



Vorgänge für mehrteilige Uploads

StorageGRID software

NetApp
October 21, 2025

Inhalt

Vorgänge für mehrteilige Uploads	1
Vorgänge für mehrteilige Uploads	1
CompleteMultipartUpload	2
Konflikte lösen	2
Unterstützte Anforderungsheader	2
Nicht unterstützte Anforderungsheader	3
Versionierung	3
Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung	4
CreateMultipartUpload	4
Unterstützte Anforderungsheader	5
Anforderungsheader für serverseitige Verschlüsselung	6
Nicht unterstützte Anforderungsheader	7
Versionierung	7
ListMultipartUploads	7
Versionierung	7
UploadPart	7
Unterstützte Anforderungsheader	8
Anforderungsheader für serverseitige Verschlüsselung	8
Nicht unterstützte Anforderungsheader	8
Versionierung	8
UploadPartCopy	8
Anforderungsheader für serverseitige Verschlüsselung	9
Versionierung	9

Vorgänge für mehrteilige Uploads

Vorgänge für mehrteilige Uploads

In diesem Abschnitt wird beschrieben, wie StorageGRID Vorgänge für mehrteilige Uploads unterstützt.

Für alle mehrteiligen Uploadvorgänge gelten die folgenden Bedingungen und Hinweise:

- Sie sollten nicht mehr als 1.000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse von ListMultipartUploads-Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse zurückgeben.
- StorageGRID erzwingt AWS-Größenbeschränkungen für mehrteilige Teile. S3-Clients müssen diese Richtlinien befolgen:
 - Jeder Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5.242.880 Bytes) und 5 GiB (5.368.709.120 Bytes) groß sein.
 - Der letzte Teil kann kleiner als 5 MiB (5.242.880 Bytes) sein.
 - Generell sollten die Teilegrößen möglichst groß sein. Verwenden Sie beispielsweise Teilgrößen von 5 GiB für ein 100-GiB-Objekt. Da jedes Teil als einzigartiges Objekt betrachtet wird, reduziert die Verwendung großer Teilegrößen den StorageGRID Metadaten-Overhead.
 - Erwägen Sie für Objekte, die kleiner als 5 GiB sind, stattdessen die Verwendung eines nicht mehrteiligen Uploads.
- ILM wird für jeden Teil eines mehrteiligen Objekts ausgewertet, wenn es aufgenommen wird, und für das Objekt als Ganzes, wenn der mehrteilige Upload abgeschlossen ist, wenn die ILM-Regel die Balanced- oder Strict-Regel verwendet. ["Aufnahmeoption"](#) . Sie sollten sich darüber im Klaren sein, welche Auswirkungen dies auf die Platzierung von Objekten und Teilen hat:
 - Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert, erfüllen einige Teile des Objekts nach Abschluss des Multipart-Uploads möglicherweise nicht die aktuellen ILM-Anforderungen. Alle Teile, die nicht richtig platziert sind, werden zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.
 - Bei der Auswertung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei der Aufnahme bei DC2 gespeichert. Wenn ILM jedoch für das gesamte Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.
- Alle mehrteiligen Upload-Vorgänge unterstützen StorageGRID ["Konsistenzwerte"](#) .
- Wenn ein Objekt per mehrteiligem Upload aufgenommen wird, ["Schwellenwert für Objektsegmentierung \(1 GiB\)"](#) wird nicht angewendet.
- Bei Bedarf können Sie ["serverseitige Verschlüsselung"](#) mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit StorageGRID-verwalteten Schlüsseln) zu verwenden, schließen Sie die `x-amz-server-side-encryption` Anforderungsheader nur in der CreateMultipartUpload-Anforderung. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der CreateMultipartUpload-Anforderung und in jeder nachfolgenden UploadPart-Anforderung dieselben drei Anforderungsheader für Verschlüsselungsschlüssel an.

