对对象执行的操作
StorageGRID 11.5

NetApp
April 11, 2024

目录

对对象执行的操作

本节介绍 StorageGRID 系统如何对对象实施 S3 REST API 操作。

- "使用 S3 对象锁定"
- "使用服务器端加密"
- "获取对象"
- "HEAD 对象"
- "后对象还原"
- "PUT 对象"
- "PUT 对象—复制"

以下条件适用于所有对象操作：

- 对对象执行的所有操作均支持StorageGRID 一致性控制、但以下操作除外：
  - 获取对象 ACL
  - `OPTIONS /`
  - PUT 对象合法保留
  - 放置对象保留
- 冲突的客户端请求(例如、两个客户端写入同一密钥)将按"`latest-WINS`"的原则进行解决。"`latest-WINS`"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 存储分段中的所有对象均归存储分段所有者所有，包括由匿名用户或其他帐户创建的对象。
- 无法通过 S3 访问通过 Swift 载入到 StorageGRID 系统的数据对象。

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

操作	实施
删除对象	多因素身份验证(MFA)和响应标头 `x-amz-mfa` 不支持。 在处理删除对象请求时， StorageGRID 会尝试立即从所有存储位置删除此对象的所有副本。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），则 StorageGRID 会将这些副本排队等待删除，然后指示客户端成功删除。 • 版本控制 * 要删除特定版本、请求者必须是存储分段所有者并使用 `versionId` 子资源。使用此子资源将永久删除此版本。如果 `versionId` 对应于删除标记、即响应标头 `x-amz-delete-marker` 返回时设置为 `true`。 • 删除对象时不使用 `versionId` 子资源在已启用版本的存储分段上、将生成删除标记。。`versionId` 对于删除标记、使用返回 `x-amz-version-id` 响应标头和 `x-amz-delete-marker` 返回的响应标头设置为 `true`。 • 删除对象时不使用 `versionId` 子资源在版本暂停的分段上、它会永久删除已存在的"null"版本或"null"删除标记、并生成新的"null"删除标记。。`x-amz-delete-marker` 返回的响应标头设置为 `true`。 • 注意 *：在某些情况下，一个对象可能存在多个删除标记。
删除多个对象	多因素身份验证(MFA)和响应标头 `x-amz-mfa` 不支持。 可以在同一请求消息中删除多个对象。
删除对象标记	使用 `tagging` 用于从对象中删除所有标记的子资源。在所有 Amazon S3 REST API 行为下实施。 • 版本控制 * 如果 `versionId` 请求中未指定查询参数、此操作将从受版本控制的存储分段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为删除标记、则会使用返回`MethodNotAllowed`状态 `x-amz-delete-marker` 响应标头设置为 `true`。
获取对象	"获取对象"

操作	实施
获取对象 ACL	如果为帐户提供了必要的访问凭据，则此操作将返回肯定响应以及对象所有者的 ID ， DisplayName 和权限，指示所有者对对象具有完全访问权限。
获取对象合法保留	"使用 S3 对象锁定"
获取对象保留	"使用 S3 对象锁定"
获取对象标记	使用 `tagging` 子资源以返回对象的所有标记。在所有 Amazon S3 REST API 行为下实施 • 版本控制 * 如果 `versionId` 请求中未指定查询参数、此操作将返回受版本控制的存储分段中对象的最新版本中的所有标记。如果对象的当前版本为删除标记、则会使用返回`MethodNotAllowed`状态 `x-amz-delete-marker` 响应标头设置为 `true`。
HEAD 对象	"HEAD 对象"
后对象还原	"后对象还原"
PUT 对象	"PUT 对象"
PUT 对象—复制	"PUT 对象—复制"
PUT 对象合法保留	"使用 S3 对象锁定"
放置对象保留	"使用 S3 对象锁定"

