多部分上传操作

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/storagegrid-117/s3/list-multipart-uploads.html on November 04, 2025. Always check docs.netapp.com for the latest.

目录

多部分上传操作 1
列出多部件上传 2
版本控制 2
启动多部件上传 2
服务器端加密的请求标头 4
请求标头不受支持 4
版本控制 5
上传部件 5
支持的请求标头 5
服务器端加密的请求标头 5
版本控制 5
上传部件—复制 6
服务器端加密的请求标头 6
版本控制 6
完成多部件上传 6
解决冲突 7
请求标题 7
版本控制 7
复制，通知或元数据通知失败 7

多部分上传操作

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的载入行为、则载入多部分对象时会针对该对象的每个部分以及完成多部分上传后对整个对象进行ILM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。如有更改、恕不另行通知。

操作	实施
列出部件	在所有 Amazon S3 REST API 行为下实施。如有更改、恕不另行通知。

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`
- `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

启动多部分上传(CreateMultipartUpload)操作将启动对象的多部分上传、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。

> 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。

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。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"

"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。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` 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。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"

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。