

Laboratorio de desafíos: Crear un sitio web estático para the Café

Primero que nada nos descargamos los ficheros que usaremos más adelante.

Creamos un bucket nuevo con las siguientes configuraciones: nicolasrr-bucket

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: nuevo**
Recomendado para buckets que utilizan únicamente S3 Express One Zone para mayor rapidez de los datos y disponibilidad.

Nombre del bucket **Información**

nicolasbucket

El nombre del bucket debe ser único dentro del espacio de nombres global y seguir las reglas de [reglas para la asignación de nombres de buckets](#)

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

Como no nos dice nada de esto lo dejamos por defecto:

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

Desactivamos bloquear todo el acceso público:

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 acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos de acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS requiere el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionen correctamente. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración 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 una es independiente entre sí.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas:**
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos de acceso público a los recursos de S3 mediante ACL.

☐ **Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista (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 acceso público nuevas**
S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets. 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 buckets y puntos de acceso pública**
S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan

Dejamos el resto por defecto.

Activamos el alojamiento de sitios web estáticos y ponemos esto:

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](#)

i Para que sus clientes puedan obtener acceso al contenido en el pu...
que todo el contenido sea legible públicamente. Para ello, puede...
público de S3 del bucket. Para obtener más información, consulte...
[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*

Redirigir las reglas, escritas en JSON, para redirigir automáticamente las solicitudes

Cargamos los archivos:

Archivos y carpetas (10 Total, 21.7 MB) Eliminar Agregar archivos

Se cargarán todos los archivos y las carpetas de esta tabla.

<input type="checkbox"/>	Nombre	Carpeta
<input type="checkbox"/>	Cafe-Owners.png	images/
<input type="checkbox"/>	Cake-Vitrine.png	images/
<input type="checkbox"/>	Coffee-and-Pastries.png	images/
<input type="checkbox"/>	Coffee-Shop.png	images/
<input type="checkbox"/>	Cookies.png	images/
<input type="checkbox"/>	Cup-of-Hot-Chocolate.png	images/
<input type="checkbox"/>	Strawberry-&-Blueberry-Tarts.png	images/
<input type="checkbox"/>	Strawberry-Tarts.png	images/
<input type="checkbox"/>	styles.css	css/
<input type="checkbox"/>	index.html	-

Respondemos la primera pregunta:

Al visualizar el sitio web después de la Tarea 3, ¿ves la página en el navegador?

Vamos a comprobarlo, vamos a nuestro bucket/propiedades/alojamiento_de_sitios_web_estáticos y abrimos el enlace:

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: SEDRZX4SXW1C1V5H
- HostId: Bu6JwnOXU1QyUFCG7K0lwCSNITQD8aHS/

An Error Occurred While Attempting to Retrieve :

- Code: AccessDenied
- Message: Access Denied

No podemos, los archivos aún no son públicos.

Tenemos que crear una política para conceder acceso público de lectura, según la documentación oficial es de la siguiente manera:

Elegimos nuestro bucket, le damos a permisos, debajo de Bloquear acceso publico, elegimos editar y desmarcamos bloquear todo el acceso publico.

- ☐ **Bloquear todo el acceso público**
Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación independientemente entre sí.
- ☐ **Bloquear el acceso público a buckets y objetos concedido a través de ACL**
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets asignados a través de ACL de acceso público para buckets y objetos existentes. Esta configuración no afecta al acceso público a los recursos de S3 mediante ACL.
- ☐ **Bloquear el acceso público a buckets y objetos concedido a través de ACL (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 nuevas**
S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público. Esta configuración no afecta a las políticas ya existentes que permiten acceso público.
- ☐ **Bloquear el acceso público y entre cuentas a buckets y objetos con políticas públicas**
S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso con políticas públicas.


Activamos la ACL:

Propiedad del objeto

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.

