Unterstützung für Amazon S3 REST API

StorageGRID software

NetApp
October 21, 2025

Inhalt

Unterstützung für Amazon S3 REST API

Details zur S3 REST API-Implementierung

Das StorageGRID -System implementiert die Simple Storage Service API (API-Version 2006-03-01) mit Unterstützung für die meisten Vorgänge und mit einigen Einschränkungen. Sie müssen die Implementierungsdetails verstehen, wenn Sie S3 REST API-Clientanwendungen integrieren.

Das StorageGRID -System unterstützt sowohl Anfragen im virtuellen gehosteten Stil als auch Anfragen im Pfadstil.

Datumsverarbeitung

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

Das StorageGRID -System unterstützt nur gültige HTTP-Datumsformate für Header, die Datumswerte akzeptieren. Der Zeitanteil des Datums kann im Format Greenwich Mean Time (GMT) oder im Format Universal Coordinated Time (UTC) ohne Zeitzonenverschiebung angegeben werden (+0000 muss angegeben werden). Wenn Sie die `x-amz-date` Header in Ihrer Anfrage, überschreibt es alle im Date-Anforderungsheader angegebenen Werte. Bei Verwendung von AWS Signature Version 4 ist die `x-amz-date` Der Header muss in der signierten Anfrage vorhanden sein, da der Datumsheader nicht unterstützt wird.

Allgemeine Anforderungsheader

Das StorageGRID -System unterstützt die gemeinsamen Anforderungsheader, die definiert sind durch "Amazon Simple Storage Service API-Referenz: Allgemeine Anforderungsheader" , mit einer Ausnahme.

Anforderungsheader	Durchführung
Genehmigung	Volle Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: • Wenn Sie den tatsächlichen Nutzlastprüfsummenwert in `x-amz-content-sha256` wird der Wert ohne Validierung akzeptiert, als ob der Wert `UNSIGNED-PAYLOAD` für den Header vorgesehen war. Wenn Sie eine `x-amz-content-sha256` Header-Wert, der impliziert `aws-chunked` Streaming (z. B. STREAMING-AWS4-HMAC-SHA256-PAYLOAD), werden die Chunk-Signaturen nicht anhand der Chunk-Daten überprüft.
x-amz-Sicherheitstoken	Nicht implementiert. Rückgaben `XNotImplemented` .

Allgemeine Antwortheader

Das StorageGRID -System unterstützt alle gängigen Antwortheader, die in der *Simple Storage Service API Reference* definiert sind, mit einer Ausnahme.

Antwortheader	Durchführung
x-amz-id-2	Nicht verwendet

Authentifizieren von Anfragen

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

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

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

Das StorageGRID -System unterstützt zwei Authentifizierungsmethoden: HTTP `Authorization` Header und Verwendung von Abfrageparametern.

Verwenden Sie den HTTP-Autorisierungsheader

Das HTTP `Authorization` Der Header wird von allen S3-API-Operationen verwendet, außer von anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der `Authorization` Der Header enthält alle erforderlichen Signaturinformationen zur Authentifizierung einer Anfrage.

Verwenden von Abfrageparametern

Sie können Abfrageparameter verwenden, um einer URL Authentifizierungsinformationen hinzuzufügen. Dies wird als Vorsignierung der URL bezeichnet und kann verwendet werden, um vorübergehenden Zugriff auf bestimmte Ressourcen zu gewähren. Benutzer mit der vorsignierten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zuzugreifen. Dadurch können Sie Dritten eingeschränkten Zugriff auf eine Ressource gewähren.

Vorgänge für den Dienst

Das StorageGRID -System unterstützt die folgenden Vorgänge für den Dienst.

Betrieb	Durchführung
Buckets auflisten (früher GET-Dienst genannt)	Implementiert mit dem gesamten Amazon S3 REST API-Verhalten. Änderungen vorbehalten.
GET-Speichernutzung	Das StorageGRID"GET-Speichernutzung" Die Anfrage gibt Auskunft über die Gesamtmenge des von einem Konto und jedem mit dem Konto verknüpften Bucket verwendeten Speichers. Dies ist eine Operation für den Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter(`?x-ntap-sg-usage`) hinzugefügt.

Betrieb	Durchführung
OPTIONEN /	Clientanwendungen können `OPTIONS /` Anfragen an den S3-Port eines Speicherknotens, ohne S3-Authentifizierungsdaten anzugeben, um festzustellen, ob der Speicherknoten verfügbar ist. Sie können diese Anfrage zur Überwachung verwenden oder um externen Lastenausgleichsmodulen zu ermöglichen, zu erkennen, wenn ein Speicherknoten ausgefallen ist.

Operationen an Buckets

Das StorageGRID -System unterstützt maximal 5.000 Buckets für jedes S3-Mandantenkonto.

Jedes Raster kann maximal 100.000 Buckets enthalten.

Um 5.000 Buckets zu unterstützen, muss jeder Speicherknoten im Grid über mindestens 64 GB RAM verfügen.

Die Einschränkungen für Bucket-Namen folgen den regionalen Einschränkungen des AWS-US-Standards, Sie sollten sie jedoch zusätzlich auf DNS-Namenskonventionen beschränken, um Anfragen im virtuellen S3-Hosting-Stil zu unterstützen.

Weitere Informationen finden Sie im Folgenden:

- "Amazon Simple Storage Service-Benutzerhandbuch: Bucket-Kontingente, Einschränkungen und Begrenzungen"
- "Konfigurieren von S3-Endpunktdomänennamen"

Die Operationen ListObjects (GET Bucket) und ListObjectVersions (GET Bucket-Objektversionen) unterstützen StorageGRID"Konsistenzwerte" .

Sie können überprüfen, ob Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind. Sehen "GET Bucket – Letzte Zugriffszeit" .

Die folgende Tabelle beschreibt, wie StorageGRID S3 REST API-Bucket-Operationen implementiert. Um diese Vorgänge auszuführen, müssen die erforderlichen Zugangsdaten für das Konto angegeben werden.

Betrieb	Durchführung
Bucket erstellen	Erstellt einen neuen Bucket. Indem Sie den Bucket erstellen, werden Sie zum Bucket-Eigentümer. • Bucket-Namen müssen den folgenden Regeln entsprechen: ◦ Muss in jedem StorageGRID -System eindeutig sein (nicht nur innerhalb des Mandantenkontos). ◦ Muss DNS-kompatibel sein. ◦ Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten. ◦ Kann eine Reihe von einem oder mehreren Labels sein, wobei benachbarte Labels durch einen Punkt getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. ◦ Darf nicht wie eine IP-Adresse im Textformat aussehen. ◦ In Anfragen im virtuell gehosteten Stil sollten keine Punkte verwendet werden. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. • Standardmäßig werden Buckets im `us-east-1` Region; Sie können jedoch die `LocationConstraint` Anforderungselement im Anforderungstext, um eine andere Region anzugeben. Bei Verwendung der `LocationConstraint` Element müssen Sie den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den zu verwendenden Regionsnamen nicht kennen. **Hinweis**: Es tritt ein Fehler auf, wenn Ihre CreateBucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde. • Sie können Folgendes einschließen: `x-amz-bucket-object-lock-enabled` Anforderungsheader zum Erstellen eines Buckets mit aktivierter S3-Objektsperre. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" . Sie müssen S3 Object Lock aktivieren, wenn Sie den Bucket erstellen. Sie können die S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. S3 Object Lock erfordert eine Bucket-Versionierung, die automatisch aktiviert wird, wenn Sie den Bucket erstellen.
Bucket löschen	Löscht den Bucket.
BucketCors löschen	Löscht die CORS-Konfiguration für den Bucket.
DeleteBucketEncryption	Löscht die Standardverschlüsselung aus dem Bucket. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, aber alle neuen Objekte, die dem Bucket hinzugefügt werden, werden nicht verschlüsselt.

