Establecer barandas y monitorear las URL prefirmadas

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Establecer barandas y monitorear las URL prefirmadas

Table of Contents

Establecer barandas y monitorear los prefirmados URLs

Ryan Baker, Amazon Web Services (AWS)

Agosto de 2025 (historial del documento)

La seguridad es una preocupación fundamental para todas las empresas y un pilar clave del AWS Well-Architected Framework. Como ingeniero de seguridad, querrá implementar barreras administrativas que estén alineadas con los requisitos de control de la organización. En el AWS Well-Architected Framework, las barandas definen los límites que limitan la actividad.

Esta guía proporciona información básica y prácticas recomendadas para el uso de objetos prefirmados URLs, que se utilizan con los objetos de Amazon Simple Storage Service (Amazon S3). Los prefirmados URLs permiten a los usuarios o aplicaciones que tienen acceso a credenciales válidas generar solicitudes que se firman previamente y se aceptan hasta un tiempo de caducidad definido. Un caso de uso común de las prefirmadas URLs es ampliar el acceso a los objetos o recursos mediante el uso compartido de estas solicitudes. Las solicitudes prefirmadas compartidas las generan sistemas o usuarios que tienen los derechos para realizar una solicitud específica y, a continuación, pueden enviarse a otros sistemas o usuarios para ampliar la capacidad de realizar esa misma solicitud.

En esta guía, aprenderá lo siguiente:

- Los conceptos de prefirmado URLs
- Casos de uso de prefirmado URLs
- Barandillas recomendadas y opcionales
- Opciones de monitoreo
- Ejemplos de cómo usar las prefirmadas Servicios de AWS URLs

Destinatarios previstos

Esta guía se ha diseñado para arquitectos e ingenieros de seguridad responsables de implementar los controles de seguridad en la Nube de AWS.

Objetivos

Como ingeniero de seguridad, querrá saber cómo los creadores de soluciones implementan la seguridad y el tipo de acceso que tienen sus usuarios finales. En esta guía se describe un tipo de acceso, prefirmado URLs, que suele utilizarse con Amazon S3. Los prefirmados URLs ofrecen a los desarrolladores opciones para unir de manera eficiente los mecanismos de autenticación.

En Amazon S3, las solicitudes prefirmadas URLs representan una categoría única de solicitudes. Los ingenieros de seguridad pueden supervisar y gestionar estas solicitudes para garantizar que se utilicen únicamente cuando sea adecuado y necesario. El objetivo de esta guía es ayudar a los ingenieros de seguridad a proporcionar este tipo de supervisión de alto nivel.

Después de leer esta guía, debe comprender qué es una URL prefirmada, cuándo se usa normalmente y las motivaciones para su uso.

Requisitos previos

Si su empresa no ha definido una política de seguridad, objetivos de control o estándares, tal como se describe en la guía Implementación de controles de seguridad en AWS, le recomendamos que complete esas tareas de gobierno antes de continuar con esta guía.

Antes de empezar, también debe familiarizarse con las prácticas recomendadas y opcionales de control y supervisión. Para obtener más información, consulte lo siguiente:

- Políticas de control de servicios (AWS Organizations documentación)
- Políticas de control de recursos (AWS Organizations documentación)
- Políticas de bucket para Amazon S3 (documentación de Amazon S3)
- Registro de solicitudes con registro de acceso al servidor (documentación de Amazon S3)
- Registro de llamadas a la API de Amazon S3 mediante AWS CloudTrail (documentación de Amazon S3)

Descripción general de los prefirmados URLs

Una URL prefirmada es un tipo de solicitud HTTP que reconoce el servicio AWS Identity and Access Management (IAM). Lo que diferencia a este tipo de solicitud de todas las demás es el AWS X-Amz-Expires parámetro de consulta. Al igual que con otras solicitudes autenticadas, las solicitudes de URL prefirmadas incluyen una firma. En el caso de las solicitudes de URL prefirmadas, esta firma se transmite en. `X-Amz-Signature` La firma utiliza las operaciones criptográficas de la versión 4 de Signature para codificar todos los demás parámetros de la solicitud.

> **Notas**
>
> - La versión 2 de Signature se encuentra actualmente en proceso de quedar obsoleta, pero algunas todavía la admiten. Regiones de AWS Esta guía se aplica a la firma de la versión 4 de Signature.
> - El servicio de recepción podría procesar encabezados sin firmar, pero el soporte para esa opción es limitado y específico, de acuerdo con las mejores prácticas. A menos que se indique lo contrario, suponga que todos los encabezados deben estar firmados para que se acepte una solicitud.

El `X-Amz-Expires` parámetro permite procesar una firma como válida con una desviación mayor de la fecha y hora codificada. Aún se están evaluando otros aspectos de la validez de la firma. Las credenciales de firma, si son temporales, no deben caducar en el momento en que se procese la firma. Las credenciales de firma deben adjuntarse a un director de IAM que cuente con la autorización suficiente en el momento del procesamiento.

Las prefirmadas URLs son un subconjunto de solicitudes prefirmadas

Una URL prefirmada no es el único método para firmar una solicitud en el futuro. Amazon S3 también admite solicitudes POST, que también suelen estar prefirmadas. Una firma POST prefirmada permite realizar cargas que cumplan con una política firmada y que tenga una fecha de caducidad incluida en dicha política.

Las firmas de las solicitudes pueden estar fechadas en el futuro, aunque esto es poco común. Mientras las credenciales subyacentes sean válidas, el algoritmo de firma no prohíbe las citas futuras. sin embargo, estas solicitudes no se pueden procesar correctamente hasta su período de

tiempo válido, lo que hace que las citas futuras no sean prácticas para la mayoría de los casos de uso.

¿Qué permite una solicitud prefirmada?

Una solicitud prefirmada solo puede permitir acciones que estén permitidas por las credenciales que se usaron para firmar la solicitud. Si las credenciales deniegan implícita o explícitamente la acción especificada en la solicitud prefirmada, la solicitud prefirmada se deniega cuando se envía. Esto se aplica a lo siguiente:

- Políticas de sesión asociadas a las credenciales
- Políticas basadas en la identidad que están asociadas al principal que está asociado a las credenciales
- Políticas de recursos que afectan a la sesión o al director
- Políticas de control de servicios que afectan a la sesión o al principal
- Políticas de control de recursos que afectan a la sesión o al director

Motivaciones para usar solicitudes prefirmadas

Como ingeniero de seguridad, debe saber qué es lo que motiva a los desarrolladores de soluciones a usar prefirmados. URLs Entender lo que es necesario y lo que es opcional le ayudará a comunicarse con los creadores de soluciones. Las motivaciones pueden incluir las siguientes:

- Respaldar un mecanismo de autenticación que no sea de IAM y, al mismo tiempo, beneficiarse de la escalabilidad de Amazon S3. Una de las principales motivaciones es comunicarse directamente con Amazon S3 para aprovechar la escalabilidad integrada que ofrece este servicio. Sin esta comunicación directa, una solución tendría que soportar la carga que supone la retransmisión de los bytes que se envían PutObjecty GetObjectlas llamadas. En función de la carga total, este requisito añade desafíos de escalado que un creador de soluciones podría querer evitar.

