# Políticas de acceso a grupos y buckets

StorageGRID software

NetApp
December 03, 2025

# Tabla de contenidos

# Políticas de acceso a grupos y buckets

## Utilice políticas de acceso a grupos y buckets

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

### Descripción general de la política de acceso

StorageGRID admite dos tipos de políticas de acceso.

- **Políticas de bucket**, que se administran mediante las operaciones de API S3 GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy o la API Tenant Manager o Tenant Management. Las políticas de depósito se adjuntan a los depósitos, por lo que están configuradas para controlar el acceso de los usuarios en la cuenta del propietario del depósito u otras cuentas al depósito y a los objetos que contiene. Una política de buckets se aplica solo a un bucket y posiblemente a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las políticas de grupo están asociadas a un grupo en la cuenta, por lo que están configuradas para permitir que ese grupo acceda a recursos específicos que pertenecen a esa cuenta. Una política de grupo se aplica solo a un grupo y posiblemente a varios grupos.

> ⓘ No hay diferencia de prioridad entre las políticas de grupo y de grupo.

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

- ID de declaración (Sid) (opcional)
- Efecto
- Director/No director
- Recurso/NoRecurso
- Acción/No acción
- Condición (opcional)

Las declaraciones de política se crean utilizando esta estructura para especificar permisos: Otorgar <Efecto> para permitir/denegar que <Principal> realice <Acción> en <Recurso> cuando se aplica <Condición>.

Cada elemento de política se utiliza para una función específica:

| Elemento | Descripción |
|---|---|
| Sid | El elemento Sid es opcional. El Sid solo pretende servir como descripción para el usuario. Se almacena pero no es interpretado por el sistema StorageGRID . |

| Elemento | Descripción |
| --- | --- |
| Efecto | Utilice el elemento Efecto para establecer si las operaciones especificadas están permitidas o denegadas. Debe identificar las operaciones que permite (o deniega) en depósitos u objetos utilizando las palabras clave del elemento Acción compatible. |
| Director/No director | Puede permitir que usuarios, grupos y cuentas accedan a recursos específicos y realicen 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, solo la cuenta raíz tiene acceso a los recursos que posee la cuenta.<br><br>Solo es necesario especificar el elemento Principal en una política de bucket. Para las políticas de grupo, el grupo al que está asociada la política es el elemento Principal implícito. |
| Recurso/NoRecurso | El elemento Recurso identifica depósitos y objetos. Puede permitir o denegar permisos para depósitos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso. |
| Acción/No acción | 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 mismo. Se deniega el acceso a menos que usted asigne permisos específicos, pero puede usar la denegación explícita para anular un permiso otorgado por otra política. |
| Condición | El elemento Condición es opcional. Las condiciones le permiten crear expresiones para determinar cuándo se debe aplicar una política. |

En el elemento Acción, 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 Recurso, puede utilizar los caracteres comodín (*) y (?). Mientras que el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter individual.

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

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

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

En el siguiente ejemplo, la declaración utiliza los elementos Efecto, Principal, Acción y Recurso. Este ejemplo

