



# **Unterstützung für Amazon S3-REST-API**

## **StorageGRID**

NetApp  
November 04, 2025

# Inhalt

Unterstützung für Amazon S3-REST-API .....	1
Details zur S3-REST-API-Implementierung .....	1
Umgang mit Daten .....	1
Allgemeine Anfragemöpfe .....	1
Allgemeine Antwortkopfzeilen .....	1
Authentifizieren von Anfragen .....	2
Verwenden Sie den HTTP-Autorisierungskopf .....	2
Abfrageparameter verwenden .....	2
Betrieb auf dem Service .....	2
Operationen auf Buckets .....	3
Operationen für Objekte .....	10
Operationen für Objekte .....	10
Verwenden Sie S3 Select .....	15
Serverseitige Verschlüsselung .....	17
CopyObject .....	19
GetObject .....	23
HeadObject .....	25
PutObject .....	28
Objekt restoreObject .....	33
SelektierObjectContent .....	35
Vorgänge für mehrteilige Uploads .....	39
Operationen für mehrteilige Uploads: Übersicht .....	39
CompleteMultipartUpload .....	40
CreateMultipartUpload .....	42
ListMultipartUploads .....	45
UploadTeil .....	45
UploadPartCopy .....	46
Fehlerantworten .....	47
Unterstützte S3-API-Fehlercodes .....	47
Benutzerdefinierte StorageGRID-Fehlercodes .....	49

# Unterstützung für Amazon S3-REST-API

## Details zur S3-REST-API-Implementierung

Das StorageGRID System implementiert die Simple Storage Service API (API Version 2006-03-01) mit Unterstützung der meisten Operationen und mit einigen Einschränkungen. Wenn Sie S3 REST-API-Client-Applikationen integrieren, sind die Implementierungsdetails bekannt.

Das StorageGRID System unterstützt sowohl Virtual-Hosted-Style-Anforderungen als auch Anforderungen im Pfadstil.

### Umgang mit Daten

Die StorageGRID Implementierung der S3-REST-API unterstützt nur gültige HTTP-Datumsformate.

Das StorageGRID-System unterstützt nur gültige HTTP-Datumsformate für alle Header, die Datumswerte akzeptieren. Der Zeitbereich des Datums kann im Greenwich Mean Time (GMT)-Format oder im UTC-Format (Universal Coordinated Time) ohne Zeitonenversatz angegeben werden (+0000 muss angegeben werden). Wenn Sie die einschließen `x-amz-date` Kopfzeile in Ihrer Anfrage, es überschreibt alle Werte, die in der Kopfzeile der Datumsanforderung angegeben sind. Bei Verwendung von AWS Signature Version 4, das `x-amz-date` Die Kopfzeile muss in der signierten Anforderung vorhanden sein, da die Datumsüberschrift nicht unterstützt wird.

### Allgemeine Anfragemöpfe

Das StorageGRID-System unterstützt die von definierten allgemeinen Anforderungsheader "[Amazon Simple Storage Service API-Referenz: Common Request Header](#)", Mit einer Ausnahme.

Kopfzeile der Anfrage	Implementierung
Autorisierung	<p>Vollständige Unterstützung für AWS Signature Version 2</p> <p>Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen:</p> <ul style="list-style-type: none"><li>• Der SHA256-Wert wird für den Körper der Anforderung nicht berechnet. Der vom Benutzer eingereichte Wert wird ohne Validierung angenommen, als ob der Wert <code>UNSIGNED-PAYLOAD</code> War für die vorgesehen <code>x-amz-content-sha256</code> Kopfzeile.</li></ul>
X-amz-Sicherheits-Token	Nicht implementiert. Kehrt Zurück <code>XNotImplemented</code> .

### Allgemeine Antwortkopfzeilen

Das StorageGRID System unterstützt alle gängigen Antwortheader, die durch die *Simple Storage Service API Reference* definiert wurden. Eine Ausnahme bilden die Antwort.

Kopfzeile der Antwort	Implementierung
X-amz-id-2	Nicht verwendet

## Authentifizieren von Anfragen

Das StorageGRID-System unterstützt über die S3-API sowohl authentifizierten als auch anonymen Zugriff auf Objekte.

Die S3-API unterstützt Signature Version 2 und Signature Version 4 zur Authentifizierung von S3-API-Anforderungen.

Authentifizierte Anfragen müssen mit Ihrer Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel signiert werden.

Das StorageGRID System unterstützt zwei Authentifizierungsmethoden: Den HTTP Authorization Kopfzeile und Verwendung von Abfrageparametern.

### Verwenden Sie den HTTP-Autorisierungskopf

Das HTTP Authorization Kopfzeile wird von allen S3-API-Operationen verwendet außer anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der Authorization Header enthält alle erforderlichen Signierungsdaten, um eine Anforderung zu authentifizieren.

### Abfrageparameter verwenden

Sie können Abfrageparameter verwenden, um Authentifizierungsinformationen zu einer URL hinzuzufügen. Dies wird als Vorsignierung der URL bezeichnet, mit der ein temporärer Zugriff auf bestimmte Ressourcen gewährt werden kann. Benutzer mit der vorgeschichteten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zuzugreifen. So können Sie beschränkten Zugriff von Drittanbietern auf eine Ressource bereitstellen.

## Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
ListBuchs (Zuvor „GET Service“ genannt)	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
GET Storage-Auslastung	Das StorageGRID " <a href="#">GET Storage-Auslastung</a> " Die Anforderung gibt an, wie viel Speicherplatz von einem Konto und für jeden mit dem Konto verknüpften Bucket insgesamt verwendet wird. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (?x-ntap-sg-usage) Hinzugefügt.

Betrieb	Implementierung
OPTIONEN /	Client-Applikationen können Probleme haben <code>OPTIONS</code> / Anfragen an den S3-Port auf einem Storage-Node ohne die Zugangsdaten für die S3-Authentifizierung, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um zu ermöglichen, dass externe Load Balancer eingesetzt werden, wenn ein Storage-Node ausfällt.

## Operationen auf Buckets

Das StorageGRID System unterstützt für jedes S3-Mandantenkonto maximal 1,000 Buckets.

Einschränkungen für Bucket-Namen folgen den regionalen Einschränkungen des AWS US Standard. Sie sollten sie jedoch weiter auf DNS-Namenskonventionen beschränken, um Anforderungen im virtuellen Hosted-Stil von S3 zu unterstützen.

Weitere Informationen finden Sie im Folgenden:

- ["Amazon Simple Storage Service User Guide: Bucket-Einschränkungen und -Beschränkungen"](#)
- ["Konfigurieren Sie die Domännennamen des S3-Endpunkts"](#)

Die Operationen `ListObjects` (GET Bucket) und `ListObjectVersions` (GET Bucket Object Versions) unterstützen StorageGRID **"Konsistenzwerte"**.

Sie können überprüfen, ob für einzelne Buckets Updates zur letzten Zugriffszeit aktiviert oder deaktiviert wurden. Siehe **"ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN"**.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Bucket-Operationen implementiert. Um einen dieser Vorgänge durchzuführen, müssen die erforderlichen Anmeldedaten für den Zugriff für das Konto bereitgestellt werden.

Betrieb	Implementierung
CreateBucket	<p>Erstellt einen neuen Bucket. Mit dem Erstellen des Buckets werden Sie zum Bucket-Eigentümer.</p> <ul style="list-style-type: none"> <li>• Bucket-Namen müssen die folgenden Regeln einhalten: <ul style="list-style-type: none"> <li>◦ Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos).</li> <li>◦ Muss DNS-konform sein.</li> <li>◦ Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten.</li> <li>◦ Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.</li> <li>◦ Darf nicht wie eine Text-formatierte IP-Adresse aussehen.</li> <li>◦ Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats.</li> </ul> </li> <li>• Standardmäßig werden Buckets im erstellten <code>us-east-1</code> Region; jedoch können Sie die verwenden <code>LocationConstraint</code> Anforderungselement im Anforderungskörper, um eine andere Region anzugeben. Bei Verwendung des <code>LocationConstraint</code> Element, Sie müssen den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den zu verwendenden Regionalnamen nicht kennen.</li> </ul> <p><b>Hinweis:</b> Ein Fehler tritt auf, wenn Ihre CreateBucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.</p> <ul style="list-style-type: none"> <li>• Sie können die einschließen <code>x-amz-bucket-object-lock-enabled</code> Kopfzeile zum Erstellen eines Buckets anfordern, wobei S3-Objektsperre aktiviert ist. Siehe <a href="#">"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"</a>.</li> </ul> <p>Sie müssen die S3-Objektsperre aktivieren, wenn Sie den Bucket erstellen. Sie können S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.</p>
DeleteBucket	Löscht den Bucket.
DeleteBucketCors	Löscht die CORS-Konfiguration für den Bucket.
DeleteBucketEncryption	Löscht die Standardverschlüsselung aus dem Bucket. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, neue Objekte, die dem Bucket hinzugefügt wurden, werden jedoch nicht verschlüsselt.