操作	实施
PUT 对象标记	使用 `tagging` 用于向现有对象添加一组标记的子资源。在所有 Amazon S3 REST API 行为下实施 • 标记更新和载入行为 * 使用 PUT 对象标记更新对象的标记时， StorageGRID 不会重新载入对象。这意味着不会使用匹配 ILM 规则中指定的 " 载入行为 " 选项。通过正常后台 ILM 进程重新评估 ILM 时，更新触发的任何对象放置更改都会进行。 这意味着，如果 ILM 规则对载入行为使用严格选项，则在无法放置所需对象时（例如，由于新需要的位置不可用），不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。 • 解决冲突 * 冲突的客户端请求(例如、两个客户端写入同一密钥)将按"`latest-WINS`"的原则进行解决。"`latest-WINS`"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。 • 版本控制 * 如果 `versionId` 未在此请求中指定查询参数、此操作会将标记添加到受版本控制的存储分段中的对象的最新版本。如果对象的当前版本为删除标记、则会使用返回`MethodNotAllowed`状态 `x-amz-delete-marker` 响应标头设置为 `true`。

相关信息

"一致性控制"

"审核日志中跟踪的 S3 操作"

使用 S3 对象锁定

如果为 StorageGRID 系统启用了全局 S3 对象锁定设置，则可以在启用了 S3 对象锁定的情况下创建存储分段，然后为添加到存储分段的每个对象版本指定保留日期和合法保留设置。

通过 S3 对象锁定，您可以指定对象级别的设置，以防止对象在固定时间内或无限期地被删除或覆盖。

StorageGRID S3 对象锁定功能提供了一种保留模式，相当于 Amazon S3 合规模式。默认情况下，任何用户都无法覆盖或删除受保护的对象版本。StorageGRID S3 对象锁定功能不支持监管模式，并且不允许具有特殊权限的用户绕过保留设置或删除受保护的对象。

为存储分段启用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分段时启用 S3 对象锁定。您可以使用以下任一方法：

- 使用租户管理器创建存储分段。

  "使用租户帐户"

- 使用PUT Bucket请求和创建存储分段 `x-amz-bucket-object-lock_enabled` 请求标题。

  "对存储分段执行的操作"

创建存储分段后，您无法添加或禁用 S3 对象锁定。S3 对象锁定需要分段版本控制，在创建分段时会自动启用分段版本控制。

启用了 S3 对象锁定的存储分段可以包含具有和不具有 S3 对象锁定设置的对象组合。StorageGRID 不支持S3对象锁定分段中的对象的默认保留、因此不支持PUT对象锁定配置分段操作。

确定是否为存储分段启用了S3对象锁定

要确定是否已启用S3对象锁定、请使用获取对象锁定配置请求。

"对存储分段执行的操作"

使用S3对象锁定设置创建对象

要在将对象版本添加到启用了 S3 对象锁定的存储分段时指定 S3 对象锁定设置，请问题描述 对 PUT 对象，PUT 对象 - 复制或启动多部件上传请求。请使用以下请求标头。

> 创建存储分段时，必须启用 S3 对象锁定。创建存储分段后，您无法添加或禁用 S3 对象锁定。

- `x-amz-object-lock-mode`、必须符合要求(区分大小写)。

  > 如果指定 `x-amz-object-lock-mode`、您还必须指定 `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
  - 保留截止日期值必须采用格式 `2020-08-10T21:46:00Z`。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 保留截止日期必须为未来日期。
- `x-amz-object-lock-legal-hold`

  如果处于合法保留状态（区分大小写），则对象将置于合法保留状态。如果关闭了合法保留，则不会进行合法保留。任何其他值都会导致 400 错误请求（ InvalidArgument ）错误。

