Políticas de acesso a grupos e buckets

StorageGRID software

NetApp
December 03, 2025

Índice

Políticas de acesso a grupos e buckets

Use políticas de acesso a buckets e grupos

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 dentro desses buckets. O sistema StorageGRID implementa um subconjunto da linguagem de política da API REST do S3. As políticas de acesso para a API do S3 são escritas em JSON.

Visão geral da política de acesso

Há dois tipos de políticas de acesso suportadas pelo StorageGRID.

- **Políticas de bucket**, que são gerenciadas usando as operações da API S3 GetBucketPolicy, PutBucketPolicy e DeleteBucketPolicy ou a API Tenant Manager ou Tenant Management. As políticas de bucket são anexadas aos buckets, portanto, elas são configuradas para controlar o acesso de usuários na conta do proprietário do bucket ou de 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 Tenant Manager ou a Tenant Management API. As políticas de grupo são anexadas a um grupo na conta, portanto, elas 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 a vários buckets.

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

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

- ID da declaração (Sid) (opcional)
- Efeito
- Principal/Não Principal
- Recurso/NãoRecurso
- Ação/NãoAção
- Condição (opcional)

As declarações de política são criadas usando esta estrutura para especificar permissões: Conceder <Efeito> para permitir/negar que <Principal> execute <Ação> em <Recurso> quando <Condição> se aplicar.

Cada elemento de política é usado para uma função específica:

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

Elemento	Descrição
Efeito	Use o elemento Efeito para estabelecer se as operações especificadas são permitidas ou negadas. Você deve identificar as operações que permite (ou nega) em buckets ou objetos usando as palavras-chave do elemento Action suportadas.
Principal/Não Principal	Você pode permitir que usuários, grupos e contas acessem recursos específicos e executem ações específicas. Se nenhuma assinatura S3 for incluída na solicitação, o acesso anônimo será permitido especificando o caractere curinga (*) como principal. Por padrão, somente o root 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/NãoRecurso	O elemento Resource identifica buckets e objetos. Você pode permitir ou negar permissões para buckets e objetos usando o Amazon Resource Name (ARN) para identificar o recurso.
Ação/NãoAção	Os elementos Ação e Efeito são os dois componentes das permissões. Quando um grupo solicita um recurso, o acesso ao recurso é concedido ou negado. O acesso será negado, a menos que você atribua permissões especificamente, mas você pode usar a negação explícita para substituir uma permissão concedida por outra política.
Doença	O elemento Condition 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 caracteres curinga (*) e (?). Enquanto o asterisco (*) corresponde a 0 ou mais caracteres, o ponto de interrogação (?) corresponde a qualquer caractere único.

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

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

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

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

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

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, todas as atualizações feitas nas políticas de grupo serão consistentes. Quando uma política de grupo se torna consistente, as alterações podem levar mais 15 minutos para entrar em vigor, devido ao cache de políticas. Por padrão, todas as atualizações feitas nas políticas de bucket são fortemente 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 interrupção do site.

Neste caso, você pode definir o `Consistency-Control` cabeçalho na solicitação PutBucketPolicy ou você pode usar a solicitação de consistência PUT Bucket. Quando uma política de bucket se torna consistente, as alterações podem levar mais 8 segundos para entrar em vigor, devido ao 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 bucket de volta para seu valor original quando terminar. Caso contrário, todas as solicitações futuras de bucket usarão a configuração modificada.

Use ARN em declarações de política

Em declarações de política, o ARN é usado nos elementos Principal e Resource.

- Use esta sintaxe para especificar o ARN do recurso 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 caracteres dentro da chave do objeto.
- Caracteres internacionais, que podem ser especificados na chave do objeto, devem ser codificados usando JSON UTF-8 ou usando sequências de escape JSON \u. A codificação percentual não é suportada.

  "Sintaxe URN RFC 2141"

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

Especificar recursos em uma política

Em declarações de política, você pode usar o elemento Resource para especificar o bucket 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 recurso S3. Por exemplo:

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

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

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

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

Especificar os principais em uma política

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

- Cada declaração de política em uma política de bucket deve incluir um elemento Principal. 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 principais são indicados pelo elemento "Principal" ou, alternativamente, "NotPrincipal" para exclusão.
- Identidades baseadas em conta devem ser especificadas usando um ID ou um ARN:

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

- Este exemplo usa o ID da 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 UUID do usuário 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` é excluído. Se um novo Alex se juntar à organização e for designado para o mesmo `Alex` nome de usuário, o novo usuário pode herdar involuntariamente 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.