Betrieb	Implementierung
DeleteBucketLifecycle	Löscht die Lebenszykluskonfiguration aus dem Bucket. Siehe " <a href="#">S3-Lebenszykluskonfiguration erstellen</a> ".
DeleteBucketRichtlinien	Löscht die dem Bucket angehängte Richtlinie.
DeleteBucketReplication	Löscht die Replikationskonfiguration, die mit dem Bucket verbunden ist.
DeleteBucketTagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Bucket zu entfernen</p> <p><b>Achtung:</b> Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, gibt es ein <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag mit einem ihm zugewiesenen Wert. Stellen Sie keine DeleteBucketTagging-Anforderung aus, wenn ein vorhanden ist <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag: Geben Sie stattdessen eine Anforderung für das PutkBucketTagging nur mit dem aus <code>NTAP-SG-ILM-BUCKET-TAG</code> Tag und der ihm zugewiesene Wert, um alle anderen Tags aus dem Bucket zu entfernen. Ändern oder entfernen Sie den nicht <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag:</p>
GetBucketAcl	Gibt eine positive Antwort und die ID, den Anzeigenamen und die Berechtigung des Bucket-Eigentümers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf den Bucket hat.
GetBucketCors	Gibt den zurück <code>cors</code> Konfiguration für den Bucket.
GetBucketEncryption	Gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
GetBucketLifecycleKonfiguration  (Zuvor namens „GET Bucket Lifecycle“)	Gibt die Lebenszykluskonfiguration für den Bucket zurück. Siehe " <a href="#">S3-Lebenszykluskonfiguration erstellen</a> ".
GetBucketLocation	Gibt die Region zurück, die mit dem festgelegt wurde <code>LocationConstraint</code> Element in der Anforderung <code>CreateBucket</code> . Wenn der Eimer-Bereich ist <code>us-east-1</code> , Eine leere Zeichenfolge wird für die Region zurückgegeben.
GetBucketNotificationKonfiguration  (Zuvor mit „GET Bucket“-Benachrichtigung bezeichnet)	Gibt die Benachrichtigungskonfiguration zurück, die mit dem Bucket verbunden ist.
GetBucketPolicy	Gibt die dem Bucket angehängte Richtlinie zurück.

Betrieb	Implementierung
GetBucketReplication	Gibt die Replikationskonfiguration zurück, die mit dem Bucket verbunden ist.
GetBucketTagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags für einen Bucket zurückzugeben</p> <p><b>Achtung:</b> Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, gibt es ein <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag mit einem ihm zugewiesenen Wert. Ändern oder entfernen Sie dieses Tag nicht.</p>
GetBucketVersioning	<p>Diese Implementierung verwendet das <code>versioning</code> subressource zur Rückgabe des Versionierungsstatus eines Buckets.</p> <ul style="list-style-type: none"> <li>• <i>Blank</i>: Die Versionierung wurde nie aktiviert (Bucket ist „unversioniert“)</li> <li>• Aktiviert: Versionierung ist aktiviert</li> <li>• Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt</li> </ul>
GetObjectLockConfiguration	<p>Gibt den Standardaufbewahrungsmodus für Bucket und den Standardaufbewahrungszeitraum zurück, sofern konfiguriert.</p> <p>Siehe <a href="#">"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"</a>.</p>
HeadBucket	<p>Legt fest, ob ein Bucket vorhanden ist und Sie über die Berechtigung verfügen, darauf zuzugreifen.</p> <p>Dieser Vorgang liefert Folgendes zurück:</p> <ul style="list-style-type: none"> <li>• <code>x-ntap-sg-bucket-id</code>: Die UUID des Buckets im UUID-Format.</li> <li>• <code>x-ntap-sg-trace-id</code>: Die eindeutige Trace-ID der zugehörigen Anfrage.</li> </ul>
ListObjects und ListObjectsV2  (Zuvor benannt nach „GET Bucket“)	<p>Gibt einige oder alle (bis zu 1,000) Objekte in einem Bucket zurück. Die Speicherklasse für Objekte kann einen von zwei Werten haben, auch wenn das Objekt mit aufgenommen wurde <code>REDUCED_REDUNDANCY</code> Option für Storage-Klasse:</p> <ul style="list-style-type: none"> <li>• <code>STANDARD</code>, Die angibt, dass das Objekt in einem Speicherpool gespeichert wird, der aus Storage-Nodes besteht.</li> <li>• <code>GLACIER</code>, Dies bedeutet, dass das Objekt in den vom Cloud-Speicherpool angegebenen externen Bucket verschoben wurde.</li> </ul> <p>Wenn der Bucket eine große Anzahl von gelöschten Schlüsseln enthält, die dasselbe Präfix haben, kann die Antwort einige enthalten <code>CommonPrefixes</code> Die keine Schlüssel enthalten.</p>
ListObjectVersions  (Zuvor namens „GET Bucket Object Versions“)	<p>Mit Lesezugriff auf einen Bucket, verwenden Sie diesen Vorgang mit dem <code>versions</code> unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.</p>



Betrieb	Implementierung
PutBucketCors	<p>Legt die CORS-Konfiguration für einen Bucket so fest, dass der Bucket Anfragen mit verschiedenen Ursprung bedienen kann. CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen <code>images</code> Zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für das <code>images</code> Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden <code>http://www.example.com</code>.</p>
PutBucketEncryption	<p>Legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Bei aktivierter Verschlüsselung auf Bucket-Ebene sind alle neuen dem Bucket hinzugefügten Objekte verschlüsselt. StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID gemanagten Schlüsseln. Wenn Sie die Konfigurationsregel für die serverseitige Verschlüsselung angeben, legen Sie die fest <code>SSEAlgorithm</code> Parameter an <code>AES256</code> Und verwenden Sie nicht die <code>KMSMasterKeyID</code> Parameter.</p> <p>Die Standardverschlüsselungskonfiguration von Buckets wird ignoriert, wenn in der Anfrage für das Hochladen von Objekten bereits eine Verschlüsselung angegeben ist (d. h., wenn die Anforderung den umfasst <code>x-amz-server-side-encryption-*</code> Kopfzeile der Anfrage).</p>
PutBucketLifecycleKonfiguration  (Zuvor PUT Bucket-Lebenszyklus genannt)	<p>Erstellt eine neue Lebenszykluskonfiguration für den Bucket oder ersetzt eine vorhandene Lebenszykluskonfiguration. StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:</p> <ul style="list-style-type: none"> <li>• Ablauf (Tage, Datum, ErstrecktObjectDeleteMarker)</li> <li>• Nicht-aktuellVersionAblauf (NewerNichtaktuellVersionen, nicht aktuelleTage)</li> <li>• Filter (Präfix, Tag)</li> <li>• Status</li> <li>• ID</li> </ul> <p>StorageGRID bietet folgende Maßnahmen nicht:</p> <ul style="list-style-type: none"> <li>• AbortInsetteMultipartUpload</li> <li>• Übergang</li> </ul> <p>Siehe "<a href="#">S3-Lebenszykluskonfiguration erstellen</a>". Informationen über die Interaktion der Aktion „Ablauf“ in einem Bucket-Lebenszyklus mit den Anweisungen zur ILM-Platzierung finden Sie unter "<a href="#">Wie ILM im gesamten Leben eines Objekts funktioniert</a>".</p> <p><b>Hinweis:</b> Die Konfiguration des Bucket-Lebenszyklus kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lebenszykluskonfiguration wird jedoch für ältere kompatible Buckets nicht unterstützt.</p>

Betrieb	Implementierung
<p>PutBucketNotificationKonfiguration</p> <p>(Zuvor namens „PUT Bucket“-Benachrichtigung)</p>	<p>Konfiguriert Benachrichtigungen für den Bucket mithilfe der XML-Benachrichtigungskonfiguration, die im Anforderungskörper enthalten ist. Sie sollten folgende Implementierungsdetails kennen:</p> <ul style="list-style-type: none"> <li>• StorageGRID unterstützt als Ziele Amazon Simple Notification Service (Amazon SNS) oder Kafka-Themen. SQS (Simple Queue Service)- oder Amazon Lambda-Endpunkte werden nicht unterstützt.</li> <li>• Das Ziel für Benachrichtigungen muss als URN eines StorageGRID-Endpunkts angegeben werden. Endpunkte können mit dem Mandanten-Manager oder der Mandanten-Management-API erstellt werden.</li> </ul> <p>Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, A 400 Bad Request Der Code gibt einen Fehler zurück InvalidArgument.</p> <ul style="list-style-type: none"> <li>• Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden <b>nicht</b> unterstützt. <ul style="list-style-type: none"> <li>◦ s3:ReducedRedundancyLostObject</li> <li>◦ s3:ObjectRestore:Completed</li> </ul> </li> <li>• Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das JSON-Standardformat, außer dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der folgenden Liste gezeigt: <ul style="list-style-type: none"> <li>◦ <b>EventSource</b></li> <li>sgws:s3</li> <li>◦ <b>AwsRegion</b></li> <li>Nicht enthalten</li> <li>◦ * X-amz-id-2*</li> <li>Nicht enthalten</li> <li>◦ <b>arn</b></li> <li>urn:sgws:s3:::bucket_name</li> </ul> </li> </ul>
PutBucketPolicy	<p>Legt die dem Bucket angehängte Richtlinie fest. Siehe "<a href="#">Verwendung von Bucket- und Gruppenzugriffsrichtlinien</a>".</p>

