



# **Unterstützte Vorgänge und Einschränkungen durch S3-REST-API**

## **StorageGRID 11.5**

NetApp  
April 11, 2024

# Inhalt

- Unterstützte Vorgänge und Einschränkungen durch S3-REST-API . . . . . 1
  - Umgang mit Daten . . . . . 1
  - Allgemeine Anfragemöpfe . . . . . 1
  - Allgemeine Antwortkopfzeilen . . . . . 2
  - Authentifizierung von Anforderungen . . . . . 2
  - Betrieb auf dem Service . . . . . 3
  - Operationen auf Buckets . . . . . 3
  - Benutzerdefinierte Vorgänge für Buckets . . . . . 18
  - Operationen für Objekte . . . . . 20
  - Vorgänge für mehrteilige Uploads . . . . . 44
  - Fehlerantworten . . . . . 53

# Unterstützte Vorgänge und Einschränkungen durch S3-REST-API

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.

- "Authentifizierung von Anforderungen"
- "Betrieb auf dem Service"
- "Operationen auf Buckets"
- "Benutzerdefinierte Vorgänge für Buckets"
- "Operationen für Objekte"
- "Vorgänge für mehrteilige Uploads"
- "Fehlerantworten"

## 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 gemeinsame Anfrageheader, die von der *Simple Storage Service API Reference* definiert wurden, 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 vorgesehenen <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

### Verwandte Informationen

["Amazon Web Services \(AWS\) Dokumentation: Amazon Simple Storage Service API Reference"](#)

## Authentifizierung von Anforderungen

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 der HTTP-Autorisierungsüberschrift

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 werden verwendet

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 vorsignierten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zugreifen zu können, wodurch Sie einen eingeschränkten Zugriff auf eine Ressource durch Dritte ermöglichen können.

## Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
GET Service	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
GET Storage-Auslastung	Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (?x-ntap-sg-usage) Hinzugefügt.
OPTIONEN /	Client-Applikationen können Probleme haben OPTIONS / 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.

### Verwandte Informationen

["Storage-Nutzungsanforderung ABRUFEN"](#)

## Operationen auf Buckets

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

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

["Amazon Web Services \(AWS\) Dokumentation: Bucket-Einschränkungen und -Einschränkungen"](#)

["Endpoint-Domain-Namen für S3-Anforderung"](#)

Operationen „GET Bucket“ (Listenobjekte) und „GET Bucket-Versionen“ unterstützen die StorageGRID-

Konsistenzkontrollen.

Sie können überprüfen, ob für einzelne Buckets Updates zur letzten Zugriffszeit aktiviert oder deaktiviert wurden.

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.

<b>Betrieb</b>	<b>Implementierung</b>
Bucket LÖSCHEN	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
Bucket-Cors LÖSCHEN	Durch diesen Vorgang wird die CORS-Konfiguration für den Bucket gelöscht.
Bucket-Verschlüsselung LÖSCHEN	Bei diesem Vorgang wird die Standardverschlüsselung aus dem Bucket gelöscht. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, neue dem Bucket hinzugefügte Objekte werden jedoch nicht verschlüsselt.
Bucket-Lebenszyklus LÖSCHEN	Bei diesem Vorgang wird die Lebenszyklukonfiguration aus dem Bucket gelöscht.
Bucket-Richtlinie LÖSCHEN	Bei diesem Vorgang wird die Richtlinie gelöscht, die dem Bucket zugeordnet ist.
Bucket-Replizierung LÖSCHEN	Bei diesem Vorgang wird die an den Bucket angeschlossene Replizierungskonfiguration gelöscht.
Bucket-Tagging LÖSCHEN	Dieser Vorgang verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Bucket zu entfernen

Betrieb	Implementierung
Get Bucket (Listenobjekte), Version 1 und Version 2	<p>Dieser Vorgang 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</p> <p>REDUCED_REDUNDANCY Option für Storage-Klasse:</p> <ul style="list-style-type: none"> <li>• STANDARD, Die angibt, dass das Objekt in einem Speicherpool gespeichert wird, der aus Storage-Nodes besteht.</li> <li>• GLACIER, 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>
Bucket-acl ABRUFEN	Dieser Vorgang gibt eine positive Antwort und die ID, DisplayName und die Erlaubnis des Bucket-Besitzers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf den Bucket hat.
Bucket-Cors ABRUFEN	Dieser Vorgang gibt den zurück <code>cors</code> Konfiguration für den Bucket.
Get Bucket-Verschlüsselung	Dieser Vorgang gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
BUCKET-Lebenszyklus ABRUFEN	Dieser Vorgang gibt die Lifecycle-Konfiguration für den Bucket zurück.
Bucket-Speicherort ABRUFEN	Dieser Vorgang gibt die Region zurück, die mit dem festgelegt wurde <code>LocationConstraint</code> Element in DER PUT Bucket Anforderung. Wenn der Eimer-Bereich ist <code>us-east-1</code> , Eine leere Zeichenfolge wird für die Region zurückgegeben.
Bucket-Benachrichtigung ABRUFEN	Dieser Vorgang gibt die Benachrichtigungskonfiguration an den Bucket zurück.
Get Bucket-Objektversionen	Mit LESEZUGRIFF auf einen Bucket erfolgt dieser Vorgang mit dem <code>versions</code> unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.

