S3 REST API 支持的操作和限制

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-115/s3/authenticating-requests.html on October 03, 2025. Always check docs.netapp.com for the latest.

目录

S3 REST API 支持的操作和限制 1
日期处理 1
通用请求标头 1
通用响应标头 1
对请求进行身份验证 2
使用HTTP授权标头 2
使用查询参数 2
对服务执行的操作 2
对存储分段执行的操作 3
创建S3生命周期配置 10
对存储分段执行自定义操作 14
对对象执行的操作 15
使用 S3 对象锁定 18
使用服务器端加密 20
获取对象 22
HEAD 对象 24
后对象还原 27
PUT 对象 28
PUT 对象—复制 32
多部分上传操作 35
列出多部件上传 37
启动多部件上传 37
上传部件 39
上传部件—复制 40
完成多部件上传 41
错误响应 42
支持的 S3 API 错误代码 42
StorageGRID 自定义错误代码 44

S3 REST API 支持的操作和限制

StorageGRID 系统实施简单存储服务 API （ API 版本 2006-03-01 ），支持大多数操作，但有一些限制。在集成 S3 REST API 客户端应用程序时，您需要了解实施详细信息。

StorageGRID 系统既支持虚拟托管模式请求，也支持路径模式请求。

- "对请求进行身份验证"
- "对服务执行的操作"
- "对存储分段执行的操作"
- "对存储分段执行自定义操作"
- "对对象执行的操作"
- "多部分上传操作"
- "错误响应"

日期处理

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

对于接受日期值的任何标头， StorageGRID 系统仅支持有效的 HTTP 日期格式。日期的时间部分可以使用格林威治标准时间（ GMT ）格式或通用协调时间（ UTC ）格式指定，并且不存在时区偏移（必须指定 +0000 ）。如果包括 `x-amz-date` 标题中指定的任何值。使用AWS签名版本4时、将显示 `x-amz-date` 签名请求中必须存在标题、因为不支持日期标题。

通用请求标头

StorageGRID 系统支持由_Simple Storage Service API参考_定义的通用请求标头、但有一个例外。

请求标题	实施
Authorization	完全支持 AWS 签名版本 2 支持 AWS 签名版本 4 ，但以下情况除外： • 不会为请求正文计算 SHA256 值。接受用户提交的值而不进行验证、就像该值一样 `UNSIGNED-PAYLOAD` 已为提供 `x-amz-content-sha256` 标题。
X-AMZ-securation-token	未实施。返回 `XNotImplemented`。

通用响应标头

StorageGRID 系统支持由 _Simple Storage Service API 参考 _ 定义的所有通用响应标头，但有一个例外。

响应标头	实施
X-AMZ-ID-2	未使用

相关信息

"Amazon Web Services （AWS）文档： Amazon Simple Storage Service API 参考"

对请求进行身份验证

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

S3 API 支持签名版本 2 和签名版本 4 对 S3 API 请求进行身份验证。

经过身份验证的请求必须使用您的访问密钥 ID 和机密访问密钥进行签名。

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

使用**HTTP**授权标头

HTTP `Authorization` 标头由所有S3 API操作使用、但在存储分段策略允许的情况下使用匿名请求除外。。 `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

您可以使用查询参数向 URL 添加身份验证信息。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。使用预签名 URL 的用户无需知道机密访问密钥即可访问资源，这样您就可以为资源提供第三方受限访问权限。

对服务执行的操作

StorageGRID 系统支持对该服务执行以下操作。

操作	实施
获取服务	在所有 Amazon S3 REST API 行为下实施。
获取存储使用量	" 获取存储使用量 " 请求会告知您帐户正在使用的存储总量以及与帐户关联的每个存储分段的存储总量。这是对服务执行的操作、路径为/、并具有自定义查询参数 (`?x-ntap-sg-usage`)。
选项 /	客户端应用程序可以使用问题描述 `OPTIONS /` 向存储节点上的S3端口发出请求、但不提供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，也可以允许外部负载平衡器确定存储节点何时关闭。

相关信息

"获取存储使用情况请求"

