Políticas de acceso a bloques y grupos

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/es-es/storagegrid-118/s3/bucket-and-group-access-policies.html on November 04, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Políticas de acceso a bloques y grupos . . . 1
Utilice las políticas de acceso de bloques y grupos . . . 1
Información general sobre las políticas de acceso . . . 1
Coherencia de las políticas . . . 3
Utilice ARN en las declaraciones de política . . . 4
Especifique recursos en una política . . . 4
Especifique los principales en una directiva . . . 5
Especificar permisos en una directiva . . . 6
Utilice el permiso PutOverwriteObject . . . 10
Especificar condiciones en una política . . . 11
Especifique las variables en una política . . . 15
Crear directivas que requieran un manejo especial . . . 16
Protección WORM (escritura única lectura múltiple) . . . 17
Ejemplo de políticas de bloque . . . 18
Ejemplo: Permitir que todos tengan acceso de solo lectura a un bloque . . . 18
Ejemplo: Permitir que todos en una cuenta tengan acceso total y que todas las personas de otra cuenta tengan acceso de solo lectura a un bloque . . . 19
Ejemplo: Permitir que todo el mundo tenga acceso de solo lectura a un bloque y acceso completo por un grupo especificado . . . 20
Ejemplo: Permitir que todo el mundo tenga acceso de lectura y escritura a un bloque si un cliente se encuentra en el rango de IP . . . 21
Ejemplo: Permitir el acceso completo a un bloque exclusivamente por un usuario federado especificado . . . 22
Ejemplo: Permiso PutOverwriteObject . . . 23
Ejemplo de políticas de grupo . . . 24
Ejemplo: Establecer la directiva de grupo mediante el Administrador de inquilinos . . . 25
Ejemplo: Permite el acceso total de grupos a todos los bloques . . . 25
Ejemplo: Permitir el acceso de solo lectura de grupo a todos los bloques . . . 25
Ejemplo: Permitir a los miembros del grupo acceso completo solo a su carpeta en un depósito . . . 26

Políticas de acceso a bloques y grupos

Utilice las políticas de acceso de bloques y grupos

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir que los inquilinos S3 controlen el acceso a bloques y objetos dentro de esos bloques. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API DE REST de S3. Las políticas de acceso para la API de S3 se escriben en JSON.

Información general sobre las políticas de acceso

Existen dos tipos de políticas de acceso compatibles con StorageGRID.

- **Políticas de cubo**, que se gestionan mediante las operaciones de la API GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy S3. Las políticas de bloque se asocian a bloques, por lo que se configuran para controlar el acceso de los usuarios de la cuenta de propietario del bloque u otras cuentas al bloque y a los objetos en él. La política de bloques se aplica únicamente a un bloque y, posiblemente, a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las directivas de grupo se asocian a un grupo de la cuenta, por lo que se configuran para permitir que dicho grupo tenga acceso a recursos específicos propiedad de dicha cuenta. La política de grupo se aplica únicamente a un grupo y, posiblemente, a varios bloques.

No hay ninguna diferencia de prioridad entre las políticas de grupo y de bloque.

Las políticas de bloque y grupo de StorageGRID siguen una gramática específica definida por Amazon. Dentro de cada política hay una serie de declaraciones de política y cada sentencia contiene los siguientes elementos:

- ID de sentencia (Sid) (opcional)
- Efecto
- Principal/NotPrincipal
- Recurso/NotResource
- Acción/NotAction
- Condición (opcional)

Las sentencias de directiva se crean utilizando esta estructura para especificar permisos: Conceda <Effect> para permitir/denegar que <Principal> ejecute <Action> en <Resource> cuando se aplique <Condition>.

Cada elemento de directiva se utiliza para una función específica:

Elemento	Descripción
SID	El elemento Sid es opcional. El Sid sólo se ha diseñado como una descripción para el usuario. El sistema StorageGRID lo almacena pero no lo interpreta.

