Políticas de acesso ao bucket e ao grupo

StorageGRID

NetApp
March 12, 2025

Índice

Políticas de acesso ao bucket e ao grupo

Use políticas de acesso de grupo e bucket

O StorageGRID usa a linguagem de política da Amazon Web Services (AWS) para permitir que os locatários do S3 controlem o acesso a buckets e objetos nesses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST S3. As políticas de acesso para a API S3 são escritas em JSON.

Visão geral da política de acesso

Existem dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy S3. As políticas de bucket são anexadas a buckets, portanto, são configuradas para controlar o acesso dos usuários na conta de proprietário do bucket ou outras contas ao bucket e aos objetos nele contidos. Uma política de bucket se aplica a apenas um bucket e possivelmente a vários grupos.
- **Políticas de grupo**, que são configuradas usando o Gerenciador do locatário ou a API de gerenciamento do locatário. As políticas de grupo são anexadas a um grupo na conta, portanto são configuradas para permitir que esse grupo acesse recursos específicos de propriedade dessa conta. Uma política de grupo se aplica a apenas um grupo e possivelmente vários buckets.

Não há diferença na prioridade entre as políticas de grupo e bucket.

As políticas de grupo e bucket do StorageGRID seguem uma gramática específica definida pela Amazon. Dentro de cada política há uma matriz de declarações de política, e cada declaração contém os seguintes elementos:

- ID de declaração (Sid) (opcional)
- Efeito
- Principal/NotPrincipal
- Recurso/não recurso
- Ação/não Ação
- Condição (opcional)

As instruções de política são criadas usando essa estrutura para especificar permissões: Grant <Effect> para permitir/negar que o <Principal> execute o <Action> no <Resource> quando o <Condition> se aplicar.

Cada elemento de política é usado para uma função específica:

Elemento	Descrição
SID	O elemento Sid é opcional. O Sid é apenas uma descrição para o usuário. Ele é armazenado, mas não interpretado pelo sistema StorageGRID.

Elemento	Descrição
Efeito	Use o elemento efeito para determinar se as operações especificadas são permitidas ou negadas. É necessário identificar operações que você permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Ação suportado.
Principal/NotPrincipal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 estiver incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente a raiz da conta tem acesso aos recursos de propriedade da conta. Você só precisa especificar o elemento principal em uma política de bucket. Para políticas de grupo, o grupo ao qual a política está anexada é o elemento principal implícito.
Recurso/não recurso	O elemento recurso identifica buckets e objetos. Você pode permitir ou negar permissões a buckets e objetos usando o Nome do recurso da Amazon (ARN) para identificar o recurso.
Ação/não Ação	Os elementos Ação e efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, é concedido ou negado o acesso ao recurso. O acesso é negado a menos que você atribua permissões especificamente, mas você pode usar Negar explícito para substituir uma permissão concedida por outra política.
Condição	O elemento de condição é opcional. As condições permitem que você crie expressões para determinar quando uma política deve ser aplicada.

No elemento Ação, você pode usar o caractere curinga (*) para especificar todas as operações ou um subconjunto de operações. Por exemplo, esta Ação corresponde a permissões como S3:GetObject, S3:PutObject e S3:DeleteObject.

```
s3:*Object
```

No elemento recurso, você pode usar os carateres curinga (**) e (?). Enquanto o asterisco (**) corresponde a 0 ou mais carateres, o ponto de interrogação (?) corresponde a qualquer caractere único.

No elemento principal, carateres curinga não são suportados, exceto para definir acesso anônimo, o que concede permissão a todos. Por exemplo, você define o caractere curinga (*) como o valor principal.

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

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

No exemplo a seguir, a instrução está usando os elementos efeito, Principal, Ação e recurso. Este exemplo mostra uma declaração de política de bucket completa que usa o efeito "permitir" para dar aos Principals, ao grupo admin `federated-group/admin` e ao grupo financeiro `federated-group/finance` , permissões para executar a Ação `s3:ListBucket` no bucket nomeado e a Ação `s3:GetObject` em todos os objetos dentro desse bucket `mybucket`.

```
{
  "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/*"
      ]
    }
  ]
}
```

A política de bucket tem um limite de tamanho de 20.480 bytes e a política de grupo tem um limite de tamanho de 5.120 bytes.

Consistência para políticas

Por padrão, quaisquer atualizações feitas para políticas de grupo são eventualmente consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao armazenamento em cache de políticas. Por padrão, todas as atualizações feitas às políticas de bucket são altamente consistentes.