如果您使用上述任一请求标头，请注意以下限制：

- 。 `Content-MD5` 如果有、则请求标头为必填项 `x-amz-object-lock-*` PUT对象请求中存在请求标头。 `Content-MD5` PUT对象-复制或启动多部件上传不需要。
- 如果存储分段未启用S3对象锁定和 `x-amz-object-lock-*` 存在请求标头、返回400错误请求(InvalidRequest)错误。
- PUT对象请求支持使用 `x-amz-storage-class: REDUCED_REDUNDANCY` 以匹配AWS行为。但是，如果在启用了 S3 对象锁定的情况下将对象载入存储分段，则 StorageGRID 将始终执行双提交载入。
- 后续的GET或HEAD对象版本响应将包括标题 `x-amz-object-lock-mode`， `x-amz-object-lock-retain-until-date`，和 `x-amz-object-lock-legal-hold`(如果已配置)以及请求发送方是否正确 `s3:Get*` 权限。
- 如果后续的删除对象版本或删除对象版本请求早于保留截止日期或处于合法保留状态，则此请求将失败。

正在更新**S3**对象锁定设置

如果需要更新现有对象版本的合法保留或保留设置，可以执行以下对象子资源操作：

- `PUT Object legal-hold`

  如果新的合法保留值为 on ，则对象将置于合法保留状态。如果合法保留值为 off ，则取消合法保留。

- `PUT Object retention`
  - 模式值必须符合要求（区分大小写）。
  - 保留截止日期值必须采用格式 `2020-08-10T21:46:00Z`。允许使用小数秒，但仅保留 3 位小数（精确度为毫秒）。不允许使用其他 ISO 8601 格式。
  - 如果对象版本具有现有的保留日期，则只能增加此保留日期。新的价值必须是未来的。

相关信息

"使用 ILM 管理对象"

"使用租户帐户"

"PUT 对象"

"PUT 对象—复制"

"启动多部件上传"

"对象版本控制"

"《 Amazon Simple Storage Service 用户指南：使用 S3 对象锁定》"

使用服务器端加密

服务器端加密可用于保护空闲对象数据。StorageGRID 会在写入对象时对数据进行加密，并在您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从两个互斥选项中选择任一选项：

- *SSE （使用 StorageGRID 管理的密钥进行服务器端加密） *：在问题描述 S3 请求以存储对象时，StorageGRID 会使用唯一密钥对对象进行加密。在问题描述 S3 请求以检索对象时， StorageGRID 会使用存储的密钥对对象进行解密。
- * SSI-C （使用客户提供的密钥进行服务器端加密） *：在问题描述 S3 请求以存储对象时，您可以提供自己的加密密钥。检索对象时，您可以在请求中提供相同的加密密钥。如果这两个加密密钥匹配，则会对对象进行解密，并返回您的对象数据。

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

  您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

  如果使用 SSE 或 SSI-C 对对象进行加密，则会忽略任何分段级别或网格级别的加密设置。

使用SSe.

要使用 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
```

以下对象操作支持此命令头：

- PUT 对象
- PUT 对象—复制
- 启动多部件上传

使用SSE-C

要使用您管理的唯一密钥对对象进行加密，请使用三个请求标头：

请求标题	Description
`x-amz-server-side-encryption-customer-algorithm`	指定加密算法。标题值必须为 `AES256`。
`x-amz-server-side-encryption-customer-key`	指定用于对对象进行加密或解密的加密密钥。密钥的值必须为 256 位 base64 编码。
`x-amz-server-side-encryption-customer-key-MD5`	根据 RFC 1321 指定加密密钥的 MD5 摘要，用于确保加密密钥的传输没有错误。MD5 摘要的值必须为 base64 编码的 128 位。

以下对象操作支持 SSI-C 请求标头：

- 获取对象
- HEAD 对象
- PUT 对象

- PUT 对象—复制
- 启动多部件上传
- 上传部件
- 上传部件—复制

将服务器端加密与客户提供的密钥（ **SSI-C** ）结合使用的注意事项

在使用 SSI-C 之前，请注意以下注意事项：

- 必须使用 https 。

> 使用 SSI-C 时， StorageGRID 会拒绝通过 http 发出的任何请求出于安全考虑，您应考虑使用 http 意外发送的任何密钥受到损坏。丢弃该密钥，并根据需要旋转。

- 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。您负责跟踪为每个对象提供的加密密钥。
- 如果您的存储分段已启用版本控制，则每个对象版本都应具有自己的加密密钥。您负责跟踪每个对象版本使用的加密密钥。
- 由于您在客户端上管理加密密钥，因此您还必须在客户端上管理任何其他保护措施，例如密钥轮换。

> 您提供的加密密钥永远不会存储。如果丢失加密密钥，则会丢失相应的对象。

- 如果为存储分段配置了 CloudMirror 复制，则无法载入 SSI-C 对象。载入操作将失败。

相关信息

"获取对象"

"HEAD 对象"

"PUT 对象"

"PUT 对象—复制"

"启动多部件上传"

"上传部件"

"上传部件—复制"

"Amazon S3 开发人员指南：使用客户提供的加密密钥（ SSI-C ）使用服务器端加密保护数据"

获取对象

您可以使用 S3 GET 对象请求从 S3 存储分段检索对象。

不支持partnumber请求参数

。 `partNumber` GET对象请求不支持请求参数。您不能执行获取请求来检索多部件对象的特定部分。返回501未实施错误、并显示以下消息：