muestra una declaración de política de bucket completa que utiliza el efecto "Permitir" para otorgar a los principales, el grupo de administración `federated-group/admin` y el grupo financiero `federated-group/finance` , permisos para realizar la Acción `s3:ListBucket` en el cubo llamado `mybucket` y la Acción `s3:GetObject` en todos los objetos dentro de ese cubo.

```
{
  "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:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de depósito tiene un límite de tamaño de 20 480 bytes y la política de grupo tiene un límite de tamaño de 5120 bytes.

## Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice en las políticas de grupo será coherente en el futuro. Cuando una política de grupo se vuelve consistente, los cambios pueden tardar 15 minutos adicionales en surtir efecto, debido al almacenamiento en caché de la política. De forma predeterminada, todas las actualizaciones que realice en las políticas de depósito serán muy coherentes.

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

En este caso, puede configurar el `Consistency-Control` encabezado en la solicitud PutBucketPolicy, o puede utilizar la solicitud de consistencia PUT Bucket. Cuando una política de bucket se vuelve consistente, los cambios pueden tardar 8 segundos adicionales en surtir efecto, debido al almacenamiento en caché de políticas.

Si establece la consistencia en un valor diferente para solucionar una situación temporal, asegúrese de restablecer la configuración de nivel de depósito a su valor original cuando haya terminado. De lo contrario, todas las futuras solicitudes de bucket utilizarán la configuración modificada.

## Utilice ARN en declaraciones de políticas

En las declaraciones de políticas, el ARN se utiliza en los elementos Principal y Recurso.

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

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

- Utilice esta sintaxis para especificar el ARN del recurso de identidad (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 del objeto.
- Los caracteres internacionales, que se pueden especificar en la clave del objeto, deben codificarse utilizando JSON UTF-8 o utilizando secuencias de escape JSON \u. No se admite la codificación porcentual.

  "Sintaxis URN RFC 2141"

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

## Especificar recursos en una política

En las declaraciones de políticas, puede utilizar el elemento Recurso para especificar el depósito o el objeto para el cual se permiten o deniegan permisos.

- Cada declaración de política requiere un elemento de recurso. En una política, los recursos se denotan mediante el elemento `Resource` , o alternativamente, `NotResource` para exclusión.
- Usted especifica recursos con un ARN de recurso S3. Por ejemplo:

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

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

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

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

## Especificar los principales en una política

Utilice el elemento Principal para identificar el usuario, grupo o cuenta de inquilino a quien se le permite o deniega el acceso al recurso mediante la declaración de política.

- Cada declaración de política en una política de grupo debe incluir un elemento Principal. Las declaraciones de política en una política de grupo no necesitan el elemento Principal porque se entiende que el grupo es el principal.
- En una política, los principales se indican con el elemento "Principal" o, alternativamente, "NoPrincipal" para su exclusión.
- Las identidades basadas en cuentas deben especificarse mediante un ID o un ARN:

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

- Este ejemplo 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 solo la cuenta raíz:

```
"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 ("Administradores"):

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

- Puede especificar un principal anónimo:

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

- Para evitar ambigüedades, puede utilizar el UUID del 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 elimina Si un nuevo Alex se une a la organización y se le asigna el mismo `Alex` nombre de usuario, el nuevo usuario podría heredar involuntariamente los permisos otorgados al usuario original.

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

## Especificar permisos en una política

En una política, el elemento Acción se utiliza para permitir o denegar permisos a un recurso. Hay un conjunto de permisos que puedes especificar en una política, que se indican con el elemento "Acción" o, alternativamente, "No acción" para la exclusión. Cada uno de estos elementos se asigna a operaciones específicas de la API REST de S3.

Las tablas enumeran los permisos que se aplican a los depósitos 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 separados para cada acción, lo que coincide con la especificación original de Amazon S3.

> Se realiza una eliminación cuando se utiliza una operación put para sobrescribir un valor existente.

**Permisos que se aplican a los buckets**

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:CrearCubo | Crear cubo | Sí.<br><br>**Nota**: Úselo solo en políticas de grupo. |
| s3:Eliminar depósito | Eliminar cubo | |
| s3:Notificación de metadatos de eliminación de depósito | Configuración de notificación de metadatos del depósito DELETE | Sí |
| s3: Eliminar política de depósito | Política de eliminación de cubos | |

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:Eliminar configuración de replicación | EliminarReplicaciónDeBucket | Sí, permisos separados para PUT y DELETE |
| s3:ObtenerAcl del depósito | ObtenerBucketAcl | |
| s3:Obtener cumplimiento del cubo | Cumplimiento de GET Bucket (obsoleto) | Sí |
| s3: Obtener consistencia del cubo | Obtener consistencia del bucket | Sí |
| s3:ObtenerBucketCORS | ObtenerBucketCors | |
| s3:Obtener configuración de cifrado | Obtener cifrado de cubo | |
| s3: Obtener hora del último acceso al depósito | GET Hora del último acceso al bucket | Sí |
| s3: Obtener ubicación del depósito | Obtener la ubicación del cubo | |
| s3:Obtener notificación de metadatos del depósito | Configuración de notificación de metadatos del depósito GET | Sí |
| s3:Obtener notificación del cubo | Configuración de GetBucketNotification | |
| s3:Configuración de bloqueo de objeto de depósito | Obtener configuración de bloqueo de objeto | |
| s3: Obtener política de depósito | Obtener política de cubo | |
| s3: Obtener etiquetado de cubo | Obtener etiquetado de cubos | |
| s3: Obtener versiones de Bucket | Obtener versiones de Bucket | |
| s3:Obtener configuración del ciclo de vida | Obtener configuración del ciclo de vida del cubo | |
| s3:Obtener configuración de replicación | Obtener réplica de cubo | |
| s3: Listar todos mis cubos | • Lista de cubos<br>• Uso de almacenamiento GET | Sí, para el uso de almacenamiento GET.<br><br>**Nota**: Úselo solo en políticas de grupo. |