对存储分段执行的操作

对于每个 S3 租户帐户， StorageGRID 系统最多支持 1 ， 000 个分段。

存储分段名称限制遵循 AWS US 标准区域限制，但您应进一步将其限制为 DNS 命名约定，以便支持 S3 虚拟托管模式请求。

"Amazon Web Services （ AWS ）文档：存储分段限制"

"S3请求的端点域名"

获取分段（列出对象）和获取分段版本操作支持 StorageGRID 一致性控制。

您可以检查是否已为各个存储分段启用上次访问时间更新。

下表介绍了 StorageGRID 如何实施 S3 REST API 存储分段操作。要执行其中任何操作，必须为帐户提供必要的访问凭据。

操作	实施
删除存储分段	在所有 Amazon S3 REST API 行为下实施。
删除存储分段或	此操作将删除存储分段的 CORS 配置。
删除存储分段加密	此操作将从存储分段中删除默认加密。现有加密对象保持加密状态，但添加到存储分段中的任何新对象不会加密。
删除存储分段生命周期	此操作将从存储分段中删除生命周期配置。
删除存储分段策略	此操作将删除附加到存储分段的策略。
删除存储分段复制	此操作将删除附加到存储分段的复制配置。
删除存储分段标记	此操作使用 `tagging` 用于从存储分段中删除所有标记的子资源。

操作	实施
获取分段（列出对象）版本 1 和版本 2	此操作将返回一个存储分段中的部分或全部（最多 1 ， 000 个）对象。对象的存储类可以具有两个值之一、即使对象是随一起载入的 `REDUCED_REDUNDANCY` 存储类选项： • `STANDARD`、表示对象存储在由存储节点组成的存储池中。 • `GLACIER`、表示对象已移至云存储池指定的外部存储分段。 如果存储分段包含大量前缀相同的已删除密钥、则响应可能包括一些密钥 `CommonPrefixes` 不包含密钥的。
获取分段 ACL	此操作将返回肯定响应以及存储分段所有者的 ID ， DisplayName 和权限，指示所有者对存储分段具有完全访问权限。
获取分段存储器	此操作将返回 `cors` 存储分段的配置。
获取存储分段加密	此操作将返回存储分段的默认加密配置。
获取存储分段生命周期	此操作将返回存储分段的生命周期配置。
获取存储分段位置	此操作将返回使用设置的区域 `LocationConstraint` PUT分段请求中的元素。如果存储分段的区域为 `us-east-1`、将返回该区域的空字符串。
获取存储分段通知	此操作将返回附加到存储分段的通知配置。
获取 Bucket 对象版本	如果对存储分段具有读取访问权限、则此操作将使用 `versions` 子资源列出了存储分段中所有版本对象的元数据。
获取存储分段策略	此操作将返回附加到存储分段的策略。
获取存储分段复制	此操作将返回附加到存储分段的复制配置。
获取存储分段标记	此操作使用 `tagging` 用于返回存储分段的所有标记的子资源。

操作	实施
获取存储分段版本控制	此实施使用 `versioning` 用于返回存储分段版本控制状态的子资源。返回的版本控制状态指示存储分段是"`未版本控制`"还是存储分段是版本"`已启用`"或"已使用`S"。`
获取对象锁定配置	此操作将确定是否为存储分段启用了S3对象锁定。 "使用 S3 对象锁定"
头存储分段	此操作将确定某个存储分段是否存在，并且您有权访问该存储分段。

操作	实施
放入存储分段	此操作将创建一个新存储分段。创建存储分段后，您就会成为存储分段所有者。 • 存储分段名称必须符合以下规则： ◦ 每个 StorageGRID 系统必须是唯一的（而不仅仅是租户帐户中的唯一）。 ◦ 必须符合 DNS 要求。 ◦ 必须至少包含 3 个字符，并且不能超过 63 个字符。 ◦ 可以是一个或多个标签的序列，并使用一个句点分隔相邻标签。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。 ◦ 不能与文本格式的 IP 地址类似。 ◦ 不应在虚拟托管模式请求中使用句点。句点会在验证服务器通配符证书时出现发生原因 问题。 • 默认情况下、将在中创建分段 `us-east-1` 区域；但是、您可以使用 `LocationConstraint` 请求正文中的请求元素以指定其他区域。使用时 `LocationConstraint` Element中、您必须指定已使用网格管理器或网格管理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。* 注 * ： 如果 PUT 存储分段请求使用的区域尚未在 StorageGRID 中定义，则会发生错误。 • 您可以包括 `x-amz-bucket-object-lock-enabled` 请求标题以创建启用了S3对象锁定的存储分段。 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。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。 "使用 S3 对象锁定"
放入存储分段箱	此操作会为存储分段设置 CORS 配置，以便存储分段可以处理跨源请求。跨源资源共享（ 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、假设您使用名为的S3存储分段 `images` 以存储图形。通过设置的CORS配置 `images` 存储分段中的图像、您可以在网站上显示该存储分段中的图像 `http://www.example.com`。