```
GET Object by partNumber is not implemented
```

使用客户提供的加密密钥（ SSI-C ）进行服务器端加密的请求标头

如果使用您提供的唯一密钥对对象进行加密，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。

> 您提供的加密密钥永远不会存储。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"`使用服务器端加密中的注意事项。`

用户元数据中的 UTF-8 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。对于用户定义的元数据中存在转义UTF-8字符的对象、获取请求不会返回 `x-amz-missing-meta` 如果密钥名称或值包含不可打印的字符、则为标题。

请求标头不受支持

不支持以下请求标头、并返回 `XNotImplemented`：

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

版本控制

如果为 `versionId` 未指定子资源、此操作将提取受版本控制的存储分段中的对象的最新版本。如果对象的当前版本为删除标记、则会使用返回"`not found`"状态 `x-amz-delete-marker` 响应标头设置为 `true`。

Cloud Storage Pool 对象的 GET 对象行为

如果某个对象已存储在云存储池中（请参见有关通过信息生命周期管理来管理对象的说明），则 GET 对象请求的行为取决于对象的状态。有关详细信息，请参见 "`head Object` " 。

> 如果某个对象存储在云存储池中，并且该对象的一个或多个副本也位于网格中，则获取对象请求将尝试从网格中检索数据，然后再从云存储池中检索数据。

对象的状态	**GET** 对象的行为
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200 OK` 检索对象的副本。
云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK` 检索对象的副本。
对象已过渡到无法检索的状态	`403 Forbidden， InvalidObjectState` 使用 POST 对象还原请求将对象还原到可检索的状态。
正在从不可检索状态还原的对象	`403 Forbidden， InvalidObjectState` 等待 POST 对象还原请求完成。
对象已完全还原到云存储池	`200 OK` 检索对象的副本。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下、可能会错误地返回GET对象请求 `200 OK` 对象的某些部分已过渡到无法检索的状态、或者对象的某些部分尚未还原。

在这些情况下：

- GET 对象请求可能会返回一些数据，但会在传输过程中停止。
- 可能会返回后续的GET对象请求 `403 Forbidden`。

相关信息

"使用服务器端加密"

"使用 ILM 管理对象"

"后对象还原"

"审核日志中跟踪的 S3 操作"

HEAD 对象

您可以使用 S3 head Object 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 head 对象确定对象的过渡状态。

使用客户提供的加密密钥（ SSI-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进行加密，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。

> 您提供的加密密钥永远不会存储。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"`使用服务器端加密中的注意事项。`

用户元数据中的 UTF-8 字符

StorageGRID 不会解析或解释用户定义的元数据中的转义 UTF-8 字符。对于用户定义的元数据中具有转义UTF-8字符的对象、如果对该对象发出机头请求、则不会返回 `x-amz-missing-meta` 如果密钥名称或值包含不可打印的字符、则为标题。

请求标头不受支持

不支持以下请求标头、并返回 `XNotImplemented`：

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

Cloud Storage Pool 对象的响应标头

如果对象存储在云存储池中（请参见有关通过信息生命周期管理来管理对象的说明），则返回以下响应标头：

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

响应标头提供了有关对象移动到云存储池，可选择过渡到不可检索状态并已还原时的状态的信息。

对象的状态	对 **head** 对象的响应
对象已载入 StorageGRID 但尚未通过 ILM 进行评估，或者存储在传统存储池中的对象或使用纠删编码	`200 OK` (不返回任何特殊的响应标头。)

云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	在将对象过渡到无法检索的状态之前、为提供的值 `expiry-date` 设置为未来的某个远程时间。确切的过渡时间不受 StorageGRID 系统控制。

对象的状态	对 **head** 对象的响应

对象已过渡到不可检索状态，但网格上至少也存在一个副本	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	的值 `expiry-date` 设置为未来的某个远程时间。
	
	• 注意 *：如果网格上的副本不可用（例如，存储节点已关闭），则必须先对后对象还原请求进行问题描述 处理，以便从云存储池还原此副本，然后才能成功检索此对象。

对象已过渡到无法检索的状态，网格上不存在任何副本	`200 OK`
	
	`x-amz-storage-class: GLACIER`

正在从不可检索状态还原的对象	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

对象已完全还原到云存储池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	。 `expiry-date` 指示何时将云存储池中的对象返回到无法检索的状态。

