管理访问策略

StorageGRID software

NetApp
July 23, 2026

目录

管理访问策略

StorageGRID 如何使用 AWS 策略来控制对 S3 存储桶和对象的访问

StorageGRID 使用 Amazon Web Services (AWS) 策略语言，允许 S3 租户控制对这些存储桶中的存储桶和对象的访问。StorageGRID 系统实现了 S3 REST API 策略语言的子集。S3 API 的访问策略以 JSON 编写。

访问策略概述

StorageGRID 支持三种访问策略：

- 存储桶策略，使用 GetBucketPolicy、PutBucketPolicy 和 DeleteBucketPolicy S3 API 操作或租户管理器或租户管理 API 进行管理。存储桶策略附加到存储桶，因此它们被配置为控制存储桶所有者帐户或其他帐户中的用户对存储桶及其中对象的访问。存储桶策略仅适用于一个存储桶，也可能适用于多个组。
- 组策略，使用租户管理器或租户管理 API 配置。组策略附加到帐户中的组，因此它们被配置为允许该组访问该帐户拥有的特定资源。组策略仅适用于一个组，也可能适用于多个存储桶。
- 会话策略，作为发出 AssumeRole 请求的一部分。会话策略仅适用于给定的会话，在组策略和存储桶策略所授予权限的基础上，进一步定义用户所拥有的权限。

> 组、存储桶和会话策略之间的优先级没有差异。

StorageGRID 存储桶和组策略遵循 Amazon 定义的特定语法。每个策略中都包含一系列策略语句，每个语句都包含以下元素：

- 语句 ID (Sid)（可选）
- 影响
- 委托人/NotPrincipal
- Resource/NotResource
- 操作/NotAction
- 条件（可选）

策略声明使用以下结构构建以指定权限：授予 <Effect> 以允许/拒绝 <Principal> 在 <Condition> 适用时对 <Resource> 执行 <Action>。

每个策略元素都用于特定的功能：

Element	问题描述
Sid	Sid 元素是可选的。Sid 仅用作对用户的描述。它由 StorageGRID 系统存储，但不作解释。

Element	问题描述
影响	使用 Effect 元素确定是否允许或拒绝指定的操作。必须使用支持的 Action 元素关键字标识您允许（或拒绝）存储桶或对象上的操作。
委托人/NotPrincipal	您可以允许用户、组和帐户访问特定资源并执行特定操作。如果请求中不包含 S3 签名，则通过指定通配符（ * ）作为主体来允许匿名访问。默认情况下，只有帐户根才能访问该帐户拥有的资源。 您只需要在存储桶策略中指定 Principal 元素。对于组策略，策略附加到的组是隐式 Principal 元素。
Resource/NotResource	Resource 元素标识存储桶和对象。您可以使用 Amazon 资源名称 (ARN) 来标识资源，以允许或拒绝对存储桶和对象的权限。
操作/NotAction	Action 和 Effect 元素是权限的两个组成部分。当组请求资源时，会被授予或拒绝对该资源的访问权限。除非您专门分配权限，否则访问将被拒绝，但您可以使用显式拒绝来覆盖其他策略授予的权限。
条件	Condition 元素是可选的。条件允许您构建表达式以确定何时应用策略。

在 Action 元素中，您可以使用通配符 (*) 指定所有操作或操作的子集。例如，此 Action 与 s3:GetObject 、s3:PutObject 和 s3:DeleteObject 等权限匹配。

```
s3:*Object
```

在资源元素中，您可以使用通配符（*）和（?）。星号（*）匹配 0 个或更多字符，问号（?）匹配任意单个字符。

在 Principal 元素中，除了设置匿名访问外，不支持通配符，匿名访问授予每个人访问权限。例如，将通配符（ * ）设置为 Principal 值。

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

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

在以下示例中，该语句使用的是 Effect、Principal、Action 和 Resource 元素。此示例显示了一个完整的存储桶策略语句，该语句使用 Effect "Allow" 授予 Principal（即 admin 组 `federated-group/admin` 和 finance 组 `federated-group/finance`）对名为 `mybucket` 的存储桶执行 Action `s3:ListBucket` 的权限，以及对该存储桶内的所有对象执行 Action `s3:GetObject` 的权限。