操作	实施
PUT 存储分段加密	此操作将设置现有存储分段的默认加密状态。启用存储分段级别加密后，添加到存储分段中的任何新对象都会进行加密。 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、请设置 `SSEAlgorithm` 参数设置为 `AES256`和、请勿使用 `KMSMasterKeyID` 参数。 如果对象上传请求已指定加密(即、如果请求包含)、则存储分段默认加密配置将被忽略 `x-amz-server-side-encryption-*` 请求标题)。
PUT 存储分段生命周期	此操作将为存储分段创建新的生命周期配置或替换现有的生命周期配置。StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素： • 到期日期（天，日期） • 非当前版本到期（非当前日期） • 筛选器（前缀，标记） • Status • ID StorageGRID 不支持以下操作： • AbortIncompleteMultipartUpload • ExpiredObjectDeleteMarker • 过渡 要了解存储分段生命周期中的到期操作如何与 ILM 放置说明交互，请参见使用信息生命周期管理功能管理对象的说明中的 "`ILM 如何在对象的整个生命周期内运行` " 。 • 注 * ： 存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但传统合规存储分段不支持存储分段生命周期配置。

操作	实施

PUT 存储分段通知	此操作将使用请求正文中包含的通知配置 XML 为存储分段配置通知。您应了解以下实施详细信息：
	
	• StorageGRID 支持将简单通知服务（ SNS ）主题作为目标。不支持简单队列服务（ SQS ）或 Amazon Lambda 端点。
	• 必须将通知目标指定为 StorageGRID 端点的 URN 。可以使用租户管理器或租户管理 API 创建端点。
	
	要成功配置通知，端点必须存在。如果端点不存在、则为 `400 Bad Request` 返回错误并显示代码 `InvalidArgument`。
	
	• 您不能为以下事件类型配置通知。这些事件类型 * 不 * 受支持。
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• 从 StorageGRID 发送的事件通知使用标准 JSON 格式，只是它们不包含某些密钥，而对其他密钥使用特定值，如以下列表所示：
	• * 事件源 *
	
	`sgws:s3`
	
	• * awsRegion*
	
	不包括
	
	• * 。 x-AMZ-id-2*
	
	不包括
	
	• * arn*
	
	`urn:sgws:s3:::bucket_name`

PUT 存储分段策略	此操作将设置附加到存储分段的策略。

操作	实施
PUT 存储分段复制	此操作将使用请求正文中提供的复制配置 XML 为存储分段配置 StorageGRID CloudMirror 复制。对于 CloudMirror 复制，您应了解以下实施详细信息： • StorageGRID 仅支持复制配置的 V1 。这意味着、StorageGRID 不支持使用 `Filter` Element中的规则、并遵循V1中有关删除对象版本的约定。有关详细信息，请参见有关复制配置的 Amazon 文档。 • 分段复制可以在分版本或未分版本的分段上配置。 • 您可以在复制配置 XML 的每个规则中指定不同的目标存储分段。一个源存储分段可以复制到多个目标存储分段。 • 必须将目标分段指定为租户管理器或租户管理 API 中指定的 StorageGRID 端点的 URN 。 要成功进行复制配置，必须存在此端点。如果端点不存在、则请求将以失败的形式出现 `400 Bad Request`。错误消息显示： `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • 您无需指定 `Role` 在配置XML中。StorageGRID 不使用此值，如果提交，则会忽略此值。 • 如果在配置XML中省略存储类、则StorageGRID 将使用 `STANDARD` 默认情况下、存储类。 • 如果从源存储分段中删除对象或删除源存储分段本身，则跨区域复制行为如下： ◦ 如果在复制对象或存储分段之前将其删除，则不会复制此对象 / 存储分段，您也不会收到通知。 ◦ 如果您在复制对象或存储分段后将其删除，则 StorageGRID 会对跨区域复制的 V1 遵循标准 Amazon S3 删除行为。