云存储池中的多部分或分段对象

如果您上传的是多部分对象或 StorageGRID 将一个大型对象拆分为多个区块，则 StorageGRID 会通过取样该对象的部分或区块来确定该对象是否在云存储池中可用。在某些情况下、可能会错误地返回HEAD对象请求 `x-amz-restore: ongoing-request="false"` 对象的某些部分已过渡到无法检索的状态、或者对象的某些部分尚未还原。

版本控制

如果为 `versionId` 未指定子资源、此操作将提取受版本控制的存储分段中的对象的最新版本。如果对象的当前版本为删除标记、则会使用返回"`not found`"状态 `x-amz-delete-marker` 响应标头设置为 `true`。

相关信息

"使用服务器端加密"

"使用 ILM 管理对象"

"后对象还原"

"审核日志中跟踪的 S3 操作"

后对象还原

您可以使用 S3 后对象还原请求还原存储在云存储池中的对象。

支持的请求类型

StorageGRID 仅支持后对象还原请求来还原对象。它不支持 `SELECT` 还原类型。选择返回请求 `XNotImplemented`。

版本控制

(可选)指定 `versionId` 还原受版本控制的存储分段中特定版本的对象。如果未指定 `versionId`、将还原对象的最新版本

对云存储池对象执行后对象还原的行为

如果某个对象存储在云存储池中（请参见有关通过信息生命周期管理管理来管理对象的说明），则根据对象的状态，后对象还原请求具有以下行为。有关详细信息，请参见 "`head Object` " 。

> 如果某个对象存储在云存储池中，并且该对象的一个或多个副本也位于网格中，则无需发出后对象还原请求来还原该对象。相反，可以使用 GET 对象请求直接检索本地副本。

对象的状态	**POST** 对象还原的行为
对象已载入 StorageGRID ，但尚未通过 ILM 进行评估，或者对象不在云存储池中	`403 Forbidden， InvalidObjectState`
云存储池中的对象，但尚未过渡到无法检索的状态	`200 OK` 不会进行任何更改。 注意：在将对象过渡到无法检索的状态之前、您无法更改其 `expiry-date`。

对象的状态	**POST** 对象还原的行为
对象已过渡到无法检索的状态	`202 Accepted` 在请求正文中指定的天数内将对象的可检索副本还原到云存储池。在此期间结束时，对象将返回到无法检索的状态。 或者、也可以使用 `Tier` 请求元素以确定还原作业完成所需的时间 (`Expedited`， `Standard`或 `Bulk` ）。如果未指定 `Tier`， `Standard` 已使用层。 注意：如果对象已过渡到S3 Glacier深度归档或云存储池使用Azure Blob Storage、则无法使用还原它 `Expedited` 层。返回以下错误 `403 Forbidden`， `InvalidTier: Retrieval option is not supported by this storage class`。
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	`200 OK` *注意：*如果对象已还原到可检索状态、则可以更改其 `expiry-date` 通过使用新值重新发出POST对象还原请求 `Days`。还原日期将相对于请求时间进行更新。

相关信息

"使用 ILM 管理对象"

"HEAD 对象"

"审核日志中跟踪的 S3 操作"

PUT 对象

您可以使用 S3 PUT 对象请求将对象添加到存储分段中。

解决冲突

冲突的客户端请求(例如、两个客户端写入同一密钥)将按"`latest-WINS`"的原则进行解决。"`latest-WINS`"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

StorageGRID 支持大小高达5 TB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的大小限制为 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是通过采用 UTF-8 编码的每个键和值的字节数之和来衡量的。

用户元数据中的 **UTF-8** 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不会解析或解释用户定义的元数据的密钥名称或值中包含的转义 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 PUT ， PUT 对象副本， GET 和 HEAD 请求将成功。
- StorageGRID 不会返回 `x-amz-missing-meta` 如果对密钥名称或值的解释值包含不可打印的字符、则为标题。

对象标记限制

您可以在上传新对象时为其添加标记，也可以将其添加到现有对象中。StorageGRID 和 Amazon S3 对每个对象最多支持 10 个标记。与对象关联的标记必须具有唯一的标记密钥。一个标记密钥的长度最多可以是 128 个 Unicode 字符，而标记值的长度最多可以是 256 个 Unicode 字符。密钥和值区分大小写。

对象所有权

在 StorageGRID 中，所有对象均归存储分段所有者帐户所有，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`

  指定时 `aws-chunked` 适用于 `Content-Encoding`StorageGRID 不会验证以下各项：

  - StorageGRID 不会验证 `chunk-signature` 针对区块数据。
  - StorageGRID 不会验证您为提供的值 `x-amz-decoded-content-length` 针对对象。
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  如果出现、则支持分块传输编码 `aws-chunked` 此外、还会使用有效负载签名。

- `x-amz-meta-`、后跟一个名称-值对、该对包含用户定义的元数据。

  为用户定义的元数据指定名称 - 值对时，请使用以下通用格式：

