支持Amazon S3 REST API

StorageGRID 11.8

NetApp
May 10, 2024

目录

支持Amazon S3 REST API

S3 REST API实施详细信息

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。

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 系统支持定义的通用请求标头 "Amazon Simple Storage Service API参考：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

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。具有预先签名URL的用户无需知道访问资源的机密访问密钥、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
List桶 (以前称为GET服务)	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。
获取存储使用量	StorageGRID "获取存储使用量" Request (请求)用于告知您帐户使用的总存储量以及与帐户关联的每个存储分段的存储量。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。

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 Standard区域限制、但您应进一步将其限制为DNS命名约定、以支持S3虚拟托管模式请求。

有关详细信息，请参见以下内容：

- "《Amazon Simple Storage Service用户指南：存储分段限制》"
- "配置S3端点域名"

ListObjects (GET Bucket)和ListObjectVersies (GET Bucket)对象版本)操作支持StorageGRID "一致性值"。

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。请参见 "获取存储分段上次访问时间"。

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
CreateBucket	创建新存储分段。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。 注意：如果CreateBucket(创建存储分段)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。请参见 "使用S3 REST API配置S3对象锁定"。 创建存储分段时，必须启用 S3 对象锁定。创建分段后、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。
DeleteBucket	删除存储分段。
DeleteBucketCors	删除存储分段的CORS配置。
DeleteBucketEncryption	从存储分段中删除默认加密。现有加密对象将保持加密状态、但添加到存储分段的任何新对象不会加密。
DeleteBucketLifecycle	从存储分段中删除生命周期配置。请参见 "创建 S3 生命周期配置"。

操作	实施
DeleteBucketPolicy	删除附加到存储分段的策略。
DeleteBucketReplication	删除附加到存储分段的复制配置。
DeleteBucketTbaging	使用 `tagging` 用于从存储分段中删除所有标记的子资源。 注意：如果为此存储分段设置了非默认ILM策略标记、则会出现 `NTAP-SG-ILM-BUCKET-TAG` 具有分配给存储分段的值的存储分段标记。如果存在、请勿问题描述一个DeleteBucketTbagingRequest `NTAP-SG-ILM-BUCKET-TAG` 存储分段标签。而是使用问题描述发出仅包含的PutBucketTagingRequest `NTAP-SG-ILM-BUCKET-TAG` 用于从存储分段中删除所有其他标记的标记及其分配值。请勿修改或删除 `NTAP-SG-ILM-BUCKET-TAG` 存储分段标签。
GetBucketAcl	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。
GetBucketCors	返回 `cors` 存储分段的配置。
GetBucketEncryption	返回存储分段的默认加密配置。
GetBucketLifecycleConfiguration (以前称为GET分段生命周期)	返回存储分段的生命周期配置。请参见 "创建 S3 生命周期配置"。
GetBucketLocation	返回使用设置的区域 `LocationConstraint` CreateBucket.如果存储分段的区域为 `us-east-1`、将返回该区域的空字符串。
GetBucketNotizationConfiguration (以前称为GET分段通知)	返回附加到存储分段的通知配置。
GetBucketPolicy	返回附加到存储分段的策略。
GetBucketReplication	返回附加到存储分段的复制配置。
GetBucketTaging	使用 `tagging` 用于返回存储分段的所有标记的子资源。 注意：如果为此存储分段设置了非默认ILM策略标记、则会出现 `NTAP-SG-ILM-BUCKET-TAG` 具有分配给存储分段的值的存储分段标记。请勿修改或删除此标记。

操作	实施
GetBucketVersioning	此实施使用 `versioning` 用于返回存储分段版本控制状态的子资源。 • *blank*：从未启用版本控制(分段已"取消版本控制") • Enabled ： 已启用版本控制 • suspended ： 先前已启用版本控制并已暂停
GetObjectLockConfiguration	返回存储分段默认保留模式和默认保留期限(如果已配置)。 请参见 "使用S3 REST API配置S3对象锁定"。
HeadBucket	确定存储分段是否存在、以及您是否有权访问该存储分段。 此操作将返回： • `x-ntap-sg-bucket-id`：UUID格式的存储分段的UUID。 • `x-ntap-sg-trace-id`：关联请求的唯一跟踪ID。
ListObjects和ListObjectsV2 (以前称为GET分段)	返回分段中的部分或全部对象(最多1、000个)。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。
ListObjectVersies (以前称为Get BucketObject Version)	在存储分段上具有读取访问权限时、将此操作与结合使用 `versions` 子资源列出了存储分段中所有版本对象的元数据。
PutBucketCors	设置存储分段的CORS配置、以便存储分段可以处理跨源站请求。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`。
PutBucketEncryption	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`，并且不要使用 `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)。