Elemento	Descripción
Efecto	Utilice el elemento Effect para establecer si se permiten o deniegan las operaciones especificadas. Debe identificar las operaciones que permite (o deniega) en cubos u objetos utilizando las palabras clave del elemento Acción admitido.
Principal/NotPrincipal	Puede permitir a los usuarios, grupos y cuentas acceder a recursos específicos y realizar acciones específicas. Si no se incluye ninguna firma S3 en la solicitud, se permite el acceso anónimo especificando el carácter comodín (*) como principal. De forma predeterminada, sólo la raíz de la cuenta tiene acceso a los recursos que pertenecen a la cuenta. Sólo es necesario especificar el elemento Principal en una política de bloque. Para las directivas de grupo, el grupo al que se asocia la directiva es el elemento Principal implícito.
Recurso/NotResource	El elemento Resource identifica los bloques y los objetos. Puede permitir o denegar permisos para cubos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/NotAction	Los elementos Acción y efecto son los dos componentes de los permisos. Cuando un grupo solicita un recurso, se le concede o se le deniega el acceso al recurso. Se deniega el acceso a menos que asigne permisos de forma específica, pero puede utilizar Denegar explícito para anular un permiso otorgado por otra directiva.
Condición	El elemento Condition es opcional. Las condiciones permiten crear expresiones para determinar cuándo se debe aplicar una directiva.

En el elemento Action , puede utilizar el carácter comodín (*) para especificar todas las operaciones o un subconjunto de operaciones. Por ejemplo, esta acción coincide con permisos como s3:GetObject, s3:PutObject y s3:DeleteObject.

```
s3:*Object
```

En el elemento Resource , puede utilizar los caracteres comodín (*) y (?). Aunque el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter.

En el elemento Principal, no se admiten caracteres comodín excepto para establecer el acceso anónimo, que otorga permiso a todos. Por ejemplo, el comodín (*) se establece como el valor Principal.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

En el ejemplo siguiente, la instrucción utiliza los elementos Effect, Principal, Acción y recurso. En este ejemplo se muestra una sentencia de directiva de bloque completa que utiliza el efecto "permitir" para dar a los principales, el grupo admin `federated-group/admin` y el grupo financiero `federated-group/finance`, Permisos para realizar la acción `s3:ListBucket` en el bloque llamado `mybucket` Y la Acción `s3:GetObject` en todos los objetos dentro de ese cucharón.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de bloque tiene un límite de tamaño de 20,480 bytes y la política de grupo tiene un límite de tamaño de 5,120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice a las directivas de grupo será consistente. Cuando una normativa de grupo es coherente, los cambios pueden tardar 15 minutos adicionales en aplicarse debido al almacenamiento en caché de la política. Por defecto, cualquier actualización que realice en las políticas de depósito es fuertemente coherente.

Según sea necesario, puede cambiar las garantías de coherencia para las actualizaciones de la política de bloques. Por ejemplo, es posible que desee que un cambio en una política de bloque esté disponible durante una interrupción del servicio del sitio.

En este caso, puede ajustar la `Consistency-Control` Cabecera en la solicitud PutBucketPolicy, o puede utilizar la solicitud de coherencia PUT Bucket. Cuando una política de depósito es coherente, los cambios pueden tardar 8 segundos adicionales en aplicarse debido al almacenamiento en caché de la política.

Si establece la consistencia en un valor diferente para resolver una situación temporal, asegúrese de volver a establecer el valor de nivel de cubo en su valor original cuando haya terminado. De lo contrario, todas las solicitudes de bloque futuras utilizarán la configuración modificada.

Utilice ARN en las declaraciones de política

En las declaraciones de política, el ARN se utiliza en los elementos Principal y Recursos.

- Utilice esta sintaxis para especificar el recurso ARN de S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilice esta sintaxis para especificar el recurso de identidad ARN (usuarios y grupos):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Otras consideraciones:

- Puede utilizar el asterisco (*) como comodín para que coincida con cero o más caracteres dentro de la clave de objeto.
- Los caracteres internacionales, que se pueden especificar en la clave de objeto, deben codificarse mediante JSON UTF-8 o mediante secuencias de escape JSON \u. No se admite el porcentaje de codificación.