  Es posible que otros medios de comunicación directa con Amazon S3, como el uso de credenciales temporales en AWS Security Token Service (AWS STS) o firmas Signature Version 4 en el exterior URLs, no sean adecuados para su caso de uso. Amazon S3 identifica a los usuarios mediante AWS credenciales, mientras que las solicitudes prefirmadas suponen la identificación mediante mecanismos distintos AWS de las credenciales. Se puede salvar esta diferencia y, al mismo tiempo, mantener la comunicación directa de los datos mediante solicitudes prefirmadas.

- Para beneficiarse de la comprensión nativa de un navegador sobre. URLs URLs los navegadores las entienden, mientras que AWS STS las credenciales y las firmas Signature Version 4 no. Esto resulta beneficioso cuando se integra con soluciones basadas en navegadores. Las soluciones alternativas requieren más código, utilizan más memoria para archivos de gran tamaño y pueden recibir un tratamiento diferente con extensiones como los escáneres de malware y virus.

Comparación con credenciales temporales AWS STS

Las credenciales temporales son similares a las solicitudes prefirmadas. Ambos caducan, permiten establecer el alcance del acceso y se suelen utilizar para vincular las credenciales que no son de IAM con el uso que requiere credenciales de AWS.

Puede limitar estrictamente una AWS STS credencial temporal a un único objeto y acción de S3, pero esto puede provocar problemas de escalamiento, ya que tiene límites. AWS STS APIs (Para obtener más información, consulte el artículo Cómo resolver la limitación de API o los errores de «tasa excedida» para IAM y en AWS STS el sitio web de AWS Re:post). Además, cada credencial generada requiere una llamada a la AWS STS API, lo que añade latencia y crea una nueva dependencia que podría afectar a la resiliencia. Una AWS STS credencial temporal también tiene un tiempo de caducidad mínimo de 15 minutos, mientras que una solicitud prefirmada puede admitir duraciones más cortas (60 segundos es práctico si se dan las condiciones adecuadas).

Comparación con soluciones que solo utilizan firmas

El único componente intrínsecamente secreto de una solicitud prefirmada es su firma de la versión 4 de firma. Si un cliente conoce los demás detalles de una solicitud y se le proporciona una firma válida que coincide con esos detalles, puede enviar una solicitud válida. Sin una firma válida, no puede hacerlo.

Las soluciones prefirmadas URLs y las de solo firma son criptográficamente similares. Sin embargo, las soluciones que solo utilizan firmas tienen ventajas prácticas, como la posibilidad de utilizar un encabezado HTTP en lugar de un parámetro de cadena de consulta para transmitir la firma (consulte la sección sobre el registro de interacciones y mitigaciones). Los administradores también deben tener en cuenta que las cadenas de consulta se tratan más comúnmente como metadatos, mientras que los encabezados se tratan con menos frecuencia como tales.

Por otro lado, AWS SDKs ofrecen menos soporte para generar y usar firmas directamente. La creación de una solución que solo utilice firmas requiere más código personalizado. Desde una perspectiva práctica, el uso de bibliotecas en lugar de código personalizado por motivos de

seguridad es una buena práctica general, por lo que el código para las soluciones que solo utilizan firmas requiere un análisis más exhaustivo.

Las soluciones que solo utilizan firmas no utilizan la cadena de `X-Amz-Expires` consulta ni proporcionan ningún período de validez explícito. IAM gestiona los períodos de validez implícita de las firmas que no tienen una fecha de caducidad explícita. Esos períodos implícitos no se publican. No suelen cambiar, pero se administran teniendo en cuenta la seguridad, por lo que no debes depender de los períodos de validez. Existe un equilibrio entre tener un control explícito sobre la fecha de caducidad y dejar que IAM gestione la caducidad.

Como administrador, es posible que prefiera una solución que solo utilice firmas. Sin embargo, en un sentido práctico, necesitará respaldar las soluciones tal como están diseñadas.

Identificación de solicitudes prefirmadas

Identificar las solicitudes que utilizaban una URL prefirmada

Amazon S3 proporciona dos mecanismos integrados para supervisar el uso a nivel de solicitud: los registros de acceso al servidor Amazon S3 y AWS CloudTrail los eventos de datos. Ambos mecanismos pueden identificar el uso de URL prefirmadas.

Para filtrar los registros en función del uso de URL prefirmadas, puede utilizar el tipo de autenticación. Para los registros de acceso al servidor, examine el campo Tipo de autenticación, que normalmente se denomina authtype cuando se define en una tabla de Amazon Athena. Para CloudTrail, examine AuthenticationMethoden el `additionalEventData` campo. En ambos casos, el valor del campo para las solicitudes que utilizan direcciones URL prefirmadas es`QueryString`, mientras que `AuthHeader` es el valor para la mayoría de las demás solicitudes.

`QueryString`el uso no siempre está asociado a las URL prefirmadas. Para restringir la búsqueda únicamente al uso de URL prefirmadas, busca las solicitudes que contengan el parámetro de cadena de consulta. `X-Amz-Expires` Para los registros de acceso al servidor, examina el URI de la solicitud y busca las solicitudes que tengan un `X-Amz-Expires` parámetro en la cadena de consulta. Para CloudTrail, examine el `requestParameters` elemento en busca de un `X-Amz-Expires` elemento.

```
{"Records": [{…, "requestParameters": {…, "X-Amz-Expires": "300"}}, …]}
```

La siguiente consulta de Athena aplica este filtro:

```
SELECT * FROM {athena-table} WHERE
  authtype = 'QueryString' AND
  request_uri LIKE '%X-Amz-Expires=%';
```

Para AWS CloudTrail Lake, la siguiente consulta aplica este filtro:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'QueryString' AND
  requestParameters['X-Amz-Expires'] IS NOT NULL
```

Identificar otros tipos de solicitudes prefirmadas

La solicitud POST también tiene un tipo de autenticación únicoHtmlForm, en los registros de acceso al servidor Amazon S3 y CloudTrail. Este tipo de autenticación es menos común, por lo que es posible que no encuentre estas solicitudes en su entorno.

La siguiente consulta de Athena aplica el filtro para: HtmlForm

```
SELECT * FROM {athena-table} WHERE
  authtype = 'HtmlForm';
```

En el caso de CloudTrail Lake, la siguiente consulta aplica el filtro:

```
SELECT * FROM {data-store-event-id} WHERE
  additionalEventData['AuthenticationMethod'] = 'HtmlForm'
```

Identificar los patrones de solicitud

Puede encontrar las solicitudes prefirmadas mediante las técnicas descritas en la sección anterior. Sin embargo, para que esos datos sean útiles, querrás buscar patrones. TOP 10Los resultados simples de la consulta pueden proporcionarte una idea, pero si eso no es suficiente, usa las opciones de agrupación de la siguiente tabla.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
Agente usuario	GROUP BY useragent	GROUP BY userAgent	Esta opción de agrupación le ayuda a encontrar el origen y el propósito de las solicitudes. El agente de usuario lo proporciona el usuario y no es fiable como mecanismo de autenticación o autorización. Sin

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			embargo, puede revelar muchas cosas si se buscan patrones, ya que la mayoría de los clientes utilizan una cadena única que es, al menos parcialmente, legible por humanos.
Solicitante	`GROUP BY requester`	`GROUP BY userIdentity['arn']`	Esta opción de agrupación ayuda a encontrar a los directores de IAM que firmaron las solicitudes. Si su objetivo es bloquear estas solicitudes o crear una excepción para las solicitudes existentes, estas consultas proporcionan suficiente información para ello. Si utilizas los roles de acuerdo con las mejores prácticas de IAM, el rol tiene un propietario claramente identificado y puedes usar esa información para obtener más información.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
Dirección IP de origen	`GROUP BY remoteip`	`GROUP BY sourceIPAddress`	Esta opción se agrupa por el último salto de traducción de red antes de llegar a Amazon S3. • Si el tráfico pasa por una puerta de enlace NAT, esta será la dirección de la puerta de enlace NAT. • Si el tráfico pasa por una puerta de enlace de Internet, será la dirección IP pública que envió el tráfico a la puerta de enlace de Internet. • Si el tráfico se origina desde fuera AWS, será la dirección pública de Internet asociada al origen. • Si pasa por un punto final de nube privada virtual (VPC) de puerta

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			de enlace, será la dirección IP de la instancia en la VPC. • Si pasa a través de una interfaz virtual pública (VIF), será la IP local del solicitante o de cualquier intermediario, como un servidor proxy o un firewall, que solo exponga su dirección IP. • Si pasa a través de un punto final de la VPC de la interfaz, podría ser la dirección IP de una instancia de la VPC. También puede ser una dirección IP de otra VPC o de una red local. Al igual que ocurre con los VIF públicos, puede ser la dirección IP de cualquier intermediario.

Opción de agrupamiento	Registros de acceso al servidor	CloudTrailLago	Descripción
			Estos datos son útiles si su objetivo es imponer controles de red. Puede que tengas que combinar esta opción con datos como `endpoint` (para los registros de acceso al servidor) o `vpcEndpointId` (para CloudTrail Lake) para aclarar la fuente, ya que diferentes redes pueden duplicar las direcciones IP privadas.
Nombre del bucket de S3	`GROUP BY bucket_name`	`GROUP BY requestParameters['bucketName']`	Esta opción de agrupación ayuda a encontrar los depósitos que recibieron solicitudes. Esto le ayuda a identificar la necesidad de excepciones.

Mejores prácticas para usar solicitudes prefirmadas

En esta sección se describen las prácticas recomendadas para el uso de solicitudes prefirmadas que un ingeniero de seguridad debería tener en cuenta. Las directrices incluyen:

- Las mejores prácticas fundamentales, que son prácticas que toda organización debe seguir.
- Restricciones adicionales, prácticas que debería tener en cuenta, pero que podría decidir implementar parcialmente o con excepciones. Su objetivo es proporcionar un control y una defensa adicionales en profundidad, pero deben equilibrarse teniendo en cuenta la complejidad general.
- Registra las interacciones, que pueden ser el resultado de dispositivos o servicios que son parte de tu responsabilidad o la de tu cliente en el modelo de responsabilidad compartida. Esta sección incluye precauciones para limitar la información a la que se puede acceder a través de los registros.

Prácticas recomendadas fundamentales

Las mejores prácticas generales que son controles efectivos para otras solicitudes de AWS API también se aplican a las solicitudes prefirmadas. En esta sección, se analizan dos de las prácticas más relevantes: los privilegios mínimos y los perímetros de datos. Estas prácticas crean una profundidad de controles que otras prácticas amplían.

Aplicación del principio de privilegios mínimos

El primer paso para limitar el uso de solicitudes prefirmadas es limitar el acceso a Amazon S3 en general. Una URL prefirmada no puede proporcionar acceso a recursos que no se hayan otorgado a la entidad principal que generó la firma de la URL prefirmada. Tampoco puede proporcionar acceso a un recurso de una manera que no se haya otorgado a ese director. Por lo tanto, aplicar las mejores prácticas para conceder a esos directores el menor privilegio es una barrera eficaz.

El proceso de creación de una URL prefirmada es una operación algorítmica que se basa en un estándar publicado (Signature versión 4) para la generación de firmas. Por lo tanto, no es posible poner límites a la generación de URL prefirmadas. Sin embargo, para que sea relevante, una URL prefirmada debe ser válida y proporcionar acceso a los recursos, por lo que la validez de una URL prefirmada también es una barrera eficaz.

Para obtener más información sobre los privilegios mínimos, consulte Otorgar acceso con privilegios mínimos en el pilar de seguridad del AWS Well-Architected Framework.

Implemente un perímetro de datos

Una extensión de privilegios mínimos es mantener un perímetro de datos que sea coherente con las necesidades de su organización. Las URL prefirmadas son compatibles con los perímetros de datos. Al igual que con otras solicitudes, la validez de una solicitud de URL prefirmada se evalúa en el momento de la solicitud. Si las propiedades de la red, el recurso, la sesión de rol y el principal cambian, se evalúan en el momento y mediante el método con el que se recibe la solicitud.

Por ejemplo, supongamos que un servicio que se ejecuta en un contenedor de Amazon Elastic Kubernetes Service (Amazon EKS) firma una solicitud. La solicitud se envía posteriormente desde el sistema informático personal del usuario que está conectado a Internet. En este caso, la SourceIp condición aws: evalúa la dirección IP pública visible de la solicitud del sistema personal del usuario, no la dirección IP del servicio en el contenedor EKS de Amazon.

Del mismo modo, si las etiquetas del principal o recurso cambian antes de que se envíe la solicitud, los valores actualizados, no los originales, se aplicarán a la solicitud mediante las ResourceTag/tag-key condiciones aws: PrincipalTag/tag-key y aws:.

Barandillas adicionales

Cuando los creadores de soluciones y los usuarios utilizan adecuadamente las solicitudes prefirmadas, proporcionan un mecanismo seguro para que los usuarios accedan a los datos. Además, la capacidad de generar solicitudes prefirmadas no proporciona a los directores un acceso que aún no tenían.

En ese contexto, ¿son necesarios controles adicionales? La justificación de los controles adicionales no se basa en la necesidad de denegar el acceso, sino en ofrecer la posibilidad de supervisar, aprobar el uso y establecer límites, además de reducir el riesgo de que los usuarios cometan errores. De esta forma, puede ayudar a garantizar que el uso sea adecuado y necesario.

Las siguientes barandillas le ayudan a lograr este objetivo. Antes de activar estos controles, es posible que desee determinar el uso actual identificando las solicitudes prefirmadas. Esta identificación le ayuda a prepararse para el impacto de la barandilla en el uso actual o a planificar excepciones cuando sea necesario.

Barandilla para S3: Signature Age

Una característica que define a las solicitudes prefirmadas es que describen un tiempo de caducidad. La firma de la solicitud contiene una fecha. Esta fecha se transmite como parámetro de cadena de

`X-Amz-Date` consulta para las URL prefirmadas y como encabezado Date o x-amz-date para las POST prefirmadas.

Amazon S3 proporciona una clave de condición, s3:SignatureAge, que puede utilizar para limitar el tiempo máximo entre la fecha de firma y el vencimiento efectivo de la solicitud. Esta condición nunca puede aumentar el período de validez, pero sí puede reducirlo.

En la siguiente política, la clave de `s3:signatureAge` condición limita las solicitudes prefirmadas a 15 minutos de validez. Todos los ejemplos siguientes utilizan 15 minutos para limitar la validez a un período de tiempo similar al que admite la firma estándar.

La segunda declaración de la política deniega cualquier acceso a la versión 2 de Signature. Esta versión del protocolo de firma está en desuso, pero algunas Regiones de AWS aún la admiten. Le recomendamos que la bloquee de forma explícita antes de que quede totalmente obsoleta.

Puede aplicar la siguiente política como política de control de AWS Organizations servicios (SCP). Los usuarios pueden seguir utilizando solicitudes prefirmadas e implementar soluciones que dependan de esas solicitudes, siempre que el tiempo entre la generación de la firma y el uso sea inferior a 15 minutos. Según la implementación, es posible que esta limitación no tenga ningún impacto, que una solución quede inutilizable o que se produzcan errores ocasionales que se puedan volver a intentar.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        }
      }
    },
    {
      "Sid": "DenySignatureVersion2",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
           "s3:signatureversion": "AWS"
        }
      }
    }
  ]
}
```