Betrieb	Implementierung
PutBucketReplication	<p>Konfiguriert <a href="#">"StorageGRID CloudMirror Replizierung"</a> Für den Bucket unter Verwendung der XML-Replikationskonfiguration, die im Anforderungskörper bereitgestellt wurde. Für die CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten:</p> <ul style="list-style-type: none"> <li>• StorageGRID unterstützt nur V1 der Replizierungskonfiguration. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstütz <code>Filter</code> Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Weitere Informationen finden Sie unter <a href="#">"Amazon Simple Storage Service User Guide: Replizierungskonfiguration"</a>.</li> <li>• Die Bucket-Replizierung kann für versionierte oder nicht versionierte Buckets konfiguriert werden.</li> <li>• Sie können in jeder Regel der XML-Replikationskonfiguration einen anderen Ziel-Bucket angeben. Ein Quell-Bucket kann auf mehrere Ziel-Bucket replizieren.</li> <li>• Ziel-Buckets müssen als URN der StorageGRID-Endpunkte angegeben werden, wie im Mandantenmanager oder der Mandantenmanagement-API angegeben. Siehe <a href="#">"CloudMirror-Replizierung konfigurieren"</a>.</li> </ul> <p>Der Endpunkt muss vorhanden sein, damit die Replizierungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, schlägt die Anforderung als <code>400 Bad Request</code>. In der Fehlermeldung steht: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> <li>• Sie müssen keinen angeben <code>Role</code> In der Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird bei der Einreichung ignoriert.</li> <li>• Wenn Sie die Storage-Klasse aus der XML-Konfiguration weglassen, verwendet StorageGRID das <code>STANDARD</code> Standardmäßig Storage-Klasse.</li> <li>• Wenn Sie ein Objekt aus dem Quell-Bucket löschen oder den Quell-Bucket selbst löschen, sieht das Verhalten der regionsübergreifenden Replizierung wie folgt aus: <ul style="list-style-type: none"> <li>◦ Wenn Sie das Objekt oder den Bucket löschen, bevor es repliziert wurde, wird das Objekt/Bucket nicht repliziert, und Sie werden nicht benachrichtigt.</li> <li>◦ Wenn Sie das Objekt oder Bucket nach der Replizierung löschen, befolgt StorageGRID das standardmäßige Löschverhalten von Amazon S3 für die V1 der regionsübergreifenden Replizierung.</li> </ul> </li> </ul>

Betrieb	Implementierung
PutBucketTagging	<p>Verwendet das <code>tagging</code> unterressource, um einen Satz von Tags für einen Bucket hinzuzufügen oder zu aktualisieren. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen:</p> <ul style="list-style-type: none"> <li>• StorageGRID und Amazon S3 unterstützen für jeden Bucket bis zu 50 Tags.</li> <li>• Tags, die einem Bucket zugeordnet sind, müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein.</li> <li>• Die Tag-Werte können bis zu 256 Unicode-Zeichen lang sein.</li> <li>• Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.</li> </ul> <p><b>Achtung:</b> Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, gibt es ein <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag mit einem ihm zugewiesenen Wert. Stellen Sie sicher, dass die <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag wird mit dem zugewiesenen Wert in allen PutketTagging-Anforderungen enthalten. Ändern oder entfernen Sie dieses Tag nicht.</p> <p><b>Hinweis:</b> Dieser Vorgang überschreibt alle aktuellen Tags, die der Bucket bereits hat. Wenn vorhandene Tags aus dem Satz weggelassen werden, werden diese Tags für den Bucket entfernt.</p>
PutBucketVersioning	<p>Verwendet das <code>versioning</code> unterressource, um den Versionierungsstatus eines vorhandenen Buckets festzulegen. Sie können den Versionierungsstatus mit einem der folgenden Werte festlegen:</p> <ul style="list-style-type: none"> <li>• Aktiviert: Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Version-ID.</li> <li>• Suspendiert: Deaktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten die Version-ID <code>null</code>.</li> </ul>
PutObjectLockKonfiguration	<p>Konfiguriert oder entfernt den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum für Bucket.</p> <p>Wenn der Standardaufbewahrungszeitraum geändert wird, bleiben die bisherigen Objektversionen unverändert und werden im neuen Standardaufbewahrungszeitraum nicht neu berechnet.</p> <p>Siehe "<a href="#">Konfigurieren Sie die S3-Objektsperre über die S3-REST-API</a>" Ausführliche Informationen finden Sie unter.</p>

## Operationen für Objekte

### Operationen für Objekte

In diesem Abschnitt wird beschrieben, wie das StorageGRID System S3-REST-API-Vorgänge für Objekte implementiert.

Die folgenden Bedingungen gelten für alle Objektvorgänge:

- StorageGRID "**Konsistenzwerte**" Werden von allen Operationen auf Objekten unterstützt, mit Ausnahme der folgenden:
  - GetObjectAcl
  - OPTIONS /
  - PutObjectLegalHold
  - PutObjectRetention
  - SelektierObjectContent
- Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.
- Alle Objekte in einem StorageGRID-Bucket sind im Eigentum des Bucket-Inhabers. Dies umfasst Objekte, die von einem anonymen Benutzer oder einem anderen Konto erstellt wurden.
- Der Zugriff auf Datenobjekte, die über Swift in das StorageGRID System aufgenommen wurden, ist nicht über S3 möglich.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Objektvorgänge implementiert.

Betrieb	Implementierung
DeleteObject	<p>Multi-Faktor Authentication (MFA) und Response Header <code>x-amz-mfa</code> Werden nicht unterstützt.</p> <p>Bei der Verarbeitung einer DeleteObject-Anforderung versucht StorageGRID sofort, alle Kopien des Objekts von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht innerhalb von 30 Sekunden alle Kopien entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien in eine Warteschlange zur Entfernung und zeigt dann den Erfolg des Clients an.</p> <p><b>Versionierung</b></p> <p>Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und den verwenden <code>versionId</code> unterresource. Durch die Verwendung dieser Unterresource wird die Version dauerhaft gelöscht. Wenn der <code>versionId</code> Entspricht einer Löschen-Markierung, dem Antwortkopf <code>x-amz-delete-marker</code> Wird auf festgelegt <code>true</code>.</p> <ul style="list-style-type: none"> <li>• Wird ein Objekt ohne gelöscht <code>versionId</code> unterresource auf einem Bucket mit Versionsfunktion führt zur Generierung einer Löschmarkierung. Der <code>versionId</code> Für die Löschen-Markierung wird mit dem zurückgegeben <code>x-amz-version-id</code> Kopfzeile der Antwort und das <code>x-amz-delete-marker</code> Der Antwortkopf wird auf festgelegt <code>true</code>.</li> <li>• Wird ein Objekt ohne gelöscht <code>versionId</code> unterresource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschmarker und der Generierung eines neuen 'null' Löschmarker. Der <code>x-amz-delete-marker</code> Der Antwortkopf wird auf festgelegt <code>true</code>.</li> </ul> <p><b>Hinweis:</b> In bestimmten Fällen können für ein Objekt mehrere Löschen-Marker vorhanden sein.</p> <p>Siehe "<a href="#">Konfigurieren Sie die S3-Objektsperre über die S3-REST-API</a>" Anleitung zum Löschen von Objektversionen im GOVERNANCE-Modus.</p>
Objekte deObjekteObjekte (Zuvor benanntes DELETE mehrere Objekte)	<p>Multi-Faktor Authentication (MFA) und Response Header <code>x-amz-mfa</code> Werden nicht unterstützt.</p> <p>In derselben Anforderungsmeldung können mehrere Objekte gelöscht werden.</p> <p>Siehe "<a href="#">Konfigurieren Sie die S3-Objektsperre über die S3-REST-API</a>" Anleitung zum Löschen von Objektversionen im GOVERNANCE-Modus.</p>

Betrieb	Implementierung
DeleteObjectTagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Objekt zu entfernen.</p> <p><b>Versionierung</b></p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang löscht alle Tags von der neuesten Version des Objekts in einem versionierten Bucket. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „MethodenNotAllowed“ mit dem zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
GetObject	"GetObject"
GetObjectAcl	Wenn für das Konto die erforderlichen Zugangsdaten bereitgestellt werden, gibt der Vorgang eine positive Antwort und die ID, DisplayName und die Berechtigung des Objekteigentümers zurück und gibt an, dass der Eigentümer vollen Zugriff auf das Objekt hat.
GetObjectLegalHold	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
GetObjectRetention	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
GetObjectTagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags für ein Objekt zurückzugeben.</p> <p><b>Versionierung</b></p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang gibt alle Tags der neuesten Version des Objekts in einem versionierten Bucket zurück. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „MethodenNotAllowed“ mit dem zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
HeadObject	"HeadObject"
Objekt restoreObject	"Objekt restoreObject"
PutObject	"PutObject"
CopyObject  (Zuvor PUT Object – Copy genannt)	"CopyObject"
PutObjectLegalHold	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

Betrieb	Implementierung
PutObjectRetention	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
PutObjectTagging	<p>Verwendet das <code>tagging</code> unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen.</p> <p><b>Grenzwerte für Objekt-Tags</b></p> <p>Sie können neue Objekte mit Tags hinzufügen, wenn Sie sie hochladen, oder Sie können sie zu vorhandenen Objekten hinzufügen. StorageGRID und Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Tags, die einem Objekt zugeordnet sind, müssen über eindeutige Tag-Schlüssel verfügen. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein, und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.</p> <p><b>Tag-Updates und Ingest-Verhalten</b></p> <p>Wenn Sie PutObjectTagging verwenden, um die Tags eines Objekts zu aktualisieren, nimmt StorageGRID das Objekt nicht erneut auf. Das bedeutet, dass die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten nicht verwendet wird. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird.</p> <p>Das heißt, wenn die ILM-Regel die strikte Option für das Aufnahmeverhalten verwendet, werden keine Maßnahmen ergriffen, wenn die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.</p> <p><b>Konflikte lösen</b></p> <p>Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.</p> <p><b>Versionierung</b></p> <p>Wenn der <code>versionId</code> Der Abfrageparameter wird in der Anforderung nicht angegeben, und der Vorgang fügt Tags zur aktuellen Version des Objekts in einem versionierten Bucket hinzu. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „MethodenNotAllowed“ mit dem zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
SelektierObjectContent	"SelektierObjectContent"



## Verwenden Sie S3 Select

StorageGRID unterstützt die folgenden Amazon S3 Select-Klauseln, Datentypen und Operatoren für die ["SelectObjectContent, Befehl"](#).