Betrieb	Implementierung
Get Bucket-Richtlinie	Dieser Vorgang gibt die Richtlinie zurück, die dem Bucket zugeordnet ist.
GET Bucket-Replizierung	Dieser Vorgang gibt die am Bucket angeschlossene Replizierungskonfiguration zurück.
Get Bucket-Tagging	Dieser Vorgang verwendet das <code>tagging</code> unterressource, um alle Tags für einen Bucket zurückzugeben
Get Bucket-Versionierung	Diese Implementierung verwendet das <code>versioning</code> subressource zur Rückgabe des Versionierungsstatus eines Buckets. Der zurückgegebene Versionierungsstatus gibt an, ob der Bucket die Version „Unversioniert“ oder die Version „Enabled“ oder „Suspended“ lautet.
Konfiguration der Objektsperre ABRUFEN	Dieser Vorgang legt fest, ob die S3-Objektsperre für einen Bucket aktiviert ist. " <a href="#">Verwenden der S3-Objektsperre</a> "
EIMER	Dieser Vorgang bestimmt, ob ein Bucket vorhanden ist und Sie über die Berechtigung zum Zugriff auf ihn verfügen.



Betrieb	Implementierung
Put Bucket	<p>Durch diesen Vorgang wird ein neuer Bucket erstellt. 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 erstellt <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 Namen der zu verwendenden Region nicht kennen. <b>Hinweis:</b> Ein Fehler tritt auf, wenn Ihre PUT Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.</li> <li>• Sie können die einschließen <code>x-amz-bucket-object-lock-enabled</code> Kopfzeile zum Erstellen eines Buckets anfordern, wobei S3-Objektsperre aktiviert ist.</li> </ul> <p>Sie müssen die S3-Objektsperre aktivieren, wenn Sie den Bucket erstellen. Sie können S3 Object Lock 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>

Betrieb	Implementierung
Bucket-Cors EINGEBEN	<p>Mit diesem Vorgang wird die CORS-Konfiguration für einen Bucket festgelegt, damit der Bucket die Cross-Origin-Requests 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>
Bucket-Verschlüsselung	<p>Dieser Vorgang 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>

Betrieb	Implementierung
PUT Bucket-Lebenszyklus	<p>Dieser Vorgang erstellt eine neue Lifecycle-Konfiguration für den Bucket oder ersetzt eine vorhandene Lifecycle-Konfiguration. 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)</li> <li>• NoncurrentVersionExpiration (NoncurrentDays)</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>• ExpiredObjectDeleteMarker</li> <li>• Übergang</li> </ul> <p>Informationen dazu, wie die Aktion zum Ablauf in einem Bucket-Lebenszyklus mit den Anweisungen zur ILM-Platzierung interagiert, finden Sie unter „wie ILM während der gesamten Lebensdauer eines Objekts funktioniert“ in den Anweisungen für das Management von Objekten mit Information Lifecycle Management.</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
PUT Bucket-Benachrichtigung	<p>Mit diesem Vorgang werden Benachrichtigungen für den Bucket mithilfe der im Anfraentext enthaltenen XML-Benachrichtigungskonfiguration konfiguriert. Sie sollten folgende Implementierungsdetails kennen:</p> <ul style="list-style-type: none"> <li>• StorageGRID unterstützt SNS-Themen (Simple Notification Service) als Ziele. Simple Queue Service (SQS)- 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>• Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der folgenden Liste gezeigt:</li> <li>• <b>EventSource</b> <pre>sgws:s3</pre> </li> <li>• <b>AwsRegion</b> <p>Nicht enthalten</p> </li> <li>• <b>* X-amz-id-2*</b> <p>Nicht enthalten</p> </li> <li>• <b>arn</b> <pre>urn:sgws:s3:::bucket_name</pre> </li> </ul>

<b>Betrieb</b>	<b>Implementierung</b>
Bucket-Richtlinie	Dieser Vorgang legt die Richtlinie fest, die an den Bucket gebunden ist.

Betrieb	Implementierung
PUT Bucket-Replizierung	<p>Dieser Vorgang konfiguriert die StorageGRID CloudMirror-Replikation für den Bucket mithilfe der im Anforderungsgremium bereitgestellten Replikationskonfigurations-XML. 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 unterstützten <code>Filter</code> Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.</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.</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 kein <code>Role</code> in der Konfigurations-XML angeben. 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 die <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 Bucket vor der Replizierung löschen, wird das Objekt/Bucket nicht repliziert, und Sie werden nicht benachrichtigt.</li> </ul> </li> </ul>

Betrieb	Implementierung
PUT Bucket-Tagging	<p>Dieser Vorgang 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>
PUT Bucket-Versionierung	<p>Diese Implementierung 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>

### Verwandte Informationen

["Amazon Web Services \(AWS\) Dokumentation: Regionsübergreifende Replizierung"](#)

["Konsistenzkontrollen"](#)

["Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"](#)

["Bucket- und Gruppenzugriffsrichtlinien"](#)

["Verwenden der S3-Objektsperre"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

["Objektmanagement mit ILM"](#)

["Verwenden Sie ein Mandantenkonto"](#)

## Erstellen einer S3-Lebenszykluskonfiguration

Sie können eine S3-Lebenszykluskonfiguration erstellen, um zu steuern, wann bestimmte Objekte aus dem StorageGRID System gelöscht werden.

Das einfache Beispiel in diesem Abschnitt veranschaulicht, wie eine S3-Lebenszykluskonfiguration das Löschen bestimmter Objekte aus bestimmten S3-Buckets kontrollieren kann. Das Beispiel in diesem Abschnitt dient nur zu Illustrationszwecken. Alle Details zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie im Abschnitt zum Lifecycle Management von Objekten im *Amazon Simple Storage Service Developer Guide*. Beachten Sie, dass StorageGRID nur Aktionen nach Ablauf unterstützt. Es werden keine Aktionen zur Transition unterstützt.

