存储分段和组访问策略

StorageGRID 11.7

NetApp
April 12, 2024

目录

存储分段和组访问策略

使用存储分段和组访问策略

StorageGRID 使用 Amazon Web Services （ AWS ） 策略语言允许 S3 租户控制对这些存储分段和对象的访问。StorageGRID 系统实施 S3 REST API 策略语言的一个子集。S3 API 的访问策略以 JSON 格式写入。

访问策略概述

StorageGRID 支持两种访问策略。

- * 分段策略 * ，使用 GET 分段策略， PUT 分段策略和 DELETE 分段策略 S3 API 操作进行配置。存储分段策略附加到存储分段，因此，可以对其进行配置，以控制存储分段所有者帐户或其他帐户中的用户对存储分段及其对象的访问。一个存储分段策略适用场景 只能包含一个存储分段，并且可能包含多个组。
- * 组策略 * ，使用租户管理器或租户管理 API 配置。组策略会附加到帐户中的某个组，因此，这些策略会配置为允许该组访问该帐户拥有的特定资源。一个组策略只对一个组进行适用场景 ，并且可能对多个存储分段进行。

> 组策略和存储分段策略之间的优先级没有差别。

StorageGRID 存储分段和组策略遵循由 Amazon 定义的特定语法。每个策略中都包含一组策略语句，每个语句都包含以下元素：

- 语句 ID （ SID ）（可选）
- 影响
- 主体 / 不重要
- 资源 /NotResource
- 操作 / 未操作
- 条件（可选）

策略语句是使用此结构构建的，用于指定权限： Grant <Effic> to allow/deny <Principe> to Perform <Action> on <Resource> when <condition> applies 。

每个策略元素都用于特定功能：

Element	Description
SID	Sid 元素是可选的。SID 仅用作用户的问题描述 。它会被存储，但不会被 StorageGRID 系统解释。
影响	使用 Effect 元素确定是否允许或拒绝指定的操作。您必须使用支持的 Action Element 关键字来确定允许（或拒绝）对存储分段或对象执行的操作。

Element	Description
主体 / 不重要	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，则可以通过指定通配符（ * ）作为主体来进行匿名访问。默认情况下，只有帐户 root 有权访问该帐户拥有的资源。 您只需要在存储分段策略中指定主体元素。对于组策略，附加该策略的组为隐式主体元素。
资源 /NotResource	资源元素用于标识分段和对象。您可以使用 Amazon 资源名称（ ARN ）来标识资源，从而允许或拒绝对存储分段和对象的权限。
操作 / 未操作	操作和效果元素是权限的两个组成部分。当组请求资源时，它们会被授予或拒绝访问该资源。除非您明确分配权限，否则访问将被拒绝，但您可以使用显式拒绝覆盖由其他策略授予的权限。
条件	条件元素是可选的。通过条件，您可以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（ * ）指定所有操作或部分操作。例如，此操作与 S3： GetObject， S3： PutObject 和 S3： DeleteObject 等权限匹配。

```
s3:*Object
```

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

在Principal元素 中、不支持使用通配符、但设置匿名访问除外、此操作会向所有人授予权限。例如，您将通配符（ * ）设置为 Principal 值。

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

在以下示例中，该语句使用的是 " 影响 "， " 主体 "， " 操作 " 和 " 资源 " 元素。此示例显示了一个完整的存储分段策略语句、该语句使用"allow"的效果为Principals即管理组 `federated-group/admin` 和财务团队 `federated-group/finance`、执行操作的权限 `s3:ListBucket` 位于名为的存储分段上 `mybucket` 和操作 `s3:GetObject` 存储在该存储分段内的所有对象上。

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

存储分段策略的大小限制为 20 ， 480 字节，而组策略的大小限制为 5 ， 120 字节。

策略的一致性控制设置

默认情况下，对组策略所做的任何更新最终都是一致的。由于策略缓存，一旦组策略保持一致，所做的更改可能还需要 15 分钟才能生效。默认情况下，对存储分段策略进行的任何更新最终也会保持一致。

