Guía del usuario

# Amazon S3 en Outposts

Versión de API 2006-03-01

# Amazon S3 en Outposts: Guía del usuario

# Table of Contents

# ¿Qué es Amazon S3 en Outposts?

AWS Outposts es un servicio totalmente administrado que ofrece la misma infraestructura de AWS, servicios de AWS, API y herramientas de prácticamente cualquier centro de datos, espacio de coubicación o instalación local para obtener una experiencia híbrida realmente uniforme.AWS Outposts es ideal para cargas de trabajo que requieren acceso de baja latencia a sistemas en las instalaciones, procesamiento de datos local, residencia de datos y migración de aplicaciones con interdependencias de sistemas locales. Para obtener más información, consulte ¿Qué es AWS Outposts? en la Guía del usuario de AWS Outposts.

Con Amazon S3 en Outposts, puede crear buckets de S3 en sus Outposts y almacenar y recuperar objetos fácilmente en las instalaciones. S3 en Outposts proporciona una nueva clase de almacenamiento, `OUTPOSTS`, que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de Outposts. Usted se comunica con su bucket de Outposts mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC).

Puede usar las mismas API y características en los buckets de Outposts que en Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST.



## Cómo funciona S3 en Outposts

S3 en Outposts es un servicio de almacenamiento de objetos que almacena datos como objetos dentro de buckets en Outpost. Un objeto es un archivo de datos y cualquier metadato que describa ese archivo. Un bucket es un contenedor de objetos.

Para almacenar datos en S3 en Outposts, primero debe crear un bucket. Al crear el bucket, debe especificar un nombre de bucket y el Outpost que lo contendrá. Para acceder a su bucket de S3 en

Outposts y realizar operaciones en objetos, debe crear y configurar un punto de acceso. También debe crear un punto de conexión para enrutar las solicitudes al punto de acceso.

Los puntos de acceso facilitan el acceso a datos para cualquier Servicio de AWS o aplicación de cliente que almacena datos en S3. Los puntos de acceso son puntos de conexión de red con nombre asociados a los buckets que se pueden utilizar para realizar operaciones con objetos, como `GetObject` y `PutObject`. Cada punto de acceso tiene permisos y controles de red distintos.

Puede crear y administrar sus buckets de S3 en Outposts, puntos de acceso y puntos de conexión mediante la AWS Management Console, AWS CLI, SDK de AWS o API de REST. Para cargar y administrar objetos en su bucket de S3 en Outposts, puede utilizar la AWS CLI, SDK de AWS o API de REST.

## Regiones

Durante el aprovisionamiento de AWS Outposts, usted o AWS crea una conexión de enlace de servicio que conecta su Outpost de nuevo a la Región de AWS elegida o la región de origen de Outposts para operaciones de buckets y telemetría. Un Outpost depende de la conectividad con la Región de AWS principal. El bastidor de Outposts no está diseñado para operaciones o entornos desconectados con conectividad limitada o nula. Para obtener más información, consulte Conectividad de Outpost a Regiones de AWS en la Guía del usuario de AWS Outposts.

## Buckets

Un bucket es un contenedor para objetos almacenados en S3 en Outposts. Puede almacenar cualquier cantidad de objetos en un bucket y puede tener hasta 100 buckets por cuenta y Outpost.

Cuando cree un bucket, introduzca un nombre de bucket y elija el Outpost donde residirá el bucket. Después de crear un bucket, no se puede cambiar su nombre ni moverlo a otro Outpost. Los nombres de los buckets deben cumplir las Reglas de nomenclatura de buckets de Amazon S3. En S3 en Outposts, los nombres de buckets son únicos de un Outpost y Cuenta de AWS. Los buckets de S3 en Outposts requieren el `outpost-id`, el `account-id` y el nombre del bucket para identificarlos.

En el siguiente ejemplo, se muestra el formato de nombre de recurso de Amazon (ARN) para los buckets de S3 en Outposts. El ARN consta de la región a la que está destinado el Outpost, su cuenta de Outpost, el ID de Outpost y el nombre del bucket.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Cuando especifica el bucket para las operaciones de objetos, se utiliza el ARN del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato de ARN del punto de acceso para S3 en Outposts, que incluye el `outpost-id`, `account-id`, y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de los buckets, consulte Trabajo con buckets de S3 en Outposts.

## Objects

Los objetos son las entidades fundamentales almacenadas en S3 en Outposts. Los objetos se componen de datos de objetos y metadatos. Los metadatos son conjuntos de pares nombre-valor que describen el objeto. Incluyen algunos metadatos predeterminados, como la fecha de la última modificación y los metadatos HTTP estándar, como `Content-Type`. También puede especificar metadatos personalizados en el momento en que se almacena el objeto. Un objeto se identifica de forma exclusiva dentro de un bucket con una clave (o nombre).

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

## Claves

Una clave de objeto (o nombre de clave) es el identificador único de un objeto dentro de un bucket. Cada objeto de un bucket tiene exactamente una clave. La combinación de un bucket y clave de objeto identifica de forma única cada objeto.

En el siguiente ejemplo, se muestra el formato ARN para los objetos de S3 en Outposts, que incluye el código de Región de AWS para la región a la que está destinado el Outpost, el ID de Cuenta de AWS, el ID de Outpost, el nombre del bucket y la clave de objeto:

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/ op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Para obtener más información sobre las claves de objetos, consulte Trabajo con objetos de S3 en Outposts.

## Control de versiones de S3

Puede usar el control de versiones de S3 en buckets de Outposts para conservar diversas variantes de un objeto en el mismo bucket. Puede utilizar el control de versiones de S3 para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de . EL control de versiones de S3 ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación.

Para obtener más información, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.

## ID de versión.

Si activa el control de versiones de S3 en un bucket, S3 en Outposts genera un ID de versión único para cada objeto agregado al bucket. Los objetos que ya existían en el bucket en el momento en que habilita el control de versiones tienen un ID de versión de `null`. Si modifica estos objetos (o cualquier otro) con otras operaciones, como PutObject, los objetos nuevos obtienen un ID de versión único.

Para obtener más información, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.

## Clase de almacenamiento y cifrado

S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (`OUTPOSTS`). La clase de almacenamiento de S3 Outposts solo está disponible para los objetos almacenados en buckets que se encuentran en AWS Outposts. Si intenta usar otras clases de almacenamiento de S3 con S3 en Outposts, S3 en Outposts devuelve el error `InvalidStorageClass`.

De manera predeterminada, los objetos almacenados en la clase de almacenamiento S3 Outposts (OUTPOSTS) siempre se cifran mediante cifrado del lado del servidor con claves de cifrado administradas (SSE-S3) de Amazon S3. Para obtener más información, consulte Cifrado de datos en S3 en Outposts.

## Política de bucket

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB.

Las políticas de buckets utilizan el lenguaje de políticas de IAM basado en JSON que es estándar en AWS. Puede utilizar directivas de bucket para agregar o denegar permisos para los objetos de un bucket. Las políticas de bucket permiten o deniegan solicitudes en función de los elementos de la política. Estos elementos puedne incluir el solicitante, las acciones de S3 en Outposts, los recursos y los aspectos o condiciones de la solicitud (por ejemplo: la dirección IP utilizada para realizar la solicitud). Por ejemplo, puede crear una política de bucket que otorgue permisos entre cuentas para cargar objetos en un bucket de S3 en Outpost y, al mismo tiempo, garantizar que el propietario del bucket tenga el control total de los objetos cargados.

En su política de bucket, puede utilizar caracteres comodín (*) en ARN y otros valores para otorgar permisos a un subconjunto de objetos. Por ejemplo, puede controlar el acceso a grupos de objetos que empiezan por un prefijo o terminar con una extensión dada, como `.html`.

## Puntos de acceso de S3 en Outposts

Los puntos de acceso de S3 en Outpost se denominan puntos de conexión de red con políticas de acceso dedicadas que describen cómo se puede acceder a los datos mediante ese punto de conexión. Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en S3 en Outposts. Los puntos de acceso se asocian a los buckets que se pueden utilizar para realizar operaciones con objetos de S3, como `GetObject` y `PutObject`.

Cuando especifica el bucket para las operaciones de objetos, se utiliza el ARN del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

Cada punto de acceso tiene permisos y controles de red distintos que S3 en Outposts se aplica a cualquier solicitud que se realice a través de ese punto de acceso. Cada punto de acceso aplica una política de punto de acceso personalizada que funciona en conjunción con la política de bucket asociada al bucket subyacente.

Para obtener más información, consulte Acceso a los buckets y objetos de S3 en Outposts.

# Características de S3 en Outposts

## Administración de accesos

Amazon S3 proporciona características para auditar y administrar el acceso a sus buckets y objetos. De forma predeterminada, los buckets de S3 en Outposts y los objetos que hay en ellos son privados. Solo tiene acceso a los recursos de S3 en Outpost que cree.

Para conceder permisos de recursos detallados que admitan su caso de uso específico o para auditar los permisos de sus recursos de S3 en Outpost, puede utilizar las siguientes características.

- Bloqueo del acceso público de S3: bloquea el acceso público a los buckets y objetos. Para buckets en Outposts, el bloqueo del acceso público siempre está habilitado de forma predeterminada.
- AWS Identity and Access Management (IAM): IAM es un servicio web que le ayuda a controlar de forma segura el acceso a los recursos de AWS, como los recursos de S3 en Outposts. Con IAM, se pueden administrar de forma centralizada los permisos que controlan a qué recursos de AWS pueden acceder los usuarios. Utilice IAM para controlar quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos.
- Puntos de acceso de S3 en Outposts: administre el acceso a los datos para los conjuntos de datos compartidos en S3 en Outposts. Los puntos de acceso se denominan puntos de conexión de red con nombre con políticas de acceso dedicadas. Los puntos de acceso se asocian a los buckets y se pueden utilizar para realizar operaciones con objetos, como `GetObject` y `PutObject`.
- Políticas de buckets: utilice el lenguaje de políticas basado en IAM para configurar permisos basados en recursos para los buckets de S3 y los objetos que hay en ellos.
- AWS Resource Access Manager (AWS RAM): comparta de forma segura su capacidad de S3 en Outposts en Cuentas de AWS, dentro de su organización o en unidades organizativas (OU) en AWS Organizations.

## Registro y monitorización

S3 en Outposts proporciona herramientas de registro y supervisión que puede utilizar para supervisar y controlar cómo se utilizan sus recursos de S3 en Outposts. Para obtener más información sobre la monitorización de , consulte .

- Métricas de Amazon CloudWatch para S3 en Outposts: realice un seguimiento del estado operativo de sus recursos y conozca la disponibilidad de su capacidad.
- Eventos de Amazon CloudWatch Events para S3 en Outposts: cree una regla para cualquier evento de API de S3 en Outposts para recibir notificaciones en todos los destinos de CloudWatch Events compatibles, incluidos Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) y AWS Lambda.
- Registros de AWS CloudTrail para S3 en Outposts: registre las medidas adoptadas por un usuario, un rol o un Servicio de AWS en S3 en Outposts. Los registros de CloudTrail le proporcionan un seguimiento detallado de la API para las operaciones a nivel de bucket y de objeto de Amazon S3.

## Consistencia sólida

S3 en Outposts proporciona una sólida coherencia de lectura tras escritura para las solicitudes PUT y DELETE de objetos del bucket de S3 en Outposts en todas las Regiones de AWS. Este comportamiento se aplica tanto a las escrituras en objetos nuevos como a las solicitudes PUT que sobrescriben objetos existentes y las solicitudes DELETE. Además, las etiquetas de objeto y los metadatos de objetos de S3 en Outposts (p. ej., el objeto HEAD) tienen una buena coherencia. Para obtener más información, consulte Modelo de consistencia de datos de Amazon S3 en la Guía del usuario de Amazon S3.

# Servicios relacionados

Una vez que cargue sus datos en S3 en Outposts, puede utilizarlos con otros Servicios de AWS. Los siguientes servicios son los que puede utilizar con más frecuencia:

- Amazon Elastic Compute Cloud (Amazon EC2): proporciona capacidad de computación escalable y segura en Nube de AWS. El uso de Amazon EC2 reduce la necesidad de invertir inicialmente en hardware, de manera que puede desarrollar e implementar aplicaciones en menos tiempo. Puede usar Amazon EC2 para lanzar tantos servidores virtuales como necesite, configurar la seguridad y las redes, y administrar el almacenamiento.

- Amazon Elastic Block Store (Amazon EBS) on Outposts: utilice Amazon EBS en instantáneas locales en Outposts para almacenar instantáneas de volúmenes en un Outpost localmente en S3 en Outposts.
- Amazon Relational Database Service (Amazon RDS) en Outposts: utilice las copias de seguridad locales de Amazon RDS para almacenar sus copias de seguridad de Amazon RDS localmente en su Outpost.
- AWS DataSync: automatice la transferencia de datos entre Outposts y Regiones de AWS mediante la elección de lo que se va a transferir, cuándo se va a transferir y cuánto ancho de banda de red se va a usar. S3 en Outposts se integra con AWS DataSync. Para las aplicaciones en las instalaciones que requieren un procesamiento local de alto rendimiento, S3 en Outposts proporciona almacenamiento de objetos en las instalaciones con el fin de minimizar las transferencias de datos y el búfer de las variaciones de red, al tiempo que permite transferir datos con facilidad entre Outposts y las Regiones de AWS.

# Acceso a S3 en Outposts

Puede trabajar con S3 en Outposts de cualquiera de las siguientes formas:

## AWS Management Console

La consola es una interfaz de usuario basada en la web para administrar S3 en Outposts y los recursos de AWS. Si se ha registrado en una Cuenta de AWS, puede acceder a S3 en Outposts iniciando sesión en la AWS Management Console y eligiendo S3 en la página de inicio de AWS Management Console. A continuación, elija Outposts buckets (Buckets de Outposts) desde el panel de navegación izquierdo.

## AWS Command Line Interface

Puede utilizar las herramientas de línea de comandos de AWS para emitir comandos o compilar scripts en la línea de comandos de su sistema con el fin de ejecutar tareas de AWS (incluidas las de S3).

AWS Command Line Interface (AWS CLI) proporciona comandos para una amplia gama de Servicios de AWS. La AWS CLI es compatible con Windows, macOS y Linux. Para empezar, consulte la AWS Command Line Interface Guía de usuario de . Para obtener más información acerca de los comandos que puede usar con S3 en Outposts, consultes3api, s3control y s3outposts en la Referencia de comandos de AWS CLI.

## SDK de AWS

AWS ofrece SDK (kits de desarrollo de software) que se componen de bibliotecas y código de muestra para diversos lenguajes de programación y plataformas (Java, Python, Ruby, .NET, iOS, Android, etc.). Los SDK de AWS proporcionan una forma cómoda de crear acceso de programación a S3 en Outposts y AWS. Dado que S3 en Outposts utiliza los mismos SDK que Amazon S3, S3 en Outposts proporciona una experiencia coherente utilizando las mismas API, automatización y herramientas de S3.

S3 en Outposts es un servicio REST. Puede enviar solicitudes a S3 en Outposts usando las bibliotecas de los SDK de AWS, que envuelven la API de REST subyacente y simplifican sus tareas de programación. Por ejemplo, los SDK se encargan de tareas como calcular firmas, firmar solicitudes criptográficamente, gestionar los errores y reintentar las solicitudes de forma automática. Para obtener información sobre los SDK de AWS (por ejemplo: cómo descargarlos e instalarlos), consulte Herramientas para crear en AWS.

# Pago de S3 en Outposts

Puede comprar una amplia variedad de configuraciones de bastidor de AWS Outposts que incluyen una combinación de tipos de instancias de Amazon EC2, volúmenes de unidades de estado sólido (SSD) de uso general de Amazon EBS (gp2) y S3 en Outposts. Los precios incluyen entrega, instalación y mantenimiento de servicios de infraestructura y parches y actualizaciones de software.

Para obtener más información, consulte Precios de bastidores de AWS Outposts.

# Siguientes pasos

Para obtener más información sobre cómo trabajar con S3 en Outposts, consulte los siguientes temas:

- Configuración de Outpost de
- ¿En qué se diferencia Amazon S3 en Outposts de Amazon S3?
- Introducción a Amazon S3 en Outposts
- Redes para S3 en Outposts
- Trabajo con buckets de S3 en Outposts
- Trabajo con objetos de S3 en Outposts

- Seguridad en S3 en Outposts
- Administración de almacenamiento de S3 en Outposts
- Desarrollo con Amazon S3 en Outposts

# Configuración de Outpost de

Para comenzar a utilizar Amazon S3 en Outposts necesita una publicación de salida con capacidad de Amazon S3 implementada en sus instalaciones. Para obtener información acerca de las opciones para solicitar una capacidad de Outpost y S3, consulte AWS Outposts. Para comprobar si sus Outposts tienen capacidad para S3, puede usar la llamada a la API ListOutpostsWithS3. Para obtener más información sobre las especificaciones y ver en qué se diferencia S3 en Outposts de Amazon S3, consulte ¿En qué se diferencia Amazon S3 en Outposts de Amazon S3?

Para obtener más información, consulte los siguientes temas.

Temas

- Solicite un nuevo Outpost de

## Solicite un nuevo Outpost de

Si necesita solicitar un nuevo Outpost con capacidad de S3, consulte los precios de AWS Outposts para comprender las opciones de capacidad de Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS) y Amazon S3.

Después de seleccionar la configuración, siga los pasos que se muestran en Crear un Outpost y solicitar la capacidad de Outpost en la Guía del usuario de AWS Outposts.

# ¿En qué se diferencia Amazon S3 en Outposts de Amazon S3?

Amazon S3 en Outposts ofrece almacenamiento de objetos a su entorno de AWS Outposts en las instalaciones. S3 en Outposts le ayuda a satisfacer el procesamiento local, la residencia de datos y las exigentes necesidades de rendimiento al mantener los datos cerca de las aplicaciones en las instalaciones. Debido a que usa las API y funciones de Amazon S3, S3 en Outposts facilita el almacenamiento, la seguridad, el etiquetado, la elaboración de informes y el control del acceso a los datos de sus Outposts y amplía la infraestructura de AWS a su instalación local para obtener una experiencia híbrida uniforme.

Para obtener más información acerca de cómo S3 en Outposts es único, consulte los siguientes temas.

Temas



## Especificaciones de S3 en Outposts

- El tamaño máximo del bucket de Outposts es de 50 TB.
- La cantidad máxima de buckets de Outposts es de 100 por Cuenta de AWS.
- Solo se puede acceder a los buckets de Outposts mediante puntos de acceso y puntos de conexión.
- El número máximo de puntos de acceso por bucket de Outposts es 10.
- Las políticas de punto de acceso tienen un límite de tamaño de 20 KB.
- El propietario de Outpost puede administrar el acceso dentro de la organización en AWS Organizations con AWS Resource Access Manager. Todas las cuentas que necesitan acceso a Outpost deben estar dentro de la misma organización que la cuenta de propietario en AWS Organizations.

- La cuenta de propietario del bucket S3 en Outposts siempre es propietaria de todos los objetos del bucket.
- Sólo la cuenta de propietario del bucket S3 en Outposts puede realizar operaciones en el bucket.
- Las limitaciones de tamaño de objeto son coherentes con Amazon S3.
- Todos los objetos almacenados en S3 en Outposts se almacenan en la clase de almacenamiento de `OUTPOSTS`.
- De forma predeterminada, todos los objetos almacenados en la clase de almacenamiento `OUTPOSTS` se almacenan mediante cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). También puede elegir almacenar objetos mediante cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C).
- Si no hay suficiente espacio para almacenar un objeto en su Outpost, la API devuelve una excepción de capacidad insuficiente (ICE).

## Operaciones de la API compatibles con S3 en Outposts

Para ver la lista de operaciones de la API que se admiten en S3 en Outposts, consulte Operaciones de la API de Amazon S3 en Outposts.

## Comandos de la AWS CLI de Amazon S3 compatibles con S3 en Outposts

Los siguientes comandos de la AWS CLI de Amazon S3 son compatibles actualmente con Amazon S3 en Outposts. Para obtener más información, consulte Comandos disponibles en la Referencia de comandos de la AWS CLI.

- `cp`, `mv` y `sync` en el mismo bucket de Outposts o entre un entorno local y un bucket de Outposts.
- `ls`
- `presign`
- `rm`

## Características de Amazon S3 no compatibles con S3 en Outposts

Las siguientes características de Amazon S3 no son actualmente compatibles con Amazon S3 en Outposts. Se rechaza cualquier intento de usarlas.

- Solicitudes condicionales
- Listas de control de acceso (ACL)
- Uso compartido de recursos entre orígenes (CORS)
- Operaciones por lotes de S3
- Informes de inventario de S3
- Cambio del cifrado predeterminado del bucket
- Buckets públicos
- Eliminación de la autenticación multifactor (MFA)
- Transiciones del ciclo de vida de S3 (además de la eliminación de objetos y la detención de cargas multiparte incompletas)
- Bloqueo de objetos de retención legal en S3
- Retención de bloqueo de objetos
- Cifrado del lado del servidor con claves AWS Key Management Service (AWS KMS) (SSE-KMS)
- Control del tiempo de replicación de S3 (S3 RTC)
- Métricas de solicitud de Amazon CloudWatch
- Configuración de métricas
- Transfer Acceleration
- Notificaciones de eventos de S3
- Los buckets de pago por solicitante
- S3 Select
- Eventos de AWS Lambda
- Server access logging (Registro de acceso del servidor)
- Solicitudes HTTP POST
- SOAP
- Acceso al sitio web

# Requisitos de red de S3 en Outposts

- Para enrutar solicitudes a un punto de acceso de S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Los siguientes límites se aplican a los puntos de enlace de S3 en Outposts:

  - Cada nube virtual privada (VPC) en un Outpost puede tener un punto de conexión asociado y puede tener hasta 100 puntos de conexión por Outpost.
  - Se pueden asignar varios puntos de acceso al mismo punto de conexión.
  - Los puntos de conexión solo se pueden agregar a VPC con bloques de CIDR en los subespacios de los siguientes rangos de CIDR:
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
- Los puntos de conexión de un Outpost solo se pueden crear a partir de las VPC que tengan bloques de CIDR no superpuestos.
- Solo se puede crear un punto de conexión desde su subred de Outposts.
- La subred utilizada para crear un punto de conexión debe contener cuatro direcciones IP para que S3 en Outposts pueda utilizarla.
- Si se especifica el grupo de direcciones IP propiedad del cliente (grupo de CoIP), este debe contener cuatro direcciones IP para que S3 en Outposts pueda utilizarlo.
- Solo puede crear un punto de conexión por Outpost por VPC.

# Introducción a Amazon S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (OUTPOSTS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST.

Amazon S3 en Outposts le permite utilizar las API y las características de Amazon S3, como el almacenamiento de objetos, las políticas de acceso, el cifrado y el etiquetado, en AWS Outposts como lo hace en Amazon S3. Para obtener información sobre S3 en Outposts, consulte ¿Qué es Amazon S3 en Outposts?

Temas

- Primeros pasos con AWS Management Console
- Introducción mediante AWS CLI y SDK para Java

## Primeros pasos con AWS Management Console

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (OUTPOSTS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

Para comenzar a utilizar S3 en Outposts mediante la consola, consulte los siguientes temas. Para comenzar a utilizar AWS CLI o AWS SDK para Java, consulte Introducción mediante AWS CLI y SDK para Java.

Temas



## Cree un bucket, un punto de acceso y un punto de conexión

El siguiente procedimiento muestra cómo crear el primer bucket en S3 en Outposts. La primera vez que crea un bucket con la consola, también crea un punto de acceso y un punto de conexión asociados al bucket para que pueda comenzar a almacenar objetos inmediatamente en el bucket.

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Seleccione Crear bucket de Outposts.
4. En Bucket name (Nombre del bucket), escriba un nombre compatible con sistema de nombres de dominio (DNS) para el bucket.

   El nombre del bucket debe:

   - Ser único dentro de la Cuenta de AWS, el Outpost y la Región de AWS al que está destinado el Outpost.
   - Tener de 3 a 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 más información sobre la nomenclatura de buckets, consulte Reglas de nomenclatura de buckets de uso general en la Guía del usuario de Amazon S3.

> **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.

5. En Outposts, elija el Outpost donde desea que resida el bucket.
6. En Bucket Versioning (Control de versiones de bucket), establezca el estado de control de versiones de S3 para su bucket de S3 on Outposts en una de las siguientes opciones:

   - Disable (Deshabilitar) (predeterminado): el bucket permanece sin versiones.
   - Enable (Habilitar): habilita el control de versiones de S3 para los objetos del bucket. Todos los objetos añadidos al bucket reciben un ID de versión único.

   Para obtener más información sobre el control de versiones de S3, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.
7. (Opcional) Agregue las etiquetas opcionales que desee asociar con el bucket de Outposts. Puede usar etiquetas para realizar un seguimiento de los criterios para proyectos individuales o grupos de proyectos o para etiquetar los buckets con etiquetas de asignación de costos.

   De manera predeterminada, todos los objetos almacenados en el bucket de Outposts se almacenan mediante cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). También puede elegir almacenar objetos mediante cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C). Para cambiar el tipo de cifrado, debe utilizar la API de REST, AWS Command Line Interface (AWS CLI) o SDK de AWS.
8. En la sección Configuración del punto de acceso de Outposts, introduzca el nombre del punto de acceso.

   Los puntos de acceso de S3 en Outposts simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en S3 en Outposts. Los puntos de acceso son puntos de enlace de red con nombre que están asociados a los buckets Outposts que se pueden utilizar para realizar operaciones con objetos de S3. Para obtener más información, consulte Puntos de acceso.

   Los nombres de los puntos de acceso deben ser únicos dentro de la cuenta para esta región y Outposts, y cumplir con las restricciones y limitaciones de puntos de acceso.

9. Elija la VPC para este punto de acceso de Amazon S3 en Outposts.

   Si no tiene una VPC, elija Create VPC (Crear VPC). Para obtener más información, consulte Crear puntos de acceso restringidos a una nube privada virtual (VPC) en la Guía del usuario de Amazon S3.

   Una nube virtual privada (VPC) le permite lanzar recursos de AWS en una red virtual que defina. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizarían en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

10. (Opcional para una VPC existente) Elija una Subred de punto de conexión para el punto de conexión.

    Una subred es un rango de direcciones IP en su VPC. Si no tiene la subred que desea, elija Create subnet (Crear subred). Para obtener más información, consulte Redes para S3 en Outposts.

11. (Opcional para una VPC existente) Elija un Grupo de seguridad de puntos de conexión para el punto de conexión.

    Un grupo de seguridad funciona como un firewall virtual para controlar el tráfico entrante y saliente.

12. (Opcional para una VPC existente) Elija el Endpoint access type (Tipo de acceso al punto de conexión):

    - Privado: para utilizarse con la VPC.
    - IP de propiedad del cliente: se utiliza con un grupo de direcciones IP (grupo CoIP) desde la red de las instalaciones.

13. (Opcional) Especifique la Outpost access point policy (Política de punto de acceso de Outpost). La consola muestra automáticamente el nombre de recurso de Amazon (ARN) para el punto de acceso, que puede utilizar en la política.

14. Seleccione Crear bucket de Outposts.

> **Note**
>
> Puede tardar hasta 5 minutos para que se cree el punto de conexión de Outpost y se pueda usar el bucket. Para configurar opciones adicionales de bucket, elija View details (Ver detalles).

## Siguientes pasos

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

Después de crear un bucket de S3 en Outposts, un punto de acceso y un punto de conexión, puede utilizar la AWS CLI o el SDK para Java para cargar un objeto en el bucket. Para obtener más información, consulte Carga de un objeto en un bucket de S3 en Outpost.

# Introducción mediante AWS CLI y SDK para Java

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (`OUTPOSTS`), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?.

Para empezar a utilizar S3 en Outposts, debe crear un bucket, un punto de acceso y un punto de conexión. Luego, puede cargar objetos en el bucket. Los siguientes ejemplos muestran cómo puede utilizar S3 en Outposts mediante AWS CLI y el SDK para Java. Para comenzar mediante la consola, consulte Primeros pasos con AWS Management Console.

Temas

- Paso 1: Crear un bucket
- Paso 2: Crear un punto de acceso
- Paso 3: Crear un punto de conexión

- Paso 4: Cargar un objeto en un bucket de S3 en Outposts

## Paso 1: Crear un bucket

Los siguientes ejemplos de AWS CLI y SDK para Java muestran cómo puede crear un bucket de S3 en Outposts.

AWS CLI

Example

En el siguiente ejemplo, se crea un bucket de S3 en Outposts (`s3-outposts:CreateBucket`) con la AWS CLI. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-
id op-01ac5d28a6a232904
```

SDK for Java

Example

En el siguiente ejemplo, se crea un bucket de S3 en Outposts (`s3-outposts:CreateBucket`) con el SDK para Java.

```
import com.amazonaws.services.s3control.model.*;

public String createBucket(String bucketName) {

    CreateBucketRequest reqCreateBucket = new CreateBucketRequest()
            .withBucket(bucketName)
            .withOutpostId(OutpostId)
            .withCreateBucketConfiguration(new CreateBucketConfiguration());

    CreateBucketResult respCreateBucket =
 s3ControlClient.createBucket(reqCreateBucket);
    System.out.printf("CreateBucket Response: %s%n", respCreateBucket.toString());

    return respCreateBucket.getBucketArn();

}
```

# Paso 2: Crear un punto de acceso

Para acceder a su bucket de Amazon S3 en Outposts, debe crear y configurar un punto de acceso. En estos ejemplos, se explica cómo crear un punto de acceso mediante AWS CLI y el SDK para Java.

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

AWS CLI

Example

En el siguiente ejemplo de la AWS CLI, se crea un punto de acceso para un bucket de Outposts. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control create-access-point --account-id 123456789012
 --name example-outposts-access-point --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket" --vpc-configuration VpcId=example-vpc-12345
```

SDK for Java

Example

En el siguiente ejemplo del SDK para Java, se crea un punto de acceso para un bucket de Outposts. Para utilizar este ejemplo, reemplace los *`user input placeholders`* con su propia información.

```
import com.amazonaws.services.s3control.model.*;

public String createAccessPoint(String bucketArn, String accessPointName) {

    CreateAccessPointRequest reqCreateAP = new CreateAccessPointRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
```

```
            .withName(accessPointName)
            .withVpcConfiguration(new VpcConfiguration().withVpcId("vpc-12345"));

    CreateAccessPointResult respCreateAP =
 s3ControlClient.createAccessPoint(reqCreateAP);
    System.out.printf("CreateAccessPoint Response: %s%n", respCreateAP.toString());

    return respCreateAP.getAccessPointArn();

}
```

## Paso 3: Crear un punto de conexión

Para dirigir solicitudes a un punto de acceso de Amazon S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Para crear un punto de conexión, necesita una conexión activa con el enlace de servicio a la región de origen de Outposts. Cada nube virtual privada (VPC) de su Outpost puede tener un punto de conexión asociado. Para obtener más información acerca de las cuotas de los puntos de conexión, consulte Requisitos de red de S3 en Outposts. Debe crear un punto de conexión para poder acceder a los buckets de Outposts y realizar operaciones de objetos. Para obtener más información, consulte Puntos de conexión.

En estos ejemplos, se muestra cómo crear un punto de conexión mediante AWS CLI y el SDK para Java. Para obtener más información acerca de los permisos necesarios para crear y administrar puntos de conexión, consulte Permisos para los puntos de conexión de S3 en Outposts.

AWS CLI

Example

En el siguiente ejemplo de la AWS CLI, se crea un punto de conexión para un Outpost con el tipo de acceso a recursos de la VPC. La VPC se obtiene de la subred. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

En el siguiente ejemplo de la AWS CLI, se crea un punto de conexión para un Outpost con el tipo de acceso de grupo de direcciones IP propiedad del cliente (grupo de CoIP). Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --
customer-owned-ipv4-pool ipv4pool-coip-12345678901234567
```

SDK for Java

Example

En el siguiente ejemplo del SDK para Java, se crea un punto de conexión para un Outpost. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.CreateEndpointRequest;
import com.amazonaws.services.s3outposts.model.CreateEndpointResult;

public void createEndpoint() {
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    CreateEndpointRequest createEndpointRequest = new CreateEndpointRequest()
                .withOutpostId("op-0d79779cef3c30a40")
                .withSubnetId("subnet-8c7a57c5")
                .withSecurityGroupId("sg-ab19e0d1")
                .withAccessType("CustomerOwnedIp")
                .withCustomerOwnedIpv4Pool("ipv4pool-coip-12345678901234567");
    // Use .withAccessType and .withCustomerOwnedIpv4Pool only when the access type
 is
    // customer-owned IP address pool (CoIP pool)
    CreateEndpointResult createEndpointResult =
 s3OutpostsClient.createEndpoint(createEndpointRequest);
    System.out.println("Endpoint is created and its ARN is " +
 createEndpointResult.getEndpointArn());
}
```

## Paso 4: Cargar un objeto en un bucket de S3 en Outposts

Para cargar un objeto, consulte Carga de un objeto en un bucket de S3 en Outpost.

# Redes para S3 en Outposts

Puede utilizar Amazon S3 en Outposts para almacenar y recuperar objetos locales para aplicaciones que requieren acceso a datos locales, procesamiento de datos y residencia de datos. En esta sección se describen los requisitos de red para acceder a S3 en Outposts.

Temas



## Elección del tipo de acceso de red

Puede acceder a S3 en Outposts desde una VPC o desde su red en las instalaciones. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión. Esta conexión mantiene el tráfico entre su VPC y sus buckets S3 en Outposts dentro de la red de AWS. Cuando se crea un punto de conexión, se debe especificar el tipo de acceso de punto de conexión entre `Private` (para enrutamiento VPC) o `CustomerOwnedIp` (para grupo de dirección IP propiedad del cliente [grupo CoIP]).

- `Private` (para el enrutamiento de VPC): si no se especifica el tipo de acceso, S3 en Outposts se utiliza `Private` de forma predeterminada. Con el tipo de acceso `Private`, las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los recursos de su Outposts. Puede trabajar con S3 en Outposts desde una VPC. Este tipo de punto de conexión es accesible desde la red en las instalaciones a través del enrutamiento directo de VPC. Para obtener más información, consulte Tablas de enrutamiento de puerta de enlace locales en la Guía del usuario de AWS Outposts.
- `CustomerOwnedIp` (para el grupo de CoIP): si no se utiliza de forma predeterminada el tipo de acceso `Private` y elige `CustomerOwnedIp`, debe especificar un rango de direcciones IP. Puede usar este tipo de acceso para trabajar con S3 en Outposts desde la red de las instalaciones y en VPC. Al acceder a S3 en Outposts dentro de una VPC, su tráfico está limitado a la banda ancha de la gateway local.

# Acceso a los buckets y objetos de S3 en Outposts

Para acceder a sus cubos y objetos de S3 en Outposts, debe tener lo siguiente:

- Un punto de acceso para VPC
- Un punto de enlace para la misma VPC
- Una conexión activa entre Outpost y su Región de AWS. Para obtener más información sobre cómo conectar su Outpost con una región, consulte Conectividad de Outpost con regiones de AWS en la AWSGuía de usuario de Outposts.

Para obtener más información acerca de cómo acceder a buckets y objetos en S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts y Trabajo con objetos de S3 en Outposts.

# Interfaces de red elástica entre cuentas

Los puntos de conexión de S3 en Outposts son recursos designados con nombres de recurso de Amazon (ARN). Cuando se crean estos puntos de enlace, AWS Outposts configura cuatro interfaces de red elástica entre cuentas. Las interfaces de red elástica entre cuentas de S3 en Outposts son como otras interfaces de red con una excepción: S3 en Outposts asocia las interfaces de red elásticas entre cuentas con instancias de Amazon EC2.

La carga del sistema de nombres de dominio (DNS) de S3 en Outposts equilibra las solicitudes sobre la interfaz de red elástica entre cuentas. S3 en Outposts crea la interfaz de red elástica entre cuentas en su cuenta de AWS que es visible desde el panel Network interfaces (Interfaces de red) de la consola de Amazon EC2.

Para los puntos de enlace que utilizan el tipo de acceso de grupo de CoIP, S3 en Outposts asigna y asocia direcciones IP a la interfaz de red elástica entre cuentas desde el grupo de CoIP configurado.

# Trabajo con buckets de S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en AWS Outposts y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (`OUTPOSTS`), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Puede usar las mismas API y características en los buckets de Outpost que en Amazon S3, como políticas de acceso, cifrado y etiquetado. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

Usted se comunica con sus buckets de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Para acceder a sus buckets y objetos de S3 en Outposts, debe tener un punto de acceso para la VPC y un punto de conexión para la misma VPC. Para obtener más información, consulte Redes para S3 en Outposts.