Betrieb	Durchführung
DeleteBucketLifecycle	Löscht die Lebenszykluskonfiguration aus dem Bucket. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
DeleteBucketPolicy	Löscht die an den Bucket angehängte Richtlinie.
DeleteBucketReplication	Löscht die an den Bucket angehängte Replikationskonfiguration.
BucketTagging löschen	Verwendet die `tagging` Unterressource zum Entfernen aller Tags aus einem Bucket. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Geben Sie keine DeleteBucketTagging-Anforderung aus, wenn ein `NTAP-SG-ILM-BUCKET-TAG` Eimer-Tag. Senden Sie stattdessen eine PutBucketTagging-Anfrage mit nur dem `NTAP-SG-ILM-BUCKET-TAG` Tag und sein zugewiesener Wert, um alle anderen Tags aus dem Bucket zu entfernen. Verändern oder entfernen Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` Eimer-Tag.
GetBucketAcl	Gibt eine positive Antwort sowie die ID, den Anzeigenamen und die Berechtigung des Bucket-Eigentümers zurück und gibt damit an, dass der Eigentümer vollen Zugriff auf den Bucket hat.
GetBucketCors	Gibt den `cors` Konfiguration für den Bucket.
GetBucketEncryption	Gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
GetBucketLifecycleConfiguration (früher GET Bucket-Lebenszyklus genannt)	Gibt die Lebenszykluskonfiguration für den Bucket zurück. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
BucketLocation abrufen	Gibt die Region zurück, die mit dem `LocationConstraint` Element in der CreateBucket-Anforderung. Wenn die Region des Buckets `us-east-1` , wird für die Region eine leere Zeichenfolge zurückgegeben.
GetBucketNotificationConfiguration (früher „GET Bucket-Benachrichtigung“ genannt)	Gibt die dem Bucket zugeordnete Benachrichtigungskonfiguration zurück.
GetBucketPolicy	Gibt die dem Bucket zugeordnete Richtlinie zurück.
GetBucketReplication	Gibt die dem Bucket zugeordnete Replikationskonfiguration zurück.

Betrieb	Durchführung
GetBucketTagging	Verwendet die `tagging` Unterressource, um alle Tags für einen Bucket zurückzugeben. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Ändern oder entfernen Sie dieses Tag nicht.
GetBucketVersioning	Diese Implementierung verwendet die `versioning` Unterressource, um den Versionsstatus eines Buckets zurückzugeben. • *blank*: Die Versionierung wurde nie aktiviert (Bucket ist „Unversioned“) • Aktiviert: Versionierung ist aktiviert • Ausgesetzt: Die Versionsverwaltung war zuvor aktiviert und ist ausgesetzt
GetObjectLockConfiguration	Gibt den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer des Buckets zurück, sofern konfiguriert. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .
Kopfeimer	Stellt fest, ob ein Bucket vorhanden ist und Sie über die Berechtigung verfügen, darauf zuzugreifen. Dieser Vorgang gibt Folgendes zurück: • `x-ntap-sg-bucket-id`: Die UUID des Buckets im UUID-Format. • `x-ntap-sg-trace-id`: Die eindeutige Trace-ID der zugehörigen Anfrage.
ListObjects und ListObjectsV2 (früher GET Bucket genannt)	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 dem `REDUCED_REDUNDANCY` Speicherklassenoption: • `STANDARD`, was darauf hinweist, dass das Objekt in einem Speicherpool gespeichert ist, der aus Speicherknoten besteht. • `GLACIER`, was darauf hinweist, dass das Objekt in den vom Cloud Storage Pool angegebenen externen Bucket verschoben wurde. Wenn der Bucket eine große Anzahl gelöschter Schlüssel mit demselben Präfix enthält, kann die Antwort einige `CommonPrefixes` die keine Schlüssel enthalten.
ListObjectVersions (zuvor GET Bucket Object-Versionen genannt)	Mit Lesezugriff auf einen Bucket kann dieser Vorgang mit dem `versions` Die Unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.

Betrieb	Durchführung
PutBucketCors	Legt die CORS-Konfiguration für einen Bucket fest, sodass der Bucket Cross-Origin-Anfragen verarbeiten kann. Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens `images` zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für die `images` Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen `http://www.example.com` .
PutBucketEncryption	Legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Wenn die Verschlüsselung auf Bucket-Ebene aktiviert ist, werden alle neuen Objekte, die dem Bucket hinzugefügt werden, verschlüsselt. StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln. Wenn Sie die serverseitige Verschlüsselungskonfigurationsregel angeben, legen Sie die `SSEAlgorithm` Parameter auf `AES256` und verwenden Sie nicht die `KMSMasterKeyID` Parameter. Die Standardverschlüsselungskonfiguration des Buckets wird ignoriert, wenn die Objekt-Upload-Anforderung bereits eine Verschlüsselung angibt (d. h. wenn die Anforderung die `x-amz-server-side-encryption-*` Anforderungsheader).
PutBucketLifecycleConfiguration (früher PUT Bucket-Lebenszyklus genannt)	Erstellt eine neue Lebenszykluskonfiguration für den Bucket oder ersetzt eine vorhandene Lebenszykluskonfiguration. StorageGRID unterstützt bis zu 1.000 Lebenszyklusregeln in einer Lebenszykluskonfiguration. Jede Regel kann die folgenden XML-Elemente enthalten: • Ablauf (Tage, Datum, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filter (Präfix, Tag) • Status • AUSWEIS StorageGRID unterstützt diese Aktionen nicht: • AbbruchUnvollständigMehrteiliger Upload • Übergang Sehen "Erstellen einer S3-Lebenszykluskonfiguration" . Informationen dazu, wie die Ablaufaktion in einem Bucket-Lebenszyklus mit ILM-Platzierungsanweisungen interagiert, finden Sie unter"Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts" . **Hinweis**: Die Bucket-Lebenszykluskonfiguration kann mit Buckets verwendet werden, bei denen S3 Object Lock aktiviert ist, die Bucket-Lebenszykluskonfiguration wird jedoch für ältere konforme Buckets nicht unterstützt.

Betrieb	Durchführung

PutBucketNotificationConfiguration
 	
(früher PUT Bucket-Benachrichtigung genannt)
	Konfiguriert Benachrichtigungen für den Bucket mithilfe der im Anforderungstext enthaltenen Benachrichtigungskonfigurations-XML. Sie sollten sich der folgenden Implementierungsdetails bewusst sein:
	
	• StorageGRID unterstützt Amazon Simple Notification Service (Amazon SNS) oder Kafka-Themen als Ziele. Simple Queue Service (SQS) oder Amazon Lambda-Endpunkte werden nicht unterstützt.
	• Das Ziel für Benachrichtigungen muss als URN eines StorageGRID Endpunkts angegeben werden. Endpunkte können mit dem Tenant Manager oder der Tenant Management API erstellt werden.
	
	Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, wird ein `400 Bad Request` Fehler wird mit dem Code zurückgegeben `InvalidArgument` .
	
	• Für die folgenden Ereignistypen können Sie keine Benachrichtigung konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und für andere bestimmte Werte verwenden, wie in der folgenden Liste gezeigt:
	◦ **Ereignisquelle**
	
	`sgws:s3`
	
	◦ **awsRegion**
	
	nicht enthalten
	
	◦ **x-amz-id-2**
	
	nicht enthalten
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Legt die dem Bucket zugeordnete Richtlinie fest. Sehen "Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien" .