操作	实施
PutBucketLifecycleConfiguration (以前称为"放置分段生命周期")	为存储分段创建新的生命周期配置或替换现有生命周期配置。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(天数、日期、ExpireObjectDeleteMarker) • 非当前版本到期(新非当前版本、非当前日期) • 筛选器（前缀，标记） • Status • ID StorageGRID 不支持以下操作： • AbortIncompleteMultipartUpload • 过渡 请参见 "创建 S3 生命周期配置"。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 "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

PutBucketNotizationConfiguration
 	
(以前称为Put Bucket"通知)
	使用请求正文中包含的通知配置XML配置分段的通知。您应了解以下实施详细信息：
	
	• StorageGRID支持将Amazon Simple Notification Service (Amazon SNS)或Kafka主题作为目标。不支持简单队列服务(SQS)或Amazon Lamba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、不同之处在于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`

PutBucketPolicy	设置附加到存储分段的策略。请参见 "使用存储分段和组访问策略"。

操作	实施
PutBucketReplication	配置 "StorageGRID CloudMirror复制" 使用请求正文中提供的复制配置XML的存储分段。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 "《Amazon Simple Storage Service用户指南：复制配置》"。 • 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 。请参见 "配置 CloudMirror 复制"。 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、则不会复制该对象或存储分段、也不会通知您。 ◦ 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。
PutBucketTaging	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。 注意：如果为此存储分段设置了非默认ILM策略标记、则会出现 `NTAP-SG-ILM-BUCKET-TAG` 具有分配给存储分段的值的存储分段标记。确保 `NTAP-SG-ILM-BUCKET-TAG` 存储分段标记包含在所有PutBucketTag请求中的已分配值中。请勿修改或删除此标记。 注意：此操作将覆盖存储分段已有的任何当前标记。如果在集合中省略了任何现有标记、则会删除存储分段中的这些标记。

操作	实施
PutBucketVersioning	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`。
PutObjectLockConfiguration	配置或删除存储分段默认保留模式和默认保留期限。 如果修改了默认保留期限，则现有对象版本的保留日期将保持不变，不会使用新的默认保留期限重新计算。 请参见 "使用S3 REST API配置S3对象锁定" 了解详细信息。

对对象执行的操作

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。

以下条件适用于所有对象操作：

- StorageGRID "一致性值" 支持对对象执行的所有操作，但以下操作除外：
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObject保留
  - SelectObjectContent
- 冲突的客户端请求（例如，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 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。
- 通过Swift加热到StorageGRID 系统的数据对象无法通过S3进行访问。

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

操作	实施
DeleteObject	多因素身份验证(MFA)和响应标头 `x-amz-mfa` 不受支持。 处理DeleteObject请求时、StorageGRID会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)、则StorageGRID 会将这些副本排队等待删除、然后向客户端指示删除成功。 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。 请参见 "使用S3 REST API配置S3对象锁定" 了解如何在监管模式下删除对象版本。
DeleteObjects (以前称为删除多个对象)	多因素身份验证(MFA)和响应标头 `x-amz-mfa` 不受支持。 可以在同一请求消息中删除多个对象。 请参见 "使用S3 REST API配置S3对象锁定" 了解如何在监管模式下删除对象版本。
DeleteObjectTagging	使用 `tagging` 用于从对象中删除所有标记的子资源。 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是删除标记、则会返回"NDotAllowed"状态 `x-amz-delete-marker` 响应标头设置为 `true`。
GetObject	"GetObject"

操作	实施
GetObjectAcl	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。
GetObjectLegalHold	"使用S3 REST API配置S3对象锁定"
GetObject保留	"使用S3 REST API配置S3对象锁定"
GetObjectTagging	使用 `tagging` 子资源以返回对象的所有标记。 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是删除标记、则会返回"NDotAllowed"状态 `x-amz-delete-marker` 响应标头设置为 `true`。
HeadObject	"HeadObject"
RestorEObject	"RestorEObject"
PutObject	"PutObject"
CopyObject (以前称为Put Object - Copy)	"CopyObject"
PutObjectLegalHold	"使用S3 REST API配置S3对象锁定"
PutObject保留	"使用S3 REST API配置S3对象锁定"

