



# 使用 **S3 REST API**

## StorageGRID software

NetApp  
July 23, 2026

# 目录

|                                            |    |
|--------------------------------------------|----|
| 使用 S3 REST API .....                       | 1  |
| StorageGRID S3 REST API 支持的版本和更新 .....     | 1  |
| 支持的版本 .....                                | 1  |
| S3 REST API 支持更新 .....                     | 1  |
| StorageGRID 中支持的 S3 API 请求 .....           | 4  |
| 通用 URI 查询参数和请求标头 .....                     | 4  |
| "AbortMultipartUpload" .....               | 4  |
| "CompleteMultipartUpload" .....            | 5  |
| "CopyObject" .....                         | 5  |
| "CreateBucket" .....                       | 6  |
| "CreateMultipartUpload" .....              | 6  |
| >DeleteBucket" .....                       | 7  |
| >DeleteBucketCors" .....                   | 7  |
| >DeleteBucketEncryption" .....             | 7  |
| >DeleteBucketLifecycle" .....              | 8  |
| >DeleteBucketPolicy" .....                 | 8  |
| >DeleteBucketReplication" .....            | 8  |
| >DeleteBucketTagging" .....                | 8  |
| "删除对象" .....                               | 9  |
| >DeleteObjects" .....                      | 9  |
| >DeleteObjectTagging" .....                | 9  |
| "GetBucketAcl" .....                       | 9  |
| "GetBucketCors" .....                      | 10 |
| "GetBucketEncryption" .....                | 10 |
| "GetBucketLifecycleConfiguration" .....    | 10 |
| "GetBucketLocation" .....                  | 10 |
| "GetBucketNotificationConfiguration" ..... | 11 |
| "GetBucketPolicy" .....                    | 11 |
| "GetBucketReplication" .....               | 11 |
| "GetBucketTagging" .....                   | 11 |
| "GetBucketVersioning" .....                | 12 |
| "获取对象" .....                               | 12 |
| "GetObjectAcl" .....                       | 13 |
| "GetObjectLegalHold" .....                 | 13 |
| "GetObjectLockConfiguration" .....         | 13 |
| "GetObjectRetention" .....                 | 13 |
| "GetObjectTagging" .....                   | 14 |
| "HeadBucket" .....                         | 14 |
| "HeadObject" .....                         | 14 |
| >ListBuckets" .....                        | 15 |
| >ListMultipartUploads" .....               | 15 |
| >ListObjects" .....                        | 15 |

|                                                    |    |
|----------------------------------------------------|----|
| "ListObjectsV2"                                    | 16 |
| "ListObjectVersions"                               | 16 |
| "ListParts"                                        | 16 |
| "PutBucketCors"                                    | 17 |
| "PutBucketEncryption"                              | 17 |
| "PutBucketLifecycleConfiguration"                  | 17 |
| "PutBucketNotificationConfiguration"               | 18 |
| "PutBucketPolicy"                                  | 19 |
| "PutBucketReplication"                             | 19 |
| "PutBucketTagging"                                 | 19 |
| "PutBucketVersioning"                              | 20 |
| "放置对象"                                             | 20 |
| "PutObjectLegalHold"                               | 21 |
| "PutObjectLockConfiguration"                       | 21 |
| "PutObjectRetention"                               | 21 |
| "PutObjectTagging"                                 | 21 |
| "RestoreObject"                                    | 22 |
| "SelectObjectContent"                              | 22 |
| "UploadPart"                                       | 22 |
| "UploadPartCopy"                                   | 22 |
| 测试 StorageGRID S3 REST API 配置                      | 23 |
| StorageGRID 实现 S3 REST API                         | 25 |
| StorageGRID S3 REST API 如何解决冲突的客户端请求               | 25 |
| StorageGRID S3 REST API 如何平衡可用性和一致性                | 25 |
| StorageGRID 如何使用对象版本控制                             | 27 |
| 使用 S3 REST API 配置 StorageGRID S3 对象锁定              | 28 |
| 了解 StorageGRID 的 S3 生命周期配置                         | 33 |
| 使用 StorageGRID 实施 S3 REST API 的建议                  | 37 |
| 支持 Amazon S3 REST API                              | 38 |
| StorageGRID 中 S3 REST API 支持的操作和限制                 | 38 |
| StorageGRID S3 REST API 如何验证请求                     | 39 |
| StorageGRID 中支持的服务操作                               | 39 |
| StorageGRID 中的 S3 存储桶操作和实施详细信息                     | 40 |
| 对象上的操作                                             | 47 |
| 多部分上传的操作                                           | 73 |
| StorageGRID S3 REST API 错误响应                       | 81 |
| StorageGRID 自定义操作                                  | 83 |
| StorageGRID 中支持的自定义存储桶操作                           | 83 |
| 使用 GET Bucket 一致性请求检索 StorageGRID 中的存储桶一致性级别       | 84 |
| 使用 PUT Bucket 一致性请求在 StorageGRID 中指定一致性级别          | 85 |
| 使用 GET Bucket 上次访问时间请求检索 StorageGRID 中的存储桶上次访问时间状态 | 86 |
| 使用 PUT Bucket 上次访问时间请求在 StorageGRID 中启用和禁用上次访问时间更新 | 87 |
| 使用 StorageGRID 中的 DELETE Bucket 元数据通知配置请求禁用搜索集成服务  | 88 |

|                                                            |     |
|------------------------------------------------------------|-----|
| 使用 GET Bucket 元数据通知配置请求在 StorageGRID 中配置搜索集成 .....         | 88  |
| 使用 PUT Bucket 元数据通知配置请求在 StorageGRID 中启用搜索集成服务 .....       | 91  |
| 使用 GET Storage Usage 请求检索 StorageGRID 中的帐户和存储桶存储使用情况 ..... | 96  |
| 旧版合规性的已弃用存储桶请求 .....                                       | 97  |
| 管理访问策略 .....                                               | 102 |
| StorageGRID 如何使用 AWS 策略来控制对 S3 存储桶和对象的访问 .....             | 102 |
| StorageGRID S3 REST API 会话策略示例 .....                       | 118 |
| StorageGRID S3 REST API 存储桶策略示例 .....                      | 118 |
| StorageGRID S3 REST API 组策略示例 .....                        | 124 |
| StorageGRID 审核日志中跟踪的 S3 操作 .....                           | 127 |
| 在审核日志中跟踪的存储桶操作 .....                                       | 127 |
| 审计日志中跟踪的对象操作 .....                                         | 128 |

# 使用 S3 REST API

## StorageGRID S3 REST API 支持的版本和更新

StorageGRID 支持 Simple Storage Service (S3) API，该 API 作为一组表示性状态传输 (REST) Web 服务实现。

对 S3 REST API 的支持使您能够将 S3 Web 服务开发的面向服务的应用程序与使用 StorageGRID 系统的本地对象存储相连接。只需对客户端应用程序当前使用的 S3 REST API 调用进行极少量更改。

### 支持的版本

StorageGRID 支持以下特定版本的 STS、S3 和 HTTP：

| 个项目                   | 版本                                                                                                                                                             |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STS AssumeRole API 规范 | <p><a href="#">"Amazon Web Services (AWS) 文档：Amazon Assumerole API Reference"</a></p> <p>有关 AssumeRole 的详细信息，请参阅 <a href="#">"设置 AssumeRole"</a>。</p>          |
| S3 API 规范             | <p><a href="#">"AWS 文档：Amazon Simple Storage Service API 参考"</a></p>                                                                                           |
| HTTP                  | <p>1.1</p> <p>有关 HTTP 的详细信息，请参见 HTTP/1.1 (RFCs 7230-35)。</p> <p><a href="#">"IETF RFC 2616：超文本传输协议 (HTTP/1.1)"</a></p> <p>注意：StorageGRID 不支持 HTTP/1.1 流水线。</p> |

### S3 REST API 支持更新

| 版本   | 注释                                                                                                                                                                                                                            |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0 | <ul style="list-style-type: none"><li>添加了对管理接口的跨源资源共享 (CORS) 支持，允许另一个域使用管理 API 访问 StorageGRID 中的数据。<a href="#">"了解更多"</a>。</li><li>添加了对 STS AssumeRole 和会话策略的支持。请参阅<a href="#">"会话策略的示例"</a>。您可以在租户组下设置 AssumeRole。</li></ul> |

| 版本   | 注释                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.9 | <ul style="list-style-type: none"> <li>添加了对以下请求和支持的标头的预先计算的 SHA-256 校验和值的支持。您可以使用此功能验证上传对象的完整性： <ul style="list-style-type: none"> <li>CompleteMultipartUpload: x-amz-checksum-sha256</li> <li>CreateMultipartUpload: x-amz-checksum-algorithm</li> <li>GetObject: x-amz-checksum-mode</li> <li>HeadObject: x-amz-checksum-mode</li> <li>ListParts</li> <li>PutObject: x-amz-checksum-sha256</li> <li>UploadPart: x-amz-checksum-sha256</li> </ul> </li> <li>添加了网格管理员控制租户级别保留和合规性设置的功能。这些设置会影响 S3 Object Lock 设置。 <ul style="list-style-type: none"> <li>存储桶默认保留模式和对对象保留模式：治理或合规（如果网格管理员允许）。</li> <li>存储桶默认保留期限和对对象保留截止日期：必须小于或等于网格管理员设置的最大保留期限所允许的值。</li> </ul> </li> <li>改进了对 `aws-chunked` 内容编码和流式传输 `x-amz-content-sha256` 值的支持。限制： <ul style="list-style-type: none"> <li>如果存在，`chunk-signature` 是可选的且不经过验证</li> <li>如果存在，则忽略 `x-amz-trailer` 内容</li> </ul> </li> </ul> |
| 11.8 | 更新了 S3 操作的名称，以匹配 <a href="#">"Amazon Web Services (AWS) 文档：Amazon Simple Storage Service API 参考"</a> 中使用的名称。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 11.7 | <ul style="list-style-type: none"> <li>已添加 <a href="#">"快速参考：支持的 S3 API 请求"</a>。</li> <li>增加了对 S3 Object Lock 使用 GOVERNANCE 模式的支持。</li> <li>增加了对 StorageGRID 特定 `x-ntap-sg-cgr-replication-status` 响应标头的支持，适用于 GET Object 和 HEAD Object 请求。此标头为跨网格复制提供对象的复制状态。</li> <li>SelectObjectContent 请求现在支持 Parquet 对象。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 11.6 | <ul style="list-style-type: none"> <li>新增了在 GET Object 和 HEAD Object 请求中使用 `partNumber` 请求参数的支持。</li> <li>增加了对 S3 Object Lock 存储桶级别的默认保留模式和默认保留期限的支持。</li> <li>增加了对 `s3:object-lock-remaining-retention-days` 策略条件键的支持，以设置对象的允许保留期范围。</li> <li>将单个 PUT Object 操作的最大_建议_大小更改为 5 GiB（5,368,709,120 字节）。如果您的对象大于 5 GiB，请改用分段上传。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| 版本   | 注释                                                                                                                                                                                                                                                                                                                                                        |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11.5 | <ul style="list-style-type: none"> <li>• 增加了对存储桶加密的管理支持。</li> <li>• 新增了对 S3 Object Lock 的支持，并弃用了旧版合规性请求。</li> <li>• 增加了对在版本化存储桶上使用DELETE Multiple Objects的支持。</li> <li>• The Content-MD5 请求标头现在已得到正确支持。</li> </ul>                                                                                                                                        |
| 11.4 | <ul style="list-style-type: none"> <li>• 增加了对 DELETE Bucket 标记、GET Bucket 标记和 PUT Bucket 标记的支持。不支持成本分配标签。</li> <li>• 对于在 StorageGRID 11.4 中创建的存储桶，不再需要限制对象密钥名称以满足性能最佳实践。</li> <li>• 增加了对 `s3:ObjectRestore:Post` 事件类型的存储桶通知的支持。</li> <li>• AWS 对多部分部件的大小限制现已强制执行。多部分上传中的每个部分必须介于 5 MiB 和 5 GiB 之间。最后一部分可以小于 5 MiB。</li> <li>• 增加了对 TLS 1.3 的支持</li> </ul> |
| 11.3 | <ul style="list-style-type: none"> <li>• 增加了对使用客户提供的密钥（SSE-C）的对象数据进行服务器端加密的支持。</li> <li>• 增加了对 DELETE、GET 和 PUT Bucket 生命周期操作（仅限 Expiration 操作）以及 `x-amz-expiration` 响应标头的支持。</li> <li>• 更新了 PUT Object、PUT Object - Copy 和 Multipart Upload，以描述在接收时使用同步放置的 ILM 规则的影响。</li> <li>• TLS 1.1 加密不再受支持。</li> </ul>                                             |
| 11.2 | <p>增加了对用于云存储池的 POST Object restore 的支持。增加了对在组和存储桶策略中使用 AWS 语法的 ARN、策略条件键和策略变量的支持。使用 StorageGRID 语法的现有组和存储桶策略将继续受到支持。</p> <p>注意：其他配置 JSON/XML（包括自定义 StorageGRID 功能中使用的配置）中 ARN/URN 的使用没有改变。</p>                                                                                                                                                            |
| 11.1 | 增加了对跨源资源共享(CORS)、S3 客户端连接到网格节点的 HTTP 以及存储桶上的合规性设置的支持。                                                                                                                                                                                                                                                                                                     |
| 11.0 | 增加了对存储桶配置平台服务（CloudMirror 复制、通知和 Elasticsearch 搜索集成）的支持。还增加了对存储桶的对象标记位置约束的支持，以及可用一致性。                                                                                                                                                                                                                                                                     |
| 10.4 | 增加了对 ILM 扫描更改版本控制、端点域名页面更新、策略中的条件和变量、策略示例以及 PutOverwriteObject 权限的支持。                                                                                                                                                                                                                                                                                     |
| 10.3 | 增加了对版本控制的支持。                                                                                                                                                                                                                                                                                                                                              |
| 10.2 | 增加了对组和存储桶访问策略以及分段复制（Upload Part - Copy）的支持。                                                                                                                                                                                                                                                                                                               |

| 版本   | 注释                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------|
| 10.1 | 增加了对多部分上传、虚拟托管式请求和 v4 身份验证的支持。                                                                      |
| 10.0 | StorageGRID 系统对 S3 REST API 的初始支持。 <i>Simple Storage Service API Reference</i> 当前支持的版本为 2006-03-01。 |

## StorageGRID 中支持的 S3 API 请求

本页总结了 StorageGRID 如何支持 Amazon Simple Storage Service (S3) API。

此页面仅包括 StorageGRID 支持的 S3 操作。



要查看每个操作的 AWS 文档，请选择标题中的链接。

### 通用 URI 查询参数和请求标头

除非另有说明，否则支持以下常见 URI 查询参数：

- `versionId`（根据对象操作的要求）

除非另有说明，否则支持以下常见请求标头：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

### 相关信息

- ["S3 REST API 实现详情"](#)
- ["Amazon Simple Storage Service API Reference：常见请求标头"](#)

## "AbortMultipartUpload"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及此附加 URI 查询参数：

- `uploadId`

请求正文

无

**StorageGRID 文档**

["多部分上传的操作"](#)

## "CompleteMultipartUpload"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及此附加 URI 查询参数：

- uploadId
- x-amz-checksum-sha256

请求正文 **XML** 标记

StorageGRID 支持这些请求正文 XML 标记：

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

**StorageGRID 文档**

["CompleteMultipartUpload"](#)

## "CopyObject"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及以下附加标头：

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode

- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

请求正文

无

**StorageGRID 文档**

["CopyObject"](#)

## "CreateBucket"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及以下附加标头：

- x-amz-bucket-object-lock-enabled

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "CreateMultipartUpload"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及以下附加标头：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

请求正文

无

**StorageGRID 文档**

["CreateMultipartUpload"](#)

## "DeleteBucket"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "DeleteBucketCors"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "DeleteBucketEncryption"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "DeleteBucketLifecycle"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

- `"${post_edited_translations.segment}"`
- ["创建 S3 生命周期配置"](#)

## "DeleteBucketPolicy"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

`"${post_edited_translations.segment}"`

## "DeleteBucketReplication"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

`"${post_edited_translations.segment}"`

## "DeleteBucketTagging"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

`"${post_edited_translations.segment}"`

## "删除对象"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及此附加请求标头：

- x-amz-bypass-governance-retention

请求正文

无

**StorageGRID 文档**

["对象上的操作"](#)

## "DeleteObjects"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及此附加请求标头：

- x-amz-bypass-governance-retention

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["对象上的操作"](#)

## "DeleteObjectTagging"

StorageGRID 支持此请求的所有 [通用参数和标头](#) 内容。

请求正文

无

**StorageGRID 文档**

["对象上的操作"](#)

## "GetBucketAcl"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "GetBucketCors"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "GetBucketEncryption"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "GetBucketLifecycleConfiguration"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

- ["\\${post\\_edited\\_translations.segment}"](#)
- ["创建 S3 生命周期配置"](#)

## "GetBucketLocation"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "GetBucketNotificationConfiguration"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "GetBucketPolicy"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "GetBucketReplication"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "GetBucketTagging"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "GetBucketVersioning"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "获取对象"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有 [通用参数和标头](#) URI 查询参数，以及以下额外的 URI 查询参数：

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

这些额外的请求标头：

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

请求正文

无

**StorageGRID 文档**

["获取对象"](#)

## "GetObjectAcl"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["对象上的操作"](#)

## "GetObjectLegalHold"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "GetObjectLockConfiguration"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "GetObjectRetention"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "GetObjectTagging"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["对象上的操作"](#)

## "HeadBucket"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "HeadObject"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及以下附加标头：

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

请求正文

无

**StorageGRID 文档**

["HeadObject"](#)

## "ListBuckets"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

无

**StorageGRID 文档**

[服务上的操作](#) › [ListBuckets](#)

## "ListMultipartUploads"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 参数，以及以下附加参数：

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

请求正文

无

**StorageGRID 文档**

["ListMultipartUploads"](#)

## "ListObjects"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 参数，以及以下附加参数：

- delimiter
- encoding-type
- marker
- max-keys
- prefix

请求正文

无

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "ListObjectsV2"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 参数，以及以下附加参数：

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

请求正文

无

### StorageGRID 文档

"\${post\_edited\_translations.segment}"

## "ListObjectVersions"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 参数，以及以下附加参数：

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

请求正文

无

### StorageGRID 文档

"\${post\_edited\_translations.segment}"

## "ListParts"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) 参数，以及以下附加参数：

- max-parts

- part-number-marker
- uploadId

请求正文

无

**StorageGRID 文档**

["ListMultipartUploads"](#)

## "PutBucketCors"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "PutBucketEncryption"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文 **XML** 标记

StorageGRID 支持这些请求正文 XML 标记：

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "PutBucketLifecycleConfiguration"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文 **XML** 标记

StorageGRID 支持这些请求正文 XML 标记：

- And
- Days

- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

#### StorageGRID 文档

- ["\\${post\\_edited\\_translations.segment}"](#)
- ["创建 S3 生命周期配置"](#)

## "PutBucketNotificationConfiguration"

#### URI 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

#### 请求正文 XML 标记

StorageGRID 支持这些请求正文 XML 标记：

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration

- Value

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "PutBucketPolicy"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

有关支持的JSON正文字段的详细信息，请参见 ["使用存储区和组访问策略"](#)。

## "PutBucketReplication"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文 **XML 标记**

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "PutBucketTagging"

**URI 查询参数和请求标头**

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

"\${post\_edited\_translations.segment}"

## "PutBucketVersioning"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文参数

StorageGRID 支持以下请求正文参数：

- VersioningConfiguration
- Status

**StorageGRID 文档**

["\\${post\\_edited\\_translations.segment}"](#)

## "放置对象"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及以下附加标头：

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

请求正文

- 对象的二进制数据

**StorageGRID 文档**

["放置对象"](#)

## "PutObjectLegalHold"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "PutObjectLockConfiguration"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "PutObjectRetention"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#)，以及此附加标头：

- x-amz-bypass-governance-retention

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["使用 S3 REST API 配置 S3 对象锁定"](#)