 Recomendamos desactivar las listas de control de acceso (ACL), a menos que necesite controlar el acceso a cada objeto individualmente o que el escritor del objeto sea el propietario de los datos que carga. Utilizar una política de bucket en lugar de ACL para compartir datos con usuarios externos a la cuenta simplifica la administración de permisos y la realización de auditorías.

Nos saldrá un aviso, le damos a Reconozco...

Ponemos que todo el mundo tiene acceso de solo lectura:

Editar lista de control de acceso (ACL) Información

Lista de control de acceso (ACL)

Conceder permisos básicos de lectura/escritura a otras cuentas de AWS. [Más información](#)

Beneficiario

Propietario del bucket (su cuenta de AWS)

ID canónico:

1c3846b133259fae3129600ddf4ae997a4f85994f10c0e381295b80cebf271ab

Todo el mundo (acceso público)

Grupo:

http://acs.amazonaws.co

Objetos

☒ Lista

☒ Escritura

☐ Lista

☐ Escritura

ACL del bucket

☒ Lectura

☒ Escritura

☒ Lectura

☐ Escritura

Y por ultimo hacemos los objetos públicos mediante ACL:

Objetos (3) Información

Copiar URI de S3

Copiar URL

Descargar

Abrir

Eliminar

Acciones

Crear carpeta

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. Puede concederles permisos de forma explícita. [Más información](#)