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:ListBucket | • Lista de objetos<br>• Cubo de cabeza<br>• Restaurar objeto | |
| s3:ListBucketMultipartUploads | • Lista de cargas de varias partes<br>• Restaurar objeto | |
| s3:ListBucketVersions | GET Versiones del Bucket | |
| s3:Cumplimiento de PutBucket | Cumplimiento del contenedor PUT (obsoleto) | Sí |
| s3:Consistencia del cubo de colocación | Consistencia del depósito PUT | Sí |
| s3:PonerCuboCORS | • EliminarBucketCors†<br>• PonerBucketCors | |
| s3:PonerConfiguraciónDeCifrado | • Eliminar cifrado del cubo<br>• Cifrado de PutBucket | |
| s3:PonerBucketÚltimoAccesoHora | Hora del último acceso al depósito PUT | Sí |
| s3:Notificación de metadatos de PutBucket | Configuración de notificación de metadatos del depósito PUT | Sí |
| s3:Notificación de depósito de colocación | Configuración de notificación de PutBucket | |
| s3:Configuración de bloqueo de objeto PutBucket | • CreateBucket con el `x-amz-bucket-object-lock-enabled: true` encabezado de solicitud (también requiere el permiso s3:CreateBucket)<br>• Configuración de bloqueo de objeto de colocación | |
| s3:Política de depósito de colocación | Política de depósito de basura | |
| s3:Etiquetado de cubo de colocación | • Eliminar etiquetado de cubos†<br>• Etiquetado de PutBucket | |
| s3:Versión de PutBucket | Versiones de PutBucket | |

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:Configuración del ciclo de vida de PutLifecycle | • Eliminar ciclo de vida del cubo†<br>• Configuración del ciclo de vida de PutBucket | |
| s3:PonerConfiguraciónDeReplicación | Replicación de PutBucket | Sí, permisos separados para PUT y DELETE |

**Permisos que se aplican a los objetos**

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:AbortarCargaMultiparte | • AbortarMultipartUpload<br>• Restaurar objeto | |
| s3: Retención de gobernanza de bypass | • Eliminar objeto<br>• Eliminar objetos<br>• PonerRetenciónDeObjeto | |
| s3:EliminarObjeto | • Eliminar objeto<br>• Eliminar objetos<br>• Restaurar objeto | |
| s3:EliminarEtiquetadoDeObjeto | Eliminar etiquetado de objetos | |
| s3: Eliminar etiquetado de versión de objeto | DeleteObjectTagging (una versión específica del objeto) | |
| s3:EliminarVersiónDeObjeto | DeleteObject (una versión específica del objeto) | |
| s3:Obtener objeto | • Obtener objeto<br>• Objeto principal<br>• Restaurar objeto<br>• Seleccionar contenido del objeto | |
| s3:ObtenerAclObjeto | ObtenerObjetoAcl | |
| s3:ObtenerRetenciónLegalDeObjeto | Obtener retención legal de objeto | |

| Permisos | Operaciones de la API REST de S3 | Personalizado para StorageGRID |
|---|---|---|
| s3:ObtenerRetenciónDeObjeto | Obtener retención de objetos | |
| s3:Obtener etiquetado de objeto | Obtener etiquetado de objetos | |
| s3: Obtener etiquetado de versión de objeto | GetObjectTagging (una versión específica del objeto) | |
| s3:ObtenerVersiónDeObjeto | GetObject (una versión específica del objeto) | |
| s3:ListaMultiparteSubirPartes | Lista de partes, Restaurar objeto | |
| s3:PonerObjeto | • PonerObjeto<br>• Copiar objeto<br>• Restaurar objeto<br>• Crear carga de varias partes<br>• Carga completa de varias partes<br>• Subir parte<br>• Subir copia parcial | |
| s3:PonerObjetoLegalRetenido | PonerObjetoLegalRetención | |
| s3:PonerRetenciónDeObjeto | PonerRetenciónDeObjeto | |
| s3:Etiquetado de objetos de colocación | Etiquetado de objetos puestos | |
| s3:Etiquetado de versión de objeto de colocación | PutObjectTagging (una versión específica del objeto) | |
| s3:PonerObjetoSobrescrito | • PonerObjeto<br>• Copiar objeto<br>• Etiquetado de objetos puestos<br>• Eliminar etiquetado de objetos<br>• Carga completa de varias partes | Sí |
| s3:RestaurarObjeto | Restaurar objeto | |

## Utilice el permiso PutOverwriteObject

El permiso s3:PutOverwriteObject es un permiso de StorageGRID personalizado que se aplica a las operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede

sobrescribir los datos de un objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3.