## "PutObjectTagging"

**URI** 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

请求正文

StorageGRID 支持实施时 Amazon S3 REST API 定义的所有请求正文参数。

**StorageGRID 文档**

["对象上的操作"](#)

## "RestoreObject"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

### 请求正文

有关支持的正文字段的详细信息，请参见 ["RestoreObject"](#)。

## "SelectObjectContent"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有[通用参数和标头](#)内容。

### 请求正文

有关受支持的正文字段的详细信息，请参见以下内容：

- ["使用 S3 Select"](#)
- ["SelectObjectContent"](#)

## "UploadPart"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) URI 查询参数，以及以下额外的 URI 查询参数：

- `partNumber`
- `uploadId`

这些额外的请求标头：

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

### 请求正文

- 零件的二进制数据

### StorageGRID 文档

["UploadPart"](#)

## "UploadPartCopy"

### URI 查询参数和请求标头

StorageGRID 支持此请求的所有 [通用参数和标头](#) URI 查询参数，以及以下额外的 URI 查询参数：

- `partNumber`

- uploadId

这些额外的请求标头：

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

请求正文

无

**StorageGRID 文档**

["UploadPartCopy"](#)

## 测试 StorageGRID S3 REST API 配置

您可以使用 Amazon Web Services 命令行界面 (AWS CLI) 测试与系统的连接并验证是否可以读写对象。

开始之前

- 您已从 ["aws.amazon.com/cli"](https://aws.amazon.com/cli) 下载并安装 AWS CLI。
- 可选地，您有 ["已创建负载均衡器端点"](#)。否则，您知道要连接到的存储节点的 IP 地址以及要使用的端口号。请参阅 ["用于客户端连接的 IP 地址和端口"](#)。
- 您有 ["创建了 S3 租户帐户"](#)。
- 您已登录到租户和 ["已创建访问密钥"](#)。

有关这些步骤的详细信息，请参见 ["配置客户端连接"](#)。

步骤

1. 配置 AWS CLI 设置以使用您在 StorageGRID 系统中创建的帐户：
  - a. 输入配置模式：aws configure
  - b. 输入您创建的帐户的访问密钥 ID。

- c. 输入您创建的帐户的私有访问密钥。
- d. 输入要使用的默认区域。例如， `us-east-1`。
- e. 请输入要使用的默认输出格式，或按 **Enter** 键选择 JSON。

## 2. 创建存储桶。

此示例假设您将负载均衡器端点配置为使用 IP 地址 10.96.101.17 和端口 10443。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

如果成功创建存储桶，则返回存储桶的位置，如以下示例所示：

```
"Location": "/testbucket"
```

## 3. 上传对象。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

如果成功上传对象，则返回 Etag，这是对象数据的哈希值。

## 4. 列出存储桶的内容以确认对象已上传。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

## 5. 删除对象。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

## 6. 删除存储桶。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

# StorageGRID 实现 S3 REST API

## StorageGRID S3 REST API 如何解决冲突的客户端请求

冲突的客户端请求（例如两个客户端写入同一密钥）将以"最新获胜"为原则进行解决。

"最新获胜"评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

## StorageGRID S3 REST API 如何平衡可用性和一致性

一致性提供了对象的可用性和这些对象在不同存储节点和站点之间的一致性之间的平衡。您可以根据应用程序的要求更改一致性。

默认情况下，StorageGRID 保证新创建的对象的后读一致性。成功完成 PUT 后的任何 GET 都可以读取新写入的数据。现有对象的覆盖、元数据更新和删除最终是一致的。

如果要以不同的一致性执行对象操作，则可以：

- 请指定 [每个存储桶](#) 的一致性。
- 为 [每个 API 操作](#) 指定一致性。
- 通过执行以下任务之一更改默认网格范围的一致性：
  - 在网格管理器中，转到\*配置\* > 系统 > 存储设置 > 默认存储桶一致性。
  - 。



对网格范围一致性的更改仅适用于更改设置后创建的存储桶。要确定更改的详细信息，请参见位于 `/var/local/log` 的审计日志（搜索 **consistencyLevel**）。

### 一致性值

一致性会影响 StorageGRID 用于跟踪对象的元数据在节点之间的分布方式。一致性会影响客户端请求对象的可用性。

可以将存储桶或 API 操作的一致性设置为以下值之一：

- 所有：所有节点立即接收对象元数据，否则请求将失败。
- **Strong-global**：保证所有站点上所有客户端请求的后读一致性。配置 Quorum 语义时，适用以下行为：
  - 当网格具有三个或更多站点时，允许客户端请求的站点容错。双站点网格不具有站点故障容限。
  - 如果一个站点关闭，以下 S3 操作将不会成功：
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold

- PutObjectLockConfiguration
- PutObjectRetention

如有需要，您可以 ["配置 StorageGRID 仲裁语义以实现强全局一致性"](#)。

- **Strong-site**：对象元数据会立即分发到站点上的其他节点。保证站点内所有客户端请求的写后读一致性。
- **Read-after-new-write**：为新对象提供写后读一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议在大多数情况下使用。
- **可用**：为新对象和对象更新提供最终一致性。对于 S3 存储桶，仅根据需要使用（例如，对于包含很少读取的日志值的存储桶，或者对于不存在的键的 HEAD 或 GET 操作）。不支持 S3 FabricPool 存储桶。

## 使用"新写后读"和"可用"一致性

当 HEAD 或 GET 操作使用"新写后读"一致性时，StorageGRID 将按以下步骤执行查找：

- 它首先使用低一致性查找对象。
- 如果查找失败，它会重复查找下一个一致性值，直到达到与 strong-global 行为等效的一致性。

如果 HEAD 或 GET 操作使用"新写后读"一致性，但对象不存在，则对象查找将始终达到与 strong-global 行为等效的一致性。由于这种一致性要求每个站点提供多个对象元数据副本，因此如果同一站点上的两个或多个存储节点不可用，则可能会收到大量 500 Internal Server 错误。

除非您需要类似于 Amazon S3 的一致性保证，否则可以通过将一致性设置为"可用"来防止 HEAD 和 GET 操作出现这些错误。当 HEAD 或 GET 操作使用"可用"一致性时，StorageGRID 仅提供最终一致性。它不会以增加一致性的方式重试失败的操作，因此不需要提供多个对象元数据副本。

## 指定 API 操作的一致性

要为单个 API 操作设置一致性，必须为该操作支持一致性值，并且必须在请求标头中指定一致性。此示例将 GetObject 操作的一致性设置为"Strong-site"。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



您必须对PutObject和GetObject操作使用相同的一致性。

## 指定bucket的一致性

要设置存储桶的一致性，您可以使用 StorageGRID ["PUT Bucket 一致性"](#) 请求。或者，您可以从租户管理器 ["更改存储桶的一致性"](#)。

在设置存储区的一致性时，请注意以下几点：

- 设置存储桶的一致性决定了对存储桶中的对象或存储桶配置执行的 S3 操作所使用的一致性。它不影响存储桶本身的操作。

- 单个 API 操作的一致性将覆盖存储桶的一致性。
- 一般来说，存储桶应使用默认的一致性，"Read-after-new-write."如果请求无法正常工作，请尽可能更改应用程序客户端行为。或者，配置客户端以指定每个 API 请求的一致性。仅作为最后手段，在存储桶级别设置一致性。

### 一致性和ILM规则如何相互作用以影响数据保护

您选择的一致性和 ILM 规则都会影响对象的保护方式。这些设置可以相互影响。

例如，存储对象时使用的一致性会影响对象元数据的初始放置，而为 ILM 规则选择的摄取行为会影响对象副本的初始放置。由于 StorageGRID 需要访问对象的元数据及其数据来满足客户端请求，因此为一致性和摄取行为选择匹配的保护级别可以提供更好的初始数据保护和更可预测的系统响应。

以下["载入选项"](#)可用于 ILM 规则：

#### 双提交

StorageGRID 立即生成对象的临时副本，并将成功返回给客户端。ILM 规则中指定的副本将在可能时创建。

#### 严格

在成功返回到客户端之前，必须创建 ILM 规则中指定的所有副本。

#### 平衡

StorageGRID 尝试在导入时生成 ILM 规则中指定的所有副本；如果无法实现，则生成临时副本并将成功状态返回给客户端。ILM 规则中指定的副本将在可能时生成。

### 一致性和 ILM 规则如何相互作用的示例

假设您有一个具有以下 ILM 规则和以下一致性的三站点网格：

- ILM 规则：创建三个对象副本，一个在本地站点，一个在每个远程站点。使用严格的载入行为。
- 一致性：强全局（对象元数据立即分发到多个站点）。

当客户端将对象存储到网格中时，StorageGRID 会创建所有三个对象副本并将元数据分发到多个站点，然后再将成功状态返回给客户端。

对象在接收成功消息时受到完全保护，不会丢失。例如，如果本地站点在载入后不久丢失，则对象数据和对象元数据的副本仍然存在于远程站点。该对象可从其他站点完全检索。

如果改为使用相同的 ILM 规则和强站点一致性，则在对象数据复制到远程站点但对象元数据分发到远程站点之前，客户端可能会收到一条成功消息。在这种情况下，对象元数据的保护级别与对象数据的保护级别不匹配。如果本地站点在载入后不久丢失，则对象元数据将丢失。无法检索对象。

一致性和 ILM 规则之间的相互关系可能很复杂。如需帮助，请联系 NetApp。

## StorageGRID 如何使用对象版本控制

如果要保留每个对象的多个版本，可以设置存储桶的版本控制状态。启用存储桶的版本控制可以帮助防止意外删除对象，并使您能够检索和还原对象的早期版本。

StorageGRID 系统实现了支持大多数功能的版本控制，但有一些限制。StorageGRID 最多支持每个对象的

10,000 个版本。

对象版本控制可以与 StorageGRID 信息生命周期管理 (ILM) 相结合，也可以与 S3 存储桶生命周期配置相结合。必须为每个存储桶显式启用版本控制。当对存储桶启用版本控制时，添加到存储桶的每个对象都会被分配一个版本 ID，该 ID 由 StorageGRID 系统生成。

不支持使用 MFA（多因素身份验证）删除。



只能在使用 StorageGRID 10.3 或更高版本创建的存储桶上启用版本控制。

## ILM 和版本控制

ILM 策略应用于对象的每个版本。ILM 扫描过程会持续扫描所有对象，并根据当前 ILM 策略对其进行重新评估。对 ILM 策略所做的任何更改都将应用于以前接收的所有对象。如果启用了版本控制，这包括先前接收的版本。ILM 扫描将新的 ILM 更改应用于先前接收的对象。

对于启用版本控制的存储桶中的 S3 对象，版本控制支持允许您创建使用“非当前时间”作为参考时间的 ILM 规则（对于“[创建 ILM 规则向导的步骤 1](#)”中的“仅将此规则应用于较旧的对象版本？”问题，请选择\*是\*）。更新对象时，其以前的版本将变为非当前版本。使用“非当前时间”筛选器允许您创建策略，以减少以前版本的对象对存储的影响。



使用多部分上传操作上传对象的新版本时，对象原始版本的非当前时间反映的是为新版本创建多部分上传的时间，而不是完成多部分上传的时间。在某些情况下，原始版本的非当前时间可能比当前版本早数小时或数天。

## 相关信息

- ["如何删除S3版本控制对象"](#)
- ["S3 版本化对象的 ILM 规则和策略（示例 4）"](#)。

## 使用 S3 REST API 配置 StorageGRID S3 对象锁定

如果为您的 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以创建启用 S3 对象锁定的存储桶。您可以为每个存储桶指定默认保留，或为每个对象版本指定保留设置。

### 如何为存储桶启用 S3 对象锁定

如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以选择在创建每个存储桶时启用 S3 对象锁定。

S3 Object Lock 是一个永久设置，只能在创建存储桶时启用。创建存储桶后，无法添加或禁用 S3 Object Lock。

要为存储桶启用 S3 Object Lock，请使用以下任一方法：

- 使用租户管理器创建存储桶。请参阅["创建 S3 存储桶"](#)。
- 使用带有 `x-amz-bucket-object-lock-enabled` 请求标头的 CreateBucket 请求创建存储桶。请参阅["\\${post\\_edited\\_translations.segment}"](#)。

S3 Object Lock 需要存储桶版本控制，在创建存储桶时自动启用。您不能暂停存储桶的版本控制。请参阅 ["对象版本控制"](#)。

## 存储桶的默认保留设置

当为存储桶启用 S3 Object Lock 时，您可以选择为存储桶启用默认保留，并指定默认保留模式和默认保留期限。

### 默认保留模式

- 在合规模式下：
  - 在达到其保留截止日期之前，无法删除此对象。
  - 对象的保留截止日期可以延长，但不能缩短。
  - 在达到该日期之前，无法删除对象的 retain-until-date。
- 在治理模式下：
  - 具有 `s3:BypassGovernanceRetention` 权限的用户可以使用 `x-amz-bypass-governance-retention: true` 请求标头绕过保留设置。
  - 这些用户可以在达到保留截止日期之前删除对象版本。
  - 这些用户可以增加、减少或删除对象的保留截止日期。

### 默认保留期限

每个存储桶可以具有以年或天为单位指定的默认保留期限。

### 如何设置存储区的默认保留时间

要设置存储区的默认保留，请使用以下任一方法：

- 从租户管理器管理存储桶设置。请参阅 "[\\${post\\_edited\\_translations.segment}](#)" 和 "[更新 S3 对象锁定默认保留](#)"。
- 向存储桶发出 PutObjectLockConfiguration 请求，以指定默认模式和默认天数或年数。

### PutObjectLockConfiguration

该 PutObjectLockConfiguration 请求允许您为启用了 S3 对象锁的存储桶设置和修改默认保留模式和默认保留期。您还可以删除以前配置的默认保留设置。

将新对象版本接收到存储桶时，如果未指定 x-amz-object-lock-mode 和 x-amz-object-lock-retain-until-date，则应用默认保留模式。如果未指定 x-amz-object-lock-retain-until-date，则使用默认保留期限来计算保留截止日期。

如果在摄取对象版本后修改了默认保留期限，则对象版本的 retain-until-date 保持不变，不会使用新的默认保留期限重新计算。

您必须具有 `s3:PutBucketObjectLockConfiguration` 权限，或者是 account root，才能完成此操作。

必须在 PUT 请求中指定 `Content-MD5` 请求标头。

### 请求示例

此示例为存储桶启用 S3 Object Lock，并将默认保留模式设置为 COMPLIANCE，将默认保留期限设置为 6 年。

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

## 如何确定存储桶的默认保留时间

要确定是否已为存储桶启用 S3 Object Lock 并查看默认保留模式和保留期限，请使用以下任一方法：

- 在租户管理器中查看存储桶。请参阅["查看 S3 存储桶"](#)。
- 发出 `GetObjectLockConfiguration` 请求。

### **GetObjectLockConfiguration**

该 `GetObjectLockConfiguration` 请求允许您确定是否已为存储桶启用 S3 对象锁定，如果已启用，请查看是否为该存储桶配置了默认保留模式和保留期。

将新对象版本载入存储桶时，如果未指定 `x-amz-object-lock-mode`，则应用默认保留模式。如果未指定 `x-amz-object-lock-retain-until-date`，则使用默认保留期限来计算保留截止日期。

您必须具有 `s3:GetBucketObjectLockConfiguration` 权限或是账户根用户，才能完成此操作。

### 请求示例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

## 响应示例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

## 如何指定对象的保留设置

启用了 S3 Object Lock 的存储桶可以包含具有和不具有 S3 Object Lock 保留设置的对象的组合。

对象级别保留设置使用 S3 REST API 指定。对象的保留设置将覆盖存储桶的任何默认保留设置。

可以为每个对象指定以下设置：

- **Retention mode:** COMPLIANCE 或 GOVERNANCE。
- **Retain-until-date:** 指定对象版本必须由 StorageGRID 保留多长时间的日期。
  - 在合规模式下，如果保留截止日期在未来，则可以检索对象，但不能对其进行修改或删除。保留截止日期可以延长，但不能缩短或删除。
  - 在 GOVERNANCE 模式下，具有特殊权限的用户可以绕过 retain-until-date 设置。他们可以在保留期结

束之前删除对象版本。他们还可以增加、减少甚至取消 retain-until-date。

- 法律冻结：对对象版本应用法律冻结会立即锁定该对象。例如，您可能需要与调查或法律纠纷相关的对象进行法律冻结。法律冻结没有到期日期，但在明确移除之前会一直存在。

对象的法律冻结设置与保留模式和保留截止日期无关。如果对象版本处于法定冻结状态，任何人都无法删除该版本。

要在将对象版本添加到存储桶时指定 S3 对象锁定设置，请发出 "放置对象"、"CopyObject" 或 "CreateMultipartUpload" 请求。

可以使用以下项：

- x-amz-object-lock-mode，可以是 COMPLIANCE 或 GOVERNANCE（区分大小写）。



如果指定 x-amz-object-lock-mode，则还必须指定 x-amz-object-lock-retain-until-date。

- x-amz-object-lock-retain-until-date
  - retain-until-date 值必须采用以下格式 2020-08-10T21:46:00Z。允许使用小数秒，但仅保留 3 位小数（精度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 保留截止日期必须在未来。
- x-amz-object-lock-legal-hold

如果法律保留已开启（区分大小写），则对象将被置于法律保留状态。如果法律保留已关闭，则不会进行法律保留。任何其他值都会导致 400 Bad Request (InvalidArgument) 错误。

如果使用以下任意请求标头，请留意以下限制：

- 如果在 PutObject 请求中存在任何 x-amz-object-lock-\* 请求标头，则必须提供 Content-MD5 请求标头。对于 CopyObject 或 CreateMultipartUpload，不需要 Content-MD5。
- 如果存储桶未启用 S3 Object Lock 且存在 `x-amz-object-lock-\*` 请求标头，则返回 400 Bad Request (InvalidRequest) 错误。
- PutObject 请求支持使用 `x-amz-storage-class: REDUCED\_REDUNDANCY` 来匹配 AWS 行为。但是，当对象被摄取到启用了 S3 对象锁定的存储桶中时，StorageGRID 将始终执行双提交摄取。
- 后续的 GET 或 HeadObject 版本响应将包括标头 x-amz-object-lock-mode、x-amz-object-lock-retain-until-date 和 x-amz-object-lock-legal-hold（如果已配置并且请求发送者具有正确的 `s3:Get\*` 权限）。

您可以使用 `s3:object-lock-remaining-retention-days` 策略条件键来限制对象的最短和最长允许保留期限。

## 如何更新对象的保留设置

如果需要更新现有对象版本的法律保留或保留设置，可以执行以下对象子资源操作：

- PutObjectLegalHold

如果新的法定冻结值为 ON，则该对象将被置于法定冻结状态。如果法定冻结值为 OFF，则解除法定冻结。

- PutObjectRetention
  - 模式值可以是 COMPLIANCE 或 GOVERNANCE（区分大小写）。
  - retain-until-date 值必须采用以下格式 2020-08-10T21:46:00Z。允许使用小数秒，但仅保留 3 位小数（精度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 如果对象版本具有现有的 retain-until-date，则只能增加它。新值必须是将来的日期。

## 如何使用 **GOVERNANCE** 模式

拥有 `s3:BypassGovernanceRetention` 权限的用户可以绕过使用治理模式的对象的活动保留设置。任何 DELETE 或 PutObjectRetention 操作都必须包含 `x-amz-bypass-governance-retention:true` 请求标头。这些用户可以执行以下附加操作：

- 执行 DeleteObject 或 DeleteObjects 操作以在对象版本的保留期结束之前将其删除。  
处于合法保留状态的对象无法删除。必须关闭合法保留。
- 在对象的保留期限到期之前，执行将对象版本的模式从 GOVERNANCE 更改为 COMPLIANCE 的 PutObjectRetention 操作。  
绝不允许将模式从 COMPLIANCE 更改为 GOVERNANCE。
- 执行 PutObjectRetention 操作以增加、减少或删除对象版本的保留期限。

## 相关信息

- ["使用 S3 Object Lock 管理对象"](#)
- ["使用 S3 Object Lock 保留对象"](#)
- ["Amazon Simple Storage Service 用户指南：锁定对象"](#)