操作	实施
放置存储分段标记	此操作使用 `tagging` 用于为存储分段添加或更新一组标记的子资源。添加存储分段标记时，请注意以下限制： • StorageGRID 和 Amazon S3 为每个存储分段最多支持 50 个标签。 • 与存储分段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包含 128 个 Unicode 字符。 • 标记值的长度最多可以为 256 个 Unicode 字符。 • 密钥和值区分大小写。
PUT 存储分版本	此实施使用 `versioning` 用于设置现有存储分段的版本控制状态的子资源。您可以使用以下值之一设置版本控制状态： • Enabled ： 为存储分段中的对象启用版本控制。添加到存储分段中的所有对象都会收到唯一的版本 ID 。 • suspended ： 为存储分段中的对象禁用版本控制。添加到存储分段中的所有对象都会收到版本ID `null`。

相关信息

"Amazon Web Services (AWS)文档：跨区域复制"

"一致性控制"

"获取分段上次访问时间请求"

"存储分段和组访问策略"

"使用 S3 对象锁定"

"审核日志中跟踪的 S3 操作"

"使用 ILM 管理对象"

"使用租户帐户"

创建**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 存储分段中删除（过期）某些对象的时间。本节中的示例仅供说明。有关创建S3生命周期配置的完整详细信息、请参见_Amazon Simple Storage Service开发人员指南_中有关对象生命周期管理的章节。请注意， StorageGRID 仅支持到期操作，不支持过渡操作。

"《 Amazon Simple Storage Service 开发人员指南：对象生命周期管理》"

什么是生命周期配置

生命周期配置是一组应用于特定 S3 分段中的对象的规则。每个规则都指定受影响的对象以及这些对象的到期时间（在特定日期或一定天数后）。

StorageGRID 在一个生命周期配置中最多支持 1 ， 000 条生命周期规则。每个规则可以包含以下 XML 元素：

- 到期日期：从对象载入开始，在达到指定日期或达到指定天数时删除对象。
- NoncurrentVersionExpiration ：从对象变为非最新状态开始，在达到指定天数时删除对象。
- 筛选器（前缀，标记）
- Status
- ID

如果将生命周期配置应用于某个存储分段，则存储分段的生命周期设置始终会覆盖 StorageGRID ILM 设置。StorageGRID 使用存储分段的 " 到期 " 设置（而不是 ILM ）来确定是删除还是保留特定对象。

因此，即使 ILM 规则中的放置说明仍适用于某个对象，该对象也可能会从网格中删除。或者，即使对象的任何 ILM 放置指令已失效，该对象也可能会保留在网格中。有关详细信息、请参见使用信息生命周期管理管理对象的说明中的"`ILM在对象的整个生命周期中的运行方式`"。

> 存储分段生命周期配置可用于启用了 S3 对象锁定的存储分段，但旧版合规存储分段不支持存储分段生命周期配置。

StorageGRID 支持使用以下存储分段操作来管理生命周期配置：

- 删除存储分段生命周期
- 获取存储分段生命周期
- PUT 存储分段生命周期

创建生命周期配置

作为创建生命周期配置的第一步，您需要创建一个包含一个或多个规则的 JSON 文件。例如，此 JSON 文件包含三个规则，如下所示：

1. 规则1仅适用于与前缀匹配的对象 `category1/`并且具有 `key2` 的值 `tag2`。。 `Expiration` 参数指定与筛选器匹配的对象将在2020年8月22日午夜到期。
2. 规则2仅适用于与前缀匹配的对象 `category2/`。。 `Expiration` 参数指定与筛选器匹配的对象将在载入后100天过期。