Las posibles configuraciones para este permiso 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 del objeto S3 no se pueden sobrescribir.
    - Cualquier operación de ingesta en curso se cancela y se devuelve un error.
    - Si el control de versiones S3 está habilitado, la configuración Denegar evita que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet de 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 estuviera configurado Permitir.

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

## Especificar condiciones en una póliza

Las condiciones definen cuándo entrará en vigor una política. Las condiciones constan de operadores y pares clave-valor.

Las condiciones utilizan pares clave-valor para la evaluación. Un elemento Condición puede contener múltiples condiciones, y cada condición puede contener múltiples pares clave-valor. El bloque de condición utiliza el siguiente formato:

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

En el siguiente ejemplo, 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 clasifican de la siguiente manera:

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

| Operadores de condición | Descripción |
|---|---|
| CadenaIgual | Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas). |
| CadenaNoIgual | Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas). |
| CadenaIgualIgnorarMayúsculas y Minúsculas | Compara una clave con un valor de cadena basándose en la coincidencia exacta (ignora mayúsculas y minúsculas). |
| CadenaNoIgualIgnorarMayúsculas y Minúsculas | Compara una clave con un valor de cadena basándose en la coincidencia negada (ignora mayúsculas y minúsculas). |
| Similar a una cadena | Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?. |
| CadenaNoMe Gusta | Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?. |
| NumericEquals | Compara una clave con un valor numérico basándose en la coincidencia exacta. |
| NuméricoNoIgual | Compara una clave con un valor numérico basándose en la coincidencia negada. |
| NuméricoMayorQue | Compara una clave con un valor numérico basándose en la coincidencia "mayor que". |
| NuméricoMayorQueIgual | Compara una clave con un valor numérico basándose en la coincidencia "mayor o igual que". |
| NuméricoMenosQue | Compara una clave con un valor numérico basándose en la coincidencia "menor que". |

| Operadores de condición | Descripción |
|---|---|
| NuméricoMenorQueIgual | Compara una clave con un valor numérico basándose en la coincidencia "menor o igual que". |
| Bool | Compara una clave con un valor booleano basándose en la coincidencia "verdadero o falso". |
| Dirección IP | Compara una clave con una dirección IP o un rango de direcciones IP. |
| No dirección IP | Compara una clave con una dirección IP o un rango de direcciones IP basándose en la coincidencia negada. |
| Nulo | Comprueba si una clave de condición está presente en el contexto de solicitud actual. |

**Claves de condición admitidas**

| Claves de condición | Comportamiento | Descripción |
|---|---|---|
| aws:FuenteIp | Operadores de IP | Se comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos.<br><br>**Nota:** Si la solicitud S3 se envió a través del servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace, esto se comparará con la dirección IP ascendente del servicio Load Balancer.<br><br>**Nota**: Si se utiliza un balanceador de carga de terceros no transparente, esto se comparará con la dirección IP de ese balanceador de carga. Cualquier `X-Forwarded-For` El encabezado se ignorará porque no se puede determinar su validez. |
| aws:nombre de usuario | Recurso/Identidad | Se comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos. |
| s3:delimitador | s3:ListBucket y<br><br>Permisos s3:ListBucketVersions | Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions. |

| Claves de condición | Comportamiento | Descripción |
| --- | --- | --- |
| s3:ExistingObjectTag/<clave de etiqueta> | s3:EliminarEtiquetadoDeObjeto<br><br>s3: Eliminar etiquetado de versión de objeto<br><br>s3:Obtener objeto<br><br>s3:ObtenerAclObjeto<br><br>3: Obtener etiquetado de objetos<br><br>s3:ObtenerVersiónDeObjeto<br><br>s3:ObtenerAcl de versión de objeto<br><br>s3: Obtener etiquetado de versión de objeto<br><br>s3:PonerObjetoAcl<br><br>s3:Etiquetado de objetos de colocación<br><br>s3:PonerObjetoVersiónAcl<br><br>s3:Etiquetado de versión de objeto de colocación | Requerirá que el objeto existente tenga la clave y el valor de etiqueta específicos. |
| s3:máximo de teclas | s3:ListBucket y<br><br>Permisos s3:ListBucketVersions | Se comparará con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions. |
| s3: días de retención restantes del bloqueo de objeto | s3:PonerObjeto | Se compara con la fecha de conservación especificada en el `x-amz-object-lock-retain-until-date` encabezado de solicitud o calculado a partir del período de retención predeterminado del depósito para asegurarse de que estos valores estén dentro del rango permitido para las siguientes solicitudes:<br><br>• PonerObjeto<br>• Copiar objeto<br>• Crear carga de varias partes |