Q

Buscar objetos por prefijo

☐ Mostrar versiones

☒

Nombre

Tipo

Última modificación

Tamaño

☒

css/

Carpeta

-

☒

images/

Carpeta

-

☒

index.html

html

4 May 2024 12:08:26 PM CEST

Descargar como

Compartir con una URL prefirada

Calcular el tamaño total

Copiar

Trasladar

Iniciar restauración

Consultar con S3 Select

Editar acciones

Cambiar el nombre del objeto

Editar clase de almacenamiento

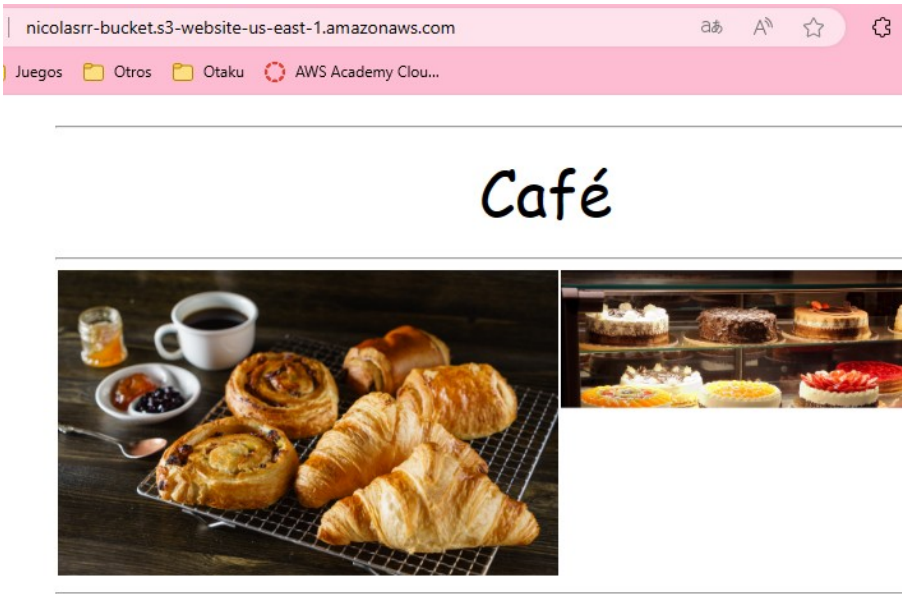
Editar cifrado del lado del servicio

Editar metadatos

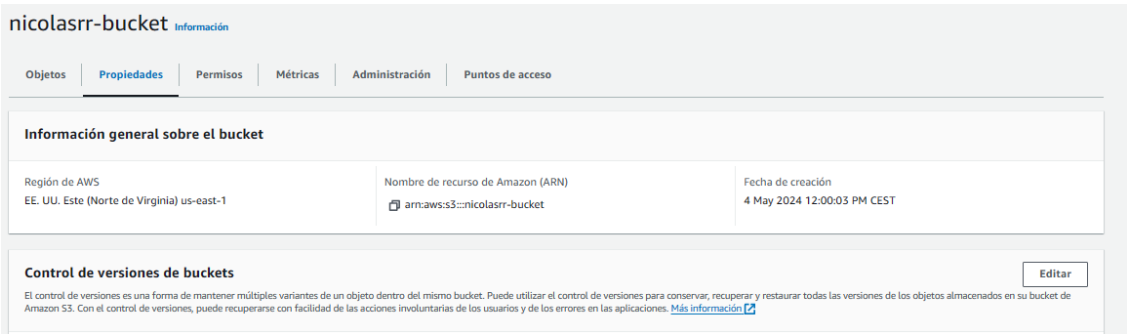
Editar etiquetas

Hacer público mediante ACL

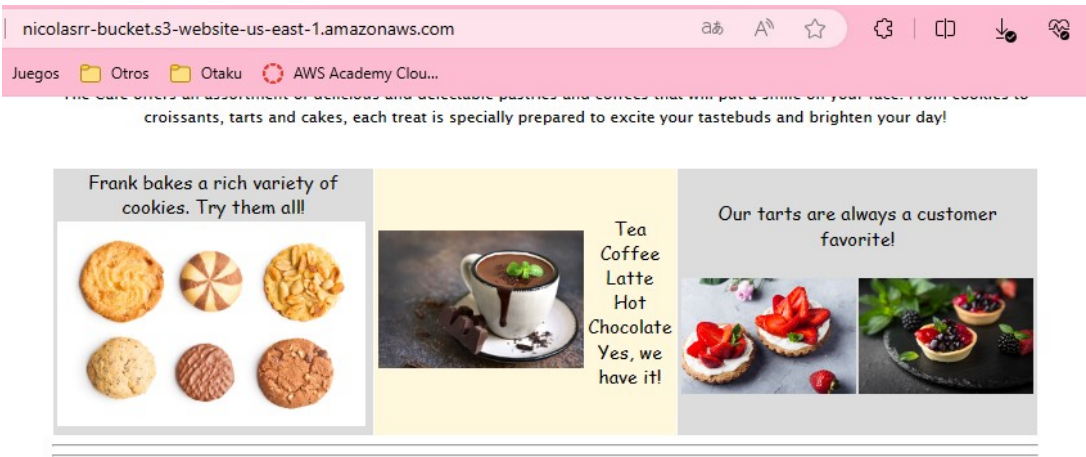
Vemos que la página se muestra:



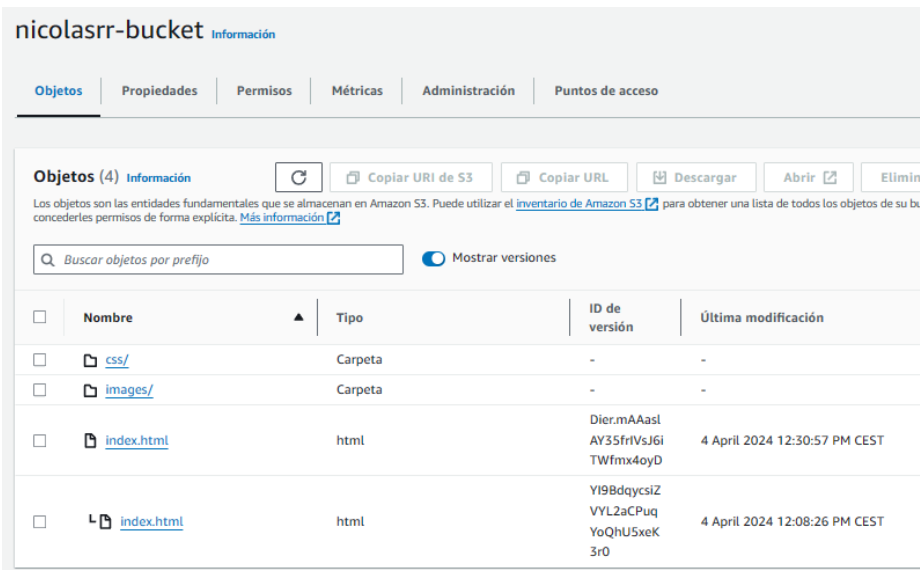
Vamos a habilitar el control de versiones en el bucket de S3, para ello nos vamos a la siguiente pestaña:



Editamos y habilitamos, está habilitado por defecto. Vamos a editar nuestro archivo html, editamos el css que tiene incluido y subimos el archivo modificado, volvemos a hacer publico mediante ACL y vemos los cambios.



Si ahora vamos a nuestro bucket y le damos al deslizador **Mostrar versiones**, vemos que index.html tiene 2 versiones:

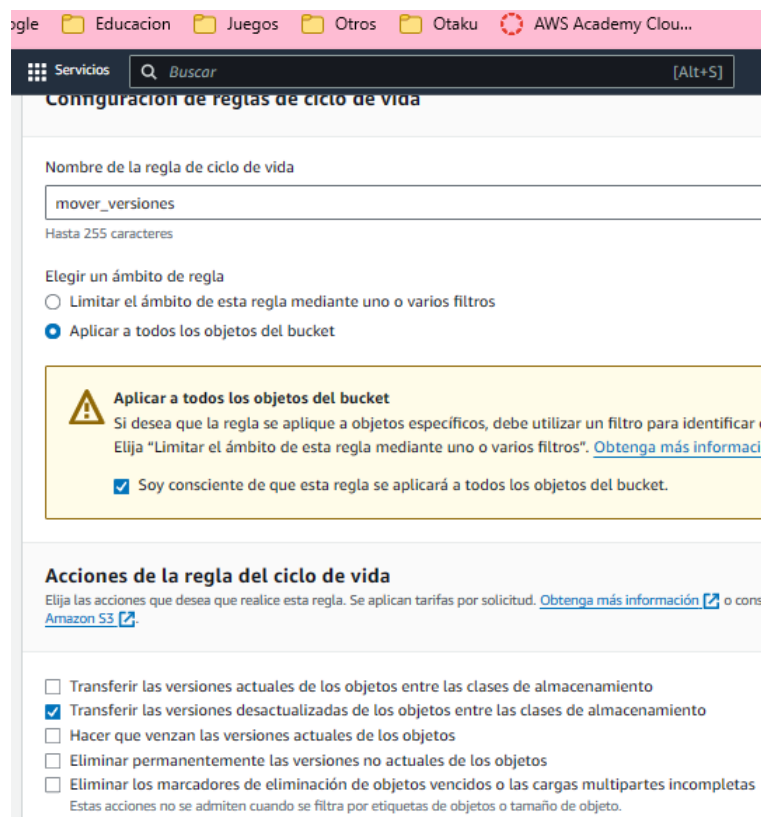
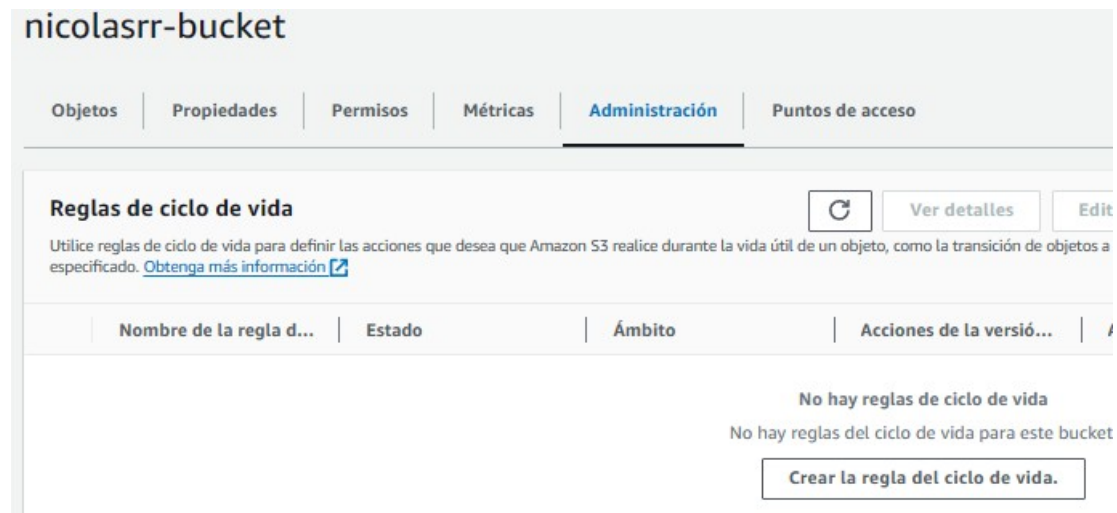