  "Sintaxis de URN RFC 2141"

  El cuerpo de la solicitud HTTP para la operación PutBucketPolicy debe estar codificado con charset=UTF-8.

Especifique recursos en una política

En las sentencias de directiva, puede utilizar el elemento Resource para especificar el bloque o el objeto para el que se permiten o deniegan los permisos.

- Cada instrucción de directiva requiere un elemento Resource. En una política, el elemento denota los recursos `Resource`o bien, `NotResource` para la exclusión.
- Se especifican recursos con un ARN de recurso S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puede usar variables de política dentro de la clave de objeto. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- El valor del recurso puede especificar un bucket que todavía no existe cuando se crea una política de grupo.

Especifique los principales en una directiva

Utilice el elemento Principal para identificar al usuario, grupo o cuenta de arrendatario que la sentencia de directiva permite o deniega el acceso al recurso.

- Cada sentencia de política de una política de bloque debe incluir un elemento Principal. Las sentencias de política de una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los principales se denotan por el elemento Principal o, alternativamente, NotPrincipal para la exclusión.
- Las identidades basadas en cuentas se deben especificar mediante un ID o un ARN:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- En este ejemplo se utiliza el ID de cuenta de inquilino 27233906934684427525, que incluye la raíz de la cuenta y todos los usuarios de la cuenta:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Puede especificar sólo la raíz de la cuenta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puede especificar un usuario federado específico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Puede especificar un grupo federado específico ("managers"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Puede especificar un principal anónimo:

```
"Principal": "*"
```

- Para evitar ambigüedades, puede utilizar el UUID de usuario en lugar del nombre de usuario:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Por ejemplo, supongamos que Alex abandona la organización y el nombre de usuario `Alex` se ha eliminado. Si un nuevo Alex se une a la organización y se le asigna la misma `Alex` nombre de usuario, es posible que el nuevo usuario herede sin querer los permisos concedidos al usuario original.

- El valor principal puede especificar un nombre de grupo/usuario que aún no existe cuando se crea una directiva de bloque.

Especificar permisos en una directiva

En una directiva, el elemento Acción se utiliza para permitir/denegar permisos a un recurso. Hay un conjunto de permisos que puede especificar en una directiva, que se indican mediante el elemento "Acción" o, alternativamente, "NotAction" para la exclusión. Cada uno de estos elementos se asigna a operaciones de API de REST de S3 específicas.

En las tablas se enumeran los permisos que se aplican a los bloques y los permisos que se aplican a los objetos.

Amazon S3 ahora usa el permiso S3:PutReplicationConfiguration para las acciones PutBucketReplication y DeleteBucketReplication. StorageGRID utiliza permisos independientes para cada acción, que coinciden con la especificación original de Amazon S3.

Se realiza una supresión cuando se utiliza una PUT para sobrescribir un valor existente.

Permisos que se aplican a los bloques

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:CreateBucket	CreateBucket	Sí. **Nota**: Usar solo en la política de grupo.
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	DELETE bucket metadata notification Configuration	Sí
s3:DeleteBucketPolicy	DeleteBucketPolicy	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sí, separe los permisos para PUT y DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	CUMPLIMIENTO de LA normativa GET Bucket (obsoleto)	Sí
s3:GetBucketConsistency	OBTENGA coherencia de bloques	Sí
s3: GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	HORA de último acceso al bloque DE GET	Sí
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OBTENGA la configuración de notificación de metadatos del bloque de datos	Sí
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	Etiquetado de GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	• ListCuchers • Obtenga el uso del almacenamiento	Sí, para OBTENER uso de almacenamiento. **Nota**: Usar solo en la política de grupo.