操作	实施
PutObjectTagging	使用 `tagging` 用于向现有对象添加一组标记的子资源。 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。 标记更新和加热行为 使用PutObjectTags更新对象的标记时、StorageGRID不会重新加载对象。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规则使用stricting选项执行加数据操作、则在无法放置所需对象(例如、新需要的位置不可用)时不会执行任何操作。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）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 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是删除标记、则会返回"NDotAllowed"状态 `x-amz-delete-marker` 响应标头设置为 `true`。
SelectObjectContent	"SelectObjectContent"

使用 **S3 Select**

StorageGRID 支持的以下Amazon S3 Select子句、数据类型和运算符 "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 的租户帐户才能进行问题描述 SelectObjectContent 查询。请参见 "使用 S3 Select 的注意事项和要求"。

条款

- 选择列表
- from 子句
- Where 子句
- Limit 子句

数据类型

- 池
- 整型
- string
- 浮点
- 小数点，数字
- timestamp

运算符

逻辑运算符

- 和
- 不是
- 或

比较运算符

- <
- >
- &lt； =
- &gt； =
- =
- =
- <>
- ！ =
- 介于之间
- 在中

模式匹配运算符

- 例如
- _
- %

统一运算符

- 为空
- 不为空

数学运算符

- +
- -
- *
- /
- %

StorageGRID 遵循Amazon S3 Select操作员优先级。

聚合函数

- 平均（）
- 计数（ * ）
- 最大值（）
- 最小值（）
- sum（ ）

条件函数

- 案例
- 合并
- NULLIF

转换函数

- cast （用于受支持的数据类型）

date 函数

- 日期添加
- 日期差异
- 提取
- to_string
- to_timestamp
- UTCNOW

字符串函数

- char_length ， character_length
- 更低
- 子字符串
- 剪切
- 上限

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 **SS**

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：

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

使用 **SSI-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：

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "上传部件"
- "上传PartCopy"

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跨网格复制或CloudMirror复制、则无法加载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进行服务器端加密(SSE-C)"

CopyObject

您可以使用S3 CopyObject请求为已存储在S3中的对象创建副本。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，两个客户端写入同一密钥）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 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

一个PutObject操作的最大_Recommended_大小为5 GiB (5、368、709、120字节)。如果您的对象大于5 GiB、请使用 "多部分上传" 而是。

一个PutObject操作的最大_supported_大小为5 TiB (5、497、555、138、880字节)。

> 如果您从StorageGRID 11.5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 Liger警报。如果您全新安装了StorageGRID 11.7或11.7、则在这种情况下不会触发警报。但是、为了符合AWS S3标准、未来版本的StorageGRID不支持上传超过5 GiB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`

    如果在发出请求时没有这些标头、则会使用存储分段默认保留设置来计算对象版本模式和保留截止日期。请参见 "使用S3 REST API配置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`

    请参见 [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` 支持请求标头、如果匹配的ILM规则使用"双提交"或"已平衡"、则会影响StorageGRID创建的对象副本数 ""INGest"选项"。

- `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CopyObject中使用x-AMZ-copy-source

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：

- 不能使用CopyObject原位加密现有对象、也不能更改原位现有对象的加密。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规则使用stricting选项执行加数据操作、则在无法放置所需对象(例如、新需要的位置不可用)时不会执行任何操作。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

如果您 "使用服务器端加密"，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加密目标对象。

- 如果源对象使用客户提供的密钥(SSE-C)进行加密、则必须在CopyObject请求中包含以下三个标头、以便可以对该对象进行解密、然后进行复制：
  - `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。

  > 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、请查看的注意事项 "使用服务器端加密"。

- 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，请在CopyObject请求中包括

此标头：

- x-amz-server-side-encryption

> 。 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。

GetObject

您可以使用S3 GetObject请求从S3存储分段中检索对象。

GetObject和多部分对象

您可以使用 partNumber 用于检索多部分或分段对象的特定部分的请求参数。 。 x-amz-mp-parts-count 响应元素指示对象有多少个零件。

您可以设置 partNumber 对于分段/多部分对象和非分段/非多部分对象、均为1；但是、 x-amz-mp-parts-count 只有分段对象或多部分对象才会返回响应元素。

