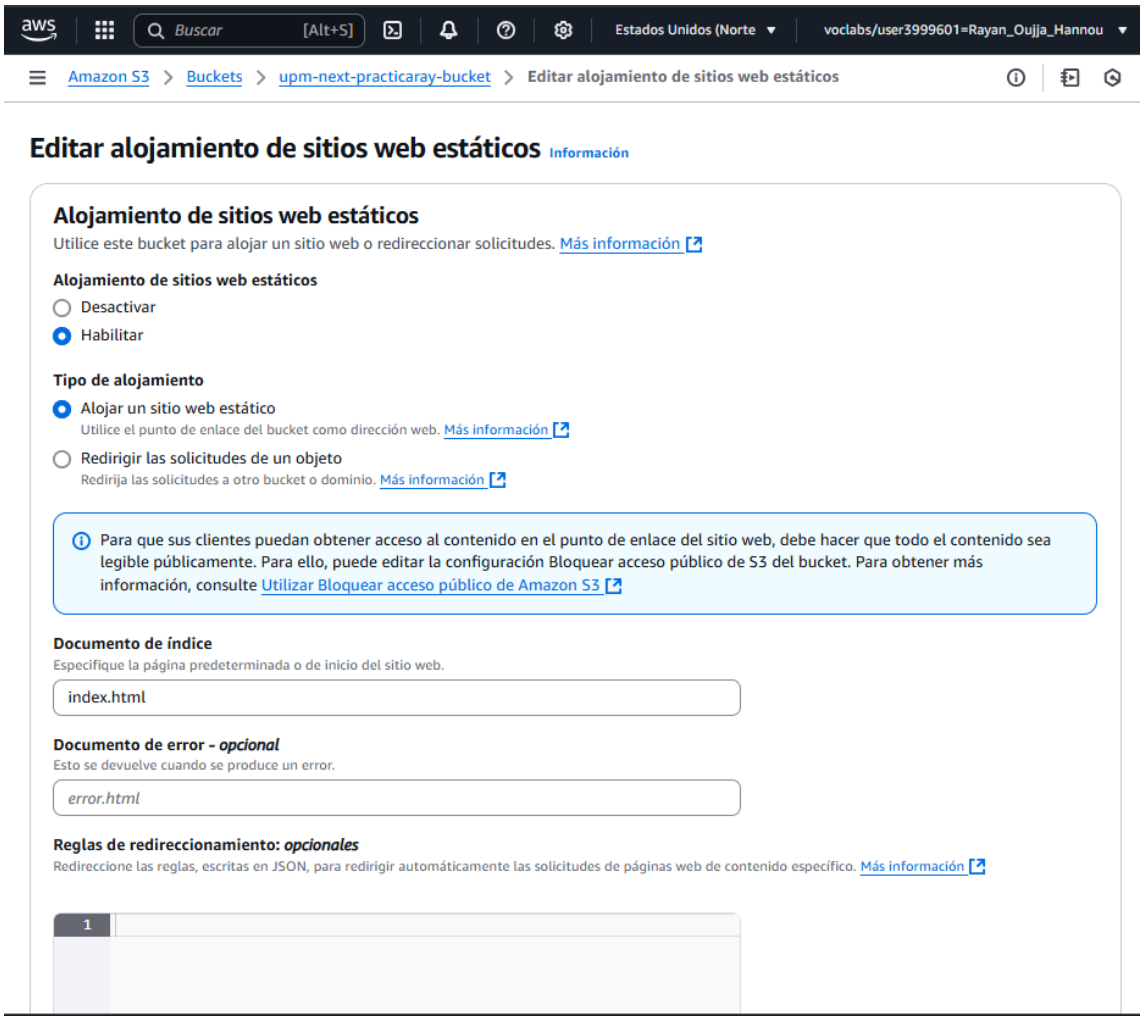
JSON Ln 17, Col 1

Editar instrucción

Seleccionar una instrucción

Seleccione una instrucción existente en la política o agregue una nueva instrucción.

+ Agregar nueva instrucción


Buscar [Alt+S]
Estados Unidos (Norte)
voclabs/user3999601=Rayan_Oujja_Hannou
Amazon S3 > Buckets > upm-next-practicaray-bucket > Editar alojamiento de sitios web estáticos
Editar alojamiento de sitios web estáticos Información
Alojamiento de sitios web estáticos
Utilice este bucket para alojar un sitio web o redireccionar solicitudes. Más información
Alojamiento de sitios web estáticos
Desactivar
Habilitar
Tipo de alojamiento
Alojar un sitio web estático
Utilice el punto de enlace del bucket como dirección web. Más información
Redirigir las solicitudes de un objeto
Redirija las solicitudes a otro bucket o dominio. Más información
Para que sus clientes puedan obtener acceso al contenido en el punto de enlace del sitio web, debe hacer que todo el contenido sea legible públicamente. Para ello, puede editar la configuración Bloquear acceso público de S3 del bucket. Para obtener más información, consulte Utilizar Bloquear acceso público de Amazon S3
Documento de índice
Especifique la página predeterminada o de inicio del sitio web.
index.html
Documento de error - opcional
Esto se devuelve cuando se produce un error.
error.html
Reglas de redireccionamiento: opcionales
Redireccione las reglas, escritas en JSON, para redirigir automáticamente las solicitudes de páginas web de contenido específico. Más información
1