Conforme necessário, você pode alterar as garantias de consistência para atualizações de política de bucket. Por exemplo, você pode querer que uma alteração em uma política de bucket esteja disponível durante uma falha no local.

Nesse caso, você pode definir o `Consistency-Control` cabeçalho na solicitação PutBucketPolicy ou usar a solicitação DE consistência de COLOCAR bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao armazenamento em cache de políticas.

Se você definir a consistência para um valor diferente para contornar uma situação temporária, certifique-se de definir a configuração do nível do balde de volta ao valor original quando terminar. Caso contrário, todas as futuras solicitações de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado em elementos Principal e recursos.

- Use esta sintaxe para especificar o ARN de recursos S3:

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

- Use esta sintaxe para especificar o ARN do recurso de identidade (usuários e 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
```

Outras considerações:

- Você pode usar o asterisco (*) como curinga para corresponder a zero ou mais carateres dentro da chave de objeto.
- Carateres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON. A codificação percentual não é suportada.

  "RFC 2141 sintaxe de URNA"

  O corpo de solicitação HTTP para a operação PutBucketPolicy deve ser codificado com charset UTF-8.

Especifique recursos em uma política

Em declarações de política, você pode usar o elemento recurso para especificar o intervalo ou objeto para o qual as permissões são permitidas ou negadas.

- Cada declaração de política requer um elemento recurso. Em uma política, os recursos são denotados pelo elemento `Resource` ou, alternativamente, `NotResource` para exclusão.
- Você especifica recursos com um ARN de recursos S3. Por exemplo:

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

- Você também pode usar variáveis de política dentro da chave de objeto. Por exemplo:

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

- O valor do recurso pode especificar um intervalo que ainda não existe quando uma política de grupo é criada.

Especifique princípios em uma política

Use o elemento principal para identificar a conta de usuário, grupo ou locatário que é permitido/negado acesso ao recurso pela declaração de política.

- Cada declaração de política em uma política de bucket deve incluir um elemento principal. As declarações de política em uma política de grupo não precisam do elemento principal porque o grupo é entendido como o principal.
- Em uma política, os princípios são denotados pelo elemento "principal" ou, alternativamente, "NotPrincipal" para exclusão.
- As identidades baseadas em contas devem ser especificadas usando um ID ou um ARN:

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

- Este exemplo usa o ID de conta de locatário 27233906934684427525, que inclui a raiz da conta e todos os usuários na conta:

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

- Você pode especificar apenas a raiz da conta:

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

- Você pode especificar um usuário federado específico ("Alex"):

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

- Você pode especificar um grupo federado específico ("gerentes"):

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

- Você pode especificar um principal anônimo:

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

- Para evitar ambiguidade, você pode usar o usuário UUID em vez do nome de usuário:

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

  Por exemplo, suponha que Alex deixe a organização e o nome de usuário `Alex` seja excluído. Se um novo Alex se juntar à organização e receber o mesmo `Alex` nome de usuário, o novo usuário poderá involuntariamente herdar as permissões concedidas ao usuário original.

- O valor principal pode especificar um nome de grupo/usuário que ainda não existe quando uma política de bucket é criada.

Especifique permissões em uma política

Em uma política, o elemento Ação é usado para permitir/negar permissões a um recurso. Há um conjunto de permissões que você pode especificar em uma política, que são denotadas pelo elemento "Ação" ou, alternativamente, "NotAction" para exclusão. Cada um desses elementos mapeia para operações específicas da API REST do S3.

As tabelas lista as permissões que se aplicam aos buckets e as permissões que se aplicam aos objetos.

> O Amazon S3 agora usa a permissão S3:PutReplicationConfiguration para as ações PutBucketReplication e DeleteBucketReplication. O StorageGRID usa permissões separadas para cada ação, que corresponde à especificação original do Amazon S3.

> Uma exclusão é executada quando uma put é usada para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:CreateBucket	CreateBucket	Sim. **Nota**: Use somente na política de grupo.
S3:DeleteBucket	DeleteBucket	
S3:DeleteBucketMetadataNotification	ELIMINAR configuração de notificação de metadados do bucket	Sim
S3:DeleteBucketPolicy	DeleteBucketPolicy	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:DeleteReplicationConfiguration	DeleteBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR
S3:GetBucketAcl	GetBucketAcl	
S3:GetBucketCompliance	OBTER conformidade com balde (obsoleto)	Sim
S3:GetBucketConsistência	OBTER consistência de balde	Sim
S3:GetBucketCORS	GetBucketCors	
S3:GetEncryptionConfiguration	GetBucketEncryption	
S3:GetBucketLastAccessTime	OBTER último tempo de acesso do Bucket	Sim
S3:GetBucketLocation	GetBucketlocalização	
S3:GetBucketMetadataNotification	OBTER configuração de notificação de metadados do bucket	Sim
S3:GetBucketNotification	GetBucketNotificationConfiguration	
S3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
S3:GetBucketPolicy	Política de GetBucketPolicy	
S3:GetBucketTagging	GetBucketTagging	
S3:GetBucketControle de versão	GetBucketControle de versão	
S3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3:GetReplicationConfiguration	GetBucketReplication	
S3:ListAllMyBuckets	• ListBuckets • OBTER uso de armazenamento	Sim, para OBTER uso de armazenamento. **Nota**: Use somente na política de grupo.

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3: ListBucket	• ListObjects • Balde para a cabeça • RestoreObject	
S3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
S3:ListBucketVersions	OBTER versões Bucket	
S3:PutBucketCompliance	COLOCAR conformidade com balde (obsoleto)	Sim
S3:PutBucketConsistência	COLOQUE a consistência do balde	Sim
S3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
S3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
S3:PutBucketLastAccessTime	COLOQUE o último tempo de acesso do balde	Sim
S3:PutBucketMetadataNotification	COLOQUE a configuração de notificação de metadados do bucket	Sim
S3:PutBucketNotification	PutBucketNotificationConfiguration	
S3:PutBucketObjectLockConfiguration	• CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de solicitação (também requer a permissão S3:CreateBucket) • PutObjectLockConfiguration	
S3:PutBucketPolicy	Política de PutBucketPolicy	
S3:PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
S3:PutBucketControle de versão	PutBucketControle de versão	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
S3:PutReplicationConfiguration	PutBucketReplication	Sim, permissões separadas para COLOCAR e EXCLUIR

Permissões que se aplicam a objetos

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
S3:BypassGovernanceretenção	• DeleteObject • DeleteObjects • Retenção PutObjectRetention	
S3:DeleteObject	• DeleteObject • DeleteObjects • RestoreObject	
S3:DeleteObjectTagging	DeleteObjectTagging	
S3:DeleteObjectVersionTagging	DeleteObjectTagging (uma versão específica do objeto)	
S3:DeleteObjectVersion	DeleteObject (uma versão específica do objeto)	
S3:GetObject	• GetObject • HeadObject • RestoreObject • Selecione ObjectContent	
S3:GetObjectAcl	GetObjectAcl	
S3:GetObjectLegalHod	GetObjectLegalHod	

Permissões	S3 OPERAÇÕES DE API REST	Personalizado para StorageGRID
S3:GetObjectRetention	GetObjectRetention	
S3:GetObjectTagging	GetObjectTagging	
S3:GetObjectVersionTagging	GetObjectTagging (uma versão específica do objeto)	
S3:GetObjectVersion	GetObject (uma versão específica do objeto)	
S3:ListMultipartUploadParts	ListParts, RestoreObject	
S3:PutObject	• PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
S3:PutObjectLegalHod	PutObjectLegalHod	
S3:retenção de objetos Put	Retenção PutObjectRetention	
S3:PutObjectTagging	Marcação de objetos	
S3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
S3:PutOverwriteObject	• PutObject • CopyObject • Marcação de objetos • DeleteObjectTagging • CompleteMultipartUpload	Sim
S3:RestoreObject	RestoreObject	

Use a permissão PutOverwriteObject

A permissão S3:PutOverwriteObject é uma permissão StorageGRID personalizada que se aplica a operações que criam ou atualizam objetos. A configuração dessa permissão determina se o cliente pode substituir os

dados de um objeto, metadados definidos pelo usuário ou marcação de objeto S3.

As configurações possíveis para essa permissão incluem:

- **Allow**: O cliente pode substituir um objeto. Esta é a configuração padrão.
- **Deny**: O cliente não pode sobrescrever um objeto. Quando definida como Negar, a permissão PutOverwriteObject funciona da seguinte forma:
  - Se um objeto existente for encontrado no mesmo caminho:
    - Os dados do objeto, metadados definidos pelo usuário ou marcação de objeto S3 não podem ser sobrescritos.
    - Todas as operações de ingestão em andamento são canceladas e um erro é retornado.
    - Se o controle de versão S3 estiver ativado, a configuração Negar impede que as operações PutObjectTagging ou DeleteObjectTagging modifiquem o TagSet para um objeto e suas versões não atuais.
  - Se um objeto existente não for encontrado, essa permissão não terá efeito.
- Quando esta permissão não está presente, o efeito é o mesmo que se permitir foi definido.

> Se a política S3 atual permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, metadados definidos pelo usuário ou marcação de objeto. Além disso, se a caixa de verificação **Prevent client modifition** estiver selecionada (**CONFIGURATION** > **Security settings** > **Network and Objects**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especifique condições em uma política