Resolvemos la siguiente pregunta:

¿cuál es otra forma de garantizar la máxima protección y evitar la eliminación accidental de una versión conservada?

La autenticación en varios factores.

Vamos a crear reglas de ciclo de vida, nos vamos a nuestro bucket/administración y creamos una nueva regla:



Realizar la transición de las versiones desactualizadas de los objetos entre las clases de almacenamiento

Elija transiciones para transferir las versiones no actuales de los objetos entre clases de almacenamiento en función del escenario de caso de uso y los requisitos de acceso de rendimiento. Estas transiciones comienzan a partir del momento en los objetos dejan de ser actuales y se aplican consecutivamente. [Más información](#)

Elegir transiciones de clase de almacenamiento

Estándar - Acceso ... ▼

Días tras los que los objetos dejan de ser actuales

30

Número de versiones más recientes que retener: *opcional*

12

Puede tener hasta 100 versiones. Todas las demás versiones no actuales se transferirán.

Eliminar

Agregar transición

Pongo 12 para que se “guarde” una por mes. Ahora crearemos una que las elimine:

Crear la regla del ciclo de vida. [Información](#)

Configuración de reglas de ciclo de vida

Nombre de la regla de ciclo de vida

borrar_versiones

Hasta 255 caracteres

Elegir un ámbito de regla

- ☐ Limitar el ámbito de esta regla mediante uno o varios filtros
- ☒ Aplicar a todos los objetos del bucket



Aplicar a todos los objetos del bucket

Si desea que la regla se aplique a objetos específicos, debe utilizar un filtro para identificar esos o Elija “Limitar el ámbito de esta regla mediante uno o varios filtros”. [Obtenga más información](#)

☒ Soy consciente de que esta regla se aplicará a todos los objetos del bucket.

Acciones de la regla del ciclo de vida

Elija las acciones que desea que realice esta regla. Se aplican tarifas por solicitud. [Obtenga más información](#) o consulte [lo Amazon S3](#).

- ☐ Transferir las versiones actuales de los objetos entre las clases de almacenamiento
- ☐ Transferir las versiones desactualizadas de los objetos entre las clases de almacenamiento
- ☐ Hacer que venzan las versiones actuales de los objetos
- ☒ Eliminar permanentemente las versiones no actuales de los objetos
- ☐ Eliminar los marcadores de eliminación de objetos vencidos o las cargas multipartes incompletas
- Estas acciones no se admiten cuando se filtra por etiquetas de objetos o tamaño de objeto.