## Buckets

En S3 en Outposts, los nombres de bucket son únicos de un Outpost y requieren el código de Región de AWS para la región a la que está destinado el Outpost, el ID de Cuenta de AWS, el ID de Outpost y el nombre del bucket para identificarlos.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Para obtener más información, consulte ARN de recursos para S3 en Outposts.

## Puntos de acceso

Amazon S3 en Outposts admite puntos de acceso únicamente de la virtual private cloud (VPC) como el único medio para acceder a los buckets de Outposts.

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

En el siguiente ejemplo, se muestra el formato ARN que se utiliza para los puntos de acceso de S3 en Outposts. El ARN de punto de acceso incluye el código de Región de AWS para la región a la que está destinado el Outpost, el ID de Cuenta de AWS, el ID de Outpost y el nombre de punto de acceso.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

## Puntos de conexión

Para enrutar solicitudes a un punto de acceso de S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Con los puntos de conexión de S3 en Outposts, puede conectar de forma privada su VPC al bucket de Outpost. Los puntos de enlace de S3 en Outposts son identificadores de recursos uniformes (URI) virtuales del punto de entrada al bucket de S3 en Outposts. Son componentes de VPC escalados horizontalmente, redundantes y de alta disponibilidad.

Cada nube virtual privada (VPC) en su Outpost puede tener un punto de conexión asociado y puede tener hasta 100 puntos de conexión por Outpost. Debe crear estos puntos de conexión para poder acceder a los buckets de Outpost y realizar operaciones de objetos. De esta forma, también hace que el modelo y los comportamientos de la API sean los mismos al permitir que las mismas operaciones funcionen en S3 y S3 en Outposts.

## Operaciones de API en S3 en Outposts

S3 en Outposts aloja un punto de conexión separado para administrar las operaciones de API de bucket de Outposts distintas de los puntos de conexión de Amazon S3. Este punto de enlace es `s3-outposts.region.amazonaws.com`.

Para utilizar las operaciones de la API de Amazon S3, debe firmar el bucket y los objetos con el formato ARN correcto. Debe pasar ARN para las operaciones de API a fin de que Amazon S3 pueda determinar si la solicitud es para Amazon S3 (`s3-control.region.amazonaws.com`) o S3 en Outposts (`s3-outposts.region.amazonaws.com`). Según el formato ARN, luego S3 puede firmar y dirigir la solicitud de forma adecuada.

Siempre que la solicitud se envía al plano de control de Amazon S3, el SDK extrae los componentes del ARN e incluye un encabezado adicional `x-amz-outpost-id` con el valor de `outpost-id` que se extrajo del ARN. El nombre del servicio del ARN se utiliza para firmar la solicitud antes de que se

dirija al punto de enlace de S3 en Outposts. Este comportamiento se aplica a todas las operaciones de API manejadas por el cliente `s3control`.

En la siguiente tabla, se enumeran las operaciones API ampliadas para Amazon S3 en Outposts y sus cambios en relación con Amazon S3.

| API | Valor del parámetro de S3 en Outposts | |
|---|---|---|
| `CreateBucket` | Nombre del bucket como ARN, ID de Outpost | |
| `ListRegionalBuckets` | ID de Outpost | |
| `DeleteBucket` | Nombre del bucket como ARN | |
| `DeleteBucketLifecycleConfiguration` | Nombre del bucket como ARN | |
| `GetBucketLifecycleConfiguration` | Nombre del bucket como ARN | |
| `PutBucketLifecycleConfiguration` | Nombre del bucket como ARN | |
| `GetBucketPolicy` | Nombre del bucket como ARN | |
| `PutBucketPolicy` | Nombre del bucket como ARN | |
| `DeleteBucketPolicy` | Nombre del bucket como ARN | |
| `GetBucketTagging` | Nombre del bucket como ARN | |
| `PutBucketTagging` | Nombre del bucket como ARN | |
| `DeleteBucketTagging` | Nombre del bucket como ARN | |
| `CreateAccessPoint` | Nombre del punto de acceso como ARN | |

| API | Valor del parámetro de S3 en Outposts | |
|---|---|---|
| `DeleteAccessPoint` | Nombre del punto de acceso como ARN | |
| `GetAccessPoint` | Nombre del punto de acceso como ARN | |
| `GetAccessPoint` | Nombre del punto de acceso como ARN | |
| `ListAccessPoints` | Nombre del punto de acceso como ARN | |
| `PutAccessPointPolicy` | Nombre del punto de acceso como ARN | |
| `GetAccessPointPolicy` | Nombre del punto de acceso como ARN | |
| `DeleteAccessPointPolicy` | Nombre del punto de acceso como ARN | |

# Creación y administración de buckets de S3 en Outposts

Para obtener más información acerca de cómo crear y administrar los buckets de S3 en Outposts, consulte los siguientes temas.

# Creación de un bucket de S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en AWS Outposts y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (`OUTPOSTS`), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede

usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede confirmarle acciones. Los buckets tienen propiedades de configuración como Outpost, etiquetas, cifrado predeterminado y valores de puntos de acceso. La configuración de punto de acceso incluye la VPC (nube virtual privada) y la política de punto de acceso para acceder a los objetos del bucket y otros metadatos. Para obtener más información, consulte Especificaciones de S3 en Outposts.
>
> Si desea crear un bucket que utilice AWS PrivateLink para proporcionar acceso a la administración de buckets y puntos de conexión a través de puntos de conexión de VPC de la interfaz en su nube privada virtual (VPC), consulte AWS PrivateLink para S3 en Outposts.

En los siguientes ejemplos se muestra cómo crear un bucket de S3 en Outposts con la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

## Uso de la consola de S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Seleccione Crear bucket de Outposts.
4. En Bucket name (Nombre del bucket), escriba un nombre compatible con sistema de nombres de dominio (DNS) para el bucket.

   El nombre del bucket debe:

   - Ser único dentro de la Cuenta de AWS, el Outpost y la Región de AWS al que está destinado el Outpost.
   - Tener de 3 a 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 más información sobre la nomenclatura de buckets, consulte Reglas de nomenclatura de buckets de uso general en la Guía del usuario de Amazon S3.

> **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.

5. En Outposts, elija el Outpost donde desea que resida el bucket.
6. En Bucket Versioning (Control de versiones de bucket), establezca el estado de control de versiones de S3 para su bucket de S3 on Outposts en una de las siguientes opciones:

   - Disable (Deshabilitar) (predeterminado): el bucket permanece sin versiones.
   - Enable (Habilitar): habilita el control de versiones de S3 para los objetos del bucket. Todos los objetos añadidos al bucket reciben un ID de versión único.

   Para obtener más información sobre el control de versiones de S3, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.
7. (Opcional) Agregue las etiquetas opcionales que desee asociar con el bucket de Outposts. Puede usar etiquetas para realizar un seguimiento de los criterios para proyectos individuales o grupos de proyectos o para etiquetar los buckets con etiquetas de asignación de costos.

   De manera predeterminada, todos los objetos almacenados en el bucket de Outposts se almacenan mediante cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). También puede elegir almacenar objetos mediante cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C). Para cambiar el tipo de cifrado, debe utilizar la API de REST, AWS Command Line Interface (AWS CLI) o SDK de AWS.
8. En la sección Configuración del punto de acceso de Outposts, introduzca el nombre del punto de acceso.

   Los puntos de acceso de S3 en Outposts simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en S3 en Outposts. Los puntos de acceso son puntos de enlace de red con nombre que están asociados a los buckets Outposts que se

pueden utilizar para realizar operaciones con objetos de S3. Para obtener más información, consulte Puntos de acceso.

Los nombres de los puntos de acceso deben ser únicos dentro de la cuenta para esta región y Outposts, y cumplir con las restricciones y limitaciones de puntos de acceso.

9. Elija la VPC para este punto de acceso de Amazon S3 en Outposts.

   Si no tiene una VPC, elija Create VPC (Crear VPC). Para obtener más información, consulte Crear puntos de acceso restringidos a una nube privada virtual (VPC) en la Guía del usuario de Amazon S3.

   Una nube virtual privada (VPC) le permite lanzar recursos de AWS en una red virtual que defina. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizarían en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

10. (Opcional para una VPC existente) Elija una Subred de punto de conexión para el punto de conexión.

    Una subred es un rango de direcciones IP en su VPC. Si no tiene la subred que desea, elija Create subnet (Crear subred). Para obtener más información, consulte Redes para S3 en Outposts.

11. (Opcional para una VPC existente) Elija un Grupo de seguridad de puntos de conexión para el punto de conexión.

    Un grupo de seguridad funciona como un firewall virtual para controlar el tráfico entrante y saliente.

12. (Opcional para una VPC existente) Elija el Endpoint access type (Tipo de acceso al punto de conexión):

    - Privado: para utilizarse con la VPC.
    - IP de propiedad del cliente: se utiliza con un grupo de direcciones IP (grupo CoIP) desde la red de las instalaciones.

13. (Opcional) Especifique la Outpost access point policy (Política de punto de acceso de Outpost). La consola muestra automáticamente el nombre de recurso de Amazon (ARN) para el punto de acceso, que puede utilizar en la política.

14. Seleccione Crear bucket de Outposts.

> **Note**
>
> Puede tardar hasta 5 minutos para que se cree el punto de conexión de Outpost y se pueda usar el bucket. Para configurar opciones adicionales de bucket, elija View details (Ver detalles).

## Uso de la AWS CLI

### Example

En el siguiente ejemplo, se crea un bucket de S3 en Outposts (`s3-outposts:CreateBucket`) con la AWS CLI. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-
id op-01ac5d28a6a232904
```

## Uso de AWS SDK para Java

### Example

En el siguiente ejemplo, se crea un bucket de S3 en Outposts (`s3-outposts:CreateBucket`) con el SDK para Java.

```
import com.amazonaws.services.s3control.model.*;

public String createBucket(String bucketName) {

    CreateBucketRequest reqCreateBucket = new CreateBucketRequest()
            .withBucket(bucketName)
            .withOutpostId(OutpostId)
            .withCreateBucketConfiguration(new CreateBucketConfiguration());

    CreateBucketResult respCreateBucket =
 s3ControlClient.createBucket(reqCreateBucket);
    System.out.printf("CreateBucket Response: %s%n", respCreateBucket.toString());

    return respCreateBucket.getBucketArn();
```

```
}
```

# Agregar etiquetas para los buckets de S3 en Outposts

Puede agregar etiquetas para los buckets de Amazon S3 en Outposts para realizar un seguimiento de los costos de almacenamiento y otros criterios para proyectos individuales o grupos de proyectos.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede cambiar sus etiquetas.

## Uso de la consola de S3

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación izquierdo, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts cuyas etiquetas desea editar.
4. Elija la pestaña Propiedades.
5. En Tags (Etiquetas), elija Edit (Editar).
6. Elija Add new tag (Agregar nueva etiqueta) e introduzca la clave y el valor opcional.

   Agregue las etiquetas que desee asociar con un bucket de Outposts para realizar un seguimiento de otros criterios para proyectos individuales o grupos de proyectos.
7. Elija Guardar cambios.

## Uso de la AWS CLI

El siguiente ejemplo de AWS CLI aplica una configuración de etiquetado a un bucket de S3 en Outposts mediante un documento JSON de la carpeta actual que especifica etiquetas (*`tagging.json`*). Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --tagging file://tagging.json
```

*tagging.json*

```
{
   "TagSet": [
     {
       "Key": "organization",
       "Value": "marketing"
     }
   ]
}
```

El siguiente ejemplo de AWS CLI aplica una configuración de etiquetado a un bucket de S3 en Outposts directamente desde la línea de comandos.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --tagging 'TagSet=[{Key=organization,Value=marketing}]'
```

Para obtener más información acerca de este comando, consulte put-bucket-tagging en la Referencia de AWS CLI.

## Administración del acceso a su bucket de Amazon S3 en Outposts mediante una política de bucket

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB. Para obtener más información, consulte Política de bucket.

Puede actualizar la política de bucket para administrar el acceso a su bucket de Amazon S3 en Outposts. Para obtener más información, consulte los siguientes temas.

Temas

- Adición o edición de una política de bucket para un bucket de Amazon S3 en Outposts
- Visualización de la política de bucket para el bucket de Amazon S3 en Outposts
- Eliminación de la política de bucket para su bucket de Amazon S3 en Outposts

- Ejemplos de política de bucket

## Adición o edición de una política de bucket para un bucket de Amazon S3 en Outposts

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB. Para obtener más información, consulte Política de bucket.

En los siguientes temas, se le mostrará cómo actualizar su política de bucket de Amazon S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS SDK para Java.

Uso de la consola de S3

Para crear o editar una política de bucket

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts cuya política de bucket desea editar.
4. Elija la pestaña Permisos.
5. En la sección Outposts bucket policy (Política del bucket de Outposts), para crear o editar una nueva política, elija Edit (Editar).

   Ahora puede agregar o editar la política de bucket S3 en Outposts. Para obtener más información, consulte Configuración de IAM con S3 en Outposts.

Mediante AWS CLI

En el siguiente ejemplo de la AWS CLI, se aplica una política en un bucket de Outposts.

1. Guarde la política de bucket siguiente en un archivo JSON. En este ejemplo, el archivo se denomina `policy1.json`. Reemplace los *`user input placeholders`* con su propia información.

```
{
   "Version":"2012-10-17",
   "Id":"testBucketPolicy",
   "Statement":[
      {
         "Sid":"st1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"123456789012"
         },
         "Action":"s3-outposts:*",
         "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket"
      }
   ]
}
```

2. Envíe el archivo JSON como parte del comando de la CLI `put-bucket-policy`. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control put-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --policy file://policy1.json
```

### Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se aplica una política en un bucket de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketPolicy(String bucketArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testBucketPolicy\",
\"Statement\":[{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
 AccountId+ "\"},\"Action\":\"s3-outposts:*\",\"Resource\":\"" + bucketArn + "\"}]}";

    PutBucketPolicyRequest reqPutBucketPolicy = new PutBucketPolicyRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
            .withPolicy(policy);
```

```
    PutBucketPolicyResult respPutBucketPolicy =
 s3ControlClient.putBucketPolicy(reqPutBucketPolicy);
    System.out.printf("PutBucketPolicy Response: %s%n",
 respPutBucketPolicy.toString());

}
```

## Visualización de la política de bucket para el bucket de Amazon S3 en Outposts

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB. Para obtener más información, consulte Política de bucket.

En los siguientes temas, se muestra cómo ver la política de bucket de Amazon S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS SDK para Java.

Uso de la consola de S3

Para crear o editar una política de bucket

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts cuyo permiso desea editar.
4. Elija la pestaña Permissions.
5. En la sección Outposts bucket policy (Política de bucket de Outposts), puede revisar su política de bucket existente. Para obtener más información, consulte Configuración de IAM con S3 en Outposts.

Mediante AWS CLI

En el siguiente ejemplo de la AWS CLI, se obtiene una política para un bucket de Outposts. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3control get-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket
```

Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se obtiene una política para un bucket de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketPolicy(String bucketArn) {

    GetBucketPolicyRequest reqGetBucketPolicy = new GetBucketPolicyRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    GetBucketPolicyResult respGetBucketPolicy =
 s3ControlClient.getBucketPolicy(reqGetBucketPolicy);
    System.out.printf("GetBucketPolicy Response: %s%n",
 respGetBucketPolicy.toString());

}
```

## Eliminación de la política de bucket para su bucket de Amazon S3 en Outposts

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB. Para obtener más información, consulte Política de bucket.

En los siguientes temas, se muestra cómo ver la política de bucket de Amazon S3 en Outposts mediante la AWS Management Console o AWS Command Line Interface (AWS CLI).

Uso de la consola de S3

Para eliminar una política de bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts cuyo permiso desea editar.
4. Elija la pestaña Permissions.
5. En la sección Outposts bucket policy (Política de bucket de Outposts), seleccione Delete (Eliminar).
6. Confirme la eliminación.

Uso de la AWS CLI

En el siguiente ejemplo, se elimina la política de bucket para un bucket de S3 en Outposts (`s3-outposts:DeleteBucket`) utilizando la AWS CLI. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control delete-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

## Ejemplos de política de bucket

Las políticas de bucket de S3 en Outposts le permiten proteger el acceso a los objetos de sus buckets de S3 en Outposts, de modo que solo los usuarios con los permisos adecuados puedan acceder a ellos. Incluso puede impedir que los usuarios autenticados que no dispongan de los permisos adecuados accedan a los recursos de S3 en Outposts.

En esta sección se presentan ejemplos de casos de uso típicos de políticas de bucket de S3 en Outposts. Para probar estas políticas, sustituya *`user input placeholders`* por su propia información (como el nombre del bucket).

Para conceder o denegar permisos a un conjunto de objetos, puede usar caracteres comodín (`*`) en nombres de recurso de Amazon (ARN) y otros valores. Por ejemplo, puede controlar el acceso a grupos de objetos que empiezan por un prefijo o terminar con una extensión dada, como `.html`.

Para obtener más información sobre el lenguaje de la política de AWS Identity and Access Management (IAM), consulte Configuración de IAM con S3 en Outposts.

> **Note**
>
> Si utiliza la consola de Amazon S3 para probar los permisos de s3outposts, debe conceder permisos adicionales requeridos por la consola como `s3outposts:createendpoint` o `s3outposts:listendpoints`, entre otros.

Recursos adicionales para crear políticas de bucket

- Para obtener una lista de las acciones, los recursos y las claves de condición de la política de IAM que puede utilizar al crear una política de bucket de S3 en Outposts, consulte Actions, resources, and condition keys for Amazon S3 on Outposts.
- Para obtener información sobre cómo crear una política de S3 en Outposts, consulte Adición o edición de una política de bucket para un bucket de Amazon S3 en Outposts.

Temas

- Gestión del acceso a un bucket de Amazon S3 en Outposts en función de determinadas direcciones IP

## Gestión del acceso a un bucket de Amazon S3 en Outposts en función de determinadas direcciones IP

Una política de bucket es una política AWS Identity and Access Management basada en recursos (IAM) que puede utilizar para conceder permisos de acceso al bucket y a los objetos que contiene. Solo el propietario del bucket puede asociar una política a un bucket. Los permisos asociados a un bucket se aplican a todos los objetos del bucket que son propiedad de la cuenta de propietario del bucket. Las políticas de bucket tienen un límite de tamaño de 20 KB. Para obtener más información, consulte Política de bucket.

Restringir el acceso a direcciones IP específicas

En el siguiente ejemplo se impide que los usuarios realicen operaciones de S3 en Outposts en objetos en los buckets especificados, a menos que la solicitud se origine en el rango de direcciones IP especificado.

> **Note**
>
> Al restringir el acceso a una dirección IP concreta, asegúrese de especificar también qué puntos de conexión de VPC, direcciones IP de origen de VPC o direcciones IP externas pueden acceder al bucket de S3 en Outposts. De lo contrario, podría perder el acceso al bucket si su política deniega a todos los usuarios realizar cualquier operación de s3outposts en los objetos de su bucket de S3 en Outposts sin contar con los permisos adecuados.

La instrucción `Condition` de esta política identifica *`192.0.2.0/24`* como el rango de direcciones IP permitidas del IP versión 4 (IPv4).

El bloque `Condition` utiliza la condición `NotIpAddress` y la clave de condición `aws:SourceIp`, que es una clave de condición general de AWS. La clave de condición `aws:SourceIp` solo puede utilizarse para rangos de direcciones IP públicas. Para obtener más información acerca de estas claves de condición, consulte Actions, resources, and condition keys for S3 on Outposts. Los valores de IPv4 `aws:SourceIp` utilizan la notación CIDR estándar. Para obtener más información, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

> **Warning**
>
> Antes de utilizar esta política de S3 en Outposts, reemplace el rango de direcciones IP *`192.0.2.0/24`* de este ejemplo por un valor adecuado para su caso de uso. De lo contrario, ya no podrá acceder a su bucket.

```
{
    "Version": "2012-10-17",
    "Id": "S3OutpostsPolicyId1",
    "Statement": [
        {
            "Sid": "IPAllow",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3-outposts:*",
            "Resource": [
                "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
accesspoint/EXAMPLE-ACCESS-POINT-NAME",
                "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/amzn-s3-demo-bucket"
```

```
            ],
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                }
            }
        }
    ]
}
```

Permitir direcciones IPv4 e IPv6

Cuando empiece a usar direcciones IPv6, le recomendamos que actualice todas las políticas de la organización con los rangos de direcciones IPv6 además de los rangos de direcciones IPv4 existentes. De este modo se asegurará de que las políticas sigan funcionando durante la transición a IPv6.

En el siguiente ejemplo de política de bucket de S3 en Outposts se muestra cómo combinar los rangos de dirección IPv4 e IPv6 para incluir todas las direcciones IP válidas de la organización. La política de ejemplo permite el acceso a las direcciones IP de ejemplo *192.0.2.1* y *2001:DB8:1234:5678::1*, y deniega el acceso a las direcciones *203.0.113.1* y *2001:DB8:1234:5678:ABCD::1*.

La clave de condición `aws:SourceIp` solo puede utilizarse para rangos de direcciones IP públicas. Los valores de IPv6 para `aws:SourceIp` deben estar en formato CIDR estándar. Para IPv6, aceptamos el uso de `::` para representar un rango de 0, (por ejemplo, `2001:DB8:1234:5678::/64`). Para obtener más información, consulte Operadores de condición de dirección IP en la Guía del usuario de IAM.

> **Warning**
>
> Antes de utilizar esta política de S3 en Outposts, sustituya los intervalos de direcciones IP del ejemplo por valores adecuados para su caso de uso. De lo contrario, puede perder la capacidad de acceder a su bucket.

```
{
    "Id": "S3OutpostsPolicyId2",
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowIPmix",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3outposts:*",
            "Resource": [
                "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/amzn-s3-demo-bucket",
                    "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-
ID/bucket/amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "2001:DB8:1234:5678::/64"
                    ]
                },
                "NotIpAddress": {
                    "aws:SourceIp": [
                        "203.0.113.0/24",
                        "2001:DB8:1234:5678:ABCD::/80"
                    ]
                }
            }
        }
    ]
}
```

# Obtención de una lista de buckets de Amazon S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (0UTP0STS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS

Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?.

Para obtener más información acerca de los buckets de S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts.

En los siguientes ejemplos, se muestra cómo devolver una lista de los buckets de S3 en Outposts con AWS Management Console, AWS CLI y AWS SDK para Java.

## Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. En Outposts buckets (Buckets de Outposts), revise la lista de buckets de S3 en Outposts.

## Uso de la AWS CLI

En el siguiente ejemplo de AWS CLI se obtiene una lista de buckets de un Outpost. Para usar este comando, sustituya *user input placeholder* por su propia información. Para obtener más información acerca de este comando, consulte list-regional-buckets en la Referencia de AWS CLI.

```
aws s3control list-regional-buckets --account-id 123456789012 --outpost-
id op-01ac5d28a6a232904
```

## Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se obtiene una lista de buckets de un Outpost. Para obtener más información, consulte ListRegionalBuckets en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void listRegionalBuckets() {

    ListRegionalBucketsRequest reqListBuckets = new ListRegionalBucketsRequest()
            .withAccountId(AccountId)
            .withOutpostId(OutpostId);
```

```
    ListRegionalBucketsResult respListBuckets =
 s3ControlClient.listRegionalBuckets(reqListBuckets);
    System.out.printf("ListRegionalBuckets Response: %s%n",
 respListBuckets.toString());

}
```

# Obtención de un bucket de S3 en Outposts mediante la AWS CLI y el SDK para Java

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (OUTPOSTS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

En los siguientes ejemplos, se muestra cómo obtener un bucket de S3 en Outposts con AWS CLI y AWS SDK para Java.

> **Note**
>
> Al trabajar con Amazon S3 en Outposts a través de los SDK de AWS CLI o AWS, se proporciona el ARN del punto de acceso para Outpost en lugar del nombre del bucket. El ARN del punto de acceso adopta la siguiente forma, donde *region* es el código de Región de AWS de la región en la que está destinado el Outpost:
> `arn:aws:s3-outposts:`*region*`:`*123456789012*`:outpost/`*op-01ac5d28a6a232904*`/accesspoint/`*example-outposts-access-point*
> Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

### Uso de la AWS CLI

El siguiente ejemplo de S3 en Outposts obtiene un bucket con la AWS CLI. Para usar este comando, sustituya *user input placeholder* por su propia información. Para obtener más información acerca de este comando, consulte get-bucket en la Referencia de AWS CLI.

```
aws s3control get-bucket --account-id 123456789012 --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket"
```

### Uso de AWS SDK para Java

El siguiente ejemplo de S3 en Outposts obtiene un bucket con el SDK para Java. Para obtener más información, consulte GetBucket en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucket(String bucketArn) {

    GetBucketRequest reqGetBucket = new GetBucketRequest()
            .withBucket(bucketArn)
            .withAccountId(AccountId);

    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);
    System.out.printf("GetBucket Response: %s%n", respGetBucket.toString());

}
```

## Eliminación del bucket de Amazon S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (0UTP0STS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS

Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?.

Para obtener más información acerca de los buckets de S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts.

La Cuenta de AWS que crea el bucket es su propietaria y la única que puede eliminarlo.

> **Note**
>
> - Los buckets de Outposts deben estar vacíos antes de que puedan eliminarse.
>
>  La consola de Amazon S3 no admite acciones de objetos S3 en Outposts. Para eliminar objetos de bucket de S3 en Outposts, debe utilizar la API REST, AWS CLI o los SDK de AWS.
> - Antes de eliminar un bucket de Outposts, debe eliminar los puntos de acceso de Outposts del bucket. Para obtener más información, consulte Eliminar un punto de acceso.
> - No se puede recuperar un bucket después de que se haya eliminado.

En los siguientes ejemplos, se muestra cómo eliminar un bucket de S3 en Outposts con la AWS Management Console y AWS Command Line Interface (AWS CLI).

## Uso de la consola de S3

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket que desea eliminar y elija Delete (Eliminar).
4. Confirme la eliminación.

## Uso de la AWS CLI

En el siguiente ejemplo, se elimina un bucket de S3 en Outposts (`s3-outposts:DeleteBucket`) con la AWS CLI. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control delete-bucket --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket
```

# Trabajo con puntos de acceso de Amazon S3 en Outposts

Para acceder a su bucket de Amazon S3 en Outposts, debe crear y configurar un punto de acceso.

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

> **Note**
>
> La Cuenta de AWS que crea el bucket de Outposts es su propietaria y la única que puede asignarle puntos de acceso.

En las secciones siguientes, se describe cómo crear y administrar los puntos de acceso de buckets de S3 en Outposts.

Temas

- Creación de un punto de acceso de S3 en Outposts
- Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts
- Visualización de información acerca de una configuración de punto de acceso
- Visualización de una lista de puntos de acceso de Amazon S3 en Outposts
- Eliminar un punto de acceso
- Adición o edición de una política de punto de acceso
- Visualización de una política de punto de acceso para un punto de acceso de S3 en Outposts

## Creación de un punto de acceso de S3 en Outposts

Para acceder a su bucket de Amazon S3 en Outposts, debe crear y configurar un punto de acceso.

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

En los siguientes ejemplos se muestra cómo crear un punto de acceso de S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

> **Note**
>
> La Cuenta de AWS que crea el bucket de Outposts es su propietaria y la única que puede asignarle puntos de acceso.

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Seleccione el bucket de Outposts para el que desea crear un punto de acceso de Outposts.
4. Seleccione la pestaña Puntos de acceso de Outposts.
5. En la sección Outposts access points (Puntos de acceso de Outposts), elija Create Outposts access point (Crear punto de acceso de Outposts).
6. En la sección Outposts access point settings (Configuración del punto de acceso de Outposts), ingrese un nombre para el punto de acceso y elija la nube virtual privada (VPC) para el punto de acceso.
7. Si desea agregar una política para su punto de acceso, puede hacerlo ingresando en la sección Outposts access point policy (Política de punto de acceso de Outposts).

   Para obtener más información, consulte Configuración de IAM con S3 en Outposts.

Mediante AWS CLI

Example

En el siguiente ejemplo de la AWS CLI, se crea un punto de acceso para un bucket de Outposts. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control create-access-point --account-id 123456789012
 --name example-outposts-access-point --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket" --vpc-configuration VpcId=example-vpc-12345
```

Uso de AWS SDK para Java

Example

En el siguiente ejemplo del SDK para Java, se crea un punto de acceso para un bucket de Outposts. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.services.s3control.model.*;

public String createAccessPoint(String bucketArn, String accessPointName) {

    CreateAccessPointRequest reqCreateAP = new CreateAccessPointRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
            .withName(accessPointName)
            .withVpcConfiguration(new VpcConfiguration().withVpcId("vpc-12345"));

    CreateAccessPointResult respCreateAP =
 s3ControlClient.createAccessPoint(reqCreateAP);
    System.out.printf("CreateAccessPoint Response: %s%n", respCreateAP.toString());

    return respCreateAP.getAccessPointArn();

}
```

## Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts

Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Cada vez que se crea un punto de acceso para un bucket, S3 en Outposts genera de forma automática un alias de punto de acceso. Puede utilizar este alias de punto de acceso en lugar de un ARN de punto de acceso para cualquier operación del plano de datos. Por ejemplo, puede usar un alias de punto de acceso para realizar operaciones a nivel de objeto, como PUT, GET, LIST y más. Para obtener una lista de las operaciones, consulte Operaciones de la API de Amazon S3 para administrar objetos.

Los siguientes ejemplos muestran un ARN y un alias de punto de acceso para un punto de acceso llamado *my-access-point*.

- ARN del punto de acceso: `arn:aws:s3-outposts:`*region*`:`*123456789012*`:outpost/`*op-01ac5d28a6a232904*`/accesspoint/`*my-access-point*
- Alias de punto de acceso: *my-access-po*`-`*o01ac5d28a6a232904e8xz5w8ijx1qzlbp3i3kuse10*`--op-s3`

Para obtener más información acerca de los ARN, consulte Nombres de recurso de Amazon (ARN) en la Referencia general de AWS.

Para obtener más información acerca de los alias de punto de acceso, consulte los siguientes temas.

Temas

- Alias de punto de acceso
- Uso de un alias de punto de acceso en una operación de objeto de S3 en Outposts
- Limitaciones

## Alias de punto de acceso

Se crea un alias de punto de acceso en el mismo espacio de nombres que un bucket de Outposts. Al crear un punto de acceso, S3 en Outposts genera de forma automática un alias de punto de acceso que no se puede modificar. Un alias de punto de acceso cumple con todos los requisitos de un nombre de bucket válido de S3 en Outposts y consta de las siguientes partes:

*access point name prefix*`-`*metadata*`--op-s3`

> **Note**
>
> El sufijo `--op-s3` está reservado para los alias de punto de acceso, por lo que se recomienda no utilizarlo para los nombres de punto de acceso o bucket. Para obtener más información acerca de las reglas de nomenclatura del bucket de S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts.

### Búsqueda del alias de punto de acceso

En los siguientes ejemplos se muestra cómo encontrar un alias de punto de acceso utilizando la consola de Amazon S3 y la AWS CLI.

Example : Buscar y copiar un alias de punto de acceso en la consola de Amazon S3

Después de crear un punto de acceso en la consola, puede obtener el alias del punto de acceso en la columna Access Point alias (Alias de puntos de acceso) de la lista Access Points (Puntos de acceso).

Para copiar un alias de punto de acceso

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. Para copiar el alias de punto de acceso, realice una de las siguientes acciones:
   - En la lista Access Points (Puntos de acceso), seleccione el botón de opción situado junto al nombre del punto de acceso y, a continuación, elija Copy Access Point alias (Copiar alias de punto de acceso).
   - Seleccione el nombre del punto de acceso. A continuación, en Outposts access point overview (Descripción general del punto de acceso de Outposts), copie el alias del punto de acceso.

Example : Crear un punto de acceso utilizando la AWS CLI y buscar el alias del punto de acceso en la respuesta

El siguiente ejemplo de la AWS CLI del comando `create-access-point` crea el punto de acceso y devuelve el alias de punto de acceso generado automáticamente. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control create-access-point --bucket example-outposts-bucket --name example-
outposts-access-point --account-id 123456789012

{
    "AccessPointArn":
    "arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
accesspoint/example-outposts-access-point",
    "Alias": "example-outp-o01ac5d28a6a232904e8xz5w8ijx1qzlbp3i3kuse10--op-s3"
```

```
}
```

Example : Obtener un alias de punto de acceso utilizando la AWS CLI

El siguiente ejemplo de AWS CLI del comando `get-access-point` devuelve información sobre el punto de acceso especificado. Esta información incluye el alias de punto de acceso. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control get-access-point --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --name example-outposts-access-point --account-id 123456789012

{
    "Name": "example-outposts-access-point",
    "Bucket": "example-outposts-bucket",
    "NetworkOrigin": "Vpc",
    "VpcConfiguration": {
        "VpcId": "vpc-01234567890abcdef"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2022-09-18T17:49:15.584000+00:00",
    "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3"
}
```

Example : Enumerar los puntos de acceso para encontrar un alias de punto de acceso mediante la AWS CLI

El siguiente ejemplo de AWS CLI del comando `list-access-points` enumera información sobre el punto de acceso especificado. Esta información incluye el alias de punto de acceso. Para ejecutar este comando, sustituya los *`user input placeholders`* con su propia información.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket

{
    "AccessPointList": [
```

```
        {
            "Name": "example-outposts-access-point",
            "NetworkOrigin": "Vpc",
            "VpcConfiguration": {
                "VpcId": "vpc-01234567890abcdef"
            },
            "Bucket": "example-outposts-bucket",
            "AccessPointArn": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point",
            "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3"
        }
    ]
}
```

## Uso de un alias de punto de acceso en una operación de objeto de S3 en Outposts

Al adoptar puntos de acceso, puede utilizar alias de puntos de acceso sin tener que hacer cambios exhaustivos en el código.

En este ejemplo de AWS CLI se muestra una operación `get-object` para un bucket de S3 en Outposts. En este ejemplo, se utiliza el alias del punto de acceso como el valor de `--bucket`, en lugar del ARN completo del punto de acceso.

```
aws s3api get-object --bucket my-access-po-
o0b1d075431d83bebde8xz5w8ijx1qzlbp3i3kuse10--op-s3 --key  testkey  sample-object.rtf

{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

## Limitaciones

- Los clientes no pueden configurar los alias.
- Los alias no se pueden eliminar, modificar ni dehabillitar en un punto de acceso.

- No puede utilizar un alias de punto de acceso para operaciones de plano de control de S3 en Outposts. Para ver la lista de operaciones del plano de control de S3 en Outposts, consulte Operaciones de la API de Amazon S3 Control para administrar buckets.
- Los alias no se pueden usar en las políticas de AWS Identity and Access Management (IAM).

## Visualización de información acerca de una configuración de punto de acceso

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

Los siguientes temas muestran cómo devolver información de configuración de un punto de acceso de S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

### Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. Elija el punto de acceso de Outposts para el que desea ver los detalles de configuración.
4. En Outposts access point overview (Resumen del punto de acceso de Outposts), revise los detalles de configuración del punto de acceso.

### Uso de la AWS CLI

En el siguiente ejemplo de la AWS CLI, se obtiene un punto de acceso para un bucket de Outposts. Sustituya los *`user input placeholders`* con su propia información.

```
aws s3control get-access-point --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se obtiene un punto de acceso para un bucket de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getAccessPoint(String accessPointArn) {

    GetAccessPointRequest reqGetAP = new GetAccessPointRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn);

    GetAccessPointResult respGetAP = s3ControlClient.getAccessPoint(reqGetAP);
    System.out.printf("GetAccessPoint Response: %s%n", respGetAP.toString());

}
```

## Visualización de una lista de puntos de acceso de Amazon S3 en Outposts

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

En los siguientes temas, se muestra cómo devolver una lista de los puntos de acceso de S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. En Outposts access points (Puntos de acceso de Outposts), revise la lista de puntos de acceso de S3 en Outposts.

Uso de la AWS CLI

En el siguiente ejemplo de la AWS CLI, se enumeran los puntos de acceso para un bucket de Outposts. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket
```

Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se enumeran los puntos de acceso para un bucket de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void listAccessPoints(String bucketArn) {

    ListAccessPointsRequest reqListAPs = new ListAccessPointsRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    ListAccessPointsResult respListAPs = s3ControlClient.listAccessPoints(reqListAPs);
    System.out.printf("ListAccessPoints Response: %s%n", respListAPs.toString());

}
```

## Eliminar un punto de acceso

Los puntos de acceso simplifican la administración del acceso a los datos a escala para los conjuntos de datos compartidos en Amazon S3. Los puntos de acceso son puntos de enlace de red con nombre y asociados a los buckets que se pueden utilizar para realizar operaciones con objetos de Amazon S3, como `GetObject` y `PutObject`. Con S3 en Outposts, debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outposts. Los puntos de acceso solo admiten el direccionamiento de tipo de host virtual.

