Amazon Simple Storage Service

Guía del usuario de la consola

Amazon Simple Storage Service: Guía del usuario de la consola

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y de ninguna manera que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Bienvenido a la guía del usuario de la consola de Amazon S3

Bienvenido a la guía del usuario de la consola de Amazon Simple Storage Service para la consola de Amazon Simple Storage Service (Amazon S3).

Amazon S3 proporciona almacenamiento prácticamente ilimitado en Internet. En esta guía se explica cómo administrar buckets, objetos y carpetas en Amazon S3 utilizando la consola de administración de AWS, una interfaz gráfica de usuario basada en navegador para interactuar con los servicios de AWS.

Para obtener información conceptual detallada acerca de cómo funciona Amazon S3, consulte ¿Qué es Amazon S3? en la guía del desarrollador de Amazon Simple Storage Service. La guía para desarrolladores también contiene información detallada acerca de las características de Amazon S3 y ejemplos de código para utilizarlas.

Temas

¿Cómo se cambia el idioma de la consola de administración de AWS?

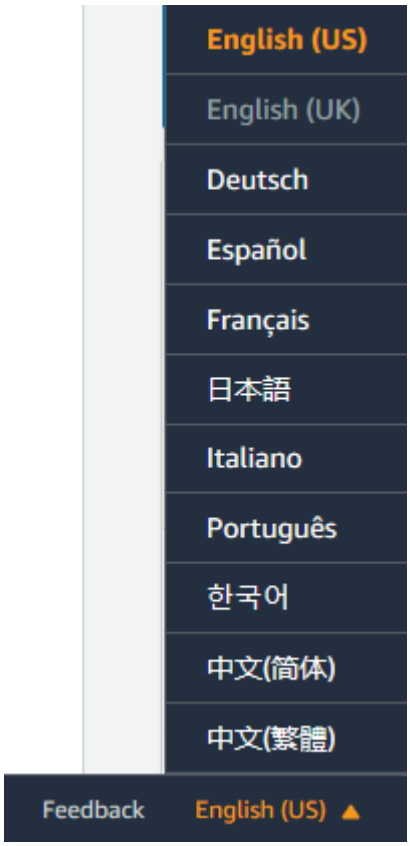
Puede cambiar el idioma en el que ver la consola de administración de AWS. Se admiten varios idiomas.

Para cambiar el idioma de la consola

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la parte izquierda de la barra de navegación inferior, elija el menú de idioma.

3. En el menú de idioma, elija el idioma que desee.

   Esto cambiará el idioma de toda la consola de administración de AWS.



Crear y configurar un bucket de S3

Para cargar sus datos (fotos, vídeos, documentos, etc.) en Amazon S3, primero tiene que crear un bucket de S3 en una de las regiones de AWS. Luego, puede cargar sus objetos de datos al bucket.

Todos los objetos almacenados en Amazon S3 residen en un bucket. Puede utilizar los buckets para agrupar objetos relacionados del mismo modo en que usa un directorio para agrupar archivos en un sistema de archivos.

Amazon S3 crea buckets en la región de AWS que usted especifica. Puede elegir cualquier región de AWS que esté geográficamente cerca suyo para optimizar la latencia, minimizar los costos o satisfacer los requisitos reglamentarios. Por ejemplo, si vive en Europa, puede resultarle más conveniente crear buckets en las regiones de UE (Irlanda) o UE (Fráncfort). Para ver una lista de las regiones de Amazon S3 AWS, consulte Regiones y puntos de enlace en la referencia general de Amazon Web Services.

No se le cobrará por la creación de un bucket. Solo se le cobrará por almacenar objetos en el bucket y por transferirlos fuera de este. Para obtener más información acerca de los precios, consulte Preguntas frecuentes sobre Amazon S3.

Los nombres de los buckets de Amazon S3 son únicos en todo el mundo, independientemente de la región de AWS en la que crea el bucket. Especifica el nombre en el momento en que crea el bucket. Para conocer directrices de nomenclatura de los buckets, consulte Restricciones y limitaciones de los buckets en la guía del desarrollador de Amazon Simple Storage Service.

En los siguientes temas se explica cómo utilizar la consola de Amazon S3 para crear, eliminar y administrar buckets.

Temas

¿Cómo se puede crear un bucket de S3?

Antes de poder cargar datos a Amazon S3, debe crear un bucket en una de las regiones de AWS para guardar los datos. Después de crear un bucket, puede cargar una cantidad ilimitada de objetos de datos en el bucket.

La cuenta de AWS que crea el bucket es su propietaria. De forma predeterminada, puede crear hasta 100 buckets en cada una de sus cuentas de AWS. Si necesita buckets adicionales, puede presentar una solicitud de aumento de la cuota de servicio para aumentar la cuota de buckets de la cuenta hasta

un máximo de 1000 buckets. Para obtener información acerca de cómo aumentar su cuota de buckets, consulte Cuotas del servicio de AWS en la referencia general de AWS.

Los buckets tienen propiedades de configuración, como la región geográfica, ajustes de acceso para los objetos del bucket y otros metadatos.

Para crear un bucket

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Elija Create bucket (Crear bucket).
3. En Bucket name (Nombre del bucket), escriba un nombre compatible con DNS para el bucket.

   El nombre del bucket debe:

   - Ser único en todo Amazon S3.
   - Tener entre 3 y 63 caracteres.
   - No contiene caracteres en mayúsculas.
   - Comenzar por una letra minúscula o un número.

   Una vez que haya creado el bucket, no podrá modificar su nombre. Para obtener información sobre cómo nombrar buckets, consulte Reglas para la nomenclatura de buckets en la guía del desarrollador de Amazon Simple Storage Service.

   > **Important**
   >
   > Evite incluir información confidencial, como números de cuenta, en el nombre del bucket. El nombre del bucket será visible en las URL que señalan a los objetos almacenados en él.

4. En Region (Región), elija la región de AWS donde desee que se encuentre el bucket.

   Puede seleccionar una región cercana para minimizar la latencia y los costos, así como para satisfacer los requisitos reglamentarios. Los objetos almacenados en una región nunca abandonarán esa región salvo que usted los transfiera de forma específica a otra. Para ver una lista de las regiones de Amazon S3 AWS, consulte Puntos de enlace del servicio de AWS en la referencia general de Amazon Web Services.

5. En Configuración del bucket para Block Public Access, elija la configuración de Block Public Access que desee aplicar al bucket.

   Le recomendamos que deje todas las configuraciones habilitadas a menos que sepa que necesita desactivar una o varias de ellas para su caso de uso, como alojar un sitio web público. La configuración de acceso público de bloqueo que habilite para el bucket también se habilitará para todos los puntos de acceso que cree en el bucket. Para obtener más información acerca del bloqueo de acceso público, consulte Usar Block Public Access de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

6. (Opcional) Si desea habilitar Bloqueo de objetos en S3, realice las siguientes acciones:

   a. Elija Configuración avanzada y lea el mensaje que aparece.

      > **Important**
      >
      > Solo se puede habilitar Bloqueo de objetos en S3 para un bucket cuando se crea. Si habilita Bloqueo de objetos para el bucket, no podrá deshabilitarlo más adelante. Al habilitar Bloqueo de objetos, también se habilita el control de versiones para el bucket. Después de habilitar Bloqueo de objetos para el bucket, debe configurar los valores de Bloqueo de objetos antes de proteger los objetos del bucket. Para obtener más información acerca de cómo configurar la protección para objetos, consulte ¿Cómo puedo bloquear un objeto de Amazon S3? (p. 37).

b. Si desea habilitar el bloqueo de objetos, escriba enable (habilitar) en el cuadro de texto y elija Confirm (Confirmar).

Para obtener más información acerca de la función Bloqueo de objetos en S3, consulte Bloqueo de objetos mediante Bloqueo de objetos en Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

7. Elija Create bucket (Crear bucket).

Más información

- ¿Cómo se elimina un bucket de S3? (p. 5)
- ¿Cómo se configuran permisos de buckets de ACL? (p. 71)

¿Cómo se elimina un bucket de S3?

Puede eliminar un bucket vacío y, si usa la consola de administración de AWS, puede eliminar un bucket que contenga objetos. Si elimina un bucket que contenga objetos, se eliminarán todos los objetos del bucket de forma permanente.

Al eliminar un bucket que tenga habilitado el control de versiones, todas las versiones de los objetos del bucket se eliminarán de forma permanente. Para obtener más información sobre versiones, consulte el tema sobre administración de objetos en un bucket con control de versiones activado en la guía del desarrollador de Amazon Simple Storage Service.

Antes de eliminar un bucket, tenga en cuenta lo siguiente:

- Los nombres de bucket son únicos. Si elimina un bucket, otro usuario de AWS podrá usar el nombre.
- Si elimina un bucket que contenga objetos, se eliminarán todos los objetos del bucket de forma permanente, incluidos los objetos que pasaron a la clase de almacenamiento `S3 Glacier`.
- Si el bucket aloja un sitio web estático y ha creado y configurado una zona hospedada de Amazon Route 53 como se describe en Creación y configuración de la zona hospedada de Amazon Route 53, debe limpiar la configuración de la zona hospedada de Route 53 que está relacionada con el bucket como se describe en Eliminación de la zona hospedada en Route 53.
- Si el bucket recibe datos de registro de Elastic Load Balancing (ELB), recomendamos que detenga el envío de registros de ELB al bucket antes de eliminarlo. Después de eliminar el bucket, si otro usuario crea un bucket con el mismo nombre, existe la posibilidad de que sus datos se registro se envíen a ese bucket. Para obtener información acerca de los registros de acceso de ELB, consulte Registros de acceso en la guía del usuario para balanceadores de carga clásicos y Registros de acceso en la guía del usuario para balanceadores de carga de aplicaciones.

Important

Si desea seguir utilizando el mismo nombre de bucket, no elimine el bucket. Le recomendamos que vacíe el bucket y lo conserve. Después de eliminar un bucket, el nombre se puede volver a utilizar, pero es posible que usted no pueda volver a utilizarlo por varias razones. Por ejemplo, puede que transcurra tiempo antes de que pueda volver a utilizar el nombre y puede que otras cuentas creen un bucket con ese nombre antes que usted.

Para eliminar un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. En la lista Buckets (Buckets), seleccione la opción situada junto al nombre del bucket que desea eliminar y, a continuación, elija Delete (Eliminar) en la parte superior de la página.
3. En la página Delete bucket (Eliminar bucket) confirme que desea eliminar el bucket introduciendo el nombre del bucket en el campo de texto y, a continuación, elija Delete bucket (Eliminar bucket).

   Note

   Si el bucket contiene objetos, vacíelo antes de eliminarlo seleccionando el vínculo empty bucket configuration (vaciar configuración de bucket) en la alerta de error This bucket is not empty (Este bucket no está vacío) y siguiendo las instrucciones de la página Empty bucket (Vaciar bucket). A continuación, vuelva a la página Delete bucket (Eliminar bucket) y elimine el bucket.

Más información

- ¿Cómo se puede vaciar un bucket de S3? (p. 6)
- Eliminación de objetos (p. 33)

¿Cómo se puede vaciar un bucket de S3?

Puede vaciar un bucket, lo que elimina todos los objetos del bucket sin eliminar el bucket. Al vaciar un bucket que tenga habilitado el control de versiones, todas las versiones de los objetos del bucket se eliminarán. Para obtener más información, consulte Administrar objetos en un bucket con control de versiones activado y Eliminar o vaciar un bucket en la guía del desarrollador de Amazon Simple Storage Service.

Para vaciar un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione la opción junto al nombre del bucket que desea vaciar y, a continuación, elija Empty (Vaciar).
3. En la página Empty bucket (Vaciar bucket), confirme que desea vaciar el bucket introduciendo permanently delete (eliminar de forma permanente) en el campo de texto y, a continuación, elija Empty (Vaciar).
4. (Opcional) Supervisar el progreso del proceso de vaciado del bucket en la página Empty bucket: Status (Vaciado del bucket: estado) .

   Warning

   Esta acción elimina todos los objetos del bucket. Espere a que finalice la acción de vaciado del bucket antes de agregar nuevos objetos. Es posible que se eliminen nuevos objetos si se agregan mientras la acción de vaciado del bucket está en curso.

¿Cómo se consultan las propiedades de un bucket de S3?

Puede ver y configurar las propiedades de un bucket de Amazon S3, incluidas las opciones para el control de versiones, las etiquetas, el cifrado predeterminado, el registro, las notificaciones y mucho más.

Para ver las propiedades para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket cuyas propiedades desea ver.
3. Seleccione Properties (Propiedades).
4. En la página Properties (Propiedades), puede configurar las siguientes propiedades para el bucket.

   - Bucket versioning (Control de versiones de bucket): el control de versiones le permite mantener varias versiones de un objeto en un bucket. De forma predeterminada, el control de versiones está deshabilitado para un nuevo bucket. Para obtener más información acerca de la habilitación del control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones para un bucket de S3?
   - Tags (Etiquetas): con la asignación de costos de AWS, puede utilizar etiquetas de bucket para registrar la facturación por el uso de un bucket. Una etiqueta es un par clave-valor que representa una etiqueta que podrá asignar a un bucket. Para añadir etiquetas, seleccione Tags (Etiquetas) y, a continuación, seleccione Add tag (Añadir etiqueta). Para obtener más información, consulte Uso de etiquetas de buckets de S3 de asignación de costos.
   - Default encryption (Cifrado predeterminado): la habilitación del cifrado predeterminado proporciona cifrado automático del lado del servidor. Amazon S3 cifra un objeto antes de guardarlo en un disco y descifra el objeto al descargarlo. Para obtener más información, consulte Cifrado predeterminado de Amazon S3 para los buckets de S3.
   - Server access logging (Registro de acceso del servidor): el registro de acceso del servidor brinda registros detallados para las solicitudes realizadas a su bucket. De forma predeterminada, Amazon S3 no recopila registros de acceso al servidor. Para obtener información acerca de cómo habilitar el registro de acceso del servidor, consulte ¿Cómo se puede habilitar el registro de acceso al servidor para un bucket de S3? (p. 10).
   - AWS CloudTrail data events (Eventos de datos de AWS CloudTrail) : utilice CloudTrail para registrar eventos de datos. De forma predeterminada, los registros de seguimiento no registran eventos de datos. Se aplican cargos adicionales a los eventos de datos. Para obtener más información, consulte Registro de eventos de datos para registros de seguimiento en la guía del usuario de AWS CloudTrail.
   - Event notifications (Notificaciones de eventos): puede habilitar ciertos eventos de bucket de Amazon S3 para enviar mensajes de notificación a un destino cuando se producen eventos. Para habilitar los eventos, seleccione Create event notification (Crear notificación de eventos) y luego especifique las configuraciones que desea utilizar. Para obtener más información, consulte Habilitación y configuración de notificaciones de eventos para un bucket de S3 (p. 19)
   - Transfer acceleration (Aceleración de transferencia): permite transferir archivos de forma rápida, fácil y segura entre su cliente y un bucket de S3 a larga distancia. Para obtener información acerca de cómo habilitar Transfer Acceleration, consulte ¿Cómo se puede habilitar Transfer Acceleration para un bucket de S3? (p. 21).
   - Object Lock (Bloqueo de objetos): use Bloqueo de objetos de S3 para evitar que se elimine o se sobrescriba un objeto durante un periodo de tiempo determinado o de manera indefinida. Para obtener más información, consulte Bloqueo de objetos mediante Bloqueo de objetos de S3.
   - Requester Pays (Pago por solicitante): puede habilitar el pago por solicitante de modo que el solicitante (en lugar del propietario del bucket) pague las solicitudes y transferencias de datos. Para obtener más información, consulte Buckets de pago por solicitante.
   - Static website hosting (Alojamiento de sitios web estáticos): puede alojar un sitio web estático en Amazon S3. Para habilitar el alojamiento de sitio web estático, seleccione Static website hosting (Alojamiento de sitios web estáticos) y luego especifique las configuraciones que desea utilizar. Para obtener más información, consulte ¿Cómo se puede configurar un bucket de S3 para que aloje sitios web estáticos? (p. 12)

¿Cómo habilito o suspendo el control de versiones en un bucket de S3?

El control de versiones le permite mantener varias versiones de un objeto en un bucket. En esta sección se describe cómo habilitar el control de versiones de un objeto para un bucket. Para obtener más información sobre compatibilidad de versiones en Amazon S3, consulte Versiones de objetos y Uso del control de versiones en la guía del desarrollador de Amazon Simple Storage Service.

Para habilitar o deshabilitar el control de versiones en un bucket de S3:

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea activar el control de versiones.
3. Seleccione Properties (Propiedades).
4. En Bucket Versioning (Versiones del bucket), elija Edit (Editar).
5. Elija Suspend (Suspender) o Enable (Habilitar) y, a continuación, elija Save changes (Guardar cambios).

   Note

   Puede utilizar la autenticación Multi-Factor Authentication (MFA) con el control de versiones. Cuando utiliza la MFA con el control de versiones, debe proporcionar las claves de acceso de su cuenta de AWS y un código válido del dispositivo MFA de la cuenta para eliminar de manera permanente una versión de un objeto o suspender o volver activar el control de versiones. Para utilizar la MFA con el control de versiones, habilite `MFA Delete`. No obstante, no puede activar `MFA Delete` al utilizar la consola de administración de AWS. Debe utilizar la API o la CLI de AWS. Para obtener más información, consulte Eliminación MFA.

¿Cómo puedo habilitar el cifrado predeterminado para un bucket de Amazon S3?

El cifrado predeterminado de Amazon S3 permite definir el comportamiento de cifrado predeterminado para un bucket de Amazon S3. Puede configurar el cifrado predeterminado en un bucket para que todos los objetos se cifren cuando se almacenen en el bucket. Los objetos se cifran utilizando el cifrado del lado del servidor con las claves administradas de Amazon S3 (SSE-S3) o las claves maestras del cliente (CMK) de AWS Key Management Service (AWS KMS).

Cuando usa el cifrado de lado servidor, Amazon S3 cifra un objeto antes de guardarlo en el disco de su centro de datos y lo descifra al descargarlo. Para obtener más información acerca de cómo proteger los datos mediante el cifrado de lado de servidor y la administración de claves de cifrado, consulte Proteger los datos con el cifrado del lado del servidor en la guía del desarrollador de Amazon Simple Storage Service.

El cifrado predeterminado funciona con todos los buckets de Amazon S3 nuevos y existentes. Sin el cifrado predeterminado, para cifrar todos los objetos almacenados en un bucket, debe incluir la información de cifrado con la solicitud de almacenamiento de cada objeto. Asimismo, debe configurar una política de bucket de Amazon S3 para rechazar las solicitudes de almacenamiento que no incluyan información de cifrado.

No se aplican cargos adicionales por usar el cifrado predeterminado de buckets de S3. Las solicitudes para configurar la característica de cifrado predeterminado generan cargos por solicitudes de Amazon S3 estándar. Para obtener información acerca de los precios, consulte Precios de Amazon S3. El

almacenamiento de CMK de SSE-KMS supone cargos de AWS KMS, los cuales se especifican en los precios de AWS KMS.

Para activar el cifrado predeterminado en un bucket de Amazon S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. Seleccione Properties (Propiedades).
4. En Default encryption (Cifrado predeterminado), elija Edit (Editar).
5. Para activar o desactivar el cifrado del lado del servidor, elija Enable (Habilitar) o Disable (Desactivar).
6. Para activar el cifrado del lado del servidor con una clave administrada por Amazon S3, en Encryption key type (Tipo de clave de cifrado), elija Amazon S3 key (SSE-S3) [Clave de Amazon S3 (SSE-S3)].

   Para obtener más información sobre cómo se usa el cifrado del lado del servidor de Amazon S3 para cifrar los datos, consulte el tema sobre protección de datos con clave de cifrado administradas por Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

   Important

   Es posible que necesite actualizar la política de bucket cuando habilite el cifrado predeterminado. Para obtener más información, consulte el tema sobre cómo cambiar a usar el cifrado predeterminado tras usar políticas de bucket para aplicar el cifrado en la guía del desarrollador de Amazon Simple Storage Service.
7. Para activar el cifrado del lado del servidor con CMK de AWS KMS, siga estos pasos:

   a. En Encryption key type (Tipo de clave de cifrado), elija la clave de AWS Key Management Service (SSE-KMS).

      Important

      Si utiliza la opción de AWS KMS para la configuración de cifrado predeterminado, se le aplicarán los límites de RPS (solicitudes por segundo) de AWS KMS. Para obtener más información acerca de los límites de AWS KMS y sobre cómo solicitar un aumento de los límites, consulte Límites de AWS KMS.

   b. Elija una de las siguientes opciones en AWS KMS key (Clave de AWS KMS):

      - AWS managed key (aws/s3) [Clave administrada de AWS (aws/s3)]
      - Elija entre sus claves maestras de KMS y elija su clave maestra de KMS.
      - Escriba el ARN de la clave maestra de KMS y escriba el ARN de la clave KMS de AWS.

      Important

      Solo puede utilizar las CMK de KMS activadas en la misma región de AWS que el bucket. Cuando elige Choose from your KMS master keys (Elegir entre las claves maestras de KMS), la consola de S3 solo muestra 100 CMK de KMS por región. Si tiene más de 100 CMK en la misma región, solo podrá ver las primeras 100 CMK en la consola de S3. Para utilizar una CMK de KMS que no aparece en la consola, elija ARN de KMS personalizado y escriba el ARN de la CMK de KMS.
      Cuando utilice una CMK de AWS KMS para el cifrado en el lado del servidor en Amazon S3, debe elegir una CMK simétrica. Amazon S3 solo admite CMK simétricos y no asimétricos. Para obtener más información, consulte Uso de claves simétricas y asimétricas en la guía para desarrolladores de AWS Key Management Service.

   Para obtener más información acerca de cómo crear una CMK de AWS KMS, consulte Creación de claves en la guía para desarrolladores de AWS Key Management Service. Para obtener más

información sobre cómo usar AWS KMS con Amazon S3, consulte el tema sobre cómo proteger datos con claves almacenadas en AWS KMS en la guía para desarrolladores de Amazon Simple Storage Service.

8. Elija Save changes.

Más información

- Cifrado predeterminado de Amazon S3 para los buckets de S3 en la guía del desarrollador de Amazon Simple Storage Service
- ¿Cómo se puede agregar cifrado a un objeto de S3? (p. 40)

¿Cómo se puede habilitar el registro de acceso al servidor para un bucket de S3?

En este tema se describe cómo activar el registro de acceso al servidor para un bucket de Amazon S3 con la consola de administración de AWS. Para obtener información acerca de cómo activar el registro mediante programación y detalles acerca de cómo se suministran los registros, consulte Registro de acceso del servidor en la guía de desarrollador de Amazon Simple Storage Service.

De forma predeterminada, Amazon Simple Storage Service (Amazon S3) no recopila registros de acceso al servidor. Cuando activa la actividad de registro, Amazon S3 envía los registros de acceso de un bucket de origen a un bucket de destino que usted selecciona. El bucket de destino debe estar en la misma región de AWS que el bucket de origen y no debe tener una configuración de periodo de retención predeterminada.

El registro de acceso al servidor brinda registros detallados para las solicitudes realizadas a un bucket de S3. Los registros de acceso al servidor resultan útiles para muchas aplicaciones. Por ejemplo, la información del registro de acceso puede ser útil en auditorías de acceso y seguridad. También puede ayudarle a conocer mejor su base de clientes y entender su factura de Amazon S3.

Una entrada de registro de acceso incluye detalles de las solicitudes realizadas a un bucket. Esta información puede incluir el tipo de solicitud, los recursos especificados en la solicitud y la hora y la fecha en que se procesó la solicitud. Para obtener más información, consulte el tema sobre formato del registro de acceso al servidor en la guía del desarrollador de Amazon Simple Storage Service.

> **Important**
>
> Habilitar el registro de acceso al servidor en un bucket de Amazon S3 ni incurre en ningún cargo adicional. Sin embargo, los archivos de registro que recibe del sistema acumularán los cargos usuales de almacenamiento. (Puede eliminar los registros en cualquier momento). No contemplamos los cargos de transferencia de datos por la entrega de los archivos de registro, pero sí aplicamos el cargo de la tasa normal de transferencia de datos por obtener acceso a los archivos de registro.

Para habilitar el registro de acceso al servidor para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea activar el registro de acceso al servidor.
3. Seleccione Properties (Propiedades).
4. En la sección Server access logging (Registro de acceso al servidor), elija Edit (Editar).

5. En Server access logging (Registro de acceso al servidor), seleccione Enable (Activar). En Target bucket (Bucket de destino), seleccione el nombre del bucket que recibirá los objetos de entrada en el registro. El bucket de destino debe estar en la misma región que el bucket de origen y no debe tener una configuración de periodo de retención predeterminada.
6. Elija Save changes.

   Puede ver los registros en el bucket de destino. Después de habilitar el registro de acceso al servidor, la entrega de los registros al bucket de destino puede tardar unos horas. Para obtener más información acerca de cómo y cuándo se suministran registros, consulte Registros de acceso al servidor en la guía del desarrollador de Amazon Simple Storage Service.

Más información

¿Cómo se consultan las propiedades de un bucket de S3? (p. 6)

¿Cómo se puede habilitar el registro en el nivel de objeto de un bucket de S3 con eventos de datos de AWS CloudTrail?

En esta sección se describe cómo habilitar un registro de seguimiento de AWS CloudTrail para registrar eventos de datos para objetos en un bucket de S3 utilizando la consola de Amazon S3. CloudTrail permite que se registren operaciones de API en el nivel de objetos de Amazon S3 como, por ejemplo, `GetObject`, `DeleteObject` y `PutObject`. Estos eventos se denominan eventos de datos. De forma predeterminada, los registros de seguimiento de AWS CloudTrail no registran eventos de datos, pero pueden configurarse para que registren eventos de datos de los buckets de S3 que usted especifique o para que registren eventos de datos de todos los buckets de Amazon S3 incluidos en la cuenta de AWS. Para obtener más información, consulte este artículo sobre el registro de llamadas a la API de Amazon S3 con AWS CloudTrail. CloudTrail no rellena eventos de datos en el historial de eventos de CloudTrail. Además, no todas las acciones de nivel de bucket se rellenan en el historial de eventos de CloudTrail. Para obtener más información, consulte Uso de patrones de filtro de Amazon CloudWatch Logs y Amazon Athena para consultar los registros de CloudTrail.