["Amazon Simple Storage Service Developer Guide: Lifecycle Management von Objekten"](#)

### Was für eine Lebenszykluskonfiguration ist

Eine Lifecycle-Konfiguration ist ein Satz von Regeln, die auf die Objekte in bestimmten S3-Buckets angewendet werden. Jede Regel gibt an, welche Objekte betroffen sind und wann diese Objekte ablaufen (an einem bestimmten Datum oder nach einigen Tagen).

StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:

- Ablauf: Löschen eines Objekts, wenn ein bestimmtes Datum erreicht wird oder wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend mit dem Zeitpunkt der Aufnahme des Objekts.
- NoncurrentVersionExpiration: Löschen Sie ein Objekt, wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend ab dem Zeitpunkt, an dem das Objekt nicht mehr aktuell wurde.
- Filter (Präfix, Tag)
- Status
- ID

Wenn Sie eine Lifecycle-Konfiguration auf einen Bucket anwenden, überschreiben die Lifecycle-Einstellungen für den Bucket immer die StorageGRID-ILM-Einstellungen. StorageGRID verwendet die Verfallseinstellungen für den Bucket und nicht ILM, um zu bestimmen, ob bestimmte Objekte gelöscht oder aufbewahrt werden sollen.

Aus diesem Grund kann ein Objekt aus dem Grid entfernt werden, obwohl die Speicheranweisungen in einer ILM-Regel noch auf das Objekt gelten. Alternativ kann ein Objekt auch dann im Grid aufbewahrt werden, wenn eine ILM-Platzierungsanleitung für das Objekt abgelaufen ist. Weitere Informationen finden Sie unter „Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts“ in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.



Die Bucket-Lifecycle-Konfiguration kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lifecycle-Konfiguration wird jedoch für ältere Buckets, die Compliance verwenden, nicht unterstützt.

StorageGRID unterstützt den Einsatz der folgenden Bucket-Operationen zum Management der Lebenszykluskonfigurationen:

- Bucket-Lebenszyklus LÖSCHEN
- BUCKET-Lebenszyklus ABRUFEN



- PUT Bucket-Lebenszyklus

## Erstellen der Lebenszykluskonfiguration

Als erster Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei mit einem oder mehreren Regeln. Diese JSON-Datei enthält beispielsweise drei Regeln:

1. Regel 1 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category1/` Und das hat ein `key2` Der Wert von `tag2`. Der `Expiration` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, um Mitternacht am 22. August 2020 ablaufen.
2. Regel 2 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category2/`. Der `Expiration` Parameter gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach der Aufnahme ablaufen.



Regeln, die eine Anzahl von Tagen angeben, sind relativ zu dem Zeitpunkt, an dem das Objekt aufgenommen wurde. Wenn das aktuelle Datum das Aufnahmedatum plus die Anzahl der Tage überschreitet, werden einige Objekte möglicherweise aus dem Bucket entfernt, sobald die Lebenszykluskonfiguration angewendet wird.

3. Regel 3 gilt nur für Objekte, die dem Präfix entsprechen `category3/`. Der `Expiration` Parameter gibt an, dass nicht aktuelle Versionen übereinstimmender Objekte 50 Tage nach deren Nichtstrom ablaufen.

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

## Anwenden einer Lebenszykluskonfiguration auf einen Bucket

Nachdem Sie die Lifecycle-Konfigurationsdatei erstellt haben, wenden Sie sie durch Ausgabe einer PUT Bucket Lifecycle-Anforderung auf einen Bucket an.

Diese Anforderung wendet die Lebenszykluskonfiguration in der Beispieldatei auf Objekte in einem Bucket mit dem Namen an `testbucket:Eimer`

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

Um zu überprüfen, ob eine Lifecycle-Konfiguration erfolgreich auf den Bucket angewendet wurde, geben Sie eine ANFORDERUNG FÜR DEN GET Bucket-Lebenszyklus aus. Beispiel:

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

Eine erfolgreiche Antwort zeigt die Konfiguration des Lebenszyklus, die Sie gerade angewendet haben.

## Überprüfung, ob der Bucket-Lebenszyklus für ein Objekt gilt

Sie können feststellen, ob eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt angewendet wird, wenn Sie eine PUT-Objekt-, HEAD-Objekt- oder GET-Objektanforderung ausgeben. Wenn eine Regel zutrifft, enthält die Antwort ein `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel übereinstimmt.



Da der Bucket-Lebenszyklus ILM überschreibt, wird der `expiry-date` Hier wird das tatsächliche Datum angezeigt, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter „wie die Aufbewahrung von Objekten bestimmt wird“ in den Anweisungen zur Durchführung der StorageGRID-Administration.

Zum Beispiel, diese PUT Objekt Anfrage wurde am 22. Juni 2020 und platziert ein Objekt in der `testbucket` Eimer.

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

Die Erfolgsreaktion zeigt an, dass das Objekt in 100 Tagen (01. Oktober 2020) abläuft und dass es mit Regel 2 der Lebenszykluskonfiguration übereinstimmt.

```
{
  *Expiration": "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\", rule-
id=\\"rule2\\",
  ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""}
}
```

Diese HEAD Object-Anfrage wurde beispielsweise verwendet, um Metadaten für dasselbe Objekt im Testbucket zu erhalten.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