```
x-amz-meta-<em>name</em>: <em>value</em>
```

如果要使用*用户定义的创建时间*选项作为ILM规则的参考时间、则必须使用 `creation-time` 作为创建对象时记录的元数据的名称。例如：

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

的值 `creation-time` 评估为自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，也不能使用平衡或严格选项来执行载入行为。创建 ILM 规则时返回错误。

- `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`

"使用 S3 对象锁定"

- SSA 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`

"S3 REST API 支持的操作和限制"

请求标头不受支持

不支持以下请求标头：

- 。 `x-amz-acl` 不支持请求标头。
- 。 `x-amz-website-redirect-location` 不支持请求标头、将返回 `XNotImplemented`。

存储类选项

。 `x-amz-storage-class` 支持请求标头。为提交的值 `x-amz-storage-class` 影响StorageGRID 在载入期间保护对象数据的方式、而不影响StorageGRID 系统中存储的对象持久副本数(由ILM决定)。

如果与已载入对象匹配的ILM规则对载入行为使用strict选项、则为 `x-amz-storage-class` 标题无效。

可以使用以下值 `x-amz-storage-class`：

- `STANDARD` （默认）
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则在载入对象后，系统会立即创建该对象的第二个副本并将其分发到其他存储节点（双提交）。评估 ILM 后， StorageGRID 将确定这些初始临时副本是否满足规则中的放置说明。否则，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中间副本。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，而 StorageGRID 无法立即创建规则中指定的所有副本，则 StorageGRID 会在不同的存储节点上创建两个临时副本。

    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、则会显示 `x-amz-storage-class` 标题无效。

- `REDUCED_REDUNDANCY`
  - * 双提交 * ： 如果 ILM 规则为载入行为指定了双提交选项，则 StorageGRID 会在载入对象时创建一个临时副本（单个提交）。
  - * 已平衡 * ： 如果 ILM 规则指定 Balified 选项，则只有在系统无法立即创建规则中指定的所有副本时， StorageGRID 才会创建一个临时副本。如果 StorageGRID 可以执行同步放置，则此标头不起作用。。`REDUCED_REDUNDANCY` 如果与对象匹配的ILM规则创建一个复制副本、则最好使用选项。在这种情况下、使用 `REDUCED_REDUNDANCY` 无需在每次载入操作中创建和删除额外的对象副本。

  使用 `REDUCED_REDUNDANCY` 在其他情况下、不建议使用此选项。 `REDUCED_REDUNDANCY` 增加载入期间对象数据丢失的风险。例如，如果最初将单个副本存储在发生故障的存储节点上，而此存储节点未能进行 ILM 评估，则可能会丢失数据。

- 注意 * ： 在任意时间段内只复制一个副本会使数据面临永久丢失的风险。如果某个对象只存在一个复制副本，则在存储节点出现故障或出现严重错误时，该对象将丢失。在升级等维护过程中，您还会暂时失去对对象的访问权限。

指定 `REDUCED_REDUNDANCY` 仅影响首次载入对象时创建的副本数。它不会影响在活动 ILM 策略评估对象时创建的对象副本数，也不会导致数据在 StorageGRID 系统中以较低的冗余级别存储。