Betrieb	Durchführung
PutBucketReplication	Konfiguriert"StorageGRID CloudMirror-Replikation" für den Bucket unter Verwendung der im Anforderungstext bereitgestellten XML-Replikationskonfiguration. Bei der CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten: • StorageGRID unterstützt nur V1 der Replikationskonfiguration. Dies bedeutet, dass StorageGRID die Verwendung des `Filter` Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Einzelheiten finden Sie unter "Amazon Simple Storage Service-Benutzerhandbuch: Replikationskonfiguration" . • Die Bucket-Replikation kann für versionierte oder nicht versionierte Buckets konfiguriert werden. • Sie können in jeder Regel der XML-Replikationskonfiguration einen anderen Ziel-Bucket angeben. Ein Quell-Bucket kann in mehr als einen Ziel-Bucket repliziert werden. • Ziel-Buckets müssen als URN von StorageGRID -Endpunkten angegeben werden, wie im Tenant Manager oder der Tenant Management API angegeben. Sehen "Konfigurieren der CloudMirror-Replikation" . Der Endpunkt muss vorhanden sein, damit die Replikationskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, schlägt die Anfrage fehl, da `400 Bad Request` Die Fehlermeldung lautet: `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • Sie müssen kein `Role` im Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird ignoriert, wenn er übermittelt wird. • Wenn Sie die Speicherklasse aus der Konfigurations-XML weglassen, verwendet StorageGRID die `STANDARD` Speicherklasse standardmäßig. • Wenn Sie ein Objekt aus dem Quell-Bucket oder den Quell-Bucket selbst löschen, ist das regionsübergreifende Replikationsverhalten wie folgt: ◦ Wenn Sie das Objekt oder den Bucket löschen, bevor es repliziert wurde, wird das Objekt/der Bucket nicht repliziert und Sie werden nicht benachrichtigt. ◦ Wenn Sie das Objekt oder den Bucket nach der Replikation löschen, folgt StorageGRID dem standardmäßigen Löschverhalten von Amazon S3 für V1 der regionsübergreifenden Replikation.

Betrieb	Durchführung
PutBucketTagging	Verwendet die `tagging` Unterressource zum Hinzufügen oder Aktualisieren eines Satzes von Tags für einen Bucket. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen: • Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 50 Tags für jeden Bucket. • Mit einem Bucket verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein. • Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. • Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag mit einem ihm zugewiesenen Wert. Stellen Sie sicher, dass die `NTAP-SG-ILM-BUCKET-TAG` Das Bucket-Tag ist mit dem zugewiesenen Wert in allen PutBucketTagging-Anfragen enthalten. Ändern oder entfernen Sie dieses Tag nicht. **Hinweis**: Dieser Vorgang überschreibt alle aktuellen Tags, die der Bucket bereits hat. Wenn vorhandene Tags aus dem Set weggelassen werden, werden diese Tags für den Bucket entfernt.
PutBucketVersioning	Verwendet die `versioning` Unterressource zum Festlegen des Versionsstatus eines vorhandenen Buckets. Sie können den Versionsstatus mit einem der folgenden Werte festlegen: • Aktiviert: Aktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Versions-ID. • Angehalten: Deaktiviert die Versionierung für die Objekte im Bucket. Alle zum Bucket hinzugefügten Objekte erhalten die Versions-ID `null` .
PutObjectLockConfiguration	Konfiguriert oder entfernt den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer des Buckets. Wenn die Standardaufbewahrungsfrist geändert wird, bleibt das Aufbewahrungsdatum vorhandener Objektversionen gleich und wird nicht anhand der neuen Standardaufbewahrungsfrist neu berechnet. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" für detaillierte Informationen.

Operationen an Objekten

Operationen an Objekten

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

Für alle Objektoperationen gelten folgende Bedingungen:

- StorageGRID"Konsistenzwerte" werden von allen Operationen an Objekten unterstützt, mit Ausnahme der folgenden:
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.
- Alle Objekte in einem StorageGRID Bucket sind Eigentum des Bucket-Eigentümers, einschließlich der von einem anonymen Benutzer oder einem anderen Konto erstellten Objekte.
- Auf Datenobjekte, die über Swift in das StorageGRID System aufgenommen werden, kann nicht über S3 zugegriffen werden.

Die folgende Tabelle beschreibt, wie StorageGRID S3 REST API-Objektoperationen implementiert.

Betrieb	Durchführung
Objekt löschen	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. Bei der Verarbeitung einer DeleteObject-Anforderung versucht StorageGRID , alle Kopien des Objekts sofort von allen gespeicherten Standorten zu entfernen. Bei Erfolg gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien zur Entfernung in die Warteschlange und zeigt dem Client anschließend den Erfolg an. **Versionierung** Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und die `versionId` Unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn die `versionId` entspricht einem Löschmarker, der Antwortheader `x-amz-delete-marker` wird zurückgegeben auf `true` . • Wenn ein Objekt gelöscht wird, ohne dass `versionId` Unterressource auf einem Bucket mit aktivierter Versionierung, führt dies zur Generierung einer Löschmarkierung. Der `versionId` für die Löschmarkierung wird mit dem `x-amz-version-id` Antwortheader und der `x-amz-delete-marker` Der Antwortheader wird auf `true` . • Wenn ein Objekt gelöscht wird, ohne dass `versionId` Unterressource auf einem Bucket mit ausgesetzter Versionierung, führt dies zu einer dauerhaften Löschung einer bereits vorhandenen „Null“-Version oder eines „Null“-Löschmarkers und zur Generierung eines neuen „Null“-Löschmarkers. Der `x-amz-delete-marker` Der Antwortheader wird auf `true` . **Hinweis**: In bestimmten Fällen können für ein Objekt mehrere Löschmarkierungen vorhanden sein. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" um zu erfahren, wie Sie Objektversionen im GOVERNANCE-Modus löschen.

Betrieb	Durchführung
Objekte löschen (früher „DELETE Multiple Objects“ genannt)	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. In derselben Anforderungsnachricht können mehrere Objekte gelöscht werden. Sehen"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" um zu erfahren, wie Sie Objektversionen im GOVERNANCE-Modus löschen.
DeleteObjectTagging	Verwendet die `tagging` Unterressource zum Entfernen aller Tags von einem Objekt. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, löscht der Vorgang alle Tags aus der aktuellsten Version des Objekts in einem versionierten Bucket. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
GetObject	"GetObject"
GetObjectAcl	Wenn die erforderlichen Zugriffsberechtigungen für das Konto bereitgestellt werden, gibt der Vorgang eine positive Antwort sowie die ID, den Anzeigenamen und die Berechtigung des Objektbesitzers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf das Objekt hat.
GetObjectLegalHold	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
GetObjectRetention	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
GetObjectTagging	Verwendet die `tagging` Unterressource, um alle Tags für ein Objekt zurückzugeben. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, gibt der Vorgang alle Tags aus der aktuellsten Version des Objekts in einem versionierten Bucket zurück. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"

Betrieb	Durchführung
PutObject	"PutObject"
Objekt kopieren (früher PUT-Objekt – Kopieren genannt)	"Objekt kopieren"
PutObjectLegalHold	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
PutObjectRetention	"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

Betrieb	Durchführung
PutObjectTagging	Verwendet die `tagging` Unterressource zum Hinzufügen einer Reihe von Tags zu einem vorhandenen Objekt. **Objekt-Tag-Grenzwerte** Sie können neuen Objekten beim Hochladen Tags hinzufügen oder Sie können sie vorhandenen Objekten hinzufügen. Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Mit einem Objekt verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden. **Tag-Updates und Aufnahmeverhalten** Wenn Sie PutObjectTagging verwenden, um die Tags eines Objekts zu aktualisieren, nimmt StorageGRID das Objekt nicht erneut auf. Dies bedeutet, dass die in der entsprechenden ILM-Regel angegebene Option für das Aufnahmeverhalten nicht verwendet wird. Alle durch die Aktualisierung ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird. Dies bedeutet, dass keine Aktion ausgeführt wird, wenn die ILM-Regel die Option „Streng“ für das Aufnahmeverhalten verwendet und die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist. **Konflikte lösen** Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst. Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen. **Versionierung** Wenn die `versionId` Wenn in der Anforderung kein Abfrageparameter angegeben ist, fügt der Vorgang der aktuellsten Version des Objekts in einem versionierten Bucket Tags hinzu. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "MethodNotAllowed" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .
SelectObjectContent	"SelectObjectContent"

Verwenden Sie S3 Select

StorageGRID unterstützt die folgenden Amazon S3 Select-Klauseln, Datentypen und Operatoren für die"SelectObjectContent-Befehl" .