您可以根据需要更改存储分段策略更新的一致性保证。例如，出于安全原因，您可能希望对存储分段策略所做的更改尽快生效。

在这种情况下、您可以设置 `Consistency-Control` 标题、或者您也可以使用PUT存储分段一致性请求。更改此请求的一致性控制时，必须使用值 * 全部 * ，这可以为读写一致性提供最高保证。如果在 PUT 存储分段一致性请求的标题中指定任何其他一致性控制值，则此请求将被拒绝。如果为 PUT 存储分段策略请求指定任何其他值，则此值将被忽略。存储分段策略保持一致后，由于策略缓存，更改可能需要额外 8 秒才能生效。

> 如果将一致性级别设置为 "**all** " 以强制新的存储分段策略更快生效，请确保在完成后将存储分段级别控制设置回其原始值。否则，所有未来的存储分段请求将使用 * 全部 * 设置。

在策略语句中使用 ARN

在策略语句中， ARN 用于 Principal 和 Resource Element 。

- 使用以下语法指定 S3 资源 ARN ：

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

- 使用以下语法指定身份资源 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，以匹配对象密钥中的零个或多个字符。
- 可以在对象密钥中指定的国际字符应使用 JSON UTF-8 或 JSON \u 转义序列进行编码。不支持百分比编码。

  "RFC 2141 URN 语法"

  PUT 存储分段策略操作的 HTTP 请求正文必须使用 charset=UTF-8 进行编码。

在策略中指定资源

在策略语句中，您可以使用资源元素指定允许或拒绝权限的分段或对象。

- 每个策略语句都需要一个资源元素。在策略中、资源由元素表示 `Resource`**或者、** `NotResource` 以排除。
- 您可以使用 S3 资源 ARN 指定资源。例如：

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

- 您也可以在对象密钥中使用策略变量。例如：

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

- 资源值可以指定创建组策略时尚不存在的存储分段。

指定策略中的主体

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。

- 存储分段策略中的每个策略语句都必须包含一个主体元素。组策略中的策略语句不需要Principal元素、因为该组被理解为主体。

- 在策略中，主体由元素 "`Principal ，` " 或 "`NotPrincipal` " 表示以表示排除。
- 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 root 和帐户中的所有用户：