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

存储区策略的大小限制为 20,480 字节，组策略的大小限制为 5,120 字节。

策略的一致性

默认情况下，您对组策略所做的任何更新最终都是一致的。当组策略变得一致时，由于策略缓存，更改可能需要额外 15 分钟才能生效。默认情况下，您对存储区策略所做的任何更新都是高度一致的。

根据需要，您可以更改存储桶策略更新的一致性保证。例如，您可能希望在站点中断期间可以对存储桶策略进行更改。

在这种情况下，您可以在 PutBucketPolicy 请求中设置 `Consistency-Control`标头，也可以使用 PUT Bucket 一致性请求。当存储桶策略变得一致时，由于策略缓存，更改可能需要额外 8 秒才能生效。

> 如果将一致性设置为不同的值以解决临时情况，请务必在完成后将存储桶级别设置恢复为其原始值。否则，将来所有存储桶请求都将使用修改后的设置。

什么是会话策略?

会话策略是一种访问策略，它暂时限制特定会话期间可用的权限，例如当用户承担某个组时。会话策略只能允许权限的子集，并且无法授予其他权限。组本身可能具有更广泛的权限。

在策略语句中使用 **ARN**

在策略声明中，ARN 用于 Principal 和 Resource 元素。

- 使用此语法指定 S3 资源 ARN：

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

- 使用此语法指定标识资源 ARN（用户和组）：

```
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
```

其他注意事项：

- 您可以使用星号(*)作为通配符来匹配对象键内的零个或多个字符。
- 可以在对象键中指定的国际字符应使用 JSON UTF-8 或使用 JSON \u 转义序列进行编码。不支持百分比编码。

  "RFC 2141 URN 语法"

  PutBucketPolicy 操作的 HTTP 请求正文必须使用 charset=UTF-8 编码。

在策略中指定资源

在策略语句中，您可以使用 Resource 元素指定允许或拒绝其权限的存储桶或对象。

- 每个策略语句都需要一个 Resource 元素。在策略中，资源由元素 `Resource`表示，或者使用 `NotResource`进行排除。
- 使用 S3 资源 ARN 指定资源。例如：

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

- 您还可以在对象键内使用策略变量。例如：

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

- 资源值可以指定在创建组策略时尚不存在的存储桶。

在策略中指定主体

使用 Principal 元素标识策略语句允许/拒绝访问资源的用户、组或租户帐户。

- 存储桶策略中的每个策略语句必须包含 Principal 元素。组策略中的策略语句不需要 Principal 元素，因为组被理解为主体。
- 在策略中，主体由元素"Principal"表示，或者用"NotPrincipal"表示排除。
- 必须使用 ID 或 ARN 指定基于帐户的身份：

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

- 此示例使用租户帐户 ID 27233906934684427525，其中包括帐户根目录和帐户中的所有用户：

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

- 您可以仅指定帐户根目录：

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

- 您可以指定特定的联合用户（"Alex"）：

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

- 您可以指定特定的联合组（"Managers"）：

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

- 您可以指定匿名主体：

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

- 为避免模糊不清，您可以使用用户 UUID 而不是用户名：

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

  例如，假设 Alex 离开组织，用户名 `Alex`被删除。如果新的 Alex 加入组织并被分配了相同 `Alex`的用户名，新用户可能会无意中继承授予原始用户的权限。

- 主体值可以指定在创建存储桶策略时尚不存在的组/用户名。

在策略中指定权限

在策略中，Action 元素用于允许/拒绝对资源的权限。您可以在策略中指定一组权限，这些权限由元素"Action"或"NotAction"（用于排除）表示。这些元素中的每一个都映射到特定的 S3 REST API 操作。

这些表格列出了应用于存储区的权限以及应用于对象的权限。

Amazon S3 现在对 PutBucketReplication 和 DeleteBucketReplication 操作均使用 s3:PutReplicationConfiguration 权限。StorageGRID 对每个操作使用独立的权限，这与原始 Amazon S3 规范相符。

当使用 PUT 覆盖现有值时，将执行删除。

适用于存储桶的权限

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3：CreateBucket	CreateBucket	是 注意：仅在组策略中使用。
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadataNotification	删除存储桶元数据通知配置	是
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	是，PUT 和 DELETE 的单独权限
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket compliance（已弃用）	是
s3:GetBucketConsistency	获取 Bucket 一致性	是
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	获取 Bucket 上次访问时间	是
s3:GetBucketLocation	GetBucketLocation	