Nicht aufgeführte Elemente werden nicht unterstützt.

Syntax finden Sie unter ["SelektierObjectContent"](#). Weitere Informationen zu S3 Select finden Sie im ["AWS-Dokumentation für S3 Select"](#).

Nur Mandantenkonten, für die S3 Select aktiviert ist, können SelectObjectContent-Abfragen ausgeben. Siehe ["Überlegungen und Anforderungen bei der Verwendung von S3 Select"](#).

### Klauseln

- Wählen Sie die Liste aus
- FROM-Klausel
- WHERE-Klausel
- BEGRENZUNGSKLAUSEL

### Datentypen

- bool
- Ganzzahl
- Zeichenfolge
- Schweben
- Dezimal, numerisch
- Zeitstempel

### Operatoren

#### Logische Operatoren

- UND
- NICHT
- ODER

#### Vergleichsoperatoren

- <
- >
- &Lt;=
- >=
- =
- =
- <>

- !=
- ZWISCHEN
- IN

#### **Operatoren für die Musteranpassung**

- GEFÄLLT MIR
- \_
- %

#### **Einheitliche Operatoren**

- IST NULL
- IST NICHT NULL

#### **Mathematische Operatoren**

- +
- -
- \*
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

#### **Aggregatfunktionen**

- DURCHSCHN.()
- ANZAHL (\*)
- MAX.()
- MIN.()
- SUMME()

#### **Bedingte Funktionen**

- FALL
- ZUSAMMENSCHMELZEN
- NULL LIF

#### **Konvertierungsfunktionen**

- CAST (für unterstützten Datentyp)

#### **Datumsfunktionen**

- DATUM\_HINZUFÜGEN
- DATE\_DIFF

- EXTRAHIEREN
- TO\_STRING
- TO\_ZEITSTEMPEL
- UTCNOW

### Zeichenfolgenfunktionen

- CHAR\_LENGTH, CHARACTER\_LENGTH
- NIEDRIGER
- TEILSTRING
- TRIMMEN
- OBEN

## Serverseitige Verschlüsselung

Die serverseitige Verschlüsselung schützt Ihre Objektdaten im Ruhezustand. StorageGRID verschlüsselt die Daten beim Schreiben des Objekts und entschlüsselt sie beim Zugriff auf das Objekt.

Wenn Sie die serverseitige Verschlüsselung verwenden möchten, können Sie eine der zwei Optionen auswählen, die sich gegenseitig ausschließen, je nachdem, wie die Verschlüsselungsschlüssel verwaltet werden:

- **SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln):** Bei der Ausgabe einer S3-Anfrage zum Speichern eines Objekts verschlüsselt StorageGRID das Objekt mit einem eindeutigen Schlüssel. Wenn Sie zum Abrufen des Objekts eine S3-Anforderung ausstellen, entschlüsselt StorageGRID das Objekt mithilfe des gespeicherten Schlüssels.
- **SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln):** Wenn Sie eine S3-Anfrage zum Speichern eines Objekts ausgeben, geben Sie Ihren eigenen Verschlüsselungsschlüssel an. Wenn Sie ein Objekt abrufen, geben Sie denselben Verschlüsselungsschlüssel wie in Ihrer Anfrage ein. Stimmen die beiden Verschlüsselungsschlüssel überein, wird das Objekt entschlüsselt und die Objektdaten zurückgegeben.

StorageGRID managt zwar alle Objektverschlüsselung und Entschlüsselungsvorgänge, muss aber die von Ihnen zur Verfügung gelegten Verschlüsselungsschlüssel verwalten.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.



Wenn ein Objekt mit SSE oder SSE-C verschlüsselt wird, werden sämtliche Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

### Verwenden Sie SSE

Um ein Objekt mit einem eindeutigen, von StorageGRID gemanagten Schlüssel zu verschlüsseln, verwenden Sie die folgende Anforderungsüberschrift:

`x-amz-server-side-encryption`

Der SSE-Anforderungsheader wird durch die folgenden Objektoperationen unterstützt:

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

## Verwenden Sie SSE-C

Um ein Objekt mit einem eindeutigen Schlüssel zu verschlüsseln, den Sie verwalten, verwenden Sie drei Anforderungsheader:

Kopfzeile der Anfrage	Beschreibung
x-amz-server-side-encryption-customer-algorithm	Geben Sie den Verschlüsselungsalgorithmus an. Der Kopfzeilenwert muss sein AES256.
x-amz-server-side-encryption-customer-key	Geben Sie den Verschlüsselungsschlüssel an, der zum Verschlüsseln oder Entschlüsseln des Objekts verwendet wird. Der Wert für den Schlüssel muss 256-Bit, base64-codiert sein.
x-amz-server-side-encryption-customer-key-MD5	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der dafür sorgt, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für das MD5 Digest muss base64-kodiert 128-Bit sein.

Die SSE-C-Anfrageheader werden durch die folgenden Objektoperationen unterstützt:

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadTeil"
- "UploadPartCopy"

## Überlegungen zur Verwendung serverseitiger Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

Beachten Sie vor der Verwendung von SSE-C die folgenden Punkte:

- Sie müssen https verwenden.



StorageGRID lehnt alle über http gestellten Anfragen bei der Verwendung von SSE-C. ab Aus Sicherheitsgründen sollten Sie jeden Schlüssel, den Sie versehentlich über http senden, in Betracht ziehen, um kompromittiert zu werden. Entsorgen Sie den Schlüssel, und drehen Sie ihn nach Bedarf.

- Der ETag in der Antwort ist nicht das MD5 der Objektdaten.
- Sie müssen die Zuordnung von Schlüsseln zu Objekten managen. StorageGRID speichert keine Schlüssel. Sie sind für die Nachverfolgung des Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.
- Wenn Ihr Bucket mit Versionierung aktiviert ist, sollte für jede Objektversion ein eigener Verschlüsselungsschlüssel vorhanden sein. Sie sind verantwortlich für das Tracking des Verschlüsselungsschlüssels, der für jede Objektversion verwendet wird.
- Da Sie Verschlüsselungsschlüssel auf Client-Seite verwalten, müssen Sie auch zusätzliche Schutzmaßnahmen, wie etwa die Rotation von Schlüsseln, auf Client-Seite verwalten.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

- Wenn die Grid-übergreifende Replizierung oder CloudMirror Replizierung für den Bucket konfiguriert ist, können SSE-C-Objekte nicht aufgenommen werden. Der Aufnahmevorgang schlägt fehl.

### Verwandte Informationen

["Amazon S3-Benutzerhandbuch: Verwenden der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln \(SSE-C\)"](#)

## CopyObject

Sie können die S3-CopyObject-Anforderung verwenden, um eine Kopie eines Objekts zu erstellen, das bereits in S3 gespeichert ist. Eine CopyObject-Operation ist die gleiche wie GetObject gefolgt von PutObject.

### Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

### Objektgröße

Die maximale *recommended* Größe für eine einzelne PutObject-Operation beträgt 5 gib (5,368,709,120 Bytes). Wenn Objekte größer als 5 gib sind, verwenden Sie ["Mehrteiliges Hochladen"](#) Stattdessen.

Die maximale *supported*-Größe für eine einzelne PutObject-Operation beträgt 5 tib (5,497,558,138,880 Bytes).



Wenn Sie ein Upgrade von StorageGRID 11.6 oder einer älteren Version durchgeführt haben, wird die Warnmeldung „S3 PUT Object size to Large“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das mehr als 5 gib überschreitet. Wenn Sie eine neue Installation von StorageGRID 11.7 oder 11.8 haben, wird die Warnmeldung in diesem Fall nicht ausgelöst. Um sich jedoch auf den AWS S3-Standard abzustimmen, werden zukünftige Versionen von StorageGRID das Hochladen von Objekten, die mehr als 5 gib betragen, nicht unterstützen.

### UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten entgangenen UTF-8 Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

## Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `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-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten
- `x-amz-metadata-directive`: Der Standardwert ist `COPY`, Mit der Sie das Objekt und die zugehörigen Metadaten kopieren können.

Sie können angeben `REPLACE` Um beim Kopieren des Objekts die vorhandenen Metadaten zu überschreiben oder die Objektm Metadaten zu aktualisieren.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Der Standardwert ist `COPY`, Mit dem Sie das Objekt und alle Tags kopieren können.