Betrieb	Durchführung
AbortMultipartUpload	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
CompleteMultipartUpload	Sehen " CompleteMultipartUpload "
CreateMultipartUpload (früher „Mehrteiligen Upload initiieren“ genannt)	Sehen " CreateMultipartUpload "
ListMultipartUploads	Sehen " ListMultipartUploads "
Teileliste	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
UploadPart	Sehen " UploadPart "
UploadPartCopy	Sehen " UploadPartCopy "

CompleteMultipartUpload

Der Vorgang „CompleteMultipartUpload“ schließt einen mehrteiligen Upload eines Objekts ab, indem er die zuvor hochgeladenen Teile zusammenfügt.



StorageGRID unterstützt nicht aufeinanderfolgende Werte in aufsteigender Reihenfolge für die `partNumber` Anforderungsparameter mit CompleteMultipartUpload. Der Parameter kann mit einem beliebigen Wert beginnen.

Konflikte lösen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

Der `x-amz-storage-class` Header beeinflusst, wie viele Objektkopien StorageGRID erstellt, wenn die entsprechende ILM-Regel Folgendes angibt: "[Option für doppeltes Commit oder ausgeglichene Aufnahme](#)".

- STANDARD

(Standard) Gibt einen Dual-Commit-Aufnahmevergang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.

- REDUCED_REDUNDANCY

Gibt einen Single-Commit-Ingest-Vorgang an, wenn die ILM-Regel die Option „Dual Commit“ verwendet oder wenn die Option „Balanced“ auf die Erstellung von Zwischenkopien zurückgreift.



Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die REDUCED_REDUNDANCY Option ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, REDUCED_REDUNDANCY Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.



Wenn ein mehrteiliger Upload nicht innerhalb von 15 Tagen abgeschlossen wird, wird der Vorgang als inaktiv markiert und alle zugehörigen Daten werden aus dem System gelöscht.



Der ETag Der zurückgegebene Wert ist keine MD5-Summe der Daten, sondern folgt der Amazon S3 API-Implementierung des ETag Wert für mehrteilige Objekte.

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

Dieser Vorgang schließt einen mehrteiligen Upload ab. Wenn die Versionierung für einen Bucket aktiviert ist, wird die Objektversion nach Abschluss des mehrteiligen Uploads erstellt.

Wenn die Versionierung für einen Bucket aktiviert ist, `versionId` wird automatisch für die Version des gespeicherten Objekts generiert. Das `versionId` wird auch in der Antwort zurückgegeben, indem der `x-amz-version-id` Antwortheader.

Wenn die Versionierung ausgesetzt ist, wird die Objektversion mit einem Nullwert gespeichert. `versionId` und wenn bereits eine Nullversion vorhanden ist, wird diese überschrieben.



Wenn die Versionsverwaltung für einen Bucket aktiviert ist, wird beim Abschließen eines mehrteiligen Uploads immer eine neue Version erstellt, auch wenn gleichzeitig mehrteilige Uploads für denselben Objektschlüssel abgeschlossen wurden. Wenn die Versionsverwaltung für einen Bucket nicht aktiviert ist, ist es möglich, einen mehrteiligen Upload zu initiieren und dann zunächst einen weiteren mehrteiligen Upload mit demselben Objektschlüssel zu initiieren und abzuschließen. Bei Buckets ohne Versionsangabe hat der zuletzt abgeschlossene mehrteilige Upload Vorrang.

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

Wenn der Bucket, in dem der mehrteilige Upload erfolgt, für einen Plattformdienst konfiguriert ist, ist der mehrteilige Upload auch dann erfolgreich, wenn die zugehörige Replikations- oder Benachrichtigungsaktion fehlschlägt.

Ein Mandant kann die fehlgeschlagene Replikation oder Benachrichtigung auslösen, indem er die Metadaten oder Tags des Objekts aktualisiert. Um unerwünschte Änderungen zu vermeiden, kann ein Mandant die vorhandenen Werte erneut übermitteln.

Weitere Informationen finden Sie unter ["Fehlerbehebung bei Plattformdiensten"](#) .

CreateMultipartUpload

Der Vorgang „CreateMultipartUpload“ (früher „Initiate Multipart Upload“) initiiert einen mehrteiligen Upload für ein Objekt und gibt eine Upload-ID zurück.