Para configurar un registro de seguimiento para registrar eventos de datos para un bucket de S3, puede utilizar la consola de AWS CloudTrail o la consola de Amazon S3. En caso de que esté configurando un registro de seguimiento para registrar eventos de datos para todos los buckets de Amazon S3 en su cuenta de AWS, es más fácil utilizar la consola de CloudTrail. Para obtener más información sobre el uso de la consola de CloudTrail para configurar un registro de seguimiento para registrar eventos de datos de S3, consulte Eventos de datos en la guía del usuario de AWS CloudTrail.

> **Important**
>
> Se aplican cargos adicionales a los eventos de datos. Para obtener más información, consulte Precios de AWS CloudTrail.

El siguiente procedimiento muestra cómo utilizar la consola de Amazon S3 para habilitar un registro de seguimiento de CloudTrail para registrar eventos de datos para un bucket de S3.

Para habilitar el registro de eventos de datos de CloudTrail para objetos en un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket.
3. Seleccione Properties (Propiedades).

4. En AWS CloudTrail data events (Eventos de datos de AWS CloudTrail), seleccione Configure in CloudTrail (Configurar en CloudTrail). Para obtener información acerca de cómo crear registros de seguimiento en la consola de CloudTrail, consulte Creación de un registro de seguimiento con la consola en la guía del usuario de AWS CloudTrail.
5. Para deshabilitar el registro de nivel de objeto para el bucket, debe acceder a la consola de CloudTrail y quitar el nombre del bucket de Data events (Eventos de datos) del registro de seguimiento.

   Note

   Si utiliza la consola de CloudTrail o la consola de Amazon S3 para configurar un registro de seguimiento para registrar eventos de datos de registro para un bucket de S3, la consola de Amazon S3 muestra que los registros de nivel de objeto están habilitados para el bucket.

Para obtener más información sobre la habilitación de registro de nivel de objeto al crear un bucket de S3, consulte ¿Cómo se puede crear un bucket de S3? (p. 3).

Más información

- ¿Cómo se consultan las propiedades de un bucket de S3? (p. 6)
- Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail en la guía del desarrollador de Amazon Simple Storage Service
- Trabajar con archivos de registro de CloudTrail en la guía del usuario de AWS CloudTrail

¿Cómo se puede configurar un bucket de S3 para que aloje sitios web estáticos?

Puede alojar un sitio web estático en Amazon S3. En un sitio web estático, cada página web incluye contenido estático. Un sitio web también puede contener scripts del lado del cliente. Por el contrario, un sitio web dinámico depende del procesamiento en el lado del servidor, incluidos los scripts del lado del servidor, como en PHP, JSP o ASP.NET. Amazon S3 no admite scripts del lado del servidor.

Puede utilizar los siguientes procedimientos rápidos para configurar un bucket de S3 para utilizarlo para alojar sitios web en la consola de Amazon S3. Para obtener más información, consulte Alojamiento de un sitio web estático en Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service Para obtener información sobre cómo configurar un sitio web estático con un dominio personalizado, consulte Configuración de un sitio web estático utilizando un dominio personalizado registrado con Route 53 en la guía del desarrollador de Amazon Simple Storage.

Temas

Paso 1: Configurar un bucket para que aloje sitios web estáticos

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. En la lista Buckets, elija el nombre del bucket que desea utilizar para alojar un sitio web estático.
3. Seleccione Properties (Propiedades).
4. Elija Static website hosting (Alojamiento de sitios web estáticos), elija Edit (Editar).
5. Elija Use this bucket to host a website (Usar este bucket para alojar un sitio web).
6. En Static website hosting (Alojamiento de sitios web estáticos), elija Enable (Habilitar).
7. En Index Document (Documento de índice), escriba el nombre de archivo del documento de índice, normalmente `index.html`.

   El nombre del documento de índice distingue entre mayúsculas y minúsculas y debe coincidir exactamente con el nombre del archivo del documento de índice HTML que tiene previsto cargar en el bucket de S3. Al configurar un bucket para el alojamiento de sitios web, debe especificar un documento de índice. Amazon S3 devuelve este documento de índice cuando se reciben solicitudes en el dominio raíz o en cualquiera de las subcarpetas. Para obtener más información, consulte Configuración de un documento de índice en la guía del desarrollador de Amazon Simple Storage Service.
8. (Opcional) Si desea proporcionar su propio documento de error personalizado para los errores de clase 4XX, en Error Document (Documento de error), introduzca el nombre de archivo del documento de error personalizado.

   El nombre del documento de error distingue entre mayúsculas y minúsculas y debe coincidir exactamente con el nombre del archivo del documento de error HTML que tiene previsto cargar en el bucket de S3. Si no especifica un documento de error personalizado y se produce un error, Amazon S3 devuelve un documento de error HTML predeterminado. Para obtener más información, consulte Configuración de un documento de error personalizado en la guía del desarrollador de Amazon Simple Storage Service.
9. (Opcional) Si desea especificar reglas de redireccionamiento avanzadas, en Redirection rules (Reglas de redireccionamiento), especifique XML para describir las reglas.

   Por ejemplo, puede dirigir condicionalmente las solicitudes según nombres de clave de objeto o prefijos específicos en la solicitud. Para obtener más información, consulte Configurar redireccionamientos condicionales avanzados en la guía del desarrollador de Amazon Simple Storage Service.
10. Elija Save changes.

    Amazon S3 permite activar el alojamiento de sitios web estáticos para su bucket. En la parte inferior de la página, en Static website hosting (Alojamiento de sitios web estáticos), verá el punto de enlace del sitio web para su bucket.
11. Cargue el documento de índice en el bucket.

    Para ver instrucciones paso a paso acerca de cómo cargar un objeto en un bucket de S3, consulte Carga de archivos con la función apuntar y hacer clic (p. 31).
12. Cargue otros archivos en su sitio web, incluidos los documentos de error personalizados opcionales.

En la siguiente sección se van a establecer los permisos necesarios para acceder a su bucket como un sitio web estático.

Paso 2: Editar la configuración de bloqueo de acceso público en S3

De forma predeterminada, Amazon S3 bloquea el acceso público a su cuenta y sus buckets. Si desea utilizar un bucket para alojar un sitio web estático, puede utilizar estos pasos para editar la configuración de bloqueo de acceso público.

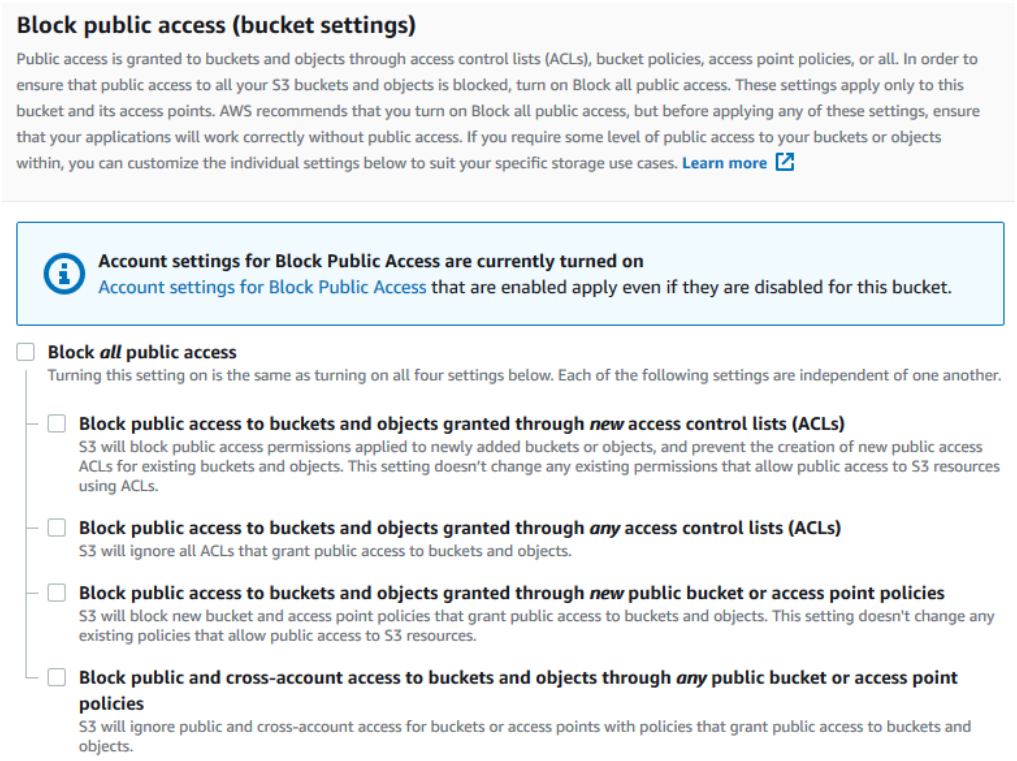
Warning

Antes de completar este paso, revise Usar Block Public Access de Amazon S3 para asegurarse de que comprende y acepta los riesgos que implica permitir el acceso público. Cuando desactiva la configuración de acceso público de bloqueo para que el bucket sea público, cualquier usuario de Internet puede acceder al bucket. Le recomendamos que bloquee todo el acceso público a sus buckets.

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. Elija el nombre del bucket que ha configurado como sitio web estático.
3. Elija Permissions.
4. En Block public access (bucket settings) (Bloqueo de acceso público [configuración de bucket]), elija Edit (Editar).
5. Desactive Block all public access (Bloquear todo el acceso público) y elija Save changes (Guardar cambios).

   Warning

   Antes de completar este paso, revise Usar Block Public Access de Amazon S3 para asegurarse de que comprende y acepta los riesgos que implica permitir el acceso público. Cuando desactiva la configuración de acceso público de bloqueo para que el bucket sea público, cualquier usuario de Internet puede acceder al bucket. Le recomendamos que bloquee todo el acceso público a sus buckets.



Amazon S3 desactiva la configuración del bloqueo de acceso público para su bucket. Para crear un sitio web público y estático, es posible que también tenga que editar la configuración del bloqueo de acceso público para su cuenta antes de agregar una política de bucket. Si la configuración de cuenta para el bloqueo de acceso público está activada actualmente, verá una nota en Block public access (bucket settings) [Bloqueo de acceso público (configuración de bucket)].

Paso 3: Agregar una política de bucket

Después de editar la configuración de acceso público de bloques de S3, debe agregar una política de bucket para garantizar el acceso de lectura público a su bucket. Cuando concede permiso de lectura público, cualquier persona de Internet puede acceder a su bucket.

> **Important**
>
> La política que se muestra a continuación es solo un ejemplo y permite acceso completo al contenido del bucket. Antes de continuar con este paso, revise ¿Cómo puedo proteger los archivos en mi bucket de Amazon S3? para asegurarse de que comprende las prácticas recomendadas para proteger los archivos en el bucket de S3 y los riesgos que implica la concesión de acceso público.

1. En Buckets, elija el nombre del bucket.
2. Elija Permissions.
3. En Bucket Policy (Política de bucket), elija Edit (Editar).
4. Para conceder acceso público de lectura a su sitio web, copie la siguiente política de bucket y péguela en el Bucket policy editor (Editor de políticas de bucket).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::example.com/*"
            ]
        }
    ]
}
```

5. Actualice el valor de `Resource` para el nombre de su bucket.

   En la política de bucket de ejemplo anterior, *example.com* es el nombre del bucket. Para utilizar esta política de bucket con su propio bucket, debe actualizar este nombre para que coincida con su nombre de bucket.
6. Elija Save changes.

   Aparecerá un mensaje que indicará que la política de bucket se ha agregado correctamente.

   Si ve un error que indica `Policy has invalid resource`, confirme que el nombre del bucket en la política del bucket coincide con el nombre de su bucket. Para obtener información acerca de cómo agregar una política de bucket, consulte ¿Cómo añado una política de bucket de S3?

   Si recibe un mensaje de error y no puede guardar la política de bucket, compruebe la configuración del bloqueo de acceso público para la cuenta y el bucket para confirmar que permite acceso público al bucket.

Después de editar la configuración de acceso público de bloques de S3, debe agregar una política de bucket para garantizar el acceso de lectura público a su bucket. Cuando concede permiso de lectura público, cualquier persona de Internet puede acceder a su bucket.

Important

La política que se muestra a continuación es solo un ejemplo y permite acceso completo al contenido del bucket. Antes de continuar con este paso, revise ¿Cómo puedo proteger los archivos en mi bucket de Amazon S3? para asegurarse de que comprende las prácticas recomendadas para proteger los archivos en el bucket de S3 y los riesgos que implica la concesión de acceso público.

Paso 4: Probar el punto de enlace del sitio web

Cuando configure el bucket como un sitio web estático y establezca los permisos correspondientes podrá acceder al sitio web a través de un punto de enlace de sitio web de Amazon S3. Para obtener más información, consulte Puntos de enlace de sitio web en la guía del desarrollador de Amazon Simple Storage Service. Para ver una lista completa de los puntos de enlace del sitio web de Amazon S3, consulte Puntos de enlace de sitio web de Amazon S3 en Referencia general de Amazon Web Services.

1. En Buckets, elija el nombre del bucket.
2. Seleccione Properties (Propiedades).
3. En la parte inferior de la página, en Static website hosting (Alojamiento de sitios web estáticos), elija el punto de enlace del sitio web del bucket.

   El documento de índice se abre en una ventana independiente del explorador.

¿Cómo se pueden redirigir solicitudes destinadas a un sitio web alojado en un bucket de S3 a otro host?

Para obtener información más detallada acerca de cómo configurar una redirección en Amazon S3, consulte Configuración de una redirección de página weben la guía del desarrollador de Amazon Simple Storage Service.

Puede redirigir todas las solicitudes de un punto de enlace de sitio web de un bucket a otro host. Si redirige todas las solicitudes, las solicitudes realizadas al punto de enlace del sitio web se redirigirán al nombre del host especificado.

Por ejemplo, si su dominio raíz es `example.com`, y desea enviar solicitudes para `http://example.com` y para `http://www.example.com`, puede crear dos buckets denominados `example.com` y `www.example.com`. A continuación, mantenga el contenido del bucket `example.com` y configure el otro bucket `www.example.com` para redirigir todas las solicitudes al bucket `example.com`. Para obtener más información, consulte Configuración de un sitio web estático mediante un nombre de dominio personalizado.

Para redirigir solicitudes para un punto de enlace de sitio web del bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En Buckets (Buckets), elija el nombre del bucket del que desea que procedan las solicitudes redirigidas (por ejemplo, `www.example.com`).
3. Seleccione Properties (Propiedades).
4. Elija Static website hosting (Alojamiento de sitios web estáticos), elija Edit (Editar).
5. Elija Redirect requests for an object (Redirigir solicitudes de un objeto).
6. En el cuadro Host name (Nombre de host) , escriba el punto de enlace de sitio web para el bucket o el dominio personalizado.

Por ejemplo, si redirigiera las solicitudes a una dirección de dominio raíz, escribiría **`example.com`**.

7. En Protocol (Protocolo), elija el protocolo para las solicitudes redirigidas (none (ninguno),http o https).

   Si no especifica un protocolo, la opción predeterminada es none (ninguno).
8. Elija Save changes.

Configuraciones avanzadas de las propiedades de un bucket de S3

En esta sección se describe cómo configurar opciones avanzadas para las propiedades del bucket de S3 para la replicación de objetos, la notificación de eventos y Transfer Acceleration.

Temas

Establecimiento de un destino en el que recibir las notificaciones de eventos de Amazon S3

Antes de poder habilitar las notificaciones de eventos para su bucket, debe configurar uno de los siguientes tipos de destinos.

Tipos de destino

Tema de Amazon SNS

Amazon Simple Notification Service (Amazon SNS) es un servicio web que coordina y gestiona la entrega o el envío de mensajes a los puntos de enlace o clientes suscritos. Puede usar la consola de Amazon S3 para crear un tema de Amazon SNS al que enviar sus notificaciones. El tema de Amazon SNS debe estar en la misma región que su bucket de Amazon S3. Para obtener información acerca de cómo crear un tema de Amazon SNS, consulte Introducción en la guía para desarrolladores de Amazon Simple Notification Service y en las preguntas frecuentes de SNS.

Antes de poder usar el tema de Amazon SNS que cree como destino de notificación de eventos, necesita lo siguiente:

- El nombre de recurso de Amazon (ARN) para el tema de Amazon SNS.
- Una suscripción válida al tema de Amazon SNS (los suscriptores del tema reciben una notificación cuando se publica un mensaje en su tema de Amazon SNS).
- Una política de permisos que establezca en la consola de Amazon SNS (según se muestra en el siguiente ejemplo).

```
{
  "Version":"2012-10-17",
```

```
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource":"arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Cola de Amazon SQS

Amazon Simple Queue Service (Amazon SQS) es una cola hospedada de confianza y escalable diseñada para almacenar mensajes mientras viajan de un equipo a otro. Puede usar la consola de Amazon SQS para crear una cola de Amazon SQS a la que enviar sus notificaciones. La cola de Amazon SQS debe estar en la misma región que su bucket de Amazon S3. Para obtener información acerca de cómo crear una cola de Amazon SQS, consulte Qué es Amazon Simple Queue Service e Introducción a Amazon SQS en la guía para desarrolladores de Amazon Simple Queue Service.

Antes de poder usar la cola de Amazon SQS como destino de notificación de eventos, necesita lo siguiente:

- El nombre de recurso de Amazon (ARN) para el tema de Amazon SQS.
- Una política de permisos que establezca en la consola de Amazon SQS (según se muestra en el siguiente ejemplo).

```
{
  "Version":"2012-10-17",
  "Id": "__example_policy_ID",
  "Statement":[
    {
      "Sid": "example-statement-ID",
      "Effect":"Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource":"arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
        "aws:SourceArn": "arn:aws:s3:::bucket-name"
         }
       }
     }
   ]
}
```

Lambda function

Puede utilizar la consola de AWS Lambda para crear una función Lambda que utilice la infraestructura de AWS para ejecutar el código en su nombre. La función de Lambda debe estar en la misma región que su bucket de S3. También debe tener el nombre o el ARN de una función Lambda para configurar la función Lambda como destino de notificación de eventos.

Warning

Si la notificación termina escribiendo en el bucket que desencadena la notificación, esto podría provocar un bucle de ejecución. Por ejemplo, si el bucket activa una función de Lambda cada vez que se carga un objeto y la función carga un objeto en el bucket, la función se activa indirectamente a sí misma. Para evitarlo, utilice dos buckets o configure el desencadenador para que solo se aplique a un prefijo que se utiliza para los objetos entrantes.
Para obtener más información y un ejemplo del uso de notificaciones de Amazon S3 con AWS Lambda, consulte Uso de AWS Lambda con Amazon S3 en la guía para desarrolladores de AWS Lambda.

Para obtener más información acerca de cómo conceder a Amazon S3 los permisos necesarios para publicar notificaciones de eventos en un destino, consulte Concesión de permisos para publicar mensajes de notificación de eventos a un destino en la guía del desarrollador de Amazon S3.

Habilitación y configuración de notificaciones de eventos para un bucket de S3

Puede habilitar ciertos eventos de Amazon S3 para enviar un mensaje de notificación a un destino cuando se producen eventos. En esta sección se explica cómo usar la consola de Amazon S3 para habilitar la notificación de eventos. Para obtener información acerca del uso de notificaciones de eventos con AWS SDK y las API de REST de Amazon S3, consulte Configuración de notificaciones de eventos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Temas

Tipos de notificación de eventos

Al configurar notificaciones de eventos para un bucket, debe especificar el tipo de eventos para los que desea recibir notificaciones. Para obtener una lista completa de tipos de eventos, consulte la sección Tipos de eventos admitidos en la guía del desarrollador de Amazon Simple Storage Service.

En la consola de Amazon S3, tiene las siguientes opciones para configurar notificaciones de eventos. Puede elegir una sola opción o varias.

- Creación de objetos
  - All object create events (Todos los eventos de creación de objetos): recibirá una notificación cuando cualquiera de las siguientes acciones de creación de objetos cree un objeto en el bucket: Put (Colocar), Post (Publicar), Copy (Copiar) y Multipart upload completed (Carga multiparte completada).
  - Put (Colocar), Post (Publicar), Copy (Copiar) y Multipart upload completed (Carga multiparte completada): recibirá una notificación sobre una de estas acciones de creación de objetos.
- Eliminación de objetos
  - All object delete events (Todos los eventos de eliminación de objetos): recibirá una notificación cada vez que se elimine un objeto del bucket.
  - Delete marker created (Marcador de eliminación creado): recibirá una notificación cuando se cree un marcador de eliminación en un objeto con control de versiones.

    Para obtener información sobre cómo eliminar objetos con control de versiones, consulte Eliminación de versiones de objetos. Para obtener información sobre control de versiones de objetos, consulte Control de versiones de objetos y Uso del control de versiones.
- Restauración de objetos desde la clase de almacenamiento de S3 Glacier o S3 Glacier Deep Archive

  - Restore initiated (Restauración iniciada): recibirá una notificación sobre el inicio de la restauración de objetos.
  - Restore completed (Restauración completada): recibirá una notificación sobre la finalización de la restauración de objetos.
- Eventos de pérdida de objeto de almacenamiento de redundancia reducida (RRS)
  - Object in RSS Lost (Objeto perdido en RRS): recibirá una notificación si se pierde un objeto de la clase de almacenamiento RRS.
- Objetos aptos para replicación mediante el control de tiempo de replicación de Amazon S3
  - Replication time missed threshold (Umbral de tiempo de replicación no superado): recibirá una notificación de que el objeto supera el umbral de replicación de 15 minutos.
  - Replication time completed after threshold (Tiempo de replicación completado después del umbral): recibirá una notificación de que el objeto se ha replicado después del umbral de replicación de 15 minutos.
  - Replication time not tracked (Tiempo de replicación sin seguimiento): recibirá una notificación de que a un objeto que cumplía los requisitos para la replicación ya no se le realiza un seguimiento con métricas de replicación.
  - Replication time failed (Error en el tiempo de replicación): recibirá una notificación de que un objeto no se ha podido replicar.

    Note

    Cuando elimina el último objeto de una carpeta, Amazon S3 puede generar un evento de creación de objeto. Cuando hay varios objetos con el mismo prefijo con una barra inclinada al final (/) como parte del nombre, esos objetos se muestran como parte de una carpeta en la consola de Amazon S3. El nombre de la carpeta se forma a partir de los caracteres que preceden a la barra inclinada al final (/).
    Cuando elimina todos los objetos incluidos en esa carpeta, no hay un objeto real disponible que represente la carpeta vacía. En tales circunstancias, la consola de Amazon S3 crea un objeto de cero bytes para representar la carpeta. Si habilitó la notificación de eventos para la creación de objetos, la acción de creación de objetos de cero bytes que ejecuta la consola desencadena un evento de creación de objeto.
    La consola de Amazon S3 muestra una carpeta en las siguientes circunstancias:

    - Cuando un objeto de cero bytes tiene una barra diagonal (/) al final del nombre. En este caso, hay un objeto real de Amazon S3 de 0 bytes que representa una carpeta.
    - Si el objeto tiene una barra diagonal (/) dentro de su nombre. En este caso, no hay un objeto real que represente la carpeta.

Habilitar y configurar notificaciones de eventos

Antes de poder habilitar las notificaciones de eventos para su bucket, debe configurar uno de estos tipos de destinos. Para obtener más información, consulte Establecimiento de un destino en el que recibir las notificaciones de eventos de Amazon S3 (p. 17)

Para habilitar y configurar notificaciones de eventos para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket para el que desea habilitar eventos.
3. Acceda a la sección Notificaciones de eventos y elija Creación de notificación de eventos.
4. En la sección Configuración general, especifique el nombre del evento descriptivo para la notificación de eventos. Opcionalmente, también puede especificar un prefijo y un sufijo para limitar las notificaciones a objetos con claves que terminen en los caracteres especificados.

a. Introduzca una descripción para el nombre del evento.

   Si no introduce un nombre, se generará un identificador único global (GUID) y se utilizará para el nombre.

b. Para filtrar opcionalmente las notificaciones de eventos por prefijo, introduzca un prefijo.

   Por ejemplo, puede configurar un filtro de prefijo para recibir notificaciones solo cuando se añadan archivos a una carpeta específica (por ejemplo, `images/`).

c. Para filtrar opcionalmente las notificaciones de eventos por sufijo, introduzca un sufijo.

   Para obtener más información, consulte Configuración de notificaciones con filtrado de nombre de clave de objeto.

5. En la sección Tipos de evento, seleccione uno o varios tipos de eventos para los que desee recibir notificaciones.

   Para obtener una lista de los tipos de eventos, consulte Tipos de notificación de eventos (p. 19).

6. En la sección Destino, elija el destino de notificación de eventos.

   Note

   Antes de poder publicar notificaciones de eventos, debe conceder a la entidad principal de Amazon S3 los permisos necesarios para llamar a la API correspondiente para publicar notificaciones en una función Lambda, un tema SNS o una cola SQS.

   a. Seleccione el tipo de destino: Función Lambda, Tema SNS o Cola SQS.
   b. Después de elegir el tipo de destino, elija una función, un tema o una cola de la lista desplegable.
   c. Como alternativa, si prefiere especificar un nombre de recurso de Amazon (ARN), seleccione Enter ARN (Introducir ARN) e introduzca el ARN.

   Para obtener más información, consulte Establecimiento de un destino en el que recibir las notificaciones de eventos de Amazon S3 (p. 17).

7. Elija Save changes (Guardar cambios) y Amazon S3 enviará un mensaje de prueba al destino de notificación de eventos.

Para obtener más información, consulte Configuración de notificaciones de eventos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

¿Cómo se puede habilitar Transfer Acceleration para un bucket de S3?

La aceleración de transferencia de Amazon Simple Storage Service (Amazon S3) permite transferir archivos de forma rápida, fácil y segura entre su cliente y un bucket de S3 a larga distancia. En este tema se describe cómo habilitar Amazon S3 Transfer Acceleration para un bucket. Para obtener más información, consulte el tema sobre la aceleración de la transferencia de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Note

Si desea comparar velocidades de subida aceleradas y no aceleradas, abra la herramienta de comparación de velocidad de Amazon S3 Transfer Acceleration.
La herramienta Comparación de velocidad utiliza cargas multipartes para transferir un archivo desde su navegador hacia diversas regiones de AWS con Amazon S3 Transfer Acceleration y sin esta herramienta. Puede comparar la velocidad de subida para las subidas directas y transferir las subidas aceleradas por región.