Sie können angeben `REPLACE` Um die vorhandenen Tags beim Kopieren des Objekts zu überschreiben oder die Tags zu aktualisieren.

- **S3-Objektsperungs-Anfrageheader:**
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

Wenn eine Anforderung ohne diese Header ausgeführt wird, werden die Standardaufbewahrungseinstellungen für Buckets verwendet, um den Versionsmodus des Objekts zu berechnen und das „behalt-bis“-Datum zu erhalten. Siehe ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

- **SSE-Anfragezeilen:**
  - `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`

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

## Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

## Optionen der Storage-Klasse

Der `x-amz-storage-class` Anforderungsheader wird unterstützt und wirkt sich darauf aus, wie viele Objektkopien StorageGRID erstellt, wenn die entsprechende ILM-Regel den doppelten Commit oder ausgewogenen verwendet ["Aufnahme-Option"](#).

- `STANDARD`

(Standard) gibt einen Dual-Commit-Aufnahmevergang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- `REDUCED_REDUNDANCY`

Gibt einen Single-Commit-Aufnahmevergang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitlicher Kopien zurückgreift.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

## Verwenden von `x-amz-copy-source` in `CopyObject`

Wenn der Quell-Bucket und der Schlüssel im angegeben sind `x-amz-copy-source` Kopfzeile: Unterscheidet sich vom Ziel-Bucket und -Schlüssel, eine Kopie der Quell-Objektdaten wird auf das Ziel geschrieben.

Wenn die Quelle und das Ziel übereinstimmen, und die `x-amz-metadata-directive` Kopfzeile wird als

angegeben `REPLACE`, Die Metadaten des Objekts werden mit den Metadaten aktualisiert, die in der Anforderung angegeben sind. In diesem Fall nimmt StorageGRID das Objekt nicht erneut auf. Dies hat zwei wichtige Folgen:

- Sie können `CopyObject` nicht verwenden, um ein vorhandenes Objekt zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts zu ändern. Wenn Sie den bereitstellen `x-amz-server-side-encryption` Kopfzeile oder der `x-amz-server-side-encryption-customer-algorithm` Header, StorageGRID lehnt die Anforderung ab und gibt sie zurück `XNotImplemented`.
- Die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten wird nicht verwendet. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird.

Das heißt, wenn die ILM-Regel die strikte Option für das Aufnahmeverhalten verwendet, werden keine Maßnahmen ergriffen, wenn die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.

## Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie "[Serverseitige Verschlüsselung verwenden](#)" Die von Ihnen bereitgestellten Anforderungsheader hängen davon ab, ob das Quellobjekt verschlüsselt ist und ob Sie das Zielobjekt verschlüsseln möchten.

- Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, müssen Sie die folgenden drei Header in die `CopyObject`-Anforderung aufnehmen, damit das Objekt entschlüsselt und dann kopiert werden kann:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angabe `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.
- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten, müssen Sie die folgenden drei Header angeben:
  - `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Geben Sie einen neuen Verschlüsselungsschlüssel für das Zielobjekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des neuen Verschlüsselungsschlüssels an.



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".

- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID (SSE) verwaltet wird, fügen Sie diesen Header in die `CopyObject`-Anforderung ein:
  - `x-amz-server-side-encryption`





Der `server-side-encryption` Wert des Objekts kann nicht aktualisiert werden. Erstellen Sie stattdessen eine Kopie mit einer neuen `server-side-encryption` Nutzen `x-amz-metadata-directive: REPLACE`.

## Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie den verwenden `x-amz-copy-source` Kopfzeile zum Kopieren der neuesten Version eines Objekts. Zum Kopieren einer bestimmten Version eines Objekts müssen Sie explizit die Version angeben, die kopiert werden soll `versionId` unterressource. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im zurückgegeben `x-amz-version-id` Kopfzeile der Antwort. Wenn die Versionierung für den Ziel-Bucket ausgesetzt ist, dann `x-amz-version-id` Gibt einen „Null“-Wert zurück.

## GetObject

Mithilfe der S3-GetObject-Anforderung können Sie ein Objekt aus einem S3-Bucket abrufen.

### GetObject- und mehrteilige Objekte

Sie können das verwenden `partNumber` Parameter anfordern, um einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abzurufen. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können festlegen `partNumber` Zu 1 für segmentierte/mehrteilige Objekte und nicht segmentierte/nicht mehrteilige Objekte; jedoch die `x-amz-mp-parts-count` Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

### UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. GET Requests for an object with escaped UTF-8 characters in user-defined metadata don't return the `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

### Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

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

## Versionierung

Wenn A `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „nicht gefunden“ mit dem zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

### Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den

Sie angegeben haben.

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



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

## Verhalten von `GetObject` for Cloud Storage Pool Objects

Wenn ein Objekt in einem gespeichert wurde "[Cloud-Storage-Pool](#)" Das Verhalten einer `GetObject`-Anfrage hängt vom Zustand des Objekts ab. Siehe "[HeadObject](#)" Entnehmen.



Wenn ein Objekt in einem Cloud Storage-Pool gespeichert ist und eine oder mehrere Kopien des Objekts ebenfalls im Raster vorhanden sind, versucht `GetObject` Requests, die Daten aus dem Raster abzurufen, bevor sie aus dem Cloud Storage-Pool abgerufen werden.

Status des Objekts	Verhalten von <code>GetObject</code>
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	200 OK  Eine Kopie des Objekts wird abgerufen.
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK  Eine Kopie des Objekts wird abgerufen.
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	403 Forbidden, InvalidObjectState  Verwenden Sie A " <a href="#">Objekt restoreObject</a> " Anforderung zur Wiederherstellung des Objektstatus in einem abrufbaren Zustand.
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	403 Forbidden, InvalidObjectState  Warten Sie, bis die Anforderung „RestoreObject“ abgeschlossen ist.
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK  Eine Kopie des Objekts wird abgerufen.

## Mehrteilige oder segmentierte Objekte in einem Cloud Storage-Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In einigen Fällen kann eine GetObject-Anforderung falsch zurückgegeben werden 200 OK Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

In diesen Fällen:

- Die GetObject-Anforderung gibt möglicherweise einige Daten zurück, hält jedoch während der Übertragung an.
- Eine nachfolgende GetObject-Anforderung kann zurückgegeben werden 403 Forbidden.

## GetObject- und Grid-übergreifende Replikation

Wenn Sie verwenden "Grid-Verbund" Und "Grid-übergreifende Replizierung" Ist für einen Bucket aktiviert, kann der S3-Client den Replikationsstatus eines Objekts durch Ausgabe einer GetObject-Anforderung überprüfen. Die Antwort bezieht sich auf das StorageGRID-spezifische `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none"><li>• <b>SUCCESS:</b> Die Replikation war erfolgreich.</li><li>• <b>AUSSTEHEND:</b> Das Objekt wurde noch nicht repliziert.</li><li>• <b>FAILURE:</b> Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.</li></ul>
Ziel	<b>REPLIKAT:</b> Das Objekt wurde aus dem Quellraster repliziert.



StorageGRID unterstützt das nicht `x-amz-replication-status` Kopfzeile.

## HeadObject

Sie können die S3 HeadObject-Anforderung verwenden, um Metadaten von einem Objekt abzurufen, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem Cloud-Speicherpool gespeichert ist, können Sie HeadObject verwenden, um den Übergangstatus des Objekts zu bestimmen.

## HeadObject- und mehrteilige Objekte

Sie können das verwenden `partNumber` Parameter anfordern, um Metadaten für einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abzurufen. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können festlegen `partNumber` Zu 1 für segmentierte/mehrteilige Objekte und nicht segmentierte/nicht mehrteilige Objekte; jedoch die `x-amz-mp-parts-count` Antwortelement wird nur für segmentierte oder mehrteilige Objekte zurückgegeben.

## UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. HEAD-Anforderungen für ein Objekt mit ausbleibenden UTF-8-Zeichen in benutzerdefinierten Metadaten geben den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

## Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

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

## Versionierung

Wenn `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „nicht gefunden“ mit dem zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

## Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei dieser Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den Sie angegeben haben.

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



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

## HeadObject-Antworten für Cloud-Storage-Pool-Objekte

Wenn das Objekt in einem gespeichert ist "[Cloud-Storage-Pool](#)", Die folgenden Antwortheader werden zurückgegeben:

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

Die Antwortheader liefern Informationen zum Status eines Objekts beim Verschieben in einen Cloud Storage Pool, beim Wechsel in einen nicht abrufbaren Zustand und wieder verfügbar.