Die Erfolgsreaktion umfasst die Metadaten des Objekts und gibt an, dass das Objekt in 100 Tagen abläuft und dass es mit Regel 2 übereinstimmt.

```
{
  "AcceptRanges": "bytes",
  *Expiration": "expiry-date=\\"Thu, 01 Oct 2020 09:07:48 GMT\\", rule-
id=\\"rule2\\",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""}
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```

## Verwandte Informationen

["Operationen auf Buckets"](#)

["Objektmanagement mit ILM"](#)

# Benutzerdefinierte Vorgänge für Buckets

Das StorageGRID System unterstützt benutzerdefinierte Bucket-Vorgänge, die der S3-REST-API hinzugefügt wurden und sich speziell auf das System beziehen.

In der folgenden Tabelle sind die von StorageGRID unterstützten benutzerdefinierten Bucket-Vorgänge aufgeführt.

Betrieb	Beschreibung	Finden Sie weitere Informationen
Get Bucket-Konsistenz	Gibt die auf einen bestimmten Bucket angewendete Konsistenzstufe zurück.	<a href="#">"Get Bucket-Konsistenzanforderung"</a>

Betrieb	Beschreibung	Finden Sie weitere Informationen
PUT Bucket-Konsistenz	Legt die Konsistenzstufe für einen bestimmten Bucket fest.	<a href="#">"PUT Bucket-Konsistenzanforderung"</a>
ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Gibt an, ob Updates der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert wurden.	<a href="#">"Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"</a>
PUT Bucket-Zeit für den letzten Zugriff	Hiermit können Sie Updates der letzten Zugriffszeit für einen bestimmten Bucket aktivieren oder deaktivieren.	<a href="#">"PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"</a>
Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Löscht die XML-Konfiguration für die Metadatenbenachrichtigung, die mit einem bestimmten Bucket verknüpft ist.	<a href="#">"Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN"</a>
Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Gibt die XML-XML-Benachrichtigungskonfiguration für Metadaten zurück, die einem bestimmten Bucket zugeordnet ist.	<a href="#">"Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN"</a>
PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket	<a href="#">"PUT Anforderung der Bucket-Metadaten-Benachrichtigung"</a>
Bucket-Änderungen für Compliance	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mit aktivierter Compliance mehr erstellen.	<a href="#">"Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"</a>
Bucket-Compliance	Veraltet, aber unterstützt: Gibt die Compliance-Einstellungen zurück, die derzeit für einen vorhandenen Legacy-konformen Bucket wirksam sind.	<a href="#">"Veraltet: GET Bucket-Compliance-Anforderung"</a>
BUCKET-Compliance	Veraltet, aber unterstützt: Ermöglicht es Ihnen, die Compliance-Einstellungen für einen vorhandenen, älteren konformen Bucket zu ändern.	<a href="#">"Veraltet: PUT Bucket-Compliance-Anforderung"</a>

#### Verwandte Informationen

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

# Operationen für Objekte

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

- "Verwenden der S3-Objektsperre"
- "Mit Server-seitiger Verschlüsselung"
- "GET Objekt"
- "HEAD Objekt"
- "WIEDERHERSTELLUNG VON POSTOBJEKTEN"
- "PUT Objekt"
- "PUT Objekt - Kopieren"

Die folgenden Bedingungen gelten für alle Objektvorgänge:

- StorageGRID Consistency Controls werden von allen Operationen für Objekte unterstützt, mit Ausnahme der folgenden:
  - GET Objekt-ACL
  - OPTIONS /
  - LEGALE Aufbewahrung des Objekts EINGEBEN
  - AUFBEWAHRUNG von Objekten
- Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst. Der Zeitpunkt für die „latest-WINS“-Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, wenn 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.
- Auf Datenobjekte, die über Swift in das StorageGRID-System aufgenommen werden, kann nicht über S3 zugegriffen werden.

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

Betrieb	Implementierung
Objekt LÖSCHEN	<p>Multi-Faktor Authentication (MFA) und Response Header <code>x-amz-mfa</code> Werden nicht unterstützt.</p> <p>Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Falls nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Standort vorübergehend nicht verfügbar ist), warteschlangen StorageGRID die Kopien zum Entfernen und zeigen 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> unterressource. Durch die Verwendung dieser Unterressource 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> unterressource auf einem Bucket mit Versionsfunktion führt zur Generierung einer Löschemarkierung. 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> unterressource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschemarker und der Generierung eines neuen 'null' Löschemarker. 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>
LÖSCHEN Sie 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>

Betrieb	Implementierung
Objekt-Tagging LÖSCHEN	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags aus einem Objekt zu entfernen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.</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 die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
GET Objekt	"GET Objekt"
GET Objekt-ACL	<p>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.</p>
HOLD-Aufbewahrung für Objekte	"Verwenden der S3-Objektsperre"
Aufbewahrung von Objekten	"Verwenden der S3-Objektsperre"
GET Objekt-Tagging	<p>Verwendet das <code>tagging</code> unterressource, um alle Tags für ein Objekt zurückzugeben. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert</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 die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>
HEAD Objekt	"HEAD Objekt"
WIEDERHERSTELLUNG VON POSTOBJEKTEN	"WIEDERHERSTELLUNG VON POSTOBJEKTEN"



<b>Betrieb</b>	<b>Implementierung</b>
PUT Objekt	"PUT Objekt"
PUT Objekt - Kopieren	"PUT Objekt - Kopieren"
LEGALE Aufbewahrung des Objekts EINGEBEN	"Verwenden der S3-Objektsperre"
AUFBEWAHRUNG von Objekten	"Verwenden der S3-Objektsperre"

Betrieb	Implementierung
<p>PUT Objekt-Tagging</p>	<p>Verwendet das <code>tagging</code> unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert</p> <p><b>Tag-Updates und Aufnahmeverhalten</b></p> <p>Wenn Sie PUT Objekt-Tagging zum Aktualisieren der Tags eines Objekts verwenden, 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 bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.</p> <ul style="list-style-type: none"> <li>• Konflikte lösen*</li> </ul> <p>Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst. Der Zeitpunkt für die „latest-WINS“-Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, wenn 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 die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „MethodNotAllowed“ zurückgegeben <code>x-amz-delete-marker</code> Antwortkopfzeile auf gesetzt <code>true</code>.</p>

## Verwandte Informationen

["Konsistenzkontrollen"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