En los siguientes ejemplos, se muestra cómo eliminar un punto de acceso mediante AWS Management Console y la AWS Command Line Interface (AWS CLI).

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. En la sección Outposts access points (Puntos de acceso de Outposts), elija el punto de acceso de Outposts que desea eliminar.
4. Elija Eliminar.
5. Confirme la eliminación.

Uso de la AWS CLI

En el siguiente ejemplo de la AWS CLI, se elimina un punto de acceso de Outposts. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3control delete-access-point --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

## Adición o edición de una política de punto de acceso

Cada punto de acceso tiene permisos y controles de red distintos que Amazon S3 en Outposts se aplica a cualquier solicitud que se realice a través de ese punto de acceso. Cada punto de acceso aplica una política de punto de acceso personalizada que funciona en conjunción con la política de bucket asociada al bucket subyacente. Para obtener más información, consulte Puntos de acceso.

En los siguientes temas, se muestra cómo agregar o editar la política de punto de acceso de su punto de acceso de S3 en Outposts mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts buckets (buckets de Outposts).
3. Elija el bucket de Outposts para el que desea editar la política de punto de acceso.
4. Seleccione la pestaña Puntos de acceso de Outposts.

5. En la sección Outposts access points (Puntos de acceso de Outposts), seleccione el punto de acceso cuya política desea editar y elija Edit policy (Editar política).
6. Agregue o edite la política en la sección Outposts access point policy (política de puntos de acceso de Outposts) . Para obtener más información, consulte Configuración de IAM con S3 en Outposts.

Mediante AWS CLI

En el siguiente ejemplo de la AWS CLI, se aplica una política en un punto de acceso de Outposts.

1. Guarde la siguiente política de punto de acceso en un archivo JSON. En este ejemplo, el archivo se denomina `appolicy1.json`. Reemplace los *`user input placeholders`* con su propia información.

```
{
   "Version":"2012-10-17",
   "Id":"exampleAccessPointPolicy",
   "Statement":[
      {
         "Sid":"st1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"123456789012"
         },
         "Action":"s3-outposts:*",
         "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point
      }
   ]
}
```

2. Envíe el archivo JSON como parte del comando de la CLI `put-access-point-policy`. Sustituya los *`user input placeholders`* con su propia información.

```
aws s3control put-access-point-policy --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --policy file://appolicy1.json
```

Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se aplica una política en un punto de acceso de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putAccessPointPolicy(String accessPointArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testAccessPointPolicy\",
\"Statement\":[{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
 AccountId + "\"},\"Action\":\"s3-outposts:*\",\"Resource\":\"" + accessPointArn +
 "\"}]}";

    PutAccessPointPolicyRequest reqPutAccessPointPolicy = new
 PutAccessPointPolicyRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn)
            .withPolicy(policy);

    PutAccessPointPolicyResult respPutAccessPointPolicy =
 s3ControlClient.putAccessPointPolicy(reqPutAccessPointPolicy);
    System.out.printf("PutAccessPointPolicy Response: %s%n",
 respPutAccessPointPolicy.toString());
    printWriter.printf("PutAccessPointPolicy Response: %s%n",
 respPutAccessPointPolicy.toString());

}
```

## Visualización de una política de punto de acceso para un punto de acceso de S3 en Outposts

Cada punto de acceso tiene permisos y controles de red distintos que Amazon S3 en Outposts aplica a cualquier solicitud que se realice a través de ese punto de acceso. Cada punto de acceso aplica una política de punto de acceso personalizada que funciona en conjunción con la política de bucket asociada al bucket subyacente. Para obtener más información, consulte Puntos de acceso.

Para obtener más información acerca del uso de puntos de acceso en S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts.

En los siguientes temas, se muestra cómo ver la política de punto de acceso de S3 en Outposts utilizando la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

### Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. Elija el punto de acceso de Outposts para el que desea ver la política.
4. En la página Permissions (Permisos), revise la política del punto de acceso de S3 en Outposts.
5. Para editar la política de punto de acceso, consulte Adición o edición de una política de punto de acceso.

### Uso de la AWS CLI

En el siguiente ejemplo de la AWS CLI, se obtiene una política para un punto de acceso de Outposts. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3control get-access-point-policy --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

### Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se obtiene una política para un punto de acceso de Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getAccessPointPolicy(String accessPointArn) {

    GetAccessPointPolicyRequest reqGetAccessPointPolicy = new
 GetAccessPointPolicyRequest()
            .withAccountId(AccountId)
            .withName(accessPointArn);

    GetAccessPointPolicyResult respGetAccessPointPolicy =
 s3ControlClient.getAccessPointPolicy(reqGetAccessPointPolicy);
```

```
    System.out.printf("GetAccessPointPolicy Response: %s%n",
 respGetAccessPointPolicy.toString());
    printWriter.printf("GetAccessPointPolicy Response: %s%n",
 respGetAccessPointPolicy.toString());

}
```

# Trabajo con puntos de conexión de Amazon S3 en Outposts

Para dirigir solicitudes a un punto de acceso de Amazon S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Para crear un punto de conexión, necesita una conexión activa con el enlace de servicio a la región de origen de Outposts. Cada nube virtual privada (VPC) de su Outpost puede tener un punto de conexión asociado. Para obtener más información acerca de las cuotas de los puntos de conexión, consulte Requisitos de red de S3 en Outposts. Debe crear un punto de conexión para poder acceder a los buckets de Outposts y realizar operaciones de objetos. Para obtener más información, consulte Puntos de conexión.

Después de crear un punto de conexión, puede utilizar el campo Estado para comprender el estado del punto de conexión. Si Outposts está desconectado, devolverá un error CREATE_FAILED. Puede comprobar la conexión del enlace de servicio, eliminar el punto de conexión y volver a intentar la operación de creación cuando se haya reanudado la conexión. Para obtener una lista de códigos de error adicionales, consulte la siguiente tabla. Para obtener más información, consulte Puntos de conexión.

| API | Status | Código de error de motivo de error | Mensaje - Motivo del error |
|---|---|---|---|
| `CreateEndpoint` | Create_Failed | OutpostNotReachable | No se ha podido crear un punto de conexión porque la conexión del enlace de servicio a la región de origen de Outposts está inactiva. Compruebe la conexión, borre el punto de conexión e inténtelo de nuevo. |
| `CreateEndpoint` | Create_Failed | InternalError | No se ha podido crear el punto de conexión debido a un error interno. Elimine el punto de conexión y vuelva a crearlo. |

| API | Status | Código de error de motivo de error | Mensaje - Motivo del error |
|---|---|---|---|
| `DeleteEndpoint` | Delete_Failed | OutpostNotReachable | No se ha podido eliminar un punto de conexión porque la conexión del enlace de servicio a la región de origen de Outposts está inactiva. Compruebe la conexión e inténtelo de nuevo. |
| `DeleteEndpoint` | Delete_Failed | InternalError | No se ha podido eliminar el punto de conexión debido a un error interno. Inténtelo de nuevo. |

Para obtener más información acerca de trabajar con buckets en S3 en Outposts, consulte Trabajo con buckets de S3 en Outposts.

En las secciones siguientes, se describe cómo crear y administrar puntos de conexión para S3 en Outposts.

Temas

- Creación de un punto de conexión en un Outpost
- Obtención de una lista de puntos de conexión de Amazon S3 en Outposts
- Eliminación de un punto de conexión de Amazon S3 en Outposts

## Creación de un punto de conexión en un Outpost

Para dirigir solicitudes a un punto de acceso de Amazon S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Para crear un punto de conexión, necesita una conexión activa con el enlace de servicio a la región de origen de Outposts. Cada nube virtual privada (VPC) de su Outpost puede tener un punto de conexión asociado. Para obtener más información acerca de las cuotas de los puntos de conexión, consulte Requisitos de red de S3 en Outposts. Debe crear un punto de conexión para poder acceder a los buckets de Outposts y realizar operaciones de objetos. Para obtener más información, consulte Puntos de conexión.

Permisos

Para obtener más información sobre los permisos necesarios para crear un punto de conexión, consulte Permisos para los puntos de conexión de S3 en Outposts.

Al crear un punto de conexión, S3 en Outposts también crea un rol vinculado a un servicio en la Cuenta de AWS. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon S3 en Outposts.

En los siguientes ejemplos, se muestra cómo crear un punto de conexión de S3 en Outposts con AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

Uso de la consola de S3

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. Seleccione la pestaña Outposts endpoints (Puntos de acceso de Outposts).
4. Elija Create Outposts endpoint (Crear punto de conexión de Outposts).
5. En Outpost, elija el Outpost en el que crear este punto de conexión.
6. En VPC, elija una VPC que aún no tenga punto de conexión y que también cumpla las reglas de los puntos de conexión de Outposts.

   Una nube virtual privada (VPC) le permite lanzar recursos de AWS en una red virtual que defina. Dicha red virtual es prácticamente idéntica a las redes tradicionales que se utilizarían en sus propios centros de datos, con los beneficios que supone utilizar la infraestructura escalable de AWS.

   Si no tiene una VPC, elija Create VPC (Crear VPC). Para obtener más información, consulte Crear puntos de acceso restringidos a una nube privada virtual (VPC) en la Guía del usuario de Amazon S3.
7. Elija Create Outposts endpoint (Crear punto de conexión de Outposts).

Uso de la AWS CLI

Example

En el siguiente ejemplo de la AWS CLI, se crea un punto de conexión para un Outpost con el tipo de acceso a recursos de la VPC. La VPC se obtiene de la subred. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

En el siguiente ejemplo de la AWS CLI, se crea un punto de conexión para un Outpost con el tipo de acceso de grupo de direcciones IP propiedad del cliente (grupo de CoIP). Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
 subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --
customer-owned-ipv4-pool ipv4pool-coip-12345678901234567
```

Uso de AWS SDK para Java

Example

En el siguiente ejemplo del SDK para Java, se crea un punto de conexión para un Outpost. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.CreateEndpointRequest;
import com.amazonaws.services.s3outposts.model.CreateEndpointResult;

public void createEndpoint() {
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    CreateEndpointRequest createEndpointRequest = new CreateEndpointRequest()
                .withOutpostId("op-0d79779cef3c30a40")
                .withSubnetId("subnet-8c7a57c5")
                .withSecurityGroupId("sg-ab19e0d1")
                .withAccessType("CustomerOwnedIp")
                .withCustomerOwnedIpv4Pool("ipv4pool-coip-12345678901234567");
    // Use .withAccessType and .withCustomerOwnedIpv4Pool only when the access type is
```

```
    // customer-owned IP address pool (CoIP pool)
    CreateEndpointResult createEndpointResult =
 s3OutpostsClient.createEndpoint(createEndpointRequest);
    System.out.println("Endpoint is created and its ARN is " +
 createEndpointResult.getEndpointArn());
}
```

## Obtención de una lista de puntos de conexión de Amazon S3 en Outposts

Para dirigir solicitudes a un punto de acceso de Amazon S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Para crear un punto de conexión, necesita una conexión activa con el enlace de servicio a la región de origen de Outposts. Cada nube virtual privada (VPC) de su Outpost puede tener un punto de conexión asociado. Para obtener más información acerca de las cuotas de los puntos de conexión, consulte Requisitos de red de S3 en Outposts. Debe crear un punto de conexión para poder acceder a los buckets de Outposts y realizar operaciones de objetos. Para obtener más información, consulte Puntos de conexión.

En los siguientes ejemplos, se muestra cómo devolver una lista de los puntos de conexión de S3 en Outposts con AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).
3. En la página Outposts access points (Puntos de acceso de Outposts), seleccione la pestaña Outposts endpoints (Puntos de conexión de Outposts).
4. En Outposts endpoints (Puntos de conexión de Outposts), puede ver una lista de sus puntos de conexión de S3 en Outposts.

Uso de la AWS CLI

En el siguiente ejemplo de AWS CLI, se muestran los puntos de conexión para recursos de AWS Outposts asociados a la cuenta. Para obtener más información acerca de este comando, consulte list-endpoints en la Referencia de AWS CLI.

```
aws s3outposts list-endpoints
```

Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se enumeran los puntos de enlace para un Outpost. Para obtener más información, consulte ListEndpoints en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.ListEndpointsRequest;
import com.amazonaws.services.s3outposts.model.ListEndpointsResult;

public void listEndpoints() {
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    ListEndpointsRequest listEndpointsRequest = new ListEndpointsRequest();
    ListEndpointsResult listEndpointsResult =
 s3OutpostsClient.listEndpoints(listEndpointsRequest);
    System.out.println("List endpoints result is " + listEndpointsResult);
}
```

## Eliminación de un punto de conexión de Amazon S3 en Outposts

Para dirigir solicitudes a un punto de acceso de Amazon S3 en Outposts, debe crear y configurar un punto de conexión de S3 en Outposts. Para crear un punto de conexión, necesita una conexión activa con el enlace de servicio a la región de origen de Outposts. Cada nube virtual privada (VPC) de su Outpost puede tener un punto de conexión asociado. Para obtener más información acerca de las cuotas de los puntos de conexión, consulte Requisitos de red de S3 en Outposts. Debe crear un punto de conexión para poder acceder a los buckets de Outposts y realizar operaciones de objetos. Para obtener más información, consulte Puntos de conexión.

En los siguientes ejemplos, se muestra cómo eliminar los puntos de conexión de S3 en Outposts con la AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

Uso de la consola de S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts access points (Puntos de acceso de Outposts).

3. En la página Outposts access points (Puntos de acceso de Outposts), seleccione la pestaña Outposts endpoints (Puntos de conexión de Outposts).
4. En Outposts endpoints (Puntos de conexión de Outposts), seleccione el punto de conexión que desea eliminar y elija Delete (Eliminar).

### Uso de la AWS CLI

En el siguiente ejemplo de la AWS CLI, se elimina un punto de enlace para un Outpost. Para ejecutar este comando, sustituya los *user input placeholders* con su propia información.

```
aws s3outposts delete-endpoint --endpoint-id example-endpoint-id --outpost-
id op-01ac5d28a6a232904
```

### Uso de AWS SDK para Java

En el siguiente ejemplo del SDK para Java, se elimina un punto de enlace para un Outpost. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.arn.Arn;
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.DeleteEndpointRequest;

public void deleteEndpoint(String endpointArnInput) {
    String outpostId = "op-01ac5d28a6a232904";
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
                .standard().build();

    Arn endpointArn = Arn.fromString(endpointArnInput);
    String[] resourceParts = endpointArn.getResource().getResource().split("/");
    String endpointId = resourceParts[resourceParts.length - 1];
    DeleteEndpointRequest deleteEndpointRequest = new DeleteEndpointRequest()
                .withEndpointId(endpointId)
                .withOutpostId(outpostId);
    s3OutpostsClient.deleteEndpoint(deleteEndpointRequest);
    System.out.println("Endpoint with id " + endpointId + " is deleted.");
}
```

# Trabajo con objetos de S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (0UTP0STS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST.

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

Los ARN de objeto utilizan el siguiente formato, que incluye la Región de AWS a la que está destinada Outposts, el ID de Cuenta de AWS, el ID de Outpost, el nombre del bucket y la clave de objeto:

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/ op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para

cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

Temas



## Carga de un objeto en un bucket de S3 en Outpost

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

Los siguientes ejemplos de AWS CLI y AWS SDK para Java muestran cómo cargar un objeto en un bucket de S3 en Outposts mediante un punto de acceso.

AWS CLI

Example

En el siguiente ejemplo, se aplica un objeto denominado `sample-object.xml` en un bucket de S3 en Outposts (`s3-outposts:PutObject`) mediante la AWS CLI. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información acerca de este comando, consulte put-object en la Referencia de AWS CLI.

```
aws s3api put-object --bucket arn:aws:s3-
outposts:Region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --key sample-object.xml --body sample-object.xml
```

SDK for Java

Example

En el siguiente ejemplo, se aplica un objeto en un bucket de S3 en Outposts mediante el SDK para Java. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ObjectMetadata;
import com.amazonaws.services.s3.model.PutObjectRequest;
```

```
import java.io.File;

public class PutObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Upload a text string as a new object.
            s3Client.putObject(accessPointArn, stringObjKeyName, "Uploaded String
 Object");

            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(accessPointArn,
 fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# Copia de un objeto en un bucket de Amazon S3 en Outposts utilizando AWS SDK para Java

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

En los siguientes ejemplos, se muestra cómo obtener una lista de objetos de bucket de S3 en Outposts con AWS SDK para Java.

## Uso de AWS SDK para Java

En el siguiente ejemplo de S3 en Outposts, se copia un objeto a un objeto nuevo en el mismo bucket con el SDK para Java. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
```

```
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

public class CopyObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String sourceKey = "*** Source object key ***";
        String destinationKey = "*** Destination object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(accessPointArn,
 sourceKey, accessPointArn, destinationKey);
            s3Client.copyObject(copyObjectRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# Obtención de un objeto de un bucket de Amazon S3 en Outposts

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

Los siguientes ejemplos muestran cómo descargar (obtener) un objeto mediante AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

## Uso de la AWS CLI

En el siguiente ejemplo, se obtiene un objeto denominado `sample-object.xml` de un bucket de S3 en Outposts (`s3-outposts:GetObject`) mediante la AWS CLI. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información acerca de este comando, consulte get-object en la Referencia de AWS CLI.

```
aws s3api get-object --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point --key testkey sample-object.xml
```

## Uso de AWS SDK para Java

En el siguiente ejemplo de S3 en Outposts, se obtiene un objeto mediante el SDK para Java. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información. Para obtener más información, consulte GetObject en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
```

```
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String accessPointArn = "*** access point ARN ***";
        String key = "*** Object key ***";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Get an object and print its contents.
            System.out.println("Downloading an object");
            fullObject = s3Client.getObject(new GetObjectRequest(accessPointArn, key));
            System.out.println("Content-Type: " +
 fullObject.getObjectMetadata().getContentType());
            System.out.println("Content: ");
            displayTextInputStream(fullObject.getObjectContent());

            // Get a range of bytes from an object and print the bytes.
            GetObjectRequest rangeObjectRequest = new GetObjectRequest(accessPointArn,
 key)
                    .withRange(0, 9);
            objectPortion = s3Client.getObject(rangeObjectRequest);
            System.out.println("Printing bytes retrieved.");
            displayTextInputStream(objectPortion.getObjectContent());

            // Get an entire object, overriding the specified response headers, and
 print the object's content.
            ResponseHeaderOverrides headerOverrides = new ResponseHeaderOverrides()
                    .withCacheControl("No-cache")
```

```
                    .withContentDisposition("attachment; filename=example.txt");
            GetObjectRequest getObjectRequestHeaderOverride = new
 GetObjectRequest(accessPointArn, key)
                    .withResponseHeaders(headerOverrides);
            headerOverrideObject = s3Client.getObject(getObjectRequestHeaderOverride);
            displayTextInputStream(headerOverrideObject.getObjectContent());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        } finally {
            // To ensure that the network connection doesn't remain open, close any
 open input streams.
            if (fullObject != null) {
                fullObject.close();
            }
            if (objectPortion != null) {
                objectPortion.close();
            }
            if (headerOverrideObject != null) {
                headerOverrideObject.close();
            }
        }
    }

    private static void displayTextInputStream(InputStream input) throws IOException {
        // Read the text input stream one line at a time and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line = null;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

# Obtención de listas de objetos en un bucket de Amazon S3 en Outposts

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

> **Note**
>
> Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

En los siguientes ejemplos, se muestra cómo obtener una lista de objetos de un bucket de S3 en Outposts mediante AWS CLI y AWS SDK para Java.

## Uso de la AWS CLI

En el siguiente ejemplo, se muestran los objetos en un bucket de S3 en Outposts (`s3-outposts:ListObjectsV2`) mediante AWS CLI. Para usar este comando, sustituya *`user input`*

*placeholder* por su propia información. Para obtener más información acerca de este comando, consulte list-objects-v2 en la Referencia de AWS CLI.

```
aws s3api list-objects-v2 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

> **Note**
>
> Al utilizar esta acción con Amazon S3 en Outposts a través de SDK de AWS, proporciona el ARN del punto de acceso de Outposts en lugar del nombre del bucket, en la siguiente manera: `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-Outposts-Access-Point`. Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

## Uso de AWS SDK para Java

En el siguiente ejemplo de S3 en Outposts, se muestran objetos en un bucket mediante el SDK para Java. Para utilizar este ejemplo, sustituya *user input placeholder* por su propia información.

> **Important**
>
> En este ejemplo se utiliza ListObjectsV2, que es la revisión más reciente de la operación de la API `ListObjects`. Recomendamos usar esta operación de API revisada para el desarrollo de aplicaciones. Para garantizar la compatibilidad con versiones anteriores, Amazon S3 aún es compatible con la versión anterior de esta operación de API.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {
```

```
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            System.out.println("Listing objects");

            // maxKeys is set to 2 to demonstrate the use of
            // ListObjectsV2Result.getNextContinuationToken()
            ListObjectsV2Request req = new
 ListObjectsV2Request().withBucketName(accessPointArn).withMaxKeys(2);
            ListObjectsV2Result result;

            do {
                result = s3Client.listObjectsV2(req);

                for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
                    System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
 objectSummary.getSize());
                }
                // If there are more than maxKeys keys in the bucket, get a
 continuation token
                // and list the next objects.
                String token = result.getNextContinuationToken();
                System.out.println("Next Continuation Token: " + token);
                req.setContinuationToken(token);
            } while (result.isTruncated());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

# Eliminación de objetos en buckets de Amazon S3 en Outposts

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

En los siguientes ejemplos, se muestra cómo eliminar un solo objeto o varios objetos en un bucket de S3 en Outposts con AWS Command Line Interface (AWS CLI) y AWS SDK para Java.

## Uso de la AWS CLI

En los ejemplos siguientes, se muestra cómo eliminar un solo objeto o varios objetos de un bucket de S3 en Outposts.

delete-object

En el siguiente ejemplo, se elimina un objeto denominado `sample-object.xml` de un bucket de S3 en Outposts (`s3-outposts:DeleteObject`) mediante la AWS CLI. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información sobre este comando, consulte delete-object en la Referencia de AWS CLI.

```
aws s3api delete-object --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --key sample-object.xml
```

delete-objects

En el siguiente ejemplo, se eliminan dos objetos denominados `sample-object.xml` y `test1.text` de un bucket de S3 en Outposts (`s3-outposts:DeleteObject`) mediante la AWS CLI. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información sobre este comando, consulte delete-objects en la Referencia de AWS CLI.

```
aws s3api delete-objects --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --delete file://delete.json

delete.json
{
  "Objects": [
    {
      "Key": "test1.txt"
    },
    {
      "Key": "sample-object.xml"
    }
  ],
  "Quiet": false
}
```

## Uso de AWS SDK para Java

En los ejemplos siguientes, se muestra cómo eliminar un solo objeto o varios objetos de un bucket de S3 en Outposts.

### DeleteObject

En el siguiente ejemplo de S3 en Outposts, se elimina un objeto de un bucket mediante el SDK para Java. Para utilizar este ejemplo, especifique el ARN del punto de acceso para Outpost y el nombre de la clave del objeto que desea eliminar. Para obtener más información, consulte DeleteObject en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** key name ****";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(accessPointArn, keyName));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### DeleteObjects

En el siguiente ejemplo de S3 en Outposts, se cargan y luego, eliminan objetos de un bucket mediante el SDK para Java. Para utilizar este ejemplo, especifique el ARN del punto de acceso

para Outpost. Para obtener más información, consulte DeleteObjects en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectsRequest;
import com.amazonaws.services.s3.model.DeleteObjectsRequest.KeyVersion;
import com.amazonaws.services.s3.model.DeleteObjectsResult;

import java.util.ArrayList;

public class DeleteObjects {

    public static void main(String[] args) {
       String accessPointArn = "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point";


        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Upload three sample objects.
            ArrayList<KeyVersion> keys = new ArrayList<KeyVersion>();
            for (int i = 0; i < 3; i++) {
                String keyName = "delete object example " + i;
                s3Client.putObject(accessPointArn, keyName, "Object number " + i + "
 to be deleted.");
                keys.add(new KeyVersion(keyName));
            }
            System.out.println(keys.size() + " objects successfully created.");

            // Delete the sample objects.
            DeleteObjectsRequest multiObjectDeleteRequest = new
 DeleteObjectsRequest(accessPointArn)
                    .withKeys(keys)
```

```
                    .withQuiet(false);

            // Verify that the objects were deleted successfully.
            DeleteObjectsResult delObjRes =
 s3Client.deleteObjects(multiObjectDeleteRequest);
            int successfulDeletes = delObjRes.getDeletedObjects().size();
            System.out.println(successfulDeletes + " objects successfully
 deleted.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## Uso de HeadBucket para determinar si existe un bucket de S3 en Outposts y si tiene permisos de acceso

Los objetos son las entidades fundamentales almacenadas en Amazon S3 en Outposts. Cada objeto está almacenado en un bucket. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Cuando especifica el bucket para las operaciones de objetos, se utiliza el Nombre de recurso de Amazon (ARN) del punto de acceso o el alias del punto de acceso. Para obtener más información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

En el siguiente ejemplo se muestra el formato ARN para los puntos de acceso de S3 en Outposts, que incluye el código Región de AWS de la Región a la que pertenece el Outpost, el ID de Cuenta de AWS, el ID de Outposts y el nombre del punto de acceso:

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Para obtener más información acerca de S3 en Outposts, consulte ARN de recursos para S3 en Outposts.

> **Note**
>
> Con Amazon S3 en Outposts, los datos de objeto siempre se almacenan en el Outpost. Cuando AWS instala un bastidor de Outpost, sus datos permanecen de manera local en su Outpost para cumplir los requisitos de residencia de datos. Sus objetos nunca salen de su Outpost y no están en una Región de AWS. Ya que la AWS Management Console está alojada dentro de la región, no puede usar la consola para cargar o administrar objetos en su Outpost. Sin embargo, puede utilizar la API de REST, AWS Command Line Interface (AWS CLI) y los SDK de AWS para cargar y administrar los objetos a través de los puntos de acceso.

En los siguientes ejemplos de AWS Command Line Interface (AWS CLI) y AWS SDK para Java, se muestra cómo usar la operación de la API HeadBucket para determinar si existe un bucket de S3 en Outposts y si tiene permiso para acceder a él. Para obtener más información, consulte HeadBucket en la Referencia de la API de Amazon Simple Storage Service.

## Uso de la AWS CLI

En el siguiente ejemplo de S3 en Outposts de AWS CLI, se utiliza el comando `head-bucket` para determinar si existe un bucket y si tiene permiso para acceder a él. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información acerca de este comando, consulte head-bucket en la Referencia de AWS CLI.

```
aws s3api head-bucket --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point
```

## Uso de AWS SDK para Java

En el siguiente ejemplo de S3 en Outposts, se muestra cómo determinar si existe un bucket y si usted tiene permiso para acceder a él. Para utilizar este ejemplo, especifique el ARN del punto de acceso para Outpost. Para obtener más información, consulte HeadBucket en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
```

```
import com.amazonaws.services.s3.model.HeadBucketRequest;

public class HeadBucket {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            s3Client.headBucket(new HeadBucketRequest(accessPointArn));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# Ejecución y administración de una carga multiparte con el SDK para Java

Con Amazon S3 en Outposts, puede crear buckets de S3 en recursos de AWS Outposts y almacenar y recuperar objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

En los siguientes ejemplos, se muestra cómo puede utilizar S3 en Outposts con AWS SDK para Java para realizar y administrar una carga multiparte.

Temas

- Realización de una carga multiparte de un objeto en un bucket de S3 en Outposts

- Copia de un objeto grande en un bucket de S3 en Outposts con la carga multiparte
- Obtención de una lista de las partes de un objeto en un bucket de S3 en Outposts
- Recuperación de una lista de cargas multiparte en curso en un bucket de S3 en Outposts

## Realización de una carga multiparte de un objeto en un bucket de S3 en Outposts

En el siguiente ejemplo de S3 en Outposts, se inicia, carga y finaliza una carga multiparte de un objeto en un bucket mediante el SDK para Java. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información. Para obtener más información, consulte Carga de un objeto con la carga multiparte en la Guía del usuario de Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);
```

```
            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(accessPointArn, sourceObjectKey);
            ObjectMetadata metadataResult =
s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(accessPointArn)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(accessPointArn)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and make
the copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    accessPointArn,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
```

```
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
```

## Copia de un objeto grande en un bucket de S3 en Outposts con la carga multiparte

En el siguiente ejemplo de S3 en Outposts se utiliza el SDK para Java para copiar un objeto en un bucket. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        try {
            // This code expects that you have AWS credentials set up per:
```

```
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest(accessPointArn, sourceObjectKey);
            ObjectMetadata metadataResult =
 s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(accessPointArn)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(accessPointArn)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }
```

```
            // Complete the upload request to concatenate all uploaded parts and make
 the copied object available.
            CompleteMultipartUploadRequest completeRequest = new
 CompleteMultipartUploadRequest(
                    accessPointArn,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

## Obtención de una lista de las partes de un objeto en un bucket de S3 en Outposts

En el siguiente ejemplo de S3 en Outposts se muestran las partes de un objeto en un bucket con el SDK para Java. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
```

```
import com.amazonaws.services.s3.model.*;

import java.util.List;

public class ListParts {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** Key name ***";
        String uploadId = "*** Upload ID ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            ListPartsRequest listPartsRequest = new ListPartsRequest(accessPointArn,
 keyName, uploadId);
            PartListing partListing = s3Client.listParts(listPartsRequest);
            List<PartSummary> partSummaries = partListing.getParts();

            System.out.println(partSummaries.size() + " multipart upload parts");
            for (PartSummary p : partSummaries) {
                System.out.println("Upload part: Part number = \"" + p.getPartNumber()
 + "\", ETag = " + p.getETag());
            }

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# Recuperación de una lista de cargas multiparte en curso en un bucket de S3 en Outposts

En el siguiente ejemplo de Amazon S3 en Outposts, se muestra cómo recuperar una lista de cargas multiparte en curso desde un bucket de Outposts mediante el SDK para Java. Para utilizar este ejemplo, sustituya *user input placeholder* por su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListMultipartUploadsRequest;
import com.amazonaws.services.s3.model.MultipartUpload;
import com.amazonaws.services.s3.model.MultipartUploadListing;

import java.util.List;

public class ListMultipartUploads {
    public static void main(String[] args) {
                String accessPointArn = "*** access point ARN ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .enableUseArnRegion()
                    .build();

            // Retrieve a list of all in-progress multipart uploads.
            ListMultipartUploadsRequest allMultipartUploadsRequest = new
 ListMultipartUploadsRequest(accessPointArn);
            MultipartUploadListing multipartUploadListing =
 s3Client.listMultipartUploads(allMultipartUploadsRequest);
            List<MultipartUpload> uploads =
 multipartUploadListing.getMultipartUploads();

            // Display information about all in-progress multipart uploads.
            System.out.println(uploads.size() + " multipart upload(s) in progress.");
            for (MultipartUpload u : uploads) {
                System.out.println("Upload in progress: Key = \"" + u.getKey() + "\",
 id = " + u.getUploadId());
```

```
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# Uso de URL prefirmadas para S3 en Outposts

Para conceder acceso por tiempo limitado a los objetos que se almacenan localmente en un Outpost sin actualizar su política de bucket, puede usar una URL prefirmada. Con las URL prefirmadas, usted, como propietario del bucket, puede compartir objetos con personas en su nube privada virtual (VPC) o concederles la capacidad de cargar o eliminar objetos.

Cuando crea una URL prefirmada con el SDK de AWS o el AWS Command Line Interface (AWS CLI), asocia la URL a una acción específica. También puede conceder acceso por tiempo limitado a la URL prefirmada eligiendo un tiempo de caducidad personalizado que puede ser de tan solo 1 segundo y de hasta 7 días. Cuando comparte la URL prefirmada, la persona de la VPC puede realizar la acción incrustada en la URL como si fuera el usuario de firma original. La URL caducará y ya no funcionará cuando llegue a su hora de vencimiento.

## Limitación de las capacidades de URL prefirmadas

Las capacidades de una URL están limitadas por los permisos del usuario que la creó. En esencia, las URL prefirmadas son tokens al portador que otorgan acceso a quienes las poseen. Por lo tanto, le recomendamos que los proteja adecuadamente.

AWS Signature Version 4 (SigV4)

Para aplicar un comportamiento específico cuando las solicitudes de URL prefirmadas se autentican mediante AWS Signature Version 4 (SigV4), puede usar claves de condición en las políticas de bucket y en las políticas de punto de acceso. Por ejemplo, puede crear una política de bucket que use la condición `s3-outposts:signatureAge` para denegar cualquier solicitud de URL prefirmada de Amazon S3 en Outposts en los objetos del bucket `example-outpost-bucket` si la

firma tiene más de 10 minutos de antigüedad. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Deny a presigned URL request if the signature is more than 10
 minutes old",
            "Effect": "Deny",
            "Principal": {"AWS":"444455556666"},
            "Action": "s3-outposts:*",
            "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
*",
            "Condition": {
                "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
                "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
            }
        }
    ]
}
```

Para obtener una lista de claves de condición y políticas de ejemplo adicionales que puede usar para imponer un comportamiento específico cuando las solicitudes de URL prefirmadas se autentican mediante Signature Version 4, consulte Claves de política de autenticación de AWS Signature Version 4 (SigV4).

Restricción de ruta de red

Si desea restringir el uso de direcciones URL prefirmadas y todo el acceso de S3 en Outposts a rutas de red concretas, puede escribir políticas que requieran una ruta de red determinada. Para establecer la restricción en la entidad principal de IAM que realiza la llamada, puede usar políticas de AWS Identity and Access Management (IAM) basadas en identidades (por ejemplo, políticas de usuario, grupo o rol). Para establecer la restricción en el recurso S3 en Outposts, puede usar políticas basadas en recursos (por ejemplo, políticas de bucket y punto de acceso).

Una restricción de ruta de red en la entidad principal de IAM requiere que el usuario de esas credenciales realice solicitudes desde la red especificada. Una restricción en el bucket o en el punto de acceso requiere que todas las solicitudes a ese recurso se originen desde la red especificada. Estas restricciones también se aplican fuera del escenario de URL prefirmada.

La condición global de IAM que utilice depende del tipo de punto de conexión. Si está utilizando el punto de conexión público para S3 en Outposts, utilice `aws:SourceIp`. Si utiliza un punto de conexión de VPC en S3 en Outposts, utilice `aws:SourceVpc` o `aws:SourceVpce`.

La siguiente instrucción de política de IAM requiere que la entidad principal acceda a AWS solo desde el rango de red especificado. Con esta declaración de política, todo acceso debe originarse desde ese rango. Esto incluye el caso de alguien que usa una URL prefirmada para S3 en Outposts. Para utilizar este ejemplo, reemplace los *`user input placeholders`* con su propia información.

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
}
```

Para ver una política de bucket de ejemplo que usa la clave de condición global `aws:SourceIP` de AWS para restringir el acceso a un bucket de S3 en Outposts a un rango de red específico, consulte Configuración de IAM con S3 en Outposts.

## Quién puede crear una URL prefirmada

Cualquiera que tenga credenciales de seguridad válidas puede crear una URL prefirmada. Sin embargo, para que un usuario de la VPC pueda acceder a un objeto correctamente, la URL prefirmada debe haber sido creada por alguien que tenga permiso para realizar la operación en la que se basa la URL prefirmada.

Puede usar estas credenciales para crear una URL prefirmada:

- Perfil de instancia de IAM: válido hasta 6 horas.
- AWS Security Token Service: válido hasta 36 horas cuando se firma con las credenciales permanentes, como, por ejemplo, las credenciales del usuario raíz de la Cuenta de AWS o un usuario de IAM.
- Usuario de IAM: válido hasta 7 días cuando se utiliza AWS Signature Version 4.

Para crear una URL prefirmada que es válida hasta 7 días, primero delegue las credenciales de usuario de IAM (la clave de acceso y la clave secreta) al SDK que está utilizando. A continuación, genere una URL prefirmada mediante AWS Signature Version 4.