注意：如果要在启用了S3对象锁定的情况下将对象载入存储分段、则 `REDUCED_REDUNDANCY` 选项将被忽略。如果要将对象载入旧的合规存储分段、则会显示 `REDUCED_REDUNDANCY` 选项返回错误。StorageGRID 将始终执行双提交载入，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 SSI-C 选项是互斥的。

- * SSE* ： 如果要使用 StorageGRID 管理的唯一密钥对对象进行加密，请使用以下标题。
  - `x-amz-server-side-encryption`
- * SSI-C* ： 如果要使用您提供和管理的唯一密钥对对象进行加密，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。
- 注意： * 您提供的加密密钥永远不会存储。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"`使用服务器端加密中的注意事项。`

注：如果使用SSE或SSE-C对对象进行加密、则会忽略任何分段级别或网格级别的加密设置。

版本控制

如果为存储分段启用了版本控制、则为唯一的 `versionId` 会自动为所存储对象的版本生成。这 `versionId` 也会使用在响应中返回 `x-amz-version-id` 响应标头。

如果版本控制已暂停、则存储对象版本时为空 `versionId` 如果已存在空版本、则该版本将被覆盖。

相关信息

"使用 ILM 管理对象"

"对存储分段执行的操作"

"审核日志中跟踪的 S3 操作"

"使用服务器端加密"

"如何配置客户端连接"

PUT 对象—复制

您可以使用 S3 PUT 对象 - 复制请求为已存储在 S3 中的对象创建副本。PUT 对象 - 复制操作与执行 GET ，然后执行 PUT 操作相同。

解决冲突

冲突的客户端请求(例如、两个客户端写入同一密钥)将按"`latest-WINS`"的原则进行解决。"`latest-WINS`"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

StorageGRID 支持大小高达5 TB的对象。

用户元数据中的 UTF-8 字符

如果某个请求在用户定义的元数据的密钥名称或值中包含（未转义） UTF-8 值，则会未定义 StorageGRID 行为。

StorageGRID 不会解析或解释用户定义的元数据的密钥名称或值中包含的转义 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，则请求将成功。
- StorageGRID 不会返回 `x-amz-missing-meta` 如果对密钥名称或值的解释值包含不可打印的字符、则为标题。

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-`、后跟一个名称-值对、该对包含用户定义的元数据
- `x-amz-metadata-directive`：默认值为 `COPY`、用于复制对象和关联的元数据。

  您可以指定 `REPLACE` 复制对象时覆盖现有元数据、或者更新对象元数据。

- `x-amz-storage-class`
- `x-amz-tagging-directive`：默认值为 `COPY`、用于复制对象和所有标记。

  您可以指定 `REPLACE` 可在复制对象时覆盖现有标记、或更新标记。

- 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`

"使用 S3 对象锁定"

- SSA 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`

"服务器端加密的请求标头"

请求标头不受支持

不支持以下请求标头：

- `Cache-Control`
- `Content-Disposition`

- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

存储类选项

。 `x-amz-storage-class` 如果匹配的ILM规则指定了双重提交或平衡的载入行为、则支持请求标头、并影响StorageGRID 创建的对象副本数。

- `STANDARD`