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3:GetBucketMetadataNotification	获取 Bucket 元数据通知配置	是
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	• ListBuckets • 获取存储使用情况	是，用于 GET Storage Usage。 注意：仅在组策略中使用。
s3:ListBucket	• ListObjects • HeadBucket • RestoreObject	
s3:ListBucketMultipartUploads	• ListMultipartUploads • RestoreObject	
s3:ListBucketVersions	GET 存储桶版本	
s3:PutBucketCompliance	PUT Bucket compliance（已弃用）	是
s3:PutBucketConsistency	PUT Bucket 一致性	是
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBucketEncryption • PutBucketEncryption	

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3:PutBucketLastAccessTime	PUT Bucket 上次访问时间	是
s3:PutBucketMetadataNotification	PUT Bucket 元数据通知配置	是
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket 带有 `x-amz-bucket-object-lock-enabled: true`请求标头（也需要 s3:CreateBucket 权限） • PutObjectLockConfiguration	
s3：PutBucketPolicy	PutBucketPolicy	
s3：PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	是，PUT 和 DELETE 的单独权限

适用于对象的权限

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3:AbortMultipartUpload	• AbortMultipartUpload • RestoreObject	
s3:BypassGovernanceRetention	• 删除对象 • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• 删除对象 • DeleteObjects • RestoreObject	

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging（对象的特定版本）	
s3:DeleteObjectVersion	DeleteObject （对象的特定版本）	
s3:GetObject	• 获取对象 • HeadObject • RestoreObject • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging（对象的特定版本）	
s3:GetObjectVersion	GetObject （对象的特定版本）	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• 放置对象 • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	

权限	**S3 REST API** 操作	自定义 **StorageGRID**
s3:PutObjectVersionTagging	PutObjectTagging（对象的特定版本）	
s3:PutOverwriteObject	• 放置对象 • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	是
s3:RestoreObject	RestoreObject	

使用 **PutOverwriteObject** 权限

s3:PutOverwriteObject 权限是应用于创建或更新对象的操作的自定义 StorageGRID 权限。此权限的设置确定客户端是否可以覆盖对象的数据、用户定义的元数据或 S3 对象标记。

此权限的可能设置包括：

- **Allow**：客户端可以覆盖对象。这是默认设置。
- 拒绝：客户端无法覆盖对象。设置为"拒绝"时，PutOverwriteObject 权限的工作原理如下：
  - 如果在同一路径中找到现有对象：
    - 无法覆盖对象的数据、用户定义的元数据或 S3 对象标记。
    - 正在进行的任何导入操作都将被取消，并返回错误。
    - 如果启用了 S3 版本控制，则拒绝设置可防止 PutObjectTagging 或 DeleteObjectTagging 操作修改对象及其非当前版本的 TagSet。
  - 如果找不到现有对象，此权限无效。
- 当此权限不存在时，效果与"允许"设置的效果相同。

> 如果当前 S3 策略允许覆盖，并且 PutOverwriteObject 权限设置为拒绝，则客户端无法覆盖对象的数据、用户定义的元数据或对象标记。此外，如果选中*防止客户端修改*复选框（配置 > 安全设置 > 网络和对象），则该设置将覆盖 PutOverwriteObject 权限的设置。

在策略中指定条件

条件定义了策略何时生效。条件由运算符和键值对组成。

条件使用键值对进行评估。Condition 元素可以包含多个条件，每个条件可以包含多个键值对。条件块使用以下格式：

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

在以下示例中，IpAddress 条件使用 SourceIp 条件键。

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

支持的条件运算符

条件运算符的分类如下：

- 字符串
- 数字
- 布尔型
- IP 地址
- 空值检查

条件运算符	问题描述
StringEquals	根据精确匹配（区分大小写）将键与字符串值进行比较。
StringNotEquals	将键与基于否定匹配的字符串值进行比较（区分大小写）。
StringEqualsIgnoreCase	根据精确匹配将键与字符串值进行比较（忽略大小写）。
StringNotEqualsIgnoreCase	根据否定匹配将键与字符串值进行比较（忽略大小写）。
StringLike	根据精确匹配（区分大小写）将键与字符串值进行比较。可以包含 * 和 ？通配符。
StringNotLike	根据否定匹配（区分大小写）将键与字符串值进行比较。可以包含 * 和 ？通配符。
NumericEquals	根据精确匹配将键与数值进行比较。
NumericNotEquals	将键与基于否定匹配的数值进行比较。