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:ListBucket	• ListObjects • Segmento de cabeza • RestoreObject	
s3:ListBucketMultipartUploads	• ListCargas multipartitas • RestoreObject	
s3:ListBucketVersions	OBTENGA las versiones DE Bucket	
s3:PutBucketCompliance	CUMPLIMIENTO de PUT Bucket (obsoleto)	Sí
s3:PutBucketConsistency	PONGA la consistencia del cucharón	Sí
s3: PutBucketCORS	• DeleteBucketCors† • A cargo de PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket última hora de acceso	Sí
s3:PutBucketMetadataNotification	Configuración de notificaciones de metadatos de PUT Bucket	Sí
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket con el `x-amz-bucket-object-lock-enabled: true` Encabezado de solicitud (también requiere el permiso s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBucketPolicy	Política de PutBucketPolicy	
s3:PutBucketEtiquetado	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:PutLipeycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sí, separe los permisos para PUT y DELETE

Permisos que se aplican a objetos

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (una versión específica del objeto)	
s3:DeleteObjectVersion	DeleteObject (una versión específica del objeto)	
s3:GetObject	• GetObject • Objeto principal • RestoreObject • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	

Permisos	OPERACIONES DE LA API DE REST DE S3	Personalizado para StorageGRID
s3:GetObjectTagging	GetObjectEtiquetado	
s3:GetObjectVersionTagging	GetObjectTagging (una versión específica del objeto)	
s3:GetObjectVersion	GetObject (una versión específica del objeto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Objeto de puta • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectEtiquetado	PutObjectEtiquetado	
s3:PutObjectVersionEtiquetado	PutObjectTagging (una versión específica del objeto)	
s3:PutOverwriteObject	• Objeto de puta • CopyObject • PutObjectEtiquetado • DeleteObjectTagging • CompleteMultipartUpload	Sí
s3:RestoreObject	RestoreObject	

Utilice el permiso PutOverwriteObject

el permiso s3:PutOverwriteObject es un permiso StorageGRID personalizado que se aplica a operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede sobrescribir los datos de un objeto, metadatos definidos por el usuario o el etiquetado de objetos S3.

Entre los posibles ajustes para este permiso se incluyen:

- **Permitir**: El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar**: El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
  - Si se encuentra un objeto existente en la misma ruta:
    - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3 no se pueden sobrescribir.
    - Se cancela cualquier operación de ingesta en curso y se devuelve un error.
    - Si el control de versiones S3 está activado, la configuración Denegar impide que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet para un objeto y sus versiones no actuales.
  - Si no se encuentra un objeto existente, este permiso no tiene efecto.
- Cuando este permiso no está presente, el efecto es el mismo que si se estableció permitir.

> Si la directiva S3 actual permite la sobrescritura y el permiso PutOverwriteObject se establece en Deny, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni el etiquetado de objetos. Además, si la casilla de verificación **Evitar modificación de cliente** está seleccionada (**CONFIGURACIÓN** > **Ajustes de seguridad** > **Red y objetos**), esa configuración anula la configuración del permiso PutOverwriteObject.

Especificar condiciones en una política

Las condiciones definen cuándo estará en vigor una política. Las condiciones consisten en operadores y pares clave-valor.

Condiciones Utilice pares clave-valor para la evaluación. Un elemento Condition puede contener varias condiciones y cada condición puede contener varios pares clave-valor. El bloque Condition utiliza el siguiente formato:

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

En el ejemplo siguiente, la condición ipaddress utiliza la clave de condición SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Operadores de condición admitidos

Los operadores de condición se categorizan de la siguiente manera:

- Cadena
- Numérico
- Booleano
- Dirección IP
- Comprobación nula

Operadores de condición	Descripción
StringEquals	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
StringNotEquals	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas).
StringEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia exacta (omite Case).
StringNotEqualizsIgnoreCase	Compara una clave con un valor de cadena basado en la coincidencia negada (omite Case).
StringLike	Compara una clave con un valor de cadena basado en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir * y ? caracteres comodín.
StringNotLike	Compara una clave con un valor de cadena basado en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir * y ? caracteres comodín.
Valores numéricos	Compara una clave con un valor numérico basado en la coincidencia exacta.
NumericNotEquals	Compara una clave con un valor numérico basado en la coincidencia negada.
NumericGreatertan	Compara una clave con un valor numérico basado en la coincidencia mayor que.
NumericGreaterThanEquals	Compara una clave con un valor numérico en función de la coincidencia mayor o igual que.
NumericLessThan	Compara una clave con un valor numérico basado en la coincidencia menor que.
NumericLesThanEquals	Compara una clave con un valor numérico en función de la coincidencia menor o igual que.