> **Note**
>
> - Si creó una URL prefirmada con un token temporal, la URL caducará cuando caduque el token, incluso si creó la URL con un tiempo de vencimiento posterior.
> - Dado que las URL prefirmadas otorgan acceso a los buckets de S3 en Outposts a quien tenga la URL, recomendamos que los proteja adecuadamente. Para obtener más información sobre la protección de las URL prefirmadas, consulte Limitación de las capacidades de URL prefirmadas.

## ¿Cuándo comprueba S3 en Outposts la fecha y hora de vencimiento de una URL prefirmada?

S3 en Outposts comprueba la fecha y hora de vencimiento de una URL firmada al realizarse la solicitud HTTP. Por ejemplo, si un cliente comienza a descargar un archivo grande inmediatamente antes de la fecha de vencimiento, la descarga continúa incluso si se sobrepasa la hora de vencimiento durante la descarga. Sin embargo, si la conexión se interrumpe y el cliente intenta reiniciar la descarga después de la hora de vencimiento, la descarga produce un error.

Para obtener más información sobre el uso de una URL prefirmada con objeto de compartir o cargar objetos, consulte los siguientes temas.

Temas

- Uso compartido de objetos con URL prefirmadas
- Generación de una URL prefirmada para cargar un objeto en un bucket de S3 en Outposts

## Uso compartido de objetos con URL prefirmadas

Para conceder acceso por tiempo limitado a los objetos que se almacenan localmente en un Outpost sin actualizar su política de bucket, puede usar una URL prefirmada. Con las URL prefirmadas,

usted, como propietario del bucket, puede compartir objetos con personas en su nube privada virtual (VPC) o concederles la capacidad de cargar o eliminar objetos.

Cuando crea una URL prefirmada con el SDK de AWS o el AWS Command Line Interface (AWS CLI), asocia la URL a una acción específica. También puede conceder acceso por tiempo limitado a la URL prefirmada eligiendo un tiempo de caducidad personalizado que puede ser de tan solo 1 segundo y de hasta 7 días. Cuando comparte la URL prefirmada, la persona de la VPC puede realizar la acción incrustada en la URL como si fuera el usuario de firma original. La URL caducará y ya no funcionará cuando llegue a su hora de vencimiento.

Cuando crea una URL prefirmada, debe proporcionar sus credenciales de seguridad y luego especificar lo siguiente:

- Un nombre de recurso de Amazon (ARN) de punto de acceso para el bucket de Amazon S3 en Outposts
- Una clave del objeto
- Un método HTTP (`GET` para descargar objetos)
- Una fecha y hora de caducidad

Una URL prefirmada solo es válida para la duración especificada. Es decir, debe comenzar la acción permitida por la URL antes de la fecha y hora de vencimiento. Puede utilizar una URL prefirmada varias veces, hasta la fecha y hora de vencimiento. Si creó una URL prefirmada con un token temporal, la URL caducará cuando caduque el token, incluso si creó la URL con un tiempo de vencimiento posterior.

Los usuarios de la nube privada virtual (VPC) que tienen acceso a la URL prefirmada pueden acceder al objeto. Por ejemplo, si tiene un video en su bucket y tanto el bucket como el objeto son privados, puede compartir el video con otros generando una URL prefirmada. Dado que las URL prefirmadas otorgan acceso a sus buckets de S3 en Outposts a quien tenga la URL, recomendamos que las proteja adecuadamente. Para obtener más información acerca de la protección de direcciones URL prefirmadas, consulte Limitación de las capacidades de URL prefirmadas.

Cualquiera que tenga credenciales de seguridad válidas puede crear una URL prefirmada. Sin embargo, la URL prefirmada debe haber sido creada por alguien que tenga permisos para realizar la operación en la que se basa la URL prefirmada. Para obtener más información, consulte Quién puede crear una URL prefirmada.

Puede generar una URL prefirmada para compartir un objeto en un bucket de S3 en Outposts mediante el SDK de AWS y la AWS CLI. Para obtener más información, consulte los ejemplos siguientes.

Uso de los AWS SDK

Puede usar los SDK de AWS para generar una URL prefirmada que puede dar a terceros para que puedan recuperar un objeto.

> **Note**
>
> Cuando use los SDK de AWS para generar una URL prefirmada, el tiempo máximo de vencimiento de una URL prefirmada es de 7 días desde el momento de su creación.

Java

Example

El siguiente ejemplo genera una URL prefirmada que puede dar a terceros de modo que puedan recuperar un objeto desde un bucket de S3 en Outposts. Para obtener más información, consulte Uso de URL prefirmadas para S3 en Outposts. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.HttpMethod;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GeneratePresignedUrlRequest;

import java.io.IOException;
import java.net.URL;
import java.time.Instant;

public class GeneratePresignedURL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
```

```
        String accessPointArn = "*** access point ARN ***";
        String objectKey = "*** object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Set the presigned URL to expire after one hour.
            java.util.Date expiration = new java.util.Date();
            long expTimeMillis = Instant.now().toEpochMilli();
            expTimeMillis += 1000 * 60 * 60;
            expiration.setTime(expTimeMillis);

            // Generate the presigned URL.
            System.out.println("Generating pre-signed URL.");
            GeneratePresignedUrlRequest generatePresignedUrlRequest =
                    new GeneratePresignedUrlRequest(accessPointArn, objectKey)
                            .withMethod(HttpMethod.GET)
                            .withExpiration(expiration);
            URL url = s3Client.generatePresignedUrl(generatePresignedUrlRequest);

            System.out.println("Pre-Signed URL: " + url.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't
 process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example

El siguiente ejemplo genera una URL prefirmada que puede dar a terceros de modo que puedan recuperar un objeto desde un bucket de S3 en Outposts. Para obtener más información, consulte

Uso de URL prefirmadas para S3 en Outposts. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;

namespace Amazon.DocSamples.S3
{
    class GenPresignedURLTest
    {
        private const string accessPointArn = "*** access point ARN ***";
        private const string objectKey = "*** object key ***";
        // Specify how long the presigned URL lasts, in hours.
        private const double timeoutDuration = 12;
        // Specify your bucket Region (an example Region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            string urlString = GeneratePreSignedURL(timeoutDuration);
        }
        static string GeneratePreSignedURL(double duration)
        {
            string urlString = "";
            try
            {
                GetPreSignedUrlRequest request1 = new GetPreSignedUrlRequest
                {
                    BucketName = accessPointArn,
                    Key = objectKey,
                    Expires = DateTime.UtcNow.AddHours(duration)
                };
                urlString = s3Client.GetPreSignedURL(request1);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
```

```
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            return urlString;
        }
    }
}
```

Python

Los siguientes ejemplos generan una URL prefirmada para compartir un objeto mediante el SDK para Python (Boto3). Por ejemplo, utilice un cliente Boto3 y la función `generate_presigned_url` para generar una URL prefirmada que le permita `GET` un objeto.

```
import boto3
    url = boto3.client('s3').generate_presigned_url(
    ClientMethod='get_object',
    Params={'Bucket': 'ACCESS_POINT_ARN', 'Key': 'OBJECT_KEY'},
    ExpiresIn=3600)
```

Con el objetivo de obtener más información acerca del uso de SDK para Python (Boto3) a fin de generar una URL prefirmada, consulte Python en la Referencia de la API de AWS SDK for Python (Boto).

Uso de la AWS CLI

El siguiente ejemplo del comando de AWS CLI genera una URL prefirmada para un bucket de S3 en Outposts. Para utilizar este ejemplo, reemplace los *`user input placeholders`* con su propia información.

> **Note**
>
> Cuando use la AWS CLI para generar una URL prefirmada, el tiempo máximo de vencimiento de una URL prefirmada es de 7 días desde el momento de su creación.

```
aws s3 presign s3://arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-
point/mydoc.txt --expires-in 604800
```

Para obtener más información, consulte presign en la Referencia de comandos de la AWS CLI.

## Generación de una URL prefirmada para cargar un objeto en un bucket de S3 en Outposts

Para conceder acceso por tiempo limitado a los objetos que se almacenan localmente en un Outpost sin actualizar su política de bucket, puede usar una URL prefirmada. Con las URL prefirmadas, usted, como propietario del bucket, puede compartir objetos con personas en su nube privada virtual (VPC) o concederles la capacidad de cargar o eliminar objetos.

Cuando crea una URL prefirmada con el SDK de AWS o el AWS Command Line Interface (AWS CLI), asocia la URL a una acción específica. También puede conceder acceso por tiempo limitado a la URL prefirmada eligiendo un tiempo de caducidad personalizado que puede ser de tan solo 1 segundo y de hasta 7 días. Cuando comparte la URL prefirmada, la persona de la VPC puede realizar la acción incrustada en la URL como si fuera el usuario de firma original. La URL caducará y ya no funcionará cuando llegue a su hora de vencimiento.

Cuando crea una URL prefirmada, debe proporcionar sus credenciales de seguridad y luego especificar lo siguiente:

- Un nombre de recurso de Amazon (ARN) de punto de acceso para el bucket de Amazon S3 en Outposts
- Una clave del objeto
- Un método HTTP (PUT para cargar objetos)
- Una fecha y hora de caducidad

Una URL prefirmada solo es válida para la duración especificada. Es decir, debe comenzar la acción permitida por la URL antes de la fecha y hora de vencimiento. Puede utilizar una URL prefirmada varias veces, hasta la fecha y hora de vencimiento. Si creó una URL prefirmada con un token temporal, la URL caducará cuando caduque el token, incluso si creó la URL con un tiempo de vencimiento posterior.

Si la acción permitida por una URL prefirmada consta de varios pasos, como una carga multiparte, todos los pasos deben comenzar antes de la hora de vencimiento. Si S3 en Outposts intenta comenzar un paso con una URL vencida, recibirá un error.

Los usuarios de la nube privada virtual (VPC) que tienen acceso a la URL prefirmada pueden cargar objetos. Por ejemplo, un usuario de la VPC que tenga acceso a la URL prefirmada puede cargar un objeto en su bucket. Dado que las URL prefirmadas otorgan acceso a su bucket de S3 en Outposts a cualquier usuario de la VPC que tenga acceso a la URL prefirmada, recomendamos que las proteja adecuadamente. Para obtener más información acerca de la protección de direcciones URL prefirmadas, consulte Limitación de las capacidades de URL prefirmadas.

Cualquiera que tenga credenciales de seguridad válidas puede crear una URL prefirmada. Sin embargo, la URL prefirmada debe haber sido creada por alguien que tenga permisos para realizar la operación en la que se basa la URL prefirmada. Para obtener más información, consulte Quién puede crear una URL prefirmada.

## Genere una URL prefirmada para una operación de objeto de S3 en Outposts mediante los SDK de AWS

Java

SDK para Java 2.x

En este ejemplo, se muestra cómo generar una URL prefirmada que puede usar para cargar un objeto en un bucket de S3 en Outposts durante un tiempo limitado. Para obtener más información, consulte Uso de URL prefirmadas para S3 en Outposts.

```
   public static void signBucket(S3Presigner presigner, String
outpostAccessPointArn, String keyName) {

       try {
           PutObjectRequest objectRequest = PutObjectRequest.builder()
                   .bucket(accessPointArn)
                   .key(keyName)
                   .contentType("text/plain")
                   .build();

           PutObjectPresignRequest presignRequest =
PutObjectPresignRequest.builder()
                   .signatureDuration(Duration.ofMinutes(10))
                   .putObjectRequest(objectRequest)
```

```
                    .build();

            PresignedPutObjectRequest presignedRequest =
presigner.presignPutObject(presignRequest);


            String myURL = presignedRequest.url().toString();
            System.out.println("Presigned URL to upload a file to: " +myURL);
            System.out.println("Which HTTP method must be used when uploading a
file: " +
                    presignedRequest.httpRequest().method());

            // Upload content to the S3 on Outposts bucket by using this URL.
            URL url = presignedRequest.url();

            // Create the connection and use it to upload the new object by using
the presigned URL.
            HttpURLConnection connection = (HttpURLConnection)
url.openConnection();
            connection.setDoOutput(true);
            connection.setRequestProperty("Content-Type","text/plain");
            connection.setRequestMethod("PUT");
            OutputStreamWriter out = new
OutputStreamWriter(connection.getOutputStream());
            out.write("This text was uploaded as an object by using a presigned
URL.");
            out.close();

            connection.getResponseCode();
            System.out.println("HTTP response code is " +
connection.getResponseCode());

        } catch (S3Exception e) {
            e.getStackTrace();
        } catch (IOException e) {
            e.getStackTrace();
        }
    }
```

Python

SDK para Python (Boto3)

En este ejemplo, se muestra cómo generar una URL prefirmada que pueda realizar una acción de S3 en Outposts durante un tiempo limitado. Para obtener más información, consulte Uso de URL prefirmadas para S3 en Outposts. Para realizar una solicitud con la URL, utilice el paquete `Requests`.

```
import argparse
import logging
import boto3
from botocore.exceptions import ClientError
import requests

logger = logging.getLogger(__name__)


def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned S3 on Outposts URL that can be used to perform an
 action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds that the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
        logger.info("Got presigned URL: %s", url)
    except ClientError:
        logger.exception(
            "Couldn't get a presigned URL for client method '%s'.",
 client_method)
        raise
    return url
```

```
def usage_demo():
    logging.basicConfig(level=logging.INFO, format='%(levelname)s: %(message)s')

    print('-'*88)
    print("Welcome to the Amazon S3 on Outposts presigned URL demo.")
    print('-'*88)

    parser = argparse.ArgumentParser()
    parser.add_argument('accessPointArn', help="The name of the S3 on Outposts
 access point ARN.")
    parser.add_argument(
        'key', help="For a GET operation, the key of the object in S3 on
 Outposts. For a "
                    "PUT operation, the name of a file to upload.")
    parser.add_argument(
        'action', choices=('get', 'put'), help="The action to perform.")
    args = parser.parse_args()

    s3_client = boto3.client('s3')
    client_action = 'get_object' if args.action == 'get' else 'put_object'
    url = generate_presigned_url(
        s3_client, client_action, {'Bucket': args.accessPointArn, 'Key':
 args.key}, 1000)

    print("Using the Requests package to send a request to the URL.")
    response = None
    if args.action == 'get':
        response = requests.get(url)
    elif args.action == 'put':
        print("Putting data to the URL.")
        try:
            with open(args.key, 'r') as object_file:
                object_text = object_file.read()
            response = requests.put(url, data=object_text)
        except FileNotFoundError:
            print(f"Couldn't find {args.key}. For a PUT operation, the key must
 be the "
                  f"name of a file that exists on your computer.")

    if response is not None:
        print("Got response:")
        print(f"Status: {response.status_code}")
```

```
        print(response.text)

    print('-'*88)


if __name__ == '__main__':
    usage_demo()
```

# Amazon S3 en Outposts con Amazon EMR en Outposts local

Amazon EMR es una plataforma de clúster administrada que simplifica la ejecución de marcos de macrodatos, tales como Apache Hadoop y Apache Spark en AWS para procesar y analizar grandes cantidades de datos. Mediante el uso de estos marcos de trabajo y proyectos de código abierto relacionados, puede procesar datos para fines de análisis y cargas de trabajo de inteligencia empresarial. Además, Amazon EMR permite transformar y trasladar grandes cantidades de datos hacia y desde otros almacenes y bases de datos de AWS, como Amazon S3 en Outposts. Para obtener más información sobre Amazon EMR, consulte Clústeres de EMR en AWS Outposts en la Guía de administración de Amazon EMR.

Para Amazon S3 en Outposts, Amazon EMR comenzó a admitir el conector S3A de Apache Hadoop en la versión 7.0.0. Las versiones anteriores de Amazon EMR no admiten S3 en Outposts localmente y tampoco son compatibles con el sistema de archivos de EMR (EMRFS).

Aplicaciones compatibles

Amazon EMR con Amazon S3 en Outposts admite las siguientes aplicaciones:

- Hadoop
- Spark
- Hue
- Hive
- Sqoop
- Pig
- Hudi
- Flink

Para obtener más información, consulte la Guía de publicación de Amazon EMR.

# Creación y configuración de un bucket de Amazon S3 en Outposts

Amazon EMR utiliza el AWS SDK para Java con Amazon S3 en Outposts para almacenar datos de entrada y de salida. Los archivos de registro de Amazon EMR se almacenan en la ubicación regional de Amazon S3 que elija pero no se almacenan localmente en Outpost. Para obtener más información, consulte Ver archivos de registro en la Guía de administración de Amazon EMR.

Los buckets de S3 on Outposts aplican ciertas restricciones y limitaciones de nomenclatura para cumplir con los requisitos de Amazon S3 y DNS. Para obtener más información, consulte Creación de un bucket de S3 en Outposts.

Con la versión 7.0.0 y posteriores de Amazon EMR, puede usar Amazon EMR con S3 en Outposts y el sistema de archivos S3A.

Requisitos previos

Permisos de S3 en Outposts: al crear el perfil de instancia de Amazon EMR, su rol debe incluir el espacio de nombres de AWS Identity and Access Management (IAM) para S3 en Outposts. S3 en Outposts tiene su propio espacio de nombres: `s3-outposts*`. Para ver un ejemplo de política que utiliza este espacio de nombres, consulte Configuración de IAM con S3 en Outposts.

Conector S3A: para configurar el clúster de EMR para que pueda acceder a los datos de un bucket de Amazon S3 en Outposts, debe utilizar el conector S3A de Apache Hadoop. Para usar el conector, asegúrese de que todos sus URI de S3 usen el esquema `s3a`. Si no es así, puede configurar la implementación del sistema de archivos que utiliza para el clúster de EMR para que sus URI de S3 funcionen con el conector S3A.

Para configurar la implementación del sistema de archivos para que funcione con el conector S3A, utilice las propiedades de configuración `fs.`*`file_scheme`*`.impl` y `fs.AbstractFileSystem.`*`file_scheme`*`.impl` del clúster de EMR, donde *`file_scheme`* equivale al tipo de URI de S3 que tenga. Para utilizar el ejemplo siguiente, sustituya *`user input placeholders`* con su propia información. Por ejemplo, para cambiar la implementación del sistema de archivos para los URI de S3 que utilizan el esquema `s3`, especifique las siguientes propiedades de configuración del clúster:

```
[
  {
"Classification": "core-site",
    "Properties": {
    "fs.s3.impl": "org.apache.hadoop.fs.s3a.S3AFileSystem",
```

```
    "fs.AbstractFileSystem.s3.impl": "org.apache.hadoop.fs.s3a.S3A"
    }
  }
]
```

Para usar S3A, defina la propiedad de configuración `fs.file_scheme.impl` en `org.apache.hadoop.fs.s3a.S3AFileSystem` y establezca la propiedad `fs.AbstractFileSystem.file_scheme.impl` en `org.apache.hadoop.fs.s3a.S3A`.

Por ejemplo, si accede a la ruta `s3a://bucket/...`, defina la propiedad `fs.s3a.impl` en `org.apache.hadoop.fs.s3a.S3AFileSystem` y establezca la propiedad `fs.AbstractFileSystem.s3a.impl` en `org.apache.hadoop.fs.s3a.S3A`.

## Introducción al uso de Amazon EMR con Amazon S3 en Outposts

En los temas que siguen se explica cómo empezar a utilizar Amazon EMR con Amazon S3 en Outposts.

Temas

- Creación de una política de permisos
- Creación y configuración de un clúster
- Información general sobre las configuraciones
- Consideraciones

### Creación de una política de permisos

Antes de poder crear un clúster de EMR que utilice Amazon S3 en Outposts, debe crear una política de IAM para adjuntarla al perfil de instancia de Amazon EC2 para el clúster. La política debe tener permisos de acceso al Nombre de recurso de Amazon (ARN) del punto de acceso de S3 en Outposts. Para obtener más información acerca de la creación de políticas de IAM para S3 en Outposts, consulte Configuración de IAM con S3 en Outposts.

En la siguiente política de ejemplo se muestra cómo conceder los permisos necesarios. Después de crear la política, adjúntela al rol de perfil de instancia que utilice para crear su clúster de EMR, tal y como se describe en la sección the section called “Creación y configuración de un clúster”. Para utilizar este ejemplo, reemplace los *user input placeholders* con su propia información.

```
{
```

```
"Version":"2012-10-17",
  "Statement": [
        {
  "Effect": "Allow",
            "Resource": "arn:aws:s3-outposts:us-
west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name,
            "Action": [
                "s3-outposts:*"
            ]
        }
    ]

 }
```

## Creación y configuración de un clúster

Para crear un clúster que ejecute Spark con S3 en Outposts, complete los siguientes pasos en la consola.

Para crear un clúster que ejecute Spark con S3 en Outposts

1. Abra la consola de Amazon EMR enhttps://console.aws.amazon.com/elasticmapreduce/.
2. En el panel de navegación izquierdo, elija Clusters (Clústeres).
3. Elija Create cluster.
4. Para la versión de Amazon EMR, elija emr-7.0.0 o posterior.
5. Para el paquete de aplicaciones, elija Interactivo con Spark. Seleccione cualquier otra aplicación que desee incluir en el clúster.
6. Para habilitar Amazon S3 en Outposts, realice la siguiente configuración.

   Ejemplo de configuración

   Para usar esta configuración de ejemplo, sustituya *user input placeholders* por su información.

   ```
   [
    {
      "Classification": "core-site",
      "Properties": {
        "fs.s3a.bucket.DOC-EXAMPLE-BUCKET.accesspoint.arn": "arn:aws:s3-outposts:us-
   west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name"
   ```

```
     "fs.s3a.committer.name": "magic",
     "fs.s3a.select.enabled": "false"
    }
  },
  {
    "Classification": "hadoop-env",
    "Configurations": [
      {
        "Classification": "export",
        "Properties": {
          "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
         }
       }
     ],
     "Properties": {}
   },
   {
     "Classification": "spark-env",
     "Configurations": [
       {
         "Classification": "export",
         "Properties": {
           "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
         }
       }
      ],
      "Properties": {}
     },
     {
      "Classification": "spark-defaults",
      "Properties": {
        "spark.executorEnv.JAVA_HOME": "/usr/lib/jvm/java-11-amazon-
corretto.x86_64",
        "spark.sql.sources.fastS3PartitionDiscovery.enabled": "false"
      }
     }
  ]
```

7. En la sección Redes, elija una nube privada virtual (VPC) y una subred que estén en su bastidor de AWS Outposts. Para obtener más información sobre Amazon EMR en Outposts, consulte Clústeres de EMR en AWS Outposts en la Guía de administración de Amazon EMR.

8. En la sección Perfil de instancia de EC2 para Amazon EMR, elija el rol de IAM que tenga adjunta la política de permisos que ha creado anteriormente.
9. Configure los ajustes de clúster restantes y, a continuación, elija Crear clúster.

## Información general sobre las configuraciones

En las siguientes tablas se describen las configuraciones de S3A y los valores que se deben especificar para los parámetros al configurar un clúster que utiliza S3 en Outposts con Amazon EMR.

| Parámetro | Valor predeterminado | Valor obligatorio para S3 en Outposts | Explicación |
|---|---|---|---|
| `fs.s3a.aws.credentials.provider` | Si no se especifica, S3A buscará el bucket de S3 de la región con el nombre del bucket de Outposts. | El ARN del punto de acceso del bucket de S3 en Outposts | Amazon S3 en Outposts admite puntos de acceso únicamente de la virtual private cloud (VPC) como el único medio para acceder a los buckets de Outposts. |
| `fs.s3a.committer.name` | `file` | `magic` | Magic es el único confirmador compatible con S3 en Outposts. |
| `fs.s3a.select.enabled` | `TRUE` | `FALSE` | S3 Select no es compatible con Outposts. |
| `JAVA_HOME` | `/usr/lib/jvm/java-8` | `/usr/lib/jvm/java-11-amazon-corretto.x86_64` | S3 en Outposts en S3A requiere la versión 11 de Java. |

En las siguientes tablas, se describen las configuraciones de Spark y los valores que se deben especificar para los parámetros al configurar un clúster que utiliza S3 en Outposts con Amazon EMR.

| Parámetro | Valor predeterminado | Valor obligatorio para S3 en Outposts | Explicación |
| --- | --- | --- | --- |
| `spark.sql.sources.fastS3PartitionDiscovery.enabled` | `TRUE` | `FALSE` | S3 en Outposts no admite la partición rápida. |
| `spark.executorEnv.JAVA_HOME` | `/usr/lib/jvm/java-8` | `/usr/lib/jvm/java-11-amazon-corretto.x86_64` | S3 en Outposts en S3A requiere la versión 11 de Java. |

## Consideraciones

Tenga en cuenta lo siguiente cuando integre Amazon EMR con los buckets de S3 en Outposts:

- Amazon S3 en Outposts es compatible con la versión 7.0.0 y posteriores de Amazon EMR.
- Se requiere el conector S3A para utilizar S3 en Outposts con Amazon EMR. Solo S3A tiene las características necesarias para interactuar con los buckets de S3 en Outposts. Para obtener información sobre la configuración del conector S3A, consulte el apartado Requisitos previos.
- Amazon S3 en Outposts solo admite el cifrado del servidor con claves administradas por Amazon S3 (SSE-S3) con Amazon EMR. Para obtener más información, consulte the section called “Cifrado de datos”.
- Amazon S3 en Outposts no admite la escritura con el FileOutputCommitter de S3A. Al escribir con el FileOutputCommitter de S3A en los buckets de S3 en Outposts, se produce el siguiente error: InvalidStorageClass: The storage class you specified is not valid.
- Amazon S3 en Outposts no es compatible con Amazon EMR sin servidor ni Amazon EMR en EKS.
- Los registros de Amazon EMR se almacenan en la ubicación regional de Amazon S3 que haya elegido pero no se almacenan localmente en el bucket de S3 en Outposts.

# Almacenamiento en caché de autorización y autenticación

S3 en Outposts almacena en caché localmente los datos de autenticación y autorización de forma segura en los bastidores de Outposts. La memoria caché elimina viajes de ida y vuelta a la Región de AWS principal por cada solicitud. Esto elimina la variabilidad que generan los viajes de ida y vuelta en la red. Con la caché de autenticación y autorización de S3 en Outposts, obtiene latencias consistentes que son independientes de la latencia de la conexión entre Outposts y la Región de AWS.

Cuando realiza una solicitud a la API de S3 en Outposts, los datos de autenticación y autorización se almacenan en caché de forma segura. Luego, los datos en caché se utilizan para autenticar las solicitudes posteriores a la API de objetos de S3. S3 en Outposts solo almacena en caché los datos de autenticación y autorización cuando la solicitud se firma utilizando Signature Version 4A (SigV4A). La caché se almacena localmente en los Outposts dentro del servicio S3 en Outposts. Se actualiza de forma asíncrona cuando se realiza una solicitud a la API de S3. La caché se cifra y en Outposts no se almacena ninguna clave criptográfica en texto sin formato.

La caché es válida durante un máximo de 10 minutos cuando el Outpost está conectado a la Región de AWS. Se actualiza de forma asíncrona cuando realiza una solicitud a la API de S3 en Outposts para garantizar que se utilicen las políticas más recientes. Si el Outpost se desconecta de la Región de AWS, la caché será válida durante un máximo de 12 horas.

## Configuración de la caché de autorización y autenticación

S3 en Outposts almacena automáticamente en caché los datos de autenticación y autorización de las solicitudes firmadas con el algoritmo SigV4A. Para obtener más información, consulte Firma de solicitudes de API de AWS en la Guía del usuario de AWS Identity and Access Management. El algoritmo SigV4A está disponible en las versiones más recientes de los SDK de AWS. Puede obtenerlo a través de una dependencia en las bibliotecas de AWS Common Runtime (CRT).

Debe usar la versión más reciente del SDK de AWS e instalar la versión más reciente de CRT. Por ejemplo, puede ejecutar `pip install awscrt` para obtener la versión más reciente de CRT con Boto3.

S3 en Outposts no almacena en caché los datos de autenticación y autorización de las solicitudes firmadas con el algoritmo SigV4.

# Validación de la firma de SigV4

Se puede utilizar AWS CloudTrail para validar que las solicitudes se hayan firmado con SigV4. Para obtener más información sobre la configuración de CloudTrail para S3 en Outposts, consulte Monitoreo de S3 en Outposts con registros de AWS CloudTrail.

Tras configurar CloudTrail, puede comprobar cómo se firmó una solicitud en el campo `SignatureVersion` de los registros de CloudTrail. Las solicitudes que se hayan firmado con SigV4A tendrán `SignatureVersion` establecido en `AWS4-ECDSA-P256-SHA256`. Las solicitudes que se hayan firmado con SigV4 tendrán `SignatureVersion` establecido en `AWS4-HMAC-SHA256`.

# Seguridad en S3 en Outposts

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta Servicios de AWS en Nube de AWS. Además, AWS proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a Amazon S3 en Outposts, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad es determinada por el Servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza S3 en Outposts. En los siguientes temas, se le mostrará cómo configurar S3 en Outposts para satisfacer sus objetivos de seguridad y conformidad. También puede obtener información sobre cómo utilizar otros Servicios de AWS que le ayuden a monitorear y proteger los recursos de S3 en Outposts.

Temas

# Configuración de IAM con S3 en Outposts

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los gestionadores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon S3 en Outposts. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional. De forma predeterminada, los usuarios no tienen permisos para los recursos y las operaciones de S3 en Outposts. Para conceder permisos de acceso para los recursos de S3 en Outposts y operaciones de API, puede usar IAM para crear usuarios, grupos o roles y adjuntar permisos.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Además de las políticas de IAM basadas en identidad, S3 en Outposts admite políticas de punto de acceso y bucket. Las políticas de punto de acceso y bucket son políticas de basadas en recursos que están asociadas al recurso S3 en Outposts.

- Una política de bucket se asocia al bucket y permite o deniega solicitudes al bucket y a los objetos que hay en él en función de los elementos de la política.
- Por el contrario, se adjunta una política de punto de acceso al punto de acceso y permite o deniega solicitudes al punto de acceso.

La política de punto de acceso funciona con la política de bucket asociada al bucket S3 en Outposts subyacente. Para que una aplicación o un usuario pueda acceder a objetos en un bucket de S3 en Outposts a través de un punto de acceso de S3 en Outposts, tanto la política de punto de acceso como la política de bucket deben permitir la solicitud.

Las restricciones que se incluyen en una política de punto de acceso solo se aplican a las solicitudes realizadas a través de ese punto de acceso. Por ejemplo, si un punto de acceso está conectado a un bucket, no puede usar la política de punto de acceso para permitir o denegar las solicitudes que se realizan directamente en el bucket. Sin embargo, las restricciones que se aplican a una política de bucket pueden permitir o denegar solicitudes realizadas directamente al bucket o a través del punto de acceso.

En una política de IAM o una política basada en recursos, usted define qué acciones de S3 en Outposts se permiten o deniegan. Las acciones de S3 en Outposts corresponden a operaciones específicas de la API S3 en Outposts. Las acciones de S3 en Outposts utilizan el prefijo de espacio de nombres `s3-outposts:`. Las solicitudes realizadas a la API de control de S3 en Outposts en una Región de AWS y las solicitudes realizadas a los puntos de conexión de la API de objeto en el Outpost se autentican mediante IAM y se autorizan en el prefijo de espacio de nombres `s3-outposts:`. Para trabajar con S3 en Outposts, configure los usuarios de IAM y autorícelos en el espacio de nombres de IAM de `s3-outposts:`.

Para obtener información, consulte Acciones, recursos y claves de condición de Amazon S3 en Outposts en la Referencia de autorizaciones de servicio.

> **Note**
>
> - S3 en Outposts no admite las listas de control de acceso (ACL).
> - S3 en Outposts toma de forma predeterminada al propietario del bucket como propietario del objeto, para ayudar a garantizar que no se pueda impedir que el propietario de un bucket acceda a los objetos o los elimine.
> - S3 en Outposts siempre tiene Bloquear Acceso público en S3 habilitado para ayudar a garantizar que los objetos nunca puedan tener acceso público.

Para obtener más información acerca de la configuración de IAM para S3 en Outposts, consulte los siguientes temas.

Temas

## Entidades principales para las políticas de S3 en Outposts

Cuando crea una política basada en recursos para conceder acceso a su bucket S3 en Outposts, debe utilizar el elemento `Principal` para especificar la persona o aplicación que puede realizar una solicitud para realizar una acción o una operación en ese recurso. Para las políticas S3 en Outposts, puede utilizar una de las siguientes entidades principales:

- Una Cuenta de AWS
- Un usuario de IAM
- Un rol de IAM
- Todas las entidades principales mediante la especificación de un carácter comodín (*) de una política que utiliza un elemento `Condition` para limitar el acceso a un rango de IP específicas

> **Important**
>
> No puede escribir una política para un bucket de S3 en Outposts que utilice un carácter comodín (`*`) en el elemento `Principal` a menos que la política también incluya una `Condition` que limite el acceso a un rango de direcciones IP específicas. Esta restricción contribuye a asegurar que no hay acceso público a su bucket de S3 en Outposts. Para ver un ejemplo, consulta Ejemplos de políticas para S3 en Outposts.

Para obtener más información acerca del elemento `Principal`, consulte Elementos de la política JSON de AWS: entidad principal en la Guía del usuario de IAM.

## ARN de recursos para S3 en Outposts

Los nombres de recurso de Amazon (ARN) para S3 en Outposts contienen el ID de Outpost, además de la Región de AWS donde está destinado el Outpost, el ID de Cuenta de AWS y el nombre del

recurso. Para acceder y realizar acciones en los buckets y objetos de Outposts, debe utilizar uno de los formatos de ARN que se muestran en la tabla siguiente.

El valor *partition* en el ARN hace referencia a un grupo de Regiones de AWS. Cada Cuenta de AWS está limitada a una partición. Las siguientes son las particiones admitidas:

- `aws` – Regiones de AWS
- `aws-us-gov`: regiones de AWS GovCloud (US)

La siguiente tabla muestra formatos ARN de S3 en Outposts.

| ARN de Amazon S3 en Outposts | Formato de ARN | Ejemplo |
|---|---|---|
| ARN de bucket | arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /bucket/*bucket_name* | arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /bucket/*amzn-s3-demo-bucket1* |
| ARN del punto de acceso. | arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /accesspoint/ *accesspoint_name* | arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /accesspoint/ *access-point-name* |
| ARN de objeto | arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /bucket/*bucket_name* /object/*object_key* | arn:*aws*:s3-outposts: *us-west-2* :*123456789012* :outpost/ *op-01ac5d28a6a232904* /bucket/*amzn-s3-demo-* |

| ARN de Amazon S3 en Outposts | Formato de ARN | Ejemplo |
|---|---|---|
| | | *bucket1 /object/m yobject* |
| ARN de objeto de punto de acceso de S3 en Outposts (utilizado en políticas) | arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* /accesspoint/ *accesspoint_name* / object/*object_key* | arn:*aws*:s3-outposts: *us-west-2* :*123456789012* : outpost/ *op-01ac5d28a6a232904* /accesspoint/ *access-point-name/object/myobject* |
| ARN de S3 en Outposts | arn:*partition* :s3-outposts: *region*: *account_id* :outpost/ *outpost_id* | arn:*aws*:s3-outposts: *us-west-2* :*123456789012* : outpost/ *op-01ac5d28a6a232904* |

## Ejemplos de políticas para S3 en Outposts

Example : política de bucket de S3 en Outposts con una entidad principal de Cuenta de AWS

La siguiente política de bucket utiliza una entidad principal de Cuenta de AWS para conceder acceso a un bucket S3 en Outposts. Para utilizar esta política de bucket, reemplace *user input placeholders* por su propia información.

```
{
   "Version":"2012-10-17",
   "Id":"ExampleBucketPolicy1",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Principal":{
            "AWS":"123456789012"
         },
         "Action":"s3-outposts:*",
```

```
         "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket"
      }
   ]
}
```

Example : política de bucket de S3 en Outposts con clave de entidad principal y condición (*) para limitar el acceso a un rango de direcciones IP específicas

La siguiente política de bucket utiliza una entidad principal comodín (*) con la condición `aws:SourceIp` para limitar el acceso a un rango de direcciones IP específicas. Para utilizar esta política de bucket, reemplace *user input placeholders* por su propia información.