## 了解 **StorageGRID** 的 **S3** 生命周期配置

您可以创建 S3 生命周期配置，以控制何时从 StorageGRID 系统中删除特定对象。

本节中的简单示例说明了 S3 生命周期配置如何控制从特定 S3 存储桶删除（过期）某些对象的时间。本节中的示例仅用于说明目的。有关创建 S3 生命周期配置的完整详细信息，请参阅 ["Amazon Simple Storage Service 用户指南：对象生命周期管理"](#)。请注意，StorageGRID 仅支持 Expiration 操作；不支持 Transition 操作。

## 什么是生命周期配置

生命周期配置是应用于特定 S3 存储桶中的对象的一组规则。每个规则都指定受影响的对象以及这些对象何时过期（在特定日期或若干天后）。

StorageGRID 在生命周期配置中最多支持 1,000 个生命周期规则。每个规则可以包含以下 XML 元素：

- 过期：当达到指定日期或从摄取对象时起达到指定天数时，删除对象。
- NoncurrentVersionExpiration：当对象变为非当前版本后，达到指定天数时删除该对象。
- 筛选（前缀、标签）
- 状态

- ID

每个对象都遵循 S3 存储桶生命周期或 ILM 策略的保留设置。配置 S3 存储桶生命周期后，生命周期到期操作将覆盖与存储桶生命周期筛选器匹配的对象 ILM 策略。与存储桶生命周期筛选器不匹配的对象使用 ILM 策略的保留设置。如果对象与存储桶生命周期筛选器匹配，并且未明确指定过期操作，则不会使用 ILM 策略的保留设置，这意味着对象版本将永久保留。请参阅 ["S3 存储桶生命周期和 ILM 策略的示例优先级"](#)。

因此，即使 ILM 规则中的放置指令仍然适用于对象，也可能从网格中删除对象。或者，即使在针对对象的任何 ILM 放置指令失效后，也可能会将对象保留在网格上。有关详细信息，请参阅 ["ILM 在对象整个生命周期中的运作方式"](#)。



Bucket 生命周期配置可用于已启用 S3 Object Lock 的 Bucket，但旧版兼容 Bucket 不支持 Bucket 生命周期配置。

StorageGRID 支持使用以下存储桶操作来管理生命周期配置：

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

### 创建生命周期配置

创建生命周期配置的第一步是创建包含一个或多个规则的 JSON 文件。例如，此 JSON 文件包括三个规则，如下所示：

1. 规则 1 仅适用于匹配前缀 `category1/` 且 `'key2'` 值为 `'tag2'` 的对象。该 `'Expiration'` 参数指定与筛选器匹配的对象将于 2020 年 8 月 22 日午夜到期。
2. 规则 2 仅适用于匹配前缀 `category2/` 的对象。该 `'Expiration'` 参数指定与筛选器匹配的对象将在摄入后 100 天过期。



指定天数的规则与摄取对象的时间有关。如果当前日期超过摄取日期加上天数，则某些对象可能会在应用生命周期配置后立即从存储桶中删除。

3. 规则 3 仅适用于与前缀 `category3/` 匹配的对象。该 `'Expiration'` 参数指定匹配对象的任何非当前版本将在其变为非当前版本后 50 天过期。

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

将生命周期配置应用于存储桶

创建生命周期配置文件后，您可以通过发出 `PutBucketLifecycleConfiguration` 请求将其应用到存储桶。

此请求将示例文件中的生命周期配置应用于名为 `testbucket` 的存储桶中的对象。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

要验证生命周期配置是否已成功应用于存储桶，请发出 `GetBucketLifecycleConfiguration` 请求。例如：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

成功的响应会列出您刚刚应用的生命周期配置。

验证存储桶生命周期过期是否适用于对象

您可以确定在发出 `PutObject`、`HeadObject` 或 `GetObject` 请求时，生命周期配置中的过期规则是否适用于特定对象。如果规则适用，则响应包含一个 `Expiration` 参数，该参数指示对象何时过期以及匹配了哪个过期规则。



由于存储桶生命周期会覆盖 ILM，因此 `expiry-date` 显示的是对象将被删除的实际日期。有关详细信息，请参见["如何确定对象保留"](#)。

例如，此 `PutObject` 请求于 2020 年 6 月 22 日发出，并将对象放入 `testbucket` 存储桶中。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功响应指示对象将在 100 天后（2020 年 10 月 1 日）过期，并且它与生命周期配置的规则 2 匹配。

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

例如，此 `HeadObject` 请求用于获取 `testbucket` 存储桶中相同对象的元数据。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功响应包括对象的元数据，并指示对象将在 100 天后过期，且与规则 2 匹配。

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



对于启用了版本控制的存储桶，`x-amz-expiration` 响应标头仅适用于当前版本的对象。

## 使用 StorageGRID 实施 S3 REST API 的建议

在实施与 StorageGRID 配合使用的 S3 REST API 时，应遵循以下建议。

### 针对不存在对象的 HEAD 建议

如果您的应用程序定期检查对象是否存在于您不希望对象实际存在的路径上，则应使用“可用”[一致性](#)。例如，如果您的应用程序在 PUT 某个位置之前对该位置执行 HEAD 操作，则应使用“可用”一致性。

否则，如果 HEAD 操作未找到对象，当同一站点上的两个或多个存储节点不可用或无法访问远程站点时，您可能会收到大量 500 内部服务器错误。

您可以使用[PUT Bucket 一致性](#)请求为每个存储桶设置“可用”一致性，也可以在单个 API 操作的请求标头中指定一致性。

### 对象键的建议

根据首次创建存储桶的时间，遵循以下有关对象键名称的建议。

#### 在 StorageGRID 11.4 或更早版本中创建的存储桶

- 请勿将随机值用作对象键的前四个字符。这与您之前 AWS 对密钥前缀的建议形成鲜明对比。而是使用非随机、非唯一的前缀，例如 `image`。
- 如果您确实遵循以前的 AWS 建议，在密钥前缀中使用随机和唯一字符，请使用目录名称作为对象密钥的前缀。也就是说，使用此格式：

```
mybucket/mydir/f8e3-image3132.jpg
```

代替此格式：

mybucket/f8e3-image3132.jpg

在 **StorageGRID 11.4** 或更高版本中创建的存储桶

不需要限制对象键名称以满足性能最佳实践。在大多数情况下，您可以为对象键名称的前四个字符使用随机值。



一个例外是 S3 工作负载在短时间内连续删除所有对象。为了最大限度地减少此用例的性能影响，请每隔几千个对象更改密钥名称的前导部分，例如日期。例如，假设 S3 客户端通常每秒写入 2,000 个对象，而 ILM 或存储桶生命周期策略会在三天后删除所有对象。为了最大限度地减少对性能的影响，您可以使用以下模式命名键：`/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

### "范围读取"的建议

如果启用了["用于压缩存储对象的全局选项"](#)，S3 客户端应用程序应避免执行指定返回字节范围的 `GetObject` 操作。这些"范围读取"操作效率低下，因为 StorageGRID 必须有效地解压缩对象才能访问所请求的字节。从非常大的对象请求小范围字节的 `GetObject` 操作效率尤其低下；例如，从 50 GB 压缩对象读取 10 MB 范围是低效的。

如果从压缩对象读取范围，则客户端请求可能会超时。



如果需要压缩对象，并且客户端应用程序必须使用范围读取，请增加应用程序的读取超时时间。

## 支持 Amazon S3 REST API

### StorageGRID 中 S3 REST API 支持的操作和限制

StorageGRID 系统实现了 Simple Storage Service API（API 版本 2006-03-01），支持大多数操作，但有一些限制。集成 S3 REST API 客户端应用程序时，需要了解实施细节。

StorageGRID 系统支持虚拟托管样式请求和路径样式请求。

### 日期处理

StorageGRID 的 S3 REST API 实施仅支持有效的 HTTP 日期格式。

StorageGRID 系统仅支持任何接受日期值的标头的有效 HTTP 日期格式。日期的时间部分可以用格林威治标准时间（GMT）格式指定，也可以用无时区偏移的通用协调时间（UTC）格式指定（必须指定 +0000）。如果在请求中包含 ``x-amz-date`` 标头，它将覆盖 Date 请求标头中指定的任何值。使用 AWS Signature Version 4 时，由于不支持日期标头，因此 ``x-amz-date`` 标头必须出现在已签名的请求中。

### 通用请求标头

StorageGRID 系统支持由 ["Amazon Simple Storage Service API Reference: 常见请求标头"](#) 定义的通用请求标头，但有一个例外。

|      |                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 请求标头 | 实施                                                                                                                                                                                                                                                                                                                                                                                                    |
| 授权   | <p>完全支持 AWS Signature Version 2</p> <p>支持 AWS Signature Version 4，但以下情况除外：</p> <ul style="list-style-type: none"> <li>当您在 <code>x-amz-content-sha256</code> 中提供实际的负载校验和值时，该值将被接受而不进行验证，就像为该标头提供了值 <code>UNSIGNED-PAYLOAD</code> 一样。当您提供 <code>x-amz-content-sha256</code> 标头值，而该值暗示进行 <code>aws-chunked</code> 流式传输时（例如 <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>），分块签名不会针对分块数据进行验证。</li> </ul> |

## 通用响应标头

StorageGRID 系统支持 *Simple Storage Service API Reference* 定义的所有常见响应标头，但有一个例外。

|                         |     |
|-------------------------|-----|
| 响应标头                    | 实施  |
| <code>x-amz-id-2</code> | 未使用 |

## StorageGRID S3 REST API 如何验证请求

StorageGRID 系统支持使用 S3 API 对对象进行身份验证访问和匿名访问。

S3 API 支持用于验证 S3 API 请求的签名版本 2 和签名版本 4。

经过身份验证的请求必须使用您的访问密钥 ID 和秘密访问密钥进行签名。

StorageGRID 系统支持两种身份验证方法：HTTP Authorization 标头和使用查询参数。

### 使用 HTTP Authorization 标头

HTTP ``Authorization`` 标头由所有 S3 API 操作使用，存储桶策略允许的匿名请求除外。``Authorization`` 标头包含对请求进行身份验证所需的所有签名信息。

### 使用查询参数

可以使用查询参数将身份验证信息添加到 URL。这称为对 URL 进行预签名，可用于授予对特定资源的临时访问权限。拥有预签名 URL 的用户无需知道访问资源所需的私有访问密钥，从而使您能够为第三方提供对资源的受限访问权限。

## StorageGRID 中支持的服务操作

StorageGRID 系统支持服务上的以下操作。

| 操作                                     | 实施                                                                                                                        |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ListBuckets<br><br>(先前命名为 GET Service) | 已使用所有 Amazon S3 REST API 行为实施。如有更改，恕不另行通知。                                                                                |
| 获取存储使用情况                               | StorageGRID <a href="#">"获取存储使用情况"</a> 请求会告诉您帐户使用的总存储量以及与帐户关联的每个存储桶的总存储量。这是对路径为 / 且已添加自定义查询参数 (?x-ntap-sg-usage 的服务执行的操作。 |
| OPTIONS /                              | 客户端应用程序可以向存储节点上的 S3 端口发出 `OPTIONS /` 请求，而无需提供 S3 身份验证凭据，以确定存储节点是否可用。您可以使用此请求进行监控，或允许外部负载均衡器识别存储节点何时关闭。                    |

## StorageGRID 中的 S3 存储桶操作和实施详细信息

StorageGRID 系统为每个 S3 租户帐户最多支持 5,000 个存储桶。

每个网格最多可包含 100,000 个存储桶。

要支持 5,000 个存储桶，网格中的每个存储节点必须至少有 64 GB RAM。

存储桶名称限制遵循 AWS US Standard 区域限制，但应进一步将其限制为 DNS 命名约定，以支持 S3 虚拟托管式请求。

有关详细信息，请参见以下内容：

- ["Amazon Simple Storage Service 用户指南：存储桶配额、限制和局限性"](#)
- ["配置 S3 端点域名"](#)

ListObjects (GET Bucket) 和 ListObjectVersions (GET Bucket object versions) 操作支持 StorageGRID ["一致性值"](#)。

您可以检查是否为单个存储桶启用或禁用了对上次访问时间的更新。请参阅 ["获取 Bucket 上次访问时间"](#)。

下表描述了 StorageGRID 如何实现 S3 REST API 存储桶操作。要执行任何这些操作，必须为帐户提供必要的访问凭据。

| 操作                      | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CreateBucket            | <p>创建一个新存储桶。通过创建存储桶，您将成为存储桶所有者。</p> <ul style="list-style-type: none"> <li>存储桶名称必须符合以下规则： <ul style="list-style-type: none"> <li>必须在每个 StorageGRID 系统中保持唯一性（不仅仅是在租户帐户中唯一）。</li> <li>必须符合 DNS 要求。</li> <li>必须至少包含 3 个且不超过 63 个字符。</li> <li>可以是一系列一个或多个标签，相邻标签由句点分隔。每个标签必须以小写字母或数字开头和结尾，并且只能使用小写字母、数字和连字符。</li> <li>不得看起来像文本格式的 IP 地址。</li> <li>不应在虚拟托管样式请求中使用句点。句点将导致服务器通配符证书验证出现问题。</li> </ul> </li> <li>默认情况下，存储区在 `us-east-1` 区域中创建；但是，您可以使用请求正文中的 `LocationConstraint` 请求元素指定不同的区域。使用 `LocationConstraint` 元素时，必须指定使用 Grid Manager 或 Grid Management API 定义的区域的确切名称。如果您不知道应使用的区域名称，请联系您的系统管理员。</li> </ul> <p>注意：如果您的 CreateBucket 请求使用了尚未在 StorageGRID 中定义的区域，则会发生错误。</p> <ul style="list-style-type: none"> <li>您可以包含 `x-amz-bucket-object-lock-enabled` 请求标头以创建启用了 S3 Object Lock 的存储桶。请参阅<a href="#">"使用 S3 REST API 配置 S3 对象锁定"</a>。</li> </ul> <p>创建存储桶时必须启用 S3 Object Lock。创建存储桶后，无法添加或禁用 S3 Object Lock。S3 Object Lock 需要存储桶版本控制，在创建存储桶时会自动启用。</p> |
| DeleteBucket            | 删除存储桶。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DeleteBucketCors        | 删除存储区的 CORS 配置。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DeleteBucketEncryption  | 从存储桶中删除默认加密。现有的加密对象保持加密状态，但添加到存储桶的任何新对象都不会被加密。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DeleteBucketLifecycle   | 从存储桶中删除生命周期配置。请参阅 <a href="#">"创建 S3 生命周期配置"</a> 。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| DeleteBucketPolicy      | 删除附加到存储区的策略。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DeleteBucketReplication | 删除附加到存储区的复制配置。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| 操作                                                                       | 实施                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DeleteBucketTagging                                                      | <p>使用 tagging 子资源从存储桶中删除所有标记。</p> <p>注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个分配了值的 NTAP-SG-ILM-BUCKET-TAG 存储桶标记。如果存在 NTAP-SG-ILM-BUCKET-TAG 存储桶标记，请勿发出 DeleteBucketTagging 请求。相反，仅使用 NTAP-SG-ILM-BUCKET-TAG 标记及其分配的值发出 PutBucketTagging 请求，以从存储桶中删除所有其他标记。请勿修改或删除 NTAP-SG-ILM-BUCKET-TAG 存储桶标记。</p> |
| GetBucketAcl                                                             | 返回肯定响应以及存储桶所有者的 ID、DisplayName 和权限，指示所有者对存储桶具有完全访问权限。                                                                                                                                                                                                                                       |
| GetBucketCors                                                            | 返回存储桶的 `cors` 配置。                                                                                                                                                                                                                                                                           |
| GetBucketEncryption                                                      | 返回存储区的默认加密配置。                                                                                                                                                                                                                                                                               |
| GetBucketLifecycleConfiguration<br><br>(先前命名为GET Bucket lifecycle)       | 返回存储桶的生命周期配置。请参阅 <a href="#">"创建 S3 生命周期配置"</a> 。                                                                                                                                                                                                                                           |
| GetBucketLocation                                                        | 返回使用 CreateBucket 请求中的 LocationConstraint 元素设置的区域。如果存储桶的区域为 `us-east-1`，则为该区域返回一个空字符串。                                                                                                                                                                                                      |
| GetBucketNotificationConfiguration<br><br>(先前命名为GET Bucket notification) | 返回附加到存储桶的通知配置。                                                                                                                                                                                                                                                                              |
| GetBucketPolicy                                                          | 返回附加到存储桶的策略。                                                                                                                                                                                                                                                                                |
| GetBucketReplication                                                     | 返回附加到存储区的复制配置。                                                                                                                                                                                                                                                                              |
| GetBucketTagging                                                         | <p>使用 tagging 子资源返回存储桶的所有标记。</p> <p>注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个 `NTAP-SG-ILM-BUCKET-TAG` 存储桶标记，并为其分配了值。请勿修改或删除此标签。</p>                                                                                                                                                                 |
| GetBucketVersioning                                                      | <p>此实现使用 versioning 子资源返回存储桶的版本控制状态。</p> <ul style="list-style-type: none"> <li>• <i>blank</i>：从未启用过版本控制（存储桶为"未版本控制"）</li> <li>• Enabled：已启用版本控制</li> <li>• 已挂起：版本控制之前已启用，现已挂起</li> </ul>                                                                                                   |

| 操作                                                           | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GetObjectLockConfiguration                                   | <p>返回存储区默认保留模式和默认保留期限（如果已配置）。</p> <p>请参阅 <a href="#">"使用 S3 REST API 配置 S3 对象锁定"</a>。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| HeadBucket                                                   | <p>确定存储桶是否存在，以及您是否有权访问它。</p> <p>此操作将返回：</p> <ul style="list-style-type: none"> <li>• x-ntap-sg-bucket-id: UUID 格式的存储桶 UUID。</li> <li>• x-ntap-sg-trace-id: 关联请求的唯一跟踪 ID。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ListObjects 和<br>ListObjectsV2<br><br>(先前命名为 GET Bucket )    | <p>返回存储桶中的部分或全部（最多 1,000 个）对象。对象的存储类可以具有两个值之一，即使对象是使用 `REDUCED_REDUNDANCY` 存储类选项接收的：</p> <ul style="list-style-type: none"> <li>• STANDARD，表示对象存储在由存储节点组成的存储池中。</li> <li>• GLACIER，指示对象已移动到 Cloud Storage Pool 指定的外部存储区。</li> </ul> <p>如果存储桶包含大量具有相同前缀的已删除密钥，则响应可能包含一些 `CommonPrefixes` 不包含密钥的内容。</p> <p>对于 HeadObject 和 ListObject 请求，StorageGRID 以不同的精度返回 LastModified 时间戳，而 AWS 以相同的精度返回时间戳，如下列示例所示：</p> <ul style="list-style-type: none"> <li>• StorageGRID HeadObject: "LastModified": "2024-09-26T16:43:24+00:00"</li> <li>• StorageGRID ListObject: "LastModified": "2024-09-26T16:43:24.931000+00:00"</li> <li>• AWS HeadObject: "LastModified": "2023-10-17T00:19:54+00:00"</li> <li>• AWS ListObject: "LastModified": "2023-10-17T00:19:54+00:00"</li> </ul> |
| ListObjectVersions<br><br>(先前命名为 GET Bucket Object versions) | <p>在存储桶上具有读取权限时，将此操作与 `versions` 子资源一起使用会列出存储桶中对象的所有版本的元数据。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| PutBucketCors                                                | <p>设置存储桶的 CORS 配置，以便存储桶可以为跨源请求提供服务。跨域资源共享 (CORS) 是一种安全机制，允许一个域中的客户端 Web 应用程序访问不同域中的资源。例如，假设您使用名为 `images` 的 S3 存储桶来存储图形。通过设置 `images` 存储桶的 CORS 配置，您可以允许该存储桶中的图像显示在网站 `http://www.example.com` 上。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| 操作                                                                 | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PutBucketEncryption                                                | <p>设置现有存储桶的默认加密状态。启用存储桶级加密后，添加到存储桶的任何新对象都将被加密。StorageGRID 支持使用 StorageGRID 管理的密钥进行服务器端加密。指定服务器端加密配置规则时，请将 SSEAlgorithm 参数设置为 `AES256`，不要使用 `KMSMasterKeyID` 参数。</p> <p>如果对象上传请求已指定加密（即，如果请求包括 `x-amz-server-side-encryption-*` 请求标头），则会忽略存储桶默认加密配置。</p>                                                                                                                                                                                                                                                                                                                                                                                 |
| PutBucketLifecycleConfiguration<br><br>(先前命名为PUT Bucket lifecycle) | <p>为存储桶创建新的生命周期配置或替换现有的生命周期配置。StorageGRID 在生命周期配置中最多支持 1,000 条生命周期规则。每条规则可以包含以下 XML 元素：</p> <ul style="list-style-type: none"> <li>• 过期（天数、日期、ExpiredObjectDeleteMarker）</li> <li>• NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays)</li> <li>• 筛选（前缀、标签）</li> <li>• 状态</li> <li>• ID</li> </ul> <p>StorageGRID 不支持以下操作：</p> <ul style="list-style-type: none"> <li>• AbortIncompleteMultipartUpload</li> <li>• 过渡</li> </ul> <p>请参见<a href="#">"创建 S3 生命周期配置"</a>。要了解存储桶生命周期中的过期操作如何与 ILM 放置说明交互，请参见<a href="#">"ILM在对象整个生命周期中的运作方式"</a>。</p> <p>注意：存储桶生命周期配置可用于启用了 S3 Object Lock 的存储桶，但旧版合规存储桶不支持存储桶生命周期配置。</p> |