## Verwenden der S3-Objektsperre

Wenn die globale S3-Objektsperre für Ihr StorageGRID System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen und dann für jede zu diesem Bucket addieren Objektversion noch bis dato und Legal-Hold-Einstellungen festlegen.

Mit S3 Object Lock können Sie Einstellungen auf Objektebene angeben, um das Löschen oder Überschreiben von Objekten für einen bestimmten Zeitraum oder für einen bestimmten Zeitraum zu verhindern.

Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

### Aktivieren der S3-Objektsperre für einen Bucket

Wenn die globale S3-Objektsperreinstellung für Ihr StorageGRID-System aktiviert ist, können Sie bei der Erstellung jedes Buckets optional die S3-Objektsperre aktivieren. Sie können eine der folgenden Methoden verwenden:

- Erstellen Sie den Bucket mit Tenant Manager.

["Verwenden Sie ein Mandantenkonto"](#)

- Erstellen Sie den Bucket mithilfe einer PUT-Bucket-Anforderung zusammen mit dem `x-amz-bucket-object-lock_enabled` Kopfzeile der Anfrage.

["Operationen auf Buckets"](#)

Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem der Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.

Ein Bucket mit aktivierter S3-Objektsperre kann eine Kombination von Objekten mit und ohne S3-ObjektLock-Einstellungen enthalten. StorageGRID unterstützt nicht die Standard-Aufbewahrung der Objekte in S3 Objektsperren-Buckets, daher wird der Vorgang PUT Object Lock Configuration nicht unterstützt.

### Ermitteln, ob die S3-Objektsperre für einen Bucket aktiviert ist

Um festzustellen, ob die S3-Objektsperre aktiviert ist, verwenden Sie die Konfigurationsanforderung FÜR DIE OBJEKTSPERRE ABRUFEN.

["Operationen auf Buckets"](#)

### Erstellen eines Objekts mit S3 Object Lock Einstellungen

Zum Festlegen von S3-Objektsperreinstellungen beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre geben Sie ein PUT-Objekt aus, PUT Object - Copy oder initiieren Sie die Anforderung zum Hochladen mehrerer Teile. Verwenden Sie die folgenden Anfrageheader.



Sie müssen die S3-Objektsperre aktivieren, wenn Sie einen Bucket erstellen. Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde.

- `x-amz-object-lock-mode`, Die COMPLIANCE sein muss (Groß-/Kleinschreibung muss beachtet werden).



Wenn Sie angeben `x-amz-object-lock-mode`, Sie müssen auch angeben `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen `2020-08-10T21:46:00Z`. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
  - Das „Aufbewahrung bis“-Datum muss in der Zukunft liegen.
- `x-amz-object-lock-legal-hold`

Wenn die gesetzliche Aufbewahrungspflichten LIEGEN (Groß-/Kleinschreibung muss beachtet werden), wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn die gesetzliche Aufbewahrungspflichten AUS DEM WEG gehen, wird keine gesetzliche Aufbewahrungspflichten platziert. Jeder andere Wert führt zu einem 400-Fehler (InvalidArgument).

Wenn Sie eine dieser Anfrageheadern verwenden, beachten Sie die folgenden Einschränkungen:

- Der `Content-MD5` Der Anforderungskopf ist erforderlich `x-amz-object-lock-*` In DER PUT-Objektanforderung ist eine Anforderungsüberschrift vorhanden. `Content-MD5` Ist für PUT Object – Copy oder Initiierung von mehrteiligen Uploads nicht erforderlich.
- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Der Anforderungskopf ist vorhanden, es wird ein 400-Fehler (InvalidRequest) zurückgegeben.
- Die PUT-Objektanforderung unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` Passend zum Verhalten von AWS. Wird ein Objekt jedoch mit aktivierter S3-Objektsperre in einen Bucket aufgenommen, führt StorageGRID immer eine Dual-Commit-Aufnahme durch.
- Eine nachfolgende ANTWORT AUF GET- oder HEAD Object-Version enthält die Kopfzeilen `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`, Wenn konfiguriert und wenn der Anforderungssender die richtige hat `s3:Get*` Berechtigungen.
- Eine Anfrage zur späteren LÖSCHUNG von Objekten oder ZUM LÖSCHEN von Objektversionen schlägt fehl, wenn sie sich vor dem Datum der Aufbewahrung bis zum Datum befindet oder wenn eine gesetzliche Aufbewahrungspflichten vorliegen.

### Einstellungen für die S3-Objektsperre werden aktualisiert

Wenn Sie die Einstellungen für die gesetzliche Aufbewahrungs- oder Aufbewahrungseinstellung einer vorhandenen Objektversion aktualisieren müssen, können Sie die folgenden Vorgänge der Unterressource des Objekts ausführen:

- PUT Object legal-hold

Wenn der neue Legal-Hold-Wert AKTIVIERT ist, wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn DER Rechtsvorenthalten-Wert DEAKTIVIERT ist, wird die gesetzliche Aufbewahrungspflichten aufgehoben.

- PUT Object retention
  - Der Moduswert muss COMPLIANCE sein (Groß-/Kleinschreibung muss beachtet werden).
  - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen 2020-08-10T21:46:00Z. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
  - Wenn eine Objektversion über ein vorhandenes Aufbewahrungsdatum verfügt, können Sie sie nur erhöhen. Der neue Wert muss in der Zukunft liegen.

## Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Verwenden Sie ein Mandantenkonto"](#)

["PUT Objekt"](#)

["PUT Objekt - Kopieren"](#)

["Initiieren Von Mehrteiligen Uploads"](#)

["Objektversionierung"](#)

["Amazon Simple Storage Service Benutzerhandbuch: S3 Object Lock verwenden"](#)

## Mit serverseitiger 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 von 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:

- PUT Objekt
- PUT Objekt - Kopieren
- Initiieren Von Mehrteiligen Uploads

## SSE-C verwenden

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:

- GET Objekt
- HEAD Objekt
- PUT Objekt
- PUT Objekt - Kopieren
- Initiieren Von Mehrteiligen Uploads
- Hochladen Von Teilen
- Hochladen Von Teilen - Kopieren

## 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 CloudMirror-Replikation für den Bucket konfiguriert ist, können Sie SSE-C-Objekte nicht aufnehmen. Der Aufnahmevorgang schlägt fehl.

## Verwandte Informationen

["GET Objekt"](#)

["HEAD Objekt"](#)

["PUT Objekt"](#)

["PUT Objekt - Kopieren"](#)

["Initiieren Von Mehrteiligen Uploads"](#)

["Hochladen Von Teilen"](#)

["Hochladen Von Teilen - Kopieren"](#)

["Amazon S3 Entwicklerleitfaden: Schutz von Daten durch serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln \(SSE-C\)"](#)

## GET Objekt

Sie können die S3-GET-Objektanfrage verwenden, um ein Objekt aus einem S3-Bucket abzurufen.

### Teilenummer-Anforderungsparameter wird nicht unterstützt

Der `partNumber` Der Anforderungsparameter wird für GET-Objektanforderungen nicht unterstützt. Sie können keine Anforderung ZUM ABRUFEN eines bestimmten Teils eines mehrteiligen Objekts ausführen. Ein nicht implementierter Fehler 501 wird mit folgender Meldung zurückgegeben:

GET Object by partNumber is not implemented