Eliminar permanentemente las versiones no actuales de los objetos

Elija cuándo Amazon S3 elimina de forma permanente las versiones no actuales especificadas de los objetos. [Más información](#)

Días tras los que los objetos dejan de ser actuales

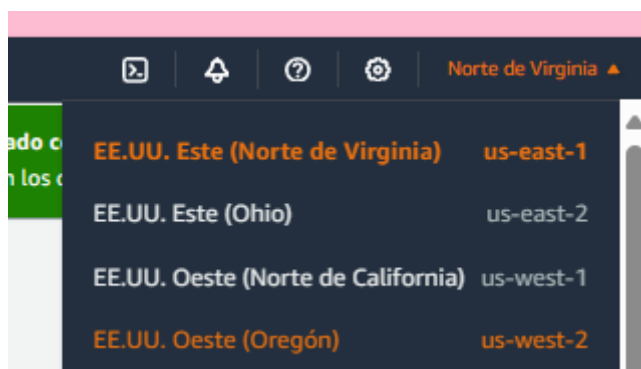
365

Número de versiones más recientes que retener: *opcional*

Número de versiones

Puede tener hasta 100 versiones. Todas las demás versiones no actuales se transferirán.

Vamos a habilitar la replicación entre regiones. Para ello debemos cambiarnos de región.



Aquí creamos un nuevo bucket:

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 buckets utilizados con S3 Express. Ofrecen un rendimiento más rápido de lectura y escritura.

Nombre del bucket **Información**

bucket_destinonicolasrr

El nombre del bucket debe ser único dentro del espacio de nombres global y seguir las reglas [reglas para la asignación de nombres de buckets](#).

Copiar la configuración del bucket existente: *opcional*
Solo se copia la configuración del bucket en los siguientes ajustes.

Elegir el bucket

Formato: <3-63 caracteres>

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 estos objetos puede especificarse mediante ACL.

⚠ Recomendamos desactivar las listas de control de acceso (ACL), a menos que necesite controlar el acceso a cada objeto individualmente o que el escritor del objeto sea el propietario de los datos.


Si necesita compartir datos con usuarios externos a la organización, considere usar una política de bucket en lugar de ACL para compartir datos con usuarios externos a la organización y la realización de auditorías.

Propiedad de objetos

☒ **Propietario del bucket preferido**
Si los nuevos objetos escritos en este bucket especifican la ACL preconfigurada bucket-owner-full-control, son propiedad del propietario del bucket. De lo contrario, son propiedad del escritor de los objetos.

- ☐ **Bloquear *todo* el acceso público**
Activar esta configuración equivale a activar las cuatro opciones que se describen a continuación.
- ☐ **Bloquear el acceso público a buckets y objetos con ACL**
S3 bloqueará los permisos de acceso público aplicados a objetos nuevos y existentes. No se aplicarán nuevas ACL de acceso público para buckets y objetos existentes.
- ☐ **Bloquear el acceso público a buckets y objetos con ACL (ACL)**
S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.
- ☐ **Bloquear el acceso público a buckets y objetos con políticas públicas nuevas**
S3 bloqueará las nuevas políticas de buckets y puntos de acceso. La configuración no afecta a las políticas ya existentes que permitan el acceso público.
- ☐ **Bloquear el acceso público y entre cuentas a bucket y puntos de acceso pública**
S3 ignorará el acceso público y entre cuentas en el caso de buckets y objetos.