Nicht aufgeführte Artikel werden nicht unterstützt.

Informationen zur Syntax finden Sie unter"SelectObjectContent" . Weitere Informationen zu S3 Select finden Sie im "AWS-Dokumentation für S3 Select" .

Nur Mandantenkonten, bei denen S3 Select aktiviert ist, können SelectObjectContent-Abfragen ausgeben. Siehe die"Überlegungen und Anforderungen zur Verwendung von S3 Select" .

Klauseln

- SELECT-Liste
- FROM-Klausel
- WHERE-Klausel
- LIMIT-Klausel

Datentypen

- bool
- ganze Zahl
- Schnur
- schweben
- Dezimal, numerisch
- Zeitstempel

Betreiber

Logische Operatoren

- UND
- NICHT
- ODER

Vergleichsoperatoren

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ZWISCHEN
- IN

Mustervergleichsoperatoren

- WIE
- _
- %

Unitäre Operatoren

- IST NULL
- IST NICHT NULL

Mathematische Operatoren

- +
- -
- *
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

Aggregatfunktionen

- AVG()
- ZÄHLEN(*)
- MAX()
- MIN()
- SUMME()

Bedingte Funktionen

- FALL
- VERSCHMELZEN
- NULLIF

Konvertierungsfunktionen

- CAST (für unterstützten Datentyp)

Datumsfunktionen

- DATE_ADD
- DATE_DIFF

- EXTRAKT
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

Zeichenfolgenfunktionen

- CHAR_LENGTH, CHARACTER_LENGTH
- UNTERE
- TEILZEICHENKETTE
- TRIMMEN
- OBERE

Verwenden Sie serverseitige Verschlüsselung

Durch die serverseitige Verschlüsselung können Sie Ihre ruhenden Objektdaten schützen. StorageGRID verschlüsselt die Daten beim Schreiben des Objekts und entschlüsselt die Daten, wenn Sie auf das Objekt zugreifen.

Wenn Sie serverseitige Verschlüsselung verwenden möchten, können Sie je nach Verwaltung der Verschlüsselungsschlüssel zwischen zwei sich gegenseitig ausschließenden Optionen wählen:

- **SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln)**: Wenn Sie eine S3-Anfrage zum Speichern eines Objekts stellen, verschlüsselt StorageGRID das Objekt mit einem eindeutigen Schlüssel. Wenn Sie eine S3-Anforderung zum Abrufen des Objekts stellen, verwendet StorageGRID den gespeicherten Schlüssel zum Entschlüsseln des Objekts.
- **SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)**: Wenn Sie eine S3-Anfrage zum Speichern eines Objekts stellen, geben Sie Ihren eigenen Verschlüsselungsschlüssel an. Wenn Sie ein Objekt abrufen, geben Sie im Rahmen Ihrer Anfrage denselben Verschlüsselungsschlüssel an. Wenn die beiden Verschlüsselungsschlüssel übereinstimmen, wird das Objekt entschlüsselt und Ihre Objektdaten werden zurückgegeben.

  Während StorageGRID alle Objektverschlüsselungs- und -entschlüsselungsvorgänge verwaltet, müssen Sie die von Ihnen bereitgestellten Verschlüsselungsschlüssel verwalten.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

> Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Verwenden Sie SSE

Um ein Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel zu verschlüsseln, verwenden Sie den folgenden Anforderungsheader:

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

Der SSE-Anforderungsheader wird von den folgenden Objektoperationen unterstützt:

- "PutObject"
- "Objekt kopieren"
- "CreateMultipartUpload"

Verwenden Sie SSE-C

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

Anforderungsheader	Beschreibung
`x-amz-server-side-encryption-customer-algorithm`	Geben Sie den Verschlüsselungsalgorithmus an. Der Headerwert muss `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 lang und base64-codiert sein.
`x-amz-server-side-encryption-customer-key-MD5`	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der verwendet wird, um sicherzustellen, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für den MD5-Digest muss base64-codiert und 128 Bit lang sein.

Die SSE-C-Anforderungsheader werden von den folgenden Objektoperationen unterstützt:

- "GetObject"
- "HeadObject"
- "PutObject"
- "Objekt kopieren"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Überlegungen zur Verwendung der serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C)

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

- Sie müssen https verwenden.

> ⚠ StorageGRID lehnt bei Verwendung von SSE-C alle über HTTP gestellten Anfragen ab. Aus Sicherheitsgründen sollten Sie jeden versehentlich über HTTP gesendeten Schlüssel als gefährdet betrachten. Entsorgen Sie den Schlüssel und drehen Sie ihn entsprechend.

- Der ETag in der Antwort ist nicht der MD5 der Objektdaten.

- Sie müssen die Zuordnung von Verschlüsselungsschlüsseln zu Objekten verwalten. StorageGRID speichert keine Verschlüsselungsschlüssel. Sie sind für die Nachverfolgung des Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.
- Wenn für Ihren Bucket die Versionierung aktiviert ist, sollte jede Objektversion über einen eigenen Verschlüsselungsschlüssel verfügen. Sie sind für die Nachverfolgung des für jede Objektversion verwendeten Verschlüsselungsschlüssels verantwortlich.
- Da Sie die Verschlüsselungsschlüssel auf der Clientseite verwalten, müssen Sie auch alle zusätzlichen Sicherheitsvorkehrungen, wie etwa die Schlüsselrotation, auf der Clientseite verwalten.

> Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt.

- Wenn für den Bucket eine Cross-Grid-Replikation oder eine CloudMirror-Replikation konfiguriert ist, können Sie keine SSE-C-Objekte aufnehmen. Der Aufnahmevorgang schlägt fehl.

Ähnliche Informationen

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

Objekt kopieren

Mit der S3 CopyObject-Anforderung können Sie eine Kopie eines Objekts erstellen, das bereits in S3 gespeichert ist. Ein CopyObject-Vorgang ist dasselbe wie die Ausführung von GetObject gefolgt von PutObject.

Konflikte lösen

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

Objektgröße

Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie"mehrteiliger Upload" stattdessen.

Die maximal *unterstützte* Größe für einen einzelnen PutObject-Vorgang beträgt 5 TiB (5.497.558.138.880 Bytes).

> Wenn Sie ein Upgrade von StorageGRID 11.6 oder früher durchgeführt haben, wird die Warnung „S3 PUT-Objektgröße zu groß“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das 5 GiB überschreitet. Wenn Sie eine Neuinstallation von StorageGRID 11.7 oder 11.8 haben, wird der Alarm in diesem Fall nicht ausgelöst. Um jedoch dem AWS S3-Standard zu entsprechen, werden zukünftige Versionen von StorageGRID keine Uploads von Objekten unterstützen, die größer als 5 GiB sind.

UTF-8-Zeichen in Benutzermetadaten

Wenn eine Anfrage (nicht maskierte) UTF-8-Werte im Schlüsselnamen oder Wert benutzerdefinierter

Metadaten enthält, ist das StorageGRID Verhalten undefiniert.