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。对用户定义的元数据中具有转义UTF-8字符的对象发出的获取请求不会返回 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是删除标记、则会随返回"未找到"状态 x-amz-delete-marker 响应标头设置为 true。

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、请查看中的注意事项 "使用服务器端加密"。

GetObject for Cloud Storage Pool对象的行为

对象已存储在中 "云存储池"，GetObject请求的行为取决于对象的状态。请参见 "HeadObject" 有关详细信息：

> 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位于网格中、则GetObject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	**GetObject**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 "RestorEObject" 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` 等待RestorEObject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、GetObject请求可能会错误地返回 `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：

- GetObject请求可能会返回一些数据、但会在传输中途停止。
- 可能会返回后续GetObject请求 `403 Forbidden`。

GetObject和跨网格复制

如果您使用的是 … "网格联盟" 和 "跨网格复制" 已为分段启用、则S3客户端可以通过发出GetObject请求来验证对象的复制状态。响应包括特定于StorageGRID的 `x-ntap-sg-cgr-replication-status` 响应标头、它将具有以下值之一：

网格	复制状态
源	• *SUCCESS *：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

> StorageGRID 不支持 `x-amz-replication-status` 标题。

HeadObject

您可以使用S3 HeadObject请求从对象中检索元数据、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确定对象的过渡状态。

HeadObject和多部分对象

您可以使用 `partNumber` 用于检索多部分或分段对象特定部分的元数据的请求参数。 。 `x-amz-mp-parts-count` 响应元素指示对象有多少个零件。

您可以设置 `partNumber` 对于分段/多部分对象和非分段/非多部分对象、均为1；但是、 `x-amz-mp-parts-count` 只有分段对象或多部分对象才会返回响应元素。

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。对用户定义的元数据中具有转义UTF-8字符的对象发出的HEAD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是删除标记、则会随返回"未找到"状态 `x-amz-delete-marker` 响应标头设置为 `true`。

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、请查看中的注意事项 "使用服务器端加密"。

云存储池对象的**HeadObject**响应

对象存储在中 "云存储池"，将返回以下响应标头：

- `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**HeadObject**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：ongoid-request="false"、thy-date="Sat, 23 7-20 203000:00:00 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：ongoid-request="false"、thy-date="Sat, 23 7-20 203000:00:00 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)、则必须使用问题描述 A "RestorEObject" 请求先从云存储池还原副本、然后才能成功检索对象。

对象的状态	对**HeadObject**的响应

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：ongoy-request="true`

对象已完全还原到云存储池	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-AMZ-restore：ongoid-request="false"、thy-date="Sat, 23 7-20 2018 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、如果某个HeadObject请求的某些部分已被转换为不可检索状态、或者该对象的某些部分尚未还原、则该请求可能会错误地返回`x-AMZ-restore：ongued-request="false"。

HeadObject和跨网格复制

如果您使用的是 … "网格联盟" 和 "跨网格复制" 已为分段启用、则S3客户端可以通过发出HeadObject请求来验证对象的复制状态。响应包括特定于StorageGRID的 `x-ntap-sg-cgr-replication-status` 响应标头、它将具有以下值之一：

网格	复制状态
源	• *SUCCESS *：复制成功。 • *pending *：对象尚未复制。 • 失败：复制失败并出现永久故障。用户必须解决此错误。
目标	**REPRAM**：对象已从源网格复制。

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

PutObject

您可以使用S3 PutObject请求将对象添加到分段。

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）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 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

一个PutObject操作的最大_Recommended_大小为5 GiB (5、368、709、120字节)。如果您的对象大于5 GiB、请使用 "多部分上传" 而是。

一个PutObject操作的最大_supported_大小为5 TiB (5、497、555、138、880字节)。

> 如果您从StorageGRID 11.5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 Liger警报。如果您全新安装了StorageGRID 11.7或11.7、则在这种情况下不会触发警报。但是、为了符合AWS S3标准、未来版本的StorageGRID不支持上传超过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PutObject、CopyObject、GetObject和HeadObject请求会成功。
- 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-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。

  > 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的加注选项。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`

    如果在发出请求时没有这些标头、则会使用存储分段默认保留设置来计算对象版本模式和保留截止日期。请参见 "使用S3 REST API配置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`

