



---

# PRACTICA FINAL TALLER AWS

---

SERVIR SITIO ESTATICO DESDE S3



JIADONG WANG

Para empezar, se creará un bucket en S3 como en las siguientes imágenes:

**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

practica\_final\_aws

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/perfil

**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 deshabilitada (recomendada)**  
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 generará 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 conceden 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 generará 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**

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**

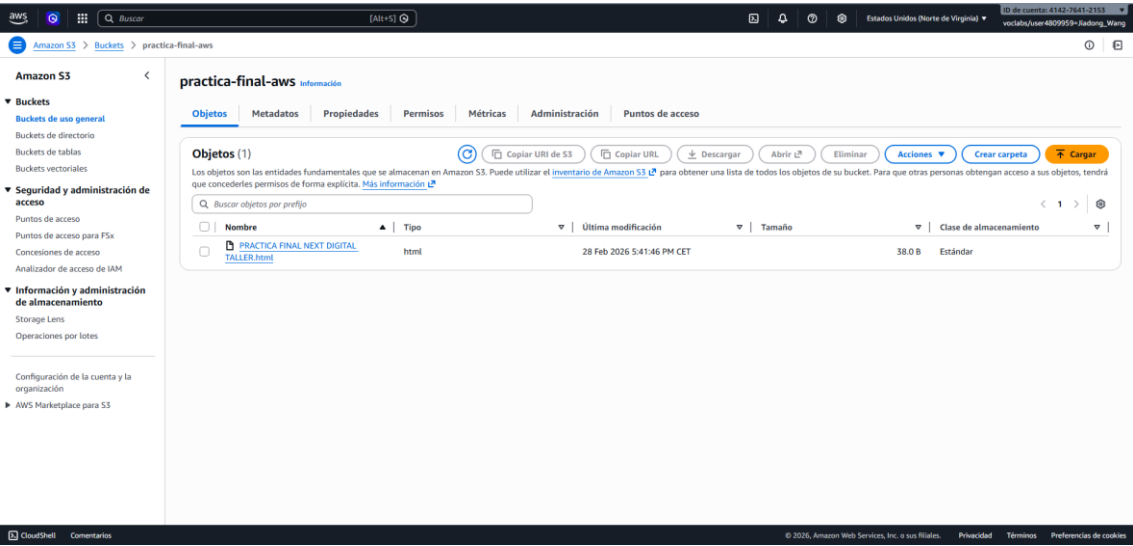
☒ **Habilitar**

**Configuración avanzada**

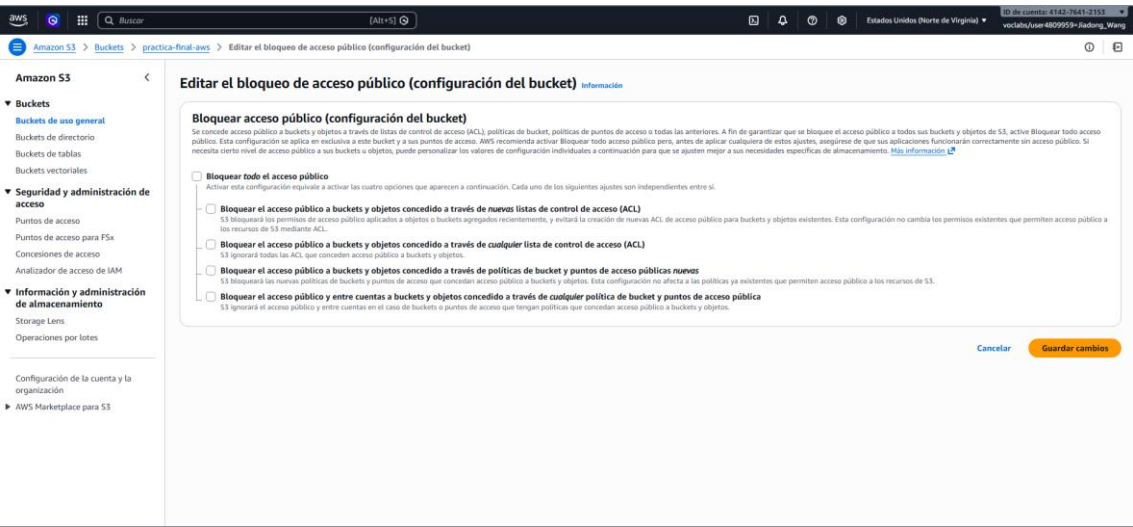
**1** Después de crear el bucket, puede cargar archivos y carpetas, y configurar ajustes adicionales en él.