Operadores de condición	Descripción
Bool	Compara una clave con un valor booleano basado en la coincidencia “true o false”.
IPAddress	Compara una clave con una dirección IP o un rango de direcciones IP.
NotIpAddress	Compara una clave con una dirección IP o un intervalo de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si hay una clave de condición en el contexto actual de la solicitud.

Teclas de condición compatibles

Teclas de condición	Acciones	Descripción
aws:SourceIp	Operadores IP	Comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos. **Nota:** Si la solicitud S3 se envió a través del servicio Load Balancer en nodos Admin y nodos de Gpuertas de enlace, se comparará con la dirección IP anterior al servicio Load Balancer. **Nota**: Si se utiliza un equilibrador de carga no transparente de terceros, se comparará con la dirección IP de ese equilibrador de carga. Cualquiera `X-Forwarded-For` el encabezado se ignorará porque no se puede determinar su validez.
aws:nombre de usuario	Recurso/identidad	Comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones de bloques u objetos.
s3:delimitador	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.

Teclas de condición	Acciones	Descripción
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectEtiquetado S3:PutObjectVersionAcl s3:PutObjectVersionEtiquetado	Requerirá que el objeto existente tenga la clave de etiqueta y el valor específicos.
s3:max-keys	s3:ListBucket y. s3:ListBucketVersions permisos	Se compara con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.
s3:retención-días restante del bloqueo de objetos	s3:PutObject	Compara con la fecha de retención hasta especificada en `x-amz-object-lock-retain-until-date` cabecera de solicitud o calculada desde el período de retención predeterminado de bloque para asegurarse de que estos valores están dentro del intervalo permitido para las siguientes solicitudes: • Objeto de puta • CopyObject • CreateMultipartUpload
s3:retención-días restante del bloqueo de objetos	s3:PutObjectRetention	Se compara con la fecha de retención especificada en la solicitud PutObjectRetention para asegurarse de que se encuentra dentro del rango permitido.

Teclas de condición	Acciones	Descripción
s3:prefijo	s3:ListBucket y. s3:ListBucketVersions permisos	Se comparará con el parámetro PreFIX especificado en una solicitud ListObjects o ListObjectVersions.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectEtiquetado s3:PutObjectVersionEtiquetado	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud del objeto incluya el etiquetado.

Especifique las variables en una política

Las variables de las directivas se pueden utilizar para rellenar la información de directivas cuando esté disponible. Se pueden usar variables de política en la `Resource` comparaciones entre elementos y cadenas en la `Condition` elemento.

En este ejemplo, la variable `${aws:username}` Forma parte del elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` forma parte del valor de condición en el bloque de condición:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Descripción
`${aws:SourceIp}`	Utiliza la clave SourceIp como la variable proporcionada.
`${aws:username}`	Utiliza la clave de nombre de usuario como la variable proporcionada.
`${s3:prefix}`	Utiliza la clave de prefijo específica del servicio como variable proporcionada.
`${s3:max-keys}`	Utiliza la clave de max-keys específica del servicio como la variable proporcionada.

Variable	Descripción
`${*}`	Carácter especial. Utiliza el carácter como carácter literal *.
`${?}`	Carácter especial. Utiliza el carácter como literal ? carácter.
`${$}`	Carácter especial. Utiliza el carácter como carácter literal $.