Para habilitar Transfer Acceleration para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket para el que desea habilitar la aceleración de transferencia.
3. Seleccione Properties (Propiedades).
4. En Transfer acceleration (Aceleración de transferencia), elija Edit (Editar).
5. Elija Enable (Habilitar) y Save Changes (Guardar cambios).

   Amazon S3 habilita la aceleración de transferencia para el bucket y muestra la pestaña Properties (Propiedades) del bucket. En Transfer acceleration (Aceleración de transferencia), el punto de enlace acelerado muestra el punto de enlace de aceleración de transferencia del bucket. Utilice este punto de enlace para acceder a transferencias de datos aceleradas desde y hacia el bucket. Si suspende Transfer Acceleration, el punto de enlace de aceleración deja de funcionar.

Introducción a los puntos de acceso de Amazon S3

Puede utilizar los puntos de acceso de Amazon S3 para administrar el acceso a sus objetos de S3. Los puntos de acceso de Amazon S3 son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de S3, como la carga y recuperación de objetos. Un bucket puede tener hasta 1.000 puntos de acceso asociados y cada punto de acceso aplica permisos y controles de red diferenciados para proporcionarle un control detallado sobre el acceso a los objetos de S3.

Para obtener más información acerca de los puntos de acceso de Amazon S3, consulte Administración de acceso de datos con puntos de acceso de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

En los temas siguientes se explica cómo utilizar la consola de administración de S3 para crear, administrar y utilizar puntos de acceso de Amazon S3.

Temas

Creación de un punto de acceso de Amazon S3

En esta sección se explica cómo crear un punto de acceso de Amazon S3 con la consola de administración de AWS. Para obtener información sobre cómo crear puntos de acceso mediante la CLI de AWS, los SDK de AWS y las API de REST de Amazon S3, consulte Administrar el acceso a datos con puntos de acceso de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Un punto de acceso está asociado con exactamente un bucket de Amazon S3. Antes de comenzar, asegúrese de haber creado un bucket que desea utilizar con este punto de acceso. Para obtener más información acerca de cómo se crean los buckets, consulte Crear y configurar un bucket de S3 (p. 3).

Para crear un punto de acceso

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación del lado izquierdo de la consola, elija Access points (Puntos de acceso).
3. En la página de puntos de acceso, elija Create access point (Crear punto de acceso).
4. Introduzca el nombre que desee para el punto de acceso en el campo Access point name (Nombre del punto de acceso). Para obtener más información acerca de cómo poner nombre a los puntos de acceso, consulte Reglas para asignar nombres a los puntos de acceso de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.
5. En el campo Bucket name (Nombre del bucket), introduzca el nombre de un bucket de su cuenta al que desee asociar el punto de acceso. Por ejemplo, `DOC-EJEMPLO-BUCKET1`. Si lo desea, también puede elegir Browse S3 (Examinar S3) para explorar su cuenta y buscar buckets. Si elige Browse S3 (Examinar S3), seleccione el bucket que le interese y seleccione Choose path (Elegir ruta) para rellenar el campo Bucket name (Nombre del bucket) con el nombre del bucket en cuestión.
6. (Opcional) Elija View (Ver) para ver el contenido del bucket especificado en una nueva ventana del navegador.

7. Seleccione un origen en Network origin (Origen de red). Si elige Virtual private cloud (VPC) [Nube virtual privada (VPC)], escriba el identificador VPC ID (ID de VPC) que desea usar con el punto de acceso.

   Para obtener más información acerca de los orígenes de red para los puntos de acceso, consulte el artículo sobre cómo crear puntos de acceso restringidos a una nube privada virtual en la guía del desarrollador de Amazon Simple Storage Service.
8. En Access point settings for Block Public Access (Configuración de punto de acceso para bloquear el acceso público, seleccione la configuración de bloqueo de acceso público que desee aplicar al punto de acceso. Todas las configuraciones de bloqueo de acceso público están activadas de forma predeterminada para los nuevos puntos de acceso. Recomendamos dejar todas estas configuraciones activadas, a menos que sepa que tiene una necesidad específica de desactivar cualquiera de ellas. Amazon S3 actualmente no admite cambiar la configuración de bloqueo de acceso público de un punto de acceso después de que se haya creado el punto de acceso.

   Para obtener más información sobre cómo usar el bloqueo de acceso público de Amazon S3 con puntos de acceso, consulte Administrar el acceso público a los puntos de acceso en la guía del desarrollador de Amazon Simple Storage Service.
9. (Opcional) En Access point policy - optional (Política de punto de acceso: opcional), especifique la política de punto de acceso. Para obtener más información acerca de cómo especificar una política de punto de acceso, consulte Ejemplos de políticas de punto de acceso en la guía del desarrollador de Amazon Simple Storage Service.
10. Elija Create access point (Crear punto de acceso).

Administración y uso de puntos de acceso de Amazon S3

En esta sección se explica cómo administrar y utilizar los puntos de acceso de Amazon S3 con la consola de administración de AWS. Antes de comenzar, vaya a la página de detalles del punto de acceso que desea administrar o utilizar, tal como se describe en el procedimiento siguiente.

Navegación a una página de detalles de un punto de acceso

Opción 1: Liste todos los puntos de acceso de su cuenta

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación del lado izquierdo de la consola, elija Access points (Puntos de acceso).
3. En la página Access points (Puntos de acceso), en Access points (Puntos de acceso), seleccione la región de AWS que contiene los puntos de acceso que desea listar.
4. (Opcional) Busque puntos de acceso por nombre escribiendo para ello un nombre en el campo de texto situado junto al menú desplegable Region (Región).
5. Elija el nombre del punto de acceso que desea administrar o utilizar.

Opción 2: Enumerar todos los puntos de acceso para un único bucket

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación del lado izquierdo de la consola, elija Buckets (Buckets).

3. En la página Buckets (Buckets), seleccione el nombre del bucket cuyos puntos de acceso desea listar.
4. En la página de detalles del bucket, elija la pestaña Access points (Puntos de acceso).
5. Elija el nombre del punto de acceso que desea administrar o utilizar.

Administración y uso de un único punto de acceso

Visualización de los detalles de configuración de un punto de acceso

1. Acceda a la página de detalles del punto de acceso cuyos detalles desea ver tal y como se describe en Navegación a una página de detalles de un punto de acceso (p. 24).
2. En Access point overview (Información general del punto de acceso), consulte los detalles de configuración y las propiedades del punto de acceso seleccionado.

Uso de un punto de acceso para acceder a su bucket

1. Acceda a la página de detalles del punto de acceso que desee utilizar tal y como se describe en Navegación a una página de detalles de un punto de acceso (p. 24).
2. En la ficha Objects (Objetos), elija el nombre de un objeto u objetos a los que desea acceder a través del punto de acceso. En las páginas de funcionamiento de objetos, la consola muestra una etiqueta encima del nombre del bucket, en la que aparece el punto de acceso que está utilizando actualmente. Mientras utiliza el punto de acceso, solo puede realizar las operaciones con objetos permitidas por los permisos de ese punto de acceso.

   Note

   - La vista de consola siempre muestra todos los objetos del bucket. El uso de un punto de acceso como se describe en este procedimiento restringe las operaciones que puede realizar en esos objetos, pero no la posibilidad de ver si existen en el bucket.
   - La consola de administración de S3 no admite el uso de puntos de acceso de nube virtual privada (VPC) para acceder a los recursos del bucket. Para acceder a los recursos del bucket desde un punto de acceso de VPC, utilice la CLI de AWS, los SDK de AWS o las API de REST de Amazon S3.

Visualización de la configuración de un punto de acceso para bloquear el acceso público

1. Acceda a la página de detalles del punto de acceso cuya configuración desea ver, tal y como se describe en Navegación a una página de detalles de un punto de acceso (p. 24).
2. Elija Permissions.
3. En Access point policy (Política de punto de acceso), revise la configuración de bloqueo de acceso público para el punto de acceso.

   Note

   No puede cambiar la configuración de bloqueo de acceso público de un punto de acceso después de crear el punto de acceso.

Para editar una política de punto de acceso

1. Acceda a la página de detalles del punto de acceso cuya política desea editar, tal y como se describe en Navegación a una página de detalles de un punto de acceso (p. 24).
2. Elija Permissions.
3. En Access point policy (Política de punto de acceso), elija Edit (Editar).

4. Escriba la política de punto de acceso en el campo de texto. La consola muestra automáticamente el nombre de recurso de Amazon (ARN) para el punto de acceso, que puede utilizar en la política.
5. Seleccione Save.

Eliminación de un punto de acceso

1. Vaya a la lista de puntos de acceso de su cuenta o de un bucket específico, tal y como se describe en Navegación a una página de detalles de un punto de acceso (p. 24).
2. Seleccione el botón de opción situado junto al nombre del punto de acceso que desea eliminar.
3. Elija Eliminar.
4. Confirme que desea eliminar el punto de acceso escribiendo su nombre en el campo de texto que aparece y elija Delete (Eliminar).

Cargar, descargar y administrar objetos.

Para cargar sus datos (fotos, vídeos, documentos, etc.) en Amazon S3, primero tiene que crear un bucket de S3 en una de las regiones de AWS. A continuación puede cargar un número ilimitado de objetos de datos en el bucket.

Los datos almacenados en Amazon S3 están compuestos por objetos. Todos los objetos residen en un bucket que haya creado en una región de AWS específica. Todos los objetos almacenados en Amazon S3 residen en un bucket.

Los objetos almacenados en una región nunca la abandonan, a menos que se transfieran expresamente a otra región. Por ejemplo, los objetos almacenados en la región UE (Irlanda) nunca salen de ella. Los objetos almacenados en una región de AWS permanecen físicamente en esa región. Amazon S3 no almacena copias de los objetos ni las traslada a ninguna otra región. Sin embargo, puede obtener acceso a los objetos desde cualquier lugar, siempre y cuando disponga de los permisos necesarios para hacerlo.

Para poder cargar un objeto en Amazon S3, debe disponer de permisos de escritura en un bucket.

Los objetos pueden tener cualquier tipo de archivo: imágenes, copias de seguridad, datos, películas, etc. Puede haber un número ilimitado de objetos en un bucket. El tamaño máximo de un archivo que puede cargar con la consola de Amazon S3 es de 160 GB. Para cargar un archivo que sobrepasa los 160 GB de tamaño, utilice la CLI de AWS, el SDK de AWS o la API de REST de Amazon S3. Para obtener más información, consulte Carga de objetos en la guía del desarrollador de Amazon Simple Storage Service.

En los siguientes temas se explica cómo utilizar la consola de Amazon S3 para cargar, eliminar o administrar objetos.

> Note
>
> Si cambia el nombre de un objeto o cambia cualquiera de las propiedades: Clase de almacenamiento, Cifrado, Metadatos, se crea un nuevo objeto para reemplazar el antiguo. Si el control de versiones de S3 está activado, se crea una nueva versión del objeto y el objeto existente se convierte en una versión anterior. El rol que cambia la propiedad también se convierte en el propietario del nuevo objeto o (versión del objeto).

Temas

- ¿Cómo puedo utilizar carpetas en un bucket de S3? (p. 45)

¿Cómo puedo cargar archivos y carpetas en un bucket de S3?

En este tema se explica cómo usar la consola de administración de AWS para cargar uno o más archivos, o carpetas completas en un bucket de Amazon S3. Para poder cargar archivos y carpetas en un bucket de Amazon S3, debe escribir permisos para el bucket. Para obtener más información acerca de los permisos de acceso, consulte Configuración de permisos de acceso a buckets y objetos (p. 66). Para obtener información acerca de cómo cargar archivos mediante programación, consulte Carga de objetos en la guía del desarrollador de Amazon Simple Storage Service.

Cuando carga un archivo en Amazon S3, este se guarda como un objeto de S3. Los objetos constan de los datos y metadatos del archivo que describen el objeto. Puede haber un número ilimitado de objetos en un bucket.

Puede cargar cualquier tipo de archivo, como imágenes, copias de seguridad, datos, películas, etc., en un bucket de S3. El tamaño máximo de un archivo que puede cargar con la consola de Amazon S3 es de 160 GB. Para cargar un archivo que sobrepasa los 160 GB de tamaño, utilice la CLI de AWS, el SDK de AWS o la API de REST de Amazon S3. Para obtener más información, consulte Carga de objetos en la guía del desarrollador de Amazon Simple Storage Service.

> Note
>
> Para cargar carpetas, debe arrastrarlas y soltarlas. Para cargar archivos, puede arrastrar y soltar o apuntar y hacer clic. Solo los navegadores Chrome y Firefox admiten la funcionalidad de arrastrar y soltar.

Para obtener más información acerca de las versiones compatibles de los navegadores Chrome y Firefox, consulte Navegadores compatibles con la consola de administración de AWS.

Cuando carga una carpeta, Amazon S3 carga todos los archivos y subcarpetas de la carpeta especificada en su bucket. Luego asigna un nombre de clave de objeto, que es una combinación del nombre del archivo cargado y el nombre de la carpeta. Por ejemplo, si carga una carpeta llamada `/images` que contiene dos archivos, `sample1.jpg` y `sample2.jpg`, Amazon S3 carga los archivos y les asigna los nombres de clave correspondientes, `images/sample1.jpg` e `images/sample2.jpg`. Los nombres de clave incluyen el nombre de la carpeta como un prefijo. La consola de Amazon S3 muestra solo la parte del nombre de clave siguiente a la última "/". Por ejemplo, dentro de una carpeta de imágenes, los objetos `images/sample1.jpg` e `images/sample2.jpg` se muestran como `sample1.jpg` y `sample2.jpg`.

Si carga archivos individuales y tiene una carpeta abierta en la consola de Amazon S3 cuando Amazon S3 carga los archivos, incluye el nombre de la carpeta abierta como el prefijo de los nombres de clave. Por ejemplo, si tiene una carpeta abierta llamada `backup` en la consola de Amazon S3 y carga un archivo llamado `sample1.jpg`, el nombre de clave será `backup/sample1.jpg`. Sin embargo, el objeto se mostrará en la consola como `sample1.jpg` la carpeta `backup`.

Si carga archivos individuales y no tiene una carpeta abierta en la consola de Amazon S3 cuando Amazon S3 carga los archivos, solo asigna el nombre del archivo como el nombre de clave. Por ejemplo, si carga un archivo llamado `sample1.jpg`, el nombre de clave será `sample1.jpg`. Para obtener más información sobre nombres de clave, consulte Claves y metadatos de objetos en la guía del desarrollador de Amazon Simple Storage Service.

Si carga un objeto con un nombre de clave que ya existe en un bucket con el control de versiones activado, Amazon S3 crea otra versión del objeto en vez de reemplazar el objeto existente. Para obtener más información sobre el control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8).

Temas

Carga de archivos y carpetas con la función arrastrar y soltar

Si usa los navegadores Chrome o Firefox, puede seleccionar las carpetas y los archivos para cargar y arrastrarlos y soltarlos en el bucket de destino. La función arrastrar y soltar es la única manera de cargar carpetas.

Carga de archivos y carpetas a un bucket de S3 con la función arrastrar y soltar

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en el que desea cargar sus carpetas o archivos.
3. En una ventana distinta de la ventana de la consola, seleccione los archivos y las carpetas que desea cargar. Después, arrastre y suelte los elementos seleccionados en la ventana de la consola que indica los objetos en el bucket de destino.

   Los archivos seleccionados aparecen en la página Upload (Cargar).
4. En la página Upload (Cargar) puede arrastrar y soltar más archivos y carpetas en la ventana de la consola que se ve en la página Upload (Cargar) . Para agregar más archivos, también puede elegir Add files (Agregar archivos) o Add folder (Agregar carpeta).
5. En la sección Destination (Destino), si el control de versiones no está activado, debe marcar la casilla para confirmar que se sobrescribirán los objetos con el mismo nombre.

   Para cargar inmediatamente los archivos y las carpetas en la lista sin otorgar o eliminar permisos para usuarios específicos ni establecer permisos públicos para todos los archivos que van a cargar, seleccione Upload (Cargar) en la parte inferior de la página. Para obtener información acerca de los permisos de acceso a objetos, consulte ¿Cómo puedo configurar permisos en un objeto? (p. 69).
6. En la sección Storage class (Clase de almacenamiento), elija la clase de almacenamiento para los archivos que esté cargando. Para obtener más información sobre la replicación, consulte Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.
7. Seleccione el tipo de cifrado para los archivos que va a cargar. Si no desea cifrarlos, elija Disable (Desactivar).

   a. Para cifrar los archivos cargados con claves que administra Amazon S3, seleccione Amazon S3 key (Clave de Amazon S3). Para obtener más información, consulte el tema sobre protección de datos con clases de claves de cifrado administradas por Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.
   b. Para cifrar los archivos cargados con AWS Key Management Service (AWS KMS), seleccione AWS Key Management Service key (Clave de AWS Key Management Service). A continuación, elija una clave maestra del cliente (CMK) en la lista de CMK de AWS KMS.

      Note

      Para cifrar objetos en un bucket, puede usar solo las CMK disponibles en la misma región de AWS que el bucket.

   Puede permitir que una cuenta externa use un objeto protegido con una CMK de AWS KMS. Para hacerlo, seleccione Custom KMS ARN (ARN de KMS personalizado) en la lista y escriba el

nombre de recurso de Amazon (ARN) para la cuenta externa. Los administradores de una cuenta externa que tienen permisos de uso de un objeto protegido por su CMK de AWS KMS pueden restringir aún más el acceso mediante la creación de una política IAM de nivel de recursos.

Para obtener más información acerca de cómo crear una CMK de AWS KMS, consulte Creación de claves en la guía para desarrolladores de AWS Key Management Service. Para obtener más información sobre cómo usar AWS KMS, consulte el tema sobre cómo proteger datos con claves almacenadas en AWS KMS (SSE-KMS) en la guía del desarrollador de Amazon Simple Storage Service.

8. En la sección Access control list (ACL) [Lista de control de acceso (ACL)] puede cambiar los permisos para el propietario de la cuenta de AWS. Propietario hace referencia al usuario raíz de su cuenta de AWS y no a un usuario de AWS Identity and Access Management (IAM). Para obtener más información acerca del usuario raíz, consulte El usuario raíz de la cuenta de AWS.

   Puede conceder acceso de lectura a los objetos al público en general (a todo el mundo) para todos los archivos que esté cargando. Otorgar acceso de lectura público es aplicable a un pequeño conjunto de casos de uso por ejemplo cuando los buckets se utilizan para sitios web. Le recomendamos que no cambie la opción predeterminada. Siempre puede realizar cambios en los permisos del objeto después de cargarlo. Para obtener información acerca de los permisos de acceso a objetos, consulte ¿Cómo puedo configurar permisos en un objeto? (p. 69).

   Elija Add grantee (Agregar beneficiario) para conceder acceso a otra cuenta de AWS. Para obtener más información sobre cómo conceder permisos a otra cuenta de AWS, consulte ¿Cómo se configuran permisos de buckets de ACL? (p. 71).
9. El etiquetado de objetos le permite categorizar el almacenamiento. Cada etiqueta es un par clave-valor. Los valores de clave y de etiqueta distinguen entre mayúsculas y minúsculas. Puede tener hasta 10 etiquetas por objeto.

   Para agregar etiquetas a todos los objetos que va a cargar, elija Add tag (Agregar etiqueta). Escriba un nombre de etiqueta en el campo Key (Clave) . Escriba un valor para la etiqueta. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 255 caracteres Unicode. Para obtener más información acerca de las etiquetas de objeto, consulte Etiquetado de objetos en la guía del desarrollador de Amazon Simple Storage Service.
10. Los metadatos de los objetos de Amazon S3 se representan mediante un par nombre-valor (clave-valor). Hay dos tipos de metadatos: metadatos definidos por el sistema y metadatos definidos por el usuario. Para agregar metadatos a todos los objetos que está cargando, elija Add metadata (Agregar metadatos).

    a. Si desea agregar metadatos definidos por el sistema de Amazon S3, en Type (Tipo), elija System Defined (Definido por el sistema). En Key (Clave), seleccione una clave. Puede seleccionar encabezados de HTTP comunes, como Content-Type (Contenido-Tipo) y Content-Disposition (Contenido-Disposición). Escriba un valor para la clave. Para ver una lista de metadatos definidos por el sistema e información sobre si puede agregar el valor, consulte el tema sobre metadatos definidos por el sistema en la guía del desarrollador de Amazon Simple Storage Service.
    b. Cualquier tipo de metadatos que comience con el prefijo `x-amz-meta-` se trata como metadatos definidos por el usuario. Los metadatos definidos por el usuario se almacenan con el objeto y se devuelven cuando lo descarga.

       Para agregar metadatos definidos por el usuario a todos los objetos que está cargando, seleccione en Type (Tipo) User Defined (Definido por el usuario). Escriba `x-amz-meta-` más un nombre de metadatos personalizado en el campo Key (Clave) . Escriba un valor para la clave. Tanto las claves como sus valores deben cumplir los estándares ASCII de EE. UU. Los metadatos definidos por el usuario pueden tener un tamaño de hasta 2 KB. Para obtener más información sobre metadatos definidos por el usuario, consulte el tema sobre metadatos definidos por el usuario en la guía del desarrollador de Amazon Simple Storage Service.
11. Seleccione Upload.

Carga de archivos con la función apuntar y hacer clic

En este procedimiento se explica cómo cargar archivos en un bucket de S3 eligiendo Upload (Cargar).

Para cargar archivos en un bucket de S3 con la función apuntar y hacer clic

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, elija el nombre del bucket en el que desee cargar los archivos.
3. Seleccione Upload.
4. En la página Upload (Cargar), elija Add files (Agregar archivos) o Add folder (Agregar carpeta).
5. Seleccione uno o más archivos para cargar y, luego, seleccione Open (Abrir).
6. Tras ver los archivos que seleccionó en el cuadro de diálogo Upload (Cargar), proceda con el paso 5 de Carga de archivos y carpetas con la función arrastrar y soltar (p. 29).

Más información

- ¿Cómo puedo configurar permisos en un objeto? (p. 69).
- ¿Cómo descargo un objeto de un bucket de S3? (p. 33)

Copia de objetos

La consola de Amazon S3 le permite copiar objetos en un bucket o en un punto de acceso dentro de la misma región de AWS. Para obtener más información, consulte Copia de objetos en la guía del desarrollador de Amazon Simple Storage Service.

Para copiar un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Desplácese hasta el bucket o la carpeta de Amazon S3 que contiene los objetos que desea copiar.
3. Seleccione la casilla de verificación situada a la izquierda de los nombres de los objetos que desea copiar.
4. Elija Actions (Acciones) y luego Copy (Copiar) en la lista de opciones que aparece.

   También puede elegir Copy (Copiar) en las opciones de la esquina superior derecha.
5. Seleccione el tipo de destino y la cuenta de destino. Para especificar la ruta de destino, seleccione Browse S3 (Examinar S3), desplácese hasta el destino y active la casilla de verificación situada a la izquierda del destino. Seleccione Choose destination (Elegir destino) en la parte inferior derecha.

   También puede escribir la ruta de destino.
6. Si no tiene activado el control de versiones del bucket, es posible que se le pida que confirme que los objetos que tengan el mismo nombre se deben sobreescribir. Si así es, seleccione la casilla de verificación y continúe. Si quiere mantener todas las versiones de los objetos en este bucket, seleccione Enable Bucket Versioning (Habilitar control de versiones de bucket). También puede actualizar las propiedades predeterminadas de cifrado y de bloqueo de objetos.
7. Elija Copy (Copiar) en la parte inferior derecha y Amazon S3 moverá los objetos al destino.

Note

- Esta acción crea una copia de todos los objetos especificados con parámetros actualizados, actualiza la fecha de última modificación en la ubicación especificada y agrega un marcador de eliminación al objeto original.
- Al mover carpetas, espere a que finalice la acción de movimiento antes de realizar cambios adicionales en las carpetas.
- Los objetos cifrados con claves de cifrado proporcionadas por el cliente (SSE-C) no se pueden copiar con la consola de S3. Para copiar objetos cifrados con SSE-C, utilice la CLI de AWS, el SDK de AWS o la API de REST de Amazon S3.
- Esta acción actualiza los metadatos para el control de versiones de bucket, el cifrado, las características de bloqueo de objetos y los objetos archivados.

Mover objetos

En la consola de Amazon S3, puede mover objetos a un bucket o a una carpeta.

Para mover objetos

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Desplácese hasta el bucket o carpeta de Amazon S3 que contiene los objetos que quiera mover.
3. Seleccione la casilla situada a la izquierda del nombre de cada uno de los objetos que quiera mover.
4. Seleccione Actions (Acciones) y después Move (Mover) en la lista de opciones que aparece.

   También puede seleccionar Move (Mover) entre las opciones de arriba a la derecha.
5. Para especificar la ruta de destino, seleccione Browse S3 (Examinar S3), desplácese hasta el destino y active la casilla de verificación situada a la izquierda del destino. Seleccione Choose destination (Elegir destino) en la parte inferior derecha.

   También puede escribir la ruta de destino.
6. Si no tiene activado el control de versiones del bucket, es posible que se le pida que confirme que los objetos que tengan el mismo nombre se deben sobreescribir. Si así es, seleccione la casilla de verificación y continúe. Si quiere mantener todas las versiones de los objetos en este bucket, seleccione Enable Bucket Versioning (Habilitar control de versiones de bucket). También puede actualizar las propiedades predeterminadas de cifrado y de bloqueo de objetos.
7. Seleccione Move (Mover) en la parte inferior derecha y Amazon S3 moverá los objetos al destino.

Note

- Esta acción crea una copia de todos los objetos especificados con parámetros actualizados, actualiza la fecha de última modificación en la ubicación especificada y agrega un marcador de eliminación al objeto original.
- Al mover carpetas, espere a que finalice la acción de movimiento antes de realizar cambios adicionales en las carpetas.
- Los objetos cifrados con claves de cifrado proporcionadas por el cliente (SSE-C) no se pueden copiar con la consola de S3. Para copiar objetos cifrados con SSE-C, utilice la CLI de AWS, el SDK de AWS o la API de REST de Amazon S3.
- Esta acción actualiza los metadatos para el control de versiones de bucket, el cifrado, las características de bloqueo de objetos y los objetos archivados.