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

- 您只能指定帐户 root ：

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

- 您可以指定一个特定的联合用户（"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": "*"
```

- 为避免歧义，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离开了组织和用户名 `Alex` 已删除。如果新的Alex加入了该组织并获得了相同的分配 `Alex` 用户名、新用户可能会意外继承授予原始用户的权限。

- 主体值可以指定在创建存储分段策略时尚不存在的组 / 用户名称。

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" 表示以表示排除。其中每个元素都映射到特定的 S3 REST API 操作。

下表列出了应用于存储分段的权限以及应用于对象的权限。

> Amazon S3 现在对 PUT 和 DELETE 分段复制操作使用 S3： PutReplicationConfiguration 权限。StorageGRID 对每个操作使用单独的权限，这些权限与原始 Amazon S3 规范匹配。

> 如果使用 PUT 覆盖现有值，则会执行删除。

应用于存储分段的权限

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： CreateBucket	放入存储分段	
S3： DeleteBucket	删除存储分段	
S3： DeleteBucketMetadataNotification	删除存储分段元数据通知配置	是的。
S3： DeleteBucketPolicy	删除存储分段策略	
S3： DeleteReplicationConfiguration	删除存储分段复制	是， PUT 和 DELETE 的权限不同 *
S3： GetBucketAcl	获取分段 ACL	
S3： GetBucketCompliance	获取存储分段合规性（已弃用）	是的。
S3： GetBucketConsistency	获取存储分段一致性	是的。
S3： GetBucketCORS	获取分段存储器	
S3： GetEncryptionConfiguration	获取存储分段加密	
S3： GetBucketLastAccessTime	获取存储分段上次访问时间	是的。
S3： GetBucketLocation	获取存储分段位置	
S3： GetBucketMetadataNotification	获取存储分段元数据通知配置	是的。

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： GetBucketNotification	获取存储分段通知	
S3： GetBucketObjectLockConfiguration	获取对象锁定配置	
S3： GetBucketPolicy	获取存储分段策略	
S3： GetBucketTagging	获取存储分段标记	
S3： GetBucketVersioning	获取存储分段版本控制	
S3： GetLifeycleConfiguration	获取存储分段生命周期	
S3： GetReplicationConfiguration	获取存储分段复制	
S3： ListAllMy桶	• 获取服务 • 获取存储使用量	是，适用于获取存储使用量
S3： ListBucket	• 获取存储分段（列出对象） • 头存储分段 • 后对象还原	
S3： ListBucketMultipartUploads	• 列出多部件上传 • 后对象还原	
S3： ListBucketVersions	获取存储分段版本	
S3： PutBucketCompliance	PUT 存储分段合规性（已弃用）	是的。
S3： PutBucketConsistency	PUT 存储分段一致性	是的。
S3： PutBucketCORS	• 删除存储分段或† • 放入存储分段箱	
S3： PutEncryptionConfiguration	• 删除存储分段加密 • PUT 存储分段加密	
S3： PutBucketLastAccessTime	PUT 分段上次访问时间	是的。
S3： PutBucketMetadataNotification	PUT 存储分段元数据通知配置	是的。

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： PutBucketNotification	PUT 存储分段通知	
S3： PutBucketObjectLockConfiguration	• 使用PUT存储分段 `x-amz-bucket-object-lock-enabled: true` 请求标头(也需要S3：CreateBucket权限) • PUT 对象锁定配置	
S3： PutBucketPolicy	PUT 存储分段策略	
S3： PutBucketTagging	• 删除存储分段标记† • 放置存储分段标记	
S3： PutBucketVersioning	PUT 存储分版本	
S3： PutLifeycleConfiguration	• 删除存储分段生命周期† • PUT 存储分段生命周期	
S3： PutReplicationConfiguration	PUT 存储分段复制	是， PUT 和 DELETE 的权限不同 *

应用于对象的权限

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： AbortMultipartUpload	• 中止多部分上传 • 后对象还原	
S3：BypassGovernanceRetention	• 删除对象 • 删除多个对象 • 放置对象保留	
S3： DeleteObject	• 删除对象 • 删除多个对象 • 后对象还原	
S3： DeleteObjectTagging	删除对象标记	

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： DeleteObjectVersionTagging	删除对象标记（对象的特定版本）	
S3： DeleteObjectVersion	删除对象（对象的特定版本）	
S3： GetObject	• 获取对象 • HEAD 对象 • 后对象还原 • 选择对象内容	
S3： GetObjectAcl	获取对象 ACL	