```
{
    "Version": "2012-10-17",
    "Id": "ExampleBucketPolicy2",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": { "AWS" : "*" },
            "Action":"s3-outposts:*",
            "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "198.51.100.0/24"
                }
            }
        }
    ]
}
```

## Permisos para los puntos de conexión de S3 en Outposts

S3 en Outposts requiere sus propios permisos en IAM para administrar las acciones de puntos de conexión de S3 en Outposts.

> **Note**
>
> - Para los puntos de conexión que utilizan el tipo de acceso de grupo de direcciones IP propiedad del cliente (grupo de CoIP), también debe tener permisos para trabajar con direcciones IP desde el grupo de CoIP, como se describe en la siguiente tabla.
> - Para cuentas compartidas que acceden a S3 en Outposts mediante AWS Resource Access Manager, los usuarios en estas cuentas compartidas no pueden crear sus propios puntos de conexión en una subred compartida. Si el usuario de una cuenta compartida desea administrar sus propios puntos de conexión, la cuenta compartida debe crear su propia subred en Outpost. Para obtener más información, consulte the section called “Uso comaprtido de S3 en Outposts”.

La siguiente tabla muestra permisos de IAM relacionados con los puntos de conexión de S3 en Outposts.

| Acción | Permisos de IAM |
| --- | --- |
| `CreateEndpoint` | `s3-outposts:CreateEndpoint`<br>`ec2:CreateNetworkInterface`<br>`ec2:DescribeNetworkInterfaces`<br>`ec2:DescribeVpcs`<br>`ec2:DescribeSecurityGroups`<br>`ec2:DescribeSubnets`<br>`ec2:CreateTags`<br>`iam:CreateServiceLinkedRole`<br>Para los puntos de enlace que utilizan el tipo de acceso de grupo de direcciones IP |

| Acción | Permisos de IAM |
| --- | --- |
| | propiedad del cliente (grupo CoIP) en las instalaciones, se requieren los siguientes permisos adicionales:<br>`s3-outposts:CreateEndpoint`<br>`ec2:DescribeCoipPools`<br>`ec2:GetCoipPoolUsage`<br>`ec2:AllocateAddress`<br>`ec2:AssociateAddress`<br>`ec2:DescribeAddresses`<br>`ec2:DescribeLocalGatewayRouteTableVpcAssociations` |
| `DeleteEndpoint` | `s3-outposts:DeleteEndpoint`<br>`ec2:DeleteNetworkInterface`<br>`ec2:DescribeNetworkInterfaces`<br>Para los puntos de enlace que utilizan el tipo de acceso de grupo de direcciones IP propiedad del cliente (grupo CoIP) en las instalaciones, se requieren los siguientes permisos adicionales:<br>`s3-outposts:DeleteEndpoint`<br>`ec2:DisassociateAddress`<br>`ec2:DescribeAddresses`<br>`ec2:ReleaseAddress` |
| `ListEndpoints` | `s3-outposts:ListEndpoints` |

> **Note**
>
> Puede utilizar etiquetas de recursos en una política del IAM para administrar permisos.

## Roles vinculados a servicios para S3 en Outposts

S3 en Outposts usa roles vinculados a servicios de IAM para crear algunos recursos de red en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon S3 en Outposts.

# Cifrado de datos en S3 en Outposts

De forma predeterminada, todos los datos almacenados en Amazon S3 en Outposts se cifran mediante cifrado del lado del servidor con claves de cifrado administradas de Amazon S3 (SSE-S3). Para obtener más información, consulte Uso del cifrado del servidor con claves administradas por Amazon S3 (SSE-S3) en la Guía del usuario de Amazon S3.

Opcionalmente, puede usar el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C). Para utilizar SSE-C, especifique una clave de cifrado como parte de las solicitudes de API de objeto. El cifrado en el servidor solo cifra los datos de objetos, no los metadatos de objetos. Para obtener más información, consulte Protección de datos con el cifrado del servidor en la Guía del usuario de Amazon S3.

> **Note**
>
> S3 en Outposts no es compatible con el cifrado del lado del servidor con claves AWS Key Management Service (AWS KMS) (SSE-KMS).

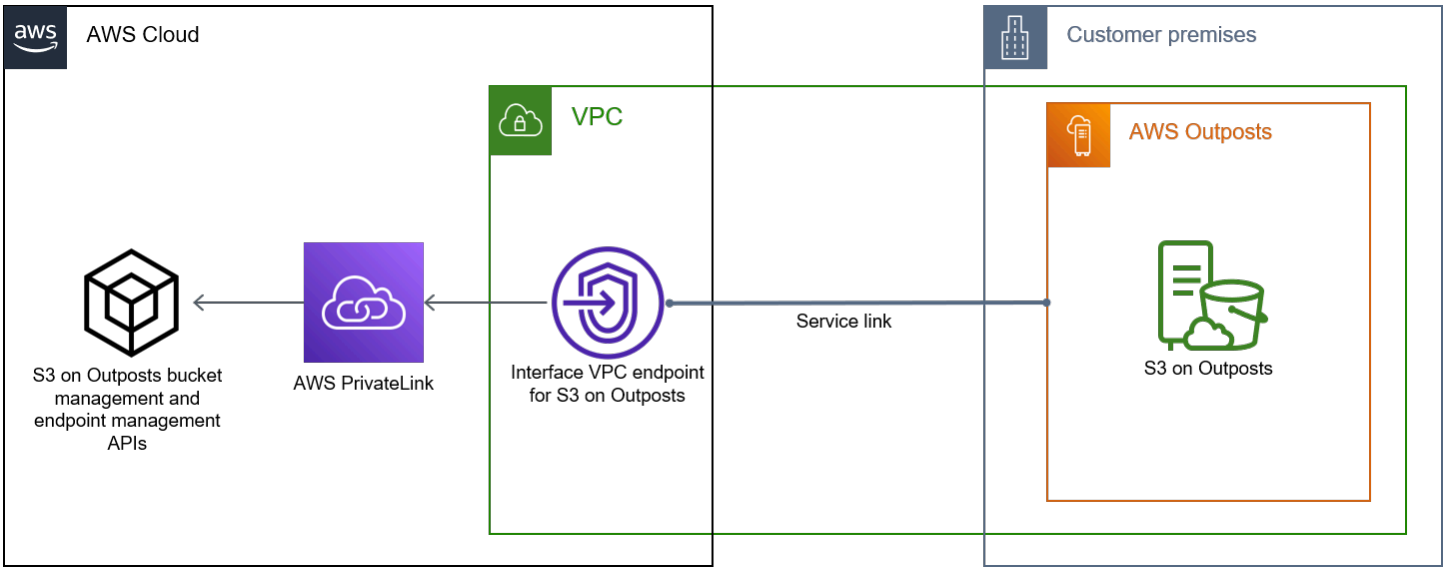
# AWS PrivateLink para S3 en Outposts

S3 en Outposts admite AWS PrivateLink, que proporciona acceso de administración directo a su almacenamiento de S3 en Outposts a través de un punto de conexión privado dentro de su red privada virtual. Esto le permite simplificar la arquitectura de su red interna y realizar operaciones de administración en el almacenamiento de objetos de Outpost mediante el uso de direcciones IP privadas en su nube privada virtual (VPC). El uso de AWS PrivateLink elimina la necesidad de utilizar direcciones IP públicas o servidores proxy.

Con AWS PrivateLink para Amazon S3 en Outposts, puede aprovisionar puntos de conexión de VPC de interfaz en la nube privada virtual (VPC) para acceder a sus API de administración de bucket y administración de puntos de conexión de S3 en Outposts. A los puntos de conexión de VPC de interfaz se puede acceder directamente desde las aplicaciones que se implementan en la VPC o en las instalaciones a través de la red privada virtual (VPN) o AWS Direct Connect. Puede acceder a las API de administración de buckets y de puntos de conexión a través de AWS PrivateLink. AWS PrivateLink no admite operaciones de API de transferencia de datos, como GET, PUT y API similares. Estas operaciones ya se transfieren de forma privada a través de la configuración de punto de acceso y punto de conexión de S3 en Outposts. Para obtener más información, consulte Redes para S3 en Outposts.

Los puntos de enlace de la interfaz se representan mediante una o más interfaces de red elásticas (elastic network interfaces, ENI) a las que se asignan direcciones IP privadas desde subredes de la VPC. Las solicitudes que se realizan a los puntos de conexión de interfaz para S3 en Outposts se enrutan automáticamente a las API de administración de buckets y de punto de conexión de S3 en Outposts en la red de AWS. Asimismo, puede acceder a los puntos de conexión de la interfaz en su VPC desde aplicaciones en las instalaciones a través de AWS Direct Connect oAWS Virtual Private Network (AWS VPN). Para obtener más información sobre cómo conectar la VPC a la red en las instalaciones, consulte la Guía del usuario de AWS Direct Connect y la Guía del usuario de AWS Site-to-Site VPN.

Los puntos de conexión de la interfaz enrutan solicitudes para las API de administración de buckets y de puntos de conexión de S3 en Outposts a través de la red de AWS y a través de AWS PrivateLink, como se ilustra en el siguiente diagrama.



Para obtener más información sobre los puntos de enlace de la interfaz, consulte Puntos de enlace de la VPC de la interfaz (AWS PrivateLink) en la Guía de AWS PrivateLink.

Temas



## Restricciones y limitaciones

Cuando accede a las API de administración de buckets y de puntos de conexión de S3 en Outposts a través de AWS PrivateLink, la VPC tiene una serie de limitaciones. Para obtener más información, consulte Propiedades y limitaciones de los puntos de enlace de interfaz y Cuotas de AWS PrivateLink en la Guía de AWS PrivateLink.

Además, AWS PrivateLink no admite lo siguiente:

- Puntos de conexión del estándar federal de procesamiento de información (FIPS)
- API de transferencia de datos de S3 en Outposts, por ejemplo, operaciones de API de objetos GET, PUT y similares.
- DNS privado

## Acceso a los puntos de conexión de la interfaz de S3 en Outposts

Para acceder a las API de administración de buckets y de puntos de conexión de S3 en Outposts mediante AWS PrivateLink, debe actualizar las aplicaciones para utilizar nombres de DNS específicos de cada punto de conexión. Cuando se crea un punto de conexión de interfaz, AWS PrivateLink genera dos tipos de nombres de S3 en Outposts específicos del punto de conexión: regional y zonal.

- Nombres DNS regionales: incluyen un ID único de punto de conexión de VPC, un identificador de servicio, la Región de AWS y `vpce.amazonaws.com`, por ejemplo, *`vpce-1a2b3c4d-5e6f`*`.s3-outposts.us-east-1.vpce.amazonaws.com`.

- Nombres DNS zonales: incluya un ID de punto de conexión de VPC único, la zona de disponibilidad, un identificador de servicio, Región de AWS y `vpce.amazonaws.com`, por ejemplo, *`vpce-1a2b3c4d-5e6f`*`-us-east-1a.s3-outposts.us-east-1.vpce.amazonaws.com`. Puede utilizar esta opción si la arquitectura aísla Zonas de disponibilidad. Por ejemplo, podría usar nombres DNS zonales para la contención de errores o para reducir los costos de transferencia de datos regionales.

> **Important**
>
> Los puntos de conexión de la interfaz de S3 en Outposts se resuelven desde el dominio de DNS público. S3 en Outposts no admite DNS privados. Utilice el parámetro `--endpoint-url` para todas las API de administración de buckets y puntos de conexión.

## Ejemplos de AWS CLI

Use los parámetros `--region` y `--endpoint-url` para acceder a las API de administración de bucket y administración de punto de conexión a través de puntos de conexión de interfaz de S3 en Outposts.

Example : Utilice la URL del punto de conexión para mostrar buckets con la API de control S3

En el siguiente ejemplo, sustituya la región *`us-east-1`*, la URL de punto de conexión de VPC de *`vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com`* y el ID de cuenta *`111122223333`* por la información adecuada.

```
aws s3control list-regional-buckets --region us-east-1 --endpoint-url
 https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com --account-
id 111122223333
```

## Ejemplos del SDK de AWS

Actualice los SDK a la versión más reciente y configure los clientes para que utilicen una URL de punto de conexión para acceder a la API de control de S3 para puntos de conexión de interfaz de S3 en Outposts.

SDK for Python (Boto3)

Example : utilice una URL de punto de conexión para acceder a la API de control de S3

En el siguiente ejemplo, sustituya la región *us-east-1* y la URL de punto de conexión de VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* por la información adecuada.

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com'
)
```

Para obtener más información, consulte AWS PrivateLink for Amazon S3 en la guía para desarrolladores de Boto 3.

SDK for Java 2.x

Example : utilice una URL de punto de conexión para acceder a la API de control de S3

En el siguiente ejemplo, sustituya la URL de punto de conexión de VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* y la región *Region.US_EAST_1* por la información adecuada.

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

 .endpointOverride(URI.create("https://vpce-1a2b3c4d-5e6f.s3-outposts.us-
east-1.vpce.amazonaws.com"))
                                  .build()
```

Para obtener más información, consulte S3ControlClient en la Referencia de la API de AWS SDK para Java.

## Actualización de una configuración DNS en las instalaciones

Al utilizar nombres DNS específicos de punto de conexión para acceder a los puntos de conexión de la interfaz de las API de administración de bucket y administración de punto de conexión de S3

en Outposts, no es necesario actualizar la resolución DNS local. Puede resolver el nombre DNS específico del punto de conexión con la dirección IP privada del punto de conexión de la interfaz desde el dominio DNS público de S3 en Outposts.

## Creación de un punto de conexión de VPC para S3 en Outposts

Para crear un punto de conexión de interfaz de VPC para S3 en Outposts, consulte Crear un punto de conexión de VPC en la Guía de AWS PrivateLink.

## Creación de políticas de bucket y políticas de punto de conexión de VPC para S3 en Outposts

Puede asociar una política de punto de conexión con el punto de conexión de VPC que controla el acceso a S3 en Outposts. También puede utilizar la condición `aws:sourceVpce` en las políticas de bucket de S3 en Outposts para restringir el acceso a buckets específicos desde un punto de conexión de VPC específico. Con las políticas de punto de conexión de VPC, puede controlar el acceso a las API de administración de bucket y las API de administración de punto de conexión de S3 en Outposts. Con las políticas de bucket, puede controlar el acceso a las API de administración de bucket de S3 en Outposts. Sin embargo, no puede administrar el acceso a las acciones de objeto para S3 en Outposts mediante `aws:sourceVpce`.

Las políticas de acceso para S3 en Outposts especifican la siguiente información:

- La entidad principal de AWS Identity and Access Management (IAM) para la que se permiten o deniegan acciones.
- Las acciones de control de S3 permitidas o denegadas.
- Los recursos de S3 en Outposts en los cuales se permiten o deniegan acciones.

En los siguientes ejemplos se muestran políticas que restringen el acceso a un bucket o a un punto de conexión. Para obtener más información acerca de la conectividad de VPC, consulte Opciones de conectividad de red a VPC en el documento técnico de AWSOpciones de conectividad de Amazon Virtual Private Cloud.

> **Important**
>
> - Al aplicar las políticas de ejemplo de puntos de conexión de VPC descritos en esta sección, es posible que bloquee el acceso al bucket sin querer. Los permisos de bucket

que limitan el acceso del bucket a las conexiones procedentes del punto de conexión de VPC pueden bloquear todas las conexiones al bucket. Para obtener información acerca de cómo corregir este problema, consulte Mi política de bucket tiene una VPC o un ID de punto de conexión de la VPC incorrectos. ¿Cómo puedo corregir la política de modo que pueda tener acceso al bucket? en el Centro de conocimientos de Soporte.

- Antes de utilizar las siguientes políticas de bucket de ejemplo, sustituya el ID del punto de conexión de VPC por un valor adecuado para su caso de uso. De lo contrario, no podrá acceder a su bucket.
- Si la política solo permite acceder a un bucket de S3 en Outposts desde un punto de conexión de VPC específico, desactiva el acceso a la consola para ese bucket porque las solicitudes de consola no se originan en el punto de conexión de VPC especificado.

Temas



## Ejemplo: restringir el acceso a un bucket específico desde un punto de conexión de la VPC

Puede crear una política de punto de conexión que restrinja el acceso solo a buckets específicos de S3 en Outposts. La siguiente política restringe el acceso de la acción GetBucketPolicy solo a *example-outpost-bucket*. Para utilizar esta política, sustituya los valores de ejemplo por los suyos.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": {"AWS":"111122223333"},
      "Action": "s3-outposts:GetBucketPolicy",
      "Effect": "Allow",
      "Resource": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-
bucket"
    }
```

```
  ]
}
```

### Ejemplo: Denegación de acceso desde un punto de conexión de VPC específico en una política de bucket de S3 en Outposts

La siguiente política de bucket de S3 en Outposts niega el acceso a GetBucketPolicy en el bucket de *example-outpost-bucket* a través del punto de conexión de VPC *vpce-1a2b3c4d*.

La condición `aws:sourceVpce` especifica el punto de conexión y no requiere un nombre de recurso de Amazon (ARN) para el recurso de punto de conexión de VPC, solo el ID de punto de conexión. Para utilizar esta política, sustituya los valores de ejemplo por los suyos.

```
{
    "Version": "2012-10-17",
    "Id": "Policy1415115909152",
    "Statement": [
        {
            "Sid": "Deny-access-to-specific-VPCE",
            "Principal": {"AWS":"111122223333"},
            "Action": "s3-outposts:GetBucketPolicy",
            "Effect": "Deny",
            "Resource": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-
bucket",
            "Condition": {
                "StringEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}
            }
        }
    ]
}
```

## Claves de política de autenticación de AWS Signature Version 4 (SigV4)

En la siguiente tabla se muestran las claves de condición relacionadas con la autenticación de AWS Signature Version 4 (SigV4) que puede utilizar con Amazon S3 en Outposts. En una política de bucket, puede agregar estas condiciones para imponer un comportamiento específico cuando las

solicitudes se autentican mediante Signature Version 4. Para ver ejemplos de políticas, consulte Ejemplos de políticas de bucket que utilizan claves de condición relacionadas con Signature Version 4. Para obtener más información sobre las solicitudes de autenticación con Signature Version 4, consulte Autenticación de solicitudes (AWS Signature Version 4) en la Referencia de la API de Amazon Simple Storage Service

| Claves aplicables | Descripción |
| --- | --- |
| `s3-outposts:authType` | S3 en Outposts admite varios métodos de autenticación. Para restringir las solicitudes entrantes para que usen un método de autenticación específico, puede usar esta clave de condición opcional. Por ejemplo, puede utilizar esta clave de condición para permitir solo el encabezado `Authorization` de HTTP que se utilizará en la autenticación de solicitudes.<br><br>Valores válidos:<br><br>`REST-HEADER`<br><br>`REST-QUERY-STRING` |
| `s3-outposts:signatureAge` | El periodo, en milisegundos, que una firma es válida en una solicitud autenticada.<br><br>Esta condición solo funciona para las direcciones URL prefirmadas.<br><br>En Signature Version 4, la clave de firma es válida por un plazo máximo de siete días. Por lo tanto, las firmas también son válidas por un plazo máximo de siete días. Para obtener más información, consulte Introducción a la firma de solicitudes en la Referencia de la API de Amazon Simple Storage Service. Puede usar esta condición para limitar aún más la antigüedad de la firma.<br><br>Ejemplo de valor: `600000` |
| `s3-outposts:x-amz-content-sha256` | Puede utilizar esta clave de condición para no permitir el contenido sin firmar en su bucket.<br><br>Cuando se utiliza Signature Version 4, para las solicitudes que utilizan el encabezado `Authorization` , agregue el encabezado `x-amz-con` |

| Claves aplicables | Descripción |
| --- | --- |
| | `tent-sha256` en el cálculo de la firma y luego establezca su valor en la carga de hash.<br><br>Puede usar esta clave de condición en su política de bucket para denegar cualquier carga en la que las cargas no estén firmadas. Por ejemplo:<br><br>• Denegar las cargas que usen el encabezado `Authorization` para autenticar las solicitudes, pero no firmar la carga. Para obtener más información, consulte Transferencia de carga en un solo fragmento en la Referencia de la API de Amazon Simple Storage Service.<br>• Denegar las cargas que utilicen URL prefirmadas. Las URL prefirmad as siempre tienen una `UNSIGNED_PAYLOAD` . Para obtener más información, consulte Autenticación de solicitudes y Métodos de autenticación en la Referencia de la API de Amazon Simple Storage Service.<br><br>Valor válido: `UNSIGNED-PAYLOAD` |

## Ejemplos de políticas de bucket que utilizan claves de condición relacionadas con Signature Version 4

Para utilizar los siguientes ejemplos, reemplace los *`user input placeholders`* con su propia información.

Example : **`s3-outposts:signatureAge`**

La siguiente política de bucket deniega cualquier solicitud de URL prefirmada de S3 en Outposts en objetos en `example-outpost-bucket` si la firma tiene más de 10 minutos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Deny a presigned URL request if the signature is more than 10
 minutes old",
```

```
            "Effect": "Deny",
            "Principal": {"AWS":"444455556666"},
            "Action": "s3-outposts:*",
            "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
*",
            "Condition": {
                "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
                "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
            }
        }
    ]
}
```

Example : **`s3-outposts:authType`**

La siguiente política de bucket solo permite las solicitudes que utilizan el encabezado `Authorization` para solicitar autenticación. Se denegará cualquier solicitud de URL prefirmada, ya que las URL prefirmadas utilizan parámetros de consulta para proporcionar información de solicitud y autenticación. Para obtener más información, consulte Métodos de autenticación en la referencia de la API de Amazon Simple Storage Service.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
               "Sid": "Allow only requests that use the Authorization header for
 request authentication. Deny presigned URL requests.",
               "Effect": "Deny",
               "Principal": {"AWS":"111122223333"},
               "Action": "s3-outposts:*",
               "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
*",
               "Condition": {
                     "StringNotEquals": {
                           "s3-outposts:authType": "REST-HEADER"
                     }
               }
         }
   ]
}
```

Example : **`s3-outposts:x-amz-content-sha256`**

La siguiente política de bucket deniega cualquier carga con cargas sin firmar, como las cargas que utilizan URL prefirmadas. Para obtener más información, consulte Autenticación de solicitudes y Métodos de autenticación en la Referencia de la API de Amazon Simple Storage Service.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
               "Sid": "Deny uploads with unsigned payloads.",
               "Effect": "Deny",
               "Principal": {"AWS":"111122223333"},
               "Action": "s3-outposts:*",
               "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/object/
*",
               "Condition": {
                     "StringEquals": {
                           "s3-outposts:x-amz-content-sha256": "UNSIGNED-PAYLOAD"
                     }
               }
         }
   ]
}
```

# Políticas administradas de AWS para Amazon S3 en Outposts

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas de AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un

nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

### Política administrada de AWS: AWSS3OnOutpostsServiceRolePolicy

Le ayuda a administrar los recursos de la red como parte del rol vinculado al servicio `AWSServiceRoleForS3OnOutposts`.

Para consultar los permisos de esta política, consulte AWSS3OnOutpostsServiceRolePolicy.

### Actualizaciones de S3 en Outposts en las políticas administradas por AWS

Consulte los detalles sobre las actualizaciones de las políticas administradas por AWS para S3 en Outposts debido a que este servicio comenzó a realizar el seguimiento de estos cambios.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| S3 en Outposts agregado a `AWSS3OnOutpostsServiceRolePolicy` | S3 en Outposts agregado a `AWSS3OnOutpostsServiceRolePolicy` como parte de un rol vinculado a un servicio `AWSServiceRoleForS3OnOutposts`, que le ayuda a administrar los recursos de red. | 3 de octubre de 2023 |
| S3 en Outposts empezó a realizar un seguimiento de los cambios | S3 en Outposts comenzó un seguimiento de los cambios en las políticas administradas de AWS. | 3 de octubre de 2023 |

## Uso de roles vinculados a servicios para Amazon S3 en Outposts

Amazon S3 en Outposts utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado

directamente a S3 en Outposts. Los roles vinculados a servicios los predefine S3 en Outposts e incluyen todos los permisos que el servicio necesita para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de S3 en Outposts porque ya no tendrá que agregar manualmente los permisos necesarios. S3 en Outposts define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo S3 en Outposts puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de S3 en Outposts, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Permisos de roles vinculados a servicios para S3 en Outposts

S3 en Outposts usa el rol vinculado a un servicio denominado AWSServiceRoleForS3OnOutposts para ayudarle a administrar los recursos de la red.

El rol vinculado al servicio `AWSServiceRoleForS3OnOutposts` depende de los siguientes servicios para asumir el rol:

- `s3-outposts.amazonaws.com`

La política de permisos de roles llamada `AWSS3OnOutpostsServiceRolePolicy` permite que S3 en Outposts complete las siguientes acciones en los recursos especificados:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
```

```
                "ec2:DescribeCoipPools",
                "ec2:GetCoipPoolUsage",
                "ec2:DescribeAddresses",
                "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
            ],
            "Resource": "*",
            "Sid": "DescribeVpcResources"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ],
            "Sid": "CreateNetworkInterface"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "CreateTagsForCreateNetworkInterface"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:ipv4pool-ec2/*"
            ],
            "Sid": "AllocateIpAddress"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:elastic-ip/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "CreateTagsForAllocateIpAddress"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DisassociateAddress",
                "ec2:ReleaseAddress",
                "ec2:AssociateAddress"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/CreatedBy": "S3 On Outposts"
                }
            },
            "Sid": "ReleaseVpcResources"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateNetworkInterface",
```

```
                        "AllocateAddress"
                    ],
                    "aws:RequestTag/CreatedBy": [
                        "S3 On Outposts"
                    ]
                }
            },
            "Sid": "CreateTags"
        }
    ]
}
```

Debe configurar permisos para permitir a una entidad de IAM (como un rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

## Creación de un rol vinculado a un servicio para S3 en Outposts

No necesita crear manualmente un rol vinculado a servicios. Cuando crea un punto de conexión de S3 en Outposts en la AWS Management Console, la AWS CLI o la API de AWS, S3 en Outposts crea un rol vinculado a un servicio para usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea un punto de conexión de S3 en Outposts, S3 en Outposts crea el rol vinculado a un servicio para usted de nuevo.

También puede utilizar la consola de IAM para crear un rol vinculado a un servicio con el caso de uso de S3 en Outposts. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `s3-outposts.amazonaws.com`. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

## Edición de un rol vinculado a un servicio para S3 en Outposts

S3 en Outposts no le permite editar el rol vinculado a servicios `AWSServiceRoleForS3OnOutposts`. Esto incluye el nombre del rol porque es posible que varias entidades hagan referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

## Eliminación de un rol vinculado a un servicio para S3 en Outposts

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de S3 en Outposts utiliza el rol cuando intenta eliminar los recursos, es posible que la eliminación produzca un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de S3 en Outposts utilizados por el rol AWSServiceRoleForS3OnOutposts

1. Elimine los puntos de conexión de S3 en Outposts de la Cuenta de AWS en todas las Regiones de AWS.
2. Elimine el rol vinculado a servicios con IAM.

   Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio de `AWSServiceRoleForS3OnOutposts`. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

## Regiones admitidas para roles vinculados a servicios de S3 en Outposts

S3 en Outposts admite el uso de roles vinculados a servicios en todas las Regiones de AWS en las que el servicio esté disponible. Para obtener más información, consulte Regiones y puntos de conexión de S3 en Outposts.

# Administración de almacenamiento de S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (`OUTPOSTS`), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

Para obtener más información sobre cómo administrar y compartir la capacidad de almacenamiento de Amazon S3 en Outposts, consulte los siguientes temas.

Temas



# Administración de control de versiones de S3 para su bucket de S3 en Outposts

Cuando está habilitado, el control de versiones de S3 guarda diversas copias de un objeto en el mismo bucket. Puede utilizar el control de versiones de S3 para conservar, recuperar y restaurar todas las versiones de los objetos almacenados en su bucket de Outposts. EL control de versiones de S3 ayuda a recuperarse de acciones no deseadas del usuario y de errores de la aplicación.

Los buckets de Amazon S3 en Outposts tienen tres estados de versiones:

- Unversioned (Sin control de versiones): si nunca ha habilitado o suspendido el control de versiones de S3 en su bucket, no tiene versiones y no muestra ningún estado de control de versiones de S3. Para obtener más información sobre el control de versiones de S3, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.
- Enabled (Habilitado): habilita el control de versiones de S3 para los objetos del bucket. Todos los objetos añadidos al bucket reciben un ID de versión único. Los objetos que ya existían en el bucket en el momento en que habilita el control de versiones tienen un ID de versión de `null`. Si modifica estos objetos (o cualquier otro) con otras operaciones, como PutObject, los objetos nuevos obtienen un ID de versión único.
- Suspended (Suspendido): suspende el control de versiones de S3 para los objetos del bucket. Todos los objetos añadidos al bucket tras la suspensión del control de versiones reciben el ID de versión `null`. Para obtener más información, consulte Agregar objetos a buckets con control de versiones suspendido en la Guía del usuario de Amazon S3.

Después de habilitar el control de versiones de S3 para un bucket de S3 en Outposts, nunca puede volver a un estado sin versiones. Sin embargo, puede suspender el control de versiones. Para obtener más información sobre el control de versiones de S3, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.

Para cada objeto de su bucket, tiene una versión actual y cero o más versiones no actuales. Para reducir los costes de almacenamiento, puede configurar las reglas del ciclo de vida de su bucket S3 para que caduquen las versiones no actuales después de un período de tiempo específico. Para obtener más información, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.

En los siguientes ejemplos se muestra cómo habilitar o suspender el control de versiones para un bucket S3 on Outposts existente utilizando la AWS Management Console y la AWS Command Line Interface (AWS CLI). Para crear un bucket con el control de versiones de S3 activado, consulte Creación de un bucket de S3 en Outposts.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede confirmarle acciones. Los buckets tienen propiedades de configuración como Outpost, etiquetas, cifrado predeterminado y valores de puntos de acceso. La configuración de punto de acceso incluye la VPC (nube virtual privada) y la política de punto de acceso para acceder a los objetos del

bucket y otros metadatos. Para obtener más información, consulte Especificaciones de S3 en Outposts.

## Uso de la consola de S3

Para editar la configuración de control de versiones de S3 para su bucket

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación izquierdo, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts para el que desea habilitar el control de versiones de S3.
4. Elija la pestaña Properties (Propiedades).
5. En Bucket Versioning (Versiones del bucket), elija Edit (Editar).
6. Edite la configuración del control de versiones de S3 para el bucket, eligiendo una de las siguientes opciones:
   - Para suspender el control de versiones de S3 y detener la creación de nuevas versiones de objetos, elija Suspend (Suspender).
   - Para habilitar el control de versiones de S3 y guardar varias copias distintas de cada objeto, elija Enable (Habilitar).
7. Elija Save changes (Guardar cambios).

## Uso de la AWS CLI

Para habilitar o suspender el control de versiones de S3 para su bucket mediante la AWS CLI, utilice el comando `put-bucket-versioning`, como se muestra en los siguientes ejemplos. Para utilizar estos ejemplos, sustituya *`user input placeholder`* por su propia información.

Para obtener más información, consulte put-bucket-versioning en la AWS CLIReferencia de .

Example : para habilitar el control de versiones de S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --versioning-configuration Status=Enabled
```

Example : para suspender el control de versiones de S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --versioning-configuration Status=Suspended
```

# Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts

Puede usar el ciclo de vida de S3 para optimizar la capacidad de almacenamiento para Amazon S3 en Outposts. Puede crear reglas de ciclo de vida para hacer vencer los objetos a medida que envejecen o se sustituyan por versiones más recientes. Puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para obtener más información acerca de S3 Lifecycle, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para crear y administrar la configuración del ciclo de vida del bucket de S3 en Outposts, consulte los siguientes temas.

Temas

- Creación y administración de una regla de ciclo de vida con la AWS Management Console
- Creación y administración de una configuración de ciclo de vida mediante la AWS CLI y el SDK para Java

## Creación y administración de una regla de ciclo de vida con la AWS Management Console

Puede usar el ciclo de vida de S3 para optimizar la capacidad de almacenamiento para Amazon S3 en Outposts. Puede crear reglas de ciclo de vida para hacer vencer los objetos a medida que

envejecen o se sustituyan por versiones más recientes. Puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para obtener más información acerca de S3 Lifecycle, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para crear y administrar una regla de ciclo de vida para un S3 en Outposts utilizando la AWS Management Console, consulte los siguientes temas.

Temas

- Creación de una regla de ciclo de vida
- Habilitar una regla de ciclo de vida
- Edición de una regla de ciclo de vida
- Eliminación de una regla de ciclo de vida

## Creación de una regla de ciclo de vida

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación izquierdo, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts para el que desea crear una regla del ciclo de vida.
4. Seleccione la pestaña Management (Administración) y seleccione Create Lifecycle rule (Crear regla de ciclo de vida).
5. Introduzca un valor para Lifecycle rule name (Nombre de regla de ciclo de vida).
6. En Rule scope (Ámbito de rol), elija una de las siguientes opciones:

   - Para limitar el alcance para filtros específicos, elija Limit the scope of this rule using one or more filters (Limitar el alcance de esta regla con uno o más filtros). A continuación, agregue un filtro de prefijo, etiquetas o tamaño del objeto.

- Para aplicar la regla a todos los objetos del bucket, elija Apply to all objects in the bucket (Aplicar a todos los objetos del bucket).

7. En Lifecycle rule actions (Acciones de regla de ciclo de vida), elija una de las siguientes opciones:

   - Expire current versions of objects (Expirar las versiones actuales de objetos): para los buckets habilitados para el control de versiones, S3 en Outposts agrega un marcador de eliminación y retiene los objetos como versiones no actuales. Para los buckets que no utilizan el control de versiones de S3, S3 en Outposts elimina permanentemente los objetos.
   - Permanently delete noncurrent versions of objects (Eliminar permanentemente las versiones no actuales de los objetos): S3 en Outposts elimina permanentemente las versiones no actuales de los objetos.
   - Delete expired object delete markers or incomplete multipart uploads (Eliminar marcadores de eliminación de objetos vencidos o cargas multiparte incompletas): S3 en Outposts elimina permanentemente los marcadores de eliminación de objetos vencidos o cargas multiparte incompletas.

     Si limita el ámbito de su regla de ciclo de vida mediante etiquetas de objetos, no puede elegir Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados). Tampoco puede elegir Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados) si elige Expire current object versions (Expirar las versiones actuales de objetos).

   > **Note**
   >
   > Los filtros basados en el tamaño no se pueden usar con marcadores de eliminación ni con cargas multiparte incompletas.

8. Si seleccionó Expire current versions of objects (Expirar las versiones actuales de los objetos) o Permanently delete noncurrent versions of objects (Eliminar permanentemente las versiones no actuales de los objetos), configure el desencadenador de la regla en función de una fecha específica o de la antigüedad del objeto.
9. Si eligió Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados), para confirmar que desea eliminar los marcadores de eliminación de objetos caducados, seleccione Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados).

10. En Timeline Summary (Resumen de línea temporal), revise su regla de ciclo de vida y seleccione Create rule (Crear regla).

## Habilitar una regla de ciclo de vida

Para habilitar o deshabilitar una regla del ciclo de vida del bucket

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts para el que desea habilitar o deshabilitar una regla del ciclo de vida.
4. Elija la pestaña Management (Administración) y a continuación en Lifecycle rule (Regla de ciclo de vida), elija la regla que desea habilitar o deshabilitar.
5. En Action (Acción), elija Enable or disable rule (Habilitar o deshabilitar regla).

## Edición de una regla de ciclo de vida

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts para el que desea editar una regla del ciclo de vida.
4. Elija la pestaña Management (Administración) y elija la regla del ciclo de vida que desea editar.
5. (opcional) Actualice el valor de Lifecycle rule name (Nombre de la regla del ciclo de vida).
6. En Rule scope (Ámbito de regla), modifique el ámbito según sea necesario:

   - Para limitar el alcance para filtros específicos, elija Limit the scope of this rule using one or more filters (Limitar el alcance de esta regla con uno o más filtros). A continuación, agregue un filtro de prefijo, etiquetas o tamaño del objeto.
   - Para aplicar la regla a todos los objetos del bucket, elija Apply to all objects in the bucket (Aplicar a todos los objetos del bucket).

7. En Lifecycle rule actions (Acciones de regla de ciclo de vida), elija una de las siguientes opciones:

   - Expire current versions of objects (Expirar las versiones actuales de objetos): para los buckets habilitados para el control de versiones, S3 en Outposts agrega un marcador de eliminación y retiene los objetos como versiones no actuales. Para los buckets que no utilizan el control de versiones de S3, S3 en Outposts elimina permanentemente los objetos.

- Permanently delete noncurrent versions of objects (Eliminar permanentemente las versiones no actuales de los objetos): S3 en Outposts elimina permanentemente las versiones no actuales de los objetos.
- Delete expired object delete markers or incomplete multipart uploads (Eliminar marcadores de eliminación de objetos vencidos o cargas multiparte incompletas): S3 en Outposts elimina permanentemente los marcadores de eliminación de objetos vencidos o cargas multiparte incompletas.