Especificar permissões em uma política

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

As tabelas listam 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, o que corresponde à especificação original do Amazon S3.

> Uma exclusão é realizada quando um put é usado para substituir um valor existente.

Permissões que se aplicam a buckets

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:CriarBucket	CriarBucket	Sim. **Observação**: Use somente em políticas de grupo.
s3:ExcluirBucket	ExcluirBucket	
s3:DeleteBucketMetadataNotification	EXCLUIR configuração de notificação de metadados do bucket	Sim
s3:DeleteBucketPolicy	Política de exclusão de balde	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ExcluirConfiguração de Replicação	DeleteBucketReplication	Sim, permissões separadas para PUT e DELETE
s3:ObterBucketAcl	ObterBucketAcl	
s3:ObterConformidade doBucket	Conformidade com o GET Bucket (obsoleto)	Sim
s3:ObterConsistência doBucket	Consistência do balde GET	Sim
s3:ObterBucketCORS	ObterBucketCors	
s3:ObterConfiguração de Criptografia	Obter criptografia do Bucket	
s3:GetBucketÚltimoAcessoHora	Último horário de acesso do Bucket GET	Sim
s3:ObterLocalização do Balde	ObterBucketLocation	
s3:GetBucketMetadataNotification	Configuração de notificação de metadados do GET Bucket	Sim
s3:GetBucketNotification	Obter configuração de notificação de bucket	
s3:GetBucketObjectLockConfiguration	ObterConfiguraçãoObjectLock	
s3:ObterPolítica deBucket	ObterBucketPolicy	
s3:Obter marcação de balde	Obter marcação de balde	
s3:GetBucketVersionamento	ObterVersionamento doBucket	
s3:ObterConfiguração do Ciclo de Vida	Obter configuração do ciclo de vida do Bucket	
s3:ObterConfiguração de Replicação	Obter replicação do Bucket	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ListarTodosOsMeusBuckets	• ListBuckets • Uso de armazenamento GET	Sim, para uso de armazenamento GET. **Observação**: Use somente em políticas de grupo.
s3:ListBucket	• Objetos de Lista • Balde de cabeça • RestaurarObjeto	
s3:ListBucketMultipartUploads	• ListarMultipartUploads • RestaurarObjeto	
s3:ListBucketVersões	Versões do GET Bucket	
s3:Conformidade com PutBucket	Conformidade com o PUT Bucket (obsoleto)	Sim
s3:ConsistênciaPutBucket	Consistência do balde PUT	Sim
s3:ColocarBucketCORS	• ExcluirBucketCors† • ColoqueBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:ColocarBucketÚltimoAcessoHora	Hora do último acesso ao bucket PUT	Sim
s3:PutBucketMetadataNotification	Configuração de notificação de metadados do PUT Bucket	Sim
s3:NotificaçãoPutBucket	Configuração de notificação PutBucket	
s3:PutBucketObjectLockConfiguração	• CreateBucket com o `x-amz-bucket-object-lock-enabled: true` cabeçalho de solicitação (também requer a permissão s3:CreateBucket) • PutObjectLockConfiguration	
s3:PolíticaPutBucket	PutBucketPolicy	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:PutBucketTagging	• ExcluirBucketTagging† • Colocar marcação de balde	
s3:PutBucketVersionamento	Versão PutBucket	
s3:PutLifecycleConfiguration	• Ciclo de vida do DeleteBucket† • Configuração do ciclo de vida do PutBucket	
s3:PutReplicationConfiguration	PutBucketReplicação	Sim, permissões separadas para PUT e DELETE

Permissões que se aplicam a objetos

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:AbortarUploadMultipart	• AbortarMultipartUpload • RestaurarObjeto	
s3:Ignorar Governança Retenção	• ExcluirObjeto • ExcluirObjetos • ColocarRetençãoDeObjeto	
s3:ExcluirObjeto	• ExcluirObjeto • ExcluirObjetos • RestaurarObjeto	
s3:ExcluirMarcaçãoDeObjeto	ExcluirMarcaçãoDeObjeto	
s3:ExcluirMarcaçãoDeVersãoDoObjeto	DeleteObjectTagging (uma versão específica do objeto)	
s3:ExcluirVersãoDoObjeto	DeleteObject (uma versão específica do objeto)	
s3:ObterObjeto	• ObterObjeto • CabeçaObjeto • RestaurarObjeto • SelecionarObjetoConteúdo	