As condições definem quando uma política estará em vigor. As condições consistem em operadores e pares de valor-chave.

Condições Use pares chave-valor para avaliação. Um elemento de condição pode conter várias condições, e cada condição pode conter vários pares de chave-valor. O bloco de condição usa o seguinte formato:

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

No exemplo a seguir, a condição ipaddress usa a chave de condição SourceIp.

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

Operadores de condição suportados

Os operadores de condição são categorizados da seguinte forma:

- Cadeia de carateres
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas).
StringNotEquals	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas).
StringEquaisIgnoreCase	Compara uma chave com um valor de string baseado na correspondência exata (ignora caso).
StringNotEquaisIgnoreCase	Compara uma chave com um valor de string baseado em correspondência negada (ignora caso).
StringLike	Compara uma chave com um valor de string baseado na correspondência exata (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
StringNotLike	Compara uma chave com um valor de string baseado em correspondência negada (sensível a maiúsculas e minúsculas). Pode incluir * e ? carateres curinga.
NumericEquals	Compara uma chave com um valor numérico baseado na correspondência exata.
NumericNotEquals	Compara uma chave com um valor numérico baseado em correspondência negada.
NumericGreaterThan	Compara uma chave com um valor numérico baseado na correspondência "maior que".
NumericGreaterThanEquals	Compara uma chave com um valor numérico baseado na correspondência "maior que ou igual".
NumericLessThan	Compara uma chave com um valor numérico baseado na correspondência "inferior a".

Operadores de condição	Descrição
NumericLessThanEquals	Compara uma chave com um valor numérico baseado na correspondência "inferior ou igual".
Bool	Compara uma chave com um valor booleano baseado na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave com um endereço IP ou intervalo de endereços IP.
NotIpAddress	Compara uma chave com um endereço IP ou um intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Teclas de condição suportadas

Teclas de condição	Ações	Descrição
AWS:SourceIp	Operadores IP	Irá comparar com o endereço IP a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos. **Observação:** se a solicitação S3 tiver sido enviada pelo serviço Load Balancer nos nós Admin e Gateways, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Nota**: Se um balanceador de carga não transparente de terceiros for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` cabeçalho será ignorado porque sua validade não pode ser determinada.
aws:nome de usuário	Recurso/identidade	Irá comparar com o nome de usuário do remetente a partir do qual a solicitação foi enviada. Pode ser usado para operações de balde ou objetos.
s3:delimitador	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.

Teclas de condição	Ações	Descrição
S3: ExistingObjectTag/<tag-key>	S3:DeleteObjectTagging S3:DeleteObjectVersionTagging S3:GetObject S3:GetObjectAcl 3:GetObjectTagging S3:GetObjectVersion S3:GetObjectVersionAcl S3:GetObjectVersionTagging S3:PutObjectAcl S3:PutObjectTagging S3:PutObjectVersionAcl S3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor específicos da tag.
s3: teclas de max	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro Max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3: object-lock-resting-retension-days	S3:PutObject	Compara com a data de retenção até especificada no `x-amz-object-lock-retain-until-date` cabeçalho da solicitação ou calculada a partir do período de retenção padrão do intervalo para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • PutObject • CopyObject • CreateMultipartUpload
s3: object-lock-resting-retension-days	S3:retenção de objetos Put	Compara com a data de retenção até especificada na solicitação PutObjectRetention para garantir que ela esteja dentro do intervalo permitido.

Teclas de condição	Ações	Descrição
s3:prefixo	S3: ListBucket e. S3:ListBucketVersions Permissions	Irá comparar com o parâmetro prefix especificado em uma solicitação ListObjects ou ListObjectVersions.
S3:RequestObjectTag/<tag-key>	S3:PutObject S3:PutObjectTagging S3:PutObjectVersionTagging	Exigirá uma chave de tag específica e um valor quando a solicitação de objeto incluir marcação.

Especifique variáveis em uma política

Você pode usar variáveis em políticas para preencher informações de política quando elas estiverem disponíveis. Você pode usar variáveis de política no `Resource` elemento e em comparações de string no `Condition` elemento.

Neste exemplo, a variável `${aws:username}` faz parte do elemento recurso:

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

Neste exemplo, a variável `${aws:username}` faz parte do valor da condição no bloco condição:

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

Variável	Descrição
`${aws:SourceIp}`	Usa a chave SourceIp como a variável fornecida.
`${aws:username}`	Usa a chave de nome de usuário como a variável fornecida.