Der `x-amz-storage-class` Anforderungsheader wird unterstützt. Der übermittelte Wert für `x-amz-storage-class` beeinflusst, wie StorageGRID Objektdaten während der Aufnahme schützt, und nicht, wie viele persistente Kopien des Objekts im StorageGRID -System gespeichert werden (was durch ILM bestimmt wird).

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die strikte ["Aufnahmeoption"](#) , Die `x-amz-storage-class` Header hat keine Wirkung.

Folgende Werte können verwendet werden für `x-amz-storage-class` :

- STANDARD(Standard)
 - **Dual Commit:** Wenn die ILM-Regel die Aufnahmeoption „Dual Commit“ angibt, wird, sobald ein Objekt aufgenommen wird, eine zweite Kopie dieses Objekts erstellt und an einen anderen Speicherknoten verteilt (Dual Commit). Bei der Auswertung des ILM ermittelt StorageGRID , ob diese ersten Zwischenkopien die Platzierungsanweisungen in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an anderen Orten erstellt und die ersten Zwischenkopien gelöscht werden.
 - **Ausgeglichen:** Wenn die ILM-Regel die Option „Ausgeglichen“ angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

Wenn StorageGRID alle in der ILM-Regel angegebenen Objektkopien sofort erstellen kann (synchrone Platzierung), `x-amz-storage-class` Header hat keine Wirkung.

- REDUCED_REDUNDANCY
 - **Dual Commit:** Wenn die ILM-Regel die Option „Dual Commit“ angibt, erstellt StorageGRID beim Einlesen des Objekts eine einzelne Zwischenkopie (Single Commit).
 - **Ausgeglichen:** Wenn die ILM-Regel die Option „Ausgeglichen“ angibt, erstellt StorageGRID nur dann eine einzelne Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat dieser Header keine Wirkung. Der REDUCED_REDUNDANCY Die Option wird am besten verwendet, wenn die ILM-Regel, die dem Objekt entspricht, eine einzelne replizierte Kopie erstellt. In diesem Fall mit REDUCED_REDUNDANCY vermeidet das unnötige Erstellen und Löschen einer zusätzlichen Objektkopie für jeden Aufnahmevergang.

Verwenden des `REDUCED_REDUNDANCY` Unter anderen Umständen wird diese Option nicht empfohlen. `REDUCED_REDUNDANCY` erhöht das Risiko eines Objektdatenverlusts während der Aufnahme. Beispielsweise können Daten verloren gehen, wenn die einzelne Kopie zunächst auf einem Speicherknoten gespeichert wird, der ausfällt, bevor die ILM-Auswertung erfolgen kann.



Wenn für einen bestimmten Zeitraum nur eine Kopie vorhanden ist, besteht die Gefahr eines dauerhaften Datenverlusts. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

Festlegen `REDUCED_REDUNDANCY` wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Es hat keinen Einfluss darauf, wie viele Kopien des Objekts erstellt werden, wenn das Objekt von den aktiven ILM-Richtlinien ausgewertet wird, und führt nicht dazu, dass Daten im StorageGRID System auf niedrigeren Redundanzebenen gespeichert werden.



Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperre aufnehmen, wird die `REDUCED_REDUNDANCY` Option ignoriert. Wenn Sie ein Objekt in einen Legacy-Compliant-Bucket aufnehmen, `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine Dual-Commit-Aufnahme durch, um sicherzustellen, dass die Compliance-Anforderungen erfüllt werden.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

Derzeit ist nur der SHA256-Wert für `x-amz-checksum-algorithm` wird unterstützt.

- `x-amz-meta-`, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten

Verwenden Sie beim Angeben des Name-Wert-Paares für benutzerdefinierte Metadaten dieses allgemeine Format:

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

Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie `creation-time` als Name der Metadaten, die aufzeichnen, wann das Objekt erstellt wurde. Beispiel:

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

Der Wert für `creation-time` wird seit dem 1. Januar 1970 in Sekunden ausgewertet.



Hinzufügen `creation-time` da benutzerdefinierte Metadaten nicht zulässig sind, wenn Sie ein Objekt zu einem Bucket hinzufügen, für den die Legacy-Compliance aktiviert ist. Es wird ein Fehler zurückgegeben.