    请参见 [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：

- 。 `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)。

如果与已加热对象匹配的ILM规则使用了严格加热选项、则 `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时、StorageGRID 会确定这些初始临时副本是否符合规则中的放置说明。否则、可能需要在不同位置创建新对象副本、并且可能需要删除初始临时副本。
  - 已平衡：如果ILM规则指定了已平衡选项、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）。
  - 均衡：如果ILM规则指定了均衡选项，则只有当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。

在任何一段时间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。它不会影响通过活动ILM策略评估对象时为对象创建的副本数、也不会导致数据在StorageGRID系统中以较低的冗余级别进行存储。

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。

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。

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、请查看的注意事项 "使用服务器端加密"。

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。

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。

授权标题的签名计算

使用时 `Authorization` 用于对请求进行身份验证的标头、StorageGRID 与AWS在以下方面有所不同：

- StorageGRID 不需要 `host` 要包含在中的标题 `CanonicalHeaders`。
- StorageGRID 不需要 `Content-Type` 将包含在中 `CanonicalHeaders`。
- StorageGRID 不需要 `x-amz-*` 要包含在中的标题 `CanonicalHeaders`。

作为一般最佳实践、请始终将这些标题包含在中 `CanonicalHeaders` 为了确保它们已通过验证；但是、如果排除这些标头、StorageGRID 不会返回错误。

有关详细信息，请参见 "授权标头的签名计算：传输单个区块中的有效负载(AWS签名版本4)"。

相关信息

"使用 ILM 管理对象"

RestorEObject

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仅支持用于还原对象的RestorEObject请求。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

云存储池对象上的**RestorEObject**的行为

对象已存储在中 "云存储池"，则根据对象的状态，RestorEObject请求具有以下行为。请参见 "HeadObject" 有关详细信息：

> 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RestorEObject请求来还原该对象。而是可以使用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：在将对象转换为不可检索状态之前，您不能更改它 `expiry-date`。
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。 重要：如果对象已迁移到S3 Glaciereep Archive或云存储池使用Azure Blb存储、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`。

对象的状态	**RestorEObject**的行为
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` 使用的新值重新发出RestorreObject请求 `Days`。还原日期将相对于请求时间进行更新。

SelectObjectContent

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参考：选择对象内容"。

开始之前

- 此租户帐户具有 S3 Select 权限。
- 您已拥有 `s3:GetObject` 要查询的对象的权限。
- 要查询的对象必须采用以下格式之一：
  - **CSX**。可以按原样使用、也可以压缩到GZIP或bzip2归档中。
  - 镶木地板。对镶木地板对象的其他要求：
    - S3 Select仅支持使用GZIP或Snappy进行列式压缩。S3 Select不支持对镶木地板对象进行整体对象压缩。
    - S3 Select不支持镶木地板输出。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。
    - 您必须使用对象架构中指定的数据类型。
    - 不能使用间隔、JSON、列表、时间或UUID逻辑类型。
- SQL 表达式的最大长度为 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>
```

镶木地板请求语法示例

```
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

此查询可从美国人口统计数据中获取状态名称， 2010 年人口， 2015 年估计人口以及变更百分比。文件中非状态的记录将被忽略。

```
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命令行界面使用示例(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,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS命令行界面使用示例(镶木地板)