Permissões	Operações da API REST do S3	Personalizado para StorageGRID
s3:ObterAclDeObjeto	ObterAclObjeto	
s3:ObterObjetoLegalHold	ObterObjetoLegalHold	
s3:ObterRetençãoDeObjeto	ObterRetençãoDeObjeto	
s3:ObterMarcaçãoDeObjeto	Obter marcação de objeto	
s3:ObterTag deVersão do Objeto	GetObjectTagging (uma versão específica do objeto)	
s3:ObterVersãoDoObjeto	GetObject (uma versão específica do objeto)	
s3:ListMultipartUploadParts	ListParts, RestaurarObjeto	
s3:ColocarObjeto	• ColocarObjeto • CopiarObjeto • RestaurarObjeto • CriarMultipartUpload • Upload completo de várias partes • UploadPart • UploadPartCopy	
s3:ColocarObjetoLegalHold	ColocarObjetoLegalHold	
s3:PutObjectRetention	ColocarRetençãoDeObjeto	
s3:PutObjectTagging	Colocar marcação de objeto	
s3:PutObjectVersionTagging	PutObjectTagging (uma versão específica do objeto)	
s3:ColocarObjetoSobrescrito	• ColocarObjeto • CopiarObjeto • Colocar marcação de objeto • ExcluirMarcaçãoDeObjeto • Upload completo de várias partes	Sim
s3:RestaurarObjeto	RestaurarObjeto	

Usar permissão PutOverwriteObject

A permissão s3:PutOverwriteObject é uma permissão personalizada do StorageGRID 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 objetos do S3.

As configurações possíveis para essa permissão incluem:

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

> ⓘ Se a política atual do S3 permitir a substituição e a permissão PutOverwriteObject estiver definida como Negar, o cliente não poderá substituir os dados de um objeto, os metadados definidos pelo usuário ou a marcação de objetos. Além disso, se a caixa de seleção **Impedir modificação do cliente** estiver marcada (**CONFIGURAÇÃO** > **Configurações de segurança** > **Rede e objetos**), essa configuração substituirá a configuração da permissão PutOverwriteObject.

Especificar condições em uma política

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

As condições usam pares chave-valor para avaliação. Um elemento Condition pode conter várias condições, e cada condição pode conter vários pares 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:

- Corda
- Numérico
- Booleano
- Endereço IP
- Verificação nula

Operadores de condição	Descrição
StringEquals	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas).
StringNotEquals	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas).
StringEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência exata (ignora maiúsculas e minúsculas).
StringNotEqualsIgnoreCase	Compara uma chave a um valor de string com base na correspondência negada (ignora maiúsculas e minúsculas).
StringLike	Compara uma chave a um valor de string com base na correspondência exata (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
StringNotLike	Compara uma chave a um valor de string com base na correspondência negada (diferencia maiúsculas de minúsculas). Pode incluir caracteres curinga * e ?.
NumericEquals	Compara uma chave a um valor numérico com base na correspondência exata.
NuméricoNãoIgual	Compara uma chave a um valor numérico com base na correspondência negada.

Operadores de condição	Descrição
NuméricoMaiorQue	Compara uma chave a um valor numérico com base na correspondência "maior que".
NuméricoMaiorQueIgual	Compara uma chave a um valor numérico com base na correspondência "maior ou igual a".
NuméricoMenorQue	Compara uma chave a um valor numérico com base na correspondência "menor que".
NuméricoMenorQueIgual	Compara uma chave a um valor numérico com base na correspondência "menor ou igual a".
Bool	Compara uma chave a um valor booleano com base na correspondência "verdadeiro ou falso".
Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP.
Não Endereço IP	Compara uma chave a um endereço IP ou intervalo de endereços IP com base na correspondência negada.
Nulo	Verifica se uma chave de condição está presente no contexto de solicitação atual.

Chaves de condição suportadas

Chaves de condição	Ações	Descrição
aws:SourceIp	Operadores de IP	Será comparado ao endereço IP de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto. **Observação:** Se a solicitação S3 foi enviada por meio do serviço Load Balancer nos nós de administração e nos nós de gateway, isso será comparado ao endereço IP upstream do serviço Load Balancer. **Observação**: se um balanceador de carga de terceiros não transparente for usado, isso será comparado ao endereço IP desse balanceador de carga. Qualquer `X-Forwarded-For` O cabeçalho será ignorado porque sua validade não pode ser verificada.
aws:nome de usuário	Recurso/Identidade	Será comparado ao nome de usuário do remetente de onde a solicitação foi enviada. Pode ser usado para operações de bucket ou objeto.