  Si limita el ámbito de su regla de ciclo de vida mediante etiquetas de objetos, no puede elegir Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados). Tampoco puede elegir Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados) si elige Expire current object versions (Expirar las versiones actuales de objetos).

> **Note**
>
> Los filtros basados en el tamaño no se pueden usar con marcadores de eliminación ni con cargas multiparte incompletas.

8. Si seleccionó Expirar las versiones actuales de los objetos o Eliminar permanentemente las versiones no actuales de los objetos, configure el desencadenador de la regla en función de una fecha específica o de la antigüedad del objeto.
9. Si eligió Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados), para confirmar que desea eliminar los marcadores de eliminación de objetos caducados, seleccione Delete expired object delete markers (Eliminar marcadores de eliminación de objetos caducados).
10. Seleccione Save (Guardar).

## Eliminación de una regla de ciclo de vida

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación de la izquierda, elija Outposts buckets (Buckets de Outposts).
3. Elija el bucket de Outposts para el que desea eliminar una regla de estilo de vida.
4. Elija la pestaña Management (Administración) y luego en Lifecycle rule (Regla de ciclo de vida), elija la regla que desea eliminar.

5. Elija Eliminar.

## Creación y administración de una configuración de ciclo de vida mediante la AWS CLI y el SDK para Java

Puede usar el ciclo de vida de S3 para optimizar la capacidad de almacenamiento para Amazon S3 en Outposts. Puede crear reglas de ciclo de vida para hacer vencer los objetos a medida que envejecen o se sustituyan por versiones más recientes. Puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para obtener más información acerca de S3 Lifecycle, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede crear, habilitar, deshabilitar o eliminar una regla de ciclo de vida.

Para crear y administrar una configuración de ciclo de vida para un bucket de S3 en Outposts mediante AWS Command Line Interface (AWS CLI) y AWS SDK para Java, consulte los siguientes ejemplos.

Temas

- Colocación de una configuración del ciclo de vida
- Obtención de la configuración de ciclo de vida en un bucket de S3 en Outposts

### Colocación de una configuración del ciclo de vida

AWS CLI

En el siguiente ejemplo de AWS CLI, se aplica una política de configuración del ciclo de vida en un bucket de Outposts. Esta política especifica que todos los objetos que tienen el prefijo marcado (*myprefix*) y las etiquetas vencen después de 10 días. Para utilizar este ejemplo, sustituya *user input placeholder* por su propia información.

1. Guarde la política de configuración del ciclo de vida en un archivo JSON. En este ejemplo, el archivo se denomina `lifecycle1.json`.

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ],
                    "ObjectSizeGreaterThan": 1000,
                    "ObjectSizeLessThan": 5000
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 10
            }
        }
    ]
}
```

2. Envíe el archivo JSON como parte del comando de la CLI `put-bucket-lifecycle-configuration`. Para usar este comando, sustituya *`user input placeholder`* por su propia información. Para obtener más información acerca de este comando, consulte [put-bucket-lifecycle-configuration] en la Referencia de AWS CLI.

```
aws s3control put-bucket-lifecycle-configuration --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket --lifecycle-configuration file://lifecycle1.json
```

SDK for Java

En el siguiente ejemplo del SDK para Java, se aplica una configuración del ciclo de vida en un bucket de Outposts. Esta configuración de ciclo de vida especifica que todos los objetos que tienen el prefijo marcado (*myprefix*) y las etiquetas vencen después de 10 días. Para utilizar este ejemplo, sustituya *user input placeholder* por su propia información. Para obtener más información, consulte PutBucketLifecycleConfiguration en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketLifecycleConfiguration(String bucketArn) {

    S3Tag tag1 = new S3Tag().withKey("mytagkey1").withValue("mytagkey1");
    S3Tag tag2 = new S3Tag().withKey("mytagkey2").withValue("mytagkey2");

    LifecycleRuleFilter lifecycleRuleFilter = new LifecycleRuleFilter()
            .withAnd(new LifecycleRuleAndOperator()
                    .withPrefix("myprefix")
                    .withTags(tag1, tag2))
                    .withObjectSizeGreaterThan(1000)
                    .withObjectSizeLessThan(5000);

    LifecycleExpiration lifecycleExpiration = new LifecycleExpiration()
            .withExpiredObjectDeleteMarker(false)
            .withDays(10);

    LifecycleRule lifecycleRule = new LifecycleRule()
            .withStatus("Enabled")
            .withFilter(lifecycleRuleFilter)
            .withExpiration(lifecycleExpiration)
            .withID("id-1");

    LifecycleConfiguration lifecycleConfiguration = new LifecycleConfiguration()
            .withRules(lifecycleRule);

    PutBucketLifecycleConfigurationRequest reqPutBucketLifecycle = new
 PutBucketLifecycleConfigurationRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn)
            .withLifecycleConfiguration(lifecycleConfiguration);
```

```
    PutBucketLifecycleConfigurationResult respPutBucketLifecycle =
 s3ControlClient.putBucketLifecycleConfiguration(reqPutBucketLifecycle);
    System.out.printf("PutBucketLifecycleConfiguration Response: %s%n",
 respPutBucketLifecycle.toString());

}
```

## Obtención de la configuración de ciclo de vida en un bucket de S3 en Outposts

### AWS CLI

En el siguiente ejemplo de la AWS CLI, se obtiene una configuración del ciclo de vida en un bucket de Outposts. Para usar este comando, sustituya *user input placeholder* por su propia información. Para obtener más información acerca de este comando, consulte get-bucket-lifecycle-configuration en la Referencia de AWS CLI.

```
aws s3control get-bucket-lifecycle-configuration --account-id 123456789012 --bucket
 arn:aws:s3-outposts:<your-region>:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket
```

### SDK for Java

En el siguiente ejemplo del SDK para Java, se obtiene una configuración del ciclo de vida para un bucket de Outposts. Para obtener más información, consulte GetBucketLifecycleConfiguration en la Referencia de la API de Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketLifecycleConfiguration(String bucketArn) {

    GetBucketLifecycleConfigurationRequest reqGetBucketLifecycle = new
 GetBucketLifecycleConfigurationRequest()
            .withAccountId(AccountId)
            .withBucket(bucketArn);

    GetBucketLifecycleConfigurationResult respGetBucketLifecycle =
 s3ControlClient.getBucketLifecycleConfiguration(reqGetBucketLifecycle);
    System.out.printf("GetBucketLifecycleConfiguration Response: %s%n",
 respGetBucketLifecycle.toString());

}
```

# Replicación de objetos para S3 en Outposts

Si tiene S3 Replication activado en AWS Outposts, puede configurar Amazon S3 en Outposts para que replique automáticamente objetos de S3 en diferentes Outposts o entre buckets del mismo Outpost. Puede utilizar S3 Replication en Outposts para conservar varias réplicas de sus datos en el mismo o en diferentes Outposts, a fin de cumplir con las necesidades de residencia de datos. S3 Replication en Outposts ayuda a satisfacer sus necesidades de almacenamiento compatibles y al intercambio de datos entre cuentas. Si necesita asegurarse de que las réplicas de los objetos sean idénticos a los datos de origen, puede usar S3 Replication en Outposts para realizar réplicas de sus objetos para conservar todos los metadatos, como la hora de creación del objeto original, las etiquetas y los ID de versión.

S3 Replication en Outposts también proporciona métricas detalladas y notificaciones para monitorear el estado de la replicación de objetos entre buckets. Puede utilizar Amazon CloudWatch para monitorear el progreso de la replicación mediante el seguimiento de los bytes pendientes de replicación, las operaciones pendientes de replicación y la latencia de replicación entre los buckets de origen y de destino. Para diagnosticar y corregir rápidamente los problemas de configuración, también puede configurar Amazon EventBridge para que reciba notificaciones sobre errores en los objetos de replicación. Para obtener más información, consulte Administración de la replicación.

Temas



## Configuración de replicación

S3 en Outposts almacena una configuración de replicación como XML. En el archivo XML de configuración de reproducción, usted especifica un rol de AWS Identity and Access Management (IAM) y una o más reglas.

```
<ReplicationConfiguration>
```

```
    <Role>IAM-role-ARN</Role>
    <Rule>
        ...
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
</ReplicationConfiguration>
```

S3 en Outposts no puede replicar objetos sin su permiso. Usted otorga permisos a S3 en Outposts con el rol de IAM que especifique en la configuración de la replicación. S3 en Outposts asume el rol de IAM para replicar objetos en su nombre. Debe conceder los permisos necesarios para el rol de IAM para que pueda empezar a replicar. Para obtener más información sobre estos permisos para S3 en Outposts, consulte Creación de un rol de IAM.

Usted agrega una regla en una configuración de replicación en los siguientes casos:

- Desea replicar todos los objetos.
- Desea replicar un subconjunto de objetos. Identifica el subconjunto de objetos añadiendo un filtro en la regla. En el filtro, usted especifica un prefijo de clave de objeto, etiquetas o una combinación de ambos, para identificar el subconjunto de objetos a los que se aplica la regla.

Agrega varias reglas en una configuración de replicación si desea replicar un subconjunto diferente de objetos. En cada regla, se especifica un filtro que selecciona un subconjunto diferente de objetos. Por ejemplo, puede elegir replicar objetos que tengan los prefijos de clave `tax/` o `document/`. Para ello, agregue dos reglas, una que especifique el filtro de prefijo de clave `tax/` y otro que especifique el prefijo de clave `document/`.

Para obtener más información sobre la configuración de replicación y las reglas de replicación de S3 en Outposts, consulte ReplicationConfiguration en la referencia de la API de Amazon Simple Storage Service.

## Requisitos de S3 Replication en Outposts

La replicación requiere lo siguiente:

- El rango CIDR de Outpost de destino debe estar asociado a la tabla de subredes de Outpost de origen. Para obtener más información, consulte Requisitos previos para crear reglas de replicación.

- Ambos buckets de origen y destino deben tener activado el control de versiones de S3. Para obtener más información sobre el control de versiones, consulte Administración de control de versiones de S3 para su bucket de S3 en Outposts.
- Amazon S3 en Outposts debe tener permisos para replicar objetos en su nombre del bucket de origen en el bucket de destino. Esto significa que debe crear un rol de servicio para delegar los permisos `GET` y `PUT` a S3 en Outposts.
  1. Antes de crear el rol de servicio, debe tener el permiso `GET` en el bucket de origen y el permiso `PUT` en el bucket de destino.
  2. Para crear el rol de servicio para delegar los permisos a S3 en Outposts, primero debe configurar los permisos para permitir que una entidad de IAM (un usuario o un rol) realice las acciones `iam:CreateRole` y `iam:PassRole`. A continuación, permite que una entidad de IAM cree el rol de servicio. Para que S3 en Outposts asuma el rol de servicio en su nombre y delegue los permisos `GET` y `PUT` a S3 en Outposts, debe asignar las políticas de confianza y de permisos necesarias al rol. Para obtener más información sobre estos permisos para S3 en Outposts, consulte Creación de un rol de IAM. Para obtener más información sobre cómo crear un rol de servicio, consulte Creación de un rol de servicio.

## ¿Qué se replica?

De forma predeterminada, S3 en Outposts replica lo siguiente:

- Objetos creados después de añadir una configuración de replicación.
- Metadatos de objeto desde los objetos de origen hasta las réplicas. Para obtener información acerca de la replicación de metadatos a partir de las réplicas de los objetos de origen, consulte Estado de replicación si la sincronización de modificación de réplica de Amazon S3 en Outposts está habilitada.
- Etiquetas de objeto, si las hay.

### Cómo afectan las operaciones de eliminación a la replicación

Si elimina un objeto del bucket de origen, las siguientes acciones se producen de forma predeterminada:

- Si realiza una solicitud `DELETE` sin especificar un ID de versión del objeto, S3 en Outposts añade un marcador de eliminación. S3 en Outposts se ocupa del marcador de eliminación de la siguiente manera:

  - S3 en Outposts no replica el marcador de eliminación de forma predeterminada.
  - Sin embargo, puede agregar la replicación de marcador de eliminación a reglas no basadas en etiquetas. Para obtener más información acerca de cómo habilitar la replicación del marcador de eliminación en su configuración de replicación, consulte Uso de la consola de S3.
- Si especifica un ID de versión de objeto para eliminar en una solicitud de `DELETE`, S3 en Outposts elimina esa versión del objeto en el bucket de origen de forma permanente. Sin embargo, no replica la eliminación en los buckets de destino. En otras palabras, no elimina la misma versión del objeto de los buckets de destino. Este comportamiento protege los datos de eliminaciones malintencionadas.

## Elementos que no se replican

De forma predeterminada, S3 en Outposts no replica lo siguiente:

- Los objetos en el bucket de origen que son réplicas, creadas por otra regla de replicación. Por ejemplo, imagine que configura la replicación donde el bucket A es el origen y el bucket B es el destino. Ahora, supongamos que añade otra configuración de replicación donde el bucket B es el de origen y el bucket C es el de destino. En este caso, los objetos en el bucket B que son réplicas de objetos en el bucket A no se replican en el bucket C.
- Objetos en el bucket de origen que ya se han replicado en un destino diferente. Por ejemplo, si cambia el bucket de destino en una configuración de replicación existente, S3 en Outposts no replicará los objetos de nuevo.
- Objetos creados con cifrado del lado del servidor con claves de cifrado proporcionadas por los clientes (SSE-C).
- Actualiza a subrecursos de bucket.

  Por ejemplo, si cambia la configuración del ciclo de vida en una configuración de notificación al bucket de origen, estos cambios no se aplican al bucket de destino. Esta característica permite tener diferentes configuraciones en los buckets de origen y destino.
- Acciones realizadas por la configuración del ciclo de vida.

  Por ejemplo, si activa la configuración del ciclo de vida en el bucket de origen y configura acciones de vencimiento, S3 en Outposts crea marcadores de eliminación para los objetos vencidos en el bucket de origen, pero no replica esos marcadores en los buckets de destino. Si desea que se aplique la misma configuración de ciclo de vida a los buckets de origen y destino, habilite la misma configuración de ciclo de vida en ambos. Para obtener más información acerca de la configuración

del ciclo de vida, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.

## ¿Qué no admite S3 Replication en Outposts?

Las siguientes características de S3 Replication no son compatibles actualmente con S3 en Outposts:

- Control del tiempo de replicación de S3 (S3 RTC) S3 RTC no es compatible porque el tráfico de objetos en S3 Replication en Outposts viaja a través de la red en las instalaciones (la puerta de enlace local). Para obtener más información acerca de las puerta de enlace locales, consulte el temas sobre trabajar con gateways locales en la guía del usuario de AWS Outposts.
- S3 Replication para operaciones por lotes.

## Configuración de la replicación

> **Note**
>
> Los objetos que había en el bucket antes de configurar la regla de replicación no se replican automáticamente. En otras palabras, Amazon S3 en Outposts no replica los objetos retroactivamente. Para replicar objetos creados antes de que configurara la replicación, puede utilizar la operación de la API `CopyObject` para copiarlos en el mismo bucket. Una vez copiados los objetos, aparecen como objetos «nuevos» en el bucket y se les aplica la configuración de replicación. Para obtener más información sobre cómo se copia un objeto, consulte Copia de un objeto en un bucket de Amazon S3 en Outposts utilizando AWS SDK para Java y CopyObject en la Referencia de la API de Amazon Simple Storage Service.

Para activar la Replicación de S3 en Outposts, añada una regla de replicación a su bucket de Outposts de origen. La regla de replicación indica a S3 en Outposts que replique los objetos de la forma especificada. En la configuración de replicación, debe proporcionar lo siguiente:

- El punto de acceso al bucket de Outposts de origen: el nombre de recurso de Amazon (ARN) o el alias del punto de acceso desde el que desea que S3 en Outposts replique los objetos. Para obtener más información, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

- Los objetos que desea replicar: puede replicar todos los objetos del bucket de Outposts de origen o de un subconjunto. Para identificar un subconjunto, proporcione un prefijo de nombre de clave, una o más etiquetas de objeto, o ambos en la configuración.

  Por ejemplo, si configura una regla de replicación para replicar solo objetos con el prefijo de nombre de clave `Tax/`, S3 en Outposts replica objetos con claves como `Tax/doc1` o `Tax/doc2`. Pero no replica objetos con la clave `Legal/doc3`. Si especifica un prefijo y una o más etiquetas, S3 en Outposts replica solo los objetos que tienen el prefijo de clave específico y las etiquetas.
- El bucket de Outposts de destino: el ARN o el alias del punto de acceso del bucket en el que desea que S3 en Outposts replique los objetos.

Puede configurar la regla de replicación mediante la API de REST, los SDK de AWS, la AWS Command Line Interface (AWS CLI) o la consola de Amazon S3.

S3 en Outposts también proporciona operaciones de API para que admita la configuración de reglas de replicación. Para obtener más información, consulte los siguientes temas en la referencia de la API de Amazon Simple Storage Service:

- PutBucketReplication
- GetBucketReplication
- DeleteBucketReplication

Temas

- Requisitos previos para crear reglas de replicación
- Creación de reglas de replicación en Outposts

## Requisitos previos para crear reglas de replicación

Temas

- Conectar las subredes de Outpost de origen y destino
- Creación de un rol de IAM

### Conectar las subredes de Outpost de origen y destino

Para que el tráfico de replicación vaya de su Outpost de origen a su Outpost de destino a través de la puerta de enlace local, debe agregar una nueva ruta para configurar la red. Debe conectar entre sí los rangos de red del enrutamiento entre dominios sin clases (CIDR) de sus puntos de acceso. Para cada par de puntos de acceso, debe configurar esta conexión solo una vez.

Algunos pasos para configurar la conexión varían según el tipo de acceso de los puntos de conexión de Outposts que estén asociados a sus puntos de acceso. El tipo de acceso para los puntos de conexión es Privado (enrutamiento directo a la nube privada virtual [VPC] para AWS Outposts) o IP propiedad del cliente (un grupo de direcciones IP propiedad del cliente [grupo CoIP] dentro de la red en las instalaciones).

#### Paso 1: Encontrar el rango de CIDR de su punto de conexión de Outposts de origen

Para encontrar el rango de CIDR de su punto de conexión de origen asociado a su punto de acceso de origen

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación izquierdo, elija Outposts buckets (Buckets de Outposts).
3. En la lista Buscar buckets de Outposts, elija el bucket de origen que desea replicar.
4. Elija la pestaña Puntos de acceso de Outposts y elija el punto de acceso de Outposts para el bucket de origen de su regla de replicación.
5. Seleccione el punto de conexión de Outposts.
6. Copie el ID de subred para usarlo en el paso 5.
7. El método que utilice para encontrar el rango de CIDR del punto de conexión de Outposts de origen depende del tipo de acceso de su punto de conexión.

   En la sección Información general sobre los puntos de enlace de Outposts, consulte Tipo de acceso.

   - Si el tipo de acceso es Privado, copie el valor del Enrutamiento entre dominios sin clases (CIDR) para usarlo en el paso 6.
   - Si el tipo de acceso es IP propiedad del cliente, haga lo siguiente:
     1. Copie el valor del grupo IPv4 propiedad del cliente para usarlo más adelante como ID del grupo de direcciones.

2. Abra la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.
3. En el panel de navegación, elija Tablas de enrutamiento de puerta de enlace de tránsito.
4. Elija el valor de ID de tabla de enrutamiento de puerta de enlace en las instalaciones del Outpost de origen.
5. En el panel de detalles, elija la pestaña Grupos de CoIP. Pegue el valor de su ID de grupo de CoIP copiado anteriormente en el cuadro de búsqueda.
6. Para el grupo de CoIP coincidente, copie el valor de CIDR correspondiente de su punto de conexión de Outposts de origen para usarlo en el paso 6.

Paso 2: Buscar el ID de subred y el rango de CIDR de su punto de conexión de Outposts de destino

Para encontrar el ID de subred y el rango de CIDR de su punto de conexión de destino asociados a su punto de acceso de destino, siga los mismos subpasos del paso 1 y cambie el punto de conexión de Outposts de origen por el punto de conexión de Outposts de destino cuando aplique esos subpasos. Copie el valor del ID de subred del punto de conexión de Outposts de destino para usarlo en el paso 6. Copie el valor de CIDR del punto de conexión de Outposts de destino para usarlo en el paso 5.

Paso 3: Encontrar el ID de puerta de enlace local del Outpost de origen

Para encontrar el ID de puerta de enlace local del Outpost de origen

1. Abra la consola de AWS Outposts en https://console.aws.amazon.com/outposts/.
2. En el panel de navegación izquierdo, elija Gateways locales.
3. En la página Gateways locales, busque el ID de Outpost del Outpost de origen que quiere utilizar para la replicación.
4. Copie el valor del ID de puerta de enlace local del Outpost de origen para usarlo en el paso 5.

Para obtener información acerca de las puerta de enlaces locales, consulte el tema sobre Gateways locales en la Guía del usuario de AWS Outposts.

Paso 4: Encontrar el ID de puerta de enlace local del Outpost de destino

Para encontrar el ID de puerta de enlace local del Outpost de destino, siga los mismos subpasos del paso 3, excepto buscar el ID de Outpost del Outpost de destino. Copie el valor del ID de puerta de enlace local del Outpost de destino para usarlo en el paso 6.

### Paso 5: Configurar la conexión desde la subred de Outpost de origen a la subred de Outpost de destino

Para conectarse desde la subred de Outpost de origen a la subred de Outpost de destino

1. Inicie sesión en la AWS Management Console y abra la consola de VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Subnets.
3. En el cuadro de búsqueda, introduzca el ID de subred del punto de conexión de Outposts de origen que ha encontrado en el paso 1. Elija una subred con el ID de subred correspondiente.
4. Para el elemento de subred coincidente, elija el valor de Tabla de enrutamiento de esta subred.
5. En la página con una tabla de enrutamiento seleccionada, elija Acciones y, a continuación, elija Editar rutas.
6. En la pestaña Editar rutas, elija Añadir rutas.
7. En Destino, introduce el rango de CIDR del punto de conexión de Outposts de destino que encontraste en el paso 2.
8. En Objetivo, elija Gateway local de Outpost e introduzca el ID de puerta de enlace local de su Outpost de origen que ha encontrado en el paso 3.
9. Elija Guardar cambios.
10. Asegúrese de que el Estado de la ruta sea Activo.

### Paso 6: Configurar la conexión desde la subred de Outpost de destino a la subred de Outpost de origen

1. Inicie sesión en la AWS Management Console y abra la consola de VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Subnets.
3. En el cuadro de búsqueda, introduzca el ID de subred del punto de conexión de Outposts de destino que ha encontrado en el paso 2. Elija una subred con el ID de subred correspondiente.
4. Para el elemento de subred coincidente, elija el valor de Tabla de enrutamiento de esta subred.
5. En la página con una tabla de enrutamiento seleccionada, elija Acciones y, a continuación, elija Editar rutas.
6. En la pestaña Editar rutas, elija Añadir rutas.

7. En Destino, introduzca el rango de CIDR del punto de conexión de Outposts de origen que ha encontrado en el paso 1.
8. En Objetivo, elija Gateway local de Outpost e introduzca el ID de puerta de enlace local del Outpost de destino que ha encontrado en el paso 4.
9. Elija Guardar cambios.
10. Asegúrese de que el Estado de la ruta sea Activo.

Después de conectar los rangos de redes de CIDR de sus puntos de acceso de origen y destino, debe crear un rol de AWS Identity and Access Management (IAM).

Creación de un rol de IAM

De forma predeterminada, todos los recursos de S3 en Outposts (buckets, objetos y subrecursos relacionados) son privados y solo el propietario del recurso puede acceder a él. S3 en Outposts necesita permisos de lectura y replicación de objetos del bucket de Outposts de origen. Para conceder estos permisos, crea un rol de servicio de IAM y luego especifique ese rol en la configuración de replicación.

En esta sección se explica la política de confianza y la política de permisos mínimos necesarios. Los tutoriales de ejemplo proporcionan instrucciones paso a paso para crear un rol de IAM. Para obtener más información, consulte Creación de reglas de replicación en Outposts. Para obtener más información acerca de los roles de IAM, consulte Roles de IAM en Guía del usuario de IAM.

- En el siguiente ejemplo, se muestra una política de confianza donde se identifica a S3 en Outposts como la entidad principal del servicio que puede asumir el rol.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3-outposts.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- En el siguiente ejemplo, se muestra una política de acceso donde se concede al rol permisos para realizar tareas de replicación en su nombre. Cuando S3 en Outposts asume el rol, adopta los permisos se hayan especificado en esta política. Para utilizar esta política, sustituya *user input placeholders* por su información. Asegúrese de sustituirlos por los ID de Outpost de sus Outposts de origen y destino y los nombres de los buckets y los puntos de acceso de sus buckets de Outposts de origen y destino.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3-outposts:GetObjectVersionForReplication",
            "s3-outposts:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/
bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
            "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/
accesspoint/SOURCE-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3-outposts:ReplicateObject",
            "s3-outposts:ReplicateDelete"
         ],
         "Resource":[
            "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/
bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
            "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/
accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
         ]
      }
   ]
}
```

La política de acceso concede permisos para las siguientes acciones:

- `s3-outposts:GetObjectVersionForReplication`: se otorga permiso para esta acción a todos los objetos para que S3 en Outposts pueda obtener una versión de objeto específica asociada a cada objeto.

- `s3-outposts:GetObjectVersionTagging`: los permisos para esta acción en los objetos del bucket *`SOURCE-OUTPOSTS-BUCKET`* (el bucket de origen) permiten que S3 en Outposts lea las etiquetas de objetos para la replicación. Para obtener más información, consulte Agregar etiquetas para los buckets de S3 en Outposts. Si S3 en Outposts no tiene el permiso, replica los objetos pero no las etiquetas de objetos.
- `s3-outposts:ReplicateObject` y `s3-outposts:ReplicateDelete`: los permisos para estas acciones en todos los objetos del bucket *`DESTINATION-OUTPOSTS-BUCKET`* (el bucket de destino) autorizan a S3 en Outposts a replicar los objetos o los marcadores de eliminación en el bucket de Outposts de destino. Para obtener información acerca de los marcadores de eliminación, consulte Cómo afectan las operaciones de eliminación a la replicación.

  > **Note**
  >
  > - El permiso para la acción `s3-outposts:ReplicateObject` en el bucket *`DESTINATION-OUTPOSTS-BUCKET`* (bucket de destino) también permite la replicación de las etiquetas de objetos. Por lo tanto, no es necesario que conceda permiso de forma explícita para la acción `s3-outposts:ReplicateTags`.
  > - Para la replicación entre cuentas, el propietario del bucket de Outposts de destino debe actualizar su política de bucket para conceder permiso para la acción `s3-outposts:ReplicateObject` en el *`DESTINATION-OUTPOSTS-BUCKET`*. La acción `s3-outposts:ReplicateObject` permite a S3 en Outposts replicar los objetos y las etiquetas de objetos en el bucket de Outposts de destino.

Para obtener una lista de las acciones de S3 en Outposts, consulte Acciones definidas por Amazon S3 en Outposts.

> **Important**
>
> La Cuenta de AWS propietaria del rol de IAM debe tener los permisos para las acciones que concede al rol de IAM.
> Por ejemplo, imagine que el bucket de Outposts de origen contiene objetos que pertenecen a otra Cuenta de AWS. El propietario de los objetos debe conceder explícitamente los

permisos necesarios a la Cuenta de AWS que posee el rol de IAM a través de la política de punto de acceso y de bucket. De lo contrario, S3 en Outposts no puede acceder a los objetos y no se pueden replicar los objetos.
Los permisos aquí descritos están relacionados con la configuración de replicación mínima. Si elige agregar configuraciones de replicación opcionales, debe otorgar permisos adicionales a S3 en Outposts.

### Concesión de permisos cuando los buckets de Outposts de origen y destino pertenecen a diferentes Cuentas de AWS

Cuando los buckets de Outposts de origen y destino no pertenecen a las mismas cuentas, el propietario del bucket de Outposts de destino debe actualizar las políticas de buckets y de puntos de acceso para el bucket de destino. Estas políticas deben conceder permisos al propietario del bucket de Outposts de origen y al rol de servicio de IAM para que puedan realizar acciones de replicación, tal como se muestra en los siguientes ejemplos de políticas, pues de lo contrario se producirá un error en la replicación. En estos ejemplos de política, *DESTINATION-OUTPOSTS-BUCKET* es el bucket de destino. Para utilizar estos ejemplos de política, sustituya *user input placeholders* por su información.

Si va a crear el rol de servicio de IAM de forma manual, defina la ruta del rol como `role/service-role/`, tal como se muestra en los siguientes ejemplos de políticas. Para obtener más información, consulte ARN de IAM en la guía del usuario de IAM.

```
{
   "Version":"2012-10-17",
   "Id":"PolicyForDestinationBucket",
   "Statement":[
      {
         "Sid":"Permissions on objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::SourceBucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action":[
            "s3-outposts:ReplicateDelete",
            "s3-outposts:ReplicateObject"
         ],
         "Resource":[
```

```
            "arn:aws:s3-outposts:region:DestinationBucket-account-
ID:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*"
         ]
      }

   ]
}
```

```
{
"Version":"2012-10-17",
   "Id":"PolicyForDestinationAccessPoint",
   "Statement":[
      {
         "Sid":"Permissions on objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::SourceBucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action":[
            "s3-outposts:ReplicateDelete",
            "s3-outposts:ReplicateObject"
         ],
         "Resource" :[
            "arn:aws:s3-outposts:region:DestinationBucket-account-
ID:outpost/DESTINATION-OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/
object/*"
         ]
      }
   ]
}
```

> **Note**
>
> Si los objetos en el bucket de Outposts de origen tienen etiquetas, tenga en cuenta lo siguiente:
> Si el propietario del bucket de Outposts de origen concede permisos a S3 en Outposts para las acciones `s3-outposts:GetObjectVersionTagging` y `s3-outposts:ReplicateTags` para replicar las etiquetas de los objetos (mediante el rol de

IAM), Amazon S3 replicará las etiquetas junto con los objetos. Para obtener información acerca del rol de IAM, consulte Creación de un rol de IAM.

## Creación de reglas de replicación en Outposts

La replicación de S3 en Outposts consiste en la replicación automática y asíncrona de los objetos de los buckets en la misma o en diferentes AWS Outposts. La replicación copia los objetos que se acaban de crear y las actualizaciones de objetos de un bucket de Outposts de origen a un bucket o buckets de Outposts de destino. Para obtener más información, consulte Replicación de objetos para S3 en Outposts.

> **Note**
>
> Los objetos que había en el bucket de Outposts de origen antes de que configurara las reglas de replicación no se replican. En otras palabras, S3 en Outposts no replica los objetos retroactivamente. Para replicar objetos creados antes de que configurara la replicación, puede utilizar la operación de la API `CopyObject` para copiarlos en el mismo bucket. Una vez copiados los objetos, aparecen como objetos «nuevos» en el bucket y se les aplica la configuración de replicación. Para obtener más información sobre cómo se copia un objeto, consulte Copia de un objeto en un bucket de Amazon S3 en Outposts utilizando AWS SDK para Java y CopyObject en la Referencia de la API de Amazon Simple Storage Service.

Al configurar la replicación, se agregan reglas de replicación al bucket de Outposts de origen. Las reglas de replicación definen qué objetos del bucket de Outposts de origen se deben replicar y el bucket o buckets de Outposts de destino donde se almacenarán 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 Outposts de destino puede estar en el mismo Outpost que el bucket de Outpost de origen o puede estar en un Outpost diferente.

Para las reglas de replicación de S3 en Outposts, debe proporcionar tanto el nombre de recurso de Amazon (ARN) del punto de acceso del bucket de Outposts de origen como el ARN del punto de acceso del bucket de Outposts de destino, en lugar de los nombres de los buckets de Outposts de origen y destino.

Si especifica un ID de versión de objeto para eliminarlo, S3 en Outposts elimina esa versión del objeto del bucket de Outposts de origen. Pero no replica la eliminación en el bucket de Outposts de destino. En otras palabras, no elimina la misma versión del objeto del bucket de Outposts de destino. Este comportamiento protege los datos de eliminaciones malintencionadas.

Cuando se añade una regla de replicación a un bucket de Outposts, la regla está activada de forma predeterminada, por lo que comienza a funcionar en cuanto se guarda.

En este ejemplo, se configura la replicación de los buckets de Outposts de origen y destino que están en Outposts distintos y son propiedad de la misma Cuenta de AWS. Se proporcionan ejemplos de cómo utilizar la consola de Amazon S3, la AWS Command Line Interface (AWS CLI), y AWS SDK para Java y AWS SDK para .NET. Para obtener más información sobre los permisos de Replicación de S3 en Outposts entre cuentas, consulte Concesión de permisos cuando los buckets de Outposts de origen y destino pertenecen a diferentes Cuentas de AWS.

Para conocer los requisitos previos para configurar las reglas de replicación de S3 en Outposts, consulte Requisitos previos para crear reglas de replicación.

Uso de la consola de S3

Siga estos pasos para configurar una regla de replicación cuando el bucket de Amazon S3 en Outposts de destino esté en un Outposts distinto del bucket de Outposts de origen.

Si el bucket de Outposts de destino está en una cuenta distinta a la del bucket de Outposts de origen, se debe añadir una política de buckets al bucket de Outposts de destino para conceder al propietario de la cuenta del bucket de Outposts de origen permiso para replicar objetos en el bucket de Outposts de destino.

Para crear una regla de replicación

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En la lista Buckets de Outposts, seleccione el nombre del bucket para el que desea usar el bucket de origen.
3. Elija Administración, desplácese hacia abajo hasta Reglas de replicación y, a continuación, elija Crear regla de replicación.
4. En Nombre de la regla de replicación, 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. En Estado, Habilitada está seleccionado de forma predeterminada. Una regla activada comienza a funcionar tan pronto se guarda. Si desea habilitar la regla más adelante, seleccione Deshabilitada.
6. En Prioridad, el valor de prioridad de la regla determina qué regla aplicar si hay reglas superpuestas. Cuando los objetos se incluyen en el ámbito de más de una de regla de replicación, S3 en Outposts utiliza estos valores de prioridad para evitar conflictos. De forma predeterminada, las reglas nuevas se agregan a la configuración de replicación con la prioridad más alta. Cuanto mayor sea el número, mayor será la prioridad.

   Para cambiar la prioridad de la regla, después de guardarla, elija el nombre de la regla en la lista de reglas de replicación, elija Acciones y, a continuación, elija Editar prioridad.
7. En Bucket de origen, tiene las siguientes opciones para establecer el origen de la replicación:

   - Para replicar todo el bucket, elija Aplicar a todos los objetos del bucket.
   - Para aplicar el filtrado de prefijos o etiquetas al origen de la replicación, elija Limitar el alcance de esta regla mediante uno o más filtros. Puede hacer uso combinado de un prefijo y etiquetas.
     - Para replicar todos los objetos que tengan el mismo prefijo, en Prefijo, introduzca un prefijo en el cuadro. Para limitar la replicación a todos los objetos que tienen nombres que empiezan con la misma cadena (por ejemplo, ), use el filtro Prefijo`pictures`.

       Si escribe un prefijo que es el nombre de una carpeta, debe usar una / (barra inclinada) como último carácter (por ejemplo, `pictures/`).
     - Para replicar todos los objetos que tienen una o varias etiquetas de objeto, elija Agregar etiqueta y escriba el par clave-valor en los cuadros. Para agregar otra etiqueta, repita el procedimiento. Para obtener más información acerca de las etiquetas de objeto, consulte Agregar etiquetas para los buckets de S3 en Outposts.
8. Para acceder a su bucket de origen de S3 en Outposts para replicarlo, en Nombre del punto de acceso de origen, elija un punto de acceso que esté adjunto al bucket de origen.
9. En Destino, elija el ARN del punto de acceso del bucket de Outposts de destino donde desea que S3 en Outposts replique objetos. Los buckets de Outposts de destino pueden estar en diferentes Cuenta de AWS o dentro de la misma región que el bucket de Outposts de origen.

   Si el bucket de destino está en una cuenta distinta a la del bucket de Outposts de origen, se debe añadir una política de buckets al bucket de Outposts de destino para conceder al propietario de la cuenta del bucket de Outposts de origen permiso para replicar objetos en el

bucket de Outposts de destino. Para obtener más información, consulte Concesión de permisos cuando los buckets de Outposts de origen y destino pertenecen a diferentes Cuentas de AWS.

> **Note**
>
> Si el control de versiones no está habilitado en el bucket de Outposts de destino, recibirá una advertencia con el botón Habilitar el control de versiones. Elija este botón para activar el control de versiones en el bucket.