```
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
```

多部分上传操作

多部分上传操作：概述

本节介绍 StorageGRID 如何支持多部件上传操作。

以下条件和注释适用于所有多部件上传操作：

- 一个分段的并发多部分上传不应超过1、000次、因为ListMultipartUploADS查询结果可能返回不完整的结果。
- 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的对象、因此使用较大的部件可降低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规则使用平衡或严格、则在载入多部分对象时、会针对该对象的每个部分以及在多部分上传完成后、针对整个对象评估ILM ""INGest"选项"。您应了解这会对对象和部件放置产生何种影响：
  - 如果在进行S3多部分上传时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ILM要求。未正确放置的任何部件将排队等待ILM重新评估、并在稍后移至正确位置。
  - 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对象整体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、则载入时、10部分多部分上传的每个1 GB部分都存储在DC2。但是、在为对象整体评估ILM时、对象的所有部分都会移至DC1。

- 所有多部分上传操作均支持StorageGRID "一致性值"。
- 您可以根据需要使用 "服务器端加密" 多部分上传。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CreateMultipartUpload请求中的请求标头。要使用SSE-C (使用客户提供的密钥进行服务器端加密)、您可以在CreateMultipartUpload请求和后续每个UploadPart请求中指定相同的三个加密密钥请求标头。

操作	实施
AbortMultipartUpload	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。
CompleteMultipartUpload	请参见 "CompleteMultipartUpload"
CreateMultipartUpload (以前称为"启动多部分上传")	请参见 "CreateMultipartUpload"
ListMultipartUploads	请参见 "ListMultipartUploads"
ListParts	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。
上传部件	请参见 "上传部件"
上传PartCopy	请参见 "上传PartCopy"

CompleteMultipartUpload

CompleteMultipartUpload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）将以 " 最新成功 " 为基础进行解决。" 最新赢单 " 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。

请求标题

。 `x-amz-storage-class` 支持请求标头、如果匹配的ILM规则指定"双提交"或"已平衡"、则会影响StorageGRID创建的对象副本数 ""INGest"选项"。

- `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。如果为分段启用了版本控制、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。对于其通知失败的最后一个对象、最后一条事件消息将显示"Ffailed to puber-nameobject key的通知"。（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。

CreateMultipartUpload

CreateMultipartUpload (以前称为启动多部分上传)操作会为对象启动多部分上传、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)。

如果与已引入对象匹配的ILM规则使用了strict ""INGest"选项"， `x-amz-storage-class` 标题无效。

可以使用以下值 `x-amz-storage-class`：

- `STANDARD` （默认）
  - *Dual Commit *：如果ILM规则指定了Dual Commit INGEST选项、则在一个对象被加注后、系统将创建该对象的第二个副本并将其分发到其他存储节点(Dual Commit)。评估ILM时、StorageGRID 会确定这些初始临时副本是否符合规则中的放置说明。否则、可能需要在不同位置创建新对象副本、并且可能需要删除初始临时副本。
  - 已平衡：如果ILM规则指定了已平衡选项、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`
  - *Dual Commit *：如果ILM规则指定了Dual Commit选项、则StorageGRID会在对象被引入时创建一个临时副本(单个提交)。
  - 均衡：如果ILM规则指定了均衡选项，则只有当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。

> 在任何一段时间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。它不会影响通过活动ILM策略评估对象时为对象创建的副本数、也不会导致数据在StorageGRID系统中以较低的冗余级别进行存储。

> 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。

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`

    如果在不使用这些标题的情况下发出请求，则存储分段默认保留设置用于计算对象版本 retain-until 日期。

"使用S3 REST API配置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`

    [服务器端加密的请求标头]

> 有关StorageGRID如何处理UTF-8字符的信息、请参见 "PutObject"。

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。请勿在任何UploadPart请求中指定此标题。
  - `x-amz-server-side-encryption`
- **SSE-C**：如果要使用提供和管理的唯一密钥对对象进行加密，请在CreateMultipartUpload请求(以及后续的每个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、请查看的注意事项 "使用服务器端加密"。

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。执行CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

ListMultipartUploads

ListMultipartUploads操作可列出分段的正在进行的多部分上传。

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CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

上传部件

UploadPart操作在对象的多部分上传中上传部件。

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`：指定与CreateMultipartUpload请求中提供的加密密钥相同的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定与CreateMultipartUpload请求中提供的MD5摘要相同的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、请查看中的注意事项 "使用服务器端加密"。

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CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

上传PartCopy

UploadPartCopy操作通过从现有对象作为数据源复制数据来上传部分对象。

所有Amazon S3 REST API行为均会实施UploadPartCopy操作。如有更改、恕不另行通知。

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`：指定与CreateMultipartUpload请求中提供的加密密钥相同的加密密钥。
- `x-amz-server-side-encryption-customer-key-MD5`：指定与CreateMultipartUpload请求中提供的MD5摘要相同的MD5摘要。

如果源对象使用客户提供的密钥(SSE-C)进行加密、则必须在UploadPartCopy请求中包含以下三个标头、以便可以解密并复制该对象：

- `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、请查看中的注意事项 "使用服务器端加密"。

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CompleteMultipartUpload操作时、系统会创建对象(如果适用、还会对其进行版本管理)。

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

Name	HTTP 状态
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
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

Name	HTTP 状态
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
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
XComplianceReducedRedundancyFor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