| 操作                                                                        | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PutBucketNotificationConfiguration<br><br>(先前命名的 PUT Bucket notification) | <p>使用请求正文中包含的通知配置 XML 配置存储区的通知。您应了解以下实施细节：</p> <ul style="list-style-type: none"> <li>StorageGRID 支持 Amazon Simple Notification Service (Amazon SNS) 主题、Kafka 主题或 webhook 端点作为目标。不支持 Simple Queue Service (SQS) 或 AWS Lambda 端点。</li> <li>通知的目标必须指定为 StorageGRID 端点的 URN。可以使用 Tenant Manager 或租户管理 API 创建端点。</li> </ul> <p>此终结点必须存在，通知配置才能成功。如果端点不存在，则会返回 400 Bad Request 错误，错误代码为 InvalidArgument。</p> <ul style="list-style-type: none"> <li>无法为以下事件类型配置通知。这些事件类型*不*受支持。 <ul style="list-style-type: none"> <li>s3:ReducedRedundancyLostObject</li> <li>s3:ObjectRestore:Completed</li> </ul> </li> <li>从 StorageGRID 发送的事件通知使用标准 JSON 格式，但不包含某些键，并为其他键使用特定值，如以下列表所示： <ul style="list-style-type: none"> <li><b>eventSource</b><br/>sgws:s3</li> <li><b>awsRegion</b><br/>不包括在内</li> <li><b>x-amz-id-2</b><br/>不包括在内</li> <li><b>arn</b><br/>urn:sgws:s3:::bucket_name</li> </ul> </li> </ul> |
| PutBucketPolicy                                                           | 设置附加到存储桶的策略。请参阅 <a href="#">"使用存储区和组访问策略"</a> 。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| 操作                   | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PutBucketReplication | <p>使用请求正文中提供的复制配置 XML 为存储桶配置 <a href="#">"StorageGRID CloudMirror 复制"</a>。对于 CloudMirror 复制，您应该了解以下实施详情：</p> <ul style="list-style-type: none"> <li>StorageGRID 仅支持复制配置的 V1。这意味着 StorageGRID 不支持对规则使用 <code>`Filter`</code> 元素，并遵循 V1 约定删除对象版本。有关详细信息，请参见 <a href="#">"Amazon Simple Storage Service 用户指南：复制配置"</a>。</li> <li>可以在版本化或未版本化的存储桶上配置存储桶复制。</li> <li>您可以在复制配置 XML 的每个规则中指定不同的目标存储桶。源存储桶可以复制到多个目标存储桶。</li> <li>目标存储桶必须指定为租户管理器或租户管理 API 中指定的 StorageGRID 终结点的 URN。请参阅 <a href="#">"配置 CloudMirror 复制"</a>。</li> </ul> <p>必须存在端点，复制配置才能成功。如果端点不存在，则请求将作为 400 Bad Request 失败。此错误消息指出： <code>`Unable to save the replication policy. The specified endpoint URN does not exist: URN.`</code></p> <ul style="list-style-type: none"> <li>您无需在配置 XML 中指定 Role。StorageGRID 不使用此值，如果提交将被忽略。</li> <li>如果在配置 XML 中省略存储类，StorageGRID 默认使用 <code>`STANDARD`</code> 存储类。</li> <li>如果从源存储桶中删除对象或删除源存储桶本身，则跨区域复制行为如下： <ul style="list-style-type: none"> <li>如果在对象或存储桶进行复制之前将其删除，则不会复制对象/存储桶，并且不会通知您。</li> <li>如果在对象或存储桶进行复制后将其删除，StorageGRID 遵循跨区域复制 V1 的标准 Amazon S3 删除行为。</li> </ul> </li> </ul> |
| PutBucketTagging     | <p>使用 <code>`tagging`</code> 子资源为存储桶添加或更新一组标记。添加存储桶标签时，请注意以下限制：</p> <ul style="list-style-type: none"> <li>StorageGRID 和 Amazon S3 支持每个存储桶最多 50 个标记。</li> <li>与存储桶关联的标签必须具有唯一的标签键。标签键的长度最多为 128 个 Unicode 字符。</li> <li>标记值的长度不得超过 256 个 Unicode 字符。</li> <li>键和值区分大小写。</li> </ul> <p>注意：如果为此存储桶设置了非默认 ILM 策略标记，则将存在一个 <code>`NTAP-SG-ILM-BUCKET-TAG`</code> 存储桶标记，并为其分配了值。确保在所有 PutBucketTagging 请求中包含带有分配值的 <code>`NTAP-SG-ILM-BUCKET-TAG`</code> 存储桶标记。请勿修改或删除此标记。</p> <p>注意：此操作将覆盖存储桶已有的任何当前标记。如果从集合中省略了任何现有标记，则这些标记将从存储桶中删除。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| 操作                         | 实施                                                                                                                                                                                                                                                               |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PutBucketVersioning        | <p>使用 <code>versioning</code> 子资源设置现有存储桶的版本控制状态。可以使用以下值之一设置版本控制状态：</p> <ul style="list-style-type: none"><li>• <b>Enabled</b>：为存储桶中的对象启用版本控制。添加到存储桶的所有对象都会收到唯一的版本 ID。</li><li>• <b>Suspended</b>：禁用存储桶中对象的版本控制。添加到存储桶的所有对象都会收到版本 ID <code>null</code>。</li></ul> |
| PutObjectLockConfiguration | <p>配置或删除存储桶默认保留模式和默认保留期限。</p> <p>如果修改了默认保留期限，则现有对象版本的 <code>retain-until-date</code> 保持不变，并且不会使用新的默认保留期限重新计算。</p> <p>有关详细信息，请参见 <a href="#">"使用 S3 REST API 配置 S3 对象锁定"</a>。</p>                                                                                 |

## 对象上的操作

### StorageGRID 如何实现对象的 S3 REST API 操作

本节介绍 StorageGRID 系统如何实现对象的 S3 REST API 操作。

以下条件适用于所有对象操作：

- StorageGRID ["一致性值"](#) 受所有对象操作的支持，以下情况除外：
  - `GetObjectAcl`
  - `OPTIONS /`
  - `PutObjectLegalHold`
  - `PutObjectRetention`
  - `SelectObjectContent`
- 冲突的客户端请求（例如两个客户端向同一密钥写入）将以"最新获胜"为原则进行解决。"最新获胜"评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。
- StorageGRID 存储桶中的所有对象都归存储桶所有者所有，包括由匿名用户或其他帐户创建的对象。

下表介绍了 StorageGRID 如何实现 S3 REST API 对象操作。

| 操作                                                   | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 删除对象                                                 | <p>在处理 DeleteObject 请求时，StorageGRID 尝试立即从所有存储位置删除对象的所有副本。如果成功，StorageGRID 会立即向客户端返回响应。如果无法在 30 秒内删除所有副本（例如，由于某个位置暂时不可用），StorageGRID 会将这些副本排队等待删除，然后向客户端指示成功。</p> <p>限制</p> <ul style="list-style-type: none"> <li>不支持多因素身份验证 (MFA) 和响应标头 x-amz-mfa。</li> <li>If-None 和 If-None-Match 标头可接受，但无效。</li> </ul> <p>版本控制</p> <p>要删除特定版本，请求者必须是存储桶所有者并使用 versionId`子资源。使用此子资源将永久删除该版本。如果 `versionId` 对应于删除标记，则响应标头 `x-amz-delete-marker` 将返回并设置为 `true`。</p> <ul style="list-style-type: none"> <li>如果在启用了版本控制的存储桶上删除对象时未使用 versionId`子资源，则会生成删除标记。删除标记的 `versionId` 通过 `x-amz-version-id` 响应标头返回，`x-amz-delete-marker` 响应标头返回值设置为 `true`。</li> <li>如果在版本控制已暂停的存储桶上删除对象时未指定 versionId`子资源，则会导致永久删除已存在的"null"版本或"null"删除标记，并生成新的"null"删除标记。返回的 `x-amz-delete-marker` 响应标头设置为 `true`。</li> </ul> <p>注意：在某些情况下，一个对象可能存在多个删除标记。</p> <p>请参见<a href="#">"使用 S3 REST API 配置 S3 对象锁定"</a>以了解如何在 GOVERNANCE 模式下删除对象版本。</p> |
| DeleteObjects<br><br>(先前命名为 DELETE Multiple Objects) | <p>不支持多因素身份验证 (MFA) 和响应标头 x-amz-mfa。</p> <p>可以在同一请求消息中删除多个对象。</p> <p>请参见<a href="#">"使用 S3 REST API 配置 S3 对象锁定"</a>以了解如何在 GOVERNANCE 模式下删除对象版本。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DeleteObjectTagging                                  | <p>使用 tagging 子资源从对象中删除所有标记。</p> <p>版本控制</p> <p>如果请求中未指定 versionId`查询参数，则操作会从版本化存储桶中的对象的最新版本中删除所有标记。如果对象的当前版本是删除标记，则返回"MethodNotAllowed"状态，并将 `x-amz-delete-marker` 响应标头设置为 `true`。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 获取对象                                                 | <a href="#">"获取对象"</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| 操作                                     | 实施                                                                                                                                                                                   |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GetObjectAcl                           | 如果为帐户提供了必要的访问凭据，则该操作将返回肯定响应以及对象所有者的 ID、DisplayName 和权限，表明所有者对该对象具有完全访问权限。                                                                                                            |
| GetObjectLegalHold                     | "使用 S3 REST API 配置 S3 对象锁定"                                                                                                                                                          |
| GetObjectRetention                     | "使用 S3 REST API 配置 S3 对象锁定"                                                                                                                                                          |
| GetObjectTagging                       | <p>使用 tagging 子资源返回对象的所有标记。</p> <p>版本控制</p> <p>如果请求中未指定 versionId 查询参数，则操作将返回版本化存储桶中对象的最新版本的所有标记。如果对象的当前版本是删除标记，则返回"MethodNotAllowed"状态，并将 `x-amz-delete-marker` 响应标头设置为 `true`。</p> |
| HeadObject                             | "HeadObject"                                                                                                                                                                         |
| RestoreObject                          | "RestoreObject"                                                                                                                                                                      |
| 放置对象                                   | "放置对象"                                                                                                                                                                               |
| CopyObject<br>(以前称为 PUT Object - Copy) | "CopyObject"                                                                                                                                                                         |
| PutObjectLegalHold                     | "使用 S3 REST API 配置 S3 对象锁定"                                                                                                                                                          |
| PutObjectRetention                     | "使用 S3 REST API 配置 S3 对象锁定"                                                                                                                                                          |

| 操作                  | 实施                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PutObjectTagging    | <p>使用 tagging 子资源向现有对象添加一组标记。</p> <p><b>对象标记限制</b></p> <p>您可以在上传新对象时向其添加标签，也可以将其添加到现有对象。StorageGRID 和 Amazon S3 都支持每个对象最多 10 个标记。与对象关联的标签必须具有唯一的标签键。标记键的长度最多可为 128 个 Unicode 字符，标记值最多可为 256 个 Unicode 字符。键和值区分大小写。</p> <p><b>标签更新和摄取行为</b></p> <p>当您使用 PutObjectTagging 更新对象的标签时，StorageGRID 不会重新摄取该对象。这意味着系统不会使用匹配的 ILM 规则中指定的“Ingest Behavior”选项。由更新触发的对象位置的任何更改都会在正常的后台 ILM 进程重新评估 ILM 时进行。</p> <p>这意味着，如果 ILM 规则使用“严格”选项进行载入行为，则在无法进行所需的对象放置时（例如，因为新要求的位置不可用），不会采取任何措施。更新的对象将保留其当前位置，直到可以进行所需的放置为止。</p> <p><b>解决冲突</b></p> <p>冲突的客户端请求（例如两个客户端向同一密钥写入）将以“最新获胜”为原则进行解决。“最新获胜”评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。</p> <p><b>版本控制</b></p> <p>如果请求中未指定 versionId 查询参数，则操作会将标记添加到版本化存储区中对象的最新版本。如果对象的当前版本是删除标记，则返回“MethodNotAllowed”状态，并将 `x-amz-delete-marker` 响应标头设置为 `true`。</p> |
| SelectObjectContent | "SelectObjectContent"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## StorageGRID 中支持的 Amazon S3 Select 操作

StorageGRID 支持以下 Amazon S3 Select 子句、数据类型和运算符，适用于 ["SelectObjectContent 命令"](#)。



不支持未列出的任何项目。

有关语法，请参见["SelectObjectContent"](#)。有关 S3 Select 的详细信息，请参见 ["适用于 S3 Select 的 AWS 文档"](#)。

只有启用了 S3 Select 的租户帐户才能发出 SelectObjectContent 查询。请参见 ["使用 S3 Select 的注意事项和要求"](#)。

## 条款

- SELECT 列表
- FROM子句
- WHERE子句
- LIMIT子句

## 数据类型

- 布尔值
- 整数
- string
- 浮点型
- decimal, numeric
- 时间戳

## 运算符

### 逻辑运算符

- 与
- 未
- 或

### 比较运算符

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- 介于
- IN

### 模式匹配运算符

- LIKE
- \_
- %

## 单元运算符

- IS NULL
- IS NOT NULL

## 数学运算符

- +
- -
- \*
- /
- %

StorageGRID 遵循 Amazon S3 Select 运算符优先级。

## 聚合函数

- AVG()
- COUNT(\*)
- MAX()
- MIN()
- SUM()

## 条件函数

- 案例
- COALESCE
- NULLIF

## 转换函数

- CAST（用于受支持的数据类型）

## 日期函数

- DATE\_ADD
- DATE\_DIFF
- EXTRACT
- TO\_STRING
- TO\_TIMESTAMP
- UTCNOW

## 字符串函数

- CHAR\_LENGTH, CHARACTER\_LENGTH
- 较低

- SUBSTRING
- TRIM
- 上限

**StorageGRID 如何使用服务器端加密**

服务器端加密允许您保护静态的对象数据。StorageGRID 在写入对象时对数据进行加密，并在访问对象时对数据进行解密。

如果要使用服务器端加密，可以根据加密密钥的管理方式选择两个互斥选项之一：

- **SSE**（使用 **StorageGRID** 管理的密钥的服务器端加密）：当您发出存储对象的 S3 请求时，StorageGRID 会使用唯一密钥加密对象。当您发出 S3 请求以检索对象时，StorageGRID 使用存储的密钥来解密对象。
- **SSE-C**（使用客户提供的密钥进行服务器端加密）：当您发出存储对象的 S3 请求时，您需要提供自己的加密密钥。检索对象时，您需要在请求中提供相同的加密密钥。如果两个加密密钥匹配，则会解密对象并返回您的对象数据。

StorageGRID 负责管理所有对象加密和解密操作，而您必须管理您提供的加密密钥。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。



如果对象使用 SSE 或 SSE-C 加密，则将忽略任何存储桶级或网格级加密设置。

**使用 SSE**

要使用由 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下请求标头：

`x-amz-server-side-encryption`

以下对象操作支持 SSE 请求标头：

- "放置对象"
- "CopyObject"
- "CreateMultipartUpload"

**使用 SSE-C**

要使用您管理的唯一密钥加密对象，请使用三个请求标头：

| 请求标头                                                         | 问题描述                                       |
|--------------------------------------------------------------|--------------------------------------------|
| <code>x-amz-server-side-encryption-customer-algorithm</code> | 指定加密算法。标头值必须为 AES256。                      |
| <code>x-amz-server-side-encryption-customer-key</code>       | 指定将用于加密或解密对象的加密密钥。密钥的值必须为 256 位，base64 编码。 |

| 请求标头                                          | 问题描述                                                                  |
|-----------------------------------------------|-----------------------------------------------------------------------|
| x-amz-server-side-encryption-customer-key-MD5 | 根据 RFC 1321 指定加密密钥的 MD5 摘要，用于确保加密密钥传输无误。MD5 摘要的值必须是 base64 编码的 128 位。 |

以下对象操作支持 SSE-C 请求标头：

- "获取对象"
- "HeadObject"
- "放置对象"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

使用客户提供的密钥（**SSE-C**）的服务器端加密的注意事项

在使用 SSE-C 之前，请注意以下注意事项：

- 您必须使用https。



使用 SSE-C 时，StorageGRID 会拒绝通过 http 发出的任何请求。出于安全考虑，您应将意外通过 http 发送的任何密钥视为已泄露。请丢弃该密钥，并根据需要进行轮换。

- 响应中的 ETag 不是对象数据的 MD5。
- 您必须管理加密密钥到对象的映射。StorageGRID 不存储加密密钥。您有责任跟踪为每个对象提供的加密密钥。
- 如果您的存储桶已启用版本控制，则每个对象版本都应有自己的加密密钥。您有责任跟踪用于每个对象版本的加密密钥。
- 由于您在客户端管理加密密钥，因此您还必须在客户端管理任何其他保护措施，例如密钥轮换。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。

- 如果为存储桶配置了跨网格复制或 CloudMirror 复制，则无法载入 SSE-C 对象。载入操作将失败。

相关信息

["Amazon S3 用户指南：使用客户提供的密钥（SSE-C）进行服务器端加密"](#)

使用 **S3 CopyObject** 请求在 **StorageGRID** 中创建对象副本

您可以使用 S3 CopyObject 请求创建已存储在 S3 中的对象的副本。CopyObject 操作与依次执行 GetObject 和 PutObject 相同。

## 解决冲突

冲突的客户端请求（例如两个客户端向同一密钥写入）将以“最新获胜”为原则进行解决。“最新获胜”评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

## 对象大小

单次 PutObject 操作的最大\_推荐\_大小为 5 GiB（5,368,709,120 字节）。如果您的对象大于 5 GiB，请改用 ["多部件上传"](#)。

单次 PutObject 操作的最大\_支持\_大小为 5 TiB（5,497,558,138,880 字节）。



如果您从 StorageGRID 11.6 或更早版本升级，则在尝试上传超过 5 GiB 的对象时，将触发 S3 PUT Object size too large 警报。如果您新安装了 StorageGRID 11.7 或 11.8，则在此情况下不会触发警报。但是，为了与 AWS S3 标准保持一致，未来版本的 StorageGRID 将不支持上传大于 5 GiB 的对象。

## 用户元数据中的 UTF-8 字符

如果请求在用户定义元数据的键名或值中包含（未转义的）UTF-8 值，则 StorageGRID 行为未定义。

StorageGRID 不解析或解释用户定义元数据的键名或值中包含的转义的 UTF-8 字符。转义的 UTF-8 字符被视为 ASCII 字符：

- 如果用户定义的元数据包含转义的 UTF-8 字符，则请求成功。
- 如果键名或键值的解释值包含不可打印的字符，StorageGRID 不会返回 `x-amz-missing-meta` 标头。