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen, die im Schlüsselnamen oder -wert benutzerdefinierter Metadaten enthalten sind. Escape-UTF-8-Zeichen werden als ASCII-Zeichen behandelt:

- Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten Escape-UTF-8-Zeichen enthalten.
- StorageGRID gibt nicht zurück `x-amz-missing-meta` Header, wenn der interpretierte Wert des Schlüsselnamens oder -werts nicht druckbare Zeichen enthält.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader 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` , wodurch Sie das Objekt und die zugehörigen Metadaten kopieren können.

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

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Der Standardwert ist `COPY` , wodurch 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 Object Lock-Anforderungsheader:
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um den Objektversionsmodus und das Aufbewahrungsdatum zu berechnen. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

- SSE-Anforderungsheader:
  - `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`

  SehenAnforderungsheader für serverseitige Verschlüsselung

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Wenn Sie ein Objekt kopieren und das Quellobjekt eine Prüfsumme hat, kopiert StorageGRID diesen Prüfsummenwert nicht in das neue Objekt. Dieses Verhalten gilt unabhängig davon, ob Sie versuchen, `x-amz-checksum-algorithm` in der Objektanforderung.

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

Speicherklassenoptionen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und beeinflusst, wie viele Objektkopien StorageGRID erstellt, wenn die entsprechende ILM-Regel Dual Commit oder Balanced verwendet."Aufnahmeoption" .

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

Verwenden von x-amz-copy-source in CopyObject

Wenn der Quell-Bucket und -Schlüssel, angegeben in `x-amz-copy-source` Header, unterscheiden sich vom Ziel-Bucket und -Schlüssel, eine Kopie der Quellobjektdaten wird in das Ziel geschrieben.

Wenn Quelle und Ziel übereinstimmen und die `x-amz-metadata-directive` Der Header wird wie folgt angegeben: `REPLACE` , werden die Metadaten des Objekts mit den in der Anfrage angegebenen Metadatenwerten aktualisiert. In diesem Fall nimmt StorageGRID das Objekt nicht erneut auf. Dies hat zwei wichtige Konsequenzen:

- Sie können CopyObject nicht verwenden, um ein vorhandenes Objekt vor Ort zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts vor Ort zu ändern. Wenn Sie die `x-amz-server-side-encryption` Kopfzeile oder die `x-amz-server-side-encryption-customer-algorithm` Header, StorageGRID lehnt die Anfrage ab und gibt zurück `XNotImplemented` .
- Die in der entsprechenden ILM-Regel angegebene Option für das Aufnahmeverhalten wird nicht verwendet. Alle durch die Aktualisierung ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird.

  Dies bedeutet, dass keine Aktion ausgeführt wird, wenn die ILM-Regel die Option „Streng“ für das Aufnahmeverhalten verwendet und die erforderlichen Objektplatzierungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.

Anforderungsheader für serverseitige Verschlüsselung

Wenn du"Verwenden Sie serverseitige Verschlüsselung" , die von Ihnen bereitgestellten Anforderungsheader hängen davon ab, ob das Quellobjekt verschlüsselt ist und ob Sie das Zielobjekt verschlüsseln möchten.

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

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

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

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

Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie die `x-amz-copy-source` Header, um die neueste Version eines Objekts zu kopieren. Um eine bestimmte Version eines Objekts zu kopieren, müssen Sie die zu kopierende Version explizit angeben, indem Sie `versionId` Unterressource. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im `x-amz-version-id` Antwortheader. Wenn die Versionierung für den Ziel-Bucket ausgesetzt ist, dann `x-amz-version-id` gibt einen „Null“-Wert zurück.

GetObject

Sie können die S3 GetObject-Anforderung verwenden, um ein Objekt aus einem S3-Bucket abzurufen.

GetObject und mehrteilige Objekte

Sie können die `partNumber` Anforderungsparameter zum Abrufen eines bestimmten Teils eines mehrteiligen oder segmentierten Objekts. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, aus wie vielen Teilen das Objekt besteht.

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

UTF-8-Zeichen in Benutzermetadaten

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten. GET-Anfragen für ein Objekt mit Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten geben nicht die `x-amz-missing-meta` Header, wenn der Schlüsselname oder -wert nicht druckbare Zeichen enthält.

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode`: Angeben `ENABLED`

  Der `Range` Header wird nicht unterstützt mit `x-amz-checksum-mode` für GetObject. Wenn Sie `Range` in der Anfrage mit `x-amz-checksum-mode` aktiviert ist, gibt StorageGRID in der Antwort keinen Prüfsummenwert zurück.

Nicht unterstützter Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt und gibt zurück `XNotImplemented` :

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

Versionierung

Wenn ein `versionId` Wenn keine Unterressource angegeben ist, ruft der Vorgang die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "Nicht gefunden" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .

Anforderungsheader für die serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)

Verwenden Sie alle drei Header, wenn das Objekt mit einem von Ihnen bereitgestellten eindeutigen Schlüssel verschlüsselt ist.

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `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 bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

Verhalten von GetObject für Cloud Storage Pool-Objekte

Wenn ein Objekt in einem"Cloud-Speicherpool" , das Verhalten einer GetObject-Anforderung hängt vom Status des Objekts ab. Sehen"HeadObject" für weitere Details.

> Wenn ein Objekt in einem Cloud-Speicherpool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Raster vorhanden sind, versuchen GetObject-Anfragen, Daten aus dem Raster abzurufen, bevor sie aus dem Cloud-Speicherpool abgerufen werden.

Zustand des Objekts	Verhalten von GetObject
In StorageGRID aufgenommenes, aber noch nicht von ILM ausgewertetes Objekt oder Objekt, das in einem herkömmlichen Speicherpool oder mithilfe von Erasure Coding gespeichert ist	`200 OK` Eine Kopie des Objekts wird abgerufen.
Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK` Eine Kopie des Objekts wird abgerufen.
Objekt in einen nicht abrufbaren Zustand überführt	`403 Forbidden` , `InvalidObjectState` Verwenden Sie ein"RestoreObject" Anforderung zum Wiederherstellen des Objekts in einen abrufbaren Zustand.

Zustand des Objekts	Verhalten von GetObject
Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`403 Forbidden` , `InvalidObjectState` Warten Sie, bis die RestoreObject-Anforderung abgeschlossen ist.
Objekt vollständig im Cloud-Speicherpool wiederhergestellt	`200 OK` Eine Kopie des Objekts wird abgerufen.

Mehrteilige oder segmentierte Objekte in einem Cloud-Speicherpool

Wenn Sie ein mehrteiliges Objekt hochgeladen haben oder StorageGRID ein großes Objekt in Segmente aufgeteilt hat, ermittelt StorageGRID , ob das Objekt im Cloud Storage Pool verfügbar ist, indem es eine Teilmenge der Teile oder Segmente des Objekts auswählt. In einigen Fällen kann eine GetObject-Anforderung fälschlicherweise zurückgeben `200 OK` wenn einige Teile des Objekts bereits in einen nicht abrufbaren Zustand überführt wurden oder wenn einige Teile des Objekts noch nicht wiederhergestellt wurden.

In diesen Fällen:

- Die GetObject-Anforderung gibt möglicherweise einige Daten zurück, stoppt jedoch mitten in der Übertragung.
- Eine nachfolgende GetObject-Anforderung könnte `403 Forbidden` .

GetObject und Cross-Grid-Replikation

Wenn Sie"Netzverbund" Und"Cross-Grid-Replikation" für einen Bucket aktiviert ist, kann der S3-Client den Replikationsstatus eines Objekts überprüfen, indem er eine GetObject-Anforderung ausgibt. Die Antwort enthält die StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte hat:

Netz	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war erfolgreich. • **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert. • **FEHLER**: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	**REPLICA**: Das Objekt wurde aus dem Quellraster repliziert.

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

HeadObject

Sie können die S3 HeadObject-Anforderung verwenden, um Metadaten aus einem Objekt abzurufen, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem

Cloud-Speicherpool gespeichert ist, können Sie HeadObject verwenden, um den Übergangszustand des Objekts zu bestimmen.

HeadObject und mehrteilige Objekte

Sie können die `partNumber` Anforderungsparameter zum Abrufen von Metadaten für einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts. Der `x-amz-mp-parts-count` Das Antwortelement gibt an, aus wie vielen Teilen das Objekt besteht.

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

UTF-8-Zeichen in Benutzermetadaten

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten. HEAD-Anfragen für ein Objekt mit Escape-UTF-8-Zeichen in benutzerdefinierten Metadaten geben nicht das `x-amz-missing-meta` Header, wenn der Schlüsselname oder -wert nicht druckbare Zeichen enthält.

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode`

  Der `partNumber` Parameter und `Range` Header werden nicht unterstützt mit `x-amz-checksum-mode` für HeadObject. Wenn Sie sie in die Anfrage aufnehmen mit `x-amz-checksum-mode` aktiviert ist, gibt StorageGRID in der Antwort keinen Prüfsummenwert zurück.

Nicht unterstützter Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt und gibt zurück `XNotImplemented` :

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

Versionierung

Wenn ein `versionId` Wenn keine Unterressource angegeben ist, ruft der Vorgang die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird der Status "Nicht gefunden" mit der `x-amz-delete-marker` Antwortheader gesetzt auf `true` .

Anforderungsheader für die serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)

Verwenden Sie alle drei Header, wenn das Objekt mit einem von Ihnen bereitgestellten eindeutigen Schlüssel verschlüsselt ist.

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `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 bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in"Verwenden Sie serverseitige Verschlüsselung" .

HeadObject-Antworten für Cloud Storage Pool-Objekte

Wenn das Objekt in einem"Cloud-Speicherpool" werden die folgenden Antwortheader zurückgegeben:

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

Die Antwortheader liefern Informationen über den Status eines Objekts, wenn es in einen Cloud-Speicherpool verschoben, optional in einen nicht abrufbaren Status versetzt und wiederhergestellt wird.

Zustand des Objekts	Antwort auf HeadObject
In StorageGRID aufgenommenes, aber noch nicht von ILM ausgewertetes Objekt oder Objekt, das in einem herkömmlichen Speicherpool oder mithilfe von Erasure Coding gespeichert ist	`200 OK`(Es wird kein spezieller Antwortheader zurückgegeben.)

Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Bis das Objekt in einen nicht abrufbaren Zustand überführt wird, ist der Wert für `expiry-date` ist auf einen fernen Zeitpunkt in der Zukunft festgelegt. Der genaue Zeitpunkt des Übergangs wird vom StorageGRID -System nicht gesteuert.

Zustand des Objekts	Antwort auf HeadObject

Das Objekt ist in den nicht abrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Raster vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Der Wert für `expiry-date` ist auf einen fernen Zeitpunkt in der Zukunft festgelegt.
	
	Hinweis: Wenn die Kopie im Grid nicht verfügbar ist (z. B. weil ein Storage Node ausgefallen ist), müssen Sie eine"RestoreObject" Fordern Sie die Wiederherstellung der Kopie aus dem Cloud-Speicherpool an, bevor Sie das Objekt erfolgreich abrufen können.

Das Objekt ist in einen nicht abrufbaren Zustand übergegangen und es ist keine Kopie im Raster vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

Objekt vollständig im Cloud-Speicherpool 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-Speicherpool in einen nicht abrufbaren Zustand zurückversetzt wird.

Mehrteilige oder segmentierte Objekte im Cloud Storage Pool

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

HeadObject und Cross-Grid-Replikation

Wenn Sie"Netzverbund" Und"Cross-Grid-Replikation" für einen Bucket aktiviert ist, kann der S3-Client den Replikationsstatus eines Objekts überprüfen, indem er eine HeadObject-Anforderung ausgibt. Die Antwort enthält die StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte hat:

Netz	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: Die Replikation war erfolgreich. • **AUSSTEHEND**: Das Objekt wurde noch nicht repliziert. • **FEHLER**: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	**REPLICA**: Das Objekt wurde aus dem Quellraster repliziert.

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

PutObject

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

Konflikte lösen

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

Objektgröße

Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie"mehrteiliger Upload" stattdessen.

Die maximal *unterstützte* Größe für einen einzelnen PutObject-Vorgang beträgt 5 TiB (5.497.558.138.880 Bytes).

Wenn Sie ein Upgrade von StorageGRID 11.6 oder früher durchgeführt haben, wird die Warnung „S3 PUT-Objektgröße zu groß“ ausgelöst, wenn Sie versuchen, ein Objekt hochzuladen, das 5 GiB überschreitet. Wenn Sie eine Neuinstallation von StorageGRID 11.7 oder 11.8 haben, wird der Alarm in diesem Fall nicht ausgelöst. Um jedoch dem AWS S3-Standard zu entsprechen, werden zukünftige Versionen von StorageGRID keine Uploads von Objekten unterstützen, die größer als 5 GiB sind.

Größe der Benutzermetadaten

Amazon S3 begrenzt die Größe benutzerdefinierter Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB. StorageGRID begrenzt Benutzermetadaten auf 24 KiB. Die Größe benutzerdefinierter Metadaten wird

gemessen, indem die Summe der Anzahl der Bytes in der UTF-8-Kodierung jedes Schlüssels und Werts berechnet wird.

UTF-8-Zeichen in Benutzermetadaten

Wenn eine Anfrage (nicht maskierte) UTF-8-Werte im Schlüsselnamen oder Wert benutzerdefinierter Metadaten enthält, ist das StorageGRID Verhalten undefiniert.

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen, die im Schlüsselnamen oder -wert benutzerdefinierter Metadaten enthalten sind. Escape-UTF-8-Zeichen werden als ASCII-Zeichen behandelt:

- PutObject-, CopyObject-, GetObject- und HeadObject-Anfragen sind erfolgreich, wenn benutzerdefinierte Metadaten Escape-UTF-8-Zeichen enthalten.
- StorageGRID gibt nicht zurück `x-amz-missing-meta` Header, wenn der interpretierte Wert des Schlüsselnamens oder -werts nicht druckbare Zeichen enthält.

Objekt-Tag-Grenzwerte

Sie können neuen Objekten beim Hochladen Tags hinzufügen oder Sie können sie vorhandenen Objekten hinzufügen. Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Mit einem Objekt verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden.

Objektbesitz

In StorageGRID sind alle Objekte Eigentum des Bucket-Eigentümerkontos, einschließlich der Objekte, die von einem Nicht-Eigentümerkonto oder einem anonymen Benutzer erstellt wurden.

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

  Wenn Sie angeben `aws-chunked` für`Content-Encoding` StorageGRID überprüft die folgenden Punkte nicht:

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

- `Transfer-Encoding`

  Chunked Transfer Encoding wird unterstützt, wenn `aws-chunked` Außerdem wird eine Nutzlastsignatur verwendet.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten.

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

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

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

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

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

  > Eine ILM-Regel kann nicht sowohl eine **benutzerdefinierte Erstellungszeit** für die Referenzzeit als auch die Aufnahmeoption „Ausgewogen“ oder „Streng“ verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

- `x-amz-tagging`
- S3 Object Lock-Anforderungsheader
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Wenn eine Anfrage ohne diese Header gestellt wird, werden die Bucket-Standardaufbewahrungseinstellungen verwendet, um den Objektversionsmodus und das Aufbewahrungsdatum zu berechnen. Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

- SSE-Anforderungsheader:
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    SehenAnforderungsheader für serverseitige Verschlüsselung

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

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

Speicherklassenoptionen

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

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die Option „Strenge Aufnahme“ verwendet, `x-amz-storage-class` Header hat keine Wirkung.