10. Configure un rol de servicio de AWS Identity and Access Management (IAM) que pueda asumir S3 en Outposts para reproducir objetos en su nombre.

    Para configurar un rol de IAM, en Rol de IAM, lleve a cabo una de las siguientes acciones:

    - Para que S3 en Outposts cree un nuevo rol de IAM para la configuración de replicación, Elegir entre los roles de IAM existentes y, a continuación, elija Crear un nuevo rol. Cuando se guarda la regla, se genera una política nueva para el rol de IAM que coincide con los buckets de Outposts de origen y destino elegidos. Le recomendamos que elija Crear un nuevo rol.
    - También puede elegir usar un rol de IAM existente. Si lo hace, debe elegir un rol que conceda a S3 en Outposts los permisos necesarios para la replicación. La replicación dará un error si este rol no concede a S3 en Outposts permisos suficientes para seguir la regla de replicación.

      Para escoger un rol existente, marque Elegir entre los roles de IAM existentes y, a continuación, seleccione el nombre en el menú desplegable. También puede elegir Ingresar un ARN de rol de IAM y, a continuación, escribir el nombre de recurso de Amazon (ARN) del rol de IAM.

    > **Important**
    >
    > Cuando añada una regla de replicación a un bucket de S3 en Outposts, debe tener los permisos `iam:CreateRole` y `iam:PassRole` para poder crear y pasar el rol de IAM que concede los permisos de replicación de S3 en Outposts. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de Servicio de AWS en la Guía del usuario de IAM.

11. Todos los objetos de los buckets de Outposts están cifrados de forma predeterminada. Para obtener más información sobre el cifrado de S3 en Outposts, consulte Cifrado de datos en S3 en Outposts. Solo se pueden replicar los objetos cifrados en el servidor con claves administradas

por Amazon S3 (SSE-S3). No se admite la replicación de objetos cifrados en el servidor con claves de AWS Key Management Service (AWS KMS) (SSE-KMS) o cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C).

12. Habilite las siguientes opciones adicionales al configurar la regla de replicación, según sea necesario:

    - Si desea habilitar métricas de replicación de S3 en Outposts en la configuración de replicación, seleccione Métricas de replicación. Para obtener más información, consulte Monitoreo del progreso con métricas de replicación.
    - Si desea habilitar la replicación de marcador de eliminación en la configuración de replicación, seleccione Delete marker replication (Eliminar replicación de marcadores). Para obtener más información, consulte Cómo afectan las operaciones de eliminación a la replicación.
    - Si desea replicar los cambios de metadatos realizados en las réplicas en los objetos de origen, seleccione Sincronización de modificación de réplicas. Para obtener más información, consulte Estado de replicación si la sincronización de modificación de réplica de Amazon S3 en Outposts está habilitada.

13. Para terminar, seleccione Crear regla.

Después de guardar la regla, puede editarla, habilitarla, deshabilitarla o eliminarla. Para ello, vaya a la pestaña Administración del bucket de Outposts de origen, desplácese hacia abajo hasta la sección Reglas de replicación, elija su regla y, a continuación, Editar regla.

Uso de la AWS CLI

Para utilizar la AWS CLI con el objetivo de configurar la replicación cuando los buckets de Outposts de origen y destino son propiedad de la misma Cuenta de AWS, debe hacer lo siguiente:

- Crear buckets de Outposts de origen y destino.
- Habilitar el control de versiones en ambos buckets.
- Crear un rol de IAM que conceda permisos a S3 en Outposts para replicar objetos.
- Agregar la configuración de replicación al bucket de Outposts de origen.

Para verificar la configuración, debe probarla.

Para configurar la replicación cuando los buckets de Outposts de origen y destino son propiedad de la misma Cuenta de AWS

1. Configure un perfil de credenciales para la AWS CLI. En este ejemplo, usamos el nombre de perfil `acctA`. Para obtener información acerca de la configuración de perfiles de credenciales, consulte Perfiles con nombre en la Guía del usuario de la AWS Command Line Interface.

   > **Important**
   >
   > Los perfiles utilizados para este ejercicio tienen que tener los permisos necesarios. Por ejemplo, en la configuración de replicación debe especificar el rol de servicio de IAM que puede asumir S3 en Outposts. Solo puede hacer esto si el perfil que utiliza tiene los permisos `iam:CreateRole` y `iam:PassRole`. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un servicio de Servicio de AWS en la Guía del usuario de IAM. Si utiliza credenciales de administrador para crear un perfil con nombre, el perfil con nombre tendrá el permiso necesario para realizar todas las tareas.

2. Cree un bucket de *origen* y habilite el control de versiones. El siguiente comando `create-bucket` crea un bucket *SOURCE-OUTPOSTS-BUCKET* en la región Este de EE. UU. (Norte de Virginia) (`us-east-1`). Para usar este comando, sustituya *user input placeholders* por su información.

   ```
   aws s3control create-bucket --bucket SOURCE-OUTPOSTS-BUCKET --outpost-id SOURCE-OUTPOST-ID --profile acctA --region us-east-1
   ```

   El siguiente comando `put-bucket-versioning` habilita el control de versiones en el bucket *SOURCE-OUTPOSTS-BUCKET*. Para usar este comando, sustituya *user input placeholders* por su información.

   ```
   aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
   ```

3. Cree un bucket de *destino* y habilite el control de versiones. El siguiente comando `create-bucket` crea un bucket *DESTINATION-OUTPOSTS-BUCKET* en la región Oeste de EE. UU. (Oregón) (`us-west-2`). Para usar este comando, sustituya *user input placeholders* por su información.

> **Note**
>
> Para establecer la configuración de replicación cuando los buckets de Outposts de origen y destino están en la misma Cuenta de AWS, debe utilizar el mismo perfil. En este ejemplo se utiliza `acctA`. Para probar la configuración de replicación cuando los buckets son propiedad de diferentes Cuentas de AWS, debe especificar diferentes perfiles para cada bucket.

```
aws s3control create-bucket --bucket DESTINATION-OUTPOSTS-BUCKET --create-bucket-
configuration LocationConstraint=us-west-2 --outpost-id DESTINATION-OUTPOST-ID --
profile acctA --region us-west-2
```

El siguiente comando `put-bucket-versioning` habilita el control de versiones en el bucket *DESTINATION-OUTPOSTS-BUCKET*. Para usar este comando, sustituya *user input placeholders* por su información.

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-
OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
```

4. Cree un rol de servicio de IAM. Más adelante en la configuración de la replicación, agregue este rol de servicio al bucket *SOURCE-OUTPOSTS-BUCKET*. S3 en Outposts asume este rol para replicar objetos en su nombre. Crea el rol de IAM en dos pasos:

   a. Crear un rol de IAM.

      i. Copie la siguiente política de confianza y guárdela en un archivo llamado `s3-on-outposts-role-trust-policy.json` en el directorio actual en su equipo local. Esta política concede permisos a la entidad principal de servicio de S3 en Outposts para asumir el rol de servicio.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
```

```
            "Service":"s3-outposts.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. Ejecute el siguiente comando para crear el rol. Reemplace los *user input placeholders* con su propia información.

```
aws iam create-role --role-name replicationRole --assume-role-policy-
document file://s3-on-outposts-role-trust-policy.json --profile acctA
```

b. Asocie una política de permisos al rol de servicio.

i. Copie la siguiente política de permisos y guárdela en un archivo llamado `s3-on-outposts-role-permissions-policy.json` en el directorio actual en su equipo local. Esta política concede permisos para varias acciones de buckets y objetos de S3 en Outposts. Para utilizar esta política, sustituya *user input placeholders* por su información.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3-outposts:GetObjectVersionForReplication",
            "s3-outposts:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-
OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
            "arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-
OUTPOST-ID/accesspoint/SOURCE-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3-outposts:ReplicateObject",
            "s3-outposts:ReplicateDelete"
```

```
            ],
            "Resource":[
               "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-
OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
               "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-
OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
            ]
         }
      ]
}
```

ii. Ejecute el siguiente comando para crear una política y asociarla al rol. Reemplace los *user input placeholders* con su propia información.

```
aws iam put-role-policy --role-name replicationRole --policy-
document file://s3-on-outposts-role-permissions-policy.json --policy-
name replicationRolePolicy --profile acctA
```

5. Agregue una configuración de replicación al bucket *SOURCE-OUTPOSTS-BUCKET*.

   a. Si bien la API de S3 en Outposts requiere la configuración de replicación en formato XML, la AWS CLI requiere que especifique la configuración de reproducción en formato JSON. Guarde la siguiente JSON en un archivo denominado `replication.json` en el directorio local en su equipo. Para usar esta configuración, sustituya *user input placeholders* por su información.

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket":
        "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-
ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT"
      }
    }
  ]
}
```

b. Ejecute el siguiente comando `put-bucket-replication` para añadir la configuración de replicación al bucket de Outposts de origen. Para usar este comando, sustituya *`user input placeholders`* por su información.

```
aws s3control put-bucket-replication --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-
ID/bucket/SOURCE-OUTPOSTS-BUCKET --replication-configuration file://
replication.json --profile acctA
```

c. Para recuperar la configuración de replicación, utilice el comando `get-bucket-replication`. Para usar este comando, sustituya *`user input placeholders`* por su información.

```
aws s3control get-bucket-replication --account-id 123456789012 --bucket
 arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/
bucket/SOURCE-OUTPOSTS-BUCKET --profile acctA
```

6. Pruebe la configuración en la consola de Amazon S3:

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

b. En el bucket *`SOURCE-OUTPOSTS-BUCKET`*, cree una carpeta llamada `Tax`.

c. Agregue objetos de ejemplo a la carpeta `Tax` en el bucket *`SOURCE-OUTPOSTS-BUCKET`*.

d. En el bucket *`DESTINATION-OUTPOSTS-BUCKET`*, compruebe lo siguiente:

- S3 en Outposts ha replicado los objetos.

> **Note**
>
> El tiempo que S3 en Outposts tarda en replicar un objeto depende del tamaño del objeto. Para obtener más información sobre cómo ver el estado de la replicación, consulte Obtención de información del estado de replicación.

- En la pestaña Propiedades, el Estado de replicación se fija en Replica (lo que lo identifica como un objeto de réplica).

# Administración de la replicación

En esta sección se describen opciones de configuración de replicación adicionales que están disponibles en S3 en Outposts, cómo determinar el estado de replicación y cómo solucionar problemas de replicación. Para obtener información acerca de la configuración de replicación principal, consulte Configuración de la replicación.

Temas



## Monitoreo del progreso con métricas de replicación

Replicación de S3 en Outposts proporciona métricas detalladas para las reglas de replicación en la configuración de la replicación. Las métricas de replicación permiten monitorear el progreso de la replicación en intervalos de 5 minutos realizando el seguimiento de los bytes pendientes de replicación, la latencia de replicación y las operaciones pendientes de replicación. También puede configurar Amazon EventBridge para recibir notificaciones de errores de replicación para ayudarlo a solucionar los problemas de configuración.

Si las métricas de replicación están habilitadas, Replicación de S3 en Outposts publica las siguientes métricas en Amazon CloudWatch:

- Bytes pendientes de replicación: número total de bytes de objetos pendientes de replicación para una regla de replicación determinada.
- Latencia de replicación: número máximo de segundos durante los cuales los buckets de destino de replicación están detrás del bucket de origen para una regla de replicación determinada.
- Operaciones pendientes de replicación: número de operaciones pendientes de replicación para una regla de replicación determinada. Las operaciones incluyen objetos, marcadores de eliminación y etiquetas.

> **Note**
>
> Las métricas de Replicación de S3 en Outposts se facturan al mismo precio que las métricas personalizadas de CloudWatch. Para obtener más información, consulte los precios de CloudWatch.

## Obtención de información del estado de replicación

El estado de replicación puede ayudar a determinar el estado actual de un objeto que replica Amazon S3 en Outposts. El estado de replicación de un objeto de origen devolverá `PENDING`, `COMPLETED`, o `FAILED`. Se devolverá el estado de replicación de una réplica `REPLICA`.

Información general sobre el estado de replicación

En un supuesto de replicación, tiene un bucket de origen en el que se configura la replicación y un bucket de destino donde S3 en Outposts replica los objetos. Cuando solicita un objeto (utilizando `GetObject`) o los metadatos de un objeto (utilizando `HeadObject`) de estos buckets, S3 en Outposts devuelve el encabezado `x-amz-replication-status` en la respuesta, del siguiente modo:

- Si solicitar un objeto del bucket de origen, S3 en Outposts devuelve el encabezado `x-amz-replication-status` si el objeto de su solicitud cumple los requisitos para la replicación.

  Por ejemplo, supongamos que especifica el prefijo del objeto `TaxDocs` en la configuración de replicación para indicar a S3 en Outposts que replique solo objetos con el prefijo de nombre de clave `TaxDocs`. Cualquier objeto que cargue que tenga este prefijo de nombre de clave, por ejemplo, `TaxDocs/document1.pdf` se replicará. Para solicitudes de objetos con este prefijo de nombre de clave, S3 en Outposts devuelve el encabezado `x-amz-replication-status` con uno de los siguientes valores para el estado de replicación del objeto: `PENDING`, `COMPLETED` o `FAILED`.

  > **Note**
  >
  > Si la replicación de objetos genera un error después de cargar un objeto, no puede volver a intentar la replicación. Deberá cargar de nuevo el objeto. Los objetos pasan a un estado `FAILED` para problemas como la falta de permisos del rol de replicación o de permisos del bucket. En el caso de errores temporales, como cuando un bucket o su Outpost no están disponibles, el estado de replicación no pasa a `FAILED`, sino que permanece como

PENDING. Después de que el recurso vuelva a estar en línea, S3 en Outposts reanuda la replicación de esos objetos.

- Cuando solicita un objeto desde un bucket de destino, si el objeto de la solicitud es una réplica creada por S3 en Outposts, S3 on Outposts devuelve el encabezado `x-amz-replication-status` con el valor `REPLICA`.

> **Note**
>
> Antes de eliminar un objeto del bucket de origen que tiene activada la replicación, revise el estado de replicación del objeto para asegurarse de que el objeto haya sido replicado.

Estado de replicación si la sincronización de modificación de réplica de Amazon S3 en Outposts está habilitada

Cuando las reglas de replicación habilitan la sincronización de la modificación de réplicas de S3 en Outposts, las réplicas pueden informar estados distintos de `REPLICA`. Si los cambios de metadatos están en proceso de replicación, el encabezado `x-amz-replication-status` para la réplica devuelve `PENDING`. Si la sincronización de modificación de réplica no replica metadatos, el encabezado para la réplica devuelve `FAILED`. Si los metadatos se replican correctamente, el encabezado para la réplica devuelve el valor `REPLICA`.

## Solución de problemas de replicación

Si las réplicas de objetos no aparecen en el bucket de Amazon S3 en Outposts de destino después de configurar la replicación, use estos consejos de solución de problemas para identificar y solucionar los problemas.

- El tiempo que tarda S3 en Outpost en replicar un objeto depende de diferentes factores, como la distancia entre los Outposts de origen y destino, y el tamaño del objeto.

  También puede comprobar el estado de replicación del objeto de origen. Si el estado de replicación del objeto es `PENDING`, significa que S3 en Outposts no ha completado la replicación. Si el estado de replicación del objeto es `FAILED`, compruebe la configuración de replicación establecida en el bucket de origen.
- En la configuración de replicación en el bucket de origen, verifique lo siguiente:
  - El nombre de recurso de Amazon (ARN) del punto de acceso del bucket de destino es correcto.

  - El prefijo de nombre de clave sea correcto. Por ejemplo, si establece la configuración para replicar objetos con el prefijo `Tax`, entonces, solo se replicarán los objetos con nombres de clave como `Tax/document1` o `Tax/document2`. No se replicará un objeto con el nombre de clave `document3`.
  - El estado es `Enabled`.
- Compruebe que el control de versiones no se ha suspendido en ningún bucket. Ambos buckets de origen y destino deben tener habilitado el control de versiones.
- Si el bucket de destino pertenece a otra Cuenta de AWS, compruebe que el propietario del bucket tenga una política de bucket en el bucket de destino que permita al propietario del bucket de origen replicar objetos. Para ver un ejemplo, consulte Concesión de permisos cuando los buckets de Outposts de origen y destino pertenecen a diferentes Cuentas de AWS.
- Si la réplica de un objeto no aparece en el bucket de destino, los siguientes problemas podría haber impedido la replicación:
  - S3 en Outposts no replica un objetos de un bucket de origen si es una réplica creada por otra configuración de replicación. Por ejemplo, si establece una configuración de replicación del bucket A en el bucket B y, luego, en el bucket C, S3 en Outposts no replica las réplicas de objetos del bucket B en el bucket C.

    Si desea replicar objetos del bucket A en el bucket B y en el bucket C, defina varios destinos de bucket en diferentes reglas de replicación para la configuración de replicación del bucket de origen. Por ejemplo, cree dos reglas de replicación en el bucket de origen A, con una regla para replicar en el bucket de destino B y la otra regla para replicar en el bucket de destino C.
  - Un propietario del bucket de origen puede conceder permisos a otras Cuentas de AWS para cargar objetos. De forma predeterminada, el propietario del bucket de origen no tiene permisos sobre los objetos creados por otras cuentas. La configuración de replicación solo replica los objetos para los que el propietario del bucket de origen tiene permisos de acceso. Para evitar problemas de replicación, el propietario del bucket de origen puede conceder permisos a otras Cuentas de AWS para crear objetos con la condición de que tengan permisos de acceso explícitos para esos objetos.
- Supongamos que en la configuración de replicación añade una regla para replicar un subconjunto de objetos con una etiqueta específica. En este caso, debe asignar la clave de etiqueta y el valor específicos en el momento de crear el objeto para que S3 en Outposts replique el objeto. Si primero crea un objeto y luego agrega la etiqueta en el objeto existente, S3 en Outposts no replica el objeto.

- La replicación devuelve un error si la política de bucket deniega el acceso a la función de replicación para cualquiera de las siguientes acciones:

  Bucket de origen:

  ```
  "s3-outposts:GetObjectVersionForReplication",
  "s3-outposts:GetObjectVersionTagging"
  ```

  Buckets de destino:

  ```
  "s3-outposts:ReplicateObject",
  "s3-outposts:ReplicateDelete",
  "s3-outposts:ReplicateTags"
  ```

- Amazon EventBridge pueden enviarle notificaciones cuando los objetos no se repliquen en su Outposts de destino. Para obtener más información, consulte Uso de EventBridge para la replicación de S3 en Outposts.

## Uso de EventBridge para la replicación de S3 en Outposts

Amazon S3 en Outposts se integra con Amazon EventBridge y utiliza el espacio de nombres `s3-outposts`. EventBridge es un servicio de bus de eventos sin servidor que se puede utilizar para conectar las aplicaciones con datos de varios orígenes. Para obtener más información, consulte What is Amazon EventBridge? (¿Qué es Amazon EventBridge?) en la Guía del usuario de Amazon EventBridge.

Puede configurar Amazon EventBridge para recibir notificaciones de eventos de error de replicación para ayudar a solucionar cualquier problema de configuración de la replicación. EventBridge pueden notificarle en instancias cuando los objetos no se repliquen en su Outposts de destino. Para obtener más información sobre el estado actual de un objeto que se replica, consulte Información general sobre el estado de replicación.

S3 en Outposts puede enviar eventos a EventBridge cada vez que se produzcan determinados eventos en el bucket. A diferencia de otros destinos, no es necesario seleccionar qué tipos de eventos desea entregar. Puede utilizar las reglas de EventBridge para dirigir los eventos hacia destinos adicionales. Una vez habilitado EventBridge, S3 en Outposts envía todos los eventos que sigan a EventBridge.

| Tipo de evento | Descripción | Espacio de nombres |
| --- | --- | --- |
| `Operation FailedRep lication` | No se ha podido replicar un objeto dentro de una regla de replicación. Para obtener más información sobre los errores de Replicación de S3 en Outposts, consulte Uso de EventBridge para ver los motivos de error de Replicación de S3 en Outposts. | `s3-outposts` |

Uso de EventBridge para ver los motivos de error de Replicación de S3 en Outposts

En la siguiente tabla se muestran los motivos de error de Replicación de S3 en Outposts. Puede configurar una regla de EventBridge para publicar y ver el motivo de error a través de Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS), AWS Lambda o Registros de Amazon CloudWatch. Para obtener más información sobre los permisos necesarios para utilizar estos recursos de EventBridge, consulte el tema sobre el uso de las políticas basadas en recursos para EventBridge.

| Motivo de error de replicación | Descripción |
| --- | --- |
| `AssumeRoleNotPermitted` | S3 en Outposts no puede asumir el rol (de IAM) AWS Identity and Access Managemen t que se especifica en la configuración de replicación. |
| `DstBucketNotFound` | S3 en Outposts no encuenta el bucket de destino especificado en la configuración de replicación. |
| `DstBucketUnversioned` | El control de versiones no está habilitado en el bucket de destino de Outposts. Habilite el control de versiones en el bucket de destino para replicar objetos con Replicación de S3 en Outposts. |

| Motivo de error de replicación | Descripción |
| --- | --- |
| `DstDelObjNotPermitted` | S3 en Outposts no puede replicar lo que se ha eliminado en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateDelete` para el bucket de destino. |
| `DstMultipartCompleteNotPermitted` | S3 en Outposts no puede completar la carga multiparte de objetos en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateObject` para el bucket de destino. |
| `DstMultipartInitNotPermitted` | S3 en Outposts no puede iniciar una carga multiparte de objetos en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateObject` para el bucket de destino. |
| `DstMultipartPartUploadNotPermitted` | S3 en Outposts no puede cargar objetos de carga multiparte en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateObject` para el bucket de destino. |
| `DstOutOfCapacity` | S3 en Outposts no puede replicarse en el Outpost de destino porque el Outpost no tiene capacidad de almacenamiento de S3. |
| `DstPutObjNotPermitted` | S3 en Outposts no puede replicar objetos en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateObject` para el bucket de destino. |

| Motivo de error de replicación | Descripción |
| --- | --- |
| `DstPutTaggingNotPermitted` | S3 en Outposts no puede replicar etiquetas de objetos en el bucket de destino. Es posible que falte el permiso `s3-outposts:ReplicateObject` para el bucket de destino. |
| `DstVersionNotFound` | S3 en Outposts no encuentra la versión del objeto requerida en el bucket de destino para replicar los metadatos de esa versión del objeto. |
| `SrcBucketReplicationConfigMissing` | S3 en Outposts no encuentra una configuración de replicación para el punto de acceso asociado al bucket de Outposts de origen. |
| `SrcGetObjNotPermitted` | S3 en Outposts no puede acceder al objeto del bucket de origen para replicarlo. Es posible que falte el permiso `s3-outposts:GetObjectVersionForReplication` para el bucket de origen. |
| `SrcGetTaggingNotPermitted` | S3 en Outposts no puede acceder a la etiqueta de objeto del bucket de origen. Es posible que falte el permiso `s3-outposts:GetObjectVersionTagging` para el bucket de origen. |
| `SrcHeadObjectNotPermitted` | S3 en Outposts no puede recuperar los metadatos de objetos del bucket de origen. Es posible que falte el permiso `s3-outposts:GetObjectVersionForReplication` para el bucket de origen. |
| `SrcObjectNotEligible` | El objeto no es apto para la replicación. Los objetos y sus etiquetas de objetos no coinciden con la configuración de replicación. |

Para obtener más información acerca de la resolución de problemas de replicación, consulte los siguientes temas:

- Creación de un rol de IAM
- Solución de problemas de replicación

Monitoreo de EventBridge con CloudWatch

Para el monitoreo, se ha integrado Amazon CloudWatch con Amazon EventBridge. EventBridge envía automáticamente métricas a CloudWatch cada minuto. Estas métricas incluyen el número de eventos que coincide con una regla y el número de veces que una regla invoca un objetivo. Cuando se ejecuta una regla en EventBridge, se invocan todos los destinos asociados a la regla. Puede monitorear su comportamiento en EventBridge a través de CloudWatch de las siguientes maneras.

- Puede monitorear las métricas de EventBridge disponibles para sus reglas de EventBridge desde el panel de CloudWatch. A continuación, puede utilizar las funciones de CloudWatch, como las alarmas de CloudWatch, para configurar alarmas en determinadas métricas. Si esas métricas alcanzan los valores límite personalizados que ha especificado en las alarmas, recibirá notificaciones y podrá tomar las medidas pertinentes.
- Puede configurar Registros de Amazon CloudWatch como destino de su regla de EventBridge. A continuación, EventBridge crea flujos de registro y CloudWatch Logs almacena el texto de los eventos como entradas de registro. Para obtener más información, consulte EventBridge y CloudWatch Logs.

Para obtener más información sobre la depuración de eventos de archivo y la entrega de evenros de EventBridge, consulte los siguientes temas:

- Política de reintentos de eventos y uso de colas de mensajes fallidos
- Archivado de eventos de EventBridge

# Uso compartido de S3 en Outposts con AWS RAM

Amazon S3 en Outposts admite el uso compartido de la capacidad de S3 en varias cuentas de una organización mediante AWS Resource Access Manager (AWS RAM). Con el uso compartido de S3 en Outposts, puede permitir que otros creen y administren los buckets, los puntos de conexión y los puntos de acceso en su Outpost.

En este tema se muestra cómo utilizar AWS RAM para compartir S3 en Outposts y los recursos relacionados con otra Cuenta de AWS en su organización de AWS.

## Requisitos previos

- La cuenta propietaria de Outpost tiene configurada una organización en AWS Organizations. Para obtener más información, consulte Creación de una organización en la Guía del usuario de AWS Organizations.
- La organización incluye la Cuenta de AWS con la que desea compartir la capacidad de S3 en Outposts. Para obtener más información, consulte Envío de invitaciones aCuentas de AWS en la Guía del usuario de AWS Organizations.
- Seleccione una de las siguientes opciones que desea compartir. Se debe seleccionar el segundo recurso (las Subnets [Subredes] u Outposts [Outposts]) para que también se pueda acceder a los puntos de conexión. Los puntos de conexión son un requisito de red para acceder a los datos almacenados en S3 en Outposts.

| Opción 1 | Opción 2 |
| --- | --- |
| S3 en Outposts | S3 en Outposts |
| Permite que el usuario cree buckets en sus Outposts y puntos de acceso y que agregue objetos en esos buckets. | Permite que el usuario cree buckets en sus Outposts y puntos de acceso y que agregue objetos en esos buckets. |
| Subredes | Outposts |
| Permite que el usuario utilice la nube privada virtual (VPC) y los puntos de conexión asociados a la subred. | Permite que el usuario vea los gráficos de capacidad de S3 y la página de inicio de la consola de AWS Outposts. También permite que los usuarios creen subredes en Outposts compartidos y que creen puntos de conexión. |

## Procedimiento

1. Inicie sesión en la AWS Management Console mediante la Cuenta de AWS propietaria del Outpost y, a continuación, abra la consola de AWS RAM en https://console.aws.amazon.com/ram/home.

2. Asegúrese de haber habilitado la opción para compartir AWS Organizations en AWS RAM. Para obtener información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM.
3. Utilice la opción 1 o la opción 2 en requisitos previos para crear un recurso compartido. Si tiene varios recursos de S3 en Outposts, seleccione los nombres de recurso de Amazon (ARN) de los recursos que desea compartir. Para habilitar los puntos de conexión, comparta la subred u Outpost.

   Para obtener información sobre cómo crear un recurso compartido, consulte Creación de un recurso compartido en la Guía del usuario de AWS RAM.
4. La Cuenta de AWS con la que compartió sus recursos debería poder utilizar S3 en Outposts. Según la opción que seleccionó en los requisitos previos, proporcione la siguiente información al usuario de la cuenta:

| Opción 1 | Opción 2 |
| --- | --- |
| El ID de Outpost | El ID de Outpost |
| El ID de la VPC | |
| El ID de subred | |
| El ID del grupo de seguridad | |

> **Note**
>
> El usuario puede confirmar que los recursos se compartieron con ellos mediante la consola de AWS RAM, la AWS Command Line Interface (AWS CLI), los SDK de AWS o la API de REST. El usuario puede ver sus recursos compartidos existentes con el comando de la CLI get-resource-shares.

## Ejemplos de uso

Una vez que haya compartido sus recursos de S3 en Outposts con otra cuenta, esa cuenta puede administrar los buckets y los objetos en su Outpost. Si compartió el recurso Subnets (Subredes), luego esa cuenta puede utilizar el punto de conexión que ha creado. En los siguientes ejemplos,

se muestra cómo un usuario puede utilizar AWS CLI para interactuar con su Outpost después de compartir estos recursos.

Example : crear un bucket

En el siguiente ejemplo, se crea un bucket denominado *amzn-s3-demo-bucket1* en el Outpost *op-01ac5d28a6a232904*. Antes de utilizar este comando, reemplace cada *user input placeholder* con los valores adecuados para su caso de uso.

```
aws s3control create-bucket --bucket amzn-s3-demo-bucket1 --outpost-
id op-01ac5d28a6a232904
```

Para obtener más información acerca de este comando, consulte create-bucket en la Referencia de AWS CLI.

Example : crear un punto de acceso

En el siguiente ejemplo, se crea un punto de acceso en un Outpost mediante los parámetros de ejemplo de la siguiente tabla. Antes de utilizar este comando, reemplace estos valores *user input placeholder* y el código de la Región de AWS con los valores adecuados para su caso de uso.

| Parámetro | Valor |
| --- | --- |
| ID de cuenta | *111122223333* |
| Nombre del punto de acceso | *example-outpost-access-point* |
| ID de Outpost | *op-01ac5d28a6a232904* |
| Nombre del bucket del Outpost | *amzn-s3-demo-bucket1* |
| ID de VPC | *vpc-1a2b3c4d5e6f7g8h9* |

> **Note**
>
> El parámetro de ID de la cuenta debe ser el ID de la Cuenta de AWS del propietario del bucket, que es el usuario compartido.

```
aws s3control create-access-point --account-id 111122223333 --name example-outpost-
access-point \
--bucket arn:aws:s3-outposts:us-east-1:111122223333:outpost/op-01ac5d28a6a232904/
bucket/amzn-s3-demo-bucket1 \
--vpc-configuration VpcId=vpc-1a2b3c4d5e6f7g8h9
```

Para obtener más información acerca de este comando, consulte create-access-point en la Referencia de AWS CLI.

Example : cargar un objeto

En el siguiente ejemplo, se carga el archivo *my_image.jpg* desde el sistema de archivos local del usuario a un objeto denominado *images/my_image.jpg* a través del punto de acceso *example-outpost-access-point* en el Outpost *op-01ac5d28a6a232904*, propiedad de la cuenta de AWS *111122223333*. Antes de utilizar este comando, reemplace estos valores *user input placeholder* y el código de la Región de AWS con los valores adecuados para su caso de uso.

```
aws s3api put-object --bucket arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-
point \
--body my_image.jpg --key images/my_image.jpg
```

Para obtener más información acerca de este comando, consulte put-object en la Referencia de AWS CLI.

> **Note**
>
> Si esta operación devuelve el error Resource not found (Recurso no encontrado) o no responde, es posible que la VPC no tenga un punto de conexión compartido.
> Para comprobar si hay un punto de conexión compartido, utilice el comando de la AWS CLI list-shared-endpoints (puntos finales de lista compartida). Si no hay un punto de conexión compartido, trabaje con el propietario del Outpost para crear uno. Para obtener más información, consulte ListSharedEndpoints en la Referencia de la API de Amazon Simple Storage Service.

Example : crear un punto de conexión

En el siguiente ejemplo, se crea un punto de conexión en un Outpost compartido. Antes de utilizar este comando, sustituya los valores *user input placeholder* para el ID de Outpost, el ID de subred y el ID del grupo de seguridad con los valores adecuados para su caso de uso.

> **Note**
>
> El usuario puede realizar esta operación solo si el recurso compartido incluye el recurso de Outposts.

```
aws s3outposts create-endpoint --outposts-id op-01ac5d28a6a232904 --subnet-id XXXXXX --
security-group-id XXXXXXX
```

Para obtener más información acerca de este comando, consulte create-endpoint en la Referencia de AWS CLI.

## Otros Servicios de AWS que usan S3 en Outposts

Otros Servicios de AWS que se ejecutan de forma local en su AWS Outposts también pueden utilizar la capacidad de Amazon S3 en Outposts. En Amazon CloudWatch, el espacio de nombres `S3Outposts` muestra métricas detalladas de los buckets dentro de S3 en Outposts, pero estas métricas no incluyen el uso de otros Servicios de AWS. Para administrar la capacidad de S3 en Outposts que consumen otros Servicios de AWS, consulte la información de la tabla siguiente.

| Servicio de AWS | Descripción | Más información |
| --- | --- | --- |
| Amazon S3 | Todo uso directo de S3 en Outposts tiene una métrica de CloudWatch de bucket y una cuenta coincidentes. | Consulte Métricas |
| Amazon Elastic Block Store (Amazon EBS) | Para Amazon EBS on Outposts, puede elegir un Outpost de AWS como destino de instantáneas y almacenarlo localmente en su S3 en Outpost. | Más información |
| Amazon Relational Database | Puede utilizar las copias de seguridad locales de Amazon RDS para almacenar sus copias de seguridad de RDS localmente en su Outpost. | Más información |

| Servicio de AWS | Descripción | Más información |
| --- | --- | --- |
| Service (Amazon RDS) | | |

# Monitoreo de S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (OUTPOSTS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

Para obtener más información sobre cómo administrar la capacidad de almacenamiento de Amazon S3 en Outposts, consulte los siguientes temas.

Temas



## Administración de la capacidad de S3 en puestos avanzados con las métricas de Amazon CloudWatch

Para ayudar a administrar la capacidad fija de S3 en Outpost, recomendamos que cree alertas de CloudWatch que le digan cuándo la utilización del almacenamiento supera un umbral determinado. Para obtener más información acerca de las métricas de CloudWatch para S3 en Outposts, consulte Métricas de CloudWatch. Si no hay suficiente espacio para almacenar un objeto en su Outpost, la API devuelve una excepción de capacidad insuficiente (ICE). Para liberar espacio, puede crear alarmas de CloudWatch que desencadenen la eliminación explícita de datos o utilizar una política de vencimiento del ciclo de vida para hacer vencer los objetos. Para guardar datos antes de la eliminación, puede usar AWS DataSync para copiar datos desde el bucket de Amazon S3 en

Outposts hasta un bucket de S3 en una Región de AWS. Para obtener más información acerca del uso de DataSync, consulte Introducción a AWS DataSync en la Guía del usuario de AWS DataSync.

## Métricas de CloudWatch

El espacio de nombres `S3Outposts` incluye las siguientes métricas de buckets de Amazon S3 en Outposts. Puede monitorear el número total de bytes de S3 en Outposts aprovisionados, el total de bytes libres disponibles para los objetos y el tamaño total de todos los objetos para un bucket determinado. Existen métricas relacionadas con el bucket o la cuenta para todo el uso directo de S3. El uso indirecto de S3, como almacenar las instantáneas locales de Amazon Elastic Block Store o las copias de seguridad de Amazon Relational Database Service en un Outpost, consume capacidad de S3, pero no se incluye en las métricas relacionadas con el bucket o la cuenta. Para obtener más información acerca de las instantáneas locales de Amazon EBS, consulte Instantáneas locales de Amazon EBS en Outposts. Para ver el informe de costos de Amazon EBS, consulte https://console.aws.amazon.com/costmanagement/.

> **Note**
>
> S3 en Outposts solo admite las siguientes métricas y ninguna otra métrica de Amazon S3. Dado que S3 en Outposts tiene un límite de capacidad fija, recomendamos crear alarmas de CloudWatch que le notifiquen cuando el uso del almacenamiento supere cierto umbral.

| Métrica | Descripción | Periodo | Unidades | Tipo |
|---|---|---|---|---|
| `Outpost` `talByte` | La capacidad total aprovisio nada en bytes para un Outpost. | 5 minutos | Bytes | S3 on Outposts |
| `Outpostl` `eeBytes` | El recuento de bytes libres disponibles en Outposts para almacenar datos de clientes | 5 minutos | Bytes | S3 on Outposts |
| `BucketU` `dBytes` | El tamaño total de todos los objetos para el bucket determinado. | 5 minutos | Bytes | S3 en Outposts. Solo para uso directo de S3. |

| Métrica | Descripción | Periodo | Unidades | Tipo |
| --- | --- | --- | --- | --- |
| AccountUsedBytes | El tamaño total de todos los objetos para la cuenta especificada de Outposts | 5 minutos | Bytes | S3 en Outposts. Solo para uso directo de S3. |
| BytesPendingReplication | Número total de bytes de objetos pendientes de replicación para una regla de replicación determinada. Para obtener más información sobre cómo activar las métricas de replicación, consulte el tema sobre cómo crear reglas de replicación entre Outposts. | 5 minutos | Bytes | Opcional. Para S3 Replication en Outposts. |
| OperationsPendingReplication | Número total de operaciones pendientes de replicación para una regla de replicación determinada. Para obtener más información sobre cómo activar las métricas de replicación, consulte el tema sobre cómo crear reglas de replicación entre Outposts. | 5 minutos | Recuentos | Opcional. Para S3 Replication en Outposts. |

| Métrica | Descripción | Periodo | Unidades | Tipo |
| --- | --- | --- | --- | --- |
| `Replica` `onLaten` | Número actual de segundos de retraso durante los cuales el bucket de destino de replicación está detrás del bucket de origen para una regla de replicación determinada. Para obtener más información sobre cómo activar las métricas de replicación, consulte el tema sobre cómo crear reglas de replicación entre Outposts. | 5 minutos | Segundos | Opcional. Para S3 Replication en Outposts. |

## Recepción de notificaciones de eventos de S3 en Outposts mediante Amazon CloudWatch Events

Puede utilizar CloudWatch Events para crear una regla para cualquier evento de API de Amazon S3 en Outposts. Al crear una regla, puede elegir recibir notificaciones a través de todos los destinos de CloudWatch compatibles, incluidos Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) y AWS Lambda. Para obtener más información, consulte la lista de servicios de AWS que pueden ser destinos de CloudWatch Events en la Guía del usuario de Eventos de Amazon CloudWatch. Para elegir un servicio de destino para trabajar con S3 en Outposts, consulte Creación de una regla de CloudWatch Events que se desencadena en una llamada a la API de AWS con AWS CloudTrail en la Guía del usuario de Eventos de Amazon CloudWatch.

> **Note**
>
> Para las operaciones de objetos de S3 en Outposts, los eventos de llamada a la API de AWS enviados por CloudTrail solo coincidirán con sus reglas si tiene registros (opcionalmente con selectores de eventos) configurados para recibir dichos eventos. Para obtener más información, consulte Uso de archivos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.

Example

A continuación se muestra una regla de ejemplo para la operación de `DeleteObject`. Para utilizar esta regla de ejemplo, sustituya *amzn-s3-demo-bucket1* por el nombre del bucket de S3 en Outposts.