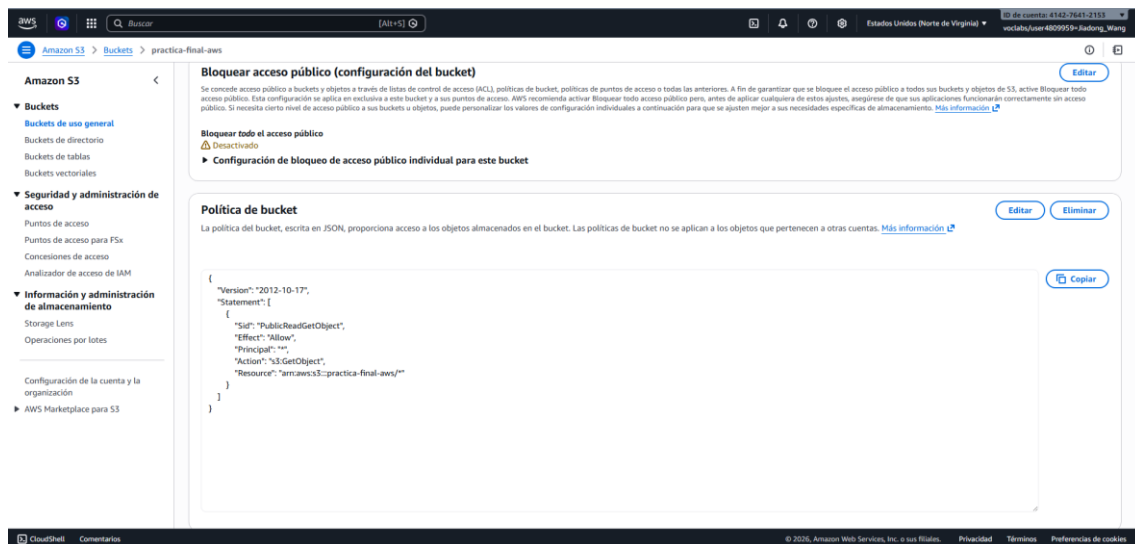
[Cancelar](#) [Crear bucket](#)

Cuando el bucket este creado, se procederá a cargar un archivo .html que servirá como página web estática:

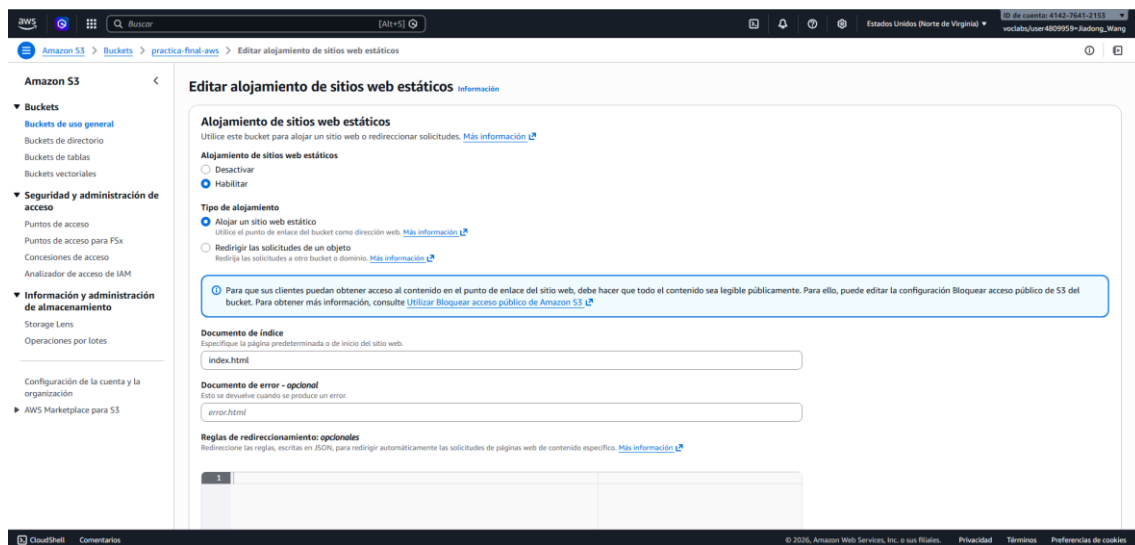


Una vez cargado el archivo, en el apartado de permisos del bucket, autorizaremos el acceso público y se añadirá una política al bucket creado:





Por último, en el apartado de las propiedades, habilitaremos la opción de alojamiento de sitios web estáticos:



Una vez hecho todo, accederemos con la URL del objeto que hemos cargado al principio y se nos abriría la página web estática:

