



Operationen für Objekte

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Operationen für Objekte 1
 - Verwenden der S3-Objektsperre 6
 - Mit serverseitiger Verschlüsselung 8
 - GET Objekt 11
 - HEAD Objekt 13
 - WIEDERHERSTELLUNG VON POSTOBJEKTEN 16
 - PUT Objekt 17
 - PUT Objekt - Kopieren 22

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>Versionierung</p> <p>Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und den verwenden <code>versionId</code> unterresource. Durch die Verwendung dieser Unterresource wird die Version dauerhaft gelöscht. Wenn der <code>versionId</code> Entspricht einer Löschen-Markierung, dem Antwortkopf <code>x-amz-delete-marker</code> Wird auf festgelegt <code>true</code>.</p> <ul style="list-style-type: none"> • Wird ein Objekt ohne gelöscht <code>versionId</code> unterresource 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>. • Wird ein Objekt ohne gelöscht <code>versionId</code> unterresource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschemarker und der Generierung eines neuen 'null' Löschemarker. Der <code>x-amz-delete-marker</code> Der Antwortkopf wird auf festgelegt <code>true</code>. <p>Hinweis: 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>Versionierung</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>Versionierung</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"

Betrieb	Implementierung
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>Tag-Updates und Aufnahmeverhalten</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"> • Konflikte lösen* <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>Versionierung</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-Objektsperreneinstellung 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 Rechtsvorethalen-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
<code>x-amz-server-side-encryption-customer-algorithm</code>	Geben Sie den Verschlüsselungsalgorithmus an. Der Kopfzeilenwert muss sein AES256.
<code>x-amz-server-side-encryption-customer-key</code>	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.
<code>x-amz-server-side-encryption-customer-key-MD5</code>	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 Aufnahmeprozess 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 Antwortheader zurückgegeben:

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

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

Status des Objekts	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 Antwortheader zurückgegeben.)
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> 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.
Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Der Wert für <code>expiry-date</code> Wird in der Zukunft auf eine ferne Zeit gesetzt. Hinweis: 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.

Status des Objekts	Reaktion auf HEAD Objekt
Das Objekt wurde in einen nicht abrufbaren Zustand versetzt, und es ist keine Kopie im Grid vorhanden	200 OK x-amz-storage-class: GLACIER
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" Der expiry-date Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.

Mehrteilige oder segmentierte Objekte in 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. Hinweis: Bevor ein Objekt in einen nicht widerrufbaren Zustand überführt wurde, können Sie dessen nicht ändern <code>expiry-date</code> .

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

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-EncodingStorageGRID überprüft die folgenden Elemente nicht:

- StorageGRID überprüft das nicht `chunk-signature` Auf die Chunk-Daten:
- StorageGRID überprüft nicht den Wert, den Sie für angeben `x-amz-decoded-content-length` Gegen das Objekt.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

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

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

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

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

Wenn Sie die Option **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-Objektsperrungs-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

einzigste 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.

Angeben 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.

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

Verwenden von x-amz-copy-source in 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"

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.