| Claves de condición | Comportamiento | Descripción |
|---|---|---|
| s3: días de retención restantes del bloqueo de objeto | s3:PonerRetenciónDeObjeto | Se compara con la fecha de retención hasta especificada en la solicitud PutObjectRetention para garantizar que esté dentro del rango permitido. |
| s3:prefijo | s3:ListBucket y<br><br>Permisos s3:ListBucketVersions | Se comparará con el parámetro de prefijo especificado en una solicitud ListObjects o ListObjectVersions. |
| s3:RequestObjectTag/<clave de etiqueta> | s3:PonerObjeto<br><br>s3:Etiquetado de objetos de colocación<br><br>s3:Etiquetado de versión de objeto de colocación | Requerirá una clave y un valor de etiqueta específicos cuando la solicitud de objeto incluya etiquetado. |

## Especificar variables en una política

Puede utilizar variables en las políticas para completar la información de políticas cuando esté disponible. Puede utilizar variables de política en el `Resource` elemento y en comparaciones de cadenas en el `Condition` elemento.

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

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

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

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

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

| Variable | Descripción |
| --- | --- |
| `${s3:max-keys}` | Utiliza la clave max-keys específica del servicio como variable proporcionada. |
| `${*}` | Carácter especial. Utiliza el carácter como un carácter literal *. |
| `${?}` | Carácter especial. Utiliza el carácter como un carácter literal ?. |
| `${$}` | Carácter especial. Utiliza el carácter como un carácter literal $. |

## Crear políticas que requieran un manejo especial

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

| Descripción de la política | Tipo de póliza | Comportamiento de Amazon | Comportamiento de StorageGRID |
| --- | --- | --- | --- |
| Negarse a sí mismo cualquier permiso a la cuenta raíz | Balde | Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3 | Mismo |
| Negarme cualquier permiso a un usuario o grupo | Grupo | Válido y ejecutado | Mismo |
| Permitir a un grupo de cuentas extranjeras cualquier permiso | Balde | Principal inválido | Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política |
| Permitir a una cuenta externa root o a un usuario cualquier permiso | Balde | Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política | Mismo |

| Descripción de la política | Tipo de póliza | Comportamiento de Amazon | Comportamiento de StorageGRID |
|---|---|---|---|
| Permitir a todos permisos para todas las acciones | Balde | Válido, pero los permisos para todas las operaciones de política de bucket S3 devuelven un error 405 Método no permitido para la raíz de la cuenta externa y los usuarios | Mismo |
| Negar a todos los permisos para todas las acciones | Balde | Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3 | Mismo |
| El principal es un usuario o grupo inexistente | Balde | Principal inválido | Válido |
| El recurso es un bucket S3 inexistente | Grupo | Válido | Mismo |
| Principal es un grupo local | Balde | Principal inválido | Válido |
| La política otorga a una cuenta que no es de propietario (incluidas las cuentas anónimas) permisos para colocar objetos. | Balde | Válido. Los objetos son propiedad de la cuenta del creador y la política de buckets no se aplica. La cuenta del creador debe otorgar permisos de acceso para el objeto mediante listas de control de acceso (ACL) de objeto. | Válido. Los objetos son propiedad de la cuenta del propietario del depósito. Se aplica la política de cubos. |

## Protección de escritura única y lectura múltiple (WORM)

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

Para garantizar que siempre se rechacen las sobrescrituras, puede:

- Desde el Administrador de red, vaya a **CONFIGURACIÓN** > **Seguridad** > **Configuración de seguridad** > **Red y objetos** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplicar las siguientes reglas y políticas S3:
  - Agregue una operación PutOverwriteObject DENY a la política S3.
  - Agregue una operación DeleteObject DENY a la política S3.

- Agregue una operación PutObject ALLOW a la política S3.

> Establecer DeleteObject como DENY en una política S3 no impide que ILM elimine objetos cuando existe una regla como "cero copias después de 30 días".

> Incluso cuando se aplican todas estas reglas y políticas, no protegen contra escrituras simultáneas (ver Situación A). Protegen contra sobrescrituras completadas secuenciales (ver Situación B).

**Situación A**: Escrituras concurrentes (sin protección)

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

**Situación B**: Sobrescrituras secuenciales completadas (protegidas contra)

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

**Información relacionada**

- "Cómo las reglas ILM de StorageGRID administran los objetos"
- "Ejemplos de políticas de depósito"
- "Políticas de grupo de ejemplo"
- "Administrar objetos con ILM"
- "Utilice una cuenta de inquilino"

# Ejemplos de políticas de depósito

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

Las políticas de depósito especifican los permisos de acceso para el depósito al que está asociada la política. Puede configurar una política de bucket mediante la API S3 PutBucketPolicy a través de una de estas herramientas:

- "Administrador de inquilinos" .
- AWS CLI usando este comando (consulte"Operaciones en buckets" ):

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

## Ejemplo: Permitir a todos el acceso de solo lectura a un depósito

En este ejemplo, todos, incluso los anónimos, pueden 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 cuenta raíz 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 a todos los usuarios de una cuenta acceso completo y a todos los usuarios de otra cuenta acceso de solo lectura a un depósito.

En este ejemplo, a todos en una cuenta específica se les permite acceso completo a un depósito, mientras que a todos en otra cuenta específica solo se les permite listar el depósito y realizar operaciones GetObject en objetos en el depósito comenzando con el `shared/` prefijo de clave de objeto.

> En StorageGRID, los objetos creados por una cuenta que no es de propietario (incluidas las cuentas anónimas) son propiedad de la cuenta del propietario del depósito. La política de bucket 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 a todos acceso de solo lectura a un depósito y acceso completo a un grupo específico

En este ejemplo, todos, incluido el anónimo, pueden listar 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 a todos el acceso de lectura y escritura a un depósito si el cliente está en el rango de IP

En este ejemplo, todos, incluso los anónimos, pueden enumerar el depósito y realizar cualquier operación de objeto en todos los objetos del depósito, siempre que las solicitudes provengan de un rango de IP específico (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se rechazarán todas las demás operaciones y todas las solicitudes 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 depósito exclusivamente a un usuario federado específico

En este ejemplo, al usuario federado Alex se le permite acceso completo a la `examplebucket` cubo y sus objetos. A todos los demás usuarios, incluido 'root', se les niega explícitamente todas las operaciones. Sin embargo, tenga en cuenta que a 'root' nunca se le niegan los permisos para Put/Get/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, el `Deny` El efecto para PutOverwriteObject y DeleteObject garantiza que nadie pueda sobrescribir o 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/*"
    }
  ]
}
```

# Políticas de grupo de ejemplo

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

Las políticas de grupo especifican los permisos de acceso para el grupo al que está asociada la política. No hay `Principal` elemento de la política porque es implícito. Las políticas de grupo se configuran mediante el Administrador de inquilinos o la API.

## Ejemplo: Establecer una política de grupo mediante el Administrador de inquilinos

Cuando agrega o edita un grupo en el Administrador de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso a S3 tendrán los miembros de este grupo. Ver "Crear 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 se les conceda acceso con una política de bucket. Si selecciona esta opción, solo el usuario root tendrá acceso a los recursos de S3 de forma predeterminada.
- **Acceso de solo lectura**: los usuarios de este grupo tienen acceso de solo lectura a los recursos de 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 puedes editar esta cadena.
- **Acceso completo**: los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puedes editar esta cadena.
- **Mitigación de ransomware**: esta política de muestra se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los depósitos que tienen habilitada la versión de objetos.

  Los usuarios del administrador de inquilinos que tienen el permiso Administrar todos los depósitos pueden anular esta política de grupo. Limite el permiso Administrar todos los depósitos a usuarios de confianza y utilice la autenticación multifactor (MFA) cuando esté disponible.

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

## Ejemplo: Permitir al grupo acceso completo a todos los depósitos

En este ejemplo, a todos los miembros del grupo se les permite acceso total a todos los depósitos propiedad de la cuenta del inquilino, a menos que la política del depósito lo deniegue explícitamente.

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

## Ejemplo: Permitir acceso de solo lectura al grupo a todos los depósitos

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a los recursos de S3, a menos que la política del bucket lo niegue 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 únicamente a su "carpeta" en un depósito

En este ejemplo, a los miembros del grupo solo se les permite enumerar y acceder a su carpeta específica (prefijo de clave) en el depósito especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la política de depósito deben considerarse 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



## Información de la marca comercial