`${s3:prefix}`	Usa a chave de prefixo específica do serviço como a variável fornecida.
`${s3:max-keys}`	Usa a chave de teclas de Max específicas do serviço como a variável fornecida.
`${*}`	Caráter especial. Usa o caractere como um caractere * literal.

Variável	Descrição
`${?}`	Caráter especial. Usa o caractere como um caractere literal ?.
`${$}`	Caráter especial. Usa o caractere como um caractere literal.

Crie políticas que exijam tratamento especial

Às vezes, uma diretiva pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário raiz da conta. A implementação da API REST do StorageGRID S3 é menos restritiva durante a validação de políticas do que a Amazon, mas igualmente rigorosa durante a avaliação de políticas.

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
Negar a si mesmo quaisquer permissões para a conta raiz	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Negar auto quaisquer permissões ao usuário/grupo	Grupo	Válido e aplicado	O mesmo
Permita a um grupo de conta estrangeiro qualquer permissão	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política
Permitir uma conta estrangeira root ou usuário qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido quando permitido por uma política	O mesmo
Permitir permissões a todos para todas as ações	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro de método 405 não permitido para a raiz da conta estrangeira e usuários	O mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento de StorageGRID
Negar permissões a todos para todas as ações	Balde	Válida e aplicada, mas a conta de usuário root mantém permissão para todas as operações de política de bucket do S3	O mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
Recurso é um bucket S3 inexistente	Grupo	Válido	O mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta que não seja proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são propriedade da conta de criador e a política de bucket não se aplica. A conta de criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são propriedade da conta de proprietário do bucket. Aplica-se a política de bucket.

Proteção WORM (write-once-read-many)

Você pode criar buckets do WORM (write-once-read-many) para proteger dados, metadados de objetos definidos pelo usuário e marcação de objetos do S3. Você configura os buckets WORM para permitir a criação de novos objetos e impedir substituições ou exclusões de conteúdo existente. Use uma das abordagens descritas aqui.

Para garantir que as substituições sejam sempre negadas, você pode:

- No Gerenciador de Grade, vá para **CONFIGURATION** > **Security** > **Security settings** > **Network and Objects**, e marque a caixa de seleção **Prevent client modification**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject NEGAR à política S3.
  - Adicione uma operação DeleteObject NEGAR à política S3.
  - Adicione uma operação PutObject PERMITIR à política S3.

> ⓘ A configuração DeleteObject para NEGAR em uma diretiva S3 não impede que o ILM exclua objetos quando uma regra como "zero cópias após 30 dias" existir.

> ⓘ Mesmo quando todas essas regras e políticas são aplicadas, elas não se protegem contra gravações simultâneas (ver situação A). Eles protegem contra substituições concluídas sequenciais (ver situação B).

Situação A: Gravações simultâneas (não protegidas contra)

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

Situação B: Substituições sequenciais concluídas (protegidas contra)

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

Informações relacionadas

- "Como as regras do StorageGRID ILM gerenciam objetos"
- "Exemplo de políticas de bucket"
- "Exemplo de políticas de grupo"
- "Gerenciar objetos com ILM"
- "Use uma conta de locatário"

Exemplo de políticas de bucket

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para buckets.

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a diretiva está anexada. As políticas de bucket são configuradas usando a API S3 PutBucketPolicy. "Operações em baldes"Consulte .

Uma política de bucket pode ser configurada usando a AWS CLI de acordo com o seguinte comando:

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

Exemplo: Permita que todos acessem somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, podem listar objetos no bucket e executar operações GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que essa política pode não ser particularmente útil porque ninguém, exceto a raiz da conta, tem permissões para gravar no bucket.

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

Exemplo: Permita que todos em uma conta tenham acesso total, e todos em outra conta tenham acesso somente leitura a um intervalo

Neste exemplo, todos em uma conta especificada têm acesso total a um bucket, enquanto todos em outra conta especificada só podem listar o bucket e executar operações GetObject em objetos no bucket começando com o `shared/` prefixo da chave do objeto.

> No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta de proprietário do bucket. A política de bucket aplica-se a esses 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/*"
        }
      }
    }
  ]
}
```