S3： GetObjectLegend	获取对象合法保留	
S3： GetObjectRetention	获取对象保留	
S3： GetObjectTagging	获取对象标记	
S3： GetObjectVersionTagging	获取对象标记（对象的特定版本）	
S3： GetObjectVersion	GET 对象（对象的特定版本）	
S3： ListMultipartUploadPart	列出部件， POST 对象还原	
S3： PutObject	• PUT 对象 • PUT 对象—复制 • 后对象还原 • 启动多部件上传 • 完成多部件上传 • 上传部件 • 上传部件—复制	
S3： PutObjectLegend	PUT 对象合法保留	
S3： PutObjectRetention	放置对象保留	
S3： PutObjectTagging	放置对象标记	
S3： PutObjectVersionTagging	PUT 对象标记（对象的特定版本）	

权限	**S3 REST API** 操作	为 **StorageGRID** 自定义
S3： PutOverwriteObject	• PUT 对象 • PUT 对象—复制 • PUT 对象标记 • 删除对象标记 • 完成多部件上传	是的。
S3： RestoreObject	后对象还原	

使用 **PutOverwriteObject** 权限

S3： PutOverwriteObject 权限是一种自定义 StorageGRID 权限，适用场景 可通过此权限创建或更新对象。此权限的设置可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：

- * 允许 *：客户端可以覆盖对象。这是默认设置。
- **deny**:客户端无法覆盖对象。如果设置为 deny ，则 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。
    - 正在执行的任何载入操作均会取消，并返回错误。
    - 如果启用了 S3 版本控制，则 deny 设置将阻止 PUT 对象标记或删除对象标记操作修改对象及其非最新版本的标记集。
  - 如果未找到现有对象，此权限将不起作用。
- 如果不存在此权限，则效果与设置了 allow 时相同。

> 如果当前S3策略允许覆盖、并且PutOverwriteObject权限设置为deny、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，如果选中了*禁止修改客户端*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。

指定策略中的条件

条件用于定义策略何时生效。条件包括运算符和键值对。

条件使用键值对进行评估。一个条件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 条件密钥。

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

支持的条件运算符

条件运算符分为以下几类：

- string
- 数字
- 布尔值
- IP 地址
- 空检查

条件运算符	**Description**
StringEquals	根据完全匹配（区分大小写）将键与字符串值进行比较。
StringNotEquals	根据否定匹配（区分大小写）将键与字符串值进行比较。
StringEqualsIgnoreCase	根据完全匹配将键与字符串值进行比较（忽略大小写）。
StringNotEqualsIgnoreCase	根据否定的匹配将键与字符串值进行比较（忽略大小写）。
StringLike	根据完全匹配（区分大小写）将键与字符串值进行比较。可以包括 * 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。可以包括 * 和? 通配符。
数值方程式	根据精确匹配将键与数字值进行比较。
NumericNotEquals	根据否定匹配将键与数字值进行比较。
数值 GreaterThan	根据 "`大于` " 匹配将键与数值进行比较。
NumericGreaterThals.	根据 "`大于或等于` " 匹配将键与数值进行比较。

条件运算符	Description
数值细小	根据 "`小于` " 匹配将键与数值进行比较。
数值 ThalEquals	根据 "`小于或等于` " 匹配将键与数值进行比较。
池	根据 "`true 或 false` " 匹配将键与布尔值进行比较。
IP 地址	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密钥。

支持的条件密钥

类别	适用的条件密钥	Description
IP 运算符	AWS： 源 Ip	将与发送请求的 IP 地址进行比较。可用于存储分段或对象操作。 • 注意： * 如果 S3 请求是通过管理节点和网关节点上的负载平衡器服务发送的，则此请求将与负载平衡器服务上游的 IP 地址进行比较。 • 注 *： 如果使用第三方非透明负载平衡器，则此负载平衡器将与该负载平衡器的 IP 地址进行比较。任意 `X-Forwarded-For` 标头将被忽略、因为无法确定其有效性。
资源 / 身份	AWS： 用户名	将与发送请求的发件人用户名进行比较。可用于存储分段或对象操作。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 分隔符	将与 GET 分段或 GET 分段对象版本请求中指定的分隔符参数进行比较。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 最大密钥	将与获取分段或获取分段对象版本请求中指定的 max-keys 参数进行比较。
S3： ListBucket 和 S3： ListBucketVersions 权限	S3： 前缀	将与获取分段或获取分段对象版本请求中指定的前缀参数进行比较。

类别	适用的条件密钥	Description
S3： PutObject	S3： object-lock-real-retenation-days	与中指定的保留截止日期进行比较 `x-amz-object-lock-retain-until-date` 请求标头或根据存储分段默认保留期限计算得出、以确保这些值处于以下请求允许的范围内： • PUT 对象 • PUT 对象—复制 • 启动多部件上传
S3： PutObjectRetention	S3： object-lock-real-retenation-days	与 PUT 对象保留请求中指定的保留截止日期进行比较，以确保其在允许的范围内。