条件运算符	问题描述
NumericGreaterThan	将键与基于"大于"匹配的数值进行比较。
NumericGreaterThanEquals	将键与基于"大于或等于"匹配的数值进行比较。
NumericLessThan	将键与基于"小于"匹配的数值进行比较。
NumericLessThanEquals	将键与基于"小于或等于"匹配的数值进行比较。
Bool	将键与基于"true或false"匹配的布尔值进行比较。
IpAddress	将密钥与 IP 地址或 IP 地址范围进行比较。
NotIpAddress	根据否定匹配将密钥与 IP 地址或 IP 地址范围进行比较。
空	检查当前请求上下文中是否存在条件键。
IfExists	附加到任何条件运算符（Null 条件除外），以检查该条件键是否不存在。如果条件键不存在，则返回 TRUE。

支持的条件键

条件键	操作	问题描述
aws:SourceIp	IP 运算符	将与发送请求的 IP 地址进行比较。可用于存储桶或对象操作。 注意： 如果 S3 请求是通过管理节点和网关节点上的负载均衡器服务发送的，这将与负载均衡器服务上游的 IP 地址进行比较。 **Note**：如果使用第三方非透明负载均衡器，这将与该负载均衡器的 IP 地址进行比较。任何 `X-Forwarded-For`标头都将被忽略，因为其有效性无法确定。
aws:username	资源/身份	将与发送请求的发件人的用户名进行比较。可用于存储桶或对象操作。
s3:delimiter	s3:ListBucket 以及 s3:ListBucketVersions 权限	将与ListObjects或ListObjectVersions请求中指定的分隔符参数进行比较。

条件键	操作	问题描述
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	将要求现有对象具有特定的标记键和值。
s3:max-keys	s3:ListBucket 以及 s3:ListBucketVersions 权限	将与 ListObjects 或 ListObjectVersions 请求中指定的 max-keys 参数进行比较。
s3:object-lock-mode	s3:PutObject	与从 PutObject、CopyObject 和 CreateMultipartUpload 请求中的请求头展开的 `object-lock-mode` 进行比较。
s3:object-lock-mode	s3:PutObjectRetention	与 PutObjectRetention 请求中从 XML 正文展开的 `object-lock-mode`进行比较。
s3:object-lock-remaining-retention-days	s3:PutObject	与 `x-amz-object-lock-retain-until-date`请求标头中指定的或从存储桶默认保留期计算的 retain-until-date 进行比较，以确保这些值位于以下请求的允许范围内： • 放置对象 • CopyObject • CreateMultipartUpload
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	与 PutObjectRetention 请求中指定的保留截止日期进行比较，以确保其处于允许范围内。

条件键	操作	问题描述
s3:prefix	s3:ListBucket 以及 s3:ListBucketVersions 权限	将与ListObjects或ListObjectVersions请求中指定的前缀参数进行比较。
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	当对象请求包括标记时，将需要特定的标记键和值。
s3:x-amz-server-side-encryption-customer-algorithm	s3:PutObject	与 PutObject、CopyObject、CreateMultipartUpload、UploadPart、UploadPartCopy 和 CompleteMultipartUpload 请求中从请求标头展开的 `sse-customer-algorithm`或 `copy-source-sse-customer-algorithm`进行比较。

在策略中指定变量

您可以使用策略中的变量来填充可用的策略信息。您可以在 `Resource`元素中使用策略变量，也可以在 `Condition`元素中的字符串比较中使用策略变量。

在此示例中，变量 `${aws:username}`是 Resource 元素的一部分：

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

在此示例中，变量 `${aws:username}`是条件块中条件值的一部分：

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

变量	问题描述
`${aws:SourceIp}`	使用 SourceIp 键作为提供的变量。
`${aws:username}`	使用用户名密钥作为提供的变量。
`${s3:prefix}`	使用特定于服务的前缀键作为提供的变量。