- S3 Object Lock-Anforderungsheader:

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

Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um das Aufbewahrungsdatum der Objektversion zu berechnen.

["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)

- SSE-Anforderungsheader:

- `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`

[Anforderungsheader für serverseitige Verschlüsselung](#)



Informationen zur Verarbeitung von UTF-8-Zeichen durch StorageGRID finden Sie unter ["PutObject"](#).

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteiliges Objekt mit serverseitiger Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE:** Verwenden Sie den folgenden Header in der `CreateMultipartUpload`-Anforderung, wenn Sie das Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel verschlüsseln möchten. Geben Sie diesen Header in keiner der `UploadPart`-Anfragen an.

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

- **SSE-C:** Verwenden Sie alle drei dieser Header in der `CreateMultipartUpload`-Anfrage (und in jeder nachfolgenden `UploadPart`-Anfrage), wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.



Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Überlegungen für "[Verwendung serverseitiger Verschlüsselung](#)".

Nicht unterstützte Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt:

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

Der `x-amz-website-redirect-location` Header>Returns `XNotImplemented`.

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang `CompleteMultipartUpload` ausgeführt wird.

ListMultipartUploads

Der Vorgang „`ListMultipartUploads`“ listet laufende mehrteilige Uploads für einen Bucket auf.

Die folgenden Anforderungsparameter werden unterstützt:

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

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang `CompleteMultipartUpload` ausgeführt wird.

UploadPart

Der Vorgang „`UploadPart`“ lädt einen Teil in einem mehrteiligen Upload für ein Objekt hoch.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie für die `CreateMultipartUpload`-Anforderung die SSE-C-Verschlüsselung angegeben haben, müssen Sie in jede `UploadPart`-Anforderung auch die folgenden Anforderungsheader einfügen:

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der `CreateMultipartUpload`-Anforderung angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie denselben MD5-Digest an, den Sie in der `CreateMultipartUpload`-Anforderung angegeben haben.



Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in ["Verwenden Sie serverseitige Verschlüsselung"](#) .

Wenn Sie während der `CreateMultipartUpload`-Anforderung eine SHA-256-Prüfsumme angegeben haben, müssen Sie in jede `UploadPart`-Anforderung auch den folgenden Anforderungsheader einfügen:

- `x-amz-checksum-sha256`: Geben Sie die SHA-256-Prüfsumme für diesen Teil an.

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang `CompleteMultipartUpload` ausgeführt wird.

UploadPartCopy

Der Vorgang „`UploadPartCopy`“ lädt einen Teil eines Objekts hoch, indem Daten aus einem vorhandenen Objekt als Datenquelle kopiert werden.

Der Vorgang „`UploadPartCopy`“ wird mit dem gesamten Amazon S3 REST-API-Verhalten implementiert. Änderungen vorbehalten.

Diese Anfrage liest und schreibt die Objektdaten, die in `x-amz-copy-source-range` innerhalb des StorageGRID -Systems.

Die folgenden Anforderungsheader werden unterstützt:

- `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`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie für die `CreateMultipartUpload`-Anforderung eine SSE-C-Verschlüsselung angegeben haben, müssen Sie in jede `UploadPartCopy`-Anforderung auch die folgenden Anforderungsheader einfügen:

- `x-amz-server-side-encryption-customer-algorithm`: Angeben AES256 .
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der `CreateMultipartUpload`-Anforderung angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie denselben MD5-Digest an, den Sie in der `CreateMultipartUpload`-Anforderung angegeben haben.

Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt ist, müssen Sie die folgenden drei Header in die `UploadPartCopy`-Anforderung aufnehmen, damit das Objekt entschlüsselt und dann kopiert werden kann:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angeben AES256 .
- `x-amz-copy-source-server-side-encryption-customer-key`: Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.



Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in "[Verwenden Sie serverseitige Verschlüsselung](#)".

Versionierung

Der mehrteilige Upload besteht aus separaten Vorgängen zum Starten des Uploads, Auflisten der Uploads, Hochladen von Teilen, Zusammenstellen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang `CompleteMultipartUpload` ausgeführt wird.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.