```
{
  "source": [
    "aws.s3-outposts"
  ],
  "detail-type": [
    "AWS API call through CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "s3-outposts.amazonaws.com"
    ],
    "eventName": [
      "DeleteObject"
    ],
    "requestParameters": {
      "bucketName": [
        "amzn-s3-demo-bucket1"
      ]
    }
  }
}
```

# Monitoreo de S3 en Outposts con registros de AWS CloudTrail

Amazon S3 en Outposts se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de Servicio de AWS en S3 en Outposts. Puede utilizar AWS CloudTrail para obtener información sobre las solicitudes en el nivel de bucket y de objeto de S3 en Outpost para auditar y registrar su actividad de eventos de S3 en Outposts.

Para activar los eventos de datos de CloudTrail para todos los buckets de Outposts o para una lista de buckets específicos de Outposts, debe crear un registro de seguimiento manualmente en CloudTrail. Para obtener más información sobre las entradas de archivos de registro de CloudTrail, consulte Entradas de archivo de registro de Amazon S3 en Outposts.

Para obtener una lista completa de los eventos de datos de CloudTrail para S3 en Outposts, consulte los Eventos de Amazon S3 CloudTrail en la Guía del usuario de Amazon S3.

> **Note**
>
> - Una práctica recomendada consiste en crear una política de ciclo de vida para el bucket de Outposts de eventos de datos de AWS CloudTrail. Configure la política de ciclo de vida para eliminar periódicamente los archivos de registro tras el periodo de tiempo que necesite para auditarlos. Esto reduce la cantidad de datos que Amazon Athena analiza para cada consulta. Para obtener más información, consulte Creación y administración de una configuración de ciclo de vida para un bucket de Amazon S3 en Outposts.
> - Para obtener ejemplos de cómo consultar los registros de CloudTrail, visite la publicación Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail and Amazon Athena del Blog de big data de AWS.

## Activar el registro de CloudTrail para objetos en un bucket de S3 en Outposts

Puede utilizar la consola de Amazon S3 para configurar una auditoría de AWS CloudTrail con el fin de registrar eventos de datos para objetos en un bucket de Amazon S3 en Outposts. CloudTrail permite que se registren operaciones de API en el nivel de objetos de S3 en Outsposts como, por ejemplo, `GetObject`, `DeleteObject` y `PutObject`. Estos eventos se denominan eventos de datos.

De forma predeterminada, los registros de seguimiento de CloudTrail no registran eventos de datos. Sin embargo, puede configurar registros de seguimiento para registrar eventos de datos para buckets de S3 en Outposts que especifique o para registrar eventos de datos para todos los buckets de S3 en Outposts de su Cuenta de AWS.

CloudTrail no rellena eventos de datos en el historial de eventos de CloudTrail. Además, no todas las operaciones de la API de nivel de bucket de S3 en Outposts se rellenan en el historial de eventos de CloudTrail. Para obtener más información acerca de cómo consultar los registros de CloudTrail, consulte el artículo del Centro de conocimientos de AWS sobre el uso de patrones de filtro de registros de Amazon CloudWatch y Amazon Athena para consultar los registros de CloudTrail.

Para configurar un registro de seguimiento para que registre eventos de datos para un bucket de S3 en Outposts, puede utilizar la consola de AWS CloudTrail o la consola de Amazon S3. En caso de

que esté configurando un registro de seguimiento con el fin de registrar eventos de datos para todos los buckets de S3 en Outposts en su Cuenta de AWS, es más fácil utilizar la consola de CloudTrail. Para obtener información sobre el uso de la consola de CloudTrail a fin de configurar un registro de seguimiento con el objetivo de registrar eventos de datos de S3 en Outposts, 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.

En el siguiente procedimiento, se muestra cómo utilizar la consola de Amazon S3 a fin de configurar un registro de seguimiento de CloudTrail con el objetivo de registrar eventos de datos para un bucket de S3 en Outposts.

> **Note**
>
> La Cuenta de AWS que crea el bucket es su propietaria y la única que puede configurar eventos de datos de S3 en Outposts para enviarlos a AWS CloudTrail.

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

1. Inicie sesión AWS Management Console Management Console y abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En el panel de navegación izquierdo, elija Outposts buckets (Buckets de Outposts).
3. Elija el nombre el bucket de Outposts cuyos eventos de datos desea registrar mediante CloudTrail.
4. Seleccione Propiedades.
5. Vaya a la sección Eventos de datos de AWS CloudTrail y elija Configurar en CloudTrail.

   Se abrirá la consola de AWS CloudTrail.

   Puede crear un nuevo registro de seguimiento de CloudTrail o reutilizar uno existente y configurar eventos de datos de S3 en Outposts para que se registren en el seguimiento.
6. En la página Panel de la consola de CloudTrail, seleccione Crear un registro de seguimiento.

7. En la página Paso 1 Elegir atributos del registro de seguimiento, proporcione un nombre para el registro de seguimiento, elija un bucket de S3 para almacenar los registros de seguimiento, especifique cualquier otra configuración que desee y, a continuación, elija Siguiente.
8. En la página Paso 2 Elegir eventos de registro, en Tipo de evento, elija Eventos de datos.

   En Tipo de evento de datos, elija S3 Outposts. Elija Siguiente.

   > **Note**
   >
   > - Al crear un registro de seguimiento y configurar el registro de eventos de datos para S3 en Outposts, debe especificar el tipo de evento de datos correctamente.
   >   - Si usa la consola de CloudTrail, elija S3 Outposts como Tipo de evento de datos. Para obtener información acerca de cómo crear seguimientos en la consola de CloudTrail, consulte Creación y actualización de un seguimiento con la consola en la Guía del usuario de AWS CloudTrail. Si quiere obtener información sobre cómo configurar el registro de eventos de datos de S3 en Outposts en la consola de CloudTrail, consulte el punto Registrar eventos de datos para objetos de Amazon S3 en la guía del usuario de AWS CloudTrail.
   >   - Si usa la AWS Command Line Interface (AWS CLI) o los SDK de AWS, defina el campo `resources.type` como `AWS::S3Outposts::Object`. Para obtener más información sobre cómo registrar eventos de datos de S3 en Outposts con la AWS CLI, consulte Registrar eventos de S3 en Outposts en la Guía del usuario de AWS CloudTrail.
   > - Si utiliza la consola de CloudTrail o la consola de Amazon S3 para configurar un registro de seguimiento para registrar eventos de datos para un bucket de S3 en Outposts, la consola de Amazon S3 muestra que los registros de nivel de objeto están activados para el bucket.

9. En la página Paso 3 Revisar y crear, revise los atributos del registro de seguimiento y los eventos de registro que ha configurado. Después, seleccione Crear un registro de seguimiento.

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

1. Inicie sesión en la AWS Management Console y abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.

2. En el panel de navegación situado a la izquierda, elija Registros de seguimiento.
3. Elija el nombre del registro de seguimiento que creo para registrar los eventos de su bucket de S3 en Outposts.
4. En la página de detalles del registro de seguimiento, seleccione Detener registro en la esquina superior derecha.
5. En el cuadro de diálogo que aparece, elija Detener registro.

## Entradas de archivo de registro de AWS CloudTrail de Amazon S3 en Outposts

Los eventos de administración de Amazon S3 en Outposts están disponibles a través de AWS CloudTrail. Además, puede habilitar el registro de eventos de datos en AWS CloudTrail de forma opcional.

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro al bucket de S3 en una región que especifique. Los registros de CloudTrail para sus buckets de Outposts incluyen un nuevo campo, `edgeDeviceDetails`, que identifica Outposts donde se encuentra el bucket especificado.

Los campos de registro adicionales incluyen la acción solicitada, la fecha y hora de la acción y los parámetros de solicitud. Los archivos de registro de CloudTrail no son un seguimiento de pila ordenado de las llamadas a la API públicas, por lo que no aparecen en un orden específico.

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail que muestra una acción PutObject en `s3-outposts`.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/yourUserName",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "yourUserName"
      },
      "eventTime": "2020-11-30T15:44:33Z",
      "eventSource": "s3-outposts.amazonaws.com",
      "eventName": "PutObject",
```

```
      "awsRegion": "us-east-1",
      "sourceIPAddress": "26.29.66.20",
      "userAgent": "aws-cli/1.18.39 Python/3.4.10 Darwin/18.7.0 botocore/1.15.39",
      "requestParameters": {
        "expires": "Wed, 21 Oct 2020 07:28:00 GMT",
        "Content-Language": "english",
        "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
        "ObjectCannedACL": "BucketOwnerFullControl",
        "x-amz-server-side-encryption": "Aes256",
        "Content-Encoding": "gzip",
        "Content-Length": "10",
        "Cache-Control": "no-cache",
        "Content-Type": "text/html; charset=UTF-8",
        "Content-Disposition": "attachment",
        "Content-MD5": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
        "x-amz-storage-class": "Outposts",
        "x-amz-server-side-encryption-customer-algorithm": "Aes256",
        "bucketName": "amzn-s3-demo-bucket1",
        "Key": "path/upload.sh"
      },
      "responseElements": {
        "x-amz-server-side-encryption-customer-key-MD5": "wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
        "x-amz-server-side-encryption": "Aes256",
        "x-amz-version-id": "001",
        "x-amz-server-side-encryption-customer-algorithm": "Aes256",
        "ETag": "d41d8cd98f00b204e9800998ecf8427f"
      },
      "additionalEventData": {
        "CipherSuite": "ECDHE-RSA-AES128-SHA",
        "bytesTransferredIn": 10,
        "x-amz-id-2": "29xXQBV20
+xOHKItvzY1suLv1i6A52E0zOX159fpfsItYd58JhXwKxXAXI4IQkp6",
        "SignatureVersion": "SigV4",
        "bytesTransferredOut": 20,
        "AuthenticationMethod": "AuthHeader"
      },
      "requestID": "8E96D972160306FA",
      "eventID": "ee3b4e0c-ab12-459b-9998-0a5a6f2e4015",
      "readOnly": false,
      "resources": [
        {
          "accountId": "222222222222",
```

```
          "type": "AWS::S3Outposts::Object",
          "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/path/upload.sh"
        },
        {
          "accountId": "222222222222",
          "type": "AWS::S3Outposts::Bucket",
          "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "444455556666",
      "sharedEventID": "02759a4c-c040-4758-b84b-7cbaaf17747a",
      "edgeDeviceDetails": {
        "type": "outposts",
        "deviceId": "op-01ac5d28a6a232904"
      },
      "eventCategory": "Data"
    }
```

# Desarrollo con Amazon S3 en Outposts

Con Amazon S3 en Outposts, puede crear buckets de S3 en Outposts de AWS y almacenar y recuperar fácilmente objetos en las instalaciones para las aplicaciones que requieren acceso local a los datos, procesamiento local de los datos y residencia de los datos. S3 en Outposts proporciona una nueva clase de almacenamiento, S3 Outposts (OUTPOSTS), que utiliza las API de Amazon S3 y está diseñada para almacenar datos de manera duradera y redundante en múltiples dispositivos y servidores de AWS Outposts. Usted se comunica con su bucket de Outpost mediante un punto de acceso y una conexión de punto de conexión a través de una nube privada virtual (VPC). Puede usar las mismas API y características en los buckets de Outposts que en buckets de Amazon S3, como políticas de acceso, cifrado y etiquetado. Puede utilizar S3 en Outposts a través de la AWS Management Console, AWS Command Line Interface (AWS CLI), AWS SDK o la API de REST. Para obtener más información, consulte ¿Qué es Amazon S3 en Outposts?

Los siguientes temas proporcionan información acerca de cómo desarrollar con S3 en Outposts.

Temas



# Regiones admitidas de S3 en Outposts

S3 en Outposts se admite en las siguientes Regiones de AWS.

- Este de EE. UU. (Norte de Virginia) (us-east-1)
- Este de EE. UU. (Ohio) (us-east-2)
- EE. UU. Oeste (Norte de California) (us-west-1)
- Oeste de EE. UU. (Oregón) (us-west-2)
- África (Ciudad del Cabo) (af-south-1)
- Asia-Pacífico (Yakarta) (ap-southeast-3)
- Asia Pacífico (Bombay) (ap-south-1)
- Asia Pacific (Osaka) (ap-northeast-3)

- Asia-Pacífico (Seúl) (ap-northeast-2)
- Asia-Pacífico (Singapur) (ap-southeast-1)
- Asia-Pacífico (Sídney) (ap-southeast-2)
- Asia-Pacífico (Tokio) (ap-northeast-1)
- Canadá (centro) (ca-central-1)
- Europa (Fráncfort) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londres) (eu-west-2)
- UE (Milán) (eu-south-1)
- UE (París) (eu-west-3)
- Europa (Estocolmo) (eu-north-1)
- Israel (Tel Aviv) (il-central-1)
- Medio Oriente (Baréin) (me-south-1)
- América del Sur (São Paulo) (sa-east-1)
- AWS GovCloud (EE. UU. Este) (us-gov-east-1)
- AWS GovCloud (EE. UU. Oeste) (us-gov-west-1)

# Operaciones de la API de Amazon S3 en Outposts

En este tema, se enumeran las operaciones de la API de Amazon S3, Amazon S3 Control y Amazon S3 en Outposts que puede usar con Amazon S3 en Outposts

Temas



## Operaciones de la API de Amazon S3 para administrar objetos

S3 en Outposts está diseñado para utilizar las mismas operaciones de la API de objetos que Amazon S3. Debe utilizar puntos de acceso para acceder a cualquier objeto de un bucket de Outpost. Al utilizar una operación de API de objetos con S3 en Outposts, proporciona el Nombre de recurso de Amazon (ARN) del punto de acceso de Outposts o el alias del punto de acceso. Para obtener más

información acerca de los alias de punto de acceso, consulte Uso de un alias de estilo de bucket para su punto de acceso de bucket de S3 en Outposts.

Amazon S3 en Outposts admite las siguientes operaciones de la API de Amazon S3:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListObjectVersions
- ListParts
- PutObject
- PutObjectTagging
- UploadPart
- UploadPartCopy

## Operaciones de la API de Amazon S3 Control para administrar buckets

S3 en Outposts admite las siguientes operaciones de la API de Amazon S3 Control para trabajar con buckets.

- CreateAccessPoint
- CreateBucket

- DeleteAccessPoint
- DeleteAccessPointPolicy
- DeleteBucket
- DeleteBucketLifecycleConfiguration
- DeleteBucketPolicy
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccessPoint
- GetAccessPointPolicy
- GetBucket
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketReplication
- GetBucketTagging
- GetBucketVersioning
- ListAccessPoints
- ListRegionalBuckets
- PutAccessPointPolicy
- PutBucketLifecycleConfiguration
- PutBucketPolicy
- PutBucketReplication
- PutBucketTagging
- PutBucketVersioning

## Operaciones de la API de S3 en Outposts para administrar Outposts

S3 en Outposts admite las siguientes operaciones de la API de Amazon S3 en Outposts para administrar puntos de conexión.

- CreateEndpoint
- DeleteEndpoint
- ListEndpoints

- Listar publicaciones salientes con S3
- ListSharedEndpoints

## Configure el cliente de control de S3 para S3 en Outposts con SDK para Java

En el siguiente ejemplo, se configura el cliente de control de Amazon S3 para Amazon S3 en Outposts con AWS SDK para Java. Para utilizar este ejemplo, sustituya *`user input placeholder`* por su propia información.

```
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;

public AWSS3Control createS3ControlClient() {

    String accessKey = AWSAccessKey;
    String secretKey = SecretAccessKey;
    BasicAWSCredentials awsCreds = new BasicAWSCredentials(accessKey, secretKey);

    return AWSS3ControlClient.builder().enableUseArnRegion()
            .withCredentials(new AWSStaticCredentialsProvider(awsCreds))
            .build();

}
```

## Realización de solicitudes a S3 en Outposts mediante IPv6

Los puntos de conexión de doble pila de Amazon S3 en Outposts y S3 en Outposts permiten realizar solicitudes a buckets de S3 en Outposts con el protocolo IPv6 o IPv4. Gracias a la compatibilidad de IPv6 con S3 en Outposts, puede acceder a sus buckets y recursos del plano de control a través de las API de S3 en Outposts mediante redes IPv6.

> **Note**
>
> Las acciones de los objetos de S3 en Outposts (como `PutObject` o `GetObject`) no son compatibles con las redes IPv6.

No hay cargos adicionales por acceder a S3 en Outposts mediante redes IPv6. Para obtener más información acerca de S3 en Outposts, consulte Precios del bastidor de AWS Outposts.

Temas



## Introducción a IPv6

Para realizar una solicitud a un bucket de S3 en Outposts mediante IPv6, debe utilizar un punto de conexión de doble pila. En la siguiente sección se describe cómo hacer solicitudes mediante IPv6 con los puntos de enlace de doble pila.

A continuación se describen algunos puntos importantes a tener en cuenta antes de acceder a un bucket de S3 en Outposts mediante IPv6:

- El cliente y la red que acceden al bucket deben estar autorizados para utilizar IPv6.
- Se admiten tanto solicitudes de estilo alojamiento virtual como de tipo ruta para el acceso a IPv6. Para obtener más información, consulte Uso de puntos de conexión de doble pila en S3 en Outposts.
- Si utiliza el filtrado de direcciones IP de origen en sus políticas de bucket de S3 en Outposts o de usuario de AWS Identity and Access Management (IAM), debe actualizar las políticas para que incluyan los rangos de direcciones IPv6.

> **Note**
>
> Este requisito solo se aplica a las operaciones de buckets de S3 en Outposts y a los recursos del plano de control en redes IPv6. Las acciones de los objetos de Amazon S3 en Outposts no son compatibles con las redes IPv6.

- Cuando utiliza IPv6, los archivos de registro de acceso al servidor producen direcciones IP en un formato de IPv6. Debe actualizar el software, las herramientas y los scripts existentes que utiliza

para analizar archivos de registro de S3 en Outposts para que puedan analizar las direcciones IP remotas con formato IPv6. A continuación, las herramientas, los scripts y el software actualizados analizarán correctamente las direcciones IP remotas con formato IPv6.

## Uso de puntos de conexión de doble pila para realizar solicitudes mediante una red IPv6

Para realizar solicitudes con llamadas a la API de S3 en Outposts a través de IPv6, puede usar puntos de conexión de doble pila mediante la AWS CLI o el SDK de AWS. Las operaciones de la API de Amazon S3 Control para administrar buckets y las operaciones de la API de S3 en Outposts para administrar Outposts funcionan igual tanto si se accede a S3 en Outposts a través de un protocolo IPv6 como de un protocolo IPv4. Sin embargo, debe de tener en cuenta que las operaciones de la API de Amazon S3 en Outposts (como `PutObject` o `GetObject`) no son compatibles con las redes IPv6.

Al usar AWS Command Line Interface (AWS CLI) y los SDK de AWS, puede utilizar un parámetro o una marca para cambiar a un punto de enlace de doble pila. También puede especificar el punto de conexión de doble pila directamente como una anulación del punto de conexión de S3 en Outposts en el archivo de configuración.

Puede utilizar un punto de conexión de doble pila para acceder a un bucket de S3 en Outposts mediante IPv6 desde cualquiera de las siguientes opciones:

- La AWS CLI, consulte Usar puntos de enlace de doble pila desde la AWS CLI.
- Para los SDK de AWS, consulte Uso de los puntos de conexión de doble pila de S3 en Outposts desde los SDK de AWS.

## Uso de direcciones IPv6 en políticas de IAM

Antes de intentar acceder a un bucket de S3 en Outposts mediante un protocolo IPv6, debe asegurarse de que los usuarios de IAM o las políticas de bucket de S3 en Outposts utilizadas para el filtrado de direcciones IP estén actualizadas e incluyan los rangos de direcciones IPv6. Si las políticas de filtrado de direcciones IP no están actualizadas para gestionar direcciones IPv6, puede perder el acceso a un bucket de S3 en Outposts al intentar usar el protocolo IPv6.

Las políticas de IAM que filtran direcciones IP utilizan operadores de condición de dirección IP. La siguiente política de buckets de S3 en Outposts identifica el rango IP 54.240.143.* de las direcciones

IPv4 permitidas con operadores de condición de dirección IP. Cualquier dirección IP fuera de este rango no podrá acceder al bucket de S3 en Outposts (`DOC-EXAMPLE-BUCKET`). Dado que todas las direcciones IPv6 están fuera del rango permitido, esta política evita que las direcciones IPv6 puedan acceder a `DOC-EXAMPLE-BUCKET`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3outposts:*",
      "Resource": "arn:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/DOC-EXAMPLE-BUCKET/*",
      "Condition": {
         "IpAddress": {"aws:SourceIp": "54.240.143.0/24"}
      }
    }
  ]
}
```

Puede modificar el elemento `Condition` de la política de bucket de S3 en Outposts para permitir los rangos de direcciones IPv4 (`54.240.143.0/24`) e IPv6 (`2001:DB8:1234:5678::/64`), tal como se muestra en el siguiente ejemplo. Puede utilizar el mismo tipo de bloque `Condition` que se muestra en el ejemplo para actualizar las políticas de bucket y de usuario de IAM.

```
       "Condition": {
         "IpAddress": {
            "aws:SourceIp": [
              "54.240.143.0/24",
               "2001:DB8:1234:5678::/64"
             ]
          }
        }
```

Antes de utilizar IPv6, debe actualizar todas las políticas de bucket y de usuario de IAM; relevantes que utilizan filtrado de direcciones IP para permitir los rangos de direcciones IPv6. Le recomendamos que actualice sus políticas de IAM con los rangos de direcciones IPv6 de la organización además de los rangos de direcciones IPv4 existentes. Para ver un ejemplo de una política de bucket que permite el acceso a través de IPv6 e IPv4, consulte Restringir el acceso a direcciones IP específicas.

Puede revisar sus políticas de usuario de IAM en la consola de IAM en https://console.aws.amazon.com/iam/. Para obtener más información acerca de IAM, consulte la guía del usuario de IAM. Para obtener información sobre las políticas de buckets de S3 en Outposts, consulte Adición o edición de una política de bucket para un bucket de Amazon S3 en Outposts.

## Probar la compatibilidad de dirección IP

Si utiliza una instancia de Linux, de Unix o una plataforma macOS X, puede probar el acceso a un punto de conexión de doble pila mediante IPv6. Por ejemplo, para probar la conexión a Amazon S3 en Outposts en los puntos de conexión mediante IPv6, utilice el comando `dig`:

```
dig s3-outposts.us-west-2.api.aws AAAA +short
```

Si el punto de conexión de doble pila a través de una red IPv6 está configurado correctamente, el comando `dig` devuelve las direcciones IPv6 conectadas. Por ejemplo:

```
dig s3-outposts.us-west-2.api.aws AAAA +short

2600:1f14:2588:4800:b3a9:1460:159f:ebce

2600:1f14:2588:4802:6df6:c1fd:ef8a:fc76

2600:1f14:2588:4801:d802:8ccf:4e04:817
```

## Uso de IPv6 con AWS PrivateLink

S3 en Outposts admite el protocolo IPv6 para los servicios y puntos de conexión de AWS PrivateLink. Gracias a la compatibilidad de AWS PrivateLink con el protocolo IPv6, puede conectarse a los puntos de conexión de servicio de su VPC a través de redes IPv6, ya sea desde conexiones en las instalaciones o desde otras conexiones privadas. La compatibilidad de IPv6 con AWS PrivateLink para S3 en Outposts también le permite integrar AWS PrivateLink con puntos de conexión de doble pila. Para ver los pasos a seguir para habilitar IPv6 para AWS PrivateLink, consulte Expedite your IPv6 adoption with AWS PrivateLink services and endpoints.

> **Note**
>
> Para actualizar el tipo de dirección IP compatible de IPv4 a IPv6, consulte Modify the supported IP address type en la Guía del usuario de AWS PrivateLink.

## Uso de IPv6 con AWS PrivateLink

Si usa AWS PrivateLink con IPv6, debe crear un punto de conexión de interfaz de VPC de doble pila o de IPv6. Para ver los pasos generales a seguir para crear un punto de conexión de VPC desde la AWS Management Console, consulte Access an AWS service using an interface VPC endpoint en la Guía del usuario de AWS PrivateLink.

AWS Management Console

Utilice el siguiente procedimiento para crear un punto de conexión de VPC de interfaz que se conecte a S3 en Outposts.

1. Inicie sesión en la AWS Management Console y abra la consola de VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Service category (Categoría de servicios), elija AWSServices (Servicios de AWC).
5. En Nombre del servicio, elija el servicio S3 en Outposts (com.amazonaws.us-east-1.s3-outposts).
6. En VPC, elija la VPC desde la que accederá a S3 en Outposts.
7. En Subredes, seleccione una subred por zona de disponibilidad desde la que accederá a S3 en Outposts. No puede seleccionar varias subredes de la misma zona de disponibilidad. Por cada subred que seleccione, se creará una interfaz de red de punto de conexión nueva. De forma predeterminada, las direcciones IP de los rangos de direcciones IP de la subred se asignan a las interfaces de red de los puntos de conexión. Para designar una dirección IP para una interfaz de red de puntos de conexión, elija Designar direcciones IP e introduzca una dirección IPv6 del rango de direcciones de la subred.
8. Para Tipo de dirección IP, elija Dualstack. Asigne ambas direcciones IPv4 e IPv6 a sus interfaces de red del punto de conexión. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de direcciones IPv4 e IPv6.
9. En Grupos de seguridad, elija los grupos de seguridad para asociarlos a las interfaces de red del punto de conexión para el punto de conexión de VPC. De forma predeterminada, el grupo de seguridad predeterminado está asociado a la VPC.
10. En Política, elija Acceso completo para permitir todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión de VPC. De lo contrario, elija

Personalizar para adjuntar una política de punto de conexión de VPC que controle los permisos que tienen las entidades principales para realizar acciones en los recursos a través del punto de conexión de VPC. Esta opción solo está disponible si el servicio admite las políticas de punto de conexión de VPC. Para obtener más información, consulte Endpoint policies.

11. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
12. Seleccione Crear punto de conexión.

Example Ejemplo de política de bucket de S3 en Outposts

Para permitir que S3 en Outposts interactúe con sus puntos de conexión de VPC, puede actualizar la política de S3 en Outposts de la siguiente manera:

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3-outposts:*",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

AWS CLI

> **Note**
>
> Para habilitar la red IPv6 en su punto de conexión de VPC, debe configurar `IPv6` para el filtro `SupportedIpAddressType` para S3 en Outposts.

En el siguiente ejemplo se utiliza el comando `create-vpc-endpoint` para crear un nuevo punto de conexión de interfaz de doble pila.

```
aws ec2 create-vpc-endpoint \
--vpc-id vpc-12345678 \
```

```
--vpc-endpoint-type Interface \
--service-name com.amazonaws.us-east-1.s3-outposts \
--subnet-id subnet-12345678 \
--security-group-id sg-12345678 \
--ip-address-type dualstack \
--dns-options "DnsRecordIpType=dualstack"
```

Según la configuración del servicio de AWS PrivateLink, es posible que el proveedor de servicios de puntos de conexión de VPC deba aceptar las conexiones de punto de conexión recién creadas antes de utilizarlas. Para obtener más información, consulte Accept and reject endpoint connection requests en la Guía del usuario de AWS PrivateLink.

En el siguiente ejemplo, se usa el comando `modify-vpc-endpoint` para actualizar el punto de conexión de VPC solo para IPV por un punto de conexión de doble pila. El punto de conexión de doble pila permite acceder a las redes IPv4 e IPv6.

```
aws ec2 modify-vpc-endpoint \
--vpc-endpoint-id vpce-12345678 \
--add-subnet-ids subnet-12345678 \
--remove-subnet-ids subnet-12345678 \
--ip-address-type dualstack \
--dns-options "DnsRecordIpType=dualstack"
```

Para ver más información sobre cómo habilitar la red IPv6 para AWS PrivateLink, consulte la publicación Expedite your IPv6 adoption with AWS PrivateLink services and endpoints.

## Uso de puntos de conexión de doble pila en S3 en Outposts

Los puntos de conexión de doble pila de S3 en Outposts permiten realizar solicitudes a los buckets de S3 en Outposts a través de IPv6 y de IPv4. En esta sección se describe cómo utilizar los puntos de conexión de doble pila de S3 en Outposts.

Temas

- Puntos de conexión de doble pila de S3 en Outposts
- Usar puntos de enlace de doble pila desde la AWS CLI
- Uso de los puntos de conexión de doble pila de S3 en Outposts desde los SDK de AWS

## Puntos de conexión de doble pila de S3 en Outposts

Cuando realiza una solicitud a un punto de conexión de doble pila, la URL del bucket de S3 en Outposts resulta en una dirección IPv6 o IPv4. Para obtener más información acerca de un bucket de S3 en Outposts mediante IPv6, consulte Realización de solicitudes a S3 en Outposts mediante IPv6.

Para obtener acceso a un bucket de S3 en Outposts mediante un punto de conexión de doble pila, use un nombre de punto de conexión de tipo ruta. S3 en Outposts solo admite nombres de puntos de conexión de doble pila regionales, por lo que debe especificar la región dentro del nombre.

Los puntos de conexión FIPS de doble pila de tipo ruta utilizan la siguiente convención de nomenclatura:

```
s3-outposts-fips.region.api.aws
```

Los puntos de conexión FIPS que no son de doble pila utilizan la siguiente convención de nomenclatura:

```
s3-outposts.region.api.aws
```

> **Note**
>
> Los nombres de punto de conexión de tipo de alojamiento virtual no son compatibles con S3 en Outposts.

## Usar puntos de enlace de doble pila desde la AWS CLI

Esta sección proporciona ejemplos de comandos de la AWS CLI. que se usan para realizar solicitudes a un punto de conexión de doble pila. Para obtener instrucciones acerca de cómo configurar la AWS CLI, consulte Introducción mediante AWS CLI y SDK para Java.

Puede establecer el valor de configuración `use_dualstack_endpoint` en `true` en un perfil de su archivo de AWS Config para dirigir todas las solicitudes de Amazon S3 que realicen los comandos `s3` y `s3api` de la AWS CLI al punto de conexión de doble pila para la región especificada. Puede especificar la región en el archivo de configuración o en un comando utilizando la opción `--region`.

Si utiliza puntos de conexión de doble pila con la AWS CLI, solo se admiten los estilos de direccionamiento `path`. El estilo de direccionamiento configurado en el archivo de configuración

determina si el nombre del bucket está en el name de host o en la URL. Para obtener más información, consulte s3outposts en la Guía del usuario de AWS CLI.

Para usar un punto de conexión de doble pila mediante la AWS CLI, utilice el parámetro `--endpoint-url` junto con el punto de conexión `http://s3.dualstack.region.amazonaws.com` o `https://s3-outposts-fips.region.api.aws` para cualquiera de los comandos `s3control` o `s3outposts`.

Por ejemplo:

```
$  aws s3control list-regional-buckets --endpoint-url https://s3-
outposts.region.api.aws
```

## Uso de los puntos de conexión de doble pila de S3 en Outposts desde los SDK de AWS

En esta sección, se proporcionan ejemplos de cómo obtener acceso a un punto de enlace de doble pila con los SDK de AWS.

AWS SDK for Java 2.xEjemplo de punto de enlace de doble pila con

En el siguiente ejemplo se muestra cómo usar las clases `S3ControlClient` y `S3OutpostsClient` para habilitar puntos de conexión de doble pila al crear un cliente S3 en Outposts con AWS SDK for Java 2.x. Para obtener instrucciones sobre cómo crear y probar un ejemplo de Java funcional para Amazon S3 en Outposts, consulte Introducción mediante AWS CLI y SDK para Java.

Example — Crear una clase de **`S3ControlClient`** con los puntos de conexión de doble pila habilitados

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsRequest;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsResponse;
import software.amazon.awssdk.services.s3control.model.S3ControlException;


public class DualStackEndpointsExample1 {
```

```
    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");
        String accountId = "111122223333";
        String navyId = "9876543210";

        try {
            // Create an S3ControlClient with dual-stack endpoints enabled.
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                                                             .region(clientRegion)
                                                             .dualstackEnabled(true)
                                                             .build();
            ListRegionalBucketsRequest listRegionalBucketsRequest =
 ListRegionalBucketsRequest.builder()

       .accountId(accountId)

       .outpostId(navyId)

       .build();

            ListRegionalBucketsResponse listBuckets =
 s3ControlClient.listRegionalBuckets(listRegionalBucketsRequest);
            System.out.printf("ListRegionalBuckets Response: %s%n",
 listBuckets.toString());
       } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 on Outposts
 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
       }
       catch (S3ControlException e) {
            // Unknown exceptions will be thrown as an instance of this type.
            e.printStackTrace();
       } catch (SdkClientException e) {
            // Amazon S3 on Outposts couldn't be contacted for a response, or the
 client
            // couldn't parse the response from Amazon S3 on Outposts.
            e.printStackTrace();
       }
    }
}
```

Example — Crear un **`S3OutpostsClient`** con los puntos de conexión de doble pila habilitados

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3outposts.S3OutpostsClient;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsRequest;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsResponse;
import software.amazon.awssdk.services.s3outposts.model.S3OutpostsException;


public class DualStackEndpointsExample2 {

    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");

        try {
            // Create an S3OutpostsClient with dual-stack endpoints enabled.
            S3OutpostsClient s3OutpostsClient = S3OutpostsClient.builder()
                                                                .region(clientRegion)
                                                                .dualstackEnabled(true)
                                                                .build();
            ListEndpointsRequest listEndpointsRequest =
 ListEndpointsRequest.builder().build();

            ListEndpointsResponse listEndpoints =
 s3OutpostsClient.listEndpoints(listEndpointsRequest);
            System.out.printf("ListEndpoints Response: %s%n",
 listEndpoints.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 on Outposts
 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        }
        catch (S3OutpostsException e) {
            // Unknown exceptions will be thrown as an instance of this type.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 on Outposts couldn't be contacted for a response, or the
 client
            // couldn't parse the response from Amazon S3 on Outposts.
            e.printStackTrace();
        }
```

```
    }
}
```

Si utiliza AWS SDK for Java 2.x en Windows, es probable que tenga que configurar adecuadamente la siguiente propiedad de la máquina virtual Java (JVM):

```
java.net.preferIPv6Addresses=true
```