Status des Objekts	Antwort auf HeadObject
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	200 OK (Es wird keine spezielle Answerheader zurückgegeben.)
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>`x-amz-restore: Laufend-request=„false“, expiry-date=„Sa, 23. Juli 20 2030 00:00:00 Uhr GMT“</p> <p>Bis das Objekt in einen nicht aufrufbaren Zustand überführt wird, wird der Wert für expiry-date Wird in der Zukunft auf eine ferne Zeit gesetzt. Die genaue Zeit der Transition wird nicht durch das StorageGRID System gesteuert.</p>
Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>`x-amz-restore: Laufend-request=„false“, expiry-date=„Sa, 23. Juli 20 2030 00:00:00 Uhr GMT“</p> <p>Der Wert für expiry-date Wird in der Zukunft auf eine ferne Zeit gesetzt.</p> <p><b>Hinweis:</b> Wenn die Kopie auf dem Raster nicht verfügbar ist (z. B. ist ein Storage Node ausgefallen), müssen Sie einen ausstellen "<a href="#">Objekt restoreObject</a>" Anforderung zur Wiederherstellung der Kopie aus dem Cloud-Storage-Pool, bevor Sie das Objekt erfolgreich abrufen können.</p>
Das Objekt wurde in einen nicht abrufbaren Zustand versetzt, und es ist keine Kopie im Grid vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>`x-amz-restore: Laufend-request=„wahr“</p>

Status des Objekts	Antwort auf HeadObject
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK  x-amz-storage-class: GLACIER  `x-amz-restore: Laufend-request=„false“, expiry-date=„Sa, 23. Juli 20 2018 00:00:00 Uhr GMT“  Der expiry-date Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.

### Mehrteilige oder segmentierte Objekte in Cloud Storage Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In einigen Fällen gibt eine HeadObject-Anforderung fälschlicherweise `x-amz-restore: Laufend-request="false" zurück, wenn einige Teile des Objekts bereits in einen nicht abrufbaren Zustand überführt wurden oder wenn Teile des Objekts noch nicht wiederhergestellt wurden.

### HeadObject- und Grid-übergreifende Replikation

Wenn Sie verwenden "Grid-Verbund" Und "Grid-übergreifende Replizierung" Ist für einen Bucket aktiviert, kann der S3-Client den Replikationsstatus eines Objekts durch Ausgabe einer HeadObject-Anforderung überprüfen. Die Antwort bezieht sich auf das StorageGRID-spezifische x-ntap-sg-cgr-replication-status Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	<ul style="list-style-type: none"> <li>• <b>SUCCESS:</b> Die Replikation war erfolgreich.</li> <li>• <b>AUSSTEHEND:</b> Das Objekt wurde noch nicht repliziert.</li> <li>• <b>FAILURE:</b> Die Replikation ist mit einem permanenten Fehler fehlgeschlagen. Ein Benutzer muss den Fehler beheben.</li> </ul>
Ziel	<b>REPLIKAT:</b> Das Objekt wurde aus dem Quellraster repliziert.



StorageGRID unterstützt das nicht x-amz-replication-status Kopfzeile.

## PutObject

Sie können die S3 PutObject-Anforderung verwenden, um einem Bucket ein Objekt hinzuzufügen.

### Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht

auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

## Objektgröße

Die maximale *recommended* Größe für eine einzelne PutObject-Operation beträgt 5 gib (5,368,709,120 Bytes). Wenn Objekte größer als 5 gib sind, verwenden Sie ["Mehrteiliges Hochladen"](#) Stattdessen.

Die maximale *supported*-Größe für eine einzelne PutObject-Operation beträgt 5 tib (5,497,558,138,880 Bytes).



Wenn Sie ein Upgrade von StorageGRID 11.6 oder einer älteren Version durchgeführt haben, wird die Warnmeldung „S3 PUT Object size to Large“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das mehr als 5 gib überschreitet. Wenn Sie eine neue Installation von StorageGRID 11.7 oder 11.8 haben, wird die Warnmeldung in diesem Fall nicht ausgelöst. Um sich jedoch auf den AWS S3-Standard abzustimmen, werden zukünftige Versionen von StorageGRID das Hochladen von Objekten, die mehr als 5 gib betragen, nicht unterstützen.

## Größe der Benutzer-Metadaten

Amazon S3 begrenzt die Größe der benutzerdefinierten Metadaten innerhalb jeder PUT-Anforderung-Kopfzeile auf 2 KB. StorageGRID begrenzt die Benutzermetadaten auf 24 KiB. Die Größe der benutzerdefinierten Metadaten wird gemessen, indem die Summe der Anzahl Bytes in der UTF-8-Codierung jedes Schlüssels und jeden Wert angegeben wird.

## UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- PutObject-, CopyObject-, GetObject- und HeadObject-Anfragen werden erfolgreich ausgeführt, wenn benutzerdefinierte Metadaten UTF-8-Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

## Grenzwerte für Objekt-Tags

Sie können neue Objekte mit Tags hinzufügen, wenn Sie sie hochladen, oder Sie können sie zu vorhandenen Objekten hinzufügen. StorageGRID und Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Tags, die einem Objekt zugeordnet sind, müssen über eindeutige Tag-Schlüssel verfügen. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein, und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.

## Objekteigentümer

In StorageGRID sind alle Objekte Eigentum des Bucket-Besitzers-Kontos, einschließlich der Objekte, die von einem Konto ohne Eigentümer oder einem anonymen Benutzer erstellt wurden.

## Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- Cache-Control
- Content-Disposition
- Content-Encoding

Wenn Sie angeben `aws-chunked` Für Content-EncodingStorageGRID überprüft die folgenden Elemente nicht:

- StorageGRID überprüft das nicht `chunk-signature` Auf die Chunk-Daten:
- StorageGRID überprüft nicht den Wert, den Sie für angeben `x-amz-decoded-content-length` Gegen das Objekt.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

Die Chunked-Übertragungscodierung wird unterstützt, wenn `aws-chunked` Zudem wird das Nutzlastsignieren verwendet.

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

Verwenden Sie bei der Angabe des Name-value-Paars für benutzerdefinierte Metadaten dieses allgemeine Format:

```
x-amz-meta-name: value
```

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie diese verwenden `creation-time` Als Name der Metadaten, die beim Erstellen des Objekts zeichnet. Beispiel:

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

Der Wert für `creation-time` Wird seit dem 1. Januar 1970 als Sekunden ausgewertet.



Eine ILM-Regel kann nicht sowohl eine **benutzerdefinierte Erstellungszeit** für die Referenzzeit als auch die Option `Balanced` oder `Strict Ingest` verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

- `x-amz-tagging`
- S3-Objektsperungs-Anfrageheader
  - `x-amz-object-lock-mode`



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

Wenn eine Anforderung ohne diese Header ausgeführt wird, werden die Standardaufbewahrungseinstellungen für Buckets verwendet, um den Versionsmodus des Objekts zu berechnen und das „behalt-bis“-Datum zu erhalten. Siehe ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

- SSE-Anfragezeilen:

- 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

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

## Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- Der x-amz-acl Die Anforderungsüberschrift wird nicht unterstützt.
- Der x-amz-website-redirect-location Die Anforderungsüberschrift wird nicht unterstützt und gibt zurück XNotImplemented.

## Optionen der Storage-Klasse

Der x-amz-storage-class Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde x-amz-storage-class Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die Option „Strict Ingest“ verwendet, wird die verwendet x-amz-storage-class Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden x-amz-storage-class:

- STANDARD (Standard)
  - **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell 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 sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt x-amz-storage-class Kopfzeile hat keine Wirkung.

- `REDUCED_REDUNDANCY`

- **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
- **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevergang nicht mehr erstellt und gelöscht werden.

Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angaben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Sie wirkt sich nicht darauf aus, wie viele Kopien des Objekts erstellt werden, wenn das Objekt durch die aktiven ILM-Richtlinien evaluiert wird, und führt nicht dazu, dass Daten mit niedrigerer Redundanz im StorageGRID System gespeichert werden.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

## Anforderungsheader für serverseitige Verschlüsselung

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

- **SSE:** Verwenden Sie den folgenden Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird.
  - `x-amz-server-side-encryption`
- **SSE-C:** Verwenden Sie alle drei dieser Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".



Wenn ein Objekt mit SSE oder SSE-C verschlüsselt wird, werden sämtliche Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

## Versionierung

Wenn die Versionierung für einen Bucket aktiviert ist, ist dies ein eindeutiger `versionId`. Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

Wenn die Versionierung unterbrochen wird, wird die Objektversion mit einem Null gespeichert `versionId`. Und wenn bereits eine Null-Version vorhanden ist, wird sie überschrieben.

## Signaturberechnungen für den Autorisierungskopf

Bei Verwendung des `Authorization` Header zur Authentifizierung von Anfragen unterscheidet sich StorageGRID von AWS folgendermaßen:

- StorageGRID erfordert nicht `host` Kopfzeilen, die in enthalten sein sollen `CanonicalHeaders`.
- StorageGRID erfordert nicht `Content-Type` in enthalten sein `CanonicalHeaders`.
- StorageGRID erfordert nicht `x-amz-*` Kopfzeilen, die in enthalten sein sollen `CanonicalHeaders`.



Als allgemeine Best Practice sollten Sie diese Kopfzeilen immer in aufnehmen `CanonicalHeaders`. Um sicherzustellen, dass sie überprüft werden; wenn Sie diese Header jedoch ausschließen, gibt StorageGRID keinen Fehler zurück.

Weitere Informationen finden Sie unter "[Signaturberechnungen für den Autorisierungskopf: Payload in einem einzelnen Chunk übertragen \(AWS Signature Version 4\)](#)".

## Verwandte Informationen

["Objektmanagement mit ILM"](#)

## Objekt `restoreObject`

Sie können die S3-Wiederherstellungs-Objekt-Anforderung verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Storage-Pool gespeichert ist.