## 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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

## UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. ABFRAGEN für ein Objekt mit entgangenen UTF-8 Zeichen in benutzerdefinierten Metadaten WERDEN nicht zurückgegeben `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 die aktuelle Version des Objekts eine Löschmarkierung ist, wird mit dem ein Status „not found“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

## Verhalten DES GET Object für Cloud-Storage-Pool-Objekte

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), hängt das Verhalten einer GET-Objektanforderung vom Status des Objekts ab. Weitere Informationen finden Sie unter „HEAD Object“.



Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, werden GET-Objektanfragen versuchen, Daten aus dem Grid abzurufen, bevor sie aus dem Cloud-Storage-Pool abgerufen werden.



Status des Objekts	Verhalten VON GET Object
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 eine Wiederherstellungsanforderung FÜR DAS OBJEKT NACH DEM Wiederherstellen, um das Objekt in einen aufrufbaren Zustand wiederherzustellen.
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	403 Forbidden, InvalidObjectState  Warten Sie, bis die Anforderung zur Wiederherstellung DES POSTOBJEKTS 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 manchen Fällen wird eine GET Object-Anforderung möglicherweise falsch zurückgegeben 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 GET Object-Anforderung gibt möglicherweise einige Daten zurück, stoppt jedoch mitten durch die Übertragung.
- Eine nachfolgende GET Object-Anforderung kann zurückgegeben werden 403 Forbidden.

### Verwandte Informationen

["Mit serverseitiger Verschlüsselung"](#)

["Objektmanagement mit ILM"](#)

["WIEDERHERSTELLUNG VON POSTOBJEKTEN"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

## HEAD Objekt

Mithilfe der S3 HEAD Object-Anfrage können Metadaten von einem Objekt abgerufen werden, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem Cloud Storage Pool gespeichert ist, können Sie MITHILFE VON HEAD Object den Übergangstatus des Objekts bestimmen.

### 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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

### UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. HEAD-Anfragen für ein Objekt mit entgangenen 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`

### Antwortkopfzeilen für Cloud-Storage-Pool-Objekte

Wenn das Objekt in einem Cloud-Storage-Pool gespeichert ist (siehe Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management), werden die folgenden Answerheader zurückgegeben:

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

Die Answerheader 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	Reaktion auf HEAD Objekt
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: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Bis das Objekt in einen nicht aufrufbaren Zustand überführt wird, wird der Wert für <code>expiry-date</code> 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: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Der Wert für <code>expiry-date</code> Wird in der Zukunft auf eine ferne Zeit gesetzt.</p> <p><b>Hinweis:</b> Wenn die Kopie im Raster nicht verfügbar ist (z. B. ein Speicherknoten ist nicht verfügbar), müssen Sie eine ANFRAGE ZUR WIEDERHERSTELLUNG DES POSTOBJEKTS stellen, um die Kopie aus dem Cloud-Speicherpool wiederherzustellen, 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: ongoing-request="true"</p>

Status des Objekts	Reaktion auf HEAD Objekt
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>Der expiry-date Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.</p>

### 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 wird möglicherweise eine HEAD Object-Anfrage falsch zurückgegeben `x-amz-restore: ongoing-request="false"` Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

### Versionierung

Wenn `VersionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird mit dem ein Status „not found“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

### Verwandte Informationen

["Mit serverseitiger Verschlüsselung"](#)

["Objektmanagement mit ILM"](#)

["WIEDERHERSTELLUNG VON POSTOBJEKTEN"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

## WIEDERHERSTELLUNG VON POSTOBJEKTEN

Sie können die Wiederherstellungsanforderung für S3-OBJEKTE NACH DEM Posten verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Storage-Pool gespeichert ist.

### Unterstützter Anforderungstyp

StorageGRID unterstützt nur ANFRAGEN zur WIEDERHERSTELLUNG EINES Objekts NACH DEM WIEDERHERSTELLEN. 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 nicht angeben `versionId`, Die neueste Version des Objekts wird wiederhergestellt

## Verhalten DER WIEDERHERSTELLUNG NACH Objekten in Cloud-Storage-Pool-Objekten

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), weist eine Anfrage zur WIEDERHERSTELLUNG NACH dem Objekt auf Basis des Status des Objekts das folgende Verhalten auf. Weitere Informationen finden Sie unter „HEAD Object“.



Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wird und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, muss das Objekt nicht durch eine Wiederherstellungsanforderung FÜR DAS POSTOBJEKT wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
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 wiederrufbaren Zustand überführt wurde, können Sie dessen nicht ändern <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 ( <code>Expedited</code> , <code>Standard</code> , Oder <code>Bulk</code> ). Wenn Sie nicht angeben <code>Tier</code> , Das <code>Standard</code> Tier wird verwendet.  <b>Achtung:</b> Wenn ein Objekt auf das S3 Glacier Deep Archive migriert wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, kann es nicht über den wiederhergestellt werden <code>Expedited</code> Ebene: Der folgende Fehler wird zurückgegeben 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	409 Conflict, RestoreAlreadyInProgress
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK  <b>Hinweis:</b> Wenn ein Objekt in einen aufrufbaren Zustand wiederhergestellt wurde, können Sie dessen <code>expiry-date</code> ändern indem Sie die Anforderung zur Wiederherstellung DES POSTOBJEKTS mit einem neuen Wert für <code>Days</code> ausgeben. Das Wiederherstellungsdatum wird zum Zeitpunkt der Anfrage aktualisiert.

### Verwandte Informationen

["Objektmanagement mit ILM"](#)

["HEAD Objekt"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

## PUT Objekt

Sie können die S3 PUT-Objektanforderung verwenden, um einem Bucket ein Objekt hinzuzufügen.

### Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

### Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

### 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:

- PUT-, PUT-Objekt-Copy-, GET- und HEAD-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.