变量	问题描述
`${s3:max-keys}`	使用特定于服务的 max-keys 键作为提供的变量。
`${*}`	特殊字符。使用字符作为字面 * 字符。
`${?}`	特殊字符。使用字符作为字面？字符。
`${$}`	特殊字符。将字符用作字面上的 $ 字符。

制定需要特殊处理的策略

有时，策略可以授予对安全性有危险或对持续操作有危险的权限，例如锁定帐户的 root 用户。StorageGRID S3 REST API 实现在策略验证期间的限制性低于 Amazon，但在策略评估期间同样严格。

策略说明	策略类型	**Amazon** 行为	**StorageGRID** 行为
拒绝自己对 root 账户的任何权限	存储桶	有效并强制执行，但 root 用户帐户保留所有 S3 存储桶策略操作的权限	相同
拒绝自己对用户/组的任何权限	组	有效且强制执行	相同
允许外部账户组具有任何权限	存储桶	无效的主体	有效，但所有 S3 存储桶策略操作的权限在策略允许时返回 405 Method Not Allowed 错误
允许外部账户 root 或用户拥有任何权限	存储桶	有效，但所有 S3 存储桶策略操作的权限在策略允许时返回 405 Method Not Allowed 错误	相同
允许所有人执行所有操作	存储桶	有效，但所有 S3 存储桶策略操作的权限对外部帐户 root 用户和普通用户返回 405 Method Not Allowed 错误	相同
拒绝所有人对所有操作的权限	存储桶	有效并强制执行，但 root 用户帐户保留所有 S3 存储桶策略操作的权限	相同
主体是不存在的用户或组	存储桶	无效的主体	有效
资源是不存在的 S3 存储桶	组	有效	相同
主体是本地组	存储桶	无效的主体	有效

策略说明	策略类型	**Amazon** 行为	**StorageGRID** 行为
策略授予非所有者帐户（包括匿名帐户）放置对象的权限。	存储桶	有效。对象归创建者账户所有，不适用存储桶策略。创建者账户必须使用对象 ACL 授予对象的访问权限。	有效。对象由存储桶所有者帐户拥有。存储桶策略适用。

一次写入多次读取（**WORM**）保护

您可以创建一次写入多次读取 (WORM) 存储桶以保护数据、用户定义的对象元数据和 S3 对象标记。您可以配置 WORM 存储桶以允许创建新对象并防止覆盖或删除现有内容。使用此处描述的方法之一。

要确保覆盖始终被拒绝，您可以：

- 从 Grid Manager 中，转到*配置* > 安全 > 安全设置 > 网络和对象，然后选中*防止客户端修改*复选框。
- 应用以下规则和 S3 策略：
  - 向 S3 策略添加 PutOverwriteObject DENY 操作。
  - 向 S3 策略添加 DeleteObject DENY 操作。
  - 向 S3 策略中添加 PutObject ALLOW 操作。

> 在 S3 策略中将 DeleteObject 设置为 DENY 不会阻止 ILM 在存在"30 天后零副本"等规则时删除对象。

> 即使应用了所有这些规则和策略，它们也不能防止并发写入（请参阅情况 A）。它们确实可以防止顺序完成的覆盖（请参阅情况 B）。

情况 **A**：并发写入（未防范）

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

情况 **B**：顺序完成覆盖（防止）

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

相关信息

- "StorageGRID ILM 规则如何管理对象"
- "存储桶策略示例"
- "组策略示例"
- "示例会话策略"

- "使用 ILM 管理对象"
- "使用租户帐户"

StorageGRID S3 REST API 会话策略示例

使用以下示例构建 StorageGRID 会话策略。

示例：设置允许对象检索的会话策略

在此示例中，会话的主体仅允许从 bucket1 检索对象。所有其他操作都会被隐式拒绝，除了特定于 StorageGRID 的操作（例如使用 "s3:PutOverwriteObject" 权限）。调用 AssumeRole API 时，可以以 JSON 文件的形式提供会话策略。

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

StorageGRID S3 REST API 存储桶策略示例

使用本节中的示例为存储桶构建 StorageGRID 访问策略。

存储区策略指定策略附加到的存储区的访问权限。您可以通过以下工具之一使用 S3 PutBucketPolicy API 配置存储区策略：

- "租户管理器"。
- 使用此命令的 AWS CLI（请参阅"${post_edited_translations.segment}"）：

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

示例：允许每个人对存储区进行只读访问

在此示例中，允许每个人（包括匿名者）列出存储桶中的对象，并对存储桶中的所有对象执行 GetObject 操作。所有其他操作将被拒绝。请注意，此策略可能不是特别有用，因为除帐户根目录外，没有人有权写入存储桶。