¿Cómo descargo un objeto de un bucket de S3?

En esta sección se explica cómo utilizar la consola de Amazon S3 para descargar objetos de un bucket de S3.

Al descargar objetos se aplican tarifas por transferencia de datos. Para obtener información sobre las características y precios de Amazon S3, consulte Amazon S3.

Important

- Si el nombre de la clave de un objeto consta de un solo punto (.) o de dos puntos (..), no puede descargar el objeto desde la consola de Amazon S3. Para descargar un objeto con un nombre de clave de "." o "..", debe utilizar la CLI de AWS, los SDK de AWS o la API de REST. Para obtener más información acerca de la nomenclatura de objetos, consulte Directrices de nomenclatura de claves de objeto en la guía del desarrollador de Amazon Simple Storage Service.
- Puede descargar un solo objeto por solicitud utilizando la consola de Amazon S3. Para descargar varios objetos, utilice la CLI de AWS, los SDK de AWS o la API de REST.

Para descargar un objeto desde un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket que contiene el objeto que desea descargar.
3. Puede descargar un objeto de un bucket de S3 de cualquiera de las siguientes maneras:

   - Seleccione el nombre del objeto que quiera descargar.

     En la página Overview (Información general), seleccione Download (Descargar).
   - Elija el nombre del objeto que quiera descargar y elija Download (Descargar) o Download as (Descargar como) en la página Action (Acción).
   - Seleccione el nombre del objeto que quiera descargar. Seleccione Latest version (Última versión) y haga clic en el icono de descarga.

Temas relacionados

- ¿Cómo puedo cargar archivos y carpetas en un bucket de S3? (p. 28)

Eliminación de objetos

En esta sección se explica cómo usar la consola de Amazon S3 para eliminar objetos. Debido a que todos los objetos en el bucket de S3 generan costos de almacenamiento, debe eliminar los objetos cuando ya no los necesita. Si acumula archivos de registro, por ejemplo, se recomienda eliminarlos cuando ya no se necesitan. También puede configurar una regla de ciclo de vida para eliminar los objetos, como los archivos de registro, de manera automática. Para obtener más información sobre las reglas de ciclo de vida, consulte ¿Cómo se crea una regla de ciclo de vida para un bucket de S3? (p. 50) en esta guía.

Para obtener información sobre las características y precios de Amazon S3, consulte Amazon S3.

Para eliminar objetos

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. Desplácese hasta el bucket o la carpeta de Amazon S3 que contiene los objetos que desea eliminar.
3. Seleccione la casilla de verificación situada a la izquierda de los nombres de los objetos que desea eliminar.
4. Elija Actions (Acciones) y después Delete (Eliminar) en la lista de opciones que aparece.

   También puede elegir Delete (Eliminar) en las opciones de arriba a la derecha.
5. Escriba **`delete`** si se le pide que confirme que desea eliminar estos objetos.
6. Elija Delete objects (Eliminar objetos) en la parte inferior derecha y Amazon S3 eliminará los objetos especificados.

   Warning

   - No se puede deshacer la eliminación de los objetos especificados.
   - Esta acción elimina todos los objetos especificados. Al eliminar carpetas, espere a que finalice la acción de eliminación antes de agregar nuevos objetos a la carpeta. De lo contrario, es posible que también se eliminen objetos nuevos.
   - No se puede deshacer la eliminación de los objetos especificados.

¿Cómo se anula la eliminación de objetos de S3?

En esta sección se explica cómo usar la consola de Amazon S3 para recuperar (anular la eliminación de) objetos eliminados.

Para poder anular la eliminación de un objeto eliminado, debe haber habilitado el control de versiones en el bucket que contuviera el objeto antes de que el objeto fuera eliminado. Para obtener más información sobre la habilitación del control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8).

Cuando se elimina un objeto en un bucket con control de versiones activado, todas las versiones permanecen en el bucket y Amazon S3 crea un marcador de eliminación para el objeto. Para anular la eliminación del objeto, debe eliminar este marcador de eliminación. Para obtener más información, consulte Versiones de objetos en la guía del desarrollador de Amazon Simple Storage Service.

Para recuperar objetos eliminados de un bucket de S3

En los siguientes pasos se describe cómo recuperar objetos eliminados que no son carpetas del bucket de S3, incluidos los objetos que se encuentran dentro de esas carpetas.

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. Para ver una lista de las versiones de los objetos en el bucket, elija el modificador List versions (Listar versiones). Podrá ver los marcadores de eliminación de los objetos eliminados.
4. Para anular la eliminación de un objeto, debe eliminar su marcador de eliminación. Marque la casilla de verificación que aparece junto al marcador de eliminación del objeto que desee recuperar y, a continuación, elija Delete (Eliminar).
5. Confirme la eliminación en la página Delete objects (Eliminar objetos) .

   a. Escriba **`permanently delete`** bajo Pemanently delete objects? (¿Eliminar los objetos de manera permanente)?

   b. Elija Delete objects (Eliminar objetos).

Note

No puede usar la consola de Amazon S3 para anular la eliminación de carpetas. Debe utilizar la CLI de AWS o el SDK. Para ver ejemplos, consulte ¿Cómo puedo recuperar un objeto de Amazon S3 que se eliminó en un bucket con control de versiones habilitado?

Más información

- ¿Cómo se consultan las versiones de un objeto de S3? (p. 39)
- ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8)
- Uso de versiones en la guía del desarrollador de Amazon Simple Storage Service

¿Cómo se recupera un objeto de S3 que se archivó?

En esta sección se explica cómo utilizar la consola de Amazon S3 para restaurar un objeto que se archivó en las clases de almacenamiento S3 Glacier o S3 Glacier Deep Archive. No se puede acceder inmediatamente a los objetos almacenados en la clase S3 Glacier o S3 Glacier Deep Archive. Para obtener acceso a un objeto de esta clase, debe restaurar una copia temporal del mismo en su bucket de S3 durante el periodo (cantidad de días) especificado. Para obtener información sobre las clases de almacenamiento S3 Glacier o S3 Glacier Deep Archive, consulte Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.

Cuando restaura un archivo, usted paga el archivo y la copia restaurada. Debido a que hay un costo de almacenamiento para la copia, restaure los objetos solo durante el tiempo que los necesite. Si desea obtener una copia permanente del objeto, cree una copia del objeto en su bucket de S3. Para obtener información sobre las características y precios de Amazon S3, consulte Amazon S3.

Después de restaurar un objeto, puede descargarlo desde la página Overview (Información general). Para obtener más información, consulte ¿Cómo se ve la información general de un objeto? (p. 38).

Temas

- Opciones de recuperación de archivos (p. 35)
- Restauración de un objeto de S3 archivado (p. 36)
- Actualizar una restauración en curso (p. 36)
- Comprobación del estado de restauración y la fecha de vencimiento de un archivo (p. 37)

Opciones de recuperación de archivos

A continuación, se muestran las opciones de recuperación disponibles al restaurar un objeto archivado:

- **`Expedited`**: las recuperaciones rápidas le permiten obtener acceso rápidamente a sus datos almacenados en la clase de almacenamiento S3 Glacier cuando son necesarias solicitudes urgentes ocasionales para un subconjunto de archivos. En todos los casos excepto para los objetos archivados de mayor tamaño (más de 250 MB), los datos a los que se obtiene acceso con solicitudes rápidas suelen estar disponibles en un plazo de entre 1 y 5 minutos. La capacidad aprovisionada garantiza que la capacidad que necesitan las recuperaciones Expedited estará disponible cuando lo necesite. Para obtener más información, consulte Capacidad aprovisionada. Las recuperaciones rápidas y la capacidad aprovisionada no están disponibles para los objetos almacenados en la clase S3 Glacier Deep Archive.

- **`Standard`**: las recuperaciones estándares le permiten acceder a sus objetos archivados en un plazo de varias horas. Esta es la opción predeterminada para las solicitudes de recuperación de S3 Glacier y S3 Glacier Deep Archive que no especifican la opción de recuperación. Las recuperaciones estándar finalizan en un plazo de entre tres y cinco horas para los objetos que están almacenados en la clase de almacenamiento S3 Glacier. Suelen finalizar en un plazo de 12 horas para los objetos que están almacenados en la clase de almacenamiento S3 Glacier Deep Archive.
- **`Bulk`**: las recuperaciones en bloque son la opción de recuperación menos costosa de Amazon S3, lo que le permite recuperar grandes cantidades de datos, incluso petabytes, de forma económica. Las recuperaciones en bloque suelen finalizar en un plazo de entre cinco y 12 horas para los objetos que están almacenados en la clase de almacenamiento S3 Glacier. Suelen finalizar en un plazo de 48 horas para los objetos que están almacenados en la clase de almacenamiento S3 Glacier Deep Archive.

Para obtener más información acerca de las opciones de recuperación, consulte Restaurar objetos archivados en la guía del desarrollador de Amazon Simple Storage Service.

Restauración de un objeto de S3 archivado

En este tema se explica cómo utilizar la consola de Amazon S3 para restaurar un objeto que se archivó en las clases de almacenamiento S3 Glacier o S3 Glacier Deep Archive. (la consola utiliza los nombres Glacier y Glacier Deep Archive para estas clases de almacenamiento).

Para restaurar objetos de S3 archivados

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), seleccione el nombre del bucket que contiene los objetos que desea restaurar.
3. En la lista Name (Nombre), seleccione el objeto o los objetos que desea restaurar, elija Actions (Acciones) y, luego, Initiate restore (Iniciar restauración).
4. En el cuadro de diálogo Initiate restore (Iniciar restauración), escriba la cantidad de días que desea que sus datos archivados estén disponibles.
5. Seleccione una de las siguientes opciones de recuperación del menú Retrieval options (Opciones de recuperación).

   - Seleccione Bulk retrieval (Recuperación en bloque) o Standard retrieval (Recuperación estándar) y, a continuación, seleccione Restore (Restaurar).
   - Elija Expedited retrieval (Recuperación rápida) (solo está disponible para la clase de almacenamiento Glacier).
6. La capacidad aprovisionada está disponible solo para la clase de almacenamiento Glacier. Si tiene capacidad aprovisionada, seleccione Restore (Restaurar) para comenzar una recuperación aprovisionada. Si tiene capacidad aprovisionada, todas sus recuperaciones rápidas funcionan con la capacidad aprovisionada. Para obtener más información sobre la capacidad aprovisionada, consulte Capacidad aprovisionada.

   - Si no tiene capacidad aprovisionada y no desea comprarla, seleccione Restore (Restaurar).
   - Si no tiene capacidad aprovisionada pero desea comprarla, seleccione Add capacity unit (Añadir unidad de capacidad) y luego seleccione Buy (Comprar). Cuando recibe el mensaje Purchase succeeded (Compra realizada correctamente), seleccione Restore (Restaurar) para comenzar la recuperación aprovisionada.

Actualizar una restauración en curso

Puede actualizar la velocidad de la restauración mientras esta se encuentra en curso.

Para actualizar una restauración en curso a una capa más rápida

1. En la lista Name (Nombre), seleccione el objeto o los objetos que desea restaurar, seleccione Actions (Acciones) y, luego, Restore from Glacier (Restaurar desde Glacier). Para obtener más información sobre cómo comprobar el estado de restauración de un objeto, consulte Comprobación del estado de restauración y la fecha de vencimiento de un archivo (p. 37).
2. Seleccione la capa a la que desea realizar la actualización y elija Restore (Restaurar). Para obtener más información acerca de cómo actualizar la capa de restauración a una más rápida, consulte Restaurar objetos archivados en la guía del desarrollador de Amazon Simple Storage Service.

Comprobación del estado de restauración y la fecha de vencimiento de un archivo

Para verificar el progreso de la restauración, consulte el panel de información general del objeto. Para obtener información acerca del panel de información general, consulte ¿Cómo se ve la información general de un objeto? (p. 38).

La sección Overview (Información general) indica que el estado de la restauración es In progress (En curso).

Cuando la copia temporal del objeto está disponible, la sección Overview (Información general) del objeto muestra Restoration expiry date (Fecha de vencimiento de la restauración). Esto indica la fecha en que Amazon S3 eliminará la copia restaurada de su archivo.

Los objetos restaurados se almacenan solo durante el número de días que usted especifica. Si desea obtener una copia permanente del objeto, cree una copia del objeto en su bucket de Amazon S3.

Amazon S3 calcula la fecha de vencimiento sumando la cantidad de días que usted especifica a la hora que solicita restaurar el objeto, y luego, redondea al siguiente día a medianoche en Universal Time Coordinated (UTC, Hora universal coordinada). Este cálculo se aplica a la restauración inicial del objeto y a cualquier extensión de disponibilidad que solicite. Por ejemplo, si un objeto se restauró el 15/10/2012 a las 10:30 h UTC y la cantidad de días que especificó es 3, el objeto está disponible hasta el 19/10/2012 a las 00:00 h UTC. Si el 16/10/2012 a las 11:00 h UTC, usted cambia la cantidad de días que desea que el objeto esté disponible a 1, Amazon S3 hace que el objeto restaurado esté disponible hasta el 18/10/2012 a las 00:00 h UTC.

Después de restaurar un objeto, puede descargarlo desde la página Overview (Información general). Para obtener más información, consulte ¿Cómo se ve la información general de un objeto? (p. 38).

Más información

- Restaurar objetos archivados en la guía del desarrollador de Amazon S3.
- restore-object en la referencia de los comandos de la CLI de AWS.
- Administración de identidades y accesos en Amazon S3 Glacier en la guía del desarrollador de S3 Glacier.
- ¿Cómo se crea una regla de ciclo de vida para un bucket de S3? (p. 50)
- ¿Cómo se anula la eliminación de objetos de S3? (p. 34)

¿Cómo puedo bloquear un objeto de Amazon S3?

El bloqueo de objetos de S3 le permite almacenar objetos en S3 con un modelo de escritura única y lectura múltiple (WORM). Puede usar el bloqueo de objetos de S3 para evitar que se elimine o se sobrescriba un objeto durante un periodo de tiempo determinado o de manera indefinida. Para obtener más información sobre cómo bloquear con la CLI de AWS, los SDK de AWS o las API de REST de Amazon S3, consulte

Bloqueo de objetos mediante el bloqueo de objetos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Para bloquear cualquier objeto debe permitir que el bucket use el bloqueo de objetos de S3. Activará el bloqueo de objetos al crear un bucket. Una vez activado el bloqueo de objetos en un bucket, puede bloquear objetos en ese bucket. Una vez que cree un bucket con bloqueo de objetos activado, no puede desactivar el bloqueo de objetos ni suspender el control de versiones en ese bucket.

Para obtener información acerca de cómo crear un bucket con bloqueo de objetos de S3 activado, consulte ¿Cómo se puede crear un bucket de S3? (p. 3).

Para bloquear un objeto de Amazon S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. En la lista Objects (Objetos), elija el nombre del objeto que desea bloquear.
4. Seleccione Properties (Propiedades).
5. Elija Object Lock (Bloquear objeto).
6. Elija un modo de retención. Puede cambiar la Retain until date (Fecha de finalización de retención). También puede optar por activar una retención legal. Para obtener más información, consulte el tema de descripción general del bloqueo de objetos de S3 en la guía del desarrollador de Amazon Simple Storage Service.
7. Elija Save (Guardar).

Más información

- Configuración de permisos de acceso a buckets y objetos (p. 66)

¿Cómo se ve la información general de un objeto?

En esta sección se explica cómo utilizar la consola de Amazon S3 para ver el panel de información general de un objeto. Este panel proporciona toda la información esencial de un objeto en un mismo lugar.

Para ver el panel de información general de un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket que contiene el objeto.
3. En la lista Name (Nombre), seleccione el nombre del objeto para el que desea ver la información general.
4. Para descargar el objeto, elija Download (Descargar) en el panel de información general del objeto. Para copiar la ruta del objeto en el portapapeles, elija Copy Path (Copiar ruta).
5. Si el bucket tiene activado el control de versiones, elija Latest versions (Últimas versiones) para ver la lista de las versiones del objeto. A continuación, puede hacer clic en el icono de descarga para descargar una versión de un objeto, o en el icono de papelera para eliminar una versión del objeto.

   Important

   Solo puede anular la eliminación de un objeto si se ha eliminado en su última versión (la más reciente). No puede anular la eliminación de una versión anterior de un objeto que se haya eliminado. Para obtener más información, consulte Versiones de objetos y Uso del control de versiones en la guía del desarrollador de Amazon Simple Storage Service.

Más información

- ¿Cómo se consultan las versiones de un objeto de S3? (p. 39)

¿Cómo se consultan las versiones de un objeto de S3?

En esta sección se explica cómo utilizar la consola de Amazon S3 para ver las distintas versiones de un objeto.

Un bucket con el control de versiones activado puede tener muchas versiones del mismo objeto: una versión actualizada (más reciente) y ninguna o varias versiones no actualizadas (previas). Amazon S3 le asigna a cada objeto un ID de versión único. Para obtener más información sobre la habilitación del control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8).

Si un bucket tiene el control de versiones activado, Amazon S3 crea otra versión de un objeto en las siguientes condiciones:

- Si carga un objeto que tiene el mismo nombre que un objeto que ya existe en el bucket, Amazon S3 crea otra versión del objeto en vez de sustituir el objeto existente.
- Si actualiza las propiedades del objeto después de cargarlo en el bucket, por ejemplo, si cambia los detalles de almacenamiento u otros metadatos, Amazon S3 crea una nueva versión del objeto en el bucket.

Para obtener más información sobre compatibilidad de versiones en Amazon S3, consulte Versiones de objetos y Uso del control de versiones en la guía del desarrollador de Amazon Simple Storage Service.

Para ver múltiples versiones de un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket que contiene el objeto.
3. Para ver una lista de las versiones de los objetos en el bucket, elija el modificador List versions (Listar versiones).

   Para cada versión de objeto, la consola muestra un ID de versión único, la fecha y la hora en que se creó la versión del objeto, y otras propiedades. (Los objetos almacenados en un bucket antes de establecer el estado del control de versiones tienen el ID de versión null (nulo)).

   Para listar los objetos sin las versiones, elija el modificador List versions (Listar versiones) .

También puede ver, descargar y eliminar las versiones de los objetos en el panel de información general de objetos. Para obtener más información, consulte ¿Cómo se ve la información general de un objeto? (p. 38).

> **Important**
>
> Solo puede anular la eliminación de un objeto si se ha eliminado en su última versión (la más reciente). No puede anular la eliminación de una versión anterior de un objeto que se haya eliminado. Para obtener más información, consulte Versiones de objetos y Uso del control de versiones en la guía del desarrollador de Amazon Simple Storage Service.

Más información

- ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8)
- ¿Cómo se crea una regla de ciclo de vida para un bucket de S3? (p. 50)

¿Cómo se consultan las propiedades de un objeto?

En esta sección se explica cómo usar la consola para ver las propiedades de un objeto.

Para ver las propiedades de un objeto:

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket que contiene el objeto.
3. En la lista Name (Nombre), seleccione el nombre del objeto para el que quiera ver las propiedades.
4. Seleccione Properties (Propiedades).
5. En la página Properties (Propiedades) podrá configurar las siguientes propiedades para el objeto.

   Note

   Si cambia las propiedades; Storage Class (Clase de almacenamiento), Enryption (Cifrado) o Metadata (Metadatos), se crea un nuevo objeto para reemplazar el antiguo. Si el control de versiones de S3 está activado, se crea una nueva versión del objeto y el objeto existente se convierte en una versión anterior. El rol que cambia la propiedad también se convierte en el propietario del nuevo objeto o (versión del objeto).

   a. Storage class (Clase de almacenamiento): todos los objetos de Amazon S3 tienen una clase de almacenamiento asociada. La clase de almacenamiento que quiera usar dependerá de la frecuencia con la que obtenga acceso al objeto. La clase predeterminada de almacenamiento para objetos de S3 es STANDARD. Puede seleccionar qué clase de almacenamiento usar al cargar un objeto. Para obtener más información sobre la replicación, consulte Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.

      Para cambiar la clase de almacenamiento tras cargar un objeto, seleccione Storage class (Clase de almacenamiento). Seleccione la clase de almacenamiento que desee y haga clic en Save (Guardar).

   b. Encryption (Cifrado): puede cifrar sus objetos de S3. Para obtener más información, consulte ¿Cómo se puede agregar cifrado a un objeto de S3? (p. 40).

   c. Metadata (Metadatos): cada objeto de Amazon S3 tiene un conjunto de pares nombre-valor que representan sus metadatos. Para obtener más información sobre la adición de metadatos a un objeto de S3, consulte Edición de metadatos de objeto (p. 42).

   d. Tags (Etiquetas): puede agregar etiquetas a un objeto de S3. Para obtener más información, consulte Edición de etiquetas de objeto (p. 44).

   e. Object lock (Bloqueo de objeto) : puede evitar que se elimine un objeto.

¿Cómo se puede agregar cifrado a un objeto de S3?

En este tema se describe cómo configurar o cambiar el tipo de cifrado que utiliza un objeto mediante la consola de Amazon S3.

Note

Si cambia el cifrado de un objeto, se crea un nuevo objeto para reemplazar el antiguo. Si el control de versiones de S3 está activado, se crea una nueva versión del objeto y el objeto existente se convierte en una versión anterior. El rol que cambia la propiedad también se convierte en el propietario del nuevo objeto o (versión del objeto).

Para añadir o cambiar el cifrado de un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Bucket, seleccione el nombre del bucket que contiene el objeto.
3. En la lista Name (Nombre), seleccione el nombre del objeto al que desea añadir cifrado o cuyo cifrado desea modificar.
4. Seleccione Properties (Propiedades) y luego Encryption (Cifrado).

   Se abre el cuadro de diálogo Encryption (Cifrado), que ofrece tres opciones para el cifrado de objetos:

   - None (Ninguno): no se aplica ningún cifrado a los objetos.
   - AES-256: cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3).
   - AWS-KMS: cifrado del lado del servidor con claves maestras de cliente (SSE-KMS) de AWS Key Management Service (AWS KMS).
5. Si desea quitar el cifrado de un objeto que ya tiene la configuración de cifrado, elija None (Ninguno) y, a continuación, Save (Guardar).
6. Si desea cifrar el objeto mediante claves administradas por Amazon S3, siga estos pasos:

   a. Elija AES-256.

      Para obtener más información sobre el uso del cifrado del lado del servidor de Amazon S3 para cifrar los datos, consulte la sección sobre Protección de datos con clases de clave de cifrado administrados por Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

   b. Elija Save (Guardar).
7. Si desea cifrar su objeto mediante AWS KMS, siga estos pasos:

   a. Elija AWS-KMS.

   b. Elija una clave maestra de cliente (CMK) de AWS KMS.

      La lista muestra las CMK administradas por el cliente que ha creado y la CMK administrada por AWS para Amazon S3. Para obtener más información sobre cómo crear un AWS KMS CMK gestionado por el cliente, consulte el capítulo sobre creación de claves en la guía para desarrolladores de AWS Key Management Service

      Important

      La consola de Amazon S3 solo enumera 100 CMK de AWS KMS por región de AWS. Si tiene más de 100 CMK en la misma región, sólo podrá ver las primeras 100 CMK en la consola S3. Para utilizar una CMK de KMS que no aparece en la consola, elija ARN de KMS personalizado y escriba el ARN de la CMK de KMS.

   c. Elija Save (Guardar).

      Important

      Para cifrar los objetos del bucket, puede usar solo las CMK habilitadas en la misma región de AWS que el bucket. Amazon S3 solo admite CMK simétricas. Amazon S3 no admite CMK asimétricas. Para obtener más información, consulte Uso de claves simétricas y asimétricas.

8. Para permitir que una cuenta externa use un objeto protegido con una CMK de AWS KMS, siga estos pasos:

   a. Elija AWS-KMS.
   b. Escriba el nombre de recurso de Amazon (ARN) para la cuenta externa.
   c. Elija Save (Guardar).

      Los administradores de una cuenta externa que tienen permisos de uso de un objeto protegido por su CMK de KMS CMK pueden restringir aún más el acceso mediante la creación de una política AWS Identity and Access Management (IAM) de nivel de recursos.

   Note

   En esta acción se aplica el cifrado a todos los objetos especificados. Al cifrar carpetas, espere a que finalice la operación de guardado antes de agregar nuevos objetos a la carpeta.

Más información

- ¿Cómo puedo habilitar el cifrado predeterminado para un bucket de Amazon S3? (p. 8)
- Cifrado predeterminado de Amazon S3 para los buckets de S3 en la guía del desarrollador de Amazon Simple Storage Service
- ¿Cómo se consultan las propiedades de un objeto? (p. 40)
- Cargar, descargar y administrar objetos. (p. 27)

Edición de metadatos de objeto

En esta sección se explica cómo utilizar la consola de Amazon S3 para editar metadatos de objetos de S3 existentes. Cada objeto de Amazon S3 puede tener un conjunto de pares clave-valor que proporcione metadatos, que son información adicional sobre el objeto. Algunos metadatos son configurados por Amazon S3 cuando carga el objeto. Por ejemplo, `Content-Length` es la clave (nombre) y el valor es el tamaño del objeto en bytes.

También puede configurar algunos metadatos cuando cargue el objeto, o después, puede editarlo a medida que cambien las necesidades. Por ejemplo, puede tener un conjunto de objetos que inicialmente almacene en la clase de almacenamiento `STANDARD`. Con el tiempo, es posible que ya no necesite que estos datos estén altamente disponibles y cambie la clase de almacenamiento a `GLACIER` editando el valor de la clave `x-amz-storage-class` de `STANDARD` a `GLACIER`.

Hay dos clases de metadatos para un objeto de S3: metadatos del sistema y metadatos definidos por el usuario de Amazon S3:

- Metadatos definidos por el sistema: dentro de los metadatos del sistema, hay dos categorías.
  - Los metadatos, como la fecha `Last-Modified` son controlados por el sistema y solo Amazon S3 puede modificar el valor.
  - También hay metadatos del sistema que puede modificar, por ejemplo, la clase de almacenamiento del objeto o el tipo de cifrado.
- Metadatos definidos por el usuario: puede definir sus propios metadatos personalizados, denominados metadatos definidos por el usuario, que asigne a un objeto al cargar el objeto o después de que se haya cargado el objeto. Los metadatos definidos por el usuario se almacenan con el objeto y se devuelven cuando lo descarga. Amazon S3 no procesa metadatos definidos por el usuario.