Exemplo: Permita que todos acessem somente leitura a um bucket e o acesso total por grupo especificado

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar operações GetObject em todos os objetos no bucket, enquanto somente usuários pertencentes ao grupo `Marketing` na conta especificada têm acesso total permitido.

```
{
  "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/*"
      ]
    }
  ]
}
```

Exemplo: Permita que todos leiam e gravem o acesso a um bucket se o cliente estiver no intervalo IP

Neste exemplo, todos, incluindo anônimos, têm permissão para listar o bucket e executar quaisquer operações de Objeto em todos os objetos no bucket, desde que as solicitações venham de um intervalo IP especificado (54.240.143.0 a 54.240.143.255, exceto 54.240.143.188). Todas as outras operações serão negadas e todas as solicitações fora do intervalo de IP serão negadas.

```
{
  "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"}
      }
    }
  ]
}
```

Exemplo: Permitir acesso total a um bucket exclusivamente por um usuário federado especificado

Neste exemplo, o usuário federado Alex tem acesso total ao `examplebucket` bucket e seus objetos. Todos os outros usuários, incluindo "root", são explicitamente negados todas as operações. Note no entanto que "root" nunca é negada permissão para colocar/obter/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/*"
      ]
    }
  ]
}
```

Exemplo: Permissão PutOverwriteObject

Neste exemplo, o `Deny` efeito para PutOverwriteObject e DeleteObject garante que ninguém pode substituir ou excluir os dados do objeto, metadados definidos pelo usuário e marcação 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/*"
    }
  ]
}
```

Exemplo de políticas de grupo

Use os exemplos nesta seção para criar políticas de acesso ao StorageGRID para grupos.

As políticas de grupo especificam as permissões de acesso para o grupo ao qual a diretiva está anexada. Não `Principal` há nenhum elemento na política porque ela está implícita. As políticas de grupo são configuradas usando o Gerenciador de inquilinos ou a API.

Exemplo: Defina a política de grupo usando o Gerenciador do locatário

Quando você adiciona ou edita um grupo no Gerenciador do locatário, você pode selecionar uma política de grupo para determinar quais permissões de acesso do S3 os membros deste grupo terão. "Crie grupos para um locatário do S3"Consulte .

- **No S3 Access**: Opção padrão. Os usuários deste grupo não têm acesso a recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar essa opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: Os usuários deste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo somente leitura aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Acesso total**: Os usuários deste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona essa opção, a cadeia de carateres JSON para uma política de grupo de acesso total aparece na caixa de texto. Não é possível editar esta cadeia de carateres.
- **Mitigação de ransomware**: Esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários deste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que têm o controle de versão de objeto habilitado.

  Os usuários do Gerenciador de locatários que têm a permissão Gerenciar todos os buckets podem substituir essa política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação multifator (MFA), onde disponível.

- **Custom**: Os usuários do grupo recebem as permissões que você especificar na caixa de texto.

Exemplo: Permitir o acesso total do grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso total a todos os buckets pertencentes à conta de locatário, a menos que explicitamente negado pela política de bucket.

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

Exemplo: Permitir acesso somente leitura de grupo a todos os buckets

Neste exemplo, todos os membros do grupo têm acesso somente leitura a recursos do S3, a menos que explicitamente negado pela política de bucket. Por exemplo, os usuários desse grupo podem listar objetos e ler dados, metadados e tags de objetos.

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

Exemplo: Permita que os membros do grupo tenham acesso total apenas à sua "pasta" em um intervalo

Neste exemplo, os membros do grupo só podem listar e acessar sua pasta específica (prefixo de chave) no intervalo especificado. Observe que as permissões de acesso de outras políticas de grupo e a política de bucket devem ser consideradas ao determinar a privacidade dessas pastas.

```
{
  "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}/*"
    }
  ]
}
```

Informações sobre direitos autorais

Informações sobre marcas comerciais