Excepciones

Si una solución requiere más tiempo antes de caducar y, por lo tanto, se ve afectada por la política anterior, le recomendamos que proporcione un método para aprobar las excepciones. Para evitar enumerar las excepciones en un SCP, utilice aws: PrincipalTag, como en la siguiente política, para gestionar las excepciones de forma escalable. Otros AWS ejemplos, como los ejemplos de políticas perimetrales de datos de AWS, utilizan esta estrategia.

Si implementa una política de excepciones mediante el usoaws:PrincipalTag, debe controlar el acceso a las etiquetas de configuración en las entidades principales. Las etiquetas de este tipo pueden provenir directamente de los directores y pueden ser controladas por un SCP, como en este ejemplo de control de los valores de las etiquetas que se pueden establecer. Una etiqueta de este tipo también puede provenir de etiquetas de sesión, que establece un proveedor de identidad (IdP) o cuando se utilizan. AWS STS Controlar el acceso a aws:PrincipalTag es un tema complejo. Sin embargo, una organización que tenga experiencia en el uso del control de acceso basado en atributos (ABAC) tendrá la experiencia y los controles necesarios para permitir el uso adecuado en este caso de aws:PrincipalTag uso.

En el siguiente ejemplo, la aws:PrincipalTag condición crea una excepción que permite asignar y establecer a cualquier principal con la etiqueta denominada (long-presigned-allowed). true Con esta excepción, no se aplica la restricción de antigüedad de la firma.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15Minutes",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
```

```
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    }
  ]
}
```

Políticas de buckets

Puede aplicar políticas de bucket a todos los buckets o a algunos de ellos mediante una política como la que se muestra en el siguiente ejemplo. A diferencia de una SCP, una política de bucket también se centra en el uso principal del servicio. El apéndice A no documenta ningún uso principal esperado de las solicitudes prefirmadas, pero si quisieras implementar un control para demostrar ese límite, la siguiente política proporcionaría ese control. Además, a diferencia de un SCP, se puede aplicar una política de grupos a los principales de tu cuenta de administración.

ABAC-based las excepciones funcionan en las políticas de bucket de la misma manera que en un SCP. El objetivo de una política agrupada podría ser aplicarla a los directores ajenos a la organización, por lo que las excepciones de la ABAC deberían limitarse a los directores a los que se aplican los controles de la ABAC.

En el siguiente ejemplo, la `aws:PrincipalTag` condición de la primera declaración crea una excepción para un director con la etiqueta denominada (`long-presigned-allowed`) asignada y establecida en. `true` Con esta excepción, no se aplica la restricción de antigüedad de la firma. La segunda declaración aplica esta restricción a todos los directores ajenos a la AWS organización propietaria del depósito. El alcance de esta segunda declaración debe coincidir con los controles de ABAC para establecer la etiqueta nombrada para los directores.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
```

```
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true"
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Políticas de control de recursos

Puede aplicar una política a los depósitos a escala mediante políticas de control de recursos (RCP). Al igual que los SCP y a diferencia de las políticas de compartimentos, los RCP no se centran en el uso principal del servicio. Los RCP afectan a los directores que no son de servicio de cualquier cuenta, pero no afectan a los recursos de la cuenta de administración. Para obtener más información, consulte la Documentación de AWS Organizations.

Al igual que ocurre con las políticas de grupos, si suele `aws:PrincipalTags` crear excepciones para los principales, tenga en cuenta el alcance de los controles de ABAC sobre el etiquetado de los principales.

El siguiente RCP restringe el uso de URL prefirmadas en todos los segmentos de S3 de una organización al limitar la antigüedad de las firmas a 15 minutos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyPresignedOver15MinWithExceptions",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalTag/long-presigned-allowed": "true",
        }
      }
    },
    {
      "Sid": "DenyPresignedOver15MinutesOutsideOrg",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::*/*",
      "Condition": {
        "NumericGreaterThan": {
          "s3:signatureAge": "900000"
        },
        "StringNotEquals": {
          "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
        }
      }
    }
  ]
}
```

Guardrail para S3: AuthType

Las URL prefirmadas utilizan la autenticación mediante cadenas de consulta y las POST prefirmadas siempre utilizan la autenticación POST. Amazon S3 admite la denegación de solicitudes en función del tipo de autenticación mediante la clave de condición s3:AuthType. `REST-QUERY-STRING`es el `s3:authType` valor de las cadenas de consulta y `POST` es el `s3:authType` valor de POST.

Puede aplicar la siguiente política como SCP. La política se utiliza `s3:authType` para permitir únicamente la autenticación basada en encabezados. También configura un método para proporcionar excepciones a usuarios o roles individuales.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

La denegación de solicitudes en función del tipo de autenticación afecta a cualquier solución o función que utilice el tipo de autenticación denegada. Por ejemplo, la denegación `REST-QUERY-STRING` impide que los usuarios realicen cargas o descargas desde la consola Amazon S3. Si desea que los usuarios utilicen la consola Amazon S3, no utilice esta barandilla o haga una excepción para los usuarios. Por otro lado, si no quiere que los usuarios usen la consola Amazon S3, puede denegársela a `REST-QUERY-STRING` los usuarios.

Quizás ya deniegue a los usuarios el acceso directo a los recursos de Amazon S3. En este caso, una barrera para el tipo de autenticación es redundante. Sin embargo, una sentencia de `s3:authType` denegación proporciona una utilidad de defensa exhaustiva, ya que las implementaciones para denegar el acceso directo suelen incluir muchas sentencias de control, algunas con excepciones.