En los temas siguientes se describe cómo editar metadatos de un objeto mediante la consola de Amazon S3.

Temas

Note

- Esta acción crea una copia del objeto con la configuración actualizada y la fecha de última modificación. Si el control de versiones de S3 está activado, se crea una nueva versión del objeto y el objeto existente se convierte en una versión anterior. El rol de IAM que cambia la propiedad también se convierte en el propietario del nuevo objeto o (versión del objeto).
- La edición de metadatos actualiza los valores de los nombres de clave existentes.
- Los objetos cifrados con claves de cifrado proporcionadas por el cliente (SSE-C) no se pueden copiar mediante la consola y deben utilizar la CLI de AWS, AWS SDK o la API de REST de Amazon S3.

Warning

- Al editar metadatos a carpetas, espere a que finalice la operación de edición de metadatos antes de agregar nuevos objetos a la carpeta. De lo contrario, es posible que también se editen nuevos objetos.
- Los objetos cifrados con claves de cifrado proporcionadas por el cliente (SSE-C) no se pueden copiar mediante la consola y deben utilizar la CLI de AWS, AWS SDK o la API de REST de Amazon S3.

Para obtener más información acerca de los metadatos de objetos, incluidos los límites y directrices de nomenclatura, consulte Metadatos de objeto en la guía del desarrollador de Amazon Simple Storage Service.

Edición de metadatos definidos por el sistema

Puede configurar algunos metadatos del sistema para un objeto de S3, pero no todos. Para obtener una lista de metadatos definidos por el sistema y si puede modificar sus valores, consulte Metadatos definidos por el sistema en la guía para desarrollador de Amazon Simple Storage Service.

Para editar metadatos definidos por el sistema de un objeto, realice las siguientes acciones:

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Desplácese hasta el bucket o carpeta de Amazon S3 y active la casilla de verificación situada a la izquierda de los nombres de los objetos con los metadatos que desee editar.
3. Abra el menú Action (Acción), vaya a la sección Edit actions (Editar acciones) y elija Edit metadata (Editar metadatos).
4. Revise los objetos que aparecen y elija Add metadata (Añadir metadatos).
5. Para el tipo de metadatos, seleccione System-defined (Definidos por el sistema).
6. Especifique una clave única y el valor de los metadatos.
7. Para editar metadatos adicionales, elija Add metadata (Añadir metadatos). También puede elegir Remove (Eliminar) para eliminar un conjunto de valores de clave-tipo.
8. Cuando haya terminado, elija Save changes (Guardar cambios) y Amazon S3 editará los metadatos de los objetos especificados.

Edición de metadatos definidos por el usuario

Puede editar metadatos definidos por el usuario de un objeto combinando el prefijo de metadatos, `x-amz-meta-` y un nombre que elija para crear una clave personalizada. Por ejemplo, si añade el nombre personalizado `alt-name`, la clave de los metadatos será `x-amz-meta-alt-name`. Los metadatos definidos por el usuario pueden tener un tamaño de hasta 2 KB. Tanto las claves como sus valores deben cumplir los estándares del American Standard Code for Information Interchange (ASCII, Código Estándar Estadounidense para el Intercambio de Información) de los EE. UU. Para obtener más información, consulte Metadatos definidos por el usuario en la guía del desarrollador de Amazon Simple Storage Service.

Para editar metadatos definidos por el usuario de un objeto, realice las siguientes acciones:

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Desplácese hasta el bucket o carpeta de Amazon S3 y active la casilla de verificación situada a la izquierda de los nombres de los objetos con los metadatos que desee editar.
3. Abra el menú Action (Acción), vaya a la sección Edit actions (Editar acciones) y elija Edit metadata (Editar metadatos).
4. Revise los objetos que aparecen y elija Add metadata (Añadir metadatos).
5. Para el tipo de metadatos, seleccione User-defined (Definidos por el usuario).
6. Introduzca una clave única y personalizada después de `x-amz-meta-`. Introduzca también un valor de metadatos.
7. Para añadir metadatos adicionales, elija Add metadata (Añadir metadatos). También puede elegir Remove (Eliminar) para eliminar un conjunto de valores de clave-tipo.
8. Cuando haya terminado, elija Save changes (Guardar cambios) y Amazon S3 editará los metadatos de los objetos especificados.

Más información

- ¿Cómo se consultan las propiedades de un objeto? (p. 40)
- Cargar, descargar y administrar objetos. (p. 27)

Edición de etiquetas de objeto

El etiquetado de objetos le permite categorizar el almacenamiento. En este tema se explica cómo utilizar la consola para añadir etiquetas a un objeto de S3 después de cargarlo. Para obtener información sobre cómo añadir etiquetas a un objeto cuando este se está cargando, consulte ¿Cómo puedo cargar archivos y carpetas en un bucket de S3? (p. 28).

Cada etiqueta es un par clave-valor que se ajusta a las reglas siguientes:

- Puede asociar hasta 10 etiquetas a un objeto. Las etiquetas asociadas con un objeto deben tener claves de etiquetas exclusivas.
- Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 256 caracteres Unicode.
- Los valores de clave y de etiqueta distinguen entre mayúsculas y minúsculas.

Para obtener más información acerca de las etiquetas de objeto, consulte Etiquetado de objetos en la guía del desarrollador de Amazon Simple Storage Service. Para obtener más información sobre restricciones

en las etiquetas, consulte Restricciones de las etiquetas definidas por el usuario en la guía del usuario de Administración de costos y facturación de AWS.

Para añadir etiquetas a un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Desplácese hasta el bucket o carpeta de Amazon S3 y active la casilla de verificación situada a la izquierda de los nombres de los objetos a los que desee agregar etiquetas.
3. Abra el menú Action (Acción), vaya a la sección Edit actions (Editar acciones) y elija Edit Tags (Editar etiquetas).
4. Revise los objetos que aparecen y elija Add tags (Agregar etiquetas).
5. Cada etiqueta de objeto es un par clave-valor. Introduzca la información pertinente en Key (Clave) y Value (Valor). Para agregar otra etiqueta, elija Add Tag (Añadir etiqueta). Cuando haya terminado, elija Save changes (Guardar cambios). Amazon S3 agregará las etiquetas a los objetos especificados.

   Puede introducir hasta 10 etiquetas para un objeto.

Para obtener más información, consulte ¿Cómo se consultan las propiedades de un objeto? (p. 40) y Cargar, descargar y administrar objetos. (p. 27) en esta guía.

¿Cómo puedo utilizar carpetas en un bucket de S3?

En Amazon S3, los buckets y objetos son los principales recursos, y los objetos se almacenan en buckets. Amazon S3 tiene una estructura sin formato en lugar de una jerarquía como la que vería en un sistema de archivos. Sin embargo, para la simplicidad organizativa, la consola de Amazon S3 admite el concepto de carpetas como medio para agrupar objetos. Amazon S3 lo hace utilizando un prefijo de nombre compartido para objetos (es decir, objetos que tienen nombres que empieza por una cadena común). Los nombres de objetos también se denominan nombres de clave.

Por ejemplo, puede crear una carpeta en la consola denominada `photos` y almacenar un objeto denominado `myphoto.jpg` en ella. El objeto luego se guarda con el nombre de clave `photos/myphoto.jpg`, donde el prefijo es `photos/`.

A continuación se incluyen dos ejemplos más:

- Si tiene tres objetos en su bucket, `logs/date1.txt`, `logs/date2.txt` y `logs/date3.txt`, la consola mostrará una carpeta con el nombre `logs`. Si abre la carpeta en la consola, verá tres objetos: `date1.txt`, `date2.txt` y `date3.txt`.
- Si tiene un objeto con el nombre `photos/2017/example.jpg`, la consola le mostrará una carpeta con el nombre `photos` que contiene la carpeta `2017` y el objeto `example.jpg`.

Temas

Puede tener carpetas dentro de carpetas, pero no buckets dentro de buckets. Puede cargar y copiar objetos directamente en una carpeta. Puede crear, eliminar y hacer públicas las carpetas, pero no les puede cambiar el nombre. Los objetos se pueden copiar de una carpeta a otra.

Important

- La consola de Amazon S3 implementa la creación de objetos de carpeta mediante la creación de objetos de cero bytes con el valor de prefijo y delimitador de carpeta como clave. Estos objetos de carpeta no aparecen en la consola. De lo contrario, se comportan como cualquier otro objeto y se pueden ver y manipular a través de la API de REST, la CLI de AWS y los SDK de AWS.
- La consola de Amazon S3 trata como una carpeta a todos los objetos que tienen un carácter de barra inclinada "/" como último carácter (final) en el nombre de clave, por ejemplo `examplekeyname/`. No se puede cargar un objeto que tiene un nombre de clave con un carácter «/» final mediante la consola de Amazon S3. Sin embargo, los objetos cuyos nombres incluyen una «/» final se pueden cargar con la API de Amazon S3 a través de la CLI de AWS, los SDK de AWS o la API de REST.
- Un objeto cuyo nombre incluye una «/» final se muestra como una carpeta en la consola de Amazon S3. La consola de Amazon S3 no muestra el contenido ni los metadatos para dicho objeto. Si se usa la consola para copiar un objeto cuyo nombre incluye una «/» final, se crea una nueva carpeta en la ubicación de destino pero los datos y metadatos del objeto no se copian.

Creación de una carpeta

En esta sección se describe cómo utilizar la consola de Amazon S3 para crear una carpeta.

Important

Si su política de buckets impide cargar objetos a este bucket sin cifrado, etiquetas, metadatos o beneficiarios de listas de control de acceso (ACL), no podrá crear una carpeta con esta configuración. En lugar de eso, cargue una carpeta vacía y especifique estos parámetros en la configuración de carga.

Para crear una carpeta

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket donde desea crear una carpeta.
3. Elija Create folder.
4. Escriba un nombre para la carpeta (por ejemplo, **`favorite-pics`**). A continuación, haga clic en Create folder (Crear carpeta).

¿Cómo se pueden eliminar carpetas de un bucket de S3?

En esta sección se explica cómo utilizar la consola de Amazon S3 para eliminar carpetas de un bucket de S3.

Para obtener información sobre las características y precios de Amazon S3, consulte Amazon S3.

Para eliminar carpetas de un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket del que desea eliminar las carpetas.

3. En la lista Name (Nombre), tilde la casilla junto a las carpetas y los objetos que desea eliminar, seleccione Actions (Acciones) y, luego, seleccione Delete (Eliminar).
4. En la página Delete objects (Eliminar objetos), compruebe que aparezcan los nombres de las carpetas que seleccionó para eliminar. Introduzca **`delete`** en la casilla proporcionada y haga clic en Delete objects (Eliminar objetos).

   Warning

   Esta acción elimina todos los objetos especificados. Al eliminar carpetas, espere a que finalice la acción de eliminación antes de agregar nuevos objetos a la carpeta. De lo contrario, es posible que también se eliminen objetos nuevos.

Temas relacionados

- Eliminación de objetos (p. 33)

Hacer púbicas las carpetas

Amazon S3 tiene una estructura sin formato en lugar de una jerarquía como la que vería en un sistema de archivos. Sin embargo, para la simplicidad organizativa, la consola de Amazon S3 admite el concepto de carpetas como medio para agrupar objetos. En Amazon S3, la carpeta es un prefijo de nomenclatura para un objeto o grupo de objetos. Para obtener más información, consulte ¿Cómo puedo utilizar carpetas en un bucket de S3? (p. 45)

Le recomendamos bloquear todo el acceso público a sus carpetas de Amazon S3 y buckets a menos que requiera específicamente una carpeta o bucket público. Al hacer pública una carpeta, cualquier persona en Internet puede ver todos los objetos que están agrupados en dicha carpeta. En la consola de Amazon S3, puede hacer pública una carpeta. También puede hacer pública una carpeta creando una política de bucket que limite el acceso mediante prefijo. Para obtener más información, consulte Configuración de permisos de acceso a buckets y objetos (p. 66).

Warning

Después de hacer una carpeta pública en la consola de Amazon S3, no puede volver a hacerla privada. En lugar de ello, debe definir permisos en cada objeto individual en la carpeta pública para que los objetos no tengan acceso público. Para obtener más información, consulte ¿Cómo puedo configurar permisos en un objeto? (p. 69)

Más información

- ¿Cómo se pueden eliminar carpetas de un bucket de S3? (p. 46)
- ¿Cómo se configuran permisos de buckets de ACL? (p. 71)
- ¿Cómo se bloquea el acceso público a los buckets de S3? (p. 67)

Introducción a Operaciones por lote en S3

Operaciones por lotes de S3 permite realizar operaciones por lotes a gran escala en objetos de Amazon S3. Puede utilizar Operaciones por lotes de S3 para copiar objetos, establecer etiquetas de objetos o listas de control de acceso (ACL), iniciar restauraciones de objetos desde Amazon S3 Glacier o invocar una función de AWS Lambda para realizar acciones personalizadas con sus objetos. Puede realizar estas operaciones en una lista personalizada de objetos o puede utilizar un informe de inventario de Amazon S3 para que la generación de las listas de objetos más grandes sea sencilla. Operaciones por lotes de S3 usa las mismas API de Amazon S3 que ya utiliza, por lo que la interfaz le resultará familiar. Para obtener información sobre cómo aplicar Operaciones por lotes de S3 mediante la CLI de AWS, AWS SDK y las API de REST de Amazon S3, consulte Aplicación de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service.

En los siguientes temas, se explica cómo utilizar la consola de Amazon S3 para configurar y ejecutar operaciones por lotes.

Temas

Creación de trabajos de operaciones por lotes de S3

En esta sección se describe cómo crear un trabajo de operaciones por lotes de S3. Para obtener información sobre cómo realizar operaciones por lotes en S3 con la CLI de AWS, los SDK de AWS y las API de REST de Amazon S3, consulte Ejecutar Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service.

Para crear un trabajo por lotes

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione Batch Operations (Operaciones por lotes) en el panel de navegación de la consola de Amazon S3.
3. Seleccione Create job (Crear trabajo).
4. Elija en Region (Región) la región en la que desea crear el trabajo.
5. En Manifest format (Formato del manifiesto), seleccione el tipo de objeto del manifiesto que desee usar.

   - Si elige S3 Inventory report (Informe de inventario de S3), escriba la ruta del objeto manifest.json que Amazon S3 ha generado con el informe de inventario con formato CSV. También puede seleccionar el ID de versión del objeto del manifiesto en caso de que desee utilizar otra versión que no sea la más reciente.
   - Si selecciona CSV, escriba la ruta del objeto del manifiesto con formato CSV. El objeto del manifiesto debe tener el mismo formato que se ha especificado en la consola. Si quiere utilizar otra versión que no sea la más reciente, puede incluir el ID de versión del objeto del manifiesto.

6. Elija Next (Siguiente).
7. En Operation (Operación), seleccione la operación que desee en todos los objetos que aparecen en el manifiesto. Rellene los datos de la operación seleccionada y haga clic en Next (Siguiente).
8. Rellene los datos de Configure additional options (Configurar otras opciones) y haga clic en Next (Siguiente).
9. En Review (Revisar), compruebe la configuración. Si necesita realizar cambios, seleccione Previous (Anterior). De lo contrario, seleccione Create Job (Crear trabajo).

Más información

- Conceptos básicos de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service.
- Crear un trabajo de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service
- Operaciones en la guía del desarrollador de Amazon Simple Storage Service

Administración de trabajos de operaciones por lotes de S3

Amazon S3 dispone de un conjunto de herramientas que le ayudarán a administrar los trabajos de operaciones por lotes de S3 una vez que los haya creado. Para obtener más información acerca de cómo administrar las operaciones por lotes de S3, consulte Administrar trabajos de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service.

Más información

- Conceptos básicos de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service.
- Crear un trabajo de Operaciones por lotes de S3 en la guía del desarrollador de Amazon Simple Storage Service
- Operaciones en la guía del desarrollador de Amazon Simple Storage Service

Administrar el almacenamiento

En esta sección se explica cómo configurar las herramientas de administración del almacenamiento en Amazon S3.

Temas

¿Cómo se crea una regla de ciclo de vida para un bucket de S3?

Puede usar las reglas de ciclo de vida para definir acciones que quiera que realice Amazon S3 durante el periodo de vida de un objeto (por ejemplo, la transición de objetos a otra clase de almacenamiento, su archivado o su eliminación tras transcurrir un periodo de tiempo especificado).

Puede definir una regla de ciclo de vida para todos los objetos o para un subconjunto de objetos del bucket mediante un prefijo compartido (nombres de objetos que comienzan por una cadena común) o una etiqueta.

Mediante una regla de ciclo de vida puede definir acciones específicas a las versiones de objetos actualizadas y no actualizadas. Para obtener más información, consulte Administración del ciclo de vida de los objetos, Control de versiones de objetos y Uso del control de versiones en la guía del desarrollador de Amazon Simple Storage Service.

Para crear una regla de ciclo de vida

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket para el que desea crear una regla de ciclo de vida.
3. Seleccione la pestaña Management (Administración) y seleccione Create lifecycle rule (Crear regla de ciclo de vida).
4. En Lifecycle rule name (Nombre de regla de ciclo de vida), escriba un nombre para la regla.

   El nombre debe ser único dentro del bucket.
5. Elija el ámbito de la regla de ciclo de vida:

   - Para aplicar esta regla de ciclo de vida a todos los objetos con un prefijo o etiqueta específicos, elija Limit the scope to specific prefixes or tags (Limitar el ámbito a prefijos o etiquetas específicos).

- Para limitar el ámbito por prefijo, en Prefix (Prefijo), escriba el prefijo.
- Para limitar el ámbito por etiqueta, seleccione Add tag (Agregar etiqueta) e introduzca la clave y el valor de la etiqueta.

Para obtener más información acerca de los prefijos de nombres de objeto, consulte Object Keys (Claves de objetos) en la guía del desarrollador de Amazon Simple Storage Service. Para obtener más información acerca de las etiquetas de objeto, consulte Etiquetado de objetos en la guía del desarrollador de Amazon Simple Storage Service.

- Para aplicar esta regla de ciclo de vida a todos los objetos del bucket, seleccione This rule applies to all objects in the bucket (Esta regla se aplica a todos los objetos del bucket) y seleccione I acknowledge that this rule applies to all objects in the bucket (Reconozco que esta regla se aplica a todos los objetos del bucket).

6. En Lifecycle rule actions (Acciones de regla de ciclo de vida), elija las acciones que desea que realice la regla de ciclo de vida:

   - Realizar la transición de versiones de objetos actuales entre clases de almacenamiento
   - Realizar la transición de versiones de objetos anteriores entre clases de almacenamiento
   - Caducar las versiones de objetos actuales
   - Eliminar permanentemente versiones de objetos anteriores
   - Eliminar marcadores de eliminación caducados o cargas multiparte incompletas

   Dependiendo de las acciones que elija, aparecerán diferentes opciones.

7. Para realizar la transición de versiones de objetos actuales entre clases de almacenamiento, en Transition current versions of objects between storage classes (Realizar la transición de versiones de objetos actuales entre clases de almacenamiento):

   a. En Storage class transitions (Transiciones de clase de almacenamiento), seleccione la clase de almacenamiento a la que quiera realizar la transición:

      - Estándar - Acceso poco frecuente
      - Intelligent-Tiering (Capas avanzadas)
      - Única zona – Acceso poco frecuente
      - Glacier
      - Glacier Deep Archive

   b. En Days after object creation (Días después de la creación del objeto), introduzca el número de días posteriores a la creación del objeto en los que quiera realizar la transición.

   Para obtener más información sobre la replicación, consulte Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service. Puede definir transiciones para versiones de objetos actuales o anteriores, o tanto para las actuales como para las anteriores. El control de versiones le permite mantener varias versiones de un objeto en un bucket. Para obtener más información sobre el control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8).

   Important

   Si elige la clase de almacenamiento Glacier o Glacier Deep Archive, sus objetos permanecen en Amazon S3. No puede acceder a ellos directamente a través del servicio independiente de Amazon S3 Glacier. Para obtener más información, consulte Transición de objetos con el ciclo de vida de Amazon S3.

8. Para realizar la transición de versiones de objetos no actuales entre clases de almacenamiento, en Transition non-current versions of objects between storage classes (Realizar la transición de versiones de objetos no actuales entre clases de almacenamiento):

a. En Storage class transitions (Transiciones de clase de almacenamiento), seleccione la clase de almacenamiento a la que quiera realizar la transición:

   - Estándar - Acceso poco frecuente
   - Intelligent-Tiering (Capas avanzadas)
   - Única zona – Acceso poco frecuente
   - Glacier
   - Glacier Deep Archive

b. En Days after object becomes non-current (Días después de que el objeto se vuelve no actual), introduzca el número de días posteriores a la creación del objeto en los que quiera realizar la transición.

9. Para hacer caducar versiones de objetos actuales, bajo Expire previous versions of objects (Hacer caducar versiones de objetos anteriores), en Number of days after object creation (Número de días después de la creación del objeto), introduzca el número de días.

   Important

   En un bucket sin control de versiones, la acción de vencimiento da como resultado que Amazon S3 elimine de forma permanente el objeto. Para obtener más información acerca de las acciones del ciclo de vida, consulte Elementos para describir las acciones del ciclo de vida en la guía del desarrollador de Amazon Simple Storage Service.

10. Para eliminar permanentemente versiones anteriores de objetos, bajo Permanently delete previous versions of objects (Eliminar permanentemente versiones anteriores de objetos), en Number of days after objects become previous versions (Número de días después de que los objetos se vuelven versiones anteriores), escriba el número de días.
11. Bajo Delete expired markers or incomplete multipart uploads (Eliminar marcadores caducados o cargas multiparte incompletas), seleccione Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados) y Delete incomplete multipart uploads (Eliminar cargas multiparte incompletas). A continuación, escriba el número de días que han de transcurrir entre el inicio de la carga multiparte y el momento en que quiera finalizarla y limpiar las cargas incompletas.

    Para obtener más información acerca de las cargas multiparte, consulte Multipart Upload Overview (Información general de carga multiparte) en la guía del desarrollador de Amazon Simple Storage Service.
12. Elija Create rule.

    Si la regla no contiene ningún error, Amazon S3 la habilita y se puede ver en la ficha Management (Administración) en Lifecycle rules (Reglas del ciclo de vida).

¿Cómo puedo agregar una regla de replicación a un bucket de S3?

La replicación consiste en la copia automática y asincrónica de los objetos de los buckets en las mismas o diferentes regiones de AWS. La replicación copia los objetos creados recientemente y las actualizaciones de objetos de un bucket de origen en un bucket de destino. Para obtener más información acerca de los conceptos de replicación y cómo usar la replicación con la CLI de AWS, los AWS SDK y las API de REST de Amazon S3, consulte Replicación en la guía del desarrollador de Amazon Simple Storage Service.

La replicación requiere la activación del control de versiones en los buckets de origen y de destino. Para examinar la lista completa de requisitos, consulte Requisitos para replicación en la guía del desarrollador de Amazon Simple Storage Service. Para obtener más información sobre el control de versiones, consulte ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8).

Las réplicas de objetos en el bucket de destino son réplicas exactas de los objetos en el bucket de origen. Tienen los mismos nombres de clave y los mismos metadatos, por ejemplo, fecha y hora de creación, propietario, metadatos definidos por el usuario, ID de versión, lista de control de acceso (ACL) y clase de almacenamiento. Si lo desea, puede especificar explícitamente otra clase de almacenamiento para las réplicas de objetos. E independientemente de quién sea el propietario del bucket de origen o del objeto de origen, puede elegir cambiar la titularidad de la réplica a la cuenta de AWS que posee el bucket de destino. Para obtener más información, consulte Cambio del propietario de la réplica en la guía del desarrollador de Amazon Simple Storage Service.

Puede utilizar S3 Replication Time Control (S3 RTC) para replicar sus datos en la misma región de AWS o en distintas regiones de AWS dentro de un periodo de tiempo predecible. S3 RTC replica el 99,99 % de los objetos nuevos almacenados en Amazon S3 dentro de un plazo de 15 minutos y la mayoría de los objetos en solo unos segundos. Para obtener más información, consulte el artículo sobre replicación de objetos mediante el control de tiempo de replicación de S3 (S3 RTC) en la guía del desarrollador de Amazon Simple Storage Service.

> Nota sobre las reglas de replicación y de ciclo de vida
>
> Los metadatos de un objeto permanecerán idénticos entre los objetos originales y los objetos replicados. Las reglas de los ciclos de vida se atienen al momento de creación del objeto original, y no al momento en el que el objeto replicado queda disponible en el bucket de destino. Sin embargo, el ciclo de vida no actúa sobre los objetos que están pendientes de replicación hasta que la replicación se haya completado.

Para agregar reglas de replicación al bucket de origen se utiliza la consola de Amazon S3. Las reglas de replicación definen qué objetos del bucket de origen se deben replicar y el bucket de destino en que se almacenan los objetos replicados. Puede crear una regla para replicar todos los objetos en un bucket o un subconjunto de objetos con un prefijo de nombre de clave específico, una o varias etiquetas de objeto, o ambos métodos. El bucket de destino puede estar en la misma cuenta de AWS que el bucket de origen, o puede estar en una cuenta diferente.

Si especifica el ID de versión de objeto que desea eliminar, Amazon S3 elimina esa versión del objeto en el bucket de origen. Pero no replica la eliminación en el bucket de destino. En otras palabras, no elimina la misma versión del objeto del bucket de destino. Esto protege los datos de eliminaciones malintencionadas.

Si el bucket de destino está en una cuenta distinta de la del bucket de origen, se debe añadir una política de bucket al bucket de destino para conceder al propietario de la cuenta del bucket de origen permiso para replicar objetos en el bucket de destino. Para obtener más información, consulte Concesión de permisos cuando los buckets de origen y destino son propiedad de diferentes cuentas de AWS en la guía del desarrollador de Amazon Simple Storage Service.

Cuando se añade una regla de replicación a un bucket, la regla está activada de forma predeterminada, por lo que comienza a funcionar tan pronto como se guarda.

Temas

Adición de una regla de replicación

Siga estos pasos para configurar una regla de replicación cuando el bucket de destino está en la misma cuenta de AWS que el bucket de origen.