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

示例：允许一个帐户中的所有人完全访问，允许另一个帐户中的所有人只读访问存储桶

在此示例中，一个指定帐户中的每个人都被允许完全访问存储桶，而另一个指定帐户中的每个人只允许列出存储桶并对存储桶中以 `shared/` 对象键前缀开头的对象执行 GetObject 操作。

> 在 StorageGRID 中，由非所有者帐户（包括匿名帐户）创建的对象归存储桶所有者帐户所有。存储桶策略适用于这些对象。

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

示例：允许每个人对存储区进行只读访问，并允许指定组进行完全访问

在此示例中，允许每个人（包括匿名用户）列出存储桶并对存储桶中的所有对象执行 GetObject 操作，而仅允许指定帐户中属于该组 `Marketing`的用户具有完全访问权限。

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

示例：如果客户端在 IP 范围内，则允许每个人对存储桶进行读取和写入访问

在此示例中，包括匿名在内的所有人都可以列出存储桶，并对存储桶中的所有对象执行任何对象操作，前提是这些请求来自指定的 IP 范围（54.240.143.0 至 54.240.143.255，54.240.143.188 除外）。所有其他操作将被拒绝，IP 范围之外的所有请求也将被拒绝。

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

示例：允许指定的联合用户独占访问存储区

在此示例中，允许联合用户 Alex 完全访问 `examplebucket`存储桶及其对象。所有其他用户，包括''root'，都会被明确拒绝所有操作。但请注意，''root'从未被拒绝对 Put/Get/DeleteBucketPolicy 的权限。

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

示例：**PutOverwriteObject** 权限

在此示例中， `Deny` PutOverwriteObject 和 DeleteObject 的 Effect 确保没有人可以覆盖或删除对象的数据、用户定义的元数据和 S3 对象标记。

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

StorageGRID S3 REST API 组策略示例

使用本节中的示例为组构建 StorageGRID 访问策略。

组策略指定策略附加到的组的访问权限。策略中没有 `Principal`元素，因为它是隐式的。组策略使用 Tenant Manager 或 API 进行配置。

示例：使用 **Tenant Manager** 设置组策略

在租户管理器中添加或编辑组时，可以选择组策略来确定此组的成员将具有哪些 S3 访问权限。请参阅"为 S3 租

户创建组"。

- 无 **S3** 访问权限：默认选项。此组中的用户无权访问 S3 资源，除非使用存储桶策略授予访问权限。如果选择此选项，默认情况下只有 root 用户才能访问 S3 资源。
- 只读访问权限：此组中的用户对 S3 资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据、元数据和标签。选择此选项后，只读组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
- 完全访问权限：此组中的用户具有对 S3 资源（包括存储桶）的完全访问权限。选择此选项时，文本框中将显示完全访问组策略的 JSON 字符串。您无法编辑此字符串。
- **Ransomware Mitigation**：此示例策略适用于此租户的所有存储桶。此组中的用户可以执行常见操作，但不能从已启用对象版本控制的存储桶中永久删除对象。

  拥有"管理所有存储桶"权限的租户管理器用户可以覆盖此组策略。将"管理所有存储桶"权限限制为受信任的用户，并在可用的情况下使用多因素身份验证 (MFA)。

- 自定义：组中的用户将获得您在文本框中指定的权限。

示例：允许组完全访问所有存储桶

在此示例中，除非存储桶策略明确拒绝，否则允许组的所有成员完全访问租户帐户拥有的所有存储桶。

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

示例：允许组只读访问所有存储桶

在此示例中，除非存储桶策略明确拒绝，否则组的所有成员都对 S3 资源具有只读访问权限。例如，此组中的用户可以列出对象并读取对象数据、元数据和标记。

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

示例：仅允许组成员完全访问存储桶中的"文件夹"

在此示例中，组中的成员仅被允许在指定存储桶中列出和访问其特定文件夹（密钥前缀）。请注意，在确定这些文件夹的隐私时，应考虑其他组策略和存储桶策略的访问权限。

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

版权信息

商标信息