Los roles que se utilizan para las cargas de trabajo no suelen necesitar acceso a la cadena de consulta ni a la autenticación. `POST` Las excepciones son las funciones que respaldan los servicios diseñados para usar solicitudes prefirmadas. Puede crear excepciones específicas para esas funciones.

También puedes aplicar una política de grupos a todos los grupos o a algunos de ellos mediante una política como la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        }
      }
    }
  ]
}
```

Esta política de segmentos tiene el efecto de denegar el uso de las UploadPartCopyAPI CopyObjecty para realizar copias entre regiones. La replicación de Amazon S3 no se ve afectada porque no depende de estas API.

Si desea utilizar una política de bucket como la política anterior y seguir siendo compatible con la UploadPartCopyAPI CopyObjecto entre regiones, añada una condición `aws:ViaAWSService` similar a la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyNonHeaderAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::{bucket-name}/*",
      "Condition": {
        "StringNotEquals": {
          "s3:authType": "REST-HEADER",
          "aws:PrincipalTag/non-header-auth-allowed": "true"
        },
        "Bool": {
```

```
          "aws:ViaAWSService": "false"
        },
      }
    }
  ]
}
```

Combinación de barandas prefirmadas y excepciones a otras barandillas

Si no tiene previsto aplicar una barrera de protección en general a sus usuarios y funciones, puede que le interese aplicarla a las excepciones de otras barreras de protección comunes, de forma que esas excepciones no admitan las solicitudes prefirmadas.

Si tienes restricciones de red, pero permites excepciones para socios externos o para casos de uso especiales, debes bloquear la cadena de consulta o la `POST` autenticación cuando se apliquen esas excepciones, a menos que se identifique específicamente que son obligatorias.

Limitaciones de S3: SignatureAge

A los administradores les resultará útil comprender sus implicaciones con mayor detalle. `s3:signatureAge` Cada solicitud firmada incluye`X-Amz-Date`, en la que se debe indicar, la hora actual. Este valor lo rellenan el cliente y el firmante de la solicitud. AWS rechaza las solicitudes que considera que tienen tiempos no válidos. Sin embargo, un firmante podría generar firmas por adelantado en future time. Amazon S3 rechaza las solicitudes que especifiquen una hora futura si se envían con demasiada antelación. Sin embargo, si la solicitud no se envía hasta el momento en que se inicia sesión en la firma, la firma podría generarse antes y enviarse más tarde.

`s3:signatureAge`limita la antigüedad máxima de `X-Amz-Date` una firma solo para las solicitudes prefirmadas. Se rechazan las solicitudes con una antigüedad superior a la especificada, incluso si han caducado `X-Amz-Expires` o si una `POST` política las hubiera declarado válidas. `s3:signatureAge`no cambia el período de validez de las solicitudes que no incluyen un vencimiento explícito. Tampoco controla el valor `X-Amz-Date` que un cliente utiliza como firma.

Si el reloj del sistema es incorrecto o si un cliente solicita intencionalmente fechas futuras, es posible que la hora firmada no sea la hora en que se generó la firma. Esto limita en qué medida `s3:signatureAge` pueden controlar las soluciones. Una solución que utiliza la hora actual para generar firmas está limitada de la forma esperada: las firmas siguen siendo válidas durante el número de milisegundos especificado en`s3:signatureAge`. Una solución que no utilice la hora actual tendrá límites diferentes. Una restricción es que las credenciales que se usaron para firmar la firma deben seguir siendo válidas. Como administrador, puede controlar la validez máxima de

las credenciales temporales emitidas. Puede permitir que las credenciales sean válidas durante un máximo de 36 horas o restringir la validez a un mínimo de 15 minutos. La caducidad de las credenciales temporales no depende del valor de`X-Amz-Date`.

Las credenciales permanentes no tienen esta restricción. Se recomienda usar solo credenciales temporales, y puedes revocar de forma explícita cualquier credencial permanente, lo que también invalidaría cualquier firma basada en esa credencial.

Aunque `s3:signatureAge` se mide en milisegundos, no es práctico configurarlo en menos de 60 segundos, incluso si el reloj está bien sincronizado y el uso de la latencia es bajo. Los ajustes inferiores a 60 segundos conllevan el riesgo de rechazar solicitudes válidas. Si prevé demoras entre la generación de la firma y el envío de la solicitud, o si hay problemas con la sincronización del reloj, debe tener en cuenta estos problemas en la gestión de los `s3:signatureAge` mismos.

Dirigirse a los grupos a gran escala

Los SCP y los RCP se pueden utilizar `aws:PrincipalTag` para hacer excepciones para los usuarios. No puedes usar etiquetas en un depósito para controlar el accesoaws:ResourceTag; solo se usan etiquetas de objetos para el control de acceso. Por lo general, no es escalable añadir una etiqueta a cada objeto al que quieras aplicar este control.

Una solución que se adapta a muchos casos de uso es aplicar la política y la excepción a nivel de cuenta, ya sea cambiando las cuentas a las que se aplica el SCP o el RCP o utilizando aws: ResourceAccount, aws: ResourceOrgPaths o aws: ResourceOrg ID. Por ejemplo, se puede aplicar un SCP o un RCP a un conjunto de cuentas de producción.

Otra solución consiste en utilizar una AWS Config regla personalizada para implementar un control detectivesco o un control responsivo. El objetivo sería que cada grupo contuviera una política de grupo con la barrera de protección adecuada. Además de probar el contenido de una política de bucket, la AWS Config regla personalizada puede recuperar las etiquetas del bucket y excluirlo de la regla si el bucket está etiquetado con un valor específico. Si esa regla no supera la comprobación de conformidad, podría marcar el depósito como no conforme o solicitar una solución para añadir el elemento de protección a la política del depósito.

> **Note**
>
> No puedes restringir el contenido de las etiquetas de las solicitudes a. PutBucketTagging Para mantener el control sobre cómo se etiqueta un depósito, debes limitar el acceso a `PutBucketTagging` y DeleteBucketTagging.

Registrar las interacciones y las mitigaciones

Una URL prefirmada contiene una firma y se puede usar, durante el período anterior a la caducidad, para realizar la operación de API específica para la que se firmó. Debe tratarse como una credencial de acceso temporal. La firma debe permanecer privada solo para las partes que necesiten conocerla. En la mayoría de los entornos, este es el cliente que envía la solicitud y el servidor que la recibe. El envío de la firma como parte de una sesión HTTPS directa mantiene su naturaleza privada, ya que solo un participante de la sesión HTTPS puede ver el URI que transmite la firma.

En el caso de las URL prefirmadas, la firma se transmite como parámetro de cadena de `X-Amz-Signature` consulta. Los parámetros de la cadena de consulta son un componente de un URI. El riesgo es que los clientes registren el URI y la firma con él. Los clientes tienen acceso a toda la solicitud HTTP y pueden registrar cualquier parte de la solicitud, los datos y los encabezados (incluidos los encabezados de autenticación). Sin embargo, por convención, esto es menos común. El registro de URI es más común y obligatorio en casos como el registro de acceso. Los clientes deben utilizar la redacción o el enmascaramiento para eliminar la firma antes de registrar los URI.