Chaves de condição	Ações	Descrição
s3:delimitador	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro delimitador especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<chave-tag>	s3:ExcluirMarcaçãoDeObjeto s3:ExcluirMarcaçãoDeVersãoDoObjeto s3:ObterObjeto s3:ObterAclDeObjeto 3: Obter marcação de objeto s3:ObterVersãoDoObjeto s3:ObterVersãoDoObjetoAcl s3:ObterTag deVersão do Objeto s3:ColocarObjetoAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exigirá que o objeto existente tenha a chave e o valor de tag específicos.
s3:max-chaves	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro max-keys especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:object-lock-remaining-retention-days	s3:ColocarObjeto	Compara com a data de retenção especificada no `x-amz-object-lock-retain-until-date` cabeçalho de solicitação ou calculado a partir do período de retenção padrão do bucket para garantir que esses valores estejam dentro do intervalo permitido para as seguintes solicitações: • ColocarObjeto • CopiarObjeto • CriarMultipartUpload

Chaves de condição	Ações	Descrição
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Compara com a data de retenção especificada na solicitação PutObjectRetention para garantir que esteja dentro do intervalo permitido.
s3:prefix	s3:ListBucket e Permissões s3:ListBucketVersions	Será comparado ao parâmetro de prefixo especificado em uma solicitação ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<chave-tag>	s3:ColocarObjeto s3:PutObjectTagging s3:PutObjectVersionTagging	Exigirá uma chave de tag e um valor específicos quando a solicitação de objeto incluir marcação.

Especificar variáveis em uma política

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

Variável	Descrição
`${s3:max-keys}`	Usa a chave max-keys específica do serviço como a variável fornecida.
`${*}`	Caractere especial. Usa o caractere como um caractere * literal.
`${?}`	Caractere especial. Usa o caractere como um caractere literal ?.
`${$}`	Caractere especial. Usa o caractere como um caractere $ literal.

Crie políticas que exijam tratamento especial

Às vezes, uma política pode conceder permissões que são perigosas para a segurança ou perigosas para operações contínuas, como bloquear o usuário root 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 do StorageGRID
Negar a si mesmo quaisquer permissões para a conta root	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Negar a si mesmo quaisquer permissões para usuário/grupo	Grupo	Válido e aplicado	Mesmo
Permitir qualquer permissão a um grupo de contas estrangeiras	Balde	Principal inválido	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política
Permitir que uma conta estrangeira root ou usuário tenha qualquer permissão	Balde	Válido, mas as permissões para todas as operações de política de bucket do S3 retornam um erro 405 Método Não Permitido quando permitidas por uma política	Mesmo

Descrição da política	Tipo de política	Comportamento da Amazon	Comportamento do StorageGRID
Permitir que todos tenham permissão para todas as ações	Balde	Válido, mas as permissões para todas as operações de política do bucket S3 retornam um erro 405 Método Não Permitido para a raiz da conta estrangeira e usuários	Mesmo
Negar a todos permissões para todas as ações	Balde	Válido e aplicado, mas a conta do usuário root mantém a permissão para todas as operações de política do bucket S3	Mesmo
Principal é um usuário ou grupo inexistente	Balde	Principal inválido	Válido
O recurso é um bucket S3 inexistente	Grupo	Válido	Mesmo
Principal é um grupo local	Balde	Principal inválido	Válido
A política concede a uma conta não proprietária (incluindo contas anônimas) permissões para colocar objetos.	Balde	Válido. Os objetos são de propriedade da conta do criador e a política de bucket não se aplica. A conta do criador deve conceder permissões de acesso ao objeto usando ACLs de objeto.	Válido. Os objetos são de propriedade da conta do proprietário do bucket. Aplica-se a política de balde.

Proteção WORM (gravação única e leitura múltipla)

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

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

- No Grid Manager, vá para **CONFIGURAÇÃO** > **Segurança** > **Configurações de segurança** > **Rede e objetos** e marque a caixa de seleção **Impedir modificação do cliente**.
- Aplique as seguintes regras e políticas do S3:
  - Adicione uma operação PutOverwriteObject DENY à política S3.
  - Adicione uma operação DeleteObject DENY à política S3.
  - Adicione uma operação PutObject ALLOW à política S3.