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.

2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. Elija Management (Administración), desplácese hacia abajo hasta Replication rules (Reglas de replicación) y, a continuación, elija Create replication rule (Crear regla de replicación).
4. En Rule name (Nombre de la regla), escriba un nombre para la regla, de modo que pueda identificarla fácilmente más tarde. El nombre es obligatorio y debe ser único dentro del bucket.
5. Configure un rol de AWS Identity and Access Management (IAM) que Amazon S3 pueda asumir para replicar objetos en su nombre.

   Para configurar un rol de IAM, en la sección Configuración de regla de replicación en Rol de IAM, realice una de las siguientes acciones:

   - Es absolutamente recomendable que elija Create new role (Crear nuevo rol) para que Amazon S3 cree un nuevo rol de IAM automáticamente. Cuando se guarda la regla, se genera una política nueva para el rol de IAM que coincide con los buckets de origen y de destino elegidos. El nombre del rol generado se basa en los nombres de los buckets y utiliza la siguiente convención de nomenclatura: replication_role_for_***`bucket-de-origen`***_to_***`bucket-de-destino`***.
   - Puede elegir usar un rol de IAM existente. Si lo hace, debe elegir un rol que conceda a Amazon S3 los permisos necesarios para la replicación. La replicación dará un error si este rol no concede a Amazon S3 permisos suficientes para seguir la regla de replicación.

     Important

     Cuando añada una regla de replicación a un bucket, debe tener el permiso `iam:PassRole` para poder pasar el rol de IAM que concede los permisos de replicación de Amazon S3. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS en la guía del usuario de IAM.
6. En Status (Estado), compruebe que Enabled (Habilitado) esté seleccionado de forma predeterminado. Una regla activada comienza a funcionar tan pronto se guarda. Si desea habilitar la regla más adelante, seleccione Disabled (Deshabilitada).
7. Si el bucket tiene reglas de replicación existentes, se le indicará que establezca una prioridad para la regla. Debe establecer una prioridad para la regla para evitar conflictos causados por objetos incluidos en el ámbito de más de una regla. En caso de solaparse las reglas, Amazon S3 usará la prioridad de la regla para determinar la regla que se va a aplicar. Cuanto mayor sea el número, mayor será la prioridad. Para obtener más información sobre la prioridad de la regla, consulte la sección de información general de la configuración de replicación en la guía del desarrollador de Amazon Simple Storage Service.
8. En Replication rule configuration (Configuración de reglas de replicación), en Source bucket (Bucket de origen), tiene las siguientes opciones para establecer el origen de la replicación:

   - Para replicar todo el bucket, elija This rule applies to all objects in the bucket (Esta regla se aplica a todos los objetos del bucket).
   - Para replicar todos los objetos que tengan mismo prefijo, elija Limit the scope of this rule using one or more filters (Limitar el ámbito de esta regla mediante uno o varios filtros). Esto limitará la replicación a todos los objetos que tengan nombres que comiencen por la cadena (por ejemplo `pictures`). Introduzca un prefijo en el cuadro.

     Note

     Si utiliza un prefijo que es el nombre de una carpeta, debe introducir / (barra inclinada) como último carácter (por ejemplo, `pictures/`).
   - Para replicar todos los objetos con una o varias etiquetas de objeto, seleccione Add tag (Agregar etiqueta) e introduzca el par de valores clave en los cuadros. Repita el procedimiento para añadir otra etiqueta. Puede hacer uso combinado de un prefijo y etiquetas. Para obtener más información acerca de las etiquetas de objeto, consulte Etiquetado de objetos en la guía del desarrollador de Amazon Simple Storage Service.

El nuevo esquema admite el filtrado por prefijos y etiquetas y la priorización de reglas. Para obtener más información acerca del nuevo esquema, consulte la sección Compatibilidad con versiones anteriores en el artículo Información general de la configuración de replicación en la guía del desarrollador de Amazon Simple Storage Service. En la guía para desarrolladores se describe el XML usado con la API de Amazon S3 que funciona detrás de la interfaz de usuario. En la guía para desarrolladores, el nuevo esquema se describe como el XML de configuración de replicación V2.

9. En Destination (Destino), tiene las siguientes opciones para establecer el destino de replicación:

   - Para replicar en un bucket de su cuenta, seleccione Choose a bucket in this account (Elegir un bucket en esta cuenta) y escriba o busque el bucket de destino.
   - Para replicar en un bucket de una cuenta de AWS diferente, seleccione Choose a bucket in another account (Elegir un bucket en otra cuenta) e introduzca el ID de cuenta del bucket de destino y escriba el nombre del bucket de destino.

     Si el bucket de destino está en una cuenta distinta de la del bucket de origen, se debe añadir una política de bucket al bucket de destino para conceder al propietario de la cuenta del bucket de origen permiso para replicar objetos en el bucket de destino. Para obtener más información, consulte Concesión de permisos cuando los buckets de origen y destino son propiedad de diferentes cuentas de AWS en la guía del desarrollador de Amazon Simple Storage Service.

     Note

     Si el control de versiones no está habilitado en el bucket de destino, recibirá una advertencia que contiene el botón Enable versioning (Habilitar el control de versiones). Elija este botón para activar el control de versiones en el bucket.

10. Si desea habilitar Object Ownership (Propiedad de objeto) para ayudar a estandarizar la propiedad de nuevos objetos en el bucket de destino, elija Change object ownership to the destination bucket owner (Cambiar la propiedad del objeto al propietario del bucket de destino). Para obtener más información acerca de esta opción, consulte Meet compliance requirements using S3 RTC (Cumplir los requisitos de cumplimiento mediante S3 RTC) en la guía del desarrollador de Amazon Simple Storage Service.

    Si desea replicar sus datos en una clase de almacenamiento específica del bucket de destino, elija Change the storage class for the replicated object(s) (Modificar la clase de almacenamiento para los objetos replicados). A continuación, elija la clase de almacenamiento que desea utilizar para los objetos replicados en el bucket de destino. Si no selecciona esta opción, la clase de almacenamiento de los objetos replicados es la misma que la de los objetos originales.

    Si desea habilitar S3 Replication Time Control (S3 RTC) en la configuración de replicación, seleccione S3 Replication Time Control. Para obtener más información acerca de esta opción, consulte Meet compliance requirements using S3 RTC (Cumplir los requisitos de cumplimiento mediante S3 RTC) en la guía del desarrollador de Amazon Simple Storage Service.

    Note

    Cuando se utiliza S3-RTC, se aplican tarifas de transferencia por GB de datos y tarifas de métricas de CloudWatch adicionales.

11. Para replicar objetos en el bucket de origen cifrado con AWS Key Management Service (AWS KMS), en Replication criteria (Criterios de replicación), seleccione Replicate objects encrypted with AWS KMS (Replicar objetos cifrados con AWS KMS). En AWS KMS key for encrypting destination objects (Clave de AWS KMS para cifrar objetos de destino) se encuentran las claves de origen que permiten utilizar la replicación. De forma predeterminada, se incluyen todas las CMK de origen. Puede optar por reducir la selección de CMK.

    Los objetos cifrados por CMK de AWS KMS que no seleccione no se replican. Una CMK o un grupo de CMK se seleccionan automáticamente, pero puede elegir las CMK que desee. Para obtener

información acerca de cómo utilizar AWS KMS con la replicación, consulte Replicación de objetos creados con el cifrado de lado del servidor (SSE) mediante claves de cifrado almacenadas en AWS KMS en la guía del desarrollador de Amazon Simple Storage Service.

Important

Cuando replica objetos que están cifrados con AWS KMS, la velocidad de solicitud de AWS KMS se duplica en la región de origen y aumenta en la región de destino en la misma cantidad. Estas mayores velocidades de llamada a AWS KMS se deben a la forma en la que los datos se vuelven a cifrar por medio de la clave maestra del cliente (CMK) que debe definir en la región de destino. AWS KMS tiene un límite de velocidad de solicitud para la cuenta a la que se llama por región. Para obtener información sobre los valores predeterminados del límite, consulte Límites de AWS KMS - Solicitudes por segundo: Variación en la guía para desarrolladores de AWS Key Management Service.
Si su velocidad de solicitud actual de objeto PUT de Amazon S3 durante la replicación es más que la mitad del límite de velocidad de AWS KMS predeterminado para su cuenta, recomendamos que solicite un aumento de los límites de velocidad de solicitud de AWS KMS. Para solicitar un aumento, abra un caso en el Centro de soporte de AWS en Contáctenos. Por ejemplo, suponga que su velocidad de solicitud de objeto PUT actual es de 1000 solicitudes por segundo y utiliza AWS KMS para cifrar sus objetos. En ese caso, recomendamos que pida a AWS Support que aumente su límite de velocidad de AWS KMS a 2500 solicitudes por segundo, tanto en la región de origen como en la de destino (si es diferente), a fin de garantizar que no haya una limitación controlada por AWS KMS.
Para ver su velocidad de solicitud de objeto PUT en el bucket de origen, consulte `PutRequests` en las métricas de solicitudes de Amazon CloudWatch para Amazon S3. Para obtener información sobre cómo ver las métricas de CloudWatch, consulte ¿Cómo creo un filtro de métricas de solicitudes para todos los objetos de mi bucket de S3? (p. 62).

Si decide replicar objetos cifrados con AWS KMS, escriba el nombre de recurso de Amazon (ARN) de la CMK de AWS KMS que se va a usar para cifrar las réplicas en el bucket de destino. Puede encontrar el ARN de CMK de AWS KMS en la consola de IAM, en Encryption keys (Claves de cifrado). O bien, puede elegir un nombre de CMK en la lista desplegable.

Para obtener más información acerca de cómo crear una CMK de AWS KMS, consulte Creación de claves en la guía para desarrolladores de AWS Key Management Service.

Important

La consola de Amazon S3 solo enumera 100 CMK de AWS KMS por región de AWS. Si tiene más de 100 CMK en la misma región, sólo podrá ver las primeras 100 CMK en la consola S3. Para utilizar una CMK de KMS que no aparece en la consola, elija ARN de KMS personalizado y escriba el ARN de la CMK de KMS.

12. Para terminar, elija Save (Guardar).
13. Después de guardar la regla, puede seleccionar la regla y elegir Edit rule (Editar regla) para editarla, habilitarla, deshabilitarla o eliminarla.

Concesión de permiso al propietario del bucket de origen para cifrar con la CMK de AWS KMS

Debe conceder permisos a la cuenta del propietario del bucket de origen para cifrar mediante su CMK de AWS KMS con una política de claves. En el procedimiento siguiente se describe cómo utilizar la consola de AWS Identity and Access Management (IAM) para modificar la política de claves para la CMK de AWS KMS que se utiliza para cifrar los objetos de réplica en el bucket de destino.

Para conceder permiso para cifrar mediante su CMK de AWS KMS

1. Inicie sesión en la consola de administración de AWS mediante la cuenta de AWS propietaria de la CMK de AWS KMS. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Elija el alias de la CMK con la que desea cifrar.
3. En la sección Key Policy (Política de claves) de la página, elija Switch to policy view (Cambiar a la vista de política).
4. Elija Editar para modificar la política de claves.
5. Mediante el editor de Key Policy (Política de claves), inserte la política de claves proporcionada por Amazon S3 en la política de claves existente y después elija Save Changes (Guardar cambios). Es posible que desee añadir la política al final de la política existente.

Para obtener más información acerca de la creación y edición de una CMK de AWS KMS, consulte Getting Started (Introducción) en la guía para desarrolladores de AWS Key Management Service.

Más información

- ¿Cómo se administran las reglas de replicación para un bucket de S3? (p. 57)
- ¿Cómo habilito o suspendo el control de versiones en un bucket de S3? (p. 8)
- Replication (Replicación) en la guía del desarrollador de Amazon Simple Storage Service

¿Cómo se administran las reglas de replicación para un bucket de S3?

La replicación consiste en la copia automática y asincrónica de los objetos de los buckets en las mismas o diferentes regiones de AWS. Replica los objetos creados recientemente y las actualizaciones de objetos de un bucket de origen en un bucket de destino especificado.

Para agregar reglas de replicación al bucket de origen se utiliza la consola de Amazon S3. Las reglas de replicación definen los objetos del bucket de origen que se deben replicar y el bucket de destino en el que se almacenan los objetos replicados. Para obtener más información sobre la replicación, consulte Replicación en la guía del desarrollador de Amazon Simple Storage Service.

Las reglas de replicación se administran en la página Replication (Replicación). Puede añadir, ver, activar, desactivar, eliminar y cambiar la prioridad de las reglas de replicación. Para obtener información acerca de cómo agregar reglas de replicación a un bucket, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52).

Para administrar las reglas de replicación para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. Seleccione Management (Administración) y desplácese hacia abajo hasta Replication rules (Reglas de replicación).
4. Las reglas de replicación pueden cambiarse de mediante los siguientes métodos.
   - Para activar o desactivar una regla de replicación, selecciónela, elija Actions (Acciones) y, en la lista desplegable, elija Enable rule (Habilitar regla) o Disable rule (Deshabilitar regla). También puede desactivar, activar o eliminar todas las reglas del bucket desde la lista desplegable Actions (Acciones).

- Para cambiar las prioridades de reglas, seleccione la regla y elija Edit (Editar), lo que iniciará el asistente de replicación para ayudarle a realizar el cambio. Para obtener información acerca de cómo utilizar el asistente, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52).

  Establece las prioridades de las reglas para evitar conflictos causados por objetos incluidos en el ámbito de más de una regla. En caso de solaparse las reglas, Amazon S3 usará la prioridad de la regla para determinar la regla que se va a aplicar. Cuanto mayor sea el número, mayor será la prioridad. Para obtener más información sobre la prioridad de la regla, consulte la sección de información general de la configuración de replicación en la guía del desarrollador de Amazon Simple Storage Service.

Más información

- ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52)
- Replication (Replicación) en la guía del desarrollador de Amazon Simple Storage Service

¿Cómo configuro el análisis de clases de almacenamiento?

Al usar la herramienta de análisis de clases de almacenamiento de Amazon S3, podrá analizar los patrones de acceso al almacenamiento para poder determinar cuándo trasladar los datos apropiados a la clase de almacenamiento apropiada. El análisis de las clases de almacenamiento observa los patrones de acceso a los datos para ayudarle a determinar cuándo trasladar el almacenamiento STANDARD al que se acceda con menos frecuencia a la clase de almacenamiento STANDARD_IA (IA quiere decir acceso poco frecuente). Para obtener más información acerca de STANDARD_IA, consulte las preguntas frecuentes y las clases de almacenamiento de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

> **Important**
>
> El análisis de clases de almacenamiento no ofrece recomendaciones para las transiciones a las clases de almacenamiento ONEZONE_IA o Glacier de S3.

Para obtener más información acerca de los análisis, consulte Análisis de Amazon S3: análisis de clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.

Para configurar el análisis de clases de almacenamiento

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, seleccione el nombre del bucket para el que desea configurar el análisis de clases de almacenamiento.
3. Elija la pestaña Metrics (Métricas).
4. En Storage Class Analysis (Análisis de clases de almacenamiento), elija Create analytics configuration (Crear configuración de análisis).
5. Escriba un nombre para el filtro. Si quiere analizar todo el bucket, deje el campo Prefix (Prefijo) vacío.
6. En el campo Prefix (Prefijo), escriba texto para el prefijo de los objetos que desee analizar.
7. Para agregar una etiqueta, elija Add tag (Añadir etiqueta). Escriba una clave y un valor para la etiqueta. Puede introducir un prefijo y varias etiquetas.

8. De manera opcional, también puede seleccionar Enable (Habilitar) en Export CSV (Exportar CSV) para exportar los informes de análisis en un archivo plano de valores separados por comas (.csv). Seleccione un bucket de destino donde poder guardar el archivo. Puede escribir un prefijo para el bucket de destino. El bucket de destino debe estar en la misma región de AWS que el bucket para el que configura el análisis. El bucket de destino puede estar en una cuenta de AWS diferente.
9. Seleccione Create configuration (Crear configuración).

   Amazon S3 crea una política de bucket en el bucket de destino que concede permisos de escritura a Amazon S3. Esto le permite escribir los datos de la exportación en el bucket.

   Note

   Esta acción configura el análisis de clase de almacenamiento para todos los buckets especificados.

Si se produce un error al intentar crear la política de bucket, recibirá instrucciones para solucionarlo. Por ejemplo, si selecciona un bucket de destino en otra cuenta de AWS y no tiene permisos para leer y escribir en la política del bucket, verá el siguiente mensaje. Debe hacer que el propietario del bucket de destino agregue la política de bucket que se muestra en el bucket de destino. Si la política no se agrega en el bucket de destino, no obtendrá los datos de exportación, ya que Amazon S3 no tiene permiso para escribir en el bucket de destino. Si el bucket de origen es propiedad de una cuenta diferente de la del usuario actual, el ID de cuenta correcto del bucket de origen debe sustituirse en la política.

Para obtener más información acerca de los datos exportados y de cómo funciona el filtro, consulte Análisis de Amazon S3: análisis de clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.

Más información

Administrar el almacenamiento (p. 50)

¿Cómo configuro el inventario de Amazon S3?

El inventario de Amazon S3 proporciona una lista de archivos sin formato de los objetos y metadatos. Esta es una alternativa prevista para la operación de la API `List` síncrona de Amazon S3. El inventario de Amazon S3 proporciona archivos de salida con valores separados por comas (CSV) u ORC (Apache optimized row columnar) o Apache Parquet (Parquet) que muestran los objetos y metadatos correspondientes diaria o semanalmente para un bucket de S3 o para objetos que comparten un prefijo (objetos con nombres que comienzan con la misma cadena). Para obtener más información, consulte Amazon S3 Inventory en la guía del desarrollador de Amazon Simple Storage Service.

Para configurar el inventario

Note

Se pueden tardar hasta 48 horas en entregar el primer informe.

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), seleccione el nombre del bucket para el que desea configurar el inventario de Amazon S3.
3. Elija Management (Administración).
4. En Inventory configurations (Configuraciones de inventario), seleccione Create inventory configuration (Crear configuración de inventario).

5. En Inventory configuration name (Nombre de configuración de inventario), escriba un nombre.
6. Defina el Inventory scope (Ámbito de inventario):
   - Escriba un prefijo opcional.
   - Elija las versiones de objeto: Current versions only (Solo versiones actuales) o Include all versions (Incluir todas las versiones).
7. En Report details (Detalles del informe), elija la ubicación de la cuenta de AWS en la que desea guardar los informes: This account (Esta cuenta) o A different account (Una cuenta diferente).
8. Seleccione el bucket de destino en el que desea guardar los informes en Destination (Destino).

   El bucket de destino debe estar en la misma región de AWS que el bucket para el que configura el inventario. El bucket de destino puede estar en una cuenta de AWS diferente. En el campo para bucket Destination (Destino) verá el permiso de bucket de destino que se agrega a la política de bucket de destino para permitir que Amazon S3 coloque datos en ese bucket. Para obtener más información, consulte Política del bucket de destino (p. 61).
9. En Frequency (Frecuencia), elija la frecuencia con la que se generará el informe: Daily (Diario) o Weekly (Semanal).
10. Elija el formato de salida del informe:
    - CSV
    - Apache ORC
    - Apache Parquet
11. En Status (Estado), seleccione Enable (Activar) o Disable (Desactivar).
12. Para utilizar el cifrado del lado del servidor, en Server-side encryption (Cifrado del lado del servidor), siga estos pasos:
    a. Elija Enable (Habilitar).
    b. En Tipo de clave de cifrado, elija Amazon S3 key (SSE-S3) [Clave de Amazon S3 (SSE-S3)] o AWS Key Management Service key (SSE-KMS) [clave de AWS Key Management Service (SSE-KMS)].

       El cifrado de lado servidor de Amazon S3 utiliza el estándar de cifrado avanzado de 256 bits (AES-256). Para obtener más información, consulte el tema sobre claves de cifrado administradas de Amazon S3 (SSE-S3) en la guía del desarrollador de Amazon Simple Storage Service. Para obtener más información acerca de SSE-KMS, consulte CMK de AWS KMS en la guía del desarrollador de Amazon Simple Storage Service.
    c. Para utilizar un CMK de AWS KMS, elija una de las siguientes opciones:
       - AWS managed key (aws/s3) [Clave administrada de AWS (aws/s3)]
       - Elija entre sus claves maestras de KMS y elija su clave maestra de KMS.
       - Escriba el ARN de la clave maestra de KMS y escriba el ARN de la clave KMS de AWS.

       > **Note**
       >
       > Para cifrar el archivo con la lista de inventario con SSE-KMS, debe conceder a Amazon S3 permiso para utilizar la CMK de AWS KMS. Para ver instrucciones, consulte Conceder permiso a Amazon S3 para cifrar mediante su CMK de AWS KMS (p. 61) .
13. En Additional fields (Campos adicionales), seleccione uno o más de los siguientes campos opcionales para agregar al informe de inventario:
    - Size (Tamaño): el tamaño del objeto en bytes.
    - Last modified date (Fecha de la última modificación): la fecha de creación del objeto o la última fecha de modificación, la última existente.

- Storage class (Clase de almacenamiento): la clase de almacenamiento utilizado para almacenar el objeto.
- ETag: la etiqueta de entidad es un hash del objeto. El elemento ETag solo refleja los cambios en su contenido, no en los metadatos. La ETag puede ser o no un resumen MD5 de los datos del objeto. Esto dependerá del método de creación del objeto y del tipo de cifrado.
- Multipart upload (Carga multiparte): especifica que el objeto se ha cargado como una carga multiparte. Para obtener más información, consulte Información general sobre la carga multiparte en la guía del desarrollador de Amazon Simple Storage Service.
- Replication status (Estado de replicación): el estado de replicación del objeto. Para obtener más información, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52).
- Encryption status (Estado de cifrado): el cifrado del lado servidor usado para cifrar el objeto. Para obtener más información, consulte Protección de datos mediante cifrado del lado del servidor en la guía del desarrollador de Amazon Simple Storage Service.
- S3 Object lock configurations (Configuraciones de bloqueo de objetos de S3): estado de bloqueo del objeto, incluidos los siguientes ajustes:
  - Retention dome (Modo de retención): grado de protección que se aplica al objeto, Governance (Gobierno) o Compliance (Cumplimiento).
  - Retain until date (Fecha hasta la que se retiene): fecha hasta la cual no se puede eliminar un objeto bloqueado.
  - Legal hold status (Estado de retención legal): estado de retención legal del objeto bloqueado.

  Para obtener información sobre el bloqueo de objetos de S3, consulte Descripción general del bloqueo de objetos de S3 en la guía del desarrollador de Amazon Simple Storage Service.

Para obtener más información sobre el contenido de un informe de inventario, consulta ¿Qué se incluye en un inventario de Amazon S3? en la guía del desarrollador de Amazon Simple Storage Service.

14. Seleccione Create (Crear).

Política del bucket de destino

Amazon S3 crea una política de bucket en el bucket de destino que concede permisos de escritura a Amazon S3. Esto permite a Amazon S3 escribir los datos para los informes de inventario en el bucket.

Si se produce un error al intentar crear la política de bucket, recibirá instrucciones para solucionarlo. Por ejemplo, si selecciona un bucket de destino en otra cuenta de AWS y no tiene permisos para leer ni escribir en la política de bucket, aparecerá un mensaje de error.

En este caso, el propietario del bucket de destino debe añadir la política del bucket indicada en el bucket de destino. Si la política no se añade al bucket de destino, no obtendrá un informe de inventario, ya que Amazon S3 no tiene permiso para escribir en el bucket de destino. Si el bucket de origen es propiedad de una cuenta diferente de la del usuario actual, el ID de cuenta correcto del bucket de origen debe sustituirse en la política.

Para obtener más información, consulte Amazon S3 Inventory en la guía del desarrollador de Amazon Simple Storage Service.

Concesión de permiso a Amazon S3 para utilizar su CMK de AWS KMS para cifrado

Para conceder permiso a Amazon S3 para cifrar mediante una clave maestra de cliente (CMK) de AWS Key Management Service (AWS KMS) gestionada por el cliente, debe utilizar una política de claves. Para

actualizar la política clave de modo que pueda usar una CMK de AWS KMS administrada por el cliente para el archivo de inventario, siga los pasos que se indican a continuación.