   > 指定天数的规则与对象的载入时间相关。如果当前日期超过载入日期加上天数，则在应用生命周期配置后，可能会立即从存储分段中删除某些对象。

3. 规则3仅适用于与前缀匹配的对象 `category3/`。。 `Expiration` 参数指定任何非最新版本的匹配对象将在其变为非最新状态50天后过期。

```
{
    "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分段

创建生命周期配置文件后，您可以通过发出 PUT 存储分段生命周期请求将其应用于存储分段。

此请求会将示例文件中的生命周期配置应用于名为的存储分段中的对象 `testbucket`：分段

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

要验证是否已成功将生命周期配置应用于存储分段，请发送问题描述 获取存储分段生命周期请求。例如：

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

成功的响应将列出您刚刚应用的生命周期配置。

验证存储分段生命周期到期适用场景 对象

在发出 PUT 对象， HEAD 对象或 GET 对象请求时，您可以确定生命周期配置适用场景 中的到期规则是否为特定对象。如果规则适用、响应将包括 `Expiration` 此参数用于指示对象何时到期以及匹配的到期规则。

> 由于存储分段生命周期会覆盖ILM、因此 `expiry-date` 显示的是删除对象的实际日期。有关详细信息、请参见执行StorageGRID 管理的说明中的"`如何确定对象保留`"。

例如、此PUT对象请求是在2020年6月22日发出的、并在中放置一个对象 `testbucket` 存储分段。

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

成功响应表示此对象将在 100 天后（ 2020 年 10 月 1 日）过期，并且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 head Object 请求用于获取测试分段中同一对象的元数据。

```
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，并且与规则 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": {}
}
```

相关信息

"对存储分段执行的操作"

"使用 ILM 管理对象"

对存储分段执行自定义操作

StorageGRID 系统支持添加到 S3 REST API 中且特定于系统的自定义存储分段操作。

下表列出了 StorageGRID 支持的自定义存储分段操作。

操作	Description	有关详细信息 ...
获取存储分段一致性	返回应用于特定存储分段的一致性级别。	"获取存储分段一致性请求"
PUT 存储分段一致性	设置应用于特定存储分段的一致性级别。	"PUT 存储分段一致性请求"
获取存储分段上次访问时间	返回为特定存储分段启用还是禁用上次访问时间更新。	"获取分段上次访问时间请求"
PUT 分段上次访问时间	用于启用或禁用特定存储分段的上次访问时间更新。	"PUT 分段上次访问时间请求"
删除存储分段元数据通知配置	删除与特定存储分段关联的元数据通知配置 XML 。	"删除存储分段元数据通知配置请求"

操作	Description	有关详细信息 ...
获取存储分段元数据通知配置	返回与特定存储分段关联的元数据通知配置 XML 。	"获取存储分段元数据通知配置请求"
PUT 存储分段元数据通知配置	配置存储分段的元数据通知服务。	"PUT 存储分段元数据通知配置请求"
为合规性修改存储分段	已弃用且不支持：您无法再在启用合规性的情况下创建新存储分段。	"已弃用：为满足合规性而修改存储分段请求"
获取存储分段合规性	已弃用但受支持：返回当前对现有旧版合规存储分段有效的合规性设置。	"已弃用：获取存储分段合规性请求"
PUT 存储分段合规性	已弃用但受支持：允许您修改现有旧版合规存储分段的合规性设置。	"已弃用： PUT 存储分段合规性请求"

相关信息

"审核日志中跟踪的 S3 操作"

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。

操作	实施
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"
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。

对象的状态	**GET** 对象的行为
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"

多部分上传操作

本节介绍 StorageGRID 如何支持多部件上传操作。

- "列出多部分上传"
- "启动多部件上传"
- "上传部件"
- "上传部件—复制"
- "完成多部件上传"

以下条件和注释适用于所有多部件上传操作：

- 一个存储分段的并发多部件上传数不应超过 1 ， 000 次，因为该存储分段的 List Multipart uploads 查询结果可能会返回不完整的结果。

- StorageGRID 对多部件部件强制实施 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）。
  - 通常，部件大小应尽可能大。例如，对于 100 GiB 对象，请使用部件大小 5 GiB 。由于每个部件都被视为唯一对象，因此使用较大的部件大小可降低 StorageGRID 元数据开销。
  - 对于小于 5 GiB 的对象，请考虑使用非多部分上传。
- 如果 ILM 规则使用严格或平衡的载入行为，则会在载入多部分对象时对其每个部分进行评估，并在多部分上传完成后对该对象作为一个整体进行评估。您应了解这会对对象和部件放置产生何种影响：
  - 如果在 S3 多部分上传过程中 ILM 发生更改，则在多部分上传完成后，对象的某些部分可能无法满足当前的 ILM 要求。任何放置不正确的部件都会排队等待 ILM 重新评估，并稍后移至正确的位置。
  - 在评估某个部件的 ILM 时， StorageGRID 会筛选该部件的大小，而不是对象的大小。这意味着，对象的某些部分可以存储在不满足整个对象的 ILM 要求的位置。例如，如果规则指定所有 10 GB 或更大的对象都存储在 DC1 中，而所有较小的对象存储在 DC2 中，则在载入时， 10 部分多部分上传的每个 1 GB 部分都存储在 DC2 中。在对对象整体进行 ILM 评估时，对象的所有部分都将移至 DC1 。
- 所有多部分上传操作均支持 StorageGRID 一致性控制。
- 您可以根据需要对多部分上传使用服务器端加密。要使用SSE (服务器端加密与StorageGRID管理的密钥)、您需要包括 `x-amz-server-side-encryption` 仅在"启动多部件上传请求"中显示请求标题。要对客户提供的密钥使用 SSI-C （服务器端加密），您可以在 " 启动多部件上传请求 " 和后续的每个 " 上传部件请求 " 中指定相同的三个加密密钥请求标头。

操作	实施
列出多部件上传	请参见 "列出多部件上传"
启动多部件上传	请参见 "启动多部件上传"
上传部件	请参见 "上传部件"
上传部件—复制	请参见 "上传部件—复制"
完成多部件上传	请参见 "完成多部件上传"
中止多部分上传	在所有 Amazon S3 REST API 行为下实施
列出部件	在所有 Amazon S3 REST API 行为下实施

相关信息

"一致性控制"

"使用服务器端加密"

列出多部件上传

" 列出多部件上传 " 操作会列出某个存储分段正在进行的多部件上传。

支持以下请求参数：

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

。 `delimiter` 不支持请求参数。

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。执行完 " 多部分上传 " 操作后，即创建对象（并在适用情况下进行版本控制）。

启动多部件上传

" 启动多部件上传 " 操作将为对象启动多部件上传，并返回上传 ID 。

。 `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。

支持以下请求标头：

- Content-Type
- 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-_name_: `value`
  ```