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

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

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

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

  Verwenden des `REDUCED_REDUNDANCY` Unter anderen Umständen wird diese Option nicht empfohlen. `REDUCED_REDUNDANCY` erhöht das Risiko eines Objektdatenverlusts während der Aufnahme.

Beispielsweise können Daten verloren gehen, wenn die einzelne Kopie zunächst auf einem Speicherknoten gespeichert wird, der ausfällt, bevor die ILM-Auswertung erfolgen kann.

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

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

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

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, von StorageGRID verwalteten Schlüssel verschlüsseln möchten.
  - `x-amz-server-side-encryption`

    Wenn die `x-amz-server-side-encryption` Header ist nicht in der PutObject-Anforderung enthalten, der rasterweite"Einstellung für die Verschlüsselung gespeicherter Objekte" wird aus der PutObject-Antwort weggelassen.

- **SSE-C**: Verwenden Sie alle drei Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

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

> Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Versionierung

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

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

Signaturberechnungen für den Autorisierungsheader

Bei Verwendung der `Authorization` Header zur Authentifizierung von Anfragen. StorageGRID unterscheidet sich in folgenden Punkten von AWS:

- StorageGRID erfordert nicht `host` Header, die in `CanonicalHeaders` .
- StorageGRID erfordert nicht `Content-Type` eingeschlossen sein in `CanonicalHeaders` .
- StorageGRID erfordert nicht `x-amz-*` Header, die in `CanonicalHeaders` .

> Als allgemeine Best Practice sollten Sie diese Header immer in `CanonicalHeaders` um sicherzustellen, dass sie überprüft werden. Wenn Sie diese Header jedoch ausschließen, gibt StorageGRID keinen Fehler zurück.

Weitere Einzelheiten finden Sie unter "Signaturberechnungen für den Autorisierungsheader: Übertragen der Nutzlast in einem einzigen Block (AWS-Signaturversion 4)" .

Ähnliche Informationen

- "Objekte mit ILM verwalten"
- "Amazon Simple Storage Service API-Referenz: PutObject"

RestoreObject

Sie können die S3 RestoreObject-Anforderung verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Speicherpool gespeichert ist.

Unterstützter Anfragetyp

StorageGRID unterstützt nur RestoreObject-Anfragen zum Wiederherstellen eines Objekts. Es unterstützt nicht die `SELECT` Art der Restaurierung. Wählen Sie Anfragen zurück `XNotImplemented` .

Versionierung

Geben Sie optional an `versionId` um eine bestimmte Version eines Objekts in einem versionierten Bucket wiederherzustellen. Wenn Sie nicht angeben `versionId` wird die aktuellste Version des Objekts wiederhergestellt

Verhalten von RestoreObject bei Cloud Storage Pool-Objekten

Wenn ein Objekt in einem"Cloud-Speicherpool" , eine RestoreObject-Anforderung weist basierend auf dem Status des Objekts das folgende Verhalten auf. Sehen"HeadObject" für weitere Details.

Wenn ein Objekt in einem Cloud-Speicherpool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

Zustand des Objekts	Verhalten von RestoreObject
Objekt in StorageGRID aufgenommen, aber noch nicht von ILM ausgewertet, oder Objekt befindet sich nicht in einem Cloud-Speicherpool	`403 Forbidden` , `InvalidObjectState`
Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	`200 OK`Es werden keine Änderungen vorgenommen. **Hinweis**: Bevor ein Objekt in einen nicht abrufbaren Zustand überführt wurde, können Sie seine `expiry-date` .
Objekt in einen nicht abrufbaren Zustand überführt	`202 Accepted`Stellt eine abrufbare Kopie des Objekts für die im Anforderungstext angegebene Anzahl von Tagen im Cloud-Speicherpool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht abrufbaren Zustand zurückversetzt. Optional können Sie die `Tier` Anforderungselement, um zu bestimmen, wie lange es dauert, bis der Wiederherstellungsjob abgeschlossen ist(`Expedited` , `Standard` , oder `Bulk`). Wenn Sie nicht angeben `Tier` , Die `Standard` Ebene verwendet wird. **Wichtig**: Wenn ein Objekt in das S3 Glacier Deep Archive verschoben wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, können Sie es nicht mit dem `Expedited` Stufe. Der folgende Fehler wird zurückgegeben `403 Forbidden` , `InvalidTier` : `Retrieval option is not supported by this storage class.`
Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	`409 Conflict` , `RestoreAlreadyInProgress`
Objekt vollständig im Cloud-Speicherpool wiederhergestellt	`200 OK` **Hinweis:** Wenn ein Objekt in einen abrufbaren Zustand zurückversetzt wurde, können Sie seine `expiry-date` durch erneutes Ausgeben der RestoreObject-Anforderung mit einem neuen Wert für `Days` . Das Wiederherstellungsdatum wird relativ zum Zeitpunkt der Anfrage aktualisiert.

SelectObjectContent

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

Weitere Informationen finden Sie unter "Amazon Simple Storage Service API-Referenz: SelectObjectContent" .

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung „S3 Select“.
- Du hast `s3:GetObject` Berechtigung für das Objekt, das Sie abfragen möchten.
- Das abzufragende Objekt muss eines der folgenden Formate aufweisen:
  - **CSV**. Kann unverändert verwendet oder in GZIP- oder BZIP2-Archive komprimiert werden.
  - **Parkett**. Zusätzliche Anforderungen für Parquet-Objekte:
    - S3 Select unterstützt nur spaltenweise Komprimierung mit GZIP oder Snappy. S3 Select unterstützt keine Ganzobjektkomprimierung für Parquet-Objekte.
    - S3 Select unterstützt keine Parquet-Ausgabe. Sie müssen das Ausgabeformat als CSV oder JSON angeben.
    - Die maximale unkomprimierte Zeilengruppengröße beträgt 512 MB.
    - Sie müssen die im Schema des Objekts angegebenen Datentypen verwenden.
    - Sie können die logischen Typen INTERVAL, JSON, LIST, TIME oder UUID nicht verwenden.
- Ihr SQL-Ausdruck hat eine maximale Länge von 256 KB.
- Jeder Datensatz in der Eingabe oder den Ergebnissen hat eine maximale Länge von 1 MiB.

Beispiel für die CSV-Anforderungssyntax

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Beispiel für die Parquet-Anforderungssyntax

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

SQL-Abfragebeispiel

Diese Abfrage ermittelt den Namen des Bundesstaates, die Bevölkerungszahlen von 2010, die geschätzten Bevölkerungszahlen von 2015 und die prozentuale Veränderung gegenüber den US-Volkszählungsdaten. Datensätze in der Datei, die keine Zustände sind, werden ignoriert.