## 支持的请求标头

支持以下请求标头：

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-，后跟包含用户定义元数据的名称-值对
- x-amz-metadata-directive：默认值为 COPY，可让您复制对象和相关的元数据。

您可以指定 `REPLACE` 在复制对象时覆盖现有元数据，或更新对象元数据。

- x-amz-storage-class
- x-amz-tagging-directive：默认值为 COPY，可让您复制对象和所有标记。

您可以指定 `REPLACE` 在复制对象时覆盖现有标记，或更新标记。

- S3 Object Lock 请求标头:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

如果在没有这些标头的情况下发出请求,则会使用存储桶默认保留设置来计算对象版本模式和 retain-until-date。请参阅 ["使用 S3 REST API 配置 S3 对象锁定"](#)。

- SSE 请求标头:

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

请参阅 [\[服务器端加密的请求标头\]](#)

不支持的请求标头

不支持以下请求标头:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

`If-Match header` 是可以接受的,但不起作用。

- If-None-Match

`If-None-Match header` 是可以接受的,但不起作用。

- x-amz-checksum-algorithm

复制对象时,如果源对象具有校验和,则 StorageGRID 不会将该校验和值复制到新对象。无论您是否尝试在对象请求中使用 x-amz-checksum-algorithm,此行为均适用。

- `x-amz-website-redirect-location`

## 存储类选项

支持 ``x-amz-storage-class`` 请求标头，如果匹配的 ILM 规则使用 Dual commit 或 Balanced "载入选项"，则会影响 StorageGRID 创建的对象副本数。

- STANDARD

(默认值) 当 ILM 规则使用双提交选项时，或当平衡选项回退到创建临时副本时，指定双提交接收操作。

- REDUCED\_REDUNDANCY

当 ILM 规则使用双提交选项，或当平衡选项回退到创建临时副本时，指定单提交接收操作。



如果要将对对象接收到启用了 S3 对象锁定的存储桶中，则该 ``REDUCED_REDUNDANCY`` 选项将被忽略。如果要将对对象摄入旧版合规存储桶，则该 ``REDUCED_REDUNDANCY`` 选项将返回错误。StorageGRID 将始终执行双提交摄取，以确保满足合规性要求。

## 将 `x-amz-copy-source` 用于 CopyObject

如果 ``x-amz-copy-source`` 标头中指定的源存储桶和密钥与目标存储桶和密钥不同，则会将源对象数据的副本写入目标。

如果源和目标匹配，并且 `x-amz-metadata-directive`` 标头指定为 ``REPLACE``，则会使用请求中提供的元数据值更新对象的元数据。在此情况下，StorageGRID 不会重新载入对象。这有两个重要后果：

- 您不能使用 CopyObject 对现有对象进行就地加密，也不能更改现有对象的就地加密。如果提供 `x-amz-server-side-encryption`` 标头或 ``x-amz-server-side-encryption-customer-algorithm`` 标头，StorageGRID 将拒绝请求并返回 ``XNotImplemented``。
- 不使用匹配的 ILM 规则中指定的 Ingest Behavior 选项。当正常后台 ILM 流程重新评估 ILM 时，将对更新触发的对象放置进行任何更改。

这意味着，如果 ILM 规则使用"严格"选项进行载入行为，则在无法进行所需的对象放置时（例如，因为新要求的位置不可用），不会采取任何措施。更新的对象将保留其当前位置，直到可以进行所需的放置为止。

## 服务器端加密的请求标头

如果您"使用服务器端加密"，则提供的请求标头取决于源对象是否已加密以及是否计划加密目标对象。

- 如果使用客户提供的密钥(SSE-C)加密源对象，则必须在 CopyObject 请求中包含以下三个标头，以便可以解密然后复制对象：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm``：指定 AES256。
  - `x-amz-copy-source-server-side-encryption-customer-key``：指定创建源对象时提供的加密密钥。
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5``：指定创建源对象时提供的 MD5 摘要。
- 如果要使用您提供和管理的唯一密钥加密目标对象（副本），请包括以下三个标头：

- `x-amz-server-side-encryption-customer-algorithm`: 指定 AES256。
- `x-amz-server-side-encryption-customer-key`: 为目标对象指定新的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`: 指定新加密密钥的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["使用服务器端加密"](#) 的注意事项。

- 如果要使用由 StorageGRID 管理的唯一密钥（SSE）对目标对象（副本）进行加密，请在 CopyObject 请求中包含此标头：

- `x-amz-server-side-encryption`



该对象的 `server-side-encryption` 值无法更新。请改为使用 `x-amz-metadata-directive: REPLACE` 制作具有新 `server-side-encryption` 值的副本。

## 版本控制

如果源存储桶已进行版本控制，则可以使用 `x-amz-copy-source` 标头复制对象的最新版本。若要复制对象的特定版本，必须使用 `versionId` 子资源显式指定要复制的版本。如果对目标存储桶进行了版本控制，则在 `x-amz-version-id` 响应标头中返回生成的版本。如果暂停目标存储桶的版本控制，则 `x-amz-version-id` 返回 "null" 值。

使用 **GetObject** 请求从 **StorageGRID** 中的存储桶检索对象

您可以使用 S3 GetObject 请求从 S3 存储桶检索对象。

## GetObject 和多部件对象

您可以使用 `partNumber` 请求参数检索多部分或分段对象的特定部分。`x-amz-mp-parts-count` 响应元素指示对象有多少个部分。

您可以将 `partNumber` 设置为 1，适用于分段/多部分对象和非分段/非多部分对象；但是，`x-amz-mp-parts-count` 响应元素仅针对分段或多部分对象返回。

## 用户元数据中的 UTF-8 字符

StorageGRID 不解析或解释用户定义元数据中转义的 UTF-8 字符。如果键名称或值包含不可打印的字符，则用户定义的元数据中具有转义 UTF-8 字符的对象的 GET 请求不会返回 `x-amz-missing-meta` 标头。

## 支持的请求标头

支持以下请求标头：

- `x-amz-checksum-mode`: 指定 ENABLED

`Range` 标头不支持与 `x-amz-checksum-mode` 一起用于 GetObject。当您在请求中包含 `Range` 且启用了 `x-amz-checksum-mode` 时，StorageGRID 不会在响应中返回校验和值。

不支持的请求标头

不支持以下请求标头，返回 `XNotImplemented`:

- `x-amz-website-redirect-location`

版本控制

如果未指定 `versionId` 子资源，则该操作将获取版本化存储区中对象的最新版本。如果对象的当前版本是删除标记，则会返回 `"Not Found"` 状态，并将 ``x-amz-delete-marker`` 响应标头设置为 ``true``。

使用客户提供的加密密钥 (**SSE-C**) 进行服务器端加密的请求标头

如果对象使用您提供的唯一密钥加密，请使用所有三个标头。

- `x-amz-server-side-encryption-customer-algorithm`: 指定 AES256。
- `x-amz-server-side-encryption-customer-key`: 指定对象的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`: 指定对象加密密钥的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["\\${post\\_edited\\_translations.segment}"](#) 中的注意事项。

GetObject 对 Cloud Storage Pool 对象的行为

如果对象已存储在 ["云存储池"](#) 中，则 `GetObject` 请求的行为取决于对象的状态。有关更多详细信息，请参见 ["HeadObject"](#)。



如果对象存储在云存储池中，并且该对象的一个或多个副本也存在于网络上，则 `GetObject` 请求将尝试从网络检索数据，然后再从云存储池检索数据。

| 对象的状态                                               | GetObject 的行为                                                                              |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------|
| 已载入 StorageGRID 但尚未经过 ILM 评估的对象，或存储在传统存储池中或使用纠删码的对象 | 200 OK<br><br>检索到对象的副本。                                                                    |
| 云存储池中的对象，但尚未转换到不可检索的状态                              | 200 OK<br><br>检索到对象的副本。                                                                    |
| 对象已转换为不可检索状态                                        | 403 Forbidden, InvalidObjectState<br><br>使用 <a href="#">"RestoreObject"</a> 请求将对象还原到可检索状态。 |
| 正在从不可检索状态还原的对象                                      | 403 Forbidden, InvalidObjectState<br><br>等待 <code>RestoreObject</code> 请求完成。               |

| 对象的状态        | GetObject 的行为           |
|--------------|-------------------------|
| 对象已完全还原到云存储池 | 200 OK<br><br>检索到对象的副本。 |

### 云存储池中的多部分或分段对象

如果您上传了多部分对象，或者 StorageGRID 将大型对象拆分为多个分段，StorageGRID 将通过对对象的部分或分段进行采样来确定该对象在云存储池中是否可用。在某些情况下，当对象的某些部分已转换为不可检索状态或对象的某些部分尚未还原时，GetObject 请求可能会错误地返回 200 OK。

在这些情况下：

- GetObject 请求可能会返回一些数据，但在传输过程中停止。
- 后续 GetObject 请求可能会返回 403 Forbidden。

### GetObject 和跨网格复制

如果您正在使用“[网格联盟](#)”并且为存储桶启用了“[跨网格复制](#)”，则 S3 客户端可以通过发出 GetObject 请求来验证对象的复制状态。响应包括 StorageGRID 特定的 `x-ntap-sg-cgr-replication-status` 响应标头，该标头将采用以下其中一个值：

| Grid | 复制状态                                                                                                                                                           |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 源    | <ul style="list-style-type: none"> <li>• <b>COMPLETED</b>：复制成功。</li> <li>• <b>PENDING</b>：对象尚未复制。</li> <li>• <b>FAILURE</b>：复制失败，出现永久性故障。用户必须解决此错误。</li> </ul> |
| 目标   | <b>REPLICA</b> ：该对象已从源网格复制。                                                                                                                                    |



StorageGRID 不支持 `x-amz-replication-status` 标头。

### 使用 S3 HeadObject 请求从 StorageGRID 中的对象检索元数据

您可以使用 S3 HeadObject 请求从对象检索元数据，而无需返回对象本身。如果对象存储在云存储池中，则可以使用 HeadObject 来确定对象的过渡状态。

### HeadObject 和多部分对象

您可以使用 `partNumber` 请求参数检索多部分或分段对象的特定部分的元数据。`x-amz-mp-parts-count` 响应元素指示对象有多少个部分。

您可以将 `partNumber` 设置为 1，适用于分段/多部分对象和非分段/非多部分对象；但是，`x-amz-mp-parts-count` 响应元素仅针对分段或多部分对象返回。

用户元数据中的 **UTF-8** 字符

StorageGRID 不解析或解释用户定义元数据中转义的 UTF-8 字符。对于在用户定义元数据中包含转义 UTF-8 字符的对象的 HEAD 请求，如果键名称或值包含不可打印的字符，则不会返回 `x-amz-missing-meta` 标头。

支持的请求标头

支持以下请求标头：

- `x-amz-checksum-mode`

The `partNumber` 参数和 `Range` 标头不支持与 `x-amz-checksum-mode` 一起用于 `HeadObject`。当您在启用了 `x-amz-checksum-mode` 的请求中包含这些参数时，StorageGRID 不会在响应中返回校验和值。

不支持的请求标头

以下请求标头不受支持，并返回 `XNotImplemented`：

- `x-amz-website-redirect-location`

版本控制

如果未指定 `versionId` 子资源，则该操作将获取版本化存储区中对象的最新版本。如果对象的当前版本是删除标记，则会返回 "Not Found" 状态，并将 `x-amz-delete-marker` 响应标头设置为 `true`。

使用客户提供的加密密钥 (**SSE-C**) 进行服务器端加密的请求标头

如果对象使用您提供的唯一密钥加密，请使用所有这三个标头。

- `x-amz-server-side-encryption-customer-algorithm`: 指定 AES256。
- `x-amz-server-side-encryption-customer-key`: 指定对象的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`: 指定对象加密密钥的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["\\${post\\_edited\\_translations.segment}"](#) 中的注意事项。

**Cloud Storage Pool** 对象的 **HeadObject** 响应

如果对象存储在 "云存储池" 中，则返回以下响应标头：

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

响应标头提供有关对象移动到云存储池、可选地转换到不可检索状态以及还原时的状态的信息。

| 对象的状态                                               | 对 <b>HeadObject</b> 的响应 |
|-----------------------------------------------------|-------------------------|
| 已载入 StorageGRID 但尚未经过 ILM 评估的对象，或存储在传统存储池中或使用纠删码的对象 | 200 OK （未返回特殊响应标头。）     |

| 对象的状态                      | 对 <b>HeadObject</b> 的响应                                                                                                                                                                                                                                                                                                      |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 云存储池中的对象，但尚未转换到不可检索的状态     | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false",<br/>expiry-date="Sat, 23 July 20 2030<br/>00:00:00 GMT"</p> <p>在对象转换为不可检索状态之前，expiry-date 的值将设置为将来某个遥远的时间。转换的确切时间不受 StorageGRID 系统的控制。</p>                                                                                      |
| 对象已转换为不可检索状态，但网格上也至少存在一个副本 | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false",<br/>expiry-date="Sat, 23 July 20 2030<br/>00:00:00 GMT"</p> <div><p><code>`expiry-date`</code><br/>的值设置为将来某个较远的时间。</p></div> <p>注意：如果网格上的副本不可用（例如，存储节点已关闭），则必须发出 <a href="#">"RestoreObject"</a> 请求，以便从云存储池还原副本，然后才能成功检索对象。</p> |
| 对象已转换为不可检索的状态，并且网格上不存在副本   | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>                                                                                                                                                                                                                                                                            |
| 正在从不可检索状态还原的对象             | <p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>                                                                                                                                                                                                                               |

| 对象的状态        | 对 <b>HeadObject</b> 的响应                                                                                                                                                                                 |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 对象已完全还原到云存储池 | <pre>200 OK  x-amz-storage-class: GLACIER  x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT"</pre> <div><code>`expiry-date`</code><br/>指示云存储池中的对象何时将返回到不可检索状态。</div> |

### 云存储池中的多部分或分段对象

如果您上传了多部分对象，或者 StorageGRID 将大型对象拆分为多个分段，StorageGRID 将通过对对象的部分或分段进行采样来确定该对象在云存储池中是否可用。在某些情况下，当对象的某些部分已转换为不可检索状态或对象的某些部分尚未还原时，HeadObject 请求可能会错误地返回 `x-amz-restore: ongoing-request="false"`。

### HeadObject 和跨网格复制

如果您正在使用“[网格联盟](#)”并且为存储桶启用了“[跨网格复制](#)”，则 S3 客户端可以通过发出 HeadObject 请求来验证对象的复制状态。响应包括 StorageGRID 特定的 ``x-ntap-sg-cgr-replication-status`` 响应标头，该标头将具有以下值之一：

| Grid | 复制状态                                                                                                                                                       |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 源    | <ul style="list-style-type: none"><li>• <b>COMPLETED</b>：复制成功。</li><li>• <b>PENDING</b>：对象尚未复制。</li><li>• <b>FAILURE</b>：复制失败，出现永久性故障。用户必须解决此错误。</li></ul> |
| 目标   | <b>REPLICA</b> ：该对象已从源网格复制。                                                                                                                                |



StorageGRID 不支持 ``x-amz-replication-status`` 标头。

使用 **S3 PutObject** 请求将对象添加到 **StorageGRID** 中的存储桶

您可以使用 S3 PutObject 请求将对象添加到存储桶。

### 解决冲突

冲突的客户端请求（例如两个客户端向同一密钥写入）将以“最新获胜”为原则进行解决。“最新获胜”评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

## 对象大小

单次 PutObject 操作的最大\_推荐\_大小为 5 GiB (5,368,709,120 字节)。如果您的对象大于 5 GiB，请改用 ["多部件上传"](#)。

单次 PutObject 操作的最大\_支持\_大小为 5 TiB (5,497,558,138,880 字节)。



如果您从 StorageGRID 11.6 或更早版本升级，则在尝试上传超过 5 GiB 的对象时，将触发 S3 PUT Object size too large 警报。如果您新安装了 StorageGRID 11.7 或 11.8，则在此情况下不会触发警报。但是，为了与 AWS S3 标准保持一致，未来版本的 StorageGRID 将不支持上传大于 5 GiB 的对象。

## 用户元数据大小

Amazon S3 将每个 PUT 请求标头中用户定义的元数据大小限制为 2 KB。StorageGRID 将用户元数据限制为 24 KiB。用户定义的元数据的大小通过计算每个键和值的 UTF-8 编码字节数之和来衡量。

### 用户元数据中的 UTF-8 字符

如果请求在用户定义元数据的键名或值中包含（未转义的）UTF-8 值，则 StorageGRID 行为未定义。

StorageGRID 不解析或解释用户定义元数据的键名或值中包含的转义的 UTF-8 字符。转义的 UTF-8 字符被视为 ASCII 字符：

- PutObject、CopyObject、GetObject 和 HeadObject 请求在用户定义的元数据包含转义的 UTF-8 字符时成功。
- 如果键名或键值的解释值包含不可打印的字符，StorageGRID 不会返回 `x-amz-missing-meta` 标头。

## 对象标记限制

您可以在上传新对象时向其添加标签，也可以将其添加到现有对象。StorageGRID 和 Amazon S3 都支持每个对象最多 10 个标记。与对象关联的标签必须具有唯一的标签键。标记键的长度最多可为 128 个 Unicode 字符，标记值最多可为 256 个 Unicode 字符。键和值区分大小写。

## 对象所有权

在 StorageGRID 中，所有对象都由存储桶所有者帐户拥有，包括由非所有者帐户或匿名用户创建的对象。

## 支持的请求标头

支持以下请求标头：

- Cache-Control
- Content-Disposition
- Content-Encoding

当您为 aws-chunked 指定 Content-Encoding 时，StorageGRID 不验证以下项目：

- StorageGRID 不会根据分块数据验证 chunk-signature。
- StorageGRID 不会根据对象验证您为 `x-amz-decoded-content-length` 提供的值。

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

如果同时使用 `aws-chunked` 有效负载签名，则支持分块传输编码。

- x-amz-checksum-sha256
- x-amz-meta-，后跟包含用户定义元数据的名称-值对。

为用户定义的元数据指定名称-值对时，请使用以下常规格式：

```
x-amz-meta-name: value
```

如果要将\*用户定义的创建时间\*选项用作 ILM 规则的参考时间，则必须使用 `creation-time` 作为记录对象创建时间的元数据的名称。例如：

```
x-amz-meta-creation-time: 1443399726
```

`creation-time` 的值计算为自 1970 年 1 月 1 日以来的秒数。



ILM 规则不能同时使用\*用户定义的创建时间\*作为参考时间和平衡或严格摄取选项。创建 ILM 规则时将返回错误。

- x-amz-tagging
- S3 对象锁定请求标头
  - x-amz-object-lock-mode
  - x-amz-object-lock-retain-until-date
  - x-amz-object-lock-legal-hold

如果在没有这些标头的情况下发出请求，则会使用存储桶默认保留设置来计算对象版本模式和 retain-until-date。请参阅 ["使用 S3 REST API 配置 S3 对象锁定"](#)。

- SSE 请求标头：
  - x-amz-server-side-encryption
  - x-amz-server-side-encryption-customer-key-MD5
  - x-amz-server-side-encryption-customer-key

◦ `x-amz-server-side-encryption-customer-algorithm`

请参阅 [\[服务器端加密的请求标头\]](#)

不支持的请求标头

不支持以下请求标头：

- `If-Match`

``If-Match header`` 是可以接受的，但不起作用。

- `If-None-Match`

``If-None-Match header`` 是可以接受的，但不起作用。

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

The `x-amz-website-redirect-location` 标头返回 `XNotImplemented`。

存储类选项

支持 ``x-amz-storage-class`` 请求标头。为 ``x-amz-storage-class`` 提交的值会影响 StorageGRID 保护对象数据的方式，而不会影响存储在 StorageGRID 系统中的对象的永久副本数量（由 ILM 确定）。