Crear directivas que requieran un manejo especial

A veces, una directiva puede otorgar permisos peligrosos para la seguridad o para operaciones continuas, como bloquear al usuario raíz de la cuenta. La implementación de la API REST de StorageGRID S3 es menos restrictiva durante la validación de políticas que Amazon, pero igual de estricta durante la evaluación de la política.

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Denegar a sí mismo cualquier permiso a la cuenta raíz	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Denegar a sí mismo cualquier permiso al usuario o grupo	Grupo	Válido y reforzado	Igual
Permitir cualquier permiso para un grupo de cuentas externo	Cucharón	Principal no válido	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política
Permitir cualquier permiso para una raíz de cuenta externa o para un usuario	Cucharón	Válidos, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un método 405 no permitido cuando lo permite una política	Igual
Permitir que todos tengan permisos para todas las acciones	Cucharón	Válido, pero los permisos para todas las operaciones de política de bloques de S3 devuelven un error de método 405 no permitido para la raíz de cuenta externa y los usuarios	Igual

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Denegar a todos los permisos a todas las acciones	Cucharón	Válido y reforzado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bloques de S3	Igual
Principal es un usuario o grupo inexistente	Cucharón	Principal no válido	Válido
El recurso es un bloque de S3 que no existe	Grupo	Válido	Igual
El director es un grupo local	Cucharón	Principal no válido	Válido
Policy otorga a una cuenta no propietaria (incluidas las cuentas anónimas) permisos para colocar objetos.	Cucharón	Válido. Los objetos son propiedad de la cuenta creadora y la política de bucket no se aplica. La cuenta de creador debe otorgar permisos de acceso al objeto mediante ACL de objeto.	Válido. Los objetos son propiedad de la cuenta de propietario del bloque. Se aplica la política de bloques.

Protección WORM (escritura única lectura múltiple)

Se pueden crear bloques DE escritura única y lectura múltiple (WORM) para proteger los datos, los metadatos de objetos definidos por el usuario y el etiquetado de objetos de S3. Puede configurar los bloques WORM para permitir la creación de objetos nuevos y evitar sobrescrituras o eliminaciones del contenido existente. Utilice uno de los enfoques aquí descritos.

Para asegurarse de que las sobrescrituras se deniegan siempre, puede:

- En Grid Manager, vaya a **CONFIGURACIÓN** > **SEGURIDAD** > **CONFIGURACIÓN DE SEGURIDAD** > **RED AND OBJECTS** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplique las siguientes reglas y políticas de S3:
  - Agregue una operación PUTOVERWRITEOBJECT DENY a la directiva S3.
  - Agregue una operación DeleteObject DENY a la directiva S3.
  - Agregue una operación PutObject ALLOW a la política S3.

> Si se configura DeleteObject como DENEGADO en una política de S3, ILM no impide que elimine objetos cuando existe una regla como «copias cero tras 30 días».

> Incluso cuando se aplican todas estas reglas y políticas, no protegen frente a escrituras simultáneas (consulte la situación A). Protegen contra sobrescrituras completadas secuenciales (consulte la situación B).

Situación A: Escrituras simultáneas (no protegidas contra)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situación B: Sobrescrituras completadas secuenciales (protegidas contra)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Información relacionada

- "Cómo gestionan las reglas de ILM de StorageGRID los objetos"
- "Ejemplo de políticas de bloque"
- "Ejemplo de políticas de grupo"
- "Gestión de objetos con ILM"
- "Usar una cuenta de inquilino"

Ejemplo de políticas de bloque

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para buckets.

Las políticas de bloque especifican los permisos de acceso para el bloque al que está asociada la directiva. Las políticas de bloque se configuran mediante la API de S3 PutBucketPolicy. Consulte "Operaciones en bloques".