  （默认）指定在 ILM 规则使用双提交选项或 balanced-option 回退到创建中间副本时执行双提交载入操作。

- `REDUCED_REDUNDANCY`

  指定在 ILM 规则使用双提交选项或 balanced-option 回退为创建中间副本时执行单提交载入操作。

> 如果要在启用了S3对象锁定的情况下将对象载入存储分段、则会显示 `REDUCED_REDUNDANCY` 选项将被忽略。如果要将对象载入旧的合规存储分段、则会显示 `REDUCED_REDUNDANCY` 选项返回错误。StorageGRID 将始终执行双提交载入，以确保满足合规性要求。

在 **PUT** 对象中使用 **x-AMZ-copy-source —**复制

如果源存储分段和密钥、请在中指定 `x-amz-copy-source` 标头与目标分段和密钥不同、源对象数据的副本将写入目标。

如果源和目标匹配、则使用和 `x-amz-metadata-directive` 标头指定为 `REPLACE`、对象的元数据将使用请求中提供的元数据值进行更新。在这种情况下， StorageGRID 不会重新载入对象。这有两个重要后果：

- 您不能使用 PUT 对象 - 复制对现有对象进行原位加密，也不能更改现有对象的加密。如果您提供 `x-amz-server-side-encryption` 标题或 `x-amz-server-side-encryption-customer-algorithm` 标头、StorageGRID 拒绝请求并返回 `XNotImplemented`。
- 不会使用匹配 ILM 规则中指定的 " 载入行为 " 选项。通过正常后台 ILM 进程重新评估 ILM 时，更新触发的任何对象放置更改都会进行。

  这意味着，如果 ILM 规则对载入行为使用严格选项，则在无法放置所需对象时（例如，由于新需要的位置不可用），不会执行任何操作。更新后的对象会保留其当前位置，直到可以进行所需的位置为止。

服务器端加密的请求标头

如果使用服务器端加密，则您提供的请求标头取决于源对象是否已加密以及是否计划对目标对象加密。

- 如果源对象使用客户提供的密钥（ SSI-C ）进行加密，则必须在 PUT Object - Copy 请求中包含以下三个标头，以便可以解密并复制此对象：
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` 指定 `AES256`。

- `x-amz-copy-source-server-side-encryption-customer-key` 指定在创建源对象时提供的加密密钥。
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`：指定在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对目标对象（副本）进行加密，请包含以下三个标题：
  - `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。
- 注意： * 您提供的加密密钥永远不会存储。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"`使用服务器端加密中的注意事项。`
- 如果要使用由 StorageGRID （ SSE ）管理的唯一密钥对目标对象（副本）进行加密，请将此标头包括在 PUT 对象 - 复制请求中：
  - `x-amz-server-side-encryption`

注意： `server-side-encryption` 无法更新对象的值。而是使用新创建副本 `server-side-encryption` 价值使用 `x-amz-metadata-directive： REPLACE`。

版本控制

如果源存储分段已版本控制、则可以使用 `x-amz-copy-source` 用于复制最新版本对象的标题。要复制对象的特定版本、必须使用明确指定要复制的版本 `versionId` 子资源。如果目标存储分段已进行版本控制、则会在中返回生成的版本 `x-amz-version-id` 响应标头。如果目标分段的版本控制已暂停、则 `x-amz-version-id` 返回"`null`"值。

相关信息

"使用 ILM 管理对象"

"使用服务器端加密"

"审核日志中跟踪的 S3 操作"

"PUT 对象"