En algunos entornos, los usuarios permiten que los intermediarios (proxies) obtengan visibilidad en sus sesiones HTTPS. La activación de los proxies requiere un alto nivel de acceso privilegiado a los sistemas cliente, ya que requieren configuración y certificados de confianza. La instalación de una configuración de proxy y de certificados de confianza, dentro del contexto local del entorno intermediario del cliente, permite un nivel de privilegios muy alto. Por esta razón, el acceso a dichos intermediarios debe estar estrictamente controlado.

El propósito de un intermediario suele ser bloquear las salidas no deseadas y rastrear otras salidas. Por ello, es habitual que estos intermediarios registren las solicitudes. Si bien los intermediarios podrían, como los clientes, registrar cualquier contenido, encabezados y datos (todos los cuales serían muy confidenciales), es más común que registren los URI, como los que incluyen el `X-Amz-Signature` parámetro de cadena de consulta.

Mitigaciones

Recomendamos que al registrar los URI se redacte el parámetro de la cadena de `X-Amz-Signature` consulta, se redacte toda la cadena de consulta o se trate la información de forma altamente confidencial, como ocurre con el acceso directo al servidor intermediario. Si bien estas protecciones son muy recomendables, el hecho de que las URL prefirmadas caduquen reduce los riesgos de exposición de los registros, siempre y cuando la exposición se retrase lo suficiente como para que las firmas caduquen.

Amazon S3 también ve las firmas y debe gestionarlas de forma adecuada. Los registros de acceso al servidor Amazon S3 incluyen el URI de la solicitud`X-Amz-Signature`, pero lo redactan como se recomienda. Lo mismo ocurre cuando se registran eventos de CloudTrail datos para Amazon S3. Puedes configurar Amazon CloudWatch Logs para que oculte los datos mediante identificadores de datos personalizados.

La siguiente expresión regular coincide con la `X-Amz-Signature` forma en que aparece en un URI:

```
X-Amz-Signature=[a-f0-9]{64}
```

La siguiente expresión regular agrega patrones de agrupamiento para identificar el texto que se va a reemplazar de manera más específica:

```
(?:X-Amz-Signature=)([a-f0-9]{64})
```

Si tiene una entrada en el registro de acceso como la siguiente:

```
X-Amz-Signature=733255ef022bec3f2a8701cd61d4b371f3f28c9f193a1f02279211d48d5193d7
```

La primera expresión regular traduce la entrada del registro de acceso a:

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

La segunda expresión regular, en los sistemas que admiten grupos que no capturan, traduce la entrada del registro de acceso a:

```
X-Amz-Signature=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Preguntas frecuentes

¿Se puede utilizar una solicitud prefirmada varias veces? ¿Es un riesgo para la seguridad?

Sí, la firma de una solicitud prefirmada se puede usar más de una vez. Si se trata de un riesgo de seguridad es una cuestión contextual. Otros métodos de acceso a los servicios de AWS también permiten la repetición. Un usuario o una carga de trabajo con AWS credenciales pueden enviar muchas solicitudes Servicios de AWS, y cualquiera de ellas podría estar duplicada.

Si su caso de uso requiere una ejecución única y solo una vez, debe implementar otros mecanismos para imponer el uso único. El uso único no es una característica de las solicitudes prefirmadas. Como ingeniero de seguridad, debe revisar los casos de uso y las implementaciones, pero en muchos casos, el uso múltiple es adecuado para un uso aceptable.

¿Puede otra persona que no sea el usuario previsto utilizar una solicitud prefirmada?

Cualquier persona que esté en posesión de la misma puede enviar la firma de una solicitud prefirmada. Solo se aceptará si supera otras formas de validación, como los controles perimetrales de datos. Si la firma ha caducado, las credenciales de firma han caducado o las credenciales de firma no tienen acceso a los recursos solicitados, se denegará la solicitud.

Lo mismo ocurre con otros métodos de autenticación con Servicios de AWS. Las credenciales que se comparten de forma inapropiada permiten un acceso inapropiado. La mejor práctica básica es compartir las credenciales y firmas solo con el público objetivo. Si no puedes confiar en el público al que estás dirigido para proteger los datos privados y no compartirlos con otras personas, esto socavará cualquier forma de autenticación.

¿Puede un usuario autorizado utilizar una solicitud prefirmada para filtrar datos?

Proteger los datos requiere una acción sólida. Permitir el acceso para los fines previstos y, al mismo tiempo, mantener un perímetro de datos requiere un enfoque integral. El acceso con privilegios

mínimos, los controles del perímetro de los datos y el uso exclusivo de credenciales de acceso temporales son las mejores prácticas generales que se aplican a la protección de los datos. El uso adecuado de estos controles también limita la capacidad de los usuarios para realizar acciones a través de las solicitudes prefirmadas que generan.

Esto se debe a que el acceso que proporcionan las solicitudes prefirmadas es un subconjunto del acceso otorgado a las credenciales que se utilizan para firmar la solicitud. En este contexto, las mejores prácticas que se aplican al acceso a los datos generalmente se aplican a las solicitudes prefirmadas, pero las solicitudes prefirmadas no crean ningún acceso nuevo a los datos.

- La caducidad máxima se limita a la caducidad de las credenciales de firma. Si se revocan las credenciales de firma, las firmas basadas en las credenciales dejarán de ser válidas.
- Si los permisos de la entidad principal de IAM asociada a las credenciales de firma no incluyen la ejecución de la acción asociada a la solicitud prefirmada, al invocar una solicitud prefirmada se obtiene una respuesta de «acceso denegado». La respuesta depende del estado actual de los permisos en el momento de la invocación, que no tiene relación con el momento en que se generó la firma de la solicitud prefirmada.
- Las propiedades del principal se evalúan en función del principal asociado a las credenciales de firma.
- Las propiedades de una sesión de rol se evalúan en función de la sesión de rol asociada a las credenciales de firma.
- Las propiedades de la red se evalúan en función de cómo se recibió la solicitud, como ocurre con las solicitudes normales.

En este contexto, el examen de los riesgos asociados a las solicitudes prefirmadas se limita a las áreas en las que se firman con credenciales diferentes de las credenciales del usuario y proporcionan un acceso que no formaba parte del principal del usuario. Este examen debería aplicarse al diseño del servicio, la carga de trabajo o la solución que genera firmas en nombre del usuario, y no a la propia capacidad de solicitud prefirmada.

¿Puedo denegar el acceso desde una URL prefirmada si sospecho que se ha compartido de forma no autorizada?

Sí. Esto requiere invalidar las credenciales con las que se firmó la URL. Existen varias formas de lograrlo:

- Elimine los permisos del principal de IAM al que pertenecen las credenciales. Si ese principal de IAM ya no tiene acceso al recurso y la operación para los que está firmada la URL, la URL no podrá ejecutar esa operación. Esto afecta a todos los usos coincidentes de ese principal de IAM.
- Si las credenciales utilizadas para firmar la URL son temporales AWS STS , puede revocar los permisos de sesión para las credenciales temporales que se emitieron antes de una hora específica para el principal de IAM. Según el caso de uso, es posible que haya otras sesiones válidas que se invaliden antes de su fecha de caducidad normal, pero las sesiones nuevas no se verán afectadas. La revocación de los permisos de sesión también invalida los URLs que se hayan firmado con las credenciales asociadas a esas sesiones, pero los nuevos permisos URLs asociados a sesiones nuevas no se verán afectados.
- Si las credenciales utilizadas para firmar la URL son permanentes, desactive la clave de acceso. Esto afecta a todo el uso vinculado a esas credenciales.

Recursos

Documentación de Amazon S3

- Solicitudes de autenticación (AWS firma, versión 4)
- Autenticación de solicitudes: uso de parámetros de consulta (AWS firma, versión 4)
- Solicitudes de autenticación: cargas basadas en el navegador mediante POST (versión de firma 4)AWS
- Claves de política de autenticación específicas de Amazon S3 Signature versión 4
- Trabajar con direcciones URL prefirmadas

Otras referencias

- Creación de un perímetro de datos en AWS (AWS documento técnico)
- SEC03-BP02 Otorgue el acceso con privilegios mínimos (marco AWS bien diseñado, pilar de seguridad)
- SEC03-BP05 Defina las barreras de permisos para su organización (Well Architected Framework, pilar de seguridad)AWS

Apéndice A: Cómo Servicios de AWS usar prefirmado URLs

Este apéndice proporciona información Servicios de AWS y características que utilizan URLs prefirmados. Esta información tiene dos propósitos:

- Proporcionar a los ingenieros de seguridad que implementan los controles información sobre los posibles impactos de esos controles.
- Para crear conciencia sobre las situaciones en las que este riesgo podría ser relevante para las interacciones de registro de URL.

> **Important**
>
> Este apéndice no proporciona una lista completa Servicios de AWS ni su uso de los prefirmados URLs. Tampoco cubre las soluciones personalizadas o de terceros.

Consola de Amazon S3

Principal: usuario de consola

Caducidad predeterminada: 5 minutos

> **Exención de responsabilidad**
>
> En esta sección se documenta el comportamiento actual de la consola Amazon S3. AWS El comportamiento de la consola está sujeto a cambios sin previo aviso.

La consola Amazon S3 admite la descarga y carga de objetos. Las descargas utilizan una URL prefirmada que tiene un tiempo de caducidad de 300 segundos (5 minutos). La URL se genera mediante una solicitud a`https://<bucket-region>.console.aws.amazon.com/s3/batch0psServlet-proxy`.

Esa solicitud se inicia cuando el usuario hace clic en un botón de descarga, por lo que la URL no se genera por adelantado ni se envía al cliente hasta que se produce la solicitud explícita de descarga.

Las subidas son similares, con la diferencia de que la consola envía dos solicitudes: `OPTIONS` una para comprobar el CORS antes del vuelo, y. `PUT` Ambas solicitudes utilizan la misma firma.

Las credenciales utilizadas para firmar son credenciales temporales que están asociadas al usuario que ha iniciado sesión actualmente. Los detalles sobre el método para obtener esas credenciales temporales están fuera del ámbito de esta guía.

Amazon S3 Object Lambda

Principal: Persona que llama al punto de acceso

Caducidad predeterminada: 61 segundos

> **Note**
>
> A partir del 7 de noviembre de 2025, S3 Object Lambda solo está disponible para los clientes actuales que utilizan el servicio actualmente, así como para algunos socios AWS Partner Network (de APN). Para obtener más información sobre capacidades similares a las de S3 Object Lambda, haga clic aquí: cambio de disponibilidad de Amazon S3 Object Lambda.

Amazon S3 Object Lambda utiliza AWS Lambda funciones para procesar y transformar automáticamente los datos a medida que se recuperan de Amazon S3. Cuando S3 Object Lambda invoca una función, la función recibe una URL prefirmada (`inputS3Url`) que puede usar para descargar el objeto original desde el punto de acceso compatible.

Estos prefirmados URLs están firmados para el punto de acceso Amazon S3 compatible, que se proporciona al configurar S3 Object Lambda. (No es lo mismo que el punto de acceso Object Lambda). En lugar de utilizar un rol vinculado a la función Lambda, la URL se firma con la identidad de la persona que llama originalmente y los permisos de ese usuario se aplicarán cuando se utilice la URL. Si hay encabezados firmados en la URL, la función Lambda debe incluir estos encabezados en la llamada a Amazon S3.