  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。

  正在添加 creation-time 由于在将对象添加到启用了旧合规性的存储分段时不允许使用用户定义的元数据。此时将返回错误。

- 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"

有关 StorageGRID 如何处理 UTF-8 字符的信息，请参见 PUT 对象的文档。

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多部分对象进行加密。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，请在 " 启动多部分上传请求 " 中使用以下标题。请勿在任何上传部件请求中指定此标题。
  - `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，请在 " 启动多部件上传请求 " （以及后续的每个 " 上传部件请求 " ）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。
- 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。`

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

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

相关信息

"使用 ILM 管理对象"

"使用服务器端加密"

"PUT 对象"

上传部件

" 上传部件 " 操作会通过多部件上传方式为对象上传部件。

支持的请求标头

支持以下请求标头：

- `Content-Length`
- `Content-MD5`

服务器端加密的请求标头

如果您为启动多部件上传请求指定了 SSI-C 加密，则还必须在每个上传部件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`：指定您在启动多部件上传请求中提供的相同加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在启动多部件上传请求中提供的相同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。`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

相关信息

"使用服务器端加密"

上传部件—复制

上传部件 - 复制操作通过将现有对象中的数据复制为数据源来上传对象的一部分。

上传部件 - 复制操作可在所有 Amazon S3 REST API 行为下实施。

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

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

如果您为启动多部件上传请求指定了 SSI-C 加密，则还必须在每个上传部件 - 复制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`：指定您在启动多部件上传请求中提供的相同加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定您在启动多部件上传请求中提供的相同MD5摘要。

如果源对象使用客户提供的密钥（ SSI-C ）进行加密，则必须在上传部件 - 复制请求中包含以下三个标题，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。