### 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-Encoding`StorageGRID 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 **benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie sie 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 ausgewogenen oder strengen Optionen für das Aufnahmeverhalten 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`

### "Verwenden der S3-Objektsperre"

- 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`

### "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"

#### Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen 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 zu einem aufgenommenen Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `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). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.
  - **Ausgewogen:** Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

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).
  - **Ausgewogen:** Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten 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 Aufnahmevorgang 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.

**Achtung:** Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. 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. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

**Hinweis:** Wenn Sie ein Objekt in einen Eimer mit aktivierter S3-Objektsperre aufnehmen, wird der 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.

**Achtung:** die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

**Hinweis:** Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket-Ebene 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.

## Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Operationen auf Buckets"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

["Mit serverseitiger Verschlüsselung"](#)

["Wie Client-Verbindungen konfiguriert werden können"](#)

## PUT Objekt - Kopieren

Sie können das S3 PUT Object – Copy-Request verwenden, um eine Kopie eines Objekts zu erstellen, das bereits in S3 gespeichert ist. Ein PUT Object - Copy-Vorgang ist der gleiche wie ein GET und dann ein PUT.

## Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst. Der Zeitpunkt für die Auswertung „latest-WINS“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

## Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

## 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 Objektmetadaten 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

### "Verwenden der S3-Objektsperre"

- 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

### "Anforderungsheader für serverseitige Verschlüsselung"

#### Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen 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` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- STANDARD

(Standard) gibt einen Dual-Commit-Aufnahmeverfahren 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-Aufnahmeverfahren 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 angezeigte `REDUCED_REDUNDANCY` Option 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 `PUT Object - Copy`

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 `PUT Object - Copy` 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 bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.

## Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie die serverseitige Verschlüsselung verwenden, hängen die von Ihnen zur Verfügung gestellten Anfrageheadern 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 ANFORDERUNG `PUT Object - Copy` einschließen, damit das Objekt entschlüsselt und kopiert werden kann:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` Angeben `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key` Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- 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.

**Achtung:** die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID (SSE) verwaltet wird, fügen Sie diesen Header in das PUT Object - Copy Request ein:

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

**Hinweis:** Das `server-side-encryption` Der 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 Wert „null“ zurück.

## Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Mit serverseitiger Verschlüsselung"](#)

["S3-Vorgänge werden in den Audit-Protokollen protokolliert"](#)

["PUT Objekt"](#)

# Vorgänge für mehrteilige Uploads

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

- ["Mehrtelige Uploads auflisten"](#)
- ["Initiieren Von Mehrteiligen Uploads"](#)
- ["Hochladen Von Teilen"](#)
- ["Hochladen Von Teilen - Kopieren"](#)
- ["Abschließen Von Mehrteiligen Uploads"](#)

Die folgenden Bedingungen und Hinweise gelten für alle mehrteiligen Uploadvorgänge:

- Sie sollten nicht mehr als 1,000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse der „List Multipart Uploads“-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 einzigartiges Objekt betrachtet wird, verringert der StorageGRID-Metadaten-Overhead durch große 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 bei Aufnahme und für das Objekt als Ganzes, wenn der Multipart-Upload abgeschlossen ist, bewertet, wenn die ILM-Regel das strenge oder ausgeglichene Aufnahmeverhalten verwendet. Sie sollten sich bewusst sein, wie dies die Objekt- und Teileplatzierung beeinflusst:
  - Wenn sich ILM-Änderungen während des Hochladens mehrerer S3-Teile ändern, erfüllt der mehrteilige Upload einige Teile des Objekts möglicherweise nicht die aktuellen ILM-Anforderungen. Nicht korrekt platzierte Teile werden zur ILM-Neubewertung in die Warteschlange verschoben und werden 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 Standorten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt als Ganzes bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- Alle mehrteiligen Uploadvorgänge unterstützen die StorageGRID-Konsistenzkontrollen.
- Falls erforderlich, können Sie die Verschlüsselung auf Serverseite mit mehrteiligen Uploads verwenden. Um SSE (serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln) zu verwenden, müssen Sie das angeben `x-amz-server-side-encryption` Kopfzeile anfordern in der Anfrage zum Senden von mehrteiligen Uploads. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der Anfrage zum Hochladen von mehreren Teilen und bei jeder nachfolgenden Anfrage zum Hochladen von Teilen dieselben Schlüsselkopfzeilen an.

Betrieb	Implementierung
Mehrteilige Uploads Auflisten	Siehe " <a href="#">Mehrteilige Uploads Auflisten</a> "
Initiieren Von Mehrteiligen Uploads	Siehe " <a href="#">Initiieren Von Mehrteiligen Uploads</a> "
Hochladen Von Teilen	Siehe " <a href="#">Hochladen Von Teilen</a> "
Hochladen Von Teilen - Kopieren	Siehe " <a href="#">Hochladen Von Teilen - Kopieren</a> "
Abschließen Von Mehrteiligen Uploads	Siehe " <a href="#">Abschließen Von Mehrteiligen Uploads</a> "
Abbrechen Von Mehrteiligen Uploads	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert

Betrieb	Implementierung
Teile Auflisten	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert

### Verwandte Informationen

["Konsistenzkontrollen"](#)

["Mit serverseitiger Verschlüsselung"](#)

## Mehrteilige Uploads Auflisten

In der Operation „Mehrteilige Uploads auflisten“ werden derzeit mehrteilige Uploads für einen Bucket aufgeführt.

Die folgenden Anforderungsparameter werden unterstützt:

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

Der `delimiter` Der Parameter der Anforderung wird nicht unterstützt.

### 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. Wenn der Vorgang zum vollständigen Hochladen mehrerer Teile ausgeführt wird, ist dies der Punkt, an dem Objekte erstellt werden (und gegebenenfalls versioniert).

## Initiieren Von Mehrteiligen Uploads

Mit dem Vorgang „Mehrteilerupload initiieren“ wird ein mehrtei. Upload für ein Objekt initiiert und eine Upload-ID zurückgegeben.

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 zu einem aufgenommenen Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `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). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.

- **Ausgewogen:** Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

Wenn StorageGRID sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigte `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).
- **Ausgewogen:** Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten 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 Aufnahmevorgang 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.

**Achtung:** Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. 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. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

**Hinweis:** Wenn Sie ein Objekt in einen Eimer mit aktivierter S3-Objektsperre aufnehmen, wird der angezeigte `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 Anfragezeilen 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 **benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie sie 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`

### "Verwenden der S3-Objektsperre"

- 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`

### "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"



Informationen zum Umgang von UTF-8-Zeichen mit StorageGRID finden Sie in der Dokumentation ZU PUT Object.

### 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 Anfrage Multipart hochladen, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird. Geben Sie diese Kopfzeile in keiner der Anforderungen zum Hochladen von Teilen an.
  - `x-amz-server-side-encryption`
- **SSE-C:** Verwenden Sie alle drei dieser Header in der Anfrage zum Initiate Multipart Upload (und in jeder nachfolgenden Anfrage zum Hochladen von Teilen), 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.

**Achtung:** die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

### 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 gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

### Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Mit serverseitiger Verschlüsselung"](#)

["PUT Objekt"](#)

### Hochladen Von Teilen

Der Vorgang „Teile hochladen“ 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 Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anfrageheader in jede Anfrage zum Hochladen von Teilen angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe AES256.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.

- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile 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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

## 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 gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

## Verwandte Informationen

["Mit serverseitiger Verschlüsselung"](#)

## Hochladen Von Teilen - Kopieren

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

Der Vorgang „Hochladen von Teilen – Kopieren“ ist mit dem Verhalten der gesamten Amazon S3-REST-API implementiert.

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 Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anforderungsheader auch in jeden Upload Part - Copy request angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe AES256.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile angegeben haben.

Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, müssen Sie die folgenden drei Header in die Anfrage „Teil hochladen – Kopieren“ aufnehmen, damit das Objekt entschlüsselt und anschließend 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 zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „serverseitige Verschlüsselung verwenden.“

## 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 gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

## Abschließen Von Mehrteiligen Uploads

Der komplette mehrteilige Upload-Vorgang führt einen mehrteiligen Upload eines Objekts durch, indem die zuvor hochgeladenen Teile zusammengebaut werden.

## Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „latest-WINS“-Basis gelöst. Der Zeitpunkt für die Auswertung „latest-WINS“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wann S3-Clients einen Vorgang starten.

## Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

## Anfragekopfzeilen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- STANDARD

(Standard) gibt einen Dual-Commit-Aufnahmeverfahren 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-Aufnahmeverfahren 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 angezeigte `REDUCED_REDUNDANCY` Option 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 diese 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 zurückgegebenen `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 „Fehler beim Veröffentlichen von Benachrichtigungen für Bucket-nameobject key“ für das letzte Objekt angezeigt, dessen Benachrichtigung fehlgeschlagen ist. (Um diese Meldung anzuzeigen, wählen Sie **Knoten** > **Speicherknoten** > **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.

## Verwandte Informationen

["Objektmanagement mit ILM"](#)

# 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
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

<b>Name</b>	<b>HTTP-Status</b>
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
MissingSecurityHeader	400 Fehlerhafte Anfrage
NoSuchBucket	404 Nicht Gefunden
NoSuchKey	404 Nicht Gefunden
NoSuchUpload	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
NoSuchBucketRichtlinien	404 Nicht Gefunden
ObjektLockKonfigurationNotgefundenFehler	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**



<b>Name</b>	<b>Beschreibung</b>	<b>HTTP-Status</b>
XBucketLifecycleNotAlled	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
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 © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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