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

Die ersten Zeilen der abzufragenden Datei, `SUB-EST2020_ALL.csv` , sehen so aus:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

AWS-CLI-Nutzungsbeispiel (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Die ersten paar Zeilen der Ausgabedatei, `changes.csv` , sehen so aus:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

AWS-CLI-Nutzungsbeispiel (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Die ersten Zeilen der Ausgabedatei changes.csv sehen folgendermaßen aus:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Vorgänge für mehrteilige Uploads

Vorgänge für mehrteilige Uploads

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

Für alle mehrteiligen Uploadvorgänge gelten die folgenden Bedingungen und Hinweise:

- Sie sollten nicht mehr als 1.000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse von ListMultipartUploads-Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse zurückgeben.
- StorageGRID erzwingt AWS-Größenbeschränkungen für mehrteilige Teile. S3-Clients müssen diese Richtlinien befolgen:
  - Jeder Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5.242.880 Bytes) und 5 GiB (5.368.709.120 Bytes) groß sein.
  - Der letzte Teil kann kleiner als 5 MiB (5.242.880 Bytes) sein.
  - Generell sollten die Teilegrößen möglichst groß sein. Verwenden Sie beispielsweise Teilgrößen von 5 GiB für ein 100-GiB-Objekt. Da jedes Teil als einzigartiges Objekt betrachtet wird, reduziert die Verwendung großer Teilegrößen den StorageGRID Metadaten-Overhead.
  - Erwägen Sie für Objekte, die kleiner als 5 GiB sind, stattdessen die Verwendung eines nicht mehrteiligen Uploads.
- ILM wird für jeden Teil eines mehrteiligen Objekts ausgewertet, wenn es aufgenommen wird, und für das Objekt als Ganzes, wenn der mehrteilige Upload abgeschlossen ist, wenn die ILM-Regel die Balanced- oder Strict-Regel verwendet."Aufnahmeoption" . Sie sollten sich darüber im Klaren sein, welche Auswirkungen dies auf die Platzierung von Objekten und Teilen hat:

- Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert, erfüllen einige Teile des Objekts nach Abschluss des Multipart-Uploads möglicherweise nicht die aktuellen ILM-Anforderungen. Alle Teile, die nicht richtig platziert sind, werden zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.
- Bei der Auswertung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei der Aufnahme bei DC2 gespeichert. Wenn ILM jedoch für das gesamte Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.

- Alle mehrteiligen Upload-Vorgänge unterstützen StorageGRID"Konsistenzwerte" .
- Wenn ein Objekt per mehrteiligem Upload aufgenommen wird,"Schwellenwert für Objektsegmentierung (1 GiB)" wird nicht angewendet.
- Bei Bedarf können Sie"serverseitige Verschlüsselung" mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit StorageGRID-verwalteten Schlüsseln) zu verwenden, schließen Sie die `x-amz-server-side-encryption` Anforderungsheader nur in der CreateMultipartUpload-Anforderung. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der CreateMultipartUpload-Anforderung und in jeder nachfolgenden UploadPart-Anforderung dieselben drei Anforderungsheader für Verschlüsselungsschlüssel an.

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

CompleteMultipartUpload

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

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

Konflikte lösen

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

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

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

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

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

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

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

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

Weitere Informationen finden Sie unter "Fehlerbehebung bei Plattformdiensten" .

CreateMultipartUpload

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

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

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

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

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

werden.

- **Ausgeglichen**: Wenn die ILM-Regel die Option „Ausgeglichen“ angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

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

- `REDUCED_REDUNDANCY`

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

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

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

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

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

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

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

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

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

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

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

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

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

- S3 Object Lock-Anforderungsheader:

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

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

  "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"

- SSE-Anforderungsheader:

  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Anforderungsheader für serverseitige Verschlüsselung

  > Informationen zur Verarbeitung von UTF-8-Zeichen durch StorageGRID finden Sie unter"PutObject" .

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteiliges Objekt mit serverseitiger

Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE**: Verwenden Sie den folgenden Header in der CreateMultipartUpload-Anforderung, wenn Sie das Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel verschlüsseln möchten. Geben Sie diesen Header in keiner der UploadPart-Anfragen an.
  - `x-amz-server-side-encryption`
- **SSE-C**: Verwenden Sie alle drei dieser Header in der CreateMultipartUpload-Anfrage (und in jeder nachfolgenden UploadPart-Anfrage), wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
  - `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

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

Nicht unterstützte Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt:

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

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

Versionierung

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

ListMultipartUploads

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

Die folgenden Anforderungsparameter werden unterstützt:

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

- `Date`
- `Authorization`

Versionierung

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

UploadPart

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

Anforderungsheader für serverseitige Verschlüsselung

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

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

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

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

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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

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

UploadPartCopy

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

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

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

Die folgenden Anforderungsheader werden unterstützt:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Anforderungsheader für serverseitige Verschlüsselung

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

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

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

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

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

Versionierung

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

Fehlerantworten

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

Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
Zugriff verweigert	403 Verboten
BadDigest	400 Ungültige Anfrage
BucketExistsAlready	409 Konflikt
EimerNichtLeer	409 Konflikt
Unvollständiger Körper	400 Ungültige Anfrage
Interner Fehler	500 Interner Serverfehler
Ungültige Zugriffsschlüssel-ID	403 Verboten
Ungültiges Argument	400 Ungültige Anfrage
Ungültiger BucketName	400 Ungültige Anfrage
Ungültiger BucketState	409 Konflikt
InvalidDigest	400 Ungültige Anfrage
Fehler „Ungültiger Verschlüsselungsalgorithmus“	400 Ungültige Anfrage
UngültigesTeil	400 Ungültige Anfrage
UngültigeTeilebestellung	400 Ungültige Anfrage
Ungültiger Bereich	416 Angeforderter Bereich nicht erfüllbar

Name	HTTP-Status
Ungültige Anfrage	400 Ungültige Anfrage
Ungültige Speicherklasse	400 Ungültige Anfrage
Ungültiges Tag	400 Ungültige Anfrage
Ungültige URI	400 Ungültige Anfrage
Schlüssel zu lang	400 Ungültige Anfrage
MalformedXML	400 Ungültige Anfrage
Metadaten zu groß	400 Ungültige Anfrage
MethodeNichtZulässig	405 Methode nicht zulässig
MissingContentLength	411 Erforderliche Länge
MissingRequestBodyError	400 Ungültige Anfrage
MissingSecurityHeader	400 Ungültige Anfrage
KeinSuchBucket	404 Nicht gefunden
NoSuchKey	404 Nicht gefunden
NoSuchUpload	404 Nicht gefunden
Nicht implementiert	501 Nicht implementiert
NoSuchBucketPolicy	404 Nicht gefunden
ObjectLockConfigurationNotFoundError	404 Nicht gefunden
Vorbedingung fehlgeschlagen	412 Vorbedingung fehlgeschlagen
RequestTimeTooSkewed	403 Verboten
Dienst nicht verfügbar	503 Dienst nicht verfügbar
Signatur stimmt nicht überein	403 Verboten
Zu viele Eimer	400 Ungültige Anfrage

Name	HTTP-Status
Benutzerschlüssel muss angegeben werden	400 Ungültige Anfrage

Benutzerdefinierte StorageGRID -Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecycleNotAllowed	Die Bucket-Lebenszykluskonfiguration ist in einem älteren konformen Bucket nicht zulässig	400 Ungültige Anfrage
XBucketPolicyParseException	Das Parsen der empfangenen Bucket-Richtlinien-JSON ist fehlgeschlagen.	400 Ungültige Anfrage
XComplianceConflict	Vorgang aufgrund veralteter Compliance-Einstellungen abgelehnt.	403 Verboten
XComplianceReduzierteRedundanzVerboten	Reduzierte Redundanz ist im Legacy-Compliant-Bucket nicht zulässig	400 Ungültige Anfrage
XMaxBucketPolicyLengthExceeded	Ihre Richtlinie überschreitet die maximal zulässige Bucket-Richtlinienlänge.	400 Ungültige Anfrage
XMissingInternalRequestHeader	Es fehlt ein Header einer internen Anfrage.	400 Ungültige Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die Legacy-Compliance nicht aktiviert.	404 Nicht gefunden
XNichtAkzeptabel	Die Anfrage enthält einen oder mehrere Accept-Header, die nicht erfüllt werden konnten.	406 Nicht akzeptabel
XNotImplemented	Die von Ihnen angegebene Anfrage impliziert eine Funktionalität, die nicht implementiert ist.	501 Nicht implementiert