如果与接收对象匹配的 ILM 规则使用“严格接收”选项，则 ``x-amz-storage-class`` 标头无效。

以下值可用于 `x-amz-storage-class`：

- STANDARD（默认）
  - **Dual commit**：如果 ILM 规则为 Ingest Behavior 指定了 Dual commit 选项，则一旦接收对象，就会创建该对象的第二个副本并分发到其他存储节点（Dual commit）。评估 ILM 时，StorageGRID 确定这些初始临时副本是否满足规则中的放置说明。如果不满足，则可能需要在不同位置创建新的对象副本，并且可能需要删除初始临时副本。
  - 平衡：如果 ILM 规则指定平衡选项，并且 StorageGRID 无法立即生成规则中指定的所有副本，StorageGRID 会在不同的 Storage Node 上生成两个临时副本。

如果 StorageGRID 可以立即创建 ILM 规则（同步放置）中指定的所有对象副本，则 ``x-amz-storage-class`` 标头无效。

- REDUCED\_REDUNDANCY

- 双提交：如果 ILM 规则为接收行为指定了双提交选项，StorageGRID 会在接收对象时创建单个中期副本（单提交）。
- 平衡：如果 ILM 规则指定平衡选项，只有在系统无法立即生成规则中指定的所有副本时，StorageGRID 才会创建单个临时副本。如果 StorageGRID 可以执行同步放置，则此标头无效。当与对象匹配的 ILM 规则创建单个复制副本时，最好使用 `REDUCED\_REDUNDANCY` 选项。在这种情况下，使用 `REDUCED\_REDUNDANCY` 可避免为每次摄取操作不必要地创建和删除额外的对象副本。

不建议在其他情况下使用 `REDUCED\_REDUNDANCY` 选项。`REDUCED\_REDUNDANCY` 会增加摄取过程中对象数据丢失的风险。例如，如果单个副本最初存储在 ILM 评估发生之前发生故障的存储节点上，则可能会丢失数据。



在任何时间段内只有一个复制副本会使数据面临永久丢失的风险。如果某个对象只有一个复制副本，则当存储节点发生故障或出现重大错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对该对象的访问权限。

指定 `REDUCED\_REDUNDANCY` 仅影响首次接收对象时创建的副本数。当对象由活动 ILM 策略评估时，它不会影响对象的副本数，也不会导致数据以较低的冗余级别存储在 StorageGRID 系统中。



如果要将对对象接收到启用了 S3 对象锁定的存储桶中，则该 `REDUCED\_REDUNDANCY` 选项将被忽略。如果要将对对象摄入旧版合规存储桶，则该 `REDUCED\_REDUNDANCY` 选项将返回错误。StorageGRID 将始终执行双提交摄取，以确保满足合规性要求。

#### 服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对对象进行加密。SSE 和 SSE-C 选项互斥。

- **SSE**：如果要使用由 StorageGRID 管理的唯一密钥加密对象，请使用以下标头。

- `x-amz-server-side-encryption`

当 `x-amz-server-side-encryption` 标头未包含在 PutObject 请求中时，全网格范围的["存储对象加密设置"](#)将从 PutObject 响应中省略。

- **SSE-C**：如果要使用您提供和管理的唯一密钥加密对象，请使用所有这三个标头。

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定新对象的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定新对象加密密钥的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["使用服务器端加密"](#) 的注意事项。



如果对象使用 SSE 或 SSE-C 加密，则将忽略任何存储桶级或网格级加密设置。

#### 版本控制

如果为存储桶启用了版本控制，则会为要存储的对象版本自动生成唯一的 `versionId`。此 `versionId` 也会通过 `x-amz-version-id` 响应标头在响应中返回。

如果版本控制被挂起，则对象版本将以 `null versionId` 存储，如果 `null` 版本已存在，则将被覆盖。

Authorization 标头的签名计算

使用 `Authorization` 标头对请求进行身份验证时，StorageGRID 与 AWS 在以下方面有所不同：

- StorageGRID 不要求将 `host` 标头包含在 `CanonicalHeaders` 中。
- StorageGRID 不需要将 `Content-Type` 包含在 `CanonicalHeaders` 中。
- StorageGRID 不要求将 `x-amz-\*` 标头包含在 `CanonicalHeaders` 中。



作为一般最佳做法，始终在 `CanonicalHeaders` 中包含这些标头，以确保它们得到验证；但是，如果排除这些标头，StorageGRID 不会返回错误。

有关详细信息，请参阅 ["授权标头的签名计算：在单个区块中传输负载（AWS Signature Version 4）"](#)。

相关信息

- ["使用 ILM 管理对象"](#)
- ["Amazon Simple Storage Service API Reference: PutObject"](#)

使用 **S3 RestoreObject** 请求在 **StorageGRID** 中还原对象

您可以使用 S3 RestoreObject 请求还原存储在云存储池中的对象。

支持的请求类型

StorageGRID 仅支持 RestoreObject 请求来还原对象。它不支持 `SELECT` 类型的还原。Select 请求返回 ``XNotImplemented``。

版本控制

（可选）指定 `versionId` 以还原版本化存储桶中对象的特定版本。如果未指定 ``versionId``，则还原对象的最新版本

RestoreObject 在云存储池对象上的行为

如果对象已存储在 ["云存储池"](#) 中，则根据对象的状态，RestoreObject 请求具有以下行为。有关更多详细信息，请参见 ["HeadObject"](#)。



如果对象存储在 Cloud Storage Pool 中，并且该对象的一个或多个副本也存在于网格上，则无需通过发出 RestoreObject 请求来还原对象。相反，可以使用 GetObject 请求直接检索本地副本。

| 对象的状态                                      | RestoreObject 的行为                                                           |
|--------------------------------------------|-----------------------------------------------------------------------------|
| 对象已摄入 StorageGRID 但尚未由 ILM 评估，或者此对象不在云存储池中 | 403 Forbidden, InvalidObjectState                                           |
| 云存储池中的对象，但尚未转换到不可检索的状态                     | 200 OK 不会进行任何更改。<br><br>注意：在对象转换为不可检索状态之前，您无法更改其 <code>expiry-date</code> 。 |

| 对象的状态          | RestoreObject 的行为                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 对象已转换为不可检索状态   | <p>202 Accepted 按请求正文中指定的天数将对象的可检索副本还原到云存储池。在此期间结束时，对象将返回到不可检索的状态。</p> <p>（可选）使用 Tier 请求元素来确定还原作业需要多长时间才能完成（Expedited、Standard 或 Bulk）。如果未指定 Tier，则使用 Standard 层。</p> <p>重要提示：如果对象已转换到 S3 Glacier Deep Archive 或云存储池使用 Azure Blob 存储，则无法使用 Expedited 层还原该对象。将返回以下错误 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class。</p> |
| 正在从不可检索状态还原的对象 | 409 Conflict, RestoreAlreadyInProgress                                                                                                                                                                                                                                                                                                                       |
| 对象已完全还原到云存储池   | <p>200 OK</p> <p>注意：如果对象已恢复到可检索状态，则可以通过使用新值重新发出 RestoreObject 请求来更改其 expiry-date Days。恢复日期相对于请求时间进行更新。</p>                                                                                                                                                                                                                                                   |

使用 **S3 SelectObjectContent** 请求过滤 **StorageGRID** 中的对象数据

您可以使用 S3 SelectObjectContent 请求根据简单的 SQL 语句筛选 S3 对象的内容。

有关详细信息，请参见 ["Amazon Simple Storage Service API Reference: SelectObjectContent"](#)。

开始之前

- 租户帐户具有 S3 Select 权限。
- 您对要查询的对象具有 s3:GetObject 权限。
- 要查询的对象必须采用以下格式之一：
  - **CSV**。可以按原样使用或压缩到 GZIP 或 BZIP2 存档中。
  - **Parquet**。Parquet 对象的其他要求：
    - S3 Select 仅支持使用 GZIP 或 Snappy 的列压缩。S3 Select 不支持 Parquet 对象的全对象压缩。
    - S3 Select 不支持 Parquet 输出。必须将输出格式指定为 CSV 或 JSON。
    - 最大未压缩行组大小为 512 MB。
    - 您必须使用在对象架构中指定的数据类型。
    - 不能使用 INTERVAL、JSON、LIST、TIME 或 UUID 逻辑类型。
- 您的 SQL 表达式最大长度为 256 KB。
- 输入或结果中的任何记录的最大长度为 1 MiB。

## CSV请求语法示例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

## Parquet 请求语法示例

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>

```

### SQL查询示例

此查询获取州名、2010 年人口、2015 年估计人口以及美国人口普查数据的变化百分比。文件中非州的记录将被忽略。

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

要查询的文件的前几行，`SUB-EST2020\_ALL.csv`如下所示：

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

#### AWS-CLI 使用示例 (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

输出文件的前几行 `changes.csv` 如下所示：

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

输出文件 changes.csv 的前几行如下所示：

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

## 多部分上传的操作

### StorageGRID 中支持的分段上传操作

本节介绍 StorageGRID 如何支持分段上传操作。

以下条件和注意事项适用于所有多部分上传操作：

- 不应超过 1,000 个并发多部分上传到单个存储桶，因为该存储桶的 ListMultipartUploads 查询结果可能会返回不完整的结果。
- StorageGRID 强制执行适用于分段上传各部分的 AWS 大小限制。S3 客户端必须遵循以下准则：
  - 多部分上传中的每个部分必须介于 5 MiB (5,242,880 字节) 和 5 GiB (5,368,709,120 字节) 之间。
  - 最后一部分可以小于 5 MiB (5,242,880 字节)。
  - 一般来说，分段大小应尽可能大。例如，对于 100 GiB 对象，使用 5 GiB 的分段大小。由于每个分段都被视为唯一的对象，因此使用较大的分段大小可减少 StorageGRID 元数据开销。
  - 对于小于 5 GiB 的对象，请考虑改用非多部分上传。
- 在多部分对象被载入时，ILM 会对其每个部分进行评估；如果 ILM 规则使用 Balanced 或 Strict ["载入选项"](#)，则在多部分上传完成时还会对整个对象进行评估。您应该了解这会如何影响对象和部件的放置：
  - 如果在 S3 多部分上传过程中更改了 ILM，则当多部分上传完成时，对象的某些部分可能不符合当前的 ILM 要求。任何未正确放置的部分都会排队等待 ILM 重新评估，并在稍后移至正确的位置。
  - 在评估某个部件的 ILM 时，StorageGRID 会根据部件的大小而非对象的大小进行筛选。这意味着对象的某些部件可以存储在不符合整个对象 ILM 要求的位置。例如，如果规则指定所有 10 GB 或更大的对象存储在 DC1，而所有较小的对象存储在 DC2，则 10 部分分段上传中的每个 1 GB 部件在写入时均存储在 DC2。但是，当对整个对象评估 ILM 时，对象的所有部件都将移动到 DC1。

- 所有多部分上传操作都支持 StorageGRID "一致性值"。
- 当使用分段上传方式载入对象时，"对象分割阈值（1 GiB）"不适用。
- 您可以根据需要将 "服务器端加密" 与分段上传结合使用。要使用 SSE（使用 StorageGRID 管理的密钥进行服务器端加密），请仅在 CreateMultipartUpload 请求中包含 x-amz-server-side-encryption 请求标头。要使用 SSE-C（使用客户提供的密钥进行服务器端加密），请在 CreateMultipartUpload 请求以及每个后续 UploadPart 请求中指定相同的三个加密密钥请求标头。
- 如果提取在基本存储桶的 Before 时间戳之前启动，则多部分上传的对象将包含在 "分支存储桶" 中，而不管上传何时完成。

| 操作                                                         | 实施                                         |
|------------------------------------------------------------|--------------------------------------------|
| AbortMultipartUpload                                       | 已使用所有 Amazon S3 REST API 行为实施。如有更改，恕不另行通知。 |
| CompleteMultipartUpload                                    | 请参阅 "CompleteMultipartUpload"              |
| CreateMultipartUpload<br>(先前命名为 Initiate Multipart Upload) | 请参阅 "CreateMultipartUpload"                |
| ListMultipartUploads                                       | 请参阅 "ListMultipartUploads"                 |
| ListParts                                                  | 已使用所有 Amazon S3 REST API 行为实施。如有更改，恕不另行通知。 |
| UploadPart                                                 | 请参阅 "UploadPart"                           |
| UploadPartCopy                                             | 请参阅 "UploadPartCopy"                       |

## StorageGRID S3 REST API 如何完成多部分上传

该 CompleteMultipartUpload 操作通过组装先前上传的部件来完成对象的多部分上传。



StorageGRID 支持 CompleteMultipartUpload 的 `partNumber` 请求参数中按升序排列的非连续值。该参数可以从任何值开始。

### 解决冲突

冲突的客户端请求（例如两个客户端向同一密钥写入）将以"最新获胜"为原则进行解决。"最新获胜"评估的时间取决于 StorageGRID 系统何时完成给定请求，而不是 S3 客户端何时开始操作。

### 支持的请求标头

支持以下请求标头：

- x-amz-checksum-sha256

- `x-amz-storage-class`

如果匹配的 ILM 规则指定了 "双提交或平衡摄取选项", 则 `x-amz-storage-class` 标头会影响 StorageGRID 创建的对象副本数量。

- STANDARD

(默认值) 当 ILM 规则使用双提交选项时, 或当平衡选项回退到创建临时副本时, 指定双提交接收操作。

- REDUCED\_REDUNDANCY

当 ILM 规则使用双提交选项, 或当平衡选项回退到创建临时副本时, 指定单提交接收操作。



如果要将对对象接收到启用了 S3 对象锁定的存储桶中, 则该 `REDUCED_REDUNDANCY` 选项将被忽略。如果要将对对象摄入旧版合规存储桶, 则该 `REDUCED_REDUNDANCY` 选项将返回错误。StorageGRID 将始终执行双提交摄取, 以确保满足合规性要求。



如果多部分上传未在 15 天内完成, 则该操作将被标记为非活动, 并从系统中删除所有相关数据。



返回的 `ETag` 值不是数据的 MD5 和, 而是遵循多部分对象的 `ETag` 值的 Amazon S3 API 实现。

不支持的请求标头

不支持以下请求标头:

- If-Match

`If-Match header` 是可以接受的, 但不起作用。

- If-None-Match

`If-None-Match header` 是可以接受的, 但不起作用。

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

版本控制

此操作完成多部分上传。如果为存储桶启用了版本控制, 则在完成多部分上传后创建对象版本。

如果为存储桶启用了版本控制, 则会为要存储的对象版本自动生成唯一的 `versionId`。此 `versionId` 也会通过 `x-amz-version-id` 响应标头在响应中返回。

如果版本控制被挂起, 则对象版本将以 `null versionId` 存储, 如果 `null` 版本已存在, 则将被覆盖。



当对存储桶启用版本控制时，完成多部分上传始终会创建新版本，即使在同一对象键上并发完成多部分上传也是如此。当未对存储桶启用版本控制时，可以启动多部分上传，然后在同一对象键上首先启动和完成另一个多部分上传。在非版本存储桶上，最后完成的多部分上传优先。

复制、通知或元数据通知失败

如果为平台服务配置了发生多部分上传的存储桶，则即使关联的复制或通知操作失败，多部分上传也会成功。

租户可以通过更新对象的元数据或标记来触发失败的复制或通知。租户可以重新提交现有值，以避免进行不必要的更改。

请参阅 ["排查平台服务故障"](#)。

**StorageGRID 中的 S3 CreateMultipartUpload 请求标头和选项**

CreateMultipartUpload（以前称为 Initiate Multipart Upload）操作为对象启动多部分上传，并返回上传 ID。

支持 `x-amz-storage-class` 请求标头。为 `x-amz-storage-class` 提交的值会影响 StorageGRID 保护对象数据的方式，而不会影响存储在 StorageGRID 系统中的对象的永久副本数量（由 ILM 确定）。

如果与接收对象匹配的 ILM 规则使用 Strict **"载入选项"**，则 `x-amz-storage-class` 标头无效。

以下值可用于 `x-amz-storage-class`：

- STANDARD（默认）
  - 双重提交：如果 ILM 规则指定双重提交接收选项，则一旦接收对象，就会创建该对象的第二个副本，并将其分发到其他存储节点（双重提交）。评估 ILM 时，StorageGRID 确定这些初始临时副本是否满足规则中的放置说明。如果不满足，则可能需要在不同位置创建新的对象副本，并且可能需要删除初始临时副本。
  - 平衡：如果 ILM 规则指定平衡选项，并且 StorageGRID 无法立即生成规则中指定的所有副本，StorageGRID 会在不同的 Storage Node 上生成两个临时副本。

如果 StorageGRID 可以立即创建 ILM 规则（同步放置）中指定的所有对象副本，则 `x-amz-storage-class` 标头无效。

- REDUCED\_REDUNDANCY
  - 双提交：如果 ILM 规则指定双提交选项，StorageGRID 会在接收对象时创建单个临时副本（单提交）。
  - 平衡：如果 ILM 规则指定平衡选项，只有在系统无法立即生成规则中指定的所有副本时，StorageGRID 才会创建单个临时副本。如果 StorageGRID 可以执行同步放置，则此标头无效。当与对象匹配的 ILM 规则创建单个复制副本时，最好使用 `REDUCED\_REDUNDANCY` 选项。在这种情况下，使用 `REDUCED\_REDUNDANCY` 可避免为每次摄取操作不必要地创建和删除额外的对象副本。

不建议在其他情况下使用 `REDUCED\_REDUNDANCY` 选项。`REDUCED\_REDUNDANCY` 会增加摄取过程中对象数据丢失的风险。例如，如果单个副本最初存储在 ILM 评估发生之前发生故障的存储节点上，则可能会丢失数据。



在任何时间段内只有一个复制副本会使数据面临永久丢失的风险。如果某个对象只有一个复制副本，则当存储节点发生故障或出现重大错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对该对象的访问权限。

指定 `REDUCED\_REDUNDANCY` 仅影响首次接收对象时创建的副本数。当对象由活动 ILM 策略评估时，它不会影响对象的副本数，也不会导致数据以较低的冗余级别存储在 StorageGRID 系统中。



如果要将对象接收到启用了 S3 对象锁定的存储桶中，则该 `REDUCED\_REDUNDANCY` 选项将被忽略。如果要将对象摄入旧版合规存储桶，则该 `REDUCED\_REDUNDANCY` 选项将返回错误。StorageGRID 将始终执行双提交摄取，以确保满足合规性要求。

支持的请求标头

支持以下请求标头：

- Content-Type
- x-amz-checksum-algorithm

目前，仅支持 `x-amz-checksum-algorithm` 的 SHA256 值。

- x-amz-meta-，后跟包含用户定义元数据的名称-值对

为用户定义的元数据指定名称-值对时，请使用以下常规格式：

```
x-amz-meta-_name_: `value`
```

如果要将\*用户定义的创建时间\*选项用作 ILM 规则的参考时间，则必须使用 `creation-time` 作为记录对象创建时间的元数据的名称。例如：