Para conceder permiso para cifrar mediante su CMK de AWS KMS

1. Con la cuenta de AWS propietaria de la CMK gestionada por el cliente, inicie sesión en la consola de administración de AWS.
2. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
3. Para cambiar la región de AWS, utilice el selector de regiones en la esquina superior derecha de la página.
4. En el panel de navegación izquierdo, elija Customer managed keys (Claves administradas por el cliente).
5. En Customer managed keys (Claves administradas por el cliente), seleccione la CMK administrada por el cliente que desee usar para cifrar el archivo de inventario.
6. En Key policy (Política de claves), seleccione Switch to policy view (Cambie a la vista de política).
7. Para actualizar la política de claves, elija Edit (Editar).
8. En Edit key policy (Editar política de claves), agregue la siguiente política de claves a la política de claves existente.

```
{
    "Sid": "Allow Amazon S3 use of the CMK",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

9. Elija Save changes.

   Para obtener más información acerca de cómo crear CMK de AWS KMS administradas por el cliente y cómo usar políticas de claves, consulte los siguientes enlaces en la guía para desarrolladores de AWS Key Management Service:

   - Introducción
   - Uso de las políticas de claves en AWS KMS

Más información

Administrar el almacenamiento (p. 50)

¿Cómo creo un filtro de métricas de solicitudes para todos los objetos de mi bucket de S3?

Existen tres tipos de métricas de Amazon CloudWatch para Amazon S3: métricas de almacenamiento, métricas de solicitud y métricas de replicación. Las métricas de almacenamiento se informan una vez al día y se entregan a todos los clientes sin costo adicional. Las métricas de solicitudes están disponibles en intervalos de un minuto después de un breve periodo de latencia para procesarlas. Las métricas de solicitud se facturan según la tarifa de CloudWatch estándar. Debe incluir métricas de solicitudes configurándolas en la consola o con la API de Amazon S3.

Para obtener más información acerca de las métricas de CloudWatch para Amazon S3, consulte Monitoreo de métricas con Amazon CloudWatch en la guía del desarrollador de Amazon Simple Storage Service.

Para crear un filtro de métricas de solicitud

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, elija el nombre del bucket que contiene los objetos para los que desea obtener métricas de solicitudes.
3. Elija la pestaña Metrics (Métricas).
4. En Bucket metrics (Métricas de bucket), seleccione View additional charts (Ver gráficos adicionales).
5. Seleccione la pestaña Request metrics (Métricas de solicitud).
6. Elija Create Filter (Crear filtro).
7. En el cuadro Filter name (Nombre del filtro), escriba el nombre del filtro.

   Los nombres solo pueden incluir letras, números, puntos, guiones y guiones bajos. Se recomienda utilizar el nombre `EntireBucket` si el filtro se aplica a todos los objetos.
8. En Choose a filter scope (Elegir un ámbito de filtro), elija This filter applies to all objects in the bucket (Este filtro se aplica a todos los objetos del bucket).

   También puede definir un filtro para que las métricas solo se recopilen y comuniquen en un subconjunto de objetos en el bucket. Para obtener más información, consulte ¿Cómo creo un filtro de métricas de solicitud que limita el ámbito por etiqueta de objeto o prefijo? (p. 63)
9. Elija Create Filter (Crear filtro).
10. En la pestaña Request metrics (Métricas de solicitud), bajo Filters (Filtros), elija el filtro que acaba de crear.

    Después de unos 15 minutos, CloudWatch comienza a hacer el seguimiento de estas métricas de solicitud. Puede verlas en la pestaña Request metrics (Solicitar métricas). Puede ver gráficos de las métricas en la consola de Amazon S3 o de CloudWatch. Las métricas de solicitud se facturan según la tarifa de CloudWatch estándar. Para obtener más información, consulte los precios de Amazon CloudWatch.

¿Cómo creo un filtro de métricas de solicitud que limita el ámbito por etiqueta de objeto o prefijo?

Existen tres tipos de métricas de Amazon CloudWatch para Amazon S3: métricas de almacenamiento, métricas de solicitud y métricas de replicación. Las métricas de almacenamiento se informan una vez al día y se entregan a todos los clientes sin costo adicional. Las métricas de solicitudes están disponibles en intervalos de un minuto después de un breve periodo de latencia para procesarlas. Las métricas de solicitud se facturan según la tarifa de CloudWatch estándar. Debe incluir métricas de solicitudes configurándolas en la consola o con la API de Amazon S3.

Para obtener más información acerca de las métricas de CloudWatch para Amazon S3, consulte Monitoreo de métricas con Amazon CloudWatch en la guía del desarrollador de Amazon Simple Storage Service.

Para filtrar métricas de solicitudes en un subconjunto de objetos en un bucket

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, elija el nombre del bucket que contiene los objetos para los que desea obtener métricas de solicitudes.

3. Elija la pestaña Metrics (Métricas).
4. En Bucket metrics (Métricas de bucket), seleccione View additional charts (Ver gráficos adicionales).
5. Seleccione la pestaña Request metrics (Métricas de solicitud).
6. Elija Create Filter (Crear filtro).
7. En el cuadro Filter name (Nombre del filtro), escriba el nombre del filtro.

   Los nombres solo pueden incluir letras, números, puntos, guiones y guiones bajos.
8. En Choose a filter scope (Elegir un ámbito de filtro), elija Limit the scope of this filter using prefix and tags (Limitar el ámbito de este filtro con un prefijo y etiquetas).
9. (Opcional) En el cuadro Prefix (Prefijo), escriba un prefijo para limitar el ámbito del filtro a una única ruta.
10. (Opcional) En Tags (Etiquetas), escriba lo correspondiente en Key (Clave) y Value (Valor).
11. Elija Create Filter (Crear filtro).

    Amazon S3 crea un filtro que utiliza las etiquetas o los prefijos especificados.
12. En la pestaña Request metrics (Métricas de solicitud), bajo Filters (Filtros), elija el filtro que acaba de crear.

    Ahora ha creado un filtro que limita el ámbito de las métricas de solicitud por etiquetas y prefijos de objeto. Aproximadamente 15 minutos después de que CloudWatch comience a realizar el seguimiento de estas métricas de solicitudes, puede ver gráficos para las métricas en las consolas de Amazon S3 y CloudWatch. Las métricas de solicitud se facturan según la tarifa de CloudWatch estándar. Para obtener más información, consulte los precios de Amazon CloudWatch.

    También puede configurar métricas de solicitud en el nivel de bucket. Para obtener información, consulte ¿Cómo creo un filtro de métricas de solicitudes para todos los objetos de mi bucket de S3? (p. 62)

¿Cómo elimino un filtro de métricas de solicitud?

En la consola de Amazon S3 puede eliminar un filtro de métricas de solicitud. Al eliminar un filtro, ya no se le aplicarán cargos por las métricas de solicitud que utilicen ese filtro específico. Sin embargo, se le seguirá cobrando por cualquier otra configuración de filtro que exista. Cuando elimina un filtro, ya no puede usar el filtro para las métricas de solicitud. La eliminación de un filtro no se puede deshacer.

Para obtener más información sobre cómo crear un filtro de métricas de solicitud, consulte ¿Cómo creo un filtro de métricas de solicitudes para todos los objetos de mi bucket de S3? (p. 62) y ¿Cómo creo un filtro de métricas de solicitud que limita el ámbito por etiqueta de objeto o prefijo? (p. 63).

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista de Buckets, elija el nombre del bucket.
3. Elija la pestaña Metrics (Métricas).
4. En Bucket metrics (Métricas de bucket), seleccione View additional charts (Ver gráficos adicionales).
5. Seleccione la pestaña Request metrics (Métricas de solicitud).
6. Seleccione Manage filters (Administrar filtros).
7. Elija el filtro.

   Important

   La eliminación de un filtro no se puede deshacer.
8. Elija Eliminar.

Amazon S3 elimina el filtro.

¿Cómo se pueden consultar métricas de replicación?

Existen tres tipos de métricas de Amazon CloudWatch para Amazon S3: métricas de almacenamiento, métricas de solicitud y métricas de replicación. Las métricas dereplicación se activan automáticamente cuando se activa la replicación con Control del tiempo de replicación de S3 (S3 RTC) a través de la consola de administración de AWS o la API de Amazon S3. Las métricas de replicación están disponibles 15 minutos después de activar una regla de replicación con Control del tiempo de replicación de S3 (S3 RTC) (S3 RTC).

Las métricas de replicación realizan un seguimiento de los ID de regla de la configuración de replicación. Un ID de regla de replicación puede ser específico de un prefijo, de una etiqueta o de una combinación de ambos. Para obtener más información sobre Control del tiempo de replicación de S3 (S3 RTC), consulte el tema sobre replicación de objetos mediante Control del tiempo de replicación de S3 (S3 RTC) en la guía del desarrollador de Amazon Simple Storage Service.

Para obtener más información acerca de las métricas de CloudWatch para Amazon S3, consulte Monitoreo de métricas con Amazon CloudWatch en la guía del desarrollador de Amazon Simple Storage Service.

Requisitos previos

Active una regla de replicación que tenga S3 RTC.

Para ver las métricas de replicación

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket que contiene los objetos cuyas métricas de replicación desea obtener.
3. Elija la pestaña Metrics (Métricas).
4. En Replication metrics (Métricas de replicación), seleccione Replication rules (Reglas de replicación).
5. Elija Display charts (Mostrar gráficos).

   Amazon S3 muestra Replication Latency (in seconds) [Latencia de replicación (en segundos)] y Operations pending replication (Operaciones pendientes de replicación) en gráficos.
6. Para ver todas las métricas de replicación, incluido Bytes pending replication (Replicación pendiente de bytes), Replication Latency (in seconds) [Latencia de replicación (en segundos)] y Operations pending replication (Replicación pendiente de operaciones), juntas en una página aparte, elija View 1 more chart (Ver 1 gráfico más).

A continuación podrá ver las métricas de replicación Replication Latency (in seconds) (Latencia de replicación (en segundos)), Operations pending replication (Operaciones pendientes de replicación) y Bytes pending replication (Bytes pendientes de replicación) para las reglas seleccionadas. Amazon CloudWatch comienza a informar de métricas de replicación 15 minutos después de activar S3 RTC en la regla de replicación respectiva. Puede ver métricas de replicación en la consola de Amazon S3 o de CloudWatch. Para obtener más información, consulte Información general de métricas de replicación en la guía del desarrollador de Amazon Simple Storage Service.

Configuración de permisos de acceso a buckets y objetos

En esta sección se explica cómo utilizar la consola de Amazon Simple Storage Service (Amazon S3) para conceder permisos de acceso a sus buckets y objetos. También se explica cómo utilizar el bloqueo de acceso público de Amazon S3 para impedir la aplicación de cualquier ajuste que permita el acceso público a los datos dentro de los buckets de S3.

Los buckets y los objetos son recursos de Amazon S3. Puede conceder permisos de acceso a sus buckets y objetos con políticas de acceso basadas en recursos. Puede asociar una política de acceso con un recurso. Una política de acceso describe quién tiene acceso a los recursos. El propietario del recurso es la cuenta de AWS que crea el recurso. Para obtener más información sobre la propiedad de los recursos y las políticas de acceso, consulte Información general sobre la administración del acceso en la guía del desarrollador de Amazon Simple Storage Service.

Los permisos de acceso a un bucket especifican qué usuarios pueden obtener acceso a los objetos que contiene un bucket y qué tipos de acceso tienen. Los permisos de acceso a un objeto especifican qué usuarios pueden obtener acceso a un objeto y qué tipos de acceso tienen. Por ejemplo, puede que un usuario tenga solo permisos de lectura y otro de lectura y escritura.

Los permisos para los buckets y los objetos son independientes entre sí. Un objeto no hereda los permisos del bucket en el que se encuentra. Por ejemplo, si crea un bucket y concede permisos de escritura a un usuario, no puede obtener acceso a los objetos de ese usuario a no ser que este le conceda acceso explícitamente. Los permisos de bucket generalmente permiten al usuario enumerar información sobre un bucket y agregar y eliminar objetos de un bucket. Los permisos de objeto generalmente permiten al usuario descargar, reemplazar o eliminar objetos.

> Note
>
> No es necesario necesariamente conceder permisos de bucket para conceder permisos de objeto y viceversa. Por ejemplo, puede utilizar la consola de AWS para conceder permisos de actualización a un usuario sobre un objeto sin conceder permisos de usuario al bucket que contiene dicho objeto. Sin embargo, si concediera permisos únicamente al objeto y no al bucket, el beneficiario no podría utilizar la consola de AWS para acceder al objeto. (No podrían ver el objeto en la consola porque no podrían ver el bucket que contiene el objeto). En su lugar, el beneficiario tendría que acceder al objeto mediante programación, por ejemplo con la CLI de AWS.

Para conceder acceso a sus buckets y objetos a otras cuentas de AWS y al público general, ha de usar políticas de acceso basadas en recursos denominadas listas de control de acceso (ACL).

Una política de bucket es una política de AWS Identity and Access Management (IAM) basada en recursos que concede a otras cuentas de AWS o usuarios de IAM acceso a un bucket de S3. Las políticas de bucket complementan y, en muchos casos, sustituyen a las políticas de acceso basadas en ACL. Para obtener más información acerca de cómo usar IAM con Amazon S3, consulte el tema sobre administración de los permisos de acceso a los recursos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Para obtener información más detallada sobre cómo administrar los permisos de acceso, consulte Introducción a la administración del acceso a los recursos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

En esta sección también se explica cómo utilizar la consola de Amazon S3 para añadir una configuración de uso compartido de recursos entre orígenes (CORS) a un bucket de S3. CORS permite que las aplicaciones web clientes cargadas en un dominio puedan interactuar con los recursos de otro dominio.

Temas

¿Cómo se bloquea el acceso público a los buckets de S3?

El bloqueo del acceso público de Amazon S3 impide que se aplique cualquier ajuste que permita el acceso público a los datos dentro de los buckets de S3. Puede configurar los ajustes de bloqueo del acceso público para un solo bucket de S3 o para todos los buckets de la cuenta. Para obtener más información sobre cómo bloquear el acceso público con la CLI de AWS, los SDK de AWS o las API de REST de Amazon S3, consulte Usar Block Public Access de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

En los siguientes temas se explica cómo utilizar la consola de Amazon S3 para configurar los ajustes de bloqueo del acceso público.

- ¿Cómo se edita la configuración de acceso público para los buckets de S3? (p. 68)
- ¿Cómo se edita la configuración de acceso público para todos los buckets de S3 en una cuenta de AWS? (p. 69)

Las siguientes secciones explican cómo ver el estado de acceso del bucket y cómo realizar búsquedas según el tipo de acceso.

Consultar el estado de acceso

La vista de lista de buckets ahora muestra si el bucket es accesible públicamente. Amazon S3 etiqueta los permisos de un bucket de la siguiente manera:

- Public (Público): todos los usuarios tienen acceso a una o más de las siguientes opciones: listar objetos, escribir objetos y leer y escribir permisos.
- Objects can be public (Los objetos pueden ser públicos): el bucket no es público, pero todos los usuarios con los permisos pertinentes pueden otorgar acceso público a objetos.
- Buckets and objects not public (Los buckets y los objetos no son públicos): los buckets y los objetos no son de acceso público.
- Only authorized users of this account (Solo usuarios autorizados de esta cuenta): el acceso se limita a los usuarios y los roles de IAM en esta cuenta y las entidades principales de servicio de AWS porque hay una política que otorga acceso público.

La columna de acceso muestra el estado de acceso de los buckets de la lista.

También puede filtrar la búsqueda de buckets por tipo de acceso. Elija un tipo de acceso de la lista desplegable al lado de la barra Search for buckets (Buscar buckets).

Más información

- ¿Cómo se edita la configuración de acceso público para los buckets de S3? (p. 68)
- ¿Cómo se edita la configuración de acceso público para todos los buckets de S3 en una cuenta de AWS? (p. 69)
- Configuración de permisos de acceso a buckets y objetos (p. 66)
- Restricción del acceso utilizando una identidad de acceso de origen en la guía del desarrollador de Amazon Simple Storage Service
- Acceso al contenido privado en Amazon CloudFront en el blog para desarrolladores de AWS

¿Cómo se edita la configuración de acceso público para los buckets de S3?

El bloqueo del acceso público de Amazon S3 impide que se aplique cualquier ajuste que permita el acceso público a los datos dentro de los buckets de S3. Esta sección describe cómo editar la configuración de bloqueo del acceso público para uno o más buckets de S3. Para obtener más información sobre cómo bloquear el acceso público con la CLI de AWS, los SDK de AWS o las API de REST de Amazon S3, consulte Usar Block Public Access de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Temas

- Editar la configuración de acceso público para un bucket de S3 (p. 68)
- Más información (p. 69)

Editar la configuración de acceso público para un bucket de S3

Siga estos pasos si tiene que cambiar la configuración de acceso público para un solo bucket de S3.

Para editar la configuración de bloqueo del acceso público de Amazon S3 de un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket en cuestión.
3. Elija Permissions (Permisos).
4. Elija Edit (Editar) para cambiar la configuración de acceso público del bucket. Para obtener más información sobre la configuración de bloqueo de acceso público de Amazon S3, consulte el tema sobre configuración del bloqueo de acceso público en la guía del desarrollador de Amazon Simple Storage Service.
5. Elija la configuración que desea cambiar y, a continuación, elija Save changes (Guardar cambios).
6. Cuando se le pida que confirme, introduzca **`confirm`**. Para guardar los cambios, elija Save (Guardar).

Puede cambiar la configuración de bloqueo del acceso público de Amazon S3 cuando se crea un bucket. Para obtener más información, consulte ¿Cómo se puede crear un bucket de S3? (p. 3).

Más información

- ¿Cómo se bloquea el acceso público a los buckets de S3? (p. 67)
- ¿Cómo se edita la configuración de acceso público para todos los buckets de S3 en una cuenta de AWS? (p. 69)
- Configuración de permisos de acceso a buckets y objetos (p. 66)

¿Cómo se edita la configuración de acceso público para todos los buckets de S3 en una cuenta de AWS?

El bloqueo del acceso público de Amazon S3 impide que se aplique cualquier ajuste que permita el acceso público a los datos dentro de los buckets de S3. Esta sección describe cómo editar la configuración de bloqueo del acceso público para todos los buckets de S3 en su cuenta de AWS. Para obtener más información sobre bloquear el uso de la CLI y los SDK de AWS o las API de REST de Amazon S3 por parte del público, consulte Uso de Amazon S3 Block Public Access en la guía del desarrollador de Amazon Simple Storage Service.

Para editar la configuración de Block Public Access para todos los buckets de S3 en una cuenta de AWS

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. Seleccione Account settings for Block Public Access (Configuración de la cuenta para bloquear el acceso público).
3. Elija Edit (Editar) para cambiar la configuración de bloqueo del acceso público para todos los buckets de su cuenta de AWS.
4. Elija la configuración que desea cambiar y, a continuación, elija Save changes (Guardar cambios).
5. Cuando se le pida que confirme, introduzca **`confirm`**. Para guardar los cambios, elija Save (Guardar).

Más información

- ¿Cómo se bloquea el acceso público a los buckets de S3? (p. 67)
- ¿Cómo se edita la configuración de acceso público para los buckets de S3? (p. 68)
- Configuración de permisos de acceso a buckets y objetos (p. 66)

¿Cómo puedo configurar permisos en un objeto?

En esta sección se explica cómo utilizar la consola de Amazon Simple Storage Service (Amazon S3) para administrar permisos de acceso para un objeto de Amazon S3 con Access Control Lists (ACL, Lista de control de acceso). Las ACL son políticas de acceso basadas en recursos que conceden permisos de acceso a buckets y objetos. Para obtener más información acerca de cómo administrar permisos de acceso con políticas basadas en recursos, consulte Información general sobre la administración del acceso en la guía del desarrollador de Amazon Simple Storage Service.

Los permisos para los buckets y los objetos son independientes entre sí. Un objeto no hereda los permisos del bucket en el que se encuentra. Por ejemplo, si crea un bucket y concede permisos de escritura a un

usuario, no puede obtener acceso a los objetos de ese usuario a no ser que este le conceda permiso explícitamente.

Puede conceder permisos a otros grupos predefinidos u otras cuentas de AWS. El usuario o grupo al que se le conceden permisos se denominabeneficiario. De forma predeterminada, el propietario, que es la cuenta de AWS que creó el bucket, tiene permisos completos.

Cada permiso que concede a un usuario o grupo añade una entrada a la ACL que está asociada con el objeto. La ACL incluye los permisos concedidos, que identifican al beneficiario y permiso concedido. Para obtener más información acerca de las ACL, consulte Administración de acceso con ACL en la guía del desarrollador de Amazon Simple Storage Service.

Para configurar permisos para un objeto

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets, elija el nombre del bucket que contiene los objetos para los que desea establecer permisos.
3. Elija la ficha Permissions (Permisos) que aparece en la lista de fichas de la sección Información general del bucket .
4. Para editar la configuración del bloqueo de acceso público, elija Edit (Editar) para bloquear o permitir el acceso público a este bucket y sus puntos de acceso. Para obtener más información, consulte Bloquear acceso público (p. 67).
5. Para editar la política de bucket, elija Edit (Editar) para editar la política de bucket JSON que proporciona acceso a los objetos almacenados en este bucket. Esta política solo se aplica a los objetos propiedad de su cuenta.

   Alternativamente, si tiene una política de bucket existente, puede elegir Eliminar para eliminar una política de bucket existente. Para obtener más información, consulte Agregar una política de bucket (p. 73).
6. Para editar la propiedad del objeto, elija Edit (Editar) para asumir la propiedad de los nuevos objetos cargados en este bucket. Para obtener más información, consulte ??? (p. 75).
7. Para editar la lista de control de acceso (ACL), elija Edit (Editar) para actualizar los permisos (enumerar, leer y escribir) a los grupos beneficiarios como el propietario del bucket (su cuenta de AWS), todos, usuarios autenticados (cualquiera que tenga una cuenta de AWS) o un grupo de entrega de registros de S3.

   a. El propietario del bucket hace referencia a su cuenta de AWS y no a un usuario de AWS Identity and Access Management (IAM). Para obtener más información acerca del usuario raíz, consulte El usuario raíz de la cuenta de AWS en la guía del usuario de IAM.

   b. Para otorgar acceso a su objeto a todos, elija Everyone (Todos). Si se conceden permisos de acceso público, cualquier persona puede acceder al objeto desde cualquier lugar.

      #### Warning

      - Extreme las precauciones a la hora de otorgar al grupo Everyone (Todos) acceso anónimos a sus objetos de Amazon S3. Al otorgar acceso a este grupo, cualquier persona puede acceder a su objeto. Si necesita otorgar acceso a todo el mundo, le recomendamos encarecidamente que solo conceda permisos para Read objects (Leer objetos).
      - Recomendamos encarecidamente que no conceda permisos de objeto de escritura sobre objetos al grupo Everyone (Todos). Al hacerlo permitirá que cualquier persona sobrescriba los permisos de ACL del objeto.

   c. Para conceder permisos a un usuario de AWS desde una cuenta de AWS diferente, introduzca el ID canónico del usuario de AWS al que desee conceder permisos de objeto. Para obtener información acerca de cómo buscar un ID canónico, consulte Identificadores de cuenta de AWS en la referencia general de Amazon Web Services. Puede añadir hasta 99 usuarios.

d. Para especificar el grupo de entrega de registros de S3, proporcione el nombre del bucket de destino donde desee que Amazon S3 guarde los registros de acceso como objetos.

Para obtener más información, consulte Configuración de permisos de buckets de ACL (p. 71) y Cómo habilitar el registro de acceso al servidor en la guía del desarrollador de Amazon Simple Storage Service.

8. Para editar Compartir recursos entre orígenes (CORS), elija Edit (Editar) para crear una configuración de CORS, que es un documento XML que define la forma en que las aplicaciones web de cliente que se cargan en un dominio interactúan con los recursos de un dominio diferente. Para obtener más información, consulte Agregar la funcionalidad de uso compartido de recursos entre dominios con CORS (p. 74).
9. Después de editar alguno de los ajustes de los pasos anteriores, elija Save changes (Guardar cambios) cuando haya terminado.

Note

Esta acción aplica permisos a todos los objetos especificados. Al aplicar permisos a carpetas, espere a que finalice la operación de guardado antes de agregar nuevos objetos.

También puede configurar permisos de objetos cuando carga objetos. Para obtener más información acerca de cómo configurar permisos cuando carga objetos, consulte Carga de objetos en S3 (p. 28).

Más información

- Configuración de permisos de acceso a buckets y objetos (p. 66)
- ¿Cómo se configuran permisos de buckets de ACL? (p. 71)

¿Cómo se configuran permisos de buckets de ACL?

En esta sección se explica cómo utilizar la consola de Amazon Simple Storage Service (Amazon S3) para administrar permisos de acceso para buckets de S3 con listas de control de acceso (ACL). Las ACL son políticas de acceso basadas en recursos que conceden permisos de acceso a buckets y objetos. Para obtener más información acerca de cómo administrar permisos de acceso con políticas basadas en recursos, consulte Información general sobre la administración del acceso en la guía del desarrollador de Amazon Simple Storage Service.

Puede conceder permisos a los usuarios de otras cuentas de AWS o a los grupos predefinidos. El usuario o grupo al que le concede permisos se denomina beneficiario. De forma predeterminada, el propietario, que es la cuenta de AWS que creó el bucket, tiene permisos completos.

Cada permiso que concede a un usuario o grupo añade una entrada a la ACL que está asociada con el bucket. La ACL incluye los permisos concedidos, que identifican al beneficiario y permiso concedido. Para obtener más información acerca de las ACL, consulte Administración de acceso con ACL en la guía del desarrollador de Amazon Simple Storage Service.

Warning

Le recomendamos encarecidamente que evite conceder acceso de escritura a los grupos Everyone (public access) (Todos [acceso público]) o Grupo de usuarios autenticados (todos los usuarios autenticados de AWS). Para obtener más información sobre los efectos de conceder acceso de escritura a estos grupos, consulte Grupos predefinidos de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

Para configurar permisos de acceso con ACL para un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea configurar permisos.
3. Elija Permissions (Permisos) y, a continuación, elija Edit (Editar) en Access Control List (Lista de control de acceso).
4. Puede administrar permisos de acceso a los buckets para lo siguiente:

   a. Acceso para el usuario raíz de su cuenta de AWS

      Propietario hace referencia al usuario raíz de su cuenta de AWS y no a un usuario de AWS Identity and Access Management (IAM). Para obtener más información acerca del usuario raíz, consulte El usuario raíz de la cuenta de AWS en la guía del usuario de IAM.

      Para cambiar los permisos de acceso al bucket del propietario, seleccione las casillas de verificación de los permisos en Bucket owner (your AWS account) [Propietario del bucket (su cuenta de AWS)].

   b. Acceso para otras cuentas de AWS