> 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。`

版本控制

多部分上传包括启动上传，发布上传，上传部件，组装上传的部件以及完成上传的操作。在执行完整的多部件上传操作时，系统会创建对象（如果适用，还会进行版本控制）。

完成多部件上传

完整的多部件上传操作通过整合先前上传的部件来完成对象的多部分上传。

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。

请求标题

。 `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。

如果多部分上传未在 15 天内完成，则此操作将标记为非活动，并从系统中删除所有关联数据。

。 `ETag` 返回的值不是数据的MD5之和、而是遵循的Amazon S3 API实施 `ETag` 多部分对象的值。

版本控制

此操作将完成多部分上传。如果为存储分段启用了版本控制，则在完成多部分上传后会创建对象版本。

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。

如果为存储分段启用了版本控制，则完成多部分上传始终会创建新版本，即使在同一对象密钥上同时完成多部分上传也是如此。如果某个存储分段未启用版本控制，则可以先启动多部分上传，然后再对同一对象密钥启动并完成另一个多部分上传。在非版本控制的存储分段上，最后完成的多部分上传将优先。

复制，通知或元数据通知失败

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

如果发生这种情况，则会在网格管理器中针对总事件（ SMT ）发出警报。最后一个事件消息显示 "`failed to publish notifications for bucket-nameobject key` " for the last object whose notification failed.(要查看此消息、请选择*节点*>*存储节点_*>*事件*。在表顶部查看上次事件。)事件消息也会在中列出 `/var/local/log/bycast-err.log`。

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。

相关信息

"使用 ILM 管理对象"

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 实施还添加了多个自定义响应。

支持的 **S3 API** 错误代码

Name	HTTP 状态
ACCESSDENIED	403 已禁用
BadDigest	400 个错误请求
BucketAlreadyExists	409 冲突
BucketNotEmpagty	409 冲突
实体不完整	400 个错误请求
内部错误	500 内部服务器错误
InvalidAccessKeyId	403 已禁用
InvalidArgument	400 个错误请求
InvalidBucketName	400 个错误请求
InvalidBucketState	409 冲突
InvalidDigest	400 个错误请求
InvalidEncryptionAlgorithmError	400 个错误请求
InvalidPart	400 个错误请求
InvalidPartOrder	400 个错误请求
InvalidRange	416 无法满足请求的范围
InvalidRequest	400 个错误请求
InvalidStorageClass	400 个错误请求
InvalidTag	400 个错误请求
InvalidURI	400 个错误请求
KeyTooLong	400 个错误请求
MalformedXML	400 个错误请求

Name	HTTP 状态
MetadataTooLarge	400 个错误请求
方法未使用	不允许使用 405 方法
MissingContent长度	411 需要长度
MissingRequestBodyError	400 个错误请求
MissingSecurityHeader	400 个错误请求
NoSuchBucket	未找到 404
NoSuchKey	未找到 404
NoSuchUpload	未找到 404
未实施	501 未实施
NoSuchBucketPolicy	未找到 404
ObjectLockConfigurationNotFoundError	未找到 404
预条件已启用	412- 前提条件失败
已请求超时	403 已禁用
服务不可用	503 服务不可用
SignatureDoesNotMatch	403 已禁用
TooMany桶	400 个错误请求
用户密钥已规范	400 个错误请求

StorageGRID 自定义错误代码

Name	Description	HTTP 状态
XBucketLifeycleNotAllowed	旧版合规存储分段不支持存储分段生命周期配置	400 个错误请求

Name	Description	HTTP 状态
XBucketPolicyParseException	无法解析收到的存储分段策略 JSON 。	400 个错误请求
XComplianceConflict	操作因原有合规性设置而被拒绝。	403 已禁用
XComplianceReducedRedundancy For禁用	原有的合规存储分段不允许减少冗余	400 个错误请求
XMaxBucketPolicyLengthExceeded	您的策略超出了允许的最大存储分段策略长度。	400 个错误请求
XMissingInternalRequestHeader	缺少内部请求的标题。	400 个错误请求
XNoSuchBucketCompliance	指定的存储分段未启用原有合规性。	未找到 404
XNotAcceptable	此请求包含一个或多个无法满足的接受标头。	406 不可接受
未实施	您提供的请求意味着未实施的功能。	501 未实施

版权信息

版权所有 © 2025 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。