```
x-amz-meta-creation-time: 1443399726
```

`creation-time` 的值计算为自 1970 年 1 月 1 日以来的秒数。



如果要将对象添加到启用了旧版合规性的存储桶，则不允许将 `creation-time` 添加为用户定义的元数据。将返回错误。

- S3 Object Lock 请求标头：

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

如果在没有这些标头的情况下发出请求，则使用存储桶默认保留设置来计算对象版本 retain-until-date。

## "使用 S3 REST API 配置 S3 对象锁定"

- SSE 请求标头：

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

### [服务器端加密的请求标头]



有关 StorageGRID 处理 UTF-8 字符的信息，请参见 ["放置对象"](#)。

## 服务器端加密的请求标头

您可以使用以下请求标头通过服务器端加密对分段对象进行加密。SSE 和 SSE-C 选项互斥。

- **SSE**：如果要使用由 StorageGRID 管理的唯一密钥对对象进行加密，请在 CreateMultipartUpload 请求中使用以下标头。不要在任何 UploadPart 请求中指定此标头。

- x-amz-server-side-encryption

- **SSE-C**：如果您想使用您提供和管理的唯一密钥加密对象，请在 CreateMultipartUpload 请求中（以及在每个后续 UploadPart 请求中）使用所有这三个标头。

- x-amz-server-side-encryption-customer-algorithm：指定 AES256。
- x-amz-server-side-encryption-customer-key：指定新对象的加密密钥。
- x-amz-server-side-encryption-customer-key-MD5：指定新对象加密密钥的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["使用服务器端加密"](#) 的注意事项。

## 不支持的请求标头

不支持以下请求标头：

- x-amz-website-redirect-location

The x-amz-website-redirect-location 标头返回 XNotImplemented。

## 版本控制

多部分上传由单独的操作组成，用于启动上传、列出上传、上传部分、组装上传的部分和完成上传。执行 CompleteMultipartUpload 操作时将创建对象（如果适用，还会进行版本控制）。

## StorageGRID 中的 S3 ListMultipartUploads 操作和支持的参数

ListMultipartUploads 操作列出存储桶正在进行的分段上传。

支持以下请求参数：

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

#### 版本控制

多部分上传由单独的操作组成，用于启动上传、列出上传、上传部分、组装上传的部分和完成上传。执行 CompleteMultipartUpload 操作时将创建对象（如果适用，还会进行版本控制）。

#### StorageGRID 中 S3 UploadPart 操作支持和不支持的请求标头

UploadPart 操作用于在对象的分段上传中上传一个分段。

支持的请求标头

支持以下请求标头：

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

#### 服务器端加密的请求标头

如果为 CreateMultipartUpload 请求指定了 SSE-C 加密，则还必须在每个 UploadPart 请求中包含以下请求标头：

- x-amz-server-side-encryption-customer-algorithm：指定 AES256。
- x-amz-server-side-encryption-customer-key：指定在 CreateMultipartUpload 请求中提供的相同加密密钥。
- x-amz-server-side-encryption-customer-key-MD5：指定您在 CreateMultipartUpload 请求中提供的相同 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 ["\\${post\\_edited\\_translations.segment}"](#) 中的注意事项。

如果在 CreateMultipartUpload 请求期间指定了 SHA-256 校验和，则还必须在每个 UploadPart 请求中包含以下请求标头：

- x-amz-checksum-sha256：指定此部件的 SHA-256 校验和。

不支持的请求标头

不支持以下请求标头：

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

版本控制

多部分上传由单独的操作组成，用于启动上传、列出上传、上传部分、组装上传的部分和完成上传。执行 `CompleteMultipartUpload` 操作时将创建对象（如果适用，还会进行版本控制）。

使用 **S3 UploadPartCopy** 操作在 **StorageGRID** 中上传对象的一部分

该 `UploadPartCopy` 操作通过从现有对象复制数据作为数据源来上传对象的一部分。

该 `UploadPartCopy` 操作使用所有 Amazon S3 REST API 行为实现。如有更改，恕不另行通知。

此请求读取和写入 `StorageGRID` 系统中 ``x-amz-copy-source-range`` 指定的对象数据。

支持以下请求标头：

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

服务器端加密的请求标头

如果为 `CreateMultipartUpload` 请求指定了 SSE-C 加密，则还必须在每个 `UploadPartCopy` 请求中包含以下请求标头：

- `x-amz-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-server-side-encryption-customer-key`：指定在 `CreateMultipartUpload` 请求中提供的相同加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在 `CreateMultipartUpload` 请求中提供的相同 MD5 摘要。

如果使用客户提供的密钥 (SSE-C) 加密源对象，则必须在 `UploadPartCopy` 请求中包含以下三个标头，以便可以解密然后复制对象：

- `x-amz-copy-source-server-side-encryption-customer-algorithm`：指定 AES256。
- `x-amz-copy-source-server-side-encryption-customer-key`：指定创建源对象时提供的加密密钥。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定创建源对象时提供的 MD5 摘要。



您提供的加密密钥绝不会被存储。如果丢失加密密钥，则会丢失相应的对象。在使用客户提供的密钥保护对象数据之前，请查看 "[\\${post\\_edited\\_translations.segment}](#)" 中的注意事项。

## 版本控制

多部分上传由单独的操作组成，用于启动上传、列出上传、上传部分、组装上传的部分和完成上传。执行 CompleteMultipartUpload 操作时将创建对象（如果适用，还会进行版本控制）。

## StorageGRID S3 REST API 错误响应

StorageGRID 系统支持所有适用的标准 S3 REST API 错误响应。此外，StorageGRID 实现还添加了几个自定义响应。

### 支持的 **S3 API** 错误代码

| 名称                              | HTTP 状态         |
|---------------------------------|-----------------|
| AccessDenied                    | 403 禁止访问        |
| BadDigest                       | 400 Bad Request |
| BucketAlreadyExists             | 409 冲突          |
| BucketNotEmpty                  | 409 冲突          |
| IncompleteBody                  | 400 Bad Request |
| InternalServerError             | 500 内部服务器错误     |
| InvalidAccessKeyId              | 403 禁止访问        |
| InvalidArgument                 | 400 Bad Request |
| InvalidBucketName               | 400 Bad Request |
| InvalidBucketState              | 409 冲突          |
| InvalidDigest                   | 400 Bad Request |
| InvalidEncryptionAlgorithmError | 400 Bad Request |
| InvalidPart                     | 400 Bad Request |
| InvalidPartOrder                | 400 Bad Request |

| 名称                                   | HTTP 状态                             |
|--------------------------------------|-------------------------------------|
| InvalidRange                         | 416 Requested Range Not Satisfiable |
| InvalidRequest                       | 400 Bad Request                     |
| InvalidStorageClass                  | 400 Bad Request                     |
| InvalidTag                           | 400 Bad Request                     |
| InvalidURI                           | 400 Bad Request                     |
| KeyTooLong                           | 400 Bad Request                     |
| MalformedXML                         | 400 Bad Request                     |
| MetadataTooLarge                     | 400 Bad Request                     |
| MethodNotAllowed                     | 405 方法不允许                           |
| MissingContentLength                 | 411 Length Required                 |
| MissingRequestBodyError              | 400 Bad Request                     |
| MissingSecurityHeader                | 400 Bad Request                     |
| NoSuchBucket                         | 404 未找到                             |
| NoSuchKey                            | 404 未找到                             |
| NoSuchUpload                         | 404 未找到                             |
| NotImplemented                       | 501 未实现                             |
| NoSuchBucketPolicy                   | 404 未找到                             |
| ObjectLockConfigurationNotFoundError | 404 未找到                             |
| PreconditionFailed                   | 412 前提条件失败                          |
| RequestTimeTooSkewed                 | 403 禁止访问                            |
| ServiceUnavailable                   | 503 服务不可用                           |

| 名称                     | HTTP 状态         |
|------------------------|-----------------|
| SignatureDoesNotMatch  | 403 禁止访问        |
| TooManyBuckets         | 400 Bad Request |
| UserKeyMustBeSpecified | 400 Bad Request |

### StorageGRID 自定义错误代码

| 名称                                    | 问题描述                       | HTTP 状态         |
|---------------------------------------|----------------------------|-----------------|
| XBucketLifecycleNotAllowed            | 旧版合规存储桶中不允许使用存储桶生命周期配置     | 400 Bad Request |
| XBucketPolicyParseException           | 无法解析接收的存储桶策略 JSON。         | 400 Bad Request |
| XComplianceConflict                   | 由于旧版合规性设置，操作被拒绝。           | 403 禁止访问        |
| XComplianceReducedRedundancyForbidden | 旧版合规存储桶中不允许降低冗余            | 400 Bad Request |
| XMaxBucketPolicyLengthExceeded        | 您的策略超出允许的最大存储桶策略长度。        | 400 Bad Request |
| XMissingInternalRequestHeader         | 缺少内部请求的标头。                 | 400 Bad Request |
| XNoSuchBucketCompliance               | 指定的存储桶未启用旧版合规性。            | 404 未找到         |
| XNotAcceptable                        | 此请求包含一个或多个无法满足的 accept 标头。 | 406 无法接受        |
| XNotImplemented                       | 您提供的请求暗示了未实现的功能。           | 501 未实现         |

## StorageGRID 自定义操作

### StorageGRID 中支持的自定义存储桶操作

StorageGRID 系统支持添加到 S3 REST API 的自定义操作。

下表列出了 StorageGRID 支持的自定义操作。

| 操作                                | 问题描述            |
|-----------------------------------|-----------------|
| " <a href="#">获取 Bucket 一致性</a> " | 返回应用于特定存储桶的一致性。 |

| 操作                          | 问题描述                            |
|-----------------------------|---------------------------------|
| "PUT Bucket 一致性"            | 设置应用于特定存储桶的一致性。                 |
| "获取 Bucket 上次访问时间"          | 返回是否为特定存储桶启用或禁用上次访问时间更新。        |
| "PUT Bucket 上次访问时间"         | 允许您启用或禁用特定存储桶的上次访问时间更新。         |
| "删除存储桶元数据通知配置"              | 删除与特定存储桶关联的元数据通知配置 XML。         |
| "获取 Bucket 元数据通知配置"         | 返回与特定存储桶关联的元数据通知配置 XML。         |
| "PUT Bucket 元数据通知配置"        | 配置存储区的元数据通知服务。                  |
| "获取存储使用情况"                  | 显示帐户使用的总存储量以及与帐户关联的每个存储桶的存储量。   |
| "已弃用：使用合规性设置的 CreateBucket" | 已弃用且不受支持：您无法再创建启用合规性的新存储桶。      |
| "已弃用：GET Bucket compliance" | 已弃用但受支持：返回当前对现有旧版兼容存储桶有效的合规性设置。 |
| "已弃用：PUT Bucket 合规性"        | 已弃用但受支持：允许您修改现有旧版兼容存储桶的合规性设置。   |

## 使用 GET Bucket 一致性请求检索 StorageGRID 中的存储桶一致性级别

通过获取存储桶一致性请求，可以确定应用到特定存储桶的一致性。

默认一致性设置为保证新创建对象的写后读一致性。

您必须具有 s3:GetBucketConsistency 权限，或者是账户 root 用户，才能完成此操作。

### 请求示例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

### 响应

在响应XML中，`<Consistency>`将返回以下值之一：

| 一致性           | 问题描述                                                                                                    |
|---------------|---------------------------------------------------------------------------------------------------------|
| all           | 所有节点立即接收数据，否则请求将失败。                                                                                     |
| strong-global | 保证所有站点上所有客户端请求的写后读一致性。                                                                                  |
| strong-site   | 保证站点内所有客户端请求的写后读一致性。                                                                                    |
| 新写入后立即读取      | (默认值) 为新对象提供写后读取一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议在大多数情况下使用。                                            |
| 可用            | 为新对象和对象更新提供最终一致性。对于 S3 存储桶，仅根据需要使用（例如，对于包含很少读取的日志值的存储桶，或者对于不存在的键的 HEAD 或 GET 操作）。不支持 S3 FabricPool 存储桶。 |

## 响应示例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

## 相关信息

["一致性"](#)

使用 **PUT Bucket** 一致性请求在 **StorageGRID** 中指定一致性级别

通过PUT Bucket一致性请求，可以指定要应用于对存储桶执行的操作的一致性。

默认一致性设置为保证新创建对象的写后读一致性。

## 开始之前

您必须具有 s3:PutBucketConsistency 权限或帐户根用户权限，才能完成此操作。

## 请求

The x-ntap-sg-consistency 参数必须包含以下其中一个值：

| 一致性           | 问题描述                                                                                                    |
|---------------|---------------------------------------------------------------------------------------------------------|
| all           | 所有节点立即接收数据，否则请求将失败。                                                                                     |
| strong-global | 保证所有站点上所有客户端请求的写后读一致性。                                                                                  |
| strong-site   | 保证站点内所有客户端请求的写后读一致性。                                                                                    |
| 新写入后立即读取      | (默认值) 为新对象提供写后读取一致性，并为对象更新提供最终一致性。提供高可用性和数据保护保证。建议在大多数情况下使用。                                            |
| 可用            | 为新对象和对象更新提供最终一致性。对于 S3 存储桶，仅根据需要使用（例如，对于包含很少读取的日志值的存储桶，或者对于不存在的键的 HEAD 或 GET 操作）。不支持 S3 FabricPool 存储桶。 |

注意：一般来说，您应该使用"新写后读"的一致性。如果请求无法正常工作，请尽可能更改应用程序客户端行为。或者，配置客户端以指定每个 API 请求的一致性。仅作为最后手段，在存储桶级别设置一致性。

#### 请求示例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### 相关信息

##### "一致性"

使用 **GET Bucket** 上次访问时间请求检索 **StorageGRID** 中的存储桶上次访问时间状态

通过获取存储区上次访问时间请求，您可以确定是否为单个存储区启用或禁用上次访问时间更新。

您必须具有 s3:GetBucketLastAccessTime 权限，或者是 account root，才能完成此操作。

#### 请求示例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 响应示例

此示例显示已为存储区启用上次访问时间更新。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

## 使用 **PUT Bucket** 上次访问时间请求在 **StorageGRID** 中启用和禁用上次访问时间更新

PUT Bucket 上次访问时间请求允许您为单个存储桶启用或禁用上次访问时间更新。禁用上次访问时间更新将提高性能，并且是使用 10.3.0 或更高版本创建的所有存储桶的默认设置。

要完成此操作，您必须具有存储桶的 s3:PutBucketLastAccessTime 权限，或者是帐户根用户。



从 StorageGRID 版本 10.3 开始，默认情况下对所有新存储桶禁用上次访问时间的更新。如果您有使用较早版本的 StorageGRID 创建的存储桶，并且希望匹配新的默认行为，则必须明确禁用每个较早存储桶的上次访问时间更新。您可以使用 PUT Bucket last access time 请求或从租户管理器中存储桶的详细信息页面启用或禁用上次访问时间的更新。请参阅["启用或禁用上次访问时间更新"](#)。

如果对存储桶禁用了上次访问时间更新，则将对存储桶上的操作应用以下行为：

- GetObject、GetObjectAcl、GetObjectTagging 和 HeadObject 请求不会更新上次访问时间。对象未添加到信息生命周期管理 (ILM) 评估队列中。
- CopyObject 和 PutObjectTagging 仅更新元数据的请求也会更新上次访问时间。该对象已添加到 ILM 评估队列。
- 如果对源存储桶禁用了对上次访问时间的更新，则 CopyObject 请求不会更新源存储桶的上次访问时间。已复制的对象未添加到源存储桶的 ILM 评估队列中。但是，对于目标，CopyObject 请求始终更新上次访问时间。对象的副本将添加到 ILM 评估队列中。
- CompleteMultipartUpload 请求更新上次访问时间。已完成的对象已添加到 ILM 评估队列。

## 请求示例

此示例启用存储桶的上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

此示例禁用存储区的上次访问时间。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 使用 **StorageGRID** 中的 **DELETE Bucket** 元数据通知配置请求禁用搜索集成服务

删除存储桶元数据通知配置请求用于通过删除配置 XML 来禁用单个存储桶的搜索集成服务。

要完成此操作，您必须具有存储桶的 `s3:DeleteBucketMetadataNotification` 权限，或者是账户根用户。

请求示例

此示例显示禁用存储区的搜索集成服务。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 使用 **GET Bucket** 元数据通知配置请求在 **StorageGRID** 中配置搜索集成

通过获取存储桶元数据通知配置请求，可以检索用于配置单个存储桶的搜索集成的配置 XML。

您必须具有 `s3:GetBucketMetadataNotification` 权限，或者是账户 root 用户，才能完成此操作。

请求示例

此请求检索名为 `'bucket'` 的存储桶的元数据通知配置。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 响应

响应正文包括存储区的元数据通知配置。通过元数据通知配置，您可以确定如何配置存储区以进行搜索集成。也就是说，它允许您确定哪些对象已编入索引，以及其对象元数据要发送到哪些端点。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

每个元数据通知配置包括一个或多个规则。每个规则指定其应用的对象以及 StorageGRID 应发送对象元数据的目标。必须使用 StorageGRID 端点的 URN 指定目标。

| 名称                                | 问题描述                                                                                                | 必填项 |
|-----------------------------------|-----------------------------------------------------------------------------------------------------|-----|
| MetadataNotificationConfiguration | 用于指定元数据通知的对象和目标的规则的容器标记。<br><br>包含一个或多个 Rule 元素。                                                    | 是   |
| 规则                                | 标识其元数据应添加到指定索引中的对象的规则的容器标记。<br><br>具有重叠前缀的规则将被拒绝。<br><br>包含在 MetadataNotificationConfiguration 元素中。 | 是   |

| 名称  | 问题描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 必填项 |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ID  | <p>规则的唯一标识符。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             | 否   |
| 状态  | <p>状态可以是"已启用"或"已禁用"。对于禁用的规则，不采取任何操作。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                                     | 是   |
| 前缀  | <p>匹配前缀的对象受规则影响，其元数据将发送到指定目的地。</p> <p>要匹配所有对象，请指定空前缀。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                    | 是   |
| 目标  | <p>规则目标的容器标记。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            | 是   |
| URN | <p>发送对象元数据的目标的 URN。必须具有以下属性的 StorageGRID 端点的 URN：</p> <ul style="list-style-type: none"> <li>• es 必须是第三个元素。</li> <li>• URN 必须以存储元数据的索引和类型结尾，格式为 domain-name/myindex/mytype。</li> </ul> <p>端点使用租户管理器或租户管理 API 进行配置。它们采用以下形式：</p> <ul style="list-style-type: none"> <li>• arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>必须在提交配置 XML 之前配置端点，否则配置将失败并出现 404 错误。</p> <p>Urn 包含在 Destination 元素中。</p> | 是   |

## 响应示例

```
`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>`
```

标签之间包含的 XML

显示了如何为存储桶配置与搜索集成端点的集成。在此示例中，对象元数据将发送到名为 `current` 的 Elasticsearch 索引和名为 `2017` 的类型，该索引和类型托管在名为 `records` 的 AWS 域中。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

## 相关信息

["使用租户帐户"](#)

## 使用 PUT Bucket 元数据通知配置请求在 StorageGRID 中启用搜索集成服务

PUT Bucket 元数据通知配置请求允许您为单个存储桶启用搜索集成服务。在请求正文中提供的元数据通知配置 XML 指定将元数据发送到目标搜索索引的对象。

要完成此操作，您必须具有存储桶的 s3:PutBucketMetadataNotification 权限，或者是账户根用户。

## 请求

请求必须在请求正文中包含元数据通知配置。每个元数据通知配置包括一个或多个规则。每个规则指定其应用的对象，以及 StorageGRID 应发送对象元数据的目标。

可以根据对象名称的前缀过滤对象。例如，您可以将具有前缀 /images 的对象的元数据发送到一个目标，并将具有前缀 /videos 的对象发送到另一个目标。

具有重叠前缀的配置无效，提交时将被拒绝。例如，不允许包含针对前缀为 `test` 的对象的一个规则以及针对前

缀为 `test2` 的对象的第二个规则的配置。

必须使用 StorageGRID 端点的 URN 指定目标。提交元数据通知配置时，端点必须存在，否则请求将失败，并返回 400 Bad Request。错误消息显示：Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

该表描述了元数据通知配置 XML 中的元素。

| 名称                                    | 问题描述                                                                                                    | 必填项 |
|---------------------------------------|---------------------------------------------------------------------------------------------------------|-----|
| MetadataNotificationConfi<br>guration | 用于指定元数据通知的对象和目标的规则的容器标<br>记。<br><br>包含一个或多个 Rule 元素。                                                    | 是   |
| 规则                                    | 标识其元数据应添加到指定索引中的对象的规则的容<br>器标记。<br><br>具有重叠前缀的规则将被拒绝。<br><br>包含在 MetadataNotificationConfiguration 元素中。 | 是   |
| ID                                    | 规则的唯一标识符。<br><br>包含在 Rule 元素中。                                                                          | 否   |
| 状态                                    | 状态可以是"已启用"或"已禁用"。对于禁用的规则，不<br>采取任何操作。<br><br>包含在 Rule 元素中。                                              | 是   |

| 名称  | 问题描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 必填项 |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 前缀  | <p>匹配前缀的对象受规则影响，其元数据将发送到指定目的地。</p> <p>要匹配所有对象，请指定空前缀。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                  | 是   |
| 目标  | <p>规则目标的容器标记。</p> <p>包含在 Rule 元素中。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          | 是   |
| URN | <p>发送对象元数据的目标的 URN。必须具有以下属性的 StorageGRID 端点的 URN：</p> <ul style="list-style-type: none"> <li>• es 必须是第三个元素。</li> <li>• URN 必须以存储元数据的索引和类型结尾，格式为 domain-name/myindex/mytype。</li> </ul> <p>端点使用租户管理器或租户管理 API 进行配置。它们采用以下形式：</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>必须在提交配置 XML 之前配置端点，否则配置将失败并出现 404 错误。</p> <p>Urn 包含在 Destination 元素中。</p> | 是   |

#### 请求示例

此示例显示对存储桶启用搜索集成。在此示例中，所有对象的对象元数据将发送到相同的目标。