Control de versiones de buckets

El control de versiones es una forma de mantener versiones para conservar, recuperar y restaurar versiones de objetos. Si se habilita el control de versiones, puede recuperarse con facilidad [información](#) 

Control de versiones de buckets

- ☐ Desactivar
- ☒ **Habilitar**

Es importante que estén en regiones diferentes:

	Nombre	Región de AWS
<input type="radio"/>	bucker-destinonicolasrr	EE. UU. Oeste (Oregón) us-west-2
<input type="radio"/>	c115383a2736356l6307911t1w647742234288-htmlbucket-q2v6b6yqimkw	EE. UU. Este (Norte de Virginia) us-east-1
<input type="radio"/>	nicolasrr-bucket	EE. UU. Este (Norte de Virginia) us-east-1

Entramos en esta ruta:

[Amazon S3](#) > [Buckets](#) > [nicolasrr-bucket](#) > [Reglas de replicación](#) > [Crear regla de replicación](#)

Crear regla de replicación [Información](#)

Y rellenamos:

Nombre de la regla de replicación

replica-entre-regiones

Hasta 255 caracteres. Para poder utilizar las métricas de CloudWatch, la regla de replicación solo debe contener caracteres en español.

Estado

Elija si la regla se habilitará o desactivará cuando se cree.

- ☒ **Habilitada**
- ☐ Deshabilitada

Bucket de origen

Nombre del bucket de origen

nicolasrr-bucket

Región de origen

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

Elegir un ámbito de regla

- ☐ Limitar el ámbito de esta regla mediante uno o varios filtros
- ☒ Aplicar a todos los objetos del bucket

Destino

Destino

Puede replicar objetos entre buckets de diferentes regiones de AWS (replicación entre regiones) o puede replicar objetos entre buckets en la misma región de AWS (replicación en la misma región). También puede especificar un bucket diferente para cada regla de la configuración. [Obtenga más información](#) o [consulte los precios de Amazon S3](#).

- ☒ Elegir un bucket de esta cuenta
- ☐ Especificar un bucket de otra cuenta

Nombre del bucket

Elija el bucket que recibirá los objetos replicados.

bucket-destinonicolasrr

Explorar S3

Región de destino

EE. UU. Oeste (Oregón) us-west-2

Rol de IAM

- ☐ Crear un nuevo rol
- ☒ Elija entre roles de IAM existentes
- ☐ Ingresar el ARN del rol de IAM

Rol de IAM

CafeRole

Y le damos a crear regla, si nos dice replicar ahora, le damos que no.

¿ves los objetos del bucket fuente en el bucket de destino?

No, le hemos dicho que no se replique.

Haremos un pequeño cambio en el index y lo volvemos a subir.

Objetos (1) Información

Copiar URI de S3

Copiar URL

Descargar

Abrir

Eliminar

Acciones ▼

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. Para obtener acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)


☒ Mostrar versiones

<input type="checkbox"/>	Nombre ▲	Tipo	ID de versión	Última modificación	Tamaño
<input type="checkbox"/>	index.html	html	yVc4j2MXRP sOow02A1P bp3KwSIux Gz.7	4 May 2024 1:07:00 PM CEST	




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. Para obtener acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

🔍 *Buscar objetos por prefijo*


☒ Mostrar versiones

<input type="checkbox"/>	Nombre	Tipo	ID de versión	Última modificación	Tamaño
<input type="checkbox"/>	 index.html	html	yVc4j2MXRP sOow02A1P bp3KwSIUx Gz.7	4 May 2024 1:07:00 PM CEST	1.0 KB

Vemos que en el bucket destino se replican los cambios.

<input type="checkbox"/>	 images/	Carpeta	-
<input type="checkbox"/>	 index.html	html	yVc4j2MXRPsOow02A1Pbp3 KwSIUxGz.7
<input type="checkbox"/>	 index.html	html	Dier.mAAasIAY35frIVsJ6ITWf mx4oyD

Vemos que en el destino aún se guarda:

<input type="checkbox"/>	Nombre	Tipo	ID de versión
<input type="checkbox"/>	 index.html	html	yVc4j2MXRPsOow02A1 Pbp3KwSIUxGz.7

(La ID de versión deben ser iguales)

¿la versión que acabas de eliminar de bucket fuente también se ha eliminado del bucket de destino?

No, no se ha eliminado.