Se puede configurar una política de bloques mediante la CLI de AWS según el siguiente comando:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Ejemplo: Permitir que todos tengan acceso de solo lectura a un bloque

En este ejemplo, a todos, incluido el anónimo, se les permite enumerar objetos en el depósito y realizar operaciones GetObject en todos los objetos del depósito. Se denegarán todas las demás operaciones. Tenga en cuenta que esta política puede no ser particularmente útil porque nadie, excepto la raíz de la cuenta, tiene permisos para escribir en el depósito.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Ejemplo: Permitir que todos en una cuenta tengan acceso total y que todas las personas de otra cuenta tengan acceso de solo lectura a un bloque

En este ejemplo, se permite a todos los integrantes de una cuenta especificada el acceso completo a un bloque, mientras que a todos los miembros de otra cuenta especificada sólo se les permite enumerar el bloque y realizar operaciones GetObject en los objetos del bloque empezando por el `shared/` prefijo de clave de objeto.

> En StorageGRID, los objetos creados por una cuenta que no es propietaria (incluidas las cuentas anónimas) son propiedad de la cuenta de propietario del bloque. La política de bloque se aplica a estos objetos.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de solo lectura a un bloque y acceso completo por un grupo especificado

En este ejemplo, todos, incluidos los anónimos, pueden enumerar el depósito y realizar operaciones GetObject en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo `Marketing` en la cuenta especificada se permite el acceso completo.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permitir que todo el mundo tenga acceso de lectura y escritura a un bloque si un cliente se encuentra en el rango de IP

En este ejemplo, todos, incluido el anónimo, pueden enumerar el bloque y realizar cualquier operación Object en todos los objetos del bloque, siempre que las solicitudes provengan de un intervalo IP especificado (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se denegarán todas las demás operaciones y se denegarán todas las solicitudes que estén fuera del rango de IP.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Ejemplo: Permitir el acceso completo a un bloque exclusivamente por un usuario federado especificado

En este ejemplo, el usuario federado Alex tiene permiso de acceso completo al `examplebucket` cucharón y sus objetos. A todos los demás usuarios, incluido "root", se les deniega explícitamente todas las operaciones. Tenga en cuenta, sin embargo, que "root" nunca se le deniegan los permisos para poner/obtener/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Ejemplo: Permiso PutOverwriteObject

En este ejemplo, la `Deny` Effect para PutOverwriteObject y DeleteObject garantiza que nadie puede sobrescribir ni eliminar los datos del objeto, los metadatos definidos por el usuario y el etiquetado de objetos S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Ejemplo de políticas de grupo

Utilice los ejemplos de esta sección para crear políticas de acceso StorageGRID para grupos.

Las directivas de grupo especifican los permisos de acceso para el grupo al que está asociada la directiva. No existe `Principal` elemento de la política porque está implícito. Las políticas de grupo se configuran con el administrador de inquilinos o la API.

Ejemplo: Establecer la directiva de grupo mediante el Administrador de inquilinos

Al agregar o editar un grupo en el Gestor de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso S3 tendrán los miembros de este grupo. Consulte "Cree grupos para un inquilino de S3".

- **Sin acceso S3**: Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
- **Acceso de sólo lectura**: Los usuarios de este grupo tienen acceso de sólo lectura a los recursos S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
- **Acceso completo**: Los usuarios de este grupo tienen acceso completo a los recursos S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.
- **Ransomware Mitigation**: Esta política de muestra se aplica a todos los cubos para este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos.

  Los usuarios del gestor de inquilinos que tengan el permiso Gestionar todos los bloques pueden sustituir esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.

- **Personalizado**: A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

Ejemplo: Permite el acceso total de grupos a todos los bloques

En este ejemplo, a todos los miembros del grupo se les permite el acceso completo a todos los segmentos que pertenecen a la cuenta de inquilino, a menos que la política de bloque lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir el acceso de solo lectura de grupo a todos los bloques

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a recursos S3, a menos que la política de bloque lo deniegue explícitamente. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir a los miembros del grupo acceso completo solo a su carpeta en un depósito

En este ejemplo, sólo se permite a los miembros del grupo que enumeren y tengan acceso a su carpeta específica (prefijo de clave) en el bloque especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la directiva de bloque deben tenerse en cuenta al determinar la privacidad de estas carpetas.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.