La URL prefirmada que se devuelve tiene un tiempo de caducidad de 61 segundos (un segundo más que la duración máxima de una función Object Lambda de S3). La URL generada solo se puede usar con el punto de acceso compatible. La persona que llama al punto de acceso S3 Object Lambda debe tener acceso a este punto de acceso. Puede limitar ese acceso al contexto de S3 Object Lambda mediante la condición. `"aws:CalledVia": ["s3-object-lambda.amazonaws.com"]` Cuando esa condición está asociada a un punto de acceso o depósito de soporte, el usuario no puede acceder directamente al punto de acceso o depósito de soporte.

El valor de este enfoque es que no es necesario conceder a la función Lambda acceso a su bucket o punto de acceso de S3. El rol asociado a la función Lambda necesitará permisos WriteGetObjectResponse, pero no los necesitará. GetObject

Cuando S3 Object Lambda genera un objeto prefirmado URLs, no añade restricciones de red, por lo que se puede utilizar una URL fuera de la función Lambda. Sin embargo, se seguirán aplicando las restricciones impuestas a la persona que llama a S3 Object Lambda. Por ejemplo, si la función Lambda se ejecuta en una VPC y restringe a la persona que llama a usar un punto de enlace de la VPC, cualquier persona que posea la URL prefirmada necesitará poder enviarla a través de ese punto de enlace de la VPC. Esta restricción también se aplica a y. SourceIpVpcSourceIp

> **Note**
>
> Para utilizar una función Object Lambda de S3 en una VPC, la VPC debe tener una ruta a los puntos finales públicos de S3 a los que pueda llamar. WriteGetObjectResponse Esto no indica que los requisitos de uso de un punto final de VPC no se apliquen a las solicitudes de recuperación de datos del depósito.

AWS Lambda Entre regiones CopyObject

Principal: internoAWS

Caducidad predeterminada: 3600 segundos

Cuando utiliza la UploadPartCopyAPI CopyObjecto para realizar copias Regiones de AWS, Amazon S3 utiliza un código prefirmado URLs internamente. Se APIs pueden llamar directamente desde SDKs o desde los AWS CLI comandos `aws s3api copy-object` y`aws s3api upload-part`. APIs No se utilizan para la replicación de Amazon S3, pero los utilizan los `aws s3 sync` comandos AWS CLI `aws s3 cp` y cuando el origen y el destino son buckets de S3. También son compatibles con `TransferManager` implementaciones en varios. AWS SDKs

AWS Lambda GetFunction

Principal: interno AWS

Caducidad predeterminada: 10 minutos

AWS Lambda almacena la versión de usuario en un bucket de S3 propiedad del equipo de Lambda antes de generar los activos desplegados en los contenedores de Lambda. Cuando desee acceder

al código de su función, llame a la GetFunctionAPI. Esta API responde con `Code.Location` una URL prefirmada que es válida durante 10 minutos (este tiempo de caducidad es el comportamiento actual y no un contrato publicado). Si no quieres el código, puedes usar una combinación de GetFunctionConfigurationGetFunctionConcurrency, y ListTagspara recuperar el resto de datos devueltos por`GetFunction`.

Lambda firma la URL devuelta no con las credenciales del usuario que ha iniciado sesión actualmente, sino en nombre del usuario. Por este motivo, las claves de condición (por ejemplo`aws:SourceIP`) que se aplican al usuario que ha iniciado sesión actualmente o a las credenciales de sesión temporales del usuario no se aplican a la URL generada. Esto es válido tanto si las claves de condición se aplican GetFunctionúnicamente al uso de las API de AWS como si se aplican a todo el uso de las API de AWS para el usuario o la sesión.

La consola Lambda también utiliza GetFunctionla URL prefirmada que devuelve. La consola utiliza las credenciales temporales asociadas al usuario que ha iniciado sesión actualmente para llamar. GetFunction Los detalles sobre la obtención de esas credenciales temporales están fuera del ámbito de este documento.

Amazon ECR

Director: AWS interno

Caducidad predeterminada: 1 hora

Amazon Elastic Container Registry (Amazon ECR) proporciona GetDownloadUrlForLayerla API, que devuelve una URL prefirmada que es válida durante una hora y permite la descarga de una sola capa desde una imagen de Amazon ECR. Sin embargo, el proxy Amazon ECR utiliza esta operación y, por lo general, los usuarios no la utilizan para extraer y empujar imágenes.

Amazon Redshift Spectrum

Principal: El rol pasó a CREATE EXTERNAL SCHEMA a través de `IAM_ROLE`

Caducidad predeterminada: 1 hora

Amazon Redshift Spectrum usa URLs prefirmados internamente y prohíbe las restricciones en la combinación del bucket y la función de Amazon Redshift que limitarían los prefirmados. URLs Puede utilizar un `s3:signatureAge` valor de 16 minutos, pero los valores muy bajos no son fiables. El valor mínimo que puede utilizar depende del tiempo y el tamaño de la consulta. Si bien un valor

inferior a 16 minutos funciona en muchos escenarios, es necesario probarlo. La función puede y debe restringirse para que la utilice únicamente Redshift Spectrum, que no revela lo que genera, URLs lo que mitiga la típica justificación de valores de caducidad más bajos.

Amazon SageMaker AI Studio

Amazon SageMaker AI Studio admite dos acciones de API: CreatePresignedDomainUrly CreatePresignedNotebookInstanceUrl. Sin embargo, no APIs están relacionadas con la función de URL prefirmada de la versión 4 de Signature. APIs Crean una URL que utiliza un `authToken` parámetro, pero no admiten ninguno de los parámetros de consulta estándar de la versión 4 de Signature.

`authToken`es un mecanismo diferente, pero tiene similitudes con el prefirmado URLs. Se envía como parámetro de cadena de consulta y admite un tiempo de caducidad de 5 minutos.

SageMaker La IA admite las restricciones de red. Si restringes la `sagemaker:CreatePresignedDomainUrl` acción, esa acción se aplica tanto a la llamada CreatePresignedDomainUrlcomo al uso de la URL generada. Si se genera una URL desde una red válida y, a continuación, se envía desde una red no válida, la llamada a la API para generar la URL se realiza correctamente, pero la solicitud que envía la URL falla. Lo mismo ocurre con la CreatePresignedNotebookInstanceUrl`sagemaker:CreatePresignedNotebookInstanceUrl`acción.

Para obtener más información, consulte la documentación sobre SageMaker IA.

Apéndice B: Cómo afectan los controles prefirmados URLs Servicios de AWS

En este apéndice se describen las interacciones entre los controles Servicios de AWS prefirmados URLs, tal como se describe en el apéndice A, y los controles descritos anteriormente en esta guía.

Barandilla para S3: SignatureAge

La consola Amazon S3 no se ve afectada por la caducidad máxima de 5 minutos establecida por la clave de `s3:signatureAge` condición. La consola Amazon S3 genera datos prefirmados URLs al pulsar el botón Descargar y aplica su propio tiempo de caducidad de 5 minutos. Una duración máxima inferior a 2 minutos puede provocar errores aleatorios en función de la sincronización del reloj y las latencias.

Amazon S3 Object Lambda utiliza un tiempo de caducidad de 61 segundos, por lo que establecer condiciones en un `s3:signatureAge` valor de 61 segundos o más no provocará ninguna interrupción. Las duraciones más cortas pueden ser menos fiables y provocar fallos intermitentes.

Amazon S3 Cross-Region CopyObjectno se ve interrumpido por una caducidad máxima de 5 minutos. Sin embargo, las duraciones más cortas pueden provocar errores aleatorios en función de la sincronización del reloj y las latencias.

En AWS Lambda, GetFunctionproporciona una URL a objetos ajenos a la cuenta del cliente, de modo que las políticas del cliente no afecten a los generados. URLs

Se probó Amazon Redshift Spectrum durante 16 minutos. `s3:signatureAge` Sin embargo, una duración más corta podría provocar interrupciones.

Barandilla para S3: AuthType cuando no se utilizan restricciones de red

La consola Amazon S3 suele verse afectada por la `s3:authType` barandilla. La consola se enruta a Amazon S3 en función de la configuración de la red local. Si la red local se enruta a Amazon S3 de la manera que lo permita la restricción de red, la consola Amazon S3 seguiría funcionando. Sin embargo, si se enruta a través de un proxy o de la Internet pública de una manera no permitida, se bloqueará su uso. Sin embargo, bloquear el uso es probablemente la intención de esta política.

El objeto Lambda de Amazon S3 se ve afectado si la función Lambda no está conectada a una VPC adecuada. En esta configuración, la VPC debe tener una puerta de enlace NAT, no para acceder al bucket de S3, sino para realizar una llamada. WriteGetObjectResponse

Amazon S3 Cross-Region CopyObjectse interrumpe si esta barrera de protección se aplica a una política de bucket sin la excepción recomendada cuando **`aws:viaAWSService`** es verdadera.

Amazon Redshift Spectrum se ve afectado por `s3:authType` la barandilla, a menos que se utilice el enrutamiento de VPC mejorado. Actualmente, Redshift Spectrum admite el enrutamiento de VPC mejorado solo con clústeres sin servidor, no con clústeres aprovisionados.

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Actualizaciones y aclaraciones	En la sección Barandillas adicionales, se agregó información sobre las excepciones RCPs y se aclararon las mismas.	8 de agosto de 2025
Publicación inicial	—	23 de julio de 2024

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.