指定策略中的变量

您可以在策略中使用变量填充可用的策略信息。您可以在中使用策略变量 `Resource` 中的元素和字符串比较 `Condition` Element。

在此示例中、为变量 `${aws:username}` 是资源元素的一部分：

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

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

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

变量	Description
`${aws:SourceIp}`	使用 SourceIp 键作为提供的变量。
`${aws:username}`	使用 username 密钥作为提供的变量。
`${s3:prefix}`	使用特定于服务的前缀密钥作为提供的变量。
`${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。使用字符作为文字 * 字符。

变量	Description
${?}	特殊字符。使用字符作为文字？字符。
${$}	特殊字符。使用字符作为文字 $ 字符。

创建需要特殊处理的策略

有时，策略可能会授予对安全性有危险或对持续操作（例如锁定帐户的 root 用户）有危险的权限。在策略验证期间， StorageGRID S3 REST API 实施的限制性要低于 Amazon ，但在策略评估期间同样严格。

策略问题描述	Policy type	Amazon 行为	StorageGRID 行为
拒绝向自己授予对 root 帐户的任何权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
拒绝用户 / 组的任何权限	组	有效且强制实施	相同
允许外部帐户组拥有任何权限	存储分段	主体无效	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误
允许外部帐户 root 或用户拥有任何权限	存储分段	有效，但如果某个策略允许，则所有 S3 存储分段策略操作的权限均会返回 405 Method not allowed 错误	相同
允许所有人对所有操作拥有权限	存储分段	有效，但对所有 S3 存储分段策略操作的权限会为外部帐户 root 和用户返回 405 Method not allowed 错误	相同
拒绝任何人对所有操作的权限	存储分段	有效且强制实施，但 root 用户帐户保留所有 S3 存储分段策略操作的权限	相同
主体是不存在的用户或组	存储分段	主体无效	有效
资源不是 S3 存储分段	组	有效	相同
主体是一个本地组	存储分段	主体无效	有效

策略问题描述	Policy type	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	存储分段	有效。对象由创建者帐户拥有，并且存储分段策略不适用。创建者帐户必须使用对象 ACL 为对象授予访问权限。	有效。对象由存储分段所有者帐户拥有。存储分段策略适用。

一次写入多读（WORM）保护

您可以创建一次写入多读（Write Once Read-Many， WORM）分段来保护数据，用户定义的对象元数据和 S3 对象标记。您可以配置 WORM 分段，以便创建新对象并防止覆盖或删除现有内容。请使用此处所述的方法之一。

为了确保覆盖始终被拒绝，您可以：

- 在网格管理器中，转到*configuration*>*Security*>*Security settings **>*Network and objects**，然后选中*prevent client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。
  - 将 DeleteObject deny 操作添加到 S3 策略中。
  - 向 S3 策略添加 PUT 对象允许操作。

> 在 S3 策略中将 DeleteObject 设置为 deny 不会阻止 ILM 在存在 "`zero copies after 30 days` " 等规则时删除对象。

> 即使应用了所有这些规则和策略、它们也无法防止并发写入(请参见情形A)。它们可以防止顺序完成的覆盖（请参见情况 B ）。

- 情形 A*：并发写入（不受保护）

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

- 情形 B*：顺序完成的覆盖（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"
- "存储分段策略示例"
- "组策略示例"

- "使用 ILM 管理对象"
- "使用租户帐户"

存储分段策略示例

使用本节中的示例为分段构建StorageGRID 访问策略。

存储分段策略用于指定附加此策略的存储分段的访问权限。存储分段策略使用 S3 PutBucketPolicy API 进行配置。请参见 "对存储分段执行的操作"。

可以按照以下命令使用 AWS 命令行界面配置存储分段策略：

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

示例：允许每个人对某个存储分段进行只读访问

在此示例中，允许包括匿名用户在内的所有人列出存储分段中的对象，并对存储分段中的所有对象执行 GET Object 操作。所有其他操作都将被拒绝。请注意、此策略可能并不特别有用、因为除了帐户root之外、没有其他人有权向存储分段写入数据。

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

示例：允许一个帐户中的每个人完全访问某个存储分段，而另一帐户中的每个人只读访问某个存储分段

在此示例中、一个指定帐户中的每个人都可以完全访问某个存储分段、而另一个指定帐户中的每个人只能列出存储分段并对以开头的存储分段中的对象执行GetObject操作 `shared/` 对象密钥前缀。

> 在 StorageGRID 中，非所有者帐户创建的对象（包括匿名帐户）归存储分段所有者帐户所有。存储分段策略适用场景 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：允许每个人对某个存储分段进行只读访问，并允许指定组进行完全访问

在此示例中、允许包括anonymous在内的所有人列出存储分段并对存储分段中的所有对象执行GET Object操作、而只允许用户属于该组 `Marketing` 在指定帐户中、允许完全访问。