## Unterstützter Anforderungstyp

StorageGRID unterstützt nur `RestoreObject`-Anfragen zur Wiederherstellung eines Objekts. Das unterstützt nicht `SELECT` Art der Wiederherstellung. Wählen Sie Rückgabeanforderungen aus `XNotImplemented`.

## Versionierung

Geben Sie optional an `versionId` Zum Wiederherstellen einer bestimmten Version eines Objekts in einem versionierten Bucket. Wenn Sie keine Angabe machen `versionId`, Die neueste Version des Objekts wird

wiederhergestellt

## Verhalten von RestoreObject auf Cloud-Storage-Pool-Objekten

Wenn ein Objekt in einem gespeichert wurde "Cloud-Storage-Pool", Eine RestoreObject-Anforderung hat das folgende Verhalten, basierend auf dem Zustand des Objekts. Siehe "HeadObject" Entnehmen.



Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Raster vorhanden sind, besteht keine Notwendigkeit, das Objekt durch Ausgabe einer RestoreObject-Anforderung wiederherzustellen. Stattdessen kann die lokale Kopie mithilfe einer GetObject-Anforderung direkt abgerufen werden.

Status des Objekts	Verhalten von RestoreObject
Objekt wird in StorageGRID aufgenommen, aber noch nicht durch ILM evaluiert oder Objekt befindet sich nicht in einem Cloud-Storage-Pool	403 Forbidden, InvalidObjectState
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK Es werden keine Änderungen vorgenommen. <b>Hinweis:</b> Bevor ein Objekt in einen nicht-abrufbaren Zustand überführt wurde, kann es nicht geändert werden <code>expiry-date</code> .
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	202 Accepted Stellt eine abrufbare Kopie des Objekts für die im Anforderungstext angegebene Anzahl an Tagen in den Cloud-Speicher-Pool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht aufrufbaren Zustand zurückgeführt.  Verwenden Sie optional den <code>Tier</code> Element anfordern, um zu bestimmen, wie lange der Wiederherstellungsauftrag dauern wird (Expedited, Standard, Oder Bulk). Wenn Sie keine Angabe machen <code>Tier</code> , Das Standard <code>Tier</code> wird verwendet.  <b>Wichtig:</b> Wenn ein Objekt in S3 Glacier Deep Archive überführt wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, können Sie es nicht mit wiederherstellen Expedited Ebene: Der folgende Fehler wird zurückgegeben 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	409 Conflict, RestoreAlreadyInProgress

Status des Objekts	Verhalten von RestoreObject
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	<p>200 OK</p> <p><b>Hinweis:</b> Wenn ein Objekt in einen aufrufbaren Zustand wiederhergestellt wurde, können Sie dessen <code>expiry-date</code> ändern. Durch erneute Ausgabe der RestoreObject-Anforderung mit einem neuen Wert für <code>Days</code>. Das Wiederherstellungsdatum wird zum Zeitpunkt der Anfrage aktualisiert.</p>

## SelektierObjectContent

Sie können die S3 SelectObjectContent-Anfrage verwenden, um den Inhalt eines S3-Objekts anhand einer einfachen SQL-Anweisung zu filtern.

Weitere Informationen finden Sie unter ["Amazon Simple Storage Service API Reference: SelectObjectContent"](#).

### Bevor Sie beginnen

- Das Mandantenkonto hat die S3 Select-Berechtigung.
- Das ist schon `s3:GetObject` Berechtigung für das Objekt, das Sie abfragen möchten.
- Das Objekt, das Sie abfragen möchten, muss eines der folgenden Formate aufweisen:
  - **CSV**. Kann wie ist verwendet oder in GZIP- oder BZIP2-Archiven komprimiert werden.
  - **Parkett**. Zusätzliche Anforderungen an Parkett-Objekte:
    - S3 Select unterstützt nur Spaltenkomprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Komprimierung ganzer Objekte für Parkett-Objekte.
    - S3 Select unterstützt keine Parkett-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
    - Die maximale Größe der nicht komprimierten Zeilengruppe beträgt 512 MB.
    - Sie müssen die im Objektschema angegebenen Datentypen verwenden.
    - Sie können KEINE logischen TYPEN VON INTERVALL, JSON, LISTE, ZEIT oder UUID verwenden.
- Ihr SQL-Ausdruck hat eine maximale Länge von 256 KB.
- Jeder Datensatz im Eingang oder Ergebnis hat eine maximale Länge von 1 MiB.

### Beispiel für eine CSV-Anfrage-Syntax

```

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>

```

### Beispiel für die Syntax der Parkettanforderung

```

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>

```

### Beispiel für eine SQL-Abfrage

Diese Abfrage erhält den Staatsnamen, 2010 Populationen, geschätzte 2015 Populationen und den Prozentsatz der Änderung von den Daten der US-Volkszählung. Datensätze in der Datei, die keine Status sind, werden ignoriert.

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

Die ersten Zeilen der abzufragenden Datei, SUB-EST2020\_ALL.csv, So aussehen:

```
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
```

### Beispiel für die Verwendung von AWS und CLI (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
```

Die ersten Zeilen der Ausgabedatei, changes.csv, So aussehen:

```
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
```



## Beispiel für die Nutzung von AWS-CLI (Parkett)

```
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
```

Die ersten Zeilen der Ausgabedatei, changes.csv, sehen wie folgt aus:

```
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
```

## Vorgänge für mehrteilige Uploads

### Operationen für mehrteilige Uploads: Übersicht

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

Die folgenden Bedingungen und Hinweise gelten für alle mehrteiligen Uploadvorgänge:

- Sie sollten 1,000 gleichzeitige mehrteilige Uploads auf einen einzelnen Bucket nicht überschreiten, da die Ergebnisse von ListMultipartUploads Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse liefern.
- StorageGRID setzt AWS Größenbeschränkungen für mehrere Teile durch. S3-Clients müssen folgende Richtlinien einhalten:
  - Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5,242,880 Byte) und 5 gib (5,368,709,120 Byte) liegen.
  - Der letzte Teil kann kleiner als 5 MiB (5,242,880 Byte) sein.
  - Im Allgemeinen sollten die Teilemaße so groß wie möglich sein. Verwenden Sie z. B. für ein Objekt mit 100 gib die Teilenummer 5 gib. Da jedes Teil als ein eindeutiges Objekt angesehen wird, sinkt der Overhead für StorageGRID Metadaten durch die Verwendung großer Teilgrößen.
  - Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.
- ILM wird für jeden Teil eines Mehrteiligen Objekts in der Aufnahme und für das Objekt als Ganzes nach Abschluss des mehrteiligen Uploads evaluiert, sofern die ILM-Regel den ausgeglichenen oder den strengen verwendet **"Aufnahme-Option"**. Sie sollten sich bewusst sein, wie dies die Objekt- und Teileplatzierung beeinflusst:

- Wenn sich ILM ändert, während ein S3-Multipart-Upload durchgeführt wird, erfüllen einige Teile des Objekts möglicherweise nicht die aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. Alle nicht korrekt platzierten Teile werden in die Warteschlange zur erneuten ILM-Bewertung gestellt und später an den richtigen Ort verschoben.
- Bei der Evaluierung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils und nicht der Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. in einer Regel festgelegt wird, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert sind, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei DC2 beim Einspielen gespeichert. Wird ILM für das gesamte Objekt evaluiert, werden alle Teile des Objekts nach DC1 verschoben.
- Alle mehrteiligen Uploads unterstützen StorageGRID **"Konsistenzwerte"**.
- Wenn ein Objekt mithilfe von mehrteiligen Uploads aufgenommen wird, wird der angezeigt **"Schwellenwert für Objektsegmentierung (1 gib)"** Wird nicht angewendet.
- Nach Bedarf können Sie verwenden **"Serverseitige Verschlüsselung"** Mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln) zu verwenden, müssen Sie das angeben `x-amz-server-side-encryption` Request Header 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 die gleichen drei Verschlüsselungsschlüsselanforderungsheader an.

Betrieb	Implementierung
AbortMehnteilaUpload	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
CompleteMultipartUpload	Siehe <b>"CompleteMultipartUpload"</b>
CreateMultipartUpload (Zuvor mehrteiliges Hochladen initiieren)	Siehe <b>"CreateMultipartUpload"</b>
ListMultipartUploads	Siehe <b>"ListMultipartUploads"</b>
ListenTeile	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
UploadTeil	Siehe <b>"UploadTeil"</b>
UploadPartCopy	Siehe <b>"UploadPartCopy"</b>

## CompleteMultipartUpload

Der CompleteMultipartUpload-Vorgang führt einen mehrteiligen Upload eines Objekts durch, indem die zuvor hochgeladenen Teile zusammengelegt werden.

## Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

## Anfragekopfzeilen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und beeinflusst die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die entsprechende ILM-Regel den doppelten Commit oder den ausgeglichenen definiert "[Aufnahme-Option](#)".

- STANDARD

(Standard) gibt einen Dual-Commit-Aufnahmeprozess an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- REDUCED\_REDUNDANCY

Gibt einen Single-Commit-Aufnahmeprozess an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitlicher Kopien zurückgreift.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt REDUCED\_REDUNDANCY Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der REDUCED\_REDUNDANCY Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.



Wenn ein mehrteiler 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 Implementierung der Amazon S3-API ETag Wert für mehrteilige Objekte.

## Versionierung

Durch diesen Vorgang ist ein mehrteiler Upload abgeschlossen. 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, ist dies ein eindeutiger `versionId` Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` Wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

Wenn die Versionierung unterbrochen wird, wird die Objektversion mit einem Null gespeichert `versionId` Und wenn bereits eine Null-Version vorhanden ist, wird sie überschrieben.



Wenn die Versionierung für einen Bucket aktiviert ist, erstellt das Abschließen eines mehrteiligen Uploads immer eine neue Version, selbst wenn mehrere Teile gleichzeitig auf denselben Objektschlüssel hochgeladen wurden. Wenn die Versionierung für einen Bucket nicht aktiviert ist, ist es möglich, einen mehrteiligen Upload zu initiieren und dann einen weiteren mehrteiligen Upload zu initiieren und zuerst auf demselben Objektschlüssel abzuschließen. In Buckets, die nicht versioniert sind, hat der mehrteilige Upload, der den letzten Teil abschließt, Vorrang.

## Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

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

In diesem Fall wird im Grid Manager on Total Events (SMTT) ein Alarm ausgelöst. In der Meldung Letztes Ereignis wird für das letzte Objekt, dessen Benachrichtigung fehlgeschlagen ist, „Benachrichtigungen für Bucket-nameobject-Schlüssel konnten nicht veröffentlicht werden“ angezeigt. (Um diese Meldung anzuzeigen, wählen Sie **NODES** > **Storage Node** > **Ereignisse**. Letztes Ereignis oben in der Tabelle anzeigen.) Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

Ein Mandant kann die fehlgeschlagene Replizierung oder Benachrichtigung auslösen, indem die Metadaten oder Tags des Objekts aktualisiert werden. Ein Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

## CreateMultipartUpload

Der Vorgang CreateMultipartUpload (zuvor Multipart-Upload initiieren) initiiert einen mehrteiligen Upload für ein Objekt und gibt eine Upload-ID zurück.

Der `x-amz-storage-class` Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde `x-amz-storage-class` Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, das strikte verwendet "Aufnahme-Option", Das `x-amz-storage-class` Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden `x-amz-storage-class`:

- **STANDARD** (Standard)
  - **Dual Commit:** Wenn die ILM-Regel die Option Dual Commit Ingest angibt, wird, sobald ein Objekt aufgenommen wird, eine zweite Kopie dieses Objekts erstellt und an einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell 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 sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- `REDUCED_REDUNDANCY`

- **Dual Commit:** Wenn die ILM-Regel die Option Dual Commit angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzige Zwischenkopie (Single Commit).
- **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevergang nicht mehr erstellt und gelöscht werden.

Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angaben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Sie wirkt sich nicht darauf aus, wie viele Kopien des Objekts erstellt werden, wenn das Objekt durch die aktiven ILM-Richtlinien evaluiert wird, und führt nicht dazu, dass Daten mit niedrigerer Redundanz im StorageGRID System gespeichert werden.



Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Die folgenden Abfragezeilen werden unterstützt:

- `Content-Type`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten

Verwenden Sie bei der Angabe des Name-value-Paars für benutzerdefinierte Metadaten dieses allgemeine Format:

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

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie diese verwenden `creation-time` Als Name der Metadaten, die beim Erstellen des Objekts zeichnet. Beispiel:

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

Der Wert für `creation-time` Wird seit dem 1. Januar 1970 als Sekunden ausgewertet.



Wird Hinzugefügt `creation-time` Da benutzerdefinierte Metadaten nicht zulässig sind, wenn Sie einem Bucket hinzufügen, auf dem die ältere Compliance aktiviert ist, ein Objekt. Ein Fehler wird zurückgegeben.

- **S3-Objektsperungs-Anfrageheader:**

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

Wenn eine Anfrage ohne diese Header erstellt wird, werden die Bucket-Standardeinstellungen zur Aufbewahrung der Objektversion herangezogen, um die Aufbewahrung bis dato zu berechnen.

["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)

- **SSE-Anfragezeilen:**

- `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 darüber, wie StorageGRID UTF-8-Zeichen verarbeitet, 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`-Anfrage, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird. Geben Sie diesen Header in keiner der `UploadPart`-Anforderungen 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`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen für prüfen "[Serverseitige Verschlüsselung](#)".

## Nicht unterstützte Anforderungsheader

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`

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

## Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und ggf. versioniert), wenn der `CompleteMultipartUpload`-Vorgang ausgeführt wird.

## ListMultipartUploads

Der Vorgang `ListMultipartUploads` listet mehrteilige Uploads für einen Bucket auf, die gerade ausgeführt werden.

Die folgenden Anforderungsparameter werden unterstützt:

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

## Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und ggf. versioniert), wenn der `CompleteMultipartUpload`-Vorgang ausgeführt wird.

## UploadTeil

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

## Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- Content-Length
- Content-MD5

## Anforderungsheader für serverseitige Verschlüsselung

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

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



Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

## Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und ggf. versioniert), wenn der CompleteMultipartUpload-Vorgang ausgeführt wird.

## UploadPartCopy

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

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

Diese Anforderung liest und schreibt die Objektdaten, die in angegeben wurden x-amz-copy-source-range Innerhalb des StorageGRID-Systems.

Die folgenden Anfragezeilen 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 die SSE-C-Verschlüsselung für die CreateMultipartUpload-Anforderung angegeben haben, müssen Sie auch die folgenden Anforderungsheader in jede UploadPartCopy-Anforderung einschließen:

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

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

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angabe 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 zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Schutz von Objektdaten verwenden, sollten Sie die Überlegungen in prüfen "[Serverseitige Verschlüsselung](#)".

## Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und ggf. versioniert), wenn der CompleteMultipartUpload-Vorgang ausgeführt wird.

## Fehlerantworten

Das StorageGRID System unterstützt alle zutreffenden S3-REST-API-Standardfehlerantworten. Darüber hinaus fügt die StorageGRID Implementierung mehrere individuelle Antworten hinzu.

### Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
AccessDenied	403 Verbotene
BadDigest	400 Fehlerhafte Anfrage
BucketAlreadyExists	409 Konflikt

<b>Name</b>	<b>HTTP-Status</b>
BucketNotEmpty	409 Konflikt
IncompleteBody	400 Fehlerhafte Anfrage
Interner Fehler	500 Fehler Des Internen Servers
InvalidAccessKey ID	403 Verbotene
InvalidArgument	400 Fehlerhafte Anfrage
InvalidBucketName	400 Fehlerhafte Anfrage
InvalidBucketState	409 Konflikt
InvalidDigest	400 Fehlerhafte Anfrage
InvalidVerschlüsselungAlgorithmFehler	400 Fehlerhafte Anfrage
InvalidTeil	400 Fehlerhafte Anfrage
InvalidPartOrder	400 Fehlerhafte Anfrage
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
InvalidRequest	400 Fehlerhafte Anfrage
InvalidStorageClass	400 Fehlerhafte Anfrage
InvalidTag	400 Fehlerhafte Anfrage
InvalidURI	400 Fehlerhafte Anfrage
KeyTooLong	400 Fehlerhafte Anfrage
MalformedXML	400 Fehlerhafte Anfrage
MetadataTooLarge	400 Fehlerhafte Anfrage
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich
MissingRequestBodyError	400 Fehlerhafte Anfrage

Name	HTTP-Status
MissingSecurityHeader	400 Fehlerhafte Anfrage
NoSuchBucket	404 Nicht Gefunden
NoSuchKey	404 Nicht Gefunden
NoSuchUpload	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
NoSuchBucketRichtlinien	404 Nicht Gefunden
ObjektLockKonfigurationNichtgefundenFehler	404 Nicht Gefunden
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
AnforderungTimeTooSkewed	403 Verbotene
Servicenicht verfügbar	503 Service Nicht Verfügbar
SignalDoesNotMatch	403 Verbotene
TooManyDickets	400 Fehlerhafte Anfrage
UserKeyMustBespezifiziert	400 Fehlerhafte Anfrage

## Benutzerdefinierte StorageGRID-Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecyleNotAlled	In einem zuvor konformen Bucket ist die Konfiguration des Bucket-Lebenszyklus nicht zulässig	400 Fehlerhafte Anfrage
XBucketPolicyParseException	Fehler beim Parsen der JSON der empfangenen Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XComplianceKonflikt	Vorgang aufgrund von Compliance-Einstellungen abgelehnt.	403 Verbotene
XComplianceReducedRAID-RedundanzVerbotenen	Reduzierte Redundanz ist in einem älteren, konformen Bucket nicht zulässig	400 Fehlerhafte Anfrage

<b>Name</b>	<b>Beschreibung</b>	<b>HTTP-Status</b>
XMaxBucketPolicyLengthexceed	Ihre Richtlinie überschreitet die maximal zulässige Länge der Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XMissingInternRequestHeader	Eine Kopfzeile einer internen Anforderung fehlt.	400 Fehlerhafte Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die veraltete Compliance nicht aktiviert.	404 Nicht Gefunden
XNotAcceptable	Die Anforderung enthält mindestens einen Übernehmen-Header, der nicht erfüllt werden konnte.	406 Nicht Akzeptabel
XNotImplemsted	Die von Ihnen gestellte Anfrage beinhaltet Funktionen, die nicht implementiert sind.	501 Nicht Implementiert

## 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, BEISPIELHAFTE 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.