```

PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

在此示例中，匹配前缀 `/images` 的对象的对象元数据将发送到一个目标，而匹配前缀 `/videos` 的对象的对象元数据将发送到第二个目标。

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

搜索集成服务生成的 JSON

为存储桶启用搜索集成服务时，每次添加、更新或删除对象元数据或标记时，都会生成 JSON 文档并将其发送到目标端点。

此示例显示了在名为 test 的存储桶中创建具有键 SGWS/Tagging.txt 的对象时可能生成的 JSON 示例。test 存储桶未启用版本控制，因此 versionId 标记为空。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

元数据通知中包含的对象元数据

该表列出了启用搜索集成时发送到目标端点的 JSON 文档中包含的所有字段。

文档名称包括存储桶名称、对象名称和版本 ID（如果存在）。

| 类型       | 项目名称      | 问题描述                      |
|----------|-----------|---------------------------|
| 存储桶和对象信息 | 存储分段      | 存储桶的名称                    |
| 存储桶和对象信息 | 密钥        | 对象密钥名称                    |
| 存储桶和对象信息 | versionID | 对象版本，适用于版本化存储桶中的对象        |
| 存储桶和对象信息 | 区域        | Bucket 区域，例如 us-east-1    |
| 系统元数据    | 大小        | 对象大小（以字节为单位），对 HTTP 客户端可见 |
| 系统元数据    | md5       | 对象哈希                      |

| 类型    | 项目名称                 | 问题描述                  |
|-------|----------------------|-----------------------|
| 用户元数据 | 元数据 <i>key:value</i> | 对象的所有用户元数据，作为键值对      |
| 标记    | 标签 <i>key:value</i>  | 为对象定义的所有对象标签，以键值对形式表示 |



对于标签和用户元数据，StorageGRID 将日期和数字作为字符串或 S3 事件通知传递给 Elasticsearch。要配置 Elasticsearch 将这些字符串解释为日期或数字，请按照 Elasticsearch 说明进行动态字段映射和映射日期格式。在配置搜索集成服务之前，必须在索引上启用动态字段映射。为文档编制索引后，您无法在索引中编辑文档的字段类型。

## 相关信息

["使用租户帐户"](#)

## 使用 **GET Storage Usage** 请求检索 **StorageGRID** 中的帐户和存储桶存储使用情况

GET Storage Usage 请求会告诉您帐户使用的总存储量以及与帐户关联的每个存储桶的总存储量。

可以通过使用带有 `x-ntap-sg-usage` 查询参数的修改版 ListBuckets 请求来获取帐户及其存储桶所使用的存储量。存储桶存储使用情况与系统处理的 PUT 和 DELETE 请求分开跟踪。根据请求的处理情况，使用值与预期值匹配之前可能会有一些延迟，尤其是在系统负载较重的情况下。

默认情况下，StorageGRID 尝试使用强全局一致性检索使用信息。如果无法实现强全局一致性，StorageGRID 尝试以强站点一致性检索使用信息。

要完成此操作，您必须具有 `s3:ListAllMyBuckets` 权限，或者是账户根用户。

## 请求示例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 响应示例

此示例显示了一个帐户，该帐户在两个存储桶中具有四个对象和 12 个字节的数据。每个存储桶包含两个对象和六个字节的数据。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

## 版本控制

存储的每个对象版本都将计入响应中的 `ObjectCount` 和 `DataBytes` 值。删除标记不会计入 `ObjectCount` 总数。

## 相关信息

["一致性"](#)

## 旧版合规性的已弃用存储桶请求

### 旧版 **StorageGRID** 合规性的已弃用存储桶请求

您可能需要使用 StorageGRID S3 REST API 来管理使用旧版合规性功能创建的存储桶。

### 合规性功能已弃用

以前的 StorageGRID 版本中提供的 StorageGRID 合规性功能已被弃用，并已被 S3 Object Lock 所取代。

如果您之前启用了全局合规性设置，则在 StorageGRID 11.6 中启用了全局 S3 对象锁定设置。您不能再创建启

用合规性的新存储桶；但是，根据需要，您可以使用 StorageGRID S3 REST API 管理任何现有的旧合规性存储桶。

- ["使用 S3 REST API 配置 S3 对象锁定"](#)
- ["使用 ILM 管理对象"](#)
- ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)

已弃用的合规性请求：

- ["已弃用 - PUT Bucket 请求修改以实现合规性"](#)

SGCompliance XML 元素已弃用。以前，您可以将此 StorageGRID 自定义元素包含在 PUT Bucket 请求的可选 XML 请求正文中，以创建 Compliant 存储桶。

- ["已弃用 - GET Bucket compliance"](#)

GET Bucket 合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版兼容存储桶有效的合规性设置。

- ["已弃用 - PUT Bucket 合规性"](#)

PUT Bucket 合规性请求已弃用。但是，您可以继续使用此请求来修改现有旧版合规存储桶的合规性设置。例如，您可以将现有存储桶置于法律保留状态或延长其保留期。

### StorageGRID 中已弃用的 SGCompliance 元素

SGCompliance XML 元素已弃用。以前，您可以在 CreateBucket 请求的可选 XML 请求正文中包含此 StorageGRID 自定义元素，以创建合规存储桶。



以前的 StorageGRID 版本中提供的 StorageGRID 合规性功能已被弃用，并已被 S3 Object Lock 所取代。有关更多详细信息，请参见以下内容：

- ["使用 S3 REST API 配置 S3 对象锁定"](#)
- ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)

您无法再创建启用了合规性的新存储桶。如果您尝试使用 CreateBucket 请求修改来创建新的合规存储桶，将返回以下错误消息：

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

### StorageGRID 中已弃用的 GET Bucket compliance 请求

GET Bucket 合规性请求已弃用。但是，您可以继续使用此请求来确定当前对现有旧版兼容存储桶有效的合规性设置。



以前的 StorageGRID 版本中提供的 StorageGRID 合规性功能已被弃用，并已被 S3 Object Lock 所取代。有关更多详细信息，请参见以下内容：

- ["使用 S3 REST API 配置 S3 对象锁定"](#)
- ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)

要完成此操作，您必须具有 `s3:GetBucketCompliance` 权限，或者是账户根用户。

请求示例

此示例请求允许您确定名为 ``mybucket`` 的存储桶的合规性设置。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

响应示例

在响应 XML 中，`<SGCompliance>` 列出了存储桶的有效合规性设置。此示例响应显示存储桶的合规性设置，其中每个对象将保留一年（525,600 分钟），从对象被载入网格时开始计算。此存储桶当前没有合法保留。每个对象将在一年后自动删除。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

| 名称                     | 问题描述                                     |
|------------------------|------------------------------------------|
| RetentionPeriodMinutes | 添加到此存储桶的对象的保留期长度，以分钟为单位。保留期从对象载入网格时开始计算。 |

| 名称         | 问题描述                                                                                                                                                         |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LegalHold  | <ul style="list-style-type: none"> <li>• True：此存储桶当前处于合法冻结状态。在解除法律保留之前，无法删除此存储桶中的对象，即使其保留期已过。</li> <li>• 错误：此存储桶当前未处于合法冻结状态。此存储桶中的对象可以在其保留期到期时删除。</li> </ul> |
| AutoDelete | <ul style="list-style-type: none"> <li>• True：此存储桶中的对象将在其保留期到期时自动删除，除非存储桶处于合法冻结状态。</li> <li>• 错误：当保留期到期时，不会自动删除此存储桶中的对象。如果需要删除这些对象，则必须手动删除它们。</li> </ul>     |

#### 错误响应

如果存储桶未创建为合规，则响应的 HTTP 状态代码为 404 Not Found，S3 错误代码为 XNoSuchBucketCompliance。

#### StorageGRID 中已弃用的 PUT Bucket compliance 请求

PUT Bucket 合规性请求已弃用。但是，您可以继续使用此请求来修改现有旧版合规存储桶的合规性设置。例如，您可以将现有存储桶置于法律保留状态或延长其保留期。



以前的 StorageGRID 版本中提供的 StorageGRID 合规性功能已被弃用，并已被 S3 Object Lock 所取代。有关更多详细信息，请参见以下内容：

- ["使用 S3 REST API 配置 S3 对象锁定"](#)
- ["NetApp 知识库：如何在 StorageGRID 11.5 中管理旧版兼容存储桶"](#)

您必须具有 s3:PutBucketCompliance 权限或帐户根用户身份，才能完成此操作。

发出 PUT Bucket 合规性请求时，必须为合规性设置的每个字段指定一个值。

#### 请求示例

此示例请求修改名为 `mybucket` 的存储桶的合规性设置。在此示例中，`mybucket` 中的对象现在将从对象被载入网格时起保留两年（1,051,200 分钟），而不是一年。此存储桶没有合法保留。每个对象将在两年后自动删除。

```

PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

| 名称                     | 问题描述                                                                                                                                                         |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RetentionPeriodMinutes | <p>添加到此存储桶的对象的保留期长度，以分钟为单位。保留期从对象载入网格时开始计算。</p> <p>重要提示 为 RetentionPeriodMinutes 指定新值时，必须指定等于或大于存储桶当前保留期的值。设置存储桶的保留期后，您不能降低该值，只能增加该值。</p>                    |
| LegalHold              | <ul style="list-style-type: none"> <li>• True：此存储桶当前处于合法冻结状态。在解除法律保留之前，无法删除此存储桶中的对象，即使其保留期已过。</li> <li>• 错误：此存储桶当前未处于合法冻结状态。此存储桶中的对象可以在其保留期到期时删除。</li> </ul> |
| AutoDelete             | <ul style="list-style-type: none"> <li>• True：此存储桶中的对象将在其保留期到期时自动删除，除非存储桶处于合法冻结状态。</li> <li>• 错误：当保留期到期时，不会自动删除此存储桶中的对象。如果需要删除这些对象，则必须手动删除它们。</li> </ul>     |

#### 合规性设置的一致性

当您使用 PUT Bucket 合规性请求更新 S3 存储桶的合规性设置时，StorageGRID 尝试跨网格更新存储桶的元数据。默认情况下，StorageGRID 使用 **Strong-global** 一致性来保证所有数据中心站点和包含存储桶元数据的所有存储节点具有更改后的合规性设置的写后读一致性。

如果由于一个数据中心站点或站点上的多个存储节点不可用，StorageGRID 无法实现 **Strong-global** 一致性，则响应的 HTTP 状态代码为 503 Service Unavailable。

如果您收到此响应，则必须联系网格管理员，以确保尽快提供所需的存储服务。如果网格管理员无法在每个站点提供足够的存储节点，技术支持可能会指导您通过强制 **Strong-site** 一致性来重试失败的请求。



除非技术支持指示您这样做，并且您了解使用此级别的潜在后果，否则切勿强制 **Strong-site** 一致性用于 PUT bucket 合规性。

当一致性降低到 **Strong-site** 时，StorageGRID 保证更新后的合规性设置仅对站点内的客户端请求具有写后读一致性。这意味着，在所有站点和存储节点可用之前，StorageGRID 系统可能暂时对此存储桶具有多个不一致的设置。设置不一致可能会导致意外和不良行为。例如，如果您将存储桶置于法律保留状态，并强制执行较低的一致性，则存储桶以前的合规性设置（即关闭法律保留）可能在某些数据中心站点继续有效。因此，当保留期到期时，您认为处于法律保留状态的对象可能会被用户或 AutoDelete（如果已启用）删除。

要强制使用 **Strong-site** 一致性，请重新发出 PUT Bucket 合规性请求并包含 Consistency-Control HTTP 请求标头，如下所示：

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

#### 错误响应

- 如果存储区未创建为合规，则响应的 HTTP 状态代码为 404 Not Found。
- 如果请求中的 RetentionPeriodMinutes 小于存储桶的当前保留期，则 HTTP 状态代码为 400 Bad Request。

#### 相关信息

["已弃用：PUT Bucket 请求修改以实现合规性"](#)

## 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。                                                                                                              |
| 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     | <p>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。</p> <p>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。</p> |
| 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 个或多个字符，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<br><br>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                     |

| 权限                                  | S3 REST API 操作                                                                                           | 自定义<br>StorageGRID                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------|
| 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                                                                                        |                                             |
| 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                 | <ul style="list-style-type: none"> <li>ListBuckets</li> <li>获取存储使用情况</li> </ul>                          | 是，用于 GET Storage Usage。<br><br>注意：仅在组策略中使用。 |
| s3:ListBucket                       | <ul style="list-style-type: none"> <li>ListObjects</li> <li>HeadBucket</li> <li>RestoreObject</li> </ul> |                                             |
| s3:ListBucketMultipartUploads       | <ul style="list-style-type: none"> <li>ListMultipartUploads</li> <li>RestoreObject</li> </ul>            |                                             |
| s3:ListBucketVersions               | GET 存储桶版本                                                                                                |                                             |

| 权限                                  | S3 REST API 操作                                                                                                                                                              | 自定义 StorageGRID      |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| s3:PutBucketCompliance              | PUT Bucket compliance（已弃用）                                                                                                                                                  | 是                    |
| s3:PutBucketConsistency             | PUT Bucket 一致性                                                                                                                                                              | 是                    |
| s3:PutBucketCORS                    | <ul style="list-style-type: none"> <li>DeleteBucketCors†</li> <li>PutBucketCors</li> </ul>                                                                                  |                      |
| s3:PutEncryptionConfiguration       | <ul style="list-style-type: none"> <li>DeleteBucketEncryption</li> <li>PutBucketEncryption</li> </ul>                                                                       |                      |
| 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 | <ul style="list-style-type: none"> <li>CreateBucket 带有 `x-amz-bucket-object-lock-enabled: true` 请求标头（也需要 s3:CreateBucket 权限）</li> <li>PutObjectLockConfiguration</li> </ul> |                      |
| s3: PutBucketPolicy                 | PutBucketPolicy                                                                                                                                                             |                      |
| s3: PutBucketTagging                | <ul style="list-style-type: none"> <li>DeleteBucketTagging†</li> <li>PutBucketTagging</li> </ul>                                                                            |                      |
| s3:PutBucketVersioning              | PutBucketVersioning                                                                                                                                                         |                      |
| s3:PutLifecycleConfiguration        | <ul style="list-style-type: none"> <li>DeleteBucketLifecycle†</li> <li>PutBucketLifecycleConfiguration</li> </ul>                                                           |                      |
| 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 | <ul style="list-style-type: none"> <li>AbortMultipartUpload</li> <li>RestoreObject</li> </ul> |                 |

| 权限                            | S3 REST API 操作                                                                                                                         | 自定义<br>StorageGRID |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| s3:BypassGovernanceRetention  | <ul style="list-style-type: none"> <li>• 删除对象</li> <li>• DeleteObjects</li> <li>• PutObjectRetention</li> </ul>                        |                    |
| s3:DeleteObject               | <ul style="list-style-type: none"> <li>• 删除对象</li> <li>• DeleteObjects</li> <li>• RestoreObject</li> </ul>                             |                    |
| 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                  | <ul style="list-style-type: none"> <li>• 获取对象</li> <li>• HeadObject</li> <li>• RestoreObject</li> <li>• SelectObjectContent</li> </ul> |                    |
| 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                                                                                                               |                    |

| 权限                         | S3 REST API 操作                                                                                                                                                                                                              | 自定义 StorageGRID |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| s3:PutObject               | <ul style="list-style-type: none"> <li>• 放置对象</li> <li>• CopyObject</li> <li>• RestoreObject</li> <li>• CreateMultipartUpload</li> <li>• CompleteMultipartUpload</li> <li>• UploadPart</li> <li>• UploadPartCopy</li> </ul> |                 |
| s3:PutObjectLegalHold      | PutObjectLegalHold                                                                                                                                                                                                          |                 |
| s3:PutObjectRetention      | PutObjectRetention                                                                                                                                                                                                          |                 |
| s3:PutObjectTagging        | PutObjectTagging                                                                                                                                                                                                            |                 |
| s3:PutObjectVersionTagging | PutObjectTagging（对象的特定版本）                                                                                                                                                                                                   |                 |
| s3:PutOverwriteObject      | <ul style="list-style-type: none"> <li>• 放置对象</li> <li>• CopyObject</li> <li>• PutObjectTagging</li> <li>• DeleteObjectTagging</li> <li>• CompleteMultipartUpload</li> </ul>                                                | 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 and 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）。  |

| 条件运算符                     | 问题描述                                                  |
|---------------------------|-------------------------------------------------------|
| 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。                                     |
| 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                                                                                                                                                                                                                                                                                             | <p>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。</p> <p>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。</p> <p><b>Note：</b>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。</p> |
| 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<br>s3:ListBucketVersions 权限                                                                                                                                                                                                                                                       | 将与ListObjects或ListObjectVersions请求中指定的分隔符参数进行比较。                                                                                                                                                           |
| s3:ExistingObjectTag/<tag-key> | s3:DeleteObjectTagging<br>s3:DeleteObjectVersionTagging<br>s3:GetObject<br>s3:GetObjectAcl<br>s3:GetObjectTagging<br>s3:GetObjectVersion<br>s3:GetObjectVersionAcl<br>s3:GetObjectVersionTagging<br>s3:PutObjectAcl<br>s3:PutObjectTagging<br>s3:PutObjectVersionAcl<br>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<br>s3:ListBucketVersions 权限                                                                                                                                                                                                                                                       | 将与 ListObjects 或 ListObjectVersions 请求中指定的 max-keys 参数进行比较。                                                                                                                                                |

| 条件键                                                | 操作                                                                | 问题描述                                                                                                                                                                                                                     |
|----------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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： <ul style="list-style-type: none"> <li>• 放置对象</li> <li>• CopyObject</li> <li>• CreateMultipartUpload</li> </ul> |
| 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。                                                                                                                                                                       |
| s3:prefix                                          | s3:ListBucket 以及<br>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<br>s3:PutObjectTagging<br>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                        |
|-------------------------------|-----------------------------|
| <code>\${aws:SourceIp}</code> | 使用 SourceIp 键作为提供的变量。       |
| <code>\${aws:username}</code> | 使用用户名密钥作为提供的变量。             |
| <code>\${s3:prefix}</code>    | 使用特定于服务的前缀键作为提供的变量。         |
| <code>\${s3:max-keys}</code>  | 使用特定于服务的 max-keys 键作为提供的变量。 |
| <code>\${*}</code>            | 特殊字符。使用字符作为字面 * 字符。         |
| <code>\${?}</code>            | 特殊字符。使用字符作为字面 ? 字符。         |
| <code>\${\$}</code>           | 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 |

| 策略说明                       | 策略类型 | Amazon 行为                                                          | StorageGRID 行为            |
|----------------------------|------|--------------------------------------------------------------------|---------------------------|
| 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 and 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}/*"
    }
  ]
}
```

## StorageGRID 审核日志中跟踪的 S3 操作

审核消息由 StorageGRID 服务生成并存储在文本日志文件中。您可以在审核日志中查看 S3 特定的审核消息，以获取有关存储区和对象操作的详细信息。

### 在审核日志中跟踪的存储桶操作

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- PUT Bucket compliance
- PutBucketTagging
- PutBucketVersioning

## 审计日志中跟踪的对象操作

- CompleteMultipartUpload
- CopyObject
- 删除对象
- 获取对象
- HeadObject
- 放置对象
- RestoreObject
- SelectObject
- UploadPart （当 ILM 规则使用平衡或严格摄取时）
- UploadPartCopy （当 ILM 规则使用平衡或严格摄取时）

### 相关信息

- ["访问审核日志文件"](#)
- ["客户端写入审核消息"](#)
- ["客户端读取审核消息"](#)

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。