      Para conceder permisos a un usuario de AWS de una cuenta de AWS diferente, elija Add grantee (Agregar beneficiario). En el campo Enter a canonical ID (Introducir un ID canónico), escriba el ID canónico o el correo electrónico del usuario de AWS al que desea conceder permisos para el bucket. Para obtener información acerca de cómo buscar un ID canónico, consulte Identificadores de cuenta de AWS en la referencia general de Amazon Web Services. Puede añadir hasta 99 usuarios.

      Seleccione las casillas de verificación junto a los permisos que desea conceder al usuario y, luego, elija Save changes (Guardar cambios).

      > Warning
      >
      > Cuando les otorga a otras cuentas de AWS acceso a sus recursos, asegúrese de que las cuentas de AWS puedan delegar sus permisos a usuarios de sus cuentas. Esto se conoce como acceso entre cuentas. Para obtener información acerca del uso del acceso entre cuentas, consulte Creación de un rol para delegar permisos a un usuario de IAM en la guía del usuario de IAM.

   c. Acceso público

      Para conceder acceso a un bucket al público en general (a todo el mundo), en Public access (Acceso público), elija Everyone (Todos). Si se conceden permisos de acceso público, cualquier persona puede acceder al bucket desde cualquier lugar. Marque las casillas de verificación para los permisos que desea conceder y, a continuación, elija Save (Guardar).

      Para deshacer el acceso público a su bucket, en Public access (Acceso público), elija Everyone (Todos). Desactive todas las casillas de permisos y, a continuación, elija Save (Guardar).

      > Warning
      >
      > Extreme las precauciones a la hora de otorgar al grupo Everyone (Todos) acceso público a su bucket de S3. Al otorgar acceso a este grupo, cualquier persona puede acceder a su bucket. Se recomienda encarecidamente que no otorgue nunca ningún tipo de acceso de escritura público en su bucket de S3.

   d. Grupo Envío de logs de S3

      Para conceder acceso a Amazon S3 para que escriba los registros de acceso al servidor en el bucket, en S3 log delivery group (Grupo de envío de registros de S3), elija Log Delivery (Envío de registros).

Si un bucket está configurado como bucket de destino para recibir registros de acceso, los permisos del bucket deben permitir al grupo Log Delivery (Envío de registros) acceso de escritura al bucket. Cuando se activa el registro de acceso al servidor en un bucket, la consola de Amazon S3 concede acceso de escritura al grupo Log Delivery (Envío de registros) para el bucket de destino que se ha elegido para recibir los registros. Para obtener más información sobre el registro de acceso del servidor, consulte ¿Cómo se puede habilitar el registro de acceso al servidor para un bucket de S3? (p. 10).

También puede configurar los permisos del bucket mientras lo crea. Para obtener más información acerca de cómo configurar los permisos al crear un bucket, consulte ¿Cómo se puede crear un bucket de S3? (p. 3).

Más información

- Configuración de permisos de acceso a buckets y objetos (p. 66)
- ¿Cómo puedo configurar permisos en un objeto? (p. 69)
- ¿Cómo se agrega una política de bucket en S3? (p. 73)

¿Cómo se agrega una política de bucket en S3?

En esta sección se explica cómo utilizar la consola de Amazon Simple Storage Service (Amazon S3) para agregar una nueva política de bucket o editar una existente. Las políticas de bucket son políticas de AWS Identity and Access Management (IAM) basadas en recursos. Puede agregar una política de bucket a un bucket para conceder a otras cuentas de AWS o usuarios de IAM permisos para el bucket y los objetos que contiene. Los permisos de objetos solo se aplican a aquellos objetos que cree el propietario del bucket. Para obtener más información sobre las políticas de bucket, consulte Información general sobre la administración del acceso en la guía del desarrollador de Amazon Simple Storage Service.

Para ver ejemplos de políticas de bucket de Amazon S3, consulte Ejemplos de políticas de bucket en la guía del desarrollador de Amazon Simple Storage Service.

Para crear o editar una política de bucket

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea crear una política de bucket o cuya política de bucket quiera editar.
3. Elija Permissions.
4. (Opcional) Elija Policy generator (Generador de políticas) para abrir el generador de políticas de AWS en una nueva ventana. En la página del generador de políticas, seleccione S3 Bucket Policy (Política de bucket de S3) en el menú desplegable Select Type of Policy (Seleccionar tipo de política) . Agregue una o varias instrucciones rellenando los campos presentados y, a continuación, elija Generate Policy (Generar política). Copie el texto de la política generada y vuelva a la página Edit bucket policy (Editar política de bucket) en la consola de Amazon S3.
5. En Bucket Policy (Política de bucket), elija Edit (Editar).
6. En el cuadro de texto Policy (Política), escriba o copie y pegue una nueva política de bucket, o edite una política existente. La política de bucket es un archivo JSON. El texto que escriba en el editor debe tener un formato JSON válido.

   Note

   Para mayor comodidad, la consola muestra el nombre de recurso de Amazon (ARN) del bucket actual encima del campo de texto Policy (Política) . Puede copiar este ARN para

utilizarlo en la política. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS en la referencia general de Amazon Web Services.

7. Elija Save (Guardar).

Más información

- Configuración de permisos de acceso a buckets y objetos (p. 66)
- ¿Cómo se configuran permisos de buckets de ACL? (p. 71)

¿Cómo se agrega la funcionalidad de uso compartido de recursos entre dominios con CORS?

En esta sección también se explica cómo utilizar la consola de Amazon S3 para agregar una configuración de uso compartido de recursos entre orígenes (CORS) a un bucket de S3. CORS permite que las aplicaciones web clientes cargadas en un dominio puedan interactuar con los recursos de otro dominio.

Para configurar su bucket para permitir solicitudes entre orígenes, debe agregar una configuración CORS al bucket. Una configuración CORS es un documento que define reglas que identifican los orígenes desde los que permitirá el acceso a su bucket, las operaciones (métodos HTTP) permitidas para cada origen y otro tipo de información específica a cada operación. En la consola de S3, la configuración de CORS debe ser un documento JSON. Para obtener más información acerca de CORS y ver ejemplos, consulte Compartir recursos entre orígenes (CORS) en la guía del desarrollador de Amazon Simple Storage Service.

Cuando activa CORS en el bucket, la lista de control de acceso (ACL) y otras políticas de permisos para la obtención de accesos seguirán aplicándose.

> **Important**
>
> En la nueva consola de S3, la configuración de CORS debe ser JSON.

Para agregar una configuración CORS a un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), seleccione el nombre del bucket para el que desea crear una política de bucket.
3. Elija Permissions.
4. En la sección Cross-origin resource sharing (CORS) [Compartir recursos entre orígenes (CORS)], elija Edit (Editar).
5. En el cuadro de texto Cross-origin resource sharing (CORS) [Compartir recursos entre orígenes (CORS)], escriba o copie y pegue una nueva configuración CORS o edite una que ya exista.

   En la consola de S3, la configuración de CORS es un archivo JSON. El texto que escriba en el editor debe tener un formato XML válido. Para obtener más información, consulte ¿Cómo puedo configurar CORS en mi bucket?
6. Elija Save changes.

   > **Note**
   >
   > Amazon S3 muestra el nombre de recurso de Amazon (ARN) del bucket junto al título CORS configuration editor (Editor de configuración de CORS). Para obtener más información

sobre los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS en la referencia general de Amazon Web Services.

Más información

- Configuración de permisos de acceso a buckets y objetos (p. 66)
- ¿Cómo se configuran permisos de buckets de ACL? (p. 71)
- ¿Cómo se agrega una política de bucket en S3? (p. 73)

Establecimiento de la propiedad de objetos de S3 como propietario del bucket preferido en la consola de administración de AWS

La propiedad de objetos de S3 se encuentra actualmente en estado de vista previa y se puede configurar a través de la consola de administración de AWS, la interfaz de línea de comandos de AWS, los SDK de AWS o las API de REST de Amazon S3. Está previsto soporte disponible para AWS CloudFormation.

La propiedad de objetos de S3 le permite asumir la propiedad de nuevos objetos que otras cuentas de AWS cargan en el bucket con la lista de control de acceso (ACL) predefinida `bucket-owner-full-control`. En esta sección se describe cómo establecer la propiedad de objetos con la consola.

Establecimiento de la propiedad de objetos como propietario del bucket preferido en un bucket de S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets (Buckets), elija el nombre del bucket para el que desea activar la propiedad de objetos de S3.
3. Elija la pestaña Permissions.
4. Seleccione Edit (Editar) en Object Ownership (Propiedad de objeto).
5. Elija Bucket owner preferred (Propietario del bucket preferido) y, a continuación, elija Save (Guardar).

¿Cómo me aseguro de que soy el propietario de los nuevos objetos?

Con los pasos anteriores, la propiedad de objetos asumirá la propiedad de cualquier nuevo objeto que otras cuentas con la ACL predefinida `bucket-owner-full-control` escriban. Para obtener más información acerca de cómo aplicar de la propiedad de objetos, consulte ¿Cómo me aseguro de que soy el propietario de los nuevos objetos? en la guía del desarrollador de Amazon Simple Storage Service.

Uso de Access Analyzer para S3

Access Analyzer para S3 le avisa de los buckets de S3 que están configurados para permitir el acceso a cualquier usuario de Internet u otras cuentas de AWS, incluidas las cuentas de AWS ajenas a su organización. Para cada bucket público o compartido, recibe los resultados sobre el origen y el nivel del

acceso público o compartido. Por ejemplo, Access Analyzer para S3 puede mostrar que un bucket tiene acceso de lectura o escritura proporcionado a través de una lista de control de acceso (ACL) de bucket, una política de bucket o una política de punto de acceso. Dotado de este conocimiento, puede adoptar medidas correctivas inmediatas y precisas para restaurar el acceso al bucket a aquel que se pretende.

Al revisar un bucket en riesgo en Access Analyzer para S3, puede bloquear todo el acceso público al bucket con un solo clic. Le recomendamos que bloquee todo el acceso a sus buckets a menos que necesite acceso público para admitir un caso de uso específico. Antes de bloquear todo el acceso público, asegúrese de que las aplicaciones seguirán funcionando correctamente sin ese acceso público. Para obtener más información, consulte Uso de Bloqueo de acceso público de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

También puede examinar a fondo las configuraciones de permisos de nivel de bucket para configurar niveles detallados de acceso. Para casos de uso específicos y verificados que requieren acceso público, como el alojamiento estático de sitios web, descargas públicas o uso compartido entre cuentas, puede reconocer y registrar su intención de que el bucket siga siendo público o compartido archivando los resultados del bucket. Puede volver a visitar y modificar estas configuraciones de bucket en cualquier momento. También puede descargar sus resultados en un informe CSV con fines de auditoría.

Access Analyzer para S3 está disponible sin coste adicional en la consola de Amazon S3. Access Analyzer para S3 está equipado con Access Analyzer de AWS Identity and Access Management (IAM). Para utilizar Access Analyzer para S3 en la consola de Amazon S3, debe visitar la consola de IAM y habilitar IAM Access Analyzer por región.

Para obtener más información acerca de IAM Access Analyzer, consulte ¿Qué es Access Analyzer? en la guía del usuario de IAM. Para obtener más información acerca de Access Analyzer para S3, revise las secciones siguientes.

Important

- Access Analyzer para S3 requiere un analizador de nivel de cuenta. Para utilizar Access Analyzer para S3, debe visitar IAM Access Analyzer y crear un analizador que tenga una cuenta como zona de confianza. Para obtener más información, consulte Habilitación de Access Analyzer en la guía del usuario de IAM.
- Cuando se agrega o modifica una política de bucket o una ACL de bucket, Access Analyzer genera y actualiza los resultados basándose en el cambio en un plazo de 30 minutos. Es posible que los resultados relacionados con la configuración de acceso público del nivel de cuenta no se generen ni actualicen hasta 6 horas después de haber cambiado la configuración.

Temas

¿Qué información proporciona Access Analyzer para S3?

Access Analyzer para S3 proporciona información sobre los buckets a los que se puede acceder fuera de la cuenta de AWS. Cualquier usuario de Internet puede acceder a los buckets enumerados en Buckets

with public access (Buckets con acceso público). Si Access Analyzer para S3 identifica buckets públicos, también muestra una advertencia en la parte superior de la página, con el número de buckets públicos de la región. Los buckets enumerados en Buckets with access from other AWS accounts — including third-party AWS accounts (Buckets con acceso desde otras cuentas de AWS — incluidas las cuentas de AWS de terceros) se comparten de manera condicionada con otras cuentas de AWS, incluidas las cuentas ajenas a su organización.

Para cada bucket, Access Analyzer para S3 proporciona la siguiente información:

- Nombre del bucket
- Detectado por Access Analyzer: cuando Access Analyzer para S3 ha detectado el acceso público o compartido a los buckets.
- Compartido a través de: indica cómo se comparte el bucket, a través de una política de bucket, de una ACL de bucket o de ambas. Un bucket se puede compartir a través de políticas y ACL. Si desea buscar y revisar el origen del acceso al bucket, puede utilizar la información de esta columna como punto de partida para adoptar medidas correctivas inmediatas y precisas.
- Estado: el estado del resultado del bucket. Access Analyzer para S3 muestra los resultados de todos los buckets públicos y compartidos.
  - Activo: no se ha revisado el resultado.
  - Archivado: el resultado se ha revisado y confirmado como previsto.
  - Todos: todos los resultados para los buckets públicos o compartidos con otras cuentas de AWS, incluidas las cuentas de AWS ajenas a su organización.
- Nivel de acceso: permisos de acceso concedidos para el bucket:
  - Lista: permite enumerar recursos.
  - Lectura: permite leer pero no editar el contenido y los atributos de los recursos.
  - Escritura: permite crear, eliminar o modificar recursos.
  - Permisos: permite conceder o modificar permisos a nivel de recursos.
  - Etiquetado: permite actualizar las etiquetas asociadas con el recurso.

Habilitación de Access Analyzer para S3

Para usar Access Analyzer para S3 debe completar los siguientes requisitos previos.

1. Concesión de permisos necesarios.

   Para obtener más información, consulte Permisos necesarios para usar Access Analyzer en la guía del usuario de IAM.
2. Visite IAM para crear un analizador de nivel de cuenta para cada región en la que desee utilizar Access Analyzer.

   Access Analyzer para S3 requiere un analizador de nivel de cuenta. Para utilizar Access Analyzer para S3, debe crear un analizador que tenga una cuenta como zona de confianza. Para obtener más información, consulte Habilitación de Access Analyzer en la guía del usuario de IAM.

Bloquear todo el acceso público

Si desea bloquear todo el acceso a un bucket con un solo clic, puede utilizar el botón Block all public access (Bloquear todo el acceso público) en Access Analyzer para S3. Cuando se bloquea todo el acceso público a un bucket, no se concede ningún acceso público. Recomendamos bloquear todo el acceso público a los buckets, a menos que se necesite acceso público para admitir un caso de uso específico y comprobado. Antes de bloquear todo el acceso público, asegúrese de que las aplicaciones seguirán funcionando correctamente sin ese acceso público.

Si no desea bloquear todo el acceso público al bucket, puede editar la configuración del bloqueo de acceso público en la consola de Amazon S3 para configurar niveles granulares de acceso a los buckets. Para obtener más información, consulte Uso de Bloqueo de acceso público de Amazon S3 en la guía del desarrollador de Amazon Simple Storage Service.

En casos excepcionales, Access Analyzer para S3 podría no tener ningún resultado para un bucket que una evaluación del bloqueo de acceso público de Amazon S3 registre como pública. Esto sucede porque el bloqueo de acceso público de Amazon S3 revisa las políticas de las acciones actuales y todas las acciones posibles que podrían añadirse en el futuro, lo que hace que un bucket se convierta en público. Por otro lado, Access Analyzer para S3 solo analiza las acciones actuales especificadas para el servicio de Amazon S3 en la evaluación del estado de acceso.

Para bloquear todo el acceso público a un bucket mediante Access Analyzer para S3

1. Inicie sesión en la consola de administración de AWS y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, en Dashboards (Paneles), elija Access analyzer for S3 (Analizador de acceso para S3).
3. En Access Analyzer para S3, elija un bucket.
4. Elija Block all public access (Bloquear todo el acceso público).
5. Para confirmar su intención de bloquear todo el acceso público al bucket, en Block all public access (bucket settings) (Bloquear todo el acceso público (configuración del bucket)), escriba **`confirm`**.

   Amazon S3 bloquea todo el acceso público a su bucket. El estado de los resultados del bucket se actualiza a resolved (resuelto) y el bucket desaparece del listado de Access Analyzer para S3. Si desea revisar los buckets resueltos, abra IAM Access Analyzer en la consola de IAM.

Revisar y cambiar el acceso al bucket

Si no tiene intención de conceder acceso a las cuentas públicas u otras cuentas de AWS, incluidas las que son ajenas a su organización, puede modificar la ACL del bucket, la política del bucket o la política del punto de acceso para eliminar el acceso al bucket. La columna Shared through (Compartido a través de) muestra todos los orígenes de acceso a bucket: política de bucket, ACL de bucket y/o política de punto de acceso.

Para revisar y cambiar una política de bucket, una ACL de bucket o una política de punto de acceso

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Access analyzer for S3 (Analizador de acceso para S3).
3. Para ver si se ha concedido acceso público o compartido mediante una política de bucket, una ACL de bucket o una política de punto de acceso, busque en la columna Shared through (Compartido a través de).
4. En Buckets, elija el nombre del bucket con la política de bucket, la ACL del bucket o la política de punto de acceso que desee cambiar o revisar.
5. Si desea cambiar o ver una ACL de bucket:

   a. Elija Permissions.
   b. Elija Access Control List.
   c. Revise la ACL del bucket y realice los cambios necesarios.

      Para obtener más información, consulte ¿Cómo se configuran permisos de buckets de ACL? (p. 71)
6. Si desea cambiar o revisar una política de bucket:

a. Elija Permissions.
b. Elija Bucket Policy.
c. Revise o cambie la política de bucket según sea necesario.

   Para obtener más información, consulte ¿Cómo se agrega una política de bucket en S3? (p. 73)

7. Si desea revisar o cambiar una política de punto de acceso:

   a. Elija Access points (Puntos de acceso).
   b. Seleccione el nombre del punto de acceso.
   c. Revise o cambie el acceso según sea necesario.

      Para obtener más información, consulte Administración y uso de puntos de acceso de Amazon S3 (p. 24).

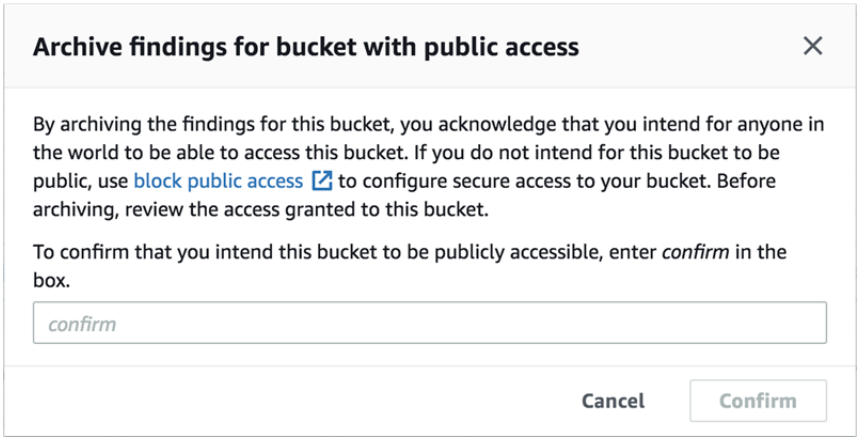
Si edita o elimina una ACL de bucket, una política de bucket o un punto de acceso para eliminar el acceso público o compartido, se actualiza el estado de los resultados del bucket, es decir, quedan resueltos. Los resultados del bucket resueltos desaparecen del listado de Access Analyzer para S3, pero se pueden ver en IAM Access Analyzer.

Archivar resultados del bucket

Si un bucket concede acceso al público o a otras cuentas de AWS, incluidas las cuentas ajenas a su organización, con el fin de admitir un caso de uso específico (por ejemplo, un sitio web estático, descargas públicas o uso compartido entre cuentas), puede archivar los resultados del bucket. Al archivar los resultados del bucket, usted confirma y registra su intención de que el bucket siga siendo público o compartido. Los resultados del bucket archivados permanecen en su listado de Access Analyzer para S3 para que pueda saber en todo momento qué buckets son públicos o compartidos.

Para archivar los resultados de buckets en Access Analyzer para S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Access analyzer for S3 (Analizador de acceso para S3).
3. En Access Analyzer para S3, elija un bucket activo.
4. Para confirmar su intención de que el público u otras cuentas de AWS puedan obtener acceso a este bucket, incluidas las cuentas ajenas a su organización, elija Archive (Archivar).
5. Escriba **`confirm`** y elija Archive (Archivar).



Activar los resultados de los buckets archivados

Después de archivar los resultados, en cualquier momento puede volver a consultarlos y cambiar su estado para activarlos e indicar que el bucket requiere otra revisión.

Para activar resultados de un bucket archivado en Access Analyzer para S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Access analyzer for S3 (Analizador de acceso para S3).
3. Elija los resultados del bucket archivado.
4. Seleccione Mark as active (Marcar como activos).

Consultar los detalles de los resultados

Si necesita ver más información sobre un bucket, puede abrir los detalles de los resultados del bucket en IAM Access Analyzer en la consola de IAM.

Para ver los detalles de los resultados en Access Analyzer para S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación, elija Access analyzer for S3 (Analizador de acceso para S3).
3. En Access Analyzer para S3, elija un bucket.
4. Elija View details.

   Los detalles del resultado se abren en IAM Access Analyzer en la consola de IAM.

Descarga de un informe de Access Analyzer para S3

Puede descargar los resultados del bucket en un informe CSV que se puede utilizar con fines de auditoría. El informe incluye la misma información que se ve en Access Analyzer para S3 en la consola de Amazon S3.

Para descargar un informe

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Access a Analyzer for S3 (Analizador de acceso para S3).
3. En el filtro Region (Región), elija la región.

   Access Analyzer para S3 se actualiza para mostrar los buckets de la región seleccionada.
4. Elija Download report (Descargar informe).

   Se genera un informe en formato CSV y se guarda en el equipo.

Historial de revisión

Última actualización de la documentación: 27 de marzo de 2019

En la siguiente tabla se describen los cambios importantes realizados en cada versión de la guía del usuario de la consola de Amazon Simple Storage Service a partir del 19 de junio de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

update-history-change	update-history-description	update-history-date
Nueva clase de almacenamiento de archivado (p. 81)	Amazon S3 ahora ofrece una nueva clase de almacenamiento de archivado, S3 Glacier Deep Archive, para almacenar objetos a los que se accede con poca frecuencia. Para obtener más información, consulte ¿Cómo se recupera un objeto de S3 que se archivó? y Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.	27 de marzo de 2019
Bloqueo del acceso público a los buckets de S3 (p. 81)	El bloqueo del acceso público de Amazon S3 impide que se aplique cualquier ajuste que permita el acceso público a los datos dentro de los buckets de S3. Para obtener más información, consulte Bloqueo del acceso público a los buckets de S3.	15 de noviembre de 2018
Filtrado de mejoras en reglas de replicación en varias regiones (CRR) (p. 81)	En una regla de CRR, puede especificar un filtro de objetos para elegir un subconjunto de objetos al que aplicar la regla. Anteriormente, solo se podía filtrar en un prefijo de clave de objeto. En esta versión, puede filtrar en un prefijo de clave de objeto, una o varias etiquetas de objeto, o ambos métodos. Para obtener más información, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3?	19 de septiembre de 2018
Actualizaciones ahora disponibles sobre RSS (p. 81)	Ahora puede suscribirse a una fuente RSS para recibir notificaciones sobre actualizaciones de la guía del usuario de la consola de Amazon Simple Storage Service.	19 de junio de 2018

Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes realizados en cada versión de la guía del usuario de la consola de Amazon Simple Storage Service antes del 19 de junio de 2018.

Cambiar	Descripción	Fecha de modificación
Nueva clase de almacenamiento	Amazon S3 ahora ofrece una nueva clase de almacenamiento, ONEZONE_IA (IA quiere decir acceso poco frecuente) para el almacenamiento de objetos. Para obtener más información, consulte Clases de almacenamiento en la guía del desarrollador de Amazon Simple Storage Service.	4 de abril de 2018
Compatibilidad con los archivos de inventario de Amazon S3 con formato ORC	Amazon S3 admite ahora el formato Apache optimized row columnar (ORC) además del formato de archivo de valores separados con comas (CSV) para los archivos de salida del inventario. Para obtener más información, consulte ¿Cómo configuro el inventario de Amazon S3? (p. 59).	17 de noviembre de 2017
Comprobación de permisos del bucket	La comprobación de permisos del bucket de la consola de Amazon S3 comprueba las política de bucket y las listas de control de acceso (ACL) del bucket para identificar los buckets accesibles públicamente. Los permisos de los buckets permiten identificar más fácilmente los buckets de S3 que proporcionar acceso público de lectura y escritura. .	06 de noviembre de 2017
Cifrado predeterminado para los buckets de S3	El cifrado predeterminado de Amazon S3 proporciona un medio de definir el comportamiento de cifrado predeterminado para un bucket de S3. Puede configurar el cifrado predeterminado en un bucket para que todos los objetos se cifren cuando se almacenen en el bucket. Los objetos se protegen mediante cifrado en el servidor aplicando claves administradas por Amazon S3 (SSE-S3) o claves administradas por AWS KMS (SSE-KMS). Para obtener más información, consulte ¿Cómo puedo habilitar el cifrado predeterminado para un bucket de Amazon S3? (p. 8).	06 de noviembre de 2017
Estado de cifrado en el inventario de Amazon S3	Amazon S3 permite ahora incluir el estado de cifrado en el inventario de Amazon S3 para que pueda saber cómo se cifran los objetos en reposo para sus requisitos de conformidad u otros fines. También puede configurar el cifrado del inventario de Amazon S3 con cifrado de lado servidor (SSE) o SSE-KMS, para que todos los archivos del inventario se cifren según corresponda. Para obtener más información, consulte ¿Cómo configuro el inventario de Amazon S3? (p. 59).	06 de noviembre de 2017
Mejoras de la replicación entre regiones	La replicación entre regiones ahora admite lo siguiente: • De forma predeterminada, Amazon S3 no replica los objetos en el bucket de origen que se hayan creado mediante el cifrado de lado servidor utilizando claves administradas por AWS KMS. Ahora puede configurar una regla de replicación para replicar estos objetos. Para obtener más información, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52). • En un escenario de replicación entre cuentas, puede configurar una regla de replicación para cambiar la titularidad de la réplica a	06 de noviembre de 2017

Cambiar	Descripción	Fecha de modificación
	la cuenta de AWS que posee el bucket de destino. Para obtener más información, consulte ¿Cómo puedo agregar una regla de replicación a un bucket de S3? (p. 52).	
Se añadió funcionalidad y documentación	La consola de Amazon S3 ya es compatible con la habilitación del registro de nivel de objeto para un bucket de S3 con registro de evento de datos de AWS CloudTrail. Para obtener más información, consulte ¿Cómo se puede habilitar el registro en el nivel de objeto de un bucket de S3 con eventos de datos de AWS CloudTrail? (p. 11).	19 de octubre de 2017
La consola antigua de Amazon S3 ya no está disponible	La versión antigua de la consola de Amazon S3 ya no está disponible, y la guía de usuario antigua se ha eliminado del sitio de documentación de Amazon S3.	31 de agosto de 2017
Disponibilidad general de la nueva consola de Amazon S3	Se ha anunciado la disponibilidad general de la nueva consola de Amazon S3.	15 de mayo de 2017

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el glosario de AWS en la referencia general de AWS.