Definir DeleteObject como DENY em uma política do S3 não impede que o ILM exclua objetos quando existe uma regra como "zero cópias após 30 dias".

Mesmo quando todas essas regras e políticas são aplicadas, elas não protegem contra gravações simultâneas (veja Situação A). Eles protegem contra sobrescritas sequenciais concluídas (veja Situação B).

Situação A: Gravações simultâneas (não protegidas)

```
/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"
- "Exemplos de políticas de bucket"
- "Exemplo de políticas de grupo"
- "Gerenciar objetos com ILM"
- "Use uma conta de inquilino"

Exemplos de políticas de bucket

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

As políticas de bucket especificam as permissões de acesso para o bucket ao qual a política está anexada. Você configura uma política de bucket usando a API PutBucketPolicy do S3 por meio de uma destas ferramentas:

- "Gerente de inquilinos" .
- AWS CLI usando este comando (consulte"Operações em baldes"):

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

Exemplo: permitir que todos tenham acesso somente leitura a um bucket

Neste exemplo, todos, incluindo anônimos, têm permissão para listar objetos no bucket e executar operações

GetObject em todos os objetos no bucket. Todas as outras operações serão negadas. Observe que esta política pode não ser particularmente útil porque ninguém, exceto o root da conta, tem permissão 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: permitir que todos em uma conta tenham acesso total e todos em outra conta tenham acesso somente leitura a um bucket

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

> No StorageGRID, os objetos criados por uma conta não proprietária (incluindo contas anônimas) são de propriedade da conta do proprietário do bucket. A política de bucket se aplica 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: permitir que todos tenham acesso somente leitura a um bucket e acesso total ao grupo especificado

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

```
{
  "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: permitir que todos tenham acesso de leitura e gravação a um bucket se o cliente estiver no intervalo de 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 de 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` balde e seus objetos. Todos os outros usuários, incluindo `root', têm todas as operações explicitamente negadas. Observe, no entanto, que` root' nunca tem permissões negadas 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/*"
      ]
    }
  ]
}
```

Exemplo: permissão PutOverwriteObject

Neste exemplo, o `Deny` O efeito para PutOverwriteObject e DeleteObject garante que ninguém possa substituir ou excluir os dados do objeto, os metadados definidos pelo usuário e a marcação de objetos do 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 do StorageGRID para grupos.

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

Exemplo: definir política de grupo usando o Gerenciador de Tenants

Ao adicionar ou editar um grupo no Gerenciador de Tenants, você pode selecionar uma política de grupo para determinar quais permissões de acesso ao S3 os membros desse grupo terão. Ver "Criar grupos para um locatário S3" .

- **Sem acesso S3**: opção padrão. Os usuários neste grupo não têm acesso aos recursos do S3, a menos que o acesso seja concedido com uma política de bucket. Se você selecionar esta opção, somente o usuário root terá acesso aos recursos do S3 por padrão.
- **Acesso somente leitura**: os usuários neste grupo têm acesso somente leitura aos recursos do S3. Por exemplo, os usuários neste grupo podem listar objetos e ler dados de objetos, metadados e tags. Quando você seleciona esta opção, a string JSON para uma política de grupo somente leitura aparece na caixa de texto. Você não pode editar esta sequência.
- **Acesso total**: os usuários neste grupo têm acesso total aos recursos do S3, incluindo buckets. Quando você seleciona esta opção, a string JSON para uma política de grupo de acesso total aparece na caixa de texto. Você não pode editar esta sequência.
- **Mitigação de ransomware**: esta política de exemplo se aplica a todos os buckets deste locatário. Os usuários neste grupo podem executar ações comuns, mas não podem excluir permanentemente objetos de buckets que tenham o controle de versão de objetos habilitado.

  Usuários do Tenant Manager que têm a permissão Gerenciar todos os buckets podem substituir esta política de grupo. Limite a permissão Gerenciar todos os buckets a usuários confiáveis e use a Autenticação Multifator (MFA) quando disponível.

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

Exemplo: permitir acesso total do grupo a todos os buckets

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

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

Exemplo: permitir acesso somente leitura do grupo a todos os buckets

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

```
{
  "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: permitir que os membros do grupo tenham acesso total apenas à sua "pasta" em um bucket

Neste exemplo, os membros do grupo só têm permissão para listar e acessar sua pasta específica (prefixo de chave) no bucket especificado. Observe que as permissões de acesso de outras políticas de grupo e da 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