```
{
  "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：如果客户端位于 IP 范围内，则允许每个人对存储分段进行读写访问

在此示例中，允许包括匿名用户在内的所有人列出存储分段并对存储分段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 到 54.240.143.255 ，但 54.240.143.188 除外）。所有其他操作都将被拒绝，并且 IP 范围以外的所有请求都将被拒绝。

```
{
  "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完全访问某个存储分段

在此示例中、允许联合用户Alex完全访问 `examplebucket` 存储分段及其对象。包括 "`root` " 在内的所有其他用户均被明确拒绝所有操作。但请注意， "`root` " 从不会被拒绝 PUT ， Get/DeleteBucketPolicy 的权限。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::9539088723000255820 2:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::9539088723000255820 2:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

示例： **PutOverwriteObject** 权限

在此示例中、将显示 `Deny` 对PutOverwriteObject和DeleteObject的影响可确保任何人都不能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/*"
    }
  ]
}
```

组策略示例

使用本节中的示例为组构建StorageGRID 访问策略。

组策略用于指定附加此策略的组的访问权限。没有 `Principal` 元素、因为它是隐式的。组策略可使用租户管理器或 API 进行配置。

示例：使用租户管理器设置组策略

在租户管理器中添加或编辑组时、您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。请参见 "为 S3

租户创建组"。

- * 无 S3 访问 * ：默认选项。此组中的用户无权访问S3资源、除非使用存储分段策略授予访问权限。如果选择此选项，则默认情况下，只有 root 用户才能访问 S3 资源。
- * 只读访问 * ：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，元数据和标记。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 * ：此组中的用户对 S3 资源（包括分段）具有完全访问权限。选择此选项后，完全访问组策略的 JSON 字符串将显示在文本框中。您无法编辑此字符串。
- **Ransmans**要 缓解：此示例策略适用场景 all b分 段for this租户。此组中的用户可以执行常见操作、但无法从启用了对象版本控制的分段中永久删除对象。

  具有"管理所有存储分段"权限的租户管理器用户可以覆盖此组策略。将"管理所有分段"权限限制为受信任用户、并在可用时使用多因素身份验证(Multi-FactorAuthentication、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分段

在此示例中，除非 bucket 策略明确拒绝，否则允许组中的所有成员对租户帐户拥有的所有分段进行完全访问。

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

示例：允许组对所有分段进行只读访问

在此示例中，组的所有成员都对 S3 资源具有只读访问权限，除非 bucket 策略明确拒绝。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：仅允许组成员对存储分段中的"`folder`"具有完全访问权限

在此示例中，组成员只能列出并访问指定存储分段中的特定文件夹（密钥前缀）。请注意，在确定其他组策略和存储分段策略的隐私时，应考虑这些文件夹的访问权限。

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