

TALLER_AWS

NextDigital

En primer lugar crearemos el Bucket en S3.

IsardVDI - Iniciar se...

aws

Buscar

[Alt+S]

Estados Unidos (Norte de Virginia)

ID de cuenta: 4775-0080-8805

voclabs/user4809956-Yujian_Chen

Amazon S3

Buckets

Crear bucket

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-digital-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.

Propiedad del objeto

☒ **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.

CloudShell

Comentarios

© 2026, Amazon Web Services, Inc. o sus filiales.

Privacidad

Términos

Preferencias de cookies

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*

Puede usar etiquetas de bucket para analizar los permisos de un bucket, además de administrarlos y especificarlos. [Más información](#)

1 Puede usar las API `s3:ListTagsForResource`, `s3:TagResource` y `s3:UntagResource` para administrar las etiquetas en los buckets de uso general de S3 para el control de acceso, además de la asignación de costos y la organización de los recursos. Para garantizar una transición fluida, proporcione permisos para realizar las acciones `s3:ListTagsForResource`, `s3:TagResource` y `s3:UntagResource`. [Más información](#)

No hay etiquetas asociadas a este bucket.

[Agregar nueva etiqueta](#)

Puede agregar hasta 50 etiquetas.

Cifrado predeterminado [Información](#)

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

Tipo de cifrado [Información](#)

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](#).

- ☒ 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)

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](#)

Luego de haberlo creado, nos meteremos dentro del Bucket y cargaremos un archivo con extensión HTML. En mi caso subiré uno de ejemplo llamada TallerAWS.html que contiene la siguiente frase: Práctica final del taller de AWS. Ejemplo de sitio web estático.

IsardVDI - Iniciar se...

aws

Buscar

[Alt+S]

Estados Unidos (Norte de Virginia)

ID de cuenta: 4775-0080-8805
voclabs/user4809956=Yujian_Chen

Amazon S3 > Buckets > upm-next-digital-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 (1 total, 65.0 B)

Eliminar Agregar archivos Agregar carpeta

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

Buscar por nombre

<input checked="" type="checkbox"/>	Nombre	Carpeta	Tipo	Tamaño
<input checked="" type="checkbox"/>	TallerAWS.html	-	text/html	65.0 B

Destino

Información

Destino

[s3://upm-next-digital-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

Luego después haremos cambios en los permisos del Bucket para que tenga acceso todo el público y confirmaremos la acción y seguiremos en añadir una política bucket

proveniente de un pastebin que usamos en el propio taller.

IsardVDI - Iniciar se...

Buscar

[Alt+S]

Estados Unidos (Norte de Virginia)

ID de cuenta: 4775-0080-8805
voclabs/user4809956=Yujian_Chen

Amazon S3 > Buckets > upm-next-digital-bucket > Editar el bloqueo de acceso público (configuración del bucket)

Amazon S3

Buckets

Buckets de uso general

Buckets de directorio

Buckets de tablas

Buckets vectoriales

Seguridad y administración de acceso

Puntos de acceso

Puntos de acceso para FSx

Concesiones de acceso

Analizador de acceso de IAM

Información y administración de almacenamiento

Storage Lens

Operaciones por lotes

Configuración de la cuenta y la organización

AWS Marketplace para S3

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 concedan 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 existentes que concedan acceso público a buckets y objetos.

Editar el bloqueo de acceso público (configuración del bucket)

Actualizar la configuración de bloqueo de acceso público de este bucket afectará a este bucket y a todos los objetos que contiene. Esto puede provocar que algunos objetos se vuelvan públicos.

Para confirmar la configuración, ingrese **confirmar** en el campo.

confirmar

Cancelar Confirmar

Cancelar

Guardar cambios

aws

Buscar

[Alt+S]

Estados Unidos (Norte de Virginia)

ID de cuenta: 4775-0080-8805

voclabs/user4809956=Yujian_Chen

Amazon S3

Buckets

upm-next-digital-bucket

Editar la política del bucket

Amazon S3

▼ Buckets

Buckets de uso general

Buckets de directorio

Buckets de tablas

Buckets vectoriales

▼ Seguridad y administración de acceso

Puntos de acceso

Puntos de acceso para FSx

Concesiones de acceso

Analizador de acceso de IAM

▼ Información y administración de almacenamiento

Storage Lens

Operaciones por lotes

Configuración de la cuenta y la organización

► AWS Marketplace para S3

Editar la política del bucket

Información

Política de bucket

Ejemplos de políticas

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

ARN del bucket

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

Política

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

Editar instrucción

Seleccionar una instrucción

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

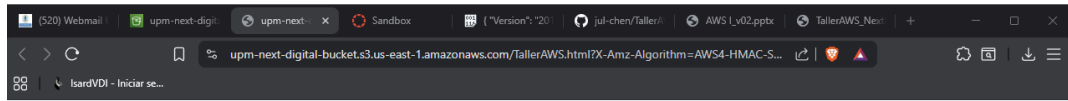
+ Agregar nueva instrucción

+ Agregar nueva instrucción

JSON

Ln 16, Col 1

Y por último editaremos para que pueda alojar sitios webs estáticos en S3



Práctica final del taller de AWS. Ejemplo de sitio web estático